KEEPER
Cybersecurity Starts Here™

DATASHEET

Judiciary Industry Brief

35
major data breaches among government agencies in 2016

21M
records stolen in U.S. Office of Personnel Management data breach

81%
of data breaches are due to weak, default or stolen passwords

The Verdict: Courts and Justice Agencies Prime Targets for Cyber Theft

Recent cyber attacks at a multitude of federal agencies and specifically the data breach at the Office of Personnel Management (OPM) underscored the importance of data security and the need for constant vigilance to protect sensitive Judiciary data and IT assets. When compared to the cybersecurity performance of 17 other major industries, government organizations ranked at the bottom of all major performers, coming in below information services, financial services, transportation and healthcare.

Regardless of their size or location, courts and justice agencies at every level share one thing in common – increasing dependence on technology is driving the need to strengthen information security policies, processes and tools.

The Greatest Risk of Breach can be Isolated to the Most Basic of Security Concepts, The “Password”

It is well-documented that passwords pose the greatest security risk to organizations today; Verizon reported over **81% of data breaches are due to weak employee passwords and poor password management practices**. Federal, state and local court systems have identified passwords as one of the weakest links in their defense against cyberattacks. Federal courts have reported that 60-70% of employees use the same password for all accounts.

The largest security gap within the justice system can be quickly and cost effectively closed with strong password policies enforced with an easy-to-use, intuitive password management solution. **Cybersecurity initiatives such as the U.S. Federal Civilian Government’s Cybersecurity Strategy and Implementation Plan (CSIP) mandates effective password management and hygiene for government entities.**

Protect Judges, Jurors and Citizens with Enterprise-Strength Password Management

All encryption and decryption is done on the user’s device. PBKDF2 with 100,000 rounds is used for deriving a key from the user’s master password. Each record is encrypted using AES-256 with a different and unique key that is randomly generated client-side. RSA encryption is used for secure record sharing between users and teams. Keeper’s infrastructure sync’s encrypted ciphertext between devices. Key pinning is enforced between client and server. All data in transit and at rest is always encrypted - it cannot be viewed by Keeper Security employees or any outside party.

Keeper Integrates with Leading SSO Solutions

Keeper is the trusted leader in password management helping organizations manage, secure and enforce strong passwords across all employee logins, applications and sites. Judges, law clerks and court administrators can access Keeper natively on all mobile devices, desktops and browsers.

Key Features

- Enhanced protection with two-factor authentication (2FA)
- Secure file storage and sharing
- Cloud-based, OS and device independent
- Admin console with reporting, auditing and analytics
- Fast deployment with AD/LDAP provisioning
- 24x7 support

Key Benefits

- Maintain regulatory compliance
- Increase employee productivity
- Enforce password policies and procedures
- Reduce help desk costs
- Minimal training, fast time-to-security
- Improve employee security awareness and behavior

Reduce Costs and Improve Productivity with Keeper

Password resets are a major burden on the productivity of IT departments. The #1 help desk call is for a forgotten password - Gartner estimates the annual industry cost for password resets is around $10B per year.

Keeper provides cost savings to customers by reducing help desk calls and increasing employee productivity. Employee passwords are encrypted and stored within Keeper so employees no longer need to remember them. Keeper auto-fills login credentials across mobile applications and browsers, which greatly improves productivity. If an employee forgets their master password, Keeper allows employees to set a security question so the master password can be recovered without IT assistance.

Finally, all Keeper users have 24x7 access to Keeper's dedicated customer care team. With Keeper, costly help desk calls will be significantly reduced and the burden of resetting passwords will become a thing of the past for the IT department.

Secure More Than Just Passwords

Passwords are one of many confidential assets that businesses need to secure. Keeper protects your sensitive files, documents, digital certificates, private keys, photos and videos in a highly-secure, encrypted digital vault.

You can securely share files with colleagues and have confidence knowing that your information is backed up in Keeper's Cloud Security Vault™.

The Keeper Difference

- Provides a simple, intuitive and unified password manager and digital vault
- Has an impenetrable security architecture with rigorous 3rd party audits (SOC II Type 2 and HIPAA compliant)
- Delivers native applications across all major devices, operating systems and browsers
- Provides password policy visibility and enforcement
- Has a dedicated customer care team 24x7x365

Keeper Third-Party Attestations and Certifications

GSA Schedule70 Contract 47QTCA18D00C9

TRUSTe CERTIFIED PRIVACY

AICPA SOC

PCI DSS COMPLIANT

HIPAA COMPLIANT

Keeper is used by local, state and federal agencies

Over 3,000 organizations trust Keeper including many local, state and federal government agencies. Keeper is honored to have as a customer the U.S Federal District Courts of the Western District of Arkansas, Vermont, Eastern District of New York, Southern District of Ohio and Middle District of Louisiana.

U.S. Federal District Courts of the Middle District of Louisiana

U.S. Federal District Courts of the Eastern District of New York

U.S. Federal District Courts of Vermont

U.S. Federal District Courts of the Southern District of Ohio

U.S. Federal District Courts of the Western District of Arkansas