KEEPER® + St. Anna Kinderkrebsforschung

FALLSTUDIE

Das St. Anna Kinderkrebsforschung GmbH gewährleistet eine sichere Passwortverwaltung

HINTERGRUND

Das St. Anna Kinderkrebsforschung GmbH mit Sitz in Wien, Österreich, arbeitet seit 1988 an dem Ziel, die Heilungsrate für krebskranke Kinder und Jugendliche zu verbessern.

Das St. Anna Kinderkrebsforschung GmbH koordiniert multizentrische Studien und beteiligt sich so aktiv an internationalen Entwicklungen in der pädiatrischen Onkologie.

Branche
Gesundheitswesen

Mitarbeiter
Mehr als 250

Lösungen
Keeper Password Manager

- Enterprise
- BreachWatch®
- Advanced Reporting & Alerts Module

DIE HERAUSFORDERUNG

Das St. Anna Kinderkrebsforschung GmbH (St. Anna) ist eine renommierte Organisation, die sich der pädiatrischen Krebsforschung widmet. Das Unternehmen stand vor großen Herausforderungen bei der Verwaltung und Sicherung seiner digitalen Anmeldeinformationen. Als Drehscheibe für wissenschaftliche Forschung und Zusammenarbeit benötigten die Mitarbeiter der Organisation, die hauptsächlich aus Forschern und Verwaltungspersonal bestand, ein System zur Passwortverwaltung, um sensible Daten sicher und effizient zu handhaben.

Vor der Implementierung von Keeper verwendete das St. Anna einen alten Password Manager, der mehrere kritische Probleme mit sich brachte. Die wesentlichen Probleme waren die geringe Akzeptanz bei den technisch weniger versierten Mitarbeitern sowie die eingeschränkte Transparenz und Berichterstattung für die Admins. Darüber hinaus behinderte das im Jahr 2022 bekannt gewordene Datenleck des Altsystems die Akzeptanz und Nutzung des Produkts durch die Benutzer. Das St. Anna benötigte einen umfassenden, sicheren und benutzerfreundlichen Password Manager, der sich in das bestehende technische System integrieren ließ, die kollaborative Arbeitsumgebung der Organisation unterstützte und das Vertrauen der Mitarbeiter wiederherstellte.

Geringe Benutzerakzeptanz - Die Endbenutzer empfanden das Altsystem als umständlich und wenig intuitiv. Infolgedessen verwendeten viele weiterhin riskante und veraltete Methoden der Passwortverwaltung, wie z. B. Haftnotizen oder gemeinsam genutzte Tabellen. Diese Praktiken stellten nicht nur ein erhebliches Sicherheitsrisiko dar, sondern behinderten auch die Produktivität und Zusammenarbeit innerhalb der Organisation.

Eingeschränkte Transparenz und Admin-Kontrollen - Die Systemadministratoren hatten mit begrenzten Zugriffskontrollfunktionen zu kämpfen, insbesondere mit der Stilllegung und Übertragung der gespeicherten Anmeldeinformationen von Mitarbeitern, die kurzfristige Auftragnehmer des Unternehmens waren. Der Mangel an kritischer Zugriffskontrolle und Transparenz war Anlass zu großer Sorge.

Sicherheitsprobleme -Als der alte Password Manager im Jahr 2022 von einer Sicherheitsverletzung betroffen war, begannen die Mitarbeiter des St. Anna, die Lösung intern zu verwerfen. Dieser Vorfall setzte das Institut nicht nur potenziellem Datendiebstahl und Cyberbedrohungen aus, sondern führte auch dazu, dass die Mitarbeiter das Vertrauen in das bestehende System verloren. Der Verstoß machte deutlich, dass eine sicherere und zuverlässigere Lösung zum Schutz der hochsensiblen Daten des Unternehmens benötigt wurde.

DIE KEEPER-LÖSUNG

Das St. Anna fand seine Lösung in Keeper, einem robusten und benutzerfreundlichen Passwortverwaltungssystem, das seine kritischen Anforderungen erfüllt. Die Plattform von Keeper bietet eine einzigartige Mischung aus nahtlosen Integrationsmöglichkeiten, Benutzerfreundlichkeit und erstklassiger Sicherheit, was sie zur idealen Wahl für die kollaborative Umgebung des Unternehmens macht.

