Sonatype

SOLUTION OVERVIEW

NEXUS FIREWALL

Nexus Firewall provides an innovative solution to block undesirable components from getting into your software at the earliest possible point: the repository manager where developers source components. Now you can automate otherwise manual, human reviews and 'golden repository' strategies in order to keep pace with the speed of today's development practices. With Nexus Firewall you can shield your application development from waste and risk by automatically and continuously blocking these unacceptable software components inbound and preventing release of applications containing such components outbound. Nexus Firewall goes beyond blocking, providing organizations with the visibility and data needed to make ideal decisions for open source component selection early, significantly reducing risk, unplanned work and technical and security debt.

WHY IS NEXUS FIREWALL NEEDED?

Seventy-five percent of organizations admit to not having meaningful controls over what open source and third party components are used in their applications.[1] This can result in quality and licensing issues or security vulnerabilities that create technical debt and operational risk. In fact, recent research shows that one in 13 components downloaded from the Central Repository include known vulnerabilities.[2]

To ensure the highest quality components are available to development teams, some organizations have turned to "golden repository" strategies where components must be requested and manually approved in accordance with open source policies before being put in a repository manager for use by development teams. The repository manager then acts as a local parts warehouse (i.e., golden repository) of approved components.

Scaling a manual approach is an enormous challenge, often ineffective, and certainly suboptimal given the availability of an automated solution. The typical volume and velocity of open source component consumption far outpaces the ability to manually review every new component request in a timely way. Proper review of version, license, and security vulnerability information can take hours for each component. This creates upstream delays which ultimately impact productivity, lead to "creative" work-arounds, and increase development costs.

