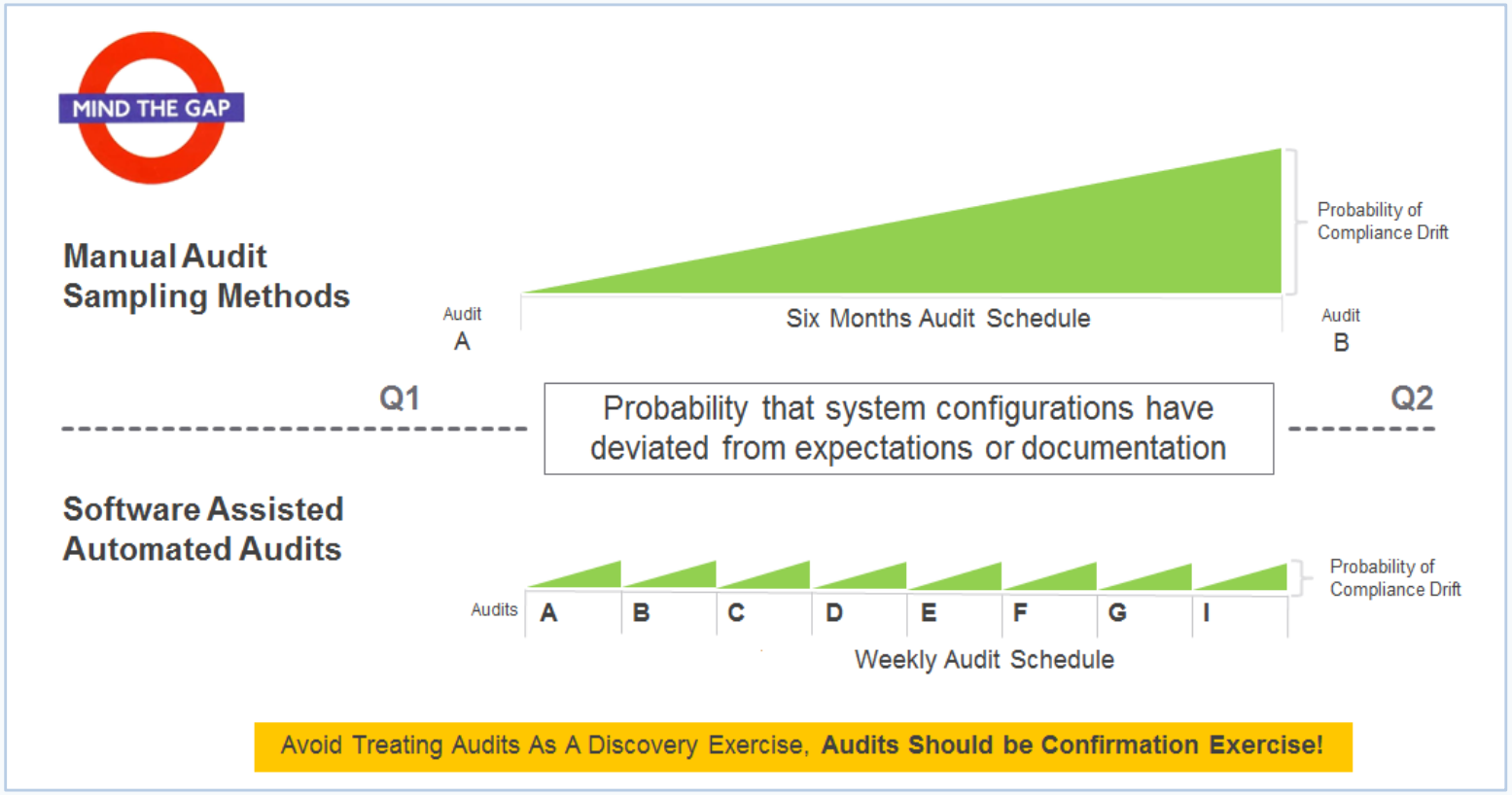
QUALYS SECURITY CONFERENCE 2019

Continuous Compliance in Hybrid Environment

New Frontier in Unified Compliance, Configuration and File Integrity Management

Shailesh Athalye
VP, Compliance Solutions, Qualys, Inc.

2014: Good Old Days of Compliance



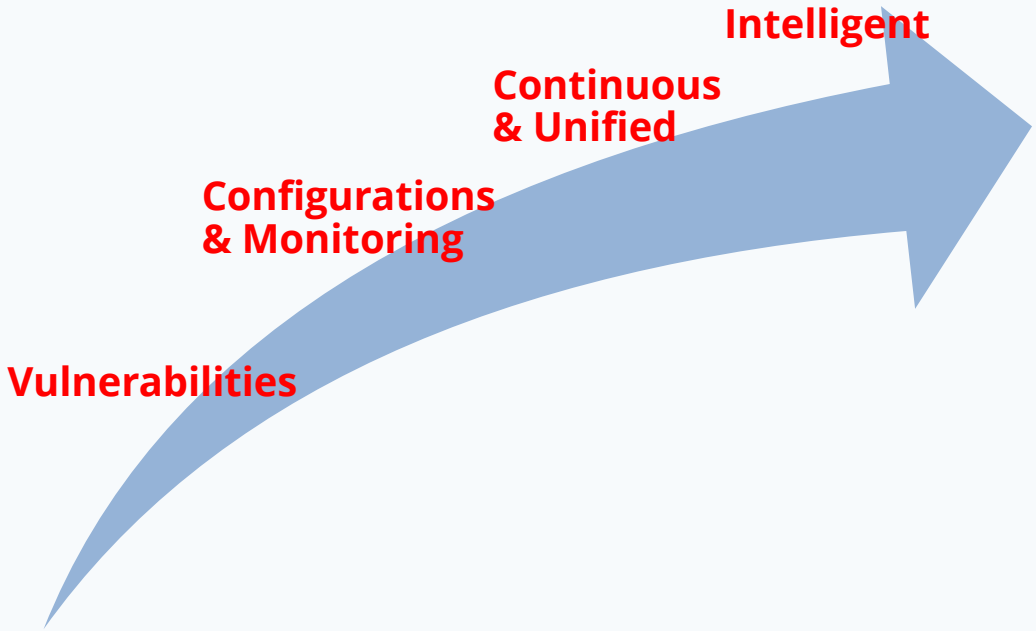
Qualys.

2019: Security is Continuous and Unified

To reduce the ‘attack surface’

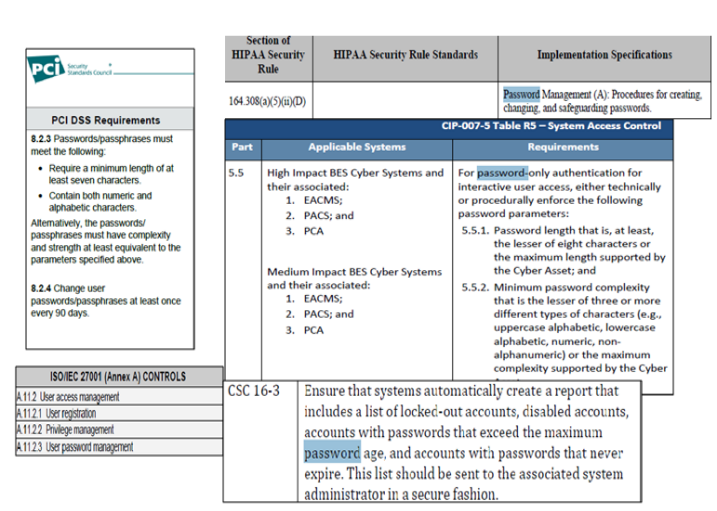
To reduce breaches due to misconfigurations, lack of monitoring

Question remains:
Is Compliance and Risk really continuous?



