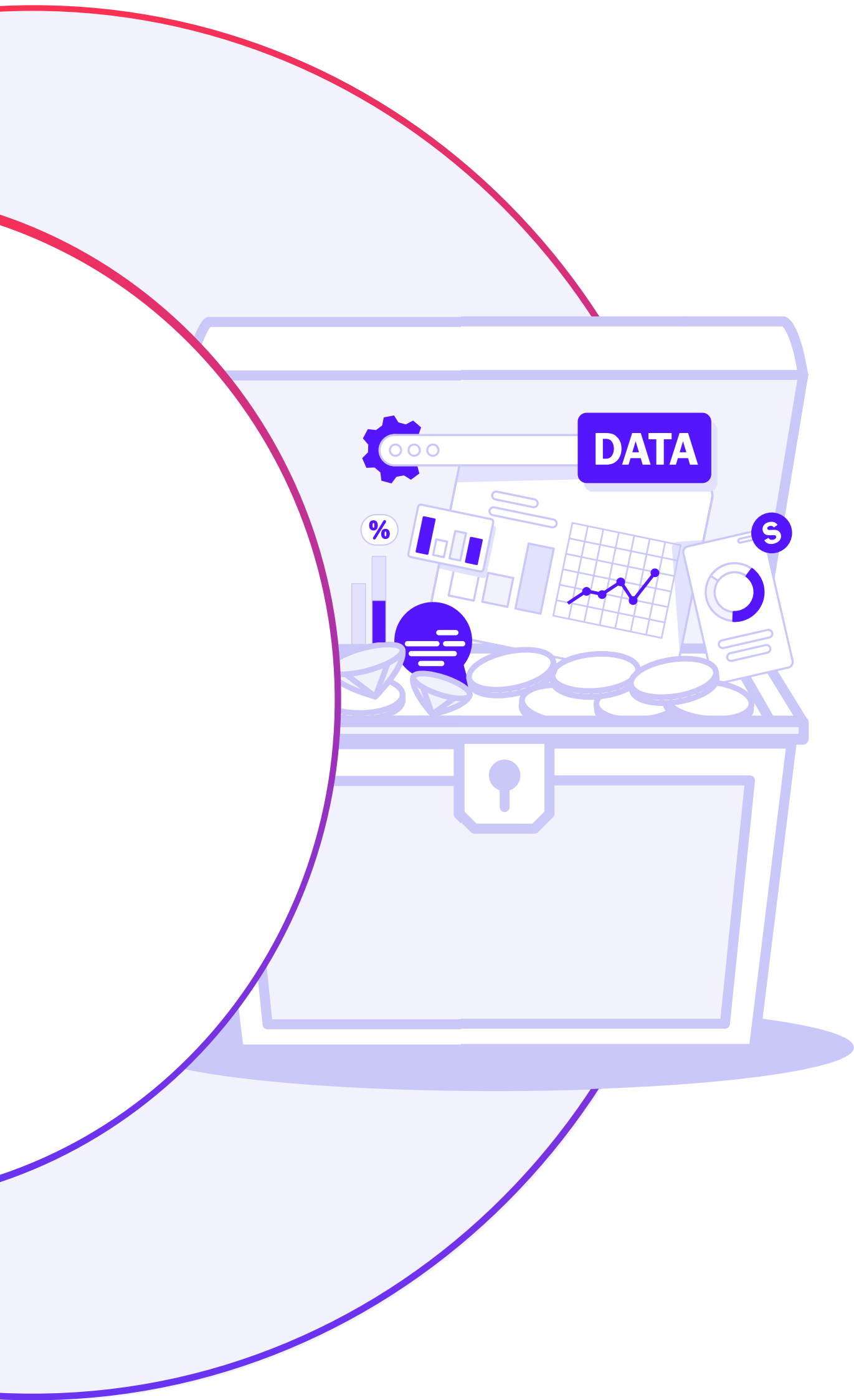




# Threat Exposure Validation Impact Report

The state of CTEM and key trends on automation and AI, cloud exposure validation and the optimization of threat prevention and detection.

**20  
25**



# TABLE OF CONTENTS

Executive Summary	3
Key Findings	4
<b>Chapter 1:</b> Threat Exposure Validation Is a Must-Have in 2025	<b>6</b>
<b>Chapter 2:</b> Organizations Are Struggling to Identify and Remediate Cloud Exposures	<b>10</b>
<b>Chapter 3:</b> Automation and AI Are Essential to Continuous Exposure Validation	<b>12</b>
<b>Chapter 4:</b> The State of Exposure Management	<b>18</b>

## EXECUTIVE SUMMARY

Threat exposure validation is critical to achieving a strong security posture in 2025 and beyond.

We surveyed 1,000 CISOs, SecOps practitioners, and red and blue teamers across the globe to find out how they validate cybersecurity in their cloud, on-prem and hybrid environments.

The *Threat Exposure Validation Impact Report 2025* explores the role of AI, the rise in automation and the need to evolve legacy best practices – like manual penetration testing – into continuous, proactive processes. The report also explores the evolution – and challenges – of exposure management within SecOps teams. The results? Organizations are realizing that reactive security methods are no longer sufficient to defend against the scale, speed and sophistication of new and emerging threats. And an offensive approach that leverages automation and AI is crucial to achieving true cyber resilience.

Our findings also shed light on the current cyber reality – the extent to which organizations have been impacted by breaches; how CISO confidence in their existing processes is at an all-time low; the struggle to identify and remediate cloud exposures; and underlying concerns about security teams' ability to defend against cyber attacks.

The results are clear: Exposure validation is evolving into a pillar of modern cybersecurity, and more organizations are integrating this into their security arsenal to optimize their defenses.





