Remediant

CURRENT STATE AND TRENDS OF

PRIVILEGED ACCESS MANAGEMENT

Organizations of all sizes and across all industries are under siege, struggling to address an expanding attack surface with hundreds of millions of new threats identified each year – and the targets and tactics of these assaults are getting more sophisticated. The **2019 Verizon Data Breach Investigations Report (DBIR)** found that C-level executives are 12 times more likely to be the target of social incidents and 9 times more likely to be the target of social breaches than in previous years. The goal of these attacks is typically to compromise or obtain the credentials of the executive to gain access to the network and sensitive data.

While there is nothing that can provide absolute protection or make your network and data invulnerable, following some essential best practices can help organizations avoid the vast majority of malware and exploits. The reality is that most attacks involve unauthorized access, abused privileges, or stolen credentials of some sort. Having tools and processes in place to prevent unauthorized access and avert abuse of privilege by those who are authorized is an essential component of effective cybersecurity.

Remediant commissioned Enterprise Management Associates (EMA) to conduct a survey to research the challenges organizations face with privileged access management (PAM), the tools and methods used to manage privileged access, and the perceived effectiveness of PAM solutions. The research revealed a number of interesting findings.

Executive Overview

IT budgets are growing.

84%

of survey participants indicated that their annual IT budget increased over the previous year—with 10% indicating their IT budget increased by 50% or more.

PAM recognized as essential component of cybersecurity. Among the organizations that have adopted privileged access management, the number one reason for doing so (36%) is to reduce security vulnerabilities, followed by protecting sensitive business data (33%)

Organizations want PAM to be automated. When asked which capabilities are most important, the top answer was "Automatically expire privileged access" (24%).

The second highest response was "Detect new privileged access" (23%)

Working with what they have.

Nearly 3 out of 10 of the organizations that have not implemented a dedicated PAM solution believe that existing access and password management tools are sufficient. The second leading reason (19%) is that PAM is too complex to implement and manage.

Growth opportunity for PAM. More than three quarters of the organizations that have not yet implemented a comprehensive PAM solution intend to do so over the next 5 years. More than 6 out of 10 indicated that they plan to adopt a PAM solution this year or next year.

Methodology

To gather insight on the current trends and emerging future of privileged access management, EMA surveyed 150 IT and cybersecurity analysts from around the world. IT professionals from around the world took part in the survey, but 96% of the participants were from North America.

The survey represents a broad range of industries and company sizes. Tech companies, finance and manufacturing have the most representation, but there are also survey participants from healthcare, government, transportation, education, and other significant industries. There is a relatively even mix of small, medium, and large or enterprise businesses in the survey. Medium sized businesses of 2,500 to 9,999 employees had the highest representation with 41%.

More than 80% of survey participants describe their familiarity with privileged access management as either Very Familiar or Expert, and more than 70 percent indicated that they are directly responsible for granting privileged access to users.

Managing PAM

Managing privileged access effectively is about more than simply assigning a level of access or privilege based on the role or functions an individual is expected to perform. There is virtually constant change as users join and leave the company, change roles or get promoted, work on sensitive projects, or have projects end. The need for privileged or elevated access is also generally limited—and not something that needs to or should be granted indefinitely in most cases.

The constantly evolving dynamics of privileged access can quickly become a full-time job for the IT admins responsible for managing it. According to the survey, the average frequency reported by administrators for requests to elevate a user's privileges is between once and twice per day—with 18% claiming they receive such requests more than twice per day.

Survey participants were also asked about the actual duration of privilege escalation compared to what was planned. In most cases, the planned and actual times seem to align fairly well, but the net result is that the average duration of privileged access exceeds the plan by about 2 hours. That is 2 hours that systems and data are unnecessarily exposed to potential risk or compromise.

PAM Requirements

The easiest thing would be to just lock away all sensitive data and never let anyone access it, but there are legitimate reasons that applications and individuals need to be able to access systems and data within a network in order to be productive and conduct business. According to the survey results, 35% of users require privileged access to their endpoint—whether it's a desktop or laptop PC. Many users also require privileged access to things like cloud-hosted business services (34%), business application databases (32%), and business application servers (31%).

Similar to the primary reasons for adopting PAM solutions above, survey participants cited protecting sensitive business data (45%) and reducing security vulnerabilities (43%) as the most important reasons for managing privileged access. Ensuring accountability on

execution of privileged tasks (27%), improving workforce productivity (23%) and achieving regulatory compliance (20%) were also among the factors mentioned. Another leading driver for PAM according to the survey is concern over undiscovered or unmanaged privileged accounts. 88% of those surveyed are worried about this to some degree, with almost a quarter revealing they are either Very (15%) or Extremely (9%) worried.

With all of that in mind, it's easy to see what a crucial role PAM plays. When asked to indicate the level of importance organizations place on effectively managing privileged access, 79% ranked it as either Very (44%) or Critically (35%) important.

PAM Adoption

The concepts of restricting or limiting access to computer resources and information through efforts such as role-based access and least-privileged access date back to the dawn of networking and computer security. What varies from one organization to the next are the tools and methods used to implement and manage privileged access, and the degree to which those processes can be automated. According to the survey, the leading method of managing privileged access is a directory service like Azure Active Directory (50%), followed closely by a dedicated PAM solution (49%) or a password vault solution (43%). On the bottom end of the range, 29% use custom scripts or applications, and 27% rely on native endpoint operating system features.

