KEEPER + West Virginia University

Case Study

West Virginia University Improves Password Management and Visibility With Keeper Security

Background

West Virginia University (WVU) is a public land-grant research university with more than 25,000 students. Its main campus is located in Morgantown, West Virginia. WVU is classified as an R1 Research University, with very high research activity, the most elite category for research-focused institutions.

Industry
Higher Education

Employees
10,000+

Solutions
Keeper Password Manager

- Enterprise
- Platinum Support

The Challenge

West Virginia University (WVU)'s Information Technology (IT) department needed an easy-to-use, secure and collaborative password management solution to replace an existing tool that no longer met their security or usability needs.

Before adopting Keeper, employees in WVU's IT team relied on a legacy password manager which had been in place for eight years. The legacy solution had a cumbersome user interface which limited adoption among end-users, as well as dated access controls which made visibility and reporting difficult for admins. Additionally, the cost of the solution had grown substantially since it was first implemented while the quality of customer support provided by the vendor had declined. Eventually, the cost outweighed the benefits and the WVU IT team decided it was time to replace the solution.

Poor User Adoption - End-users were often frustrated with the way records were stored and shared. As a result, some employees would use shared spreadsheets or other outdated and risky methods to store and share passwords.

Limited Visibility and Admin Controls - The system administrators often struggled with limited access control capabilities, especially when decommissioning and transferring the stored passwords of employees who had left the organization. The lack of critical access control caused IT teams to waste resources resolving issues within the solution.

Cost and Support - The vendor continuously raised costs and although updates and enhancements were released, the cost of the solution outweighed any additional value. In addition, the customer support team was unresponsive to requests and was not proactive in providing training or enablement materials for end-users.

Security Concerns - The vendor's security architecture only supported encryption at the vault level - a major security flaw. In 2022 a data breach occurred which put end-user vault data at risk.

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, Linus, 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) to 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 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 GovRAMP Authorized.

> **As soon as we got Keeper, it went right into our governance policies and procedures. We have the utmost confidence in the tool.**
>
> **Whinston Antion**
> **Assistant Director of Identity & Access Management**

Organization Impact

WVU was able to seamlessly transition from its legacy password management system to Keeper, providing a better end-user experience, improved adoption and organizational security, with a strong return on the investment.

Implementation - WVU leveraged Keeper Commander to easily import all of the IT teams critical records. Keeper Commander provides robust APIs to integrate into current and future systems. WVU now has improved visibility into the organization's security, allowing admins to keep a close eye on compliance with password best-practices and security policies.

> **We're able to go in and audit the security of the accounts and the password security, and make sure that everybody has their multi-factor set up. There's a lot of nice features in Keeper that give us the ability to lock everything down.**
>
> **Whinston Antion**
> **Assistant Director of Identity & Access Management**

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. Administrators have successfully transitioned Keeper Vaults using Account Transfer to maintain operations when offboarding occurs.

Security and Visibility - WVU utilized Role-Based Access Controls (RBAC) to gain visibility and control over employee password usage across the organization. The IT team also integrated Keeper with their SSO Provider and Multi-Factor Authentication (MFA) solution. Allowing employees to seamlessly verify their identity when signing in to accounts. For online accounts, KeeperFill®, Keeper's secure browser extension, allows users to instantly autofill credentials.

These integration capabilities and ease of use, along with Keeper's clear pricing structure, provided WVU with a holistic 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 GovRAMP 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
- 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 transforming cybersecurity for millions of individuals and thousands of organizations 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 organization 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