Cool Vendors in DevSecOps

Published 17 May 2021 - ID G00746834 - 8 min read

By Analyst(s): Dionisio Zumerle

Initiatives: Security of Applications and Data

Innovation in the application security sector focuses on meeting the speed and automation requirements of DevOps development styles. This report profiles four vendors whose innovative technologies introduce security to these new development styles and enable efficient DevSecOps.

Overview

Key Findings

- Enabling DevSecOps requires automated security capabilities that traditional development tools do not provide.
- Solutions that use risk-based mechanisms are helping security teams identify the specific application code that most needs attention, thus reducing the time spent on nonproductive testing.
- The challenges of placing application security controls into the continuous innovation/continuous delivery (CI/CD) pipeline encourage security teams to look for new tools that can more simply and seamlessly integrate into the DevOps toolchain without slowing it.

Recommendations

Security and risk management leaders responsible for DevSecOps should:

- Perform security testing exclusively on code changes that truly merit security attention, by assessing each change based on the risk it could introduce.
- Assess and monitor application components and configurations in order to automatically identify potentially risky changes to applications and address any drift in threat modeling.

- Experiment with new approaches that enable automatic remediation of code vulnerabilities between development and deployment.

Analysis

This research does not constitute an exhaustive list of vendors in any given technology area, but rather is designed to highlight interesting, new and innovative vendors, products and services. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

