Enterprise Strategy Group | Getting to the bigger truth.™

ESG WHITE PAPER

Automated Application Security Testing for Faster Development

Automated Application Security Testing that Increases Efficiency across the Software Development Lifecycle

By Melinda Marks, ESG Senior Analyst

September 2022

Invicti

This ESG White Paper was commissioned by Invicti and is distributed under license from TechTarget, Inc.

Contents

Executive Summary

In the first half of 2022, ESG interviewed Invicti customers to learn about how they are adapting their application security strategies as they undergo business transformation, moving workloads to the cloud for faster development cycles. These interviews with security leaders covered their top challenges, the tools they have in place, and their strategies moving forward.

Based on these interviews, ESG concludes:

- Organizations are undergoing digital transformation, modernizing application development processes to speed up release cycles and innovation and to better serve customers and compete. However, with the speed and volume of releases, traditional application security solutions don't work with modern software development because they are disruptive and produce extra work with too many alerts, slowing development down.
- Security teams are looking for the right security solutions that fit into modern software development workflows to incorporate the right security tools and processes throughout the software development lifecycle. This helps developers work more efficiently in their own tools and workflows to improve the quality and security of their code while helping security teams scale even as the number of releases exponentially grows.
- Invicti is a trusted vendor for building security into development processes by providing accurate, comprehensive security testing with complete coverage, helping security teams bake security into everything from application architecture design, test, deployment, and management.

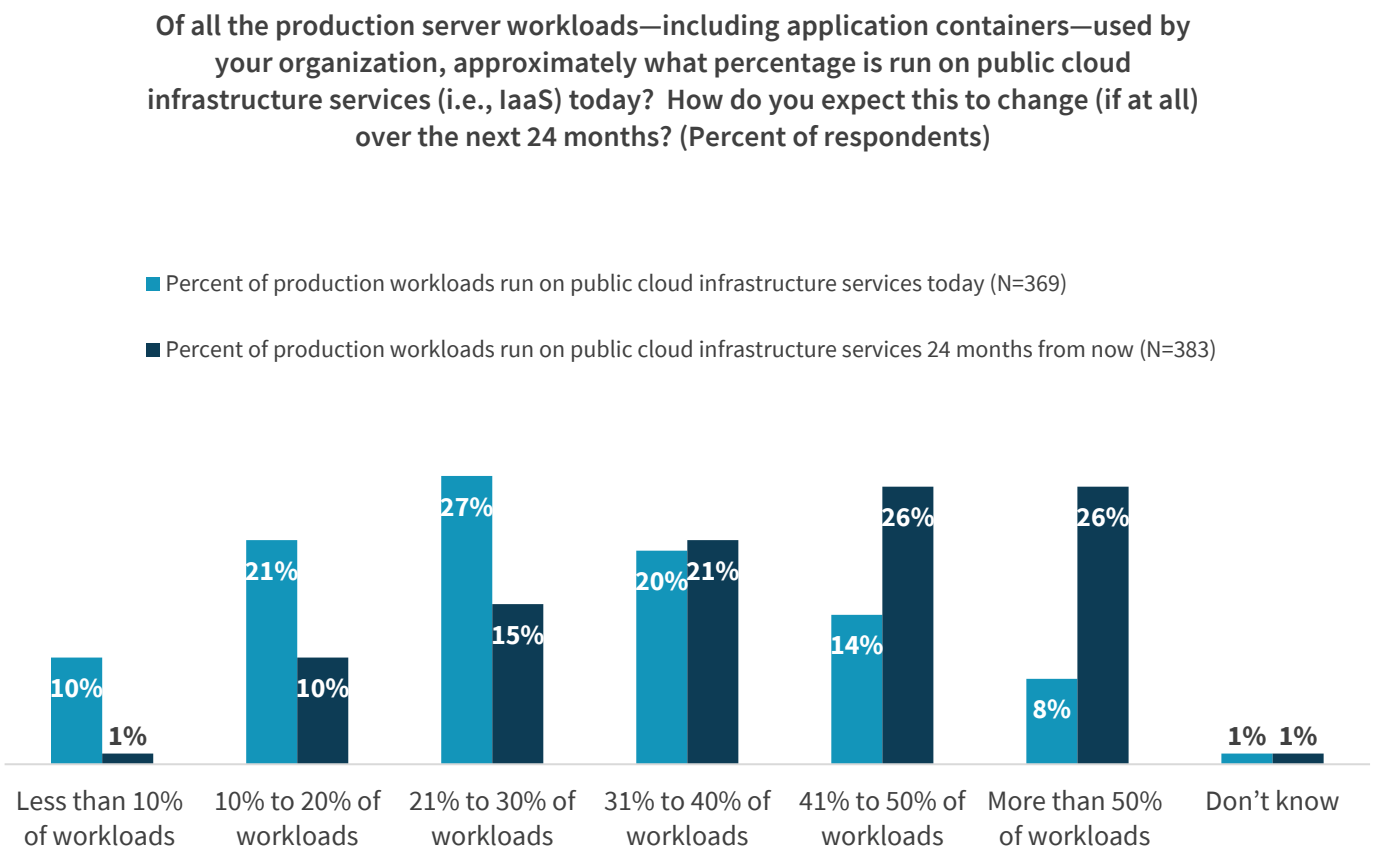
Security teams want to enable their organizations to embrace newer technologies for faster product releases and innovation cycles instead of holding them back with security processes or security risk. Invicti is helping security teams scale by automating key security processes within development lifecycles while giving security teams the visibility and control they need to reduce risk effectively.

