



Better managed Qualys subscription = Better Cyber Risk program:

# Get More Out of Your Qualys Subscription



**Himanshu Kathpal**

Senior Director, Product Management  
Qualys Platform & Sensors



---

# Enterprise TruRisk™ Platform

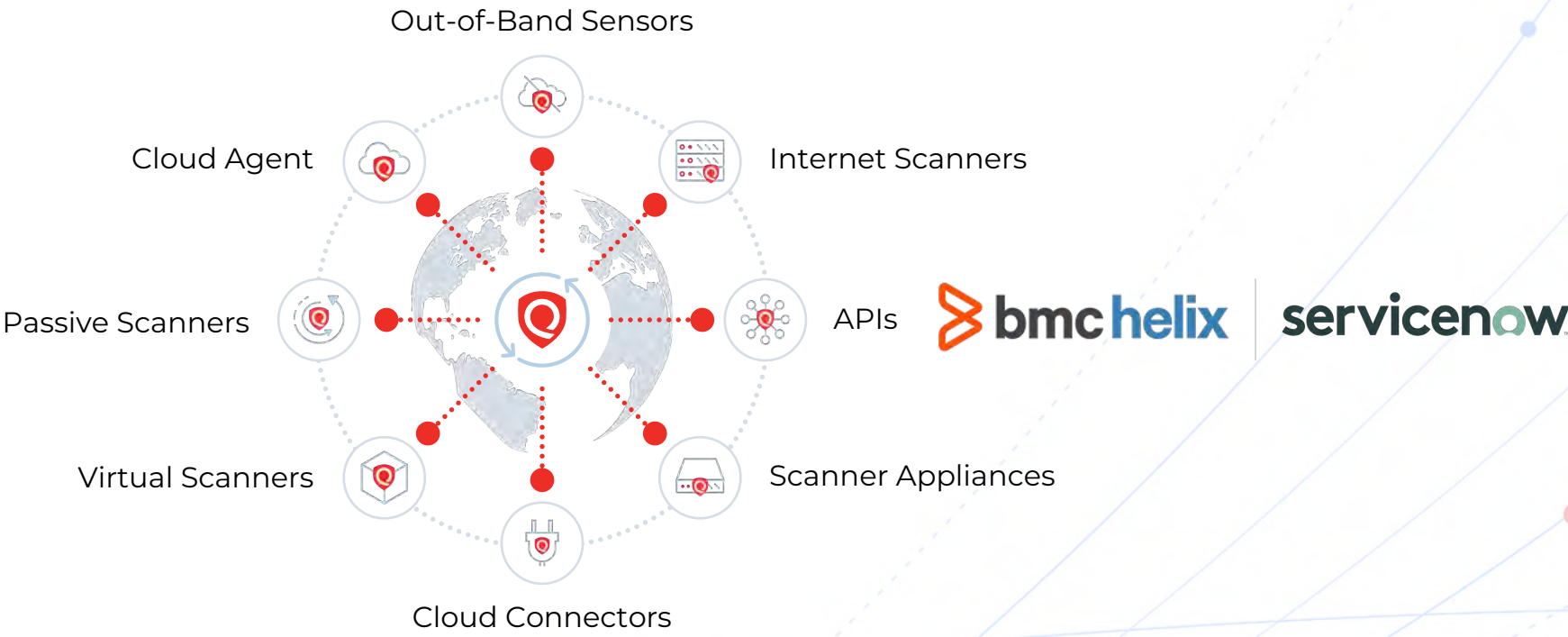
Measure, communicate, and eliminate cyber risk.

---

**De-risk your business.**

# Qualys Enterprise TruRisk™ Platform

Helps to Effectively Measure Asset Inventory Risk



**100% Visibility via versatile sensors for a complete, accurate landscape**

# Qualys Enterprise TruRisk™ Platform

Helps to Effectively Measure Risk



### Optimize Asset Management

Organize and Tag assets with a comprehensive tagging strategy, Leverage Asset criticality for business context

**Create New Tag**

Name: OSC Demo

Mark as Favorite

Description: Add a brief description for this rule

**Asset Criticality Score**

This score represents the criticality of that asset to your business infrastructure.

Here, score 1 being the lowest criticality and 3 being the highest criticality assigned to an asset, when selected.

**Asset Merging**

The Manager primary contact can choose from the following options for identifying assets by a unique Qualys asset UUID and/or Agent correlation ID and merging the data based on the unique asset UUID and/or Agent correlation ID.

We provide several options for merging results from agent scans and IP scans. This merging will only apply when you have authorized scans with agentless tracking identifier enabled and/or unauthenticated/authenticated scans with Agent correlation identifier enabled.

Do not merge data  
Select this option if you do NOT want to merge scan results for cloud agents or IP scans. Each agent and scanned IP interface of an asset would result in a separate asset record.

Merge data by scan method  
All scanned interfaces of an asset will be merged into a single asset record (tracked by IP). Results of network scans and agentless scans will NOT be merged; you will get a separate asset record (tracked by agent UUID) from this cloud agent scan results.

Merge data for a single unified view  
You'll get a single asset record with results from cloud agent scans and results from all scanned IP interfaces merged for a single unified view of the asset. Assets with a cloud agent will be tracked by agent UUID and assets without a cloud agent will be tracked by IP.

Enable smart merging  
We'll automatically detect whether a cloud agent is installed and merge results into a single unified view of the asset only when an agent is found. Assets with a cloud agent will be tracked by agent UUID and all the interfaces of an asset without a cloud agent.

### Accurate Threat Landscape

- Asset Merge for unified view
- Asset Purge to focus on live risk

**Asset Scope**

Add criteria to select assets you want to add to the purge scope. [Learn More](#)

**Criteria: Cloud Agent-Based Assets**

Assets that match all the following conditions:

lastActivity OLDER THAN 30

**Criteria: Cloud Provider Metadata-Based Assets**

When the cloud provider is AWS

Assets that match all the following conditions:

aws.ec2.instanceState Select the Operator TERMINATED

Remove the cloud agent and associated license.  
Assets, a cloud agent, and its license will be removed from your subscription.

Precise Evaluation and Insights for prioritizing up to 85% fewer vulnerabilities

# Qualys Enterprise TruRisk™ Platform

Helps to Effectively Measure Risk



**Scan Strategies**  
Optimal assessment strategies (Combination of Agent, Auth, Un-auth Scans & API Based) regardless of asset type

**Know Tech-Debt and Shift Left**  
Proactively monitor versions, know EOL/EOS, Shift left by streamlining development to deployment processes with integrations

**Run Scan**

**Scan Type**

Inventory Scan

Note: Scan would be launched only on the modules that are activated for the agent.

Use CPU Throttle limits set in the respective Configuration Profile for the agents. By default, Windows Agent uses the CPU throttle value of 80 and Linux Agent uses the value 0 (no throttling).



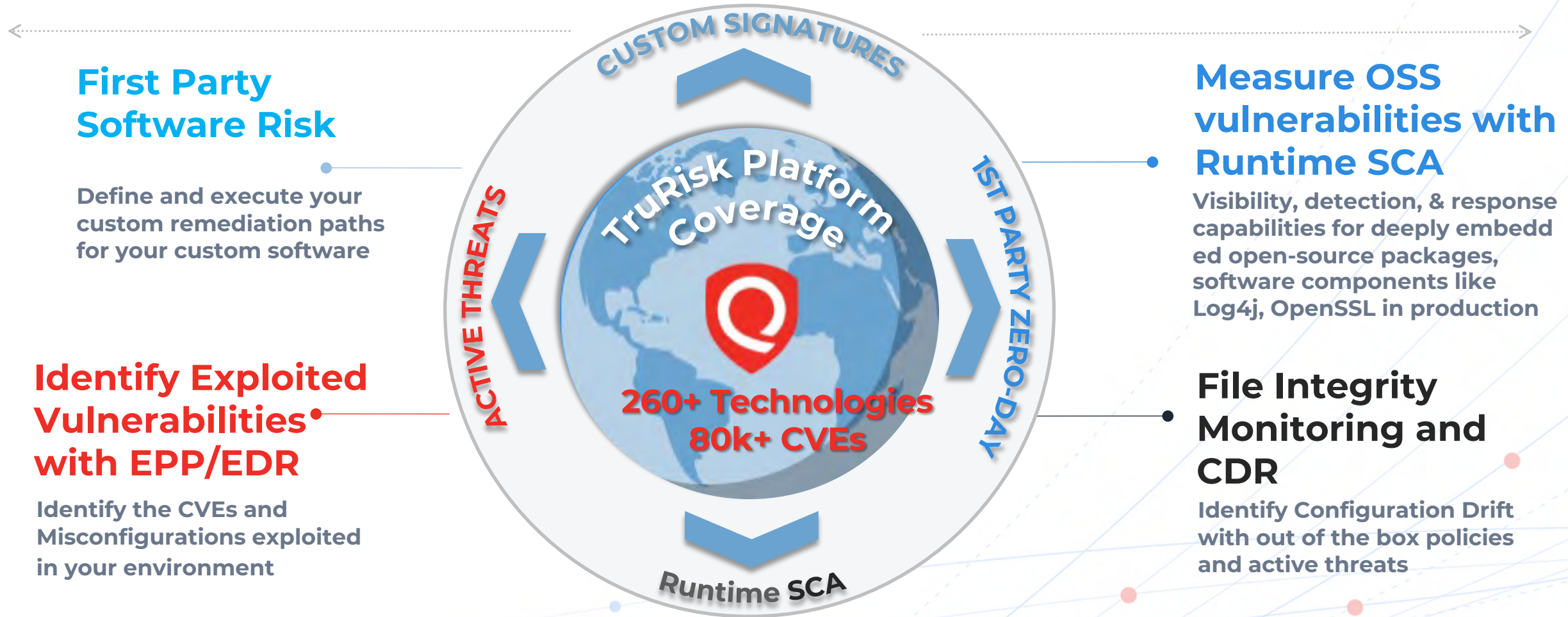
Visual Studio Code

Azure DevOps

Scans	
Title	Status
<input type="checkbox"/> CertView - External - WAS - Sites	Green
<input type="checkbox"/> Azure-US-AuthScan	Green
<input type="checkbox"/> AWS-EC2-UE1.2 Perimeter Scan	Green
<input type="checkbox"/> AWS-EC2-AS1 Perimeter Scan	Green

