

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

FINJAN, INC., a Delaware Corporation,)	
)	
Plaintiff,)	
)	
v.)	C.A. No.
)	
RAPID7, INC., a Delaware Corporation)	JURY TRIAL DEMANDED
and RAPID7 LLC, a Delaware Limited)	
Liability Company,)	
)	
Defendants.)	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Finjan, Inc. (“Finjan”) files this Complaint for Patent Infringement and Demand for Jury Trial against Rapid7, Inc. and Rapid7 LLC (collectively, “Defendants” or “Rapid7”) and alleges as follows:

THE PARTIES

1. Finjan is a Delaware Corporation with its principal place of business at 2000 University Avenue, Suite 600, E. Palo Alto, California 94303.
2. Rapid7, Inc. is a Delaware Corporation with its principal place of business at 100 Summer Street, Boston, Massachusetts.
3. Rapid7 LLC is a Delaware limited liability company and a wholly-owned subsidiary of Rapid7, Inc. with its principal place of business at 100 Summer Street, Boston, Massachusetts.

JURISDICTION AND VENUE

4. This action arises under the Patent Act, 35 U.S.C. § 101 *et seq.* This Court has original jurisdiction over this controversy pursuant to 28 U.S.C. §§ 1331 and 1338.

5. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(b) and (c) and 1400(b).

6. This Court has personal jurisdiction over Defendants. Defendants are organized under the laws of Delaware. In addition, the Court has personal jurisdiction over Defendants because Defendants have established minimum contacts with the forum and the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice.

FINJAN'S INNOVATIONS

7. Finjan was founded in 1997 as a wholly-owned subsidiary of Finjan Software Ltd., an Israeli corporation. In 1998, Finjan moved its headquarters to San Jose, California. Finjan was a pioneer in developing proactive security technologies capable of detecting previously unknown and emerging online security threats, recognized today under the umbrella term “malware.” These technologies protect networks and endpoints by identifying suspicious patterns and behaviors of content delivered over the Internet. The United States Patent and Trademark Office (“USPTO”) has awarded Finjan, and Finjan continues to prosecute, numerous patents covering innovations in the United States and around the world resulting directly from Finjan’s more than decades-long research and development efforts, supported by a dozen inventors and over \$65 million in R&D investments.

8. Finjan built and sold software, including application program interfaces (APIs) and appliances for network security, using its patented technologies. Finjan’s licensing partners continue to support these products and related customers. At its height, Finjan employed nearly 150 employees around the world, building and selling security products and operating the Malicious Code Research Center, through which it frequently published research regarding network security and current threats on the Internet. Finjan’s pioneering approach to online

security drew equity investments from two major software and technology companies, the first in 2005 followed by the second in 2006. Finjan generated millions of dollars in product sales and related services and support revenues through 2009, when it spun off certain hardware and technology assets in a merger. Pursuant to this merger, Finjan was bound to a non-compete and confidentiality agreement, under which it could not make or sell a competing product or disclose the existence of the non-compete clause. Finjan became a publicly traded company in June 2013, capitalized with \$30 million. After Finjan's obligations under the non-compete and confidentiality agreement expired in March 2015, Finjan re-entered the development and production sector of secure mobile products for the consumer market.

FINJAN'S ASSERTED PATENTS

9. On July 5, 2011, the USPTO issued to Moshe Rubin, Moshe Matitya, Artem Melnick, Shlomo Touboul, Alexander Yermakov and Amit Shaked U.S. Patent No. 7,975,305 ("the '305 Patent"), titled METHOD AND SYSTEM FOR ADAPTIVE RULE-BASED CONTENT SCANNERS FOR DESKTOP COMPUTERS. A true and correct copy of the '305 Patent is attached to this Complaint as Exhibit 1 and is incorporated by reference herein.

10. All rights, title, and interest in the '305 Patent have been assigned to Finjan, who is the sole owner of the '305 Patent. Finjan has been the sole owner of the '305 Patent since its issuance.

11. The '305 Patent is generally directed towards network security and, in particular, rule based scanning of web-based content for exploits. One of the ways this is accomplished is by using parser and analyzer rules to describe computer exploits as patterns of types of tokens. Additionally, the system provides a way to keep these rules updated. The '305 Patent discloses and specifically claims inventive concepts that represent significant improvements over

conventional network security technology that was available at the time of filing of the '305 Patent and are more than just generic software components performing conventional activities.

12. On July 17, 2012, the USPTO issued to Moshe Rubin, Moshe Matitya, Artem Melnick, Shlomo Touboul, Alexander Yermakov and Amit Shaked U.S. Patent No. 8,225,408 ("the '408 Patent"), titled METHOD AND SYSTEM FOR ADAPTIVE RULE-BASED CONTENT SCANNERS. A true and correct copy of the '408 Patent is attached to this Complaint as Exhibit 2 and is incorporated by reference herein.

13. All rights, title, and interest in the '408 Patent have been assigned to Finjan, who is the sole owner of the '408 Patent. Finjan has been the sole owner of the '408 Patent since its issuance.

14. The '408 Patent is generally directed towards network security and, in particular, rule based scanning of web-based content for a variety of exploits written in different programming languages. One of the ways this is accomplished is by expressing the exploits as patterns of tokens. Additionally, the disclosed system provides a way to analyze these exploits by using a parse tree. The '408 Patent discloses and specifically claims inventive concepts that represent significant improvements over conventional network security technology that was available at the time of filing of the '408 Patent and are more than just generic software components performing conventional activities

15. On July 13, 2010, the USPTO issued to David Gruzman and Yuval Ben-Itzhak U.S. Patent No. 7,757,289 ("the '289 Patent"), titled SYSTEM AND METHOD FOR INSPECTING DYNAMICALLY GENERATED EXECUTABLE CODE. A true and correct copy of the '289 Patent is attached to this Complaint as Exhibit 3 and is incorporated by reference herein.

16. All rights, title, and interest in the '289 Patent have been assigned to Finjan, who is the sole owner of the '289 Patent. Finjan has been the sole owner of the '289 Patent since its issuance.

17. The '289 Patent is generally directed towards a system and method for inspecting dynamically generated executable code. The claims generally cover receiving content with an original call function and replacing the original call function with a substitute call function, and then determining whether it is safe to invoke the original call function. The '289 Patent discloses and specifically claims inventive concepts that represent significant improvements over conventional network security technology that was available at the time of filing of the '289 Patent and are more than just generic software components performing conventional activities.

18. On November 3, 2009, the USPTO issued to Yuval Ben-Itzhak U.S. Patent No. 7,613,918 ("the '918 Patent"), titled SYSTEM AND METHOD FOR ENFORCING A SECURITY CONTEXT ON A DOWNLOADABLE. A true and correct copy of the '918 Patent is attached to this Complaint as Exhibit 4 and is incorporated by reference herein.

19. All rights, title, and interest in the '918 Patent have been assigned to Finjan, who is the sole owner of the '918 Patent. Finjan has been the sole owner of the '918 Patent since its issuance.

20. The '918 Patent is generally directed towards a system and method for enforcing a security context on a Downloadable. One way this is accomplished is by making use of security contexts that are associated within certain user/group computer accounts when deriving a profile for code received from the Internet. The '918 Patent discloses and specifically claims inventive concepts that represent significant improvements over conventional network security

technology that was available at the time of filing of the '918 Patent and are more than just generic software components performing conventional activities.

21. On December 13, 2011, the USPTO issued to Yigal Mordechai Edery, Nimrod Itzhak Vered, David R. Kroll and Shlomo Touboul U.S. Patent No. 8,079,086 ("the '086 Patent"), titled MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS. A true and correct copy of the '086 Patent is attached to this Complaint as Exhibit 5 and is incorporated by reference herein.

22. All rights, title, and interest in the '086 Patent have been assigned to Finjan, who is the sole owner of the '086 Patent. Finjan has been the sole owner of the '086 Patent since its issuance.

23. The '086 Patent is generally directed towards computer networks and, more particularly, provides a system that protects devices connected to the Internet from undesirable operations from web-based content. One of the ways this is accomplished is by creating a profile of the web-based content and sending these profiles and corresponding web-content to another computer for appropriate action. The '086 Patent discloses and specifically claims inventive concepts that represent significant improvements over conventional network security technology that was available at the time of filing of the '086 Patent and are more than just generic software components performing conventional activities.

24. On March 20, 2012, the USPTO issued to David Gruzman and Yuval Ben-Itzhak U.S. Patent No. 8,141,154 ("the '154 Patent"), titled SYSTEM AND METHOD FOR INSPECTING DYNAMICALLY GENERATED EXECUTABLE CODE. A true and correct copy of the '154 Patent is attached to this Complaint as Exhibit 6 and is incorporated by reference herein.

25. All rights, title, and interest in the '154 Patent have been assigned to Finjan, who is the sole owner of the '154 Patent. Finjan has been the sole owner of the '154 Patent since its issuance.

26. The '154 Patent is generally directed towards a gateway computer protecting a client computer from dynamically generated malicious content. One of the ways this is accomplished is by using a content processor to process a first function and invoke a second function if a security computer indicates that it is safe to invoke the second function. The '154 Patent discloses and specifically claims inventive concepts that represent significant improvements over conventional network security technology that was available at the time of filing of the '154 Patent and are more than just generic software components performing conventional activities.

27. On March 18, 2014, the USPTO issued to Yigal Mordechai Edery, Nimrod Itzhak Vered, David R. Kroll, and Shlomo Touboul U.S. Patent No. 8,677,494 ("the '494 Patent"), titled MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS. A true and correct copy of the '494 Patent is attached to this Complaint as Exhibit 7 and is incorporated by reference herein.

28. All rights, title, and interest in the '494 Patent have been assigned to Finjan, who is the sole owner of the '494 Patent. Finjan has been the sole owner of the '494 Patent since its issuance.

29. The '494 Patent is generally directed towards a method and system for deriving security profiles and storing the security profiles. One of the ways this is accomplished is by deriving a security profile for a downloadable, which includes a list of suspicious computer operations, and storing the security profile in a database. The '494 Patent discloses and

specifically claims inventive concepts that represent significant improvements over conventional network security technology that was available at the time of filing of the '494 Patent and are more than just generic software components performing conventional activities.

FINJAN'S NOTICE OF INFRINGEMENT TO DEFENDANTS

30. Defendants are well aware of Finjan's patents, including the Asserted Patents, and have continued their infringing activity, despite this knowledge, for years. Finjan gave written notice to Defendants of their infringement of Finjan's patents by letter dated March 23, 2016, which specifically identified Finjan's '305, '086, and '494 Patents. This letter also identified many of Defendants' infringing products, including that Defendants' Nexpose products infringed Finjan's '086 and '494 Patents. Finjan also included an exemplary infringement claim chart with its March 23, 2016 letter showing how Defendants' AppSpider product infringes Finjan's '305 Patent. The AppSpider product works with and contributes to many of Defendants' other accused products, including InsightAppSec.

31. Finjan met in person with Defendants on or about May 11, 2016. During this meeting Finjan explained how Defendants' products infringe Finjan's Patents, including how Defendants' Nexpose products infringe Finjan's '086 and '494 Patents and how the AppSpider product infringes the '305 Patent.

32. From on or about May 11, 2016, through on or about January 4, 2018, Finjan attempted to engage in good faith negotiations with Defendants regarding their ongoing infringement of Finjan's patent portfolio. For example, Finjan contacted Defendants on or about May 24, 2016, to follow up on the parties' initial meeting. Finjan also informed Defendants on or about May 24, 2016, that a third-party competitor of Defendants had recently taken a license to Finjan's Patents, including the Asserted Patents here. Finjan contacted Defendants again on or

about August 1, 2016, and multiple times in or around September 2016. But Defendants largely ignored Finjan’s repeated requests to engage in good faith licensing discussions.

33. On or about January 4, 2018, Finjan sent another letter to Defendants that expressly reminded Defendants that their Nexpose products infringed the ‘494 Patent, and that their AppSpider product continued to infringe the ‘305 Patent.

34. Finjan gave Defendants a PowerPoint presentation on or about February 8, 2018, during which Finjan described to Defendants how their Nexpose, Metasploit, InsightVM, InsightAppSec, and AppSpider products variously infringed Finjan’s patents, including at least Finjan’s ‘494, ‘305, ‘408, ‘289, ‘154, ‘918, and ‘086 Patents. An excerpt from Finjan’s PowerPoint presentation to Defendants is copied below, and is just one image out of the dozens of pages in the February 8, 2018 PowerPoint presentation:

finjan Cybersecurity Exemplary Patents			RAPID7 ipid7 Products and Technologies			
Technology Cluster	US Patent No.	Granted Foreign Patent	Nexpose Vulnerability Management	InsightVM Vulnerability Management	AppSpider Application Security on-Premise	InsightAppSec Application Security in the Cloud
Finjan Inc.	Behavior-Based Security	6,092,194 6,154,844 8,677,494	EP0965094 CA2275771 JP3952315 IL129729	X	X	
	Parsing Tokens	7,975,305 8,225,408	IL181611			X X
	Two Stage Validation	7,757,289 8,141,154				X X
Finjan Blue	Appending Profile	7,613,918 8,079,086		X X		
	Security Audit	7,770,225 7,346,929		X X		

Finjan’s patent portfolio contains additional technologies useful in cybersecurity:

- Histograms, Searching, Sandboxing, Hashing, Network Management, Splitting SSL Connections etc.

35. Finjan's PowerPoint presentation to Defendants on or about February 8, 2018 also identified every patent Finjan owns by number, including their approximate expiration dates.

36. Following up on its PowerPoint presentation, on or about February 12, 2018, Finjan emailed representative claim charts to Defendants showing how Defendants' Nexpose products infringed Finjan's '494 Patent (and another Finjan Patent, U.S. 6,154,844).

37. Thus, despite Finjan's best efforts to inform Defendants that their products infringe Finjan's patents and to engage Defendants in good-faith licensing discussions, Defendants refused to take a license to Finjan's patents. As shown above, Defendants knew that they infringed the Asserted Patents well before Finjan filed this action, and Defendants acted egregiously and willfully in that they continued to infringe Finjan's patents and, on information and belief, took no action to avoid infringement. Instead, Defendants continued to develop additional technologies and products that infringe the Asserted Patents. As such, Defendants have continued to willfully, wantonly, and deliberately engage in acts of infringement of the Finjan Patents.

DEFENDANTS' INFRINGING PRODUCTS AND TECHNOLOGIES

38. Defendants are closely related companies that operate as a single business entity directed and controlled by Rapid7, Inc., making, using, selling, offering for sale, and importing into the United States and this District infringing products and services that utilize InsightIDR, InsightVM (Nexpose), InsightAppSec, AppSpider, Metasploit and Komand technologies, including Rapid7 Insight Platform products (collectively, the "Accused Products").

39. Defendants represent themselves to be one entity with respect to the Accused Products in their annual reports submitted to the United States Securities and Exchange Commission (Form 10-K). *See*, Ex. 8 (Rapid7 2017 Annual Report) at 2-8.

40. Both Rapid7, Inc. and Rapid7 LLC share the same principal place of business and many of the same corporate executives and directors.

