ESG a division of TechTarget Enterprise Strategy Group | Getting to the bigger truth.™

ESG SHOWCASE

# Scaling Security for Modern Software Development Using Application Security Operations

**Date:** June 2022 **Author:** Melinda Marks, Senior Analyst

**ABSTRACT:** As organizations adopt modern software development processes to increase innovation and productivity with continuous releases and updates for customers, security is more important than ever but harder to ensure. Security teams need a platform that incorporates application security operations within development. This enables them to scale security with the speed of modern software development by enabling them to centrally manage security risk, rolling out tools and processes for development. By integrating application security operations into development, security teams can efficiently manage risk and meet compliance regulations even as development scales to meet business demands and competitive pressures.

## The Challenge of Scaling Security with Modern Software Development

Organizations are adopting modern software development processes and leveraging cloud services to better collaborate and speed up release cycles. As development teams grow and there are more frequent software releases, there is a higher chance for mistakes as the teams dynamically configure their cloud resources. The complexity of interconnected components and exposure on the internet increases the attack surface.

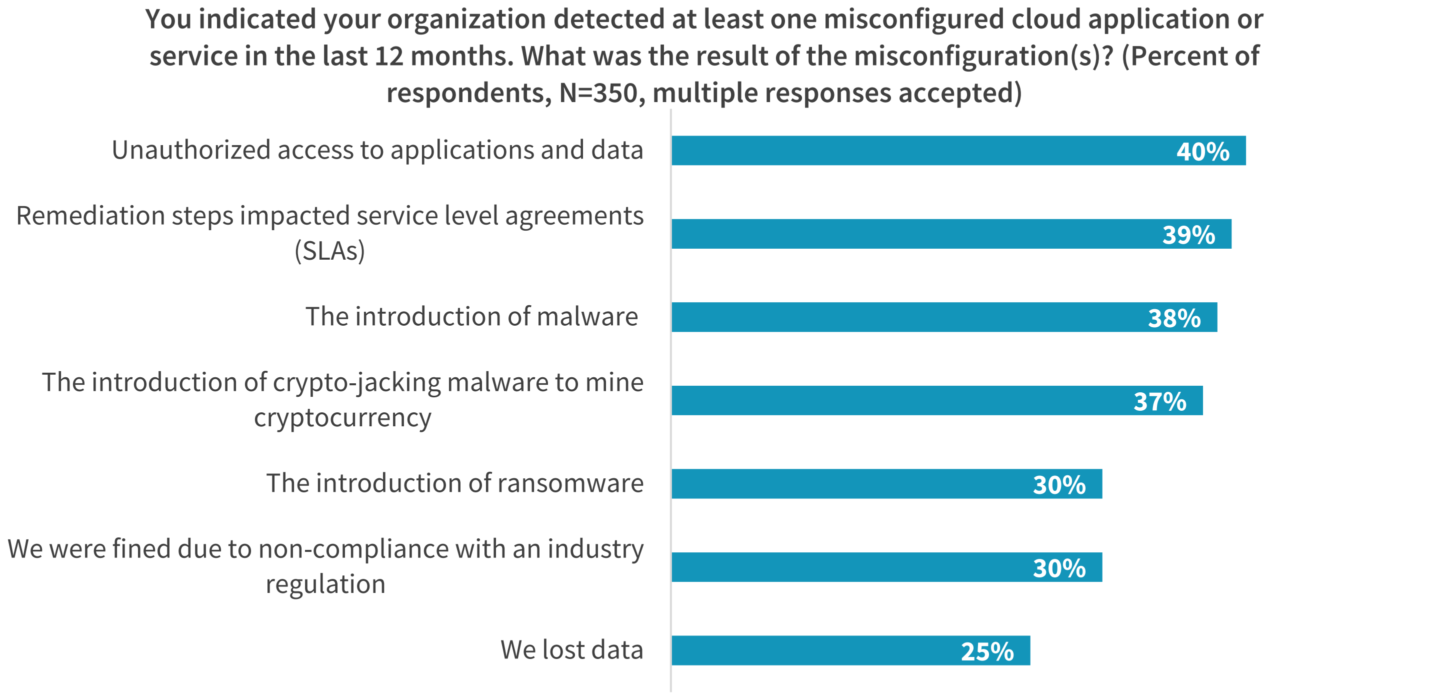
Instead of waiting for other teams to provision servers or infrastructure, developers are now empowered to provision their own infrastructure using scripts and templates with infrastructure as code (IaC), and they use microservices architectures to create their applications in virtual machines, containers, or serverless functions that can be deployed to the cloud.

