KEEPER

Industry Brief: Financial Services

The Financial Services Industry Is Under Attack

Financial Services Firms Are Targets
Financial services firms have long been a primary target of cybercriminals, both because of the client data they have and the potential for large payouts. In 2022, 74% of financial services firms were the target of one or more ransomware attacks, and 63% paid the ransom. The average breach cost firms $5.97 million in 2022, according to IBM, among the most expensive of any industry.

Sensitive Data Is At Risk
Cybercriminals target financial services firms because of valuable data, which can be leveraged to launch downstream attacks on client businesses. Information such as business plans, tax records, intellectual property, compliance audits and forms of personally Identifiable Information (PII) put both employees and customers at risk.

Hybrid Model Introduces New Risk
As FINRA and similar regulatory agencies relaxed in-office requirements for the industry in the wake of the COVID-19 pandemic, firms have maintained a hybrid work model. However, home networks and personal devices may have weaker security measures compared to corporate networks and devices. This creates more entry points for attackers to exploit and gain unauthorized access to sensitive information or systems.

Compliance Is Costly and Chaotic
Stringent regulatory frameworks, such as Sarbanes-Oxley (SOX) and Payment Card Industry Data Security Standard (PCI DSS), require certain controls to maintain compliance and ensure the secure exchange of sensitive information. Non-compliance is increasingly an issue, with 74% of banking CISOs in a 2022 KPMG survey reporting it as a primary issue and area of focus.[4]

Industry Experiences Record Rise in Ransomware Attacks

82%

of data breaches involved compromised credentials according to Verizon Data Breach Investigations Report 2022[1]

74%

of financial institutions experienced one or more ransomware attacks in the last year[2]

$6M

the average cost of a data breach in 2022[3]

[1] 2022 Verizon Data Breach Investigations Report
[2] VMWare, Modern Bank Heists 5.0
[3] IBM, Cost of a Data Breach Report 2022
[4] KPMG, Cybersecurity: 2022 Banking Industry Survey

Cybersecurity Starts with Protecting Your Passwords, Secrets and Credentials

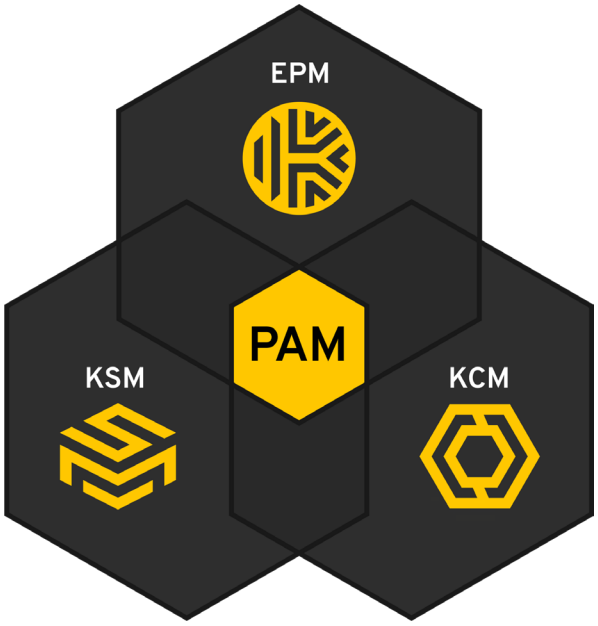
Keeper Security's next-gen privileged access management (PAM) solution delivers enterprise-grade password, secrets and privileged connection management in one unified platform.

Keeper gives financial services firms the visibility and control they need to prevent credential-based cyberattacks by enabling IT administrators to manage employee password usage and systems access throughout the data environment. With Keeper, firms gain privileged account session management, secrets management, Single sign-on (SSO) integration, privileged account credential management and powerful credential vaulting and access control.

Protect Employee Passwords and Credentials
Keeper's unique security architecture protects data and systems with a solution that is quick to deploy and easy to use. Securely store, share and manage passwords across the entire organization.

Simplify Secure Remote Access
Securely manage your remote desktop connections from anywhere – no VPN required.

Streamline Compliance and Audits
Provide on-demand visibility of access permissions to your organization's credentials and secrets.



KEEPER® PASSWORD MANAGER

Enables organizations to securely manage, protect, discover, share and rotate passwords with full control and visibility to simplify auditing and compliance.

KEEPER® SECRETS MANAGER

Delivers a fully-managed, cloud-based solution to secure infrastructure secrets such as API keys, database credentials, access keys and certificates.

KEEPER® CONNECTION MANAGER

Provides an agentless remote desktop gateway for instant privileged session management, remote infrastructure access and secure remote database access with RDP, SSH keys, database and Kubernetes – without the need for a VPN.