White Paper

Using a Modern DevSecOps Platform to Drive Organizational Success

Sponsored by: Veracode

Jim Mercer Melinda-Carol Ballou

April 2022

EXECUTIVE SUMMARY

The applications used to run your business and engage with your customers are strategic for success and a top target for cyberattacks. In the midst of recovering from a global pandemic and increasing geopolitical disruptions, the stakes for application security have never been higher. In 2021, IDC estimated there were 195 million applications worldwide, and by 2025, this number is expected to reach 750 million (see *750 Million New Logical Applications: More Background,* IDC #US48441921, December 2021). The explosion of new applications has increased the overall attack surface, making applications a soft target for malicious actors. In a recent vulnerability report by Risk Based Security, the company that produces the popular VulnDB vulnerability database, 28,695 vulnerabilities were disclosed in 2021, the highest number ever recorded. In response, organizations are adopting DevSecOps to ensure security is considered early in application development.

IDC defines DevSecOps as a methodology that asserts that security needs to be prioritized at the beginning of the DevOps delivery pipeline. It enables development and DevOps teams to act as key stakeholders in defining and implementing security policies. The challenge lies in getting all the application security stakeholders aligned and working together. While there are undoubtedly cultural aspects of this challenge, many organizations grapple with too many different application security tools used across many different development and DevOps teams. Furthermore, these tools are not integrated, resulting in a haphazard collection of disparate security reports. This lack of supplication security clarity makes it nearly impossible for CISOs and security teams to get a top-level view of which applications across the portfolio are at risk — and why.

This white paper reveals the challenges organizations face regarding application security and DevSecOps and how a modern DevSecOps platform can help unify stakeholders while delivering continuous security and reducing organizational risk. Veracode is examined as a provider of a continuous DevSecOps security platform, including a case study of a Veracode customer that overcame many of these DevSecOps challenges and achieved a collaborative DevSecOps culture.

SITUATION OVERVIEW

As teams try to implement DevSecOps and integrate security into their pipelines, they are burdened with the need to glue together various sundered application security components. Each of these components creates different reports that must be manually unified and analyzed to make informed application security decisions. While DevSecOps security tools provide valuable insights, each focuses on a particular area; even within a specific security category, disparate vendors offer different strengths and insights. These application security data silos lead to costly and error-prone manual reconciliation of security findings and results. Some of these security findings turn out to be duplicates reported by multiple tools at various stages of the application life cycle.

Increasing awareness of application security vulnerabilities has led to an array of security tools being used across diverse security domains provided by an assortment of different vendors. This added security complexity can cause application development and DevOps teams to suffer from information overload and to lack visibility into their true security risk exposure.

The cacophony of different tools and reports requires in-house experts to manually sift through the various results and findings to piece together and prioritize application security and manage risk. Overwhelming numbers of security reports and alerts coupled with inadequate staffing inevitably leave critical vulnerabilities unaddressed. As a result, many organizations and their customers are exposed to considerable security vulnerabilities.

