Qualys.

ROCon 25

The Risk Operations Conference

AMERICAS

One Agent to Rule Them All

Consolidation, Coverage, and Control Without the Sprawl

Spencer Brown

Principal Product Manager,
Cloud Agent, Qualys

Agenda

One Agent to Rule Them All

01 Agent Fatigue

02 Qualys Cloud Agent

03 New Capabilities

04 Innovations

05 Customer

Too Many Agents, Not Enough Time

Agent sprawl slows teams, increases risk, and drains resources.

3–5

Organizations run three to five agents per device, but some endpoints still have 10 or more, creating performance and management headaches.

11%

Only 11% of MSPs report their tools integrate seamlessly, meaning most are stuck juggling disconnected dashboards and manual workflows

75%

Three out of four security buyers are actively consolidating vendors to simplify operations, cut costs, and reduce risk

Business Impact of Agent Consolidation

Driving efficiency, savings, and strategic value

Faster Time-to-Value

Centralized, consistent data enables quicker insights and faster business decisions.

Improved Resource Efficiency

Less CPU, memory, and storage usage across endpoints minimizes hardware strain.

Reduced Operational Overhead

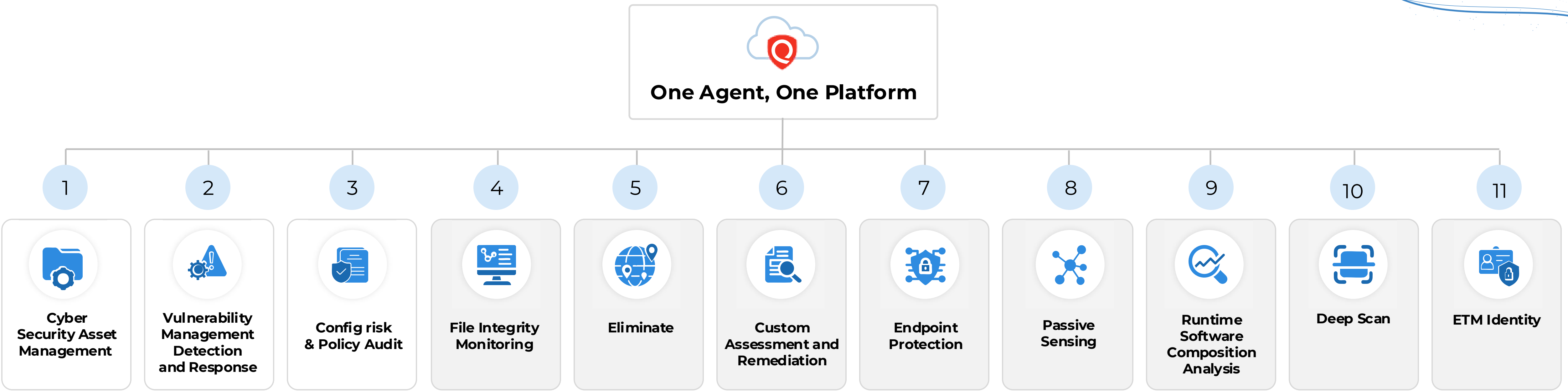
Simplified management cuts time spent on upgrades, troubleshooting, and conflicts.

Lower IT Costs

Fewer agents to license, deploy, and maintain reduces overall infrastructure and support expenses.

One Agent to Rule Them All

Qualys ROCon 25
The Risk Operations Conference
AMERICAS



One Agent, One Platform

1. **Cyber Security Asset Management**
   - 2-second Visibility
   - Identify 30% unknown assets
2. **Vulnerability Management Detection and Response**
   - 95K+ CVE's
   - <24-hour response for critical CVE's
   - 4-hour MTTD
3. **Config risk & Policy Audit**
   - Elevating from CIS-scanning service to risk management compliance
4. **File Integrity Monitoring** ▨
   - Be compliant with government and industry standards
5. **Eliminate** ▨
   - Avg 40+% Faster Remediation for critical vulnerabilities
6. **Custom Assessment and Remediation** ▨
   - Detect vulnerabilities in first-party applications
7. **Endpoint Protection** ▨
   - Protect against attacks
8. **Passive Sensing** ▨
   - Discover 100% network traffic and cover internal attack surface
9. **Runtime Software Composition Analysis** ▨
   - Next Log4j finder
10. **Deep Scan** ▨
    - Discover vulnerabilities in non-standard locations
11. **ETM Identity** ▨
    - Uncover identity risks and enforce least-privilege access

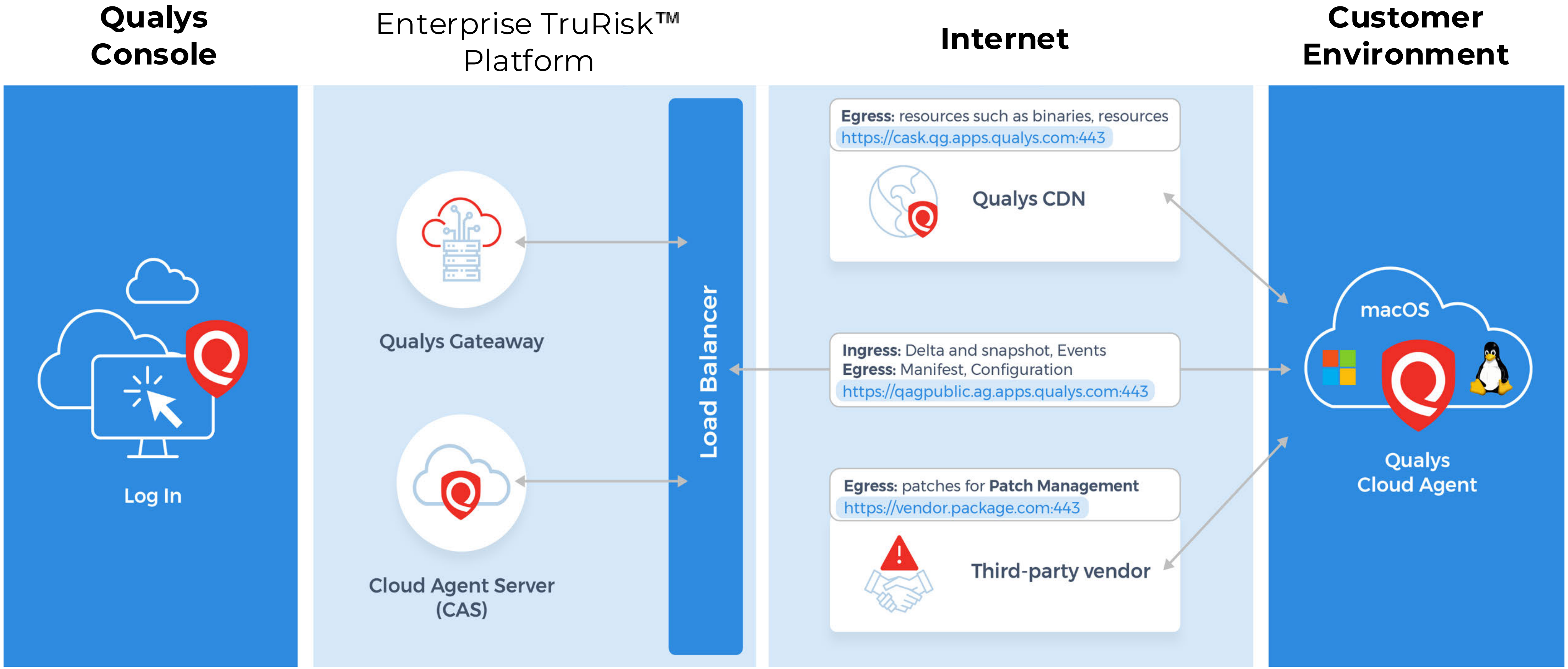
▨ - Qualys Cloud Agent Only

Most Expansive Platform Coverage

Windows .exe (x86_64)	**Windows** .exe (ARM64 with emulation)	**Linux** .rpm (x86_64)	**Linux** .rpm (ARM64)	**Linux** .rpm (ppc64le)	**Linux** .deb (x86_64)
Windows .exe (x86_64)	▨ **zSystems LinuxONE** .rpm (s390x)	▨ **zSystems LinuxONE** .rpm (s390x)	**Mac** .pkg (x86_64)	**Mac** .pkg (Apple Silicon)	**BSD UNIX** .txz (x86_64)
AIX .bff (POWER)	**Solaris** .pkg (x86_64,SPARC)	▨ **GenToo** .tar (x86_64)	▨ **ChromeOS** .apk (x86_64)	**SQL Server**	**Oracle Database**
▨ - Qualys Only	▨ **Bottlerocket OS** .tar (x86_64)	**Container-optimized OS by Google** .tar (x86_64)	▨ **CoreOS** .tar (x86_64)		

