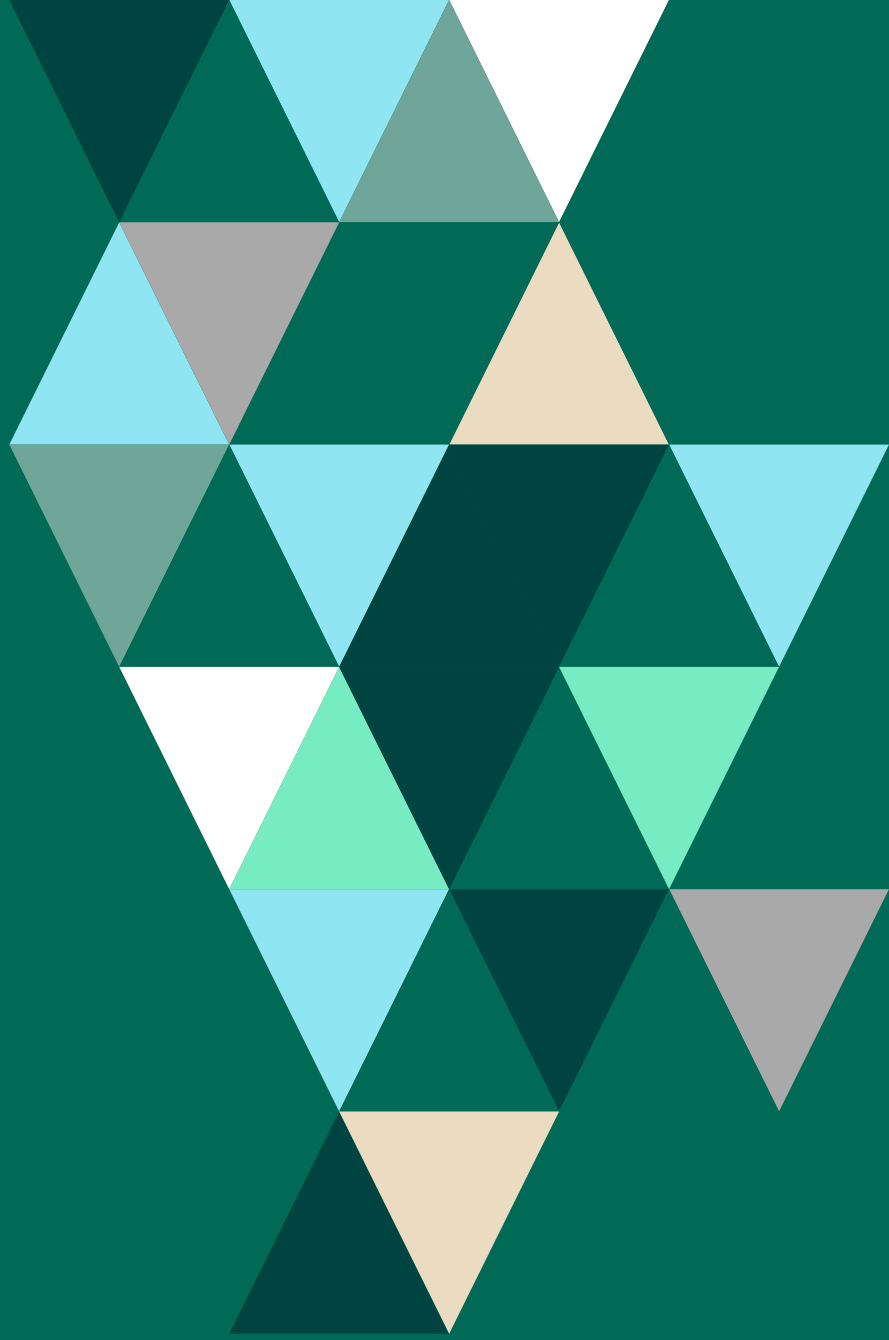
FORTRA™

2024 Penetration Testing Report



Introduction

Offensive cybersecurity practices like pen testing stand apart from other security methods. Unlike traditional defensive measures that are often forced to react to threats as they arise, offensive security can take advantage of the calm and focus that comes with planning and taking action before an attack has been launched. However, determining the most effective strategies while navigating the static of emerging threats, new security measures, and countless techniques can be a daunting task.

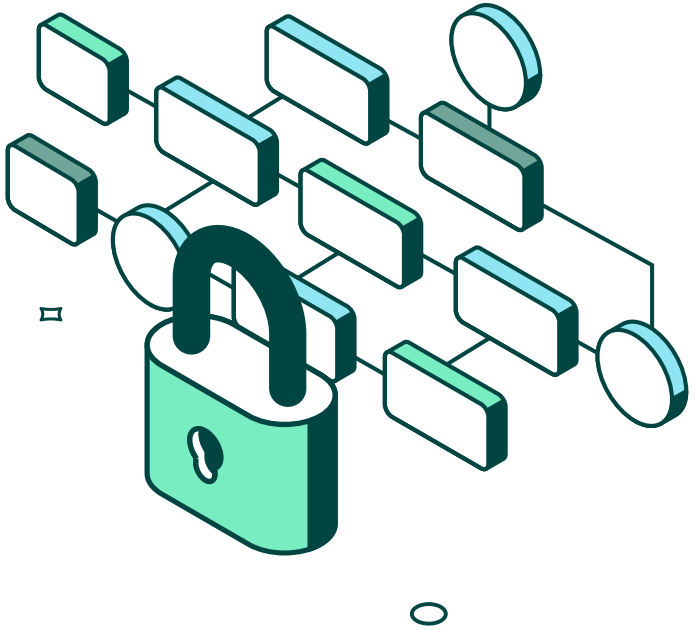
By learning how other organizations are utilizing penetration testing, we gain valuable perspectives on the efficacy of different approaches, challenges encountered, and lessons learned. Sharing knowledge empowers cybersecurity professionals to make informed decisions that align with their organization's unique needs.

With this in mind, Fortra's Core Security developed a penetration testing survey to collect, analyze, and distribute information about how cybersecurity professionals are using penetration testing and other proactive solutions.

Now in its fifth year, this survey continues to track year-over-year changes, trends, challenges, and areas of development. The information collected is a valuable resource for cybersecurity professionals who are committed to growing and maintaining a proactive, resilient security posture. This report aims to add insights into the current state of pen testing practices, providing ongoing, useful data on the following key issues related to pen testing:

- Effectiveness of pen testing in breach prevention
- Top security concerns like phishing, ransomware, and lack of patching
- Challenges with pen testing like personnel shortages and lack of remediation resources
- Relevant regulations and compliance concerns
- Usage of in-house pen testing teams
- Selecting third-party teams
- Evaluating pen testing toolsets
- Other security assessment tools like vulnerability scanning and red teaming
- Vendor consolidation
- Pen testing in different environments

In addition to examining this year's findings, we'll provide a comparison with 2023's results to gain further understanding of the progression of the penetration testing field.



Value of Pen Testing

What value does pen testing provide?

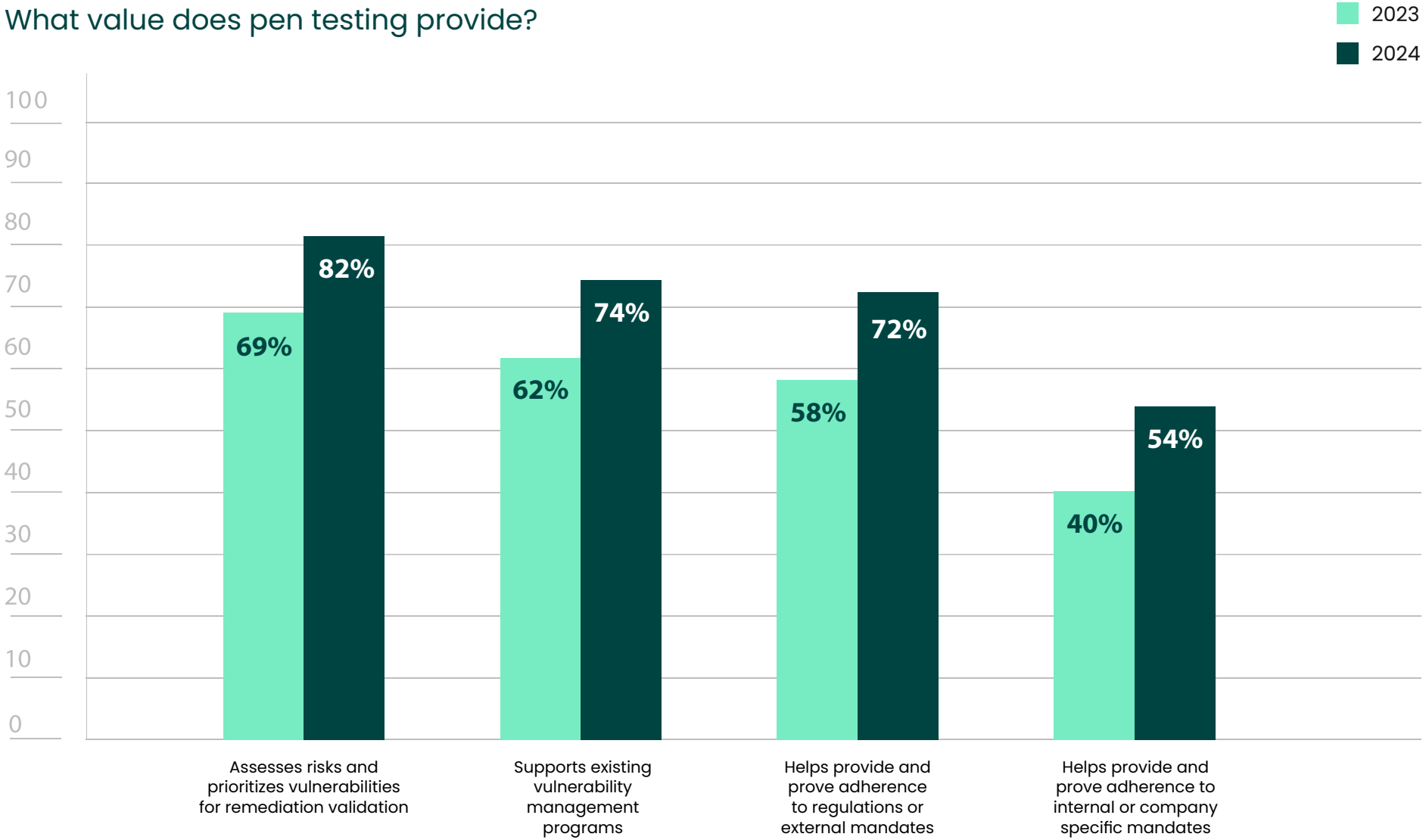


Figure 1: Value of pen tests

Value of Pen Testing

The results of this year's survey show the continued value that organizations find in penetration testing. With every category experiencing a sizeable boost from last year, organizations may also be discovering an increasing number of use cases for pen testing.

Assessing risk and prioritizing vulnerabilities for remediation is the primary objective of pen testing and a foundational offensive security practice. So, it is unsurprising that it has continued to be the most common response (82%) (Figure 1). The 12% increase from last year may be tied to the similarly sized increases reflected in those who use pen testing for external compliance (72%) and internal mandates (54%). Organizations that began using pen testing as a way to maintain and prove adherence may have quickly realized that penetration testing is much more than just a box to be ticked. Pen testing provides uniquely in-depth analysis on the potential impact of vulnerabilities being exploited. This gives insights into which weaknesses are causing the most risk, providing the most strategic path forward in closing security gaps.

Perhaps the greatest proof of the value of penetration testing is that 72% of respondents felt that pen testing has prevented a breach at their organization (Figure 2). This underscores the importance of proactive efforts that identify and address vulnerabilities before they can be exploited.

It is worth noting that the second most common value that respondents found in pen testing was its role in supporting existing vulnerability management programs (74%) (Figure 1). While some organizations may rely solely on one proactive solution, like pen testing, it is vital to recognize the value of layering offensive security. Incorporating pen testing into a unified, tactical program with complementary solutions like vulnerability scanning and red teaming enables organizations to enhance coverage and efficacy.

Do you feel pen testing has prevented a breach at your organization?

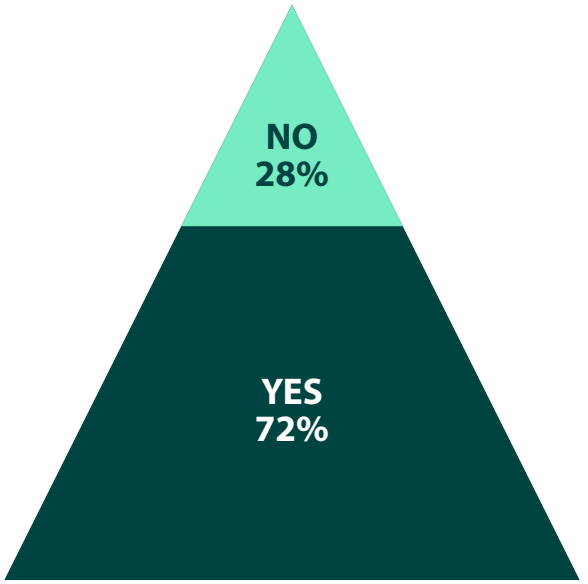


Figure 2: Efficacy of pen testing for breach prevention

Common Security Concerns

What common security risks/entry points are you most concerned about?

