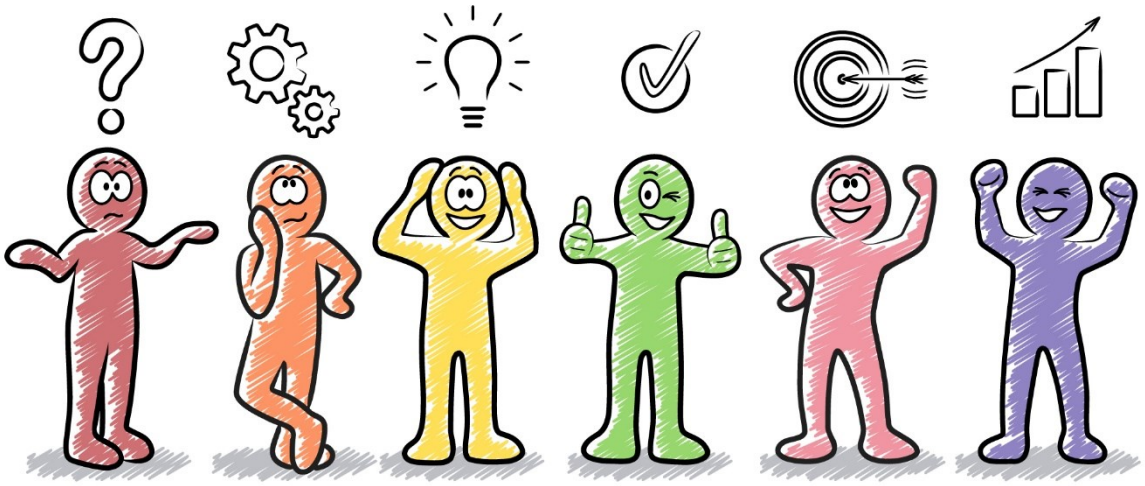
Password Management Tools for Businesses and Institutions

IMPROVING CYBERSECURITY BY ELIMINATING WEAK, REUSED, AND COMPROMISED PASSWORDS

Richard Edwards

Cybersecurity often depends on the choices made by individuals. Most of these individuals are conscientious when it comes to preserving the confidentiality, integrity, and availability of corporate systems and customer data. However, if we consider how passwords and account credentials are used and managed, we can easily see weaknesses in our cybersecurity defences.

Richard Edwards, IT industry research analyst.



R N E 2 4 7 . C O M

Contents

Executive Summary

Catalyst

Cybersecurity often depends on the choices made by individuals. Most of these individuals are conscientious when it comes to preserving the confidentiality, integrity, and availability of corporate systems and customer data. However, if we consider how passwords and account credentials are used and managed, we can easily see weaknesses in our cybersecurity defences.

Password management tools have entered the mainstream, with more than 70 apps competing for user attention in the Google Play Store alone. There's also a good selection of products targeting teams, businesses, and enterprises. However, these products need to adapt and evolve to win new business, protect against new cybersecurity threats, and support the move toward a "password-less" enterprise.

Market view

Key findings from an industry survey of IT decision-makers and enterprise employees reveals that password management practices are out of date, overly reliant on manual processes, and highly dependent on employees "doing the right thing". If the alarm bell isn't ringing, it should be. Cybersecurity training and awareness programs are useful, but to keep the business safe and secure, employees across all roles and at all levels require tools and applications to help alleviate the burden and risks associated with workplace passwords, credentials, logins, and access codes.

