Your Security Eyes: Leveraging Purpose-Built Sensors to Combat Cyber Threats

Himanshu Kathpal
Senior Director, Product Management
Qualys Platform & Sensors

Your **Cybersecurity** program is ONLY as **accurate** as the inventory you can **see, measure, manage and secure** across your hybrid environment!

The Numerous Sources of Cyber Risk

New and evolving risk factors

Risk Sources		Risk Factors	
Data Center	Installed Software	Vulnerabilities	Unauthorized software
AI	Cloud Resources	Infra/DB Misconfigurations	Open-source vulnerabilities
IT Assets	Workloads	Access risks	Missing required software
IoT	Identities	Unauthorized File Changes	Cloud Misconfigurations
SaaS Apps	Modules & Packages	Sensitive data leakage risks	Endpoint Malicious activities
		Technology debt risks	Web application risks

APPLICATIONS

OPERATING SYSTEMS

CLOUD / CONTAINERS / VMs

IT / WORKSTATIONS / SERVERS

IOT

EXTERNAL DEVICES

The Numerous Sources of Cyber Risk

New and evolving risk ecosystem

Risk Sources

Data Center	Installed Software
AI	Cloud Resources
IT Assets	Workloads
IoT	Identities
SaaS Apps	Modules & Packages

Risk Factors

- Vulnerabilities
- Unauthorized software
- Infra/DB Misconfigurations
- Open-source vulnerabilities
- Access risks
- Missing required software
- Unauthorized File Changes
- Cloud Misconfigurations
- Sensitive data leakage risks
- Endpoint Malicious activities
- Technology debt risks
- Web application risks

Apps & Environments

Cloud Misconfiguration Fixes

Application, Open-source vulnerabilities

Dev Teams

SOC, Pen-test team

& many more...

CISO

APPLICATIONS

OPERATING SYSTEMS

CLOUD / CONTAINERS / VMs

IT / WORKSTATIONS / SERVERS

IOT

EXTERNAL DEVICES

The Numerous Sources of Cyber Risk

...And new stakeholders to communicate with

Risk Sources

Data Center	Installed Software
AI	Cloud Resources
IT Assets	Workloads
IoT	Identities
SaaS Apps	Modules & Packages

Risk Factors

Vulnerabilities	Unauthorized software
Infra/DB Misconfigurations	Open-source vulnerabilities
Access risks	Missing required software
Unauthorized File Changes	Cloud Misconfigurations
Sensitive data leakage risks	Endpoint Malicious activities
Technology debt risks	Web application risks

Apps & Environments

Cloud Misconfiguration Fixes

Application, Open-source vulnerabilities

Dev Teams

SOC, Pen-test team

Risk Stakeholders

CISO

- CIO
- CEO
- IT/Ops Teams
- DevOps Teams
- Vulnerability Management
- Audit / GRC

