WHITEPAPER

Rethinking privileged access management

imprivata®

Gartner lists privileged access management (PAM) as a top security project for chief information security officers (CISOs) that can provide immediate benefits.

But privileged users and accounts are not new to businesses or IT departments. Managers, system administrators, and IT professionals have used privileged accounts to access critical systems for years. So, what has changed to make PAM a top security project for CISOs?

While we often hear about individual user accounts getting compromised, denial-of-service attacks, or even cyber espionage in the news, they are not always the most common attacks.

74%
of breached companies say the breach involved access to a privileged account

In fact, many studies report that it is actually “privileged misuse” that is the second-most common category of attack. With the average breach taking weeks or even months to detect, the risk to your business can be substantial. This makes privileged access management a top priority for all organizations.

Executives are surprised to learn that many organizations have more privileged account logins and passwords then individual / employee logins. Privileged accounts come in many different forms from admin, domain, emergency, service, to application. Often these account logins and passwords are known and shared across teams or team members.

If a privileged account is compromised, the risk can be significantly greater as the hacker now has access to a higher level of system features and sensitive information. Not only can hackers move around your network, applications, and equipment, they can add, update, or delete settings and users, as well as create persistent backdoors into the network.

The sheer volume of privileged accounts and the sharing of credentials make it hard for businesses to manage. More importantly, it makes privileged account a big target for hackers.

Manual strategies aren’t enough

Traditionally, companies have managed privileged accounts and credentials using manual processes and password enforcement. It’s not unusual for organizations to rely on spreadsheets or a basic password manager (a bit of an improvement over a spreadsheet) to keep track of account controls. But a manual process can quickly become hard to manage and outdated. Often times, spreadsheets and password managers are not updated when new accounts are created or when employees leave and passwords need to be changed.

Relying on password policies alone can also cause you to fall short in providing advanced security to devices and servers. Longer and more complex passwords aren't sufficient protection when the account information is shared. Plus, password policies do not provide an audit trail on who is accessing your IT systems.

The changing IT landscape and rise of cloud services and applications make manual approaches even more challenging. Today, there are multiple layers of technology with an organization with HR, marketing, and supply chain managing their own specific applications or technology. This makes manual account and permissions management impossible for IT teams.

Privileged access management software

Privileged access management solutions are available and help organizations better control and monitor privileged access to anything within the network. PAM solutions help distribute user information and access controls by managing which access controls and permissions get assigned to devices and computer systems. Utilizing a central platform has the benefit of controlling all account access and permissions easily, as well as providing a central management and monitoring solution.

Gartner says that "privileged access management, is intended to make it harder for attackers to access privileged accounts as well as allowing security teams to monitor behaviors for unusual access."[1]

1. https://www.gartner.com/smarterwithgartner/gartner-top-10-security-projects-for-2018

The simple way to secure privileged accounts

Discover
Find privileged accounts on network devices: computer local administrators, factory defaults, IoT logins, router, firewall default accounts, and more.

Share
Store privileged credentials in an encrypted vault with capability to share them among team members and external contractors, as well as use them in scripts and workflows via APIs.

Rotate
Change passwords for privileged accounts periodically or after certain events so that the PAM system is the only source of up-to-date information on passwords and certificates.

Delegate
Elevate privileges of regular users for designated tasks in a managed, permissions-controlled way with audit log capability.

Connect
Let designated users establish sessions to remote computers with disclosing credentials, providing a session recording for future audit needs.

To help mitigate many of the risks, organizations face, privileged access management software features:

- **Authorized system access** | Many organizations are solely focused on blocking access to devices, servers, or systems, when, in reality, controlling who is allowed access is even more important. PAM solutions provide controls to define the applications, systems, devices, or servers that specific accounts can access as well as the approval and time allowed.

- **Just-in-time access** | Who, when, and why an IT or end user account accesses systems within the corporate network is an important part of any cybersecurity plan. PAM systems, provide just-in-time approved account and access control, ensuring that accounts only have access when needed and if and when that access is approved.

49%
of businesses do not have strong user access policies

- **No direct account access** | A PAM system ensures that all accounts are protected and hidden. Secured connections are then used, with the required or needed credentials provided through the secure credential store. If an IT administrator or end user does not know the credentials for systems, then, in the unlikely event of a phishing attack, these credentials cannot be compromised.

- **Central management** | A key factor in using a PAM solution is the ability to manage it centrally, making it easy to perform updates, management, and tasks that instantly affect any user requiring access to the account credentials or accessing systems.

- **Unalterable audit trail** | An unalterable trail log of all actions, events, and activity performed by any account is also kept, allowing for better forensics in the unlikely event of a security and data breach. Security and IT Teams can then be notified immediately of issues, as well as run reports on any account within the authentication store.

83%
of all organizations do not have adequate PAM practices to prevent breaches

Tips for selecting PAM software

$3.92 million
is the average cost of a data breach, with costs in the healthcare industry topping $6.45 million

For many businesses, PAM solutions have felt out of reach to due to cost, IT resources, and complexity. Today, that is all changing due to new modern and affordable PAM solutions. When evaluating PAM solutions, consider the follow questions:

1. How is the PAM solution deployed? Can it work on-premises or in the cloud? In physical or virtual environments? Hosted on Windows or Linux OS?
2. What is the solution's pricing model? Is it a unified pricing model?
3. How long does it take to implement? What does the client install and server footprint look like, and is it agentless?
4. Can you store and share secret data securely with credentials?
5. Can you automate tasks such as password resets and discovery for servers and network devices?
6. Does it offer a full audit trail for all privileged access and permissions? Extensive logging and reports, as well as integration into other systems?
7. Can you establish secured connections to remote devices and system?

Conclusion

A lot has changed in the security world, but one thing remains the same – compromised or misused privileged accounts are responsible for too many data breaches. It's now time for companies to rethink their manual approach to PAM. Today's PAM solutions are easy to install, affordable, and cloud-ready. PAM is one IT project that CISOs can implement immediately to significantly reduce risk, secure their networks and information, and realize a big business impact.

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-rethinking-pam-0921