Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **January 2026**
Sponsored by **Abnormal AI**

Strengthening Identity Security: Governance, Visibility and Autonomous Remediation

Executive summary

Threats against identities and their protections are worsening. Cybercriminals are more interested in stealing and abusing compromised credentials, organizations often can't detect exposed credentials on the dark web, and visibility into the actions and behaviors of service accounts is lacking. Threat actors are increasingly leveraging social engineering for compromising credentials. Internally, most organizations lack the optics and processes to detect identity-led threats.

New identity security solutions are emerging to protect identities—both human and non-human—by layering additional protections on identity and access management tools. These include solutions for visibility, governance, and autonomous remediation. While the organizations in this research claim high maturity for current identity security deployments, evidence of high maturity is lacking for most. All organizations must urgently revisit their identity security protections, deploy new or advanced solutions to strengthen identity security posture, and reduce exposure to the negative implications of identity-led threats.

New identity security solutions are emerging to protect identities—both human and non-human—by layering additional protections on identity and access management tools.

KEY TAKEAWAYS

The key takeaways from this research are:

- **Identity-led and identity-implicated threats are escalating**
  72.1% of the organizations in this research say that the threat level of 15 identity-led and identity-implicated cyberattacks has increased or remained unchanged over the past 12 months. The use of AI by threat actors to create highly personalized attacks had the most significant increase.
- **The importance of identity security technologies is rising rapidly**
  Across 22 identity-related capabilities, average importance is anticipated to increase from 47% two years ago to 68.1% in two years. The ability to detect identity misuse persists as the most important capability, and capabilities that enable the rightsizing of access rights increase in importance the most.
- **Claims of high maturity in identity security deployments lack supporting evidence**
  68.7% of organizations claim their current identity security deployments are mature, yet flow-on outcomes undermine this assertion. Organizations claiming high maturity would be well advised to check alignment with actual outcomes—and take the necessary steps to address systemic weaknesses.
- **Improving visibility into identity threats is fundamental**
  Over three quarters of organizations have less than full and complete visibility into 14 different identity threats and security fundamentals. Lack of visibility into identity vulnerabilities is a critical shortcoming to address because identity-led attacks start with just one compromised identity-related asset, such as a credential for sale on a dark web forum. Enhanced visibility combined with automated detection and remediation of compromised credentials is essential for closing this gap.
- **Identity configurations in identity platforms need resilience and recovery options**
  Identity configuration data—especially in platforms like Microsoft Entra ID—is a blind spot in many security strategies. Organizations must back up identity platforms as they would any other critical system to ensure resilience and recovery.

ABOUT THIS WHITE PAPER

Abnormal AI sponsored this white paper. Information about Abnormal AI is provided at the end of this paper.

What is identity security?

There was a time when a username and password was enough to limit access by authorized people to the systems and data they needed to do their work. The world was less interconnected, cross-system traversal subject to more friction, and the risk of credential compromise too insignificant for most to enact a higher posture of protection. Those times have gone—and they are not coming back. Consider:

- Hackers in Brazil paid $2,760 to use an employee's credentials and used it to steal $140 million from Brazilian banks.[1]
- 1 in 10 Fortune 500 employees have had their credentials exposed in the last three years, posing a significant risk for account takeover.[2]
- In one dataset of 11.8 billion newly breached identity records in 2024, 6.4 billion records included an email address and 2.5 billion a password.[3]
- In 95% of data breaches, human error is a factor. These error types include credential misuse and poor password hygiene.[4]
- Infostealer activity increased dramatically during 2024 to steal credentials for cloud accounts, for use in further credential compromise attacks.[5]
- Famous Chollima, a threat actor group aligned with the North Korean government, has infiltrated thousands of organizations with fake IT workers. With high-privilege access to cloud and other accounts, these workers have compromised cloud accounts, planted malware, and more.[6]
- The increase in non-human identities (NHI) is exacerbating an already challenging problem. NHIs outnumber human identities by more than 50:1, a number which will grow rapid as adoption of AI agents increases. To make it worse, 40% of NHIs are without a clear owner.[7]

When the world was less interconnected, cross-system traversal subject to more friction, and credential compromise risks insignificant, a username and password was often enough. Not anymore.

Against the backdrop of an intensifying threat landscape, new solutions are emerging to protect—not just manage—identities, including:

- **Visibility** of which identities are protected and unprotected, risk scoring of identity vulnerability, which credentials are compromised on the dark web, and where identities are being used across the complete lattice of on-premises and cloud systems used by an organization and its employees. Behavioral baselining assists with detecting insider threats and outsider intrusions.
- **Governance** to ensure identities are provisioned with the correct level of access rights to systems and data as the employee associated with a given identity changes work roles over their employment lifecycle.
- **Autonomous remediation** combines preemptive protection with proactive remediation, acting without human intervention when compromised identities or abnormal usage patterns are detected. This could be step-up authentication when an identity is used from an unusual geography, identity lock-out when credentials are listed for sale on the dark web, granting limited access to an identity, and ensuring tight change controls on identity platforms.

These solutions are part of identity security, an emerging area in cybersecurity that focuses on protecting identities—both human and non-human—to assure only authorized access to resources, prevent credential misuse, protect against lateral movement and help teams detect and respond to identity-based attacks. It layers additional protections on identity and access management (IAM) tools and processes, a complementary area of cybersecurity that focuses on verifying user identities and providing access to resources.

Identity protections are under attack

Identities and their protections are routinely under attack, as evidenced by the high frequency of identity as a root cause in successful breaches,[8] advances in credential stuffing attack capabilities,[9] advanced phishing attacks that overcome multi-factor authentication (MFA) protections,[10] and the potential for threat actors to aggregate data breach records to create a profile of target victims for phishing and social engineering,[11] among others. In this section, we look at identity threat realities for the organizations in this research.

EXTERNAL AND INTERNAL THREATS FROM IDENTITY ATTACKS

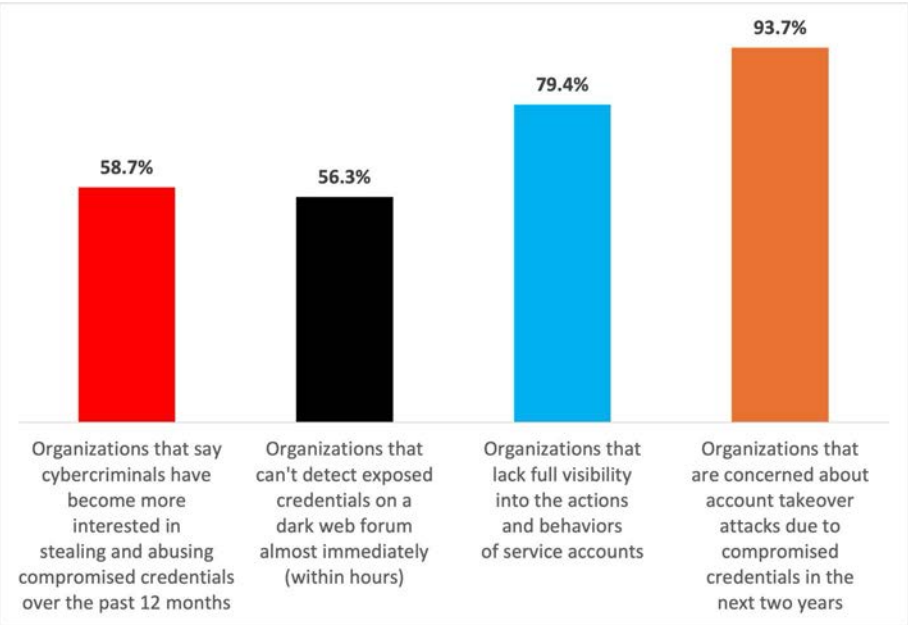
The threat level of attacks that weaponize, compromise, or leverage identity for malicious purposes has increased at organizations. In this research, 58.7% of respondents say that cybercriminals have become more interested in stealing and abusing compromised credentials over the past 12 months, and another 12.7% say the threat of compromised credentials has remained constant over that timeframe. The external threat landscape that compromises identity is getting worse.

Internal realities contribute to the threat of identity attacks. Most organizations lack the ability to immediately detect when the credentials of employees are exposed on dark web forums (56.3%), elongating the threat timeframe before valid but compromised credentials can be revoked or otherwise subjected to elevated protections. Almost 80% lack visibility into what service accounts are doing, such as the actions being taken and flagging unexpected behaviors. Given the worsening of the external threat landscape and the lack of security protections internally, it is unsurprising that almost all organizations are concerned about account takeover attacks due to compromised credentials in the next two years (93.7%).

See Figure 1.

58.7% of respondents say that cybercriminals have become more interested in stealing and abusing compromised credentials over the past 12 months.

