HUNTRESS with UserEvidence

# Huntress 2025 Managed ITDR Report:

## Identity Is the New Security Perimeter

HUNTRESS

# Table of Contents

# Executive Summary

Cybersecurity is undergoing a fundamental shift, and identity is becoming the new security endpoint. Threat actors have become more sophisticated, quickly changing up tradecraft to compromise email and cloud infrastructure, making cloud-based productivity platforms like Microsoft 365 and Google Workspace more susceptible to identity attacks.

As the Huntress 2025 Cyber Threat Report shows, infostealers stand out as a major threat across government, healthcare, and technology—accounting for 24% of all observed security incidents in 2024. Instead of wasting time breaking into your networks the hard way, hackers are using infostealers to grab credentials, session cookies, and access tokens in seconds. Once stolen, attackers can bypass endpoint security and weak multi-factor authentication (MFA), infiltrating cloud apps and moving laterally without triggering alarms.

But this attack vector is just the beginning. VPN rule violations and business email compromise (BEC) tactics like inbox rule modification also stand out as some of the most prevalent identity-based threats. These identity threats allow attackers to access resources, steal login data, and siphon email information, potentially creating major data breaches and disrupting business critical communications.

While tactics like malicious application deployment and token theft happen less frequently, they're often hard to detect. This gives attackers the opportunity to cause significant damage—including system downtime, reputational damage, and direct costs—as they move laterally and maintain persistence.

We set out to understand how organizations have been impacted by identity-based attacks, how they handle these threats, and the identity protection changes they plan to make in the year ahead. We surveyed 600+ IT and security professionals, including executives, directors, managers, and administrators at organizations with between 250 and 5,000 endpoints. Our report reveals both encouraging progress and alarming risks.

Instead of exclusively focusing more sophisticated attacks on enterprise-level users, attackers now use these well-tested techniques on businesses of all sizes. For many organizations, the consequences can be devastating. Direct financial impacts often exceed $50,000, while damaged trust and reputations cause long-lasting consequences. Because of this, most organizations have already increased their identity protection investments, with mid-size organizations (500-5,000 endpoints) now prioritizing identity protection.

As identity threats keep evolving, most organizations strategically hire in-house experts. But due to technology complexity, integration challenges, and skill shortages make it hard for many businesses to implement what they really need to protect their identities.

This report shows that traditional identity protection, like MFA, isn't enough anymore. A comprehensive identity threat detection and response (ITDR) solution has emerged as an essential component of today's security architecture and has become necessary for defending against increasingly sophisticated attacks.

# Key Takeaways

**Slow detection and response times lead to major financial losses.**

Over two-thirds (68%) of organizations can't detect or respond to identity-related threats until attackers have established persistence. The business impact of identity-based attacks has become impossible to ignore, with 32% of organizations reporting financial consequences of $100,000 on up.

**Identity protection gains traction as identity attacks increase.**

Nearly half (45%) of organizations report having advanced identity protection, and 65% have adopted ITDR. In-house identity expertise already outweighs endpoint expertise, with 70% saying they have more expertise to address identity threats versus endpoint threats.

**Technical hurdles block advanced identity protection maturity.**

The data shows a clear shift in attack vectors, with 67% of respondents reporting an increase in identity-related incidents over the past three years. Yet technical issues like solution complexity (62%) and integration limitations (41%) are the biggest points of friction to achieving true identity protection maturity.

## Investments are going up, but ROI is hard to measure.

Identity-related incident costs have led to a new POV on resources, with 68% of businesses increasing their investments in identity protection. However, measuring the ROI of these investments is still somewhat or extremely difficult for 71% of organizations.

## Identity protection is positioned to be a priority in the future.

Looking ahead, 89% of organizations expect to prioritize identity protection in the coming year, and 74% plan to implement ITDR in the next 12 months. This change signals a focus on identity as the modern security perimeter.

Chapter 1

# The Identity Threat Landscape: Rising Attacks, Mounting Costs, & Lagging Responses

Identity protection is top of mind for modern businesses. As users access resources from cloud services more and more, identity-based attacks have also gone up, causing attackers to shift their focus accordingly. Identity-related incidents now represent a significant and growing percentage of security breaches.

While BEC leads this wave of threats, it's far from the only major concern. Between the growing range of attack vectors and lagging detection and response times, many organizations have had major financial impacts from identity attacks.

> *Over the past 12 months, we've seen a massive shift. Attackers aren't just dropping malware—they're going after identities first. Infostealers are flooding the underground, handing cybercriminals access to Microsoft 365 and other critical systems without triggering traditional defenses. Stolen session tokens, MFA bypasses, and SaaS abuse are all on the rise. The pattern is clear: identity is the new attack surface, and hackers are exploiting it at scale. If you're not actively detecting and responding to these threats, you're already compromised.*
>
> **Kyle Hanslovan**
> **Huntress CEO**

## Identity Attack Vectors Shift & Create Big Financial Impacts

As a longstanding threat, BEC has been actively tracked as a financial cyber threat for more than a decade. Between 2013 and 2023 it caused $55 billion in losses, according to the FBI's Internet Crime Complaint Center.

But it's still a major risk factor for organizations in 2025. In fact, BEC is the most common identity-related security incident, with more than half (51%) of respondents confirming that they've experienced it in the past 12 months (Figure 1).

However, BEC is the tip of the iceberg. Both credential theft/stuffing and account takeover (ATO) are common, with more than a third (39% and 34%, respectively) of respondents reporting that they've experienced these types of identity attacks in the past year.

Additionally, nearly half have encountered rogue/malicious applications (45%) and VPN abuse/misuse (43%). The Huntress 2025 Cyber Threat Report also highlights VPN rule violations as a major threat but qualifies malicious applications as a much less frequent concern. This difference could signal a rise in rogue/malicious application incidents.

## Identity-Related Security Incidents

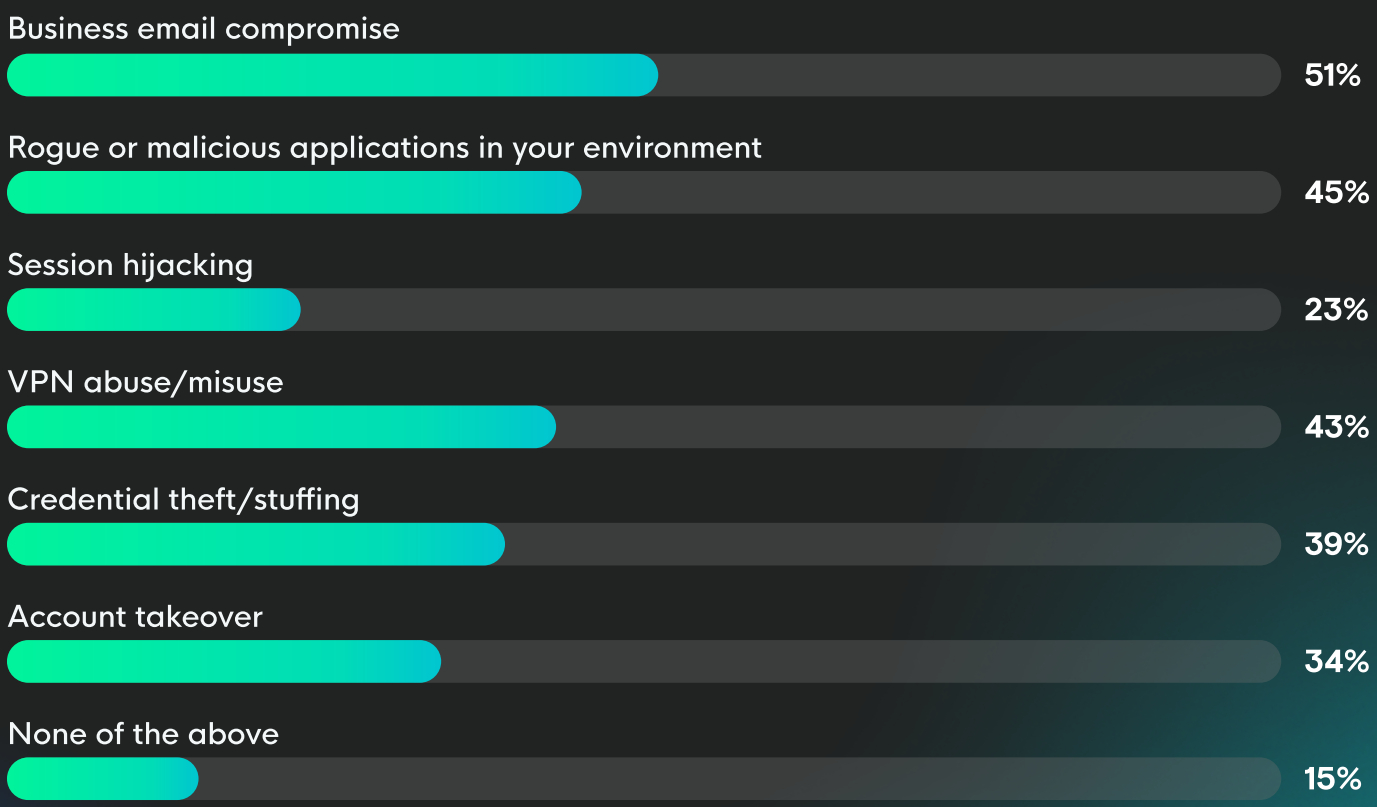


*Figure 1: In the past 12 months, has your organization experienced any of the following identity-related security incidents?*

> *Over the past 12 months, identity attacks have become more targeted, more automated, and more deceptive—and businesses that rely on outdated defenses are getting steamrolled. ATO attacks have evolved. Automated credential stuffing and brute-force tools are tearing through weak and reused passwords at scale. Attackers aren't just bypassing MFA—they're actively exploiting it. SIM swapping, MFA fatigue, and token theft are rendering SMS-based MFA ineffective, making phishing-resistant authentication more critical than ever.*
>
> **Prakash Ramamurthy**
> Huntress Chief Product Officer

Regardless of the tradecraft, identity-based threats have become a significant concern. More than a third (35%) of respondents report that identity-based threats account for over 40% of the incidents they've experienced in the past 12 months (Figure 2).

## Identity-Related Incidents as a Percentage of Overall Security Incidents

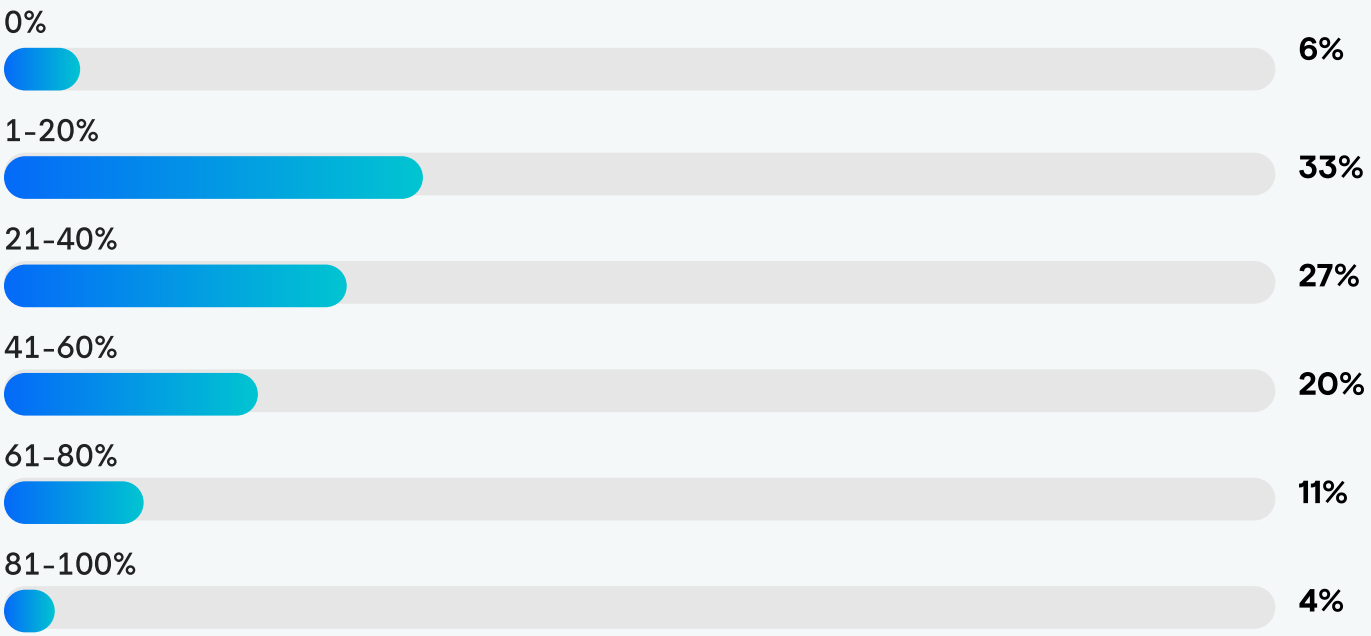


*Figure 2: What percentage of your overall security incidents in the past 12 months were identity-related?*

This data shows how important comprehensive ITDR is. While respondents may have focused on attacks on the traditional perimeter (e.g., endpoints) in the recent past, incidents related to the new perimeter (e.g., identity) present more pressing concerns.