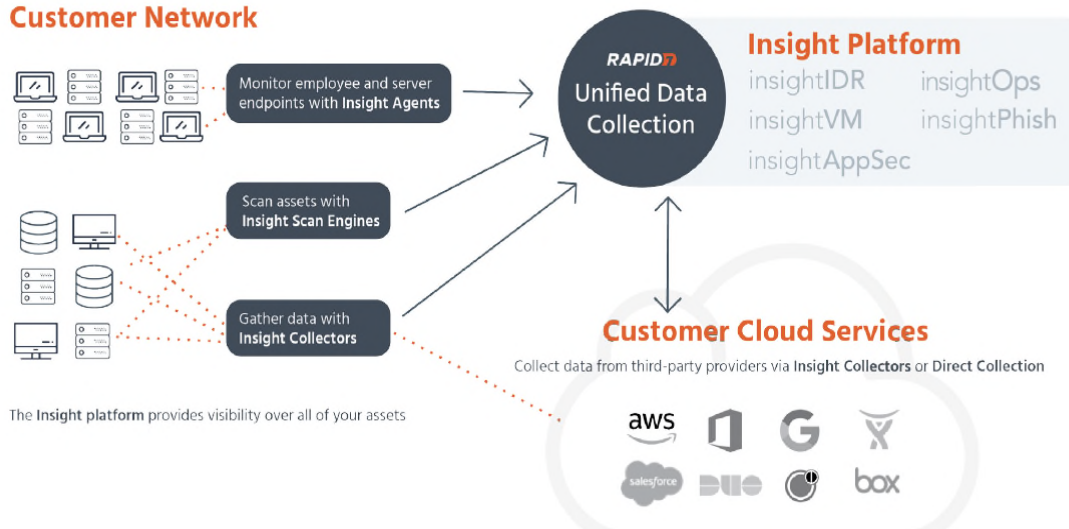
41. Defendants' products are all interrelated through the Rapid7 Insight Platform. The Rapid7 Insight Platform integrates Defendants' detection and analytic technologies across various product offerings, briefly described below.



Ex. 9 (rapid7-product-brochure.pdf).

Insight Platform Architecture

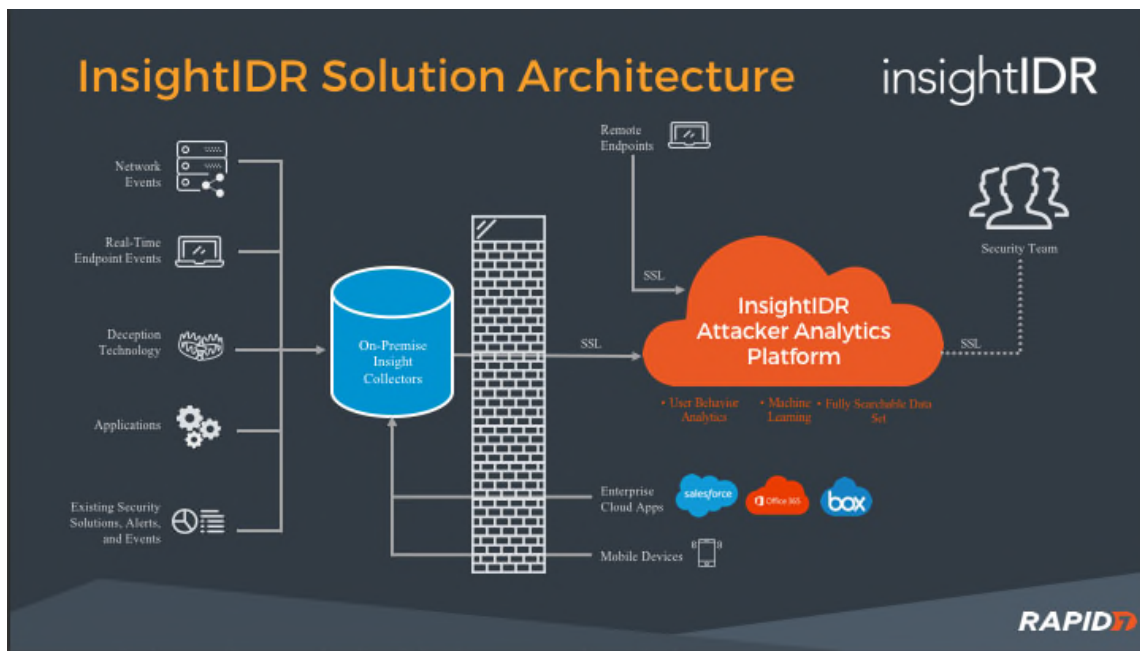
Customer Network



Ex. 10 (Rapid7 Insight Platform Security) at 3.

InsightIDR

42. InsightIDR receives data from a network’s endpoints, cloud and virtual services, and utilizes a combination of scanning technology, machine learning, live threat feeds, and a library of behavioral threat analytics in order to scan and monitor network events for both new and existing threats. InsightIDR is commonly deployed along with Rapid7’s InsightVM.



Ex. 11 (<https://insightidr.help.rapid7.com/docs>).

InsightVM (Nexpose)

43. InsightVM (Nexpose) receives data from a network’s endpoints, cloud and virtual services, and utilizes a combination of scanning technology, live threat feeds, and a library of threat analytics in order to scan and monitor the network for both new and existing vulnerabilities. InsightVM uses RealRisk to assign a risk score to each detected threat.

Focus on the Highest Risks Using RealRisk™

Nexpose provides an advanced vulnerability scoring algorithm, RealRisk™, that provides insights into the most critical vulnerabilities. It leverages threat intelligence such as exploit and malware kit exposure, CVSS v2, temporal risk, and asset importance metrics to give you a granular score for risk prioritization.

$$\text{Rapid7 Real Risk} = \frac{\text{CVSS Impact Metrics}}{\text{CVSS Likelihood Metrics}} \times \text{Exposure} \left(\frac{\text{Malware Kits}}{\text{Exploit Rank}} \cdot \text{time} \right)$$

Exs. 12, 46.

InsightAppSec and AppSpider

44. InsightAppSec crawls and assesses web applications to detect SQL Injection, XSS, and CSRF threats. InsightAppSec normalizes network traffic and uses scan engines (cloud or on-premise) to detect threats, which includes scans for over 90 different known attack types. InsightAppSec works alongside AppSpider to detect and generate a summary of vulnerabilities, which Defendants’ other Accused Products also use.

- **Regex Builder**
 - Build and test regular expressions, used in InsightAppSec and AppSpider to define scan scope.
- **Defend**
 - Import the XML summary of vulnerabilities generated by AppSpider to create custom WAF rules.

Ex. 13 (<https://blog.rapid7.com/2018/06/14/new-insightappsec-releases-compliance-reports-and-the-appsec-toolkit/>).

Metasploit

45. Metasploit is a penetration testing software that utilizes a database of exploits. Metasploit allows simulation of real-world attacks on the network so that further cybersecurity measures can be implemented.

All scan data collected from Nexpose is stored in a Metasploit project and can be viewed from the Analysis area. The information gathered from each host includes the IP address, host name, operating system, running services, and possible vulnerabilities. Metasploit Pro maps each vulnerability to a related module, if one exists in the module database for it. These modules are viewable from the *Modules* tab on the single host view.

Ex. 14 (<https://metasploit.help.rapid7.com/docs/vulnerability-scanning-with-nexpose>).

Komand

46. Komand connects existing cybersecurity tools to a library of plugins in order to integrate, orchestrate and automate workflows in order to efficiently detect and contain malicious malware, domains, and other threat indicators.

DEFENDANTS' WILLFUL INFRINGEMENT OF FINJAN'S PATENTS

47. Defendants have been and are infringing, and continue to infringe, the '305, '408, '289, '918, '086, '154, '494 Patents (collectively, the "Asserted Patents") in this Judicial District and elsewhere in the United States by, among other things, making, using, importing, selling, and offering for sale the Defendants' products and services that utilize InsightIDR, InsightVM (Nexpose), Metasploit and Komand technologies, including Rapid7 Insight Platform products (collectively, the "Accused Products").

48. In addition to directly infringing the Asserted Patents under 35 U.S.C. § 271(a), either literally or under the doctrine of equivalents, or both, Defendants indirectly infringe the '305, '408, '289, '918, '086 and '494 Patents by instructing, directing, and requiring others, including their customers, purchasers, users, and developers, to perform all or some of the steps of the method claims, either literally or under the doctrine of equivalents, or both, of the '305, '408, '289, '918, '086 and '494 Patents.

COUNT I

(Direct Infringement of the ‘494 Patent pursuant to 35 U.S.C. § 271(a))

49. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

50. Defendants infringed Claims 3-5, and 7-18 of the ‘494 Patent in violation of 35 U.S.C. § 271(a).

51. Defendants’ infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

52. Defendants’ acts of making, using, importing, selling, and offering for sale infringing products and services were without the permission, consent, authorization, or license of Finjan.

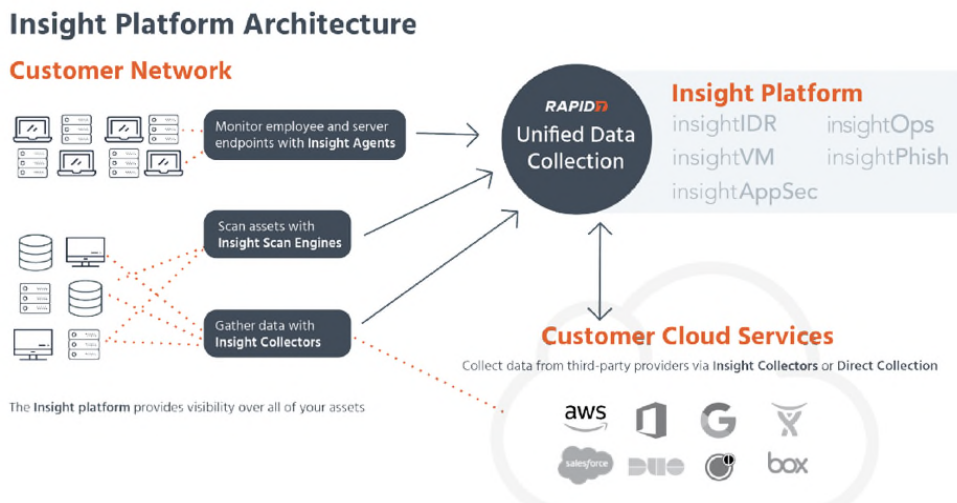
53. Defendants’ infringement included, the manufacture, use, sale, importation and offer for sale of Defendants’ products and services that utilize InsightIDR, InsightVM (Nexpose), Metasploit and Komand technologies, including Rapid7 Insight Platform products (collectively, the “‘494 Accused Products”).

54. The ‘494 Accused Products practice the patented invention of the ‘494 Patent and infringed the ‘494 Patent because they make or use the system and perform the steps of deriving security profiles and storing the security profiles by, for example, deriving a security profile for a downloadable, which includes a list of suspicious computer operations, and storing the security profile in a database.

55. To the extent the ‘494 Accused Products used a system that includes modules, components or software owned by third parties, the ‘494 Accused Products still infringed the ‘494 Patent because Defendants are vicariously liable for the use of the patented system by controlling the entire system and deriving a benefit from the use of every element of the entire

system. Similarly, to the extent Defendants’ customers perform a step or steps of the patented method or the ‘494 Accused Products incorporate third parties’ modules, components or software that perform one or more patented steps, Defendants’ ‘494 Accused Products still infringed the ‘494 Patent because the ‘494 Accused Products condition receipt by the third parties of a benefit upon performance of a step or steps of the patented method and establish the manner or timing of that performance.

56. For example, as shown below, the ‘494 Accused Products are computer-based systems that manage Downloadables with a receiver for receiving an incoming Downloadables (e.g., web applications and files) from network devices and scan and detect threats in the received Downloadables:



Ex. 10 (Rapid7 Insight Platform Security) at 3.

57. The Insight Agent and InsightIDR are receivers that receive incoming Downloadables from an endpoint.

Detect earlier in the attack chain
Most breaches start on the endpoint, and real-time visibility and detection is essential. InsightIDR collects endpoint data via the Insight Agent. From a combination of User and Attacker Behavior Analytics and curated threat intelligence, you get early detections with comprehensive defense-in-depth.

Gain complete visibility across endpoints and users
With InsightIDR, it's easy to have visibility across your network, including remote workers and cloud services. You'll learn about anomalous running processes, risky user behavior, and malicious activity—all in real time.

Detect local indicators of compromise
Leverage the Insight Agent to detect behaviors on your endpoints that indicate compromise. Identify suspicious activities such as local log deletions and privileged escalations occurring on endpoints, which may otherwise be missed by monitoring solutions.

Hunt and collect real-time data on endpoints
When you uncover an indicator of compromise, InsightIDR allows you to easily search across all of your endpoints to see if similar behavior is occurring elsewhere.

<https://www.rapid7.com/products/insightidr/features/endpoint-detection-and-visibility/>

58. The '494 Accused Products receive Downloadables in order to detect various threats and suspicious activity from received Downloadables across the network.

Threats

Overview

A "threat" is something for which you want to monitor access. It is typically a known bad IP address, domain, or URL for which you want to be alerted if someone in the organization accesses it. A threat in InsightIDR can also be a hash for which you want to be alerted if someone runs it.

<https://insightidr.help.rapid7.com/docs/threats>

ACCOUNT RECEIVED SUSPICIOUS LINK 35 Alert

A user has received an email containing a link flagged by the community or threat feeds.

<https://insightidr.help.rapid7.com/docs/alerts>

59. The '494 Accused Products include various Downloadable scanners - Scan Engines - coupled to receivers (e.g., Nexpose, Insight Platform components, Insight Agents) that receive incoming Downloadables (e.g., web applications and files) from network devices and use various Scan Engines to scan them and detect threats and vulnerabilities to derive security profile data for the Downloadables.

Architecture and functionality

Understanding the Nexpose architecture will help you make to make the best use of the functions in the API.

Nexpose is a unified vulnerability solution that scans networks to identify the devices running on them and to test these devices for vulnerabilities and policy compliance. It analyzes the scan data and processes it for reports. You can use these reports to help you assess your network security at various levels of detail and remediate any vulnerabilities quickly.

Vulnerability checks identify security weaknesses in all layers of a network computing environment, including operating systems, databases, applications, and files. Checks can identify areas in your infrastructure that may be at risk for an attack and verify patch updates and security compliance measures.

Nexpose consists of two main components: Scan Engines and a Security Console. One or more Scan Engines (NSEs) search networks to discover devices and the processes running on them, such as operating systems, programs, and databases. The Scan Engines then test discovered assets for vulnerabilities, patches, and other security-related factors. A Security Console collects, analyzes, and stores the scan data, and it generates reports and vulnerability remediation procedures. Additionally, the console controls the Scan Engines and provides a Web-accessible user interface for managing all Nexpose functions.

An organization can deploy Scan Engines within its network or outside its firewall. It also can use Hosted Scanning Engines that are located in Rapid7 data centers.