Figure 1
Identity threats and risks
Percentage of respondents



Source: Osterman Research (2025)

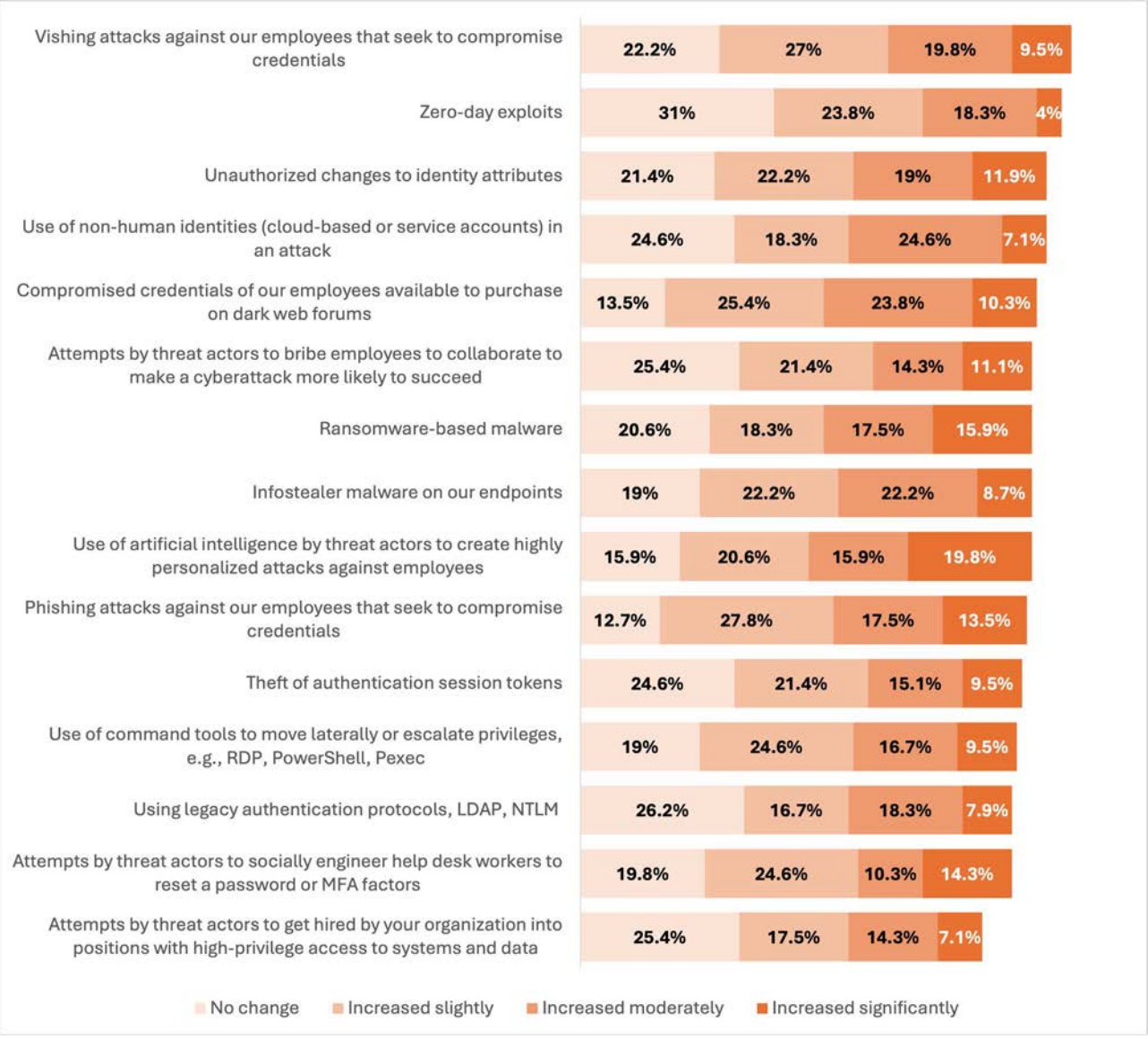
THREAT LEVELS OF IDENTITY-LED AND -IMPLICATED ATTACKS ARE INCREASING

Across a range of common identity-led and identity-implicated cyberattacks against organizations over the past 12 months, 72.1% of the organizations in this research say that the threat level has increased or remained unchanged. Over half say the threat level has increased. Vishing attacks against employees tops the list, followed by zero-day exploits and unauthorized changes to identity attributes.

The threats that increased at the highest intensity rating over the past 12 months are the use of AI by threat actors to create highly personalized attacks against employees (19.8%), ransomware-based malware (15.9%), and the social engineering of help desk employees to enable credential compromise (14.3%).

See Figure 2.

Figure 2
Change in threat level of identity and other attacks over the past 12 months
Percentage of respondents



Source: Osterman Research (2025)

VISIBILITY INTO IDENTITY USAGE AND SECURITY POSTURE IS LACKING

Over three quarters of organizations have less than full and complete visibility into 14 different identity threats and security fundamentals, such as which high-privilege users are not using MFA, historical changes to identity configurations, and even SaaS apps being used by employees. Analysis of the 14 threats and fundamentals are presented over the next three sections.

Lack of visibility into identity vulnerabilities is a critical shortcoming to address because identity-led attacks start with just one compromised identity-related asset. From there, through lateral movement and privilege escalation techniques, threat actors compromise a wider selection of identities, systems, and data, hence laying the foundation for a ransomware attack, data breach, or other nefarious plan.

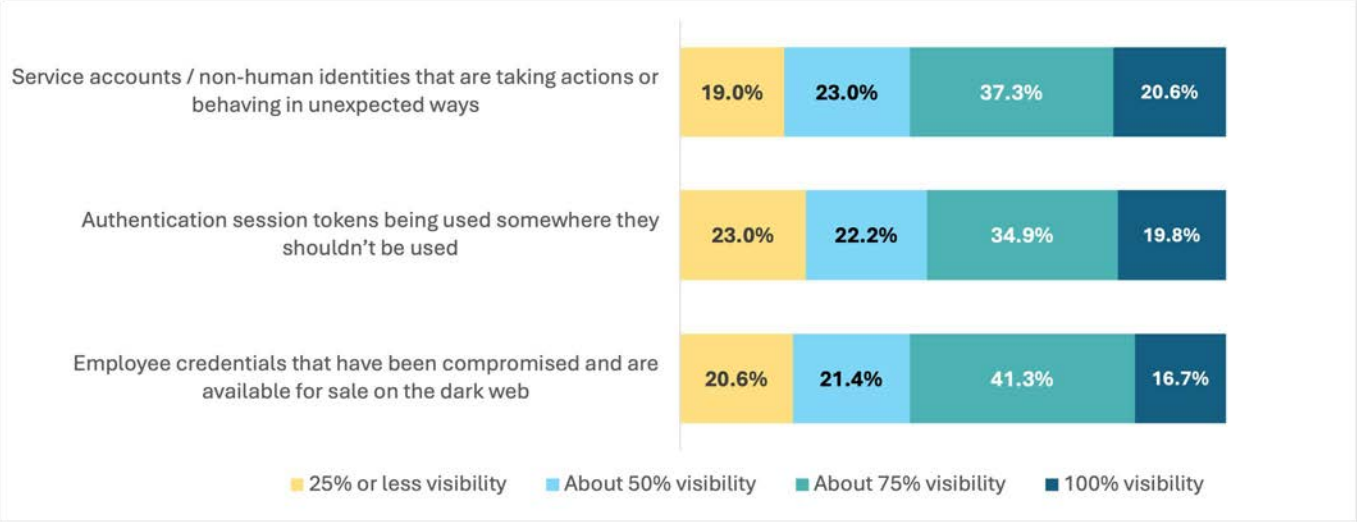
Most organizations cannot see when critical identity threats are under active exploitation.

Visibility into active threats under active exploitation

Three of the 14 threats or fundamentals represent situations of active threat under exploitation. Only 19% of organizations, on average, have complete visibility into these types of identity-based threats: service accounts (or non-human identities) behaving in unexpected ways, authentication session tokens being used in abnormal places, or compromised employee credentials for sale on the dark web. Most cannot see when critical identity threats are being actively worked on by threat actors.

See Figure 3.

Figure 3
Visibility into active threats under active exploitation
Percentage of respondents



Source: Osterman Research (2025)

Of the three, service accounts/non-human identities likely contain the greatest future threat to organizations, due to the rapid forecasted adoption of AI agents that have the rights to act autonomously across systems and data. The non-deterministic decision engines in AI could easily lead to agents running amok, inadvertently leaving cybersecurity weaknesses and incidents in their wake. Lack of visibility into this type of identity and process could threaten organizational viability.

Visibility into MFA posture—usage and factors

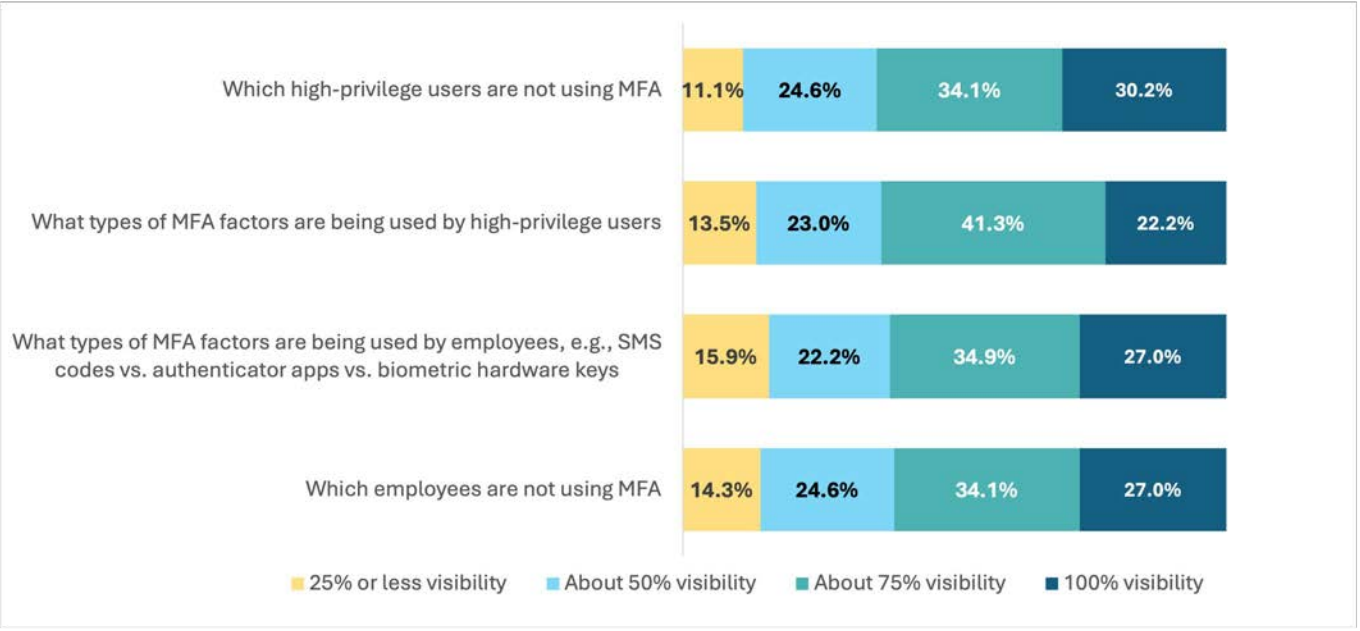
Four of the 14 threats or fundamentals deal with MFA, a near-universal recommendation for strengthening identity security. The details with MFA matter significantly in stopping modern threats, such as types of factors being used:

- 70% of organizations lack complete visibility into whether MFA is being used or not by high-privilege users.
- Almost 80% don't know what types of MFA factors are being used by high-privilege users.
- 73% don't have the full picture of what types of MFA factors are being used by employees.