The Challenge Securing Cloud-native Applications

ESG research shows that 9 out of 10 organizations are under pressure to move faster than three years ago for their teams to deploy applications, infrastructure, and services.[1] They are increasingly moving production workloads to the cloud (see Figure 1)[2] for faster release cycles and to make their services and applications available for their customers, partners, and employees.

[1] Source: ESG Research Report, *Data Infrastructure Trends*, November 2021.
[2] Source: ESG Research Report, *The Maturation of Cloud-native Security*, May 2021.

Figure 1. The Shift of Production Workloads to Public Clouds



Source: ESG, a division of TechTarget, Inc.

As cloud adoption enables continuous integration and continuous deployment (CI/CD) by leveraging microservice application architectures that can be packaged and released to the cloud, the computing environments are dynamic and ephemeral, bringing new challenges to securing the applications.

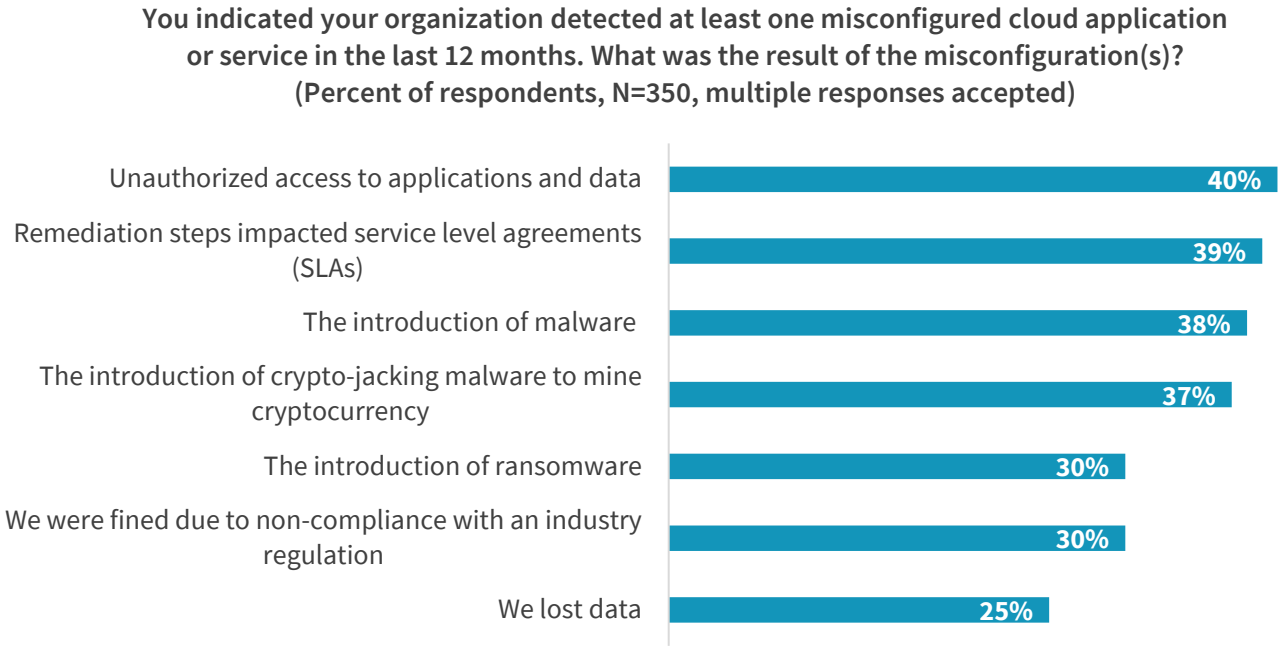
Security teams are under pressure to keep up; while modern software development enables them to do more business and transactions, security is more important than ever to protect company and customer data.