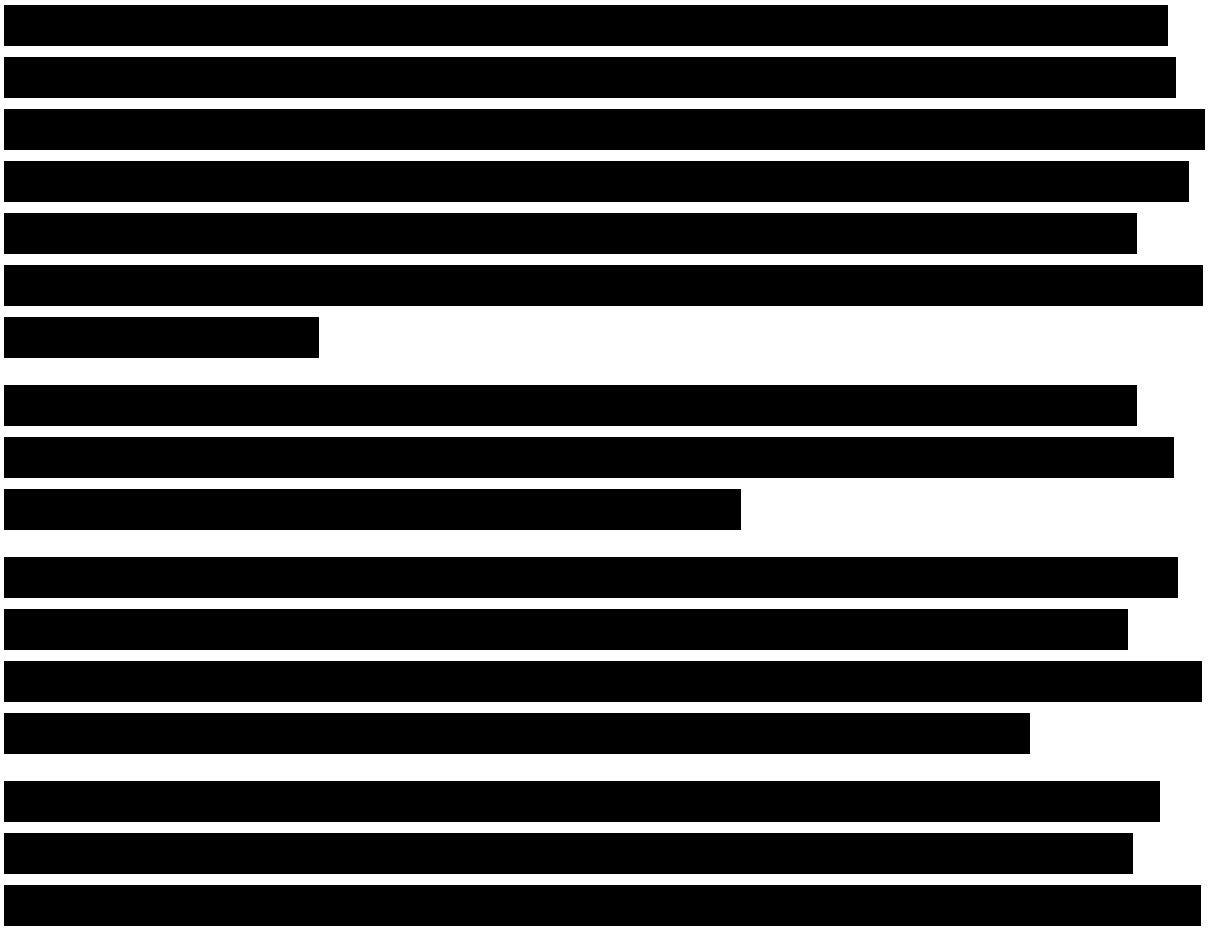
Key messages

- Passwords are for more than just the web. Desktop applications, mobile apps, IT infrastructure, and building facilities require credentials and passcodes.
- Password management tools complement single sign-on (SSO) initiatives and privileged access management (PAM) solutions.
- Expect to pay between $20 and $80 per user per year. The pricing differential reflects the functionality on offer, delivery model, and extent of enterprise capabilities.
- Multifactor authentication, password sharing, login automation, and form filling are examples of functionality afforded by more advanced tools.

- Account creation, user onboarding, and software deployment are vital considerations for any enterprise-wide software deployment initiative.
- Eliminate passwords wherever possible. If users already log into a computer, terminal, or device, don't ask them to log in again if you can help it.
- Organisations deploying Windows 10 can use Windows Hello to increase login convenience with biometrics and replace passwords with multifactor authentication.
- While far from ideal, IT and operational business requirements often necessitate the sharing of logins, account details, and passwords.
- When considering software-as-a-service (SaaS) and cloud-based products, businesses and institutions should look for relevant vendor certifications, accreditations, and reporting standards.
- Organisations must consider password management in terms of security controls covering people and processes, as well as technology.

Recommendations

Recommendations for businesses and institutions



[redacted]

Recommendations for vendors

[redacted]

Scoping the Market

The business value of better password management

Usernames and passwords are the primary means by which IT systems are secured and protected, but they are also the most targeted surface for cyber attacks. For corporate IT to remain secure, business leaders and IT professionals need to reduce the risks

associated with passwords, and this means investing in password management tools, user education, and practical policies.

Password management tools offer a more secure and convenient way of coping with password overload and the risks associated with weak, stolen, or shared credentials. Using any trusted password manager is almost always better than not using one at all, but costs need to balance risks.

A growing number of consumers and business users are making use of free and paid-for password management tools. These tools often complement existing SSO capabilities and provide a useful way of tracking personal account credentials and other sensitive pieces of information. At the other end of the spectrum, IT departments are investing in privileged access management (PAM) products to enhance operational efficiency while maintaining the highest levels of IT security. Some of the offerings assessed in this Market Radar offer PAM capabilities, and almost all add value to existing SSO solutions and enterprise identity infrastructure.

Most of the products assessed in this report are priced based on the number of users or seats, and range between $20 and $80 per year. The pricing differential reflects the range of functionality on offer, delivery model, and the extent of enterprise capabilities. With over 80% of significant data breaches traced back to a single compromised identity, it's hard to imagine any well-informed CFO baulking at the business case. However, IT and security teams should consider how password management products can pay for themselves, such as in reduced calls to the help desk, slicker business processes, fewer security incidents, and a more productive workforce. Moreover, if your organisation has an outward-facing website, consider ways in which it could become password-less.

Password management: What capabilities do you need?

The products presented in this Market Radar can all manage website passwords and credentials, but it is important to consider employee roles and occupations within the business and the nature of their needs. For example, the workstyles and requirements of executive officers, professionals, and associate professionals are likely to be different from those of administration and customer service staff. Also, different computing platforms (desktop, mobile, terminal, kiosk) require consideration.

Password management tools tend to be associated with web browsers, websites, and the management of online credentials. However, traditional line-of-business

applications and bespoke IT systems often require passwords and passcodes, as do terminal-based logins, such as Windows RDP, SSH, and Telnet sessions. If you work for an established organisation or large enterprise, you're likely to have a diverse computing environment, therefore reflect this in the capabilities of the password management solution and its usefulness across the organisation.

