




 Sonatype

EVOLVE FASTER THAN THE THREAT

PROTECT OPEN SOURCE
IN MISSION CRITICAL
APPLICATIONS

Introduction

Agencies that are not evaluating, monitoring, and tracking the use open source and third-party application components within the scope of their Risk Management Framework (RMF) Assessment and Authorization processes, are exposing themselves to significant and elective risks. Open source and third-party components are the foundation of mission-critical applications in Government, but often contain cyber security vulnerabilities that represent a large and fast-expanding attack surface for adversaries.



“It is estimated that 90% of a typical application is comprised of open source components.”


Open source components have become a favorite target for cyber adversaries since they are a highly efficient gateway. A single open source component may be embedded in hundreds or even thousands of applications; a stunning force multiplier. Instead of launching a single attack on a single application, it is now common to target a vulnerable open source component to potentially compromise thousands of applications.

To address today’s threats and to achieve the objectives of the NIST Risk Management Framework (RMF), agencies need a method to technically govern the use of open source software. To avoid becoming a soft target and falling into the trap set by bad actors, agencies must take new approaches to ensure open source components are of the highest quality and free from known vulnerabilities that put their missions, their data, and their IT assets at risk.

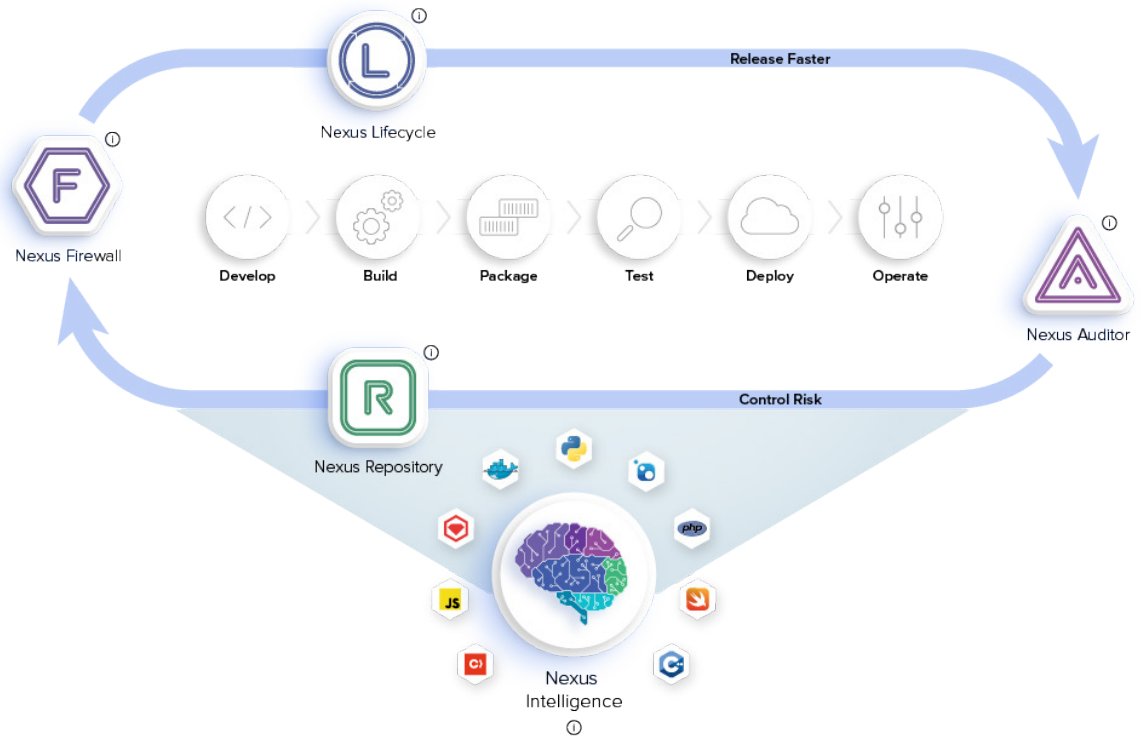


“Suspected or known open source breaches increased 55% YoY.”

Sonatype’s Nexus Platform is a DevOps-native solution that uses Advanced Binary Fingerprinting to precisely identify vulnerable components (including partially modified components / matches), enabling agencies to govern and track open source components underpinning mission critical applications. Armed with this intelligence, information security architects define automated controls to restrict the use of known vulnerable open source components. By automating RMF security objectives, agencies can operate at the speed of mission and significantly accelerate system delivery and continuous security.



“Research shows a single development team within a federal agency or a large government contractor might consume 200,000 open source and third-party software components each year to accelerate application development.”



