GIGAOM

REPORT

GigaOm Radar for Evaluating DevSecOps Tools v1.0

JON COLLINS | NOV 19, 2020 - 12:14 PM CST

TOPICS: DEV & OPS DEVSECOPS

GIGAOM

GigaOm Radar for Evaluating DevSecOps Tools

TABLE OF CONTENTS

1. Summary

As we learned in the associated report, "Key Criteria for Evaluating DevSecOps Tools," the field of DevSecOps is part principle and part tooling. The principle hinges on bringing security best practices as early as possible into DevOps-based software creation, delivery, and operation—so-called "shift-left." The tooling should enable this to take place.

We can see DevSecOps tooling as the set of capabilities that directly increases pipeline governance to reduce application and infrastructure risk, without increasing associated costs and overheads. DevSecOps tools offer capabilities that automate best practices, augment the pipeline, and support development activities, addressing security challenges across the software development and operations.

As we consider how to evaluate vendors for DevSecOps, we need to take two points into account:

- All vendors involved in improving application security can contribute to an organization's overall DevSecOps stance.
- Many vendors are aligning themselves to DevSecOps, even though their solution set is not particularly specific to improving security across the DevOps pipeline.

In this report, we have identified a number of vendors that address the specific needs of DevSecOps, which we articulate in this report as table stakes, key criteria, and evaluation metrics. While we assess 10 vendor solutions here, we ruled out many more, including several offering capabilities such as software composition analysis (SCA) and static application security testing (SAST) with CI/CD APIs. This alone was not deemed sufficient to define a vendor solution as falling into the DevSecOps category. For example, a number of providers that do not appear in this report offer scanning capabilities that merited review in our forthcoming Key Criteria and Radar Report on Vulnerability Management.

With all this in mind, read on.

HOW TO READ THIS REPORT

This GigaOm report is one of a series of documents that helps IT organizations assess competing solutions in the context of well-defined features and criteria. For a fuller understanding consider reviewing the following reports:

Key Criteria report: A detailed market sector analysis that assesses the impact that key product features and criteria have on top-line solution characteristics—such as scalability, performance, and TCO—that drive purchase decisions.

GigaOm Radar report: A forward-looking analysis that plots the relative value and progression of vendor solutions along multiple axes based on strategy and execution. The Radar report includes a breakdown of each vendor's offering in the sector.

Vendor Profile: An in-depth vendor analysis that builds on the framework developed in the Key Criteria and Radar reports to assess a company's engagement within a technology sector. This analysis includes forward-looking guidance around both strategy and product.

2. Market Categories and Deployment Types

For a better understanding of the market and vendor positioning (**Table 1**), we assess how well solutions for DevSecOps are positioned to serve specific market segments.

- **Large enterprise:** Here offerings are assessed on their ability to support large and business-critical projects, across broader environments. Such organizations will have security and governance functions in place, but these may exist at arms' length to DevOps teams. Optimal solutions in this category will have a strong focus on manageability, collaboration, and policy-based delivery, as well as scalability and performance.
- **Mid-market:** In this category we assess solutions on their ability to meet the needs of organizations ranging from small businesses to medium-sized companies. These organizations will have a less well-defined security capability but will also benefit from fewer legacy systems and less rigid thinking. Ease of use and deployment become more important than extensive management functionality.
- **Cloud-native/startup:** These organizations will not be hampered by existing practices but may be less mature when it comes to security and governance. Features that support changes in thinking—for example, enabling a shift-left mindset—can help here, as do tools that offer better management visibility and support a collaborative approach to improvement.

In addition, we recognize three predominant deployment models for solutions in this report:

- **On-premises:** Software deploys on an organization's own servers, which means scaling is dictated by the resources the organization provides.
- **(Self-) Cloud-hosted:** Similar to on-premises solutions, but installed in the public cloud. The user still keeps full control of the infrastructure and therefore costs.
- **SaaS:** These solutions are entirely offered as a service, with costs based on a per-use or subscription model.

Advantages and disadvantages exist for each model: the overall goal is to give the reader a broader perspective and context regarding the different solutions available in the market and how they can fit with organizational and business needs.

Table 1: Vendor Positioning

	MARKET SEGMENT			DEPLOYMENT MODEL		
	Enterprise	Mid-Market	Cloud-Native/ Startup	On-Premises	(Self) Cloud-Hosted	SaaS
Alcide.io	++	++	+++	-	-	++
BridgeCrew	++	++	++	-	-	++
Chef Compliance	+++	++	+	++	++	+
DBmaestro	++	++	+	++	++	++
GitLab	++	+++	++	++	++	++
JFrog	+++	++	++	+++	+++	+++
Micro Focus	+++	++	++	++	-	++
Sonatype	++	+++	+++	++	++	-
Veracode	+++	++	+	-	-	+++
ZeroNorth	++	++	++	-	-	++

Source: GigaOm 2020

+++ Strong focus and perfect fit of the solution
++ The solution is good in this area, but there is still room for improvement
+ The solution has limitations and a narrow set of use cases
- Not applicable or absent.

