PAUL ANDRE (State Bar No. 196585)
pandre@kramerlevin.com
LISA KOBIALKA (State Bar No. 191404)
lkobialka@kramerlevin.com
JAMES HANNAH (State Bar No. 237978)
jhannah@kramerlevin.com
KRAMER LEVIN NAFTALIS & FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800

Attorneys for Plaintiff
FINJAN, INC.

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

FINJAN, INC., a Delaware Corporation, Plaintiff, v. QUALYS INC., a Delaware Corporation, Defendant.	Case No.: **COMPLAINT FOR PATENT INFRINGEMENT** **DEMAND FOR JURY TRIAL**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Finjan, Inc. ("Finjan") files this Complaint for Patent Infringement and Demand for Jury Trial against Qualys Inc. ("Defendant" or "Qualys") 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. Upon information and belief, Qualys Inc. is a Delaware Corporation with its principle place of business at 919 E. Hillsdale Boulevard, 4th Floor, Foster City, California 94404.

JURISDICTION AND VENUE

3. 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.

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

5. This Court has personal jurisdiction over Defendant. Defendant regularly and continuously does business in this District and has infringed or induced infringement, and continues to do so, in this District. Upon information and belief, Defendant maintains an office within this District in Foster City, California. Upon information and belief, Defendant's office in Foster City is a regular and established place of business and its principal place of business. In addition, the Court has personal jurisdiction over Defendant because minimum contacts have been established with the forum and the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice.

INTRADISTRICT ASSIGNMENT

6. Pursuant to Local Rule 3-2(c), Intellectual Property Actions are assigned on a district-wide basis.

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") awarded to 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 these patented technologies. These products and related customers continue to be supported by Finjan's licensing partners. 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 November 28, 2000, the USPTO issued to Shlomo Touboul and Nachshon Gal U.S. Patent No. 6,154,844 ("the '844 Patent"), titled "SYSTEM AND METHOD FOR ATTACHING A DOWNLOADABLE SECURITY PROFILE TO A DOWNLOADABLE." A true and correct copy of the '844 Patent is attached to this Complaint as Exhibit 1 and is incorporated by reference herein.

10. All rights, title, and interest in the '844 Patent have been assigned to Finjan, who is the sole owner of the '844 Patent. Finjan has been the sole owner of the '844 Patent since its issuance.

11. The ‘844 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 linking a security profile to such web-based content to facilitate the protection of computers and networks from malicious web-based content. The ‘844 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 ‘844 Patent and are more than just generic software components performing conventional activities.

12. 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 2 and is incorporated by reference herein.

13. 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.

14. 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.

15. 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 3 and is incorporated by reference herein.

16. 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.

17. 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.

18. 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 4 and is incorporated by reference herein.

19. 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.

20. 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.

21. On November 15, 2005, the USPTO issued to Shlomo Touboul U.S. Patent No. 6,965,968 (“the ‘968 Patent”), titled “POLICY-BASED CACHING.” A true and correct copy of the ‘968 Patent is attached to this Complaint as Exhibit 5 and is incorporated by reference herein.

22. All rights, title, and interest in the '968 Patent have been assigned to Finjan, who is the sole owner of the '968 Patent. Finjan has been the sole owner of the '968 Patent since its issuance.

23. The '968 Patent is generally directed towards methods and systems for enabling policy-based cache management to determine if digital content is allowable relative to a policy. One of the ways this is accomplished is scanning digital content to derive a content profile and determining whether the digital content is allowable for a policy based on the content profile. The '968 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 '968 Patent and are more than just generic software components performing conventional activities.

24. On August 26, 2008, the USPTO issued to Shlomo Touboul U.S. Patent No. 7,418,731 ("the '731 Patent"), titled "METHOD AND SYSTEM FOR CACHING AT SECURE GATEWAYS." A true and correct copy of the '731 Patent is attached to this Complaint as Exhibit 6 and is incorporated by reference herein.

25. All rights, title, and interest in the '731 Patent have been assigned to Finjan, who is the sole owner of the '731 Patent. Finjan has been the sole owner of the '731 Patent since its issuance.

26. The '731 Patent is generally directed towards methods and systems for providing an efficient security system. One of the ways this is accomplished is by implementing a variety of caches to increase performance of the system. The '731 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 '731 Patent and are more than just generic software components performing conventional activities.

27. 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 7 and is incorporated by reference herein.

28. 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.

29. The '154 Patent is generally directed towards methods and systems for providing an efficient security system. One of the ways this is accomplished is by implementing a variety of caches to increase performance of the system. 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.

30. The patents in paragraphs 9-29 are collectively referred to as the "Asserted Patents."

FINJAN'S NOTICE OF INFRINGEMENT TO DEFENDANT

31. Defendant is well aware of Finjan's patents, including the Asserted Patents, and has continued its infringing activity, despite this knowledge, for years. Finjan gave written notice to Defendant of its infringement of Finjan's patents by letter dated November 12, 2015, which specifically identified Finjan's '844, '494, '305, '968, and '154 Patents. This letter also identified many of Defendant's infringing products including how Defendant's Malware Detection Systems (MDS), Web Application Firewall (WAF), Web Application Scanner (WAS), and Vulnerability (VM) solutions including Qualys Cloud Platform products infringe various of Finjan's Asserted Patents. *See* November 12, 2015 Letter from Finjan to Qualys, attached hereto as Exhibit 23.

32. Finjan also gave Defendant another letter on or about December 7, 2017, in which Finjan described to Defendant how the Accused Products variously infringe Finjan's patents, including at least Finjan's '844, '494, '305, and '968 Patents. *See* December 7, 2017 Letter from Finjan to Qualys, attached hereto as Exhibit 24.

33. Thus, despite Finjan's best efforts to inform Defendant that its products infringe Finjan's patents and to engage Defendant in good-faith licensing discussions, Defendant refused to take a license to Finjan's patents. As shown above, Defendant knew that it infringed the Asserted Patents well before Finjan filed this action, and Defendant acted egregiously and willfully in that it continued to infringe Finjan's patents and, on information and belief, took no action to avoid infringement. Instead, Defendant continued to develop additional technologies and products that

infringe the Asserted Patents. As such, Defendant has continued to willfully, wantonly, and deliberately engage in acts of infringement of the Asserted Patents.

DEFENDANT'S INFRINGING PRODUCTS AND TECHNOLOGIES

34. Defendant makes, uses, sells, offers for sale, and imports into the United States and this District infringing products and services that utilize Vulnerability Management, Threat Protection, Continuous Monitoring, Indicators of Compromise, Container Security, Web App Firewall, Web App Scanning, and Compliance Monitoring, including Qualys Cloud Platform products (collectively, the "Accused Products").

35. Qualys' products are all interrelated through the Qualys Cloud Platform. The Qualys Cloud Platform integrates Qualys' detection and analytic technologies across various product offerings, briefly described below.

Vulnerability Management (VM)

36. Qualys VM continuously scans and identifies vulnerabilities with high-precision accuracy, protecting IT assets on premises, in the cloud, and at mobile endpoints. Its executive dashboard displays an overview of security posture and access to remediation details. VM generates custom, role-based reports for multiple stakeholders, including automatic security documentation for compliance auditors. Additionally, Qualys VM offers vulnerability management for hybrid IT environments.

37. In addition to scanners, VM also works with Qualys Cloud Agents, extending its network coverage to assets that cannot be scanned. The lightweight, all-purpose, self-updating agents reside on the assets they monitor so they do not require scan windows, credentials, or firewall changes, and vulnerabilities can be found with minimal network impact. When VM is paired with Continuous Monitoring (CM), InfoSec teams are proactively alerted about potential threats so problems can be tackled before turning into breaches. Alerts can be tailored to notify about general or specific changes.

Threat Protection

38. Threat Protection continuously correlates external threat information against a vulnerabilities and IT asset inventory, leveraging Qualys Cloud Platform's back-end engine to

automate this large-scale and intensive data analysis process and alert which threats pose the greatest risk at any given time. As Qualys engineers continuously validate and rate new threats from internal and external sources, Threat Protections' Live Threat Intelligence Feed displays the latest vulnerability disclosures and maps them to impacted IT assets.

39. A single, dynamic dashboard includes customizable views, graphs and charts to provide a clear and comprehensive view of the threat landscape at a glance in real time. Multiple dashboard views can be created to break down vulnerabilities by real-time threat indicator types, such as zero-day exploits. Further, Threat Protection's search engine can sort, filter, drill down and fine-tune results for specific assets and vulnerabilities by crafting ad hoc queries with multiple variables and criteria. Queries can be saved and turned into dashboard widgets, which can display trend graphs for up to 90 days.

Continuous Monitoring (CM)

40. CM works in tandem with VM to discover hosts and digital certificates, organize assets by business or technology function, and be alerted as soon as vulnerabilities appear on the global perimeter from a single console. CM acts as a sentinel in the cloud, constantly monitoring the network for changes that could put the network at risk. CM automates monitoring of the global perimeter, tracking systems in the global network, wherever they are.

41. CM can identify and proactively address potential problems. Alerts can be tailored for a wide variety of conditions impacting systems, certificates, ports, services and software. Each rule can be configured to detect common, general changes or tuned to very specific circumstances. Different recipients can be assigned for each alert, so that the appropriate person is notified. The dashboard displays the network's big-picture status at a glance, giving a graphical representation of recent activity to spot anomalies. Important alerts can be flagged and trivial ones can be hid. Specific alerts and their corresponding details can be found using CM's search engine.

Indicators of Compromise (IOC)

42. Qualys IOC uses the Cloud Agent's non-intrusive data collection and delta processing techniques to transparently capture endpoint activity information from assets on and off the network

that is more performant than query-based approaches or log collectors. Customers can use pre-defined threat hunting rules and easily import indicators of compromise artifacts into widgets, dashboards, and saved searches to quickly verify threat intelligence, scale of infections, first-infected asset ("Patient Zero"), and timeline of compromises.

43. Threat hunting, suspicious activity detection, and OpenIOC processing are performed in the Qualys Cloud Platform on billions of active and past system events, and coupled with threat intelligence data from Qualys Malware Labs to identify malware infections (indicators of compromise) and threat actor actions (indicators of activity).

44. Qualys IOC creates a Single View of the Asset, showing threat hunting details unified with other Qualys Cloud Apps for hardware and software inventory, vulnerability posture, policy compliance controls, and file integrity monitoring change alerts for on-premise servers, cloud instances, and off-net remote endpoints. A single user interface significantly reduces the time required for incident responders and security analysts to hunt, investigate, detect, and respond to threats before breach or compromise can occur.

Container Security (CS)

45. Qualys Container Security gives complete visibility of container hosts wherever they are in the global IT environment, on premises and in clouds. It gathers comprehensive topographic information about container projects — images, image registries, and containers spun from the images. The complete inventory and security posture from containers to hosts are viewable from dynamic, customizable dashboards.

46. With Qualys CS, security teams can enforce policies to block the use of images that have specific vulnerabilities, or that have vulnerabilities above a certain severity threshold. Developers can do continuous vulnerability detection and remediation in the DevOps pipeline by deploying plugins for CI/CD tools like Jenkins or Bamboo, or via REST APIs.

47. Qualys CS can search for images that have high-severity vulnerabilities, unapproved packages, and older or test release tags. Their impact can be assessed by identifying all containers — active or dormant — that use the unapproved, vulnerable images. Qualys CS helps determine if these

images are cached on different hosts, and identifies all the containers on exposed vulnerable network ports running with privileges, which could lead to attacks.

48. Qualys CS scans, protects, and secures the running containers. Qualys CS also detects containers drifting from the parent image, breaking the immutable behavior with a different vulnerability posture and software configuration. Qualys CS also features policy-based orchestration to stop containers vulnerable images from being spun up in Kubernetes clusters. Qualys CS can drill down to the host level to identify vulnerabilities and patch compliance to understand how the host impacts the containers.

Web App Firewall (WAF)

49. WAF can deploy virtual patches for confirmed vulnerabilities and can be managed from a centralized portal. With no special hardware to buy nor maintain, Qualys WAF's virtual appliance can be deployed and scaled up quickly on premises using VMware, Hyper-V or Docker, and in public cloud platforms, such as AWS, Azure or Google Cloud Platform. WAF continuously communicates with the Qualys Cloud Platform, tracking configuration changes and sending it the latest security events.

50. WAF gives complete visibility into its data for continuous monitoring, risk assessments and remediation plans. A dashboard summarizes website traffic information and security event trends that include detailed threat information, suspicious activity, and actionable insights into the threat data. WAF continuously indexes security events into local Elasticsearch or Splunk clusters, making data instantly discoverable.

51. WAF protects web apps using security policies backed by Qualys' security intelligence, and one-click responses to security events. Security needs can be addressed with simple, customizable and reusable policies and rules. Qualys' out-of-the-box policies are designed for popular platforms such as WordPress, Joomla, Drupal, Outlook Web Application and Sharepoint. It also includes generic templates for unknown applications and frameworks.

Web App Scanning (WAS)

52. WAS finds and catalogs all web apps in the network, including new and unknown ones, and scales from a handful of apps to thousands. Qualys WAS tags applications with labels to control reporting and limit access to scan data. WAS' dynamic deep scanning covers all apps on the perimeter, in the internal environment and under active development, and even APIs that support mobile devices. It also covers public cloud instances, and gives instant visibility of vulnerabilities like SQLi and XSS. With programmatic scanning of SOAP and REST API services, WAS tests IoT services and APIs used by mobile apps and modern mobile architectures.

53. WAS can insert security into application development and deployment in DevSecOps environments. WAS detects code security issues early and often, tests for quality assurance and generates comprehensive reports. With its tight Qualys WAF integration, WAS continuously monitors and virtually patches production apps. WAS scans an organization's websites, and identifies and reports infections, including zero-day threats via behavioral analysis. Detailed malware infection reports accompany infected code for remediation. A central dashboard displays scan activity, infected pages and malware infection trends, and lets users initiate actions directly from its interface. Malware detection functionality is provided via an optional add-on.

Compliance Monitoring

54. Qualys' Compliance Monitoring Solutions include Policy Compliance, Security Assessment Questionnaire, and PCI. Compliance Monitoring ensures that the organization must enforce internal policies, comply with external regulatory mandates, and assess the risk of doing business with vendors and other third parties. Compliance Monitoring uses a cloud-based solution to automate assessment of security and compliance controls in order to demonstrate a repeatable and trackable process to auditors and stakeholders.

DEFENDANT'S WILLFUL INFRINGEMENT OF FINJAN'S PATENTS

55. Defendant has infringed the '844, '494, '305, '408, '968, '731, and '154 Patents (collectively, the "Asserted Patents") and continues to infringe the '305, '408, '968, '731 and '154

Patents in this Judicial District and elsewhere in the United States by, among other things, making, using, importing, selling, and offering for sale the Accused Products.

56. In addition to directly infringing the Asserted Patents under 35 U.S.C. § 271(a), Defendant indirectly infringed the '844, '494, '305, '408, '968 and '731 Patents and continues to indirectly infringe the '305, '408, '968 and '731 Patents by instructing, directing, and requiring others, including its 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.

COUNT I
(Direct Infringement of the '844 Patent pursuant to 35 U.S.C. § 271(a))

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

58. Defendant infringed Claims 1-44 of the '844 Patent in violation of 35 U.S.C. § 271(a).

59. Defendant's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

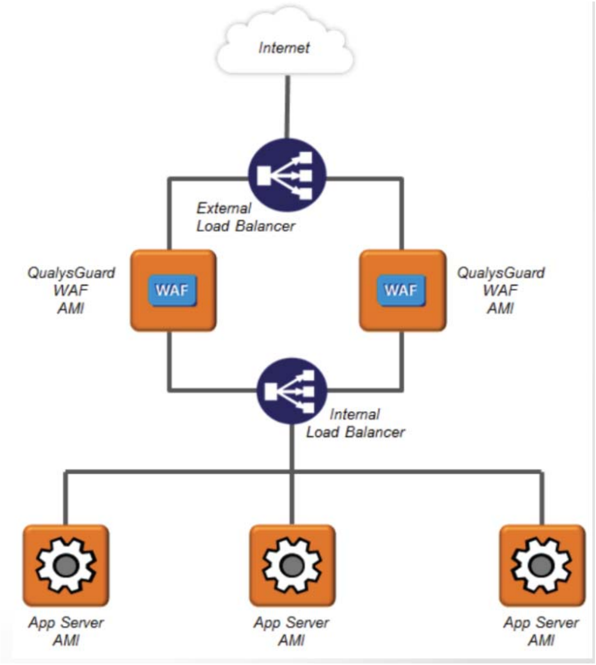
60. Defendant's acts of making, using, importing, selling, and offering for sale infringing products and services were without the permission, consent, authorization, or license of Finjan.

61. Defendant's infringement included the manufacture, use, sale, importation and offer for sale of Defendant's products and services that utilize Vulnerability Management, Threat Protection, Continuous Monitoring, Indicators of Compromise, Container Security, Web App Firewall, Web App Scanning, and Compliance Monitoring, including Qualys Cloud Platform products (collectively, "the '844 Accused Products").

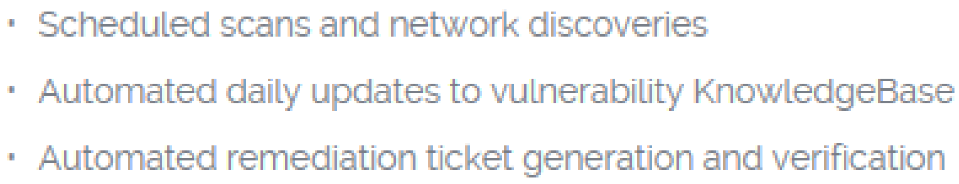
62. The '844 Accused Products practiced the patented invention of the '844 Patent and infringed the '844 Patent because they made or used the system and performed the steps of receiving a downloadable by an inspector, generating, by the inspector, a downloadable security profile that identifies suspicious code in the received downloadable, and linking, by the inspector, the downloadable security profile to the downloadable before a web server makes the downloadable available to web clients.

63. To the extent the ‘844 Accused Products used a system that includes modules, components or software owned by third parties, the ‘844 Accused Products still infringed the ‘844 Patent because Defendant is 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 Defendant’s customers performed a step or steps of the patented method or the ‘844 Accused Products incorporated third parties’ modules, components or software that performed one or more patented steps, Defendant’s ‘844 Accused Products still infringed the ‘844 Patent because the ‘844 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.

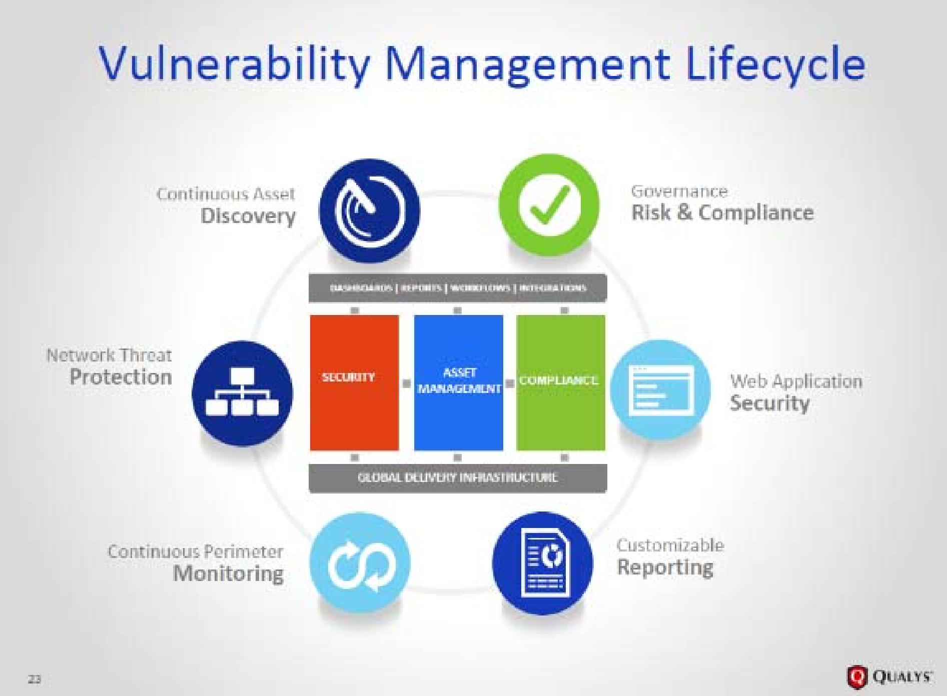
64. The ‘844 Accused Products include an inspector that receives Downloadables for scanning.



QualysGuard Web Application Security presentation at 30, attached hereto as Exhibit 8.



- Scheduled scans and network discoveries
- Automated daily updates to vulnerability KnowledgeBase
- Automated remediation ticket generation and verification



Vulnerability Management Lifecycle

Continuous Asset
Discovery

Governance
Risk & Compliance

DASHBOARDS | REPORTS | WORKFLOWS | INTEGRATIONS

Network Threat
Protection

SECURITY

ASSET
MANAGEMENT

COMPLIANCE

Web Application
Security

GLOBAL DELIVERY INFRASTRUCTURE

Continuous Perimeter
Monitoring

Customizable
Reporting

23

QUALYS

https://www.dts-solution.com/solutions/compliance-monitoring/vulnerability-management/, attached hereto as Exhibit 9.

65. Network mapping is an essential step in discovering vulnerabilities and consists of enumeration of all IP addresses in registered networks in an attempt to find live hosts. Network mapping is implemented using QualysGuard Vulnerability Management Scans – Maps:

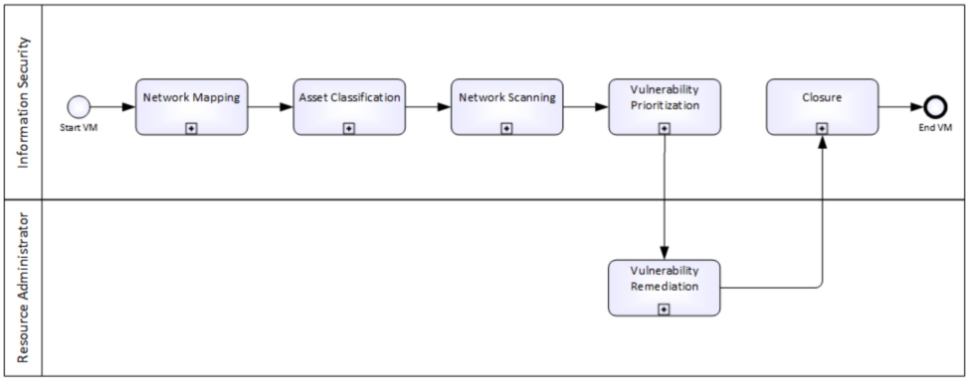
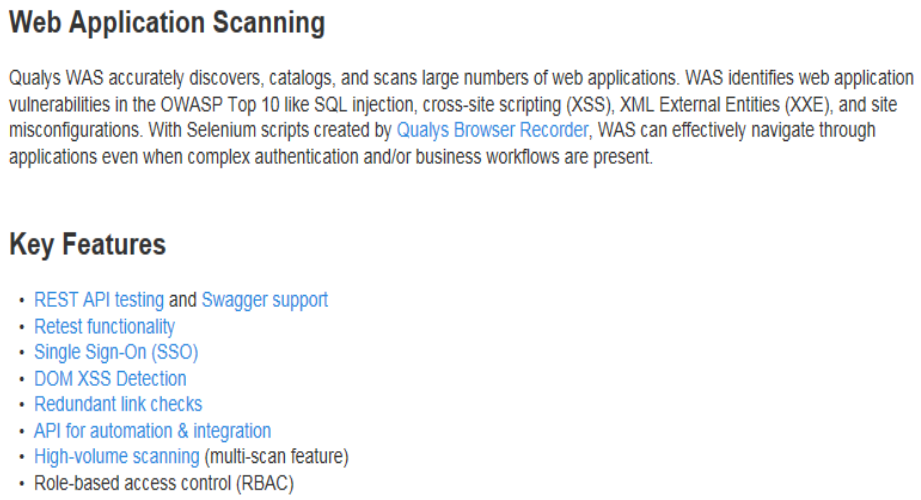


Figure 1: Vulnerability management process

https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.

66. The '844 Accused Products generate a first Downloadable security profile that identifies suspicious code in the received Downloadable (such as SQL injection, cross-site scripting (XSS), XML External Entities (XXE) and site misconfigurations):



Web Application Scanning

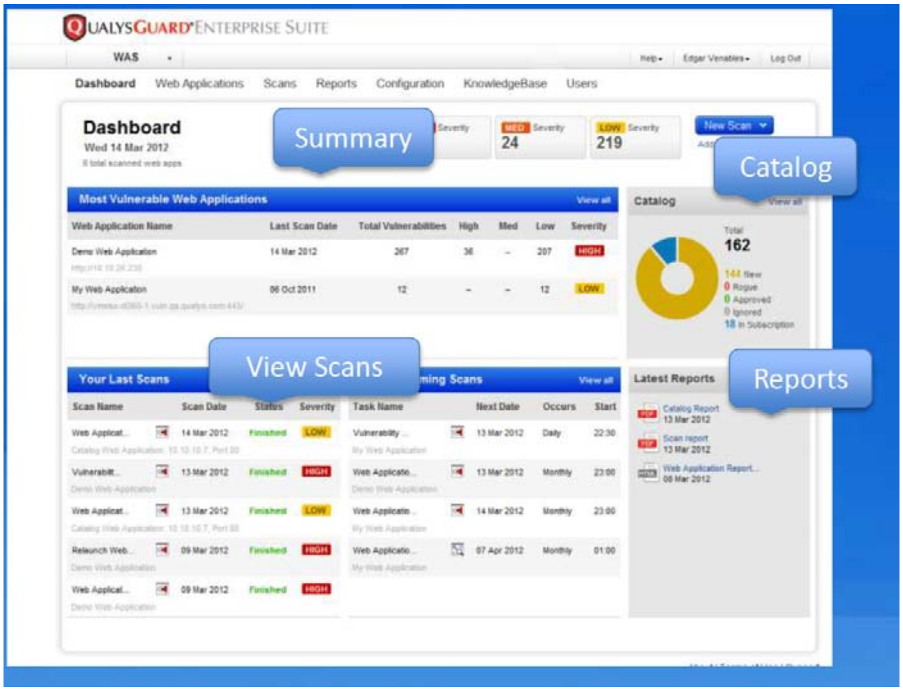
Qualys WAS accurately discovers, catalogs, and scans large numbers of web applications. WAS identifies web application vulnerabilities in the OWASP Top 10 like SQL injection, cross-site scripting (XSS), XML External Entities (XXE), and site misconfigurations. With Selenium scripts created by Qualys Browser Recorder, WAS can effectively navigate through applications even when complex authentication and/or business workflows are present.

Key Features

- REST API testing and Swagger support
- Retest functionality
- Single Sign-On (SSO)
- DOM XSS Detection
- Redundant link checks
- API for automation & integration
- High-volume scanning (multi-scan feature)
- Role-based access control (RBAC)

https://community.qualys.com/community/web-application-scanning, attached hereto as Exhibit 11.

67. The '844 Accused Products catalog new threats and suspicious code in Downloadables:



Dashboard
Wed 14 Mar 2012
8 total scanned web apps

Severity | MED Severity 24 | LOW Severity 219

Most Vulnerable Web Applications

Web Application Name	Last Scan Date	Total Vulnerabilities	High	Med	Low	Severity
Demo Web Application	14 Mar 2012	267	36	-	207	HIGH
My Web Application	06 Oct 2011	12	-	-	12	LOW

Catalog

Total 162
144 New
0 Rogue
0 Approved
0 Ignored
18 In Subscription

Your Last Scans

Scan Name	Scan Date	Status	Severity
Web Applicat...	14 Mar 2012	Finished	LOW
Vulnerabil...	13 Mar 2012	Finished	HIGH
Web Applicat...	13 Mar 2012	Finished	LOW
Relaunch Web...	09 Mar 2012	Finished	HIGH
Web Applicat...	09 Mar 2012	Finished	HIGH

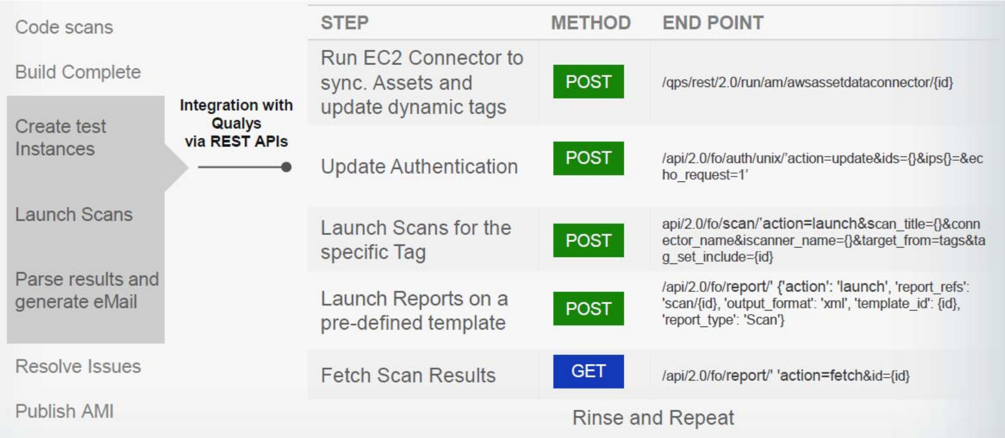
...ming Scans

Task Name	Next Date	Occurs	Start
Vulnerability ...	13 Mar 2012	Daily	22:30
Web Applicatio...	13 Mar 2012	Monthly	23:00
Web Applicatio...	14 Mar 2012	Monthly	23:00
Web Applicatio...	07 Apr 2012	Monthly	01:00

Latest Reports

Catalog Report 13 Mar 2012
Scan report 13 Mar 2012
Web Application Report... 08 Mar 2012

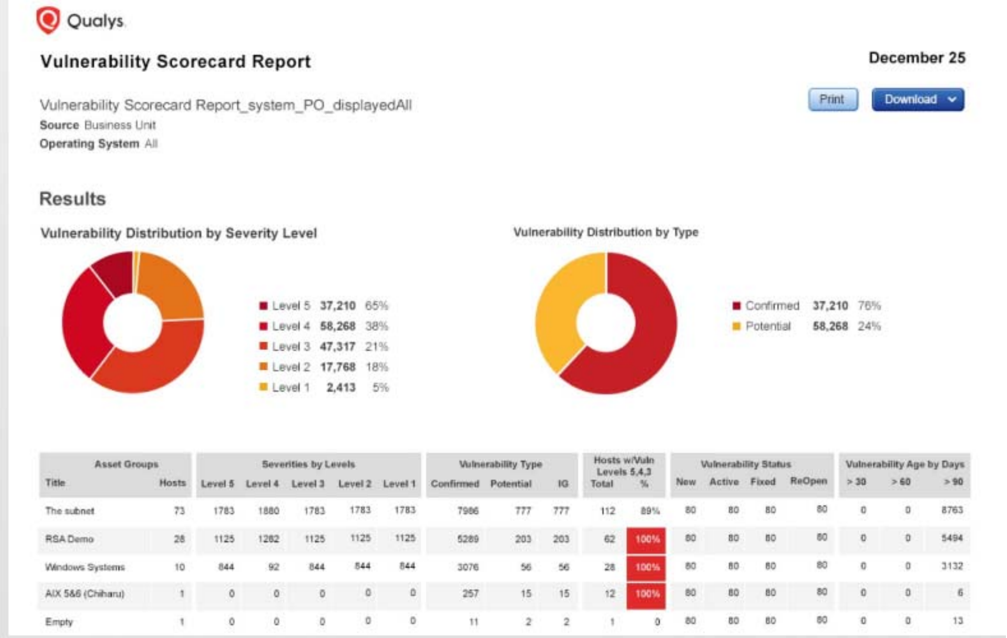
QualysGuard InfoDay 2014 presentation at 29, attached hereto as Exhibit 12.



STEP	METHOD	END POINT
Run EC2 Connector to sync. Assets and update dynamic tags	POST	/qps/rest/2.0/run/am/awsassetdataconnector/{id}
Update Authentication	POST	/api/2.0/fo/auth/unix/'action=update&ids={}&ips{}=&echo_request=1'
Launch Scans for the specific Tag	POST	api/2.0/fo/scan/'action=launch&scan_title={}&connector_name&iscanner_name={}&target_from=tags&tag_set_include={id}
Launch Reports on a pre-defined template	POST	/api/2.0/fo/report/' {'action': 'launch', 'report_refs': 'scan/{id}, 'output_format': 'xml', 'template_id': {id}, 'report_type': 'Scan'}
Fetch Scan Results	GET	/api/2.0/fo/report/' 'action=fetch&id={id}

Rinse and Repeat

Securing Public Cloud Infrastructure using Qualys presentation at 31, attached hereto as Exhibit 13.



Vulnerability Scorecard Report

December 25

Vulnerability Scorecard Report_system_PO_displayedAll
Source Business Unit
Operating System All

Results

Asset Groups		Severities by Levels					Vulnerability Type			Hosts w/Vuln Levels 5,4,3		Vulnerability Status				Vulnerability Age by Days		
Title	Hosts	Level 5	Level 4	Level 3	Level 2	Level 1	Confirmed	Potential	IG	Total	%	New	Active	Fixed	ReOpen	> 30	> 60	> 90
The subnet	73	1783	1880	1783	1783	1783	7986	777	777	112	89%	80	80	80	80	0	0	8763
RSA Demo	28	1125	1282	1125	1125	1125	5289	203	203	62	100%	80	80	80	80	0	0	5494
Windows Systems	10	844	92	844	844	844	3076	56	56	28	100%	80	80	80	80	0	0	3132
AIX 5&6 (Chiharu)	1	0	0	0	0	0	257	15	15	12	100%	80	80	80	80	0	0	6
Empty	1	0	0	0	0	0	11	2	2	1	0	80	80	80	80	0	0	13

https://www.qualys.com/apps/vulnerability-management/, attached hereto as Exhibit 14.

68. The '844 Accused Products link the Downloadable security profile to the Downloadable for vulnerability protection and remediation before the web server makes the Downloadable available to web clients.

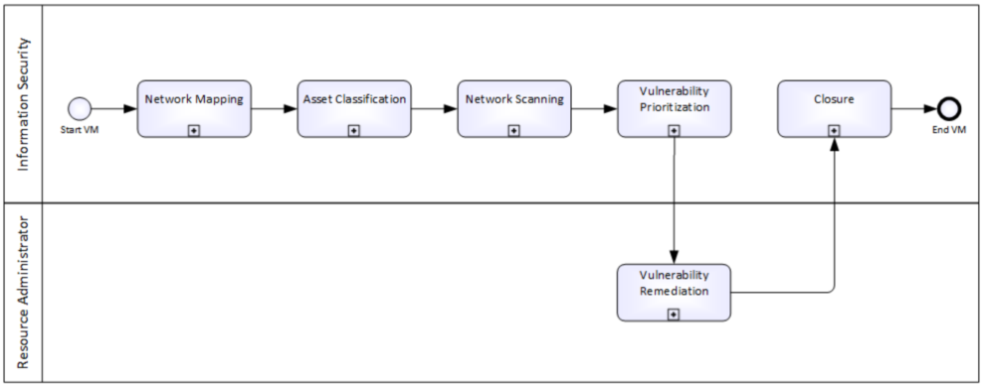
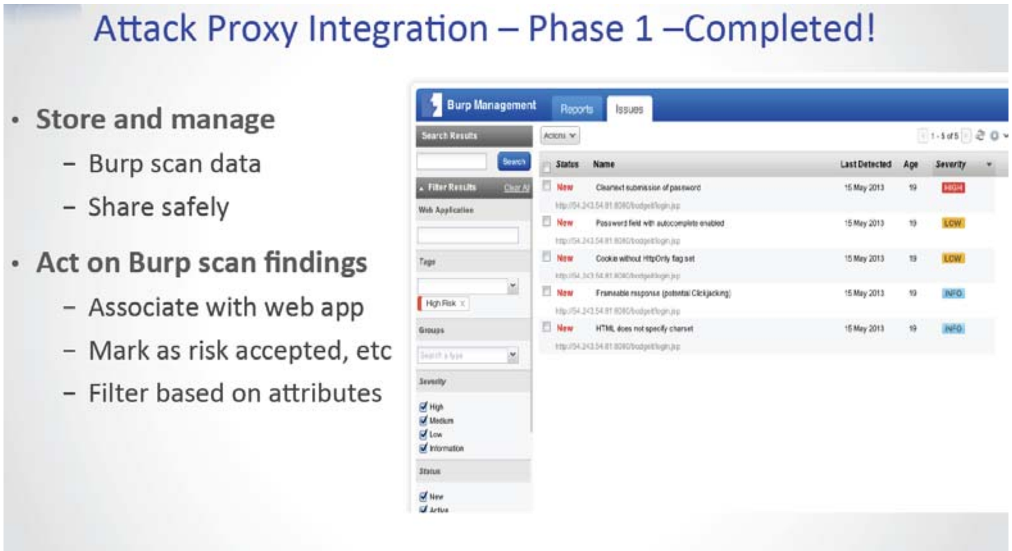


Figure 1: Vulnerability management process

https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.



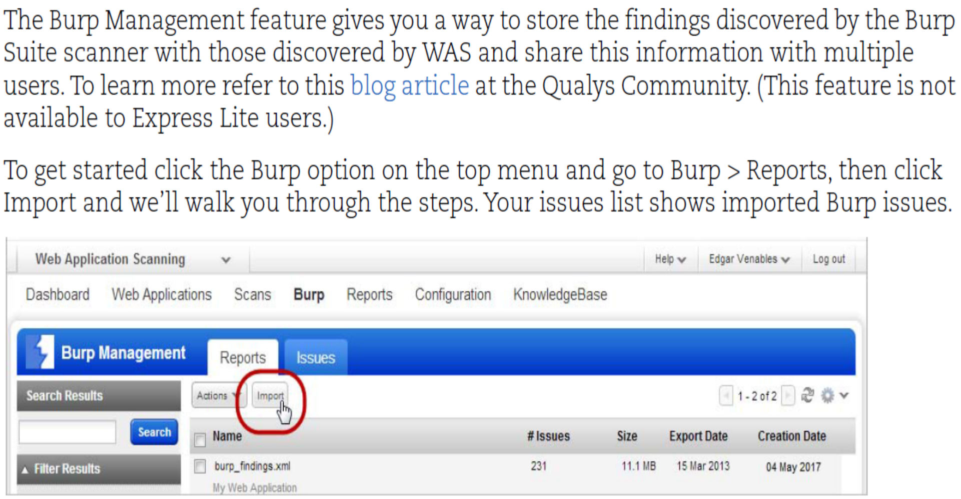
Attack Proxy Integration – Phase 1 –Completed!

- Store and manage
  - Burp scan data
  - Share safely
- Act on Burp scan findings
  - Associate with web app
  - Mark as risk accepted, etc
  - Filter based on attributes

Status	Name	Last Detected	Age	Severity
New	Cleartext submission of password http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	HIGH
New	Password field with autocomplete enabled http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	LOW
New	Cookie without HttpOnly flag set http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	LOW
New	Frameable response (potential Clickjacking) http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	INFO
New	HTML does not specify charset http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	INFO

QualysGuard Web Application Security presentation at 8, attached hereto as Exhibit 8.

69. The ‘844 Accused Products link Downloadable security profiles to Downloadables so that a user may have the findings for a particular downloadable stored for future reference so that when the downloadable is received again, a web server may block or allow it before it is made available to web clients:



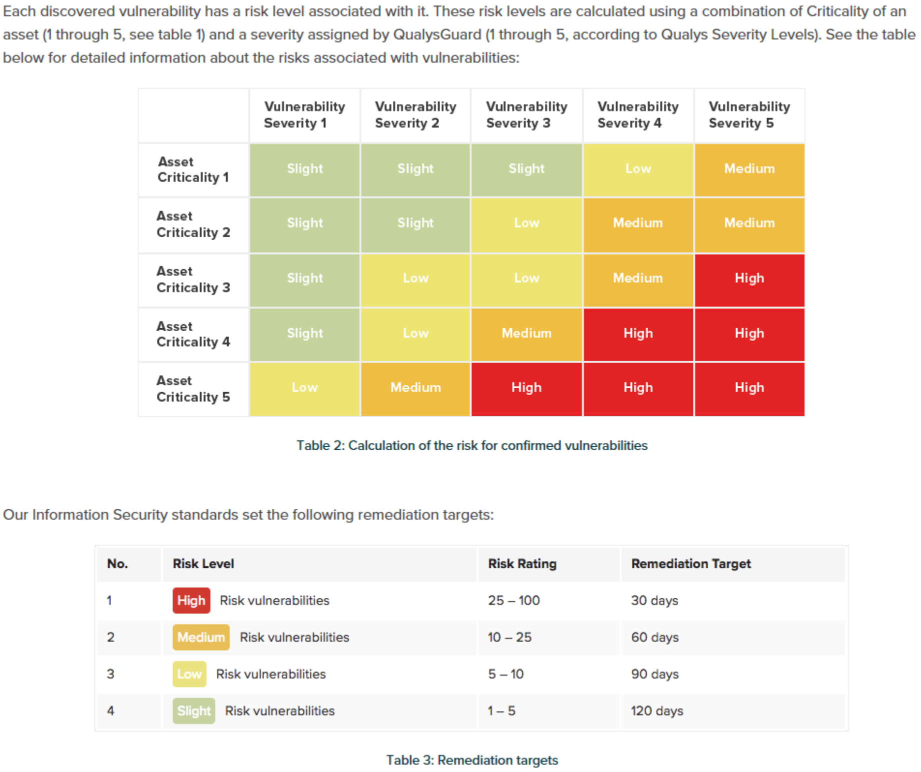
The Burp Management feature gives you a way to store the findings discovered by the Burp Suite scanner with those discovered by WAS and share this information with multiple users. To learn more refer to this blog article at the Qualys Community. (This feature is not available to Express Lite users.)

To get started click the Burp option on the top menu and go to Burp > Reports, then click Import and we'll walk you through the steps. Your issues list shows imported Burp issues.

	Name	# Issues	Size	Export Date	Creation Date
□	burp_findings.xml My Web Application	231	11.1 MB	15 Mar 2013	04 May 2017

Qualys Web Application Scanning Getting Started Guide Version 6.0.1 at 20, attached hereto as Exhibit 15.

70. The '844 Accused Products link Downloadable security profiles including "risk levels" with each discovered vulnerability in the Downloadables.



Each discovered vulnerability has a risk level associated with it. These risk levels are calculated using a combination of Criticality of an asset (1 through 5, see table 1) and a severity assigned by QualysGuard (1 through 5, according to Qualys Severity Levels). See the table below for detailed information about the risks associated with vulnerabilities:

	Vulnerability Severity 1	Vulnerability Severity 2	Vulnerability Severity 3	Vulnerability Severity 4	Vulnerability Severity 5
Asset Criticality 1	Slight	Slight	Slight	Low	Medium
Asset Criticality 2	Slight	Slight	Low	Medium	Medium
Asset Criticality 3	Slight	Low	Low	Medium	High
Asset Criticality 4	Slight	Low	Medium	High	High
Asset Criticality 5	Low	Medium	High	High	High

Table 2: Calculation of the risk for confirmed vulnerabilities

Our Information Security standards set the following remediation targets:

No.	Risk Level	Risk Rating	Remediation Target
1	High Risk vulnerabilities	25 – 100	30 days
2	Medium Risk vulnerabilities	10 – 25	60 days
3	Low Risk vulnerabilities	5 – 10	90 days
4	Slight Risk vulnerabilities	1 – 5	120 days

Table 3: Remediation targets

https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.

71. Defendant's infringement of the '844 Patent injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty.

72. Defendant has been long-aware of Finjan's patents, including the '844 Patent, and continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendant for nearly three years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that its products infringe Finjan's patents, including the '844 Patent, on information and belief Defendant made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendant's blatant and egregious disregard for Finjan's patent rights.

73. Despite its knowledge of Finjan's patent portfolio and Asserted Patents, and its specific knowledge of its own infringement, Defendant continued to sell the '844 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 '844 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 '844 Patent pursuant to 35 U.S.C. § 271(b))

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

75. In addition to directly infringing the '844 Patent, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 1-14 and 22-31 of the '844 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its customers to perform the steps of the method claims of the '844 Patent, either literally or under the doctrine of equivalents.

76. Defendant knowingly and actively aided and abetted the direct infringement of the '844 Patent by instructing and encouraging its customers and developers to use the '844 Accused Products. Such instructions and encouragement included advising third parties to use the '844 Accused Products

in an infringing manner, providing a mechanism through which third parties may infringe the '844 Patent, by advertising and promoting the use of the '844 Accused Products in an infringing manner, and by distributing guidelines and instructions to third parties on how to use the '844 Accused Products in an infringing manner. *See, e.g.*, QualysGuard Web Application Security presentation, attached hereto as Exhibit 8; https://www.dts-solution.com/solutions/compliance-monitoring/vulnerability-management/, attached hereto as Exhibit 9; https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10; https://community.qualys.com/community/web-application-scanning, attached hereto as Exhibit 11; QualysGuard InfoDay 2014 presentation, attached hereto as Exhibit 12; Securing Public Cloud Infrastructure using Qualys presentation, attached hereto as Exhibit 13; https://www.qualys.com/apps/vulnerability-management/, attached hereto as Exhibit 14; Qualys Web Application Scanning Getting Started Guide Version 6.0.1, attached hereto as Exhibit 15.

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

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

78. Defendant infringed Claims 3-5 and 7-18 of the '494 Patent in violation of 35 U.S.C. § 271(a).

79. Defendant's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

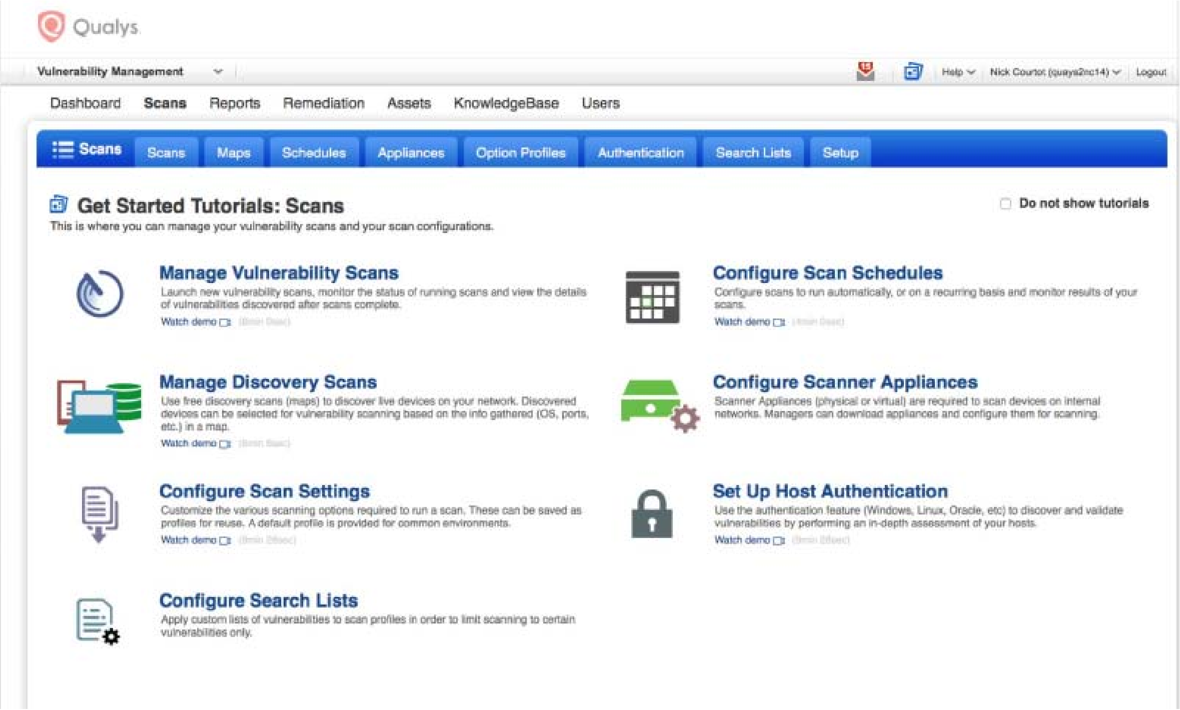
80. Defendant's acts of making, using, importing, selling, and offering for sale infringing products and services were without the permission, consent, authorization, or license of Finjan.

81. Defendant's infringement included the manufacture, use, sale, importation and offer for sale of Defendant's products and services that utilize Vulnerability Management, Threat Protection, Continuous Monitoring, Indicators of Compromise, Container Security, Web App Firewall, Web App Scanning, and Compliance Monitoring, including Qualys Cloud Platform products (collectively, "the '494 Accused Products").

82. The ‘494 Accused Products practiced 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.

83. 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 Defendant is 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 Defendant’s customers performed a step or steps of the patented method or the ‘494 Accused Products incorporated third parties’ modules, components or software that perform one or more patented steps, Defendant’s ‘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.

84. The ‘494 Accused Products are systems for managing Downloadables by performing vulnerability scans and creating vulnerability management reports using Virtual management (VM), Qualys Threat Protection, Web Application Filter (WAF) and Web Application Scanner (WAS):



Get Started Tutorials: Scans

This is where you can manage your vulnerability scans and your scan configurations.

□ Do not show tutorials

Manage Vulnerability Scans

Launch new vulnerability scans, monitor the status of running scans and view the details of vulnerabilities discovered after scans complete.

Watch demo

Configure Scan Schedules

Configure scans to run automatically, or on a recurring basis and monitor results of your scans.

Watch demo

Manage Discovery Scans

Use free discovery scans (maps) to discover live devices on your network. Discovered devices can be selected for vulnerability scanning based on the info gathered (OS, ports, etc.) in a map.

Watch demo

Configure Scanner Appliances

Scanner Appliances (physical or virtual) are required to scan devices on internal networks. Managers can download appliances and configure them for scanning.

Configure Scan Settings

Customize the various scanning options required to run a scan. These can be saved as profiles for reuse. A default profile is provided for common environments.

Watch demo

Set Up Host Authentication

Use the authentication feature (Windows, Linux, Oracle, etc) to discover and validate vulnerabilities by performing an in-depth assessment of your hosts.

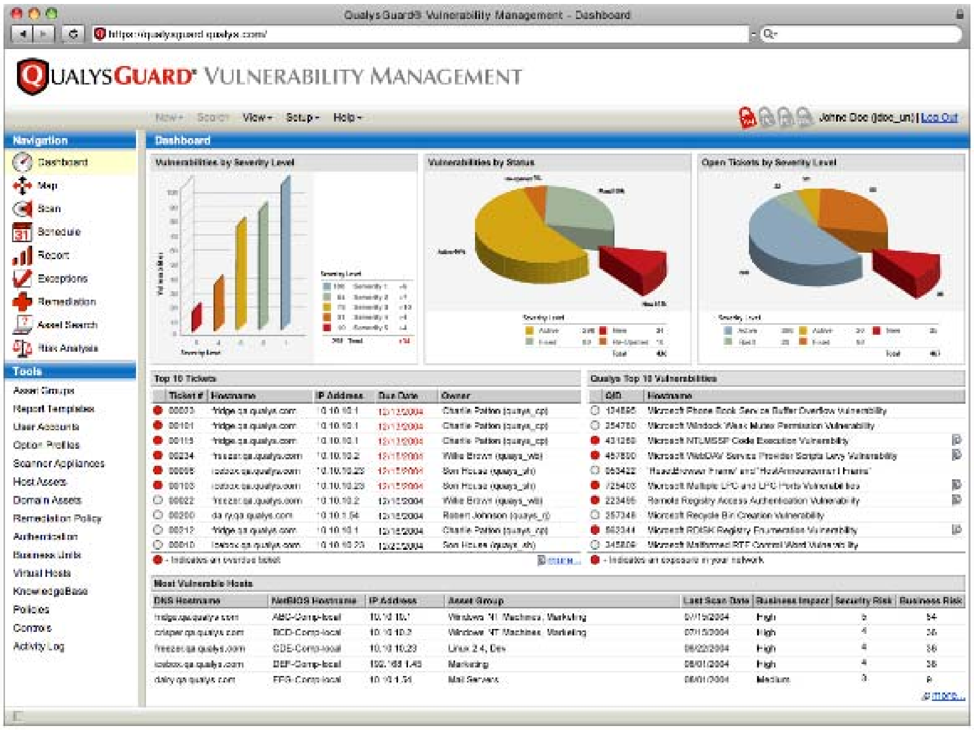
Watch demo

Configure Search Lists

Apply custom lists of vulnerabilities to scan profiles in order to limit scanning to certain vulnerabilities only.

