Ovum Market Radar: Password Management Tools

Improving cybersecurity by eliminating weak, reused, and compromised passwords

Publication Date: 17 Aug 2019 | Product code: INT005-000010KEEPER

Richard Edwards

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 the ways in which passwords and account credentials are used and managed, we can easily see weaknesses in our cybersecurity defenses.

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.

Ovum view

Key findings from an Ovum survey of IT decision-makers and enterprise employees reveals that password management practices are out of date, overly reliant on manual processes, and highly dependent on employees "doing the right thing".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. Credentials and passcodes are required for desktop applications, mobile apps, IT infrastructure, physical access, and more.
- 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 key 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 login again if you can help it.
- Organizations deploying Windows 10 can use Windows Hello to increase login convenience with biometrics, and replace passwords with multifactor authentication.
- While far from ideal, the sharing of logins, account details, and passwords is done for IT and business operational reasons.
- When considering software-as-a-service (SaaS) and cloud-based products, businesses and institutions should look for relevant vendor certifications, accreditations, and reporting standards.
- Organizations must consider password management in terms of security controls covering people and processes, as well as technology.

Recommendations

Recommendations for enterprises

Adopting any trusted password manager is almost always going to be better than not adopting one at all. Ovum research reveals that over 80% of major data breaches can be traced back to a single compromised identity, so password management needs to be top of the cybersecurity agenda. Evaluate products originating in the consumer market and consider the benefits of offering password management tools to employees to extend for personal use. It could make practical sense to deploy more than one product in larger organizations.

Automating the password change process requires action from application and website property owners, so consider if there's anything you can do to help customers, citizens, and partners better manage their passwords.

If moving business and productivity workloads to the cloud, add strong authentication to enhance the security of employee user IDs and passwords. Password managers present an obvious target for hackers and cybercriminals, so consider which multifactor authentication mechanisms are likely to work best for staff and employees.

Security should be at the heart of any modern digital workplace strategy, so password management tools need to be considered alongside device, operating system, browser, and application management strategies. Microsoft and Google are introducing customers to their password-less strategies, so IT and security teams should consider the relevance of these initiatives as part of any password management-related project.

Do employees use their own equipment to access business applications and data? Do employees access personal websites and services using their business-issued smartphones and computers? If the answer to either question is yes, think carefully about password segregation. If employees use their browsers to remember logins and passwords, consider how many of these are likely to be for work and how many would be considered private. Each should be managed differently.

Recommendations for vendors

When considering SaaS and cloud-based solutions, enterprises look for vendors they can trust. Consider relevant certifications, accreditations, and reporting standards, such as SOC 2 for trust, ISO 27001 for information security management, ISO 22301 for business continuity, PCI DSS for payment security, and ISO 27018 for protection of personally identifiable information.

The FIDO Alliance is an important industry association from the perspective of password management, so consider how best to support and promote a password-less future while addressing the immediate needs of the market. An organization must consider password management in terms of security controls covering people and processes, as well as technology.

Many enterprises are moving business and productivity workloads to the cloud, so it's a time of great upheaval for IT and security teams. This means that new business will flow to vendors that can provide customers with a smooth deployment and ongoing service experience. This is where channel partners play an important role. Vendors should consider their route to market carefully. Self-service will adequately facilitate proof-of-concept and pilot projects, but complexity will rear its head sooner or later and services will be required. Be ready.

Scoping the password management tools 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 cyberattacks. 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 products 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 major data breaches traced back to a single compromised identity, it's hard to imagine any well-informed CFO balking 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. And if your organization has an outward-facing website, consider ways in which it could be 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 to those of administration and customer service staff. And different computing platforms (desktop, mobile, terminal, kiosk) also require consideration.

Password management tools tend to be associated with web browsers, websites, and the management of online credentials. However, passwords and passcodes are often required for traditional line-of-business applications and bespoke IT systems. And then there are terminal-based logins, such as Windows RDP, SSH, and Telnet sessions. If you work for an established organization or large enterprise, you're likely to have a diverse computing environment. This needs to be reflected in the capabilities of the password management solution and its usefulness across the organization.

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 secure shared credentials.

Organizations 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 is 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. And if something is missing, the APIs and command line interfaces offered by some of the products assessed in this report provide IT, developers, and system integrators with opportunities to fill the feature gap.