Qualys.

Compliance and Risk are Not Connected with Security



PCI DSS Requirements

8.2.3 Passwords/passphrases must meet the following:

- Require a minimum length of at least seven characters.
- Contain both numeric and alphabetic characters.

Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above.

8.2.4 Change user passwords/passphrases at least once every 90 days.

Section of HIPAA Security Rule	HIPAA Security Rule Standards	Implementation Specifications
164.308(a)(5)(ii)(D)		Password Management (A): Procedures for creating, changing, and safeguarding passwords.

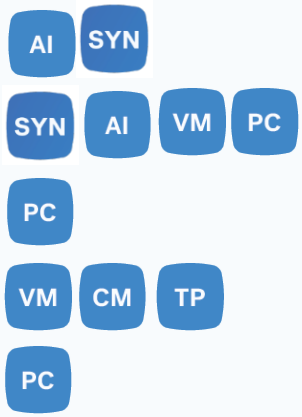
CIP-007-5 Table R5 – System Access Control

Part	Applicable Systems	Requirements
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber

ISO/IEC 27001 (Annex A) CONTROLS
A.11.2 User access management
A.11.2.1 User registration
A.11.2.2 Privilege management
A.11.2.3 User password management

CSC 16-3	Ensure that systems automatically create a report that includes a list of locked-out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire. This list should be sent to the associated system administrator in a secure fashion.

Inventory Your Systems
Inventory and Restrict Software
Secure Configurations
Continuous VM



Qualys.

Semi-automated Way for Connecting

Time to value

Time to see roll up the operational data

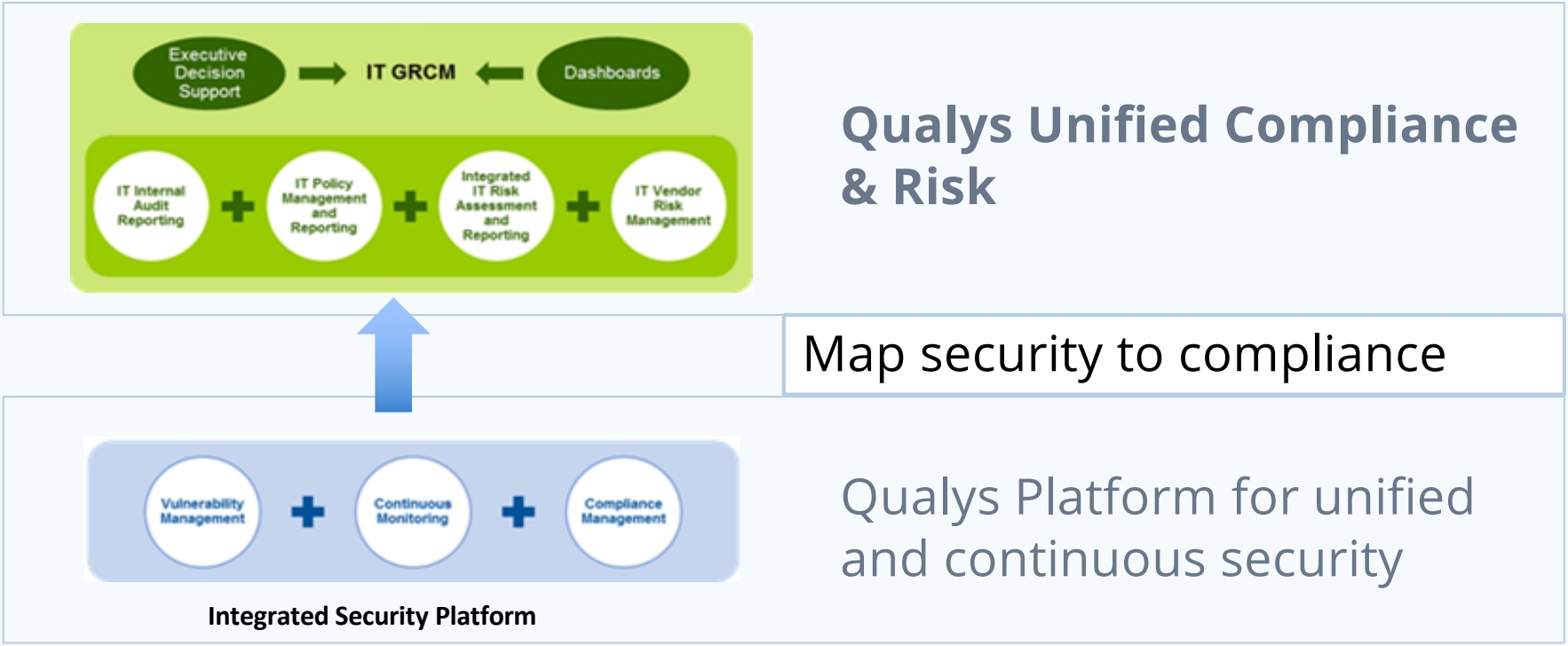
Security data of varied nature

- FIM, Patch, Malware
- Scoping and Tracking ‘In-Scope’ Assets

Application complexity with connectors

Qualys.

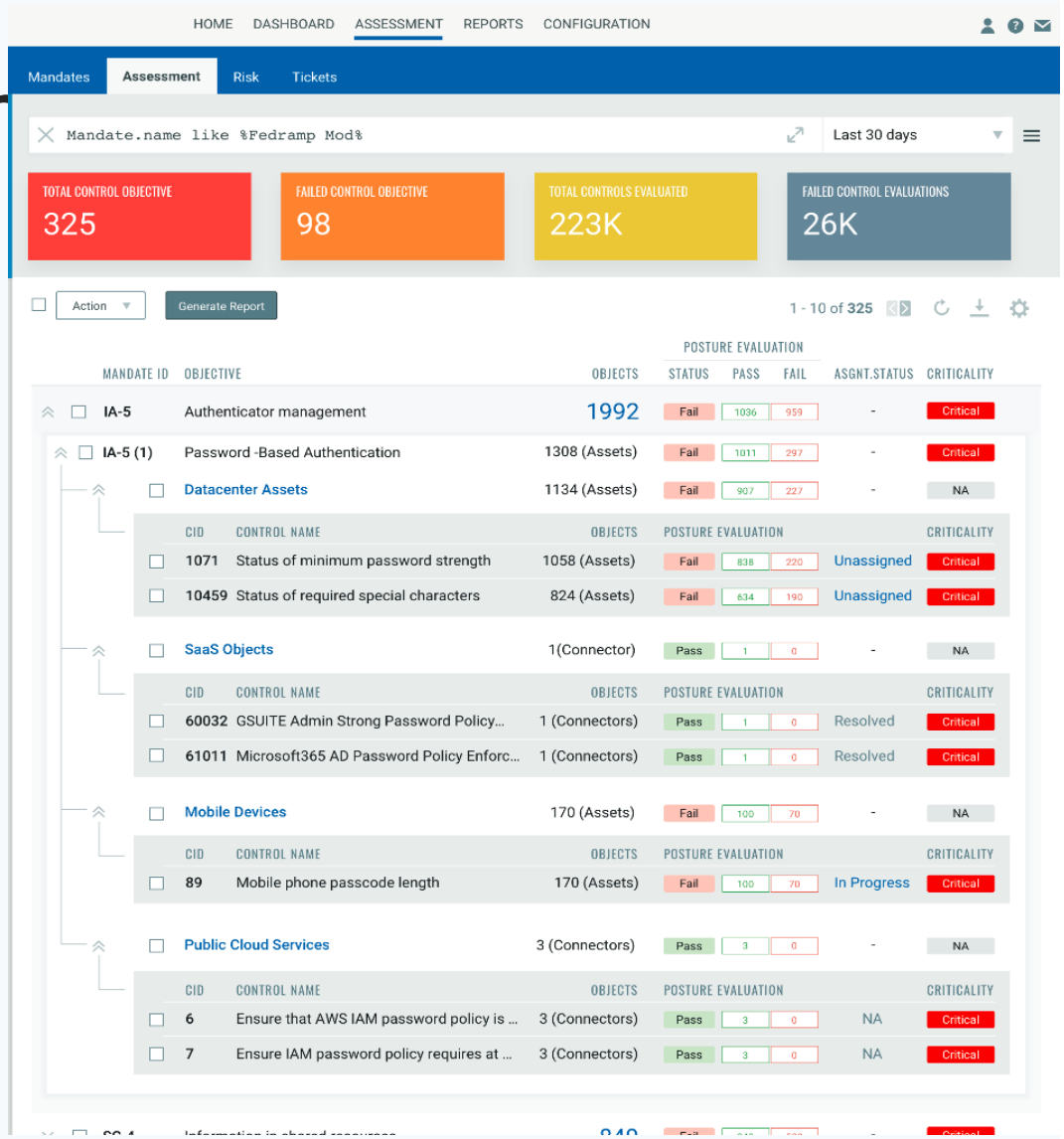
Continuous Compliance & Risk From Continuous Security