> Qualys' ability to track vulnerability data across hosts and time lets you use reports interactively to better understand the security of your network. Use a library of built-in reports, change what's shown or choose different sets of assets — all without having to rescan. Reports can be generated on demand or scheduled automatically and then shared with the appropriate recipients online, in PDF or CSV.

https://www.qualys.com/apps/vulnerability-management/, attached hereto as Exhibit 14.



Top 10 Tickets

	Ticket #	Hostname	IP Address	Due Date	Owner
●	00003	fridge.qa.qualys.com	10.10.10.1	12/13/2004	Charlie Patton (qualys_cp)
●	00101	fridge.qa.qualys.com	10.10.10.1	12/13/2004	Charlie Patton (qualys_cp)
●	00115	fridge.qa.qualys.com	10.10.10.1	12/13/2004	Charlie Patton (qualys_cp)
●	00234	freezer.qa.qualys.com	10.10.10.2	12/15/2004	Willie Brown (qualys_wb)
●	00095	icebox.qa.qualys.com	10.10.10.23	12/15/2004	Son House (qualys_sh)
●	00103	icebox.qa.qualys.com	10.10.10.23	12/15/2004	Son House (qualys_sh)
○	00022	freezer.qa.qualys.com	10.10.10.2	12/15/2004	Willie Brown (qualys_wb)
○	00200	dairy.qa.qualys.com	10.10.1.54	12/15/2004	Robert Johnson (qualys_rj)
○	00212	fridge.qa.qualys.com	10.10.10.1	12/15/2004	Charlie Patton (qualys_cp)
○	00010	icebox.qa.qualys.com	10.10.10.23	12/22/2004	Son House (qualys_sh)

● - Indicates an overdue ticket

more...

Qualys Top 10 Vulnerabilities

	QID	Hostname
○	104886	Microsoft Phone Book Service Buffer Overflow Vulnerability
○	254780	Microsoft Windock Weak Mutex Permission Vulnerability
●	431260	Microsoft NTLMSSP Code Execution Vulnerability
●	457800	Microsoft WebDAV Service Provider Scripts Lazy Vulnerability
○	053422	"ReadBrowser Frame" and "HostAnnouncement Frame"
●	725403	Microsoft Multiple LPC and LPC Ports Vulnerabilities
●	223456	Remote Registry Access Authentication Vulnerability
○	257348	Microsoft Recycle Bin Creation Vulnerability
●	562344	Microsoft RDISK Registry Enumeration Vulnerability
○	345806	Microsoft Malformed RTF Control Word Vulnerability

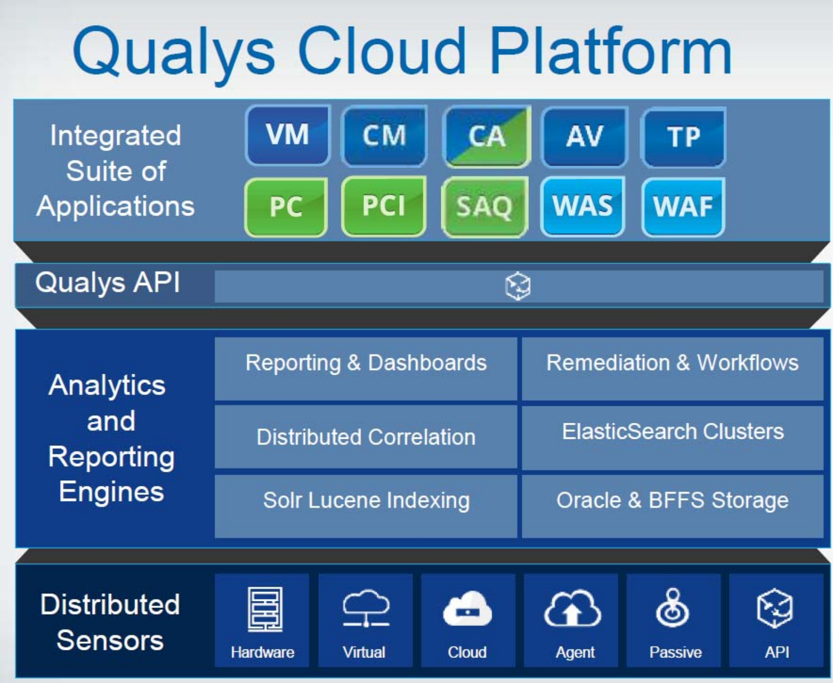
● - Indicates an exposure in your network

Most Vulnerable Hosts

DNS Hostname	NetBIOS Hostname	IP Address	Asset Group	Last Scan Date	Business Impact	Security Risk	Business Risk
fridge.qa.qualys.com	ABC-Comp-local	10.10.10.1	Windows NT Machines, Marketing	07/15/2004	High	5	54
crisper.qa.qualys.com	BCD-Comp-local	10.10.10.2	Windows NT Machines, Marketing	07/15/2004	High	4	36
freezer.qa.qualys.com	CDE-Comp-local	10.10.10.23	Linux 2.4, Dev	06/22/2004	High	4	36
icebox.qa.qualys.com	DEF-Comp-local	192.168.1.45	Marketing	08/01/2004	High	4	36
dairy.qa.qualys.com	EFG-Comp-local	10.10.1.54	Mail Servers	08/01/2004	Medium	3	9

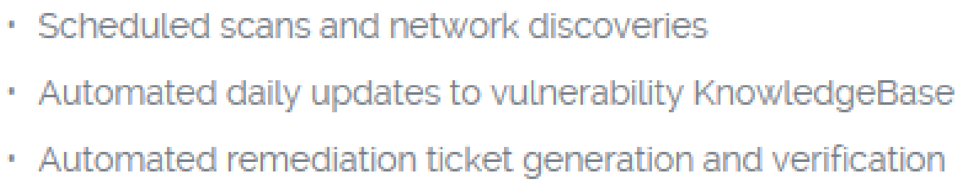
more...

https://www.dts-solution.com/solutions/compliance-monitoring/vulnerability-management/, attached hereto as Exhibit 9.

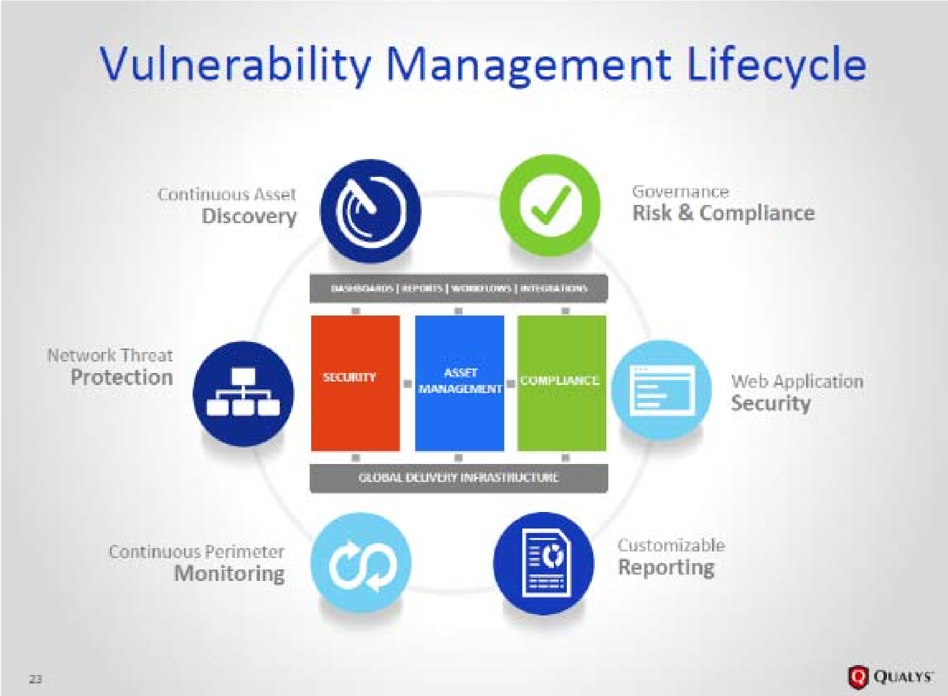


Securing Public Cloud Infrastructure using Qualys presentation at 12, attached hereto as Exhibit 13.

85. The '494 Accused Products include a receiver for receiving an incoming Downloadable for continuous asset discovery:



- Scheduled scans and network discoveries
- Automated daily updates to vulnerability KnowledgeBase
- Automated remediation ticket generation and verification



Vulnerability Management Lifecycle

Continuous Asset Discovery
Governance Risk & Compliance
DASHBOARDS | REPORTS | WORKFLOWS | INTEGRATIONS
Network Threat Protection
SECURITY
ASSET MANAGEMENT
COMPLIANCE
Web Application Security
GLOBAL DELIVERY INFRASTRUCTURE
Continuous Perimeter Monitoring
Customizable Reporting
23
QUALYS

https://www.dts-solution.com/solutions/compliance-monitoring/vulnerability-management/, attached hereto as Exhibit 9.

86. Network mapping is an essential step in discovering vulnerabilities and consists of enumeration of all IP addresses in registered networks in an attempt to find live hosts. Network mapping is implemented using QualysGuard Vulnerability Management Scans – Maps which receive incoming Downloadables.

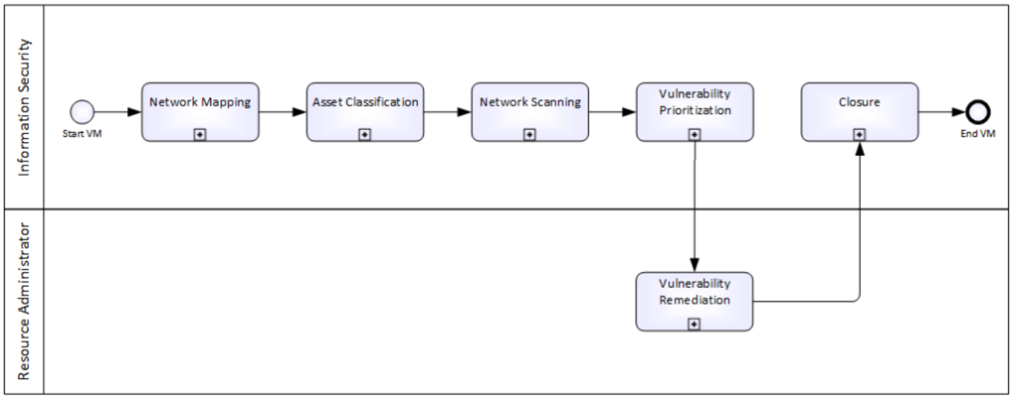


Figure 1: Vulnerability management process

https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.

87. The '494 Accused Products include a Downloadable scanner coupled with the receiver, for deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable.

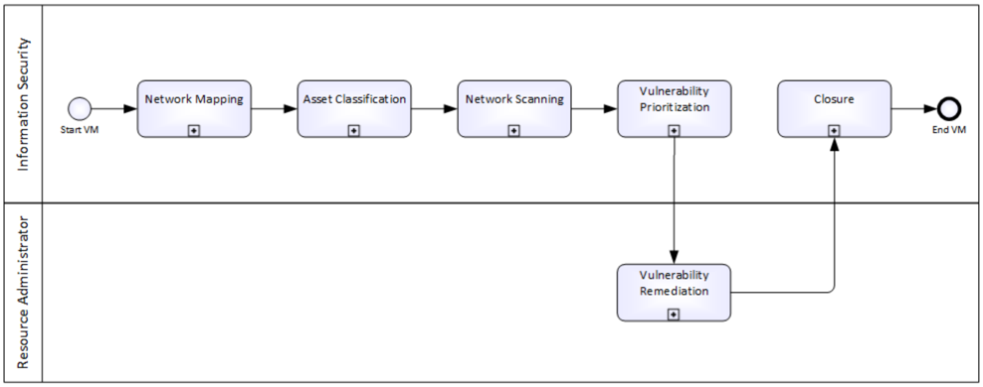
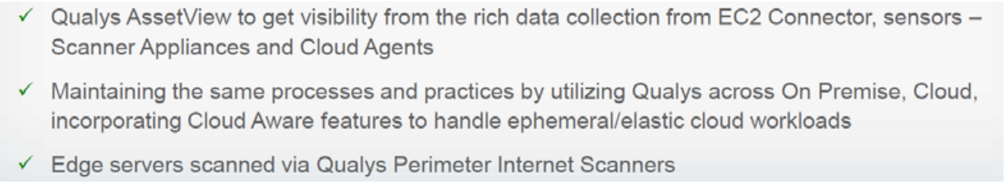
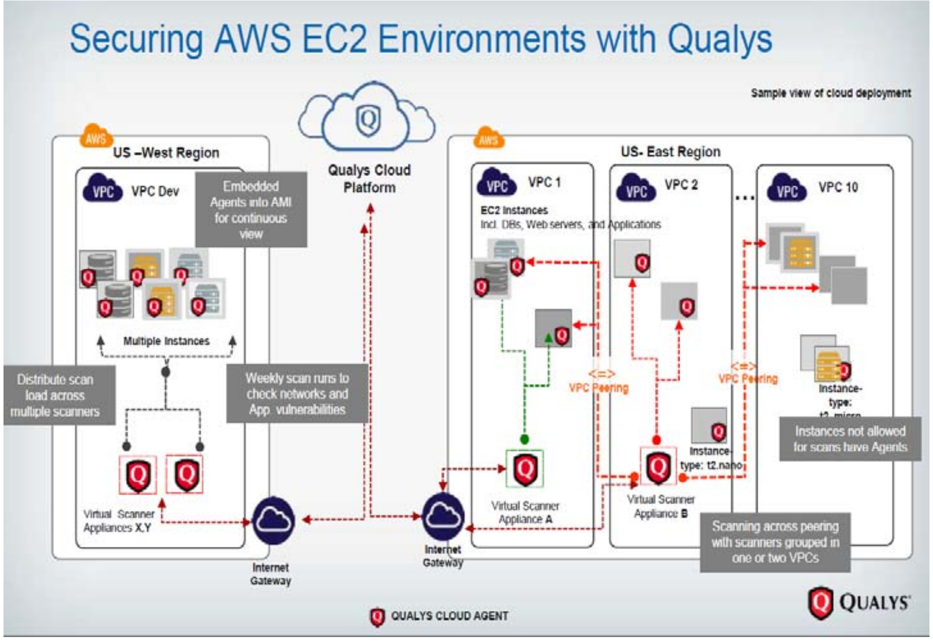


Figure 1: Vulnerability management process

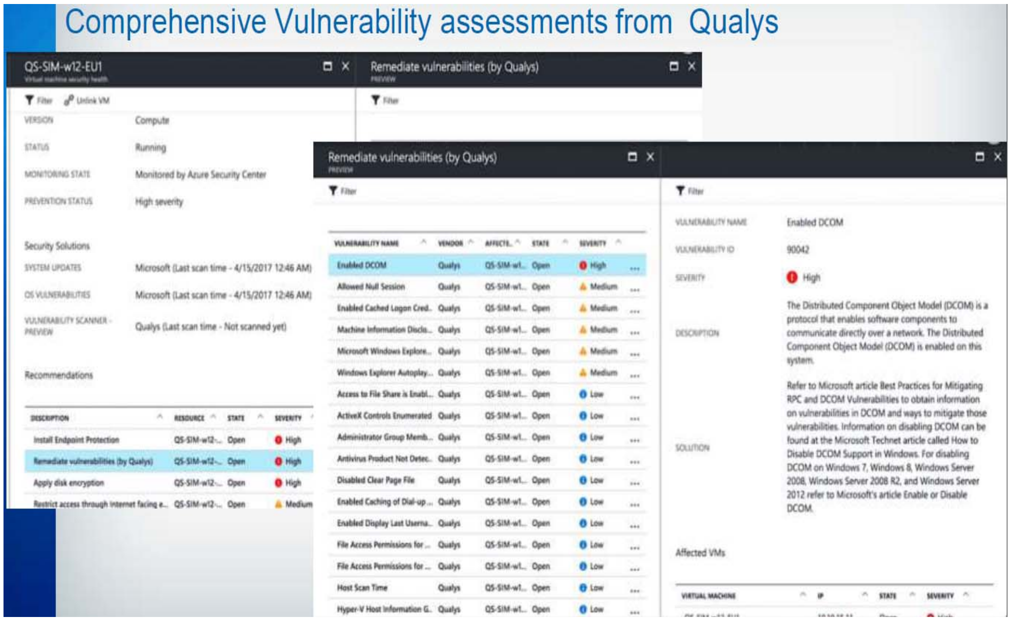
https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.



- ✓ Qualys AssetView to get visibility from the rich data collection from EC2 Connector, sensors – Scanner Appliances and Cloud Agents
- ✓ Maintaining the same processes and practices by utilizing Qualys across On Premise, Cloud, incorporating Cloud Aware features to handle ephemeral/elastic cloud workloads
- ✓ Edge servers scanned via Qualys Perimeter Internet Scanners


Securing AWS EC2 Environments with Qualys
Sample view of cloud deployment
Qualys Cloud Platform
AWS
US –West Region
VPC
VPC Dev
Embedded Agents into AMI for continuous view
Multiple Instances
Distribute scan load across multiple scanners
Weekly scan runs to check networks and App vulnerabilities
Virtual Scanner Appliances X,Y
Internet Gateway
AWS
US- East Region
VPC
VPC 1
EC2 Instances
Incl. DBs, Web servers, and Applications
VPC
VPC 2
VPC
VPC 10
<=> VPC Peering
<=> VPC Peering
Virtual Scanner Appliance A
Virtual Scanner Appliance B
Instance-type: t2.nano
Instance-type: t2.micro
Instances not allowed for scans have Agents
Scanning across peering with scanners grouped in one or two VPCs
Internet Gateway
QUALYS CLOUD AGENT
QUALYS

Securing Public Cloud Infrastructure using Qualys presentation at 29, attached hereto as Exhibit 13.


Comprehensive Vulnerability assessments from Qualys

QS-SIM-w12-EU1
Virtual machine security health

VERSION Compute
STATUS Running
MONITORING STATE Monitored by Azure Security Center
PREVENTION STATUS High severity

Security Solutions
SYSTEM UPDATES Microsoft (Last scan time - 4/15/2017 12:46 AM)
OS VULNERABILITIES Microsoft (Last scan time - 4/15/2017 12:46 AM)
VULNERABILITY SCANNER - PREVIEW Qualys (Last scan time - Not scanned yet)

Recommendations

DESCRIPTION	RESOURCE	STATE	SEVERITY
Install Endpoint Protection	QS-SIM-w12-...	Open	High
Remediate vulnerabilities (by Qualys)	QS-SIM-w12-...	Open	High
Apply disk encryption	QS-SIM-w12-...	Open	High
Restrict access through internet facing e...	QS-SIM-w12-...	Open	Medium

Remediate vulnerabilities (by Qualys)
PREVIEW

Remediate vulnerabilities (by Qualys)
PREVIEW

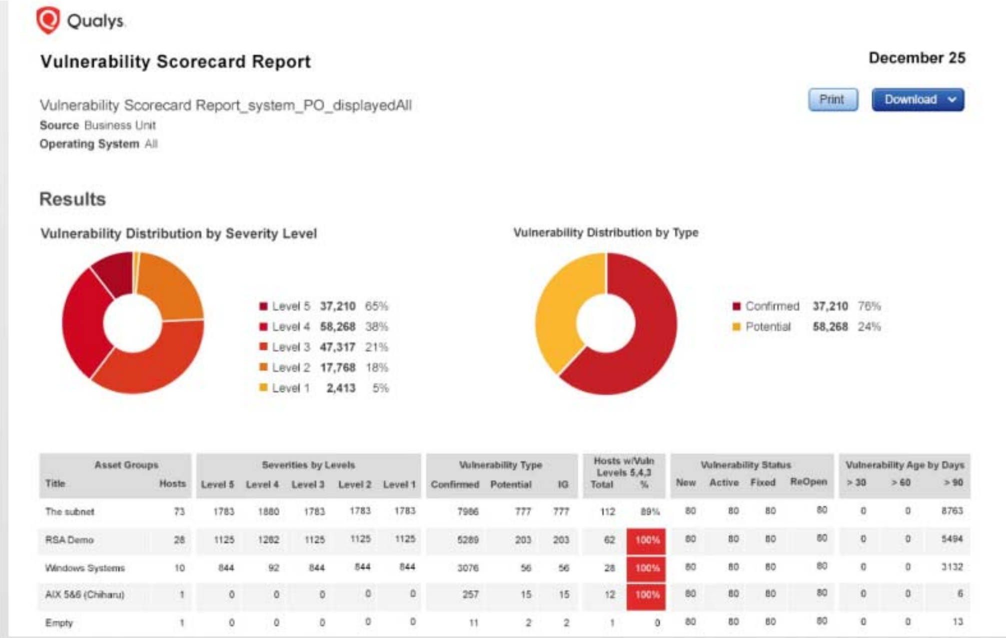
VULNERABILITY NAME	VENDOR	AFFECTE...	STATE	SEVERITY	
Enabled DCOM	Qualys	QS-SIM-wl...	Open	High	...
Allowed Null Session	Qualys	QS-SIM-wl...	Open	Medium	...
Enabled Cached Logon Cred...	Qualys	QS-SIM-wl...	Open	Medium	...
Machine Information Disclo...	Qualys	QS-SIM-wl...	Open	Medium	...
Microsoft Windows Explore...	Qualys	QS-SIM-wl...	Open	Medium	...
Windows Explorer Autoplay...	Qualys	QS-SIM-wl...	Open	Medium	...
Access to File Share is Enabl...	Qualys	QS-SIM-wl...	Open	Low	...
ActiveX Controls Enumerated	Qualys	QS-SIM-wl...	Open	Low	...
Administrator Group Memb...	Qualys	QS-SIM-wl...	Open	Low	...
Antivirus Product Not Detec...	Qualys	QS-SIM-wl...	Open	Low	...
Disabled Clear Page File	Qualys	QS-SIM-wl...	Open	Low	...
Enabled Caching of Dial-up ...	Qualys	QS-SIM-wl...	Open	Low	...
Enabled Display Last Userna...	Qualys	QS-SIM-wl...	Open	Low	...
File Access Permissions for ...	Qualys	QS-SIM-wl...	Open	Low	...
File Access Permissions for ...	Qualys	QS-SIM-wl...	Open	Low	...
Host Scan Time	Qualys	QS-SIM-wl...	Open	Low	...
Hyper-V Host Information G...	Qualys	QS-SIM-wl...	Open	Low	...

VULNERABILITY NAME Enabled DCOM
VULNERABILITY ID 90042
SEVERITY High
DESCRIPTION The Distributed Component Object Model (DCOM) is a protocol that enables software components to communicate directly over a network. The Distributed Component Object Model (DCOM) is enabled on this system.
SOLUTION Refer to Microsoft article Best Practices for Mitigating RPC and DCOM Vulnerabilities to obtain information on vulnerabilities in DCOM and ways to mitigate those vulnerabilities. Information on disabling DCOM can be found at the Microsoft Technet article called How to Disable DCOM Support in Windows. For disabling DCOM on Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 refer to Microsoft's article Enable or Disable DCOM.

Affected VMs

VIRTUAL MACHINE	IP	STATE	SEVERITY

Securing Public Cloud Infrastructure using Qualys presentation at 37, attached hereto as Exhibit 13.



Qualys

Vulnerability Scorecard Report

December 25

Vulnerability Scorecard Report_system_PO_displayedAll

Source Business Unit

Operating System All

Results

Vulnerability Distribution by Severity Level

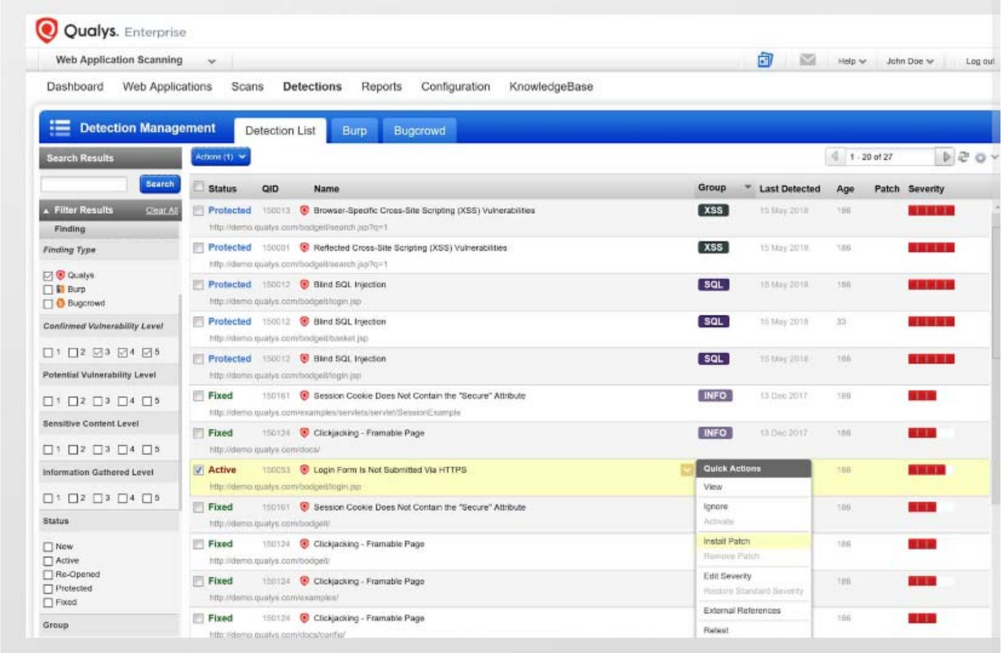
■ Level 5	37,210	65%
■ Level 4	58,268	38%
■ Level 3	47,317	21%
■ Level 2	17,768	18%
■ Level 1	2,413	5%

Vulnerability Distribution by Type

■ Confirmed	37,210	76%
■ Potential	58,268	24%

Asset Groups		Severities by Levels					Vulnerability Type			Hosts w/Vuln Levels 5,4,3		Vulnerability Status				Vulnerability Age by Days		
Title	Hosts	Level 5	Level 4	Level 3	Level 2	Level 1	Confirmed	Potential	IG	Total	%	New	Active	Fixed	ReOpen	> 30	> 60	> 90
The subnet	73	1783	1880	1783	1783	1783	7986	777	777	112	89%	80	80	80	80	0	0	8763
RSA Demo	28	1125	1282	1125	1125	1125	5289	203	203	62	100%	80	80	80	80	0	0	5494
Windows Systems	10	844	92	844	844	844	3076	56	56	28	100%	80	80	80	80	0	0	3132
AIX 5&6 (Chiharu)	1	0	0	0	0	0	257	15	15	12	100%	80	80	80	80	0	0	6
Empty	1	0	0	0	0	0	11	2	2	1	0	80	80	80	80	0	0	13

https://www.qualys.com/apps/vulnerability-management/, attached hereto as Exhibit 14.



Qualys. Enterprise

Finding

Finding Type

☑ Qualys
□ Burp
□ Bugcrowd

Confirmed Vulnerability Level

□ 1 □ 2 ☑ 3 ☑ 4 ☑ 5

Potential Vulnerability Level

□ 1 □ 2 □ 3 □ 4 □ 5

Sensitive Content Level

□ 1 □ 2 □ 3 □ 4 □ 5

Information Gathered Level

□ 1 □ 2 □ 3 □ 4 □ 5

Status

□ New
□ Active
□ Re-Opened
□ Protected
□ Fixed

Group

Status	QID	Name	Group	Last Detected	Age	Patch	Severity
□ Protected	150013	Browser-Specific Cross-Site Scripting (XSS) Vulnerabilities http://demo.qualys.com/bodgeit/search.jsp?q=1	XSS	15 May 2018	186		■■■■■
□ Protected	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities http://demo.qualys.com/bodgeit/search.jsp?q=1	XSS	15 May 2018	186		■■■■■
□ Protected	150012	Blind SQL Injection http://demo.qualys.com/bodgeit/login.jsp	SQL	15 May 2018	186		■■■■■
□ Protected	150012	Blind SQL Injection http://demo.qualys.com/bodgeit/basket.jsp	SQL	15 May 2018	33		■■■■■
□ Protected	150012	Blind SQL Injection http://demo.qualys.com/bodgeit/login.jsp	SQL	15 May 2018	186		■■■■■
□ Fixed	150161	Session Cookie Does Not Contain the "Secure" Attribute http://demo.qualys.com/examples/servlets/servlet/SessionExample	INFO	13 Dec 2017	186		■■■
□ Fixed	150124	Clickjacking - Framable Page http://demo.qualys.com/docs/	INFO	13 Dec 2017	186		■■■
☑ Active	150053	Login Form Is Not Submitted Via HTTPS http://demo.qualys.com/bodgeit/login.jsp			186		■■■■
□ Fixed	150161	Session Cookie Does Not Contain the "Secure" Attribute http://demo.qualys.com/bodgeit/			186		■■■
□ Fixed	150124	Clickjacking - Framable Page http://demo.qualys.com/bodgeit/			186		■■■
□ Fixed	150124	Clickjacking - Framable Page http://demo.qualys.com/examples/			186		■■■
□ Fixed	150124	Clickjacking - Framable Page http://demo.qualys.com/docs/config/			186		■■■

https://www.qualys.com/apps/web-app-firewall/, attached hereto as Exhibit 16.

88. The '494 Accused Products include a database manager coupled with the Downloadable scanner, for storing the Downloadable security profile data in a database.

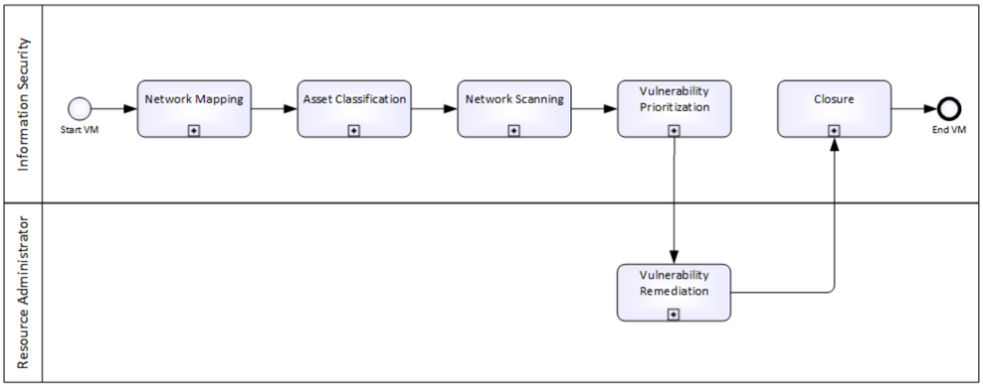
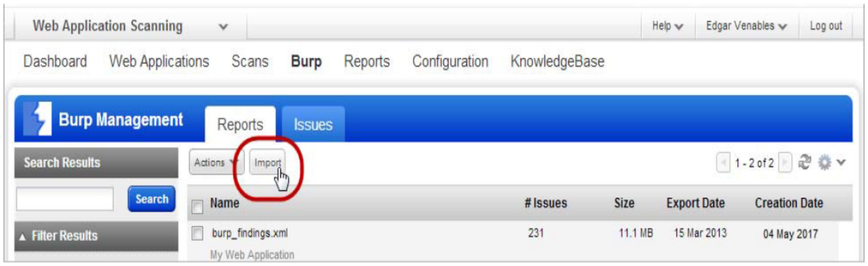


Figure 1: Vulnerability management process

https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.

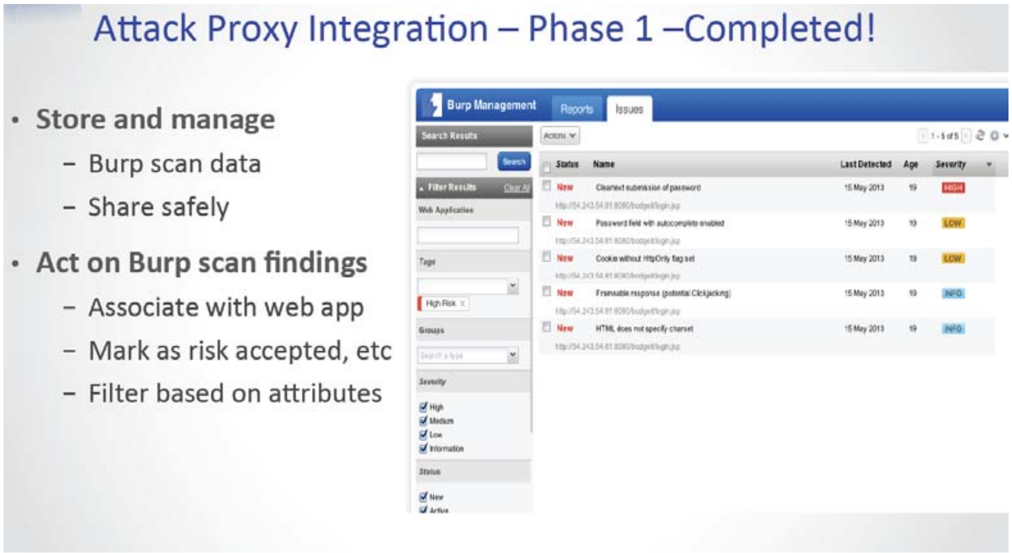
> The Burp Management feature gives you a way to store the findings discovered by the Burp Suite scanner with those discovered by WAS and share this information with multiple users. To learn more refer to this blog article at the Qualys Community. (This feature is not available to Express Lite users.)
>
> To get started click the Burp option on the top menu and go to Burp > Reports, then click Import and we'll walk you through the steps. Your issues list shows imported Burp issues.



Name	# Issues	Size	Export Date	Creation Date
burp_findings.xml My Web Application	231	11.1 MB	15 Mar 2013	04 May 2017

Qualys Web Application Scanning Getting Started Guide Version 6.0.1 at 20, attached hereto as Exhibit 15.

89. The '494 Accused Products store security profiles in a policy index (high/low risk) data including entries that relate cache content and policies:

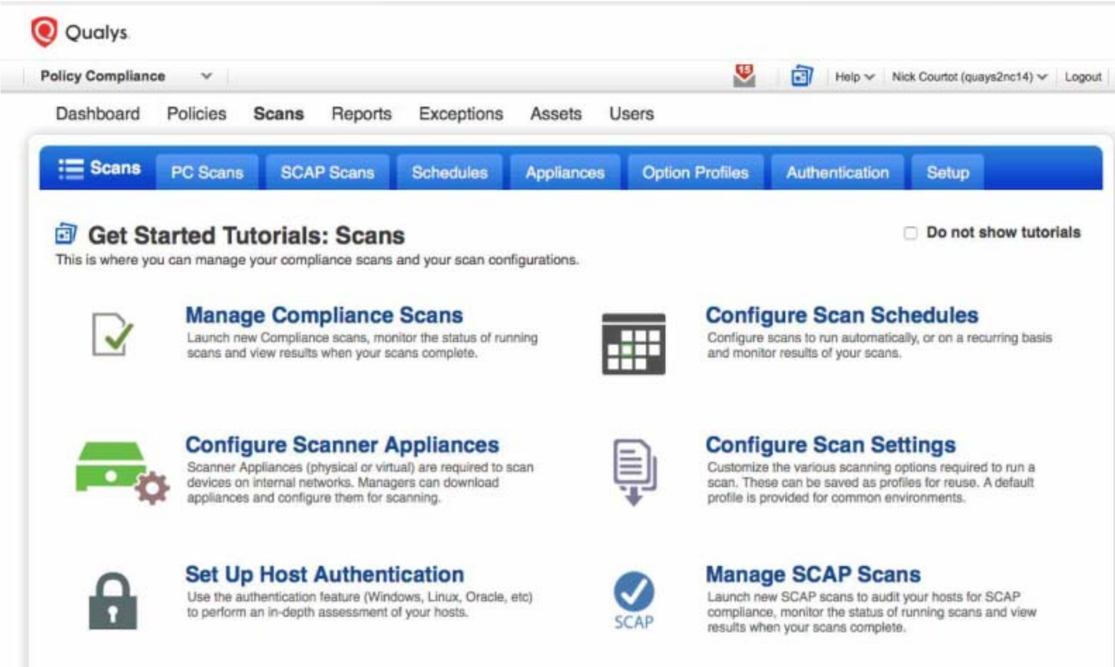


Attack Proxy Integration – Phase 1 –Completed!

- Store and manage
  - Burp scan data
  - Share safely
- Act on Burp scan findings
  - Associate with web app
  - Mark as risk accepted, etc
  - Filter based on attributes

	Status	Name	Last Detected	Age	Severity
□	New	Cleartext submission of password http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	HIGH
□	New	Password field with autocomplete enabled http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	LOW
□	New	Cookie without HttpOnly flag set http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	LOW
□	New	Framable response (potential Clickjacking) http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	INFO
□	New	HTML does not specify charset http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	INFO

QualysGuard Web Application Security presentation at 8, attached hereto as Exhibit 8.



Get Started Tutorials: Scans

This is where you can manage your compliance scans and your scan configurations.

Manage Compliance Scans
Launch new Compliance scans, monitor the status of running scans and view results when your scans complete.

Configure Scan Schedules
Configure scans to run automatically, or on a recurring basis and monitor results of your scans.

Configure Scanner Appliances
Scanner Appliances (physical or virtual) are required to scan devices on internal networks. Managers can download appliances and configure them for scanning.

Configure Scan Settings
Customize the various scanning options required to run a scan. These can be saved as profiles for reuse. A default profile is provided for common environments.

Set Up Host Authentication
Use the authentication feature (Windows, Linux, Oracle, etc) to perform an in-depth assessment of your hosts.

Manage SCAP Scans
Launch new SCAP scans to audit your hosts for SCAP compliance, monitor the status of running scans and view results when your scans complete.

https://www.qualys.com/apps/policy-compliance/, attached hereto as Exhibit 17.

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

91. Defendant has been long-aware of Finjan's patents, including the '494 Patent, and continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendant for nearly three

years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that its products infringe Finjan's patents, including the '494 Patent, on information and belief Defendant made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendant's blatant and egregious disregard for Finjan's patent rights.

92. Despite its knowledge of Finjan's patent portfolio and Asserted Patents, and its specific knowledge of its own infringement, Defendant continued to sell the '494 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 IV
(Indirect Infringement of the '494 Patent pursuant to 35 U.S.C. § 271(b))

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

94. In addition to directly infringing the '494 Patent, Defendant knew or was willfully blind to the fact that it was 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 its customers to perform the steps of the method claims of the '494 Patent, either literally or under the doctrine of equivalents.

95. Additionally, Defendant knew or was willfully blind to the fact that it was 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 its customers to perform the steps of the method claims of the '494 Patent, either literally or under the doctrine of equivalents.

96. Defendant knowingly and actively aided and abetted the direct infringement of the '494 Patent by instructing and encouraging its 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*., QualysGuard Web Application Security presentation, attached hereto as Exhibit 8; https://www.dts-solution.com/solutions/compliance-monitoring/vulnerability-management/, attached hereto as Exhibit 9.; https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10; Securing Public Cloud Infrastructure using Qualys presentation, attached hereto as Exhibit 13; https://www.qualys.com/apps/vulnerability-management/, attached hereto as Exhibit 14; https://www.qualys.com/apps/web-app-firewall/, attached hereto as Exhibit 16; https://www.qualys.com/apps/policy-compliance/, attached hereto as Exhibit 17.

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

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

98. Defendant has infringed and continues to infringe Claims 3-4, 6-12, and 14-25 of the ‘305 Patent in violation of 35 U.S.C. § 271(a).

99. Defendant’s infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

100. Defendant’s acts of making, using, importing, selling, and offering for sale infringing products and services has been without the permission, consent, authorization or license of Finjan.

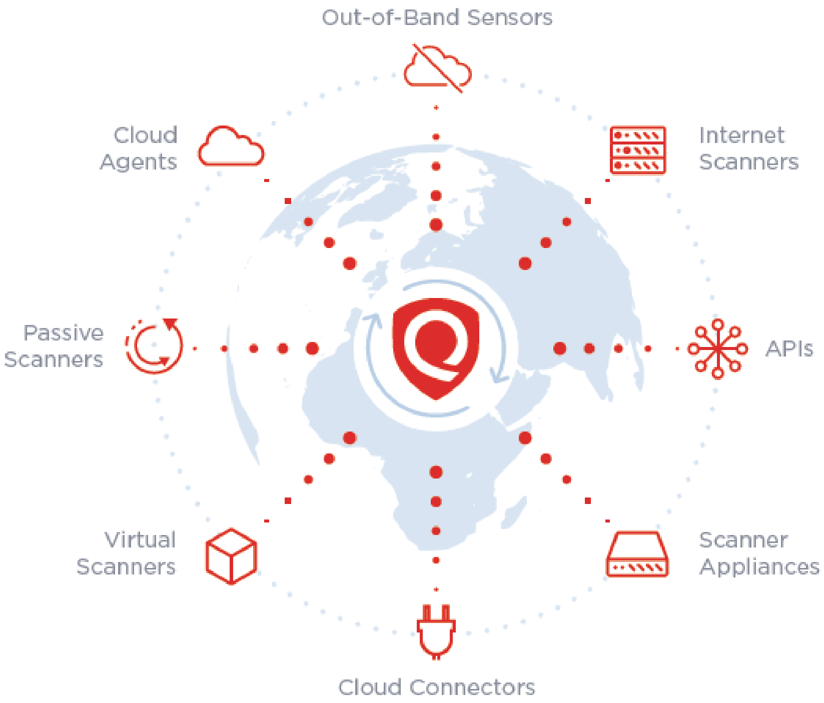
101. Defendant’s infringement includes the manufacture, use, sale, importation and offer for sale of Defendant’s products and services that utilize Vulnerability Management, Threat Protection, Continuous Monitoring, Indicators of Compromise, Container Security, Web App Firewall, Web App Scanning, and Compliance Monitoring, including Qualys Cloud Platform products (collectively, “the ‘305 Accused Products”).

102. 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

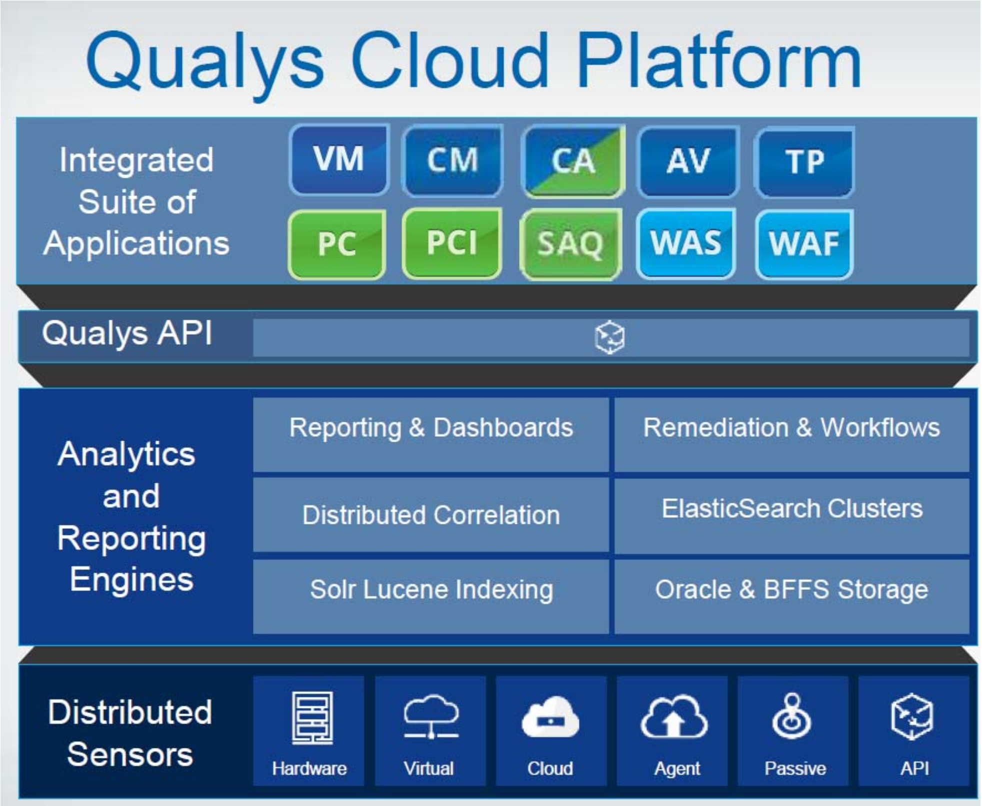
of rule-based scanning of web-based content for exploits by, for example, using parser and analyzer rules to describe computer exploits as patterns of types of tokens.

103. To the extent the ‘305 Accused Products use a system that includes modules, components or software owned by third parties, the ‘305 Accused Products still infringe the ‘305 Patent because Defendant is 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 Defendant’s customers perform a step or steps of the patented method or the ‘305 Accused Products incorporate third parties’ modules, components or software that perform one or more patented steps, Defendant’s ‘305 Accused Products still infringe 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.

104. The ‘305 Accused Products are security systems for scanning content within a computer including Web Application Filter (WAF) and Web Application Scanner (WAS):



Qualys Cloud Platform datasheet at 2, attached hereto as Exhibit 22.



Qualys Cloud Platform

Integrated Suite of Applications

VM CM CA AV TP

PC PCI SAQ WAS WAF

Qualys API

Analytics and Reporting Engines

Reporting & Dashboards

Remediation & Workflows

Distributed Correlation

ElasticSearch Clusters

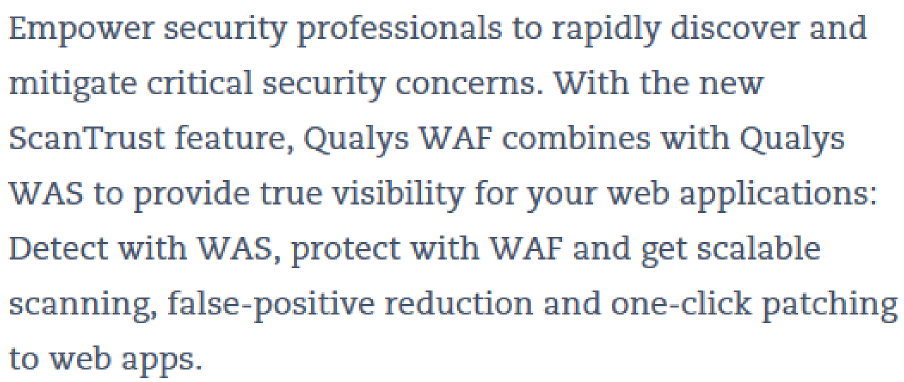
Solr Lucene Indexing

Oracle & BFFS Storage

Distributed Sensors

Hardware Virtual Cloud Agent Passive API

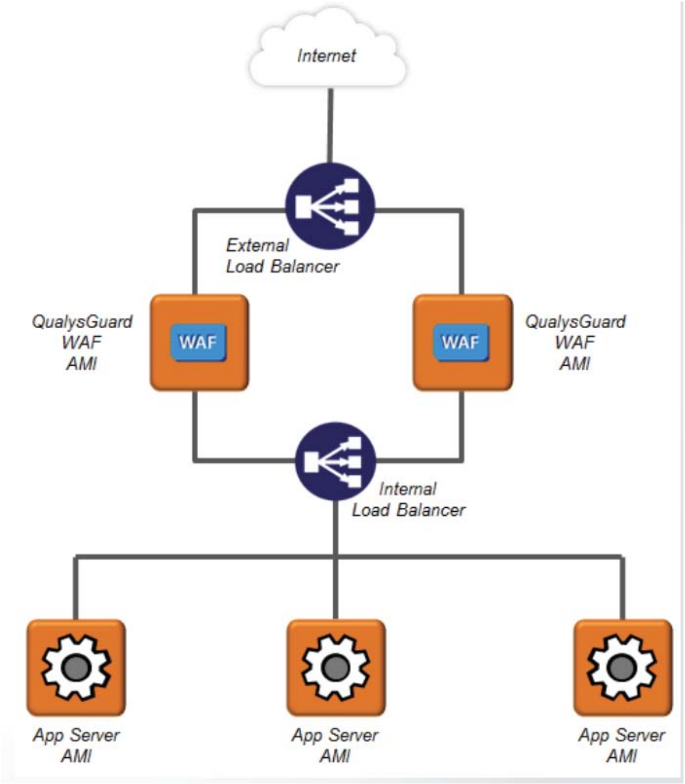
Securing Public Cloud Infrastructure using Qualys presentation at 12, attached hereto as Exhibit 13.



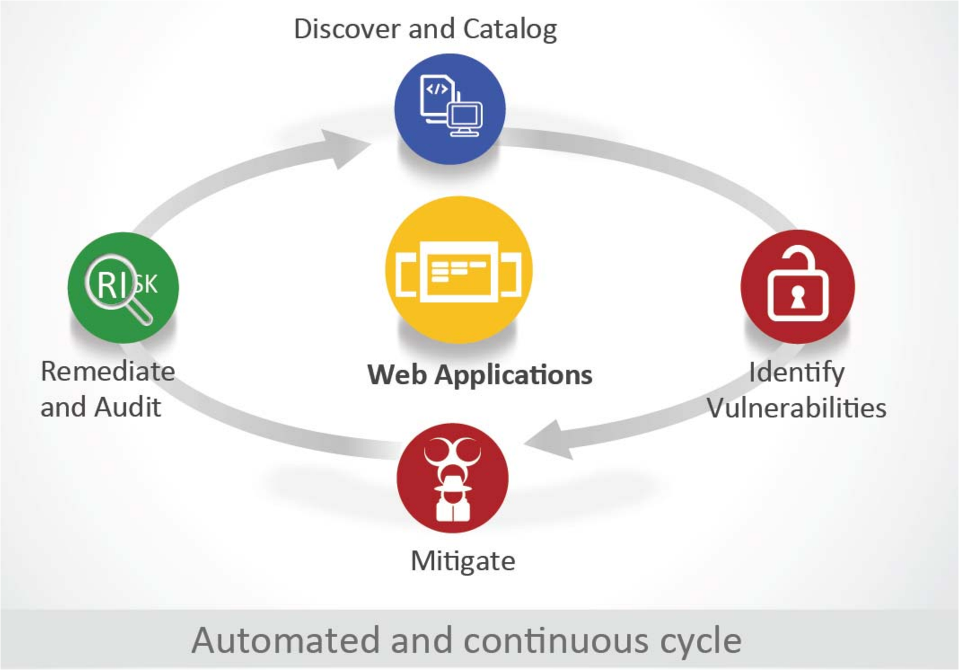
> Empower security professionals to rapidly discover and mitigate critical security concerns. With the new ScanTrust feature, Qualys WAF combines with Qualys WAS to provide true visibility for your web applications: Detect with WAS, protect with WAF and get scalable scanning, false-positive reduction and one-click patching to web apps.

https://www.qualys.com/apps/web-app-firewall/, attached hereto as Exhibit 16.

