keeper

What To Look For When Evaluating A Password Management Solution

A practical guide for a mission-critical decision

Introduction

Today's data threat environment can be defined as **dynamic**, **dangerous** and **diverse**.

By **dynamic**, we mean the environment is in hyper-drive when it comes to changing very quickly, with new threats and threat actors popping up almost daily.

It is **dangerous** in that the damage unleashed by successful attacks can devastate a company, particularly small- to mid-sized business.

It is **diverse** in that threat vectors are coming from all directions, with the undeniable fact that the overwhelming majority of successful attacks result from stolen or compromised passwords.

This guide is intended to serve as a roadmap in evaluating password management solutions, which are a highly effective bulwark against attacks targeting chronically weak password hygiene practices that exist within many organizations. It lists and evaluates several important factors in considering a password management solution, taking much of the guesswork out of this key business decision. But first, the guide will look at the many factors which, when combined, essentially mandate that all organizations, SMBs in particular, deploy and use the best password management solution for their unique needs.

The SMB threat environment

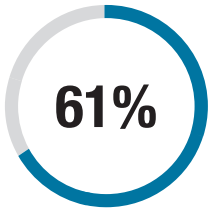
There is a great misconception floating around many SMBs today that the biggest security vulnerabilities lie with the bigger enterprise-class organizations. In fact, there is a growing body of evidence to the contrary, which suggests that SMBs are becoming huge targets for cyber attacks. Why? Simply because they are 'softer' targets than enterprise organizations.

In fact, CSO, the leading magazine for cybersecurity, believes SMBs must do two things. First, they must do much more about cybersecurity than they are doing today. Second, they must pay particular attention "especially (to) the password practices of their employees."

In addition, the widely respected 2017 State of Cyber Security 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:

of respondents reported a data breach in the past year, listing 'employee negligence' or poor password practices as the main root cause

individual records on average were involved in the breach



reported a cyber attack in the last year, up significantly from 55% the previous year

Costs to an SMB of a successful attack exceed $1 million due to damage and theft of IT assets.

An additional $1.2 million is spent owing to damage and disruption of normal business process.

of ransomware attacks caused by weak and/or stolen passwords were reported by respondents last year

The bottom line is that SMBs today are high-value targets for hackers, who go after the weakest spots in a company's cyber defenses. Those weak spots most often involve poor password practices.

An SMB's greatest vulnerabilities

Anyone looking for proof of the business value of an effective password management solution need look no further than Verizon's vaunted 2017 Data Breach Investigations Report.The study unearthed many alarming statistics, but the following may have been the most shocking:

of hacking-related breaches leveraged either stolen passwords and/or weak or guessable passwords.

Leading security analysts have long been critical of the lack of visibility that both IT and non-IT managers have in regards to the password practices of their employees. Based on *Keeper's Study of Ten Million Passwords* which were breached by hackers, common employee password practices are the greatest interior security threat in an organization.

Birthdays are also very commonly used and exceptionally easy for hackers to crack.

Study after study shows employees' fondness for blithely sharing passwords with co-workers or third parties. Many simply write passwords for various accounts on paper and keep it in plain sight or an otherwise easily accessible location. Still others use the same password over and over or with slight, easily detected variations.

The very fast-growing Internet of Things (IoT) further poses significant risks to SMBs, as thousands of these devices appear in offices, on walls as smart thermostats, in break rooms, and other seemingly innocuous places. The reason is that these devices come shipped from foreign manufacturers bearing very simple, factory-installed passwords that are supposed to be changed for security.

But a first-time, large-scale survey of IoT usage found that nearly three in four millennials (25-34 age range) are not even aware that these devices arrive from most manufacturers with simple, pre-set default passwords. Some 65% of these millennials, who are the most active buyers of IoT devices, are unaware of the rising tide of concern centered around IoT device security. And the same percentage of millennials (65%) say the current evaluation regarding the security of IoT devices isn't that serious of an issue.

Why a password management solution?

It is rare when there exists an affordable and comprehensive solution to essentially bulletproofing an organization against the root cause of the overwhelming number of cyber attacks. But that is precisely the case with password management solutions. Choosing then deploying the right solution gives the upper hand in the cyber wars to the company and not the hackers when it comes to protecting against the most common attacks and attack vectors.

For starters, these solutions machine-generate highly complex, virtually unhackable passwords that feature long combinations of letters, numbers, and symbols. While it is true that no password is totally unhackable, the fact is that the more difficult they are to break, the more likely that hackers will just move on to another target. Of course, such passwords would be impossible for users to remember, which is why most don't use them in the first place. But the password manager requires that only one password be remembered. That password then unlocks the very complex passwords from a secure vault.

In the better password management solutions, that vault is inaccessible to anyone but you, not even IT managers or administrators. But what these managers do gain immediately is a very comprehensive vision of just how well all employees are following prescribed password practices, without ever having access to employee passwords. For example, managers can instantly assess the strength of passwords in use, but cannot see the actual passwords. Managers can also determine if employees are using the same password for multiple sites – another password no-no.

One other thing. There is a dangerous and very misleading notion that passwords will soon become obsolete, owing largely to advances in biometrics that will obviate the need for passwords. Believing this can put an organization in great danger. A recent major survey found that biometrics by itself cannot provide security on its own, but rather as a component of the kind of multi-factor authentication that virtually all security experts advocate today. Passwords are always part of such a multi-factor authentication strategy.

Smart Choices

So what matters when selecting a password manager? We recommend looking at the following options.

