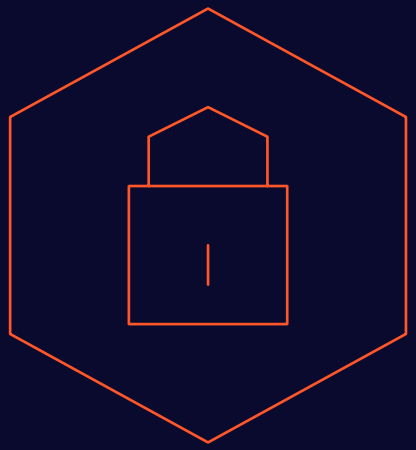
sonatype

Best Practices for Safe and Compliant Open Source Use

Start secure, stay fast — no bad components, no wasted cycles, just better builds.

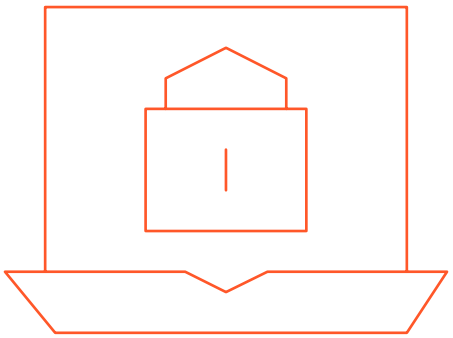


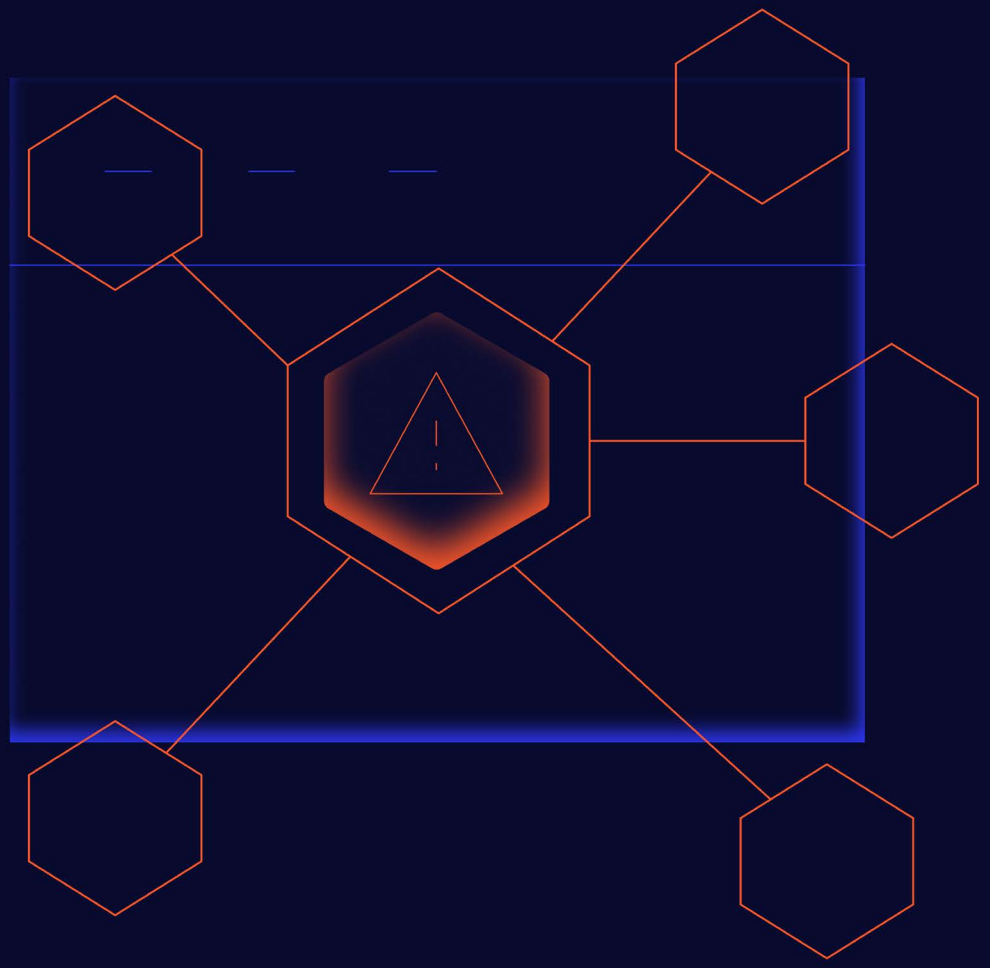
Introduction

Modern software development thrives on speed, efficiency, and innovation—fueled by the rapid adoption of open source components, including a growing number of AI and ML models. But as usage scales, so do the risks. Teams face a wide spectrum of issues: from insecure or outdated packages, to license violations, to malicious code intentionally embedded in open source components and AI models. These risks often enter through routine development workflows—via proxy repositories, automation, or direct downloads—without clear visibility or controls.

Security incidents aren't the only concern. Unapproved or non-compliant components create downstream friction, slow delivery cycles, and increase the burden on developers to fix issues late in the process. Relying on manual review or post-ingestion scanning makes it harder to scale securely without impacting velocity.

To stay ahead, engineering leaders are turning to policy-compliant components—a proactive approach to enforcing security, licensing, and operational standards at the point of ingestion. Policy compliant components give teams the guardrails they need to move fast with confidence, while protecting the integrity of the software supply chain.





Securing Your Proxy Repository

