KEEPER®

Data Sheet: Keeper Security Government Cloud (KSGC)

KSGC was created to fully protect perimeterless and multi-cloud environments with just the features you need.
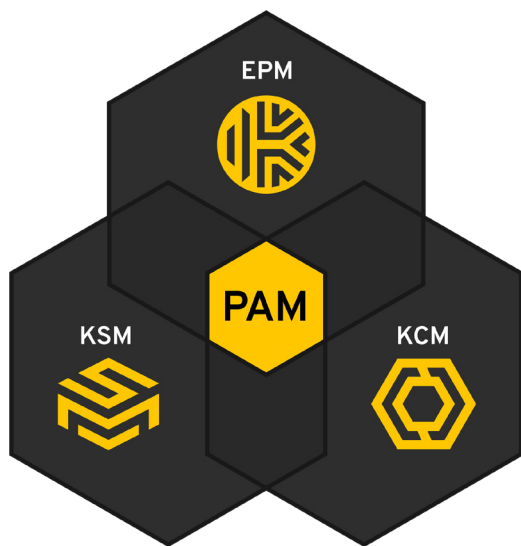
FR FedRAMP

StateRAMP

FIPS VALIDATED 140-2 FIPS 140-2

Simplified privilege management for every user on every device from every location.

EPM

KSM PAM KCM

Keeper Security Government Cloud (KSGC)

Keeper's patented PAM platform enables organizations to achieve complete visibility, security, control and reporting across every user on every device in any organization. The platform is cloud-based, enables zero-trust and zero-knowledge security and meets compliance mandates by unifying three integral solutions into one unified solution.

ⓘ 74% of breaches involve the human element - with the majority due to stolen or weak passwords, credentials and secrets.[1]

KEEPER® PASSWORD MANAGER

Enables organizations to securely manage, protect, discover, share and rotate passwords with full control and visibility to simplify auditing and compliance.

KEEPER® SECRETS MANAGER

Delivers a fully-managed, cloud-based solution to secure infrastructure secrets such as API keys, database credentials, access keys and certificates.

KEEPER® CONNECTION MANAGER

Provides an agentless remote desktop gateway for instant privileged session management, remote infrastructure access and secure remote database access to RDP, SSH keys, database and Kubernetes endpoints – no VPN required.

Reduce your attack surface to protect employees and devices.

Keeper provides the most critical components of privileged access management (PAM) without the complexity of traditional PAM solutions.

- Privileged account and session management (PASM)
- Secrets management
- Single sign-on (SSO) integration
- Password Management

- Privileged account credential management
- Credential vaulting and access control
- Session management, monitoring and recording
- Zero-Trust Security

Traditional PAM products are ugly, expensive, difficult to deploy, difficult to use and do not monitor and protect every user on every device from every location.

Reduced Operational Costs. Includes management of passwords, secrets and connections all in one platform – minimal IT staff required.

Fast Provisioning. Seamlessly deploys in just a few hours, not a few months.

Easy to Use. Provides a unified admin console and modern UI for every employee on all device types – average total training time is less than 2 hours.

Pervasive Visibility. Simplifies auditing and compliance with organization-wide role-based access control (RBAC), event logging and reporting.

World-Class Security. Utilizes best-in-class security with a zero-trust framework and zero-knowledge security architecture.

50+ Integrations. Integrates with your existing tech and IAM stack to achieve enterprise-wide coverage and visibility.

FedRAMP StateRAMP FIPS-140-2 Level 2 ISO 27001 SOC 2

PCI DSS Level 1 TRUSTe HIPAA GDPR FDA 21 CFR Part 11 Compliant