



**Nexus Intelligence**  
Precise data for automated open source governance

Public databases like GitHub provide a valuable initial and ongoing outside view of open source security vulnerabilities, licenses, and architectural risks. Our data collection engine has ingested and analyzed more than 60 million components and over one billion lines of code (including all public GitHub repositories) to identify and analyze open source project updates to advisory notices, license changes, CVE notices, and a plethora of vulnerability data.

Nexus Intelligence powers the Nexus Platform with precise data to automate open source governance at scale across every phase of the SDLC.

**Discovering Pro**  
Identify license, build artifacts, and other metadata across the SDLC.

**Build**  
Leverage continuous security risk, vulnerability, and compliance information across every phase of your SDLC.

**Package**  
Leverage OSS vulnerability and provenance information.

**Deploy**  
Leverage OSS vulnerability and provenance information.

**Operate**  
Leverage OSS vulnerability and provenance information.

**Nexus Intelligence**  
Superior open source data services continuously refined by AI, machine learning, and 60 world class researchers power our products.

**Analyze: What's Deployed, Versus What's Declared**  
Alternative tools are prone to false positives and negatives because they scan apps "as declared" and trust developers to disclose the truth about dependencies embedded in software.

Nexus scans apps "as deployed" utilizing Advanced Binary Fingerprinting (ABF). The result is precise read on embedded dependencies and is Software Bill of Materials (SBOM) that reflects the truth about the deployed file.


www.sonatype.com


# Sonatype Intelligence

## Sonatype Whitepaper


Thank you for downloading this Sonatype resource! Carahsoft serves as the Master Government Aggregator and Distributor for Sonatype, offering expertise in government procurement processes and practices with purchasing available via GSA, SEWP V, The Quilt and other contract vehicles.


To learn how to take the next step toward acquiring Sonatype solutions, please check out the following resources and information:


 For additional resources:  
[carah.io/SonatypeResources](https://carah.io/SonatypeResources)

 For upcoming events:  
[carah.io/SonatypeEvents](https://carah.io/SonatypeEvents)

 For additional solutions:  
[carah.io/SonatypeProducts](https://carah.io/SonatypeProducts)

 For additional Open Source solutions:  
[carah.io/OpenSourceSolutions](https://carah.io/OpenSourceSolutions)

 To set up a meeting:  
[Sonatype@Carahsoft.com](mailto:Sonatype@Carahsoft.com)  
(877)-742-8468

 To purchase, check out the contract vehicles available for procurement:  
[carah.io/SonatypeContracts](https://carah.io/SonatypeContracts)

# Nexus Intelligence

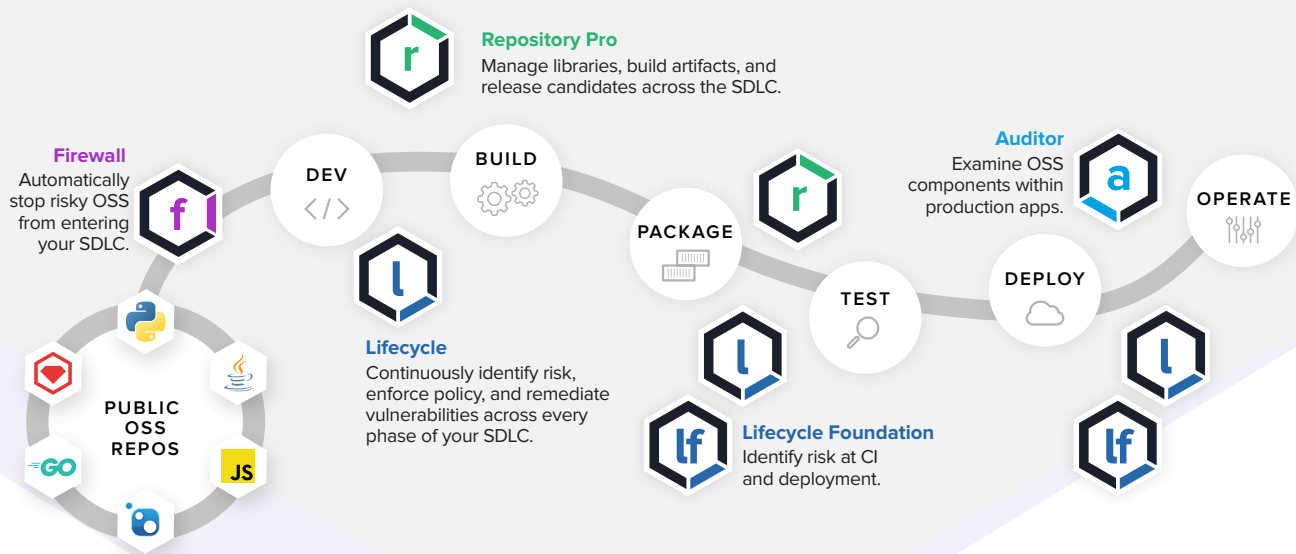
## Precise data for automated open source governance

Public databases like NVD provide a relatively small and typically outdated view of open source security vulnerabilities. Nexus Intelligence delivers a universal and timely understanding of open source security, license, and architectural risk. Our data collection engine has ingested and analyzed more than 65 million components and never stops learning — using natural language processing and AI to dynamically monitor every GitHub commit to every open source project, updates to advisory websites, Google search alerts, OSS Index, and a plethora of vulnerability sites.

Nexus Intelligence powers the Nexus Platform with precise data to automate open source governance at scale across every phase of the SDLC.

