

FEBRUARY 2023

Building a Cost Effective and Operationally Efficient Application Security Strategy

Melinda Marks, Senior Analyst

Abstract: Security teams are under pressure to support modern application development objectives to meet business needs for increased productivity and innovation. As security teams face resource constraints, including budget and staffing challenges, an efficient approach is required to keep pace with the speed and volume of releases and the complexity of the attack surface of cloud-native applications and infrastructure.

The use of multiple siloed security products takes time and effort to deploy and manage while also complicating triaging findings and alerts. Organizations need an operationally efficient solution built to scale with the speed of cloud-native software development. An integrated solution will orchestrate key security processes throughout the software development lifecycle (SDLC) to help developers produce secure code and efficiently remediate issues. At the same time, the solution should connect and analyze data to produce risk-based insights to drive the actions that have the highest impact on reducing security risk.

Security Challenges Keeping Pace with Modern Software Development

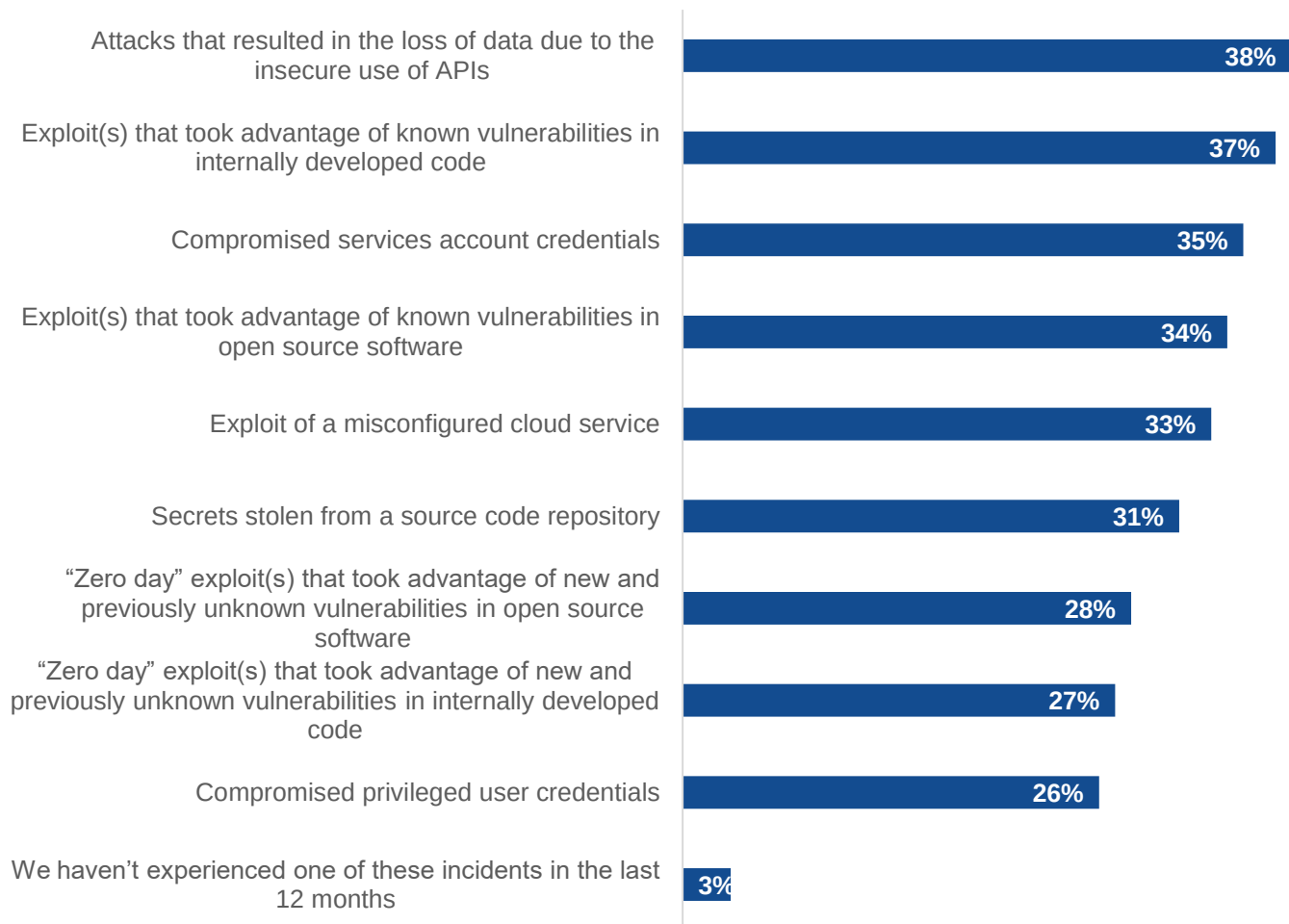
Organizations are increasingly employing cloud-native development for faster development cycles with continuous integration and continuous deployment (CI/CD). By leveraging cloud services, developers are empowered to provision their own infrastructure—dynamically configuring cloud resources—and build their applications using a technology stack comprised of ephemeral infrastructure and resources that can be dynamically spun up or spun down. Developers are also utilizing templates and open source software (OSS) to save time. While these modernized software development processes help businesses optimize productivity and gain a competitive advantage, security teams need to scale to ensure they can support faster release cycles and growing teams.

