KEEPER

Industry Brief: Law Enforcement

Keeper Security Government Cloud Password Manager and Privileged Access Manager for Law Enforcement

Police Departments Are Targets

Public safety agencies, including police departments, are targets for ransomware attacks because of cybercriminals' desire for profit, retaliation and notoriety.

Police departments often have limited cybersecurity budgets, large attack surfaces, unpatched legacy systems and increasingly distributed digital workforces.[1]

Law Enforcement Data Is at Risk

Police departments and law enforcement agencies maintain a wealth of sensitive data, including personnel files, investigative files and intelligence reports. Police departments are critical public institutions, and any disruption to their operations can have serious consequences.

CJIS Compliance Is Essential

According to the Criminal Justice Information Services (CJIS) security policy, all passwords used by law enforcement agencies must be a minimum of 20 characters. Failure to comply with the CJIS security policy can result in denial of access to any FBI database or CJIS system, along with fines and even criminal charges.

Failure To Act Is Costly

When police departments are breached, attackers have access to confidential employee data, case records, intelligence reports and investigative files. Recovering from a cyberattack can be expensive. Agencies might need to hire external experts, replace compromised hardware, purchase new software or pay ransoms.

69%

The percentage of local and state government organizations that were hit by ransomware in 2022.[2]

52%

More than half of respondents in a recent survey of law enforcement personnel identified ransomware as their top concern when asked about cybersecurity challenges.[3]

74%

The percentage of data breaches that are due to the human element, with stolen or weak passwords acting as a primary vector for cybercriminals.

$1.8M

It cost organizations on average $1.82 million to recover from a ransomware attack in 2023 — and that doesn't even include paying a ransom.[4]

[1] How to Respond to Growing Ransomware Attacks on Government and Police
[2] 2023 Sophos Survey
[3] Motorola Solutions 2022 Law Enforcement Survey
[4] Motorola Solutions 2022 Law Enforcement Survey

KEEPER

Industry Brief
Law Enforcement

Cybersecurity Starts with Protecting Your Passwords, Secrets and Credentials

Keeper Security Government Cloud (KSGC) Password Manager and Privileged Access Manager delivers enterprise-grade password, passkey, secrets and privileged connection management in one unified platform.

Keeper enables law enforcement and local governments to quickly and cost-effectively meet CJIS compliance requirements.

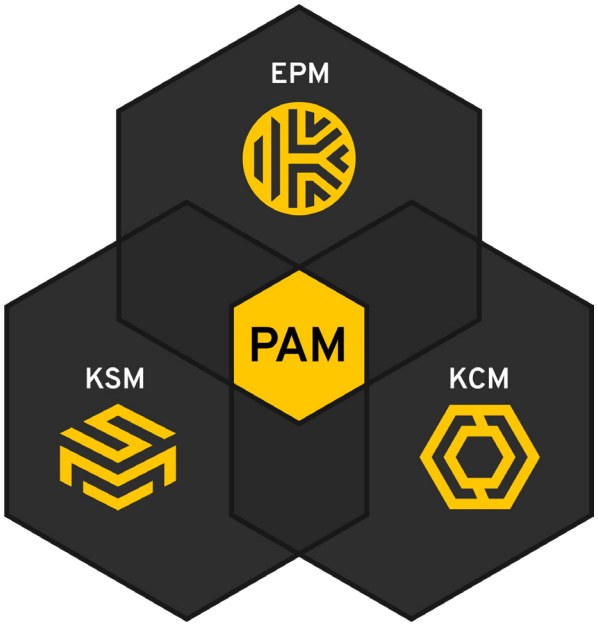
Keeper gives law enforcement agencies the visibility and control they need to prevent credential-based cyberattacks by enabling IT administrators to manage employee password use and systems-access throughout the data environment.

Keeper provides privileged account session management, secrets management, Single Sign-On (SSO) integration, privileged account credential management, and powerful credential vaulting and access control.

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 endpoints – without the need for a VPN.