KEEPER®

The Hidden Dangers of Legacy PAM

Why Your Security Solution May Actually Be a Risk

By James Scobey, CISO | Keeper Security

As a former federal CISO who has spent decades designing and securing enterprise infrastructure, I've grown increasingly concerned as organizations continue to rely on legacy **Privileged Access Management** (PAM) solutions designed for a different era.

These systems, once the gold standard in security, have become dangerous liabilities in today's modern cloud-native world. Let me explain why your legacy PAM solution isn't just ineffective — it's actively putting your organization at risk.

The perimeter-based security fallacy

The fundamental problem with legacy PAM solutions lies in their architectural DNA. These systems were built for an era of clear network boundaries, where a strong perimeter was enough to keep threats at bay. In today's environment of hybrid clouds, remote work and interconnected systems, this model isn't just outdated — it poses a significant threat.

> **"We continue to cling to the idea of 'trusted' and 'untrusted' networks bound by security controls. Keeper facilitates a perimeterless environment by protecting secrets and passwords throughout the lifecycle, wherever they are."**

Consider a typical federal legacy PAM deployment: It requires opening numerous firewall ports (443, 80, 8080, 22, 23, 1434) just for basic functionality. Each port represents a potential entry point for attackers, creating "Swiss cheese security" — a perimeter full of necessary holes that can compromise the enterprise.

In contrast, modern solutions like **Keeper** operate on a **zero-trust model**, where every access request is authenticated and encrypted at the device level, eliminating the need for permanent firewall openings.

The implementation nightmare

What keeps me up at night isn't just the architectural weaknesses — it's the reality of how these systems are used. In my experience, I've consistently seen organizations implement only 20-30% of their legacy PAM solution's capabilities. The reason is simple: these systems are so complex and cumbersome that full implementation becomes practically impossible.

This partial implementation creates a dangerous false sense of security. Organizations believe they're protected because they have a PAM solution, but they've inadvertently created a shadow IT nightmare. When users find the official system too cumbersome, they devise workarounds — storing passwords in unauthorized locations, sharing credentials through unofficial channels and creating unmonitored admin accounts "just to get the job done."

The cloud-native disconnect

The most critical failure of legacy PAM solutions is their inability to support modern cloud-native operations. These systems were never designed for the dynamic nature of today's infrastructure, where containers spin up and down in seconds, and infrastructure is defined by code rather than hardware.

> **"Unimplemented features in your legacy PAM solution increase your attack surface and make your enterprise less secure. Capability bloat is a bug, not a feature."**

The impact is severe: DevOps teams, faced with PAM solutions that can't integrate with their CI/CD pipelines or handle dynamic secret injection, often bypass security measures entirely.

Modern solutions address this through API-first designs and native integration with development workflows. For instance, Keeper's Secrets Manager provides zero-knowledge encryption while seamlessly integrating with CI/CD pipelines. It allows for automatic secret injection and rotation without compromising security or development velocity.

The zero-trust imperative

In today's threat landscape, the assumption of trust once inside a network perimeter is a luxury we can no longer afford. Legacy PAM solutions, however, continue to operate on this outdated principle. Once users authenticate to the PAM system, they often gain broad access with limited ongoing verification.

Modern security demands a zero-trust approach where every access request is authenticated, authorized and encrypted. This requires implementing record-level encryption, device-level security and continuous validation of security posture. For example, **Keeper's architecture** ensures that each stored vault record is individually encrypted using AES-256 Galois/Counter Mode (GCM), with encryption and decryption occurring locally on the device — never in the cloud or on central servers.

The compliance quagmire

The compliance implications of legacy PAM solutions are becoming increasingly problematic. As regulatory requirements evolve to address modern threats, many legacy systems struggle to provide the necessary controls and visibility. Their logging and audit capabilities often miss critical access events, making compliance validation a manual and error-prone process.

Modern PAM solutions address this with comprehensive logging and reporting capabilities that integrate directly with SIEM systems. For instance, Keeper's advanced reporting and alerting features provide detailed audit trails of all access attempts and changes while maintaining zero-knowledge encryption to ensure data privacy. Keeper is FedRAMP Authorized and helps organizations strengthen auditing and compliance with support for Role-Based Access Control (RBAC), Two-Factor Authentication (2FA), FIPS 140-3 encryption, HIPAA and more.

Zero-knowledge architecture reimagined

Modern PAM's core is a **zero-knowledge architecture** that eliminates traditional vulnerabilities. Keeper's implementation takes this to the next level with a multi-layered encryption model.

Each vault record is encrypted using a unique 256-bit AES key in GCM generated on the client device. This record-level encryption ensures that even if one record is compromised, other records remain secure. The encryption and decryption process happens entirely on the user's device — never in the cloud or Keeper's servers.

