Best Practices: Selecting, Deploying, And Managing Enterprise Password Managers

Solutions Reduce The Risk Of Breaches From Compromised Credentials

by Merritt Maxim and Andras Cser

January 8, 2018

Why Read This Report

Despite the known risks, passwords remain the most common method of user authentication. The increased number of apps employees need for their jobs, coupled with the effort required to migrate to new authentication technologies, means that security pros need to plan for password coexistence. EPMs help manage passwords until the security team is ready to replace them. This report offers practical EPM guidance and recommendations security pros can use to keep password costs and risks in check while maximizing employee productivity.

Key Takeaways

Despite Frequent Data Breaches, Many Users Still Practice Poor Password Hygiene

While security teams have invested time and resources building strong password policies and security awareness training, the real-world results are disappointing as users continue to select weak passwords that increase the risk of breaches.

Centralized Password Management Helps Mitigate Security Risks

The continued parade of high-profile consumer data breaches, many of which involve compromised user credentials, has served to highlight password-related risks. Stricter enterprise requirements relating to regulatory compliance, auditability, and minimization of risk are all driving the need for deploying EPM solutions.

EPM Solutions Can Help Manage Password Costs And Realize Compelling ROI

Passwords incur direct costs, such as service desk staffing, and indirect costs, such as impacts to employee productivity. Security pros can justify investment in EPM solutions by demonstrating how they alleviate these password costs. Furthermore, EPM solutions deliver additional benefits beyond cost savings in the form of consistent policies and risk reduction.

Best Practices: Selecting, Deploying, And Managing Enterprise Password Managers

Solutions Reduce The Risk Of Breaches From Compromised Credentials

by Merritt Maxim and Andras Cser
with Stephanie Balaouras, Salvatore Schiano, Madeline Cyr, and Peggy Dostie

January 8, 2018

Table Of Contents

Related Research Documents

Forrester's IAM Maturity Assessment

The Future Of Identity And Access Management

Understand The State Of Identity And Access Management: 2017 To 2018

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

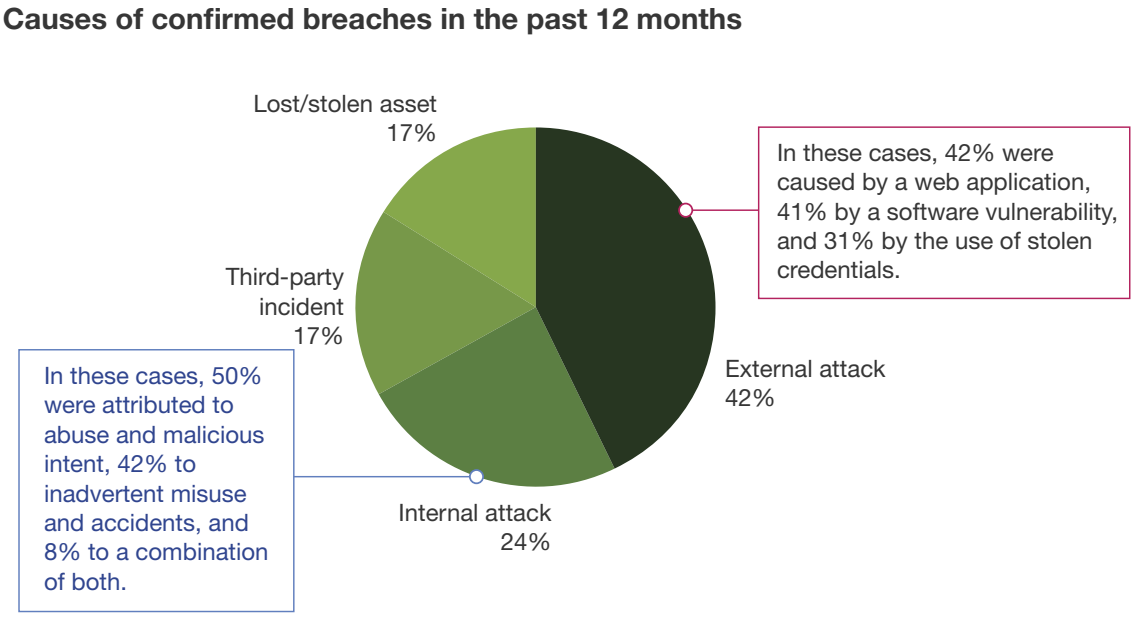
Password Risks Are High, And So Are The Costs

