Advancing Privileged Access Management (PAM) to Address Modern Business Requirements

By Steve Brasen

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Research Report Summary
December 2020

Sponsored by:

Bravura Security, Inc.

Advancing Privileged Access Management (PAM) to Address Modern Business Requirements

Table of Contents

Advancing Privileged Access Management (PAM) to Address Modern Business Requirements

Executive Summary

Security breaches of privileged accounts can be catastrophic to any business by allowing bad actors unfettered access to the company's most sensitive data and IT systems. Related vulnerabilities have accelerated in recent years due to increased IT infrastructure complexities and broad distribution of business-critical services. To assist organizations with identifying the most effective methods for managing privileged access, EMA conducted primary, survey-based research into the real-world requirements, challenges, and management techniques employed for securing privileged access. Key findings from the research include:

- On average, roughly 19% of business users (non-administrators) have been granted privileged access to enterprise data, apps, and servers
- 54% of organizations have granted privileged access on business systems to users who are not direct employees of the company
- 80% of organizations discovered that a privileged access policy violation had occurred within the preceding 12 months
- 87% of businesses that experienced a policy violation in the preceding 12 months reported significant impacts to business operations as a consequence
- One out of five businesses that suffered a policy breach experience serious impacts to overall business performance, including a direct loss of revenue, a loss of customers, and/or damage to the company's reputation
- 87% of survey respondents indicated that shared privileged accounts were in use in their organization
- Organizations that adopted a PAM solution that specifically defines which business services or devices receive privileged access for each user were determined to be 33% less likely to have experienced a privileged access policy breach
- Businesses that lacked automation capabilities for auditing privileged access were seven times more likely to experience a privileged access policy violation than organizations with that capability
- 97% of survey respondents reported that their organization maintains at least some standing privileged accounts
- Among survey respondents, 28% reported that they maintained rarely used standing privileged accounts, while 69% noted the existence of never-used accounts
- Reported incidents of privileged access policy violations were 44% less frequent among organizations with policies that define the length of time privileged access is authorized
- Organizations that lacked the ability to automatically expire privileged access when it is no longer required (such as with "just in time" access capabilities) were three times more likely to report privileged access policy violations
- 88% of survey respondents reported that their organization grants employees local privileged administrator rights to their personal desktop or laptop
- Organizations that allow users privileged access to their endpoint devices were determined to be 34% more likely to report privileged credentials were compromised

The Necessity of Managing Privileged Access

It is an unfortunate fact of IT security that no system is entirely unbreachable. Even the most hardened computing environment enforcing the most comprehensive security protocols must enable human actors to access stored information and perform administrative tasks. At some point, every IT system must be updated, patched, configured, and analyzed. The very existence of these access points inherently brings with it significant vulnerabilities. In the majority of cases, however, the most sensitive system components require elevated privileges to access. Typically (although not always), dedicated IT administrators are specifically authorized and granted enhanced privileges to perform IT management tasks. Similarly, some stored information, such as financial records and company secrets, may only be accessible by high-level business personnel specifically authorized to access such information.

Traditional methods for enabling privileged access evolved from an expansion of common password management practices that have been the hallmark of security since the earliest days of computing. Unfortunately, techniques such as enforcing the use of strong password strings (i.e., using a complex mix of alphabetic, numeric, and special characters) and requiring periodic password resets have proven to be woefully ineffective on their own. Such approaches failed to address the fact that human brains are not equipped to memorize numerous complex strings that are constantly changing, and most users will bypass security best practices by using the same privileged password for multiple accounts or sharing privileged passwords with their peers. Additionally, hackers and other bad actors have become rather adept at finding ways to bypass traditional password-based controls, such as by utilizing cracking software, engaging in phishing attacks, employing keyloggers and spyware, or performing brute-force attacks.

Unfortunately, techniques such as enforcing the use of strong password strings and requiring periodic password resets have proven to be woefully ineffective on their own.

While the use of poor user authentication processes will create significant vulnerabilities with typical user accounts, they are catastrophic when employed with privileged accounts. By their very nature, privileged accounts are completely unrestricted, so anyone able to gain access to a privileged account can perform any task and open any file. In many cases, privileged access granted to one system may enable the performance of privileged tasks on another system, so breaches could spread throughout the business IT environment.

It should also be noted that the dangers of employing weak security for protecting privileged accounts is not just limited to preventing attacks from malicious attackers. Employees who have been granted privileged access may also misuse their authorization to perform tasks that could disrupt business operations. For instance, they may change operating system parameters, install software, or otherwise make unapproved changes to key system components that could crash or decrease the performance of applications and servers. Additionally, privileged users may intentionally or inadvertently delete critical data or share sensitive files with unauthorized individuals. Since traditional methods for managing privileged accounts do not record activities, privileged users are not held accountable for their actions.

Practices supporting privileged access management (PAM) were developed to ensure the responsible delegation and governance over privileged accounts and services. Key components of a PAM strategy include:

- Identification of privileged access users and accounts
- Authorization and approval processes for granting privileged access
- Restriction of activities that can be performed with privileged access
- Limitation of duration of privileged access
- Recording, alarming, and auditing of privileged access use

While most organizations recognize the importance and value of adopting PAM practices, adopted approaches vary widely. Certainly, PAM requirements are dependent on business use cases. Organizations managing more sensitive data and more stringent compliance attainment goals will need more effective methods for monitoring and controlling privileged access. However, even in less security-conscious environments, a lack of effective PAM controls can be disastrous to business operations. Finding the right balance of adopted PAM solutions necessitates an understanding of the different processes and technologies, how effective they are at meeting security goals, and the impact they will have on business productivity.

```
server sshd[8016]: Failed password for root
server sshd[8189]: Failed password for root
sshd[8189]: last message repeated 2 times
server sshd[8194]: Failed password for root
server sshd[8194]: Failed password for root
server sshd[8304]: Failed password for root
sshd[8304]: last message repeated 2 times
server sshd[8309]: Failed password for root
server sshd[8309]: Failed password for root
server sshd[8547]: Failed password for root
server sshd[8553]: Failed password
```

Research and Methodology

To assist organizations with making strategic decisions on the PAM approaches and management platforms that will most effectively ensure the security of their most sensitive accounts and IT resources, Enterprise Management Associates (EMA) conducted primary research evaluating real-world enterprise experiences on the requirements, challenges, and management techniques employed for securing privileged access. The intent was to evaluate outcomes and experiences between the different approaches in order to quantify which provide the greatest value in reducing risks and improving management efficiencies in today's demanding and dynamic IT environments.

For the research, EMA surveyed 160 IT professionals knowledgeable about PAM practices and how they are employed in their organization. All respondents were located in North America and distributed across a wide range of industry types and sizes to enable visibility into requirements and experiences by market segment. All respondents were carefully vetted to ensure they were knowledgeable about the topic and use of IAM solutions in their organizations. Eighty-four percent of respondents were from IT departments, of which 76% held a senior-level position, including IT manager, IT director, IT security director, CISO, CTO, or CIO.

Business Usage of Privileged Access

Enterprise requirements for monitoring and securing privileged access to business IT resources vary greatly depending on individual organizational goals and supported environments. The identification of optimal PAM practices relies on understanding key business requirements so adopted solutions can be aligned appropriately. Even across businesses recognizing a near-identical set of requirements, the priority of introducing specific PAM capabilities will radically differ depending on the emphasis each organization places on specific goals. For instance, some businesses may target solutions that are specifically designed to reduce management efforts over those that provider greater security improvements or increased cost-effectiveness.

In any identification of an appropriate PAM solution to adopt, an initial determination should be made on the scope of IT support the approach will require. At a basic level, this can be determined by identifying the number of users that will be managed by an adopted solution. It can generally be presumed that all IT administrators will be authorized with privileged access. After all, how else can they be expected to perform their primary job function? While this represents a relatively small portion of a typical business's workforce, the scale of privileged access usage substantially increases when including non-administrators who are not directly responsible for managing IT systems. According to EMA survey results, on average, 18.67% of regular users have been granted privileged access to business servers, applications, and data. To be clear, this just includes support for enterprise hosting environments and does not including users who have been granted privileged access to endpoint devices, such as personal PCs (a topic covered later in this document). Among survey respondents, 98% indicated that at least some non-administrators were granted privileged access to business systems in their organization. Roughly one third of respondents indicated privilege access was granted to greater than 25% of their workforce.

The percentage of business users granted privileged access remains relatively consistent across business sizes (Figure 1). This indicates particularly worrisome conditions for large enterprises. For instance, a large business with 10,000 employees is likely to have granted, on average, almost 1,800 users with privileged access. Clearly, the greater the use of privileged access, the more likely organizations will face incidents of abuse and misuse and the more challenging the environment will be to monitor and secure.

