CSO

Password Management

SURVIVAL GUIDE

Ignore the world's worst passwords; look at how they're created | *Better passwords are possible with better security leadership* | **Employees have no qualms in selling corporate passwords** | How to evaluate password managers | *Review: Best password managers for the enterprise*

Making peace with passwords

By now we're all well aware of what makes a bad password—it's us.

A glance at SplashData's annual reporting on the world's worst passwords shows just how laughably bad at creating passwords us humans really are. But what's worse, as Steve Ragan's analysis of leaked passwords shows, is that many passwords on the naughty list adhere to the carefully crafted password policies in use in companies today.

How can security leaders do better? For one thing, we can stop blaming users, says Michael Santarcangelo. Instead, we can focus on providing them with technology that makes the job easier.

That's where this guide comes in.

We'll help you communicate the challenges and what is at stake and evaluate and choose the right enterprise password management solution for your business.

CONTENTS

Ignore the world's worst passwords; look at how they're created

SplashData's worst passwords list is irrelevant for the most part; the real lesson is what makes the passwords so bad in the first place

BY STEVE RAGAN

Every year SplashData releases a list of the world's worst passwords, and for the last five years that list hasn't changed much. While the list is an amusing look at password blunders, the real lessons are in how and why those passwords exist in the first place.

I've collected some raw data in order to help clarify some of these lessons.

After cracking a list of passwords leaked to the Darknet in 2015, two observations were immediately clear; people have taken classic password creation advice to heart, but no one has taught them that technology has rendered it obsolete.

The other lesson is that humans are really bad at doing random. It isn't in us to create a random password that someone with a dictionary and a set of rules can't crack.

The world's worst passwords

The following table contains the world's worst passwords (Top 25) according to SplashData:

123456	password	12345678	qwerty	12345
123456789	football	1234	1234567	baseball
welcome	1234567890	abc123	111111	1qaz2wsx
dragon	master	monkey	letmein	login
princess	qwertyuiop	solo	passw0rd	starwars

It's true, each one of the passwords in the table above are comical examples of password-based security. And yet, if altered slightly, some of them will pass many of the corporate password policies that are used worldwide.

Such policies might seem familiar: Passwords should be X characters in length (usually 5-8, sometimes longer), using a mix of both uppercase and lowercase letters, digits, and special characters.

Such policies are designed to protect corporate assets and users, but they're easily predicted by password cracking software and skilled attackers. Moreover, these policies are the same ones people use outside of the office to create their own passwords, and again, they're vulnerable to the same set of flaws.

Enter MMO Kings

In late 2015, someone compromised the MMO Kings database and leaked it. The leaked data included unsalted MD5 password hashes, which (next to clear text) is the worst possible way to store passwords in a database.

For those who don't know, MMO Kings is a website that allows gamers (such as those on World of Warcraft) to purchase gold or other in-game currencies for actual cash, but it also offers a power leveling services.

I took the leaked hashes and spent a small amount of time cracking them using Hashcat on Kali Linux. After the passwords were cracked, I ran some stat analysis using Pipal (created by Robin Wood) and Passpal by T. Alexander Lystad.

Collection:

In all, the leaked hash list included 89,872 accounts. After removing 22,324 duplicate hashes, we were left with a list 67,547 to crack.

As a testament to the weakness of common passwords, such as those highlighted by SplashData, and the weakness of non-random password generation – it took less than three minutes to crack 74-percent of the hashes.

In under an hour, we had cracked 54,473 hashes, or about 80-percent of the list.

A second clean up was performed, which removed a single blank password, as well as 556 duplicate passwords. It's worth noting that within the removed set, there were 20 accounts that used an email address as a password – something you should never do.

This left us with a list of 53,917 passwords to examine.

Note: The passwords were cracked with Hashcat. The process included a single NVIDIA GeForce GTX 970 GPU, the RockYou.com wordlist (which includes the SplashData set from the last five years), and various rules that ran against the wordlist. In all, we gave the hash list ten passes before we felt we had enough data to work with.

The stats:

Of the passwords recovered from the hash list, 76-percent of them contained 1-8 characters, thus, only 24-percent of them were more than 8 characters in length.

As a side note, there were 11,593 passwords recovered that used a maximum of 6 characters.

Passwords this small can be easily recovered with modern tools and hardware, suggesting that the accounts were either non-essential to the user, or they picked something personal and easy to remember.

Given that most of the passwords recovered included dates, months, or days of the week, the personal nature of these smaller passwords is almost a sure bet.

Yet, the standout metric in the recovered password list are the base words. These are the words used to create the final password when stripped of variation and additions.

Compare the table below to the SplashData list and look at the common elements.

password	dragon	blue	qwerty	shadow
mike	alex	monkey	killer	soccer
andrew	michael	john	pass	gold
chris	hello	silver	death	master

The most common characters in the recovered passwords are:

`a e 1 o r n 2 i s l`

The most common symbols:*

`! @ - . * # _ ? )`

**Please note that a blank space is included on this list, fourth spot from the right*

The base word list and the common character stats prove that people are still using the password creation rules of old. So the problem isn't the weak passwords as highlighted by SplashData, it's the construction methodologies and policies that govern them.

Passwords with a minimum of eight characters, uppercase and lowercase letters, numbers, and symbols were solid rules to live by ten years or so ago. But that was then, these days those rules are obsolete when stacked against modern technology.

Again, in 45 minutes we cracked 80-percent of the list using basic words and common cracking rules, that's far from a professional job.

However, every day professionals crack passwords the world over during Red Team engagements with the same set of tools, because nothing stronger is needed. That's a problem.

Building a better password

Passwords aren't going anywhere anytime soon. There has been some serious progress made in the authentication market over the last few years, and perhaps eventually passwords

will go away altogether. But until that happens, passwords are what we have.

When it comes to developing a password policy for your organization or for yourself, the key thing to remember is — perfection isn't going to happen. Let it go. You'll never develop a perfect, impossible to crack password. It's not going to happen.