According to our Forrester Data Global Business Technographics® Security Survey, 2017 of enterprise organizations that have suffered at least one data breach attributed to an external attack, cybercriminals used stolen user credentials to carry out 31% of the attacks (see Figure 1). Today's employees must interact with a wide range of systems and applications. While technologies such as two-factor authentication (2FA), web single sign-on (SSO), and privileged identity management are helping to reduce reliance on static, easy-to-hack passwords, security teams still require passwords and use them to authenticate employees into a range of commercial and custom applications. Consequently, security professionals must still manage and deal with password-related issues such as:

- **High support costs.** The support costs related to passwords (whether for employees or customers or both) can be quite significant for today's digital businesses. Forrester has spoken with several large US-based organizations in different verticals that allocate over $1 million annually just for password-related support costs (mostly in staffing and infrastructure expenses). And in most cases, these support costs continue to increase, despite concerted efforts to introduce automation and reset tools to alleviate this password burden.
- **Increased security risks for legacy applications and systems.** While identity and access management (IAM) solutions such as SAML-based web SSO and identity management can alleviate the password burden and keep support costs in check, most organizations rely on a hybrid heterogeneous computing environment often composed of other legacy systems that may not support SAML. This forces security teams to continue to rely on password-based authentication for these systems, meaning that password-related risks are not removed completely. This is especially true for legacy (desktop, green screen, etc.) applications that play a crucial role in supporting business but are expensive to replace with more modern technology.
- **Increased risk of insider attacks.** Many security teams still rely on a shared spreadsheet or document to store and track passwords, especially for privileged accounts, even though this is not a recommended security best practice. This may appear to help keep administrator productivity high, but it is a major security risk. Malicious insiders can easily compromise such documents, and with no monitoring or governance of the shared files or the credentials themselves, the risk of a malicious or inadvertent data breach is significant. Consider that, according to our data surveying network security decision makers, 24% of breaches in the last 12 months were the result of an internal attack.[1]
- **Lost end user productivity.** While passwords can generate a significant administrative cost, they also have an indirect effect on employees' productivity. Every minute an employee spends unable to access a system because of a lockout is lost productivity. This issue can be even more critical for applications that support customer-facing initiatives. While the productivity costs can be harder to estimate, they cannot be overlooked. Forrester's workforce enablement research rests on the intuitive and proven premise that happy employees lead to happy customers, and happy customers drive financial performance.[2]

› **High compliance costs.** The ability to show to auditors how your firm handles passwords is especially complex for distributed passwords and processes. Providing audit information on a huge number of passwords sprawled out in individual spreadsheets on employees' desktops is a manual and costly process — and increases risks that not every system is tracked or managed, leading to potential data breaches.

FIGURE 1 Causes Of Breaches



Base: 1,525 confirmed breaches by 317 global network security decision makers whose enterprise firms (1,000 employees or more) have had a security breach in the past 12 months
Source: Forrester Data Global Business Technographics® Security Survey, 2017

