Data Sheet

Keeper Security Government Cloud (KSGC)

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

FedRAMP

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:

1. An organization consists of human and machine credentials that need to be protected.
2. Distributed remote work and multi-cloud computing have made traditional IT perimeters obsolete.
3. Attack surfaces are expanding exponentially as billions of additional devices, credentials and secrets are connected to distributed networks - both on and off-premises.
4. Conventional cybersecurity solutions are heterogeneous and siloed in nature, thereby creating critical gaps in visibility, security, control, compliance and reporting.
5. Government agencies must adhere to strict compliance mandates when purchasing third-party solutions

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 (KSGC) password manager and privileged access manager is FedRAMP and StateRAMP Authorized and available in the AWS GovCloud.

KSGC is a next-generation Privileged Access Management (PAM) solution that enables organizations to achieve complete visibility, security, control and reporting across every user on every device. KSGC is cloud-based, enables zero-trust and zero-knowledge security and helps organizations meet compliance mandates by unifying three integral solutions into one unified platform – enterprise-grade password, secrets and privileged connection management.

About Keeper Security

Keeper Security is transforming cybersecurity for people and organizations around the world.

Keeper's affordable and easy-to-use cybersecurity solutions are built on a foundation of zero-trust and zero-knowledge security to protect every user on every device. Millions of individuals and thousands of organizations rely on Keeper for best-in-class password, passkey and secrets management, Privileged Access Management (PAM), secure remote access and encrypted messaging. Our next-generation cybersecurity platform deploys in minutes and seamlessly integrates with any tech stack to prevent breaches, reduce help desk costs and ensure compliance.

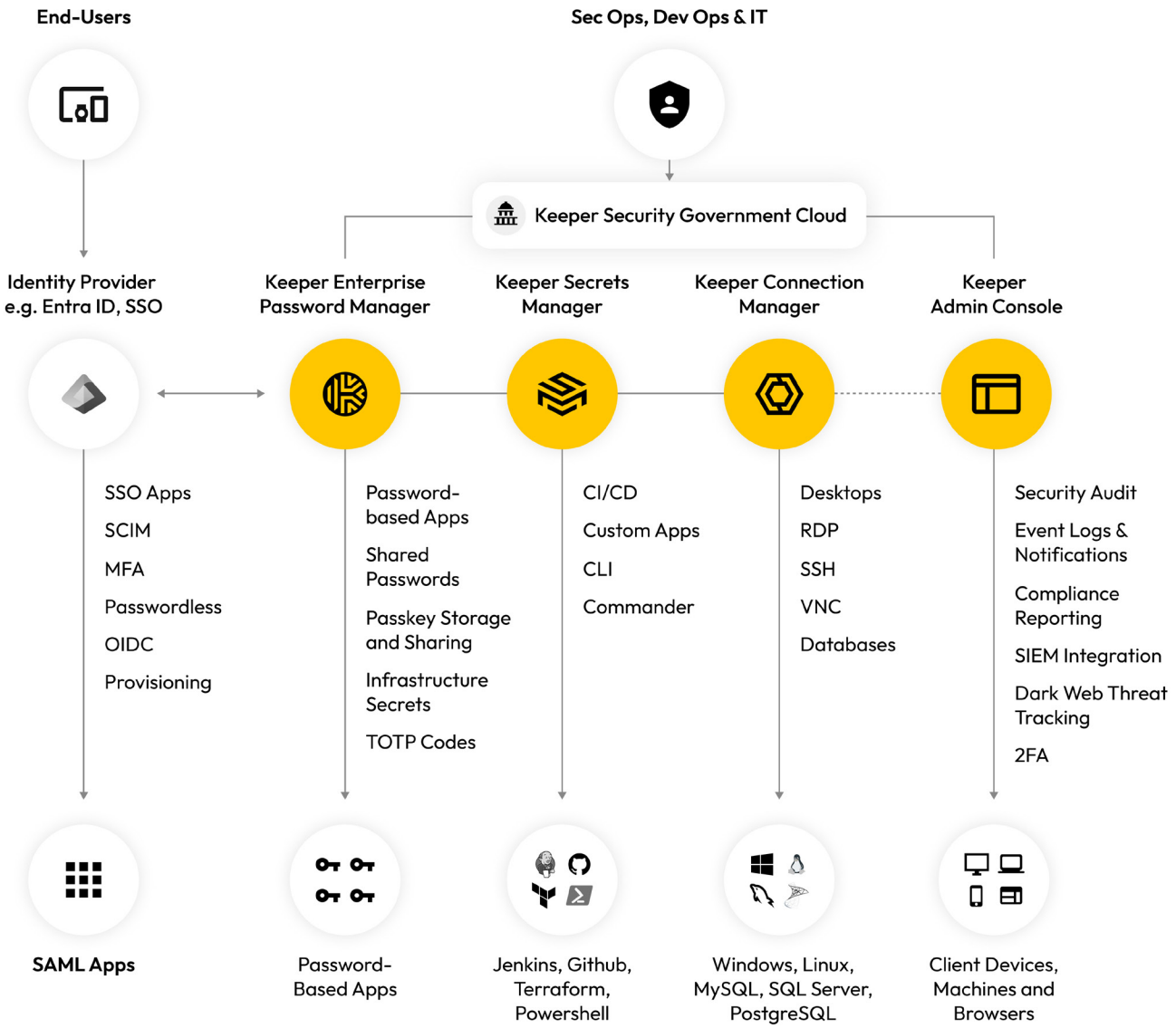
Keeper Security is backed by leading private equity firms Insight Partners and Summit Partners.

Keeper Security
Don't get hacked.

Learn more
keepersecurity.com

Schedule a personalized demo
keepersecurity.com/contact

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.
- Improve your agency's cybersecurity by providing employees with a simple and effective method to adopt password security best practices and reduce the burden of password-related tickets for your helpdesk and IT teams.

Key Capabilities

- Privileged Account and Session Management (PASM)
- Secrets Management
- Single sign-on (SSO) integration
- Privileged Account Credential Management
- Credential vaulting and access control
- Session management, monitoring and recording
- Privileged Elevation and Delegation Management (PEDM)