105. The ‘305 Accused Products include a network interface, housed within a computer, for receiving incoming content from the Internet on its destination to an Internet application running on the computer.



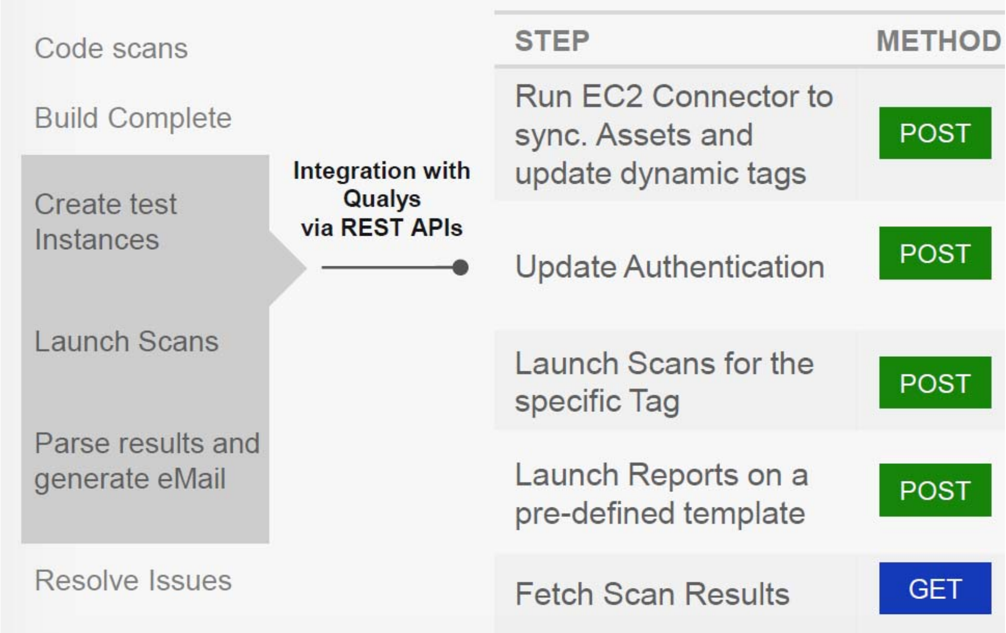
QualysGuard Web Application Security presentation at 30, attached hereto as Exhibit 8.



QualysGuard Web Application Security presentation at 5, attached hereto as Exhibit 8.

106. The ‘305 Accused Products include a database of parser and analyzer rules corresponding to computer exploits, stored within the computer, computer exploits being portions of program code that are malicious, and the parser and analyzer rules describe computer exploits as patterns of types of tokens, tokens being program code constructs, and types of tokens including a punctuation type, an identifier type and a function type.

107. The ‘305 Accused Products parse the scanning results to discover and catalog applications searching for portions of program code that are malicious according to analyzer rules (such as SQL injection, cross-site scripting (XSS), XML External Entities (XXE) and site misconfigurations), or pattern matching describing the computer exploits as patterns of types of tokens:



Code scans

Build Complete

Create test Instances

Launch Scans

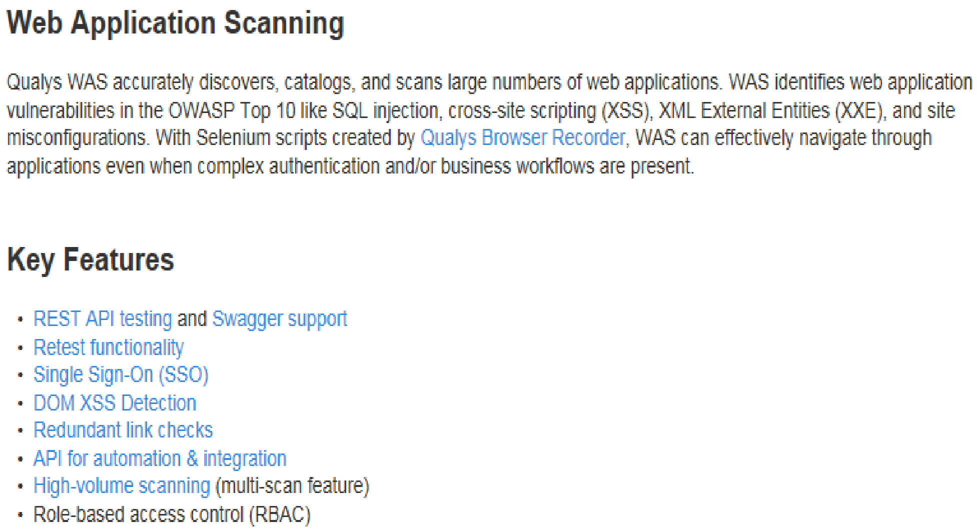
Parse results and generate eMail

Resolve Issues

Integration with Qualys via REST APIs

STEP	METHOD
Run EC2 Connector to sync. Assets and update dynamic tags	POST
Update Authentication	POST
Launch Scans for the specific Tag	POST
Launch Reports on a pre-defined template	POST
Fetch Scan Results	GET

Securing Public Cloud Infrastructure using Qualys presentation at 31, attached hereto as Exhibit 13.



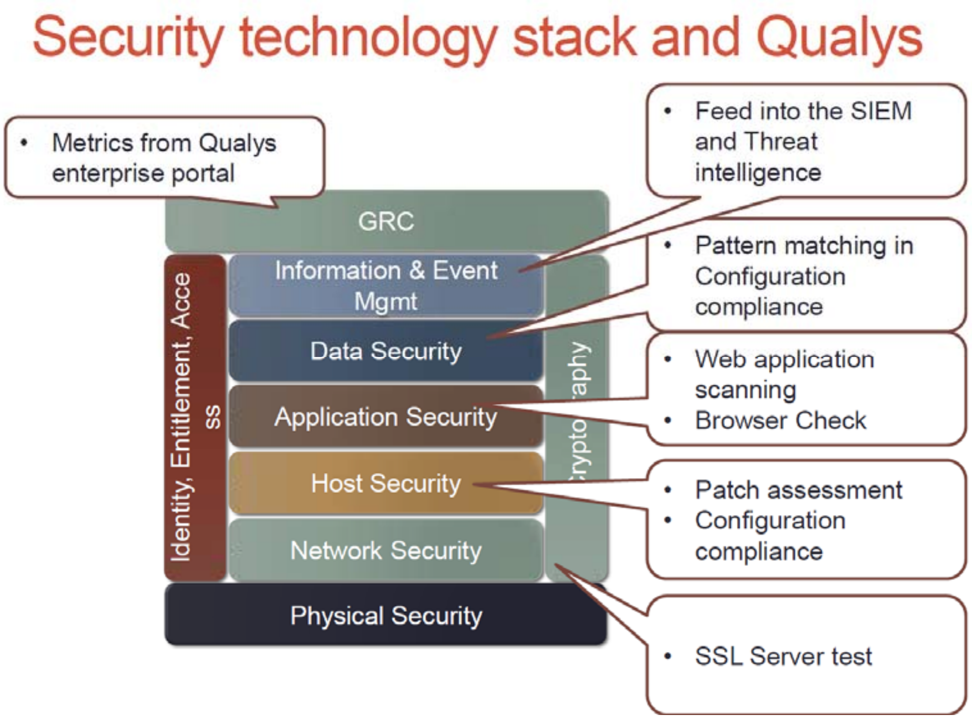
Web Application Scanning

Qualys WAS accurately discovers, catalogs, and scans large numbers of web applications. WAS identifies web application vulnerabilities in the OWASP Top 10 like SQL injection, cross-site scripting (XSS), XML External Entities (XXE), and site misconfigurations. With Selenium scripts created by Qualys Browser Recorder, WAS can effectively navigate through applications even when complex authentication and/or business workflows are present.

Key Features

- REST API testing and Swagger support
- Retest functionality
- Single Sign-On (SSO)
- DOM XSS Detection
- Redundant link checks
- API for automation & integration
- High-volume scanning (multi-scan feature)
- Role-based access control (RBAC)

https://community.qualys.com/community/web-application-scanning, attached hereto as Exhibit 11.

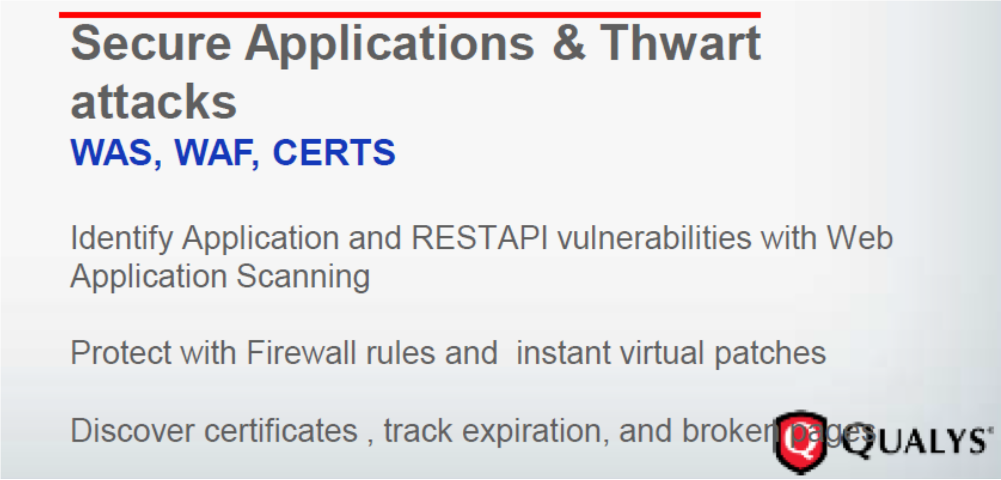


Security technology stack and Qualys

• Metrics from Qualys enterprise portal
GRC
Information & Event Mgmt
Data Security
Application Security
Host Security
Network Security
Physical Security
Identity, Entitlement, Acce ss
Crypto aphy
• Feed into the SIEM and Threat intelligence
• Pattern matching in Configuration compliance
• Web application scanning
• Browser Check
• Patch assessment
• Configuration compliance
• SSL Server test

Integrating Qualys into the Patch and Vulnerability Management Processes presentation at 4, attached hereto as Exhibit 18.

108. The '305 Accused Products protect content using Firewall (analyzer) rules:



Secure Applications & Thwart attacks

WAS, WAF, CERTS

Identify Application and RESTAPI vulnerabilities with Web Application Scanning

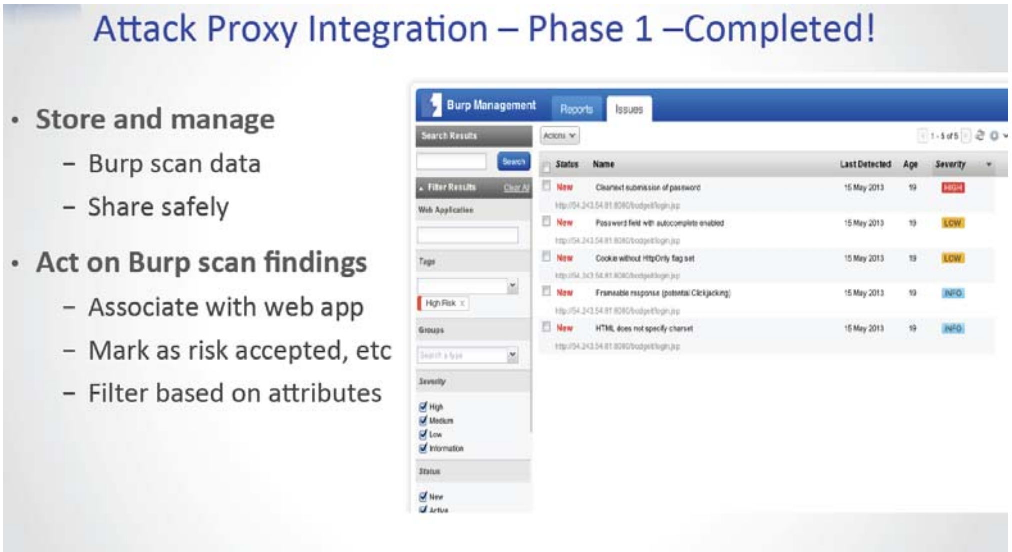
Protect with Firewall rules and instant virtual patches

Discover certificates , track expiration, and broken pages

Securing Public Cloud Infrastructure using Qualys presentation at 19, attached hereto as Exhibit 13.

109. The ‘305 Accused Products include a database of parser and analyzer rules, operatively coupled with the network interface, for scanning incoming content received by the network interface to recognize the presence of potential computer exploits.

110. The ‘305 Accused Products use Policy Compliance to evaluate content profiles, and the results (high/low risk) are saved as entries in the policy index for the data including entries that relate cache content and policies:

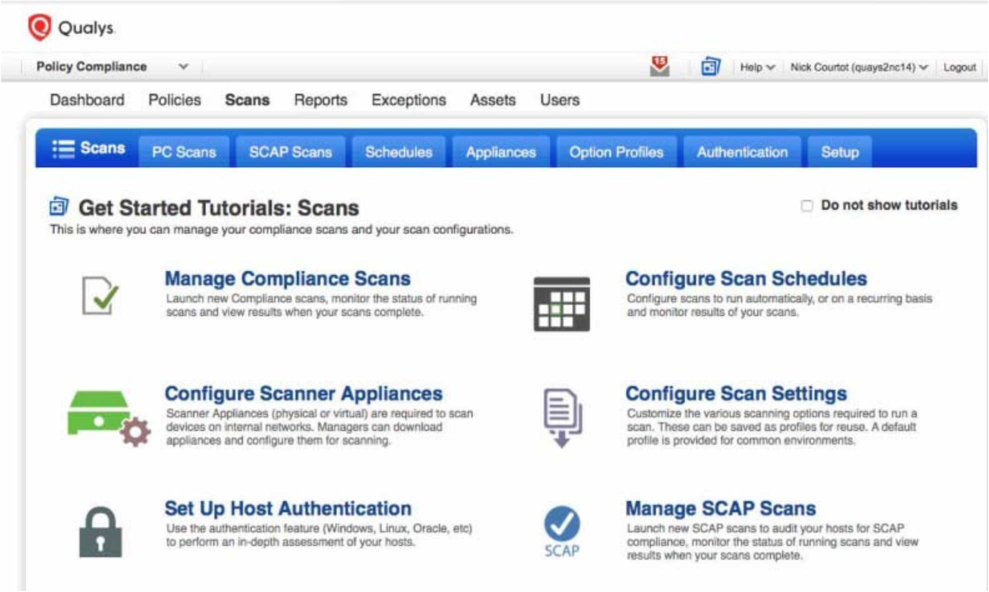


Attack Proxy Integration – Phase 1 –Completed!

- Store and manage
  - Burp scan data
  - Share safely
- Act on Burp scan findings
  - Associate with web app
  - Mark as risk accepted, etc
  - Filter based on attributes

Status	Name	Last Detected	Age	Severity
New	Cleartext submission of password http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	HIGH
New	Password field with autocomplete enabled http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	LOW
New	Cookie without HttpOnly flag set http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	LOW
New	Frameable response (potential Clickjacking) http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	INFO
New	HTML does not specify charset http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	INFO

QualysGuard Web Application Security presentation at 8, attached hereto as Exhibit 8.



Get Started Tutorials: Scans

☐ Do not show tutorials

This is where you can manage your compliance scans and your scan configurations.

Manage Compliance Scans
Launch new Compliance scans, monitor the status of running scans and view results when your scans complete.

Configure Scan Schedules
Configure scans to run automatically, or on a recurring basis and monitor results of your scans.

Configure Scanner Appliances
Scanner Appliances (physical or virtual) are required to scan devices on internal networks. Managers can download appliances and configure them for scanning.

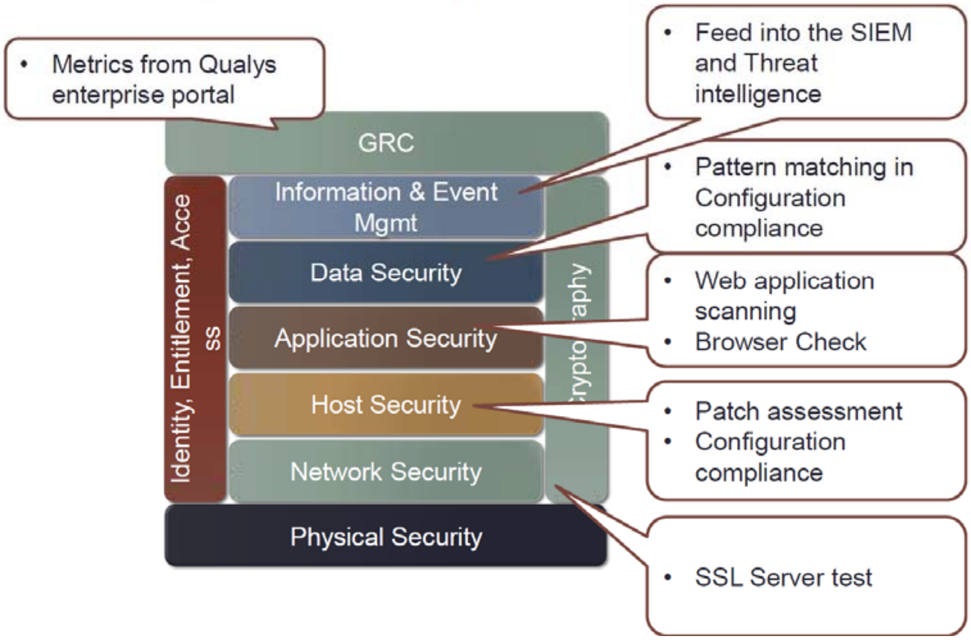
Configure Scan Settings
Customize the various scanning options required to run a scan. These can be saved as profiles for reuse. A default profile is provided for common environments.

Set Up Host Authentication
Use the authentication feature (Windows, Linux, Oracle, etc) to perform an in-depth assessment of your hosts.

Manage SCAP Scans
Launch new SCAP scans to audit your hosts for SCAP compliance, monitor the status of running scans and view results when your scans complete.

https://www.qualys.com/apps/policy-compliance/, attached hereto as Exhibit 17.

Security technology stack and Qualys



- Metrics from Qualys enterprise portal

- Feed into the SIEM and Threat intelligence

- Pattern matching in Configuration compliance

- Web application scanning
- Browser Check

- Patch assessment
- Configuration compliance

- SSL Server test

GRC

Identity, Entitlement, Acce ss

Information & Event Mgmt

Data Security

Application Security

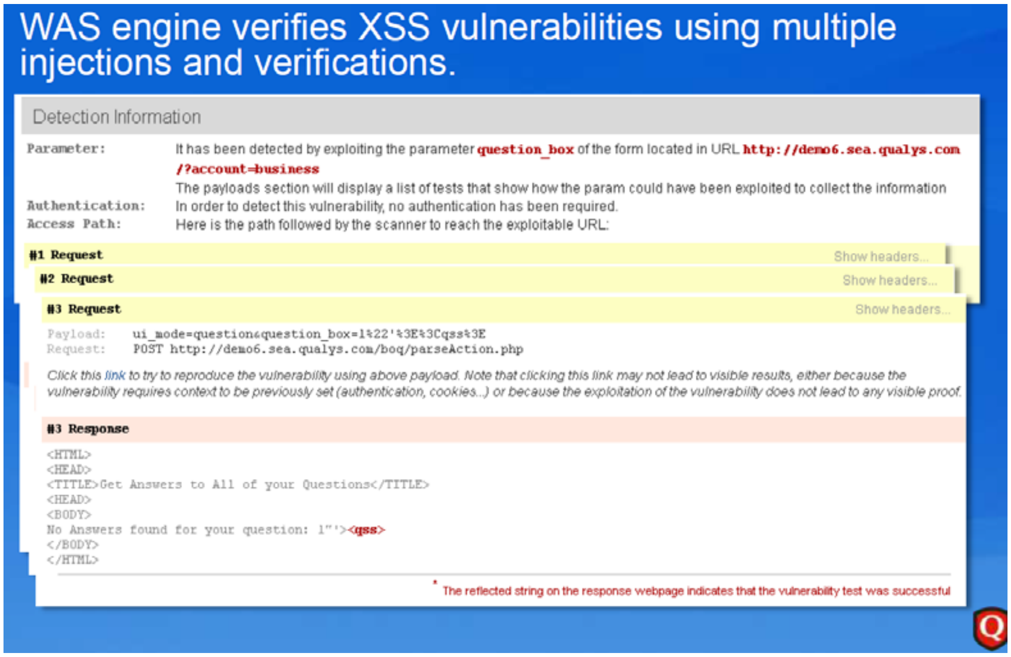
Host Security

Network Security

Crypto raphy

Physical Security

Integrating Qualys into the Patch and Vulnerability Management Processes presentation at 4, attached hereto as Exhibit 18.



WAS engine verifies XSS vulnerabilities using multiple injections and verifications.

Detection Information

Parameter:	It has been detected by exploiting the parameter **question_box** of the form located in URL **http://demo6.sea.qualys.com/?account=business** The payloads section will display a list of tests that show how the param could have been exploited to collect the information
Authentication:	In order to detect this vulnerability, no authentication has been required.
Access Path:	Here is the path followed by the scanner to reach the exploitable URL:

#1 Request Show headers...

#2 Request Show headers...

#3 Request Show headers...

```
Payload:   ui_mode=question&question_box=1%22'%3E%3Cqss%3E
Request:   POST http://demo6.sea.qualys.com/boq/parseAction.php
```

Click this link to try to reproduce the vulnerability using above payload. Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

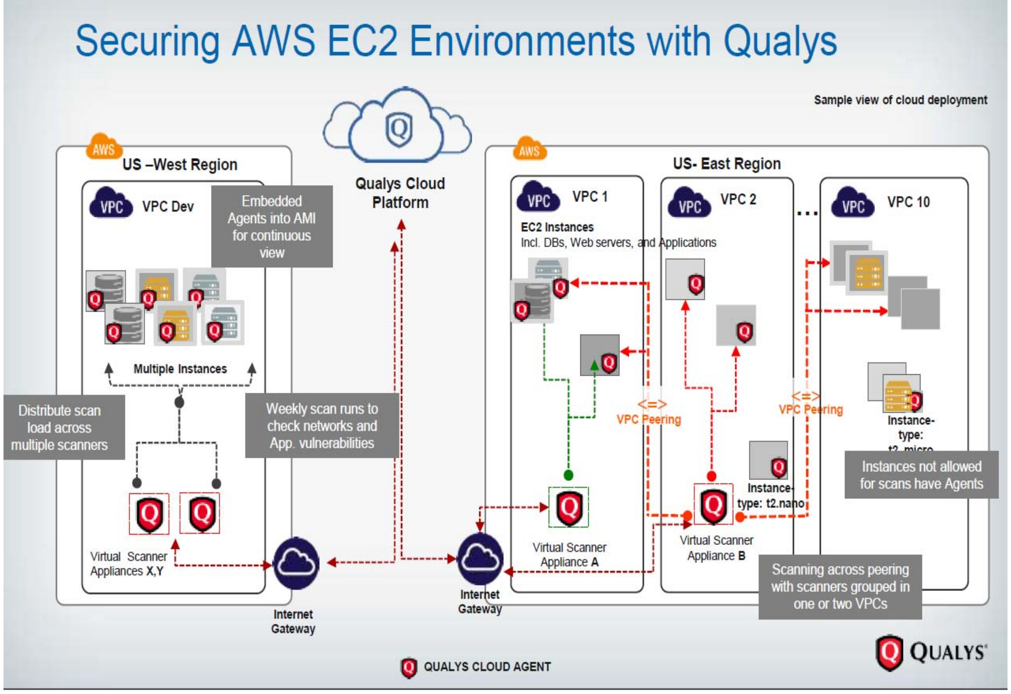
#3 Response

```
<HTML>
<HEAD>
<TITLE>Get Answers to All of your Questions</TITLE>
<HEAD>
<BODY>
No Answers found for your question: 1"'><qss>
</BODY>
</HTML>
```

* The reflected string on the response webpage indicates that the vulnerability test was successful

QualysGuard InfoDay 2014 presentation at17, attached hereto as Exhibit 12.

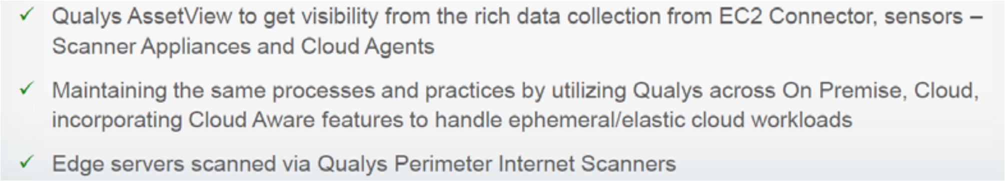
111. The '305 Accused Products include a network traffic probe, operatively coupled to the network interface and to the rule-based content scanner, for selectively diverting incoming content from its intended destination to the rule-based content scanner.



Securing AWS EC2 Environments with Qualys

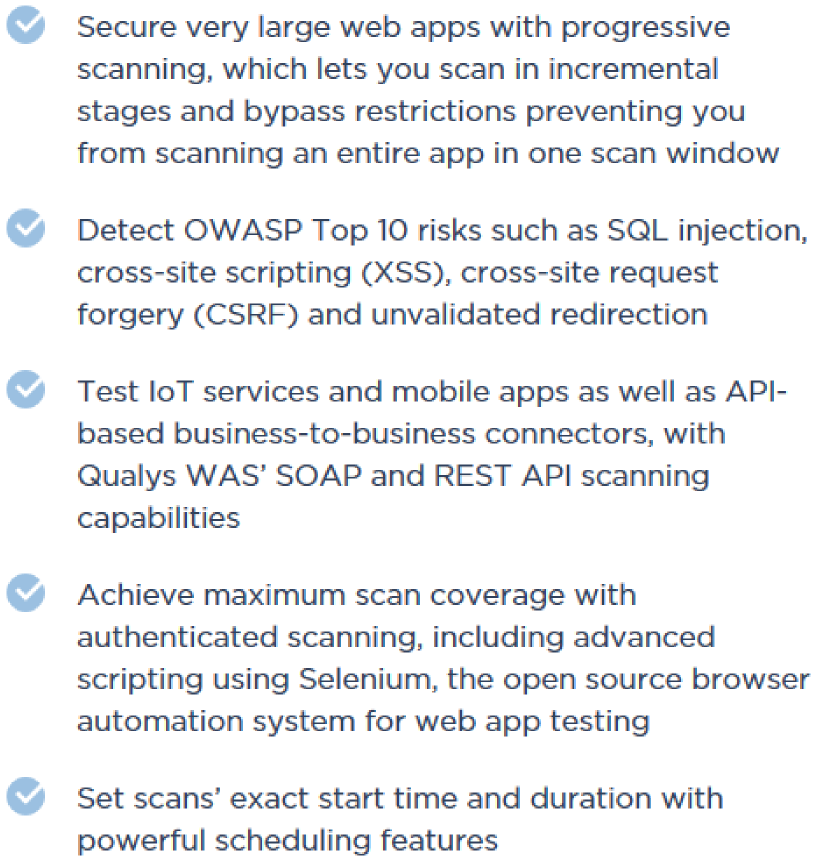
Sample view of cloud deployment

AWS
US –West Region
VPC
VPC Dev
Embedded Agents into AMI for continuous view
Multiple Instances
Distribute scan load across multiple scanners
Weekly scan runs to check networks and App. vulnerabilities
Virtual Scanner Appliances X,Y
Internet Gateway
Qualys Cloud Platform
Internet Gateway
AWS
US- East Region
VPC 1
EC2 Instances
Incl. DBs, Web servers, and Applications
VPC 2
VPC 10
<=>
VPC Peering
<=>
VPC Peering
Virtual Scanner Appliance A
Virtual Scanner Appliance B
Instance-type: t2.nano
Instance-type:
Instances not allowed for scans have Agents
Scanning across peering with scanners grouped in one or two VPCs
QUALYS CLOUD AGENT
QUALYS

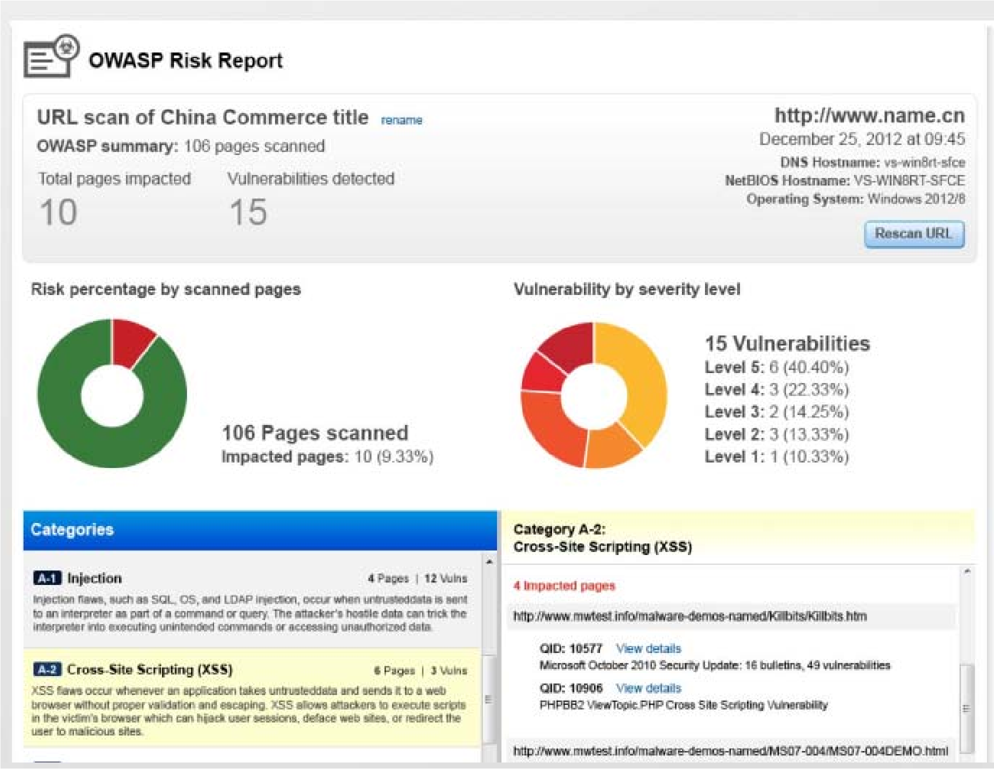


- ✓ Qualys AssetView to get visibility from the rich data collection from EC2 Connector, sensors – Scanner Appliances and Cloud Agents
- ✓ Maintaining the same processes and practices by utilizing Qualys across On Premise, Cloud, incorporating Cloud Aware features to handle ephemeral/elastic cloud workloads
- ✓ Edge servers scanned via Qualys Perimeter Internet Scanners

Securing Public Cloud Infrastructure using Qualys presentation at 28-29, attached hereto as Exhibit 13.



- ✓ Secure very large web apps with progressive scanning, which lets you scan in incremental stages and bypass restrictions preventing you from scanning an entire app in one scan window
- ✓ Detect OWASP Top 10 risks such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF) and unvalidated redirection
- ✓ Test IoT services and mobile apps as well as API-based business-to-business connectors, with Qualys WAS' SOAP and REST API scanning capabilities
- ✓ Achieve maximum scan coverage with authenticated scanning, including advanced scripting using Selenium, the open source browser automation system for web app testing
- ✓ Set scans' exact start time and duration with powerful scheduling features



OWASP Risk Report

URL scan of China Commerce title

OWASP summary: 106 pages scanned

Total pages impacted 10

Vulnerabilities detected 15

http://www.name.cn

December 25, 2012 at 09:45

DNS Hostname: vs-win8rt-sfce

NetBIOS Hostname: VS-WIN8RT-SFCE

Operating System: Windows 2012/8

Risk percentage by scanned pages

106 Pages scanned

Impacted pages: 10 (9.33%)

Vulnerability by severity level

15 Vulnerabilities

Level 5: 6 (40.40%)

Level 4: 3 (22.33%)

Level 3: 2 (14.25%)

Level 2: 3 (13.33%)

Level 1: 1 (10.33%)

Categories

A-1 Injection 4 Pages | 12 Vulns

Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusteddata is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.

A-2 Cross-Site Scripting (XSS) 6 Pages | 3 Vulns

XSS flaws occur whenever an application takes untrusteddata and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

Category A-2:
Cross-Site Scripting (XSS)

4 Impacted pages

http://www.mwtest.info/malware-demos-named/Killbits/Killbits.htm

QID: 10577 View details

Microsoft October 2010 Security Update: 16 bulletins, 49 vulnerabilities

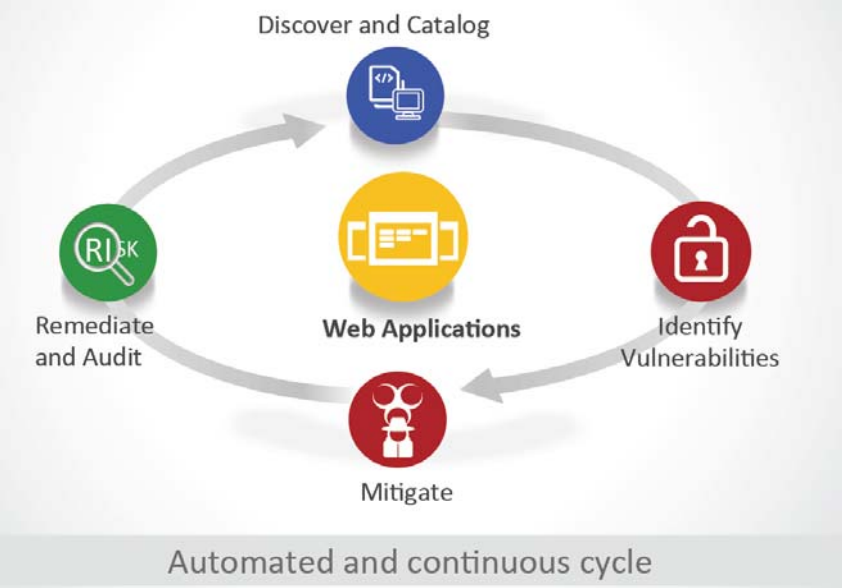
QID: 10906 View details

PHPBB2 ViewTopic.PHP Cross Site Scripting Vulnerability

http://www.mwtest.info/malware-demos-named/MS07-004/MS07-004DEMO.html

https://www.qualys.com/apps/web-app-scanning/, attached hereto as Exhibit 19.

112. The '305 Accused Products include a rule update manager that communicates with the database of parser and analyzer rules, for updating the database of parser and analyzer rules periodically to incorporate new parser and analyzer rules that are made available.



Discover and Catalog

Web Applications

Identify Vulnerabilities

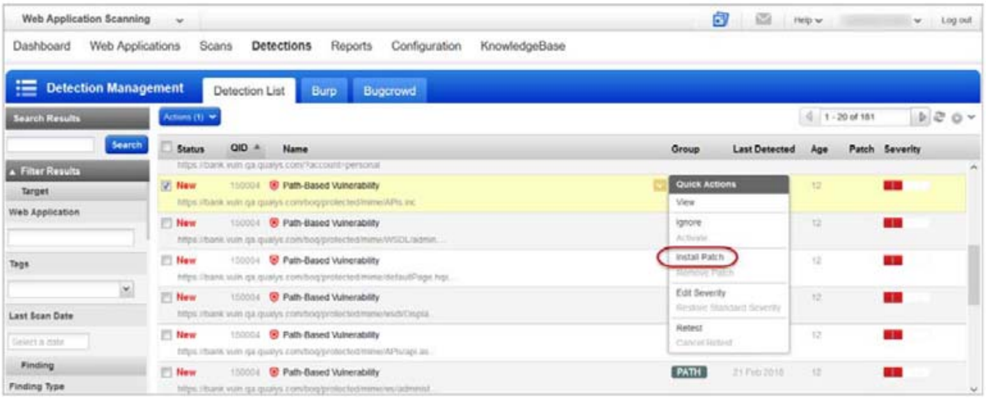
Mitigate

Remediate and Audit

Automated and continuous cycle

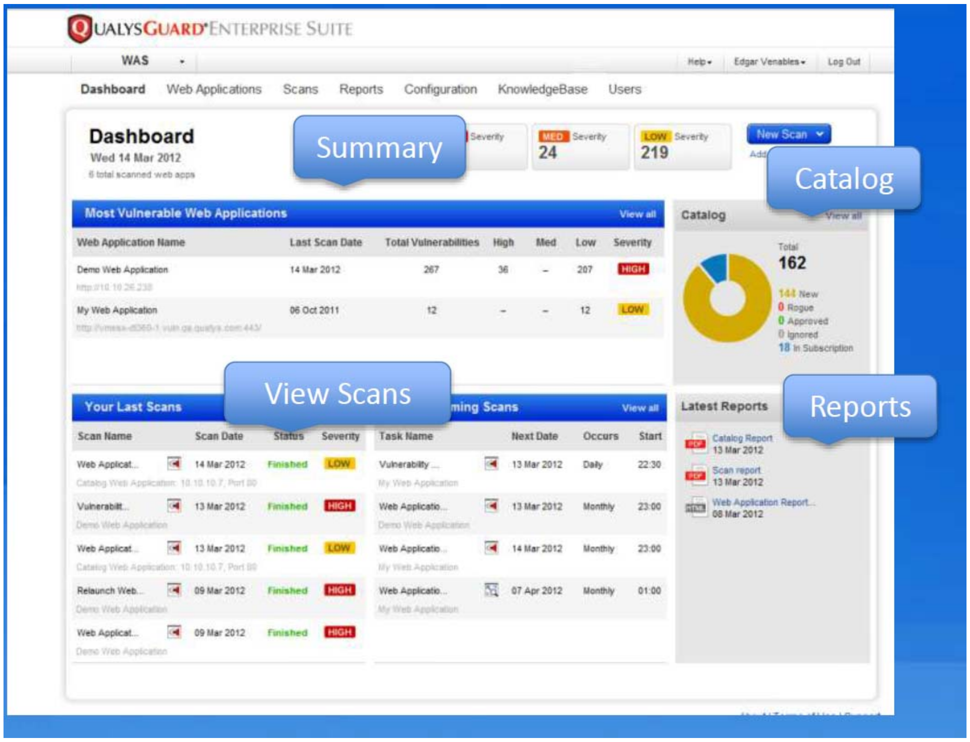
QualysGuard Web Application Security presentation at 5, attached hereto as Exhibit 8.

113. Virtual patching is the process of creating and implementing a temporary policy that is used to mitigate exploitation risks associated with the discovery of new security vulnerabilities. The '305 Accused Products add virtual patches upon vulnerability detection and catalog new threats in order to update parser and analyzer rules:



Status	QID	Name	Group	Last Detected	Age	Patch	Severity
		https://bank.vuln.qa.qualys.com/?account=personal					
☑ New	150004	Path-Based Vulnerability https://bank.vuln.qa.qualys.com/boq/protected/mime/APIs.inc			12		
☐ New	150004	Path-Based Vulnerability https://bank.vuln.qa.qualys.com/boq/protected/mime/WSDL/admin...			12		
☐ New	150004	Path-Based Vulnerability https://bank.vuln.qa.qualys.com/boq/protected/mime/defaultPage.hqx...			12		
☐ New	150004	Path-Based Vulnerability https://bank.vuln.qa.qualys.com/boq/protected/mime/wsdl/Displa			12		
☐ New	150004	Path-Based Vulnerability https://bank.vuln.qa.qualys.com/boq/protected/mime/APIs/api.as			12		
☐ New	150004	Path-Based Vulnerability https://bank.vuln.qa.qualys.com/boq/protected/mime/ws/adminst	PATH	21 Feb 2018	12		

Qualys Web Application Firewall Getting Started Guide at 27, attached hereto as Exhibit 20.



Dashboard
Wed 14 Mar 2012
6 total scanned web apps

Severity | MED Severity 24 | LOW Severity 219

Most Vulnerable Web Applications

Web Application Name	Last Scan Date	Total Vulnerabilities	High	Med	Low	Severity
Demo Web Application http://10.10.26.238	14 Mar 2012	267	36	–	207	HIGH
My Web Application http://vmesx-d060-1.vuln.qa.qualys.com:443/	06 Oct 2011	12	–	–	12	LOW

Catalog

Total 162
144 New
0 Rogue
0 Approved
0 Ignored
18 In Subscription

Your Last Scans

Scan Name	Scan Date	Status	Severity
Web Applicat... Catalog Web Application: 10.10.10.7, Port 80	14 Mar 2012	Finished	LOW
Vulnerabilit... Demo Web Application	13 Mar 2012	Finished	HIGH
Web Applicat... Catalog Web Application: 10.10.10.7, Port 80	13 Mar 2012	Finished	LOW
Relaunch Web... Demo Web Application	09 Mar 2012	Finished	HIGH
Web Applicat... Demo Web Application	09 Mar 2012	Finished	HIGH

ming Scans

Task Name	Next Date	Occurs	Start
Vulnerabilty ... My Web Application	13 Mar 2012	Daily	22:30
Web Applicatio... Demo Web Application	13 Mar 2012	Monthly	23:00
Web Applicatio... My Web Application	14 Mar 2012	Monthly	23:00
Web Applicatio... My Web Application	07 Apr 2012	Monthly	01:00

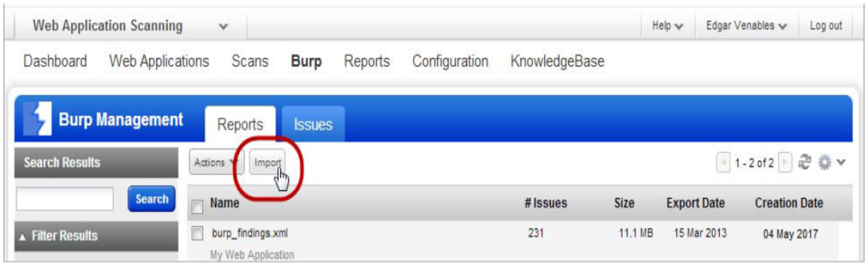
Latest Reports

Catalog Report 13 Mar 2012
Scan report 13 Mar 2012
Web Application Report... 08 Mar 2012

QualysGuard InfoDay 2014 presentation at 29, attached hereto as Exhibit 12.

114. The ‘305 Accused Products include a database manager for storing scanned data in a database:

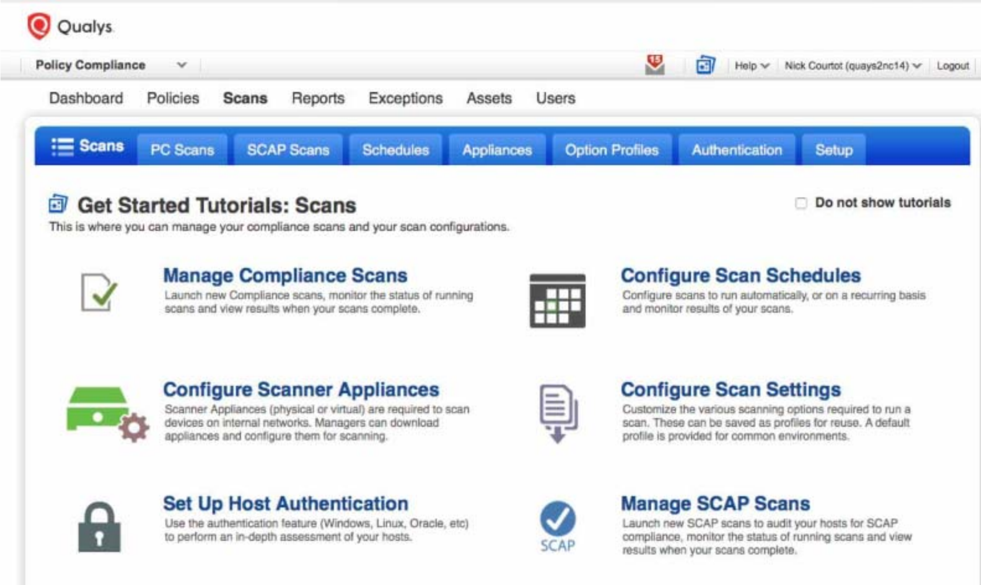
> The Burp Management feature gives you a way to store the findings discovered by the Burp Suite scanner with those discovered by WAS and share this information with multiple users. To learn more refer to this blog article at the Qualys Community. (This feature is not available to Express Lite users.)
>
> To get started click the Burp option on the top menu and go to Burp > Reports, then click Import and we'll walk you through the steps. Your issues list shows imported Burp issues.



Name	# Issues	Size	Export Date	Creation Date
burp_findings.xml My Web Application	231	11.1 MB	15 Mar 2013	04 May 2017

Qualys Web Application Scanning Getting Started Guide Version 6.0.1 at 20, attached hereto as Exhibit 15.

115. The ‘305 Accused Products use Policy Compliance to evaluate content profiles, and the results are saved as entries in the policy index.



Get Started Tutorials: Scans

This is where you can manage your compliance scans and your scan configurations.

□ Do not show tutorials

Manage Compliance Scans
Launch new Compliance scans, monitor the status of running scans and view results when your scans complete.

Configure Scan Schedules
Configure scans to run automatically, or on a recurring basis and monitor results of your scans.

Configure Scanner Appliances
Scanner Appliances (physical or virtual) are required to scan devices on internal networks. Managers can download appliances and configure them for scanning.

Configure Scan Settings
Customize the various scanning options required to run a scan. These can be saved as profiles for reuse. A default profile is provided for common environments.

Set Up Host Authentication
Use the authentication feature (Windows, Linux, Oracle, etc) to perform an in-depth assessment of your hosts.

Manage SCAP Scans
Launch new SCAP scans to audit your hosts for SCAP compliance, monitor the status of running scans and view results when your scans complete.

https://www.qualys.com/apps/policy-compliance/, attached hereto as Exhibit 17.

116. Defendant's 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 Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendant compete in the security software space, and Finjan is actively engaged in licensing its patent portfolio. Defendant's 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.

117. Defendant has been long-aware of Finjan's patents, including the '305 Patent, and continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendant for nearly three years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that its products infringe Finjan's patents, including the '305 Patent, on information and belief Defendant made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendant's blatant and egregious disregard for Finjan's patent rights.

118. Despite its knowledge of Finjan's patent portfolio and Asserted Patents, and its specific knowledge of its own infringement, Defendant continued to sell the '305 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 VI
(Indirect Infringement of the '305 Patent pursuant to 35 U.S.C. § 271(b))

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

120. In addition to directly infringing the ‘305 Patent, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 14-24 of the ‘305 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its customers to perform the steps of the method claims of the ‘305 Patent, either literally or under the doctrine of equivalents.

121. Additionally, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 14-24 of the ‘305 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its developers to perform the steps of the method claims of the ‘305 Patent, either literally or under the doctrine of equivalents.

122. Defendant knowingly and actively aided and abetted the direct infringement of the ‘305 Patent by instructing and encouraging its 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. *See, e.g.*, QualysGuard Web Application Security presentation, attached hereto as Exhibit 8; https://community.qualys.com/community/web-application-scanning, attached hereto as Exhibit 11; QualysGuard InfoDay 2014 presentation , attached hereto as Exhibit 12; Securing Public Cloud Infrastructure using Qualys presentation, attached hereto as Exhibit 13; Qualys Web Application Scanning Getting Started Guide Version 6.0.1, attached hereto as Exhibit 15; https://www.qualys.com/apps/web-app-firewall/, attached hereto as Exhibit 16; https://www.qualys.com/apps/policy-compliance/, attached hereto as Exhibit 17; Integrating Qualys into the Patch and Vulnerability Management Processes presentation, attached hereto as Exhibit 18; https://www.qualys.com/apps/web-app-scanning/, attached hereto as Exhibit 19; Qualys Web Application Firewall Getting Started Guide, attached hereto as Exhibit 20.

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

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

124. Defendant has infringed and continues to infringe Claims 1-35 of the ‘408 Patent in violation of 35 U.S.C. § 271(a).

125. Defendant’s infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

126. Defendant’s acts of making, using, importing, selling, and offering for sale infringing products and services has been without the permission, consent, authorization or license of Finjan.

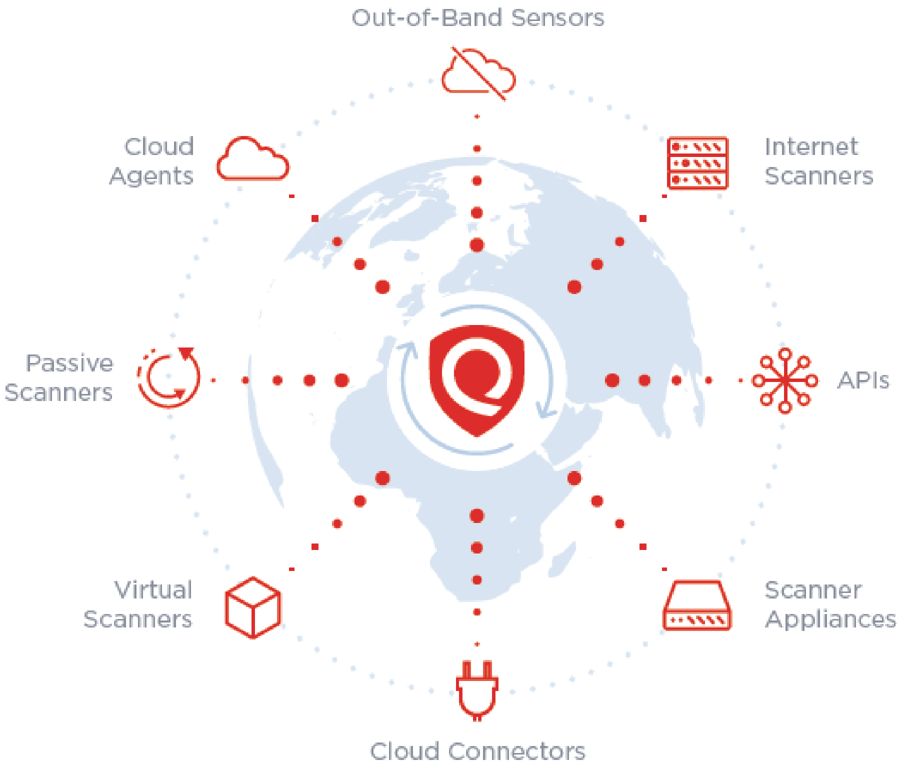
127. Defendant’s infringement includes the manufacture, use, sale, importation and offer for sale of Defendant’s products and services that utilize Vulnerability Management, Threat Protection, Continuous Monitoring, Indicators of Compromise, Container Security, Web App Firewall, Web App Scanning, and Compliance Monitoring, including Qualys Cloud Platform products (collectively, “the ‘408 Accused Products”).

128. 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.

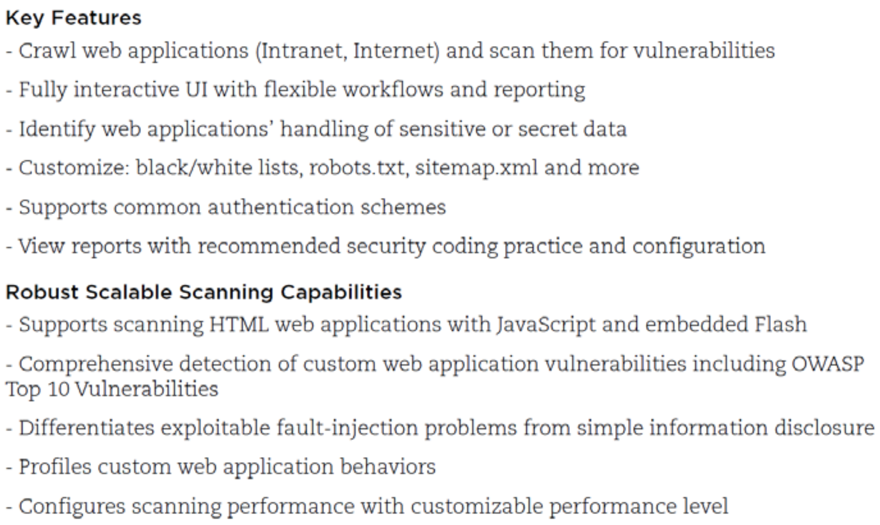
129. To the extent the ‘408 Accused Products use a system that includes modules, components or software owned by third parties, the ‘408 Accused Products still infringe the ‘408 Patent because Defendant is vicariously liable for the use of the patented system by controlling the entire system and deriving a benefit from the use of every element of the entire system. Similarly, to the extent Defendant’s customers perform a step or steps of the patented method or the ‘408 Accused Products incorporate third parties’ modules, components or software that perform one or more patented steps, Defendant’s ‘408 Accused Products still infringe 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.

