Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **September 2023**
Commissioned by **Silverfort**

The State of the Identity Attack Surface: Insights into Critical Protection Gaps

Executive Summary

This survey discloses a critical gap in organizations' ability to protect themselves against identity threats—with 83% already having experienced a breach involving compromised credentials. Account takeover, lateral movement, and ransomware spread are a prominent cyber risk. To gain resiliency against these attacks, organizations strive to have the ability to prevent—in real time—malicious access with compromised credentials to their resources. **The common practice today is to lean on solutions such as MFA and PAM, as well as manual monitoring of service accounts**, to get this protection. **However, surveys of identity security teams reveal that in most cases, these solutions fail to deliver the required level of protection**. This failure manifests in the vast majority of organizations experiencing an identity-related data breach, as well as a shared notion among identity teams that they don't have the ability to thwart such attacks in the future.

KEY TAKEAWAYS

The key takeaways from this research are:

- **Over 80% of organizations have experienced an identity-related breach that involved the use of compromised credentials**
  Almost half of organizations experienced such a breach in the past 12 months.

- **65.4% of organizations have not implemented MFA comprehensively enough to provide sound protection**
  Organizations are not protecting their entire workforce with MFA, and only one in eight have more than 70% of their resources and access methods covered.

- **Only 5.7% of organizations have full visibility into their service accounts**
  Very few organizations have full visibility into the activity and usage of their service accounts, while 62% only have partial visibility.

- **Protection of service accounts introduces a huge challenge to organizations with only 22% able to prevent adversaries from using them for malicious access**
  78% of organizations cannot prevent the misuse of service accounts in real time, since security is sporadic or missing.

- **73.4% of organizations struggle with getting their PAM solutions fully onboarded and working**
  Many organizations have encountered difficulties in their PAM implementation, causing progress to halt. Most know what to do but are too resource-constrained to move ahead.

- **Only one in five organizations are highly confident that they could prevent identity threats**
  Very few organizations are confident they can stop initial access or lateral movement due to the malicious use of compromised credentials.

Protection on the identity attack surface is alarmingly insufficient, with very few organizations possessing real-time protection against the use of compromised credentials.

ABOUT THIS WHITE PAPER

The survey and white paper were commissioned by Silverfort. Information about Silverfort and details on the survey methodology are provided at the end of the paper.

Introducing the identity attack surface and its protection measures

The identity attack surface includes all the organizational resources that are accessed with user credentials. Attacks that target it use compromised credentials to gain malicious access to these resources—prominent examples of which are account takeover, lateral movement, and internal ransomware spread. Hence, **the protection of this attack surface manifests in the ability to detect and prevent such access in real time**.

The key challenge in achieving this type of protection is that these attacks use legitimate credentials with malicious intent. In order to prevent them, one must have the ability to identify when valid credentials are used in a malicious context and respond with blocking the access attempt altogether.

To be effective, this protection should apply to all types of user accounts—standard users, administrators with high privilege access, and machine-to-machine service accounts. In a similar manner, it should also cover all on-premises and cloud resources and access methods.

The prominent security solutions that aim to deliver real-time protection against this type of malicious access are MFA and PAM. While these are most often applied to standard user and administrator accounts, service accounts are typically excluded from MFA and are only partially subject to PAM protection.

Identity threats use compromised credentials for malicious access to targeted resources.

RESEARCH GOAL

The purpose of this research is to examine the manner, scope, and effectiveness in which these protections are implemented. To do that, we surveyed identity security practitioners with four groups of questions:

1. MFA coverage across users and resources
2. PAM onboarding and coverage
3. Visibility and protection of service accounts
4. Overall resilience level against identity threats

FOUR-LEVEL MATURITY MODEL

For each group of questions, we've aggregated respondents' answers and created a four-level maturity model:

- **Level 1. Chaotic**
  The organization has acquired technology solutions to fortify the identity attack surface, but usage and application of these solutions are informal or ad-hoc. Usage reflects an "add-on" mentality, where new tools and processes for identity security are added to existing solutions and organizational approaches.

- **Level 2. Opportunistic**
  The opportunistic level represents the initial steps into a disciplined approach to identity security, with a greater attempt made to extend current approaches to repel identity attacks. Usage across the workforce and resources remains unevenly distributed.

- **Level 3. Identified and defined**
  At this level, organizations recognize which solutions are required to confront identity threats, as well as the subsequent implementation of tools and processes. However, these are not fully implemented for various reasons, leaving some unaddressed gaps in the protection they deliver.

- **Level 4. Disciplined and implemented**
  Organizations at this highest level are optimizing their processes, people, and solutions to protect the identity attack surface. While organizations at level four are not immune to identity breach, both the likelihood and the fallout are low.

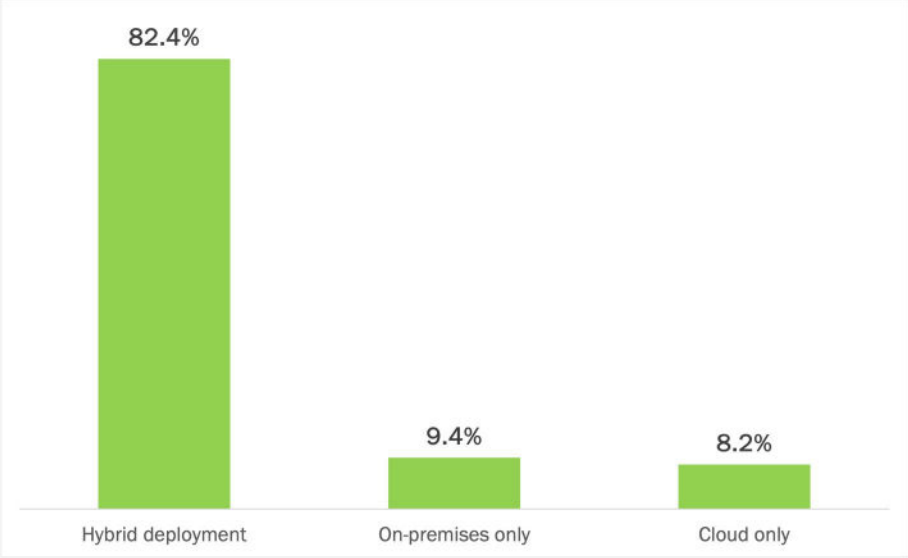
ON-PREMISES IDENTITY INFRASTRUCTURE IS STILL THE COMMON PRACTICE

More than a decade into the shift to the cloud, most organizations are still deploying an on-premises identity infrastructure. This means **identity weaknesses and attack methods that target the on-premises environment are still a core part of the cyberthreat landscape**.