Forty three percent of surveyed cybersecurity professionals previously reported that half or more of their code base is pulled from open source,[1] which likely saves developers precious time. However, while open source software (OSS) may be high quality and is often maintained by well-established vendors, it is still risky to pull code from third parties and templates. It increases the chance to propagate any code flaws, and attackers will target vulnerabilities in commonly used code.

With faster release cycles and growing development teams, there is a high chance of security mistakes, and it is difficult to apply consistent security metrics, processes, and tools across teams. ESG research shows that organizations have suffered losses, including losing customer confidence from preventable security mistakes/misconfigurations ranging from unauthorized access to applications and data, to introduction of ransomware, to compliance fines, to lost data (see Figure 1).[2]

[1] Source: ESG Survey Results, *Modern Application Development Security*, November 2020.
[2] Source: ESG Research Report, *The Maturation of Cloud-native Security*, May 2021.

## Figure 1. Results from Misconfigurations

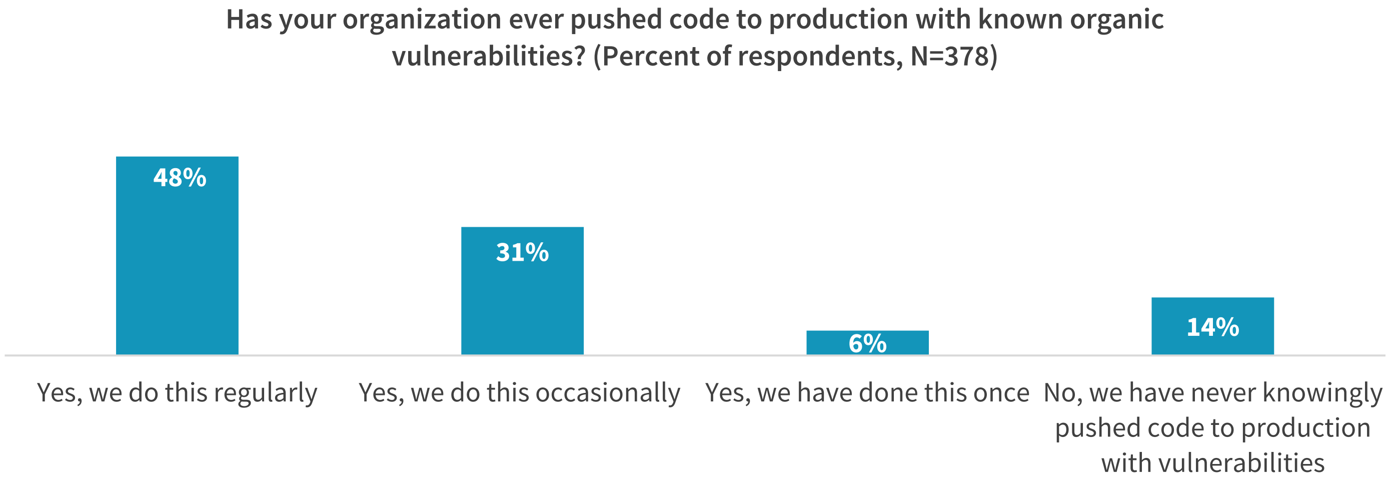


*Source: ESG, a division of TechTarget, Inc.*

Waiting for the security team to check code or to insert processes works against developer workflows, slowing down the software development process and the delivery of software. It also causes friction between teams if development has to wait for security approvals.

As organizations focus on product development with faster release cycles, security teams are vastly outnumbered, so security is sacrificed to meet aggressive release cycles. ESG research shows a high percentage of developers regularly pushing vulnerable code to meet product deadlines (see Figure 2).[3]

## Figure 2. Developers Pushing Vulnerable Code



*Source: ESG, a division of TechTarget, Inc.*

[3] Source: ESG Survey Results, *Modern Application Development Security*, November 2020.

