



QUALYS SECURITY CONFERENCE 2019

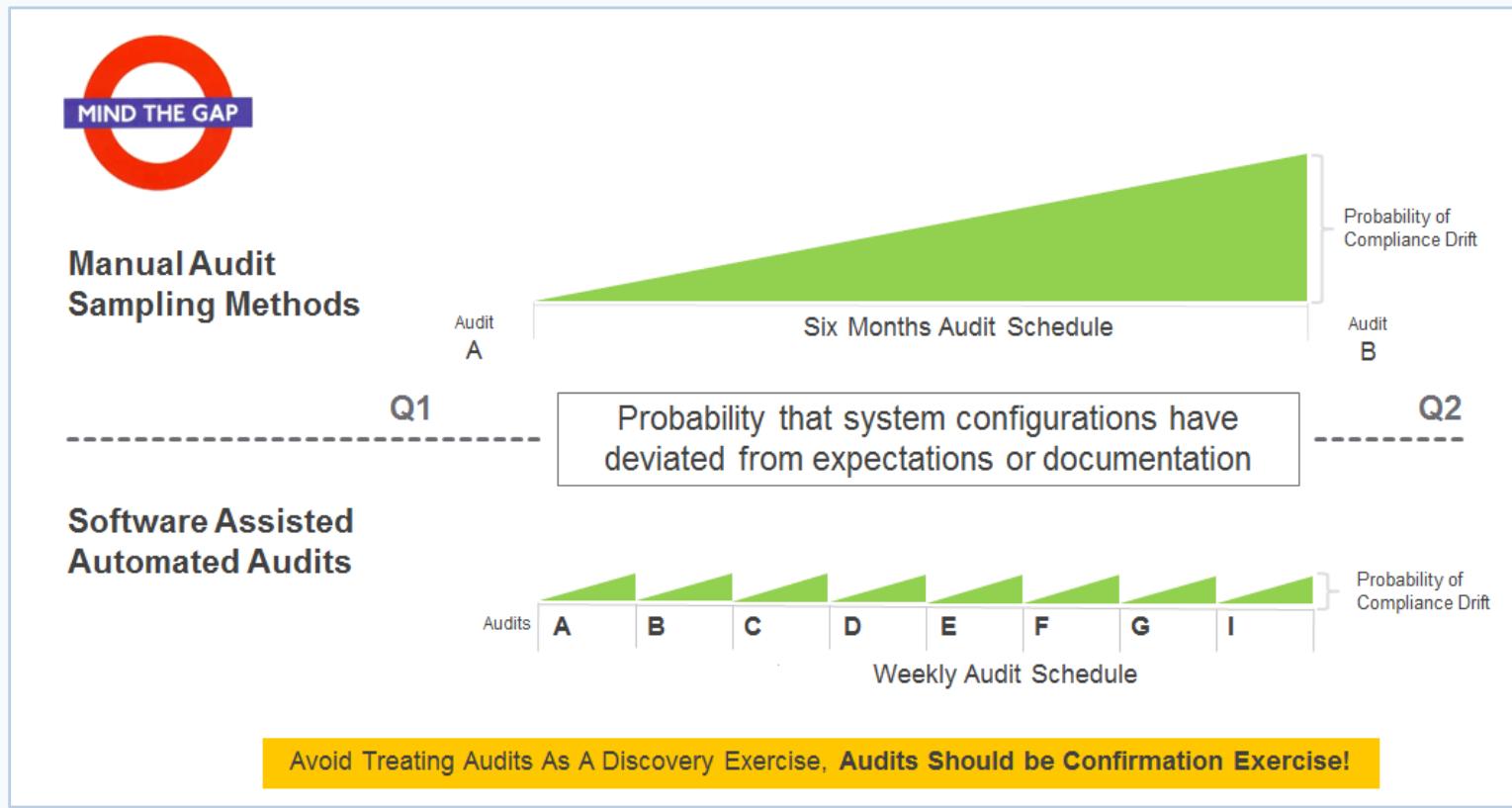
Continuous Compliance in Hybrid Environment

New Frontier in Unified Compliance, Configuration
and File Integrity Management

Shailesh Athalye

VP, Compliance Solutions, Qualys, Inc.

2014: Good Old Days of Compliance

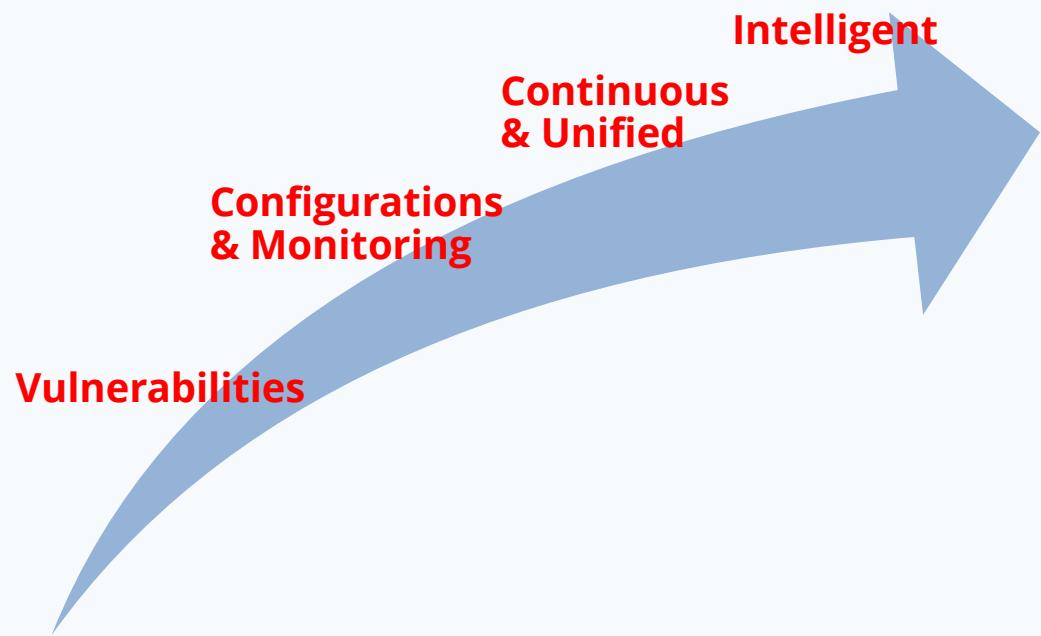


2019: Security is Continuous and Unified

To reduce the 'attack surface'

To reduce breaches due to misconfigurations, lack of monitoring

Question remains:
Is Compliance and Risk really continuous?