Most organizations in this research operate a hybrid identity deployment (82.4%), combining an on-premises directory (e.g., Microsoft Active Directory or alternatives such as Oracle Directory Server) with either a cloud identity provider (e.g., Okta or Microsoft Entra (formerly Azure AD)) or an identity federation server (e.g., Microsoft AD FS or Ping Federate). Some use on-premises infrastructure only (9.4%), and the rest (8.2%) are cloud only, with no on-premises identity infrastructure to manage. See Figure 1.

Most organizations still maintain an on-premises identity infrastructure, making protection against identity threats targeting the on-premises environment a must-have.

Figure 1
Identity Infrastructure Distribution: On-Premises, Hybrid and Cloud Only
Percentage of respondents



Source: Osterman Research (2023)

Protecting the Identity Attack Surface

Security solutions that protect the identity attack surface greatly reduce the likelihood of a successful attack. These solutions work in real time to stop attacks that use compromised credentials. In this section, we look at the solutions available and assess how organizations are putting these to work.

MATURITY OF MULTI-FACTOR AUTHENTICATION (MFA)

MFA significantly decreases the likelihood of success of a credential compromise attack because it demands additional identity verification and assurance before granting access to the requested account or resource. It has become a near-universal recommendation for improving identity security and is increasingly an essential security control incorporated into cyber insurance assessments.

It matters how and where MFA is used. Having MFA available within the environment but not in widespread usage by the workforce decreases the scope of security. The contribution of MFA to identity security is undermined when:

- **MFA is not practiced by the entire workforce**
  When MFA is not used by people in the workforce who are targeted by identity threats, credentials alone are enough to gain access to the requested account or resource.

- **MFA is not applied on all resources and access methods**
  When MFA does not protect the full scope of resources and access methods under attack, the elevated security promised by MFA is diminished as adversaries can still access resources without the MFA barrier. Moreover, when a resource has MFA applied to one access method but lacks MFA on another, the MFA protection is void since an adversary will simply use the unprotected method to access the resource.

Full MFA coverage of all users, resources, and access methods is imperative, as any gap opens a path for malicious access.

How Organizations Are Using MFA

In assessing how organizations are using MFA to reduce the identity attack surface, we looked at two security controls.

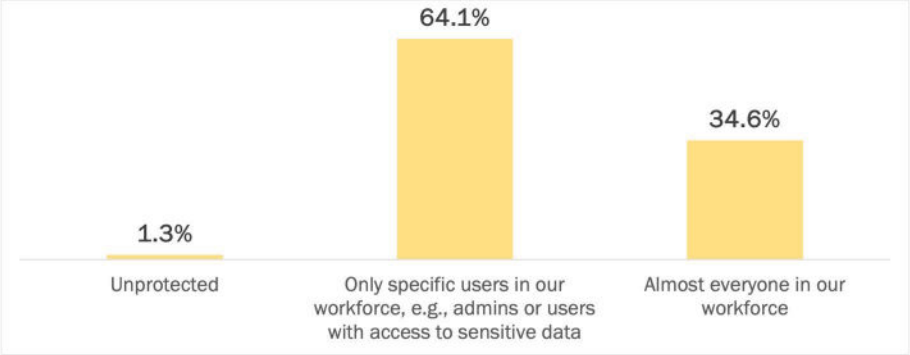
The proportion of the workforce protected by MFA

How widely is MFA applied to the workforce? The three options we queried were none, specific users in the workforce (e.g., administrators or users with access to sensitive data), and almost everyone.

In this research, **34.6% of organizations are protecting almost everyone in the workforce with MFA, and 64.1% are protecting only specific users**. While attackers seek to compromise administrators with privileged access for lateral movement, standard users can be useful targets, too. Attackers follow a playbook of privilege escalation, discovering permission misconfigurations or looking for loose access policies to grant users excessive access rights beyond what they need for their job role.

See Figure 2.

Figure 2
Proportion of Workforce Protected by MFA
Percentage of respondents



Source: Osterman Research (2023)

Critical resources and access methods

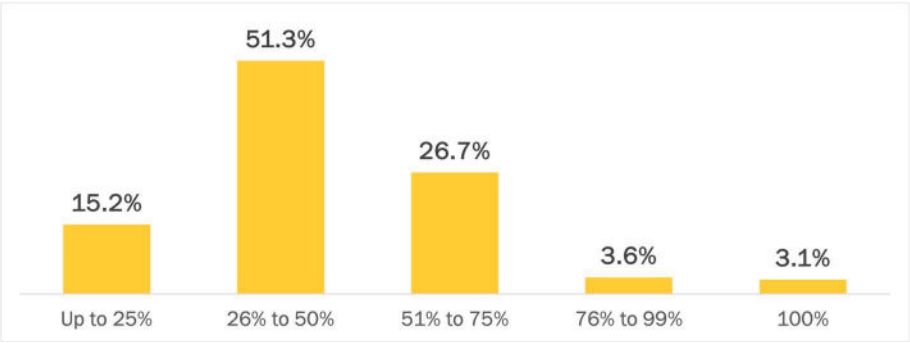
We assessed the share of resources and access methods protected by MFA. The options were none, partial, and all, as well as don't know and not applicable. Listed alphabetically, the resources and access methods we asked about were:

- Command line remote access, e.g., PowerShell, PsExec
- Desktop login, e.g., Windows, Mac
- Homegrown and legacy apps
- IT infrastructure, especially management consoles
- Operational technology (OT) systems
- Remote Desktop Protocol (RDP)
- Secure Shell or Secure Socket Shell (SSH)
- Shared network drives
- Virtual Desktop Infrastructure (VDI)
- Virtual Private Network (VPN) and other remote connection methods
- Virtualization platforms and hypervisors, e.g., VMware, Citrix

Only 34.6% of organizations have MFA protection in place for the majority of their workforce, including both admin and standard users.

