KEEPER | msp

REV 7.21.20

CYBERSECURITY STARTS WITH PASSWORD SECURITY

81%

of data breaches are due to weak, default or stolen passwords[1]

93%

of at-home workers admit to reusing passwords across accounts

62%

of employees reuse passwords across work & personal accounts

Poor password practices are the biggest threat to enterprise cybersecurity. Over 80% of successful data breaches are caused by stolen or compromised passwords. When employees use weak passwords, reuse passwords across accounts, or store their passwords insecurely (sticky notes, spreadsheets, etc.), they put their employers at risk.

Keeper gives businesses full visibility into their employees' password practices and complete control to enforce company password policies, such as requiring strong, unique passwords for every account and mandating the use of two-factor authentication (2FA). Companies also get advanced identity and access management (IAM) features, such as role-based access control (RBAC) and controlled credentials sharing.

At the same time, Keeper makes it easy for staff members to practice good password hygiene by providing each employee with a private, encrypted digital vault that they can access from their device using one master password – the only password the employee will ever have to remember. Keeper automatically generates strong, unique passwords for every account and automatically fills in login fields on all websites and apps.

YOU NEED PASSWORD SECURITY, AND SO DO YOUR CLIENTS

Because they have high-level remote access privileges to multiple organizations' IT systems, MSPs are highly attractive targets for cybercrime. By breaching just one MSP, a cybercriminal can gain access to dozens, perhaps hundreds of other companies. Cybercriminals can also use MSPs as conduits for ransomware; in 2019, at least 13 MSPs were used to deploy ransomware on their clients' systems.

MSPs' clients are also at risk. In one survey, three out of four MSPs reported that 10% to 20% of their clients had experienced at least one cyberattack in the previous year. As cyberattacks grow more complex, frequent, and costly, these companies are turning to their MSPs for assistance; 95% of MSPs have had clients approach them for help with cybersecurity.

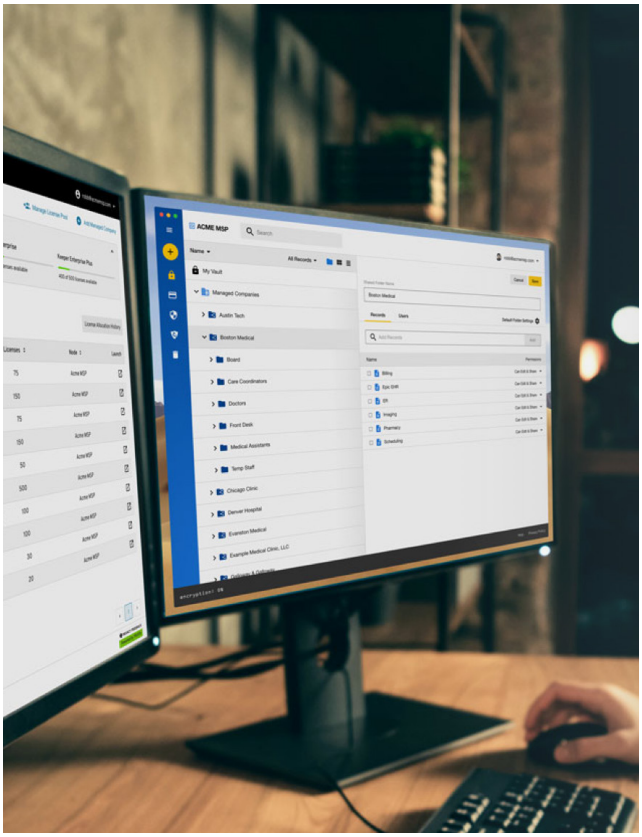
INCREASE YOUR REVENUE AND PROTECT YOUR DATA

Designed specifically for managed service and managed security service providers, KeeperMSP enables your MSP/MSSP to:

- Solve your own password management and security issues with Keeper, the market leading, top-rated zero-knowledge security and encryption platform for preventing password-related data breaches and other cyberthreats
- Solve your clients' password management and security issues, and earn additional revenue, by reselling the Keeper password manager as a service

With KeeperMSP, managed service providers can independently provision, manage, and monitor multiple customers from a central admin dashboard, with robust reporting and auditing tools to enforce security and compliance requirements such as RBAC, 2FA, SIEM event reporting, and regulatory and industry compliance.

In addition to world-class security and functionality, KeeperMSP includes MSP-friendly licensing options, monthly billing, and generous volume pricing terms.



