sonatype *repository firewall*

Block malicious open source at the door.

Sonatype solves your challenges:

742% growth

742% growth rate year over year in software supply chain attacks

Block malicious packages from entering your repository
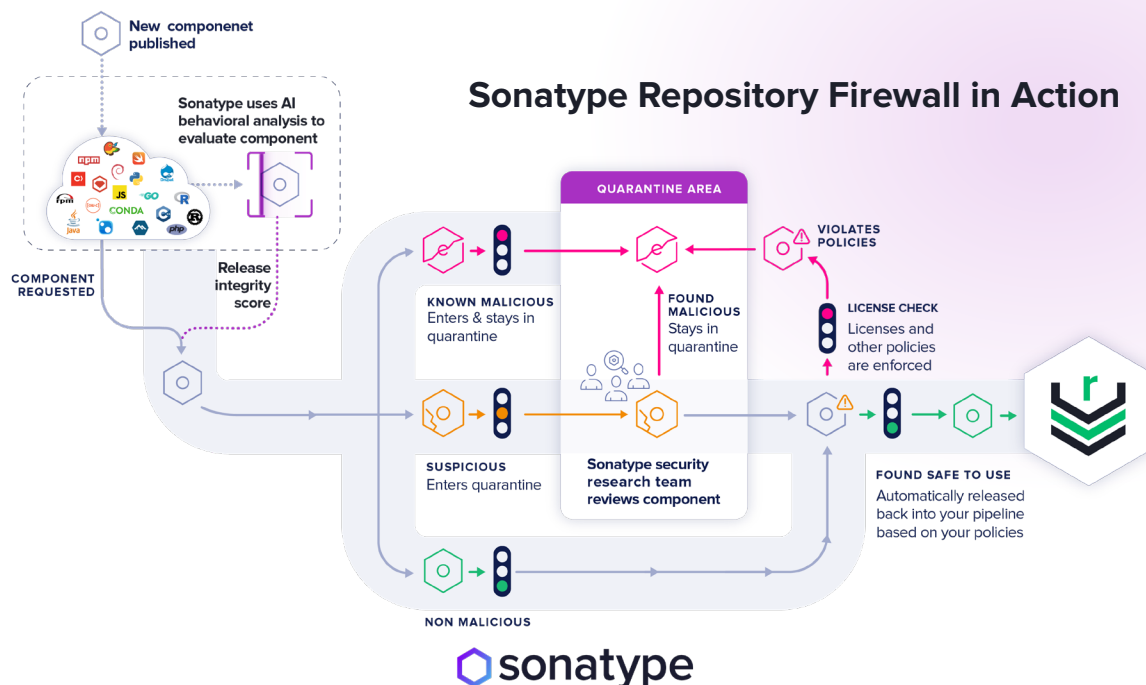
Bad actors are constantly evolving their attack vectors

Repository Firewall has identified and blocked **over 108k malicious and suspicious packages**
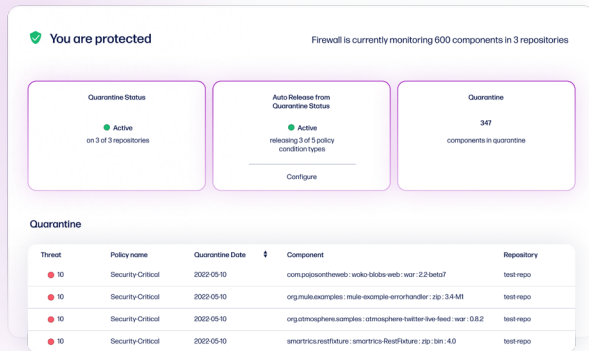
Keep your dev teams innovating

Automated policy enforcement ensures your dev team are always using the safest OSS code

Improve your software supply chain security by automatically detecting known and unknown malware from entering development cycles. Sonatype's Repository Firewall is the only automated solution to protect your software supply chain from malware and vulnerabilities. Using next-generation artificial intelligence (AI) behavioral analysis and automated policy enforcement to evaluate components before they enter your repository, it enables developers to continue innovating with the most recent safe code, mitigating more costly issues that can occur further in the software development lifecycle.

Sonatype Repository Firewall in Action

New componenet published

Sonatype uses AI behavioral analysis to evaluate component

COMPONENT REQUESTED

Release integrity score

QUARANTINE AREA

KNOWN MALICIOUS Enters & stays in quarantine

FOUND MALICIOUS Stays in quarantine

VIOLATES POLICIES

LICENSE CHECK Licenses and other policies are enforced

SUSPICIOUS Enters quarantine

Sonatype security research team reviews component

FOUND SAFE TO USE Automatically released back into your pipeline based on your policies

NON MALICIOUS

sonatype

First Line of Defense

✓ Stop malware at the repository level
with automatic quarantining of malicious and suspicious packages.

✓ Protect your SDLC from evolving threats.
Repository Firewall protects you from vulnerabilities, malware, next-gen supply-chain attacks, brandjacking, typosquatting, dependency confusion-type attacks, and more.

✓ Remediate violations faster.
Contextual remediation information lets you know why components were blocked and offers alternatives so you can fix issues quickly.

POLICY COMPLIANCE

Don't sacrifice security or innovation

### ✓ Developers don't have to change behavior
Repository Firewall blocks malicious code before it enters your workstream so your dev team are always using safe components.

✓ Set it and forget it.
Automated policy enforcement means you are always delivering the safest version of requested components.

✓ Create policy-based rules
that control what OSS components are allowed into your SDLC, what to quarantine, and what is released from quarantine.
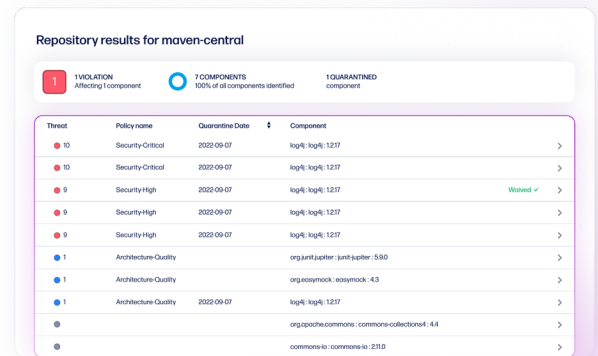
Sonatype is the software supply chain management company. We enable organizations to innovate faster in a highly competitive market. Our industry-leading platform empowers engineers to develop software fearlessly and focus on building products that power businesses. Sonatype researchers have analyzed more than 120 million open source components — 40x more than its competitors — and the Sonatype platform has automatically blocked over 115,000 malicious components from attacking software development pipelines. Enabling high-quality, secure software helps organizations meet their business needs and those of their customers and partners. More than 2,000 organizations, including 70% of the Fortune 100 and 15 million software developers, rely on our tools and guidance to be ambitious, move fast and do it securely. To learn more about Sonatype, please visit **www.sonatype.com**.