Humans cannot do random, and *m@k1ng Y0ur P@55w0rd l00k 1ik3 th15* isn't going to *help1234*.

Eventually, given enough time and resources, someone or something can crack your password. The key is to make that process expensive in both time and effort.

As far as application development and password protection is concerned, organizations would be wise to follow OWASP's advice, including no limits on character sets and long max lengths (up to 160 characters) for passwords.

In addition, passwords should be salted and use an adaptive one-way function, such as PBKDF2, scrypt, or bcrypt.

For the rest of us, the easiest path would be to use a password manager.

Why a password manager?

The rule has been drilled into the public for years – you need a long, randomly generated password for each website you have an account on. However, remembering all of those passwords is near impossible, so instead people pick a single password – one they assume is secure – and use it everywhere.

That's where the problem starts. Using the same password across multiple websites, or a variation of the same password, never works. The moment one account is compromised, all others are placed at risk.

Password managers remove the requirement to remember those long strings of random characters. They even remove the problems with randomness during the creation step, because they'll create a proper random password for you.

Now, all anyone has to do is remember the single master password that makes all the other passwords available for use.

Generating a solid master password

One fantastic way to generate a solid master password is to use Diceware.

In 1995, Arnold Reinhold developed Diceware as a means to help people create strong and memorable PGP passwords.

You start with a wordlist and then roll five (5) six-sided die. Each roll will correspond to a word in the list. The goal is to get at least six words, but eight is best (for now). Anything less is risky.

There's a whole science behind Diceware, and it's a great way to develop something both memorable and secure, which has no real connection to you personally. If you wanted to support a small business, a sixth grader in New York City will develop a Diceware password for you, the cost is $4 per password.

Once you have a Diceware password generated, it isn't going to take too much effort to remember it. Another reason why it makes for a solid master password is the overall length and the randomness in which it was created.

If you don't want to use a Diceware password, and you'd prefer to create you own, the SANS guidelines are a solid starting point.

The best bet these days is to use a password manager and to generate a random, lengthy password, for each website you've got an account on. From there, use a master password that is long, such as a phrase that if ever spoken aloud, would make absolutely no sense to anyone around you. That's where Diceware comes into play.

Better passwords are possible with better security leadership

Renewed focus on "bad passwords" and blaming people overlooks the real problem and the need for security leaders to drive change.

BY MICHAEL SANTARCANGELO

Are you enjoying the annual parade of the worst passwords?

This year it's not just the trade media lamenting the terrible state of passwords. It's capturing national headlines. It pops up on local media with the admonition to "change your password."

Now it includes a never ending spate of social media commentary that amount to a collective sigh. Then the poor conclusion that people are just too dumb. This annual parade of negativity prompts a smug question:

"When are people going to learn?"

Before jumping on the bandwagon, give me a chance to reframe the challenge. And to show you why it's your leadership opportunity.

Instead of asking "when are people going to learn?" ask "When are we going to learn to serve people better?"

Is this a failure of people? Or of the security community?

The theme this year seems to be, "Again? Didn't we have this conversation last year?"

Yup. We sure did. And the year before that, too. For at least a decade or longer. Except we're conflating "complaining publicly" with "conversation." We sidestep root cause analysis in favor of confirmation bias. A chance to decry our "people problem." And renewed calls for a "post password age."

Passwords aren't going away.

And they don't need to. What if the failure we lament is actually a signal that we missed the opportunity to serve people?

A password is a component of authentication. A common mechanism to allow an individual (identity) to authenticate themselves to systems. They need this access to process and act on information. Identity, authentication, and authorization is vital to how we protect systems and information.

Passwords are powerful they are easy to use. They are easy to change — useful in a variety of situations. They are ubiquitous, too. And that's part of the reason passwords seem like a problem.

How the drive for complexity turned into obscurity. And comedy.

Consider how the collective industry explains the need for complexity. Or is it length? What about handling password resets?

The only constant here is the confusion.

Almost no consistency between applications, organizations, or experiences. Befuddling and archaic requirements mixed with minimums and even maximums. Oddly worded guidance and warnings.

This is maddening to most of us.

But it's comedy gold for the local networks. Everyone has a password joke. And a strategy to contend with it. Designed to get back to get-

ting their work done. That means the headlines intended to guide (or is it goad) action turn into comedy. From late night programs to social media, everyone has a password joke.

And bad passwords. Openly and freely admitted. Almost like a badge.

So what happened?

Part of the problem with passwords is that we never really taught people how they work. I don't mean the technical details. Just a high-level functional overview. Connected with the value of a password to their work instead of an inconvenience to endure.

The direct impact is the introduction of friction. Lots of it. It erodes our value, increases the cost of connecting to people, and makes it harder to fix.

Then we got caught in a cycle.

We created longer lists of steps to guide people. We confused them on "best practices." Then we implemented technology to "prevent" poor password choices. Driving people to find routines that worked — but might not increase the strength.

We pushed them into password reuse.

The risk of password reuse is real: why won't someone do something?

We created the conditions. Our efforts to increase complexity drove the need for reuse. Our efforts to promote password hygiene disconnected people from the process. Instead of investing time to understand, they found a way to get by.

We missed early opportunities to break down the complexity. To offer understandable insights and guidance. Instead of offering people password managers, we argued over their security.

I've invested a few hundred hours into understanding passwords. On exploring ways to translate the complexity of passwords into understanding. To develop - and test - how to teach people how to manage, use, and protect their passwords.

Success comes from investing the time to distill to clarity. The caveat is the need for technical accuracy explained in a functional way. It means an investment in communication over technology. Success comes when bringing people together and offering them a hands-on opportunity to learn.

But when I ask companies the value of solving this problem… crickets. Is it worth $1/person? $10? I'm still trying to figure this out.

I don't mean slapping together a few slides to tell people. Or part of an annual program. What if we actually offered people a pathway to understand. A way to act. And then supported them with password managers and other programs to make it easier.

