QSC 24

Navigating the Threat Landscape for Your Supply Chain and Custom Apps

Unified Risk Management of Open-Source Software (OSS) and First-Party Vulnerabilities

Himanshu Kathpal
Senior Director, Product Management
Qualys Platform & Sensors

Agenda

01 Software Supply Chain Risk from Open-Source Software and First Party

02 Customer Challenges

03 Solution Overview

04 Demo

05 Customer Benefits

Supply Chain Risk from Open Source

… And OSS Packages are Ubiquitous

Many organizations today run their business using proprietary or **“First-Party” software built on 80% open-source components.**

Security Teams manage in CI/CD but have **No Visibility in Production**

OSS Are Deep-Embedded

High Risk CVEs

CVE-2022-23181	**Privilege Escalation**
CVE-2021-44832	**Remote Code Execution**
CVE-2022-27772	**Broken Access Control**
CVE-2022-31129	**RegEx Denial of Service**
CVE-2022-28347	**SQL Injection**
CVE-2020-36518	**Denial of Service**
CVE-2021-43138	**JS Prototype Pollution**
CVE-2022-24785	**Directory Traversal**
CVE-2020-29652	**Null Pointer De-reference**
CVE-2022-23307	**Deserialisation of Untrusted Data**

Vulnerabilities in Open Source

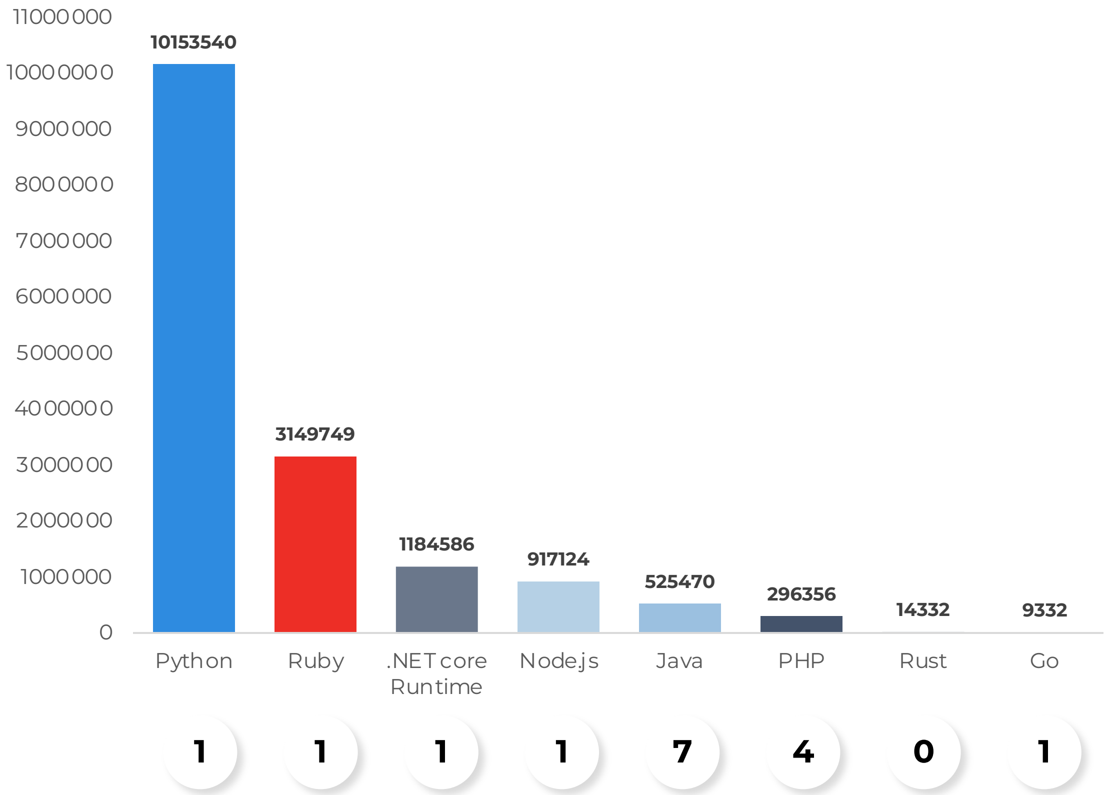
48%

Codebases have high-risk vulnerabilities

56

Average Vulnerable OSS packages per asset

Type Wise Numbers



Expand to Measure First-Party Application Risk

Home Grown, Custom Applications

Measure & Communicate your own custom risk in production

