THE STATE OF PENTESTING 2025

SURVEY REPORT

PENTERA

USA EDITION

Table of contents

Introduction

Welcome to the 2025 State of Pentesting Report. Now in its fourth year, this survey brings together insights from 500 CISOs around the world to provide a clear view of how organizations are testing, validating, and evolving their security programs in a rapidly shifting threat landscape.

Over the past decade, the role of pentesting has changed dramatically. What was once a periodic compliance exercise is now a strategic practice, embedded in day-to-day operations and increasingly shaped by the **adversarial perspective**. Organizations are moving beyond reactive defenses, increasingly turning to proactive testing to identify their most critical exposures.

This evolution has been driven by a range of factors: the introduction of structured frameworks like Continuous Threat Exposure Management (CTEM), the need to meet expanding regulatory requirements, and the constant pressure to keep pace with adversaries who never stop refining their tactics.

So where do we stand in 2025?
What does enterprise cybersecurity look like?
Are risk and vulnerability management budgets going up or down?
What's driving security validation programs today?
What is cyber insurance demanding of the technology stack?

This report answers those questions and more, providing a data-backed view into the current state of security validation - and how enterprises are adapting their strategies for what's next.

For any feedback or inquiries, please contact noam.hirsch@pentera.io
Wishing you a meaningful read

– The Pentera Market Research Team

Methodology

500 Pentera commissioned a global survey of 500 CISOs and senior security executives, 200 of them are from the United States

3000+ Representing organizations with 3,000 employees or more across a range of industries

The average time to complete the survey was 9 minutes and 3 seconds

All respondents held C-level or VP roles in IT and cybersecurity functions

The survey was conducted by Global Surveyz, an independent research firm, in January 2025. Participants were recruited through a global B2B research panel and invited via email to complete the survey

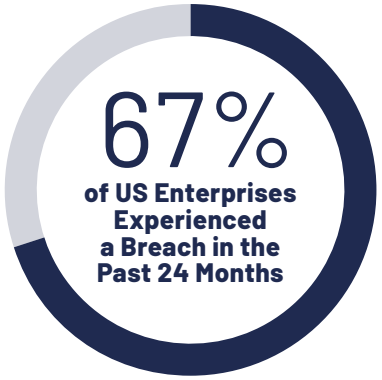
To minimize order bias, the answer choices for most non-numerical questions were randomized

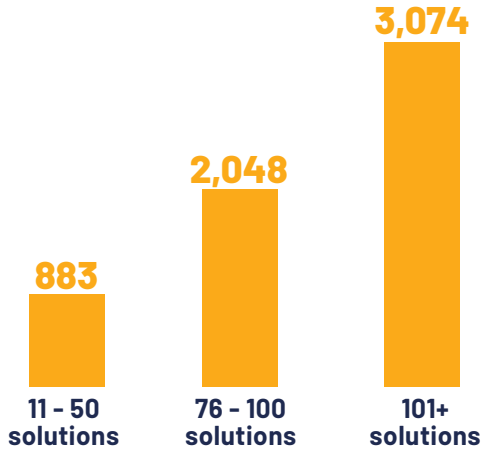
Executive summary

01

67% of US Enterprises Experienced a Breach in the Past 24 Months

Enterprise **CISOs manage an average of 75 security tools across their IT environments**, with 45% reporting stack growth over the past year. Despite these investments, 67% experienced a breach in the past 24 months, underscoring the persistent challenges of securing complex environments.





02

Large Security Stacks: Increased Vulnerability Data Volume

While a broader security stack increases visibility of potential issues, it also increases operational complexity, making it harder to prioritize and respond to the most critical threats. Organizations with 11–50 security tools generate an average of 883 alerts per week. **Enterprises with 76–100 tools face over 2,048 alerts weekly**, while those with more than 101 tools see an average of 3,074 alerts.

03

Pentesting Represents Around 11% of the Total IT Security Budget

US enterprises spend an average of $187,000 annually on pentesting which is about 10.5% of their total IT Security budgets. IT Security budgets are on the rise: Over 50% of CISOs report that they will be raising their pentesting budgets in 2025 and 48% will be raising their overall IT security budgets.

$187K

Average annual pentesting budget

04

Software-Based Pentesting is Gaining Traction

55% of enterprises now use software-based tools to support in-house testing programs, and 50% of CISOs cite software-based testing as a primary method for uncovering exploitable security gaps within their IT environments. This reflects a growing trust in the safety of software solutions. Enterprises are shifting toward scalable adversarial testing approaches.

05

Cyber Insurance Providers are a NEW Driving Force for Technology Adoption

Cyber insurance providers are driving security control technology adoption. In the US **59% of enterprises have implemented at least one cybersecurity solution at the request of their insurance provider.** An additional 34% reported receiving recommendations for specific solutions.

06

Confidence in Government Support is Not High

22% of CISOs say they cannot rely on the government for cybersecurity support at all. Another 64% of US enterprises acknowledge government actions, but believe these efforts are insufficient. Only 14% believe the government is truly doing its part to help protect the private sector.

22%

of CISOs say they cannot rely on the government for cybersecurity support at all.

Survey report findings

Increasing complexity of cyber infrastructure

As enterprise IT environments evolve - spanning cloud, on-prem, and hybrid infrastructures - security teams are integrating more security solutions to address diverse risks to distributed assets. Security infrastructure today is highly complex, with enterprises managing dozens - sometimes hundreds - of cybersecurity tools across their environments.

On average, US enterprises report using 75 security solutions across their environments. **62% report operating more than 75 within their organization, while only 18% of organizations utilize 50 or fewer solutions.**

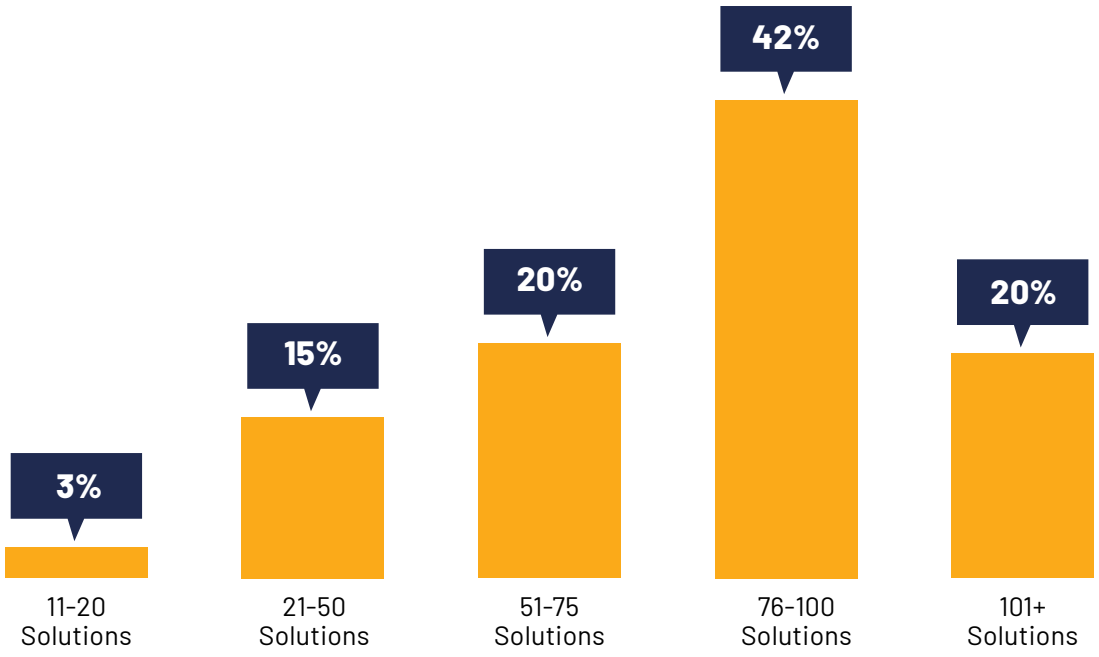
Number of security solutions by organization size

75
3,000-4,999 Employees

76
5,000- 9,999 Employees

79
10,000+ Employees

How many security solutions do you currently use across your organization?



While the number of security solutions tends to increase with organizational size, the difference is relatively modest. Enterprises with 3,000–4,999 employees report an average of 75 tools, compared to 79 tools in enterprises with over 10,000 employees.

Large stacks are growing larger

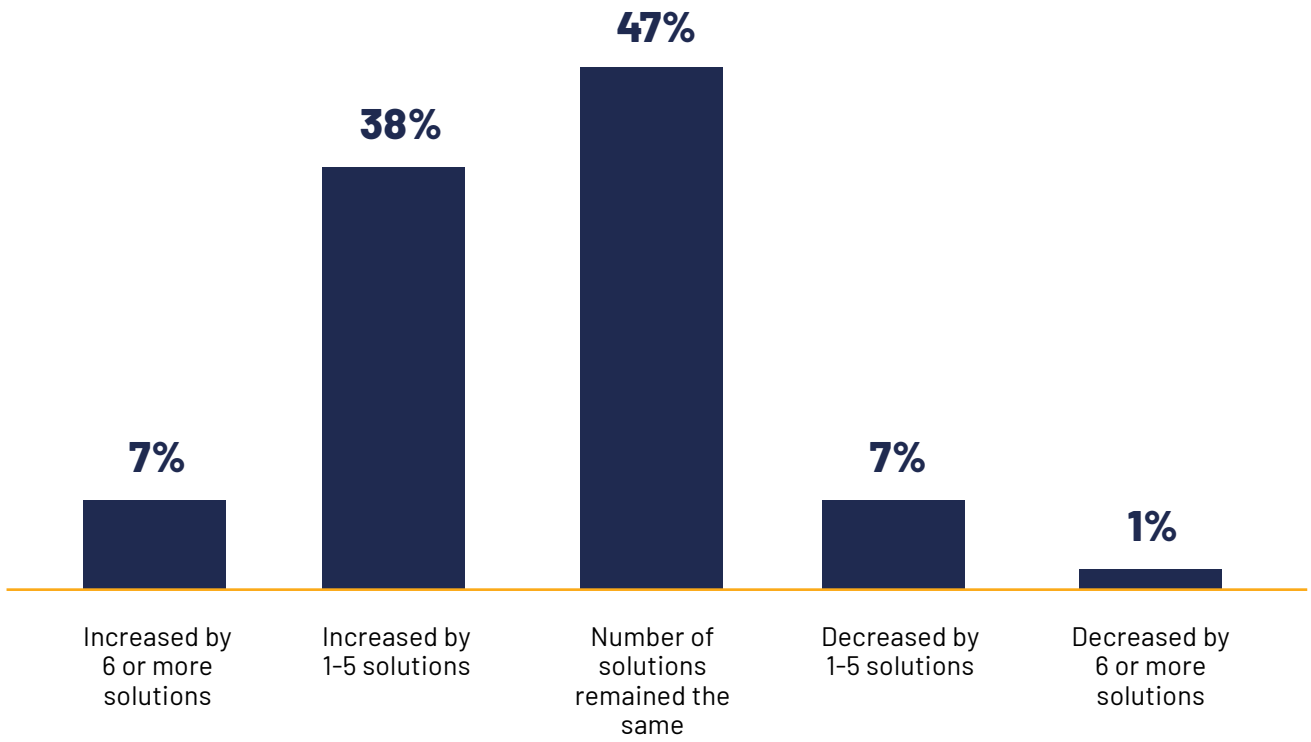
Already complex security ecosystems are continuing to grow. **In the US, 45% of CISOs reported a year-over-year increase in the net number of tools within their security stacks.** Nearly half reported no change, while only a small minority indicated a reduction.

Consolidation has become a common theme in cyber industry conversations, but the data doesn't support a contraction of security stacks. Our thoughts here are that as in many cases, the idea of consolidation is a desire among CISOs who would like to reduce complexity. It would be nice if feasible, but it appears that the majority of CISOs are not successful at shrinking their stacks.

Another potential here is that consolidation may be taking the form of vendor unification. CISOs may be consolidating multiple separate solutions under platforms offered by larger players. So while the total number of solutions can rise, the vendor number will decrease.