3. Key Criteria Comparison

Building on the findings from the GigaOm report, "Key Criteria for Evaluating DevSecOps," **Table 2** and **Table 3** summarizes how each vendor included in this research performs in the areas that we consider differentiating and critical in this sector. The objective is to give the reader a snapshot of the technical capabilities of different solutions and define the perimeter of the market landscape.

Table 2. Key Criteria

	KEY CRITERIA					
	Policy-Driven Automation	Dependency Analysis	Audit Reporting	Secrets Management	Drift Identification	Support For IaC
Alcide.io	++	+	+	++	+++	+
BridgeCrew	+++	-	++	-	++	+++
Chef Compliance	+++	+	+++	+	++	+++
DBmaestro	++	++	++	++	++	+
GitLab	++	+++	++	++	++	+
JFrog	++	+++	+++	++	+	+
Micro Focus	++	++	++	+	+	++
Sonatype	+++	+++	++	++	+	+
Veracode	+++	++	+++	+	+	+
ZeroNorth	+++	+++	++	+	+	++

+++ Strong focus and perfect fit of the solution
++ The solution is good in this area, but there is still room for improvement
+ The solution has limitations and a narrow set of use cases
- Not applicable or absent.

Source: GigaOm 2020

Table 3. Evaluation Metrics

	EVALUATION METRICS					
	Flexibility & Usability	Shift-Left Effectiveness	End-to-End Coverage	Solution Ecosystem	Licensing & Support*	Overall ROI/TCO
Alcide.io	++	++	+	+	++	++
BridgeCrew	++	+++	++	++	++	++
Chef Compliance	+++	++	+++	++	+++	+++
DBmaestro	+	++	+	++	++	++
GitLab	++	+++	+++	+	++	++
JFrog	++	++	+++	++	++	++
Micro Focus	++	++	+++	++	++	++
Sonatype	++	++	+++	++	++	++
Veracode	+++	+++	++	++	++	+++
ZeroNorth	++	+++	+++	++	++	++

*Incl OSS Entry Level

+++ Strong focus and perfect fit of the solution
++ The solution is good in this area, but there is still room for improvement
+ The solution has limitations and a narrow set of use cases
- Not applicable or absent.

Source: GigaOm 2020

It is worth noting that, as defined, the DevSecOps category is relatively immature. Some vendors are strong in software development lifecycle (SDLC) terms, which is normal as the development pipeline in the past ended prior to the deployment stage. Equally, some vendors are stronger on the infrastructure and deployment aspects of the DevOps lifecycle.

In terms of table stakes, all vendors should be able to integrate with security and development tools across the pipeline, offering clarity on risk, clear feedback, and dashboards (capabilities we identify in the Key Criteria report as Toolchain and SecOps Integration). They should also offer an element of process control, based on policy and risk (addressed as Security Gates and Checks in the Key Criteria report), while Role-Based Access should be a non-differentiating capability. Finally, we see the ability to guide and direct developers and decision makers toward a shift-left stance as an essential element of DevSecOps, reflected in our table stakes category of Opinionated Remediation.

When it comes to the differentiating key criteria that define the relative impact and value of solutions in this space, the focus is more on how DevSecOps is maturing from a tooling perspective. As development, operations, and security teams work together, they can benefit from a collaborative

approach to policy, which automation can then enable to set-and-forget (reflected in the Policy-Driven Automation key criteria). Tools can also deliver on process governance needs; for example, collating information that can be used for compliance (Audit Reporting). Specific features that boost development and delivery are represented in Dependency Analysis—enabling individual activities to be linked to a broader context—and Secrets Management, which is highly important for cloud-native development (reflected in the Dependency Analysis and Secrets Management key criteria).

Finally, we note that DevOps is not only about development, but also about infrastructure and operations, all of which needs to be treated with security in mind. Criteria therefore cover infrastructure aspects: Support for Infrastructure as Code addresses configuration information that is defined textually and managed alongside program code, while Drift Identification covers the ability to identify and treat changes to baseline configurations over time.

