ManageEngine
PAM360

Password and privileged access management for enterprises and managed service providers

Richard Edwards

www.manageengine.com/pam360

To reduce employee password fatigue and help reduce cybersecurity threats, organizations large and small are starting to invest in password management tools while also exploring passwordless strategies from companies such as Google and Microsoft. But what about the IT department? How can you, as an IT professional, eliminate weak, reused, or leaked passwords across the myriad devices, servers, systems, and services that are in use across your company? And if you already have a password management system in place, is it helping you control, monitor, audit, and protect privileged access to other sensitive digital assets, like SSH keys, digital certificates, license keys, and virtualized IT infrastructures?

Moving beyond password management

Take a moment to perform a quick mental audit of your corporate environment. It's likely that passwords and credentials are shared everywhere—for example,the company's Twitter and Facebook account credentials. Now, let's take this a step further and consider how privileged access to your most sensitive systems is managed. Hopefully, you'll start to see how the security and operational efficiency of your IT department could be enhanced and improved with better tools and mechanisms, and the same goes for other business functions too, such as HR, Finance, and Marketing.

If you work in a large enterprise, your team likely spends a lot of time is dealing with the diversity and complexity of your organization's business-critical computing infrastructure. For many companies, critical infrastructures extend way beyond IT, with assets, systems, and networks that provide services, functions, and utilities necessary for our modern way of life, from generating electricity to supplying clean water. If this sounds like your environment, then you need to consider the benefits that a privileged access management (PAM) solution can provide.

Protecting your crown jewels

Another way of thinking about privileged passwords is to consider them as keys to your organization's digital crown jewels. Holding these credentials means you have virtually unlimited access and full control of IT and other resources. Your organization will have hundreds, if not thousands, of privileged credentials, many of which are used and shared across your IT environment.

Privileged accounts are used to fix faults, apply patches, and perform operational business duties. But how are privileged credentials stored? I've asked this question many times, and typical responses include text files (both encrypted and unencrypted), spreadsheets, printouts, home-grown tools, and the office safe. That last one is interesting, as what use is a master password list if you can't get at it during a time of a pandemic or other disaster?

Shared credentials grants users a level of anonymity, which can lead to misuse with relatively little traceability. IT passwords don't usually belong to individuals, so by definition this makes them shared. Using privileged passwords in an unmanaged way will inevitably lead to security threats and data breaches, so deploying a PAM solution immediately puts the business-critical credentials in a much safer place while still permitting authorized shared access.

Eliminating chinks in your cybersecurity armor

As IT professionals, we're familiar with consumer-oriented password management tools, particularly those that have gone on to develop functionality that IT teams find useful. However, these products are still associated with web browsers, websites, and the management of online credentials. For system administrators, operations managers, and developers, credentials are also required for line-of-business applications and customized on-premises IT systems. And then there are terminal-based logins to consider—Windows RDP, SSH, and Telnet sessions—and digital assets such as virtual machines and containers.

The security of your organization, especially during this COVID-19 pandemic, depends on the daily decisions and choices made by staff within its employ. It's important to preserve the confidentiality, integrity, and availability of corporate systems and customer data, but if you consider the many ways in which passwords and account credentials are used and managed, particularly in the IT department, you'll spot a few chinks in your cybersecurity armor. So, how do you tighten up security?

PAM products provide a centralized password vault for all the managed password-policy-controlled resources and personal logins in IT. A PAM solution can securely manage employee credentials, accounts, services, and applications that have privileged and elevated permissions to business-critical resources and systems.

Spotting unusual behavior during unusual times

Enterprises usually have audit and IT security teams, so consider their needs and requirements as you explore PAM solutions. If your organization uses an "audit by exception" approach, the changes and reconfigurations implemented by the business to respond to COVID-19 will have triggered many alarms. But how do you spot unusual behavior during unusual times?

Enterprise IT systems are no longer confined to the corporate network, but IT operations and administration functions are often restricted to on-premises locations, such as a datacenter using a highly managed PC or admin console. Extending these functions beyond the corporate firewall requires a trusted user utilizing a trusted device in a trusted location over a trusted connection. But who's keeping an eye on trusted user sessions?

Privileged session management is essential in a PAM solution. Advanced PAM solutions provide one-click connections to remote hosts through secure, password-less gateways. The user is assigned just-in-time privileged access with the system automatically revoking permissions after a set period. These sessions can also be remotely monitored and recorded with playback capabilities for audit purposes.

Advanced PAM solutions are starting to use AI and machine learning to provide privileged user behavior analytics. However, IT security management requires a holistic approach, so you'll need to consider things like integration with your security information and event management tools, and business/industry-specific auditing and reporting requirements.

Managing privileges in a dynamic, complex, services-centric world

IT professionals may have greater tolerance when it comes to using sophisticated software, but IT security must be kept simple to avoid error and confusion. No one wants something getting in the way of the job at hand, so a PAM solution should ideally speed-up IT management processes rather than slowing them down.

Different PAM solutions address the challenge of efficacy in a variety of ways, typically combining the idea of a centralized vault (encrypted database records) with workflow, automation, and audit facilities, but pay particular consideration to the following capabilities as you prioritize your requirements:

- Automatic discovery and onboarding features, especially for large and complex estates, to rapidly secure privileged accounts.

- Use of one-click connections and just-in-time privilege elevation to minimize privileged credential exposure, reduce risk, and simplify operations.
- Real-time monitoring and recording of privilege user activity to address audit requirements and support rapid assessment of future investigations.
- Privileged user behavior analytics to identify activity that could adversely affect IT systems and prove harmful to the business.
- Role-based access control and workflow approval to support third-party access requests, such as service providers and contractors.

About the author:

Richard Edwards

Richard worked in the IT sector for over 30 years and has a background in technology consulting, workplace modernization, process improvement and management training. His focus and attention are generally directed toward productivity and business improvement through the effective use of communication, collaboration and information management platforms.

www.manageengine.com/pam360

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.manageengine.com/pam360

ManageEngine
PAM360