Customer Case Study

Enterprise-Grade Cybersecurity for a Regional Credit Union

Comprehensive password management solution strengthens defense against growing cyber threat.

Strong security is as mission-critical to a regional credit union as it is to national financial institutions. Regardless of size, all credit unions store sensitive personal and financial information in digital files. They are subject to the same government regulations and data compliance rules. They have vital data assets on customers, operations, disaster recovery, business intelligence and other competitive items.

Further, all credit unions are targets of phishing attacks and other social engineering malfeasance. With credit union staff using a growing number of mobile devices to access this data anywhere and at anytime, password management has risen to the top of the priority list for credit union CIOs everywhere.

That was certainly the case at Quest Federal Credit Union. When current CIO Brian Sprang arrived at Quest two years ago, he had some experience with password management solutions from his previous job. He noticed that Quest's management staff had deployed a solution from Keeper to protect their personal passwords, files and other digital assets. But with the ever-shifting threat environment, Sprang and top executives at Quest realized a comprehensive password management solution was needed for all Quest employees.

Banishing Weak Password Practices

"As at many places, I saw weak password management with handwritten passwords stuffed into top drawers and the use of the same password repeatedly," Sprang recalls. "These are some of the many unsafe password practices that are so common."

Working with the executive team and the security officer at Quest, Sprang drew up a list of criteria for a password management solution. It included:

- Secure and encrypted password management
- Ability of the solution to be deployed on all desktop and mobile devices, regardless of OS as Quest maintains a BYOD policy
- Strong auditing capabilities to provide the CIO maximum visibility into who is using the solution and how strong their password practices are
- Rapid deployment and low maintenance capabilities

"We also wanted a solution that would allow us to securely share passwords across management teams in the event someone is on vacation or otherwise indisposed," Sprang notes. "The solution from Keeper Security fit all our requirements."

Quest Federal Credit Union

- Originally organized in 1969 in Kenton, Ohio
- Currently operates four branches with expansion to a fifth planned
- Nearly $100 million in assets
- More than 13,000 credit union members
- Goal: To embrace cyber security the same way as national financial institutions

Keeper Delivers for Quest

For starters, Sprang was able to rapidly deploy Keeper to all employees. Sprang took advantage of Keeper's two-factor authentication protection and found deployment to be seamless across all devices types and operating systems.

Keeper has given Quest's CIO visibility into who is using the solution and the ability to set enforcement policies for the use of strong-passwords and two-factor authentication. He is able to drive password-management best practices that support strong internal control policies.

"The reporting features are very robust," Sprang says of the Keeper solution. He immediately noticed a reduction in time spent resetting passwords and in the quantity of associated help-desk calls. Keeper allowed Quest to conform to necessary compliance regulations.

> **"With Keeper, I know we all sleep better at night."**
>
> **Brian Sprang**
> CIO, Quest Federal Credit Union