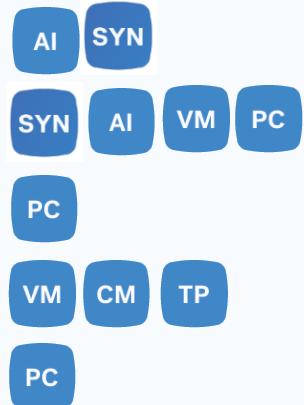


Compliance and Risk are Not Connected with Security

| PCI DSS Requirements | | |
|--|--|---|
| PCI DSS Requirements | | |
| 8.2.3 Passwords/passphrases must meet the following: | | |
| <ul style="list-style-type: none">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. | | |
| ISO/IEC 27001 (Annex A) CONTROLS | | |
| A.11.2 User access management | | |
| A.11.1 User registration | | |
| A.11.2.2 Privilege management | | |
| A.11.2.3 User password management | | |
| Section of HIPAA Security Rule | | |
| PCI DSS Requirements | HIPAA Security Rule Standards | |
| 8.2.3 Passwords/passphrases must meet the following: | | |
| 8.2.4 Change user passwords/passphrases at least once every 90 days. | | |
| Implementation Specifications | | |
| PCI DSS Requirements | | |
| 8.2.3 Passwords/passphrases must meet the following: | | |
| 8.2.4 Change user passwords/passphrases at least once every 90 days. | | |
| CIP-007-5 Table R3 – System Access Control | | |
| Part | Applicable Systems | Requirements |
| 5.5 | High 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 Asset; |
| CSC 16-3 | Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA | 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



