



# 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



## Manual Audit Sampling Methods



Probability that system configurations have deviated from expectations or documentation

## Software Assisted Automated Audits



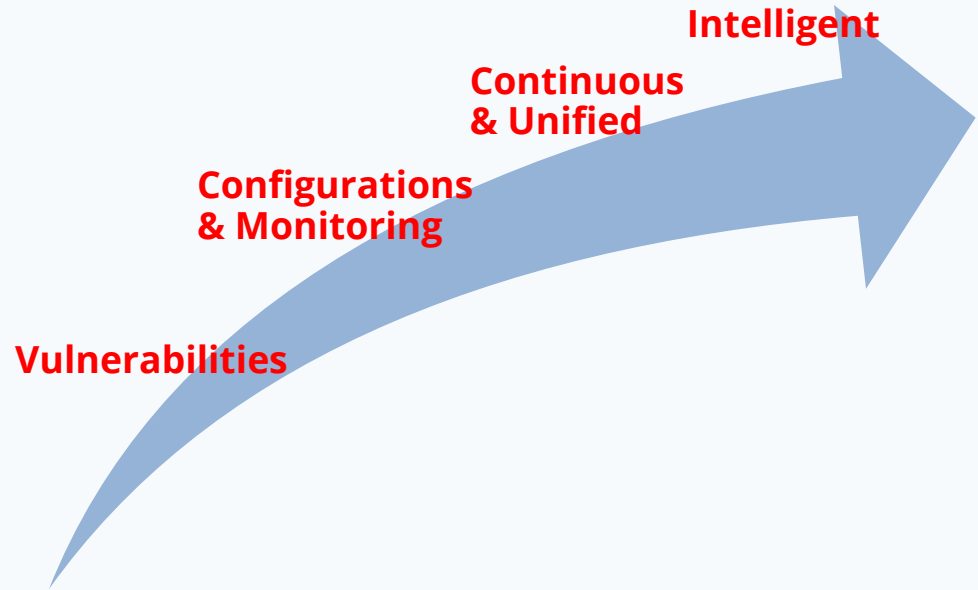
Avoid Treating Audits As A Discovery Exercise, Audits Should be Confirmation Exercise!

# 2020: 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


<b>PCI DSS Requirements</b>
<b>8.2.3</b> Passwords/passphrases must meet the following: <ul style="list-style-type: none"> <li>Require a minimum length of at least seven characters.</li> <li>Contain both numeric and alphabetic characters.</li> </ul> Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.
<b>8.2.4</b> 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: <ol style="list-style-type: none"> <li>EACMS;</li> <li>PACS; and</li> <li>PCA</li> </ol> Medium Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> <li>EACMS;</li> <li>PACS; and</li> <li>PCA</li> </ol>	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: <b>5.5.1.</b> Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and <b>5.5.2.</b> 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

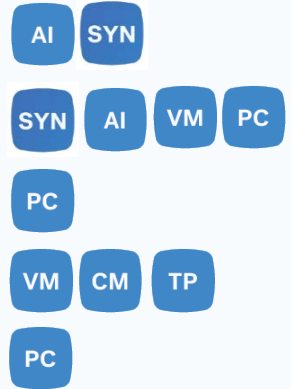
CSC 16-3	Ensure that systems automatically create a report that includes a list of locked-out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire. This list should be sent to the associated system administrator in a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



Inventory Your Systems

Inventory and Restrict Software

Secure Configurations  
 Continuous VM  
 Review Access Rights



# Semi-automated Way for Connecting is old!

Time to value

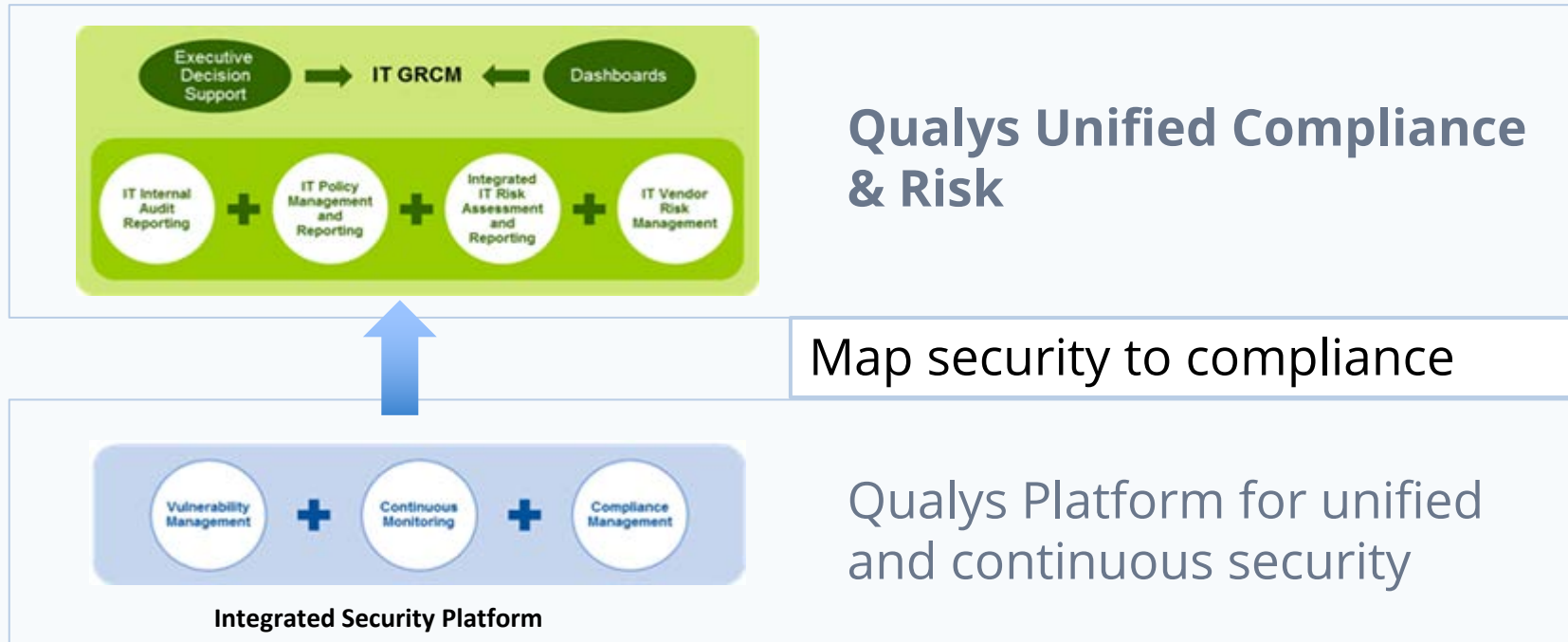
Time to see roll up the operational data