Benutzerakzeptanz und -schulung – Keeper bietet eine intuitive Webbrowser-Erweiterung, die ein nahtloses automatisches Ausfüllen von Passwörtern und Anmeldeinformationen ermöglicht. So müssen sich die Mitarbeiter nicht mehr an ihre Anmeldeinformationen erinnern oder sie manuell eingeben. Diese Funktion ist besonders für technisch wenig versierte Nutzer von Vorteil, da sie ihre täglichen Abläufe vereinfacht. Darüber hinaus bietet das Dokumentationsportal von Keeper umfangreiche und leicht zu navigierende Ressourcen für Administratoren. Für Endbenutzer sorgen die intuitiven Produktanleitungen und Schulungsvideos von Keeper für eine hohe Akzeptanz bei den Mitarbeitern, unabhängig von deren technischen Kenntnissen.

Rollenbasierte Zugriffskontrollen (RBAC) – Die Plattform von Keeper bietet leistungsstarke Kollaborations- und Organisationsfunktionen wie die sichere Passwortfreigabe und rollenbasierte Zugriffskontrollen. Mit diesen sofort einsatzbereiten Funktionen können Administratoren spezifische Kontrollen für die gemeinsame Nutzung von Datensätzen und Passwörtern einrichten und so die unternehmensweite Einhaltung von Sicherheitsrichtlinien gewährleisten.

Erstklassige Sicherheit – Die Zero-Trust- und Zero-Knowledge-Sicherheitsarchitektur von Keeper ist unübertroffen, wenn es um den Schutz von Informationen und die Minderung des Risikos eines Datenlecks geht. Keeper verfügt über die am längsten bestehenden SOC 2- und ISO 27001-Zertifizierungen in der Branche. Keeper ist DSGVO-, CCPA- und HIPAA-konform sowie FedRAMP- und StateRAMP-autorisiert, PCI DSS-zertifiziert und von TrustArc für den Datenschutz zertifiziert.

Keeper kombiniert Elliptische Kurven-Kryptografie auf Geräteebene mit mehreren Verschlüsselungsebenen (auf Tresor-, Ordner- und Datensatzebene), Multifaktor- und biometrischer Authentifizierung sowie FIPS-140-2-validierter AES 256-Bit-Verschlüsselung plus PBKDF2.

> **Im Hinblick auf die IT-Sicherheit waren die größten Bedenken die Verwendung von Notizen auf dem Schreibtisch und die unsichere Aufbewahrung von Passwörtern und Anmeldeinformationen. Für die Akzeptanz bei den Endnutzern war die Kollaborationsfunktion zur gemeinsamen Nutzung von Datensätzen und Dateien der Schlüssel. Keeper wurde besser angenommen, weil die Zusammenarbeit viel einfacher ist als alles, was bisher gemacht wurde.**
>
> **Ingomar Schmickl | Head of IT**
> **St. Anna Children's Cancer Research Institute**

AUSWIRKUNGEN AUF DIE ORGANISATION

Die Implementierung von Keeper im St. Anna markierte einen bedeutenden Wendepunkt in der Herangehensweise der Organisation an Datensicherheit und betriebliche Effizienz. Die Umstellung von dem alten System zur Passwortverwaltung auf Keeper hat nicht nur die Sicherheit verbessert, sondern auch den gesamten Arbeitsablauf und die Produktivität innerhalb des Unternehmens nachhaltig beeinflusst.

Implementierung – Das St. Anna hatte einen Zeitraum von drei Monaten für die Übertragung seiner Datensätze und Anmeldeinformationen von seinem Altsystem auf Keeper vorgesehen. Doch dank der automatisierten Import-Tools von Keeper konnte dieser Prozess erheblich beschleunigt und Monate früher als geplant abgeschlossen werden, und das bei minimaler Unterbrechung des laufenden Betriebs. Diese Effizienz ist ein Beweis für das benutzerfreundliche Design und die nahtlosen Integrationsmöglichkeiten von Keeper. Konkret lässt sich Keeper in den bestehenden Identitätsanbieter (IdP) des St. Anna integrieren, was die Verwaltungsfunktionen und die Benutzerverwaltung weiter vereinfacht und gleichzeitig die Sicherheit erhöht.

Benutzerakzeptanz – Das St. Anna nutzt die Funktion für freigegebene Ordner von Keeper – eine Funktion, die es Benutzern ermöglicht, den Zugriff auf kritische Systeme wie Forschungsdatenbanken effizient und sicher zu verwalten. Die einmalige Freigabe-Funktion von Keeper ermöglicht die sichere Freigabe von Dateien und Anmeldeinformationen in einer zeitlich begrenzten und gerätegeschützten Kapazität. Durch die Verwendung von freigegebenen Ordnern und der einmaligen Freigabe können die Teams des St. Anna problemlos gemeinsam arbeiten und die erforderlichen Anmeldeinformationen austauschen, ohne dabei Kompromisse bei der Sicherheit einzugehen. Der Schutz ihrer Forschung ist gewährleistet.