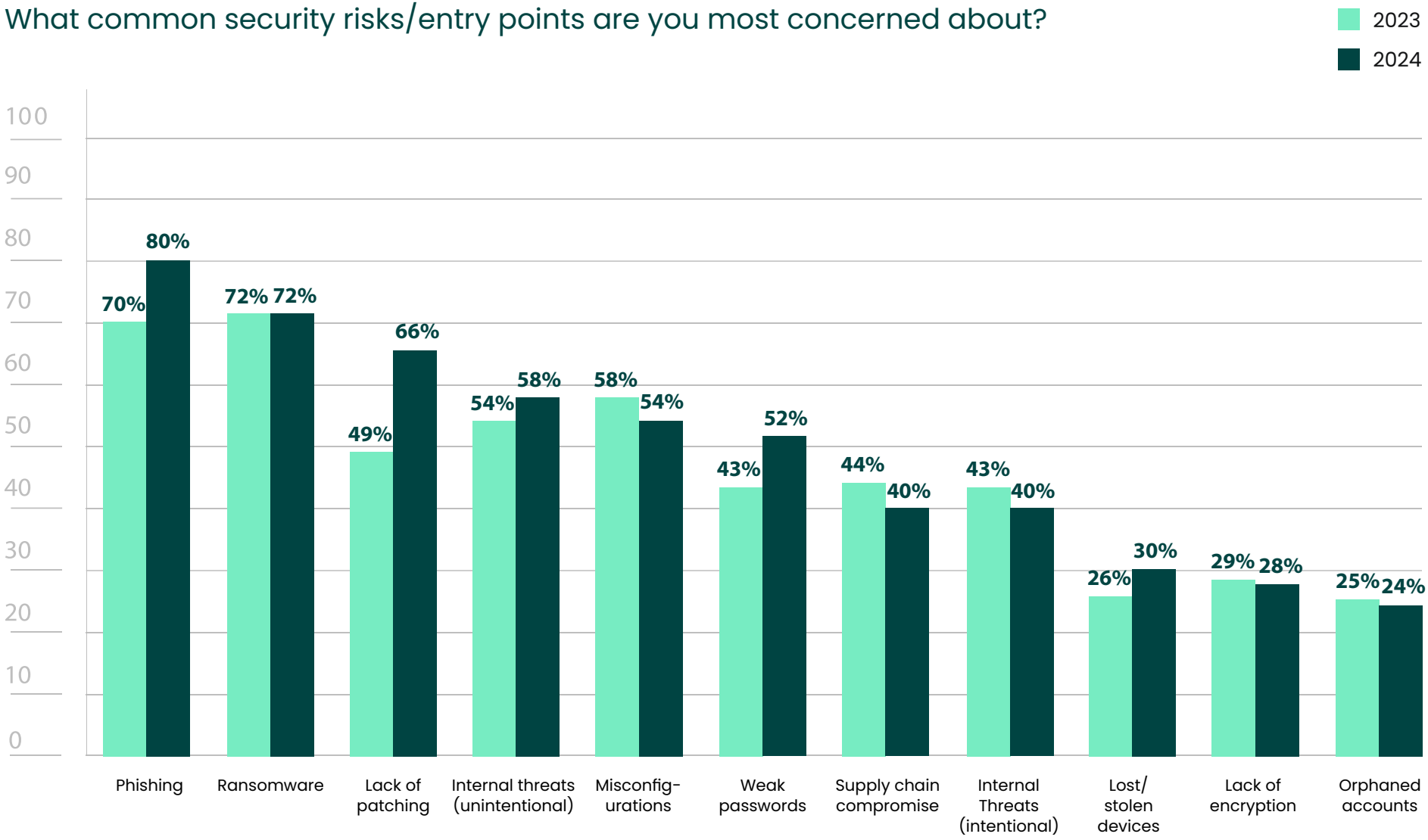


Figure 3: Common security concerns

Common Security Concerns

Phishing (80%) and ransomware (72%) were once again the top security concerns (Figure 3) for survey participants. Phishing and ransomware have remained the top two concerns for the past three years, and for good reason. The Anti-Phishing Working Group reported that 2023 was the worst year on record for phishing, with over five million phishing attacks observed.

Ransomware has also been on the rise in the past year, with SANS reporting a 73% increase in ransomware attacks. Phishing is the most common delivery method for ransomware, so it's expected that these two closely tied threats continue to dominate the concerns of security professionals.

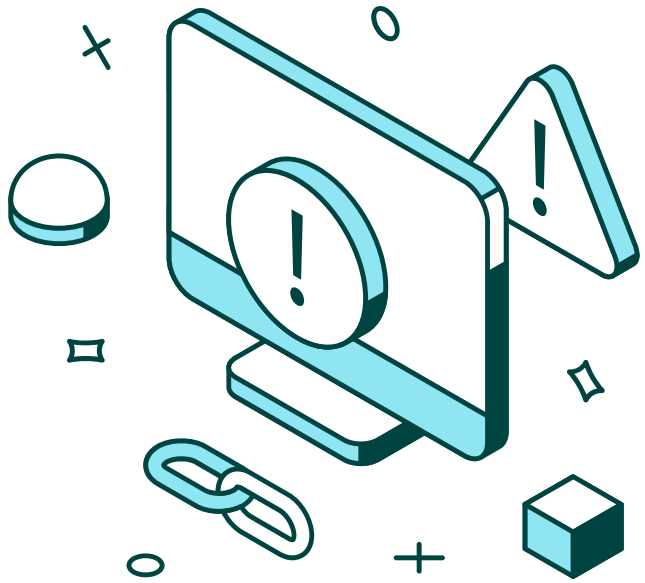
What makes phishing and ransomware such pervasive threats? A few reasons:

- Kits and services offered on the dark webhave a low barrier to entry that even allows attackers with limited skills to use them.
- Decentralized operations and the complexity of prosecuting international crime make ransomware and phishing fairly low risk, and potentially very high reward.
- Phishing and ransomware capitalize on human error, which is challenging to prevent and makes them universal methods that can target every industry.

As these threats continue to pay off year after year, it's unlikely that attackers will drop these techniques anytime soon. Consequently, organizations need to be equally committed to proactive security practices like pen testing to reduce risk as much as possible.

And speaking of the need for proactive security, lack of patching (66%) is the third most common concern—up 17% from last year (Figure 3). When vulnerabilities are discovered, the only way to ensure an attacker can't exploit it is to apply a patch as soon as it is available. And with over 1000 vulnerabilities in CISA's Known Exploited Vulnerabilities Catalog, the need for applying timely updates is more critical than ever. Though it seems a simple enough practice, there are multiple challenges that may prevent routine patching at an organization. A lack of personnel can cause patching to become deprioritized. Compatibility issues and downtime/ disruption to business may also cause delays. And the increasing complexity of IT environments means that IT and security professionals are facing hundreds of patches. Organizations should enlist the aid of vulnerability management and pen testing tools, which can automate scanning, prioritize patches based on risk, and ensure that they've been properly implemented.

With attackers continuously adapting their techniques to bypass security controls and exploit emerging vulnerabilities, the concern over phishing, ransomware, lack of patching, and other security threats is certainly not unwarranted. However, security experts are not being idle— they are also refining their strategies, regularly engaging in collaborative efforts, and leveraging new research. And by having offensive and defensive tools, engaging in regular blue team training, and fostering a culture of vigilance, organizations can do their part to stay ahead of attackers.



General Pen Testing Challenges

What challenge(s) does your organization face with your penetration testing program?

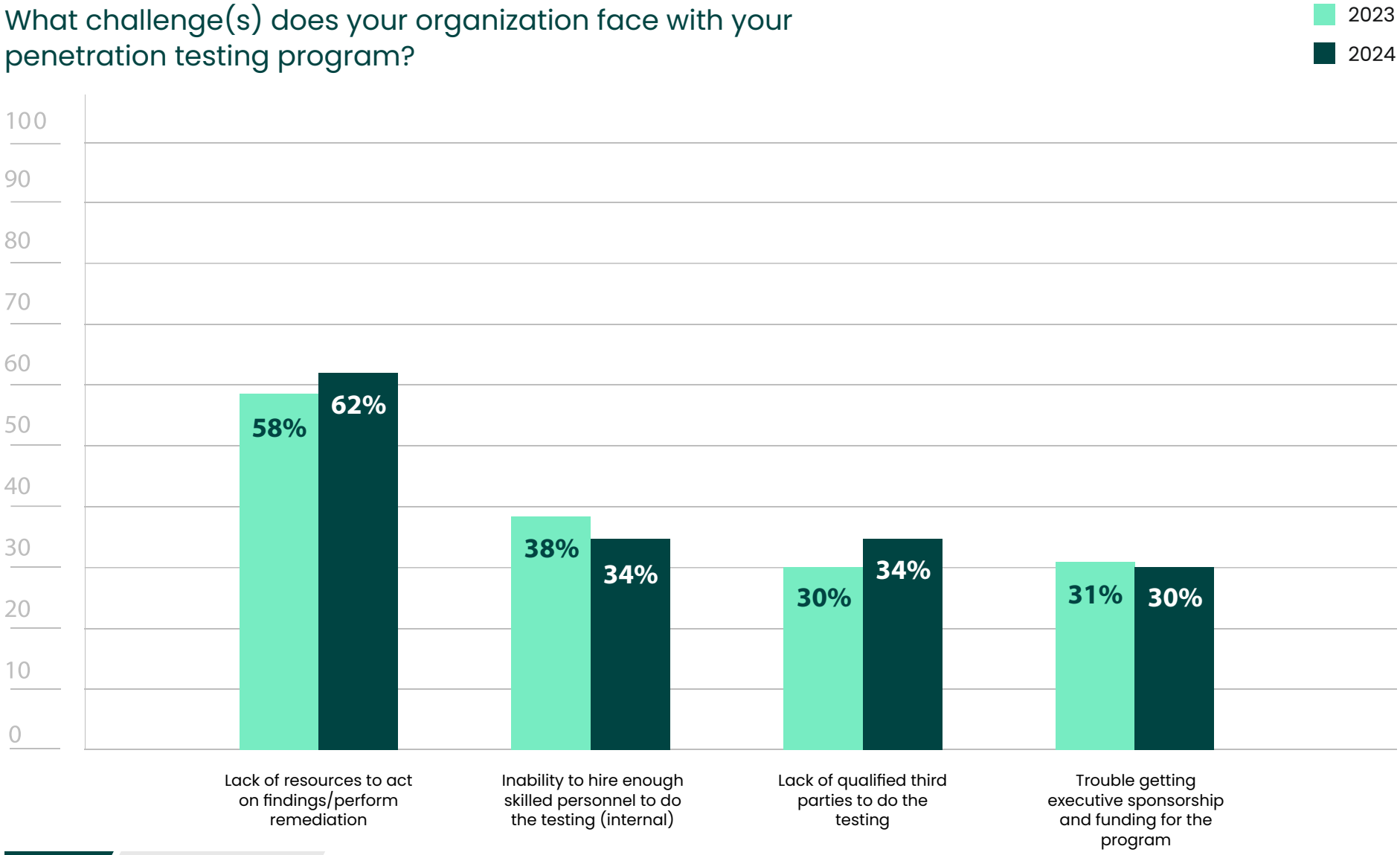


Figure 4: Pen testing challenges

General Pen Testing Challenges

Though pen testing is clearly a valuable offensive security practice, deploying and managing pen testing initiatives do come with challenges. The lack of resources to act on findings/perform remediation is still the most common challenge respondents faced (62%), up 6% from last year (Figure 4). This can occur for a variety of reasons. In certain cases, decision makers may not fully understand the urgency or severity of pen test findings. Particularly when pen tests are being run for regulatory adherence, there may be a misperception that meeting compliance mandates means the organization is fully secure. If changes are substantial and could cause disruption to regular business operations, there may also be hesitancy from decision makers to approve changes that need to be made. But the most common reason is simply that limited budgets and personnel create competing priorities and remediation falls through the cracks.

In addition to advocating for more support for remediation efforts, security teams should make sure that their remediation plans are as clearly outlined as their pen testing plans. While good pen test reports include follow-up recommendations, a remediation plan should be fleshed out in more detail. This includes outlining the specific steps required to address the highest priority risks, resources needed, timelines, and dependencies.

The inability to hire skilled personnel (34%) and the lack of qualified third parties (34%) are both likely continued evidence of the cybersecurity skills gap (Figure 4). Penetration testing seems particularly affected by this ongoing shortage. According to (ISC)²'s 2023 Cybersecurity Workforce Study, penetration testing was the fourth most common skill that SOC teams were missing. The lack of qualified third parties certainly indicates that demand outweighs supply.

Even when pen testing services are available, this does not necessary mean they are "qualified." Unfortunately, there are pen testing teams whose services consist of little more than a few automated scans. They may use deceptive marketing tactics, such as offering unrealistically low prices or fake testimonials. Additionally, malicious actors have begun creating fake companies and posing as legitimate penetration testing firms to gain access to sensitive information or credentials. This underscores the need for organizations to carefully vet potential providers to make sure they're selecting a reputable team with adequate experience. Joining the growing wait list may be frustrating, but it certainly beats getting scammed.

Compliance and Pen Testing

Unsurprisingly, PCI DSS is the most common regulation for which respondents reported using pen testing (43%) (Figure 5). While most regulations require security assessments, PCI DSS explicitly requires penetration testing. Requirement 11.3 mandates that organizations perform external and internal penetration testing at least annually and after any significant infrastructure or application change.

Even when not explicitly required, pen tests are commonly used to fulfill security assessment requirements and help verify adherence to other regulations, proving to auditors or other authorities that mandated security measures are in place or working properly. Up 11% from last year (figure 6), more organizations are having to increase the number of pen tests they are running, likely because of updates and additions in cybersecurity law and regulation.

Compliance initiatives have become a global priority, with more changes expected in the coming years. The updated Network and Information Security Directive (NIS2) expanded its requirements for risk management and is required to be transposed into the national law of all EU member countries by October 2024. The Digital Operational Resilience Act (DORA) will add risk management requirements to financial institutions beginning in 2025. According to Gartner, 75% of the global population will have its personal data under privacy regulations by the end of 2024.

Interestingly, there was a 23% increase in respondents that needed to broaden the scope of their penetration tests (Figure 6). There may be a few reasons for this. For example, supply chain attacks have led to more scrutiny over third party risk management, so organizations may feel more pressure to include third-party systems and networks in engagements. Additionally, if new or updated regulations are requiring organizations to assess more systems, budget constraints may lead them to broaden the scope instead of increasing the number of tests they're running.

Other common alterations in pen testing strategies included additional emphasis on network security tests (36%) and phishing campaigns/social engineering (30%). Down 7% from last year, only 9% of participants reported that there was no impact to their pen testing strategies as a result of compliance needs, illustrating the ongoing influence compliance continues to have on pen testing approaches.

Do you use pen testing for any of these compliance regulations?