Employee Behavior Exacerbates Password Risks

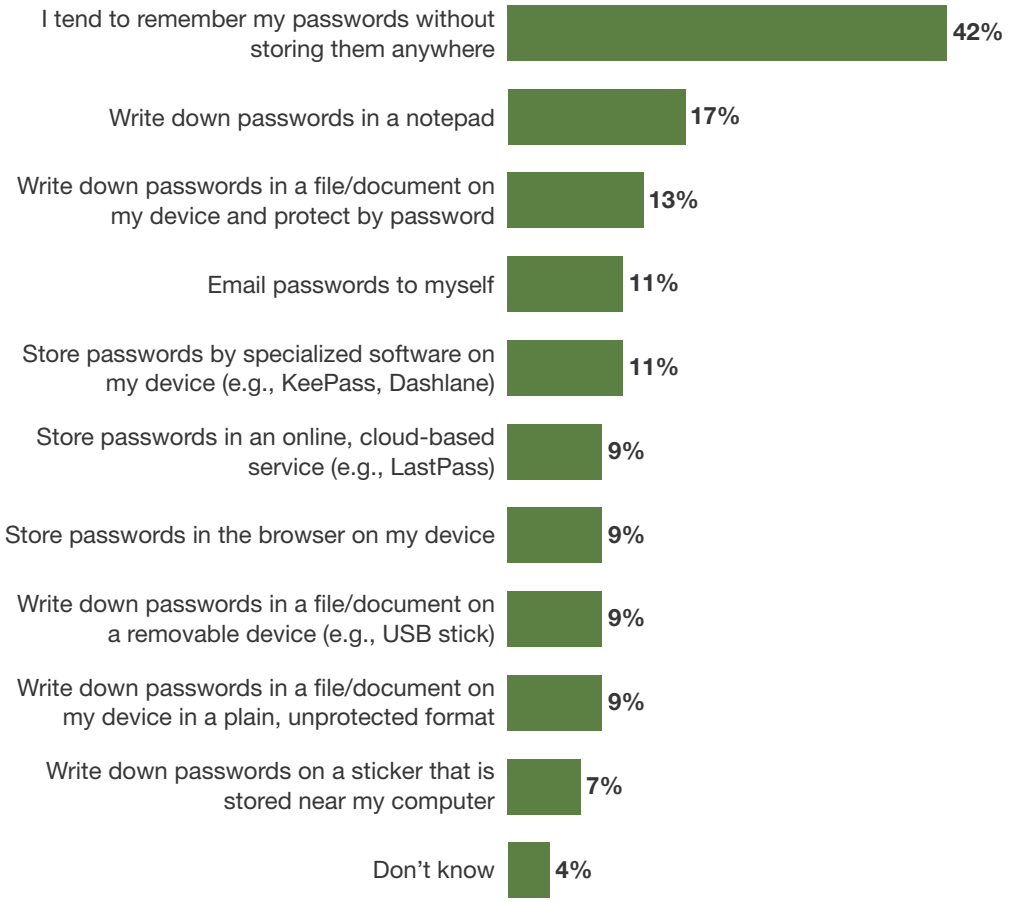
While there is consensus on the need to move away from passwords, a complete replacement of all passwords is still in the future for most firms. Unfortunately, hackers are aware of the persistence of passwords and continue to seek to gain access to systems to exfiltrate data by compromising password credentials. Tools such as rainbow tables and the existing trove of compromised user name and passwords provide vast resources that hackers can utilize to access websites fraudulently. How massive is this trove of stolen data? Well, in just the last 12 months, the Yahoo and Equifax breaches provided cybercriminals with 3 billion compromised consumer accounts. Unfortunately, the password problem appears to be getting worse because:

- **Users have more and more online accounts to manage.** By some estimates, the average adult possesses more than 25 active online accounts, and that number is growing.[3] Such a proliferation of accounts makes it very challenging for users to maintain strong password discipline. It invariably leads to weak password selection and weak password reuse across services, which only increases potential of data breaches since users often use the same user name/password combination across multiple sites.
- **Despite data breaches, users still generally practice poor password hygiene.** The frequency of large-scale data breaches has raised consumer awareness of the importance of online security, but such awareness has not always been accompanied by an equivalent change in behavior such as replacing weak passwords with stronger alternatives.[4] Many websites don't require periodic password changes, so users can be content to rely on weak passwords. Users' continued willingness to become victimized by phishing emails only further adds to the problem. According to survey data from global network security decision makers employed at enterprise firms (of 1,000 or more employees) that have had an external breach in the past 12 months, 18% of external attacks were carried out by phishing schemes.[5]
- **Users compound password issues with inadequate storage of weak passwords.** While selecting a weak password is bad, users often compound this problem by then keeping a list of passwords on a piece of paper or sticky note either on a desk or on a hard drive (see Figure 2). This means that successful password exploits don't even require digital expertise; merely looking at a user's desk may be sufficient for garnering intel about the user's online accounts.
- **SSO/IDaaS solutions may not always cover the entire hybrid application environment.** SSO and IDaaS solutions are compelling choices to alleviate password burden by enabling single sign-on into commercial applications via proven protocols such as SAML. However, organizations often have a mix of homegrown and custom applications that lack SAML support, forcing organizations to continue to rely on password-based authentication. We spoke with a global financial services provider currently deploying a commercial IDaaS solution that is planning to complement that with an enterprise password manager (EPM) solution to manage the password-based access to its many custom on-prem apps.
- **Sites often compromise password security in the name of user experience.**[6] While many B2C sites are aware of the problems posed by weak passwords, they often face internal resistance on requiring more stringent password policies out of concerns that such policies can impede the user experience, detract from brand loyalty, and negatively influence margins because of increased support for password-related issues. Faced with these tradeoffs, businesspeople often overrule their security counterparts and allow weaker passwords to remain. While this may help optimize user experience, it's done at the expense of security and increases potential risks of data breaches.
- **Mobile and bring-your-own-device (BYOD) scenarios add to password complexity.** In addition to users having to manage an increasing number of online accounts, users are no longer tethered to a desktop and a desktop browser. Users increasingly rely on mobile devices to interact with

different sites. And while the convenience of the mobile device is hard to overlook, complex password entry can be challenging on mobile devices, thereby forcing users to select weaker passwords. Furthermore, in BYOD scenarios, employees may be interacting directly with sensitive corporate data in the cloud via the mobile device, limiting the effectiveness of most organizations' existing perimeter-based security controls.