But there is a gap between developers who are more self-sufficient in deploying infrastructure and their applications and security teams that need to ensure that the products have undergone security testing. It's also important to drive efficiency to help developers fix discovered issues—ideally, early in development before the applications are deployed, but also during runtime if an issue is detected. 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 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 2).[3]

[3] Ibid.

Figure 2. Results from Misconfigurations



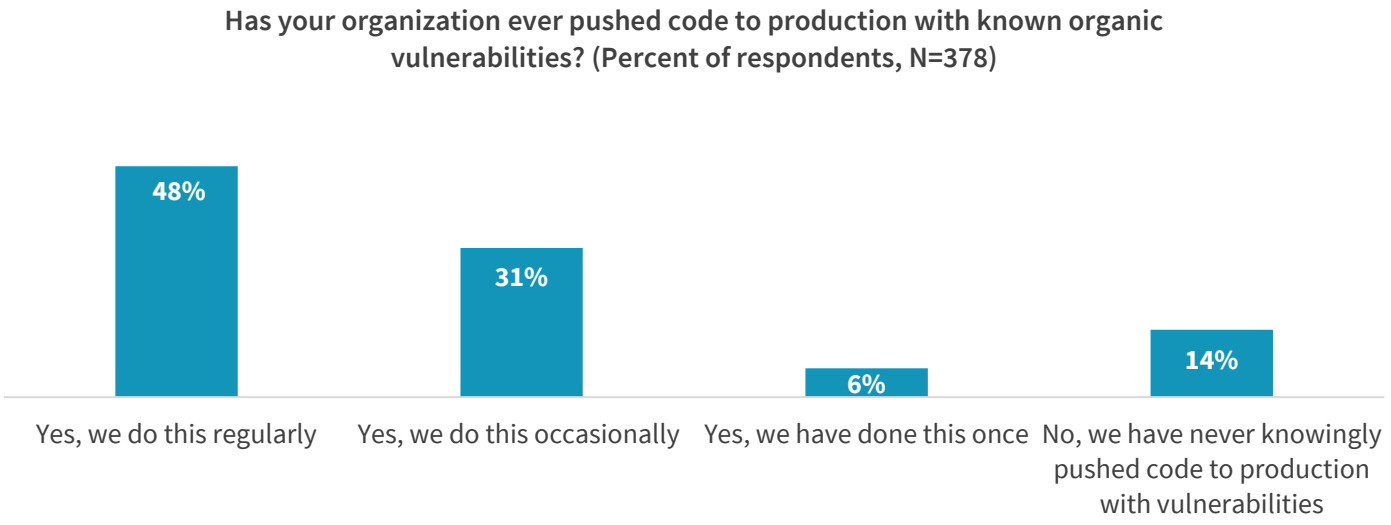
Source: ESG, a division of TechTarget, Inc.

Waiting for the security team to check code or to insert processes works against developer workflows, slowing processes down. It's also problematic because it causes bottlenecks; there is friction if development has to wait for security testing or approvals. The security teams are also vastly outnumbered by the developers they support, compounded by the challenge of finding cloud security expertise. ESG research shows the biggest gap in cybersecurity skills is in cloud security.[4]

The result of this skills shortage is that security is often sacrificed to meet aggressive release cycles. ESG research shows a high percentage of developers regularly pushing vulnerable code to meet product deadlines (see Figure 3).[5]

[4] Source: ESG Research Report, *The Life and Times of Cybersecurity Professionals 2021 Volume V*, July 2021.
[5] Source: ESG Survey Results, *Modern Application Development Security*, November 2020.