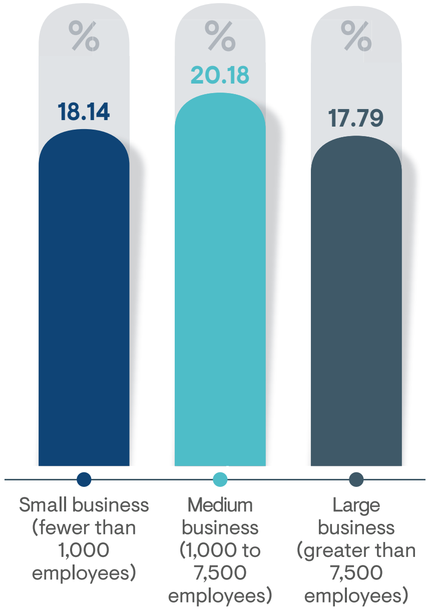

Figure 1: Average percentage of users (i.e., non-administrators) in respondent's organization who have been granted privileged access to business servers, applications, and data by organization size

The types of supported users granted privileged access will also impact the security requirements of an organization (Figure 2). Unsurprisingly, IT administrators were noted as the most likely users of privileged accounts. However, in about one-third of cases, IT administration was reported to be performed exclusively by or in conjunction with external managed service providers (MSP). Database administrators (DBAs) were noted as the non-systems-administrator business role most likely to have been granted privileged access. Typically, DBAs require privileges in order to configure system parameters in order to optimize database performance and perform other routine tasks, such as backups, updates, and storage management. Similarly, software developers often require privileged access to change system settings in order to resolve conflicts and performance issues with the applications they are developing.

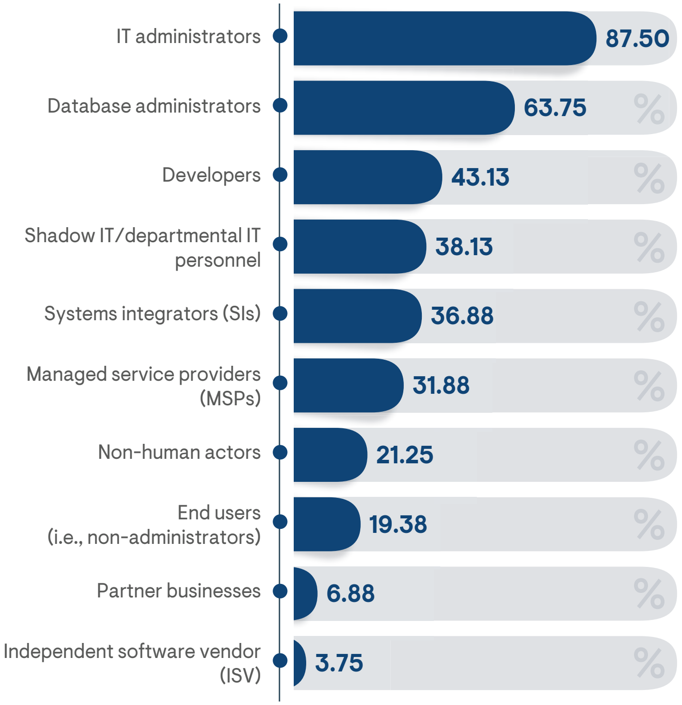

Figure 2: Percentage of survey respondents indicating the types of users granted privileged access in their organization

The percentage of users granted privileged access is, again, fairly consistent across business sizes, with only a few easily accountable exceptions. DBAs are almost twice as likely to be granted privileged access in large businesses as in small businesses (71% to 42%, respectively), which is consistent with the distribution of database deployments. MSPs are somewhat more frequently empowered with privileged access in small businesses than with large businesses (40% to 30%, respectively), exemplifying the increased reliance on managed services by smaller businesses. The granting of privileged access to non-human actors—including applications, IT services, and IoT devices—was almost nonexistent in small businesses but indicated to be in use by 34% of large businesses.

While it can be expected that IT administrators will utilize their elevated privileges fairly regularly as part of their primary job function, usage by non-administrators varies greatly between businesses. Across all users in all organizations, an authorized non-administrator can be expected to employ privileged access 280 times each year. More than one-third of all non-administrators utilize their privileged access multiple times per day, and 25% employ their privileged access only once per month or less frequently. An argument can easily be made that users who do not require privileged access less than once per month should not be granted privileges at all because they can easily request that privileged activities be performed by IT administrators without significant disruption to business productivity.

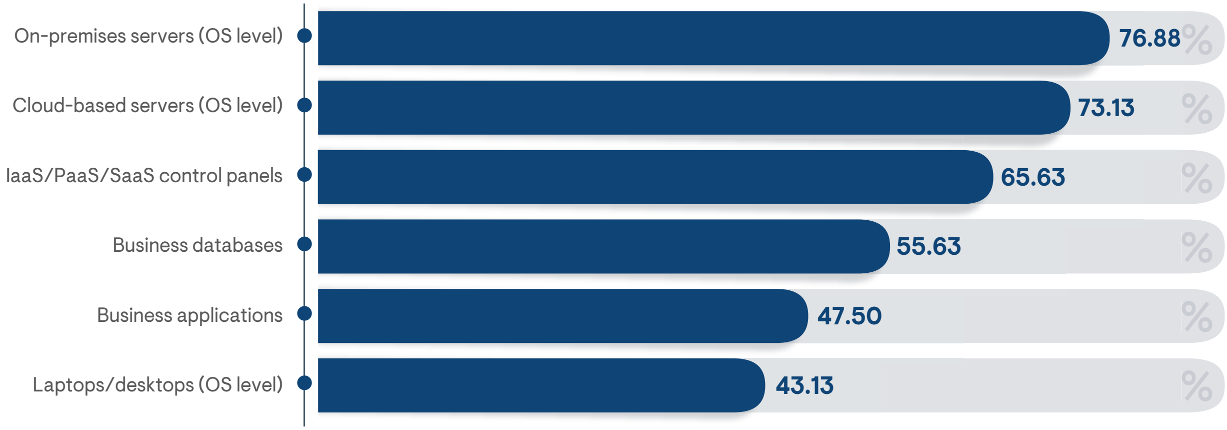
On-premises servers (OS level)
76.88%
Cloud-based servers (OS level)
73.13%
IaaS/PaaS/SaaS control panels
65.63%
Business databases
55.63%
Business applications
47.50%
Laptops/desktops (OS level)
43.13%

Figure 3: Percentage of respondents indicating on which resources their organization manages privileged access

For many organizations, the scope of PAM is not limited to the number of supported users and frequency of use, but also includes the diversity of managed resources. While almost 77% of total respondents indicated their organization manages privileged access to on-premises servers, nearly the same amount noted support for cloud-hosted servers (Figure 3). Among small businesses (with less than 1,000 employees), PAM processes were reported to be employed more frequently to support cloud-hosted servers than on-premises servers (86% and 74% of respondents, respectively). This is emblematic of the somewhat increased reliance on cloud services by small businesses in comparison to medium and large businesses.

PAM platforms are principally being introduced to support server environments rather than end-user workstations, as indicated by the relatively low (43%) of respondents who noted PAM support was extended to endpoints. In the majority of organizations, endpoint device administrator accounts and end-user privileges are either maintained by the users themselves or set using basic operating system or domain control settings. Respondents from healthcare and manufacturing institutions were the least likely to note PAM support for endpoints (25% and 28% of respondents, respectively), while professional services businesses were indicated to provide the broadest endpoint device support, as noted by 70% of related respondents.

Challenges to Securing Privileged Access

Unfortunately, currently adopted security practices and solutions are, in general, insufficient to fully secure privileged access use. Based on the survey results, 80% of organizations are indicated to have experienced a privileged access policy violation within the previous year (Figure 4), and these numbers only reflect known policy breaches. The true results are likely somewhat higher, since many organizations lack the monitoring tools necessary to identify all violations. Among respondents who were able to detect breach events, the most frequently noted was the discovery of active privileged accounts for former employees or contractors. It is often the case that IT administrators are unaware of all the privileged accounts to which users were granted at the time of their termination. These unrecognized accounts may remain available and active indefinitely, making them prime targets for bad actors seeking clandestine methods for attaining privileged credentials. These types of breaches were more broadly noted by respondents from large businesses (37%) than small businesses (25%), likely due to the higher density of employee turnover rates apparent in larger organization sizes. More than half (55%) of all respondents from organizations utilizing a free or low-cost password vault as their primary method of controlling privileged access reported incidents of discovered privileged accounts for former users in the last year, indicating it to be the least effective method for enabling privileged account visibility.