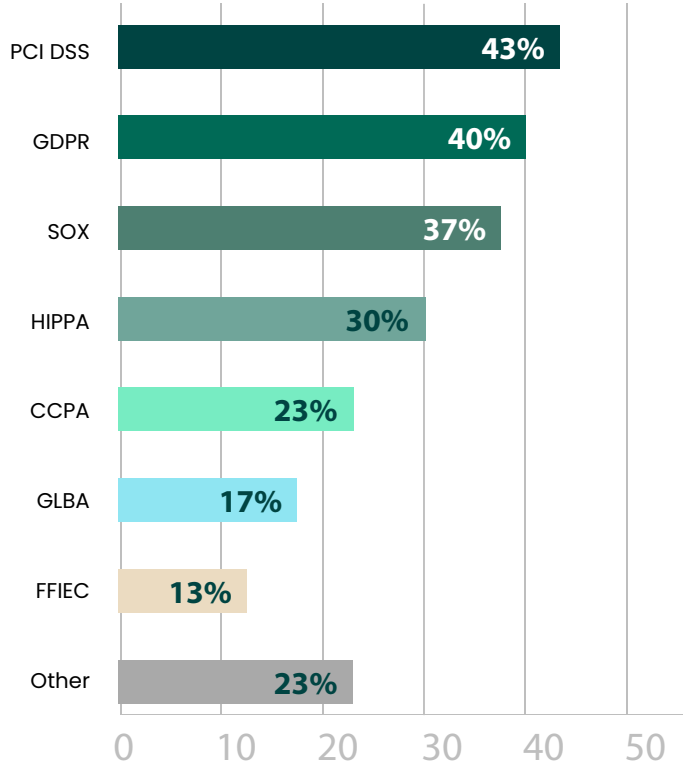


Figure 5: Compliance regulations for which pen testing is utilized

Compliance and Pen Testing

How has the increase in compliance regulations/mandates affected your pen testing strategy or priorities?

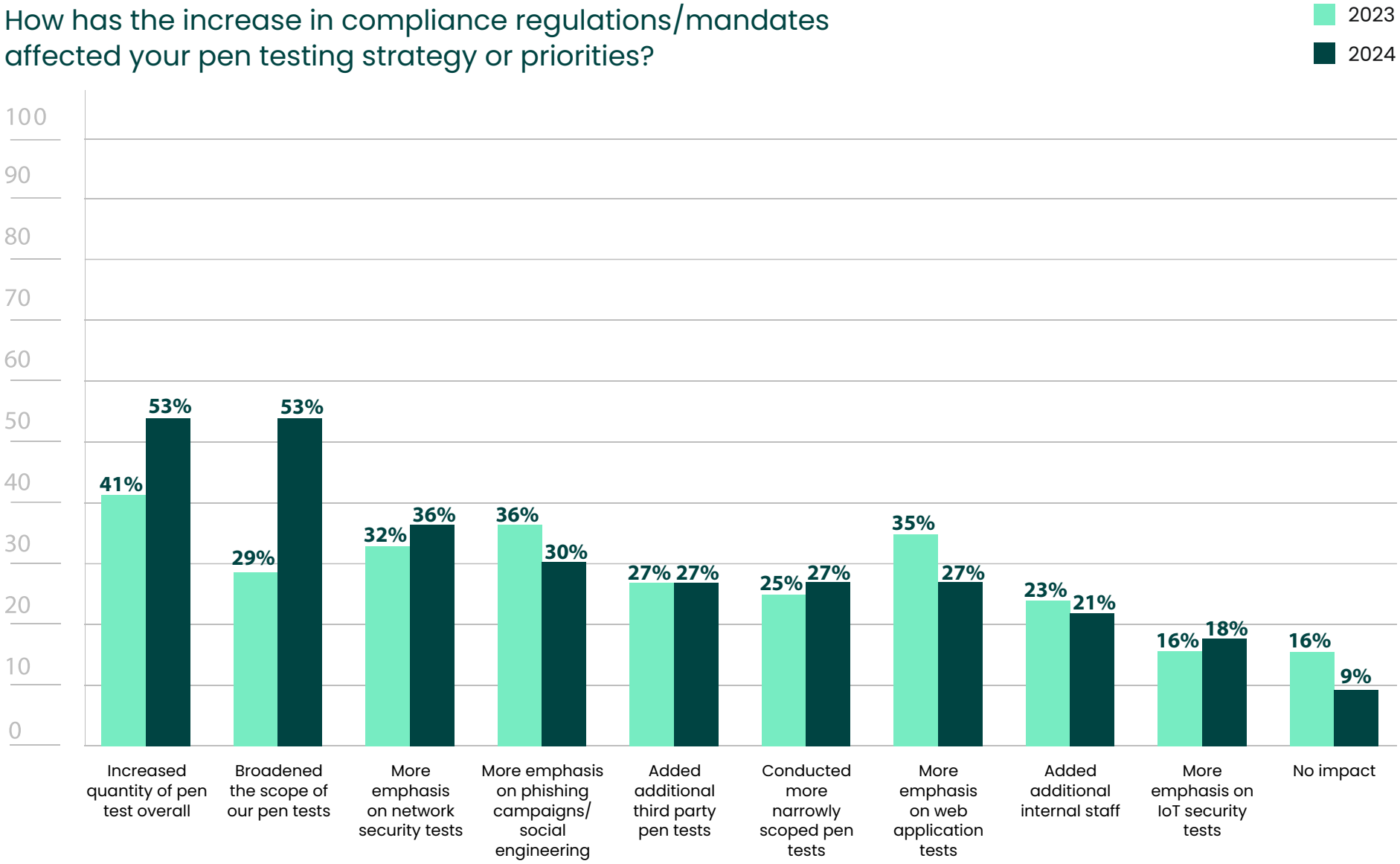


Figure 6: Impact of compliance mandates on pen testing strategies

Phishing

With estimates of over three billion phishing emails sent per day, it's no wonder that phishing was the most common security concern of respondents (80%) (Figure 3).

Though phishing attacks are nothing new, attackers are always finding ways to change up their tactics. For example, generative AI has led to an explosion of phishing emails, with a 1,265% increase in malicious emails since 2022. Business Email Compromise (BEC) attacks have also become increasingly common, with the FBI receiving 21,489 complaints in 2023 alone. And the top social engineering threat last year was hybrid vishing. This multi-staged attack strategy typically uses a spoofed email that requests the victim to follow up via phone. This enables the attacker to bypass basic security filters, since the payload is only a phone number.

As phishing is more widespread than ever, it was disappointing to see a downward trend in the frequency of social engineering exercises. Quarterly exercises were down 7%, while there was a 6% increase in participants who never run these exercises (Figure 7). Though these aren't huge shifts, given the prevalence of these attacks, social engineering exercises should only be on the rise.

Simulation exercises are one of the only ways to reduce the risk of social engineering attacks. There is a common misperception that these exercises are limited to raising awareness among employees about the tactics used by attackers. However, phishing simulations help validate security practices, providing data on how well email filters are detecting phishing emails and measuring the efficacy of training programs. They can also help improve incident response, ensuring that security teams can respond effectively to real phishing attacks.

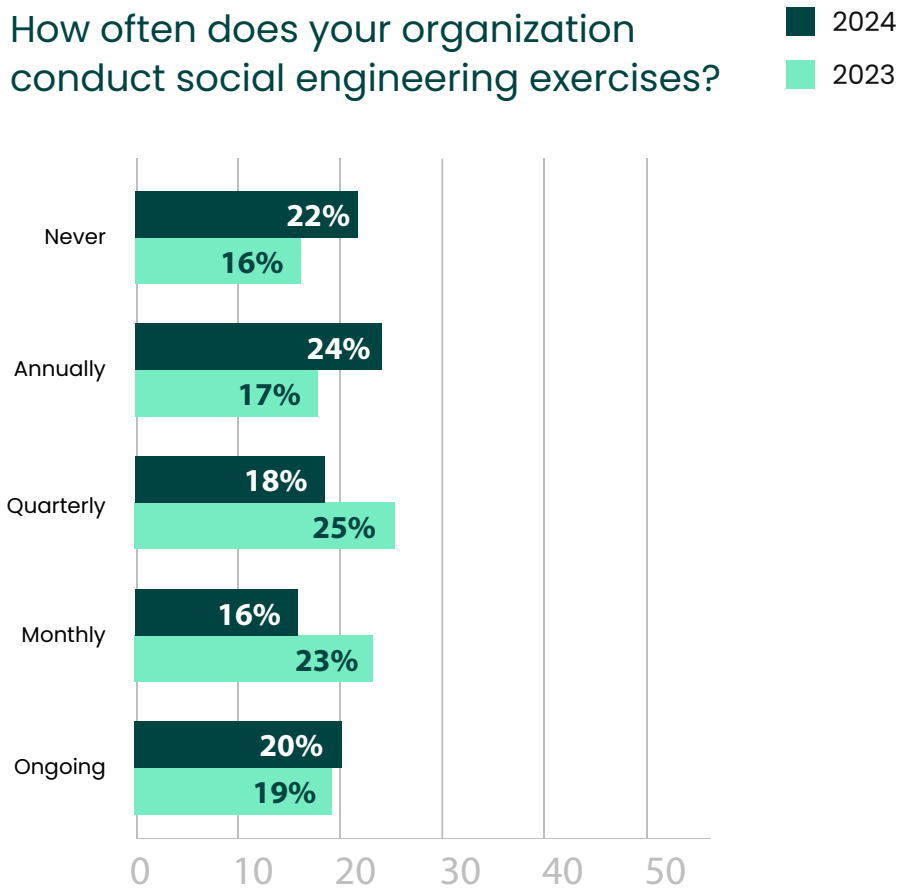


Figure 7: Frequency of social engineering exercises

Penetration Testing Frequency

As with phishing campaigns, there was a slight drop in general pen testing frequency, with a 9% decrease in quarterly tests, a 5% increase in organizations that test a couple times a year (43%), and a 3% increase in organizations that never pen test (17%) (Figure 8).

There is no magic number when it comes to pen testing frequency. Instead, it depends on the size of the organization, the complexity of its technical infrastructure, the type of data it handles, and applicable compliance regulations. Most organizations should be running at least once a year, but additional tests should be run if substantial changes are made to the IT environment, if vulnerabilities are discovered, or if a security incident has occurred.

Another reason to consider more than one test a year is to get assurance that the vulnerabilities identified during the initial penetration test have been properly addressed and remediated. This includes confirming the proper implementation of patches and the effectiveness of new security controls like firewalls, intrusion detection/prevention systems, and access controls.

Retesting in a timely manner ensures that fixes don't become new flaws. However, it is still difficult to get them approved, as evidenced by respondents encountering challenges with the lack of follow up after pen testing (62%) (Figure 4). Retesting can often be viewed as less urgent, with many stakeholders seeing initial efforts as sufficient or having reluctance about needing to make additional changes.

Ultimately, though both testing and retesting should be run more often, best practices often collide with the real-world practicalities of resources and budgets. In such cases, taking a layered approach to proactive security can be an effective approach, as vulnerability management solutions can help fill in gaps between pen tests. These solutions are typically highly automated and can easily be scheduled to run on a daily or weekly basis. This ensures that the organization can stay up to date with some form of assessment.

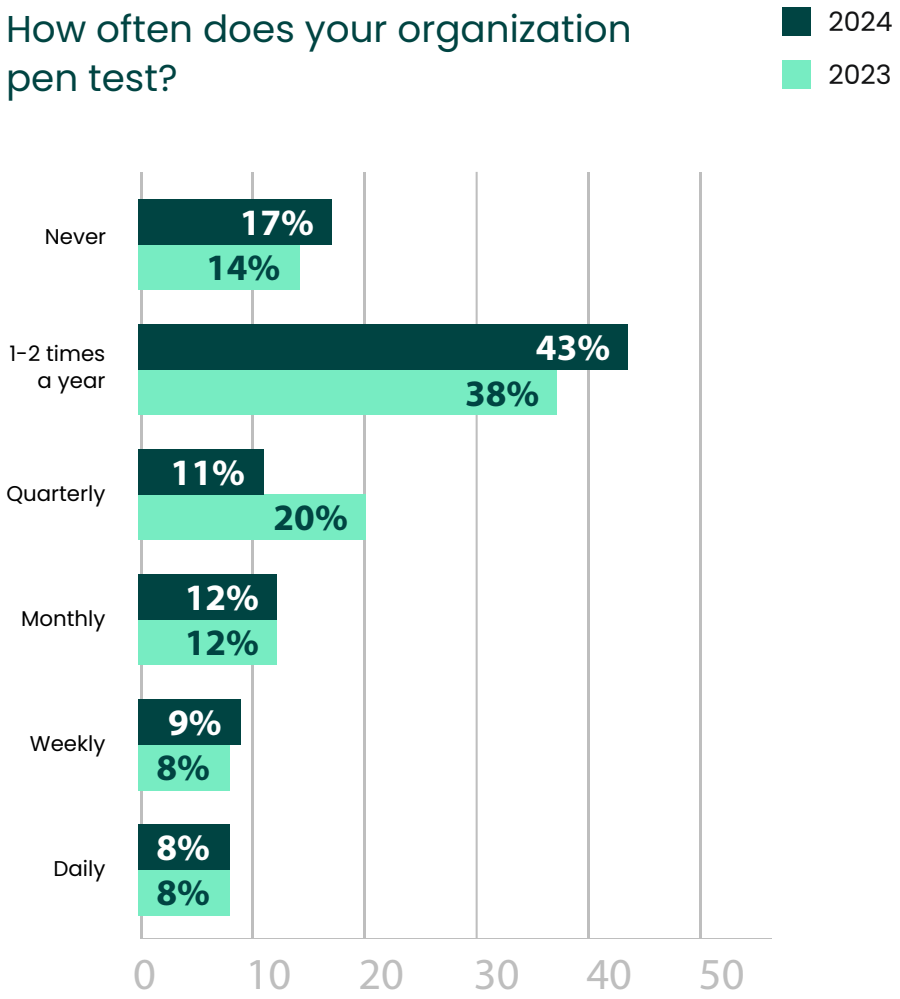


Figure 8: Frequency of penetration testing

In-House Pen Testing Efforts

Organizations may decide to add in-house pen testing capabilities for several reasons. An in-house pen testing team has more familiarity with the business operations and IT infrastructure, making it easier to tailor testing methodologies and approaches to suit the organization's specific security needs. They can also run tests more frequently, allowing them to bring attention to emerging threats in a timely manner, potentially take part in the remediation process, and retest to ensure any fixes were appropriately implemented.

This year shows a 15% decrease in the number of respondents who have in-house pen testing teams (Figure 9). However, the percentage of participants who no longer have teams stayed flat at 14%, so it does not appear to indicate that organizations are finding in-house pen testing less helpful. Instead, this decrease may be explained by the 16% increase in respondents that leverage third parties exclusively (Figure 10).

