Industry Brief

Critical Infrastructure Security

Protecting critical infrastructure with Keeper Security Government Cloud

Keeper Security Government Cloud (KSGC) is a FedRAMP High Certified environment that hosts KeeperPAM, an AI-powered, cloud-native Privileged Access Management (PAM) platform designed to protect Critical Infrastructure (CI), including water systems, energy grids, K-12 education networks and transportation systems. As state and federal policy shifts greater cybersecurity responsibility to State, Local, Tribal and Territorial (SLTT) governments, Keeper delivers a zero-trust, zero-knowledge platform that helps CI owners and operators meet compliance mandates, close credential security gaps and rapidly deploy enterprise-grade identity security protections.

Credential and secrets management

State regulations increasingly require the elimination of default credentials, enforcement of complex password policies and mandatory Multi-Factor Authentication. Keeper's password and secrets management capabilities provide rapid commercial-off-the-shelf compliance solutions for under-resourced local governments, securing human and non-human identities across infrastructure systems.

Zero-Trust Network Access (ZTNA)

Keeper provides agentless, zero-trust remote access to critical infrastructure systems, including air-gapped and segmented environments, without exposing services to unsecured networks. Keeper is a modern, zero-trust alternative to legacy VPNs, allowing CI operators to enforce strict access controls while maintaining operational continuity.

Privileged access and session monitoring

KeeperPAM helps prevent identity-based and privileged access attacks, which remain a leading cause of modern breaches, while providing continuous session recording and automated event logging. These capabilities support audit readiness, incident response, and cyber incident reporting requirements under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA).

AI-enabled threat detection

KeeperAI enables real-time threat detection and incident response across its platform. When threats emerge, such as data exfiltration attempts, unauthorized access or privilege escalation, KeeperAI responds immediately by terminating high-risk sessions before damage occurs. Compromised credentials and insider threats are neutralized at machine speed, well before a human analyst could intervene.

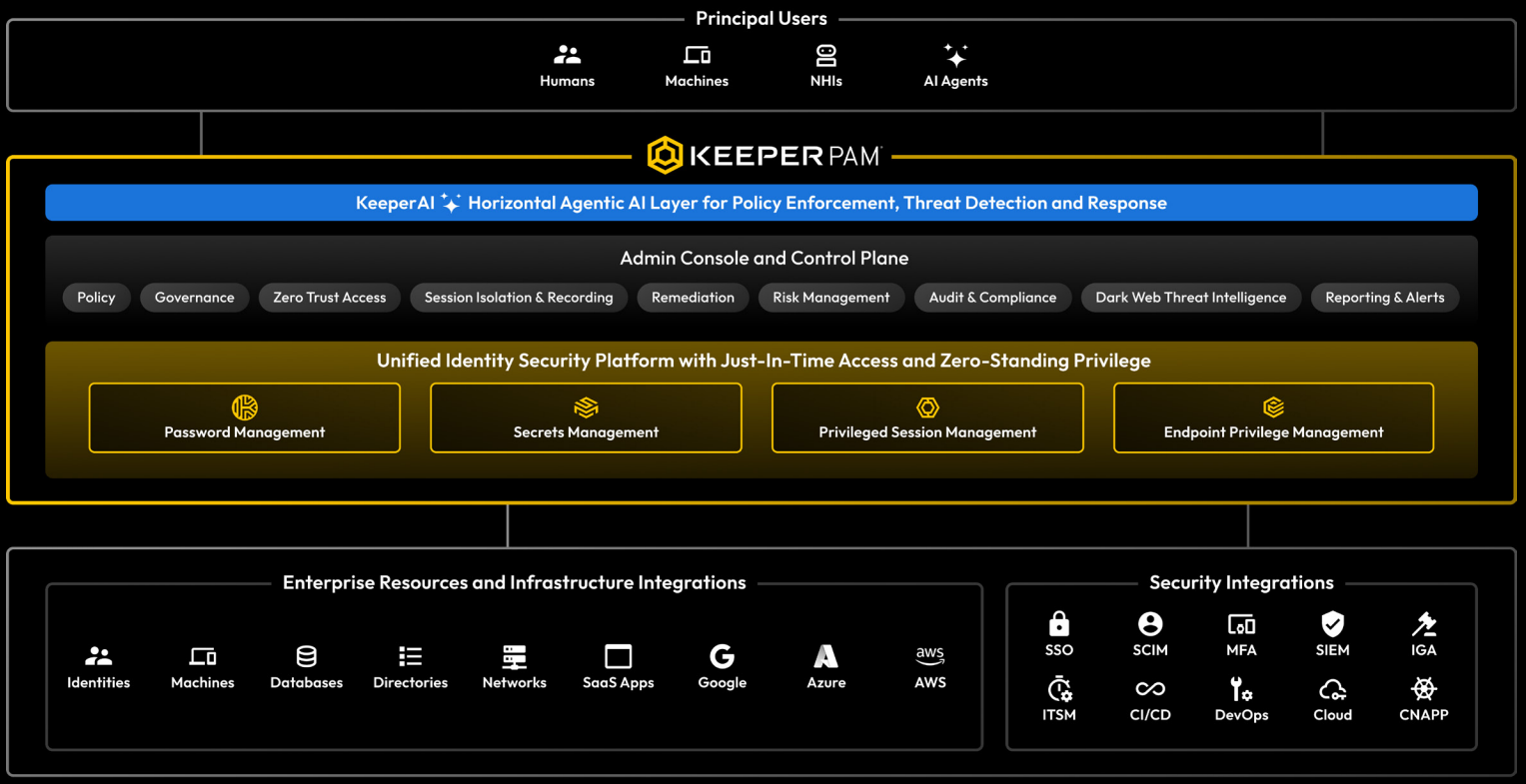
Zero-knowledge encryption

All data is encrypted and decrypted locally on the user's device, never in the cloud. Keeper combines 256-bit AES record-level encryption with elliptic curve and hybrid quantum-resistant cryptography, protecting data from both current and emerging threat vectors led by nation-state adversaries and hacktivists.

Compliance and grant eligibility

KSGC is FedRAMP High Certified, GovRAMP High Authorized, FIPS 140-3 compliant and listed on CISA's Continuous Diagnostics and Mitigation (CDM) Approved Products List (APL). Keeper is also a reimbursable investment under the State and Local Cybersecurity Grant Program (SLCGP).

The Zero-Trust, AI-Enabled Identity Security Platform



Why Keeper for critical infrastructure?

- **Rapid deployment:** Integrates with any tech or identity stack and can be rapidly deployed, eliminating lengthy procurement cycles.
- **Cost efficiency:** A unified platform requiring minimal IT staff and eligible for deployment through SLCGP and state CI grant funding.
- **Quantum readiness:** Hybrid quantum-resistant cryptography helps protect against both current and next-generation threats.
- **Zero-knowledge architecture:** Keeper's zero-knowledge encryption ensures only you can access your data – no one else, not even Keeper.

FedRAMP High Certified

GovRAMP High Authorized

FIPS 140-3

AWS GovCloud