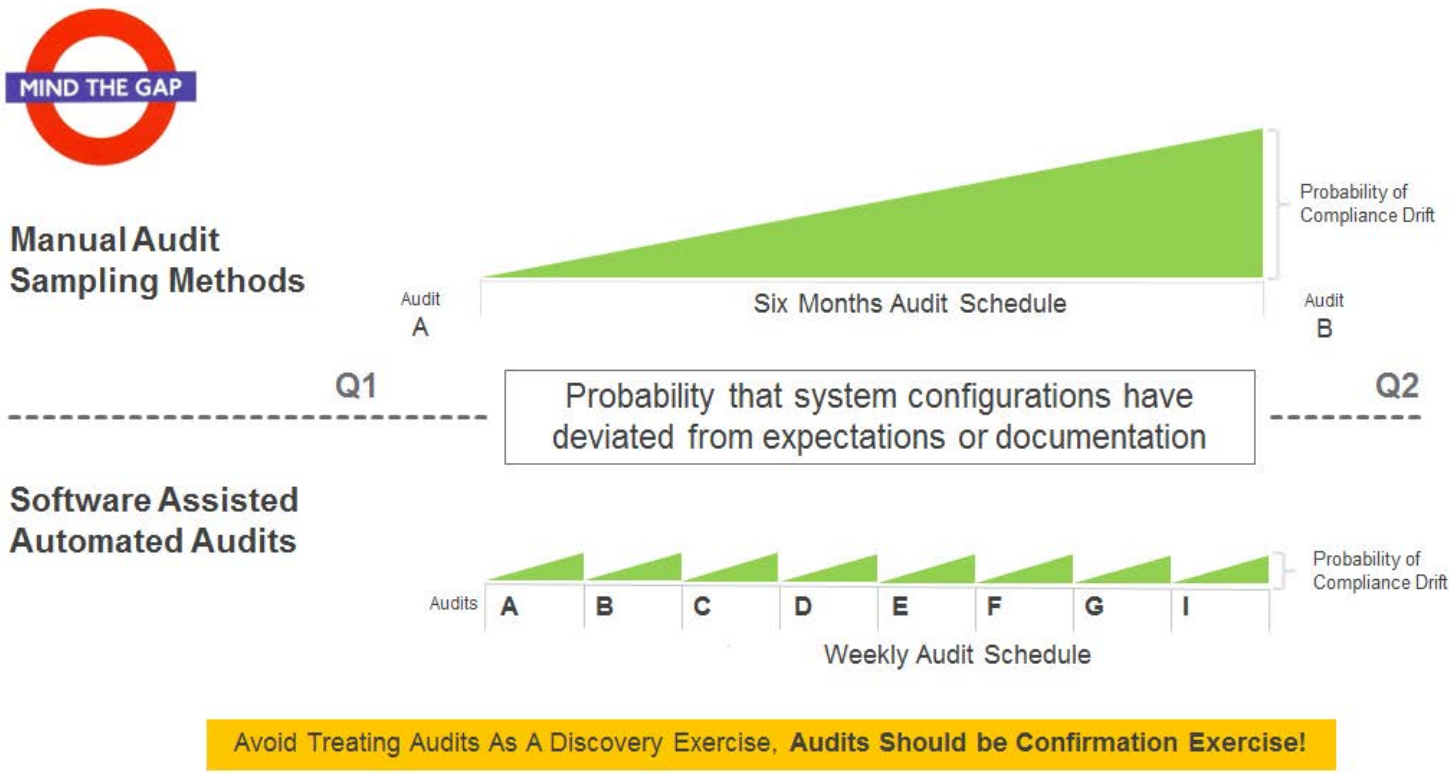
QSC20

QUALYS SECURITY CONFERENCE 2020

Continuous Compliance in Hybrid Environment

Shailesh Athalye
VP, Compliance Solutions, Qualys, Inc

2014: Good Old Days of Compliance



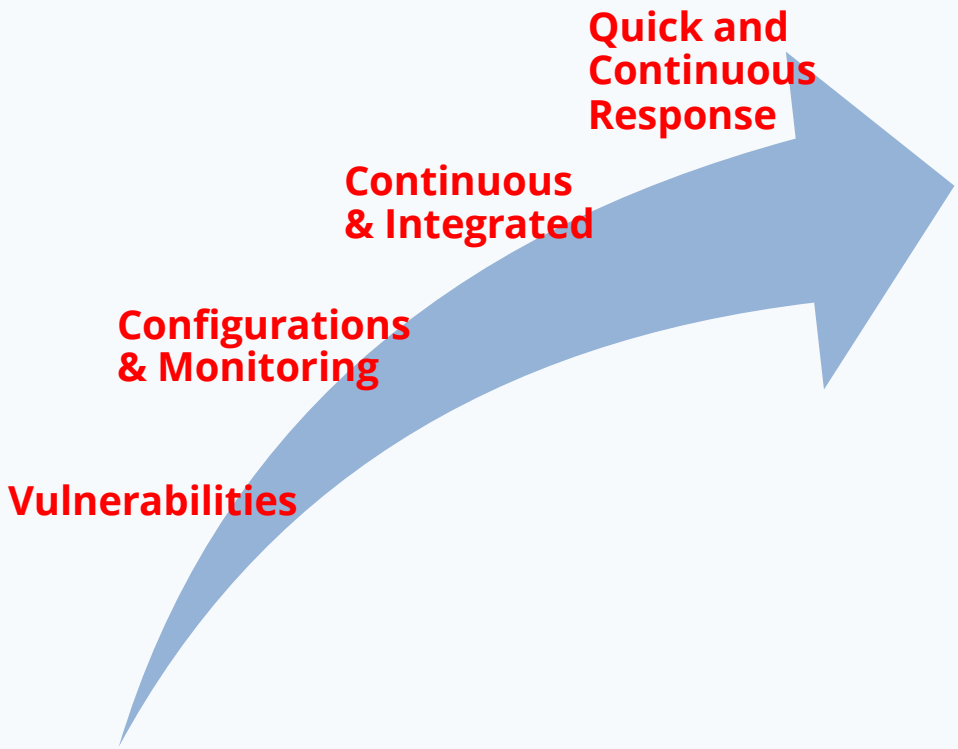
Avoid Treating Audits As A Discovery Exercise, **Audits Should be Confirmation Exercise!**