Varied types of Security and Assets data  
FIM, Patch, Malware, VM, threats  
Scoping and Tracking Assets

Point solutions injecting data with connectors, never normalize



# Continuous Compliance & Risk From Continuous Security



# Continuous Risk and Compliance from Continuous Security

Qualys Unified Compliance maps every app's output to 25+ Compliance standards and Risk objectives

The screenshot displays the Qualys Unified Compliance Assessment interface. At the top, navigation tabs include HOME, DASHBOARD, ASSESSMENT (selected), REPORTS, and CONFIGURATION. Below the navigation, there are four summary cards: TOTAL CONTROL OBJECTIVE (325), FAILED CONTROL OBJECTIVE (98), TOTAL CONTROLS EVALUATED (223K), and FAILED CONTROL EVALUATIONS (26K). The main content area shows a search bar with the query 'Mandate.name like %Fedramp Mod%' and a filter for 'Last 30 days'. A table lists assessment results for Mandate ID IA-5, 'Authenticator management', with 1992 objects. The table includes columns for Mandate ID, Objective, Objects, Posture Evaluation (Status, Pass, Fail), Assignment Status, and Criticality. The table is expanded to show details for 'Password-Based Authentication' (1308 Assets) and its sub-objects: 'Datacenter Assets' (1134 Assets), 'SaaS Objects' (1 Connector), and 'Mobile Devices' (170 Assets). Each sub-object has its own table of control evaluations with columns for CID, Control Name, Objects, Posture Evaluation, and Criticality.

MANDATE ID	OBJECTIVE	OBJECTS	STATUS	PASS	FAIL	ASGNT.STATUS	CRITICALITY	
IA-5	Authenticator management	1992	Fail	1036	959	-	Critical	
IA-5 (1)	Password-Based Authentication	1308 (Assets)	Fail	1011	297	-	Critical	
	Datacenter Assets	1134 (Assets)	Fail	907	227	-	NA	
	CID	CONTROL NAME	OBJECTS	POSTURE EVALUATION	CRITICALITY			
	1071	Status of minimum password strength	1058 (Assets)	Fail	838	220	Unassigned	Critical
	10459	Status of required special characters	824 (Assets)	Fail	634	190	Unassigned	Critical
	SaaS Objects	1 (Connector)	Pass	1	0	-	NA	
	CID	CONTROL NAME	OBJECTS	POSTURE EVALUATION	CRITICALITY			
	60032	GSUITE Admin Strong Password Policy...	1 (Connectors)	Pass	1	0	Resolved	Critical
	61011	Microsoft365 AD Password Policy Enforc...	1 (Connectors)	Pass	1	0	Resolved	Critical
	Mobile Devices	170 (Assets)	Fail	100	70	-	NA	
	CID	CONTROL NAME	OBJECTS	POSTURE EVALUATION	CRITICALITY			
	89	Mobile phone passcode length	170 (Assets)	Fail	100	70	In Progress	Critical
	Public Cloud Services	3 (Connectors)	Pass	3	0	-	NA	
	CID	CONTROL NAME	OBJECTS	POSTURE EVALUATION	CRITICALITY			
	6	Ensure that AWS IAM password policy is ...	3 (Connectors)	Pass	3	0	NA	Critical
	7	Ensure IAM password policy requires at ...	3 (Connectors)	Pass	3	0	NA	Critical

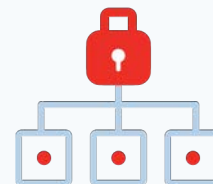
# New-age Challenges: Teams Speaking Different Languages



