KuppingerCole Report

EXECUTIVE VIEW

By Martin Kuppinger

April 12, 2022

Keeper Enterprise

Password Management remains a key requirement for users and organizations, with passwords still being ubiquitous, and thus imposing a major security risk to organizations. Modern Enterprise Password Managers (EPM) help in securely managing passwords and the secure login. Keeper Enterprise is one of the leading EPM solutions, providing a secure and convenient approach and an excellent range of integrations to IdPs (Identity Providers), endpoints, and other systems.

By **Martin Kuppinger**
mk@kuppingercole.com

Content

1 Introduction

Password Management is an established discipline in IT. However, there is a dichotomy between the factual need for having such solutions in place in a world of widespread use of passwords and other secrets, and the perception of a diminishing relevance of passwords. The latter, unfortunately, is a perception that is backed by reality only to a rather limited extent. While we observe an increase in solutions for passwordless authentication, and a broader use of Identity Federation as a mechanism for Single Sign-On, the use of passwords still is prevalent.

Passwords are ubiquitous. This starts with passwords as fallback for many of the (not so truly) passwordless authentication approaches. Passwords are still common for many legacy applications, but also network devices and other systems. Passwords are common when accessing applications of business partners, not to mention retail web sites or other web sites that are frequently accessed, e.g., for industry news.

With passwords rightly being perceived as a major security risk, there is a need for protecting and managing passwords and adding security to all the use cases where passwords can't easily be replaced and will not disappear in foreseeable time.

This is where Password Managers and, closely related to them, Enterprise Single Sign-On solutions (E-SSO) come into play. They help organizations in managing and protecting passwords. Password Manager solutions are available as both single user editions, targeted at consumers and individual users, and enterprise solutions, which add centralized management across all users and other enterprise-level features. The line between enterprise-grade Password Managers and E-SSO is blurring, these solutions are often complementary. The main distinction is the client-side support of E-SSO for password-based login into legacy, non-web applications, which is not a common capability for Password Managers. The latter commonly focus on username and password fill into web applications and sometimes extend to support for identity federation protocols such as OAuth, but lesser to authentication for legacy solutions.

The core requirement for any Password Manager solution is security. Storing passwords centrally increases the risk, if not done right. There are multiple potential points of attack:

- The password store, commonly named "vault", where passwords and other secrets are centrally kept and managed, must be well-protected. HSM (Hardware Security Module) support is a key requirement.
- The admin console, which allows altering the configuration to the favor of attackers, must be well-protected.
- The transmission of secrets to the endpoints also exposes an attack surface and requires strong protection.

- Finally, the client components themselves are subject to attacks.

While today's enterprise-grade Password Manager solutions commonly provide a strong set of security features, this remains, aside of usability and integration, a key differentiator between the various offerings in the market. These solutions, implemented correctly, provide a significantly higher level of security than the unmanaged, decentralized use of passwords.

Keeper Enterprise is one enterprise-grade Password Manager with a well thought out security model categorized as "zero trust/zero knowledge", and a broad set of integrations to IdPs, target services, and security components such as HSMs.

2 Product Description

Keeper Security is an established provider of security solutions. Their core focus is on Enterprise Password Management (EPM). Aside of that, there is a consumer product for password management, as well as additional password security and PAM (Privileged Access Management) solutions. The company holds patents for password security and password management for mobile devices and computers. Their EPM solution Keeper Enterprise supports management of both passwords and other secrets such as API keys in an integrated solution.

Keeper goes beyond the common scope of EPM solutions in multiple areas. While it supports capabilities such as delivering insight and control about passwords and their security & hygiene, for all types of devices, they also support integrated checks on password leakage to the dark web, and, as mentioned above, the management of secrets and other sensitive information beyond just passwords.

Keeper EPM is a cloud service and can support a variety of models, from on-premises installations to private cloud and hybrid cloud deployments. Additionally, there are MSP (Managed Service Provider) multi-tenant offerings available . This gives customers a broad choice and flexibility for running and managing this critical element of their security infrastructure.

On the other end, Keeper EPM comes with extensive device support, including applications for Windows, Linux and Mac endpoints as well as iOS and Android mobile devices including Apple Watch. It also supports all major browsers, including Chrome, Safari, Firefox, Opera, IE and Edge. The desktop app provides a \"Native App filler\" which will input credentials, notes, OTPs and other data into legacy windows apps.

