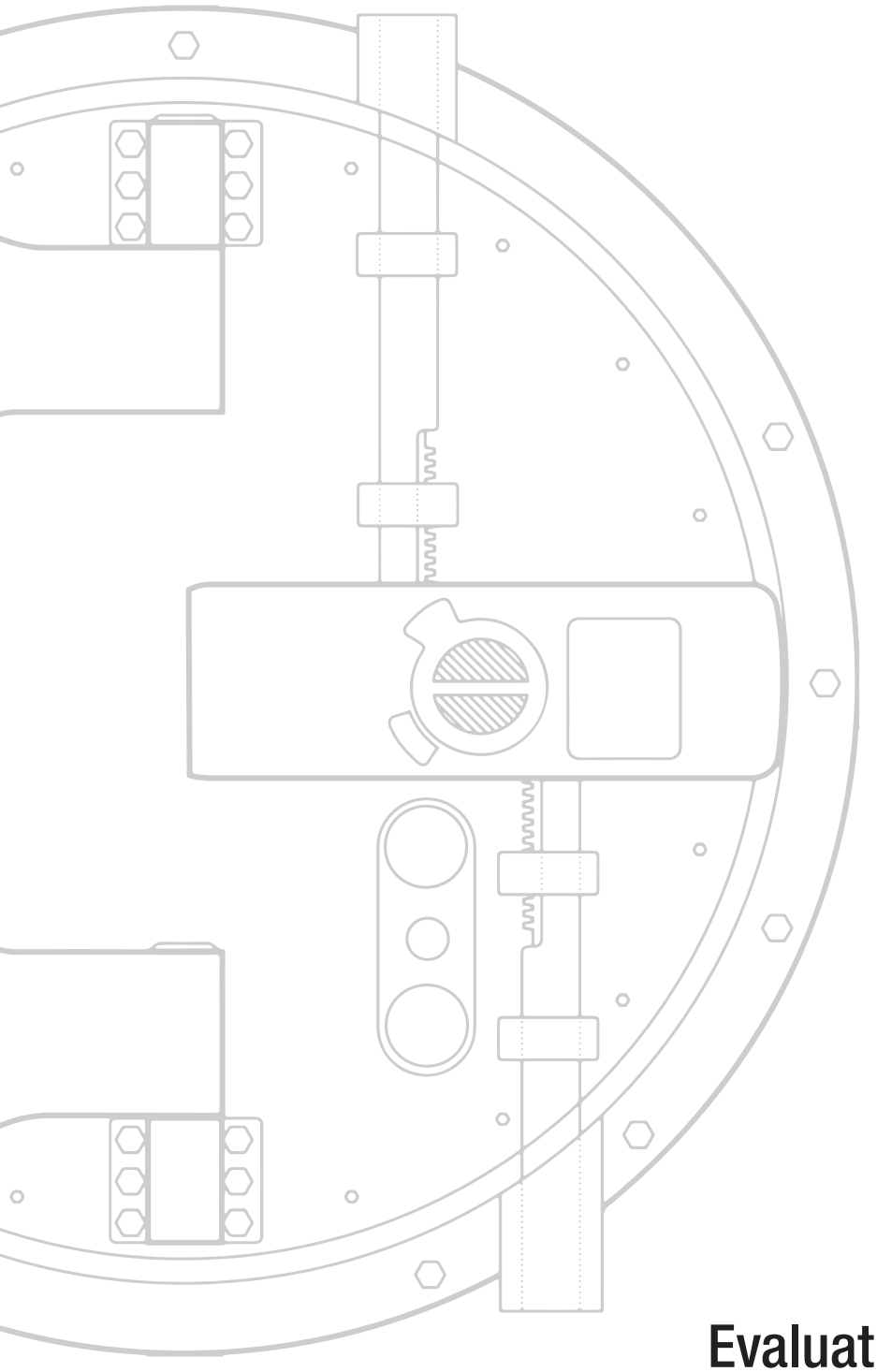
keeper



Password Management Evaluation Guide for Businesses

White Paper **2016**

Keeper Security, Inc. ©2016

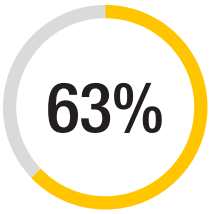
Executive Summary

Passwords – and the need for effective password management – are at the heart of the rise in costly data breaches. Various evolving business challenges complicate password management by increasing exposure to hacking and phishing attacks, or complicating protective measures. To help businesses address these challenges, various password management solutions are entering the marketplace, each with different capabilities. This white paper provides a guide for evaluating password management solutions. It describes recommended features of password management solutions in operational, implementation, management and administration, and support areas. The paper concludes with a summary of the wide range of business benefits that can be realized by implementing an effective password management solution.