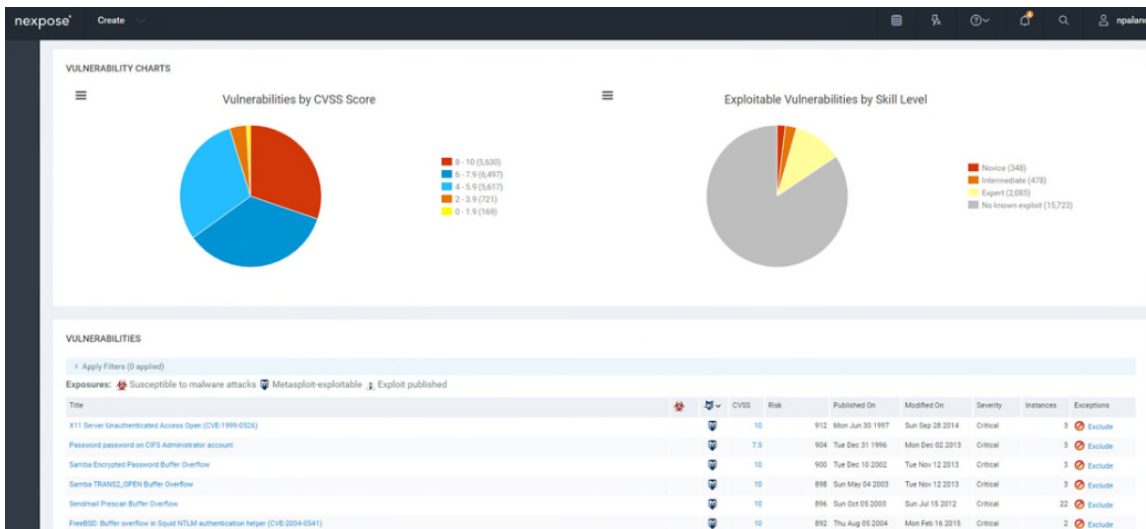
The simplest configuration consists of a single Scan Engine and the Security Console on one host.

Ex. 15 (Nexpose API 1.1 and 1.2 Guide (v. 6.0)) at 14.

60. The Downloadable scanners derive security profile data for the received Downloadables and compute it into risk scores for the Downloadables.

Real Risk Score

The standard 1-10 CVSS score results in thousands of “critical” vulnerabilities. Our vulnerability scanner’s Real Risk Score provides more actionable insight. Taking into account vulnerability age, as well as public exploits/malware kits, our 1-1000 scale highlights the vulnerabilities most likely to be used in an attack, helping you prioritize truly critical issues. When used with our robust tagging system, you can even prioritize the systems most critical to your business, automatically.



Ex. 16 (<https://www.rapid7.com/products/nexpose/features/>).

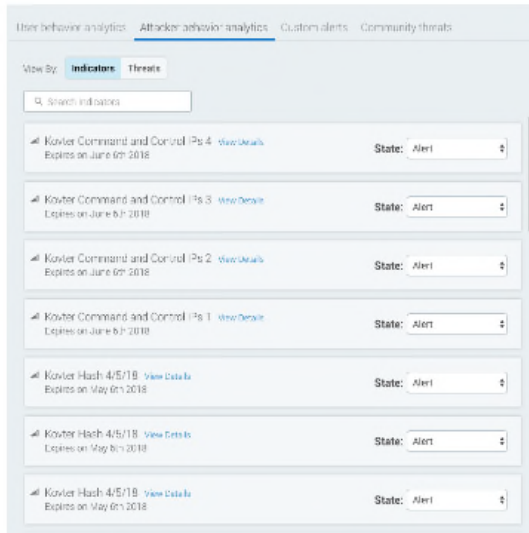
61. To derive the security data profile for the Downloadables, the Downloadable scanners utilize a library of suspicious operations that may be attempted by the Downloadables.

Attacker Behavior Analytics (ABA)

Attacker Behavior Analytics are pre-built detections modeled around our wide array of threat intelligence. Attacker Behavior Analytics expose the finite ways attackers gain persistence on an asset, and send and receive commands to victim machines.

Each ABA detection hunts for a unique attacker behavior, which you can toggle to an alert, whitelist, or track as notable behavior. To manage these settings, go to Settings > Alert Settings > Attacker Behavior Analytics. Find the indicator or threat you want to manage and change the state in the provided dropdown menu.

See [Attacker Behavior Analytics \(ABA\)](#) for more information.



Ex. 17 (<https://insightidr.help.rapid7.com/docs/new-features>).

Attacker Behavior Analytics Library

Below is a list of released ABA detections, all of which come with our threat detection solution, [InsightIDR](#), and automatically match against your data in real time. This is threat intelligence that moves at the speed of the attacker—if a new exploit comes out, our team will craft a detection, test it against the [Rapid7 Insight platform](#), and deploy it in InsightIDR—all within hours. Still craving that aged, open-source threat feed now?

Ex. 18 (<https://www.rapid7.com/solutions/attacker-behavior-analytics/>)

62. Once vulnerabilities and threats are detected in Downloadables by Scan Engines, they are added to the Rapid7 database by the coupled database manager.

Every vulnerability discovered in the scanning process is added to the vulnerability database. This extensive, full-text, searchable database also stores information on patches, downloadable fixes, and reference content about security weaknesses. The application keeps the database current through a subscription service that maintains and updates vulnerability definitions and links. It contacts this service for new information every six hours.

The database has been certified to be compatible with the MITRE Corporation's Common Vulnerabilities and Exposures (CVE) index, which standardizes the names of vulnerabilities across diverse security products and vendors. The index rates vulnerabilities according to MITRE's Common Vulnerabilities Scoring System (CVSS) Version 2 and Version 3, if it is available.

An application algorithm computes the CVSS score based on ease of exploit, remote execution capability, credentialed access requirement, and other criteria. The score, which ranges from 1.0 to 10.0, is used in Payment Card Industry (PCI) compliance testing. For more information about CVSS scoring, go to the FIRST Web site <https://www.first.org/cvss/>.

Ex. 19 (<https://nexpose.help.rapid7.com/docs/working-with-vulnerabilities>).

63. Database managers coupled with the Downloadable scanners store the Downloadable security profiles in a database, which can be accessed at a later time.

I want to look at my scan data and make sense of it.

Go to the Assess section and find out how to locate assets and vulnerabilities and to sort them by different security metrics to help you prioritize your security threats.

Ex. 20 (<https://insightvm.help.rapid7.com/docs/welcome-to-help>).

64. Defendants' infringement of the '494 Patent injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty.

65. Defendants have been long-aware of Finjan's patents, including the '494 Patent, and continued their unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendants for over two years regarding Defendants' infringement of Finjan's Asserted Patents. Even after being shown that their products infringe Finjan's patents, including the '494 Patent, on information and belief Defendants made no effort to avoid infringement. Instead, Defendants continued to incorporate their infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendants' blatant and egregious disregard for Finjan's patent rights.

66. Despite their knowledge of Finjan's patent portfolio and Asserted Patents, and their specific knowledge of their own infringement, Defendants continued to sell the Accused Products in complete and reckless disregard of Finjan's patent rights. As such, Defendant acted recklessly, willfully, wantonly, and deliberately engaged in acts of infringement of the '494 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT II
(Indirect Infringement of the '494 Patent pursuant to 35 U.S.C. § 271(b))

67. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

68. In addition to directly infringing the '494 Patent, Defendants knew or were willfully blind to the fact that they were inducing infringement of at least Claims 3-5 and 7-9 of the '494 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring their customers to perform the steps of the method claims of the '494 Patent, either literally or under the doctrine of equivalents.

69. Additionally, Defendants knew or were willfully blind to the fact that they were inducing infringement of at least Claims 3-5 and 7-9 of the '494 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring their customers to perform the steps of the method claims of the '494 Patent, either literally or under the doctrine of equivalents.

70. To the extent one Defendant is deemed to direct and control the other Defendant to directly infringe the '494 Patent, the former Defendant is liable for inducing the latter Defendant to directly infringe the '494 Patent.

71. Defendants knowingly and actively aided and abetted the direct infringement of the '494 Patent by instructing and encouraging their customers and developers to use the '494

Accused Products. Such instructions and encouragement included advising third parties to use the '494 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '494 Patent, by advertising and promoting the use of the '494 Accused Products in an infringing manner, and by distributing guidelines and instructions to third parties on how to use the '494 Accused Products in an infringing manner. See, *e.g.*, Ex. 15 (Nexpose API 1.1 and 1.2 Guide (v. 6.0)); Ex. 15

(https://www.rapid7.com/docs/download/Nexpose_API_guide.pdf); Ex. 19

(<https://nexpose.help.rapid7.com/docs/working-with-vulnerabilities>); Ex. 21

(<https://insightidr.help.rapid7.com/docs/threats>); Ex. 14

(<https://metasploit.help.rapid7.com/docs/vulnerability-scanning-with-nexpose>); Ex. 18

(<https://www.rapid7.com/solutions/attacker-behavior-analytics/>); Ex. 22

(<https://nexpose.help.rapid7.com/docs/sending-custom-fingerprints-to-paired-scan-engines>);

Ex. 23 (<https://blog.rapid7.com/2018/04/17/attacker-behavior-analytics-detects-unknown-threats/>).

COUNT III

(Direct Infringement of the '305 Patent pursuant to 35 U.S.C. § 271(a))

72. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

73. Defendants have infringed and continue to infringe Claims 1-25 of the '305 Patent in violation of 35 U.S.C. § 271(a).

74. Defendants' infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

75. Defendants' acts of making, using, importing, selling, and offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

76. Defendants' infringement includes the manufacture, use, sale, importation and offer for sale of Defendants' products and services that utilize InsightIDR, InsightVM (Nexpose), Metasploit and Komand technologies, including Rapid7 Insight Platform products (collectively, the "305 Accused Products").

77. The '305 Accused Products embody the patented invention of the '305 Patent and infringe the '305 Patent because they make or use the patented system or perform the patented method of rule-based scanning of web-based content for exploits by, for example, using parser and analyzer rules to describe computer exploits as patterns of types of tokens.

78. To the extent the '305 Accused Products used a system that includes modules, components or software owned by third parties, the '305 Accused Products still infringed the '305 Patent because Defendants are vicariously liable for the use of the patented system by controlling the entire system and deriving a benefit from the use of every element of the entire system. Similarly, to the extent Defendants' customers performed a step or steps of the patented method or the '305 Accused Products incorporate third parties' modules, components or software that performed one or more patented steps, Defendants' '305 Accused Products still infringed the '305 Patent because the '305 Accused Products condition receipt by the third parties of a benefit upon performance of a step or steps of the patented method and establish the manner or timing of that performance.

79. For example, as shown below, the ‘305 Accused Products provide a platform, including Scan Engines, which operates on a computer to scan content to prevent malicious code and threats from accessing the client computer.

Rapid7 InsightIDR leverages both User and Attacker Behavior Analytics to detect intruder activity, cutting down false positives and days’ worth of work for your security professionals. It hunts all of the top attack vectors behind breaches: the use of stolen credentials, malware, and phishing, and alerts on stealthy intruder behavior as early as possible in the attack chain.

Ex. 24 (InsightIDR:From Compromise to Containment. Fast) at 1.

Real-time endpoint detection and investigation.

InsightIDR natively collects data off the endpoint with the Insight Agent and Endpoint Scan. This gives you real-time detection for malware, fileless attacks, and the use of stolen credentials even on assets off the corporate network.

Id. at 2.

80. The content includes suspicious web page content containing HTML, PDFs, JavaScript, drive-by downloads, obfuscated code, or other blended web malware.

Fileless malware. Spear phishing. Crypto-jacking. Attackers' techniques for persistence shift, but they remain finite. As our analysts contribute Attacker Behavior Analytics, these detections are tested against the Rapid7 Insight platform to ensure you only get high-fidelity alerts in InsightIDR.

Our analyst teams are able to build detections against the rich tapestry of data collected by InsightIDR—this includes network, cloud application, and directly from the endpoint. We are identifying malicious underlying behaviors, not matching against aging open source threat intelligence.

Ex. 25 (<https://www.rapid7.com/products/insightidr/use-cases/identify-evolving-attacker-behavior/>).

What Do These New Detections Cover?

Attacker Behavior Analytics expose the finite ways attackers gain persistence on an asset, and send and receive commands to victim machines. This identifies:

- Malware, malware droppers, maldocs, and fileless malware (opportunistic & targeted)
- Cryptojacking: Stealing CPU cycles to mine cryptocurrency
- Pen testing & attack tools
- Suspicious persistence
- Anomalous data exfiltration
- New attacker behavior

Ex. 23 (<https://blog.rapid7.com/2018/04/17/attacker-behavior-analytics-detects-unknown-threats/>).

81. As shown below, Rapid7 products include the InsightIDR Scan Engines which make use of various methods, including identification and analysis of hashed files, to scan content within a computer.

The screenshot displays the 'Process Hash Details' interface. It includes a 'FILE DETAILS' section with the following information:

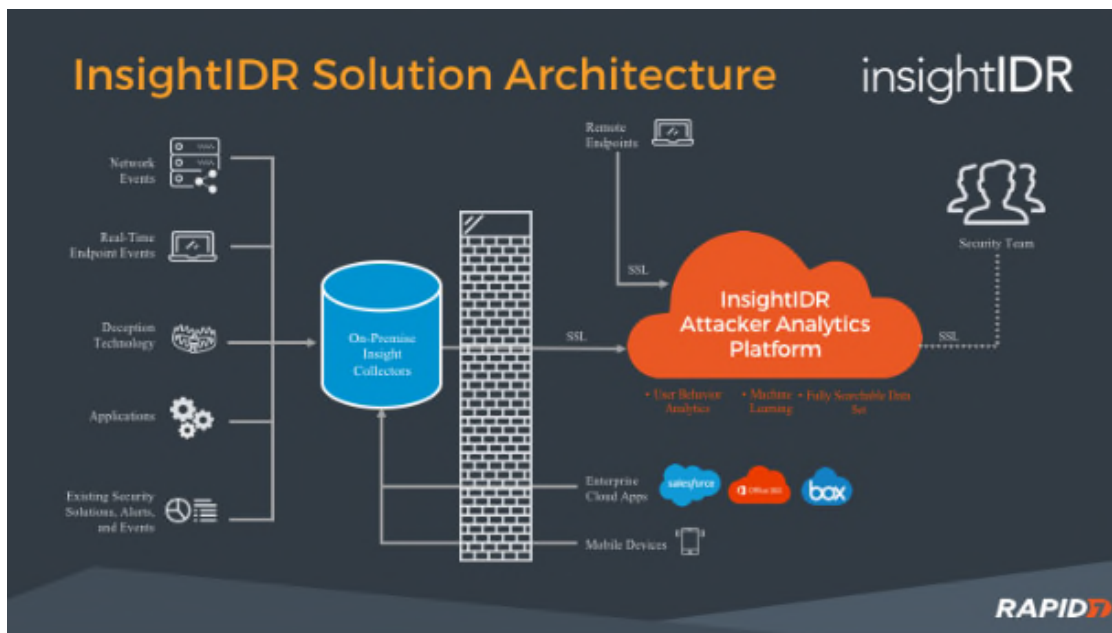
- MD5:** e4c53ce8409dcff708c790a0ac76398d
- SHA1:** 44cbf8dff2fe6aa7b264eaaa33e02ad1fa4a6796
- Operating System:** Microsoft Windows
- File Size:** 264 kB
- Signature Verification:** Signed, verified signature
- Commonality:** Rare
- Signers:** C=US, S=California, L=Fremont, O="Logitech, Inc.", OU=Digital ID Class 3 - Microsoft Software Validation v2, CN="Logitech, Inc."
C=US, O="VeriSign, Inc.", OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 Code Signing 2010 CA
C=US, O="VeriSign, Inc.", OU=VeriSign Trust Network, OU="(c) 2006 VeriSign, Inc. - For authorized use only", CN=VeriSign Class 3 Public Primary Certification Authority - G5
- File Names:** camerahelpershell.exe
- VirusTotal Report:** See Report

Below the file details is an 'ASSETS RUNNING THIS HASH' section with a search filter set to '1w' (last week).