Figure 3. Developers Pushing Vulnerable Code



Source: ESG, a division of TechTarget, Inc.

Organizations need to find the right tools so their teams can scale with rapid development. One Invicti customer, the Associate Director for Security Testing and Assurance for a leading global travel and vacation company, said, "Our teams are skilled in security but not in secure code development skills or development, so we look for the right tools to fill in the gap."

The Need for Complete Coverage

Organizations need to find ways to scale their security teams to keep up with the rapid pace of modern software development. For them, it is a matter of time and resource use because of the importance of the applications they need to protect.

Invicti customers described that they can't use methods that are too expensive or time-intensive; with these restrictions, they would only apply those methods to business-critical applications.

"We have a variety of applications through acquisitions posted in AWS, Azure, and on-premises that need coverage; we need to support the business with plans to move to the cloud for agility and flexibility."

– Associate Director for Security Testing and Assurance, leading global travel and vacations company

With the move to the cloud to serve their customers, organizations need a cost-effective, easy-to-use solution that gives them protection and coverage for all of their applications, not just certain business-critical applications due to cost issues. Otherwise, simple coding mistakes can leave them vulnerable to attacks that could compromise company or customer data.

For the global travel and vacations company, it was important to enable consistent, secure processes for its applications and acquired companies.

> **"We need to ensure that everything we do is done safely."**
>
> – CISO, leading television network company

Ensuring consistent, secure processes is also important for a television service network serving 26 million viewers. The television network's CISO described the criticality of protecting the information collected online, particularly the personally identifiable information (PII) of viewers and staff, and protecting its own company data and intellectual property.

Working in Developer Workflows

In order to scale security for cloud-native applications, organizations need the right tools in place to ensure that teams can work efficiently, instead of getting bogged down in tedious, manual processes.

Invicti customers described how they are incorporating security into DevOps processes to catch and fix coding issues before they are deployed. By automating security testing at build time and setting policies, they can reduce their chance of releasing faulty code.

They are also monitoring for issues at runtime to detect any security issues. With an integrated solution, they can deliver alerts directly to the developers within their workflows to shorten the feedback loops and reduce work across teams. The Invicti customers described the importance of not forcing developers to use separate security tools; the developers need to receive the notifications within their own tools for bug fixes so they can continue to work in their normal integrated development environments (IDEs) and workflows.

> **"We can't get a group to do something fundamentally different than what they are doing every day. We have to ask them to do things in their own tools and workflows."**
>
> – Associate Director for Security Testing and Assurance, leading global travel and vacations company

> **"We don't want to have to run scans at the end of a project and find the problems and have to rebuild everything; it's not efficient."**
>
> – CISO, leading television network company

With accurate testing and monitoring in place, Invicti provides Proof-Based Scanning, reporting only vulnerabilities that need to be fixed, saving developers from wasting their time on false positives or issues that don't matter.

Invicti customers also described how they are setting policies as guardrails to set up mechanisms to prevent developers from being able to push code with misconfigurations. They described how Invicti helps ensure that their staff can work efficiently instead of getting bogged down in tedious, manual processes for setting up the policies or running testing tools.

Turning Security into Enablers Instead of Blockers

Although scaling security for the speed of modern software development has its challenges, security teams strive to enable the secure use of cloud-native technologies that speed development to help drive better business results.

Invicti customers described how having the right security tools and processes in place drives a culture to support faster development instead of blocking it.

This helps to build a partnership with development so they can work together, as opposed to developers feeling like security might slow them down.

"The culture the CISO and I strive for is that we're business enablers. The mission is not to say, 'You can't do that.' It's, 'What do we need to do to make sure it's secure?' Security is engaged so we make good decisions for the direction the business wants to take."

– Associate Director for Security Testing and Assurance, leading global travel and vacations company

Continuously Securing All Applications with Invicti

"Invicti keeps us on point and ensures that we can deliver projects on time and on budget."