Qualys.

2020: Matured Cybersecurity Risk Management

Performing vulnerability management with a context to reduce the “attack surface”

Quick continuous assessment and fix cycles before images are in production

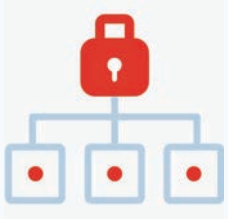


Qualys.

Teams Speak Different Languages

Elastic, Kafka, custom web servers

Identify risk and compliance

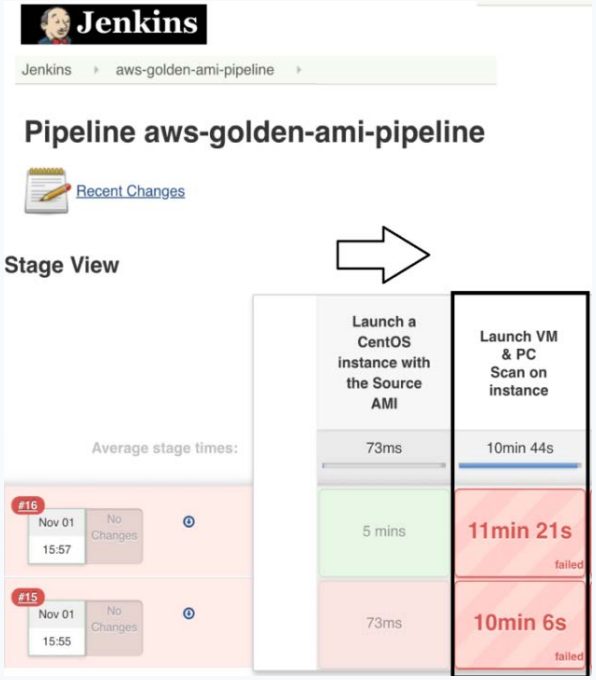


Secure hosts, config/integrity/ vulnerability management

Security & Compliance assessment should be baked into DevOps

Qualys.

