








Identify Vulnerabilities and License Compliance Issues
with SCA Powered by Trivy and Grype

OpsMx Delivery Shield includes Software Composition Analysis (SCA) as part of its comprehensive suite of application security capabilities. OpsMx SCA is powered by Trivy and Grype, open-source vulnerability and security scanners recognized for their robust Software Composition Analysis (SCA) capabilities. It empowers developers and security teams to identify vulnerabilities and license compliance issues across their software supply chain. With OpsMx organizations can ensure secure and compliant applications while maintaining development agility.

OpsMx Software Composition Analysis Key Features

-  **Comprehensive Vulnerability Detection**
 - Wide Ecosystem Coverage:** OpsMx Delivery Shield supports scanning for vulnerabilities in multiple ecosystems, including container images, file systems, Git repositories, and Infrastructure as Code (IaC).
 - Extensive Vulnerability Database Integration:** Aggregates data from multiple sources, such as the National Vulnerability Database (NVD), GitHub Security Advisories, and Linux Distribution Security Notices, to deliver up-to-date insights.
-  **License Compliance Management**
 - Automated License Scanning:** OpsMx Delivery Shield identifies open-source components and flags those with incompatible or high-risk licenses, helping organizations adhere to their compliance policies.
 - Customizable Policies:** Users can define organization-specific license policies to enforce compliance across projects.
-  **Seamless Integration**
 - CI/CD Pipeline Support:** Integrates seamlessly with popular CI/CD platforms like Jenkins, GitHub Actions, and GitLab CI/CD, enabling automated scans during development.
 - DevOps-Friendly CLI:** Command-line interface is easy to use and supports integrations with various DevOps tools.
-  **Efficient and Fast Scanning**
 - Low Overhead:** OpsMx Delivery Shield leverages local caching to reduce network dependency and optimize scanning performance.
 - Incremental Scanning:** Scans changes incrementally to save time, focusing only on newly introduced dependencies.
-  **Developer-Centric Insights**
 - Actionable Reporting:** OpsMx Delivery Shield provides detailed vulnerability reports, including CVSS scores, descriptions, and remediation steps, ensuring developers can address issues efficiently.
 - Integration with IDEs:** Integrates with developer environments like Visual Studio Code to offer real-time feedback.

Common Use Cases

- Vulnerability Management:** Identify and remediate known vulnerabilities in container images, IaC, and source code repositories.
- Compliance Assurance:** Monitor and enforce compliance with open-source license policies to reduce legal risks.