MFA has been widely advocated for strengthening identity security over the past decade, but even so, only an average of 26.6% of organizations have 100% visibility into these MFA posture details. Critically, the protection that MFA provides is only as strong as each individual factor, including the password, so every factor must remain secure.

See Figure 4.

Figure 4
Visibility into MFA posture
Percentage of respondents



Source: Osterman Research (2025)

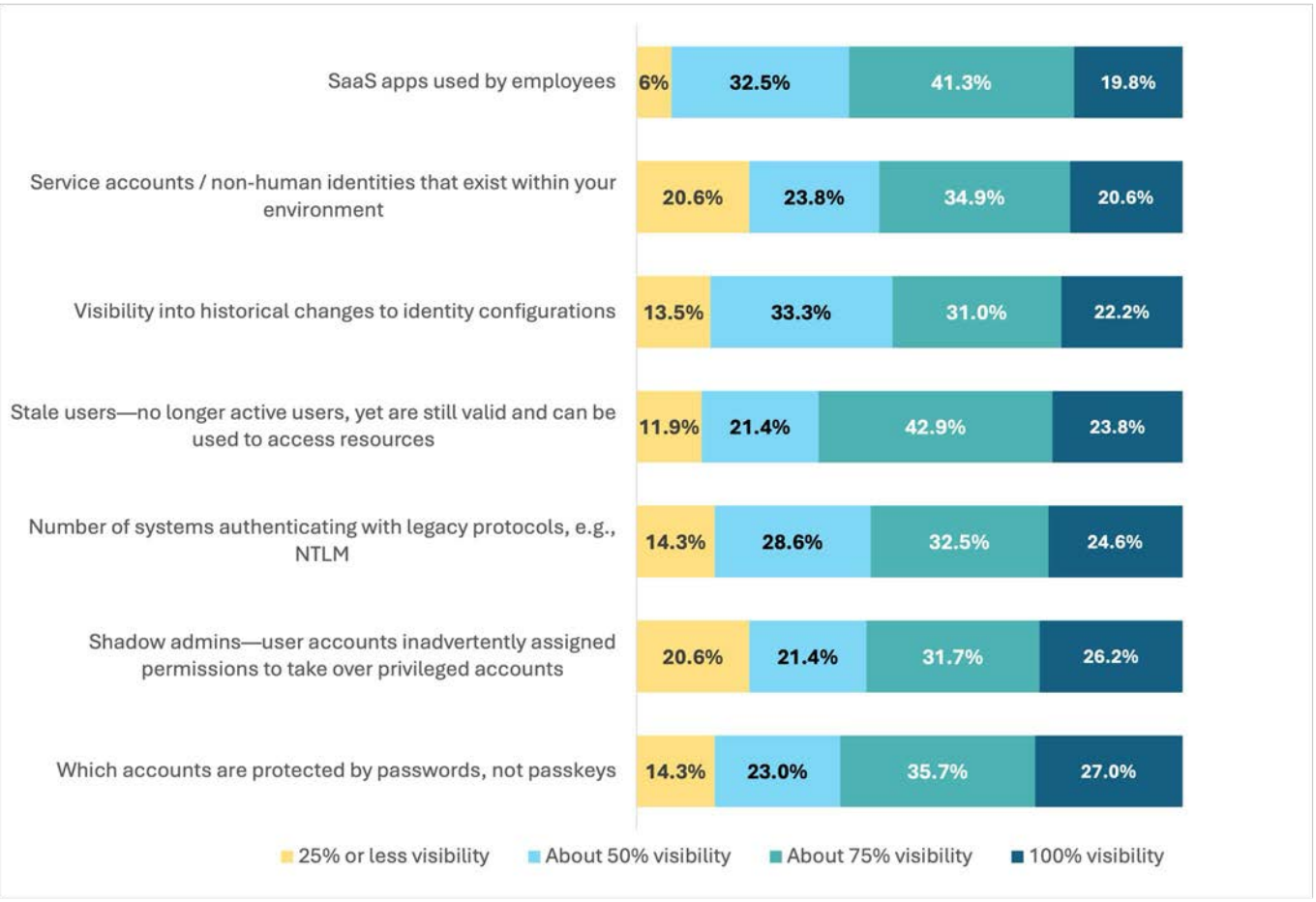
Visibility into potential identity posture weaknesses

The remaining threats or fundamentals we asked about represent the details on identity security posture for an organization. Each contains the sense of a weakness that could be actively exploited for malicious purposes, even though that is not necessarily happening currently. Only an average of 23.5% of organizations have 100% visibility across the potential weaknesses in Figure 5. This includes accounts protected by passwords rather than passkeys, employee credentials that have been compromised and are available for sale on the dark web, user accounts inadvertently assigned elevated permissions, and the presence of an audit trail on changes to identity configurations, among others.

For the potential weaknesses in this grouping, visibility enables proactive remediation such as using automated tools to help employees choose strong and secure passwords, revoking elevated permissions to rightsize previously over-permissioned accounts, and rolling back inappropriate or outdated identity configuration changes. Without visibility, identity configurations drift out of ideal tolerance ranges, inadvertently opening access pathways for identity compromise, unauthorized system access, and data breach.

See Figure 5.

Figure 5
Visibility into potential identity posture weaknesses
Percentage of respondents



Source: Osterman Research (2025)

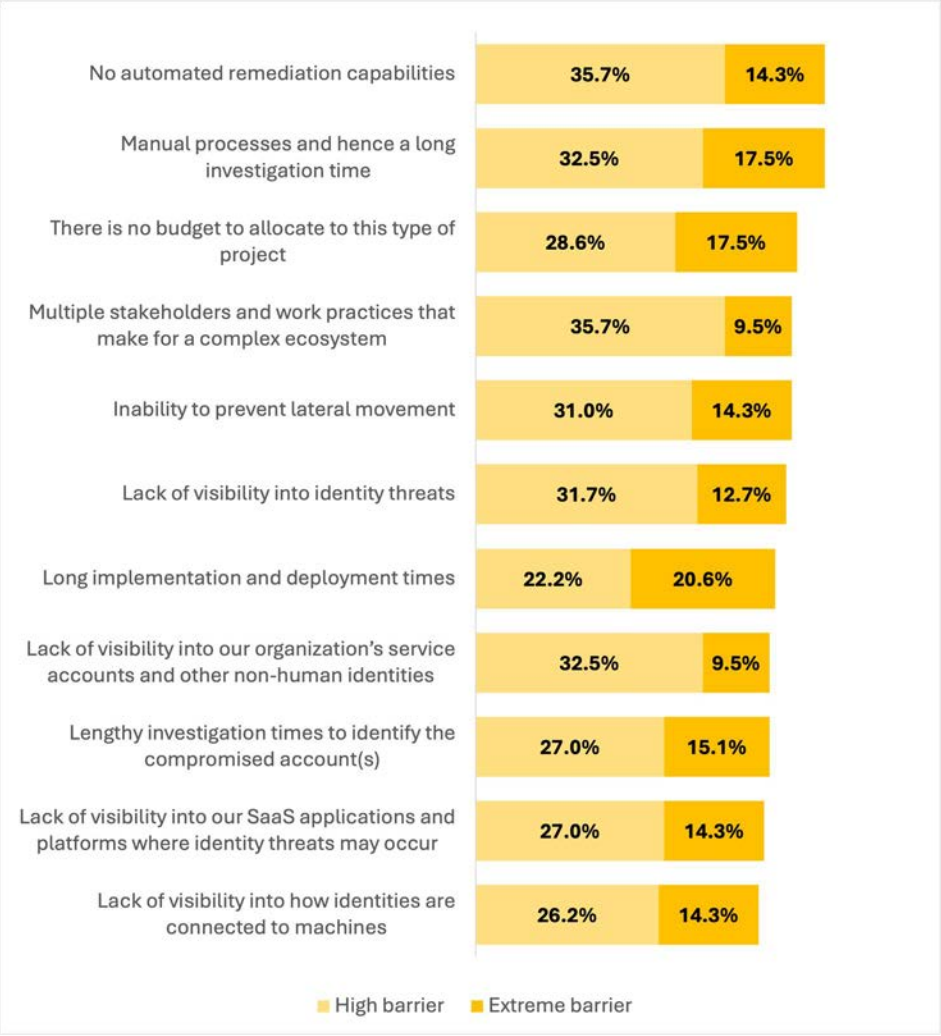
BARRIERS TO STOPPING IDENTITY THREATS

The top barriers for stopping identity threats are the lack of automated remediation capabilities, followed by manual processes and hence a long investigation time. These are one and the same barrier. The third barrier is lack of budget to allocate to identity security investments. Organizations appear to have prioritized spending any available money on funding manual processes—which will not scale as threats increase in volume and sophistication—rather than investing in new identity security solutions that introduce automated remediation capabilities to an organization.