FIGURE 2 Password Management Methods

"Which of the following methods do you use to manage passwords on the device(s) that you use for work?"



Base: 3,540 global enterprise (of 1,000 or more employees) information workers
Note: Multiple responses were accepted.
Source: Forrester Data Global Business Technographics® Workforce Benchmark Recontact Survey, 2017

Enterprise Password Managers Help Securely Manage Password Chaos

While freeware and single-use password wallets have existed for many years, vendors designed these solutions for the web and mobile world and they don't lend themselves to enterprise deployments. EPM solutions have emerged in the last five years to help manage password-related risks and challenges for more-distributed enterprise environments. EPM solutions combine the familiar password wallet model with other administrative tools and multiple deployment models (desktop, mobile app, and web), to simplify deployment and ensure consistent password policy enforcement across a range of target systems, including on-premises, web, and SaaS applications. The result is that EPM solutions enable security pros to manage passwords in a centralized, consistent fashion.

EPM Solutions Bridge The Gap And Complement Other IAM Capabilities

Given the continued concerns around passwords, some may question whether an EPM solution should be part of any IAM strategy and whether the security team should focus on moving toward SSO/IDaaS solutions and two-factor authentication (2FA). The reality is that while passwords introduce security risks, password coexistence is still the norm, not the exception. And if password coexistence is the current state, an EPM solution helps provide policy consistency around passwords, which reduces the risk of account compromise from weaker passwords.

In the last year, Forrester has spoken with a range of clients in different industries who have either deployed or are considering an EPM solution. In most cases, the EPM solution is part of a broader IAM review and complements existing or planned IAM investments. For example, we spoke with a healthcare provider that is using EPM solutions for specific applications that don't integrate with its existing 2FA model. And while SSO and 2FA should be an essential component of any IAM strategy, EPM solutions can complement these initiatives by providing capabilities that improve employee experience and productivity and still help contain password-related risks. EPM solutions provide core capabilities such as:

- **Secure local storage of passwords and private information.** EPM solutions provide a secure local vault of password information. This vault may also reside in the cloud so users can access it via a mobile device. The vault also enables the autofilling of credentials across devices and can enforce other requirements such as password complexity and password rotation. Most EPM solutions utilize a zero-knowledge model, meaning that the encryption key used to encrypt/decrypt the user's data is only done locally on the device so that the EPM provider never has access to individual encryption keys or password data.
- **Support for both personal and business password vaults.** Most EPM solutions enable users to create separate credential vaults — one for business, one for personal — as well as a quick mechanism to enable account switching so employees can quickly switch between work and personal vaults. This lets users keep their passwords in a single location but also allows security teams to enforce stronger password policies for enterprise accounts and also allows users to still access their personal passwords after leaving the organization.

- **Flexible deployment models.** EPM solutions make the credentials accessible via a range of approaches including a native website, mobile application, desktop application, or browser plug-in. The EPM solution syncs changes across all formats, so users can securely access sites regardless of the access model. The native application model can also simplify the user experience by enabling users to launch Windows RDP, SQL, SSH, Telnet, and web sessions directly from the app instead of having to conduct a copy-paste action.
- **An administrative console for management.** EPM provides an administrative console that assists in the deployment, management, and monitoring of the EPM endpoint solutions. In the console, security administrators can create roles and teams, enforce management policies, invite and enroll new users, and offboard users without risk of losing critical business information.
- **Account use auditing, monitoring, and management.** EPM solutions from Lieberman Software and ManageEngine focus on privileged accounts and thus can continuously discover and track privileged accounts across platforms and automatically provide each account with unique and frequently changing credentials.
- **SDKs and APIs for application integration.** Many EPM solutions also include dedicated APIs and documented APIs, which administrators can leverage to secure passwords embedded in app-to-app connections, scripts, and other locations across platforms. Applications can then access the secure password data store programmatically via an API as needed to ensure strong password compliance in these data flows.

