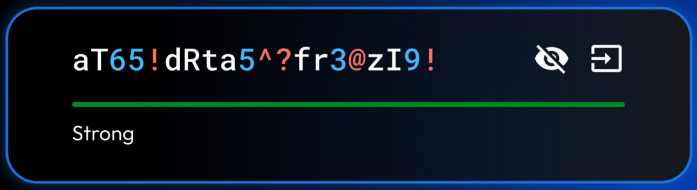
KEEPER | HyCloud Computing



Case Study

How MSP HyCloud Made 20-Character Passwords Practical

Background

Founded in 2015, HyCloud Computing is an Ontario-based managed service provider supporting approximately **250 endpoints** for clients in the construction, legal and healthcare industries.

From the beginning, HyCloud has focused on helping businesses adopt technologies that can adapt as their needs change. The company embraced cloud infrastructure from its inception, reflecting an early focus on adaptable technologies that could evolve alongside its clients.

Today, its services span managed IT, cybersecurity, cloud infrastructure and strategic IT consulting. The company combines day-to-day technology management with longer-term guidance to help clients make informed technology decisions and continually improve their IT environments. Layered security is a baseline for every client HyCloud supports, extending beyond traditional IT management to essential protections like email security and dark web monitoring.

That same forward-looking mindset shapes how HyCloud builds its technology stack. The company continually evaluates new tools and capabilities to determine whether there is a better way to support and protect its clients.

Industry

Managed Service Provider (MSP)

Employees

<50

Solutions

KeeperMSP®

The Challenge

As HyCloud's clients became more dependent on cloud applications and web-based tools, the number of accounts and credentials employees had to manage continued to multiply. At the same time, HyCloud began enforcing stricter password policies as part of its broader security strategy.

HyCloud saw firsthand how quickly those higher standards could create challenges for employees. Within its own environment, HyCloud enforces complex, randomly generated passwords of approximately 20 characters. While these stronger passwords make accounts more difficult to compromise, expecting employees to create, remember and manually enter them across numerous applications was not sustainable over the long term.

HyCloud also identified weaknesses in how clients stored, shared and managed credentials. Some customers still relied on spreadsheets to store credentials. Shared accounts created additional challenges when multiple employees needed access to the same systems. Without centralized control over credential access, clients risked passwords being copied, passed between employees or remaining tied to individuals long after access should have been revoked.

Employee departures made those weaknesses particularly clear. When employees left without properly handing over credentials associated with their roles, HyCloud saw the consequences firsthand. Clients could suddenly find themselves locked out of critical accounts, scrambling to regain access and figure out which credentials needed to change.

Credential exposure raised the stakes even further. HyCloud had worked with clients whose passwords appeared in known breaches, turning password management from an everyday IT issue into an immediate security concern. Reducing that exposure required more than simply increasing password length and complexity.

The impact extended to HyCloud's support team. When client employees forgot passwords or lost access to credentials, the team had to step in to reestablish access. Each request meant time spent resolving an avoidable issue instead of focusing on higher-value client needs.

HyCloud needed to solve both sides of the problem: give clients greater control over how they managed and accessed passwords while making better password practices easier for internal employees to maintain. What was missing was a consistent way to manage credentials throughout their lifecycle, from creation and everyday access to sharing, onboarding and offboarding.

© 2026 Keeper Security, Inc.

The Keeper Solution

HyCloud evaluated several password managers, including LastPass, before selecting Keeper Security. Recent breaches involving other password management providers made vendor trust a key consideration in HyCloud's decision. Keeper's well-established reputation for robust security, ease of use and consistently positive user feedback helped distinguish the platform during HyCloud's assessment.

Before recommending Keeper to clients, HyCloud validated the platform through an internal implementation. This allowed the team to assess Keeper under real-world conditions, from onboarding and usability to deployment and day-to-day management. That experience gave HyCloud a stronger foundation for guiding clients through their own adoption.

> **"We use Keeper internally before recommending it to our customers. That gives us confidence that we're providing a solution that meets our security standards and is something we can truly stand behind.'"**
>
> **Joe Araujo, CIO**

KeeperFill quickly showed how HyCloud could maintain rigorous password standards without adding friction. By automatically filling stored credentials across websites and applications, Keeper made long, randomly generated passwords easier for employees to use.

Compatibility with HyCloud's Microsoft-focused environment was another technical priority. Keeper integrated smoothly with Microsoft 365 and Entra ID, while its mobile application enabled employees to access their vaults beyond their desktops. That cross-device flexibility was critical for users who relied on uninterrupted access to credentials while working from multiple devices throughout the day.

Beyond everyday access, Keeper directly addressed credential management challenges HyCloud had previously identified within different client environments. Shared Folders provided a controlled way for teams to collaborate around common accounts and adjust access as employees joined or changed roles. Vault Transfer extended that control through offboarding, allowing organizations to retain ownership of business credentials and transfer records to another user when an employee left.

Keeper gave HyCloud additional ways to identify compromised credentials and enforce stronger access controls. BreachWatch continuously monitors stored credentials for exposure and alerts users when a password may have been compromised, helping teams respond before that credential can be exploited. MFA requires an additional verification step beyond a password, while SSO gives organizations a centralized way to authenticate users and manage access. Together, these capabilities gave HyCloud deeper insight into credential risk and tighter control over how users authenticate and access sensitive accounts.

Organization Impact

An Ontario-based company demonstrated the real-world impact of HyCloud's password management strategy. For years, the business used spreadsheets and shared accounts to manage credentials. The risks became tangible when passwords linked to the organization appeared in a known breach, and employee departures made it difficult to regain access to shared accounts.

Changing those practices required more than introducing new technology. HyCloud first educated the company on the risks created by its current password practices before making the case for dedicated password management. Rather than leading with the product, the MSP framed the conversation around each customer's environment and the business consequences of leaving existing gaps unresolved. HyCloud applies that same education-first model across its entire client base.

Clients have different budgets, priorities and levels of security maturity. Some quickly recognize the security and operational value of dedicated password management, while others need more time and context to understand how it addresses the risks they - knowingly or unknowingly – face. This gives customers a clearer reason to change and helps HyCloud drive adoption around an understood business need rather than another security tool.

For the company, simplified collaboration was a crucial factor in adopting Keeper. After deployment, the business replaced spreadsheets with a centralized way to share credentials and collaborate around common accounts. It could also maintain ownership of business credentials when employees left, resolving an issue that had previously created unnecessary access problems.

Keeper also delivered meaningful productivity gains to HyCloud and its managed companies. With employees accessing numerous applications throughout the day, Keeper significantly reduced the time spent locating and manually entering credentials. The MSP estimates that Keeper saves approximately 45 seconds to one minute per login. Across repeated logins, that adds up to approximately 20 minutes of saved time per user each day.

20

Min. per user, per day

Time saved on repeated logins with Keeper.

HyCloud Estimate

250

Endpoints supported

Client enviornments HyCloud manages.

Company Profile

© 2026 Keeper Security, Inc.

Automated password generation changed how users approached password creation. Instead of choosing credentials based on what they could remember, teams could routinely use unique, randomized passwords for their accounts. This helped HyCloud make secure, randomized passwords part of clients' everyday workflows rather than something dependent on individual employee behavior.

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 High Certified 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 for integration with 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 100,000 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**.

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)

Globee Awards 2026
Cybersecurity Silver Winner

© 2026 Keeper Security, Inc.