Tools that dictate processes versus tools that support processes

There's a saying: "Man shapes the tool; thereafter the tool shapes man." We've seen this happen repeatedly, 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 isn't always a negative thing (best practices and industry standards often develop this way), but it's important to recognize 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 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 and center ground of course, but larger organizations may find that implementing two or three different password management products is an easier 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 in a more secure and productive way. Desktop apps, mobile apps, and browser extensions help users shoulder the cognitive burden that is associated with the modern digital workplace. In their simplest form, password managers can be used to remember web login credentials and passwords. But 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 standardized language or approach either. This could be a recipe for confusion, especially if employees have been using their own favored solution, so it's worth canvasing 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, very visible 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 behavior.

Minimize deployment and administration overhead

As with all software purchases, organizations must do their own due diligence when selecting a password management tool. However, adopting any trusted password manager is almost always going to be better than not adopting one at all. Each day that goes by without some form of business oversight relating to the passwords used by employees presents a significant risk to the business.

Personal password management tools are becoming mainstream consumer products, so thought should be given to business- and job-related password import options from these offerings. Some products presented in this Market Radar enable side-by-side use of personal and business accounts, while others require organizations to consider if managing personal passwords is something they want to do at all. Workplace privacy and data protection legislation are hot topics, so consider the ways in which passwords can be segregated in situations where corporate devices are authorized for personal use.

Account creation, user onboarding, and software deployment are key considerations for any enterprise-wide initiative, and the last couple of years has seen plenty of progress in this area as vendors upscale their offerings to address enterprise requirements. This has resulted in some cloud-only products offering on-premises components to enable Active Directory integration while extending support for cloud-based directory services, SAML 2.0 authentication and authorization, and System for Cross-domain Identity Management (SCIM).

Trust is the central tenet of any password management product, which means using a combination of cryptography standards, approaches, and techniques. Vendors generally do a good job of hiding this complexity in their products, but it invariably comes to the surface during the onboarding process when users are asked to create passwords and passphrases before they can use the password management tool. This can be circumvented to some degree when the solution is integrated with enterprise authentication systems, but this can then inhibit the privacy aspects that were discussed earlier, because a secure password "vault" requires its own private digital key.

Reduce the user-visible password surface area

The general advice from security experts is to eliminate passwords wherever possible. So, if users already login to a Windows PC, don't ask them to login again if you can help it. Companies such as

Microsoft and Google are developing password-less environments for the enterprise, and it’s good to see that these are already being embraced by password management tool vendors.

Organizations deploying Windows 10 PCs can use Windows Hello for Business to increase login convenience with biometrics and replace passwords with strong multifactor authentication (MFA). Microsoft Authenticator (and Google Authenticator) enable users to authenticate with a mobile device, receiving a push notification to verify their identity with a biometric or PIN. And using security keys, such as those from Yubico, replaces passwords using MFA. As password management products are examined, consider how these elements are supported and integrated as part of the solution.

Using two-factor (or multifactor) authentication and security keys to access a password management system undoubtedly strengthens the overall security of the solution, but it can present a barrier to user adoption if it is not done well. Again, staff education and training are essential for successful implementation. This aspect of password manager capability generally requires organizations to adopt modern operating systems, modern devices, and modern web browsers, so making it part of any desktop refresh program or operating system upgrade initiative makes good sense.

Monitor, audit, and review password-related threats and issues

Password managers promise to improve the security posture of organizations 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/or 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.

While not ideal, the sharing of logins, account details, and passwords 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. However, most products address key requirements (who, what, where, and when), particularly where administrator actions are concerned. Products offering PAM capabilities tend to offer more reporting and auditing capabilities and integrate with security information and event management (SIEM) tools.

Do your due diligence

Organizations adopting password management products need to do their due diligence, especially if operating in regulated industries or where strict security protocols are in place. It’s the customer, not the vendor, that has responsibility for ensuring it is complying with any applicable laws and regulations. When considering SaaS and cloud-based solutions, businesses and institutions should look for relevant vendor certifications, accreditations, and reporting standards, such as SOC 2 for trust, ISO 27001 for information security management, ISO 22301 for business continuity, PCI DSS for payment security, and ISO 27018 for protection of personally identifiable information.

On-premises password management products have been around for well over a decade and represent some of the most mature products in this segment of the software market. They're generally easy to install and quick to configure, but additional ongoing effort is required to protect these systems from targeted attacks and system vulnerabilities by securing and hardening the server environment.

Organizations are understandably wary of "black box" IT solutions, especially when relating to information security management, so it's worth considering the merits and transparency of open source products/projects. Proprietary or open source, IT security teams should reference cybersecurity and infrastructure security resources (e.g. www.us-cert.gov, nvd.nist.gov, www.kb.cert.org) to understand the nature of vulnerabilities that affect passwords more generally.