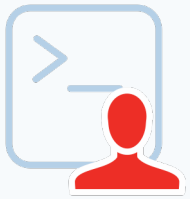
Qualys.

Continuous Compliance from Continuous Security

Qualys Unified Compliance maps every app's output to compliance requirements

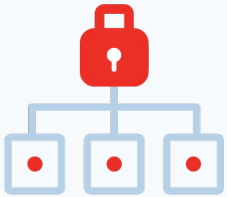


New-age Challenges: Teams Speaking Different Languages



Elastic, Kafka, custom web servers

Identify risk and compliance

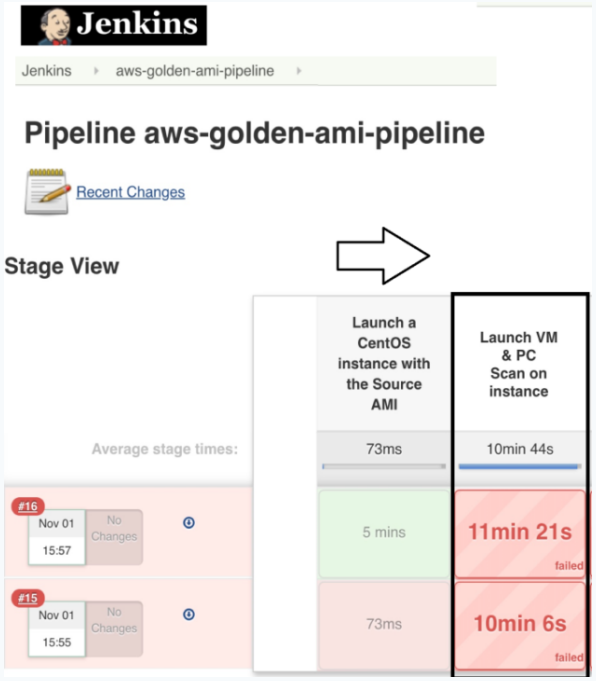


Secure hosts, config/integrity/ vulnerability management

Security & Compliance needs should be running with DevOps from the start

Qualys.

Start Compliant, Stay Compliant in DevOps with Qualys PC



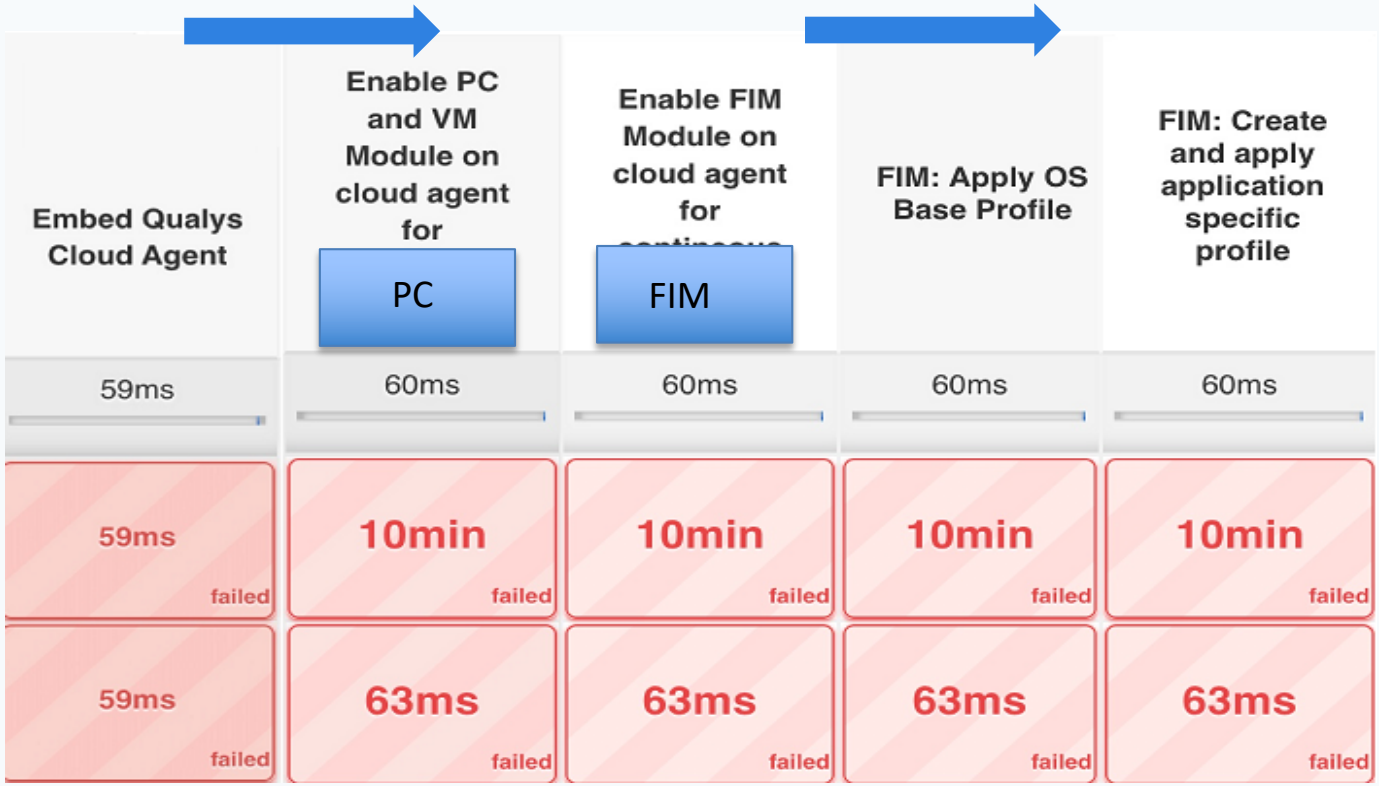
QUALYS POLICY COMPLIENCE RESULTS

Show 10 entries

CID	Title	Technology	Criticality
14602	Status of the 'nosuid' option for '/tmp' partition using 'mount' command	CentOS 7	4
10804	Status of the SELinux current mode (running configuration)	CentOS 7	4
10643	Status of iptables package	CentOS 7	4
12815	List of runtime audit rules for '/etc/passwd' file, using auditctl	CentOS 7	4
10664	Status of the 'OPTIONS' setting within '/etc/sysconfig/chronyd' file	CentOS 7	4
9473	Existence of the 'extraneous' files and directories (Sensitive files/Directories)	Tomcat 8	3
9477	Status of 'X-Powered-By' setting within 'server.xml' file	Tomcat 8	4
9551	Status of the 'secure' attribute for each 'Connector' elements whose 'SSL Enabled' are set to 'true'	Tomcat 8	4
9605	Status of the command-line flag 'STRICT_SERVLET_COMPLIANCE' set for the Tomcat process	CentOS 7	4
9565	Status of the 'web server processes' which are not started with 'Security Manager'	CentOS 7	4

Qualys.