Most respondents fully protect less than half of their applicable resources and access methods (66.5%). See Figure 3.

Figure 3
Proportion of Applicable Resources and Access Methods Protected by MFA
Percentage of respondents



Source: Osterman Research (2023)

Assessing the Maturity of MFA

To assess the maturity of how organizations are using MFA to reduce the identity attack surface, we correlated how respondents answered these two questions. We divided the answers into our four maturity levels (see Figure 4):

- **Disciplined and implemented (7%)**
  Requires that the organization is protecting almost everyone in the workforce by MFA, and that at least 60% of the applicable 11 resources and access methods are strongly protected by MFA. To achieve this level, at least one of two essential items must be strongly protected by MFA: an access method (command line remote access) and/or a resource (homegrown and legacy apps). Only 7% of organizations met these requirements.

- **Identified and defined (30%)**
  Requires that the organization is protecting either everyone in the workforce or specific users only. This level relaxes the resources and access methods requirement, so that at least 40% of the applicable 11 resources and access methods are strongly protected. Three in ten organizations met these requirements.

- **Opportunistic (36%)**
  Includes organizations that provide only partial workforce coverage via MFA, lack strong protections for either of the two essential items, and provide only partial coverage for most resources and access methods. Just over one third of organizations met these requirements.

- **Chaotic (26%)**
  Respondents that failed to meet the requirements of the three levels above. This encompasses 26% of the organizations we surveyed.

Only 7% of organizations have reached the required level of discipline in how they use MFA to protect their users from compromise.

Figure 4
Identity Security Maturity: MFA
Percentage of respondents

Source: Osterman Research (2023)

MATURITY OF PRIVILEGED ACCOUNT MANAGEMENT (PAM)

PAM strengthens identity security by enforcing elevated access controls over privileged accounts. System administrators and other IT personnel have highly privileged access to the systems under their control—and rightly so, as this enables them to carry out their duties within the system. However, the existence of highly privileged accounts creates an identity security risk for the organization, due to the potential impact for compromise and malicious use by attackers.

PAM solutions enforce greater scrutiny and protection over accounts with highly privileged access rights. For instance, system administrators' credentials are stored in a protected vault and are subject to continuous password rotation, which places stronger barriers against credential compromise attempts. PAM solutions also record the actions taken by an administrator in each session for enhanced monitoring, behavioral baselining, and anomaly detection.

How Organizations Are Using PAM

We assessed how organizations are using PAM by looking at their deployment status with a PAM solution and two security controls.

Where organizations are in their PAM journey

While most organizations are investing in PAM, few are fully deployed with all privileged accounts onboarded and protected. Most are still in the process of working toward full deployment, and many of these are struggling to overcome deployment challenges. See Figure 5, where 14% of organizations have not yet started deploying PAM and 10.2% are fully deployed, leaving the overwhelming majority somewhere between these two extremes.

Only 10.2% of organizations have their PAM solutions fully deployed and onboarded.

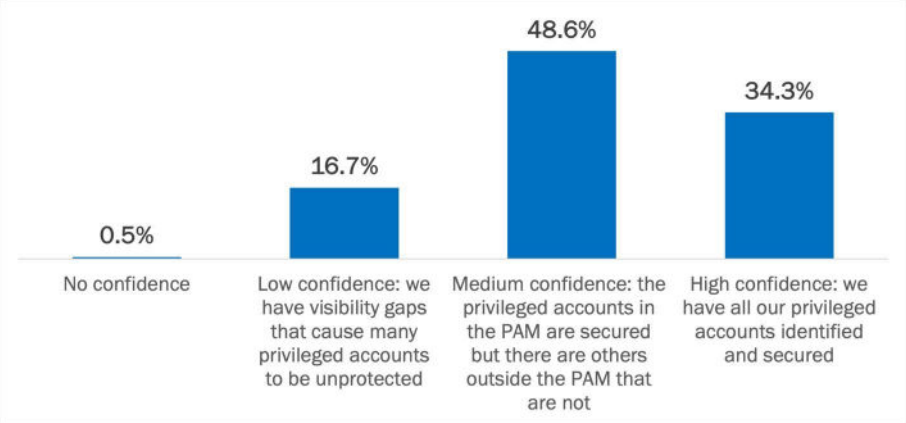
Figure 5
Current Status of the PAM Journey
Percentage of respondents

Source: Osterman Research (2023)

Confidence to prevent attackers from using compromised privileged user accounts for malicious access

One ultimate test of the efficacy of a PAM solution is high confidence to prevent misuse of privileged user credentials. We asked respondents to indicate their level of confidence. Per Figure 6, 34.3% of respondents indicate their organization is at the high confidence level—which means all privileged accounts have been identified and secured.

Figure 6
Confidence to Prevent Malicious Use of Privileged Credentials by Attackers
Percentage of respondents

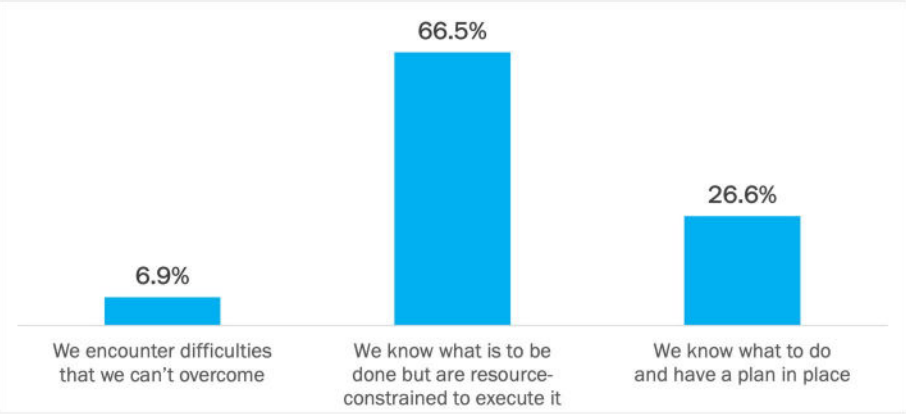


Source: Osterman Research (2023)

Approach to overcoming implementation difficulties

The deployment process for any major security system comes with its fair share of difficulties. Unresolved implementation difficulties hamper the security protections available from PAM, irrespective of whether those difficulties stem from a lack of knowledge of the solution or lack of resources to complete the deployment. We asked respondents to indicate how they are overcoming the difficulties experienced during the implementation of PAM. See Figure 7.