The Nexus Platform automates open source governance at scale across every phase of the SDLC and includes:

- **Nexus Firewall** – automatically blocks vulnerable components from entering the software supply chain.
- **Nexus Lifecycle** – continuously identifies and monitors risk across the entire pipeline.
- **Nexus Auditor** – examines production apps and automatically creates a software bill of materials.
- **Nexus Repository** – stores and manages open source components, binaries, and build artifacts across every phase of the SDLC.
- **Nexus Intelligence** – fuels the Nexus Platform with precise and actionable intelligence curated by expert researchers.

"Public vulnerability databases lack information on more than 1.3 million open source security advisories."

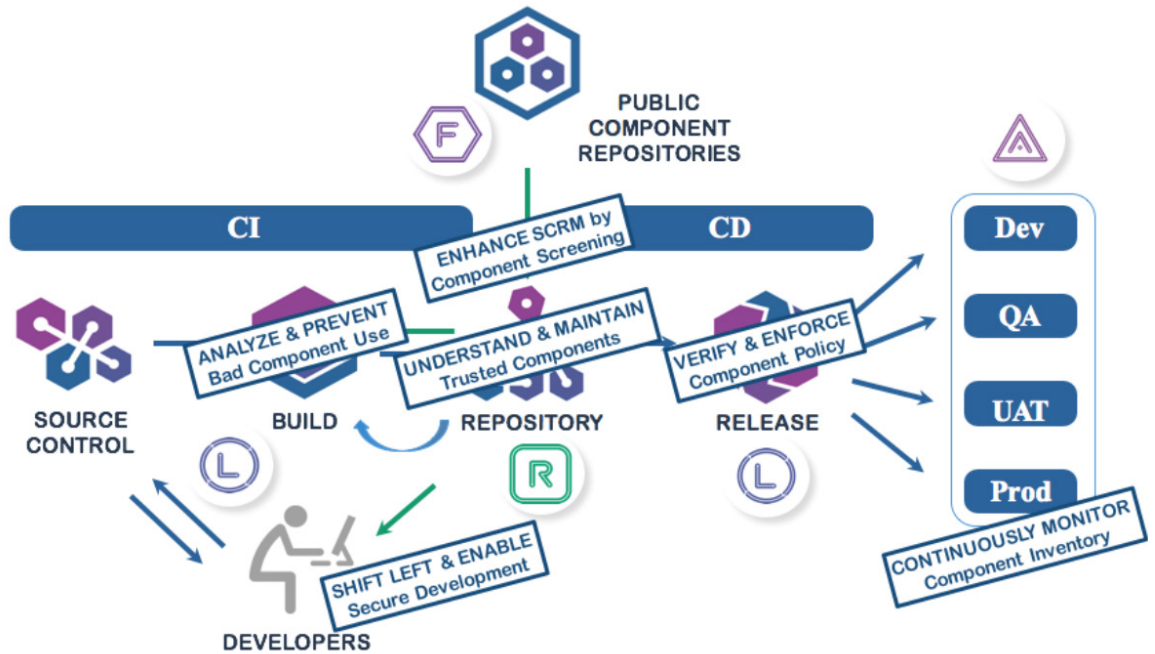
Maximize the use of automation. Prevent problems before it's too late.

Precise identification of components makes it possible to automate the discovery and remediation of vulnerabilities, allowing oversight teams to keep pace with development and eliminate the need for costly manual component reviews, saving time for developers. Policies in Nexus Lifecycle detail the threat level, constraints, conditions, actions and notifications that will be automated. For example, a policy might be added to prevent a developer from using any open source component with a CVSS score between 7 and 10. When this policy is added to a Jenkins server, the resulting action could break the build and/or notify the appropriate personnel of the violation. Policies can also be used to help developers evaluate safer, alternative component choices. This type of frictionless feedback increases quality and decreases the time and cost of ATO significantly.

Security assessment teams having the CVEs and the CVSS score during the testing process is not enough; developers need to have access to component intelligence in a frictionless manner. Infusing open source intelligence early and often in the SDLC will empower information system developers to select only secure components. Shifting security practices left reduces late stage costs, building security into system design. Automating open source policies and making component intelligence available in the IDE, enables the efficient delivery of security objectives.

The Nexus Platform maintains a complete inventory of components used in development to produce a software Bill of Materials (BoM) for each application. Security assessment reports can be automatically created, precisely identifying all open source and third-party components used during design, build, and release. The Nexus Platform provides a dashboard view to continuously monitor policy violations that have been discovered and identifies those pending further investigation. Assessing security policy compliance is straight-forward for program owners, development managers, and independent security teams.

"DevOps teams are 90% more likely to comply with open source governance when policies are automated."



 Nexus Repository
  Nexus Firewall
  Nexus Lifecycle
  Nexus Auditor

The Nexus Platform is a key RMF control provider for Government programs using open source and third party components, providing automated methods to enhance the security posture for controls in Configuration Management, System and Service Acquisition, System and Information, Risk Assessment, and Incident Response.

