



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.

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.**

The diagram illustrates the Sonatype component evaluation pipeline. It starts with a cloud icon representing a new component arriving. This leads to a 'PENDING' state, shown as a grey hexagon with a traffic light. The next step is 'Sonatype evaluates the component based on your policies', represented by a bracketed grey hexagon. From here, the pipeline branches into three paths:

- KNOWN CRITICALLY MALICIOUS:** A red path with a red lightning bolt icon and a red traffic light. The component enters and stays in quarantine.
- SUSPICIOUS:** An orange path with a yellow lightning bolt icon and a yellow traffic light. The component enters quarantine.
- KNOWN SAFE:** A green path with a green hexagon icon and a green traffic light. The component enters the pipeline.

The 'QUARANTINE AREA' is a purple box containing the 'Sonatype security research team reviews component' step, represented by a yellow hexagon with a magnifying glass icon. Components in the 'KNOWN CRITICALLY MALICIOUS' and 'SUSPICIOUS' paths enter this area. From the quarantine area, two outcomes are possible:

- FOUND CRITICALLY MALICIOUS:** A red path with a red lightning bolt icon and a red traffic light. The component stays in quarantine.
- FOUND SAFE TO USE:** A green path with a green hexagon icon and a green traffic light. The component is automatically released back into the pipeline based on policies.

The final step is a green infinity loop, indicating the component is back in the pipeline.



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.

## Repository results for maven-central

Oldest evaluation 2 months ago

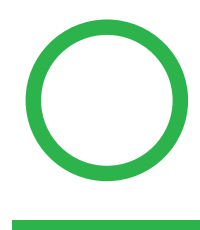
<b>62</b> COMPONENTS IDENTIFIED 100% OF ALL COMPONENTS ARE IDENTIFIED	<b>2</b> POLICY ALERTS AFFECTING 3 COMPONENTS	<b>4</b> QUARANTINED COMPONENTS
FILTER: <b>All</b> Exact Unknown VIOLATIONS: <b>Summary</b> All Quarantined Waived		
Policy Threat	Component	Quarantined
Search Name	Search Coordinates	
<b>Security-Critical</b>	commons-collections : commons-collections : 3.2.1	
	org.codehaus.plexus : plexus-utils : 3.0.9	
<b>Security-High</b>	apache-beanutils : commons-beanutils : 1.7.0	
<b>Architecture-Cleanup</b>	junit : junit : 3.8.1	
<b>Architecture-Quality</b>	apache-velocity : velocity : 1.5	
	asm : asm : 3.3.1	
	commons-logging : commons-logging : 1.0.4	
	commons-validator : commons-validator : 1.2.0	
	org.apache.maven : maven-plugin-api : 2.0.9	
	org.apache.maven : maven-plugin-descriptor : 2.0.9	
	org.apache.maven : maven-plugin-parameter-documenter : 2.0.9	
	org.apache.maven : maven-repository-metadata : 2.0.9	

## 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](https://www.sonatype.com), or connect with us on [Facebook](#), [Twitter](#), or [LinkedIn](#).