CYCOGNITO

RESEARCH REPORT

# 2024 State of Web Application Security Testing

## The Need to Improve Testing and Remediation Effectiveness

# Introduction

Modern digital businesses depend upon the performance and reliability of their web applications. Because these apps are so important, they are a top target in attacks. According to research from Verizon, web applications were the most commonly exploited vector in both incidents and breaches in 2023, far outstripping email and human carelessness.[1] Protecting these mission-critical assets isn't easy.

To learn more about the current state of web application security, what stakeholders are doing to mitigate risks, and where their challenges lie, we surveyed 349 security professionals in the UK and US. All respondents had significant experience conducting vulnerability scanning, web application security testing or other security operations tasks, or were responsible for managing others who did.

## Key Findings

- **Organizations are exposing 100s of web applications.** Web application attack surfaces are large and growing. Survey participants' organizations maintain dozens if not hundreds of custom web apps developed in-house and by third-party partners.
- **Over 60% update web applications weekly or more often.** Web applications change frequently. More than eight in ten respondents (87%) update their web apps at least once a month, and 61% update their web apps on a weekly basis or even more often.
- **Over 25% experience a major web application security incident every week.** Web application security incidents and breaches are common. More than one-third of respondents (35%) experience a significant security event involving a web app at least once a week, while more than one-quarter (26%) experience a major incident that often.
- **Nearly 75% test their web applications monthly or less often, leaving more than 40% of the attack surface untested.** Web application security testing is conducted infrequently and coverage is lacking. Most respondents are testing fewer than half of their organization's web applications monthly or less often. More than one in four survey participants (26%) work for organizations with no formal process for testing production web applications. This isn't enough to effectively mitigate web application security risks.
- **70% said the number of web applications in their environment was too large for adequate testing.** Other top-ranked inhibitors to adequate web application testings include the volume of APIs in production environments (cited as a large or very large blocker by 67%) and the time required to test and monitor changes (66%).
- **More than 50% struggle to remediate web application vulnerabilities.** When it comes to web application security testing, clear, actionable findings are a must-have. More than half (53%) of the participants in our survey struggle to remediate the vulnerabilities their web application security tests reveal.
- **65% are planning to increase automation within their web application security testing workflows.** Looking to the future, they are interested in creating efficiencies. They are also interested in building out continuous testing capabilities.

1. Verizon, 2023 Data Breach Investigations Report.

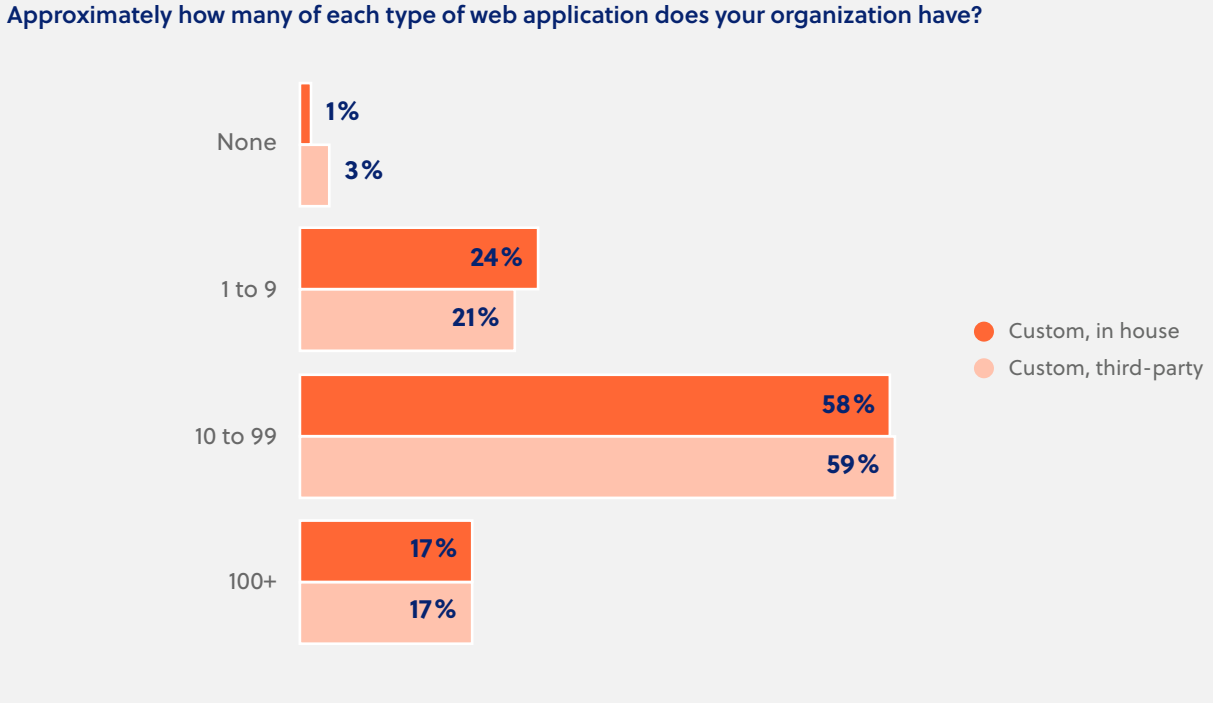
# Understanding Production Web Applications

Web application attack surfaces are large, change frequently, and are challenging to protect.

## How expansive are modern attack surfaces?

They are both extremely large and growing. More than one in every six respondents works for an organization with over one hundred web applications currently in production. Larger enterprises tend to have more, with some running thousands of web apps.

