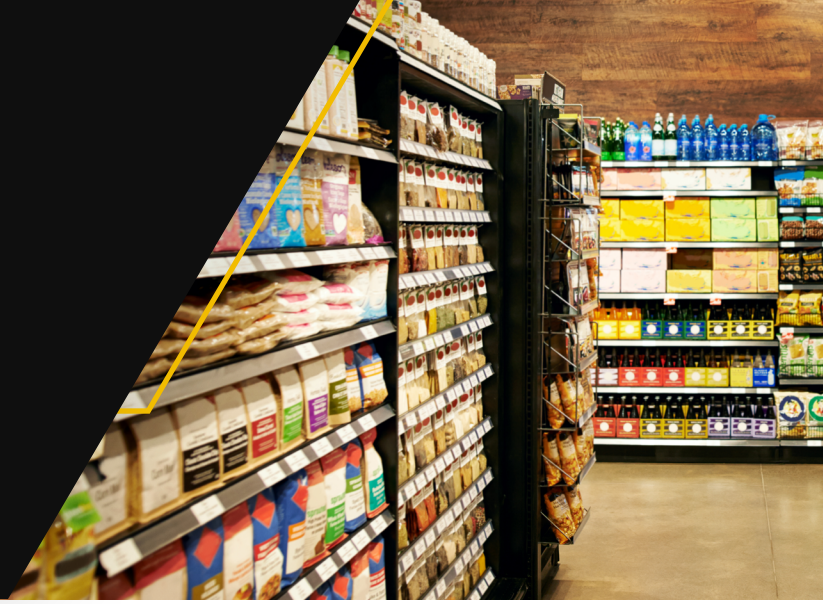
KEEPER +

CASE STUDY

Retailer Strengthens Password Management with Keeper Security



BACKGROUND

This retail conglomerate is one of the largest companies in Australia. The company's portfolio includes brick-and-mortar stores under a number of leading global brands, as well as several business divisions in healthcare and energy. Over the years, the company has diversified its holdings in new sectors while maintaining a strong presence in retail.

Industry
Retail

Organization Size
5,000+ employees

Solutions
Keeper Password Manager

- Enterprise
- BreachWatch®
- Advanced Reporting & Alerts Module
- Compliance Reporting
- Platinum Support

THE CHALLENGE

For an organization of its size, the enforcement of security standards is a serious challenge. The many subsidiaries, business units, departments, and their individual and sometimes competing needs, complicate the goal of having a unified corporate strategy for information technology and security. This retail conglomerate was no stranger to this story of silos and fragmentation, which impeded the visibility of IT personnel into employee password behavior.

Without enterprise visibility into password strength, the organization lacked the ability to prevent and mitigate cyberattacks involving human credentials — which account for 82% of all cyberattacks. Audit and compliance requirements also depend on streamlined reporting on password behavior and account access from all corners of the business.

The company's lack of visibility led to wasted spending on help desk tickets and audits, redundancy in password storage methods, confusion among employees and challenges with compliance. It also created a security risk for the organization.

The organization lacked a centralized method to track password-related security events. A few divisions were using Keeper Password Manager to securely store and share important credentials and information. Other teams were using different password managers, spreadsheets or pen and paper to store their passwords.

The Chief Information Security Officer (CISO) launched an enterprise-wide initiative to unify password management, recognizing it as the organization's first line of defense against cyberattacks.

THE KEEPER SOLUTION

As part of the CISO's initiative, the IT department evaluated the various password managers used by different departments. The initial teams using Keeper Password Manager noted its ease of deployment and widespread adoption, suggesting a similar process for rolling out the solution to the rest of the organization.

Keeper integrated with the organization's Azure Active Directory to enable user provisioning. For end-users, integrations with Single Sign-On (SSO) and multi-factor authentication provided an extra layer of security and verification without giving them more passwords to remember. They just have to remember one password — their Master Password.

As a publicly-traded company subject to many regulations, the retailer was also interested in a solution that would streamline compliance audits and reporting. With cybersecurity and e-commerce regulations increasing globally, regulatory compliance was expensive — especially in the absence of standardized data.

Keeper Password Manager offered critical and centralized visibility into account access and password-related events. Keeper Compliance Reports and the Advanced Reporting and Alerts Module (ARAM) offered the ability to unify on-demand visibility of access permissions for the company's privileged accounts and employee passwords — both critical areas for overall compliance.

> **Since deploying Keeper across business lines and departments, the solution has allowed systems administrators to holistically assess the risk of a cyberattack against individual end-users and the organization as a whole, including whether credentials are exposed.**

BUSINESS IMPACT

Since deploying Keeper across business lines, the solution has allowed systems administrators to holistically assess the risk of a cyberattack against individual end-users and the organization as a whole, including whether credentials are exposed. With BreachWatch, the information security team can monitor employee passwords for possible exposure on the dark web — and require employee password resets when necessary.

Role-based access controls restricted end-user access by job responsibility, limiting access to the least necessary permissions in order to protect the wider organization. The ARAM module supports audits and monitors password-related events through customized reporting and integration with the company's preferred Security Information and Event Management (SIEM) solutions. And with Keeper Compliance Reports, the organization can report the access permissions of privileged accounts across the entire organization, while still maintaining a zero-knowledge framework.

Keeper Password Manager is a core technology in enabling the retailer's long-term security strategy. A single, centralized enterprise manager has enabled the retailer to enforce standard password policies across its workforce and take proactive steps to remedy non-compliant credentials. For auditing and compliance reporting, streamlined compliance reporting has enabled the team to more efficiently generate reports in the audit process. Keeper has saved the retailer time, money and energy, all the while improving employee security hygiene and overall cybersecurity.

The retailer found an enthusiastic and collaborative security partner with Keeper. Insight into Keeper's product roadmap demonstrated a common vision for future innovation and feature development. And the CISO and IT departments, alongside Keeper's product management and business support teams, maintained a shared, partner-oriented approach to information security.

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 Password Manager solves this challenge by providing ultimate security, visibility and control.

Data is protected in Keeper's zero-knowledge security architecture with 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 existing SSO solutions.

Keeper was 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 cyberthreats
- Strengthen compliance
- Boost employee productivity
- Enforce password policies and procedures
- Reduce help desk costs
- Minimal training, 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