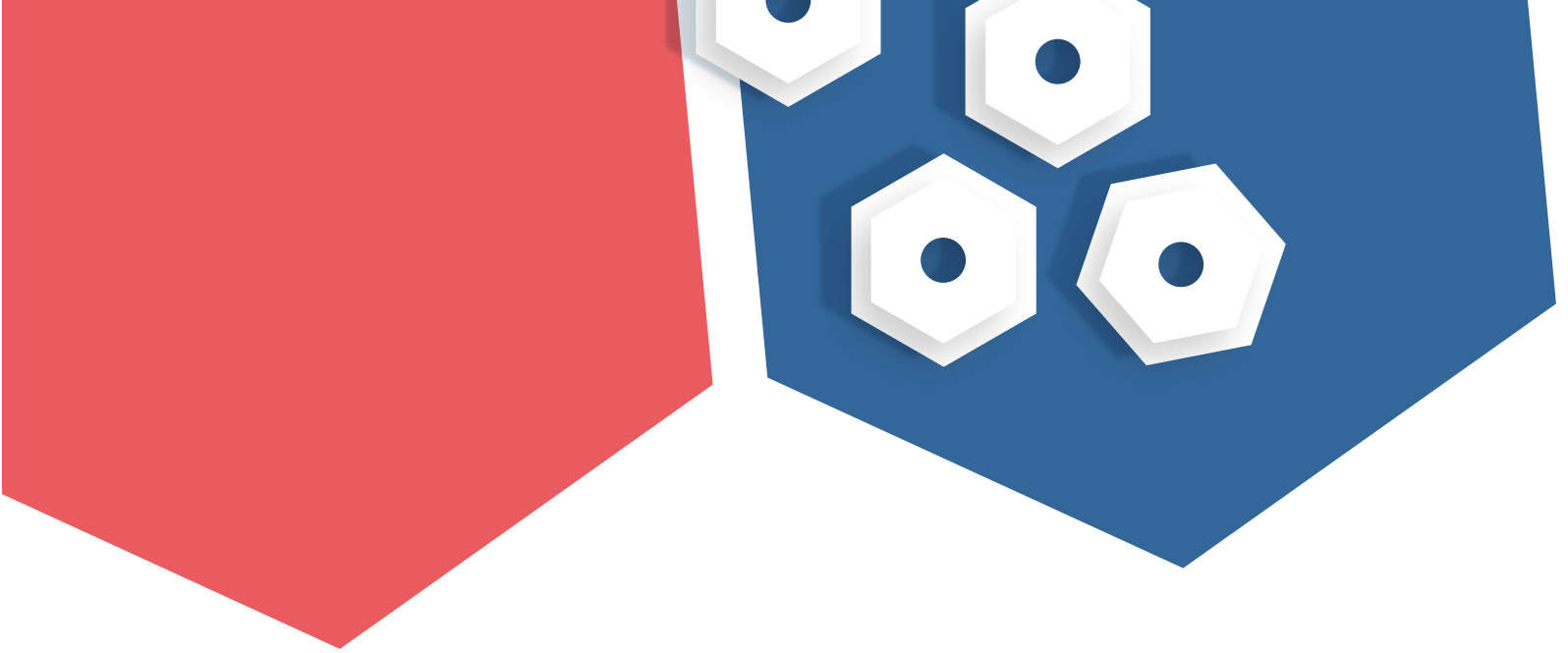
Conclusion

Open source usage is massive and it continues to grow exponentially. According to a recent study¹, 87 billion Java open source components were downloaded from the Central Repository in 2017. While open source usage fuels innovation and speeds time to mission, it does come with some inherent risk. In the same study, Sonatype researchers discovered that 12.1% of those Java downloads contained known security vulnerabilities, a 120% year-over-year increase.

"Open source vulnerabilities increased 120% YoY and their mean time to exploit compressed 93%."

The good news is that there are solutions to automate open source governance at scale across the software development lifecycle. From blocking risky components at the front door, to providing precise component intelligence within the developer's IDE, to continuously monitoring applications in production, Nexus is used by government agencies to mitigate risk in support of the RMF guidelines.

¹2018 State of the Software Supply Chain, Sonatype



More than 10 million software developers rely on Sonatype to innovate faster while mitigating security risks inherent in open source. Sonatype's Nexus platform combines in-depth component intelligence with real-time remediation guidance to automate and scale open source governance across every stage of the modern DevOps pipeline. Sonatype is privately held with investments from TPG, Goldman Sachs, Accel Partners, and Hummer Winblad Venture Partners. Learn more at www.sonatype.com

Headquarters

8161 Maple Lawn Blvd, Suite 250
Fulton, MD 20759
United States – 1.877.866.2836

European Office

1 Primrose Street
London EC2A 2EX
United Kingdom

APAC Office

5 Martin Place, Level 14
Sydney 2000, NSW
Australia

Sonatype Inc.

www.sonatype.com
Sonatype Copyright 2018
All Rights Reserved.