Figure 1: Number of web applications

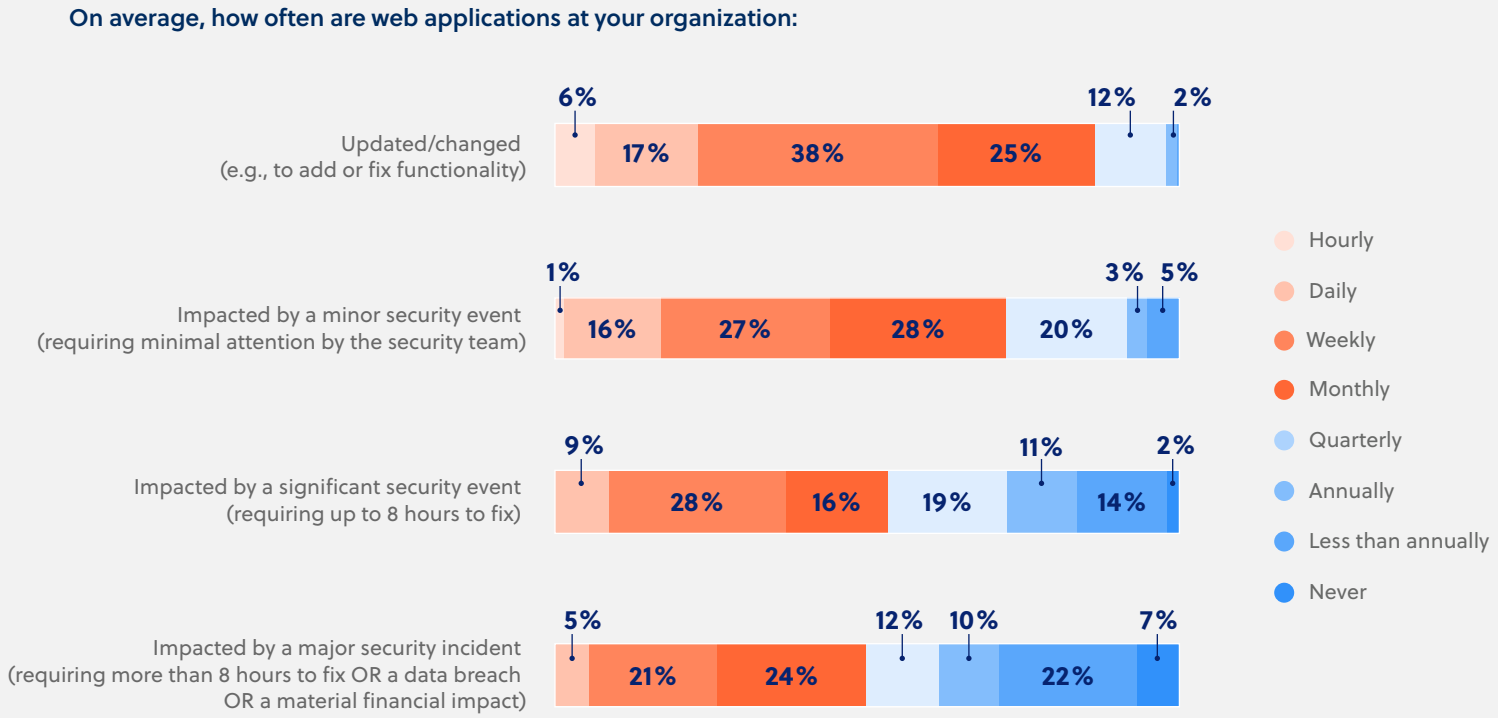



Today's organizations operate many web applications, about half of which were built in-house and half by external developers. Three-quarters of respondents (75%) have more than ten custom web apps their organizations developed in-house, and the same number (75%) have more than ten custom web apps that were built by a third party. Most respondents (58-59%) manage between ten and 99 web apps of each type, with nearly 20% maintaining more than 100.

## How rapidly are these attack surfaces changing—and how often are they attacked?

Continuous delivery is the norm in today's organizations, with most respondents reporting that their web applications are being updated on a weekly basis. More than one quarter (26%) of respondents' organizations are impacted by at least one major security incident a week.

Figure 2: Web application changes and attacks




On average, 61% of web applications are being updated weekly, or more often. An even larger group (87%) is being updated at least once per month.

Security events, incidents and breaches are arriving at almost as rapid of a pace. Close to half of respondents (44%) work for an organization that experiences a minor security event at least once a week, while nearly three-quarters (72%) are impacted by such an event monthly or more often.

More than one-third of respondents (35%) experience a significant security event at least once each week, and more than one-quarter (26%) experience a major incident at least weekly.

## What are stakeholders' biggest web application security concerns?

We asked survey participants how they perceive five major risks to their web apps.

Figure 3: Web application security concerns


Respondents cited threats to their organization's web apps as their area of greatest concern, underlining the overall importance of web applications and their security.

The second-most highly ranked concern was lack of collaboration. Multiple teams—development, operations, IT, and security—are typically responsible for attack surface management. Traditionally, siloes between them have created a disconnect, impeding collaboration and shared visibility. DevSecOps evolved to address this issue, but our findings suggest it's not yet as widely embraced as it needs to be.

Third-most highly ranked was concern about the effectiveness of existing tools. Organizations struggle with the ineffectiveness of the tools they are using to protect their web applications. An example may be web application firewalls (WAFs). While WAFs provide important detection and blocking capabilities, these may not be enough to protect critical operational processes.

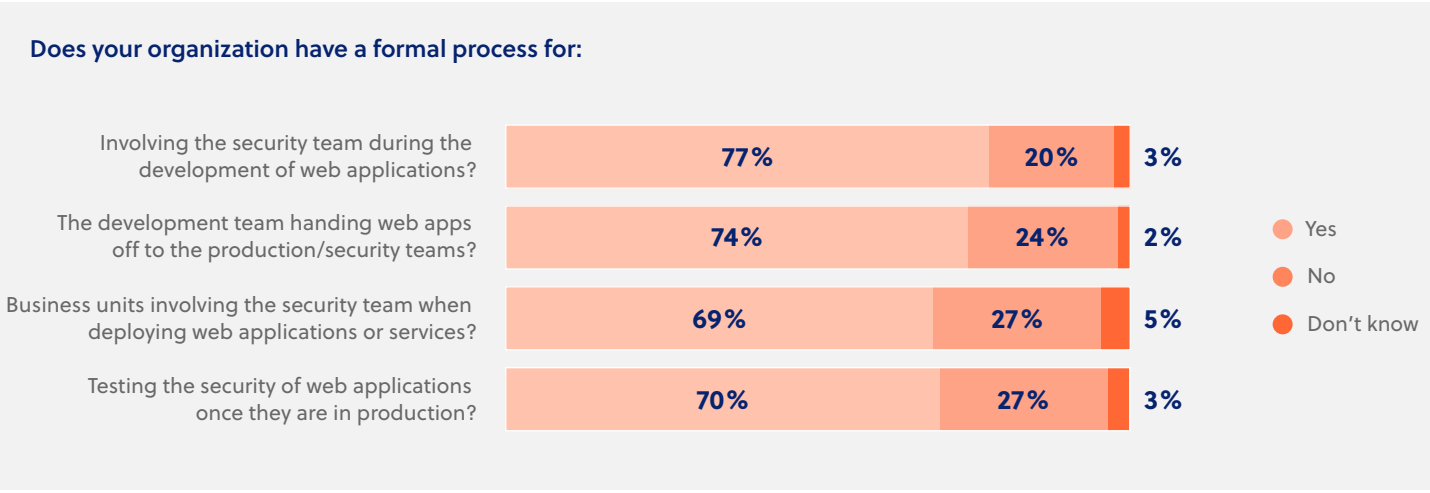
# Web Application Testing Processes, Coverage, and Challenges