Unique to Your Environment Risk

Example: Flag assets where a key service is not running, Create vulnerabilities for assets with unauthorized plugins or addons

2024 Data Breach Investigations Report

verizon business

Supply Chain Attacks:

A Growing Cyber Threat

"The 2024 Verizon DBIR highlights a significant rise in breaches tied to third-party software and supply chain attacks, now accounting for 15% of all data breaches — a **68% increase from the previous year."**

Customer Challenges

How OSS and First-Party Create Risk

Uphill Battle for Security Team to Reduce Software Supply Chain Risk

No lifecycle management of vulnerabilities

OSS and First-Party vulnerabilities are not managed end-to-end from discovery to remediation like third-party vulnerabilities.

No central reporting and prioritization of risk

Organizations often **need to create one-off scripts** to detect custom risk. Reporting is not centralized, and these scripts have minimal security oversight.

Lack of visibility in open-source components

Organizations have **limited visibility into open-source components** (e.g., Log4j) used in first-party and third-party applications and commercial off-the-shelf tools.

Security Silos, Disparate & Manual Processes

Too **many agents and Tools**, Inefficient **manual process** introduce significant burden.

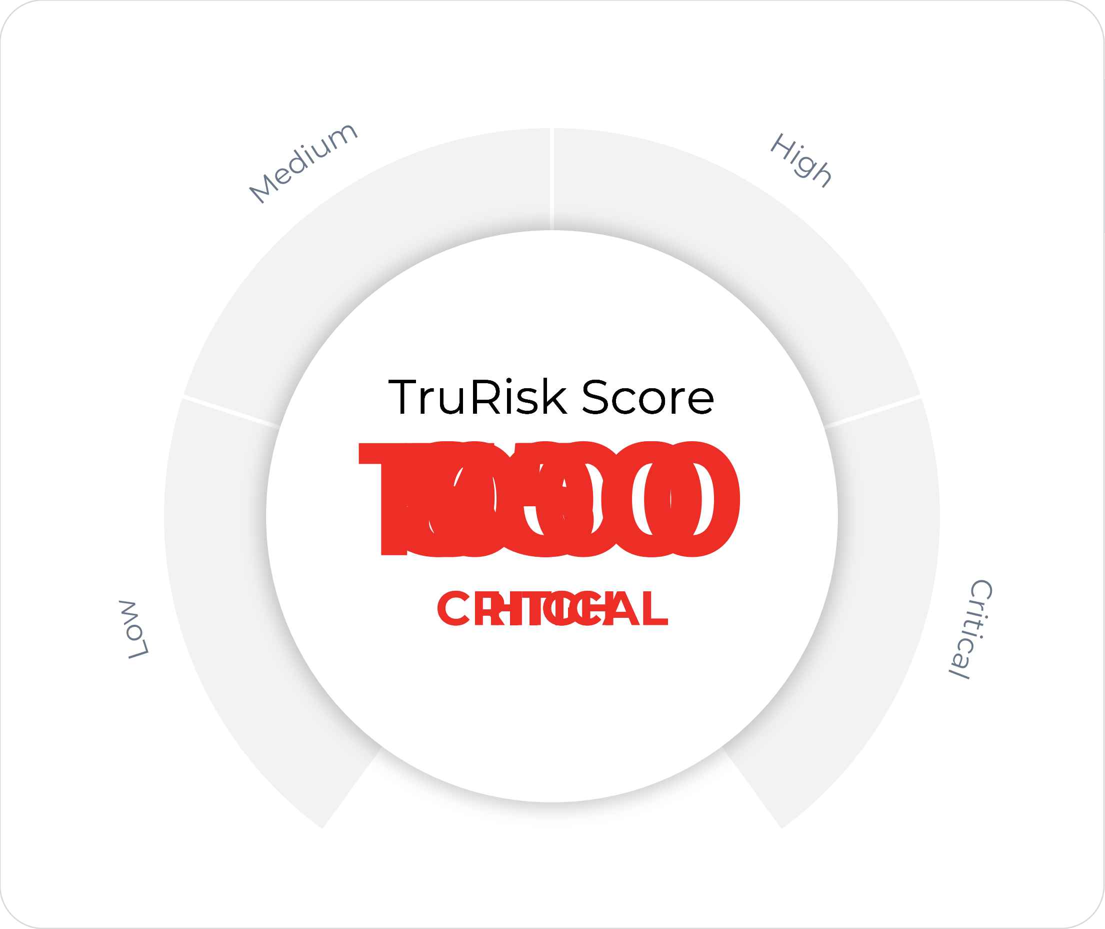
Runtime Software Composition Analysis with the Qualys Cloud Agent