Among 23% of survey respondents, incidents of users employing the same password for multiple privileged accounts were also detected over the preceding year. In these instances, an attacker who has managed to attain a password (such as by brute force, phishing, or cracking tools attacks) on one business system would be able to utilize it to gain access to

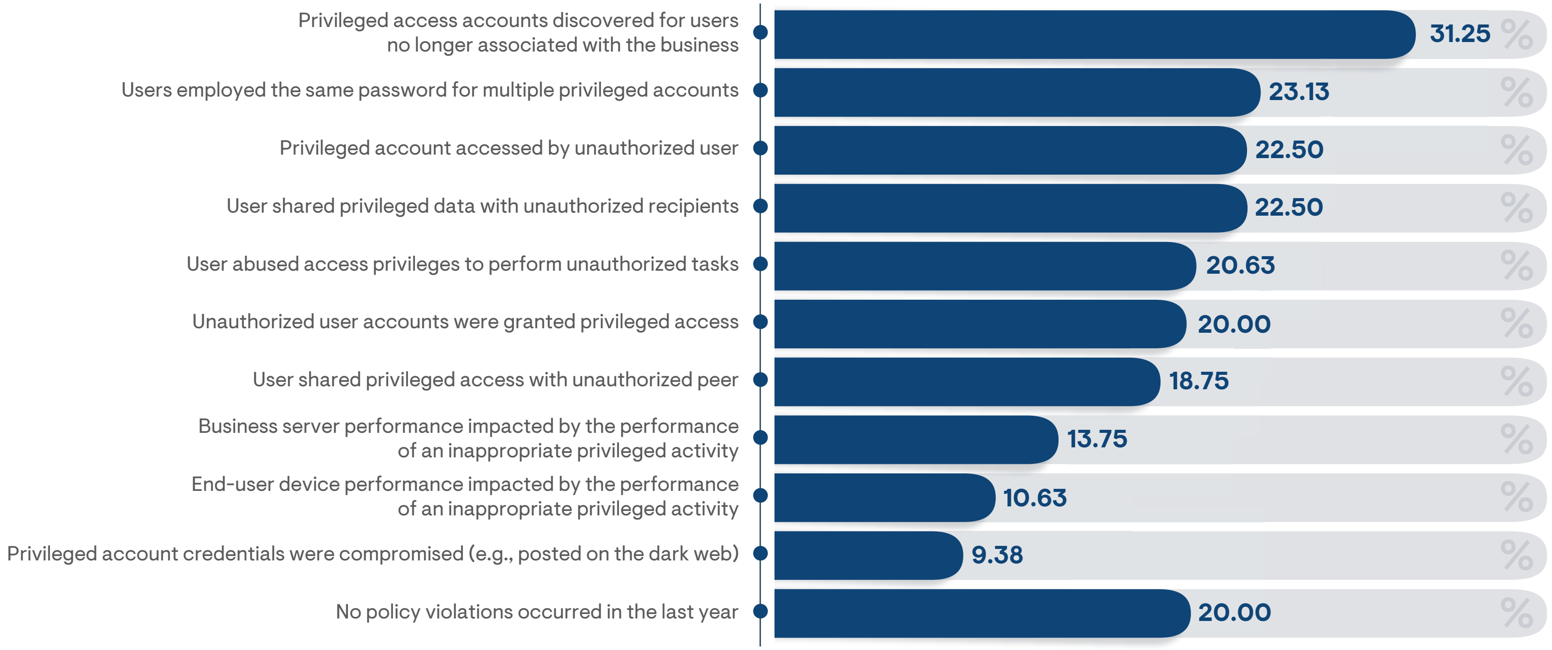

Figure 4: Percentage of respondents indicating privileged access policy violations that had occurred in their organization over the preceding year

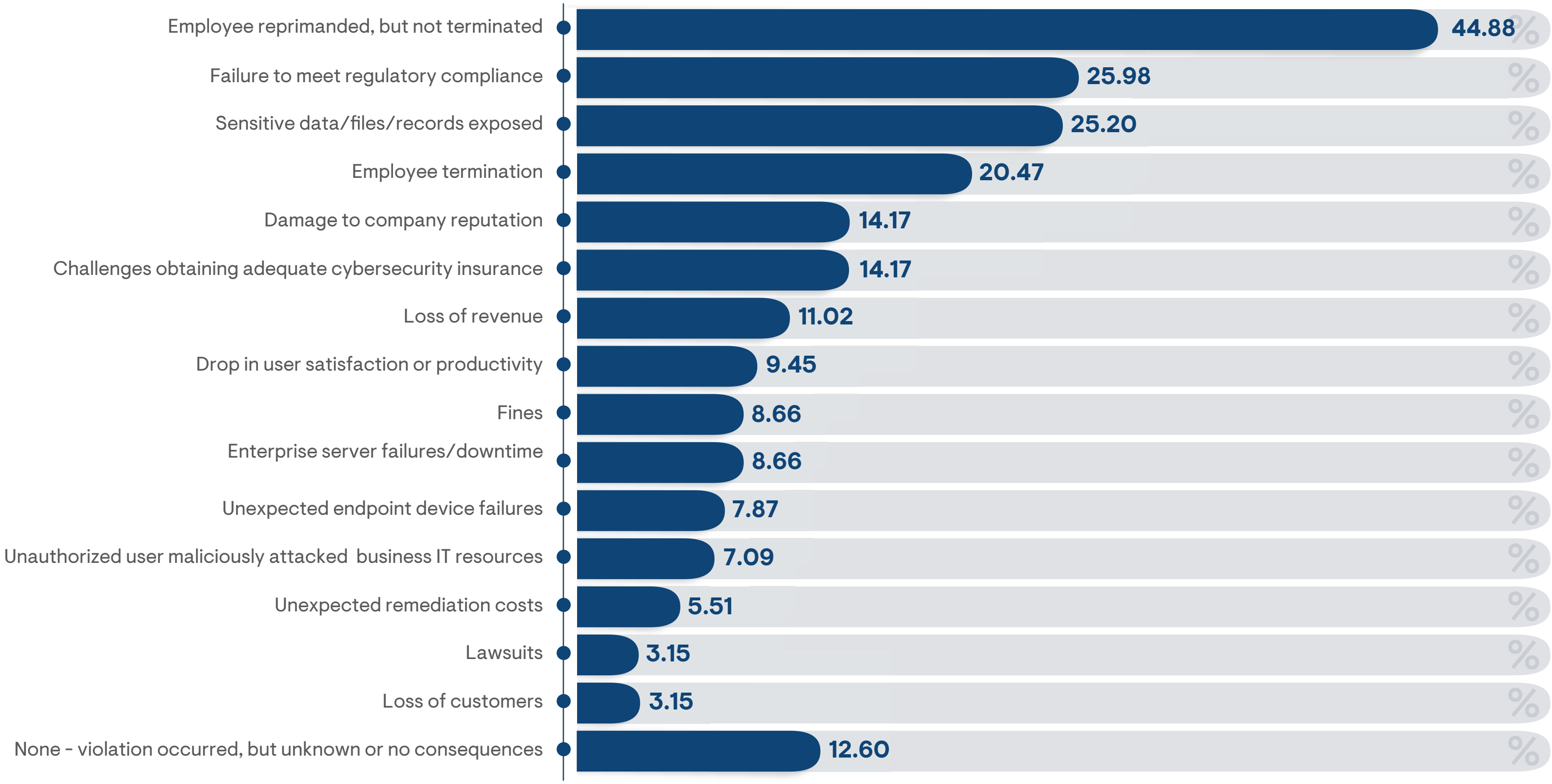
Employee reprimanded, but not terminated
44.88
Failure to meet regulatory compliance
25.98
Sensitive data/files/records exposed
25.20
Employee termination
20.47
Damage to company reputation
14.17
Challenges obtaining adequate cybersecurity insurance
14.17
Loss of revenue
11.02
Drop in user satisfaction or productivity
9.45
Fines
8.66
Enterprise server failures/downtime
8.66
Unexpected endpoint device failures
7.87
Unauthorized user maliciously attacked business IT resources
7.09
Unexpected remediation costs
5.51
Lawsuits
3.15
Loss of customers
3.15
None - violation occurred, but unknown or no consequences
12.60
%

Figure 5: Percentage of survey respondents indicating consequences that directly occurred due to a violation of their organization's privileged access management policies

additional business systems. Related incidents were most frequently noted among respondents from financial institutions (36%). They were also most significantly reported by organizations relying on native endpoint operating system tools for securing privileged accounts, clearly because these offer the least effective password controls.

The clearest violation of privileged access policies—a privileged account accessed by an authorized user—was discovered to have occurred by more than 22% of respondents. Related incidents were twice as likely to have occurred in large businesses as in small businesses (31% to 14% of respondents, respectively). High incident rates for this breach were particularly noted by respondents from finance (44%) and healthcare (38%) industries. Organizations using free or low-cost password vaulting solutions and those relying on simple shared spreadsheets to manage privileged access were most likely to have experienced an unauthorized privileged account usage, as reported by about 30% of respondents from each demographic. Interestingly, more than half of organizations that grant privileged access to

non-administrators reported an unauthorized use of privileged accounts, indicating end users are more likely to employ poor security practices and are not sufficiently being governed in the majority of businesses.

Organizations that experienced privileged access policy violations overwhelmingly indicated to have suffered direct business consequences related to the breach. In total, about 87% of survey respondents from breached organizations reported specific impact to business operations (Figure 5). The most frequently noted (and also least impactful) were incidents of employee reprimands. However, one in five respondents reported that an employee was terminated as a consequence of a privileged access breach event. Clearly, users share the responsibility for securing access to their authorized privileged access with their business and are held equally liable for any consequences resulting from the misuse of their elevated access.