In effect, organizations may be reducing operational complexity (by streamlining vendor management and interfaces), not security complexity (the number of tools in play).

In the past 12 months, how has the NET number of security solutions in your security stack changed?



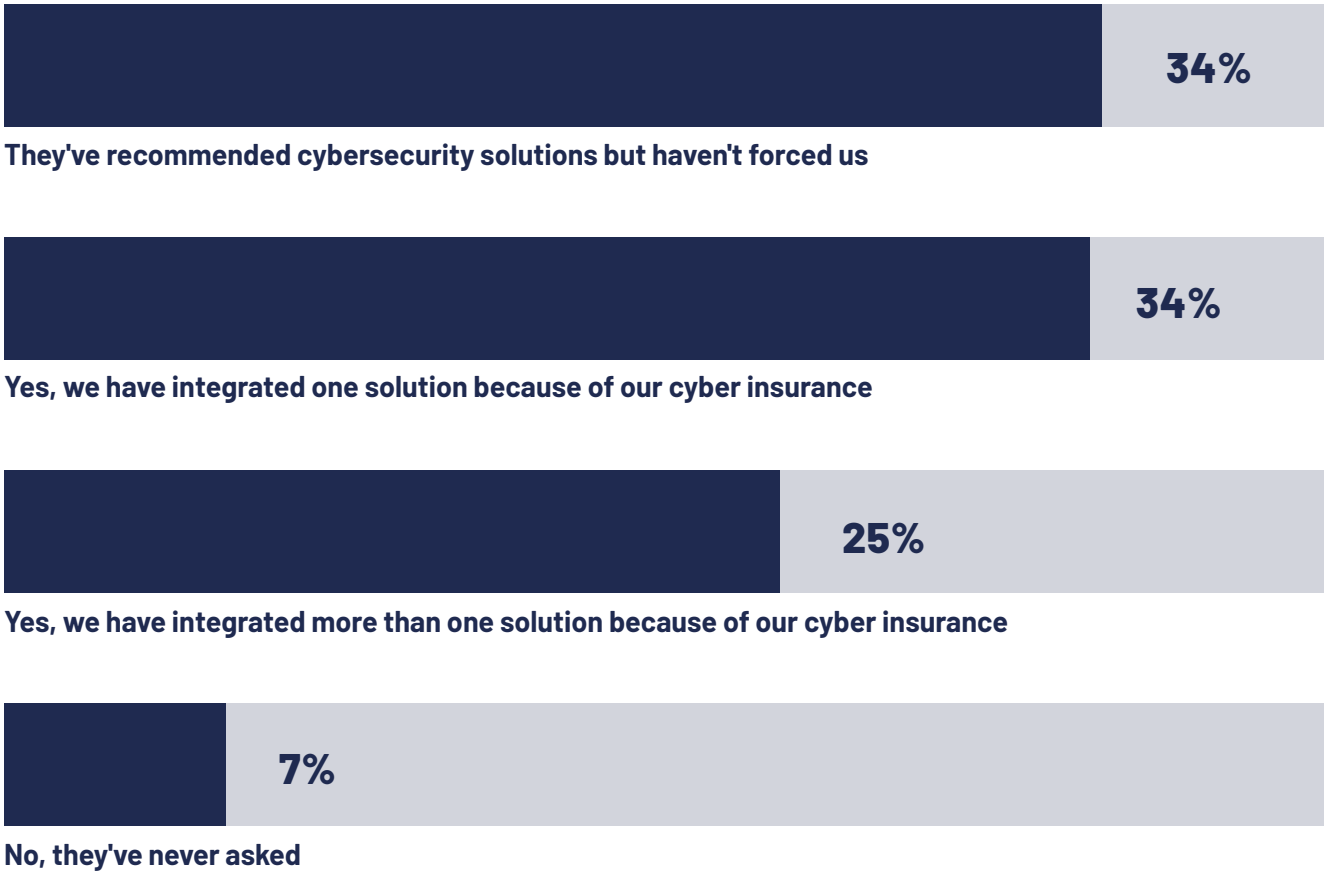
Cyber insurance providers are driving tool adoption

After years of rapidly rising premiums, cyber insurance rates have begun to stabilize. This shift is due in part to stricter underwriting practices and increased demands for improved cyber hygiene from insurers.

Given the frequency and cost of breaches, it's no surprise that insurers are highly involved in shaping their clients' security postures. **93% of CISOs report that their cyber insurance provider has either recommended or required the adoption of security solutions not previously in place.**

In fact, 59% of organizations report implementing at least one security tool at the direct request of their insurance provider. **Only 7% have never received such a recommendation or request from their cyber insurance provider.**

Has your cyber insurance provider compelled you to integrate a cybersecurity solution you were not previously considering?



Larger security stacks, fewer breaches yet no guarantees

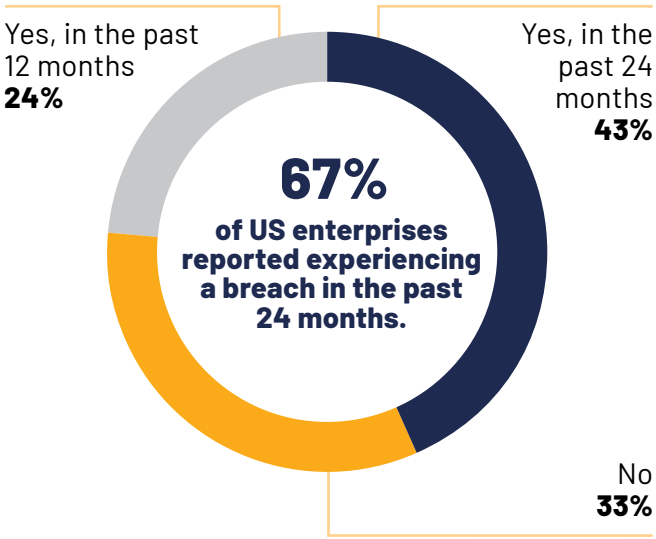
Despite extensive cybersecurity stacks, breaches remain common. **67% of US enterprises reported experiencing a breach in the past 24 months.**

Of those who agreed to provide details of their breach, **76% reported an impact on the confidentiality, integrity, and/or availability of their data.** Only 24% reported no significant impact as a result of the breach. 36% reported unplanned downtime, while 28% cited financial loss.

There is a clear correlation between the size of the stack and the probability of a breach. Among organizations with fewer than 50 security tools, 93% reported a breach. That percentage steadily declines as stack size increases, dropping to 61% among those using more than 100 tools.

This suggests that while there is no panacea, deploying multiple layers of defense does indeed enhance resilience.

Has your organization been compromised by a cyberattack over the past 24 months?



Did your organization experience any disruption or impact as a result of the cyberattack(s)

✱ Question allowed more than one answer and as a result, percentages will add up to more than 100%

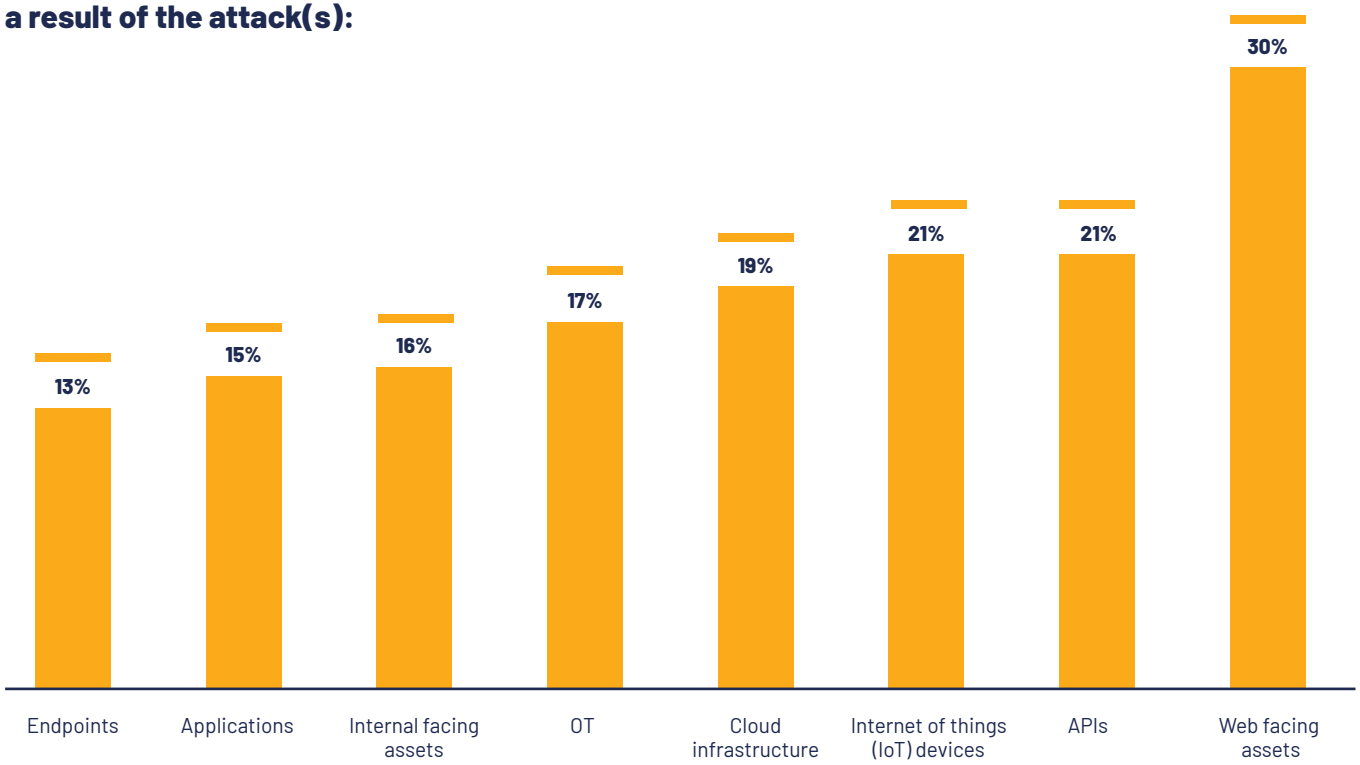
No surface is safe: Threats are spread across the entire attack surface

Organizations reported breaches across the attack surface, reinforcing a key reality: **Threat actors are opportunistic. Rather than focusing on specific systems or vectors, they exploit any available entry point.**

On an individual level, threat actors often have preferred techniques and favored parts of the attack surface. For example, APT29 (also known as Cozy Bear) is known for targeting cloud and identity infrastructure, relying heavily on living-off-the-land techniques and token theft rather than deploying traditional malware. FIN7, by contrast, operates with a very different MO - focusing attacks on Point-of-Sale (POS) systems, web-facing assets, remote access tools like RDP, and third-party vendors as initial access points.

But the broader threat landscape is far less predictable. It's not just you against Cozy Bear or FIN7 - it's you against the collective ingenuity of the global threat actor community. To defend effectively, organizations must be prepared for any type of attack, across any part of the attack surface.

Which aspect(s) of your organization's infrastructure were compromised as a result of the attack(s):



Nearly a third of enterprises reported a compromise on their Web Facing Assets, reflecting the perception of their exposure and accessibility as "low-hanging fruit." External attack surfaces were compromised at nearly twice the rate of internal networks and servers, which are generally better protected and harder to reach.

This emphasizes the importance of securing the perimeter - if the external surface isn't protected, it becomes the easiest way in.

✱ Question allowed more than one answer and as a result, percentages will add up to more than 100%

More tools, more alerts: Prioritization is more critical than ever

Enterprise IT and security teams are inundated with alerts. **In the United States the average organization sees 2,000 alerts per week.**

For the purpose of this survey an "alert" is defined as a security matter that requires a remediation action. Examples include: Vulnerability to be patched, Endpoint Isolation/Quarantine.

