



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



Q1

Probability that system configurations have deviated from expectations or documentation

Q2

Software Assisted Automated Audits



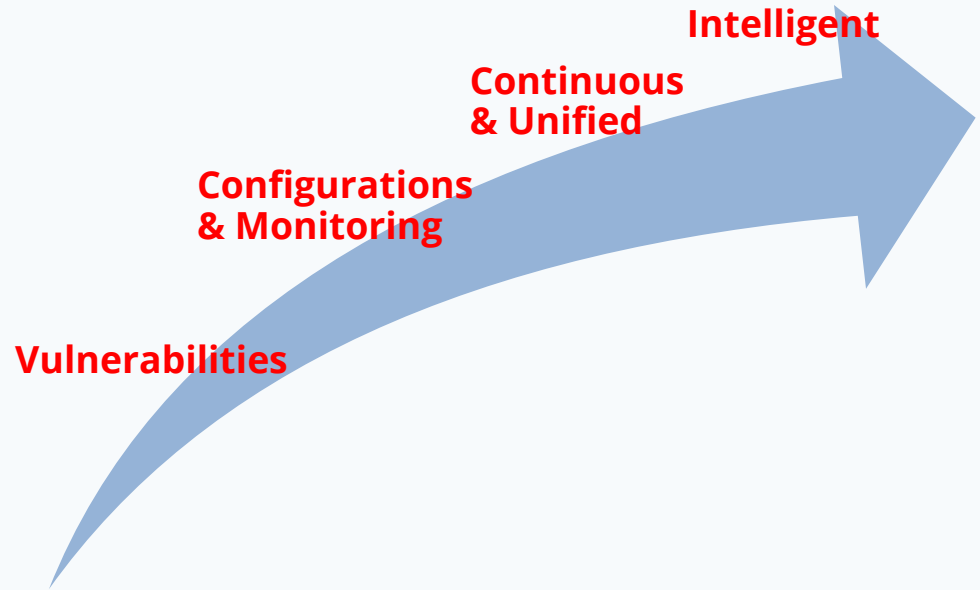
Avoid Treating Audits As A Discovery Exercise, Audits Should be Confirmation Exercise!

2020: Security is Continuous and Unified

To reduce the 'attack surface'

To reduce breaches due to misconfigurations, lack of monitoring

Question remains:
How to make Compliance and Risk continuous?



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



Connect Security with Compliance and Risk



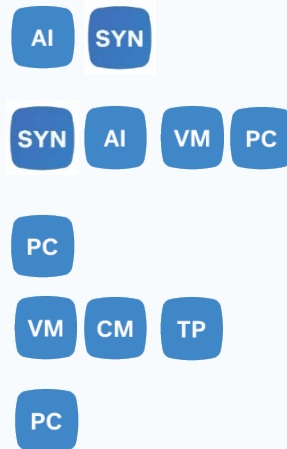
Inventory Your Systems

Inventory and Restrict Software

Secure Configurations and Data Security

Continuous VM

Review Access Rights



PCI DSS Requirements
<p>8.2.3 Passwords/passphrases must meet the following:</p> <ul style="list-style-type: none"> Require a minimum length of at least seven characters. Contain both numeric and alphabetic characters. <p>Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.</p> <p>8.2.4 Change user passwords/passphrases at least once every 90 days.</p>

