The Invicti™ AppSec Indicator

Fall 2021 Edition:
Security and the Innovation Imperative

Invicti

Table of Contents

Innovation is a strategic imperative for every business, government, and nonprofit.

It's the path to competitive advantage, improved customer experience, and delivery on even the loftiest of missions. Never has the pace of innovation been as rapid as it is at this moment, and this pace will only increase.

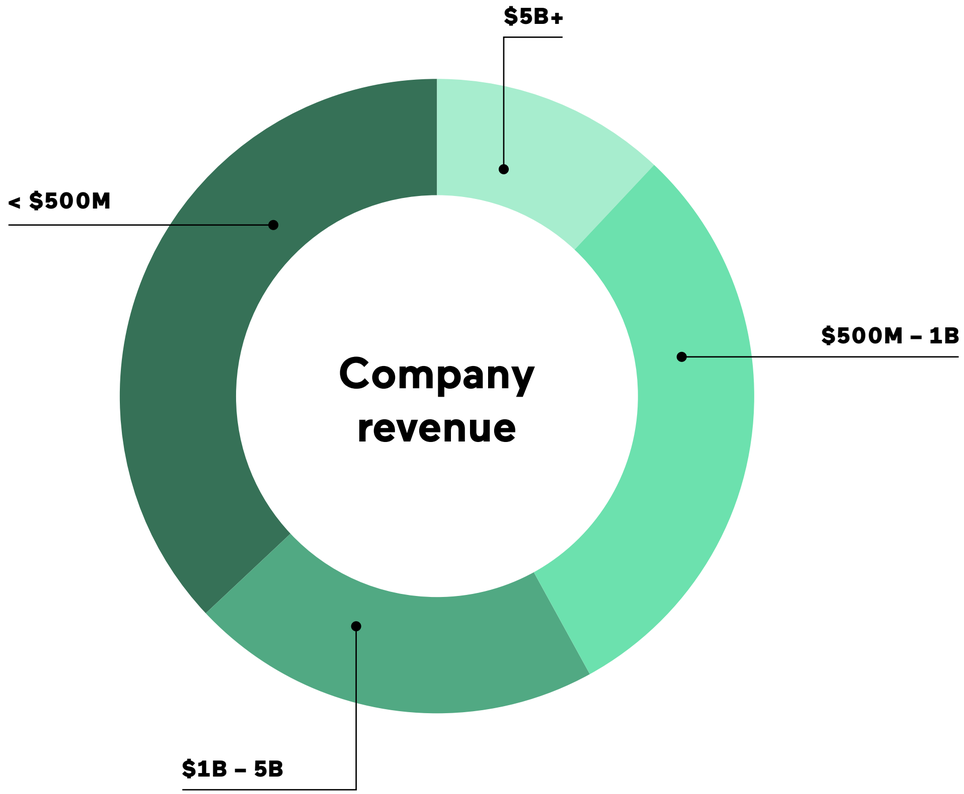
Software, and web applications specifically, are central to innovation. Organizations build them to improve service delivery, operational efficiency, and create entirely new categories of products that solve what's next.

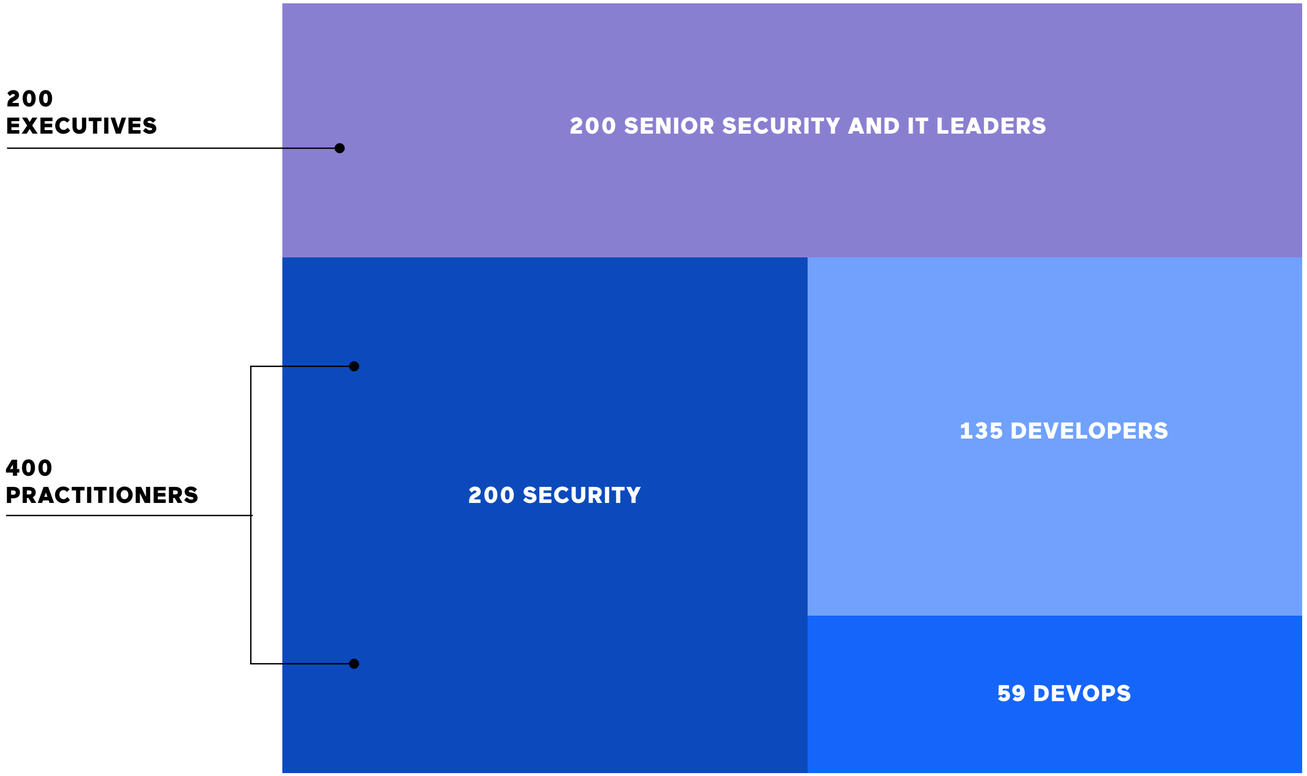
As innovations in web applications drive the world forward, new risks with serious consequences have emerged. Billions of web applications today represent a significant attack vector for malicious actors, who now use them nearly 40% of the time to gain access.[1] Complicating the situation are the massive shift to workforce virtualization, the breakneck migration to cloud, and ransomware payouts that fund continued research and advancements for cybercriminal organizations.

