QSC20

QUALYS SECURITY CONFERENCE 2020

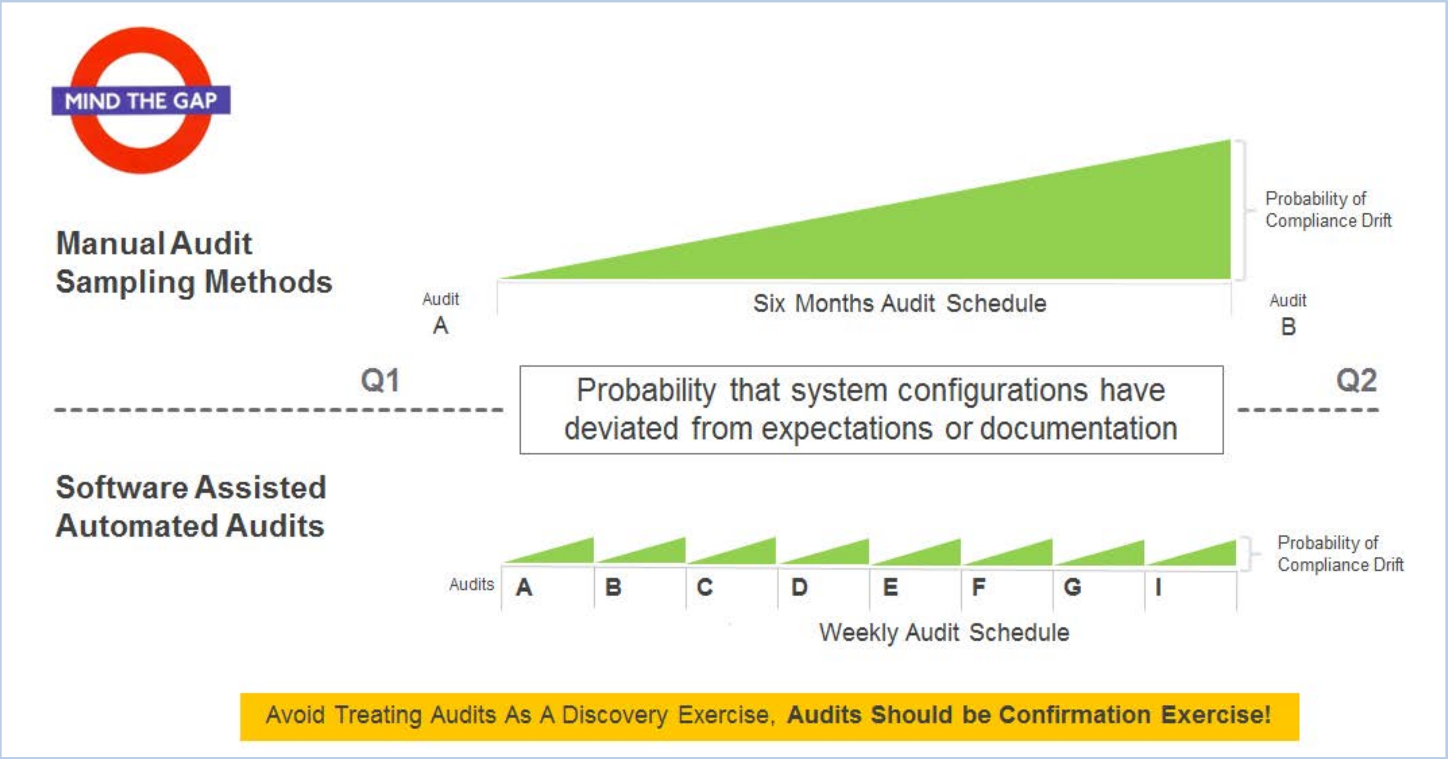
Continuous Compliance in Hybrid Environment

New Frontier in Unified Compliance, Configuration and File Integrity Management

Shailesh Athalye

VP, Compliance Solutions, Qualys, Inc.

2014: Good Old Days of Compliance


MIND THE GAP
Manual Audit Sampling Methods
Audit A
Six Months Audit Schedule
Audit B
Probability of Compliance Drift
Q1
Q2
Software Assisted Automated Audits
Audits
A
B
C
D
E
F
G
I
Weekly Audit Schedule
Probability of Compliance Drift

Probability that system configurations have deviated from expectations or documentation

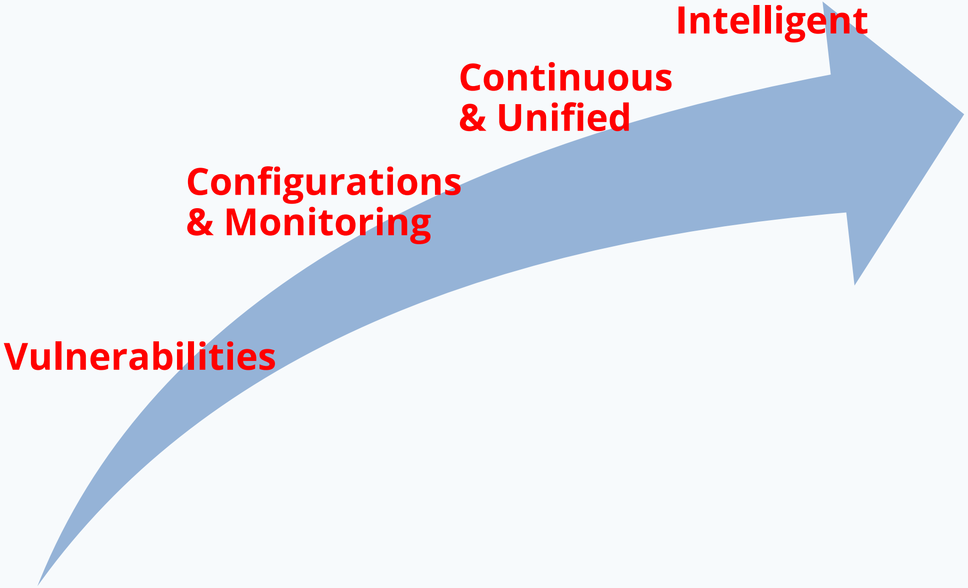
Avoid Treating Audits As A Discovery Exercise, **Audits Should be Confirmation Exercise!**

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

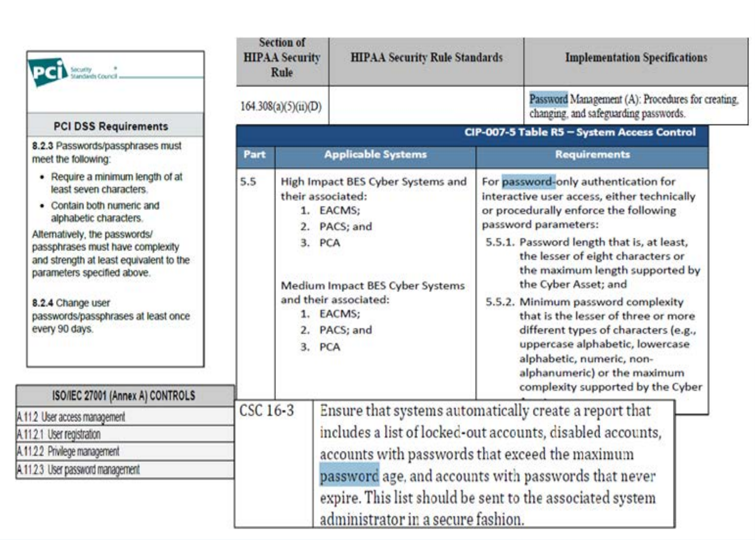
Time to see roll up the operational data

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

Point solutions injecting data with connectors, never normalize

GOVERNANCE
RISK
COMPLIANCE
GRC
Evolution

Connect Security with Compliance and Risk



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

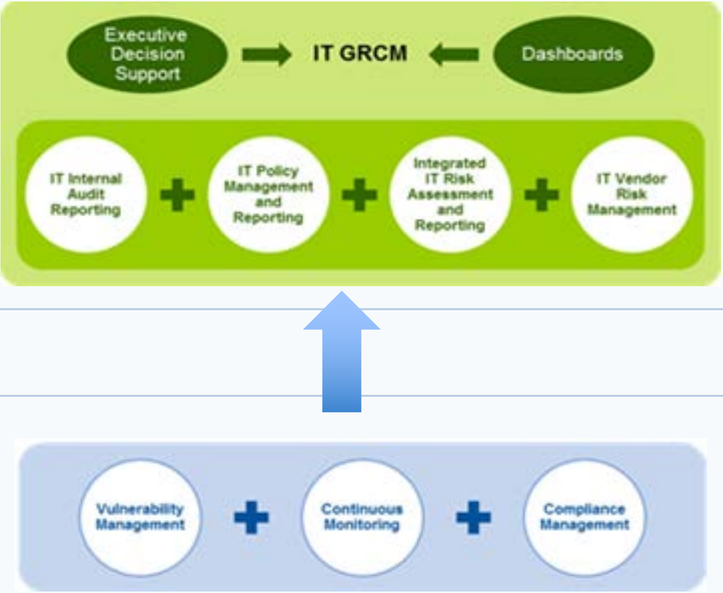
Part	Applicable Systems	Requirements
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally 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	AI SYN
Inventory and Restrict Software	SYN AI VM PC
Secure Configurations and Data Security	PC
Continuous VM	VM CM TP
Review Access Rights	PC

