Qualys.

ROCon 25

The Risk Operations Conference

AMERICAS

Build a Strategic Risk Foundation: Turn VMDR Best Practices into Impact

Prepare your organization for the next evolution in cyber risk management

Russ Sanderlin

Director, Subject Matter Expert
VMDR Product Team

VMDR Best Practices

Breadth of Coverage

Inventory assets across perimeter, on premise, public cloud, OT, Mobile, and IoT

Vulnerability Scanning

Build confidence in results with continuous assessments and accurate results with authentication

Prioritization

Too many vulnerabilities can be difficult to prioritize and remediate with spreadsheets

Secure by Design

Scan new assets with VM and SCA to shrink the attack surface and stop vulnerabilities before deployment.

Monitor Subscription Health

Maintain the integrity of VMDR to ensure consistent coverage and accuracy

Breadth of Coverage

External Scanner Appliances

Achieve **and outside-in** visibility of all internet-facing assets representing exposures with the most inherent risk.

Cloud Agents

Real-time visibility, continuous monitoring, and enables features like Eliminate, EDR, FIM, and CAPS.

Scanner Appliances

Achieve a complete attacker's point of view for Cloud Agent enabled assets and assess network devices

Cloud Connectors

Inventory workload data from public cloud providers

Passive Sensors

Identify any gaps in coverage with network passive senor appliances or Cloud Agent enabled passive sensors

Asset Context

Integrate with CMDBs to add business context to identify mission critical assets

Active Sensors

Agents Remote Scanners

Passive Sensors

NPS CAPS

Cloud Connectors

aws ORACLE

Infra Connectors

Active Directory servicenow vmware bmc Webhook

VM Scanning and Maintenance

Continuous Vulnerability Assessments

While Cloud Agents check in approximately every 4 hours, traditional external and internal scans should occur at least weekly

Use Authentication

For the most accurate results, use authentication where possible to achieve maximum depth of coverage

Asset Merging

Use asset merging to consolidate multiple detections on multi-homed assets and assets that are using Cloud Agents

Purge Stale Assets

Remove data for decommissioned, terminated, or deleted assets from your subscription

Internal Firewall Configurations

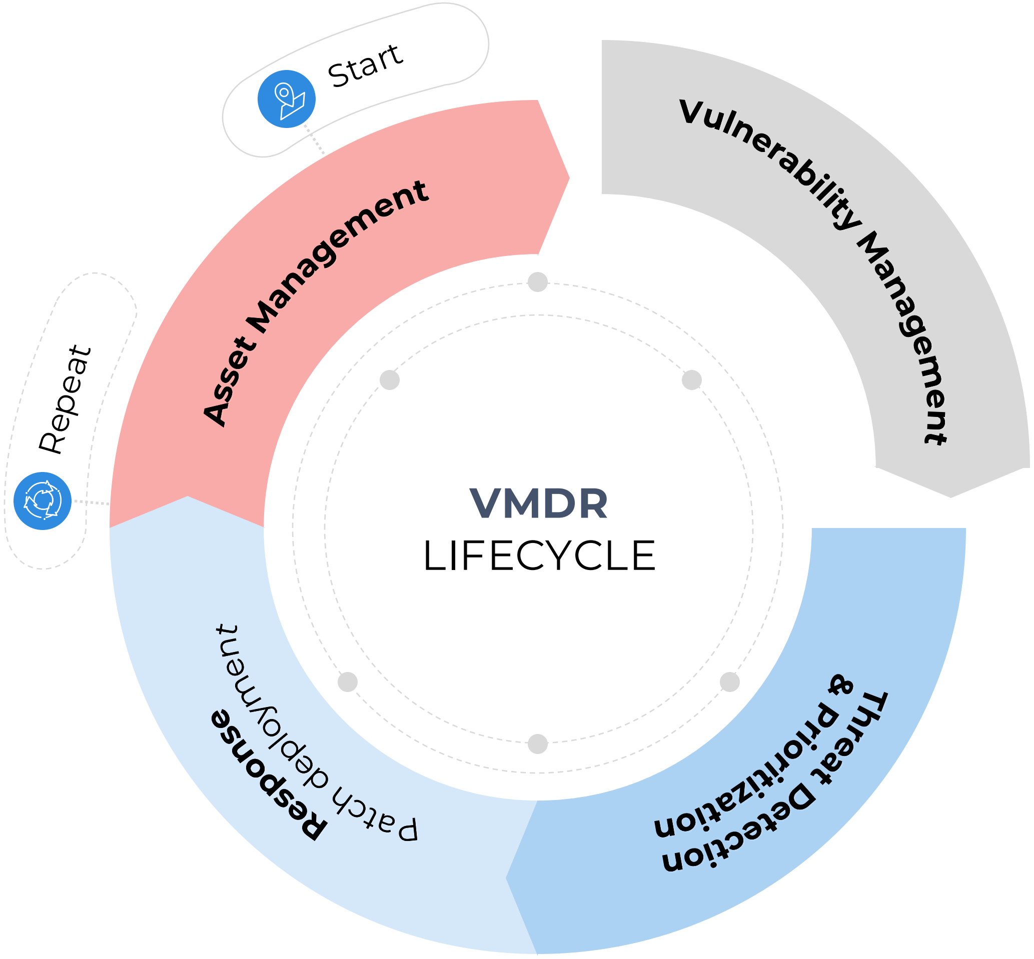
Scanner appliances should have full TCP/UDP access to target assets for a thorough analysis