Qualys Cloud Agent Architecture

Qualys ROCon 25 The Risk Operations Conference AMERICAS



Qualys Console

Enterprise TruRisk™ Platform

Internet

Customer Environment

Log In

Qualys Gateaway

Cloud Agent Server (CAS)

Load Balancer

Egress: resources such as binaries, resources
https://cask.qg.apps.qualys.com:443

Qualys CDN

Ingress: Delta and snapshot, Events
Egress: Manifest, Configuration
https://qagpublic.ag.apps.qualys.com:443

Egress: patches for **Patch Management**
https://vendor.package.com:443

Third-party vendor

macOS

Qualys Cloud Agent

Qualys Cloud Agent Missing from Hosts

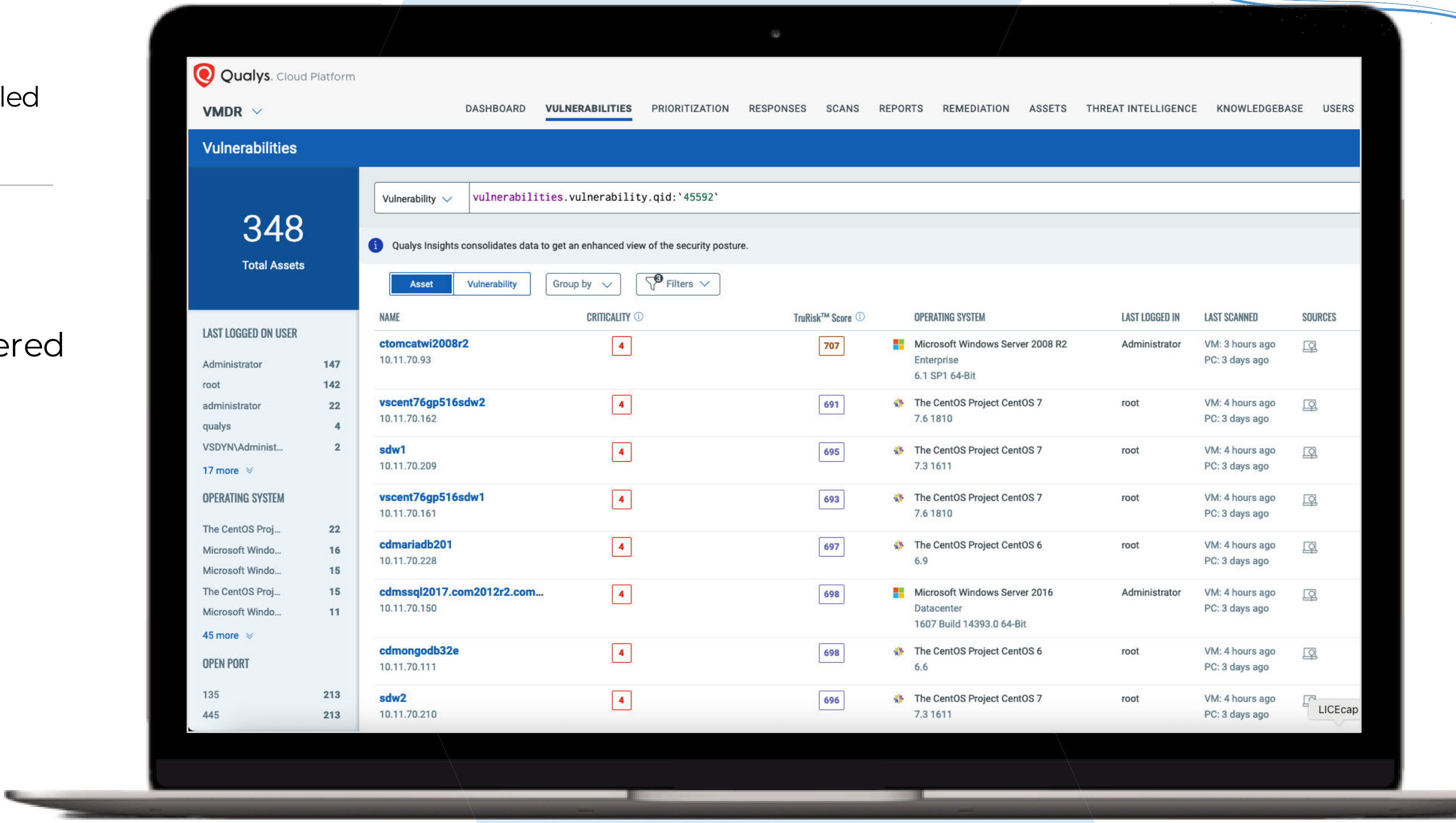
Discover eligible assets which are missing the Qualys Cloud Agent

QID: 45592

Title: Qualys Cloud Agent Not Installed

About

- Authenticated Information Gathered QID
- Supported by Scanner
- Flags on eligible assets only
- Create alerts
- Monitor via dashboards



Vulnerabilities

348
Total Assets

Vulnerability `vulnerabilities.vulnerability.qid:`45592``

Qualys Insights consolidates data to get an enhanced view of the security posture.

LAST LOGGED ON USER	
Administrator	147
root	142
administrator	22
qualys	4
VSDYN\Administ...	2
17 more	

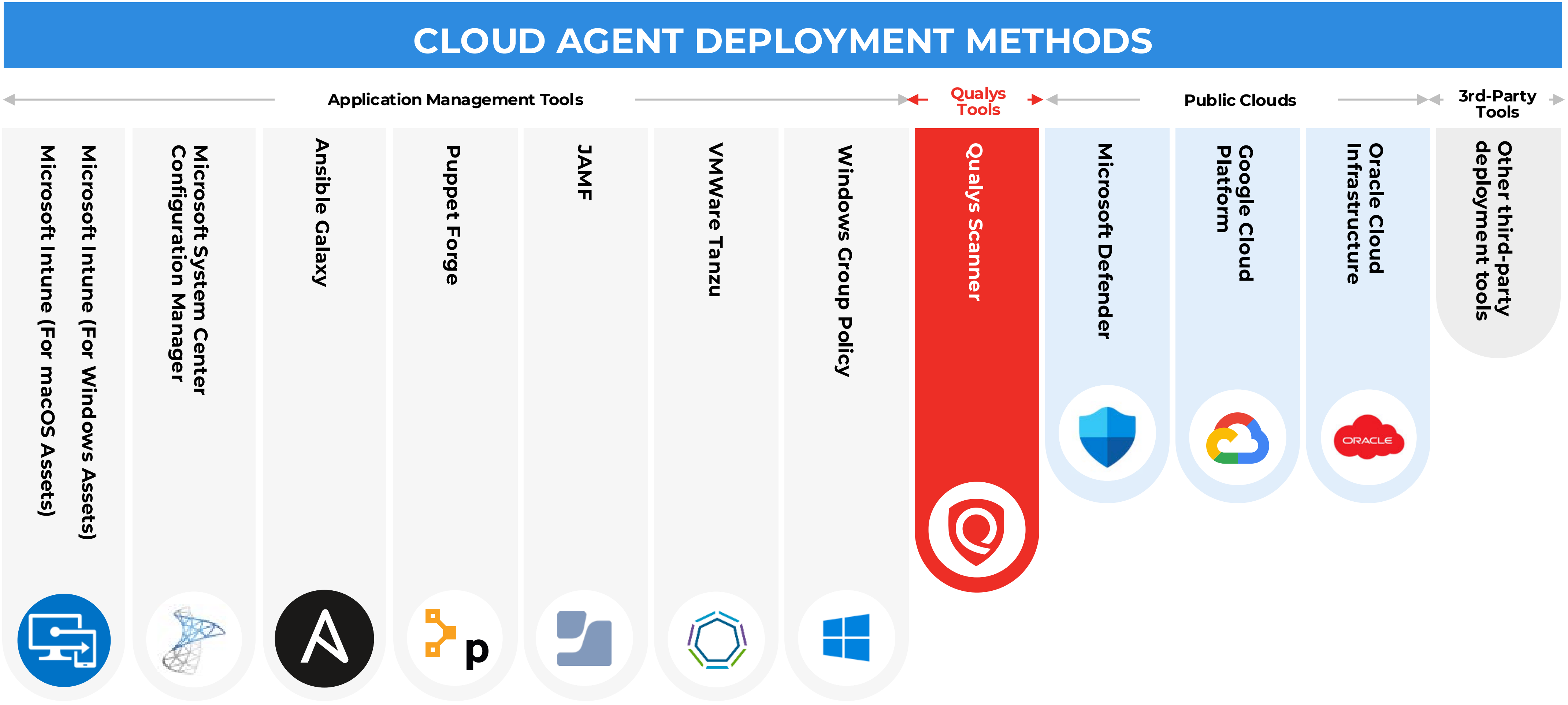
OPERATING SYSTEM	
The CentOS Proj...	22
Microsoft Windo...	16
Microsoft Windo...	15
The CentOS Proj...	15
Microsoft Windo...	11
45 more	