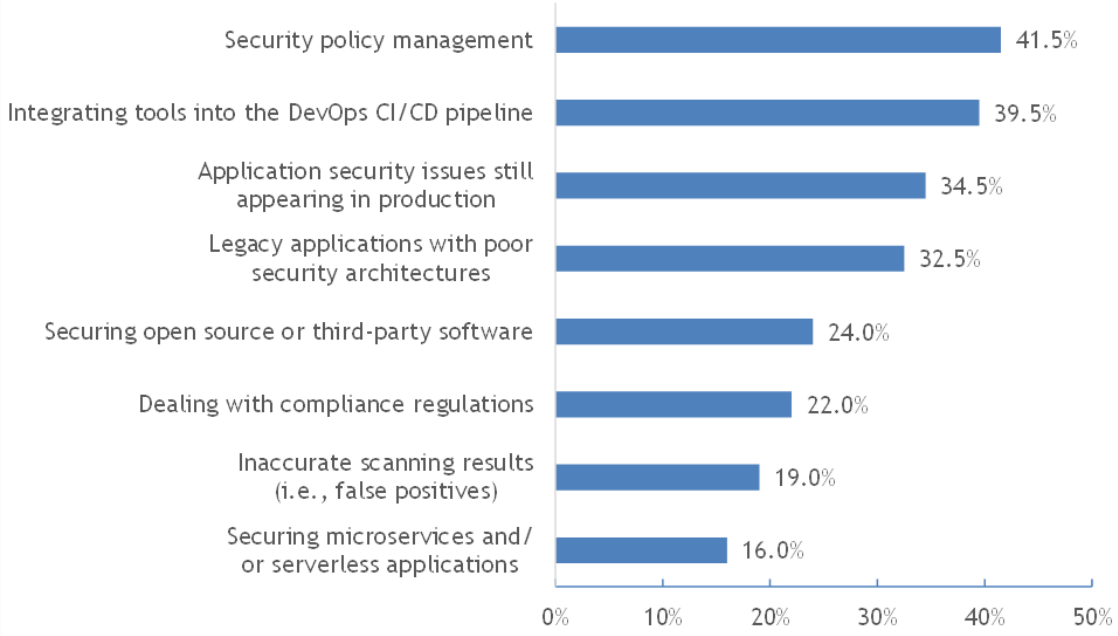
This noise makes it difficult for DevOps teams, who are generally not security experts, to effectively discern critical vulnerabilities and inject security and compliance into their DevOps pipelines. Further, the security teams cannot manage application security at scale without a centralized view of application security. Often it takes multiple weeks to patch vulnerabilities in production.

Unfortunately, bad actors move quickly, and open source vulnerabilities are typically exploited within 48 hours of the common vulnerability and exposure (CVE) being published.

Figure 1 shows the results of a recent IDC survey of teams adopting DevSecOps that showed the top technical challenges to be security policy management and seamlessly integrating DevSecOps tools into the CI/CD pipeline.

FIGURE 1

DevSecOps Adoption Technology Challenges



n = 200

Note: For more information, see *DevSecOps Adoption, Techniques, and Tools Survey* (IDC #US47597321, April 2021).

Source: IDC, 2021

Security teams, which developers outnumber at a 150:1 ratio, are ill-equipped to establish policies to ensure appropriate security due diligence at scale. This imbalance of resources makes it challenging to define, evaluate, and adjust policy for enterprise applications. Security teams become overwhelmed trying to keep up with the DevOps teams and may periodically attempt to regain control by slowing down DevOps teams to ensure application security. On the other hand, developers are incentivized to move fast and push application updates out as soon as possible.

With all these different DevSecOps tools, organizations struggle to consistently establish security policies across DevOps teams. This lack of centralized control makes it challenging to ensure that the appropriate security checks are invariably taking place across all the different applications and their associated DevOps pipelines.

Addressing the Needs of DevSecOps Stakeholders

The broad spectrum of DevSecOps tools spans the software development life cycle (SDLC), and many different tools can often equate to many different stakeholders. Unfortunately, each stakeholder has their own focus area and application security tool or report of choice. This means that each stakeholder has a limited view of application security and their own version of the truth. This siloed approach to DevSecOps can lead to miscommunications and ultimately mistrust as different stakeholders gravitate to their own data. As a result, different views of application security are created depending upon roles and responsibilities.

This siloed approach to DevSecOps can lead to miscommunications and ultimately mistrust as different stakeholders gravitate to their own data.

Table 1 illustrates some of the different responsibilities and DevSecOps concerns of some key stakeholders involved with application security, recognizing that each organization is different and may use different titles and combinations of job functions across roles.