Semi-automated Way for Connecting

Time to value

Time to see roll up the operational data

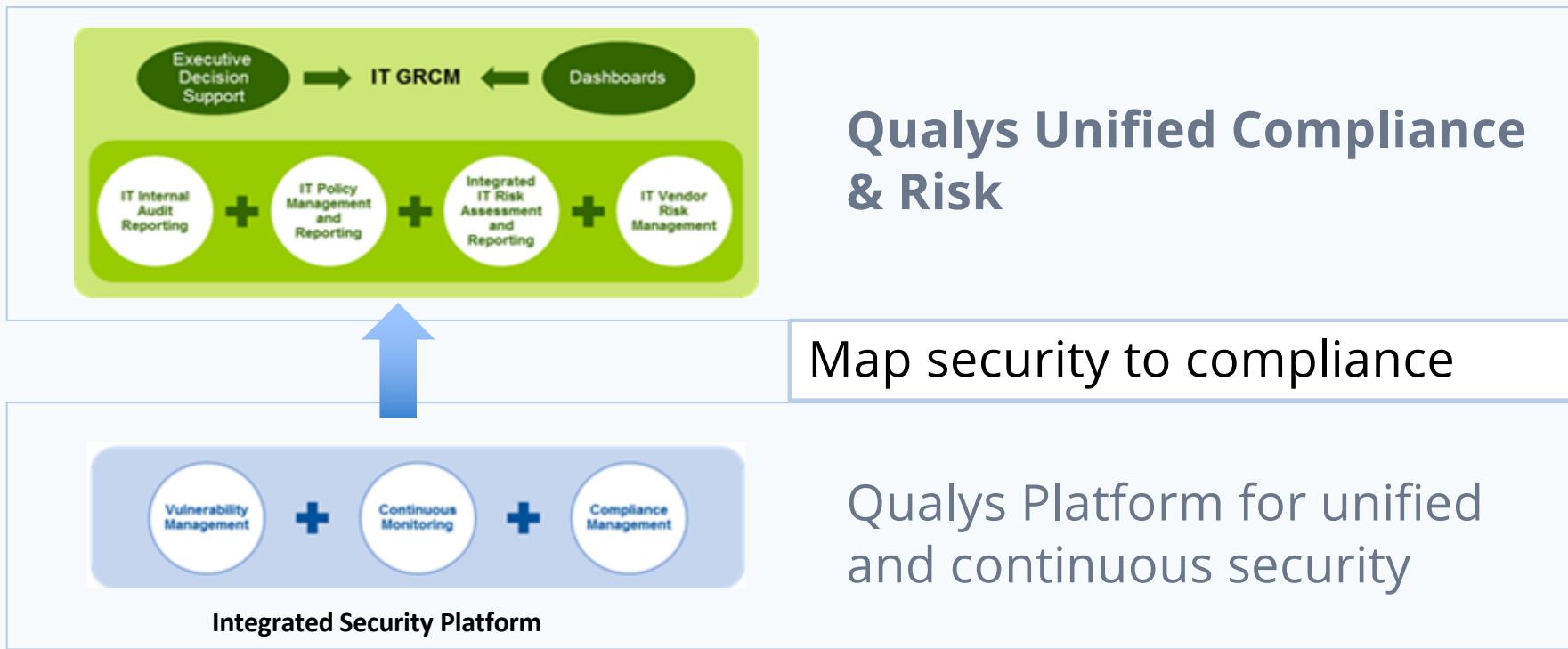
Security data of varied nature

FIM, Patch, Malware
Scoping and Tracking 'In-Scope'
Assets

Application complexity with connectors

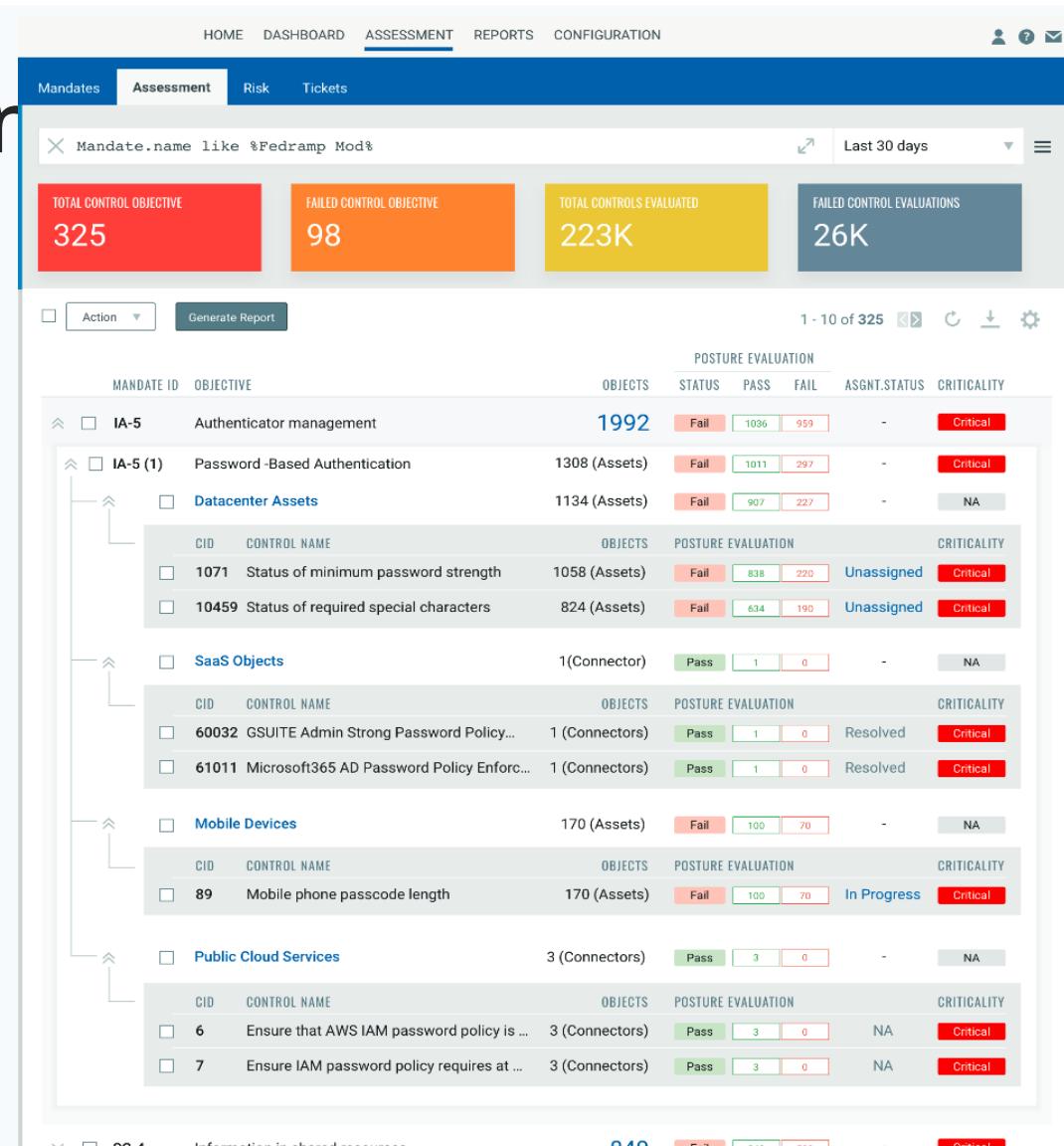


Continuous Compliance & Risk From Continuous Security

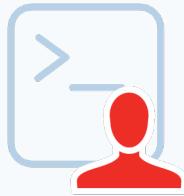


Continuous Compliance from Continuous Security

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



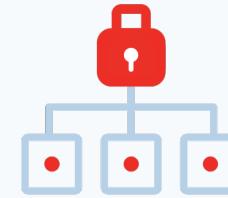
New-age Challenges: Teams Speaking Different Languages



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

Start Compliant, Stay Compliant in DevOps with Qualys PC

Jenkins

Jenkins aws-golden-ami-pipeline

Pipeline aws-golden-ami-pipeline

Recent Changes

Stage View

Average stage times:

#16 Nov 01 15:57 No Changes

#15 Nov 01 15:55 No Changes

Launch a CentOS instance with the Source AMI

73ms

5 mins

11min 21s failed

Launch VM & PC Scan on instance

10min 44s

73ms

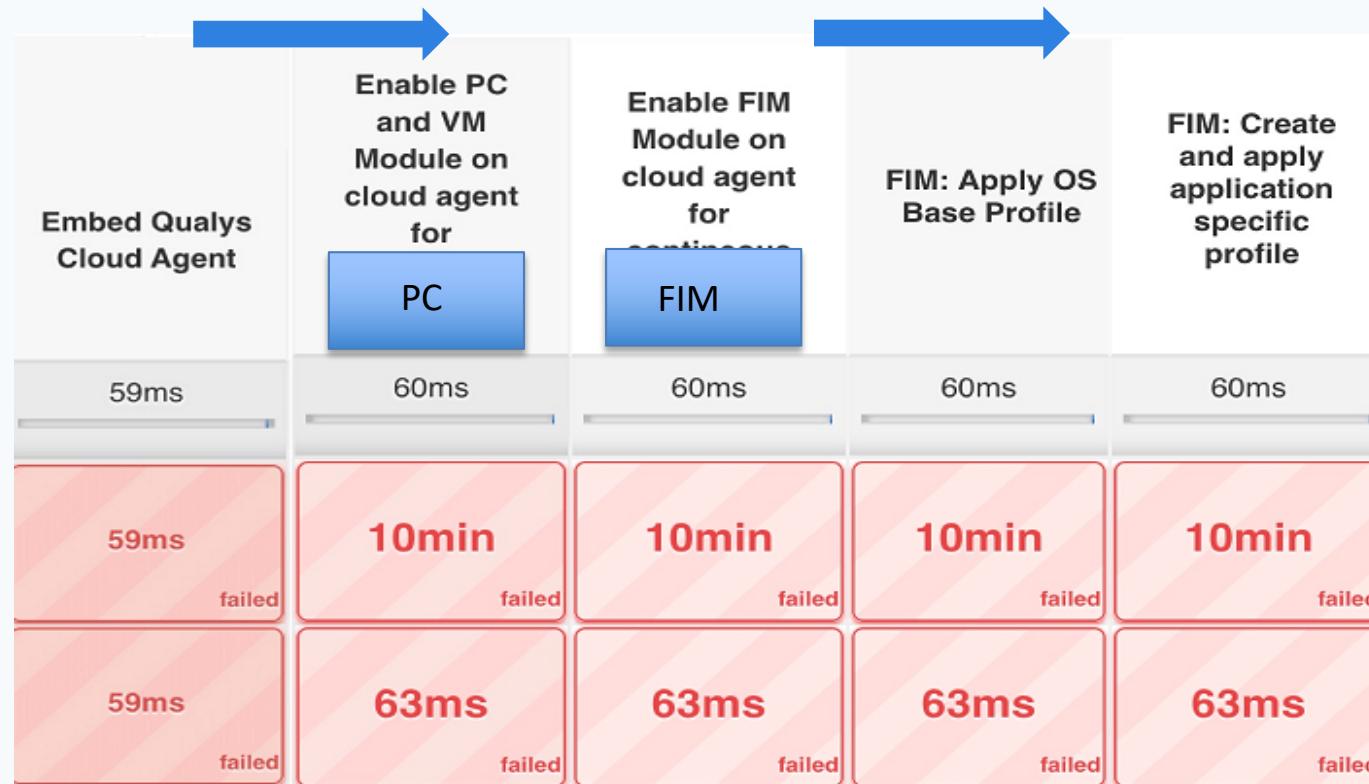
10min 6s failed

QUALYS POLICY COMPLIANCE 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 FIM Monitors From CD Phase