## #1: Threat exposure validation is a must-have in 2025.

- 71% of security leaders agree that threat exposure validation is absolutely essential in 2025
- Organizations that run exposure validation processes at least once per month have experienced a 20% reduction in breaches
- The benefits of deploying exposure validation:
  - Improved mean time to detection (47%)
  - Increased threat resilience against the latest immediate threats (40%)
  - Continuous validation and tuning of security controls (37%)
- 95% of security leaders say testing the threat prevention and detection capabilities of their security controls is important
- 97% of respondents who use automated security control validation and measure cyber program effectiveness have seen a positive impact since implementation

## #2: Organizations are struggling to identify and remediate cloud exposures.

- 61% of security leaders agree their organization lacks the ability to identify and remediate exposures in their cloud environments
- 37% say it can take up to 24 hours to validate cloud exposures
- Only 9% of organizations run exposure validation in their cloud environment daily



### #3: Automation and AI are essential to continuous exposure validation.

- On average, respondents say that compared to manual security testing methods, they can test over 230x more threats with automated security validation
- 89% of security teams have already begun to implement AI into exposure validation processes
- 7 in 10 agree they want their organization to take an innovative approach to leveraging AI adoption for security this year
- On average, it takes organizations who have implemented AI into their exposure validation process 24 fewer hours to test their defenses against newly identified cyber threats
- 65% of security leaders say that missing exposures due to manual penetration testing is an issue for their organization
- 67% say that infrequent testing (e.g., not automated or continuous) leaving gaps in assessments is an issue for their organization when it comes to penetration testing
- More than two-thirds (67%) say that scope limitations are an issue for their organization when it comes to penetration testing

### #4: Successful CTEM depends on validation.

- Almost all (98%) of security leaders say they plan to invest in exposure management in the future, with almost 9 in 10 (89%) stating that they plan to invest within the next 12 months
- 90% of security leaders say they apply validation in their exposure management process at least once a month
- 31% of security leaders say a lack of resources or capacity is one of the biggest challenges they face when remediating identified exposures, while almost half (49%) cite this as a factor that influences their decision to deprioritize exposure remediation

# CHAPTER 1

## Threat Exposure Validation Is a Must-Have in 2025

### Reactive security is no longer enough.

As cyberattacks grow more sophisticated, most security leaders are worried about the ability of their existing security defenses to protect against threats. With 96% of surveyed organizations experiencing at least one security breach in the last year, and long testing times leaving them vulnerable, it's critical that SecOps teams know that their security controls are effective and working as intended. However, the research highlights widespread concern from CISOs over their ability to prevent complex threats.

In fact, 84% of security leaders say they are concerned about their security defenses withstanding an attack from a sophisticated threat actor, with 42% saying they are very concerned about this. Offensive security processes, such as threat exposure validation, are key.

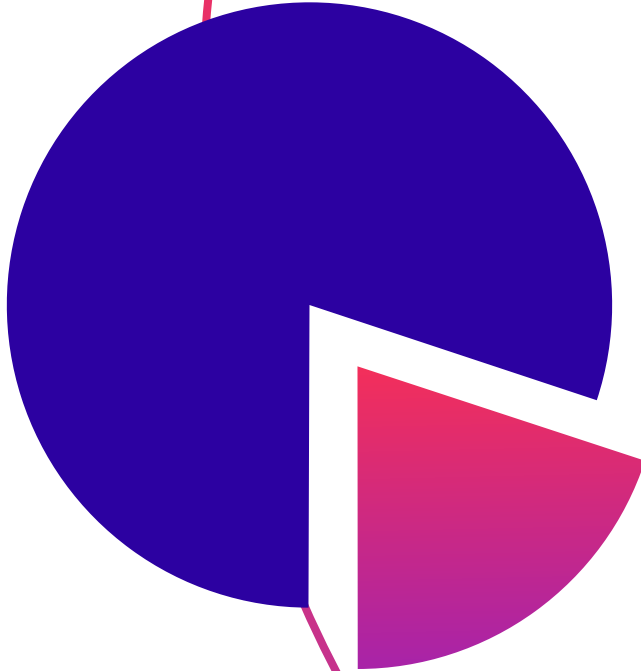
### Threat Exposure Validation, Defined.

Gartner® defines threat exposure validation as part of the **Continuous Threat Exposure Management (CTEM)** process. Threat exposure validation is the process of confirming that an exposure can be exploited. It uses offensive security methods to test security controls, identify weaknesses and validate the exploitability of vulnerabilities and unpatchable points of threat exposure. Use cases include defense optimization, exposure awareness and scaling offensive testing.

According to the research, organizations have implemented various aspects of threat exposure validation, including security control validation (51%) and filtering threat exposures based on the effectiveness of security controls to mitigate threats (48%).

At the same time, nearly all respondents say they have implemented exposure validation in one or more areas, including cloud security (53%), security controls (49%), response (36%) and threats (34%).

These implementations are providing organizations with benefits that help align them to their business goals and risks, including reducing the number of breaches, improving detection mean time, increasing threat resilience and continuous validation and tuning.



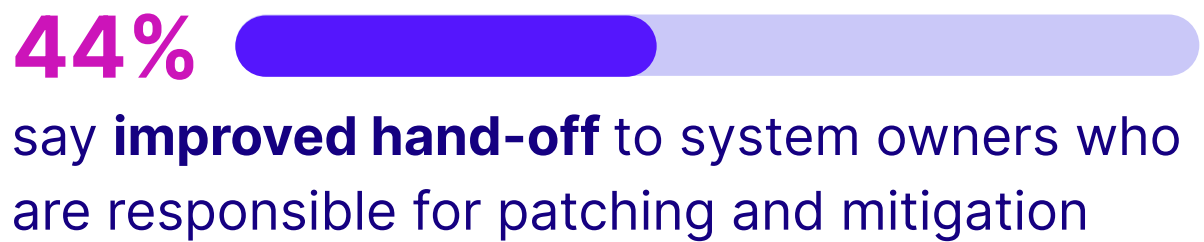
Organizations that run exposure validation testing at least once per month have experienced a **20% reduction in breaches.**

### The Benefits of Exposure Validation

Organizations that run exposure validation testing at least once per month have experienced a 20% reduction in breaches.

Prioritization of security gaps is another benefit highlighted by survey respondents. 37% who have implemented an exposure validation solution say it's resulted in a more efficient prioritization of exposures that are most likely to impact the organization. And 30% say exposure validation has resulted in having readily available cyber resilience metrics.

Here are the top benefits of exposure validation, according to respondents:





## THE BOTTOM LINE:

Exposure validation is a critical part of any CTEM solution. While the benefits – like improved security control effectiveness, more efficient patching and mitigation, and increased resilience against the latest threats – are clear, exposure validation enables security teams to optimize cyber defenses and validate real threat exposures – all with the full context of security control effectiveness, active threat intelligence and business impact.

It's no surprise that 71% of security leaders say that threat exposure validation, which encompasses offensive security technologies, is absolutely essential in 2025.



71%

of security leaders say that threat exposure validation is absolutely essential in 2025.



# CHAPTER 2

## Organizations Are Struggling to Identify and Remediate Cloud Exposures

Cloud environments are complex, ephemeral and often multi-layered – and each layer relies on different security controls for protection. Because of these factors, common cloud security technologies, like cloud security posture management (CSPM), don't validate cloud security effectiveness – leaving organizations in doubt about their true cloud security posture.

