

Case Study

Making Password Management Non-Negotiable:

How Real Solutions Standardized Credential Security With Keeper



Background

Real Solutions of North America

is a New Jersey-based managed service provider that grew out of an established ERP consulting business. The company originally specialized in helping manufacturers and distributors streamline complex supply chain and inventory operations through custom ERP integrations.

As client needs evolved, so did Real Solutions. Today, Real Solutions delivers managed IT and cybersecurity services to organizations across manufacturing, distribution, print and apparel, banking, legal and healthcare.

With many of its customers operating in regulated industries, the MSP has built its practice around delivering consistent, security-first solutions that help organizations reduce cyber risk and strengthen their overall security posture.

Industry

Managed Service Provider (MSP)

Employees

<50

Solutions

KeeperMSP®



The Challenge

As Real Solutions expanded its managed security services, one issue continued to surface across customer environments: password management. Many organizations were still storing passwords in browsers, sharing credentials between employees or relying on inconsistent password practices that created unnecessary risk. At the same time, the company's previous password management provider was discontinued following a major security incident, underscoring the importance of selecting a solution with a security architecture the company could trust.

Beyond the security concerns, Real Solutions sought a platform that could scale operationally. As the company added more managed companies, technicians needed a consistent way to deploy, manage and secure credentials across distinct environments. Supporting different password managers or relying on browser-stored credentials created additional complexity, made administration less efficient and increased the likelihood of human error. The team wanted to standardize on a single, comprehensive platform that would improve both security and day-to-day operations.

At the same time, customer expectations were changing. More organizations were facing cyber insurance requirements, Department of Defense mandates and contractual obligations that increasingly emphasized identity security. Real Solutions needed a platform that would deliver consistent credential management across every customer environment while supporting evolving compliance requirements.

The Real Solutions team took a unique approach to helping its customers understand the need for stronger credential security. They didn't just talk about why browser-based storage was risky; they actually showed it firsthand.

During customer assessments, the team would use a credential extraction tool to demonstrate how passwords stored in Google Chrome or Microsoft Edge could be recovered from an employee's workstation within 30 seconds. The exercise revealed usernames, passwords and business-critical accounts that had been sitting inside their browsers. Seeing those credentials exposed in real time turned an abstract discussion into a tangible business risk, reinforcing the need for a dedicated enterprise password manager. The demo successfully turned awareness into urgency.



The Keeper Solution

After evaluating several password managers, Real Solutions selected Keeper because it aligned with both its security philosophy and its MSP operating model.

Keeper's zero-knowledge and zero-trust security architecture became a key differentiator. Even if Keeper itself were ever compromised, customer vaults always remain encrypted and inaccessible. That security model gave Real Solutions the confidence to introduce Keeper to customers who were increasingly concerned about password manager breaches.

"The fact that Keeper keeps every customer's vault separate is a game changer. Even if Keeper was compromised, there's nothing that a hacker can do with our data. We really value that peace of mind."

Shawn Walter, IT Director

Keeper has also simplified day-to-day operations. Single sign-on with Microsoft Entra ID streamlined onboarding, while the centralized MSP management console allowed technicians to manage every client from a single pane of glass. Shared folders enabled secure collaboration between Real Solutions and customer IT teams, eliminating the need to exchange credentials through emails or spreadsheets. The MSP also valued features such as one-time sharing, integrated MFA and passkey support, which contributed to a stronger security posture and a better user experience. Ultimately, Keeper helped Real Solutions make credential management a foundational component of its managed security offering, rather than an optional add-on.



Organization Impact

Integrating Keeper into every managed security deployment has delivered measurable benefits for both the MSP and its managed companies.

Onboarding is straightforward. After configuring Microsoft 365 single sign-on, users receive an invitation, import their existing passwords and begin using Keeper with minimal assistance. The intuitive experience has helped drive adoption while reducing onboarding and support-related requests. Shared credential folders have also streamlined collaboration between Real Solutions technicians and customer IT administrators, ensuring everyone has secure access to the latest credentials without relying on emails or phone calls.

The operational impact has been significant. For one regional manufacturing customer, password-related support tickets dropped from approximately 50 per month to fewer than 10, with each avoided ticket saving an estimated 30 to 60 minutes of technician time. Keeper also continues to help customers satisfy growing security requirements.

Another manufacturing customer working with the New Jersey Transit Authority was required to implement a password manager before employees could support certain projects. Because Keeper was already built into Real Solutions' managed security offering, meeting that requirement required little additional effort. Real Solutions' IT Director, Shawn Walter, also adds that he is seeing credential management appear more frequently in cyber insurance questionnaires, reflecting a broader shift toward treating identity security as a business requirement rather than a best practice.

Today, Keeper is embedded in every managed security package delivered. Instead of allowing customers to pick and choose foundational security controls, the MSP establishes a consistent security baseline from day one, ensuring every client starts with the protection they need.

"You include it, and you don't let them use the browser anymore. You're responsible for securing your customers, so give them everything they need to be secure."

Shawn Walter, IT Director

That mindset has become an integral part of how Real Solutions delivers managed services. By making password management a standard requirement, the MSP has simplified deployments, reduced operational overhead and given customers a more resilient approach to protecting business credentials.

For security-minded MSPs such as Real Solutions, the takeaway is clear: Foundational security shouldn't be optional. It should already be built into the service customers receive.



Keeper Password Manager

Most businesses have limited visibility into their employees' password practices, 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 used to encrypt and decrypt their information.

Keeper integrates with Active Directory and LDAP servers, which streamlines provisioning and onboarding. **Keeper SSO Connect**® integrates into existing SSO solutions and is FedRAMP and StateRAMP Authorized. integrates into existing SSO solutions and is FedRAMP 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 to integrate into current and future systems.

Why you need **KeeperMSP** for your business:

- Easy to use multi-tenant management for MSPs
- Prevent password-related data breaches and cyber attacks
- Support passkeys for effortless authentication
- Enable just-in-time access and privilege management
- Generate new revenue streams
- Enforce password policies and enable password rotation
- Enhance compliance and reporting
- 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, protecting over 95,000 organizations and millions of people across 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. Recognized for its innovation in the Gartner Magic Quadrant for Privileged Access Management (PAM), Keeper secures passwords and passkeys, infrastructure secrets, remote connections and endpoints with role-based enforcement policies, least privilege and just-in-time access. Learn why Keeper is trusted by leading organizations to defend against modern cyber threats at [KeeperSecurity.com](https://keepersecurity.com).

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