Those responsible for building and protecting these assets, and in turn, their leaders, have never had a harder job. To innovate with security built-in, they must collaborate deeply and use the most powerful tools available. ***And their leaders must prioritize application security, enroll in the challenges their teams face, and create the context for them to succeed.***

[1] *Verizon DBIR*

We wanted to examine how this challenge is playing out in the day-to-day reality of organizations.





We partnered with Wakefield Research to survey 600 individuals. Our sample spanned security, development and DevOps, and tapped both executives and hands-on-keyboard practitioners for their perspectives. We sought to uncover what is working well in their efforts to protect their organizations, what isn't — and where they see potential for things to get better.

We discovered encouraging trends and some continued challenges.

On the one hand, the rumors of developer-security animosity are greatly exaggerated, and seem to be continually improving. And developer and security teams are hungry to deepen their collaboration. Developers know security is a core attribute of quality code. Also encouraging is the fact that the organizations they work in are increasing their focus on web application security.

And yet. ***Integrating security into the Software Development Life Cycle (SDLC) is still work in progress,*** and active protection of deployed applications remains more aspiration than reality. Practitioners' experience on the ground doesn't always match what their leaders see. The "release fast or die" ethos is overshadowing security practices. Additionally, noise and false positives in many security tools are disrupting harmony and effectiveness among security and development. And these teams are stressed - leading to burnout, churn, and animosity that threaten to increase cyber risk.

What will the future hold? Organizations will continue to innovate because the best ones do - and must - to stay competitive. But when these organizations can't protect their customers, innovation can be value-destroying. Respondents have interesting and sometimes conflicting expectations about what holds promise, both to improve and further compromise security.

Leaders recognize that innovation shouldn't happen at the expense of security. That enhancements in their technology are only as good as their defense against an inevitable attack. And maybe we are moving toward a world where security will be viewed as an essential ingredient of innovation. Our current outlook is that it must.

Our cross-section of dev and security respondents spans 23 industries, including:

17%
MANUFACTURING

17%
TECHNOLOGY

11%
GOVERNMENT & EDUCATION

10%
RETAIL

9%
HEALTHCARE

7%
BANKING

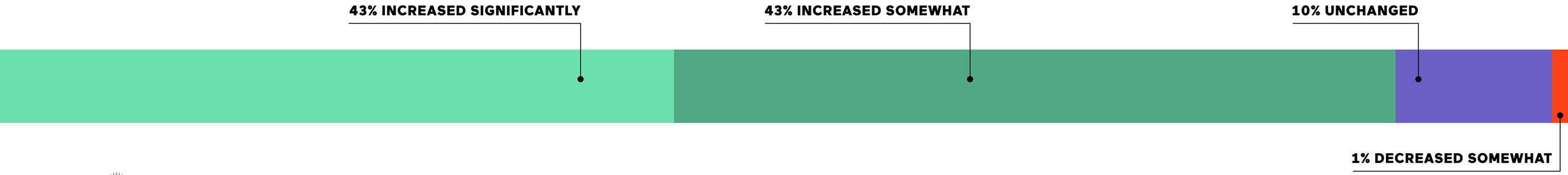
Application security is everyone's job now.

Organizations have brought web application security into sharper focus … but the benefits have not yet emerged.

Organizations know web application security is a must and are feeling the urgency. In the past 12 months alone, 89% increased their focus in the area, and no organizations significantly reduced their focus.

But web applications are not yet showing evidence that they are better-secured. Our Spring 2021 edition of the Invicti AppSec Indicator examined the prevalence of common vulnerabilities in 3500 web applications during 2020. The prevalence of medium-severity vulnerabilities held steady year over year at 63%, while high-severity vulnerabilities actually increased in prevalence from 26% to 27% from 2019-2020. This followed several years of consistent decline.

How, if at all, has your organization's focus on web application security changed over the past 12 months?



Fortunately, the rumors about Dev - Sec animosity have been greatly overstated.

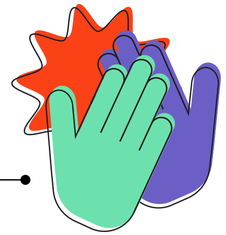
Good news and bad news. While 76% of respondents said they were "family" or "besties" with their counterparts, 24% describe the relationship between security and development as "frenemies" or even "strangers."

But security is less enthusiastic than development about the relationship:

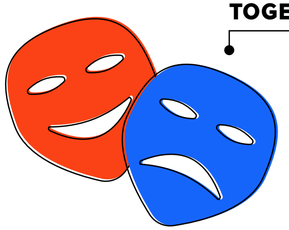
- 37% of security respondents said "family" vs. 55% of developers
- 9% of security said "strangers" vs. only 6% of developers

Which of the below best describes the relationship between the security team and the development team at your organization?