130. The '408 Accused Products are computer systems for multi-lingual content scanning.



Qualys Cloud Platform datasheet at 2, attached hereto as Exhibit 22.



Key Features

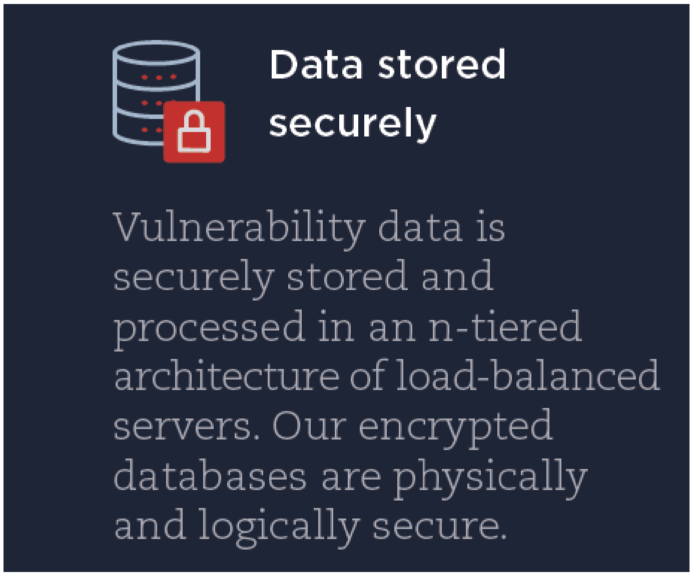
- Crawl web applications (Intranet, Internet) and scan them for vulnerabilities
- Fully interactive UI with flexible workflows and reporting
- Identify web applications' handling of sensitive or secret data
- Customize: black/white lists, robots.txt, sitemap.xml and more
- Supports common authentication schemes
- View reports with recommended security coding practice and configuration

Robust Scalable Scanning Capabilities

- Supports scanning HTML web applications with JavaScript and embedded Flash
- Comprehensive detection of custom web application vulnerabilities including OWASP Top 10 Vulnerabilities
- Differentiates exploitable fault-injection problems from simple information disclosure
- Profiles custom web application behaviors
- Configures scanning performance with customizable performance level

Qualys Web Application Scanning Getting Started Guide Version 6.0.1 at 4, attached hereto as Exhibit 15.

131. The ‘408 Accused Products include a non-transitory computer-readable storage medium (i.e., computer software) storing computer-executable program code that is executed by a computer to scan incoming program code.



Data stored securely

Vulnerability data is securely stored and processed in an n-tiered architecture of load-balanced servers. Our encrypted databases are physically and logically secure.

Qualys Cloud Platform datasheet at 3, attached hereto as Exhibit 22.

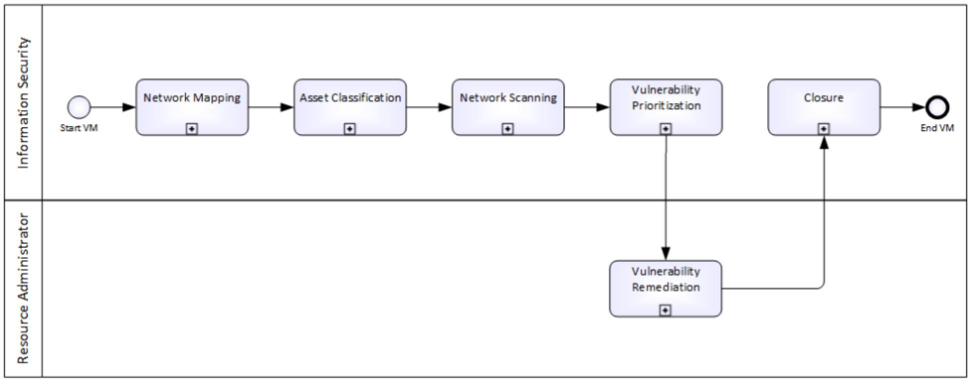
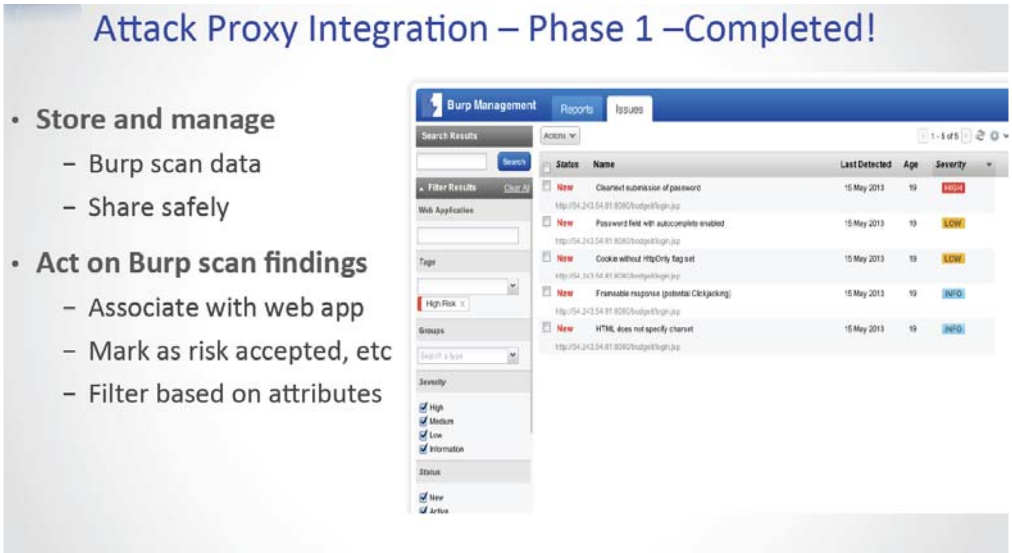


Figure 1: Vulnerability management process

https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.



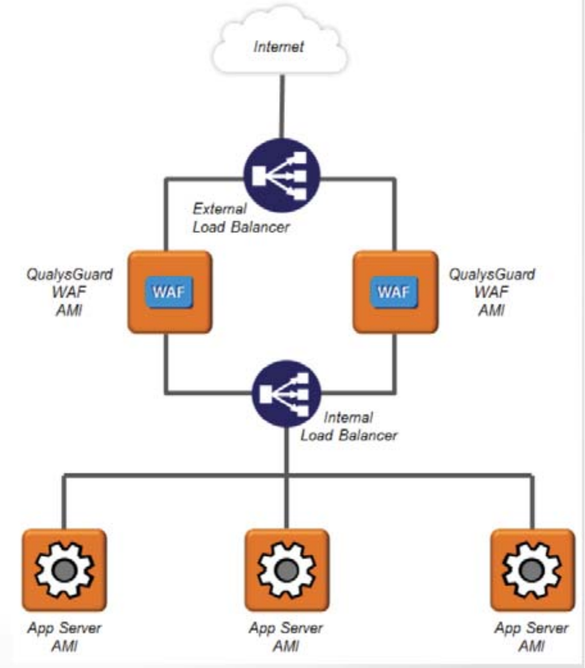
Attack Proxy Integration – Phase 1 –Completed!

- Store and manage
  - Burp scan data
  - Share safely
- Act on Burp scan findings
  - Associate with web app
  - Mark as risk accepted, etc
  - Filter based on attributes

Status	Name	Last Detected	Age	Severity
New	Cleartext submission of password http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	HIGH
New	Password field with autocomplete enabled http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	LOW
New	Cookie without HttpOnly flag set http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	LOW
New	Framable response (potential Clickjacking) http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	INFO
New	HTML does not specify charset http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	INFO

QualysGuard Web Application Security presentation at 8, attached hereto as Exhibit 8.

132. The ‘408 Accused Products include a receiver, stored on the medium and executed by the computer, for receiving an incoming stream of program code.



QualysGuard Web Application Security presentation at 30, attached hereto as Exhibit 8.

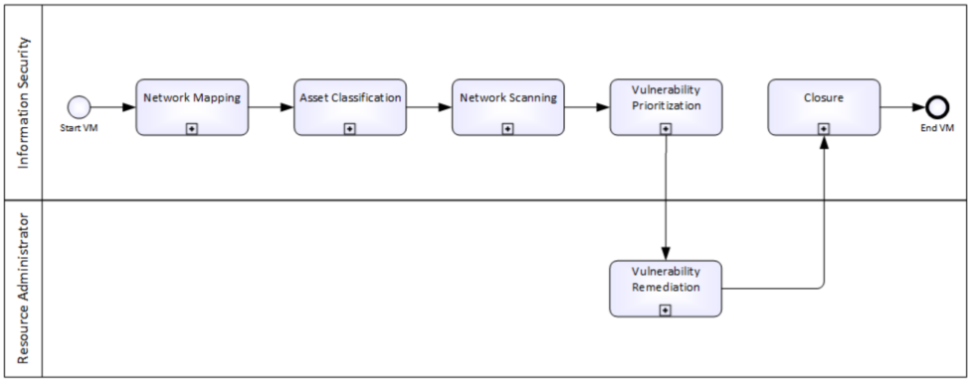
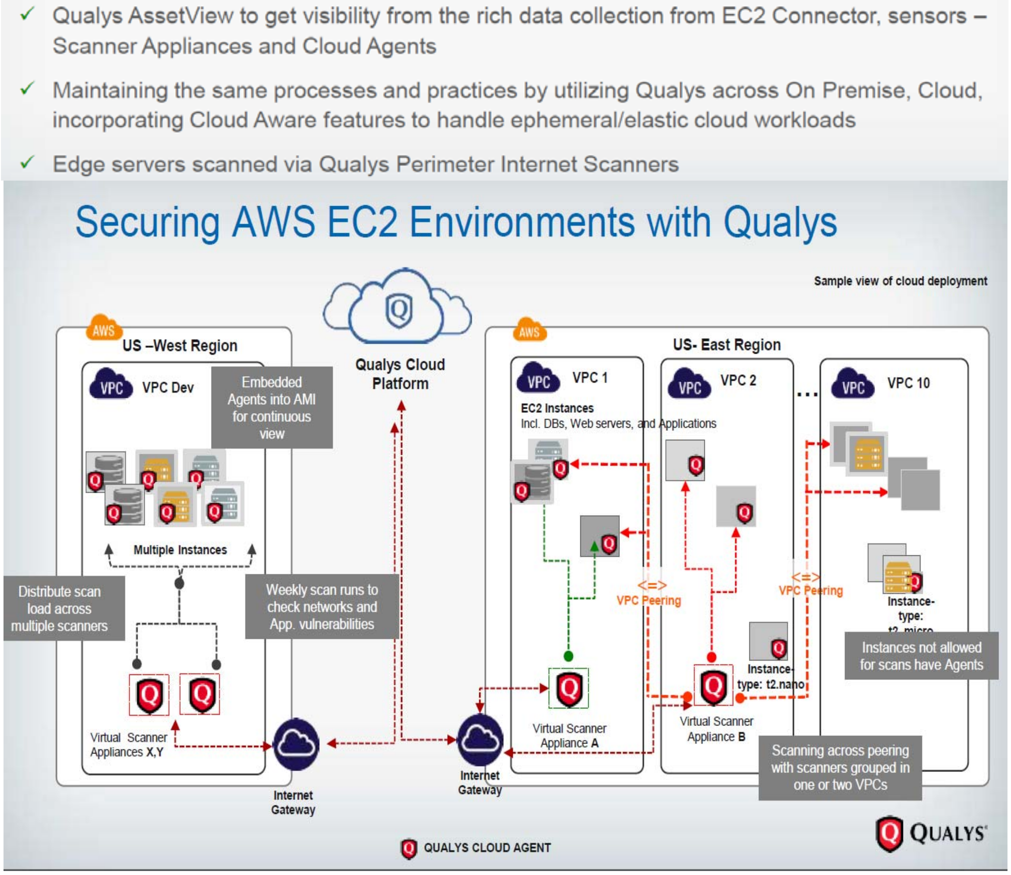


Figure 1: Vulnerability management process

https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.



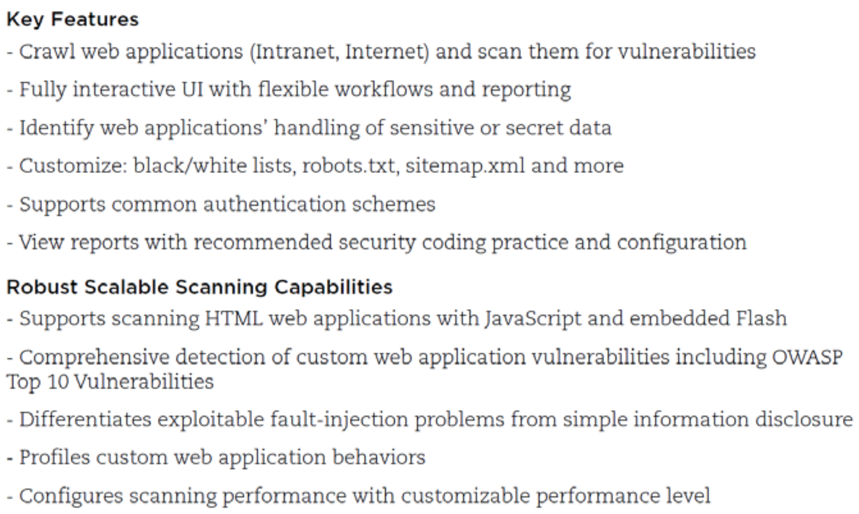
- ✓ Qualys AssetView to get visibility from the rich data collection from EC2 Connector, sensors – Scanner Appliances and Cloud Agents
- ✓ Maintaining the same processes and practices by utilizing Qualys across On Premise, Cloud, incorporating Cloud Aware features to handle ephemeral/elastic cloud workloads
- ✓ Edge servers scanned via Qualys Perimeter Internet Scanners

Securing AWS EC2 Environments with Qualys

Sample view of cloud deployment
AWS
US –West Region
VPC
VPC Dev
Embedded Agents into AMI for continuous view
Qualys Cloud Platform
Multiple Instances
Distribute scan load across multiple scanners
Weekly scan runs to check networks and App. vulnerabilities
Virtual Scanner Appliances X,Y
Internet Gateway
AWS
US- East Region
VPC 1
EC2 Instances
Incl. DBs, Web servers, and Applications
VPC 2
VPC 10
<=>
VPC Peering
<=>
VPC Peering
Instance-type: t2.micro
Instances not allowed for scans have Agents
Instance-type: t2.nano
Virtual Scanner Appliance A
Virtual Scanner Appliance B
Scanning across peering with scanners grouped in one or two VPCs
Internet Gateway
QUALYS CLOUD AGENT
QUALYS

Securing Public Cloud Infrastructure using Qualys presentation at 28-29, attached hereto as Exhibit 13.

133. The ‘408 Accused Products include a multi-lingual language detector, stored on the medium and executed by the computer, operatively coupled to the receiver for detecting the programming language in which the incoming stream is written:



Key Features

- Crawl web applications (Intranet, Internet) and scan them for vulnerabilities
- Fully interactive UI with flexible workflows and reporting
- Identify web applications’ handling of sensitive or secret data
- Customize: black/white lists, robots.txt, sitemap.xml and more
- Supports common authentication schemes
- View reports with recommended security coding practice and configuration

Robust Scalable Scanning Capabilities

- Supports scanning HTML web applications with JavaScript and embedded Flash
- Comprehensive detection of custom web application vulnerabilities including OWASP Top 10 Vulnerabilities
- Differentiates exploitable fault-injection problems from simple information disclosure
- Profiles custom web application behaviors
- Configures scanning performance with customizable performance level

Qualys Web Application Scanning Getting Started Guide Version 6.0.1 at 4, attached hereto as Exhibit 15.

134. The ‘408 Accused Products include a scanner instantiator, stored on the medium and executed by the computer, operatively coupled to the receiver and the multi-lingual language detector for instantiating a scanner for the specific programming language.

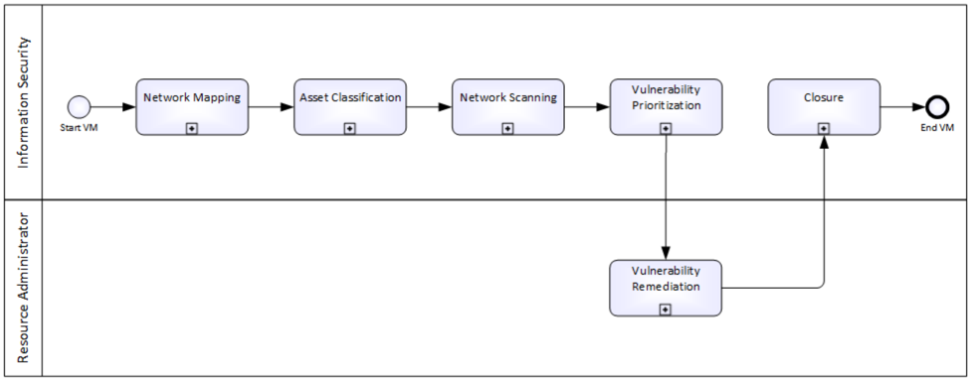
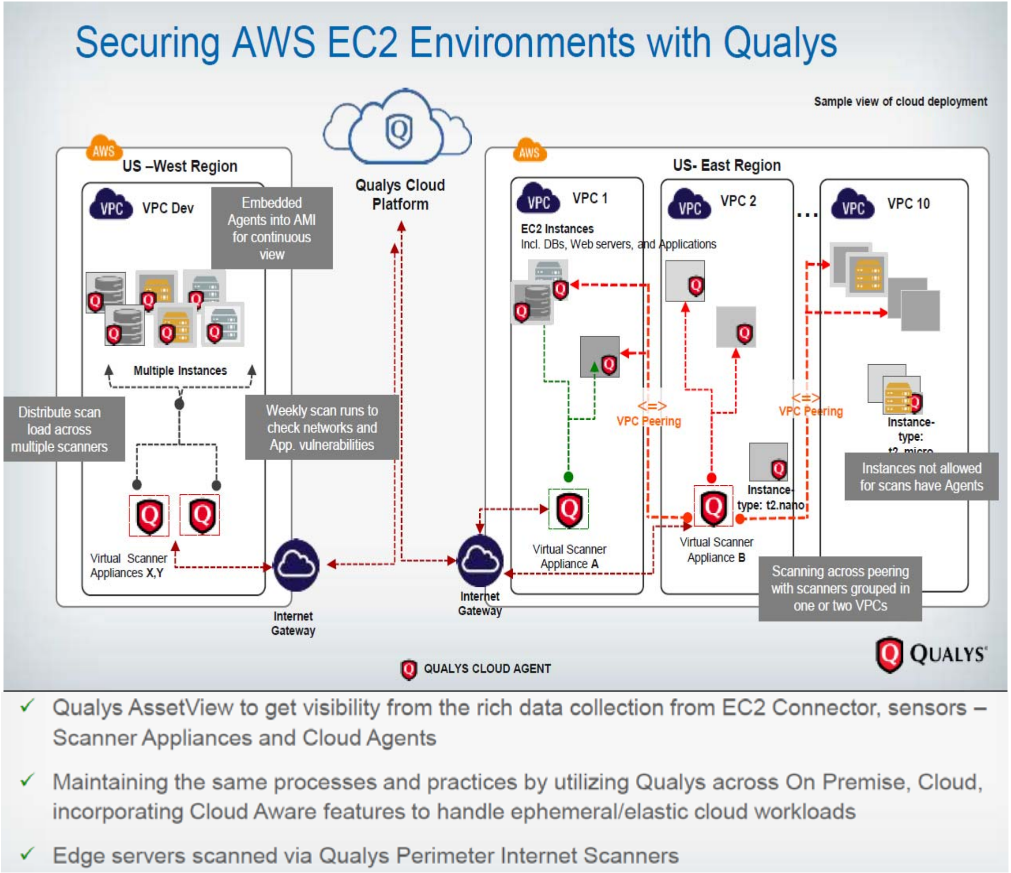


Figure 1: Vulnerability management process

https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.



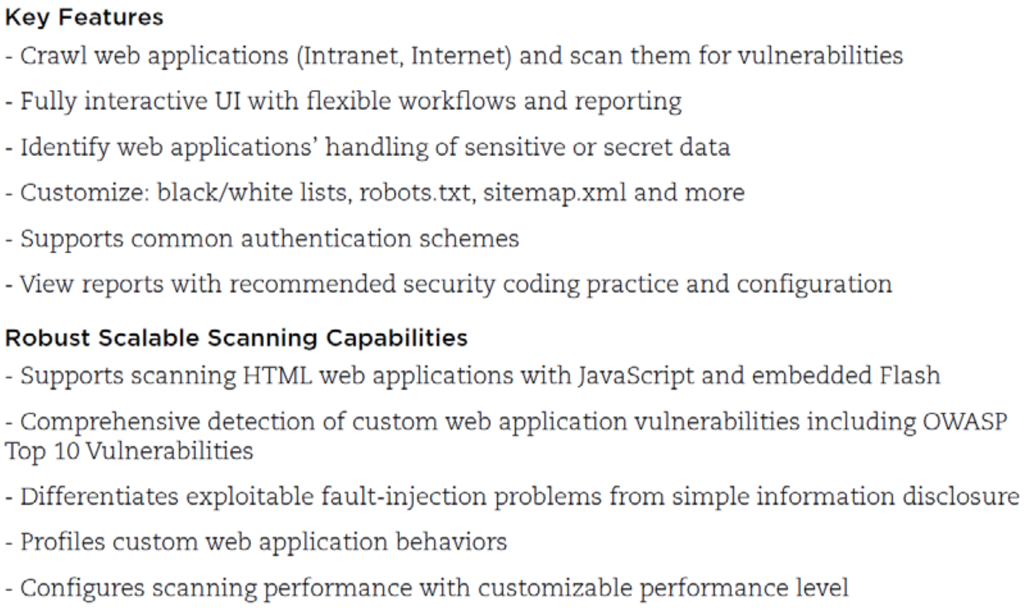
Securing AWS EC2 Environments with Qualys

Sample view of cloud deployment

AWS
US –West Region
VPC
VPC Dev
Embedded Agents into AMI for continuous view
Qualys Cloud Platform
Multiple Instances
Distribute scan load across multiple scanners
Weekly scan runs to check networks and App. vulnerabilities
Virtual Scanner Appliances X,Y
Internet Gateway
AWS
US- East Region
VPC 1
EC2 Instances
Incl. DBs, Web servers, and Applications
VPC 2
VPC 10
<=> VPC Peering
<=> VPC Peering
Instance-type: t2.micro
Instances not allowed for scans have Agents
Instance-type: t2.nano
Virtual Scanner Appliance A
Virtual Scanner Appliance B
Internet Gateway
Scanning across peering with scanners grouped in one or two VPCs
QUALYS CLOUD AGENT
QUALYS

- ✓ Qualys AssetView to get visibility from the rich data collection from EC2 Connector, sensors – Scanner Appliances and Cloud Agents
- ✓ Maintaining the same processes and practices by utilizing Qualys across On Premise, Cloud, incorporating Cloud Aware features to handle ephemeral/elastic cloud workloads
- ✓ Edge servers scanned via Qualys Perimeter Internet Scanners

Securing Public Cloud Infrastructure using Qualys presentation at 28-29, attached hereto as Exhibit 13.



Key Features

- Crawl web applications (Intranet, Internet) and scan them for vulnerabilities

- Fully interactive UI with flexible workflows and reporting

- Identify web applications' handling of sensitive or secret data

- Customize: black/white lists, robots.txt, sitemap.xml and more

- Supports common authentication schemes

- View reports with recommended security coding practice and configuration

Robust Scalable Scanning Capabilities

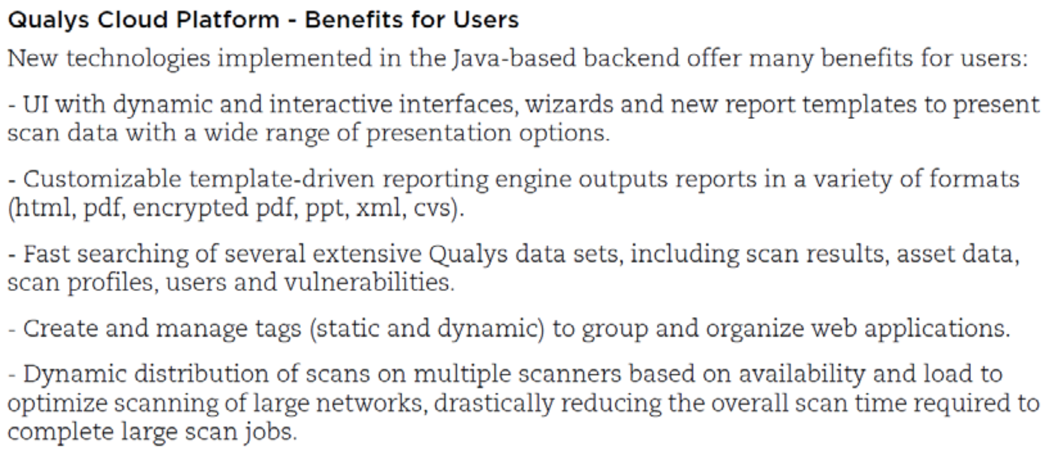
- Supports scanning HTML web applications with JavaScript and embedded Flash

- Comprehensive detection of custom web application vulnerabilities including OWASP Top 10 Vulnerabilities

- Differentiates exploitable fault-injection problems from simple information disclosure

- Profiles custom web application behaviors

- Configures scanning performance with customizable performance level



Qualys Cloud Platform - Benefits for Users

New technologies implemented in the Java-based backend offer many benefits for users:

- UI with dynamic and interactive interfaces, wizards and new report templates to present scan data with a wide range of presentation options.

- Customizable template-driven reporting engine outputs reports in a variety of formats (html, pdf, encrypted pdf, ppt, xml, cvs).

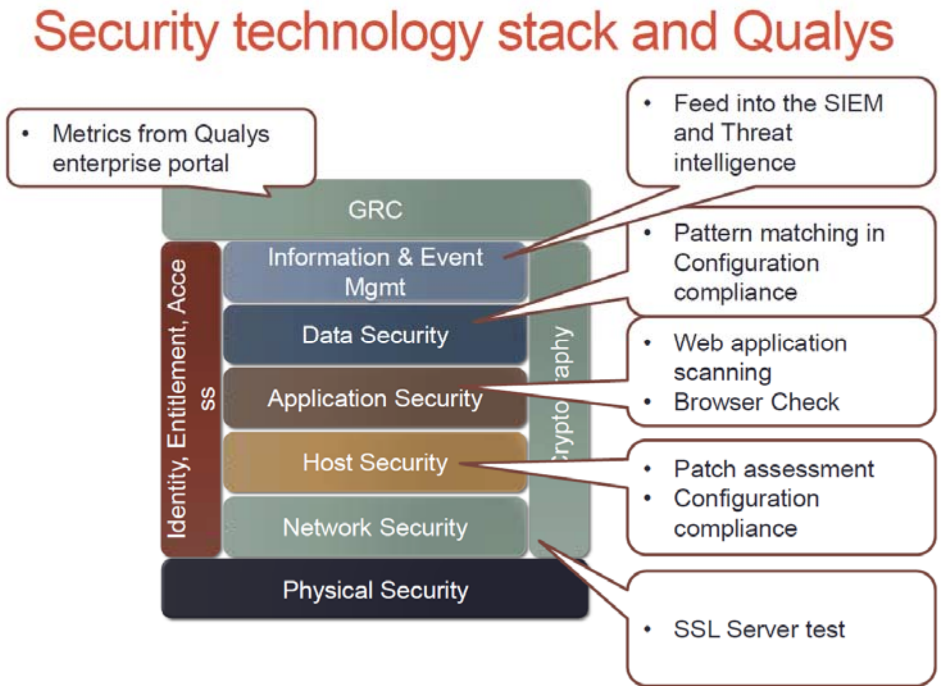
- Fast searching of several extensive Qualys data sets, including scan results, asset data, scan profiles, users and vulnerabilities.

- Create and manage tags (static and dynamic) to group and organize web applications.

- Dynamic distribution of scans on multiple scanners based on availability and load to optimize scanning of large networks, drastically reducing the overall scan time required to complete large scan jobs.

Qualys Web Application Scanning Getting Started Guide Version 6.0.1 at 4, attached hereto as Exhibit 15.

135. The '408 Accused Products include a rules accessor for accessing parser rules and analyzer rules for the specific programming language, where the parser rules define certain patterns in terms of tokens, tokens being lexical constructs for the specific programming language, and where the analyzer rules identify certain combinations of tokens and patterns as being indicators of potential exploits, exploits being portions of program code that are malicious.

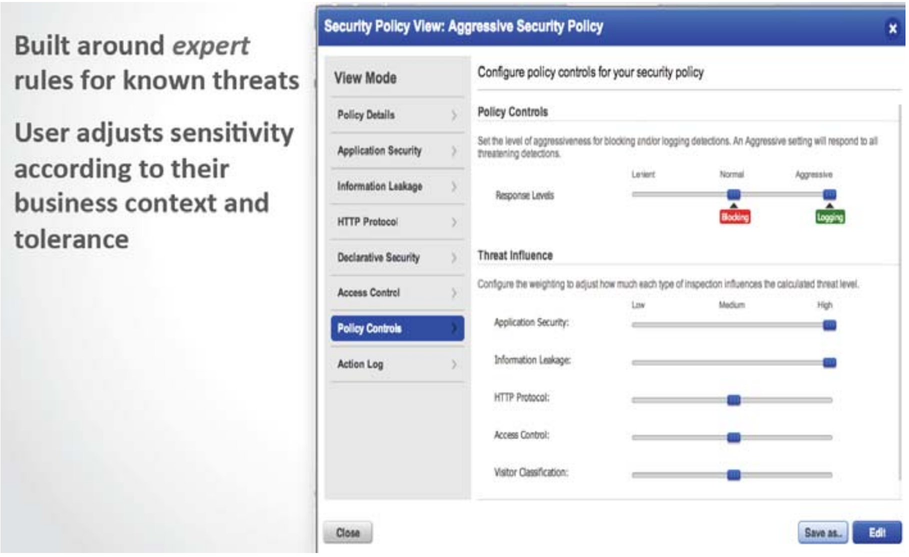


Security technology stack and Qualys

• Metrics from Qualys enterprise portal
• Feed into the SIEM and Threat intelligence
GRC
Information & Event Mgmt
Data Security
Application Security
Host Security
Network Security
Physical Security
Identity, Entitlement, Access
Cryptography
• Pattern matching in Configuration compliance
• Web application scanning
• Browser Check
• Patch assessment
• Configuration compliance
• SSL Server test

Integrating Qualys into the Patch and Vulnerability Management Processes presentation at 4, attached hereto as Exhibit 18.

136. The ‘408 Accused Products use rules-based scanners and detect indictors of malware such as certificates, track expirations, and broken pages:



Built around *expert* rules for known threats

User adjusts sensitivity according to their business context and tolerance

Security Policy View: Aggressive Security Policy

Configure policy controls for your security policy

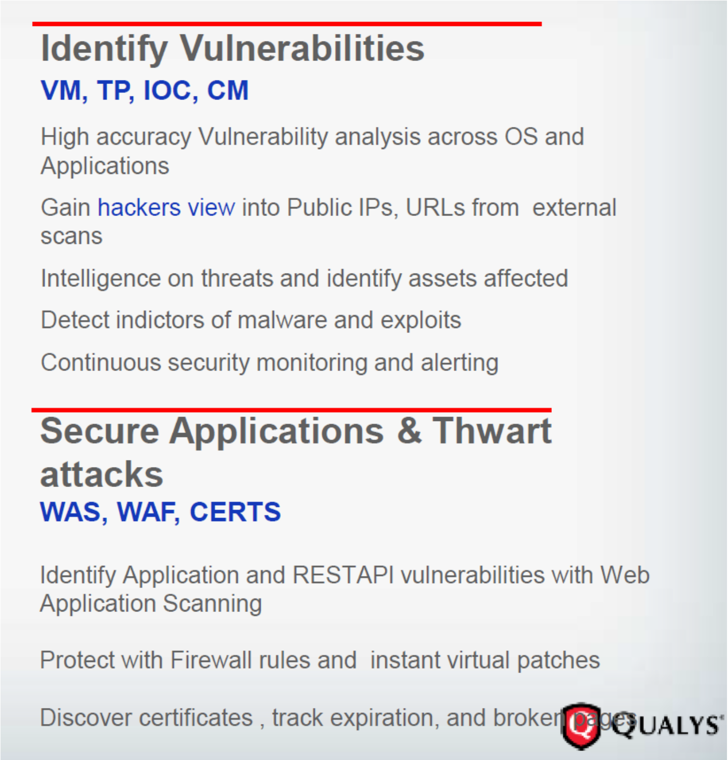
Policy Controls

Set the level of aggressiveness for blocking and/or logging detections. An Aggressive setting will respond to all threatening detections.

Threat Influence

Configure the weighting to adjust how much each type of inspection influences the calculated threat level.

QualysGuard Web Application Security presentation at 33, attached hereto as Exhibit 8.



Identify Vulnerabilities

VM, TP, IOC, CM

High accuracy Vulnerability analysis across OS and Applications

Gain hackers view into Public IPs, URLs from external scans

Intelligence on threats and identify assets affected

Detect indictors of malware and exploits

Continuous security monitoring and alerting

Secure Applications & Thwart attacks

WAS, WAF, CERTS

Identify Application and RESTAPI vulnerabilities with Web Application Scanning

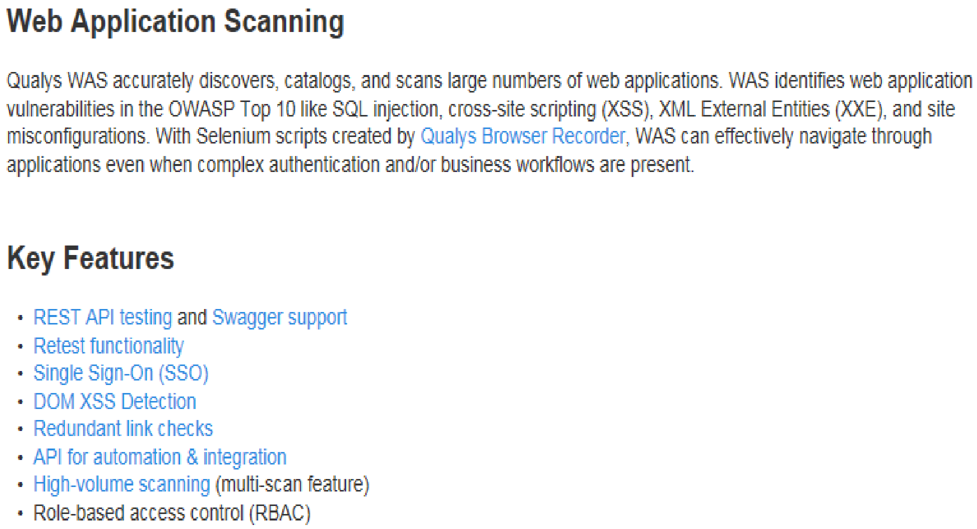
Protect with Firewall rules and instant virtual patches

Discover certificates , track expiration, and broken pages

Securing Public Cloud Infrastructure using Qualys presentation at 19, attached hereto as Exhibit 13.

137. The ‘408 Accused Products include a tokenizer, for identifying individual tokens within the incoming stream.

138. The ‘408 Accused Products scan, discover and catalog applications searching for portions of program code that are malicious according to token-based analyzer rules (such as SQL injection, cross-site scripting (XSS), XML External Entities (XXE) and site misconfigurations):



Web Application Scanning

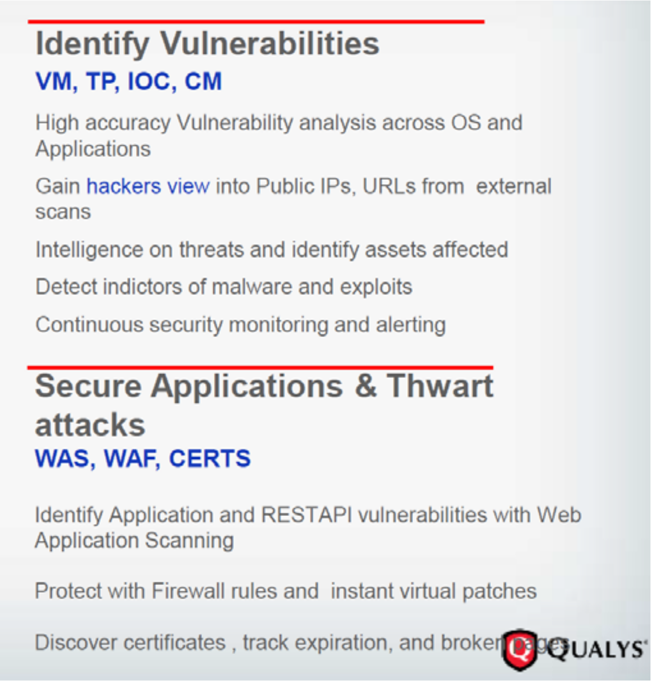
Qualys WAS accurately discovers, catalogs, and scans large numbers of web applications. WAS identifies web application vulnerabilities in the OWASP Top 10 like SQL injection, cross-site scripting (XSS), XML External Entities (XXE), and site misconfigurations. With Selenium scripts created by Qualys Browser Recorder, WAS can effectively navigate through applications even when complex authentication and/or business workflows are present.

Key Features

- REST API testing and Swagger support
- Retest functionality
- Single Sign-On (SSO)
- DOM XSS Detection
- Redundant link checks
- API for automation & integration
- High-volume scanning (multi-scan feature)
- Role-based access control (RBAC)

https://community.qualys.com/community/web-application-scanning, attached hereto as Exhibit 11.

139. The ‘408 Accused Products detect indictors of malware such as certificates, track expirations, and broken pages:



Identify Vulnerabilities

VM, TP, IOC, CM

High accuracy Vulnerability analysis across OS and Applications

Gain hackers view into Public IPs, URLs from external scans

Intelligence on threats and identify assets affected

Detect indictors of malware and exploits

Continuous security monitoring and alerting

Secure Applications & Thwart attacks

WAS, WAF, CERTS

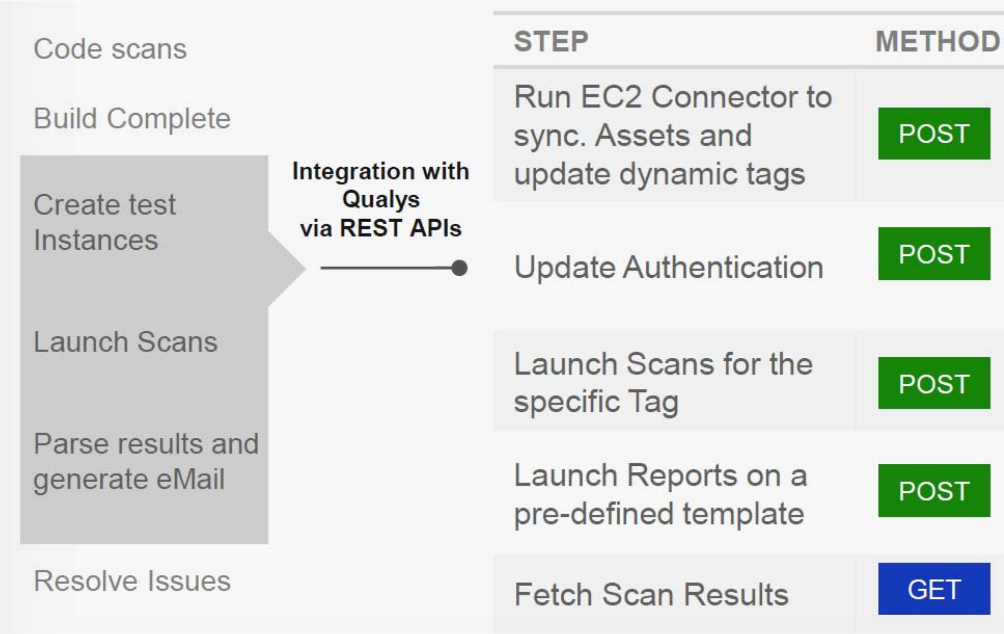
Identify Application and RESTAPI vulnerabilities with Web Application Scanning

Protect with Firewall rules and instant virtual patches

Discover certificates , track expiration, and broken pages

Securing Public Cloud Infrastructure using Qualys presentation at 19, attached hereto as Exhibit 13.

140. The '408 Accused Products include a parser, for dynamically building a parse tree while the receiver is receiving the incoming stream, where the parse tree nodes represent tokens and patterns in accordance with the parser rules accessed by the rules accessor.



Code scans

Build Complete

Create test Instances

Launch Scans

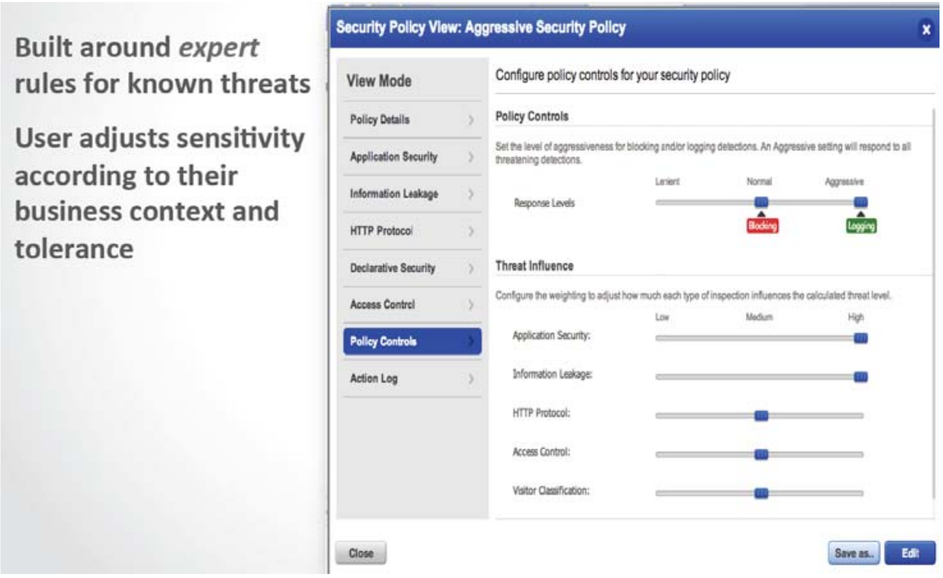
Parse results and generate eMail

Resolve Issues

Integration with Qualys via REST APIs

STEP	METHOD
Run EC2 Connector to sync. Assets and update dynamic tags	POST
Update Authentication	POST
Launch Scans for the specific Tag	POST
Launch Reports on a pre-defined template	POST
Fetch Scan Results	GET

Securing Public Cloud Infrastructure using Qualys presentation at 31, attached hereto as Exhibit 13.



Built around *expert* rules for known threats

User adjusts sensitivity according to their business context and tolerance

Security Policy View: Aggressive Security Policy

Configure policy controls for your security policy

Policy Controls

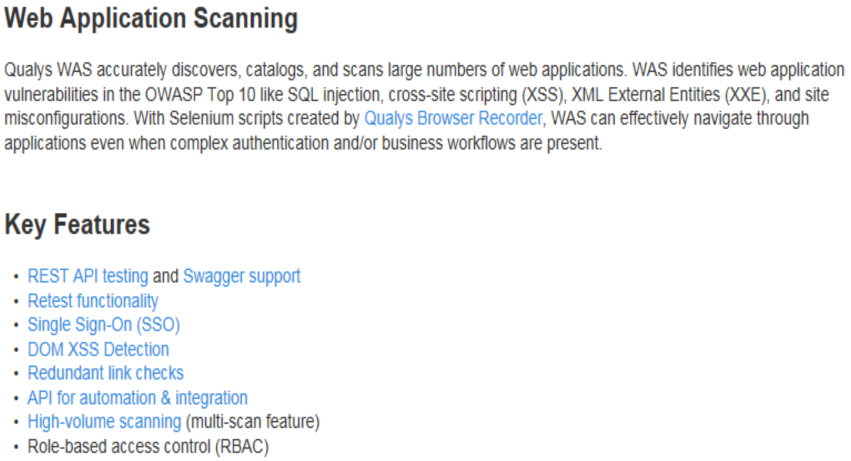
Set the level of aggressiveness for blocking and/or logging detections. An Aggressive setting will respond to all threatening detections.

Threat Influence

Configure the weighting to adjust how much each type of inspection influences the calculated threat level.

QualysGuard Web Application Security presentation at 33, attached hereto as Exhibit 8.

141. The '408 Accused Products scan, discover and catalog applications searching for portions of program code that are malicious according to analyzer rules (such as SQL injection, cross-site scripting (XSS), XML External Entities (XXE) and site misconfigurations):



Web Application Scanning

Qualys WAS accurately discovers, catalogs, and scans large numbers of web applications. WAS identifies web application vulnerabilities in the OWASP Top 10 like SQL injection, cross-site scripting (XSS), XML External Entities (XXE), and site misconfigurations. With Selenium scripts created by Qualys Browser Recorder, WAS can effectively navigate through applications even when complex authentication and/or business workflows are present.

Key Features

- REST API testing and Swagger support
- Retest functionality
- Single Sign-On (SSO)
- DOM XSS Detection
- Redundant link checks
- API for automation & integration
- High-volume scanning (multi-scan feature)
- Role-based access control (RBAC)

https://community.qualys.com/community/web-application-scanning, attached hereto as Exhibit 11.

142. The '408 Accused Products include an analyzer, for dynamically detecting, while the parser is dynamically building the parse tree, combinations of nodes in the parse tree which are indicators of potential exploits, based on the analyzer rules.

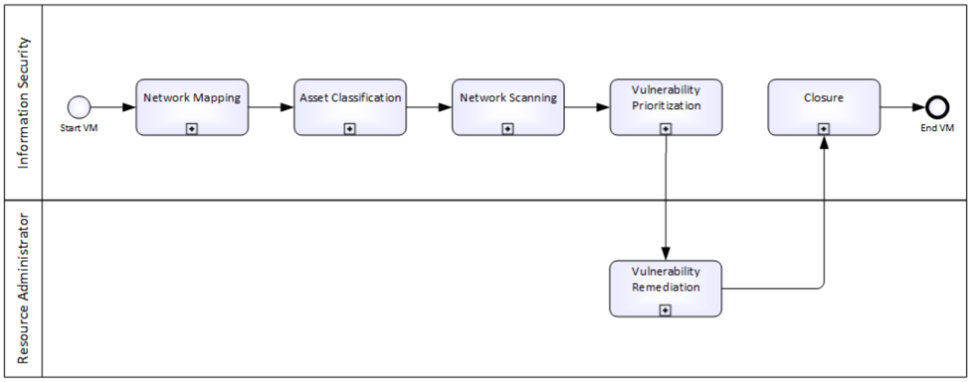
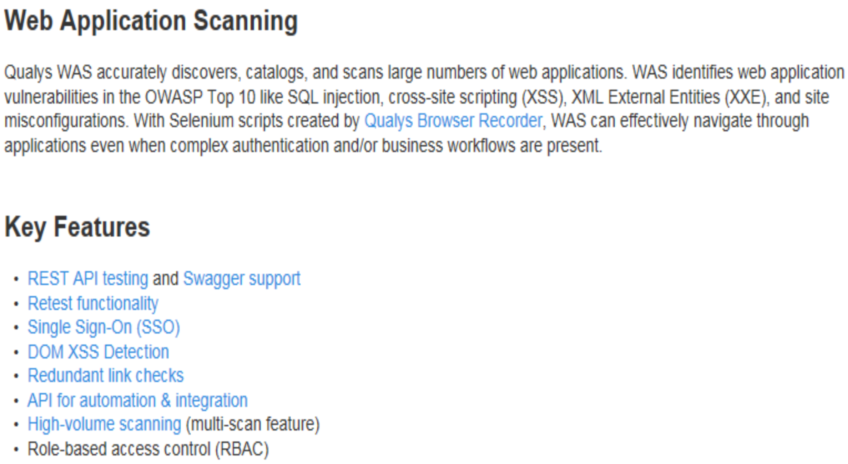


Figure 1: Vulnerability management process

https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.

143. The '408 Accused Products scan, discover and catalog applications searching for portions of program code that are malicious according to analyzer rules (such as SQL injection, cross-site scripting (XSS), XML External Entities (XXE) and site misconfigurations):



Web Application Scanning

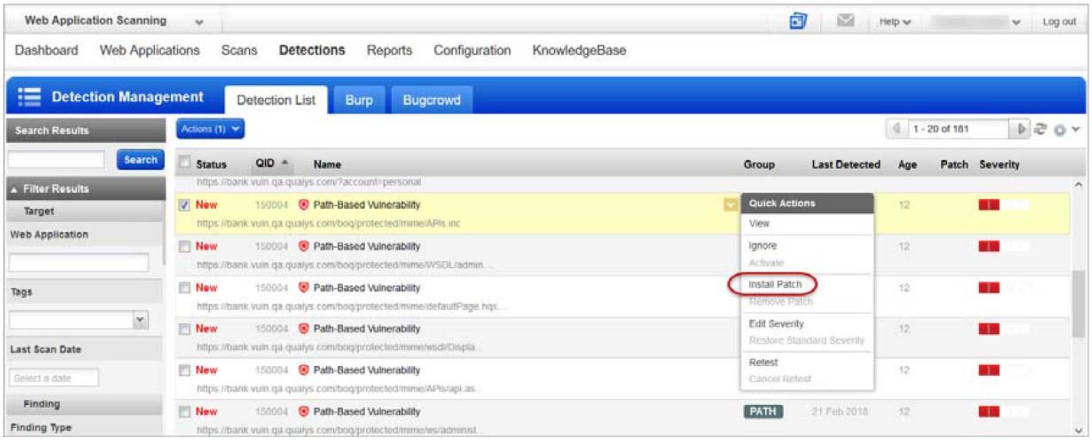
Qualys WAS accurately discovers, catalogs, and scans large numbers of web applications. WAS identifies web application vulnerabilities in the OWASP Top 10 like SQL injection, cross-site scripting (XSS), XML External Entities (XXE), and site misconfigurations. With Selenium scripts created by Qualys Browser Recorder, WAS can effectively navigate through applications even when complex authentication and/or business workflows are present.

Key Features

- REST API testing and Swagger support
- Retest functionality
- Single Sign-On (SSO)
- DOM XSS Detection
- Redundant link checks
- API for automation & integration
- High-volume scanning (multi-scan feature)
- Role-based access control (RBAC)

https://community.qualys.com/community/web-application-scanning, attached hereto as Exhibit 11.