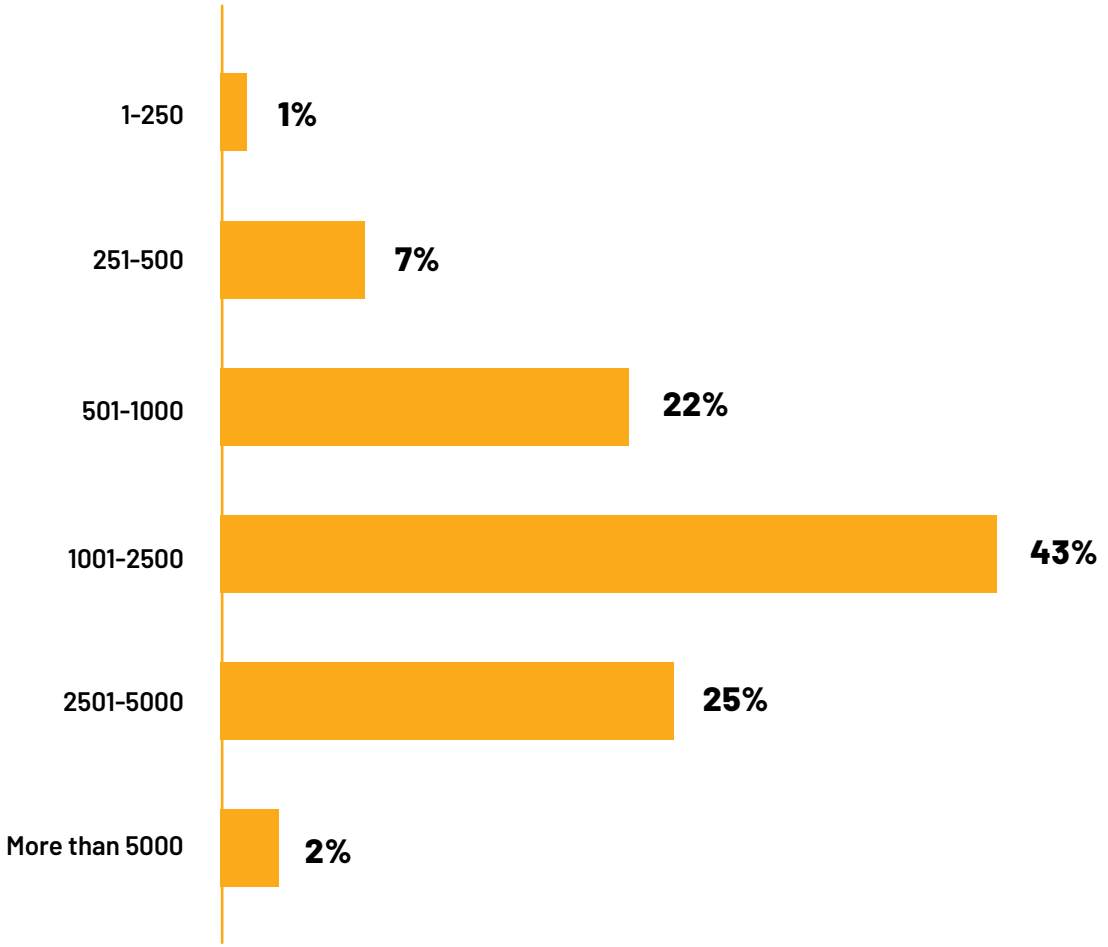
As organizations deploy more tools, the number of weekly alerts increases accordingly:

11–50 tools:	51–75 tools:	76–100 tools:	101+ tools:
883 alerts	**1,512 alerts**	**2,048 alerts**	**3,074 alerts**

More security tools mean greater visibility and more data points to act on, but also more information to process. This places a greater necessity on the ability to prioritize alerts effectively and respond to what matters most.

If not managed well, the sheer volume of alerts can overwhelm security teams, delay response times, and allow critical threats to go unnoticed, leading to increased risk of breaches, operational disruption, or data loss.

How many security "alerts" does your organization receive per week?



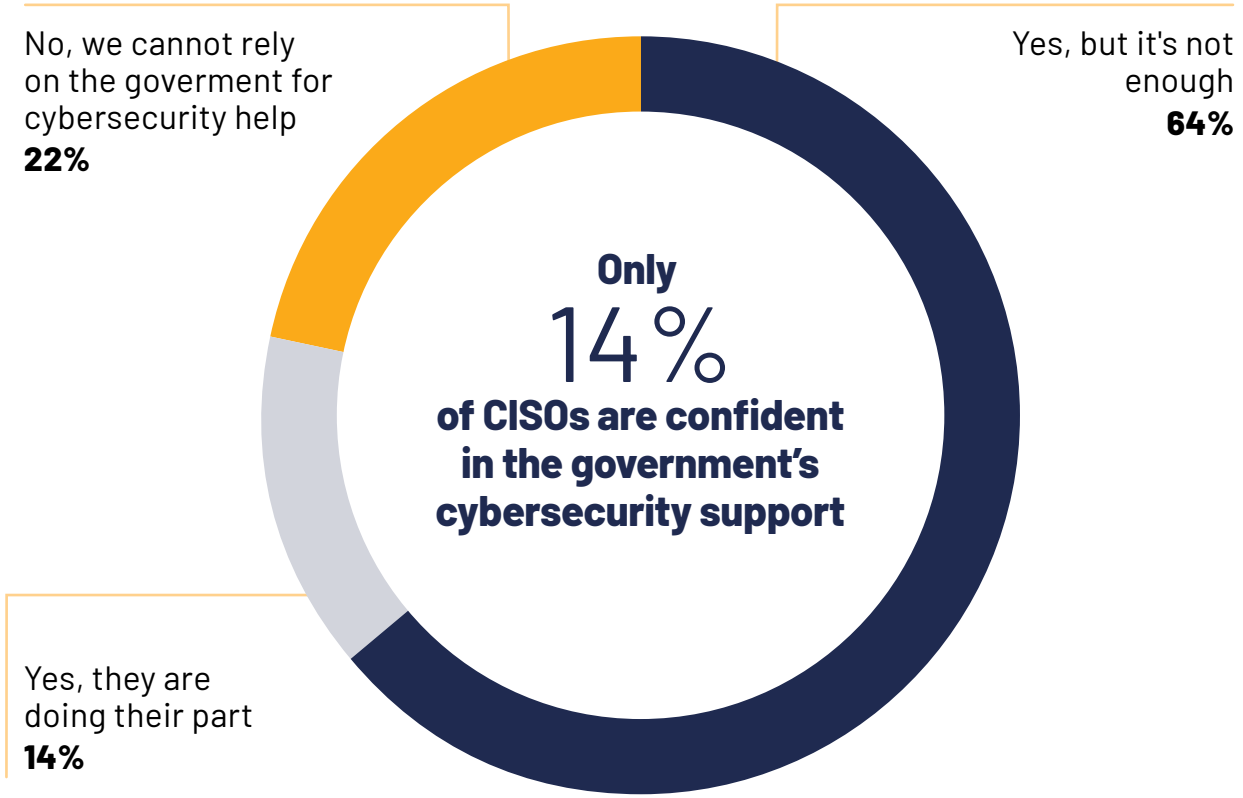
Confidence in government cyber support is low

When asked about their confidence in the government's role in aiding and protecting the private sector from cyberattacks, **only 14% of US CISOs said they believe the government is truly doing its part to help protect the private sector.** Another 64% of enterprises acknowledge government efforts, such as threat intelligence sharing and cybersecurity funding, but view these actions as insufficient.

22% of CISOs said they cannot rely on the government for cybersecurity support.

Government agencies play an important role in shaping cybersecurity policy and enabling collaboration, but their structure and scale often limit their ability to move at the speed required by today's rapidly evolving threat landscape. Initiatives like CISA's Known Exploited Vulnerabilities (KEV) catalog have been valuable in promoting transparency and accelerating information sharing around high-priority threats, helping organizations focus on the vulnerabilities most likely to be used in real-world attacks. Still, the majority of enterprise CISOs recognize that while these efforts are helpful, securing the private sector is not something they can rely on government help for.

Do you feel that your government is doing enough to aid and protect the private sector from cyberattacks?



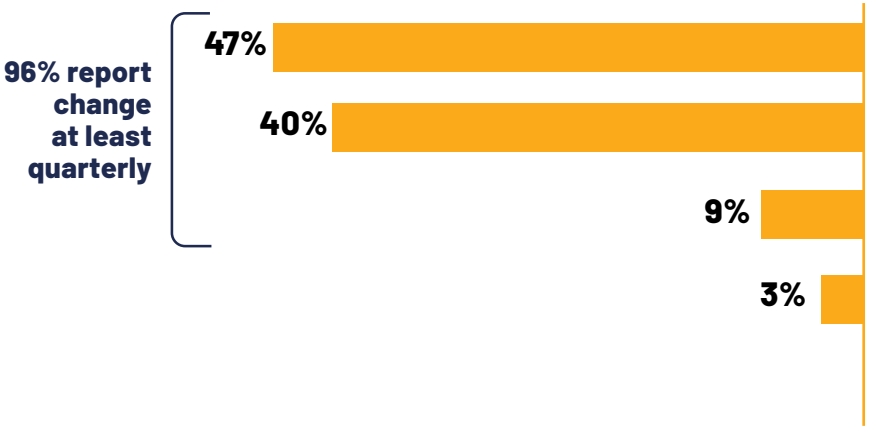
Change outpacing the rate of security validation

Changes to enterprise infrastructure (such as new configurations, added users, and permission updates) occur at a far more rapid pace than security validation. **96% of US enterprises report making such changes on at least a quarterly basis, yet only 30% are pentesting at the same frequency.** These ongoing changes introduce new exploitable security gaps, but most organizations go through long periods where their security controls are left untested, creating exposures that threat actors can capitalize on.

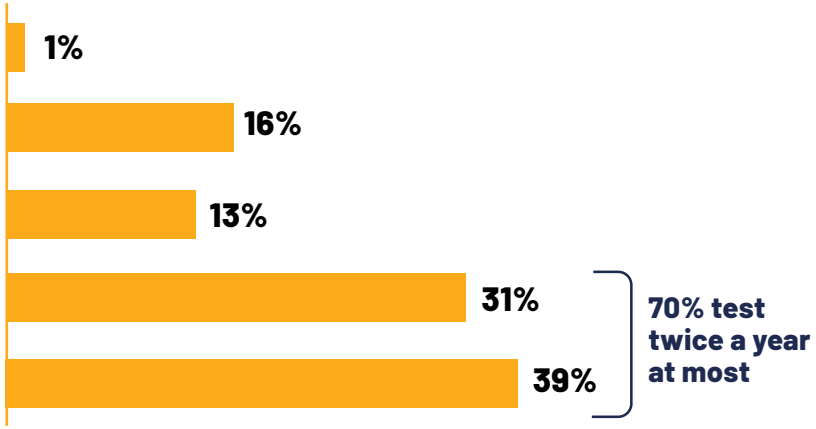
The largest enterprises appear to test more frequently. While 40% of enterprises with 3,000–4,999 employees reported pentesting only once per year, only 22% of enterprises with over 10,000 employees said the same.

Among the largest organizations, 28% conduct pentesting quarterly, compared to just 13% in the smallest group.

How often are you adding and/or changing infrastructure



How often does your organization conduct pentest assessments?



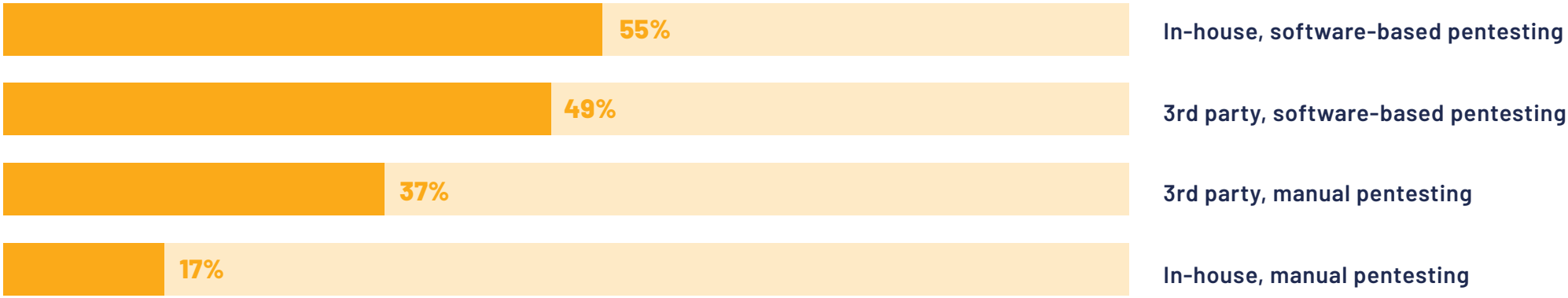
The rise of software-based pentesting

While traditionally a completely manual exercise, pentesting has evolved with software-based approaches now leading the way. A decade ago, allowing automated solutions to execute pentests within the IT environment would have been unthinkable, for fear of accidentally causing an outage. But we are seeing this fear rapidly decline, and software is becoming the standard.