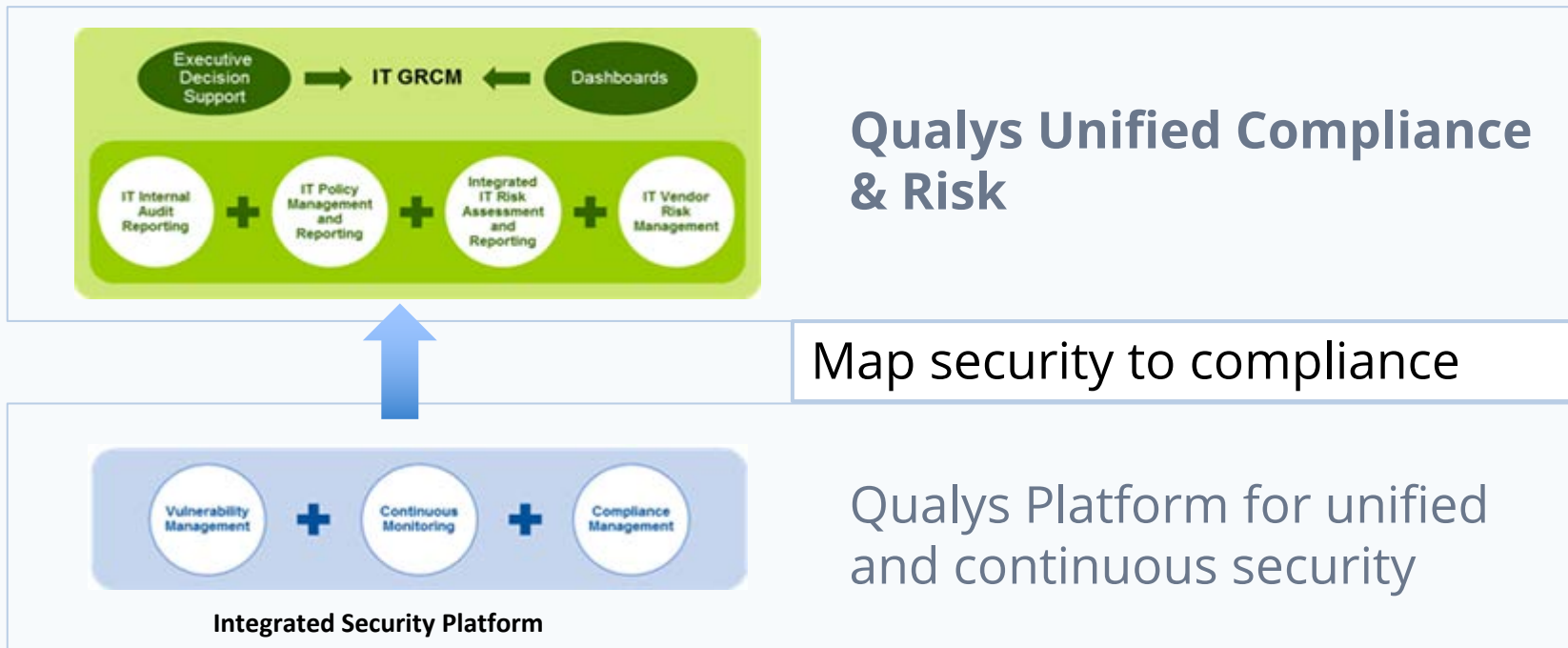
Section of HIPAA Security Rule	HIPAA Security Rule Standards	Implementation Specifications
164.308(a)(5)(ii)(D)		Password Management (A): Procedures for creating, changing, and safeguarding passwords.

CIP-007-5 Table R5 – System Access Control		
Part	Applicable Systems	Requirements
5.5	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> EACMS; PACS; and PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> EACMS; PACS; and PCA 	<p>For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:</p> <p>5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and</p> <p>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</p>

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

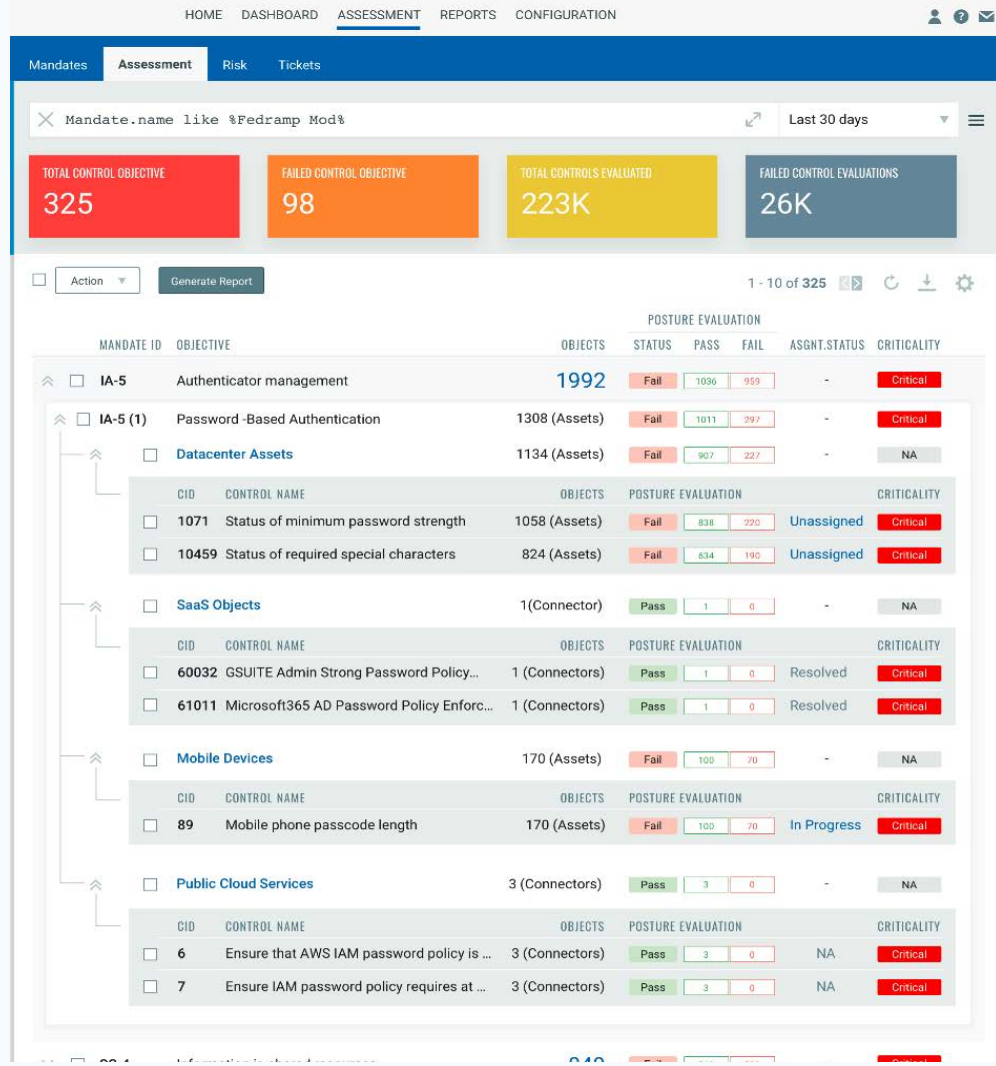
CSC 16-3	<p>Ensure that systems automatically create a report that includes a list of locked-out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire. This list should be sent to the associated system administrator in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