Ex. 26 (<https://www.rapid7.com/explore/insightidr/endpoint-capabilities/index.php?step=8>).

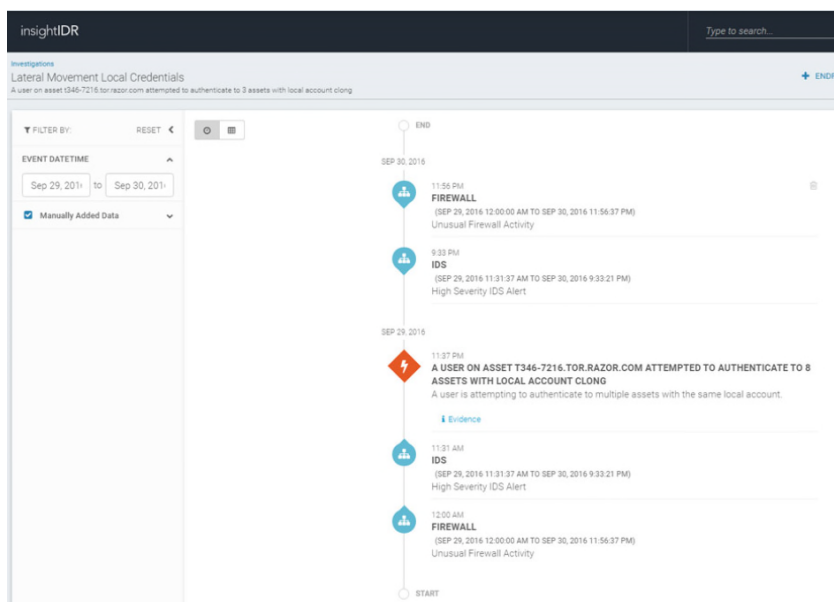
82. The '305 Accused Products utilize and integrate with existing gateways, firewalls and routers to selectively divert incoming content, such as web pages or email for rule-based

content scanning, thereby capturing suspicious traffic between external attackers and internal targets, where such traffic are then analyzed by Rapid7 Cloud Products.



Ex. 11 (<https://insightidr.help.rapid7.com/docs>).

83. The '305 Accused Products monitor communications between web browsers and remote servers to divert and block malicious incoming content.



Ex. 27 (<https://www.rapid7.com/explore/insightidr/detect-lateral-movement/index.php?step=3>).



Ex. 11 (<https://insightidr.help.rapid7.com/docs>).

84. Rapid7 Cloud Products performs deep analysis of code, using purser and analyzer rules, extracting the patterns that are responsible for its behavior.

If you develop custom fingerprints, you can have the Security Console distribute them automatically to any paired Scan Engine that is currently in use when a scan is run. To do so, simply copy the fingerprint files to the [installation_directory]/plugins/fp/custom/ directory on your Security Console host.

Every fingerprint contains a *pattern* attribute with the regular expression to match against the data.

An optional flags attribute controls how the regular expression is to be interpreted. See the [Recog documentation for FLAG_MAP](#) for more information.

Each fingerprint contains a *description* element with a human-readable string describing the fingerprint.

Ex. 22 (<https://nexpose.help.rapid7.com/docs/sending-custom-fingerprints-to-paired-scan-engines>)

85. Defendants' infringement of the '305 Patent has injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty. Additionally, as a result of Defendants' unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendants compete in the security software space, and Finjan is actively engaged in licensing its patent portfolio, as described above. Defendants' continued infringement of the '305 Patent causes harm to Finjan in the form of price erosion, loss of goodwill, damage to reputation, loss of business opportunities, inadequacy of money damages, and direct and indirect competition. Monetary damages are insufficient to compensate Finjan for these harms, and thus Finjan is entitled to preliminary and/or permanent injunctive relief.

86. Defendants have been long-aware of Finjan's patents, including the '305 Patent, and continued their unauthorized infringing activity despite this knowledge. As discussed above,

Finjan actively and diligently attempted to engage in good faith negotiations with Defendants for over two years regarding Defendants' infringement of Finjan's Asserted Patents. Even after being shown that their products infringe Finjan's patents, including the '305 Patent, on information and belief Defendants made no effort to avoid infringement. Instead, Defendants continued to incorporate their infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendants' blatant and egregious disregard for Finjan's patent rights.

87. Despite their knowledge of Finjan's patent portfolio and Asserted Patents, and their specific knowledge of their own infringement, Defendants continued to sell the Accused Products in complete and reckless disregard of Finjan's patent rights. As such, Defendant acted recklessly, willfully, wantonly, and deliberately engaged in acts of infringement of the '305 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT IV

(Indirect Infringement of the '305 Patent pursuant to 35 U.S.C. § 271(b))

88. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

89. In addition to directly infringing the '305 Patent, Defendants knew or were willfully blind to the fact that they were inducing infringement of at least Claims 13-24 of the '305 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring their customers to perform the steps of the method claims of the '305 Patent, either literally or under the doctrine of equivalents.

90. Additionally, Defendants knew or were willfully blind to the fact that they were inducing infringement of at least Claims 13-24 of the '305 Patent under 35 U.S.C. § 271(b) by

instructing, directing and requiring their developers to perform the steps of the method claims of the '305 Patent, either literally or under the doctrine of equivalents.

91. To the extent one Defendant is deemed to direct and controlling the other Defendant to directly infringe the '305 Patent, the former Defendant is liable for inducing the latter Defendant to directly infringe the '305 Patent.

92. Defendants knowingly and actively aided and abetted the direct infringement of the '305 Patent by instructing and encouraging their customers, purchasers, users, and developers to use the '305 Accused Products. Such instructions and encouragement included advising third parties to use the '305 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '305 Patent, by advertising and promoting the use of the '305 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '305 Accused Products in an infringing manner.

93. *See, e.g.*, Ex. 15 (Nexpose API 1.1 and 1.2 Guide (v. 6.0)); Ex. 15 (https://www.rapid7.com/docs/download/Nexpose_API_guide.pdf); Ex. 19 (<https://nexpose.help.rapid7.com/docs/working-with-vulnerabilities>); Ex. 21 (<https://insightidr.help.rapid7.com/docs/threats/>); Ex. 14 (<https://metasploit.help.rapid7.com/docs/vulnerability-scanning-with-nexpose>); Ex. 18 (<https://www.rapid7.com/solutions/attacker-behavior-analytics/>); Ex. 22 (<https://nexpose.help.rapid7.com/docs/sending-custom-fingerprints-to-paired-scan-engines>); Ex. 23 (<https://blog.rapid7.com/2018/04/17/attacker-behavior-analytics-detects-unknown-threats/>).

COUNT V

(Direct Infringement of the ‘408 Patent pursuant to 35 U.S.C. § 271(a))

94. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

95. Defendants have infringed and continue to infringe Claims 1-35 of the ‘408 Patent in violation of 35 U.S.C. § 271(a).

96. Defendants’ infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

97. Defendants’ acts of making, using, importing, selling, and offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

98. Defendants’ infringement includes the manufacture, use, sale, importation and offer for sale of Defendants’ products and services that utilize InsightIDR, InsightVM (Nexpose), Metasploit and Komand technologies, including Rapid7 Insight Platform products (collectively, the “408 Accused Products”).

99. The ‘408 Accused Products embody the patented invention of the ‘408 Patent and infringe the ‘408 Patent because they make or use the patented system or perform the patented method of rule-based scanning of web-based content for exploits written in different programming languages, by, for example, expressing the exploits as patterns of tokens or using a parse tree.

100. To the extent the ‘408 Accused Products used a system that includes modules, components or software owned by third parties, the ‘408 Accused Products still infringed the ‘408 Patent because Defendants are vicariously liable for the use of the patented system by controlling the entire system and deriving a benefit from the use of every element of the entire

system. Similarly, to the extent Defendants' customers performed a step or steps of the patented method or the '408 Accused Products incorporated third parties' modules, components or software that performed one or more patented steps, Defendants' '408 Accused Products still infringed the '408 Patent because the '408 Accused Products condition receipt by the third parties of a benefit upon performance of a step or steps of the patented method and establish the manner or timing of that performance.

101. For example, the '408 Accused Products provide a platform, including Scan Engines, which operates on a computer to scan content to prevent malicious code and threats from accessing the client computer.

Rapid7 InsightIDR leverages both User and Attacker Behavior Analytics to detect intruder activity, cutting down false positives and days' worth of work for your security professionals. It hunts all of the top attack vectors behind breaches: the use of stolen credentials, malware, and phishing, and alerts on stealthy intruder behavior as early as possible in the attack chain.

Ex. 24 (InsightIDR:From Compromise to Containment. Fast) at 1.

Real-time endpoint detection and investigation.

InsightIDR natively collects data off the endpoint with the Insight Agent and Endpoint Scan. This gives you real-time detection for malware, fileless attacks, and the use of stolen credentials even on assets off the corporate network.

Ex. 24 (InsightIDR:From Compromise to Containment. Fast) at 2.

102. The '408 Accused Products performs deep analysis of code, using purser and analyzer rules, extracting the patterns that are responsible for its behavior.

If you develop custom fingerprints, you can have the Security Console distribute them automatically to any paired Scan Engine that is currently in use when a scan is run. To do so, simply copy the fingerprint files to the [installation_directory]/plugins/fp/custom/ directory on your Security Console host.

Every fingerprint contains a *pattern* attribute with the regular expression to match against the data.

An optional flags attribute controls how the regular expression is to be interpreted. See the [Recog documentation for FLAG_MAP](#) for more information.

Each fingerprint contains a *description* element with a human-readable string describing the fingerprint.

Ex. 22 (<https://nexpose.help.rapid7.com/docs/sending-custom-fingerprints-to-paired-scan-engines>).

103. Defendants' infringement of the '408 Patent has injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty. Additionally, as a result of Defendants' unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendants compete in the security software space, and Finjan is actively engaged in licensing its patent portfolio, as described above. Defendants' continued infringement of the '408 Patent causes harm to Finjan in the form of price erosion, loss of goodwill, damage to reputation, loss of business opportunities, inadequacy of money damages, and direct and indirect competition. Monetary damages are insufficient to compensate Finjan for these harms, and thus Finjan is entitled to preliminary and/or permanent injunctive relief.

104. Defendants have been long-aware of Finjan's patents, including the '408 Patent, and continued their unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendants for over two years regarding Defendants' infringement of Finjan's Asserted Patents. Even after being shown that their products infringe Finjan's patents, including the '408 Patent, on information and belief Defendants made no effort to avoid infringement. Instead, Defendants

continued to incorporate their infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendants' blatant and egregious disregard for Finjan's patent rights.

105. Despite their knowledge of Finjan's patent portfolio and Asserted Patents, and their specific knowledge of their own infringement, Defendants continued to sell the Accused Products in complete and reckless disregard of Finjan's patent rights. As such, Defendant acted recklessly, willfully, wantonly, and deliberately engaged in acts of infringement of the '408 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT VI
(Indirect Infringement of the '408 Patent pursuant to 35 U.S.C. § 271(b))

106. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

107. In addition to directly infringing the '408 Patent, Defendants knew or were willfully blind to the fact that they were inducing infringement of at least Claims 1-8, 23-28 of the '408 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring their customers to perform the steps of the method claims of the '408 Patent, either literally or under the doctrine of equivalents.

108. Additionally, Defendants knew or were willfully blind to the fact that they were inducing infringement of at least Claims 1-8, 23-28 of the '408 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring their developers to perform the steps of the method claims of the '408 Patent, either literally or under the doctrine of equivalents.

109. To the extent one Defendant is deemed to direct and control the other Defendant to directly infringe the '408 Patent, the former Defendant is liable for inducing the latter Defendant to directly infringe the '408 Patent.

110. Defendants knowingly and actively aided and abetted the direct infringement of the '408 Patent by instructing and encouraging their customers and developers to use the '408 Accused Products. Such instructions and encouragement included advising third parties to use the '408 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '408 Patent, and by advertising and promoting the use of the '408 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '408 Accused Products in an infringing manner. *See, e.g.*, Ex. 15 (Nexpose API 1.1 and 1.2 Guide (v. 6.0)); Ex. 15

(https://www.rapid7.com/docs/download/Nexpose_API_guide.pdf); Ex. 19

(<https://nexpose.help.rapid7.com/docs/working-with-vulnerabilities>); Ex. 21

(<https://insightidr.help.rapid7.com/docs/threats>); Ex. 14

(<https://metasploit.help.rapid7.com/docs/vulnerability-scanning-with-nexpose>); Ex. 18

(<https://www.rapid7.com/solutions/attacker-behavior-analytics/>); Ex. 22

(<https://nexpose.help.rapid7.com/docs/sending-custom-fingerprints-to-paired-scan-engines>);

Ex. 23 (<https://blog.rapid7.com/2018/04/17/attacker-behavior-analytics-detects-unknown-threats/>).

COUNT VII

(Direct Infringement of the '289 Patent pursuant to 35 U.S.C. § 271(a))

111. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

112. Defendants have infringed and continue to infringe Claims 1-46 of the '289 Patent in violation of 35 U.S.C. § 271(a).

113. Defendants' infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

114. Defendants' acts of making, using, importing, selling, and offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

115. Defendants' infringement includes the manufacture, use, sale, importation and offer for sale of Defendants' products and services that utilize InsightIDR, InsightVM (Nexpose), Metasploit and Komand technologies, including Rapid7 Insight Platform products (collectively, the "'289 Accused Products").

116. The '289 Accused Products embody the patented invention of the '289 Patent and infringe the '289 Patent because they make or use the patented system or perform the patented method for inspecting dynamically generated executable code by receiving content with an original function and replacing the original call function with a substitute call function, and then determining whether it is safe to invoke the original call function.

117. To the extent the '289 Accused Products used a system that includes modules, components or software owned by third parties, the '289 Accused Products still infringed the '289 Patent because Defendants are vicariously liable for the use of the patented system by controlling the entire system and deriving a benefit from the use of every element of the entire system. Similarly, to the extent Defendants' customers performed a step or steps of the patented method or the '289 Accused Products incorporated third parties' modules, components or software that performed one or more patented steps, Defendants' '289 Accused Products still

infringed the '289 Patent because the '289 Accused Products condition receipt by the third parties of a benefit upon performance of a step or steps of the patented method and establish the manner or timing of that performance.