Whether conducted by internal teams or third-party providers, organizations are increasingly using software to scale testing efforts efficiently. Over 50% of enterprises in the sample utilize software-based pentesting to support their in-house programs, nearly three times the number relying primarily on manual methods.

This shift doesn't inherently signal the end of manual testing, but rather a rebalancing of effort. By offloading elements to software, organizations are able to scale their testing significantly while enabling human testers to focus on the complex, adaptive scenarios that require deeper context and critical thinking.

How does your organization conduct pentesting assessments today?



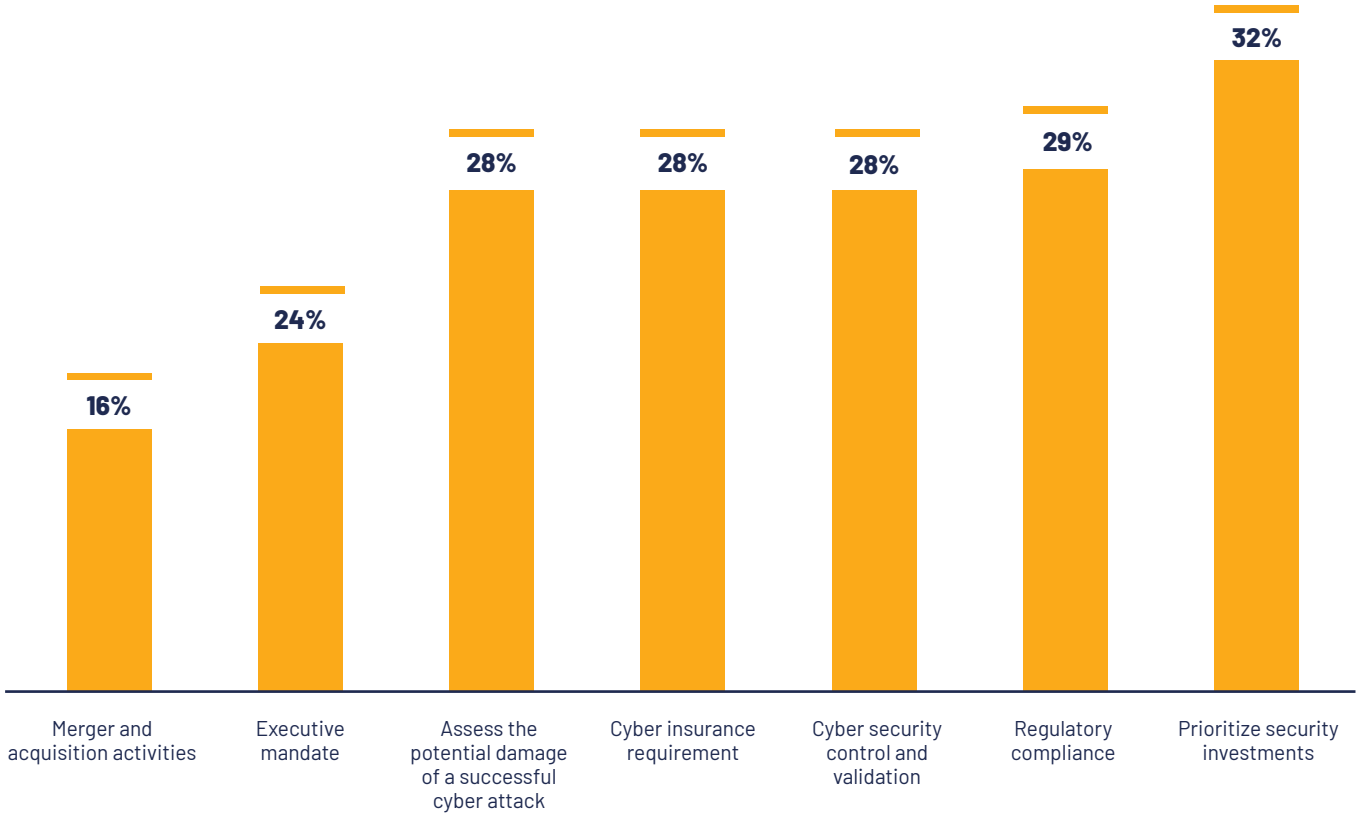
✱ Question allowed more than one answer and as a result, percentages will add up to more than 100%

Pentesting: From compliance obligation to strategic value

While once seen primarily as a compliance requirement, pentesting has evolved into a core component of modern security strategy. Regulatory frameworks in many industries still mandate testing. PCI DSS 4.0.1, for example, requires any organization that stores, processes, or transmits payment card data to perform external and internal penetration testing at least annually, as well as after significant infrastructure changes. The presence of regulation will always compel testing, but many CISOs have moved beyond regulations and it no longer serves as a primary motivator for their testing practices.

For the third consecutive year, **control validation and impact assessment have ranked among the top drivers for pentesting, highlighting the growing strategic importance of validation in security programs.** Enterprises are also utilizing pentesting as a tool for due diligence to prepare for high-stakes business events like mergers and acquisitions.

What are the main reasons your organization conducts pentesting?



✱ Question allowed more than one answer and as a result, percentages will add up to more than 100%

Pentester availability and budget consciousness rise to the top

Despite the growing importance of continuous security validation, there are inhibitors preventing enterprises from growing their pentesting programs and pentesting frequency. This year's data highlights the top inhibitors to more frequent testing, revealing a mix of resource constraints, operational risk concerns, and budgetary pressures.

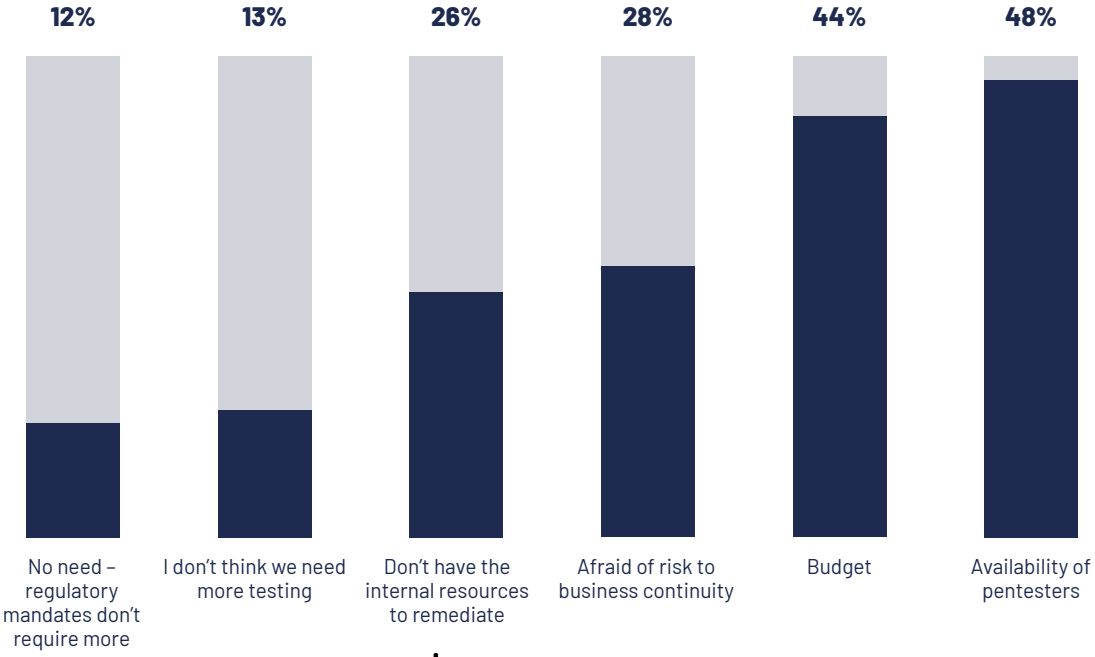
Pentester availability remains one of the most consistent barriers. According to the World Economic Forum, there is a global shortfall of 4 million cybersecurity professionals. For the third consecutive year, the lack of available pentesters ranks among the top two obstacles to more frequent testing among our surveyed CISOs.

Budget constraints have emerged as a more prominent inhibitor in 2025. In the US, 44% of CISOs named budget as a key limiting factor, up sharply from 24% in 2024. As CISOs become more cost-conscious, snapshot-style testing no longer aligns with the expectation for continuous assurance and evolving compliance requirements.

https://initiatives.weforum.org/bridging-the-cyber-skills-gap/home

Operational risk remains a relevant inhibitor, though its priority has declined. Disruption to business continuity was the top concern in 2023, ranked second in 2024, and now sits in third place. Nearly 30% of CISOs cite the risk of outages as a barrier to more frequent pentesting. This concern is especially pronounced in large enterprises, where 41% of CISOs at organizations with over 10,000 employees identify it as a key inhibitor.

Why are you not conducting pentesting assessments more often?



✱ Question allowed more than one answer and as a result, percentages will add up to more than 100%

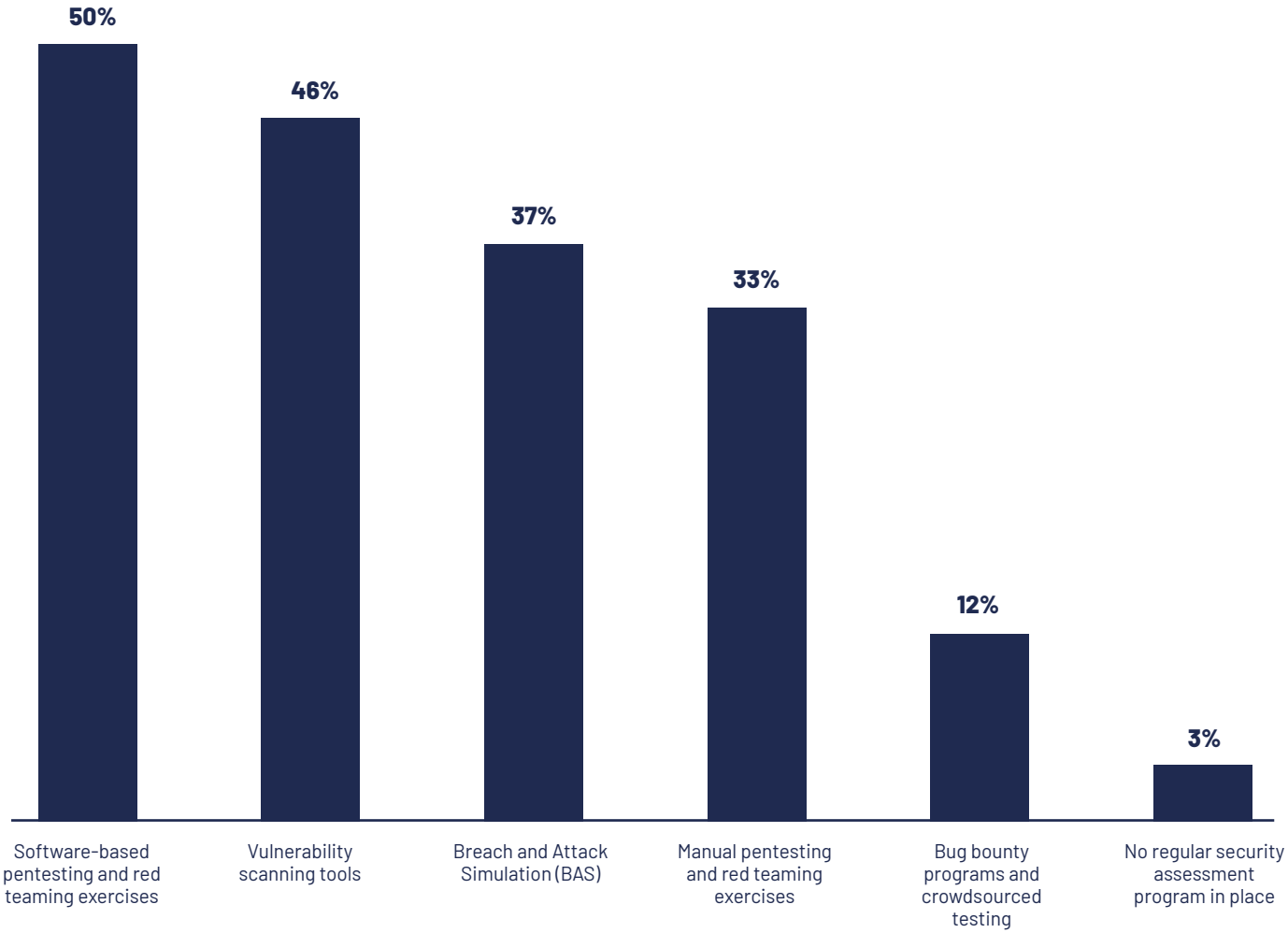
The shift toward automated adversarial testing

While 33% of organizations still rely primarily on manual testing, many are moving toward automated approaches that offer greater scale and efficiency. **Software-based pentesting and red teaming (50%) have become the most widely adopted proactive testing methods,** with Breach and Attack Simulation (BAS) (37%) also gaining traction.