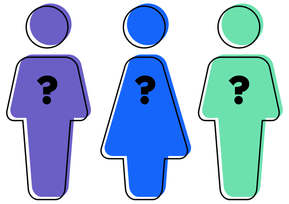
41%
FAMILY – THE TEAMS HAVE A SHARED PASSION FOR SECURITY AND WORK AS ONE TEAM



35%
BESTIES – THE TEAMS COLLABORATE OFTEN TO ADDRESS SECURITY ISSUES



17%
FRENEMIES – THE TEAMS WORK TOGETHER BECAUSE THERE IS NO CHOICE

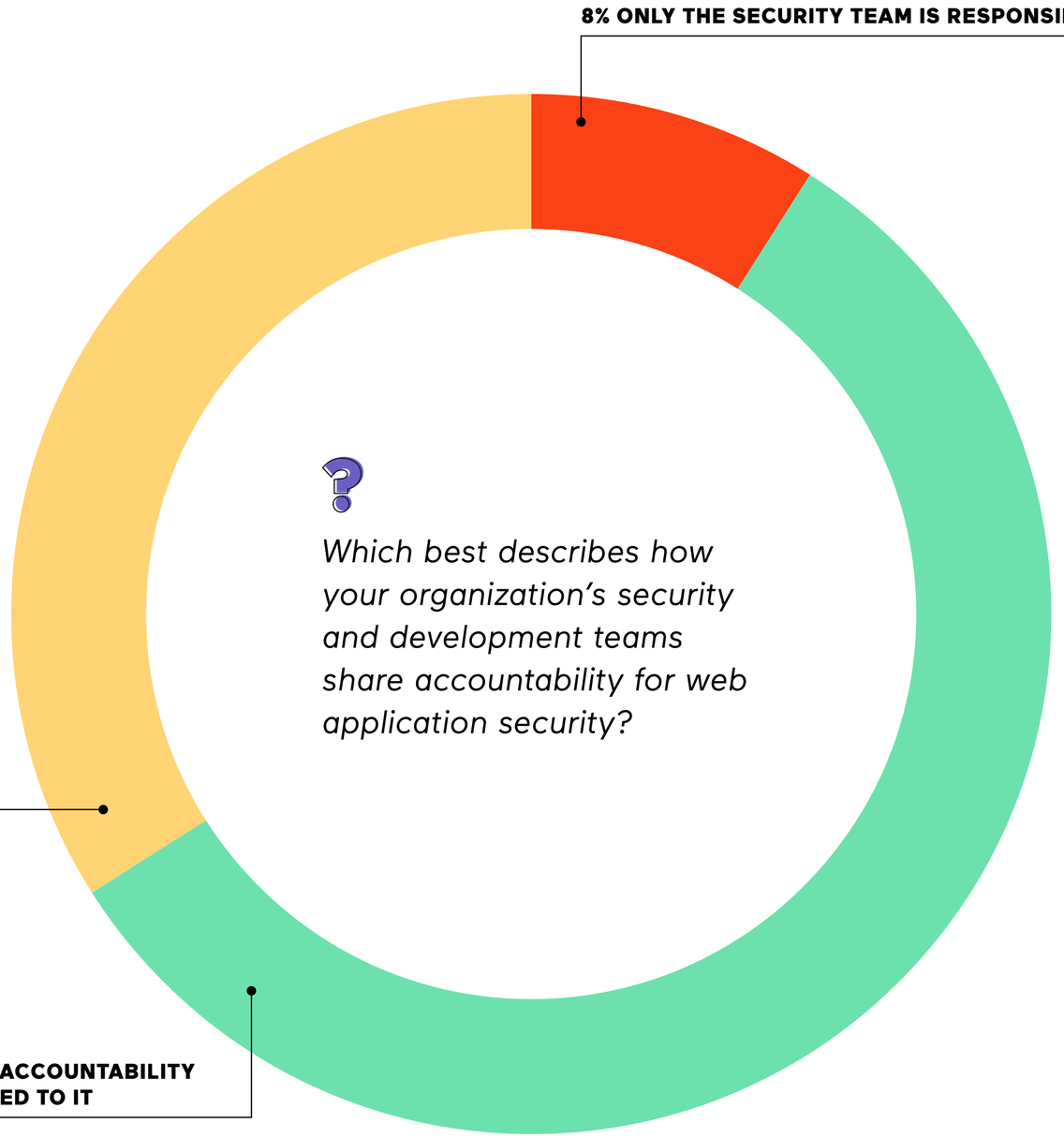


7%
STRANGERS - THE TEAMS DO NOT COLLABORATE

The eternal question: Whose responsibility is security?

(Spoiler alert: everyone's)

Security incentives are increasingly aligned across organizations, but accountabilities are falling short. Leaders have work to do to bring true accountability to the question of web application security. Shared KPIs will further encourage deep alignment and collaboration among development, security, and DevOps.



Developers now spend a lot of their time tackling security issues - even though it often impacts delivery.

Security and devs know that rapidly delivered innovation that puts vulnerable code into production can do much more harm than good. But security work is consuming developers' time and delaying delivery. The fix: deeply integrate security into the SDLC to mitigate its impact to timelines, identify effective security tools that can be used efficiently, and hold everyone accountable for security outcomes.

On average, respondents estimated that

51%

of a web developer's time is spent on security issues

Among respondents in organizations where security is fully integrated into the SDLC, 70% cite delays

80%

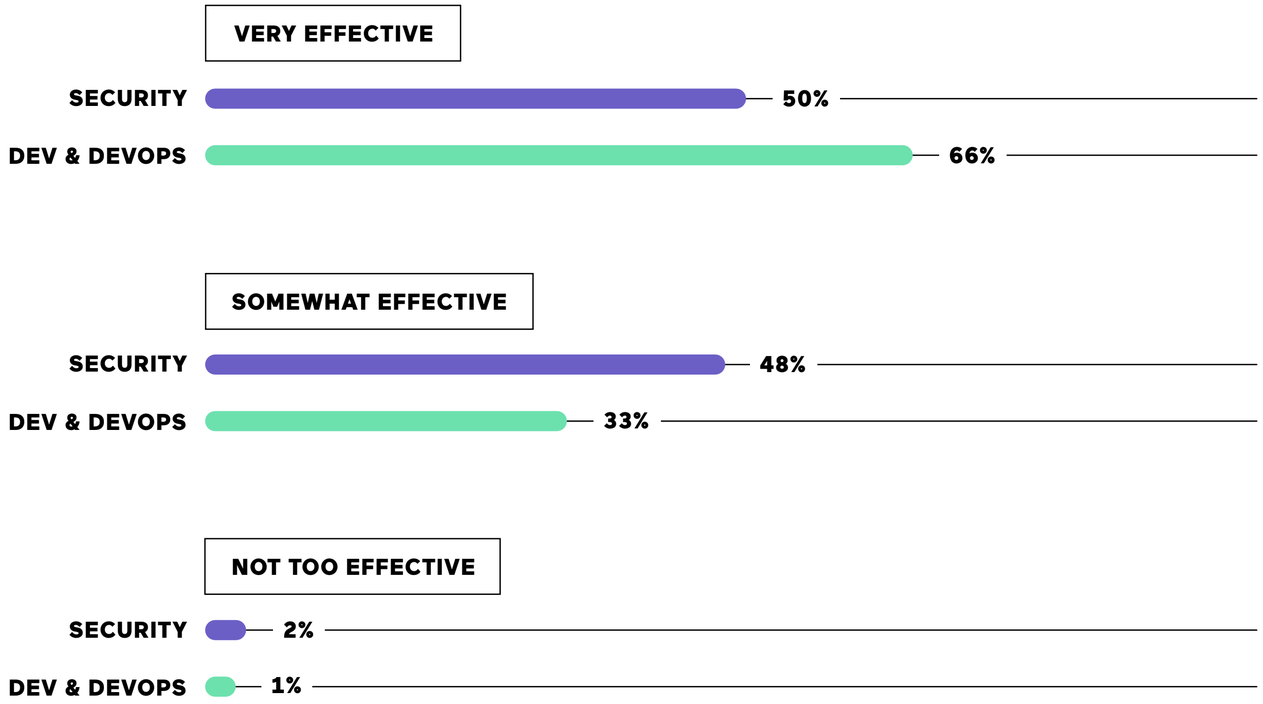
of respondents said that **security processes delay their delivery timelines "somewhat" or "significantly"**

Where security is not integrated into the SDLC, 83% cite delays

Security gives devs pretty high marks, but devs might overestimate their own performance.

With the security skills gap worsening,[2] organizations can't simply expect devs to have depth in security on arrival. Leaders must invest in developer training and enablement on secure coding and remediation and leverage security champions[3] to improve effectiveness.

How effective is your development team at handling security issues?



