

Case Study

BASF Standardises Enterprise Password Management Across a Global Workforce With Keeper



Background

BASF is one of the world's largest chemical companies, operating across multiple business divisions and geographies with a global workforce of more than 100,000 employees. BASF's IT organisation is responsible for delivering secure, scalable digital services to tens of thousands of users across its global operations.

Industry
Chemical producer

Employees
100,000+

Solutions
Enterprise Password Management



The Challenge

For a global enterprise operating across multiple markets and business divisions, managing employee credentials at scale is both a security imperative and an operational challenge. BASF needed a modern, enterprise-grade password management solution capable of supporting its large and diverse workforce while upholding strict internal password policies.

Ageing Legacy Tool Falling Short - BASF's existing credential management tool was built on an ageing codebase that had not kept pace with the demands of a modern enterprise. As the workforce and work methods evolved, the platform could not easily support essential capabilities such as multiple credential types, cross-device synchronisation and secure sharing.

Balancing Security With User Convenience - Corporate policy required strong, regularly rotated passwords for all users. However, without an effective way to generate and store complex credentials, employees risked resorting to insecure workarounds such as writing passwords down or modifying existing weak passwords by just one character. BASF needed a solution that made strong password hygiene practical for employees without adding unnecessary friction. The platform also needed to support enterprise scale, a site license was procured, with roughly 29,000 active unique users logged over the past year, making it one of the largest deployments of its kind at the time — while integrating with Microsoft Entra ID via SCIM provisioning, and with the company's SIEM environment.



The Keeper Solution

BASF's IT team conducted a formal RFI/RFP process to evaluate password management solutions, with Keeper emerging as the strongest choice based on both technical capability and commercial value. Keeper's zero-knowledge security architecture, cross-device synchronisation, support for a wide range of credential types and competitive pricing made it the clear choice for an organisation of BASF's scale and complexity.

"We did an analysis of the players on the market. From a technical perspective, Keeper scored the best with the most points and, after the RFP, was also the best in terms of price."

**Michael Roos | Product Owner and IT Security
Solution Architect, BASF**

Universal Access Across the Organisation - BASF deployed Keeper as its company-wide password management platform, making it available to all employees with a BASF user ID and establishing it as a standard component of the digital workplace rather than a tool limited to a specific team or function. Whether storing credentials for internal systems, external partner platforms or shared functional accounts, users across departments and geographies rely on a single secure vault. This directly addressed the informal workarounds that had emerged under the previous solution.

Seamless Integration With Enterprise Infrastructure - Keeper integrated with BASF's Microsoft Entra ID via SCIM for automated user provisioning and synchronisation, while event logging was connected to the organisation's SIEM environment to improve visibility and auditability across security operations.

Secure Credential Sharing - Prior to Keeper, shared credentials for functional and external accounts were often distributed via email or written down. Keeper's sharing capabilities gave teams a governed, auditable alternative, eliminating a significant source of unnecessary risk.

Autofill and Strong Password Generation - Keeper generates and stores complex passwords, autofilling them at login without requiring users to remember them. The result is consistently stronger credentials across the organisation, with no additional burden on employees.

"I don't have to remember my password because Keeper knows it for me. I just use Keeper to autofill and sign in, and still have it secured and encrypted."

**Michael Roos | Product Owner and IT Security
Solution Architect, BASF**



Organisation Impact

By deploying Keeper to approximately 29,000 employees, BASF established a scalable, enterprise-wide approach to password security that balanced rigorous protection with genuine usability.

Stronger Password Hygiene at Scale - Keeper enabled BASF to enforce corporate password policies, including length, complexity and annual rotation requirements, in a practical way for users rather than simply a mandate. Credentials are automatically generated, stored and managed within Keeper, removing the need for employees to create or manually track complex passwords.

Reduced Risk and IT Overhead - Insecure workarounds became unnecessary after Keeper was implemented, and password-related support requests to the service desk decreased over time as users gained the ability to manage their own credentials through Keeper's intuitive interface.

A Platform That Grows With the Business - Since deployment, BASF has seen continuous improvements to Keeper's administrator console, including expanded enforcement settings, configuration options and user management capabilities that have strengthened the organisation's ability to govern access at scale.

"Keeper made a lot of improvements based on our feedback, not only related to performance but also related to functionality and how it is used in big enterprises."

**Michael Roos | Product Owner and IT Security
Solution Architect, BASF**

Transparency That Builds Long-Term Trust - During the evaluation process, BASF conducted a detailed security assessment of Keeper's architecture, controls and documentation. Keeper's transparency and technical maturity helped support the organisation's long-term confidence in the platform.

"Keeper was very open right from the start. We did quite a big security assessment, and it was highly positive. The trust in the security of Keeper is extremely high."

**Michael Roos | Product Owner and IT Security
Solution Architect, BASF**

Ongoing Partnership - Keeper's support during the initial onboarding phase, along with its responsiveness to product feedback, has remained an important part of the long-term partnership - with input from BASF directly shaping Keeper's product roadmap.



Keeper Enterprise Password Management

Most businesses have limited visibility into employees' password practices, which significantly 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 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 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 for integration with current and future systems.

Business Use Cases: KeeperPAM

- 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 behavior

Protect your organisation with Keeper

To learn more about how Keeper can protect your organisation with an easy-to-use platform, [contact our sales team](#) for a free trial or personalised demo.

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.

Gartner

Keeper Security® was recognised 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