At the same time, traditional vulnerability scanning (46%) remains a staple in many security programs, with organizations continuing to rely on it to uncover exploitable security gaps despite its limitations in validating real-world risk.

The shift towards automated solutions is expected to accelerate as more organizations adopt Continuous Threat Exposure Management (CTEM) frameworks, which emphasizes continuous testing and validation over point-in-time testing.

What are your primary methods for identifying exploitable security gaps in your organization?



✱ Question allowed more than one answer and as a result, percentages will add up to more than 100%

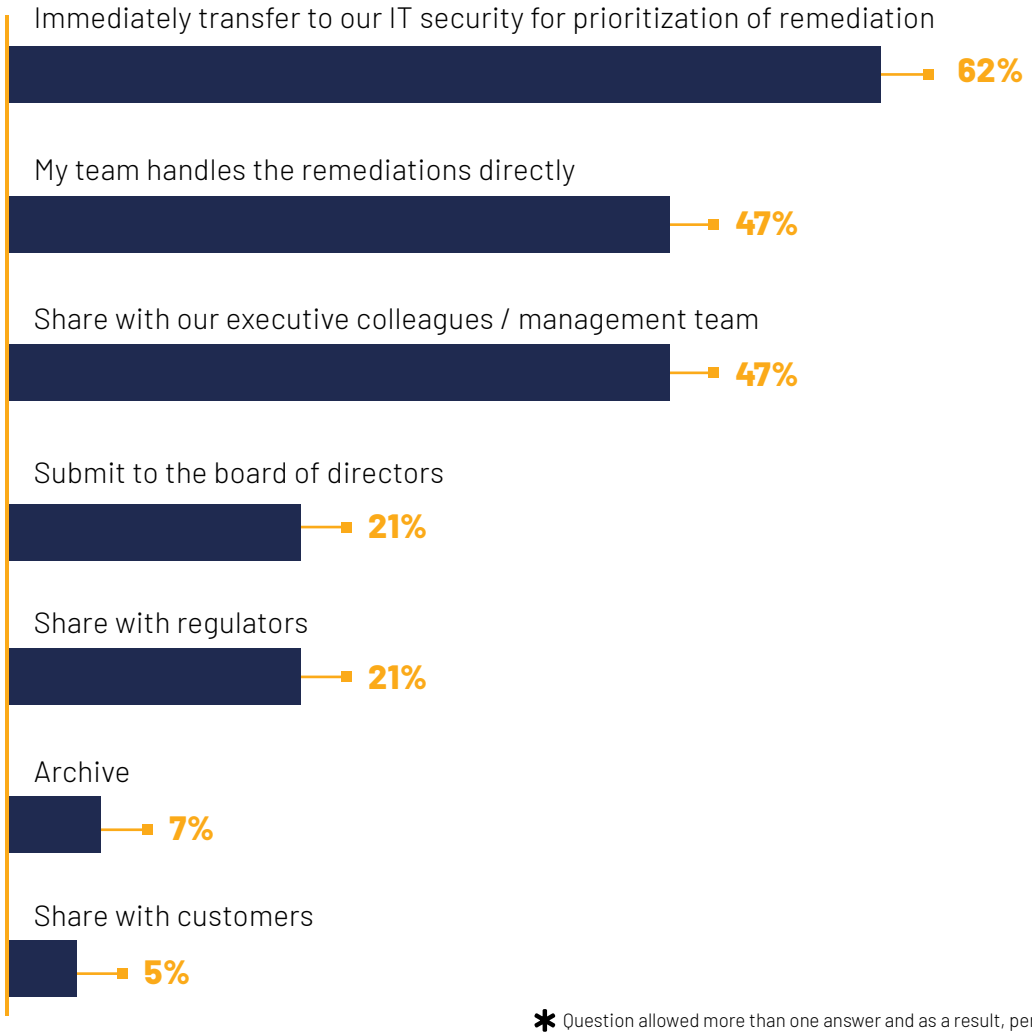
Pentest findings are being operationalized

When it comes to communicating and addressing findings from pentesting, the two most common approaches are either transferring remediation tasks to IT or handling them directly within the security team. In many cases, there's overlap. Some CISOs report using both approaches, depending on the nature of the issue. Security teams may address certain findings directly, while others are handed off to IT teams responsible for the systems or tools involved.

Pentesting reports are also being used well beyond the security function. **Nearly 50% of organizations share results with company executives or senior management,** and 21% share findings with regulators or their board of directors.

This highlights how pentesting is being operationalized; not just as a technical task, but as a risk communication vehicle. Reports are not being shelved; they are informing decisions, justifying investment, and helping translate technical findings into business risk.

What do you do with your pentest report?



✱ Question allowed more than one answer and as a result, percentages will add up to more than 100%

Alignment of risk perception, breaches, and testing focus

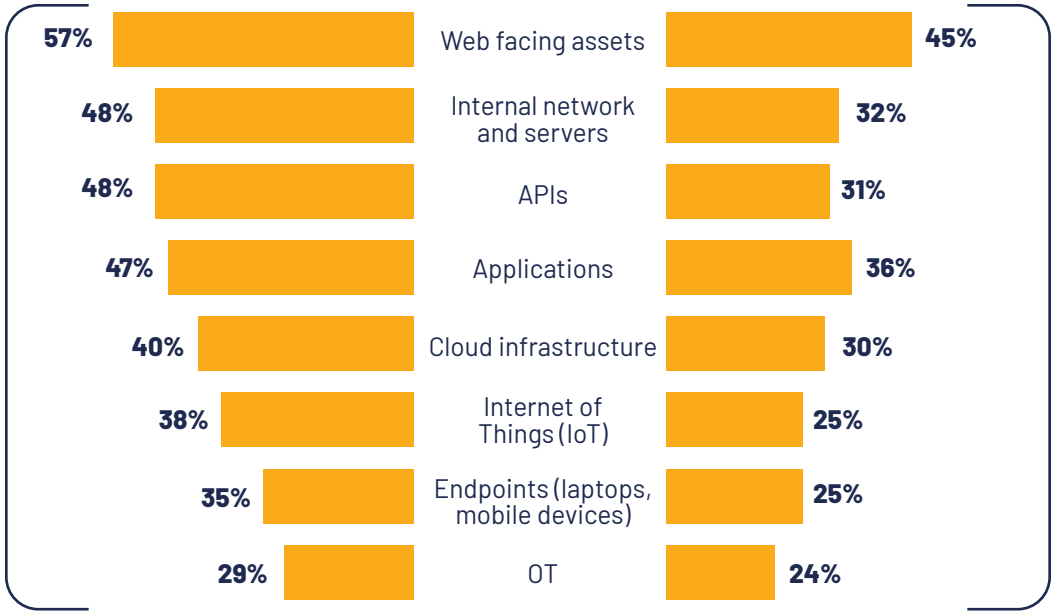
As attack surfaces expand, security leaders are becoming more deliberate in where they direct their testing efforts. **Globally, there is a clear alignment between where organizations perceive risk, where breaches have occurred, and where pentesting activity is focused.**

This alignment is most apparent around external-facing assets, which consistently rank as both the most targeted and most tested components of the enterprise environment. APIs have also emerged as a growing area of concern valued for their role in application logic and system integrations, but often challenging to monitor. Their visibility gaps make them attractive to attackers, and increasingly, a priority for testing.

The data, reinforced by patterns observed in the global attack map, underscores a common mindset: Security leaders recognize that risk is distributed, not concentrated. In response, organizations are expanding their testing strategies to ensure broad coverage, visibility, and readiness across every layer of the attack surface.

This approach aligns closely with the principles of **Continuous Threat Exposure Management (CTEM)**. By testing continuously, security teams can move beyond assumptions and gain real insight into where their true exposures lie, closing the gap between perceived risk and actual risk.

During a penetration test, where do you direct the pentesters to target/test?



Which attack surfaces do you believe are the most vulnerable in your organization?

✱ Question allowed more than one answer and as a result, percentages will add up to more than 100%

What are enterprises spending on their security?

US enterprises allocate an average of $187K annually to pentesting, accounting for 10.5% of their total IT security budget of $1.77M.

Not surprisingly, the data shows that larger organizations tend to invest more. Companies with over 10K employees spend on average $216K on pentesting, while those with 3K-5K employees allocate $168K.

This trend also holds for overall IT security budgets, which grow in parallel with company size, ranging from $1.4M for smaller enterprises to $2M for the largest ones. These findings highlight how security investments scale with organizational complexity, reflecting the increasing need for robust testing as attack surfaces expand.

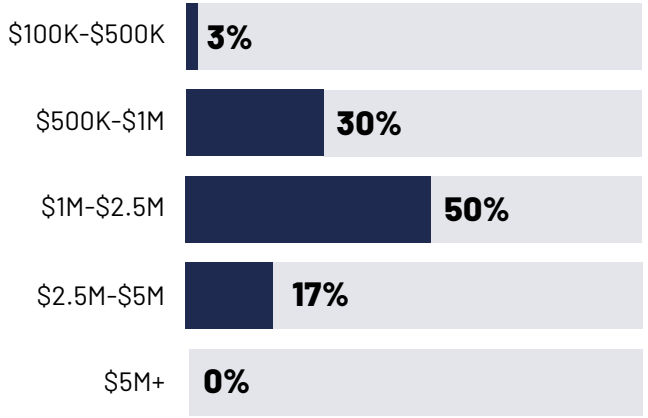
$1.77M

Average annual IT Security budget

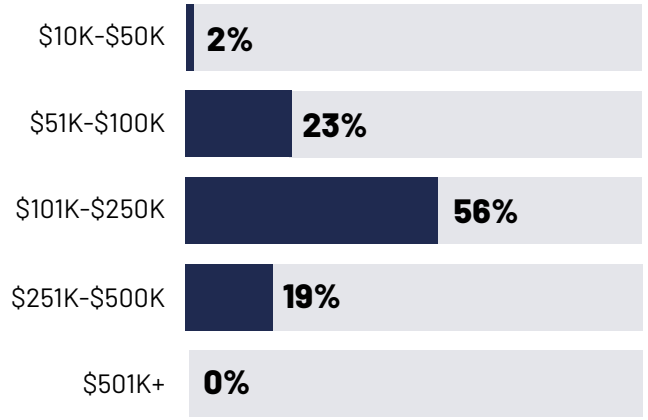
$187K

Average annual pentesting budget

What is your current annual budget in 2024 for overall IT Security across your organization?



What is your current annual budget for pentesting in 2024?



