Regional Credit Union Gets Strong Returns on Password Management

KEEPER®

A growing credit union uncovers opportunities to update and fortify outmoded password management procedures.

Challenge

- Requirement to comply with strict data security requirements
- Weak password practices among employees

Solution

- Password manager and digital vault
- 2FA for extra protection
- Auditing capabilities
- Secure password sharing

Results

- Password management visibility
- Stronger password policy enforcement
- Reduced help desk calls

KEEPER®

About Quest Federal Credit Union

Quest Federal Credit Union, based in Kenton, Ohio, has $119 million in assets, more than 13,700 member/owners and nine branch locations. In 2019, Quest celebrated its 50th year serving member/owners and the communities in their three-county area.

The Challenge

As a small but fast-growing financial institution, Quest Federal Credit Union is subject to the same government regulations and data compliance rules as large national players. Quest stores member/owners' sensitive personal and financial data as well as information related to operations, disaster recovery, business intelligence and other mission-critical functions. Although strong cybersecurity was a high priority, Quest was vulnerable when it came to password management.

> **Quest is subject to the same government regulations and data compliance rules as large national players.**

Since financial institutions are common targets of phishing attacks and other cybercrime, Quest's management team had deployed Keeper's password manager to protect their personal passwords, files and other digital assets. Chief Information Officer Brian Sprang and other executives soon realized they needed the same comprehensive data security for all Quest employees. "As in many companies, I saw weak password management with handwritten passwords stuffed into top desk drawers and the same passwords used repeatedly," Brian recalled. "These are some of the many unsafe password practices that are so common."

Working with Quest's executive team and security officer, Brian made a list of criteria for an enterprise-wide password management solution. They insisted on encryption for security, auditing capabilities for visibility into employees' password practices, secure password sharing across management teams, rapid deployment and low maintenance.

Importantly, they wanted to deploy the solution on all desktop and mobile devices, regardless of operating system, to accommodate Quest's BYOD (bring your own device) policy.

The Keeper Solution

After evaluating several options, Brian chose the Keeper password management solution for all Quest employees. In addition to features such as private vaults for each employee, an automated password generator, secure file storage and shared folders and passwords, Quest took advantage of Keeper's two-factor authentication (2FA) for an added layer of protection. "The solution from Keeper Security fit all our requirements," said Brian. "We were able to rapidly deploy it to all our employees, across all device types and operating systems."

The Results

Keeper gives Brian and other Quest executives visibility into who is using the password management solution. This enables them to enforce password and 2FA policies, drive best practices and leverage internal controls. "The reporting features are very robust," Brian said of the Keeper solution. He noticed an immediate reduction in time spent resetting passwords and in the number of associated help desk calls. Keeper also improved Quest's compliance with security regulations. "I know we all sleep better at night knowing Keeper is protecting us."

> **I know we all sleep better at night knowing Keeper is protecting us.**

The Impact

Financial services firms experience cybersecurity attacks 300 times more often than businesses in other industries.[1] Weak passwords, which lead to 81 percent of data breaches across all industries,[2] are a big contributing factor.

> **Weak passwords lead to 81 percent of data breaches.**

Password management must be prioritized for all employees who have access to valuable data. For Quest, the Keeper solution helps them protect member/owner assets and continue to serve their communities with integrity.

About Keeper

Keeper Security develops leading password manager and security software for protecting businesses and client information. Keeper works with companies of all sizes across every industry to mitigate the risk of data breaches, bolster data security and privacy, increase employee productivity and strengthen cybersecurity reporting and compliance.

To learn more about Keeper Security's leading password manager and security software, visit **keepersecurity.com.**

---

[1] Mirchandani, Bhakti. "Laughing All The Way To The Bank: Cybercriminals Targeting U.S. Financial Institutions," Forbes, August 28, 2018

[2] Verizon Data Breach Investigations Report, 2017