Enterprise software vendors are more likely to share security reviews and software audits (usually under NDA) with partners and customers, but IT professionals will also consider how operating system and browser vulnerabilities might impact the use of password managers.

Vendor go-to-market strategy

The products profiled in this Market Radar present a broad snapshot of the password management tools marketplace. There are on-premises offerings from well-established enterprise IT product vendors, cloud-based services from "consumer-first" product companies, and new open source solutions from small startups.

The way in which these vendors take their products to market also differs. Enterprises that are comfortable with SaaS can confidently explore what the cloud-based password management market has to offer. Likewise, organizations requiring, or favoring, on-premises products also have plenty of choice. Multi-year licensing deals are offered by some vendors, and perpetual licenses are available from others. Organizations requiring a "managed account" can have this need met, and firms looking for bespoke capabilities also have options.

Professional services are available from some of the larger vendors, but there is plenty of opportunity for cybersecurity consultancies to participate in the market. If your organization is serious about password management, thought should be given to the password-less initiatives being driven by the likes of Google and Microsoft, and how these fit with vendor product roadmaps.

The FIDO Alliance is an influential industry association from the perspective of the world's over-reliance on passwords, and it is worth noting that Dashlane, Keeper Security, and LastPass (LogMeIn) are associate-level members. The FIDO Alliance is working to change the nature of authentication with open standards that are more secure than passwords, simpler for consumers to use, and easier for service providers to deploy and manage.

Market landscape and participants

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 two main approaches. The first of these is the centralized 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.

Key trends in the password management market

There’s no shortage of password management products for the individual, with more than 70 apps available in this category in the Google Play Store. Of the vendors presented in this Market Radar, Keeper Security wins the popular vote with more than 10 million downloads of Keeper Password Manager & Security Vault. LastPass Password Manger comes next with more than 5 million installs, followed by 1Password and Dashlane with about 1 million installs each. However, it’s worth noting that Bitwarden has the highest rating on the Google Play Store.

We’ve already said that password managers have been around for well over a decade, but the enterprise solutions market started to take shape in 2017 and 2018. Developments in browser extension technology, password authenticators, security keys, and other forms of two-factor and multifactor authentication have boosted interest and action.

Cisco’s 2018 acquisition of Duo Security, a provider of multifactor authentication delivered through the cloud, provided another piece of the jigsaw puzzle. Google’s entry to the security key market around the same time drew more attention to the subject of password management and strong authentication.

Acquisitions in the password management market have been surprisingly few. LastPass was acquired by LogMeIn in 2015 for $10m, and Jungle Disc acquired TeamPassword in 2018. Dashlane acquired passOmatic in 2014 and LastPass acquired Xmarks way back in 2010. Of the 12 vendors featured in this Market Radar, 11 are private companies and only one of them can be said to be headquartered in Silicon Valley. Canada is home to three of the products assessed, and two are based in the EU.

Future market development

A password-less future is still some way off, so vendors participating in the password management tools market have a significant window of opportunity. Password management products don’t command a high price, but everyone who uses a computer or mobile device probably needs the kind of functionality on offer. This means it’s a volume game, and with well over 1 billion seats up for grabs, the market could be worth well over $30bn by 2020. That said, companies such as Amazon, Apple, and Google may enter the market in a grab for closer consumer ties, while Microsoft could offer a product to consumers and businesses as part of Office 365.

From an enterprise perspective, password management sits between two key identity and access management software categories: SSO and PAM. Vendors participating in these markets might find additional value in the broader password management market. Conversely, there’s also an opportunity for business to flow in the opposite direction, especially among small and midsize businesses.

As is evident in the consumer market, password management sits comfortably alongside computer security and management software. This is a domain familiar to ManageEngine. Password management can also be a key element of collaboration, which is a market that LogMeIn knows something about. Other adjacent markets include web browsers, secure communications (Dashlane already offers a secure VPN service to individuals), and digital workplace services. Vendors such as VMware will almost certainly be watching this market closely.

Vendor landscape

The password management tools landscape consists of startups, established enterprise vendors, and companies that are extending their products to address consumer and business requirements. LastPass Enterprise and ManageEngine Password Manager Pro are developed by larger enterprise vendors that have a broad portfolio of products and solutions. The remaining vendors presented in this Market Radar have between 10 and 150 employees.

Geographically, the vendors presented in this report tend to be headquartered in North America, although only one vendor (LastPass, a private subsidiary of LogMeIn) is located in the Bay Area.