Security budgets are growing in 2025

Very few organizations are cutting back on cybersecurity spending in 2025. In the United States, 90% of CISOs report either maintaining or increasing their overall IT security budgets for the year ahead. Pentesting budgets show a similar trend, with 87% of CISOs reporting stable or growing investment. Only 10% expect a decrease in overall IT security budgets, and 13% anticipate cuts to pentesting spend.

50% of enterprises report an increase to their pentesting budgets in the coming year, while 48% report a rise in their overall security budgets. This indicates that even in the face of economic pressures, security remains a strategic priority particularly in areas focused on validation and exposure management.

Your annual pentesting budget for 2025 is due to:

Your annual overall IT security budget for 2025 is due to:

A detailed look at the numbers behind this report

Industries of respondents

18.4%
Retail & eCommerce

12.8%
Information Technology

12.2%
Software Development

9.2%
Transportation & Logistics

8%
Energy & Utilities

7%
Industrials (Manufacturing, Construction, etc.)

7%
Insurance

5.6%
Health & Pharma

5%
Technology (excluding software development)

4.4%
Banking

2.6%
Telecom

1.6%
Media

1.6%
Public Services

1.4%
Financial Services

1.4%
Travel & Hospitality

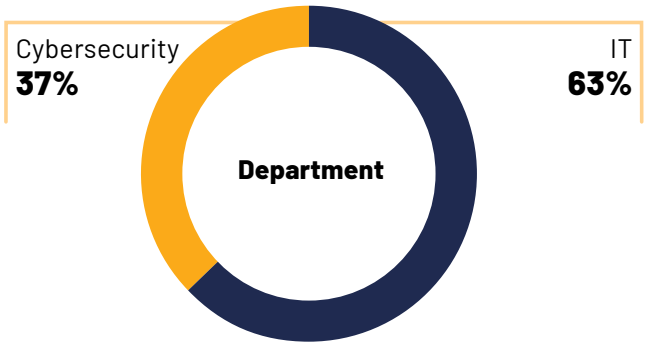
0.8%
Education

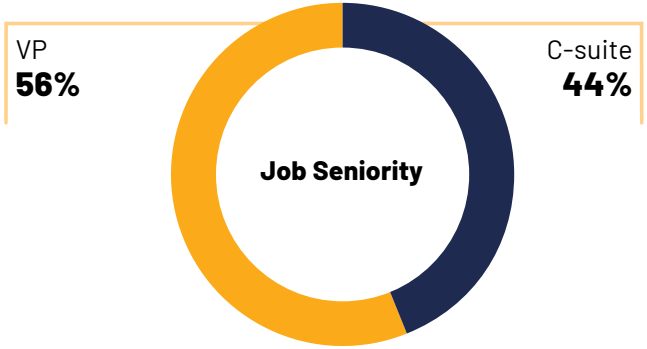
0.4%
Agriculture & Mining

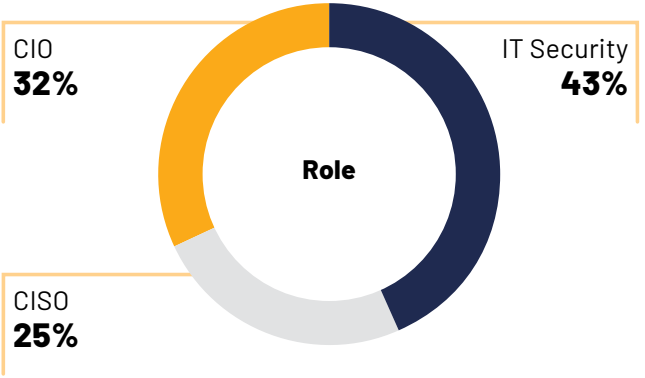
0.2%
Food

0.2%
Non Profit

0.2%
Professional Services







Size of organizations

30%

MID-SIZED
3K-5K Employees

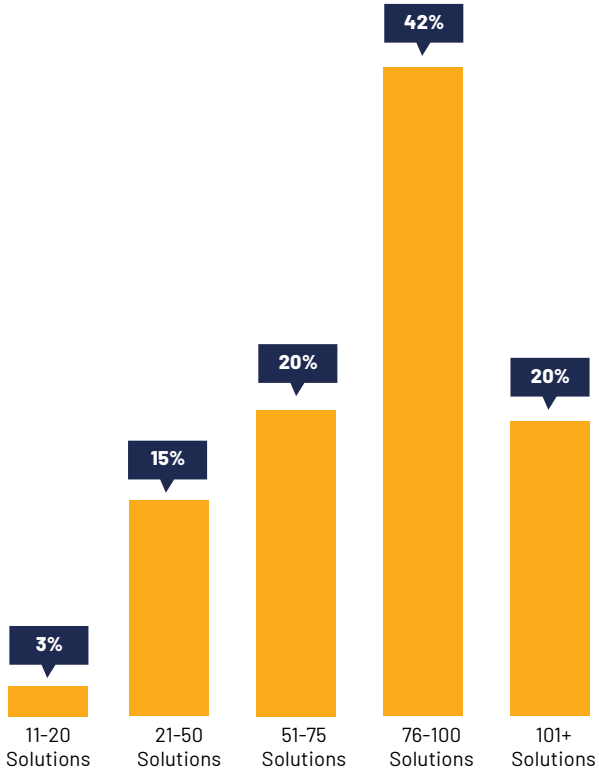
50%

LARGE
5K-10K Employees

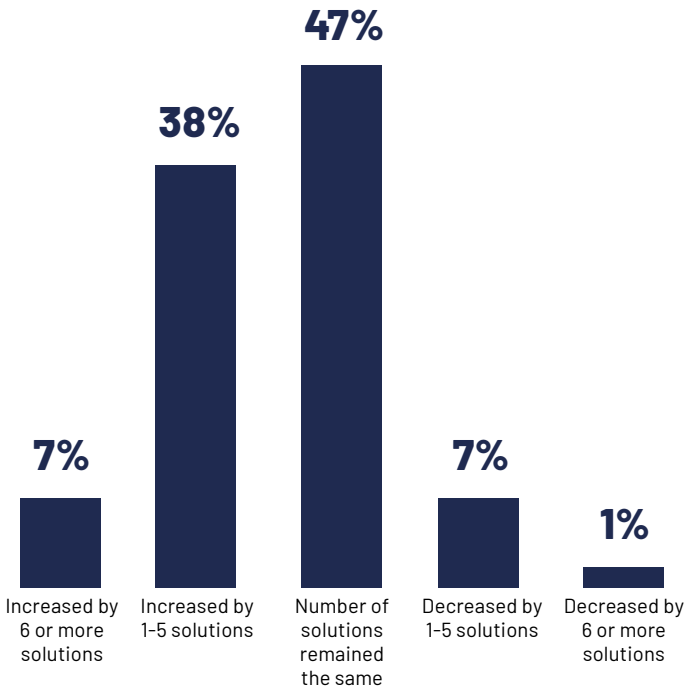
20%

X-LARGE
10k+ Employees

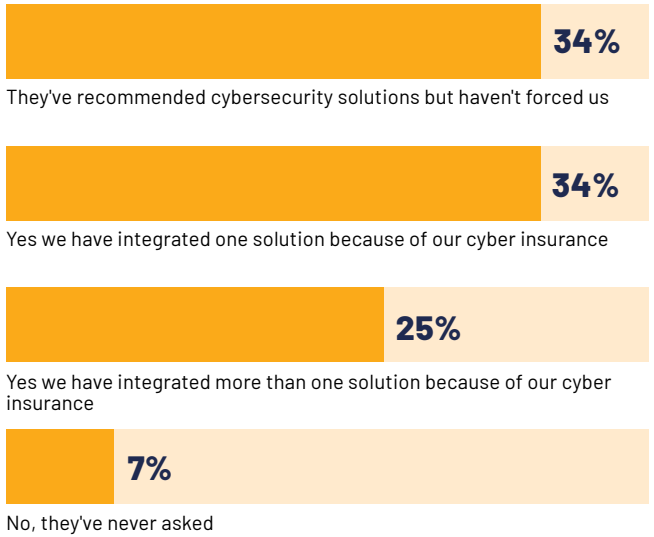
How many security solutions do you currently use across your organization?



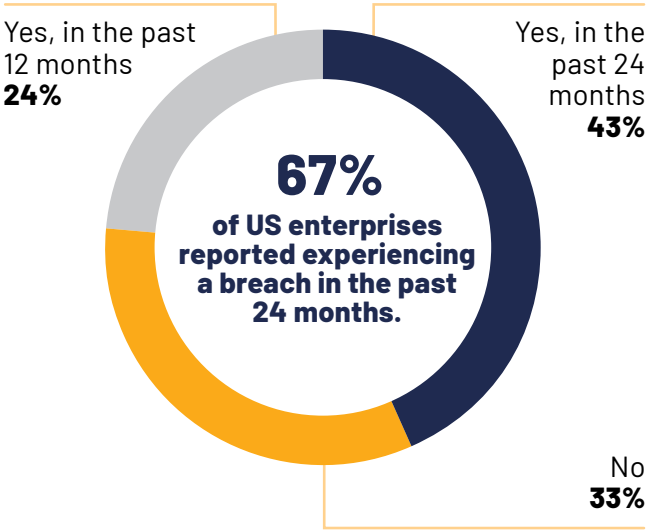
In the past 12 months, how has the NET number of security solutions in your security stack changed?



Has your cyber insurance provider compelled you to integrate a cybersecurity solution you were not previously considering?

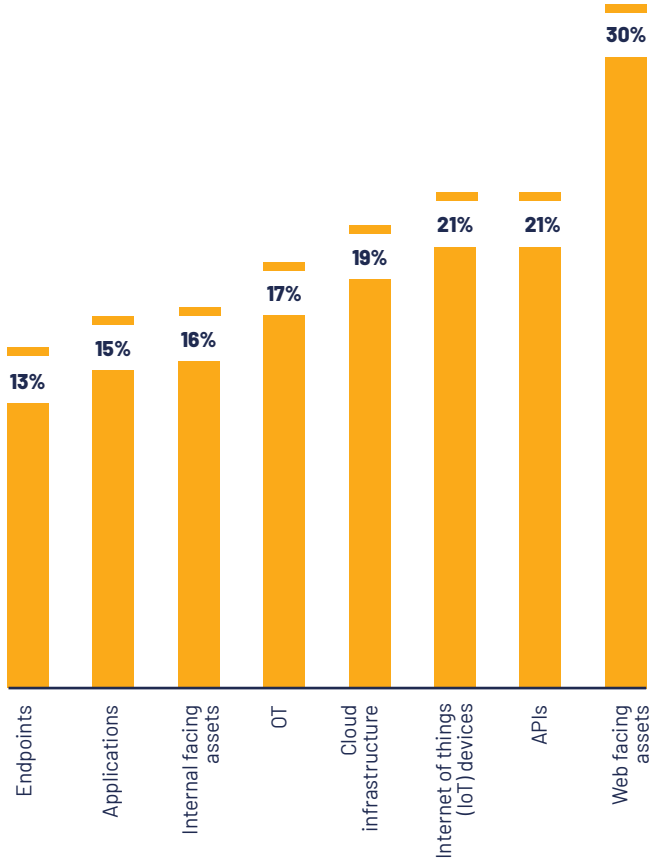


Has your organization been compromised by a cyberattack over the past 24 months?