Figure 7
Approach to Overcoming PAM Implementation Difficulties
Percentage of respondents



Source: Osterman Research (2023)

73% of organizations lack either the knowledge or resources to resolve PAM implementation difficulties.

Assessing the Maturity of PAM

To assess the maturity of how organizations are using PAM to strengthen identity security, we correlated how respondents answered the three questions above. We divided the answers into our four maturity levels (see Figure 8):

- **Disciplined and implemented (7%)**
  Organizations at this highest level have fully deployed a PAM solution, which means they have onboarded and protected all privileged accounts. They also indicate they have high confidence in their ability to prevent malicious use of privileged credentials by attackers and have an operational plan for addressing any outstanding implementation difficulties.

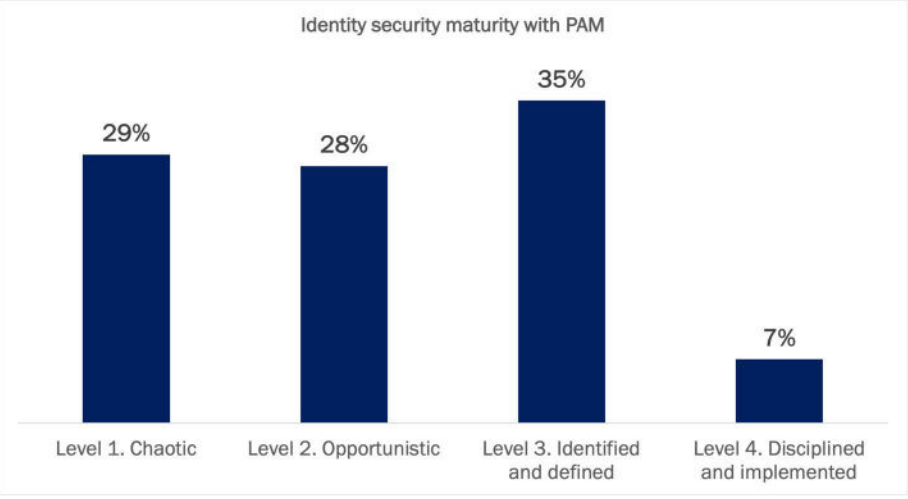
- **Identified and defined (35%)**
  At this level, organizations are working toward but have not yet attained a fully deployed PAM solution. They have a medium or high level of confidence in their ability to prevent malicious use of privileged credentials. These organizations either have a plan for resolving outstanding implementation difficulties or know what to do but are resource-constrained to get there. While they have not achieved the highest maturity level, they are making solid progress by identifying and defining the requisite processes.

- **Opportunistic (28%)**
  Organizations at the opportunistic level have taken tentative first steps into the use of PAM, but have not completed the deployment process and have only medium or lower confidence in their ability to prevent misuse of privileged accounts.

- **Chaotic (29%)**
  Respondents that failed to meet the requirements of the three maturity levels above. This encompasses 29% of the organizations in this research.

Only 7% of organizations have fully deployed PAM and have high confidence in its ability to prevent malicious use of privileged credentials.

Figure 8
Identity Security Maturity: PAM
Percentage of respondents



Source: Osterman Research (2023)

MATURITY OF PROTECTING SERVICE ACCCOUNTS

MFA and PAM are widely recognized as security controls for protecting the account credentials of people—the standard users and administrators with highly privileged access in the workforce. However, service accounts that are used for machine-to-machine access are just as prevalent. **In this section, we look at how organizations are protecting against the compromise of service accounts for malicious access**.

The Challenge of Service Accounts in Identity Security

Service accounts can be compromised just like any other user account within the environment. There are three characteristics that make service accounts an especially lucrative target for attackers:

- **Low to zero visibility**
  No IT tools deliver out-of-the-box filtering and visibility capabilities for service accounts, so unless strict documentation is practiced, there is no easy way to tell how many service accounts exist in an organization.

- **High access privileges**
  Service accounts are created for machine-to-machine access. They have higher access privileges than standard user accounts—making them of high interest to attackers.

- **Lack of MFA protection**
  Since service accounts are for machines, not humans, they are excluded from MFA protection. They cannot be questioned or asked to verify their identities in any manner, so a critical identity protection layer is missing.

- **Difficulties in protecting with PAM**
  Passwords for service accounts cannot easily be rotated in a PAM vault as happens for privileged human accounts. This is because the scripts that run service accounts can't be automatically synced with the PAM's password rotation. As a result, password change due to rotation would cause service account logins to fail, disrupting the communication processes they execute and causing outages and errors in business processes.

The aggregated impact of unmonitored, highly privileged accounts that cannot be protected by MFA and are hard to include in PAM turns service accounts into an ideal compromise target for performing lateral movement.

Limited visibility, high access privilege, lack of MFA, and several PAM protection challenges make service accounts the ultimate compromise goal for attackers.