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



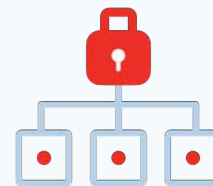
New-age Challenges: Teams Speaking Different Languages



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

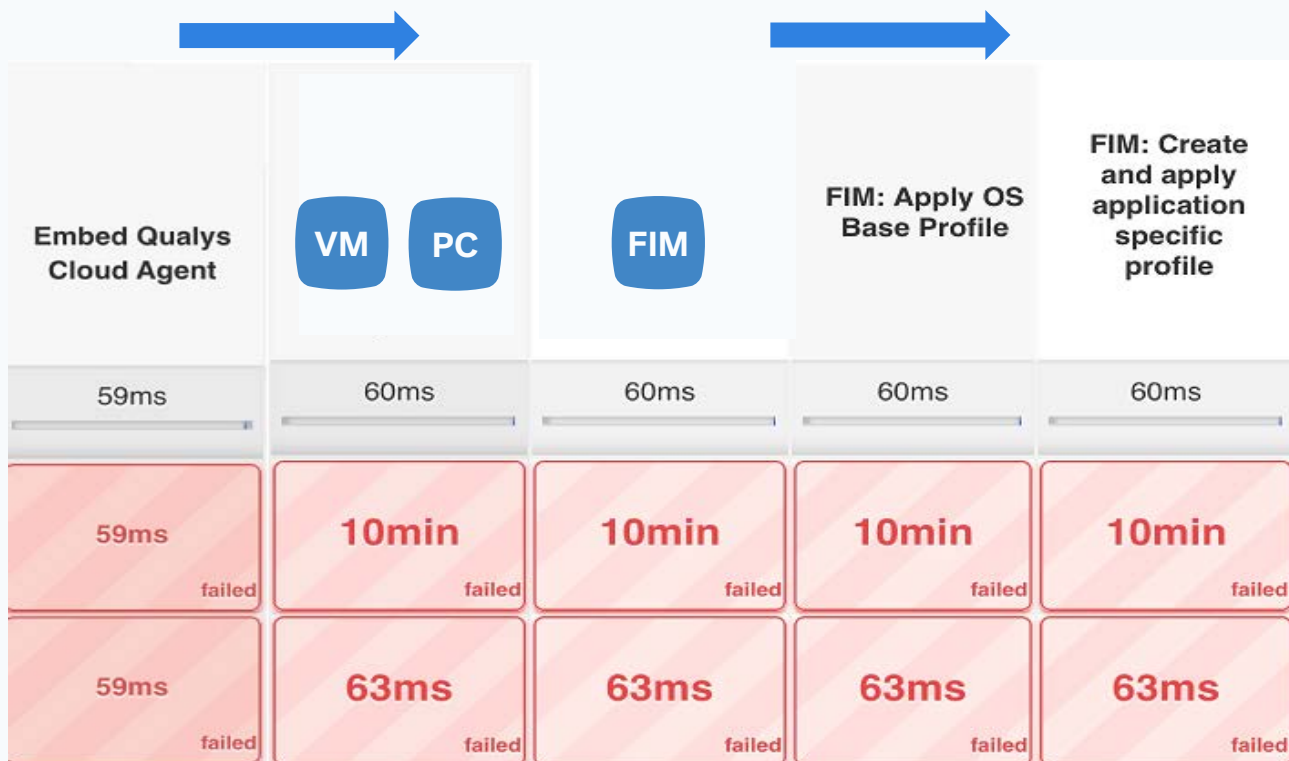
The screenshot shows the Jenkins pipeline configuration for 'aws-golden-ami-pipeline'. It features a 'Stage View' with two stages: 'Launch a CentOS instance with the Source AMI' and 'Launch VM & PC Scan on instance'. The first stage has an average time of 73ms and is successful. The second stage has 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

The screenshot displays a security assessment tool interface for Apache Tomcat 8.x. The interface is organized into a tree view under the heading 'Apache Tomcat 8.x'. A summary bar at the top right shows 'PASS' in a green box, a score of '80' in a light green box, and '0' in red boxes for 'CRITICAL' and 'SERIOUS' findings. The main content is a list of findings, each with a severity level, a description, and a status.