This is our opportunity.

One more thing: where did they get the password list(s)?

Where did the lists come from anyway?

From authentication *systems* that weren't protected. Poor implementations combined with missing maintenance. It's the system that the password depends on. Not the password itself.

Misplaced focus on the password. And miss the real tragedy of the system.

It doesn't have to be this way.

Headlines and stories like these highlight our need to change. To translate our complexity into comprehension for others. To design *usable* systems. To support people with technology that makes their jobs easier — while protecting information.

We need leaders to stop lamenting symptoms and start leading solutions.

It's time for the security leaders to emerge and lead the change we need

Addressing passwords — even if you want to replace them — is a leadership opportunity. It means ending the steady diet of negative infor-

mation. Rejecting the "evidence" that people are the weakest link. And embracing the notion that we're in this for the long haul (the infinite game).

The operative question is "are we better today than yesterday?"

The exceptional leader asks "are the people around me better today than they were yesterday?" Then see to it that the answer is yes.

In that effort, invest in how you and your team communicate. Install and protect better systems. Integrate user design into the process. Reconsider how we explain and teach people to create, manage, and use passwords. Offering them access to password managers.

Solve the problems we can today so we're able to focus on what tomorrow brings.

Employees have no qualms in selling corporate passwords

Insider threats come in many forms, and one of the most difficult to counter is the employee who is willing to sell corporate passwords.

BY TAYLOR ARMERDING

Plenty of people are careless with their own personal passwords – using the same one for multiple sites, and/or making them so simple that they are comically easy to crack – but hardly anyone would intentionally sell them for a few bucks to someone they know would use them to do them harm.

Apparently, however, some of them don't have those qualms about selling corporate passwords. A global survey of 1,000 employees at large (more than 3,000 workers) organizations, commissioned by vendor SailPoint, found that one in seven would sell their password to an outsider for as little as $150.

This is not a new problem, however. And $150 is, relatively speaking, big bucks. A 2012 survey conducted in the UK found that almost half of the respondents would sell their corporate passwords for less than 5 pounds, while 30% would sell them for just 1 pound.

It also doesn't surprise people like Christopher Frenz, director of IT infrastructure at Interfaith Medical Center, who said, "other research groups were able to get people to reveal their passwords for something as small as a chocolate bar."

But, Frenz added that it is important to know how rigorous such research is. "These surveys tend to interview people who self-select themselves for participation, so they're not a representative cross section," he said. "They (the surveys) often lack proper controls, and do not typically try to verify if the user is actually revealing a real password. It makes you wonder how many people just make up a password on the spot for the free chocolate or the few dollars?"

Understanding the problem

Still, even if the actual percentage is smaller than the surveys found, it is enough to blow a major hole in any company's data security.

"Human beings are fallible, and this sort of issue is a real problem," said Muddu Sudhakar, CEO of Caspida, recalling headlines about a Morgan Stanley financial adviser who was fired after he allegedly stole account information from about 350,000 wealth management clients and posted the information of 900 online.

In that case, the leaked information reportedly included names and account numbers but not passwords. But it clearly illustrates that insiders offering sensitive corporate information for sale can indeed be "a real problem."

One obvious question is why even a minority of workers would risk losing their jobs, and therefore not just their immediate livelihood but also their entire career, for just a few bucks?

Joseph Loomis, founder and CEO of CyberSponse, said employee loyalty should not be assumed. "How many employees do you know who truly care about the organization where they work?" he said. "Excluding some of the top organizations in the marketplace, employee morale or care is always a concern for triggering insider threats."

Sudhakar said he suspects workers know that if their personal passwords were compromised, the consequences would be certain and severe, while they might view a corporate password as, "someone else's problem or think there might not be a consequence to misusing it."

Frenz said some workers might not realize how important their corporate passwords are. "This is particularly true if the data they handle at work would not normally be considered sensitive," he said, "as they likely fail to grasp that their account may provide a doorway that can be used a staging ground to gain access to more sensitive data via privilege escalation and like methods."

Sudhakar agreed. A compromised password is just the first step, he said. "Bad guys establish a foothold within the enterprise, escalate privileges, move laterally to get at the data, maintain their presence until they can get at sensitive data and ex-filtrate the goodies," he said.

Some argue that selling passwords is not as big a problem as weak passwords, because they are so easy to hack. Indeed, any password of fewer than 10 characters that is an actual word, even in reverse with a few upper-case letters thrown in, is like an unlocked door to hackers with even minimal skills and the right software. That, they say, makes for a sale price of next to nothing.

Loomis doesn't buy that entirely. He said offering passwords for sale does make it easier for criminals, since it eliminates them having to try even two or three times to gain access – an anomaly that security countermeasures could pick it up as suspicious.

In search of a solution

Whatever their value on the market, a relatively new group – the FIDO (Fast Identity Online) Alliance – says it is one more reason to eliminate passwords entirely.

FIDO Vice President Ramesh Kesanupalli, also founder of Nok Nok Labs, said in a statement that, "enterprise users selling passwords demonstrates yet another example of how flawed and risky password-centric authentication is."

FIDO, a nonprofit formed in 2012, has published standards for strong authentication that require, "exchanges of cryptographic data with FIDO servers – not vulnerable personal information of any kind," Kesanupalli said.

Still, even with authentication credentials much more secure than passwords, if people are willing to sell them, the problem remains, or perhaps could be even worse, since those credentials would likely be more valuable.

That, experts say, means the need for better security awareness training is essential. Frenz said it is important to let employees know that it is not just corporate data that is at risk. "Reminding people that work not only stores customer data but a lot of their personal data in the form of HR and payroll records can often help to put things in perspective," he said.

And the website Malicious Link argued that enterprises need to understand the psychology of employees and to provide incentives for them not to be tempted to sell their credentials.

If security professionals become, "familiar with the emerging studies under the banner of cognitive psychology/behavioral economics," they will be able to understand "irrationalities" in human judgment, and, "design better incentive systems and security control schemes," the post said.