Creating a secure, efficient development environment starts with governance over the repositories developers depend on. Effective proxy repository security ensures developers can move fast without introducing risk.

Centralized Management with Repository Manager:

- Use Sonatype Nexus Repository Manager to centralize control of open source libraries, including AI/ML models, container images and general-purpose components.
- Cache and store vetted components and models locally, reducing risk and eliminating surprises from transitive dependencies or namespace collisions.
- Enforce access controls and governance to maintain uniform security policies across all teams and services.
- Schedule automated tasks to scan and remediate existing artifacts that may violate compliance policies or pose security threats.

sonatype
nexus
repository

Enforcing Your Organization's Risk Tolerance

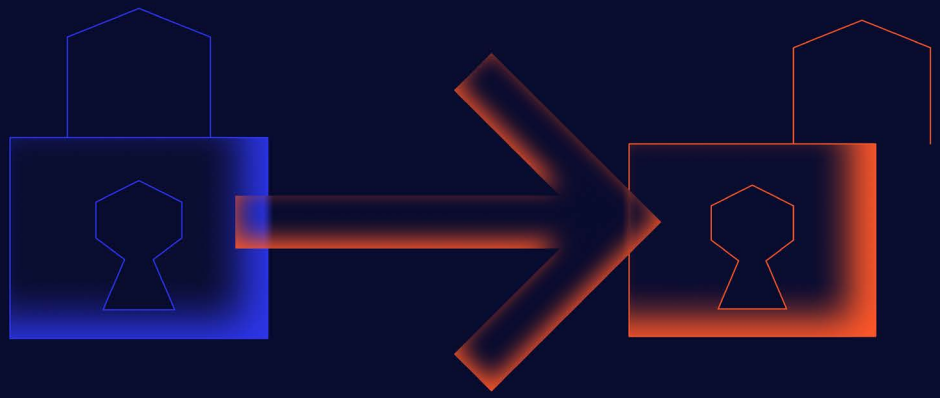
Repository Firewall Policy Enforcement

Configure Repository Firewall to enforce your organization's specific tolerance for risk at the proxy level. This includes quarantining or blocking components based on:

- **Security-Malicious:** to block components with known malicious intent.
- **Integrity-Rating:** to quarantine components under review for potential threats.
- **Security-Critical:** to restrict components with vulnerabilities scoring 9 or higher on CVSS.
- **License-Banned:** to avoid components with prohibited licenses that pose legal and financial risks.
- **Policy-Compliant Component Selection (PCCS):** to ensure only approved versions of components are downloaded.
- **Namespace Confusion Protection:** to prevent attacks exploiting namespace collisions.

