William Blair

Equity Research
Technology, Media, Communications

July 7, 2025

Jonathan Ho +1 312 364 8276
Jason Ader, CFA +1 617 235 7519
Arjun Bhatia, CPA +1 312 364 5696
Jake Roberge +1 312 364 8056
Sebastien Naji +1 212 245 6508
Garrett Burkam +1 312 364 5152

On the Ground and In the Cloud

A Developer Technology Quarterly: DevSecOps Refresh Edition

Contents

Introduction

On the Ground and In the Cloud is a quarterly publication produced by the William Blair technology team that delves into trends impacting developer technologies across a wide scope of topics that includes software development, DevOps, database, analytics, and observability. Over the past decade, developers have become increasingly important influencers across all organizations, as software applications and digital transformation have become critical to business operations, customer interaction, and competitive advantage. More recently, this trend has been accentuated by black swan events like the COVID-19 pandemic and a slew of software supply chain attacks. Developers represent the early adopters who will determine the success of a particular software product or project. As a result, we believe it is essential to examine the key technological and cultural dynamics impacting this all-important cohort of workers.

In this DevSecOps Refresh edition of *On the Ground and In the Cloud*, we provide updated results from our most recent proprietary survey of developers/practitioners, examine the overall DevSecOps market and its major players and how it has changed over the last year, and discuss the latest trends in the space. We also provide our thoughts on what impact AI might have on DevSecOps, and we highlight relevant private companies.

Executive Summary

DevSecOps is the practice of embedding security throughout the software development lifecycle (SDLC) to ensure that security testing, policies, and controls are integrated directly into developer and DevOps workflows. Instead of treating security as a separate phase at the end of the development process, DevSecOps makes it a continuous and shared responsibility across IT operations, development, and security teams. This approach aligns with agile and cloud-native software delivery methods, which enables faster and safer software releases by catching issues earlier in the process and fostering greater collaboration between traditionally siloed teams. Applications and APIs also represent a major attack vector, with 25% of all data breaches targeting application layer vulnerabilities, according to Verizon's latest Data Breach Investigations Report. Software supply chain security is also gaining more attention after high-profile breaches, like the SolarWinds and Equifax attacks, highlighted the need to secure all elements involved in creating and delivering software, especially open-source software given that it accounts for up to 90% of modern applications. These types of attacks are showing no signs of slowing, with Check Point recently discovering a threat actor known as Stargazer Goblin that had created a network of over 3,000 GitHub accounts to distribute malware and malicious links as part of a distribution-as-a-service (DaaS) operation.

Please see our primer piece on DevSecOps here: On the Ground and In the Cloud: DevSecOps Edition.

We believe DevSecOps is essential because traditional security practices are siloed and too slow and reactive for today's rapid software delivery cycles. DevSecOps platform solutions help organizations detect and remediate vulnerabilities early in the development process by integrating security into the entire SDLC. These solutions provide organizations with the ability to scale security across multiple teams and pipelines; enhance visibility into application security and compliance posture; improve collaboration between developers, security, and IT operations teams; support security for modern application architectures; better integrate DevSecOps tooling; and embed security throughout the software development process. DevSecOps solutions also reduce the cost of remediating vulnerabilities while enhancing developer productivity to ultimately enable organizations to ship secure code faster with fewer disruptions and lower long-term security and compliance costs.

From our conversations with private companies, public companies, and industry experts in the space, we believe the DevSecOps competitive landscape has four major types of players: 1) legacy application security vendors (like Cisco, Broadcom, IBM, and Micro Focus/OpenText); 2) modern application security vendors (like Snyk and Contrast Security); 3) developer platform providers (like GitHub and GitLab); and 4) cloud-native application protection platform (CNAPP) vendors (like Wiz, Sysdig, Palo Alto Networks, and CrowdStrike). In our view, developer platforms, modern application security vendors, and CNAPP vendors have the right to win in the market over the medium term. Developer platforms benefit from unmatched integration into developer workflows, broad developer adoption, and significant platform effects, making these solutions easy choices for developers already using the platform to ship software. However, security is not these platforms' core competency, so we believe CNAPPs and modern application security vendors also have the right to win. Modern application security and DevSecOps vendors are focused on developer security with deep expertise in this domain, while CNAPPs offer unified cloud and application security solutions that secure software all the way from code to runtime. Longer term, we believe modern DevSecOps capabilities are likely to face competitive pressure from broader platforms that increasingly offer similar functionality and will be consolidated into developer platforms and CNAPPs. In our view, developer platforms and CNAPPs have the value propositions of reducing tool sprawl, unifying security and development workflows, and making security a more intrinsic part of the software development lifecycle with improved capabilities over time. We also believe that hyperscalers are likely to compete more seriously in the DevSecOps space, as they own the cloud infrastructure where modern applications are being built and run and can integrate security capabilities, which could accelerate given Google's recent acquisition of Wiz.

Key trends shaping DevSecOps include the rise of platform engineering, AI and automation, software supply chain security, application security posture management (ASPM), application detection and response (ADR), growing but challenging adoption, and the preference for platform solutions. We believe artificial intelligence is reshaping DevSecOps by automating vulnerability detection, event triage, incident reports, session summaries, and remediation while also introducing new risks and challenges with AI-generated code. We view AI as a double-edged sword, as it brings significant advantages in terms of developer productivity and cybersecurity efficacy, but also new challenges and security risks. For example, Meta conducted a study on AI code generation and found that the better an LLM is at writing code, the worse it is at avoiding vulnerable coding practices. We expect this to improve over time, but it illustrates the heightened risk AI brings in the near term. Longer term, we believe AI agents will further drive the need for DevSecOps tools as the software developer role shifts to the development of AI agents that will need to be secure by design. Overall, we believe the DevSecOps market is set to benefit from AI as a result of the advantages of AI-enhanced cybersecurity, developers using it to write more code, DevSecOps tools becoming more efficient and user-friendly, and the need to secure AI itself, all of which we expect to contribute to higher demand and adoption rates.

Key Takeaways

1. **Modern DevSecOps vendors are gaining market share due to greater developer adoption, integrations, performance, new technology coverage, and usability.** We believe legacy application security vendors have major limitations with integrating into CI/CD pipelines, poor delivery performance, and lagged coverage for emerging threat vectors. Traditional tools also typically function as standalone products used solely by security teams, leading to an inefficient back-and-forth workflow with developers that slows software development and leads to security issues being identified late in the process. Modern vendors, on the other hand, solve for these challenges and have a major advantage with greater developer adoption given that they are designed to be used by developers. The shift to cloud has also benefited modern vendors, as legacy tools were originally built for on-premises environments and have been slow to support newer cloud technologies.

2. **DevSecOps market remains highly fragmented and relatively immature.** IDC forecasts the overall DevSecOps software tools market to grow to $15.6 billion in 2028, representing a five-year CAGR of 21.6% (from 2023 through 2028), driven by the need to ship applications securely and quickly. The top five market share leaders (Synopsys, Microsoft, Veracode, Palo Alto Networks, and Checkmarx) represent just 26.5% of the overall market, suggesting that the market is still dynamic and maturing.

3. **In the intermediate term, we believe developer platforms, CNAPPs, and modern application security vendors have the right to win in the DevSecOps market.** Developer-centric platforms benefit from unparalleled integration into developer workflows, broad adoption, and significant platform effects. Security, however, is not these vendors' core competency, so we believe CNAPP vendors and modern application security vendors also have a right to win. CNAPP players enable unified cloud and application security with comprehensive solutions that help bridge software development and runtime environments. We believe modern DevSecOps vendors, like Snyk, are well positioned over the medium term due to their developer-first approach and ease of use, allowing developers to proactively address security issues directly in code. Modern vendors have been expanding their capabilities, though they face competitive pressures from broader platforms that increasingly offer similar functionality. In our view, however, modern DevSecOps vendors' specialization in developer security puts them ahead of the competition and provides the opportunity to potentially partner with CNAPP vendors or continue expanding capabilities.

4. **Longer term, DevSecOps capabilities will likely consolidate into broader platforms offered by developer platform providers and CNAPP vendors.** In our view, organizations have a strong desire for simplicity, reduced tool sprawl, and unified security and development workflows, and as security becomes a more intrinsic part of the software development lifecycle over time, platforms providing end-to-end software development and cloud management capabilities have very strong value propositions. We believe developer platforms, like GitHub and GitLab, and CNAPP vendors, like Wiz, Palo Alto Networks, and CrowdStrike, will ultimately consolidate DevSecOps features into a broader platform solution. Hyperscalers (Amazon, Microsoft, and Google) also have an opportunity to consolidate DevSecOps features longer term, as they own the cloud infrastructure and can integrate security capabilities, which could accelerate given Google's recent acquisition of Wiz, in our view.

5. **Looking ahead, we believe the DevSecOps market will move toward more unification, intelligence, and alignment with business needs through a consolidated set of platforms covering application security across the full spectrum of code to runtime.** We believe these platforms will leverage AI and automation for speed and accuracy, emphasize software supply chain integrity, and be embedded into developer workflows to minimize as much friction as possible. We expect major competitors in different areas (like the hyperscalers, developer platforms, specialized DevSecOps vendors, and CNAPPs) to play distinct roles based off their core competencies, and that customers will likely grow their DevSecOps programs with one of these types of vendors depending on their type of organization and its maturity level.

6. **Purchases of DevSecOps tools are still ultimately made by security teams, as security budgets largely win out over developers.** Developers and security teams used to have relatively comparable influence on decision making. However, as breaches have taken place and security has become a higher priority, developer influence appears to be waning relative to the budget and authority wielded by security teams. Based on our discussions, it appears that CISOs, application security teams, and DevSecOps teams typically control the budget for making purchasing decisions for DevSecOps tools, while developers do not currently have much influence despite them also using these products. Thus, vendors need to provide a tool that is developer friendly while communicating its value to a security person, which we believe has been a challenge in the industry and an inhibitor to adoption because developers simply will not use the tool if it is too cumbersome for their workflow.

7. **DevSecOps tool capabilities are increasingly overlapping with broader platforms as vendors continue to expand their capabilities.** We believe enterprises are seeking holistic solutions that seamlessly integrate with CI/CD pipelines to have all necessary security functions in one place, which will likely contribute to further consolidation going forward. We believe the distinction between DevSecOps and cloud security tools will continue to fade over time as they become part of one toolchain that delivers continuous security from code to cloud. DevSecOps submarkets, software supply chain security, and API security are also blending together and further blurring the boundaries of DevSecOps. In our view, the three areas experiencing consolidation in DevSecOps are application security testing vendors, developer platform providers, and CNAPP vendors. We also expect vendor consolidation through acquisitions to accelerate, as 2024 had record-high M&A activity in the software development and deployment space.

8. **Overall, the DevSecOps market is set to benefit from AI, but it also represents one of the biggest security challenges today.** We expect AI to drive higher demand and adoption rates in DevSecOps as a result of the advantages of AI-enhanced cybersecurity capabilities, AI coding assistants being leveraged to write more code that needs to be secured, DevSecOps tools becoming more efficient and user-friendly, and the need to secure AI itself. Longer term, we believe AI agents will further drive the need for DevSecOps as software development begins to focus on developing AI agents that will need to be secure by design like an application. We view questions over how to safely use AI as some of the most important cybersecurity questions that will need to be answered before enterprise adoption accelerates.

9. **Automation and developer experience are critical components of DevSecOps tools.** We believe DevSecOps revolves around automation, as it helps remove the friction between DevOps and security teams and enables faster and safer development cycles. We also believe automation will be at the center of next-generation tools, especially as AI adoption accelerates, for better security testing, faster vulnerability detection, and automatic remediation of code issues. Automation is also important for improving the developer experience as to not impede and slow down their workflows. Most developers want to focus on writing code, and automation reduces the cognitive load for developers, with automated security measures integrated directly into their workflows, making it easier for developers to resolve issues as they arise and helping with DevSecOps adoption.

10. **DevSecOps adoption is mixed among organizations and maturity levels vary greatly, even within organizations.** We believe there is further room for adoption as less than half (47%) of organizations regularly employ DevSecOps practices, according to a survey by Techstrong Research. Many organizations have been slow to adopt DevSecOps practices and technologies because application security is difficult and constantly evolving with new technologies (like AI) and software supply chain concerns, DevSecOps requires a lot of tools and resources that may be new attack vectors, collaboration between different teams can be complex, and developer experience remains a challenge. We believe every DevOps program today should be a DevSecOps program given the fast pace of modern software development, the fact that cybersecurity risk now represents overall business risk, and that attacks on applications and APIs continue to increase.

11. **Despite challenges, DevSecOps adoption continues to grow as organizations recognize the importance of delivering secure software and the long-term benefits of reduced vulnerabilities, faster incident response times, and improved compliance.** We believe organizations will continue to adopt and mature DevSecOps practices as platform engineering becomes more popular, software supply chains need greater security, AI drives more code and vulnerabilities, developers become more familiar with security tools and aware of secure coding practices, and organizations recognize the need for their software to be secure by design.

12. **DevSecOps is becoming synonymous with software supply chain security.** DevSecOps tools are increasingly focusing on securing the software supply chain, with a greater emphasis on managing open-source components, application build integrity, and SBOM generation as software supply chain exploits remain on the rise. We believe open-source software risk is top of mind for organizations as up to 90% of a modern application is composed of open-source components. Effective software supply chain security involves managing these open-source and third-party elements, secure coding practices, and CI/CD security, all of which overlap with DevSecOps practices.

13. **DevSecOps platforms embed security into software development workflows to deliver secure software without sacrificing the rapid pace of modern development practices.** DevSecOps platform solutions help organizations detect and remediate vulnerabilities early in the development process by integrating security into the entire software development lifecycle. These solutions provide organizations with the ability to scale security across multiple teams and pipelines; enhance visibility into application security and compliance posture; improve collaboration between developers, security, and IT operations teams; support security for modern application architectures; better integrate DevSecOps tooling; and embed security throughout the software development process.

Examining the DevSecOps Market Landscape

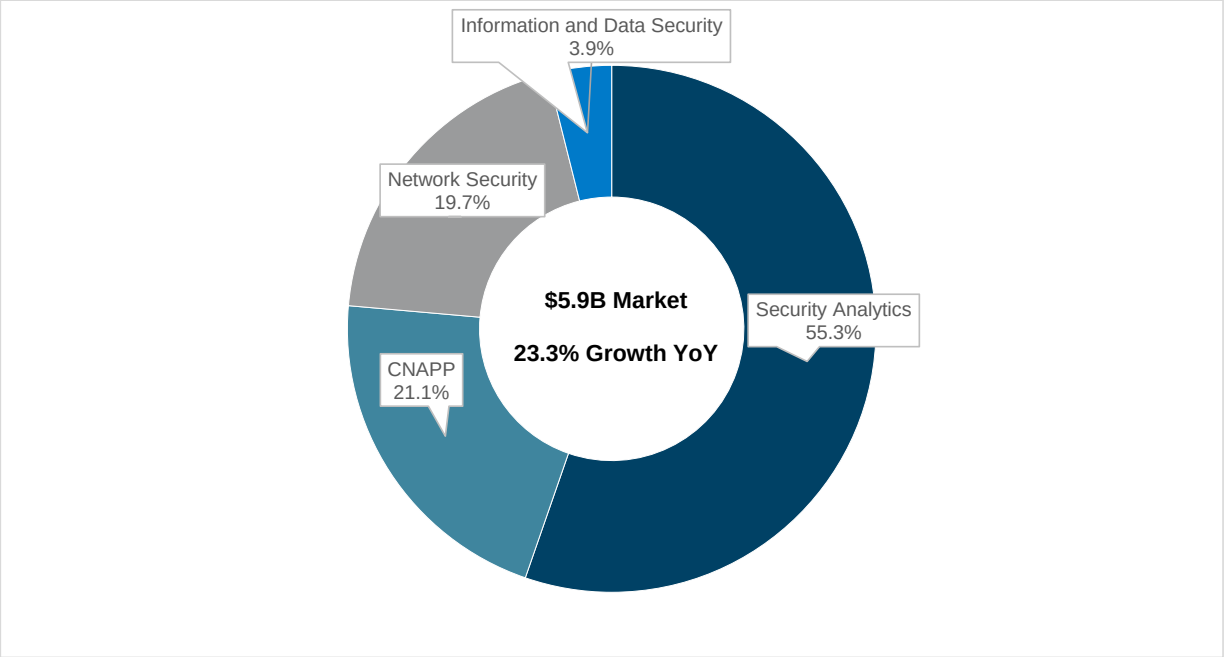
In IDC's Worldwide DevSecOps Software Tools Market Shares snapshot for 2023, it estimated the market size to be $5.9 billion with growth of 23.3% from the prior year. The top five leading vendors in the market are Synopsys, with a 6.6% market share; Microsoft, with a 5.6% share; Veracode, with a 5.4% share; Palo Alto Networks, with a 5.3% share; and Checkmarx, with a 3.5% share. Together, these five vendors represent just 26.5% of the overall market, which we believe indicates that the market is still evolving and relatively immature. According to IDC, in many mature software markets, the top five vendors represent more than two-thirds of the total revenue.