Precise Evaluation and Insights for prioritizing up to 85% fewer vulnerabilities

# Qualys Enterprise TruRisk™ Platform Helps to Effectively Measure Risk



**Extend your Measurement of Risk Assessment**

# Qualys Enterprise TruRisk™ Platform

Helps to Communicate Risk Better

Accurate, customized reporting to “C” Level and Auditors

- ✓ Key Risk Indicators (TruRisk, high-risk assets, MTTR.)
- ✓ Mandate and MITRE based reports
- ✓ Same UI and Microservice

Useful widgets for Persona-wise widgets

Prioritize based on

- ✓ Risk
- ✓ Age
- ✓ RTIs

Disk Space, Pending Reboot , Tech Debt, Missing Critical Software

Qualys Provided Dashboards

<https://success.qualys.com/support/s/article/000005975>



TAGS	COUNT ↓	RISK SCORE ⓘ
Servers	8010	566
Tagged	5831	567
Linux	5140	521
Desktops	3315	357
SAP	2590	525
Syntax_Internal	1462	354
EBS	1459	674
Internet Facing Assets	1328	291
AWS	1264	529

### Qualys Detection Score Breakdown

CVE-2021-36942 ..... 95

Attributes contributing to the CVSS score -

Technical Attributes	Temporal Attributes
CVSS Score: 5.3	Exploit Code Maturity (ECM): poc,weaponized
CISA known exploitable: Yes	Malware: Babuk,LockFile

Prioritized Vulnerabilities

Instances of 807K	Unique
87.2K	2.12K

# Qualys Enterprise TruRisk™ Platform

Helps to Communicate Risk Better

## Alerting and Continuous Monitoring

- ✓ Unknown and Unprotected Assets and Ports
- ✓ Customizable rule-engine to detect, alert for absence of AV, presence of risky software
- ✓ Exploitable Vulnerabilities on Internet Facing Assets
- ✓ Malware events and Suspicious Activity

## Ecosystem Integrations

- ✓ Provides immediate threat detection and monitoring
- ✓ Supports reporting and response management

The screenshot displays the configuration for a rule named "Rule for Unmanaged Assets". The rule is triggered 8 hours ago and has a status of "Success". Below the rule configuration, there are two tabs: "Response Action" and "Impacted Assets". The "Response Action" tab is active, showing an email alert configuration for "Alert for Unmanaged Assets" sent to "rbali@qualys.com". The "Impacted Assets" tab is also visible. To the right, there is a preview of an "IT-Sec Alerts" email, which includes a description, action settings, and a message body.

The screenshot shows an email alert titled "Alert: Unmanaged Assets Identified by CAPS". The email is from "noreply@qualys.net" to "Richima Bali". The body of the email states: "CAPS has identified unmanaged assets. Unmanaged assets can pose significant risk to an organization's security, compliance and overall operations". At the bottom, it provides a URL for the Qualys Platform and identifies the rule owner as "Richima Bali".



VMware Tanzu



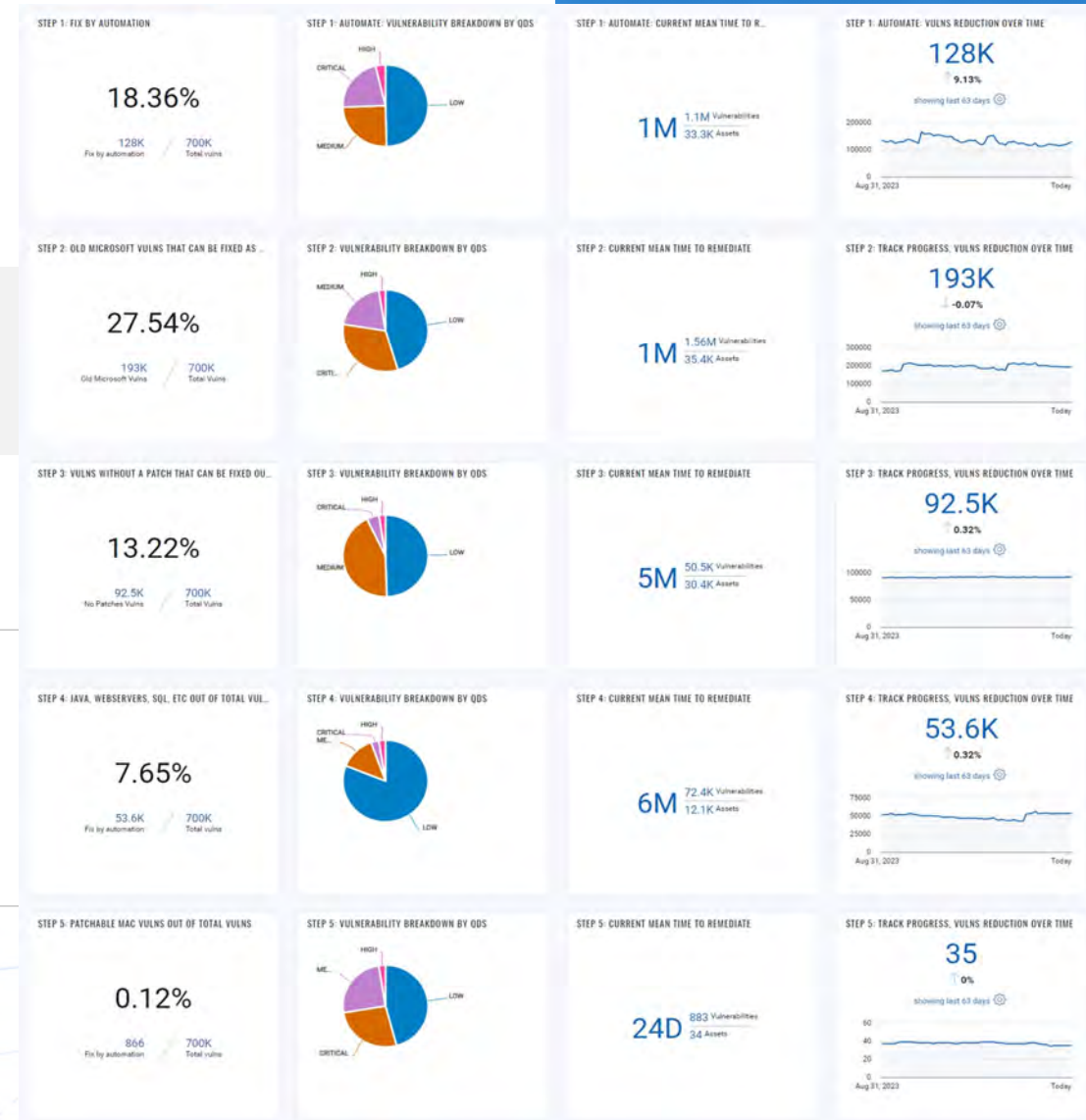


# Qualys Enterprise TruRisk™ Platform

Helps to Eliminate Risk Faster!

Unified Workflows for Patching across the environment

- ✔ Shorten Patching efforts from days to hours
- ✔ Zero-touch patching based on – risk priorities, Patch Tuesday, thresholds, **89.5%** Improvement in Patching Rates, **43.1%** Improvement in MTTR Speed
- ✔ Smarter remediation based on the risk profiles.



# Qualys Enterprise TruRisk™ Platform

Helps to Eliminate Risk Faster!

## Auto-Response based on Risk threshold

- ✓ Automate installation of missing software, Uninstallation of unauthorised software OR EOL/EOS Software
- ✓ Automate Security/Operational challenges
- ✓ Out of the box automation options to define your risk thresholds and response like Isolate host based on vulnerabilities, Automatically kill the process when a malicious hash is detected



The screenshot displays the Qualys Enterprise TruRisk Platform interface. At the top, a blue header shows '215 Total Scripts'. Below this is a table with columns for 'CATEGORY', 'TITLE', 'TYPE', and 'LAST UPDATED'. The table lists several scripts, including 'Users with o...', 'Unlinked dis...', 'Reversible p...', 'Recent defa...', and 'Netlogon se...'. A configuration window titled 'Add Software To Authorization Rule' is overlaid on the interface, showing options for 'Visual C++ 2008 Redistributable' and 'Authorization' settings. The window also includes a table with columns for 'ORDER NUMBER', 'RULE', 'STATUS', and 'TAGS', listing rules like 'Database Servers', 'Web Server', and 'Data Center Server'.