OPEN PORT	
135	213
445	213

NAME	CRITICALITY	TruRisk™ Score	OPERATING SYSTEM	LAST LOGGED IN	LAST SCANNED	SOURCES
ctomcatwi2008r2 10.11.70.93	4	707	Microsoft Windows Server 2008 R2 Enterprise 6.1 SP1 64-Bit	Administrator	VM: 3 hours ago PC: 3 days ago	
vscent76gp516sdw2 10.11.70.162	4	691	The CentOS Project CentOS 7 7.6 1810	root	VM: 4 hours ago PC: 3 days ago	
sdw1 10.11.70.209	4	695	The CentOS Project CentOS 7 7.3 1611	root	VM: 4 hours ago PC: 3 days ago	
vscent76gp516sdw1 10.11.70.161	4	693	The CentOS Project CentOS 7 7.6 1810	root	VM: 4 hours ago PC: 3 days ago	
cdmariadb201 10.11.70.228	4	697	The CentOS Project CentOS 6 6.9	root	VM: 4 hours ago PC: 3 days ago	
cdmssql2017.com2012r2.com... 10.11.70.150	4	698	Microsoft Windows Server 2016 Datacenter 1607 Build 14393.0 64-Bit	Administrator	VM: 4 hours ago PC: 3 days ago	
cdmongodb32e 10.11.70.111	4	698	The CentOS Project CentOS 6 6.6	root	VM: 4 hours ago PC: 3 days ago	
sdw2 10.11.70.210	4	696	The CentOS Project CentOS 7 7.3 1611	root	VM: 4 hours ago PC: 3 days ago	

Cloud Agent Deployment Methods

Qualys Cloud Agent supports various deployment methods to accommodate different systems and varying user requirements. Following are the important deployment methods you can use to deploy Cloud Agents on on-premise and remote assets.



CLOUD AGENT DEPLOYMENT METHODS

Application Management Tools

- Microsoft Intune (For Windows Assets)
- Microsoft Intune (For macOS Assets)
- Microsoft System Center Configuration Manager
- Ansible Galaxy
- Puppet Forge
- JAMF
- VMWare Tanzu
- Windows Group Policy

Qualys Tools

- Qualys Scanner

Public Clouds

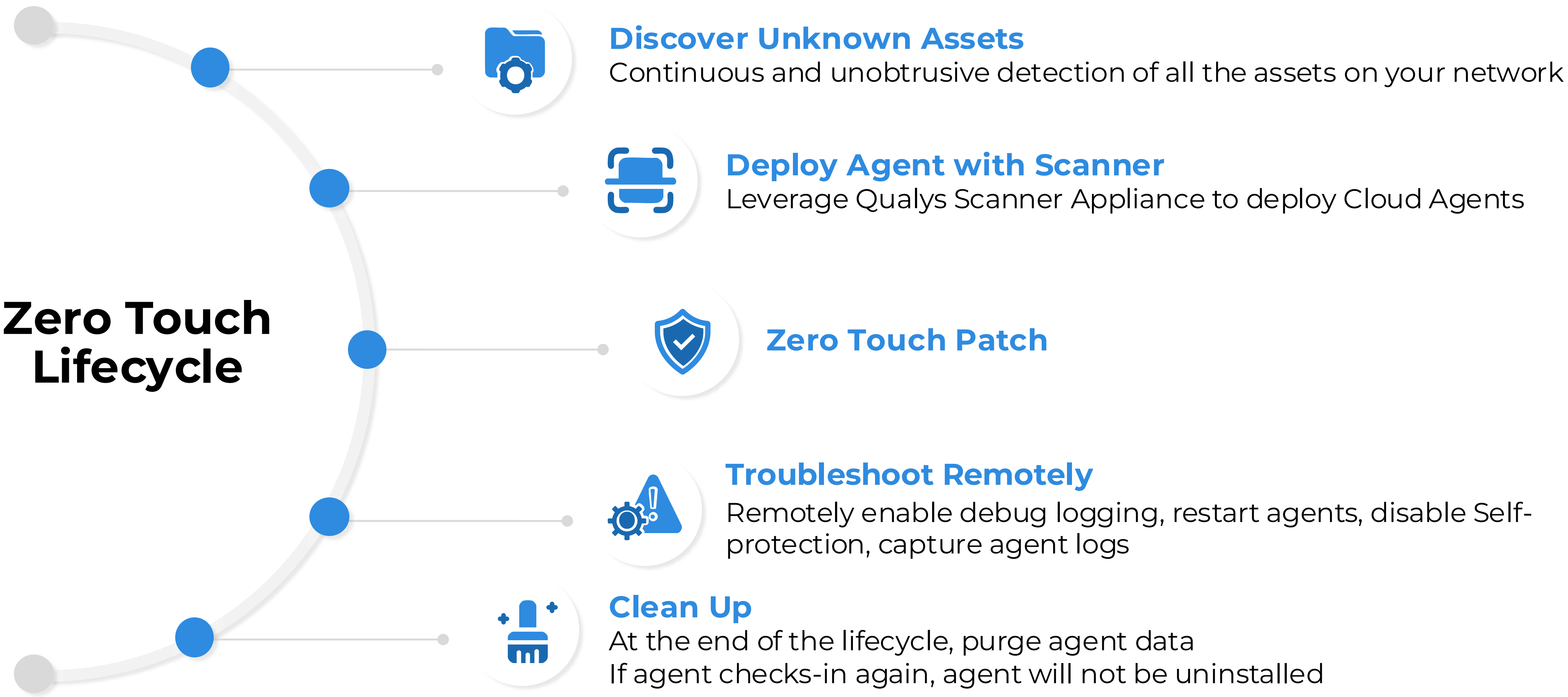
- Microsoft Defender
- Google Cloud Platform
- Oracle Cloud Infrastructure

3rd-Party Tools

- Other third-party deployment tools

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

Zero Touch Patch

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

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

New Capabilities

Manifest Version Control

Flexibility and Stability for Your Critical Environments

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

Control & Flexibility

- Delay updates for critical systems while applying them to non-production assets immediately.