The most common reason organizations don't have in-house pen testing is a lack of need for a full-time pen tester/team (55%) (Figure 10). Smaller organizations may have relatively simple IT environments or a small attack surface, making the need for frequent or extensive penetration testing less apparent. They also might not have the foundational security controls, security awareness, or resources to be at the security maturity level that is required to begin pen testing. Alternatively, organizations may find their needs sufficiently met by having pen testing be one aspect of a broader cybersecurity role.

Having more general cybersecurity roles has been a common way for organizations to cope with the cybersecurity skills gap. The skills gap is also the second most common reason for not having an in-house pen testing team (39%) (Figure 10). According to (ISC)²'s 2023 Cybersecurity Workforce Study, the skills gap continues to widen, growing 12.6% from last year with a record high shortage of nearly four million.

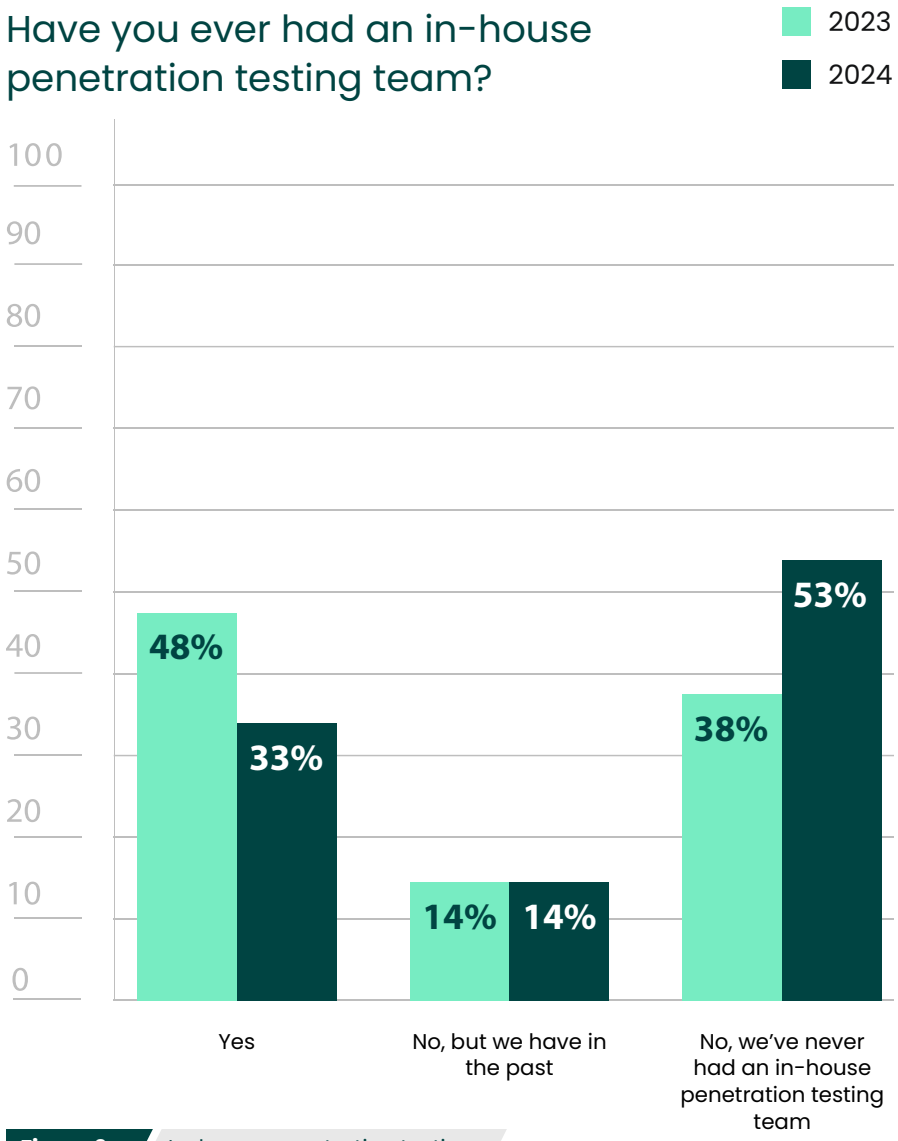


Figure 9: In-house penetration testing

In-House Pen Testing Efforts

Why does your organization not have an in-house penetration testing team?

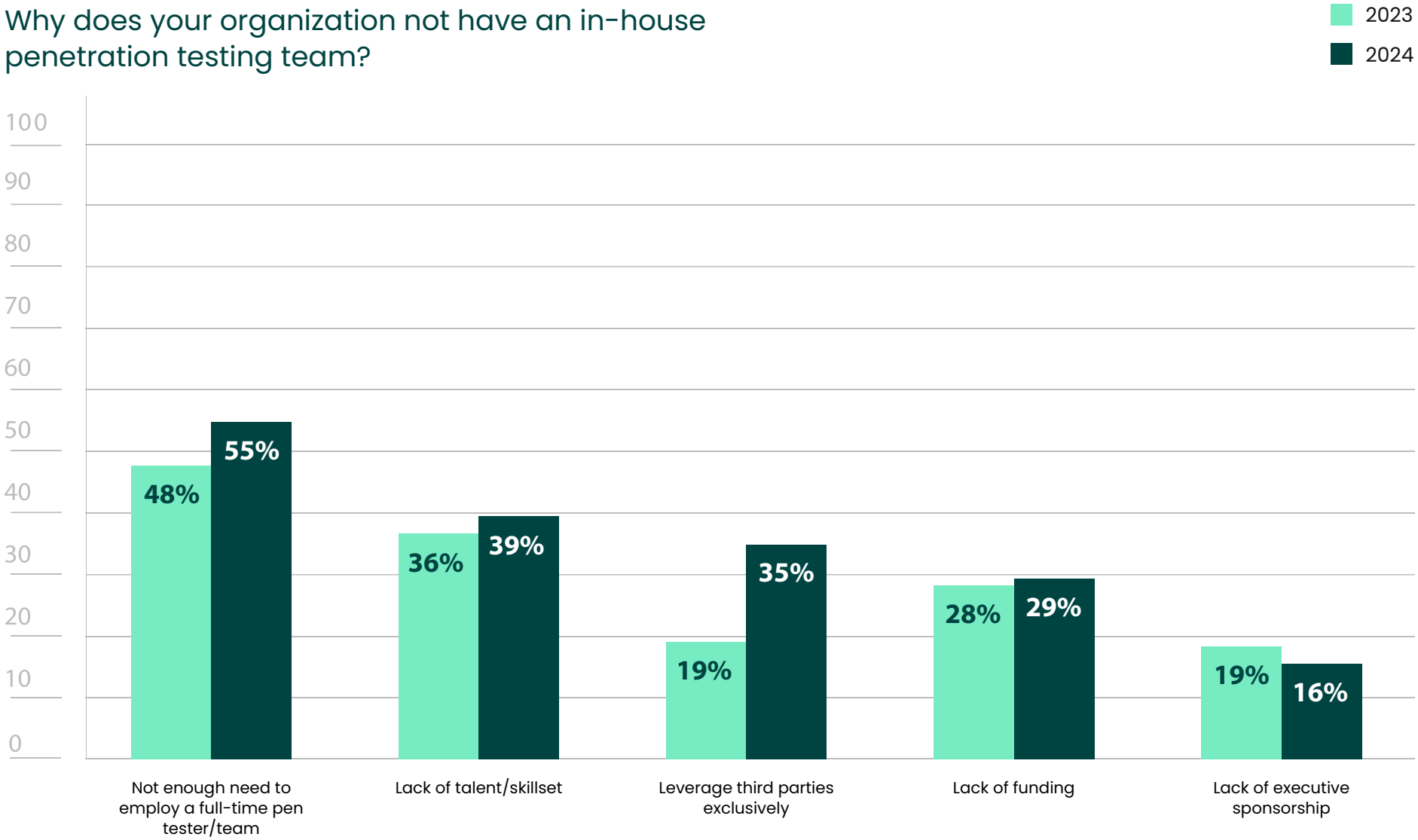


Figure 10: Reasons for not having an in-house pen testing team

Third Party Services

What is the current split between using internal and third-party penetration testing resources?

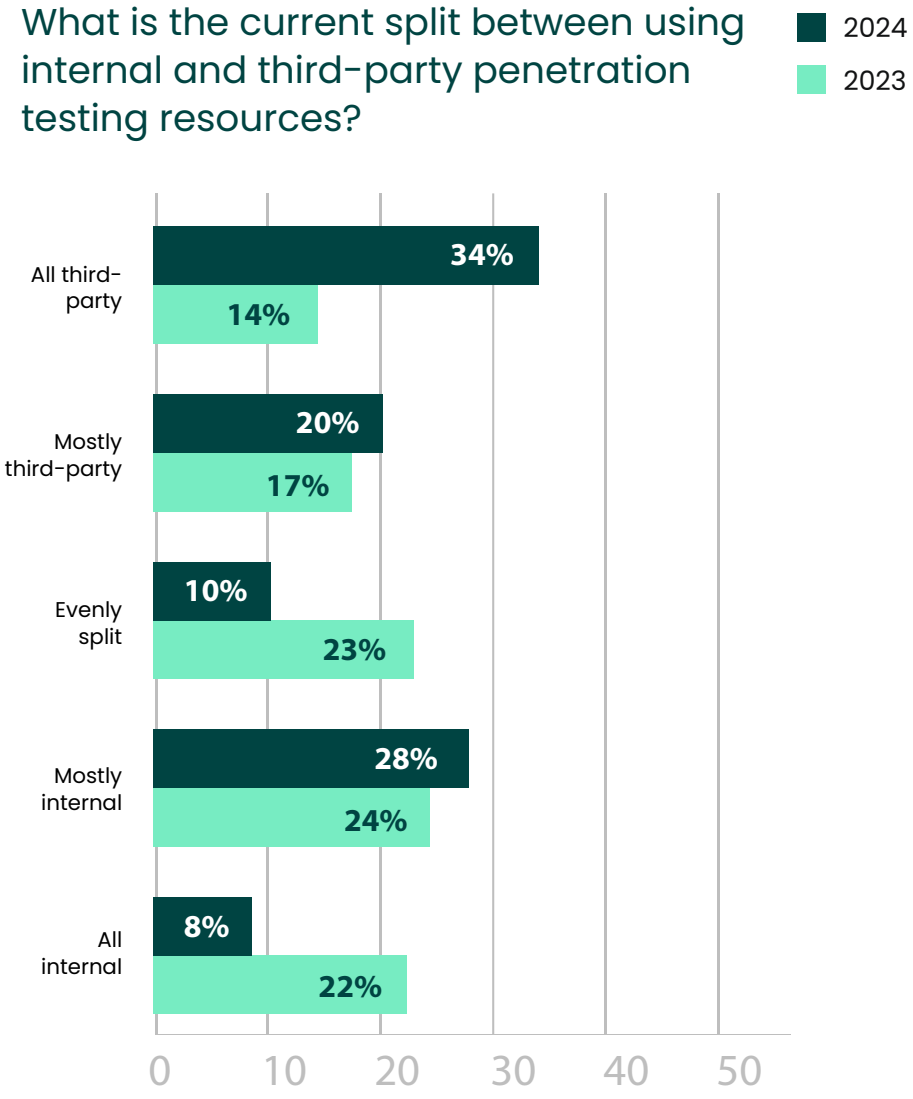


Figure 11: Split between internal and third-party pen testing services

How often do you change which third-party pen testing service you work with?