[2] *Enterprise Security Group and Information Systems Security Association, 2021*

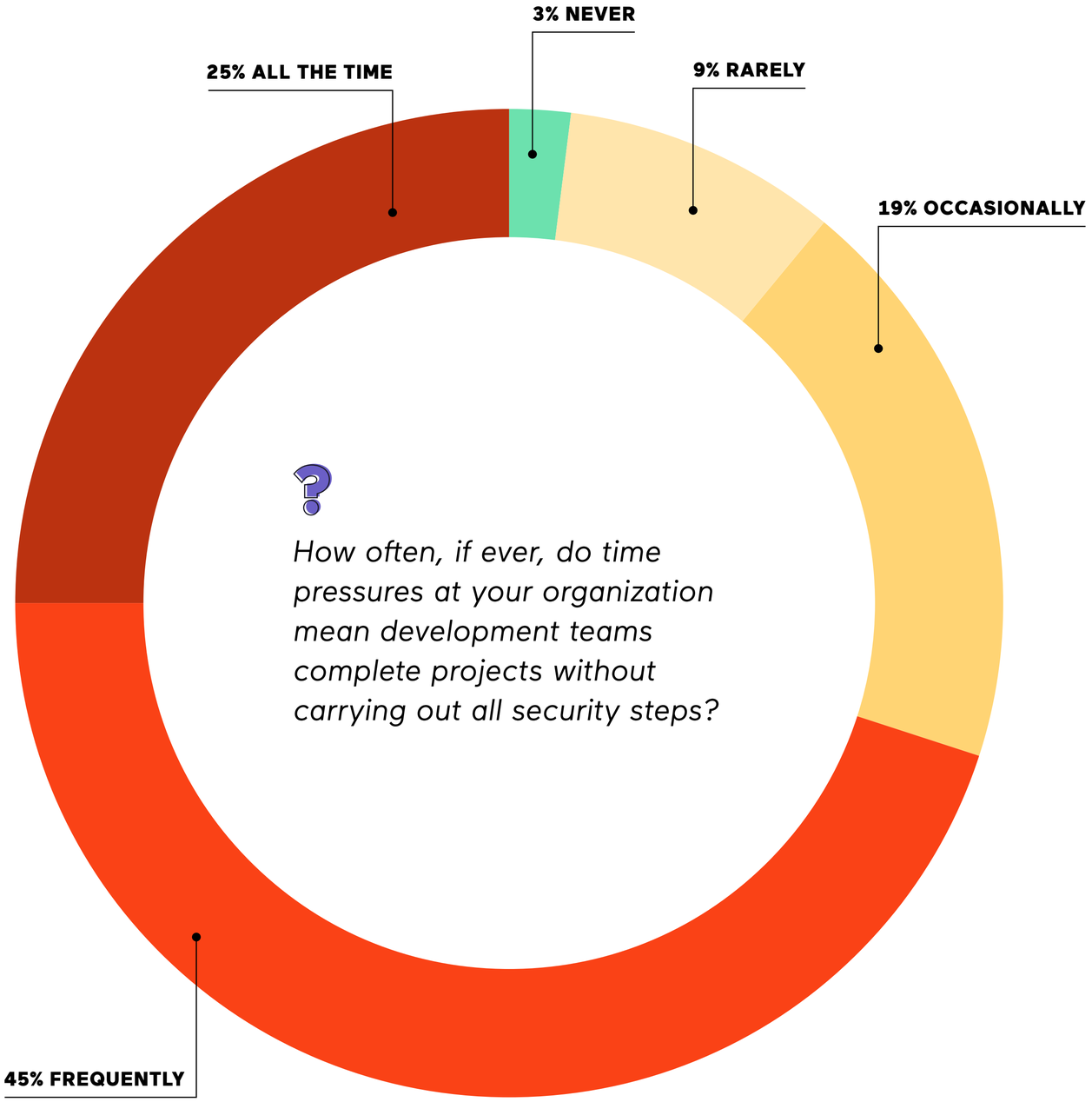
[3] *HackEDU*

What got us here won't get us there.

Although organizations have increased focus on security and started to integrate it into development and DevOps, we are still at the beginning of a journey that has, so far, unfolded incrementally. Can the dual challenges of innovation and security propel leaders to move faster?

In most organizations, innovation pressures still outweigh security priorities.

Tight timelines. Constant pressure to innovate. Developers have their work cut out for them and security can feel like a bottleneck on delivery timelines. It's no surprise, then, that skipping security steps is commonplace.



Executives underestimate just how often this happens.

14% of executives estimate that their teams "rarely or never" skip security steps, but only 6% of developer respondents agree.

Secure design isn’t the norm …

… yet.

Now its own category in the OWASP Top 10 list of vulnerabilities, insecure design remains a vexing problem. When code is inherently vulnerable from day one, the problems flow downstream (and risk increases).

Developers are increasing their knowledge of secure design practices, but this is not yet the default approach. Among our respondents, only 42% spend most of their time remediating issues identified in the IDE, with the balance of remediation focused on issues caught during QA or in production.

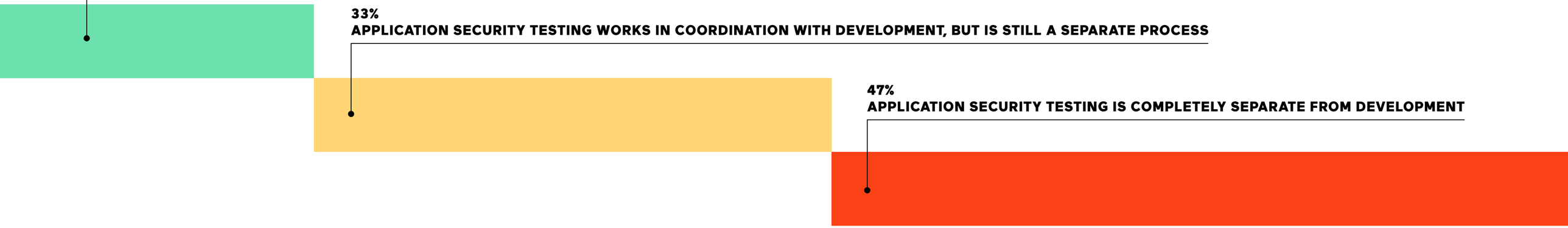
issues under remediation made it to production without being caught in the test or dev stages.

Shifting left is a marathon, not a sprint.

In an effort to reduce the amount of vulnerable code that makes it to production, many organizations are pursuing a "shift left" approach - bringing security closer to the software development lifecycle (SDLC). But the reality is that the end state of complete shift left remains elusive in many organizations.

Only 1 in 5 respondents reported that they've fully shifted left, and 47% have not integrated into the SDLC at all. Another third report they're in the "messy middle," pointing to an overall trend that integration is lacking in web app security.

Which of the following best describes your application security testing model?