Qualys.

TruRisk... By Correlating Security Data

Contributing Factors

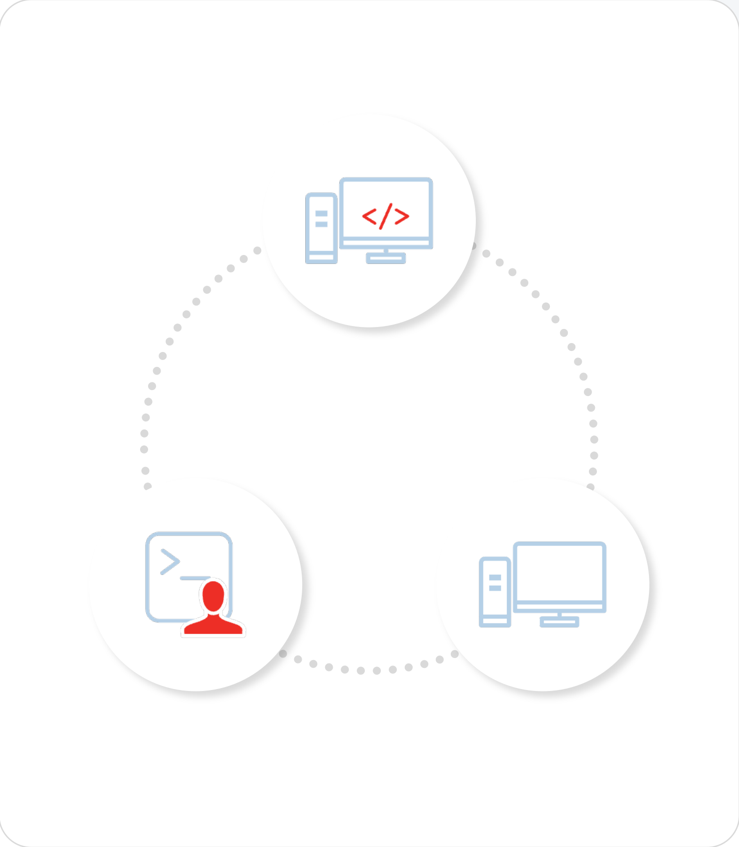
- ○ External facing +RDP misconfig
- ○ Ransomware
- ○ OSS vulnerabilities
- ○ First Party Risks
- ○ Business-critical asset



It Starts with Visibility

Get Visibility into First and Third-Party OSS Risk

01 | Discover



Enable SwCA in a Single Click

- ✓ Flexible environment specific scanning and configuration controls
- ✓ Deep file system scan, Continuous evaluation and data enrichment on platform

