How to Select DevSecOps Tools for Secure Software Delivery

Published 16 January 2023 - ID G00772114 - 10 min read

By Analyst(s): Manjunath Bhat, Mark Horvath, Dale Gardner

Initiatives: Software Engineering Technologies; Build a World-Class Software Engineering Organization; Security of Applications and Data; Software Engineering Leadership; Software Engineering Practices

Agile development practices, cloud-native architectures and the increased usage of open-source software amplify the need for continuous security and compliance. Software engineering leaders must guide their teams to integrate developer-friendly security tools into their DevOps pipelines.

Additional Perspectives

- Invest Implications: How to Select DevSecOps Tools for Secure Software Delivery (25 January 2023)

Overview

Key Findings

- Software engineering leaders are tasked with ensuring software security and compliance throughout the software development life cycle (SDLC). This task becomes increasingly difficult as security extends into production environments and software supply chain attacks are on the rise.

- The plethora of choices and overlapping capabilities between tools in the DevSecOps landscape makes tool selection a difficult endeavor.

- Selecting DevSecOps tools can be a daunting task, and software engineering teams are often unsure where to start.

Recommendations

Software engineering leaders should:

- Adopt a continuous approach to security by defining security needs across the full software development life cycle, including the underlying software delivery pipeline.
- Select DevSecOps tools by mapping security needs to tools that adapt to development workflows and reduce developer friction. Prioritize ease of integration and improved developer experience as much as the effectiveness of the tool itself.
- Start small by benchmarking application security capabilities against their peers and aim to continually reduce DevSecOps toolchain debt.

Introduction

This document was revised on 8 February 2023. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

Software applications are one of the primary attack vectors for security breaches. The use of agile development practices, cloud-native architectures and open-source software improves development agility. However, it can also increase security and compliance risks. Mitigating these risks requires software engineering teams to integrate security into the SDLC by adopting developer-centric application security tools. This reduces developer friction in addition to strengthening the security posture.

Software supply chain attacks have added a new dimension to software security problems because the software delivery pipelines and the tools used to build and deploy software are the new attack vectors. Therefore, protecting the delivery pipeline becomes as important as securing the software that is built. However, it is incredibly complex to secure software supply chains because they typically extend beyond the confines of any single organization. They span a network of vendors, partners and open-source ecosystems (see How Software Engineering Leaders Can Mitigate Software Supply Chain Security Risks).

These threats require software engineering leaders to not only shift security left, but also to extend security into production. This research guides software engineering leaders in selecting the right DevSecOps tools to deliver secure software across the SDLC.

Analysis

Define Security Needs Across the Software Development Life Cycle

Software engineering leaders must treat security and compliance as a continuum, and they should not look at development and production as separate security concerns. Rather, they must take a continuous approach to security that meet three distinct needs:

- **Build and deliver secure software.** Select tools that integrate security seamlessly into developer workflows without compromising developer experience. This ensures that software is "secure by default." They should adopt tools at each phase of the SDLC — plan, create, verify, preproduction, release, configure and operate.

- **Protect development and production environments from attackers.** Implement security tools that reduce the attack surface and remediate associated risks through continuous risk assessment.

- **Secure the software supply chain.** Secure the usage of both internal and external code dependencies; protect integrity of software delivery pipelines by providing provenance, visibility and traceability; and govern access to development and operating environments.

> Securing the software delivery pipeline is as important as securing the software that is delivered.