Elastic, Kafka, custom  
web servers



Identify risk and  
compliance



Secure hosts, config/integrity/  
vulnerability management

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



# Start Compliant, Stay Compliant in DevOps with Qualys PC in CI Phase

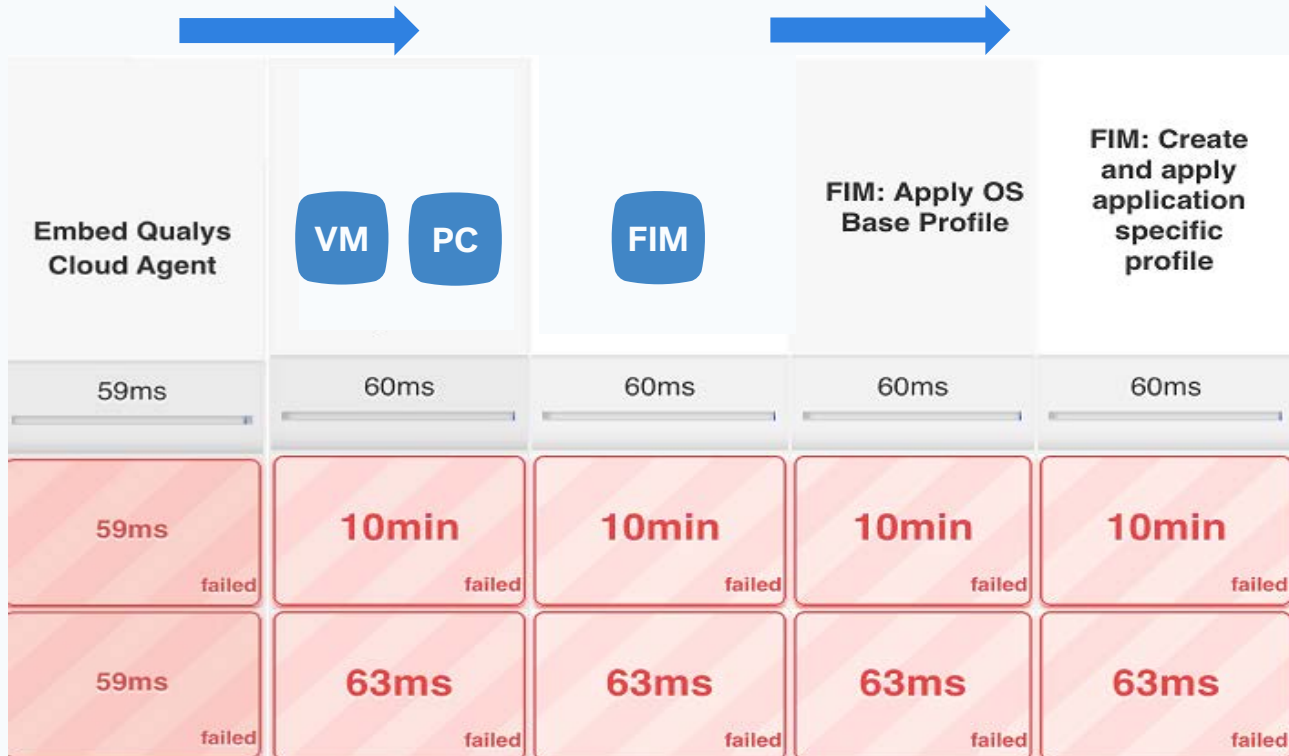
The screenshot shows the Jenkins pipeline configuration for 'aws-golden-ami-pipeline'. It features a 'Stage View' with two stages: 'Launch a CentOS instance with the Source AMI' and 'Launch VM & PC Scan on instance'. The first stage has an average time of 73ms and is currently running. The second stage has an average time of 10min 44s and is marked as 'failed' with a duration of 11min 21s. A white arrow points from the 'Stage View' to the 'QUALYS POLICY COMPLIANCE RESULTS' table on the right.

## 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/chronydc' 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

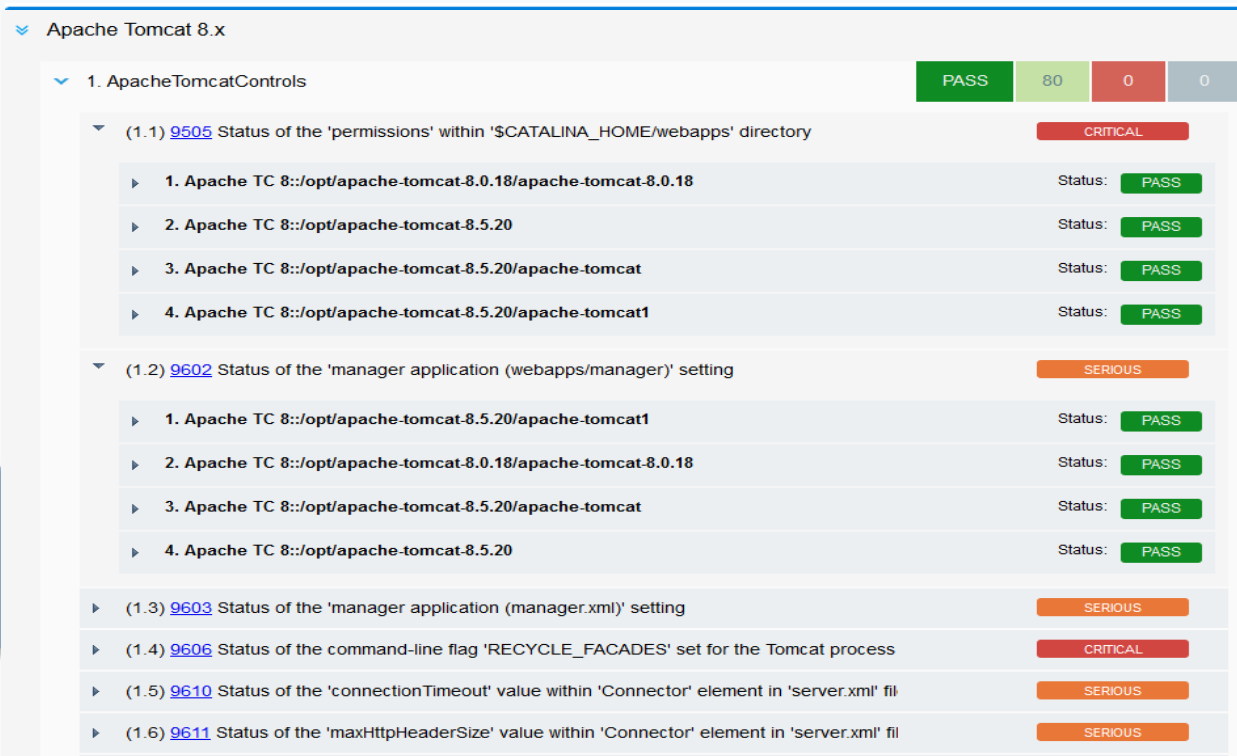
# Qualys FIM Monitors From CD Phase



# Automatically Discover and Assess Middleware with Dynamic Paths

Just based on host scans,  
discover unauthorized  
technologies,  
web servers,  
databases automatically