Training, Communication, And Smart Policies Are Essential For Successful Implementation

While EPM solutions can provide a range of benefits and operational efficiencies from reducing password-related support costs, improved end user productivity, and stronger password policies, security teams have to consider several factors to ensure a smooth and successful EPM deployment. In our discussions with clients and EPM vendors, the following criteria emerged as best practices for successful EPM deployment:

- **Emphasize changing user password poor hygiene.** Like many technology implementations, successful EPM implementations are often more rooted in people and process than in technology. EPM implementation often requires users to change existing behavior and how they manage and utilize online accounts and passwords. Often, these habits are ingrained, hard to break, and will generate strong user resistance with claims that any change would have significant negative implications on employee productivity. This means that any EPM deployment must be coupled with thorough education on proper password policy and the business value of making such changes. This approach often requires security pros to collaborate with other teams such as HR to deliver a compelling message that motivates users to change.

- **Conduct adequate scoping with focus on higher risk systems and users first.** While EPM can integrate with a wide variety of applications, some security teams may not have the ability to enforce password changes across the organization. In such scenarios, focusing on users and systems that engage with the most sensitive data is a good compromise. Your firm may have to conduct a data inventory and risk assessment exercise for this.[7] This may mean limiting the EPM deployment to just privileged users and accounts, but if those are the only sessions managed through EPM, there is still significant risk reduction.
- **Assess integration with Active Directory.** Active Directory (AD) is the de facto authoritative identity store for most enterprises today and therefore can play a key role in complementing any EPM implementation. A successful EPM/AD integration provides synchronization to ensure that whenever users are added or removed in AD, the same happens in EPM. Furthermore, EPM solutions can often leverage existing AD authentication protocols, enabling users to single sign-on into their password vault with their AD credential. The integration can also be used predeployment to prepopulate AD user and group information into the EPM console. However, an EPM solution also needs to work in disconnected mode when the corporate AD is not accessible on a laptop, such as from a hotel room.
- **Provide comprehensive training and communication for admins and employees.** EPM requires a detailed rollout plan describing the changes, along with a range of training for both admins and employees. The training should not just focus on the functional changes but also highlight the value and benefit that EPM is delivering so that users can assess the implementation in context. EPM administrative tools can also track the progress of the deployment and enable the organization to respond to any kinks in the schedule and training and minimize any potential disruptions. Once the deployment is live, security pros should ensure that a knowledge base/FAQ is available and updated so that all new employees can enroll in EPM quickly and easily.
- **Track deployment status.** The EPM admin console can be a very useful tool for monitoring adoption and use. Most EPM solutions provide base-level reporting and visualization so security pros can assess the success of the deployment. These dashboards may also indicate potential bottlenecks that security pros can mitigate in real time to prevent end user disruption and allow the deployment to proceed as planned.
- **Assessing ways the EPM solution can integrate with other IAM initiatives.** EPM has strong synergy with other IAM solutions for single sign-on, identity federation, user provisioning, and privileged identity management. Security pros considering EPM solutions should identify areas of synergy where EPM can complement IAM policies and capabilities and vice versa. The result will be a more holistic and consistent identity-centric security infrastructure.
- **Develop policies for managing and responding to alerts.** EPM solutions provide different forms of alerting and reporting capabilities based on predefined rules and policies. Since these alerts may often be the first evidence of compromised accounts, it's important that security teams have a basic incident response plan in place to deal with these alerts or other related audit findings.

These defined processes help avoid delays or other disruptions when incidents occur and allow the security team to respond quickly and efficiently to any alerts. Longer term, security pros need to consider developing more-sophisticated alerts that might only alert when a range of certain conditions are met, and which might be indicative of potential malicious activity, which will enable security teams to achieve more predictive guidance about potential attacks.

› **Assess the implications of your changing application portfolio on EPM.** Today's businesses are continually changing, through internal reorganizations, strategic M&A, or a mix of both. At the same time, they are also adopting more cloud-based services at a rapid rate. As organizations adopt these new services, they need to assess how the EPM solutions will integrate with the cloud applications. Security pros should avoid one-off approaches that don't fit into the existing EPM framework, as such exceptions create inconsistencies and potential security blind spots hackers can exploit. This means security pros need to remain engaged with their app development counterparts to ensure any changes to the enterprise application portfolio can be accommodated within the EPM deployment if necessary.

