KEEPER® + KAMIND® Cloud Solutions Advisors

Case Study

KAMIND Protects Regulated Client Environments with KeeperMSP®

Background

KAMIND is a Managed Security Service Provider (MSSP) that delivers Microsoft-based security and cloud services to regulated organizations across the U.S. Its primary customer base includes defense contractors pursuing CMMC Level 2 certification, as well as a wide range of healthcare, manufacturing and professional services firms.

Security is fundamental to KAMIND's business. The company has aligned its internal and customer environments with CMMC and NIST 800-171R2 requirements since 2019. Headquartered in Lake Oswego, Oregon, the MSSP supports clients in 37 states and has been featured six times on the Inc. 5000 list.

Industry
Managed Service Provider (MSP)

Employees
<50

Solutions

- KeeperMSP®
- Keeper Password Manager

The Challenge

As KAMIND expanded its security practice and client footprint, credential management emerged as a critical concern. Supporting regulated environments at scale required a cloud-based solution that could meet stringent compliance standards, integrate seamlessly with Microsoft security tools and reduce operational overhead.

Before implementing Keeper, the MSSP maintained over 160 internal accounts throughout government and commercial systems using multiple password storage systems. KAMIND's customers faced similar sprawl, often lacking a structured approach to credential management, which negatively impacted them in more than one way.

Common challenges consisted of:

- Limited visibility into who had access to what
- Inconsistent password policies between systems
- Ad hoc and insecure credential sharing
- Services that were not FedRAMP Moderate or higher in classification

Beyond the operational friction, poor credential hygiene significantly increased the risk of identity-based attacks and data breaches for KAMIND's customers. For defense contractors pursuing CMMC Level 2 certification, this created heightened pressure to demonstrate strong access controls, auditability and proof of execution during assessments.

Compliance stakes were particularly high for KAMIND. Any security tool under consideration had to comply with FedRAMP Moderate Authorization or higher, along with several other industry regulations. The False Claims Act remained top of mind for KAMIND, as organizations must prove they are correctly executing the security controls they have stated to avoid severe legal and financial consequences.

KAMIND needed a leading password management platform that minimized complexity, enhanced security and could be easily managed across hundreds of customer environments without adding labor, risk or support burden.

The Keeper Solution

After reviewing multiple credential management solutions, KAMIND selected Keeper Security in 2020. The final decision was driven by three core pre-requisites: compliance, integration and efficiency.

Keeper's FedRAMP High Authorization immediately set it apart, aligning perfectly with CMMC Level 2 and NIST 800-171 requirements. Other vendors were quickly disregarded as they lacked the necessary FedRAMP compliance or had no roadmap to achieve it. Keeper also stood out for its ability to meet data sovereignty requirements under NIST 800-171 and ITAR, unlike competing solutions. These two non-negotiables eliminated other prospective solutions from consideration in the evaluation process.

From an integration standpoint, Keeper functioned seamlessly with Microsoft 365, Azure and Azure Government environments. This alignment was crucial as KAMIND fully deploys Microsoft security controls for its customers and, prior to Keeper, used an enterprise-grade password manager that fit into that ecosystem. In addition, Keeper's native integrations with Azure Sentinel and KAMIND's internal compliance audit programs further solidified its value.

Efficiency was the final differentiator. Designed with zero-knowledge architecture, there was no doubt that Keeper would deliver reliable password policy enforcement while ensuring the product benefits KAMIND sought. Specific features such as role-based access, 256-bit AES encryption and BreachWatch dark web monitoring appealed to the MSSP as essential factors in further preventing credential exposure.

Due to its intuitive user experience, Keeper drastically reduced training time and support requests, making it ideal to scale through an MSSP delivery model. It's also worth noting that KAMIND does not sell Keeper as a standalone product. Instead, Keeper is included as a mandatory component of every customer's security deployment.

> "Keeper is ingrained into our comprehensive security offering. We've standardized it for a while and find our customers appreciative in the long run. If you don't have it, we're going to give you one because it makes everyone's life easier."
>
> **Matt Katzer, CEO and Founder**

Organization Impact

Since investing in Keeper, KAMIND has noted several key advantages, both in terms of internal use and external standardization.

Onboarding and Adoption – Overall, deployments have been described as consistently smooth, even in the most complex client environments. Customers have frequently highlighted the friendly interface and general ease of use, resulting in rapid onboarding and user adoption. As these organizations grow, Keeper effortlessly supports the addition of more credentials and increasingly intricate workflows.

Support inquiries have remained minimal from day one. KAMIND rarely has to engage Keeper's technical support team, and when occasional questions arise, Katzer affirms that the response has always been swift and effective.

Security Improvements – In addition to Keeper's various compliance achievements, it met KAMIND's need for auditable security controls. KAMIND can now enable both commercial customers and defense contractors using a single, standardized platform, including those operating in Azure Government environments.

Operational Efficiency – Standardizing on Keeper directly benefited the MSSP by cutting labor costs and IT overhead. Users and engineers have become power users faster, and ticket volumes have dropped, allowing many IT teams to reallocate their time and effort to more valuable initiatives.

> "Our success as a business is to offer highly efficient solutions that are 100% vertically focused. We don't want to support multiple password managers."
>
> **Matt Katzer, CEO and Founder**

Business Growth – Reflecting on the partnership, Katzer credits Keeper with strengthening his company's ability to serve regulated markets while scaling securely and sustainably. Looking ahead, the MSSP projects at least 30% revenue growth in 2026, with corresponding gross margin growth, driven in part by standardizing Keeper into its existing security stack.

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