Cloud-based productivity platforms are frequently the source of identity attacks. About half (49%) of organizations report that more than 40% of their identity-related incidents involved Microsoft 365 or Google Workspace (Figure 3).

## Identity-Related Incidents Involving Microsoft 365 or Google Workspace

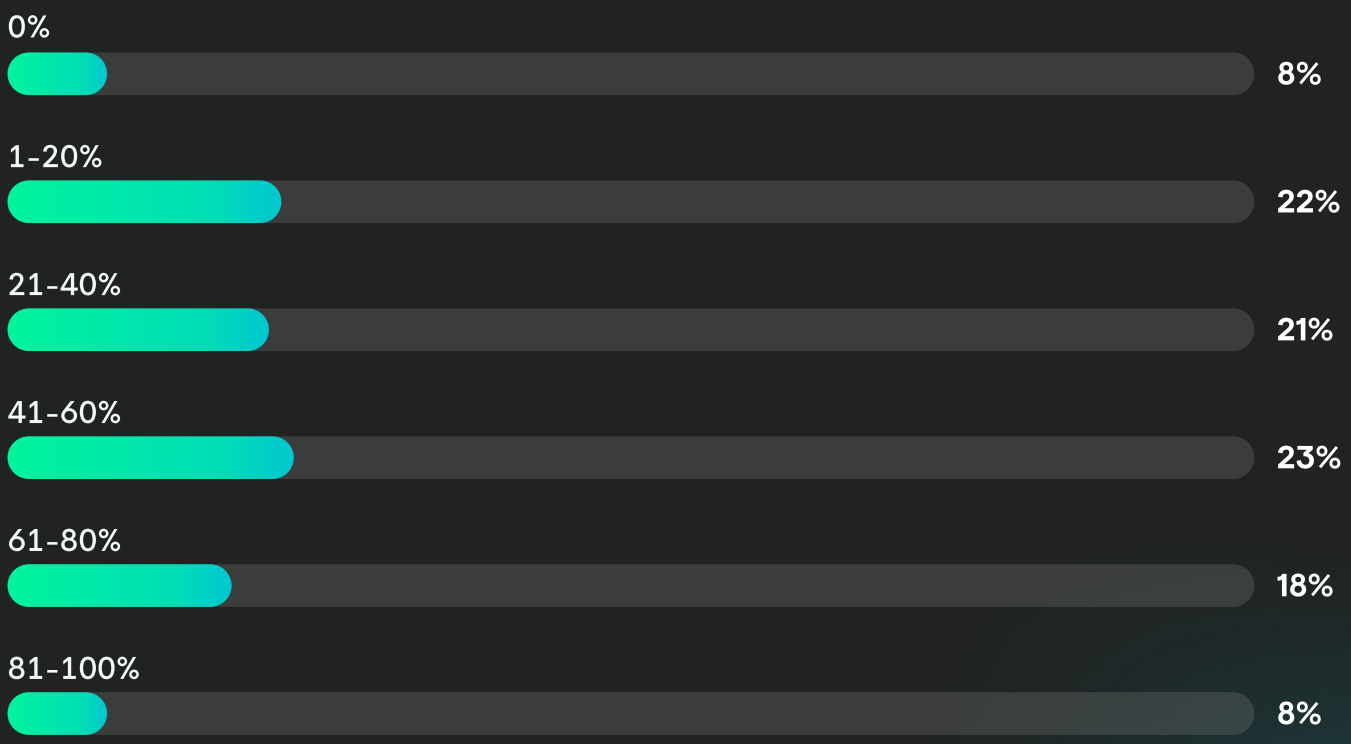


*Figure 3: What percentage of your identity-related incidents involved Microsoft 365 or Google Workspace?*

The prevalence of incidents involving Microsoft 365 and Google Workspace suggests that organizations may overlook the risk that business-critical applications present. They may also overestimate the security measures they've implemented for these platforms.

> *The threat from rogue Microsoft 365 cloud applications is huge. Many organizations don't even realize that any user can install any application into the Microsoft tenant by default. The best defense against this is to disable user-consent for applications without admin approval and regularly audit application installations and activity.*
>
> **Kyle Hanslovan**
> **Huntress CEO**

For most organizations (87%), identity-based incidents have had fallout like a major financial impact. Nearly a third of respondents estimate experiencing at least $100,000 in losses from identity attacks. Altogether, over 50% report encountering at least $50,000 in losses (Figure 4).

## Financial Impact From Identity-Related Incidents


*Figure 4: If you experienced any incidents, what was the estimated financial impact?*

The full impact of identity-related incidents extends far beyond financial losses. Respondents also report consequences ranging from unplanned downtime to reputation damage to lost customer trust.

# Threat Detection & Response Timelines Need Improvement

To avoid these outcomes and implement effective identity protection, organizations must be quick to respond. However, many organizations have delayed detection and response timelines that permit identity-based attacks to escalate.

About a third (32%) of organizations typically detect identity threats during the initial compromise stage (Figure 5). This early detection allows them to evaluate and respond to threats before attackers establish persistence, move laterally, or exfiltrate data.

However, two-thirds (68%) of organizations detect these threats later in the attack lifecycle. In fact, 20% can't detect threats until data exfiltration, and 5% can't detect attacks until after the incident has happened. These lengthy delays create golden opportunities for attackers to escalate access, steal sensitive data, and make ransom demands.

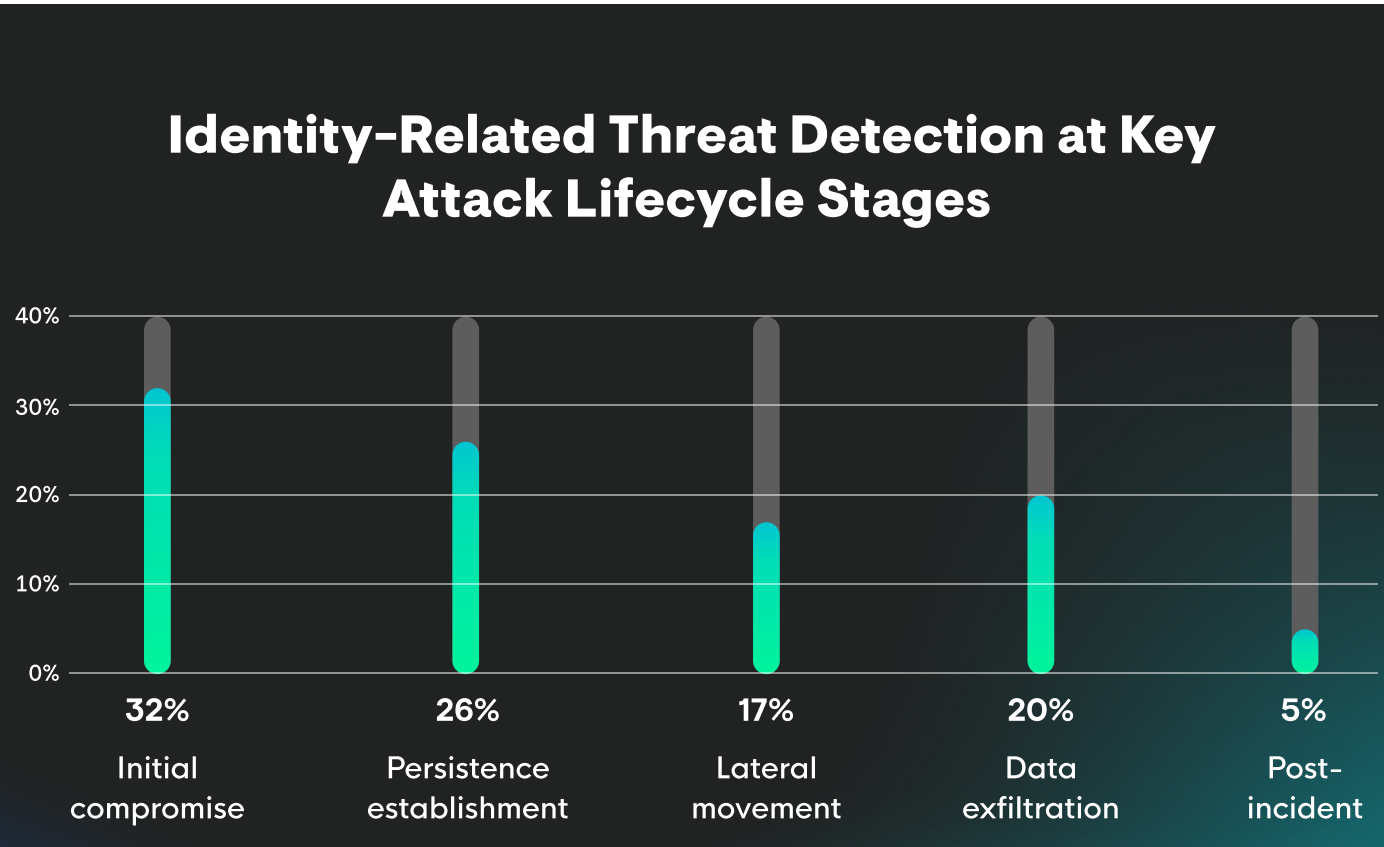


*Figure 5: At which stage of the attack lifecycle do you typically detect identity-related threats?*

> *Once attackers steal credentials, they don't waste time—they move laterally, escalate privileges, and set up persistence to maintain access. The key is catching these behaviors before they hit exfiltration. Organizations need to monitor for VPN and location anomalies, MFA enrollments on new devices, shadowy inbox and forwarding rule creation, privilege escalation attempts, and unusual access to sensitive data. If a standard user suddenly starts poking around admin settings or downloading mass amounts of files, that's your red flag. Identity threats don't start with ransomware—they start with quiet takeovers. Detect them early, and you stop the breach before it spirals.*
>
> **Kyle Hanslovan**
> **Huntress CEO**

To find and stop breaches early, organizations should ideally monitor and respond to identity-related incidents in real time, but most have much longer detection and response timelines.

Only a quarter (25%) of respondents report being able to detect an identity-based security incident within minutes. More than half (53%) can detect attacks within hours. Yet detection takes days for 16% of respondents and weeks for the remaining 5% (Figure 6).

## Average Time to Detect Identity-Related Security Incidents

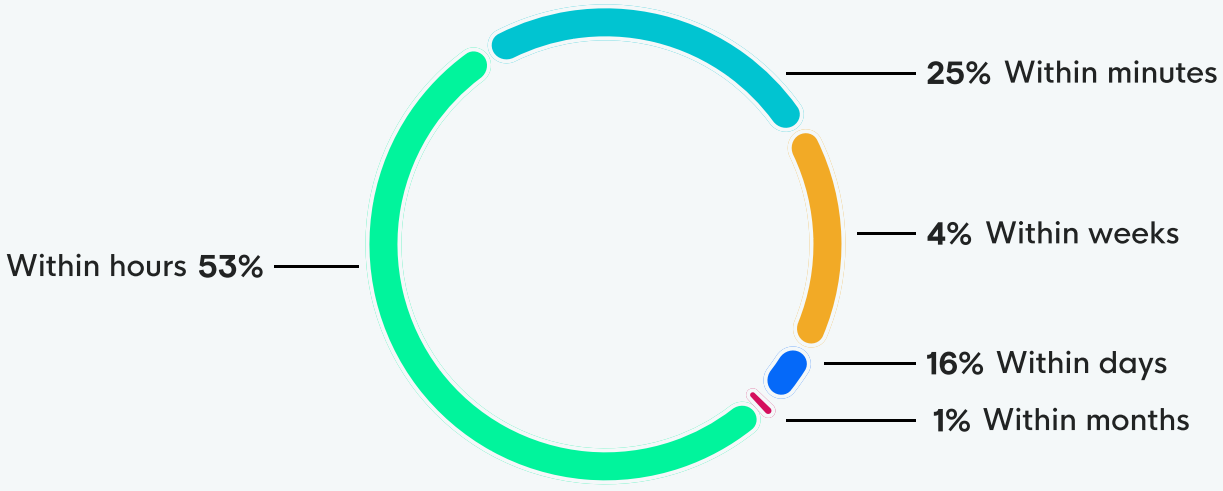


*Figure 6: What is your organization's average time to detect an identity-related security incident?*

Most organizations report similar detection and remediation timelines. A quarter (25%) typically respond to identity-related security incidents within minutes, and 50% remediate them within hours. 21% take days to respond, and 4% take weeks to remediate (Figure 7).