CATEGORY	TITLE	TYPE	LAST UPDATED
QID without Patch	55		
AD Security Post...	42		
Post Patch	30		
Application Secu...	14		
User Account Se...	14		
17 more			

TITLE	TYPE	LAST UPDATED	AD Security Posture	WINDOWS
Users with o... Version 1	Custom Script Detection	Nov 7, 2023 02:00 PM		PowerShell-Script
Unlinked dis... Version 1	Custom Script Detection	Nov 7, 2023 02:00 PM		PowerShell-Script
Reversible p... Version 1	Custom Script Detection	Nov 7, 2023 02:00 PM		PowerShell-Script
Recent defa... Version 1	Custom Script Detection	Nov 7, 2023 02:00 PM	AD Security Posture	PowerShell-Script
Netlogon se... Version 1	Custom Script Detection	Nov 7, 2023 02:00 PM	AD Security Posture	PowerShell-Script
Custom Script action		Nov 4, 2023 04:30 PM	AD Security Posture	PowerShell-Script
Custom Script action		Nov 2, 2023 09:30 AM	AD Security Posture	PowerShell-Script

**Add Software To Authorization Rule**  
Track the software product as authorized/unauthorized.

Visual C++ 2008 Redistributable  
Auxiliary Software / Other

This Update (9.0.30729.6161)  Entire Product

Authorization \*  CIDS

Mark as Required

ORDER NUMBER	RULE	STATUS	TAGS
<input type="radio"/>	1 Database Servers	Enabled	Type: Database Se...
<input type="radio"/>	2 Web Server	Enabled	Cloud Agent
<input type="radio"/>	3 Data Center Server	Enabled	1 more

# Qualys Enterprise TruRisk™ Platform

Helps to Eliminate Risk Faster!

## Certificates Associated Risk

- ✓ Consistent approach to managing certificates regardless of the issuing Certificate Authorities across protocols and technology
- ✓ Reduce operational incidents associated with missed and incomplete certificate renewals

## Cloud Misconfigurations Associated Risk

- ✓ Eliminate Cloud misconfigurations reducing the risks of exposure
- ✓ Shortened the feedback loop to DevOps team to reduce the remediation efforts



### Certificate Information



DigiCert Extended Validation CA G3

Expires in 2560d 14h 10m by Nov 11, 2030 07:00 AM

Issued by DigiCert Global Root G3

Valid

#### Issued to

Name: DigiCert Extended Validation CA G3  
Organization: [DigiCert Inc](#)   
Country: US

#### Issued by

Name: DigiCert Global Root G3  
Organization: DigiCert Inc  
Issuer: DigiCert Global Root G3  
Country: US

#### Fingerprints

Fingerprint: 7C0912E5DE8478BB86E8EA46BA5AE65D  
C3870BCEFCBC2F46795EEECF648CFBE7  
Parent Fingerprint: -

### Activity Details

#### Inventory Details

Resource ID	sg-07b9665bbdc9c0ea	Resource Type	Security Group	Cloud Provider	AWS
Account ID	860454016470	Region	Cape Town (af-south-1)		

#### Control Details

Control CID	41	Control Name	Ensure no security groups allow
Policy Name	Fedramp		
	<a href="#">2 more</a>		

#### Remediation Activity

Action	Control Remediation	Triggered On	Oct 22, 2023 11:51 PM	Triggered By	Nirav Kamdar - CORP-Demo
--------	---------------------	--------------	-----------------------	--------------	--------------------------

# Book a Meeting With Me and My Team

- Get free health check for your environment
- Get tailored recommendations to de-risk your environment







# Strengthening Your Security and Compliance Posture with a Single Qualys Cloud Agent



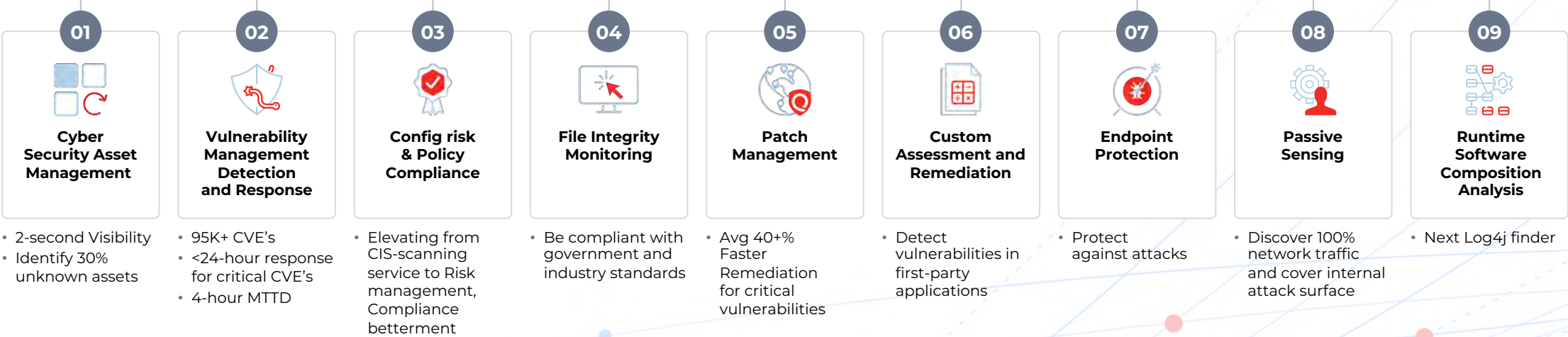
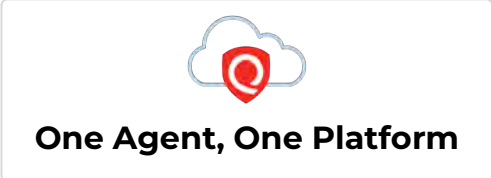
**Spencer Brown**  
Product Manager  
Qualys Cloud Agent

# Agenda

- 01** Qualys Cloud Agent Capabilities and Extensive Platform Support
- 02** The **Power** of Agent with Qualys Enterprise TruRisk™ Platform
- 03** Finetuning Agent for Optimum Performance
- 04** Agent Enhancements



# Measure, Communicate and Eliminate Risk with Cloud Agent





Asset Details: 135355-T490AD

- INVENTORY
  - Asset Summary
  - System Information
  - Network Information
  - Open Ports
  - Installed Software
  - Traffic Summary
  - Business Information
- SECURITY
  - TruRisk Score
  - Vulnerabilities
  - VMDR Prioritization
  - Patch Management
  - EDR
  - Certificates
- COMPLIANCE
  - File Integrity Monitoring
  - Policy Compliance
- SOURCES
  - Summary
  - Passive Sensor
  - CAPS

### System Information

- SPECIFICATIONS
- SERVICES
- USERS
- CUSTOM ATTRIBUTES

#### Operating System

Name  
Microsoft Windows Server 2012 Standard (6.2)

Installed Date  
Dec 9, 2020 01:36 PM

Lifecycle Information  
**End-of-Service (Unsupported)**

Sep 03 2012 Oct 08 2018 Oct 09 2023

Generally Available End-of-Life End-of-Service

#### Hardware

Category  
Virtualized / Virtual Machine

Manufacturer/Model  
VMware VMWare Virtual Platform



















Lifecycle Information  
Unknown

#### Other Information

Timezone GMT +05:30	Last System Boot Oct 14, 2023 05:55 PM	Total Memory 4 GB
BIOS Description Phoenix Technologies LTD 6.00	BIOS Asset Tag NoAssetTag	BIOS Serial Number VMware-42 2a 66 2a d8 39 29 d3-06 72 e6 c8 6c c9 85 0c
BIOS Hardware UUID 2A662A42-39D8-0329-0672-E6C860C9850C	Domain Role Primary Domain Controller	



# Extensive Multi-Platform Support

 <b>Windows</b> .exe (x86_64)	 <b>Windows</b> .exe (ARM64)	 <b>Linux</b> .rpm (x86_64)	 <b>Linux</b> .rpm (ARM64)	 <b>Linux</b> .rpm (ppc64le)	 <b>Linux</b> .deb (x86_64)
 <b>Windows</b> .exe (x86_64)	 <b>zSystems LinuxONE</b> .rpm (s390x)	 <b>zSystems LinuxONE</b> .rpm (s390x)	 <b>Mac</b> .pkg (x86_64)	 <b>Mac</b> .pkg (Apple Silicon)	 <b>BSD UNIX</b> .txz (x86_64)
 <b>AIX</b> .bff (POWER)	 <b>Solaris</b> .pkg (x86_64,SPARC)	 <b>CoreOS</b> .tar (x86_64)	 <b>ChromeOS</b> .apk (x86_64)	 <b>SQL Server</b>	 <b>Oracle Database</b>

 - Qualys Only

# Qualys Cloud Agent

Install anywhere with minimal impact, and stay updated in real-time

Install anywhere with minimal impact, and stay updated in real-time



### Light weight, extensible, self-updating & centrally managed:

Brings the functionality of Qualys Cloud Platform and enables to move beyond traditional remote scans.