Customizable Profiles

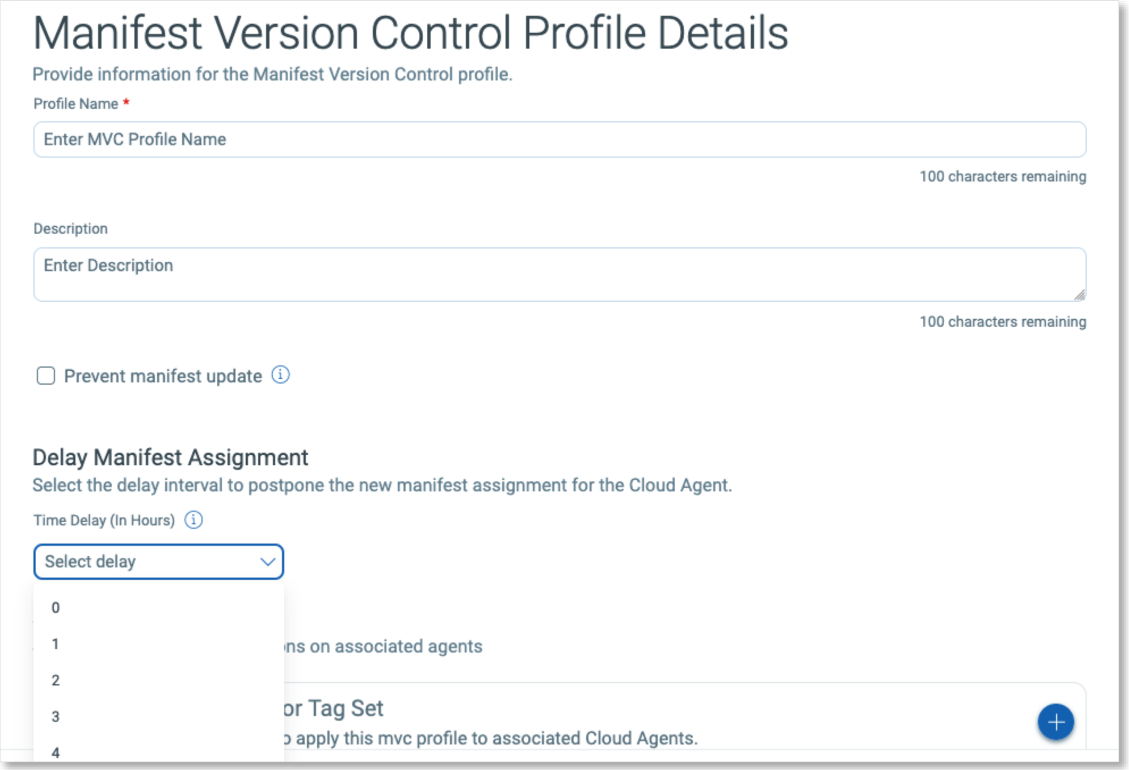
- **Delay:** Delay updates by a set number of hours based on daily manifest changes.

Increased Visibility

- Clear details on each manifest, including QID, and title plus change classification:
  - **High Delta** – Command modifications or introductions.
  - **Low Delta** – Minor changes such as registry keys or file path inclusions.

Incident Management

- Pause updates globally during issues, ensuring stability for critical environments.



Manifest Version Control Profile Details

Provide information for the Manifest Version Control profile.

Profile Name *

Enter MVC Profile Name

100 characters remaining

Description

Enter Description

100 characters remaining

□ Prevent manifest update ⓘ

Delay Manifest Assignment

Select the delay interval to postpone the new manifest assignment for the Cloud Agent.

Time Delay (In Hours) ⓘ

Select delay

0
1
2
3
4

ıns on associated agents

or Tag Set

ɔ apply this mvc profile to associated Cloud Agents.

Join Upcoming Webinar

Access Available. Submit a Support Ticket

Deep Scan: Discover Vulnerabilities in Non-Standard Installations

Detect risks in widely used technologies—no matter where they're installed.

Qualys. ROCon 25 The Risk Operations Conference AMERICAS

Expanded Detection Coverage

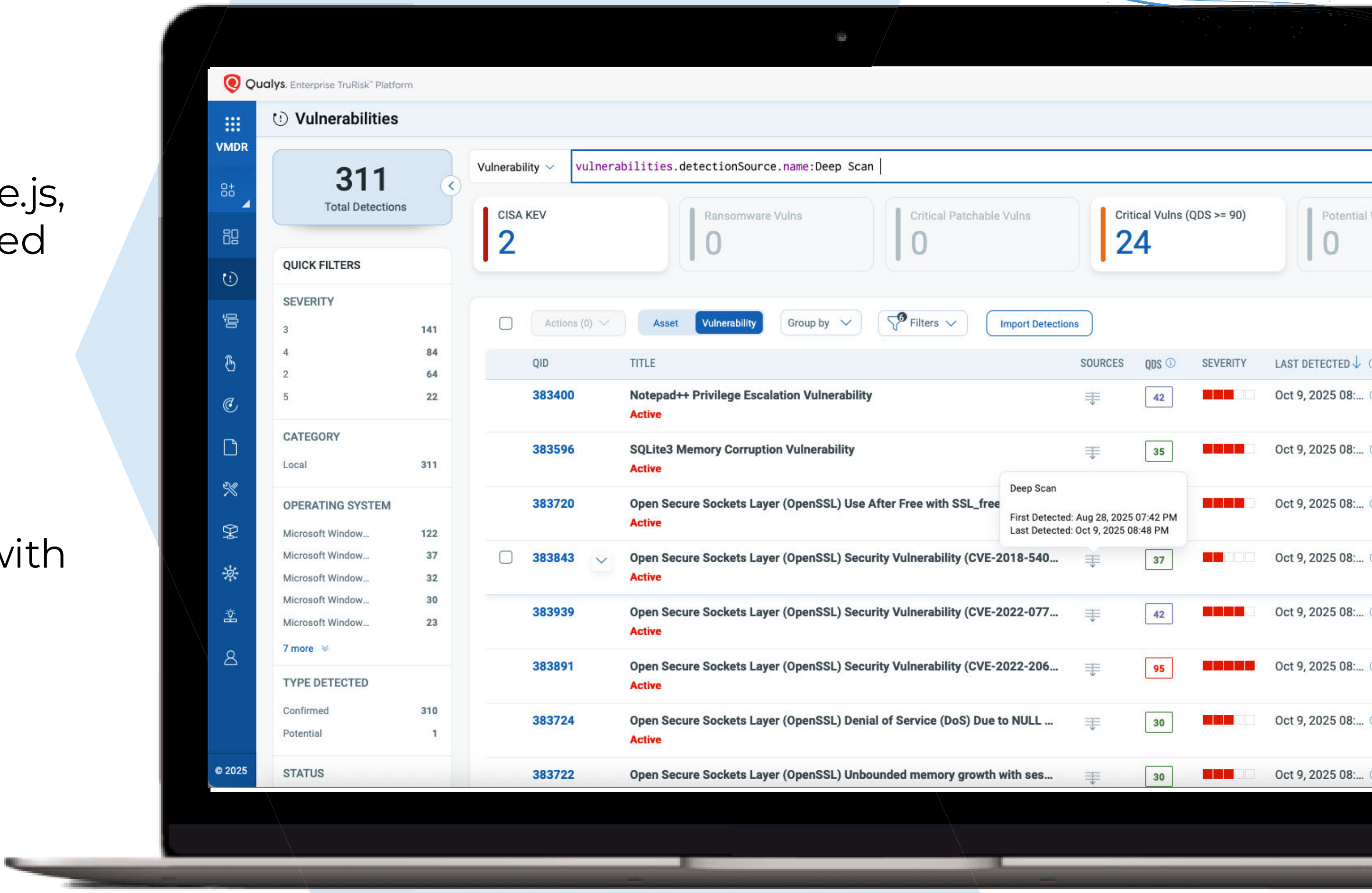
Find vulnerabilities in supported technologies such as OpenSSL, PHP, Node.js, Notepad++, and more—even when installed outside default system directories.

Configurable and Efficient Scanning

Define which folders or drives to scan or exclude, set scan intervals, timeouts, and CPU usage—all to balance performance with deeper coverage.

