MANDIANT

NOW PART OF Google Cloud

THREAT INTELLIGENCE
WHITE PAPER

6 Tips for Implementing Privileged Asset Management

The content in this document was originally published in The Defender's Advantage Cyber Snapshot Issue 4.

MANDIANT

Cyber Snapshot Report Issue 4

Increased adoption of cloud services and SaaS applications is exponentially growing the number of accounts organizations must operate and manage. For example, today the average employee can access 30 corporate accounts and applications. Further, machine identities, digital certificates and keys now outnumber human identities by a factor of 45x[1].

For organizations that are struggling to reduce unnecessary accounts and remove excessive privileges for humans and systems that do not require it, implementing Privileged Access Management (PAM) can help.

PAM is a practice of controlling and securing access to assets within a business, by

- **Creating authorization workflows**
- **Securely storing and encrypting secrets**
- **Auditing, monitoring, and logging privileged access events**
- **Setting policies for secrets management (e.g. Password Changes)**
- **Securing and isolating access to target systems via a session manager**

Traditionally, organizations lean on multi-factor authentication (MFA) solutions as a primary technology in their approach to PAM. If not implemented properly and maintained, the MFA solution can present unintended risk to the organization.

[1] 5 Reasons to Prioritize Privileged Access Management, CyberArk, 2022

2017	2019	2021	
Equifax Attackers gain across to PII of approximately 147 million consumers.	**Australian National University** Attackers access 19 years worth of PII of staff and students.	**Verkada** A supply chain attack in which attackers access the Verkada security camera system used by hospitals, schools and prisons.	**U.S. Dept. of Veterans Affairs** Sensitive credentials to systems containing health records exposed on GitHub.

FIGURE 7: Timeline of Breaches caused when attackers exploit Privileged Access Management solutions.

Attackers have historically exploited vulnerabilities in access management solutions with a high degree of success. Notable data breaches in size and scope cite PAM vulnerabilities dating back to 2017 with Equifax where attackers gained access to personal and privileged information for 147 million consumers[2]. Followed by the Australian National University where sensitive credentials to systems containing health records were exposed on GitHub[3]. In 2021 a supply chain attack against physical security vendor Verkanda exposed access to security camera systems used by hospitals, schools, and prisons[4]. Finally, in 2022 the U.S. Department of Veterans Affairs was victim to a data exposure of privileged account credentials by a contractor[5].

Mandiant has observed threat actors successfully bypassing MFA controls on multiple instances. In one case, Russian-based Advanced Persistent Threat (APT) groups performed MFA Fatigue Attacks[6] by repeatedly pushing second-factor authentication requests to the target victim's email, phone, or registered devices to gain access to email accounts resulting in wire fraud incidents.

In another example, Mandiant observed APT29[7] taking advantage of the self-enrollment process for MFA in an organization, which allowed anyone with a username and password to enroll a device. APT29 performed password guessing attacks to attempt to find accounts without enrolled devices and added their own.

Regardless of the organization's size or the maturity of the PAM program, security leaders should take the time to review these 7 tips when implementing PAM to help secure their business.

[2] Wallix Cybersecurity, Equifax Breach: Preventing Data Breaches with Privileged Access Management
[3] Australian National University, Incident Report on the Breach of the Australian national Universities Administrative Systems, 2019
[4] Verkanda, Summary: March 9, 2021 Security Incident Report, 2021
[5] FedScoop, VA investigates breach after federal contractor publishes source code, September 2022
[6] Mandiant, Suspected Russian Activity Targeting Government and Business Entities Around the Globe, December 2021
[7] Mandiant, You Can't Audit Me: APT29 Continues Targeting Microsoft 365, August 2022

01

Understand Privileged Accounts

Security and IT leaders are often asked, "What is a privileged account?" While the generic answer is that all accounts may have some level of privilege, following are several categories of accounts that provide higher privileges:

- **Domain Administrators:** Users that have full control over a domain.
- **Personal Privileged Accounts:** User accounts with more privileges than a regular user. Users utilize this on a case by case basis.
- **Default Accounts:** Accounts created automatically by the system or application (e.g. SA, Root, mysql, ec2-user).
- **Service Accounts:** Accounts that are assigned to machines and provide access to corporate systems, services and applications.
- **Root, Super Administrator, or Global Admin (Cloud):** Additional administrator accounts for a system that grants user full control over the local device.
- **Break-glass Accounts:** Accounts used to gain access to systems in the event of a security incident.
- **Security Accounts:** Accounts used by security personnel to access systems to perform security audits and investigations.

It is important to understand the risk associated with the misuse of accounts that provide privileged access. Start with least privilege to ensure that each user is only able to perform the actions defined by their role.

Pay special attention to roles that access personally identifiable information (PII) or intellectual property (IP).