144. Virtual patching is the process of creating and implementing a temporary policy that is used to mitigate exploitation risks associated with the discovery of new security vulnerabilities. The '408 Accused Products add virtual patches upon vulnerability detection:

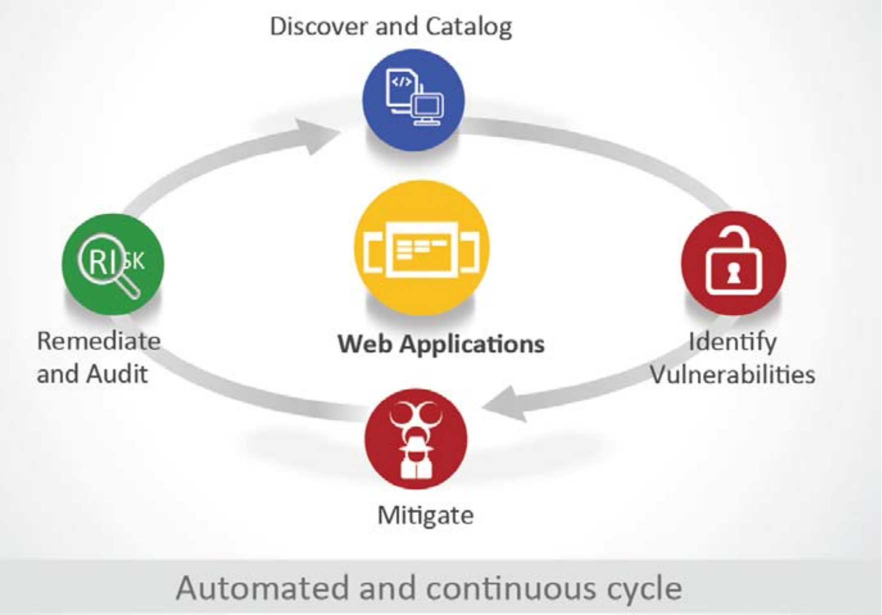


Status	QID	Name	Group	Last Detected	Age	Patch	Severity
		https://bank.vuln.qa.qualys.com/?account=personal					
☑ New	150004	Path-Based Vulnerability https://bank.vuln.qa.qualys.com/boq/protected/mime/APIs.inc			12		
□ New	150004	Path-Based Vulnerability https://bank.vuln.qa.qualys.com/boq/protected/mime/WSDL/admin...			12		
□ New	150004	Path-Based Vulnerability https://bank.vuln.qa.qualys.com/boq/protected/mime/defaultPage.hqx...			12		
□ New	150004	Path-Based Vulnerability https://bank.vuln.qa.qualys.com/boq/protected/mime/wsdl/Displa...			12		
□ New	150004	Path-Based Vulnerability https://bank.vuln.qa.qualys.com/boq/protected/mime/APIs/api.as...			12		
□ New	150004	Path-Based Vulnerability https://bank.vuln.qa.qualys.com/boq/protected/mime/ws/administ...	PATH	21 Feb 2018	12		

Qualys Web Application Firewall Getting Started Guide at 27, attached hereto as Exhibit 20.

145. The '408 Accused Products include a notifier, stored on the medium and executed by the computer, operatively coupled to said scanner instantiator for indicating the presence of potential exploits within the incoming stream, based on the results from the analyzer.

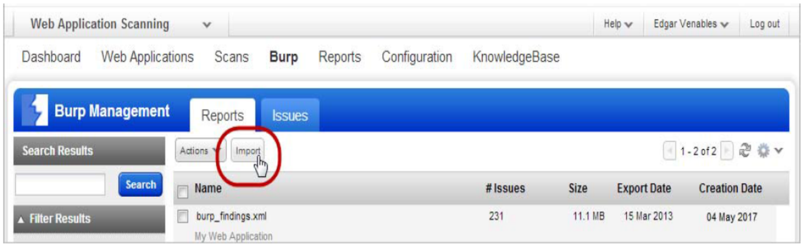
146. The '408 Accused Products perform continuous asset discovery by receiving incoming content and indicating the presence of potential exploits:



QualysGuard Web Application Security presentation at 5, attached hereto as Exhibit 8.

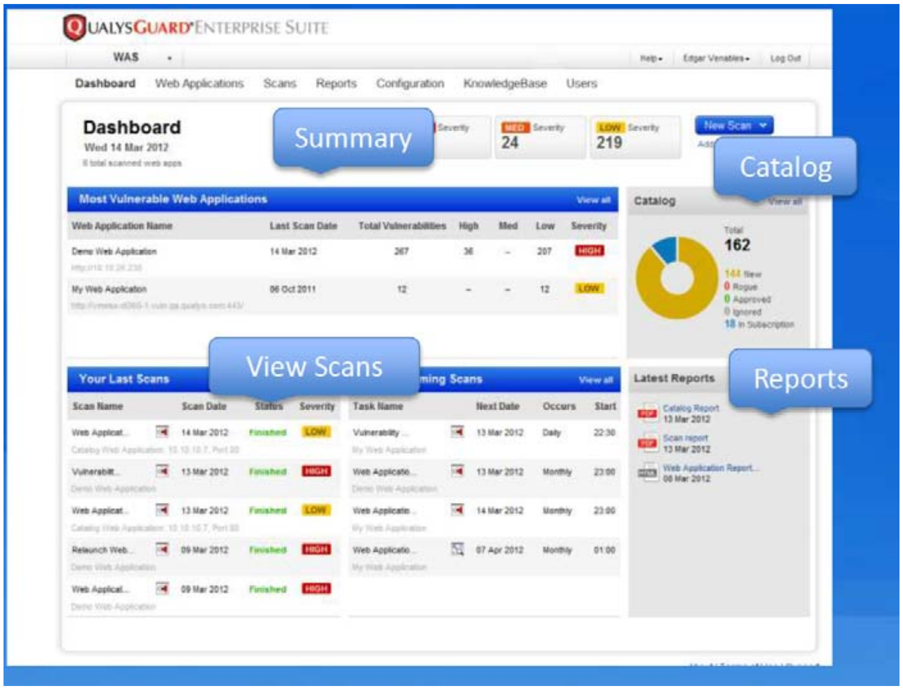
The Burp Management feature gives you a way to store the findings discovered by the Burp Suite scanner with those discovered by WAS and share this information with multiple users. To learn more refer to this blog article at the Qualys Community. (This feature is not available to Express Lite users.)

To get started click the Burp option on the top menu and go to Burp > Reports, then click Import and we'll walk you through the steps. Your issues list shows imported Burp issues.



	Name	# Issues	Size	Export Date	Creation Date
□	burp_findings.xml My Web Application	231	11.1 MB	15 Mar 2013	04 May 2017

Qualys Web Application Scanning Getting Started Guide Version 6.0.1 at 4, attached hereto as Exhibit 15.



Most Vulnerable Web Applications

Web Application Name	Last Scan Date	Total Vulnerabilities	High	Med	Low	Severity
Demo Web Application	14 Mar 2012	267	36	-	207	HIGH
My Web Application	06 Oct 2011	12	-	-	12	LOW

Your Last Scans

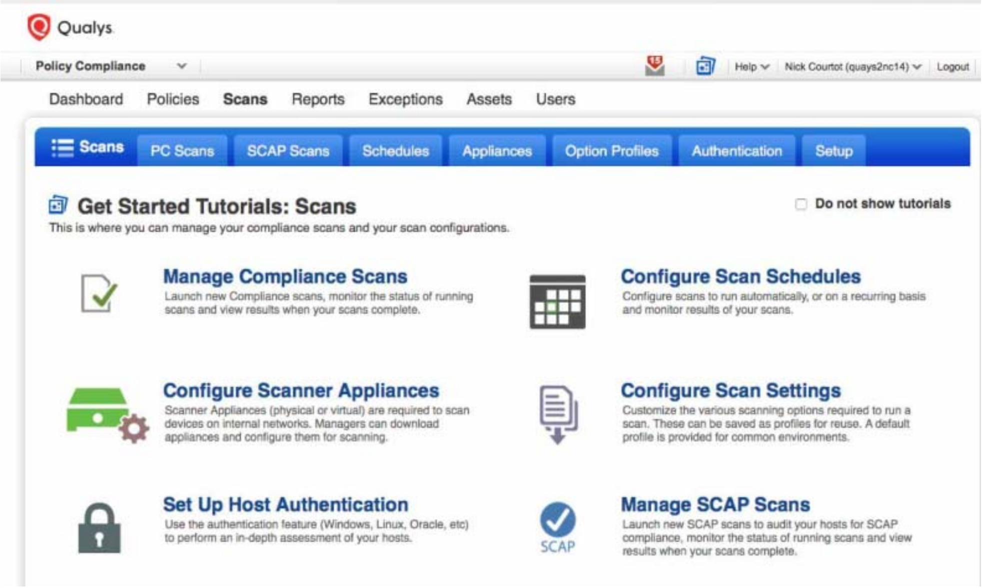
Scan Name	Scan Date	Status	Severity
Web Applicat... Catalog Web Application: 10.10.10.7, Port 80	14 Mar 2012	Finished	LOW
Vulnerabil... Demo Web Application	13 Mar 2012	Finished	HIGH
Web Applicat... Catalog Web Application: 10.10.10.7, Port 80	13 Mar 2012	Finished	LOW
Relaunch Web... Demo Web Application	09 Mar 2012	Finished	HIGH
Web Applicat... Demo Web Application	09 Mar 2012	Finished	HIGH

ming Scans

Task Name	Next Date	Occurs	Start
Vulnerability ... My Web Application	13 Mar 2012	Daily	22:30
Web Applicatio... Demo Web Application	13 Mar 2012	Monthly	23:00
Web Applicatio... My Web Application	14 Mar 2012	Monthly	23:00
Web Applicatio... My Web Application	07 Apr 2012	Monthly	01:00

QualysGuard InfoDay 2014 presentation at 29, attached hereto as Exhibit 12.

147. The '408 Accused Products use Policy Compliance to evaluate content profiles, and the results are saved as entries in the policy index.



Get Started Tutorials: Scans

This is where you can manage your compliance scans and your scan configurations.

□ Do not show tutorials

Manage Compliance Scans
Launch new Compliance scans, monitor the status of running scans and view results when your scans complete.

Configure Scan Schedules
Configure scans to run automatically, or on a recurring basis and monitor results of your scans.

Configure Scanner Appliances
Scanner Appliances (physical or virtual) are required to scan devices on internal networks. Managers can download appliances and configure them for scanning.

Configure Scan Settings
Customize the various scanning options required to run a scan. These can be saved as profiles for reuse. A default profile is provided for common environments.

Set Up Host Authentication
Use the authentication feature (Windows, Linux, Oracle, etc) to perform an in-depth assessment of your hosts.

Manage SCAP Scans
Launch new SCAP scans to audit your hosts for SCAP compliance, monitor the status of running scans and view results when your scans complete.

https://www.qualys.com/apps/policy-compliance/, attached hereto as Exhibit 17.

148. Defendant's 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 Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendant compete in the security software space, and Finjan is actively engaged in licensing its patent portfolio. Defendant's 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.

149. Defendant has been long-aware of Finjan's patents, including the '408 Patent, and continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendant for nearly three years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that its products infringe Finjan's patents, on information and belief Defendant made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing technology into additional

products, such as those identified in this complaint. All of these actions demonstrate Defendant's blatant and egregious disregard for Finjan's patent rights.

150. Despite its knowledge of Finjan's patent portfolio and Asserted Patents, and its specific knowledge of its own infringement, Defendant continued to sell the '408 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 VIII
(Indirect Infringement of the '408 Patent pursuant to 35 U.S.C. § 271(b))

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

152. In addition to directly infringing the '408 Patent, Defendant knew or was willfully blind to the fact that it was 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 its customers to perform the steps of the method claims of the '408 Patent, either literally or under the doctrine of equivalents.

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

154. Defendant knowingly and actively aided and abetted the direct infringement of the '408 Patent by instructing and encouraging its 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.*, QualysGuard Web Application Security presentation,

attached hereto as Exhibit 8; https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10; https://community.qualys.com/community/web-application-scanning, attached hereto as Exhibit 11; QualysGuard InfoDay 2014 presentation, attached hereto as Exhibit 12; Securing Public Cloud Infrastructure using Qualys presentation, attached hereto as Exhibit 13; Qualys Web Application Scanning Getting Started Guide Version 6.0.1, attached hereto as Exhibit 15; https://www.qualys.com/apps/policy-compliance/, attached hereto as Exhibit 17; Integrating Qualys into the Patch and Vulnerability Management Processes presentation, attached hereto as Exhibit 18; Qualys Web Application Firewall Getting Started Guide at 27, attached hereto as Exhibit 20.

COUNT IX
(Direct Infringement of the '968 Patent pursuant to 35 U.S.C. § 271(a))

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

156. Defendant has infringed and continues to infringe Claims 1-38 of the '968 Patent in violation of 35 U.S.C. § 271(a).

157. Defendant's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

158. Defendant's acts of making, using, importing, selling, and offering for sale infringing products and services has been without the permission, consent, authorization or license of Finjan.

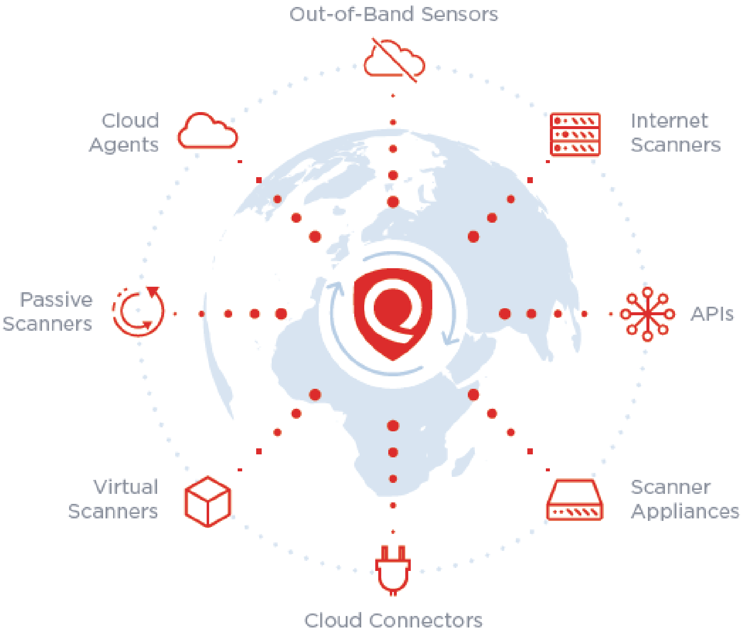
159. Defendant's infringement includes the manufacture, use, sale, importation and offer for sale of Defendant's products and services that utilize Vulnerability Management, Threat Protection, Continuous Monitoring, Indicators of Compromise, Container Security, Web App Firewall, Web App Scanning, and Compliance Monitoring, including Qualys Cloud Platform products (collectively, "the '968 Accused Products").

160. The '968 Accused Products embody the patented invention of the '968 Patent and infringe the '968 Patent because they make or use the patented system or perform the patented method

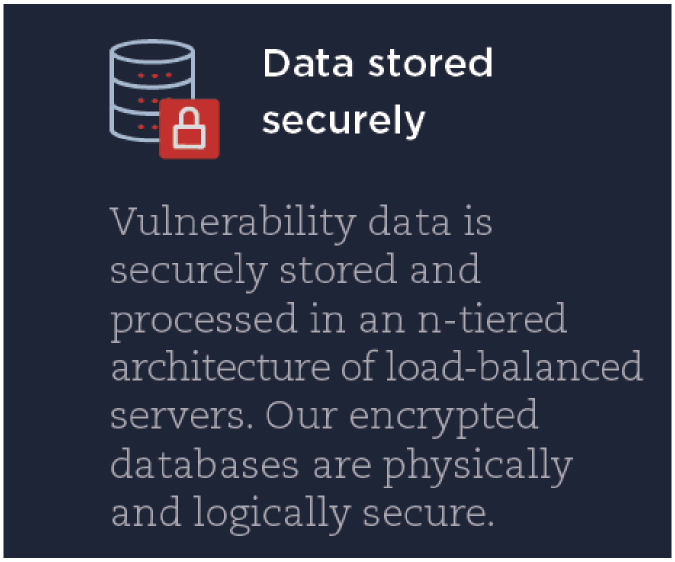
of rule-based scanning of web-based content for exploits written in different programming languages, by, for example, expressing the exploits as patterns of tokens or using a parse tree.

161. To the extent the '968 Accused Products use a system that includes modules, components or software owned by third parties, the '968 Accused Products still infringe the '968 Patent because Defendant is 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 Defendant's customers perform a step or steps of the patented method or the '968 Accused Products incorporate third parties' modules, components or software that perform one or more patented steps, Defendant's '968 Accused Products still infringe the '968 Patent because the '968 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.

162. The '968 Accused Products include policy-based cache managers that scan and securely store internet traffic:



Qualys Cloud Platform datasheet at 2, attached hereto as Exhibit 22.

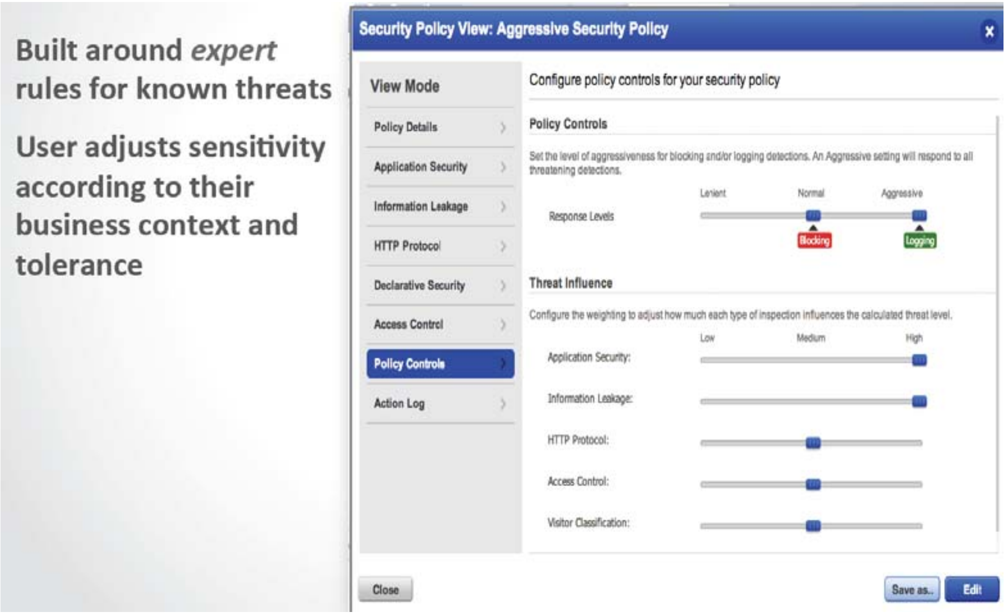


Data stored securely

Vulnerability data is securely stored and processed in an n-tiered architecture of load-balanced servers. Our encrypted databases are physically and logically secure.

Qualys Cloud Platform datasheet at 3, attached hereto as Exhibit 22.

163. The '968 Accused Products use rules for managing known threats that provide policy-based cache managers:



Built around *expert* rules for known threats

User adjusts sensitivity according to their business context and tolerance

Security Policy View: Aggressive Security Policy

Configure policy controls for your security policy

Policy Controls

Set the level of aggressiveness for blocking and/or logging detections. An Aggressive setting will respond to all threatening detections.

Response Levels: Lenient — Normal — Aggressive (Blocking: Normal; Logging: Aggressive)

Threat Influence

Configure the weighting to adjust how much each type of inspection influences the calculated threat level.

Low — Medium — High

Application Security: High

Information Leakage: High

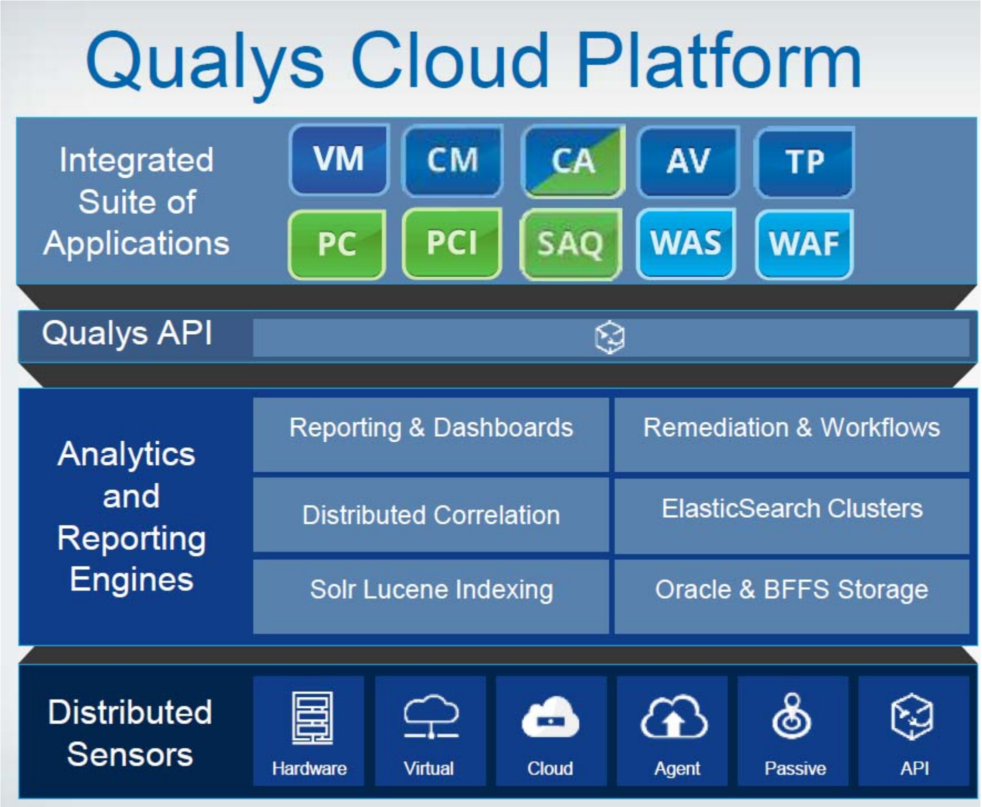
HTTP Protocol: Medium

Access Control: Medium

Visitor Classification: Medium

QualysGuard Web Application Security presentation at 33, attached hereto as Exhibit 8.

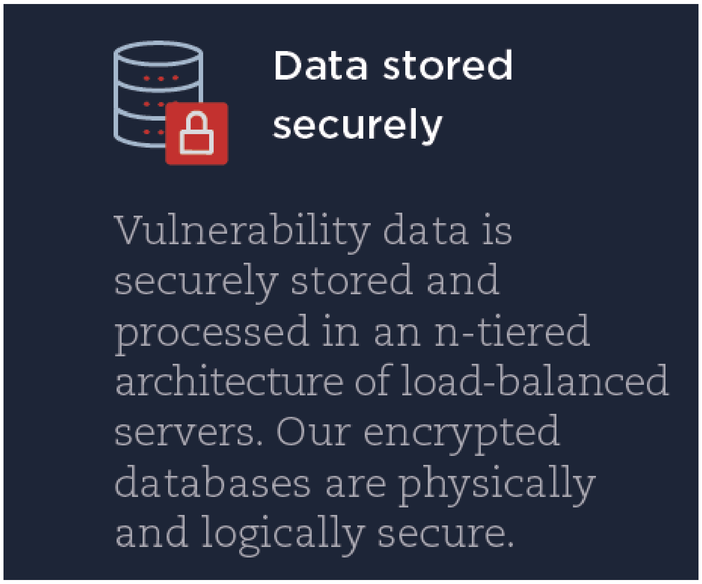
164. The '968 Accused Products also use web Application Filter (WAF) and Web Application Scanner (WAS) to apply and enforce rules and policies:



Securing Public Cloud Infrastructure using Qualys presentation at 12, attached hereto as Exhibit 13.

165. The ‘968 Accused Products include a memory storing a cache of digital content, a plurality of policies, and a policy index to the cache contents, the policy index including entries that relate cache content and policies by indicating cache content that is known to be allowable relative to a given policy, for each of a plurality of policies.

166. The ‘968 Accused Products securely store scanned data. Further, Qualys documents confirm that the stored data are physically and logically secured in an n-tiered architecture of load balanced servers:

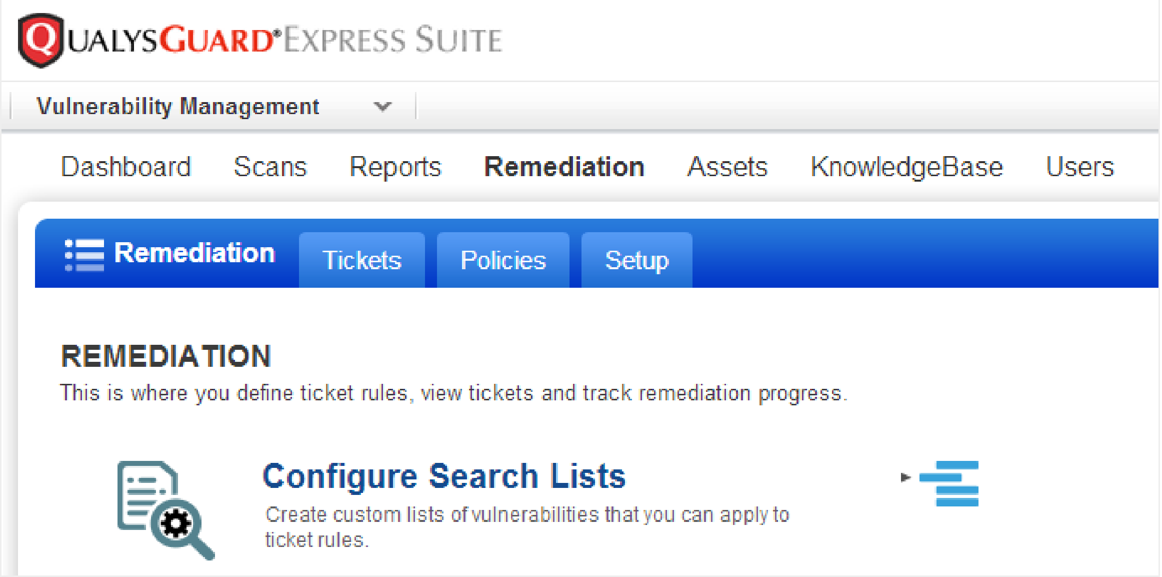


Data stored securely

Vulnerability data is securely stored and processed in an n-tiered architecture of load-balanced servers. Our encrypted databases are physically and logically secure.

Qualys Cloud Platform datasheet at 3, attached hereto as Exhibit 22.

167. The '968 Accused Products come with a policy-based ticketing module including entries that relate cached content and policies:



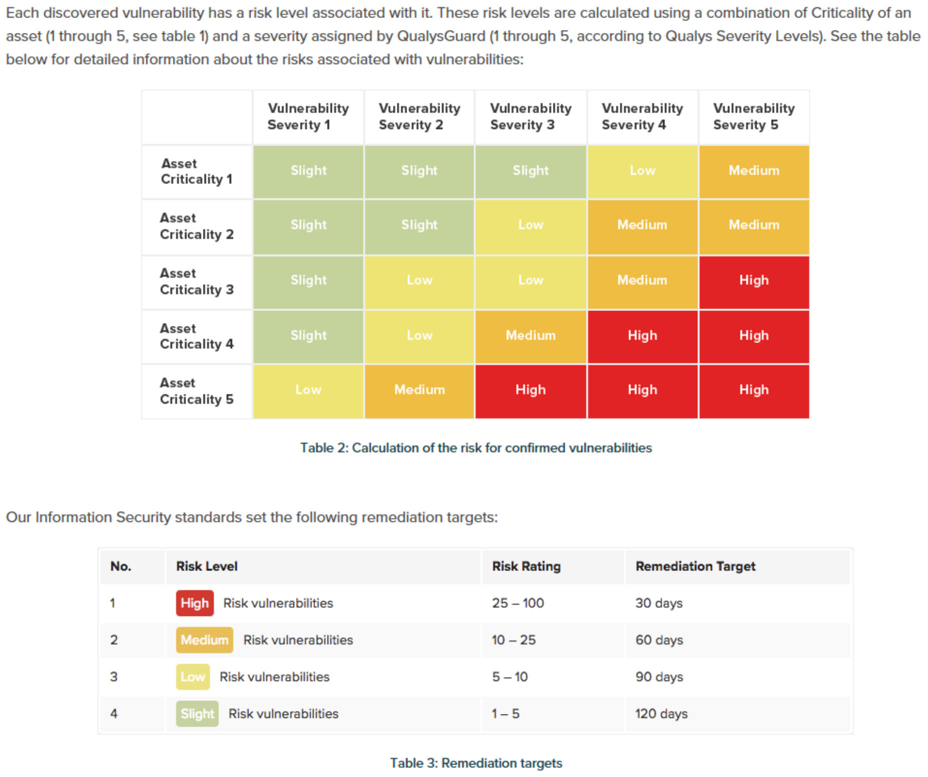
REMEDIATION

This is where you define ticket rules, view tickets and track remediation progress.

Configure Search Lists

Create custom lists of vulnerabilities that you can apply to ticket rules.

Figure 4: Qualys remediation module



Each discovered vulnerability has a risk level associated with it. These risk levels are calculated using a combination of Criticality of an asset (1 through 5, see table 1) and a severity assigned by QualysGuard (1 through 5, according to Qualys Severity Levels). See the table below for detailed information about the risks associated with vulnerabilities:

	Vulnerability Severity 1	Vulnerability Severity 2	Vulnerability Severity 3	Vulnerability Severity 4	Vulnerability Severity 5
Asset Criticality 1	Slight	Slight	Slight	Low	Medium
Asset Criticality 2	Slight	Slight	Low	Medium	Medium
Asset Criticality 3	Slight	Low	Low	Medium	High
Asset Criticality 4	Slight	Low	Medium	High	High
Asset Criticality 5	Low	Medium	High	High	High

Table 2: Calculation of the risk for confirmed vulnerabilities

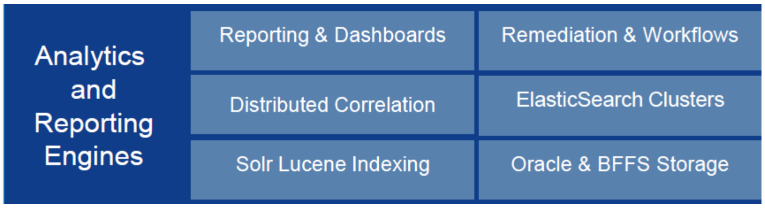
Our Information Security standards set the following remediation targets:

No.	Risk Level	Risk Rating	Remediation Target
1	High Risk vulnerabilities	25 – 100	30 days
2	Medium Risk vulnerabilities	10 – 25	60 days
3	Low Risk vulnerabilities	5 – 10	90 days
4	Slight Risk vulnerabilities	1 – 5	120 days

Table 3: Remediation targets

https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.

168. The '968 Accused Products investigate and remediate vulnerabilities using analytics and reporting engines:



Analytics and Reporting Engines

Reporting & Dashboards

Remediation & Workflows

Distributed Correlation

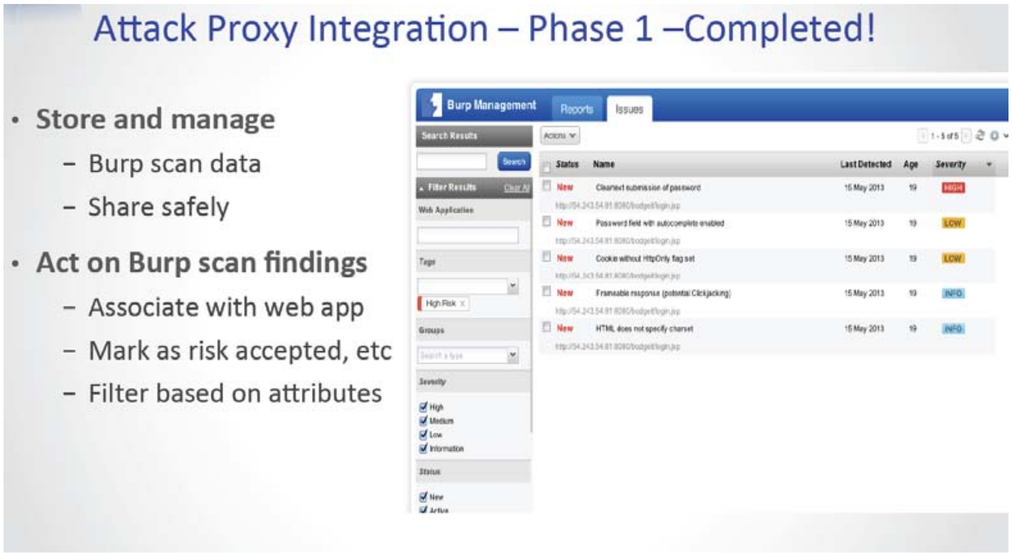
ElasticSearch Clusters

Solr Lucene Indexing

Oracle & BFFS Storage

Securing Public Cloud Infrastructure using Qualys presentation at 12, attached hereto as Exhibit 13.

169. The '968 Accused Products store policy index (high/low risk) data including entries that relate cache content and policies:



Attack Proxy Integration – Phase 1 –Completed!

- Store and manage
  - Burp scan data
  - Share safely
- Act on Burp scan findings
  - Associate with web app
  - Mark as risk accepted, etc
  - Filter based on attributes

	Status	Name	Last Detected	Age	Severity
□	New	Cleartext submission of password http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	HIGH
□	New	Password field with autocomplete enabled http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	LOW
□	New	Cookie without HttpOnly flag set http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	LOW
□	New	Framable response (potential Clickjacking) http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	INFO
□	New	HTML does not specify charset http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	INFO

QualysGuard Web Application Security presentation at 8, attached hereto as Exhibit 8.

170. The '968 Accused Products include a content scanner (e.g., network scanners), communicatively coupled with memory, for scanning a digital content received, to derive a corresponding content profile to protect against vulnerabilities and are coupled with memory in order to be processed:

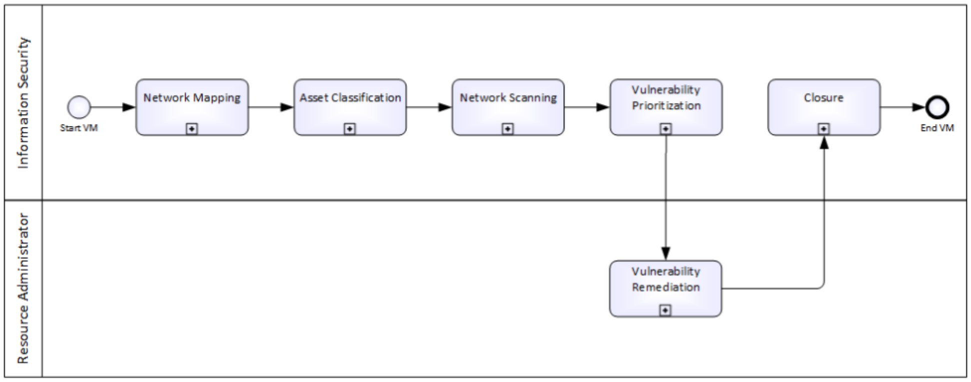
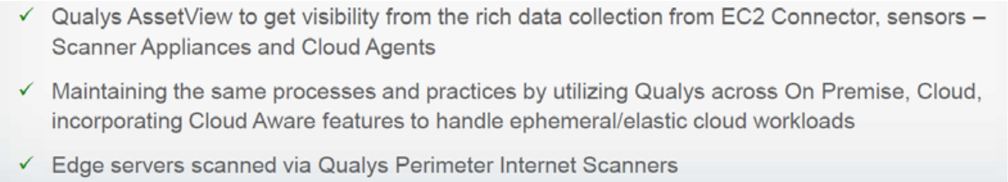
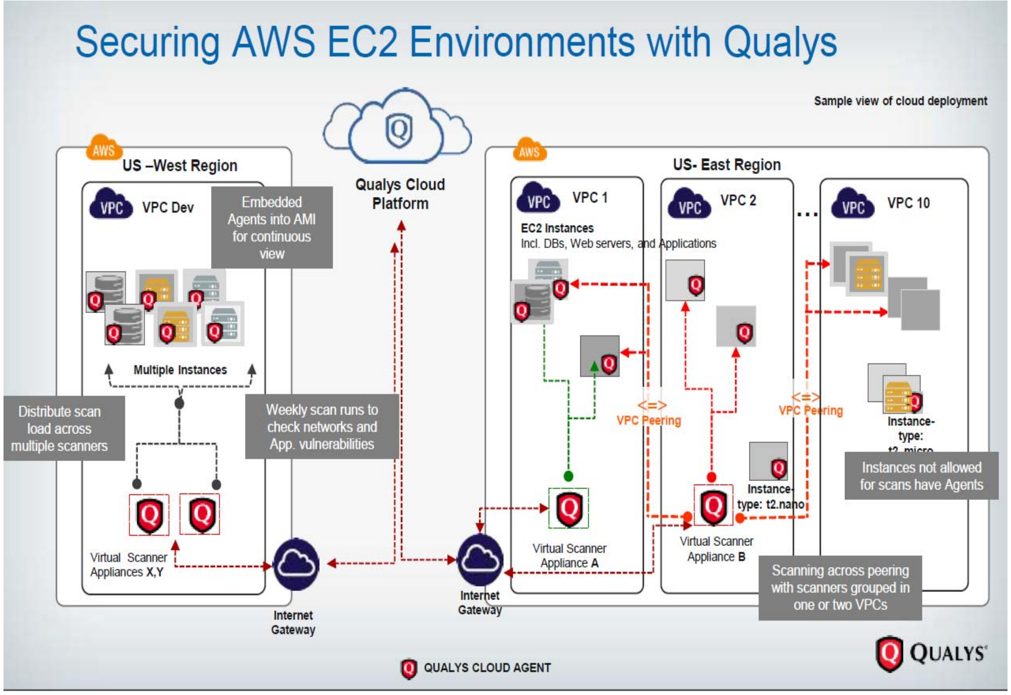


Figure 1: Vulnerability management process

https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.



- ✓ Qualys AssetView to get visibility from the rich data collection from EC2 Connector, sensors – Scanner Appliances and Cloud Agents
- ✓ Maintaining the same processes and practices by utilizing Qualys across On Premise, Cloud, incorporating Cloud Aware features to handle ephemeral/elastic cloud workloads
- ✓ Edge servers scanned via Qualys Perimeter Internet Scanners

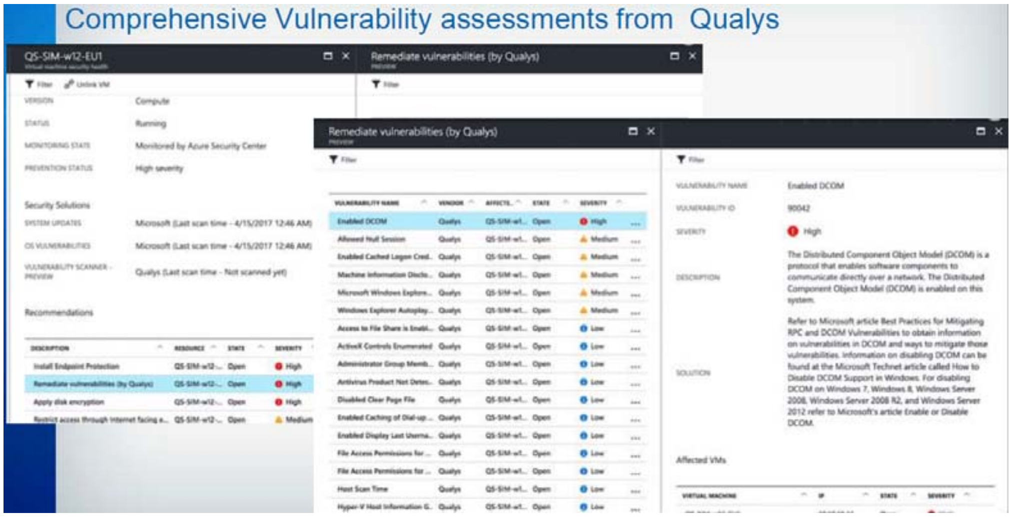


Securing AWS EC2 Environments with Qualys

Sample view of cloud deployment

AWS
US –West Region
VPC
VPC Dev
Embedded Agents into AMI for continuous view
Qualys Cloud Platform
Multiple Instances
Distribute scan load across multiple scanners
Weekly scan runs to check networks and App. vulnerabilities
Virtual Scanner Appliances X,Y
Internet Gateway
Internet Gateway
AWS
US- East Region
VPC
VPC 1
EC2 Instances
Incl. DBs, Web servers, and Applications
VPC
VPC 2
VPC
VPC 10
<=>
VPC Peering
<=>
VPC Peering
Instance-type: t2.micro
Instances not allowed for scans have Agents
Instance-type: t2.nano
Virtual Scanner Appliance A
Virtual Scanner Appliance B
Scanning across peering with scanners grouped in one or two VPCs
QUALYS CLOUD AGENT
QUALYS

Securing Public Cloud Infrastructure using Qualys presentation at 29, attached hereto as Exhibit 13.



Comprehensive Vulnerability assessments from Qualys

QS-SIM-w12-EU1

Virtual machine security health

VERSION	Compute
STATUS	Running
MONITORING STATE	Monitored by Azure Security Center
PREVENTION STATUS	High severity

Security Solutions

SYSTEM UPDATES	Microsoft (Last scan time - 4/15/2017 12:46 AM)
OS VULNERABILITIES	Microsoft (Last scan time - 4/15/2017 12:46 AM)
VULNERABILITY SCANNER - PREVIEW	Qualys (Last scan time - Not scanned yet)

Recommendations

DESCRIPTION	RESOURCE	STATE	SEVERITY
Install Endpoint Protection	QS-SIM-w12-...	Open	● High
Remediate vulnerabilities (by Qualys)	QS-SIM-w12-...	Open	● High
Apply disk encryption	QS-SIM-w12-...	Open	● High
Restrict access through Internet facing e...	QS-SIM-w12-...	Open	▲ Medium

Remediate vulnerabilities (by Qualys)

PREVIEW

Remediate vulnerabilities (by Qualys)

PREVIEW

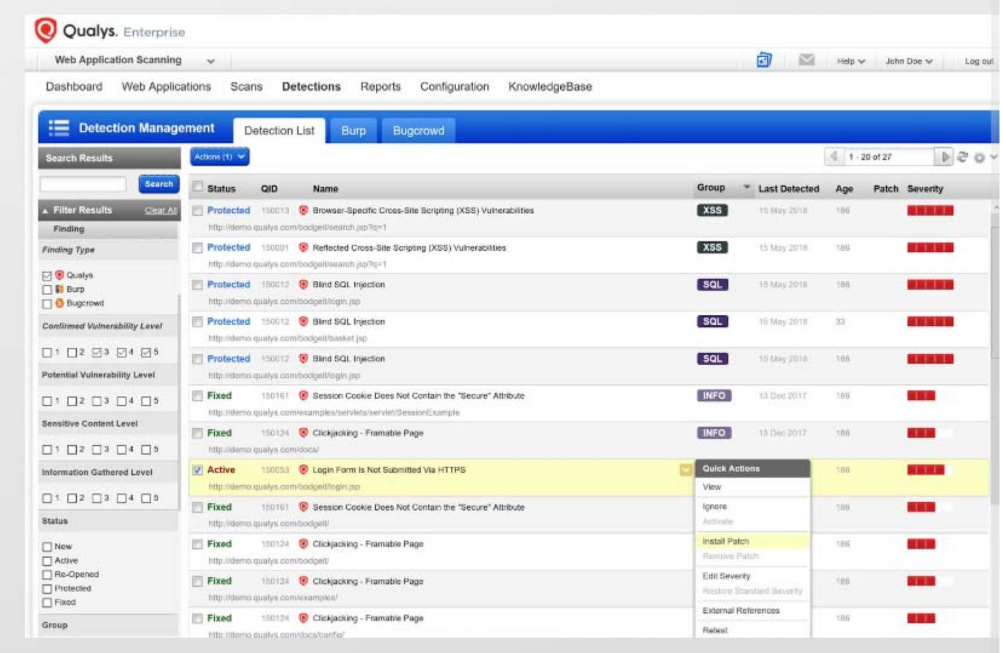
VULNERABILITY NAME	VENDOR	AFFECTE...	STATE	SEVERITY	
Enabled DCOM	Qualys	QS-SIM-w1...	Open	● High	...
Allowed Null Session	Qualys	QS-SIM-w1...	Open	▲ Medium	...
Enabled Cached Logon Cred...	Qualys	QS-SIM-w1...	Open	▲ Medium	...
Machine Information Disclo...	Qualys	QS-SIM-w1...	Open	▲ Medium	...
Microsoft Windows Explore...	Qualys	QS-SIM-w1...	Open	▲ Medium	...
Windows Explorer Autoplay...	Qualys	QS-SIM-w1...	Open	▲ Medium	...
Access to File Share is Enabl...	Qualys	QS-SIM-w1...	Open	● Low	...
ActiveX Controls Enumerated	Qualys	QS-SIM-w1...	Open	● Low	...
Administrator Group Memb...	Qualys	QS-SIM-w1...	Open	● Low	...
Antivirus Product Not Detec...	Qualys	QS-SIM-w1...	Open	● Low	...
Disabled Clear Page File	Qualys	QS-SIM-w1...	Open	● Low	...
Enabled Caching of Dial-up ...	Qualys	QS-SIM-w1...	Open	● Low	...
Enabled Display Last Userna...	Qualys	QS-SIM-w1...	Open	● Low	...
File Access Permissions for ...	Qualys	QS-SIM-w1...	Open	● Low	...
File Access Permissions for ...	Qualys	QS-SIM-w1...	Open	● Low	...
Host Scan Time	Qualys	QS-SIM-w1...	Open	● Low	...
Hyper-V Host Information G...	Qualys	QS-SIM-w1...	Open	● Low	...

VULNERABILITY NAME	Enabled DCOM
VULNERABILITY ID	90042
SEVERITY	● High
DESCRIPTION	The Distributed Component Object Model (DCOM) is a protocol that enables software components to communicate directly over a network. The Distributed Component Object Model (DCOM) is enabled on this system.
SOLUTION	Refer to Microsoft article Best Practices for Mitigating RPC and DCOM Vulnerabilities to obtain information on vulnerabilities in DCOM and ways to mitigate those vulnerabilities. Information on disabling DCOM can be found at the Microsoft Technet article called How to Disable DCOM Support in Windows. For disabling DCOM on Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 refer to Microsoft's article Enable or Disable DCOM.

Affected VMs

VIRTUAL MACHINE	IP	STATE	SEVERITY

Securing Public Cloud Infrastructure using Qualys presentation at 37, attached hereto as Exhibit 13.



Filter Results Clear All

Finding

Finding Type

☑ Qualys
□ Burp
□ Bugcrowd

Confirmed Vulnerability Level

□ 1 □ 2 ☑ 3 ☑ 4 ☑ 5

Potential Vulnerability Level

□ 1 □ 2 □ 3 □ 4 □ 5

Sensitive Content Level

□ 1 □ 2 □ 3 □ 4 □ 5

Information Gathered Level

□ 1 □ 2 □ 3 □ 4 □ 5

Status

□ New
□ Active
□ Re-Opened
□ Protected
□ Fixed

Group

	Status	QID	Name	Group	Last Detected	Age	Patch	Severity
□	Protected	150013	Browser-Specific Cross-Site Scripting (XSS) Vulnerabilities http://demo.qualys.com/bodgeit/search.jsp?q=1	XSS	15 May 2018	186		
□	Protected	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities http://demo.qualys.com/bodgeit/search.jsp?q=1	XSS	15 May 2018	186		
□	Protected	150012	Blind SQL Injection http://demo.qualys.com/bodgeit/login.jsp	SQL	15 May 2018	186		
□	Protected	150012	Blind SQL Injection http://demo.qualys.com/bodgeit/basket.jsp	SQL	15 May 2018	33		
□	Protected	150012	Blind SQL Injection http://demo.qualys.com/bodgeit/login.jsp	SQL	15 May 2018	186		
□	Fixed	150161	Session Cookie Does Not Contain the "Secure" Attribute http://demo.qualys.com/examples/servlets/servlet/SessionExample	INFO	13 Dec 2017	186		
□	Fixed	150124	Clickjacking - Framable Page http://demo.qualys.com/docs/	INFO	13 Dec 2017	186		
☑	Active	150053	Login Form Is Not Submitted Via HTTPS http://demo.qualys.com/bodgeit/login.jsp			186		
□	Fixed	150161	Session Cookie Does Not Contain the "Secure" Attribute http://demo.qualys.com/bodgeit/			186		
□	Fixed	150124	Clickjacking - Framable Page http://demo.qualys.com/bodgeit/			186		
□	Fixed	150124	Clickjacking - Framable Page http://demo.qualys.com/examples/			186		
□	Fixed	150124	Clickjacking - Framable Page http://demo.qualys.com/docs/config/			186		

https://www.qualys.com/apps/web-app-firewall/, attached hereto as Exhibit 16.

171. The '968 Accused Products include a content evaluator, communicatively coupled with memory, for determining whether a given digital content is allowable relative to a given policy, based on the content profile, the results of which are saved as entries in the policy index.

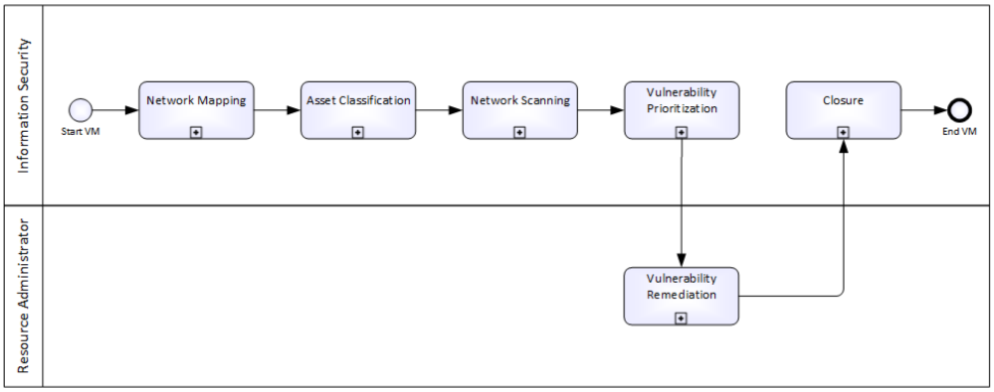
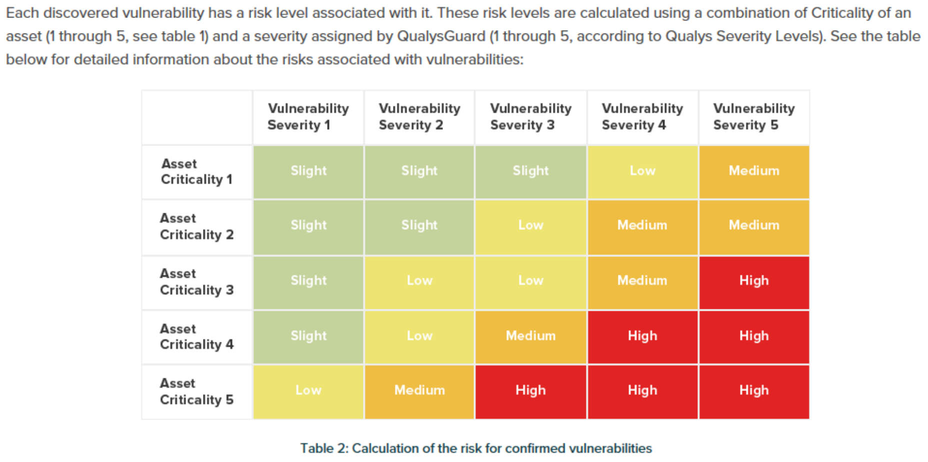


Figure 1: Vulnerability management process

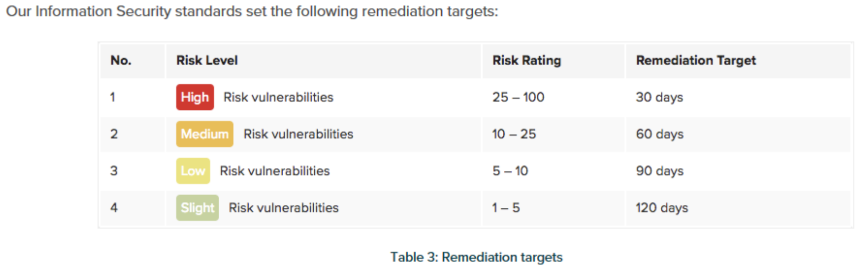
https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.