And...  
There's no need to  
create authentication  
records



Category	Severity	Count
PASS	80	0

Item	Status
1. ApacheTomcatControls	CRITICAL
(1.1) 9505 Status of the 'permissions' within '\$CATALINA_HOME/webapps' directory	CRITICAL
1. Apache TC 8::/opt/apache-tomcat-8.0.18/apache-tomcat-8.0.18	PASS
2. Apache TC 8::/opt/apache-tomcat-8.5.20	PASS
3. Apache TC 8::/opt/apache-tomcat-8.5.20/apache-tomcat	PASS
4. Apache TC 8::/opt/apache-tomcat-8.5.20/apache-tomcat1	PASS
(1.2) 9602 Status of the 'manager application (webapps/manager)' setting	SERIOUS
1. Apache TC 8::/opt/apache-tomcat-8.5.20/apache-tomcat1	PASS
2. Apache TC 8::/opt/apache-tomcat-8.0.18/apache-tomcat-8.0.18	PASS
3. Apache TC 8::/opt/apache-tomcat-8.5.20/apache-tomcat	PASS
4. Apache TC 8::/opt/apache-tomcat-8.5.20	PASS
(1.3) 9603 Status of the 'manager application (manager.xml)' setting	SERIOUS
(1.4) 9606 Status of the command-line flag 'RECYCLE_FACADES' set for the Tomcat process	CRITICAL
(1.5) 9610 Status of the 'connectionTimeout' value within 'Connector' element in 'server.xml' file	SERIOUS
(1.6) 9611 Status of the 'maxHttpHeaderSize' value within 'Connector' element in 'server.xml' file	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 to test and confirm that security tools have their pre-requisites in place and are configured properly on all endpoints

# Security Control Validation from Policy Compliance

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

**Reports**

**51**  
Total Control Instances

**Control View**

pc.policy.name: "Qualys Security windows" and pc.control.category: "Anti-Virus/Malware"

1 - 50 of 51

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

# Start Gold, Continuously Assess, Remediate

Policy Compliance ▾ DASHBOARD POLICIES SCANS **REPORTS** EXCEPTIONS ASSETS USERS 👤 ? 📧

**Reports** Reports Schedules Policy Summary **Control View** Templates Setup

72  
Total Controls

LABELS  
Qualys 72

TAGS  
USproduction 72

Policy.name like '%RDP%' and asset.tagName='USproduction' and control.status='failed' Last 24 Hrs

Display: Unified Control Asset

CONTROL COMPLIANCE Policy.name like '%RDP%'

100%

● Failing 06

TRENDING

1 - 50 of 75 [🔍] [🔄] [📄] [⚙️]

Actions ▾ Group by... ▾

**Create Remediation Job**

Create Alert

Add Exception

	CONTROL NAME	TECHNOLOGY	ASSET NAME	POLICY EVALUATION
<input checked="" type="checkbox"/>	Status of the 'Terminal Services' service	Windows 2008 Server	XAVIERHQ39WIN 10.10.31.30	Jun 02, 2018
<input checked="" type="checkbox"/> Failed Mar 21, 2018	Status of the 'Terminal Services' service	Windows 7	SFO03HQLP79 10.10.35.242	Mar 21, 2018
<input checked="" type="checkbox"/> Failed Jun 02, 2017	Status of the 'Set time limit for active Remote Desktop Services sessions' setting	Windows 10	SFO04HQLP713 10.10.35.241	May 03, 2018
<input checked="" type="checkbox"/> Failed Jun 12, 2018	Current list of Groups and User Accounts granted the 'Deny logon through terminal (Remote Desktop)...	Windows 2008 Server	DC03SJC1SQLDB 10.10.31.129	Oct 22, 2018

# Network Devices, Printers and sensitive hosts can't be Scanned but are in Security & Compliance Scope

## Use Qualys Out-of-Band Config Assessment (OCA)

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

Controls validate settings

Report vulnerabilities, security and misconfigurations

The screenshot shows the HP Qualys OCA interface. At the top, there is a blue header with the HP logo and a menu (File, View, Help). Below the header, the main content area is titled "Detailed Results".

The main results section shows the IP address 154.36.214.3 (hp-in01-prn02, HP-IN01-PRN02) and the asset name HP FutureSmart 4. A summary bar indicates 12 controls passed (100%), 2 failed, and 0 errors. The tracking method is OCA, and the last scan date is 09/05/2019 at 11:12:12 (GMT+0530).

Below the summary, there is a section for "HP FutureSmart 4.x" with a sub-section for "1. System Configuration". This section lists several checks with their IDs, descriptions, severity levels, and statuses:

ID	Description	Severity	Status
(1.1) 1116	Status of the 'File Transfer Protocol (FTP)' service	CRITICAL	PASS
(1.2) 1861	Status of the 'telnet' service	CRITICAL	FAIL
(1.3) 10270	Status of the SNMP community strings	SERIOUS	PASS
(1.4) 12413	Status of the 'AppleTalk' protocol	SERIOUS	PASS
(1.5) 13857	Status of version of firmware stored in boot PROM	CRITICAL	PASS
(1.6) 14039	Status of SNMP configuration of version SNMPv1	CRITICAL	PASS

# Policy Compliance

Best in class technology and content coverage  
For Configuration Management

- >450 Policies, >14,000 controls
- >150 technologies (traditional, emerging)
- > Widest coverage for CIS, STIG, Mandates and beyond
- > Qualys security experts author CIS benchmarks