## Average Time to Respond to and Remediate Identity-Related Security Incidents

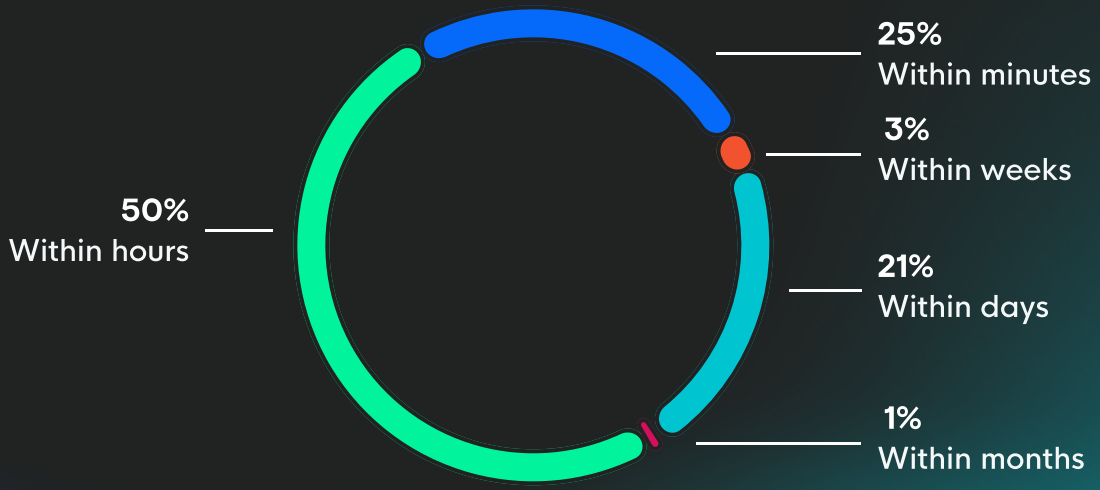


*Figure 7: What is your organization's average time to respond to and remediate an identity-related security incident?*

Responding to attacks within hours may seem reasonable, but in this amount of time, attackers can escalate permissions, move laterally, exfiltrate data, and deploy ransomware.

As the Huntress 2025 Cyber Threat Report shows, the average time-to-ransom (TTR) is almost 17 hours. Before ransom, attackers complete an average of 18 actions. While actual TTR depends on the ransomware group and factors like initial access point, network pathing, and the need for data exfiltration, it's clear that extensive damage can happen in a matter of hours.

As a result, identity monitoring and response is now more important than ever. With a real-time ITDR solution, organizations can detect and respond to identity attacks within minutes, efficiently addressing critical security threats and avoiding significant financial impacts.

Chapter 2

# The Identity Protection Reality Gap: Confidence vs. Capability

For many organizations, their confidence in identity protection measures is more than their actual maturity, revealing a concerning disconnect. Many businesses continue to rely on MFA and other less advanced defenses, putting them at risk of rising identity threats.

At the same time, most organizations report a meaningful shift in their security focus. Most prioritize in-house identity expertise over endpoint knowledge. However, many still lack sufficient in-house expertise, leaving them open to identity-based attacks.

> *Hackers have it easy right now—businesses need to start making them work for access. The first and most important step mid-market organizations can take is to enforce phishing-resistant MFA everywhere, especially for privileged accounts. Weak authentication is the backbone of identity attacks. Infostealers and phishing kits are handing attackers valid credentials and session tokens on a silver platter. If you're still relying on SMS-based MFA or not enforcing MFA at all, you're making their job way too easy.*
>
> **Prakash Ramamurthy**
> Huntress Chief Product Officer

## Identity Protection Confidence Levels Exceed Actual Measures

Less than half (45%) of organizations say their identity protection maturity level is "advanced" and report having a comprehensive ITDR strategy in place. More than half of organizations (55%) have comparatively immature identity protection (Figure 8).

Breaking down this number further, 41% rate their identity protection maturity level as "developing," meaning they've implemented only some monitoring solutions. 12% consider their maturity "basic," meaning they mainly rely on MFA and password policies instead of more robust solutions.

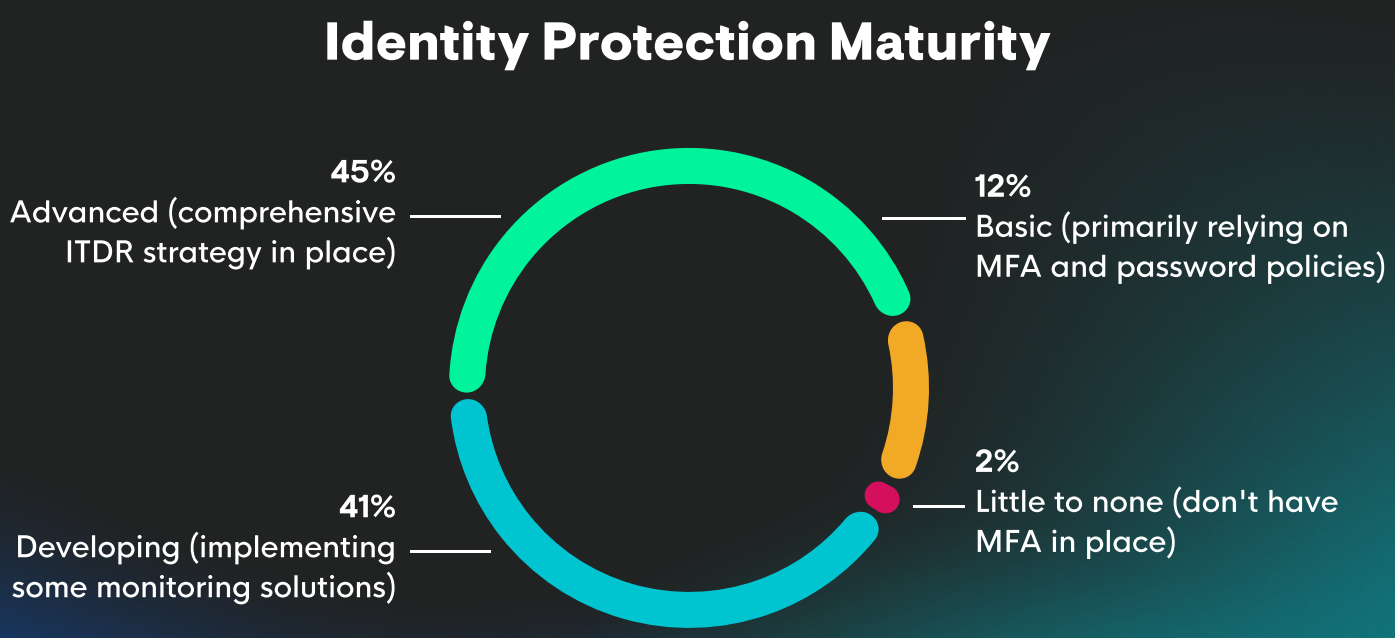


*Figure 8: How would you rate your organization's current identity protection maturity?*

These responses indicate that most organizations have plenty of room for improvement. As the Huntress 2025 Cyber Threat Report reveals, attackers are often able to get credentials without MFA, meaning organizations must think beyond this defense alone.

Long a widely accepted security practice, MFA has become essential across organizations and applications in recent years. More than three-quarters (78%) of respondents report using MFA in their environments (Figure 9).

> *In the past year, we've seen an incredible rise in the number of successful token theft attacks. These attacks can bypass MFA completely, which many companies still struggle with implementing fully and consistently across their organizations.*
>
> **Rich Mozeleski**
> Huntress Staff Product Manager

Because sophisticated identity attacks can now bypass MFA, organizations need multi-layered defenses to be safe. Two-thirds (66%) of respondents report using ITDR solutions, while 62% have set up email filtering protection. Half (50%) use continuous access monitoring, and a similar percentage (47%) report implementing privileged access management.

## Current Identity Protection Measures

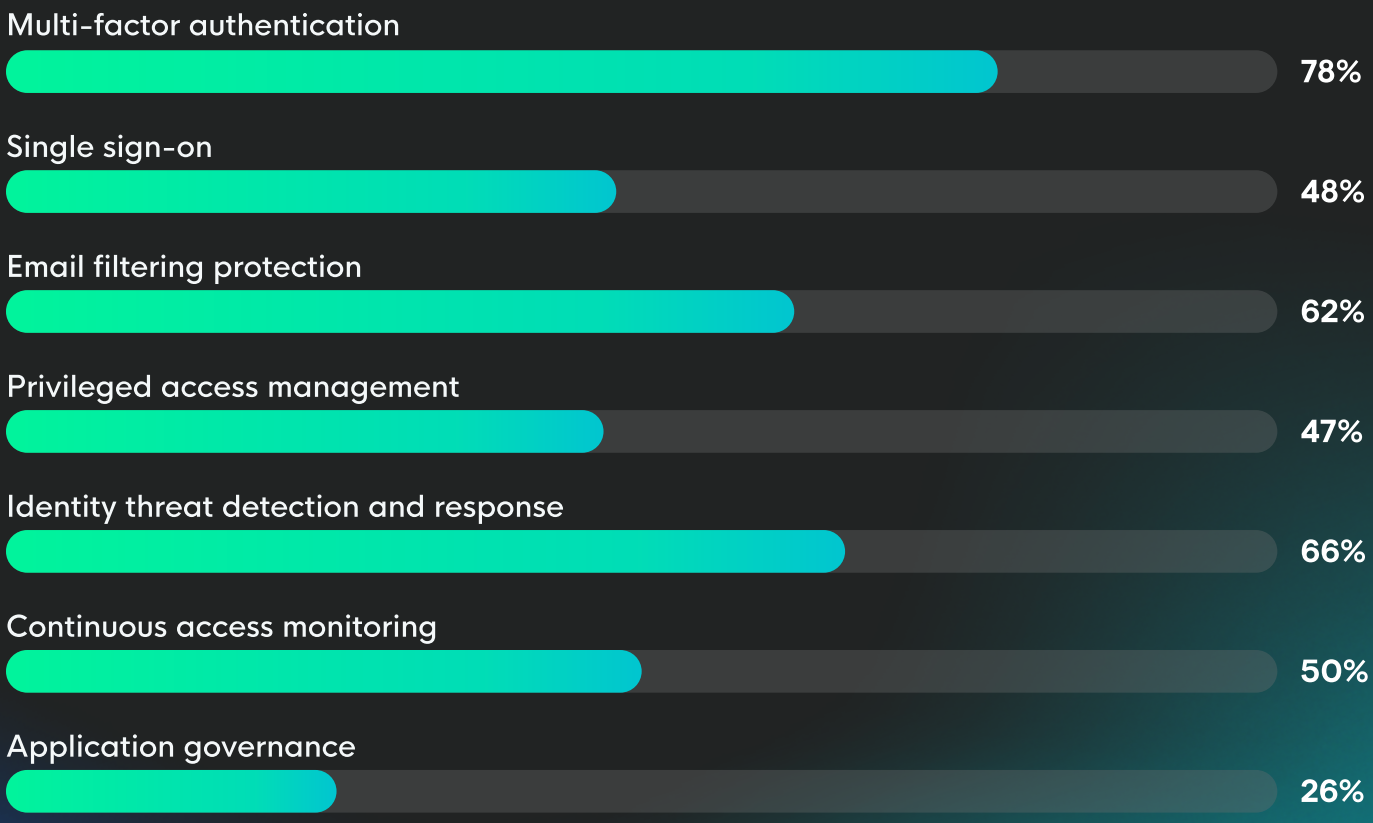


*Figure 9: Which of the following identity protection measures do you currently have in place?*

Unlike many static identity protection measures, ITDR provides more comprehensive protection. Its active monitoring capabilities detect and respond to identity attacks like BEC, credential theft, session hijacking, and ATO in real time. As a result, it's become an essential solution to address modern identity threats.