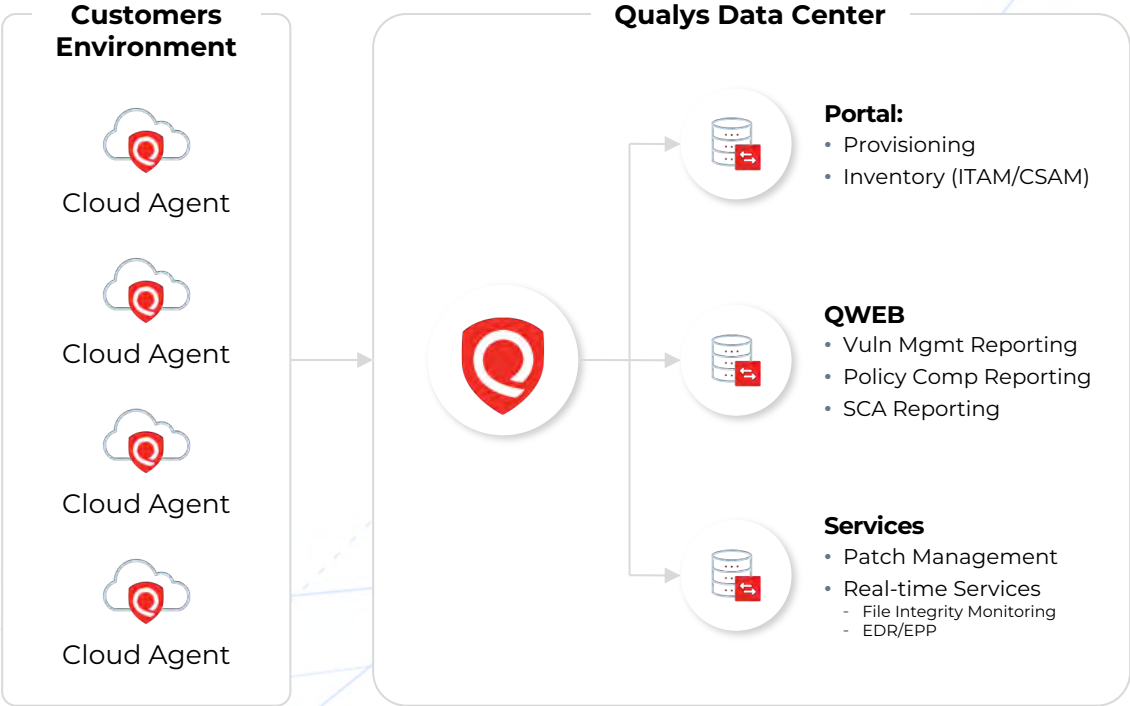
### Real-time actionable delta collection with customizable configuration profile:

Raw data points and cloud metadata are collected in real-time with Delta Based Approach (Patented, 5-350 K.B per day with 1-2% CPU)



### Continuous evaluation and data enrichment on platform, seamless API integration :

Data matched against Qualys KB/Threat Intel feeds. MTD is 2.5 hours.



# Qualys Cloud Agent Performance Metrics

	Memory Usage	CPU
VM	23.46 MB	2.35%
PC	11.57 MB	2.2%
Inventory	7.88 MB	2.10%
VM + FIM	48.01 MB	2.8%
INV + FIM	34.31 MB	2.3%
INV + Auto-Disc	34.31 MB	2.27%

# Finetuning Agent General Settings

## for Optimum Performance



[Best Practices Guide](#)



### Auto-upgrade

80% of all Cloud Agents have auto-upgrade enabled

- Feature Enhancements
- Bug Fixes
- Security Updates



### Memory and Disk I/O Flexibility

In-Memory SQLite Databases allows users the choice to write to disk or keep scans in memory

Step 1 of 12

- 1 General Info ✓
- 2 Blackout Windows ✓
- 3 Performance ✓
- 4 Assign Hosts
- 5 Agent Scan Merge
- 6 VM Scan Interval
- 7 PC Scan Interval
- 8 SCA Scan Interval
- 9 FIM
- 10 EDR
- 11 PM

Configure a profile for your agents

Customize agent behavior by defining a configuration profile. (\*) REQUIRED

#### Profile Name\*

QSC Rocks!

- Make this the default profile for the subscription
- Suspend data collection for VM, PC, SCA and Inventory for all agents using this profile
- In-Memory SQLite Databases
- Prevent auto updating of the agent binaries

Enter a description for this configuration profile.

#### Description

# Finetuning Agent Performance

## for Optimum Performance

- ✓ **Agent Status Interval** – Set this to 900 seconds so the agent can check with the platform every 15 minutes for updates. As each check-in is less than 1KB, there is no impact on the agent or network.
- ✓ **Delta Upload Interval** – Unless the host's network is severely constrained, set this between 10 and 20 seconds.
- ✓ **Chunk Size for File Fragment Uploads** – Unless the host's network is severely constrained, set this to at least 2048 KB (2MB).
- ✓ **Upgrade Reattempt Interval** – Set a timeout of 64,800 seconds so that if the agent binary upgrade fails, it will try again in 18 hours.
- ✓ **CPU Limit** – As a minimum, keep this at 10% or above. Setting this below 10% will exponentially increase scan times and affect scan data timeliness.
- ✓ **CPU Throttle** – As a minimum, keep this at 20ms or below. Setting this above 20ms will exponentially increase scan times.



## Best Practices Guide

**Step 3 of 12**

- 1 General Info ✓
- 2 Blackout Windows ✓
- 3 Performance ✓**
- 4 Assign Hosts
- 5 Agent Scan Merge
- 6 VM Scan Interval
- 7 PC Scan Interval
- 8 SCA Scan Interval
- 9 PM
- 10 EDR
- 11 PM

### Configure Agent Performance

These settings govern how an agent behaves, from how often it checks into the Qualys platform, to how often it checks the host for changes. It also includes performance settings that control CPU and network utilization.

#### Performance

Select one of the performance levels below. Keep the default settings or customize them. **Customize**

Based On:

#### Set Parameters

<b>Agent Status Interval*</b> Push interval in seconds to update system with Agent's status	<input type="text" value="900"/> sec
<b>Delta Upload Interval*</b> Interval an agent attempts to upload detected changes	<input type="text" value="20"/> sec
<b>Chunk sizes for file fragment uploads*</b> This is the upload block size, and combined with the above Network throttle Tx, determines network utilization	<input type="text" value="2048"/> KB
<b>Upgrade Reattempt Interval*</b> Interval an agent will retry applying a new upgrade to itself	<input type="text" value="64800"/> sec(32400)

# Finetuning Agent General Settings

## for Optimum Performance



[Best Practices Guide](#)

### Agent Scan Merge

- Merge network scanner and the Qualys Cloud Agent scans
- Validate ports

### VM Scan Interval

Data Collection Interval at 240 minutes (4 hours)

### PC/SCA Scan Interval

- Data Collection Interval to 2160 minutes (36 hours) or higher. It is usually set between 4320 minutes (3 days) and 10080 minutes (7 days)
- On-Demand scan



**Step 5 of 12**

- 1 General Info ✓
- 2 Blackout Windows ✓
- 3 Performance
- 4 Assign Hosts ✓
- 5 Agent Scan Merge**
- 6 VM Scan Interval
- 7 PC Scan Interval
- 8 SCA Scan Interval
- 9 FIM
- 10 CDN
- 11 VM

### Configure Agent Scan Merge

Enable Agent Scan Merge for this profile

Ports\*

Customized ports must be included in the Option Profile for scanner to capture. Make sure to use ports that aren't used by any other service in your environment.

Bind All

#### On Premise Detection

IP Address(In Range)  /

Gateway

Subnet Mask

DNS Suffix Regex  E.g ^

# Rapid Certificate Deployment and Renewal with Cloud Agent



## Certificate Challenges

- Lack of visibility
- Lack of automation
- Major Internet organizations moving to 90-day expirations



## Same Agent

- Collect certificate information including expiration date
- Automate deployment
- Leverage Qualys Enterprise TruRisk™ Platform

The screenshot displays the Qualys Cloud Platform interface for Certificate Auto-Renewal. The page title is "Certificate Auto-Renewal : Digi-Cert". A sidebar on the left shows "STEPS 1 / 3" with "General Settings" selected. The main content area is titled "General Settings" with a sub-heading "Sub Heading". Below this is a section for "Selected Expiring Certificates" showing a table of certificates with columns for Name/Organisation, Expiration, Last Found, Instances, and Asset. Below the table is a section for "Selected CSR Template" with a table showing details for the "DigiCert Template".