Each discovered vulnerability has a risk level associated with it. These risk levels are calculated using a combination of Criticality of an asset (1 through 5, see table 1) and a severity assigned by QualysGuard (1 through 5, according to Qualys Severity Levels). See the table below for detailed information about the risks associated with vulnerabilities:

	Vulnerability Severity 1	Vulnerability Severity 2	Vulnerability Severity 3	Vulnerability Severity 4	Vulnerability Severity 5
Asset Criticality 1	Slight	Slight	Slight	Low	Medium
Asset Criticality 2	Slight	Slight	Low	Medium	Medium
Asset Criticality 3	Slight	Low	Low	Medium	High
Asset Criticality 4	Slight	Low	Medium	High	High
Asset Criticality 5	Low	Medium	High	High	High

Table 2: Calculation of the risk for confirmed vulnerabilities



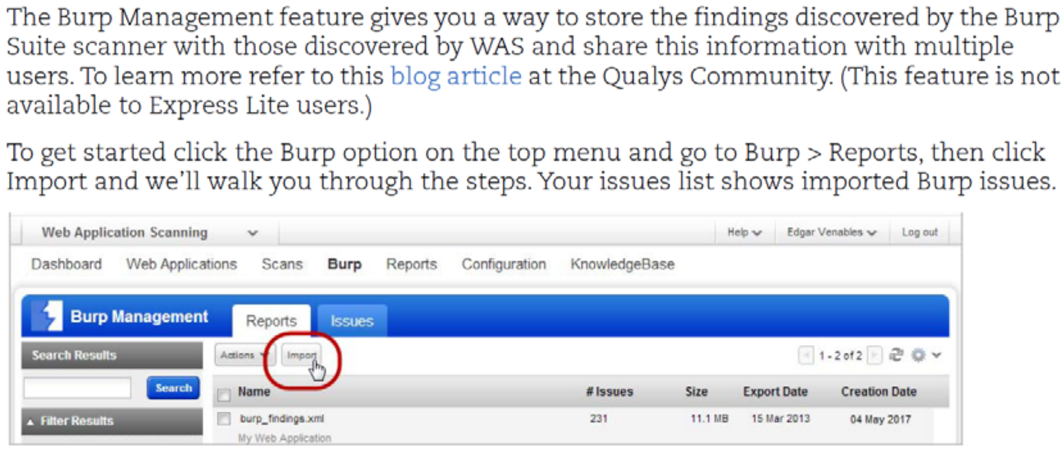
Our Information Security standards set the following remediation targets:

No.	Risk Level	Risk Rating	Remediation Target
1	High Risk vulnerabilities	25 – 100	30 days
2	Medium Risk vulnerabilities	10 – 25	60 days
3	Low Risk vulnerabilities	5 – 10	90 days
4	Slight Risk vulnerabilities	1 – 5	120 days

Table 3: Remediation targets

https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.

172. The '968 Accused Products evaluate information about system vulnerabilities relative to a given policy by using virtual scanner appliances and share it with multiple users:

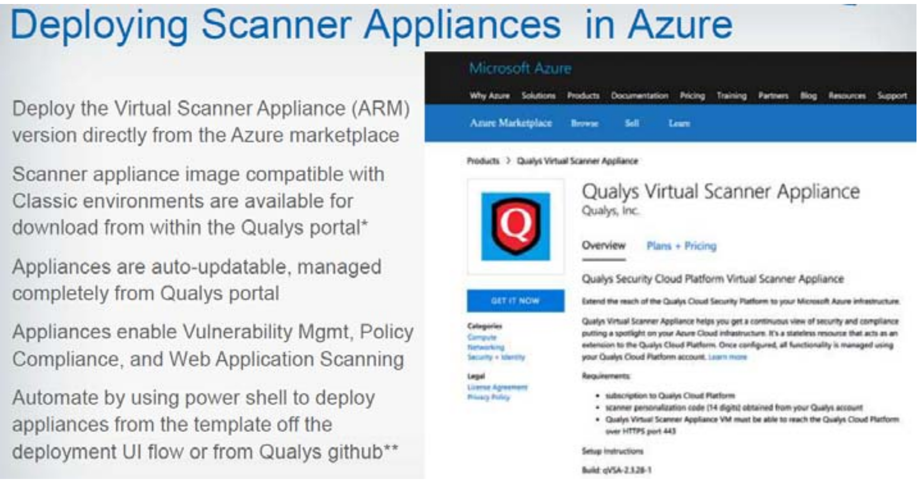


The Burp Management feature gives you a way to store the findings discovered by the Burp Suite scanner with those discovered by WAS and share this information with multiple users. To learn more refer to this blog article at the Qualys Community. (This feature is not available to Express Lite users.)

To get started click the Burp option on the top menu and go to Burp > Reports, then click Import and we'll walk you through the steps. Your issues list shows imported Burp issues.

Name	# Issues	Size	Export Date	Creation Date
burp_findings.xml My Web Application	231	11.1 MB	15 Mar 2013	04 May 2017

Qualys Web Application Scanning Getting Started Guide Version 6.0.1 at 20, attached hereto as Exhibit 15.



Deploying Scanner Appliances in Azure

- Deploy the Virtual Scanner Appliance (ARM) version directly from the Azure marketplace
- Scanner appliance image compatible with Classic environments are available for download from within the Qualys portal*
- Appliances are auto-updatable, managed completely from Qualys portal
- Appliances enable Vulnerability Mgmt, Policy Compliance, and Web Application Scanning
- Automate by using power shell to deploy appliances from the template off the deployment UI flow or from Qualys github**

Microsoft Azure
Why Azure Solutions Products Documentation Pricing Training Partners Blog Resources Support
Azure Marketplace Browse Sell Learn
Products > Qualys Virtual Scanner Appliance
GET IT NOW
Categories
Compute
Networking
Security + Identity
Legal
License Agreement
Privacy Policy
Overview Plans + Pricing

Qualys Virtual Scanner Appliance
Qualys, Inc.

Qualys Security Cloud Platform Virtual Scanner Appliance

Extend the reach of the Qualys Cloud Security Platform to your Microsoft Azure infrastructure.

Qualys Virtual Scanner Appliance helps you get a continuous view of security and compliance putting a spotlight on your Azure Cloud infrastructure. It's a stateless resource that acts as an extension to the Qualys Cloud Platform. Once configured, all functionality is managed using your Qualys Cloud Platform account. Learn more

Requirements:

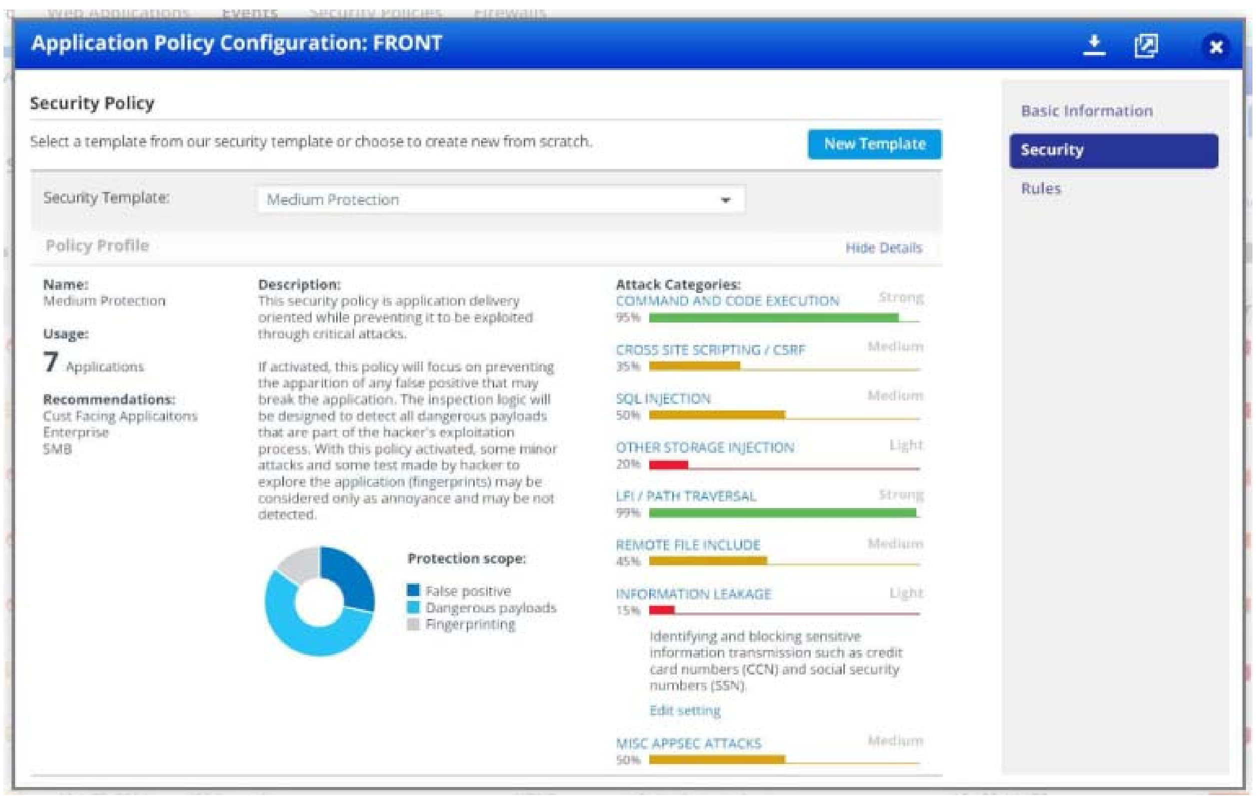
- subscription to Qualys Cloud Platform
- scanner personalization code (14 digits) obtained from your Qualys account
- Qualys Virtual Scanner Appliance VM must be able to reach the Qualys Cloud Platform over HTTPS port 443

Setup Instructions

Build: qVSA-2.3.28-1

Securing Public Cloud Infrastructure using Qualys presentation at 34, attached hereto as Exhibit 13.

173. The '968 Accused Products use Policy Compliance to compare application security profiles to the security policies, evaluate content profiles, and the results are saved as entries in the policy index:



Application Policy Configuration: FRONT

Security Policy

Select a template from our security template or choose to create new from scratch.

Security Template: Medium Protection

Policy Profile

Name:
Medium Protection

Usage:
7 Applications

Recommendations:
Cust Facing Applicaitons
Enterprise
SMB

Description:
This security policy is application delivery oriented while preventing it to be exploited through critical attacks.

If activated, this policy will focus on preventing the apparition of any false positive that may break the application. The inspection logic will be designed to detect all dangerous payloads that are part of the hacker's exploitation process. With this policy activated, some minor attacks and some test made by hacker to explore the application (fingerprints) may be considered only as annoyance and may be not detected.

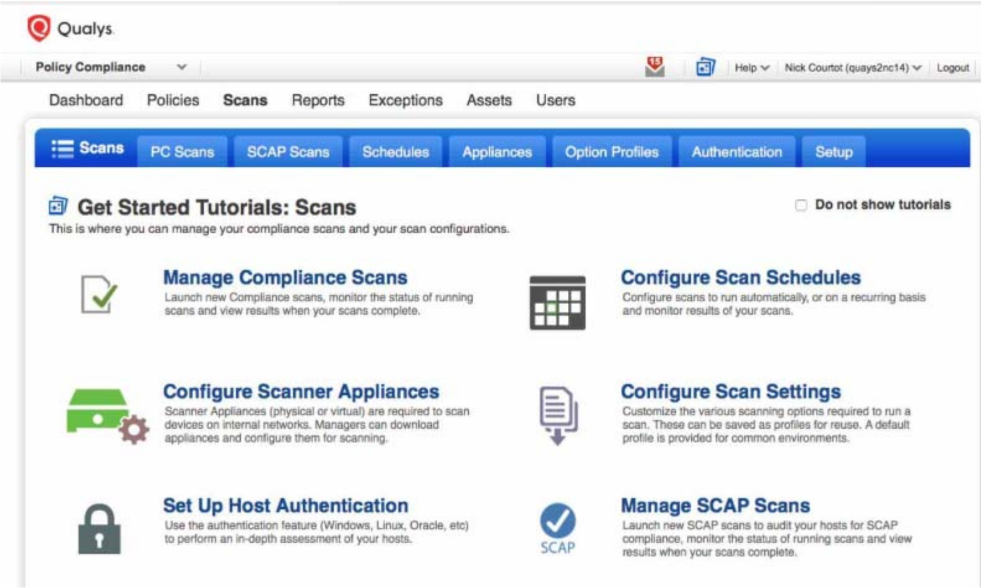
Protection scope:
- False positive
- Dangerous payloads
- Fingerprinting

Attack Categories:

COMMAND AND CODE EXECUTION	95%	Strong
CROSS SITE SCRIPTING / CSRF	35%	Medium
SQL INJECTION	50%	Medium
OTHER STORAGE INJECTION	20%	Light
LFI / PATH TRAVERSAL	99%	Strong
REMOTE FILE INCLUDE	45%	Medium
INFORMATION LEAKAGE	15%	Light
MISC APPSEC ATTACKS	50%	Medium

Identifying and blocking sensitive information transmission such as credit card numbers (CCN) and social security numbers (SSN).

https://www.qualys.com/apps/web-app-firewall/, attached hereto as Exhibit 16.



Get Started Tutorials: Scans

This is where you can manage your compliance scans and your scan configurations.

Manage Compliance Scans

Launch new Compliance scans, monitor the status of running scans and view results when your scans complete.

Configure Scan Schedules

Configure scans to run automatically, or on a recurring basis and monitor results of your scans.

Configure Scanner Appliances

Scanner Appliances (physical or virtual) are required to scan devices on internal networks. Managers can download appliances and configure them for scanning.

Configure Scan Settings

Customize the various scanning options required to run a scan. These can be saved as profiles for reuse. A default profile is provided for common environments.

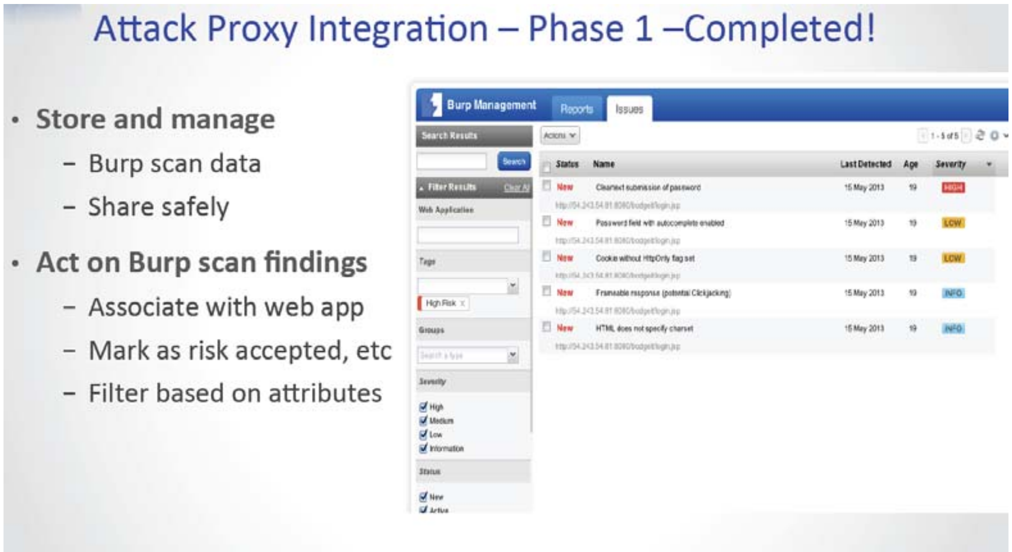
Set Up Host Authentication

Use the authentication feature (Windows, Linux, Oracle, etc) to perform an in-depth assessment of your hosts.

Manage SCAP Scans

Launch new SCAP scans to audit your hosts for SCAP compliance, monitor the status of running scans and view results when your scans complete.

https://www.qualys.com/apps/policy-compliance/, attached hereto as Exhibit 17.



Attack Proxy Integration – Phase 1 –Completed!

- Store and manage
  - Burp scan data
  - Share safely
- Act on Burp scan findings
  - Associate with web app
  - Mark as risk accepted, etc
  - Filter based on attributes

Status	Name	Last Detected	Age	Severity
New	Cleartext submission of password http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	HIGH
New	Password field with autocomplete enabled http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	LOW
New	Cookie without HttpOnly flag set http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	LOW
New	Frameable response (potential Clickjacking) http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	INFO
New	HTML does not specify charset http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	INFO

QualysGuard Web Application Security presentation at 8, attached hereto as Exhibit 8.

174. Defendant's infringement of the '968 Patent has injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty. Additionally, as a result of Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendant compete in the security software space, and Finjan is actively engaged in licensing its patent portfolio. Defendant's continued infringement of the '968

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.

175. Defendant has been long-aware of Finjan's patents, including the '968 Patent, and continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendant for nearly three years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that its products infringe Finjan's patents, including the '968 Patent, on information and belief Defendant made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendant's blatant and egregious disregard for Finjan's patent rights.

176. Despite its knowledge of Finjan's patent portfolio and Asserted Patents, and its specific knowledge of its own infringement, Defendant continued to sell the '968 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 '968 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
(Indirect Infringement of the '968 Patent pursuant to 35 U.S.C. § 271(b))

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

178. In addition to directly infringing the '968 Patent, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 13-22 and 25-31 of the '968 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its customers to perform the steps of the method claims of the '968 Patent, either literally or under the doctrine of equivalents.

179. Additionally, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 13-22 and 25-31 of the ‘968 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its developers to perform the steps of the method claims of the ‘968 Patent, either literally or under the doctrine of equivalents.

180. Defendant knowingly and actively aided and abetted the direct infringement of the ‘968 Patent by instructing and encouraging its customers and developers to use the ‘968 Accused Products. Such instructions and encouragement included advising third parties to use the ‘968 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the ‘968 Patent, and by advertising and promoting the use of the ‘968 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the ‘968 Accused Products in an infringing manner. *See, e.g*., QualysGuard Web Application Security presentation, attached hereto as Exhibit 8; https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10; Securing Public Cloud Infrastructure using Qualys presentation, attached hereto as Exhibit 13; Qualys Web Application Scanning Getting Started Guide Version 6.0.1, attached hereto as Exhibit 15; https://www.qualys.com/apps/web-app-firewall/, attached hereto as Exhibit 16; https://www.qualys.com/apps/policy-compliance/, attached hereto as Exhibit 17.

COUNT XI
(Direct Infringement of the ‘731 Patent pursuant to 35 U.S.C. § 271(a))

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

182. Defendant has infringed and continues to infringe Claims 1-22 of the ‘731 Patent in violation of 35 U.S.C. § 271(a).

183. Defendant’s infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

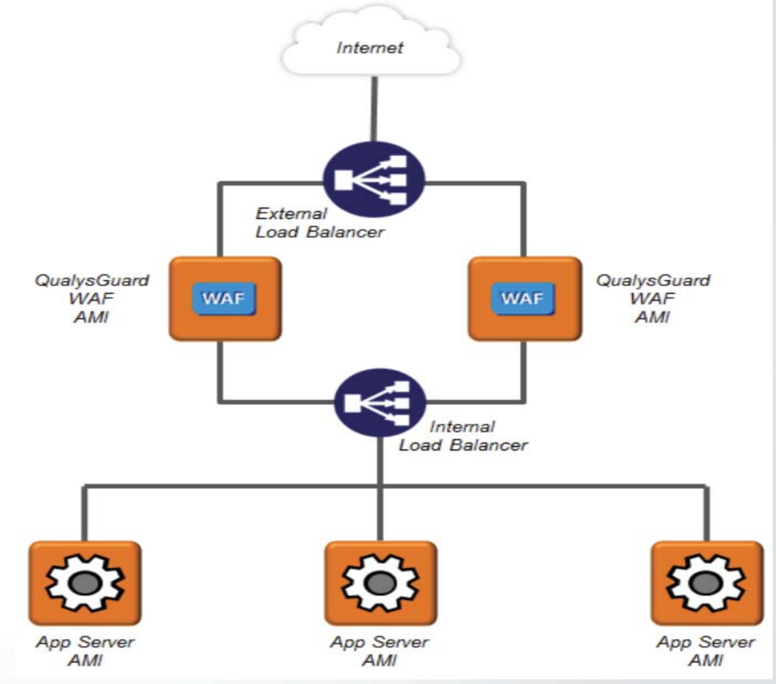
184. Defendant’s acts of making, using, importing, selling, and offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

185. Defendant's infringement includes the manufacture, use, sale, importation and offer for sale of Defendant's products and services that utilize Vulnerability Management, Threat Protection, Continuous Monitoring, Indicators of Compromise, Container Security, Web App Firewall, Web App Scanning, and Compliance Monitoring, including Qualys Cloud Platform products (collectively, "the '731 Accused Products").

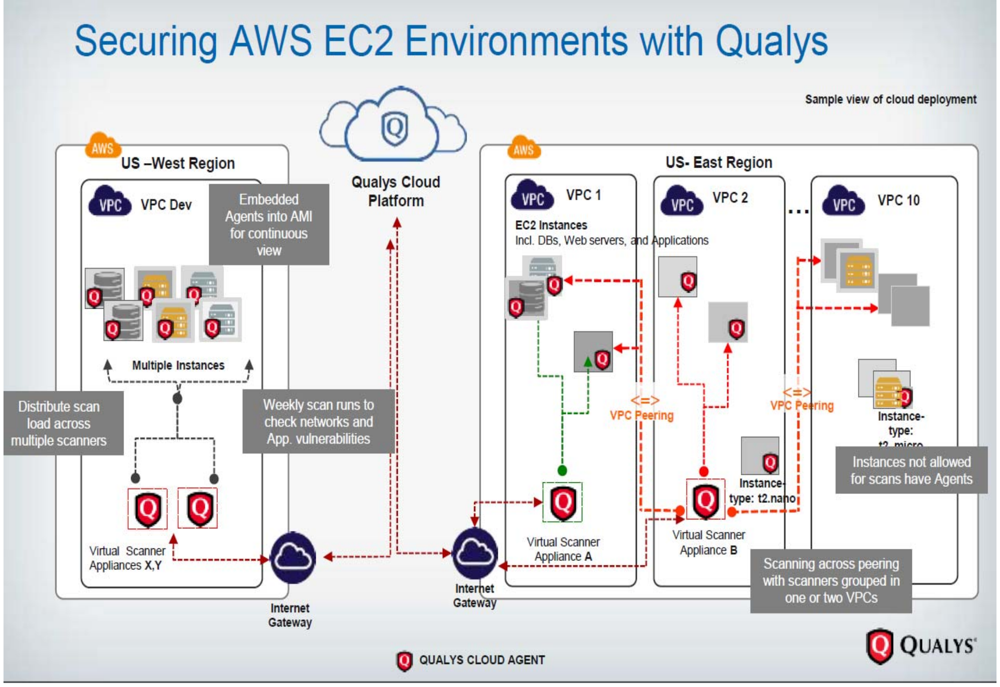
186. The '731 Accused Products embody the patented invention of the '731 Patent and infringe the '731 Patent because they make or use the patented system or perform the patented method of rule-based scanning of web-based content for exploits written in different programming languages, by, for example, expressing the exploits as patterns of tokens or using a parse tree.

187. To the extent the '731 Accused Products use a system that includes modules, components or software owned by third parties, the '731 Accused Products still infringe the '731 Patent because Defendant is 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 Defendant's customers perform a step or steps of the patented method or the '731 Accused Products incorporate third parties' modules, components or software that perform one or more patented steps, Defendant's '731 Accused Products still infringe the '731 Patent because the '731 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.

188. The '731 Accused Products are computer gateways for intranets of computers.



QualysGuard Web Application Security presentation at 30, attached hereto as Exhibit 8.

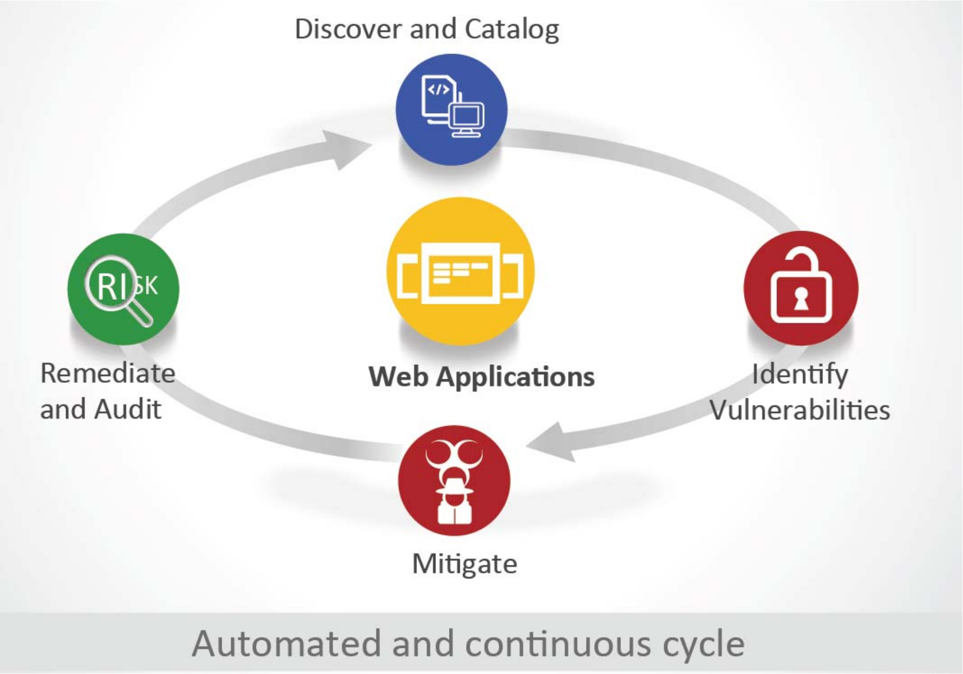


Securing AWS EC2 Environments with Qualys

Sample view of cloud deployment
AWS
US –West Region
VPC
VPC Dev
Embedded Agents into AMI for continuous view
Qualys Cloud Platform
Multiple Instances
Distribute scan load across multiple scanners
Weekly scan runs to check networks and App. vulnerabilities
Virtual Scanner Appliances X,Y
Internet Gateway
AWS
US- East Region
VPC
VPC 1
EC2 Instances
Incl. DBs, Web servers, and Applications
VPC
VPC 2
VPC
VPC 10
<=>
VPC Peering
<=>
VPC Peering
Instance-type: t2.micro
Instances not allowed for scans have Agents
Instance-type: t2.nano
Virtual Scanner Appliance A
Virtual Scanner Appliance B
Scanning across peering with scanners grouped in one or two VPCs
Internet Gateway
QUALYS CLOUD AGENT
QUALYS

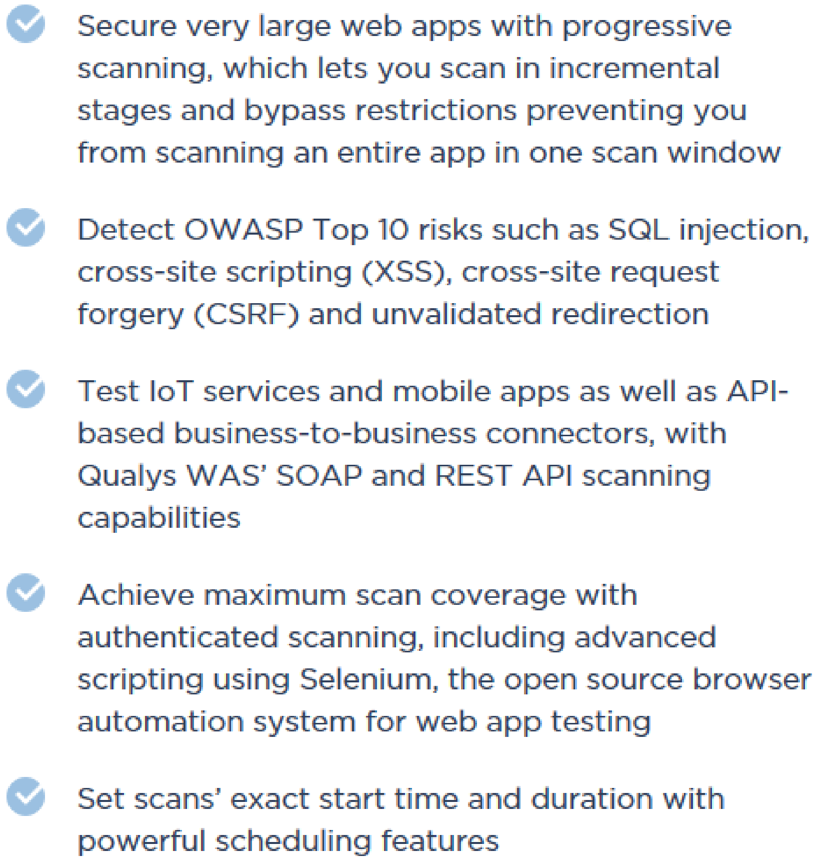
- ✓ Qualys AssetView to get visibility from the rich data collection from EC2 Connector, sensors – Scanner Appliances and Cloud Agents
- ✓ Maintaining the same processes and practices by utilizing Qualys across On Premise, Cloud, incorporating Cloud Aware features to handle ephemeral/elastic cloud workloads
- ✓ Edge servers scanned via Qualys Perimeter Internet Scanners

Securing Public Cloud Infrastructure using Qualys presentation at 28-29, attached hereto as Exhibit 13.



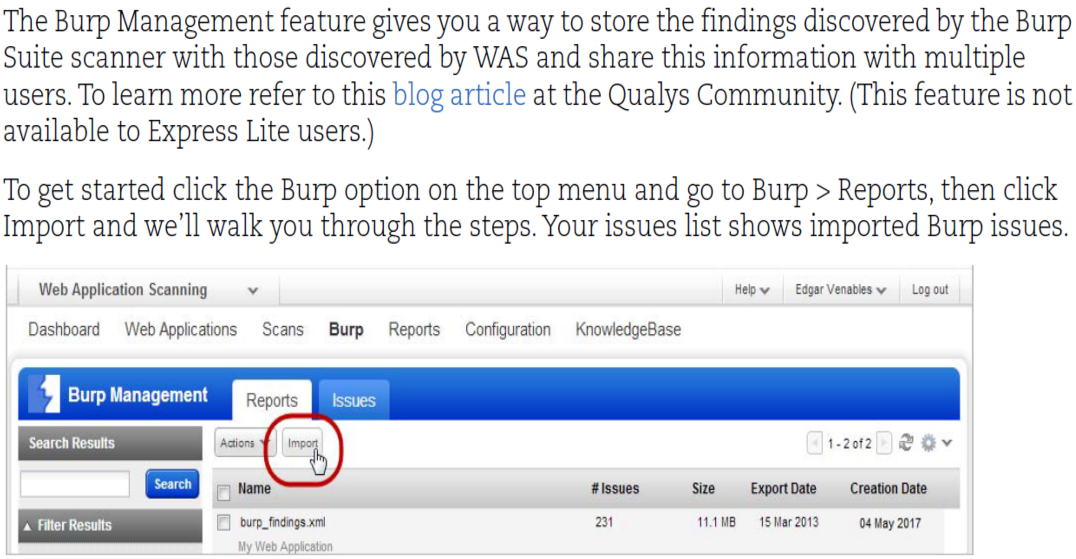
QualysGuard Web Application Security presentation at 5, attached hereto as Exhibit 8.

189. The ‘731 Accused Products include a scanner for scanning incoming files from the Internet and deriving security profiles for the incoming files, where each of the security profiles includes a list of computer commands that a corresponding incoming file is programmed to perform.



- ✓ Secure very large web apps with progressive scanning, which lets you scan in incremental stages and bypass restrictions preventing you from scanning an entire app in one scan window
- ✓ Detect OWASP Top 10 risks such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF) and unvalidated redirection
- ✓ Test IoT services and mobile apps as well as API-based business-to-business connectors, with Qualys WAS' SOAP and REST API scanning capabilities
- ✓ Achieve maximum scan coverage with authenticated scanning, including advanced scripting using Selenium, the open source browser automation system for web app testing
- ✓ Set scans' exact start time and duration with powerful scheduling features

https://www.qualys.com/apps/web-app-scanning/, attached hereto as Exhibit 19.



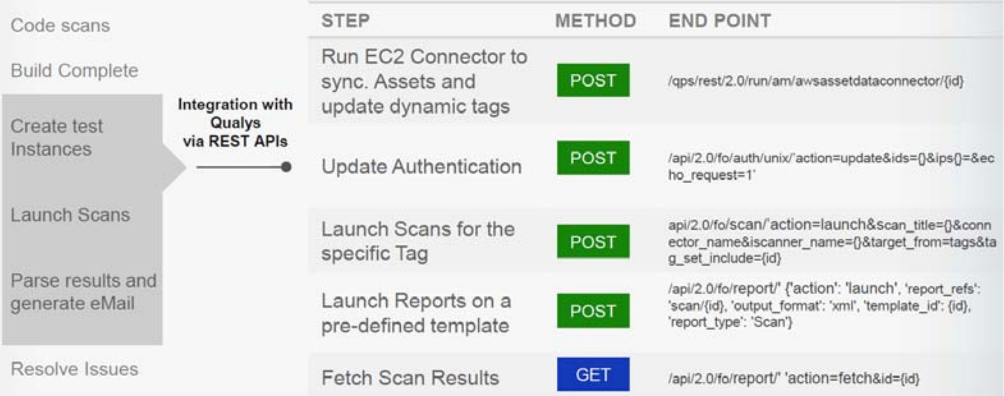
The Burp Management feature gives you a way to store the findings discovered by the Burp Suite scanner with those discovered by WAS and share this information with multiple users. To learn more refer to this blog article at the Qualys Community. (This feature is not available to Express Lite users.)

To get started click the Burp option on the top menu and go to Burp > Reports, then click Import and we'll walk you through the steps. Your issues list shows imported Burp issues.

□ Name	# Issues	Size	Export Date	Creation Date
□ burp_findings.xml My Web Application	231	11.1 MB	15 Mar 2013	04 May 2017

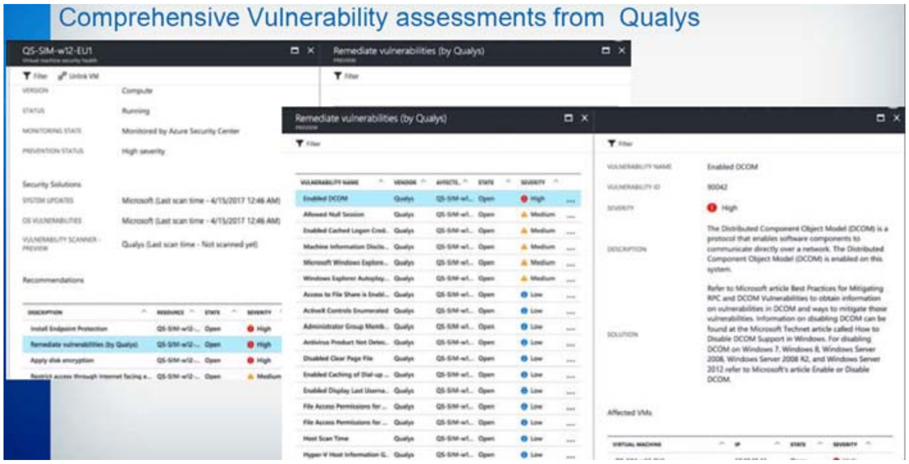
Qualys Web Application Scanning Getting Started Guide Version 6.0.1 at 20, attached hereto as Exhibit 15.

190. The '731 Accused Products perform code scans and save lists of computer commands the incoming files are programmed to perform in the security profiles:



STEP	METHOD	END POINT
Run EC2 Connector to sync. Assets and update dynamic tags	POST	/qps/rest/2.0/run/am/awsassetdataconnector/{id}
Update Authentication	POST	/api/2.0/fo/auth/unix/'action=update&ids={}&ips{}=&echo_request=1'
Launch Scans for the specific Tag	POST	api/2.0/fo/scan/'action=launch&scan_title={}&connector_name&iscanner_name={}&target_from=tags&tag_set_include={id}
Launch Reports on a pre-defined template	POST	/api/2.0/fo/report/' {'action': 'launch', 'report_refs': 'scan/{id}, 'output_format': 'xml', 'template_id': {id}, 'report_type': 'Scan'}
Fetch Scan Results	GET	/api/2.0/fo/report/' 'action=fetch&id={id}

Securing Public Cloud Infrastructure using Qualys presentation at 31, attached hereto as Exhibit 13.


Comprehensive Vulnerability assessments from Qualys

QS-SIM-w12-EU1
Virtual machine security health
Filter
Unlink VM
Remediate vulnerabilities (by Qualys)
Preview
Filter

VERSION	Compute
STATUS	Running
MONITORING STATE	Monitored by Azure Security Center
PREVENTION STATUS	High severity

Security Solutions

SYSTEM UPDATES	Microsoft (Last scan time - 4/15/2017 12:46 AM)
OS VULNERABILITIES	Microsoft (Last scan time - 4/15/2017 12:46 AM)
VULNERABILITY SCANNER - PREVIEW	Qualys (Last scan time - Not scanned yet)

Recommendations

DESCRIPTION	RESOURCE	STATE	SEVERITY
Install Endpoint Protection	QS-SIM-w12-...	Open	● High
Remediate vulnerabilities (by Qualys)	QS-SIM-w12-...	Open	● High
Apply disk encryption	QS-SIM-w12-...	Open	● High
Restrict access through Internet facing e...	QS-SIM-w12-...	Open	▲ Medium

Remediate vulnerabilities (by Qualys)

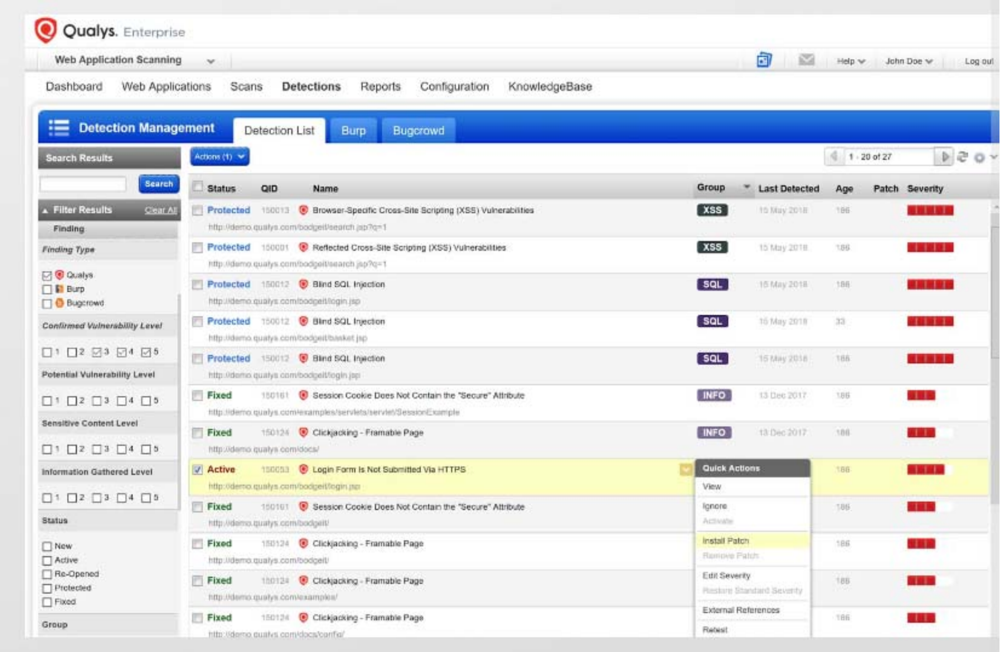
VULNERABILITY NAME	VENDOR	AFFECTE...	STATE	SEVERITY
Enabled DCOM	Qualys	QS-SIM-w1...	Open	● High
Allowed Null Session	Qualys	QS-SIM-w1...	Open	▲ Medium
Enabled Cached Logon Credi...	Qualys	QS-SIM-w1...	Open	▲ Medium
Machine Information Disclo...	Qualys	QS-SIM-w1...	Open	▲ Medium
Microsoft Windows Explore...	Qualys	QS-SIM-w1...	Open	▲ Medium
Windows Explorer Autoplay...	Qualys	QS-SIM-w1...	Open	▲ Medium
Access to File Share is Enabl...	Qualys	QS-SIM-w1...	Open	● Low
ActiveX Controls Enumerated	Qualys	QS-SIM-w1...	Open	● Low
Administrator Group Memb...	Qualys	QS-SIM-w1...	Open	● Low
Antivirus Product Not Detec...	Qualys	QS-SIM-w1...	Open	● Low
Disabled Clear Page File	Qualys	QS-SIM-w1...	Open	● Low
Enabled Caching of Dial-up ...	Qualys	QS-SIM-w1...	Open	● Low
Enabled Display Last Userna...	Qualys	QS-SIM-w1...	Open	● Low
File Access Permissions for ...	Qualys	QS-SIM-w1...	Open	● Low
File Access Permissions for ...	Qualys	QS-SIM-w1...	Open	● Low
Host Scan Time	Qualys	QS-SIM-w1...	Open	● Low
Hyper-V Host Information G...	Qualys	QS-SIM-w1...	Open	● Low

VULNERABILITY NAME	Enabled DCOM
VULNERABILITY ID	90042
SEVERITY	● High
DESCRIPTION	The Distributed Component Object Model (DCOM) is a protocol that enables software components to communicate directly over a network. The Distributed Component Object Model (DCOM) is enabled on this system.
SOLUTION	Refer to Microsoft article Best Practices for Mitigating RPC and DCOM Vulnerabilities to obtain information on vulnerabilities in DCOM and ways to mitigate those vulnerabilities. Information on disabling DCOM can be found at the Microsoft Technet article called How to Disable DCOM Support in Windows. For disabling DCOM on Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 refer to Microsoft's article Enable or Disable DCOM.

Affected VMs

VIRTUAL MACHINE	IP	STATE	SEVERITY

Securing Public Cloud Infrastructure using Qualys presentation at 37, attached hereto as Exhibit 13.



Finding

Finding Type

☑ Qualys
□ Burp
□ Bugcrowd

Confirmed Vulnerability Level

□ 1 □ 2 ☑ 3 ☑ 4 ☑ 5

Potential Vulnerability Level

□ 1 □ 2 □ 3 □ 4 □ 5

Sensitive Content Level

□ 1 □ 2 □ 3 □ 4 □ 5

Information Gathered Level

□ 1 □ 2 □ 3 □ 4 □ 5

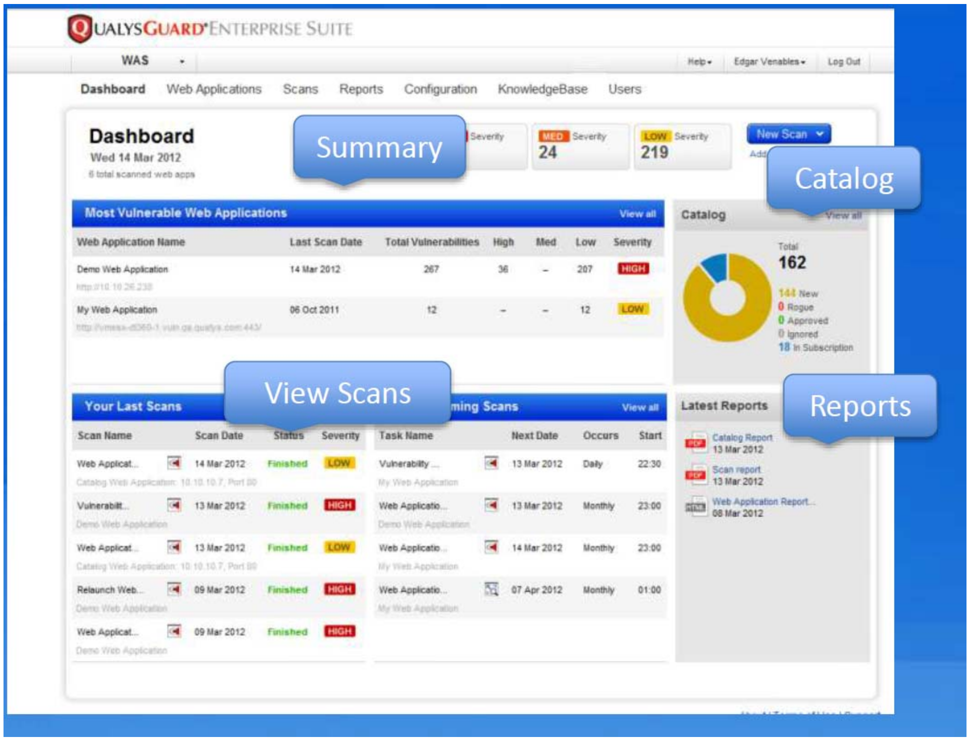
Status

□ New
□ Active
□ Re-Opened
□ Protected
□ Fixed

Group

	Status	QID	Name	Group	Last Detected	Age	Patch	Severity
□	Protected	150013	Browser-Specific Cross-Site Scripting (XSS) Vulnerabilities http://demo.qualys.com/bodgeit/search.jsp?q=1	XSS	15 May 2018	186		
□	Protected	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities http://demo.qualys.com/bodgeit/search.jsp?q=1	XSS	15 May 2018	186		
□	Protected	150012	Blind SQL Injection http://demo.qualys.com/bodgeit/login.jsp	SQL	15 May 2018	186		
□	Protected	150012	Blind SQL Injection http://demo.qualys.com/bodgeit/basket.jsp	SQL	15 May 2018	33		
□	Protected	150012	Blind SQL Injection http://demo.qualys.com/bodgeit/login.jsp	SQL	15 May 2018	186		
□	Fixed	150161	Session Cookie Does Not Contain the "Secure" Attribute http://demo.qualys.com/examples/servlets/servlet/SessionExample	INFO	13 Dec 2017	186		
□	Fixed	150124	Clickjacking - Framable Page http://demo.qualys.com/docs/	INFO	13 Dec 2017	186		
☑	Active	150053	Login Form Is Not Submitted Via HTTPS http://demo.qualys.com/bodgeit/login.jsp			186		
□	Fixed	150161	Session Cookie Does Not Contain the "Secure" Attribute http://demo.qualys.com/bodgeit/			186		
□	Fixed	150124	Clickjacking - Framable Page http://demo.qualys.com/bodgeit/			186		
□	Fixed	150124	Clickjacking - Framable Page http://demo.qualys.com/examples/			186		
□	Fixed	150124	Clickjacking - Framable Page http://demo.qualys.com/docs/config/			186		

https://www.qualys.com/apps/web-app-firewall/, attached hereto as Exhibit 16.



Dashboard
Wed 14 Mar 2012
6 total scanned web apps

Severity | MED Severity 24 | LOW Severity 219

Most Vulnerable Web Applications

Web Application Name	Last Scan Date	Total Vulnerabilities	High	Med	Low	Severity
Demo Web Application http://10.10.26.238	14 Mar 2012	267	36	–	207	HIGH
My Web Application http://vmesx-d360-1.vuln.qa.qualys.com:443/	06 Oct 2011	12	–	–	12	LOW

Catalog

Total 162
144 New
0 Rogue
0 Approved
0 Ignored
18 In Subscription

Your Last Scans

Scan Name	Scan Date	Status	Severity
Web Applicat... Catalog Web Application: 10.10.10.7, Port 80	14 Mar 2012	Finished	LOW
Vulnerabilit... Demo Web Application	13 Mar 2012	Finished	HIGH
Web Applicat... Catalog Web Application: 10.10.10.7, Port 80	13 Mar 2012	Finished	LOW
Relaunch Web... Demo Web Application	09 Mar 2012	Finished	HIGH
Web Applicat... Demo Web Application	09 Mar 2012	Finished	HIGH

ming Scans

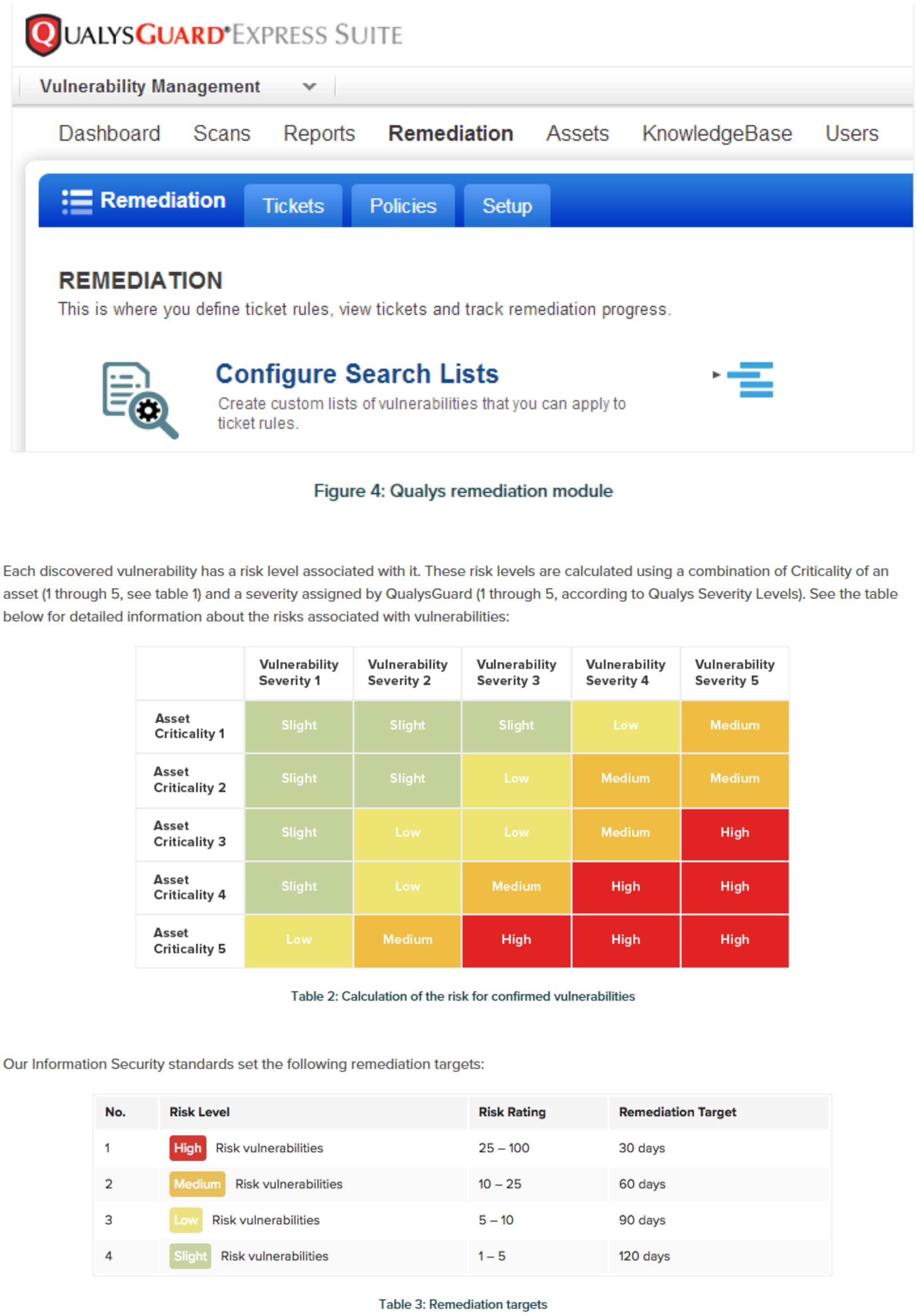
Task Name	Next Date	Occurs	Start
Vulnerability ... My Web Application	13 Mar 2012	Daily	22:30
Web Applicatio... Demo Web Application	13 Mar 2012	Monthly	23:00
Web Applicatio... My Web Application	14 Mar 2012	Monthly	23:00
Web Applicatio... My Web Application	07 Apr 2012	Monthly	01:00

Latest Reports

Catalog Report 13 Mar 2012
Scan report 13 Mar 2012
Web Application Report... 08 Mar 2012

QualysGuard InfoDay 2014 presentation at 29, attached hereto as Exhibit 12.