Qualys FIM Monitors From CD Phase

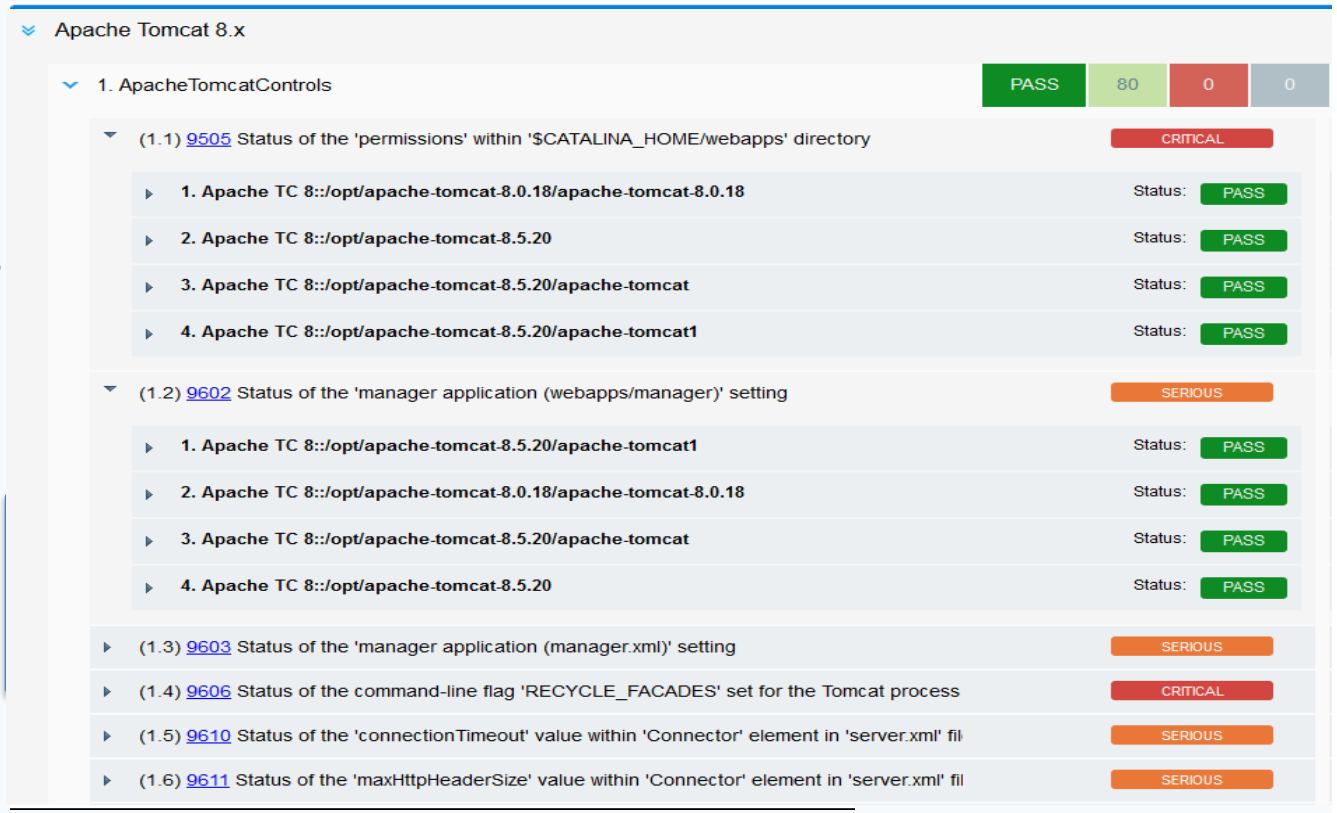


Qualys.

Discover and Assess Technologies with Dynamic Paths

Qualys PC enables automatic discovery and assessment of middleware technologies from host scans

There’s no need to create authentication records



CISO Responsibility: Ensure Security Controls are in Place and Functioning https://www.bitsight.com/blog/ciso-roles-and-responsibilities

Is Anti-virus active, updated for signatures, scanning?

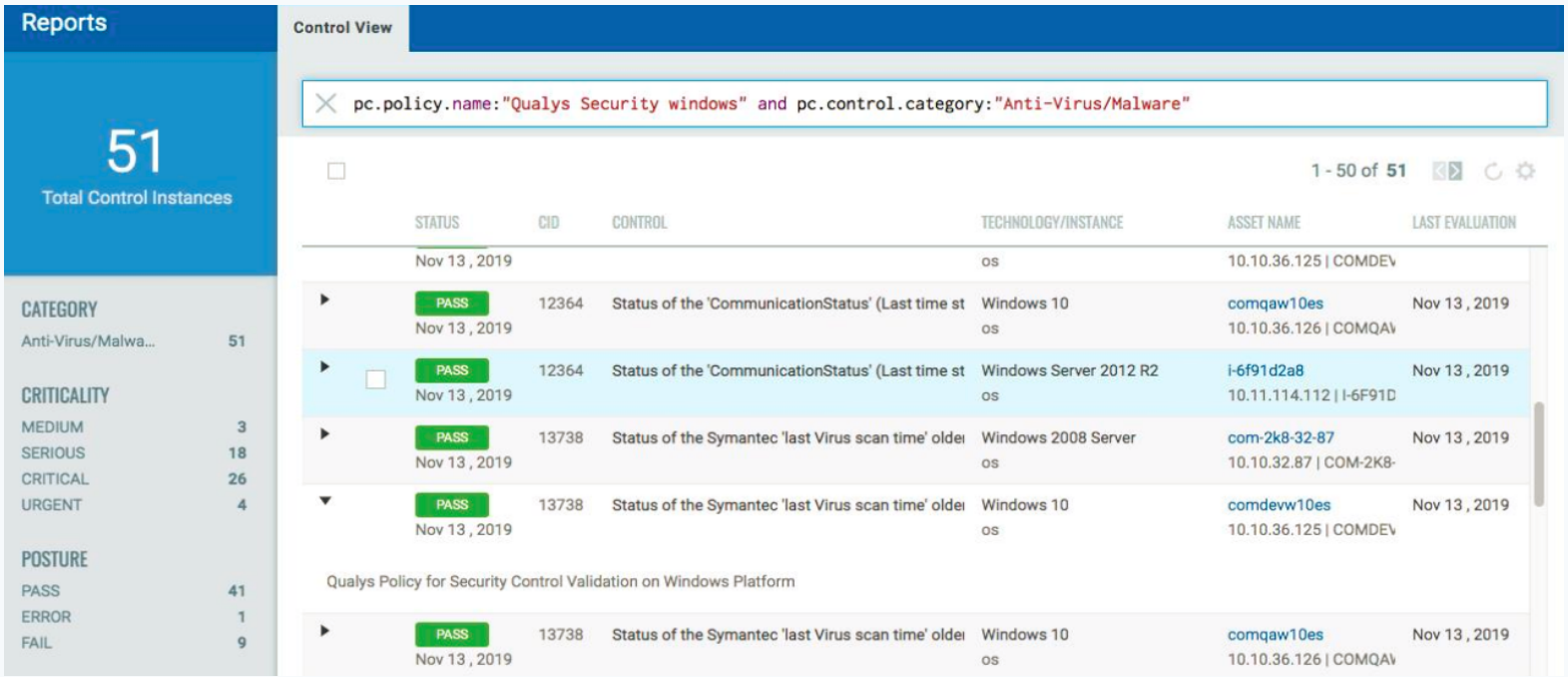
Is FIM, EDR agent configured correctly to monitor?