For authentication of users to the Keeper EPM client-side modules, it integrates with any identity provider that supports SAML , delivering a SSO (Single Sign-On) experience to the user. Thus, the capabilities for strong MFA (Multi Factor Authentication) and passwordless authentication provided by these IdPs can be utilized for secure access to Keeper EPM. Supported identity providers include, amongst others

- Microsoft Azure Active Directory
- Microsoft Active Directory Federation Services (ADFS)
- Google Workspace
- Okta
- Duo
- OneLogin
- JumpCloud

Additionally, there is the option to synchronize with Microsoft Active Directory or OpenLDAP, using the Keeper AD Bridge.

As for every EPM solution, security of password vaults and transmissions is one of the key differentiating criteria. Keeper Security positions its solution as both zero knowledge and zero trust. Zero Knowledge is about securely storing and transmitting the passwords and other secrets, while not providing insight into passwords for administrators or others. The customer keeps control of secrets and can manage these, while passwords remain encrypted. Zero Trust refers to the fact that the internal control environment of the customer remains isolated and protected, with strict enforcement policies regarding access, and comprehensive reporting.

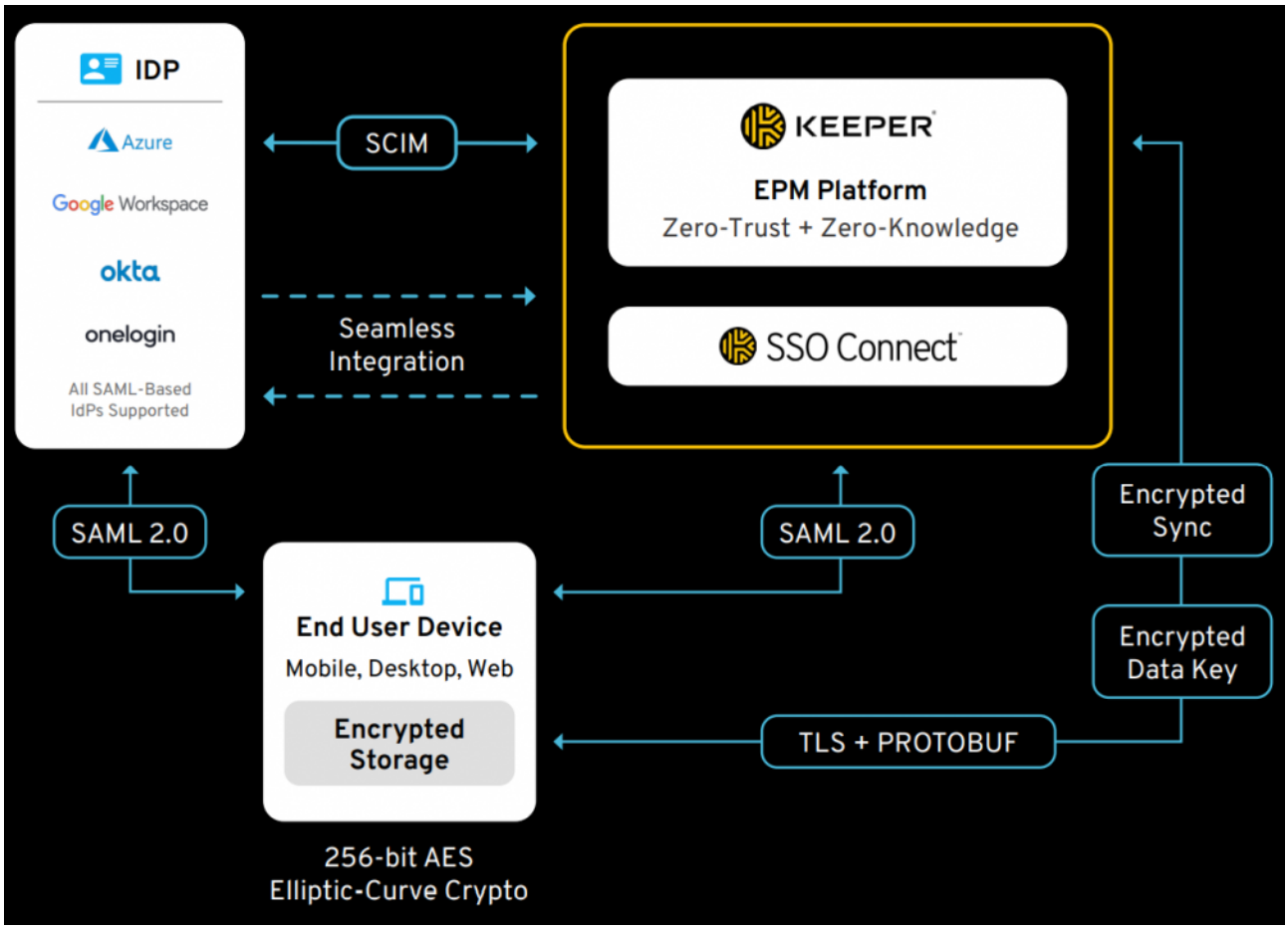

Figure 1: The high-level security architecture of Keeper Enterprise (Source: Keeper Security).

