Keeper Security Government Cloud

KSGC password manager and privileged access manager is FedRAMP and GovRAMP Authorized and available in the AWS GovCloud.

FedRAMP GovRAMP

Challenges

Weak and stolen passwords, credentials and DevOps secrets are a leading cause of data breaches at public sector organizations. Unfortunately, many IT teams lack visibility into these threats and have no way to enforce security best practices across every employee, in every location, across every device, application and system. This creates a series of challenges for IT administrators.

01

Government agencies must adhere to complex rules and strict compliance mandates when purchasing third-party solutions.

02

Attack surfaces are expanding exponentially as devices, credentials and secrets are connected to distributed networks – both on and off-premises.

03

Modern ways of working with distributed remote work and multi-cloud computing have made traditional IT perimeters obsolete, increasing risk for everyone.

04

Conventional cybersecurity solutions are siloed in nature, creating critical gaps in visibility, security, control, compliance and reporting.

Public sector organizations that don't address these core challenges face a heightened risk of data breaches, compliance violations and operational friction.

Solution

Keeper Security Government Cloud password manager and privileged access manager is FedRAMP and GovRAMP Authorized and maintains a zero-trust security framework alongside a zero-knowledge security architecture. This ensures that organizations have complete management and control over credentials and encryption keys.

KSGC provides a human-centric cybersecurity solution to your team and organization. Improve your agency's cybersecurity by providing employees with a simple and effective method to adopt password security best practices like Multi-Factor Authentication (MFA) and integration with your SSO to eliminate security gaps.

Learn more
keepersecurity.com

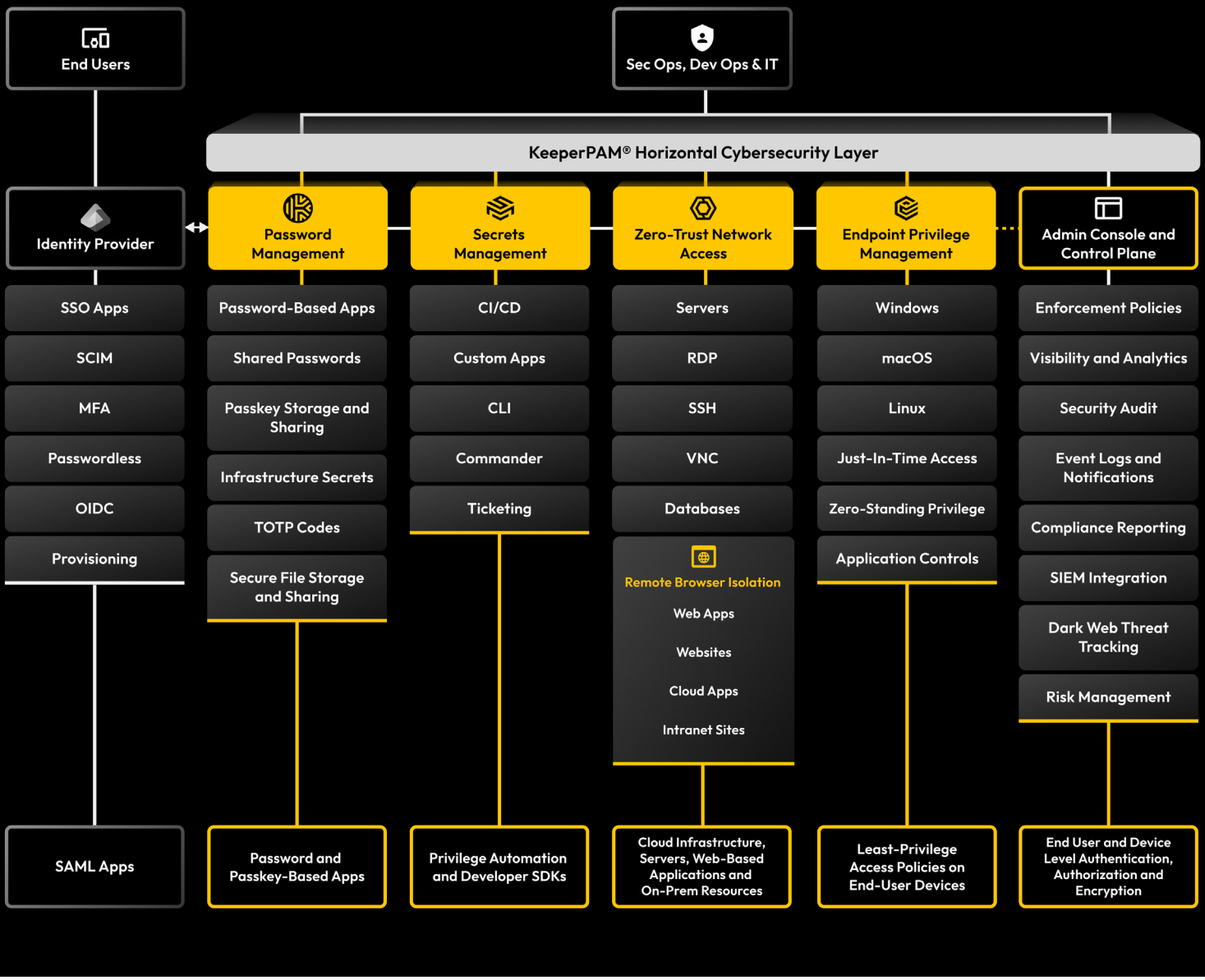
Request a demo
keeper.io/demo

About Us

Keeper Security is transforming cybersecurity for millions of individuals and thousands of organizations globally. Built with end-to-end encryption, Keeper's intuitive cybersecurity platform protects every user, on every device, in every location. Our patented zero-trust and zero-knowledge privileged access management solution unifies enterprise password, secrets and connections management with zero-trust network access and remote browser isolation.

© 2025 Keeper Security, Inc.

Keeper Privileged Access Management Platform



Organization Value

- Prevent ransomware and credential-related cyber attacks
- Protect every user on every device from every location
- Strengthen your organization with zero-trust security and policies to help meet zero-trust mandates
- Enhance and extend your existing Single Sign-On (SSO) deployment
- Provide employees with a simple and effective method for adopting password security best practices and reduce the burden of password-related tickets for your helpdesk and IT teams

Key Capabilities

- Credential vaulting and access control
- Secrets management
- Single Sign-On (SSO) integration
- Privileged account credential management
- Session management, monitoring and recording
- Smart card authentication
- FedRAMP and GovRAMP Authorized
- Industry compliance and reporting

© 2025 Keeper Security, Inc.