KEEPER
Cybersecurity Starts Here™

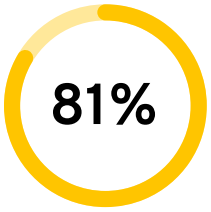
Password Management is Critical to Your Cybersecurity Strategy

From generating strong passwords to monitoring the security score of your company, today's world-class password managers are powerful assets in the war to defend your company against cybercriminals.

Table of Contents

Passwords Are the Keys to the Kingdom

Organizations can spend millions of dollars on cybersecurity defenses and consultants. Beyond the traditional tools like firewalls, SIEMs and anti-virus, it is easy to get caught up in the most sophisticated threat detection using artificial intelligence, machine learning and user behavior and analytics. All of these tools have their place and can be very valuable, however, one problem looms large:



of hacking-related breaches leveraged stolen and/or weak passwords.[1]

Passwords are frequently the only thing protecting confidential business plans, intellectual property, communications, network access, employee census information and customer data. Unfortunately, due to human error, negligence and simple lack of knowledge, passwords are also the weakest link in security. Attacking password issues head-on provides the maximum return on investment for security.

Passwords Are Not Going Away

A common belief is that biometrics, such as fingerprint, iris or facial scans, can be used to eliminate traditional passwords. There are several reasons why this is not true.

1. In one of the most common use-cases, Touch ID (fingerprint scan) on iPhones is used to unlock the PIN, which in-turn is used to unlock the phone. Therefore, the Touch ID feature is convenient, but the phone is just as vulnerable to a weak PIN with or without the fingerprint scanner.

2. There are many use-cases where the password is required to derive an encryption key. The PBKDF2 algorithm very securely converts the user's master password to an encryption key to decrypt important data. This method eliminates the need to store the encryption keys on the device. Since biometrics are always based on an approximation, they can never be reliably converted to an encryption key. Similar to the Touch ID case above, biometrics can only be used to unlock encryption keys stored on the device. This means those encryption keys may be vulnerable to attack.

3. Biometrics can't be changed, so if the corresponding file is ever compromised, then the user has to revert back to passwords.

4. Finally, despite most mobile devices coming with biometrics, a complete organization deployment means scanners have to be deployed to every computer and appliance and connected to a central authentication system. The costs of integration, broken and lost scanners and the liability of storing employee biometric files explain why biometrics has not been widely deployed already.

Biometrics remain a great option to use in conjunction with passwords when strong (two-factor) authentication is required, but passwords are here to stay for the foreseeable future.

Single Sign-On (SSO) Isn't a Silver Bullet

SSO was created to solve many of the issues associated with passwords, but most legacy and even many newer applications don't support the SAML protocols. Many privileged access accounts don't support SAML or even use passwords, so storing encryption keys (SSH, AES, RSA), digital certificates and access keys are use-cases that SSO doesn't address. Enterprises that use SSO should use a password manager to complement their SSO deployment and fill these potential gaps.

For SMBs a password manager may be the complete identity and access management (IAM) solution due to the flexibility to work with any application, website, or privileged assets like servers, databases and network appliances. Additionally, SMBs may not have the money, time or expertise for full SSO integration.

Is My SMB Really a Target?

Yes, and it's a big target. There is a common misconception among small and medium businesses (SMB) today that the biggest security vulnerabilities lie with the bigger enterprise-class organizations. In fact, there is a growing body of evidence to the contrary, which suggests that SMBs are becoming more frequent targets for cyber attacks. Why? Simply because they are 'softer' targets than enterprise organizations. A top bank knows they are a major target, but they also have the resources to spend on their own secure operations center, teams of security experts, threat feeds and the latest technology The pervasiveness of password issues means that even the largest enterprises would benefit from a password manager, but SMBs must stick to the fundamentals and get the most out of any technology that they implement. Managing passwords has to be at the top of the list.

The widely respected **2018 State of Cybersecurity in Small and Medium-Sized Businesses** study undertaken by the Ponemon group revealed eye-opening data for SMBs from the more than 1000 US and UK respondents. Included in these findings are the following:

- 58% of respondents reported a data breach in the past year, listing "employee negligence" as the main root cause
- 10,848 individual records on average were involved in the breach
- 40% of respondents said their companies experienced an attack involving the compromise of employees' passwords
- Costs of a successful attack to small and mid-sized businesses exceed $1.03 million due to damage and theft of IT assets. An additional $1.56 million is spent owing to damage and disruption of business operations.