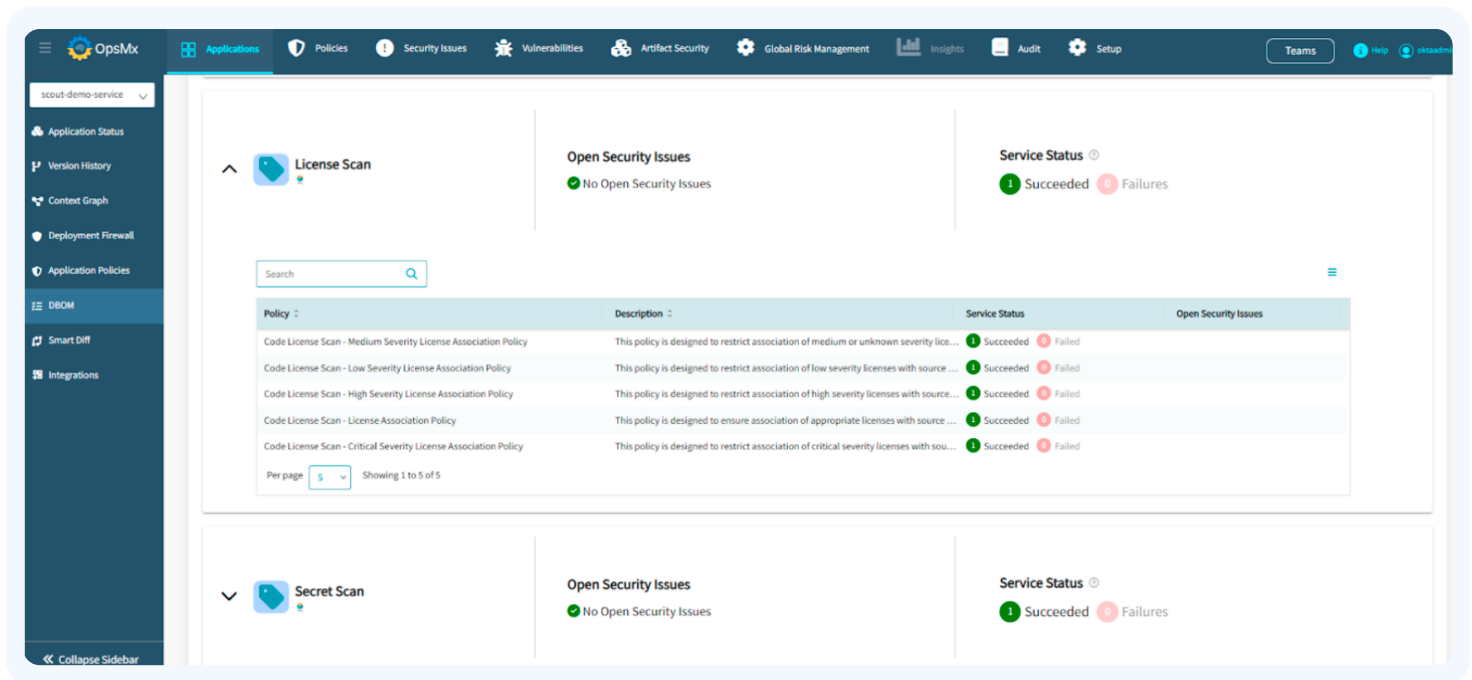


- **DevSecOps Enablement:** Empower DevSecOps teams with automated security scanning integrated into the software development lifecycle.

Benefits

- **Enhanced Security Posture:** Proactively address vulnerabilities and security risks across the software supply chain.
- **Streamlined Compliance:** Simplify license management and avoid costly compliance breaches.
- **Increased Efficiency:** Save time with automated and incremental scans tailored for modern DevOps workflows.
- **Lower Security Costs:** Leverage open source in place of expensive vendor tools, many of which are built on the same open source technologies.

OpsMx Delivery Shield's SCA capabilities make it an essential tool for organizations aiming to secure their software supply chain and ensure compliance with minimal overhead. By embedding security into the development process, Delivery Shield SCA enables teams to build and deploy applications with confidence.



The screenshot displays the OpsMx dashboard interface. The top navigation bar includes sections for Applications, Policies, Security Issues, Vulnerabilities, Artifact Security, Global Risk Management, Insights, Audit, and Setup. A sidebar on the left lists various application management features like Application Status, Version History, Context Graph, Deployment Firewall, Application Policies, DBOM, Smart Diff, and Integrations. The main content area is divided into two primary sections: License Scan and Secret Scan. Each section shows a summary of 'Open Security Issues' (both indicating 'No Open Security Issues') and 'Service Status' (both showing 'Succeeded' and 'Failures' counts). Below the License Scan summary is a table with columns for Policy, Description, Service Status, and Open Security Issues. The table lists five different license association policies, each with a 'Succeeded' status and a 'Failed' status indicator.

Policy	Description	Service Status	Open Security Issues
Code License Scan - Medium Severity License Association Policy	This policy is designed to restrict association of medium or unknown severity lice...	1 Succeeded 1 Failed	
Code License Scan - Low Severity License Association Policy	This policy is designed to restrict association of low severity licenses with source ...	1 Succeeded 1 Failed	
Code License Scan - High Severity License Association Policy	This policy is designed to restrict association of high severity licenses with source ...	1 Succeeded 1 Failed	
Code License Scan - License Association Policy	This policy is designed to ensure association of appropriate licenses with source ...	1 Succeeded 1 Failed	
Code License Scan - Critical Severity License Association Policy	This policy is designed to restrict association of critical severity licenses with sou...	1 Succeeded 1 Failed	

ABOUT US

OpsMx secures and intelligently automates software delivery from developer to deployment, building on an Open Software Delivery architecture and AI/ML-powered DevSecOps. OpsMx products and services enable hundreds of thousands of developers at Google, Cisco, Western Union, and other leading global enterprises to ship better software faster.

FOR MORE INFORMATION, CONTACT US:

OPSMX, INC | 350 OAKMEAD PKWY, SUNNYVALE, CA 94085 | INFO@OPSMX.COM
[WWW.OPSMX.COM/SECURE SOFTWARE DELIVERY](http://WWW.OPSMX.COM/SECURE_SOFTWARE_DELIVERY)