New Vulnerability Found:

Executive Overconfidence

Invicti

TABLE OF CONTENTS

Invicti

Executive summary

Organizations worldwide rely on web applications to do business, so ensuring web application security is vital to prevent breaches and downtime. Research has shown that while companies are fully aware of this and prioritize web application security in their IT security efforts, applying policies and procedures in practice faces serious challenges. Notably, there is a significant disconnect between executive perceptions of web application security and the realities faced by security personnel and developers, with executives generally taking an overoptimistic view of their security posture and workflow effectiveness.

Companies have widely adopted agile methodologies such as DevOps to develop and maintain their own web applications, so the effectiveness of complex workflows related to development, testing, and operations now has a direct bearing on the business. The rapid pace of development combined with the growing number of web assets leaves many organizations unable to fully secure all their applications, with executives once again overestimating the effectiveness of security efforts.

This report highlights key findings from a recent study conducted in order to understand the theory and practice of web application security in organizations worldwide. Research confirms that while organizations appreciate the importance of security in web application development and operations, they are still struggling to implement effective workflows and gain full visibility and control of their web application environments.

Research Objectives

Aiming to evaluate the maturity and effectiveness of web application security programs in modern organizations, Invicti Security teamed up with Dimensional Research to conduct a survey. We asked 382 security professionals across multiple industries and geographies about their expectations and everyday experience of web application security. Covering a variety of topics related to web application security, the study was intended to:

1. **Understand the importance of web application security to organizations** to learn more about the significance of web applications in modern businesses and the overall level of security awareness.
2. **Examine how executive visions of web application security align with everyday practice** to see whether high-level strategies, policies, and procedures translate into real-life security improvements when implemented.
3. **Gauge the effectiveness of existing web application security workflows** to determine whether the tools and processes currently used by organizations across multiple industries are fit for the job and can actually ensure security.

Research highlights

Web application security is recognized as a critical priority area of IT security.

Organizations that rely on web applications to do business are increasingly aware of the importance of web application security in preventing data breaches and downtime. Because most develop and maintain their own web applications, they have first-hand experience of how vulnerabilities are introduced and how costly they can be to find and resolve, so they appreciate the importance and benefits of maintaining a solid security posture.

Many companies don't scan all their web applications.

Modern web application environments can contain thousands of web assets, including not only user-accessible web pages and applications but also microservices and API endpoints. For reasons of cost, technical limitations, or insufficient resources, it is not unusual to restrict vulnerability scanning to the most critical resources.

Vulnerabilities are introduced faster than they can be fixed.

It only takes a second to introduce a vulnerability but often many days to find and fix it. Without the right tools and streamlined workflows, many organizations are struggling with a backlog of issues that just keeps growing.

Executives have an overly optimistic view of web application security.

CISOs and other executives feel that they have the right policies and controls in place to ensure web application security, but security professionals and developers tend to be less optimistic. Seen from the trenches, existing web application security workflows are more fragile and less effective than the C-suite believes.

Web application security workflows are hindered by internal inefficiencies.

Growing awareness is one thing, but implementing effective web application security workflows is quite another. Delayed feedback, inefficient escalation procedures, and false positives plague developers and security teams alike, adding up to a significant performance overhead.

Seen from the trenches, existing web application security workflows are more fragile and less effective than the C-suite believes.

Web application security considered a top priority, but practice lags behind theory

Business applications continue to move to the cloud, and with good reason. As web technologies have matured to a level that allows web applications to match the performance and functionality of desktop software, organizations have embraced the operational benefits and agility of cloud-based deployments. Coupled with the lower barrier to entry compared to desktop software, one consequence of this continuing shift is that web application development is moving in-house, with a massive 81% of surveyed companies developing their own web applications.

Moving to in-house development and operations brings many benefits, such as cost savings and greater business agility, but also comes with numerous challenges. Crucially, companies are now building the software that their own business depends on, so any bugs, performance issues or vulnerabilities can have a direct business impact. In this new world, it should be expected that business continuity concerns would boost application security awareness.