Among consequences incurred on business operations, a failure to meet regulatory compliance and an exposure of sensitive business IT information were most frequently noted by survey responders. The two challenges are inextricably tied because the latter will undoubtedly result in the former. Roughly one out of every five business that suffered a policy breach were indicated to have experienced serious impacts to overall business performance, including a direct loss of revenue, a loss of customers, and/or damage to the company's reputation. While only noted by 14% of affected survey respondents, the sudden inability to obtain cybersecurity insurance due to a breach event is a relatively new consequence that is beginning to increase in prominence.

The high frequency rate of privileged access policy violations and their consequences can be broadly attributed to ineffective or poorly deployed PAM solutions. The inhibitors to adopting more effective methods for governing privileged access are principally related to dealing with increasing IT management complexities. In particular, 57% of survey respondents indicated that ensuring their adopted PAM solution integrates with third-party platforms is moderately or very difficult to achieve (Figure 6). Many commercially available cloud and enterprise-hosted

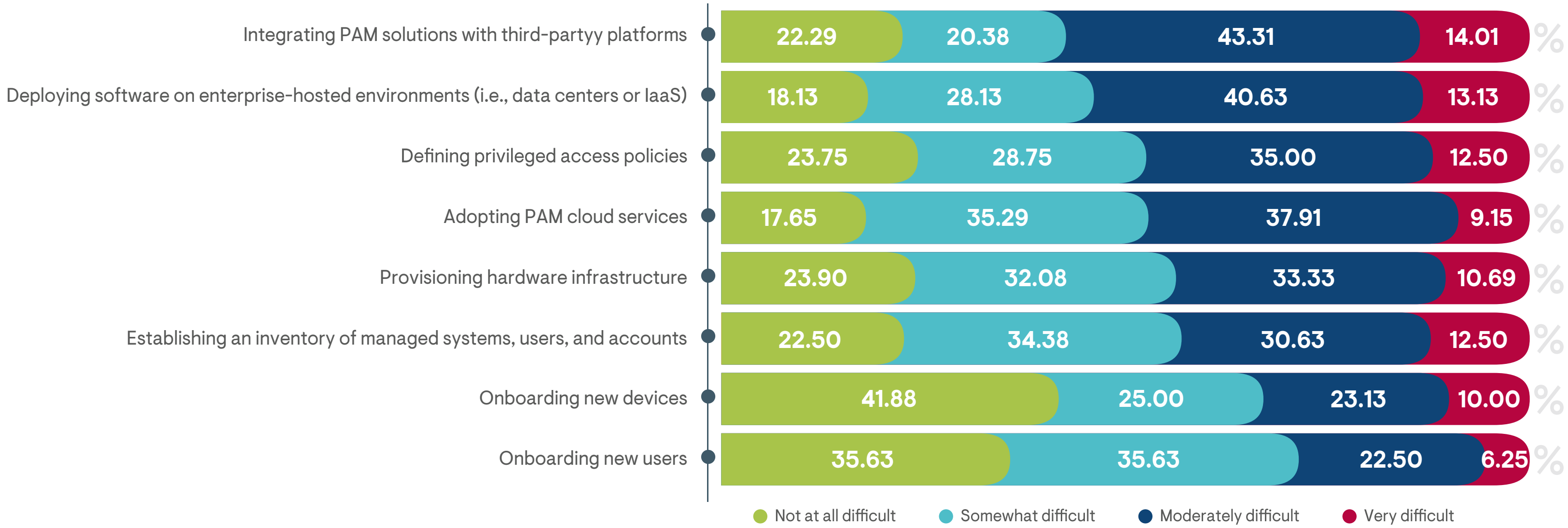

Figure 6: Percentage of survey respondents indicating the level of difficulty experienced with deployment processes for their organization's current PAM solution

software products include their own access processes that are designed to operate independently. Getting these to work seamlessly with a centralized PAM solution often requires the development of integration points using available APIs or SDKs, which need to be maintained and are typically not fully supported by either solution provider. Integrations were determined to be the most difficult for organizations utilizing custom scripts or shared spreadsheets for managing privileged access and were the easiest to enable by businesses that had adopted a PAM-specific platform.

PAM Practices and Processes

The effectiveness of any adopted PAM solution can be evaluated by the breadth of key management processes it enables. While most PAM approaches, at minimum, provide the basic capabilities of authenticating users and defining the resources to which the identified users are granted privileged access, the granularity of access definitions and methods for secure privileged activities vary widely across popularly employed solutions. According to survey respondents, most privileged access policies are able to define which specific users are empowered with privileged access to which IT services (Figure 7). Lacking this capability, privileged access is only granted to group accounts (such as "root" or "administrator" accounts) with common authenticators shared by multiple users, substantially reducing security effectiveness.

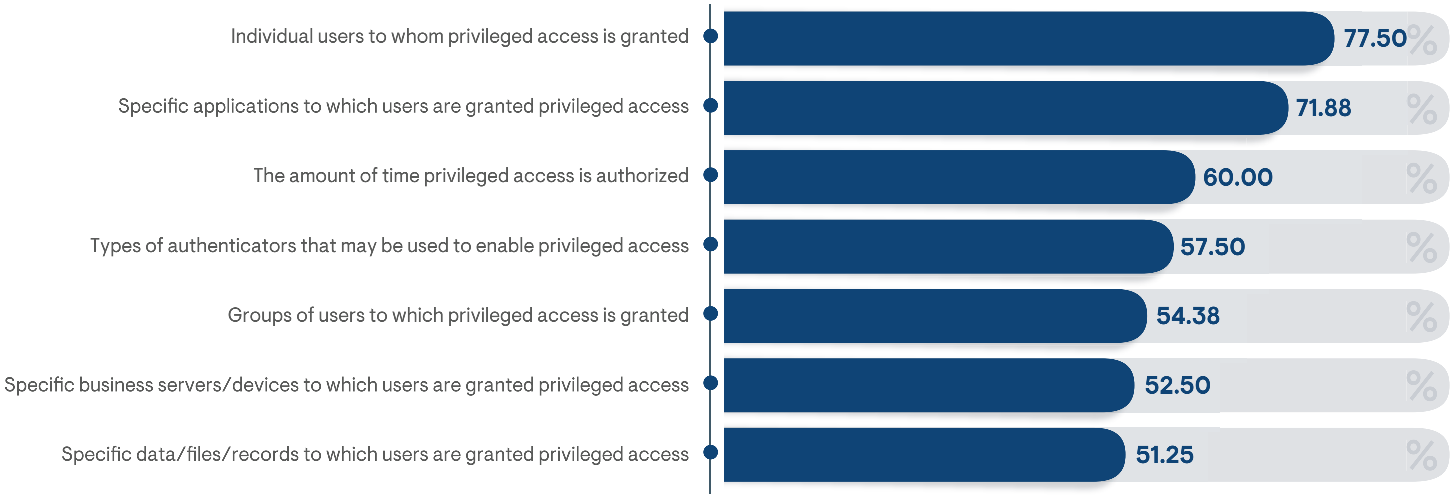

Figure 7: Percentage of respondents indicating privileged access policies specifically defined in their organization

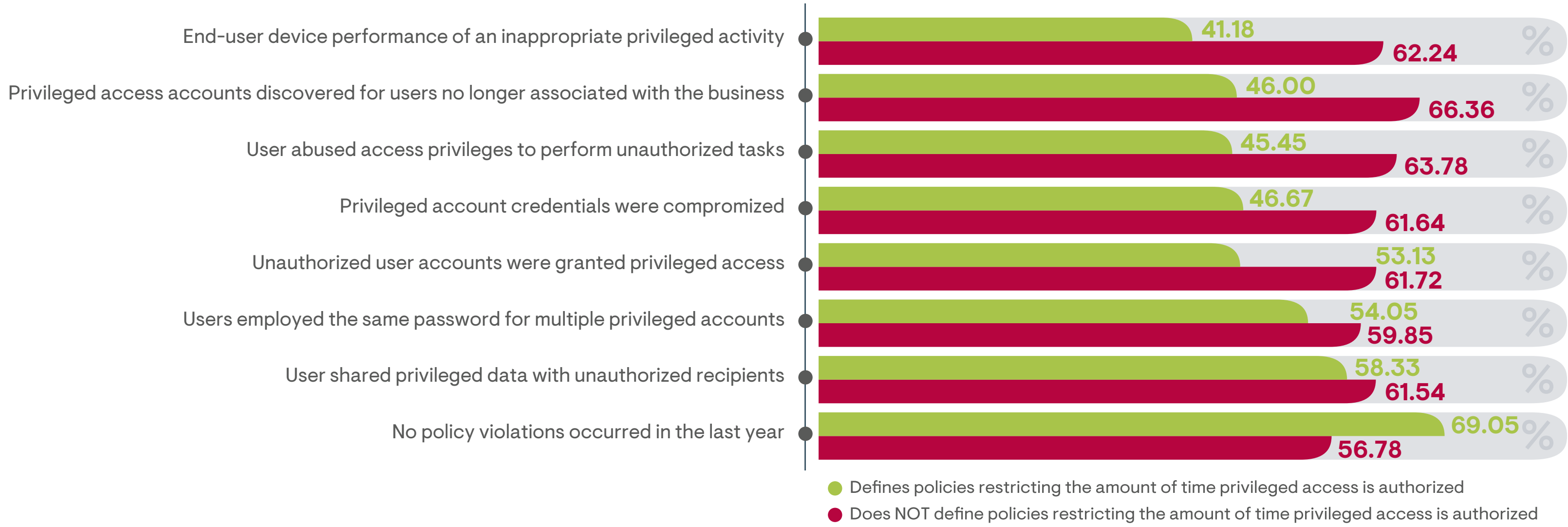
End-user device performance of an inappropriate privileged activity
41.18
62.24
Privileged access accounts discovered for users no longer associated with the business
46.00
66.36
User abused access privileges to perform unauthorized tasks
45.45
63.78
Privileged account credentials were compromized
46.67
61.64
Unauthorized user accounts were granted privileged access
53.13
61.72
Users employed the same password for multiple privileged accounts
54.05
59.85
User shared privileged data with unauthorized recipients
58.33
61.54
No policy violations occurred in the last year
69.05
56.78
%
● Defines policies restricting the amount of time privileged access is authorized
● Does NOT define policies restricting the amount of time privileged access is authorized