If legacy technologies or older computer systems don't integrate with Active Directory or SSO solutions, then it's up to users to manage their passwords. Password managers can also be relevant in the physical worlds. Consider building access codes and premises security controls. Remembering one four-digit combination might be easy enough, but what about a dozen or more?

IT teams aren't the only employees that need to share passwords, credentials, and access codes. Today's social media platforms were not developed with multiuser business accounts in mind, so sharing the company Twitter, Facebook, or Instagram login is a common occurrence across marketing teams and within digital agencies. Likewise, specialist or niche applications tend to be shared among individuals (just as friends and families might share a Netflix or Spotify account), so consider if this use case would be better managed through securely shared credentials.

Organisations that operate within regulated industries are required to keep detailed audit logs and records. Keeping track of who has (and who had) access to corporate systems is something that IT departments have managed for decades, but the uptake of commercial online services and SaaS applications are often way ahead of any SSO implementation or configuration. Password managers can help regain control of company accounts and lead to a better experience for users and IT.

Like many other enterprise software segments, the password management tools market offers a broad range of products catering for almost every imaginable requirement. Also, if something is missing, the APIs and command line interfaces provided by some of the products assessed in this report offer IT, developers, and system integrators with opportunities to fill the feature gap.

Tools that support operations vs dictate process

There's a saying: "Man shapes the tool; thereafter the tool shapes man." We've seen this repeatedly happen, particularly with information technology tools. An IT vendor might develop a useful application that companies adopt, and before you know it, other businesses are changing their processes to fit the way the application works. This

change isn't always a negative thing (best practices and industry standards often develop this way), but it's important to recognise the market origin of certain password management products.

Several offerings have developed through the consumer channel, while others originated in the operations segment of the IT management market. This landscape is reflected in bottom-up and top-down approaches to password management, especially where personal password management and password sharing are concerned. There's overlap in the centre ground of course, but larger organisations may find that implementing two or three different password management products is a more natural and more successful approach than confining the business to a single corporate standard.

IT security technologies are developing at pace, so it's probably worth adopting a tactical, rather than strategic, approach to password management tools. Having said that, if the "password-less enterprise" figures in your IT strategy, then a strategic relationship with your password management vendor makes good sense.

Reduce the complexity of the digital workplace

Password management tools are ostensibly there to help staff and employees do their job more securely and productively. Desktop apps, mobile apps, and browser extensions help users shoulder the cognitive burden that is associated with the modern digital workplace. In their purest form, password managers can be used to remember web login credentials and passwords. However, as always, there's plenty of additional functionality on offer for those that require it.

Multifactor authentication, password sharing, login automation, and form filling are just a few examples of the kind of functionality afforded by some of today's password management tools. However, each product has a different way of delivering these capabilities, and there's no standardised language or approach either. This could be a recipe for confusion, especially if employees have been using their favoured solution, so it's worth canvassing the workforce for insights and opinion.

Staff IT training budgets seem to be a thing of the past, but it's worth considering the extent of the learning curve where IT security solutions are concerned. Depending on the product, password managers can be very interactive pieces of software, and can, therefore, require tailored user training, even within the IT department. YouTube videos

help, but they aren't a replacement for formal training and relevant cybersecurity education focused on changing behaviour.

Minimise deployment and administration overhead

[redacted]

Reduce the user-visible password surface area

[redacted]

[redacted]

Monitor, audit, and review password-related threats

Password managers promise to improve the security posture of organisations by reducing the number of weak, reused, or compromised passwords. Using various algorithms, password managers can compute the strength of a password and prompt the user to change it (automatically generating and storing a random password) if required. Automating the password change process is something the W3C's Web Application Security Working Group has been working on since 2016, but a standard has yet to emerge. In the meantime, some products offer PAM-like scripts and mechanisms to accomplish this task.

Most of the products presented in this report offer a dashboard of some kind, flagging "at risk" credentials to users and system administrators. Increasingly, password management products can also flag leaked or stolen passwords found on the dark web, alerting users and system administrators when logins and accounts have been compromised.

The sharing of logins, account details, and passwords is not ideal, but it is often necessary for IT and business operational reasons. This is when monitoring, auditing, and reporting capabilities matter most. Judging by the products assessed in this Market Radar, capabilities vary considerably, although most address key requirements (who, what, where, and when) where administrator actions are concerned. Products offering PAM capabilities tend to provide more reporting and auditing capabilities and integrate with security information and event management (SIEM) tools.

Do your due diligence

Vendor go-to-market strategies

[redacted]