Exhibit 1
On the Ground and In the Cloud; A Developer Technology Quarterly
DevSecOps Market Shares, 2023 ($ in Millions)

	2021	2022	2023	2023 Share (%)	2022-2023 Growth (%)
Synopsys	$314	$344	$388	6.6%	12.9%
Microsoft	$181	$257	$332	5.6%	28.9%
Veracode	$225	$272	$318	5.4%	16.8%
Palo Alto Networks	$146	$222	$312	5.3%	40.9%
Checkmarx	$151	$172	$209	3.5%	21.9%
Snyk	$62	$143	$208	3.5%	45.0%
OpenText	$192	$192	$193	3.3%	0.2%
IBM	$150	$158	$166	2.8%	4.8%
Akamai	$121	$138	$157	2.7%	14.2%
GitLab	$49	$96	$156	2.7%	62.3%
Trend Micro	$110	$128	$142	2.4%	11.4%
Google	$67	$101	$122	2.1%	20.5%
Amazon Web Services	$74	$94	$107	1.8%	13.7%
Lacework	$58	$81	$100	1.7%	23.1%
F5	$59	$70	$87	1.5%	24.3%
Cisco	$70	$73	$76	1.3%	4.7%
Perforce	$56	$63	$73	1.2%	15.6%
Mend	$41	$55	$64	1.1%	15.7%
Salt Security	$19	$34	$62	1.1%	83.1%
CyberArk	$41	$48	$62	1.0%	27.7%
Contrast Security	$42	$52	$60	1.0%	16.0%
Aqua Security	$26	$35	$56	1.0%	62.3%
Other	$1,614	$1,949	$2,441	41.4%	25.3%
Total	**$3,867**	**$4,775**	**$5,889**	**100.0%**	**23.3%**

Source: William Blair Equity Research based on IDC estimates; IDC DevSecOps Software Tools Market Shares, August 2024

Exhibit 2
On the Ground and In the Cloud; A Developer Technology Quarterly
DevSecOps Market Shares by Functionality, 2023



Source: William Blair Equity Research based on IDC estimates; IDC DevSecOps Software Tools Market Shares, August 2024

We believe there are four main groups of competitors in the DevSecOps market: 1) legacy application security vendors, 2) modern application security vendors, 3) CNAPP players, and 4) developer platform providers. Over the long term, we believe developer platforms (GitHub and GitLab) and CNAPP vendors (Wiz, Palo Alto Networks, and CrowdStrike) have the strongest right to win market share. Developer platforms benefit from unmatched workflow integration, developer familiarity, and platform effects of developers naturally adopting built-in security capabilities as they streamline and consolidate tools. CNAPP vendors offer unified cloud and application security with broad capabilities (security from code to runtime) and deep cloud-native security expertise. In the medium term, we believe modern application security vendors (such as Snyk and Contrast Security) have a place in the market, as they are highly innovative and developer-centric but face pressure from platforms that are increasingly embedding security functionality. In our view, these vendors will have a place in the market as long as the developer platforms and CNAPP vendors lag in their developer security capabilities. They could also partner with CNAPP vendors, though longer term, we see potential for these broader vendors to more effectively compete or possibly acquire some pure application security vendors to ensure they have a strong set of capabilities. We believe legacy vendors are currently losing market share and are continually having to adapt to modern workflows. Overall, we believe the value propositions of developer platforms and CNAPP vendors are very strong and that they hold a strategic advantage in the DevSecOps landscape based on integrated workflows, platform consolidation, enterprise adoption, and the accelerated shift toward cloud-native architectures.

Legacy Application Security Vendors

Legacy vendors in the DevSecOps space are those that typically originated from early application security tools before the cloud-native era. These vendors include companies like Cisco, IBM, Broadcom, and Micro Focus (OpenText) that generally built their reputations on traditional static application security testing (SAST) and dynamic application security testing (DAST) tools that were usually delivered as on-premises enterprise solutions. We believe these legacy tools are not built for the speed that DevSecOps requires and are less integrated into developer workflows. Over time, legacy vendors have expanded their solutions by adding capabilities (such as software composition analysis) and offering cloud options in order to stay relevant, but oftentimes the market still views these legacy products as heavy or slow compared with newer competitors. Legacy vendors also typically serve large enterprises and government organizations with compliance needs, and their tools often excel in accuracy and policy enforcement but struggle with speed and developer adoption. In many cases, security teams have to manage these tools separately, creating a stack of disconnected application

security tools that add noise and bottlenecks to the software development process. We believe these gaps have created opportunities for newer vendors to introduce more streamlined and cloud-friendly solutions.

Modern Application Security Vendors
Modern application security vendors, such as Snyk, Veracode, Contrast Security, Synopsys, and Checkmarx, focus on developer-first security (with tools like SAST, SCA, DAST, IaC scanning, secrets detection, and more) that is embedded into development workflows and CI/CD pipelines. These companies aim to help developers find and fix vulnerabilities early in the software development lifecycle and they tightly integrate products with code repositories, internal developer environments, and pipelines, helping developers remediate issues in code and configurations before deployment to make security a seamless part of software delivery. This proactive approach reduces the cost of fixes and security debt. These modern solutions also empower developers to write secure code with real-time feedback and security teams gain visibility through dashboards and policy controls. Modern application security vendors make security a normal part of development while speeding up remediation and fostering a security-aware development culture.

Cloud-Native Application Protection Platform (CNAPP) Vendors
CNAPP vendors in the DevSecOps space, like Palo Alto Networks, CrowdStrike, Wiz (Google), Sysdig, Lacework (Fortinet), Check Point, and more, focus on offering end-to-end cloud security from development through runtime. These players incorporate DevSecOps capabilities into broader cloud security suites that also cover runtime workload protection and posture management. These vendors typically offer a single platform for multi-cloud environments where misconfigurations, vulnerabilities, and threats are tracked with context. By scanning IaC templates, container images, and other artifacts in CI/CD pipelines, cloud risk visibility is extended into the software development process. This means developers get feedback on cloud security issues before deployment within the same platform that will help protect the application when it is running in production. The value proposition with these vendors is unification, tying together developer and runtime security while prioritizing contextualized risk.

Developer Platform Vendors
Major developer platforms like GitHub and GitLab have expanded into DevSecOps by embedding security features directly into various development workflows on their platform. GitHub Advanced Security adds native security tools to its platform with features for static code scanning (SAST), secrets scanning, dependency checks, security workflow integrations, and AI-assisted remediation. These features are tightly integrated into GitHub's developer workflow, which we believe helps lower the friction between security and developers and thus encourages adoption. GitLab has been a pioneer in integrating DevSecOps into a single application and has a comprehensive suite of security testing tools built into its CI/CD pipeline. We believe this approach helps reduce tool sprawl from external security tools and allows developers to address security findings within their normal development process that they are already familiar with. However, these built-in-tools need to balance depth with ease of use, as they currently do not provide the same level of security as dedicated DevSecOps tools. Therefore, we believe modern application security vendors remain relevant for organizations with advanced security needs, though many organizations also find that the built-in security tools cover the majority of their needs. These developer platforms also support integrations with third-party security tools to allow users to use external tools if needed. We believe these platforms reduce the need to purchase many standalone security tools and have the strong value proposition of being natively integrated in workflows that developers already use and are familiar with. In our view, this puts pressure on application security vendors and has led to further consolidation among both customers and vendors. Snyk, for example, has partnered with Bitbucket to remain a key part of its ecosystem.

Adjacencies and Point Solution Providers
The DevSecOps landscape is still highly fragmented and includes many specialized vendors in areas like container security, IaC scanning, API security, and secrets detection. These vendors often provide best-of-breed depth in their respective domain and are frequently acquisition targets for larger platform providers looking to fill in gaps in their broad solutions. For example, Bridgecrew, which was focused on IaC security to codify infrastructure protections during software development, was acquired by Palo Alto Networks in 2021 and is now part of the Prisma Cloud suite. These specialized tools offer deeper insights and tailored features for their focus areas, so the trend in the industry has been that many point solutions get acquired or merged into larger platforms once they have a proven approach. In today's market, however, we do not believe point solutions will succeed as organizations move away from them given the complexity and difficulties of managing many disparate tools.

Adjacent markets to DevSecOps include container and Kubernetes security, IaC security, ASPM, software supply chain security, API security, and runtime application security. Container and Kubernetes security addresses risks unique to containerized applications through vendors like Aqua Security and Sysdig. IaC security provides early detection and remediation of vulnerabilities within infrastructure templates. ASPM orchestrates and centralizes application security activities for visibility and management across multiple application security tools and processes, led by vendors like ArmorCode and Enso Security. Software supply chain security vendors like Chainguard and Sonatype manage risks associated with open-source dependencies and third-party software. API security has become top of mind as it protects increasingly prevalent API endpoints from misuse and exploitation, which is critical given the proliferation of APIs in modern applications. Lastly, runtime application protection, like with Contrast Security, offers real-time detection and defense capabilities within actively running applications, complementing build-time security measures. These adjacent markets extend beyond core application security and create a more comprehensive approach to mitigating software and infrastructure risks across the entire software lifecycle.

The vulnerability management players (Qualys, Tenable, and Rapid7) have also expanded into DevSecOps by integrating their scanning capabilities into development workflows. These three vendors provide application vulnerability scanning (dynamic web application testing/DAST) to detect flaws in code, along with container and cloud infrastructure scanning capabilities to help secure container images and cloud configurations before deployment. They also offer CI/CD pipeline integrations, so security scans can be automatically run during application builds and releases. These vulnerability management players complement core DevSecOps platforms through deep vulnerability assessment and risk visibility into the software delivery process.

There are also open-source backed vendors with products built on or originating from open-source projects. Companies like Sonatype, Sonar, JFrog, and Anchore leverage community-driven innovation and typically offer a commercial platform or support on top of an open-source core. These business models often involve a free community edition with a paid enterprise edition or providing cloud services for an open tool. This approach helps features evolve faster and results in broad developer mindshare. We believe the open-source backed players align well with DevOps teams that already use open-source tools, as they emphasize transparency and interoperability.

Anchore built its solution around open-source container scanners and has open-source tools Grype (for vulnerability scanning) and Syft (for SBOM generation) that are widely used for container images. The company's enterprise solution is an SBOM-powered platform for software supply chain security that adds policy enforcement, CI/CD integration, and reporting capabilities. Anchore is differentiated by its focus on container and artifact scanning via open source, and its tools can be plugged into development pipelines to detect vulnerabilities in container images and cloud configurations. Its community-driven approach helps the company keep pace with emerging container threats and highlights how open standards are embraced to integrate security throughout the software development lifecycle.

Integration and Overlap Trends in the DevSecOps Market

A notable trend in DevSecOps is the increasing overlap of tool capabilities and the integration of security into broader platforms. DevSecOps tools are largely no longer isolated and are becoming features of larger DevOps or cloud platforms. For example, developer platforms like GitHub and GitLab have been incorporating security natively to provide a more seamless experience. GitHub's Advanced Security solution offers code scanning, secrets scanning, and dependency scanning built into its repository hosting service. As a result, a developer that pushes code to GitHub automatically triggers security analyses with results showing up directly in the pull request. Similarly, GitLab has bundled security tools in its all-in-one solution and the company's survey reports show that more and more organizations are using built-in scans every year as part of their development pipeline. DevSecOps tools are also being integrated with broader security companies, as seen with CNAPPs. For example, Palo Alto Networks' Prisma Cloud now covers everything from IaC template scans to container image scanning and live cloud workload protection, which in the past would likely require three or four separate tools. CrowdStrike acquired Bionic for its ASPM capabilities to fill out its cloud security suite, and Check Point's CloudGuard solution integrates SAST and DAST with runtime cloud security. The idea is to give security and DevOps teams a single platform to manage cybersecurity risk across the entire application lifecycle. We believe enterprises seek holistic solutions that seamlessly integrate with CI/CD pipelines to have all necessary security functions in one place, which will likely contribute to further consolidation. In our view, the distinction between

DevSecOps and cloud security tools will fade over time as they become part of one toolchain that delivers continuous security from code to cloud, which is what we are now seeing with Wiz's platform.

Another overlap trend is in the area of software supply chain security, where DevSecOps tools are expanding into what was traditionally configuration or release management. For example, generating and verifying SBOMs is now a DevSecOps concern that involves tooling during the build and deployment stages. Companies like Sonatype (with its Nexus repository firewall) and JFrog (with artifact signing and scanning) work closely with pipeline tools to ensure code integrity coming from third-party sources. Toolchain integrations are also becoming more out-of-the box as many DevSecOps vendors partner with popular DevOps tools. For example, Snyk and Anchore have official plugins for Jenkins, Azure DevOps, and GitHub Actions, which allow developers to mix and match which security tools they use within their pipeline orchestrator. Users benefit from this trend by getting better features without needing to procure a new product for every niche area, and oftentimes can use a platform solution or a tightly integrated suite that covers many bases.

Why Modern DevSecOps Vendors Are Gaining Market Share

Legacy application security vendors have robust engines and enterprise features, but also major limitations like lacking integration in DevOps pipelines, poor delivery pipeline performance, and lagged coverage for emerging threat vectors that contributes to modern vendors taking market share. Traditional application security tools such as SAST/DAST often functioned as standalone products used solely by security teams, which forced developers to switch between interfaces and wait for security reports and led to an inefficient back-and-forth workflow. This slowed software development and caused security issues to be identified late in the process. Legacy tools are also ill-suited for CI/CD pipelines that run on every code commit because they are resource-intensive and slow, which is not compatible with the speed of modern development cycles. Legacy DAST tools also struggle with APIs and single-page applications as they were built for older architectures. Also, newer threat vectors, such as container images and infrastructure-as-code, are not part of traditional application security suites. Legacy tools also often create additional burdens because they require expert tuning to cut down their number of false positive alerts. Modern tools have become much better at cutting down the noise; for example, Contrast Security's instrumentation approach verifies exploits at runtime to all but eliminate false positives, and Snyk's DeepCode SAST technology uses AI to prioritize real vulnerabilities. Overall, modern tools have introduced innovations for greater integrations, improved performance, new technology ecosystem coverage, and improved usability for speed, breadth, and intelligence that was not present before. They allow security to keep up with agile and DevOps development and deployment and help security become a natural part of delivering high-quality software instead of being a blocker.

Developer adoption is also a major factor for modern vendors gaining market share because modern solutions are designed to be used by developers during development rather than solely for security teams after an application has been built, as is the case with legacy tools. For example, Snyk and GitLab integrate security checks directly into source code management, CI/CD pipelines, and developer environments to provide near-instant feedback. This helps address the speed issue to not slow down development as legacy scanning tools often took hours or days and happened late in the software development lifecycle. Modern tools provide results in seconds or minutes and highlight potential vulnerabilities as they arise to help developers fix security issues before they reach production. Developers will not use the tool without a friendly design with clear remediation guidance and integration with developer workflows, so developer friendliness is an incredibly important aspect that gives modern vendors an advantage with adoption.

Another major driver is modern solutions' ability to cover new technology stacks. Modern applications are cloud-native and composed of microservices, containers, open-source libraries, and infrastructure as code. Legacy vendors have been slow to support these new technologies, allowing modern vendors to gain traction by securing Kubernetes and cloud configurations from the ground up. Modern vendors are also typically SaaS-based, which appeals to companies that prefer not to maintain on-premises security infrastructure.

Future Outlook on the Market

We believe the DevSecOps market will head toward more unification, intelligence, and alignment with business needs through a consolidated set of platforms (some native to cloud security platforms and others independent) that cover the spectrum of software security all the way from code to runtime. We believe these platforms will leverage AI and automation for speed and accuracy, emphasize supply chain integrity, and be embedded into

developer workflows to minimize as much friction as possible. We also expect organizations to not treat DevSecOps as a siloed category but as an important part of their DevOps toolchain and risk management strategy.

We expect vendor consolidation through acquisitions to accelerate, as 2024 saw record-high M&A activity in software development and deployment, which we believe will continue as larger players continue to seek to offer end-to-end security platforms. Boundaries between DevSecOps submarkets are blurring as vendors expand their offerings, and we expect additional cross-category moves, like SAST vendors moving to IaC scanning, or CNAPP vendors integrating DevSecOps capabilities. We also expect vendors to expand into emerging and faster-growth adjacent areas, such as secrets scanning, API security, cloud configuration monitoring, and more through either acquisitions or product development in pursuit of end-to-end code to cloud security portfolios. We also believe some DevSecOps vendors, such as Snyk, Contrast Security, and Sonatype, have the potential to go public when market conditions improve.

As the market matures, we expect different types of companies (like cloud platforms, developer platforms, and CNAPPs) to have different positioning and to play distinct roles. We believe the hyperscalers are embedding more DevSecOps features natively into their cloud platforms and CI/CD services, as evidenced by Google's recent acquisition of Wiz. We believe these companies will aim to make basic application security "free" and seamless within their ecosystems to put pressure on smaller vendors to deliver deeper capabilities. For developer platforms like GitHub and GitLab, we expect security to be integrated into development workflows by default, and they already bundle code scanning, secrets detection, and dependency auditing into their platforms. We expect developer friendliness to continue improving to drive further adoption and for developer platforms to partner with security specialists for advanced features. For specialized DevSecOps vendors, we expect additional innovations in both depth and breadth to stay ahead of competition, but also many integrations to ensure their tools interoperate well with platforms and to fit into toolchains. Many DevSecOps vendors have already expanded cross-functionality into code, open-source, container, and IaC scanning in one suite, but we expect more of this and an emphasis on orchestration and risk prioritization. We believe most DevSecOps vendors will be acquired by larger players while a few will pursue IPOs. For the CNAPP vendors like Wiz, Lacework (acquired by Fortinet), Palo Alto Networks, CrowdStrike, and more, we expect them to continue bridging the gap between developer and runtime security to catch cloud misconfigurations and vulnerabilities early in the software development lifecycle. The value proposition of CNAPP vendors is end-to-end visibility in the cloud and we expect them to increasingly highlight integrations with CI/CD pipelines and code repositories.

In terms of the technology and product direction of the DevSecOps market, we expect solutions to integrate AI to achieve automation capabilities. We believe automation will be at the center of next-generation DevSecOps tools to help organizations perform security tests smarter, detect vulnerabilities faster, and automatically remediate code issues. We are already seeing signs of this, with companies experimenting with generative AI to produce fixes or provide security recommendations in code. Longer term, we see potential for AI agents to be embedded in software development pipelines that autonomously find and patch common vulnerabilities (like an AI that can detect a SQL injection and provide a code fix). We expect virtually all leading DevSecOps vendors to utilize AI features for intelligent code scanning, predictive risk scoring, AI-assisted threat modeling, and more over time. We also expect DevSecOps to continue shifting focus to the software supply chain for greater emphasis on managing open-source components, application build integrity, and SBOM generation as software supply chain exploits remain on the rise. Governments are pushing for this as well, so we believe future DevSecOps pipelines will embed capabilities to produce and validate SBOMs for each software release to track components and detect tampering. API security is another major concern, and we believe API security testing will be further integrated into developer pipelines, as 70% of web traffic is now made up of APIs, representing a huge attack vector.

DevSecOps Taxonomy

In exhibit 11 on the following page, we highlight companies in the cybersecurity space that offer solutions that are represented in DevSecOps efforts.