Are OS native application protection, memory protection configured?

Need to have Security Control Validation (SCV) in place test and confirm that security tools configured properly on all endpoints

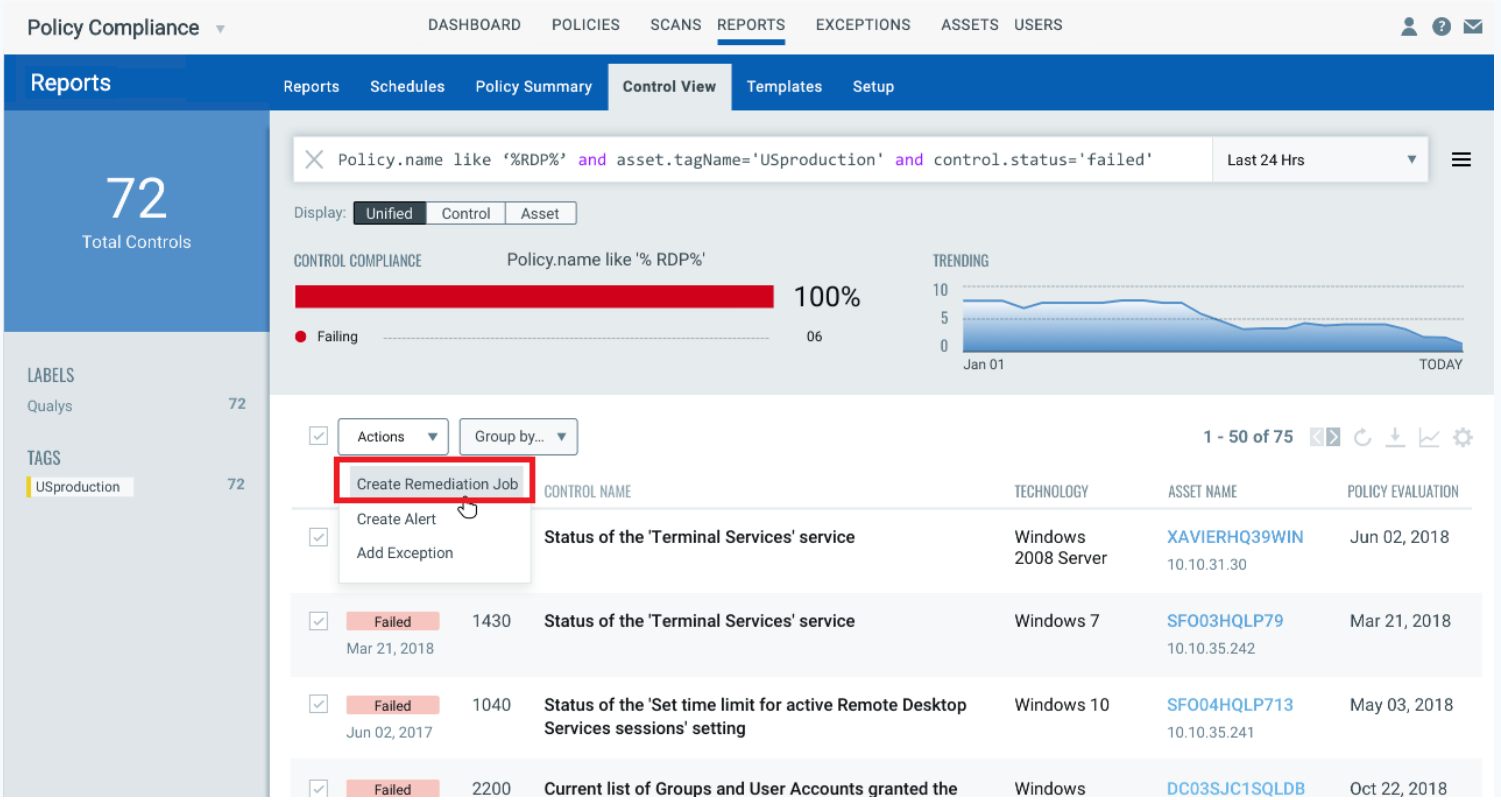
Security Control Validation from Policy Compliance

Anti-virus technologies | Qualys FIM Agent | Splunk | Kafka | Native Malware Protection



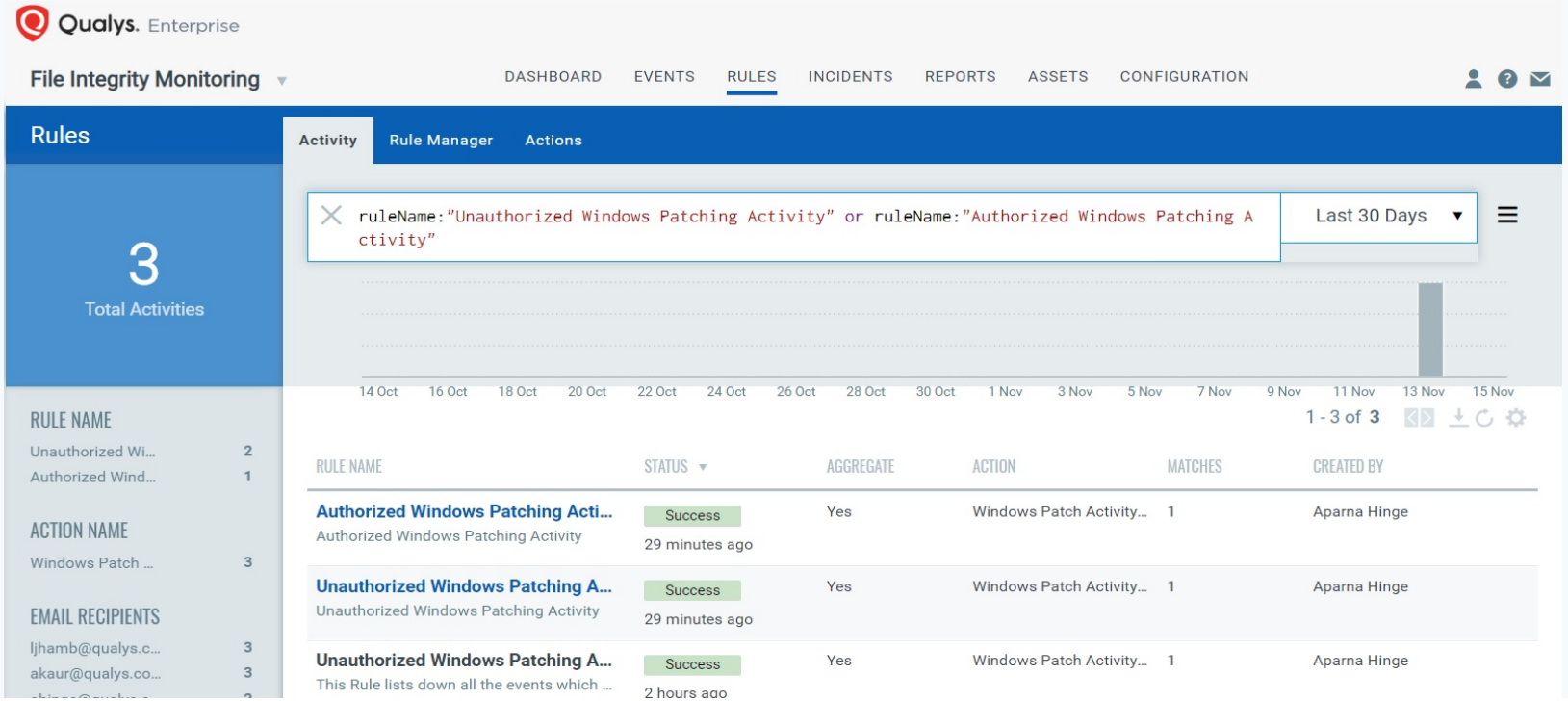
Qualys.