Figure 8: Comparing the percentage of survey respondents indicating policy violations that occurred in their organization in the last year between those that restrict the time privileged access is authorized with those that do not

The establishment of more granular policy controls was indicated to directly result in increased security effectiveness. In particular, organizations that managed policies specifying to which business services or devices privileged access is granted were determined to be 33% less likely to have experienced a privileged access policy breach in the preceding year. Similarly, survey respondents from organizations that established policies granting privileged access to specific files were 23% less likely to report policy breaches. Ironically, both granular policy definitions were identified as the least likely to be included by respondents' organizations in support of PAM processes.

Exceptional security improvements were also notably achieved by organizations that introduced PAM policies limiting the amount of time privileged access is authorized (Figure 8). The longer privileged access is enabled for a user account, the greater the risk it will be misused. By limiting the amount of time privileged access is required to just the duration required to complete specifically authorized tasks, bad actors are less likely to discover and exploit idle accounts. Survey results bear this out. Incidents of IT device performance impacted by inappropriate privileged activity was reported 44% less frequently by respondents from organizations that disable privileged access after a specified period. Additionally, discoveries of privileged accounts for terminated employees were reported 31% less frequently, incidents of privileged access abuse were noted 29% less frequently, and detections of credentials posted on the dark web were acknowledged 24% less frequently by responders from businesses that limit privileged access times.

PAM solutions that employ automation to enforce privileged access policies are overwhelmingly recognized as an essential component for managing elevated privileges. In fact, survey respondents with at least some PAM

automation capabilities estimated, on average, they had achieved 50% of their overall PAM goals, while responders that lacked automated solutions were only 17% of the way into their PAM journey. Automated tools enable the real-time monitoring of privileged access use and the rapid remediation of detected problems and vulnerabilities.

Among organizations that employ automation as part of their PAM solution, the most frequently noted capability is the continuous identification of privileged accounts and their usage across all managed environments (Figure 9). This is differentiated from solutions that only audit access events periodically (e.g., once per day/week/month). Management solutions specifically designed to govern privileged access were the type most frequently noted (by 65% of survey respondents) for supporting continuous monitoring features. Continuous monitoring of privileged accounts and activities ensures any potential risks are addressed in real time, substantially reducing security risks. Organizations that only performed periodic monitoring of privileged access were 2.5 times more likely to have experienced a policy breach in the preceding year than those utilizing continuously monitoring feature sets. In addition, survey respondents, on average, recognized PAM solutions employing continuous monitoring to be "somewhat easy" to manage, while those utilizing periodic monitoring solutions recognized the management of PAM processes to be "somewhat difficult."

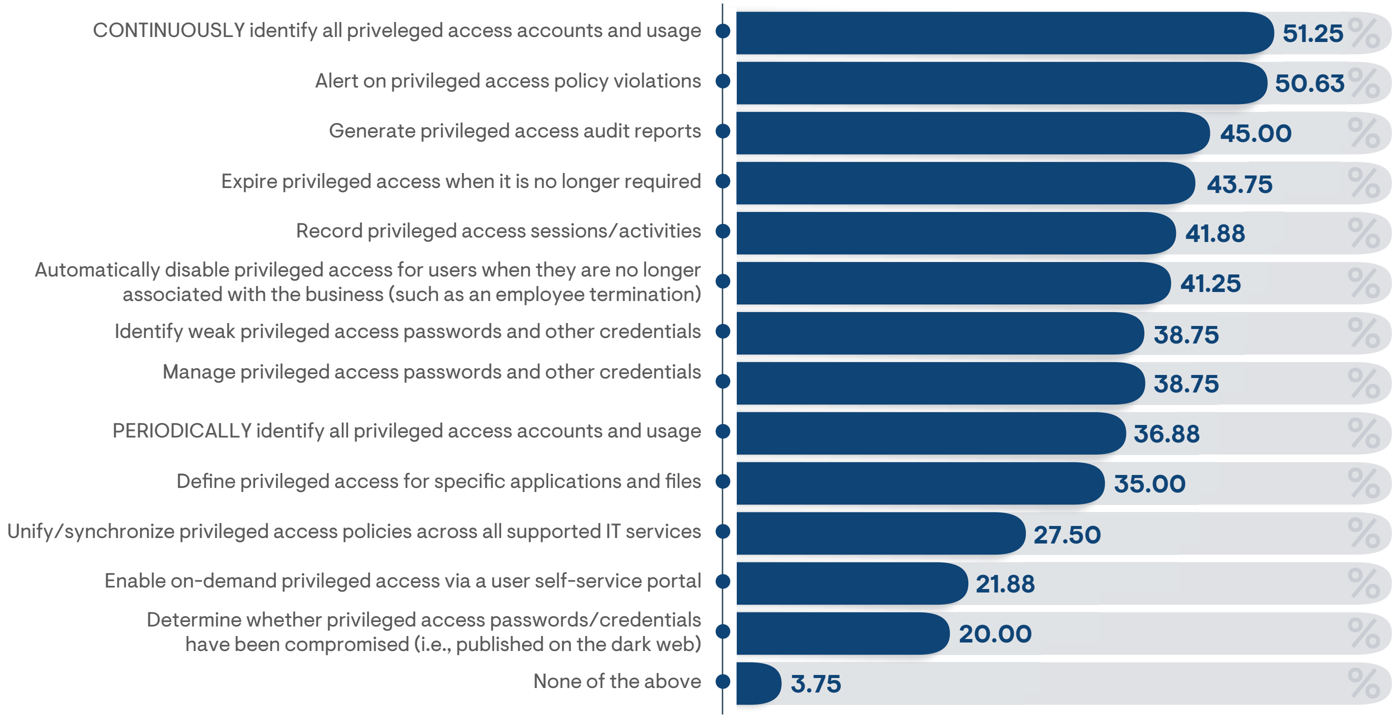

Figure 9: Percentage of survey responders indicating the PAM capabilities currently supported by automated solutions in their organization

PAM automation is essential for enabling holistic visibility into privileged access usage for governance and accountability. In fact, survey respondents that lacked automation capabilities in their adopted PAM solution consistently reported the basic process of establishing an inventory of managed systems, users, and accounts to be "very difficult" to achieve. Accelerating business requirements for reducing management efforts are driving the adoption of PAM solutions that simplify the monitoring of privileged access information. Roughly half of survey respondents indicated their organization leverages automation to detect and alert on privileged access policy violations. Timely notifications on vulnerabilities and breaches are critical to ensuring rapid responses to mitigate risks and proactively prevent privileged account misuse.

Improvements to privileged access visibility also simplifies processes for conducting periodic audits for governance and regulatory compliance attainment. Audit processes can be extremely costly and time-consuming if performed manually. Automation can substantially reduce auditing processes by collecting and generating prebuilt reports on the privileged access granted to users and how they are being used. This timely and accurate information can have a significant impact on reducing security vulnerabilities. According to survey results, organizations that employ automation to generated privileged access audit reports are indicated to have substantially reduced rates of policy breach events. For example, businesses that lacked these capabilities were indicated to be more than seven times more likely to discover that privileged account credentials had been compromised (i.e., posted on the dark web) during the preceding year.

The greatest inhibitor to enabling holistic visibility and management of privileged access is increasing IT infrastructure complexity. Only about 27% of survey respondents noted the ability to unify PAM policies across all supported IT services, including on-premises servers, cloud-hosted environments, web services, and endpoint devices. However, more organizations that had adopted solutions enabling PAM policy synchronization were able to report decreased breach rates. In particular, organizations that adopted a unified PAM approach were indicated to be 72% less likely to have discovered active privileged access accounts for users that had been terminated. This correlation can be attributed to the fact that typically, when users depart, administrators only disable known accounts and fail to recognize access privileges that were granted to less frequented resources. With a unified solution, the disablement of privileged accounts need only be executed in a single location.