Continuous Compliance & Risk From Continuous Security


Executive Decision Support
IT GRCM
Dashboards
IT Internal Audit Reporting
IT Policy Management and Reporting
Integrated IT Risk Assessment and Reporting
IT Vendor Risk Management
Vulnerability Management
Continuous Monitoring
Compliance Management

Integrated Security Platform

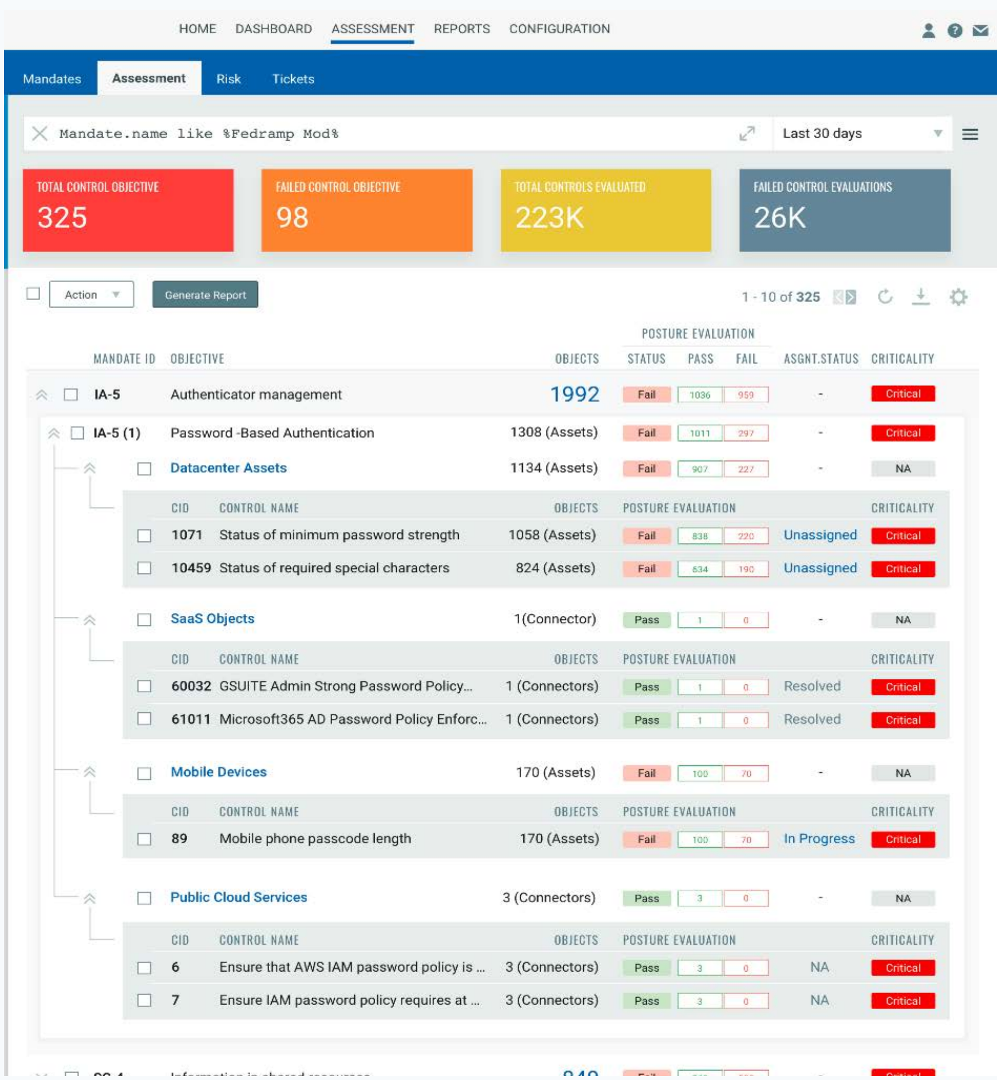
Qualys Unified Compliance & Risk

Map security to compliance

Qualys Platform for unified and continuous security

Continuous Risk and Compliance from Continuous Security

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



Mandate.name like %Fedramp Mod%

Last 30 days

TOTAL CONTROL OBJECTIVE	FAILED CONTROL OBJECTIVE	TOTAL CONTROLS EVALUATED	FAILED CONTROL EVALUATIONS
325	98	223K	26K

1 - 10 of 325

			POSTURE EVALUATION				
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

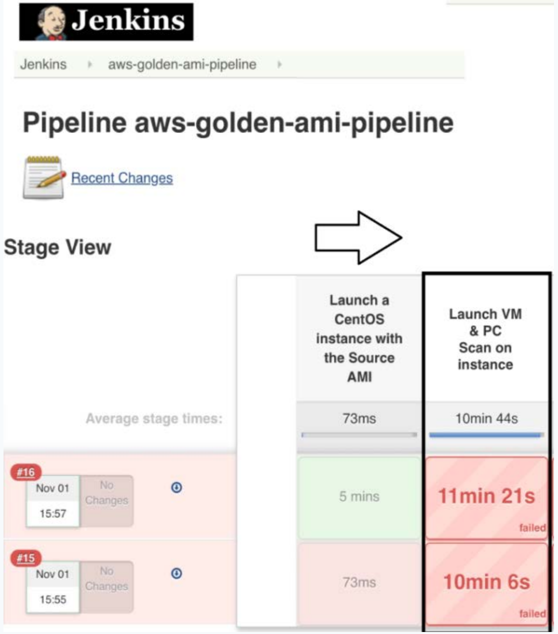
Elastic, Kafka, custom web servers

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



Jenkins

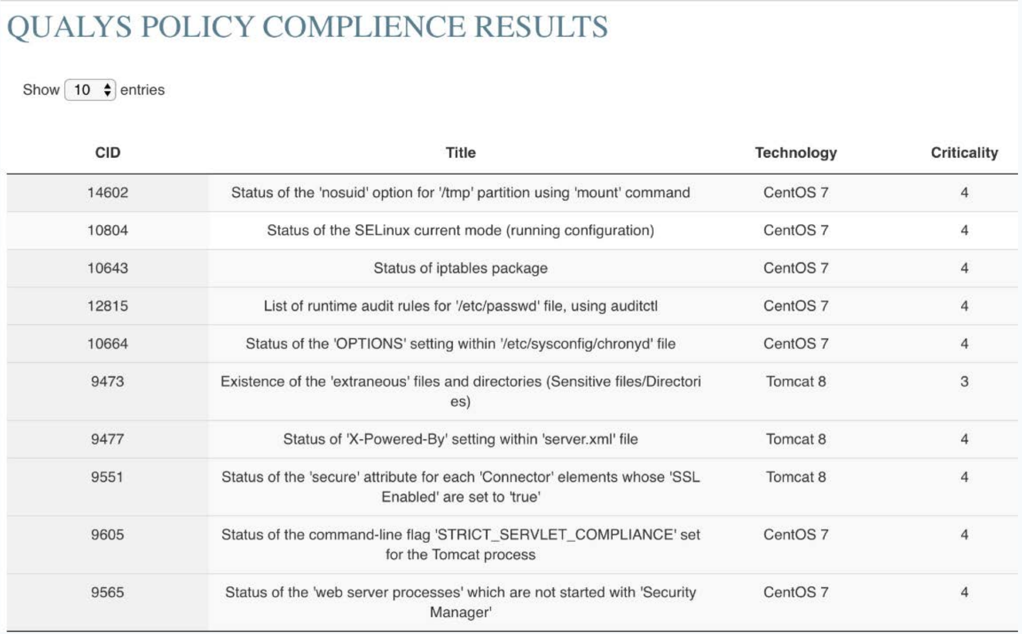
Jenkins › aws-golden-ami-pipeline ›

Pipeline aws-golden-ami-pipeline

Recent Changes

Stage View

	Launch a CentOS instance with the Source AMI	Launch VM & PC Scan on instance
Average stage times:	73ms	10min 44s
#16 Nov 01 15:57 No Changes	5 mins	11min 21s failed
#15 Nov 01 15:55 No Changes	73ms	10min 6s failed