The good news, according to Sudhakar, is that even if people willingly sell or compromise their credentials, technology has gotten better at spotting the inevitable breach that follows.

"Innovations in data science and machine learning are improving early breach detection from compromised credentials or insiders gone bad," he said.

That, combined with better training and an awareness of disgruntled employees, may be the best defense. As Frenz notes, passwords do have a major advantage over other, more secure, forms of authentication like biometrics.

"They are very easy to change once compromised," he said.

How to evaluate password managers

All password managers have up to as many as four separate products for storing passwords, but not all tools support all four mechanisms.

BY DAVID STROM

All password managers have as many as four separate products for storing passwords: a desktop and mobile app, a browser extension, or a pure Web-based service that doesn't require any other software beyond a regular browser. There are various use cases that demand having this array of mechanisms. Not all tools support all four mechanisms.

Most tools on the market have a separate Windows desktop app and most can handle Windows 7 and newer versions. TeamsID, Keeper and LogMeOnce have only browser-based versions. Dashlane limits to 32-bit OS or 32-bit browsers. Others add Mac and Linux desktop apps. In addition to traditional desktops, most of the products support iOS and Android devices. Keeper, LastPass, and StickyPassword also have versions that work on Kindles, BlackBerries and Windows Phone mobiles. Browser extensions for some of the major vendors (Firefox, Chrome, IE and Safari) are supported in most products. And half of them have direct Web-based SaaS portal pages that you can login in and obtain your password in a pinch without having to install any software.

Login process

Second, how these tools automate the login process differs. There are subtle differences in how each tool completes the login process, and they also differ across the operating systems. For example, on the desktop or with a browser extension, most tools will automatically fill in the login information (except for TeamsID) and then (if you select this option) perform an auto-login to the site. On mobile phones, the products will bring up a protected browser session (1Password), auto-fill the information (Keeper), or make you cut and paste the details manually (LastPass). The behavior on mobile devices is important, particularly as more of your users migrate to doing more work there and want better password management tools. Note that SingleID has a very different process.

Motivating users

Third, can you motivate your users to have better password hygiene with these tools? Maybe. The temptation to reuse passwords, and use ones that are simple (and therefore easy to crack) is great, but these products all try to move the needle towards better password usage. They all have some feature that will produce a random complex password of many digits using symbols and upper and lower case: at least you have a more secure login than something that you could come up with on your own.

Password replace

Several of the products (including Manage Engine, Dashlane and LogMeOnce) can do a one-button quick password replace across your entire vault, which is useful if you are either ultra-paranoid or have been compromised. Many of the products offer dashboards or graphical displays that show you a summary of your entire password portfolio, or send a series of nagging emails to try to get your users to remove duplicate or simple passwords.

Synchronization

Next, how synchronization with your vault happens across multiple devices differs. The ideal use case for these products would be for a user to move effortlessly among different endpoint devices: Start with an iPhone in the morning, move to their Windows desktop during the workday, and then to a Chromebook or some borrowed desktop's browser at a remote meeting location. LastPass and LogMeOnce both do the best job of this. Other products, like 1Password, have very cumbersome synchronization mechanics. When you evaluate these products, pay attention to where they store their password vaults and how these vaults are protected.

Aging endpoints

What if you have older endpoint versions? Some of the products don't support older OS versions, particularly on mobile phones and tablets. That could be a concern depending on the mix of vintages present in your end user device population, and knock a few of these tools out of the running. For example, the latest version of 1Password only supports Macs running Yosemite and LogMeOnce doesn't work with iOS versions before 8.0.

Windows 10

Speaking of operating systems, dealing with Windows 10 is a problem for all of these tools. Microsoft hasn't made it easier for these password managers with the release of Windows 10 and its Edge browser. Edge doesn't support any browser extensions and therefore won't work with any of these products. If you want to make use of them you will either have to install another browser such as Firefox or Chrome, or try to make do with the built-in version 11 of Internet Explorer. This seems counter to what Microsoft was trying to do to make a more secure browsing environment.

MFA support

Many vendors have improved their multifactor authentication (MFA) support, although none of the vendors mentioned here offer authentication methods on a per-login basis that could step up authentication for particularly sensitive logins: for that level of granularity you will need to use an SSO tool. But each vendor offers different MFA tools, with LastPass the most flexible and LogMeOnce the easiest to set up. Both of these offer multiple MFA methods as part of their tools. StickyPassword and Dashlane offer the fewest MFA methods, while the others are in between these extremes.

Admin features

Finally, consider how each product is managed by an enterprise IT administrator. Most products have a separate web-based portal that admins can use to set up security policies and directory synchronization, among other features.

Review: Best password managers for the enterprise

LastPass, Keeper top the field in test of 10 password managers.

BY DAVID STROM

In 2013, we reviewed six password managers, some suitable for enterprises and some primarily for consumers. The field has exploded and today there are more than two dozen products on the market. Even the popular TV show "Shark Tank" evaluated a password manager startup.

But this level of activity doesn't necessarily indicate quality. We found that some of the products we reviewed then haven't improved as much as they could have. And some of the newer products are still a work in progress.

Password managers are an important first step for organizations that want to strengthen their security by helping users cope with multiple logins. While browsers have gotten more intelligent about storing passwords and synchronizing them across different platforms, you might want to have more control over the way your users manage passwords, which is where these tools come into play. Password managers are often seen as a less expensive and easier to implement solution than single sign-on products.

In this review, we looked at 10 tools: Dashlane for Business, Keeper Security Enterprise, LastPass Enterprise (now part of LogMeIn), Lieberman Enterprise Random Password Manager, LogMeOnce Enterprise Edition, Manage Engine Password Pro, Agilebits1Password for Teams, StickyPassword, SplashID TeamsID, and SingleID. (Manage Engine is now owned by Zoho, which has a separate SaaS-based password product called Vault. We didn't test it because it's more consumer-oriented.)