TABLE 1

Key Stakeholder Roles and Their DevSecOps Concerns

Role	DevSecOps Concerns
Architect	▪ Struggles to incorporate application security into the architectural runway ▪ Needs insights into existing application design issues that may make or have made the application vulnerable ▪ Must go through a threat modeling exercise to develop a resilient application architecture
Developer/ DevOps	▪ Lacks formal security knowledge ▪ Aims to avoid false positives; poor prioritization of application vulnerabilities that hamper application development velocity ▪ Interested in a straightforward way to find and address insecure code ▪ Clear insights into production security challenges needed to improve application resilience
IT operations	▪ Response to production vulnerabilities promptly challenging ▪ Lacks a fast feedback loop into application design and development backlogs and has little visibility into security testing ▪ Has found it difficult to transition to DevOps, DevSecOps, and cloud-native applications
Product/ business owner	▪ Needs to ensure that end-user data is not at risk of being compromised via insecure coding or open source vulnerabilities ▪ Often finds it challenging to consider security as a functional requirement when under constant pressure to deliver new application functionality ▪ Must be able to promote application security as a differentiator rather than just a cost of doing business ▪ Wants an application security solution that does not distract developers from writing business logic

TABLE 1

Key Stakeholder Roles and Their DevSecOps Concerns

Role	DevSecOps Concerns
Risk and compliance	▪ Aims to create governance and compliance policies that ensure application security complies with relevant business regulations ▪ Needs access to security data for fast and efficient auditability of DevSecOps activities ▪ Requires that application security due diligence aligns with business regulations, strategies, risk management, and compliance policies
Security	▪ Attempts to define, manage, evaluate, and scale an organizationwide security policy to ensure an adequate level of application security ▪ Insufficient resources to keep up with all the DevOps teams and the disparate DevSecOps tools and vulnerability reports ▪ Has difficulty getting into design and development planning discussions — seen as an outsider who will slow things down

Source: IDC, 2022

While each role and tool add value to the overall application security effort, this siloed approach to DevSecOps makes it difficult for these groups to collaborate effectively. What is needed is a visible 360-degree view of your application security posture that all the DevSecOps stakeholders can share.

Increased Efficiencies Across Multiple Teams

The crux of the DevSecOps methodology is about bringing security and DevOps teams together under the common goal of delivering high-quality software quickly and securely. Misalignment among the roles that make up the DevSecOps landscape can seriously impact organizational efficiency and risk posture. This disconnect introduces more opportunities for human error and misunderstandings, and even a single mistake can have far-flung ramifications for an organization, particularly when it comes to software development and security.

Without a way to automatically assess the overall security posture of the application portfolio, let alone communicate findings, DevSecOps stakeholders and the organizations they support are in danger of operating with blind spots in a volatile application security environment.

Although there are essential separations of concerns among the different roles to drive operational efficiency, they need a common platform for collecting and sharing intelligence on application security risks. The platform needs to integrate into the DevOps pipeline and enable the development and security teams to work together – rather than against one another.

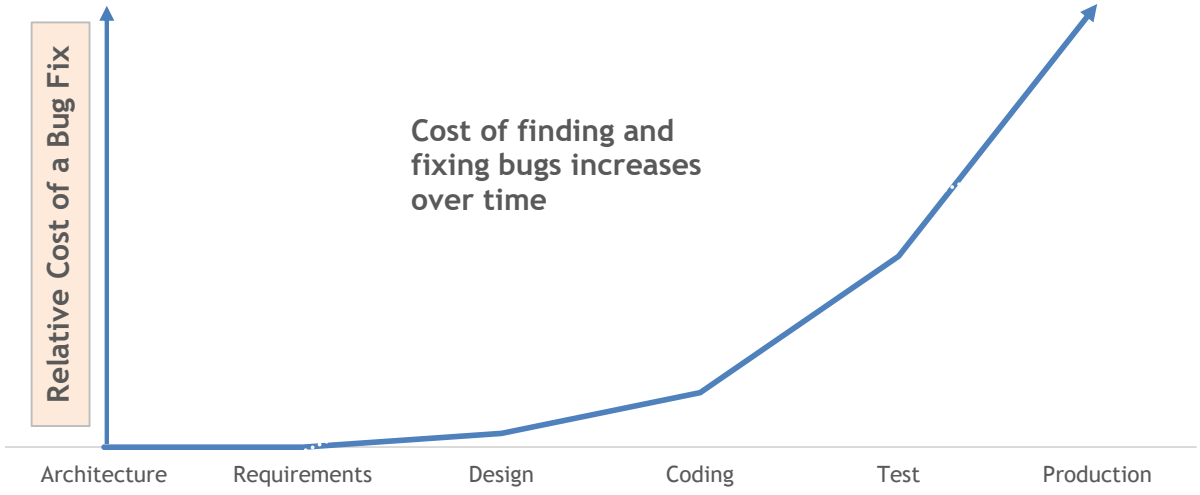
The Positive Impact of a DevSecOps Platform for Continuous Security