Research from TechTarget's Enterprise Strategy Group shows that security teams are challenged keeping up with faster development cycles due to the increased speed and volume of releases, introducing a higher risk for mistakes and resulting in security issues. Despite having security tools and products in place, these teams are often unable to identify and remediate security issues pre-deployment, resulting in a wide range of problematic security incidents (see Figure 1).¹

¹ Source: Enterprise Strategy Group Research Report, [Walking the Line: GitOps and Shift Left Security](#), November 2022.

Figure 1. Cybersecurity Incidents with Cloud-Native Applications

Which of the following cybersecurity incidents, if any, has your organization experienced in the last 12 months related specifically to internally developed cloud-native applications? (Percent of respondents, N=350, multiple responses accepted)

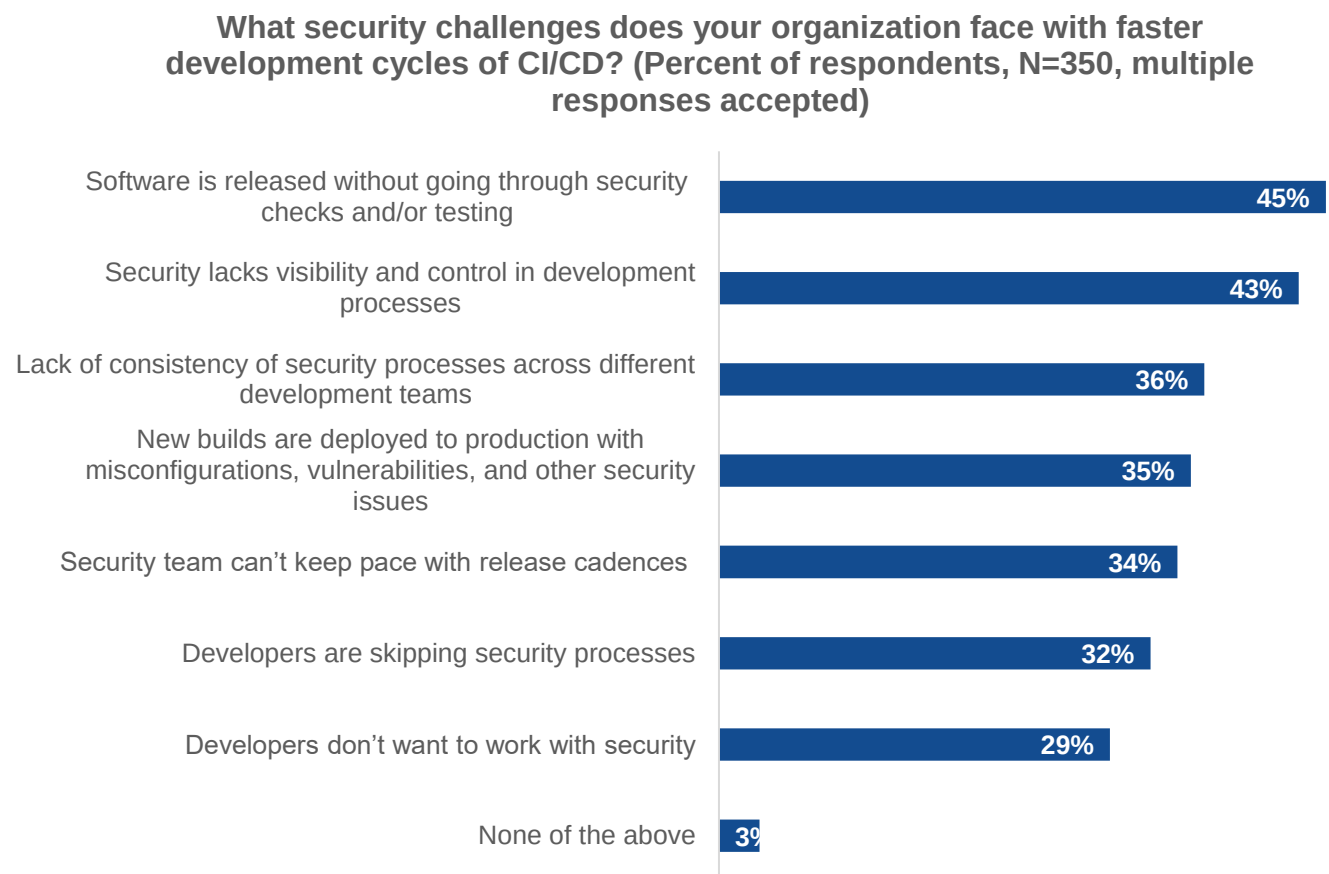


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Organizations have tried to address these challenges by implementing multiple security solutions across the SDLC and across different elements of the tech stack to identify and correct security issues. For example, project teams may be using Infrastructure-as-Code (IaC) security testing; software composition analysis (SCA) to scan OSS; vulnerability scanning for proprietary code; image scanning for virtual machines, containers, or serverless functions; and posture management and monitoring solutions in runtime.

Having multiple security products and tools in place can still result in security issues. Enterprise Strategy Group research highlights the challenges organizations are facing with faster development cycles of CI/CD, with 43% of respondents reporting that their security teams lack the visibility and control needed to ensure the appropriate tools are used everywhere they are needed (see Figure 2).²

² Ibid.

Figure 2. Security Challenges from Faster Development Cycles

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Enterprise Strategy Group research further shows that the use of multiple siloed security tools is difficult to implement and manage (see Figure 3).³ Many of the challenges around the current application security solutions relate to how much friction they introduce to development processes. Developers want to focus on building their applications; they don't want to have to become security experts or use separate security tools. But developers do want to produce higher quality secure code, and to do so, they need to understand how to best use their time efficiently. Tools that can help developers prioritize changes will make a difference.

³ Source: Enterprise Strategy Group Research Report, [Securing Modern Application Development Environments](#), December 2020.

Figure 3. Top Five Challenges Experienced with Current Application Security Tools

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Building the Most Efficient Program to Stay Ahead of Threats

To effectively manage security risk, organizations need an efficient, cost-effective solution that works across the SDLC without disrupting development processes. Such an approach provides context as issues are found to determine what needs attention and in what order to protect applications from attacks. While it is much harder to identify and track resources in cloud environments due to the nature of elastic infrastructure and services, there are opportunities for security solutions to work with modern development workflows to efficiently manage risk.

