nexus firewall

Your first line of defense against modern supply chain attacks.

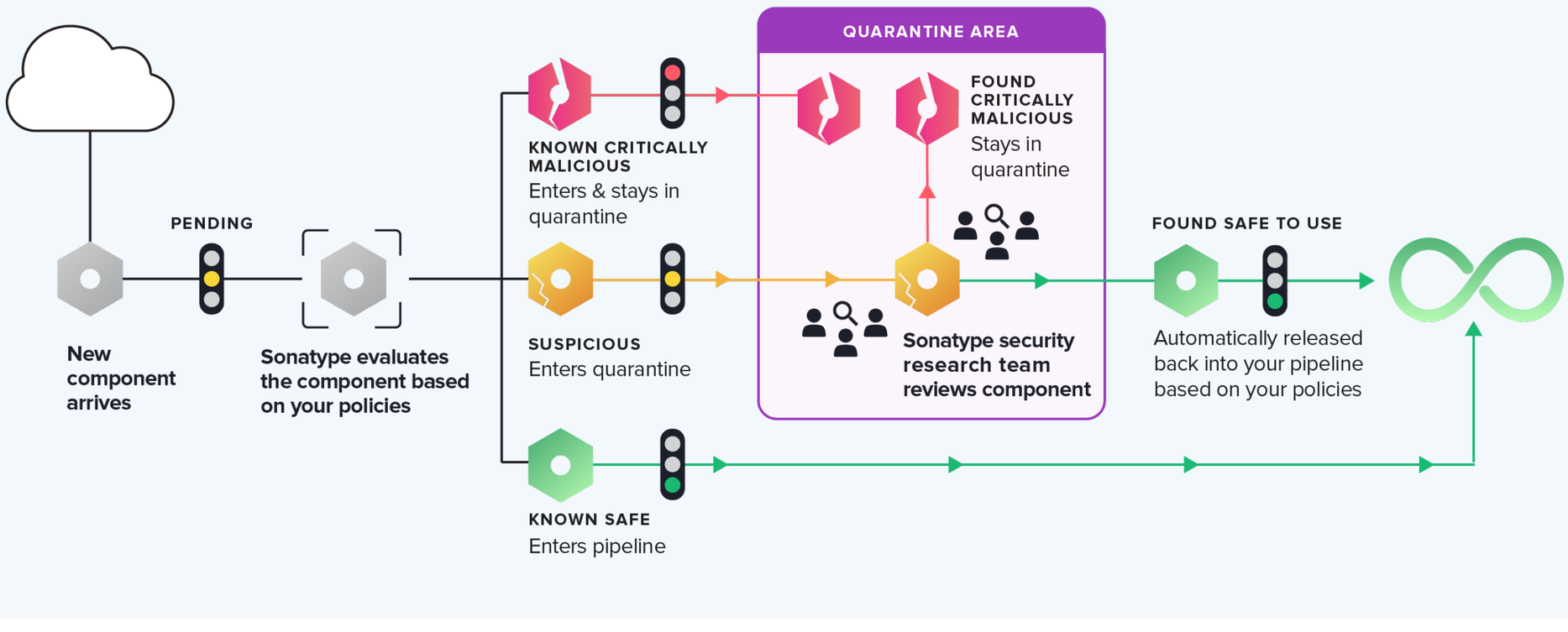
Cybercrime and adversaries are getting craftier and more sophisticated with their attacks. Looking at the state of open source projects today, 21,000+ new versions of OSS libraries are being released per day. Supply chain/malware attacks are on the rise with no chance of slowing down.

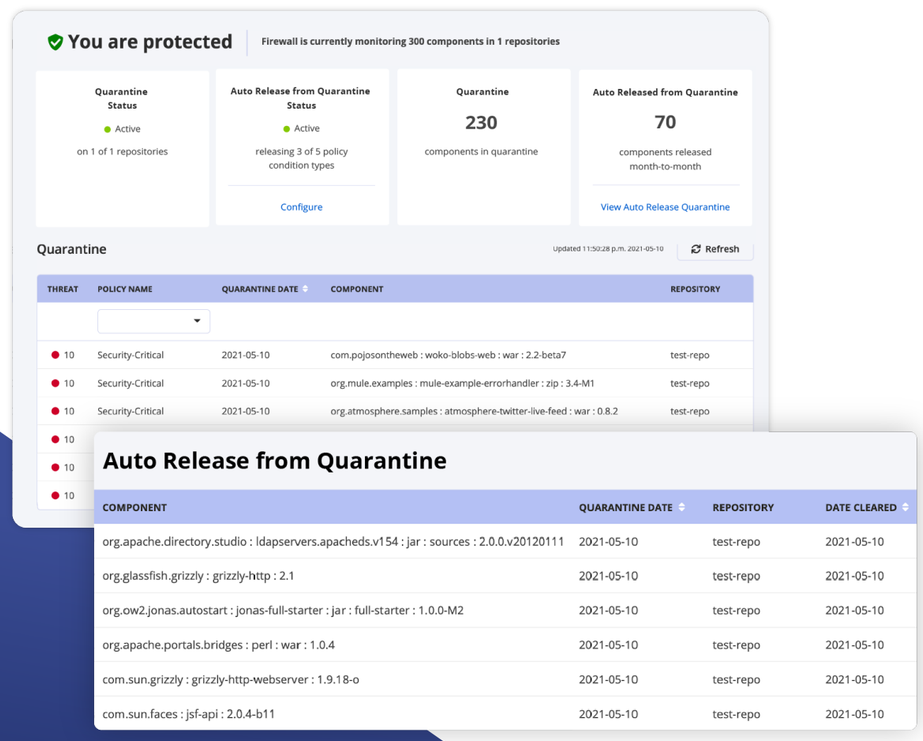
While hackers used to wait for public vulnerability disclosures to exploit in the wild, they're now proactively manufacturing vulnerabilities and publishing these into repositories — the most popular being the npm repository.