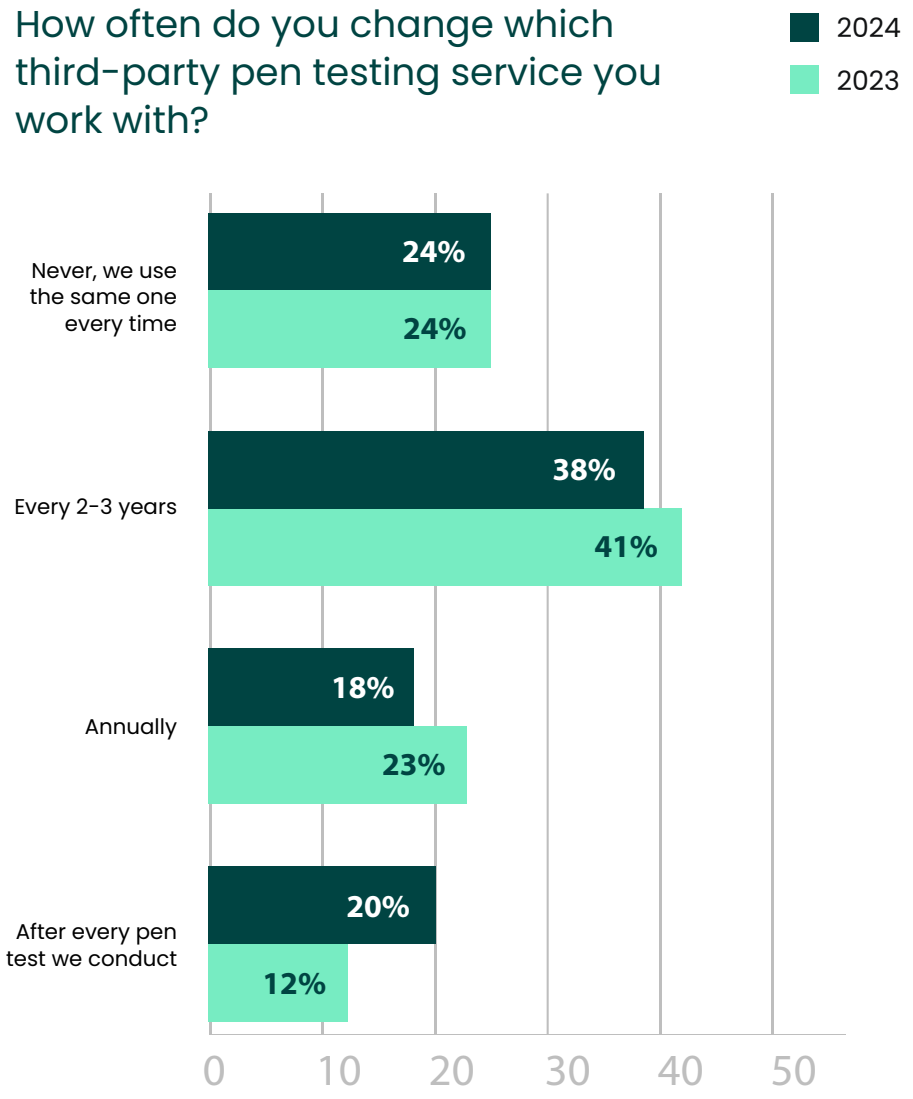


Figure 12: Rotation frequency of third-party pen testing services

Third Party Services

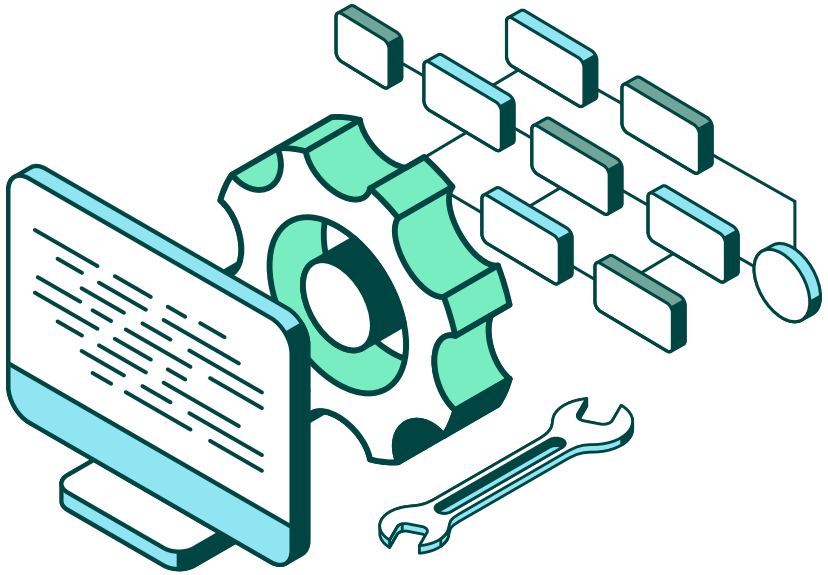
Third-party pen testing dramatically increased this year, with 92% of respondents leveraging third-party teams in some capacity (Figure 11). As discussed earlier, this aligns with the 16% increase in respondents that leverage third parties exclusively (Figure 10).

The top reason third-party services are solicited is still because of their external, objective point of view (62%) (Figure 13). Since security teams are so familiar with their own infrastructures, third-party services can help uncover blind spots, biases, and assumptions that internal personnel may overlook. Additionally, since third-party services focus solely on testing, they are often more up to date on emerging threats, attack trends, and best practices. Though different skillsets seem to go hand-in-hand with an external point of view, there was a 17% dip in participants using third-party services for their different skillsets (33%). Perhaps participants assumed that this option was only relevant to organizations with in-house testers, since "different" may be interpreted as "different from the skillsets of the in-house pen testing team. If this is the case, the reduction in in-house team use would explain this drop.

There was an 11% increase in the use of third-party services for compliance (56%) (Figure 13). This aligns with the increase in the number of pen tests run for compliance (Figure 6). Compliance is also frequently cited as the reason organizations rotate vendors. However, it is unclear just how often organizations should be changing vendors. This may explain why there is so much variation, with 24% never switching, 38% switching every 2-3 years, 18% switching every year, and 20% switching after every test (Figure 12). The truth is, no regulation explicitly requires organizations to switch out vendors, it's just a generally recommended practice.

That said, with the challenges to find qualified third-party teams (Figure 4) and the desire to consolidate vendors (Figure 22), organizations may find it beneficial to find vendors with large teams. Organizations can leverage internal rotation to ensure that different team members are assigned to conduct testing engagements, which allows for fresh perspectives, varied expertise, and independent assessments—all with a single, trusted vendor.

Organizations may also still benefit from adding some component of internal pen testing. In-house testing can be particularly helpful for retesting purposes. It may be difficult to justify to stakeholders the need to hire a third-party service to come back so soon to validate remediation efforts. Having a general cybersecurity professional assume pen testing duties may be an easier case to make. Additionally, having someone who can use pen testing tools may be especially useful if organizations continue to face the challenge of finding qualified third parties (Figure 4). If the wait for availability proves longer than anticipated, an in-house pen tester can help bridge the gap.



Third Party Services

Why does your organization utilize third-party penetration testers?

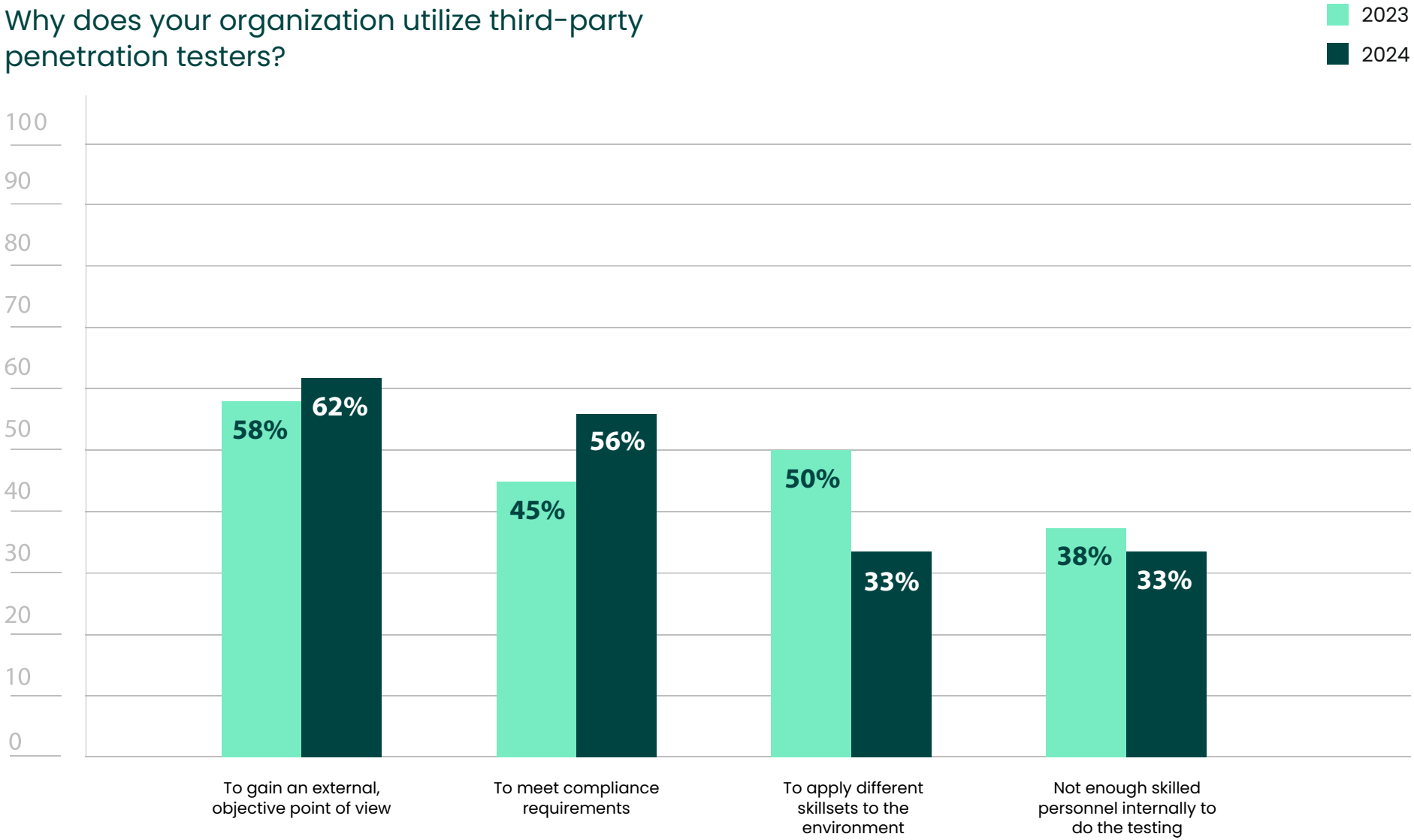


Figure 13: Reasons for utilizing third-party pen testing services

Pen Testing Tools

Penetration testing tools are a wide-ranging category and can include specialized tools like port scanners, password crackers, or SQL injection tools, as well as more comprehensive tools that offer multiple features to centralize the testing process. Pen testing tools are often divided into two categories: open-source and enterprise. Open-source tools are typically developed and maintained by the cybersecurity community. Enterprise tools are commercial solutions offered by cybersecurity vendors. While open-source tools are free to use, they often lack advanced features and can't offer extensive support. Enterprise tools do come with a price tag, but they tend to offer features designed to meet compliance regulations and keep up with the needs of complex IT environments.

This year 28% of respondents do not use pen testing tools at all—a noteworthy 27% increase (Figure 14). This is at least partially due the decrease in respondents with in-house pen testing teams (Figure 9). However, this increase, in addition to the rise in the use of only open-source tools (33%) (Figure 14) and the increased percentage of respondents that see cost as a top criteria (75%) (Figure 16), is also likely reflective of inflation and global economic volatility. With cybersecurity budget growth falling by 65% last year, many organizations may be relying more on open-source when possible.

However, there is still strong interest in commercial pen testing tools, particularly in the features/functionality they can offer (73%) (Figure 16). Reporting (65%), templates/automation capabilities (65%), and having an extensive threat library (65%) are the top three sought after capabilities in paid penetration testing tools (Figure 15). Reporting is essential to both verify and prove compliance to security regulations. Automation capabilities not only fully automate basic tests, but they can also enable a hybrid pen testing model. Automation takes care of routine tasks, allowing a tester to focus on more complex issues. This speeds up the testing process without increasing headcount or sacrificing accuracy. Lastly, an extensive threat library provides access to expertly written exploits that are regularly kept up to date, making the pen testing process more efficient and safer.

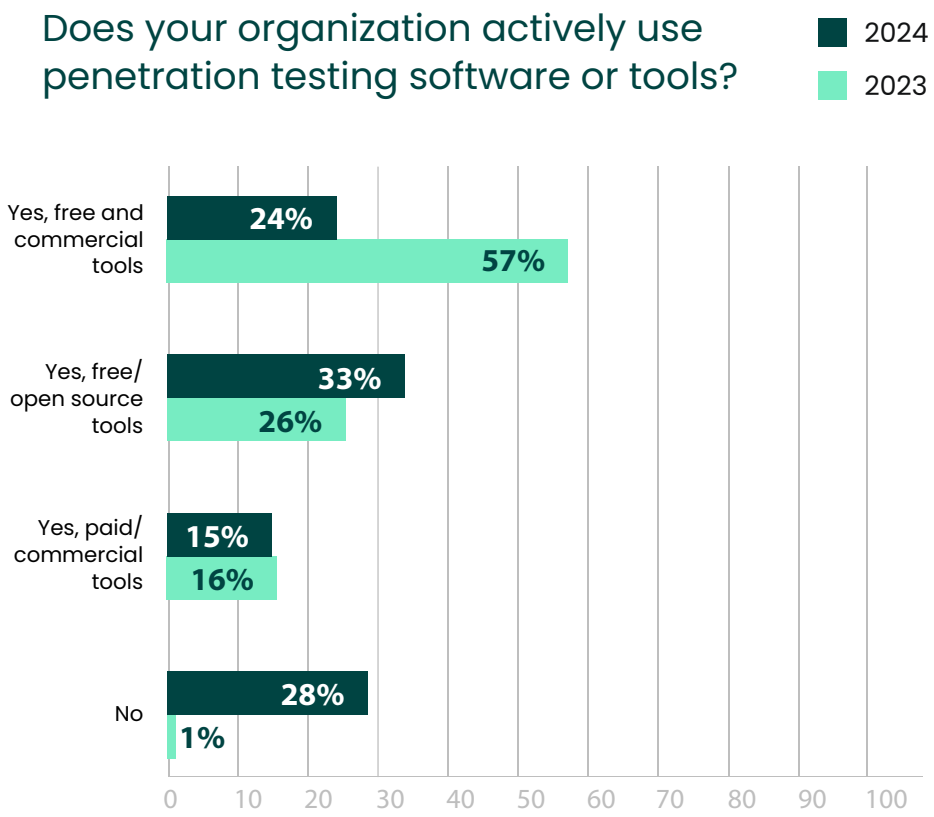


Figure 14: Active use of penetration testing software

Pen Testing Tools

What features are most important in paid/commercial penetration testing tools?