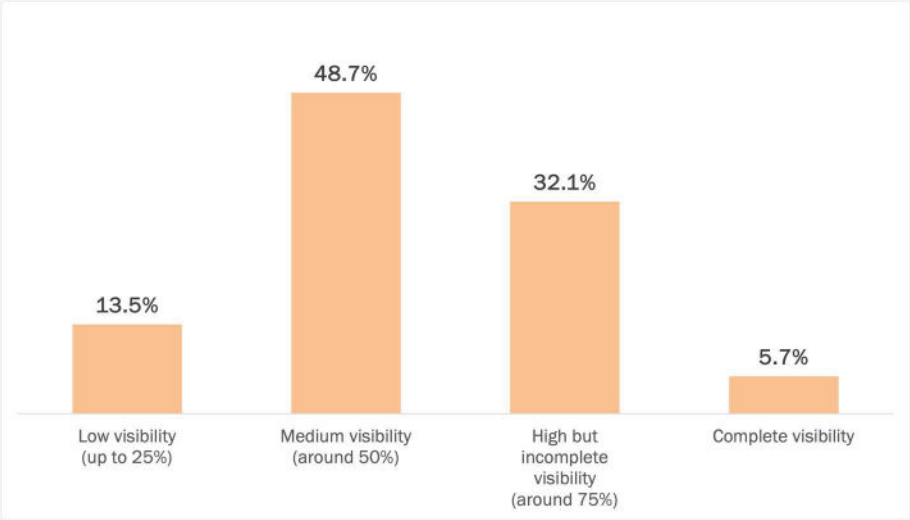
How are Organizations Protecting Service Accounts

In assessing how organizations are protecting the service accounts used across their environment, we looked at three security controls.

Visibility of service accounts

The ability to know what service accounts exist is a foundational security control. Visibility enables the use of subsequent security controls to protect the organization from misuse of service accounts and, as these are put in place, the mandate to ensure they are achieving desired protections. See Figure 9, where only 5.7% of organizations have complete visibility into all service accounts in their environment, with a further 32.1% having high but incomplete visibility.

Figure 9
Level of Visibility into Service Accounts
Percentage of respondents



Source: Osterman Research (2023)

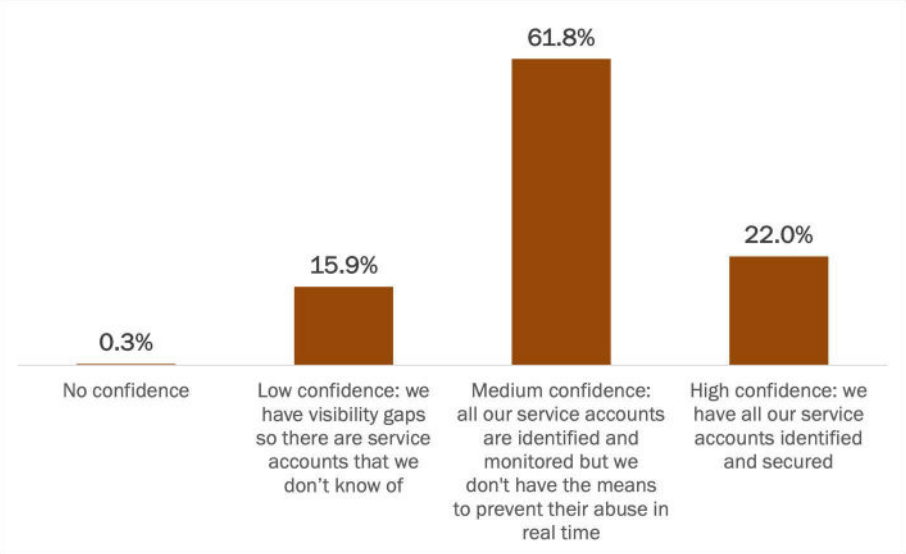
Only 5.7% of organizations have complete visibility into all service accounts in their environment.

Confidence in the ability to prevent attackers from misusing service accounts

One ultimate test of the efficacy of how an organization is managing its service accounts is its level of confidence to prevent misuse of service accounts by an attacker. High confidence requires strong security management practices and mature change processes. We asked respondents to assess their confidence in the overall efficacy of their security management processes for service accounts.

See Figure 10, where 22% of respondents have high confidence that they can prevent misuse by attackers since all service accounts have been identified and secured. Most respondents (61.8%) have only medium confidence, meaning that while their service accounts have been identified and are being monitored, the ability to enact real-time controls is missing, unreliable, or not yet operational.

Figure 10
Confidence to Prevent Malicious Access of Service Accounts by Attackers
Percentage of respondents



Source: Osterman Research (2023)

Confidence in the ability to manage service accounts

Managing service accounts encompasses several interrelated processes:

- **Discovering service accounts**
  Discovering which service accounts exist in the environment.

- **Activity mapping of service accounts**
  Gaining insight into the activity and usage of service accounts. This includes reports on source and destination machines and the processes and apps managed by service accounts.

- **Securing service accounts**
  Enforcing secure access controls to alert or prevent access if a service account is suspected of being compromised.

- **Elevating service accounts' security with password rotation**
  Automating password rotation for service accounts elevates password security through a regular change cadence. This means service account passwords are not static and are therefore less vulnerable to password compromise.

We asked respondents to indicate their confidence level in managing these processes. **Fewer than three in ten respondents are extremely confident in their organization's ability to manage any of these aspects of service accounts**.

78% of organizations aren't confident in their ability to block malicious access that's carried out with a compromised service account.

Assessing the Maturity of Service Accounts

To assess the maturity of how organizations are dealing with the service accounts in their environment, we correlated how respondents answered the three questions above. We divided the answers across four maturity levels (see Figure 11):

- **Disciplined and implemented (9%)**
  The first requirement for the highest maturity level is that the organization has high or full and complete visibility into all machine-to-machine service accounts in their environment. Secondly, they must be extremely confident in their ability to manage two or more of the aspects associated with service accounts and have high confidence in their ability to prevent attackers from using service accounts for malicious access. Just under one in ten organizations meet these three requirements for service accounts.

- **Identified and defined (25%)**
  The requirement of having high or full and complete visibility into service accounts remains consistent at this level, however the other two requirements are somewhat less intensive. Firstly, confidence to manage the aspects of service accounts now encompasses organizations that are "moderately confident," and the confidence to prevent misuse by attackers includes the medium confidence level. One in four organizations meet these requirements.

- **Opportunistic (53%)**
  Includes organizations that have less than high or full and complete visibility into their service accounts, and those that do not have high confidence in their ability to prevent misuse of service accounts by attackers. In terms of managing the four aspects of service accounts, organizations required an average of "somewhat confident" in their ability to do so. Just over one half of organizations are at the opportunistic maturity level.

- **Chaotic (13%)**
  Respondents that failed to meet the requirements of the three levels above. This encompasses one in eight of the organizations we surveyed.