Exhibit 3
On the Ground and in the Cloud; A Developer Technology Quarterly
DevSecOps Cybersecurity Taxonomy Landscape

SAST	DAST	IAST	API Security	SCA	RASP	ASPM	Secrets Management	CNAPP	SBOM	CI/CD Security	Container and Kubernetes Security	IaC Security
Appknox	Appknox	Checkmarx	42Crunch	Anchore	Contrast Security	Apiiro	Akeyless	Trend Micro	Anchore	Anchore	Anchore	Apiiro
Checkmarx	Checkmarx	Contrast Security	Akamai	Apiiro	Datadog	ArmorCode	Apiiro	Aqua Security	Apiiro	Aqua Security	Aqua Security	Checkmarx
CodeScan	Detectify	Invicti	Apiiro	Canvass Labs	Digital.ai	Bionic/ CrowdStrike	Aqua Security	Check Point	Appknox	ArmorCode	Chainguard	Check Point
CodeSecure	Beyond Security/Fortra	New Relic	APISec	Checkmarx	Dynatrace	Checkmarx	Amazon Web Services	CrowdStrike	Bionic/ CrowdStrike	Checkmarx	Check Point	Cycode
Contrast Security	GitLab	NowSecure	Appknox	CodeSecure	Signal Sciences/ Fastly	Cycode	CyberArk	Lacework/Fortinet	Checkmarx	Check Point	Checkmarx	Harness
Cycode	Invicti	Synopsys	Bionic/ CrowdStrike	Contrast Security	Imperva/Thales	Legit Security	Delinea	Microsoft	CAST Software	Contrast Security	F5 Networks	JFrog
Beyond Security/Fortra	Micro Focus/ OpenText	Veracode	Cequence	Cycode		Snyk	GitLab	Orca Security	Fossa	Cycode	Alert Logic/Fortra	Lacework/Fortinet
GitHub/Microsoft	NowSecure		Check Point	Datadog		Synopsys	Google	Palo Alto Networks	GitLab	Datadog	GitLab	Legit Security
GitLab	PortSwigger		Checkmarx	Endor Labs		Tromzo	HashiCorp/IBM	SentinelOne	Legit Security	Endor Labs	Lacework/Fortinet	Orca Security
JFrog	Qualys		Cisco	Fossa		Veracode	JFrog	Sysdig	Mend	Harness	Mirantis	Palo Alto Networks
Kiuwan	Rapid7		Corsha	GitHub/Microsoft			Microsoft	Wiz/Google	OX Security	Invicti	NeuVector/SUSE	SentinelOne
Mend	StackHawk		Curity	GitLab			Qwiet AI		Qwiet AI	Legit Security	Orca Security	Snyk
Micro Focus/ OpenText	Synopsys		Data Theorem	Invicti			BeyondTrust		Revenera	OX Security	Palo Alto Networks	Sysdig
NetSPI	Tenable		Datadog	JFrog			IBM		ReversingLabs	Palo Alto Networks	Qualys	Wiz/Google
NowSecure	Veracode		F5 Networks	Kiuwan			GitHub		Sonatype	PortSwigger	Qwiet AI	
Qwiet AI			GitLab	Mend					Wiz/Google	Qwiet AI	Rapid7	
Snyk			Google	Micro Focus/ OpenText						ReversingLabs	SentinelOne	
Sonar			Imperva/Thales	Orca Security						Sophos	Snyk	
Synopsys			Invicti	Palo Alto Networks						StackHawk	Sysdig	
Veracode			Orca Security	Qwiet AI						Synopsys	Tenable	
HCL Technologies			Palo Alto Networks	Revenera						Veracode	Trend Micro	
Perforce			Salt Security	Snyk						Wiz/Google	Veracode	
IBM			StackHawk	Sonatype							Wiz/Google	
			Traceable/ Harness	Synopsys								
			VMWare/ Broadcom	Veracode								
				Tenable								
				Wiz/Google								

Source: William Blair Equity Research

AI's Impact on DevSecOps

Generative AI

We believe questions over how to safely use AI are some of the most important questions in cybersecurity today and that AI in the context of DevSecOps continues to be a double-edge sword, as it offers significant advantages in terms of developer productivity and cybersecurity efficacy, but also new challenges and security risks. Overall, we believe the DevSecOps market is set to benefit from AI as a result of the advantages of AI-enhanced cybersecurity, developers using it to write more code, DevSecOps tools becoming more efficient and user-friendly, and the need to secure AI itself, which we expect to drive higher demand and adoption rates.

AI is already helping developers write code more efficiently, with GitHub estimating that 46% of code on the platform was written by Copilot (its AI coding assistant) and that developers complete engineering tasks 55% faster, figures we believe will only increase over the medium term. Meta conducted a study on AI code generation and found that the better an LLM is at writing code, the worse it is at avoiding vulnerable coding practices. We expect this to improve over time as LLMs become smarter and more specialized, though it presents more risk in the near term, as we believe AI will drive more software and more developers, not less, because it creates more productive developers and lower barriers to entry for coding, both of which lead to additional code that needs to be secured. We believe this also increases the distance between developers and security teams, as AI coding assistants lead to more code with more issues. Snyk also conducted a study showing that roughly one in three AI-generated code segments contain vulnerabilities, and that it produces code faster than developers or security teams can properly review and secure it.

Another issue with AI code generation is that it raises intellectual property concerns given that some generative AI models are trained on someone else's proprietary or licensed code and can inadvertently reproduce it. This poses a legal risk as developers use AI suggestions for coding and they could unknowingly violate license or copyright agreements. Also, integrating company-specific data into AI models (either through training or fine-tuning) can backfire if that data contain vulnerabilities or sensitive information. AI models trained on insecure code will inevitably learn and propagate those insecure patterns, which can compromise the AI system itself as the model may later regurgitate the vulnerable code or confidential details. Poisoning or tampering with training data to include exploitable backdoors or vulnerabilities can undermine a model's integrity and cause these weaknesses to surface in the AI's output. Beyond code generation, AI also automates routine and time-consuming tasks for developers, such as text analysis, technical document summarization, and more. Going forward, we believe AI code generation will improve significantly so it can be used for a lot more creative problem solving and bigger development projects.

In our view, AI over the last couple of years has been performing single-step inference but is starting to move toward multi-step inferences with more ambiguous commands. We believe this will lead to AI doing bigger tasks that could take developers weeks or months, such as upgrading an application to a newer Java version. Also, we believe there will eventually be autonomous coding agents that can handle the vast majority of routine coding tasks and detect and fix bugs. There are, however, limitations with current AI models, like hallucinations, restricted context length, overreliance, and, of course, introducing additional security vulnerabilities.

We believe AI introduces advanced capabilities that enhance both the efficiency and effectiveness of security operations within software development processes. Security teams currently have many constraints, including development speed, attention/human limitations, cybersecurity skills gap, and more, which are challenges that we believe AI helps resolve. Also, we believe AI is driving more investment in DevSecOps tooling, as it makes established areas gain renewed attention because it has better analysis capabilities. For example, AI improves code security analysis, so SAST solutions are better at reviewing code and finding vulnerabilities as a result. Overall, we believe AI provides more scale and scope than a traditional security team and can help organizations write code, fix security vulnerabilities, accelerate code review and testing, and improve collaboration between teams. These benefits can lead to advanced threat detection capabilities, automated remediation, predictive security analytics, natural language understanding, and more. Some more specific ways AI is impacting DevSecOps from a security perspective include:

- Session summarization: AI can read and summarize session timelines to uncover potential signals that would otherwise go unnoticed, thus helping with threat detection.

- Event triage: AI aids with the analysis, prioritization, and response to security events and helps teams collaborate more effectively by getting a message to the right place.

- Draft incident reports: AI can write the first draft of an incident report to save time for security teams.
- Automation of certain processes to allow employees to work fast while having the appropriate oversight.
- Bug bounty: AI can automate and streamline the identification, classification, and prioritization of vulnerabilities reported by researchers.

Additionally, we believe AI is creating a new market of products related to AI security that involves securing the data used for training LLMs, enhancing privacy, managing the lifecycle of AI models, ensuring compliance, AI development security, robustness testing, and more. The emergence of these products is a response to the challenges posed by AI technologies, and we expect the demand for specialized AI security products will grow as AI continues to evolve and be used by more companies in various sectors. Going forward, we believe AI security should be another component that is integrated into the SDLC. Companies in the AI security space include Protect AI (acquired by Palo Alto Networks), HiddenLayer, Securiti, and Adversa.

AI Developments in the Market

In the DevSecOps market, Snyk has its DeepCode AI technology that uses multiple security-specific and self-hosted LLMs to deliver AI code analysis and fixes directly in developers' workflows. One of Snyk's major focus points is on the vulnerability fix rate, and the company is leveraging this AI technology to accelerate vulnerability remediation capabilities, as the amount of code being written is exploding with AI. Checkmarx's platform offers AI tools to suggest remediation steps for identified vulnerabilities, build natural language queries for SAST and IaC scanners, and integrate with ChatGPT and GitHub Copilot to help secure AI generated code. JFrog is integrating MLOps into its platform to offer a solution to build, deploy, manage, and monitor all of an organization's AI workflows. GitHub utilizes AI-powered application security testing tools, and GitLab offers AI-assisted generation of merge requests and vulnerability explanations. Recently, GitLab announced its Duo Agent Platform, which extends AI capabilities across the software development lifecycle by allowing users to employ AI agents across all the different facets of the SDLC. CrowdStrike has its Charlotte AI SOC analyst/assistant that cuts across its entire platform and saves analysts an average of two hours of work per day. We view AI as an important component of DevSecOps vendors' product portfolios, as it is a major part of implementing security without slowing down development by helping bring security information to developers at the time they need it and to help developers navigate an application's codebase. We believe DevSecOps companies will continue working to integrate AI security capabilities in the software development lifecycle and it will be something that needs to be offered in order to stay competitive.

Recently, Snyk unveiled its new AI Trust Platform, which is an industry first AI-native security platform built to secure and govern software development in the generative AI era. This is a comprehensive solution that enables organizations to embrace AI-driven innovation at a high velocity without compromising security. We believe Snyk is addressing the reality that the vast majority of software code may soon be AI-generated (Microsoft projects about 95% of code to be written by AI by 2030), which tends to be more insecure and would certainly introduce many more code vulnerabilities. With AI integrated throughout the software development lifecycle, this platform provides real-time visibility into AI usage, intelligent risk prioritization, and automated policy enforcement for AI workflows. Snyk's new platform also introduces capabilities like an AI-powered developer assistant for instant secure coding guidance, autonomous security agents that can generate and validate fixes on the fly, and AI-driven guardrails to continuously enforce security policies as applications evolve. In our view, this platform launch places Snyk as a leader in the AI-era of DevSecOps and extends the company's developer-first approach into an AI world. We believe this AI Trust Platform not only strengthens Snyk's product portfolio, but also sets a benchmark for the industry as it challenges the DevSecOps market to address emerging AI-driven threats (from insecure code to attacks like prompt injections) and embed security automation and governance into the fast-expanding world of AI-assisted development. We view this as a strategic move by Snyk that should accelerate how development and security teams adapt to the coming AI-powered wave of software innovation.

Agentic AI

Longer term, we believe AI agents will further drive the need for DevSecOps tooling as the software developer role shifts toward the development of AI agents that will need to be secure by design. AI agents are autonomous systems that make decisions and take actions to achieve specific goals. Looking ahead, AI agents are expected to act autonomously in partnership with humans and other AI in carrying out more complex tasks across multiple areas of a business (HR, sales, IT, marketing, finance, R&D, etc.). Agentic AI adoption is driven by organizations' desire to change

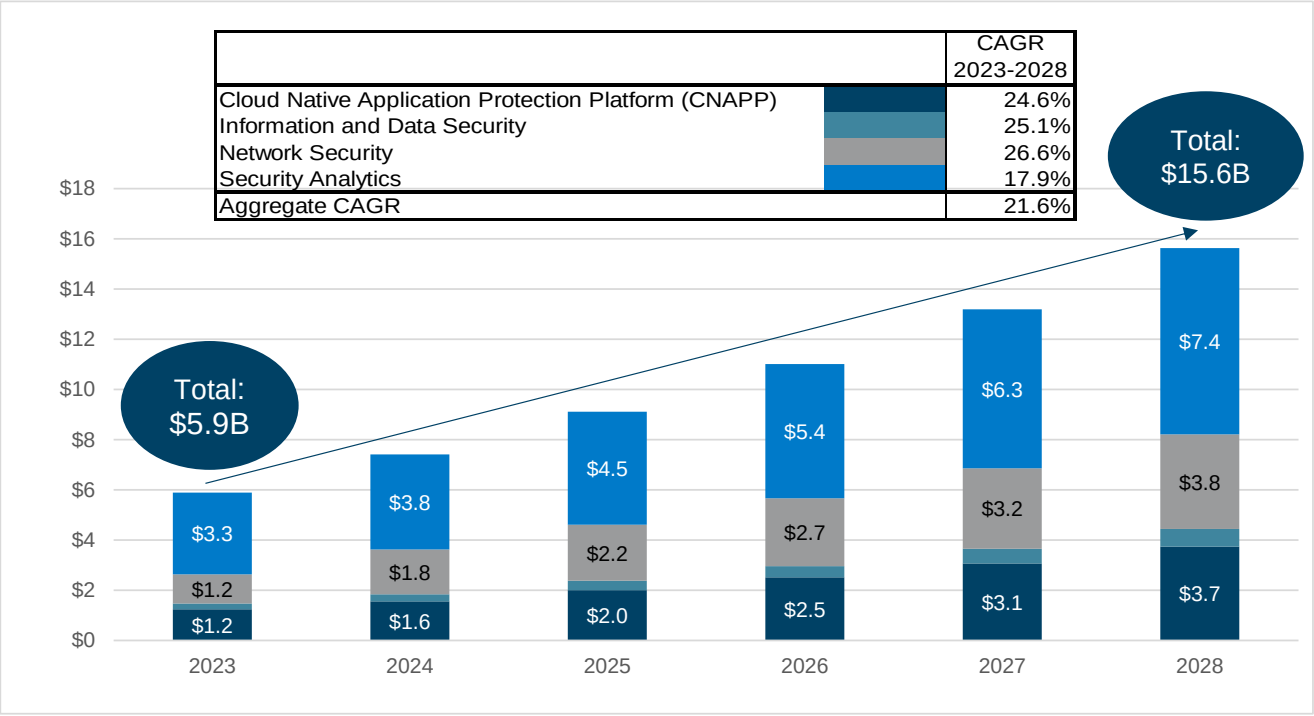
the business status quo, reinvent workflows, solve labor shortage challenges, unlock machine scale beyond productivity gains, reduce technical debt, and more. Potential inhibitors to adoption include job displacement fears, geopolitics, trustworthiness of AI models, high costs, and more. Immature multi-agent systems also represent a barrier; however, we expect these to improve over the next one to two years and adoption to accelerate.

We believe enterprises will develop agentic AI use-cases in-house and that many software developers' roles will evolve to focus on developing AI agents to be used within the organization. We expect companies to increase their investments in personalized/custom software because AI agents can be tailored to automate specific tasks, enhance productivity, and provide competitive advantages. Custom AI solutions allow businesses to align their technology with their unique workflows, data, and strategic goals, but they also represent an expanding attack surface requiring security. We believe software development in the agentic AI era is likely to include natural language coding, AI agent builder platforms, and agents creating software themselves.

DevSecOps Market Size and Growth Outlook

IDC projects the worldwide DevSecOps software tools market to grow at a compound annual rate of 21.6% over the forecast period of 2023 to 2028, which is about 200 basis points lower than the previous five-year forecast of 23.8%. In 2023, overall market revenue was pegged at $5.9 billion (about 23% growth year-over-year) and is projected to reach $15.6 billion by 2028. IDC updated the four segments that make up the overall DevSecOps market to now include security analytics, network security, information and data security (added information security), and CNAPP (changed from endpoint security).

Exhibit 4
On the Ground and In the Cloud; A Developer Technology Quarterly
IDC: DevSecOps Market Forecast, 2023-2028
($, in billions)



Source: William Blair Equity Research based on IDC estimates; IDC DevSecOps Software Tools Forecast, August 2024

1. ***Security analytics***—this market is made up of certain security and compliance scanning, remediation, and automation tools that are integrated into CI/CD pipelines and/or agile production use-cases. This submarket is expected to grow at a five-year compound annual rate of 17.9%, which is the lowest growth rate among the four

segments, but it is also the largest segment, with a 55.3% share in 2023. Sample vendors provided in this space remain Synopsys, Checkmarx, Veracode, and Contrast Security.

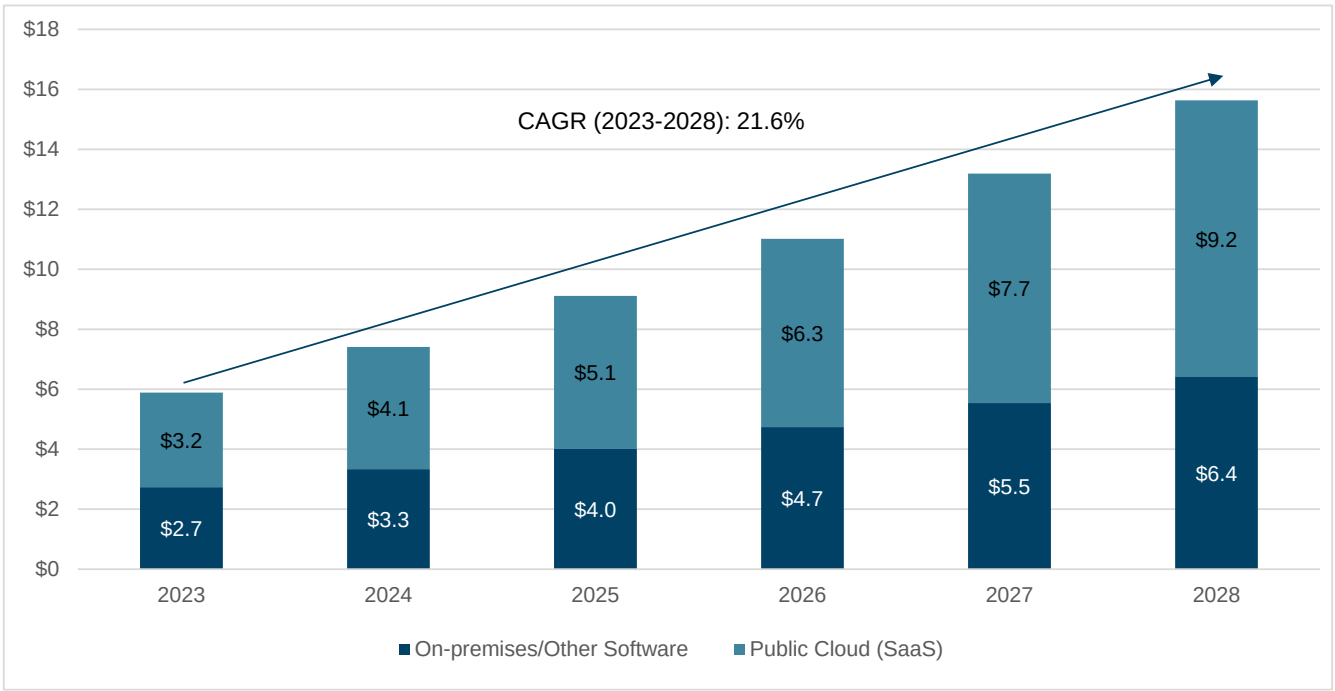
2. ***Network security***—defined as active application security tools, such as WAF and API security with sample vendors of F5 Advanced Web Application Firewall, Salt Security API Protection Platform, Google Apigee, and Imperva Web Application Firewall. Network security is expected to grow at a five-year compound annual rate of 26.6%, which is the highest projected growth rate among the segments, driven by strong demand for API security solutions.