Full Port Scan on External Assets

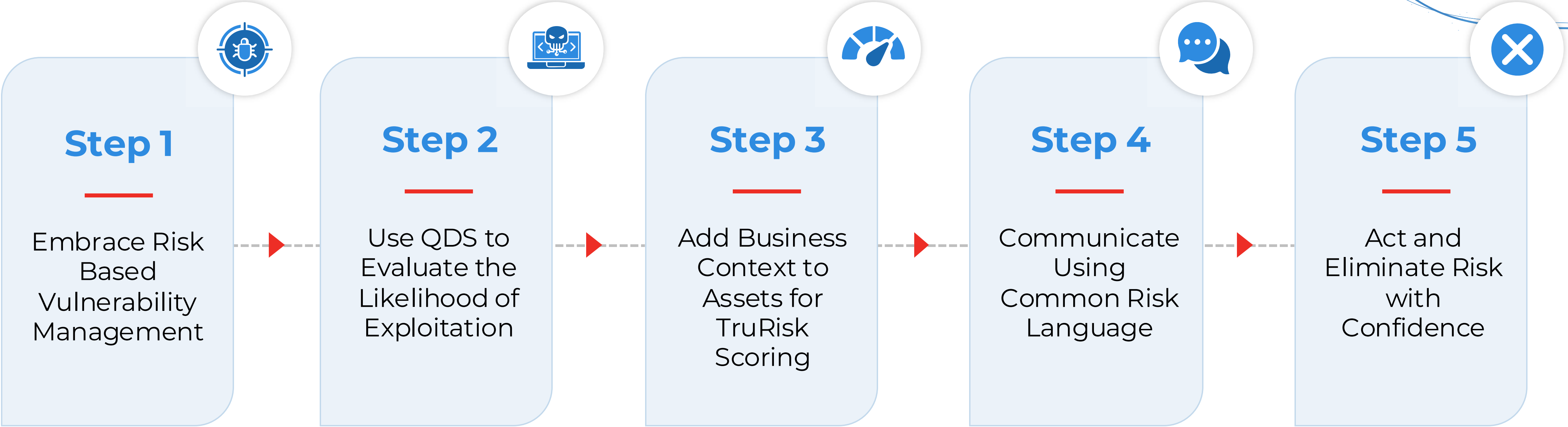
Simulate an external attacker's perspective to uncover and close unintended exposures.