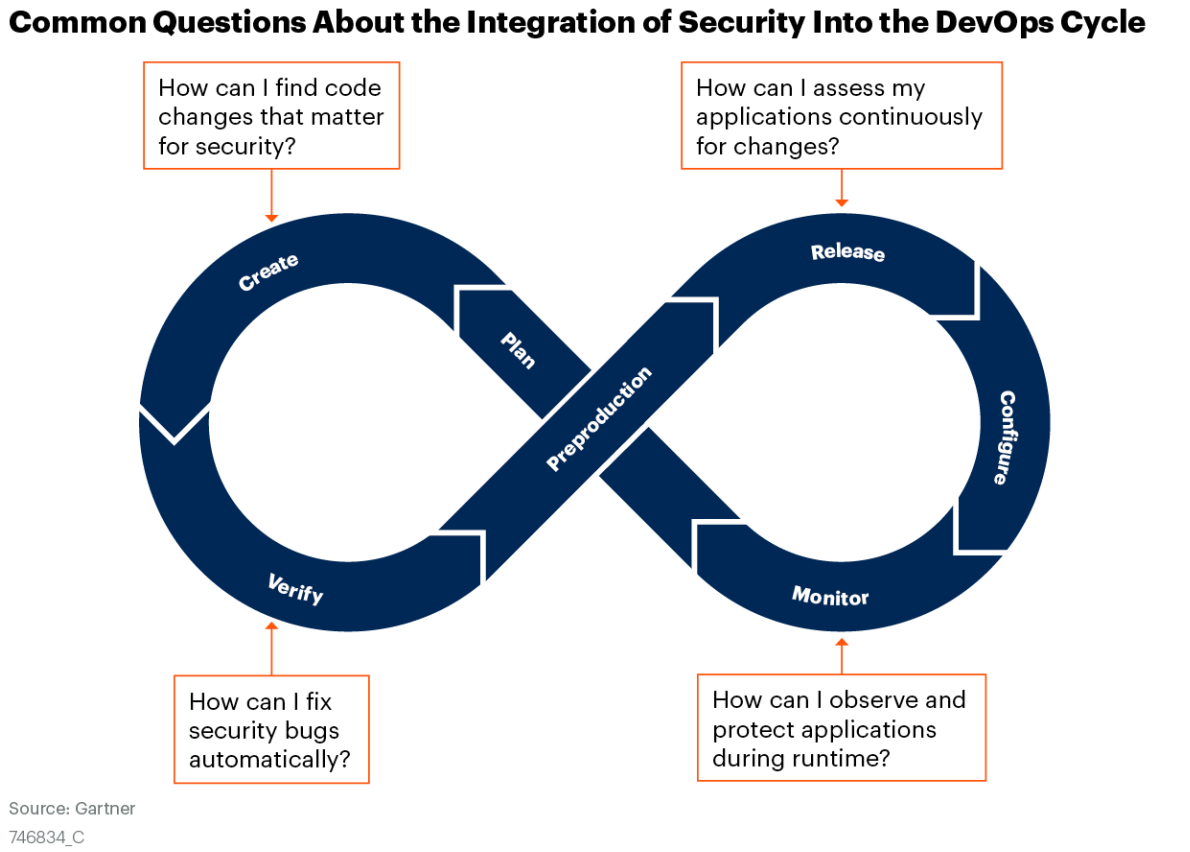
What You Need to Know

DevOps introduces a security challenge. [1] By bringing development and operations teams closer together, the aim of DevOps is to deliver new applications and features rapidly and continuously. Traditional security processes and tools are not designed for this approach, and they slow DevOps processes. This reduces the agility advantages of DevOps, without significantly improving security.

The aspiration with DevSecOps is to overcome the security challenge posed by DevOps. [2] DevSecOps introduces security to DevOps processes without hindering the speed and flexibility brought about by DevOps. To achieve this, DevSecOps needs to focus on what really matters from a security standpoint, and provide automated ways to fix those issues.

This report profiles four vendors whose innovative solutions exemplify how security and application development leaders can remove clutter and automate DevSecOps. Their offerings help answer common questions, shown in Figure 1, about the incorporation of security into the DevOps cycle.

Figure 1: Common Questions About the Integration of Security Into the DevOps Cycle



The four profiled vendors are:

- **Apiiro,** which identifies material changes in code that merit security attention, based on risk, which is evaluated by assessing technical findings and information such as the skills of developers.
- **Bionic,** which monitors application components and configurations in order to identify risky changes that may require revision of threat-modeling conclusions.
- **Jaroona,** which provides automatic code vulnerability remediation — something that has been elusive in the application security testing sector.
- **Sqreen,** a previous Cool Vendor that provides application runtime monitoring and protection. It is profiled in the "Where Are they Now?" section at the end of this report.

Apiiro

Tel Aviv, Israel (www.apiiro.com)

Analysis by Dionisio Zumerle

Why Cool: Apiiro provides a way to automatically identify material changes to code that require security attention. It eliminates the majority of changes that do not present a security risk and that therefore may not require security testing. It does so based on historical and continuous analysis of code and development metadata, such as commit messages, pull request discussions and user stories, as well as factors such as the seniority of developers. Apiiro connects with the enterprise source control manager and the ticket system, and optionally connects with application security testing (AST) tools, such as static AST (SAST) scanners, as well as software composition analysis tools and API gateways.

Challenges:

- As Apiiro's solution operates transparently, buyers may struggle to communicate its value internally.
- Apiiro's solution discounts immaterial changes that do not merit security attention, based on indicators of risk. This approach potentially leaves room for false negatives.
- Apiiro's clients have to undergo a requirements assessment exercise to determine their needs and how to reflect them in the tool.

Who Should Care:

- Security leaders looking for a way to simplify their involvement in the secure development life cycle should monitor the approach taken by Apiiro.

Bionic

Palo Alto, California, U.S. (www.bionic.ai)

Analysis by Dale Gardner

Why Cool: Bionic has developed an agentless approach that establishes a baseline inventory of application components and their configurations, thus providing much needed visibility into complex and rapidly changing applications — including their service dependencies, data flows and architectural drift. As applications become more complex and ephemeral, and as the velocity of development increases, this visibility helps application security teams maintain their understanding of an application architecture and ensure architectural standards are followed. It also facilitates rapid identification of changes to threat models, potential security or compliance violations, and vulnerabilities.

The need for application security teams to keep pace with development — and avoid creating friction and "drag" on the process —— has been a long-standing challenge, which is heightened by faster development processes and more complex architectures. Bionic's approach enables a security team to understand the security implications of new code as it passes along the pipeline, without slowing the code introduction process.

Challenges:

- Bionic's tool gathers a comprehensive array of architectural, control and data flow information, but users still need to translate that information into actionable tasks. Bionic is likely to have to pay attention to how successful customers are in this regard, and to offer them additional integrations with security and development infrastructure, and playbooks or workflows.
- The information offered is of value to multiple constituencies within an organization — among them, security staff, developers and architects — and potentially competes with other tools that gather subsets of data. This implies a need for precise differentiation from other tools that claim to offer similar types of data.
- Although Bionic offers a useful range of integrations, especially for DevOps tools and cloud platforms, customers will need to make additional integrations to ensure a good fit for their environments and to keep pace with emerging information sources.