Start Compliant, Stay Compliant



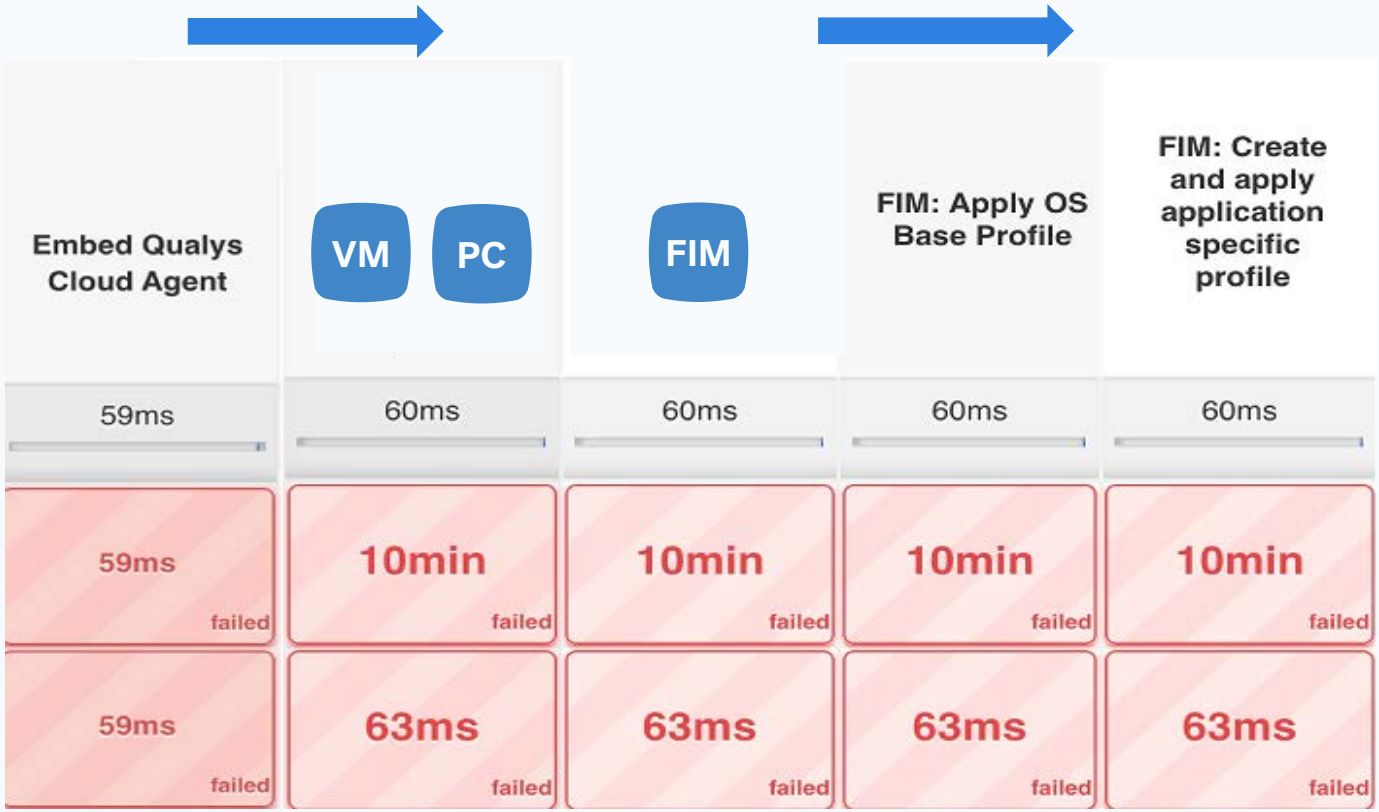
QUALYS POLICY COMPLIENCE RESULTS

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.

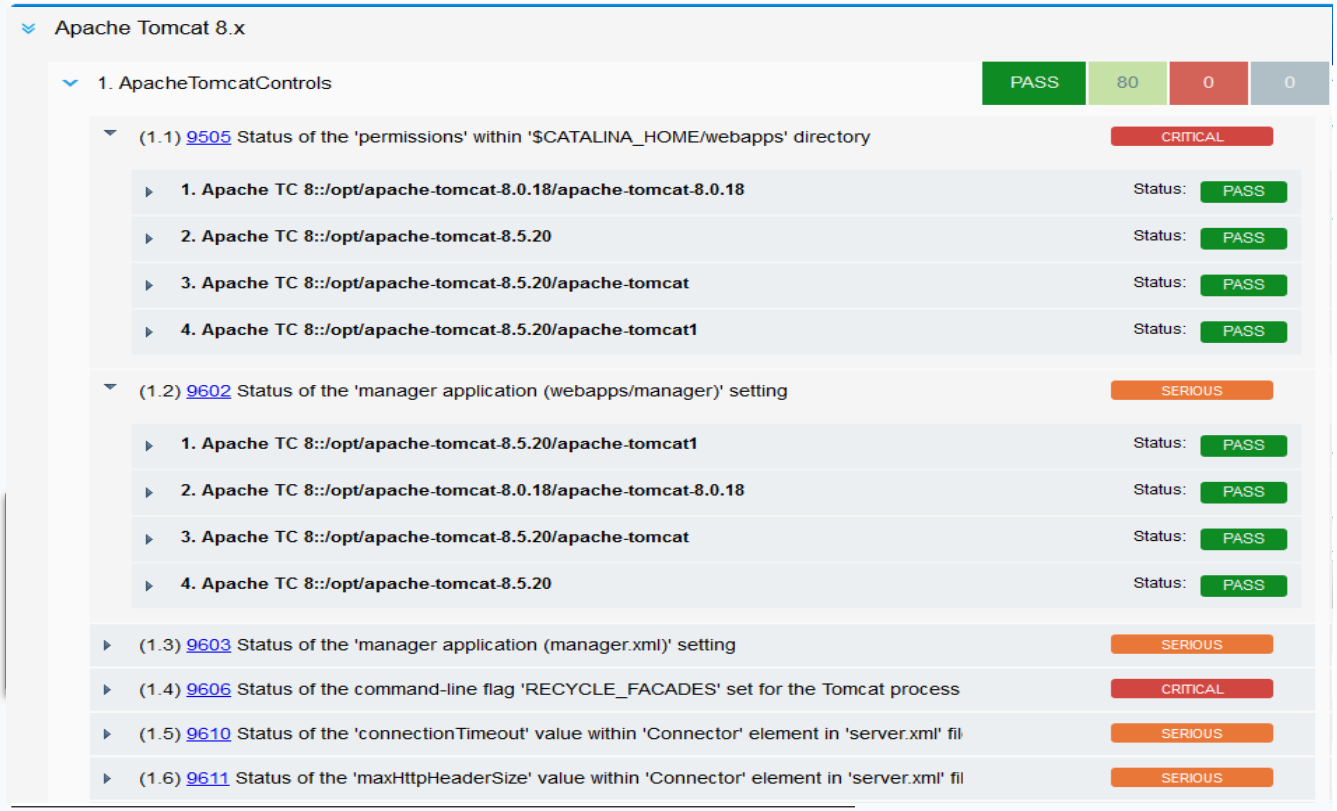
Monitor Critical Files From CD Phase



Qualys.