A DevSecOps platform provides comprehensive application security coverage, can mitigate miscommunication between roles, and provides clarity and critical business value. Working from the same data set and dashboards facilitates and simplifies collaboration among DevSecOps stakeholders. Everyone uses the same data and speaks the same language when it comes to application security and risk. A common DevSecOps platform can help close the historical chasm of mistrust between development and security teams.

IDC data indicates that just 10% of organizations adopt DevSecOps during application design and architecture (see *DevSecOps Adoption, Techniques, and Tools Survey,* IDC #US47597321, April 2021). Unfortunately, this creates a tremendous follow-on cost to the business since the cost and risk to the business increase exponentially as you move to the right of the SDLC (see Figure 2).

FIGURE 2

Cost Trends of Finding and Fixing Bugs



Source: IDC, 2022

Those organizations that inject security into their application design and architecture can uncover critical application security issues earlier, significantly reducing the risk and cost to the business.

A single DevSecOps platform can provide visibility across the SDLC and enable a beneficial application security feedback loop. With this added transparency, security issues such as insecure code architecture and risky open source components previously identified in production are unlikely to be missed when designing new application features and releases. The security team can be included in architecture and design discussions, facilitating better collaboration. Using a consolidated DevSecOps platform can provide an integrated collection of DevSecOps tools to drive automation with speed and velocity into the process. Security teams can configure security policies and efficiently monitor DevOps teams using a unified dashboard and alerts, ensuring application security without slowing things down. So DevOps velocity can increase without sacrificing quality or security, thereby reducing the risk of missing a critical security vulnerability.

A modern DevSecOps platform should not feel bolted onto the DevOps pipeline and must work seamlessly within the development workstreams. The platform should be almost invisible to developers and only noticeable when a security issue needs to be addressed. The DevSecOps platform should include inline remediation of application security issues and possibly auto-remediation capabilities.

In some cases, relevant secure coding instructions are made available, so developers not only fix the code but do so as a practical application of the new learnings. This contextual approach enables development teams to improve their responsiveness to vulnerabilities while providing insights into when and where application security is relevant, reinforcing the learning.

Further, since all the DevOps teams are using the same integrated platform, they are all using the same data and speaking a common dialect, making it is easier for developers to move between teams without facing the hurdle of getting acclimated to new DevSecOps tools every time they change teams.

Key Integrated Components of the Platform

Static application security testing (SAST) analyzes the application source code to identify potential threats or security exposures within the code. SAST should be woven into the developers' IDE and be a part of code reviews checking for insecure code before merging it into the master branch. This way, security becomes a natural part of the developer workflow by enabling developers to find and fix vulnerabilities straightaway within their IDE.

Dynamic application security testing (DAST) inspects the application at runtime impersonating an actual hacker. DAST does not require access to the application source or binaries because it tests the exposed interfaces of the running application for threats and vulnerabilities. DAST testing can be incorporated into the SDLC before the application is released into production, identifying complex vulnerabilities that can only be found by exercising a running application. This runtime interrogation of the application adds additional security assurance before being released into production.