APPLICATIONS

OPERATING SYSTEMS

CLOUD / CONTAINERS / VMs

IT / WORKSTATIONS / SERVERS

IOT

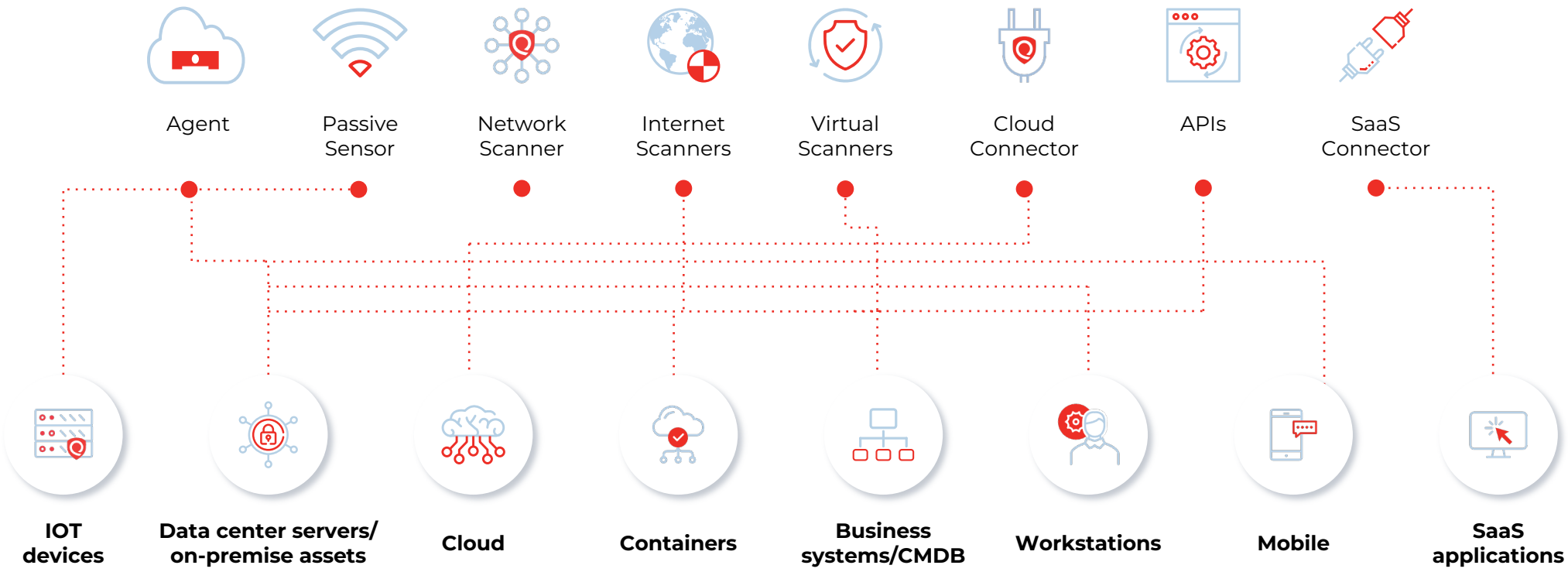
EXTERNAL DEVICES

DE-RISK YOUR BUSINESS

Qualys.

Expanding Attack Surface

Today's enterprise requires a wide range of sensors to secure sprawling environments



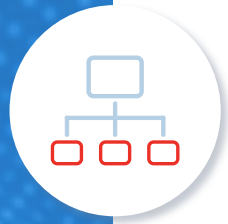
Customer Challenges

Reduce risk with an end-to-end approach for every environment

Uphill battle for security team to have attacker and defender's view!

Does my vendor provider sensors for ALL of my environment?

One size does not fit all, Comprehensive risk management is limited to only **63% of your assets** as Some vendors are Agent based, Some are Agentless, Some have partial coverage for specific environments excluding **exotic systems.**



How many agents I need to install for different use cases?

How many **subscriptions/agents do you have for VM, Config Assessment, Patch, FIM,, EDR, Cloud Security? How can I install/push agents?**

What about my legacy environment?

Organizations have **limited visibility into legacy O.S like Cent O.S 5, XP** but are used for **critical use cases like ATMs,** and most vendors have stop support for it.

Security silos, disparate & manual processes, cost for sensors

- Too **many vendors and tools**, inefficient **manual process** introduce significant burden.
- How much do you think you are paying for duplicate asset records? How much time does your team spend auditing?

Must-Have for CISA

Scanners are MUST Have for
100% coverage for CISA

You are knowingly accepting the RISK for your org by not having ~100% CISA KEV coverage

We safeguard the enterprises with coverage for **1,174** out of **1,190** CVE items in the CISA KEV, amounting to **98.7%** coverage.

Our focus is on what matters most. The remaining 1.3% comprises predominantly vulnerabilities in outdated services, off-market, or minimal enterprise value products.

We set the industry standard with the most comprehensive coverage of CISA KEV.

20.64%

of CVEs are for actively exploited network and perimeter devices.

Augmenting Endpoint Agents based approach

Get Outside-in view

Vulnerability Detection and Assessment

Cyber risk: Limited visibility of remote-only and SSL-based vulnerabilities.

Digital Certificate Assessment

Cyber risk: Some certificates are not present in registry/system

De-Risk Dynamic Hybrid Environment

Cyber risk: Cloud environments often have blind spots, No coverage for network devices or firewall

CIS Benchmarking

Cyber risk: On average, 50% of CIS benchmark controls fail across CSPs.