Discover and Assess Middleware Automatically

Discover unauthorized technologies based on host scans

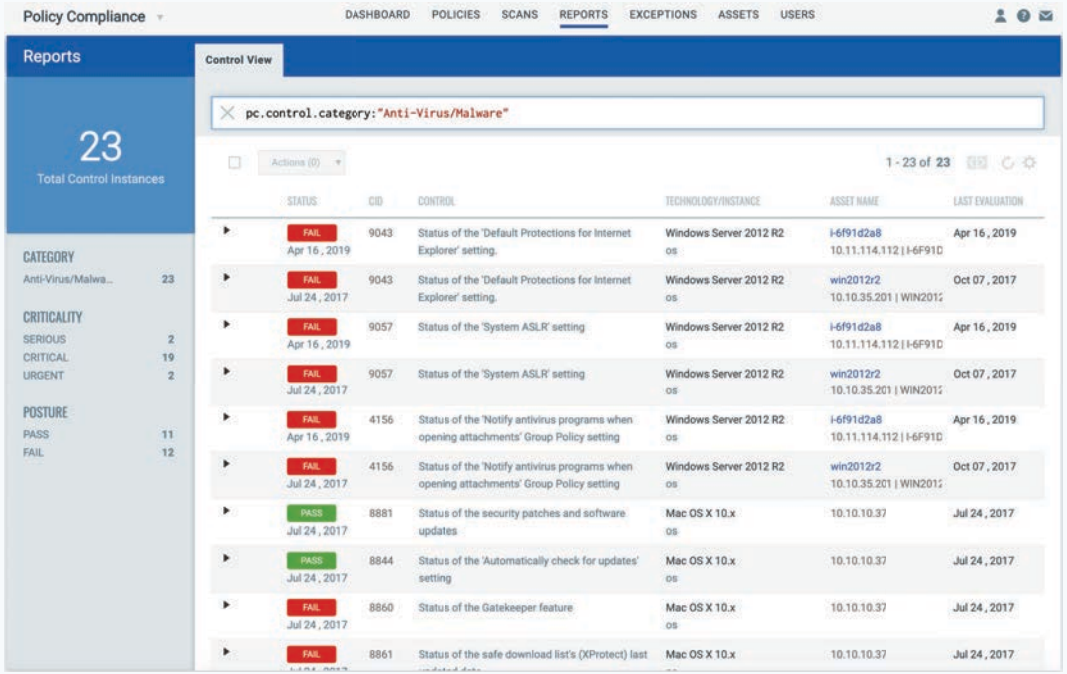


Security Control Validation (SCV)

Top five responsibilities of CISOs
https://www.bitsight.com/blog/ciso-roles-and-responsibilities

Pre-requisites and configurations

Native security features



Anti-virus | FIM Agents | Splunk | Kafka | Native Malware Protection | Jenkins

Qualys.

Qualys. Enterprise

Create New : **Remediation**

STEP 4 / 5

1. Basic Information
2. Select Assets
3. Select Controls
4. Schedule
5. Review and Confirm

Schedule

Schedule the remediation job to run on demand or in the future

On Demand | Schedule

Remediation Window

You can configure a remediation windoe to run to

- (●) None
- ( ) Set Duration

Note: Not setting the patch window will allow the cloud agent to take as much time as it needs to complete the job.

Cancel | Previous | Next

New Policy Compliance UI

Security for Inaccessible & Exotic Hosts

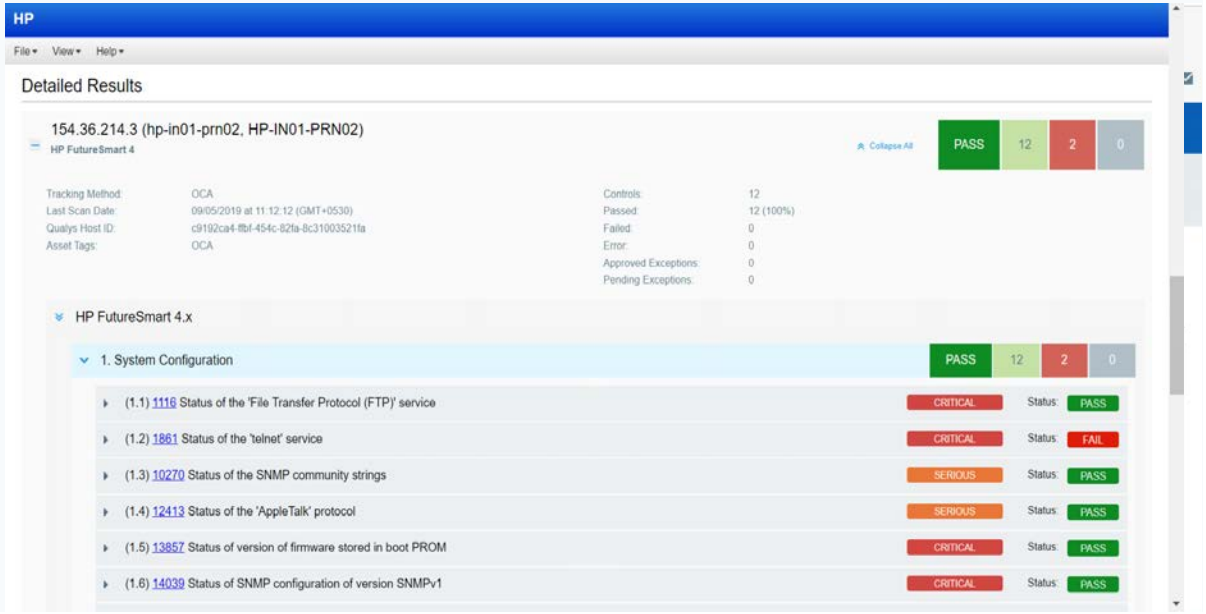
Use APIs/UI and push data to Qualys

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

Validate settings and data

Report vulnerabilities, security and misconfigurations

Qualys Out-of-Band Config Assessment (OCA)



