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.

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.

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
5 How to Respond to Growing Ransomware Attacks on Government and Police

© 2023 Keeper Security, Inc.
Cybersecurity Starts with Protecting Your Passwords, Secrets and Credentials


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.

Enables organizations to securely manage, protect, discover, share and rotate passwords and passkeys with full control and visibility to simplify auditing and compliance.

Delivers a fully-managed, cloud-based solution to secure infrastructure secrets such as API keys, database credentials, access keys and certificates.

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.