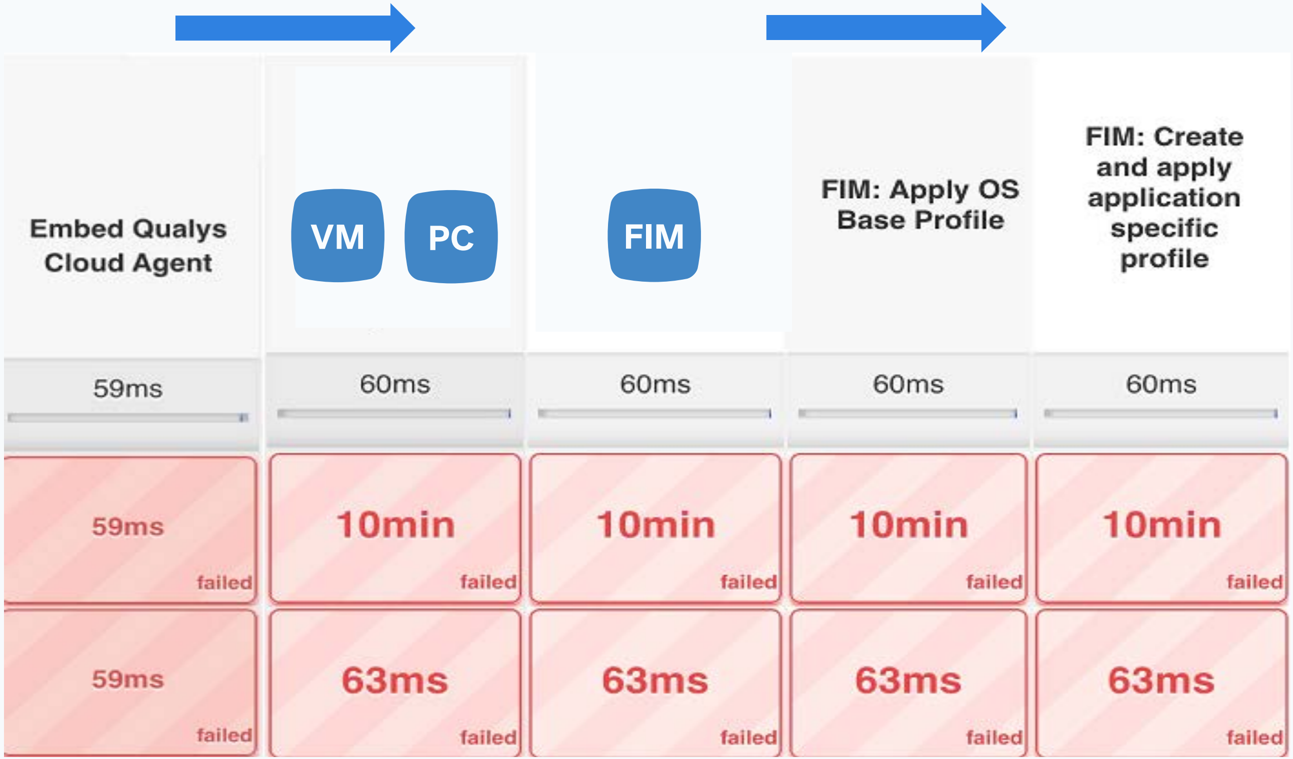


QUALYS POLICY COMPLIENCE RESULTS

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/Directori es)	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

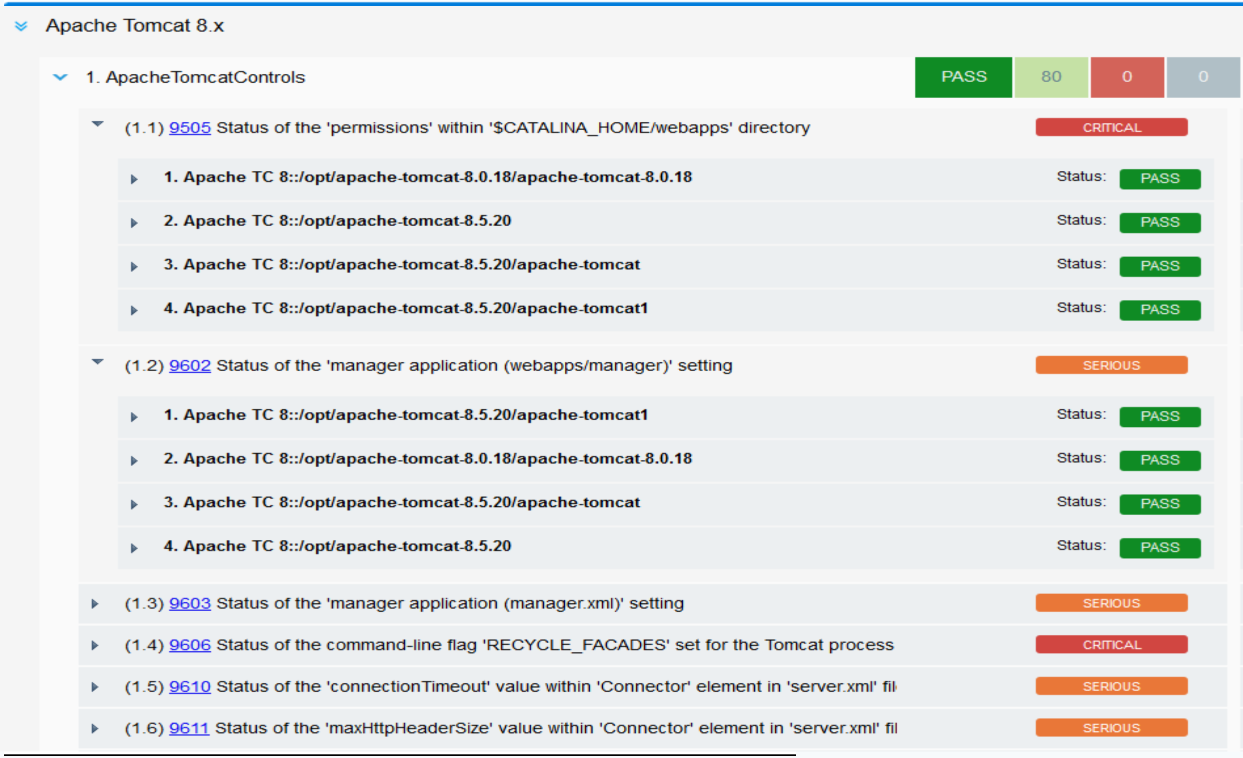


Embed Qualys Cloud Agent	VM PC	FIM	FIM: Apply OS Base Profile	FIM: Create and apply application specific profile
59ms	60ms	60ms	60ms	60ms
59ms failed	10min failed	10min failed	10min failed	10min failed
59ms failed	63ms failed	63ms failed	63ms failed	63ms failed

Automatically Discover and Assess Middleware with Dynamic Paths

Just based on host scans, discover unauthorized technologies,
web servers,
databases <u>automatically</u>

And…
There’s no need to create authentication records



Apache Tomcat 8.x

1. ApacheTomcatControls PASS 80 0 0

(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** 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 SERIOUS

- **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 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' fil SERIOUS

(1.6) 9611 Status of the 'maxHttpHeaderSize' value within 'Connector' element in 'server.xml' fil 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?

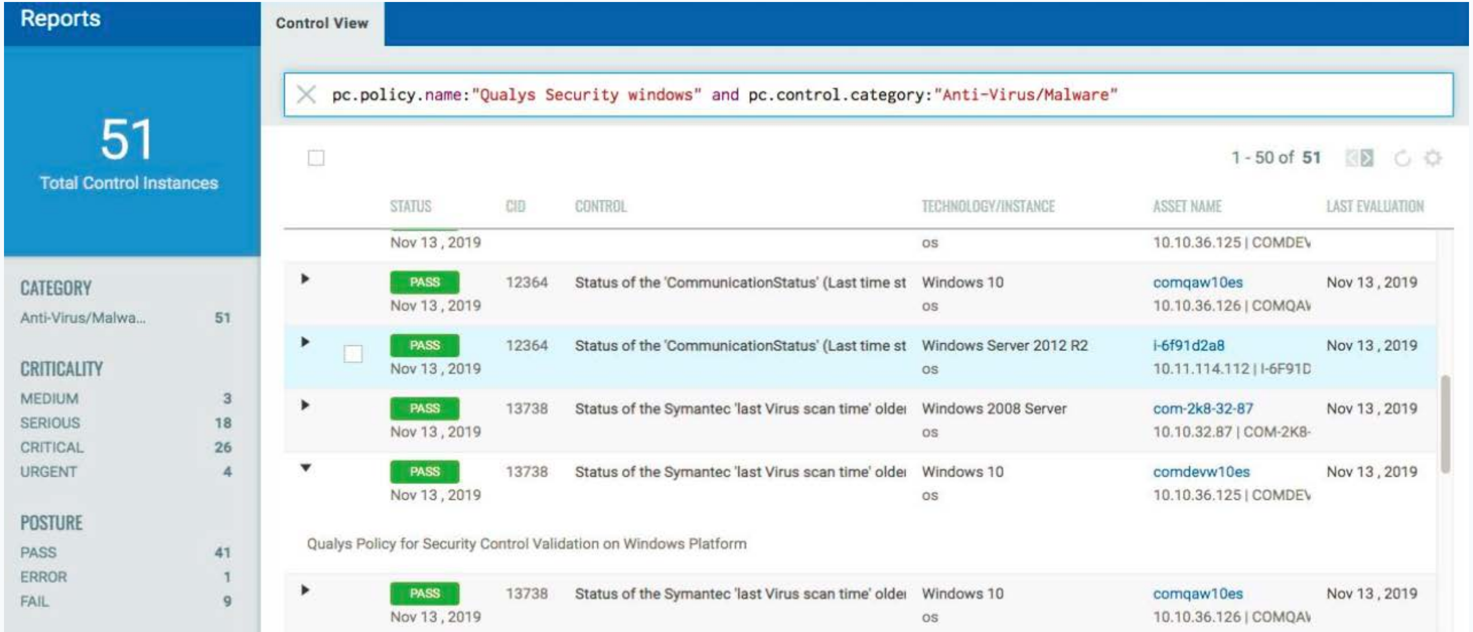
Is FIM, EDR agent configured correctly to monitor?

