KEEPER
Cybersecurity Starts Here

DATASHEET
Insurance Industry Brief

Insurance Companies Struggle to Secure Policyholder Data

of insurance providers said they worry "some" or a "great deal" about cyberthreats[1]

cyberattacks of insurance companies on average every year[2]

insurance cyberattacks results in a successful data breach[3]

Breaches of Policyholder Information Cost Insurers Millions

The insurance industry is entirely data-driven. In the normal course of business, insurers collect, process, and store highly sensitive data on their customers, including financial information, privileged healthcare information (PHI), work history and other professional data, and personal identifying information (PII). Cybercriminals have long targeted insurers to get at this treasure trove of valuable data.

In recent years, insurance companies have digitally transformed in an effort to better serve existing customers, penetrate new markets, and expand their product portfolios. Insurers have invested heavily in digital technologies such as web and mobile-based agency portals, policy applications, and claims-filing apps. They are also embracing big data, smart analytics, and Internet of Things (IoT) technologies, such as smart devices to track car mileage, to better predict risk and price products.

These technologies have expanded insurers' capabilities and market share, but they have also opened up insurance companies to new and highly sophisticated cyberattacks, such as targeted social engineering schemes. While today's cybercriminals are more skilled, educated, and well-funded than ever before, insurers frequently don't have the resources to effectively defend themselves. In the U.S. alone, insurance breaches have compromised sensitive data belonging to over 100 million consumers.

Insurance data breaches cost the industry millions in regulatory fines, legal fees, and mitigation fees each year. Additionally, the insurance industry revolves around trust; consumers trust that their insurers will keep their personal information secure. An insurance data breach severely erodes consumer trust, tarnishing the insurer's brand image and prompting customers to flee to competitors.

Keeper Helps Insurance Companies Protect Policyholder Data and Maintain Compliance

Many insurance brokers feel they cannot afford to properly secure their systems. However, many large insurance companies have made capital investments in high-tech security defenses, then ended up getting breached anyway. This is because they neglected a very basic, inexpensive step: securing their employees' passwords. Verizon estimates that about 80% of successful data breaches are due to weak or compromised passwords.

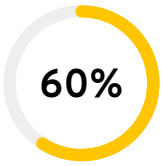
Keeper gives insurance companies of all sizes the visibility and control they need to prevent password-related cyberattacks by enabling IT administrators to manage employee password usage and systems access throughout the data environment, including role-based access control (RBAC) tools, customizable audit logs, and event reporting.

Secure More than Just Passwords with Keeper Secure File Storage

In addition to securing employee passwords, Keeper helps insurance companies prevent data loss by allowing them to store sensitive files, documents, digital certificates, private keys, photos, and videos in a highly secure, encrypted digital vault. Employees can securely share files with colleagues with confidence, knowing that company information is backed up in Keeper Password Manager and Vault™.

Two-Factor Authentication

Keeper supports multiple two-factor authentication (2FA) methods, including SMS, Keeper DNA® (smartwatch tap), TOTP (e.g., Google Authenticator and Authy), FIDO U2F (e.g. Yubikey), Duo, and RSA SecurID. 2FA may also be enforced through RBAC.



of insurance companies don't realize they've been breached until the damage is done[4]

americans have had sensitive personal data compromised in insurance data breaches[5]

Zero-Knowledge Architecture

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 syncs 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.

IT Admin Insight

Every user is provided a secure digital vault. A security dashboard in the Admin Console provides an overview of weak passwords, password reuse and two-factor authentication enforcement. Keeper enables role-based access controls to enforce least privilege policies. Administration may be delegated to department or team leaders and folders and records can be securely shared and revoked. The vault of an administrator or staff member who leaves can be automatically locked and be securely transferred. Access logs to Keeper vaults can be audited for compliance or forensics.

Email Auto-Provisioning

Easily and quickly provision Keeper vaults to thousands of users with a domain match on email addresses. With minimum administration, large scale deployment can be accomplished using an existing email channel or portal. 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 (organizational units), Users, Roles, and Teams. Keeper enables role-based access control (RBAC) and the ability to track roles when employee positions or job duties change. This includes automatically locking vaults when employees depart the company.

About Keeper Security, Inc.

Keeper Security, Inc. (Keeper) is the market-leading, top-rated cybersecurity platform for preventing password-related data breaches and cyberthreats. Keeper's zero-knowledge security and encryption software is trusted by millions of people and thousands of businesses across the globe to mitigate the risk of cybertheft, boost employee productivity and meet compliance standards. Keeper has been named PC Magazine's Best Password Manager of the Year & Editors' Choice, PCWorld's Editors' Choice and is the winner of four G2 Best Software Awards and the InfoSec Award for Best Product in Password Management for SMB Cybersecurity. Keeper is SOC-2 and ISO 27001 Certified and is also listed for use by the U.S. federal government through the System for Award Management (SAM). Learn more at **https://keepersecurity.com.**

[1] Insurance Journal [2] NU Property & Casualty [3] Varonis [4] NU Property & Casualty [5] Superior Access [6] Superior Access