Actions to take

- Perform a risk assessment of privileged access within your organization. Identify accounts for both humans and systems that present risk to critical assets and information. Consider the types of permissions, including identification procedures such as interactive logon. Prioritize the high-risk PAM accounts.
- Get buy-in from senior and executive management to drive the implementation of tools that are going to reduce the overall risk within an organization.
- Ensure that security and information technology teams collaborate in the implementation to account for the needs of various user groups and the communications and change management required in PAM implementations.
- Perform recertification and validation of permissions assigned to accounts. When maintaining this account, it should not change, if there is a new use case then the right type of account should be created, or a time limited policy for access should be granted, following the right approvals.

02

Establish a Continuous Process for Account Creation, Discovery and Onboarding

As PAM is implemented across an environment, PAM teams should be proactively addressing security gaps within the organization. A critical aspect of this effort is to onboard all necessary accounts that have been identified by application teams and any implications of managing these accounts through the PAM solution are understood.

Failing to onboard all necessary accounts can result in the proliferation of unsecured privileged accounts, leaving an organization vulnerable. Attackers can exploit these accounts to gain access to your systems, elevate privileges, move laterally, and establish persistence.

The problem of unsecured privileged accounts is particularly challenging when new accounts and services are added to an environment. These additions further increase the attack surface and scope of discovery for privileged accounts, exacerbating the risk of a security breach.

By maintaining a comprehensive inventory of all old and new accounts within an environment, organizations can quickly identify which accounts are at risk during a security incident. This helps to secure those accounts, identify the systems they have access to, and create trusted routes for accessing critical assets. This can alleviate the pressure on your security team, incident responders, and incident managers when responding to security incidents.

Actions to take

- Onboard accounts when they are created and avoid increasing the 'Discovery Scope'
- Use discovery tools to identify accounts that have been missed, onboard them, and implement effective controls to manage the account's lifecycle.
- Understand the scope of privileged accounts. Consider where Intellectual property, PII or PHI is stored, and how it is accessed.
- Establish a continuous process for account discovery. Work with the teams to adopt automation for creation, discovery and onboarding.
- Leverage the MITRE ATT&CK® framework to review dozens of commonly abused adversary techniques used in privilege escalation attacks.

03

Ensure Proper Access Controls for the PAM Implementation

PAM is designed to protect the keys to the kingdom. Therefore access to PAM solutions should be managed as these user accounts and systems can become targets.

Authorizations for PAM administration should not be linked to the directories it is protecting. Use the PAM tool's built in Directory to manage this access.

Also consider the workflow for authorization. This control improves the ability for the organization to defend against insider threats, and helps the PAM team to understand how to control the system implemented for PAM.

Actions to take

- Onboard these types of accounts
  - PAM Tool administrators
  - Application accounts
  - Server accounts
  - Automation and Scripting
- Review the Access Model for using the PAM solution and identify toxic combinations of privilege.
- Make sure the administration accounts for the PAM solution are correctly permissioned, limiting access to the credentials the application secures.
- Set up authorization and access workflows to secure critical accounts.
- Enable your teams with essential security knowledge to continuously improve the organization's security posture through training, enablement and support from experts.

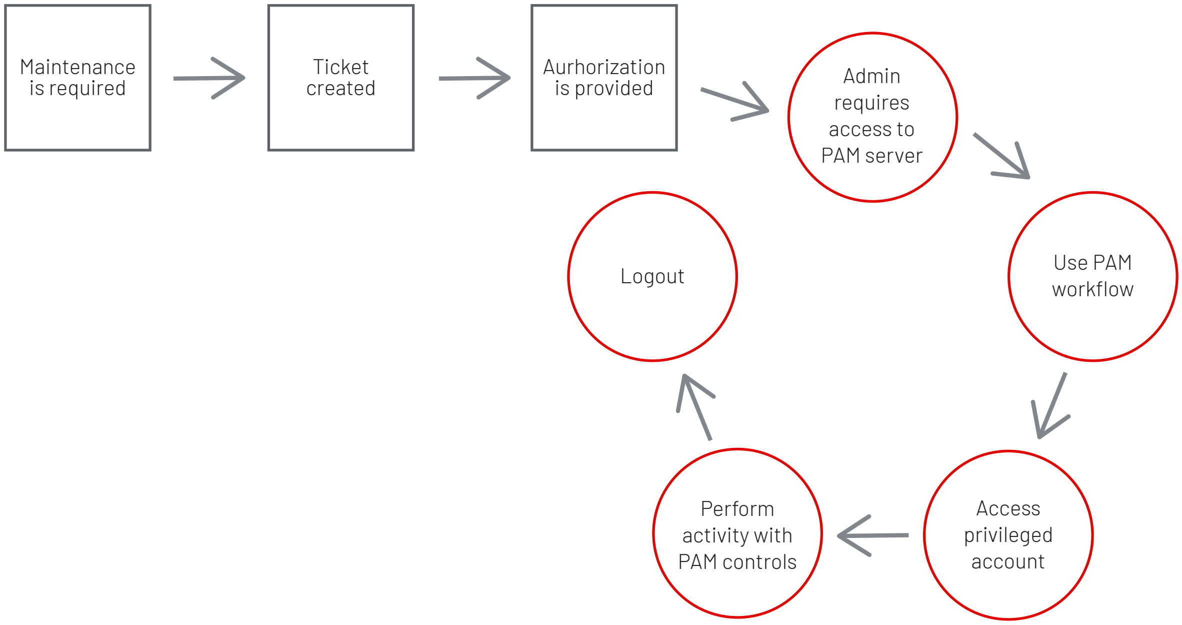
Maintenance is required
Ticket created
Aurhorization is provided
Admin requires access to PAM server
Use PAM workflow
Access privileged account
Perform activity with PAM controls
Logout