Near real-time scanning for latest vulnerabilities

- ✓ 4-HR MTTD, <24-hour response for critical CVE’s, 17K+ SCA QIDs

It Starts with Visibility

Get Visibility into First and Third-Party OSS Risk

Business Context

- Business Criticality
- Asset Exposure (internal vs external)

Without context being applied, risk **estimations will be inaccurate**

Risk Context

- Exploitability
- Evidence of Exploitation
- Likelihood of Exploitation

Risk Score: **600**

Without OSS

- ✓ Visibility without your OSS risk
- ✓ Prioritizing the known risks
- ✓ Remediation of third-party applications

Risk Score: **850**

With OSS

- ✓ First-party and Third-party party OSS Risk
- ✓ Prioritizing overall risk
- ✓ Custom remediation ready to deploy

Measure TruRisk, Comprehensively

Asset Critically

Location of the Asset

Infra Vulnerabilities

Infra, DB misconfigurations/ control failures

Certificates

Open-source software vulns

EOL Software

Web Application vulnerabilities

Cloud Misconfigurations

Unauthorized software, Absence of security tools

External Attack Surface/Exposures – ports, services

Qualys Detection Score (QDS):

Threat mapping: Exploitation, CISA, EPSS augmented, Ransomware, Darkweb (with VMDR)

25+ Threat Feeds

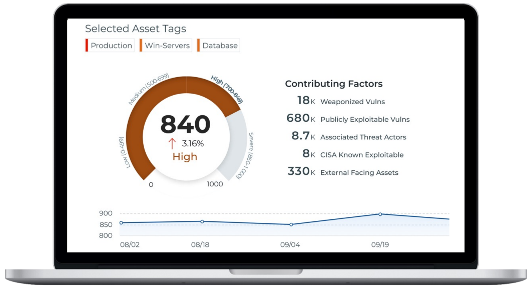
Business Asset Context:

Criticality, Ownership, role, exposure (Enhanced with CSAM) + Compensating controls

Asset Context – CMDB, AD, EASM, Asset Attribution

Qualys TruRisk Score:

Quantified Score, transparent formula and weightages (comes with VMDR)



