Data Sheet

KEEPER + FedRAMP

Why Legacy PAM Is a Risk You Can't Afford

Discover the Keeper Advantage

Today's cyber threats demand more than outdated tools — they require a modern, agile approach to security. **If your organization still relies on a legacy Privileged Access Management (PAM) solution, you're not just behind the curve — you're at risk**. Let us show you how **Keeper Security** is redefining privileged access management with an unparalleled zero-trust approach.

Outdated PAM solutions are a liability

Legacy PAM systems were designed for a world of static networks and secure perimeters. But in today's fast-paced, cloud-native world of hybrid environments and remote work, these outdated solutions leave critical vulnerabilities:

01 Gaps in security

Legacy PAM requires multiple firewall openings (ports 443, 80, 22, etc.), creating a porous network that's ripe for exploitation.

02 Underutilized complexity

Many organizations deploy only a limited number of legacy PAM features, creating shadow IT issues and a false sense of security.

03 Cloud-native disconnect

Legacy systems can't keep up with modern CI/CD pipelines, dynamic secrets management or automated secret rotation.

The result? Increased attack surfaces, inefficiency and operational bottlenecks.

Why organizations of all sizes choose Keeper

Keeper is the **zero-trust, cloud-native PAM solution** built for the challenges of today and tomorrow. Here's how Keeper solves problems that legacy PAM systems can't:

Perimeterless security with zero-trust

- No open firewall ports required.
- Every access request is authenticated and encrypted at the device level.

Seamless DevOps integration

- API-first design integrates with CI/CD workflows.
- Automated secret injection and rotation ensure secrets stay secure without slowing developers down.

Ironclad zero-knowledge encryption

- Each record is encrypted individually using **AES-256** GCM, ensuring no single breach compromises your entire system.

Simplified deployment and full utilization

- User-friendly design eliminates shadow IT and ensures every feature works out of the box.
- Teams adopt Keeper effortlessly, avoiding cumbersome workarounds.

Advanced compliance & audit capabilities

- Comprehensive logging and reporting integrate seamlessly with SIEM systems.
- Full visibility ensures compliance with evolving regulations, including GDPR, HIPAA and more.

The Keeper edge: Built for the modern era

Unlike legacy solutions patched to accommodate cloud technologies, Keeper was built for the cloud from day one:

- **FedRAMP Authorized and available in the AWS GovCloud:** High availability with global data sovereignty options.
- **Double encryption:** Data at rest is encrypted locally, while data in transit uses TLS 1.3 with an additional payload encryption layer.
- **Breach prevention:** Features like **BreachWatch**® actively monitor for compromised credentials without exposing sensitive data.

Empower your security with Keeper

When you switch to Keeper, you're not just getting a PAM solution — you're future-proofing your organization. Our platform combines cutting-edge technology, zero-trust architecture and seamless integration to ensure:

- **Reduced attack surfaces** and fewer vulnerabilities.
- **Improved operational efficiency** without sacrificing security.
- **Regulatory compliance** with the most advanced encryption and logging capabilities.

Act now before it's too late

Don't let your legacy PAM solution become your Achilles' heel. Let Keeper Security empower your organization with modern, scalable and ironclad privileged access management.

Schedule a demo today to see how Keeper can revolutionize your organization's security posture while driving business agility.

About Keeper Security

Keeper Security is a leader in zero-trust and zero-knowledge cybersecurity solutions, trusted by thousands of businesses worldwide. Learn why organizations across industries choose Keeper to protect their most sensitive data.

Your security deserves more than a legacy solution. Make the move to Keeper today.