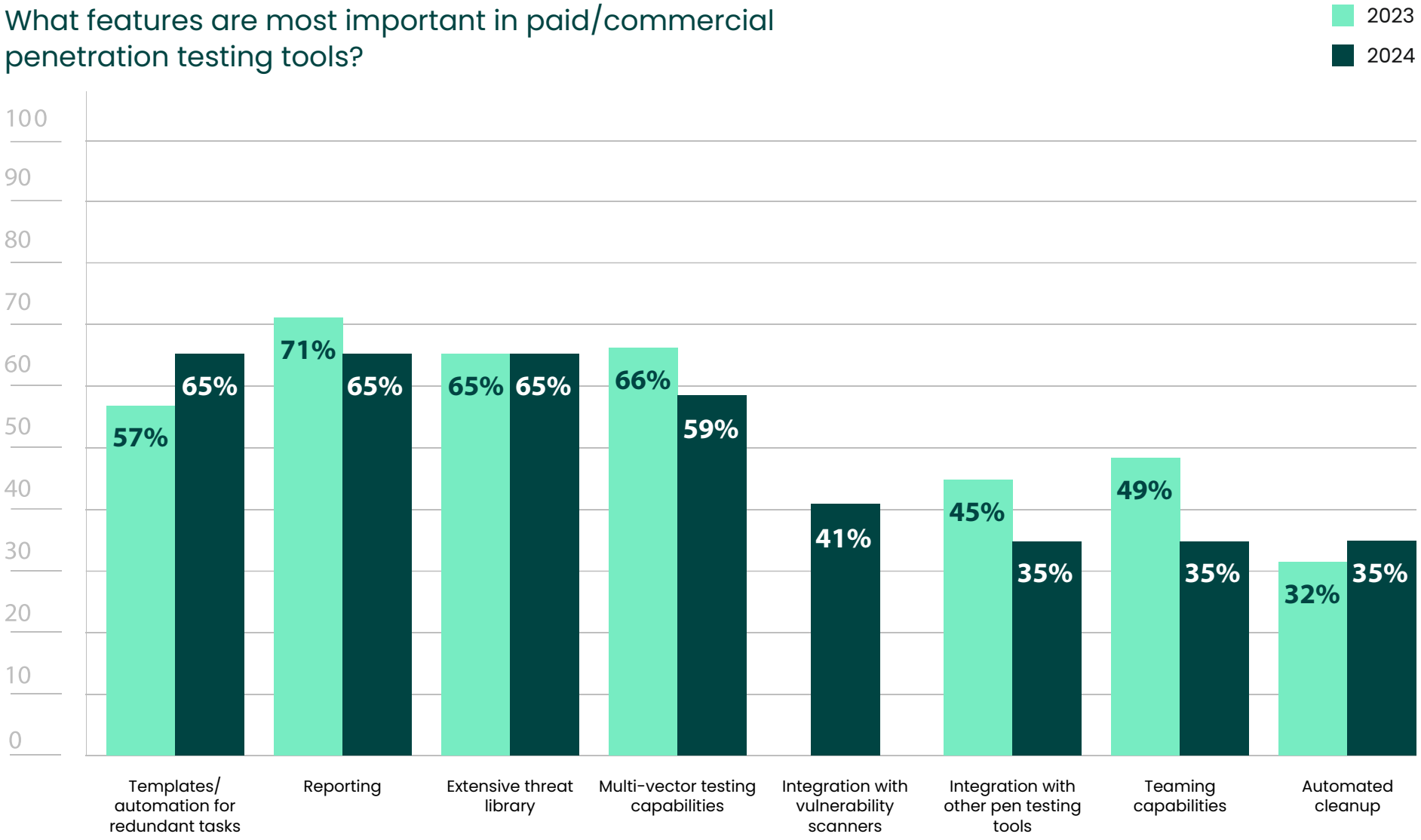


Figure 15: Most important features in pen testing software

Pen Testing Tools

What criteria do you consider most important when evaluating penetration testing software?

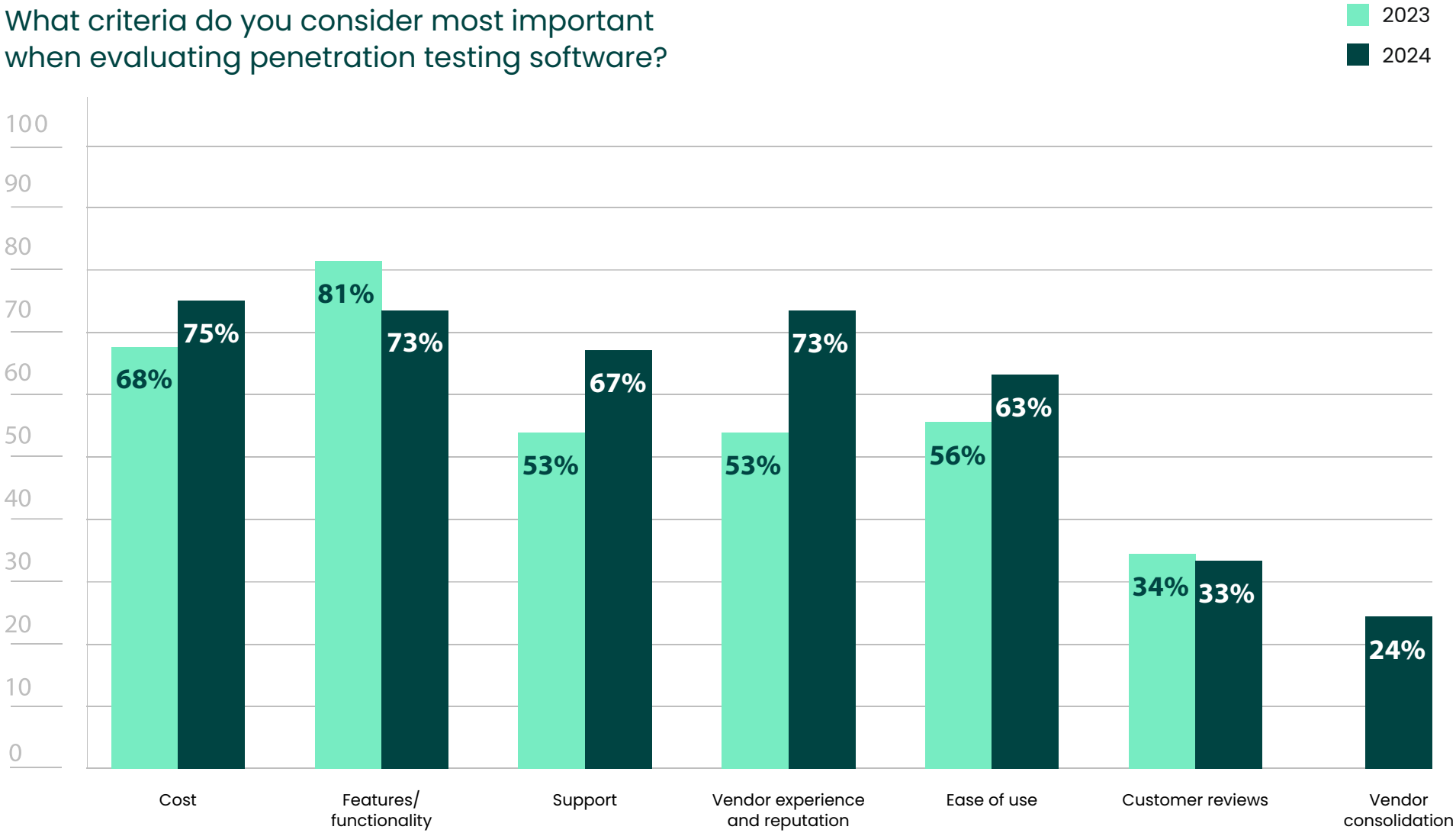


Figure 16: Most important criteria for evaluating pen testing software

Other Security Assessment Solutions

Penetration testing is just one part of offensive security and should be part of a strong portfolio of solutions that focus on prevention and continuous improvement of an organization's security posture. The most foundational tool in offensive security are vulnerability scanners, which identify, assess, and report security vulnerabilities within an IT infrastructure's network or applications. Since they are automated, vulnerability scanners typically provide the most up-to-date picture of an organization's security posture. Adding penetration testing is a logical next phase, since the data vulnerability scans provide can be used to inform penetration tests, providing insights into which weaknesses should be explored further. 77% of survey participants that have used pen testing also have vulnerability scanners (Figure 18). Interestingly, 85% of respondents that do not use pen testing do have vulnerability scanners (Figure 17). Their interest in taking a survey on pen testing indicates that they are beginning to consider expanding their offensive security portfolio.

Security awareness training (66%) is another foundational offensive security tool. These training sessions are typically required for all personnel at an organization, so they help promote a culture of security and ensure that everyone is familiar with security best practices. Since training is one of the only ways to reduce the risk of social engineering attacks, research is regularly being done on how to best convey these critical lessons in an efficient, memorable manner. Gamification, responsive design, and varied media formats are just a few of the ways that training continues to evolve.

SAST (32%) and DAST (27%), both used for testing applications, demonstrate how proactive security can be integrated into the development process. Post-exploitation (20%), red teaming (27%) and adversary simulation (23%) are typically only used by more mature programs, so participants may not yet be at this stage in their security journey. Even those that have reached advanced maturity levels may exclusively use red teaming services.

75% of respondents had cost as a top criterion when considering proactive solutions (Figure 19). While cost is always a primary concern, 2023 was especially challenging. As noted earlier, inflation and other economic concerns have impacted cybersecurity budgets. This trend is likely to continue, with a predicted 41% cut in cybersecurity spending this year. As a result, organizations have to carefully scrutinize each purchase—a difficult task when no aspect of cybersecurity feels like it can be deemed optional.

What types of vulnerability and/or threat management solutions does your organization use?

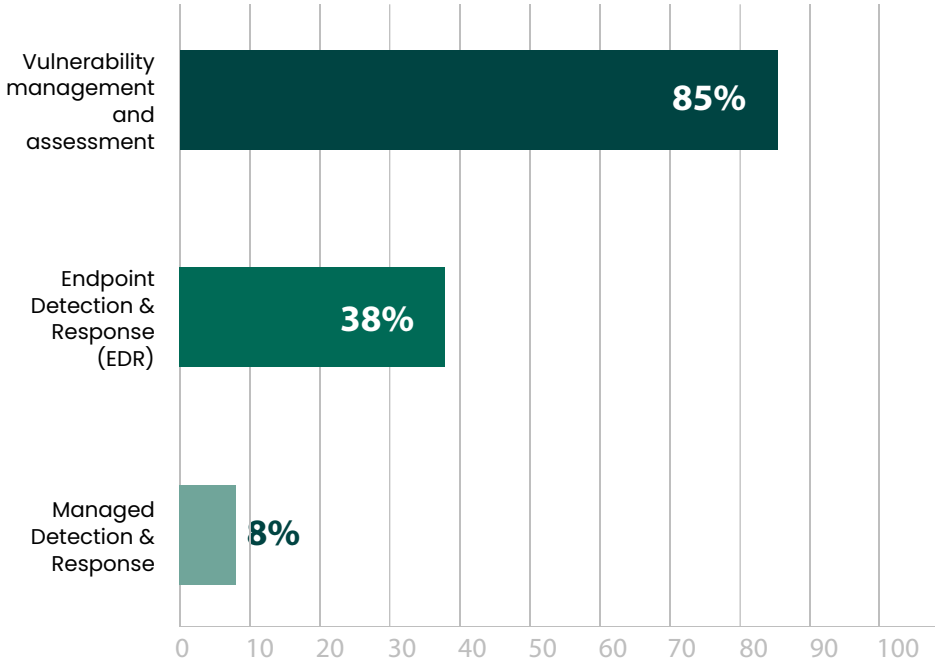


Figure 17: Other security assessment solutions used by respondents that do not pen test

Other Security Assessment Solutions

Do you use any of these other security assessment technology solutions?

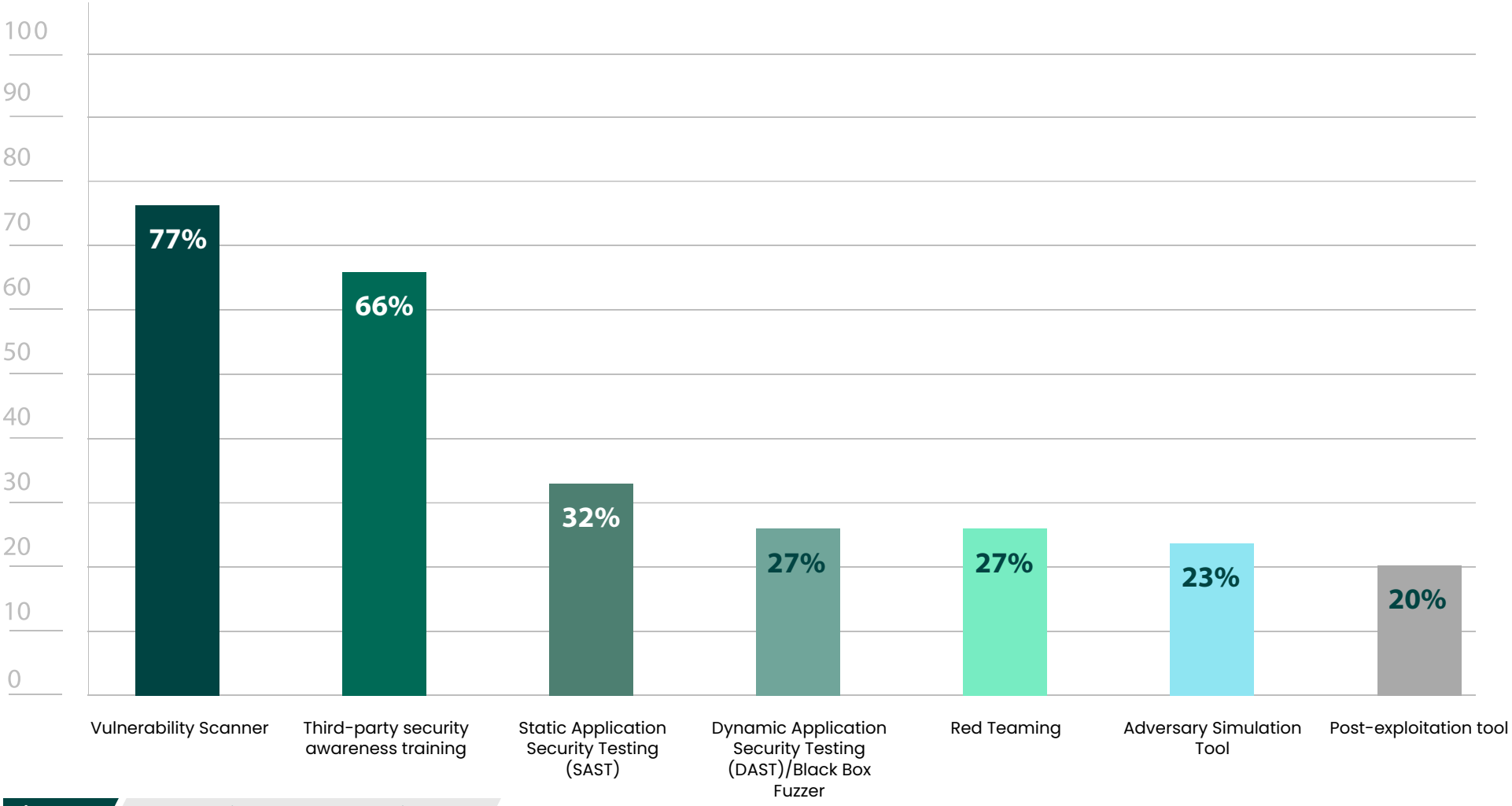


Figure 18: Other security assessment solutions used

Other Security Assessment Solutions

What criteria do you consider most important when evaluating these proactive security solutions?

