keeper

Customer Case Study

Healthcare Organization Cures Password Problem with Keeper

Keeper with DUO Provides Highly Efficient and Secure Password Management

As a fast-growing healthcare system serving its communities for 57 years, Grand River Hospital District (GRHD) has aggressively hired more and more staff to improve the health and well-being of its community members. In doing so, its IT department now manages an increasing number of passwords for the entire organization.

Given the need for an effective, efficient and secure way to manage passwords, the IT department looked into password management software. “The multi-page paper master password list was outgrowing our department,” said Daniel Wilson, Network Engineer at GRHD, “so the biggest thing for us is to have role-based permission to passwords and keep them secure.” The multi-page password list was not a viable option.

Filling in Needs of Mobile First and Zero-Knowledge Security Architecture

GRHD had multiple functional requirements for its password management software in addition to security. Like many organizations, they sought a solution with the ability to:

1. Easily import and export passwords
2. Access all platforms (especially mobile)
3. Access the password vault offline

The GRHD IT department is increasingly mobile and needs a mobile-friendly solution. Daniel said, “Keeper is the only password manager we looked at that provides an excellent mobile experience and passes our security requirements. Being mobile is an absolute advantage in today’s world.” Regardless of the device or platform your employees use, Keeper is able to enforce password best practices. The records automatically sync across your devices with full online and offline access.

Security is central to GRHD’s requirements. Keeper stood out with its *zero-knowledge* architecture. Daniel added that “One of the things that we liked about Keeper is that no one in your staff has access to our records.” The Keeper user is the only person that has full control over their data. With Keeper, encryption and decryption occur only on the user’s device upon logging into the vault.

Rich Features Designed for Businesses

Password resets are a major burden to IT departments. In fact, according to Gartner’s research, 50% of help desk calls are the result of a forgotten password. GRHD faced the same problem, and Keeper solved that by adapting service to GRHD’s organizational structure and policies. Keeper’s configurable roles, role-based permissions and admin privileges, all assignable by specific organizational hierarchy, ensure a perfect fit with any unique environment.

grand river Health

At a Glance

- A local healthcare system located in Rifle, Colorado
- Formed in 1961, designed around the needs of the communities it serves
- Covers 1,500 square miles and its 55 affiliated physicians and over 300 employees serve a population base exceeding 27,000

Challenge

- As the organization grew and systems became more complex, the IT department was challenged to handle an increasing number of accounts
- The old way of managing passwords through paper master password lists, lacked the security and efficiency requirements of the organization

"The biggest advantage for GRHD is that now if help desk agents need a password, they can come to anyone in the IT department. As the admins of our Keeper vault, we can share the password with the controlled credential," said Daniel. Access to records can be retracted at any time. Hence, Keeper securely manages the lifecycle of privileged account credentials.

Having configurable roles and role-based permissions for password management is critical to GRHD, especially for employees' onboarding. When a new person starts, IT can slowly give them access to what they need. It allows the IT department to streamline the onboarding process. At the same time, your employees have on-demand access to passwords, websites and applications increasing their productivity while protected with best-in-class security.

Two-Factor Authentication: Keeper's Strategic Alignment to Improve Security

Two-Factor Authentication (2FA) provides an extra layer of security when logging into websites or applications. Keeper has partnered with DUO Security to provide easy 2FA for business customers. DUO Security is a cloud-based trusted access provider protecting the world's fastest-growing companies and thousands of organizations worldwide. With DUO, IT administrators can monitor login attempts from any user, in any location, from any device.

GRHD uses DUO 2FA with Keeper. The integration provides the added layer of protection to prevent unauthorized access. Daniel said, "we needed a second factor to access the password vault and have been happy with DUO."

> Learn more about 2FA with Keeper

> Become a Keeper Business User

Solution

- Keeper provided a role-based password management solution that can scales with any sized business
- Keeper stood out with its *zero-knowledge* security methodology and and advanced features, including team sharing, departmental auditing and delegated administration
- Utilization of Duo added an extra layer of protection against unauthorized access