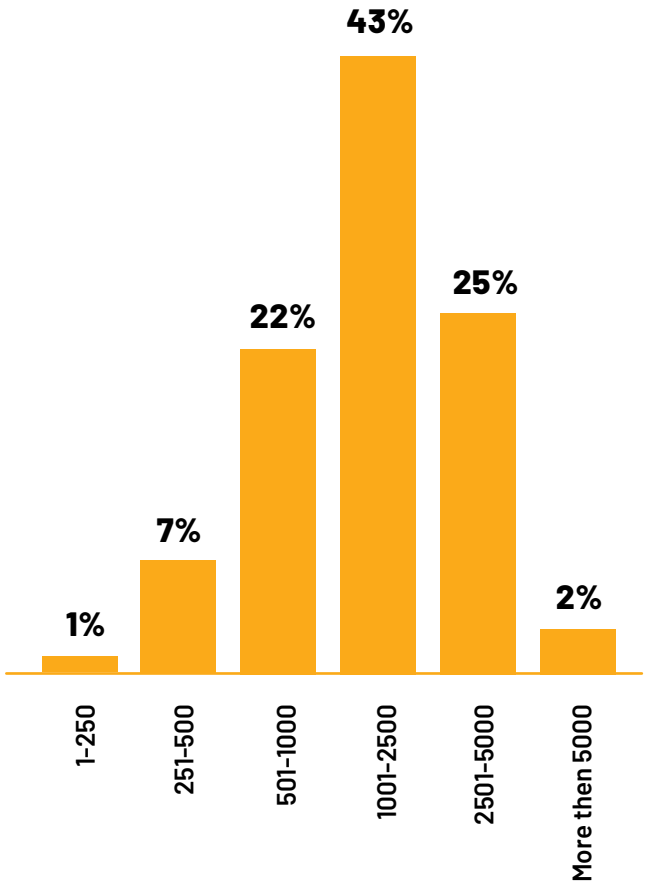


Did your organization experience any disruption or impact as a result of the cyberattack(s) (Select all that apply)

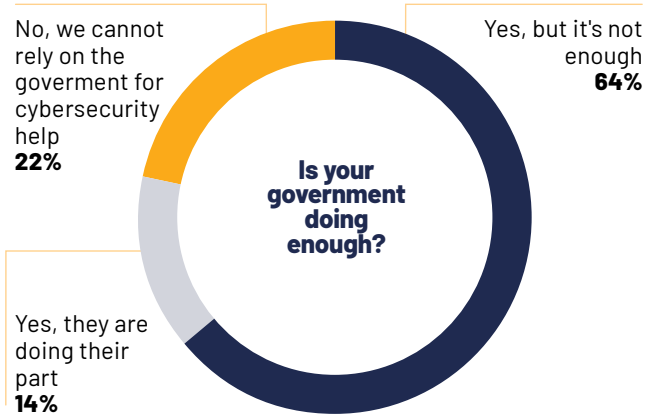
Which aspect(s) of your organization's infrastructure were compromised as a result of the attack(s): (Select all that apply)



How many security "alerts" does your organization receive per week?

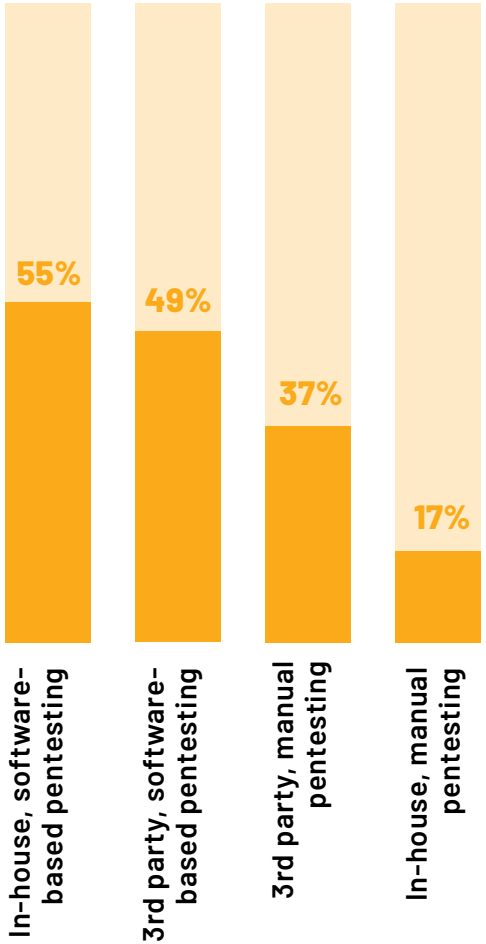


Do you feel that your government is doing enough to aid and protect the private sector from cyberattacks?

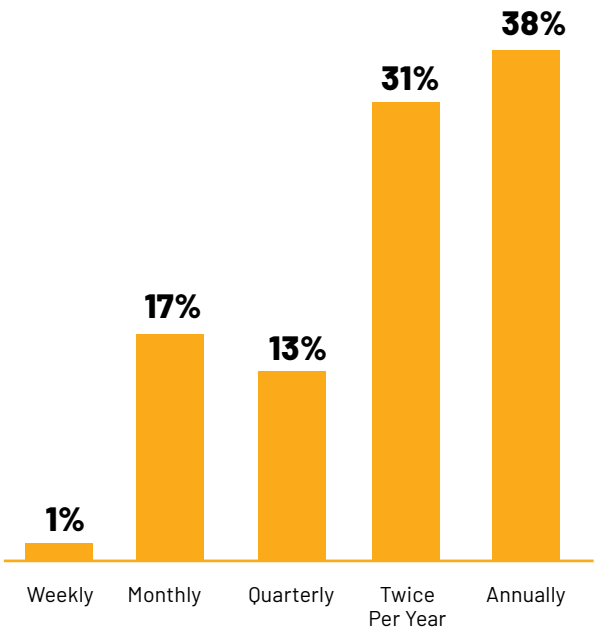


How does your organization conduct pentesting assessments today?

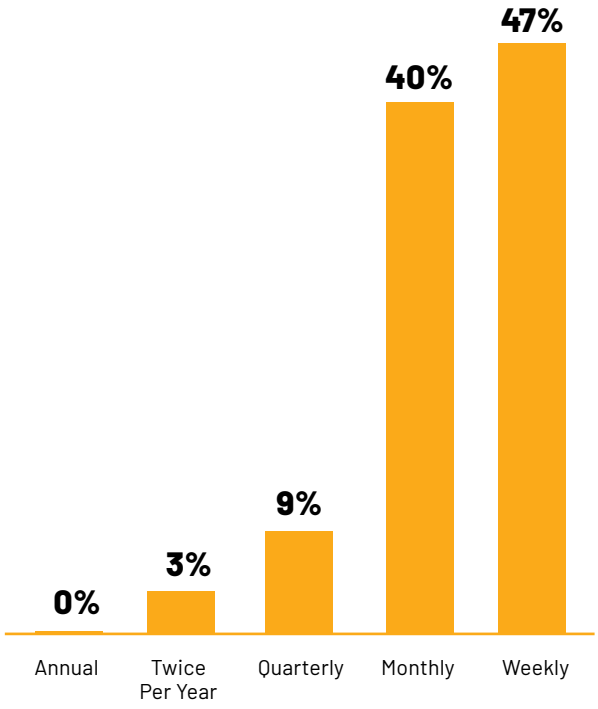
(Select all that apply)



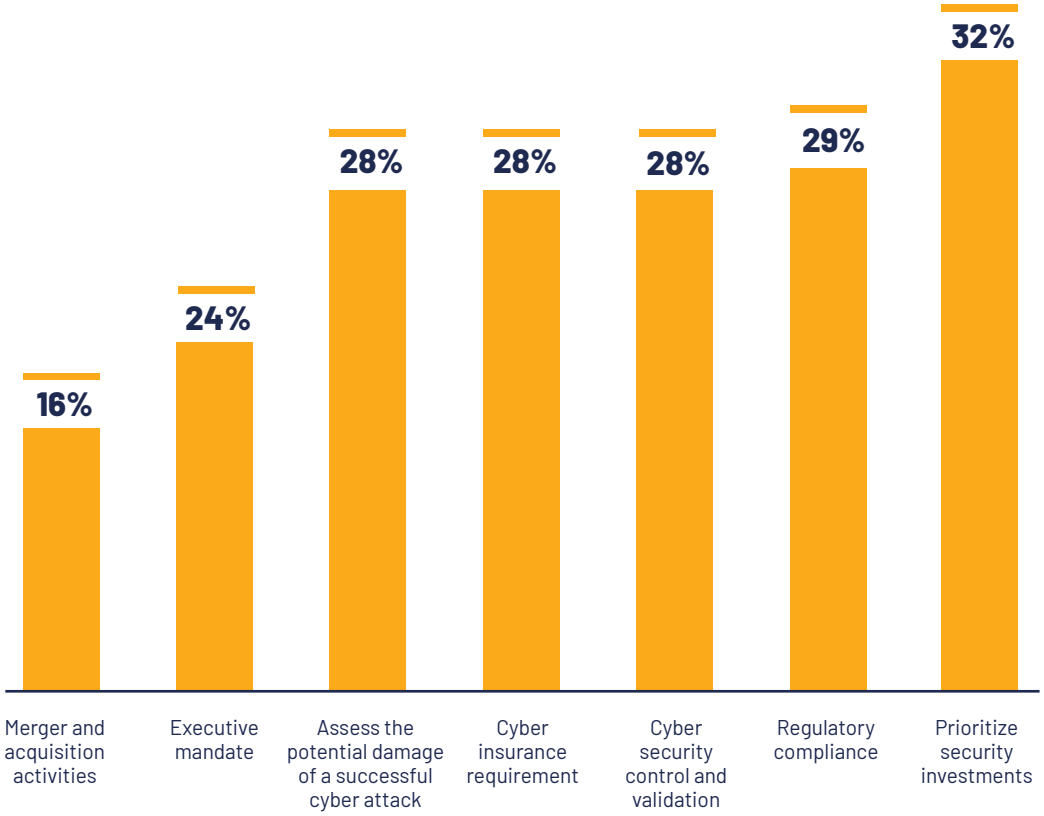
How often does your organization conduct pentest assessments?



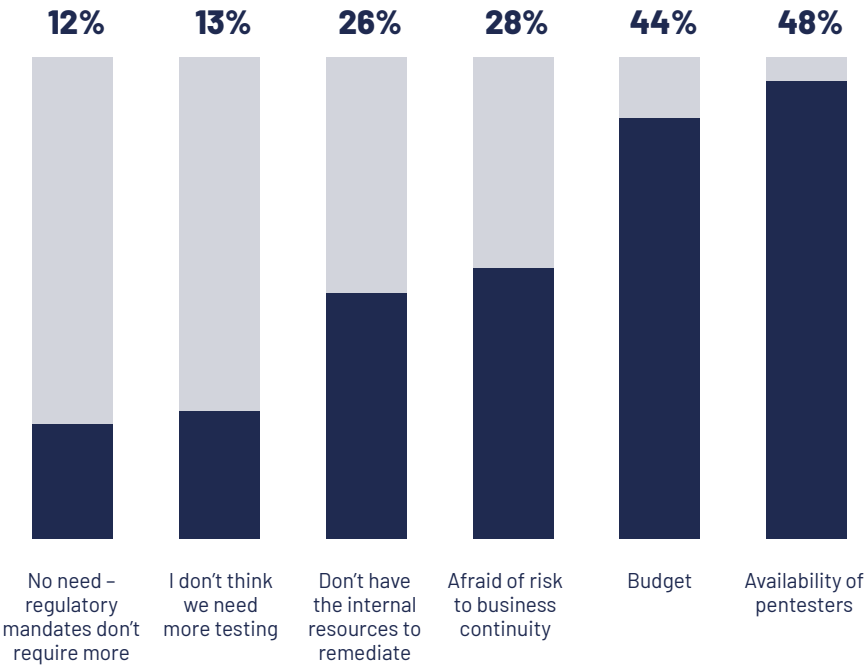
How often are you adding and/or changing infrastructure, applications, or identities in your network?



