KEEPER®

Next-Gen Privileged Access Management for State, Local and Higher Education Organizations

A global survey of IT professionals found that 87% of respondents would prefer a “pared down” form of Privileged Access Management (PAM) that is easier to use than traditional PAM solutions. This is especially true for public sector agencies and organizations with limited cybersecurity budgets.

KeeperPAM addresses the key pain points and requirements for Identity, Credential and Access Management (ICAM) in government organizations to prevent data breaches without the complexity or cost of legacy PAM solutions.

Privileged Access Management (PAM) solutions have historically been used by IT and software development teams to strictly control access permissions within an organization’s IT environment. Privileged accounts are a prime target for cybercriminals because they hold sensitive information, such as customer and employee data, that criminals can sell on the dark web. Additionally, if a privileged account is breached, attackers can potentially shut down critical systems and perform other malicious activities.

PAM solutions are designed to protect organizations from a variety of threats that target privileged accounts, credentials and access. Traditional PAM products, however, are expensive, difficult to deploy, difficult to use and do not monitor and protect every user on every device. Luckily, Next-gen PAM solutions have evolved to provide an easy-to-deploy and easy-to-integrate alternative. These new solutions are used by both IT departments and other functional groups in an organization to protect access to sensitive data and files, such as HR, accounting and finance teams.

Who Are Privileged Users?

Privileged users within your organization are simply individuals who have elevated access to sensitive data or systems. Think of IT administrators, for example. They can “log in” to several highly sensitive applications, systems and databases at most organizations. Because of their access, these employees are prime targets for cybercriminals who seek to compromise user accounts to deploy ransomware, extract data or perform other malicious actions. In order to mitigate the risk of a data breach, organizations need to take proactive steps to identify, manage and secure their privileged users.

What Is a PAM Solution?

Privileged access management, or PAM, systems help administrators effectively and accurately organize, manage and secure privileged credentials, so that they can restrict access to critical systems to only the individuals who need that access to perform their duties. Additionally, PAM solutions secure and store credentials for both humans and machines (machine credentials are known as secrets, and are often used by DevOps teams), manage and monitor sessions, and generate detailed audit and compliance reports.

However, PAM solutions are not ubiquitous, and even when organizations do deploy them, their cost and complexity may prevent widespread adoption. Traditional PAM solutions are deployed on-premises, meaning the software and infrastructure are hosted within an organization’s own data center. Many IT security professionals have found traditional PAM solutions difficult to deploy and hard to integrate with their existing systems. For example, some vendors use agents for many of their features or require the installation of many different server components. This leads to higher costs, as the legacy, on-prem solutions that require multiple infrastructure pieces and extensive maintenance generally also require professional services packages from the vendor.

What Is Next-Gen PAM?

Luckily, next generation PAM solutions have emerged as a cost-effective alternative that offer scalability and flexibility. They don't require infrastructure management or professional services to deploy, allowing administrators to quickly scale privileged access capabilities. These "next-gen" PAM solutions are fully-managed, easy to deploy and require minimal changes to your environment. They can also integrate with your existing tech and Identity Access Management (IAM) stack.

Modern PAM solutions cover password and secrets management, as well as session management. By combining passwords and secrets into a single, user-friendly UI, IT admins can easily manage complex policies and create detailed reporting. With session management, security teams can monitor, record and analyze privileged sessions without having to onboard any physical assets.

Traditional PAM solutions are cost prohibitive, difficult to deploy and contain unused features. KeeperPAM™ addresses the key pain points and requirements in organizations to prevent data breaches with just the features you need.

Cost Effective

A single platform with minimal IT staff required to manage it

Fast Provisioning

Seamlessly deploys and integrates with any tech or identity stack in just a few hours

Easy To Use

Unified admin console and modern UI for every employee on all device types – average training time is less than 2 hours

Understanding the Risk

Cyber threats and ransomware attacks can be crippling for public sector organizations. The cost of ransomware attacks in government often runs into the millions of dollars, which mostly stems from downtime and recovery (or in some cases, paying the ransom). Government agencies and educational institutions are often targeted in cybercrimes due to the sensitive information they have access to. Cybercriminals also know that public sector organizations tend to have smaller IT teams, budgets and resources to thwart cyber attacks.

A 2023 report on the state of ransomware noted that in 2023, the education sector saw the highest ransomware attack rate of any industry, with 80% of schools reporting a ransomware attack. Local and state government agencies are not far behind, with 69% reporting a ransomware attack.

Examples of prominent data breaches targeting government organizations are, unfortunately, not difficult to come by. For example, Clark County School District in Nevada, the fifth-largest school district in the United States, experienced a massive data breach in October of 2023, exposing the sensitive data of over 200,000 students and staff. According to a class-action lawsuit, that personal information includes student and employee records, medical information, Social Security numbers and health insurance information. The hacker group that claimed responsibility for the attack, SingularlyMD, leveraged weak passwords — in this case, students' dates of birth — and flimsy Google Workspace file-sharing practices, to access a multitude of sensitive data.

