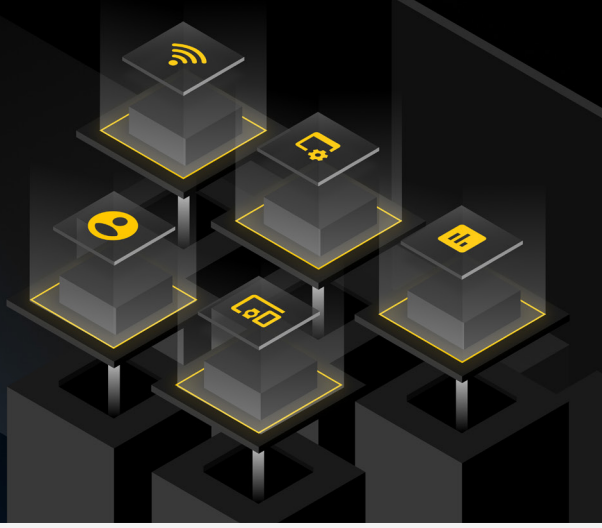
KEEPER

Industry Brief: Zero-Trust Security

The Five Pillars of Zero-Trust and How Keeper Addresses Each One

FedRAMP FIPS 140-2 AWS GovCloud



Federal agencies are required to adopt a zero-trust security framework by the end of fiscal year 2024, which requires a fundamental shift in their approach to cybersecurity. Instead of relying on a perimeter-based security model, where trust is granted to users and devices inside the network, agencies must adopt a "never trust, always verify" approach. This requires a comprehensive evaluation and overhaul of existing security practices, investing in new technologies and solutions, and retraining staff. The goal of zero trust is to reduce the attack surface, prevent unauthorized access, detect and respond to threats more quickly, and ultimately, better protect the sensitive data and resources that federal agencies manage.

Keeper Security Government Cloud (KSGC) password manager and privileged access manager is FedRAMP Authorized to deliver enterprise-grade password, secrets and privileged connection management in one unified platform. KSGC helps federal agencies address all five of the pillars that make up a Zero-Trust security framework.

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 network/environment pillar with fully distributed ingress/egress 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. Encryption and decryption take place on each user's device. Combining 256-bit 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.

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

Keeper holds the longest-standing SOC 2 attestation and ISO 27001 compliance in the industry. Keeper is a zero-knowledge and zero-trust password manager, secrets manager, privileged access manager and remote desktop gateway. All information stored in Keeper is only accessible by the end-user. The platform provides total control over employee password practices. IT administrators can control password use across an organization and implement role-based access controls.

Exceed 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.

Protect Passwords and Credentials

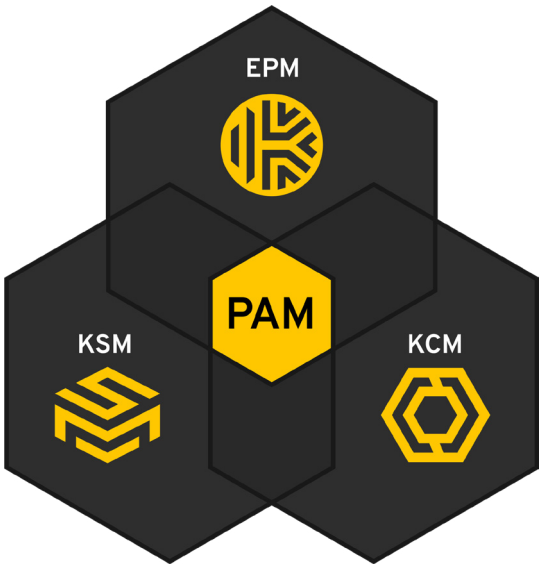
Keeper's unique security architecture protects data and systems with a solution that is quick to deploy and easy to use. Securely store, share and manage passwords across the entire organization.

Simplify Secure Remote Access

Securely manage your remote connections from anywhere – no VPN required.

Streamline Compliance and Audits

Provide on-demand visibility of access permissions to your organization's credentials and secrets.



KEEPER PASSWORD MANAGER

Enables organizations to securely manage, protect, discover, share and rotate passwords and passkeys 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 with RDP, SSH keys, database and Kubernetes – without the need for a VPN.