While most organizations prioritize MFA in lieu of a comprehensive ITDR strategy, the majority have high confidence in their ability to manage identity-based threats. Because of this, confidence levels appear to exceed actual identity protection maturity.

Nearly two-thirds (65%) of respondents report being very confident in their ability to uncover rogue or malicious applications within their environment. Yet the remaining respondents are comparatively less secure in this capability. Just over a third (34%) report being somewhat confident, while less than 1% are not at all confident (Figure 10).

## Confidence Level in Uncovering Rogue or Malicious Applications

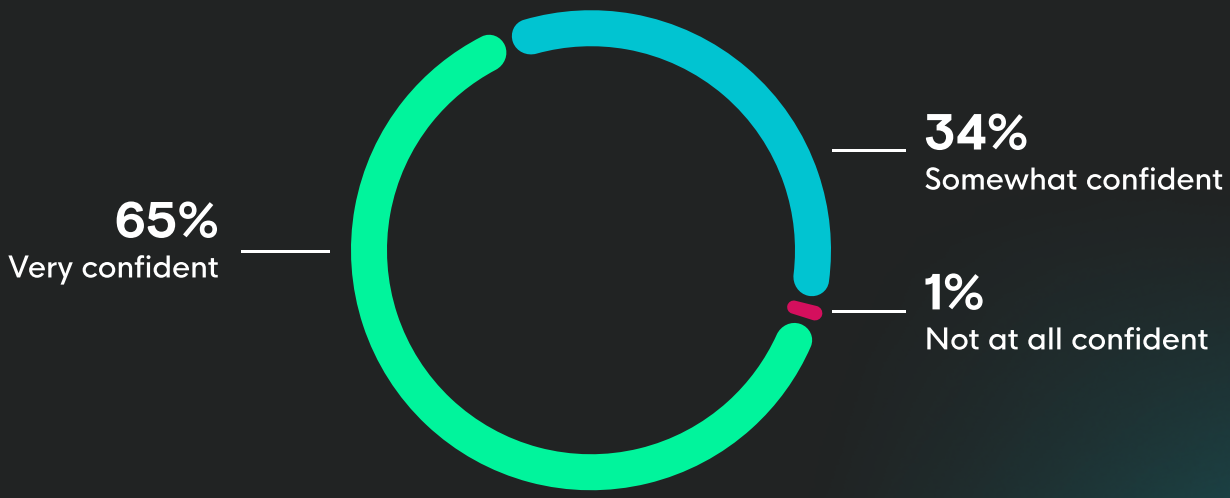


*Figure 10: What is your level of confidence in uncovering rogue or malicious applications within your environment?*

This confidence gap is concerning considering that more than half of organizations saw financial losses of $50,000 or more due to identity-based attacks. These responses suggest that organizations should consider revisiting their identity protection measures, as many may benefit from stronger technology, enhanced security awareness training, or a fully managed solution with comprehensive protection.

# Identity Expertise Now Outpaces Endpoint Knowledge

Despite varied maturity levels, most organizations have internal teams that handle identity protection. Nearly two-thirds (65%) of organizations manage identity-based threats in-house, while the remaining third (33%) rely on a third-party vendor (Figure 11).

## Identity-Related Threat Management Approach

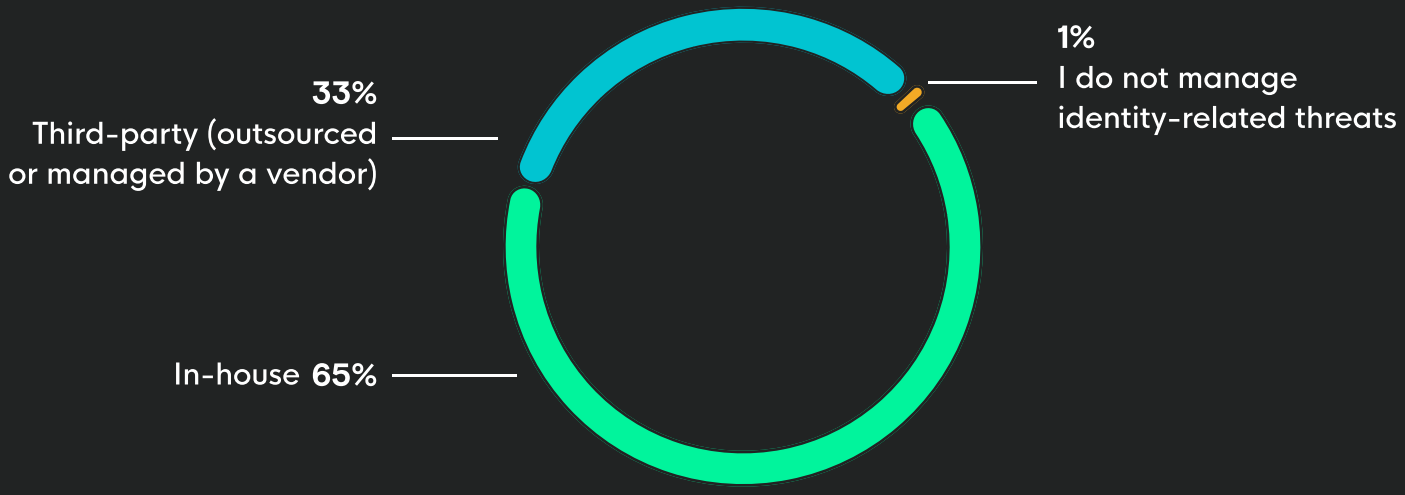


*Figure 11: How are you managing identity-related threats?*

More than half of organizations (54%) report having enough in-house expertise to find and respond to identity-related threats. Yet 44% have only some expertise, indicating that nearly half would benefit from more advanced training or third-party management (Figure 12).

## In-House Expertise for Identity-Related Threats


*Figure 12: How much in-house expertise do you have to address identity-related threats?*

Organizations may already be starting to invest in identity threat expertise. Most (70%) of respondents report having significantly or somewhat more in-house expertise to address identity threats than endpoint threats (Figure 13).

## In-House Expertise for Identity vs. Endpoint Threats

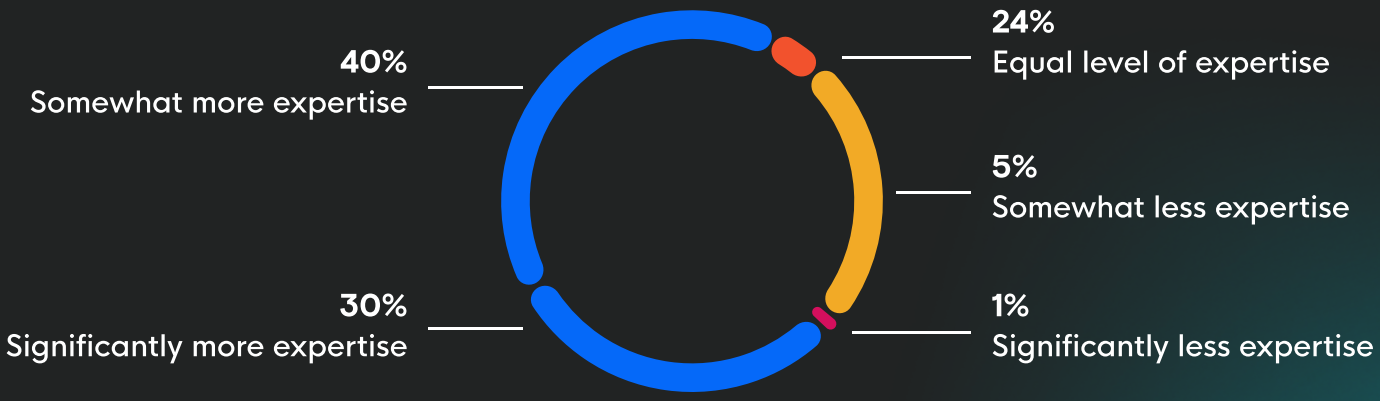


*Figure 13: How much in-house expertise do you have to address identity threats compared to endpoint threats?*

This breakdown suggests that most organizations are investing more in identity-related expertise over endpoint-related knowledge. Given the rise in identity-related attacks over the last year, this expertise distribution may bode well for organizations as they fight off evolving identity threats like BEC, VPN abuse/misuse, and credential theft.

Chapter 3

# The Identity Defense Crossroads: Balancing Concerns & Implementation Challenges

Over the past three years, identity-based attacks have surged. This trend has caught the attention of IT and security professionals and made concern levels for identity threats to rise—especially in comparison to worrying about endpoint threats.

However, implementing a successful identity protection solution is still a challenge for many organizations. Technical issues present a major barrier, creating a dangerous situation that leaves many businesses vulnerable despite them knowing the threat is real.

> *Now, identity itself is the target. As organizations centralize access through cloud identity providers, attackers are pivoting to exploit misconfigurations, API vulnerabilities, and weak access controls in these systems. Supply chain attacks are increasingly hitting identity management vendors, giving attackers a way to compromise multiple organizations at once. Businesses need to move beyond static defenses and start actively detecting unauthorized access, monitoring risky authentications, and locking down identity providers before attackers take advantage of these blind spots.*
>
> **Prakash Ramamurthy**
> Huntress Chief Product Officer

# Concerns for Identity Threats Now Outrank Those for Endpoint Threats

For most organizations, identity threats are only going up. More than two-thirds (67%) report that the frequency of identity-related attacks has increased compared to three years ago. Over a quarter (26%) indicate that identity-related attacks have significantly increased, while 42% report that they've somewhat increased (Figure 14).

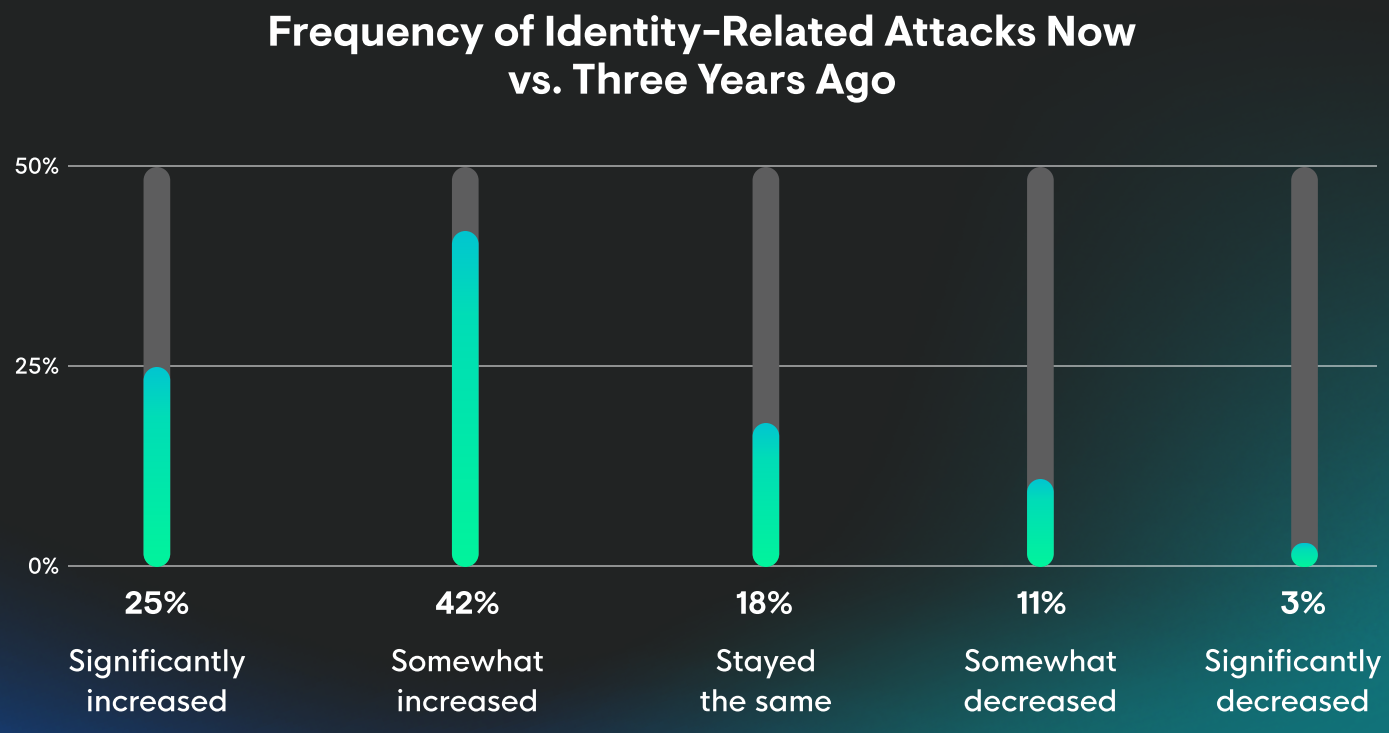


*Figure 14: Compared to three years ago, how has the frequency of identity-related attacks changed?*

Few respondents (14%) report that identity attacks have somewhat or significantly decreased over the past three years. These responses align with findings from the Huntress 2025 Cyber Threat Report, which highlights the increasing prevalence in attacks on Microsoft 365 environments.

