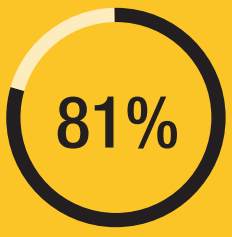
of healthcare organizations have been breached

records stolen from healthcare organizations in 2015



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

Data breaches are a growing epidemic in healthcare

The digital revolution is creating transformational change in healthcare. Finally, providers, payers, and patients are realizing the tremendous promise of an all-digital healthcare ecosystem with improved care and lower costs. With the transition to digital however, personal medical data is now under attack. Today the healthcare industry represents more than two thirds of the total number of data breaches. Why the increase in healthcare breaches? It comes down to economics. Medical information is worth 10 times more than a credit card number on the black market. So how do we stop healthcare cyber crime?

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. Data breaches can be very costly and result in escalating response costs, lost productivity, regulatory fines and tarnished brand. It is estimated that each healthcare breach costs an average of over $2 million.

Protect your organization and patients with enterprise-strength password management

Keeper is the trusted leader in password management helping organizations manage, secure and enforce strong passwords across all employee logins, applications and sites. Employees can access Keeper natively on all mobile operating systems, desktops and browsers.

Data is protected in Keeper's *zero-knowledge* security architecture with world-class encryption. Zero-knowledge means that only the user has knowledge of and access to their Master Password and the encryption key that is used to encrypt and decrypt their information. Keeper uses 256-bit AES encryption, which is used to encrypt classified data designated as TOP SECRET by the U.S. Government. Keeper also supports two-factor authentication to protect access to systems storing patient data, as recommended by HIPAA.

Key Features

- Effective and intuitive password management
- Enhanced protection with two-factor authentication
- 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

- Mitigate cyber risk
- Maintain HIPAA 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

For more information contact sales@keepersecurity.com or call 312.829.2680

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, those 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

Only Keeper….

- 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 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

Who uses Keeper?

Over 3,000 organizations trust Keeper including Siemens, Philips Healthcare, Cornerstone Healthcare Group, Robert Wood Johnson University Hospital and more.