Since our last test, most of the products have made at least some strides in strengthening their features and sharpened their focus on the enterprise, although some (like Dashlane and TeamsID) are still just a small step up from a consumer product.

Others, such as LastPass and Manage Engine, have improved to the point that they could be close to offering what a single sign-on tool has, without the additional administrative hassles.

The basics for these products haven't changed: all (except SingleID) create some kind of master "vault" that stores your login information and is protected with a special password. The tools automate your logins to various online and local servers, and manage the strength and diversity of your password collection.

Winners and Losers

The two strongest products in terms of protecting individual user logins are LastPass and Keeper. Always a strong product, LastPass has gotten stronger in the past two years and has the largest collection of enterprise security policies.

While Keeper supports a larger collection of mobile devices, LastPass isn't far behind. Keeper has a more elegant login method for mobiles, which could be a consideration. Keeper will cost at least twice as much as LastPass, however.

If you want a password management tool mainly for your IT team that has to administer many servers, then consider either Lieberman or Manage Engine. While Lieberman's tool has

Features

Product	Annual Price (per user)	Versions	Mobile Apps	Features
Dashlane for Business	$40	Windows, Mac, Browsers, SaaS	iOS, Android	Enterprise management, multifactor authentication
Keeper Security Enterprise	$48 +$750/year/ installation	Browsers, SaaS	iOS >8.0, Android, BlackBerry, Kindle, Nook, Windows Phone	Enterprise management, multifactor authentication, Active Directory support
Lastpass Enterprise	$24	Windows, Mac, Linux, Browsers, SaaS	iOS, Android, BlackBerry, Windows Phone	Enterprise management, multifactor authentication, Active Directory support
Lieberman Enterprise	$25,000 (one time)	Windows, SaaS (2)	None	Enterprise management, multifactor authentication, Active Directory support
LogmeOnce Enterprise Edition	$65	Browsers	iOS >8.0, Android	Enterprise management, multifactor authentication, Active Directory support
Manage Engine Password Manager Pro	Starting at $1,238 (one-time)	Windows, Linux	iOS, Android	Enterprise management, multifactor authentication, Active Directory support
AgileBits 1Password for Teams	$60	Windows, Mac, Browsers	iOS, Android	Limited enterprise management
SingleID	Free	None	iOS, Android, Windows Phone	Multifactor authentication support
Sticky Password Premium	$20	Windows, Mac, Browsers, SaaS	iOS, Android, BlackBerry, Kindle	Multifactor authentication support
TeamsID	$36	SaaS	None	Limited enterprise management

long been around for this purpose, its interface is showing its age and Manage Engine can be a cheaper and just as functional alternative.

We included SingleID in this review because it is trying to do something quite innovative: part password manager, part identity manager. Basically, you use its smartphone app to encode your identity in a single, six-digit passcode to build your own secure identity infrastructure.

The other tools are more for individual consumers or lag behind in terms of features.

Pricing on these products is all over the map: some charge an annual per-user subscription fee that is generally less than $50, others charge a one-time license fee that can be a few thousand dollars (Manage Engine) to multiple thousands of dollars (Lieberman), and one is completely free (SingleID).

Individual reviews:

Score card

Product	Client breadth	Mobile ease of use and support	Enterprise management depth	Total
Dashlane for Business	4	4	2	3.3
Keeper Security Enterprise	5	5	3	4.3
Lastpass Enterprise	5	3	5	4.3
Lieberman Enterprise	3	0	5	2.7
LogmeOnce Enterprise	3	4	3	3.3
Manage Engine Password Manager Pro	3	2	5	3.3

Dashlane for Business

Consumer-focused Dashlane recently entered the enterprise market with its Business product, which is still a work in progress. Dashlane for Business adds a thin veneer of additional enterprise and team management software that is available via a browser window.

The Business version lacks an Active Directory agent, although they are working on it for next year. Instead, you have to export a list of Active Directory users and import it into their product.

The current version only works on iOS v8 and above, although it will install an earlier version for older operating systems. That is a nice touch, and we wish other vendors would follow their lead here, rather than locking out older smartphone models entirely. Another nice touch is that you can quickly import your entire password vault from several competitors' products, including iPassword, Keeper and LastPass. That's good if you want to migrate away from those tools.

One rather unique aspect of the product is a web-based email inbox scanner, which anyone can access even if you aren't a current customer. Once you grant the scanner temporary access to your inbox, it will produce a report that shows you how many account passwords are present in your inbox. The theory is that if they can find them, so can a hacker who might get into your account. In my account, there were hundreds of passwords, and it also spotted my favorite reused password with ease.

It has simple two-factor support: you have just a single option, to enable this for new devices when you add them or for all logins; there is no step-up authentication for individual apps. It just supports Google Authenticator now and there are plans to add Yubico's MFA key and other tools in January. You can also make use of the fingerprint readers for the mobile phone versions as an additional factor.

Dashlane comes with a separate management dashboard web page that shows you summary statistics, such as the number of users and passwords that it is storing and their overall strength. The information is available for your entire enterprise too. This is just for display purposes: other products have more actionable

dashboards.

Dashlane has a SaaS version, which is very stripped down and just used to login to existing sites. You can't make any changes or add new sites: you have to do that in either the desktop or mobile versions.

Dashlane doesn't support 64-bit IE versions, you'll need to launch the 32-bit version. We had trouble getting IE v8 setup and suggest that if you are still using that ancient version, this isn't the product for your enterprise. Overall, Dashlane has some solid features for individual use but Keeper and LastPass have moved ahead of them in the past few years for the enterprise.

Dashlane for Business comes with a free onboarding session, whereby a consultant helps you get started, imports your users, and makes sure that the product is setup properly. This is included in its price, which makes it a good value.

Dashlane has a free version that has limited features. Both the consumer and business versions cost $40 per year per user, with large discounts for quantity purchases.