New-Age File Integrity Monitoring

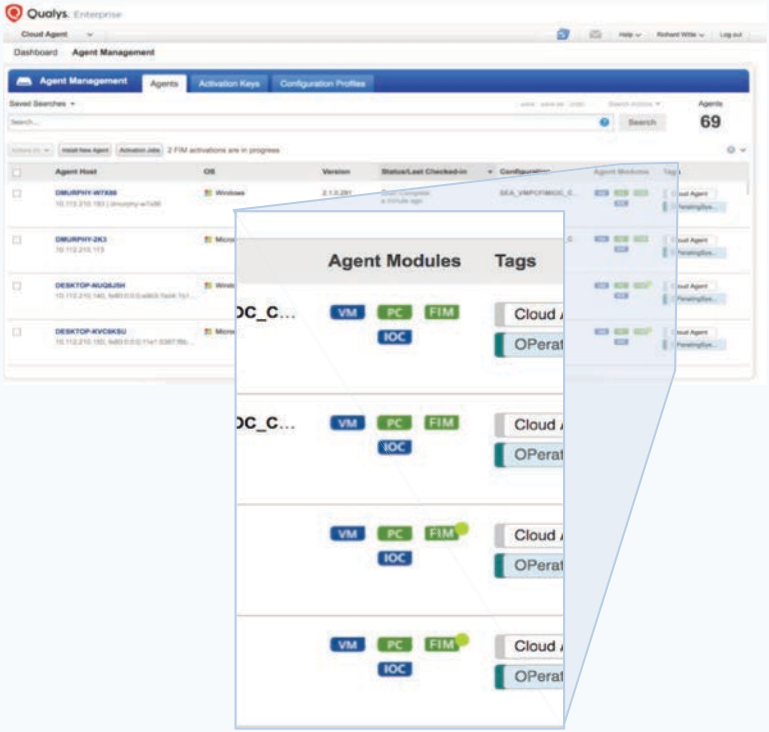
Built on the same Qualys Cloud Agent you use for VM, PC, Inventory

Real-time detection for high volume, high scale

Automated incident management and alerting

Out of the box PCI monitoring profiles for OS and applications

No infrastructure or data load for you to manage



Qualys.