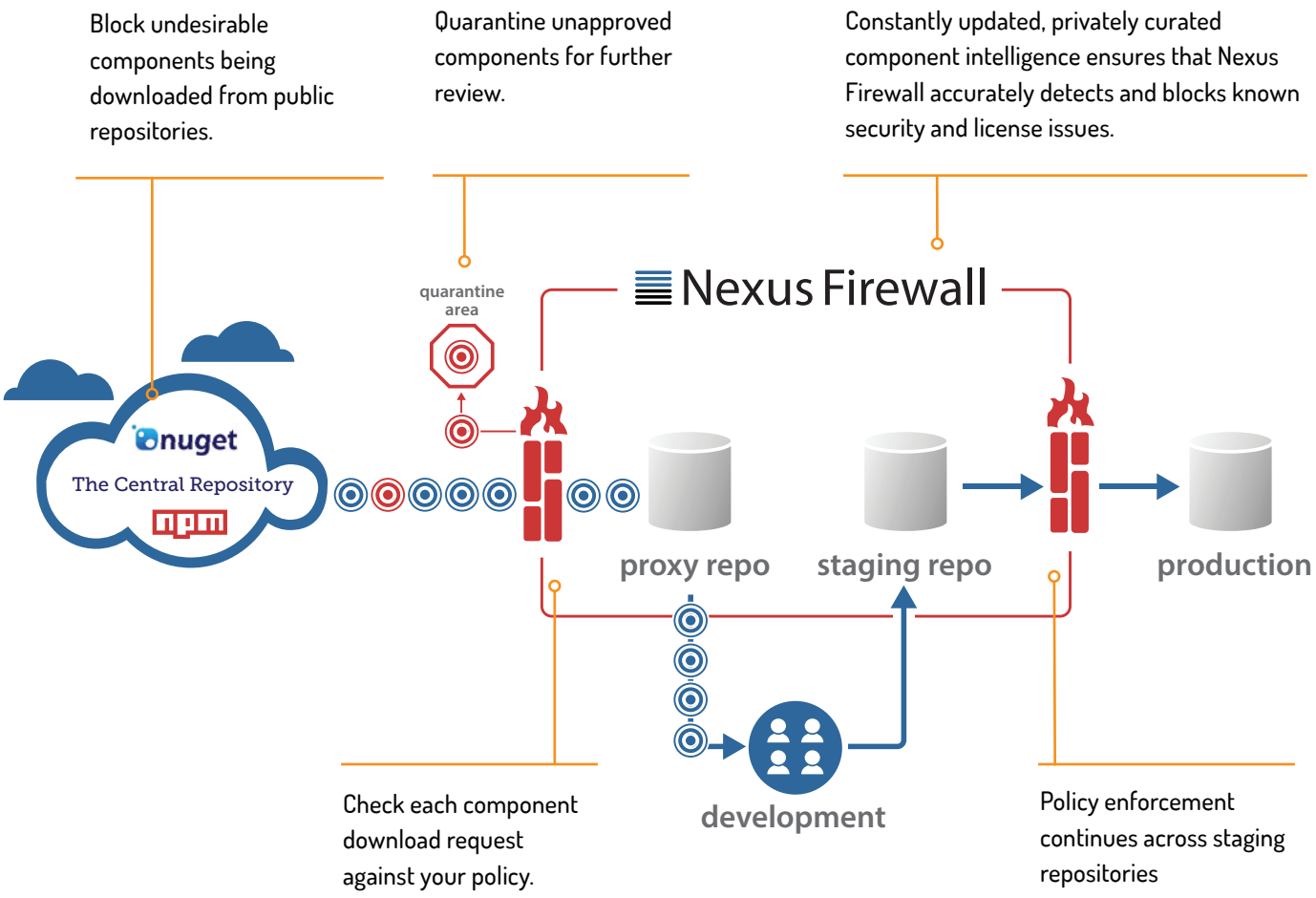
Keeping pace with modern development

To keep pace with the volume of component download requests (development organizations each requested an average of 240,000 components in 2014[3]), Nexus Firewall uses automated policies to perform a real-time assess-

[1] Source: 2014 Sonatype Open Source Development survey
[2] Source: Sonatype analysis of Application Health Checks
[3] Source: Based on Sonatype's analysis of downloads from (Maven) Central Repository

ment of components. This happens before they enter your repository based on security, license and quality attributes that are established in advance. Components that meet these standards are automatically delivered with the speed and timeliness development teams expect and need. Those that do not are held in quarantine and blocked from further use. Performing this validation at "line speed" ensures the right components are being used without introducing unnecessary delays. Most importantly, organizations avoid the risk associated with using the wrong components.

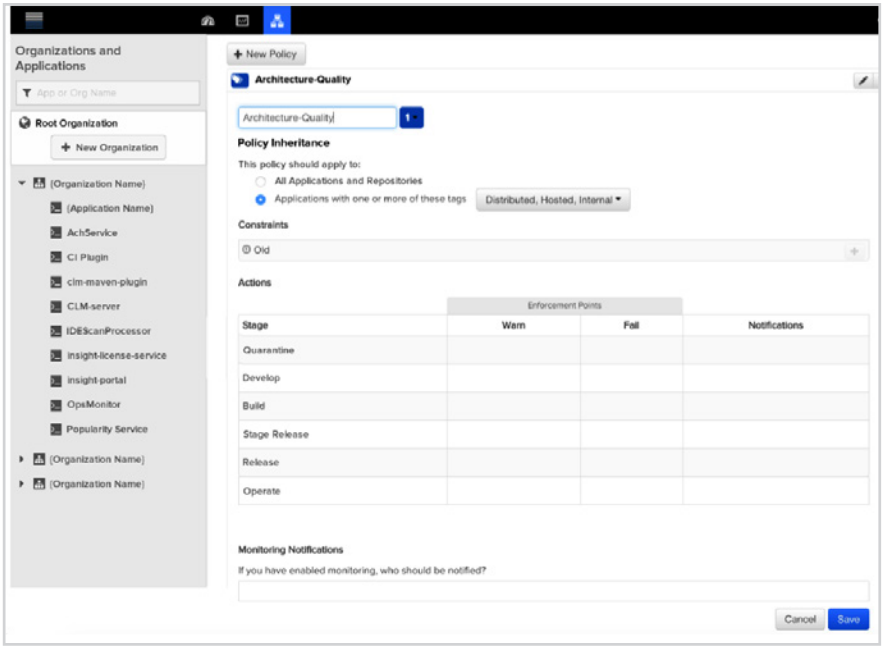
FEATURE	EXPLANATION	BENEFIT
Customizable out-of-the-box policies	• Leverage a set of pre-defined policies that alert you when newly requested open source and third party components are out of compliance. In addition to generating alerts, policies can be established to block access to undesirable components. • Policies can be customized to enforce a variety of use cases including preventing access to components that are out of date, contain restrictive licenses, or include known security vulnerabilities.	• Establish a first line of defense in your software supply chain. • Replace paper-based open source policies with automated policies. • Automate compliance by leveraging attribute-based policies and real-time component intelligence to eliminate the need for manual reviews of all components.
Continuous monitoring	• Ensure continuous visibility of components being downloaded to your repository manager. Every component download request is accurately and automatically identified and checked against the policy.	• Replace the burden of manual workflows and reviews. • Eliminate hours of investigation for licenses, versions, and vulnerabilities for thousands of components.
Continuous enforcement	• Components that are recognized as out of compliance are quarantined within the repository manager, pending further reviews aided by detailed violation data. • Components not meeting policy standards will not be made available to developers or tools originating the request. • After passing through the initial download checkpoint, enforcement of policies continues across staging repositories with Nexus Firewall.	Developers are alerted immediately if a component does not meet policy guidelines, eliminating days or weeks of wait time for developers who once relied on manual investigations and approvals.
Continuous intelligence	Sonatype's real-time IQ Data Services deliver constantly updated component intelligence based on proprietary curation of vulnerability, license, version and other data from numerous sources. The curation process reduces false positive alerts and speeds remediation with better root cause indications.	Component research is done for you and is always up to date, eliminating hours of manual research once required for component approvals.
Continuous reporting	The repository audit report of Nexus Firewall lists the compliance status of all components housed in the repository manager, allowing you to audit your repository.	Once components being downloaded are approved by Nexus Firewall, there is always a chance that a new vulnerability for that artifact may be discovered. Repository audit reports are updated continuously with the latest research intelligence.