We expect the category of DevSecOps to evolve quickly in at least three dimensions. On top of the inevitability of tighter integration, better automation, and stronger insights (potentially driven by use of machine learning), we see how DevSecOps needs to shift up to deliver better policy-driven support for compliance, and shift right to offer stronger links to operations and pre- and post-deployment architecture. Here, emerging technologies identified in the Key Criteria report, such as compliance support and broader architectural support, come into play. Ultimately we see the goal as doing things right the first time, enabling innovation while minimizing risk—which is why we see tools analyzing, and responding to engineering behaviors in real time (addressed in the emerging technology category of behavioral analytics). And while we are not judging vendors on these criteria today, we can highlight examples to understand where they are heading to tomorrow.

By combining the information provided in the tables above, the reader should gain a clear understanding of the sector and the technical solutions available in the market.

4. GigaOm Radar

This report synthesizes the analysis of key criteria and their impact on evaluation metrics to inform the GigaOm Radar graphic in **Figure 1**. The resulting chart is a forward-looking perspective on all the vendors in this report, based on their products' technical capabilities and feature sets.

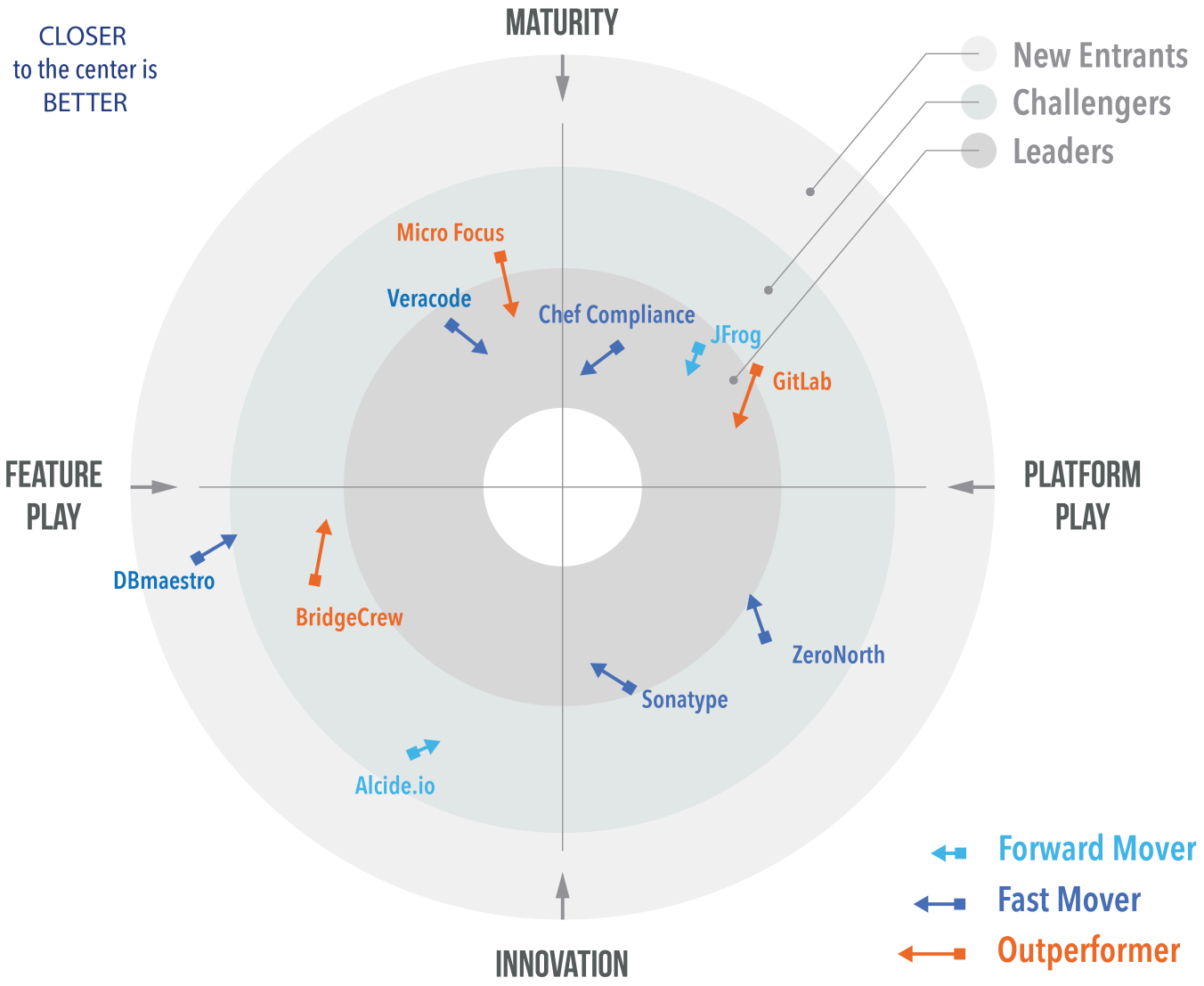

Figure 1: GigaOm Radar for DevSecOps

The GigaOm Radar plots vendor solutions across a series of concentric rings, with those set closer to center judged to be of higher overall value. The chart characterizes each vendor on two axes—Maturity versus Innovation, and Feature Play versus Platform Play—while providing an arrow that projects each solution's evolution over the coming 12 to 18 months.

