WHITEPAPER

It’s time to put privileged access at the center of your security strategy

imprivata®

The world of cybersecurity is rapidly changing. As companies embrace digital transformation – cloud computing, remote work, third party applications and partners – traditional security perimeters are dissolving. What was previously safe behind a network wall is either no longer protected at all or exposed at a much higher level than before. Hackers know this and are actively taking advantage of it. Critical assets, access points and, most essentially, credentials, are more vulnerable, and it's high time organizations create a new security blueprint that puts privileged access at the center of their security strategy.

As business evolves, so do the threats

Over the last decade, we have seen a dramatic shift in how businesses operate, how people work, and the tools/technology used. We've moved into a digital age where business processes are more connected, and employees can work from anywhere in the world. But these advances come with new security risks that hackers exploit at alarming rates.

Many businesses no longer have physical offices, singular server rooms, or desktop computers protected by a single password. Instead, workers and trusted third-party partners access systems and applications from a variety of unsecure remote networks. They are more likely to use personal or mobile devices for work and overlap/interconnect personal and business-critical services in the same sessions. These networks and personal devices are less secure and increase the attack surface that a company must protect. Now more than ever, bad actors are looking to take advantage of this vulnerability to gain access to user identities through targeted phishing or malware attacks.

IT departments have had a harder time controlling and securing information and credentials using traditional perimeter defenses (castle and moat architecture) and VPNs. There are simply too many ways for a bad actor to acquire credentials despite programs to rotate, complicate, and obfuscate passwords. Once a hacker has a user's identity and credentials, they can break through the virtual wall and use that starting bridgehead to access anything and everything. They can modify, destroy, or steal your data, causing severe damage to your business reputation and putting you in violation of compliance regulations.

This legacy security approach puts you at risk. The reality is:

- 61% of breaches are **attributed to leveraged credentials**
- 51% of organizations suffered a data breach over the past year **due to poor third-party security**
- Ransomware has become the most **common attack method of third-party attacks,** responsible for 27% of breach initiations

To meet emerging security challenges, companies need to move beyond the perimeter to secure endpoints, and identity and remote access. It's time to re-evaluate your security blueprint, and put privileged access management (PAM) at its center.

CYBERSECURITY AFFECTS EVERY INDUSTRY

Healthcare

71% increase in cyberattacks targeted at healthcare

40% of healthcare IT decision-makers say their HDO is at greater risk of security breaches due to inadequate expertise in data protection

Critical infrastructure

30% of infrastructure organizations will experience a security breach that halts mission critical system operations

649 critical infrastructure entities were hit by ransomware in 2021

Manufacturing

23% of all ransomware attacks targeted the manufacturing sector

Manufacturing has the largest ransomware payout of any industry

Government

38% of local and state government employees have proper ransomware prevention training

1 in 6 government employees stated that their department has been hit by a ransomware attack

SECURING CREDENTIALS AND ACCESS

IT environments are now decentralized – every person, application, and connected device is an access point to company assets; a gateway to critical data you cannot afford to lose yet must be made readily available. To prevent attacks, you need to secure access to resources – starting with the most sensitive systems and privileged credentials.

This is where privileged access management software helps, as it's designed to manage and monitor access to systems and data. PAM falls within the identity and access management (IAM) discipline that enables the right individuals to access the right resources at the right times for the right reasons. PAM software focuses on applying additional protections on accounts with privileged or administrative rights and controlling access.

Companies have thousands of privileged credentials: these accounts are used by both privileged users and trusted third parties and by machines, IT systems, and cloud applications. Each privileged credential is an access point.

Why is this important? Privileged accounts have elevated permissions, access to confidential information, and the ability to change settings. If access is compromised, considerable damage could be made to organizational operations. And companies have thousands of privileged credentials: these accounts are used by both privileged users and trusted third parties and by machines, IT systems, and cloud applications. Each privileged credential is an access point.

PAM software works by gathering the credentials of privileged accounts into a secure repository, or password vault, to isolate their use and log their activity. This separation is intended to lower the risk of administrative credentials being stolen or misused. System admins and other privileged users must go through the PAM software and be authenticated in order to access their credentials. Users never see the actual credentials or passwords, which are kept out of view and rotated frequently with complex password variants. When users do not know the credentials being used, companies avoid the risks of poor password selection, password re-use and, most importantly, credential theft. Users can't share a password they don't know. At the same time, the PAM software logs, records, and monitors each privileged session, providing critical problem and security event management response details as well as audit and compliance data trails.

Meeting business and security challenges with PAM

Placing privileged access management at the center of security strategy addresses several business challenges.

COMPLIANCE AND AUDITING

A few years ago, PAM adoption was driven by the need to satisfy crucial controls across multiple compliance regulations and security audits – such as HIPAA, GDPR, HITRUST, PCI, SOX, NIST, and others. Targeted initially at highly regulated industries, many of these controls are being implemented at the state or national level to protect consumer data. It's now considered a best practice for companies to document how they secure, monitor, and track privileged credentials. Implementing PAM not only meets compliance requirements, it also helps to streamline and simplify the security audit process.

REMOTE WORKING

While remote working isn't new, it accelerated during the pandemic. It's estimated that **36.2 million Americans will work remotely by 2025.** Some companies are even going 100% remote. For companies, remote working can be a cost savings – less office space and overhead and access to a broader pool of workers – and for employees, it provides greater flexibility. In fact, **65% of remote workers** don't want to return to a traditional office.