Software composition analysis (SCA) identifies application security, quality, and compliance risk derived from embedded open source software and other third-party libraries. The constant flow of newly discovered CVEs makes it challenging to respond to a vulnerability found in production. With an integrated DevSecOps platform that includes SCA, IT operations has access to the application software bill of material (SBOM). An SBOM is akin to a manufacturing bill of materials (BOM) — an inventory that tracks the parts needed to create a product. IT operations teams equipped with this type of security information are not caught flat-footed by critical CVE announcements (i.e., Log4J CVE-2021-44228). The SBOM report enables them to quickly identify the application exposure to new CVEs and how and where they need to respond.

Compliance and governance are becoming increasingly important components of DevSecOps. As such, many DevOps teams are being expected to understand and adhere to applicable compliance regulations. With an integrated DevSecOps platform, the tracking and auditing of DevSecOps activities are monitored and logged. This tracking enables corporate governance, risk, and compliance (GRC) stakeholders to monitor compliance activities and configure compliance policies to ensure business reliance.

In this context, let's consider the security platform capabilities of Veracode.

VERACODE'S PRODUCT PORTFOLIO

Veracode's product is the Veracode Platform, which includes Veracode Static Analysis (SAST), Veracode Software Composition Analysis, Veracode Dynamic Analysis (DAST), Veracode Interactive Analysis (IAST), Veracode Discovery, Veracode Security Labs, Veracode Security Labs Community Edition, and Veracode eLearning.

Founded in 2006, Veracode has provided cloud-native, SaaS-based application security testing (AST) solutions since the launch of Veracode Static Analysis in 2007. The company is headquartered in Burlington, Massachusetts, and employs about 800 people. Veracode has scanned trillion lines of code over almost two decades, has expanded its portfolio, and has a customer base of more than 2,600 as of 4Q21. The company has grown its product line primarily organically, adding DAST, IAST, SCA, attack surface detection, manual penetration test, and experiential, contextual education to its capabilities, while providing a comprehensive platform experience like unified reporting. Veracode's former parent company's (CA Technologies') acquisition of SourceClear in 2Q18 also increased SCA functionality. Together these capabilities form the Veracode Platform, delivering comprehensive security testing in a common application.

Consistent, visionary leadership from CEO Sam King and execution from product development and go-to-market teams help sustain continued strategic performance for the company.

Company Strategy

The Veracode Continuous Secure Software Platform delivers broad capabilities spanning the spectrum of security testing requirements. Veracode's foundational product, Veracode Static Analysis, introduces SAST earlier and often in the development cycle by scanning in three locations: IDE Scans are done prebuild and provide flaw feedback in the developer's context, Pipeline Scans are run within the CI/CD pipeline at every code commit, and Policy Scans evaluate the entire application against one policy and summarize its security posture in a singular report. Veracode Software Composition Analysis can run SCA alongside these Policy Scans or throughout the development life cycle. Powered by machine learning, Veracode Software Composition Analysis provides insights in real time; prioritizes findings based on technical risk, size of change, and effort to fix; and automates remediation through autopull requests.

Next, the Veracode Platform provides two mechanisms for web application scanning. Veracode Discovery identifies and inventories public-facing applications inside and outside an organization's web perimeter through a combination of DNS keyword searches, production stage crawling, and page redirect analysis. This attack surface detection advises which web applications should be included in the scans conducted by Veracode Dynamic Analysis, which performs automated, real-time tests to find exploitable vulnerabilities. New API scanning capabilities were incorporated into Veracode's DAST solution in 4Q21 as a part of the core product. Veracode Interactive Analysis ties up the platform, leveraging CI/CD tools and the existing test scripts that development teams have already created to exercise the scan. Built on a proprietary language, Live Track, the tool deploys a single, language-agnostic agent that externally analyzes the code, instead of instrumenting from within the code itself.

Complementing the AST capabilities of the platform, Veracode offers training for security testing that enables developers to fix their vulnerabilities in addition to finding them. In Veracode Security Labs, developers are provided experiential and hands-on training to teach AppSec skills. The lab-based approach utilizes practical examples and allows developers to apply new skills immediately in

interactive threat scenarios. Veracode delivers Security Labs in both a community and an enterprise edition, offering additional training topics and features to paid users. In addition, the Veracode Platform includes a suite of courses, videos, and tutorials in Veracode eLearning to further disseminate AppSec awareness and knowledge throughout an organization.