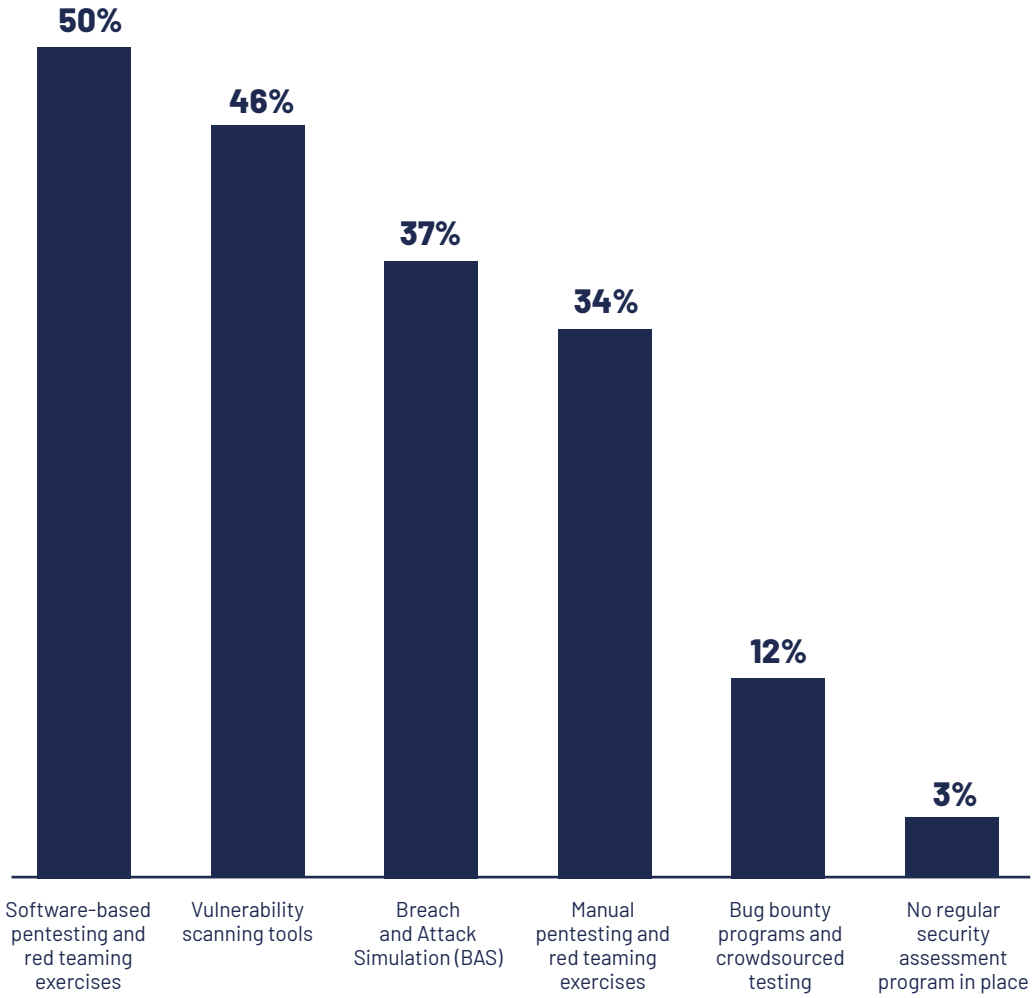
What are the main reasons your organization conducts pentesting? (Select top 2)



Why are you not conducting pentesting assessments more often? (Select all that apply)

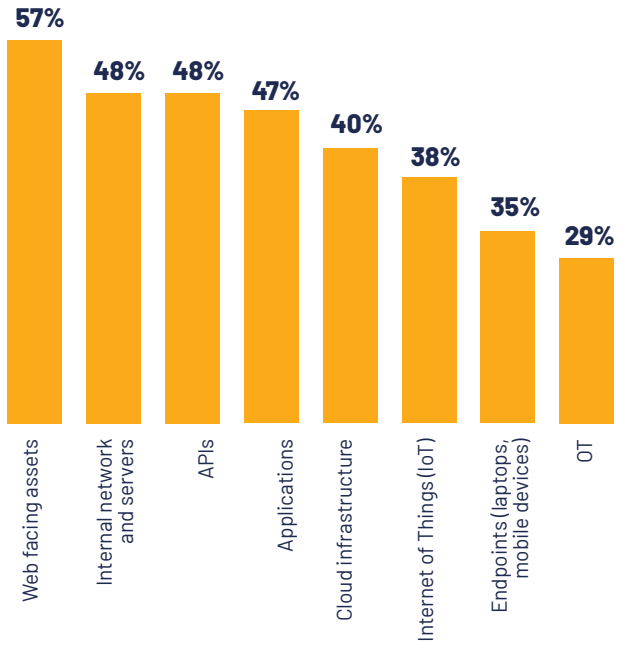


What are your primary methods for identifying exploitable security gaps in your organization? (Select top 2)

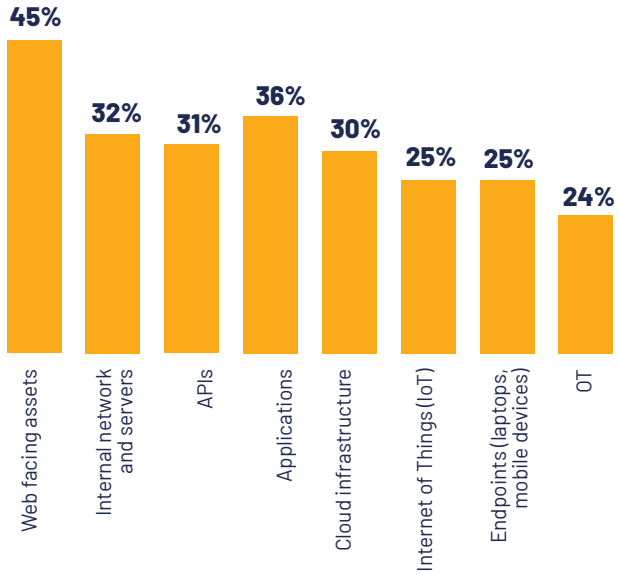


What do you do with your pentest report? (Select all that apply)

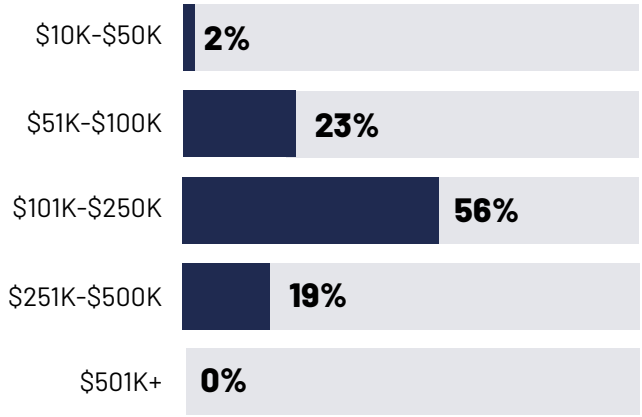
During a penetration test, where do you direct the pentesters to target/test?
(Select all that apply)



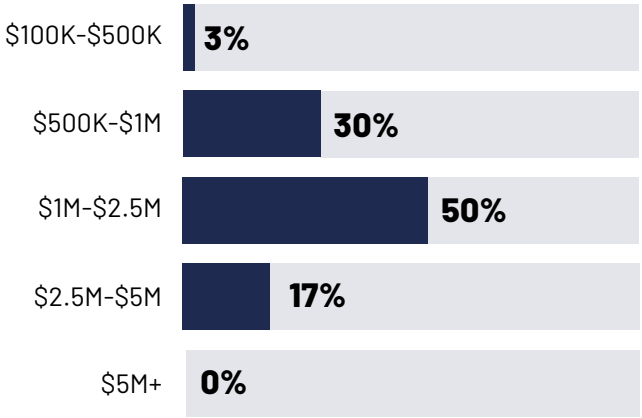
Which attack surfaces do you believe are the most vulnerable in your organization?
(Select all that apply)



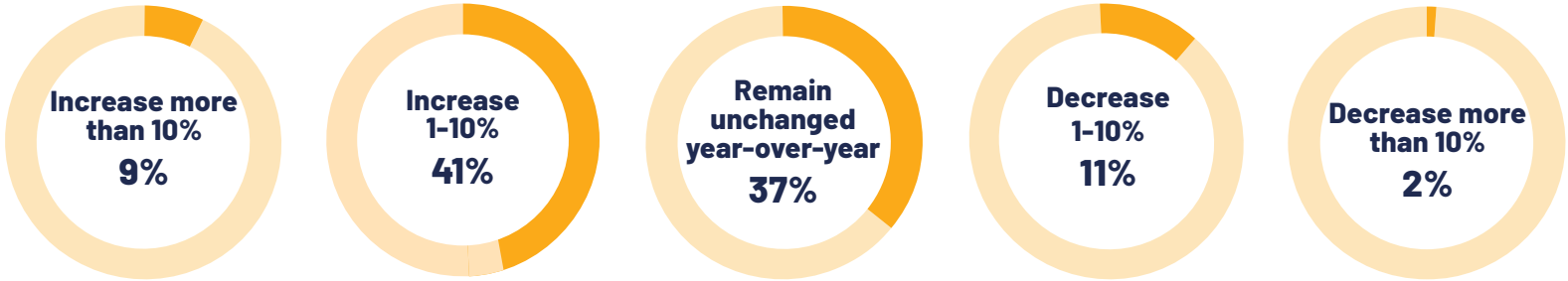
What is your current annual budget for pentesting in 2024?



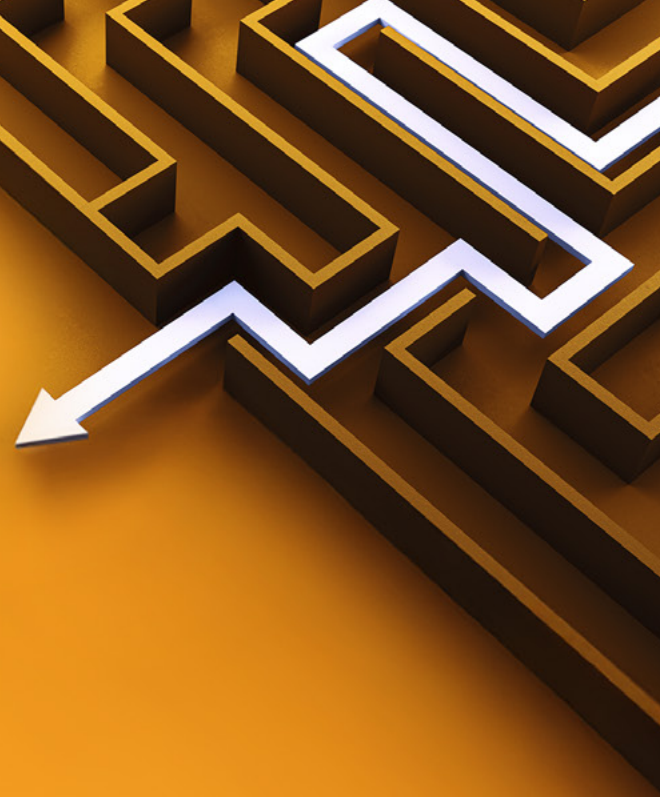
What is your current annual budget in 2024 for overall IT Security across your organization?



Your annual pentesting budget for 2025 is due to:



Your annual overall IT security budget for 2025 is due to:



Pentera's Automated Security Validation Platform

The Pentera Platform automatically uncovers real exposures in the organization's IT environment. Pentera uses an adaptive, rule-based, algorithm to scan and challenge the entire attack surface - Internal, External, and Cloud, providing real-time security validation at scale. Pentera safely performs the actions a malicious adversary would — reconnaissance, sniffing, spoofing, cracking, (harmless) malware injection, file-less exploitation, post-exploitation, lateral movement, and privilege escalation — all the way to data exfiltration. Requiring no agents or pre-installations, the platform gives security teams a complete attack operation view that provides a true assessment of their resiliency against real attacks, prioritizing remediation efforts with a threat-facing perspective. Pentera applies the latest hacking techniques, including ransomware strains and leaked credentials, enabling organizations to focus their resources on the remediation of the vulnerabilities that take part in a damaging "kill chain." With Pentera, organizations continuously reduce cyber exposure and maintain the highest resilience posture by performing validation tests as frequently as needed - daily, weekly, or monthly. This gives companies a better grasp not only of their security gaps but also allows them to test the efficiency of the security stack and maintain consistency across the organization.

About Pentera

Pentera is the market leader in Automated Security Validation, empowering companies to proactively test all their cybersecurity controls against the latest cyberattacks. Pentera identifies true risk across the entire attack surface, guiding remediation to effectively reduce exposure. The company's security validation capabilities are essential for Continuous Threat Exposure Management (CTEM) operations. Thousands of security professionals around the world trust Pentera to close security gaps before threat actors can exploit them. **For more info, visit: pentera.io**