While organizations are using a variety of security methods, including cloud SIEM (38%), cloud native tools (38%) and cloud infrastructure entitlement management (CIEM) (38%), their ability to quickly validate cloud exposures on a continuous basis is lacking. The research reveals that many security leaders are unable to adequately manage cloud exposures. In fact, 61% of security leaders say their organization lacks the ability to identify and remediate exposures in their cloud environments.

An additional 37% say it can take up to 24 hours to validate cloud exposures. And only 9% of organizations run exposure validation in their cloud environments on a daily basis. Just 1 in 6 (16%) say they are able to validate exposures in their cloud within one hour.

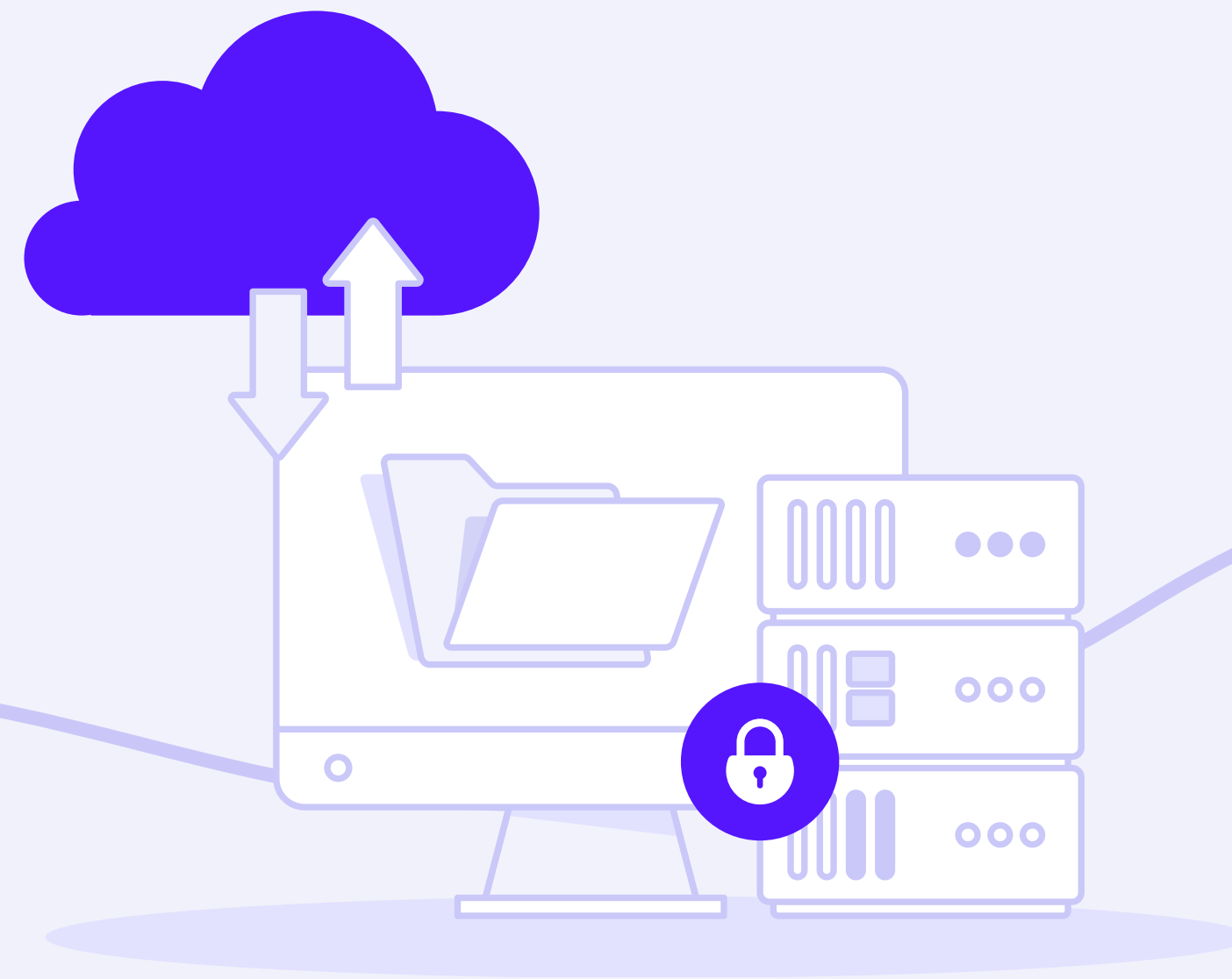
61%



of security leaders agree their organization lacks the ability to identify and remediate exposures in their cloud environments.

## THE BOTTOM LINE:

Securing the cloud isn't the same as securing the perimeter. The same methods, resources and technologies simply aren't enough to stop threat actors from accessing and exploiting valuable – often confidential – resources. The solution? Implement a comprehensive exposure validation platform that actively tests each layer of your cloud architecture to validate effective security and identify points of threat exposure.



# CHAPTER 3

## Automation and AI Are Essential to Continuous Exposure Validation

**The use of automation and AI continues to grow across enterprise environments.** Manual processes simply can't keep up with the countless alerts, misconfigurations, gaps and potential threats plaguing organizations on a daily basis. It's no surprise that many organizations are implementing automation and AI into their security processes. When asked what security validation methods they use, respondents surveyed were most likely to say automated security control validation (44%) and automated penetration testing (39%).

Automation is having a major impact on organizations' ability to filter through alerts and identify the threats that require immediate remediation. On average, respondents surveyed say that compared to manual security testing methods, they can test over 230x more threats with automated security control validation. Further, respondents who have had 1-3 security breaches in the past year can test 197x more threats with automated security validation vs. manual methods, compared to those who have had 7-9 security breaches, who can test 356x more.