– CISO, leading television network company

Invicti helps organizations continuously provide comprehensive testing for all of their applications instead of having to limit their coverage to high-priority applications. Before using Invicti, customers described feeling frustrated only being able to conduct testing on a limited number of business-critical applications because other security testing solutions were expensive. As the number of cloud-native production workloads continues to grow, customers wanted to provide complete and comprehensive coverage for all of their applications.

They also described the comprehensiveness of the solution. Invicti provides application discovery and visibility into the threat landscape while incorporating highly accurate security testing—including software composition analysis (SCA), dynamic application security testing (DAST), and interactive application security testing (IAST)—automated throughout the SDLC. Invicti's combination DAST scanner and IAST sensor crawls every corner of an application, helping teams discover their full attack surface and verify vulnerabilities. Using this paired with Invicti's Proof-Based Scanning weeds out false positives, helping teams cut back on time-wasting manual work.

"Security issues show up in their Jira queue, their Azure DevOps tickets, whatever they use, so they don't even care if it came from the security team. It's just another bug to fix. If we do that, it's successful. If we throw a PDF at them that says, 'Here's all the stuff that's wrong; go fix it,' we're not successful."

– Associate Director for Security Testing and Assurance, Leading Global Travel and Vacations Company

Invicti customers can run the tests upon code pushes, and they can also run scheduled scans to ensure that the applications are regularly tested. Information on any code issues is sent directly to developers within their CI/CD pipeline or ticketing system, providing them with the information needed to remediate their code so they can efficiently make the needed changes.

> **"(It) makes our lives a lot easier rather than getting to the end of a project, then running a vulnerability or penetration test, and realizing there are weaknesses, and then having to go back to redesign or redevelop that."**
>
> – CISO, leading television network company

For the global vacation company, developers can fix security issues as they would fix any bug in their normal development workflows, without context switching. The Invicti customers said this is much more effective than what they were doing before, which was generating security testing results and giving developers lists of issues that they needed to go fix.

For the television network, the CISO also described the effectiveness of regular, automated security testing throughout the software development process instead of only running tests right before the product was released. While this may have worked well for waterfall development processes, it doesn't work well with CI/CD processes in cloud-native environments, where finding flaws at the end of the process creates huge rework projects to rebuild their applications, setting them back. As mentioned earlier in the paper, developers are under pressure with their release deadlines, so security testing has often been too disruptive to developer workflows, with developers often deciding to just push the vulnerable application, causing risk to the business.

Invicti customers also described how the solution's accuracy saved developers from wasting their time fixing false positives. The global vacations company said it makes it easy for the developers to improve the code. "There are a lot less arguments from developers about fixing things. There is no more, 'Why do we need to do that?' It's also much better than having a manual process of giving a developer a PDF of things they need to fix when they are about to deploy their applications," said the associate director for security testing and assurance for the travel and vacations company.

> **"Once it's set up, it can free up 10-15 hours of time for each person, with automated scans and reports instead of taking time with manual tasks testing an application."**
>
> – Associate Director for Security Testing and Assurance, leading global travel and vacations company

Saving Time and Money

> **"By using Invicti products, we probably saved ourselves, in the first year alone, $180,000."**
>
> – CISO, leading television network company

The Invicti customers also reported measurable time and cost savings. For the global vacations company, anytime it acquires a company or needs to add a new website, it simply plugs in Invicti and automates security scans. The developers get notified about security issues, and they can fix them in their workflows. The security team gets visibility and reports of testing status so they can effectively manage their risk, with the ability to provide those reports to their executive leadership.

The television network also reported cost savings because it can work more efficiently with security integrated with developer workflows. Security teams no longer have to use external tools, hire consultants, and use penetration testing services.

The Bigger Truth

Organizations need a way to build comprehensive security testing into development processes to scale with the speed of modern software development. Invicti helps organizations secure their applications by providing comprehensive, automated security testing across the software development lifecycle and enabling developers to remediate issues within their workflows.

Customers use the Invicti platform to cost-effectively protect all of their applications instead of only applying more expensive security solutions to business-critical applications. Customers reported that Invicti provides accurate results to developers so they can fix issues in their workflows, saving them from wasting time on false positives and from having to find out problems later when they become big projects to fix.

The Invicti platform gives security teams the visibility and control to effectively manage security risk for modern software development, helping them scale by eliminating manual, tedious processes and reducing security incidents.

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