DevSecOps leadership is considered for vendors who exhibit breadth of coverage, use of policy-based automation, and the overall ability to drive a shift-left approach. As you can see in the Radar chart in **Figure 1**, few vendors offer all of these elements, though Chef is probably the best able to do so today, followed by GitLab and Micro Focus, which both have strong end-to-end coverage. Veracode and Sonatype hold their own well, though more on the Dev side of the house, so we consider these more as feature players in our assessment. We also have an interesting set of startups and smaller companies to consider: Alcide.io and Bridgecrew address DevSecOps needs for Infrastructure as Code, and DBmaestro focuses on data structures.

INSIDE THE GIGAOM RADAR

The GigaOm Radar weighs each vendor's execution, roadmap, and ability to innovate to plot solutions along two axes, each set as opposing pairs. On the Y axis, **Maturity** recognizes solution stability, strength of ecosystem, and a conservative stance, while **Innovation** highlights technical innovation and a more aggressive approach. On the X axis, **Feature Play** connotes a narrow focus on niche or cutting-edge functionality, while **Platform Play** displays a broader platform focus and commitment to a comprehensive feature set.

The closer to center a solution sits, the better its execution and value, with top performers occupying the inner Leaders circle. The centermost circle is almost always empty, reserved for highly mature and consolidated markets that lack space for further innovation.
The GigaOm Radar offers a forward-looking assessment, plotting the current and projected position of each solution over a 12- to 18-month window. Arrows indicate travel based on strategy and pace of innovation, with vendors designated as Forward Movers, Fast Movers, or Outperformers based on their rate of progression.

Note that the Radar excludes vendor market share as a metric. The focus is on forward-looking analysis that emphasizes the value of innovation and differentiation over incumbent market position.

5. Vendor Insights

Alcide

Alcide emerged from stealth this year with the goal to provide a single pane of glass for DevOps, security, and cloud architecture teams looking to secure Kubernetes workloads. While Alcide offers a range of security solutions across threat detection, log monitoring, and compliance reporting, it merits inclusion here due to its Alcide Advisor tool.

From a scanning perspective (outside the scope of this report), Alcide Advisor covers Kubernetes workloads running in virtualized, containerized, and serverless target architectures, on-premise or in the cloud. It is API rather than agent-based.

The tool offers reporting and scoring of configuration risks from a vulnerability and a more general "hygiene" perspective, enabling comparison against a baseline configuration profile (which can be auto-generated). It also identifies and reports "drift," that is, increase of risk over time caused by gradual changes to a baseline as-planned configuration.

Alcide Advisor is policy-driven for both scanning and admission controls, supporting policy customization by the security team. Policies (which follow OPA protocols) can be enforced on the runtime environment. Alcide Advisor also monitors for dev team and administrator changes to the tool itself to ensure these do not introduce risk.

Alcide Advisor is "free forever," with a policy-based guardrails module available at additional cost, priced per node. The full solution also includes process whitelisting and admission controls. It would be suited to Kubernetes environments that are looking to get on top of configuration risks, even if they have other tools in place.

Strengths: Good integration for Kubernetes toolchain, with drift identification, risk scoring, and remediation recommendations. OPA-based policy definition.

Challenges: Kubernetes only. Not so strong on end-to-end coverage prior to IaC. Too early for the vendor to have established an ecosystem.

Bridgecrew

Bridgecrew has recently emerged from stealth. Its mission is to address the challenges that arise when security flaws are caused by misconfigurations of the build or deployment environment. Not only do such flaws increase risk; they are often fixed by directly reconfiguring the infrastructure concerned. In Infrastructure as Code (IaC) environments, this can result in a mis-alignment between what's documented in the Infrastructure as Code and what the target actually looks like.

Focusing on the IaC use case, Bridgecrew's product addresses these challenges in two ways. First, it can use predefined policies to identify misconfigurations in the target infrastructure, creating "as-code" fixes that can be applied automatically. Second and in parallel, it can apply the same corrections to the Infrastructure as Code files concerned, so that the issues will not arise again on a subsequent redeployment.

Bridgecrew also offers integrations with source control to ensure fixes are implemented in, and managed with, development code. This addresses both the security challenge and the resulting bottlenecks caused when security professionals and engineers have to coordinate a response.