Assign Tags to Assets

Tagging is great for scanning and critical for reporting



Prioritize with TruRisk™



Step 1

Embrace Risk Based Vulnerability Management

Step 2

Use QDS to Evaluate the Likelihood of Exploitation

Step 3

Add Business Context to Assets for TruRisk Scoring

Step 4

Communicate Using Common Risk Language

Step 5

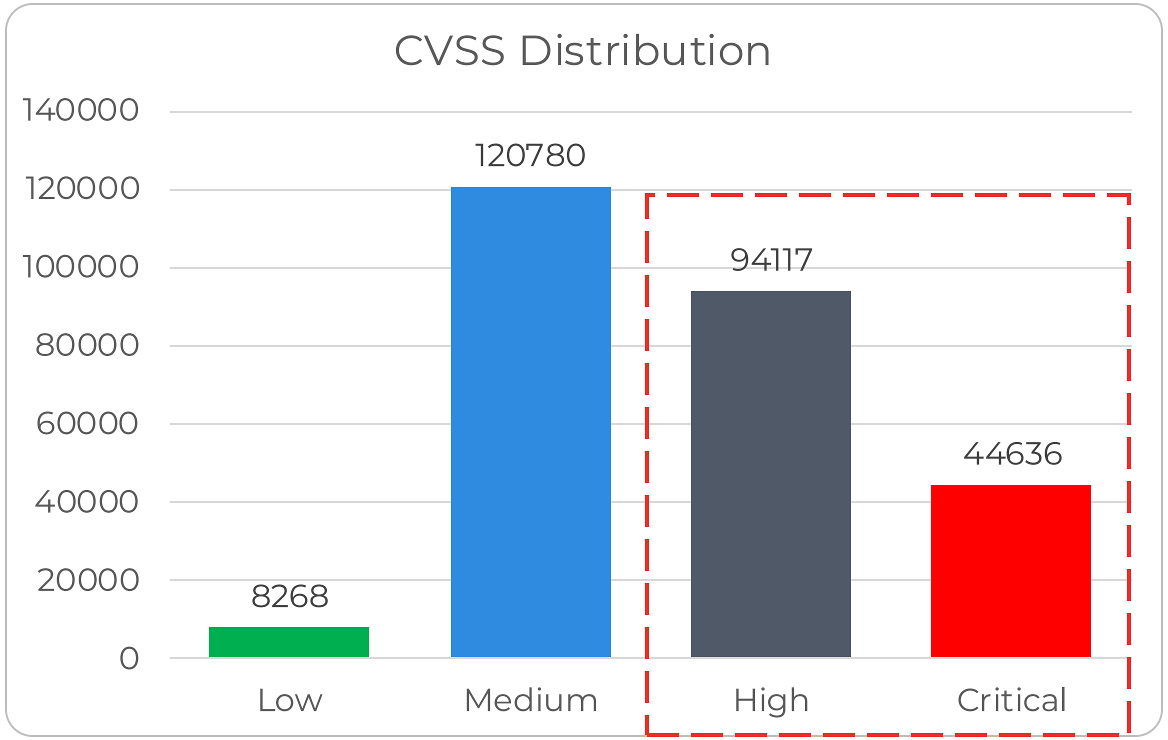
Act and Eliminate Risk with Confidence

Risk = Likelihood x Impact

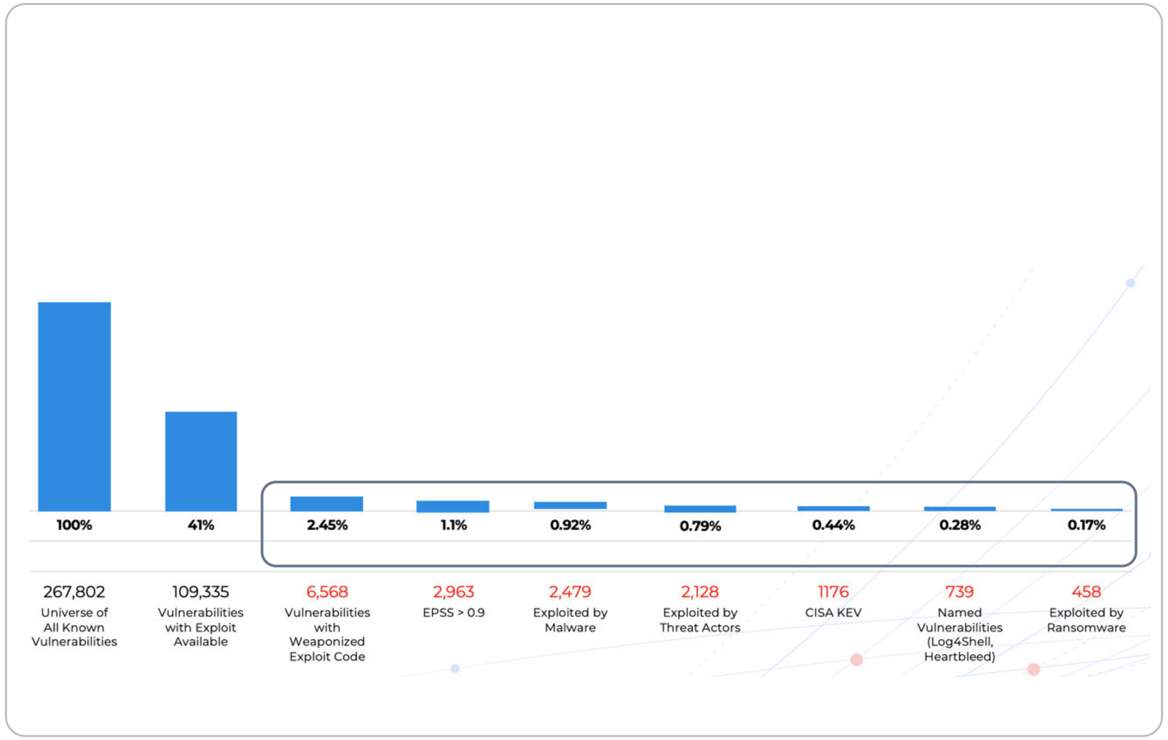
TruRisk™ = QDS x ACS

Too Many Vulns Have Been Deemed 'Critical'