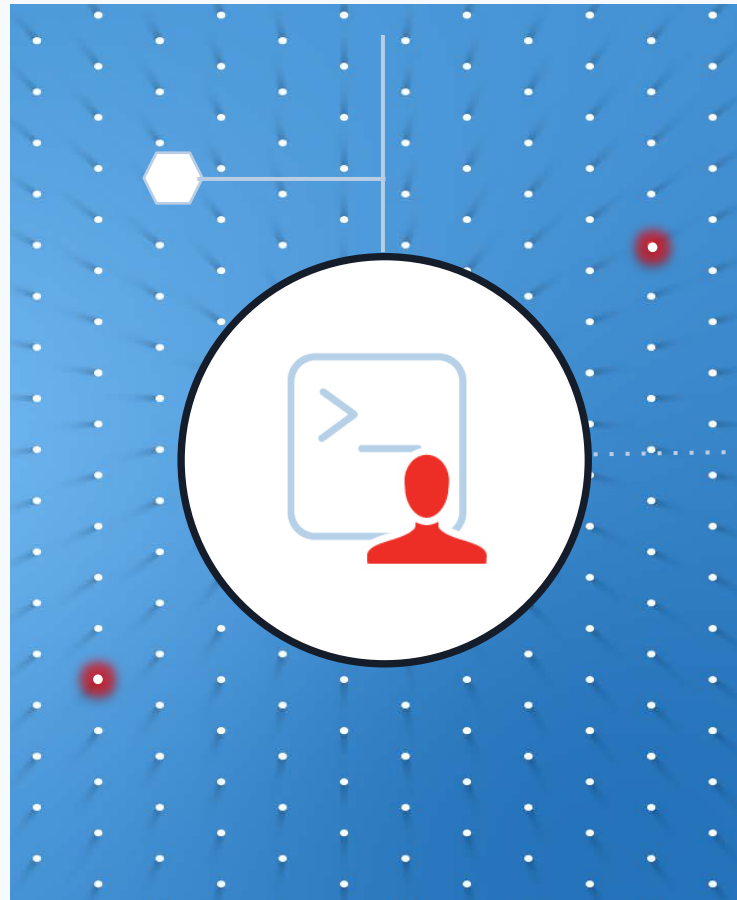
Data collection from all Qualys sensors

Custom database security & integrity controls


Auto-discovery of middleware technologies

File, Directory Integrity, Network Shares  
Monitoring

Auto-remediation for configuration failures







# New PC UI and Customizable Dashboard

# Policy Compliance Roadmap

**Q4 - 2018**

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

**2020 Q1**

**New PC UI, customizable dashboards**  
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

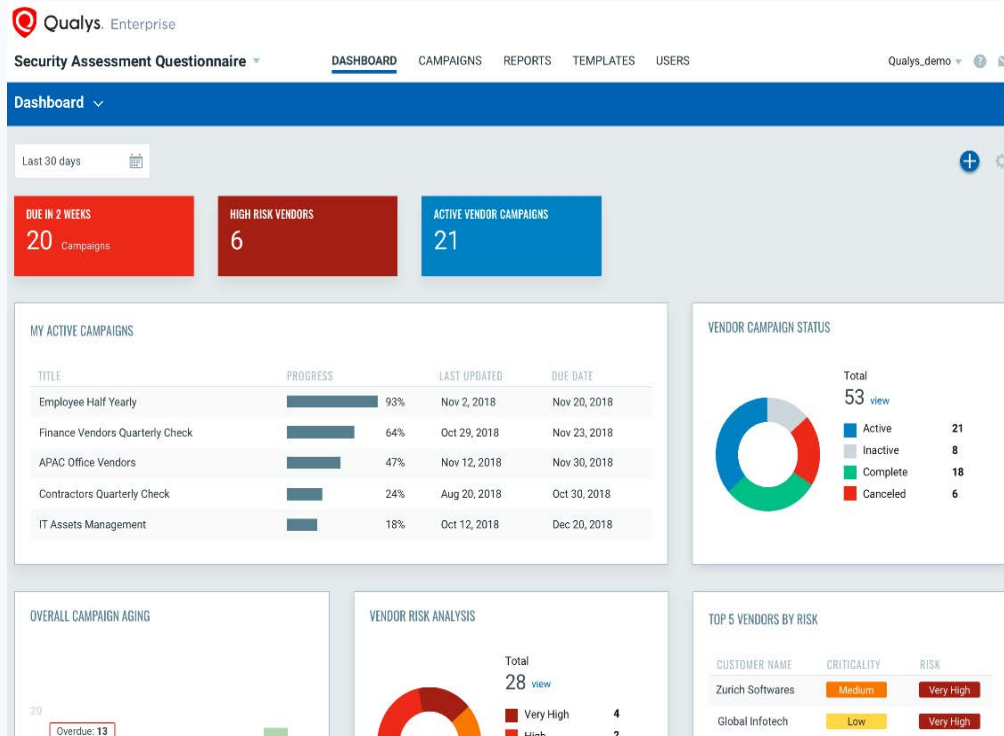
**2020 Q2**

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

# Your security is only as strong as your weakest vendor

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

With **SAQ**, consolidate your vendor security and process compliance with technical security posture on the same platform



The background is a solid blue color with a pattern of small white dots arranged in a grid. The dots are slightly larger and more prominent in the center, creating a subtle gradient effect.

# File Integrity Monitoring (FIM)

# Qualys FIM: In just Second Year, 190+ customers

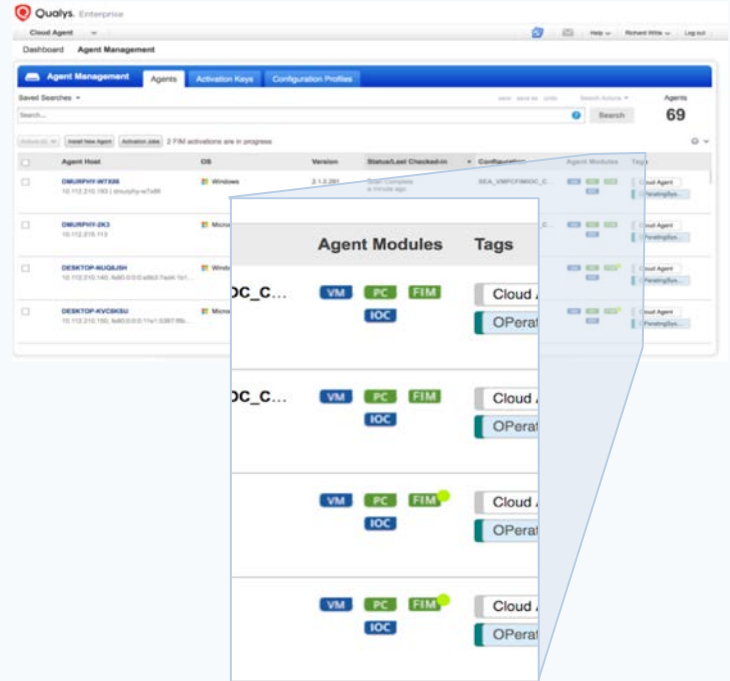
Built on the same Qualys Cloud Agent you use for VM, PC