> **"Deploying your PAM on-premise means you're trusting all the layers of infrastructure that you already know are insecure – your network, your hypervisor, your operating systems."**

This model extends further for enterprise deployments: record keys in shared folders are wrapped with a 256-bit AES shared folder key, and the record and folder keys are encrypted with another 256-bit AES key called the data key. This creates multiple layers of encryption that must be breached to access any single piece of information, preventing any lateral movement and additional compromises.

KEEPER

Authentication reinvented

Device Verification

Modern cloud-based PAM solutions integrate an essential device approval and verification step before granting user access. This additional layer of security mitigates enumeration attacks and blocks brute-force login attempts, ensuring only authorized devices are allowed to connect.

Zero-Knowledge Single Sign-On (SSO)

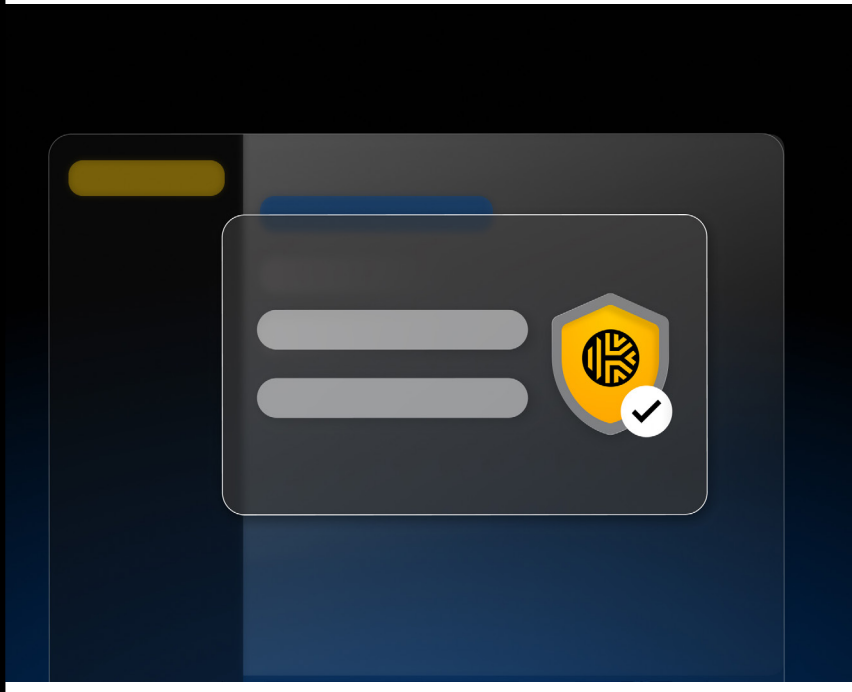
Keeper's PAM solution can seamlessly integrate with enterprise identity providers while maintaining zero-knowledge security. This is made possible through innovative encryption methods, such as the generation and local storage of cryptographic private keys. By leveraging browser-based CryptoKeys, native device keychains or secure Android keystores, advanced PAM solutions offer secure authentication without exposing sensitive user data.

Multi-Factor Authentication (MFA)

Cloud-native PAM platforms also offer robust MFA options, including FIDO2 WebAuthn hardware keys, biometrics, and **Time-Based One-Time Passwords** (TOTPs). Notably, MFA is typically performed after device verification but prior to password entry, creating a sequential, multi-layered defense system to ensure optimal protection against unauthorized access.

Real-time breach protection

Modern PAM solutions incorporate breach detection mechanisms to proactively identify **compromised passwords**. These systems often utilize separate, self-contained architectures and cryptographic processes to ensure security. For instance, client-side password hashes are processed using algorithms like HMAC_SHA512, while server-side validation occurs through Hardware Security Modules (HSMs) with non-exportable keys. By employing a "hash-of-hashes" approach, actual passwords remain fully protected and are never exposed during the breach detection process.



DevOps integration that truly works

Keeper Secrets Manager provides proper DevOps integration for development teams without sacrificing security. The implementation includes:

01

Zero-Knowledge API Access

Applications securely retrieve secrets using client-side encryption methods, such as 256-bit AES encryption in GCM mode. Each secret is encrypted individually, and all encryption and decryption processes occur locally on the device, ensuring sensitive information remains protected and confidential.

02

Secure Key Distribution

When secrets need to be shared between users or applications, Keeper uses **Elliptic Curve Cryptography**, to securely distribute keys between users and applications. This ensures that even during key exchange, sensitive data is never exposed, maintaining a zero-knowledge approach throughout the process.