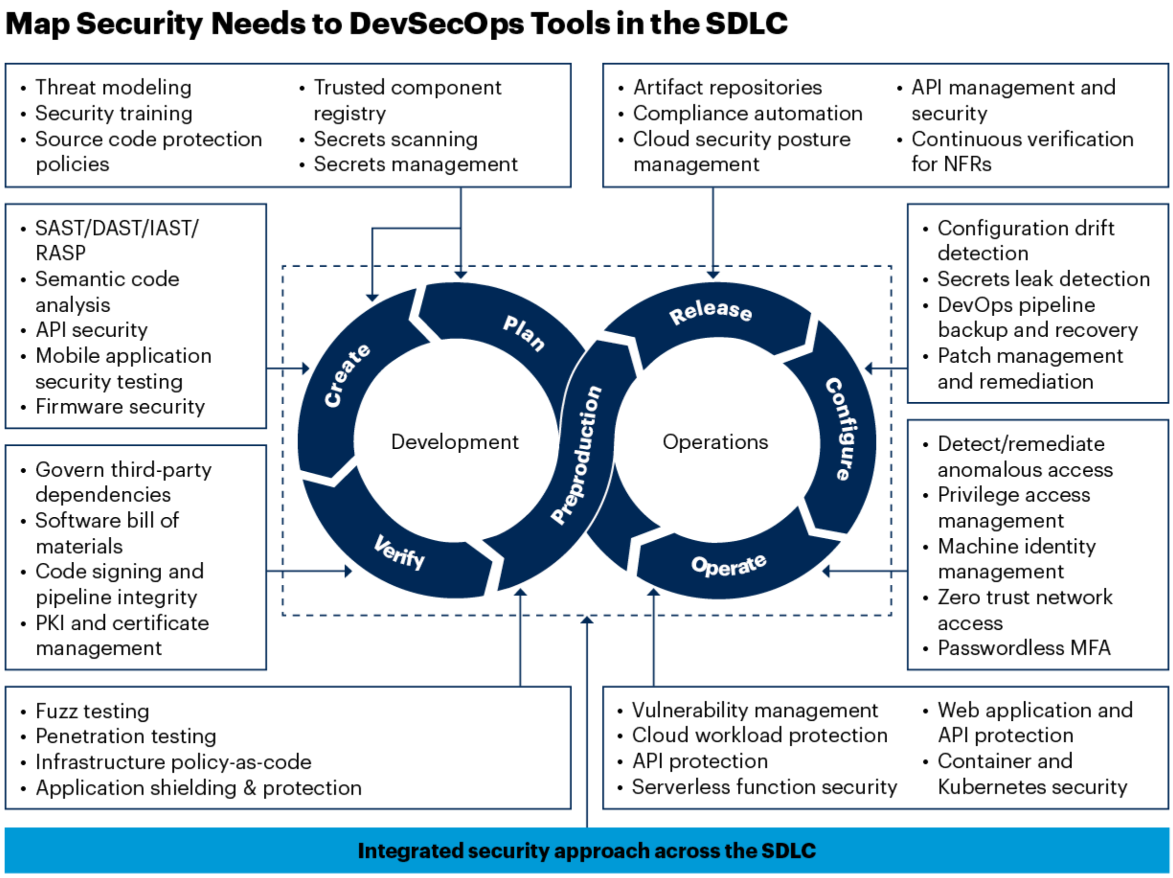
Map Security Needs to Tools That Adapt to Development Workflows and Reduce Developer Friction

To implement a continuous approach to security, software engineering leaders must adopt integrated security and defense-in-depth approaches to software development and delivery. In addition, developers benefit from automated security controls as part of their development platforms. The goal is to build software that is secure by default and ensure full traceability between what is deployed, how it was built and why it is needed.

> Gartner research reveals that more than half of software engineering leaders are directly responsible for application security, and another third share responsibility.

Figure 1 outlines the seven phases of the SDLC and highlights categories of DevSecOps tools that align with each phase. Software engineering leaders should collaborate with security and risk teams as well as their counterparts in infrastructure and operations to integrate tools at each phase of the SDLC. In addition to securing software, they should also secure access to machines and environments and take an integrated security approach that extends to production.

Figure 1: Select DevSecOps Tools to Secure the Complete SDLC



Map Security Needs to DevSecOps Tools in the SDLC

- Threat modeling
- Security training
- Source code protection policies
- Trusted component registry
- Secrets scanning
- Secrets management

- Artifact repositories
- Compliance automation
- Cloud security posture management
- API management and security
- Continuous verification for NFRs

- SAST/DAST/IAST/RASP
- Semantic code analysis
- API security
- Mobile application security testing
- Firmware security

- Configuration drift detection
- Secrets leak detection
- DevOps pipeline backup and recovery
- Patch management and remediation

- Govern third-party dependencies
- Software bill of materials
- Code signing and pipeline integrity
- PKI and certificate management

- Detect/remediate anomalous access
- Privilege access management
- Machine identity management
- Zero trust network access
- Passwordless MFA

- Fuzz testing
- Penetration testing
- Infrastructure policy-as-code
- Application shielding & protection