Given the rise in identity-related attacks, most organizations perceive this type of threat to be potentially significant. Nearly two-thirds (62%) of respondents are very concerned about identity threats, while a third (34%) are somewhat concerned (Figure 15).

## Concern Level for Identity Threats


*Figure 15: How concerned are you about identity threats?*

Based on their experiences over the past one to three years, most organizations have paid closer attention to identity-related attacks. More than half (60%) are now more concerned about identity threats than endpoint threats. Less than a quarter (22%) report the same amount of concern for the two types of threats (Figure 16).

## Concern Level for Identity vs. Endpoint Threats

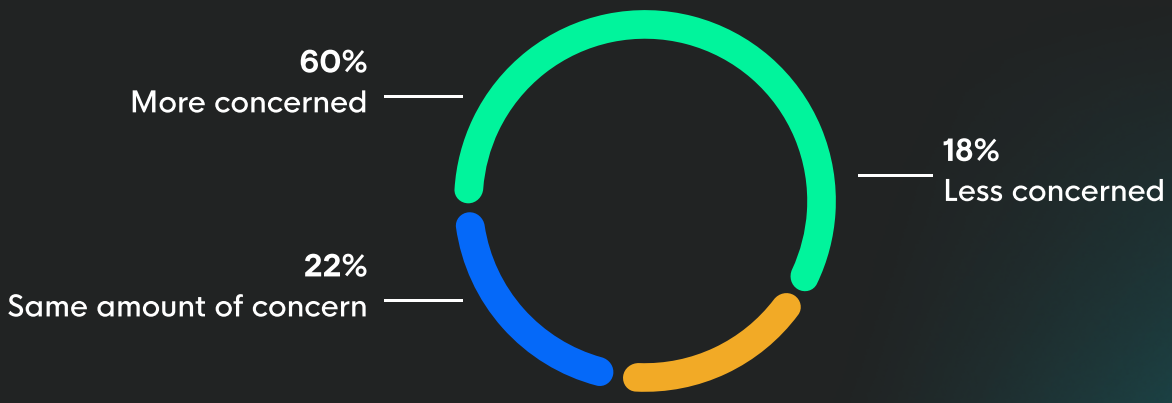


*Figure 16: How concerned are you about identity threats compared to endpoint threats?*

However, it's important to avoid over-prioritizing one aspect at the cost of ignoring the other. Organizations should aim to balance identity and endpoint protection as both types of threats are real, common, and potentially expensive.

> *Organizations frequently underestimate endpoint-originating identity compromise, particularly from credential-stealing malware. These stealthy threats quietly extract stored credentials, browser tokens, and session cookies directly from user devices—giving attackers direct access without raising alarms. Securing endpoints, detecting abnormal credential use, and closely monitoring identity behaviors are essential to preventing these attacks from silently escalating.*
>
> **Matt Kiely**
> Huntress Principal Product Researcher

# Threat Detection & Response Timelines Need Improvement

Organizations' identity-related concerns largely mirror the threats they've experienced over the past 12 months. BEC is the top identity-related concern, with nearly two-thirds (63%) of respondents citing it as a primary issue (Figure 17). This data suggests that BEC attacks show no signs of slowing.

However, BEC is far from the only major identity threat. Almost half (49% and 46% of respondents, respectively) consider ATO and rogue applications in the environment to be primary issues. In addition, 41% report session hijacking and VPN abuse/misuse as top concerns.

Although most organizations report having enough in-house expertise and many report advanced identity protection maturity, almost all organizations have challenges when implementing solutions.

Nearly two-thirds (62%) of organizations have issues with technology complexity, suggesting a need for more user-friendly tools, better product training, or a switch to a managed solution. Many (41%) also report issues with integrating solutions with existing systems, which can open the door to identity-related attacks (Figure 18).

# Top Identity-Related Concerns

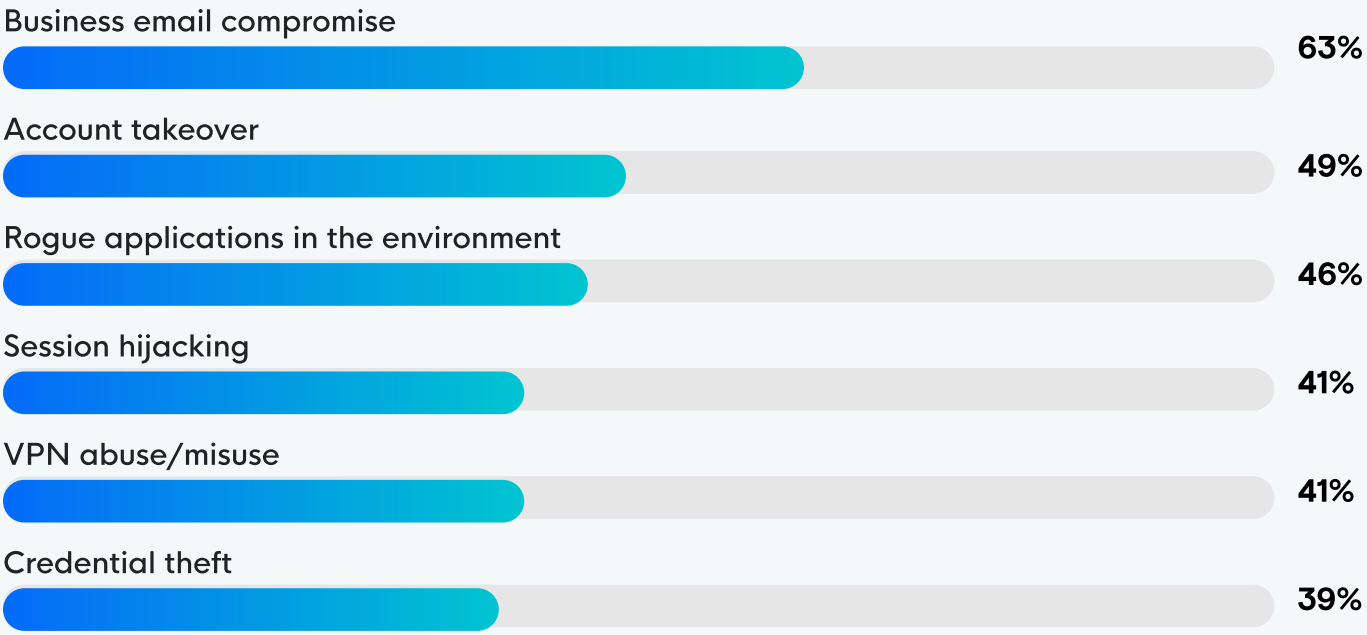


*Figure 17: What are your top identity-related concerns?*

The variety of responses reflect the wide range of concerns organizations need to pay attention to. Identity threats pull organizations in multiple directions, making it more important than ever to invest in solutions that can monitor and respond to a complete list of identity-related attacks.

> *The last 12 months have shown that threat actors still favor the tried and true identity attack methods like credential stuffing, token theft, and transparent proxy phishing. But the increase in the proliferation of credential stealer malware and its availability in the criminal underground markets means that credentials are now easier to procure than ever. Couple this with the fact that credential stealer malware can also compromise browser-based authentication material like session cookies and tokens, which presents convenient MFA bypass opportunities, and you have a recipe for opportunistic attacks.*
>
> **Matt Kiely**
> Huntress Principal Product Researcher

# Biggest Identity Protection Challenges

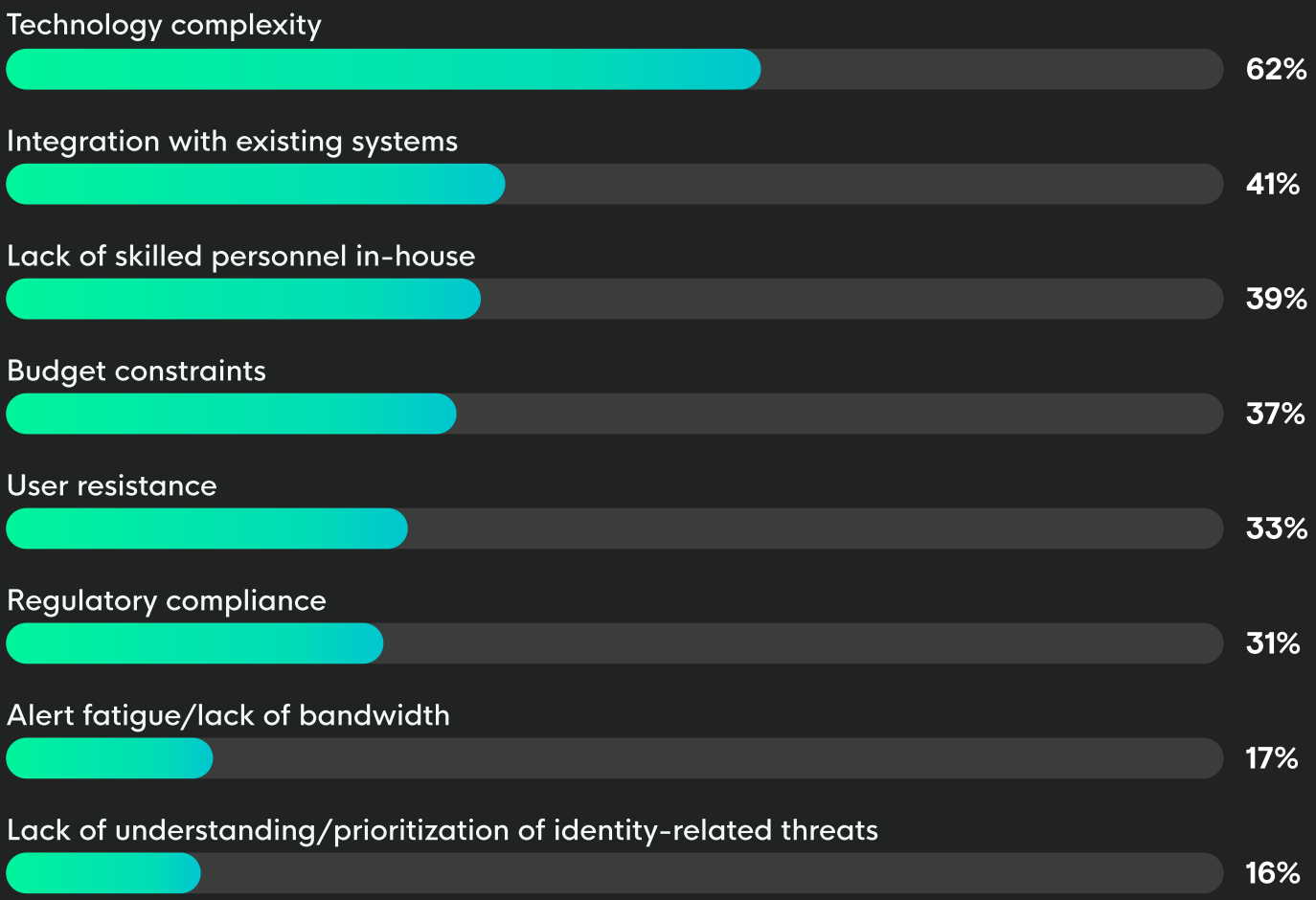


*Figure 18: What are your biggest identity protection challenges?*

More than a third (39%) of respondents report a lack of skilled personnel in-house, which may align with those who say they don't have enough in-house expertise. Between staffing problems and tech issues, it's clear that many organizations would benefit from revisiting their identity protection maturity, goals, and solutions.