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, data load for you to manage



# Alert and Incident Management for Authorized vs Unauthorized Changes During Patching with Qualys FIM

The screenshot displays the Qualys Enterprise File Integrity Monitoring (FIM) interface. The top navigation bar includes 'File Integrity Monitoring' and various menu items: DASHBOARD, EVENTS, RULES (selected), INCIDENTS, REPORTS, ASSETS, and CONFIGURATION. A search bar contains the query: `ruleName:"Unauthorized Windows Patching Activity" or ruleName:"Authorized Windows Patching Activity"`. A filter dropdown is set to 'Last 30 Days'. Below the search bar is a bar chart showing activity levels over time, with a peak on 13 Nov. The main content area features a table with columns: RULE NAME, STATUS, AGGREGATE, ACTION, MATCHES, and CREATED BY. The table lists three entries, all with a 'Success' status and one match each, created by 'Aparna Hinge'.

**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

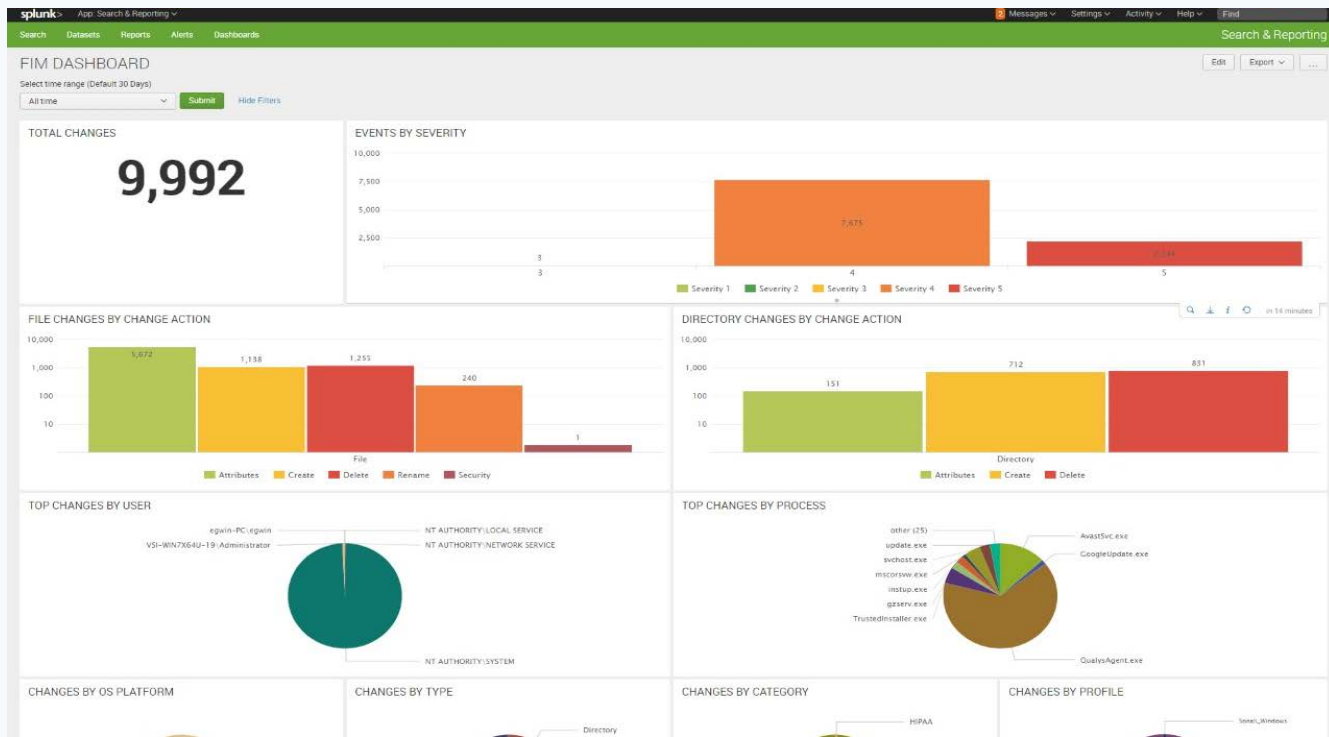
3 Total Activities

RULE NAME	STATUS	AGGREGATE	ACTION	MATCHES	CREATED BY
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

1 - 3 of 3

Qualys

# Open APIs: Integrate with Any External SIEM, DWH



# Qualys FIM gives context of changes in cloud

Qualys. Enterprise

← Asset Details : i-076e2369b896dfe3e

- INVENTORY
  - Asset Summary
  - System Information
  - Network Information
  - Open Ports
  - Traffic Summary
  - Cloud Information
- SECURITY
  - Vulnerabilities
  - Threat Protection
  - Patch Management
  - Indication of Compromise
  - Certificates
  - Secure Access Control
  - SOAR
- COMPLIANCE
  - Policy Compliance
  - File Integrity Monitoring
- SENSORS
  - Agent Summary
  - Connector Summary
  - Passive Sensor
  - Alert Notifications

## File Integrity Monitoring

Cloud Agent FIM Events | S3 FIM Events

UNAUTHORIZED EVENTS ON S3 BUCKET FROM INSTANCE (INSTANCE ID)