118. For example, "Rapid7 InsightIDR leverages both User and Attacker Behavior Analytics to detect intruder activity ... hunts all of the top attack vectors behind breaches: the use of stolen credentials, malware, and phishing, and alerts on stealthy intruder behavior as early as possible in the attack chain." Ex. 24 (InsightIDR: From Compromise to Containment. Fast) at 1. And Attacker Behavior Analytics cover various forms of attacks as shown below:



What Do These New Detections Cover?

Attacker Behavior Analytics expose the finite ways attackers gain persistence on an asset, and send and receive commands to victim machines. This identifies:

- Malware, malware droppers, maldocs, and fileless malware (opportunistic & targeted)
- Cryptojacking: Stealing CPU cycles to mine cryptocurrency
- Pen testing & attack tools
- Suspicious persistence
- Anomalous data exfiltration
- New attacker behavior

Ex. 23 (<https://blog.rapid7.com/2018/04/17/attacker-behavior-analytics-detects-unknown-threats/>). This Attacker Behavior Analytics (ABA) "reveal[s] unknown variants of successful attacker techniques, and are continually crafted by Rapid7's global security analysts and threat intelligence teams." Ex. 28 (<https://www.rapid7.com/about/press-releases/attacker-behavior-analytics-brings-together-machine-learning-and-human-security-expertise/>). "With the addition of ABA, all InsightIDR customers will automatically receive high-fidelity alerts on evolving attacker behaviors built from thousands of incident investigations, including the use of file-less malware, crypto-jacking, and spear phishing. When these malicious techniques are identified,

alerts highlight notable behavior from the affected user and asset, making it significantly easier for security teams to respond quickly and with confidence.” *Id.*

On the detection and response front, the Insight Agent used with [InsightIDR](#) will detect fileless and obfuscated malware by searching for underlying malicious behaviors, such as suspicious persistence and remote code execution, as opposed to static, aging threat intelligence. For more on how the Insight Agent detects threats, check out our [Attacker Behavior Analytics library](#), built by our [Managed Detection and Response](#) and threat intelligence teams.

When used with our vulnerability assessment tool, [InsightVM](#), the Insight Agent gives you that illusive insight into your complete modern environment. Virtual, cloud, and remote assets are now—finally—all being continuously evaluated for risk in real time.

Because the Insight Agent is highly interoperable, one agent works across our products to help you prevent, detect, and respond to attacks. [InsightVM](#) and [InsightIDR](#) are commonly deployed together, enabling you to expose user and asset risk ([InsightVM](#)) and detect malicious behavior across the attack chain ([InsightIDR](#))—all with the same agent. Combined with [risk prioritization](#) based on our data-backed, industry-leading knowledge of the attacker mindset, you can measurably reduce your attack surface, detect “unknown-unknowns” in real time, and save time across your [incident response](#) lifecycle.

Ex. 29 ([https://blog.rapid7.com/2018/08/29/endpoint-agents-are-necessary-for-todays-modern-environment-heres-why-part-2/.](https://blog.rapid7.com/2018/08/29/endpoint-agents-are-necessary-for-todays-modern-environment-heres-why-part-2/))

119. The ‘289 Accused Products collect and receive content at a gateway (e.g., web proxy and VPN/firewalls at the edge of the network to connect to outside networks) for processing.

Rapid7 uses collectors to gather information from on-premises and cloud networks and to securely transfer data to the Insight platform. Collectors sit behind the client’s firewall, respond to changes in the environment, and securely transmit relevant data to the Insight platform for analysis. Collectors were designed with the following core tenets in mind:

- Collectors can be configured only by administrators.
- All data is secured during the transmission process, which uses strong encryption protocols.
- Data transferred from each separate collector is uniquely identified and stored and cannot be accessed by any third parties.

Ex. 11 (<https://insightidr.help.rapid7.com/docs>).

120. The content received at the gateway includes a call to a function with an input such as a function to open a web page and URL address. The ‘289 Accused Products protect against such malware.

At a Glance:

If you've ever studied famous battles in history, you'll know that no two are exactly alike. Still, there are similar strategies and tactics often used in battle because they are time-proven to be effective.

Similarly, when a criminal is trying to hack an organization, they won't re-invent the wheel unless they absolutely have to: They'll draw upon a common arsenal of attacks that are known to be highly effective, such as malware, phishing, or cross-site scripting (XSS). Whether you're trying to make sense of the latest data breach headline in the news or analyzing an incident in your own organization, it helps to understand the different ways an attacker might try to cause harm. Here's an overview of some of the most common types of attacks seen today.

IN THIS SECTION

Types of Cybersecurity Attacks

Common Types of Cybersecurity Attacks

Phishing Attacks

SQL Injection Attacks (SQLi)

Cross-Site Scripting (XSS)

Man-in-the-Middle (MITM) Attacks

Malware Attacks

Denial-of-Service Attacks

Spear Phishing Attacks

Whaling Phishing Attacks

Brute-Force and Dictionary Attacks

Ex. 30 (<https://www.rapid7.com/fundamentals/types-of-attacks/>).

121. In some instances, a first function with the input is used to conceal an intent to call a second function with the input. Some examples of calls for invoking a second function with the input include: “the downloader will initiate a connection to a command and control domain to download additional files,” “accessing device configuration data, downloading additional files, executing commands, modifying the registry, capturing screen shots, and exfiltrating data,” “downloading and installing malware, installing proxy and remote access trojans (RATs), connect to command control (C&C) servers to receive instructions, and alter the victim’s firewall to allow incoming connections,” and spreading ransomware “via phishing emails or malicious links.”

KEYMARBLE, a remote access trojan being used by North Korean entities that is capable of accessing device configuration data, downloading additional files, executing commands, modifying the registry, capturing screen shots, and exfiltrating data.

Typeframe, a trojan being used by North Korea state-sponsored cybercriminals. This family consists of 32-bit and 64-bit Windows executable files, as well as a malicious Microsoft Word document that contains Visual Basic for Applications (VBA) macros. According to their research, these files are capable of downloading and installing malware, installing proxy and remote access trojans (RATs), connect to command control (C&C) servers to receive instructions, and alter the victim’s firewall to allow incoming connections.

Detections added to InsightDR: 23, for KEYMARBLE and Typeframe trojans.

Satan Ransomware

Verticals targeted: None, offered as ransomware-as-a-service

Satan Ransomware appeared in early 2017 and was one of the original "Ransomware as a Service" offerings on dark websites. The ransomware is spread via phishing emails or malicious links, and has recently been updated to include the EternalBlue SMB exploit for spreading within a network.

Detections added to InsightIDR: 6, which identify variants of the Satan ransomware and dropper, the EternalBlue SMB exploit, and suspicious associated command line activity.

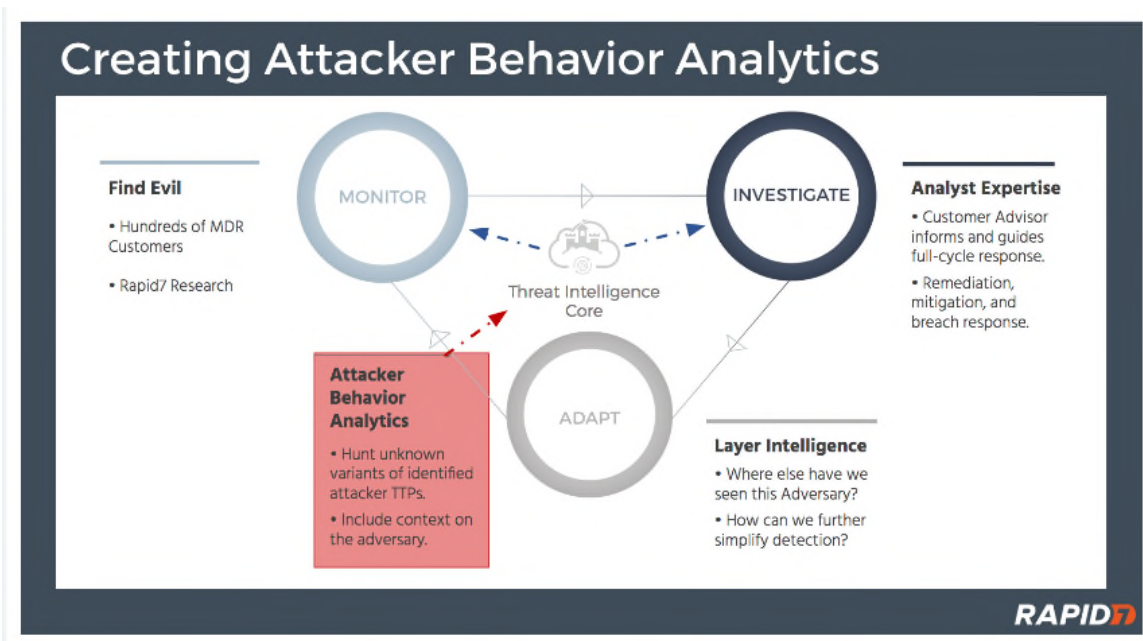
Ex. 31 (<https://www.rapid7.com/solutions/attacker-behavior-analytics/>).

122. The Accused '289 Products modify the received content where operation of the function causes the modified content (and input) to be inspected in a sandbox or other virtualized environment for behavioral analysis.

Rapid7 uses collectors to gather information from on-premises and cloud networks and to securely transfer data to the Insight platform. Collectors sit behind the client's firewall, respond to changes in the environment, and securely transmit relevant data to the Insight platform for analysis. Collectors were designed with the following core tenets in mind:

- Collectors can be configured only by administrators.
- All data is secured during the transmission process, which uses strong encryption protocols.
- Data transferred from each separate collector is uniquely identified and stored and cannot be accessed by any third parties.

Ex. 10 (Rapid7 Insight Platform Security) at 4.



This library of detections powered the majority of the reporting output for our MDR clients, and not long after, the feature was dubbed Attacker Behavior Analytics and added to our InsightIDR solution as well.

Ex. 32 (<https://blog.rapid7.com/2018/07/03/behind-the-scenes-attacker-behavior-analytics-with-mdr-team/>).

Fileless malware. Spear phishing. Crypto-jacking. Attackers' techniques for persistence shift, but they remain finite. As our analysts contribute Attacker Behavior Analytics, these detections are tested against the Rapid7 Insight platform to ensure you only get high-fidelity alerts in InsightIDR.

Our analyst teams are able to build detections against the rich tapestry of data collected by InsightIDR—this includes network, cloud application, and directly from the endpoint. We are identifying malicious underlying behaviors, not matching against aging open source threat intelligence.

123. <https://www.rapid7.com/products/insightidr/use-cases/identify-evolving-attacker-behavior/>

124. The '289 Accused Products also provide methods for using plug-in and API triggers for modifying the content at the gateway computer, comprising replacing the call to the

original function with a corresponding call to a substitute function that sends the input to a security computer for inspection.

When you build a workflow, the Trigger is what kickstarts the workflow into action. When you create a new workflow, you first choose your trigger type and trigger source. Here, you can either create a new trigger source or choose one from a list of available triggers. Komand supports two different categories: plugin based triggers, and API triggers.

Plugin-based triggers

Plugin-based triggers provide a wide variety of functionality to connect to different services. Additionally, these plugins have specifically built trigger actions included within its integration.

To find community-contributed plugins, checkout the [Komand Marketplace](#).

Common Triggers

Plugins also have the following plugin categories:

- Timer Plugins trigger a workflow based on a schedule you define, such as every minute, hour, day, or week.
- Mailbox Triggers include Gmail, Office 365, Exchange, and IMAP Plugin.

API Triggers

You can customize an API trigger that will ingest information via its schema and variables that you specify.

[API Triggers](#) allow you to create a generic POST-based REST endpoint that accepts JSON to trigger a workflow. You can use an API trigger to connect Komand to any service that can POST JSON data to Komand to trigger some automation.

Ex. 33 (<https://docs.komand.com/docs/triggers>).

VirusTotal

This plugin can enrich data source by verifying if a found indicator is malicious, and if so, why. It is a popular threat intel source.

ExtractIt

A commonly used utility plugin that is included with your Komand instance. This provides the capability to parse sensitive information such as URLs, IP addresses, hashes, file paths, etc. This plugin eliminates the need to write regex to match these patterns and parse out the given data.

Ex. 34 (<https://docs.komand.com/docs/popular-plugins>).

How To Use

You should now be presented with a 'How To Use' URL, which gives you a URL you can use to configure for your application.

How to Use

Trigger Workflow

Use this URL to run all workflows with this trigger.

API Call URL

Note: The HTTP Authorization header must contain your api key.

`https://komand.komand.net/v2/triggers/8e58f270-21f8-47e8-925e-5d5940957466/events` COPY

Sample cURL Command

```
curl -X POST -d '{"ip": "", "event": {}}' -H 'Authorization: eeeeeee-c7b1-4a2d-be9b-7be6da964c56' https://komand.komand.net/v2/triggers/8e58f270-21f8-47e8-925e-5d5940957466/events
```

COPY

Ex. 35 (<https://docs.komand.com/docs/creating-api-triggers>).

125. Defendants' infringement of the '289 Patent has injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty. Additionally, as a result of Defendants' unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendants compete in the security software space, and Finjan is actively engaged in licensing its patent portfolio, as described above. Defendants' continued infringement of the '289 Patent causes harm to Finjan in the form of price erosion, loss of goodwill, damage to reputation, loss of business opportunities, inadequacy of money damages, and direct and indirect competition. Monetary damages are insufficient to compensate Finjan for these harms, and thus Finjan is entitled to preliminary and/or permanent injunctive relief.

126. Defendants have been long-aware of Finjan's patents, including the '289 Patent, and continued their unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendants for

over two years regarding Defendants' infringement of Finjan's Asserted Patents. Even after being shown that their products infringe Finjan's patents, including the '289 Patent, on information and belief Defendants made no effort to avoid infringement. Instead, Defendants continued to incorporate their infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendants' blatant and egregious disregard for Finjan's patent rights.

127. Despite their knowledge of Finjan's patent portfolio and Asserted Patents, and their specific knowledge of their own infringement, Defendants continued to sell the Accused Products in complete and reckless disregard of Finjan's patent rights. As such, Defendant acted recklessly, willfully, wantonly, and deliberately engaged in acts of infringement of the '289 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT VIII

(Indirect Infringement of the '289 Patent pursuant to 35 U.S.C. § 271(b))

128. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

129. In addition to directly infringing the '289 Patent, Defendants knew or were willfully blind to the fact that they were inducing infringement of at least Claims 1-9, 19-21, 25-29, 35-40 of the '289 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring their customers to perform the steps of the method claims of the '289 Patent, either literally or under the doctrine of equivalents.

130. Additionally, Defendants knew or were willfully blind to the fact that they were inducing infringement of at least Claims 1-9, 19-21, 25-29, 35-40 of the '289 Patent under 35

U.S.C. § 271(b) by instructing, directing and requiring their developers to perform the steps of the method claims of the '289 Patent, either literally or under the doctrine of equivalents.