3. ***Cloud-native application protection platform (CNAPP)***—this market includes tools used for cloud workload security (including container security and runtime protection) and cloud security posture management (including IaC security). Sample vendors in this market include Aqua Security, Sysdig, Palo Alto Networks, and Trend Micro. The CNAPP market is expected to grow at a five-year compound annual rate of 24.6% driven by the increasing number of cloud-native applications and the growing adoption of multi-cloud strategies.

4. ***Information and data security***—this market includes vendors for secrets management tools to manage digital authentication credentials, keys, and APIs, and sample vendors provided include CyberArk Conjur, Akeyless, and HashiCorp Vault. Information and data security is expected to grow at a five-year compound annual rate of 25.1%, representing the smallest portion of the aggregate market with 3.9% share in 2023, driven by the need for organizations to properly store, provision, and manage secrets to avoid data leaks.

In addition, IDC estimates that 54% of DevSecOps software tools were delivered as SaaS in 2023 and is projecting this to increase to 59% by 2028.

Exhibit 5
On the Ground and In the Cloud; A Developer Technology Quarterly
DevSecOps Market Forecast by Deployment Type, 2023-2028
($, in billions)



Source: William Blair Equity Research based on IDC estimates; IDC DevSecOps Software Tools Forecast, August 2024

In our view, the IDC market forecast for worldwide DevSecOps software tools provides a comprehensive view of the size and expected growth rate of the overall market. We believe the market's robust growth will be driven by organizations realizing that applications need to be secure by design, the need to manage the complexity of modern software supply chains, and to maintain compliance amid increasing regulatory requirements. Thus, we believe

having automated and integrated security tools throughout the software development lifecycle that are robust and provide visibility is a necessity for organizations to securely build and use software applications.

Macro Tailwinds Driving Adoption

We believe that every DevOps program today should be a DevSecOps program, and that organizations should embrace DevSecOps for three primary reasons: 1) the fast pace of application development today makes securing each phase of the SDLC much more important; 2) the fact that cyber risk is now an overall business risk, and new regulatory standards and requirements heighten this; and 3) the proliferation of cyberattacks only continues to increase, including software supply chain and API-based attacks. Modern, cloud-native applications today are more complex and have faster-paced lifecycles than in the past. This phenomenon leads to multiple deployments of production code per day and the need to automate solutions to make it possible. We believe DevSecOps revolves around automation, as it helps remove the friction between DevOps and security teams to enable faster and safer development cycles. The importance of DevSecOps and automation becomes exacerbated with the introduction of AI, as developers' productivity increases with the ability to write more code, which inevitably also creates more vulnerabilities. Therefore, we believe DevSecOps will become a higher priority for organizations as developers adopt AI tools to be used in software development. Virtually every company today uses software in some capacity, whether it is to be more competitive in the marketplace to draw more customers, interact with employees and customers, and/or to optimize internal back-end processes, and more secure applications are needed because digital experiences have the power to make or break organizations. Disruptions to software/applications can cause organizations to lose revenue, become less productive, incur higher cybersecurity insurance premiums, pay compliance breach fines, and experience data theft and reputational harm. On top of increased cyberthreats, new standards and regulations (e.g., the White House executive order, SEC rules requiring cyberbreach disclosure, NIST standards, or OWASP frameworks) add to the pressure of organizations needing to adopt security tools. For these reasons, we believe it is critical for organizations that develop software to bake in security from the start and they should drive further adoption of DevSecOps tools and processes. API-based attacks are an emerging attack vector as microservices architectures and CI/CD practices have driven faster development with more applications and more frequent deployments. Modern applications use APIs to efficiently communicate with other applications, so they represent a type of backdoor into applications that have been traditionally left unprotected. Many organizations have focused on securing the front end of their applications, where users interact with the application, but have neglected API security. In addition, organizations are still dealing with the lack of cybersecurity professionals, with the latest statistics estimating the current global cybersecurity workforce shortage to be nearing 4 million people, again emphasizing the need for automated security tools and DevSecOps adoption.

DevSecOps Trends

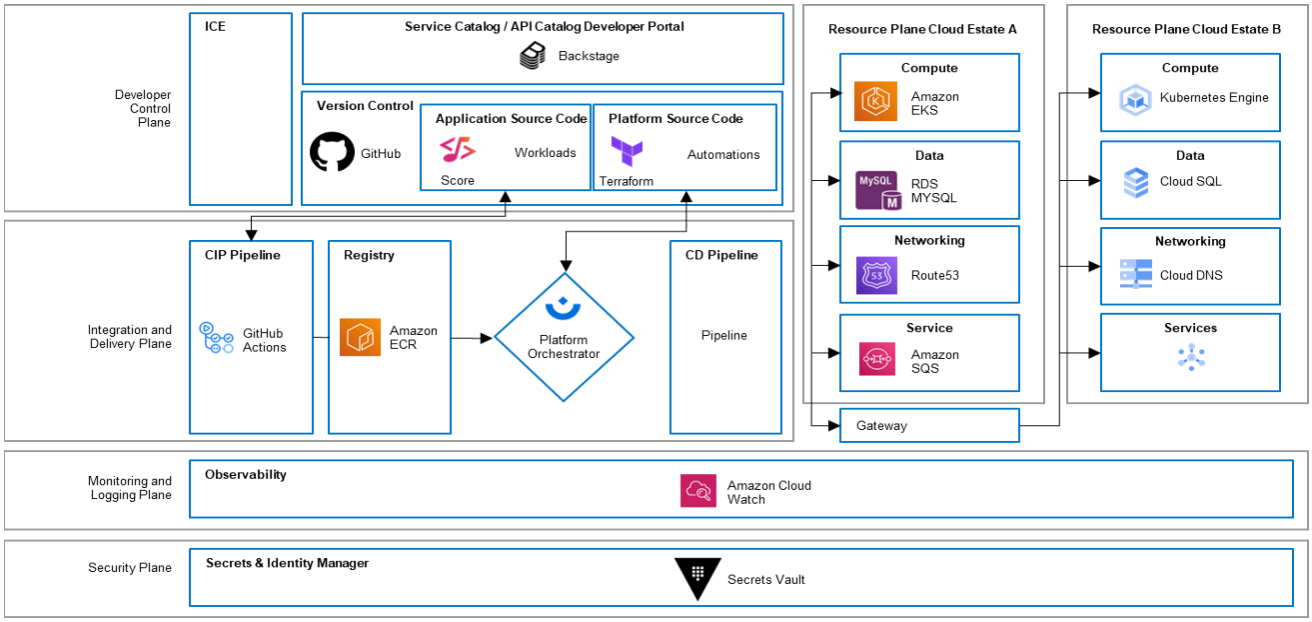
Platform Engineering

Over the past year, we have seen the trend of platform engineering mature from being a popular buzzword to being a real practice. According to an IDC survey, there was a significant increase in the number of organizations either piloting, using, or expanding their use of an internal developer platform (IDP), with 80% indicating they were doing so this year compared to just 40% of organizations in last year's survey. We believe platform engineering is sticking around because of the benefits it provides to IT operations teams. Platform engineering focuses on building and maintaining IDPs that streamline and automate the backend processes for software development teams. IDPs are customized environments and toolsets built to enhance software development and to provide developers with pre-configured resources, automation, and collaboration tools specific to their needs (see exhibit 6). This approach enhances developer productivity by offering robust, scalable, and secure environments that simplify deployment, monitoring, and resource management through self-service capabilities. The ultimate goal of platform engineering is the same as DevSecOps, which is to develop and deliver high-quality applications quickly and securely. We believe platform engineering's rise in popularity will lead to further DevSecOps tool adoption as IDPs integrate security into the overall platform, because, in our view, the foundation of a good platform engineering program is operational and application security.

The emergence of platform engineering is a result of software developers' jobs shifting toward managing and running code instead of just writing it, which many do not want to do. We believe organizations are adopting platform engineering in an effort to improve developer productivity, increase standardization, scale software development more easily, enhance their application security posture, and to remain compliant across the organization. In addition,

for modern applications built on Kubernetes and microservices, platform engineering is not just about building functional systems but also about embedding security directly into those systems. We believe platform engineering can help any company that develops software, with examples like IDPs for financial services firms, self-service portals in e-commerce, automated compliance for healthcare companies, scalable infrastructure for media streaming services, microservices orchestration in logistics, and development standardization in software companies.

Exhibit 6
On the Ground and in the Cloud; A Developer Technology Quarterly
Internal Developer Platform



Source: William Blair Equity Research

Automation

We view automation as a focal point of a strong DevSecOps foundation because we believe the key to building secure applications is to fix security issues as they arise (whether the code is coming from humans or AI). Automation in DevSecOps refers to the integration of automated security measures directly into the DevOps pipeline. We believe automation is crucial because it enables organizations to maintain the rapid pace of modern software development while ensuring security is not left as an afterthought. The primary benefits of automation include being able to perform security checks, like vulnerability scans, compliance audits, and threat detections, at the speed of DevOps processes without manual intervention, which also eliminates human errors and reduces the risk of security oversights. Also, automation helps reduce the cognitive load for developers because it integrates security directly into their workflows and makes it easier for developers to resolve issues, especially considering that many software developers are not well-versed in cybersecurity. We believe every DevSecOps program needs to automate various tasks and processes in order for organizations to stay competitive while delivering secure software.

Implementing automation in DevSecOps processes typically begins with integrating security tools directly into version control systems (such as GitHub and GitLab) where developers initiate changes to code. For instance, pre-commit hooks can automatically trigger SAST and DAST scans before code is even merged into the main branch. Once the new code is integrated, it can be automatically analyzed for potential vulnerabilities and feed results back to developers through the CI/CD pipeline, providing an almost immediate feedback loop to developers, which we believe is incredibly important in building secure software. Additionally, automated compliance scanning tools continuously check configurations against regulatory standards and organizational policies, providing alerts and recommendations when deviations are detected. Runtime protection mechanisms can be automated through tools like web application firewall (WAF) and RASP technologies, which actively monitor and block threats in real time.

We view automated remediation, where DevSecOps tools provide actual vulnerability remediations that can be accepted and automatically implemented in the code base, as a future trend in the DevSecOps space that is starting to gain early traction. This goes beyond remediation recommendations that offer potential sample code, a vulnerability

explanation, or advice that then requires additional work to resolve. Automated remediation tools also help with not interrupting the developer's workflow, as users of certain solutions can accept fixes with one click in their IDP. There is some variation among automated remediation tools in the market today, as some perform scanning to identify vulnerabilities as well, while others integrate with existing application security testing tools. Generative AI is driving some of these automated remediation capabilities, so we will likely see more DevSecOps vendors begin offering this in the near term. Companies like Checkmarx, Veracode, and GitLab have automated remediation capabilities, as have some smaller startup companies, such as Mobb, Corgea, Moderne, and Seal Security.

Software Supply Chain Security

We believe the prevalence of software supply chain security has continued to rise over the past year as the number of software supply chain attacks continues to increase, with new research from Cyble suggesting that a software supply chain attack occurs at least once every two days in the United States. Open-source software (OSS) risk is top of mind in software supply chain security as organizations rely heavily on open-source components, which are now estimated to account for up to 90% of modern software applications. Sonatype's latest *State of the Software Supply Chain* report highlights the issue of open-source malware, noting a 156% increase in malicious open-source packages over the past year. Software supply chain security aims to protect all of the elements involved in creating and delivering software products, which encompasses the application's source code, third-party components, development and deployment processes, as well as the underlying infrastructure.

In our view, DevSecOps is becoming synonymous with software supply chain security, because effective software supply chain security involves rigorous management of open-source and third-party elements, secure coding practices, and CI/CD security, all of which overlap with DevSecOps practices. We believe software supply chain security will be a big problem for organizations going forward, as software today is built as if it is in a factory with all of its third-party dependencies and open-source components. Therefore, we believe software supply chain security is an area of need and will drive further adoption of DevSecOps tooling and practices.

In our view, holistic software bills of materials (SBOMs) are needed for better software supply chain security, because every single open-source component (which make up to 90% of application code) needs to be traced, as well as all of the changes to those components. As a reminder, SBOMs are detailed and formal records that list all of the components contained in a piece of software. Over the last 18 months or so, the U.S. federal government has released several requirements for procurement contracts with the federal government, as well as guidelines that can be used by the entire industry. The Secure Software Development Framework (SSDF) and Security Technical Implementation Guidelines (STIGs) are two examples that include SBOM requirements, and we believe that private companies will expect the same due diligence from their partners and vendors as more and more organizations adopt these high security standards. We view Anchore as a leader in the SBOM management space with its SBOM-powered platform solution that generates comprehensive SBOMs, continuously scans them for vulnerabilities, secrets, and malware, and includes automated compliance enforcement. Anchore's platform also enables DevSecOps with the mentioned capabilities and its various integrations with products in different areas, such as CI/CD pipelines, containers and container orchestration tools, collaboration products such as Slack and Jira, and cybersecurity tools.

Application Security Posture Management

Another persisting trend in the DevSecOps space is application security posture management (ASPM), which we believe has gained further traction over the past year. ASPM is designed to systematically manage and improve the security of software applications throughout their development lifecycle and operational use. These solutions help organizations continuously assess, monitor, and mitigate security risks, with the primary goal of maintaining a robust security posture that evolves with new threats and adapts to changes in application environments. The key features of ASPM solutions include continuous vulnerability assessment, automated security testing integration, compliance monitoring and reporting, risk management and prioritization, policy management, and visibility. This solution was born as a result of the challenge of prioritizing vulnerabilities in application code as many end-users have thousands or tens of thousands of vulnerabilities in their backlog with no resources or prioritization to remediate them. ASPM came out of ASOC (application security orchestration and correlation) solutions, which aggregated security alerts and provided some level of normalization, but ASPM goes further with added business context, tagging, and more. More recently, ASPM solutions have evolved further to become platforms that offer scanning tools out of the box as well.

We believe ASPM will be more successful in the mid-market where companies may not have a lot of security or a sporadic approach to security and are trying to consolidate. At the enterprise level, we believe much more integration will be involved and that ASPM will eventually be part of a broader platform, likely with a CNAPP or AST (application

security testing) platform. For example, CrowdStrike acquired Bionic to incorporate ASPM into its CNAPP offering, and Snyk acquired Enso Security for its ASPM capabilities and Helios for its application runtime information capabilities to be included in its ASPM solution. Currently, there is a lot of variation in what ASPM solutions offer from different vendors, but we view Apiiro as the most mature ASPM vendor, with other players in the space including Snyk, Checkmarx, Cycode, Veracode, and CrowdStrike.

Application Detection and Response

We view application detection and response (ADR) as a recent and emerging trend in cybersecurity that represents the latest extension of detection and response technology into the application layer. ADR focuses on the real-time monitoring, detection, and mitigation of threats in software application environments, and it uses advanced analytics, such as machine learning and behavioral analysis, to identify anomalies and potential security incidents that deviate from normal application behavior. This helps organizations detect sophisticated threats like zero-day exploits, SQL injections, and cross-site scripting attacks. When a threat is identified, ADR solutions can automatically initiate responses to mitigate the risk involved, which is similar to how other detection and response solutions improve security such as EDR with endpoints, NDR with networks, CDR with the cloud, and ITDR with identities. We believe these detection and response solutions provide better visibility and control of an organization's endpoints, network, cloud, and identities, and now ADR is bringing that to applications and APIs to close that visibility gap and provide better overall cybersecurity for the organization. Also, ADR solutions can integrate with existing security infrastructure such as SIEMs and incident response platforms (like XDR and CNAPPs), which leads us to believe that ADR will be an important component of an organization's cybersecurity technology stack going forward. It is still very early days, but we believe that in the long term ADR solutions are likely to follow consolidation trends familiar in the cybersecurity industry and become a part of application security platforms (that focus on application security testing and runtime security) or even broader cybersecurity platforms.

At the Black Hat 2024 cybersecurity industry conference, Contrast Security introduced its ADR solution to help security teams identify vulnerabilities, detect threats, and stop attacks that target custom applications and APIs. Based on our conversations at the conference, Contrast evolved RASP (runtime application security protection) into ADR with added observability, and the company simplified its product portfolio to application security testing and ADR under one platform. Its ADR solution is embedded within the application code and enforces behavioral rules to detect bad behavior quickly. Contrast's ADR also includes API security as the company believes application security and API security go hand in hand as F5's 2024 *State of Application Strategy Report* demonstrates that 41% of organizations are managing at least as many APIs as applications. Also, we believe Contrast's ADR is effective at protecting older and existing software applications, which is important as many organizations already use dozens of software applications that may not be cloud native.

DevSecOps Adoption

In a recent survey conducted by Techstrong Research, respondents indicated that less than half (47%) of organizations regularly employ DevSecOps practices, which represents a steady gain from last year but also highlights the room still ahead for further adoption. In our view, organizations have been generally slow to adopt DevSecOps practices for a few main reasons: application security is very difficult and always evolving (like with software supply chain security and AI security); DevSecOps requires a lot of tools and resources that security teams view as potential new attack vectors; collaboration between developers, security, and IT operations teams is complex; and developer experience remains a challenge.