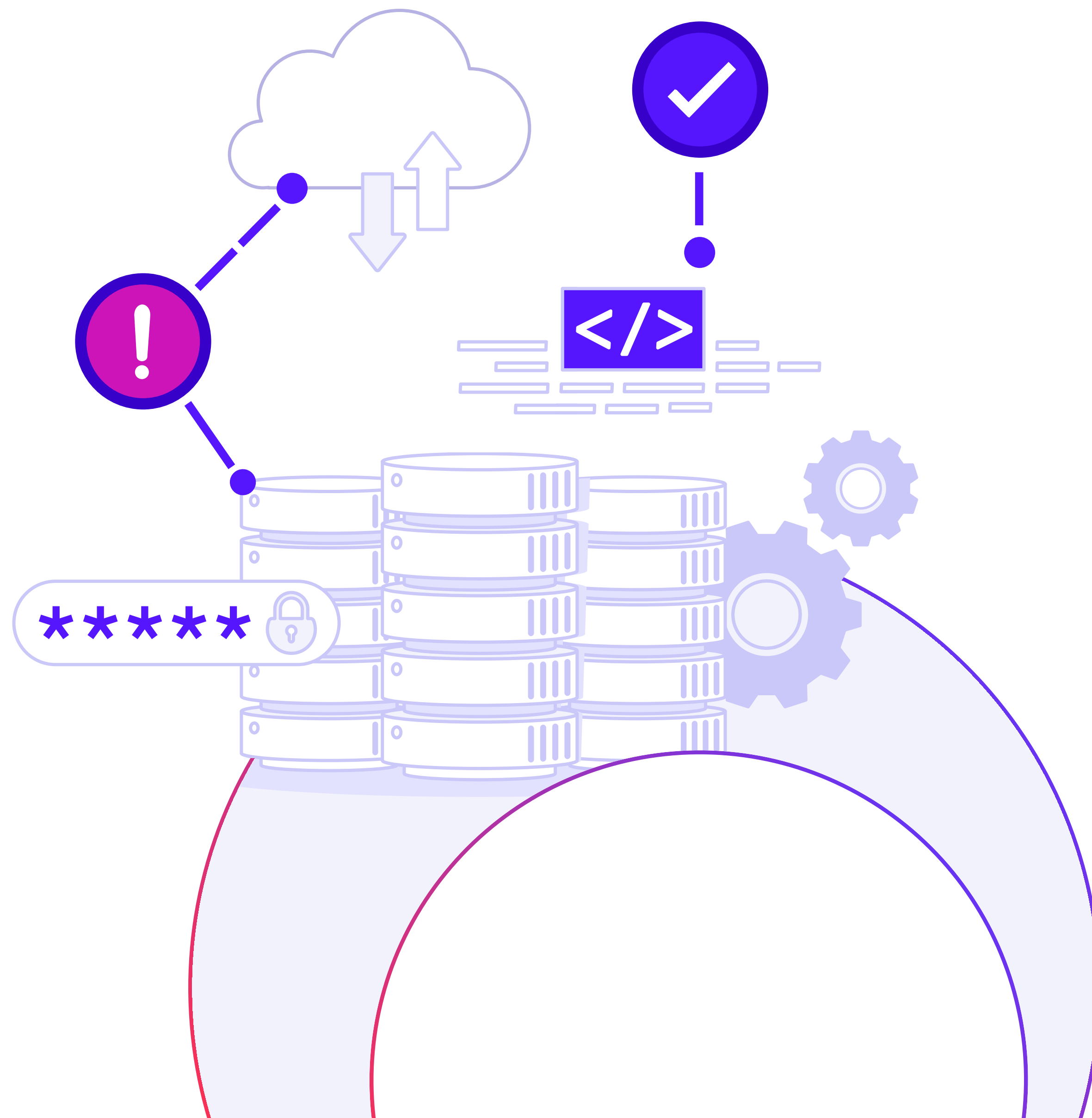
### Automated Security Control Validation vs. Automated Pen Testing

While both technologies are forms of proactive security, automated security control validation uses technologies like breach and attack simulation (BAS) to test and optimize each control against the full MITRE ATT&CK framework and active threat campaigns. Each control is scored separately for its prevention and detection effectiveness while identifying security drift.

In contrast, automated pen testing targets the infrastructure and applications with automated threat emulation to identify security weaknesses and highlight the impact of a successful attack.

**230x  
more  
threats**

can be tested with  
automated security  
validation compared  
to manual security  
testing methods.



## Multiple Methods of Automated Security Control Validation are Already in Play

The majority of security leaders recognize the importance of testing their security controls using automation, and various security validation methods are already being deployed across multiple areas. In fact, 95% of survey respondents say testing the threat prevention and detection capabilities of their security controls is important.

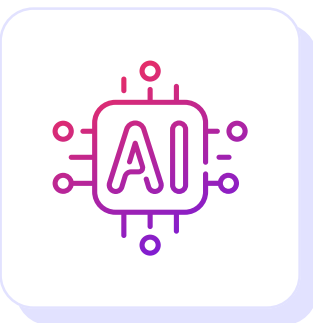
Almost all (97%) of survey respondents who use automated security control validation and measure cyber program effectiveness report they have seen positive changes in their security metrics since implementing automated security control validation, including a decrease in breaches or associated costs.




### Enterprises are Embracing AI

The research also indicates that organizations are embracing AI as a way of bolstering their cybersecurity protocols. 89% of respondents have already begun to implement AI into their exposure validation processes. And 7 in 10 agree that this year they want their organization to take an innovative approach to leveraging AI adoption for security.

The evidence points to AI having a positive impact on identifying cyber threats. On average, it takes organizations who have implemented AI into their exposure validation process 24 fewer hours to test their defenses against newly identified cyber threats, compared to those who have not implemented AI.