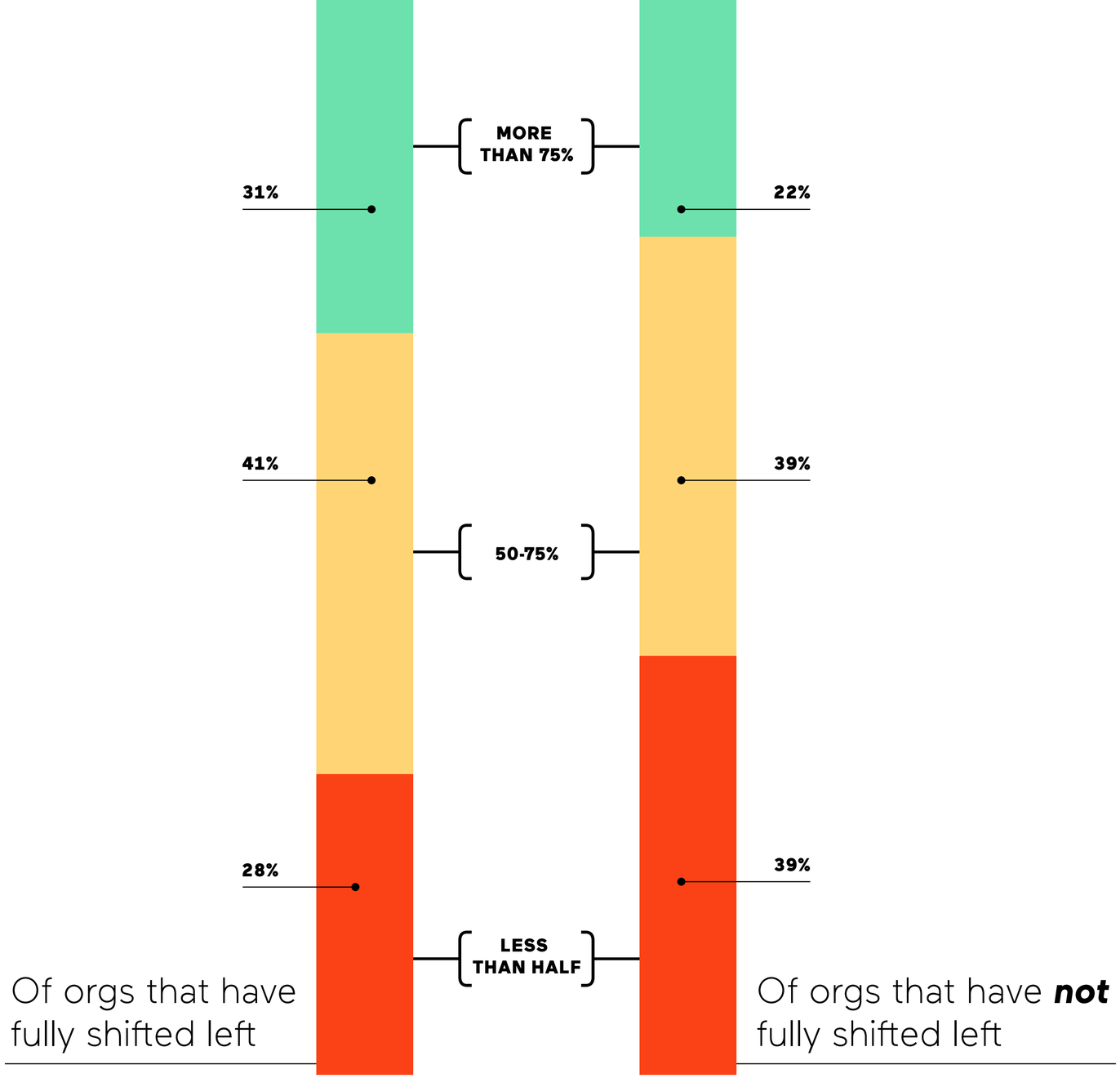


And when organizations do shift left, they often put the right side at risk.

Although organizations that have integrated application security testing into the SDLC tend to report higher coverage of the attack surface, they still fall short of full coverage.

Overemphasis on shifting left can also draw resources and attention from the production attack surface. With agile models driving frequent code updates and new vulnerabilities emerging, production applications represent significant risk. To address this risk, organizations should strive to achieve coverage of 75-100% of apps.

What percentage of your organization's web applications are regularly scanned for vulnerabilities and then remediated?

