KEEPER
Cybersecurity Starts Here™

DATASHEET
Government Industry Brief

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

>28K
security incidents were reported by federal executives[1]

>70%
of phishing attacks sought to steal login credentials[1]

90%
increase in credential theft attacks[1]

Keeper Security is the most secure Enterprise Password Management (EPM) Platform because it incorporates a Zero-Trust Security Framework alongside a Zero-Knowledge Security Architecture. This ensures customers have complete knowledge of, management and control over, its credentials and encryption keys. Keeper EPM compliments and bolsters an organization's Identity & Access Management (IAM) architecture.

Further, Keeper equips organizational IT administrators with complete visibility and control over employee 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.

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]

Federal government agencies have larger budgets and can afford more robust cybersecurity defenses, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), data loss prevention (DLP) tools, and 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 use weak passwords across multiple work-related accounts. They also fall prey to phishing attacks aimed at stealing login credentials.The good news for budget-strapped federal, state, and municipal agencies 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. If an administrator or employee leaves the agency, their vault can be automatically locked and securely transferred. Access logs to Keeper vaults can be audited for compliance or forensics.

Simple to Deploy & Use

Keeper takes only minutes to deploy, requires minimal ongoing management, and scales to meet the needs of any size government agency, from a small municipality to a large federal department. IT administrators can easily and quickly provision Keeper vaults to all of their users with a domain match on email addresses. With minimum 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 all online services and apps, including legacy LOB apps, and it integrates into any SSO deployment.

Plans to Fit Any Budget

Securing employee passwords doesn't have to cost a fortune! With subscriptions for government agencies starting at only $3.75 per user, per month, Keeper will be the least expensive, yet most powerful component in your agency's security stack.

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:

- If a user forgets their password, they're locked out of multiple sites and apps instead of just one. Conversely, if a user's password is stolen, cybercriminals can access multiple systems instead of just one.
- SSO doesn't provide administrators with any visibility or control of user password habits, so they can't enforce security policies such as using a strong, unique password for every account or enabling 2FA on all accounts that support it.
- Not all apps support SSO. Most government agencies still use at least some legacy line-of-business (LOB) apps because they contain essential data or perform critical functions, and it's not feasible to replace them. These legacy apps aren't compatible with SSO. Not all modern apps support it, either.

Keeper SSO Connect™ 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-prem. It easily and seamlessly integrates with all popular SSO IdP platforms, including Microsoft 365, Azure, ADFS, Okta, Ping, JumpCloud, Centrify, OneLogin, and F5 BIG-IP APM.

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 company 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.

Data breach victims are typically the last ones to know they've been compromised. It can take a breached organization months, even years to detect a breach, but cybercriminals don't wait. When they steal login credentials, they put them to use very quickly, either by launching their own cyberattacks or by putting them up for sale on the Dark Web - the part of the World Wide Web that is only accessible by means of special software.

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

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.

Microsoft Active Directory Synchronization

Keeper® AD Bridge synchronizes to Microsoft Active Directory or OpenLDAP. This enables rapid user provisioning and automatically adds Nodes,, Users, Roles, and Teams. Keeper enables RBAC and the ability to track roles when employee positions or job duties change. This includes automatically locking vaults when employees depart the agency.

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 businesses 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 businesses of all sizes across every major industry sector.

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