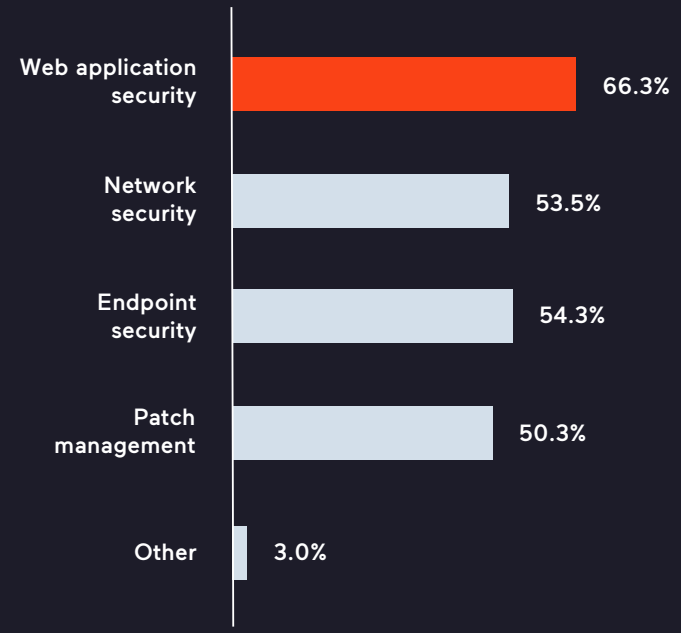
Over 66% of respondents named web application security as a priority area – more than any other aspect of IT security.

To verify this, we asked companies which areas of IT security they need to prioritize. Results confirm that web application security is high on the agenda across all roles. In fact, over 66% of respondents named web application security as a priority area – more than any other aspect of IT security. On the flip side, this means that a third of organizations don't feel the need to expand their web application security efforts. This can be interpreted in at least two ways: either they are satisfied with their current security program in this area or they don't consider it a priority.

Application scanning coverage

Web technologies combined with agile development methodologies have created an environment where adding new applications and modifying existing ones is relatively quick and easy, especially compared to traditional waterfall models. Coupled with the transition from monolithic applications to service-based architectures, this has led to an exponential increase in the number of web assets that organizations need to manage and secure. What used to be one application can now be a dozen loosely coupled services that communicate via application programming interfaces (APIs), posing a major challenge for security testing.

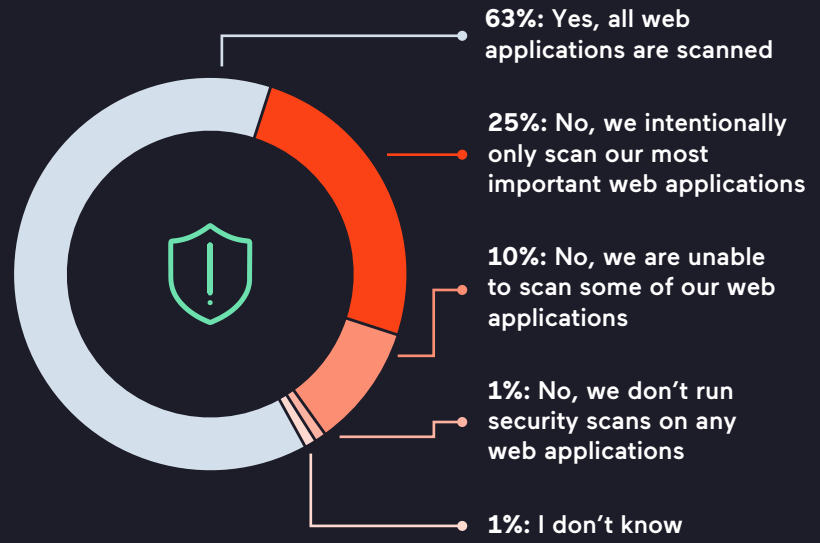
Which of these areas do you think your company needs to focus on more?



To see how confident organizations are in their security testing coverage, we asked if they consistently run security scans on all their web applications. Close to two-thirds (63%) confirmed that they do scan all their web applications, which initially seems encouraging and (perhaps not coincidentally) is similar to the proportion of companies that acknowledge web application security as a priority area. However, turning this result around, this means that 37% of organizations are not confident that all their web applications are covered by security testing. Considering that just a single vulnerability in one application may lead to a data breach or worse, this is a chilling thought.

Drilling into the details, we can discover some of the reasons why organizations don't include all their applications in security testing. 10% of respondents indicated that they are unable to scan all their assets due to limited resources or technical issues, such as unsuitable tooling. More interesting is that 25% intentionally scan only their most important applications. There can be several reasons for this, most obviously cost factors and insufficient human or technical resources. However, the decision to only scan critical applications could also mean that vulnerabilities in the remaining web assets are not considered a risk (or are treated as an acceptable risk) or – and this would not show up in the results – that some respondents simply don't know exactly what non-critical web assets they have.

Does your company run security scans consistently for all web applications?



Executives are overly optimistic about the realities of web application security

Security is notoriously difficult to quantify and means different things to different people. Web applications can be especially challenging due to the dynamic and distributed nature of development and deployment environments. For example, modern applications typically combine in-house code with third-party libraries and frameworks that might not be covered by security testing during development. The move to service-oriented architectures compounds visibility problems, as one application can now consist of dozens of separate services and API endpoints.