131. To the extent one Defendant is deemed to direct and control the other Defendant to directly infringe the '289 Patent, the former Defendant is liable for inducing the latter Defendant to directly infringe the '289 Patent.

132. Defendants knowingly and actively aided and abetted the direct infringement of the '289 Patent by instructing and encouraging their customers and developers to use the '289 Accused Products. Such instructions and encouragement included advising third parties to use the '289 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '289 Patent, and by advertising and promoting the use of the '289 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '289 Accused Products in an infringing manner. *See, e.g.*, Ex. 15 (Nexpose API 1.1 and 1.2 Guide (v. 6.0)); Ex. 15

(https://www.rapid7.com/docs/download/Nexpose_API_guide.pdf); Ex. 19

(<https://nexpose.help.rapid7.com/docs/working-with-vulnerabilities>); Ex. 21

(<https://insightidr.help.rapid7.com/docs/threats>); Ex. 14

(<https://metasploit.help.rapid7.com/docs/vulnerability-scanning-with-nexpose>); Ex. 18

(<https://www.rapid7.com/solutions/attacker-behavior-analytics/>); Ex. 22

(<https://nexpose.help.rapid7.com/docs/sending-custom-fingerprints-to-paired-scan-engines>);

Ex. 23 (<https://blog.rapid7.com/2018/04/17/attacker-behavior-analytics-detects-unknown-threats/>).

COUNT IX

(Direct Infringement of the ‘154 Patent pursuant to 35 U.S.C. § 271(a))

133. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

134. Defendants have infringed and continue to infringe Claims 1-12 of the ‘154 Patent in violation of 35 U.S.C. § 271(a).

135. Defendants’ infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

136. Defendants’ acts of making, using, importing, selling, and offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

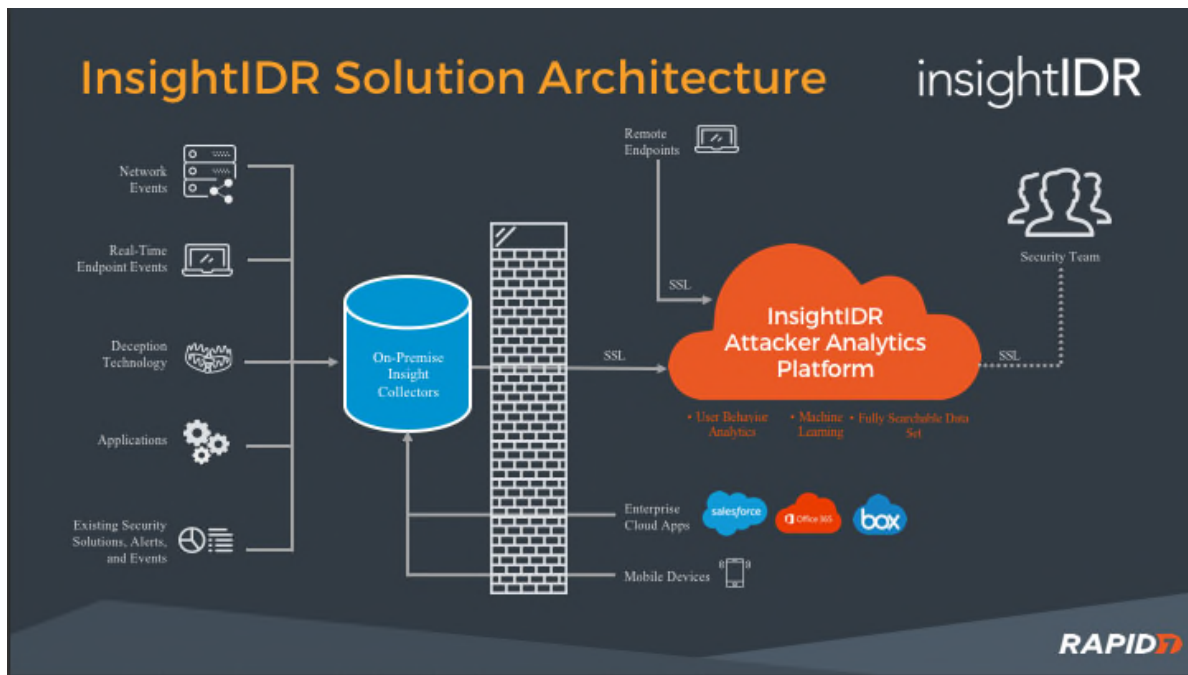
137. Defendants’ infringement includes the manufacture, use, sale, importation and offer for sale of Defendants’ products and services that utilize InsightIDR, InsightVM (Nexpose), Metasploit and Komand technologies, including Rapid7 Insight Platform products (collectively, the “‘154 Accused Products”).

138. The ‘154 Accused Products embody the patented invention of the ‘154 Patent and infringe the ‘154 Patent because they make or use the patented system for protecting a computer from dynamically generated malicious content by, for example, using a content processor to process a first function and invoke a second function if a security computer indicates that it is safe to invoke the second function.

139. To the extent the ‘154 Accused Products use a system that includes modules, components or software owned by third parties, the ‘154 Accused Products still infringe the ‘154 Patent because Defendants are vicariously liable for the use of the patented system by controlling the entire system and deriving a benefit from the use of every element of the entire system.

Similarly, to the extent Defendants’ customers perform a step or steps of the patented method or the ‘154 Accused Products incorporate third parties’ modules, components or software that perform one or more patented steps, Defendants’ ‘154 Accused Products still infringed the ‘154 Patent because the ‘154 Accused Products condition receipt by the third parties of a benefit upon performance of a step or steps of the patented method and establish the manner or timing of that performance.

140. For example, as shown below, the ‘154 Accused Products use a security computer utilizing various scanning and detection technologies to determine if invoking the second function with the input is safe. The content processor will only invoke the second function with the input if the security computer indicates that such invocation is safe.



Ex. 11 (<https://insightidr.help.rapid7.com/docs/welcome-to-insightidr>).

141. The ‘154 Accused Products use transmitters (e.g., “The Collector” and “Insight Agent”) for transmitting the input to the security computer for inspection, when the first function is invoked.

Data Collection Methods

Asset & Endpoint Data Collection

InsightIDR gathers information about your network and assets in two different ways: **the Collector and the Insight Agent**

The Collector

The **Collector** is an on-premise component of InsightIDR that gathers data from [event sources](#).

The Insight Agent

The **Insight Agent**, however, is a service on your individual assets (employee computers, guest laptops, workstations, etc) that collects system information and sends it back to InsightIDR for analysis and user attribution services. The Insight Agent has **two modes**: the persistent mode, which is an installed service that collects information about your asset on an ongoing basis, and the scan mode, which is not an installed service but monitors your assets and endpoints at specific intervals during a collector's scan.

Ex. 36 (<https://insightidr.help.rapid7.com/docs/collection-methods>).

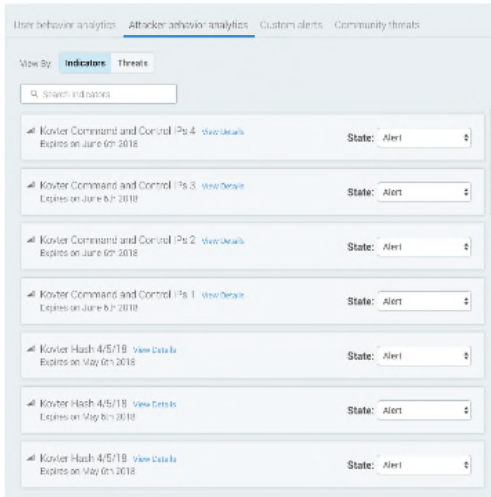
142. The security computer indicates to the receiver whether it is safe to invoke the second function with the input.

Attacker Behavior Analytics (ABA)

Attacker Behavior Analytics are pre-built detections modeled around our wide array of threat intelligence. Attacker Behavior Analytics expose the finite ways attackers gain persistence on an asset, and send and receive commands to victim machines.

Each ABA detection hunts for a unique attacker behavior, which you can toggle to an alert, whitelist, or track as notable behavior. To manage these settings, go to Settings > Alert Settings > Attacker Behavior Analytics. Find the indicator or threat you want to manage and change the state in the provided dropdown menu.

See [Attacker Behavior Analytics \(ABA\)](#) for more information.

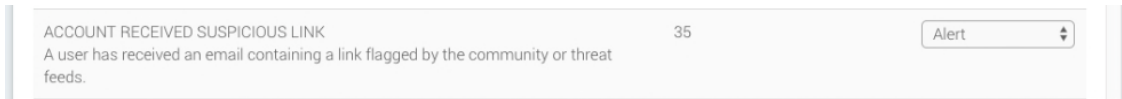


Ex. 17 (<https://insightidr.help.rapid7.com/docs/new-features>).

Managing Built-in Alerts

By default, InsightIDR will generate an alert when any kind of attack behavior is detected. You can change how InsightIDR alerts you if you need to.

Ex. 37 (<https://insightidr.help.rapid7.com/docs/alerts>).



Id.

Quickly respond to phishing attacks underway

Once a malicious phishing campaign has been identified, InsightPhish enables you to immediately notify your organization; this rapid response limits the impact of the campaign.

Ex. 9 (rapid7-product-brochure.pdf) at 13.

InsightIDR

Rapid7's flagship incident detection and response tool, InsightIDR, improves visibility across your entire ecosystem to find intruders earlier in the attack chain. In other words, you'll be alerted to suspicious activity as soon as it happens, so you can investigate and respond before critical data is compromised.

Ex. 38 (<https://www.rapid7.com/solutions/incident-detection-and-response/>).

143. Defendants' infringement of the '154 Patent has injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty. Additionally, as a result of Defendants' unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendants compete in the security software space, and Finjan is actively engaged in licensing its patent portfolio, as described above. Defendants' continued infringement of the '154 Patent causes harm to Finjan in the form of price erosion, loss of goodwill, damage to reputation, loss of business opportunities, inadequacy of money damages, and direct and indirect competition. Monetary damages are insufficient to compensate Finjan for these harms, and thus Finjan is entitled to preliminary and/or permanent injunctive relief.

144. Defendants have been long-aware of Finjan's patents, including the '154 Patent, and continued their unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendants for over two years regarding Defendants' infringement of Finjan's Asserted Patents. Even after being shown that their products infringe Finjan's patents, including the '154 Patent, on information and belief Defendants made no effort to avoid infringement. Instead, Defendants continued to incorporate their infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendants' blatant and egregious disregard for Finjan's patent rights.

145. Despite their knowledge of Finjan's patent portfolio and Asserted Patents, and their specific knowledge of their own infringement, Defendants continued to sell the Accused

Products in complete and reckless disregard of Finjan's patent rights. As such, Defendant acted recklessly, willfully, wantonly, and deliberately engaged in acts of infringement of the '408 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT X

(Direct Infringement of the '918 Patent pursuant to 35 U.S.C. § 271(a))

146. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

147. Defendants infringed Claims 1-36 of the '918 Patent in violation of 35 U.S.C. § 271(a).

148. Defendants' infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

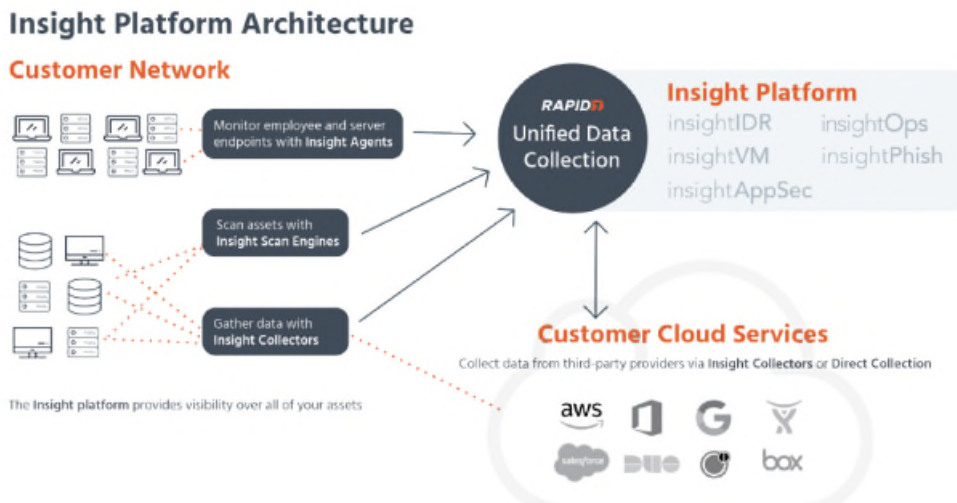
149. Defendants' acts of making, using, importing, selling, and offering for sale infringing products and services were without the permission, consent, authorization or license of Finjan.

150. Defendants' infringement included the manufacture, use, sale, importation and offer for sale of Defendants' products and services that utilize InsightIDR, InsightVM (Nexpose), Metasploit and Komand technologies, including Rapid7 Insight Platform products (collectively, the "918 Accused Products").

151. The '918 Accused Products embody the patented invention of the '918 Patent and infringed the '918 Patent because they make or use the patented system or perform the patented method for enforcing a security context on a downloadable by, for example, making use of security contexts that are associated within certain user/group computer accounts when deriving a profile for code received from the Internet.

152. To the extent the ‘918 Accused Products used a system that includes modules, components or software owned by third parties, the ‘918 Accused Products still infringed the ‘918 Patent because Defendants are vicariously liable for the use of the patented system by controlling the entire system and deriving a benefit from the use of every element of the entire system. Similarly, to the extent Defendants’ customers performed a step or steps of the patented method or the ‘918 Accused Products incorporated third parties’ modules, components or software that performed one or more patented steps, Defendants’ ‘918 Accused Products still infringed the ‘918 Patent because the ‘918 Accused Products condition receipt by the third parties of a benefit upon performance of a step or steps of the patented method and established the manner or timing of that performance.

153. For example, the ‘918 Accused Products are computer-based platforms that include the Rapid7 Scanning Engines which control the function and operation of various computers and servers to provide security and analyze content that may contain potentially malicious content.



Ex. 10 (Rapid7 Insight Platform Security) at 3.

154. Rapid7 Cloud Products provides the ability to manage and oversee client computers and user accounts in real time.

Rapid7's Insight Platform is a single place for you to manage your Rapid7 product(s) from one place, focused on better user management, product management, and enhanced security to your data. Other products include InsightIDR, InsightVM, InsightAppSec, and other upcoming products.

Ex. 39 (<https://insightops.help.rapid7.com/docs/insightops-insightplatform>).

Data Enrichment

InsightOps automatically enriches your live data with the relevant details needed to identify problems quickly. You can use the InsightOps [Collector](#) to normalize your unstructured data automatically into a consistent JSON format.