Severity	Description	Status
Critical	(1.1) 9505 Status of the 'permissions' within '\$CATALINA_HOME/webapps/' directory	CRITICAL
Pass	1. Apache TC 8::/opt/apache-tomcat-8.0.18/apache-tomcat-8.0.18	PASS
Pass	2. Apache TC 8::/opt/apache-tomcat-8.5.20	PASS
Pass	3. Apache TC 8::/opt/apache-tomcat-8.5.20/apache-tomcat	PASS
Pass	4. Apache TC 8::/opt/apache-tomcat-8.5.20/apache-tomcat1	PASS
Serious	(1.2) 9602 Status of the 'manager application (webapps/manager)' setting	SERIOUS
Pass	1. Apache TC 8::/opt/apache-tomcat-8.5.20/apache-tomcat1	PASS
Pass	2. Apache TC 8::/opt/apache-tomcat-8.0.18/apache-tomcat-8.0.18	PASS
Pass	3. Apache TC 8::/opt/apache-tomcat-8.5.20/apache-tomcat	PASS
Pass	4. Apache TC 8::/opt/apache-tomcat-8.5.20	PASS
Serious	(1.3) 9603 Status of the 'manager application (manager.xml)' setting	SERIOUS
Critical	(1.4) 9606 Status of the command-line flag 'RECYCLE_FACADES' set for the Tomcat process	CRITICAL
Serious	(1.5) 9610 Status of the 'connectionTimeout' value within 'Connector' element in 'server.xml' file	SERIOUS
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	
PASS	12364	Status of the 'CommunicationStatus' (Last time st	Windows 10	comqaw10es	Nov 13, 2019
Nov 13, 2019			os	10.10.36.126 COMQA	
PASS	12364	Status of the 'CommunicationStatus' (Last time st	Windows Server 2012 R2	i-6f91d2a8	Nov 13, 2019
Nov 13, 2019			os	10.11.114.112 I-6F91D	
PASS	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-	
PASS	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					
PASS	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	

CATEGORY
Anti-Virus/Malwa... 51

CRITICALITY
MEDIUM 3
SERIOUS 18
CRITICAL 26
URGENT 4

POSTURE
PASS 41
ERROR 1
FAIL 9

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. Below it, a navigation bar contains 'File', 'View', and 'Help'. The main content area is titled 'Detailed Results' and shows the following information:

154.36.214.3 (hp-in01-prn02, HP-IN01-PRN02)
HP FutureSmart 4

Tracking Method: OCA
Last Scan Date: 09/05/2019 at 11:12:12 (GMT+0530)
Qualys Host ID: c9192ca4-fbf-454c-82fa-8c31003521fa
Asset Tags: OCA

Controls: 12
Passed: 12 (100%)
Failed: 0
Error: 0
Approved Exceptions: 0
Pending Exceptions: 0

Below this, there is a section for 'HP FutureSmart 4.x' with a sub-section '1. System Configuration'. This section contains a list of checks:

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

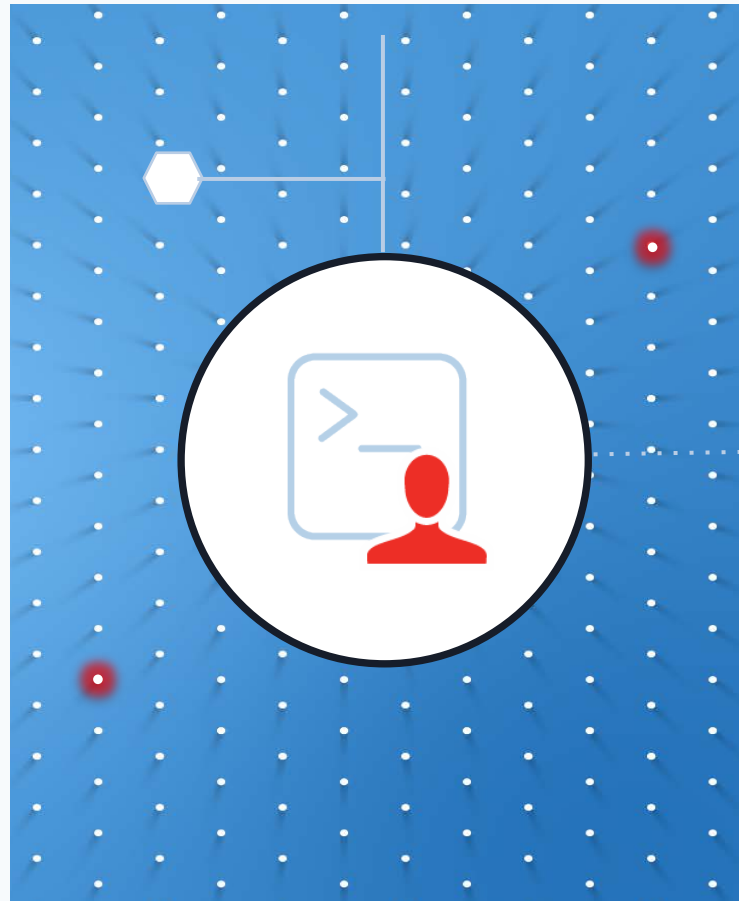
Data collection from all Qualys sensors


Custom database security & integrity controls

Auto-discovery of middleware technologies

File, Directory Integrity, Network Shares
Monitoring

Auto-remediation for configuration failures



The background is a solid blue color with a pattern of small white dots arranged in a grid-like fashion, with some dots missing or faded, creating a subtle texture.