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

The screenshot shows a detailed assessment report for Apache Tomcat 8.x. At the top, there is a summary bar with the following metrics: PASS (green), 80 (light green), 0 (red), and 0 (grey). Below this, the main report structure is visible:

- Apache Tomcat 8.x** (Expended):
 - 1. ApacheTomcatControls** (Expended):
 - (1.1) [9505](#) Status of the 'permissions' within '\$CATALINA_HOME/webapps' directory
 - 1. Apache TC 8::/opt/apache-tomcat-8.0.18/apache-tomcat-8.0.18 (Status: PASS)
 - 2. Apache TC 8::/opt/apache-tomcat-8.5.20 (Status: PASS)
 - 3. Apache TC 8::/opt/apache-tomcat-8.5.20/apache-tomcat (Status: PASS)
 - 4. Apache TC 8::/opt/apache-tomcat-8.5.20/apache-tomcat1 (Status: PASS)
 - (1.2) [9602](#) Status of the 'manager application (webapps/manager)' setting
 - 1. Apache TC 8::/opt/apache-tomcat-8.5.20/apache-tomcat1 (Status: PASS)
 - 2. Apache TC 8::/opt/apache-tomcat-8.0.18/apache-tomcat-8.0.18 (Status: PASS)
 - 3. Apache TC 8::/opt/apache-tomcat-8.5.20/apache-tomcat (Status: PASS)
 - 4. Apache TC 8::/opt/apache-tomcat-8.5.20 (Status: PASS)
 - (1.3) [9603](#) Status of the 'manager application (manager.xml)' setting (Status: SERIOUS)
 - (1.4) [9606](#) Status of the command-line flag 'RECYCLE_FACADES' set for the Tomcat process (Status: CRITICAL)
 - (1.5) [9610](#) Status of the 'connectionTimeout' value within 'Connector' element in 'server.xml' fil (Status: SERIOUS)
 - (1.6) [9611](#) Status of the 'maxHttpHeaderSize' value within 'Connector' element in 'server.xml' fil (Status: SERIOUS)

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

The screenshot shows the Qualys Control View interface. On the left, a sidebar displays statistics: 51 Total Control Instances, categorized by Anti-Virus/Malware (51), Criticality (Medium: 3, Serious: 18, Critical: 26, Urgent: 4), and Posture (Pass: 41, Error: 1, Fail: 9). The main pane shows a search bar with the query: pc.policy.name:"Qualys Security windows" and pc.control.category:"Anti-Virus/Malware". Below the search bar, a table lists 51 control instances. The columns are STATUS, CID, CONTROL, TECHNOLOGY/INSTANCE, ASSET NAME, and LAST EVALUATION. The table includes several rows of audit results, such as:

| STATUS | CID | CONTROL | TECHNOLOGY/INSTANCE | ASSET NAME | LAST EVALUATION |
|---|-------|---|------------------------------|---|-----------------|
| Nov 13, 2019 | | | os | 10.10.36.125 COMDEV | |
| PASS Nov 13, 2019 | 12364 | Status of the 'CommunicationStatus' (Last time st | Windows 10 os | comqaw10es 10.10.36.126 COMQA\ | Nov 13, 2019 |
| PASS Nov 13, 2019 | 12364 | Status of the 'CommunicationStatus' (Last time st | Windows Server 2012 R2 os | i-6f91d2a8 10.11.114.112 I-6F91D | Nov 13, 2019 |
| PASS Nov 13, 2019 | 13738 | Status of the Symantec 'last Virus scan time' older | Windows 2008 Server os | com-2k8-32-87 10.10.32.87 COM-2K8- | Nov 13, 2019 |
| PASS Nov 13, 2019 | 13738 | Status of the Symantec 'last Virus scan time' older | Windows 10 os | comdevw10es 10.10.36.125 COMDEV | Nov 13, 2019 |
| Qualys Policy for Security Control Validation on Windows Platform | | | | | |
| PASS Nov 13, 2019 | 13738 | Status of the Symantec 'last Virus scan time' older | Windows 10 os | comqaw10es 10.10.36.126 COMQA\ | Nov 13, 2019 |

Start Gold, Continuously Assess, Remediate

Screenshot of the Qualys Policy Compliance interface showing a remediation job creation process.

The dashboard displays 72 Total Controls. A search bar shows a query: Policy.name like '%RDP%' and asset.tagName='USproduction' and control.status='failed'. The timeline shows 'TRENDING' data from Jan 01 to TODAY.

A dropdown menu under 'Actions' has a red box around the 'Create Remediation Job' option, which is being clicked.

| CONTROL NAME | TECHNOLOGY | ASSET NAME | POLICY EVALUATION |
|--|---------------------|------------------------------|-------------------|
| Status of the 'Terminal Services' service | Windows 2008 Server | XAVIERHQ39WIN 10.10.31.30 | Jun 02, 2018 |
| Status of the 'Terminal Services' service | Windows 7 | SFO03HQLP79 10.10.35.242 | Mar 21, 2018 |
| Status of the 'Set time limit for active Remote Desktop Services sessions' setting | Windows 10 | SFO04HQLP713 10.10.35.241 | May 03, 2018 |
| Current list of Groups and User Accounts granted the | Windows | DC03SJC1SQLDB | Oct 22, 2018 |

Qualys logo is in the bottom right corner.

Alert and Incident Management for Authorized vs Unauthorized Changes During Patching

Qualys Enterprise

File Integrity Monitoring ▾ DASHBOARD EVENTS RULES INCIDENTS REPORTS ASSETS CONFIGURATION

Rules Activity Rule Manager Actions

ruleName:"Unauthorized Windows Patching Activity" or ruleName:"Authorized Windows Patching Activity"

Last 30 Days

3 Total Activities

RULE NAME STATUS AGGREGATE ACTION MATCHES CREATED BY

| RULE NAME | STATUS | AGGREGATE | ACTION | MATCHES | CREATED BY |
|--|---------|-----------|---------------------------|---------|--------------|
| Unauthorized Windows Patching Activity | Success | Yes | Windows Patch Activity... | 1 | Aparna Hinge |
| Authorized Windows Patching Activity | Success | Yes | Windows Patch Activity... | 1 | Aparna Hinge |
| Unauthorized Windows Patching Activity | Success | Yes | Windows Patch Activity... | 1 | Aparna Hinge |
| Unauthorized Windows Patching Activity | Success | Yes | Windows Patch Activity... | 1 | Aparna Hinge |