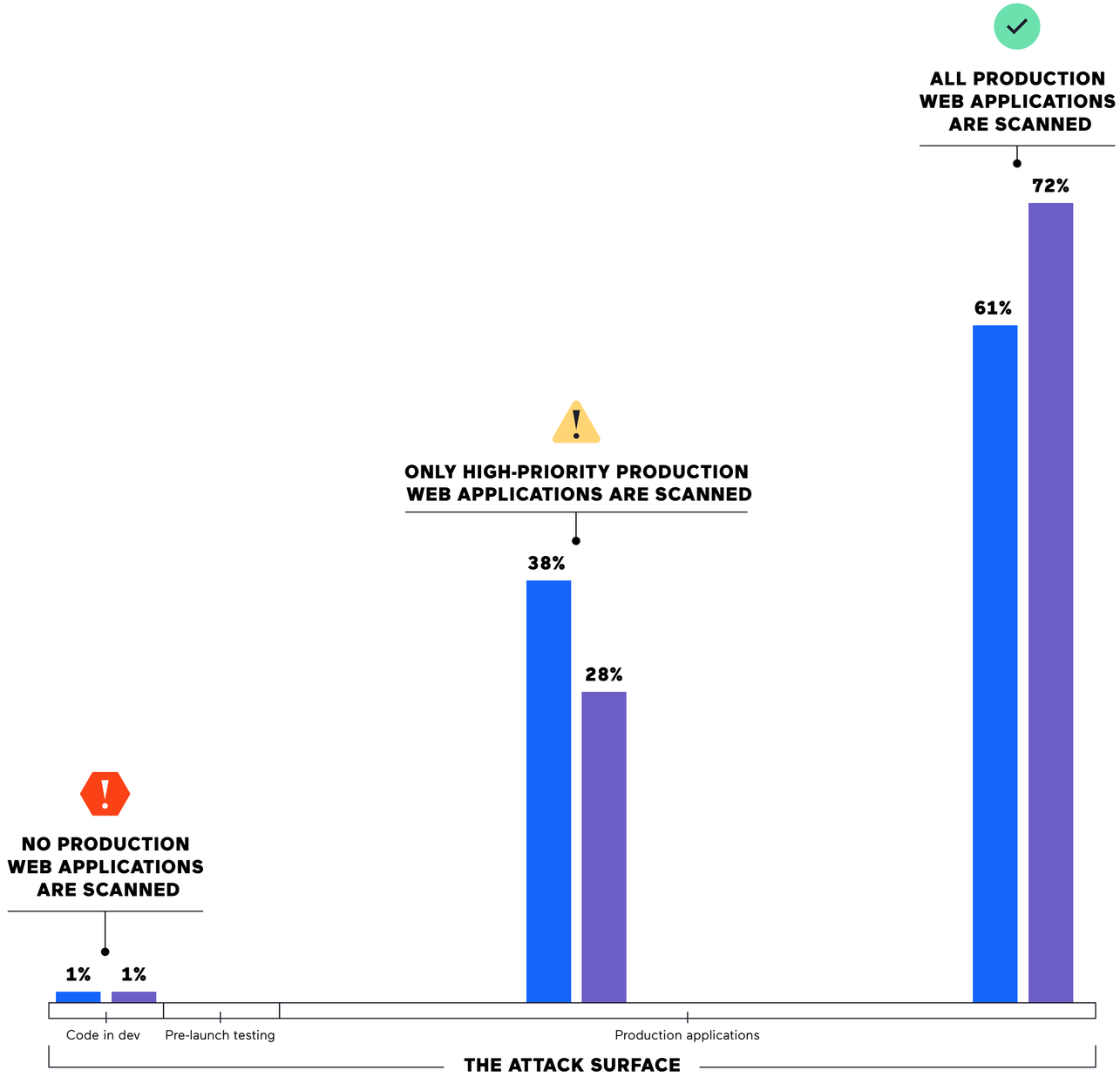


A too-narrow focus on flagship assets creates security blind spots.

Organizations are overwhelmed by the idea of securing all of their web applications. This can mean they choose to secure what they believe to be the most vital for their business, while ignoring the rest - leaving much of their attack surface exposed. That's a big problem, since even the most innocuous app can be the attack vector.

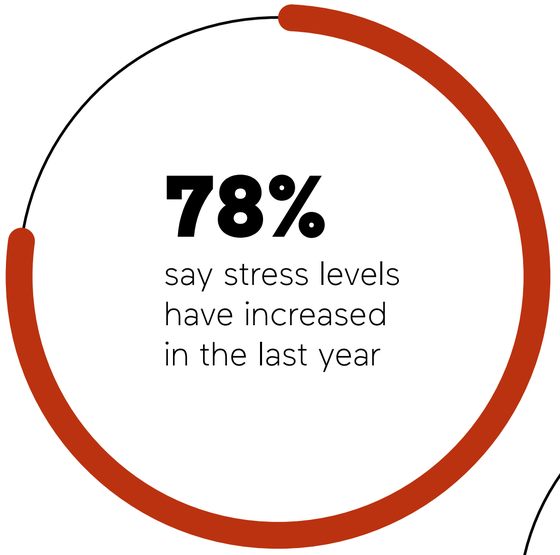
And executives are missing the full picture, overestimating their coverage compared to what their teams on the ground know.

To what extent, if at all, does your organization run vulnerability scans for production web applications?



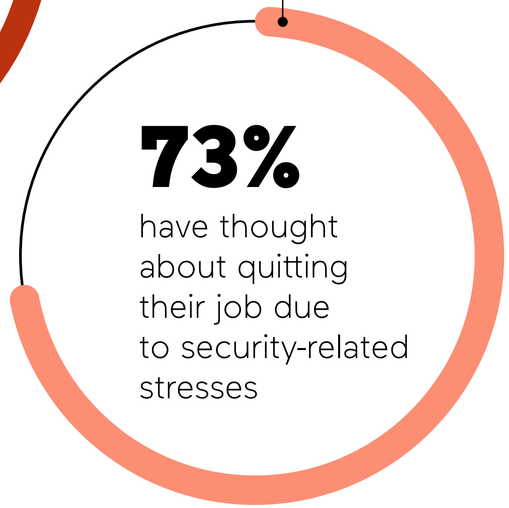
A day in the life: What it's *really* like on the front lines.

Security, developer, and DevOps practitioners spend every day situated in the tension between shipping code fast and maintaining security. A deeper understanding of their real-world challenges can show leaders where to intervene.



BREAKOUT BY ROLE

- **DevOps (81%)**
- **Security (79%)**
- **Devs (73%)**



Teams are constrained and stressed.

The ongoing challenges of protecting their organizations from security threats have taken their toll on development and security professionals alike. Hardest hit are those in DevOps roles, likely because they are accountable for both the on-time delivery of new features and the coordination of security and quality fixes.

With stress threatening to create significant staff retention problems, organizations will struggle to meet their innovation goals. Executives cite IT talent shortages as the chief barrier to their adoption of nearly two-thirds of emerging technologies, including cloud migration, automation, and security tools themselves.[4]

[4] *Gartner, 2021*

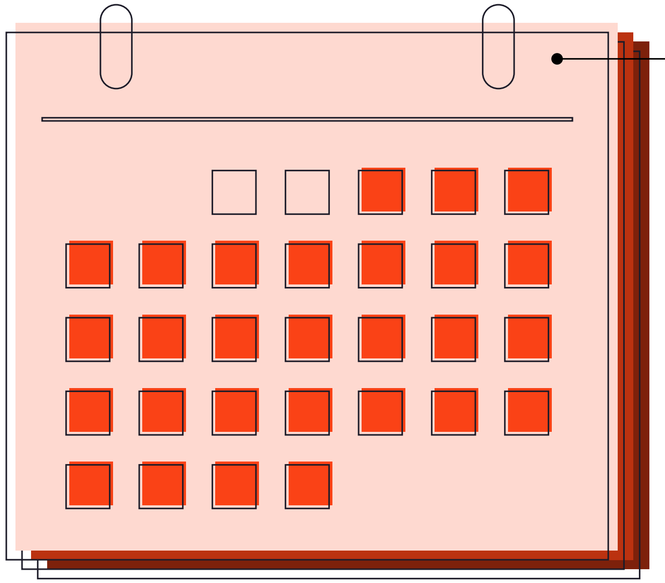
[5] *ISC2 Global Workforce Study*

4 million

unfilled cyber-security roles[5]

