THE **RAPIDFORT** SOLUTION

Automatically identify and mitigate up to 90% of vulnerabilities

BACKGROUND

Approximately 50%–90% of all software in today's production environments is unused, mainly because of how we build and package modern software applications. Unused software components present a continuous maintenance burden and a significant security risk. They also generate a lot of noise – making it challenging to identify and prioritize risks in the applications' execution path – and provide hackers with existing vulnerabilities to breach an organization's network, "live off the land" undetected, and access sensitive data.

A lot of risky, unused code stems from open-source software (OSS), which constructs 70%–90% of software in modern applications,* and constitutes a majority of an organization's software attack surface. OSS is provided "as is," and security teams must manage its risk differently than in-house or vendor software. It's crucial to be vigilant about OSS vulnerabilities and to remove or monitor access to unused components.

How do organizations protect themselves today?

Many organizations leverage scanning solutions to find and report vulnerabilities within their OSS and infrastructure. However, these scans typically provide an unwieldy number of vulnerabilities to address, and more importantly, they do not provide an effective prioritization method.

This leaves security teams overwhelmed, using an inefficient "whack-a-mole" approach to solving vulnerabilities that does not secure their software and prevents them from making meaningful progress in managing vulnerabilities.

* Linux Foundation, "A Summary of Census II: Open Source Software Application Libraries the World Depends On," 2022

THE **RAPIDFORT** SOLUTION

A better, faster way to secure your software

RapidFort's comprehensive Software Attack Surface Management (SASM) platform enables organizations to scan their software infrastructure, gain a deep understanding of their software attack surface, and automatically "lock out" unused code. ***The result?*** **A 50%–90% reduction in vulnerabilities – maintained automatically and continuously.**

Our flexible and powerful toolset can be used by security teams to manage and remediate vulnerabilities in unused components without wasting developers' time – a task that would otherwise require months of patching with highly technical, costly developers. It can also be used by developers while they build new software, automatically hardening and securing code as they go.

Run-time Toolset (Security)

Scan & Observe

Scan your infrastructure (Registries, Kubernetes, VMs)

Generate SBOMs

Create accurate vulnerability reports

Measure risk with Rapid Risk Scores ML model

Opportunity-to-improve metrics with reduction estimates statistical model

Profile & Understand

Understand your software attack surface

Generate RBOMs (Real BOMs)

Prioritize vulnerability remediation

Obtain full list of unused packages for discussion with engineering

Harden & Secure

Minimize your software attack surface

Reduce your workload size

Improve your security posture

Manage 80% less software: Less risk, vulnerabilities, patches, alerts

Build-time Toolset (Devs)

See how RapidFort can help you identify and mitigate risk – automatically.

Get Started