Veracode is differentiated in offering a single, integrated, and open application security platform solution that gives customers a broad view of security challenges. The platform's capability to analyze across the development phases for proprietary, open source, and functional code is complemented by security experts, hands-on training, and remediation resources. As a result, the platform helps companies reduce security risk in part by learning how to prevent critical security flaws before they get created. Veracode also balances developer-centered testing capabilities with central compliance and governance functionality. This consonance allows developers to prioritize their remediation efforts, security teams to understand their security posture, and executives to make data-driven decisions. In that context, Veracode also evolved a more flexible policy engine within its SCA engine in 2H21, with support for a variety of use cases such as license risk management to help support requirements for legal and governance, risk, and compliance. Veracode plans to extend its policy capabilities across the platform to help unify and simplify policy management. This can help contextualize reporting and analytics to make it actional for organizations. IDC's DevSecOps research indicates security policy as a primary and growing concern and area of focus.

Veracode began a full digital transformation on its own platform in 2021, implementing a new product architecture employing containerization, Kubernetes orchestration, service mesh, and single-click deployment. (Evolving its own product portfolio also gives Veracode context for similar evolution needed and experienced by its customers.) This architecture underpins the new Veracode European region, which provides cloud-based SaaS capabilities with full data residency for EU customers, and the Veracode FedRAMP instance, which will serve U.S. government customers. The company is on target to achieve FedRAMP Moderate certification in 2Q22. Veracode provides its products as a multitenant, cloud-based SaaS solution, offering a cost-effective strategy to deploy software that centralizes IT management, security, and infrastructure to help lower application security program costs.

Customer references with whom IDC spoke chose Veracode as their AST vendor because of the company's broad portfolio, or what they described as the ability to "do it all." One customer mentioned that it was particularly attracted to Veracode's robust integrations, as the company has grown through acquisition and with that has many teams working with different tooling. Another customer indicated that Veracode's SaaS delivery model was standout at the time and found that onboarding and implementation of the platform were the fastest it had experienced. Customer references also spoke highly of collaborative support from Veracode to enable success of security programs from an organizational and process perspective (in addition to consistent automation adoption) and to engage developers with better security practices as part of code creation. In that context, let's consider the experience of one of these references.

Supply Chain Provider Manhattan Associates Leverages Veracode Platform to Coordinate Security Strategy for Microservices and DevOps

Manhattan Associates, a 25-year-old supply chain solution provider with approximately 4,000 employees and an R&D department where the company has developed more than 30 solutions (pivoting to cloud-native and microservices offerings over the past two to three years), adopted the Veracode Platform as part of its security strategy, which has evolved since 2015. Partnering closely with Veracode, the company has benefited from application security testing, security composition

analysis (SCA) and penetration test automation, process and organizational change, and improved visibility and execution to help reduce risk, increase efficiency, and create security policies. It also leverages the security practices it has evolved to provide support for its customers as part of product and service offerings for corporate compliance.

Security Challenges

During the 2014 time frame, the company started waking up to security in part due to publicized security breaches on the part of other companies that garnered attention. Prior to that, its teams were doing DAST scanning and experiencing a lot of friction understanding results due to tremendous false positive rates; with thousands of issues to look at, knowing which to consider and which to ignore became a significant impediment to progress. According to George Garza, director of Risk and Security at Manhattan Associates, DAST was the wrong place to start as it created significant overhead for reviewing results. "At that point, we shifted and started looking at SAST, which gained momentum and made more sense to be able to resolve flaws from the code perspective first," said Garza. "We decided that a more effective approach was to begin with static analysis and then augment with dynamic analysis to help set policy and prioritize."

Adopting and Leveraging Veracode

The teams did an evaluation and opted for Veracode due to its cloud support and the strength of its SAST product and an easy on-ramp, with a nonlicensed approach pilot to run initial scans with four to five licenses. "Within 35-40 days, we were scanning and resolving issues and had visibility that hadn't been seen previously and began buying licenses as fast as we could implement them (up to around 47 licenses currently)," said Garza. "While SAST offers 'bread and butter' capabilities for us, we also added DAST and pen testing."