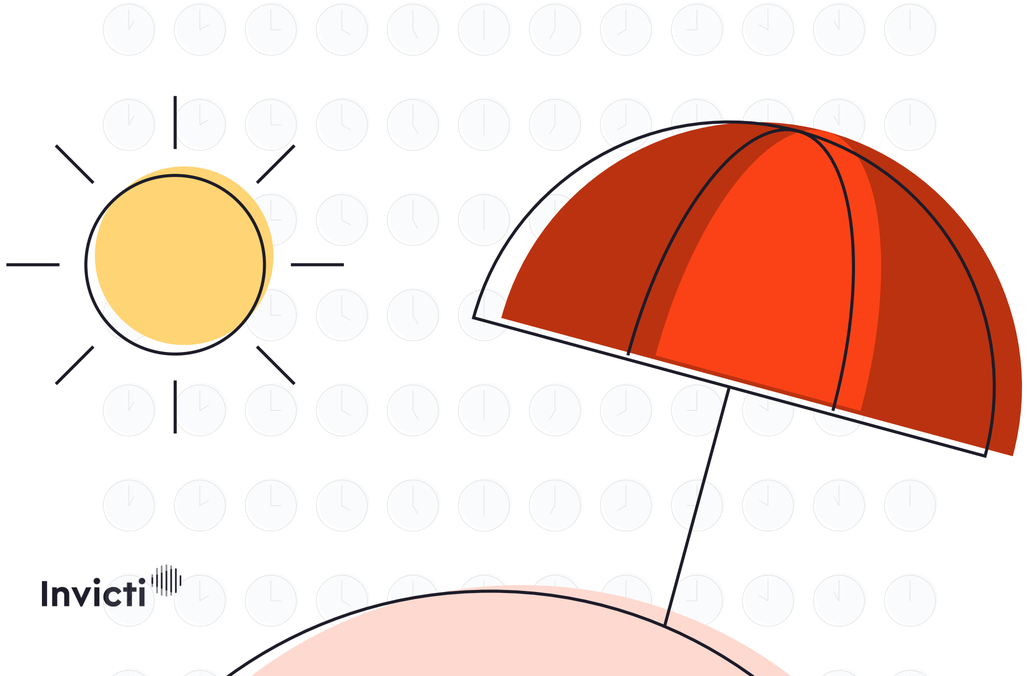
The security backlog looms large

Clearing security debt currently sitting in remediation backlogs takes time - a lot of time. In fact, it would take as long as a really nice vacation.



But 17% of respondents think it could take between

4 - 14 weeks (so, as much as 650 hours)



112 hours (2 weeks) per team member

Average estimated time needed for IT teams to address current backlog of security issues facing their organizations - if they don't work on anything else

96%

say **false positives are problematic** at their organization

False positives are a constant headache.

False positives - or the flagging of a vulnerability that is not, in fact, a real vulnerability - are a huge problem in web app security.

False positives are more than just a time-suck:

- **39%** say they increase friction between development and security professionals
- **32%** say they cause developers to be less likely to integrate security into their workflows
- **25%** say they undermine confidence in app security testing software

Where tools fall short on accuracy, organizations have to lean on human intervention.

The good news is that the robots haven't taken away everyone's jobs. The bad news is that robots haven't even taken away the bad parts of people's jobs. Painstaking manual efforts to address verification of false positives draw time and energy away from more strategic security and development priorities, and come at a real cost to organizations. Our own analysis indicates that the average large enterprise may waste as much as half a million dollars every year on manual verifications.

Only 53%

of security professionals are confident in the accuracy of their web vulnerability scanning software

78%

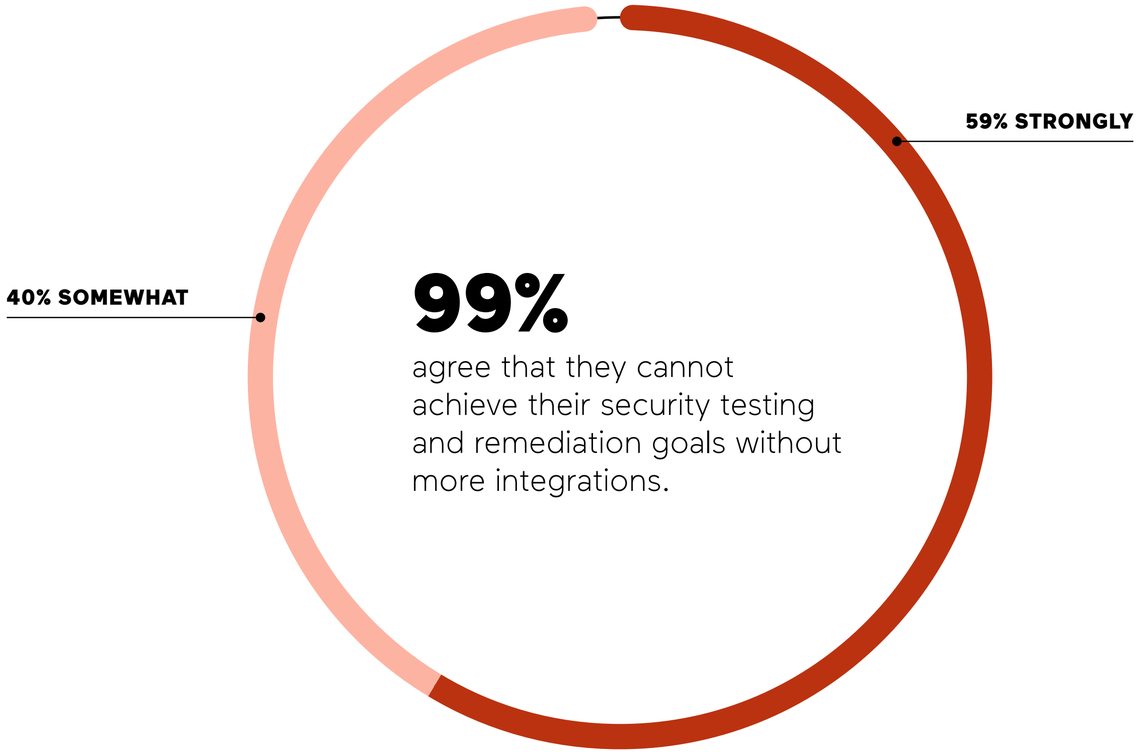
say they always or frequently perform manual verification of flagged vulnerabilities

Each manual verification takes, on average,

65 minutes to investigate

We’re going to need a bigger (security automation) engine

Even the best human horsepower can’t address the challenges of web application security alone, and practitioners and developers know it. Their tools need to work much harder to ever have hope of staying on top of threats. Automation is the only way forward, but organizations are falling short on this element and the integrations that make it possible.



60%

said that their organizations **do not have enough automation in place today** to test and remediate security issues.

Even worse: much of the risk is coming from *inside the house.*

Who, exactly, is creating security threats? ***It turns out that attackers are getting an assist from some unexpected sources.***

Security and development pros have enough to contend with given the threat landscape, resource constraints, and underpowered tools. But respondents face low-tech risks as well. We asked about the biggest human threats to security in their organization. The surprising finding: respondents more frequently cited human error and leadership apathy as the biggest security threats, assigning lower concern to malicious actors inside and outside their organization.

So what *will* get us there?

The future holds promise and threat.