DIFFERENTIATE YOUR COMPANY IN A CROWDED MARKET

Store All of Your Confidential Data and Files

In addition to your passwords, with Keeper Secure File Storage, you can also store all of your private keys, digital certificates, access keys, API keys, and other sensitive data in an encrypted digital vault, which you can access on any device, running any OS. Keeper fully encrypts your digital assets locally, on the device level, with 256-bit AES.

Securely Access Your Clients' Systems

KeeperMSP provides tools for seamless integration into the networks you manage through AD/Open LDAP synchronization, SSO Integration, multi-factor authentication (2FA), and system log reporting.

Differentiate Your MSP in a Crowded Market

Standard MSP services, such as remote administration and backup, are rapidly becoming commoditized, making it difficult for MSPs to differentiate their firms from the competition.

By leveraging Keeper, your MSP has a unique competitive advantage in security and cost savings. In addition to enhancing your clients' security, you can help them:

- Reduce help desk costs by eliminating password-reset requests; Forrester estimates that a single password reset costs $70 in help desk labor
- Increase productivity by putting all of their passwords at their fingertips
- Meet compliance standards with features such as time-stamped, searchable audit logs to detect anomalies or unusual behavior, or conduct forensics investigations

All the Sales Collateral You Need

- Keeper's design team will arm you with the co-branded material you need to resell Keeper to your customers
- Take advantage of our Partner Portal, loaded with up-to-date, on-demand data sheets, marketing material, certification courses, training material, users guides, and more

First-Class Technical Support

- 24/7, white-glove technical support, delivered from our four global offices
- Optional support to help onboard your managed companies

Establish an Additional, Steady Source of Revenue for Your MSP

As cyberattacks grow more complex, frequent, and costly, companies are turning to their MSPs for assistance; 95% of MSPs have had clients approach them for help with cybersecurity. KeeperMSP offers you a turnkey opportunity to help your clients defend their livelihoods against the #1 cause of cyberattacks: **compromised employee passwords.**

Whether your MSP is a small startup or an established service provider, your company will benefit from Keeper's aggressive volume pricing, robust reseller margins, and simplified monthly billing plans, with pro-rated purchasing mid-cycle and no contracts.

Cement Your Status as Your Clients' Trusted Advisor

Passwords are the "keys to the kingdom" for cybercriminals, which is why compromised passwords are cybercriminals' primary attack vector. A robust password manager is a simple and inexpensive, yet powerful way to prevent cyberattacks. By offering your clients the Keeper password management solution as a service, you help them take control of their employees' password habits and prevent password-related cyberattacks, cementing your role as their trusted advisor.

DEPLOYMENT MODELS TO FIT EVERY MSP AND EVERY CLIENT COMPANY

KeeperMSP supports a wide spectrum of deployment models, from full service (“white glove”) MSPs who manage everything for their users, to pure resellers who perform little or no administration for their clients.

Full-Service Model

MSP technicians have access to their managed clients’ Keeper Admin Console. They have full rights to provision end users and set up MC-specific roles, login enforcements, and teams for sharing credentials. MSP technicians may also choose to set up login credentials for users, which can be done by sharing records from their private vaults to those belonging to their MC. This allows MSPs to offer a fully integrated set of services that include a set of pre-configured login credentials they can update if needed.

Reseller Model

In this model, resellers primarily act as distributors and sell Keeper software to customers who can administer the solution themselves. The MSP can designate an administrator user at the MC to handle all system management.

Hybrid Model

In the hybrid model, the MSP Technician and the MC Administrator share system management responsibilities.

- The “local” MC administrator manages settings that frequently change or are highly specific, such as which employees should have access to a team folder
- The MSP handles large-scale initial provisioning and configuration using Keeper’s Active Directory bridge, SSO, or other provisioning methods

KEEPER BENEFITS FOR YOUR CLIENTS

Keeper's password management solutions help thousands of companies all over the world prevent password-related data breaches, improve productivity, and enforce compliance, with industry-leading features such as:

- Exclusive, proprietary zero-knowledge security model - all encryption and decryption is done at the device level
- Three-in-one solution for small businesses; in addition to password management, SMBs can use Keeper as their SSO and privileged access management (PAM) solution
- Ease of use for both IT admins and end users; rapid deployment on all devices with no upfront equipment or installation costs - get your clients up and running right away
- Support for RBAC, 2FA, auditing, event reporting, and multiple compliance standards, including HIPAA, DPA, FINRA, and GDPR
- Easy integration with SSO; no need for separate logins
- Secure storage for sensitive files, documents, photos, and videos on unlimited devices
- Secure sharing of credentials and files
- Private vaults for each employee, plus shared folders, subfolders, and passwords for teams
- Complete flexibility; whether your client is a tiny startup or a multinational, Keeper scales to the size of their business