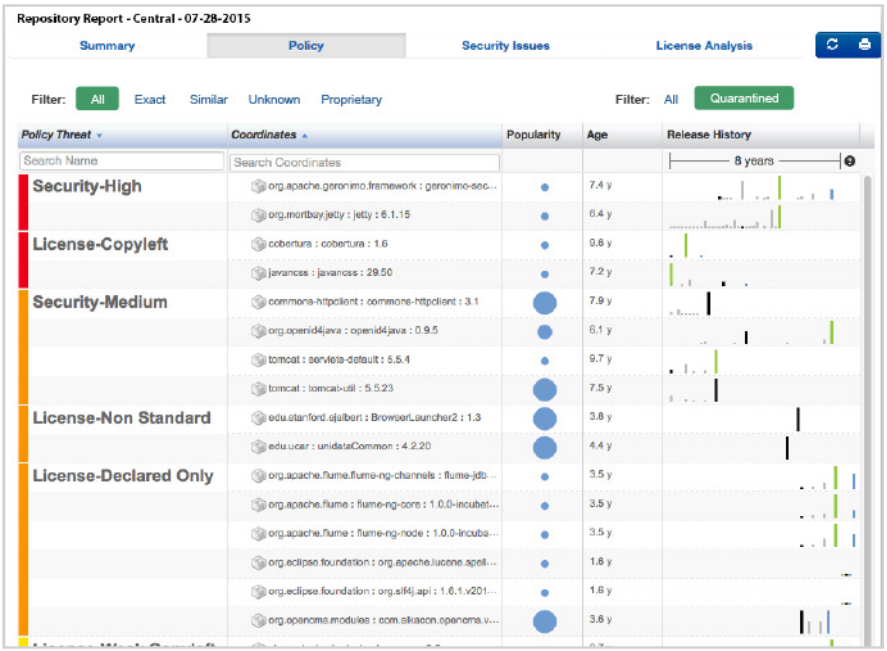
NEXUS SOLUTIONS AT-A-GLANCE

Nexus Firewall is one of Sonatype's Software Supply Chain Automation solutions and features the Sonatype IQ Server. To meet the needs and priorities of all organizations, Sonatype offers different integration points so that component intelligence and policy management can be leveraged in different ways across the life cycle. Please use the chart below to compare our various solutions, or for more detailed information go to www.sonatype.com/nexus/try-compare-buy/compare

	Repository Management	Software Supply Chain Automation							
	Repository Manager	IQ Server	Key Integration Points				Additional Integrations		
	Full-featured component warehouse & distribution manager	*Software supply chain intelligence & policy management*	*Repository*	*IDE*	*CI Server*	*Staging/ Release*	*SonarQube*	*Command Line (CLI)*	*Custom (API)*
Nexus Repository	●								
Nexus Auditor		●						●	
Nexus Firewall		●	●			●			
Nexus Lifecycle		●		●	●	●	●	●	●



Automate policies to ensure developers use the highest quality components from the start and replace the burden of manual reviews.



Audit reports can identify which components triggered policy violations and were quarantined by Nexus Firewall. The reports also provide data to help further refine and strengthen policies.

NEXT STEPS

Use Nexus Firewall as a front line defense to shield your repository from undesirable components and dramatically increase your visibility of component usage across your organization. If you want full control of component usage across the software life cycle, a defense-in-depth strategy is possible with Nexus Lifecycle. www.sonatype.com

Sonatype Inc. • 8161 Maple Lawn Blvd, Suite 250 • Fulton, MD 20759 • 1.877.866.2836 • www.sonatype.com