

Case Study

How Leading MSP CloudByte Partnered with Keeper to Win More Highly Regulated Clients



Background

Headquartered in the Washington, D.C., area, **CloudByte** cybersecurity-focused Managed Service Provider (MSP) that supports organizations across healthcare, legal, financial services, hospitality, aerospace and defense.

Originally founded to serve commercial organizations, CloudByte later expanded to work with government-focused businesses, contractors and other highly regulated clients. Today, the MSP helps its customers strengthen their security posture while meeting common industry frameworks such as CMMC, NIST 800-171, FedRAMP, HIPAA and FINRA.

In recent months, CloudByte has intentionally condensed its technology stack, replacing commercial-grade tools with FedRAMP Certified solutions that better support defense contractors and compliance-driven organizations. This strategy enables CloudByte to deliver more robust security while simplifying compliance across highly complex IT environments.

Industry

Managed Service Provider (MSP)

Employees

<50

Solutions

KeeperMSP[®]



The Challenge

CloudByte already recognized the importance of password management and had incorporated it into its managed service offering. At the time, the company was using Bitwarden internally and had planned to extend it across client environments. However, CloudByte's continued growth in highly regulated industries exposed the need for a more robust platform with stronger security controls, compliance capabilities and administrative visibility.

Across the industries it served, CloudByte encountered organizations storing passwords in shared drives and SharePoint folders or exchanging sensitive information through collaboration tools that were not designed or configured for regulated data. Employees sometimes shared confidential files, including HIPAA-related information and Personally Identifiable Information (PII), through platforms that lacked appropriate access controls, auditing and secure-sharing capabilities.

As CloudByte expanded its work with healthcare organizations, financial services firms and government contractors, its clients faced increasingly demanding requirements under CMMC, NIST 800-171, HIPAA, FINRA and related security programs. CloudByte also needed the technologies supporting these environments to align with federal requirements, including FedRAMP certification where applicable. Basic password storage was no longer sufficient. These experiences did not change CloudByte's belief in password management; they reinforced the need for a platform that could better support its evolving business. While Bitwarden had served the company well, CloudByte ultimately needed a solution with a stronger emphasis on FedRAMP certification and the security and compliance capabilities required to support its growing base of regulated clients.



The Keeper Solution

CloudByte evaluated several password management platforms, including LastPass and 1Password. While these products offered similar password management capabilities, Keeper distinguished itself with its security architecture, FedRAMP High Certification and support for compliance frameworks such as CMMC. For CloudByte, that investment ultimately drove its decision.

“When we learned that Keeper placed real emphasis on CMMC and the FedRAMP side of things, that made all the difference for us. There are very few companies investing in FedRAMP authorization.”

Alexandros Voskidis, Founder & CEO

Beyond password management, Keeper provided CloudByte with a platform for privileged access, secrets management, encrypted sharing, role-based access controls and built-in multi-factor authentication. Rather than deploying multiple standalone solutions, the MSP could address a growing range of client security needs through a single platform.

Keeper’s MSP partner program naturally aligned with CloudByte’s business model. As a lean team supporting companies nationwide, CloudByte needed centralized management, bulk provisioning and a platform that could scale efficiently across multiple client environments. Once the company standardized on Keeper internally, the platform became a required component of every deployment. Administrators can preconfigure vaults, permissions and role-based access controls before inviting users, creating a consistent onboarding experience while reducing administrative overhead.

Clients quickly adopted the platform because of its browser extension, cross-platform support and intuitive user experience. Instead of logging into separate password management portals, users could securely access credentials directly within their existing workflows. Keeper gave CloudByte a single platform it could deploy across healthcare providers, law firms, government contractors and large enterprise organizations alike.



Organization Impact

Keeper has become a core part of CloudByte’s managed security offering and a key differentiator for the company in regulated industries.

Deployment has been consistently seamless across even the most complex customer environments. Organizations have replaced passwords stored in SharePoint folders and shared drives with secure Keeper vaults, while role-based access controls have simplified permission management, helping minimize the risk of unauthorized access. The team confirms that administrative tasks that once took five to ten minutes each, such as sharing records, assigning permissions and managing vault access, now take about 30 seconds.

CloudByte has also experienced measurable operational improvements. The company estimates **password reset tickets have decreased by approximately 75%**, allowing technicians to spend less time resolving routine support requests and more time helping clients strengthen their security and compliance posture.

Following a business email compromise at a healthcare staffing agency, CloudByte deployed Keeper to help strengthen credential security and modernize the organization’s overall security strategy. After implementing secure credential management, vault controls and multi-factor authentication, the organization’s cyber insurance provider **reduced its premium by approximately \$500 per month**, resulting in annual savings of roughly \$6,000.

CloudByte’s investment in Keeper has also produced new opportunities for business growth. The company regularly highlights its FedRAMP Certified security stack when pursuing government and compliance-focused opportunities, giving it a competitive advantage over MSPs that use non-FedRAMP security platforms. When engaging prospective clients, Keeper is one of the first solutions CloudByte presents to support zero trust initiatives, regulatory compliance and long-term security strategy.

“Keeper became the de facto tool for us. It saves us time, money and headaches. The fact that we can consolidate under a single platform is awesome.”

Alexandros Voskidis, Founder & CEO

So, what’s on the horizon for CloudByte?

Currently, the MSP is preparing to pursue one of its largest opportunities yet: an aerospace and defense organization with approximately **2,200 users**. The company expects Keeper to play a central role in that deployment, just as it has for organizations with 50 to 250 users. Whether serving a

regional healthcare provider or pursuing large-scale enterprise opportunities, CloudByte relies on Keeper to deliver the security, compliance and operational efficiency its clients expect. As the company continues to grow, Keeper remains an integral part of its strategy to scale secure managed services and expand its presence in regulated industries.



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://www.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