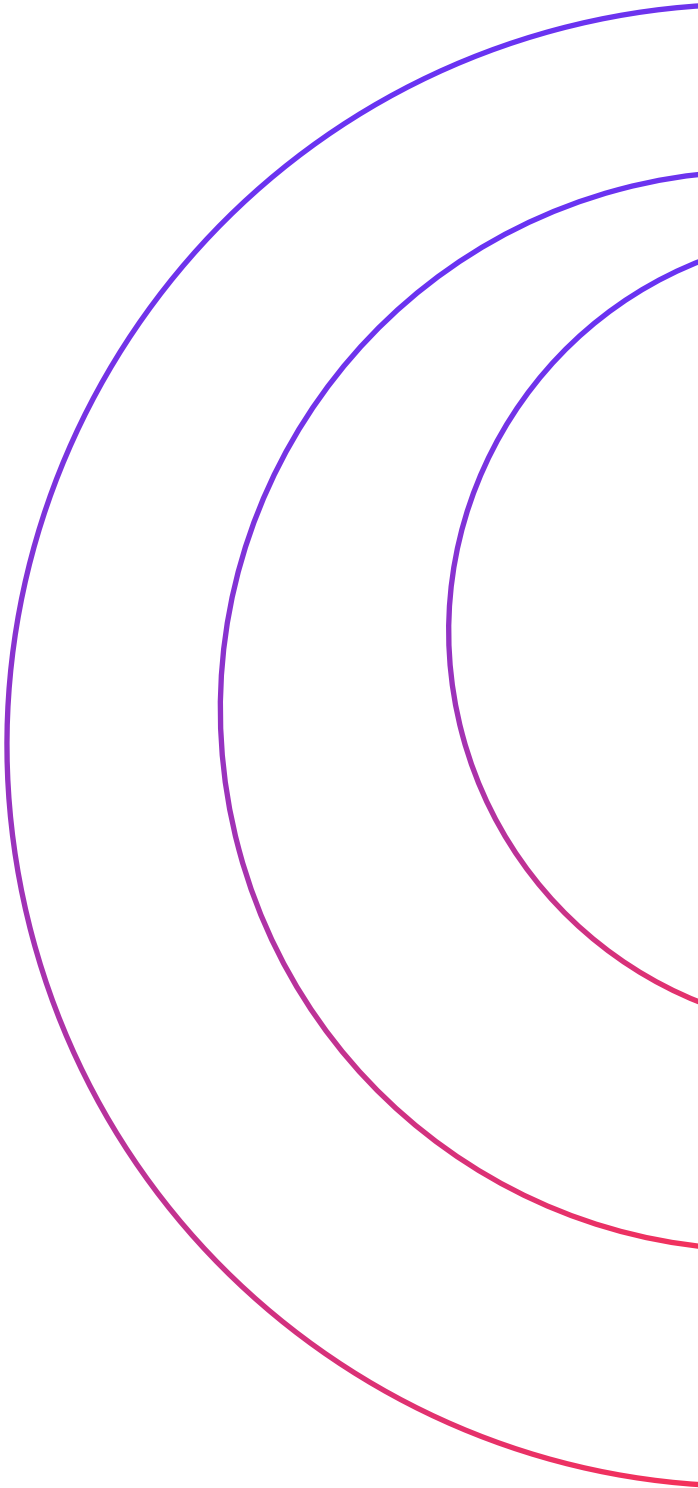
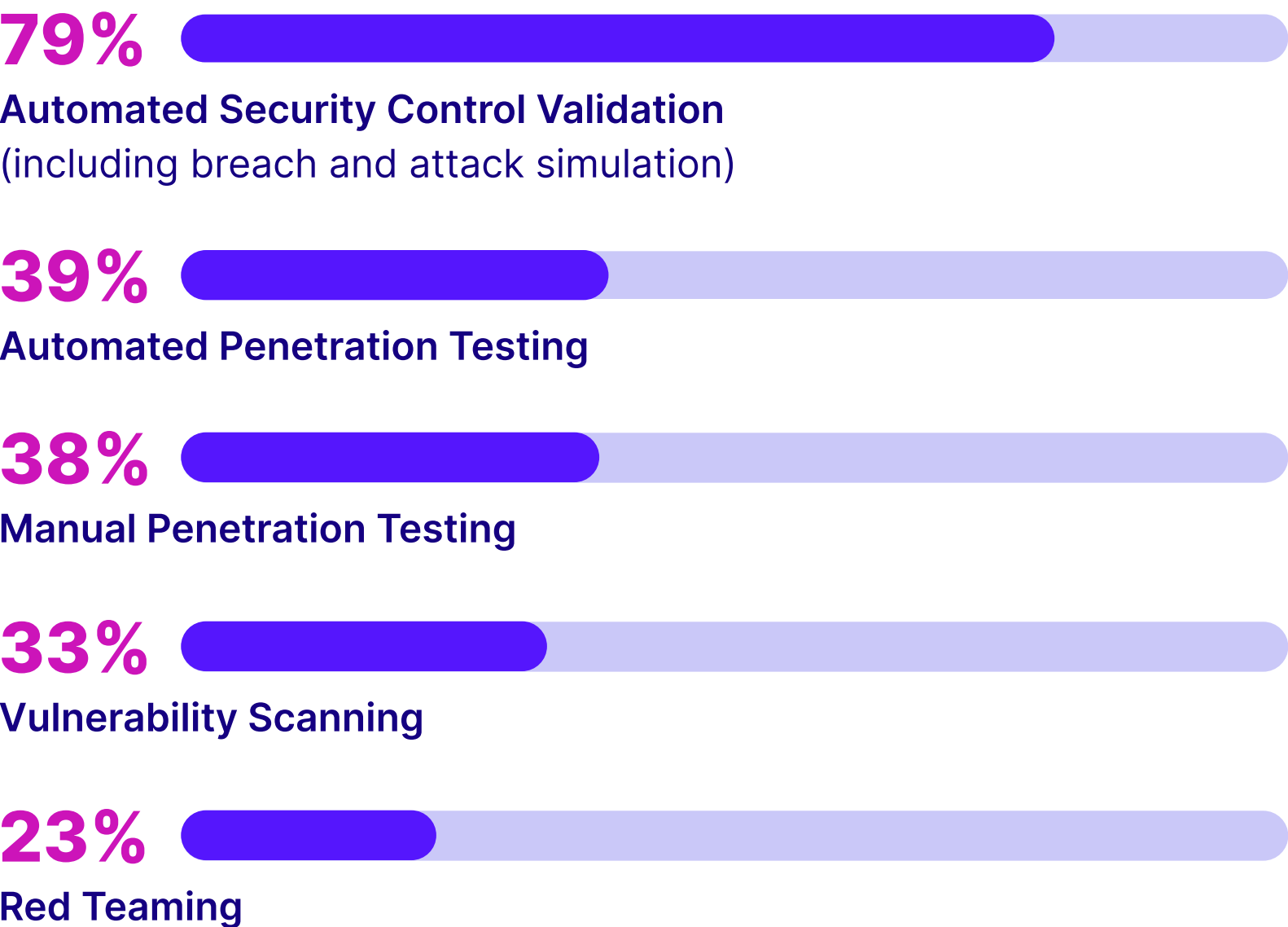


**89%**   
have implemented AI into their exposure validation process.

### Manual Pen Testing Leaves Gaps, Exposures and Limitations

The research highlights that despite the shift towards automation and AI, some organizations are still reliant on legacy security systems and processes.

Multiple security validation methods are already being deployed:





Pen testing is a good example of legacy security processes. It's manual, costly, limited in scope and has reduced defense efficacy. Pen tests only provide a point-in-time assessment, so they're most effective when combined with other security practices – like automated security control validation – to create a multi-layered defense strategy.

In fact, 67% of respondents say that when it comes to manual pen testing, the major drawback is the infrequent testing (e.g., not automated or continuous testing). This leaves long gaps between assessments, so they don't identify security control drift or understand the potential impact of new threats.