Total Events  
5.0K

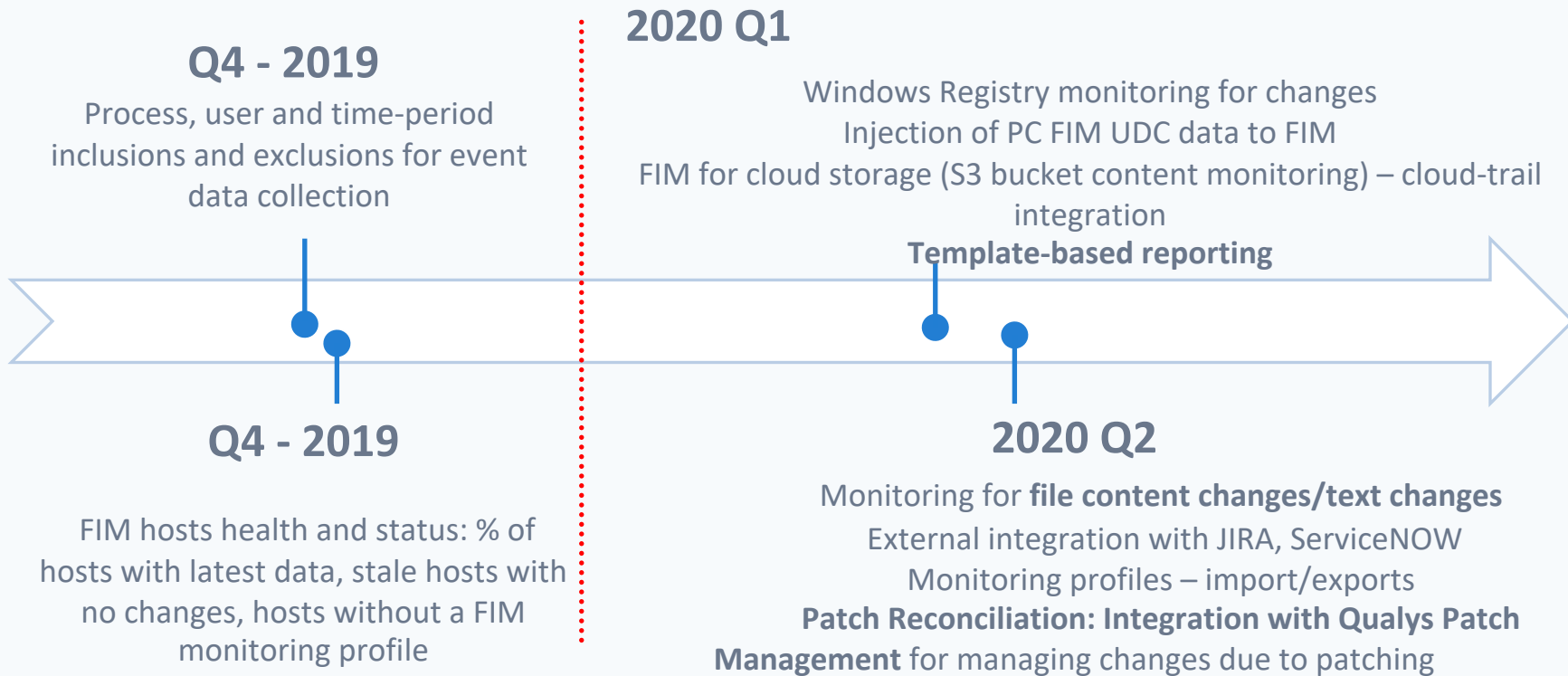
- Authorized 4584
- Unauthorized 498

TIME	TARGET	ACTION	ACTOR	EVENT STATUS	SEVERITY
an hour ago 12:08:18 PM	bucketauditreports/ 636123215182/us-west-1	PutBucketPolicy	InstanceProfile/i-07f6... assumed-role	Access ⚠	██████
an hour ago 12:08:18 PM	bucketauditreports/L... 636123215182/us-west-1	GetObject	InstanceProfile/i-07f6... assumed-role	Access ⚠	██████
an hour ago 12:08:18 PM	bucketauditreports/ec2... 636123215182/us-east-1	DeleteObject	InstanceProfile/i-07f6... assumed-role	Unauthor ⚠	██████
an hour ago 12:08:18 PM	bucketauditreports/RDS... 636123215182/us-west-1	DeleteObject	InstanceProfile/i-07f6... assumed-role	Unauthor ⚠	██████
an hour ago 12:08:18 PM	bucketauditreports/tom... 636123215182/us-west-1	DeleteObject	InstanceProfile/i-07f6... assumed-role	Unauthor ⚠	██████