NAME/ORGANISATION	EXPIRATION	LAST FOUND	INSTANCES	ASSET
winsrv2016-2001.qualys.com	Nov 20, 2023	Nov 3, 2023	1	
winsrv2016-2002.qualys.com	Nov 21, 2023	Nov 3, 2023	1	
winsrv2016-2003.qualys.com	Nov 21, 2023	Nov 3, 2023	1	
winsrv2016-2008.qualys.com	Nov 23, 2023	Nov 3, 2023	1	
winsrv2016-2009.qualys.com	Nov 23, 2023	Nov 3, 2023	1	
winsrv2016-2014.qualys.com	Nov 25, 2023	Nov 3, 2023	1	
winsrv2016-2019.qualys.com	Nov 25, 2023	Nov 3, 2023	1	
winsrv2016-2022.qualys.com	Nov 25, 2023	Nov 3, 2023	1	
winsrv2016-2023.qualys.com	Nov 25, 2023	Nov 3, 2023	1	
winsrv2016-2028.qualys.com	Nov 25, 2023	Nov 3, 2023	1	

TEMPLATE NAME	CERTIFICATE AUTHORITY	KEY ALGORITHM	PRIVATE KEY REUSE
DigiCert Template	DigiCert	RSA 2048, RSA 3072, RSA 4096	No

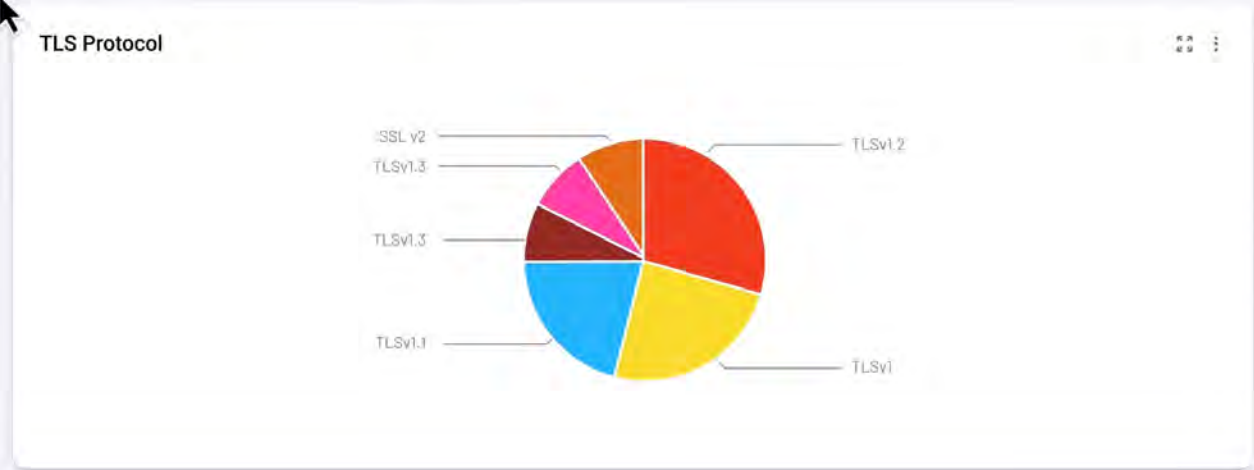
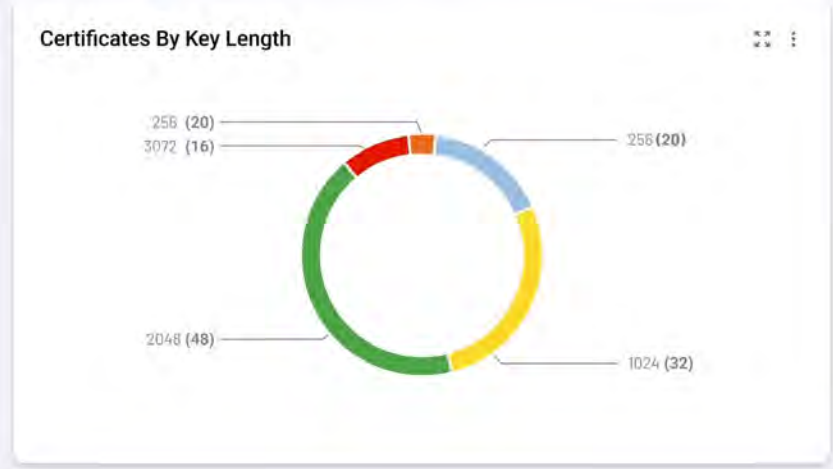
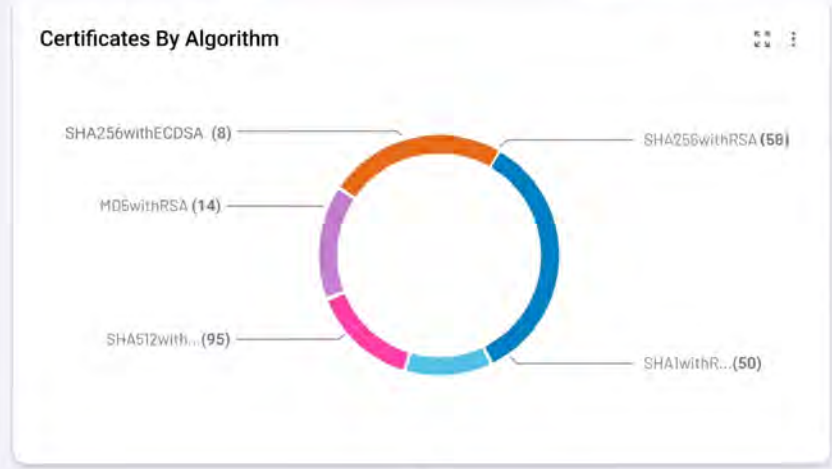


Qualys Certificate View

Any All Last 30 Days

Total Widgets Count: 20 / 80 Add Widget

25 TLS Secure Renegotiation | 45 Self-Signed-Certs | 23 SSL Insecure Protocol | 15 SSL Certs-Signature Verification | 17 Signature Verification Failed | 7 Windows Has SSLV2 Enabled



# Local Agent Health Check

Bundled Command Line Utility



## Third-Party Deployment Tools

Leverage Intune, Ansible or JAMF to monitor agent health more than just installation and running process



## Qualys Scanner

Leverage your authenticated scans and be notified of unhealthy agents



## Local Agent Troubleshooting

Give IT admins the tools necessary to troubleshoot without learning the minutiae of the agent



json

```
{
  "HEALTH": "GOOD",
  "CUSTOMER": "22D2B914-911D-432F-8010-FA67B8421E70",
  "AGENT": "B6746F9A-9273-4E62-9DD1-BBEDCE8813B9",
  "CONFIG": "CBC48E66-8F89-47B5-9DC2-83981F1491CD",
  "PROVISIONED": "YES",
  "RUNNING": "YES",
  "LAST SUUCCESSFUL COMMUNUCATION": "2023-04-09 22:31:50.308",
  "VERSION": "5.1.0-18",
  "CERTIFICATE MISSING": "NONE",
  "PROXY": "10.10.101.234:80",
  "LOG LEVEL": 5,
  "DRIVER": {
    "VERSION": "5.0",
    "STATE": "RUNNING"
  },
  "MANIFESTS": {
    "INVENTORY": {
      "VERSION": "2.2.467.7",
      "UUID": "09546E9C-E032-4A41-9CD1-489BEEDC962D"
```

# Enhanced Visibility

with Health and Status Messages



## Health and Status Messages

Agents send Health and Status Messages every 5 minutes to the Qualys Cloud Platform



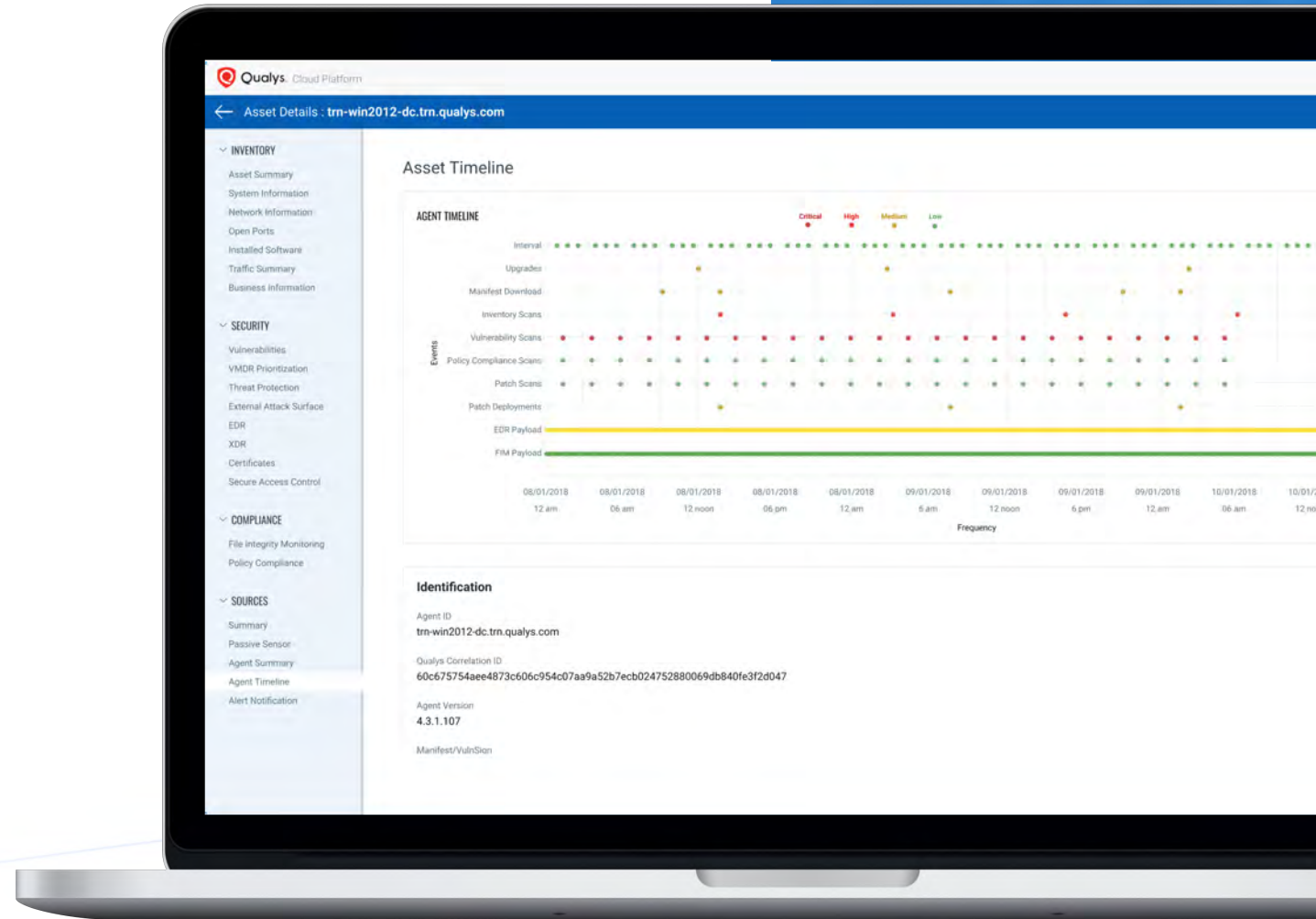
## Visibility

Search agent events such as On-demand Scan, Agent Upgrade and Manifest Download giving you the visibility for troubleshooting



