WHITEPAPER

Fundamentals of privileged access management

imprivata®

Having a successful privileged access management (PAM) strategy is more important than ever. With cybersecurity threats on the rise, companies that control and manage privileged access reduce their risks. Yet, some companies believe privileged access management is too complicated and out of reach. But it doesn't have to be. With the right approach and tools, companies can simplify their PAM implementations while improving their overall security.

Many companies jump right in to PAM software implementations without establishing a clear process or strategy. When this happens, it's easy for PAM to get complicated, run over-budget, and frustrate IT and security teams.

The key to implementing privileged access management strategies and software is understanding that it's a journey. You can't run before you walk. Starting with a clear vision and process allows companies to move through the different stages of PAM maturity. Beginning with the PAM fundamentals and moving to advanced capabilities helps set companies up for success.

Discover, track, and secure all privileged accounts

You can't secure what you don't know about. Privileged access management begins with discovery. You need to identify and find all privileged accounts. This includes accounts used by privileged users (people) and by machines, IT systems, or cloud software for intercommunication. Everything from admin, domain, network, local, active directory, cloud, emergency, and service to application accounts must be uncovered and tracked. Privileged accounts left at factory setting or unsecured, even for a short amount of time, creates unnecessary risk.

Once accounts are discovered, you can take inventory of them to understand what they access and what type of resource it is. Do the accounts contain sensitive information such as PII or PHI and need privileged access? Gathering this information allows you to set governance policies around the privileged accounts and determine actions to secure the accounts.

Discovery can be challenging to do manually. Companies are managing thousands of privileged credentials used by people, machines, or IT systems. As companies embrace digital transformation, new IoT devices and cloud software are added to the network. Manual processes make it impossible to effectively discover and track all credentials at scale.

Privileged access management software can simplify discovery by allowing you to run discovery queries across your entire network to identify and track privileged accounts and their configurations. This allows you to manage the accounts, remove or clean up accounts, and determine how to secure them.

Remember, this step needs to be done continuously. Your company, employees, and systems are always changing. Discovery is not a one-time task. It needs to be done on a regular basis to onboard new accounts and offboard others. PAM software can be scheduled to automatically discover and report new records at set intervals so they can be quickly put under management.

You can't secure what you don't know about.

Control access

With privileged credentials identified, companies can begin to control access to those resources. The goal should be to implement the principle of least privileged which is designed to restrict a user's access to just the resources required to do their job. To achieve this, companies should begin with the PAM basics, such as securing accounts in an enterprise password vault and setting up password policies.

Securing your network means having visibility into how systems and data are accessed, by whom, and how they are changed.

Unlike basic password vaults which are used for personal passwords, enterprise vaults are designed to handle all types of privileged credentials and secrets. They provide the enhanced security, control, and visibility required to lock down sensitive credentials.

At this stage, many companies need to identify and prioritize which type of privileged credentials they want to implement and control now, and which can be captured later. Often times, companies begin with privileged users accounts then move to service accounts and application-to-application accounts.

This can vary, however. Companies that have numerous third-party business partners, and/or contractors, may prioritize remote access control earlier in their PAM journey. Or some may prioritize controls over software-as-a-service (SaaS) if they rely on a cloud infrastructure.

As companies progress in their implementation of PAM, they can move towards a just-in-time privileged access model which limits the time a privileged account exists on a critical system. It limits the time a privileged user has to access systems and eliminates accounts and access during idle times.

PAM solutions allow companies to create and enforce access management policies for privileged accounts (users and software) with parameters like time of day, physical locations (as determined by IP address), days of the week (workdays), or other combinations. Each account needs specific justification/approvals for accessing the target system or sensitive data for a set length of time. With policy-based controls, you make sure that a user or system only has access to the target system/data they need, for a limited time and nothing else. The goal is rightsizing each privileged account to a specific task.

Governance and auditing

Securing your network means having visibility into how systems and data are accessed, by whom, and how they are changed. Monitoring privileged activities are fundamental to any PAM strategy. The ability to record and playback sessions in the future is essential to being able to learn about user behaviors, comply with industry regulations, or investigate incidents.

Companies should retain 12 months of logs and session activities for auditing and forensics. On average, it takes companies anywhere from six to eight months to discover they have been breached.

Privileged session managers are designed to record, monitor, replay, search, and report on all actions taken during a privileged session. Depending on the session this might include video recording, text input, keystrokes, or some combination. Look for a PAM solution that provides full session management capabilities while making it easy to quickly search and review activity. This is essential – otherwise IT and auditors could spend hours reviewing sessions.

When it comes to implementing session managers, the goal should be to monitor all privileged sessions and review all human-driven privileged activity. If you are constrained by resources, prioritize reviewing higher risk sessions that involve access to IP, PII, etc. or high-risk users such as third-party partners and contractors.

More advanced session manager capabilities include setting up alerts to notify managers of suspicious activity. This might include privileged access that bypasses PAM tools, abnormal times and locations, changes in frequency, or accounts accessing resources they don't normally access. These sessions can then be reviewed or terminated in real-time.

Companies should retain 12 months of logs and session activities for auditing and forensics. On average, it takes companies anywhere from six to eight months to discover they have been breached.

Automation

The last fundamental of PAM is automation. A PAM solution can automate simple and repetitive tasks, which offers real value to IT administrators, freeing up time and resources to focus on high-value tasks. This includes automating password-related tasks such as resets and automating alerts to notify administrators of password requests or web application transactions. Other areas for automation include configuration changes, software installations, log management, and startup and shutdown processes.

Leveraging PAM software as part of a larger identity and access management strategy is a best practice and helps automate user provisioning.

Once basic PAM functionality is implemented, companies can integrate PAM into their larger IT and security strategies. Leveraging PAM software as part of a larger identity and access management strategy is a best practice and helps automate user provisioning. Advanced automation capabilities allow companies to move beyond basic PAM functionality to just-in-time access and zero trust strategies.

Privileged access management is a journey

Companies that jump headfirst into privileged access management can quickly get overwhelmed and frustrated. Whether you are moving from manual processes or legacy PAM solutions, it's important to establish a process and clear goals. Remember: PAM is a journey. Start by identifying your most important priorities and implementing core functionality. From there, it is easy to expand on privileged access strategies in a way that supports your needs, requirements, and budget.

Imprivata Privileged Access Manager

Discover how Imprivata solutions can help you simplify privileged access management and grow with you.

Imprivata Privileged Access Management addresses critical security and compliance challenges by controlling access to all types of privileged accounts and credentials. What's more, it combines privileged account management, session management with recording, job management, a secure enterprise password vault, and multifactor authentication to deliver a comprehensive, enterprise PAM solution that is affordable and easy to maintain.

Contact us today for a demo and learn how we can help you on your PAM journey.

imprivata®

Imprivata, the digital identity company for healthcare, provides identity, authentication, and access management solutions that are purpose-built to solve healthcare's unique workflow, security, and compliance challenges.

forward® advantage

Why choose Forward Advantage as your Imprivata Privileged Access Management Reseller and Deployment Partner?

With more than 25 years of healthcare experience and a deep understanding of clinical workflows, Forward Advantage offers an exceptional customer experience from purchase through implementation and beyond. Our professional services are customizable to meet each customer's unique needs so you and your providers can spend more time on what really matters: improving patient health.

Let Forward Advantage help make your goals a reality. Talk to one of our solution experts today!

877.636.7927
info@forwardadvantage.com

www.forwardadvantage.com
7255 N. First Street, Suite 106, Fresno, CA 93720

PAM-WP-fundamentals-0921