Veracode helped the company transition and manage across a broad spectrum of teams — with 400 developers and merely two support staff for security initially, the company pivoted from an ineffective, centralized security approach organizationally to distributed security. The company established 12 security champions who became associated with each team. As the company moved to microservices, it paralleled decomposition in sandboxes to align with developers and shifted its approach to be more developer centric and aligned.

Leadership for this initiative focused on risk and security operations, coordinating application security and quality assurance.

"The shift to cloud native and microservices over the course of 24 months drove tremendous adoption of automation," said Garza. "We had already moved from monolithic scanning to decomposing applications in the sandbox and shifted from a cadence of once or twice per month to two to three times per week." The decomposition of the components made it easy to align the results back to the teams and across resources to roll up to the main application. Veracode was a key, active partner for the organization in its transition to cloud native and microservices, as the company was going through its own transition, and collaboration for both process change and additional product evolution were pivotal resources for Manhattan Associates (along with broader discussions with other transitioning organizations).

The company has two architecture branches — one for application architecture (upstream for R&D) and another for DevOps architecture. Uniting the organization includes coordination across architects, who must be involved from the beginning. Over the course of the past 12-18 months, the organization has been shifting from a "push" to a "pull" momentum, designing a holistic system beyond the data.

This approach is one of "what can the system I have in place teach me" and aligning with the application teams to establish preventative measures up front architecturally and in other ways. The company has been partnering closely with Veracode to help enable this key shift.

Manhattan Associates is now leveraging security testing/scanning as part of its DevOps strategy in a variety of ways using the Veracode Platform. The company's teams have incorporated AST as part of its DevOps pipeline and relevant criteria. The company is scanning every few days to see if any flaws exist with an automated system that produces results prior to code getting committed and as code gets committed. Garza spearheaded this initiative and previously led the company's quality engineering program before moving to the security side in 2015. Much of the company's testing is now embedded in application coding; the company shifted to functional testing and workflows to unit tests in code so that every developer is running one long series of tests. In its model, every developer runs tests on their components and then runs product assurance tests and automation tests as part of a more of detailed function, which is timed to dovetail with SAST on a two-week delivery cycle to a Change Advisory Board (CAB). The CAB reviews testing results for functional and performance engineering along with security scanning results that are integrated with test management, automation, repository planning and tracking, and flaw identification. The CAB determines if the delivery is to be allowed into production for customer use.

For the scanning itself, the company has a CI/CD staff member who allocates half their time to enable and monitor scans and make sure that the scan runs and completes. The company has about 70 scrum teams at any given time, and security champions number typically one per scrum team. The security champions monitor and respond to scanning results and resolve or assign issues that appear to scrum teams. "An advantage of Veracode is that flaws are reported with clear data paths, which aid the developer in identifying specific lines of code to address," said Garza. "They keep the machine running constantly [and] compile and configure to make it efficient to consume, and developers depend on their security scan cycles as if they were a QA team." Another advantage of Veracode in this context is that it manages the opening and closing of flaws automatically (e.g., Veracode would report a flaw "number 10," go and fix it, and the whole thing closes with automated confirmation [versus the labor-intensive and error-prone process of manual management and confirmation of flaw resolution]). The company said that another value of Veracode in this context is the self-managing ticketing process, and that once an issue is resolved, it rarely has reopenings. (At this point, Manhattan Associates takes for granted fundamentals of automation that the company leverages with Veracode.)