- Vulnerability management
- Cloud workload protection
- API protection
- Serverless function security
- Web application and API protection
- Container and Kubernetes security

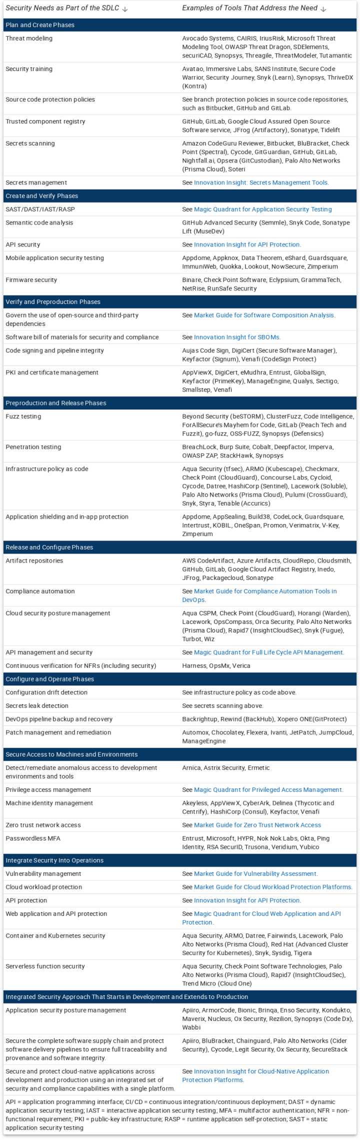
Source: Gartner

772114_C

Table 1 provides a representative, nonexhaustive list of DevSecOps tools to implement secure development practices (for a list of open-source tools, see Tool: Open-Source Security Utilities).

Table 1: Security Platforms and Tools That Address the Needs of Different Phases of the DevOps Pipeline

(Enlarged table in Appendix)