People Are the Weak Link in Security

Keeper's Study of Ten Million Passwords that were breached by hackers shows that common employee password practices are the greatest interior security threat in an organization. The top 25 most commonly used passwords listed below represented over 50% of the 10M passwords analyzed. Nearly 17% were "123456" alone. Hackers create and maintain "dictionary lists" of these passwords and use them first when trying to break into a website, database or service. They also know that more than 60% of all people tend to use the same password on multiple websites, services and applications.

Top 25 Most Common Passwords Used in Dictionary-Based Cyberattacks

1. 123456	8. password	14. 666666	20. 3rjs1la7qe
2. 123456789	9. 123123	15. 18atcskd2w	21. google
3. qwerty	10. 987654321	16. 7777777	22. 1q2w3e4r5t
4. 12345678	11. qwertyuiop	17. 1q2w3e4r	23. 123qwe
5. 111111	12. mynoob	18. 654321	24. zxcvbnm
6. 1234567890	13. 123321	19. 555555	25. 1q2w3e
7. 1234567			

If employees aren't using passwords on this list, then they use birthdays, addresses, names of their pets, their favorites sports team, or any number of easily guessable combinations. It isn't their fault, it is impossible to remember strong, unique passwords for every account.

Employees often give up trying to come up with unique passwords and use the same password across several accounts. The obvious issue here is if any service is breached, then the hackers immediately have access to all their other services. The Yahoo breach alone provided 3 billion credentials. Hackers can do this same analysis and build "cracking dictionaries" that they use for "credential stuffing" attacks. In other words, they try the most popular passwords and have a very impressive success rate.

Other employee tactics include storing passwords on sticky notes or in a spreadsheet or other electronic document. Also, most browsers today offer to store passwords and automatically logs in when they visit a site. Now a hacker doesn't even have to be that clever in attacking the passwords. All they need is physical access to the computer, or in the case of storing passwords in spreadsheets or browsers, remote access through a means like RDP. If this sounds far-fetched, consider that Trustwave found that remote access was the top contributor (29.7%) to breaches, ahead of phishing (18.8%).[2]

Bring your own device (BYOD) policy, where employees are allowed to use their personal devices for work, provides companies with flexibility, reduces costs and increases productivity. BYOD also opens the door to security, administration and compliance issues. When employees use personal devices to log in to work accounts, they need the passwords and again, store them in files or in the browser, compounding the problems with those solutions.

After all the lost productivity and security issues employees incur trying to create and remember passwords, they still forget and call the helpdesk. Gartner found that up to 50% of helpdesk calls are password-related. One study showed the cost of each help desk call is $31. Forrester found that several large companies have allocated over $1 million annually for password-related support.

Even privileged users (IT admins) often share a spreadsheet by emailing or copying them to a USB drive where they can be intercepted or lost. Copies can easily be made and there is no way to see who can access those copies or prevent employees that leave from taking them. There is no audit trail of when the passwords change or who has access to them, making compliance with any security standard impossible.

Why Does My Business Need a Password Manager?

Employee Behavior

Keeper enables organizations to have visibility of their password hygiene and risk factors that can result in a data breach and reduce employee productivity as a result of password-related issues. This may include excess time searching for passwords, forgotten passwords, insecure sharing of passwords, contacting the helpdesk for assistance in resetting a password, etc. Aside from the security breach costs, the productivity losses are substantial because employees transact with login credentials throughout their entire day, across multiple sites, systems and applications. Keeper also allows the employee (the user) to take control of their passwords and use a unique, random and high-strength password for every site, system and application. Every employee is provided a secure, cloud-based digital vault that stores passwords and any other critical information such as encryption keys and digital certificates. Keeper will generate strong, random passwords and automatically fill them for users. This saves them time, frustration and eliminates the need for them to reuse and remember passwords. The Keeper vault is available to employees from any device and location. All of this makes the entire organization more secure, increases productivity and drastically cuts helpdesk calls.

Password Visibility

Most businesses have limited visibility into the password practices of their employees which greatly increases cyber risk. Password hygiene cannot be improved without critical information regarding password usage and compliance. Keeper solves this by providing comprehensive password reporting, auditing, analytics and notifications. The Keeper Admin Console provides at-a-glance views of employee password strength, reuse and two-factor authentication status through the security audit screen.

Securely Share Passwords

Each user has a 2,048-bit RSA key pair that is used for sharing password records and messages between users. Shared information is encrypted with the recipient's public key. Keeper's record sharing methodology is easy to use, secure and intuitive.