Keeper Security Enterprise

Keeper comes in browser extensions that really don't do much more than bring up the SaaS-based version of the product. There are many different mobile versions (more than most of its competitors) including BlackBerry, Kindle, Nook, and Windows Phone, plus iOS and Android. Perhaps this is why Keeper is preinstalled on numerous smartphones by both Orange and AT&T. Note that for iOS you'll need at least v8. Keeper comes a close second to LastPass in terms of overall benefit.

The mobile versions bring up a protected browser session, and your username and password information are shown across the top. When you get to the part where you want to login, you tap on each credential and they are placed in the appropriate spots on the app. That is a very neat and clean way to do the logins and better than any other product we looked at. If your users need something to support logins from their phones, this should be the first product you look at.

Their security scorecard for each user is somewhat basic, but nice to have.

Keeper supports a variety of second authentication factors, including RSA SecurID, SMS, voice calls and Google Authenticator. You can only have one method active for your account at any time, and there is no step-up authentication for individual apps.

Keeper uses a separate Web-based portal for its enterprise specific features, such as the ability to enforce a second authentication factor, password complexity requirements, a list of users and their supported mobile devices, and the Active Directory agent.

Like the other tools, it has a complex password generator. You just click the button next to the password field and it fills in with some random sequence. Unlike LastPass and some of the other tools, you don't have any options for its format, other than the enterprise-level complexity parameters.

Keeper does not have access to any vault data as all of this is encrypted in the cloud and the key to encrypt and decrypt it resides with the user and occurs at their device.

The base plan for Keeper Enterprise is an annual $750 fee plus $48 per user per year. There is also a personal version that starts at $10 per user per year for a single device.

LastPass Enterprise

LastPass continues to have one of the largest collections of supported clients, spanning mobile (including Blackberry and Windows Phone), Web and desktop versions. Their enterprise management has been significantly improved, adding some solid features.

LastPass had a busy year in 2015. First, there was a well-publicized security breach and then at a session at BlackHat Europe, two researchers were able to compromise an account via a series of exploits. In November, the company

was acquired by LogMeIn. Despite these issues, they still have a solid solution.

The product has always been designed for the enterprise and there are now several ways to provision users: via a bulk series of emails, synchronization with its Active Directory agent, writing custom code with its documented API, integration with the standard Windows Login process, and via SAML connections.

SAML is supported for a variety of third-party apps and also includes the ability to provision and de-provision users on Google Apps, Box, Amazon Web Services, WordPress, and some others. De-provisioning is important: this means as you delete users from your enterprise accounts (such as from Active Directory), they automatically are deleted from your LastPass records and from the corresponding service provider. Many of LastPass' competitors have ways to synchronize with Active Directory but not take this additional step. LastPass also works with authentication systems such as SecureAuth or RSA SecurID. All of this is impressive, and certainly more useful than any other password utility we tested.

Like other tools, these features are managed via a series of web menus. But unlike the others, LastPass' are somewhat difficult to initially navigate. This reflects how the product has grown in the past several years. Configuration screens are spread across four menu trees: one for more than 50 security policy setup options, one for user management, one for various reports and one for managing SAML connections.

Speaking of those security policies, this is a very extensive collection, the largest of any of the 10 products we examined. You can specify password lengths, prevent mobile logins, control logoff behavior, prevent the tool from being used on TOR exit nodes, and restrict to particular IP address ranges. There are lots more choices and they can be applied across all of your users or selectively to specific groups. We tried to get a screenshot showing many of them but the list was too long. Instead, we'll offer a link to some solid suggestions about how to strengthen your password management techniques in a blog post they wrote in November in response to the BlackHat exploit.

LastPass also has the largest collection of multifactor methods, with more than a dozen vendors and methods supported. You can turn on as many of these as you desire, unlike some of its competitors that only allow a single method per user.

There are also several ways to install its Mac and Windows desktop software, which reflects its enterprise heritage: via an executable, via a "silent mode" with a command line interface, or via a Windows group policy object using an MSI file.

The LastPass vault is stored in the cloud, where each component can access the information. Browser-based products connect to the cloud, while the desktop and mobile versions make and automatically synchronize their copies to the local desktop.

LastPass has an amusing and somewhat annoying way to remind you to update your password portfolio, sending out a periodic email trying to shame you into changing the similar and simpler passwords with a subject line "Improve your passwords sucker!" when it detects more than three similar passwords. Also one of its tools available from the browser extensions menu is called "security challenge" where it will scan your vault and show you how poor your password choices are. Whether this will motivate your users isn't known, but at least it is a nice attempt.

It also has the ability with one click to change multiple passwords in your vault, like some of its competitors.

One issue for LastPass is you will need to first bring up its mobile app and paste the password into your browser session; it doesn't transfer this information automatically.

LastPass costs $24 per user per year, with volume discounts starting at 100 users.

Lieberman Enterprise Random Password Manager

We reviewed the Enterprise Random Password Manager (ERPM) product two years ago and it is still the gold standard for setting up massive password collections to protect large local server infrastructures, although Manage Engine has a somewhat nicer interface. ERPM's menus and basic command structure hasn't changed much in the past two years.

ERPM comes with a Windows app that connects to its database and has both its own user interface and a Web-based one. Administrators use mostly the former, and ordinary end users the latter. This is because the Web UI doesn't have the full complement of controls that the native Windows apps does. Passwords are stored in a local database on the server. For example, a user can recover their password from the Web UI.

It has the ability to discover SSH keys and manage them, both the public and private keys, and authorize users for these keys. Indeed, the goal of the product is to make your logins so effortless that you won't ever need to remember your passwords.

You can schedule how often the passwords change, and have this happen automatically, again, so your users don't have to bother with this chore. It has more powerful scheduling features that can update your entire password collection, or be used to create reports, or automate other activities.

It performs the logins via its own Remote Desktop connection from its server, what Lieberman calls a jump server. It does this via a series of several dozen Visual Basic scripting apps, which come as part of the product and which you can customize for your own circumstances.