Comprised of an ever-changing array of cloud services, SaaS apps, and custom web apps, today's enterprise attack surfaces are sprawling. Infrequent testing and low coverage are top contributors to enterprise risk.

## Do organizations have well-planned, strategic web application security programs?

About one-quarter of respondents report that their organizations are lacking key processes to drive and define effective web application security programs.

Figure 4: Web application security programs




Dismantling internal silos—especially between security and development teams—is now a familiar concept, one that's been popularized in the DevSecOps approach. Many enterprises claim they have implemented DevSecOps. Nonetheless, one in five respondents (20%) said their organization did not have a formal process in place for involving the security team in web app development.

Nearly one quarter (24%) reported that their organization lacked a formal handoff process when web apps were delivered into production and security teams became responsible for testing, monitoring, and protecting them. An even larger percentage (27%) said that individual business units didn't have a process for involving the security team in web app deployment, while a similar number (27%) had no process for testing the security of web applications once in production.

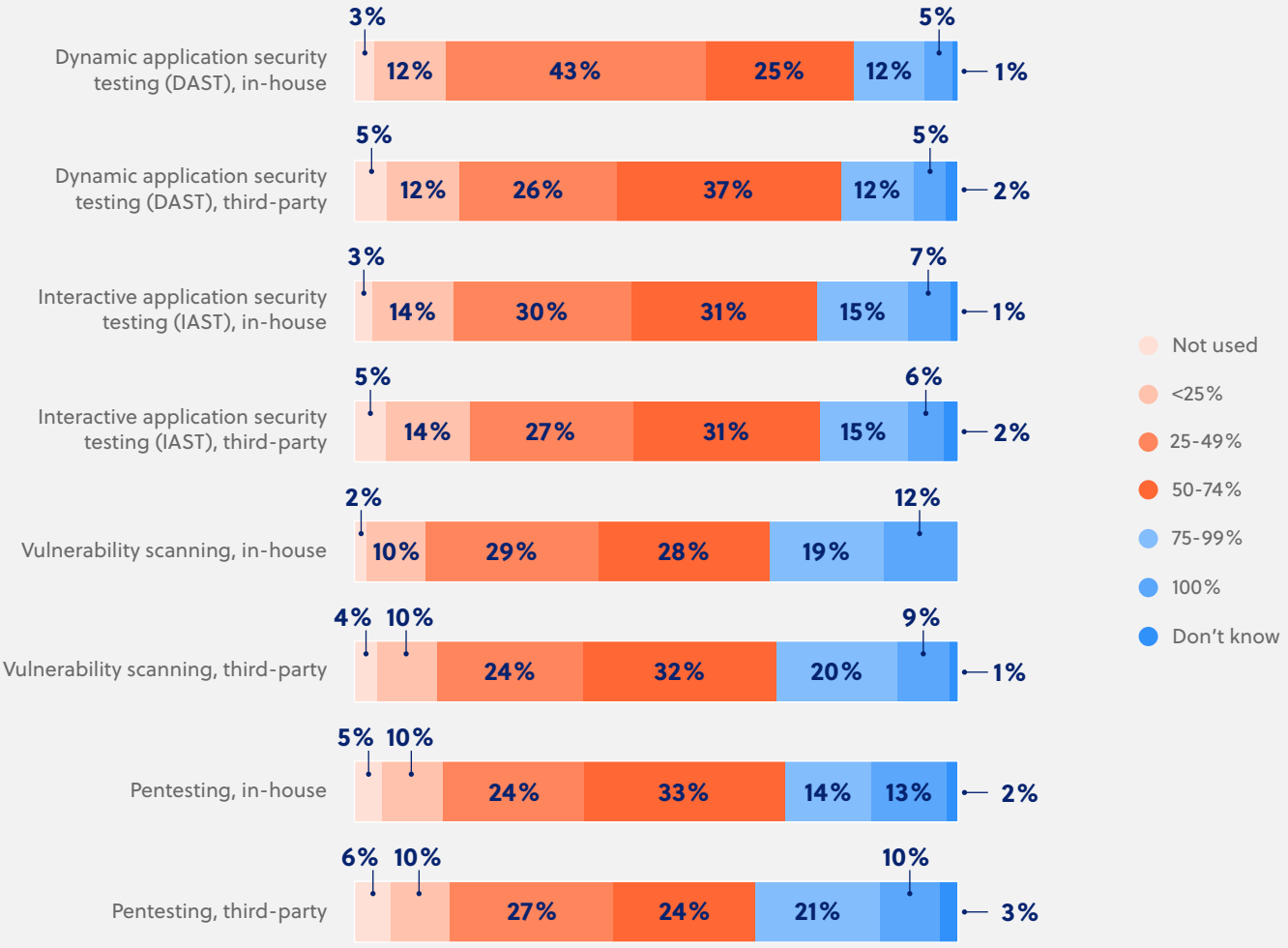
This isn't surprising: with accelerating demands for ever-faster delivery, involving security teams in development and handoff can be easy to overlook.

## How broad is web application security testing coverage?

Organizations are employing multiple test types and techniques, including dynamic application security testing (DAST) and penetration testing, to find vulnerabilities in their production web applications.