Enable Secure Bring Your Own Device (BYOD)

A password manager is critical for companies that have a BYOD policy as the administrator has more power over the Keeper Vault regardless if the device is employee or employer owned.

Keeper Enterprise enables IT admins to control what platforms (web, browser extensions, mobile and desktop) are allowed to access Keeper Vaults. The admin has control over the logout timer, so they can ensure that the employee must log in to the vault regardless off if they have a PIN set on their device. Two-factor authentication can be required and the method can be selected.

Zero-Knowledge Architecture

Zero-Knowledge is a system architecture that guarantees the highest levels of security and privacy by adhering to the following principles:

1. Data is encrypted and decrypted at the device level (not on the server)
2. The application never stores plain text (human readable) data
3. The server never receives data in plain text
4. No Keeper employee or third-party can view the unencrypted data
5. The keys to decrypt and encrypt data are derived from the user's master password
6. Multi-Layer encryption provides access control at the user, group and admin level
7. Sharing of data uses Public Key Cryptography for secure key distribution

The best solutions support 256-bit AES encryption and PBKDF2, which are widely accepted as the strongest forms of encryption available.

No Compromise on Cloud vs On-Premises

Cloud-based services have the allure of lower upfront and ongoing maintenance costs due to their scale. If cloud services become obsolete, a business can move rapidly without ripping out and replacing entire data centers. Businesses that are able to take advantage of these lower costs and agility have a huge advantage in the marketplace. However, many organizations hesitate moving to cloud-based services due to security concerns.

The key is the Keeper zero-knowledge encryption model, which is quite different from other cloud solutions. All of Keeper's user-facing applications are on-device, meaning key generation and encryption/decryption is done on-premises. That gives IT admins complete control over the private keys and the physical access to the records stored in the vault. Admins may restrict platforms, locations and control every aspect of the usage model.

The cloud component of our product is purely for the synchronization of encrypted data syncing and access controls. Keeper is fanatical about protecting customer data, but in the unlikely event Keeper was hacked, the attackers could only possibly access the worthless AES-256 ciphertext.

Multi-factor Authentication Support for Additional Security

Keeper allows IT administrators to select and enforce two-factor authentication to the Keeper Vault. Options include: Text, TOTP (Google Authenticator, Authy), Smartwatch, DUO, RSA and FIDO U2F (Yubikey).

More Than Passwords. Protect Against Trust-Based Attacks

Trust-based attacks occur when hackers are able to obtain digital certificates or encryption keys to critical services. By definition, a trust-based attack is difficult or impossible to detect. Imagine the losses and liabilities associated with these critical services:

Remote Access: Networks and people are distributed worldwide so businesses have no choice but to offer it. Securing remote access requires multiple layers of SSH keys, digital Certificates for VPN and Multi-factor authentication.

Cloud Services: Entire businesses are now built in the cloud. Amazon AWS, Google Cloud and Azure management all require more than usernames and passwords. IT admins need Access Keys, Secret Keys and API Keys.

Website: This is the new storefront for businesses. A successful attack carried out against a digital certificate can have disastrous effects on an organization. And aside from the security aspect, expired certificates cost companies millions of dollars in lost business.

App Deployment: Apple, Google and Microsoft all require the use of code signing certificates to distribute applications through their platforms. Each individual team member within a software company must be responsible for managing their own keys and ensuring that production-level keys are protected.

Keeper stores all of your private keys, digital certificates, access keys, API keys and other secret data in an encrypted digital vault. Keeper provides a simple way to access your private information across any device type or OS. With Keeper, these digital assets are fully encrypted locally on your device with 256-bit AES and the ciphertext is stored in Keeper's Cloud Security Vault.

Microsoft Active Directory (AD) for Rapid Deployment and Role-Based Access Control (RBAC)

Businesses are constantly changing with new people starting and current employees moving or leaving. Not only do people change roles, but the IT services and accounts businesses offer are constantly changing. It is impossible for the IT team to manually provision, maintain and log all of these activities needed to keep systems secure and meet compliance. Microsoft Active Directory has become the standard for centralizing user roles and access.

Keeper Bridge allows businesses running Microsoft Active Directory or Open LDAP to integrate Keeper password management software within their current systems, automatically adding any number of Nodes (organizational units), Users, Roles and Teams. Once connected, Keeper enables role-based access control (RBAC) at any Node. These controls include master password strength, masking, rotation, 2FA, IP whitelisting, biometrics, platforms, sharing and account transfers. Those controls can be cascaded to all lower Nodes if desired. Teams may be provisioned for sharing credentials. As the people move throughout the organization, Keeper keeps their roles updated through AD. This includes locking an account when an employee leaves and the ability to transfer those credentials to a trusted admin.