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



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

51
Total Control Instances

CATEGORY	
Anti-Virus/Malwa...	51

CRITICALITY	
MEDIUM	3
SERIOUS	18
CRITICAL	26
URGENT	4

POSTURE	
PASS	41
ERROR	1
FAIL	9

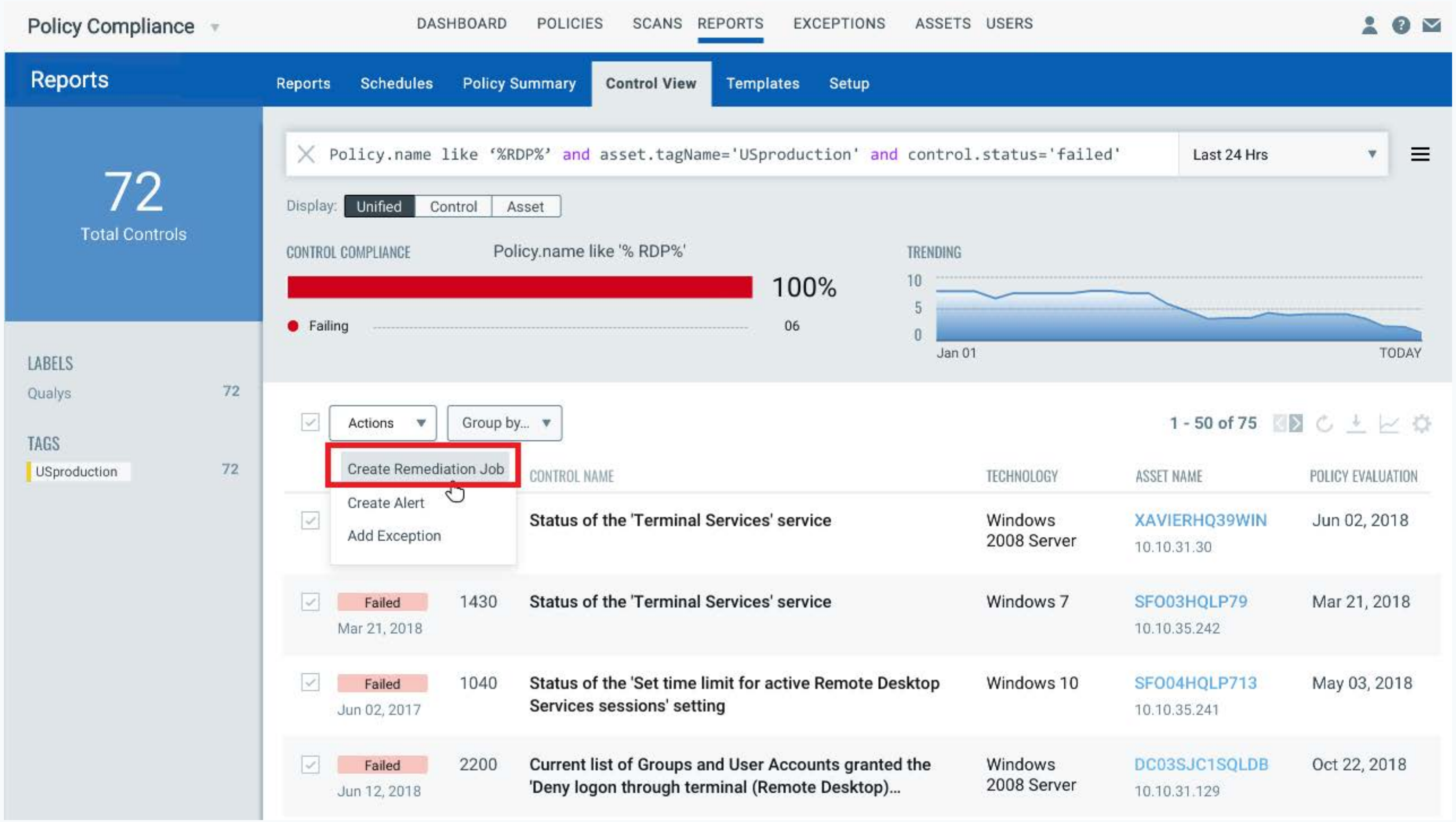
□ 1 - 50 of 51

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 | COMQAV	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' olde	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' olde	Windows 10 os	comdevw10es 10.10.36.125 | COMDEV	Nov 13 , 2019
PASS Nov 13 , 2019	13738	Status of the Symantec 'last Virus scan time' olde	Windows 10 os	comqaw10es 10.10.36.126 | COMQAV	Nov 13 , 2019

Qualys Policy for Security Control Validation on Windows Platform

Qualys.

Start Gold, Continuously Assess, Remediate



```
Policy.name like '%RDP%' and asset.tagName='USproduction' and control.status='failed'
```

Last 24 Hrs

CONTROL COMPLIANCE Policy.name like '% RDP%' 100%

● Failing 06

		CONTROL NAME	TECHNOLOGY	ASSET NAME	POLICY EVALUATION
		Status of the 'Terminal Services' service	Windows 2008 Server	XAVIERHQ39WIN 10.10.31.30	Jun 02, 2018
Failed Mar 21, 2018	1430	Status of the 'Terminal Services' service	Windows 7	SFO03HQLP79 10.10.35.242	Mar 21, 2018
Failed Jun 02, 2017	1040	Status of the 'Set time limit for active Remote Desktop Services sessions' setting	Windows 10	SFO04HQLP713 10.10.35.241	May 03, 2018
Failed Jun 12, 2018	2200	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

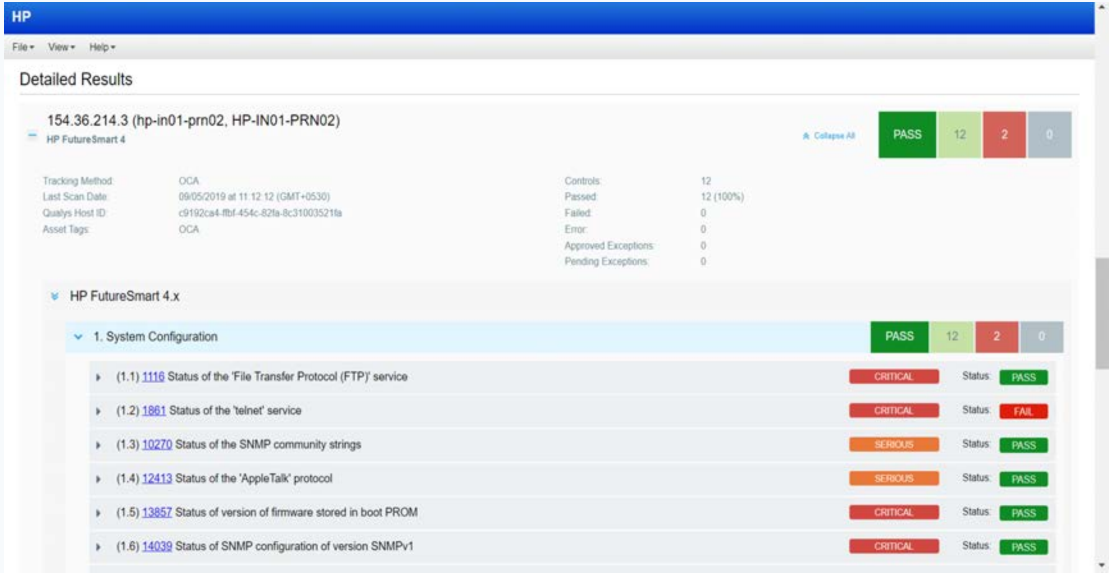
Network Devices, Printers and sensitive hosts can’t be Scanned but are in Security & Compliance Scope

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



Detailed Results

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

PASS 12 2 0

Tracking Method:	OCA	Controls:	12
Last Scan Date:	09/05/2019 at 11:12:12 (GMT+0530)	Passed:	12 (100%)
Qualys Host ID:	c9192ca4-ffbf-454c-82fa-8c31003521fa	Failed:	0
Asset Tags:	OCA	Error:	0
		Approved Exceptions:	0
		Pending Exceptions:	0