Sicherheit und Transparenz – Um sicherzustellen, dass die Mitarbeiter ihre Anmeldeinformationen nicht mehr mit veralteten Methoden speichern oder weitergeben, nutzte das St. Anna die Admin-Konsole von Keeper, um Transparenz und Kontrolle über die Passwortnutzung der Mitarbeiter zu erhalten. Diese Funktion ermöglicht es den Administratoren, sich schnell und einfach einen Überblick über den Stand der Sicherheit der Passwörter und Anmeldeinformationen in ihrem Unternehmen zu verschaffen. Durch den Einsatz von Keeper für die Passwortverwaltung sind die Speicherung von Passwörtern und die gemeinsame Nutzung von Datensätzen nun im gesamten Institut standardisiert.

Die unternehmensweite Einführung von Keeper hat das St. Anna an die Spitze der Datensicherheit gebracht. Die erfolgreiche Umstellung auf Keeper und die zusätzlichen Sicherheitsebenen dienen als Modell für andere Organisationen, die vor ähnlichen Herausforderungen bei der Sicherung ihrer sensiblen Daten und der Aufrechterhaltung von Sicherheitsprotokollen stehen.

KEEPER PASSWORD MANAGER

Die meisten Unternehmen haben nur einen begrenzten Einblick in die Passwortpraktiken ihrer Mitarbeiter, was das Cyberrisiko erheblich erhöht. Die Passworthygiene kann nicht verbessert werden, wenn keine wichtigen Informationen über die Verwendung von Passwörtern und deren Einhaltung vorliegen. Keeper löst dieses Problem, indem es für ultimative Sicherheit, Transparenz und Kontrolle sorgt.

Die Daten sind mit der Zero-Knowledge-Sicherheitsarchitektur und der erstklassigen Verschlüsselung von Keeper geschützt. Zero-Knowledge bedeutet, dass nur der Benutzer Wissen und Zugriff auf sein Master-Passwort sowie den Verschlüsselungsschlüssel hat, der zur Ver- und Entschlüsselung seiner Informationen verwendet wird.

Keeper ist unabhängig von der Größe eines Unternehmens intuitiv und einfach zu implementieren. Keeper kann mit Active Directory- und LDAP-Servern integriert werden, was die Bereitstellung und das Onboarding optimiert. Keeper SSO Connect® lässt sich mit SAML 2.0 in alle vorhandenen SSO-Lösungen integrieren.

Keeper ist so konzipiert, dass es für jede Unternehmensgröße geeignet ist. Funktionen wie rollenbasierte Berechtigungen, Team-Sharing, Abteilungsaudits und delegierte Verwaltung unterstützen Organisationen bei ihrem Wachstum. Keeper Commander bietet robuste APIs, die sich in aktuelle und zukünftige Systeme integrieren lassen.

Geschäftsbezogene Anwendungsfälle: Keeper Password Manager

- Verhindern Sie passwortbezogene Datenverletzungen und Cyberangriffe
- Stärken Sie die Compliance
- Steigern Sie die Produktivität der Mitarbeiter
- Setzen Sie Passwortrichtlinien und -verfahren durch
- Reduzieren Sie die Helpdesk-Kosten
- Minimieren Sie Schulungen mit schnellen Sicherheitszeitsmaßnahmen
- Verbessern Sie das Sicherheitsbewusstsein und das Verhalten der Mitarbeiter

Über Keeper

Keeper Security ist eines der am schnellsten wachsenden Unternehmen für Cybersicherheitssoftware und schützt über 100.000 Organisationen und Millionen von Menschen in mehr als 150 Ländern. Keeper ist ein Pionier der Zero-Knowledge- und Zero-Trust-Sicherheit für jede IT-Umgebung. Das Herzstück, KeeperPAM®, ist eine KI-fähige, Cloud-native Plattform, die alle Benutzer, Geräte und Infrastrukturen vor Cyberangriffen schützt. Keeper wurde für seine Innovationen im Gartner Magic Quadrant für Privileged Access Management (PAM) ausgezeichnet und sichert Passwörter und Passkeys, Infrastrukturgeheimnisse, Remote-Verbindungen und Endpunkte mit rollenbasierten Durchsetzungsrichtlinien, Least-Privilege und Just-in-Time-Zugriff. Erfahren Sie auf **KeeperSecurity.com**, warum führende Organisationen auf Keeper vertrauen, um sich gegen moderne Cyberbedrohungen zu verteidigen.

Auf Keeper vertrauen Tausende Unternehmen und Millionen Menschen weltweit.

G2
Führend in Unternehmen

PCMag
Editor's Choice

App Store
Erstklassig bewertete Produktivität

Google Play
Über 10 Millionen Installationen