Live Endpoint Visibility

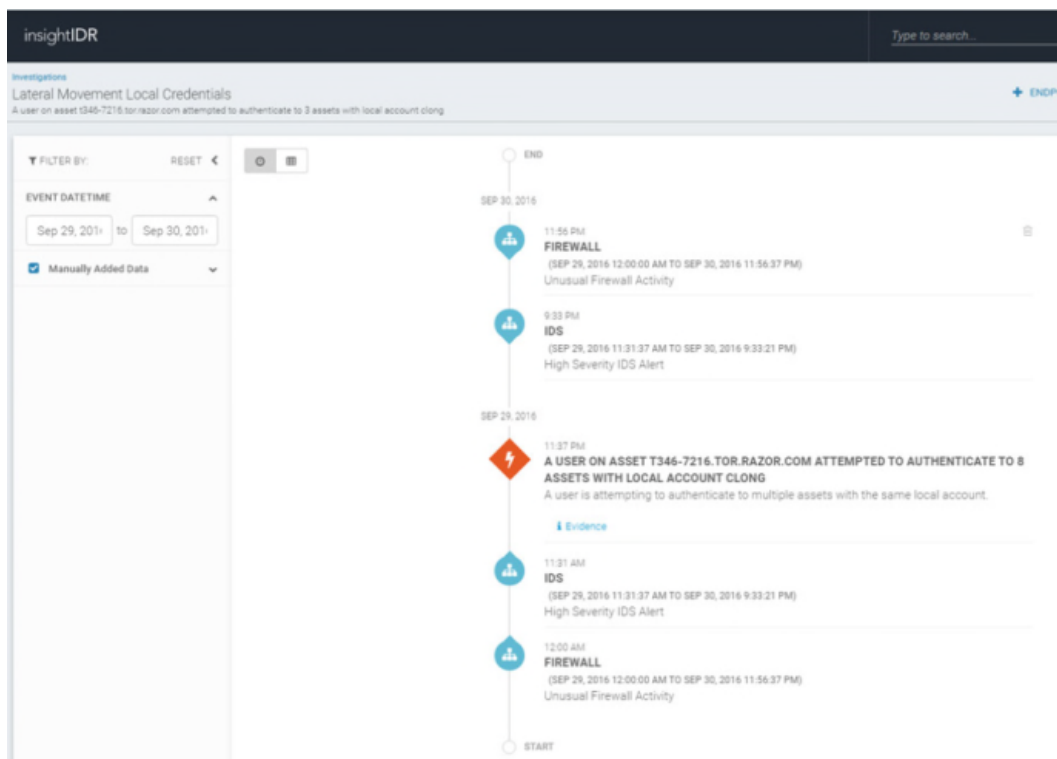
Sometimes you need answers beyond what traditional logs can provide. What processes are running on a particular server? Which laptop on my network is sending the most traffic? With [Endpoint Interrogator](#), you can ask specific questions of your endpoints for immediate answers.

Rapid7 is your operations center for endpoint visibility and infrastructure analytics and combines live endpoint visibility with log analytics, creating one console for total infrastructure awareness.

InsightOps is an easy-to-use log management and analytics service for teams of all sizes. In addition, it provides world-class search capabilities, enhanced log analysis tooling, and the ability to monitor and query the real-time state of your infrastructure.

Ex. 40 (<https://insightops.help.rapid7.com/docs/>).

155. The '918 Accused Products may block content from being processed and alert an appropriate computer account (e.g., administrator account) which may then process the content or approve an exception to a security policy:



Ex. 41 (<https://www.rapid7.com/explore/insightidr/detect-lateral-movement/index.php?step=3>).



Ex. 11 (<https://insightidr.help.rapid7.com/docs>); Ex. 42 (<https://www.rapid7.com/docs/nexpose-wcl-report09.pdf>); Ex. 43 (<https://www.rapid7.com/products/insightvm/integrations/>); Ex. 44 (<https://blog.rapid7.com/2013/11/05/nexpose-and-controlsinsight-better-together-2/>).

If the vulnerability has the following exception status...	...and you have the following permission...	...you can take the following action:
never been submitted for an exception	Submit Exception Request	submit an exception request
previously approved and later deleted or expired	Submit Exception Request	submit an exception request
under review (submitted, but not approved or rejected)	Review Vulnerability Exceptions	approve or reject the request
excluded for another instance, asset, or site	Submit Exception Request	submit an exception request
under review (and submitted by you)		recall the exception
under review (submitted, but not approved or rejected)	Delete Vulnerability Exceptions	delete the request
approved	Review Vulnerability Exceptions	view and change the details of the approval, but not overturn the approval
rejected	Submit Exception Request	submit another exception request
approved or rejected	Delete Vulnerability Exceptions	delete the exception, thus overturning the approval

Your ability to work with vulnerability exceptions depends on your permissions. If you do not now know what your permissions are, consult your Global administrator.

Three permissions are associated with the vulnerability exception workflow:

- Submit Vulnerability Exceptions: A user with this permission can submit requests to exclude vulnerabilities from reports.
- Review Vulnerability Exceptions: A user with this permission can approve or reject requests to exclude vulnerabilities from reports.
- Delete Vulnerability Exceptions: A user with this permission can delete vulnerability exceptions and exception requests. This permission is significant in that it is the only way to overturn a vulnerability request approval. In that sense, a user with this permission can wield a check and balance against users who have permission to review requests.

Ex. 45 (<https://nexpose.help.rapid7.com/docs/working-with-vulnerability-exceptions>).

156. Defendants’ infringement of the ‘918 Patent injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty.

157. Defendants have been long-aware of Finjan’s patents, including the ‘918 Patent, and continued their unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendants for

over two years regarding Defendants' infringement of Finjan's Asserted Patents. Even after being shown that their products infringe Finjan's patents, including the '918 Patent, on information and belief Defendants made no effort to avoid infringement. Instead, Defendants continued to incorporate their infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendants' blatant and egregious disregard for Finjan's patent rights.

158. Despite their knowledge of Finjan's patent portfolio and Asserted Patents, and their specific knowledge of their own infringement, Defendants continued to sell the Accused Products in complete and reckless disregard of Finjan's patent rights. As such, Defendant acted recklessly, willfully, wantonly, and deliberately engaged in acts of infringement of the '918 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT XI

(Indirect Infringement of the '918 Patent pursuant to 35 U.S.C. § 271(b))

159. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

160. In addition to directly infringing the '918 Patent, Defendants knew or were willfully blind to the fact that they were inducing infringement of at least Claims 1-11, 22-27, 34 of the '918 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring their customers to perform the steps of the method claims of the '918 Patent, either literally or under the doctrine of equivalents.

161. Additionally, Defendants knew or were willfully blind to the fact that they were inducing infringement of at least Claims 1-11, 22-27, 34 of the '918 Patent under 35 U.S.C.

§ 271(b) by instructing, directing and requiring their developers to perform the steps of the method claims of the '918 Patent, either literally or under the doctrine of equivalents.

162. To the extent one Defendant is deemed to direct and control the other Defendant to directly infringe the '918 Patent, the former Defendant is liable for inducing the latter Defendant to directly infringe the '918 Patent.

163. Defendants knowingly and actively aided and abetted the direct infringement of the '918 Patent by instructing and encouraging their customers and developers to use the '918 Accused Products. Such instructions and encouragement included advising third parties to use the '918 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '918 Patent, and by advertising and promoting the use of the '918 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '918 Accused Products in an infringing manner. *See, e.g.*, Ex. 15 (Nexpose API 1.1 and 1.2 Guide (v. 6.0)); Ex. 15

(https://www.rapid7.com/docs/download/Nexpose_API_guide.pdf); Ex. 19

(<https://nexpose.help.rapid7.com/docs/working-with-vulnerabilities>); Ex. 21

(<https://insightidr.help.rapid7.com/docs/threats>); Ex. 14

(<https://metasploit.help.rapid7.com/docs/vulnerability-scanning-with-nexpose>); Ex. 18

(<https://www.rapid7.com/solutions/attacker-behavior-analytics/>); Ex. 22

(<https://nexpose.help.rapid7.com/docs/sending-custom-fingerprints-to-paired-scan-engines>);

Ex. 23 (<https://blog.rapid7.com/2018/04/17/attacker-behavior-analytics-detects-unknown-threats/>).

COUNT XII

(Direct Infringement of the '086 Patent pursuant to 35 U.S.C. § 271(a))

164. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

165. Defendants infringed Claims 1-42 of the '086 Patent in violation of 35 U.S.C. § 271(a).

166. Defendants' infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

167. Defendants' acts of making, using, importing, selling, and offering for sale infringing products and services were without the permission, consent, authorization or license of Finjan.

168. Defendants' infringement included the manufacture, use, sale, importation and offer for sale of Defendants' products and services that utilize InsightIDR, InsightVM (Nexpose), Metasploit and Komand technologies, including Rapid7 Insight Platform products (collectively, the "'086 Accused Products").

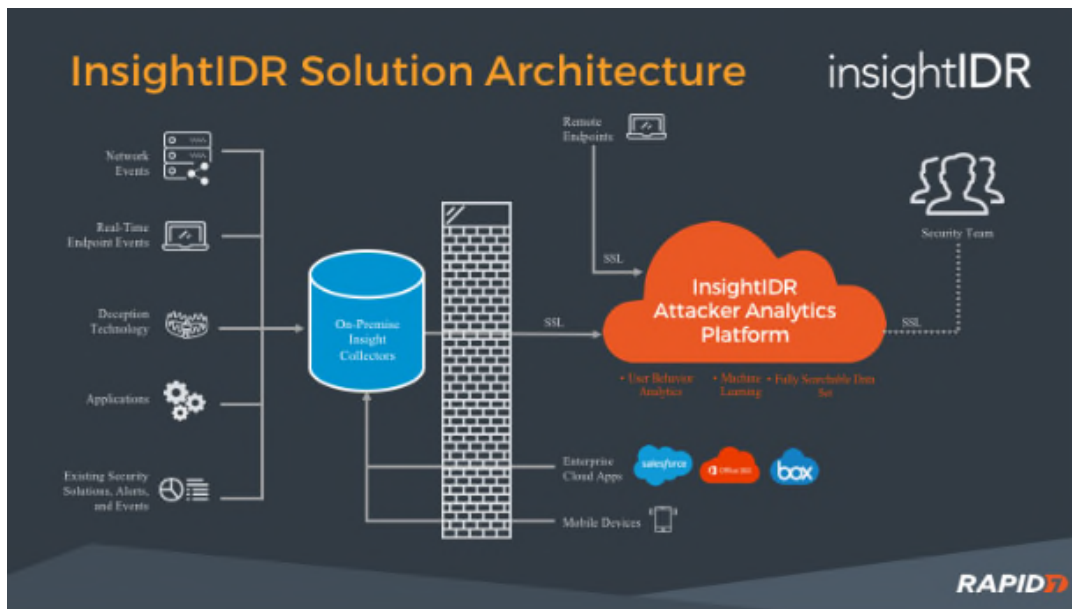
169. The '086 Accused Products embody the patented invention of the '086 Patent and infringed the '086 Patent because they make or use the patented system or perform the patented method of protecting devices connected to the Internet from undesirable operations from web-based content, by, for example, creating a profile of the web-based content and sending a representation of these profiles to another computer for appropriate action.

170. To the extent the '086 Accused Products used a system that includes modules, components or software owned by third parties, the '086 Accused Products still infringed the '086 Patent because Defendants are vicariously liable for the use of the patented system by controlling the entire system and deriving a benefit from the use of every element of the entire

system. Similarly, to the extent Defendants’ customers performed a step or steps of the patented method or the ‘086 Accused Products incorporated third parties’ modules, components or software that performed one or more patented steps, Defendants’ ‘086 Accused Products still infringed the ‘086 Patent because the ‘086 Accused Products condition receipt by the third parties of a benefit upon performance of a step or steps of the patented method and established the manner or timing of that performance.

171. For example, as shown below, the ‘086 Accused Products receive and collect incoming Downloadables, including suspicious web page content containing HTML, PDFs, JavaScript, drive-by downloads, obfuscated code, or other blended web malware.

Downloadables that pass through the firewall are received by the InsightIDR platform.



Ex. 11 (<https://insightidr.help.rapid7.com/docs>).

Rapid7 uses collectors to gather information from on-premises and cloud networks and to securely transfer data to the Insight platform. Collectors sit behind the client's firewall, respond to changes in the environment, and securely transmit relevant data to the Insight platform for analysis. Collectors were designed with the following core tenets in mind:

- Collectors can be configured only by administrators.
- All data is secured during the transmission process, which uses strong encryption protocols.
- Data transferred from each separate collector is uniquely identified and stored and cannot be accessed by any third parties.

Ex. 10 (Rapid7 Insight Platform Security) at 4.

172. The '086 Accused Products include Rapid7 Scan Engines, which detect vulnerabilities and pattern attributes using behavioral analytics to derive a security profile. The '086 Accused Products also store certain attributes in a database and use them in the future to speed up analyses by comparing the behavioral patterns (e.g., pattern attributes) against other Downloadables.

Every vulnerability discovered in the scanning process is added to the vulnerability database. This extensive, full-text, searchable database also stores information on patches, downloadable fixes, and reference content about security weaknesses. The application keeps the database current through a subscription service that maintains and updates vulnerability definitions and links. It contacts this service for new information every six hours.

The database has been certified to be compatible with the MITRE Corporation's Common Vulnerabilities and Exposures (CVE) index, which standardizes the names of vulnerabilities across diverse security products and vendors. The index rates vulnerabilities according to MITRE's Common Vulnerabilities Scoring System (CVSS) Version 2 and Version 3, if it is available.

An application algorithm computes the CVSS score based on ease of exploit, remote execution capability, credentialed access requirement, and other criteria. The score, which ranges from 1.0 to 10.0, is used in Payment Card Industry (PCI) compliance testing. For more information about CVSS scoring, go to the FIRST Web site <https://www.first.org/cvss/>.

Ex. 21 (<https://nexpose.help.rapid7.com/docs/working-with-vulnerabilities>).

Every fingerprint contains a *pattern* attribute with the regular expression to match against the data.

An optional flags attribute controls how the regular expression is to be interpreted. See the [Recog documentation for FLAG_MAP](#) for more information.

Each fingerprint contains a *description* element with a human-readable string describing the fingerprint.

If you develop custom fingerprints, you can have the Security Console distribute them automatically to any paired Scan Engine that is currently in use when a scan is run. To do so, simply copy the fingerprint files to the [installation_directory]/plugins/fp/custom/ directory on your Security Console host.

Ex. 22 (<https://nexpose.help.rapid7.com/docs/sending-custom-fingerprints-to-paired-scan-engines>).

Attacker Behavior Analytics Library

Below is a list of released ABA detections, all of which come with our threat detection solution, **InsightIDR**, and automatically match against your data in real time. This is threat intelligence that moves at the speed of the attacker—if a new exploit comes out, our team will craft a detection, test it against the **Rapid7 Insight platform**, and deploy it in InsightIDR—all within hours. Still craving that aged, open-source threat feed now?

Ex. 18 (<https://www.rapid7.com/solutions/attacker-behavior-analytics/>).

173. Rapid7 Cloud Products also assign an advanced RealRisk™ score based on a Common Vulnerability Scoring System (CVSS), temporal risk and asset importance metrics associated with vulnerabilities associated with the Downloadable.