52% are rated high or critical by CVSS

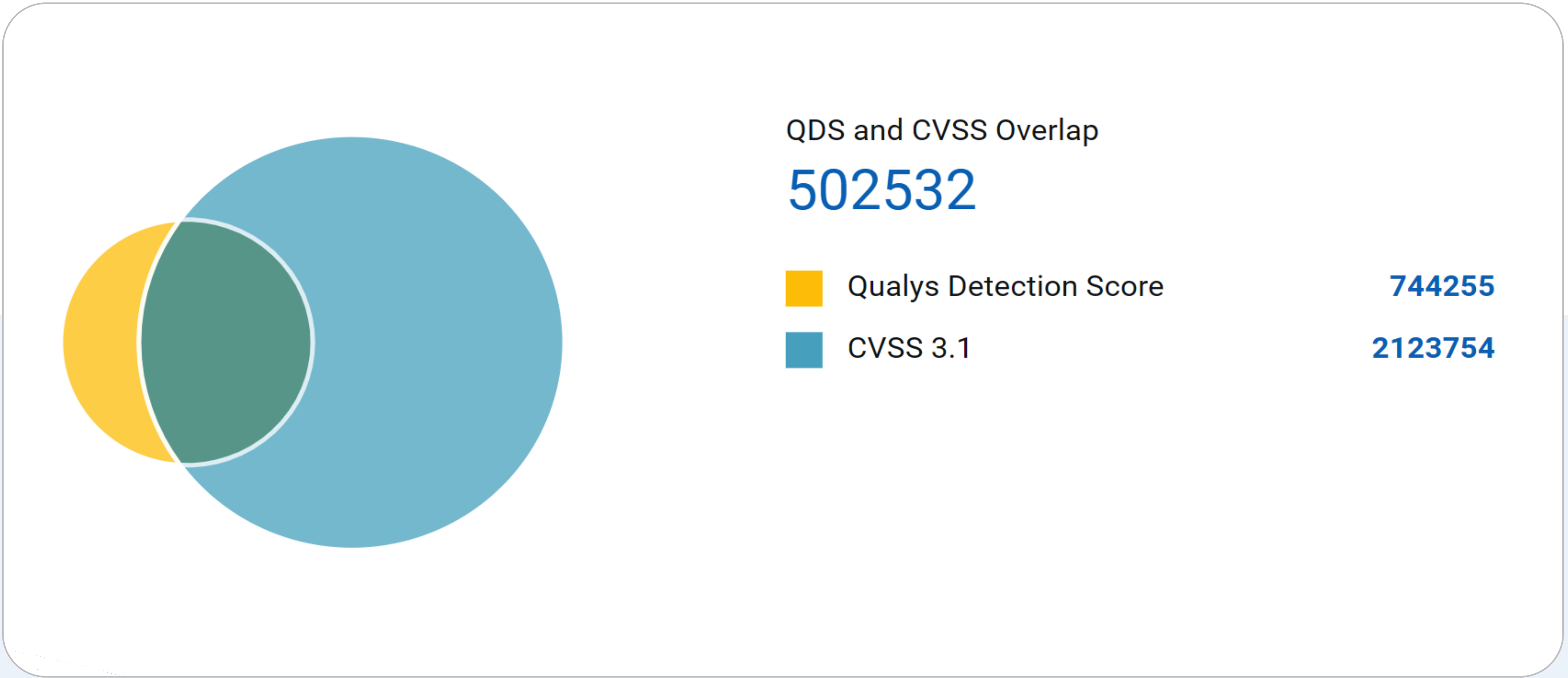


<6% of Vulnerabilities Contribute to material risk



Source: NVD

Use QDS to Quantify the Likelihood of Exploitation



QDS and CVSS Overlap

502532

🟨	Qualys Detection Score	744255
🟦	CVSS 3.1	2123754

Use ACS when Assigning Tags

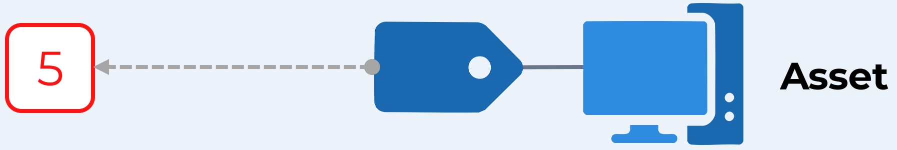
TruRisk

=

QDS
(Likelihood)

X

ACS
(Impact)



ACS	Criticality	Financial Impact	Reputational
5	Severe Impact	5,000,000+ / Day	Brand Crisis
4	Major Impact	1,000,000-4,999,999/Day	Public Fallout
3	Moderate Impact	500,000-999,999/Day	Heightened Scrutiny
2	Minor Impact	10,000-499,999/Day	Emerging Concern
1	Negligible Impact	0-9,999/Day	Stable Reputation