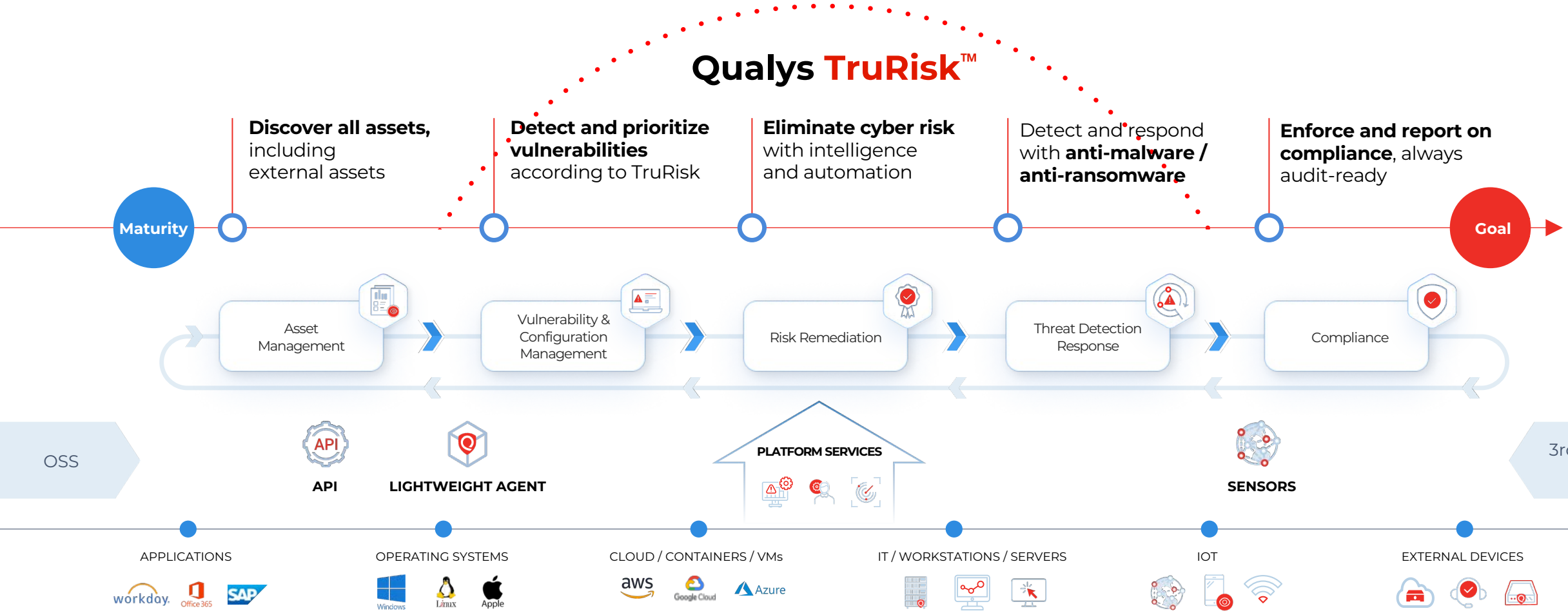
The Qualys Difference:

The ‘How we do it’ part...

Qualys®

The Enterprise TruRisk Platform

End to end cyber risk management



Powered by Purpose-Built Sensors

Ingest data insights anywhere to constantly monitor, detect, and defend against threats in real-time

- Local Scanners
- Internet Scanners
- Headless Scanner
- Qualys Gateway Service
- Cloud Agents
- Cloud Connectors

- Passive Scanners
- Offline Scanners
- Container Sensors
- Snapshot
- API
- SaaS Connectors

Scan Resiliency using Qualys

Vulnerability management alternatives

Qualys Scanner Appliance

Qualys Network Passive Sensor

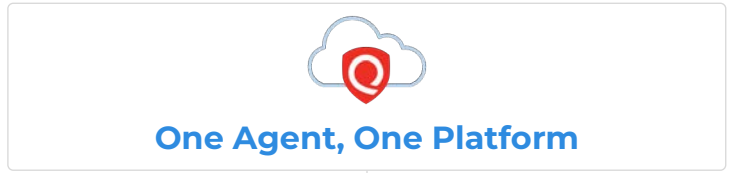
Qualys API and Snapshot

Qualys provides customers with a variety of solutions to detect and manage vulnerabilities without the exclusive use of an endpoint agent.