The first step is shifting security left to enable developers to identify and mitigate security issues as early in the development lifecycle as possible. A platform that orchestrates security testing tools, utilizing automated testing and policy enforcement, enables developers to efficiently identify and fix security issues, reducing the chance of deploying insecure code to the cloud.

Traditional approaches have leveraged separate siloed tools with limited visibility and context across the SDLC, making alert prioritization a huge challenge. A modernized approach enables risk-based prioritization to efficiently drive the actions needed that have the highest impact on reducing risk. Correlating how an application is built to how it will run in the cloud, including expected behaviors, networks and communications with resources, and user behavior, provides context to understand what needs attention and what can be ignored.

This makes it easier for teams to address high priority issues without the need for time-intensive manual triage or analysis. It's costly and inefficient to use multiple security tools, even if they are less expensive or open source tools, as they generate siloed alerts without context on how to prioritize or fix the issues.

A modern solution should utilize capabilities and telemetry from multiple sources, providing the context and information to mitigate security issues in time to prevent security incidents. The solution should prioritize alerts

based on context and business risk, rather than according to generic industry scores or vendor rankings. Solutions can also help speed remediation by working within established development workflows and providing auto-remediation workflows to save time across teams.

Reducing Costs

By building a modernized approach to application security that optimizes efficiency, organizations can ensure the cost-effectiveness of their programs. The top cost factors to consider include:

- **Licensing costs.** Avoid overpriced, complex products with unneeded or redundant features or capabilities or that have multiple added fees.
- **Operational costs.** Each product takes time to deploy and manage. Evaluate each product's usability, including features and capabilities that eliminate tedious manual processes, such as correlating data and results across tools. It is also important to understand that, while some free or low-cost solutions, including OSS security tools, may have lower upfront costs, customization requirements may impact developer velocity.
- **Time savings.** It is also important to consider staff time savings. An integrated solution will help developers more efficiently find and fix code issues. As a result, fewer defects are deployed into production, resulting in fewer incidents and less triage work sorting through alerts. Faster remediation can also eliminate manual work associated with determining each instance needing a patch.

Introducing Cyscale

Cyscale provides a modern approach that enables organizations to effectively secure their cloud-native applications with cost-efficient utilization of tooling and staff across the SDLC. It provides:

- **A single unified software supply chain security platform**, consolidating SAST, SCA, container scanning, IaC scanning, pipeline security and governance, code tampering, secret scanning, and code leak detection.
- **Complete visibility** of application security risks with rapid deployment and agentless integrations.
- **Alert prioritization** to optimize remediation based on “code-to-cloud” correlation from building the application to how it runs in the cloud.
- **Integration with developer workflows** to incorporate security processes into development while giving security teams visibility and control to reduce security risk.

Cyscale enables security teams to successfully enable digital transformation with a cost-effective and operationally efficient program delivering:

- High efficiency risk mitigation.
- Tool consolidation and cost reduction.
- Operational efficiency and business acceleration.

Conclusion

In today's application-driven economy, organizations rely on the speed of modern software development to optimize productivity, but security teams need to keep up, even if budgets are tight. Security is more important than ever, and security teams need a cost-effective, operationally efficient solution to support cloud-native application development objectives. A security solution that supports the fast pace and volume of releases, the organization's development processes, and the full technology stack, including OSS, while also integrating with CI tools, is required.

Organizations can employ a solution like Cycode to meet the demands of modern software development. Cycode ensures essential security processes are orchestrated across the SDLC, while helping security teams and developers collaborate to mitigate security risks. By optimizing efficiency in their application security programs, organizations can realize cost savings and greater efficiency by helping their security teams make the best use of their staff and resources, while ensuring that their applications are secure.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at contact@esg-global.com.

About Enterprise Strategy Group

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community. © TechTarget 2023.

 contact@esg-global.com

 www.esg-global.com