Risk and the Changing Role of the CISO: KRIs vs. KPIs

Mike Orosz
CISO
Vertiv

Mike Orosz

Vertiv | CISO

CISO at Vertiv accountable for all aspects of global information and product security.

Previously Sr. Director Global Cyber and Physical Security at Citrix and Global compliance Officer for Citi.

Resides Ann Arbor, Michigan; Master's Degree in Information Sciences, Cybersecurity from Penn State University.

Vertiv (NYSE: VRT) brings together hardware, software, analytics and ongoing services to enable its customers' vital applications to run continuously, perform optimally and grow with their business needs. Based in Westerville, Ohio, Vertiv does business in more than 130 countries.

Qualys.

Cyber Risk Grows with Time

More Threats, Less Time, and More Stakeholders

Time to Discover

- **69%** of organizations experienced **attack from unknown assets** last year
- Breaches sometimes **take months to discover**

Time to Measure

- Using CVSS alone, **more than half of vulnerabilities** can be marked as critical

Time to Communicate

- **47%** of CISOs report to the **CEO**
- **CISOs** participating in **board meetings** is common

01 **100%** Technology

02 **100%** Government

03 **94%** Communication and media

04 **88%** Healthcare

05 **86%** Manufacturing

Time to Remediate

- It takes **30+ Days** to remediate weaponized vulnerabilities
- **50%** incident response involve significant **exploitations**

Qualys.

The Need for KPI Metrics

Tailoring KPIs for the Information of Today and Tomorrow

- What do I have in my environment?
- What is my current cyber risk in dollars and percentages over time?
- Where is my risk and how do I reduce it?
- What are the best proactive measures?
- How am I doing compared to others?

Qualys.

The Solution

Aggregating Intelligence for a Single Source of Truth

Qualys TruRisk™

- **Asset Criticality**
- **Business Function**
- **Asset Internal/External**
- **Aggregate Risk Signals**
- **Threat Intel – active exploitation**

01 **Measures Aggregated Risk with prioritization**

02 **Criticality by Business Function:**
Talk to stakeholders with evidence

Qualys.

Turning KPIs into Clear Communication

Addressing Cyber Risk Communication & Enumeration

Board

What are we doing to address cybersecurity risk?

Validate it.

CEO & Executives

How is cybersecurity risk efforts balanced against business operations priorities?

Validate it.

Business

We are busy earning revenue, what are the highest cybersecurity priorities we need to focus on right now?

Prove it.

Auditors

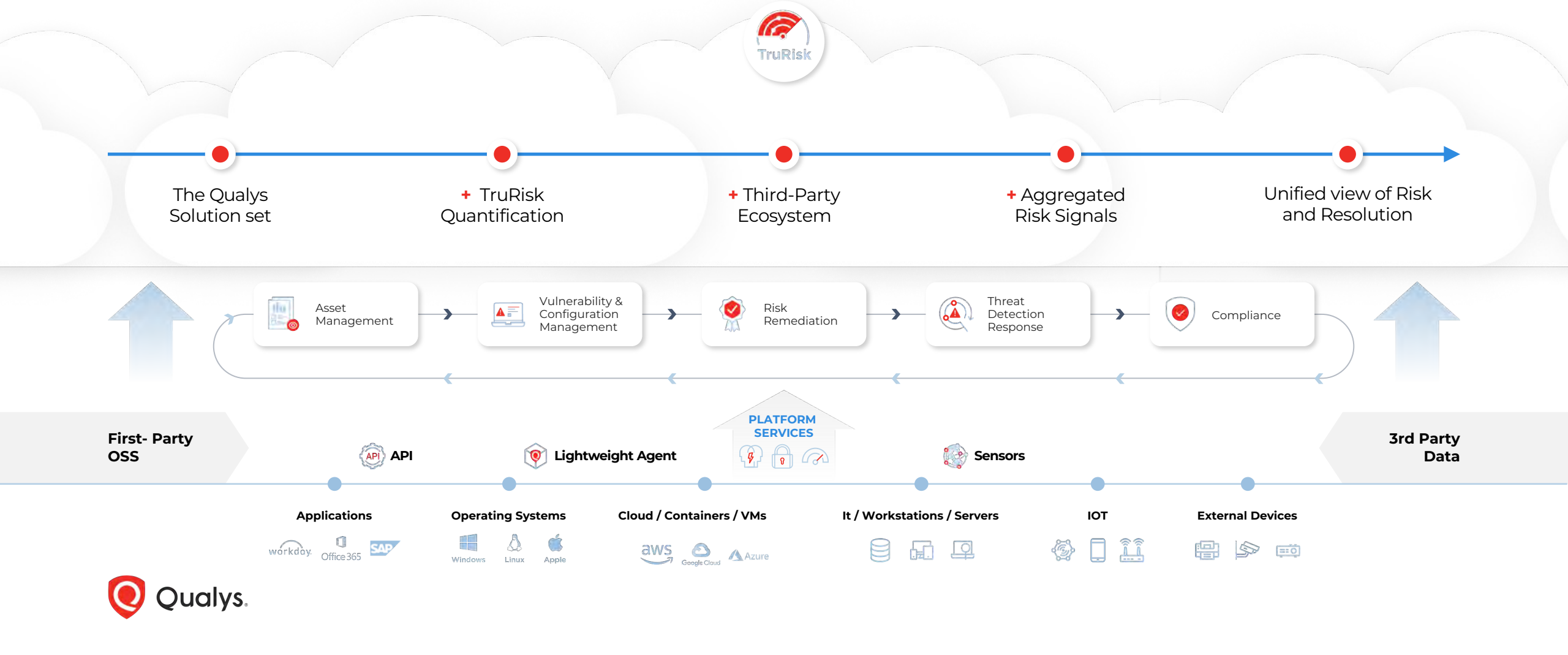
Are you compliant with regulation _____?

Prove it.

Qualys.

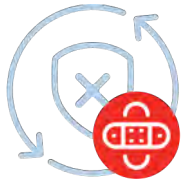
Aligning Risk with Cyber Risk Management

Continuous Measurement, Communication and Elimination Cycle



Qualys.

TruRisk Elimination



Deploy Patches & Configuration Changes

Deploy the right patches and/or conf changes to the right devices, anywhere

Custom Remediation

For Zero Days and custom apps

Qualys.

Aligning Risk with Cyber Risk Management

Continuous Measurement, Communication and Elimination Cycle

TruRisk

Measure

Communicate

Eliminate

Asset Management → Vulnerability & Configuration Management → Risk Remediation → Threat Detection Response → Compliance

First- Party OSS

3rd Party Data

PLATFORM SERVICES

API | **Lightweight Agent** | **Sensors**

Applications: workday. Office 365 SAP

Operating Systems: Windows Linux Apple

Cloud / Containers / VMs: aws Google Cloud Azure

It / Workstations / Servers

IOT

External Devices

Qualys.


SC
23