Bridgecrew works with a variety of IaC platforms, including Terraform and CloudFormation, and while initial customers have largely been AWS-based, the product also works with Azure and is cloud-target agnostic. The company sees runtime scanning as a commodity and has thus open sourced its own Chekov scanning engine. This has enabled a growing community to build checks and plugins across a variety of target environments.

Bridgecrew offers a free Community edition as well as standard, Pro and Enterprise tiers that enable scanning of larger numbers of resources and enhanced features. While the capability is currently more feature than product, it is developing fast; for example, its recently announced drift analysis.

Strengths: Custom policy-based scanning and benchmarking. Enables policies and fixes to be stored alongside code

Challenges: Does not cover the application side of DevSecOps currently but would fit well with a best-of-breed approach.

Chef

Any review of Chef products needs to take into account the recently announced acquisition by Progress Software, as the latter builds out its development tooling portfolio. Chef is primarily known for IaC-based deployment automation, but has been incorporating products that help engineers assess and assure security and compliance across the development toolchain. While the company has offered capabilities in this area for several years, it has increased its focus as an area of differentiation (likely because of the increasing adoption of Terraform for deployment automation, a factor that may have led to the company open sourcing its software in 2019).

After several changes, Chef has chosen Chef Compliance (rather than Chef InSpec) as the name of its "continuous compliance" product line. This incorporates Chef Compliance Audit, which follows a policy-as-code approach, based on the InSpec language (a derivative of Ruby Rshell)—a simple example might be "don't allow unencrypted telnet sessions." This enables users to determine and set the desired baseline for security and compliance, and then map this against activities and outcomes. Chef InSpec can then pull data from pipeline and security tools to check whether the baseline is being adhered to.

Policy checks are given an impact score, based on the National Institute of Standards and Technology's Common Vulnerability Scoring System (NIST CVSS) and on the number of systems concerned. Should significant policy breaches take place, they can be fed back into the pipeline for remediation (for example, using Chef Compliance Remediation), and halt deployment—the system does allow for waivers to allow the pipeline to continue if necessary.

Overall, Chef Compliance helps ensure that software artifacts are "clean" by the time they reach production (or a trusted artifact store), both in terms of how they have been developed and what they contain. It catalyzes the shift of security responsibility towards developers, encouraging better practices and encouraging fixing problems before they reach deployment. It also fits organizations looking to set policy in advance and collaboratively, as a way of bringing development and security teams together. Chef works across heterogeneous infrastructure types, so InSpec suits organizations looking to secure pipelines regardless of target environment.

Strengths: Policy-driven automation, audit reporting, and automated remediation across heterogeneous environments. Highly flexible. OSS availability across full suite

Challenges: Larger learning curve, which may be overkill for homogeneous cloud-native environments with simpler pipelines. Not designed for dependency analysis.

DBmaestro

DBmaestro offers policy-based database delivery automation and versioning. It is an interesting offering as it doesn't deliver the standard tools expected in this category, yet it integrates well with common CI/CD pipeline tools and works in a way that fits with DevSecOps practice. DBmaestro doesn't fully fit with the DevSecOps category as defined in this report (and hence can only be positioned as a feature player), yet it deserves mention as an area that DevOps teams should address.

Specifically, DBmaestro enables users to create and then enforce policies for how databases are managed, both at a structural and process level. For example, structural changes might be "who can drop a column," while process policies might be "who can release a new database version." While several tools offer capabilities to help database releases (such as Liquidbase and notably Microsoft with tools such as the SQL Server Data Tools add-in for Visual Studio), DBmaestro brings more enterprise-class features (such as auditing) to market.

DBmaestro enables these policies to be managed as code alongside code in development, bringing (what we could call) database configuration management into alignment with software configuration management, enabling such capabilities as version control and drift detection (which can be a source of risk). Databases supported include Microsoft SQL Server, DB2, Oracle, MySQL, MongoDB, and PostgreSQL, across on-premises and cloud environments. From a database perspective, the product does cover dependency and analysis and drift identification, and supports secrets management via integration with CyberArk.

DBmaestro has two product versions, which are due to merge by the end of 2020, working both as a

PaaS platform and as an on-premises solution. The company works with DevOps teams in large enterprises and medium-large startups, which are looking to simplify database design activity through secure automation. Many customers are in the financial sector.

Strengths: Covers a neglected area of software-based innovation, with a strong feature set.

Challenges: Not a full DevSecOps solution as per the key criteria used in this report, as its features focus on the database.

GitLab

GitLab is a frequent flyer when it comes to GigaOm's DevOps-related Key Criteria and Radar report series, offering a broad platform as it does. The company merits inclusion in this DevSecOps report, as it integrates process-oriented Security and Compliance dashboards into its more general toolkit. These can pull information from built-in and third-party testing/scanning tools and present issues both graphically and textually; for example, showing vulnerabilities over time.