One objective of this survey was to see how perceptions of web application security posture vary across the different roles involved in security. So far we've seen that, overall, roughly two-thirds of organizations believe they scan all their web applications. Splitting these results by role, however, we see a significant disconnect between executives and security personnel: while 75% of executives are convinced that they scan all their applications, this optimistic view is not shared by security teams. In fact, security staff indicate that nearly half of companies don't consistently scan all the web applications in their environments.

***Nearly half** of companies **don't consistently scan** all the web applications in their environments.*

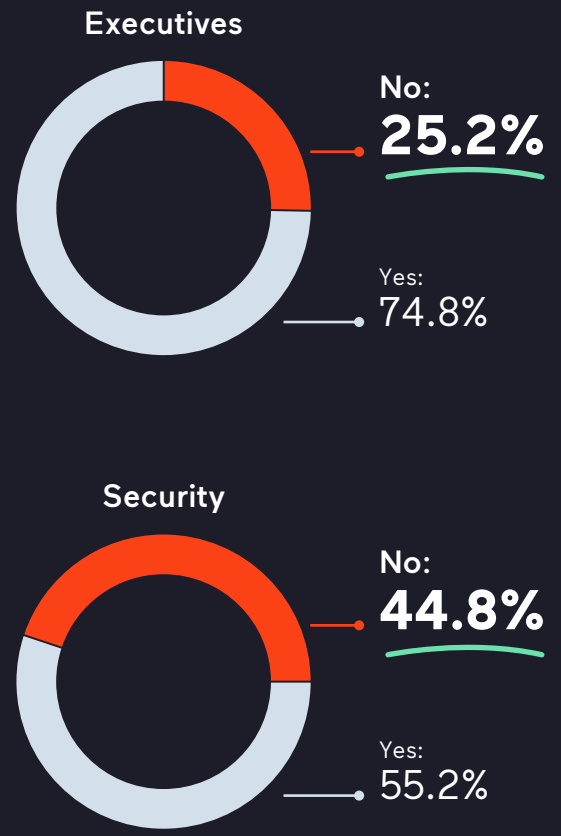
For organizations that intentionally limit scanning to their most important applications, separating the results by role brings another eye-opener: while close to 32% of security staff admit to this practice, for executives this is just over 18%. This suggests that many executives may be in the dark about the criteria for selecting what to scan and when to scan it.

Keeping up with vulnerabilities

Any serious web application security program includes a variety of metrics to measure the effectiveness of security initiatives and track trends. One vital strategic metric is open vulnerabilities per time period, showing whether an organization is reducing its vulnerability counts in the long term. If the total number of open issues keeps decreasing month-to-month despite new vulnerabilities being discovered, there is a good chance that the current security program is effective and overall web application security is improving.

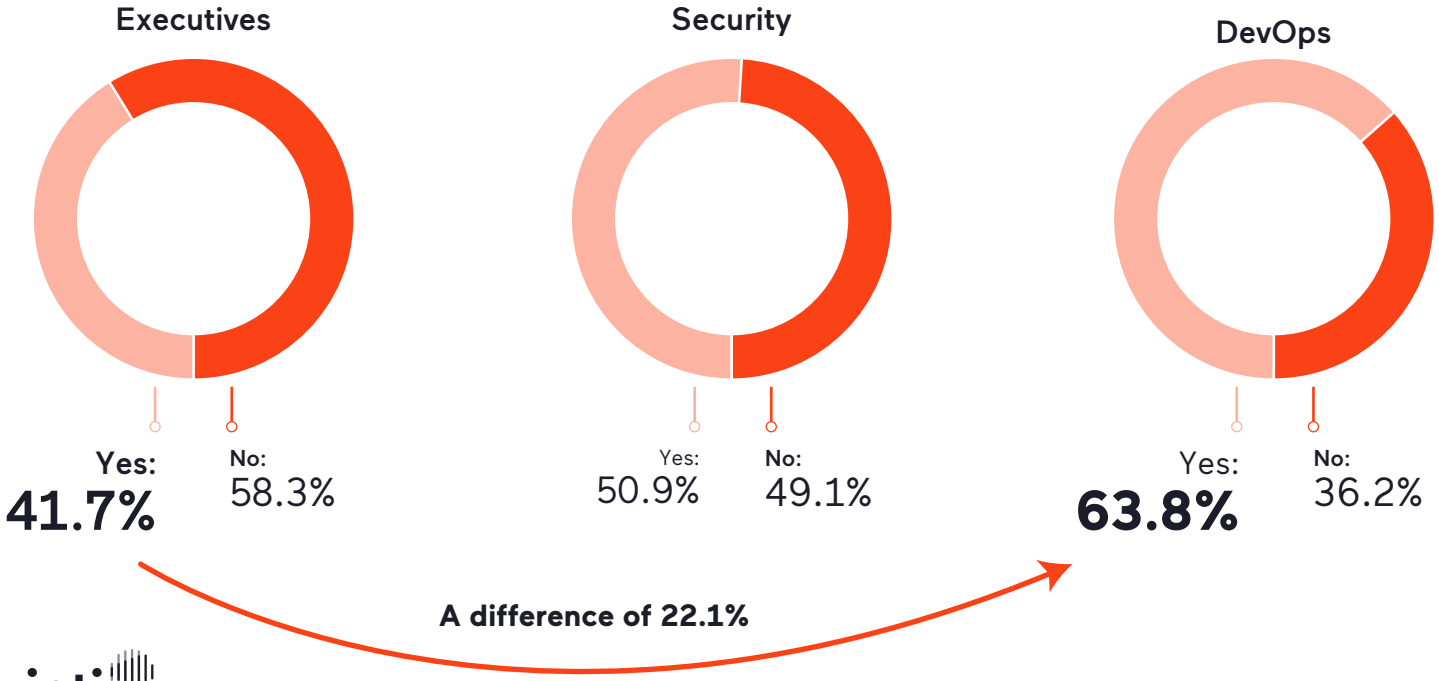
To learn how confident organizations are about dealing with web application vulnerabilities, we asked respondents whether they feel that security vulnerabilities are being discovered faster than they can be fixed. Overall, the responses were roughly a 50-50 split, which means that half of organizations are struggling to reduce their backlog of vulnerabilities. However, separating out the results per role brings even more interesting insights.