Security Needs as Part of the SDLC ↓	*Examples of Tools That Address the Need* ↓
Plan and Create Phases	
Threat modeling	Avocado Systems, CAIRIS, IriusRisk, Microsoft Threat Modeling Tool, OWASP Threat Dragon, SDElements, securiCAD, Synopsys, Threagile, ThreatModeler, Tutamantic
Security training	Avatao, Immersive Labs, SANS Institute, Secure Code Warrior, Security Journey, Snyk (Learn), Synopsys, ThriveDX (Kontra)
Source code protection policies	See branch protection policies in source code repositories, such as Bitbucket, GitHub and GitLab.
Trusted component registry	GitHub, GitLab, Google Cloud Assured Open Source Software service, JFrog (Artifactory), Sonatype, Tidelift
Secrets scanning	Amazon CodeGuru Reviewer, Bitbucket, BluBracket, Check Point (Spectral), Cycode, GitGuardian, GitHub, GitLab, Nightfall.ai, Opsera (GitCustodian), Palo Alto Networks (Prisma Cloud), Soteri
Secrets management	See Innovation Insight: Secrets Management Tools.
Create and Verify Phases	
SAST/DAST/IAST/RASP	See Magic Quadrant for Application Security Testing
Semantic code analysis	GitHub Advanced Security (Semmle), Snyk Code, Sonatype Lift (MuseDev)
API security	See Innovation Insight for API Protection.
Mobile application security testing	Appdome, Appknox, Data Theorem, eShard, Guardsquare, ImmuniWeb, Quokka, Lookout, NowSecure, Zimperium
Firmware security	Binare, Check Point Software, Eclypsium, GrammaTech, NetRise, RunSafe Security
Verify and Preproduction Phases	
Govern the use of open-source and third-party dependencies	See Market Guide for Software Composition Analysis.
Software bill of materials for security and compliance	See Innovation Insight for SBOMs.
Code signing and pipeline integrity	Aujas Code Sign, DigiCert (Secure Software Manager), Keyfactor (Signum), Venafi (CodeSign Protect)
PKI and certificate management	AppViewX, DigiCert, eMudhra, Entrust, GlobalSign, Keyfactor (PrimeKey), ManageEngine, Qualys, Sectigo, Smallstep, Venafi
Preproduction and Release Phases	
Fuzz testing	Beyond Security (beSTORM), ClusterFuzz, Code Intelligence, ForAllSecure's Mayhem for Code, GitLab (Peach Tech and Fuzzit), go-fuzz, OSS-FUZZ, Synopsys (Defensics)
Penetration testing	BreachLock, Burp Suite, Cobalt, Deepfactor, Imperva, OWASP ZAP, StackHawk, Synopsys
Infrastructure policy as code	Aqua Security (tfsec), ARMO (Kubescape), Checkmarx, Check Point (CloudGuard), Concourse Labs, Cycloid, Cycode, Datree, HashiCorp (Sentinel), Lacework (Soluble), Palo Alto Networks (Prisma Cloud), Pulumi (CrossGuard), Snyk, Styra, Tenable (Accurics)
Application shielding and in-app protection	Appdome, AppSealing, Build38, CodeLock, Guardsquare, Intertrust, KOBIL, OneSpan, Promon, Verimatrix, V-Key, Zimperium
Release and Configure Phases	
Artifact repositories	AWS CodeArtifact, Azure Artifacts, CloudRepo, Cloudsmith, GitHub, GitLab, Google Cloud Artifact Registry, Inedo, JFrog, Packagecloud, Sonatype
Compliance automation	See Market Guide for Compliance Automation Tools in DevOps.
Cloud security posture management	Aqua CSPM, Check Point (CloudGuard), Horangi (Warden), Lacework, OpsCompass, Orca Security, Palo Alto Networks (Prisma Cloud), Rapid7 (InsightCloudSec), Snyk (Fugue), Turbot, Wiz
API management and security	See Magic Quadrant for Full Life Cycle API Management.
Continuous verification for NFRs (including security)	Harness, OpsMx, Verica
Configure and Operate Phases	
Configuration drift detection	See infrastructure policy as code above.
Secrets leak detection	See secrets scanning above.
DevOps pipeline backup and recovery	Backrightup, Rewind (BackHub), Xopero ONE(GitProtect)
Patch management and remediation	Automox, Chocolatey, Flexera, Ivanti, JetPatch, JumpCloud, ManageEngine
Secure Access to Machines and Environments	
Detect/remediate anomalous access to development environments and tools	Arnica, Astrix Security, Ermetic
Privilege access management	See Magic Quadrant for Privileged Access Management.
Machine identity management	Akeyless, AppViewX, CyberArk, Delinea (Thycotic and Centrify), HashiCorp (Consul), Keyfactor, Venafi
Zero trust network access	See Market Guide for Zero Trust Network Access
Passwordless MFA	Entrust, Microsoft, HYPR, Nok Nok Labs, Okta, Ping Identity, RSA SecurID, Trusona, Veridium, Yubico
Integrate Security Into Operations	
Vulnerability management	See Market Guide for Vulnerability Assessment.
Cloud workload protection	See Market Guide for Cloud Workload Protection Platforms.
API protection	See Innovation Insight for API Protection.
Web application and API protection	See Magic Quadrant for Cloud Web Application and API Protection.
Container and Kubernetes security	Aqua Security, ARMO, Datree, Fairwinds, Lacework, Palo Alto Networks (Prisma Cloud), Red Hat (Advanced Cluster Security for Kubernetes), Snyk, Sysdig, Tigera
Serverless function security	Aqua Security, Check Point Software Technologies, Palo Alto Networks (Prisma Cloud), Rapid7 (InsightCloudSec), Trend Micro (Cloud One)
Integrated Security Approach That Starts in Development and Extends to Production	
Application security posture management	Apiiro, ArmorCode, Bionic, Brinqa, Enso Security, Kondukto, Maverix, Nucleus, Ox Security, Rezilion, Synopsys (Code Dx), Wabbi
Secure the complete software supply chain and protect software delivery pipelines to ensure full traceability and provenance and software integrity.	Apiiro, BluBracket, Chainguard, Palo Alto Networks (Cider Security), Cycode, Legit Security, Ox Security, SecureStack
Secure and protect cloud-native applications across development and production using an integrated set of security and compliance capabilities with a single platform.	See Innovation Insight for Cloud-Native Application Protection Platforms.