Manual processes for addressing identity security weaknesses have exceeded their remit. Preventing lateral movement (barrier 5), giving visibility to identity threats (barrier 6), and even lengthy investigation times to identify compromised accounts (barrier 9) are all barriers that can only be solved by new identity security solutions.

See Figure 6.

Figure 6
Barriers to stopping identity threats
Percentage of respondents



Source: Osterman Research (2025)

Organizations appear to have prioritized spending any available money on funding manual processes—which will not scale as identity threats further escalate.

Identity security: An evolving slate of protections

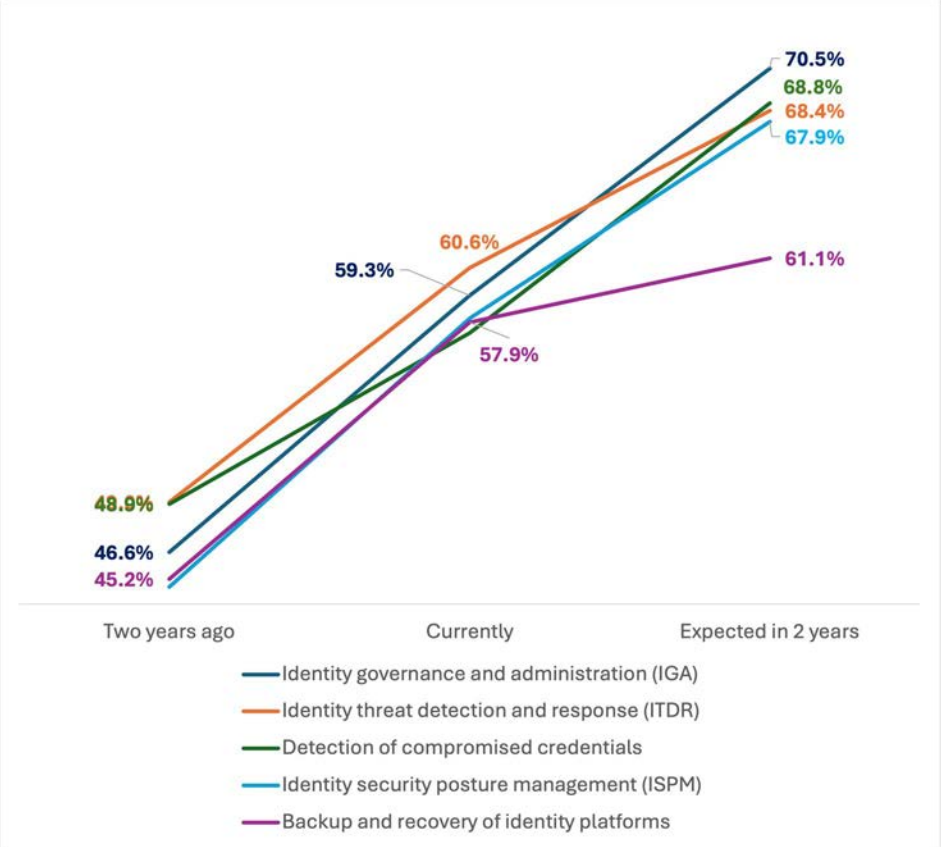
Identity security protections are rapidly becoming more important to organizations, and most are planning to deploy new or advanced capabilities over the next two years.

IMPORTANCE OF SECURING IDENTITIES IS RISING

We asked respondents to assess the importance of 22 identity-related capabilities to their organization over three time periods: two years ago, currently, and the anticipated importance in two years' time. The average importance of all 22 capabilities increased across the three time periods—from 47% of respondents saying "very important" or "extremely important" two years ago, to 58.3% currently, and an anticipation of 68.1% in two years' time.

Figure 7 shows the increase in importance for the capabilities grouped by the identity security technology they normally fit into.

Figure 7
Importance of identity security capabilities—grouped by technology area
Percentage of respondents indicating "very important" or "extremely important"



Source: Osterman Research (2025)

Identity security capabilities are rapidly becoming significantly more important to organizations.

Figure 8 shows the overall ranking of identity security capabilities currently. Detecting identity misuse and compromise top the list.

Figure 8
Current importance of identity security capabilities
Percentage of respondents indicating "very important" or "extremely important"

Source: Osterman Research (2025)

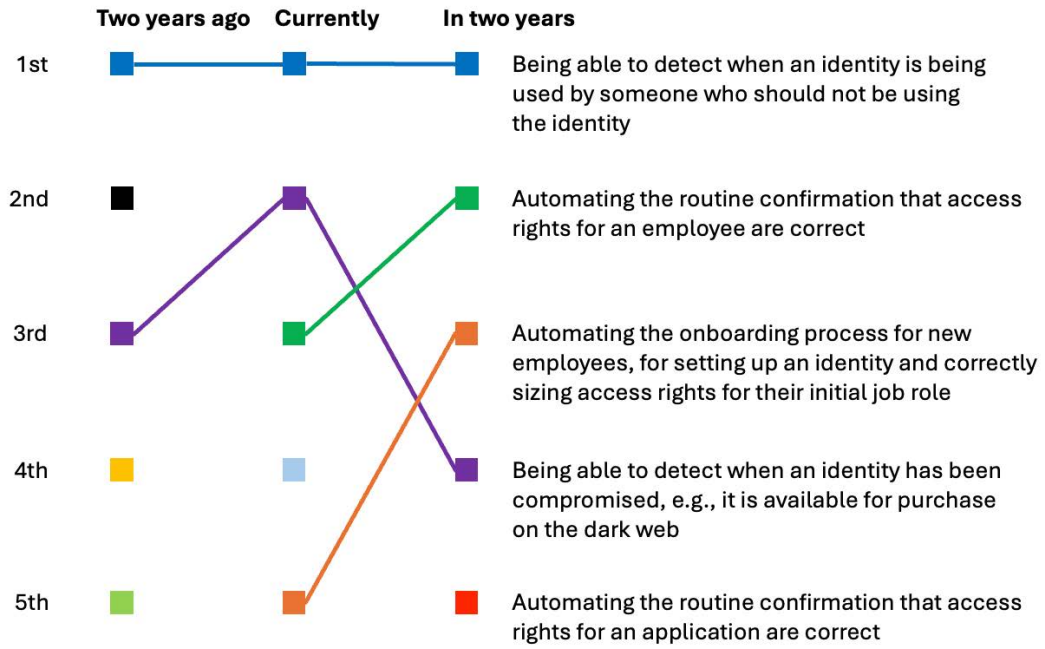
FIVE HIGHEST-RATED IDENTITY SECURITY CAPABILITIES

The capability rated the most important across all three time periods is the ability to detect when an identity is being used by someone who should not be using the identity. Solving for this problem is one of the goals of all identity security solutions.

Four of the capabilities ranked highest currently are expected to carry forward in high importance in two years' time, too.

See Figure 9.

Figure 9
Importance of identity capabilities
Respondents indicating "very important" or "extremely important"



Source: Osterman Research (2025)

The five capabilities with the highest growth in importance over the three time periods are shown in Figure 10.

Figure 10
Importance of identity capabilities
Percentage increase in importance ("very important" or "extremely important") from two years ago compared to anticipated importance in two years' time

Rank	Identity capability	Increase
1	Automating the routine confirmation that access rights for an application are correct	62.5%
2	Automating the routine confirmation that access rights for an employee are correct	62.1%
3	Automating the departing employee process for offboarding employees and rescinding their identity and access rights	57.9%
4	Discovery and mapping of non-human identities, e.g., tokens, API keys, service accounts	55.4%
5	Providing actionable recommendations to remediate identity weaknesses like misconfigurations	53.8%

Source: Osterman Research (2025)

The key theme in Figure 10 is the proactive rightsizing of access rights—ensuring that access rights for both applications and employees are always correct and valid. As part of a cohesive identity security strategy, proactive rightsizing holds the potential for fewer identity-led incidents.

Proactive rightsizing of access rights holds the potential of fewer identity-led incidents.

The deeper trendline, however, is the growth among respondents selecting the "extremely important" rating rather than the "very important" rating for the 22 capabilities. While the "very important" rating increased an average of 6.1% across the three time periods, the rating for "extremely important" rose by an average of 132.2%. The capabilities with the highest growth rate for the extremely important rating are shown in Figure 11.