Does your company run security scans consistently for all web applications?



Once again, executives are far more optimistic about their companies' security posture, with just under 42% admitting that vulnerabilities can't be resolved quickly enough. For security personnel, the "yes" answers accounted for over 50%, and for DevOps staff this rose to a whopping 64%. This shows another disconnect between executives and line-level personnel and suggests that the rapid changes typical of DevOps workflows are outpacing the security processes.

At your company, are security vulnerabilities discovered faster than they can be fixed?



Rapid changes typical of DevOps workflows are outpacing the security processes.

Process inefficiencies and internal friction hinder web application security efforts

Successfully managing web application security is a massive juggling act that requires organizations to constantly balance security, performance, business priorities, and resource constraints. To be effective at scale across multiple environments and teams, application security policies need to be an integral part of an organization's culture, workflows, and tool choices. Research indicates that companies are still struggling to apply their policies in practice across these three pillars of security.

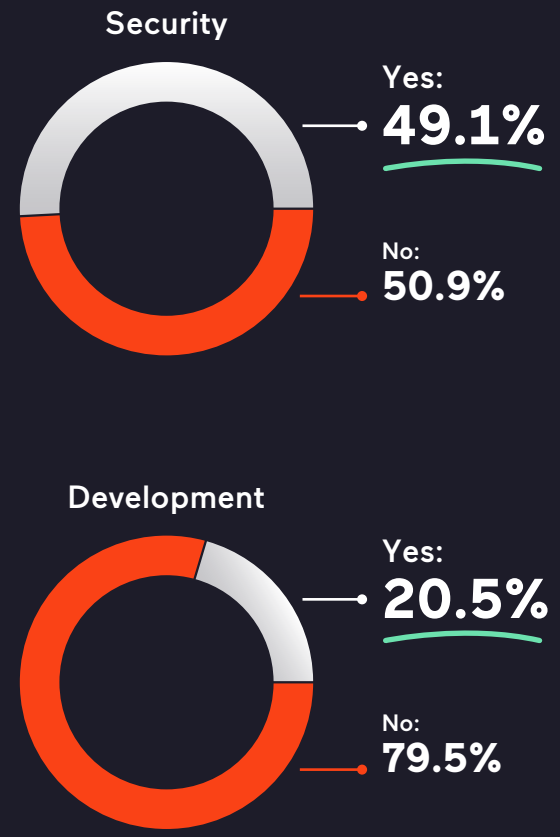
Treating security testing as an isolated stage of the development workflow inevitably brings delays, friction, and inefficiencies due to conflicting interests. Developers focus on making things work and delivering releases on schedule, often under management pressure to get new features out of the door as soon as possible. The job of testers and security personnel, on the other hand, is to find bugs, vulnerabilities, and other issues – in other words, to prove that things don't work after all. To reconcile both approaches, organizations must incorporate security into the development culture and make it an integrated part of the application lifecycle rather than a separate phase.