When asked what the primary reason is for adopting privileged access management solutions at all, organizations that have adopted PAM cited reducing security vulnerabilities (36%) and protecting sensitive data (33%) as the leading reasons. Not all of the reasons are security related, though. Lowering administrative costs (22%) and improving workforce productivity (18%) and other operational and financial considerations also made the list.

Different regions, industries, and organizations have different ideas for what constitutes privileged access management. Survey participants were asked to identify what they consider to be the most important capabilities for a PAM solution, and automation tops the list. The top two capabilities were automatically expire privileged access (24%) and detect new privileged access (23%). Some of the other interesting results include enable privileged access based on contextual information (15%) and grant temporary privileged access quickly—in under 5 seconds (12%).

The survey also explored why some organizations have not embraced a dedicated PAM solution. Of the organizations that have not implemented a PAM solution, the leading justification is the belief that existing access and password management tools are sufficient (29%). The other top reasons include that PAM solutions are too complex (19%), too expensive (14%), or that the organization simply does not see any value in a dedicated PAM solution (14%).

There is a growing market for PAM solutions, though. Most of the organizations that have not yet adopted a comprehensive PAM solution plan to do so in the near future. More than 75% indicated plans to implement a PAM solution in the next 5 years, with 62% responding that they plan to do so either this year (30%) or next year (32%).

Challenges of PAM

Effective management of privileged access can be complex—especially when trying to implement privileged access management using manual processes or relying on tools and features that are not really designed for the task. When asked how many violations of privileged access management policy occurred in the last 12 months, nearly a quarter claimed to have zero but the average among the responses was 3.2. When that data is examined as a function of the importance the organization places on privileged access management, though, it reveals more enlightening results. Among the organizations that believe PAM is not at all important, the number is more than double with 7 violations in the past 12 months.

There are also some counterintuitive findings as well. For example, viewed as a function of the methods used by organizations to manage privileged access, two of the top three highest in terms of PAM policy violations were dedicated PAM solutions (3.62) and password vaults (3.58). Organizations that rely on features that are part of the network security management platform or native endpoint operating system tools were among the lowest in terms of policy violations.

Those privileged access management policy violations had consequences and costs as well. Nearly 4 out of 10 (37%) experienced a malware infection or compromised data as a result of policy violations, and 30% resulted in unexpected server failures or problems. The average cost to the organization for a privileged access management policy violation was $5,580—or $23,400 per year.

Policy violations also impact operations and incur costs in terms of the time spent by administrators to remediate issues and repair damage. Survey respondents reported an average of 8.5 hours spent each year to remediate or repair issues caused by violations of privileged access management policies. Interestingly, organizations that depend on native endpoint operating system tools for privileged access management spent the least time—just 7.69 hours on average per year—while those with dedicated PAM solutions were in the middle of the pack with an average of 8.78 hours, and password vaults were on the high end at 9.41 hours.

While most of those surveyed believe that the various tools and processes for managing privileged access increase user productivity, it is worth noting that a significant number also believe they decrease user productivity. 20 percent of the organizations using a dedicated PAM solution and 19% of those using a password vault claim that it either somewhat or greatly reduces user productivity.

Perhaps one of the most concerning findings in the survey is the amount of time administrators have to devote to managing privileged access. Half of the survey participants indicated that manually granting temporary privileged access is either Very (29%) or Extremely (21%) time consuming. Manually revoking temporary privileged access is also a drain with 50% reporting that it is either Very (33%) or Extremely (17%) time consuming. Across the board, the tasks necessary for effective privileged access management are seen as time consuming. The least time-consuming task reported in the survey is enforcing password rules—and even that one has 69% who claim it is either Somewhat (25%), Very (25%), or Extremely (19%) time consuming.

Outcomes of PAM

In spite of the sentiment that privileged access management is time consuming, and that PAM policy violation still occur, most of the survey participants are happy with their privileged access management strategies. More than 8 out of 10 indicated that they are either Somewhat (45%) or Very (37%) satisfied with their current PAM approach.

More than 9 out of 10 also believe that their current PAM approach results in quantifiable cost savings for the organization. 93% reported that they believe (55%) or somewhat believe (38%) they are seeing quantifiable cost savings.

The level of satisfaction with the current PAM strategy and the belief in quantifiable cost savings seems to be at odds, however, with the response to the question of how well survey participants believe their PAM strategy will actually prevent security breaches or incidents of abuse of privileged access. Almost 40% shared that they feel their PAM solution will only prevent some inappropriate use of privileged accounts—or may not prevent inappropriate use of privileged accounts at all. Even among responses from organizations with a dedicated PAM solution, 30% believe it will only prevent some inappropriate use of privileged access and 8% don't think it will help prevent abuse of privileged access at all.

A Better Way to Manage Privileged Access

Taken together, the survey findings paint a picture where effective privileged access management is crucial to security. Privileged access—whether an inside attack or through compromised credentials—represents the leading attack vector for security breaches. Users, roles, and functions are constantly changing—and the need or lack thereof for privileged access changes with them. Administrators are wasting too much time and organizations are not getting the peace of mind and confidence they should expect with traditional PAM solutions.

Remediant SecureONE operates on a zero trust security model, providing access in real-time with Just-in-Time, Just-Enough privileged access using two-factor authentication. Automating the process of granting temporary privileges on an as-needed basis reduces the attack surface while freeing up administrators to focus on more productive or valuable tasks.