Only 9% of organizations have protection at the disciplined and implemented maturity level for their service accounts.

Figure 11
Identity Security Maturity: Service Accounts
Percentage of respondents

Source: Osterman Research (2023)

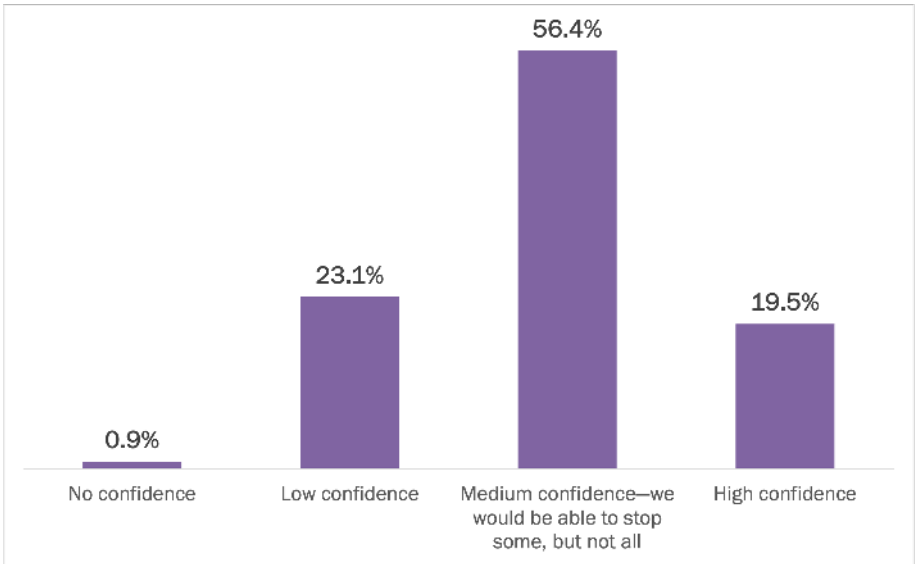
CONFIDENCE IN RESILIENCE AGAINST IDENTITY THREATS

The synergistic contribution of identity security solutions that have been well-implemented should result in high confidence in the ability to stop the misuse of compromised credentials. We assessed the validity of this assertion by investigating confidence across four key dimensions.

Preventing Initial Access

Compromised credentials are prominently used by attackers as a beachhead into a targeted environment. We asked respondents to indicate their overall confidence level in stopping an attacker from gaining such initial access to their environment. This confidence should be influenced by the identity security solutions the organization has deployed and the processes it has developed. See Figure 12, where the majority have medium (56.4%) or lower (24.0%) confidence.

Figure 12
Confidence to Stop the Use of Compromised Credentials: Initial Access
Percentage of respondents



Source: Osterman Research (2023)

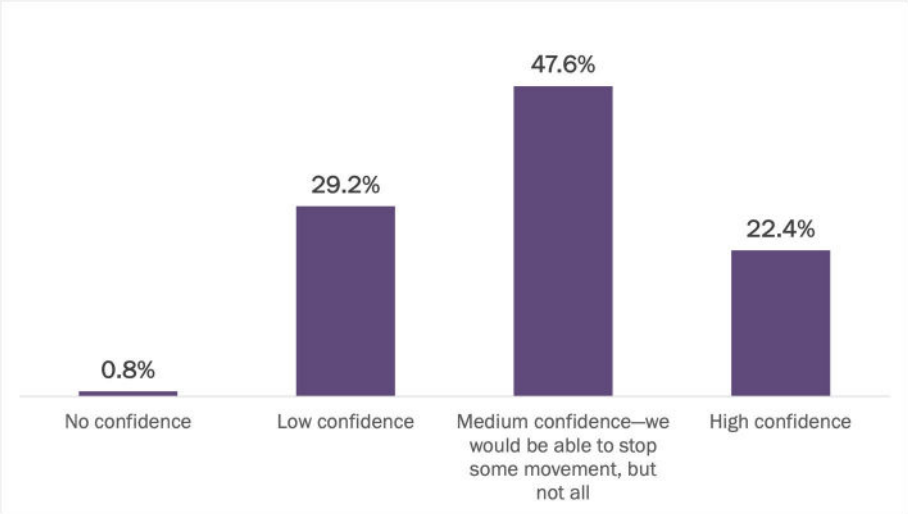
80.5% of organizations have low to partial confidence in their ability to block malicious access with compromised credentials.

Stopping Lateral Movement

Another prominent use case for compromised credentials is to move laterally within an environment after initial access has been gained—regardless of how initial access was achieved, e.g., via compromised credentials, malware, or exploitation. In the course of this lateral movement, attackers try to access as many reources as needed to fulfill the objective of their attack. This can include attempting to compromise additional user identities to gain access to new resources that were inaccessible using the original credentials, as well as administrative credentials with elevated access rights beyond those associated with the original credentials.

We asked respondents to indicate their confidence level in stopping lateral movement by an attacker. See Figure 13, where most have medium (47.6%) or lower (30.6%) levels of confidence.

Figure 13
Confidence to Stop the Use of Compromised Credentials: Lateral Movement
Percentage of respondents



Source: Osterman Research (2023)

Only 22.4% of organizations are confident they can stop lateral movement with compromised credentials in their environments.