## Confidence

Give leadership confidence so you can focus on what really matters (stopping attacks)



# Zero Touch Lifecycle

No More Remote Sessions or IT Tickets



## Zero Touch Lifecycle



### Discover Unknown Assets

Continuous and unobtrusive detection of all the assets on your network



### Deploy Agent with Scanner

Leverage Qualys Scanner Appliance to deploy Cloud Agents



### Be Secure



### Troubleshoot Remotely

- Remotely enable debug logging
- Remotely restart agents
- Remotely disable Self-protection
- Remotely capture agent logs



### Clean Up

- At the end of the lifecycle, purge agent data
- If agent checks-in again, agent will not be uninstalled

# Agent Exclusions

Exclude Directories, Commands and Detections from Agent Scans



## Global Set Up

Create exclusions for all agents and apply to all agent scans regardless of activated modules



## Awareness

Know the impact of the exclusion to avoid blind spots

## Exclusion Types

- Paths and Directories or all network drives
- Commands
- Detections



## Add Exclusion

Sub Heading

OS \*

Linux

Command \*

slapd -V

Files & Directories \*

/var/log

Cancel

Exclude

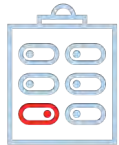
# Asset Identification Rules

## Improvements for VDI Environments



### Asset Identification Service

New service to merge newly provisioned Qualys Agents with existing records using asset attributes such as MAC address, Hostname and Netbios



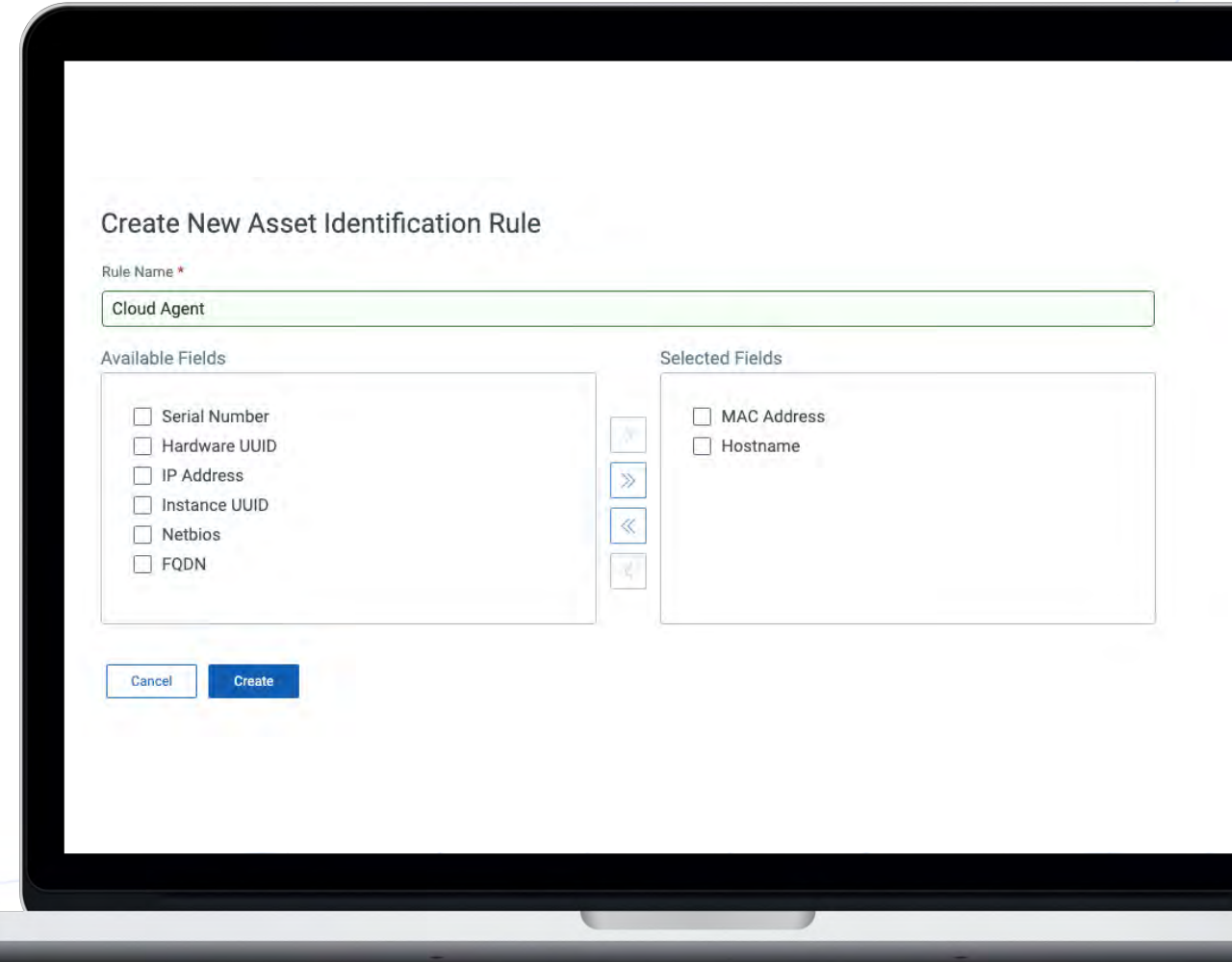
### Built for VDI Environments

Merge persistent and non-persistent VDI assets into a single record while maintaining created and first found dates



### Set It and Forget It

No additional configuration needed on the endpoint. Simply set up the rule and the Qualys Cloud Platform will take care of the rest



# Agent Version Control

Lock Your Agents to Specific Versions

## Up-to-date Agent Version

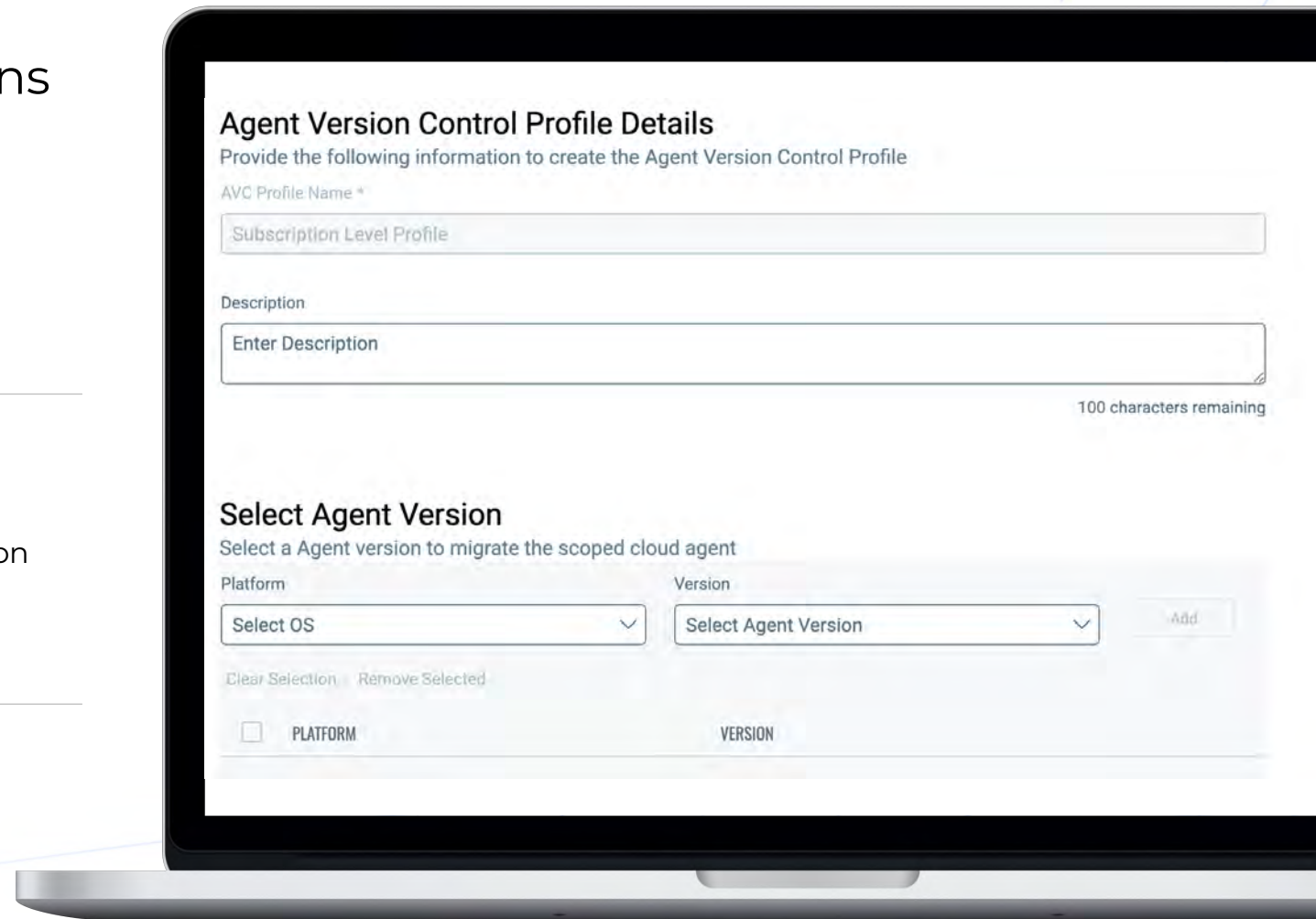
- ✔ Feature Enhancements
- ✔ Security Updates
- ✔ Bug Fixes