Start Gold, Continuously Assess, Remediate



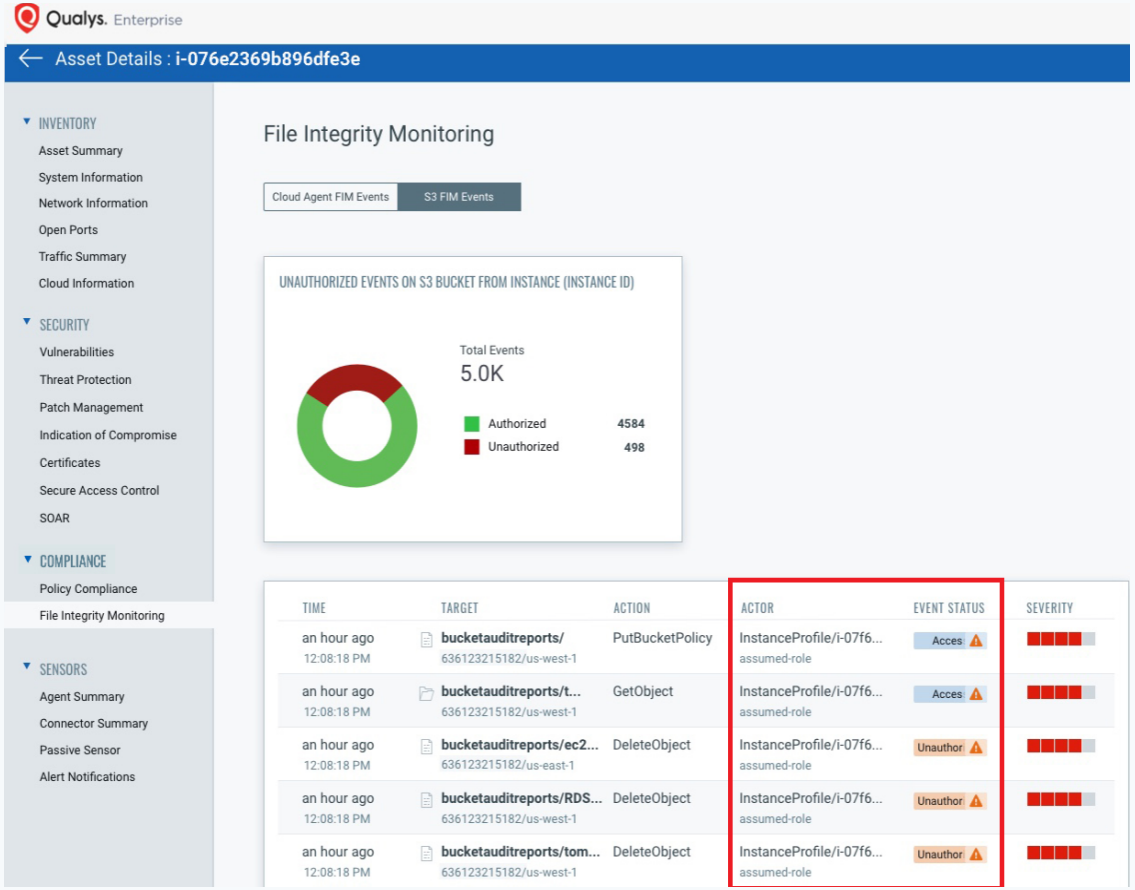
Qualys.

Alert and Incident Management for Authorized vs Unauthorized Changes During Patching



Qualys.

FIM gives context of changes in cloud



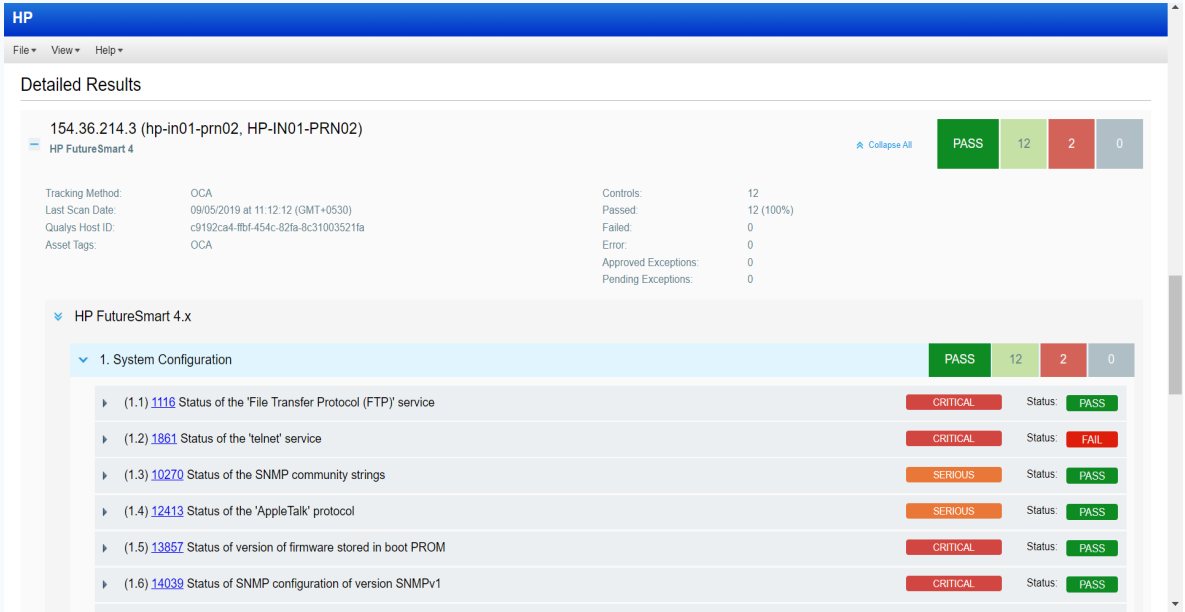
Qualys.

Network Devices Can’t be Scanned or Hosts too Sensitive but in Security & Compliance Scope

Use OCA APIs
- Create custom assets
- Push command output, vulnerability, config data