Integrated Results

View and analyze Deep Scan detections directly within VMDR for consistent remediation workflows.



```
vulnerabilities.detectionSource.name:Deep Scan
```

311 Total Detections

CISA KEV	Ransomware Vulns	Critical Patchable Vulns	Critical Vulns (QDS >= 90)	Potential
2	0	0	24	0

QUICK FILTERS

SEVERITY	
3	141
4	84
2	64
5	22
CATEGORY	
Local	311
OPERATING SYSTEM	
Microsoft Window...	122
Microsoft Window...	37
Microsoft Window...	32
Microsoft Window...	30
Microsoft Window...	23
7 more	
TYPE DETECTED	
Confirmed	310
Potential	1
STATUS	

QID	TITLE	SOURCES	QDS	SEVERITY	LAST DETECTED
383400	Notepad++ Privilege Escalation Vulnerability Active		42	■■■□□	Oct 9, 2025 08:...
383596	SQLite3 Memory Corruption Vulnerability Active		35	■■■■□	Oct 9, 2025 08:...
383720	Open Secure Sockets Layer (OpenSSL) Use After Free with SSL_free Active			■■■■□	Oct 9, 2025 08:...
383843	Open Secure Sockets Layer (OpenSSL) Security Vulnerability (CVE-2018-540... Active		37	■■□□□	Oct 9, 2025 08:...
383939	Open Secure Sockets Layer (OpenSSL) Security Vulnerability (CVE-2022-077... Active		42	■■■■□	Oct 9, 2025 08:...
383891	Open Secure Sockets Layer (OpenSSL) Security Vulnerability (CVE-2022-206... Active		95	■■■■■	Oct 9, 2025 08:...
383724	Open Secure Sockets Layer (OpenSSL) Denial of Service (DoS) Due to NULL ... Active		30	■■■□□	Oct 9, 2025 08:...
383722	Open Secure Sockets Layer (OpenSSL) Unbounded memory growth with ses...		30	■■■□□	Oct 9, 2025 08:...

Deep Scan

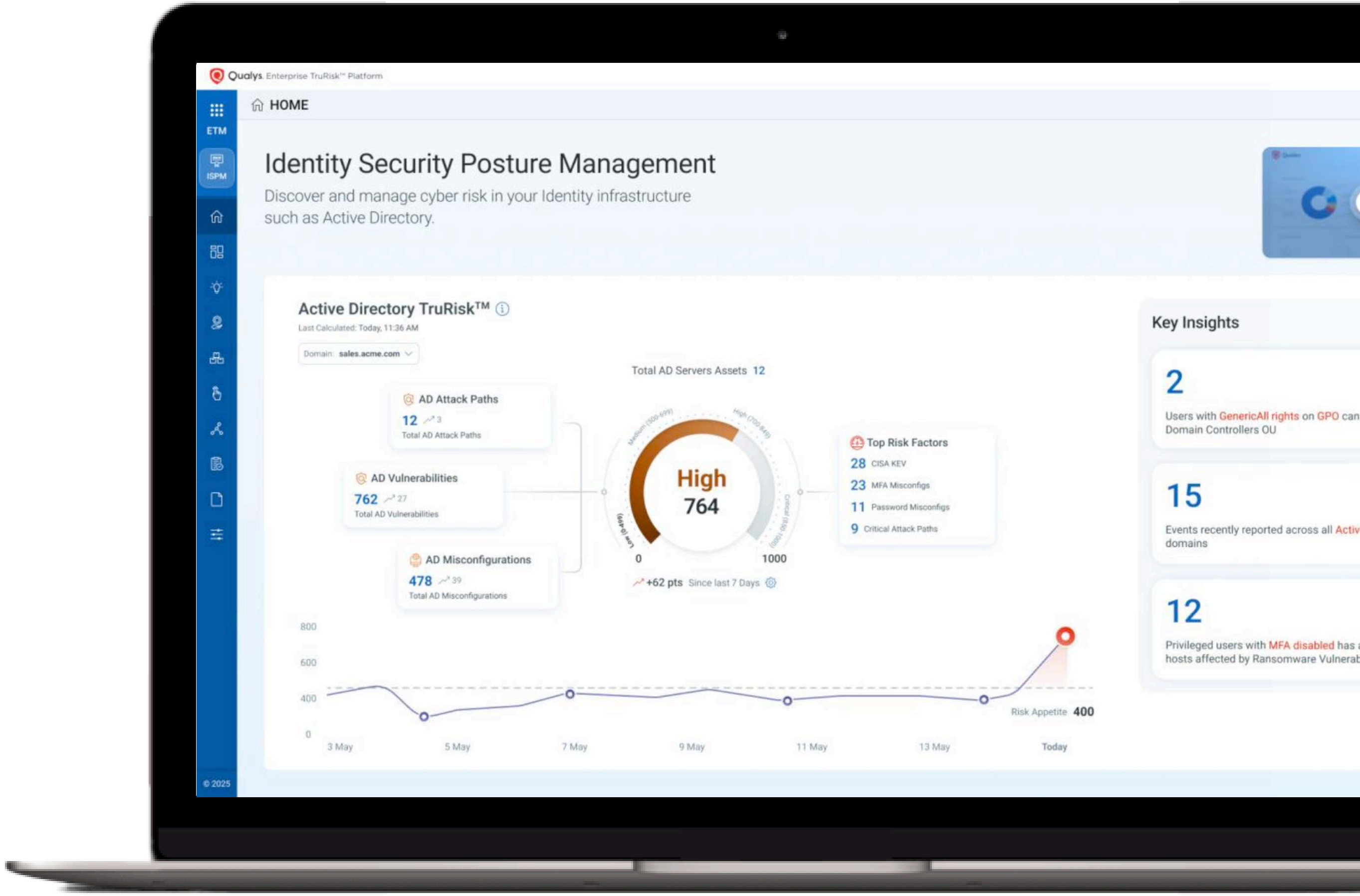
First Detected: Aug 28, 2025 07:42 PM
Last Detected: Oct 9, 2025 08:48 PM

Access Available. Submit a Support Ticket

De-risk human and machine identities for reduced identity-driven attack surface

Built inside Qualys ETM, **Qualys ETM Identity** consolidates identity security and active directory posture into **a single prioritized risk view** to **measure, communicate, and eliminate identity risks** across your entire identity attack surface.

- **Measure** identity posture with full inventory of identities across AD, Entra ID, IDaaS,/IdPs.
- **Communicate** identity risks in a single TruRisk^{TM} score to prioritize responses.
- **Eliminate** high-risk attack paths with policy enforcement, automated remediation.



Qualys. Enterprise TruRisk™ Platform

HOME

Identity Security Posture Management

Discover and manage cyber risk in your Identity infrastructure such as Active Directory.

Active Directory TruRisk™

Last Calculated: Today, 11:36 AM

Domain: sales.acme.com

Total AD Servers Assets 12

AD Attack Paths: 12 (3) Total AD Attack Paths

AD Vulnerabilities: 762 (27) Total AD Vulnerabilities

AD Misconfigurations: 478 (39) Total AD Misconfigurations

High 764

+62 pts Since last 7 Days

Top Risk Factors

- 28 CISA KEV
- 23 MFA Misconfigs
- 11 Password Misconfigs
- 9 Critical Attack Paths

Key Insights

2 Users with GenericAll rights on GPO can Domain Controllers OU

15 Events recently reported across all Activ domains

12 Privileged users with MFA disabled has hosts affected by Ransomware Vulnerab

Access Available. Contact TAM

Unified View Across All Sensor Types

Correlate Scanner Data with Agents and Other Sensors for Complete Coverage

Reduce Duplication

Prevent multiple records for the same asset when data comes from different sensors.