Shift Left with Assessments and Hardening

Reduce Attack Surface

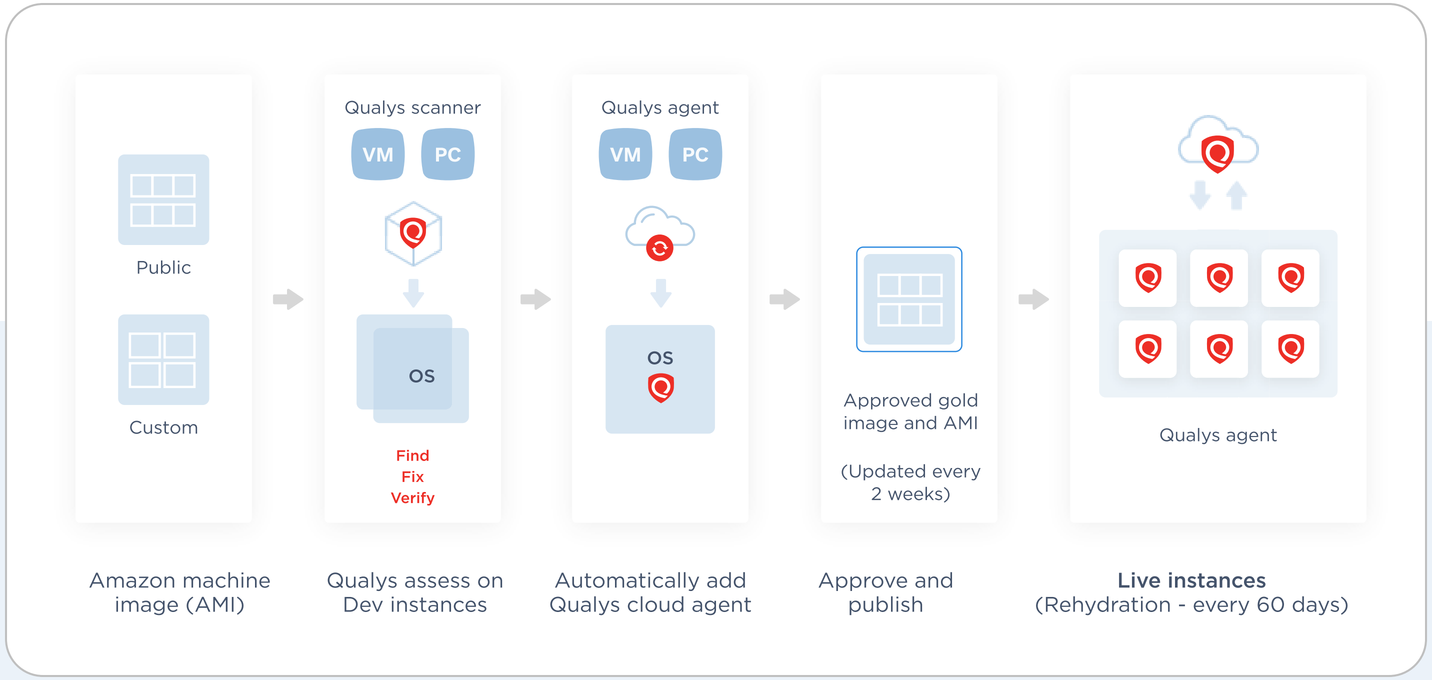
Reduce your attack surface to close entry points like open ports, unused software, unused services, and misconfigurations.

Integrate Scanning in Image Pipelines

Embed detection early by hardening system images before deployment to prevent vulnerabilities from reaching production.

Drift Detection

Continuously monitor and remediate configuration drift to maintain compliance and reduce risk over time

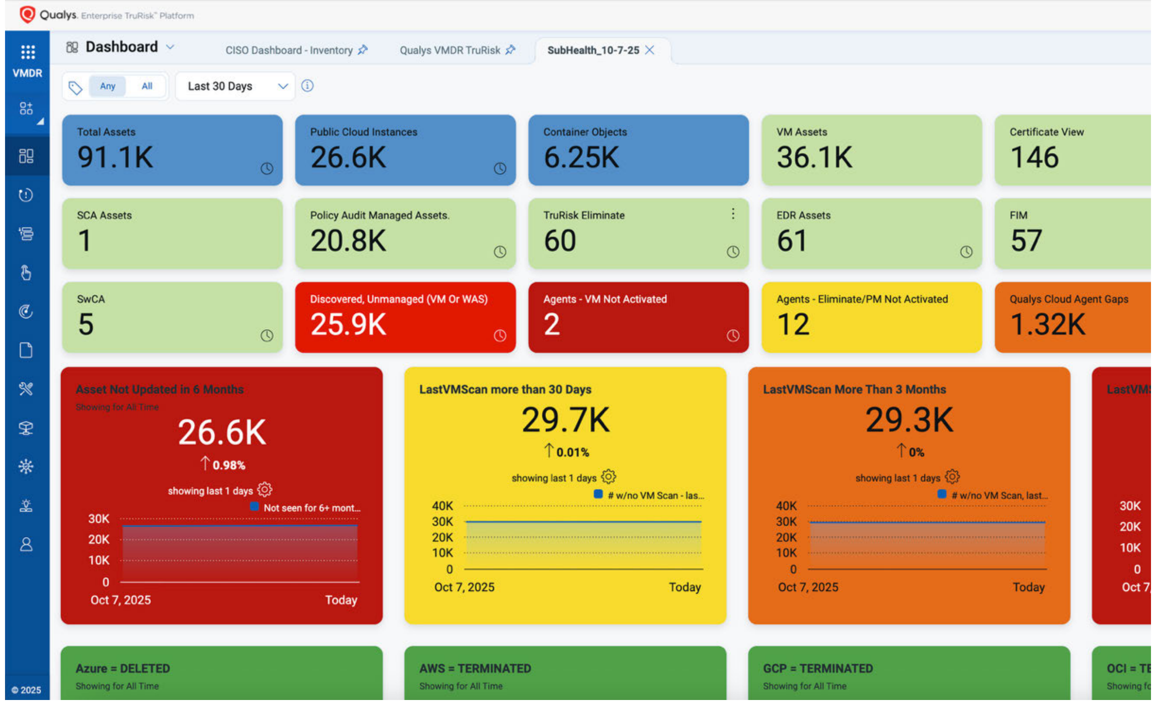

Public
Custom
Qualys scanner
VM
PC
OS
Find
Fix
Verify
Qualys agent
VM
PC
OS
Approved gold image and AMI
(Updated every 2 weeks)
Qualys agent
Amazon machine image (AMI)
Qualys assess on Dev instances
Automatically add Qualys cloud agent
Approve and publish
Live instances
(Rehydration - every 60 days)