Market Landscape

Market origin and dynamics

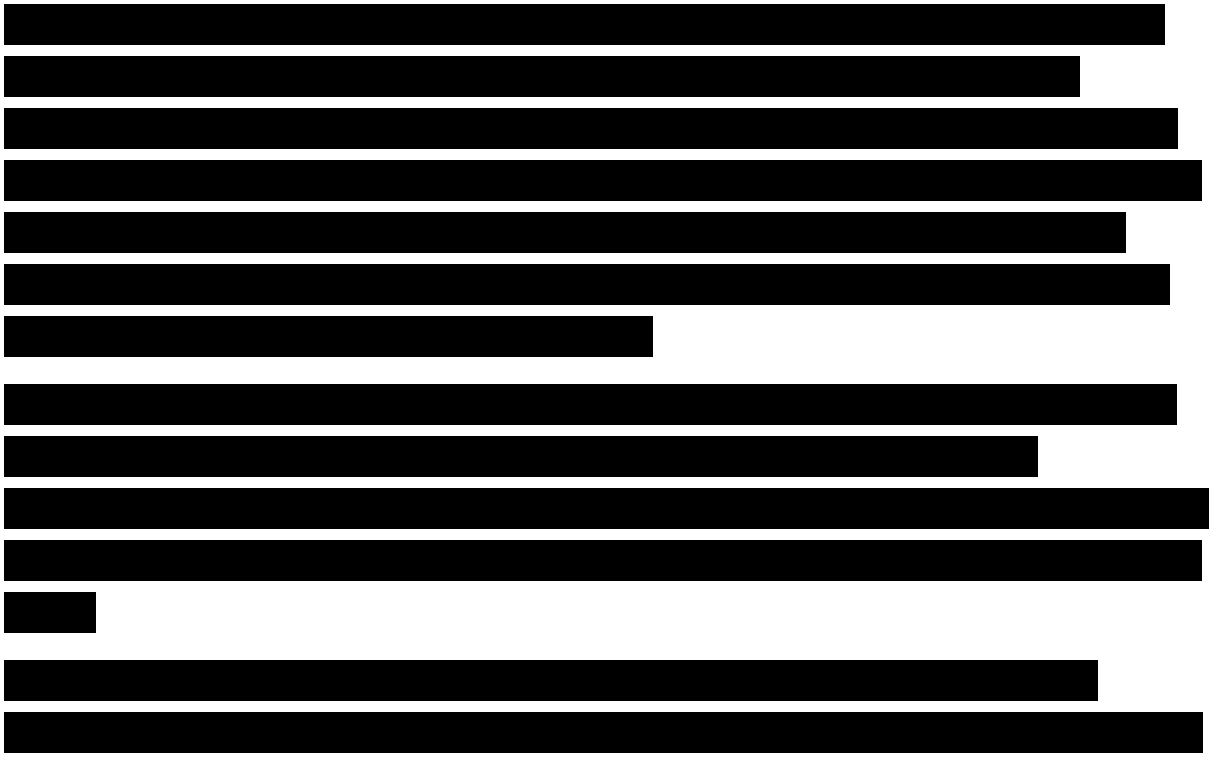
The password management tools market has been around for well over a decade (Siber Systems, the vendor behind RoboForm, was founded in 1995). A natural progression from automated form filling and IT automation products, password management tools have developed along with two main approaches. The first of these is the centralised database, such as ManageEngine Password Manager Pro.

The second approach is that of the standalone application, using encryption mechanisms and a “master password” to protect a database of passwords held on the device, significantly more convenient than perhaps a spreadsheet stored on a computer. Use of multiple devices introduced the need for passwords everywhere, so sync technology, using the cloud as a sync hub, was added to the mix. Passwords are encrypted/decrypted on the user’s device with the hashed version (PBKDF2, bcrypt, scrypt) stored in the cloud (private, public, or managed). Data is encrypted in transit and at rest.

2014 and 2015 saw a flurry of activity in the password management tools market, with a slew of new offerings for individuals. This activity continued at a pace and resulted in products targeting families, teams, and businesses. 2017 and 2018 witnessed more password management products targeting the enterprise, with the kinds of features and capabilities discussed earlier.

1Password, Dashlane, Keeper, and LastPass are among the most popular products used by individuals and businesses, while ManageEngine Password Manager Pro, Pleasant Password Server, and RoboForm have long served the commercial market and IT pros. Bitwarden, Bluink, Passbolt, Passwork, and TeamPassword offer alternative approaches, including open source projects.

Password management market trends



[redacted]

Future developments

[redacted]

Vendor landscape

[redacted]

[redacted]

Figure 1: Password Management Tools

[redacted]

1Password Business

Product summary

[redacted]

Key messages

- 1Password Business encourages staff to adopt strong passwords and better cybersecurity habits. Versions are also available for individuals, families, and teams.
- 1Password is more than a password manager: it helps business users remember, track, and share the information they need to live and work in the digital age.
- Integration with cloud-based identity providers enables organisations to embrace modern secure authentication. Less straightforward is Active Directory integration.
- Watchtower is a useful feature that alerts users to password breaches and other security problems, helping organisations to remain safe and secure.

Why put 1Password Business on your radar?

[redacted]

Highlights

[redacted]

An extra layer of security to protect super-sensitive information

[redacted]

Deployment considerations for businesses and large enterprises

[redacted]

Minimising administrative overhead

[redacted]

[redacted]

Background

Founded in 2005 by Dave Teare and Roustem Karimov, AgileBits introduced 1Password to the market in 2006. The company introduced 1Password Teams in 2015, followed by 1Password Business in 2018. A private company, the vendor is now better known as 1Password.