## Version Control

- ✔ Create an Agent Version Control Profile to lock specific platforms (Windows, Linux, etc.) to a certified agent version by your organization
- ✔ Download previous binaries for testing and deployments

## Auto-upgrade with Control

Leverage auto-upgrade when your organization is ready while alleviating dependency and workload on other teams



# Reduced Activity Period

## Flexible Control Over Agent Activity and Network Transmission

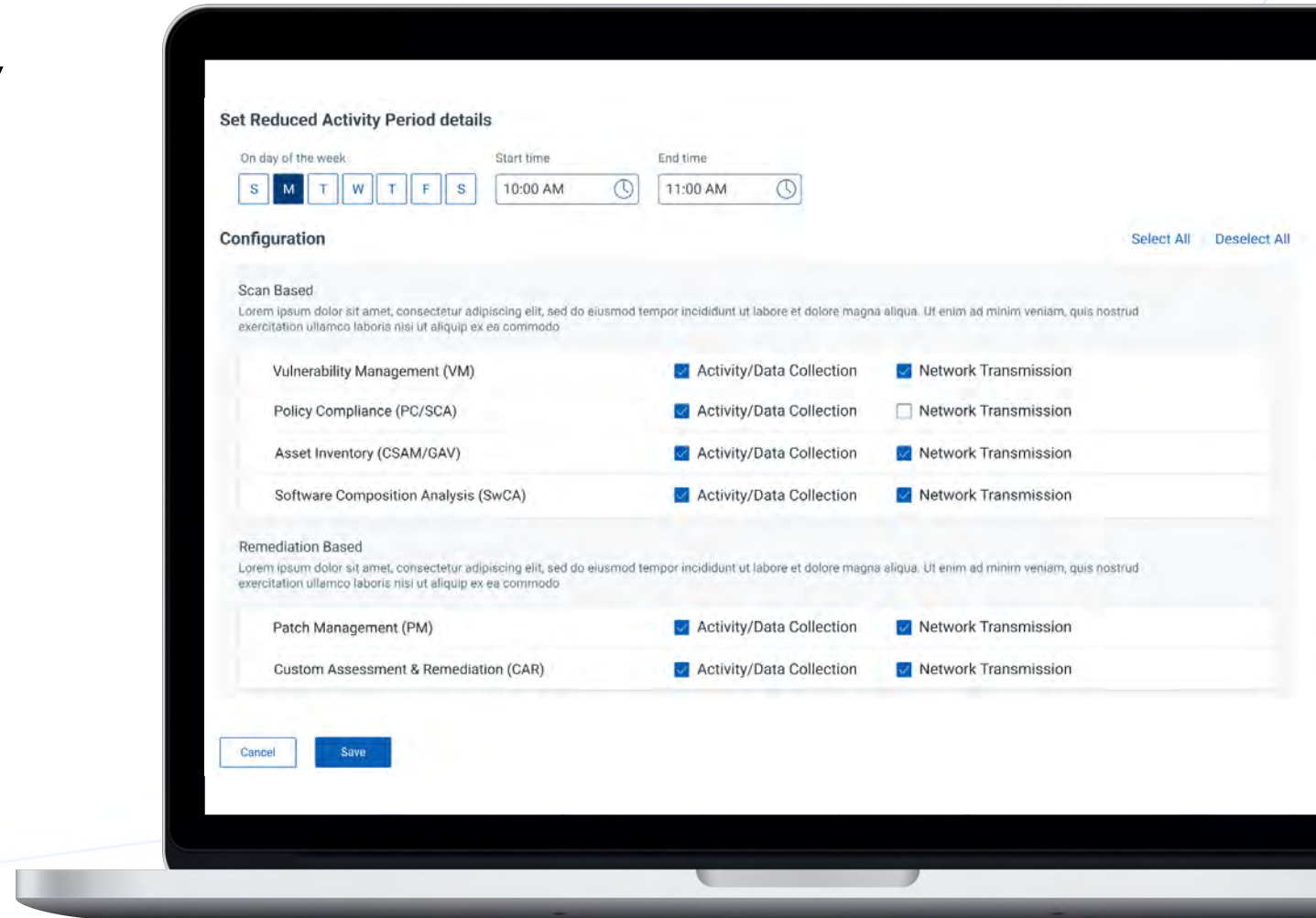


### Meet Business Needs

Comply with security requirements while also playing nice with others to meet business needs

### Flexibility

- ✓ Day and Time
- ✓ Agents
- ✓ Modules
- ✓ Activity and Data Collection
- ✓ Network Transmission









Associated  
British Foods  
plc

# Increasing Visibility and Reducing Risk with Associated British Foods

Tom Copeland  
Associated British Foods



# Tom Copeland



Head of Governance,  
Risk & Compliance



Lives near London in the UK



10 Years in ABF holding  
various Security roles



Worked with Qualys  
since 2014



**Associated  
British Foods**  
plc

# We're Associated British Foods

A Summary



Global, highly diversified and federated organization with a range of retail, food and ingredients businesses over **73 different brands**



**132,000** employees, **\$25+ billion** annual revenues



Operates in **55 countries**

# Challenges

## Distributed, Segmented, and Rigid Risk Measurement



### Highly Federated

- Global organization
- 300+ Qualys Users in 30+ countries
- Many distinct BUs with their own needs and compliance requirements



### Years of Organic Development

- Many BUs built-up dashboards, tags, users, etc.
- 300+ dashboards, many unused or redundant
- Multiple Siloed tools
- Exclusions heavily used, not clear picture of what the real risk is



### Rigid Risk Reporting

- Multiple Home-grown system's for prioritizing and reporting vulnerabilities
- Resource intensive to maintain and expensive to enhance, creating a rigid reporting structure
- Difficult to get a consolidated view of risk at the corporate and BU level

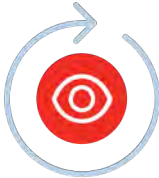
# Success Criteria: Implementation

Requirements for Success



## Standardization

Standardize the use of Qualys platform using one agent approach across ABF.



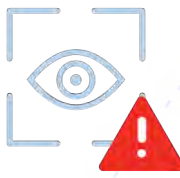
## Optimization

Ensure all ABF BUs maximize their ROI on Qualys modules.



## Autonomy

Give autonomy back to patching teams and evolve from custom built solutions such as Protection Scores.

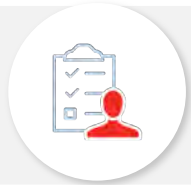


## Risk Awareness

Embed new reporting metrics such as TruRisk, Qualys Detection Scores and Mean Time to Remediate.

# Solution: Cybersecurity Enhancement Project

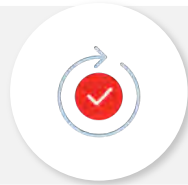
100k Cloud Agents were deployed on laptops, VMs, Servers and Cloud



## STEP 01 Define

### Develop Vulnerability Management Standards

- ✓ Tagging structure
- ✓ Exception policy
- ✓ Access Control
- ✓ Reporting
- ✓ Review Module & Qualys Best Practice
- ✓ Change Management – Circulate changes and seek input from BUs