Risk Visibility and Management, Efficiency Outcomes, and Recommendations

Overall, one of the key benefits for Manhattan Associates is the ability to manage risk with significant feedback mechanisms with regard to current state and emerging trends leveraging Veracode. New team members might join and inject flaws without realizing it; for instance, with multiple moving targets and multiple vulnerabilities identified (including third-party libraries), Veracode continues to help the organization improve its scanning strategy to move toward less and less risk. The organization leverages statistics, incorporates methodologies, and increases efficiency (for instance, by helping ensure that the company doesn't duplicate effort by scanning the same thing in two different places). Automated scanning helped eliminate scan-to-scan inconsistencies while avoiding time spent on "reconciling scans." The organization saved developer prep time from 30 minutes to 2 hours per scan and moved from merely 5,000 scans (3 billion lines of code) in 2019 to 18,000 scans (or 30 billion lines of code) in 2020. Both Veracode's scan data path and readouts on more complex flaws reduce developer time to gain clarity and resolve issues. And staff alignment from the sandbox to agile scrum teams increases developer efficiency by reducing time spent to discover flaws and remediate them.

Garza recommends leveraging service-based solutions and a security platform that is hosted where organizations don't have to install and configure and, most importantly, a provider that can actively partner and collaborate with a trajectory that aligns with core emerging needs — considering the total value proposition. In that context, the Veracode Platform is a continuous scanning engine that can enable a strategy that places less emphasis on a product portfolio and more on a platform that learns and adapts.

STRENGTHS

Veracode's ability to provide the company's customers with a broad and deep set of automated security solutions, spanning SAST, DAST, SCA, IAST, and attack surface detection and delivered through a unified platform, makes it a dominant provider in the highly competitive DevSecOps market. Veracode's data layer — that can help turn nearly two decades of data and learning into intelligent orchestration and remediation — is a differentiator. Incorporating automation into practice is another core focus for Veracode. The inclusion of practical skills training and mentoring for security testing in the platform recognizes the imperative for developer training to enable execution and tools adoption. And offering a community edition of Veracode Security Labs helps seed the market, increase context for prospects, and benefit the community overall. Veracode commonly comes up for user evaluations as part of RFPs, and for organizations needing cloud (but not on-premises) solutions, Veracode stands apart. Other areas of strength for Veracode include streamlined GRC, policy management, and integrated reporting and analytics. Veracode's leadership has been consistent across multiple acquisitions, and the company's acquisition by Thoma Bravo in 2018 provides it with the independence, expertise, and financial capabilities needed to continue to grow. Its most recent acquisition by TA Associates in 1Q22 strengthens Veracode's position strategically in a highly dynamic, competitive, and business-critical market.

CHALLENGES

The application security testing marketplace is crowded, with many players offering similar base-level functionality. In addition, communicating the extent of Veracode's capabilities in brief is challenging. As a result, Veracode must work diligently to define, delineate, and convey its differentiators. Although Veracode offers a broad set of security tools, it has some coverage area gaps such as configuration files and container scanning, which the company says it is working to address in 1H22. (Veracode's teams in this context are seeking to expand beyond a mere lexical scanner. Veracode has chosen to solve a more complex problem of providing in-context security information and subsequently pushed back delivery of initial capabilities until later in 2022.) In addition, because Veracode scans binaries and not source code, it can be harder to match the source code to the binary code and correlate findings, according to one reference. Finally, Veracode's choice to forgo an on-premises offering limits customers' deployment options, which can disqualify the solution for some organizations with sensitive data and security requirements.

CONCLUSION

- User demand and growth in this development arena result from the need for code quality analytics and insight into impact on quality and security across application portfolios in increasingly complex development and deployment environments. When organizations empower developers with appropriate automated tools, process/policies, and contextualized training, the results are more secure applications, faster remediation, and developers taking ownership of security.
- With the adoption of multiple scanning and other DevSecOps automation tools (most organizations have many), both orchestration and security policy management strategies are a core execution gap and opportunity.
- User engagement and the need for visibility into architecture and code quality and security, along with effective metrics to assess performance of internal and external resources, are driving adoption in this area of automated software quality and DevSecOps adoption.
- In a volatile economy (along with geopolitical upheaval), financial constraints, global competition, and innovation drive demand for rapid access to AST, SCA, and quality solutions and metrics to evaluate code and project success.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com