EPM Vendors Offer Clear Pricing, Multiple Deployment Options

In our client interactions, Forrester has encountered several software vendors that provide EPM solutions to address both the end user and administrative aspects of passwords. Many of these vendors had a strong presence in North America across a range of vertical markets. Most vendors also offer a freemium or free single-user consumer version. We also found that most vendors favor per-user per-year subscription pricing with volume tiers, although vendors that focus on privileged accounts also price their offerings based on the number of endpoints, not number of users. EPM vendors also provide different form factors, including a desktop app, mobile app, and browser plug-in. The general trend is to offer EPM-as-a-service (which helps support multidevice models), but some solutions can be hosted onsite by a single enterprise if needed. The typical list of EPM vendors that we have encountered in our research and client interactions include (see Figure 3):

› **Keeper Security.** Keeper started with a consumer-based wallet and has since expanded to offer Keeper Business targeted for the enterprise market. Keeper Business is a zero-knowledge cloud-based EPM solution that provides secure storage of passwords and private info, shared passwords, autofilling of credentials across every type of device, and password rotation. The Keeper administrative interface enables administrators to deploy Keeper to end user uses, manage Active Directory integrations, create roles and teams, enforce password management policies, monitor activity, and offboard users.

› **LastPass.** LastPass was acquired by LogMeIn in October 2015, which has since merged with GetGo, a subsidiary of Citrix. LastPass Enterprise is a SaaS-based EPM solution and available as web, browser extension plug-in, or mobile app. Data stored in LastPass is encrypted locally and then stored both locally — on the end user's hard drive — as well as on LastPass servers located in multiple tier 1 data centers. LastPass Enterprise includes an administrative dashboard for managing and monitoring the LastPass Enterprise deployments.

- **Lieberman Software.** Lieberman has been managing privileged accounts for decades and has a strong enterprise install base. Lieberman RED Identity Management is designed for managing privileged credentials for cloud and on-premises environments. The solution can discover and track privileged accounts across platforms and automatically generate unique credentials for one-time use. Lieberman RED can manage passwords for service and super-user accounts and also manage SSH keys. The solution provides a full administrative interface for managing privileged accounts and supporting audit-related activities.
- **ManageEngine.** Password Manager Pro is a web application password vault primarily used for storing shared privileged account passwords. It offers role-based access control to administrators and end users to access and perform management actions on those passwords. It provides password life-cycle management for endpoints, including the ability to change the password after every use or on a defined schedule. The solution stores all password-related actions in a tamper-proof database to support audit activities and can integrate with security analytics solutions for notification and alerts.
- **RoboForm.** RoboForm provides a free consumer version but also offers RoboForm for Business, which is comprised of two components: centralized management console (hosted by vendor or on-premises) and the RoboForm client application, which can run on either the user's device or browser and can store passwords as well as other data used to complete online forms. The solution is SaaS only but does allow for hosting by the customer if necessary. The centralized administrative console allows administrators to deploy RoboForm account to employees, enforce security and other policies.

FIGURE 3 Vendor Capabilities

Keeper Security

Founded	2011
HQ	Chicago
EPM product name	Keeper Business
GA release date of evaluated version	July 2017
Approximate geographic revenue split	Forrester estimates: 80% North America; 15% EMEA; 5% ROW
Pricing	$30/user/year with tiered pricing options. Optional components premium support $750/year 1 TB of file storage at $18/user/year
Deployment model	SaaS with mobile and desktop applications
Offer freeware consumer password manager?	Yes
Desktop app?	Yes
Mobile app?	Yes
Provide browser extension plug-in?	Yes
Provide password management for app-to-app passwords and Windows service accounts?	No
Can users share passwords from your EPM solution with other users or groups?	Yes
Detect and manage SSH keys?	Yes
Support password escrow?	Yes
Support separate storage of personal and enterprise passwords?	Yes
Support 2-factor authentication into the password vault?	Yes
Support time-limited access to specific passwords?	Yes
Ability to manage Active Directory accounts?	Yes
Provide utilities to schedule when passwords must be changed?	Yes

FIGURE 3 Vendor Capabilities (Cont.)