Better Outcomes

...With CLOUD AGENT

Measure, Communicate and Eliminate Risk



01 Cyber Security Asset Management

- 2-second Visibility
- Identify 30% unknown assets

02 Vulnerability Management Detection and Response

- 100K+ CVE's
- <24-hour response for critical CVE's
- 4-hour MTTD

03 Config risk & Policy Compliance

- Elevating from CIS-scanning service to Risk management, Compliance betterment

04 File Integrity Monitoring

- Be compliant with government and industry standards

05 Patch Management

- Avg 40+% Faster Remediation for critical vulnerabilities

06 Custom Assessment and Remediation

- Detect vulnerabilities in first-party applications

07 Endpoint Protection

- Protect against attacks

08 Passive Sensing

- Discover 100% network traffic and cover internal attack surface

09 Runtime Open-source software assessment

- Next Log4j finder

Multi-Platform Support

Industry's most extensive coverage

Windows .exe (x86_64)	**Windows** .exe (ARM64)	**Linux** .rpm (x86_64)	**Linux** .rpm (ARM64)	**Linux** .rpm (ppc64le)	**Linux** .deb (x64)	**Linux** .deb (ARM)
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)
CoreOS .tar (x86_64)	**ChromeOS** .apk (x86_64)	**SQL Server**	**Oracle Database**	**Bottlerocket OS** .tar (x86_64)	**Container – optimized OS by Google** .tar (x86_64)	**GenToo** .tar (x86_64)

Qualys Only

Qualys Cloud Agent

Quality, security, and safety

User Mode: **VM, PC, SwCA, CAPS, CAR, Patch Management, and CSAM** are developed in user mode; eliminating the risk of a Blue Screen of Death scenario.

Phased Deployment: Agent Binaries follow **ring deployment**, Automated checks are in place to **prevent malicious commands** like rm, kill, mv, etc.

Apps with Kernel Mode: **Only for EDR and FIM** running on Windows OS, Any driver changes are released as new Agent versions after being certified by Microsoft.

Qualys testing protocols include (Not limited to):

- Static code, memory leak and binary analysis of new features and changes.
- Driver load-unload tests on all supported Windows platforms.
- Performance impact assessments.
- Longevity and performance.
- WHQL Certification Test Suite.

Industry's widest Support for Scanner Platforms

aws

Azure

Google Cloud

ORACLE Cloud Infrastructure

NEW IBM Cloud

NEW Alibaba Cloud

vmware

openstack

NEW NUTANIX

Red Hat KVM, RHV

CITRIX

NEW docker

PROXMOX

Scanner Usage

Scanners

70,000+

Active Scanners
in Production

Assets

2+ Billion

Assets Scanned
in last 12 months

Customers

12,000+

Customers
using Scanners

Sensors Powers Every Qualys Solution

Key stats for vulnerabilities that matter

103,521+

Identified Vulnerabilities/CVEs

194,995+

Detection Signatures (QIDs)

99%+ Parity

For Authenticated QIDs b/w scanner and Agent

11,301 Remote QIDs

Remote Only QIDs (Only Via scanner, including for network devices, 4,477 CVE has Auth detection)

Qualys Native Integrations for Unified SecOps Experience

Bridging IT & security silos to measure, communicate and eliminate risk

Asset Inventory	servicenow, bmc helix, Active Directory	Brings complete visibility into your managed and unmanaged assets
Real-time Monitoring	splunk>, Radar, VMware Tanzu	Provides immediate threat detection and monitoring
Reporting and Ticketing	splunk>, Radar, Jira	Supports reporting and response management
Develop-Build-Deploy	Jenkins, Azure DevOps, Atlassian Bamboo, Visual Studio Code, GitHub Actions	Shift left by streamlining development to be secure

Customer Benefits

Consolidation of Security tools with Qualys Sensors and how we do it better!

Unparalleled Visibility: Extend coverage for ALL of your environment, reduce risk from blind spots with industry's widest sensors feeding into a single pane of glass view across the infrastructure.

Reduce Total Cost of Ownership (TCO): By consolidating multiple siloed point products, Integrations and Operational Simplicity, Native Correlation eliminates manual work, Save more on computing.

Reduce Mean Time to Remediation (MTTR): Respond faster to threats with industry's widest coverage for devices.

Start Your 30-Day Free Trial of **Qualys Platform** and Streamline Risk Management Across Your Enterprise!

Qualys®