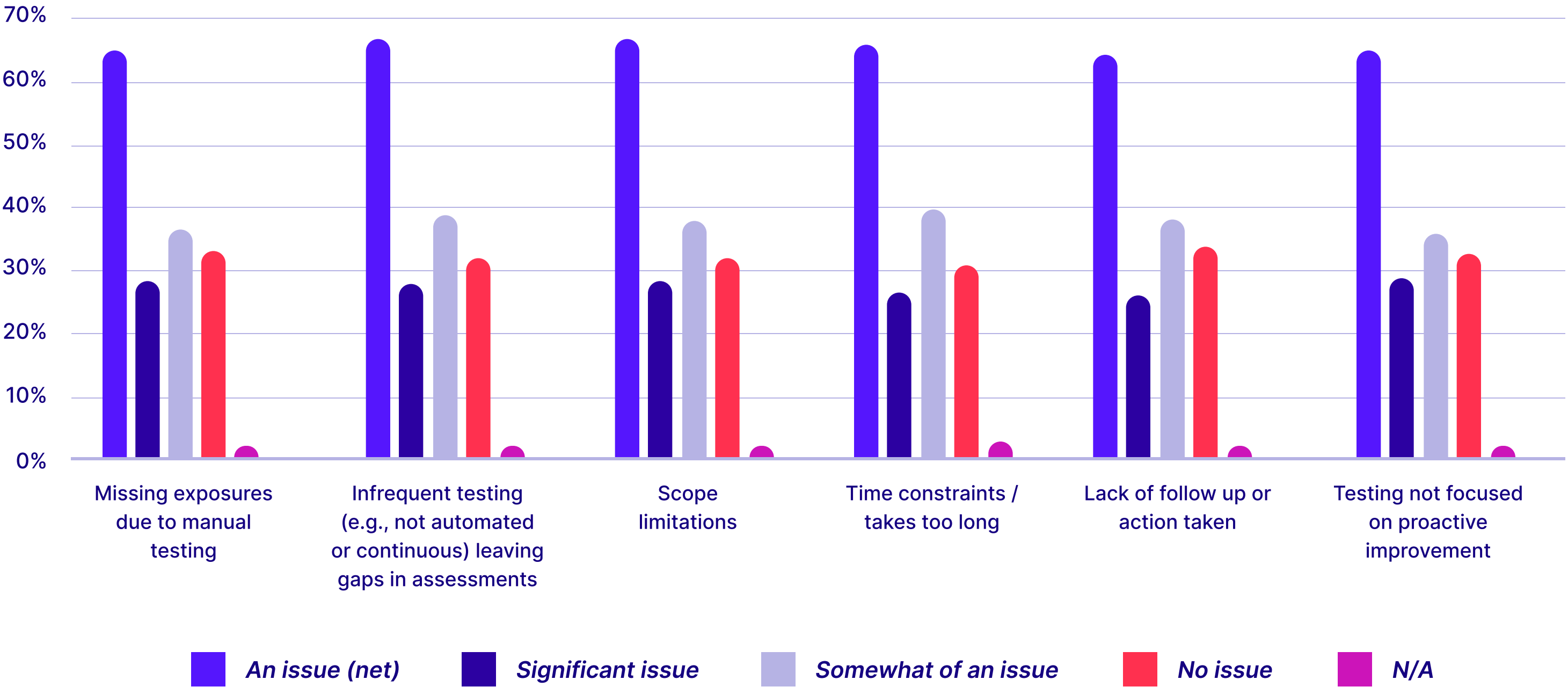


**67%**

say infrequent testing due to manual pen tests leaves gaps in assessments

**The majority of security leaders agree:** Manual pen tests can't deliver on security validation. More than two-thirds (67%) say that scope limitations are an issue for their organization when it comes to penetration testing. Plus, time constraints (66%) and missing exposures due to manual testing (65%) are also cited as issues, highlighting a clear opportunity for organizations to achieve more value, efficacy and results through automation.

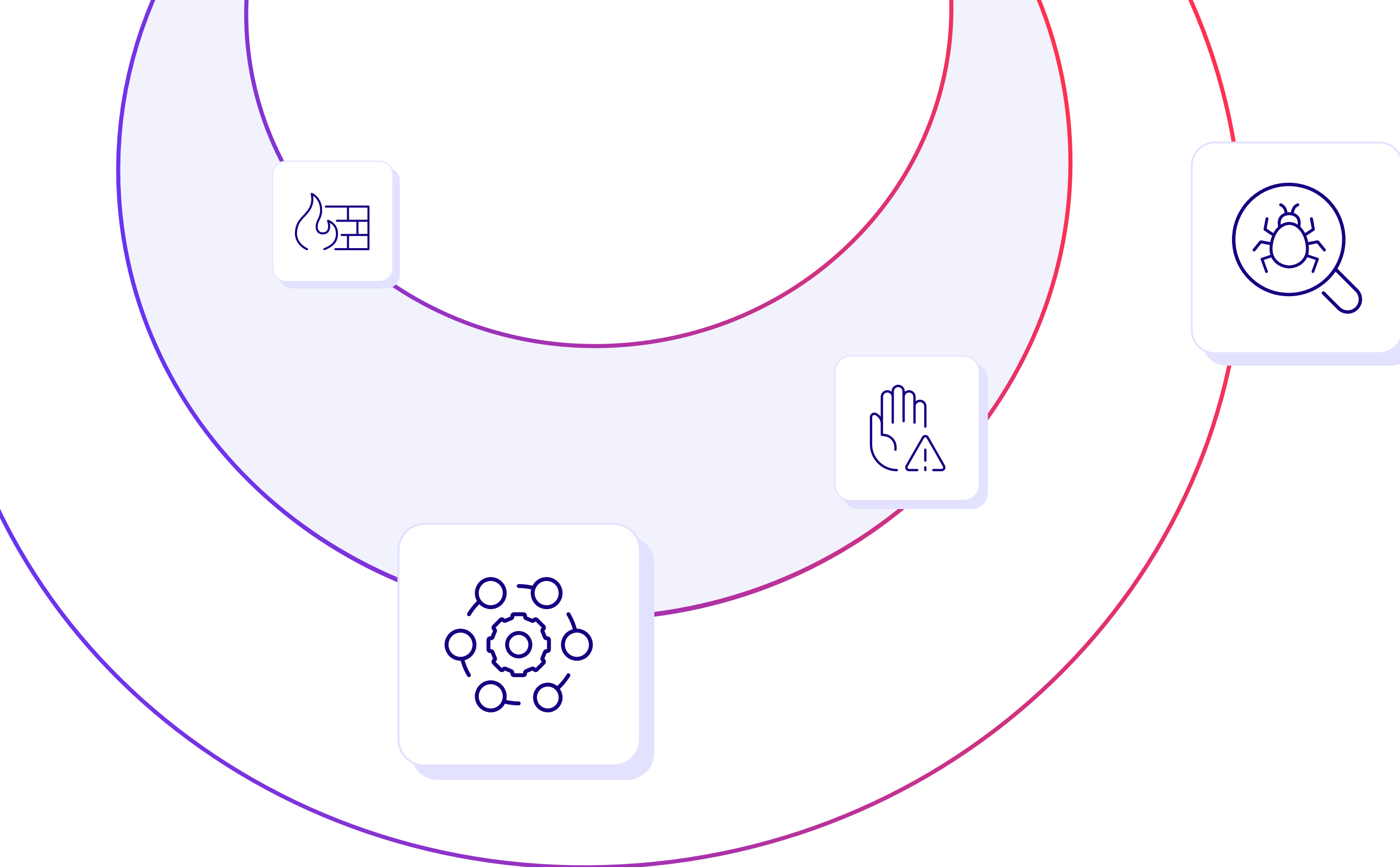
**The biggest issues with pen testing:**