An Unhealthy Reliance on Shared Privileged Accounts

Despite the obvious risks associated with enabling privileged accounts shared by multiple users, a majority of organizations continue to rely on group accounts as a method of enabling quick and easy privileged access. In fact, 87% of survey respondents indicated that shared privileged accounts were in use in their organization (Figure 10). What makes the use of group accounts so inherently dangerous is the fact that they eliminate the possibility of accountability. Even organizations that stringently monitor and record the execution of privileged tasks are unable to conclusively identify the specific individual responsible for making an unauthorized change if they used a shared account. In addition, the more users who know a password or retain other credentials enabling access to a shared privileged access account, the greater the chances that account will be compromised.

The use of shared privileged accounts can be directly correlated with security breaches (Figure 11). Among survey responders whose organizations did not support shared privileged accounts, there were no reported cases of privileged account credentials reported on the dark web and no impacts to endpoint device performance due to inappropriate privileged activity. Additionally, incidents of privileged accounts accessed by an unauthorized user and users sharing privileged access with a peer were both indicated to be roughly five times more likely with organizations that support shared accounts.

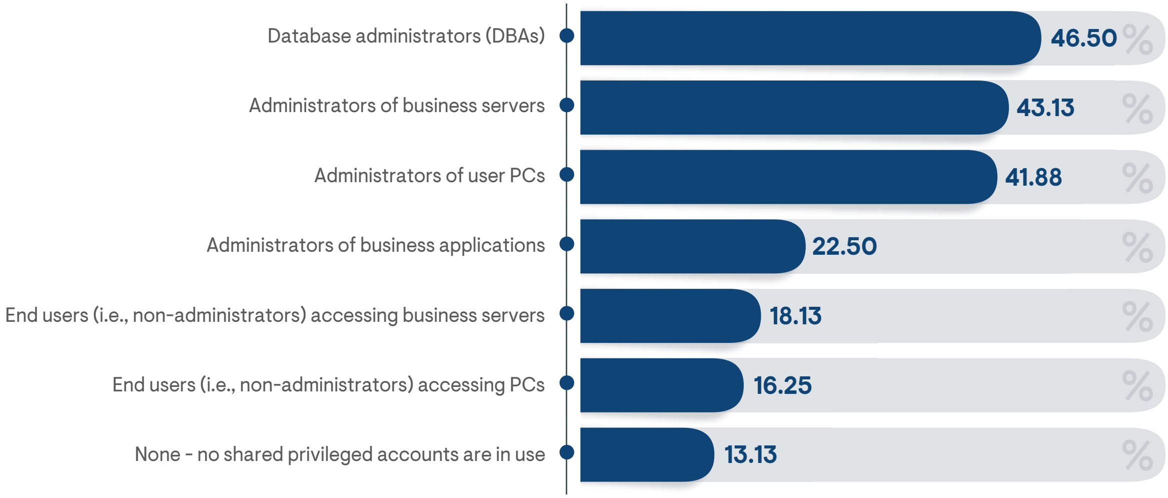

Figure 10: Percentage of respondents indicating the types of users who have access to shared privileged accounts in their organizations

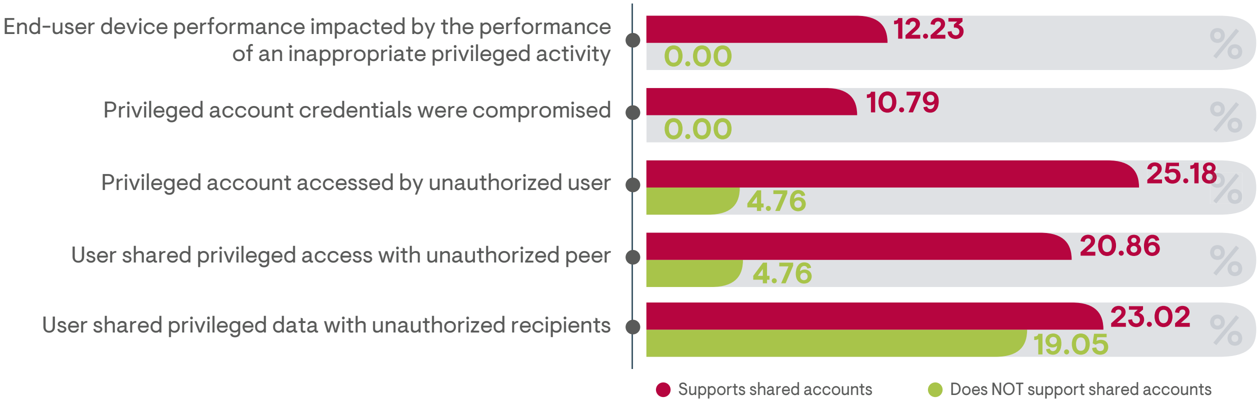

Figure 11: Comparing the average percentage of privileged access policy violations between organizations supporting shared privileged accounts and those that do not support shared privileged accounts

Rather than relying on unfettered group accounts to enable multiple privileged users, survey results suggest that a more secure approach is to adopt solutions that adhere to the "principle of least privilege." At any given time, authorized users only need to perform a specific set of privileged tasks. By limiting privileged access authorizations to just performing those required tasks, organizations eliminate the chance that elevated permissions will be misused to perform unapproved tasks. PAM platforms supporting "least privilege" allow organizations to centrally define specific policies governing which tasks can be performed by which specific users. This also provides a level of accountability not available in shared accounts since permissions to perform privileged tasks not already approved require a specific authorization.

Risks of Standing Privileged Accounts

Despite increasing evidence and business recognition that utilizing standing privileged accounts is inherently insecure, most organizations continue to employ user accounts that indefinitely retain elevated privileges. In total, 97% of survey respondents indicated their organization maintains at least some standing privileged accounts. Standing privileged accounts are prime targets for hackers and other bad actors because they enable a single access point that completely bypasses security controls allowing unfettered activities. By far the most common standing privileged accounts are those created for specific IT administrators (Figure 12). However, standing privileged group accounts that are shared by multiple administrators were also indicated to be in use by a majority of survey responders. Large businesses were determined to be the least dependent on standing privileged accounts. In particular, finance and healthcare organizations were indicated to be most responsible in reducing the use of standing privileged accounts.

While an argument can be made that IT administrators may require standing privileged accounts in order to support management tasks, this does not account for the relatively high frequency of rarely used or completely unused standing privileged accounts. Among survey respondents, 28% reported they maintained rarely used accounts, while 69% noted the existence of never-used accounts.

Default OS standing accounts—including "root" or "administrator" accounts that come preinstalled with typical OS environments—were as frequently noted to be unused as they were reported to be used. Organizations often fail to deactivate default accounts once alternative privileged access has been enabled, either out of concern that they require a failsafe method of privileged access or because they simply lack an understanding of the inherent dangers. Default OS standing accounts are always the first privileged accounts targeted by attackers because the account names are well known and very commonly in use. Among survey

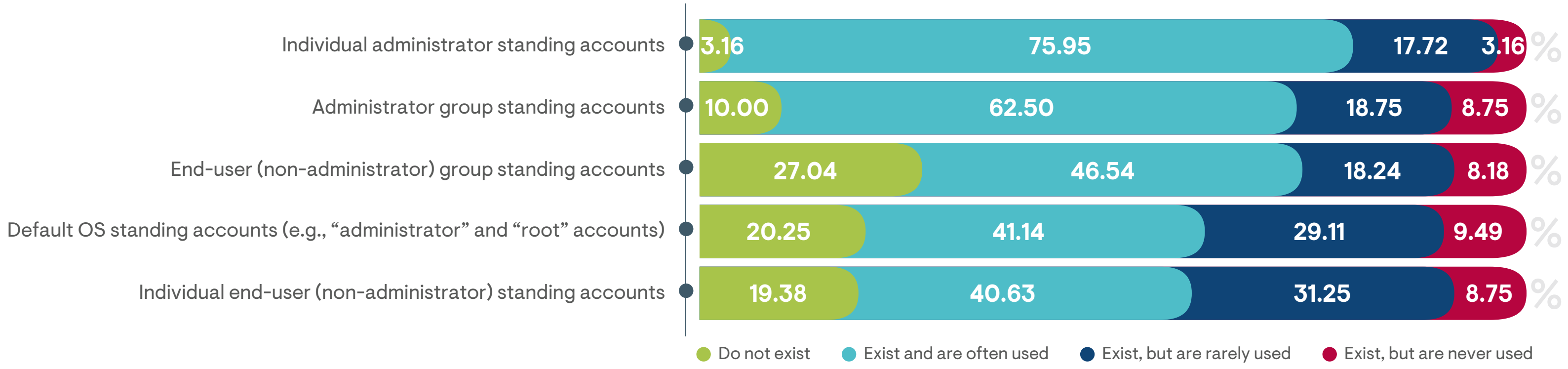

Figure 12: Percentage of survey respondents indicating the types of standing privileged accounts that currently exist in their organizations