Figure 11
Importance of identity capabilities
Percentage increase in importance ("extremely important" only) from two years ago compared to anticipated importance in two years' time

Rank	Identity capability	Increase
1	Being able to see what security controls are being used across all users, e.g., whether MFA is being used, what types of MFA are being used, admin accounts that are not vaulted, etc.	212.5%
2	Preventing lateral movement	200%
3	Preventing privilege escalation	193.3%
4	Automating the onboarding process for new employees to set up an identity and correctly sizing access rights for their initial job role	188.2%
5	Automating the internal move process for employees to ensure access rights are updated and correct when an employee moves to a new role within the organization	175%

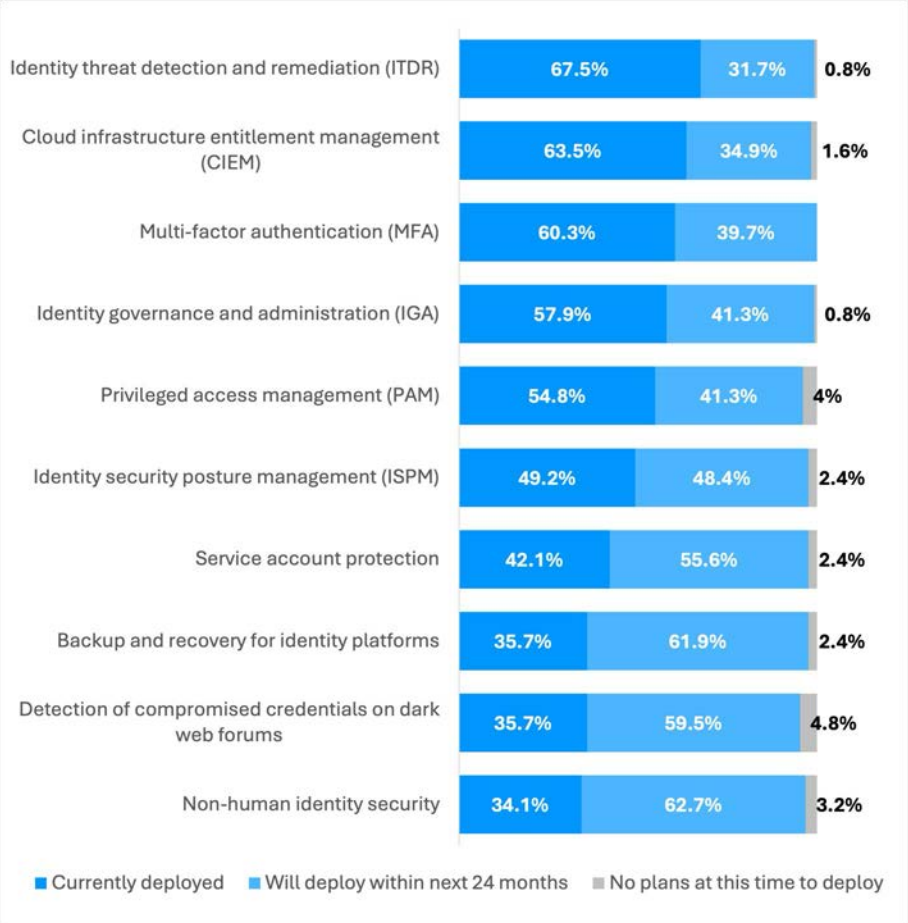
Source: Osterman Research (2025)

IDENTITY SECURITY TECHNOLOGY STACK—CURRENT STATE

More than half of the organizations in this research say they have adopted some form of ITDR, CIEM, MFA, IGA, and PAM technologies within their identity security technology stack. This is an assessment of adoption status (yes or no), not of deployment maturity. Solutions with lower adoption rates are non-human identity security (34.1%), detection of compromised credentials on dark web forums (35.7%), and backup and recovery of identity platforms (35.7%), among others.

Among organizations not currently using the identity security technologies we asked about in this research, as shown in Figure 12, the vast majority plan to deploy new technologies within the next 24 months.

Figure 12
Current posture of the identity security technology stack
Percentage of respondents



Source: Osterman Research (2025)

On average, 2.2% of the organizations in this research do not currently have plans to deploy the technologies shown in Figure 12.

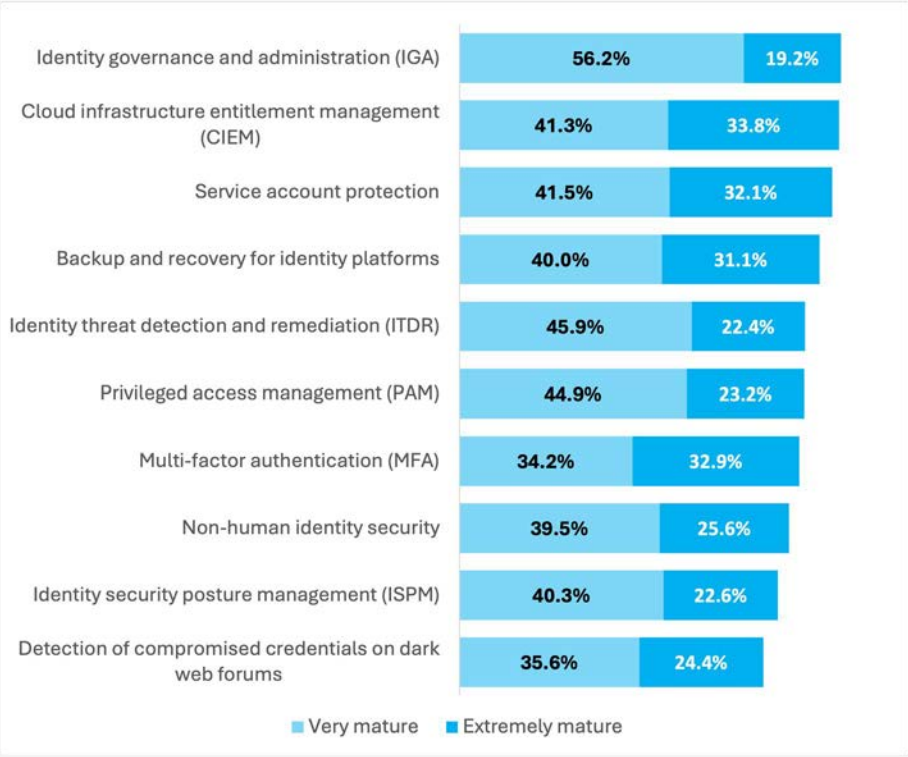
Within 24 months, almost all organizations anticipate having a full complement of identity security solutions.

HIGH MATURITY CLAIMED FOR IDENTITY SECURITY TECHNOLOGIES

68.7% of organizations currently using the identity security technologies we asked about say they have reached a deployment status of "very mature" (average 41.9%) or "extremely mature" (average 26.7%). Organizations claimed the highest maturity ratings for CIEM, MFA, and service account protection, and the lowest for IGA, ITDR, ISPM, and PAM.

See Figure 13.

Figure 13
Maturity of the identity security technology stack
Percentage of respondents currently using the identity security technology



Source: Osterman Research (2025)

The organizations in this research claim high maturity for their deployment of identity security technologies.

Of the four identity security technologies with the lowest showing for the "extremely mature" option, IGA is likely to improve the most over the next two years. Per Figure 10 and Figure 11 above, IGA tops the list of capabilities with rapidly growing importance over that timeframe. This includes automation of the following:

- Routine confirmation that access rights for an application are correct
- Routine confirmation that access rights for an employee are correct
- Offboarding employees and rescinding identity and access rights
- Onboarding new employees to set up an identity and correctly size access rights for their initial job role
- Ensuring access rights are updated and correct when an employee moves to a new role within the organization

CLAIMED MATURITY IS HIGHER THAN THE EVIDENCE WARRANTS

Many respondents claiming high maturity in their identity security deployments do not exhibit sufficient evidence in flow-on outcomes to warrant this claim. For example:

- **Identity threat detection and remediation**
  67.5% of respondents are currently using ITDR capabilities in some form (Figure 12), and of this group, 68.3% claim high maturity in their deployment ("very mature" or "extremely mature")—see Figure 13. When we look for evidence of mature ITDR capabilities in how respondents answered related questions, however, only 42.4% of respondents have a high-maturity deployment. This evidence includes aspects such as visibility into threats ITDR solutions would capture, along with confidence to detect misuse of valid credentials. Some of the group with evidence of high maturity didn't rate their deployment as highly mature, and of the original cohort claiming high maturity, only half produce evidence to back up the claim.
- **Detection of compromised credentials on dark web forums**
  35.7% of respondents are currently using technologies for detecting compromised credentials on dark web forums (Figure 12), and of this group, 60% claim their deployment is highly mature ("very mature" or "extremely mature")—per Figure 13. After cross-checking each respondent's answers to three other questions—the level of visibility into compromised credentials, the timeframe for detecting a credential exposure, and current confidence in the ability to detect an attempt to use valid but compromised credentials, only 22% of those claiming high maturity give evidence of high maturity. Automating the detection and remediation of compromised credentials is a critical part of elevating maturity in this area.
- **Backup and recovery of identity platforms**
  35.7% of respondents indicate they are using some form of backup and recovery for identity platforms, with 71% claiming their deployment is very or extremely mature. We looked for evidence to back up these claims, and the reality was often different. We correlated visibility into historical changes to identity configurations along with confidence levels to recover from attacks where malicious actors make unauthorized changes to identity configurations, e.g., Entra ID roles or groups. For example, unauthorized deletions of Entra ID group memberships or admin roles—whether malicious or accidental—often go unlogged, unrecoverable, and unnoticed until access issues cascade. Without full historical snapshots and point-in-time recovery, organizations are left without a safety net. In total, only 41% give sufficient evidence of high maturity, not 71%.

Organizations claiming high maturity would be well advised to check alignment with actual outcomes—and take the necessary steps to address systemic weaknesses.

Identity security is an emerging area in cybersecurity and is different to the protections and capabilities available in underlying IAM platforms. The disparity between claimed maturity and evidenced maturity will arise from different places across the organizations in this research. For some respondents, the issue will be lack of education on what's needed, possible, and different from existing protections at this stage of the development of new identity security capabilities. For others, it's an assumption that capabilities bundled with IAM platforms are sufficient—and hence a lack of recognition that identity threats have shifted. And for others still, it's a blindness to identity threats and realities often due to insufficient visibility.

Whatever its source, organizations claiming high maturity would be well advised to check alignment with actual outcomes—and take the necessary steps to address systemic weaknesses. If not, when an identity-led attack successfully compromises the organization, the illusion of maturity will shatter—at significant financial and reputational cost.