HP FutureSmart 4.x

1. System Configuration — PASS 12 2 0

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

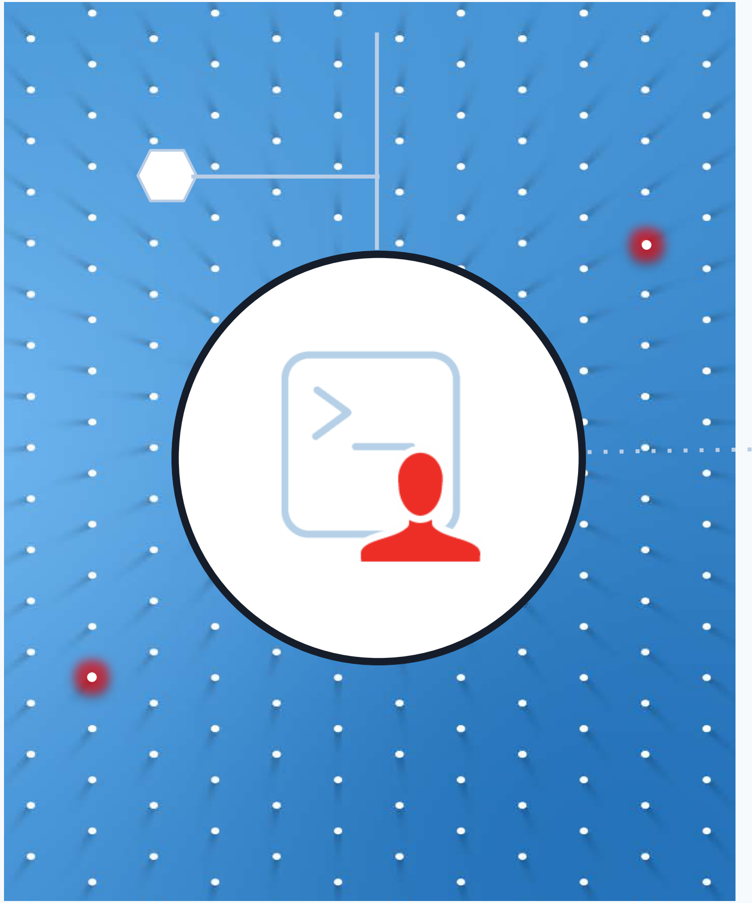
Data collection from all Qualys sensors

Custom database security & integrity controls

Auto-discovery of middleware technologies

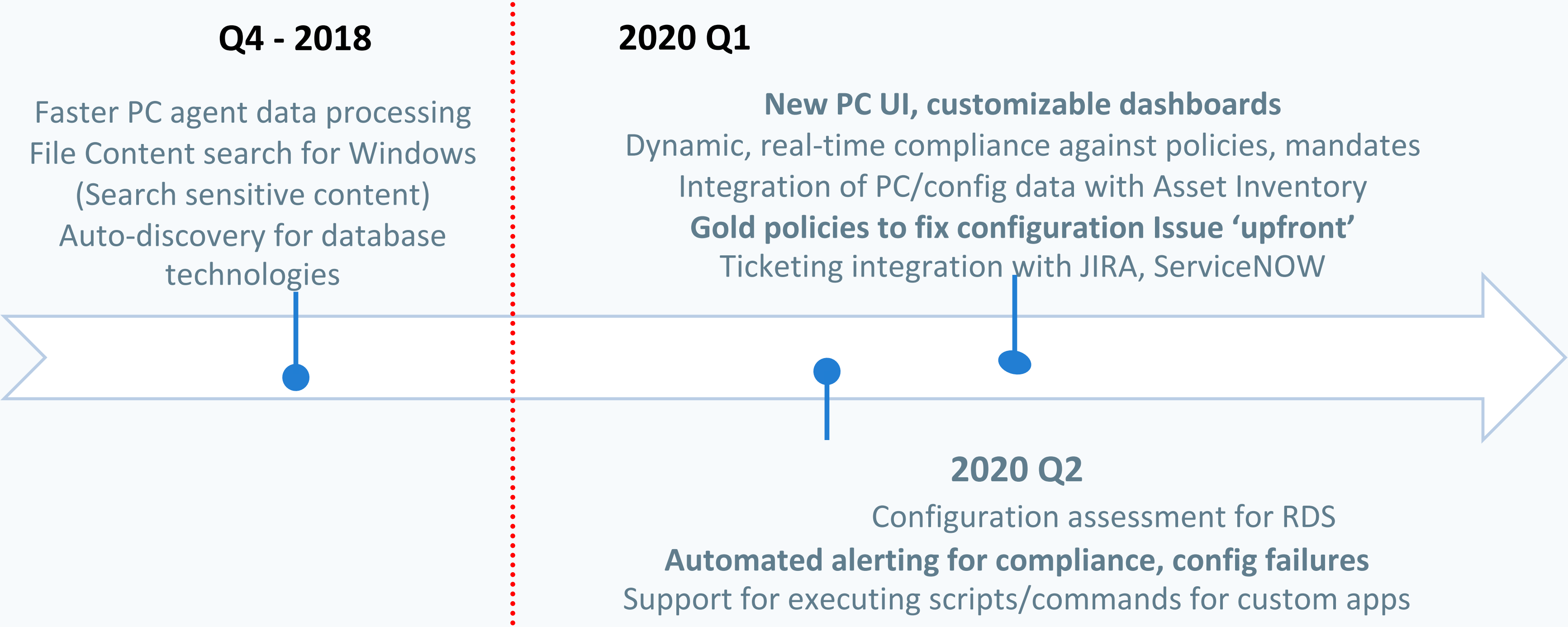
File, Directory Integrity, Network Shares Monitoring

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

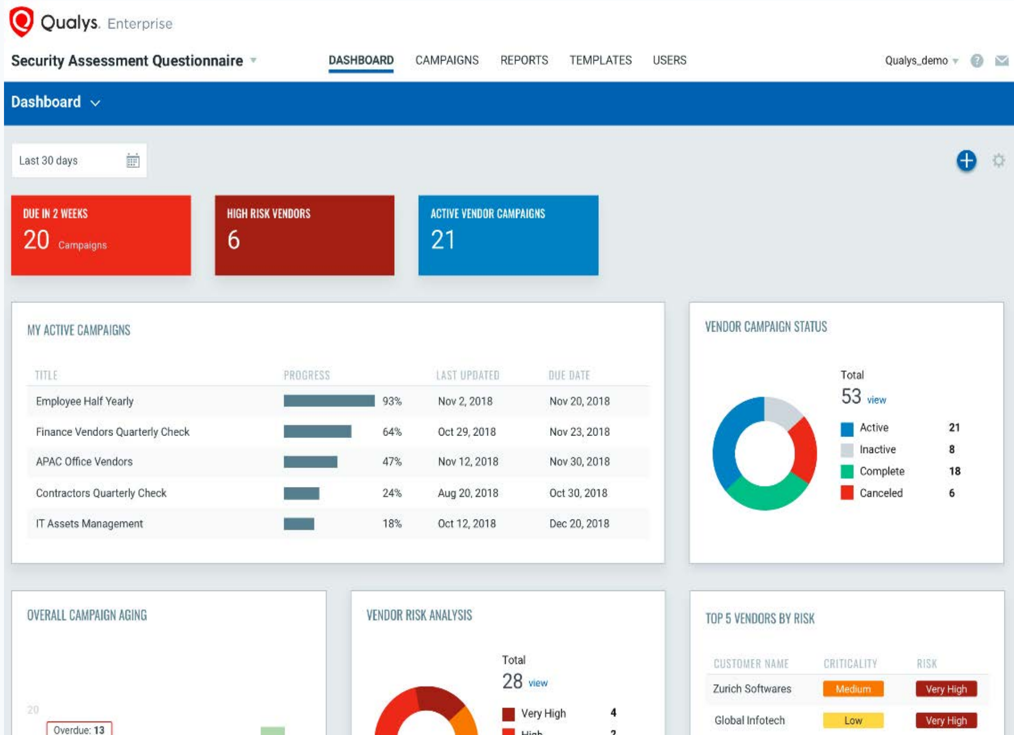
Configuration assessment for RDS
Automated alerting for compliance, config failures
Support for executing scripts/commands for custom apps
PC agent support for web server technologies
Compliance trending

Qualys.

Your security is only as strong as your weakest vendor

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

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



DUE IN 2 WEEKS 20 Campaigns

HIGH RISK VENDORS 6

ACTIVE VENDOR CAMPAIGNS 21

MY ACTIVE CAMPAIGNS

TITLE	PROGRESS	LAST UPDATED	DUE DATE
Employee Half Yearly	93%	Nov 2, 2018	Nov 20, 2018
Finance Vendors Quarterly Check	64%	Oct 29, 2018	Nov 23, 2018
APAC Office Vendors	47%	Nov 12, 2018	Nov 30, 2018
Contractors Quarterly Check	24%	Aug 20, 2018	Oct 30, 2018
IT Assets Management	18%	Oct 12, 2018	Dec 20, 2018

VENDOR CAMPAIGN STATUS

Total 53 view

🟦 Active	21
⬜ Inactive	8
🟩 Complete	18
🟥 Canceled	6

OVERALL CAMPAIGN AGING

VENDOR RISK ANALYSIS

Total 28 view

🟥 Very High	4
🟥 High	2

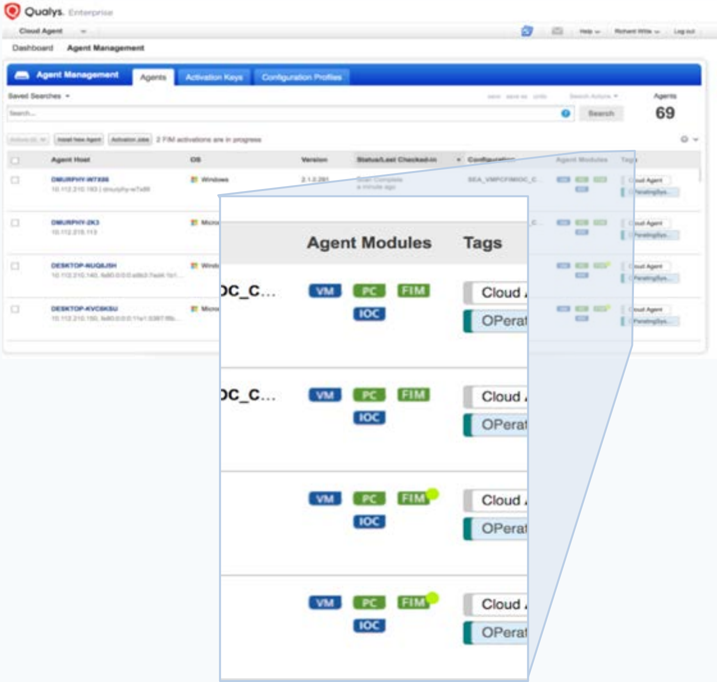
TOP 5 VENDORS BY RISK

CUSTOMER NAME	CRITICALITY	RISK
Zurich Softwares	Medium	Very High
Global Infotech	Low	Very High