Focus on the Highest Risks Using RealRisk™

Nexpose provides an advanced vulnerability scoring algorithm, RealRisk™, that provides insights into the most critical vulnerabilities. It leverages threat intelligence such as exploit and malware kit exposure, CVSS v2, temporal risk, and asset importance metrics to give you a granular score for risk prioritization.

- **Comprehensive Vulnerability Database** with more than 96,500 vulnerability checks for over 34,000 vulnerability definitions.
- **Largest public database of quality-assured exploits and payloads**, making your penetration tests both realistic and safe to simulate attacks on your infrastructure.

$$\text{Rapid7 Real Risk} = \frac{\text{CVSS Impact Metrics}}{\text{CVSS Likelihood Metrics}} \times \text{Exposure} \left(\frac{\text{Malware Kits}}{\text{Exploit Rank}} \cdot \text{time} \right)$$

Exs. 12, 46.

174. The '086 Accused Products also store these vulnerabilities using a unique ID.

Name	Description	Datatype	Range
vuln-id	a unique identifier of a vulnerability in the application's vulnerability database (required)	xs:string	any sequence of characters allowed in XML; of any length
vuln-key	a string representing the specific vulnerable component in a discovered instance of the vulnerability referenced by the vuln-id attribute, such as a program, file or user account (optional)	xs:string	any sequence of characters allowed in XML; of any length

Ex. 15 (Nexpose API 1.1 and 1.2 Guide (v. 6.0)) at 175, 176; *see id.* at 28, 178.

175. The vulnerability data are stored in a database.

Analyzing the vulnerabilities discovered in scans is a critical step in improving your security posture. By examining the frequency, affected assets, risk level, exploitability and other characteristics of a vulnerability, you can prioritize its remediation and manage your security resources effectively.

Every vulnerability discovered in the scanning process is added to the vulnerability database. This extensive, full-text, searchable database also stores information on patches, downloadable fixes, and reference content about security weaknesses. The application keeps the database current through a subscription service that maintains and updates vulnerability definitions and links. It contacts this service for new information every six hours.

Ex. 21 (<https://nexpose.help.rapid7.com/docs/working-with-vulnerabilities>).

176. The ‘086 Accused Products perform a hash of the Downloadables in order to associate the information with the unique hash of a particular Downloadable.

The screenshot displays the 'Process Hash Details' for a file. It includes a list of file details such as MD5, SHA1, Operating System, File Size, Signature Verification, Commonality, Signers, File Names, and VirusTotal Report. Below the details, there is a section for 'ASSETS RUNNING THIS HASH' with a filter set to '1w'.

FILE DETAILS	
MD5	e4c53ce8409dcff708c790a0ac76398d
SHA1	44cbf8dff2fe6aa7b264eeaa33e02ad1fa4a6796
Operating System	Microsoft Windows
File Size	264 kB
Signature Verification	Signed, verified signature
Commonality	Rare
Signers	C=US, S=California, L=Fremont, O=Logitech, Inc., OU=Digital ID Class 3 - Microsoft Software Validation v2, CN=Logitech, Inc. C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 Code Signing 2010 CA C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G5
File Names	camerahelpershell.exe
VirusTotal Report	See Report


ASSETS RUNNING THIS HASH

loom **1w** 1m All

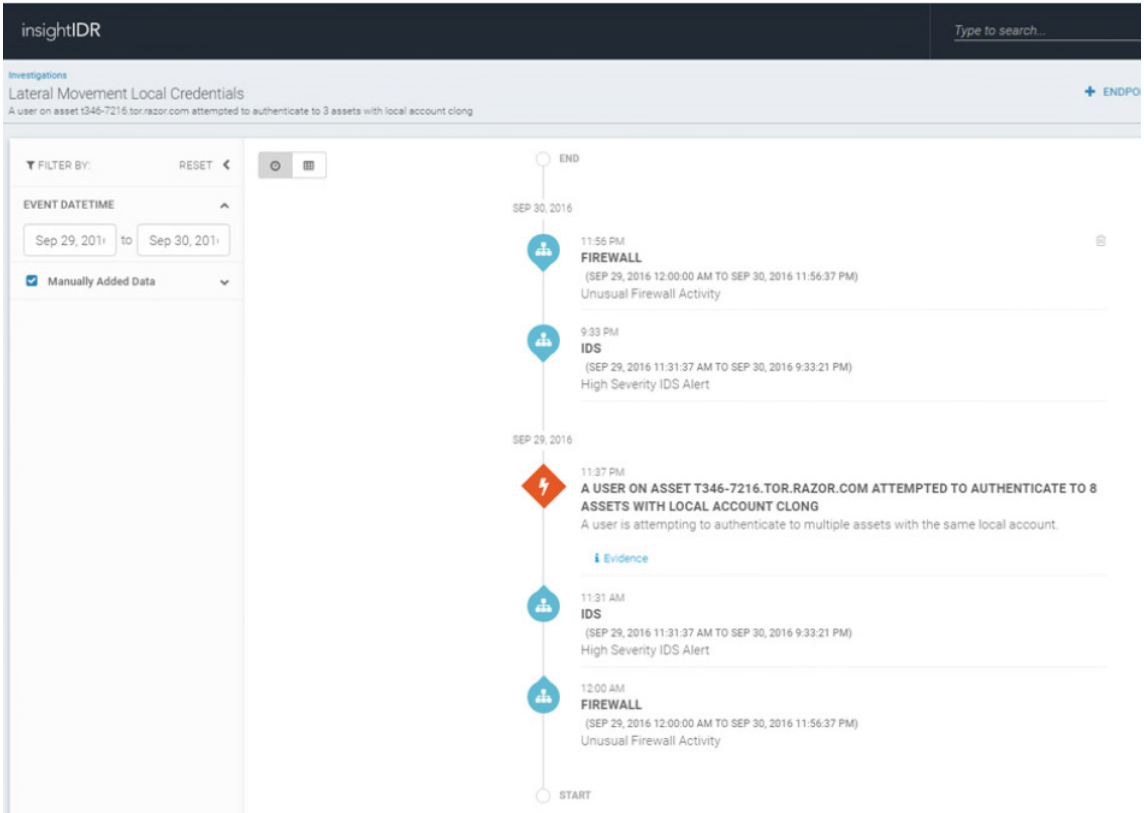
Ex. 26 (<https://www.rapid7.com/explore/insightidr/endpoint-capabilities/index.php?step=8>).

177. The ‘086 Accused Products append a representation of the Downloadable security profile data to the Downloadable to generate an appended Downloadable because the ‘086 Accused Products create metadata about suspicious or malicious files which are a representation of the Downloadable security profile data. These metadata, including for example, the

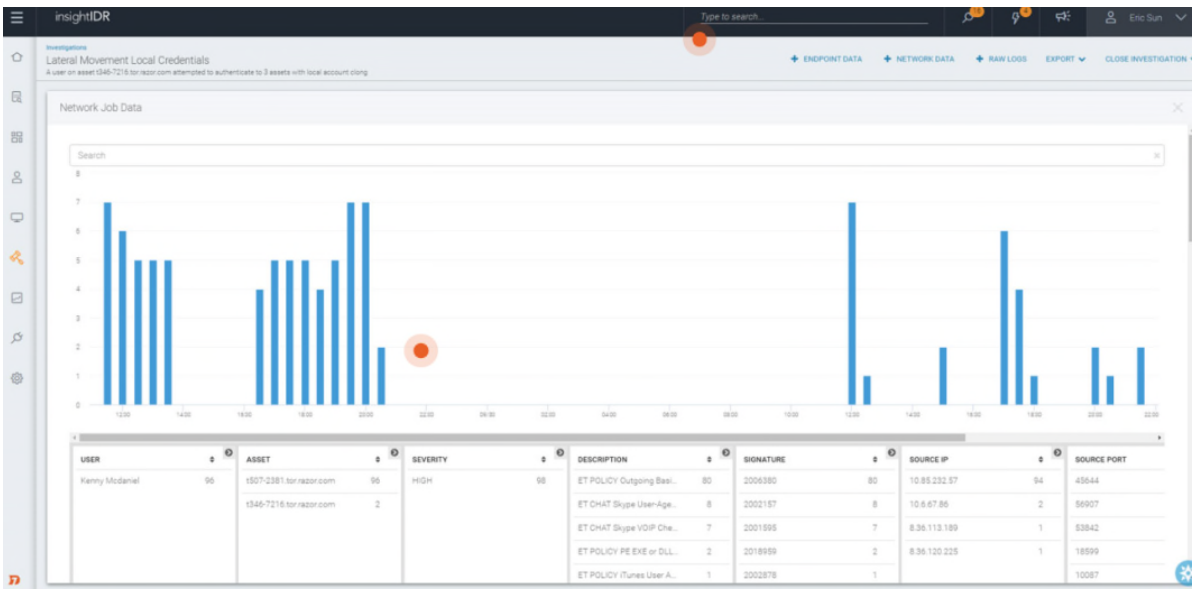
vulnerability ID, pattern attributes, and RealRisk Score are appended to the Downloadable. For example, a Downloadable with at least one malware is sent with appended metadata and the metadata can be readily viewed by selecting an icon

For each discovered vulnerability that has at least one malware kit (also known as an *exploit kit*) associated with it, the console displays a malware exposure icon . If you click the icon, the console displays the *Threat Listing* pop-up window that lists all the malware kits that attackers can use to write and deploy malicious code for attacking your environment through the vulnerability. You can generate a comma-separated values (CSV) file of the malware kit list to share with others in your organization. Click the **Export to CSV** icon . Depending on your browser settings, you will see a pop-up window with options to save the file or open it in a compatible program.

178. These metadata are sent appended with a sample or copy of the file in which the threat appeared, and includes the path to that file, the filename, the date and time, information pertaining to the downloadable, the process by which the threat appeared and information about the operating system.



Ex. 41 (<https://www.rapid7.com/explore/insightidr/detect-lateral-movement/index.php?step=3>).



Ex. 47 (<https://www.rapid7.com/explore/insightidr/detect-lateral-movement/index.php?step=5>).

179. Defendants’ infringement of the ‘086 Patent injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty.

180. Defendants have been long-aware of Finjan's patents, including the '086 Patent, and continued their unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendants for over two years regarding Defendants' infringement of Finjan's Asserted Patents. Even after being shown that their products infringe Finjan's patents, including the '086 Patent, on information and belief Defendants made no effort to avoid infringement. Instead, Defendants continued to incorporate their infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendants' blatant and egregious disregard for Finjan's patent rights.

181. Despite their knowledge of Finjan's patent portfolio and Asserted Patents, and their specific knowledge of their own infringement, Defendants continued to sell the Accused Products in complete and reckless disregard of Finjan's patent rights. As such, Defendant acted recklessly, willfully, wantonly, and deliberately engaged in acts of infringement of the '086 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT XIII

(Indirect Infringement of the '086 Patent pursuant to 35 U.S.C. § 271(b))

182. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

183. In addition to directly infringing the '086 Patent, Defendants knew or were willfully blind to the fact that they were inducing infringement of at least Claims 1-23, 31-36, 39, 41 of the '086 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring their customers to perform the steps of the method claims of the '086 Patent, either literally or under the doctrine of equivalents.

184. Additionally, Defendants knew or were willfully blind to the fact that they were inducing infringement of at least Claims 1-23, 31-36, 39, 41 of the '086 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring their developers to perform the steps of the method claims of the '086 Patent, either literally or under the doctrine of equivalents.

185. To the extent one Defendant is deemed to direct and control the other Defendant to directly infringe the '086 Patent, the former Defendant is liable for inducing the latter Defendant to directly infringe the '086 Patent.

186. Defendants knowingly and actively aided and abetted the direct infringement of the '086 Patent by instructing and encouraging their customers and developers to use the '086 Accused Products. Such instructions and encouragement included advising third parties to use the '086 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '086 Patent, and by advertising and promoting the use of the '086 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '086 Accused Products in an infringing manner. *See, e.g.*, Ex. 15 (Nexpose API 1.1 and 1.2 Guide (v. 6.0)); Ex. 15

(https://www.rapid7.com/docs/download/Nexpose_API_guide.pdf); Ex. 19

(<https://nexpose.help.rapid7.com/docs/working-with-vulnerabilities>); Ex. 21

(<https://insightidr.help.rapid7.com/docs/threats>); Ex. 14

(<https://metasploit.help.rapid7.com/docs/vulnerability-scanning-with-nexpose>); Ex. 18

(<https://www.rapid7.com/solutions/attacker-behavior-analytics/>); Ex. 22

(<https://nexpose.help.rapid7.com/docs/sending-custom-fingerprints-to-paired-scan-engines>);

Ex. 23 (<https://blog.rapid7.com/2018/04/17/attacker-behavior-analytics-detects-unknown-threats/>).

PRAYER FOR RELIEF

WHEREFORE, Finjan prays for judgment and relief as follows:

A. An entry of judgment holding that Defendants infringed the ‘305, ‘408, ‘289, ‘918, ‘086, ‘154, and ‘494 Patents; are infringing the ‘305, ‘408, ‘289, and ‘154 Patents; induced infringement of the ‘305, ‘408, ‘289, ‘918, ‘086, and ‘494 Patents and are inducing infringement of ‘305, ‘408, and ‘289 Patents.

B. A preliminary and permanent injunction against Defendants and their officers, employees, agents, servants, attorneys, instrumentalities, and those in privity with them, from infringing the ‘305, ‘408, ‘289, and ‘154 Patents, and from inducing the infringement of the ‘305, ‘408, and ‘289 Patents, and for all further and proper injunctive relief pursuant to 35 U.S.C. § 283;

C. An award to Finjan of such past damages, not less than a reasonable royalty, as it shall prove at trial against Defendants that is adequate to fully compensate Finjan for Defendants’ infringement of the ‘305, ‘408, ‘289, ‘918, ‘086, ‘154, and ‘494 Patents;

D. A determination that Defendants’ infringement has been willful, wanton, and deliberate and that the damages against it be increased up to treble on this basis or for any other basis in accordance with the law;

E. A finding that this case is “exceptional” and an award to Finjan of its costs and reasonable attorneys’ fees, as provided by 35 U.S.C. § 285;

F. An accounting of all infringing sales and revenues, together with post judgment interest and prejudgment interest from the first date of infringement of the ‘305, ‘408, ‘289, ‘918, ‘086, ‘154, and ‘494 Patents; and

G. Such further and other relief as the Court may deem proper and just.

DEMAND FOR JURY TRIAL

Finjan demands a jury trial on all issues so triable.

POTTER ANDERSON & CORROON LLP

OF COUNSEL:

Paul J. Andre
Lisa Kobialka
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
(650) 752-1700

Aaron M. Frankel
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
1177 Avenue of the Americas
New York, NY 10036
(212) 715-9100

Dated: October 1, 2018
5943233

By: /s/ Philip A. Rovner
Philip A. Rovner (#3215)
Jonathan A. Choa (#5319)
Hercules Plaza
P.O. Box 951
Wilmington, DE 19899
(302) 984-6000
provner@potteranderson.com
jchoa@potteranderson.com

*Attorneys for Plaintiff
Finjan, Inc.*