Start with permissive policies that allow critical builds to proceed using existing dependencies while blocking malicious risks. Then progressively tighten controls to minimize disruption while improving security posture.

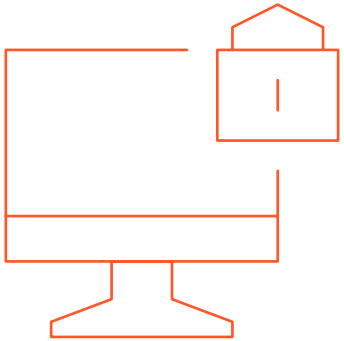
sonatype
repository
firewall



Integrating Perimeter Security

Modern development teams often pull packages outside of managed systems—especially when exploring new open source tools or AI frameworks. Integrating your policy framework with perimeter defenses is critical to stopping unapproved components at the edge..

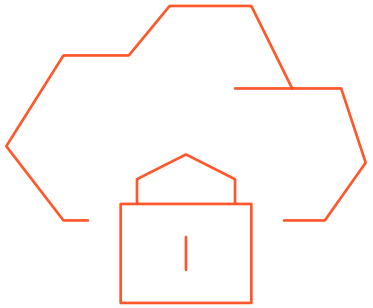
- **Network-Level Malware Blocking:**
  - Integrate Repository Firewall with perimeter security tools such as Zscaler to extend malware blocking to the network edge.
- **Malware Intelligence API Integration:**
  - Embed Sonatype's Malware Intelligence API into your security workflows for real-time, automated malware checks across your CI/CD pipeline and perimeter tools.



Educating Teams and Streamlining Security Enforcement

Policy enforcement must be automatic and consistent—but clear communication and streamlined processes help reduce confusion, accelerate adoption, and keep development moving efficiently.

- **Team Education and Awareness:**
  - Emphasize that policies are enforced automatically and consistently—education supports understanding, not enforcement.
  - Deliver regular enablement sessions that explain risks tied to policy violations (e.g., legal, security, rework costs).
  - Highlight the increasing risks around open source AI/ML models, including embedded malware, malicious datasets, or non-permissive licenses.
  - Reinforce how policies protect developers by reducing downstream rework and bottlenecks.
- **Defining and Communicating the Waiver Process:**
  - Establish and communicate a clear waiver process for components blocked by enforcement.
  - Inform developers about key contacts, how to request a waiver, and expected response timelines to streamline resolution.
  - Scope waivers broadly when appropriate (e.g., across version ranges or component families) to reduce repeated interruptions caused by frequent updates.



Conclusion

Delivering secure software at speed means more than blocking threats—it requires giving developers a clear path forward using components that are trusted, approved, and compatible with organizational goals.

By shifting your focus to policy-compliant components, and by integrating repository controls with perimeter defenses, you can proactively manage risk while enabling engineering velocity. These best practices create scalable safeguards across your software supply chain—whether you're shipping microservices, mobile apps, or AI-enabled systems.

Stay productive. Stay compliant. Stay secure.

For a personalized demo, please visit **www.sonatype.com/request-a-personalized-demo**

sonatype

Sonatype is the leader in secure software development built on open source and AI. As the maintainers of Maven Central and creators of Nexus Repository, Sonatype has spent two decades pioneering how the world manages and secures open source software — making Sonatype the trusted authority for modern software supply chains. With unmatched open source visibility and a unified product suite built for modern software development, Sonatype gives enterprises the intelligence and automated governance they need to harness the full potential of open source and AI. Sonatype handles the complexity behind the scenes: guiding component and model selection, blocking harmful malicious code, automating dependency and vulnerability management, and ensuring faster, more reliable builds — so developers spend more time on innovation and less time on remediation and rework. Trusted by more than 15 million developers, Sonatype helps power secure, modern software development at nearly 2,000 global organizations including 70% of the Fortune 100. To learn more about Sonatype, please visit www.sonatype.com