API = application programming interface; CI/CD = continuous integration/continuous deployment; DAST = dynamic application security testing; IAST = interactive application security testing; MFA = multifactor authentication; NFR = non-functional requirement; PKI = public-key infrastructure; RASP = runtime application self-protection; SAST = static application security testing

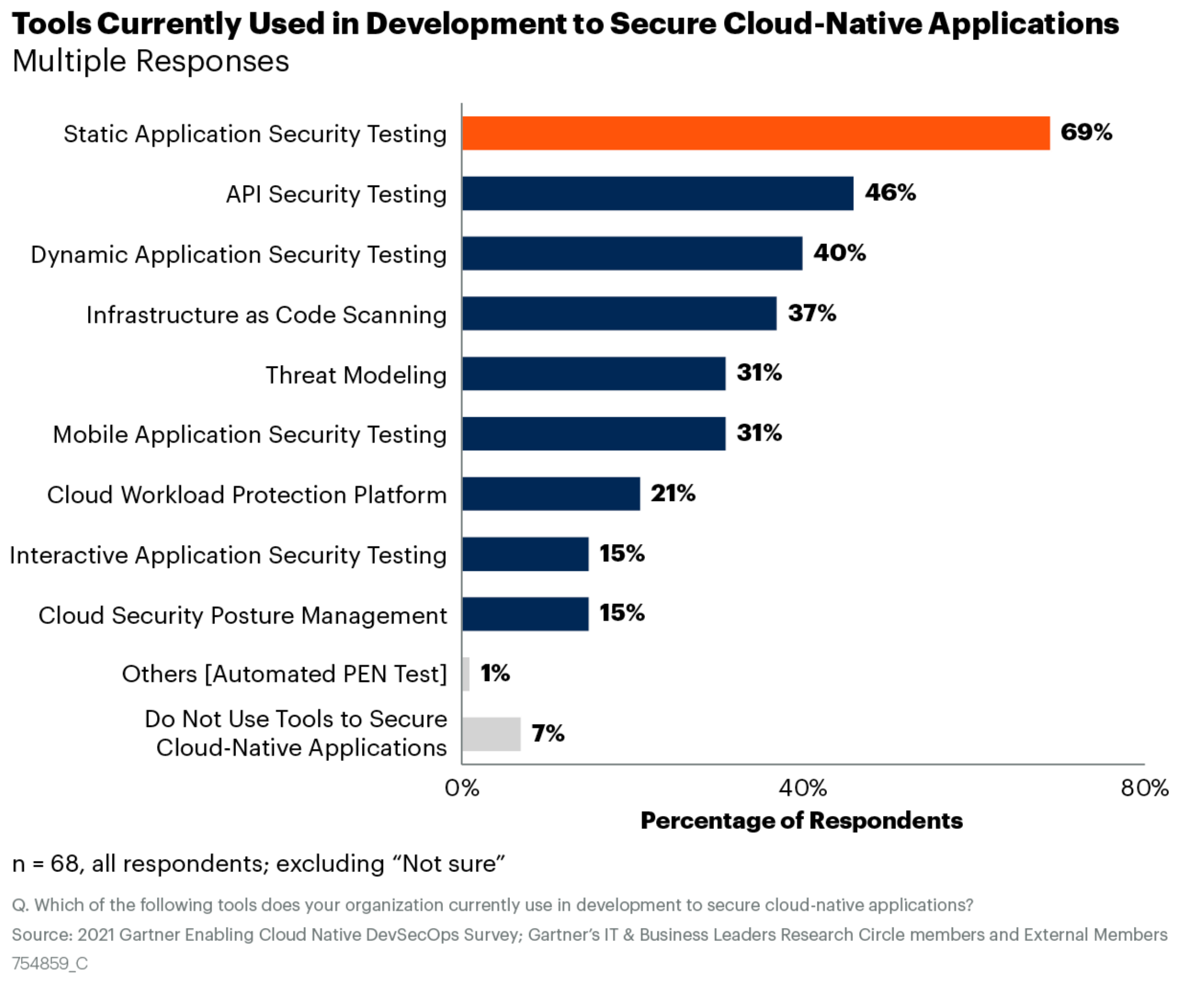
Source: Gartner

Benchmark Use of Tools Against Peers

Results from Gartner's 2021 Enabling Cloud-Native DevSecOps Survey show that 69% of respondents use static application security testing (SAST) in development, 75% use web application firewalls (WAFs), and 60% use application security monitoring in production. Still, newer tools such as API security testing (46%), infrastructure as code scanning (40%) and mobile application security testing (31%) are also used during development (see Survey Analysis: Enabling Cloud-Native DevSecOps).