With today's rapid pace of software development, complexity of modern software architectures, and evolving threat landscape, coupled with fulfilling regulatory requirements and not degrading the user experience, we believe application security is inherently challenging and requires a multifaceted approach that integrates robust technology, skilled professionals, and effective processes throughout an application's entire lifecycle. Application security also includes complex elements like software supply chain security where organizations must also secure all the third-party components and dependencies that are integrated into their applications. Also, DevSecOps requires the integration of various security tools such as SAST, DAST, IAST, RASP, SCA, container security, IaC security, automation processes, and more into CI/CD pipelines to work harmoniously without disrupting developer workflows, which can be technically challenging especially for smaller organizations. In general, developers want to focus on writing code, and they do not like to be forced to do something different, like cybersecurity. Therefore, DevSecOps tools need to seamlessly integrate into the developer's workflow so as to not interrupt the developer and to deal with security issues quickly as they arise. We also believe that collaboration at the management level needs to be viewed as a shared goal so traditional siloes between security, development, and operations teams work together toward the goal

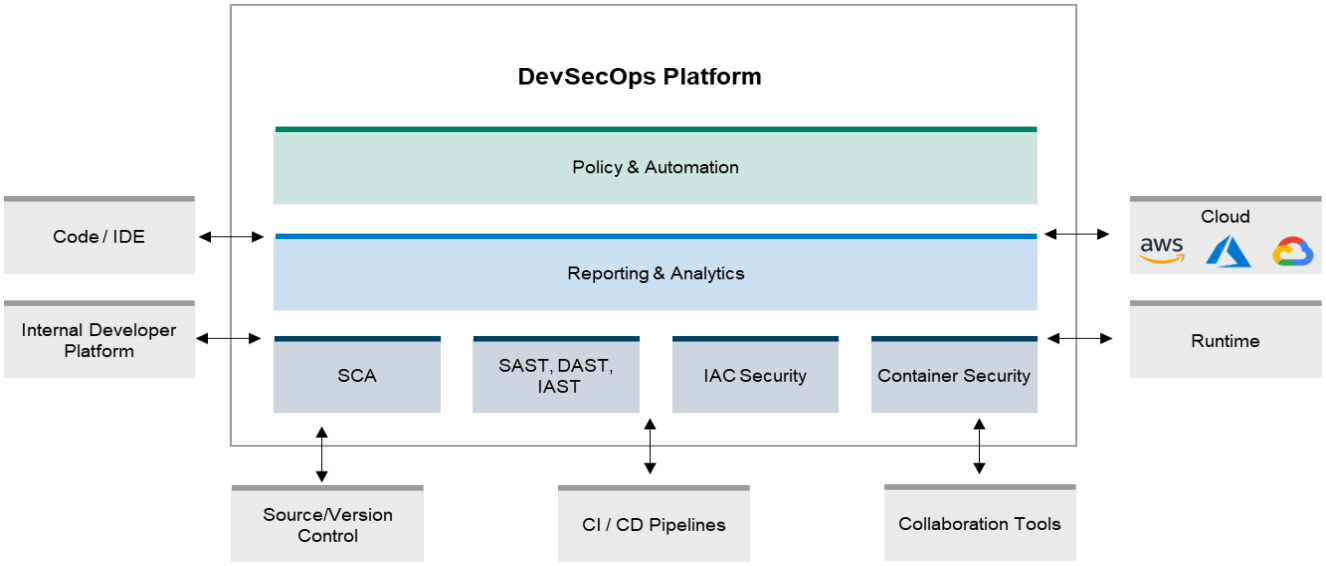
of efficiently shipping high-quality and secure applications. The resistance to change is a big inhibitor to DevSecOps adoption (selected by 41% of respondents in our survey), particularly in established companies with ingrained cultures and processes. Despite all of these challenges, DevSecOps adoption continues to grow as organizations recognize the importance of having secure software applications and the long-term benefits such as reduced vulnerabilities, faster response times, improved compliance, and more.

Vendor Consolidation and Preference for Platform Solutions

From our conversations with application security companies and industry practitioners, we believe the trend of vendor and tool consolidation is continuing in the DevSecOps space as well as the broader cybersecurity industry. According to an IDC survey from earlier this year, 86% of organizations are either consolidating or planning to consolidate their security tools, and we believe DevSecOps tools are part of the tool sprawl problem given the proliferation of specialized products designed to address specific segments of the development, security, and operations pipeline. In our view, however, point solutions are likely to be acquired to be part of a broader platform solution such as an application security platform, developer platform, or a CNAPP. We are also seeing companies partner with and acquire strategic vendors to offer customers greater functionality, cost efficiency, visibility, scalability, and control. For example, over the last couple years, Micro Focus acquired OpenText for its application security portfolio, HashiCorp acquired BluBracket to bolster its secrets management solution, CrowdStrike acquired Bionic for ASPM, Snyk acquired Enso Security also for its ASPM capabilities, and Palo Alto Networks acquired Cider Security for CI/CD security capabilities. More recently, Snyk acquired Helios for its application runtime data capabilities, GitLab acquired Oxeye to offer SAST capabilities and improve its SCA and compliance tools, IBM acquired HashiCorp, and Google acquired Wiz for its CNAPP capabilities. In our view, there are three areas experiencing consolidation in the DevSecOps market: 1) application security testing vendors, 2) DevOps platform vendors moving into DevSecOps, and 3) cloud-native application protection platform vendors.

Core Value Propositions of DevSecOps Platforms

Exhibit 7
On the Ground and in the Cloud; A Developer Technology Quarterly
DevSecOps Platform



Source: William Blair Equity Research

Ability to Scale Security Across Multiple Teams and Pipelines

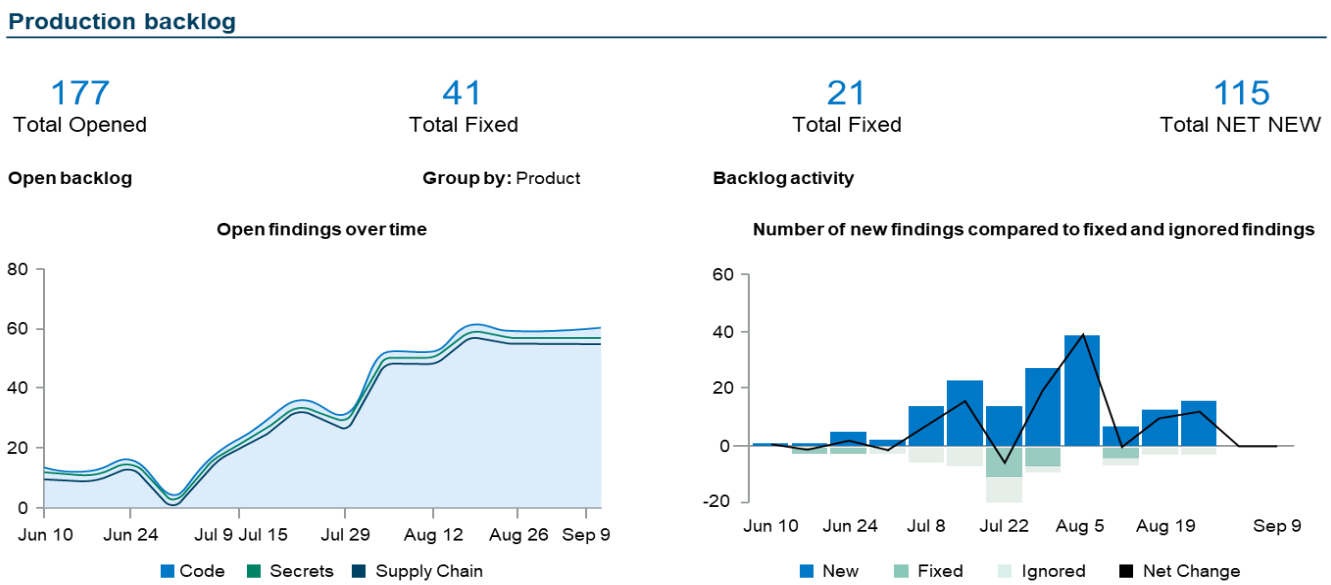
Large and growing organizations face challenges with managing cybersecurity consistently across different development teams, technologies, and workflows as they often operate in fast-paced and complex environments that include on-premises infrastructure, cloud services, and containerized applications. DevSecOps platforms better enable organizations to scale security across multiple teams and pipelines through automated security testing, consistent security policies, security-as-code, and multi-environment security. Platform solutions provide automated tools for

static application security testing (SAST), dynamic application security testing (DAST), and software composition analysis (SCA), which are integrated directly into CI/CD pipelines so that every code change is automatically subjected to security checks, no matter which team the change comes from. Also, DevSecOps platforms offer a centralized mechanism for defining, enforcing, and managing security policies, such as vulnerability thresholds, access controls, and encryption standards, through security-as-code. Security-as-code allows for security policies to be written as code and versioned, similar to application code, to ensure the same security rules are consistently applied across different pipelines rather than manually configuring security settings for each one, which is cumbersome, error-prone, and can lead to inconsistent security practices within an organization. Lastly, DevSecOps platforms are designed to support security management across different environments, which also helps them scale security in a consistent manner without needing different tools or workflows for each environment.

Enhanced Visibility Into an Organization's Entire Application Security and Compliance Posture

DevSecOps platforms centralize security data, automate security and compliance monitoring, and provide real-time dashboards that aggregate information from various tools and stages of software development. These platforms continuously track vulnerabilities, misconfigurations, and compliance violations to give DevSecOps teams a unified and enhanced view into their entire environment. Organizations often lack visibility when they have disparate tools separated by different operating environments and teams, which leads to security gaps going undetected, vulnerabilities being discovered too late, and compliance requirements going overlooked. With centralized dashboards, organizations can more easily track and manage security across multiple pipelines, identify high-risk areas, and prioritize remediation efforts, which improves response times. These dashboards consolidate data from security scans, compliance checks, and incident response tools to provide a single-pane-of-glass view. Also, organizations can set compliance benchmarks and automatically block any non-compliant code from being deployed while also continuously monitoring code and infrastructure to ensure compliance with standards and regulations such as GDPR, HIPAA, and PCI-DSS.

Exhibit 8
On the Ground and in the Cloud; A Developer Technology Quarterly
DevSecOps Platform Dashboard



Source: William Blair Equity Research

Improved Collaboration Between Development, Cybersecurity, and IT Operations Teams

A major barrier to organizations shipping applications that are secure by design is due to a lack of communication between security, development, and operations teams as they traditionally worked in siloes; this led to communication gaps, misaligned priorities, and delays in resolving security vulnerabilities. Developers tend to focus on speed and functionality while security teams emphasize risk management and compliance, which can lead to tension between the two when security concerns and remediation efforts are introduced late in the development process. IT operations teams are then tasked with managing deployments of the applications, so traditional processes led to a disconnect between each team that DevSecOps platforms aim to solve. In particular, DevSecOps platforms can

integrate with existing collaboration tools, such as Slack or PagerDuty, to provide teams with automated alerts and notifications about incidents for faster and more coordinated responses to security threats. These platforms also integrate with Git repositories, CI/CD pipelines, ticketing platforms like Jira, and more to break down siloes and improve communication to deliver on the goal of collaborating efficiently to ship secure software applications.

Strong Security Support for Modern Application Architectures
Modern application architectures, such as cloud-native, microservices, and containerized environments, present additional cybersecurity challenges because they are more complex, distributed, dynamic, and dependent on external services and APIs. In traditional monolithic applications, security controls are centralized and applied uniformly to the entire application, but modern applications are composed of many smaller and independently deployed components (like microservices), which each have their own APIs, databases, and configurations. This creates a much larger attack surface as every microservice, API, or container becomes a potential entry point for attackers. DevSecOps platforms can integrate with existing tools or provide capabilities for securing containers, infrastructure as code (IaC), APIs, cloud environments, and microservices architectures, while also providing a centralized dashboard to bring everything together for a unified view of the entire application infrastructure. In addition, DevSecOps platforms have runtime application self-protection (RASP) and other application security tools to monitor deployed applications in real-time for any suspicious behavior to also provide security support for modern applications.

Greater Integration of DevSecOps Tooling
Instead of requiring separate, standalone security processes, DevSecOps platforms integrate key security features – such as continuous security monitoring, SAST, DAST, SCA, vulnerability prioritization, compliance monitoring, IaC security, container security, cloud-native application security, API protection, and more – into development and IT operations workflows so that security checks are an automated aspect of the software development lifecycle. In our view, DevSecOps tools have contributed to the tool sprawl problem in cybersecurity, so we believe platform solutions reduce tool fragmentation and eliminate siloes between security, development, and operations teams. In turn, this integrated approach accelerates both the adoption of security practices and the speed of resolving security issues as they arise. DevSecOps platforms also integrate with software development tools like version control systems, issue tracking tools, and collaboration platforms to help make sure security alerts and issues are communicated to the correct teams in real time. More recently, DevSecOps platforms are integrating in the application runtime to help prioritize which vulnerabilities need to be remediated first by knowing what all is in production.

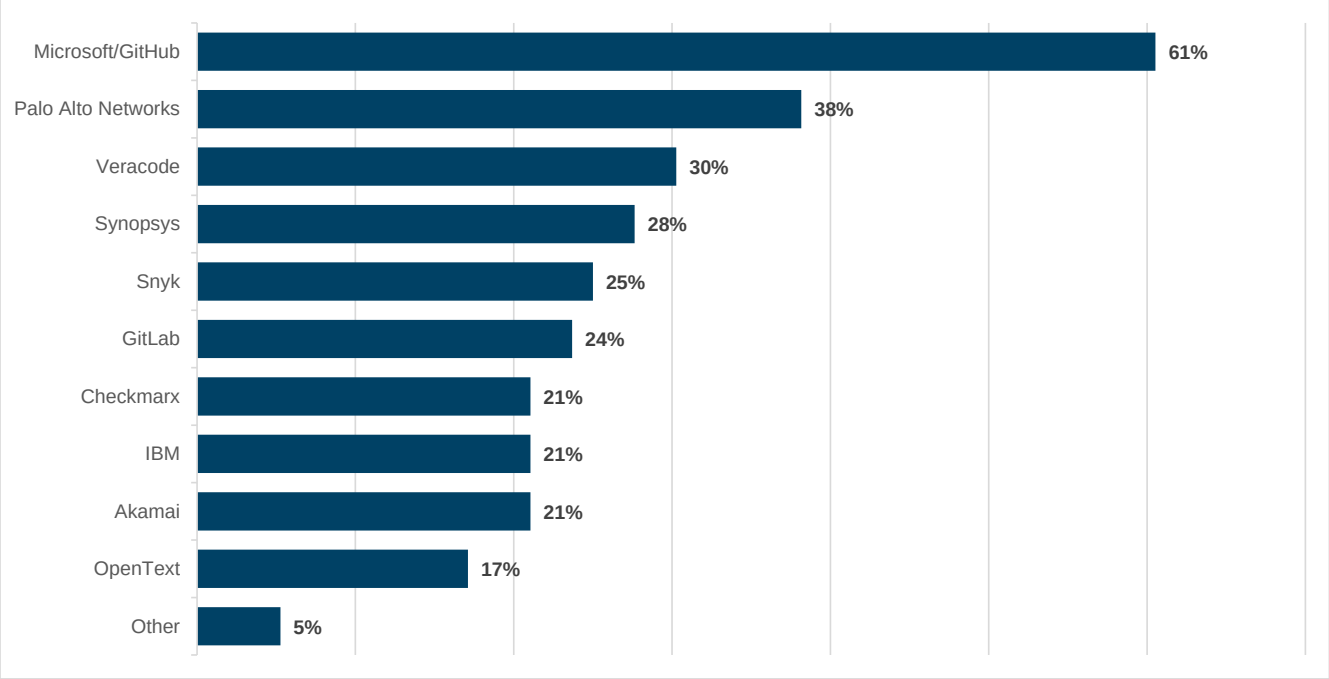
Security Embedded Throughout Software Development
With greater tooling integration, DevSecOps platforms have various security tools and practices at every stage of the software development lifecycle. These platforms provide security at the code level, continuous security in CI/CD pipelines, automated policy enforcement, runtime security in production, real-time feedback and remediation, and end-to-end security audits and compliance. At the code level, DevSecOps platforms scan code as it is being written to help developers identify vulnerabilities, insecure coding practices, and vulnerable dependencies early in the development process to help ensure security is addressed before the code moves further through the pipeline. During the continuous integration and delivery process, security testing (particularly DAST) and container security is automatically embedded to run checks each time new code is integrated for potential runtime issues such as authentication flaws, SQL injections, or insecure configurations. DevSecOps platforms also provide real-time feedback to developers with actionable remediation recommendations within their workflow as security vulnerabilities are detected during software development or testing. Platform solutions also have runtime security features for applications in production that aim to monitor, detect, and block attacks post-deployment.

Proprietary Survey of Developers

The William Blair technology team performed a proprietary survey of developers and security teams. Our goal with this survey was to better understand how DevOps and security teams view the DevSecOps market, which technologies and vendors are enabling adoption, and how the market may have changed over the last year. Much of our research to date has centered on speaking with dozens of DevSecOps vendors and industry experts to analyze the market from a technological perspective. With this survey, we aim to gain the perspective from the people using DevSecOps tools and practices and to parse out any potential disconnects between perceived market trends and what is happening on the ground with customers.

We surveyed a total of 76 developers/practitioners involved in the DevSecOps toolchain. We again asked respondents about which DevSecOps vendors they use for tooling; not surprisingly, Microsoft/GitHub was the most popular (selected by 61% of respondents). GitHub is a popular developer platform, with over 100 million users, and we believe many software developers opt to use GitHub's built-in security features because they are already familiar with the platform. The next most popular vendors from our survey were Palo Alto Networks (selected by 38% of respondents), Veracode (30%), Synopsys (28%), and Snyk (25%) to round out the top five. We continue to view the DevSecOps tools market as fragmented among different types of security companies. For example, Microsoft/GitHub and GitLab are developer platforms with added security features, Synopsys and Veracode are legacy application security vendors that are adding modern capabilities (such as application security posture management and automated remediation) to their product portfolios, Palo Alto Networks is a broad CNAPP vendor, and Snyk is a modern application security platform provider.