Data Breaches: Causes and Costs

Data breaches are a growing epidemic – and a costly one. According to a 2015 IBM Cost of Data Breach Study, the average cost of a data breach is $3.8 million [1]. The number one cause (63 percent) of these data breaches is weak passwords [2]. This is not surprising. One study showed that 60 percent of people use the same password across multiple websites [3], and a second study determined that 90 percent of employee passwords can be cracked [4].

Weak passwords are at the center of the data breach epidemic



of data breaches are due to weak, default or stolen passwords

of people use the same password for everything

is spent on password resets every year

In addition to the high cost of data breaches, weak passwords and poor password management imposes other costs on organizations, including reduced employee productivity. The average user has an unmanagable amount of passwords, stores passwords on sticky notes or in Excel, uses easy-to-remember passwords, uses the same or similar passwords, and forgets passwords. This inefficient situation leads to wasted time as employees search for their passwords and contact the help desk, incurring further costs. In fact, according to Gartner, the number one help desk call (up to 50%) is for forgotten passwords and the annual industry cost for password resets is $10 billion [5].

Evolving Business Challenges

This rampant poor password hygiene by employees increases the vulnerability of organizations to hacking and phishing attacks. Yet these poor password practices are only the beginning of the problem. Organizations face a variety of challenges today that increase their exposure to security threats or complicate password protective measures (see Figure 2). For example, the proliferation of employee devices, including laptops, tablets, and smartphones, increases the number of password exposure pathways. Employees bring many of these devices to the workplace (so called "bring your own devices" or BYOD) and access confidential information using less-than-rigorous password practices, without IT department control or supervision.

Another challenge is the rising utilization of numerous cloud applications, including deployment of mission critical apps to the cloud. These apps use login credentials, of course, expanding the range of the password management challenge. More generally, the complexity of many businesses is rising, calling for an increasing number of services, and a corresponding increase in the number of systems to access. As if this wasn't enough, many businesses face increasing security-related regulations that impact how they operate.

Business complexities exacerbate the password management challenge

Utilize numerous cloud apps with login credentials

Increasingly vulnerable to hacking & phishing attacks

BYOD adds substantial complexity

End users are privilege users

Increasing number of services

Mission critical apps deployed through cloud

Password Management Solutions: Recommended Capabilities

To address the problem of poor password hygiene and password management, many leading organizations are adopting password management solutions. Yet these solutions vary significantly. This section of the paper presents recommended attributes for a password management solution in the following four areas:

- Operational recommendations
- Implementation recommendations
- Management and administration recommendations
- Support recommendations

Operational Recommendations

At its core, a password management solution must provide secure and encrypted password management. In addition, to ensure comprehensive protection, the solution must function seamlessly across a broad array of device types, operating systems and browsers that employees use. The solution must also support local storage as well as cloud storage (see Figure 3).

The password management solution should support a broad range of platforms, operating systems, and storage capabilities

Given that passwords can fall into the wrong hands, support for two-factor authentication (2FA) is recommended in password management solutions. 2FA requires the user to incorporate two authentication factors from a list that includes: something the employee has (e.g., a card or token), something the employee knows (e.g., a PIN or password), and something the employee "is" (e.g., some form of biometrics such as a fingerprint login or Smartwatch). Examples of solutions that offer one of these factors include SMS, DUO™, RSA SecurID™, Google Authenticator, Yubikey and others. Password management solution providers have a variety of options from which to choose in the 2FA space. The key recommendation here is to select a password management solution that 1) supports a range of 2FA types that suit the particular business needs, and 2) provides usable 2FA solutions that promote broad adoption within the business.

Password management solutions typically provide a secure vault to store the passwords, which is typically accessed using a master password. However, in many organizations, the need to securely store data extends beyond passwords. This can include SSH keys, digital certificates, as well as a range of confidential business documents, files, videos, photos, etc. Hence, a recommended feature of password management solutions is the ability to securely store these additional types of information as well.

Implementation Recommendations

Implementation considerations include encryption, cloud-based implementation, scalability, transparency, and certification.

Encryption considerations, in turn, consist of 1) defining who has control over the encryption and decryption process, and 2) the type of encryption used. The definition of who has encryption/decryption control involves the concept of "zero knowledge." In the case of a zero-knowledge password management solution provider, the user is the only person who has full control over the encryption and decryption of their data. The encryption key that is needed to decrypt the data always resides with the user; neither the password management solution provider nor the cloud provider can decrypt the user's stored data. This approach is recommended for the following reasons:

- The hacking of any involved provider would not compromise the data because it is encrypted at the end user.
- The hacking of any data while in transit between users and providers would not compromise the data because the data remains encrypted while in transit.

The type of encryption itself is an important consideration; without strong encryption, sophisticated hackers can hack the passwords. Today, the recommended method of encryption is the well-known, trusted algorithm called AES (Advanced Encryption Standard) with a 256-bit key length. Per the Committee on National Security Systems publication CNSSP-15, AES with 256-bit key-length is sufficiently secure to encrypt classified data up to top secret classification for the U.S. Government.