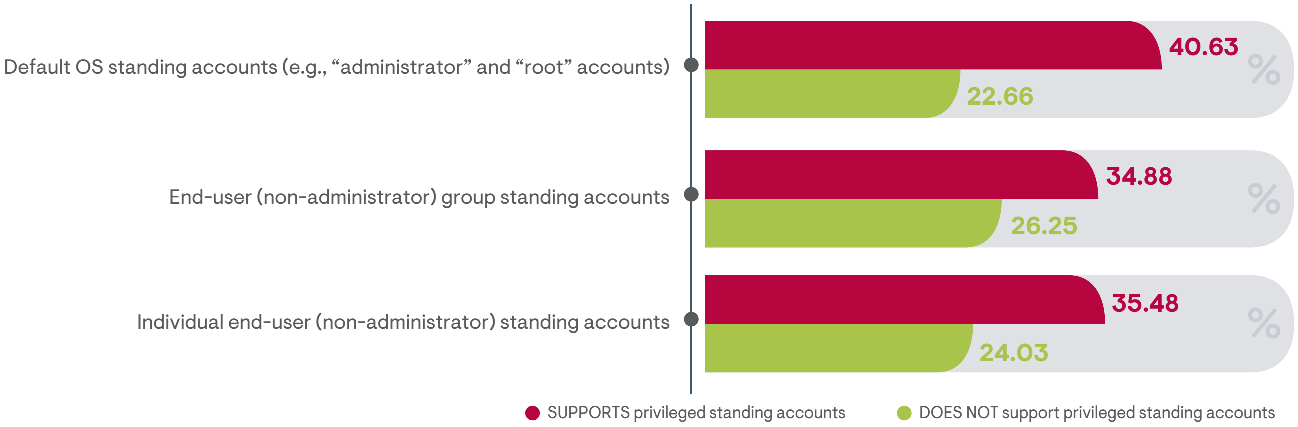
Default OS standing accounts (e.g., “administrator” and “root” accounts)
40.63
22.66
%
End-user (non-administrator) group standing accounts
34.88
26.25
%
Individual end-user (non-administrator) standing accounts
35.48
24.03
%
● SUPPORTS privileged standing accounts
● DOES NOT support privileged standing accounts

Figure 13: Comparing the percentage of survey respondents indicating they had no policy violations in the preceding year between those whose organizations support standing accounts and those whose do not[1]

respondents that maintain default OS standing privileged accounts, 77% reported they had experienced a privileged access policy violation in the preceding year. By comparison, only about 59% of respondents that did not rely on default OS standing accounts experience a policy violation during that time period (Figure 13).

The high rate of low use or unused standing privileged accounts was also noted to exist for non-administrators. These accounts are typically created to assist a user with resolving a specific problem, but then sit idle indefinitely, increasing business security risks. Among survey respondents permitting the use of non-administrator standing privileged accounts (both individual and group accounts), the incident rate for policy violations was noted to be 30% higher than for organizations that prevent the use of such accounts.

The most popular approach to reducing or eliminating standing privileged accounts is the employment of just-in-time (JIT) privileged access authorization technologies. JIT solutions authorize privileged access tasks to be performed by user accounts that would not otherwise be authorized to perform privileged activities, and only authorize the elevated permissions during a predetermined period of time. At the conclusion of the time period, all privileged authorizations are rescinded for the user accounts. Any future privileged access activities that need to be performed by the user’s account requires the initiation of a new authorization process. In this way, business risks are significantly reduced because any compromised accounts are unlikely to retain elevated privileges at any given time.

The key component of a JIT approach is the deactivation of privileged authorizations when they are no longer required. In total, roughly 44% of survey respondents indicated their organization has the ability to

[1] Author’s note: this chart does not include information on non-standard administrator standing privileged accounts because the number of survey respondents whose organizations did not rely on such accounts were too small to achieve statistical relevance.

automatically expire privileged access when it is no longer required. Among these respondents, 43% indicated their organization experienced no policy violations in the preceding year. By comparison, only 13% of organizations without the ability to expire privileged access reported no policy violations. This indicates a more than threefold increase in security effectiveness by introducing this one key PAM feature.

Of course, JIT solutions require users to request privileged access each time it is required, which can become quite laborious if performed frequently using cumbersome processes, such as requiring a user to contact a help desk. These impacts to user productivity can be greatly reduced by enabling an automated user self-service portal for requesting privileged access. Among survey respondents belonging to organizations that automatically expire privileged access after use, one-third employ a user portal for requesting privileged access. These respondents reported lower frequencies of policy violations specifically related to irresponsible user activities (Figure 14). Most notably, the use of on-demand privileged access via a user self-service portal was indicated to decrease the chances of a user employing the same password for multiple privileged accounts by as much as 80%. This is because multiple privileged accounts are simply not required when using a centralized authentication mechanism. Policy-based controls governing self-service portal authorizations ensure privileged access is restricted to specific devices or applications required for the legitimate performance of privileged tasks, so each individual IT component does not require an independent standing privileged account.

Security improvements with the use of a self-service portal for authorizing JIT privileged access can also be seen with a lower frequency of policy violations that affect the performance of business IT systems. Users who are tempted to use privileged access to make impactful and unauthorized operating system changes are less likely to do so if such tasks require authorization. Additionally, related PAM solutions with policy-based controls can limit self-service portals from authorizing OS changes that can affect system performance. For instance, a user may be authorized to use granted privileged access to install an application but may not be able to change registry or kernel settings.

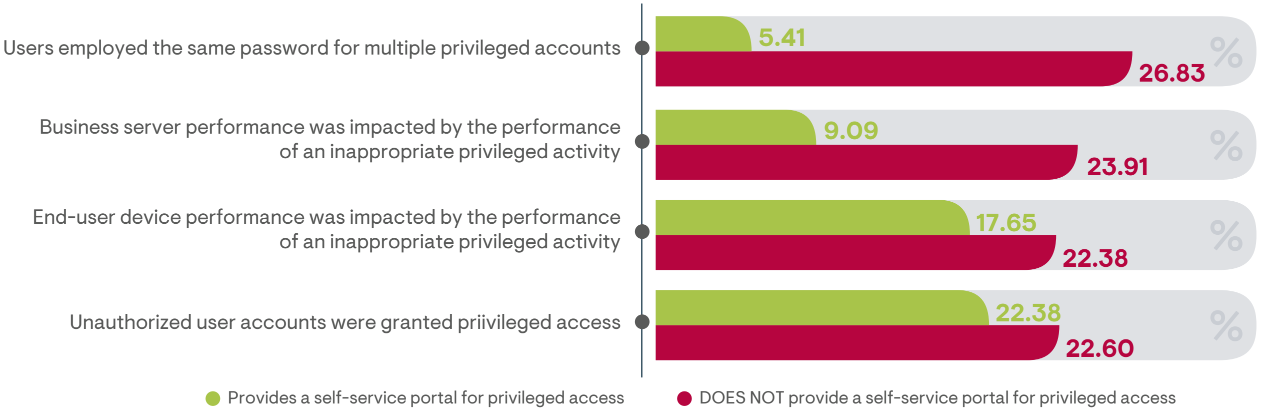

Figure 14: Comparing the percentage of survey respondents whose organizations experienced a policy violation in the preceding year between those providing a user self-service portal for granting privileged access and those that do not

Managing Privileged Access on Endpoint Devices

While much of the focus of PAM solutions and practices tends to be on protecting cloud and on-premises server hosting environments, impacts to end-user devices (i.e., desktop or laptop PCs) should not be overlooked. Roughly 88% of survey respondents indicated that their organization provides employees with local administrator rights to their company-supplied PC or laptop. On average, endpoint privileged access is granted to roughly 24% of business employees. The percentage of users granted endpoint device administrator rights increases with company size, and fully one-quarter of large business employees are empowered with elevated privileges on their workstations (Figure 15). That is a staggeringly high number considering the potential impacts to business operations from privileged access misuse. In an organization of 10,000 employees, about 2,500 can be expected to retain privileged access to their devices. Respondents from healthcare institutions were indicated to be most likely to allow users local administrator rights, granting it to 46% of their workforce, on average.

Organizations that grant users privileged access to their endpoint devices are exposed to some elevated security risks. In particular, survey respondents from businesses that allow users to retain local administrator rights were 34% more likely to report incidents of a compromised privileged account credential. Since non-administrators are more likely to employ easily guessable password and reuse passwords across multiple accounts (including with non-business resources, such as public email or social media tools), they are at greater risk of exposing credentials and having them posted on dark websites.

In addition, incidents of end-user device performance impacted by an inappropriate privileged activity were reported twice as frequently by organizations that allow privileged device users than by those that limit this access to qualified administrators. Non-administrators often lack the expertise required to perform advanced operating system management tasks and are unaware of business rules governing system changes. However, it is not uncommon for end users to believe they have enough of an understanding to make system updates without taking the time to open a help desk ticket or otherwise involve IT administrators.

