KEEPER

Industry Brief: Zero-Trust Security

# Advanced Zero-Trust Adoption with Keeper Security Government Cloud

## KSGC helps organizations advance zero-trust initiatives with capabilities aligned to all key pillars of the CISA Zero Trust Maturity Model framework

Keeper Security Government Cloud (KSGC) is an AI-enabled, cloud-native Privileged Access Management (PAM) platform that delivers comprehensive security and seamless integration – helping organizations achieve full visibility, security, control and reporting across every user, system and device. Recognized in the 2025 Gartner® Magic Quadrant™ for PAM, Keeper holds the longest-standing SOC 2 attestation and ISO 27001 compliance in the industry. KSGC meets FedRAMP, FIPS 140-3 and ITAR compliance requirements, and supports adherence to NIST 800-63B, FITARA, CMMC, HIPAA, DPA, FISMA and more. Keeper is also on CISA's Continuous Diagnostics and Mitigation (CDM) Approved Products List (APL).

### Identity Pillar

KSGC supports the identity pillar with a zero-knowledge authentication and authorization model. Identities can be entirely managed within Keeper. Our platform is capable of full integration into any existing zero-trust identity provider. Keeper's security model supports several advanced authentication methods, including continuous validation at the vault, device and record level and real-time machine learning analysis.

### Device Pillar

Keeper's solution supports the device pillar with constant device security monitoring, device-based access controls, and validation and data access. Keeper works with existing device management tools such as Azure's conditional access policies. Information stored within our platform is encrypted and decrypted locally at the device level. Elliptic Curve (EC) encryption technology is utilized at the device level to protect data and support the zero-trust model.

### Network/Environment Pillar

Keeper's solution supports the Networks pillar with fully distributed micro-perimeters, machine-learning-based threat protection, zero-knowledge encryption and record-level access controls. Information is encrypted at rest using 256-bit AES record-level encryption and device-level EC encryption. Network communication between the Keeper Vault on the device to the Keeper cloud is protected with TLS 1.3, plus additional layers of transmission-level encryption to protect against several attack vectors such as Man in the Middle (MITM) attacks, brute force attacks and enumeration.

### Application Workload Pillar

Keeper's solution optimizes the application workload pillar where access is continuously authorized and there is strong integration into the application workflow. By default, Keeper can be accessed over the internet without any VPN connection. Administrators can manage user role accessibility through access control policies. Keeper's Advanced Reporting and Alerts Module (ARAM) capabilities provide agencies with telemetry data covering hundreds of event types that can trigger real-time alerts or other threat-based actions.

### Data Pillar

Keeper's solution supports the data pillar with zero-knowledge encryption. Zero-knowledge is a framework that ensures the highest levels of privacy and security. Only you can access your data – no one else, not even Keeper. Encryption and decryption happen locally – on the user's device – never in the cloud. Data is secure at rest, in transit and in use. Combining 256-bit Advanced Encryption Standard (AES) and elliptic curve cryptography, Keeper ensures that our users' information is safe and secure at every level. Visit our documentation portal to read more about our full encryption model.