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

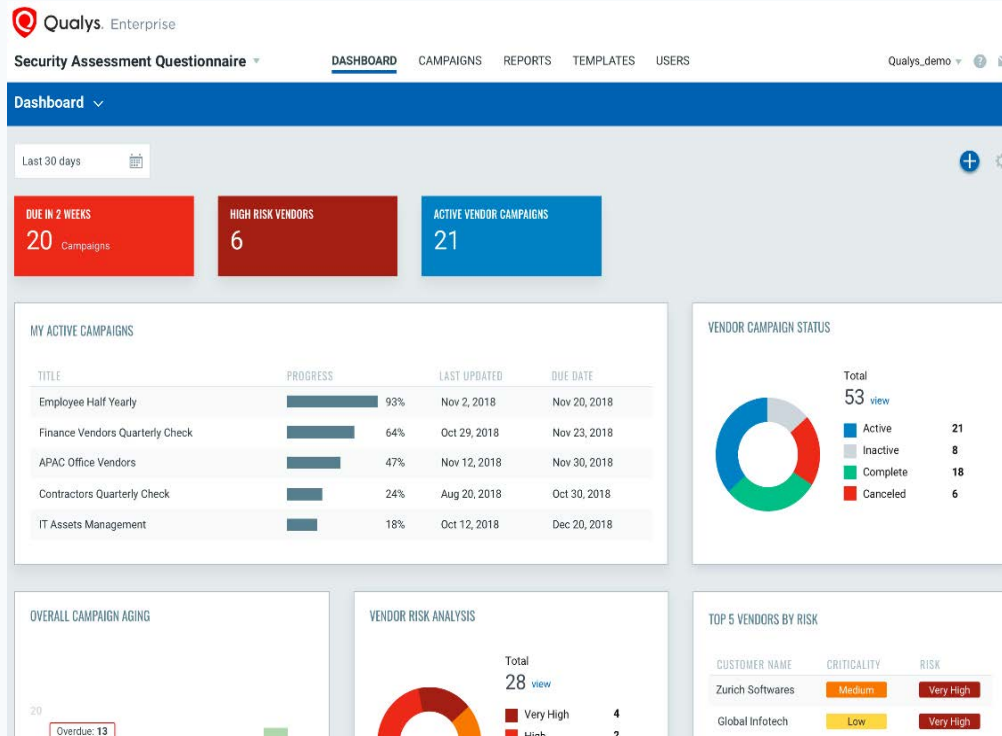
2020 Q2

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 subtle pattern of small white dots arranged in a grid. A large, faint, light blue circle is centered behind the text, creating a gradient effect.

File Integrity Monitoring (FIM)

Qualys FIM: In just Second Year, 190+ customers

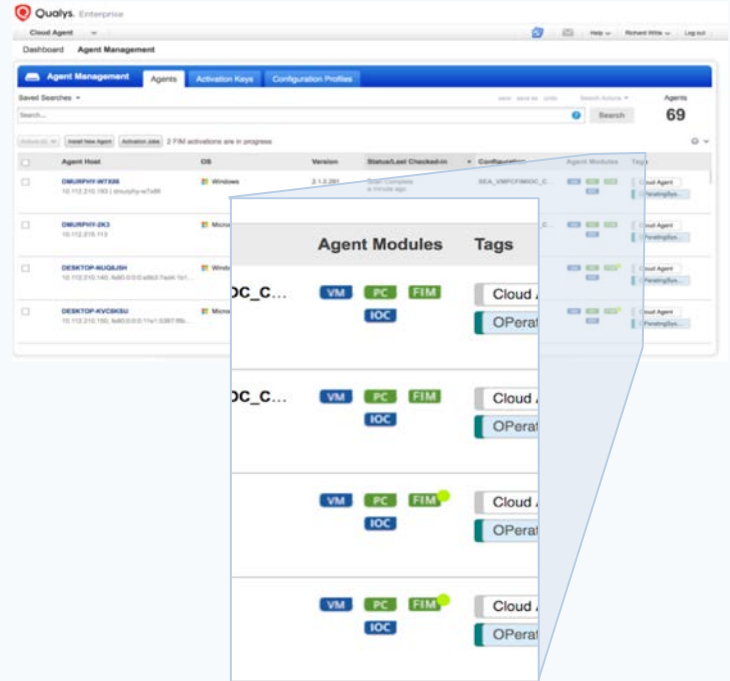
Built on the same Qualys Cloud Agent you use for VM, PC

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

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	2				
Authorized Windows Patching Activity	1				
ACTION NAME					
Windows Patch ...	3				
EMAIL RECIPIENTS					
ljhamb@qualys.c...	3				
akaur@qualys.co...	3				
shing@qualys.c...	2				