## STEP 02 Implementation

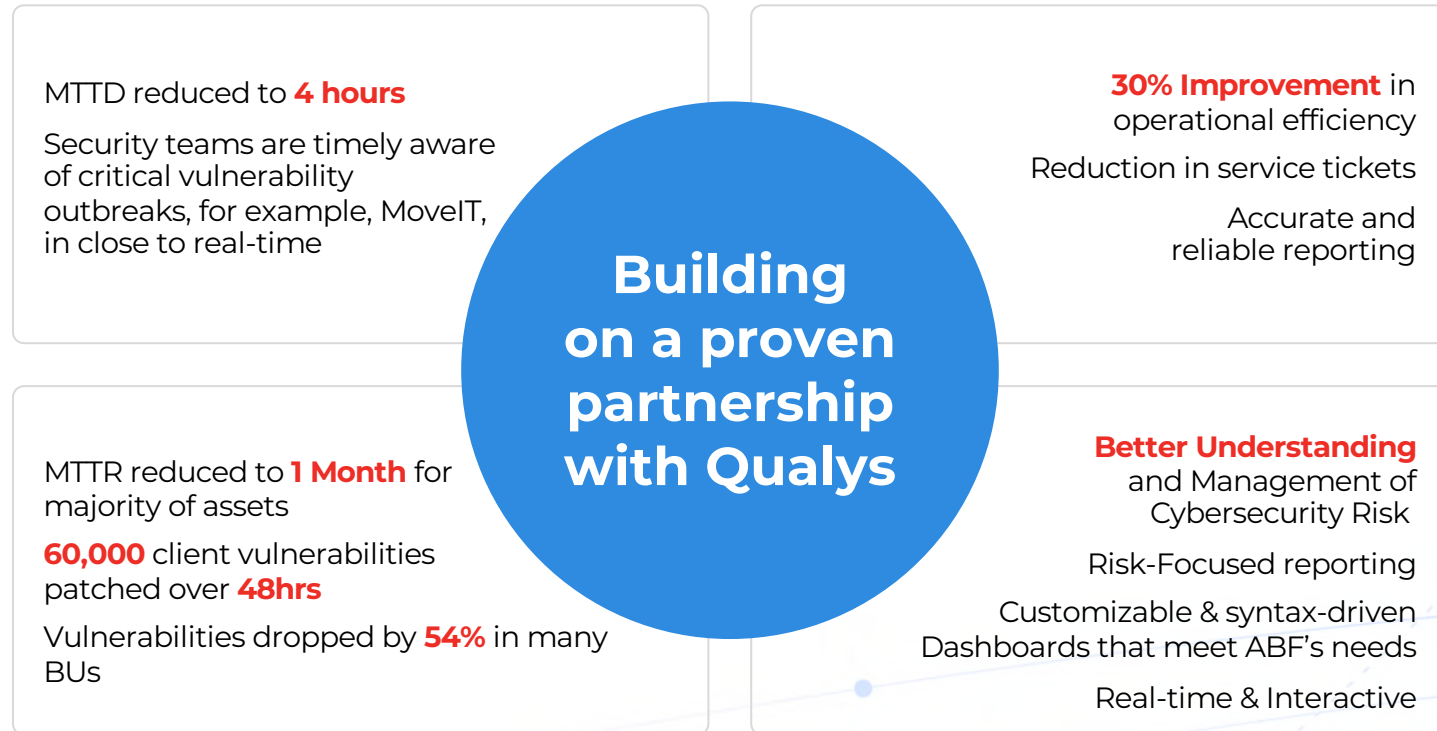
- ✓ Clear down tagging structure and rebuild to standard
- ✓ Remove all exclusions
- ✓ Update access
- ✓ Tru Risk reporting
- ✓ Application Patching
- ✓ Data Centre Scanners
- ✓ Asset Management & Hardening



## STEP 03 Continuous improvement

# Driving Outcomes with Qualys

100k+ cloud agents were deployed on laptops, VMs, Servers & Cloud



- ✓ Allows other metrics to be utilized.  
Focus shift to time it takes remediate vulnerabilities
- ✓ Lowered asset risk scores by 70% in less than a year
- ✓ Custom, accurate, trusted reporting to the C-Level
- ✓ Maintained low CPU consumption with no impact to business applications
- ✓ Quickly prioritized high-risk external facing assets



# The Solution: Qualys TruRisk Platform

Transparent and Uniform Means of Quantifying Risk

## Adopting TruRisk

Hygiene  
Tags

Hygiene  
Users

Hygiene  
External URLs

Refresh Dashboards  
and Metrics

## Replace existing legacy risk metrics with Qualys TruRisk



**More flexibility, leveraging multiple risk variables** including business criticality, asset exposure, and other risk factors



**Give BUs autonomy** to create, measure, and **optimize their own VM strategies**



**Deliver metrics** in a scalable, consistent, and supportable manner, removing reliance on custom home-grown solution

# The Solution: Qualys TruRisk Platform

## Implementing Consistent Tags

- Adopting TruRisk
- Hygiene Tags**
- Hygiene Users
- Hygiene External URLs
- Refresh Dashboards and Metrics

### Develop consistency in how tags are applied across ABF



Key to **accurate reflection of risk** and remediation strategies



Collaborate with BUs to **trim tags** down to logical and succinct set



**Apply new tags**



**Give BUs 60 days to update tag-dependent dashboards** and reports

# The Solution: Qualys TruRisk Platform

Enforcing User Policy and Privileges

- Adopting TruRisk
- Hygiene Tags
- Hygiene Users**
- Hygiene External URLs
- Refresh Dashboards and Metrics

## Groom user base to ensure proper usage and permissions



**Reduce/slash unused user accounts** created unnecessary clutter and confusion



Disable accounts not logged in within 30 days



Delete accounts not logged in within 60 days

# The Solution: Qualys TruRisk Platform

Web Access and Web Application Scanning (WAS)

Adopting TruRisk

Hygiene  
Tags

Hygiene  
Users

Hygiene  
External URLs

Refresh Dashboards  
and Metrics

Ensure external scanning is optimized to eliminate unnecessary licensing



**Collaborate with BUs** to review current list, **add/remove sites as needed**



**Apply correct and standard tagging** rules as part of review process.

# The Solution: Qualys TruRisk Platform

## Consolidated and Uniform Dashboards

Adopting TruRisk

Hygiene  
Tags

Hygiene  
Users

Hygiene  
External URLs

Refresh Dashboards  
and Metrics

### Develop consistency in dashboards and reporting across BUs



**More than 300 dashboards**, many broken or obsolete, made reporting a challenge, especially across BUs



Standardized on 3 dashboard concepts:

- **Management**
- **SecOps**
- **IT Ops**



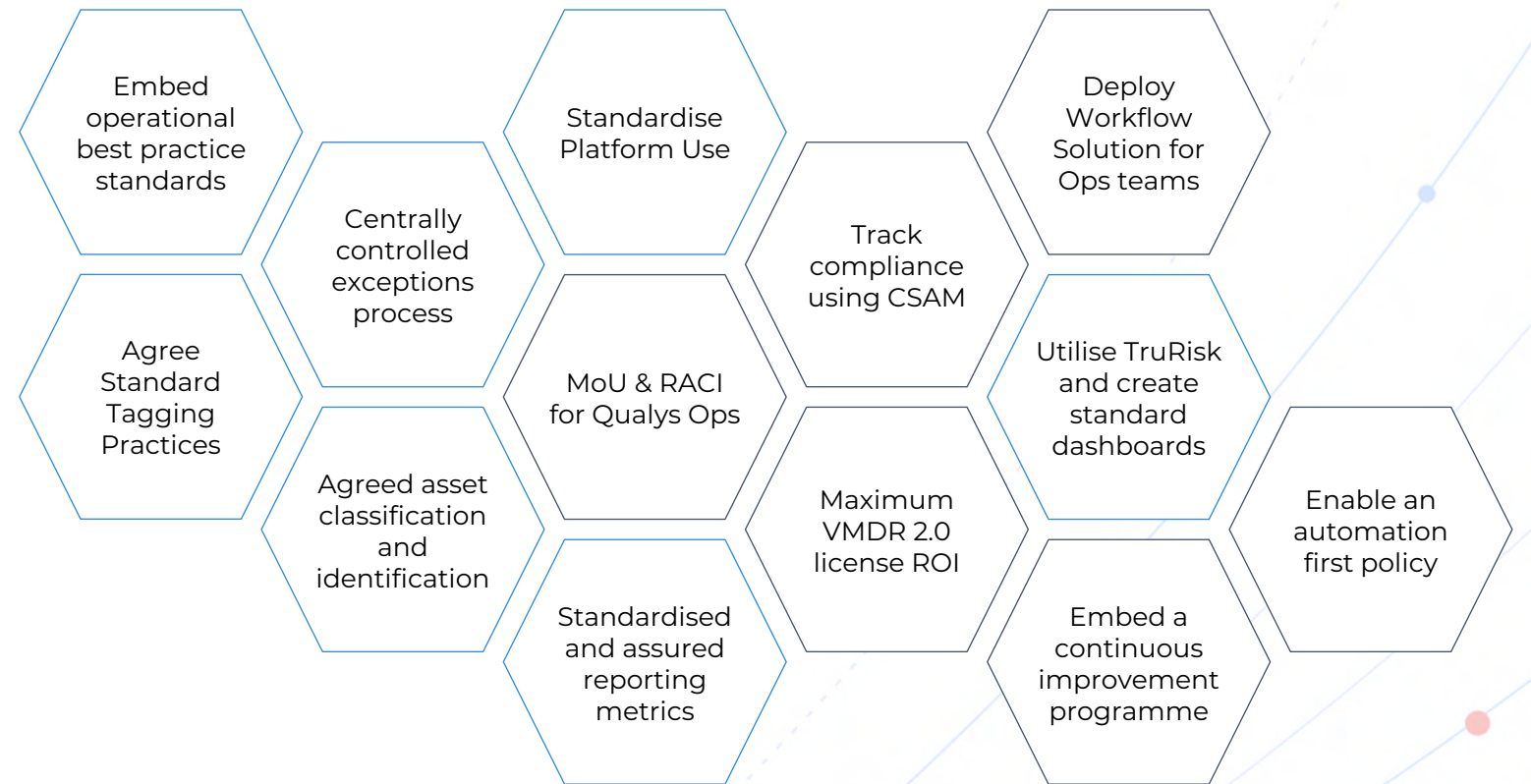
Solicited feedback from BUs on metrics to include in each



BUs to remove obsolete dashboards once standardized dashboards are in place

# Risk Journey: Reducing Risk with Qualys

End-to-End Platform for Risk-based Vulnerability Management



In Progress

Maturity

# “Success in vulnerability management is not just about finding and fixing weaknesses;

it's about building a culture of continuous improvement and security awareness, where every identified vulnerability is an opportunity to strengthen our defenses and protect what matters most.”

**Tom Copeland**