Figure 5: Web application security testing coverage

**How extensively does your organization use each security testing tool/method to uncover vulnerabilities, misconfigurations, and other weaknesses in production web applications?**




Penetration testing (pen testing) and vulnerability scanning are used somewhat more than the other testing methods, particularly when we consider the organizations that are able to achieve broader coverage of their web app attack surfaces, i.e., more than 50%. Interactive application security testing (IAST) and dynamic application security testing (DAST) are being used to cover similar portions of the attack surface; in both cases, approximately half of web apps are being tested.

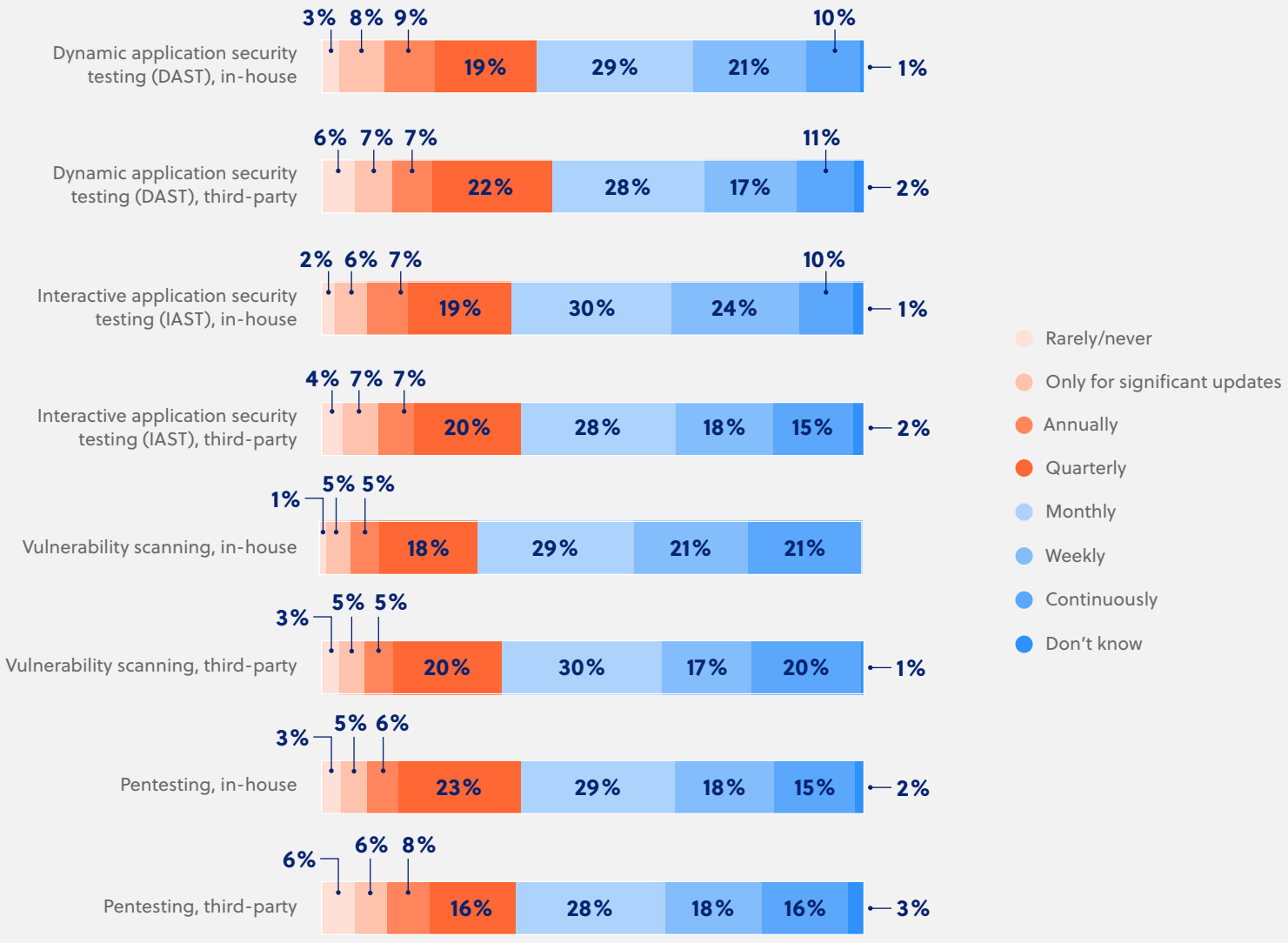
Legacy tools like vulnerability scanners lack automated discovery capabilities, so they require frequent re-configuration to keep pace with the changes in application environments. More often than not, this labor-intensive process leaves unmanaged web apps untested.

Pen testing can provide a clear picture of how an attacker might gain access to an environment, but it is expensive and time-consuming. Its labor-intensive nature means it's usually conducted no more often than once or twice each year, and only on a small fraction of the organization's web apps.

## How frequently are organizations testing the security of their web applications?

Coverage of the web application attack surface is important, but it needs to be understood in conjunction with testing frequency. For example, if you are conducting vulnerability scans on 80% of your web applications, but only doing this testing on an annual basis (or even less often), your risks remain significant.

Figure 6: Web application security testing frequency




For all of the types of testing in this survey, approximately 60-70% of organizations are testing monthly or less often. Approximately 30-40% of testing (of all types) is being conducted quarterly or less frequently. As many as 10% of respondents indicated that their organizations are testing web apps only once a year or just for significant updates.

This testing frequency is inadequate to protect against present-day threats. Organizations must conduct testing regularly and comprehensively in order to uncover and mitigate risks effectively.

# The Benefits of Continuous Monitoring

Continuous monitoring requires ongoing visibility into an organization's digital assets and infrastructure. This helps the organization stay ahead of the constantly changing threat landscape. Adopting continuous monitoring brings several key benefits.

- **Manage Risks Proactively**
  Traditional cybersecurity approaches are reactive by design. This leaves the organization vulnerable to the next as-yet-undiscovered threat. Continuous monitoring detects vulnerabilities early, reducing the probability that an attack will succeed.

- **Prioritize Remediation Activities**
  Not all vulnerabilities pose the same degree of risk to the organization. By continuously monitoring and assessing risks, it is possible to prioritize and allocate resources appropriately. This way, the most critical threats will be addressed first.