Dashboards work on a by-project, by-group, or by-instance basis, so managers can review security issues in parallel with other criteria (such as requirements, timelines, and bottlenecks) to better decide priorities—a definite strength when it comes to shifting security left. To support this further, the platform also offers general analytics, such as percentage of code scanned, or mean time to resolution and how this changes over time.

Looking more broadly, GitLab offers a number of features that help towards an organization's DevSecOps goals. The platform builds in secrets management (which we see as a future table stake), and also incorporates policy-based license compliance and dependency-based analysis, both high-value features given the nature of modern development which is often based on open source or external libraries. It also offers suggested solutions and a level of automated remediation for certain code/targets, and enables issues to be treated and merged confidentially to protect the security of the code.

GitLab offers an integrated approach aimed at both development and security teams; for example, enabling security gates, and automating creation of trouble tickets should a vulnerability be identified. As we have said in other reports, this all-in approach is not going to suit all organizations, in what remains a complex and heterogeneous world (particularly for enterprises). However, from a security perspective, GitLab's one-stop-git-based-shop is a definite boon, reducing potential risks caused by fragmented toolchains and pipelines. As a more strategic tool, it may be best-suited to mid-market organizations.

GitLab licensing is on a per-seat basis, with tiered functionality—most of the above capabilities are in the top tier only.

Strengths: Integrated approach—can see security information in context of project, aiding decision

making and shift-left stance. Policy-based compliance support. Includes secrets management.

Challenges: Limited guidance to developers fixing issues. A relatively compact security ecosystem, though this is evolving. Does not cover infrastructure as code.

JFrog

While JFrog's portfolio may have extended across the pipeline in recent years (see our CI/CD report), at its heart it remains Artifactory, a repository for managing executable binaries. This repository sits at the handshake between continuous integration (creating binaries) and continuous deployment (deploying them).

From a security perspective, these binaries create risks if not handled correctly. For example, security pros need to know what each binary contains, as a bill of materials; whether the contents have been tampered with, verifying, for example, through exhaustive granular metadata, checksums, and digital signing; and what dependencies exist on other libraries, internal or external.

JFrog deals with these needs. The JFrog DevOps Platform includes JFrog Xray for DevSecOps and SCA, which enables low-level scanning to identify any OSS security vulnerabilities and license compliance violations throughout the SDLC. More important for DecSecOps is how this integrates with other capabilities. Based on provenance, binary metadata, and scanning information, the user can trigger automatic actions from their CI/CD pipelines—either using the Platform's native JFrog Pipelines solution, or any other CI tool of their choosing. In addition, JFrog provides a release bundle of signed artifacts and binary files, enabling releases to be distributed with an audit trail of their component parts, making this an attractive option for highly distributed (that is, edge-based or containerized) applications. (On this note, JFrog Distribution incorporates a protocol to optimize network utilization.)

Following the identification of an issue in a developer repository or a production environment, the product highlights at-risk packages and can instigate an action, such as creating an alert, preventing a deployment, or triggering a pipeline step. It can also prohibit a package with security violations from being downloaded, to prevent use of contaminated artifacts as early as possible in delivery. JFrog's security-first credentials extend back across the pipeline—while JFrog offers CI/CD, its security and distribution capabilities also integrate with other pipeline tools such as Jenkins, GitHub, CircleCI, and others.

The company has experience with large enterprises, particularly those facing challenges of deployment/distribution, DevSecOps at scale, and compliance and regulation requirements, and which need a centrally managed, automated solution for both DevOps and Security. By focusing on this area, JFrog enables innovation teams to experiment at the same time as ensuring resulting applications are auditably confirmed to be secure.

Strengths: Strong set of deployment options. Good end-to-end coverage, with tight integration of scanning, and robust security and compliance gates. Suits highly distributed applications.

Challenges: Does not offer much in terms of opinionated remediation. No direct focus on configuration as code.

Micro Focus

A couple of years have now elapsed since the Micro Focus acquisition of HPE's software development tools portfolio, and the company confirms that DevOps is a strategic pillar of its business—this is important as Micro Focus recognizes it has integration work to do.

From a security perspective, Micro Focus leads with the Fortify product, which acts as a dashboard onto other elements of its portfolio. Fortify ScanCentral integrates with common repositories to offer static and dynamic scanning of source code and containers at pull request or commit, with source analysis provided via an OEM relationship with Sonatype, providing coverage across development, CI, and CD. The product can also produce a bill of materials for containers.