ACTION NAME

EMAIL RECIPIENTS

ljhamb@qualys.com, akaur@qualys.com

Q Qualys

FIM gives context of changes in cloud

Qualys. Enterprise

← Asset Details : i-076e2369b896dfe3e

File Integrity Monitoring

Cloud Agent FIM Events S3 FIM Events

UNAUTHORIZED EVENTS ON S3 BUCKET FROM INSTANCE (INSTANCE ID)

Total Events 5.0K

Authorized 4584
Unauthorized 498

| TIME | TARGET | ACTION | ACTOR | EVENT STATUS | SEVERITY |
|----------------------------|---|-----------------|---------------------------|--------------|----------|
| an hour ago 12:08:18 PM | bucketauditreports/ 636123215182/us-west-1 | PutBucketPolicy | InstanceProfile/i-07f6... | Accessed | Medium |
| an hour ago 12:08:18 PM | bucketauditreports/t... | GetObject | InstanceProfile/i-07f6... | Accessed | Medium |
| an hour ago 12:08:18 PM | bucketauditreports/ec2... | DeleteObject | InstanceProfile/i-07f6... | Unauthorized | Medium |
| an hour ago 12:08:18 PM | bucketauditreports/RDS... | DeleteObject | InstanceProfile/i-07f6... | Unauthorized | Medium |
| an hour ago 12:08:18 PM | bucketauditreports/tom... | DeleteObject | InstanceProfile/i-07f6... | Unauthorized | Medium |

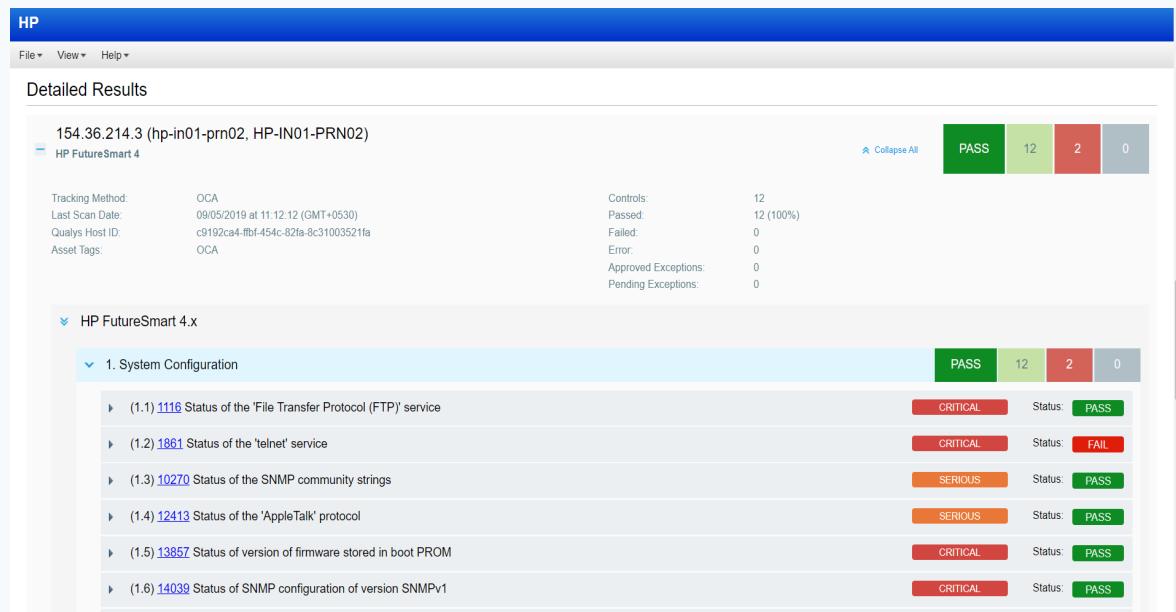
Network Devices Can't be Scanned or Hosts too Sensitive but in Security & Compliance Scope