And it also records each of your sessions, and can play them back, so you can view what is going on with your users and see if something is amiss.

ERPM works with a number of trouble ticketing systems, including Jira, CA Service Desk, and others. It supports a number of OATH two-factor authentication tokens. There are extensive reports that can be customized in the Windows interface.

Lieberman's biggest drawback is its price tag: a $25,000 one-time fee. However, if you are running a large installation of servers in your data center, this is probably one product that you will need to deploy.

LogmeOnce Enterprise Edition

The newest product on the password management scene is LogMeOnce (which is not affiliated with another company LogMeIn). They use a browser extension (and a mobile app) and are still a work in progress, which is to be expected since the product was released in November.

Once the browser extension is installed, you go to their website where you see a dashboard with various controls across the top. Here is where you add logins, strengthen your security, and control the tool's overall behavior. They have several nice features:

First is an app catalog, similar to many of the SSO tools, listing several thousand apps. You can choose login/password combination or make use of SAML to authenticate yourself. The built-in app for American Airlines didn't initially work but was fixed after we mentioned the issue.

Next is support for several multifactor authentication methods, including sending a SMS text, voice or email message, and Google Authenticator. You can turn on multiple methods and select the most convenient one when you login to your vault. Setting these up is very simple: for example to enable the SMS you send a code to your phone and enter it in the appropriate dialog box on screen. While impressive for its ease of use (this product was the easiest

of the 10 to set up for MFA), these MFA tools are just to secure the initial access to the tool: like the other products, there is no way to step up authentication for specific apps.

It comes with a complex password generator that you just invoke by clicking in the password field from your browser. But there is also a separate generator that is available for non-customers via its own web page, should you feel that you are missing out on this action.

Its overall security scorecard has a series of reports, including login activity with date, time and IP address along with which sites you're logged into and their password strength indicators. LogMeOnce also can save notes in its password vault too.

And there is an add-in that will encrypt your entire Dropbox collection— this is included in the Enterprise edition.

They are one of the few password vaults where you can choose the location of your vault, depending on your paranoia level: on a USB thumb drive, locally on your desktop, or in their cloud. You can change it at will with a simple click of the mouse. The other tools are less flexible in this regard.

They also support OpenID and SAML in the Enterprise edition, along with connections to a variety of enterprise directory providers such as Oracle and CA.

There are several versions, ranging from the free consumer and Business editions to the more capable Enterprise edition. Pricing is based on particular features: You start with the basic set for $2 per month per user and add items such as directory integration or risk-based authentication (both are another dollar per month per user each), user provisioning ($2 per month per user), with a discount of $5.40 per month per user if you purchase all the options. The mobile apps are free, regardless of which plan you choose.

Manage Engine Password Manager Pro

Manage Engine's Password Manager Pro (PMP) is similar to the Lieberman product and designed for enterprise teams that want to manage a large and mostly local server collection. The product takes the form of a server running on either Windows or Linux. Either server uses a Web interface; there are also mobile apps and browser extensions to automate logins that are used by individual users.

Once you install the software and setup some basic parameters, PMP stores encrypted copies of passwords in its password vault in a local SQL server, which it calls its resources. It has a long list of different kinds of information that it can contain, ranging from Windows and Linux application servers to fairly esoteric things such as AS/400 minicomputers and Juniper firewalls. One drawback was that it wasn't as capable with web-based logins: it couldn't automate the login on our American Airlines site that has three data fields. That is a pretty basic issue on an otherwise capable product. You download the browser extensions and set up your mobile apps from the main console.

You will need to ensure that your users can access the PMP server across your enterprise network by having its default Port 7272 open: administrative users connect via their browsers to run the configuration screens. Normal users can make do with browser extensions to access their pre-configured resources.

PMP supports several user access roles including super admin, admin, and regular password users. You can enable two-factor authentication and mobile access for specific users or groups. Users can be regularly imported from an Active Directory store just by furnishing the Active Directory credentials and setting up a synchronization service in PMP, there is no need for additional agent software. Each resource can be set up to be viewed, modified, or managed according to specific access rights policies.

There is also a unique series of advanced administrative policies where you can set up a resource to require a "double authentication" by two network administrators. All these policies have the effect whereby a user doesn't have to know their password to access a resource, yet the login can be protected with a very strong password. You can also set up specific circumstances where users can have access to a resource for a limited time, such as a few minutes, to complete a certain task. For highly sensitive servers, this can be very useful.

PMP has similar feature to ERPM where it can record every session that involves making use of a login. It does this by opening a Remote Desktop or SSH connection inside the browser, and connecting from its own server to the network resource. These recordings can then be played back so you can see exactly what each user was doing. You can also "shadow" an active login session and terminate it if something is amiss. PMP also comes with a wide collection of audit and compliance reports.

PMP also supports SSO, and has built-in tools to enable high availability and failovers for its SQL servers.

Finally, it offers on-demand password resets across the board or schedule regular password changes.

Pricing is very transparent and available in either of six configurations: standard, premium or enterprise, and either as a monthly subscription or a perpetual license. The lowest perpetual license is a two-administrator package for $1,238 with an annual maintenance fee of $248 for the standard edition. The enterprise edition supports 10 administrators and will cost $7,488 and $1,498 for the annual maintenance. These licenses include unlimited numbers of resources and users.

Agilebits 1Password for Teams

1Password comes as paid Windows or Mac desktop versions with free iOS and Android mobile versions. There are also browser extensions. 1Password has a large collection of items that it can store in its vault besides passwords, including file attachments and free-form text notes. But since we reviewed them two years ago the product has somewhat stagnated, although in November they came out with a beta version called Teams for enterprises. The Teams version was still a work in progress, with an admin console that was far from complete. Still, it represents a good direction for the company.

On its desktop version, there are rough indicators of password strength: many of the other products have made this more useful and actionable. And one nice feature in Teams is an "emergency rescue kit" that contains information on how to recover your vault, should you lose your master password.