Figures 2 and 3 list the tools used to secure cloud-native applications during development and in production. Gartner's Magic Quadrant for Application Security Testing provides an evaluation of the vendors that provide these capabilities as part of an integrated security test suite (see Magic Quadrant for Application Security Testing). Although the quality of execution can vary considerably, all vendors in the Magic Quadrant have delivered these capabilities to market, and espouse a developer-centric approach to application security.

Figure 2: DevSecOps Tools in Development to Secure Cloud-Native Applications



Tools Currently Used in Development to Secure Cloud-Native Applications
Multiple Responses

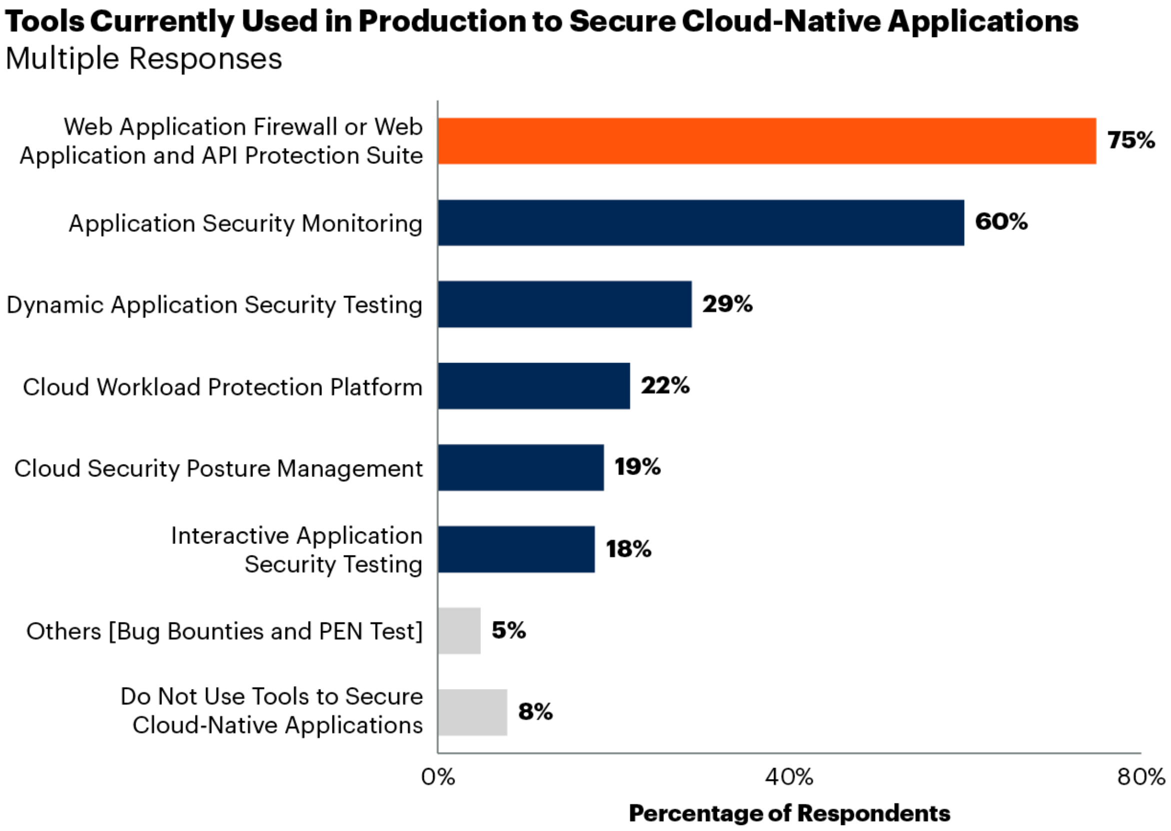
n = 68, all respondents; excluding "Not sure"

Q. Which of the following tools does your organization currently use in development to secure cloud-native applications?

Source: 2021 Gartner Enabling Cloud Native DevSecOps Survey; Gartner's IT & Business Leaders Research Circle members and External Members

754859_C

Figure 3: DevSecOps Tools in Production to Secure Cloud-Native Applications



n = 73, all respondents; excluding "Not sure"