So, we know that security is not keeping up with the speed of software development. With so many incidents resulting from simple misconfigurations, organizations realize that they need to find a way to scale security with rapid development cycles.

## The Need for Application Security Operations in Development

Modern software development has shifted operations left with DevOps, where developers are empowered to provision their own infrastructure in the cloud. But security and security operations have not shifted left and cannot keep up with the pace of development.

Modern software development processes leveraging cloud services enable development to move quickly without the help from other groups, but developers need the right tools in place to empower them to secure their own code without having to become security experts. At the same time, security needs visibility and control to effectively manage security risk and meet compliance requirements.

Shifting application security operations left to developers and incorporating the right security tools and processes in development, including policies and testing procedures, is the only way that security can keep up with the pace of modern software development. It makes it easier for developers to test and secure their own code without disruption; they can work more efficiently without having to interact with the security team.

This fosters a culture of secure development with both teams working efficiently. This modern approach empowers developers to build, test, and deliver secure, high-quality code that meets functional, performance, and security requirements, from design to build to test and deployment, while security gains visibility and control.

## Scaling Your Security Team to Support Rapid Development

Building security into development processes enables organizations to better utilize their security teams. Instead of having security identifying and fixing issues, the security team's role moves to laying the groundwork, defining processes, and being mentors for developers to secure their own code.

### The Importance of Automation

The key to scaling is having a security platform that can reduce manual, tedious tasks. While organizations typically use multiple security tools to test and monitor their applications, the tools generate too much data for security teams to sift through, and developers don't need more alerts on coding issues needing to be fixed.

Organizations need a platform that can pull information from various sources to provide context and automate critical application security workflows for faster actions and decisions to efficiently mitigate security risk as development scales.

Security can set up the automated security processes throughout the software development lifecycle (SDLC), optimized for each stage of the process, staying focused on deep alignment within each stage of design, build, test and deploy. By automating processes to occur within development, security teams no longer have to manually go through security results and manage remediation. Instead, developers get the information they need to produce secure code.

This includes codifying security rules as guardrails in the development process to prevent vulnerabilities. For example, setting policies ensures that databases are not exposed and that S3 buckets aren't open.

The security team should partner with developers to help them use the tools that work best for them in their workflows so they can quickly and efficiently find and fix security issues. This reduces the chance for security issues to be deployed in production, while also making it easier to respond to any issues found in runtime.

A platform approach gives the security team a centralized view to manage security posture to get a picture of assets, security risk, mitigation status, and compliance. Security champion or coaching programs can also help scale the impact of the security team, building trust and collaboration with the development team.

## Introducing ArmorCode

ArmorCode provides an Application Security Operations (AppSecOps) platform to operationalize security tools and processes in development, enabling organizations to scale application security for CI/CD in both cloud-native and traditional deployment environments. It integrates the process of identifying, prioritizing, remediating, and preventing security issues with modern developer workflows.

ArmorCode facilitates secure development by:

- Providing a unified view for managing application security posture, centralizing findings and remediations from more than 100 AppSec, cloud, and infrastructure security tools (including SAST, DAST, SCA, bug bounties, pen testing, CSPM, container security, and more) as well as development and operations systems (such as Jira, Slack, GitHub).
- Normalizing, deduplicating, and correlating findings to provide actionable insights that focus efforts and reduce remediation time for the most important vulnerabilities.
- Automating manual tasks and critical AppSec workflows to meet SLAs and unify security, development, and operations teams.
- Elevating tribal knowledge within the development organization, enabling developers to fix issues fast and effectively without specialized training and skills.

## The Bigger Truth

As organizations continue to embrace modern software development, security can only keep up by moving security operations left to development so that security teams can scale to effectively manage risk. Organizations can look to the ArmorCode AppSecOps platform to provide a centralized view of security posture along with a way to operationalize security tools and processes into development within their workflows. This enables organizations to scale their application security program to meet the accelerated delivery schedules for modern software development.

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.

a division of TechTarget

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.

www.esg-global.com contact@esg-global.com 508.482.0188