Flexible Correlation Rules

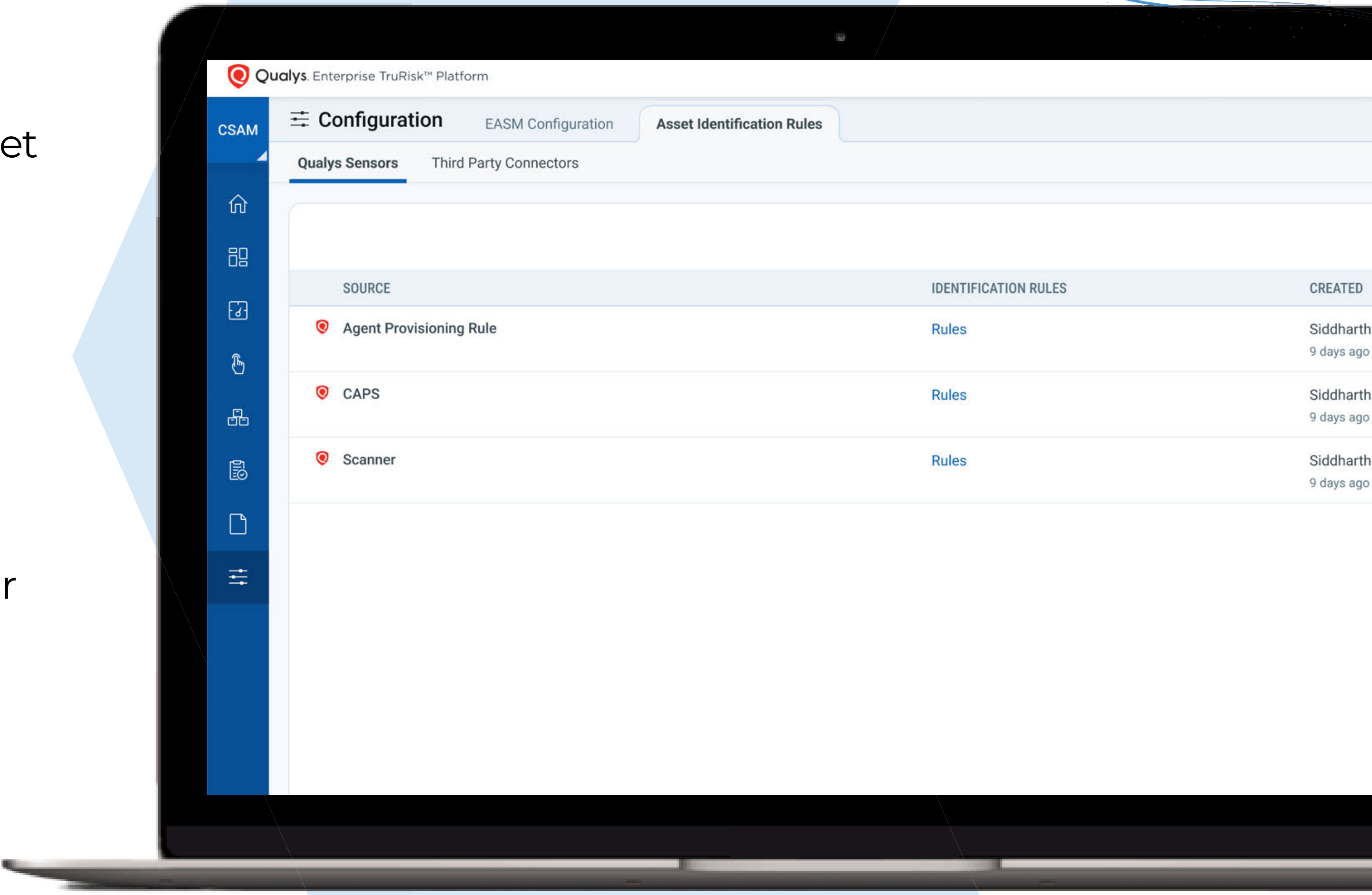
Define how assets are matched using attributes like MAC address, hostname, or serial number.

Comprehensive Visibility

Combine scanner, agent, and other sensor data into a single, accurate asset record.

Stronger Insights

Improve detection accuracy, reporting consistency, and overall security posture.



SOURCE	IDENTIFICATION RULES	CREATED
Agent Provisioning Rule	Rules	Siddharth 9 days ago
CAPS	Rules	Siddharth 9 days ago
Scanner	Rules	Siddharth 9 days ago

Beta Available End of 2025

Qualys. ROCon 25 The Risk Operations Conference AMERICAS

Innovations

Peer-to-Peer Caching

Optimize Bandwidth and Speed by Allowing Agents to Share Resources Locally

Accelerate Patch Deployment

Agents can download and share patch resources among themselves, reducing download times.

Reduce Bandwidth Usage

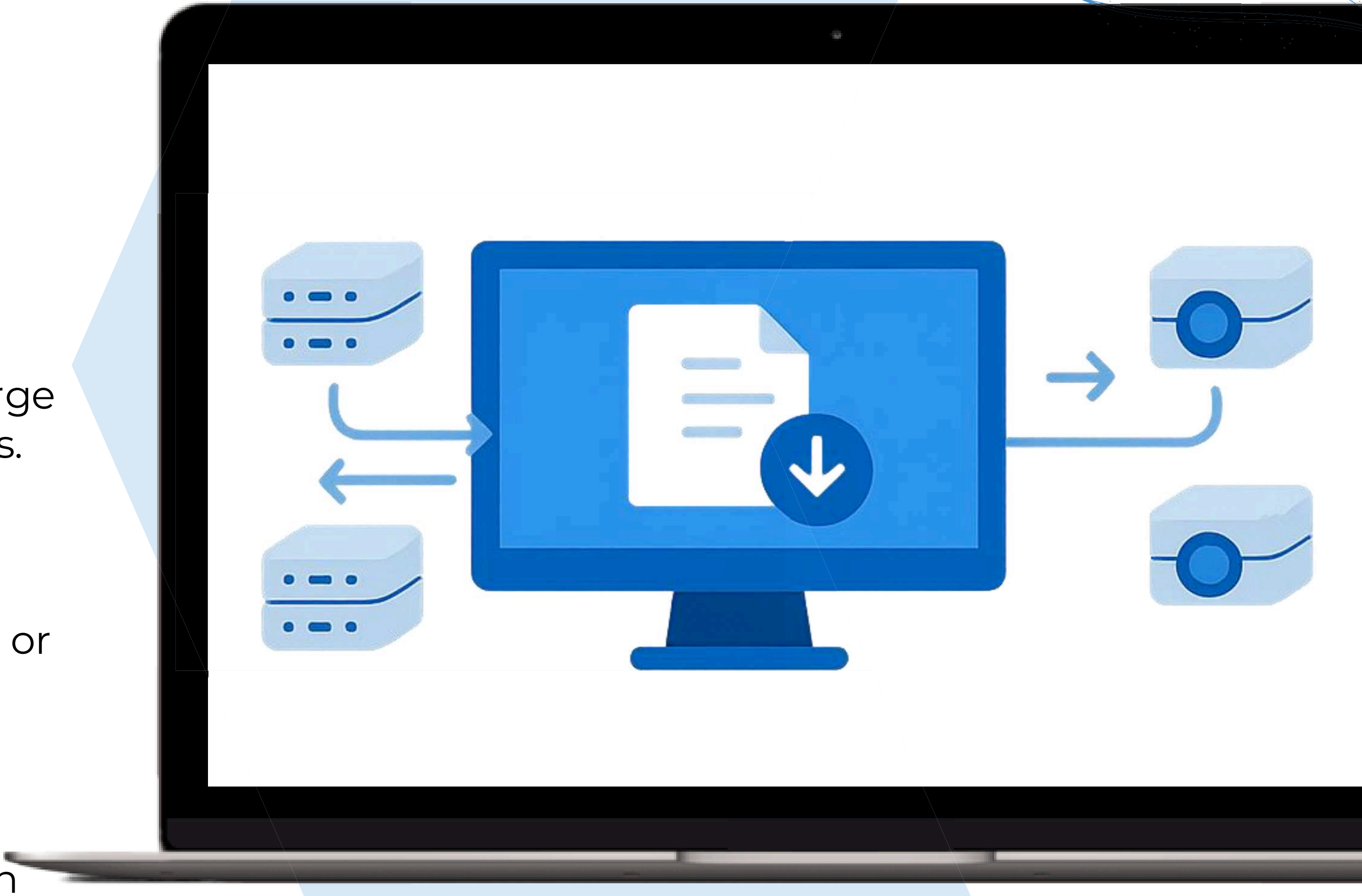
Minimize redundant downloads across large environments, especially for big patch files.