Revenue figures for the password management market can only be estimated, because most of the vendors examined in this report are private companies. Estimated revenue figures obtained from Owler, the community-based competitive insights platform, suggest that 1Password, Dashlane, Keeper Security, LastPass, and Siber Systems shared annual revenue of approximately $90m in 2018.

Figure 1, the Ovum Market Radar for Password Management tools, illustrates the relative strengths and weaknesses of 12 competing offerings. All products selected for this report offer good deployment and administration capabilities, so there’s no reason for not deploying a suitable product.

No single vendor stands out head and shoulders above the rest. However, the leading products are: 1Password Business, Dashlane Business, Keeper Enterprise, LastPass Enterprise, ManageEngine Password Manager Pro, Pleasant Password Server, and RoboForm for Business.

Figure 1: Ovum Market Radar for Password Management Tools

	1Password Business	Bitwarden	Bluink Enterprise	Dashlane Business	Keeper Enterprise	LastPass Enterprise	ManageEngine Password Manager Pro	Passbolt	Passwork	Pleasant Password Server	RoboForm for Business	TeamPassword
Password management capabilities	🟦	🟪	🟪	🟦	🟦	🟦	🟦	🟪	🟪	🟦	🟦	🟥
Range of business and workstyle fit	🟪	🟪	🟪	🟪	🟪	🟪	🟦	🟪	🟪	🟦	🟦	🟥
Ease of use for employees and staff	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟦	🟦	🟪	🟦	🟪
Deployment and administration	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪
Identity and authentication integration	🟦	🟪	🟦	🟦	🟦	🟦	🟦	🟪	🟪	🟦	🟪	🟥
Monitoring, auditing, and reporting	🟪	🟪	🟥	🟪	🟦	🟪	🟦	🟥	🟪	🟦	🟪	🟥
Product maturity and market adoption	🟦	🟪	🟥	🟦	🟦	🟦	🟦	🟥	🟥	🟦	🟦	🟥
Vendor go-to-market strategy	🟦	🟥	🟥	🟦	🟦	🟦	🟪	🟥	🟥	🟪	🟪	🟥
Categorization	**LEADER**	**CHALLENGER**	**CHALLENGER**	**LEADER**	**LEADER**	**LEADER**	**LEADER**	**CHALLENGER**	**CHALLENGER**	**LEADER**	**LEADER**	**CHALLENGER**

🟦 Very good
🟪 Good
🟥 Fair

Source: Ovum

The open source products from Bitwarden and Passbolt both show strong potential and demonstrate what can be accomplished by small teams. Bluink deserves a mention for its mobile-first approach to password management, especially the geofencing capabilities of Bluink Enterprise. And finally, kudos to Passwork and TeamPassword for developing easy-to-use password management solutions that address the specific needs of startups and digital marketing agencies.

Keeper Enterprise

Ovum view

Keeper Security's password management and cybersecurity offerings can boost the digital defenses of individuals, families, businesses, and enterprises. The password management market has plenty of headroom for today's competing vendors, but Keeper Security is investing in new security add-ons that enhance and distinguish its products. Keeper has become a well-established cybersecurity platform that encompasses password security and management, secure file storage, encrypted messaging, advanced reporting, and dark web monitoring with BreachWatch.

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 organization.
- Using Keeper AD Bridge and Keeper SSO Connect, organizations can more easily provision and authenticate employees using existing enterprise IT infrastructure.
- Keeper is not a full-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?

Keeper was designed to scale for any sized business. Features such as role-based permissions, team sharing, departmental auditing, and delegated administration support business growth and digital transformation initiatives. Keeper Security is a zero-knowledge security provider, which means that only the user can encrypt/decrypt data.

The company has several OEM relationships and partnerships with security technology providers including RSA, Duo, and Yubico. It also collaborates with a range of channel partners, bringing password management and digital vault capabilities to global businesses of all sizes in all industries.

Highlights

Because Keeper Enterprise is a zero-knowledge password management solution, all encryption and decryption processes take place on the user's computer or mobile device. In-transit data is encrypted using transport layer security (TLS) and data at rest is encrypted using AES-256. The plain text version of the data is never available to Keeper Security employees or any third party. This means that if Keeper were to be hacked, attackers could only access the worthless ciphertext.

Enterprise password management provisioning and user onboarding

The best way to evaluate Keeper Enterprise is via a 14-day trial account. This enables users to explore the product's features and functions. The web-based Admin Keeper Console is uncluttered and well laid out, and it offers some thoughtful touches, such as ready access to well-structured documentation and the ability to schedule a 30-minute demo.