- **Act with Confidence**
  Continuous monitoring provides valuable insights into the organization's security posture, the effectiveness of its defenses and the nature of the threats it faces. These insights can be used to inform decision-making, guide security strategy development and identify areas for improvement.

## How often are organizations relying on SaaS providers to conduct web application security testing?

More than three-quarters of respondents (77%) expect their cloud provider to do at least some security testing and remediation.

Figure 7: Reliance on SaaS providers for web application security testing

**To what extent does your organization rely on the SaaS provider to perform security testing and remediation of SaaS applications used by your organization?**

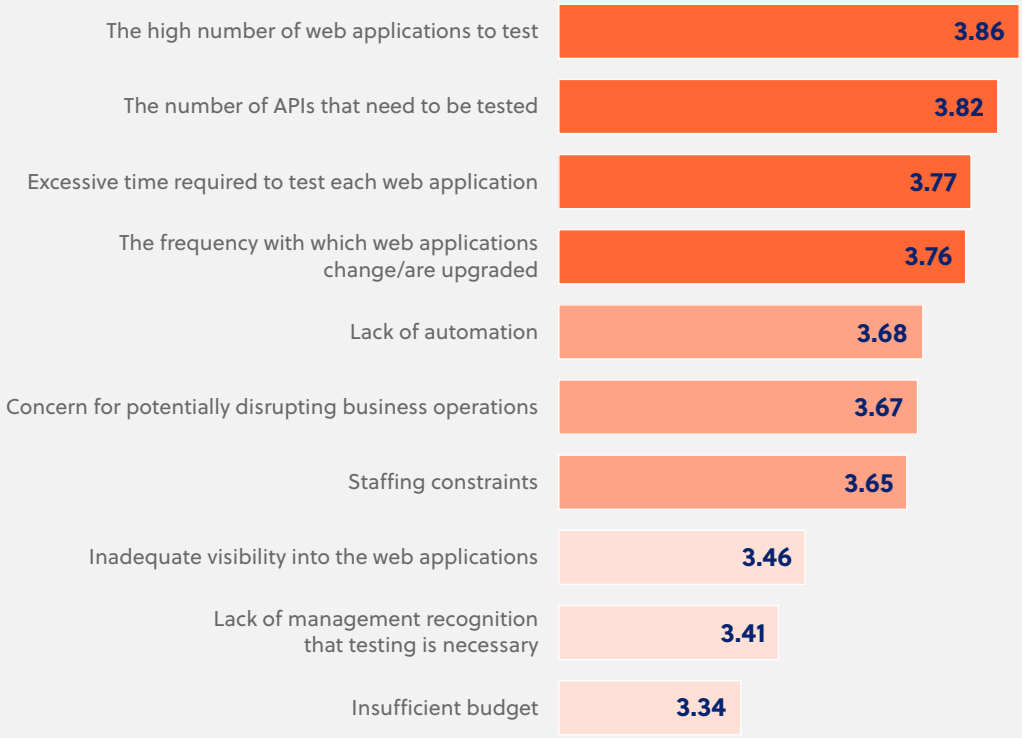

More than one in five respondents (20%) said their organization relies *exclusively* on SaaS providers to test and remediate security issues impacting the SaaS apps they use, while 77% of respondents are at least somewhat reliant upon their SaaS provider for this. Nearly one-quarter of respondents (23%) do most of their own testing. Many SaaS vendors focus their application protections primarily on access control, an approach that doesn't prevent attackers from turning compromised credentials into "the keys to the kingdom."

## What's holding organizations back from building effective web application security testing programs?

Large numbers of web applications and APIs and the time required to test are the greatest inhibitors to the effectiveness of testing programs.

Figure 8: Inhibitors to successful web application security testing

**On a scale of 1 (not at all) to 5 (extensively), rate how each of the following inhibits your organization's ability to test production web applications for security issues or weaknesses:**




The most-mentioned inhibitor was the number of web apps in need of testing, closely followed by the number of APIs. The time testing takes was also highly ranked, as was the ever-changing nature of web apps. Too little automation, worries about disruption to the business, and staffing shortages rounded out the top seven.

All of these responses indicate that web app security testing takes more time than resource-constrained teams have at their disposal.

Interestingly, neither a lack of management recognition of the problem nor insufficient budget appeared among the top responses. This is evidence that security leaders are increasingly aware of the significant security risks posed by web application vulnerabilities and are allocating funding accordingly.

# Leveraging Automation in Web Application Security Testing: Best Practices

Automation can save time, effort, and money, but only if automated workflows are easy to implement and use. To ensure that an automated solution won't cause more problems than it solves, look for one that:

- Doesn't add noise with false positives
- Can filter out low-priority issues or events that don't require immediate attention
- Will prioritize the most relevant issues through analysis of context and intelligence
- Can automatically create events, tickets, and workflows based on different use cases
- Integrates with popular incident management platforms and security orchestration solutions out of the box
- Will attribute discovered assets to the business unit or entity that owns them, reducing confusion and making it so that stakeholders clearly understand which steps to take next

# Vulnerability Remediation

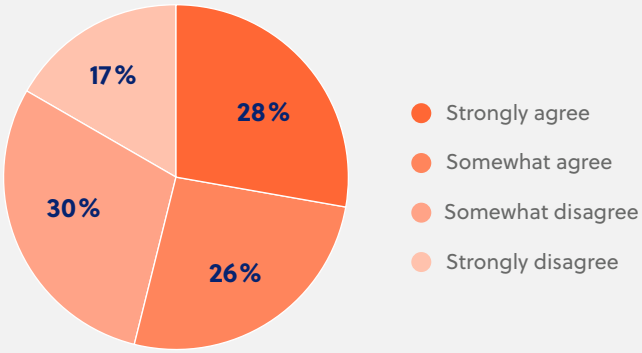
The number of common vulnerabilities and exposures (CVEs) disclosed monthly has increased more than tenfold over the past decade,[2] making it impossible for resource-constrained teams to be able to patch everything right away. Thus, prioritization is critical.

## Is web application security testing helping organizations mitigate real-world risks?

To mitigate risks successfully, security teams need to remediate the vulnerabilities the security tests uncover in a timely fashion, addressing the most pressing risks first.