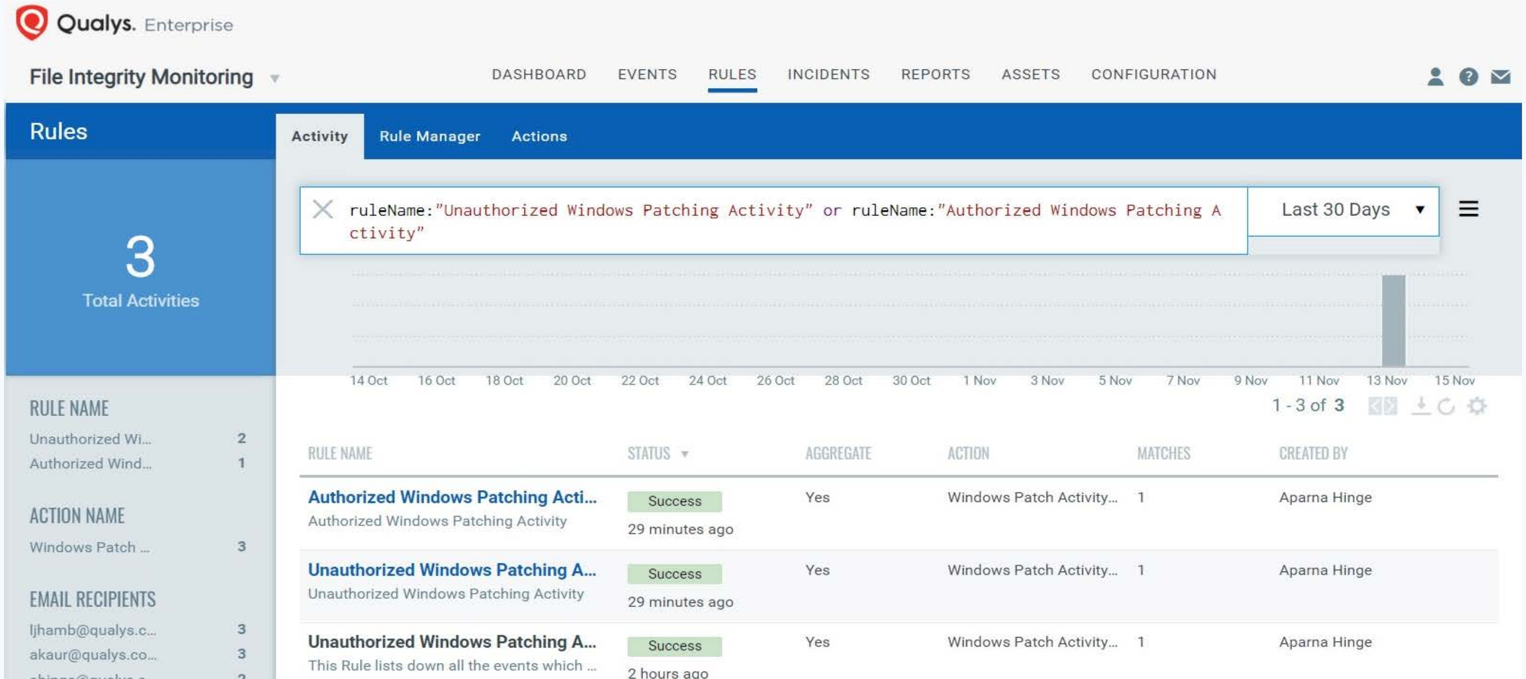
File Integrity Monitoring (FIM)

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



```
ruleName:"Unauthorized Windows Patching Activity" or ruleName:"Authorized Windows Patching A
ctivity"
```

3
Total Activities

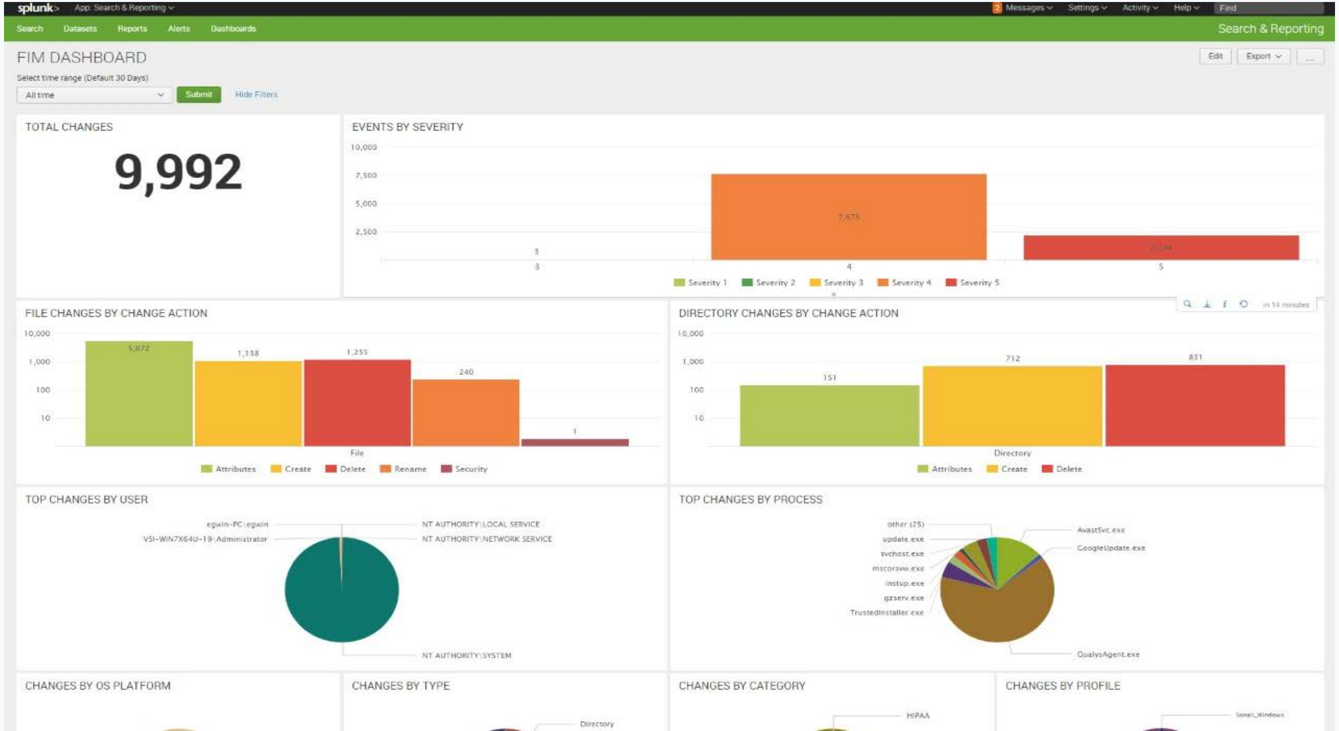
RULE NAME	
Unauthorized Wi...	2
Authorized Wind...	1