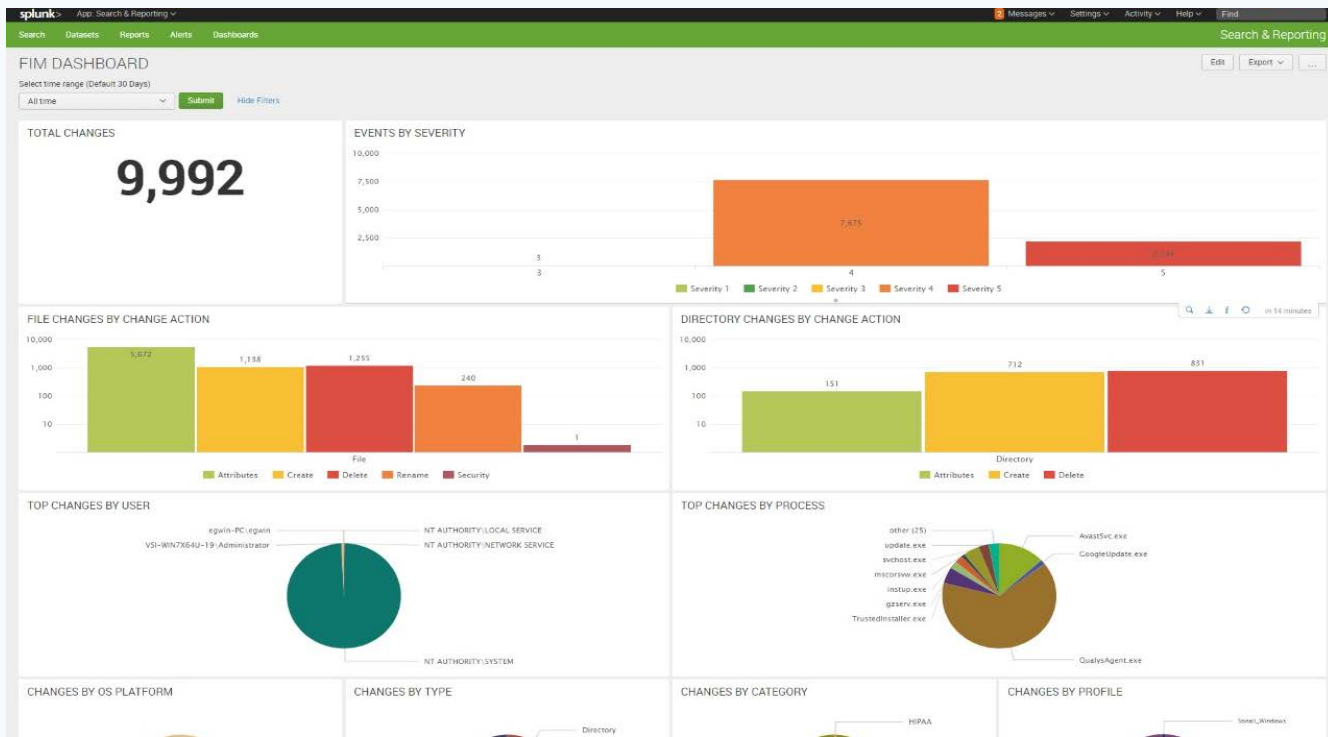
RULE NAME	STATUS	AGGREGATE	ACTION	MATCHES	CREATED BY
Authorized Windows Patching Acti...	Success	Yes	Windows Patch Activity...	1	Aparna Hinge
Authorized Windows Patching Activity	29 minutes ago				
Unauthorized Windows Patching A...	Success	Yes	Windows Patch Activity...	1	Aparna Hinge
Unauthorized Windows Patching Activity	29 minutes ago				
Unauthorized Windows Patching A...	Success	Yes	Windows Patch Activity...	1	Aparna Hinge
This Rule lists down all the events which ...	2 hours ago				

14 Oct 16 Oct 18 Oct 20 Oct 22 Oct 24 Oct 26 Oct 28 Oct 30 Oct 1 Nov 3 Nov 5 Nov 7 Nov 9 Nov 11 Nov 13 Nov 15 Nov

1 - 3 of 3



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)