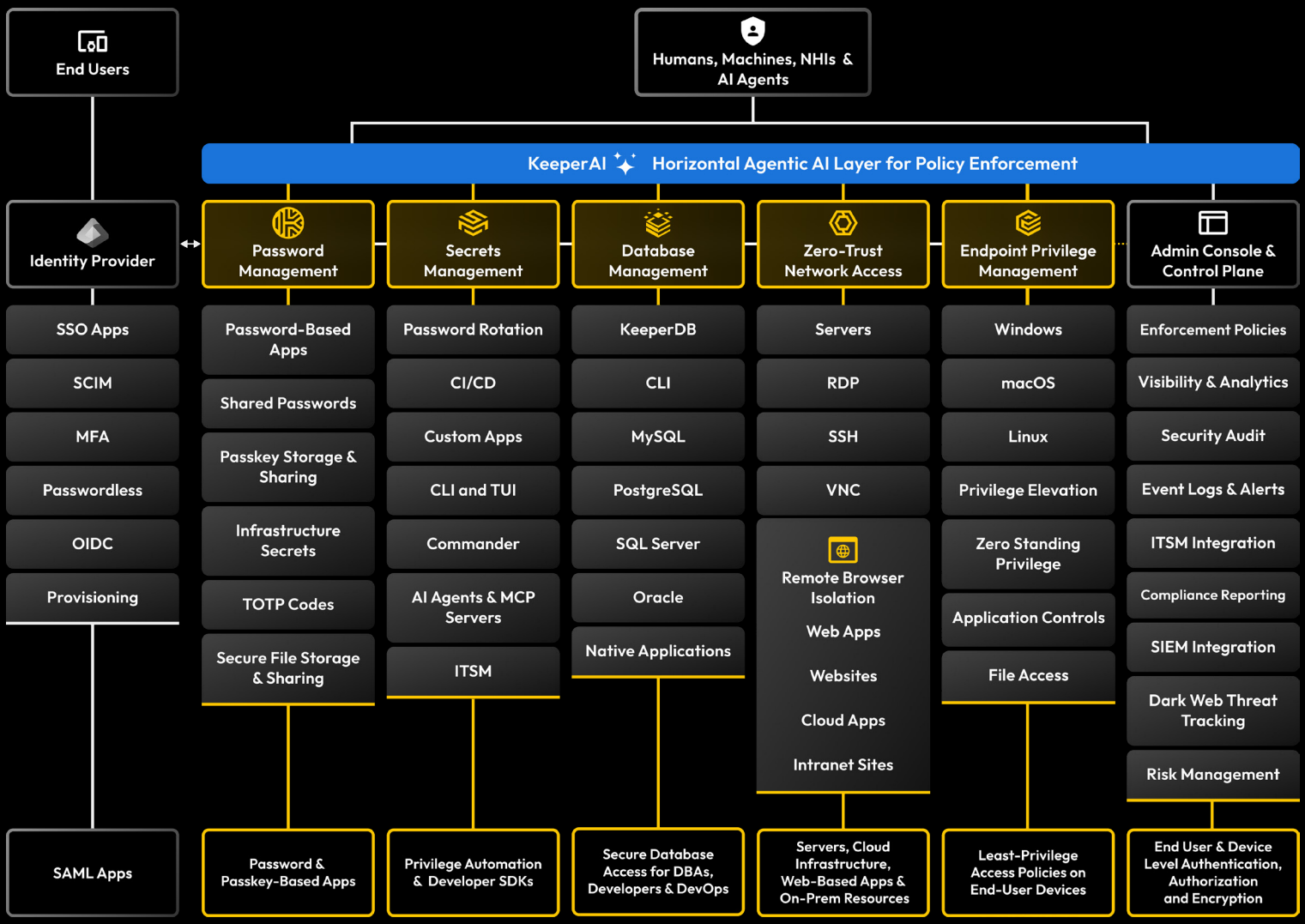
FedRAMP High Authorized

FIPS 140-3

AWS GovCloud

KEEPER PAM

# Keeper Privileged Access Management Platform




## Keeper Security Government Cloud (KSGC) Protects Your Agency With Zero-Trust Cybersecurity

Federal agencies faced a September 2024 deadline to submit zero-trust implementation plans and show meaningful progress toward adopting Zero Trust Architecture (ZTA), emphasizing continuous verification and strong identity controls. By September 2027, all Department of Defense components must reach “target level” zero-trust cybersecurity.

## Exceed Identity, Credential and Access Management (ICAM) requirements with KSGC

KeeperPAM addresses the key pain points and requirements in organizations to prevent data breaches with just the features you need.

- **Cost Effective:** A single platform with minimal IT staff required to manage it.
- **Fast Provisioning:** Seamlessly deploys and integrates with any tech or identity stack in just a few hours.
- **Easy to Use:** Unified admin console and modern UI for every employee on all device types – average training time is less than 2 hours.