While just 20% of developers believe that development teams are resistant to incorporating security, close to half of security professionals encounter developer resistance, with 49% indicating this as an issue.

To see how companies are dealing with this challenge, we asked respondents whether they perceived developers as resistant to incorporating security in web application development. Overall, 60% responded that this is not an issue, but drilling into the results reveals a different picture. While just 20% of developers believe that development teams are resistant to incorporating security, close to half of security professionals encounter developer resistance, with 49% indicating this as an issue.

Such a significant difference points to a major disconnect in practices and expectations around web application security. This could be caused by insufficient or unsuitable training programs, where developer training is not aligned with the organization's actual security needs. Communication and workflow issues could have much the same effect – developers may be expecting more guidance and feedback around security, but not getting it. And, finally, there is the natural human tendency to see other people's shortcomings more clearly than our own, which could at least partly explain the discrepancy. Even so, the results suggest that given the right information and workflows, developers are open to building applications with a security-first mindset.

In your opinion, are developers resistant to incorporating security in web application development?

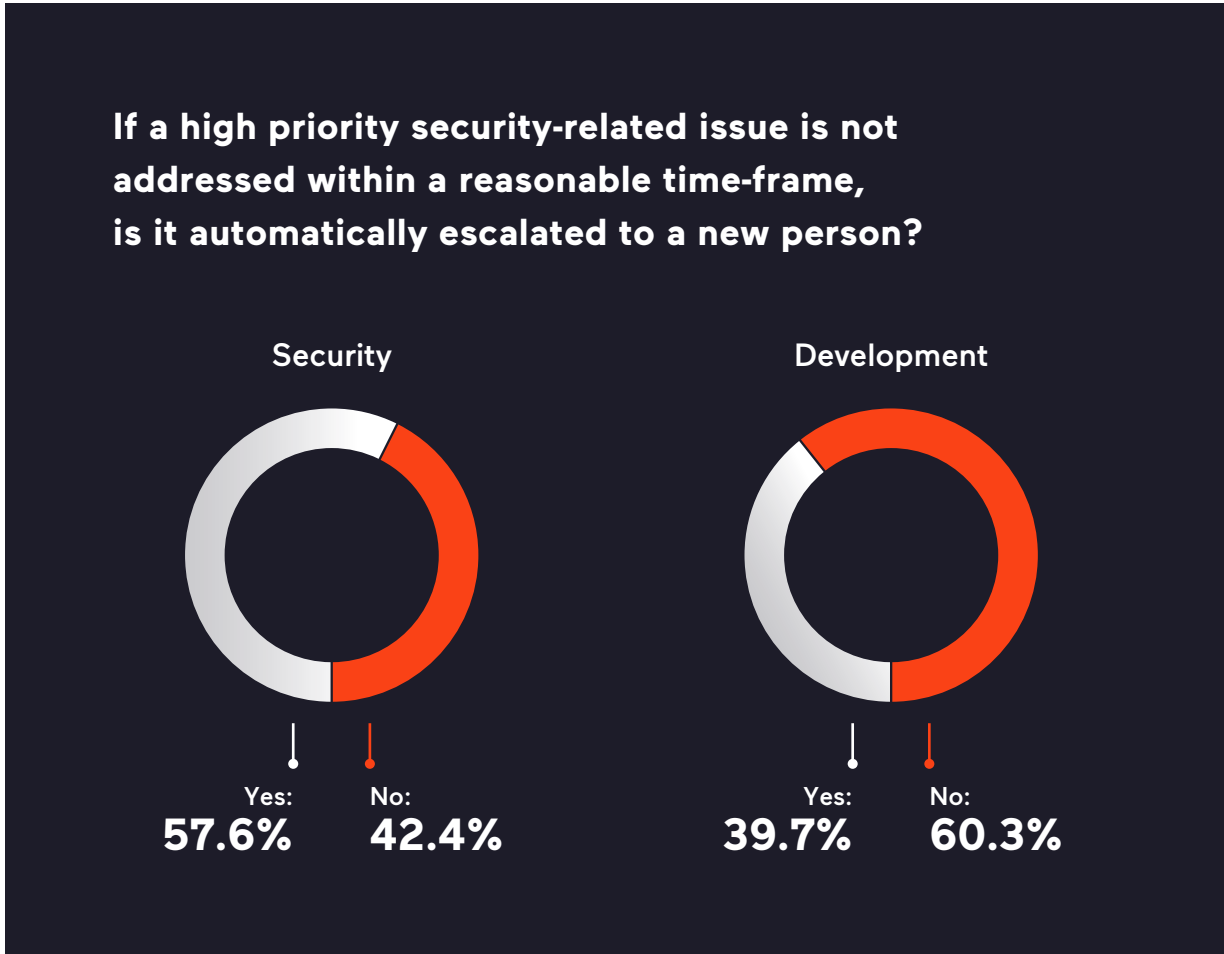


Security workflow effectiveness

Effective workflows are a vital requirement in application development. By automating routine manual tasks and integrating a variety of specialist tools, developers are able to build complex software and coordinate work inside and across teams. Truly effective application security requires the same level of workflow automation – yet tools and processes related to web application security are still lagging behind when compared to mature development environments.