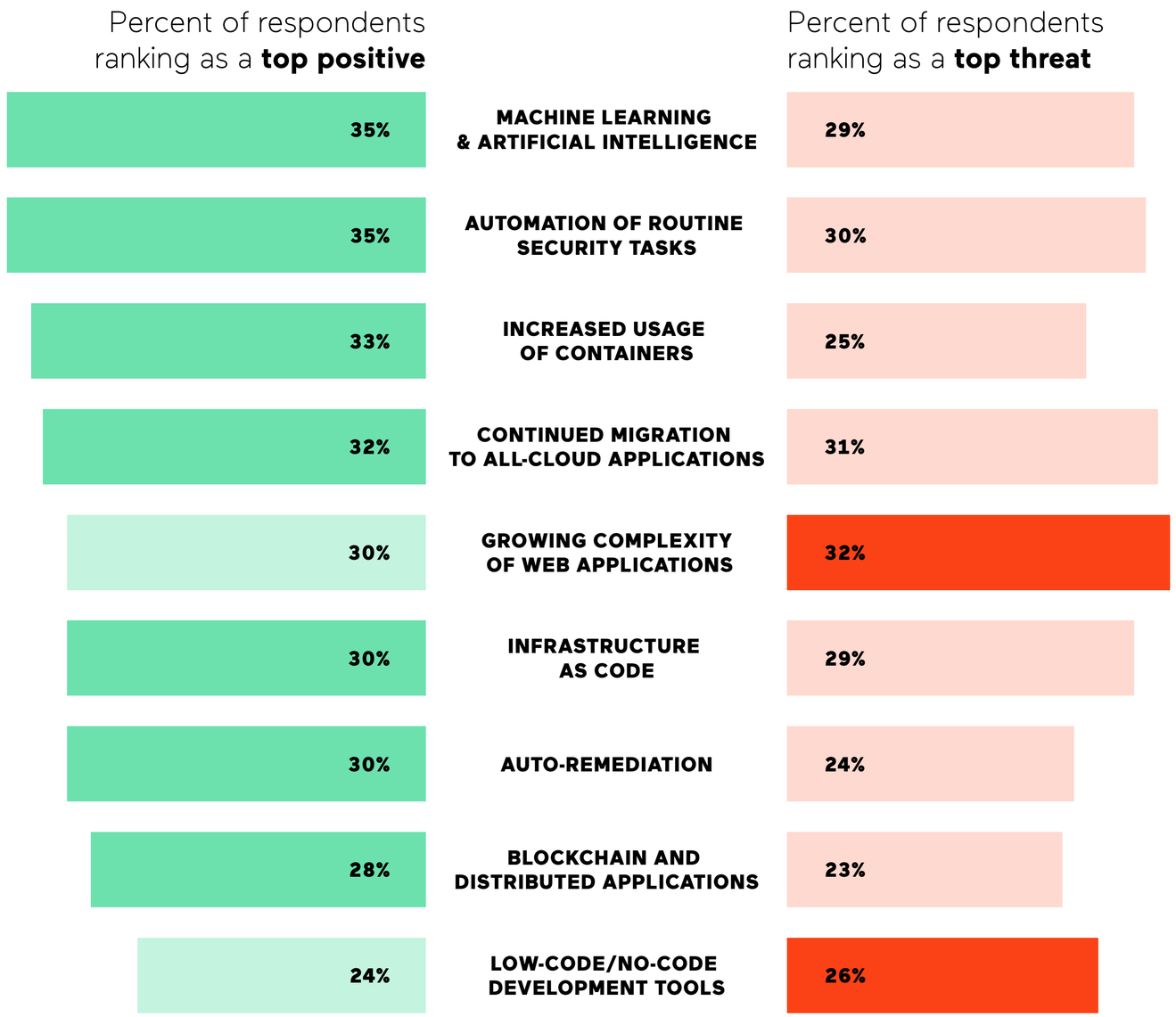
Emerging technology advancements present a double-edged sword for the future of web app security. Most of the advancements that hold promise for making things better also have the potential to increase threat when in the wrong hands. Our respondents are optimistic and pessimistic in nearly equal measure.

The most frequently-cited technology threat to security is the continued migration to all-cloud applications (cited by 31% of respondents). But 32% of respondents also think that cloud migration is one of the strongest benefits to security.

The biggest sources of optimism? Automation and machine learning (both cited by 35% of respondents).

Source of hope, or increased threat?

Organizations have set their sights on a range of technologies that promise digital transformation and speed innovation. But as they rush to embrace things like ML/AI, cloud, containerization, and increasingly sophisticated web technologies, they cannot fail to ensure their security strategy keeps pace.



What's next?

Cybersecurity matters to every human on earth and will only accelerate as an issue of global importance in the years to come. Those on the front lines of delivering both innovation and security will continue to have some of the most challenging work out there. But there is much within our power to make things better.

Recognize that security and innovation aren’t at odds, but inherently linked.

Build an organizational culture that aligns incentives, fosters collaboration, and enrolls security, developers, and DevOps in a mission to deliver continuously protected innovation.

Empower teams to code securely and remediate effectively.

Executives may be overestimating their teams’ ability to code securely and their confidence in addressing security issues. Equip them with the training and tools they need to be successful in delivering on the protected innovation mission.

Shift left and prioritize secure design, but also shift right.

With 1 in 3 security issues making it to production without being caught in development, there’s never been a more important time to shift left. But organizations can’t stop there, and must prioritize security of applications in production too.

Invest in tools that automate everything that can possibly be automated.

While dev and sec aren’t as hostile as they’re chalked up to be, friction and a lack of accountability remains. Doubling down in these areas improves the relationship by reducing manual tasks and freeing up time for more important projects and product innovation.

Heed the threats of machine learning, but embrace its massive opportunity.

Often considered a threat to security, machine learning also presents some of the biggest opportunities. The industry should continue to invest in this area as it offers modern solutions to some of our biggest challenges, like understanding the threat context of a vulnerability and prioritizing remediation.

Methodology

Conducted in partnership with Wakefield Research, this online survey involved 600 stakeholders in U.S. companies with more than 2,500 employees. Respondents included an equal mix of the following: executives with titles VP or higher, such as Directors of IT, VPs or SVPs of IT or EVPs leading technology or IT security divisions at their company; practitioners with a manager title or equivalentwho direct IT security at their organization with responsibilities that include application security, DevOps, vulnerability management, information security, security architects, software security, software development, security engineering or penetration testing; and developers who write code regarding security programs or IT security at their organization, with roles like developer or software engineer. Participants were invited via email.

Results of any sample are subject to sampling variation. The magnitude of the variation is measurable, and is affected by the number of interviews and the level of the percentages expressing the results. For the interviews conducted in this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 4.0 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

About Invicti

Invicti Security is changing the way web applications are secured by organizations across the world. Invicti's two products, Netsparker and Acunetix, prevent costly data breaches and other security incidents by identifying web vulnerabilities from the early stages of application development through production. Netsparker is the leading enterprise DAST + IAST solution and the first to deliver automatic verification of vulnerabilities with its proprietary Proof-Based Scanning technology, enabling unparalleled scalability for even the largest organizations. Known for its ease of use, speed, and accuracy, Acunetix enables even small businesses to leverage best-in-class web application security tools, and was the first-ever automated web application security scanner to feature both DAST and IAST. Invicti is headquartered in Austin, Texas, and serves organizations all around the world.

www.invicti.com