Q. Which of the following tools does your organization currently use in production to secure cloud-native applications?

Source: 2021 Gartner Enabling Cloud Native DevSecOps Survey; Gartner's IT & Business Leaders Research Circle members and External Members

754859_C

Evidence

2021 Gartner Enabling Cloud Native DevSecOps Survey. This survey was conducted online from 12 May through 21 May 2021 to identify the emerging governing structures, security owners, technologies used and the current challenges in the DevSecOps pipeline to secure cloud-native applications. In total, 85 IT and business leaders with involvement in DevSecOps initiatives participated in the survey. Eighty-two were from Gartner's IT and Business Leaders Research Circle — a Gartner-managed panel — and three were from an external sample. Participants from North America (37), EMEA (29), Asia/Pacific (7) and Latin America (11) responded to the survey. The survey was developed collaboratively by a team of Gartner analysts and Gartner's Research Data, Analytics and Tools team. Disclaimer: Results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

How Software Engineering Leaders Can Mitigate Software Supply Chain Security Risks

Magic Quadrant for Application Security Testing

Market Guide for Software Composition Analysis

Innovation Insight for SBOMs

Innovation Insight for Cloud-Native Application Protection Platforms

5 Frequently Asked Questions About Threat Modeling

Using 'Policy as Code' to Secure Application Deployments and Enforce Compliance

Table 1: Security Platforms and Tools That Address the Needs of Different Phases of the DevOps Pipeline

Security Needs as Part of the SDLC ↓	*Examples of Tools That Address the Need* ↓
Plan and Create Phases	
Threat modeling	Avocado Systems, CAIRIS, IriusRisk, Microsoft Threat Modeling Tool, OWASP Threat Dragon, SDElements, securiCAD, Synopsys, Threagile, ThreatModeler, Tutamantic
Security training	Avatao, Immersive Labs, SANS Institute, Secure Code Warrior, Security Journey, Snyk (Learn), Synopsys, ThriveDX (Kontra)
Source code protection policies	See branch protection policies in source code repositories, such as Bitbucket, GitHub and GitLab.
Trusted component registry	GitHub, GitLab, Google Cloud Assured Open Source Software service, JFrog (Artifactory), Sonatype, Tidelift
Secrets scanning	Amazon CodeGuru Reviewer, Bitbucket, BluBracket, Check Point (Spectral), Cycode, GitGuardian, GitHub, GitLab, Nightfall.ai, Opsera (GitCustodian), Palo Alto Networks (Prisma Cloud), Soteri
Secrets management	See Innovation Insight: Secrets Management Tools.
Create and Verify Phases	
SAST/DAST/IAST/RASP	See Magic Quadrant for Application Security Testing
Semantic code analysis	GitHub Advanced Security (Semmle), Snyk Code, Sonatype Lift (MuseDev)

Security Needs as Part of the SDLC ↓	*Examples of Tools That Address the Need* ↓
API security	See Innovation Insight for API Protection.
Mobile application security testing	Appdome, Appknox, Data Theorem, eShard, Guardsquare, ImmuniWeb, Quokka, Lookout, NowSecure, Zimperium
Firmware security	Binare, Check Point Software, Eclypsium, GrammaTech, NetRise, RunSafe Security
Verify and Preproduction Phases	
Govern the use of open-source and third-party dependencies	See Market Guide for Software Composition Analysis.
Software bill of materials for security and compliance	See Innovation Insight for SBOMs.
Code signing and pipeline integrity	Aujas Code Sign, DigiCert (Secure Software Manager), Keyfactor (Signum), Venafi (CodeSign Protect)
PKI and certificate management	AppViewX, DigiCert, eMudhra, Entrust, GlobalSign, Keyfactor (PrimeKey), ManageEngine, Qualys, Sectigo, Smallstep, Venafi
Preproduction and Release Phases	
Fuzz testing	Beyond Security (beSTORM), ClusterFuzz, Code Intelligence, ForAllSecure's Mayhem for Code, GitLab (Peach Tech and Fuzzit), go-fuzz, OSS-FUZZ, Synopsys (Defensics)
Penetration testing	BreachLock, Burp Suite, Cobalt, Deepfactor, Imperva, OWASP ZAP, StackHawk, Synopsys