Figure 9: Challenges operationalizing results

**Describe your agreement with this statement: "In general, our organization struggles to operationalize the findings of our application security tests (i.e., remediate or mitigate the issues uncovered)."**




More than half (54%) of respondents struggle to remediate the vulnerabilities their web application security tests reveal. Nearly one third (28%) strongly agree that they are not able to readily operationalize vulnerability test findings.

Though this is a high number, it may not capture the full picture. Most organizations test only a fraction of their web applications, and don't test them continuously, so vulnerabilities may remain undetected for long periods of time.

The challenges are even greater for the very largest enterprises. More than two in three respondents from organizations with more than 25,000 employees generally agree that their organizations struggle to operationalize web application security test findings.

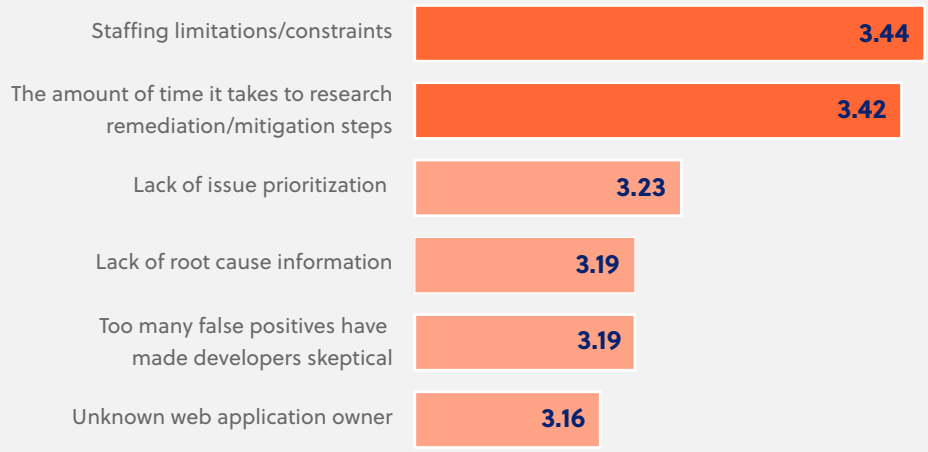
2. Coalition, Cyber Threat Index 2023.

## When it comes to remediating web application vulnerabilities promptly and effectively, what's holding organizations back?

In an industry where the skills gap is pervasive, it's no surprise that staffing shortages make vulnerability remediation difficult to accomplish, especially when workflows are complex and time-consuming.

Figure 10: Challenges remediating issues

**On a scale of 1 (not at all) to 5 (extensively), rate how each of the following inhibits your organization's ability to remediate or mitigate security issues/weaknesses with its web applications:**




For respondents, staffing constraints are the biggest inhibitor to effectively mitigating the security risks that web application security testing reveals. The amount of time it takes to research remediation/mitigation steps closely follows, evidencing that today's security professionals are very much in need of guidance on what to do with test results.

Slightly lower ranked, but also important, is a lack of issue prioritization.

# What's Next: Future Plans and Needed Capabilities

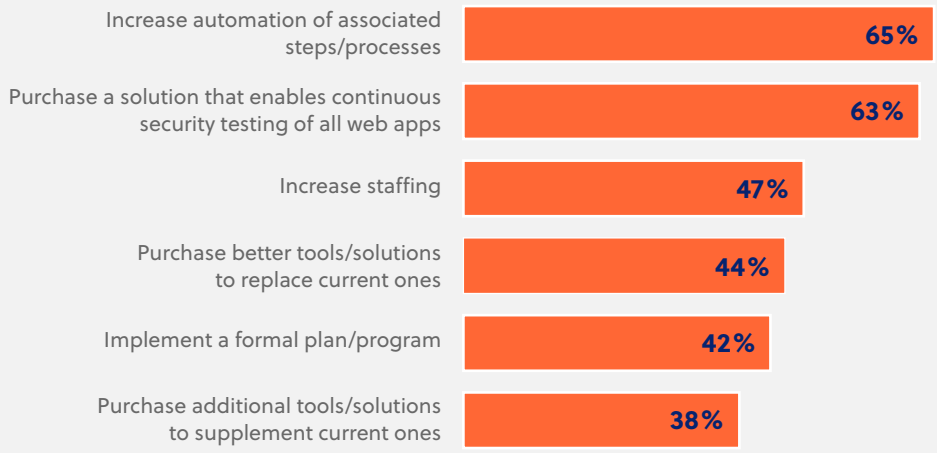
With significant numbers of today's data breaches beginning with the compromise of a web app,[3] it's mission-critical for organizations that want to mitigate real-world risk to focus on improving their web application security testing programs.

## What steps are organizations taking to boost their ability to secure web applications?

Nearly two thirds (65%) of respondents prioritize increasing automation in their web application security testing over the next year.

Figure 11: Web application security testing priorities

**What are your organization's top priorities over the next 12 months for improving web application security testing and remediation? Select three.**




Given the amount of manual work in today's web application security testing workflows—especially for remediation—it's no surprise that incorporating automation tops the list of responses. Nearly two-thirds of respondents (65%) cited this as one of their top priorities for the coming year. Interest in purchasing a solution that enables continuous security testing is also running high.

Mid-sized and larger organizations (those with more than 5,000 employees) are more interested in adding continuous testing to their web application security processes, even over automation.

When it comes to implementing new web application security capabilities, respondents generally prefer to purchase new tools instead of supplementing existing ones. This could be evidence that many of the existing approaches (including vulnerability scanning) are inadequate and ineffective, and there is strong need for a new approach.

