

# Comprehensive Application Security

A Simpler, Cheaper Path to Complete Application Security  
with OpsMx Delivery Shield



Fast-growing companies often struggle to implement a complete application security program due to costly tools, complex processes, and limited security expertise in the organization. OpsMx Delivery Shield offers a simpler, cheaper path to complete enterprise-grade application security.

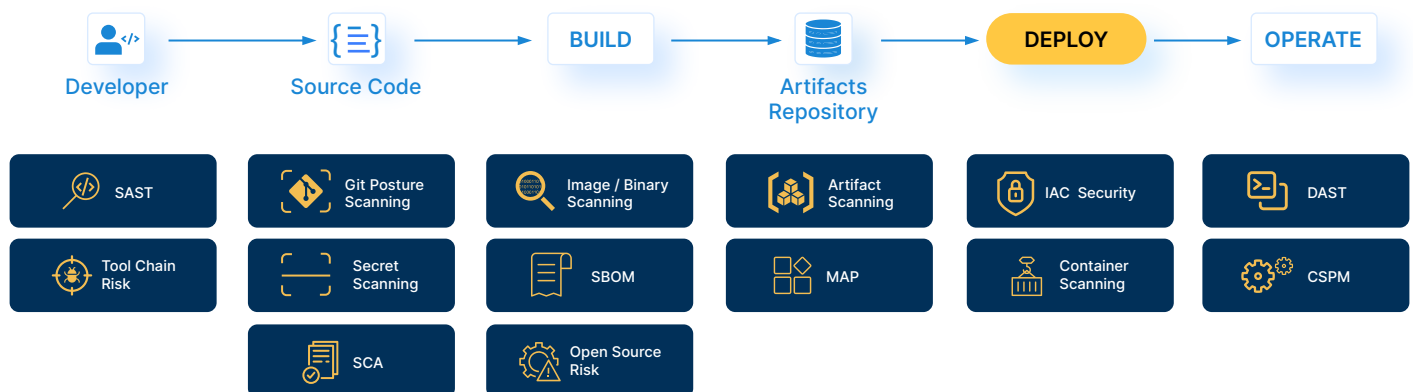
OpsMx's "AppSec in a Box" approach accelerates the delivery of secure applications with an integrated suite of open source AppSec tools, prioritization of security risks across attack vectors, automated compliance, and guided remediation.

## OpsMx Delivery Shield Core Application Security Capabilities

Comprehensive application security requires visibility and risk assessment across the full software delivery process (SDLC). This is achieved using multiple tools, each specialized in one aspect of application security. OpsMx Delivery Shield includes the following categories of application security tools, implemented using open source projects supplemented by OpsMx development:

- Static Application Security Testing (SAST)
- Git Posture Scanning
- Software Composition Analysis (SCA)
- Secrets Scanning
- Image / Binary Scanning
- Open Source Risk
- Artifact Scanning
- Mobile Application Protection (MAP)
- Infrastructure as Code (IAC) Security
- Container Scanning
- Dynamic Application Security Testing (DAST)
- Cloud Security Posture Management (CSPM)
- Software Bill of Materials (SBOM)
- Tool Chain Risk







Customers can choose tools from as many or as few categories as needed to meet their security requirements, in place of or in addition to any AppSec tools they have in place today.









## “AppSec in a Box”, Not “Some Assembly Required”

OpsMx’s flexible, unified approach to Application Security offers key advantages over “do it yourself” AppSec solutions:

-  **Single Vendor Simplicity.** Security tools are pre-preintegrated and packaged with OpsMx Delivery, ready to install. There is no uncertainty about “will these tools work together?”
-  **Unified Management.** OpsMx consolidates data from multiple security tools into a single unified view of application security for simplified risk assessment, management and reporting.
-  **Open Source Risk.** Open source components are a key element of modern software development. OpsMx Delivery Shield unified data reveals the risks in each component, enabling informed decisions on what to keep, what to remove, and what to upgrade.
-  **Compatibility with Existing Tools.** Are there AppSec tools already in place that work well? OpsMx Delivery Shield can also integrate to your existing AppSec tools. No “rip and replace.”
-  **Automated Orchestration.** OpsMx adds an orchestration layer across all AppSec tools, automatically launching security scans and risk assessments at each state of the SDLC.
-  **Simple, Cost Effective Pricing.** OpsMx Delivery Shield costs about the same as one of the classes of security tools it contains. A single flat price gives access to as many of the integrated tools as you need.



## Built on Leading Open Source Security Tools

OpsMx Delivery Shield relies on leading open source security projects to provide its foundation of security tooling and data collection. Using open source offers key benefits to customers, including:

-  **Proven Security Capabilities.** Developed and tested over years, the capabilities of open source security tools meet or exceed the security needs of all but the very largest global enterprises. In fact, many paid vendor solutions are actually built on the same open source tools used by OpsMx.
-  **Cost-Effectiveness.** By definition, open source tools are free to use and operate. Why pay a vendor to license the same capabilities?
-  **Community-Driven Innovation.** Thousands of developers around the world provide ongoing enhancements and innovations. The number of contributors to each open source project often exceeds the number of developers any security vendor has working on their tool.
-  **Fast Vulnerability Resolution.** Community-driven efforts result in faster identification and patching of security flaws than what is possible in a vendor release process.