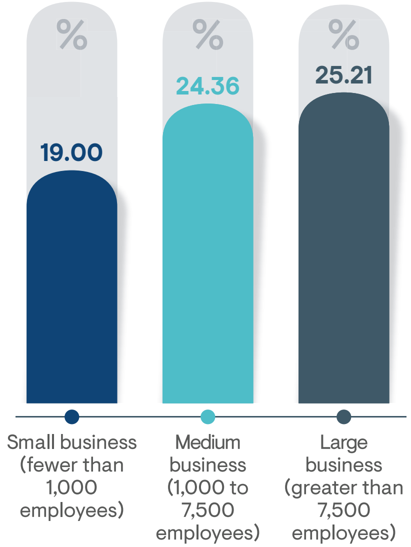

Figure 15: Average percentage of end users (i.e., non-administrators) granted privileged access to their personal endpoint devices by organization size as noted by survey respondents

Despite the fact that many organizations grant end users privileged access in order to reduce the day-to-day management burden on IT administrators, survey results indicate this approach delivers the opposite outcome. One-third of survey respondents from organizations that allow end users privileged access to their workstations report that they find overall PAM processes to be somewhat or very difficult to manage. Only 21% of organizations that restrict non-administrator privileged access to endpoint devices noted PAM to be somewhat difficult to manage, and no respondents from this group identified PAM support to be very difficult.

In fact, survey respondents indicated that PAM administration challenges across all primary practices are very significantly diminished among organizations that do not grant employee access rights (Figure 16).

Not surprisingly, the greatest reduction to management challenges achieved by organizations that do not grant end users privileged access to their workstations was with managing endpoint device administrator accounts. This can be simply attributed to a significant reduction in the number of privileged accounts that need to be monitored and supported.

Similarly, more granular PAM policy enforcement requirements—such as limiting privileged access times and the types of privileged tasks that can be performed—are indicated to be greatly simplified by a reduction in the number of privileged users. A key implication from this result suggests that organizations that necessitate the granting of local administrator rights to end users should adopt a PAM-specific platform that specifically defines and enforces policies supporting "least privilege" requirements on endpoint devices in order to reduce management efforts while boosting security effectiveness.

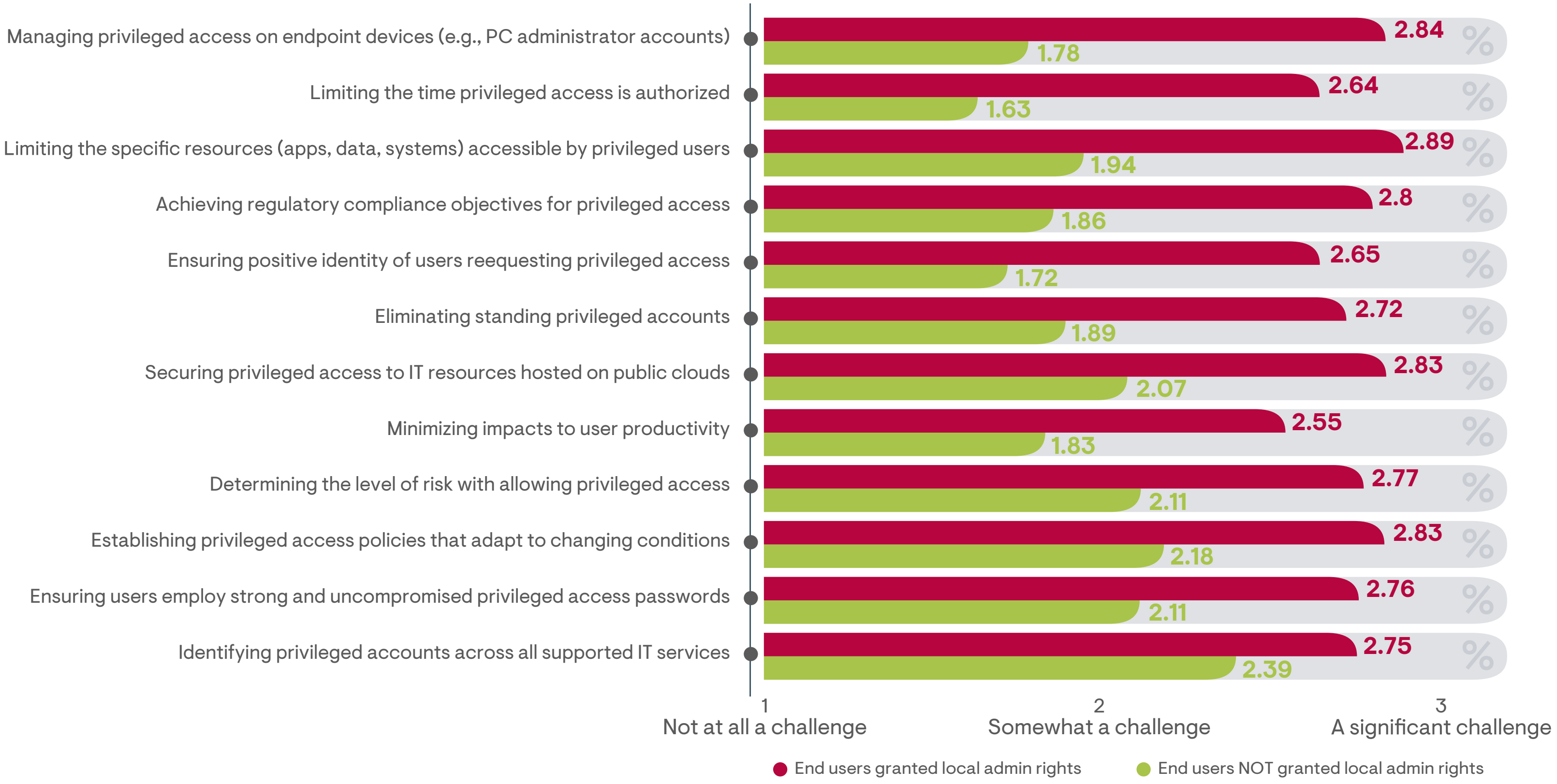

Figure 16: Comparing the average level of challenge in performing critical PAM tasks between survey responders from organizations that grant end users local admin rights to their personal workstation and those that do not

EMA Perspective

A lack of sufficient privileged access controls is placing the vast majority of businesses at extreme risk of significant security breaches. With 87% of survey respondents indicating their organization had experienced a privileged access policy violation in just the preceding 12 months and 93% reporting that they do not even have confidence that their adopted solutions will prevent privileged access security breaches, it is clear that currently adopted PAM processes are, in the majority of cases, insufficient to provide the level of protection they were introduced to achieve. Despite the overwhelming evidence, however, many organizations seem content to continue utilizing weak PAM solutions, as evidenced by the high overall satisfaction rates.

The reluctance to establish more effective PAM approaches is undoubtedly related to concerns about the deployment complexity and manageability of more advanced PAM technologies, and many organizations are prioritizing budgets toward alternative methods of security management, such as security information and event management (SIEM) and threat detection systems. While these technologies certainly merit consideration, related solutions may all be rendered completely ineffective by an attacker who has managed to gain privileged access. The broad and continued use of standing and shared privileged accounts certainly provides prime targets for bad actors to bypass even the most stringent security controls.

EMA survey results plainly indicate there are significant advantages to the adoption of an enterprise-class PAM platform that was specifically architected to support the principles of least privilege access. Organizations that adopted solutions with policy-based controls defining which specific resources privileged users have been granted access to were determined to be 33% less likely to have experienced a policy breach. Even more effective PAM solutions are those that limit the amount of time privileged access is authorized. Related platforms supporting JIT functionality that automatically expires privileged access when it is no longer in use were recognized as reducing the chances of a policy violation by 44%, on average. Additionally, PAM platforms that are able to centrally manage privileged access across endpoint devices were shown to reduce the chances of a compromised privileged account credential by 34%, on average. Collectively, these security improvements fundamentally transform enterprise security by minimizing risks to the business's most sensitive and vulnerable access points.

EMA survey results plainly indicate there are significant advantages to the adoption of an enterprise-class PAM platform that is specifically architected to support the principles of least privilege access.

Perhaps the greatest unsung advantage to adopting an enterprise-class PAM platform is the effect it has on actually reducing the complexity of security management and related costs. In fact, 71% of survey respondents recognized "simplifying management efforts" as the principal advantage of enterprise-class PAM adoption. Automated monitoring and task execution substantially reduce the day-to-day burden on IT administrators with dynamic support for policy management, auditing processes, and credential enforcement. This is further enhanced by solutions that provide self-help user portals that allow authorized users to responsibly gain privileged access without disturbing IT administrators at all. In regard to deployment concerns, the majority of surveyed organizations (57%) indicated their primary challenge was related to difficulties with integrating the platform with third-party solutions. This issue can be significantly mitigated by adopting PAM solutions that offer direct integrations with key technologies (most notably, service management tools).

Advancing Privileged Access Management (PAM) to Address Modern Business Requirements

The most effective approach to any enterprise security strategy is to prioritize solutions that address the organization's greatest vulnerabilities first, and the distribution of privileged access accounts and their use certainly qualifies as a top-of-the-list item in most cases. With the right PAM solution in place, businesses transition from reacting to systemic privileged policy breaches to proactively preventing breaches from occurring. In addition, organizations advantaged by an enterprise-class PAM solution realize reductions to management efforts and operational costs while ensuring users are limited to utilizing elevated privileges only when absolutely necessary, and only to perform authorized, business-required tasks.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
www.enterprisemanagement.com
4057.120820