Current position

[redacted]

Datasheet

1Password Business

Product name	1Password Business	**Product classification**	Password management
Version number	1Password 7	**Release date**	2018
Industries covered	All	**Geographies covered**	North America, Europe
Relevant company sizes	Small and midsize companies, enterprises.	**Licensing options**	Per-user, monthly, or annually
URL	1Password.com	**Routes to market**	Direct
Company headquarters	Toronto, Canada	**Number of employees**	>100

Bitwarden

Product summary

[redacted]

Key messages

- Bitwarden is an open source software solution. The codebase is hosted on GitHub where anyone can review, audit, and contribute to it.
- On-premises hosting using Docker enables organisations to exercise complete control over their Bitwarden deployment and password data.
- Bitwarden apps are available on Windows, macOS, Android, and iOS, plus browser extensions for Chrome, Firefox, Edge, Safari, Opera, Vivaldi, Brave, and Tor Browser.
- Bitwarden does not offer password policies, and while enterprise directory sync is a supported feature, integration with single sign-on and Windows Hello is not.

Why put Bitwarden on your radar?

[redacted]

Highlights

[redacted]

[redacted]

Choice of deployment options and password data segmentation

[redacted]

Reporting, auditing, and automating

[redacted]

[redacted]

Background

As with so many modern applications, Bitwarden started as the personal project of Kyle Spearrin, the founder of 8bit Solutions. The product was initially released in August 2016 and is now used by more than 2,000 companies and 500,000 consumers. Bitwarden is licensed under the GNU Affero General Public License v3.0.

Current position

[redacted]

[redacted]

Datasheet

Bitwarden by 8bit Solutions

Product name	Bitwarden	**Product classification**	Password management
Version number	April 2019	**Release date**	August 2016
Industries covered	All	**Geographies covered**	Available in multiple languages
Relevant company sizes	All	**Licensing options**	GPL v3. Per user/month
URL	www.bitwarden.com	**Routes to market**	Direct.
Company headquarters	Jacksonville, FLA, US	**Number of employees**	<10

Bluink Enterprise

Product summary

[redacted]

Key messages

- Bluink Enterprise is a comprehensive identity and access management platform that enables organisations to adopt strong passwords without burdening the employee.
- A smartphone-based solution, Bluink Enterprise provides a range of multifactor authentication (MFA) and single sign-on (SSO) capabilities.
- Centralised password sharing ensures strong company oversight and governance, but employees may want (or need) to share passwords in an ad hoc manner.
- The combination of Bluink mobile app and Bluetooth Bluink Key works very well. A browser extension or desktop app might provide extra convenience for some users.

Why put Bluink Enterprise on your radar?

[redacted]

Highlights

[redacted]

Smartphones are the key to a password-less future

[redacted]

Centralised management and control of business credentials

[redacted]

Administration and reporting features determine enterprise readiness

[redacted]

Background

Founded in 2010, Bluink Ltd specialises in identity and access management and customer identity verification. The company has a presence in North America and supports global users from its Canadian headquarters. The company is led by Steve Borza (CEO) and Larry Hamid (CTO).

Current position

[redacted]

Datasheet

Bluink Enterprise by Bluink

Product name	Bluink Enterprise	**Product classification**	Identity and access management; password management
Version number	v4.2.1 (April 2019)	**Release date**	September 2017
Industries covered	All	**Geographies covered**	Localised in English and French.
Relevant company sizes	Mid-sized companies and enterprises.	**Licensing options**	Per user per month
URL	www.bluinc.ca	**Routes to market**	VAR channel and direct
Company headquarters	Ottawa, Ontario, Canada	**Number of employees**	<25

Dashlane Business

Product summary

[redacted]

Key messages

- Dashlane Business is an extension of the vendor's well-regarded, consumer-oriented password management and digital wallet solution.
- Dashlane's "zero-knowledge" architecture ensures it has no access to any user data on its servers. Master passwords are used to grant access and cypher data locally.
- SAML provisioning and Active Directory integration are available, but other business features, such as auditing and reporting, are less well developed.
- Dashlane provides dark web monitoring for leaked or stolen personal information. It also alerts users when compromised, reused, or weak passwords are detected.

Why put Dashlane Business on your radar?

[redacted]

Highlights

[redacted]

A zero-knowledge architecture ensures password privacy and security

[redacted]

Directory integration accelerates deployment and adoption

[redacted]

[redacted]

[redacted]

[redacted]

Secure password sharing with groups and individuals

[redacted]

[redacted]

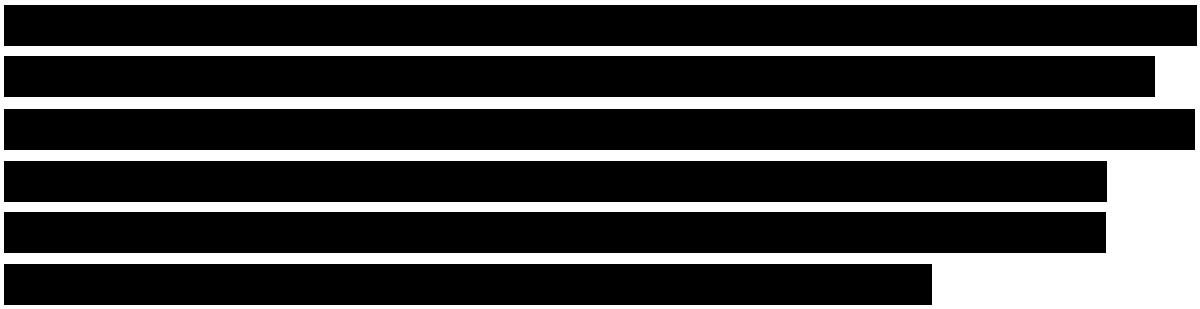
Additional layers of security and account protection

[redacted]

Background

Dashlane was co-founded in 2009 by Bernard Liautaud (former CEO of Business Objects), Jean Guillou (lead software architect), Guillaume Maron (VP of engineering) and Alexis Fogel (now at stonly.com). Emmanuel Schalit is the CEO. Headquartered in New York, with offices in Paris and Lisbon, Dashlane has raised more than $100m in venture funding. In 2014 Dashlane acquired passOmatic, a web-based automatic password changer.