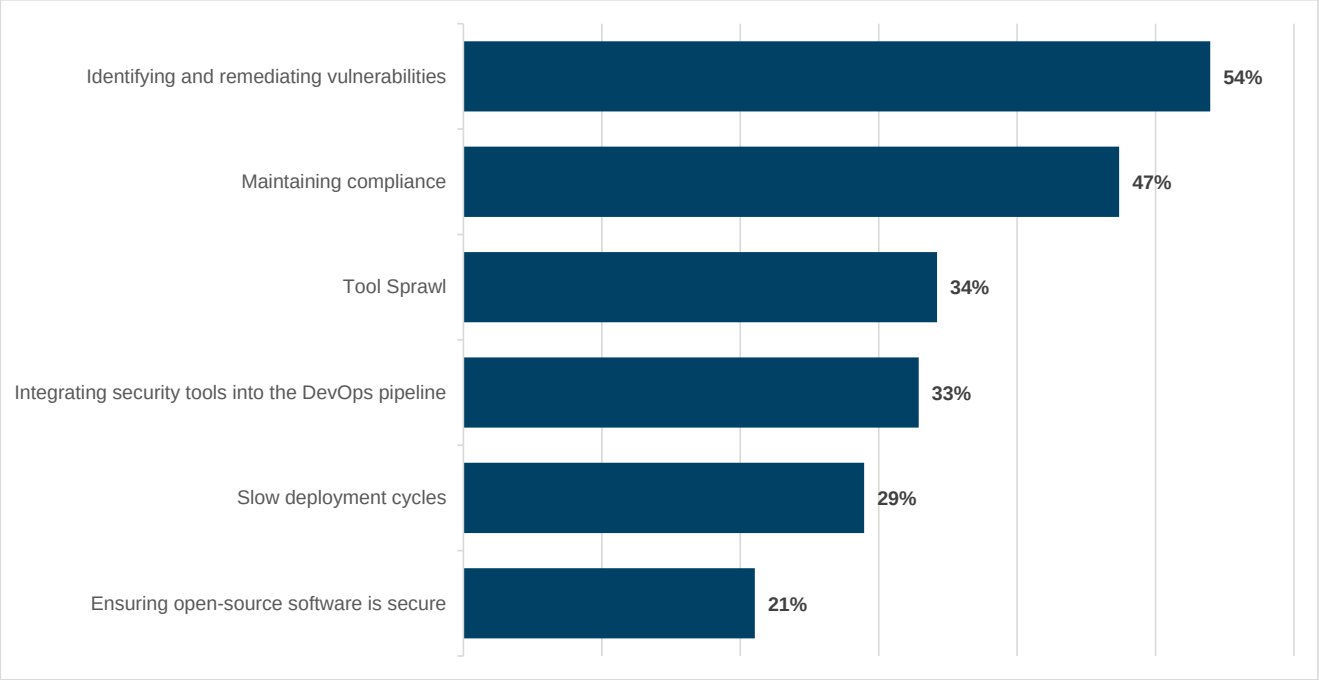
Exhibit 9
On the Ground and In the Cloud; A Developer Technology Quarterly
Which vendor(s) do you use for DevSecOps tools?



n = 76
Source: William Blair Equity Research

We also asked survey respondents to identify their top pain points in their developer workflows when it comes to security, and, of course, the top issue is identifying and remediating vulnerabilities. Removing vulnerabilities from application source code is difficult and one of the main purposes of DevSecOps (along with not slowing down the development process with security), so we expect this to be a top issue for at least the near future. The next two biggest pain points are: 1) maintaining compliance, which we believe is top of mind for organizations given the rise of global regulations (like GDPR and PCI DSS) and modern security standards (such as NIST and OWASP frameworks), and 2) tool sprawl, which has been a consistent problem and driver of vendor consolidation trends due to the fragmented view increasing complexity and risk while reducing efficiency and visibility.

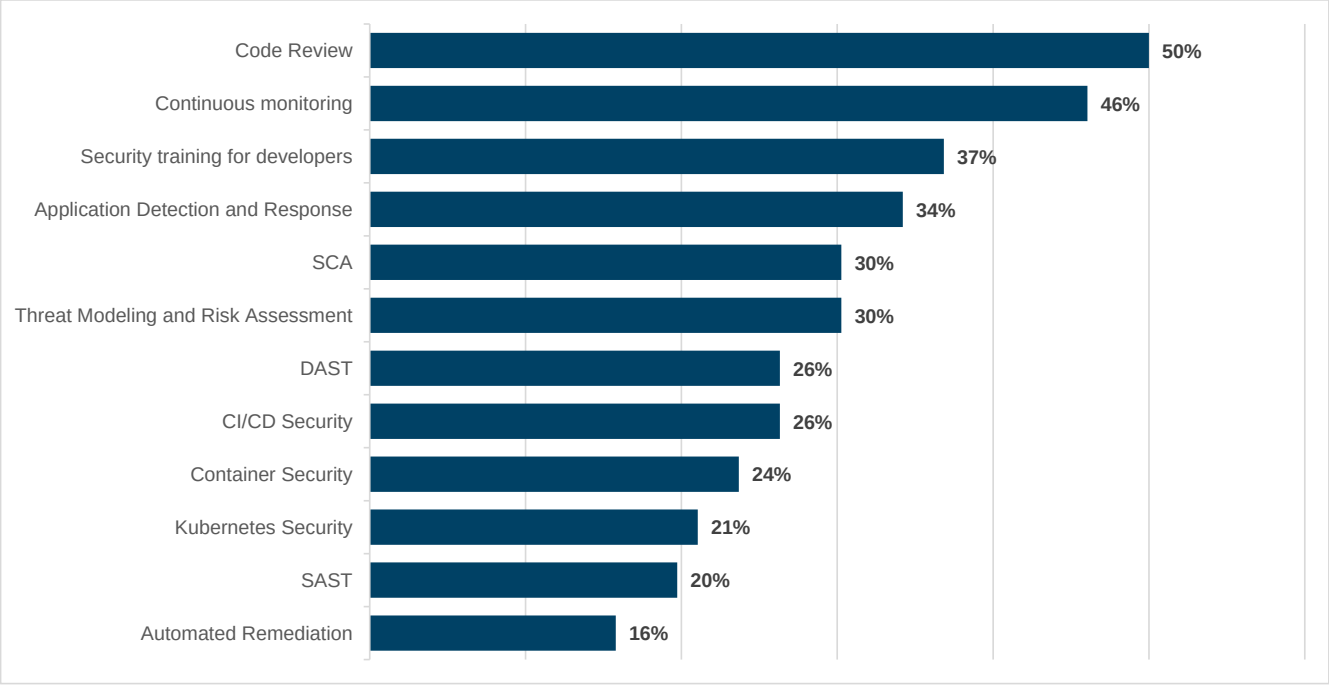
Exhibit 10
On the Ground and In the Cloud; A Developer Technology Quarterly
What are the biggest pain points in your developer workflow with regard to security?



n = 76
Source: William Blair Equity Research

We again asked about the specific types of DevSecOps tools and practices to see if there was a change in what is being most used by developers. Code review is again the most common among respondents (selected by 50%), which we are still not surprised by given that it is a traditional practice where a developer or team of developers reviews someone else's code for quality assurance before deploying it. Continuous monitoring remains behind code review, with 46% of respondents using tools to automatically monitor systems and processes for security risks and compliance issues. Different from our survey last year, security training for developers (selected by 37% of respondents) is the third most common practice, which we believe is a result of organizations realizing how important it is to ship secure software applications and communicating that to developers. Application detection and response was selected by 34% of respondents, which is a bit of a surprise for us given that it is a relatively new and emerging category; however, we believe it has potential to be an important technology in the detection and response landscape. Automated remediation was another new answer option we added to this survey question this year, and it ranked as the least used DevSecOps practice (with a 16% selection rate), which is expected because we view automated remediation as a future trend in the space.

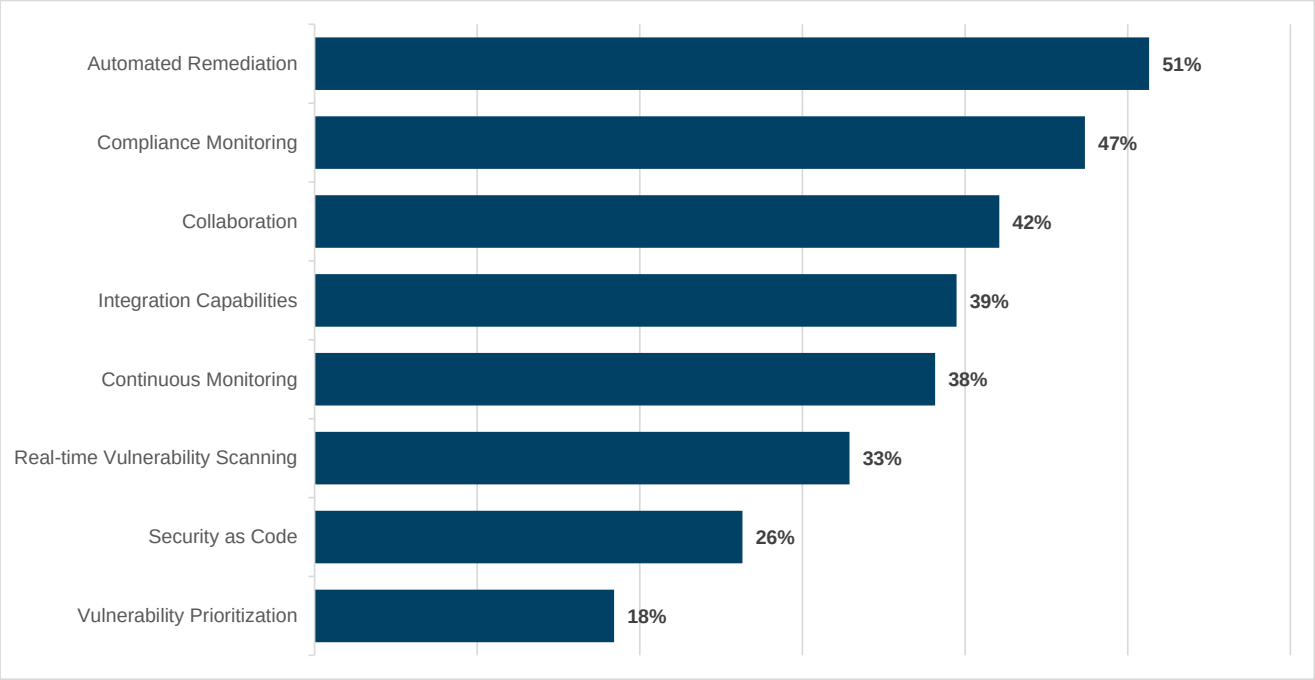
Exhibit 11
On the Ground and In the Cloud; A Developer Technology Quarterly
Which of the following security tools/practices do you currently implement as part of your DevSecOps program?



n = 76
Source: William Blair Equity Research

In terms of the features developers would like to see in their DevSecOps toolchains, automated remediation was the most selected at 51%, which tracks with the previous question where it was found to be the least used among respondents because it is a very early and emerging trend. In our view, automated remediation is needed for every DevSecOps program in order to seamlessly integrate security measures throughout the software development lifecycle, and we believe it makes developers' and security teams' jobs easier to maintain security while not sacrificing development speed. Compliance monitoring was selected by 47% of respondents to be the second most desired feature, which makes sense to us given that maintaining compliance is a major pain point for DevSecOps teams. The next two features selected were collaboration (42%) and integration capabilities (39%), which we believe demonstrates a major challenge that DevSecOps teams face of not having tools to easily work with other areas of an organization. We believe this has been a major hurdle for companies to overcome in order to achieve the goals of DevSecOps.

Exhibit 12
On the Ground and In the Cloud; A Developer Technology Quarterly
What are the key features you would like your DevSecOps tools to include?

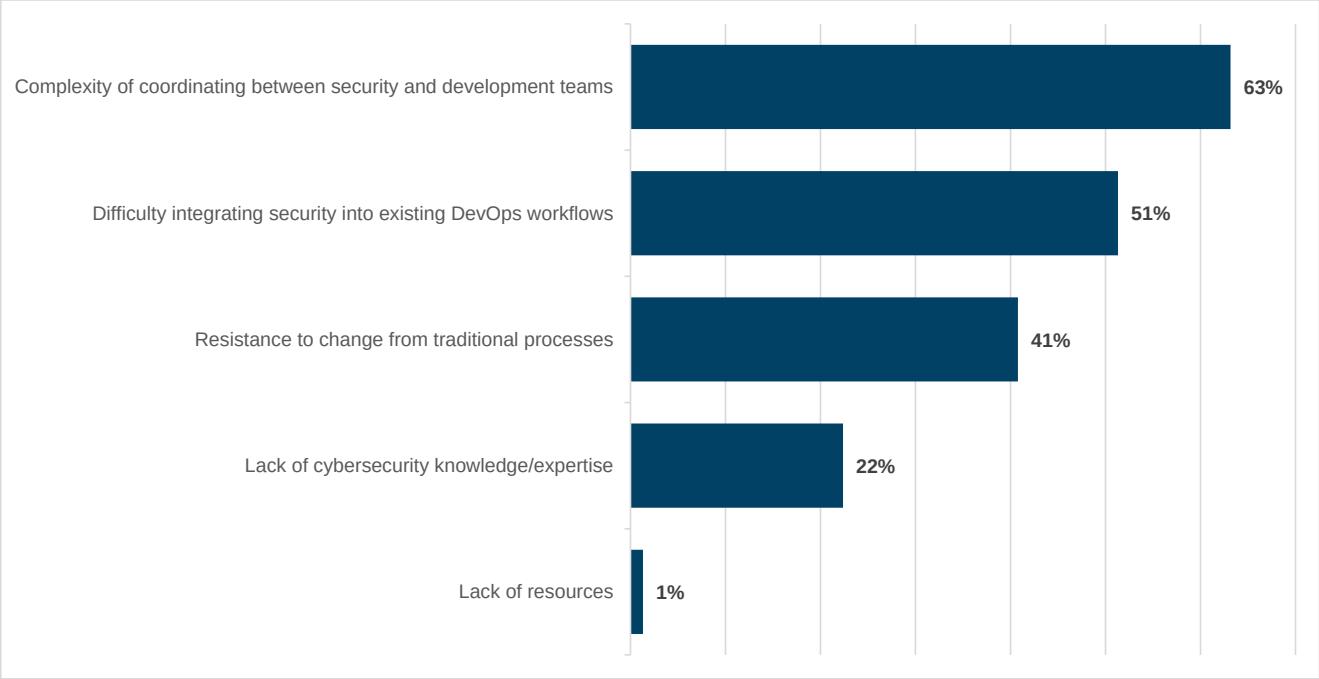


n = 76

Source: William Blair Equity Research

We asked the same question about the key challenges that may be hindering adoption of DevSecOps tools, and there was some change in answers from our survey last year. Currently, 63% of respondents selected complexity of coordinating between security and development teams as their biggest challenge, marking a significant increase from 40% last year. Difficulty integrating security into existing DevOps workflows was selected by 51% of respondents to be the second key challenge, which is also an increase from 41% in our previous survey. Resistance to change from traditional processes decreased from 48% to 41%, representing a slight improvement in developers' willingness to integrate security into their workflows. Lastly, just 22% of respondents selected lack of cybersecurity knowledge/expertise as a key challenge, which we view as a positive sign that organizations are gaining visibility into their security posture after 55% of respondents selected this option as a key challenge last year.

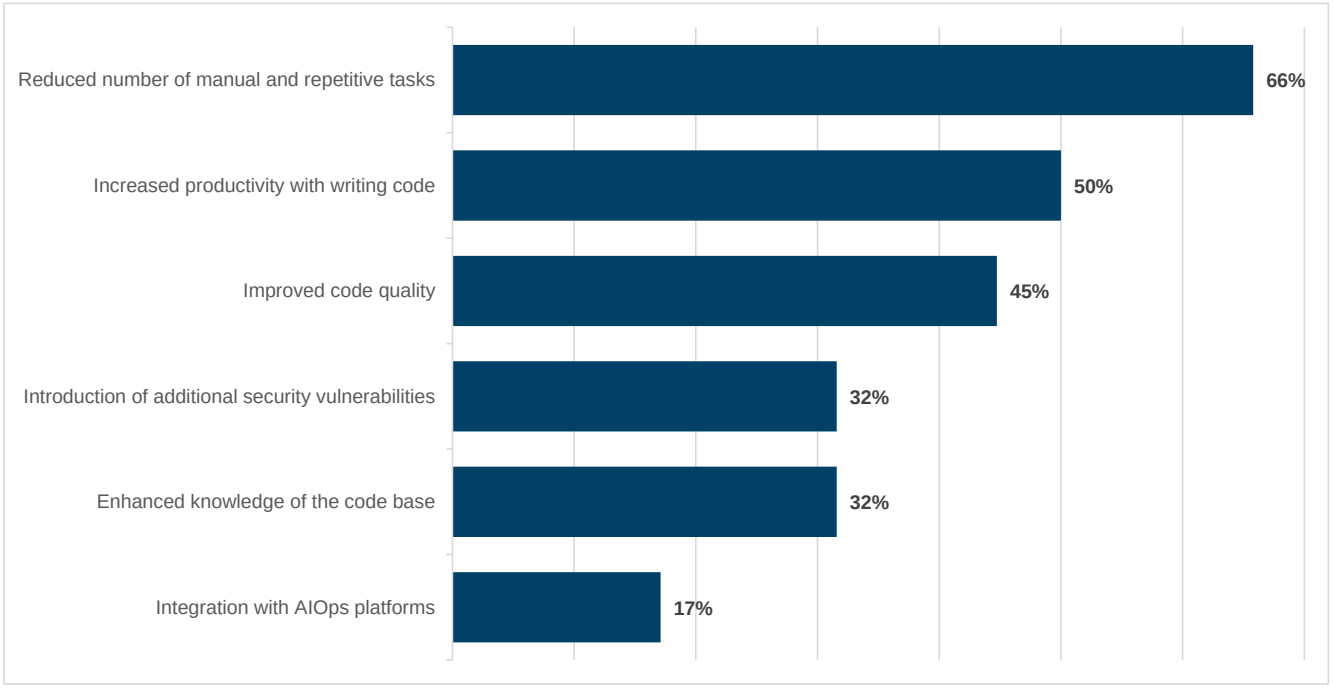
Exhibit 13
On the Ground and In the Cloud; A Developer Technology Quarterly
In your view, what are the key challenges that may be preventing you from adopting DevSecOps tooling?



n = 76
Source: William Blair Equity Research

Regarding generative AI, we expected many potential impacts to software development, cybersecurity, and the DevSecOps space. The top impact on developers' workflows (with 66% of responses) is reducing the number of manual and repetitive tasks in software development, which in turn should lead to increased productivity with writing code (50%). These top two impacts of generative AI were followed by improved code quality, additional security vulnerabilities introduced, enhanced knowledge of the code base, and integration with AIOps platforms. These responses align with early generative AI use-cases of gathering information and turning natural language prompts into code, which should lead to fewer manual tasks and increased coding productivity. We believe it remains to be seen whether generative AI will improve code quality or introduce many new vulnerabilities; however, 45% of our respondents believe it will improve code quality (while 32% believe it will introduce more vulnerabilities), which we believe is likely over time as large language models improve and become more specialized.