Selected Asset Tags

Production | Win-Servers | Database

Contributing Factors

18K Weaponized Vulns

680K Publicly Exploitable Vulns

8.7K Associated Threat Actors

8K CISA Known Exploitable

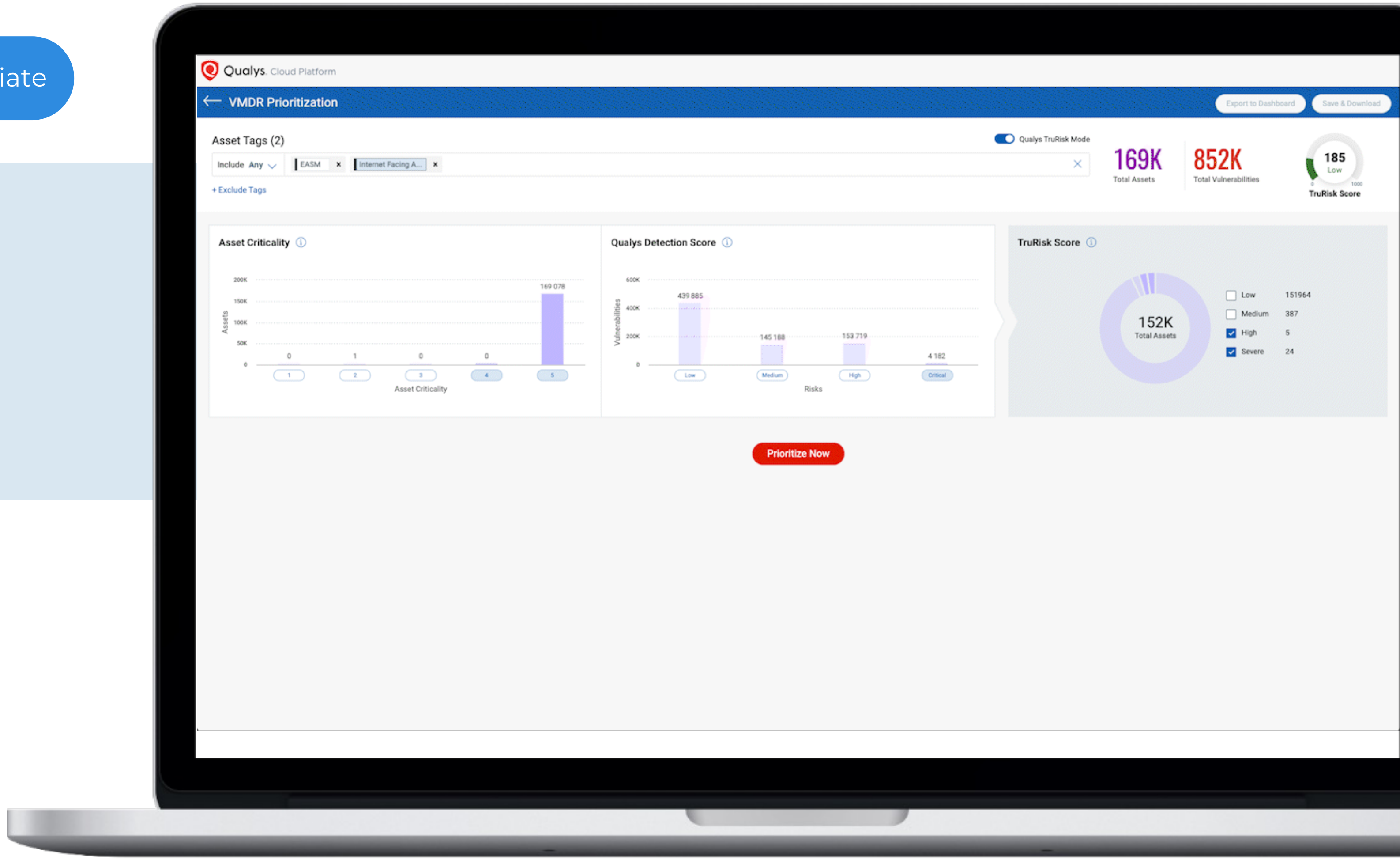
330K External Facing Assets

03 | Prioritize + 04 | Remediate

Focus on What Matters

Prioritize & Remediate Based on Business & Risk Context

Software applications, affected assets, and available assets **on a single dashboard and reporting**



Asset Tags (2)

Include Any: EASM ×, Internet Facing A... ×

□ Low	151964
□ Medium	387
☑ High	5
☑ Severe	24

Eliminate Custom Risk

Create your Own Remediation Logic! (comes with CAR)

python PowerShell vbscript Perl Lua

Respond to zero days before the official patch is delivered

Fix your custom risk

Update Open-Source libraries

Bring it All Together

Discover, Assess, Prioritize, Remediation **+ Repeat**

01 | Discover — Extend visibility and discovery of software supply chain

02 | Assess — Analyze vulnerabilities & Misconfigurations across the organization

03 | Prioritize — Measure Risk & Prioritize based on business & Risk context.

04 | Remediate — Integrated remediation across the organizations

Product Demo

Qualys®

One Place to Manage Supply Chain, 1st & 3rd Party Risk

Customer Benefits

Improved Visibility: Extend vulnerability coverage for OSS, and First-party orchestrated within existing VMDR workflows including SBOM generation.

Detect, Prioritize and remediate the risk of next Log4j and other deep-embedded open-source packages: Proactively defend when a zero-day breaks out potentially affecting a popular library.

Reduce Mean Time to Remediation (MTTR): Respond faster (upto 60%) to first-party threats and third-party zero-day OSS threats.

Reduce Total Cost of Ownership (TCO): Reduce TCO by consolidating multiple siloed point products into Unified One-platform-one-agent.

Start Your 30-Day Free Trial of **Qualys VMDR** and take control of Software Supply chain risk today!

Qualys®