A 2023 Data Breach Investigations Report from Verizon Business notes that 74% of all breaches involve the human element, with the majority due to weak or stolen passwords.

The City of Dallas dealt with a ransomware attack in May of 2023 and was forced to shut down some of its IT systems, with a number of functional areas including the police and fire department, experiencing disruption. The ransomware group Royal gained access to the city's network using a stolen domain service account, and it has been reported that over 26,000 people had their information stolen, including names, addresses and medical information.

These examples are not meant to point fingers at any particular organization. In fact, attacks like these can and do happen to public-sector organizations of all types and sizes on a weekly basis. Instead, these examples are meant to illustrate the need for increased cybersecurity measures.

Every organization needs to secure its passwords, credentials, secrets and connections to reduce the risk of cyber attacks and defend against internal and external threat vectors.

Understanding the Limitations of Legacy PAM Solutions

1. **Legacy PAM solutions are deployed on-premises.** The complexity and high cost of legacy on-prem PAM solutions create challenges for IT and security professionals. One key challenge is that 85% of organizations require a dedicated staff to manage and maintain their on-premises PAM solutions– an unjustifiable expense as budgets tighten in the public sector.

2. **Legacy PAM solutions require professional services to configure and integrate**. It can take several months to configure and deploy a complex, legacy PAM solution. Several traditional PAM solution providers charge costly implementation fees and "professional services," adding to the cost of an already expensive solution. Adding integrations, such as identity and access management and Security Information and Event Management (SIEM), can also add expensive fees to a deployment.

3. **Legacy PAM solutions are designed for engineers and do not work well for less-technical employees.** In today's hybrid workplace, the network perimeter has expanded beyond the office, and the number of devices and accounts that need to be protected has increased dramatically. When multiple departments have dozens of systems they regularly log in to, this results in a sprawl of administrator privilege that is hard to track and increases the risk of a compromised account. Traditional PAM solutions are designed for engineers and IT professionals, but generally do not protect other types of accounts that hold sensitive or confidential information.

Understanding Next-Gen PAM

Next generation PAM solutions take a holistic approach to protecting privileged accounts. Rather than having multiple on-prem solutions from multiple vendors to address password and session management, next-gen solutions address the core components of PAM within a unified platform that is both cloud based and fully managed. This includes credential vaulting and access control, secrets management and privileged session management.

The benefits of simplified, next-gen PAM solutions:

1. **Cloud based.** PAM solutions based in the cloud are agentless and clientless, meaning they don't require installing dedicated software agents on individual endpoints. Public sector organizations choose cloud-based PAM for its scalability as well as operational efficiency in reducing maintenance time and cost. Maintenance for patches, upgrades and the rollout of new features is done by the provider and included in the cost.

2. **Protects all users.** While PAM focuses on users and accounts that pose a higher security threat and data breach risk by having privileged access, many of these users and accounts do not reside in the IT department. Next-gen PAM is "PAM for everyone" and is an easy way for employees in HR, legal, finance, accounting and marketing departments to securely share logins to accounts, access secure files, and configure access when onboarding or offboarding employees.

3. **Easier to use and deploy.** Being agentless, cloud-based PAM solutions are easier to deploy and manage as they don't require installation on each endpoint. An agentless approach allows for easier scaling and adapting when there are changes to an organization's IT infrastructure. Initial setup can be done in a day vs months for traditional solutions.

4. **Secure and cost-effective.** Cloud PAM solutions provide a very secure way to protect passwords, credentials, secrets and connections, especially if the solution utilizes a zero-trust framework and zero-knowledge security architecture. The significantly reduced upfront and operational costs of cloud-based PAM makes it an ideal choice for public sector organizations who do not need an expensive legacy PAM solution.

A global survey of 400 IT and security executives conducted in January 2023 revealed a desire for simpler PAM solutions, with 87% of respondents saying they would prefer a "pared down" form of PAM that is easier to deploy and use than legacy PAM solutions.

KeeperPAM™ for the Public Sector

Keeper Security Government Cloud (KSGC) Password Manager and Privileged Access Manager is FedRAMP Authorized and StateRAMP Authorized and maintains the Keeper Security zero-trust security framework alongside a zero-knowledge security architecture, so users have complete knowledge, management and control over credentials and encryption keys.

Safeguard Against Ransomware Attacks.
Mitigate risks that lead to breaches by providing real-time protection and access to applications, systems, secrets and IT resources.

Save Money and Time with Quick Set-Up.
Easy, fast and affordable to integrate and deploy for organizations, departments and agencies of any size with world-class customer support.

Powerful Security Insights.
Provide analytics into credential security and hygiene across all endpoints and systems with native SIEM integration.

Robust Compliance and Reporting.
Simplify and strengthen auditing and compliance with support for RBAC, 2FA, FIPS 140-2 encryption, HIPAA, FINRA, SOC, ITAR and more.

Public sector organizations need a way to protect privileged accounts that is highly secure, easy to deploy and cost effective. Keeper's next-gen, zero-trust and zero-knowledge PAM solution protects organizations of all sizes - from small municipalities and institutions to large state agencies and college campuses.