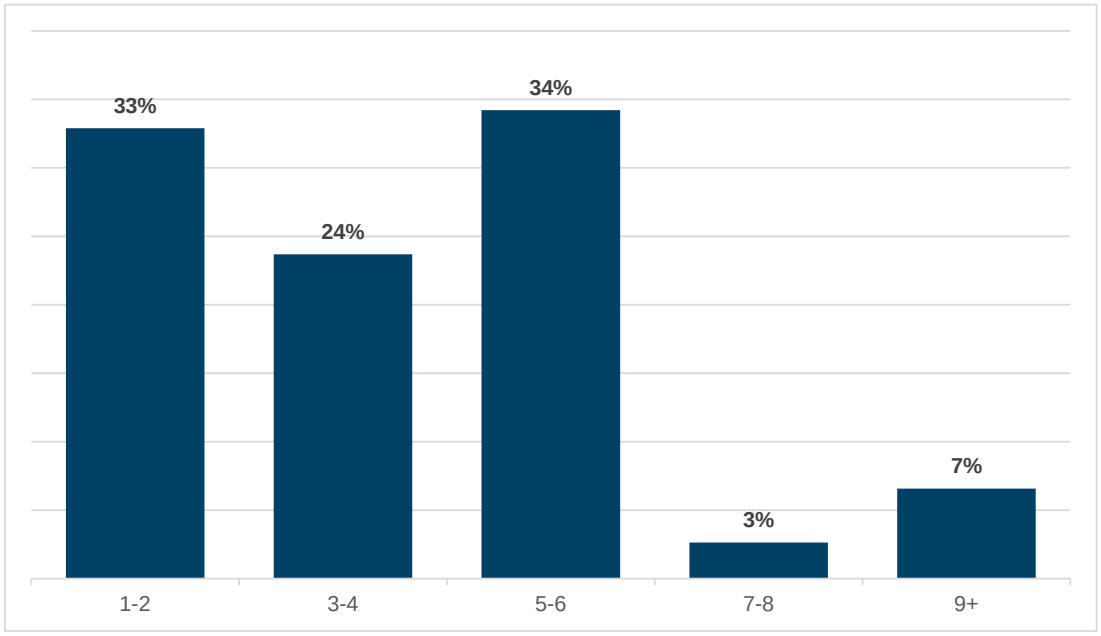
Exhibit 14
On the Ground and In the Cloud; A Developer Technology Quarterly
How do you see generative AI impacting your workflow?



n = 76
Source: William Blair Equity Research

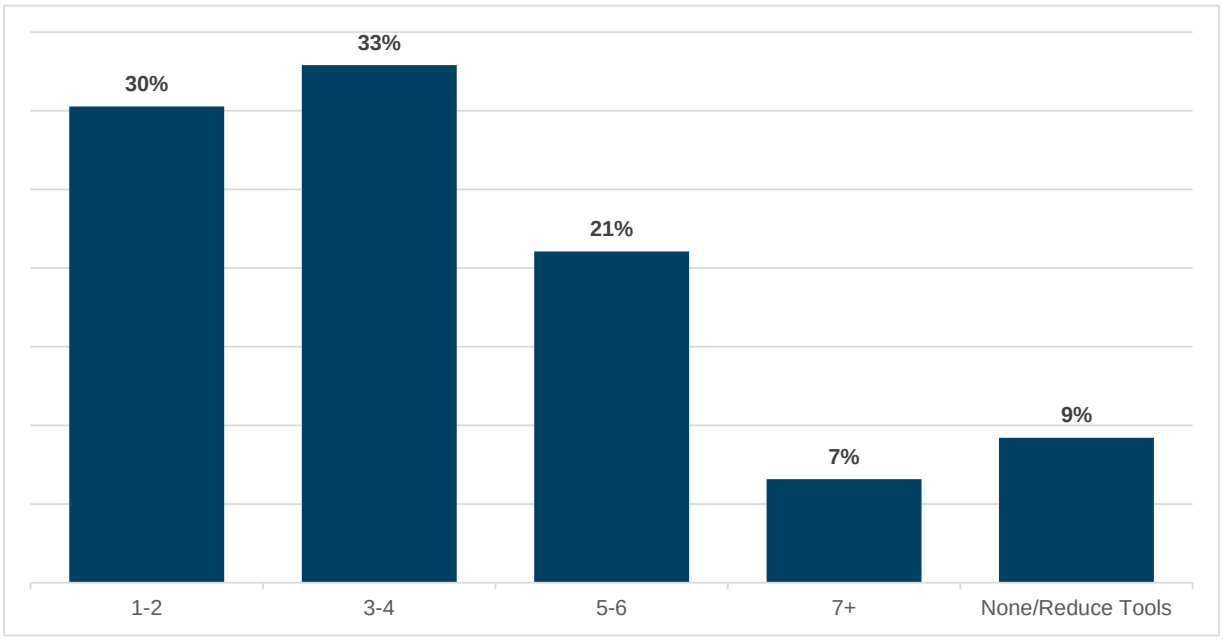
Lastly, for our final two questions, we asked the same questions as last year with regard to the adoption of DevSecOps tools. Currently, 34% of respondents use 5-6 DevSecOps tools, while 33% use 1-2 and 24% use 3-4. This differs from last year, when 47% of respondents had 3-4 tools, leading us to believe that many practitioners added 1 or 2 tools over the past year. Also, looking at the number of security tools our respondents would like to add to their DevSecOps toolchain, 91% of respondents want more security solutions. In addition, 63% of our respondents would like to add one to four tools, while only 28% would like to add five or more, suggesting that there is still an appetite to adopt more DevSecOps tools; however, it is for fewer solutions than in the past. The responses to these two questions also confirm our view that DevSecOps adoption is generally mixed among organizations and its maturity varies greatly between different teams.

Exhibit 15
On the Ground and In the Cloud; A Developer Technology Quarterly
How many security tools are you currently using within your DevSecOps toolchain?



n = 76
Source: William Blair Equity Research

Exhibit 16
On the Ground and In the Cloud; A Developer Technology Quarterly
How many security tools would you like to add to your DevSecOps toolchain?



n = 76
Source: William Blair Equity Research

Appendix – Private Company Profiles

This section contains many private companies involved in the DevSecOps space but is by no means comprehensive.

ActiveState	**ActiveState** https://www.activestate.com/	Founded in 1997 and based in Vancouver, Canada, ActiveState provides an end-to-end open-source supply chain security platform to help protect customers' software development process. ActiveState focuses on securing the use of open-source software by vetting open-source code to enable developers to safely build applications. ActiveState's latest funding came from a private equity round in 2021.
anchore	**Anchore** https://anchore.com/	Founded in 2016 and based in Santa Barbara, California, Anchore provides an SBOM-powered software supply chain security and management platform. The company's platform solution helps customers with generating and scanning SBOMs, container security, Kubernetes security, CI/CD compliance, DevSecOps, and more. Since inception, Anchore has raised a total of $41 million over seven rounds of funding.
apiiro	**Apiiro** https://apiiro.com/	Founded in 2018 and based in New York, New York, Apiiro enables application security and development teams to proactively detect and remediate risk for their cloud applications and software supply chains. The company's ASPM platform offers comprehensive application security posture management that unifies risk visibility, prioritization, and remediation with context. In November 2022, Apiiro raised $100 million in a series B funding round, bringing its total capital raised to $135 million since 2020.
aqua	**Aqua Security** https://www.aquasec.com/	Founded in 2015 with headquarters in Burlington, Massachusetts, and Israel, Aqua Security is a cloud-native security company focused on developer and cloud security. The company's cloud-native application protection platform automates the detection, prevention, and remediation across application lifecycles to provide developer and cloud security. Aqua has raised a total of $325 million over eight rounds of funding since inception, with its latest being a series E for $60 million in January 2024.
ArmorCode	**ArmorCode** https://www.armorcode.com/	Founded in 2020 and based in Palo Alto, California, ArmorCode provides an ASPM platform that provides capabilities for application security, vulnerability management, and software supply chain security to help customers ship applications faster and more securely. ArmorCode has raised a total of $65 million over four rounds of funding, with the latest being a series B round for $40 million in December 2023.
BeyondTrust	**BeyondTrust** https://www.beyondtrust.com/	Founded in 1985 and based in Johns Creek, Georgia, BeyondTrust is an identity security company that primarily focuses on privileged access management (PAM) to secure and protect privileged accounts across passwords, endpoints, and access. In the realm of DevSecOps, BeyondTrust offers a secrets management solution that manages privileged passwords, accounts, keys, secrets, and sessions for humans and machines and has capabilities for application password management. The company's latest funding came from a private equity round in June 2021.
BIONIC A CrowdStrike Company	**Bionic** https://www.crowdstrike.com/platform/cloud-security/aspm/	Founded in 2019 in Palo Alto, California, Bionic offers an application security posture management platform that proactively reduces cyber risk for applications in production. The platform analyzes application architectures and all of its dependencies to help organizations manage the security of applications they are using. In September 2023, CrowdStrike acquired Bionic for $350 million.
Chainguard.	**Chainguard** https://www.chainguard.dev/	Founded in 2021 with headquarters in Kirkland, Washington, Chainguard is a software supply chain security company with products and services that enable container security and cloud-native application security. Chainguard has raised a total of $612 million over five rounds of funding, with Sequoia Capital leading the company's series A round.

	Checkmarx https://checkmarx.com/	Founded in 2006 and based in Atlanta, Checkmarx is a leading application security vendor, offering a wide range of application security and DevSecOps tools. The company's platform offering, Checkmarx One, is a comprehensive application security platform that integrates Checkmarx's full suite of application security testing solutions, including SAST, SCA, SCS, API security, DAST, container security, and IaC security. The company has raised a total of $92 million over four rounds of funding, with its latest being a series C round in 2015.
	Contrast Security https://www.contrastsecurity.com/	Founded in 2014 and based in Los Altos, California, Contrast Security is a code security platform company that enables DevSecOps to protect customers from attacks on their software applications. The company's platform solutions span capabilities such as IAST, SAST, RASP, SCA, and serverless. In November 2021, Contrast Security raised $150 million in a series E round of funding, bringing its total capital raised to $269 million since inception.
	Cycode https://cycode.com/	Founded in 2019 with headquarters in Tel Aviv, Israel, Cycode provides an application security posture management platform that includes capabilities of SAST, SCA, IaC security, secrets detection, and CI/CD security. The company has raised $80.6 million in funding over three rounds, with its latest being a series B round in November 2021 for $56 million.
	Delinea https://delinea.com/	Founded in 2004 and based in San Francisco, Delinea offers privileged access management (PAM) solutions. The company also has a platform to extend PAM throughout an enterprise for just-in-time access controls with additional identity and access management capabilities. In March 2021, Delinea was acquired by private equity firm TPG for $1.4 billion through a merger between Centrify and Thycotic.
	Detectify https://detectify.com/	Founded in 2013 with headquarters in Stockholm, Sweden, Detectify provides an external attack surface management platform by combining its surface monitoring, which continuously monitors known and unknown internet-facing assets, and application scanning, which is a DAST solution. Detectify has raised a total of $42 million over five rounds of funding since 2015 and was acquired by private equity firm Insight Partners in October 2024.
	Digital.ai https://digital.ai/	Founded in 2020 and based in Raleigh, North Carolina, Digital.ai aims to help organizations plan, test, secure, and deploy software through its AI-powered DevSecOps platform. The platform has capabilities for application security, continuous testing, release orchestration, deployment automation, and more. The company was formed through mergers and acquisitions of several companies.
	Endor Labs https://www.endorlabs.com/	Founded in 2021 and based in Palo Alto, California, Endor Labs offers an open-source dependency lifecycle management platform that facilitates the security and maintenance of open-source software that customers use in their applications. Endor Labs has raised a total of $188 million in funding over five rounds since 2022, with the latest being a $93 million series B round in April 2025.
	Flexera https://www.flexera.com/	Founded in 2008 with headquarters in Itasca, Illinois, Flexera helps organizations discover and manage their software, SaaS apps, hardware, containers, and more for improved visibility into IT assets and optimized application usage. The company was acquired by private equity firm Thoma Bravo for $2.9 billion in December 2020.
	Fortra https://www.fortra.com/	Founded in 1982 and based in Minneapolis, Fortra provides cybersecurity, network and systems management, automation, business intelligence, and compliance solutions to monitor and automate processes and encrypt and secure data. The company also offers penetration and application security testing. Fortra was acquired by private equity firm H.I.G. Capital in August 2015.

	Fossa https://fossa.com/	Founded in 2015 and based in San Francisco, Fossa helps customers track open-source code they use and automate license scanning and compliance with its open-source risk management platform offering. The company's platform provides capabilities for risk detection, a policy engine, and actionable intelligence. Fossa has raised a total of $38.4 million in funding over five rounds since inception.
	GrammaTech https://www.grammatech.com/	Founded in 1988 and based in Bethesda, Maryland, GrammaTech offers cybersecurity research and development services and tools to the U.S. defense and intelligence community. In September 2023, Battery Ventures acquired the software products division of GrammaTech, including the CodeSonar (SAST) and CodeSentry (SCA) product lines.
	HackerOne https://www.hackerone.com/	Founded in 2012 and based in San Francisco, HackerOne provides solutions for application security, cloud security, and vulnerability management. The company's Attack Resistance Platform offering provides a comprehensive solution to secure each phase of the software development lifecycle. The company also connects businesses with penetration testers and cybersecurity researchers. HackerOne has raised a total of $159.4 million over five rounds of funding, with its latest being a series E round for $49 million.
	Harness https://www.harness.io/	Founded in 2017 with headquarters in San Francisco, Harness provides a software delivery platform to assist software-producing organizations with a modern CI/CD pipeline, improved developer experience, secure software delivery, and cloud spend optimization. The company's platform leverages AI throughout for coding assistance and automation, and it supports over 100 integrations to fit into existing environments. Harness has raised a total of $575 million over 8 rounds of funding since inception.
	Immersive Labs https://www.immersivelabs.com/	Founded in 2017 with headquarters in Bristol, England, Immersive Labs is a cybersecurity training company that offers labs, simulations, and exercises for individuals, teams, and organizations. Regarding application security, Immersive Labs measures and improves security teams' application security posture and capabilities across their software development lifecycle. The company has raised a total of $189.7 million in funding over seven rounds since its founding.
	Imperva https://www.imperva.com/	Founded in 2002 and based in San Mateo, California, Imperva provides solutions for activity monitoring, real-time protection, and risk management to enable application security and performance, data security, and network security for customers. In July 2023, Imperva was acquired by Thales Group for $3.6 billion.
	Invicti https://www.invicti.com/	Founded in 2018 and based in Austin, Texas, Invicti provides a comprehensive application security platform that enables customers to continuously scan and secure their web applications and APIs. The company enables DevSecOps as its platform builds security automation into every step of the software development lifecycle. In October 2021, Summit Partners acquired Invicti Security for $625 million.
	Ivanti https://www.ivanti.com/	Founded in 1985 with headquarters in South Jordan, Utah, Ivanti provides integrated IT and cybersecurity solutions across broad areas of endpoint management, enterprise service management, network security, and exposure management. The company offers ASPM, secure access to apps, and application control capabilities. In a debt financing round in April 2025, Ivanti raised $350 million.
	Kiuwan https://www.kiuwan.com/	Founded in 2012 and based in Houston, Kiuwan offers application security testing solutions to provide SAST and SCA as well as code analysis and governance. The company's products also integrate with third-party tools to enable DevSecOps. Kiuwan was acquired by Idera, which is private equity held, in October 2018 for an undisclosed amount.

	**Lacework** https://www.lacework.com/	Founded in 2015 in Mountain View, California, Lacework began with a focus on cloud detection and response and subsequently built out many components of the CNAPP stack, including workload protection, posture management, and code security capabilities such as software composition analysis and application security testing. In June 2024, Fortinet acquired the company for an undisclosed amount.
	**Legit Security** https://www.legitsecurity.com/	Founded in 2021 and based in Palo Alto, California, Legit Security provides an application security posture management platform that has capabilities for software supply chain security, code to cloud traceability, an application security control pane, compliance, and SBoM generation. Since inception, Legit Security has raised a total of $73.5 million over three rounds, with its latest being a series B round for $40 million in September 2023.
	**Mend.io** https://www.mend.io/	Founded in 2011 with headquarters in Boston, Mend provides an integrated application security platform that emphasizes automated remediation capabilities. The company's AppSec platform integrates its SAST, SCA, and supply chain security solutions. Since inception, Mend has raised a total of $121.2 million over five rounds of funding.
	**New Relic** https://newrelic.com/	Founded in 2008 with headquarters in San Francisco, New Relic provides an observability platform to deliver visibility and analytics to enterprises. Its capabilities include interactive application security testing, infrastructure monitoring, and Kubernetes monitoring in the realm of DevSecOps. New Relic has raised $214.5 million over eight rounds of funding since inception.
	**Akamai API Security** https://www.akamai.com/products/api-security	Founded in 2020 in San Jose, California, Noname Security provides a comprehensive API security platform that has capabilities for runtime protection, discovery, posture management, and security testing. The company raised a total of $220 million over three rounds of funding and was acquired by Akamai for $450 million in May 2024.
	**NowSecure** https://www.nowsecure.com/	Founded in 2009 and based in Chicago, NowSecure provides automated mobile application security testing with its platform offering, which can also test any mobile application language or framework. The company has raised a total of $27.5 million in funding over four rounds, with its latest being a debt financing round in June 2022.
	**Offensive Security (OffSec)** https://www.offsec.com/	Founded in 2006 and based in New York, New York, OffSec is a cybersecurity training company that offers a wide range of courses in areas such as penetration testing, web applications, exploit development, security operations, and more on basic fundamentals. The company was acquired by Leeds Equity Partners in October 2024.
	**Orca Security** https://orca.security/	Founded in 2019 with headquarters in Portland, Oregon, Orca Security provides a comprehensive cloud security platform with capabilities for CNAPP, container and Kubernetes security, application security, and API security, among others. Orca offers security solutions for an application's entire lifecycle from coding to deployment. The company has raised a total of $632 million over five rounds of funding, with its latest being a series C round for $340 million in September 2021.
	**OX Security** https://www.ox.security/	Founded in 2021 with headquarters in Boston, OX Security provides an end-to-end software supply chain security solution that integrates into DevOps workflows to identify vulnerabilities, prioritize and remediate risks, protect against unknown security risks, and automate the CI/CD process. The company has raised a total of $94 million in funding over four rounds since inception, with its latest being a series B round for $60 million in May 2025.