FIGURE 1: PAM authorization workflow

04

Map and Secure Access Routes

When accessing assets within the organization there are key activities to secure privileged access. One action is to avoid letting passwords become exposed on an endpoint system. There are also considerations of what happens between the user and the target system.

Is traffic being sent through or across a trusted path?
How can this be enforced?

Other questions to ask include:

- Does the connection involve a web resource?
- Is the web resource being connected to directly from a workstation?
- Is HTTPS being used for connections?

Understanding the flow and path to targets helps to calculate the risk of a threat. How applications are accessing secrets and how those secrets are used between applications and servers should also be considered.

Actions to take

Create a map of access within the environment, and check that the architecture maps to what is provided with the PAM tools.

- Identify the secure protocols that should be used and identify the routes that must be taken to gain access to session managers and targets.
  - Connect over HTTPS instead of over RDP
  - Consider using a reverse listener to keep NACL's clear and only allow outbound access.
  - Establish a credential and access tiering model.
- Make sure third parties are secured with secure authentication mechanisms and authorization has been correctly provisioned.
- Confirm that third parties are connecting over a secure method.
- Identify access routes:
  - Path through internal and public networks
  - Clean source systems
  - Strong access tiers
  - Credential protection
  - Test access routes

05

Implement Logging with Adequate Retention

Logging and monitoring provide valuable information that is critical in the aftermath of a cyber attack. Logging and monitoring aim to assist in identifying the scope and impact of a cyber incident. Forensic investigators use log sources to answer many questions during a cyber incident. For example, in order to identify data exfiltration, forensic investigators rely heavily on firewall or netflow log data. These logs can answer questions around data exfiltration and how much data has left the network. Another example involves tracking user activity. If a privileged account is compromised, logging can help track down actions performed by that user.

Actions to take

- Implement a logging and monitoring solution that captures privileged accounts activities across the organization.
- Ensure adequate log retention: Develop a logging and monitoring policy which outlines the types of activities that need to be logged and the retention for those logs.
- Confirm that log data is being sent to appropriate systems, but more importantly that the data is being used to enrich defenses within the organization. Security teams can leverage threat analytics to further improve the controls that have been put in place, and as indicators of a threat actor landing within the environment.
- Look for anomalies of user activity including system access.
- Understand the plan of action when an incident occurs. Create a plan to review the audit logs and data if not storing these in a SIEM.

06

Implement MFA

Multi-factor authentication (MFA) is important to prove digital identity and secure access to a system via a single actor or entity.

MFA requires users to provide multiple authentication factors to access an application. Two of the most common forms of MFA are one-time passcodes (OTP) and push notifications. OTP are codes that users receive on their mobile devices through MFA applications (e.g. Google Authenticator), which can be used to authenticate. Push notifications send a notification to a user's mobile device to approve or reject a login attempt.

Both of these methods are vulnerable to phishing attempts or man in the middle attacks. Recent attacks have shown that MFA push notifications, or SMS delivered codes are not enough to protect access. For example, an MFA fatigue[8] attack occurs when threat actors bombard a user with push notifications in hopes of the user getting frustrated and hitting accept.

Actions to take

- Implement strong and phishing resistant MFA
  - FIDO2 authentication by using biometrics or hardware keys (e.g. YubiKey)
  - Use challenge response mechanisms that do not simply allow accept (number matching)
- Conduct employee-wide training to ensure employees have the knowledge available to utilize MFA correctly
- Introduce alerting and risk-based tagging against accounts that seem to be under attack
  - Geo-location
  - Abnormal hours of access
  - Excessive requests for MFA challenge response
- Review the authentication assurance of the authenticators being used
- Perform threat hunting against these identities

[8] Mandiant, Suspected Russian Activity Targeting Government and Business Entities Around the Globe, December 2021

In Conclusion

As more enterprises move towards implementing PAM solutions to enhance their security posture, it is critical that these tools are appropriately configured and implemented. Misconfigurations, lack of appropriate access management and not fully utilizing built-in capabilities are some of the key factors that can result in creating a false sense of security and, in some unique cases, may result in increasing enterprise risk.

Read more articles from **The Defender's Advantage Cyber Snapshot**.

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Mandiant is a recognized leader in dynamic cyber defense, threat intelligence and incident response services. By scaling decades of frontline experience, Mandiant helps organizations to be confident in their readiness to defend against and respond to cyber threats. Mandiant is now part of Google Cloud.

MANDIANT®
NOW PART OF Google Cloud