Authorized vs Unauthorized Changes

Qualys. Express

File Integrity Monitoring

DASHBOARD EVENTS RULES INCIDENTS REPORTS ASSETS CONFIGURATION

Incidents

All Incidents | Correlation Rules

101
Total Incidents

ruleId:8fc42fcc-4028-45e8-88da-672254ed1493

Assigned to me
101

Pending
1

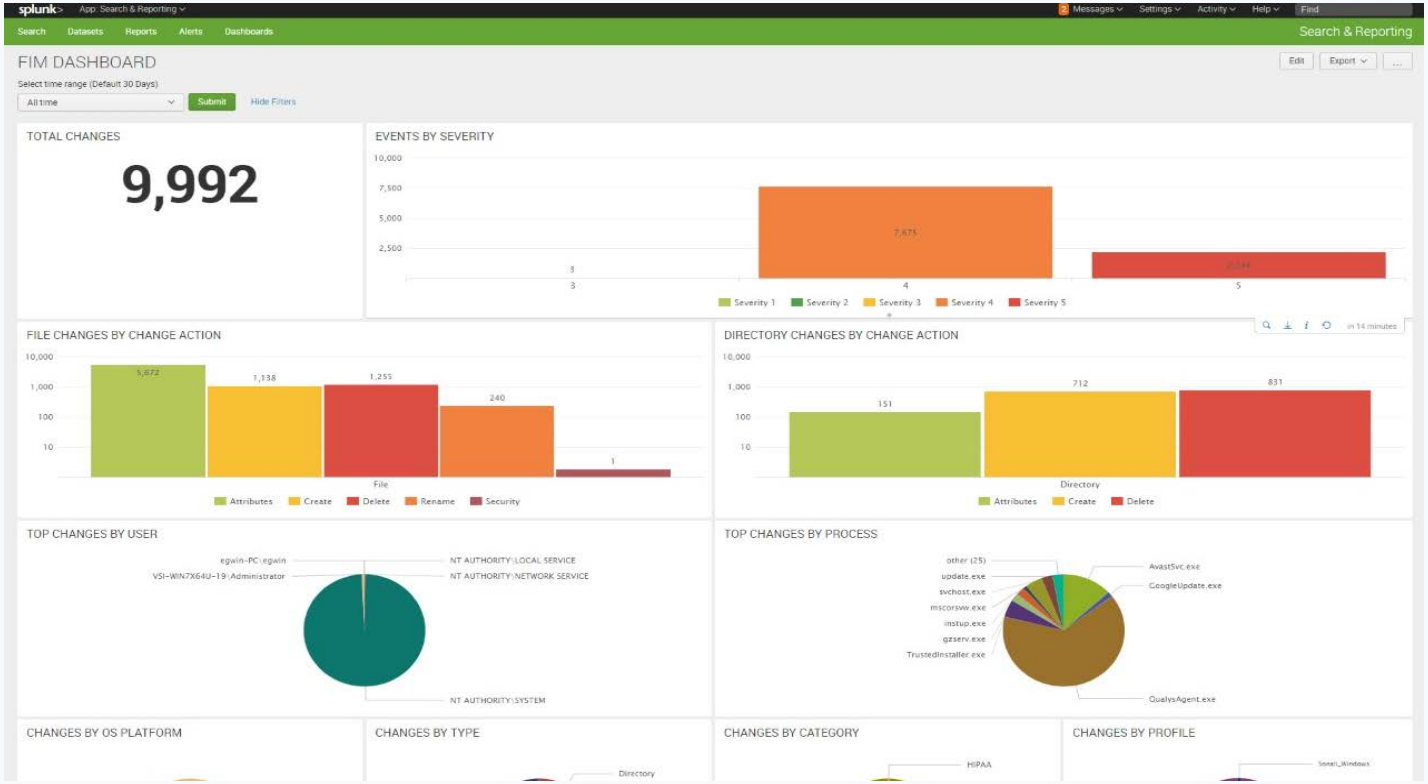
STATUS
CLOSED 100
OPEN 1

1 - 50 of 101

CREATED	NAME	TYPE	STATUS	ASSIGNEE	DISPOSITION	CHANGE TYPE	APPROVAL
21 hours ago 10:30:00 AM	Unauthorized Windows Patc...	AUTOMATED	OPEN	quays_qd		-	-
2 days ago 10:30:00 AM	Unauthorized Windows Patc...	AUTOMATED	CLOSED	quays_qd	PATCHING	AUTOMATED	POLICY_VIOLA...
3 days ago 10:30:00 AM	Unauthorized Windows Patc...	AUTOMATED	CLOSED	quays_qd	PATCHING	AUTOMATED	POLICY_VIOLA...
4 days ago 10:30:00 AM	Unauthorized Windows Patc...	AUTOMATED	CLOSED	quays_qd	PATCHING	AUTOMATED	POLICY_VIOLA...
5 days ago 10:30:00 AM	Unauthorized Windows Patc...	AUTOMATED	CLOSED	quays_qd	PATCHING	AUTOMATED	POLICY_VIOLA...
6 days ago 10:30:00 AM	Unauthorized Windows Patc...	AUTOMATED	CLOSED	quays_qd	PATCHING	AUTOMATED	POLICY_VIOLA...
7 days ago 10:30:00 AM	Unauthorized Windows Patc...	AUTOMATED	CLOSED	quays_qd	PATCHING	AUTOMATED	POLICY_VIOLA...

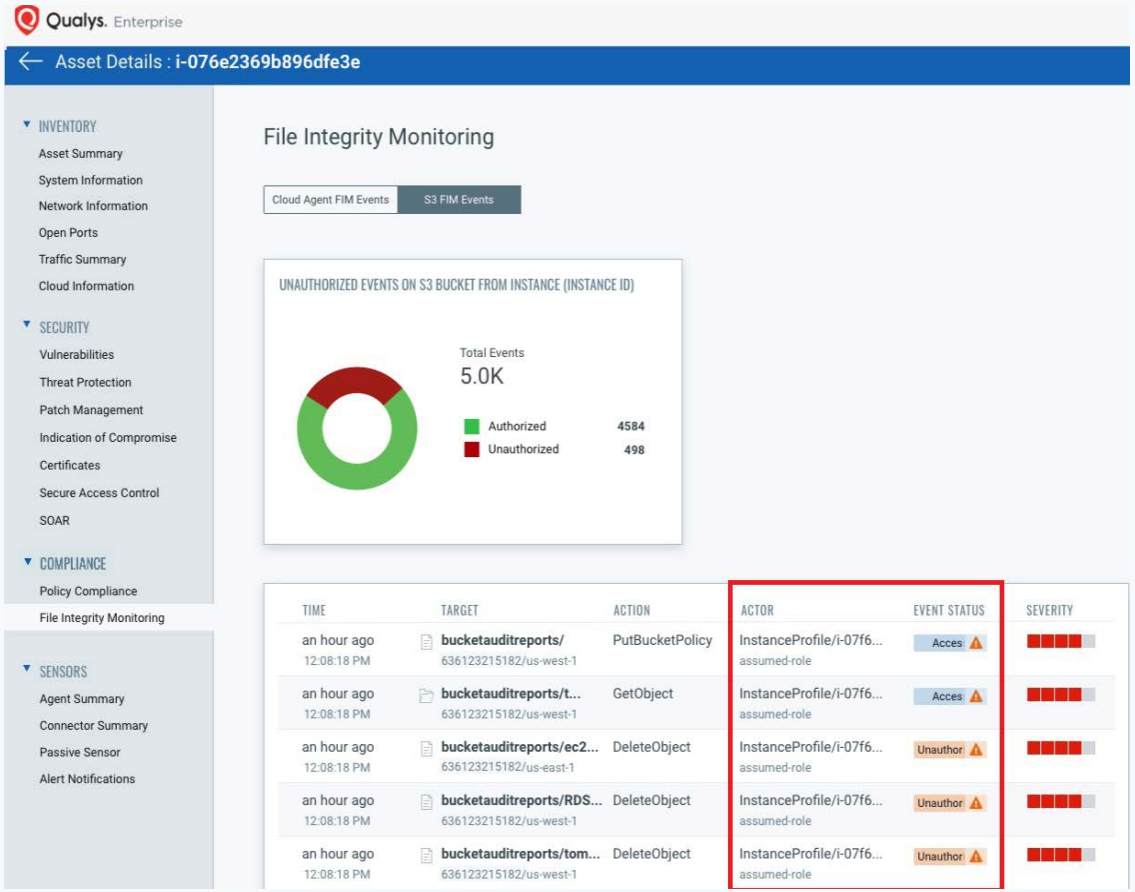
Qualys.

Open APIs for Integration



Qualys.