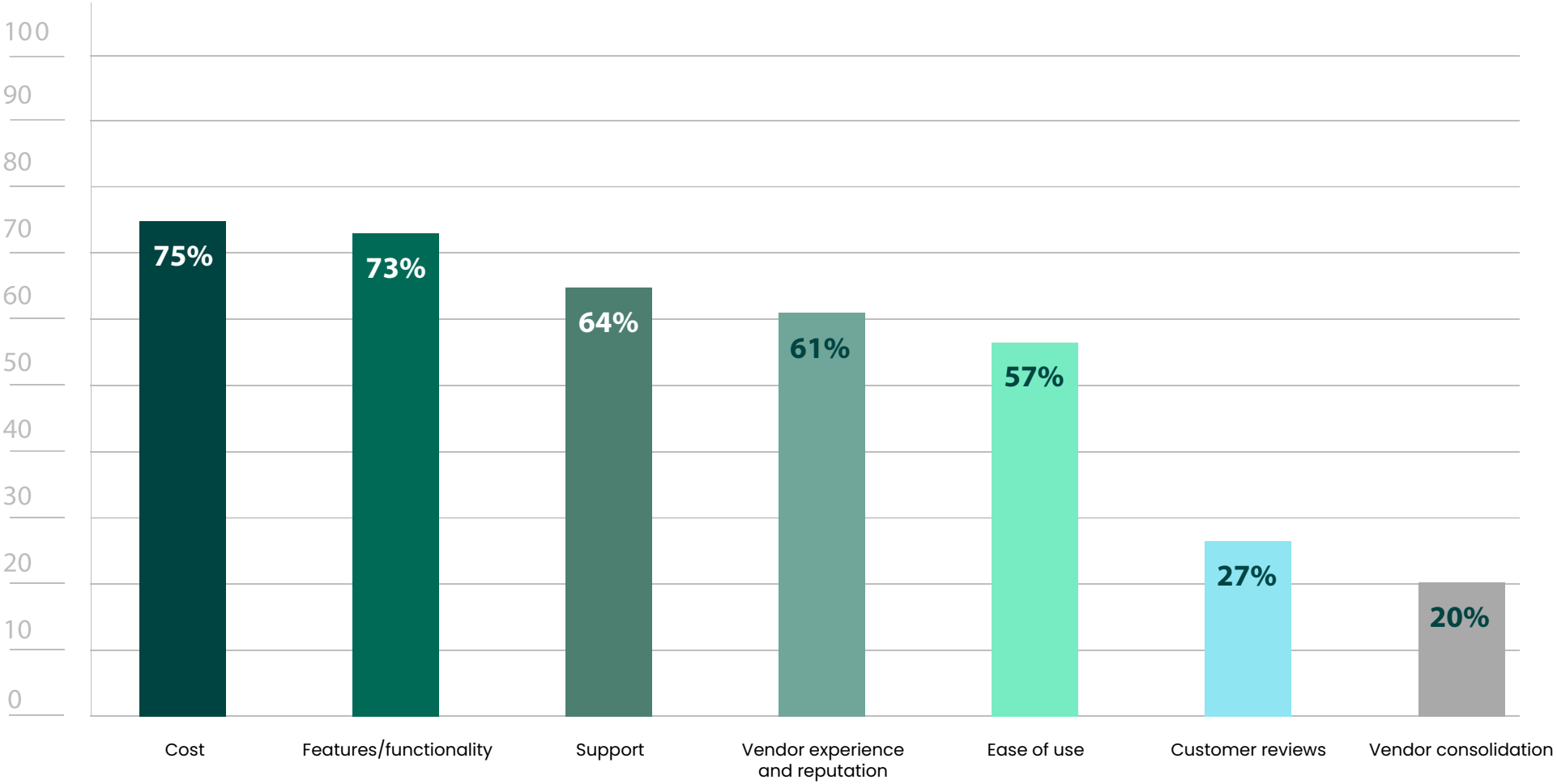


Figure 19: Most important criteria for evaluating proactive security solutions

Red Teaming

Does your organization conduct red team engagements or utilize red team services?

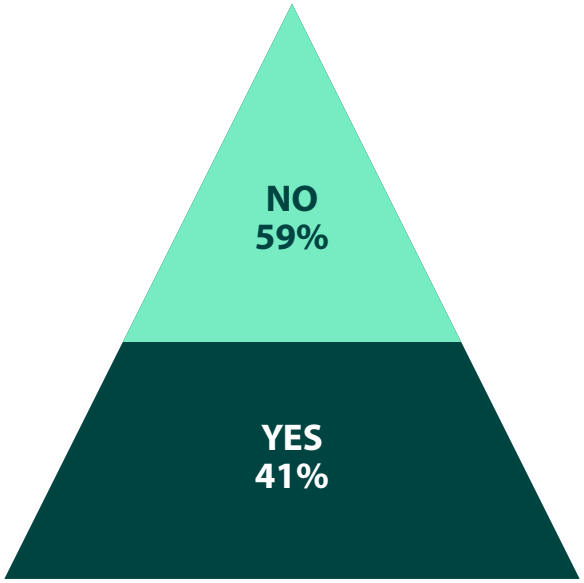


Figure 20: Use of red teaming

Do you feel red teaming has prevented a breach at your organization?

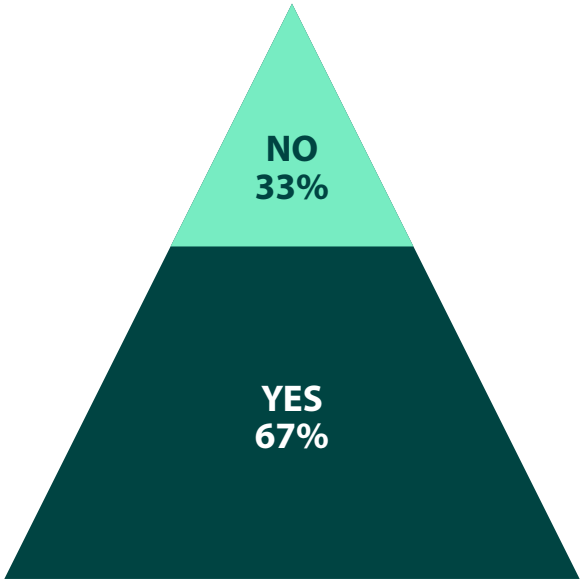


Figure 21: Efficacy of red teaming for breach prevention

Penetration tests and red team engagements are often conflated, with many using the terms interchangeably. However, there are significant differences between the two. Red teaming involves realistic simulations of cyber-attacks, while pen tests offer a more targeted approach, focusing on exploiting vulnerabilities on specific systems, networks, or applications. The goal of red teaming is to test organizational defenses and improve blue team responses, while the goal of pen testing is to assess the effectiveness of security controls. A layered offensive security strategy includes both of these complementary security assessments to close security gaps and enhance their technical defenses.

It makes sense that only 41% of respondents conduct or utilize red team services (Figure 20), since red teaming should be reserved for organization's that have reached a fairly advanced security maturity level. While most participants (67%) found red team engagements effective at preventing breaches (Figure 21), those who found them ineffective may not have been mature enough to fully benefit from them. If an organization hasn't yet implemented advanced threat detection or does not have incident response capabilities in place, they're not ready to practice responding to a live attack simulation.

Vendor Consolidation

How important is it to consolidate vendors for your security solutions?

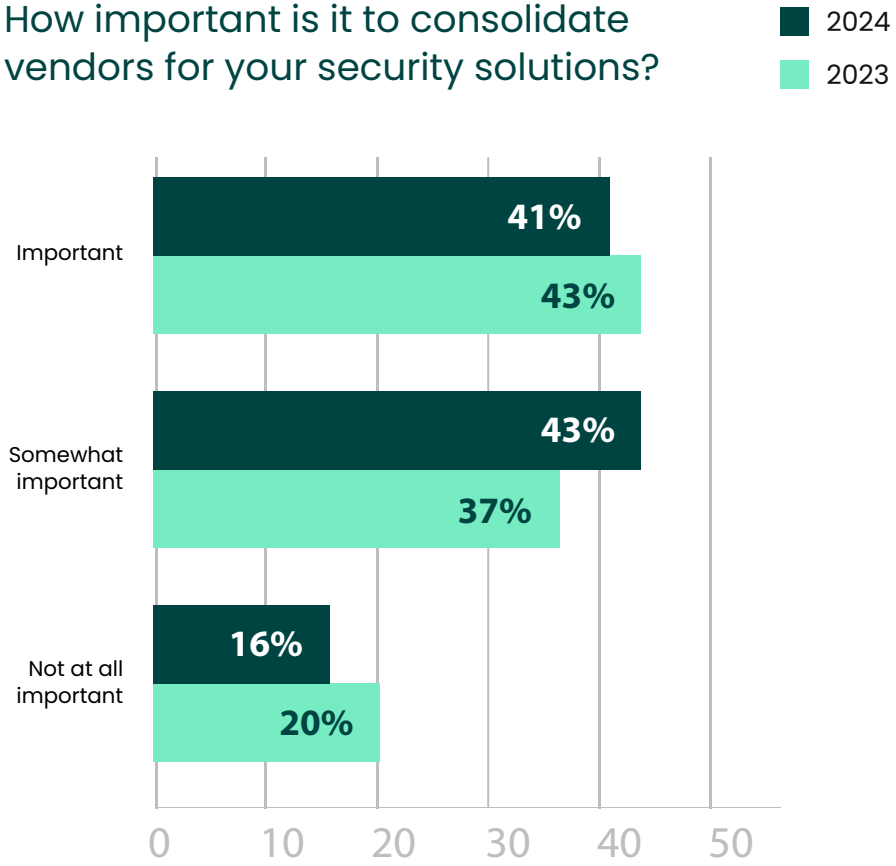


Figure 22: Importance of vendor consolidation

Would you consider adding pen testing or other proactive solutions to your portfolio if one of your current vendors offered them?

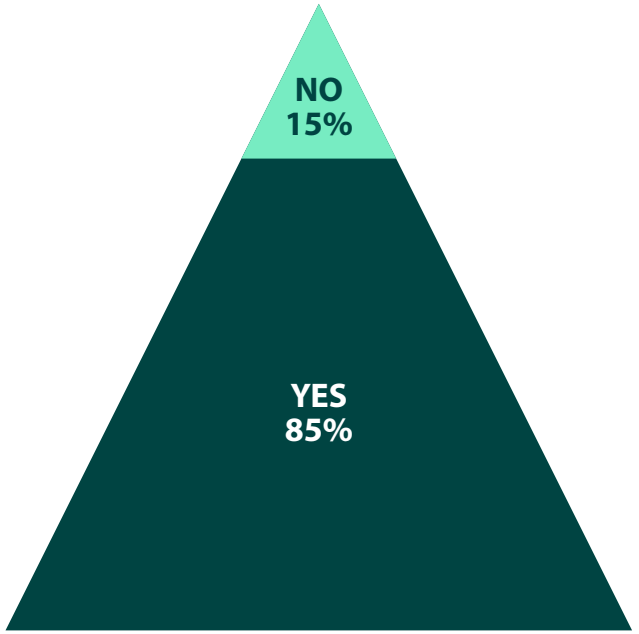


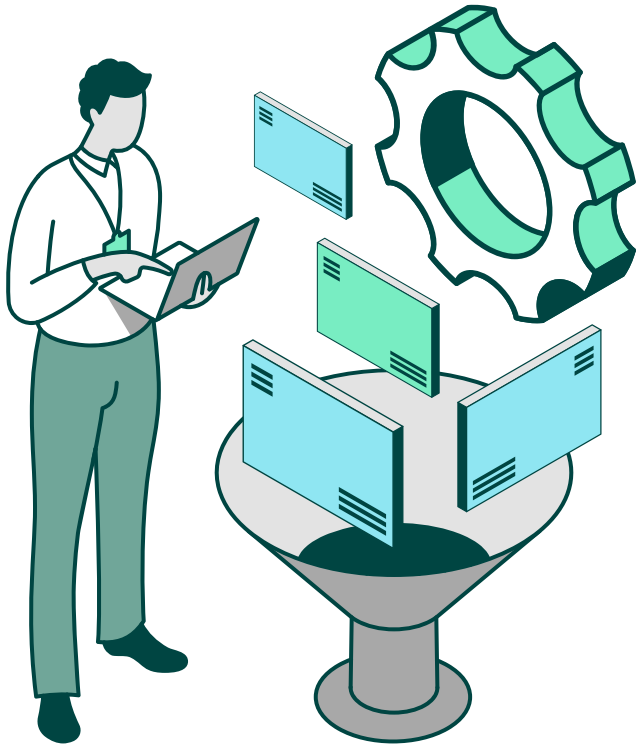
Figure 23: Likelihood of vendor consolidation for non-pen testers

Vendor Consolidation

Vendor consolidation continues to be of interest to respondents, with 84% saying it is at least somewhat important to their organization (Figure 22). Vendor consolidation offers several advantages. As IT infrastructures become more complex, organizations have found increasing amounts of time dedicated to the unanticipated task of managing numerous vendors. Dealing with fewer vendors simplifies management and reduces time spent on related administrative tasks. Developing relationships with a select number of vendors can also lead to smoother communication and easier contract negotiations.

Having multiple vendors may also unintentionally add more risk, especially with the dramatic increase in supply chain attacks last year. In fact, according to Gartner, 60% of supply chain organizations will use cybersecurity risk as a factor in determining which third-parties they work with. With an increased need for due diligence and risk assessment before entering into a contract, having a smaller set of trusted vendors can significantly increase efficiency.

Vendor consolidation can also incentivize organizations to mature their security strategies. 85% of participants that don't currently use pen testing said that they would consider adding proactive solutions if a current vendor offered them (Figure 23). Solutions offered by an existing vendor are especially advantageous when they offer interoperability and integration between products, which can simplify initial deployment, streamline operations, and reduce complexity. When organizations begin looking for vendors that offer the solution they are currently looking for, it may be prudent to find those that also provide additional options for future investments.



Pen Testing in Different Environments

Which environments or operating systems are you most concerned about pen testing?

