Case Study

Global IT Firm Enhances Security and Compliance With Keeper

Background

The organisation is a technology services company with clients across diverse industries, including finance, telecommunications, media, retail and healthcare.

Industry
Technology Services

Employees
11,000+

Solutions
Enterprise Password Manager

- Platinum Support

The Challenge

As a rapidly growing company with a global workforce, the organisation felt strongly about wanting to increase password security. Employees were using various password management solutions, leading to fragmentation, inconsistency and a lack of visibility into credential management.

Additionally, IT administrators wanted to impart security best practices across departments. As the organisation enhanced ISO and other cybersecurity standards, the lack of a unified password management solution created compliance gaps and administrative inefficiencies.

Key challenges included:

Limited Visibility and Access Control: Employees used different tools, such as **browser-based password managers**, making security enforcement and maintaining data hygiene difficult.

Compliance Requirements and Security Risks: Meeting continued improvement for ISO and cybersecurity certification standards required a structured, enterprise-grade solution. The organisation needed further visibility into credential hygiene and a seamless way to enforce data security best practices.

> We wanted to unify our password management under a single, secure solution that our cybersecurity team could review and manage.
>
> **- Head of Project Delivery Management**

The Keeper Solution

The organisation evaluated multiple password management solutions before selecting Keeper Security. Keeper stood out as one of the most secure and feature-rich options, offering enterprise-grade password protection, secure credential sharing and best-in-class security. Keeper's solution provides many benefits, including:

Centralised Password Management - Keeper provided the organisation with a single, secure platform for storing and managing the organisation's passwords. This ensured that all credentials were protected with Keeper's zero-trust and zero-knowledge architecture.

User Adoption and Training - Keeper is recognised as the leading password manager for organisations 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 user adoption.

> We offered our team both end-user training and training for the admins. It's quite an intuitive interface, and we had a really smooth implementation experience.
>
> **– Head of Project Delivery Management**

Advanced Security Features - Keeper's robust security measures, including Multi-Factor Authentication (MFA) and end-to-end encryption, ensure that sensitive internal communications and data are protected. The ability to securely and seamlessly share credentials among team members without exposing sensitive data adds an extra layer of protection.

Cost-Effective - No matter the size or type of organisation, Keeper has a cost-effective plan to fit and scale with organisational needs. Keeper's transparent pricing model paired with world-class customer support – ranked #1 in Enterprise Customer Support on G2 – ensures that organisations maximise 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 levels), multi-factor and biometric authentication, as well as FIPS 140-3 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 Authorised.

Organisation Impact

By implementing Keeper across the entire organisation – a globally distributed workforce of 11,000+ employees – the organisation gained centralised control over password and passkey security. This enabled the IT team to enforce strong password policies, monitor credential hygiene and facilitate secure access management. The key impacts include:

Stronger Security and Compliance - Keeper improved the organisation's security posture and ensured compliance with many industry-standard certifications, such as ISO certification requirements. IT administrators can now leverage Keeper's centralised dashboard to monitor credential security in real time.

Streamlined Onboarding and Offboarding - With Keeper, access to account credentials can be seamlessly provisioned or decommissioned during the onboarding or offboarding process. This, along with rolling Keeper out organisation-wide, has streamlined collaboration and operational efficiency.

User Adoption and Seamless Collaboration – Keeper's intuitive interface and ease of use have driven high adoption rates, particularly among non-technical staff. Keeper also offers a free Family Plan to all business users, which speeds up adoption. The user-friendly browser extension simplifies password and passkey management, improving collaboration across departments and reducing friction when accessing shared records.

> The team really liked how Keeper included a free family plan. It was an extra perk that made user adoption go even faster.
>
> **– Head of Project Delivery Management**

Security and Visibility – The organisation seamlessly integrated Keeper with its SSO provider, allowing employees to authenticate into Keeper with their SSO credentials as well as securely access the organisation's cloud and native applications that don't support SSO. KeeperFill® – a feature on Keeper's browser extension, mobile app and desktop app – allows users to instantly autofill credentials across websites and apps.

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

Keeper Password Manager

Most businesses have limited visibility into the password practices of their employees, which can greatly increase 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 the knowledge of, and access to their master password, and the encryption key used to encrypt and decrypt their information.

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

Keeper is designed to scale for organisations of any size. Features such as role-based permissions, team sharing, departmental auditing and delegated administration, support organisations 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
- Support passkeys for effortless authentication
- Strengthen compliance
- Boost employee productivity
- Enforce password policies and procedures
- Reduce help desk costs
- Minimise training with fast time-to-security
- Improve employee security awareness and behaviour

About Keeper

Keeper Security is transforming cybersecurity for millions of individuals and thousands of organisations globally. Built with end-to-end encryption, Keeper's intuitive cybersecurity platform is trusted by Fortune 100 companies to protect every user, on every device, in every location. Our patented zero-trust and zero-knowledge privileged access management solution unifies enterprise password secrets and connections management with zero-trust network access and remote browser isolation. By combining these critical identity and access management components into a single cloud-based solution, Keeper delivers unparalleled visibility, security and control while ensuring compliance and audit requirements are met. Learn how Keeper can defend your organisation against today's cyber threats 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