Subscription Health Overview

Monitor Utilization, Authentication, and Stale Asset Counts

Gain Insights At a Glance

- ✓ Review License Consumption
- ✓ Track Stale Assets
- ✓ Identify Failed Authentication
- ✓ Capture Potential Ghost Hosts



Total Assets 91.1K

Public Cloud Instances 26.6K

Container Objects 6.25K

VM Assets 36.1K

Certificate View 146

SCA Assets 1

Policy Audit Managed Assets. 20.8K

TruRisk Eliminate 60

EDR Assets 61

FIM 57

SwCA 5

Discovered, Unmanaged (VM Or WAS) 25.9K

Agents - VM Not Activated 2

Agents - Eliminate/PM Not Activated 12

Qualys Cloud Agent Gaps 1.32K

Asset Not Updated in 6 Months
Showing for All Time
26.6K
↑ 0.98%
showing last 1 days

LastVMScan more than 30 Days
29.7K
↑ 0.01%
showing last 1 days

LastVMScan More Than 3 Months
29.3K
↑ 0%
showing last 1 days

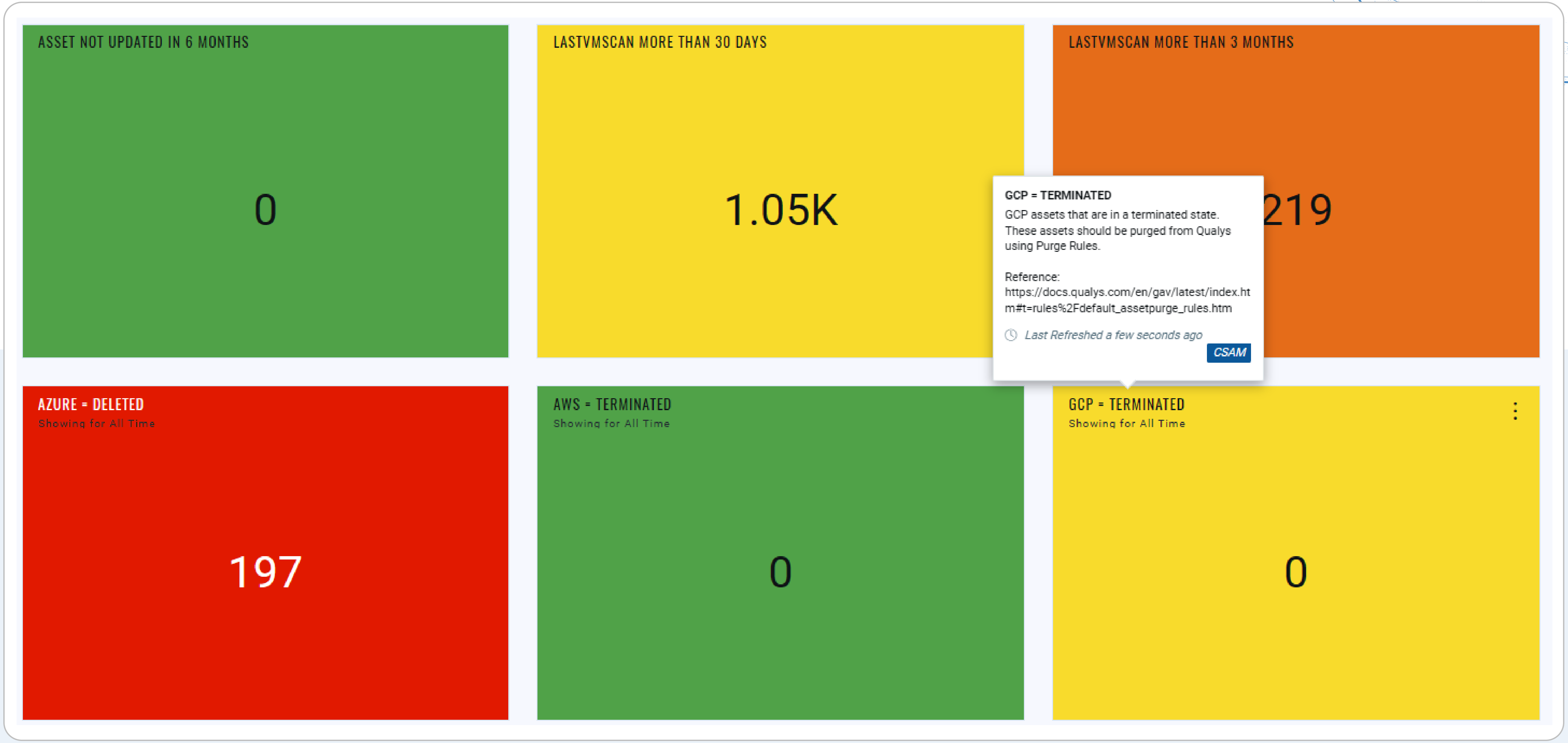
Azure = DELETED
Showing for All Time

AWS = TERMINATED
Showing for All Time

GCP = TERMINATED
Showing for All Time

OCI = TE
Showing fo

Maintain Subscription Hygiene



ASSET NOT UPDATED IN 6 MONTHS

0

LASTVMSCAN MORE THAN 30 DAYS

1.05K

LASTVMSCAN MORE THAN 3 MONTHS

219

GCP = TERMINATED

GCP assets that are in a terminated state. These assets should be purged from Qualys using Purge Rules.