Security Needs as Part of the SDLC ↓	*Examples of Tools That Address the Need* ↓
Infrastructure policy as code	Aqua Security (tfsec), ARMO (Kubescape), Checkmarx, Check Point (CloudGuard), Concourse Labs, Cycloid, Cycode, Datree, HashiCorp (Sentinel), Lacework (Soluble), Palo Alto Networks (Prisma Cloud), Pulumi (CrossGuard), Snyk, Styra, Tenable (Accurics)
Application shielding and in-app protection	Appdome, AppSealing, Build38, CodeLock, Guardsquare, Intertrust, KOBIL, OneSpan, Promon, Verimatrix, V-Key, Zimperium
Release and Configure Phases	
Artifact repositories	AWS CodeArtifact, Azure Artifacts, CloudRepo, Cloudsmith, GitHub, GitLab, Google Cloud Artifact Registry, Inedo, JFrog, Packagecloud, Sonatype
Compliance automation	See Market Guide for Compliance Automation Tools in DevOps.
Cloud security posture management	Aqua CSPM, Check Point (CloudGuard), Horangi (Warden), Lacework, OpsCompass, Orca Security, Palo Alto Networks (Prisma Cloud), Rapid7 (InsightCloudSec), Snyk (Fugue), Turbot, Wiz
API management and security	See Magic Quadrant for Full Life Cycle API Management.
Continuous verification for NFRs (including security)	Harness, OpsMx, Verica
Configure and Operate Phases	
Configuration drift detection	See infrastructure policy as code above.
Secrets leak detection	See secrets scanning above.
DevOps pipeline backup and recovery	Backrightup, Rewind (BackHub), Xopero ONE(GitProtect)

Security Needs as Part of the SDLC ↓	*Examples of Tools That Address the Need* ↓
Patch management and remediation	Automox, Chocolatey, Flexera, Ivanti, JetPatch, JumpCloud, ManageEngine
Secure Access to Machines and Environments	
Detect/remediate anomalous access to development environments and tools	Arnica, Astrix Security, Ermetic
Privilege access management	See Magic Quadrant for Privileged Access Management.
Machine identity management	Akeyless, AppViewX, CyberArk, Delinea (Thycotic and Centrify), HashiCorp (Consul), Keyfactor, Venafi
Zero trust network access	See Market Guide for Zero Trust Network Access
Passwordless MFA	Entrust, Microsoft, HYPR, Nok Nok Labs, Okta, Ping Identity, RSA SecurID, Trusona, Veridium, Yubico
Integrate Security Into Operations	
Vulnerability management	See Market Guide for Vulnerability Assessment.
Cloud workload protection	See Market Guide for Cloud Workload Protection Platforms.
API protection	See Innovation Insight for API Protection.
Web application and API protection	See Magic Quadrant for Cloud Web Application and API Protection.
Container and Kubernetes security	Aqua Security, ARMO, Datree, Fairwinds, Lacework, Palo Alto Networks (Prisma Cloud), Red Hat (Advanced Cluster Security for Kubernetes), Snyk, Sysdig, Tigera

Security Needs as Part of the SDLC ↓	*Examples of Tools That Address the Need* ↓
Serverless function security	Aqua Security, Check Point Software Technologies, Palo Alto Networks (Prisma Cloud), Rapid7 (InsightCloudSec), Trend Micro (Cloud One)
Integrated Security Approach That Starts in Development and Extends to Production	
Application security posture management	Apiiro, ArmorCode, Bionic, Brinqa, Enso Security, Kondukto, Maverix, Nucleus, Ox Security, Rezilion, Synopsys (Code Dx), Wabbi
Secure the complete software supply chain and protect software delivery pipelines to ensure full traceability and provenance and software integrity.	Apiiro, BluBracket, Chainguard, Palo Alto Networks (Cider Security), Cycode, Legit Security, Ox Security, SecureStack
Secure and protect cloud-native applications across development and production using an integrated set of security and compliance capabilities with a single platform.	See Innovation Insight for Cloud-Native Application Protection Platforms.
API = application programming interface; CI/CD = continuous integration/continuous deployment; DAST = dynamic application security testing; IAST = interactive application security testing; MFA = multifactor authentication; NFR = non-functional requirement; PKI = public-key infrastructure; RASP = runtime application self-protection; SAST = static application security testing	

Source: Gartner