Context of Changes in Cloud



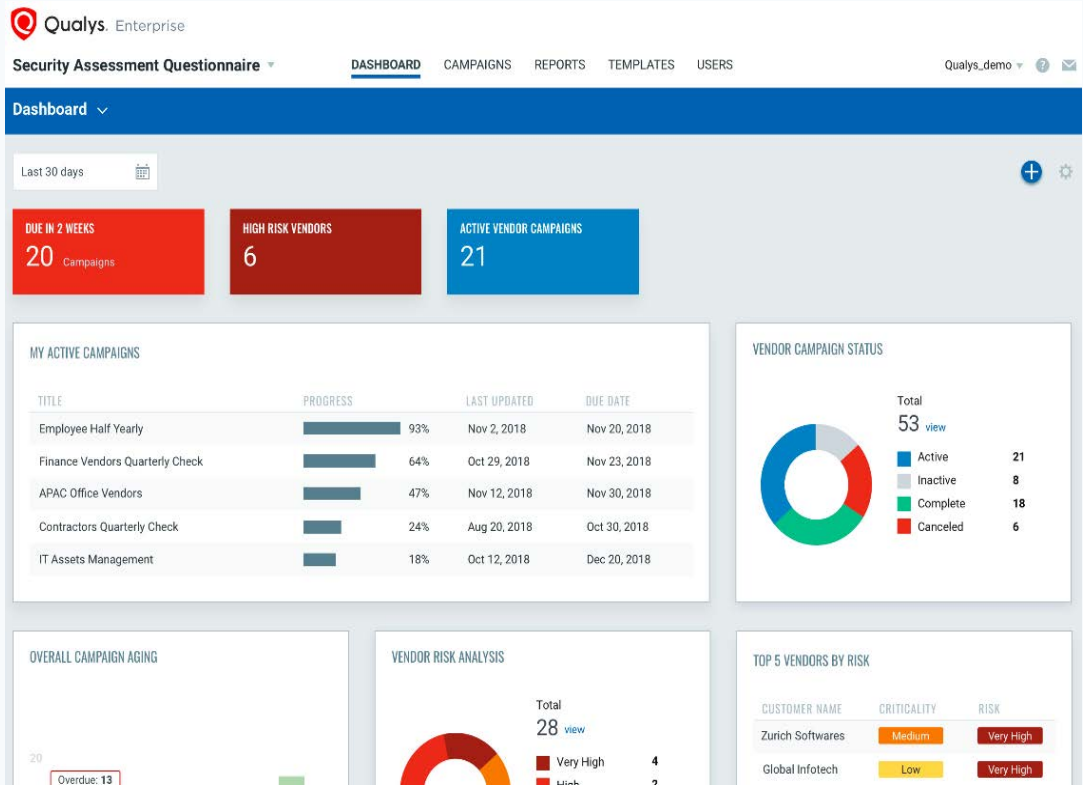
Qualys.

Assess Vendor Security

Manage vendor risk per vendor criticality

Unify Vendor security and process compliance with technical security

Qualys Security Assessment Questionnaire (SAQ)



SaaS Applications Challenges

Public cloud spending skyrockets as SaaS shines
IDG

IDC: Cloud spending to grow 21% by 2021
CIO DIVE

Office 365 box

Microsoft, Google Make Cloud Offerings More Enticing
eWEEK

HR gets the cloud treatment
THE AUSTRALIAN

Workday Rises on Demand for Business Cloud-Based Software
Bloomberg

workday. Namely

Spending On CRM Apps Predicted To Soar In 2018
COMPUTERWORLD

salesforce ZOHO

Qualys.