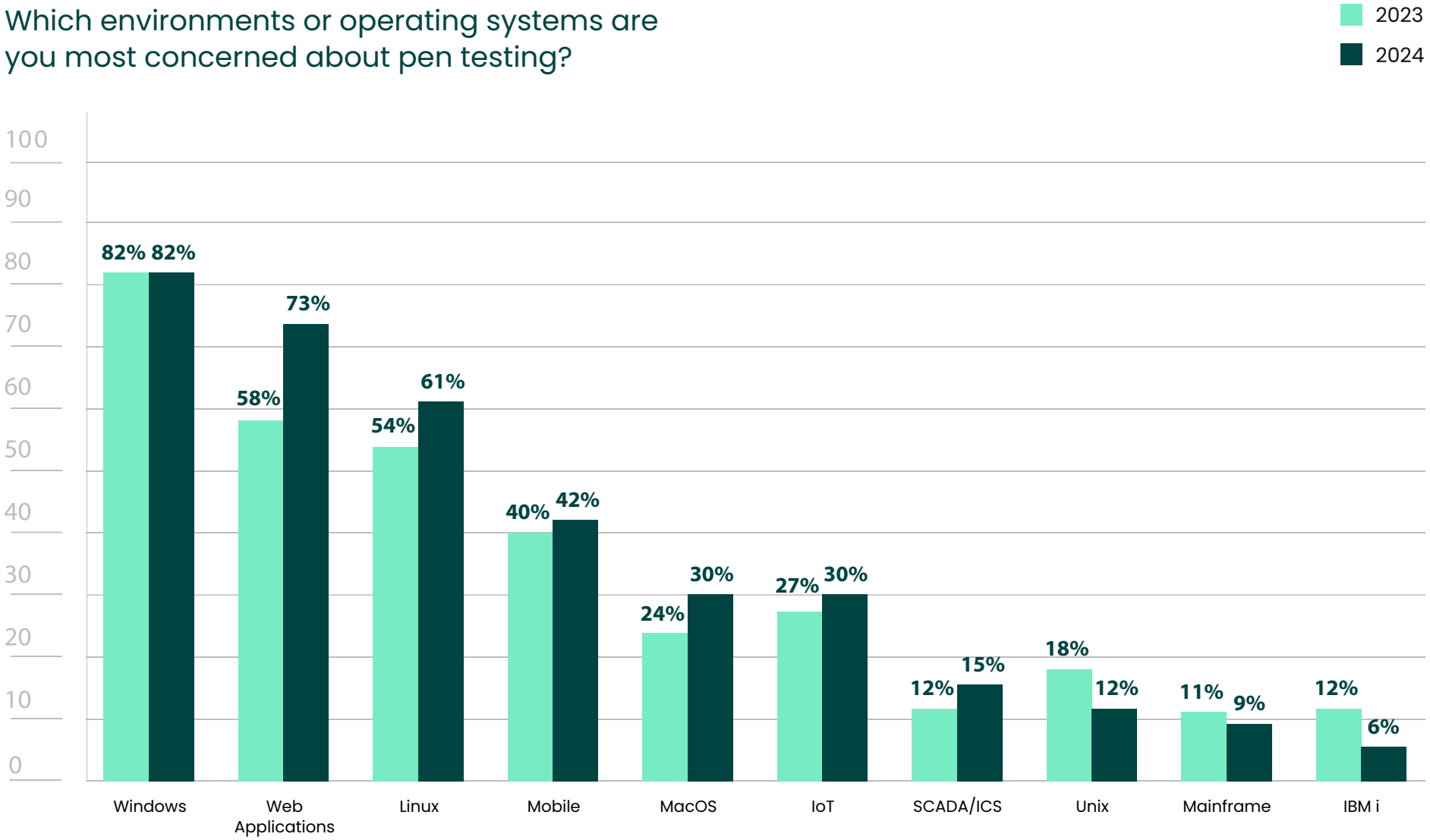


Figure 24: Environments in need of pen testing

Pen Testing in Different Environments

With its ubiquity across various organizational assets, including workstations, servers, and other endpoints, Windows (82%) once again stands out as the predominant operating system of concern (Figure 24). Windows Active Directory is a high-value target for attackers, as it serves as the centralized repository for authentication, authorization, and configuration information. If Active Directory is compromised, threat actors can have full control of the entire network, so securing Windows environments and safeguarding Active Directory against exploitation is crucial for minimizing cybersecurity risks and protecting organizational assets.

Web applications remain common environments for pen testing, but the 15% increase from last year is worth noting (Figure 24). It may reflect the increase in participants from the finance industry, whose web applications became an even more popular target last year (Figure 29). In fact, web application attacks were responsible for 77% of all breaches in the finance and insurance sector, according to the Verizon Data Breach Investigations Report (DBIR). Additionally, the DBIR found that 95% of attacks were financially motivated, making financial applications particularly tempting, as they can store bank account numbers, credit card details, Social Security numbers, and transaction history.

The 20% increase in pen testing for cloud infrastructures (Figure 25) was a promising change, especially as cloud environments become increasingly relied upon. For example, cloud native computing grew 175% from 2022 to 2023. Unfortunately, an upward trend in use typically means an upward trend in attacks. Sure enough, over 80% of data breaches last year involved data storage in the cloud. Organizations would be wise to continue including cloud environments in their pen testing strategies.

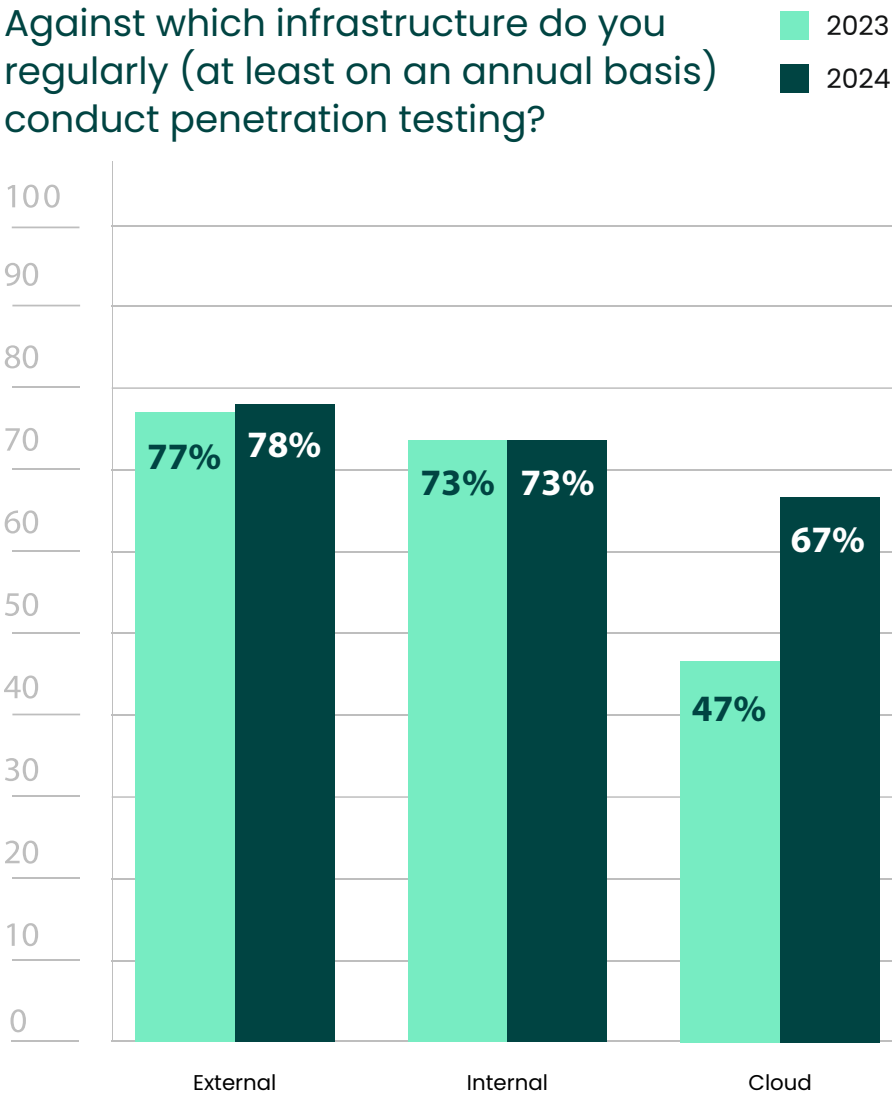


Figure 25: Infrastructures regularly pen tested

Demographics

This report is based on the results of a survey focused on presenting an accurate picture of the cybersecurity concerns penetration testing addresses, how it is deployed by different organizations, and the challenges in creating and managing a penetration testing program. Cybersecurity professionals around the globe participated, with respondents representing a diverse cross-section of industries, company size, job level, and region.

Which region is your organization headquartered In?

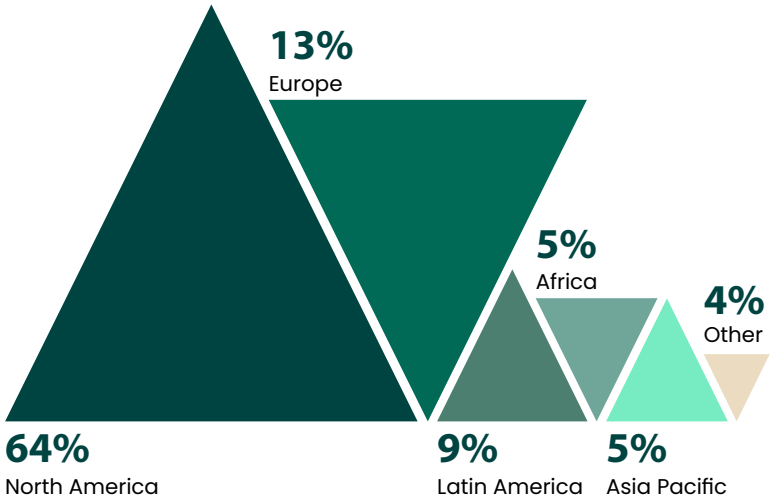


Figure 26: Regions Surveyed

What is your primary industry?

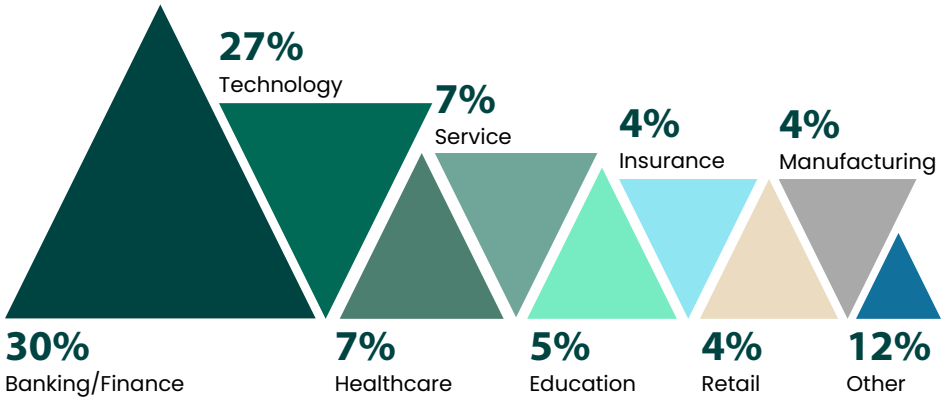


Figure 27: Industries Surveyed

Demographics

What is your job level?

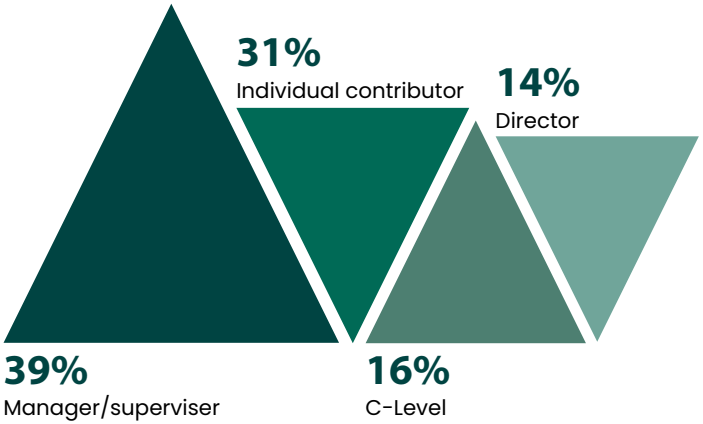


Figure 28: Job Levels Surveyed

How many employees does your organization have?

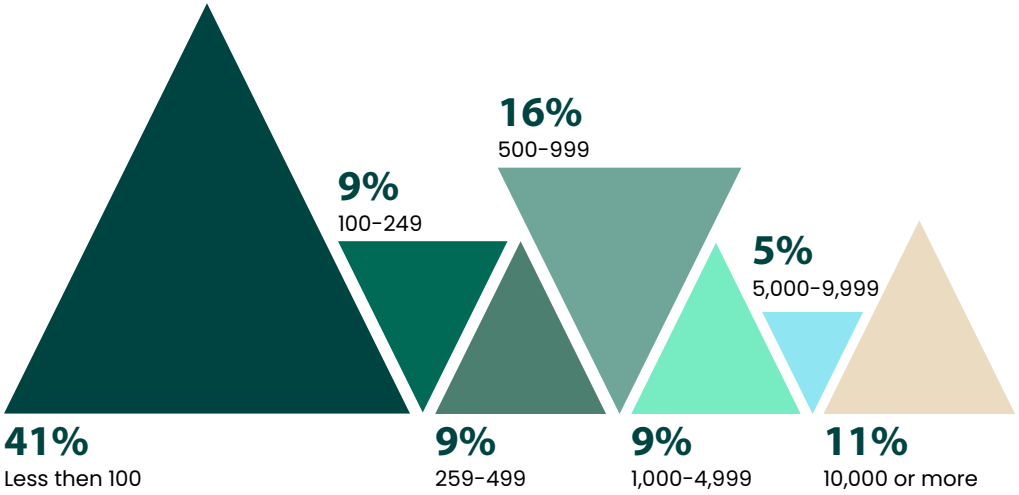


Figure 29: Size of Organizations Surveyed

Conclusion

The results of this survey highlight the importance of pen testing as a strategic component of an organization's proactive cybersecurity portfolio. Just as pen test assess infrastructure security, organizations must also regularly evaluate their pen testing approach, carefully considering the available tools and methodologies to ensure they are effectively addressing their unique security needs and requirements.

Pen testing programs are not without their obstacles. The pervasiveness of limited resources was evident throughout the survey analysis, with fewer in-house pen testing teams, more organizations going without any commercial pen testing tools, and cost becoming the top criterion for both pen testing solutions and other proactive security tools. Though organizations may be able to reduce costs through vendor consolidation, continuing financial challenges may require difficult decisions about how many tests to run, how extensive they should be, and who should be running them.

But the importance of penetration testing extends beyond the immediate scope of the tests themselves. Incorporating pen testing in any form opens the door to adopting a proactive security mindset.

FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-cs-gd-0424-db