Reference:
https://docs.qualys.com/en/gav/latest/index.htm#t=rules%2Fdefault_assetpurge_rules.htm

Last Refreshed a few seconds ago

CSAM

AZURE = DELETED
Showing for All Time

197

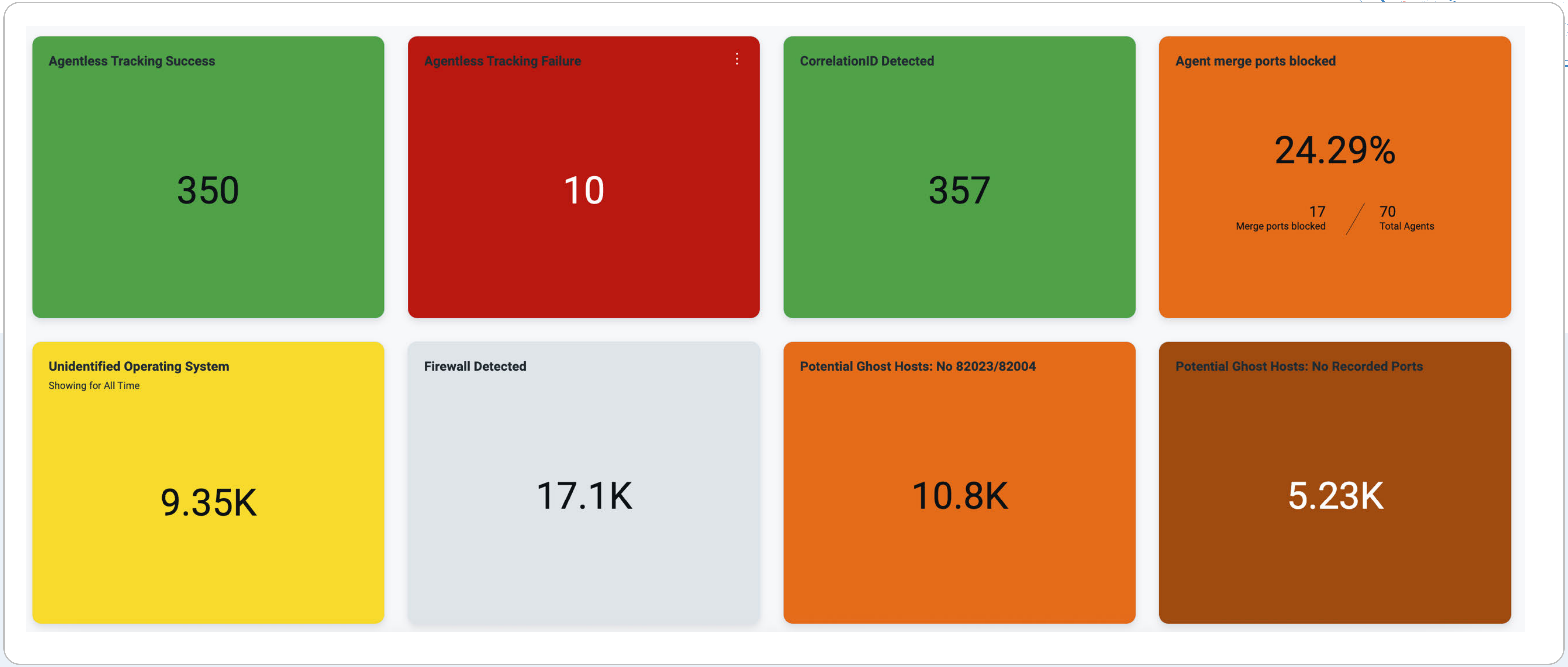
AWS = TERMINATED
Showing for All Time

0

GCP = TERMINATED
Showing for All Time

0

Asset Correlation and Network Anomalies



Agentless Tracking Success

350

Agentless Tracking Failure

10

CorrelationID Detected

357

Agent merge ports blocked

24.29%

17 Merge ports blocked / 70 Total Agents

Unidentified Operating System

Showing for All Time

9.35K

Firewall Detected

17.1K

Potential Ghost Hosts: No 82023/82004

10.8K

Potential Ghost Hosts: No Recorded Ports

5.23K

Get the Most Value Out of VMDR

Inventory

- **Cloud Agents & Network Scanners**
  Streamline inventory, detections, and compliance data
- **Cloud Connectors**
  Public cloud inventory and security posture
- **Container Inventory**
  Inventory containers at runtime
- **VMDR Mobile**
  iOS, Android, and Chrome endpoints
- **Certificate Management**
  Inventory, assess, renew certificates