Escalations are one area of security issue management that can make the difference between timely resolution and lingering vulnerabilities that take many months to address, potentially leaving applications open to attack. Ideally, critical security issues that are not resolved within a defined time should be escalated automatically to ensure that nothing slips under the radar. We asked survey participants if this is the case in their organizations. The responses reveal not only gaps in automation, but also yet another significant difference of opinion.

Just under 40% of developers indicated that automatic escalation of critical security issues is in place, which shows that organizations still have a long way to go to fully integrate security into the software development process. However, close to 60% of security staff responded that their organizations do use automatic escalation. This disconnect suggests that application security is not fully incorporated into development workflows, perhaps because development and security teams use separate issue tracking systems with insufficient integration.



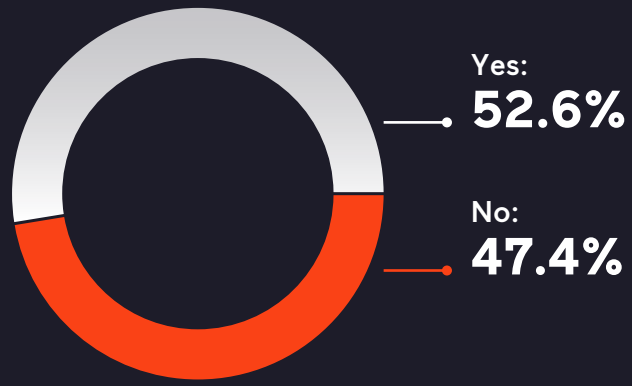
Delayed security feedback

To act on security issues, developers need to know about them. If a critical vulnerability is discovered at a late stage of development and testing and not communicated to the development team, it could become a blocker for the entire release. In a mature application security program, feedback to the developers is immediate and automated wherever possible to prevent delays, with detailed information provided to avoid misunderstandings and unnecessary back-and-forth.

As part of our research, we asked if developers complain about delayed security feedback that impacts deployment deadlines. The responses were roughly a 50-50 split, with broad agreement across roles. This indicates that around half of organizations are still struggling to get timely and actionable security feedback to developers, leading to delays downstream. There can be several reasons for this, including ineffective communication, missing or insufficient integration and automation, and a lack of resources.

> **Half of organizations are still struggling to get timely and actionable security feedback to developers, leading to delays downstream.**

Do developers complain that security feedback is too late and slows deployments?



The impact of false positives

Tooling is the third pillar of effective web application security. Without the right tools, even the best developers and security professionals will struggle to find vulnerabilities and resolve them before they can be exploited by attackers. When small teams need to secure hundreds or thousands of web assets, automated scanning is an obligatory part of the web security toolbox. To ensure accuracy, automated security tools need to walk a fine line to find as many real issues as possible while not raising false alarms for legitimate code.

Automated scanners have traditionally been associated with a high proportion of false positives. Knowing this, security staff were often forced to manually verify each result, negating many of the benefits of automation. Worse still, if an unverified false positive issue was relayed to developers as a real vulnerability, it could lead to many man-hours being wasted on searching for non-existent vulnerabilities and heated exchanges with security staff.

> **Results confirm that security executives consider wasted developer time the most serious consequence of false positives, with 62% flagging this issue.**

While modern tools already exist that can greatly reduce the problems caused by false positives, organizations with less mature workflows are still at risk.

Executives: At your company, what are the ramifications of security false positives?

To see if companies still struggle with false positives, we asked if security false positives are a source of friction between developers and security teams. Just over half of the participants reported that false positives do not cause conflicts – far from a majority, but most likely a higher proportion than we would get a few years ago. On the other hand, this still leaves 48% who do struggle with the internal friction caused by false positives. At the same time, we can speculate that some of the organizations who don't report problems with false positives simply do not get enough scan results, which could leave them with undiscovered vulnerabilities.

