KEEPER + PROTEUS DISCOVERY GROUP

Case Study

eDiscovery Services Provider Safeguards Data and Enforces Secure Password Management With Keeper

Background

Proteus Discovery Group is an eDiscovery services provider that offers data solutions to corporate clients, law firms and government entities during litigation, investigations and regulatory matters.

Industry
Legal Services

Employees
<50

Solutions
Keeper Password Manager

- Enterprise
- Platinum Support

The Challenge

Proteus needed an easy-to-use, secure and collaborative password management solution to protect its organization. Before adopting Keeper, employees at Proteus relied on methods such as shared documents in Sharepoint and emails.

Lack of Security: Proteus began the process of improving its compliance and visibility of data and credentials throughout the organization. During the shift, they realized they needed a secure, user-friendly password management platform to assist with their day-to-day operations as well as aid their compliance efforts.

Limited Visibility and Admin Controls: The organization often struggled with limited access-control capabilities, due to not having a password management platform. This was particularly problematic when they needed to share passwords with, or provide temporary access to, their clients or vendors. The lack of critical access control was risky and difficult to manage.

> **The main driver to finding a password manager was having a secure centralized location so we could have access to those different passwords. Within Keeper we are easily able to keep secure records for passwords across our systems.**
>
> **Austin Hagen | Vice President**
> Operations

The Keeper Solution

User Adoption and Training: Keeper is recognized as the leading password manager for organizations 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 end-user adoption.

Additionally, Keeper's award-winning User Interface (UI) provides an intuitive and accessible platform that is easy for non-technical employees to understand and adopt. Keeper also supports cross-platform use on Windows, Mac, Linux, iOS and Android, ensuring that the solution works seamlessly no matter the platform or device.

Role-Based Access Controls (RBAC): Keeper provides granular sharing enforcement for administrators to leverage Role-Based Access Controls (RBAC) that ensure organization-wide security policies are adhered to and compliance is met. Designating roles within the organization streamlines provisioning for administrators and allows for specific rule sets to be leveraged to maintain least privilege access and increase the organization's security posture.

Cost Effective: No matter the size or type of organization, Keeper has a cost-effective plan to fit and scale with organizational needs. Keeper's transparent pricing model, paired with world-class customer support, ranking #1 in Enterprise Customer Support on G2, ensures that organizations maximize 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 level), multi-factor and biometric authentication, as well as FIPS-140-2 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 Authorized.

Organization Impact

Proteus seamlessly transitioned its credentials to Keeper, providing a better end-user experience, improving user adoption and fortifying the organization's security posture. The organization regularly works with third-party vendors that require differing visibility into records or credentials, and Keeper assists the organization in maintaining best-in-class security.

Implementation: The organization was able to transition its credentials into Keeper quickly and seamlessly. By implementing Keeper, the organization now has improved visibility, allowing admins to keep a close eye on compliance with password hygiene best practices and security policies.

> **Keeper has improved security, increased speed and reduced frustration.**
>
> **Austin Hagen | Vice President**
> Operations

User Adoption: Keeper's streamlined user interface and detailed enablement training materials resulted in high user adoption. Keeper has made it possible for employees to securely share passwords with each other, while still leveraging Keeper's encryption.

Across teams, the Shared Folder feature allows the organization to maintain an orderly and secure method of sharing critical passwords and information. Keeper's One-Time Share has enabled secure sharing of files and credentials in a limited capacity with clients and vendors.

Security and Visibility: The organization seamlessly integrated Keeper with their SSO provider, allowing employees to authenticate into Keeper with their SSO credentials as well as securely access the organization's cloud and native applications that don't support SSO. For online accounts, KeeperFill®, Keeper's secure browser extension, allows users to instantly autofill credentials on any device.

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

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 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 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 and is FedRAMP and StateRAMP Authorized.

Keeper is 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 cyber attacks
- 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 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