## THE BOTTOM LINE:

The cyber threat landscape is evolving at lightning pace, and it's becoming commonplace for threat actors to use AI in their attack methods. Now, more than ever, it's critical that organizations move away from manual security testing and embrace the inclusion of AI and automation in their technologies and cyber best practices. One way to do this is to implement an AI-powered exposure validation solution, which will enable security teams to quickly, efficiently and intelligently focus on the most relevant threats, exposures and vulnerabilities across their IT environment.





**98%**   
plan to invest in exposure management

There are still significant questions around exposure management within SecOps – where it sits, how to effectively identify exposures and how to implement the right CTEM processes with limited resources. Yet, exposure management is a priority when it comes to security budget. And security leaders recognize that exposure management is an effective way to achieve actionable risk intelligence.

According to the research, almost all (98%) of SecOps teams say they plan to invest in exposure management in the future, with almost 9 in 10 (89%) stating that they plan to invest within the next 12 months.

## CHAPTER 4

### The State of Exposure Management



90%

of organizations apply validation to their exposure management process at least once a month

### The Evolution to Exposure Management

Exposure management is a proactive security measure that gives SecOps an attacker's view of security gaps and insight on how security controls and processes respond to threats and weaknesses. By implementing this proactive security measure into an ongoing process within a security program, organizations evolve into CTEM.

To build and execute a continuous effort to optimize both the short-term response and the long-term security posture, Gartner® created the CTEM framework that integrates scoping, discovery, prioritization, validation and mobilization.

### Resources are Lacking

Ultimately, there remains a lack of resources to properly adopt a robust exposure management program, which could result in major challenges when it comes to identifying and remediating vulnerabilities. This could also lead to a disconnect around who owns CTEM within an organization.

According to the research, exposure management is most likely to fall under the remit of an organization's SOC (security operations center) (34%), while 27% say it's spread across multiple different teams.



Further, while 32% say the role in charge of CTEM is responsible for prioritizing, 25% say validating, 24% say fixing and 19% say scoping.



### The Impact of Validating Exposure Management

Survey respondents recognize the importance of validating exposures in their environment as a means of assessing the impact of exploitation (45%), validating compensating controls (45%), testing the detection of exploitation attempts (43%) and validating that exposures are not a false positive (42%).

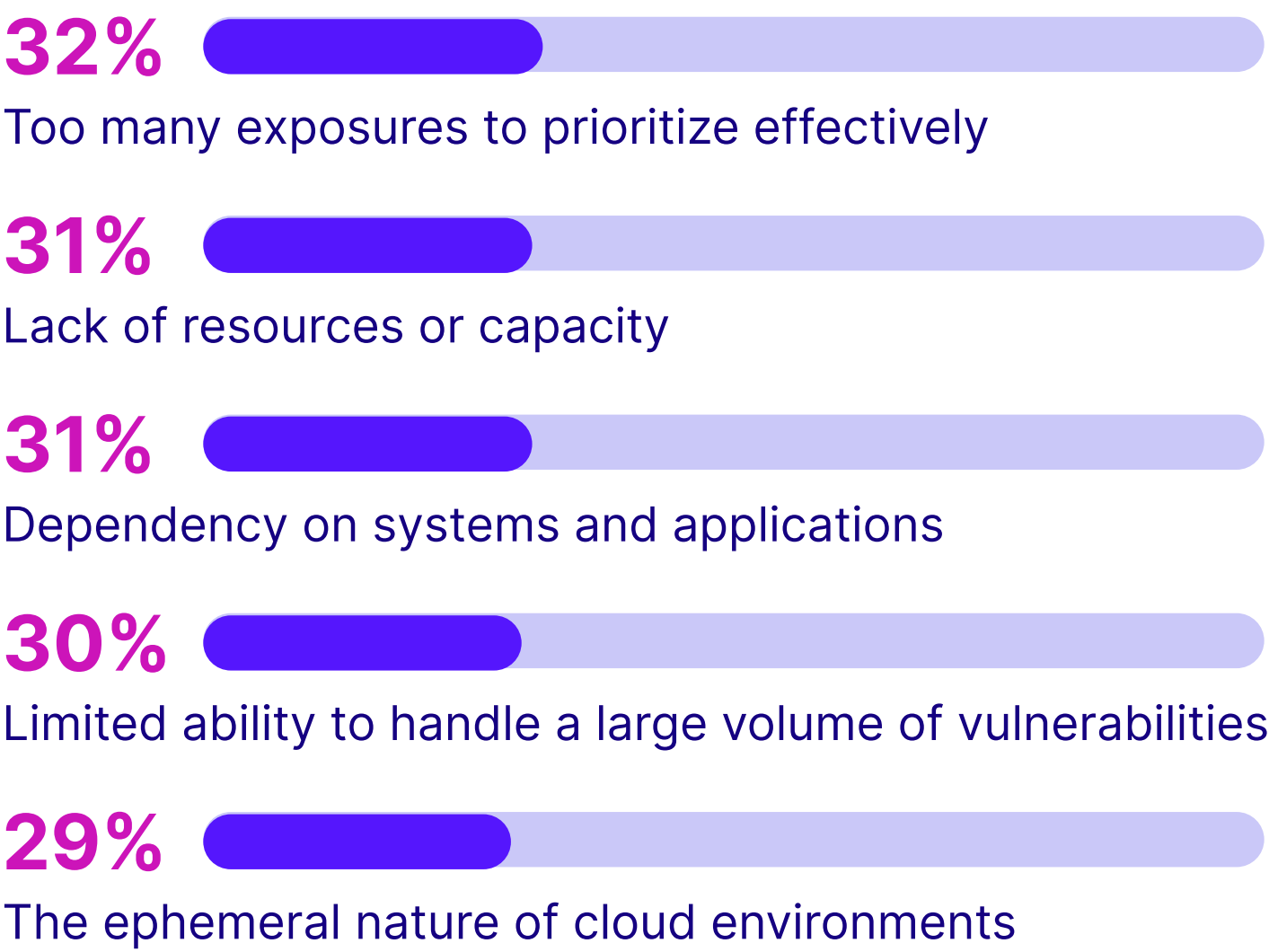
It’s not surprising that 90% of security leaders say they apply validation in their exposure management process at least once a month. The more organizations apply validation to their exposure management processes, the more likely they are to experience a decrease in security breaches.