PERFORCE	**Perforce** https://www.perforce.com/	Founded in 1995 and based in Minneapolis, Perforce provides a DevSecOps platform solution that aims to secure applications' code, data, and infrastructure while bringing quality and timeliness to an organization's software development process. The company can continuously test software quality, automate infrastructure configurations, securely manage APIs, and more in security. Perforce has raised $30 million in funding and was acquired by private equity firm Clearlake Capital Group in January 2018.
PortSwigger	**Portswigger** https://portswigger.net/	Founded in 2008 and based in Cheshire, United Kingdom, PortSwigger provides solutions for web application security and testing with its web vulnerability scanner, web penetration testing tool, and web application security scanning for CI/CD pipelines. In June 2024, PortSwigger raised over $135 million in a private equity round of funding led by Brighton Park Capital.
qwiet AI	**Qwiet AI** https://qwiet.ai/	Founded in 2016 and based in San Jose, California, Qwiet AI offers an AI-powered application security platform that contains capabilities for SAST, SCA, container security, SBoM generation, and secrets management. The company's platform can also integrate with existing CI/CD pipelines, ticketing systems, and development tools. Qwiet AI's latest funding came from a series C round worth $29 million in May 2022.
REVERSINGLABS	**ReversingLabs** https://www.reversinglabs.com/	Founded in 2009 and based in Cambridge, Massachusetts, ReversingLabs provides a comprehensive software supply chain security platform that helps protect software development workflows, containers, and software release packages. It has raised a total of $81 million over three rounds of funding since inception; the latest was a series B round in August 2021 for $56 million.
SALT	**Salt Security** https://salt.security/	Founded in 2018 and based in Palo Alto, California, Salt Security is a leading API security company that provides a comprehensive API protection platform to provide security across the entire API lifecycle. Salt Security helps customers discover all their APIs, prevent API attacks and data leaks, remediate API vulnerabilities, and simplify compliance. The company has raised a total of $271 million in funding over eight rounds since inception, putting Salt Security at a post-money valuation of $1.4 billion.
SECURE CODE WARRIOR	**Secure Code Warrior** https://www.securecodewarrior.com/	Founded in 2015 with headquarters in Sydney, Australia, Secure Code Warrior provides cybersecurity training to software developers to help them apply secure coding techniques. The company provides a secure code training platform for development teams to practice coding without security vulnerabilities. Secure Code Warrior has raised a total of $101.5 million in funding over five rounds since inception, with the latest being a series C round for $50 million in July 2023.
SECURITY JOURNEY	**Security Journey** https://www.securityjourney.com/	Founded in 2016 and based in Pittsburgh, Pennsylvania, Security Journey is a developer security training company that has an application security education platform to help developers build more secure applications. The platform can be integrated with customers' application security tools to provide customized training based on their needs. Security Journey was acquired by HackEDU in May 2022.
snyk	**Snyk** https://snyk.io/	Founded in 2015 with headquarters in Boston, Snyk is a leader in developer security with its automated developer security platform. Snyk provides comprehensive solutions to enable application security and software supply chain security, with products including SAST, SCA, container security, and IaC security. Snyk has raised a total of $1.2 billion in funding over 13 rounds, with its latest being a corporate round for $25 million in January 2023.
sonar	**Sonar** https://www.sonarsource.com/	Founded in 2008 and based in Geneva, Switzerland, Sonar provides a platform solution with the goal of helping customers deliver better software. The company offers SAST and code review products and integrates with popular DevOps platforms. In April 2022, Sonar raised $412 million in a funding round led by General Catalyst and Advent International, giving the company a post-money valuation of $4.7 billion. The company intends to use the funds to grow its go-to-market team.

	**Sonatype** https://www.sonatype.com/	Founded in 2008 and based in Fulton, Maryland, Sonatype provides a software supply chain security platform solution that focuses on securing open-source software components. The platform combines firewall, repository, and lifecycle components to help automate software supply chain security and mitigate open-source risk across the software development lifecycle. Sonatype raised a total of $154.7 million from 2008 to 2018. In November 2019, private equity firm Vista Equity Partners acquired Sonatype for an undisclosed amount.
	**Sophos** https://www.sophos.com/en-us	Founded in 1985 in Oxford, England, Sophos provides a broad range of threat management and security products across endpoint, network, email, and the cloud. The company also offers fully managed cybersecurity through its managed detection and response solution. In October 2019, Sophos was acquired by private equity firm Thoma Bravo for $3.9 billion.
	**StackHawk** https://www.stackhawk.com/	Founded in 2019 and based in Denver, StackHawk provides API and web application security testing capabilities with its modern DAST solution that helps developers remediate vulnerabilities in applications before they go into production. The company has raised a total of $47.3 million over five rounds of funding since inception.
	**Sysdig** https://sysdig.com/	Founded in 2013 and based in San Francisco, Sysdig provides cloud, Kubernetes, and container security solutions. The company's cloud-native application protection platform combines cloud detection and response, vulnerability management, cloud security posture management, and permissions and entitlement management capabilities. The company has raised a total of $729.5 million in funding over nine rounds, with its latest being a $350 million raise in a series G round in December 2021.
	**Traceable** https://www.traceable.ai/	Founded in 2018 and based in San Francisco, Traceable is an API security company with a platform offering that provides capabilities for security posture management (with API discovery), threat protection, and threat management for APIs. In February 2025, Traceable merged with Harness.
	**Veracode** https://www.veracode.com/	Founded in 2006 and based in Burlington, Massachusetts, Veracode provides its software security platform that helps organizations secure each phase of their software development lifecycle. The company offers application security products and services including SAST, DAST, SCA, container security, remediation capabilities, and more. In March 2022, Veracode was acquired by private equity firm TA Associates for $2.5 billion.
	**F5 API Security** https://www.f5.com/products/distributed-cloud-services/api-security	Founded in 2021 in Tel Aviv, Israel, Wib offers a comprehensive, end-to-end API security platform for securing APIs across their lifecycles. The company provides continuous and complete visibility and control over an organization's APIs. Wib was acquired by F5 in February 2024 in the tens of millions of dollars range.
	**Wiz** https://www.wiz.io/	Founded in 2020 with headquarters in New York, New York, Wiz is a leading player in the cloud security market with its cloud-native application protection platform (CNAPP) solution that provides a unified approach to identifying, preventing, and remediating cyber risk in cloud environments. Wiz's CNAPP brings together capabilities to enable secure cloud application development, cloud workload protection, and cloud threat detection and response. In March 2025, Wiz was acquired by Google for $32 billion.

Glossary

1. **Agile Methodology –** Agile is a project management philosophy that emphasizes an iterative, adaptable, and incremental approach to project delivery.

2. **Application Programming Interface (API) –** APIs are sets of rules and protocols that allow different software applications to communicate and interact with each other to enable the exchange of data and functionality.

3. **Application Security Posture Management (ASPM) –** Holistic approach to application security using a set of tools and solutions to assess, monitor, and improve the security posture of applications throughout the software development lifecycle by identifying and prioritizing vulnerabilities in order to reduce business risk.

4. **Artifacts** – Outputs or byproducts generated throughout the software development lifecycle that describe the software's function, architecture, and design in the form of executables, documentation, or container images.

5. **Artificial Intelligence (AI) –** AI refers to the simulation of human intelligence in machines to perform tasks such as problem-solving, learning, understanding natural language, and decision-making.

6. **Attack Surface –** An attack surface refers to the total sum of vulnerabilities and entry points into a system or application that can be exploited by cyberthreat actors to launch malicious attacks.

7. **Certificates –** Digital documents issued by a trusted authority that verify the authenticity and identity of entities, such as websites or individuals, often through technologies like SSL/TLS.

8. **Cloud-Native Application Protection Platform (CNAPP) –** Cybersecurity solution designed to provide comprehensive protection for cloud-native applications to ensure their security and compliance in cloud environments.

9. **Cloud Security Posture Management (CSPM) –** Cybersecurity tool that focuses on continuously monitoring and optimizing the security configuration of cloud resources to align with best practices and compliance standards.

10. **Containers –** Lightweight, isolated software environments that package applications and their dependencies to enable consistent and efficient software deployment across various computing environments.

11. **Continuous Integration/Continuous Deployment (CI/CD) –** Software development approach that automates the integration of code changes, testing, and deployment to production environments to streamline and accelerate the software development lifecycle.

12. **Cryptographic Keys –** Unique strings of data used to encrypt and decrypt information to secure and protect sensitive data from unauthorized access.

13. **Developer Operations (DevOps) –** Software development and IT operations approach that aims to merge development and operations teams to streamline the software development lifecycle.

14. **Developer, Security, Operations (DevSecOps) –** DevSecOps is an extension of the DevOps methodology that aims to merge DevOps and security teams to ensure each phase of the software development lifecycle incorporates cybersecurity.

15. **Dynamic Application Security Testing (DAST) –** Application security testing method that assesses the security of an application by analyzing it in a running state by simulating real-world attacks to identify vulnerabilities and weaknesses.

16. **Infrastructure as Code (IaC) –** A method to manage computer systems by writing code that defines how they should be set up and configured to make it easier to automate and manage IT infrastructure like servers and networks.

17. **Interactive Application Security Testing (IAST) –** Application security testing method that analyzes application behavior during runtime, similar to DAST, and does so in a way that combines black-box testing, scanning, and internal application flows analysis.

18. **Kubernetes –** Open-source container orchestration platform that automates the deployment, scaling, and management of containerized applications to simplify the use of container-based architectures.

19. **Large Language Models (LLMs) –** Advanced artificial intelligence models that use deep learning techniques to process and generate human-like text based on inputs received.

20. **Microservices –** A software architecture that structures an application as a collection of loosely coupled, independently deployable services that are each responsible for specific functions or features of a software application.

21. **Open-Source –** Software or other products whose source code or design is available to the public to allow anyone to view, use, modify, and/or distribute.

22. **Platform Engineering –** Discipline of designing, building, and maintaining the foundational software and hardware infrastructure that enables the development and deployment of applications across an organization.

23. **Runtime –** In computing, runtime refers to the period when a program or application is actively executing and performing tasks on a computer or system.

24. **Security-as-Code** – Practice of embedding security measures directly into software development and operations processes by defining and automating security controls and policies as code to ensure consistent and scalable security across infrastructure and applications.

25. **Serverless Architecture** – Cloud computing model where developers build and run applications without managing underlying servers as the cloud service provider handles the setup, scaling, and maintenance.

26. **Software Bill of Materials (SBOM) –** Detailed inventory document that lists all software components and their dependencies within an application to facilitate transparency, tracking, and management of software assets and vulnerabilities.

27. **Software Composition Analysis (SCA) –** Practice that identifies and assesses security vulnerabilities and issues in a software application by analyzing its open-source and third-party component dependencies.

28. **Software Development Lifecycle (SDLC) –** Structured process for planning, creating, testing, deploying, and maintaining software systems to ensure they meet quality, security, and functionality requirements throughout the entire process.

29. **Static Application Security Testing (SAST) –** Application security testing method that analyzes the source code of an application to identify vulnerabilities and weaknesses without executing the code.

30. **Tokens –** Digital or physical objects or credentials used to authenticate a user's identity, grant access to systems or resources, and ensure secure communications and transactions.

31. **Virtual Machines** – Software that enables a single physical computer to host multiple isolated operating environments that each run its own operating system and applications as if they were on separate hardware.

32. **Waterfall Methodology –** Traditional method to software development that uses a linear approach where each phase (planning, design, development, testing, and deployment) of a project is completed sequentially.

33. **Web Application Firewall (WAF) –** Cybersecurity solution that protects web applications by filtering and monitoring HTTP requests and responses to identify and block malicious web traffic.

The prices of the common stock of public companies mentioned in this report follow:

Akamai Technologies, Inc. (Outperform)	$79.06
Alphabet, Inc. (Outperform)	$177.56
Amazon.com, Inc. (Outperform)	$274.18
Broadcom Inc. (Outperform)	$874.56
Check Point Software Technologies Ltd. (Outperform)	$222.99
Cisco Systems, Inc. (Market Perform)	$68.93
CrowdStrike Holdings, Inc. (Outperform)	$505.46
CyberArk Software Ltd. (Outperform)	$401.46
Datadog, Inc. (Outperform)	$152.41
Dynatrace, Inc. (Outperform)	$56.64
F5, Inc. (Market Perform)	$299.26
Fastly, Inc. (Market Perform)	$7.05
Fortinet, Inc. (Market Perform)	$106.65
GitLab, Inc. (Outperform)	$46.55
International Business Machines Corp.	$292.47
JFrog, Ltd. (Outperform)	$42.32
Meta Platforms, Inc. (Outperform)	$718.35
Microsoft Corporation (Outperform)	$497.72
Open Text Corporation	$29.84
Palo Alto Networks, Inc. (Outperform)	$201.42
Qualys, Inc. (Outperform)	$146.94
Rapid7, Inc. (Outperform)	$23.89
SentinelOne, Inc. (Outperform)	$18.20
Synopsys, Inc.	$536.52
Tenable Holdings, Inc. (Outperform)	$34.25
Trend Micro, Inc.	$67.85

IMPORTANT DISCLOSURES

This report is available in electronic form to registered users via R*Docs™ at https://williamblairlibrary.bluematrix.com or www.williamblair.com.

Please contact us at +1 800 621 0687 or consult https://www.williamblair.com/equity-research/coverage for all disclosures.

Jason Ader, Jake Roberge, Jonathan Ho, Arjun Bhatia and Sebastien Naji attests that 1) all of the views expressed in this research report accurately reflect his/her personal views about any and all of the securities and companies covered by this report, and 2) no part of his/her compensation was, is, or will be related, directly or indirectly, to the specific recommendations or views expressed by him/her in this report. We seek to update our research as appropriate. Other than certain periodical industry reports, the majority of reports are published at irregular intervals as deemed appropriate by the research analyst.

DOW JONES: 44828.50
S&P 500: 6279.35
NASDAQ: 20601.10

Additional information is available upon request.

Current Rating Distribution (as of July 7, 2025):

Coverage Universe	Percent	Inv. Banking Relationships *	Percent
Outperform (Buy)	72	Outperform (Buy)	11
Market Perform (Hold)	28	Market Perform (Hold)	2
Underperform (Sell)	1	Underperform (Sell)	0

*Percentage of companies in each rating category that are investment banking clients, defined as companies for which William Blair has received compensation for investment banking services within the past 12 months.

The compensation of the research analyst is based on a variety of factors, including performance of his or her stock recommendations; contributions to all of the firm's departments, including asset management, corporate finance, institutional sales, and retail brokerage; firm profitability; and competitive factors.

OTHER IMPORTANT DISCLOSURES

Stock ratings and valuation methodologies: William Blair & Company, L.L.C. uses a three-point system to rate stocks. Individual ratings reflect the expected performance of the stock relative to the broader market (generally the S&P 500, unless otherwise indicated) over the next 12 months. The assessment of expected performance is a function of near-, intermediate-, and long-term company fundamentals, industry outlook, confidence in earnings estimates, valuation (and our valuation methodology), and other factors. Outperform (O) - stock expected to outperform the broader market over the next 12 months; Market Perform (M) - stock expected to perform approximately in line with the broader market over the next 12 months; Underperform (U) - stock expected to underperform the broader market over the next 12 months; not rated (NR) - the stock is not currently rated. The valuation methodologies include (but are not limited to) price-to-earnings multiple (P/E), relative P/E (compared with the relevant market), P/E-to-growth-rate (PEG) ratio, market capitalization/revenue multiple, enterprise value/EBITDA ratio, discounted cash flow, and others. Stock ratings and valuation methodologies should not be used or relied upon as investment advice. Past performance is not necessarily a guide to future performance.

The ratings and valuation methodologies reflect the opinion of the individual analyst and are subject to change at any time.

Our salespeople, traders, and other professionals may provide oral or written market commentary, short-term trade ideas, or trading strategies-to our clients, prospective clients, and our trading desks-that are contrary to opinions expressed in this research report. Certain outstanding research reports may contain discussions or investment opinions relating to securities, financial instruments and/or issuers that are no longer current. Investing in securities involves risks. This report does not contain all the material information necessary for an investment decision. Always refer to the most recent report on a company or issuer. Our asset management and trading desks may make investment decisions that are inconsistent with recommendations or views expressed in this report. We will from time to time have long or short positions in, act as principal in, and buy or sell the securities referred to in this report. Our research is disseminated primarily electronically, and in some instances in printed form. Research is simultaneously available to all clients. This research report is for our clients only. No part of this material may be copied or duplicated in any form by any means or redistributed without the prior written consent of William Blair & Company, L.L.C.

This is not in any sense an offer or solicitation for the purchase or sale of a security or financial instrument.

The factual statements herein have been taken from sources we believe to be reliable, but such statements are made without any representation as to accuracy or completeness or otherwise, except with respect to any disclosures relative to William Blair or its research analysts. Opinions expressed are our own unless otherwise stated and are subject to change without notice. Prices shown are approximate.

This report or any portion hereof may not be copied, reprinted, sold, or redistributed or disclosed by the recipient to any third party, by content scraping or extraction, automated processing, or any other form or means, without the prior written consent of William Blair. Any unauthorized use is prohibited.

If the recipient received this research report pursuant to terms of service for, or a contract with William Blair for, the provision of research services for a separate fee, and in connection with the delivery of such research services we may be deemed to be acting as an investment adviser, then such investment adviser status relates, if at all, only to the recipient with whom we have contracted directly and does not extend beyond the delivery of this report (unless otherwise agreed specifically in writing). If such recipient uses these research services in connection with the sale or purchase of a security referred to herein, William Blair may act as principal for our own account or as riskless principal or agent for another party. William Blair is and continues to act solely as a broker-dealer in connection with the execution of any transactions, including transactions in any securities referred to herein.

For important disclosures, please visit our website at williamblair.com.

This material is distributed in the United Kingdom and the European Economic Area (EEA) by William Blair International, Ltd., authorised and regulated by the Financial Conduct Authority (FCA). William Blair International, Limited is a limited liability company registered in England and Wales with company number 03619027. This material is only directed and issued to persons regarded as Professional investors or equivalent in their home jurisdiction, or persons falling within articles 19 (5), 38, 47, and 49 of the Financial Services and Markets Act of 2000 (Financial Promotion) Order 2005 (all such persons being referred to as "relevant persons"). This document must not be acted on or relied on by persons who are not "relevant persons."

This report is being furnished in Brazil on a confidential basis and is addressed to the addressee personally, and for its sole benefit. This does not constitute an offer or solicitation for the purchase or sale of a security by any means that would constitute a public offering in Brazil under the regulations of the Brazilian Securities and Exchange Commission (*Comissão de Valores Mobiliários*) or an unauthorized distribution under Brazilian laws and regulations. The securities are authorized for trading on non-Brazilian securities markets, and this report and all the information herein is intended solely for professional investors (as defined by the applicable Brazilian regulation) who may only acquire these securities through a non-Brazilian account, with settlement outside Brazil in a non-Brazilian currency.

Any statements in this report that are attributable to IDC Research, Inc. ("IDC") represent William Blair's interpretation of data, research opinion or viewpoints published as part of a syndicated subscription service by IDC and have not been reviewed by IDC. IDC's research is current as of the date IDC published it, not the date that William Blair's reports are published. Further, IDC's research contains IDC's opinion, not representations of fact, and are subject to change without notice.

William Blair & Company, L.L.C. licenses and applies the SASB Materiality Map® and SICSTM in our work.