Use OCA APIs

- Create custom assets
- Push command output, vulnerability, config data

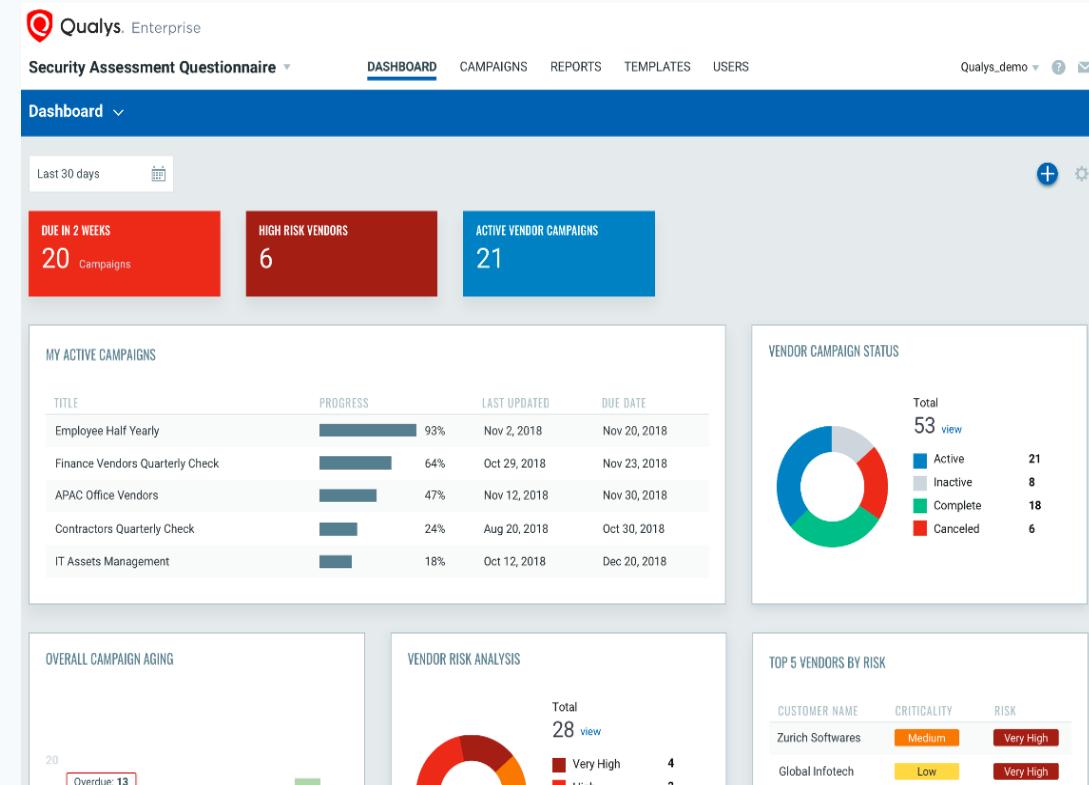
Controls validate settings

Report vulnerabilities, security and misconfigurations

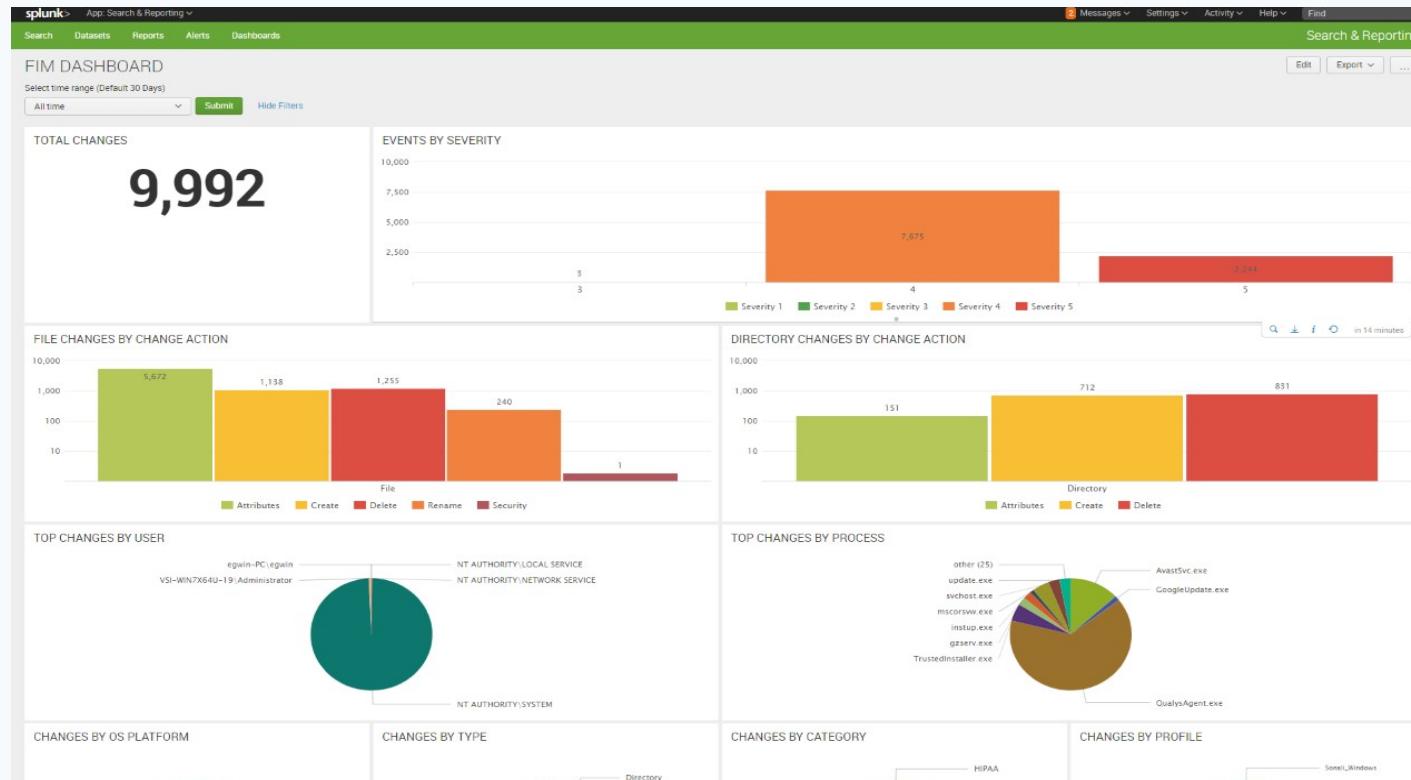


Your security is only as strong as your weakest vendor

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



Open APIs: Integrate with Any External SIEM, DWH



Policy Compliance (PC)

Policy Compliance Advantages

Best in class technology and content coverage
For Configuration Management

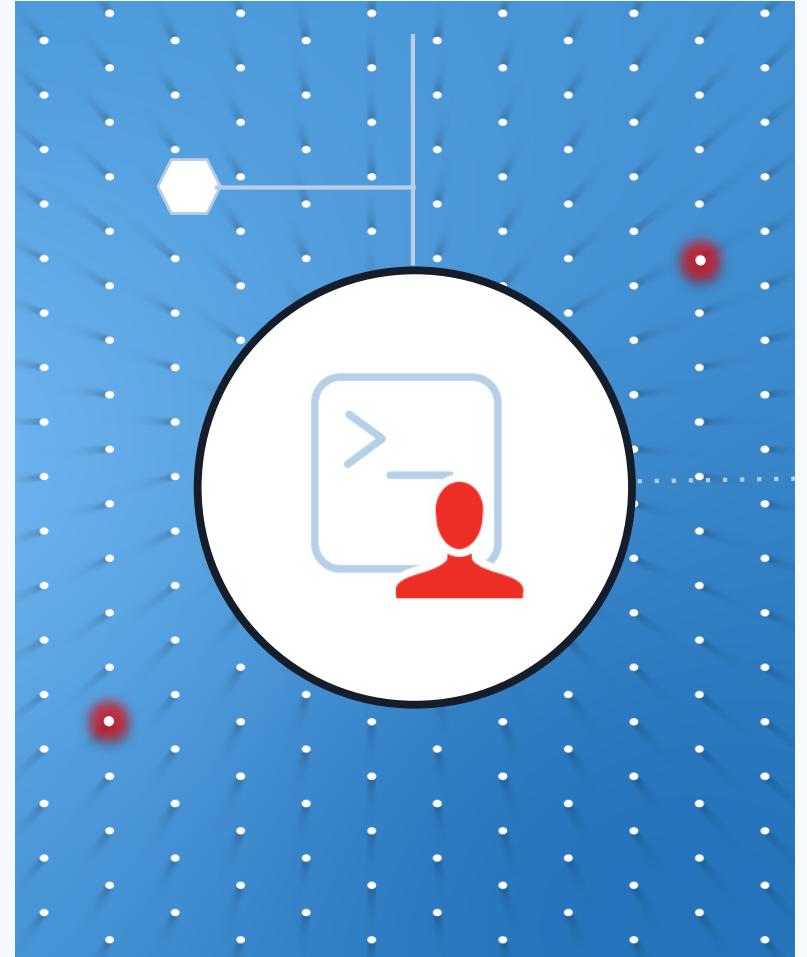
- >400 Policies, >10,000 controls
- >150 technologies (traditional, emerging)
- > Widest coverage for CIS, STIG, Mandates and beyond