> *Mid-market organizations need an ITDR solution that actually catches threats in progress—not just one that checks a compliance box. The top capabilities to look for? Real-time threat detection, proactive 24/7 identity monitoring, and fast, expert response to compromised accounts. You need visibility into suspicious logins, shadow workflows, rogue applications, and session hijacking because these are the constantly evolving attack vectors hackers are using. Just having alerts isn't enough.*
>
> **Kyle Hanslovan**
> Huntress CEO

Chapter 4

# The Identity Protection Investment Paradox: Budget Allocation & ROI Challenges

Organizations are allocating more resources to identity protection than ever before, with most reporting budget increases over the previous year. However, identity protection still lags in terms of budget allocation, often making up less than half of total cybersecurity spending.

Measuring return on investment (ROI) is still difficult for most organizations. This makes it challenging to assess the value of current identity protection programs, justify current expenditures, or prioritize additional investments. Security leaders need more sophisticated approaches to investments and performance measurement to make sure they have identity protection in place and are aligned with business objectives.

> *Organizations need an ITDR solution that doesn't just detect identity threats but actively stops them in real time. The top capabilities to look for include continuous identity monitoring, integration with existing systems, SIEM and security tool integration, behavioral anomaly detection, and automated response. Most importantly, your solution must be built for an identity-first world. Attackers are moving beyond the endpoint. If your defenses aren't watching the identity attack surface, you're already compromised.*
>
> **Kyle Hanslovan**
> Huntress CEO

# Identity Budgets Don't Yet Match the Growing Threat Landscape

Most organizations (90%) have more money for identity protection compared to the previous year. Over two-thirds (68%) have significantly or moderately increased budgets, while just under a quarter (22%) report a slight increase. Few organizations (9%) have maintained the same identity protection budget as last year (Figure 19).

## Identity Protection Budget Changes Over the Past 12 Months

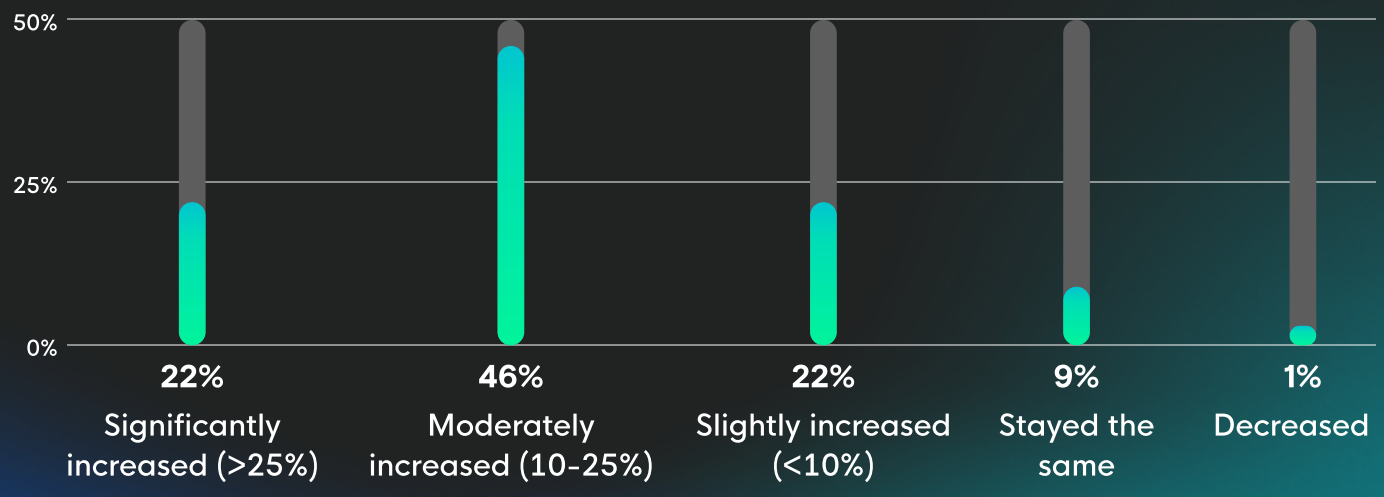


*Figure 19: How has your budget for identity protection changed compared to last year?*

This data aligns with identity-related incidents going up and the higher level of identity threat concern that most organizations report. But these budget increases may not be enough to address current or projected levels of identity-related attacks.

Almost all organizations (91%) allocate up to 50% of their overall security budget to identity protection, with the largest group (44%) dedicating 11-25% to this area. Few (8%) dedicate more than 50% of their security budget to identity protection (Figure 20).

## Identity Protection as a Percentage of Overall Security Budget


*Figure 20: What percentage of your overall security budget is allocated to identity protection?*

This breakdown aligns with this report's finding that more than half of organizations saying their identity protection maturity is "developing" or "basic" (Figure 8). Yet it contrasts with the rising frequency of identity threats.

Given the increase in identity-related attacks over the past 12 months, organizations that underfund identity protection do so at their own risk. Security budget allocation will be a key factor for organizations to reconsider in the near future as they work through the technical and integration issues that exist in their current identity protection solutions.

# Most Organizations Struggle to Measure Identity Protection ROI

To estimate how successful identity protection programs are, organizations typically focus on speed and incident reduction. Two-thirds (66%) prioritize time to detect/respond, and 62% measure reduction in incidents (Figure 21).

This focus on speed contrasts with respondents' reported time to detect and respond to incidents. About three-quarters of organizations take hours, days, or even weeks to spot and respond to identity threats (Figure 6). Because this delayed timeline puts them behind the average TTR, organizations may benefit from prioritizing more fast-acting solutions.

## Identity Protection Program Measurement

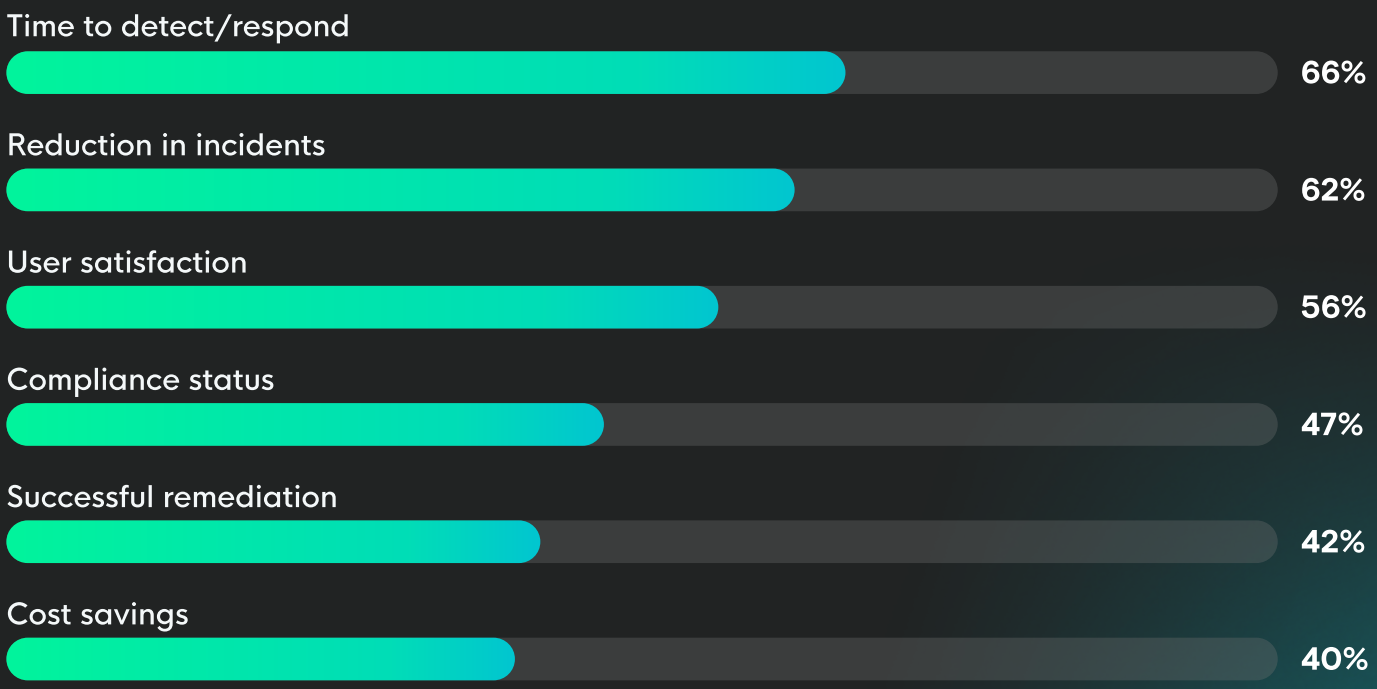


*Figure 21: How do you measure the success of your identity protection program?*

In comparison, respondents are less concerned with compliance status (47%), successful remediation (42%), and cost savings (40%). This data suggests that organizations are willing to spend on faster solutions and a lower incident rate, which tracks with budget-related identity protection trends.

But for most organizations, ROI isn't exactly easy to gauge. In fact, more than two-thirds (71%) report finding ROI somewhat or extremely difficult to measure. Only 28% find identity protection ROI not at all difficult to measure (Figure 22).

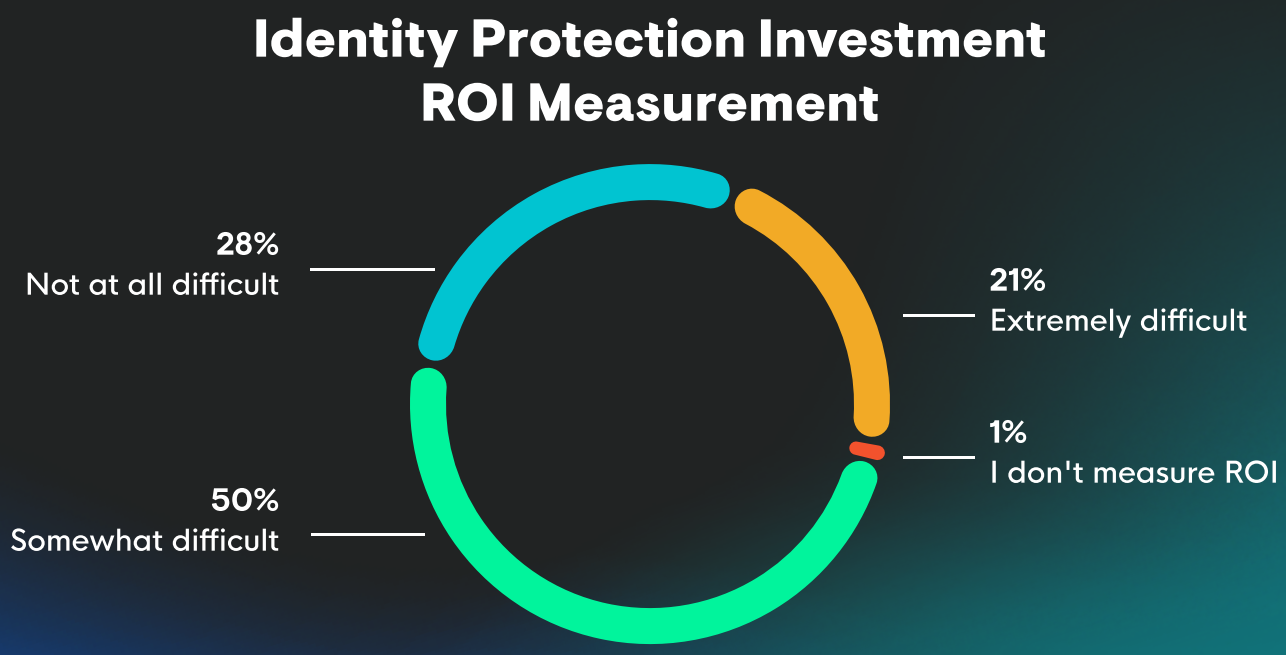


*Figure 22: How difficult is it to calculate the ROI on your identity protection investments?*

The struggle many organizations have with accurately measuring ROI may be rooted in the technical complexity and integration challenges they report. If they can't reliably access analytics or integrate identity protection solutions into their existing tech stack, organizations may not be able to track ROI—which compromises their ability to plan future ITDR investments.

