KEEPER® + saint apollonia

Case Study

Saint Apollonia Increases Security and Enforces Secure Password Management With Keeper

Background

Saint Apollonia is an organization within the healthcare management industry for dentistry services and more. While focused on modern dental techniques and training with the latest technology and materials, their subsidiary MINT Dentistry is one of the fastest-growing dental practices in the United States.

Industry
Healthcare Management - Dentistry

Employees
1,200

Solutions
Keeper Password Manager

- Enterprise
- Platinum Support

The Challenge

Saint Apollonia's Information Technology (IT), Human Resources (HR), billing and insurance departments needed an easy-to-use, secure and collaborative password management solution to replace an existing password management tool that was lacking flexibility, security and adoption across the organization.

Before adopting Keeper, employees at Saint Apollonia relied on the legacy password manager which took a significant amount of time to set up and was not providing the tools needed to fortify their security posture. The legacy solution had a cumbersome user interface which limited adoption among end-users, as well as dated access controls, a lack of customer support and a long, non-intuitive onboarding process. Additionally, the cost of internal resources needed to maintain the legacy solution outweighed the benefits. The Saint Apollonia IT team decided it was time to look for better options.

Poor User Adoption: Within the healthcare industry, companies such as Saint Apollonia work with numerous insurance providers, all with their own login portals and processes, which results in many different credentials for the billing, insurance and HR departments to keep track of. As a result, some employees would use shared spreadsheets or other unsecure methods to store and share passwords across teams.

Limited Visibility and Admin Controls: The system administrators often struggled with limited access control capabilities, especially when decommissioning and transferring the stored credentials of employees who had left the organization as well as contractors who needed short-term visibility. The lack of critical access control was risky and difficult to manage.

Lack of Resources and Support: The legacy vendor's customer support team would be unable to solve Saint Apollonia's requests for onboarding and connecting integrations. Furthermore, the vendor was not proactive in providing training or enablement materials for end-users.

The Keeper Solution

User Adoption and Training: Keeper is recognized as the leading password manager for organizations of all sizes and is designed to be easy to use and quick to deploy. Keeper's extensive documentation portal provides detailed instructions and system best practices to help administrators get the most out of their deployment. For end-users, detailed product guides and training videos drive high end-user adoption.

Additionally, Keeper's award-winning User Interface (UI) provides an intuitive and accessible platform that is easy for non-technical employees to understand and adopt. Keeper also supports cross-platform use on Windows, Mac, Linux, iOS and Android, ensuring that the solution works seamlessly no matter the platform or device.

Role-Based Access Controls (RBAC): Keeper provides granular sharing enforcement for administrators to leverage Role-Based Access Controls (RBAC) that ensure organization-wide security policies are adhered to and compliance is met. Designating roles within the organization streamlines provisioning for administrators and allows for specific rule sets to be leveraged to maintain least privilege access and increase the organization's security posture.

Cost Effective: No matter the size or type of organization, Keeper has a cost-effective plan to fit and scale with organizational needs. Keeper's transparent pricing model, paired with world-class customer support, ranking #1 in Enterprise Customer Support on G2, ensures that organizations maximize their investment.

Best-in-Class Security: Keeper's zero-trust and zero-knowledge security architecture is unmatched in safeguarding information and mitigating the risk of a data breach. Keeper combines device-level, Elliptic-Curve Cryptography (ECC) with multiple layers of encryption (at the vault, folder and record level), multi-factor and biometric authentication, as well as FIPS-140-2 validated AES 256-bit encryption plus PBKDF2.

Keeper is SOC 2 and ISO 27001 compliant - with the longest-standing compliance in the industry - as well as FedRAMP and StateRAMP Authorized.

Organization Impact

Saint Apollonia seamlessly transitioned from its legacy password management system to Keeper, providing a better end-user experience, improved user adoption and organizational security. The organization works with third-party vendors who require certain security policies to be adhered to and Keeper assists the organization in maintaining best-in-class security.

Implementation: Saint Apollonia was able to transition their credentials from the legacy password manager into Keeper within hours. The previous solution took three months to set up; therefore, they allotted time to get Keeper up and running and were surprised at how fast it was to deploy. By implementing Keeper, the organization now has improved visibility, allowing admins to keep a close eye on compliance with password hygiene best-practices and security policies.

> **I have used Keeper for years and it just works. I had Keeper completely set up and imported our credentials in less than one day.**
>
> **Cody Jensen | Application Support Manager**

User Adoption: Keeper's streamlined user interface and detailed enablement training materials resulted in high user adoption. Keeper has made it possible for employees to securely share passwords with each other, while still leveraging Keeper's encryption.

Across teams, the Shared Folder feature allows the organization to maintain an orderly and secure method of sharing critical passwords and information. Keeper's One-Time Share has enabled secure sharing of files and credentials in a limited capacity.

Security and Visibility: The organization seamlessly integrated Keeper with their SSO provider, allowing employees to authenticate into Keeper with their SSO credentials as well as securely access the organization's cloud and native applications that don't support SSO. For online accounts, KeeperFill®, Keeper's secure browser extension, allows users to instantly autofill credentials on any device.

These integration capabilities and ease of use, along with Keeper's best-in-class security and zero-knowledge security architecture, provided Saint Apollonia with a secure password management solution to protect their organization against cyber threats.

Keeper Password Manager

Most businesses have limited visibility into the password practices of their employees, which greatly increases cyber risk. Password hygiene cannot be improved without critical information regarding password usage and compliance. Keeper solves this by providing ultimate security, visibility and control.

Data is protected with Keeper's zero-knowledge security architecture and world-class encryption. Zero-knowledge means that only the user has knowledge of and access to their master password and the encryption key that is used to encrypt and decrypt their information.

Keeper is intuitive and easy to deploy, regardless of the size of a business. Keeper integrates with Active Directory and LDAP servers, which streamline provisioning and onboarding. Keeper SSO Connect® integrates into existing SSO solutions and is FedRAMP and StateRAMP Authorized.

Keeper is designed to scale for any sized organization. Features such as role-based permissions, team sharing, departmental auditing and delegated administration, support organizations as they grow. Keeper Commander provides robust APIs to integrate into current and future systems.

Business Use Cases: Keeper Password Manager

- Prevent password-related data breaches and cyber attacks
- Strengthen compliance
- Boost employee productivity
- Enforce password policies and procedures
- Reduce help desk costs
- Minimize training with fast time-to-security
- Improve employee security awareness and behavior

About Keeper

Keeper Security is transforming cybersecurity for people and organizations around the world with next-generation privileged access management. Keeper's easy-to-use cybersecurity solutions are built with zero-trust and zero-knowledge security to protect every user on every device. Trusted by millions of individuals and thousands of organizations, Keeper is the leader for password management, secrets management, privileged access, secure remote access and encrypted messaging. Learn more at KeeperSecurity.com.

Keeper is trusted and loved by thousands of companies and millions of people globally.

G2
Enterprise Leader

PCMag
Editor's Choice

App Store
Top-Rated Productivity

Google Play
Over 10 Million Installs