SaaS Security and Compliance

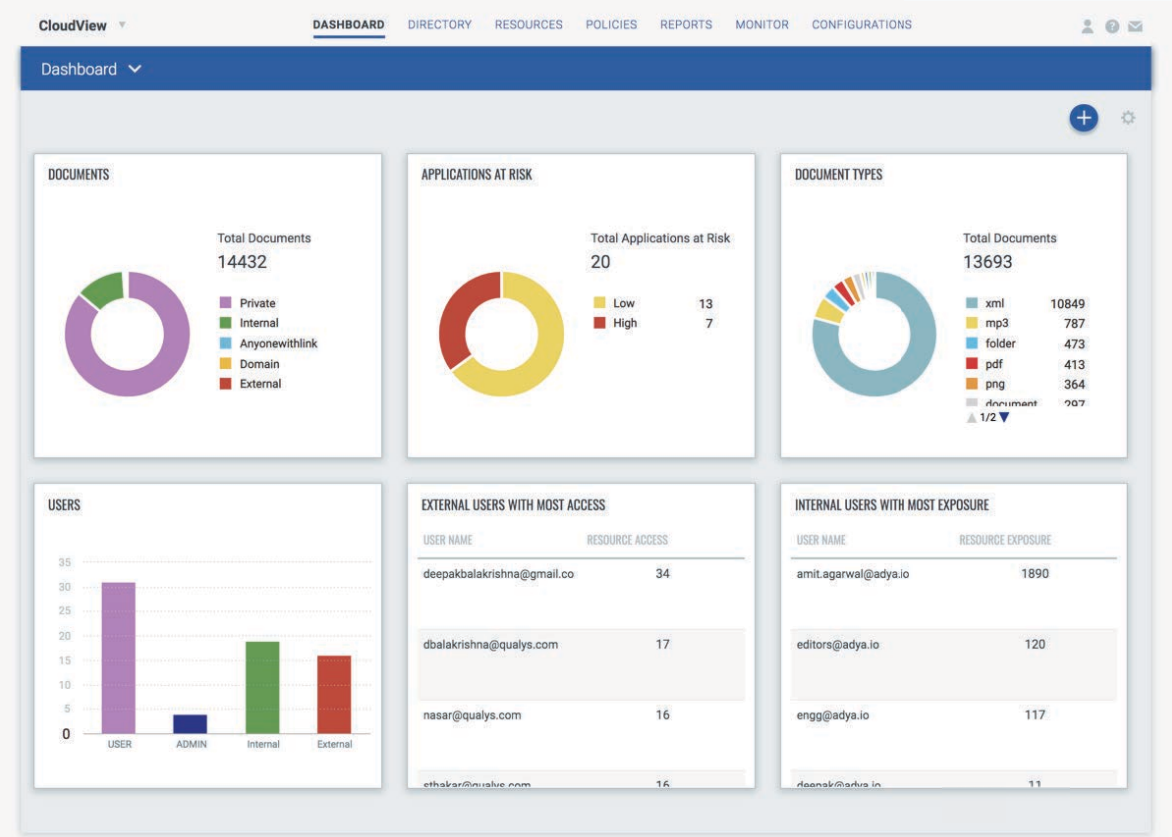
Inventory

Access

Exposure

Security Configurations

Office365, Google Suite, Salesforce
GitHub, Okta, Slack



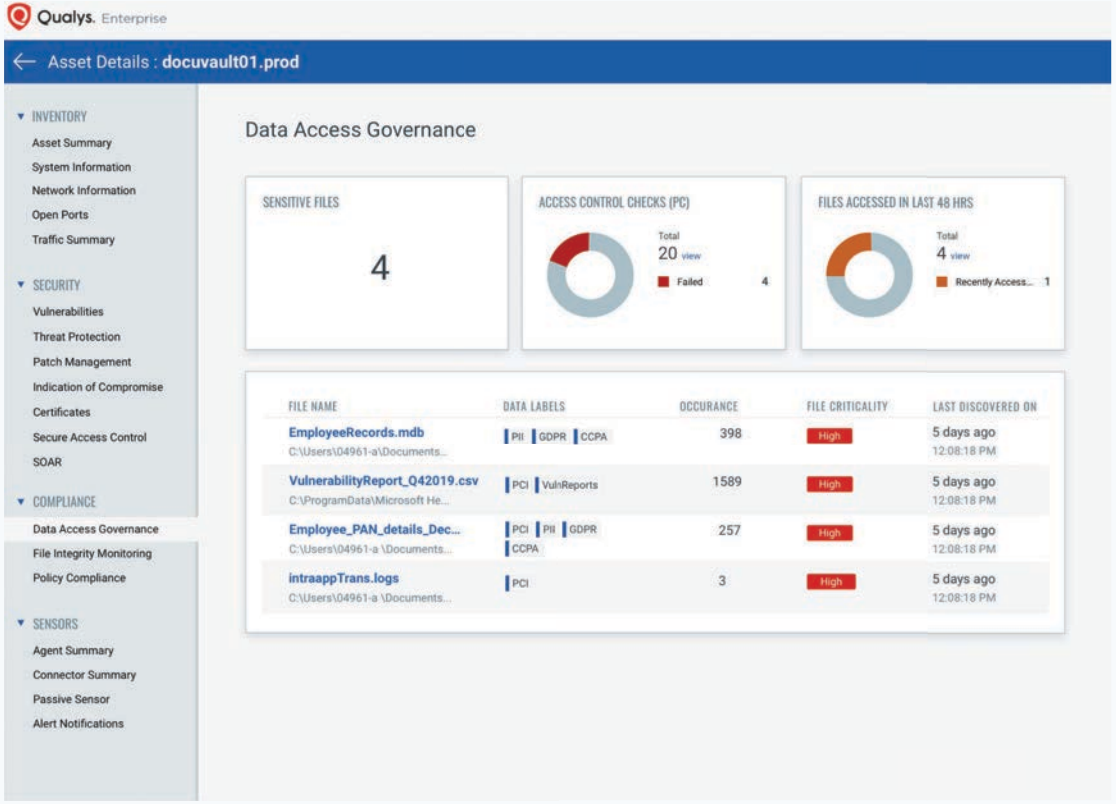
Sensitive Data Discovery and Security

Discovery

Access Visibility

Activity Monitoring

Context for security

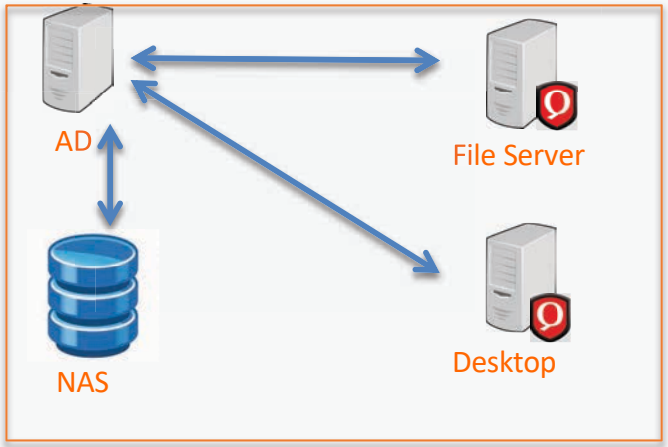


Cloud Applications

Directory / Metadata / Access /Classification

Adya/CV/CloudTrail

Qualys Agent (MFT)



On Premises Unstructured Data

Directory / Metadata / Access / Based on rules

Qualys Cloud Platform

Unstructured Data Discovery

Visibility in ITAM – know assets hold sensitive data

Secure through PC - Create permission/share/access controls to check their access

Compliance
GDPR / CCA / HIPAA/ etc

Monitor through FIM

Qualys.

Quick Demo

Thank You

Compliance Team and Shailesh Athalye
sathalye@qualys.com