191. The '731 Accused Products come with a policy-based ticketing module including entries that relate cache content and policies:



REMEDIATION

This is where you define ticket rules, view tickets and track remediation progress.

Configure Search Lists

Create custom lists of vulnerabilities that you can apply to ticket rules.

Figure 4: Qualys remediation module

Each discovered vulnerability has a risk level associated with it. These risk levels are calculated using a combination of Criticality of an asset (1 through 5, see table 1) and a severity assigned by QualysGuard (1 through 5, according to Qualys Severity Levels). See the table below for detailed information about the risks associated with vulnerabilities:

	Vulnerability Severity 1	Vulnerability Severity 2	Vulnerability Severity 3	Vulnerability Severity 4	Vulnerability Severity 5
Asset Criticality 1	Slight	Slight	Slight	Low	Medium
Asset Criticality 2	Slight	Slight	Low	Medium	Medium
Asset Criticality 3	Slight	Low	Low	Medium	High
Asset Criticality 4	Slight	Low	Medium	High	High
Asset Criticality 5	Low	Medium	High	High	High

Table 2: Calculation of the risk for confirmed vulnerabilities

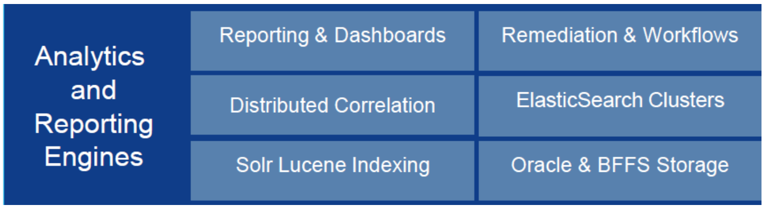
Our Information Security standards set the following remediation targets:

No.	Risk Level	Risk Rating	Remediation Target
1	High Risk vulnerabilities	25 – 100	30 days
2	Medium Risk vulnerabilities	10 – 25	60 days
3	Low Risk vulnerabilities	5 – 10	90 days
4	Slight Risk vulnerabilities	1 – 5	120 days

Table 3: Remediation targets

https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.

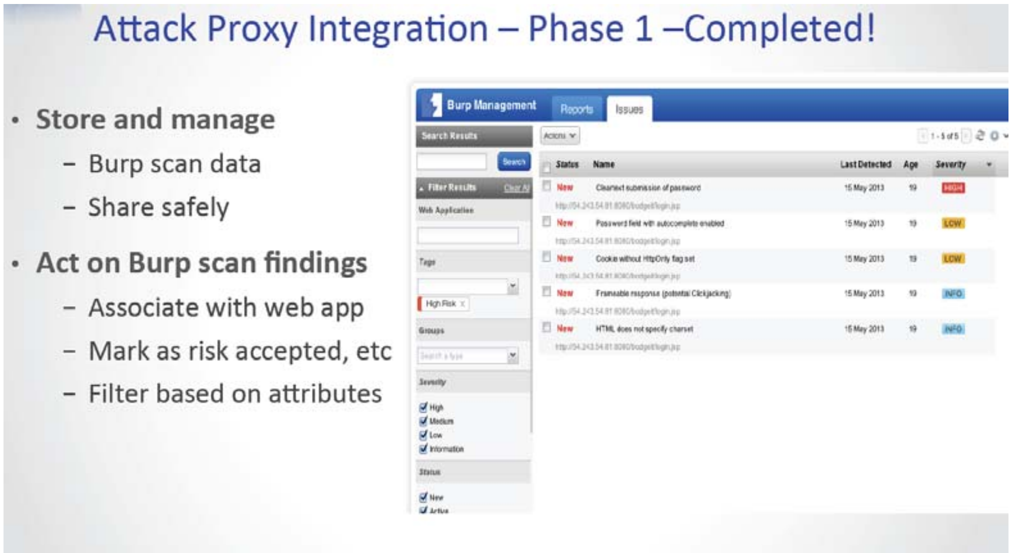
192. The '731 Accused Products investigate and remediate vulnerabilities:



Analytics and Reporting Engines	Reporting & Dashboards	Remediation & Workflows
	Distributed Correlation	ElasticSearch Clusters
	Solr Lucene Indexing	Oracle & BFFS Storage

Securing Public Cloud Infrastructure using Qualys presentation at 12, attached hereto as Exhibit 13.

193. The '731 Accused Products store policy index (high/low risk data) including entries that relate cache content and policies:



Attack Proxy Integration – Phase 1 –Completed!

- Store and manage
  - Burp scan data
  - Share safely
- Act on Burp scan findings
  - Associate with web app
  - Mark as risk accepted, etc
  - Filter based on attributes

Status	Name	Last Detected	Age	Severity
New	Cleartext submission of password http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	HIGH
New	Password field with autocomplete enabled http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	LOW
New	Cookie without HttpOnly flag set http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	LOW
New	Framable response (potential Clickjacking) http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	INFO
New	HTML does not specify charset http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	INFO

QualysGuard Web Application Security presentation at 8, attached hereto as Exhibit 8.

194. The '731 Accused Products include a file cache for storing files that have been scanned by a scanner for future access, where each of the stored files is indexed by a file identifier.

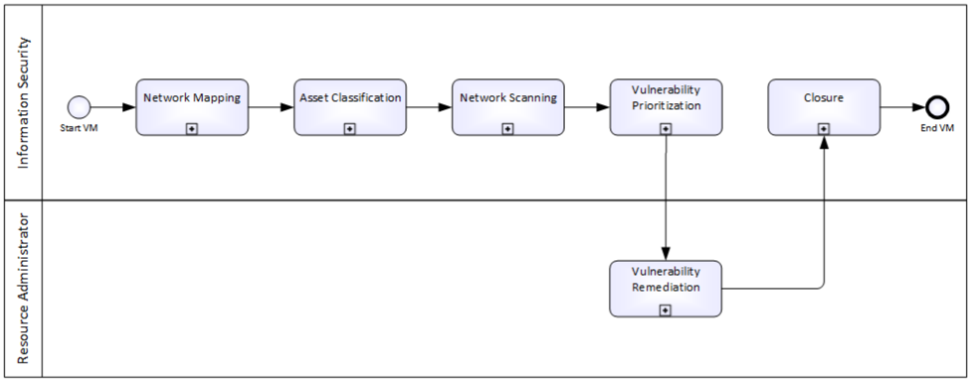
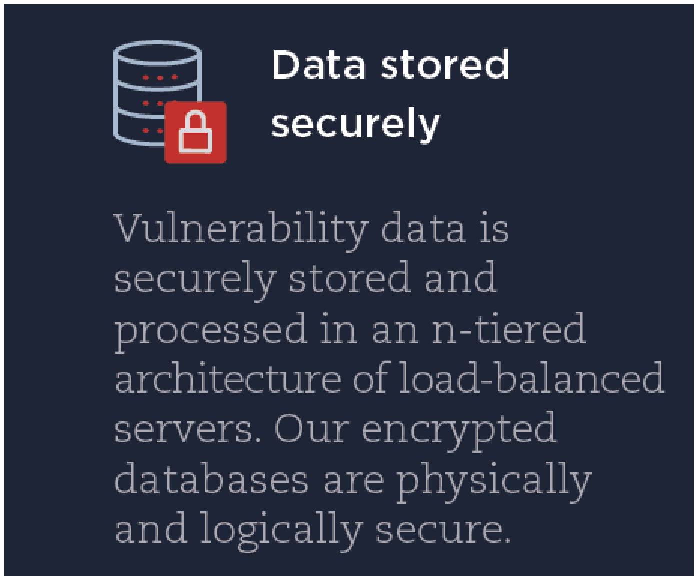


Figure 1: Vulnerability management process

https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.

195. The ‘731 Accused Products securely store scanned data in an n-tiered architecture with load balanced servers:

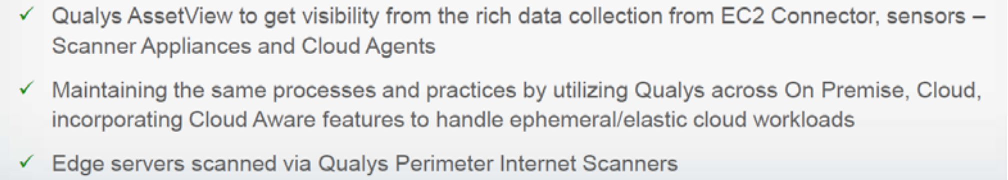


Data stored securely

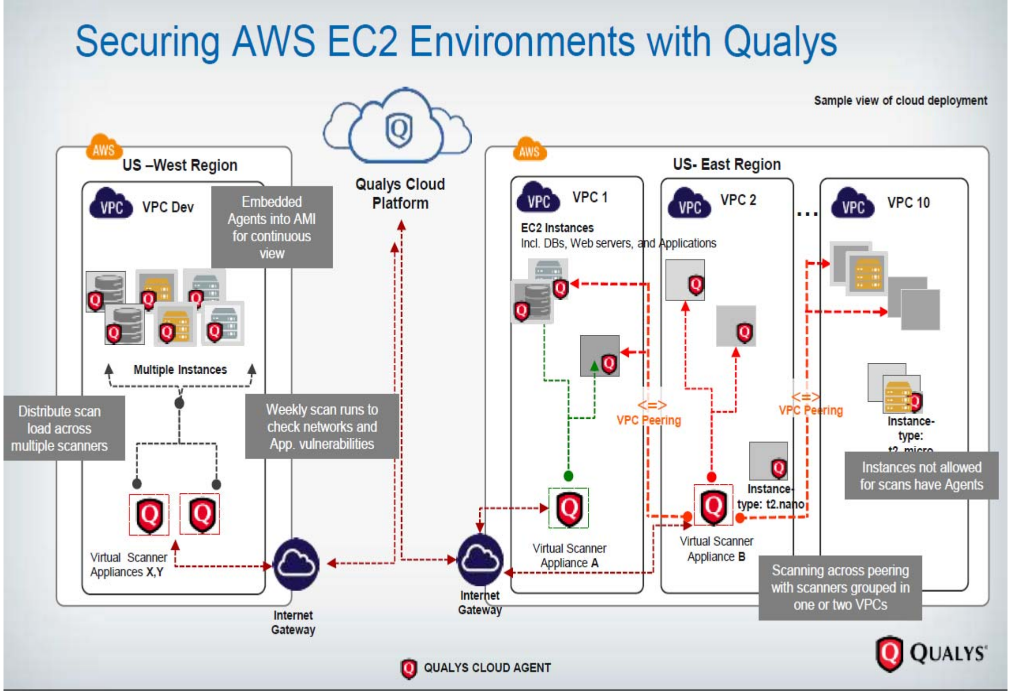
Vulnerability data is securely stored and processed in an n-tiered architecture of load-balanced servers. Our encrypted databases are physically and logically secure.

Qualys Cloud Platform datasheet at 3, attached hereto as Exhibit 22.

196. The ‘731 Accused Products scan content and derive security profiles:



- ✓ Qualys AssetView to get visibility from the rich data collection from EC2 Connector, sensors – Scanner Appliances and Cloud Agents
- ✓ Maintaining the same processes and practices by utilizing Qualys across On Premise, Cloud, incorporating Cloud Aware features to handle ephemeral/elastic cloud workloads
- ✓ Edge servers scanned via Qualys Perimeter Internet Scanners

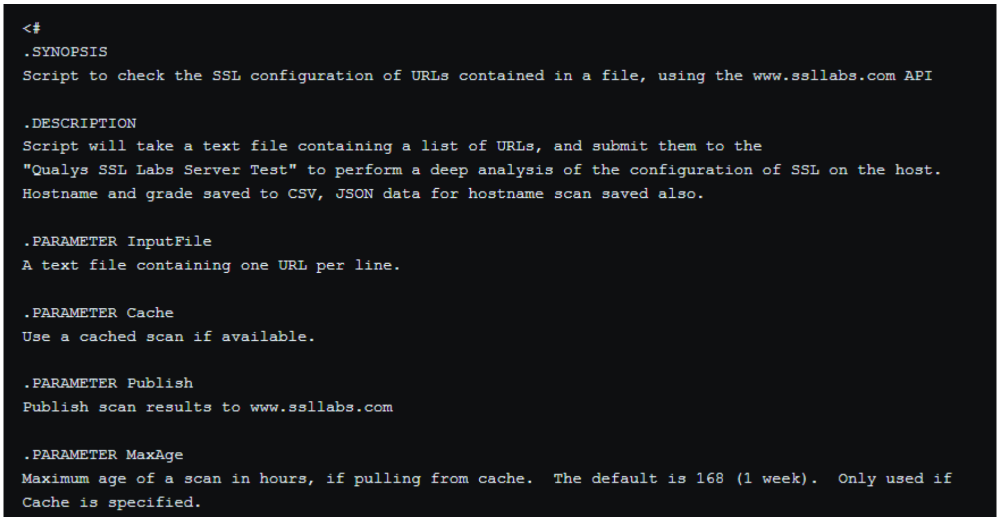


Securing AWS EC2 Environments with Qualys

Sample view of cloud deployment
AWS
US –West Region
VPC
VPC Dev
Embedded Agents into AMI for continuous view
Qualys Cloud Platform
Multiple Instances
Distribute scan load across multiple scanners
Weekly scan runs to check networks and App. vulnerabilities
Virtual Scanner Appliances X,Y
Internet Gateway
AWS
US- East Region
VPC 1
VPC 2
VPC 10
EC2 Instances
Incl. DBs, Web servers, and Applications
<=>
VPC Peering
<=>
VPC Peering
Instance-type: t2.micro
Instance-type: t2.nano
Instances not allowed for scans have Agents
Virtual Scanner Appliance A
Virtual Scanner Appliance B
Internet Gateway
Scanning across peering with scanners grouped in one or two VPCs
QUALYS CLOUD AGENT
QUALYS

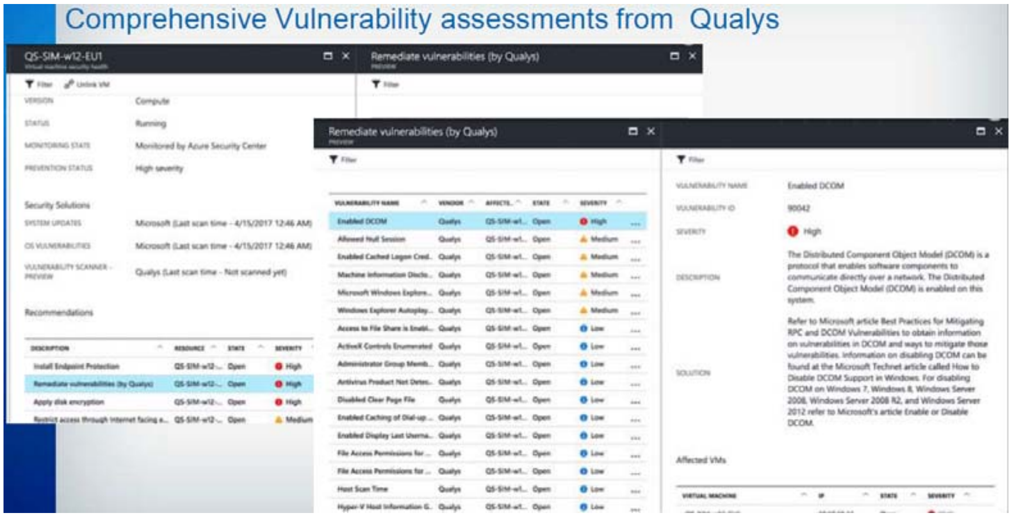
Securing Public Cloud Infrastructure using Qualys presentation at 29, attached hereto as Exhibit 13.

197. The '731 Accused Products perform a deep analysis of the configuration of SSL on the host. The Hostname scan is saved, and a cached scan is used if available:



```
<#
.SYNOPSIS
Script to check the SSL configuration of URLs contained in a file, using the www.ssllabs.com API

.DESCRIPTION
Script will take a text file containing a list of URLs, and submit them to the
"Qualys SSL Labs Server Test" to perform a deep analysis of the configuration of SSL on the host.
Hostname and grade saved to CSV, JSON data for hostname scan saved also.

.PARAMETER InputFile
A text file containing one URL per line.

.PARAMETER Cache
Use a cached scan if available.

.PARAMETER Publish
Publish scan results to www.ssllabs.com

.PARAMETER MaxAge
Maximum age of a scan in hours, if pulling from cache.  The default is 168 (1 week).  Only used if
Cache is specified.
```

https://www.musingitoutloud.com/powershell-ssl-labs/, attached hereto as Exhibit 21.



Comprehensive Vulnerability assessments from Qualys

QS-SIM-w12-EU1
Virtual machine security health
Filter
Unlink VM
Remediate vulnerabilities (by Qualys)
PREVIEW
Filter

VERSION	Compute
STATUS	Running
MONITORING STATE	Monitored by Azure Security Center
PREVENTION STATUS	High severity

Security Solutions

SYSTEM UPDATES	Microsoft (Last scan time - 4/15/2017 12:46 AM)
OS VULNERABILITIES	Microsoft (Last scan time - 4/15/2017 12:46 AM)
VULNERABILITY SCANNER - PREVIEW	Qualys (Last scan time - Not scanned yet)

Recommendations

DESCRIPTION	RESOURCE	STATE	SEVERITY
Install Endpoint Protection	QS-SIM-w12-...	Open	High
Remediate vulnerabilities (by Qualys)	QS-SIM-w12-...	Open	High
Apply disk encryption	QS-SIM-w12-...	Open	High
Restrict access through Internet facing e...	QS-SIM-w12-...	Open	Medium

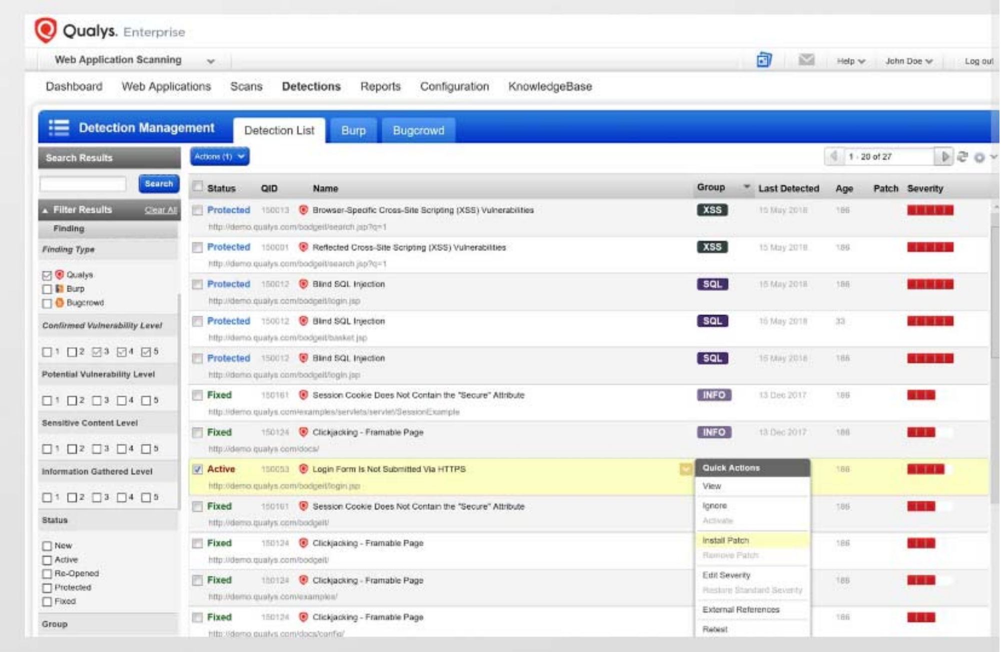
VULNERABILITY NAME	VENDOR	AFFECTE...	STATE	SEVERITY	
Enabled DCOM	Qualys	QS-SIM-w1...	Open	High	...
Allowed Null Session	Qualys	QS-SIM-w1...	Open	Medium	...
Enabled Cached Logon Cred...	Qualys	QS-SIM-w1...	Open	Medium	...
Machine Information Disclo...	Qualys	QS-SIM-w1...	Open	Medium	...
Microsoft Windows Explore...	Qualys	QS-SIM-w1...	Open	Medium	...
Windows Explorer Autoplay...	Qualys	QS-SIM-w1...	Open	Medium	...
Access to File Share is Enabl...	Qualys	QS-SIM-w1...	Open	Low	...
ActiveX Controls Enumerated	Qualys	QS-SIM-w1...	Open	Low	...
Administrator Group Memb...	Qualys	QS-SIM-w1...	Open	Low	...
Antivirus Product Not Detec...	Qualys	QS-SIM-w1...	Open	Low	...
Disabled Clear Page File	Qualys	QS-SIM-w1...	Open	Low	...
Enabled Caching of Dial-up ...	Qualys	QS-SIM-w1...	Open	Low	...
Enabled Display Last Userna...	Qualys	QS-SIM-w1...	Open	Low	...
File Access Permissions for ...	Qualys	QS-SIM-w1...	Open	Low	...
File Access Permissions for ...	Qualys	QS-SIM-w1...	Open	Low	...
Host Scan Time	Qualys	QS-SIM-w1...	Open	Low	...
Hyper-V Host Information G...	Qualys	QS-SIM-w1...	Open	Low	...

VULNERABILITY NAME	Enabled DCOM
VULNERABILITY ID	90042
SEVERITY	High
DESCRIPTION	The Distributed Component Object Model (DCOM) is a protocol that enables software components to communicate directly over a network. The Distributed Component Object Model (DCOM) is enabled on this system.
SOLUTION	Refer to Microsoft article Best Practices for Mitigating RPC and DCOM Vulnerabilities to obtain information on vulnerabilities in DCOM and ways to mitigate those vulnerabilities. Information on disabling DCOM can be found at the Microsoft Technet article called How to Disable DCOM Support in Windows. For disabling DCOM on Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 refer to Microsoft's article Enable or Disable DCOM.

Affected VMs

VIRTUAL MACHINE	IP	STATE	SEVERITY

Securing Public Cloud Infrastructure using Qualys presentation at 37, attached hereto as Exhibit 13.



Filter Results Clear All

Finding

Finding Type

☑ Qualys
☐ Burp
☐ Bugcrowd

Confirmed Vulnerability Level

☐1 ☐2 ☑3 ☑4 ☑5

Potential Vulnerability Level

☐1 ☐2 ☐3 ☐4 ☐5

Sensitive Content Level

☐1 ☐2 ☐3 ☐4 ☐5

Information Gathered Level

☐1 ☐2 ☐3 ☐4 ☐5

Status

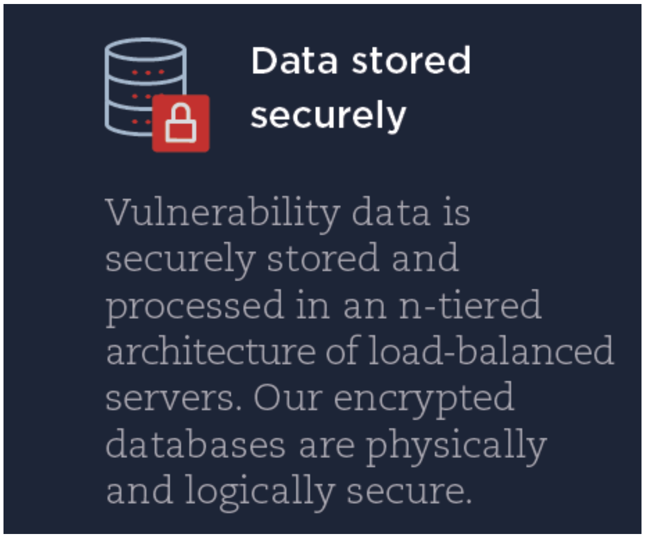
☐ New
☐ Active
☐ Re-Opened
☐ Protected
☐ Fixed

Group

Status	QID	Name	Group	Last Detected	Age	Patch	Severity
☐ Protected	150013	Browser-Specific Cross-Site Scripting (XSS) Vulnerabilities http://demo.qualys.com/bodgeit/search.jsp?q=1	XSS	15 May 2018	186		▮▮▮▮▮
☐ Protected	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities http://demo.qualys.com/bodgeit/search.jsp?q=1	XSS	15 May 2018	186		▮▮▮▮▮
☐ Protected	150012	Blind SQL Injection http://demo.qualys.com/bodgeit/login.jsp	SQL	15 May 2018	186		▮▮▮▮▮
☐ Protected	150012	Blind SQL Injection http://demo.qualys.com/bodgeit/basket.jsp	SQL	15 May 2018	33		▮▮▮▮▮
☐ Protected	150012	Blind SQL Injection http://demo.qualys.com/bodgeit/login.jsp	SQL	15 May 2018	186		▮▮▮▮▮
☐ Fixed	150161	Session Cookie Does Not Contain the "Secure" Attribute http://demo.qualys.com/examples/servlets/servlet/SessionExample	INFO	13 Dec 2017	186		▮▮▮
☐ Fixed	150124	Clickjacking - Framable Page http://demo.qualys.com/docs/	INFO	13 Dec 2017	186		▮▮▮
☑ Active	150053	Login Form Is Not Submitted Via HTTPS http://demo.qualys.com/bodgeit/login.jsp			186		▮▮▮▮
☐ Fixed	150161	Session Cookie Does Not Contain the "Secure" Attribute http://demo.qualys.com/bodgeit/			186		▮▮▮
☐ Fixed	150124	Clickjacking - Framable Page http://demo.qualys.com/bodgeit/			186		▮▮▮
☐ Fixed	150124	Clickjacking - Framable Page http://demo.qualys.com/examples/			186		▮▮▮
☐ Fixed	150124	Clickjacking - Framable Page http://demo.qualys.com/docs/config/			186		▮▮▮

https://www.qualys.com/apps/web-app-firewall/, attached hereto as Exhibit 16.

198. The '731 Accused Products include a security profile cache for storing the security profiles derived by the scanner, where each of the security profiles is indexed in the security profile cache by a file identifier associated with a corresponding file stored in the file cache.

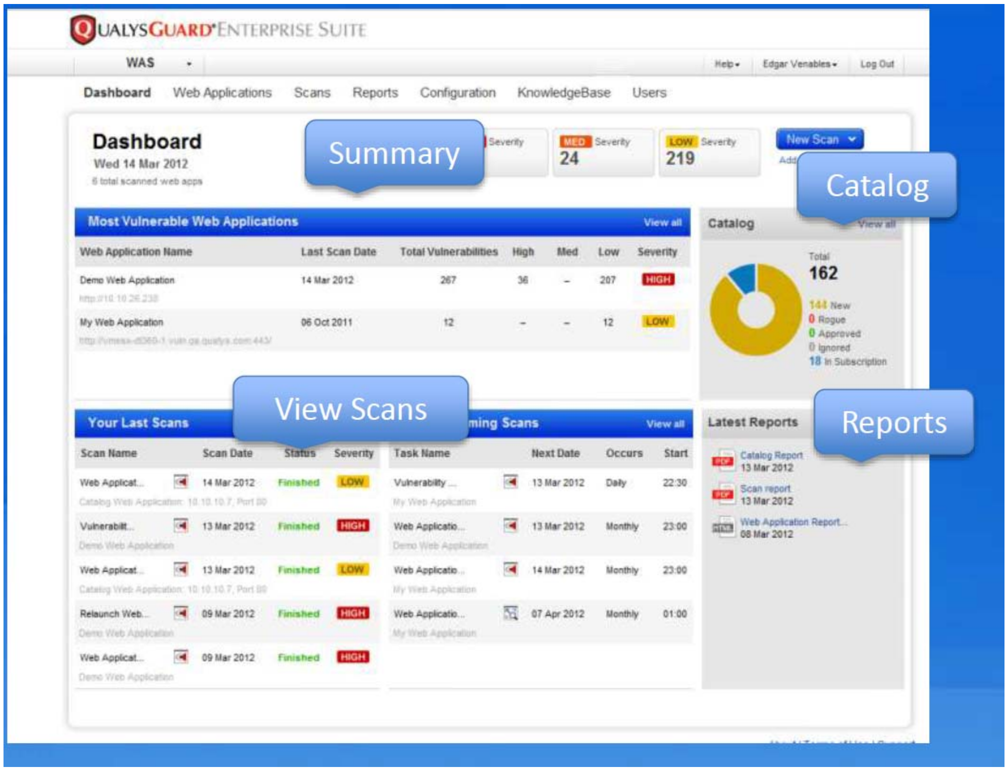


Data stored securely

Vulnerability data is securely stored and processed in an n-tiered architecture of load-balanced servers. Our encrypted databases are physically and logically secure.

Qualys Cloud Platform datasheet at 3, attached hereto as Exhibit 22.

199. The '731 Accused Products' security profiles are indexed using a file identifier:



Dashboard
Wed 14 Mar 2012
6 total scanned web apps

Severity | MED Severity 24 | LOW Severity 219

Most Vulnerable Web Applications — View all

Web Application Name	Last Scan Date	Total Vulnerabilities	High	Med	Low	Severity
Demo Web Application http://10.10.26.238	14 Mar 2012	267	36	–	207	HIGH
My Web Application http://vmesx-d060-1.vuln.qa.qualys.com:443/	06 Oct 2011	12	–	–	12	LOW

Catalog — View all

Total 162
144 New
0 Rogue
0 Approved
0 Ignored
18 In Subscription

Your Last Scans

Scan Name	Scan Date	Status	Severity
Web Applicat... Catalog Web Application: 10.10.10.7, Port 80	14 Mar 2012	Finished	LOW
Vulnerabilit... Demo Web Application	13 Mar 2012	Finished	HIGH
Web Applicat... Catalog Web Application: 10.10.10.7, Port 80	13 Mar 2012	Finished	LOW
Relaunch Web... Demo Web Application	09 Mar 2012	Finished	HIGH
Web Applicat... Demo Web Application	09 Mar 2012	Finished	HIGH

...ming Scans — View all

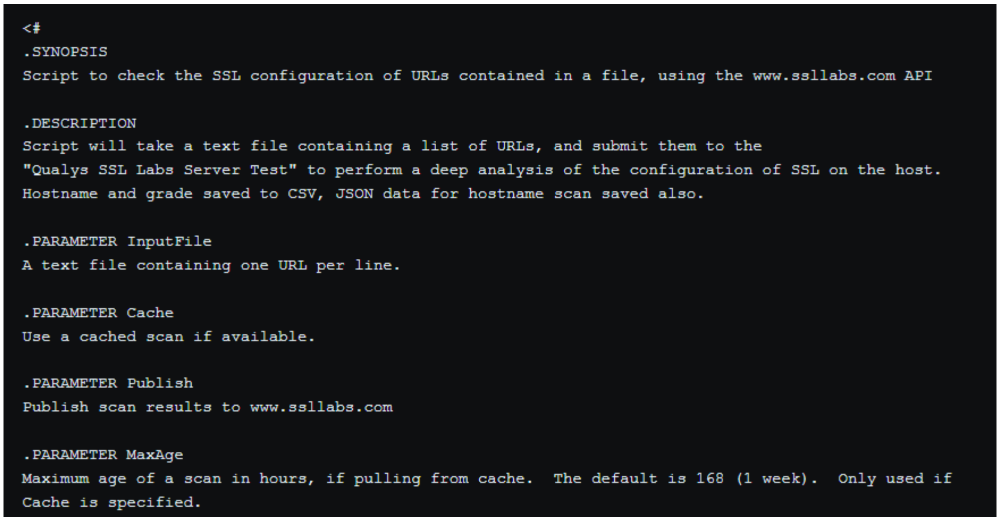
Task Name	Next Date	Occurs	Start
Vulnerability ... My Web Application	13 Mar 2012	Daily	22:30
Web Applicatio... Demo Web Application	13 Mar 2012	Monthly	23:00
Web Applicatio... My Web Application	14 Mar 2012	Monthly	23:00
Web Applicatio... My Web Application	07 Apr 2012	Monthly	01:00

Latest Reports

- PDF Catalog Report 13 Mar 2012
- PDF Scan report 13 Mar 2012
- HTML Web Application Report... 08 Mar 2012

QualysGuard InfoDay 2014 presentation at 29, attached hereto as Exhibit 12.

200. The '731 Accused Products perform a deep analysis of the configuration of SSL on the host. The scan is saved, and a cached scan is used if available:



```
<#
.SYNOPSIS
Script to check the SSL configuration of URLs contained in a file, using the www.ssllabs.com API

.DESCRIPTION
Script will take a text file containing a list of URLs, and submit them to the
"Qualys SSL Labs Server Test" to perform a deep analysis of the configuration of SSL on the host.
Hostname and grade saved to CSV, JSON data for hostname scan saved also.

.PARAMETER InputFile
A text file containing one URL per line.

.PARAMETER Cache
Use a cached scan if available.

.PARAMETER Publish
Publish scan results to www.ssllabs.com

.PARAMETER MaxAge
Maximum age of a scan in hours, if pulling from cache.  The default is 168 (1 week).  Only used if
Cache is specified.
```

https://www.musingitoutloud.com/powershell-ssl-labs/, attached hereto as Exhibit 21.

201. The '731 Accused Products include a security policy cache for storing security policies for intranet computers within the intranet, the security policies each including a list of restrictions for files that are transmitted to a corresponding subset of the intranet computers.

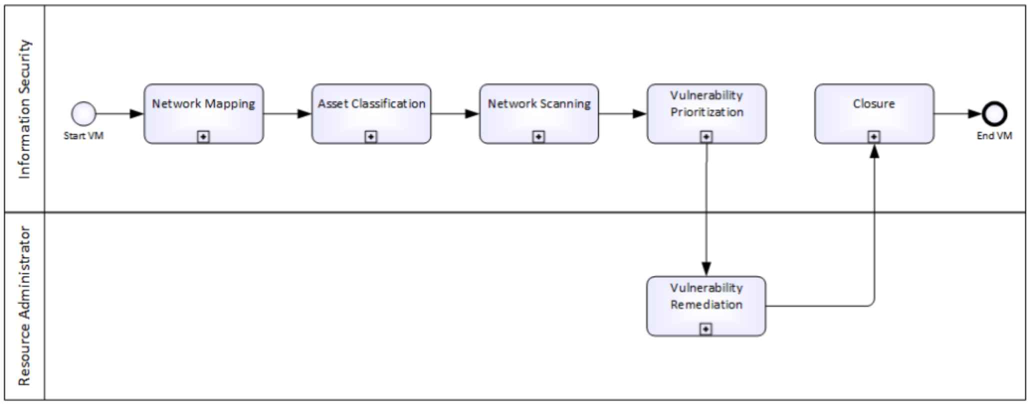
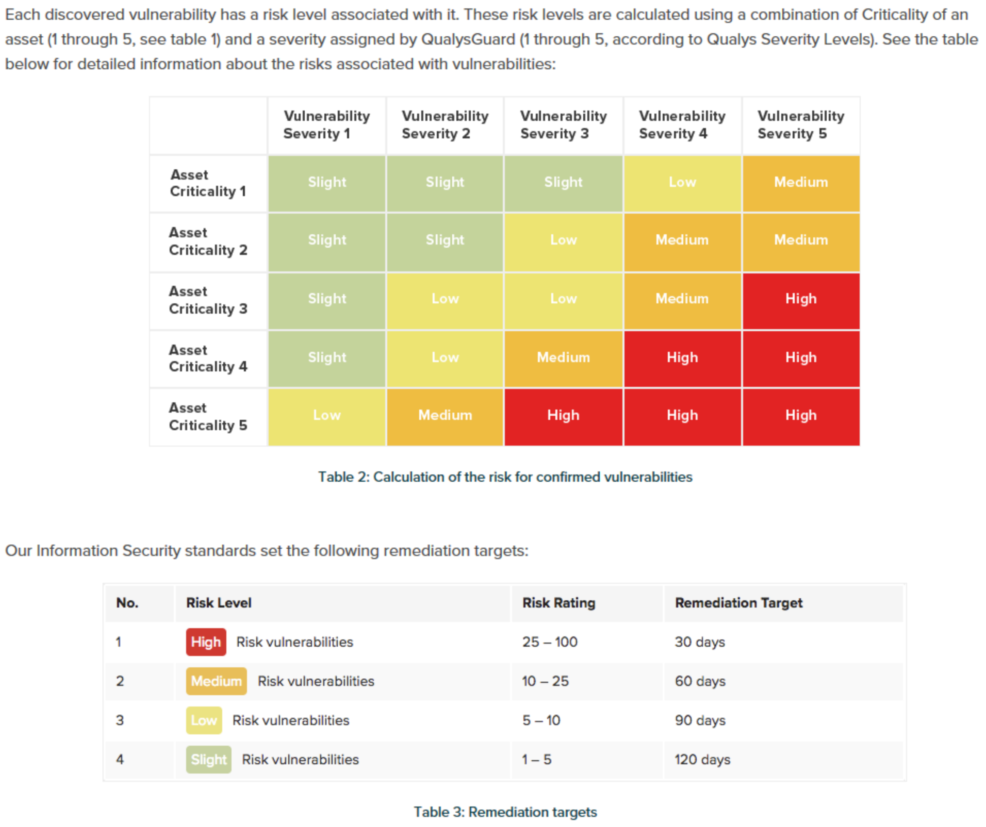


Figure 1: Vulnerability management process

https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.



Each discovered vulnerability has a risk level associated with it. These risk levels are calculated using a combination of Criticality of an asset (1 through 5, see table 1) and a severity assigned by QualysGuard (1 through 5, according to Qualys Severity Levels). See the table below for detailed information about the risks associated with vulnerabilities:

	Vulnerability Severity 1	Vulnerability Severity 2	Vulnerability Severity 3	Vulnerability Severity 4	Vulnerability Severity 5
Asset Criticality 1	Slight	Slight	Slight	Low	Medium
Asset Criticality 2	Slight	Slight	Low	Medium	Medium
Asset Criticality 3	Slight	Low	Low	Medium	High
Asset Criticality 4	Slight	Low	Medium	High	High
Asset Criticality 5	Low	Medium	High	High	High

Table 2: Calculation of the risk for confirmed vulnerabilities

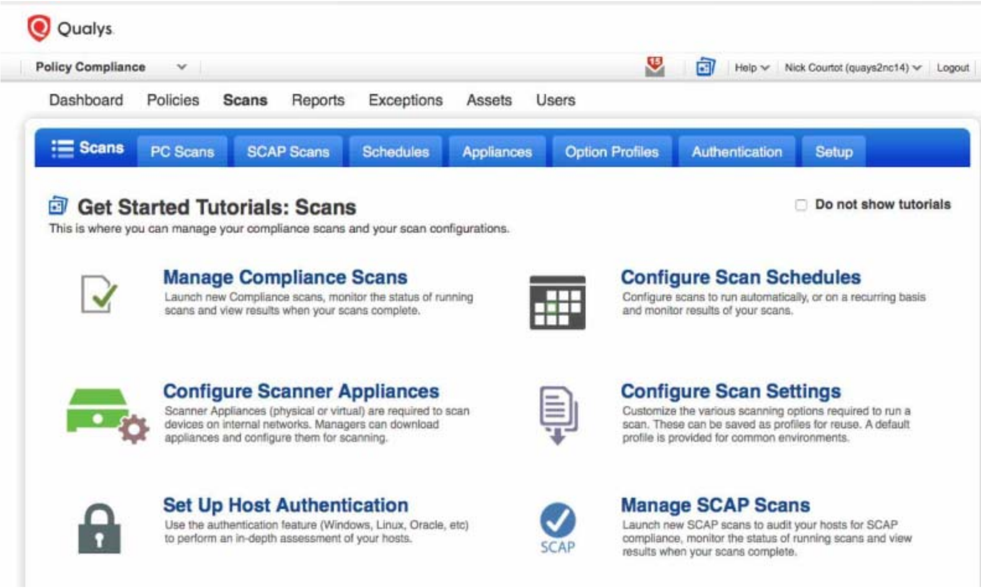
Our Information Security standards set the following remediation targets:

No.	Risk Level	Risk Rating	Remediation Target
1	High Risk vulnerabilities	25 – 100	30 days
2	Medium Risk vulnerabilities	10 – 25	60 days
3	Low Risk vulnerabilities	5 – 10	90 days
4	Slight Risk vulnerabilities	1 – 5	120 days

Table 3: Remediation targets

https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.

202. The '731 Accused Products use Policy Compliance to evaluate content profiles, save the results as entries in the policy index, and share it with multiple users.



Get Started Tutorials: Scans

☐ Do not show tutorials

This is where you can manage your compliance scans and your scan configurations.

Manage Compliance Scans
Launch new Compliance scans, monitor the status of running scans and view results when your scans complete.

Configure Scan Schedules
Configure scans to run automatically, or on a recurring basis and monitor results of your scans.

Configure Scanner Appliances
Scanner Appliances (physical or virtual) are required to scan devices on internal networks. Managers can download appliances and configure them for scanning.

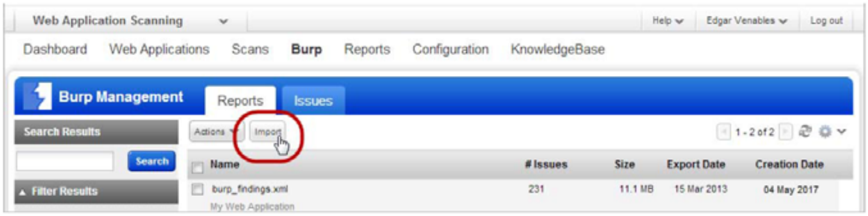
Configure Scan Settings
Customize the various scanning options required to run a scan. These can be saved as profiles for reuse. A default profile is provided for common environments.

Set Up Host Authentication
Use the authentication feature (Windows, Linux, Oracle, etc) to perform an in-depth assessment of your hosts.

Manage SCAP Scans
Launch new SCAP scans to audit your hosts for SCAP compliance, monitor the status of running scans and view results when your scans complete.

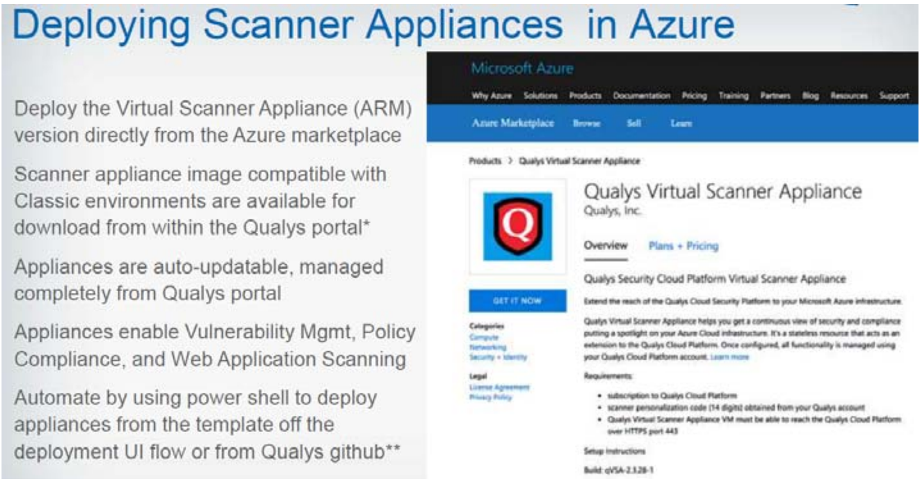
https://www.qualys.com/apps/policy-compliance/, attached hereto as Exhibit 17.

> The Burp Management feature gives you a way to store the findings discovered by the Burp Suite scanner with those discovered by WAS and share this information with multiple users. To learn more refer to this blog article at the Qualys Community. (This feature is not available to Express Lite users.)
>
> To get started click the Burp option on the top menu and go to Burp > Reports, then click Import and we'll walk you through the steps. Your issues list shows imported Burp issues.



Name	# Issues	Size	Export Date	Creation Date
burp_findings.xml My Web Application	231	11.1 MB	15 Mar 2013	04 May 2017

Qualys Web Application Scanning Getting Started Guide Version 6.0.1 at 20, attached hereto as Exhibit 15.



Deploying Scanner Appliances in Azure

- Deploy the Virtual Scanner Appliance (ARM) version directly from the Azure marketplace
- Scanner appliance image compatible with Classic environments are available for download from within the Qualys portal*
- Appliances are auto-updatable, managed completely from Qualys portal
- Appliances enable Vulnerability Mgmt, Policy Compliance, and Web Application Scanning
- Automate by using power shell to deploy appliances from the template off the deployment UI flow or from Qualys github**

Qualys Virtual Scanner Appliance
Qualys, Inc.

Qualys Security Cloud Platform Virtual Scanner Appliance

Extend the reach of the Qualys Cloud Security Platform to your Microsoft Azure infrastructure.

Qualys Virtual Scanner Appliance helps you get a continuous view of security and compliance putting a spotlight on your Azure Cloud infrastructure. It's a stateless resource that acts as an extension to the Qualys Cloud Platform. Once configured, all functionality is managed using your Qualys Cloud Platform account. Learn more

Requirements:

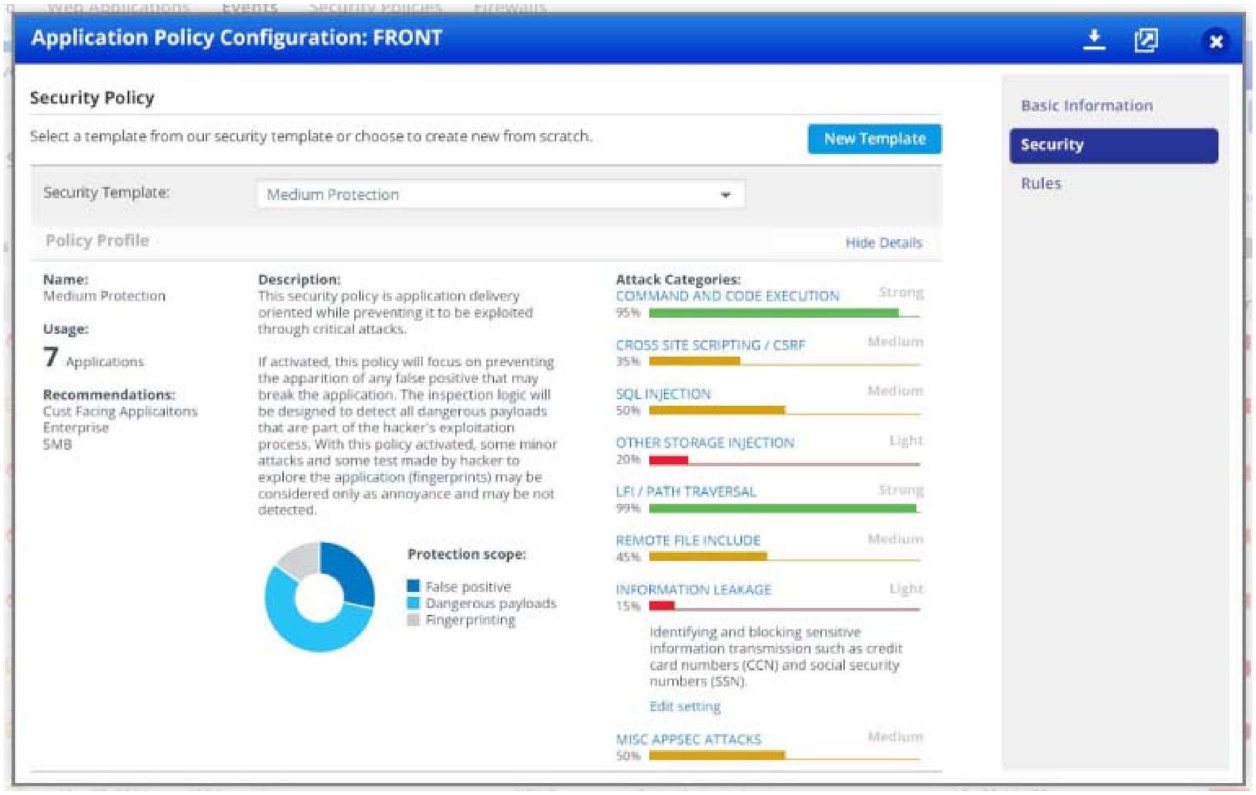
- subscription to Qualys Cloud Platform
- scanner personalization code (14 digits) obtained from your Qualys account
- Qualys Virtual Scanner Appliance VM must be able to reach the Qualys Cloud Platform over HTTPS port 443

Setup Instructions

Build: qVSA-2.3.28-1

Securing Public Cloud Infrastructure using Qualys presentation at 34, attached hereto as Exhibit 13.

203. The '731 Accused Products compare application security profiles to the security policies:



Application Policy Configuration: FRONT

Security Policy

Select a template from our security template or choose to create new from scratch.

Security Template: Medium Protection

Policy Profile

Name:
Medium Protection

Usage:
7 Applications

Recommendations:
Cust Facing Applicaitons
Enterprise
SMB

Description:
This security policy is application delivery oriented while preventing it to be exploited through critical attacks.

If activated, this policy will focus on preventing the apparition of any false positive that may break the application. The inspection logic will be designed to detect all dangerous payloads that are part of the hacker's exploitation process. With this policy activated, some minor attacks and some test made by hacker to explore the application (fingerprints) may be considered only as annoyance and may be not detected.

Protection scope:
- False positive
- Dangerous payloads
- Fingerprinting

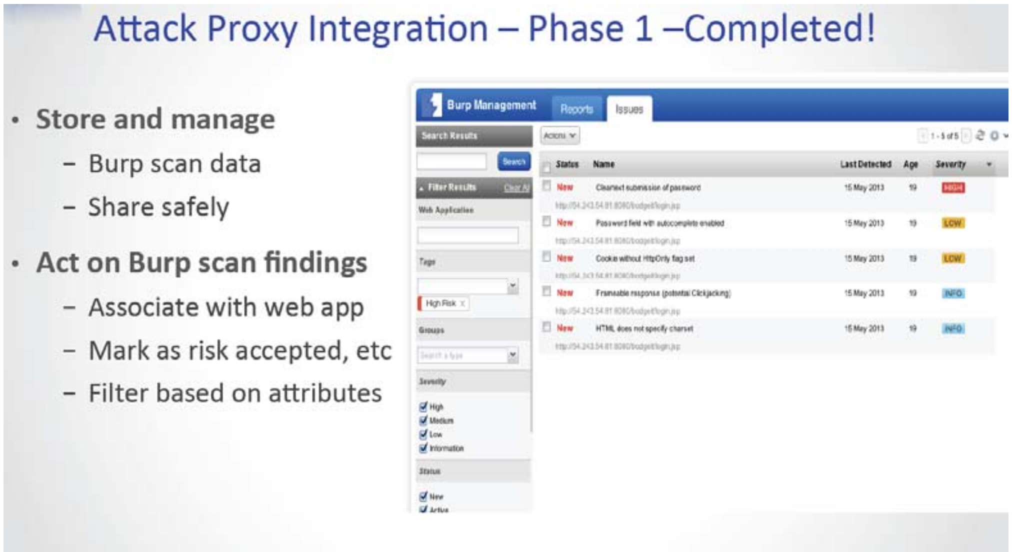
Attack Categories:

COMMAND AND CODE EXECUTION	95%	Strong
CROSS SITE SCRIPTING / CSRF	35%	Medium
SQL INJECTION	50%	Medium
OTHER STORAGE INJECTION	20%	Light
LFI / PATH TRAVERSAL	99%	Strong
REMOTE FILE INCLUDE	45%	Medium
INFORMATION LEAKAGE	15%	Light
MISC APPSEC ATTACKS	50%	Medium

Identifying and blocking sensitive information transmission such as credit card numbers (CCN) and social security numbers (SSN).

https://www.qualys.com/apps/web-app-firewall/, attached hereto as Exhibit 16.