ACTION NAME	
Windows Patch ...	3

EMAIL RECIPIENTS	
ljhamb@qualys.c...	3
akaur@qualys.co...	3

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

Open APIs: Integrate with Any External SIEM, DWH



FIM DASHBOARD

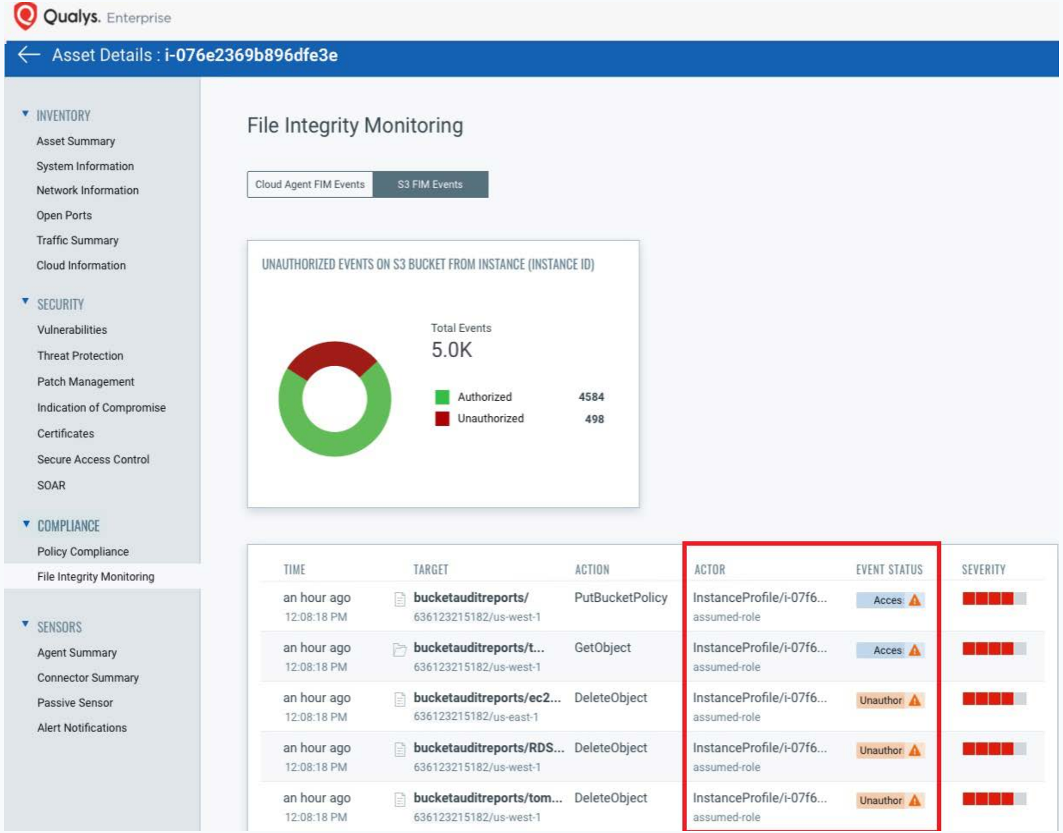
Select time range (Default 30 Days)

All time

TOTAL CHANGES

9,992

Qualys FIM gives context of changes in cloud



Asset Details : **i-076e2369b896dfe3e**

File Integrity Monitoring

UNAUTHORIZED EVENTS ON S3 BUCKET FROM INSTANCE (INSTANCE ID)

Total Events

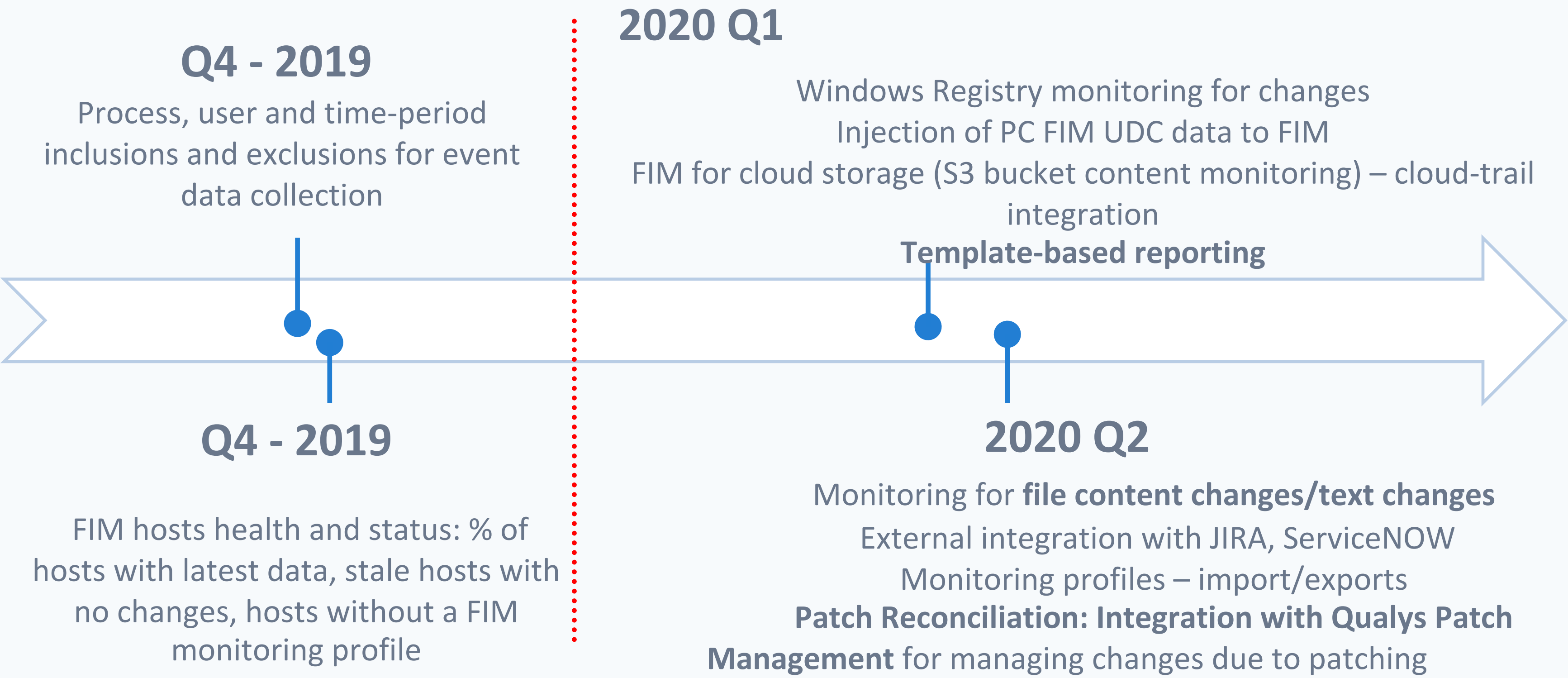
5.0K

🟩	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	Acces ⚠	■■■■□
an hour ago 12:08:18 PM	**bucketauditreports/t...** 636123215182/us-west-1	GetObject	InstanceProfile/i-07f6... assumed-role	Acces ⚠	■■■■□
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



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
Injection of PC FIM UDC data to FIM
FIM for cloud storage (S3 bucket content monitoring) – cloud-trail integration
Template-based reporting

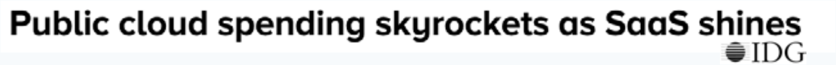
2020 Q2

Monitoring for **file content changes/text changes**
External integration with JIRA, ServiceNOW
Monitoring profiles – import/exports
Patch Reconciliation: Integration with Qualys Patch Management for managing changes due to patching

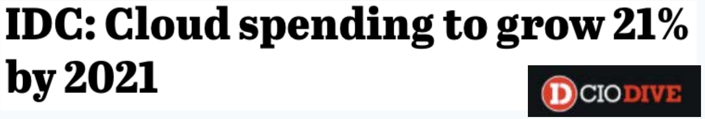
Qualys.