## Prioritization, Compliance, and Remediation







Comprehensive coverage of the SDLC is the foundation for application security. An enterprise-grade AppSec solution also needs to go further to support the organization’s broader business objectives and accelerate the release of secure applications. OpsMx Delivery Shield enables this with:






-  **Consolidated Risk Management.** OpsMx aggregates and consolidates data from its integrated security tools to provide a unified view of security risks across applications and environments.
-  **Prioritization.** Using its consolidated data, OpsMx generates a single list of security risks that need attention. Keep the team focused on security risks that could have the greatest impact.

- 
**Continuous Risk Assessment.** New security risks and new application releases mean that security posture is constantly changing. OpsMx continuously monitors internal and external events to identify security risks as they emerge.
- 
**Policy Compliance.** Secure organizations need to be in compliance with their defined security policies. OpsMx can automatically evaluate and report how well any team or application conforms to defined security policies.
- 
**Developer Enablement.** OpsMx keeps developers productive by reducing the time they spend tracking down and understanding security issues they are responsible for.
- 
**Guided Remediation.** OpsMx also provides AI powered step-by-step guidance for developers to resolve security issues.

## OpsMx Delivery Shield Open Source Tool Catalog

OpsMx Delivery Shield is built on the power of leading open source security tools powered by thousands of community developers around the world.

Tool Name	Project Description	What OpsMx Uses It For	Contributors
 <p><b>grype</b></p>	Grype is a vulnerability scanner for container images and filesystems, identifying known vulnerabilities.	<ul style="list-style-type: none"> <li>Software Composition Analysis (SCA)</li> <li>Image / Binary Scanning</li> <li>Artifact Scanning</li> </ul>	90+ contributors
 <p><b>Kubescape</b></p>	Kubescape is an open-source Kubernetes security platform for your IDE, CI/CD pipelines, and clusters. It includes risk analysis, security, compliance, and misconfiguration scanning, saving Kubernetes users and administrators precious time, effort, and resources.	<ul style="list-style-type: none"> <li>Infrastructure as Code (IAC) Security</li> <li>Container Scanning</li> <li>Cloud Security Posture Management (CSPM)</li> </ul>	130+ contributors
 <p><b>MOBSF</b></p>	Mobile Security Framework (MobSF) is an open-source security tool for mobile application security testing.	<ul style="list-style-type: none"> <li>Mobile Application Protection (MAP)</li> </ul>	90+ contributors
 <p><b>OpenSSF</b> OPEN SOURCE SECURITY FOUNDATION</p>	OpenSSF is a foundation that provides open-source security guidance and tooling for software supply chain security.	<ul style="list-style-type: none"> <li>Git Posture Scanning</li> </ul>	20+ contributors
 <p><b>Scoutsuite</b></p>	Scout Suite is an open source multi-cloud security-auditing tool, which enables security posture assessment of cloud environments. Using the APIs exposed by cloud providers, Scout Suite gathers configuration data for manual inspection and highlights risk areas.	<ul style="list-style-type: none"> <li>Cloud Security Posture Management (CSPM)</li> </ul>	75+ contributors
 <p><b>Semgrep</b></p>	Semgrep is an open-source static analysis tool that scans source code for patterns and enforces security policies.	<ul style="list-style-type: none"> <li>Static Application Security Testing (SAST)</li> </ul>	170+ contributors

	<p>SonarQube is an open-source platform for continuous inspection of code quality and security.</p>	<ul style="list-style-type: none"> <li>• Static Application Security Testing (SAST)</li> </ul>	<p>240+ contributors</p>
	<p>Syft is a forensic toolkit for file and system analysis, often used in incident response.</p>	<ul style="list-style-type: none"> <li>• Software Bill of Materials (SBOM)</li> </ul>	<p>90+ contributors</p>
	<p>Terrascan is an open-source IaC security analyzer that detects compliance and security violations in Terraform.</p>	<ul style="list-style-type: none"> <li>• Infrastructure as Code (IAC) Security</li> </ul>	<p>82+ contributors</p>
	<p>Trivy is an open-source tool that finds vulnerabilities, misconfigurations, secrets, SBOM in containers, Kubernetes, and more.</p>	<ul style="list-style-type: none"> <li>• Software Composition Analysis (SCA)</li> <li>• Secrets Scanning</li> <li>• Image / Binary Scanning</li> <li>• Artifact Scanning</li> </ul>	<p>400+ contributors</p>
 <b>OWASP ZAP</b>	<p>OWASP ZAP is a widely used web application security scanner that identifies vulnerabilities in web applications.</p>	<ul style="list-style-type: none"> <li>• Dynamic Application Security Testing (DAST)</li> </ul>	<p>210+ contributors</p>

## ABOUT US

OpsMx simplifies and accelerates comprehensive application security from developer to deployment building on AI-driven automation, open source security tools, and a deep understanding of the software delivery process. OpsMx enables tens of thousands of developers at both fast moving innovators and global enterprises to deliver more secure software faster.

## FOR MORE INFORMATION, CONTACT US:

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