Data collection from all Qualys sensors

Custom database security & integrity controls

Auto-discovery of middleware technologies

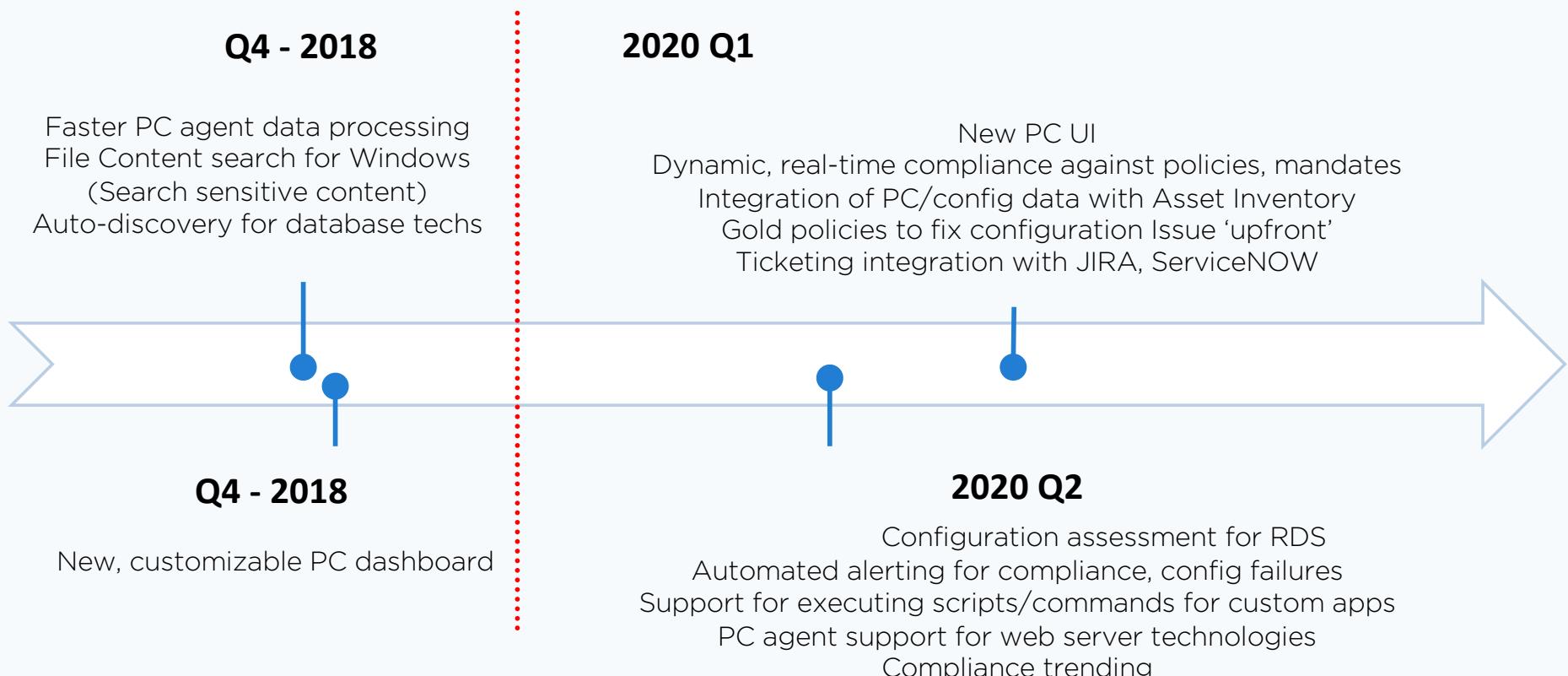
Auto-remediation for configuration failures





New PC UI and
Customizable
Dashboard

PC Roadmap



File Integrity Monitoring (FIM)

Qualys FIM: In First Year

Built on the same Qualys Cloud Agent

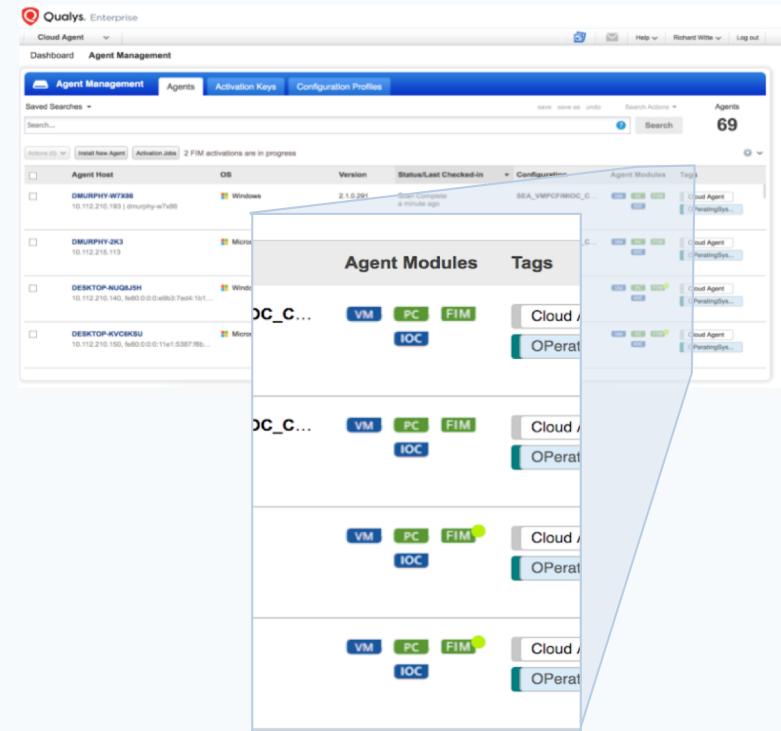
Real-time detection for high volume, high scale