User provisioning is an important aspect of any enterprise offering and tends to set the mood of those evaluating a new product. Keeper Enterprise offers five different provisioning methods: Active Directory or LDAP Sync, single sign-on (SAML 2.0), SCIM (System for Cross-Domain Identity Management), email auto-provisioning, and command line provisioning. Each organizational node can use a different provisioning mechanism if required.

Organizations using Active Directory need to deploy Keeper Bridge software on premises. Organizations using SAML 2.0 are required to deploy Keeper SSO Connect either on-premises or on the cloud. SCIM automatically provisions users and teams through Azure Active Directory, Okta, and G Suite via an SCIM connection.

For user onboarding, administrators can use the Keeper web-based admin console to send custom email invitations to new users, directing them to activate their Keeper account. Installing the Keeper Browser Extension is usually the first action the user needs to do. Users will be asked to provide a master password or, more likely, use an enterprise SSO login which negates the need for such.

Using two-factor authentication adds an extra layer of protection. This can be enforced for specific roles within the organization, such as IT admins. 2FA methods include SMS, Google, and Microsoft Authenticator, Apple Watch or Android Wear, RSA SecurID, and Duo Security.

Keeper works on smartphones, tablets, and computers, and supports Chrome, Safari, Firefox, Edge, Opera, and IE browsers. Native app installation is available from the Keeper website and iTunes, Google Play, and Microsoft Store. The Keeper web vault and browser extension will be enough for most users, but the desktop apps (Windows, macOS, Linux) have extra capabilities, such as being able to autofill native apps, import existing passwords, and provide offline access.

Encouraging good password management behaviors

Keeper Enterprise provides users with a personal security audit, highlighting password strength and the date last changed (based on first use with Keeper). And with BreachWatch, leaked and breached passwords are also flagged. Administrators are presented with an overall Security Audit Score for the organization. This is further broken down by password strength, unique passwords, master password strength, and two-factor authentication use. A detailed report by user can be exported if required.

With password sharing, Keeper Enterprise balances security and convenience. Under the hood, each user has a 2048-bit RSA key pair that is used for sharing password records. Shared information is encrypted with the recipient's public key. Passwords and logins or other records (files and photos as Keeper calls them) can be shared by users quickly and securely. An invite is sent to other Keeper users and they confirm their acceptance. All parties receive visible notifications. This should prevent users from reverting to the use of email and other insecure channels. The ability to share files offers an interesting alternative to tools such as Dropbox.

If a set of passwords needs to be shared for business purposes, such as by a team of marketers or a group of social media professionals at a digital agency, a shared folder containing the relevant logins/passwords is a more effective mechanism. Shared folders can contain nested folders to help organize and structure information.

Sharing beyond the enterprise domain is supported. Keeper sends an email invitation to join Keeper (using a free account). If the external user already has a Keeper account, they will receive a visible alert via their vault. Changes made to shared folders appear almost immediately. This is another important factor to consider when evaluating password management products, because impatient users will quickly fall back to less secure methods if the tool is preventing them from getting work done.

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

Keeper Security has built a compelling password manager for individuals, families, businesses, and enterprises. Keeper is a cloud-based product, so there will be concerns over security, privacy, and availability. While potential customers should perform their own due diligence, the company has a long list of certifications, including SOC2, ISO 27001, TRUSTe, and PCI DSS.

Keeper Enterprise is priced at $45 per user per year. Optional add-ons include Secure File Storage, KeeperChat, Advanced Reporting & Alerts Module (ARAM), and Dedicated Service and Support. The company offers a 14-day free business trial for up to 10 users. Several mobile operators preload Keeper on their subscribers’ mobile phones and tablets to protect against cybertheft. Keeper also works with leading OEMs to enhance device security and mobile productivity.

Data sheet

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

Source: Ovum

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. Although On the Radar vendors may not be ready for prime time, they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Further reading

Keeping the business safe and secure with better password management
Report ID: INT005-000008 (May 2019)

Author

Richard Edwards, Associate Analyst

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Whilst reasonable efforts have been made to ensure that the information and content of this product was correct as at the date of first publication, neither Informa Telecoms and Media Limited nor any person engaged or employed by Informa Telecoms and Media Limited accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard – readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

CONTACT US

ovum.informa.com

askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Boston
Chicago
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
Paris
San Francisco
Sao Paulo
Shanghai
Singapore
Sydney
Tokyo