Preventing Malicious Access to Critical Resources

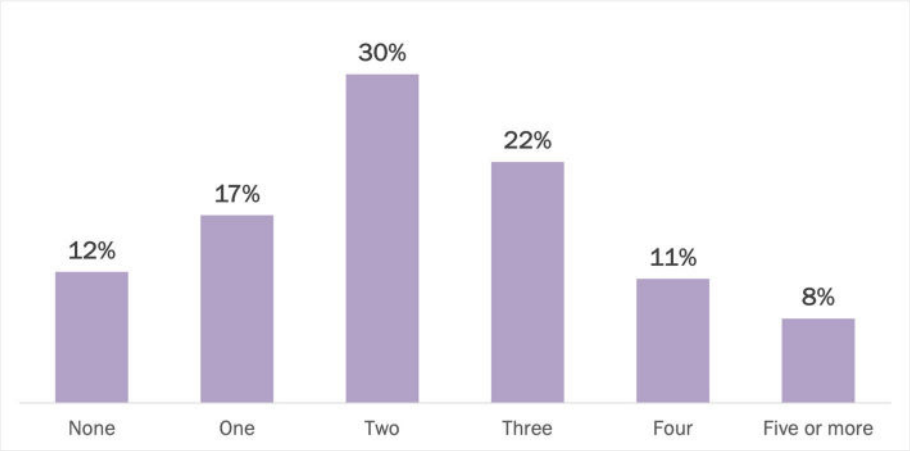
If an attacker can get into an organization's IT environment, they will attempt to access as many resources as possible—for purposes including data exfiltration, installing backdoors to enable persistent access, or spreading ransomware in preparation for detonating an attack. We asked respondents to indicate their confidence in preventing malicious access to the following eight resource types once an attacker was inside their environment (listed alphabetically):

- IT infrastructure, especially management consoles
- Legacy on-premises applications
- Operational technology (OT) systems
- Shared network drives
- Workstations and servers via command line, such as PsExec, PowerShell, and Windows Management Instrumentation
- Workstations and servers via remote desktop protocol (RDP)
- Virtual Desktop Infrastructure (VDI)
- Virtualization platforms and hypervisors, e.g., VMware, Citrix

See Figure 14, where most respondents are confident in their ability to protect two of the eight resources (30%). Only one in twelve had the highest level of confidence in their ability to prevent malicious access against five or more of the eight resources.

Only 8% of organizations have high confidence in their ability to protect five or more of their critical resource types.

Figure 14
Confidence to Prevent Malicious Access to Resources
Percentage of respondents indicating high confidence



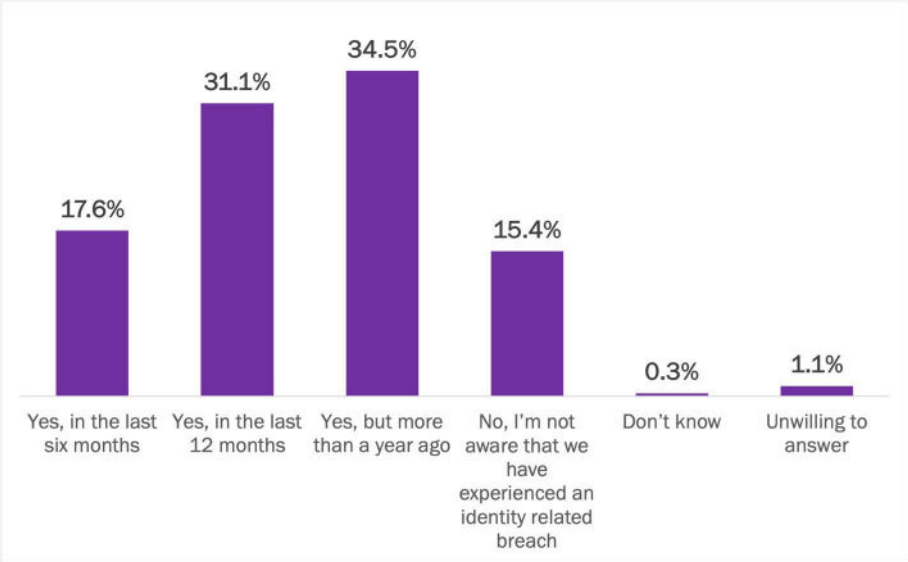
Source: Osterman Research (2023)

Avoiding Identity-Related Security Breaches

The fourth and final area for assessing resilience against identity threats is whether the organization has experienced an identity-related security breach in the recent past. We asked respondents to say if compromised credentials had been used for malicious access to their resources, and if so, when this happened last.

See Figure 15, where 17.6% of respondents acknowledge an identity-related breach in the previous six months, and a further 31.1% in the six-to-12-month timeframe. One in six respondents were not aware of any identity-related breaches, didn't know, or were unwilling to answer the question.

Figure 15
Identity-Related Security Breaches
Percentage of respondents



Source: Osterman Research (2023)

It is important to note that Figure 15 profiles the occurrence of identity-related breaches, not identity-related incidents. The two are different:

- **Identity-related breach**
  When compromised credentials are used to gain access to a resource, resulting in a breach of access, confidential data, lateral movement, or the spread of ransomware. Of all maturity assessment activity, an actual breach provides the strongest identity security posture warning signal for an organization—albeit a costly and disruptive one.
- **Identity-related incident**
  Attempted attacks which the organization successfully defended against. Incidents represent regular infraction attempts that offer proof of maturity at identifying, disrupting, and preventing such activity.

83% of organizations have experienced a known data breach that involved the use of compromised credentials.

Assessing Confidence Level Against Identity Threats

To assess organizational maturity against identity threats, we correlated the answers to the four questions above. See Figure 16:

- **Disciplined and implemented (6%)**
  The highest maturity level requires high confidence in stopping both initial access and lateral movement, and the highest level of confidence in preventing malicious access to six or more of the eight resources we asked about. It also requires that the organization has not experienced an identity-related security breach in the previous 12 months. Only 6% of organizations meet these four requirements.

- **Identified and defined (26%)**
  This level softens the requirement for the highest levels of confidence for the first three areas of analysis, encompassing medium confidence for both stopping initial access and lateral movement, and requiring only moderate confidence for at least half of the eight resources. It holds constant, however, the requirement that the organization has not experienced an identity-related security breach in the previous 12 months. One quarter of organizations meet these requirements.

- **Opportunistic (41%)**
  Organizations at the opportunistic level have low maturity against identity threats, characterized by low or medium confidence to stop either initial access or lateral movement, as well as mid-range confidence in preventing access to half of the resources. These organizations have suffered an identity-related security breach, albeit not in the previous six months. Two in five organizations in this research were unable to meet the requirements of the two higher maturity levels.

- **Chaotic (27%)**
  Respondents that failed to meet the requirements of the three maturity levels above. This encompasses one in four of the organizations we surveyed.

Only 6% of organizations meet the requirements for the disciplined and implemented level of maturity for identity threats.