Drilling into DevSecOps, Micro Focus takes a developer-centric approach, building security tools into developer workflows without (in principle) getting in the way. Fortify integrates with PulseUno CI for a full-build scan, and to instrument approval processes. It also links with artifact repositories, and offers code repository scanning, library vulnerability scanning, and license scanning.

Time to remediation is a focus: for example, the company sees direct (human) services as a key element to support delivery of actionable results. Further supporting this are language-specific rules, such as Java Try With Resources; administrators can also suppress non-critical scans to minimize noise.

The company has recently added support for FedRamp—a federal certified workflow. Future features include noise reduction (explored in the GigaOm Radar for AIOps report) and real-time analysis to further increase immediacy (and hence actionability) of results.

The company mainly works with application security budget holders but is seeing growing interest from (increasingly influential) development organizations as shift-left practices are adopted. Models include Fortify On Demand and On-Premise.

Strengths: Developer-focused offering within a comprehensive portfolio, auto-code packaging of containers

Challenges: Could offer broader integration with CI/CD ecosystem

Sonatype

Sonatype is focused on securing the range of open-source components used across many cloud-native and other software programs today. While Sonatype is known more for its database of open-source vulnerabilities, the vendor started out as a repository company for Java components. The

Nexus Repository Manager product (available as open source) is still core to Sonatype's portfolio, managing binaries and other artifacts.

Building on this are vulnerability scanning capabilities, a firewall to automatically block vulnerable components from entering the software supply chain, and tools for examining open-source components within production and third-party applications for security and licensing issues. These are powered by a data layer known as Nexus Intelligence, which leverages information from Nexus tools and an in-house team of specialist researchers, who provide the vulnerability information that powers the platform, alongside public databases, and anonymized information gleaned from its user base.

The Nexus Platform and products work across the development and operations lifecycle, identifying known problems to be treated. For example, Nexus Lifecycle can scan early looking at a manifest, but can also scan a binary before or after production. Any issues can be flagged and linked to the correct component or application via integrations with common tools such as Slack or Jira. Sonatype sees itself as a best-of-breed player, providing the platform for external scanning solutions and code and artifact repository providers. This principle also applies to Infrastructure-as-Code security, where Sonatype works with a third party.

Tools are policy-based; for example, policies can be set to report on issues, to put builds on hold while they are remediated, or to quarantine artifacts. Taking things a step further, the recent Advanced Development Pack release offers policy-based guidance on how to remediate issues when found, and where problems might be coming from (such as bad actors injecting malicious code).

Overall, Sonatype looks to help development teams mature in terms of best practice, first bringing in vulnerability scans (for instance, "composition security") and then building policies around them. This approach enables an on-ramp to better practice without jeopardizing short-term productivity.

Strengths: Particularly appropriate for organizations using a lot of OSS components. Best-of-breed platform approach. Policy-based gates. Solid future roadmap.

Challenges: Policy-based automation and compliance only available with enterprise tier of Nexus Platform. Opinionated remediation not yet available. Not directly equipped for Infrastructure as Code.

Veracode

Veracode started out over a decade ago as an online software analysis tool. While its heritage is in software vulnerability management, the company sets its stall around enabling its key stakeholders (specifically, developers) to play a central role in reducing the risk in the code they create. A core principle is that the earlier a problem is spotted, the more likely it is to be fixed and therefore, the lower the risk.

As such, Veracode plays more than just lip service to the principles and practices of DevSecOps, at least for development and software security teams. Yes, Veracode offers comprehensive scanning for

both in-house code and open-source libraries and dashboards to prioritize issues based on risk. From a DevSecOps perspective, Static Pipeline Scan offers fast build-time scanning, and the product also makes real-time recommendations to developers on potential security issues, portraying itself as a "spell checker for code security." In some cases, it can also offer automated resolution.

Turning to the needs of development teams, Veracode takes into account how individual changes can impact the other areas of a product, using policies to determine whether a build should be interrupted or, say, a grace period should be introduced for a fix. Policies also feed into production software analysis, and can be configured per application or release; for instance, allowing pre-production policies to be less stringent.

In parallel with tooling, Veracode emphasizes education, offering a consulting service to help teams start on the right foot as they look to up their security game, as well as hands-on training for developers. This teaches secure coding practices through interactive web apps based on modern threats and can be directed based on the kinds of security issues flagged for a particular team.

Veracode suits organizations that are looking to improve the security of software in development. It has some stand-out features to this end, not least the ability to support compliance audits based on its penetration testing capability. However, while it works across the development lifecycle, it does not currently cover post-production, nor does it address challenges of infrastructure as code during or post-deployment, which may be seen as important areas for cloud-native applications.

Strengths: Developer-centric approach, with actionable feedback and remediation advice. Policy-driven automation for teams. Support for compliance audits. Services built into the offer.