Current position



Datasheet

Dashlane Business by Dashlane

Product name	Dashlane Business	**Product classification**	Password management
Version number	April 2019	**Release date**	September 2017
Industries covered	All	**Geographies covered**	Localised in 11 languages, including Japanese, Chinese, and Korean.
Relevant company sizes	Small and midsize businesses	**Licensing options**	Subscription, per user per month.
URL	www.dashlane.com	**Routes to market**	Direct
Company headquarters	New York, NY, US	**Number of employees**	~150

Keeper Enterprise

Product summary

[redacted]

Key messages

- Keeper Enterprise is a password management and cybersecurity platform. All information handled by Keeper is only accessible by the end user.
- Using two-factor authentication adds an extra layer of protection, and this can be enforced for specific roles within the organisation.
- Keeper AD Bridge enables organisations using Microsoft Active Directory to integrate Keeper password management software with existing enterprise IT infrastructure.
- Keeper is not a fully fledged privileged access management (PAM) solution, but it provides advanced event reporting, logging, and auditing capabilities that integrate with leading security information and event management products.

Why put Keeper Enterprise on your radar?

[redacted]

Highlights

[redacted]

Enterprise password management provisioning and user onboarding

[redacted]

[redacted]

Encouraging good password management behaviours

[redacted]

Background

Keeper Security is a privately held company. It was co-founded in 2011 by CEO Darren Guccione and CTO Craig Lurey who were partners at Apollo Solutions, a software company for the computer reseller industry which was acquired by CNET in 2000, and at JiWire (now Ninth Decimal), a creator of WiFi technology applications and hotspot advertising software.

Current position

[redacted]

Datasheet

Keeper Enterprise by Keeper Security

Product name	Keeper Enterprise	**Product classification**	Password management
Version number	April 2019	**Release date**	2016
Industries covered	All	**Geographies covered**	All
Relevant company sizes	All	**Licensing options**	Annual recurring subscription; per seat.
URL	www.keepersecurity.com	**Routes to market**	Direct and channel partner sales
Company headquarters	Chicago, IL, US	**Number of employees**	> 100

LastPass Enterprise

Product summary

[redacted]

Key messages

- LastPass encourages best practice and eliminates bad habits.
- With the help of autofill, a password generator, and a security challenge, users are encouraged to improve their password security.
- LastPass balances convenience with security by managing the use of shared logins, and policies enable admins to configure the system to meet specific needs.
- A cloud-based solution, LastPass Enterprise leans more toward web logins and business users than IT infrastructure logins and IT departments.

Why put LastPass Enterprise on your radar?

[redacted]

Highlights

[redacted]

[redacted]

[redacted]

Policies, audits, and reports protect vulnerable IT entry points

[redacted]

[redacted]

[redacted]

[redacted]

Encouraging employees to make good security decisions

[redacted]

Background

Founded in 2003, LogMeIn provides unified communications and collaboration, identity, and access management, and customer engagement and support solutions. The company is headquartered in Boston, Massachusetts, with additional locations in North America, South America, Europe, Asia, and Australia. LogMeIn acquired LastPass (founded in 2008) in 2015. The company generated revenues of $1.2bn in the fiscal year ending December 31, 2018.

Current position

[redacted]

[redacted]

Datasheet

LastPass Enterprise by LogMeIn

Product name	LastPass Enterprise	**Product classification**	Password management
Version number	April 2019	**Release date**	2010
Industries covered	All	**Geographies covered**	All
Relevant company sizes	All	**Licensing options**	Per user/per month; site licensing
URL	www.lastpass.com	**Routes to market**	Direct
Company headquarters	Boston, MA, US	**Number of employees**	>2,500

ManageEngine Password Manager Pro

Product summary

[redacted]

Key messages

- ManageEngine Password Manager Pro provides a centralised password vault for a variety of IT-managed, password policy-controlled, resources, and personal logins.
- Password Manager Pro can automatically discover IT resources and help secure all privileged logins, randomising passwords after that at set intervals.
- Password Manager Pro's dashboard provides administrators with the real-time password-related information they need to keep the business safe and secure.
- Integration with third-party data breach monitoring services would provide additional benefit to enterprises and help employees better protect their passwords.

Why put Password Manager Pro on your radar?

[redacted]

Highlights

[redacted]

Comprehensive enterprise password management

[redacted]

[redacted]

[redacted]

Securing enterprise endpoints, resources, and sessions

[redacted]

[redacted]

[redacted]

[redacted]

Background

Launched in 2002, ManageEngine is now the IT management division of Zoho, an Indian company founded in 1996. Zoho is headquartered in Pleasanton, California, with offices in North America, Europe, and Asia. ManageEngine offers a broad range of products and solutions to meet the needs of enterprise IT teams and managed service providers.