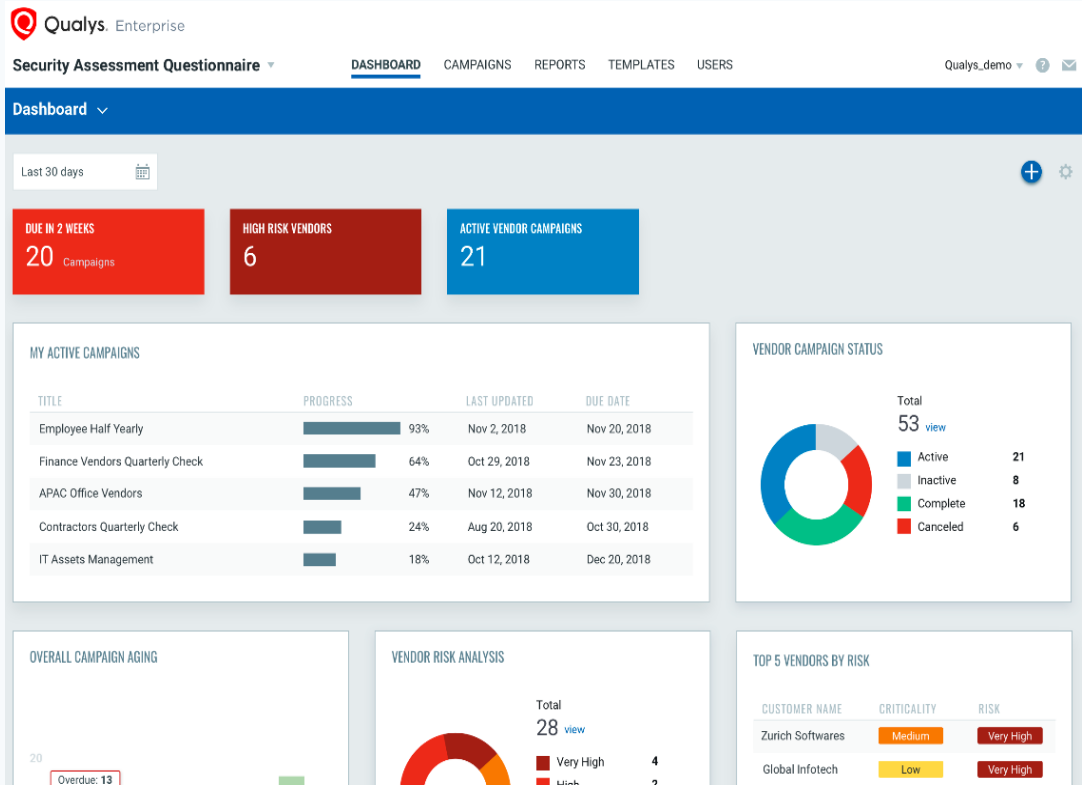
Controls validate settings

Report vulnerabilities, security and misconfigurations

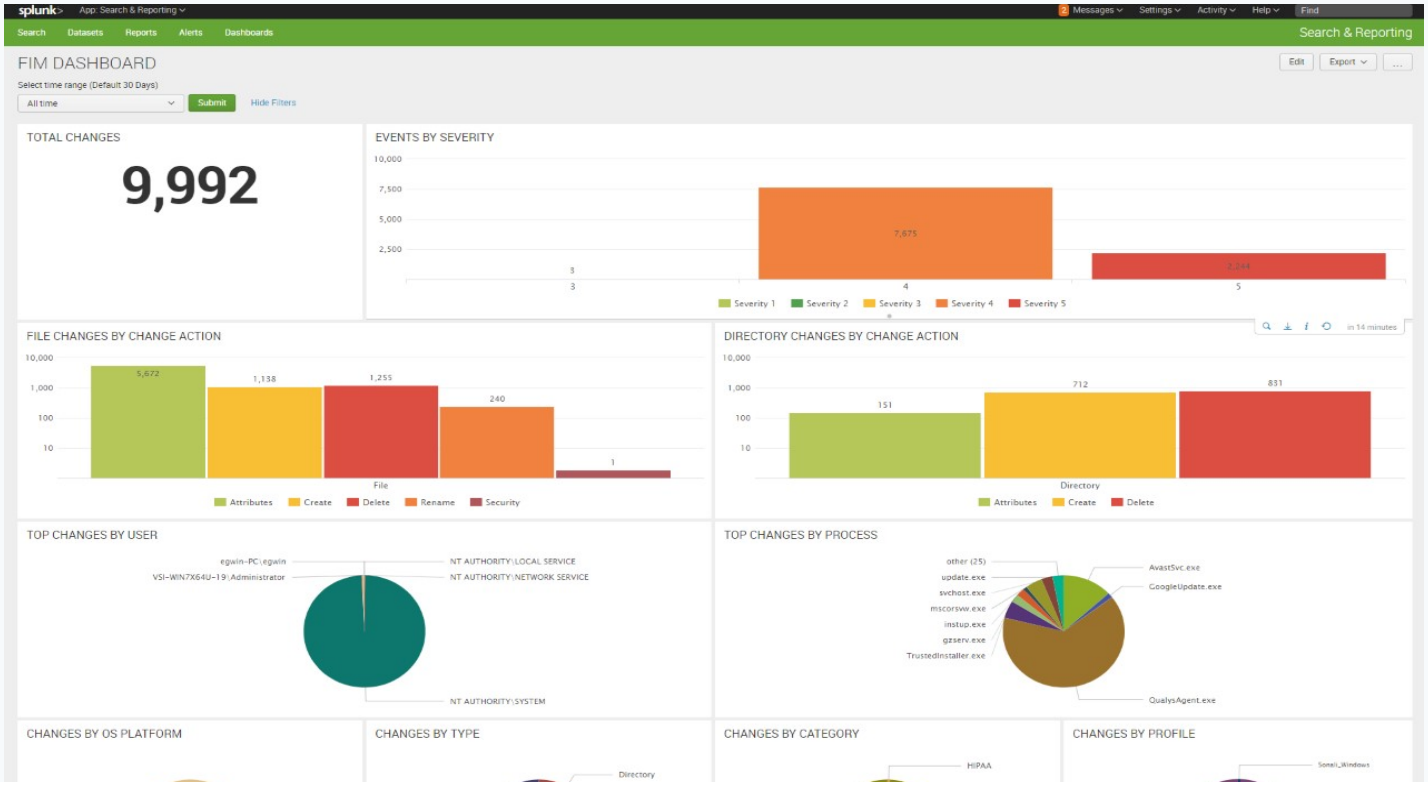


Your security is only as strong as your weakest vendor

Qualys Security Assessment Questionnaire (SAQ) helps in managing vendor risk per criticality



Open APIs: Integrate with Any External SIEM, DWH



Qualys.

Policy Compliance (PC)

Policy Compliance Advantages

Best in class technology and content coverage
For Configuration Management

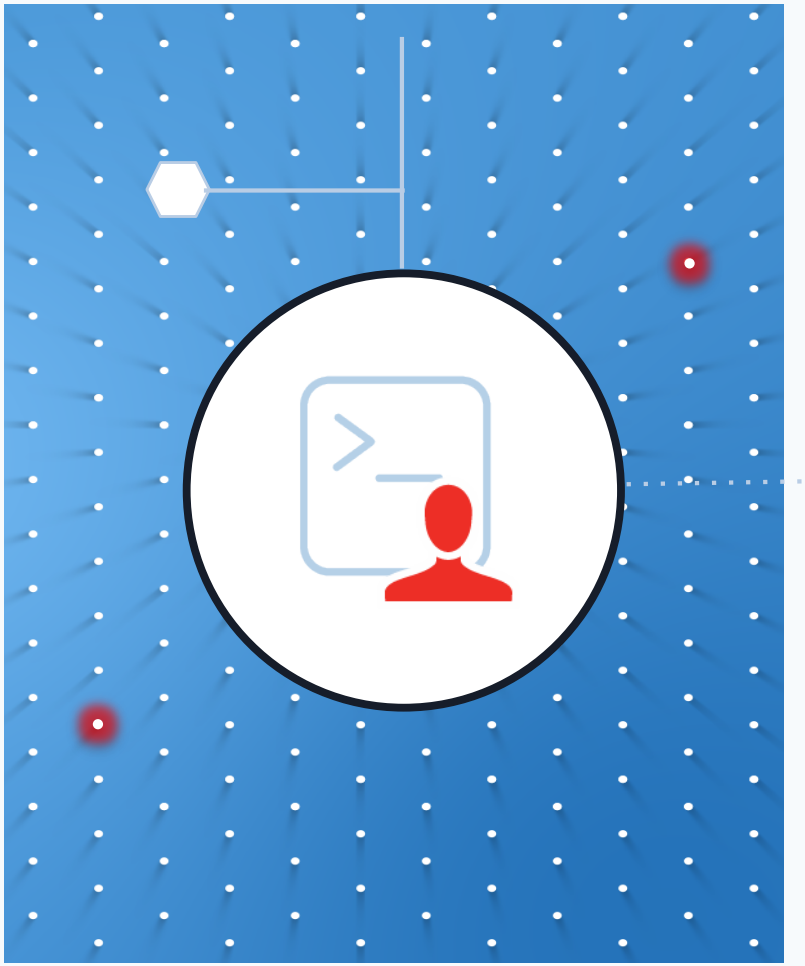
>400 Policies, >10,000 controls
>150 technologies (traditional, emerging)
> Widest coverage for CIS, STIG, Mandates and beyond