> *Our biggest challenge remains placing a valuation on the impact to clients for an identified incident. It's hard to convince a client of ROI on something that has not happened to them, or that they do not think can happen to them. When the solution is deployed, we show our clients the instances of exposed credentials, risky admin behavior, and lateral movement attempts. Additionally, as the use of the tool expands, we can leverage this data to demonstrate the value of the tool to prospective clients as well.*
>
> **Ryan Rowbottom**
> Director of IT Services and Incident Response, PCS

Chapter 5

# The Identity-Centric Future of Security

The data shows a clear shift: identity protection is now a critical concern that IT and security professionals expect to continue to prioritize in the near future. Most organizations expect known threats like BEC and credential theft to escalate, but they may be overlooking growing concerns like token theft and VPN abuse.

To address these threats, most organizations anticipate hiring in-house expertise and investing in training over the coming year. Most also intend to implement or expand ITDR, demonstrating the importance of an identity protection solution that goes beyond prevention or alerts.

> *Mid-market companies need more than alerts—they need real-time identity threat detection, rapid automated response, comprehensive visibility of human and machine identities, and intuitive integration with existing tools. Look for ITDR solutions that detect early, respond automatically, and scale easily. Without these, identity protection becomes ineffective complexity.*
>
> **Matt Kiely**
> Huntress Principal Product Researcher

## Organizations Expect Significant Escalation in Identity Threats

In the past 12 months, identity-related attacks have become the largest portion of security incidents for many organizations (Figure 2). This trend shows no signs of slowing and instead appears positioned to rise over the next year.

Most organizations (89%) expect identity protection to be much more important to their overall security strategy over the next 12 months. Only 11% expect it to be about the same, and none believe identity protection will become less important (Figure 23).

## Identity Protection Importance Comparing Next Year vs. Last Year

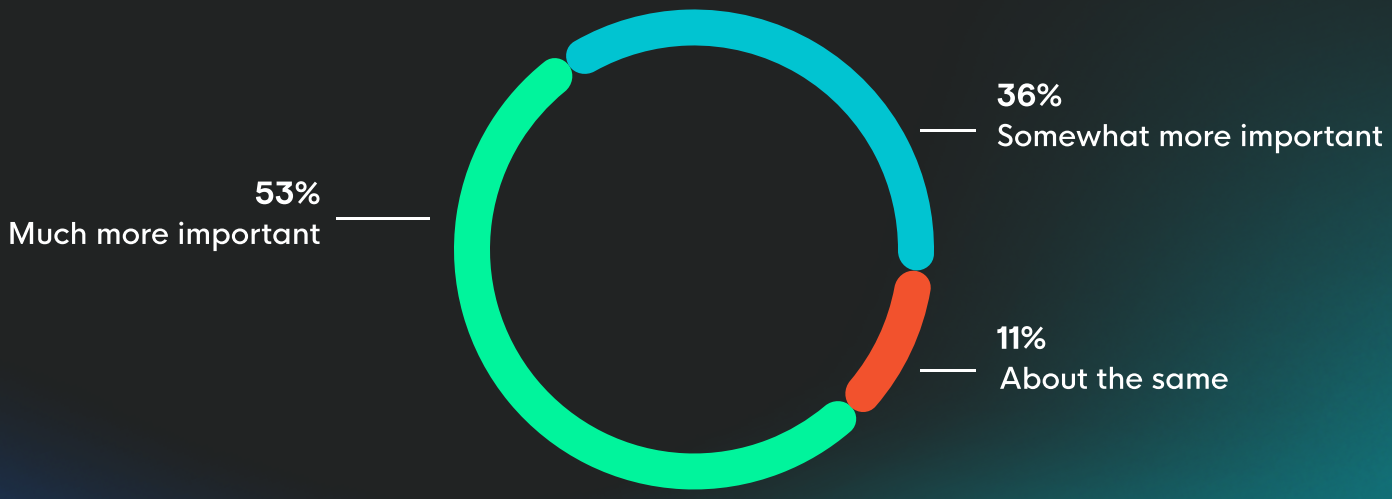


*Figure 23: How important do you expect identity protection to be to your overall security strategy in the next 12 months compared to the past 12 months?*

As identity-based attacks increasingly compromise security, it's more important than ever to choose an effective identity protection solution. Organizations may also benefit from addressing in-house skill and resource gaps or outsourcing to a managed solution provider (MSP) that handles technological complexity, system integrations, and real-time monitoring.

Among all identity threats, organizations most expect BEC to increase (63%) in the coming year. This data shows that this attack vector is likely to continue to threaten organizations, potentially at a larger scale. Many also anticipate more issues with credential theft/stuffing (58%) and rogue or malicious applications (52%) (Figure 24).

# Identity-Related Threats Expected to Increase in the Next 12 Months


*Figure 24: Which identity-related threats do you expect to increase most in the next 12 months?*

As the Huntress 2025 Cyber Threat Report indicates, these threats represent just a fraction of common ITDR incidents. Organizations must stay alert and aware of incidents like VPN rule violations, token theft, and adversary-in-the-middle attacks (AiTM) attempts.

While organizations overwhelmingly report that they're confident in uncovering threats like rogue or malicious applications, those with slower detection and response timelines or less advanced identity protection maturity may benefit from revisiting their security protocols and ITDR investments—especially as incident scale or frequency escalates.

> *An ITDR vendor must provide detection of token theft and AiTM attacks, which are steadily becoming the most popular vector to facilitate account takeover. An ITDR vendor that simply regurgitates Microsoft alerting for these events is not doing enough.*
>
> **Rich Mozeleski**
> Huntress Staff Product Manager

# Investment Priorities Center on ITDR Solutions & In-House Expertise

Plans to address growing identity protection concerns vary, but many center around the human element. More than half (53%) of organizations plan to hire identity protection experts in-house over the next 12 months. Nearly half (49%) intend to implement security training and awareness programs (Figure 25).

These investments respond to the lack of sufficient in-house expertise that nearly half of respondents report (Figure 12). However, they overlook the technical limitations that hold many organizations back from achieving advanced identity protection maturity.

## Identity Protection Investment Priorities in the Next 12 Months

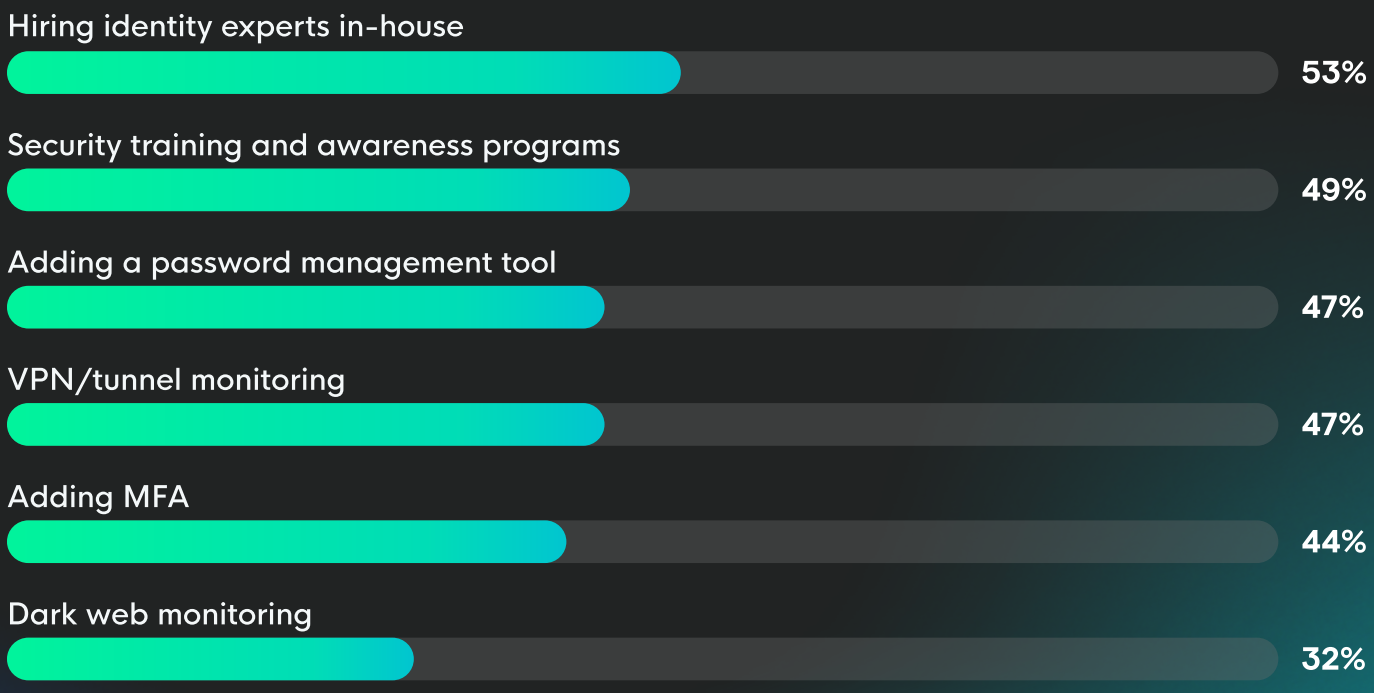


*Figure 25: What are your top priorities for identity protection investments in the next 12 months?*

Many organizations do plan to invest in identity protection technology over the coming year. Almost half (47% and 47%, respectively) plan to add a password management tool and use VPN tunnel monitoring. An additional 44% intend to add MFA protection.

While these additions may help deter some identity attacks, organizations should know that as attackers become more sophisticated, MFA and passwords become easier to bypass. To implement more robust identity protection and achieve advanced maturity, organizations should consider a comprehensive ITDR solution that detects and responds to threats in real time, incorporating both automated technology and analyst review.

> *Implementing Huntress ITDR has been especially effective during the onboarding of new clients. We've uncovered dormant accounts with risky privileges, malicious enterprise app connections, and suspicious mailbox rules—often present for long periods before our involvement. The biggest impact has been stopping identity-based attacks before any damage is done. These prevented incidents save us countless remediation hours and protect our clients from potential financial loss and reputational harm.*
>
> **Ryan Rowbottom**
> Director of IT Services and Incident Response, PCS

Most organizations plan to increase investments in ITDR solutions over the coming year. More than half (53%) of respondents definitely plan to implement or expand ITDR solutions in the next 12 months, while 41% will likely do so (Figure 26).

## ITDR Implementation Plans in the Next 12 Months

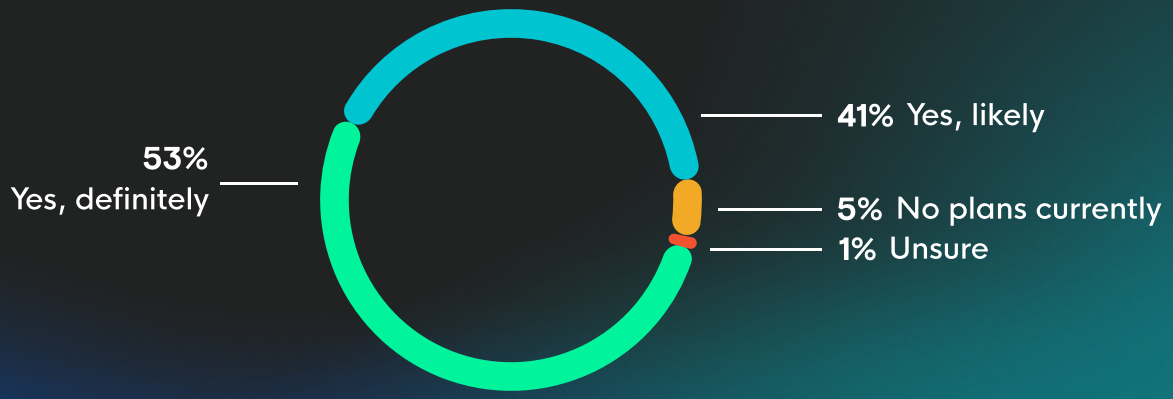


*Figure 26: Do you plan to implement or expand ITDR solutions in the next 12 months?*

Organizations that don't plan to implement or expand ITDR solutions in the near future are in the extreme minority. Only 5% don't currently have plans for ITDR investments.

This breakdown reinforces the importance of prioritizing investments in ITDR. Rather than focusing on prevention, ITDR has the tools and processes to detect and respond to identity-based attacks and emerging threats in real time.

But ITDR investments represent much more than a robust defense against cyber threats. As the fourth edition of the Deloitte Global Future of Cyber Survey states, organizations with more advanced cyber maturity expect nearly two times the positive business outcomes. Rather than making organizations immune to threats, it helps them be more prepared, become more resilient, and ensure business continuity.