Zero-knowledge architecture

The master password used to access the password vault is the key to the kingdom, and should never be stored outside of the user's control. Zero knowledge architecture ensures that no one – not even the developer of the password management software – has access to the master password. Users can protect against accidental disablement of the vault to designated contacts without sharing the master password. A zero-knowledge architecture should work across the continuum of use, both when data is at rest on the device and when it is in transition to another location, such as a cloud security vault.

Experience and customer validation

Password managers come and go, as several have entered the market only recently. Look for a solution that's battle-tested over a long period of time. Check the number of downloads on app stores, as well as the number of positive user reviews for evidence that a password manager has withstood the test of time and demonstrated a commitment to remaining current, and to solving customer needs.

Quality of support

For some developers, password management is a sideline to their core business. Others, particularly in the consumer market, work on a low-cost, high volume basis and keep support costs at a minimum. When choosing a password manager for your business, check customer testimonials, online help resources and support policies. A reputable supplier should promise 24/7 live customer support. Anything less could lead you in the lurch if you are out of the country and can't call during the business hours that are convenient to the vendor.

Built-in encryption capabilities

Numerous government and regulatory guidelines, including the National Institute of Standards and Technology[1] and the European Union's General Data Protection Regulation[2] recommend encryption as the most effective form of data protection. All password managers encrypt data at some level, but not all encryption is the same. The best solutions support 256-bit AES encryption and PBKDF2, which are widely accepted as the strongest forms of encryption available. They also provide multiple layers of encryption at the record, folder and team level. Data should never be unencrypted at any point. Data in transit should be protected by 256-bit TLS/SSL encryption and all of the applications should be protected with Key Pinning.. Protection of "data in motion" has been an issue in the past with products that may briefly decrypt data during transmission, or while stored on cloud servers for their own convenience.

Ubiquitous access to the password vault from any device

We live in a multi-device world, but that shouldn't inconvenience people who need access to valuable information no matter where they are. Look for solutions that support all major types of mobile devices, as well as the most popular browsers, both on the desktop and the phone or tablet. Flexibility is key. Users of mobile devices may want an extra layer of protection via two-factor authentication. The password manager should support all the native features of the user's preferred device. For performance reasons, users should be able to synchronize a fully encrypted local copy of their password vault for offline access. Any changes to the vault should be instantly replicated across all devices for consistency and security.

Secure file storage

Business-critical files stored on public Web servers are an invitation to attack. Unfortunately, many users have little choice if they need to share files with colleagues or business partners. For utmost safety, look for secure file storage that uses government-grade encryption and sharing features that apply both to individual files and entire vaults. Many password managers don't offer file storage. Integrating this feature with an existing zero-knowledge security architecture avoids the need for stand-alone file-sharing services and the related complexity and vulnerability that accompanies them.

Robust group features

Organizations need to share access to common applications. A shared password manager can provide security, structure and administrative accountability. It can also deliver valuable backup protection in case people leave the company and take their password vaults with them.

When considering group features, look for the ability to assign passwords at both the individual and group level to sites, folders and vaults. Permissions and policies should be flexible enough to support your internal standards but strong enough to prevent unauthorized access. Role-based permissions, credential sharing, and scheduled password rotation can enforce access policies automatically and ensure that strong passwords are always in use.

Most importantly, strong IT administrative features should give IT management full visibility into groups, roles, and permissions. Administrators should be able to designate backup access to individual vaults in case employees leave the company unexpectedly. If your company uses Active Directory or LDAP, ensure that the password manager integrates seamlessly with those services. For Single Sign On (SSO) integration, look for compatibility with platforms such as Amazon AWS, Okta, OneLogin, Ping Identity, F5 BIG-IP APM, Google G-Suite and Microsoft ADFS/Azure AD..

The Keeper Difference

Keeper Security has been building the world's most secure and functional password managers for nearly a decade. Unlike companies that make password management a sideline, Keeper is 100% focused on this market. Built for IT Admins, it was designed from the ground up to provide the highest levels of security for business professionals working with sensitive information.

Our breadth of coverage and depth of features speak for themselves. Keeper runs on all major smartphones, tablets and computers, including iOS, Android, Windows, Mac, Linux, Kindle and BlackBerry. It's available in 21 languages and 80 countries. Keeper is the most-rated password management app in app stores, with more than 50,000 5-star reviews. It's used by millions of people worldwide.

Keeper builds the most secure solution for individuals on the market. For businesses, its functionality is unparalleled. It enables organizations to integrate password management into their existing permissions and authentication structure, with full tracking and reporting for compliance and security purposes. Users can share passwords with individuals, groups and by business role. They can also optionally share files in vaults protected by 256-bit AES encryption. Powerful administrative functions enable IT to view and change access roles with full audit trail functionality.

Sources: 1 - NIST Digital Identity Guidelines
2 - EU GDPR website

Business Sales

Americas & APAC
+1 312 829 2680

EMEA
+353 21 229 6011

United Kingdom
+44 20 3405 8853

Germany & DACH
+49 89 143772993

Iberia & Italy
+34 919 01 65 13

Ireland
+353 21 229 6020

Sweden & Nordics
+46 8 403 049 28

Netherlands
+31 20 262 0932

Support

Americas & APAC (Consumer)
+1 312 971 5702

Americas & APAC (Business)
+1 312 226 4782

EMEA (Business)
+353 21 229 6019

https://keepersecurity.com

sales@keepersecurity.com