MAPPING INVESTMENT REQUIRED AND 12-MONTH PRIORITY

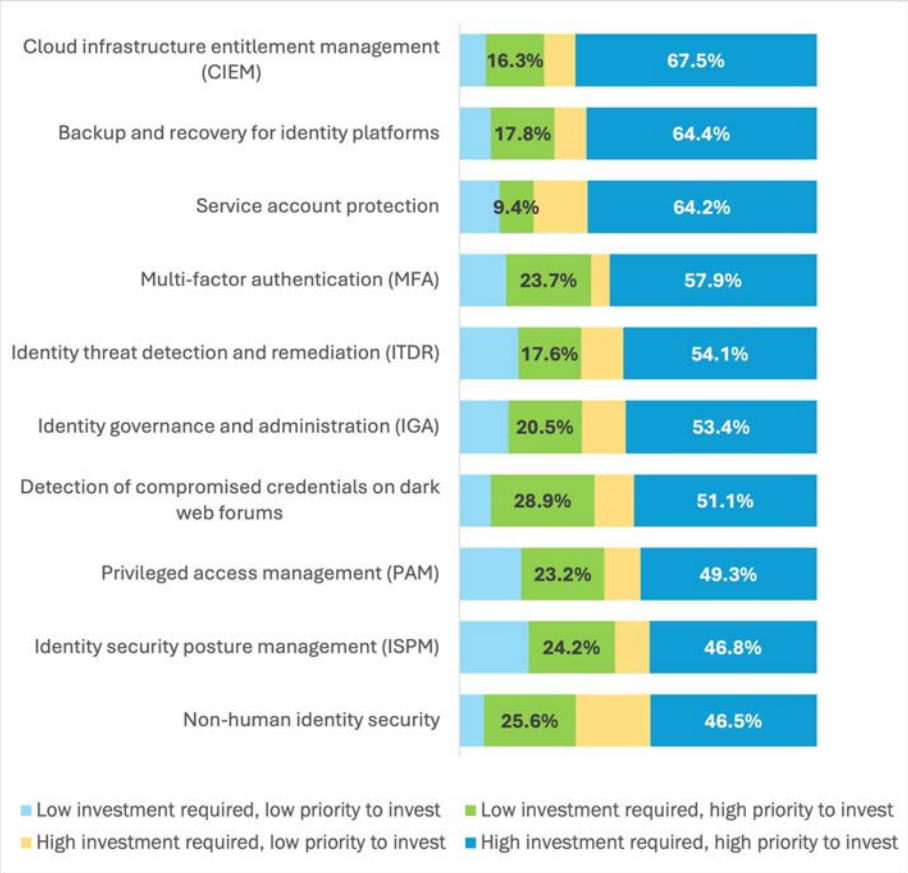
For the organizations in this research already using some form of the identity security technologies we asked about, we correlated two data points: first, the level of financial investment required to lift each identity security technology to the desired standard of the organization, and second, the priority of investing in each area over the next 12 months. On average, three out of four organizations in this research are placing a high priority on investing in a range of technologies.

The most common pattern is where high priority for improving the strength of an identity security technology is set against the backdrop of high required investment (average 55.5%). Organizations in this situation are lacking in identity security capabilities and are investing under urgency to catch up.

The second most common pattern is organizations that have low investment requirements matched with high priority. Such organizations have previously invested in building identity security capabilities but are investing further to strengthen current capabilities.

See Figure 14.

Figure 14
Identity security investment levels and priority over the next 12 months
Percentage of respondents currently using the identity security solution



Source: Osterman Research (2025)

Over half of organizations are lacking in identity security capabilities and are investing under urgency to catch up.

TIMEFRAME FOR DEPLOYING NEW IDENTITY SECURITY SOLUTIONS

Among organizations not currently using the identity security solutions we asked about, nine out of ten intend to deploy new solutions in the next 12 months. MFA, detection of compromised credentials on dark web forums, and ITDR lead the list for deployment within the next three months. Backup and recovery for identity platforms, ISPM, and ITDR feature strongly in the 4-6 months timeframe.

See Figure 15.

Figure 15
Deployment timeframes for new identity security solutions
Percentage of respondents not currently using the identity security solution

Source: Osterman Research (2025)

Almost 90% of organizations will do an initial deployment of previously unused identity security solutions over the next 12 months.

Roadmap for strengthening identity security

This section advocates a roadmap for strengthening identity security posture.

ENHANCE DETECTION OF MISUSED COMPROMISED CREDENTIALS

The use of valid but compromised credentials provides credential-appropriate access to systems and data to unauthorized people. Credentials can be compromised through a phishing attack, credential stuffing campaign, infostealer malware, purchase from a dark web forum, or a payment to an insider for the use of their credentials (e.g., as happened in Brazil in mid-2025 with a payment of $2,760 to a turncoat insider for credential use, which resulted in the theft of $140 million by the threat actors[12]). A mega breach containing 16 billion stolen credentials—more than double the world's internet users—was discovered in early 2025.[13]

76.2% of respondents say they are highly confident that their systems and processes could detect an attempt by a threat actor to use valid but compromised credentials for malicious purposes. This is up from 71.4% two years ago. This is anticipated to increase to 83.3% in two years' time, with the major relative change coming from those selecting "extremely confident" rather than "very confident."

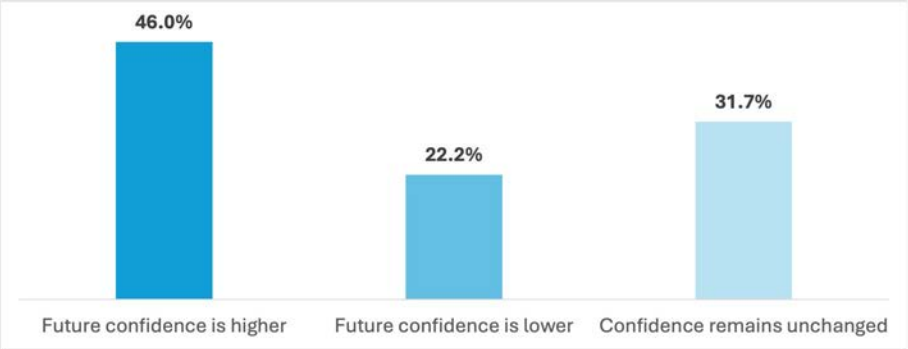
The achievement of elevated confidence is predicated on organizations embracing appropriate identity security technologies and driving towards a cohesive and mature deployment. Investing in the following technologies will be needed:

- Detection of compromised credentials on dark web forums for proactive autonomous remediation and reduction of the potential threat space. The real test is how quickly your monitoring system spots and neutralizes a leaked password.
- Stronger forms of MFA to eliminate the possibility of MFA bypass attacks.
- ITDR for detecting inappropriate credential use based on correlating underlying signals and behavioral abnormalities.

Detecting compromised credentials is necessary but insufficient; the real test is how quickly a leaked password is neutralized.

Figure 16 shows the patterns of change in confidence over the three time periods we asked about—two years ago, currently, and anticipated confidence in two years' time. With most organizations acknowledging the elevation of identity-driven threats, an anticipation of reduced or unchanged confidence should be a warning sign.

Figure 16
Confidence to detect the use of compromised credentials for malicious purposes
Percentage of respondents



Source: Osterman Research (2025)

STOP LATERAL MOVEMENT AND PRIVILEGE ESCALATION IN REAL-TIME

Lateral movement and privilege escalation are two of the malicious tricks in the threat actor playbook. Lateral movement occurs when additional systems or devices are compromised after the threat actor has gained an initial foothold in an environment. Privilege escalation occurs when elevated rights to systems, devices, and data are enabled for an identity beyond what was intended, appropriate, or reasonable. When driven by malicious actors, neither leads to positive outcomes for an organization.

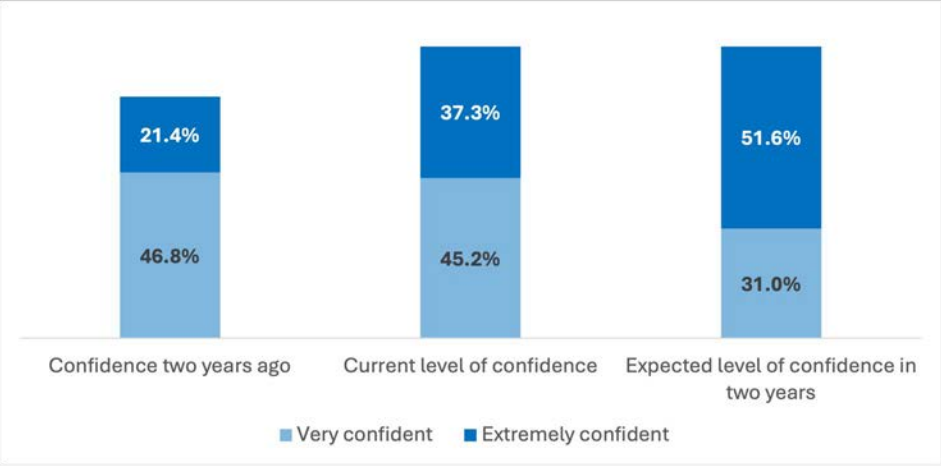
Both malicious tricks are addressed via a constellation of identity security capabilities working in concert, including:

- Detection of compromised credentials on dark web forums for proactive autonomous remediation and reduction of the potential threat space.
- Visibility into where identities are being used to access systems and data, combined with tracking of changing rights and privileges. Visibility and tracking enable baselining of the behaviors and actions associated with each identity, as input for detecting deviations driven by malicious activity, human error, and process error (e.g., deviant AI agents).
- Extending MFA processes to all access interfaces and authentication protocols across an Active Directory environment, including command line access tools like PsExec and PowerShell. These are tools of choice by threat actors for lateral movement. Inline authentication controls can determine if an authentication is legitimate or not, preemptively stopping suspicious authentications.
- Backup and recovery for identity platforms, for autonomous reversal of malicious, accidental, or unwarranted changes to identity attributes. Backup and historical recovery serve as both a diagnostic and corrective tool—restoring a known-good state after privilege escalation or lateral identity drift has occurred.

In this research, half of organizations believe their confidence for stopping lateral movement or privilege escalation will increase with better tooling. The major trend line is the growth in the “extremely confident” rating over the three time periods. See Figure 17.