How can organizations combat these supply chain attacks that continue to grow in sophistication? It's more than auditing your repositories for vulnerabilities.

To truly get ahead of supply chain attacks, you must block vulnerable open source packages before they are downloaded into your repository. Nexus Firewall does this for you, providing an early warning detection system to prevent the download of critically malicious and suspicious/unverified risk from entering your SDLC.

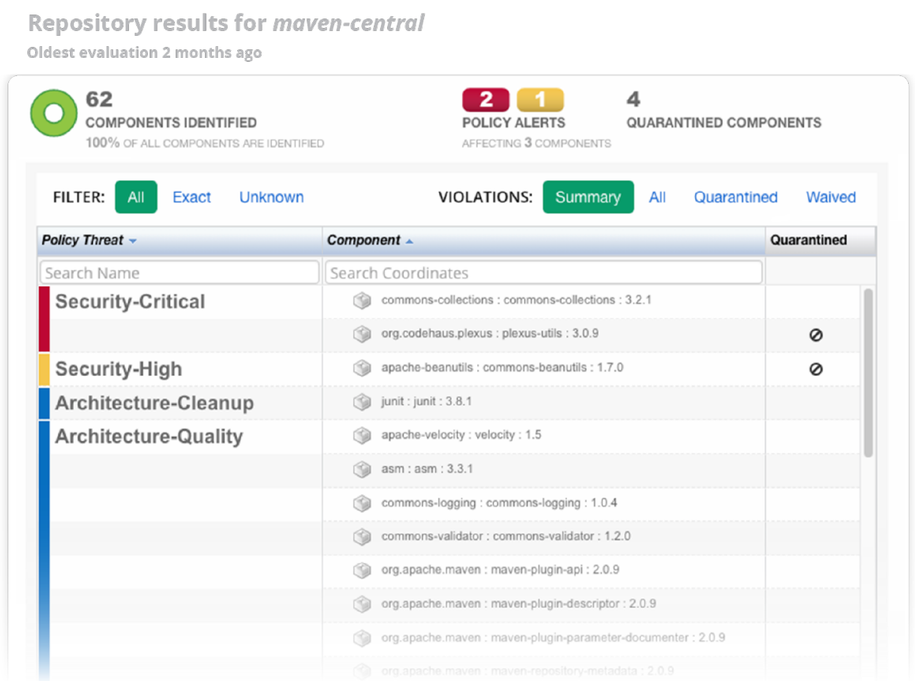
RELEASE INTEGRITY WITH NEXUS FIREWALL: POWERED BY NEXUS INTELLIGENCE





Block Critically Malicious Components and Suspicious npm Packages

Decrease the risk of a security breach by automatically blocking known vulnerabilities and harmful OSS releases from downloading into your repository or quarantining suspicious releases from the npm repository. Our ML/AI identifies threats based on different behaviors and marks them "Normal", "Suspicious", or "Malicious". Critically malicious components are always blocked, and those npm packages deemed suspicious are blocked until they're confirmed or cleared by Sonatype's security research team. If cleared, then it can be automatically quarantined or released into your development pipeline based on your policy.



Create and Enforce Policy Rules

Decide which components are allowed into your SDLC based on common risk factors, including age, popularity, and licensing credentials. From there, configure policy actions to automatically prevent applications from moving forward with unwanted or unapproved components.

Language Coverage

Nexus Firewall proactively prevents known risk from Java, Ruby, .NET, Python Go, RPM and more, as well as unknown risk from JavaScript.

JFrog ARTIFACTORY

nexus repository

Universal Repository Support

Available for Nexus Repository OSS and PRO, and JFrog Artifactory

Key Benefits of Nexus Firewall

Early identification and warning against freshly detected suspicious components within hours of release from the npm repository.

Automatic protection against known critically malicious components.

When combined with Nexus Lifecycle, avoid recommended versions that are marked as suspicious.

sonatype

Sonatype is the leader in developer-friendly, full-spectrum software supply chain management providing organizations total control of their cloud-native development lifecycles, including third-party open source code, first-party source code, infrastructure as code, and containerized code. The company supports 70% of the Fortune 100 and its commercial and open source tools are trusted by 15 million developers around the world. With a vision to transform the way the world innovates, Sonatype helps organizations of all sizes build higher quality software that's more aligned with business needs, more maintainable, and more secure.

Sonatype has been recognized by Fast Company as one of the **Best Workplaces for Innovators** in the world, two years in a row and has been named to the Deloitte Technology Fast 500 and Inc. 5000 list for the past five years. For more information, please visit **Sonatype.com,** or connect with us on **Facebook, Twitter,** or **LinkedIn.**