

Case Study

From Excel to Encrypted Vaults: How a Food Distributor Secured Its Credentials



Background

With operations spanning six countries across Central and Eastern Europe, this certified food distributor supplies major retail chains and employs approximately 300 people across a remote, multi-market workforce. Securing credentials consistently across teams and partner systems is fundamental to how the business operates.

Over the past three years, the organization has undergone a significant IT modernization effort, shifting from a largely reactive security posture to a proactive enterprise-grade one. Keeper became a core part of that investment.

Industry

Food Distribution

Employees

300+

Solutions

Business/Enterprise Password Manager

BreachWatch[®]



The Challenge

Managing credentials across multiple countries and a growing number of partner integrations, their lean IT team had let informal practices become a liability. Passwords lived in Excel files on shared drives with no access controls, no audit trail and more than 200 credentials with no consistent oversight. When someone was on leave, colleagues had no secure way to pick up where they left off. Meanwhile, service accounts from the testing phase kept their weak passwords indefinitely, creating security gaps that no automated process would ever catch.

Unprotected, Untracked and Unmonitored

The risks weren't just internal. Without visibility into whether credentials had been exposed in external breaches, the team had no way of knowing if a compromised password was already being exploited elsewhere. Credentials changed hands informally, least-privilege access went unenforced and there was no mechanism to surface weak or reused passwords before they became an incident. The gap between what the team could see and what was actually happening across their environment was significant, and growing.

“Half of all IT threats begin with credentials that were compromised or stolen. Sometimes users have a really easy password and it can be guessed immediately. That’s why password management is extremely important — and why we use Keeper now to make life easier.”

Head of IT





The Keeper Solution

The organization chose Keeper as its centralized password management platform for its cloud-native architecture, ease of use and security certifications. Starting with a small number of IT licenses, the deployment expanded progressively as additional teams were onboarded, with no implementation project required.

Centralized Credential Management for IT and Business Teams

Keeper replaced the Excel files and informal sharing with a single encrypted vault for each employee, enabling shared folders with role-based access. The IT team now manages all service accounts, partner credentials and shared system passwords from one place, giving every team member access to exactly what they need and nothing more.

“Onboarding was super easy — we paid for the licenses with a company credit card, and that was it. Most users don’t need any additional training at all.”

Head of IT

Secure Credential Sharing and One-Time Access

Keeper’s One-Time Share feature gave the team a secure way to hand off credentials to external engineers and vendors without permanently exposing passwords. Certificates, configuration documents and other sensitive files are stored in the vault alongside credentials, giving the team a single location for operationally critical assets.

Dark Web Monitoring With BreachWatch®

When the Head of IT first ran BreachWatch, a dark web monitoring add-on, it surfaced weak service account passwords left over from test phases — credentials that would never have been caught manually. Weak or exposed passwords are now automatically flagged the instant they’re uncovered, significantly reducing the risk of breaches.



Organization Impact

Since deploying Keeper, the organization has replaced an ad hoc approach to credential storage with a structured and auditable system. The IT team has a centralized view of all credentials across the business for the first time, significantly reducing the risk associated with weak or forgotten passwords.

A Single Source of Truth for Credentials Across the Organization

Keeper’s One-Time Share feature gave the team a secure way to hand off credentials to external engineers and vendors without permanently exposing passwords. Certificates, configuration documents and other sensitive files are stored in the vault alongside credentials, giving the team a single location for operationally critical assets.

“We have a clear overview of all the necessary passwords for IT and for other teams. We don’t have any issues now if someone is not available or if data was lost. It’s a single source of truth.”

Head of IT

Stronger Password Hygiene Across the Workforce

Employees now create and store unique, randomly generated passwords for every application and partner system. If an external partner suffers a breach, the exposure is limited to a single credential, not a reused password leveraged across multiple systems. BreachWatch provides ongoing assurance that nothing in the vault has been exposed on the dark web.

“The overall quality of passwords across the organization is much better.”

Head of IT





Keeper Password Manager

Most businesses have limited visibility into employees' password practices, which can significantly 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 only the user knows and has 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 business size. Keeper integrates with Active Directory and LDAP servers, which streamlines provisioning and onboarding. **Keeper SSO Connect**® integrates into existing SSO solutions and is FedRAMP High Certified and GovRAMP High Authorized.

Keeper is designed to scale for organizations of any size. Features such as role-based permissions, team sharing, departmental auditing and delegated administration support organizations as they grow. **Keeper Commander** provides robust APIs for integration with 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
- Minimize training with fast time-to-security
- Improve employee security awareness and behavior

About Keeper

Keeper Security is one of the fastest-growing cybersecurity software companies that protects thousands of organisations and millions of people in over 150 countries. Keeper is a pioneer of zero-knowledge and zero-trust security built for any IT environment. Its core offering, KeeperPAM®, is an AI-enabled, cloud-native platform that protects all users, devices and infrastructure from cyber attacks. Recognised for its innovation in the Gartner Magic Quadrant for Privileged Access Management (PAM), Keeper secures passwords and passkeys, infrastructure secrets, privileged sessions and endpoints with role-based enforcement policies, least privilege and just-in-time access..

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

Gartner

Gartner

Keeper Security® was recognized in 2026 as the second fastest-growing security software company globally.



Cybersecurity Stars Awards 2026

AI Security Innovator of the Year, Best Privileged Access Management Platform for Enterprises.



Cybersecurity Excellence Awards

Privileged Access Management.



Global InfoSec Awards

AI-Powered Cybersecurity Solution, Cybersecurity Company, Privileged Access Management (PAM)



Globe Awards 2026

Cybersecurity Silver Winner