Challenges: Not currently very strong for architectural and post-deployment security, such as for Infrastructure as Code.

ZeroNorth

ZeroNorth offers a DevOps-facing integration hub, results repository, and analytics dashboard for scanning and vulnerability management tools. While the product acts more as an oversight and orchestration tool, it's fair to say that ZeroNorth "gets" DevSecOps. The company's platform focuses on automating security across the pipeline, initiating scans, and collating results into a repository, which the tool analyzes and feeds to ticketing systems. A useful feature is noise reduction—the product distills multiple results and remediation recommendations from different tools into a single ticket so they can be addressed as one issue.

ZeroNorth is policy based, enabling teams to specify what tools need to be run when, and what success/failure looks like (e.g. meeting specific service-level agreements or compliance requirements). Results from scans can be applied to the pipeline; for example, to block deployment if a severe issue is identified. Both application and infrastructure scanning can be included, including the ability to create a composite risk score for an application stack, or indeed for a group of applications. Because the tool acts in more of an overseeing role however, it offers only remediation recommendations derived from

the scans.

Turning to ethos, ZeroNorth is focused on driving DevSecOps best practices by supporting and catalyzing the implementation of what it calls a “continuous application security program” across developers, security professionals, and the business. Insights from the product’s analysis help focus where training should be applied; for example, around software composition analysis versus static application scanning.

ZeroNorth works with both large and small companies that are looking to establish or re-establish a DevOps security program. Larger companies may find that the speed of DevOps poses a challenge to their security practices, whereas smaller organizations may find themselves hitting security issues that can impair DevOps success. Either case can benefit from a program that links security improvement goals with top-down visibility on security—something that ZeroNorth provides.

Strengths: Broad integration of tools (open source and commercial) across the toolchain. Offers an effective top-down platform for DevSecOps, including composite risk score.

Challenges: Acts as a hub/orchestrator, so it lacks direct intervention and remediation. No secrets management nor infrastructure configuration drift.

6. Analyst's Take

So what can we learn from the current state of the DevSecOps market? The picture we get is of a work in progress, with vendors coming from the left, the right, and below:

- From the left, we see more mature players such as Veracode and Microfocus delivering SDLC-enabled capabilities
- From the right, we see newer vendors, such as Alcide.io, Bridgecrew, and others, delivering infrastructure-facing capabilities
- From below, we see vendors such as JFrog and Sonatype bringing an end-to-end view on top of scanning and other capabilities

As DevSecOps brings together these areas, we expect to see mergers between some of these players and/or acquisitions by larger companies to fill gaps in their portfolios. Point-solution companies such as DBmaestro (which helps manage risk associated with data structures) can be seen as a symptom of the currently fragmented landscape: In the future, we expect end-to-end DevSecOps to become the norm, not the exception. To catalyze this, we'd like to see vendors offer more process-oriented features in their entry-level packages, rather than offering such features only in their top-tier packages.

In the meantime, can a DevSecOps solution exist in isolation of a variety of other security solutions, vulnerability management, and so on? All vendors have their strengths; for example, Chef Compliance with its process view on DevSecOps. Some of the solutions here, such as GitLab, incorporate broader features, whereas in other cases end-user organizations will need to use a third-party offering alongside DevSecOps—we reinforce the point that SCA/SAST with a CI/CD API is not DevSecOps, however.

For users of existing providers in this report, or indeed security vendors that claim to align with DevSecOps, we would recommend pushing them into a process-oriented role—for example, leveraging features such as review gates and so on, rather than making use of simpler functionality such as audit reports. If DevSecOps is about practices and tools, it is incumbent on its users to seek to improve the former, enabled by the latter. Put bluntly, don't think you are "doing" DevSecOps simply because you have adopted a tool that says it is doing DevSecOps. Rather, seek actively to measure and reduce risk, improve practice, and solve problems as early as possible in the pipeline, with tools such as those listed here helping you to automate these activities.

7. About Jon Collins

Jon Collins has advised the world's largest technology companies in product and go to market strategy, acted as an agile software consultant to a variety of Enterprise organizations, advised government departments on IT security and network management, led the development of a mobile healthcare app and successfully managed a rapidly expanding Enterprise IT environment. Jon is frequently called upon to offer direct and practical advice to support IT and digital transformation strategy has served on the editorial board for the BearingPoint Institute thought leadership program and is currently a columnist for IDG Connect.

Jon wrote the British Computer Society's handbook for security architects and co-authored The Technology Garden, a book offering CIOs clear advice on the six principles of sustainable IT delivery. He has written innumerable papers and guides about getting the most out of technology and is an accomplished speaker, facilitator, and presenter.

8. About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.

9. Copyright