Who Should Care:

- Application security teams, who can use Bionic's tool both to enforce security standards and as a data source that can help them understand applications and thus ease efforts to identify — and remediate — compliance and vulnerability issues. Bionic's tool has also been used in application modernization efforts, to help development teams rearchitect applications for cloud environments.

- Security leaders seeking practical mechanisms to increase their understanding of complex application environments, in order to improve threat modeling and risk assessment, ensure compliance with security and architectural standards, and maintain that understanding.

Jaroona

Vienna, Austria (https://jaroona.com)

Analysis by Mark Horvath

Why Cool: Jaroona has a novel technology for identifying security vulnerabilities and suggesting code fixes. Rather than provide developers with suggested best practices to remediate vulnerabilities, Jaroona has trained a machine learning (ML) algorithm that scans code fixes from other SAST tools and open-source software before suggesting an autoremediation. It then scans the autoremediated code to ensure it fixes the issues without causing other problems, and thus delivers much cleaner and faster solutions.

Challenges:

- Most vendors in the SAST space claim to have this ability, but they really just provide suggestions based on best practices and high-level guidance, or in some cases, remote humans via chat. Although Jaroona's remediation functionality is unique, the vendor faces a challenge to distinguish itself from others who exaggeratedly claim to offer the same thing.
- Jaroona's technology, though interesting and potentially highly beneficial, remains unproven in large deployments.
- Automated code fixes contravene DevOps principles like "own your code," which mandates that only the developer should change code because only the developer has responsibility for it. Although that principle is meant to apply to code authorship, rather than repair, it might nevertheless be a significant hurdle.
- Automated code engines have a mixed reputation. In the past, these types of ML tools have fixed code at the expense of performance or reliability. However, Jaroona's technology can be set to Confirmation mode, whereby a developer has to confirm a fix before it is applied. Also, before providing autofix suggestions to a developer, Jaroona reruns them through detection analytics to ensure that any previously reported vulnerability has been fixed.

Who Should Care:

- Developer organizations that have little experience with secure coding, or that have a large backlog of security-related technical debt, relative to their workload.
- Small or midsize teams that lack the time or resources required for a properly secure software development life cycle.
- Security and risk management leaders and heads of development tasked with lowering the risk that unsecure code poses to their organization.

Where Are They Now?

Sqreen

San Francisco, California (www.sqreen.com)

Analysis by Dionisio Zumerle

Profiled in Cool Vendors in Security and Risk Management, 2H19

Why Cool Then: Sqreen secures applications by monitoring their behavior during runtime and providing protection from the inside. It offers a series of modules that provide runtime application self-protection (RASP), an in-app web application firewall (WAF), content security policy and virtual patching, depending on the needs of each application.

Where They Are Now: In 2021, Sqreen was acquired by Datadog, an application performance monitoring vendor. Gartner had already described how Application Performance Monitoring and Application Security Monitoring Are Converging, and this move furthers that development. A possible integration between the two vendors' solutions could compete with Cisco's AppDynamics security offering, as well as with Dynatrace's security offering.

Who Should Care:

- Security and application leaders of organizations looking for an innovative, modular and platform-based approach to monitor and secure critical applications.

Evidence

[1] DevOps represents a change in IT culture, focusing on rapid IT service delivery through the adoption of agile, lean practices in the context of a system-oriented approach. DevOps emphasizes people (and culture), and it seeks to improve collaboration between operations and development teams. DevOps implementations utilize technology — especially automation tools that can leverage an increasingly programmable and dynamic infrastructure from a life cycle perspective.

[2] DevSecOps is the integration of security into emerging agile IT and DevOps development as seamlessly and as transparently as possible. Ideally, this is done without reducing the agility or speed of developers or requiring them to leave their development toolchain environment.

Recommended by the Author

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

12 Things to Get Right for Successful DevSecOps

3 Steps to Integrate Security Into DevOps

Hype Cycle for Application Security, 2020

7 Tips to Set Up an Application Security Program Without Breaking the Bank

Market Guide for Software Composition Analysis