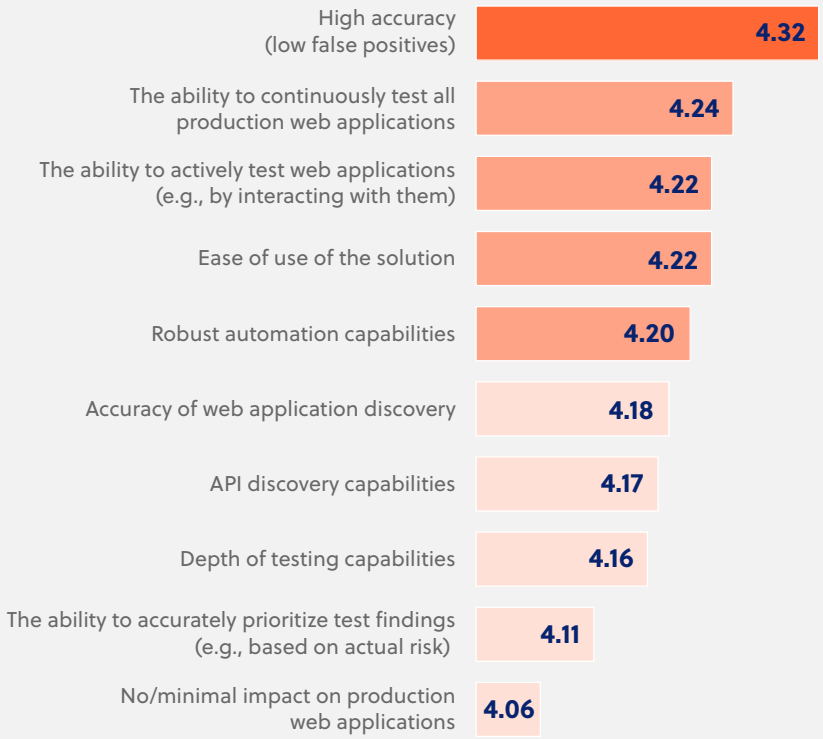
3. Acunetix, Web Application Security Without Compromise: A Buyer's Guide.

## What capabilities are security stakeholders looking for in a new web application security testing solution?

When time and labor are in short supply, it's essential to minimize wasted effort. This likely explains why high accuracy (and a low false positive rate) topped the list of respondents' must-haves in a new web application security testing solution.

Figure 12: Desired capabilities in web application security testing solutions

**On a scale of 1 (not at all) to 5 (extremely), rate the importance of each capability for an ideal web application security testing product:**




High accuracy (meaning a low false positive rate) was the most important capability in a new web application security testing solution among respondents. Also highly ranked were the ability to continuously test all web applications in production, the ability to actively test web apps, the solution's ease of use, and robust automation capabilities.

We were surprised to see a couple of issues near the bottom of the list: the ability to prioritize test findings on the basis of risk and impact on production applications. Both of these things *should* be of importance. Prioritization matters when stakeholders often find themselves with too few people and too much to do. Having no (or minimal) impact on production web applications also matters. It may be that security teams are so accustomed to testing a non-production instance of the application they don't even consider "live" testing to be an option.

It's important to keep in mind that these responses are tightly clustered, with the average respondent rating every single one higher than four on a scale of one to five. Even the lowest-ranked capabilities are still very much desired in a new web application security testing solution.

# Live web application security testing: Why it matters

It's common practice to test an offline copy of apps. But many elements may be missing from that copy, typically running in a sandboxed environment. The non-production instance usually doesn't have (among other things):

- Access to live databases
- Protection under a web application firewall (WAF)
- Access to shared an identical version of open source libraries
- Authentication mechanisms identical to those running in production

For all these reasons, testing an offline copy introduces uncertainty into test results.

# The Next Generation of Web Application Security Testing

Organizations commonly test only a small portion of their external-facing web applications. What's needed to effectively mitigate these significant and growing real-world risks is active application security testing that's conducted frequently or continuously across the entire asset inventory. The only way to achieve this is to leverage automation—but it must be done in ways that are accurate and effective.

An automated active security testing solution should be able to:

- Incorporate insights from asset discovery and contextualization—so that teams can be confident that web applications aren't being missed—while eliminating labor-intensive, error-prone manual discovery processes.
- Actively test production systems without impacting performance or requiring scheduled downtime.
- Provide visibility into complex risks through payload-based dynamic testing.
- Prioritize issues based on real-world risks and potential impact to the business.
- Identify risk exposures with greater than 90% accuracy, delivering results that can be trusted.

## Introducing CyCognito Active Security Testing

The CyCognito platform performs continuous scanning and active security testing at a global scale to help security teams keep pace with the risks of today's constantly changing web applications.

### CYCOGNITO PROVIDES:

#### Continuous, Automated Discovery of Exposed Web Applications

Gain deep knowledge about assets by leveraging machine learning to discover and attribute web apps to their organizational owners, whether these are business units, subsidiaries or partners. Keep up with daily changes to IT infrastructure with ongoing discovery of security issues.

#### Intelligent Dynamic Testing

Payload-based active testing provides comprehensive visibility into complex risks. CyCognito tests for tens of thousands of attacks, including validated coverage of the OWASP top 10. Examples of tests include:

- Remote code injection
- Authentication bypass
- Data exposure detection
- Application misconfigurations
- Cross-site scripting (XSS)
- Cross-site request forgery (XSRF)
- Weak Javascript libraries
- Weak encryption
- SSO/CAPTCHA detection
- WAF detection

#### Global Scale Without Performance Impact

Web application test payloads are delivered from CyCognito's network of over 60,000 nodes spread across more than 100 countries. Individual tests are distributed across multiple test nodes to anonymize the interaction, and resource impact is carefully monitored at all times, covering both load (bandwidth) and depth (number of interactions) to ensure that there's no impact on application performance. Tests are unauthenticated; tested assets are never modified or compromised.

#### Actionable, Validated Results

Test results are collected, validated, and delivered continuously. The CyCognito prioritization engine considers test findings in relation to exploit intelligence and business context, ranking issues for remediation.