Half of organizations believe their confidence for stopping lateral movement or privilege escalation will increase with better tooling.

Figure 17
Confidence to stop lateral movement or privilege escalation in real-time
Percentage of respondents



Source: Osterman Research (2025)

IMPROVE CAPABILITIES FOR RECOVERING FROM IDENTITY-RELATED ISSUES

One out of four organizations have the highest confidence that they could recover from the following identity-related issues:

- Malicious actors making unauthorized changes to identity configurations, e.g., Entra ID roles or groups
- Accidental deletion of identity policies or user access settings
- Compromise or misconfiguration of cloud identity platforms, e.g., Entra ID, Okta
- Failure of automated provisioning/deprovisioning pipelines

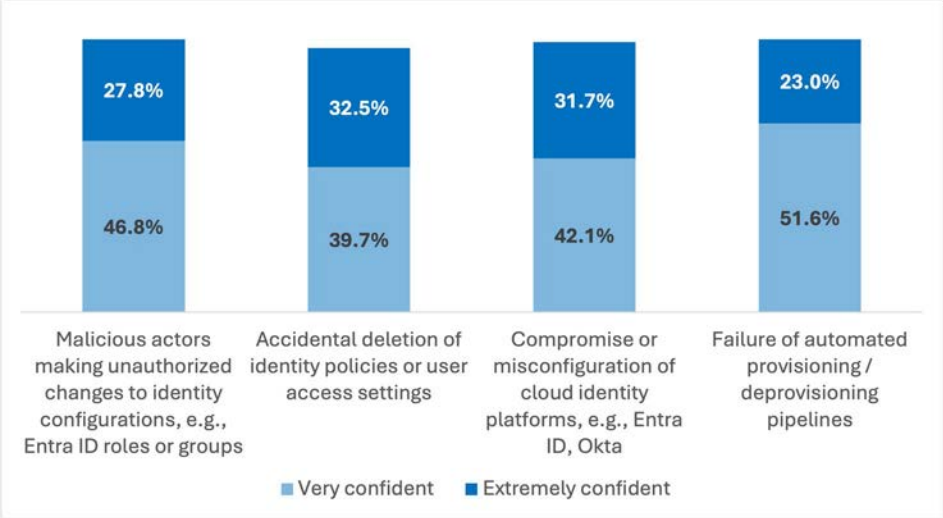
Confidence is not evenly spread within organizations on these issues, with most organizations not confident on how they would recover from 1.7 of the four issues.

Cloud identity platforms like Microsoft Entra ID are increasingly critical to daily operations—but they are not inherently resilient against misconfiguration or unauthorized changes. Without third-party backup solutions, changes to Entra roles, group memberships, or policies cannot be rolled back, leaving organizations exposed to prolonged outages, compliance failures, or privilege escalations. Implementing dedicated identity platform backup and restore solutions is an essential step towards a mature identity security strategy.

See Figure 18.

Implementing dedicated identity platform backup and restore solutions is an essential step towards a mature identity security strategy.

Figure 18
Confidence to recover from identity-related issues
Percentage of respondents



Source: Osterman Research (2025)

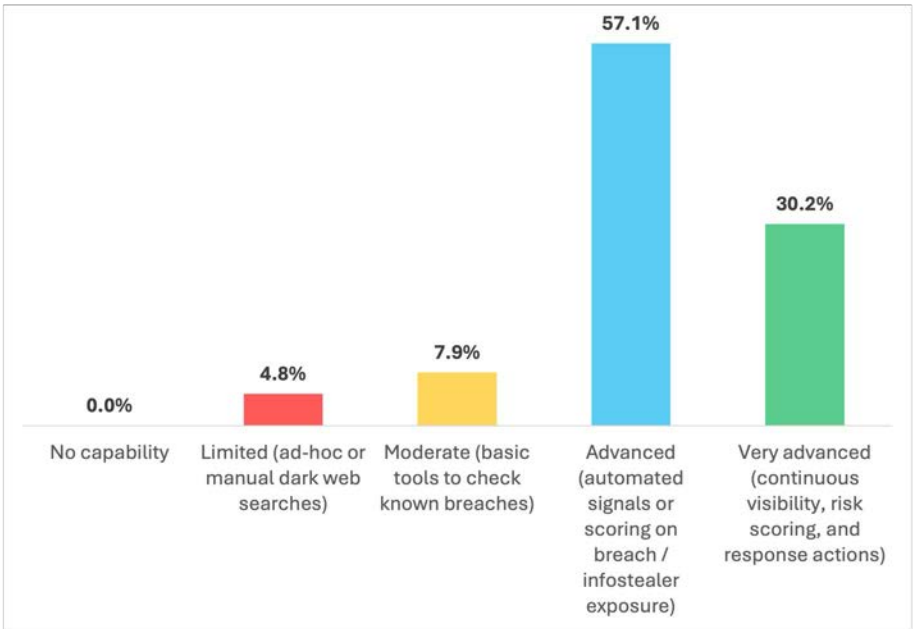
Only 6.3% of organizations say they have the highest confidence level in their ability to recover across all four of these issues, and an additional 25.4% are either "extremely confident" or "very confident" across all four. Most organizations claim strength to recover from two of the issues, but don't have the same confidence across all four.

CAPTURE IDENTITY SIGNALS TO ASSESS EXPOSURE RISK

Assessing the exposure risk of specific users or user groups based on compromised identity signals offers a quantitative assessment for early-stage interventions before a compromised identity can be leveraged to unleash havoc. If an organization has the optics to see the early signals of compromise and the process maturity to respond, the fastest and optimal response is an autonomous one. Depending on the circumstances—including which users or user groups are in the crosshairs—this action could be restricting the access scope of the identity, requiring the completion of elevated authentication requirements, or reverting unwarranted changes in an identity platform pending review.

For the organizations in this research, 30.2% say they have achieved this standard based on continuous visibility, risk scoring, and response actions. A much larger group of organizations in the research (57.1%) say they have the automated signals and scoring part, but lack the ability to respond autonomously. See Figure 19.

Figure 19
Assessing the exposure risk of specific users
Percentage of respondents



Source: Osterman Research (2025)

On cross-checking the answer to this question with the level of visibility each respondent indicated for a range of identity signals that would underlie such an analysis—see Figure 3 above—at best, the organizations claiming the "advanced" or "very advanced" levels in Figure 19 need to improve their visibility posture as a matter of first priority. All organizations in these two cohorts had a visibility level of less than 75% on average.

Organizations with the optics to see the early signals of compromise and the process maturity to respond autonomously are best placed to minimize identity-led threats.

ENRICH IDENTITY SECURITY DETECTIONS AND POLICIES

Driving toward elevated maturity in identity security detections and policies increases the likelihood of the early detection of malicious and abnormal identity signals. External threat intelligence and breach data feeds offer organizations a way of enriching internal assessment capabilities without having to do the heavy lifting alone. It enables organizations to see emergent threat signals that are already threatening others but haven't yet been targeted in their direction.

We asked respondents if they were relying on internal data only or were using one or more of the following external threat intelligence and breach data feed capabilities:

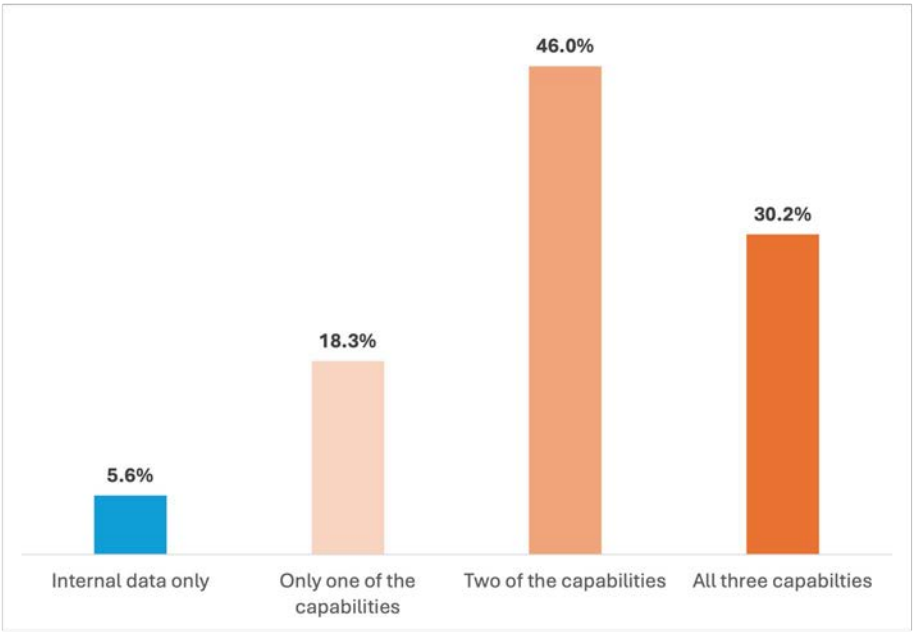
- External breach intelligence, e.g., dark web, infostealers, third-party compromise
- Correlation of external breach data with user accounts or identities
- Integration of external breach signals into automated identity policy enforcement

A small proportion of the organizations in this research rely on internal data only (5.6%). The vast majority are using one or more of the capabilities we asked about. As the capabilities are additive to identity security, not isolated and standalone, using all three offers the strongest approach. For external data sources, it is essential that they be updated frequently; ideally, a continuous feed enables the fastest remediation and helps prevent problems before they occur.

See Figure 20.

External threat intelligence and breach data feeds offer organizations a way of enriching internal assessment capabilities without having to do the heavy lifting alone.