Assessment

- **103K+ CVE Coverage**
  Streamline inventory, detections, and compliance data
- **99% CISA KEV Coverage**
  Public cloud inventory and security posture
- **Software Composition Analysis**
  Prioritize and eliminate risk from first-party software
- **Secure Hardening**
  Automate security configuration assessments based on CIS Benchmarks
- **PCI ASV Assessments**
  PCI compliance testing and reporting

Prioritization

- **TruRisk™ Scoring**
  25+ sources for threat intel, asset criticality, and multiplying risk factors for effective prioritization
- **MITRE ATT&CK Matrix**
  Understand top Tactics and Techniques from an attacker's perspective and prioritize using threat-informed defense
- **Threat Protection**
  Threat intelligence feeds to your existing Assets

Response

- **Patch & Mitigation Detection**
  Detect missing patches and mitigations on endpoints
- **Continuous Monitoring**
  Alerts for risky software, risky ports, critical vulns to Slack, Pager Duty, or email
- **Rule-based Automation**
  No code/Low code automation with QFlow
- **ITSM/Jira Integration**
  Automatically map tickets to ServiceNow, Jira, and more
- **Flexible API**
  Orchestrate response to critical risk with custom workflows

JON BLEVINS

Cybersecurity Director

3 years at Syniverse

Extensive experience leading **enterprise threat** and **vulnerability management programs**

7+ years threat analysis, containment, and remediation syniverse®

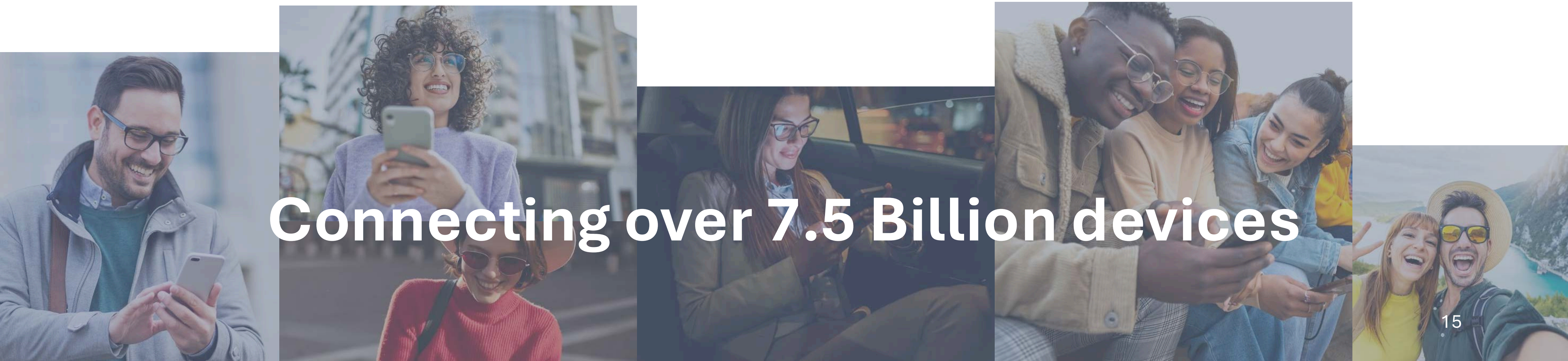
HEADQUARTERS
Tampa, Florida

FOUNDED
1987

INDUSTRY
Telecommunications

For 35+ years,

Syniverse has pioneered connectivity and mobility, transforming how information is exchanged and how people connect, so you can unlock the full potential of communications technology today – and grow the business tomorrow.



Connecting over 7.5 Billion devices

Traditional
Vulnerability Management

Focuses on volume metrics

Relies on tickets, spreadsheets, manual processes

Struggles with scanning coverage gaps and incomplete business mapping

Alert/ticket fatigue leads to unclear remediation priorities

INSIGHTS

The Vulnerability Management program relied on manual processes & ticketing, leading to challenges with coverage, scanning, and issues around prioritizing work efficiently

Industry Shift – Risk-Based Vulnerability Management

Contextualizes vulnerabilities based on risk, not just volume

Prioritizes exploitability, asset value, and business impact

Integrates business context to identify what truly matters

Collaboration improves clarity and reduces noise

INSIGHTS

By adopting risk-based strategies, Syniverse was able to begin focusing on high-impact vulnerabilities, while shifting the culture within the business to help drive decision-making more effectively

Benefits of Risk-Based Approach

85%

Reduction in remediation workload due to TruRisk

50%

Faster MTTR for critical threats

Greatly enhanced visibility, accountability, and communication

Using Qualys – VMDR & TruRisk

Enables better detection, risk assessment, and remediation workflows

Business-specific context and threat intelligence drive prioritization

Dashboarding enhances reporting and resource efficiency

Facilitates collaboration and measurable security improvements

INSIGHTS

Syniverse leverages Qualys VMDR & TruRisk capabilities to enhance detection, prioritization, and dashboarding - thus supporting a more efficient and effective vulnerability management program

Qualys.

ROCon 25

The Risk Operations Conference

AMERICAS