Granular Control

Define which groups of agents can share resources and limit sharing by geography or network boundaries.

Built-In Intelligence

Assets automatically determine when to share locally or download directly when on VPN or remote networks.



Coming 2026

Full Coverage with Agent-Based Remote Detections

Achieve Complete Visibility Without a Scanner Appliance

Eliminate the Need for Two Sensor Types

Prevent multiple records for the same asset when data comes from different sensors.

Simplify Operations

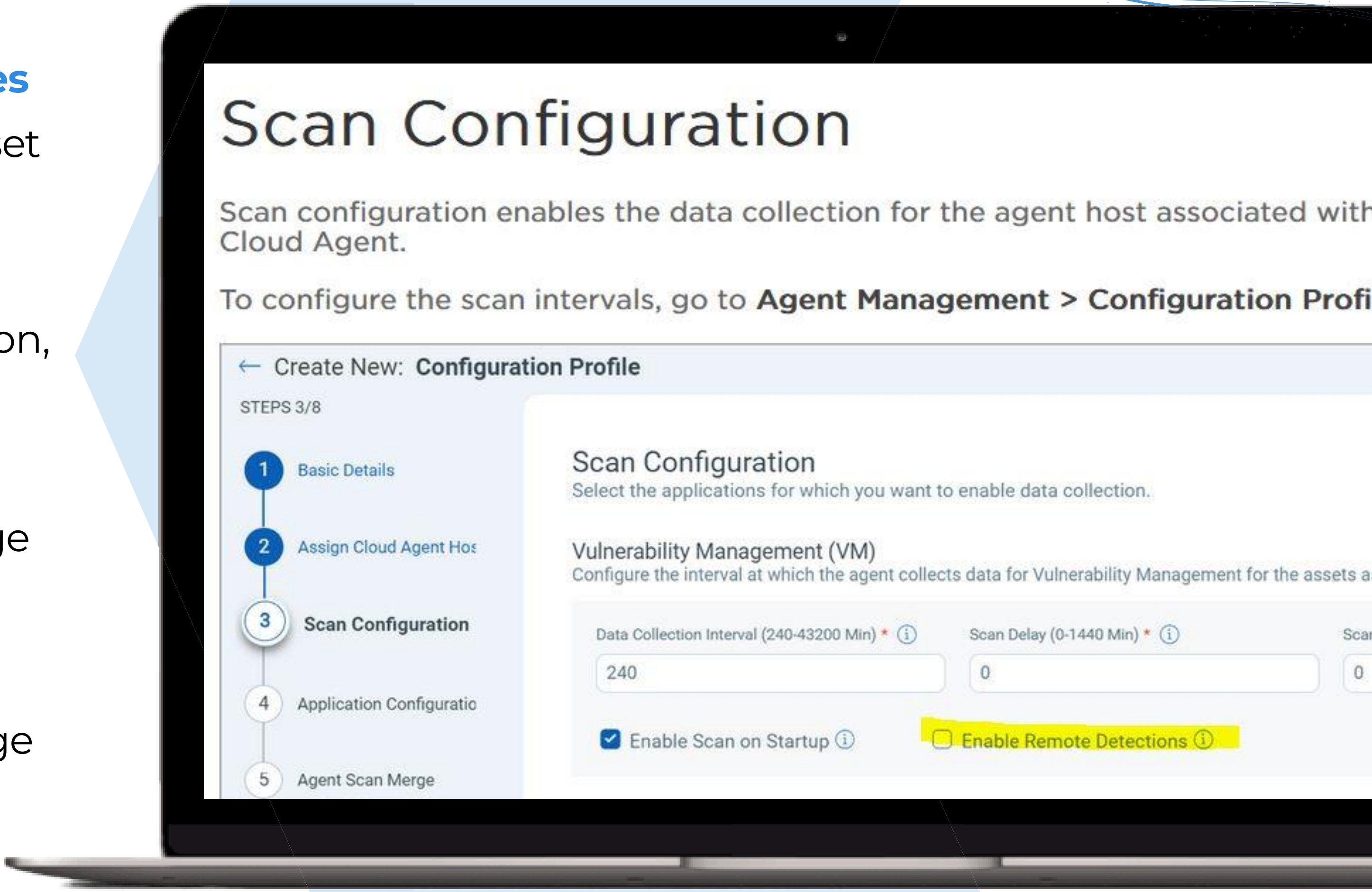
No more managing scanner authentication, scheduling, or network access.

Reduce Network Load

Fewer scans mean lower bandwidth usage and faster assessments.

Avoid Data Gaps and Overlap

End issues like duplicate detections, merge complexity, and detection flip-flops.



Scan Configuration

Scan configuration enables the data collection for the agent host associated with Cloud Agent.

To configure the scan intervals, go to **Agent Management > Configuration Profi**

← Create New: **Configuration Profile**

STEPS 3/8

1 Basic Details
2 Assign Cloud Agent Hos
3 **Scan Configuration**
4 Application Configuratio
5 Agent Scan Merge

Scan Configuration
Select the applications for which you want to enable data collection.

Vulnerability Management (VM)
Configure the interval at which the agent collects data for Vulnerability Management for the assets a

Data Collection Interval (240-43200 Min) * ⓘ: 240
Scan Delay (0-1440 Min) * ⓘ: 0
Sca: 0

☑ Enable Scan on Startup ⓘ
□ Enable Remote Detections ⓘ

POC Available. Contact TAM

Qualys.

ROCon 25

The Risk Operations Conference

AMERICAS

Thank You!

Qualys®

ROCon 25

The Risk Operations Conference

AMERICAS

October 15, 2025

The Risk Operations Conference

Qualys Cloud Agent and Patch Management

Ali Zaher CISSP, CISM, PMP

Cyber Security Vulnerability Manager, SLB

Ali Zaher

CISSP, CISM, PMP

Cyber Security Vulnerability Manager

22+ years with SLB

Expertise spans

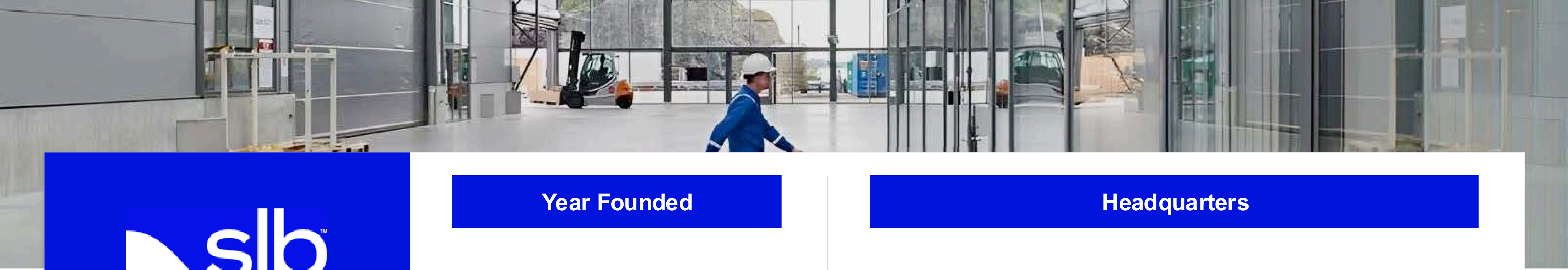
Vulnerability Management

Cyber Security Performance & Metrics

Large-scale Data Center Infrastructure Deployment

B.Sc. Degree in Computer Science, American University of Beirut, and maintains globally recognized certifications including **CISSP, CISM, and PMP**

Committed to advancing SLB's security posture and ensuring the organization remains protected, compliant, and resilient against evolving cyber threats.



Year Founded

1926

Headquarters

Houston, TX

SLB, formerly known as Schlumberger, is a global technology company that provides advanced solutions for the energy industry, focusing on decarbonizing fossil fuels and developing scalable new energy technologies.

With a presence in over **100 countries**, SLB offers services in reservoir characterization, drilling, production, and processing, utilizing digital and AI-powered tools to enhance operational efficiency.

