Unwrapping SBOMs for knowing, Managing & Reducing Risk of Software Supply Chain

Pablo Quiroga
Director, Product Management
Attack Surface Management

Open-Source Software Vulnerabilities

The Toll on Cybersecurity Teams

79%

Of software running on servers is open-source

96%

Of first-party (homegrown) software contains open-source components

40+%

Contain high-risk factors such as exploitable vulnerabilities

52%

Of enterprises spent more than a month remediating Log4Shell

Qualys.

Remediation Gaps

In Software Supply Chain Risk

52%

Of teams took more than one month to remediate Log4Shell.

Why?

- **No catalog** of all software components
- Limited SBOMs from **third-party apps**
- Difficult to ingest & correlate SBOMs from **first-party apps**
- **Limited risk assessment** at runtime
- Manual remediation without **business context**

Qualys.

Typical Remediation Timeline

For an Open-Source Component Vulnerability such as Log4Shell

Day 0

- Assessment starts.
- Align resources, create scripts and start scoping vulnerability scans

Day 7

- News from security community alerting of a new file
- Fine-tuning scripts and re-scan
- Monitoring list of impacted software and manually connecting to assets

Day 14

- Begin detecting vulnerabilities and building datasets
- Begin prioritizing based on asset critically (if it's available)
- Manual analysis of components to software – triage begins.

Day 21

- Manually trace application owners and triage remediation process
- Prioritize and start remediation.

Day 31

- **Average remediation time: 17 days**
- Initially detected vulnerabilities are starting to be patched

40+ Days

- **30% of vulnerabilities still unpatched (Qualys research)**

Qualys.

Supply Chain Risk Management Must Be Proactive and Continuous

Qualys.

Existing Solutions

DevSecOps (CI/CD)

Repository Assessment

aqua, JFrog, sonar, Rezilion, REVERSINGLABS, snyk, mend.io, SYNOPSYS Black Duck, LINEAJE Tenable Ventures, FOSSA, SECURESTACK, ENDOR LABS

Runtime Security

Production Environment

adolus, TANIUM, Balbix, Qualys

Software Builders (DevSecOps)

- Internal Developers
- Software Publishers

Software Consumers & Operators

- Corporate IT, Security, Risk & IT Ops
- Vulnerability Management Teams

Gaps in Software Supply Chain Risk Management

With Available Solutions

DevSecOps (CI/CD)

Repository Assessment

- ✓ Covers internally developed apps
- ✗ Difficult to track production drift – blind spots in production environment

Runtime Security

Production Environment

- ✓ Covers major technologies in production to confirm vulns
- ✗ Lack of correlation with SBOMs / Apps.
  No business context (App Name, Owner...)

Lack of integration between DevSecOps and Runtime Security

Qualys.

Why Focus on SBOM?

How Does It Help?

"SBOMs provide increased transparency, provenance, and speed at which **vulnerabilities can be identified and remediated**."

- National Institute of Standards and Technology (NIST)

Qualys.

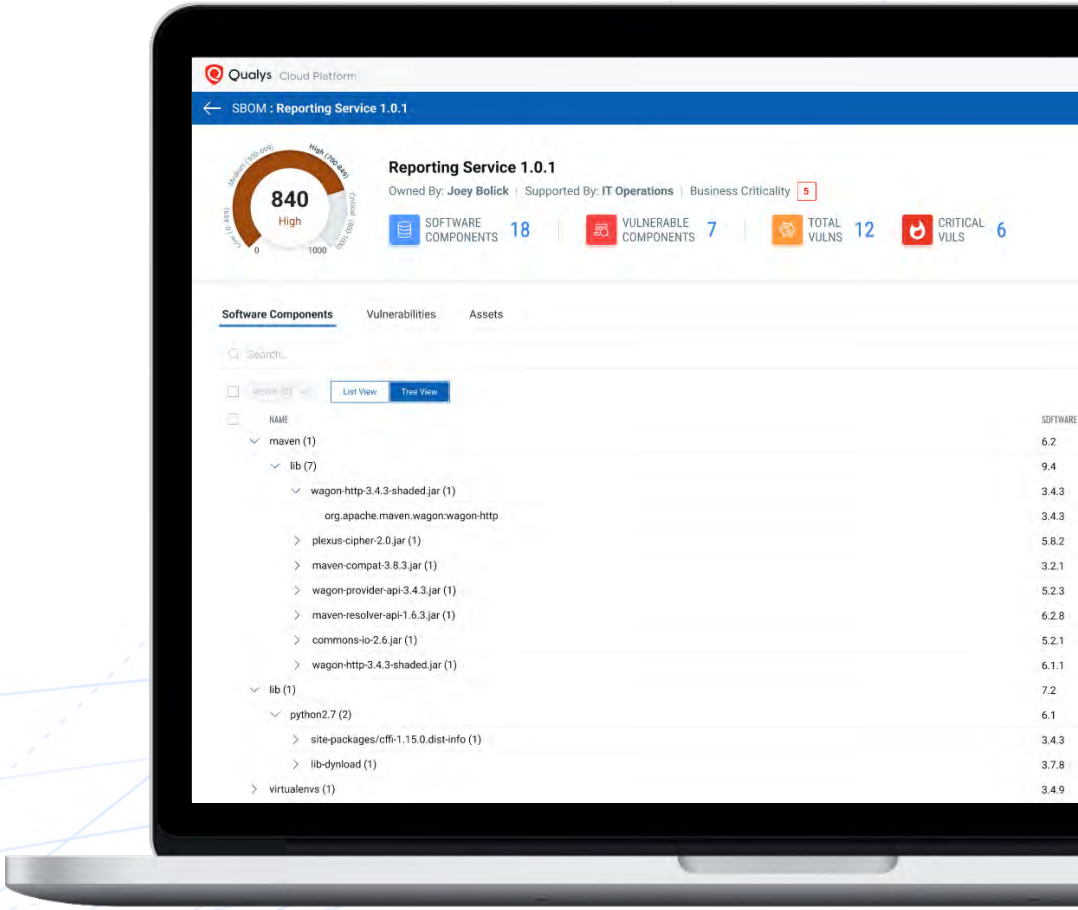
Qualys SBOM Risk Analysis

Track all SBOMs in a single place, analyze software component vulnerabilities and measure impact to your production environment

01 Single SBOM repository for third-party software & first-party apps

02 Continuous visibility of all software components Vulns in production

03 Centrally prioritize TruRisk of your entire Software Supply Chain, with Business & Asset Context



Qualys.

Demo

Measure, Communicate & Reduce Risk of Your Software Supply Chain

Qualys.

Reduce the Software Supply Chain Risk

Respond immediately to zero-day vulnerabilities

Qualys.

Detection time
14 Days

1 Day

Triage & Prioritization time
17 Days

Hours or Couple of Days

End-to-end Response
31+ Days

3-7 Days

Qualys CyberSecurity Asset Management (CSAM)

With External Attack Surface Management

Inventory your full IT ecosystem

Automatically identify all IT assets, whether on-perm, mobile, clouds, containers, OT and IoT for a complete, categorized inventory

Detect inventory security gaps

Know when unknown devices connect to the network, unauthorized software is detected, or required security software is missing; and detect end of life for software and hardware

Report and respond to risks

Create asset security health reports for PCI-DSS and FedRAMP, get automated, pre-defined alerts and take response actions like uninstalling unauthorized software

Scale effortlessly with VMDR

Execute scripts at scale across the enterprise and orchestrate scans, through one-click automated workflow with Qualys VMDR

Sign up for a free 30-day trail

Qualys.


SC
23