Case Study

Greater Control, Lower Risk: How ITS Scales Credential Management

Background

Intelligent Technical Solutions (ITS) is a growing managed security services provider that supports small and mid-sized businesses across the U.S., with a major footprint in regulated and government-adjacent sectors.

Based in Las Vegas, Nevada, ITS manages approximately 25,000 endpoints across roughly 700-800 clients. The company employs over 400 people, with teams operating in the U.S., the Philippines, Western Europe and South Africa, enabling true regional support.

ITS differentiates itself by combining traditional MSP services with strong in-house cybersecurity and governance capabilities. In addition to offering help desk and infrastructure support, ITS delivers security best practices, regulatory compliance guidance and fractional leadership services such as virtual CIO (vCIO) and virtual CISO (vCISO). While many MSPs outsource those services, ITS keeps them in-house.

Industry

Managed Service Provider (MSP)

Employees

<450

Solutions

- KeeperMSP®
- Keeper Password Manager

The Challenge

As compliance pressure increased across its customer base – from CIS Controls and NIST CSF to SOC 2 and CMMC requirements – ITS needed to ensure that its security stack could support more mature, auditable environments. Password management became a crucial piece of that foundation.

Password management was not a new concept for ITS. As a security-focused MSP, the team understood early on that passwords and other sensitive secrets needed centralized control. However, the tools they initially relied on were not purpose-built password management platforms; they were documentation systems with password functionality layered in. This created friction and vulnerabilities, as documentation systems lack the ability to tightly restrict access and provide robust secrets handling features.

Around the same time, customer demand was changing. In the mid-2010s, cyber insurance applications began to include more stringent security questionnaires. By the early 2020s, frameworks like CIS Controls (Implementation Group 1), NIST CSF, SOC 2 Type II and CMMC made password management an explicit requirement. What had once been a recommendation became a baseline prerequisite.

ITS also noted practical security gaps in the field. Many of their end users relied on browser-based password storage. During internal penetration testing, the MSSP learned that once an attacker gained a foothold on a machine, browser-stored password vaults were often trivial to extract. That meant a single compromised endpoint could expose far more than one account.

Another challenge emerged around scale. ITS sought a solution that worked the way MSPs operate. It needed multi-tenant visibility, structured role-based access controls and automated provisioning, as well as clean billing and licensing workflows. Many other password managers were built for a single enterprise, not service providers managing hundreds of distinct client environments.

ITS evaluated several platforms. Some lacked a strong MSP channel model, while others had suffered public security breaches. Some required administrative access levels that created unnecessary risk. ITS needed a platform that aligned with its internal standards and could support its operational model.

The Keeper Solution

Keeper initially stood out for an especially vital reason: It was built with both security and MSP operations in mind.

From a security perspective, Keeper's zero-knowledge architecture amplified client trust. ITS could confidently tell clients that even as administrators, they could not access secrets.

The MSSP appreciated core capabilities such as SSO integration with Microsoft Entra ID and automated provisioning/deprovisioning via SCIM. This enabled identity management from a single source. If an employee were terminated at 5:00 PM, access could be removed immediately across all systems. Such low-latency offboarding ultimately minimized exposure.

Device-based approval added another layer of protection. New device logins triggered approval requests, and with Keeper Automator, ITS could define conditional access policies. Trusted devices were automatically approved, while unknown devices triggered review.

Operationally, Keeper's MSP console provided a single pane of glass across managed clients. ITS segmented access via role-based controls and organizational hierarchies. Technicians only saw what they needed, and finance teams could be assigned billing roles without vault access. Competing platforms lacked this level of control flexibility.

> **"The account transfer feature addressed a key pain point. When someone left a client organization, vault contents could be securely transferred. No drama, no lost credentials."**
>
> **Edward Griffin, CISO**

Keeper emerged as the right choice because it was easy to manage, easy to resell and aligned with critical compliance requirements and daily MSP workflows.

Organization Impact

Keeper is embedded in both the company's operations and client service model. Internally, every ITS employee receives Keeper access upon hire and is required to use it.

The MSSP calls out the effectiveness of Keeper's PowerShell module, designed to securely transfer secrets and files from the Keeper Vault into PowerShell scripts. Staff also appreciate access to their own personal vaults, an exclusive benefit of their MSP licensing.

Keeper replaced a fragmented approach that included one primary system and several satellite tools. Standardizing on Keeper created consistency and an enforceable policy across ITS' infrastructure.

Keeper for Clients:
Keeper is positioned as a foundational security control, especially for clients pursuing SOC 2, CIS alignment, NIST CSF maturity, CMMC compliance or a stronger cyber insurance posture.

ITS reports simplified user lifecycle management by leveraging Keeper Enterprise to implement SSO via clients' primary Identity Provider (IdP), typically Microsoft Entra ID. Integration with IdPs and billing systems has significantly reduced administrative overhead.

In addition to streamlined deployment, support burden has remained low. ITS confirms minimal one-off issues and limited ticket noise related to the platform itself.

Most importantly, Keeper enhances the partner's ability to deliver on its security promise. It allows ITS to confidently check compliance boxes, decrease credential exposure, enforce structured access controls and maintain operational efficiency across hundreds of distinct client environments.

> **"For us, password management is no longer a side feature within a documentation platform. It is a dedicated, security-first system that supports the scale and maturity we need."**
>
> **Edward Griffin, CISO**

For other MSPs evaluating their own security stack, ITS's experience is clear: password management must be purpose-built, operationally aligned and secure by design.

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 85,000 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**.

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