KEEPER
Cybersecurity Starts Here®

DATASHEET
Government Industry Brief

Keeper Helps Government Agencies Secure Sensitive Assets, Prevent Data Breaches and Maintain Compliance

security incidents were reported by federal executives[1]

of phishing attacks sought to steal login credentials[1]

increase in credential theft attacks[1]

Passwords are often the only security measure protecting government agencies and assets, especially on the state and municipal level. Most states dedicate less than 3% of their IT budgets to cybersecurity, as opposed to more than 10% in the private sector. Nearly half of all U.S. states lack a dedicated cybersecurity budget line item.[2]

Keeper Enterprise Password Management (EPM) Platform utilizes a Zero-Trust Security Framework alongside a Zero-Knowledge Security Architecture. This means users have complete knowledge, management and control over credentials and encryption keys. Keeper EPM complements and bolsters an organization's Identity & Access Management (IAM) architecture.

Further, Keeper equips organizational IT administrators with complete visibility and control over password security practices across the entire organization on all devices, enabling them to enforce the use of strong, unique passwords, multi-factor authentication (2FA), role-based access control (RBAC), event logging, reporting and other security policies. Keeper EPM provisions with and integrates into any IT environment and identity stack.

Federal government agencies have diverse cybersecurity defenses, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), data loss prevention (DLP) tools, system information and event management (SIEM) systems, as well as single sign-on (SSO) deployments. While these tools have their place, a very simple problem looms large: 81% of successful data breaches leverage weak or stolen passwords.[3]

Employees often use weak passwords across multiple work-related accounts. They fall prey to phishing attacks aimed at stealing login credentials. The good news for budget-strapped federal, state, and municipal organizations is that their largest security gap can be closed quickly and cost-effectively by implementing comprehensive password security policies and enforcing them through an easy-to-use, intuitive password management platform such as Keeper.

How Keeper Works

Keeper provides every employee with a secure digital vault that they can access from any device, running any operating system.

A security dashboard in the Admin Console provides InfoSec or IT administrators with an overview of weak passwords, password reuse, and multi-factor authentication (2FA) enforcement, along with role-based access controls (RBAC) to enforce least-privilege policies. Administration may be delegated according to department or by team leader, and folders and records can be securely shared and revoked. Access logs to Keeper vaults can be audited for compliance or forensics. If an administrator or employee leaves the agency, their vault can be automatically locked and securely transferred.

Protect Against Ransomware Attacks

Cybercriminals exploit stolen, weak and reused passwords to execute ransomware attacks. Keeper protects your organization against ransomware attacks using robust administration, controls and visibility over strong password security and real-time dark web monitoring.

Simplify Compliance Enforcement & Reporting

Keeper simplifies compliance monitoring and reporting with robust internal controls through delegated administration, enforcement policies, event tracking, monitoring, and reporting, as well as customizable audit logs and event reporting.

Plans to Fit Any Budget

Securing employee passwords doesn't have to cost a fortune. Keeper Enterprise is a powerful, cost-effective solution designed to help protect, secure your agency from cyberthreats and reduce help desk costs.

Extend Your SSO Deployment & Eliminate SSO Security Gaps

For all the benefits of SSO, it's not a panacea. SSO solutions leave significant security and functionality gaps such as when users who forget their password and are locked out of multiple sites and apps or if a password is stolen by cybercriminals, multiple systems are in jeopardy instead of one.

- SSO has limited administrative controls for passwords, so they cannot enable requirements like 2FA. Keeper Enterprise extends administrative controls in order to enforce security policies and password best practices.
- Most government agencies still use legacy systems to essential data or perform critical functions, and legacy apps may not be compatible with SSO. Keeper SSO is a fully managed, SAML 2.0 SaaS solution that can be deployed on any instance or in any Windows, Mac OS, or Linux environment, in the cloud or on-premise.

Keeper SSO Connect enables government agencies to significantly enhance and extend their SSO deployments with an integrated zero-knowledge password encryption system that provides all of Keeper's advanced password management, sharing, and security capabilities.

Defend Against Third-Party Vendor Breaches with BreachWatch™

Even if your password security is solid, your organization could be compromised through one of your vendors. With remote workforces having rapidly expanded, cybercriminals are taking advantage of the myriad of SaaS solutions that businesses are deploying to enable their remote workforces.

Keeper's BreachWatch protects your organization against third-party vendor breaches. BreachWatch doesn't depend on public breach notifications. It scans Dark Web forums and notifies an organization in real-time if any employee passwords have been compromised all through a zero knowledge, zero-trust platform. This allows IT administrators to force password resets right away, minimizing the risk of cybercriminals using them to breach systems.

Simple to Deploy & Use

Keeper takes only minutes to deploy, requires minimal ongoing management, and scales to meet the needs of any size organization, from a small municipality to a large federal agency. IT administrators can easily and quickly provision Keeper vaults to all of their users with a domain match on email addresses. With minimal administration, a large-scale deployment can be accomplished using an existing email channel or portal.

Keeper integrates seamlessly into any data environment — single cloud, multi-cloud, or hybrid — and any security stack. It works with online services and apps, including legacy LOB apps, and it integrates into any SSO deployment.

Simplify Compliance Enforcement & Reporting

Keeper simplifies compliance monitoring and reporting with robust internal controls through delegated administration, enforcement policies, event tracking, monitoring, and reporting, as well as customizable audit logs and event reporting.

Flexible Provisioning

Keeper supports the ability to seamlessly provision users and teams from Microsoft Azure AD or other identity platforms using the SCIM protocol. Keeper also supports API-based, command line provisioning through the use of Keeper® Commander SDK. The Keeper Commander SDK is open-source Python code that is available for download from Keeper's Github repository.

About Keeper Security, Inc.

Keeper Security, Inc. ("Keeper") is transforming the way organizations and individuals protect their passwords and sensitive digital assets to significantly reduce cybertheft and data breaches. Keeper is the leading provider of zero-trust, zero-knowledge security and encryption software covering password management, dark web monitoring, digital file storage, advanced reporting and messaging. Named PC Magazine's Best Password Manager & Editors' Choice and awarded the Publisher's Choice Cybersecurity Password Management InfoSec Award, Keeper is trusted by millions of people and thousands of organizations to protect their digital assets and help mitigate the risk of a data breach. Keeper is SOC-2 (Type 1 and 2) and ISO 27001 Certified and is also listed for use by the Federal government through the System for Award Management (SAM). Keeper protects organizations of all sizes across every major industry sector.

[1] CIO Dive [2] NASCIO [3] Verizon DBIR