Implementation of the password management solution on one of the leading cloud storage providers is recommended. This enables the password management solution provider to offer the following:

- Scalable resources on-demand
- A fast, secure cloud storage environment
- Instant syncing of passwords across devices
- Encrypted cloud backups to avoid data loss

It is recommended that the password management provider operate both multi-zone and multi-region environments to maximize uptime and provide the fastest response time to users.

Client-side encryption, rather than encryption at the cloud-based provider, is recommended. In client encryption, the client (e.g., iPhone, Android device, Web app, etc.) performs all of the encryption work. In this arrangement, the cloud provider stores a raw binary that is essentially useless to an intruder. Even if the data is captured when it is transmitted between the client device and the cloud storage, it cannot be decrypted or utilized to attack or compromise the user's private data.

The ability to scale the password management solution to the rapidly growing needs of businesses is an important consideration. Password management solution providers can use features such as role-based permissions, team sharing, departmental auditing, and delegated administration to enable scalability.

Transparency or visibility into the specific security measures implemented in the password management solution is highly recommended. Rather than offering the solution as a "black box," businesses need to be able to verify the specifics of the password management solution.

A variety of types of third-party security scanning and penetration testing of the solution, as well as certifications, are recommended. The password management solution provider should enlist the services of a leading third-party security company to ensure that the provider's web application and cloud storage are secure from known remote exploits, vulnerabilities, and denial-of-service attacks. In addition, the following certifications are recommended (note that this is not a complete list):

- SOC II Type 2
- TRUSTe
- PCI-DSS
- HIPAA
- Trustwave
- U.S. Department of Commerce Export Licensed under Export Administration Regulations (EAR)

Management and Administration Recommendations

Recommended management and administration capabilities of the solution include the following:

- The solution should enable easy creation and management of users, as well as establishment of user and group policies for passwords.
- The solution should also enable visibility and auditing of password usage, compliance, and hygiene to improve user behavior. This is particularly important due to the fact that many organizations currently have no visibility into employee password hygiene. User password behavior cannot be improved, nor can password policies be enforced, without visibility into password usage and hygiene.
- Enforcement of password policies (e.g., password strength, scheduled password rotation for backend IT systems) aids regulatory compliance. In addition to the extra security that employee password rotation provides, password rotation also helps maintain security when credentials are shared with vendors.
- Provision for management and secure sharing of privileged account passwords is needed.
- Additional recommended capabilities include role-based permissions and controlled credential sharing.
- Active Directory and LDAP integration, which enables scalability and rapid deployment, is recommended.
- Visibility and reporting, which enables password policy enforcement, should include dashboards, notifications, and analytics; as well as support for auditing.
- Like any enterprise software solution, top-notch user and administrator support is essential. The solution provider should offer 24x7 support, FAQs, video tutorials, and user guides, for example.

Potential Business Benefits

Implementation of a password management solution that meets the recommendations outlined in this paper can provide several significant business benefits. Of course, the solution can help minimize likelihood of data breaches. This, in turn, helps to protect company reputation, minimize legal costs, and avoid breach recovery costs. Additional potential business benefits include the following:

- Fast time to security, via short time to deployment
- Improved employee security awareness and behavior
- Maintained regulatory compliance
- Increased employee productivity
- Reduced help desk costs
- Minimized training costs
- Minimized total cost of ownership

About Keeper Security Solution

Keeper Security is transforming the way businesses and individuals protect their passwords and sensitive digital assets to significantly reduce cyber theft. As the leading password manager and digital vault, Keeper helps millions of people and thousands of businesses substantially mitigate the risk of a data breach. Keeper is SOC 2 Certified and utilizes best-in-class encryption to safeguard its customers. Keeper protects industry-leading companies including Sony, Chipotle, and The University of Alabama at Birmingham. Keeper partners with global OEMs and mobile operators to preload Keeper on smartphones and tablets.

References

1. IBM, “2015 Cost of Data Breach Study,” conducted by Ponemon Institute, 2015, http://www-03.ibm.com/security/data-breach/

2. Verizon, “2016 Data Breach Investigations Report,” Executive Summary, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

3. As reported: Dancho Danchev for Zero Day on ZDNet.com, “Survey: 60 percent of users use the same passwords across more than one of their online accounts,” September 30, 2011, http://www.zdnet.com/article/survey-60-percent-of-users-use-the-same-password-across-more-than-one-of-their-online-accounts/

4. As reported: InfoSecurity magazine, “90% of passwords can be cracked in seconds,” January 15, 2013, http://www.infosecurity-magazine.com/news/90-of-passwords-can-be-cracked-in-seconds/.

5. Gartner Group

Contact

keepersecurity.com

312.226.5544

sales@keepersecurity.com