> *Phishing isn't just about mass email blasts anymore. Attackers are leveraging breached data, open-source intelligence, and AI-generated deepfakes to craft highly personalized lures. We're seeing convincing deepfake audio used in wire fraud, generative AI powering phishing emails that evade detection, and attackers social engineering their way past identity verification.*
>
> **Prakash Ramamurthy**
> Huntress Chief Product Officer

# Conclusion

Identity incidents are only becoming more common, with BEC, VPN abuse/misuse, and rogue or malicious applications leading the way. These attack vectors are more than a passing trend. They represent a shift in focus, signaling that identity has become the new perimeter.

For most organizations, the financial stakes from identity threats are huge. While most report confidence in their defenses against identity-based attacks, many still lack in-house expertise or advanced identity protection maturity.

In most cases, technology stands in the way. While most organizations use MFA or plan to implement it in the near future, this defense mechanism isn't a complete solution—especially as attacks become more sophisticated.

> *Organizations set up identity protection tools but don't proactively monitor them 24/7 due to resource constraints. They assume MFA is a silver bullet and ignore alerts until it's too late. Instead of just deploying security tools, businesses need to proactively hunt for identity threats, monitor login behaviors, and shut down suspicious activity in real time—or pay for managed services that will.*
>
> **Prakash Ramamurthy**
> Huntress Chief Product Officer

To combat rising threats in the future, organizations need to pivot to proactive identity protection strategies with continuous monitoring, threat hunting, and automated response capabilities. Managed ITDR solutions give a compelling path forward, as they combine automated technology with human expertise.

As identity becomes a critical component of the security perimeter, the organizations that thrive will be those that prioritize comprehensive identity threat detection and response. With sufficient investment and strategic implementation, these organizations can reduce their risk while becoming stronger.

> *Here's the reality: no single control will stop every attack. Tenant configurations can be misconfigured, users will still fall for phishing, and attackers will find a way in. That's why detection and response is just as critical. You need to monitor for abnormal logins, track risky token use, and shut down compromised sessions before attackers can escalate privileges. Not doing these things means you risk exploitation of your most critical business assets.*
>
> **Prakash Ramamurthy**
> Huntress Chief Product Officer

# Methodology & Demographics

Huntress commissioned an independent market survey from UserEvidence of 608 IT security professionals about their approach to identity-related attacks and identity protection.

The largest cohorts (39% and 38% of respondents, respectively) held an IT/security role at the manager or director level. The remaining respondents were IT/security executives, administrators, and staff (Figure 27).

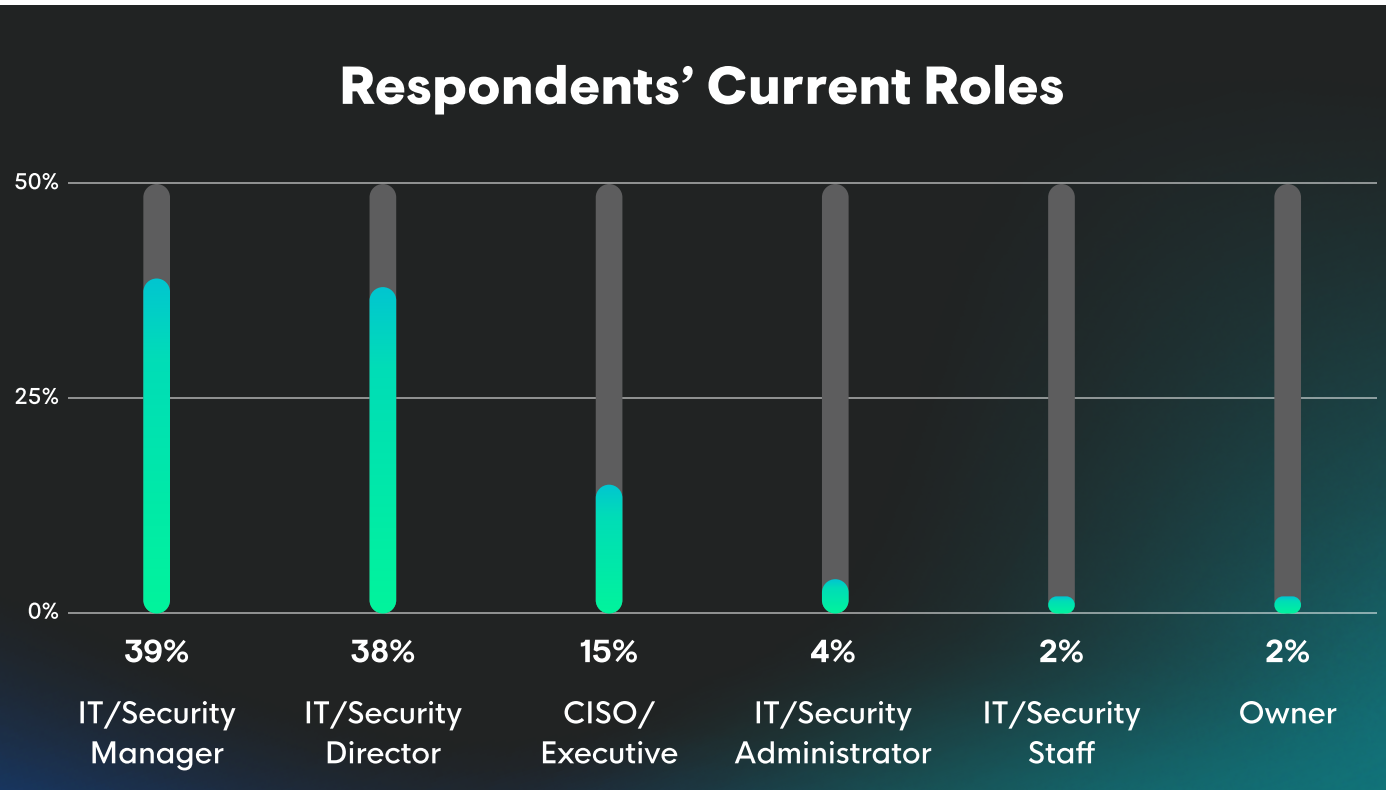


*Figure 14: Compared to three years ago, how has the frequency of identity-related attacks changed?*

Most respondents (70%) were part of internal IT/security teams. The remaining 30% delivered IT and security services via an MSP or outsourced IT and security vendor (Figure 28).

## Respondents' Roles in Delivering IT & Security Services


*Figure 28: Which of the following best describes your role in delivering IT & security services?*

Over three-quarters (79%) of respondents were from mid-size organizations with 500-5,000 endpoints, while the remaining 21% were from businesses with 250-499 endpoints (Figure 29).

## Respondents' Organization Size


*Figure 29: What is your organization's size (measured by number of endpoints)?*

Microsoft 365 was the dominant cloud productivity suite, as the primary software for 61% of respondents. The remaining 39% reported using Google Workspace (Figure 30).

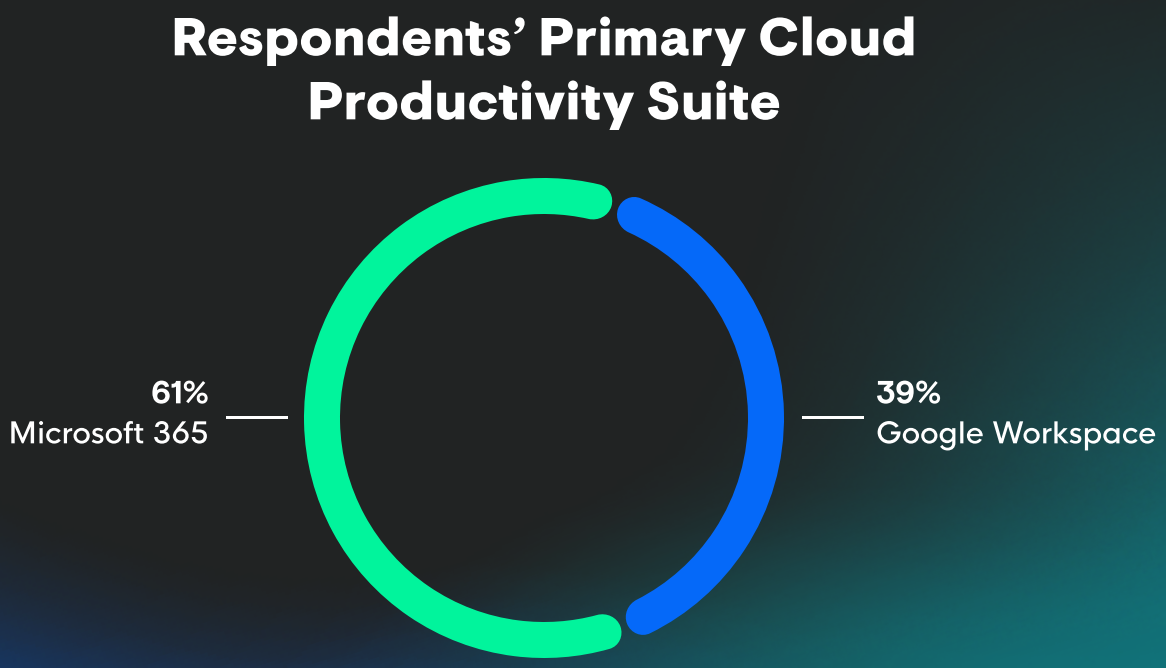


*Figure 30: Which cloud productivity suite does your organization primarily use?*

# About UserEvidence

UserEvidence is a software company and independent research partner that helps B2B technology companies produce original research content from practitioners in their industry. All research completed by UserEvidence is verified and authentic according to their research principles: Identity verification, significance and representation, quality and independence, and transparency. All UserEvidence research is based on real user feedback without interference, bias, or spin from our clients.

## UserEvidence Research Principles

These principles guide all research efforts at UserEvidence—whether working with a vendor's users for our Customer Evidence offering, or industry practitioners in a specific field for our Research Content offering. The goal of these principles is to give buyers trust and confidence that you are viewing authentic and verified research based on real user feedback, without interference, bias, and spin from the vendor.

## 1. Identity Verification

These principles guide all research efforts at UserEvidence—whether working with a vendor's users for our Customer Evidence offering, or industry practitioners in a specific field for our Research Content offering. The goal of these principles is to give buyers trust and confidence that you are viewing authentic and verified research based on real user feedback, without interference, bias, and spin from the vendor.

## 2. Significance and Representation

UserEvidence believes trust is built by showing an honest and complete representation of the success (or lack thereof) of users. We pursue statistical significance in our research, and substantiate our findings with a large and representative set of user responses to create more confidence in our analysis. We aim to canvas a diverse swatch of users across industries, seniorities, personas—to provide the whole picture of usage, and allow buyers to find relevant data from other users in their segment, not just a handful of vendor-curated happy customers.

## 3. Quality and Independence

UserEvidence is committed to producing quality and independent research at all times. This starts at the beginning of the research process with survey and questionnaire design to drive accurate and substantive responses. We aim to reduce bias in our study design, and use large sample sizes of respondents where possible. While UserEvidence is compensated by the vendor for conducting the research, trust is our business and our priority, and we do not allow vendors to change, influence, or misrepresent the results (even if they are unfavorable) at any time.

## 4. Transparency

We believe research should not be done in a black box. For transparency, all UserEvidence research includes the statistical N (number of respondents), and buyers can explore the underlying blinded (de-identified) raw data and responses associated with any statistic, chart, or study. UserEvidence provides clear citation guidelines for clients when leveraging research that includes guidelines on sharing research methodology and sample size.

# About Huntress

Huntress is the enterprise-grade, people-powered cybersecurity solution for all businesses, not just the 1%. With fully owned technology developed by and for its industry-defining team of security analysts, engineers, and researchers, Huntress elevates underresourced tech teams whether they work within outsourced IT environments or in-house IT and security teams.

The 24/7 industry-leading Huntress Security Operations Center (SOC) covers cyber threats for outsourced IT and in-house teams through remediation with a false-positive rate of less than 1%. With a mission to break down barriers to enterprise-level security and always give back more than it takes, Huntress is often the first to respond to major hacks and threats while protecting its partners and shares tradecraft analysis and threat advisories with the community as they happen.

As long as hackers keep hacking, Huntress keeps hunting. Join the hunt at www.huntress.com and follow us on X, Instagram, Facebook, and LinkedIn.