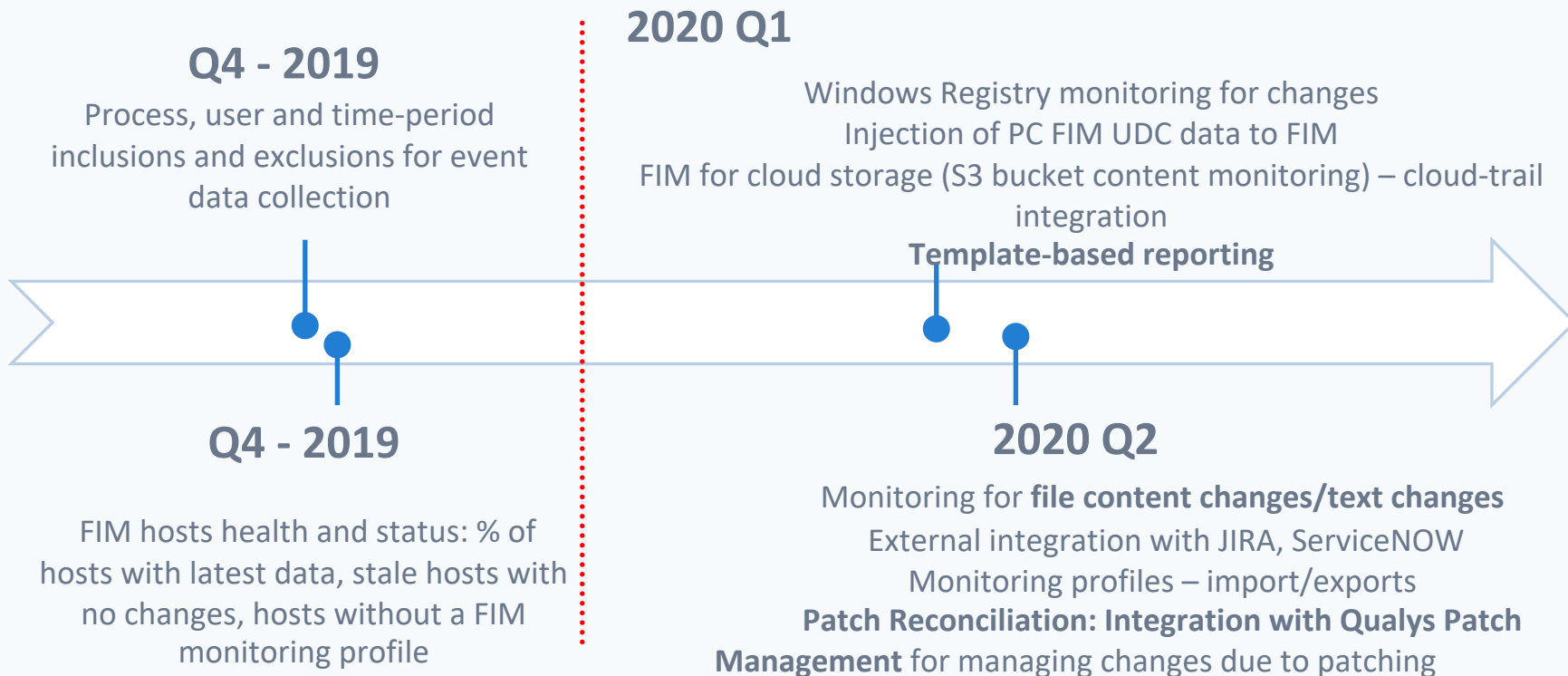
Total Events
5.0K

- 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



Microsoft, Google Make Cloud Offerings More Enticing

eWEEK

Spending On CRM Apps Predicted To Soar In 2018

COMPUTERWORLD



Manage Access, Exposure, Configuration and Compliance of SaaS Applications

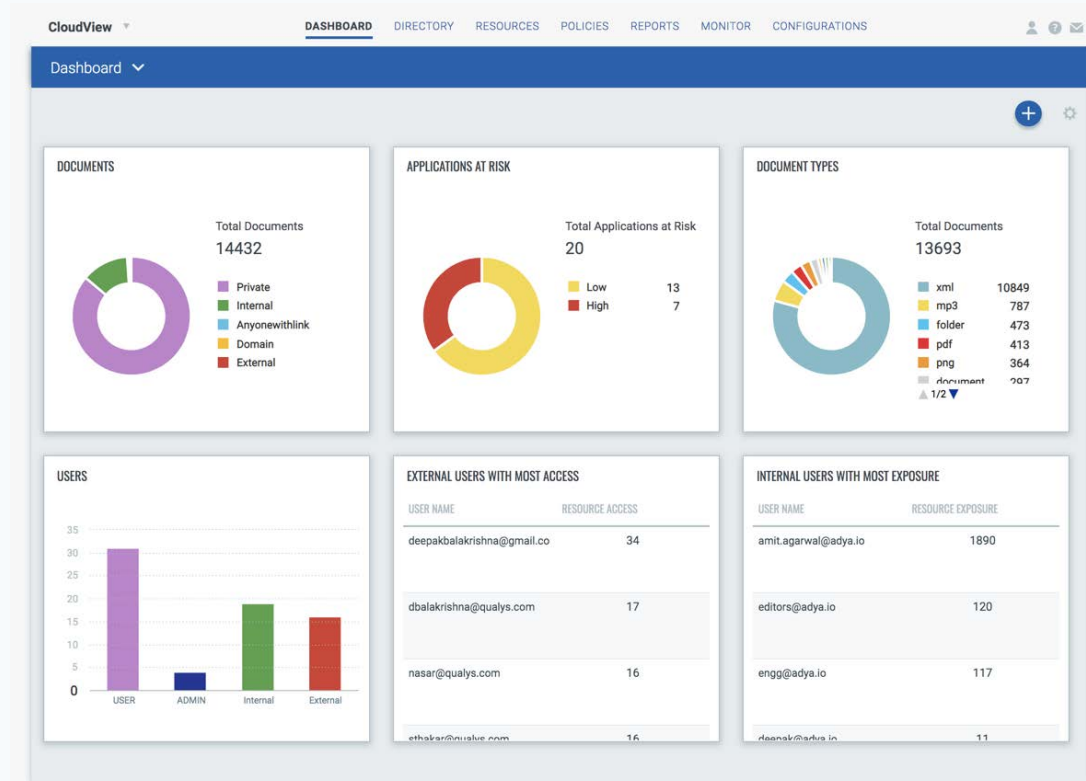
Qualys SaaS Security and Compliance (SSC) enables