LastPass/LogMeIn

Founded	2008/acquired 2015
HQ	Boston
EPM product name	LastPass Enterprise, Version 4.1
GA release date of evaluated version	July 2017
Approximate geographic revenue split	Forrester estimates: 70% North America 20% EMEA; 10% APAC
Pricing	Two options: 1) Self-service-user-based pricing ranging from $30-$48/user/year (depending on volume) 2) Flat annual rate based on total org size (list prices ranged from $10K-$400K based on company size)
Deployment model	SaaS with mobile and desktop applications
Offer freeware consumer password manager?	Yes
Desktop app?	Yes
Mobile app?	Yes
Provide browser extension plug-in?	Yes
Provide password management for app-to-app passwords and Windows service accounts?	Yes
Can users share passwords from your EPM solution with other users or groups?	Yes
Detect and manage SSH keys?	Detect: No. Manage: Yes.

FIGURE 3 Vendor Capabilities (Cont.)

LastPass/LogMeIn

Support password escrow?	No
Support separate storage of personal and enterprise passwords?	Yes
Support 2-factor authentication into the password vault?	Yes
Support time-limited access to specific passwords?	No
Ability to manage Active Directory accounts?	Yes
Provide utilities to schedule when passwords must be changed?	No

FIGURE 3 Vendor Capabilities (Cont.)

Lieberman Software

Founded	1978
HQ	Los Angeles
EPM product name	Lieberman RED — Rapid Enterprise Defense
GA release date of evaluated version	June 2017
Approximate geographic revenue split	Forrester estimates: 65% North America; 20% EMEA; 10% APAC 5% ROW
Pricing	Pricing begins at $10,000. The product is licensed per-managed end point (IP or hostname).
Deployment model	On-premises application
Offer freeware consumer password manager?	No
Desktop app?	No
Mobile app?	No
Provide browser extension plug-in?	No
Provide password management for app-to-app passwords and Windows service accounts?	Yes
Can users share passwords from your EPM solution with other users or groups?	No
Detect and manage SSH keys?	Yes
Support password escrow?	Yes
Support separate storage of personal and enterprise passwords?	Yes
Support 2-factor authentication into the password vault?	Yes
Support time-limited access to specific passwords?	Yes
Ability to manage Active Directory accounts?	Yes
Provide utilities to schedule when passwords must be changed?	Yes

FIGURE 3 Vendor Capabilities (Cont.)

ManageEngine/Zoho Corp

Founded	1996
HQ	Pleasanton, California
EPM product name	ManageEngine; Password Manager Pro
GA release date of evaluated version	June 2017
Approximate geographic revenue split	Forrester estimates: 55% North America; 30% EMEA; 10% APAC; 5% ROW
Pricing	Standard edition starts at $495 for two administrators/year. Premium edition starts at $1,195 for five administrators/year. Enterprise edition starts at $2,995 for 10 administrators/year.
Deployment model	On-premises application
Offer freeware consumer password manager?	Yes
Desktop app?	No
Mobile app?	Yes
Provide browser extension plug-in?	Yes
Provide password management for app-to-app passwords and Windows service accounts?	Yes
Can users share passwords from your EPM solution with other users or groups?	Yes
Detect and manage SSH keys?	Yes
Support password escrow?	No
Support separate storage of personal and enterprise passwords?	Yes
Support 2-factor authentication into the password vault?	Yes
Support time-limited access to specific passwords?	Yes
Ability to manage Active Directory accounts?	Yes
Provide utilities to schedule when passwords must be changed?	Yes

FIGURE 3 Vendor Capabilities (Cont.)

RoboForm

Founded	1995
HQ	Fairfax, Virginia
EPM product name	RoboForm for Business
GA release date of evaluated version	June 2017
Approximate geographic revenue split	Forrester estimates: 65% North America; 30% EMEA; 5% APAC
Pricing	Starts at $29.95/user/year for 1-10 users for one-year subscription. Starts at $25.45/user/year for 1-10 users for three-year subscription. Starts at $22.45/user/year for 1-10 users for five-year subscription. Volume discounts available for larger user quantities.
Deployment model	SaaS with mobile and desktop applications
Offer freeware consumer password manager?	Yes
Desktop app?	Yes
Mobile app?	Yes
Provide browser extension plug-in?	Yes
Provide password management for app-to-app passwords and Windows service accounts?	Yes
Can users share passwords from your EPM solution with other users or groups?	Yes
Detect and manage SSH keys?	No

FIGURE 3 Vendor Capabilities (Cont.)