“The data quality is really good. They’ve got the best in the industry, [and] it helps us to resolve problems faster. The visibility of the data, as well as their features that allow us to query and search — and even use it in the development IDE — allow us to remediate and find things faster.”

— RUSSELL WEBSTER  
(Financial Services),  
IT Central Station Review



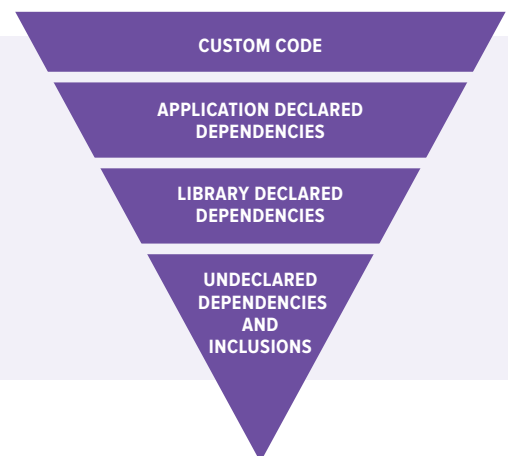
### Nexus Intelligence

Superior open source data service continuously refined by AI, machine learning, and 65 world class researchers powers our products.

### Analyze What's Deployed, Versus What's Declared

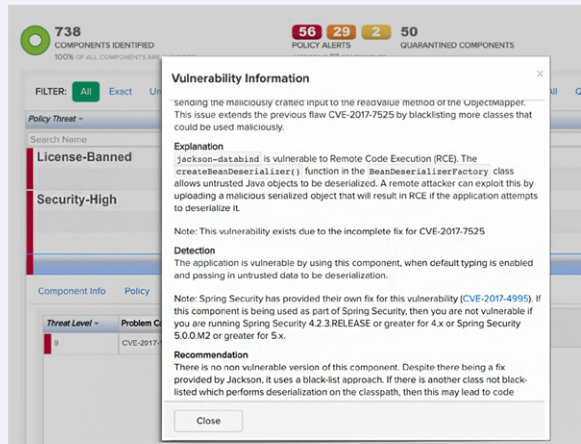
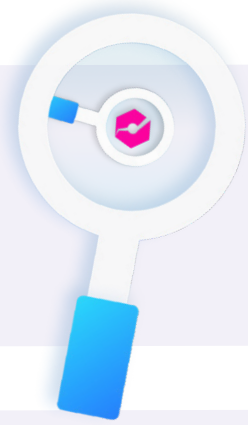
Alternative tools are prone to false positives and negatives because they scan apps “as declared” and trust developers to disclose the truth about dependencies embedded in software.

Nexus scans apps “as deployed” utilizing Advanced Binary Fingerprinting (ABF). The result is a precise read on embedded dependencies and a Software Bill of Materials (SBOM) that reflects the truth about third-party risk.



## Go Above and Beyond Public Data with Secondary Expansion

Nexus Intelligence is the only data security research service that actively practices “secondary expansion,” an extra level of investigation to determine if newly discovered vulnerabilities are also present and exploitable in other components. If a single vulnerability exists in multiple libraries, we automatically let you know. Over the past 5 years, we’ve associated vulnerabilities to 3 million more components than public databases.



## Remediate Faster with Expert Guidance Designed for Developers

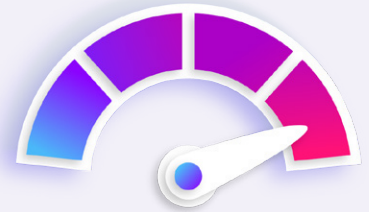
Nexus Intelligence includes actionable information to help development and security teams evaluate, triage, and remediate threats faster than adversaries can attack.

Remediation guidance is carefully curated and written for easy consumption by frontline software developers. Nexus Intelligence provides developers step-by-step instructions on how to detect and remediate the vulnerability, including the upgrade path and relative risk to other component versions.

## Understand the Threat Faster

When it comes to managing the constantly evolving security threats within open source, speed is critical. That’s why Nexus Intelligence works 24x7x365 to keep organizations abreast of the changing threat landscape.

- ▶ 70% more vulnerability coverage than alternative databases
- ▶ 65 world class Data Security Researchers with 500+ years experience
- ▶ 118,000 hours of data security research over 10 years
- ▶ 10X faster than National Vulnerability Database



## Key Benefits of Nexus Intelligence

- ✓ Automate open source governance with precise and accurate data so developers and security teams can concentrate on remediating what matters.
- ✓ Understand the holistic risk to your organization with the ability to see what’s deployed, versus what’s declared.
- ✓ Stay one step ahead of the threat with intelligence that is always on and integrated into the Nexus Platform and your existing DevSecOps pipeline.

“The reason we picked Lifecycle over the other products is while the other products were flagging stuff too, they were flagging things that were incorrect. **Nexus has low false-positive results, which give us a high confidence factor.**”

— E. KWAN  
(Financial Services),  
IT Central Station Review



Sonatype is the leader in software supply chain automation technology with more than 300 employees, over 1,000 enterprise customers, and is trusted by over 10 million software developers. Sonatype’s Nexus platform enables DevOps teams and developers to automatically integrate security at every stage of the modern development pipeline by combining in-depth component intelligence with real-time remediation guidance.

For more information, please visit [Sonatype.com](https://www.sonatype.com), or connect with us on [Facebook](https://www.facebook.com/sonatype), [Twitter](https://twitter.com/sonatype), or [LinkedIn](https://www.linkedin.com/company/sonatype).