03

Automated Secret Rotation

A unique gateway is installed in the customer's environment, establishing secure outbound connections to Keeper's infrastructure. This enables automated password rotation without exposing internal systems.

Session security reimagined

For remote access scenarios, Keeper Connection Manager reimagines secure session management:

01

Zero-Trust Connections

Remote sessions are established using a zero-trust model, where connections are secured through cryptographic protocols like WebRTC and protected by symmetric keys. These keys are stored securely and tied to the relevant records.

02

Secure Tunneling

For port forwarding or remote access, data is transmitted securely through encrypted tunnels, such as WebRTC connections. Sessions are protected with AES-256 encryption keys dynamically generated on secure gateways, ensuring end-to-end protection for all transmitted data.

03

Session Recording

All session recordings are protected by a unique AES-256 encryption key generated for each session, which is further wrapped by an HKDF-derived AES-256 resource key.

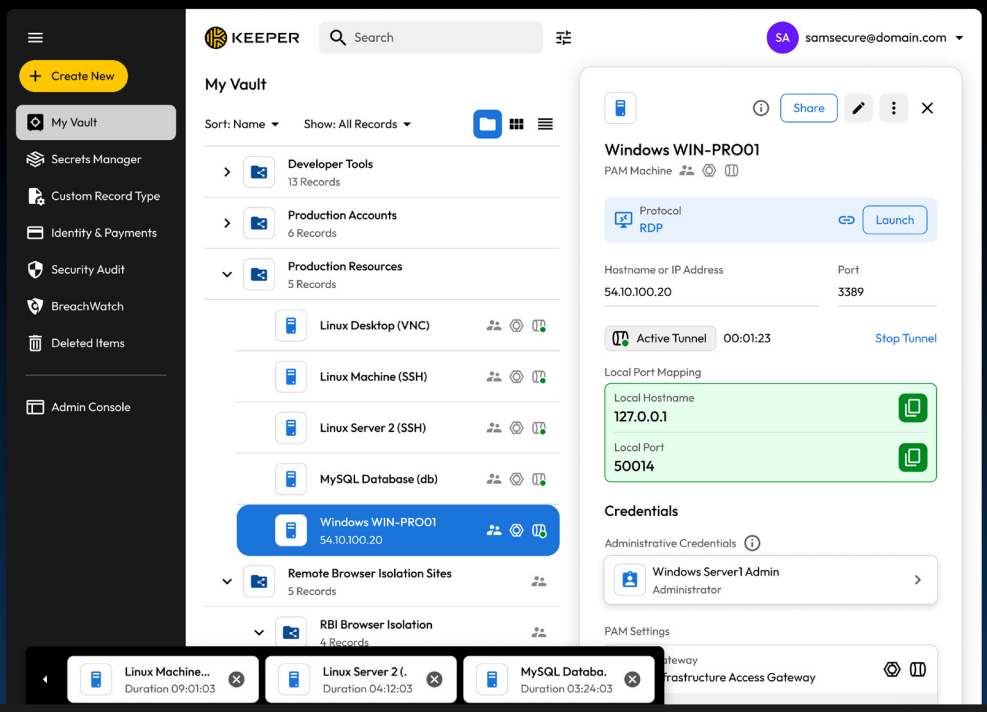
The path forward

The transition to modern PAM isn't just about adopting new technology — it's about embracing a fundamentally different approach to security. Organizations must recognize that their legacy PAM solution, far from being a security asset, may actually be a significant liability.

The good news is that solutions like Keeper demonstrate how modern PAM can provide ironclad security with seamless usability. By combining zero-knowledge architecture, device-level encryption and native integration with modern workflows, organizations can achieve true privileged access management without compromising security or user experience.

In today's threat landscape, the right PAM solution isn't just about managing privileges — it's about ensuring your security foundation enables business agility rather than hindering progress. The technology exists; the question is whether organizations will transition before their legacy solutions become their undoing.

Book a demo today to see how KeeperPAM can help secure your environment.



James Scobey, CISO

James Scobey is the Chief Information Security Officer (CISO) of Keeper Security, Inc. He previously worked at the US Securities and Exchange Commission (SEC) as a Chief Information Security Officer. Prior to his position as CISO at the SEC, Scobey served as President and Chief Executive Officer (CEO) of SigmaCyber, Chief Technology Officer (CTO) and Assistant Director of Cybersecurity Operations at the SEC, as well as Principal Systems Engineer and Cyber Performance Systems Engineer at the federally funded research and development organization MITRE. Scobey has also served in leadership and engineering roles at S2i2, Federal Data Systems, USmax Corporation, By Light Professional IT Services and SMS Data Products Group.