According to the research, respondents who say their organization experienced 4-9 breaches in the past year say they apply validation in their exposure management process 6 times per month. However, those that do this 10 times per month experienced just 1-3 breaches.

### Preparing for Exposure Management

While the majority of organizations have either adopted exposure management processes or plan to do so in the future, the research shows that security teams still face significant challenges and a lack of preparedness. For example, when remediating identified exposures, SecOps report that they experience challenges with prioritizing effectively (32%).

Here are the biggest challenges facing SecOps when it comes to remediating identified exposures:



What's more, SecOps may be left with no choice but to ignore some vulnerabilities due to a lack of resources. Just over 3 in 10 (31%) state that a lack of resources or capacity is one of the biggest challenges they face when remediating identified exposures, while almost half (49%) cite this as a factor that influences their decision to deprioritize exposure remediation. An additional 47% say the effectiveness of compensating controls to prevent or detect an exploit is a key factor in their decision to deprioritize exposure remediation.

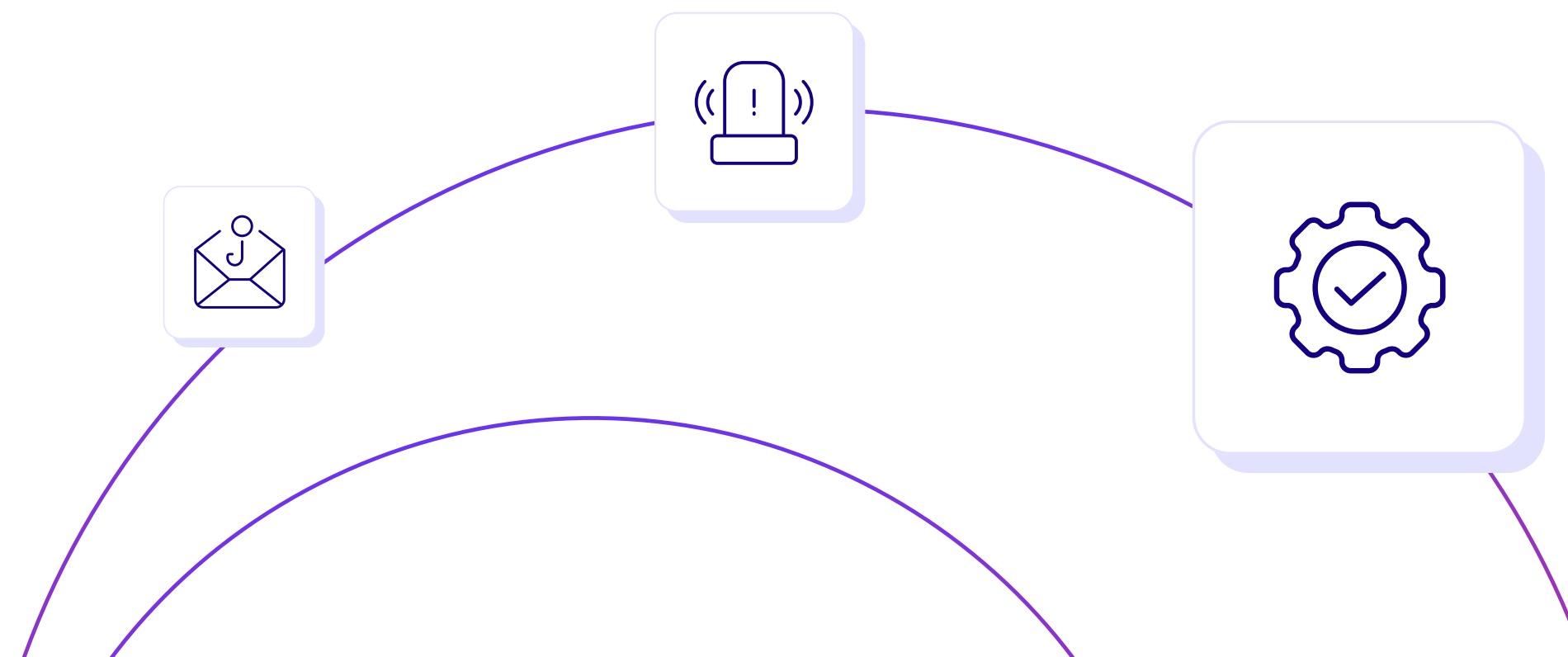
Despite these challenges, organizations are employing a number of strategies to better prepare for exposure management, and to help them determine which vulnerabilities are most critical to mitigate. These include asset classification/business impact (35%), validating attack paths to critical assets (34%) and ensuring the effectiveness of controls to prevent or detect an exploit (34%).

# 47%

deprioritize exposure remediation due to the effectiveness of compensating controls to prevent or detect an exploit

## How do you determine which vulnerabilities are most critical to mitigate?

- 35% Asset classification / business impact
- 34% Validated attacks paths to critical assets
- 34% Effectiveness of controls to prevent or detect an exploit
- 34% Threat intelligence
- 33% Risk assessment
- 23% CVSS score



## THE BOTTOM LINE:

Exposure management is set to play a key role in 2025. Not only are organizations seeing a reduction in breaches as the result of implementing a CTEM process, the vast majority are planning to invest further in the coming year. However, the success of exposure management hinges on the right approach and the right technology that proves the exploitability of the exposure within a specific environment. And validation is a critical component to a successful CTEM process.





### Schedule a Demo

Get a private demo to see the benefits for your organization

[Request a Demo](#)

### About Cymulate

Cymulate, the leader in security and exposure validation, provides the single source of truth for threat exposure and the actions required to close security gaps before attackers can exploit them. More than 1,000 customers worldwide rely on the Cymulate platform to baseline their security posture and strengthen cyber resilience with continuous discovery, validation, prioritization, and guided remediation of security weaknesses. Cymulate automates advanced offensive security testing to validate controls, threats, and attack paths. As an open platform, Cymulate integrates with existing security and IT infrastructure and drives the workflows of the exposure management process. For more information, visit [www.cymulate.com](https://www.cymulate.com).

### SURVEY DEMOGRAPHICS

Cymulate commissioned global market research consultancy, Censuswide, to survey 1,000 enterprise security leaders and practitioners (including CISOs, red teams, blue teams, IT security managers and vulnerability management) across the U.S., UK, Spain, Germany, France and Italy. Industry sectors included healthcare, manufacturing, education and financial services.