1Password has two major weaknesses: its mobile versions and how it synchronizes its vault. The mobile apps are very bare bones and bring up ordinary Safari browser sessions, but don't always autofill the username and password credentials. Adding logins from the browser is clunky; it is far easier to do so when you are on your desktop and the software will capture the information with a single click. There is also no support for additional authentication factors, unlike most of its competitors.

1Password relies on a third-party synchronization service to keep its vaults communicating with the latest password information: you can make use of a local Wi-Fi connection (if all of your devices are on the same Wi-Fi network) using Apple's Bonjour service. Probably you will use Dropbox to store your vault, which means you have to explicitly synchronize your devices. There is also a way to use iCloud, but only if you have all Apple devices. That is less elegant than some of the other products that have the syn-

chronization built in. This was an issue when we reviewed them two years ago, and others such as LastPass, Keeper and LogMeOnce have made their synchronization much easier.

A desktop license of 1Password costs $49 with quantity discounts. The Teams version is free while it is under beta, and will most likely be priced at $5 per month per user.

SingleID

We included SingleID in this review because it is going in a very different and innovative direction from the rest of the password tools. Rather than build a vault to store your password collection, it approaches the problem from the mindset of not having the user deal with any passwords at all.

To accomplish this, they have two components for their tool: first is a series of smartphone apps (including Windows Phone along with iOS and Android). Once you install the app, you set up your identity; either by typing this information directly into the app or via a webpage that you can import the details via a QR code scan. You can include all sorts of things in this identity besides your name and address, including credit card numbers and other personal and business details. All of this identity information is tied to an eight-digit ID number in their database that is then displayed on your phone.

The second component of SingleID is a piece of open source PHP code that you place on your website. This turns the typical login dialog into a special form that asks for your SingleID login ID number. Once you type in the number (which looks like a one-time password but doesn't ever change), SingleID then authenticates you back to your phone, and asks if you want to login to this particular site. There are code snippets for Wordpress blogs and regular web servers to get you started in adding the SingleID protection to these sites.

It is a clever hack, and once you get it setup you avoid a lot of infrastructure to get a secure login. Think of the SingleID login ID number as your username for their service, so you don't have to worry about keeping it a secret (like a OTP) because no one can do anything with this information. There is no trusted (or even untrusted) third party because all the communication is between your smartphone app and the server that you wish to access. This means that you also don't have to worry about man-in-the-middle attacks, because there isn't anything in the "middle."

The advantage, apart from having to no longer have to manage multiple passwords, is that you retain complete control over your identity information. There is nothing stored on any cloud: your information is stored and encrypted on your smartphone. As the vendor says, "SingleID is a distributed platform and thus no database of sensitive personal data is being built up anywhere."

Of course, the downside is that you have to instrument all the websites that you want to make use of the SingleID process, which won't help you when you want to login to Dropbox or American Airlines or the hundreds of other commercial sites that you already have accounts on. But for internal applications, this could be a very useful and inexpensive solution, since it is completely free. The GitHub documentation is very clear, and it should take an average developer just an hour or so to review it and implement its code.

StickyPassword

Sticky comes with desktop and mobile and browser extensions. The mobile versions include Blackberry, Kindle Fire, and Nokia X phones, in addition to iOS (7.x and higher) and Android (2.3 and higher) phones. There is a limited SaaS control for certain administrative features, but this is because it doesn't really have any enterprise management features. Each user has to manage their own account, using the SaaS app.

It has limited browser support: there is no

Safari Windows extension and on Macs just Safari and Chrome browsers are supported.

It also has limited second factor authentication where if you change the SaaS settings, it will send an OTP to your email address when you attempt to register a new device. Other tools have more granularity for their MFA feature.

Sticky's complex password generator is also behind the times of its competitors. The browser extension merely copies the complex password into the clipboard. If you want something more sophisticated, you will have to use the desktop version to incorporate it into the login process. We had problems logging into our Southwest Airlines account using their mobile app.

One nice feature is that Sticky presents you with two browser options on their mobile app: using the phone's native browser or its own protected version.

Sticky has a free version that doesn't have password synchronization across all its platforms: to have that feature, you will have to pay for the Premium version. The one-year subscription is available for $19.99, and the lifetime license is available for $99.99.

TeamsID

TeamsID is a very simple password manager that is designed for enterprises. You set up groups of users within your organization that share the same password collections. It is currently available as a pure SaaS app, other versions are in the works for mobile and desktop apps and browser extensions.

By simple we mean that there are none of the other features that most of its competitors offer: there is no support for multifactor authentication and no Active Directory connector. TeamsID stores its vault in the cloud, as you might suspect.

When you save your login information, you are also prompted to save additional information, such as an attached file, tags, or other notes about the login to the record. The software tries to find an appropriate logo for each record, but it was somewhat inconsistent when we tested it. Records can be for individual logins or for groups. You can choose from a number of blank templates to fill in, such as for a bank or an airline frequent flyer account.

Records are shown in alphabetical order on the main dashboard, and the password details are shown in plain text which made us somewhat nervous: most of its competitors hide this information, at least by default. Finally, one large issue is that these records are just for reference only: there is no automation of the login: you will have to copy and paste the URL, login and password from each individual field.

TeamsID has begun to build a solid product but it vastly incomplete, especially when compared to some of the more established tools.

TeamsID has a 30-day free trial and an annual contract of $36 per user.

How we tested password managers

We installed each product on Windows 7 and 10 desktops as a starting point. We also used Android and iOS phones and Mac desktops (if a client was available for these systems). We then set up logins to various Web-based services such as Dropbox, Gmail, different airline accounts and a WordPress blog site to test these logins. We connected to the various websites with at least Firefox and Chrome browsers to try out the associated plug-ins. We looked to see whether our password data was synchronized across to the various clients. We examined any enterprise management-related features if they were available. Finally, we took notes on the relative differences in the clients across different operating systems both in terms of functionality and user interface.