Data collection from all Qualys sensors

Custom database security & integrity controls

Auto-discovery of middleware technologies

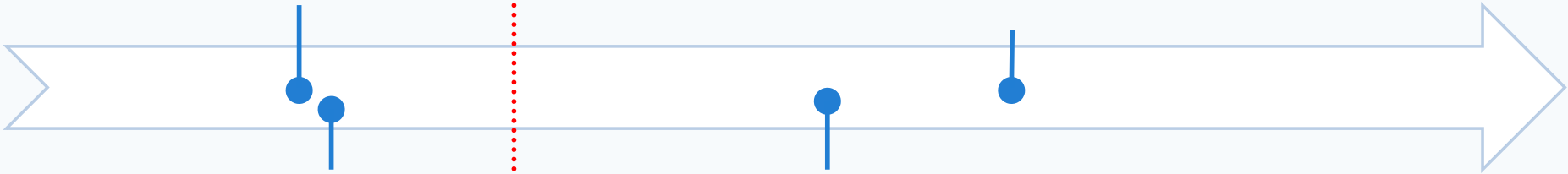
Auto-remediation for configuration failures



Qualys.

New PC UI and Customizable Dashboard

PC Roadmap



Q4 - 2018

Faster PC agent data processing
File Content search for Windows
(Search sensitive content)
Auto-discovery for database techs

Q4 - 2018

New, customizable PC dashboard

2020 Q1

New PC UI
Dynamic, real-time compliance against policies, mandates
Integration of PC/config data with Asset Inventory
Gold policies to fix configuration Issue 'upfront'
Ticketing integration with JIRA, ServiceNOW

2020 Q2

Configuration assessment for RDS
Automated alerting for compliance, config failures
Support for executing scripts/commands for custom apps
PC agent support for web server technologies
Compliance trending

File Integrity Monitoring (FIM)

Qualys FIM: In First Year

Built on the same Qualys Cloud Agent

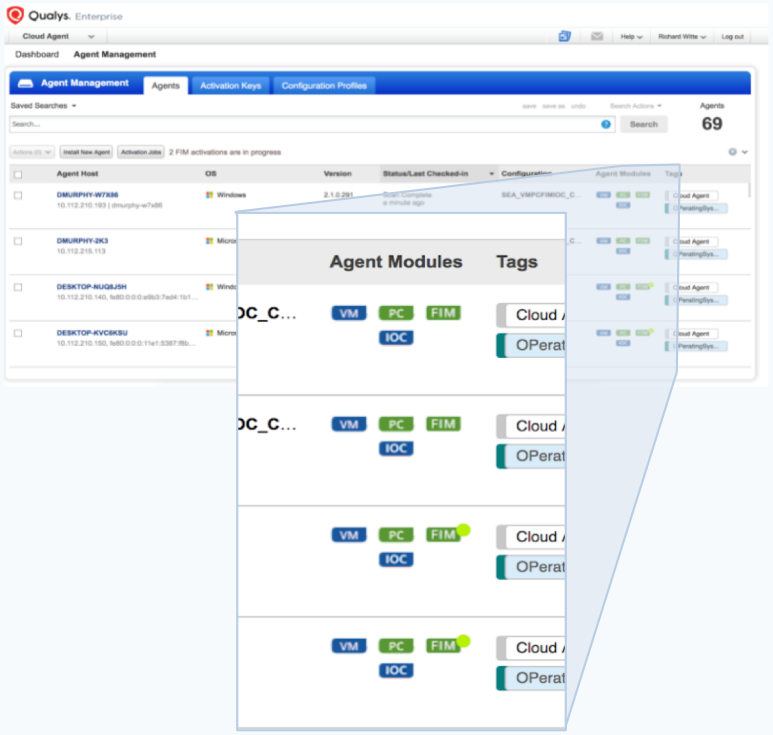
Real-time detection for high volume, high scale

Nothing to install, easy to configure, quick win

Automated incident management and alerting

Out of the box PCI monitoring profiles for OS and applications

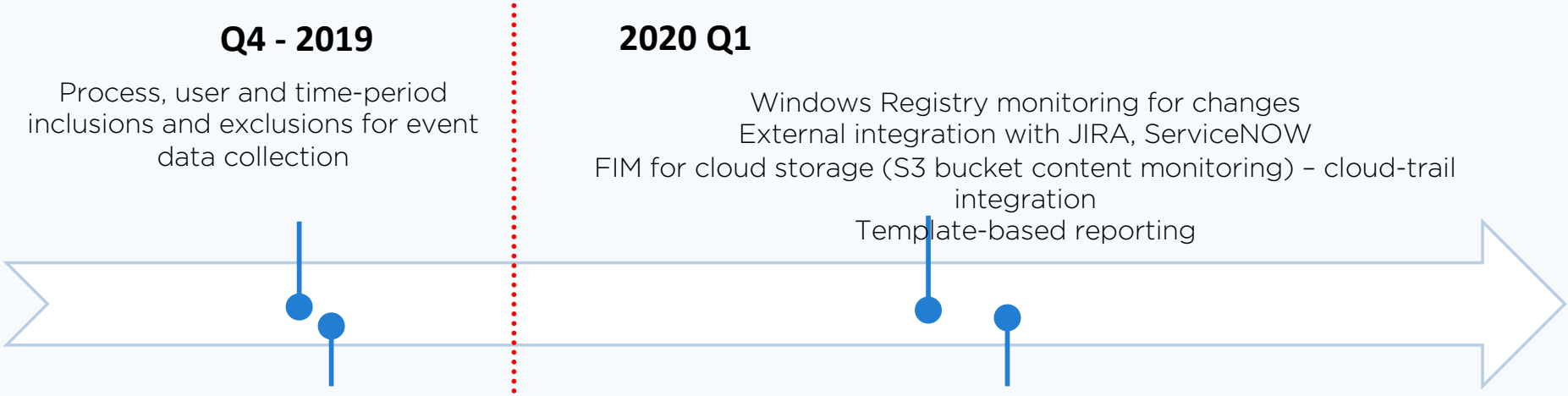
No infrastructure, data load for you to manage



Qualys.

Demo

FIM Roadmap



Q4 - 2019

Process, user and time-period inclusions and exclusions for event data collection

Q4 - 2019

FIM hosts health and status: % of hosts with latest data, stale hosts with no changes, hosts without a FIM monitoring profile

2020 Q1

Windows Registry monitoring for changes
External integration with JIRA, ServiceNOW
FIM for cloud storage (S3 bucket content monitoring) – cloud-trail integration
Template-based reporting

2020 Q2

Monitoring for file content changes/text changes
Graph-based topology view of file change alerts and incidents with actor, process
Monitoring profiles – import/exports
Integration with Qualys Patch Management for managing changes due to patching

Qualys.

Thank You

Compliance Team and Shailesh Athalye
sathalye@qualys.com