Figure 20
Use of external threat intelligence or breach data feeds
Percentage of respondents



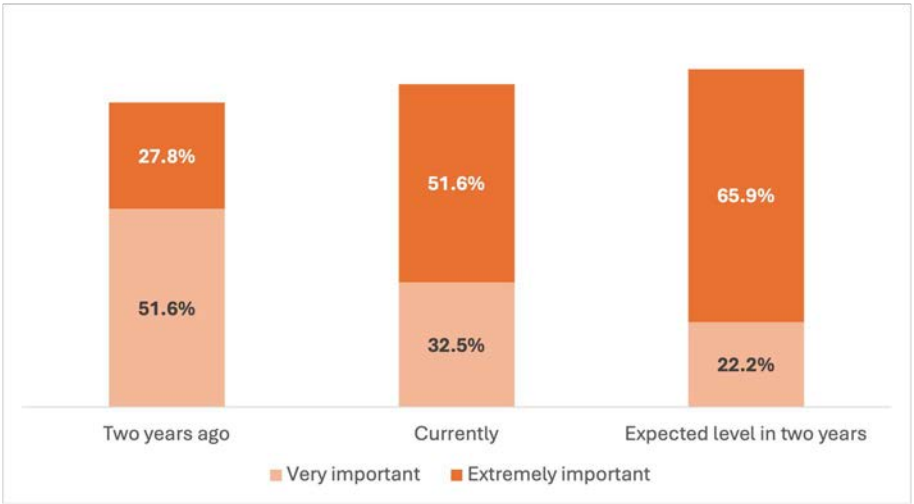
Source: Osterman Research (2025)

STRENGTHEN EXECUTIVE SUPPORT FOR IDENTITY SECURITY

Executives play a key role in validating the growing importance of securing identities and allocating budget and support for the investments required to lift an organization's identity security posture.

For the organizations in this research, the importance of identity security to their executives is surging. While there is a marginal increase in those selecting the two highest importance ratings from two years ago (79.4%) to the expected level in two years' time (88.1%), the intensity of the highest importance rating is the main story. This more than doubles in a surge from 27.8% to 65.9%, reflecting a growing sense at executive levels of the importance of safeguarding credentials and protecting identities as fundamental building blocks of cybersecurity. See Figure 21.

Figure 21
Importance of identity security to executives
Percentage of respondents



Source: Osterman Research (2025)

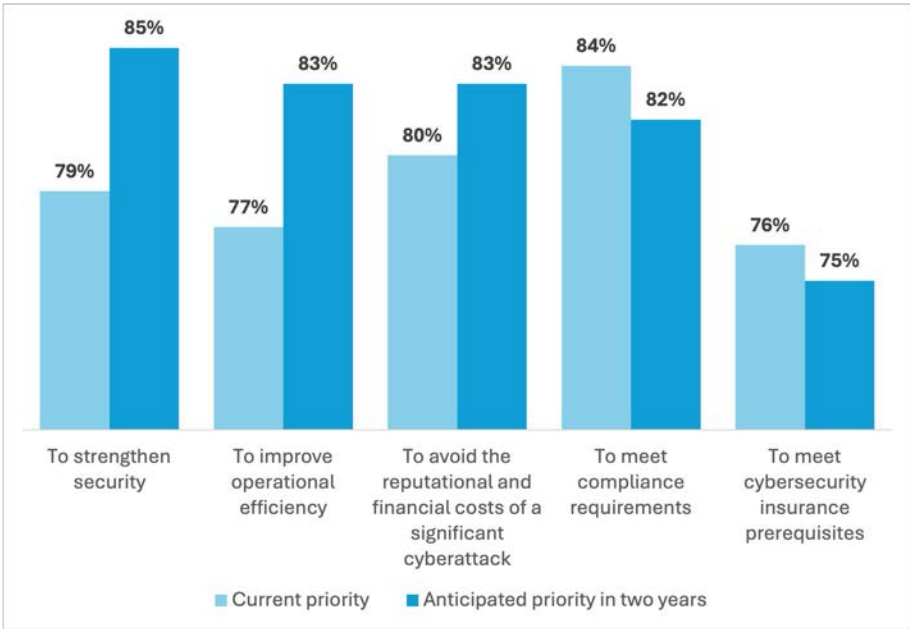
There is a growing sense at executive levels of the importance of safeguarding credentials and protecting identities as fundamental building blocks of cybersecurity.

REASONS FOR IMPROVING IDENTITY SECURITY

The surge in the importance of identity security to executives is aligned with a switch from a compliance-dominated perspective to a security-predicated one. Two compliance-first drivers are expected to decrease in importance over the next two years, while security and operational efficiency drivers increase. Compliance regulations are helpful in setting a minimum baseline standard across industry cohorts but are too often approached with a checkbox mentality. Even with MFA increasingly being required by compliance regulations and for cybersecurity insurance coverage, embracing a minimum-only approach will not succeed against threat actors following a do-anything, maximal-attack methodology.

See Figure 22.

Figure 22
Reasons why identity security is important to executives
Percentage of respondents



Source: Osterman Research (2025)

Conclusion

IAM is a necessary but insufficient technology to protect identities as threat actors weaponize compromised identities and their protections to unleash havoc on organizations. All organizations need to revisit their security posture for identities, ensuring the right technologies are deployed, processes are brought to maturity, and elevated protections operationalized.

Embracing a minimum-only approach to identity security will not succeed against threat actors following a do-anything, maximal-attack methodology.

Sponsored by Abnormal AI

Abnormal AI is the leading AI-native human behavior security platform, leveraging machine learning to stop sophisticated attacks and detect compromised accounts across email and connected applications. Our anomaly detection engine leverages identity and context to analyze normal behavior and assess the risk of every cloud email event—detecting and stopping sophisticated, socially-engineered attacks that target your organization's most valuable cybersecurity asset: your people.

You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the value of the platform instantly. Additional protection from Abnormal is available for Slack, Workday, ServiceNow, Zoom, and multiple other cloud applications. Abnormal is currently trusted by thousands of organizations, including more than 25% of the Fortune 500, as it continues to redefine how cybersecurity works in the age of AI.

Learn more at abnormal.ai.

abnormal.ai

@Abnormal_AI_Inc

LinkedIn: Abnormal AI

Methodology

This white paper is based on findings from a survey conducted by Osterman Research. One hundred twenty-six (126) respondents who have direct responsibility for planning, managing, and optimizing the identity security strategy at their organization were surveyed during June 2025. To qualify, respondents had to work at organizations with at least 500 employees. All surveys were conducted in the United States. The survey was cross-industry and no industries were excluded or restricted.

ORGANIZATION SIZE

500 to 999 employees	36.5%
1,000 to 5,000 employees	54.8%
More than 5,000 employees	8.7%

JOB ROLE

IAM manager, director or head	41.3%
CISO	25.4%
Identity infrastructure manager	17.5%
Cybersecurity manager	11.9%
Identity architect	3.2%
Security architect	0.8%

INDUSTRY

Agriculture, forestry or mining	0.8%
Computer hardware or computer software	7.1%
Data infrastructure or telecom	6.3%
Education	4.0%
Energy or utilities	1.6%
Financial services	8.7%
Government	7.9%
Healthcare	4.0%
Hospitality, food or leisure travel	3.2%
Industrials (manufacturing, construction, etc.)	11.1%
Information technology	13.5%
Life sciences or pharmaceuticals	7.9%
Media or creative industries	1.6%
Professional services (law, consulting, etc.)	9.5%
Public service or social service	0.8%
Retail or ecommerce	9.5%
Transport or logistics	2.4%

---

[1] Jose Antonio Lanz, How a Hacker Spent Only $2.7K to Steal $140 Million from Brazilian Banks, July 2025, at https://decrypt.co/328700/hacker-spent-2k-steal-140-million-brazil-central-bank

[2] Enzoic, Fortune 500 Employee-Linked Account Exposure: 2022 through 2024, January 2025, at https://resources.enzoic.com/fortune-500-report/

[3] Constella Intelligence, 2025 Identity Breach Report, July 2025, at https://constella.ai/2025-identity-breach-report/

[4] Mimecast, The State of Human Risk 2025, March 2025, at https://www.mimecast.com/resources/ebooks/state-of-human-risk-2025/

[5] CrowdStrike, CrowdStrike 2025 GlobalThreat Report, February 2025, at https://www.crowdstrike.com/en-us/global-threat-report/

[6] CrowdStrike, CrowdStrike 2025 GlobalThreat Report, February 2025, at https://www.crowdstrike.com/en-us/global-threat-report/

[7] Silverfort, Insecurity in the shadows: New data on the hidden risks of non-human identities, July 2025, at https://resources.silverfort.com/insecurity-in-the-shadows/home

[8] Verizon, Verizon's 2025 Data Breach Investigations Report: Alarming surge in cyberattacks through third-parties, April 2025, at https://www.verizon.com/about/news/2025-data-breach-investigations-report

[9] Abnormal AI, Inside Atlantis AIO: Credential Stuffing Across 140+ Platforms, March 2025, at https://abnormal.ai/blog/atlantis-aio-credential-stuffing-140-platforms

[10] Osterman Research, Safeguarding Identity Security: We Need to Talk about MFA, September 2024, at https://ostermanresearch.com/2024/09/04/orwp_0361/

[11] Osterman Research, Some thoughts on Hoxhunt's research on AI-powered phishing versus human-written phishing, May 2025, at https://ostermanresearch.com/2025/05/14/hoxhunt-phishing/

[12] Jose Antonio Lanz, How a Hacker Spent Only $2.7K to Steal $140 Million from Brazilian Banks, July 2025, at https://decrypt.co/328700/hacker-spent-2k-steal-140-million-brazil-central-bank

[13] Davey Winder, 16 Billion Apple, Facebook, Google And Other Passwords Leaked, June 2025, at https://www.forbes.com/sites/daveywinder/2025/06/20/16-billion-apple-facebook-google-passwords-leaked---change-yours-now/