KEEPER
Cybersecurity Starts Here®

DATASHEET
E-commerce Industry Brief

Cybercrime Costs E-commerce Industry Billions of Dollars Annually

annual cost of data breaches for online retailers[1]

retailers suffered a cyberattack over the past 12 months[2]

of consumers are likely to stop buying from a merchant if their account is compromised[3]

Online Sales and Cyberattacks are Skyrocketing

COVID-19 has had a profound impact on e-commerce. Between April 2019 and April 2020, buy online, pick up in-store (BOPIS) sales increased by an astounding 208%. With the high risk COVID-19 presents for in-store shoppers, and with consumers becoming accustomed to the convenience of online shopping, experts agree that customers will continue to embrace e-commerce.

Cyberattacks against e-commerce sites are an ongoing problem that is costing the industry billions of dollars and deeply eroding consumer trust and brand loyalty. Online retailers depend heavily on third-party app developers for online store platforms, payment processing, and other IT services; this translates into a very broad potential attack surface. As online sales rose dramatically in the wake of the pandemic, so did cyberattacks targeting online retailers, and many merchants are not prepared to defend themselves.

Retailers Grapple with Regulatory Compliance

Online retailers have long needed to ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS), a set of security standards for handling payment card information. In recent years, consumer advocates have also pushed for and gotten legislators to enact a number of major data security and privacy regulations that online retailers must comply with, including:

- The General Data Protection Act (GDPR): The most stringent data security and privacy law in the world, the GDPR applies to any company, worldwide, that does business with customers who are located in the European Union.
- The California Consumer Privacy Act (CCPA): Sometimes called the “American GDPR,” the CCPA regulates how businesses worldwide must handle and secure the personal information of customers who live in California.

Achieving and maintaining compliance with all applicable frameworks is a continuous and complex process, and the penalties for non-compliance are potentially ruinous. Businesses that violate the GDPR can be fined up to 10 million euros (approximately $11 million USD), or up to 2% of their entire global turnover for the preceding fiscal year, whichever is higher.

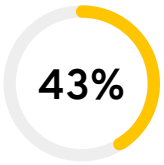
Keeper Helps Online Retailers Prevent Cyberattacks & Maintain Compliance

Verizon estimates that about 80% of successful data breaches are due to weak or compromised passwords. Keeper gives online retailers 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.

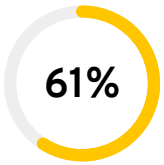
Additionally, Keeper simplifies compliance monitoring and reporting by giving IT administrators full visibility and control over employee password usage and role-based systems access throughout their data environments, with customizable audit logs and event reporting.

Secure More than Just Passwords with Keeper Secure Storage

Passwords are only one of many confidential digital assets that businesses need to secure. Keeper helps e-commerce businesses 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 Vault™.



of online retailers experienced a severe data breach[4]



of consumers believe that the companies that have access to their data are the ones who are responsible for preventing fraud[5]

of login attempts on e-commerce sites were from cybercriminals using stolen data[6]

IT Admin Insight

Every employee is provided with a secure digital vault. A security dashboard in the Admin Console provides an overview of weak passwords, password reuse, and 2FA enforcement, along with RBAC to enforce least privilege policies. Administration may be delegated according to department or by team leader, and folders and records can be securely shared and revoked. If an administrator or employee leaves the company, their vault can be automatically locked and 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.

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 role-based access controls (RBAC).

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.

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 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] Retail Times [2] Grant Thorton [3] Business Wire [4] Retail Times [5] Total Retail [6] Retail Times