Single Sign-On (SSO)

The password manager should enhance any Single Sign-On solution by providing a secure password manager that stores not only login credentials and passwords, but also proprietary customer data, access credentials to restricted systems and sensitive documents.

Keeper SSO Connect is a SAML 2.0 application which leverages Keeper's zero-knowledge security architecture to securely and seamlessly authenticate users into their Keeper Vault and dynamically provision users to the platform. SSO Connect works with popular SSO IdP platforms such as Okta, Centrify, AWS, OneLogin, Ping Identity, F5 BIG-IP APM, GSuite, Microsoft ADFS/Azure AD and JumpCloud to provide businesses the utmost in authentication flexibility.

Compliance and Auditing

Password management solutions are key to meeting global compliance standards and best practices for strong cybersecurity policies for your company. Strong password hygiene and password management systems are integral to any company's InfoSec policy, regardless of size or industry.

Access control is part of any cybersecurity framework and passwords should be the primary focus.

NIST Cybersecurity Framework PR.AC-1: Identities and credentials are managed for authorized devices and users

PCI-DSS Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Requirement 8: Identify and authenticate access to system components

HIPAA 164.308 (a) (5): Log-in Monitoring and Password Management

ISO 27001 A.9.4.3 Password management system: Password management systems shall be interactive and shall ensure quality passwords.

Most frameworks try not to be prescriptive because they are meant to be adaptable to any environment. Therefore, your credential management system could be done on paper or in a spreadsheet, but keeping them secure, updated and audited is impossible if you have more than a few employees and assets to protect.

Every cybersecurity framework requires audit/logging capabilities.

NIST Cybersecurity Framework PR.AC-1: Audit/log records are determined, documented, implemented and reviewed inaccordance with policy.

PCI-DSS Requirement 10: Track and monitor all access to network resources and cardholder data

HIPAA 164.308(a)(6): Response and Reporting

ISO 27002 12.4.1: Event Logging

Keeper provides audit logs complete with timestamps and filters to enable rapid searches for anomalies, bad behavior or forensics.

HIPAA 164.308 (a) (5): Log-in Monitoring and Password Management

ISO 27001 A.9.4.3 Password management system: Password management systems shall be interactive and shall ensure quality passwords.

Most frameworks try not to be prescriptive because they are meant to be adaptable to any environment. Therefore, your credential management system could be done on paper or in a spreadsheet, but keeping them secure, updated and audited is impossible if you have more than a few employees and assets to protect. Every cybersecurity framework requires audit/logging capabilities.

NIST Cybersecurity Framework PR.AC-1: Audit/log records are determined, documented, implemented and reviewed inaccordance with policy

PCI-DSS Requirement 10: Track and monitor all access to network resources and cardholder data

HIPAA 164.308(a)(6): Response and Reporting

ISO 27002 12.4.1: Event Logging

Keeper provides audit logs complete with timestamps and filters to enable rapid searches for anomalies, bad behavior or forensics.

Conclusion

Passwords are the “keys to the kingdom” for hackers and are their primary attack vector. Companies can spend millions on cybersecurity and many do, but a solid password manager should be the first investment for formidable, proactive protection and ROI. From a security perspective, the vast majority of breaches start with stolen or weak credentials. From a cost perspective, Keeper Enterprise will increase employee productivity and materially reduce help desk costs. Keeper offers rapid provisioning solutions for every organization, regardless of size and can seamlessly integrate with Active Directory, LDAP and all major SSO solutions.

To learn more about how Keeper can protect your business and increase employee productivity through the use of our industry-leading, privileged password management solution, please contact sales@keepersecurity.com.

Sources: [1] - Verizon Data Breach Investigation Report 2017
[2] - Trustwave Global Security Report 2017

Business Sales

Americas & APAC
+1 312 829 2680

United Kingdom
+44 20 3405 8853

Germany & DACH
+49 89 143772993

Ireland
+353 21 229 6020

EMEA
+353 21 229 6011

Netherlands
+31 20 262 0932

Iberia & Italy
+34 919 01 65 13

Sweden & Nordics
+46 8 403 049 28

Support

Consumer
+1 312 971 5702

Business (Americas & APAC)
+1 312 226 4782

Business (EMEA)
+353 21 229 6019