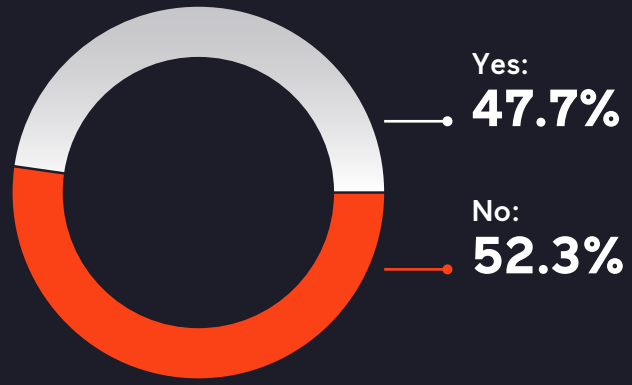
> **Results confirm that security executives consider wasted developer time the most serious consequence of false positives.**

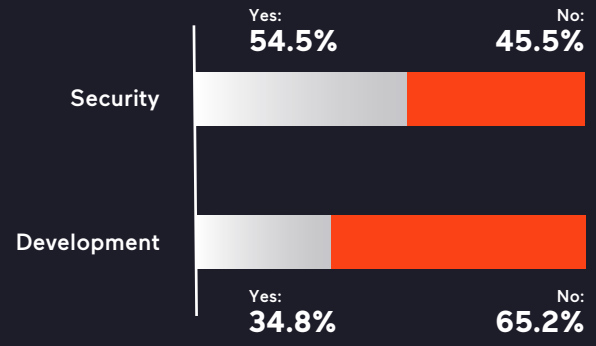
Separating out the results by role, we see that just under 35% of developers report friction caused by security false positives, compared to over 54% of security staff. This suggests that security teams bear the bulk of extra work caused by false alarms, presumably due to verification, triaging, assignments, and retesting being handled mostly manually by security personnel.

54%

of security staff report friction caused by security false positives.

Are security false positives a source of friction between the security and development team?



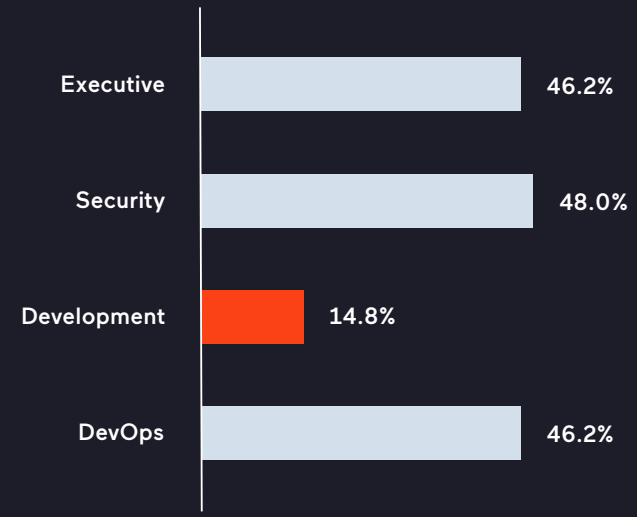


Tool effectiveness

As web application environments grow larger and more complex, ensuring maximum scan coverage becomes a serious technological challenge. Among organizations that only scan a portion of their web applications, around 40% of participants indicated inadequate tools as the reason. However, it is interesting to note that only 15% of developers believe this, as compared to over 45% in all other roles.

This suggests that while developers have the necessary tools to test individual applications, organizations are struggling with security testing across their entire web application environments. Developers are also the only role to indicate low risk as the top reason for not scanning some applications, with 67% of developers selecting this response.

Tools are incapable of scanning all our web applications



Conclusions

The survey shows a worrying disconnect between the theory and practice of web application security. While most organizations appreciate the importance of web security, many still don't scan all their applications and an even greater number struggle to deal with vulnerabilities in a timely manner. Perceptions and expectations of web application security also vary widely depending on the role, with executives generally taking a less realistic view than security staff or developers.

The practical implementation of web security programs and policies also leaves a lot to be desired, with internal workflow inefficiencies generating extra work and friction among teams. Inadequate security issue tracking and escalation workflows are another problem area, often leading to delays that impact downstream work and releases. Persistent problems with false positives are an indication that many organizations still rely on older scanning technologies and therefore can't be fully confident in the results they get.

Our research has shown that the vast majority of companies that use web applications also develop and maintain them in-house, often using modern agile methodologies. While they have the necessary resources and expertise for application development, delivering on their security aspirations is far more difficult due to culture, workflow, and tooling issues. For most organizations, it is still early days on the road to mature web application security.

For most organizations, it is still early days on the road to mature web application security.