The challenge is providing remote workers with secure access to company systems and resources. As highlighted above, legacy security systems aren't designed to protect expanding endpoints created by remote workers. VPNs are an aging technology that generically provide far too much access with limited logging and control capabilities for auditing. In addition, VPNs can be quite costly to maintain, especially if you try to segment them.

PAM software can be used as a remote gateway to securely lock your company's systems behind a firewall and force remote users to use the gateway to access critical assets.

THIRD-PARTY ACCESS

Most companies rely on the work of trusted third parties – outsourced workers, contractors, consultants, or even temp workers. With the great resignation and a tight labor force, reliance on third parties is growing. For example, many companies outsource elements of their IT help desk, network maintenance, and more, and these workers need elevated access to sensitive systems and data. In some cases, even heating/repair or other operational system technicians need access to networks to run diagnostics and perform regular maintenance on IoT machines/equipment that uses sensors, big data, and analytics.

PAM software and enterprise access solutions are designed to secure both internal and external users. It separates internal employee access from external access from vendors, third parties, and contractors.

Managing and securing these third-party access points isn't easy. A recent Ponemon Institute report on third-party remote access found that 54% of responding organizations lacked a comprehensive inventory of the third parties with access to their network. Furthermore, 65% said their organizations don't know which third-parties have access to their most sensitive data.

Legacy remote access methods are designed for internal users, not third-party access. This creates security gaps and prevents organizations from being able to enforce access controls, observe session activity, analyze user behavior, or leverage Zero Trust policies.

PAM software and enterprise access solutions are designed to secure both internal and external users. It separates internal employee access from external access from vendors, third parties, and contractors. You can maintain visibility over third parties, control access, set policies, limit permissions, and ensure access isn't being misused. It also helps with authentication, monitoring, and auditing.

CYBER INSURANCE

As if cyberattacks weren't enough to keep executives awake at night, they now have to contend with the cost of cyber insurance, which has become a must-have requirement for businesses. But it's increasingly harder to obtain, renew, and maintain.

Global cyber insurance rates have increased across all industry sectors by about **32% in the past year,** and one prominent insurer raised prices by almost **40% globally.** Combined with rising attacks, the Council of Insurance Agents and Brokers (CIAB) cites **poor risk management protocols and lack of employee training** among the leading causes of these dramatic cost increases.

Cyber insurance brokers now require documented evidence and a formal assessment of an organization's IAM strategy. They assess the quality of a company's risk management preparedness, processes, security controls, and tools – before determining whether to grant coverage.

Securing the best cyber insurance rate and policy coverage is about lowering your risk and the carrier's risk. To do this, insurance providers are looking for companies that leverage best practices and proven technologies, including PAM, secure remote access, multifactor authentication, single sign-on (SSO), end point protection, and identity governance tools.

Designing a PAM blueprint for success

Companies must consistently re-evaluate their security strategy to ensure it meets both changing business requirements and the evolving threat landscape. If privileged access hasn't been a core part of your strategy, it should be.

The key to implementing privileged access management is understanding that it's a journey. You can't run before you walk. A successful PAM strategy begins with these three steps.

START SMALL AND DEPLOY INCREMENTALLY

A typical organization will have more privileged credentials and passwords than individual/employee logins. Privileged credentials are on every IT asset, application, and IoT device. Add the internal and external user credentials required to access and manage the systems, plus the sheer volume of credentials? It’s no surprise that PAM implementations can seem overwhelming.

Start off small and create realistic deployment goals and timeframes. Begin by identifying the most critical assets you need to protect – put those credentials in a password vault and set password and user policies. Most companies begin with securing internal privileged user accounts and then move to service or third-party accounts and application to application accounts.

> **Start off small and create realistic deployment goals and timeframes. Begin by identifying the most critical assets you need to protect.**

Think of it as a bullseye. Start at the center and work your way out, adding more applications, groups, or capabilities. Having a phased approach allows you to set achievable goals and show value.

GET USER SUPPORT AND CREATE PAM AMBASSADORS

It’s important to remember that implementing a PAM solution is about change management. You are asking your privileged users to change their current process. If users do not adopt the new process, the overall implementation will not succeed. It's critical to involve users early in the process.

Starting with a smaller deployment usually means a smaller internal user base. This allows you to work closely with the users to establish PAM ambassadors. Once people get comfortable using the PAM solution to access credentials, they quickly see the benefit. For users, they no longer need to remember multiple credentials and passwords. With PAM software, they never see them.

Often, the ambassadors ask for PAM to be expanded to other applications and user groups. This quickly leads to broader support for PAM across the organization as users do not want to manage passwords. From a security perspective, companies can secure credentials and access points.

PROVIDE JUST ENOUGH ACCESS

Whether it’s IT admins, business users, third-party partners, or other privileged users, you want to limit access to ONLY what the users need in order to perform their jobs. It’s the difference between having a key that works on every door and one that only opens certain rooms.

This means implementing a least privileged approach and establishing strong role-based policies. The ideal goal is rightsizing each privileged account to a specific task.

PAM software allows you to create granular policies that control and limit access to resources. You can use parameters like time of day, physical locations (as determined by IP address), days of the week (workdays), or other combinations. With policy-based controls, you ensure that a user or system only has access to what they need, for a limited time and nothing else.

Least privilege is a component of a Zero Trust network access strategy that focuses on ‘never trust and always verify’ user access. Zero Trust and least privileged approaches block threats by limiting access and minimizing attack surfaces.

Take back control

When you put privileged access management at the center of your security strategy, you can improve security for critical assets, address remote access concerns, and meet compliance and audit requirements, all while reducing the risk of a data breach. That means streamlined, secure access for both your internal and third-party users – and peace of mind for you.

imprivata®

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

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com