RoboForm

Support password escrow?	Yes
Support separate storage of personal and enterprise passwords?	Yes
Support 2-factor authentication into the password vault?	Yes
Support time-limited access to specific passwords?	No
Ability to manage Active Directory accounts?	Yes
Provide utilities to schedule when passwords must be changed?	Yes

Recommendations

Use EPM Solutions To Handle Your Password Issues

While security pros should strive to wean the organization off passwords, the reality is that the transition to a password-free world is still in the future. In the interim, security pros need to evaluate solutions that can help minimize password-related chaos and frustration. EPM solutions can serve such a purpose, and for that reason, security pros should conduct a thorough assessment to determine how an EPM offering can coexist with other security controls. Based on our discussions with security pros who manage password and other identity-related implementations, here are key recommendations:

- **Make EPM part of your IAM strategy and portfolio.** EPM solutions provide needed value to many organizations both in managing organizational password chaos and improving security of password-based systems. Given the breadth and complexities of other identity-related issues, EPM should be just one tool in your IAM arsenal, not your only tool. As you assess your organization's fit with EPM, consider EPM's relation to other IAM capabilities such as access governance, single sign-on, and privileged identity management. This will require assessing how EPM can complement and integrate with their other IAM capabilities to provide a comprehensive IAM architecture.
- **Establish a cross-functional and departmental EPM planning and deployment process.** The extent of password-based systems in most enterprise means that any solution like EPM will require the implementation support of other functional groups such as application development, enterprise architecture, and possibly even the infrastructure and operations teams. Each of these groups may have separate and competing agendas, which can impede the success of any EPM implementation, particularly if the EPM implementation will change how users access applications or whether the

strong passwords provided via an EPM solution can integrate with legacy apps. This means that security pros need to establish a cross-functional approach as part of any EPM implementation. To minimize roadblocks during the deployment, you will have to collaborate with your application development and delivery, compliance, and IT operations teams for maximum success.

› **Plan for EPM coexistence with 2FA.** Given that passwords will likely still be required for some systems in the short term, security pros should plan for password coexistence for the near term. EPM solutions can become an important component of that strategy. Deploying EPM does not mean that security teams should not still consider and assess where and when 2FA and other non-password means of authentication can play a role in your organization. This means looking at EPM solutions as a possible mechanism to help bridge the gap to other forms of authentication in the future.

Supplemental Material

Survey Methodology

The Forrester Data Global Business Technographics Security Survey, 2017 was fielded between May and June 2017. This online survey included 3,752 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester's Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Research Now fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

The Forrester Data Global Business Technographics Workforce Benchmark Recontact Survey, 2017 was fielded in August 2017. This online survey included 7,021 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester's Business Technographics ensures that the final survey population only includes information workers who use a connected device for work at least 1 hour per day. Research Now fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Please note that the brand questions included in this survey should not be used to measure market share. The purpose of Forrester's Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time.

Companies Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

Keeper Security

LastPass

Lieberman Software

ManageEngine

RoboForm

Endnotes

[1] Source: Forrester Data Global Business Technographics Security Survey, 2017.

Base: 330 North American or European network security decision makers whose firms have had a security breach in the past 12 months.

[2] For more information, please see the Forrester report "Engineer Your Technology Environment To Improve Employee Productivity And Flow."

[3] Source: Carole Mahoney, "Easing the Pain of Password Management," University of Maryland University College Global Media Center, January 20, 2017 (https://globalmedia.umuc.edu/2017/01/20/easing-the-pain-of-password-management/).

[4] Security researchers discovered that Donald Trump's former campaign manager Paul Manafort may have used a weak password, "bond007," to access his Adobe and Dropbox online storage accounts. Source: Jonathan Vanian, "Paul Manafort May Have Used 'bond007' as His Online Password," Fortune, October 31, 2017 (http://fortune.com/2017/10/31/donald-trump-paul-manafort-bond007/).

[5] Source: Forrester Data Global Business Technographics Security Survey, 2017.

[6] As retailers expand their digital offerings and work to attract more customers, they must offer secure, customer-friendly websites or risk losing business. We evaluated Amazon, The Home Depot, Macy's, Staples, and Walmart to see how their online channels meet Forrester's security and ease criteria. For more information, please see the Forrester report "Security Strength And Ease Benchmark: US Online Retailers 2017."

[7] Data is the lifeblood of today's digital businesses, and sophisticated cybercriminals are determined to steal it. Forrester's data security and privacy playbook shows S&R pros how to navigate the complex market for data security and privacy solutions and take a holistic approach. For more information, please see the Forrester report "Protect Your Intellectual Property And Customer Data From Theft And Abuse."

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.