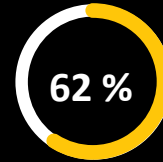**KEEPER**
Cybersecurity Starts Here®

Cybercrime Costs Financial Services Sector More Than Any Other Industry

$210 average cost per record [1]

$388 the highest cost per record of mega data breaches [2]

62 % of exposed data came from the financial industry [3]

Most Breached Data Comes from Financial Services Companies

As the financial services industry ramps up operations to manage large numbers of remote workers, sudden organizational and network system changes may leave them vulnerable to cyberattacks. Cybercriminals are already targeting the financial services industry with phishing campaigns and other malicious attacks that can adversely impact highly sensitive financial information.

The typical financial services data breach is extremely large and very costly. In 2019, 62% of all compromised data came from financial services companies, even though the industry accounted for only 6.5% of data breaches. An average breach costs financial services firms $210 per record, second only to healthcare records.[4] Many companies in the finance sector are not taking the steps they need to secure their employee passwords or their customer data in the modern digital environment, even as they implement new digital channels, automation, BYOD, and remote work technologies that expand their potential attack space.

Keeper gives financial services firms 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.

Simplify Regulatory & Industry Compliance with Keeper

An alphabet soup of regulatory and industry compliance standards mandate that financial services organizations enhance customer privacy protections, minimize systemic cyber risk, and harmonize security and privacy protocols.

Not all frameworks apply to all companies. For example, only cloud services providers that are U.S. federal contractors must comply with FedRAMP. However, most companies must comply with multiple frameworks, including:

- Sarbanes-Oxley (SOX): Anti-fraud controls that apply to public companies and companies eyeing a potential initial public offering (IPO).

- Payment Card Industry Data Security Standard (PCI DSS): Security standards for handling payment card information.

- Statement on Standards for Attestation Engagements No. 18 (SSAE-18): Monitors and enforces controls around the applications and application infrastructure that impact financial reporting.

- NYDFS Cybersecurity Regulation: A comprehensive data privacy and cybersecurity regulation that applies to insurance companies and financial services firms located in the State of New York.

- National Credit Union Administration (NCUA) Guidelines for Safeguarding Member Information (12 CFR Part 748): Applies to credit unions operating in the U.S.

Achieving and maintaining compliance with all applicable frameworks is a continuous and complex process. Both the cyber threat landscape and organizational data environments are in constant flux, and the effectiveness of individual controls can erode over time. This is why compliance frameworks typically mandate regular monitoring and reporting, and what constitutes "regular" depends on the framework.

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.

Microsoft Active Directory Synchronization

Keeper® AD Bridge synchronizes with Microsoft Active Directory and 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 as employees switch job positions or their job duties change. Automatically lock vaults when employees depart the company.

Reduce Support Costs

Eliminate help desk tickets for lost and forgotten passwords, and free up internal IT staff to work on other projects.

Increase Productivity

Save employees time and frustration, and eliminate help desk tickets for lost and forgotten passwords. Keeper generates strong, random passwords and automatically fills user login credentials on all sites and apps. The Keeper vault, with a responsive and intuitive UI, is accessible from any device, on any OS, and at any location. Everything Keeper does is geared towards quick user adoption and security. Keeper is published in 21 languages for global use.

Automate Back-End Password Rotation

Keeper ® Commander SDK provides IT admins and developers with command-line tools and Python source code to perform password management, password rotation, and vault functionality. Eliminate hard-coded or plaintext backend passwords. Connectors include Unix, Windows, and AD logins; Oracle, Microsoft SQL, MySQL, Postgres, and Dynamo databases; and AWS password and API access keys.

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://www.destinycorp.com**.

Keeper Third-Party Attestations and Certifications

Keeper Awards and Recognition

2020 Enterprise Leader	**Editors' Choice**	**Gartner Peer Insights**	**Spiceworks**
4.7 out of 5 stars	4.5 out of 5 stars	4.9 out of 5 stars	5 out of 5 stars