Inventory
Access

Exposure

Security Configurations

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

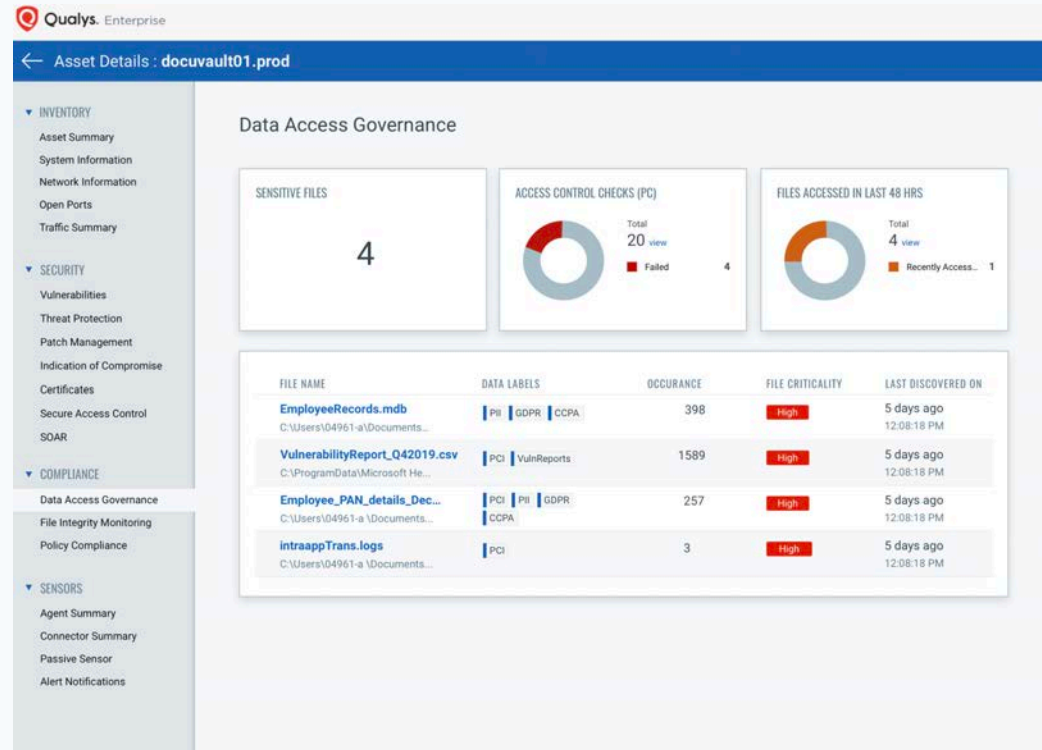


Discover Sensitive data and make sure it is secure and monitored for changes with Qualys DAG

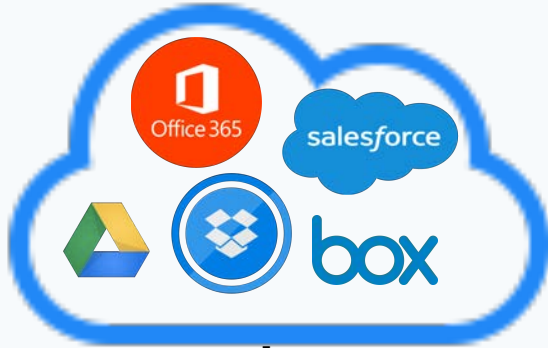
Qualys Data Access Governance (DAG) will help with regulatory compliance

Discovery
Access Visibility
Activity Monitoring

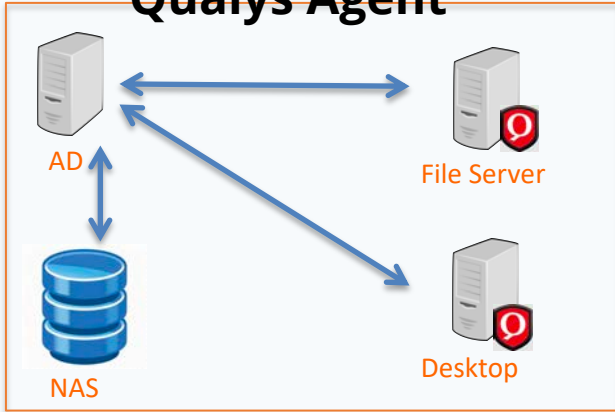
For your sensitive, critical data



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