204. The '731 Accused Products store policy index (high/low risk) data including entries that relate cache content and policies:



Attack Proxy Integration – Phase 1 –Completed!

- Store and manage
  - Burp scan data
  - Share safely
- Act on Burp scan findings
  - Associate with web app
  - Mark as risk accepted, etc
  - Filter based on attributes

Severity: ☑ High ☑ Medium ☑ Low ☑ Information

Status: ☑ New ☑ Active

Status	Name	Last Detected	Age	Severity
New	Cleartext submission of password http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	HIGH
New	Password field with autocomplete enabled http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	LOW
New	Cookie without HttpOnly flag set http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	LOW
New	Frameable response (potential Clickjacking) http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	INFO
New	HTML does not specify charset http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	INFO

QualysGuard Web Application Security presentation at 8, attached hereto as Exhibit 8.

205. Defendant's infringement of the '731 Patent has injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty. Additionally, as a result of Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendant compete in the security software space, and Finjan is actively engaged in licensing its patent portfolio. Defendant's continued infringement of the '731 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.

206. Defendant has been long-aware of Finjan's patents, including the '731 Patent, and continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendant for nearly three years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that its products infringe Finjan's patents, on information and belief Defendant made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendant's blatant and egregious disregard for Finjan's patent rights.

207. Despite its knowledge of Finjan's patent portfolio and Asserted Patents, and its specific knowledge of its own infringement, Defendant continued to sell the '731 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 '731 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 XII
(Indirect Infringement of the '731 Patent pursuant to 35 U.S.C. § 271(b))

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

209. In addition to directly infringing the '731 Patent, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 7-12, 14-16, and 20-21 of the '731 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its customers to perform the steps of the method claims of the '731 Patent, either literally or under the doctrine of equivalents.

210. Additionally, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 7-12, 14-16, and 20-21 of the '731 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its developers to perform the steps of the method claims of the '731 Patent, either literally or under the doctrine of equivalents.

211. Defendant knowingly and actively aided and abetted the direct infringement of the '731 Patent by instructing and encouraging its customers and developers to use the '731 Accused Products. Such instructions and encouragement included advising third parties to use the '731 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '731 Patent, and by advertising and promoting the use of the '731 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '731 Accused Products in an infringing manner. *See, e.g.*, QualysGuard Web Application Security presentation, attached hereto as Exhibit 8; https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10; QualysGuard InfoDay 2014 presentation, attached hereto as Exhibit 12; Securing Public Cloud Infrastructure using Qualys presentation, attached hereto as Exhibit 13; Qualys Web Application Scanning Getting Started Guide Version 6.0.1, attached hereto as Exhibit 15; https://www.qualys.com/apps/web-app-firewall/, attached hereto as Exhibit 16; https://www.qualys.com/apps/policy-compliance/, attached hereto as Exhibit 17; https://www.qualys.com/apps/web-app-scanning/, attached hereto as Exhibit 19; https://www.musingitoutloud.com/powershell-ssl-labs/, attached hereto as Exhibit 21.

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

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

213. Defendant has infringed and continues to infringe Claims 1-12 of the '154 Patent in violation of 35 U.S.C. § 271(a).

214. Defendant's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

215. Defendant's 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.

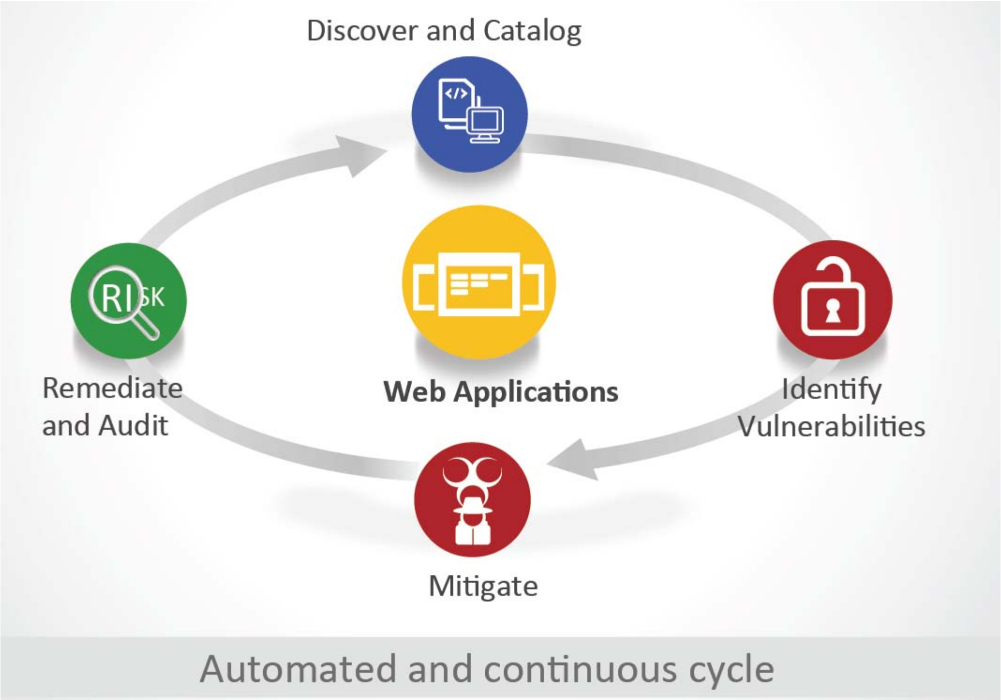
216. Defendant's infringement includes the manufacture, use, sale, importation and offer for sale of Defendant's products and services that utilize Vulnerability Management, Threat Protection, Continuous Monitoring, Indicators of Compromise, Container Security, Web App Firewall, Web App Scanning, and Compliance Monitoring, including Qualys Cloud Platform products (collectively, "the '154 Accused Products").

217. 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 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.

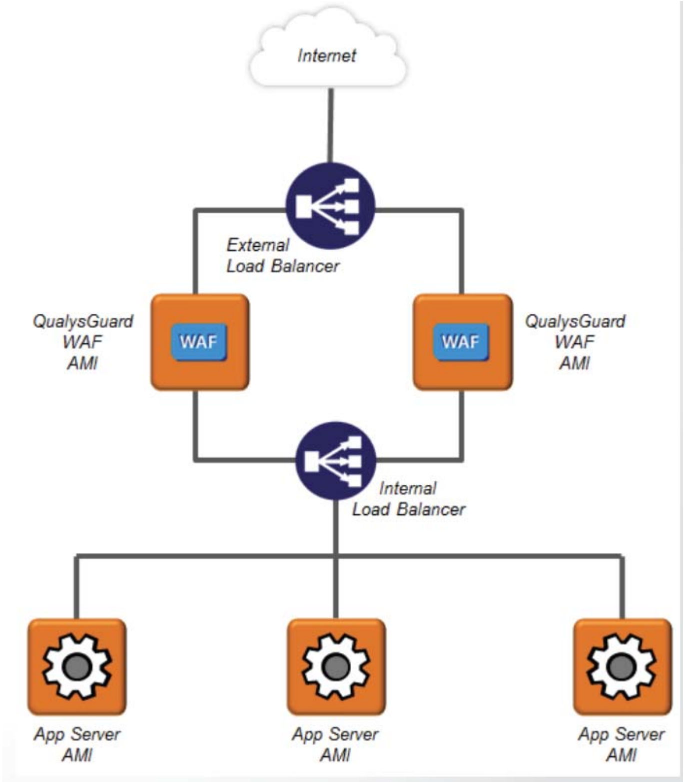
218. To the extent the '154 Accused Products use a system that includes modules, components or software owned by third parties, the '154 Accused Products still infringe the '154 Patent because Defendant is vicariously liable for the use of the patented system by controlling the entire system and deriving a benefit from the use of every element of the entire system. Similarly, to the extent Defendant's 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, Defendant's '154 Accused Products still infringe 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.

219. The '154 Accused Products are systems for protecting computers from dynamically generated malicious content.

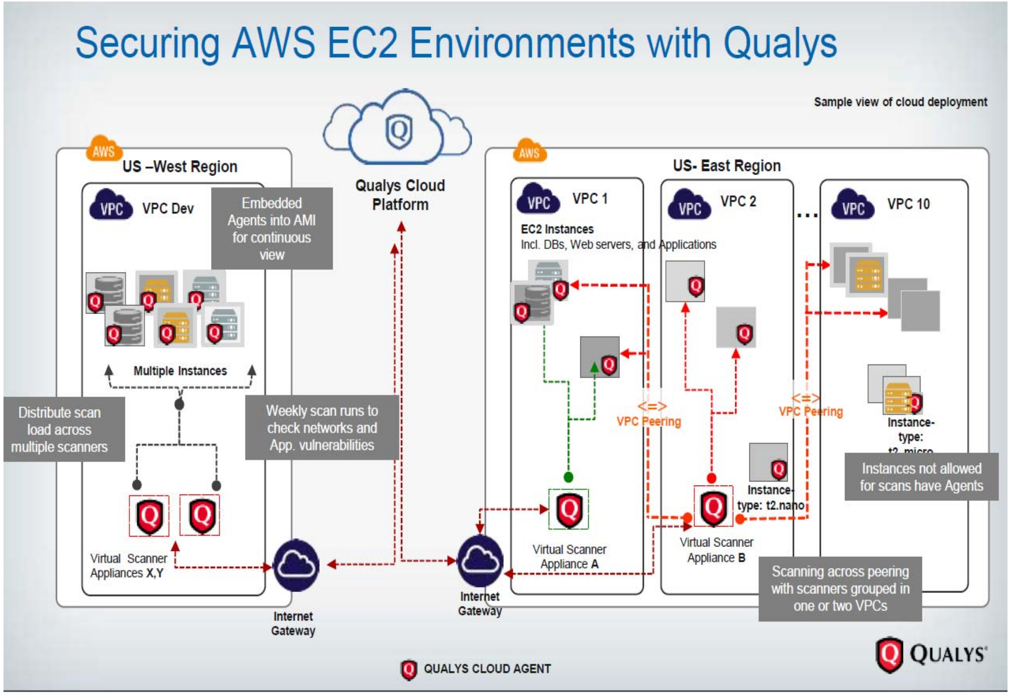


QualysGuard Web Application Security presentation at 5, attached hereto as Exhibit 8.



QualysGuard Web Application Security presentation at 30, attached hereto as Exhibit 8.

220. The '154 Accused Products dynamically scan and evaluate content, including dynamically generated malicious content:



Securing AWS EC2 Environments with Qualys

Sample view of cloud deployment

Embedded Agents into AMI for continuous view

Distribute scan load across multiple scanners

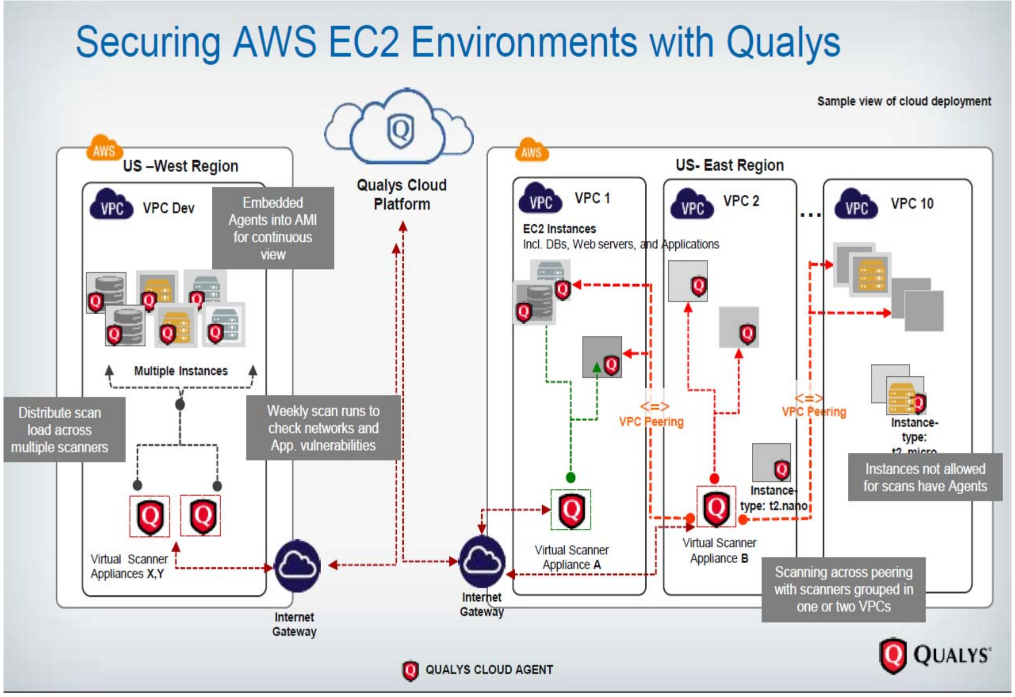
Weekly scan runs to check networks and App. vulnerabilities

Instances not allowed for scans have Agents

Scanning across peering with scanners grouped in one or two VPCs

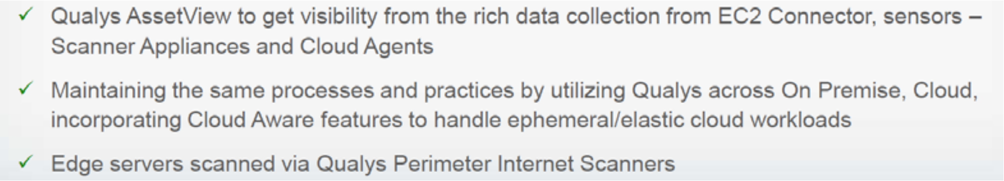
Securing Public Cloud Infrastructure using Qualys presentation at 29, attached hereto as Exhibit 13.

221. The '154 Accused Products include a content processor for processing content received over a network, the content including a call to a first function, and the call including an input, and for invoking a second function with the input if a security computer indicates that such invocation is safe:



Securing AWS EC2 Environments with Qualys

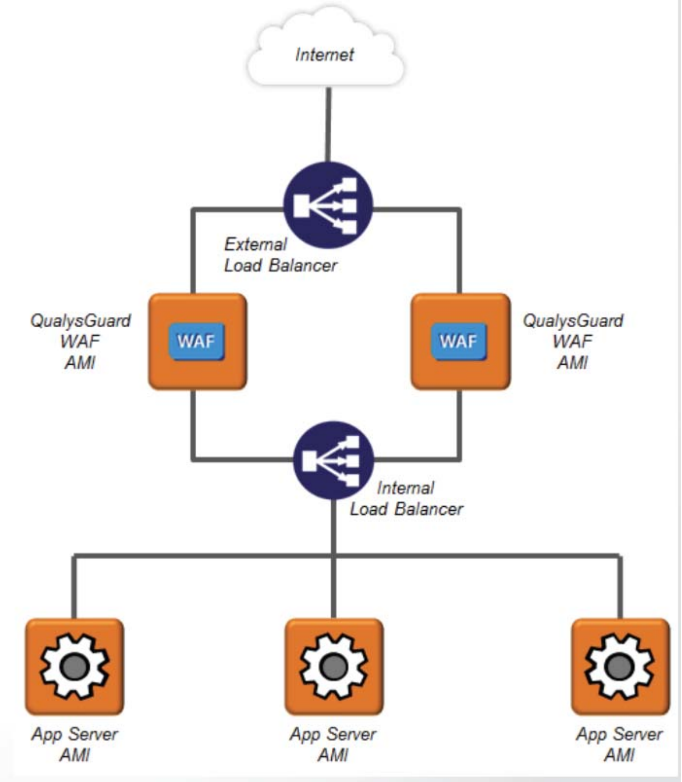
Sample view of cloud deployment
AWS
US –West Region
VPC
VPC Dev
Embedded Agents into AMI for continuous view
Multiple Instances
Distribute scan load across multiple scanners
Weekly scan runs to check networks and App. vulnerabilities
Virtual Scanner Appliances X,Y
Internet Gateway
Qualys Cloud Platform
AWS
US- East Region
VPC 1
EC2 Instances
Incl. DBs, Web servers, and Applications
VPC 2
VPC 10
<=> VPC Peering
<=> VPC Peering
Instance-type: t2.micro
Instances not allowed for scans have Agents
Instance-type: t2.nano
Virtual Scanner Appliance A
Virtual Scanner Appliance B
Internet Gateway
Scanning across peering with scanners grouped in one or two VPCs
QUALYS CLOUD AGENT
QUALYS



- ✓ Qualys AssetView to get visibility from the rich data collection from EC2 Connector, sensors – Scanner Appliances and Cloud Agents
- ✓ Maintaining the same processes and practices by utilizing Qualys across On Premise, Cloud, incorporating Cloud Aware features to handle ephemeral/elastic cloud workloads
- ✓ Edge servers scanned via Qualys Perimeter Internet Scanners

Securing Public Cloud Infrastructure using Qualys presentation at 28-29, attached hereto as Exhibit 13.

222. The '154 Accused Products process received content which can include a call to a first function including an input:



QualysGuard Web Application Security presentation at 30, attached hereto as Exhibit 8.

223. Network mapping is an essential step in discovering vulnerabilities and consists of enumeration of all IP addresses in registered networks in an attempt to find live hosts. Network mapping is implemented using QualysGuard Vulnerability Management Scans – Maps:

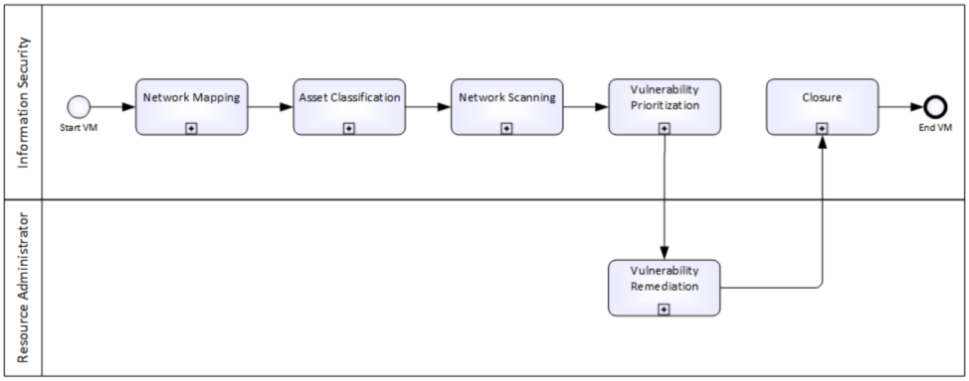
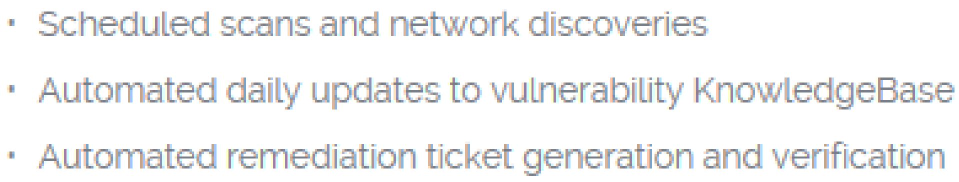
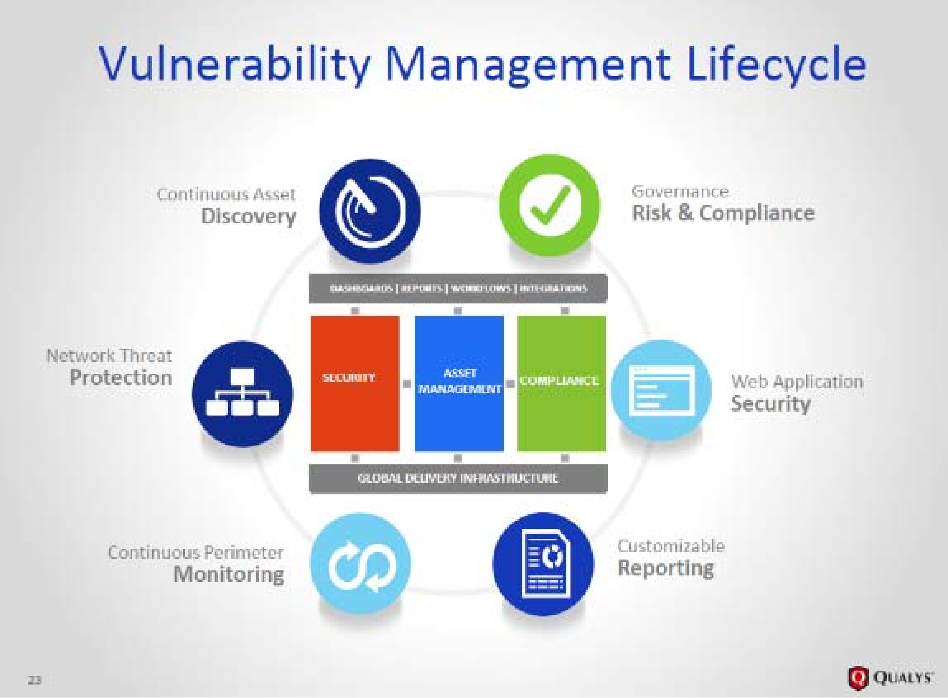


Figure 1: Vulnerability management process

https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.



- Scheduled scans and network discoveries
- Automated daily updates to vulnerability KnowledgeBase
- Automated remediation ticket generation and verification



Vulnerability Management Lifecycle

Continuous Asset Discovery

Governance Risk & Compliance

DASHBOARDS | REPORTS | WORKFLOWS | INTEGRATIONS

SECURITY

ASSET MANAGEMENT

COMPLIANCE

GLOBAL DELIVERY INFRASTRUCTURE

Network Threat Protection

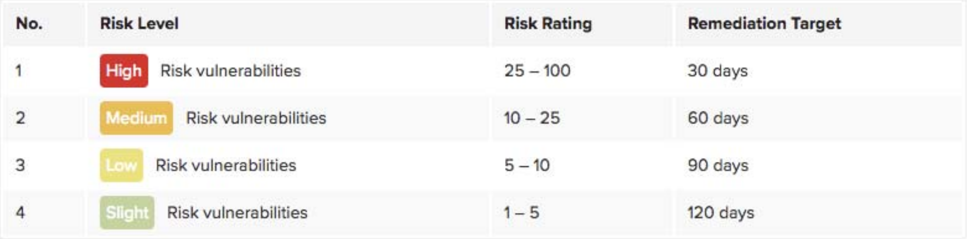
Web Application Security

Continuous Perimeter Monitoring

Customizable Reporting

https://www.dts-solution.com/solutions/compliance-monitoring/vulnerability-management/, attached hereto as Exhibit 9.

224. The '154 Accused Products invoke a second function with an input, only if a security computer indicates that such invocation is safe:

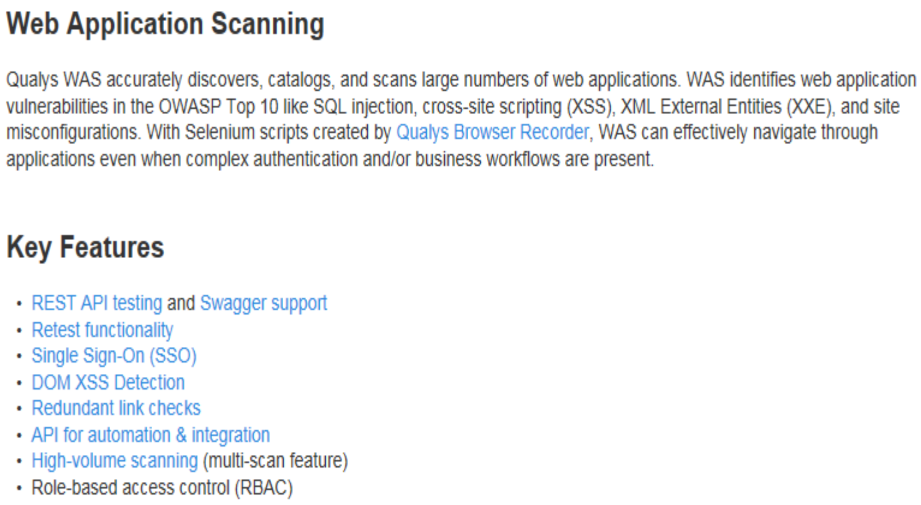


No.	Risk Level	Risk Rating	Remediation Target
1	High Risk vulnerabilities	25 – 100	30 days
2	Medium Risk vulnerabilities	10 – 25	60 days
3	Low Risk vulnerabilities	5 – 10	90 days
4	Slight Risk vulnerabilities	1 – 5	120 days

Table 3: Remediation targets

https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.

225. The ‘154 Accused Products scan, discover and catalog applications searching for portions of program code that are malicious according to analyzer rules (such as SQL injection, cross-site scripting (XSS), XML External Entities (XXE) and site misconfigurations):



Web Application Scanning

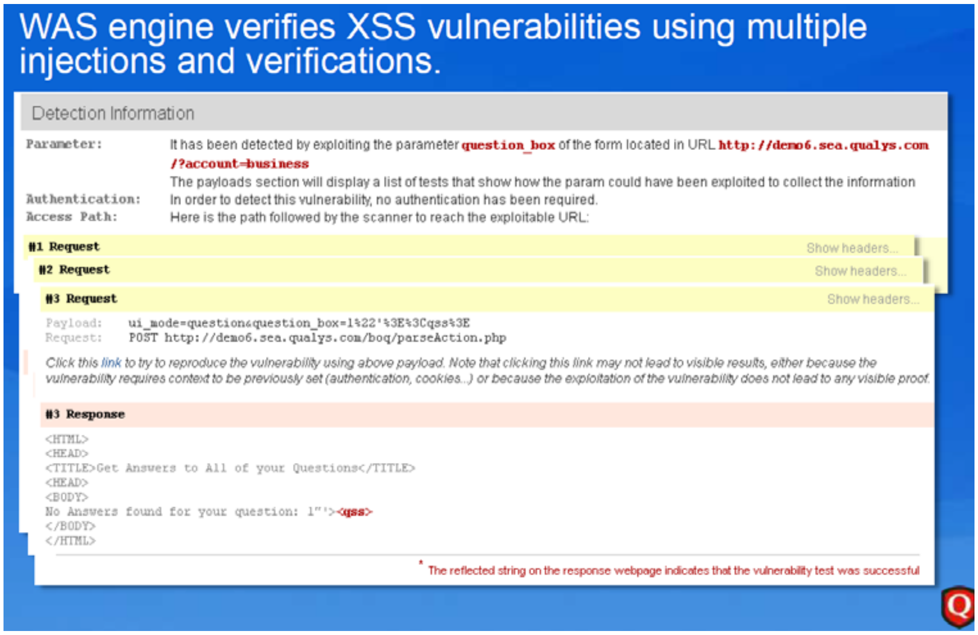
Qualys WAS accurately discovers, catalogs, and scans large numbers of web applications. WAS identifies web application vulnerabilities in the OWASP Top 10 like SQL injection, cross-site scripting (XSS), XML External Entities (XXE), and site misconfigurations. With Selenium scripts created by Qualys Browser Recorder, WAS can effectively navigate through applications even when complex authentication and/or business workflows are present.

Key Features

- REST API testing and Swagger support
- Retest functionality
- Single Sign-On (SSO)
- DOM XSS Detection
- Redundant link checks
- API for automation & integration
- High-volume scanning (multi-scan feature)
- Role-based access control (RBAC)

https://community.qualys.com/community/web-application-scanning, attached hereto as Exhibit 11.

226. The ‘154 Accused Products scan incoming content received by the network interface to recognize the presence of potential computer exploits:



WAS engine verifies XSS vulnerabilities using multiple injections and verifications.

Detection Information

Parameter: It has been detected by exploiting the parameter **question_box** of the form located in URL **http://demo6.sea.qualys.com/?account=business**
The payloads section will display a list of tests that show how the param could have been exploited to collect the information
Authentication: In order to detect this vulnerability, no authentication has been required.
Access Path: Here is the path followed by the scanner to reach the exploitable URL:

#1 Request Show headers...

#2 Request Show headers...

#3 Request Show headers...

```
Payload:   ui_mode=question&question_box=1%22'%3E%3Cqss%3E
Request:   POST http://demo6.sea.qualys.com/boq/parseAction.php
```

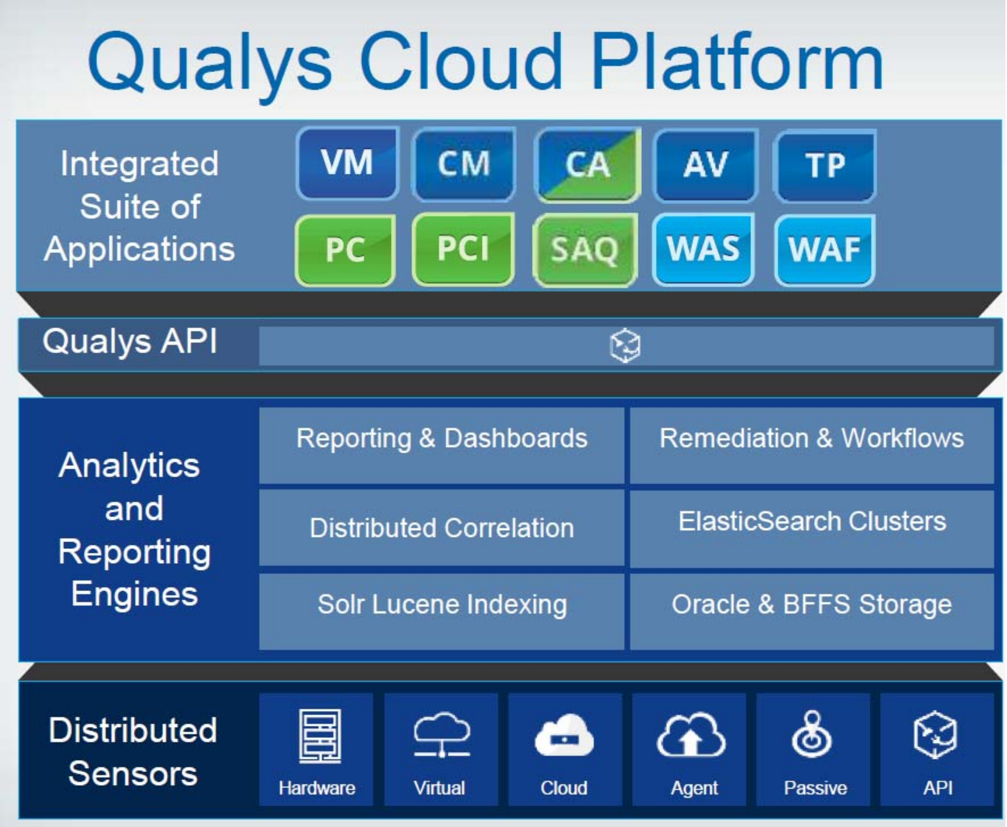
Click this link to try to reproduce the vulnerability using above payload. Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#3 Response

```
<HTML>
<HEAD>
<TITLE>Get Answers to All of your Questions</TITLE>
<HEAD>
<BODY>
No Answers found for your question: 1"'><qss>
</BODY>
</HTML>
```

* The reflected string on the response webpage indicates that the vulnerability test was successful

QualysGuard InfoDay 2014 presentation at 29, attached hereto as Exhibit 12.



Qualys Cloud Platform

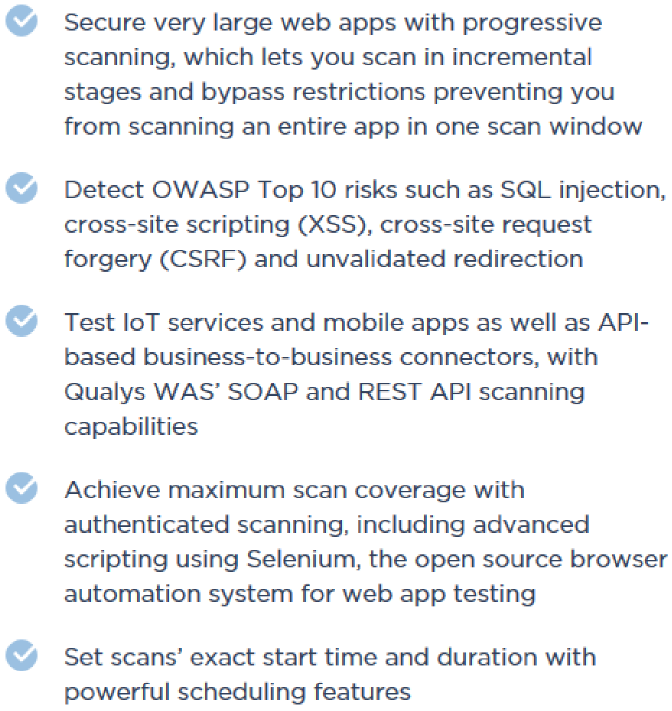
Integrated Suite of Applications

Qualys API

Analytics and Reporting Engines

Distributed Sensors

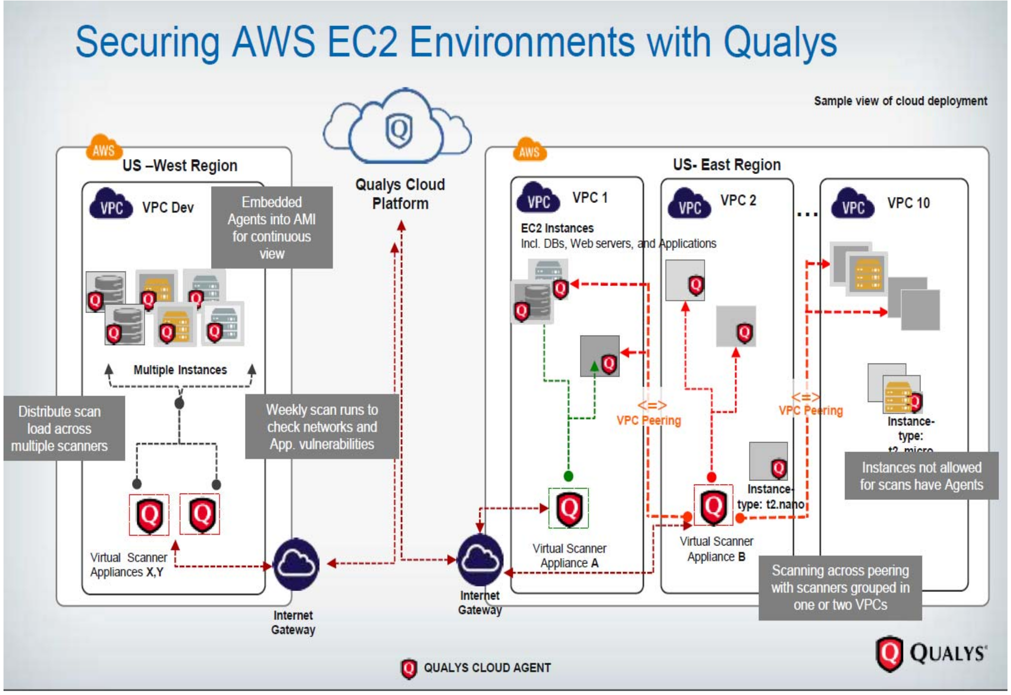
Securing Public Cloud Infrastructure using Qualys presentation at 12, attached hereto as Exhibit 13.



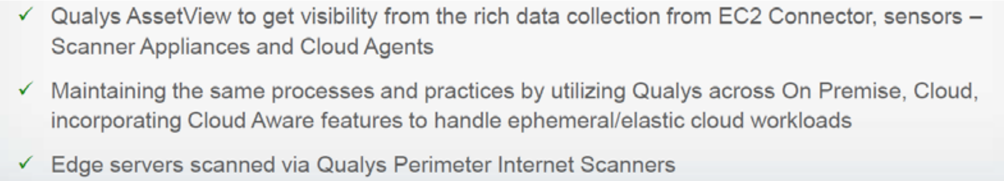
- ✓ Secure very large web apps with progressive scanning, which lets you scan in incremental stages and bypass restrictions preventing you from scanning an entire app in one scan window
- ✓ Detect OWASP Top 10 risks such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF) and unvalidated redirection
- ✓ Test IoT services and mobile apps as well as API-based business-to-business connectors, with Qualys WAS' SOAP and REST API scanning capabilities
- ✓ Achieve maximum scan coverage with authenticated scanning, including advanced scripting using Selenium, the open source browser automation system for web app testing
- ✓ Set scans' exact start time and duration with powerful scheduling features

https://www.qualys.com/apps/web-app-scanning/, attached hereto as Exhibit 19.

227. The ‘154 Accused Products include a transmitter for transmitting input to a security computer (such as the Qualys Cloud) for inspection, when a first function is invoked.

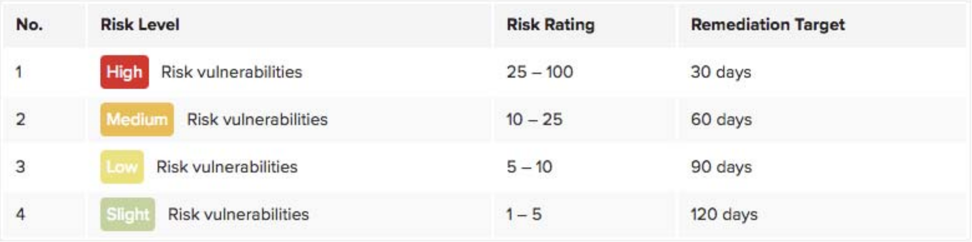

Securing AWS EC2 Environments with Qualys

Sample view of cloud deployment
AWS
US –West Region
VPC
VPC Dev
Embedded Agents into AMI for continuous view
Multiple Instances
Distribute scan load across multiple scanners
Weekly scan runs to check networks and App. vulnerabilities
Virtual Scanner Appliances X,Y
Internet Gateway
Qualys Cloud Platform
Internet Gateway
AWS
US- East Region
VPC 1
EC2 Instances
Incl. DBs, Web servers, and Applications
VPC 2
VPC 10
<=> VPC Peering
<=> VPC Peering
Instance-type: t2.micro
Instances not allowed for scans have Agents
Instance-type: t2.nano
Virtual Scanner Appliance A
Virtual Scanner Appliance B
Scanning across peering with scanners grouped in one or two VPCs
QUALYS CLOUD AGENT
QUALYS


- ✓ Qualys AssetView to get visibility from the rich data collection from EC2 Connector, sensors – Scanner Appliances and Cloud Agents
- ✓ Maintaining the same processes and practices by utilizing Qualys across On Premise, Cloud, incorporating Cloud Aware features to handle ephemeral/elastic cloud workloads
- ✓ Edge servers scanned via Qualys Perimeter Internet Scanners

Securing Public Cloud Infrastructure using Qualys presentation at 28-29, attached hereto as Exhibit 13.

228. The ‘154 Accused Products include a receiver for receiving an indicator (risk level) from a security computer of whether it is safe to invoke a second function:

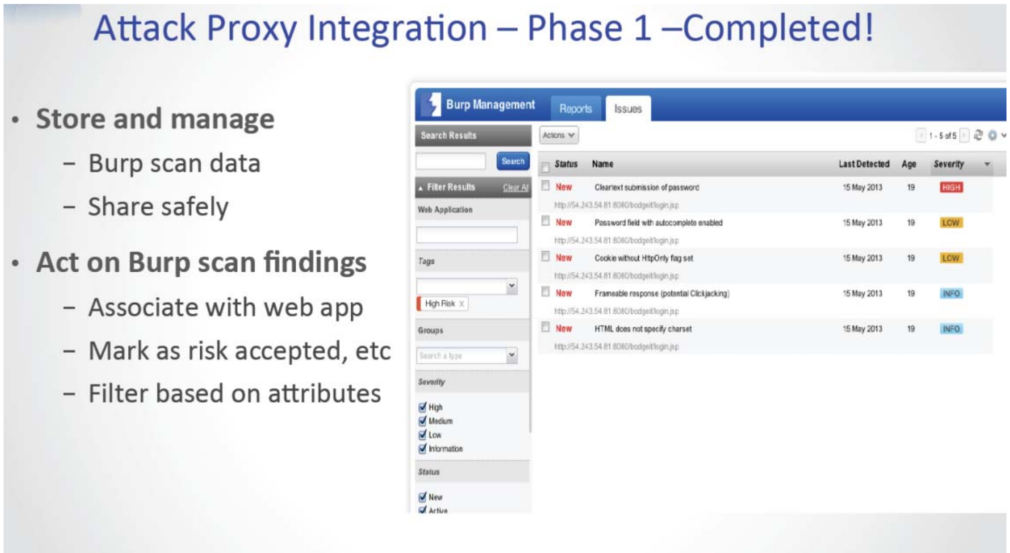


No.	Risk Level	Risk Rating	Remediation Target
1	High Risk vulnerabilities	25 – 100	30 days
2	Medium Risk vulnerabilities	10 – 25	60 days
3	Low Risk vulnerabilities	5 – 10	90 days
4	Slight Risk vulnerabilities	1 – 5	120 days

Table 3: Remediation targets

https://blog.thousandeyes.com/efficient-vulnerability-management-qualys/, attached hereto as Exhibit 10.

229. The '154 Accused Products store an indicator (risk level) including entries that relate risk report and policies:

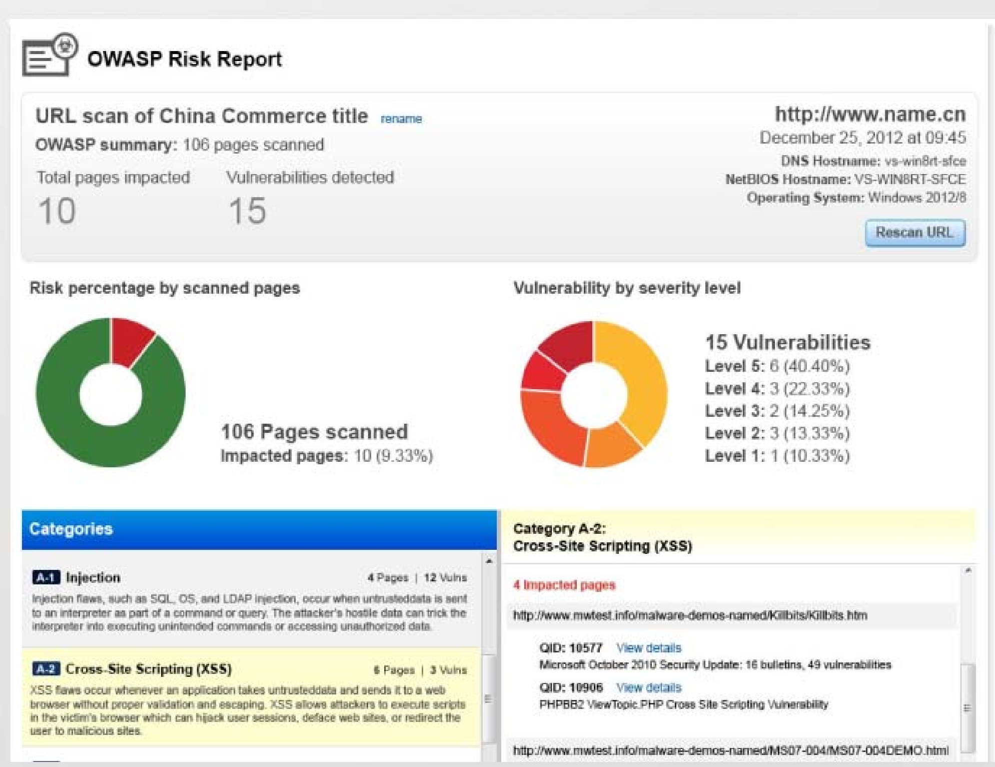


Attack Proxy Integration – Phase 1 –Completed!

- Store and manage
  - Burp scan data
  - Share safely
- Act on Burp scan findings
  - Associate with web app
  - Mark as risk accepted, etc
  - Filter based on attributes

	Status	Name	Last Detected	Age	Severity
□	New	Cleartext submission of password http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	HIGH
□	New	Password field with autocomplete enabled http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	LOW
□	New	Cookie without HttpOnly flag set http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	LOW
□	New	Frameable response (potential Clickjacking) http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	INFO
□	New	HTML does not specify charset http://54.243.54.81:8080/bodgeit/login.jsp	15 May 2013	19	INFO

QualysGuard Web Application Security presentation at 8, attached hereto as Exhibit 8.



OWASP Risk Report

URL scan of China Commerce title rename
OWASP summary: 106 pages scanned

Total pages impacted: 10
Vulnerabilities detected: 15

http://www.name.cn
December 25, 2012 at 09:45
DNS Hostname: vs-win8rt-sfce
NetBIOS Hostname: VS-WIN8RT-SFCE
Operating System: Windows 2012/8

Risk percentage by scanned pages

106 Pages scanned
Impacted pages: 10 (9.33%)

Vulnerability by severity level

15 Vulnerabilities
Level 5: 6 (40.40%)
Level 4: 3 (22.33%)
Level 3: 2 (14.25%)
Level 2: 3 (13.33%)
Level 1: 1 (10.33%)

Categories

A-1 Injection 4 Pages | 12 Vulns
Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusteddata is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.

A-2 Cross-Site Scripting (XSS) 6 Pages | 3 Vulns
XSS flaws occur whenever an application takes untrusteddata and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

**Category A-2:
Cross-Site Scripting (XSS)**

4 Impacted pages

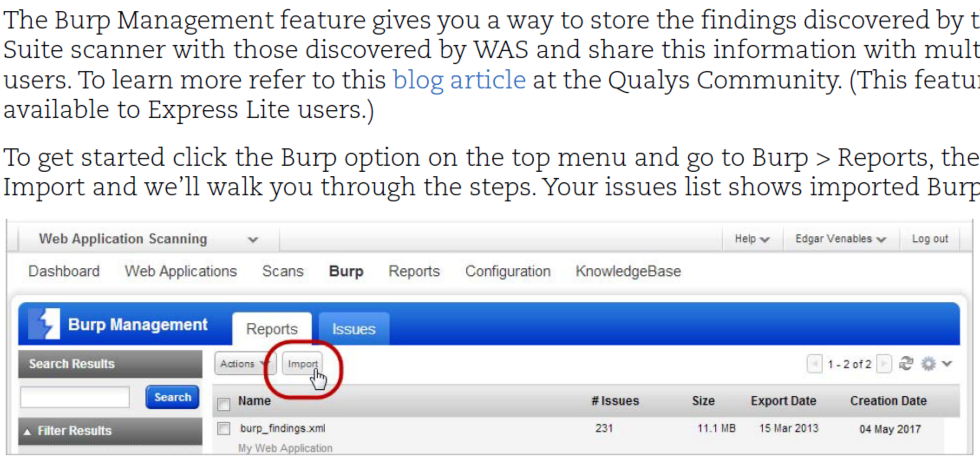
http://www.mwtest.info/malware-demos-named/Killbits/Killbits.htm

QID: 10577 View details
Microsoft October 2010 Security Update: 16 bulletins, 49 vulnerabilities

QID: 10906 View details
PHPBB2 ViewTopic.PHP Cross Site Scripting Vulnerability

http://www.mwtest.info/malware-demos-named/MS07-004/MS07-004DEMO.html https://www.qualys.com/apps/web-app-scanning/, attached hereto as Exhibit 19.

230. If the security computer indicates that it is safe to invoke the second function with the input, the '154 Accused Products make that input available to the user:

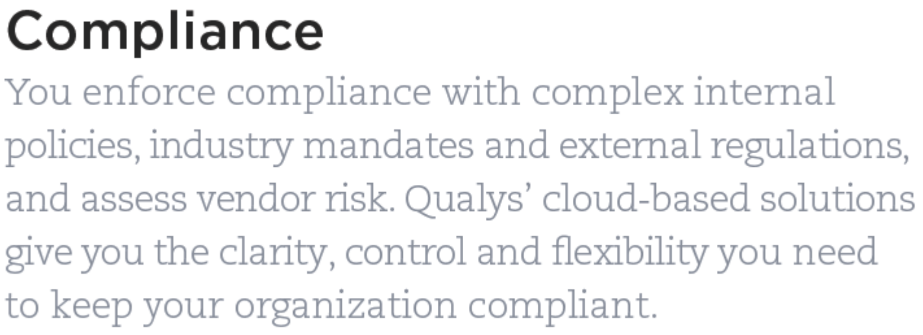


The Burp Management feature gives you a way to store the findings discovered by the Burp Suite scanner with those discovered by WAS and share this information with multiple users. To learn more refer to this blog article at the Qualys Community. (This feature is not available to Express Lite users.)

To get started click the Burp option on the top menu and go to Burp > Reports, then click Import and we'll walk you through the steps. Your issues list shows imported Burp issues.

Name	# Issues	Size	Export Date	Creation Date
burp_findings.xml My Web Application	231	11.1 MB	15 Mar 2013	04 May 2017

Qualys Web Application Scanning Getting Started Guide Version 6.0.1 at 20, attached hereto as Exhibit 15.



Compliance

You enforce compliance with complex internal policies, industry mandates and external regulations, and assess vendor risk. Qualys' cloud-based solutions give you the clarity, control and flexibility you need to keep your organization compliant.

Qualys Cloud Platform datasheet at 6, attached hereto as Exhibit 22.

231. Defendant's 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 Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendant compete in the security software space, and Finjan is actively engaged in licensing its patent portfolio. Defendant's 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.

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

233. Despite its knowledge of Finjan's patent portfolio and Asserted Patents, and its specific knowledge of its own infringement, Defendant continued to sell the '154 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 '154 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.

PRAYER FOR RELIEF

WHEREFORE, Finjan prays for judgment and relief as follows:

A. An entry of judgment holding that Defendant infringed the '844, '494, '305, '408, '968, '731, and '154 Patents; are infringing the '305, '408, '968, '731, and '154 Patents; induced infringement of the '844, '494, '305, '408, '968, and '731 Patents and are inducing infringement of the '305, '408, '968, and '731 Patents;

B. A preliminary and permanent injunction against Defendant and its officers, employees, agents, servants, attorneys, instrumentalities, and those in privity with them, from infringing the '305, '408, '968, '731, and '154 Patents, and from inducing the infringement of the '305, '408, '968, and '731 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 Defendant that is adequate to fully compensate Finjan for Defendant's infringement of the '844, '494, '305, '408, '968, '731, and '154 Patents;

D. A determination that Defendant's 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 '844, '494, '305, '408, '968, '731, and '154 Patents; and

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

Respectfully submitted,

Dated: November 29, 2018

By: *_/s/ Paul J. Andre_*

Paul J. Andre (State Bar No. 196585)
Lisa Kobialka (State Bar No. 191404)
James Hannah (State Bar No. 237978)
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com

Attorneys for Plaintiff
FINJAN, INC.

DEMAND FOR JURY TRIAL

Finjan demands a jury trial on all issues so triable.

Respectfully submitted,

Dated: November 29, 2018

By: *\/s/ Paul J. Andre*

Paul J. Andre (State Bar No. 196585)
Lisa Kobialka (State Bar No. 191404)
James Hannah (State Bar No. 237978)
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com

Attorneys for Plaintiff
FINJAN, INC.