Figure 16
Identity Security Maturity: Against Identity Threats
Percentage of respondents

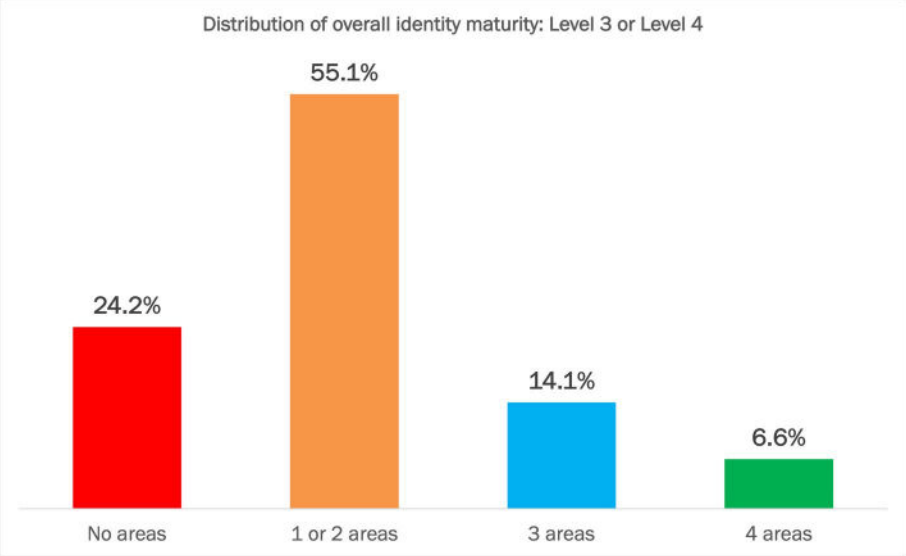
Source: Osterman Research (2023)

Assessing Identity Security Resilience

We have examined the maturity of organizations across four areas of identity security: MFA, PAM, service accounts, and confidence in resilience against identity threats. To assess the combined profile of maturity across these four areas, we looked at the distribution of organizations for the two highest levels—level 3 (identified and defined) and level 4 (disciplined and implemented). We counted how many organizations achieved either level 3 or level 4 across our areas of analysis.

See Figure 17, where 24.2% of organizations did not achieve either of these maturity levels in any of the four areas, 55.1% achieved it in one or two of the areas, 14.1% in three, and the remaining 6.6% achieved it in all four areas. Most organizations evidence the higher maturity levels in one or two areas, while few have achieved it in three or more areas.

Figure 17
Identity Security Maturity: Distribution of Level 3 and Level 4 Maturity Levels
Percentage of respondents



Source: Osterman Research (2023)

Most organizations are alarmingly vulnerable to account takeover, lateral movement, and the spread of ransomware.

What this means is that most organizations remain alarmingly vulnerable to account takeover, lateral movement, and the spread of ransomware. Few organizations can identify and prevent identity attacks across all areas of assessment in real time. Most organizations cannot defend against an attacker with legitimate credentials—the malicious request will be authenticated, the resource accessed by an unauthorized adversary, and the attack will spread without interruption.

Conclusion

This research was conducted to gain insight into the identity attack surface's actual security posture. Its main value to the individual reader is the clear methodology it provides to answer a simple question: *How resilient is the environment I am accountable for against malicious activity that employs compromised credentials?*

The results fundamentally undermine the assumption that the mere existence of MFA and PAM in an environment is enough to protect the entire identity attack surface. Rather, security stakeholders should take the following questions and direct them internally:

- What is the scope of MFA coverage?
- What level of visibility into service accounts and their activities do you have?
- What is the state of your PAM journey?
- Are you confident that you could stop an attacker from gaining initial access or lateral movement?

Identity threats are a core cyber risk. Understanding the current state of an environment's identity attack surface is an essential first step in securing it.

About Silverfort

Silverfort is the leader in Identity Threat Protection, enabling secure authentication and access in a unified manner across all corporate resources, both on-premises and in the cloud, to detect and stop identity-based attacks including account takeover and ransomware spread. Using patented technology, Silverfort enforces its protection as a layer on top of the customer's existing IAM infrastructure, without requiring modifications to endpoints, servers or applications—a capability which is unmatched in the market. This includes resources that couldn't be protected before, such as legacy applications, command-line interfaces, industrial systems, machine-to-machine access and more. Its platform enables Identity Threat Detection and Response (ITDR), agentless Multi-Factor Authentication (MFA), discovery and protection of service accounts (non-human identities), and adaptive Zero Trust security policies. Silverfort is trusted by hundreds of enterprise customers around the world, including Fortune 100 companies, and received dozens of other industry awards.

For more information, visit www.silverfort.com.

www.silverfort.com

@silverfort

+972 77 202 4900

+1 202 688 3098

Methodology

This white paper was commissioned by Silverfort and conducted by Osterman Research. Six hundred thirty-seven (637) respondents in identity roles were surveyed during May-June 2023. To qualify, respondents had to work at organizations with at least 1,000 employees. The surveys were conducted in six countries, with the surveys in France and Germany fielded in French and German respectively. The survey was cross-industry, and no industries were excluded or restricted.

JOB ROLE

Identity architect	33.8%
Identity infrastructure manager	31.7%
IAM manager, director, or head	34.5%

ORGANIZATION SIZE

1,000 to 2,499 employees	69.1%
2,500 to 4,999 employees	21.2%
5,000 or more employees	9.7%

GEOGRAPHY

United States	50.7%
Germany	14.9%
France	11.9%
United Kingdom	11.5%
Australia	9.1%
Singapore	1.9%

INDUSTRY

Hospitality, Food, Leisure Travel	16%
Retail, eCommerce	11%
Healthcare	11%
Industrials (Manufacturing, Construction, etc.)	8%
Professional Services (Law, Consulting, etc.)	8%
Computer Hardware, Computer Software	7%
Financial Services	6%
Education	6%
Transport, Logistics	5%
Energy, Utilities	5%
Life Sciences	5%
Data Infrastructure, Telecom	4%
Public Service, Social Service	3%
Media, Creative Industries	3%
Agriculture, Forestry, Mining	0.8%
Construction	0.3%
Non-Profit	0.2%