# FIM Demo

# FIM Roadmap



# Software as a Service (SaaS) Security & Compliance

# Even Cloud is bloated; Need just SaaS Applications

Public cloud spending skyrockets as SaaS shines 

**IDC: Cloud spending to grow 21% by 2021**



**HR gets the cloud treatment**

THE AUSTRALIAN

**Workday Rises on Demand for Business Cloud-Based Software**

Bloomberg



Spending On CRM Apps Predicted To Soar In 2018

COMPUTERWORLD



Microsoft, Google Make Cloud Offerings More Enticing

eWEEK

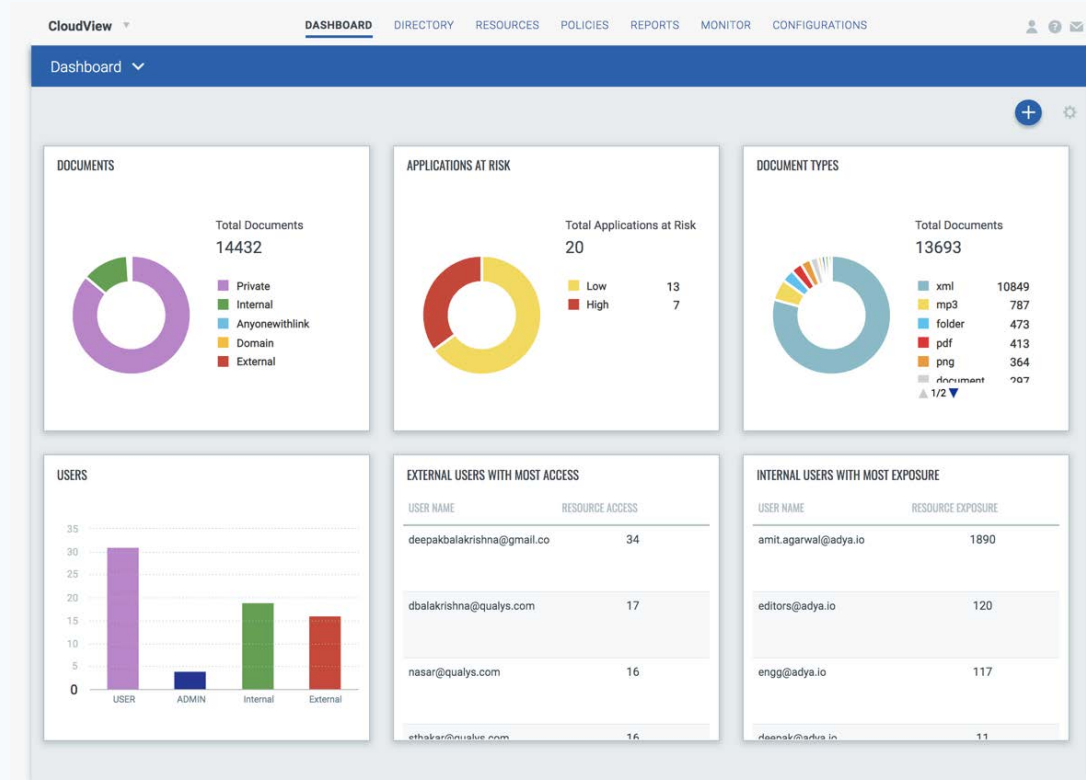


# Manage Access, Exposure, Configuration and Compliance of SaaS Applications

**Qualys SaaS Security and Compliance (SSC)** enables

Inventory  
Access  
Exposure  
Security Configurations

of SaaS applications and resources  
E.g. Office365, Gsuite, Salesforce

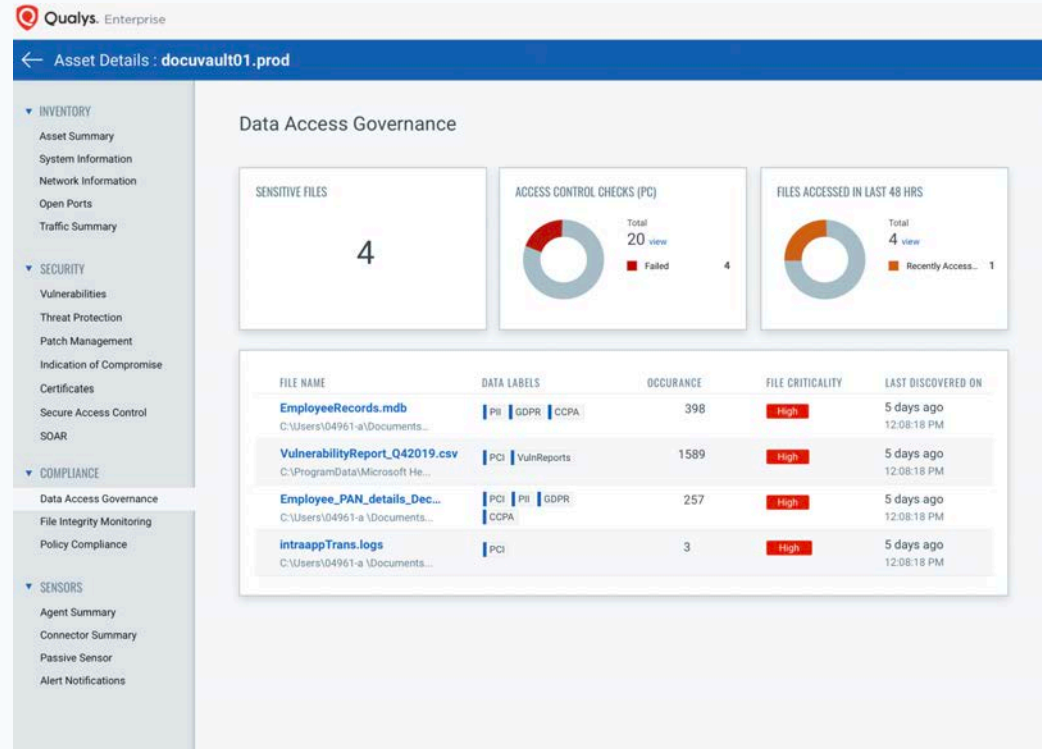


# Discover Sensitive data and make sure it is secure and monitored for changes with Qualys DAG

**Qualys Data Access Governance (DAG)** will help with regulatory compliance

Discovery  
Access Visibility  
Activity Monitoring

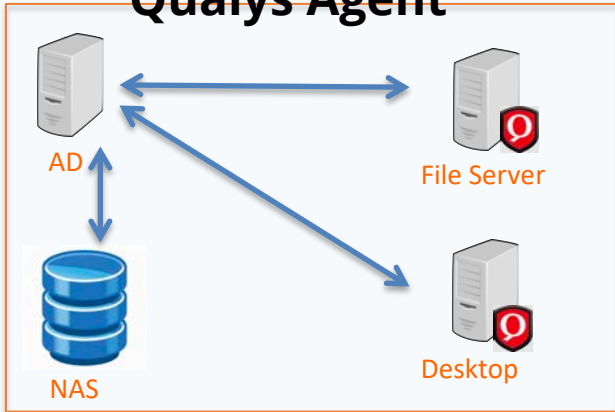
For your sensitive, critical data



# Cloud Applications



## Qualys Agent



### On Premise Unstructured Data

Directory / Metadata / access / classification  
Adya/CV/CloudTrail

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 them through FIM



# Thank You

Compliance Team and Shailesh Athalye  
[sathalye@qualys.com](mailto:sathalye@qualys.com)