Agenda

Cloud Connectors, Agent Capabilities, and Patch Management Benefits

1 Understanding Cloud Connectors

2 **Agent Capabilities:**
Enhancing Security Posture

3 **Patch Management:**
A Critical Component

4 Integrating Cloud Connectors and Agents for Optimal Performance

5 **Conclusion:**
Key Takeaways and Future Directions

Qualys Deployment— Scale, Coverage & Platform

Deployment footprint, agent coverage, and platform diversity within our enterprise environment

Global Deployment & Business Scope

Deployment: Cloud & On-Prem

OS Platforms Covered

Client and Server Coverage

Understanding Qualys Cloud Connectors

Definition and purpose of Cloud connectors

Cloud Connectors bridge Qualys & multi-cloud environments, extending visibility to cloud assets while automatically tracking active VMs and removing inactive ones to maintain an accurate inventory

Integration with existing systems

Integrates Qualys with existing IT systems, ensuring consistent security across on-premises and cloud environments.

Real-time data access and analysis

Cloud Connectors provide real-time security data for faster analysis and response to emerging threats and vulnerabilities.

Agent Capabilities: Enhancing Security Posture

Overview of Agent functionalities:

Qualys Agents continuously monitor and assess endpoints, collecting essential security data to ensure compliance with organizational policies.

Benefits of deploying Agents:

Agents enhance endpoint visibility, enable rapid vulnerability detection, and simplify compliance reporting, strengthening overall security posture.

Case studies of successful implementations:

Organizations using Qualys Agents report stronger security posture and fewer incidents through continuous visibility and proactive risk mitigation.

Patch Management: A Critical Component

Definition and importance of Patch Management

Patch Management involves the systematic process of managing updates for software applications and technologies, crucial for mitigating vulnerabilities and ensuring system integrity.

How it fits into the security framework

Effective Patch Management is integral to a comprehensive security framework, as it addresses known vulnerabilities and reduces the risk of exploitation by malicious actors.

Statistics on vulnerabilities and patching

Research indicates that a significant percentage of security breaches are due to unpatched vulnerabilities, underscoring the critical need for robust Patch Management practices.

Benefits of Using Patch Management

Reduction in security incidents, Improved compliance and reporting, and resource optimization

Reduction in security incidents

Improved compliance and reporting

Resource optimization

Cloud Agent Does It All

Imagine needing a separate agent for every task — now, imagine not needing that

Unified Security & Compliance

Real-Time Inventory & Detection

Lightweight & Non-Intrusive

Supports Multiple Use Cases

Conclusion: Key Takeaways and Future Directions

1 **Key insights:**

The integration of solutions, including Cloud connectors, Agents, and Patch Management, is essential for enhancing security in modern environments.

2 **Future trends in security management:**

As cyber threats evolve, organizations must adopt proactive security measures, including automation and real-time monitoring, to stay ahead.

Thank You!

October 15, 2025

The Risk Operations Conference

Qualys Cloud Agent and Patch Management

Ali Zaher **CISSP, CISM, PMP**

Cyber Security Vulnerability Manager, SLB

Ali Zaher

CISSP, CISM, PMP

Cyber Security Vulnerability Manager

22+ years with SLB

Expertise spans

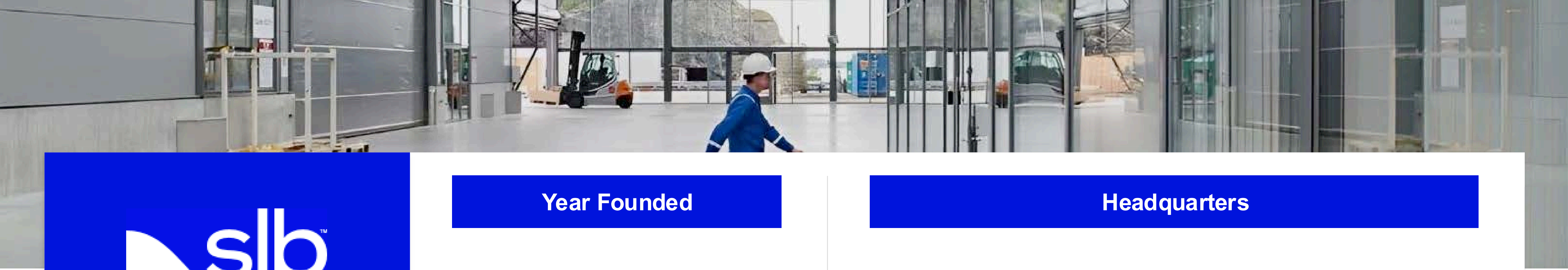
Vulnerability Management

Cyber Security Performance & Metrics

Large-scale Data Center Infrastructure Deployment

B.Sc. Degree in Computer Science, American University of Beirut, and maintains globally recognized certifications including **CISSP, CISM, and PMP**

Committed to advancing SLB's security posture and ensuring the organization remains protected, compliant, and resilient against evolving cyber threats.



Year Founded

1926

Headquarters

Houston, TX

SLB, formerly known as Schlumberger, is a global technology company that provides advanced solutions for the energy industry, focusing on decarbonizing fossil fuels and developing scalable new energy technologies.

With a presence in over **100 countries**, SLB offers services in reservoir characterization, drilling, production, and processing, utilizing digital and AI-powered tools to enhance operational efficiency.

Agenda

Cloud Connectors, Agent Capabilities, and Patch Management Benefits

1 Understanding Cloud Connectors

2 **Agent Capabilities:**
Enhancing Security Posture

3 **Patch Management:**
A Critical Component

4 Integrating Cloud Connectors and Agents for Optimal Performance

5 **Conclusion:**
Key Takeaways and Future Directions

Qualys Deployment— Scale, Coverage & Platform

Deployment footprint, agent coverage, and platform diversity within our enterprise environment

Global Deployment & Business Scope

Deployment: Cloud & On-Prem

OS Platforms Covered

Client and Server Coverage

Understanding Qualys Cloud Connectors

Definition and purpose of Cloud connectors

Cloud Connectors bridge Qualys & multi-cloud environments, extending visibility to cloud assets while automatically tracking active VMs and removing inactive ones to maintain an accurate inventory

Integration with existing systems

Integrates Qualys with existing IT systems, ensuring consistent security across on-premises and cloud environments.

Real-time data access and analysis

Cloud Connectors provide real-time security data for faster analysis and response to emerging threats and vulnerabilities.

Agent Capabilities: Enhancing Security Posture

Overview of Agent functionalities:

Qualys Agents continuously monitor and assess endpoints, collecting essential security data to ensure compliance with organizational policies.

Benefits of deploying Agents:

Agents enhance endpoint visibility, enable rapid vulnerability detection, and simplify compliance reporting, strengthening overall security posture.

Case studies of successful implementations:

Organizations using Qualys Agents report stronger security posture and fewer incidents through continuous visibility and proactive risk mitigation.

Patch Management: A Critical Component

Definition and importance of Patch Management

Patch Management involves the systematic process of managing updates for software applications and technologies, crucial for mitigating vulnerabilities and ensuring system integrity.

How it fits into the security framework

Effective Patch Management is integral to a comprehensive security framework, as it addresses known vulnerabilities and reduces the risk of exploitation by malicious actors.

Statistics on vulnerabilities and patching

Research indicates that a significant percentage of security breaches are due to unpatched vulnerabilities, underscoring the critical need for robust Patch Management practices.

Benefits of Using Patch Management

Reduction in security incidents, Improved compliance and reporting, and resource optimization

Reduction in security incidents

Improved compliance and reporting

Resource optimization

Cloud Agent Does It All

Imagine needing a separate agent for every task — now, imagine not needing that

Unified Security & Compliance

Real-Time Inventory & Detection

Lightweight & Non-Intrusive

Supports Multiple Use Cases

Conclusion: Key Takeaways and Future Directions

1 **Key insights:**

The integration of solutions, including Cloud connectors, Agents, and Patch Management, is essential for enhancing security in modern environments.

2 **Future trends in security management:**

As cyber threats evolve, organizations must adopt proactive security measures, including automation and real-time monitoring, to stay ahead.

Thank You!

Qualys

ROCon 25

The Risk Operations Conference

AMERICAS