As mentioned, Keeper EPM integrates at the backend with various IdPs. User Management is supported via the SCIM (System for Cross-Domain Identity Management) standard that allows to provision and deprovision users from the IdP. Users then can authenticate using the SAML 2.0 standard protocol, with the Keeper end user components acting as the relying party/service provider in that authentication. SAML 2.0 is therefore used for authentication of endpoints to the Keeper Enterprise backend services.

Keeper provides native MFA support for customers that do not have an identity provider, providing an easy path for multi-factor authentication which supports email, text, KeeperPush, OTP, biometrics and more. The mobile application supports FIDO 2 WebAuthn, enabling use of Yubikeys and device biometrics as authentication factors as well.

At the device, there is encrypted storage, using strong cryptographic algorithms (AES 256-Bit, elliptic curve). Keeper uses multiple layers of encryption where each individual record has its own key. Similarly, the communication between the encrypted storage and the central modules of Keeper Enterprise is encrypted and protected. Based on the zero-knowledge principle, Keeper only stores a hash of the record and has no access whatsoever to user credentials or secrets.

Keeper Enterprise also supports automated back-end password rotation. Based on the Keeper Commander SDK, admins and developers can improve password security across own code and backend systems, from Windows and Linux servers to databases and AWS passwords.

The rollout of the client-side components is straightforward. It can, amongst other approaches, run via eMail with links, where verification is based on the organization's domain. The client-side components come with a modern user interface, allowing seamless access and management of the user's credentials and other secrets. The control of users secrets can be flexibly managed and restricted. For the administration, Keeper Enterprise follows a role-based access control approach.

The central admin console provides both management capabilities across the various endpoints and users, and insight into the current state. This allows for real-time security monitoring and enables administrators to take immediate actions. The dashboards deliver risk scores and detailed insight. For efficient management, Keeper Enterprise comes with pre-configured policies to adhere to regulations and compliance reports such as HIPAA, DPA, GDPR, SOX, and others. Policies can be flexibly configured with a wide range of features, e.g., mandating MFA or whitelisting IP addresses. Keeper BreachWatch also integrates dark web monitoring to identify leaked passwords that are for sale.

3 Strengths and Challenges

Keeper Enterprise is a mature solution for EPM with a modern user interface and supporting the current standards in authentication, identity provisioning, and -- most importantly -- encryption. It comes with broad support for endpoints and is easy to deploy. The security concepts are well thought out. The administration interface is powerful and delivers real-time insights into password-related threats.

The solution excels with overall strong integration capabilities, both to IdPs for authentication and user management, and to backends and supporting systems such as HSMs. Deployment is highly flexible and roll-out of the client-side components is straightforward. Keeper Enterprise is built to operate well-integrated into existing IT environments, e.g., for authentication, and does not provide built-in MFA capabilities. Being an EPM focused on web applications and backend integration via an SDK, Keeper Enterprise also lacks integrated support for password-based login to legacy Windows applications (fat client applications) and thus is no full replacement for E-SSO solutions.

With its broad set of capabilities, Keeper Enterprise counts amongst the leading EPM platforms. Given that most organizations still must manage and secure a vast amount of passwords, this is an important addition to the cybersecurity tools portfolio. We recommend evaluating Keeper Enterprise when looking for an EPM solution.

Strengths

- Strong security concepts
- Support for most modern and secure cryptographic algorithms
- Flexible, broad, and standards-based integration to IdPs for strong authentication
- Modern user interface for both end users and administrators
- Dashboard for administrators delivering insight into current risks
- Flexible, policy-based configuration of security
- Out-of-the-box support for common regulations such as HIPAA
- Flexible deployment models
- Broad endpoint support for both desktops and mobile devices
- SDK for backend integration and automated password rotation

Challenges

- Even though there is caching to support offline work, it is a cloud service. There is no on-premises deployment available.
- While affordable, it is an additional investment relative to free password storage capabilities in browsers and devices.
- Flexible deployment, but no QR code-based deployment approach supported yet

4 Related Research

Blog Post: Not so dead yet - why passwords will survive all of us
Advisory Note: Identity Authentication Standards

Content of Figures

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.