Software as a Service (SaaS) Security & Compliance

Even Cloud is bloated; Need just SaaS Applications

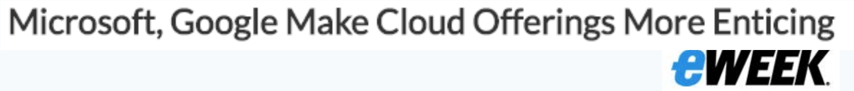

Public cloud spending skyrockets as SaaS shines

IDG

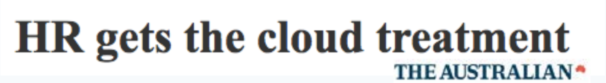

IDC: Cloud spending to grow 21% by 2021

CIO DIVE

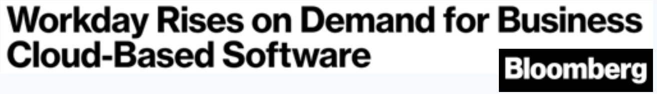
Office 365 box


Microsoft, Google Make Cloud Offerings More Enticing

eWEEK

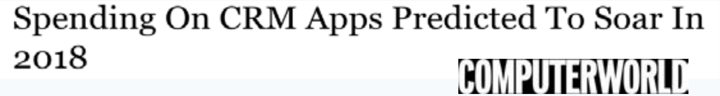

HR gets the cloud treatment

THE AUSTRALIAN


Workday Rises on Demand for Business Cloud-Based Software

Bloomberg

workday. Namely


Spending On CRM Apps Predicted To Soar In 2018

COMPUTERWORLD

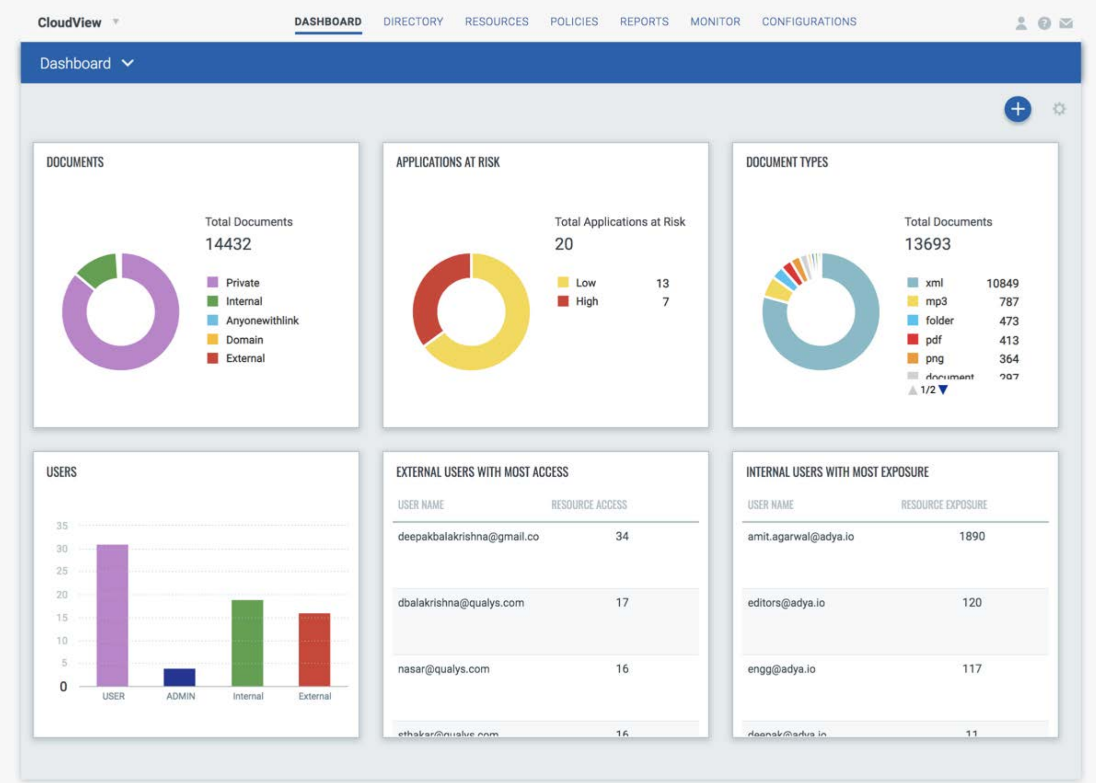
salesforce ZOHO

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



EXTERNAL USERS WITH MOST ACCESS

USER NAME	RESOURCE ACCESS
deepakbalakrishna@gmail.co	34
dbalakrishna@qualys.com	17
nasar@qualys.com	16
sthakar@qualys.com	16

INTERNAL USERS WITH MOST EXPOSURE

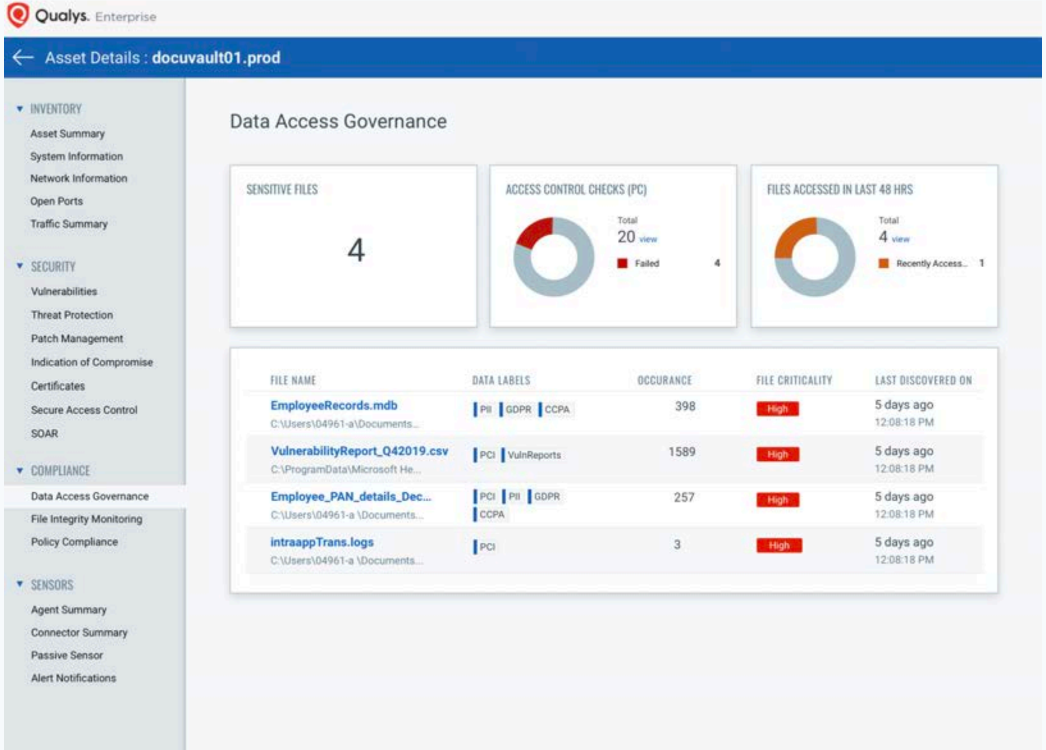
USER NAME	RESOURCE EXPOSURE
amit.agarwal@adya.io	1890
editors@adya.io	120
engg@adya.io	117
deepak@adya.io	11

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



Asset Details : **docuvault01.prod**

Data Access Governance

SENSITIVE FILES: 4

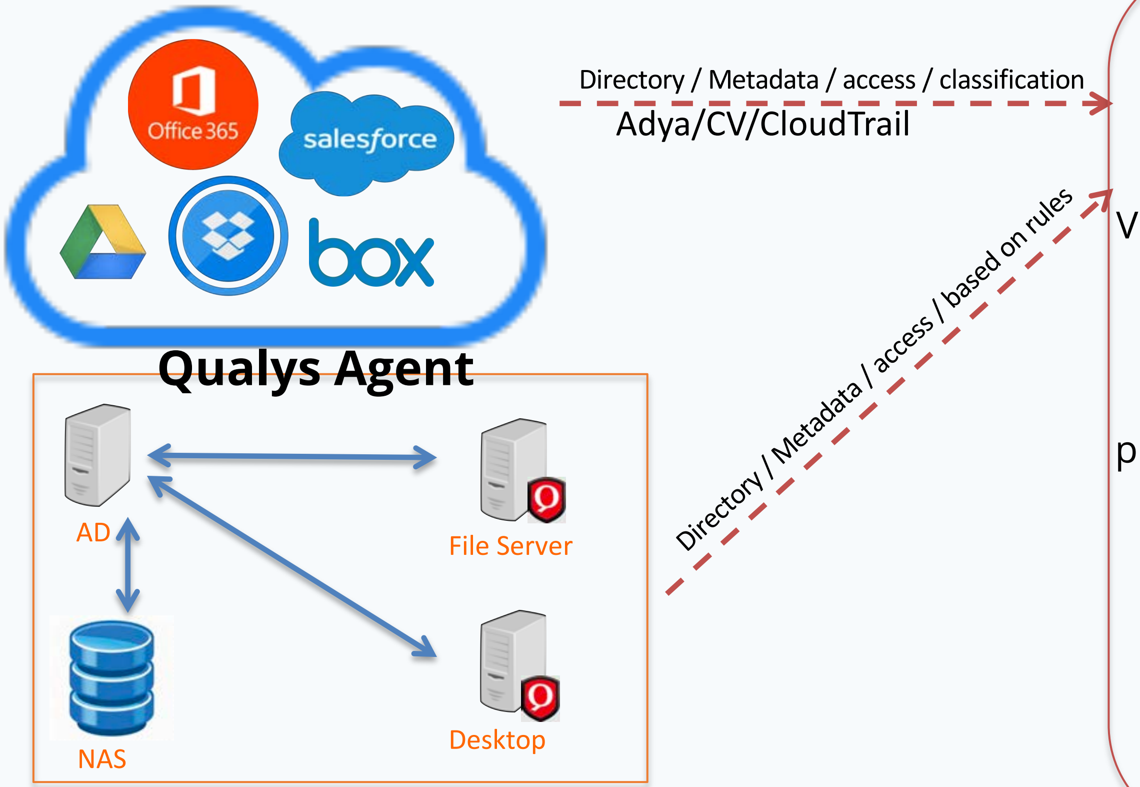
ACCESS CONTROL CHECKS (PC): Total 20 view; 🟥 Failed 4

FILES ACCESSED IN LAST 48 HRS: Total 4 view; 🟧 Recently Access... 1

FILE NAME	DATA LABELS	OCCURANCE	FILE CRITICALITY	LAST DISCOVERED ON
EmployeeRecords.mdb C:\Users\04961-a\Documents...	PII GDPR CCPA	398	High	5 days ago 12:08:18 PM
VulnerabilityReport_Q42019.csv C:\ProgramData\Microsoft He...	PCI VulnReports	1589	High	5 days ago 12:08:18 PM
Employee_PAN_details_Dec... C:\Users\04961-a \Documents...	PCI PII GDPR CCPA	257	High	5 days ago 12:08:18 PM
intraappTrans.logs C:\Users\04961-a \Documents...	PCI	3	High	5 days ago 12:08:18 PM

Cloud Applications

Qualys Cloud Platform


Office 365
salesforce
box
Directory / Metadata / access / classification
Adya/CV/CloudTrail
Qualys Agent
AD
File Server
NAS
Desktop
Directory / Metadata / access / based on rules

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

On Premise Unstructured Data

Thank You

Compliance Team and Shailesh Athalye
sathalye@qualys.com