Current position

[redacted]

Datasheet

ManageEngine Password Manager Pro by Zoho Corporation

Product name	ManageEngine Password Manager Pro	**Product classification**	Privileged access management; password management
Version number	10.0	**Release date**	April 2007
Industries covered	All	**Geographies covered**	All
Relevant company sizes	Enterprise	**Licensing options**	Annual subscription or perpetual license
URL	www.manageengine.com	**Routes to market**	Direct to the customer and via channel
Company headquarters	Pleasanton, CA, US; Chennai, Tamil Nadu, India	**Number of employees**	~ 7,000

Passbolt

Product summary

[redacted]

Key messages

- Passbolt is an open source password manager designed primarily for teams. The product can be integrated with mail and other tools using the product API.
- Built around OpenPGP, Passbolt adds an extra layer of security to password management. This can be used for other public/private key encryption purposes.
- Passbolt is an open source product distributed under AGPL. It can be hosted on premises for the management of passwords and logins used across the organisation.
- Several features, including mobile apps, folders, secure files and notes, access control lists (ACLs), and external password sharing are scheduled for release in 2019.

Why put Passbolt on your radar?

[redacted]

[redacted]

Highlights

[redacted]

Passbolt is easy to configure and easy to use

[redacted]

[redacted]

Keeping passwords secure by preventing phishing attacks

[redacted]

Flexible hosting options to control all business passwords

[redacted]

[redacted]

Background

Founded in 2016 by Kevin Muller, Cédric Alfonsi, and Rémy Bertot, Passbolt is a private company based in Luxembourg. Passbolt is part of the Luxembourg national startup incubator program and is financially supported by the Digital Tech Fund led by Expon Capital, as well as the Luxembourg government. The company has received VC funding totalling €632,000.

Current position

[redacted]

Datasheet

Passbolt

Product name	Passbolt	**Product classification**	Password manager
Version number	April 2019	**Release date**	March 2016
Industries covered	All	**Geographies covered**	Localised in English
Relevant company sizes	All	**Licensing options**	Subscription service
URL	www.passbolt.com	**Routes to market**	Online and direct sales
Company headquarters	Luxembourg	**Number of employees**	<10

Passwork

Product summary

[redacted]

Key messages

- Passwork is a password manager for teams. Available as a cloud service or on-premises product, Passwork is evolving rapidly to become a viable business solution.
- Passwork is a browser-centric product that uses the “vault” metaphor to manage and share passwords securely. Every user can create (and share) multiple vaults.
- Passwork presents a folder-based, easy to navigate, drag-and-drop user interface, and a security dashboard provides users with an analysis of their passwords.
- The Passwork Auto Logon browser extension helps users to log in to websites, but it doesn’t yet capture new login credentials. Mobile apps are still in their early stages.

Why put Passwork on your radar?

[redacted]

Highlights

[redacted]

Trust is an essential part of keeping passwords safe and secure

[redacted]

Flawless password sharing within a business environment

[redacted]

Background

Passwork (Passwork Oy) was Founded in 2014 and is based in Helsinki, Finland. Passwork is part of Aii Corporation, a business incubator and private investment firm with offices in Finland, Russia, US, and Canada.

Current position

[redacted]

Datasheet

Passwork

Product name	Passwork	**Product classification**	Password management
Version number	April 2019	**Release date**	2015
Industries covered	All	**Geographies covered**	Localised in English, German, and Russian
Relevant company sizes	Small and midsize companies	**Licensing options**	SaaS and perpetual licensing
URL	www.passwork.me	**Routes to market**	Direct and via affiliates
Company headquarters	Helsinki, Finland	**Number of employees**	<25

Pleasant Password Server

Product summary

[redacted]

Key messages

- Pleasant Password Server adds business and enterprise features to the popular KeePass open source password manager used by millions of individuals worldwide.
- Organisations can quickly and easily install the Windows-based Pleasant Password Server in a location of their choice (datacenter, private cloud, or public cloud).
- Pleasant Password Server can be enhanced using Pleasant Universal SSO, an add-on module that eliminates the need for direct access to account passwords.
- Users already familiar with KeePass can easily switch to Pleasant Password Server. Users familiar with other password managers may expect a browser extension.

Why put Pleasant Password Server on your radar?

[redacted]

Highlights

[redacted]

Balancing business security and user convenience

[redacted]

Reducing system administration overheads

[redacted]

[redacted]

[redacted]

[redacted]

Logging and reporting features are mandatory

[redacted]

Background

Pleasant Solutions is a software development company headquartered in Edmonton, Canada, with satellite offices throughout North America. Pleasant Solutions is a privately held company Founded in 2007. Its CEO is Thomas Stachura. The company has two subsidiaries: BridgeGateData, a provider of verification and identity middleware to telcos, and Trusted Health Services, a provider of secure file management services to the health sector.