About Dimensional Research

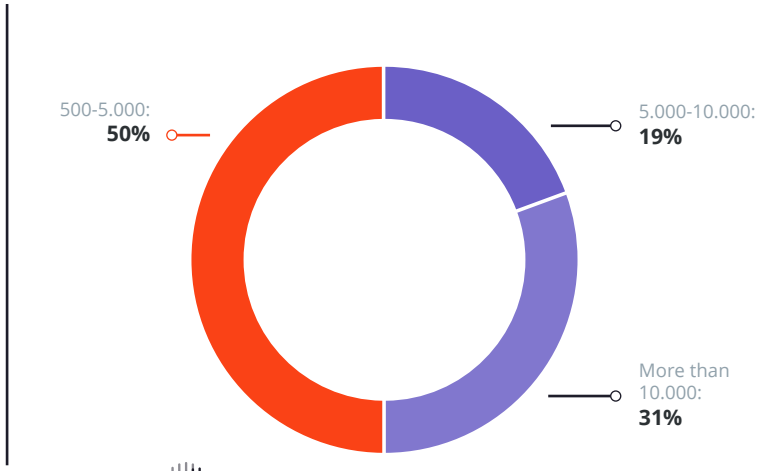
Dimensional Research® provides practical market research to help companies make smarter business decisions. For more information, visit https://dimensionalresearch.com.

Research methodology

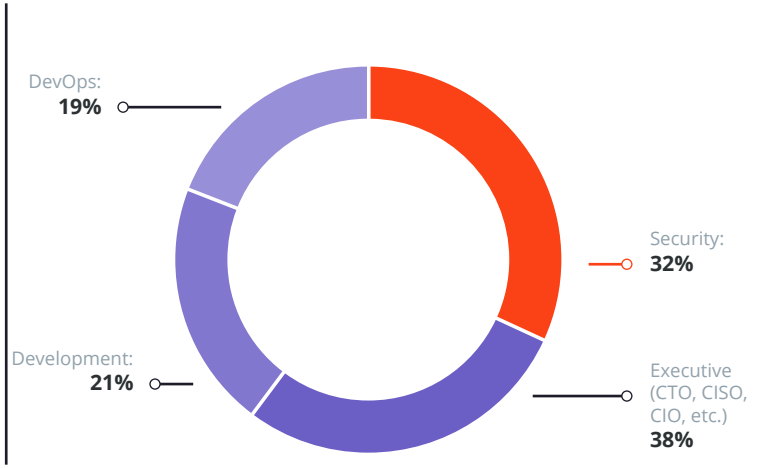
Invicti Security worked with Dimensional Research to perform primary research with security professionals, aiming to understand current trends and challenges for securing web applications. Executive and manager-level security professionals sourced by Dimensional Research were invited to participate in a survey on their company's web application security approaches, tools, and processes. The research also captured metrics on discovered security issues as well as investigated security tools used as part of the development process and development and security team interaction.

The survey was conducted from July 21 through July 28, 2020. A total of 382 qualified participants completed the survey; all respondents are directly responsible for web application security for their company. Participants were from all 5 continents. The survey was administered electronically and participants were offered a token compensation for their participation.

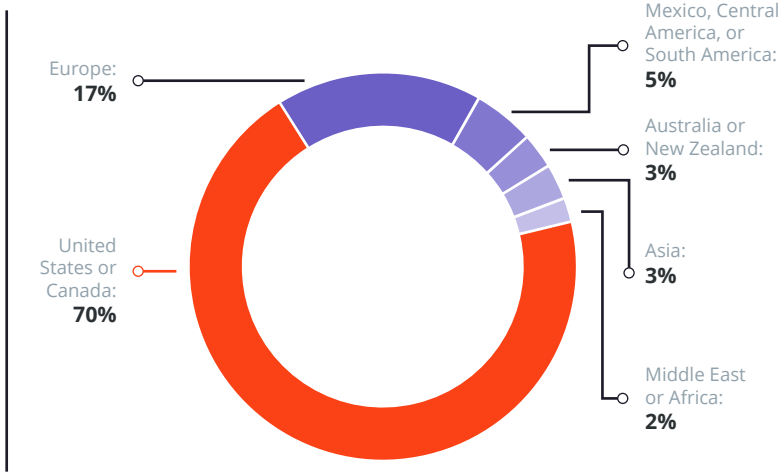
Survey participants company size (number of employees)



Survey participants role



Survey participants location



Invicti

About Invicti Security

Invicti Security is changing the way web applications are secured. A global leader in web application security for more than 15 years, Invicti's dynamic and interactive application security products help organizations in every industry scale their overall security operations, make the best use of their security resources, and engage developers in helping to improve their overall security posture. Invicti's product Netsparker delivers industry-leading enterprise web application security, while Acunetix is designed for small and medium-sized companies. Invicti is backed by Turn/River Capital, and is headquartered in Austin, Texas, with offices in London, Malta, and Istanbul.

www.invicti.com