KEEPER + St. Anna Kinderkrebsforschung

CASE STUDY

St. Anna Children's Cancer Research Institute Enables Secure Password Management

BACKGROUND

St. Anna Children's Cancer Research Institute, based in Vienna, Austria, has been working towards the goal of improving the cure rate for children and adolescents with cancer since 1988. The St. Anna Children's Cancer Research Institute coordinates multicenter studies, and thus, actively participates in international developments on pediatric oncology.

Industry
Healthcare

Employees
250+

Solutions
Keeper Password Manager

- Enterprise
- BreachWatch®
- Advanced Reporting & Alerts Module

THE CHALLENGE

St. Anna Children's Cancer Research Institute (St. Anna CCRI), a prominent organization dedicated to pediatric cancer research, faced significant challenges in managing and securing their digital credentials. As a hub of scientific research and collaboration, the organization's workforce, composed primarily of researchers and administrative staff, required a password management system to handle sensitive data securely and efficiently.

Prior to implementing Keeper, St. Anna CCRI relied on a legacy password manager that had several critical problems. The primary issues were the low adoption rate among the non-technical staff, as well as the limited visibility and reporting for admins. Additionally, the highly publicized 2022 data breach of the legacy system further hindered user adoption and utilization of the product. St. Anna CCRI needed a comprehensive, secure and user-friendly password manager that could integrate with its existing tech stack, support the organization's collaborative work environment and restore trust among staff.

Poor User Adoption - End-users found the legacy system cumbersome and unintuitive. As a result, many continued to use risky and outdated methods of password management, such as sticky notes or shared spreadsheets. These practices not only posed a significant security risk, but also hindered productivity and collaboration within the organization.

Limited Visibility and Admin Controls - The system administrators struggled with limited access control capabilities, especially with decommissioning and transferring the stored credentials of employees who were short-term contractors for the company. The lack of critical access control and visibility was a major cause for concern.

Security Issues - When the legacy password manager experienced a public security breach in 2022, St. Anna CCRI staff began to abandon the solution internally. This incident not only exposed the institute to potential data theft and cyber threats, but also resulted in staff losing trust in the existing system. The breach highlighted the need for a more secure and reliable solution to safeguard the organization's highly sensitive information.

THE KEEPER SOLUTION

St. Anna CCRI found its solution in Keeper, a robust and user-friendly password management system that addresses their critical needs. Keeper's platform offers a unique blend of seamless integration capabilities, ease of use and best-in-class security making it the ideal choice for the organization's collaborative environment.

User Adoption and Training – Keeper provides an intuitive web browser extension that enables seamless autofill of passwords and login information, eliminating the need for employees to remember or manually enter credentials. This feature is particularly beneficial for non-technical staff, simplifying their daily operations. Additionally, Keeper's documentation portal provides extensive and easy-to-navigate resources for administrators. For end users, Keeper's intuitive product guides and training videos ensure high employee adoption, no matter what their level of technical proficiency may be.

Role-Based Access Controls (RBAC) – Keeper's platform provides powerful collaboration and organizational features such as secure password sharing and role-based access controls. These out-of-the-box features enable administrators to set specific controls on record and password sharing, ensuring organization-wide compliance with security policies.

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 has the longest-standing SOC 2 and ISO 27001 certifications in the industry. Keeper is GDPR, CCPA and HIPAA compliant, as well as FedRAMP and StateRAMP Authorized, PCI DSS certified and certified by TrustArc for privacy.

Keeper combines device-level, elliptic curve cryptography with multiple layers of encryption (at the vault, folder and record level), multi-factor and biometric authentication, and FIPS-140-2 validated AES 256-bit encryption plus PBKDF2.

> **From the IT security side, the biggest concern was the usage of notes on the desk and the insecure storage of the passwords and credentials. For the acceptance from the end-users, the collaboration feature for sharing records and files was the key. Keeper was more accepted because collaboration is much easier than anything they have done before.**
>
> **– Ingomar Schmickl | Head of IT**
> St. Anna Children's Cancer Research Institute

ORGANIZATION IMPACT

The implementation of Keeper at St. Anna CCRI marked a significant turning point in the organization's approach to data security and operational efficiency. The transition from the legacy password management system to Keeper not only enhanced their security posture but also had a profound impact on overall workflow and productivity within the organization.

Implementation – St. Anna CCRI had allocated a three-month period for the transition of their records and credentials from their legacy system to Keeper. However, due to Keeper's automated import tools, this process was significantly expedited, and completed months ahead of schedule with minimal disruption to daily operations. This efficiency is a testament to Keeper's user-friendly design and seamless integration capabilities. Specifically, Keeper integrates with St. Anna CCRI's existing Identity Provider (IdP), further streamlining administrative functionality and user management, while enhancing security.

User Adoption – St. Anna CCRI leverages Keeper's shared folders feature– functionality that allows users to manage access to critical systems, such as research databases, efficiently and securely. Keeper's One-Time Share feature enables secure sharing of files and credentials in a time-limited and device-locked capacity. By using shared folders and One-Time Share, St. Anna CCRI teams can easily collaborate and share necessary credentials without compromising on security– safeguarding their research.

Security and Visibility – To ensure their employees were no longer storing or sharing their credentials using outdated methods, St. Anna CCRI leveraged Keeper's Admin Console to gain visibility and control over employee password usage. This feature allows the admins to quickly and easily understand the state of their organization's password and credential security. By utilizing Keeper for password management, password storage and record sharing is now standardized across the whole institute.

The organization-wide adoption of Keeper has positioned St. Anna CCRI at the forefront of data security. The successful transition to Keeper, along with the added layers of security, serve as a model for other organizations facing similar challenges in securing their sensitive data and maintaining security protocols.

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 any existing SSO solutions using SAML 2.0.

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