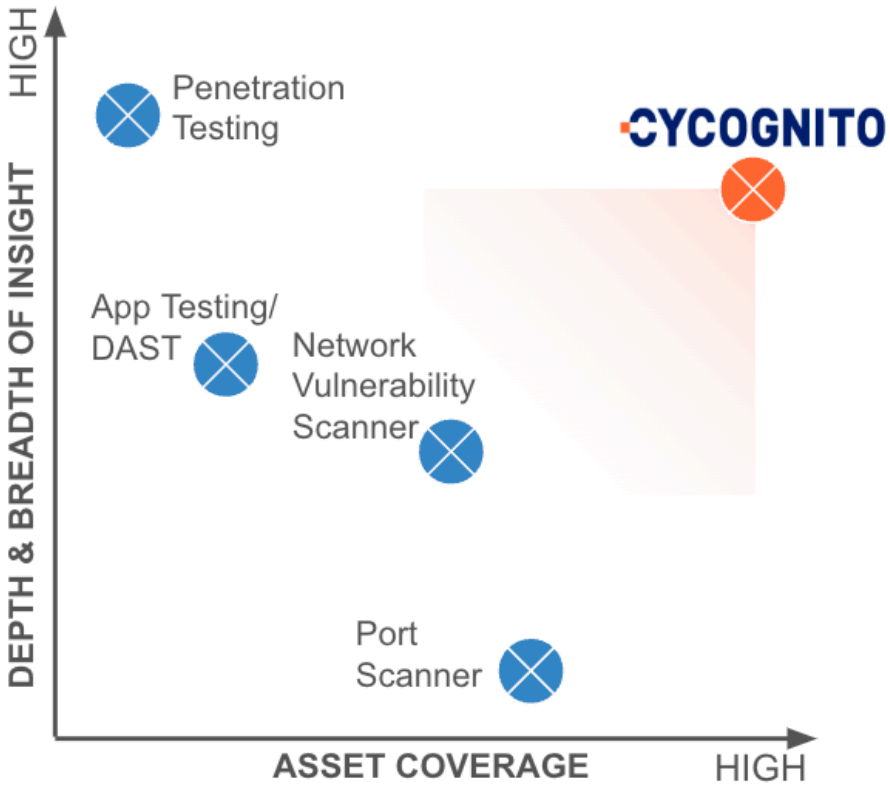
#### Web Application Security Testing Technologies

Security and IT operations teams need web application security testing solutions that reduce complexity while providing accurate, actionable results.

Even high insight across 50% of web apps leaves significant gaps. You need full asset coverage in order to confidently reduce risk.

Various technologies provide varying degrees of insight. However, due to design limitations, cost constraints, and the amount of manual effort required, they tend to be applied to too few apps.

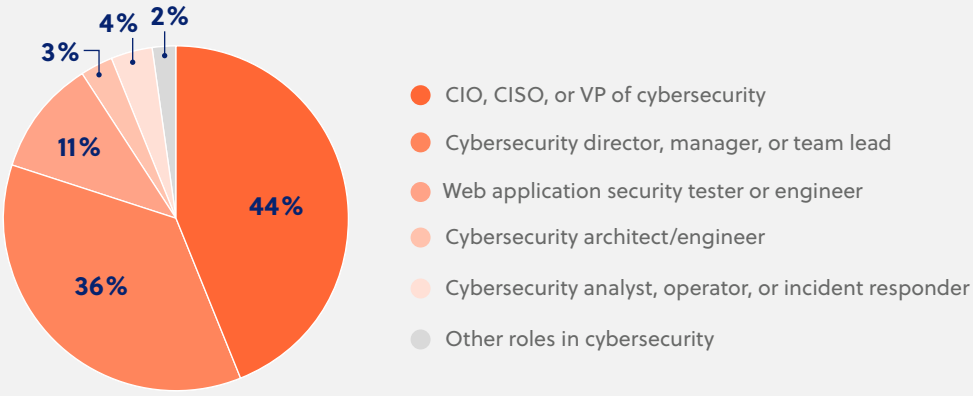
CyCognito removes the barriers to full active web application security testing, giving you high-fidelity insights with no manual effort.



## Demographics

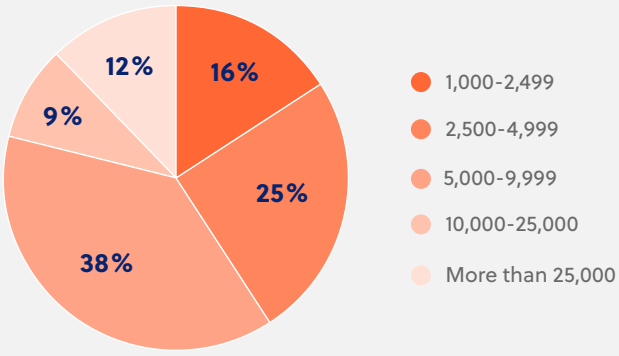
This report is based on a survey of 349 qualified professionals from the United States and United Kingdom. Participants were required to hold full-time positions as cybersecurity leaders or practitioners, with significant hands-on experience discovering, testing, and remediating vulnerabilities in public-facing web applications, or supervising others who do so. Respondents' roles included Chief Information Security Officer (CISO), Chief Information Officer (CIO), VP of Cybersecurity, and Cybersecurity Director, Manger, or Team Lead. Other participants were web application security testers and engineers, as well as cybersecurity architects, engineers, analysts, operators, and incident responders.

### Which best describes your role?




All participants in this survey came from organizations with at least 1,000 employees. The largest group (38%) was working in organizations with 5,000 to 9,999 employees, while the second-largest group (25%) was working in organizations with 2,500 to 4,999 employees. A significant percentage (21%) came from organizations with 10,000 or more employees, and 12% from major enterprises (with over 25,000 employees).

### How many employees are in your organization worldwide?



## Methodology

CyCognito and the AimPoint Group worked together to develop a 14-question survey. The survey was promoted via email to 349 cybersecurity professionals in the US and UK and administered via a web-based survey instrument. The global survey margin of error for this research study (assuming a standard 95% confidence interval) is five percent.

All respondents were required to meet three filter criteria: (1) they must have a full-time role in an organization's cybersecurity department, (2) their job responsibilities must include hands-on experience discovering, testing and remediating vulnerabilities in public-facing web applications, or supervising others who do so, and (3) they must be employed by an organization with a minimum of 1,000 employees.

## A Word from the Sponsor

CyCognito is an exposure management platform that reduces risk by discovering, testing and prioritizing security issues. The platform scans billions of websites, cloud applications and APIs and uses advanced AI to identify the most critical risks and guide remediation. Emerging companies, government agencies and Fortune 500 organizations rely on CyCognito to secure and protect from growing threats.

*For more information, visit* https://www.cycognito.com/

CYCOGNITO