Current position

[redacted]

[redacted]

Datasheet

Pleasant Password Server by Pleasant Solutions

Product name	Pleasant Password Server	**Product classification**	Password management
Version number	v7.9.21 (May 2019)	**Release date**	2012
Industries covered	All	**Geographies covered**	North America, Europe, Oceana
Relevant company sizes	Companies of all sizes.	**Licensing options**	Perpetual license, per seat
URL	www.pleasantsolutions.com	**Routes to market**	Direct and via resellers
Company headquarters	Edmonton, Alberta, Canada	**Number of employees**	75+

RoboForm for Business

Product summary

[redacted]

Key messages

- RoboForm for Business is a password management solution that helps mitigate cybersecurity threats while increasing the productivity of employees and teams.
- RoboForm eliminates weak, reused, forgotten, and vulnerable passwords. It can also reduce the costs associated with password resets and user downtime.
- RoboForm enforces password policies and provides managers with oversight of employee password security. Active Directory integration speeds up product rollout.
- Product terminology may complicate features for some users. Browser extensions and mobile apps provide good functionally. Desktop apps are useful for power users.

Why put RoboForm for Business on your radar?

[redacted]

Highlights

[redacted]

Employee onboarding, policy configuration, and reporting

[redacted]

[redacted]

[redacted]

Browser extensions, desktop applications, and mobile apps

[redacted]

[redacted]

[redacted]

Boosting business productivity with secure sharing

[redacted]

[redacted]

[redacted]

Background

Siber Systems is a privately held company headquartered in Fairfax, Virginia. Founded in 1995, Siber Systems released RoboForm, its first consumer product, in 2000. Customers range from individual users and small businesses to government agencies and Fortune 500 companies. The company also offers a file backup, sync, and share product called GoodSync.

Current position

[redacted]

Datasheet

RoboForm for Business by Siber Systems

Product name	RoboForm for Business	**Product classification**	Password management
Version number	RoboForm v8,5,8	**Release date**	2009
Industries covered	All	**Geographies covered**	All
Relevant company sizes	All	**Licensing options**	Pay-as-you-go; per user, per year
URL	www.roboform.com	**Routes to market**	Direct and resellers
Company headquarters	Fairfax, VA, US	**Number of employees**	<100

TeamPassword

Product summary

[redacted]

Key messages

- TeamPassword is particularly suited to digital agencies and teams that need access to shared login credentials to access communal services and single-user websites.
- Logins with long, complex passwords can be easily managed using TeamPassword groups, enabling one-click sharing with colleagues and teams.
- An activity log shows admins when logins are accessed, added, edited, or removed. Reports highlighting exposed, reused, or weak passwords would be useful.
- Users can log into TeamPassword using a linked Google identity via Google Sign-In. Two-step verification using an authenticator app adds an extra layer of protection.

Why put TeamPassword on your radar?

[redacted]

Highlights

[redacted]

Introducing order to chaos

[redacted]

Encouraging cybersecurity best practice with complex passwords

[redacted]

Background

Initially released in 2012, TeamPassword started life as an alternative to LastPass (a password manager designed initially for individuals) for digital agencies. TeamPassword was acquired in 2018 by Jungle Disk, a provider of cybersecurity solutions for small businesses. Jungle Disk has been in business since 2006 (acquired by Rackspace in 2008) when it created one of the first products to leverage Amazon's S3 storage service. The team moved to San Antonio, Texas, in 2010, before assuming its current form as an independent company in 2016.

Current position

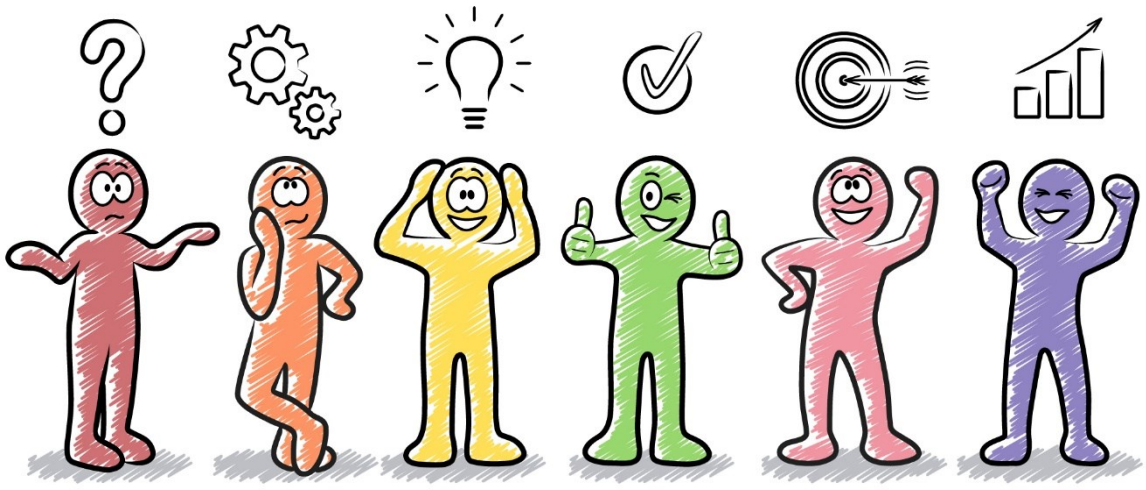
[redacted]

[redacted]

Datasheet

TeamPassword by Jungle Disk

Product name	TeamPassword	Product classification	Password management
Version number	April 2019	Release date	October 2012
Industries covered	Well suited to digital agencies	Geographies covered	Service available globally in English
Relevant company sizes	Small business	Licensing options	Tier-based pricing based on the number of users.
URL	www.jungledisk.com	Routes to market	Direct to customer and G Suite Marketplace.
Company headquarters	San Antonio, TX, US	Number of employees	<50



R N E 2 4 7 . C O M