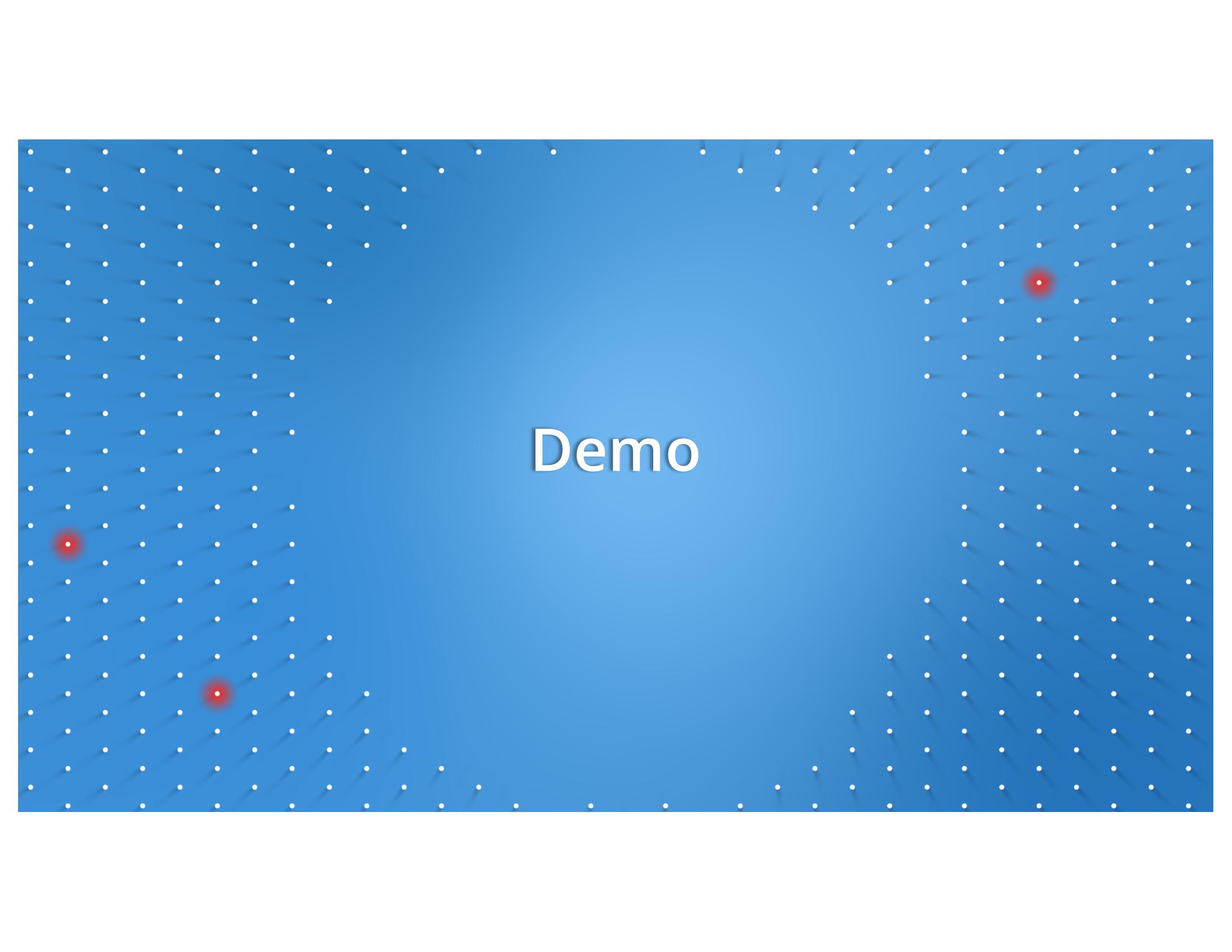
Nothing to install, easy to configure, quick win

Automated incident management and alerting

Out of the box PCI monitoring profiles for OS and applications

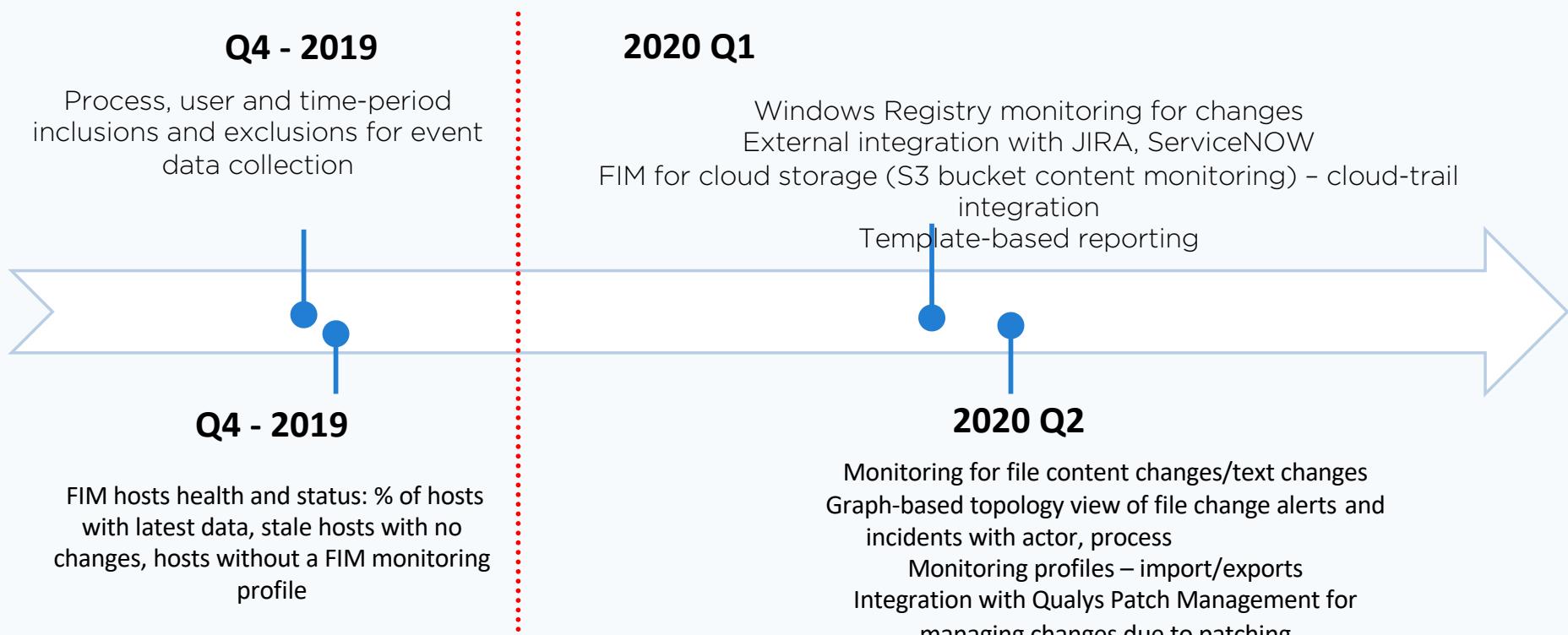
No infrastructure, data load for you to manage



The background is a solid blue color with a subtle texture. Overlaid on it is a grid of small, white, circular dots. Three specific dots in this grid are highlighted with a red glow, creating a focal point. The first highlight is located in the lower-left quadrant, the second in the center-left area, and the third in the upper-right quadrant.

Demo

FIM Roadmap





QUALYS SECURITY CONFERENCE 2019

Thank You

Compliance Team and Shailesh Athalye
sathalye@qualys.com