KuppingerCole Report

EXECUTIVE VIEW

By Martin Kuppinger

May 10, 2022

Keeper Enterprise

Die Verwaltung von Passwörtern ist und bleibt eine wichtige Anforderung für Benutzer und Unternehmen, da Passwörter immer noch allgegenwärtig sind und damit weiterhin ein großes Sicherheitsrisiko für Unternehmen darstellen. Moderne Enterprise Password Manager (EPM) können bei der sicheren Verwaltung von Passwörtern und dem sicheren Login helfen. Keeper Enterprise ist eine der führenden EPM-Lösungen, die eine sichere und bequeme Verwaltung von Passwörtern ermöglicht und breite Unterstützung von Schnittstellen zu IdPs (Identity Providers), Endgeräten und anderen Systemen bietet.

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

Inhalt

1 Einleitung

Die Verwaltung von Passwörtern ist ein etablierter Teilbereich der IT. Heute besteht jedoch eine Diskrepanz zwischen der öffentlichen Wahrnehmung einer abnehmenden Bedeutung von Passwörtern und der tatsächlichen Notwendigkeit solcher Lösungen in einer Welt, in der Passwörter weiterhin weit verbreitet sind. Die Wahrnehmung, dass Passwörter keine große Bedeutung mehr haben, entspricht nur bedingt der Realität. Es gibt zwar ein deutliches Wachstum bei Lösungen für die passwortlose Authentifizierung und eine immer breitere Nutzung von Identity Federation als Mechanismus für Single Sign-On. Passwörter sind aber immer noch weit verbreitet.

Das beginnt mit Passwörtern als Notfalllösung für viele der (nicht so wirklich) passwortlosen Authentifizierungsansätze, wenn beispielsweise die biometrische Authentifizierung nicht funktioniert. Bei Legacy-Anwendungen, aber auch für Netzwerkgeräte und andere Systeme, ist die Nutzung von Passwörtern für den Zugriff nach wie vor üblich. Passwörter müssen oft auch beim Zugriff auf Anwendungen von Geschäftspartnern genutzt werden, ganz zu schweigen von Websites im Onlinehandel oder anderen viel genutzten Websites wie beispielsweise News-Seiten oder Wissensdatenbanken.

Da Passwörter zu Recht als ein großes Sicherheitsrisiko angesehen werden, besteht also ein Bedarf an Schutz und Verwaltung von Passwörtern und an zusätzlicher Sicherheit für alle die Anwendungsfälle, in denen Passwörter nicht einfach ersetzt werden können und in absehbarer Zeit nicht verschwinden werden.

An dieser Stelle kommen Passwort-Manager und, eng damit verbunden, Enterprise Single Sign-On-Lösungen (E-SSO) ins Spiel. Sie helfen Unternehmen bei der Verwaltung und dem Schutz von Passwörtern. Passwort-Manager-Lösungen sind sowohl als Einzelbenutzer-Editionen erhältlich, die sich an Privatanwender und Einzelbenutzer richten, als auch als Unternehmenslösungen, die eine zentralisierte Verwaltung für alle Benutzer und andere Funktionen auf Unternehmensebene bieten. Die Grenze zwischen unternehmenstauglichen Passwort-Managern und E-SSO ist fließend, da sich diese Lösungen oft ergänzen. Der Hauptunterschied liegt in der Unterstützung von E-SSO für die passwortbasierte Anmeldung bei älteren, nicht webbasierten Anwendungen über eine auf dem lokalen System installierte Anwendung, die Passwortaufforderungen erkennt und die Passwörter im Hintergrund übergibt, was bei Passwortmanagern nicht üblich ist. Letztere konzentrieren sich in der Regel auf die Eingabe von Benutzernamen und Passwörtern in Webanwendungen und bieten zum Teil auch Unterstützung für Federation-Protokolle wie OAuth, aber selten für die Authentifizierung an Legacy-Anwendungen.

Die Hauptanforderung an jede Password Manager-Lösung ist Sicherheit. Die zentrale Speicherung von Passwörtern ist ein potentielles Sicherheitsrisiko. Dabei gibt es mehrere potenzielle Angriffspunkte:

- Der Passwortspeicher, allgemein als "Vault" bezeichnet, in dem Passwörter und andere Secrets zentral aufbewahrt und verwaltet werden, muss gut geschützt sein. Dafür ist die Unterstützung von

HSM (Hardware Security Module) eine wichtige Voraussetzung. Einige Lösungen verzichten auch auf einen zentralen Vault und legen die Informationen nur lokal auf den Clients ab, wodurch die Angriffsfläche verteilt und verkleinert wird.

- Die Verwaltungskonsole, über die die Konfiguration zu Gunsten von Angreifern geändert werden kann, muss gut geschützt sein.
- Die Übertragung von Secrets an die Endpunkte stellt ebenfalls eine Angriffsfläche dar und erfordert einen starken Schutz.
- Schließlich sind auch die Client-Komponenten selbst angreifbar.

Obwohl die heutigen Passwort-Manager-Lösungen für Unternehmen in der Regel eine Reihe starker Sicherheitsfunktionen bieten, sind diese Funktionen neben der Benutzerfreundlichkeit und der Integration ein wichtiges Unterscheidungsmerkmal zwischen den verschiedenen Angeboten auf dem Markt. Richtig implementiert, gewährleisten diese Lösungen ein deutlich höheres Sicherheitsniveau als die unkontrollierte, dezentrale Verwendung von Passwörtern.

Keeper Enterprise ist ein Passwort-Manager für Unternehmen mit einem gut durchdachten Sicherheitsmodell, das als "Null Vertrauen/Null Wissen" (Zero Trust/Zero Knowledge) bezeichnet wird. Das Produkt stellt eine einer breiten Palette an Schnittstellen zu IdPs, Anwendungen und anderen Sicherheitskomponenten wie HSMs bereit.

2 Produktbeschreibung

Keeper Security ist ein etablierter Anbieter von Sicherheitslösungen. Der Schwerpunkt liegt auf dem Enterprise Password Management (EPM). Daneben gibt es ein Consumer-Produkt für die Passwortverwaltung sowie weitere Lösungen für Passwortsicherheit und PAM (Privileged Access Management). Das Unternehmen hält Patente für Passwortsicherheit und Passwortmanagement für mobile Geräte und Computer. Die EPM-Lösung Keeper Enterprise unterstützt dabei die Verwaltung von Passwörtern und von anderen Secrets wie API-Schlüsseln in einer integrierten Lösung.

Keeper geht dabei in mehreren Bereichen über den üblichen Umfang von EPM-Lösungen hinaus, denn es unterstützt nicht nur Funktionen wie die Überwachung der Nutzung und die Kontrolle über Passwörter und deren Sicherheit für alle Arten von Geräten, sondern auch Funktionen für die Analyse von Passwortlecks, die dazu führen, dass Passwörter im Dark Web auftauchen und gehandelt werden. Außerdem wird, wie oben erwähnt, die Verwaltung von Secrets und anderen sensiblen Informationen über Passwörter hinaus unterstützt.

Keeper EPM ist ein Cloud-Service und kann eine Vielzahl von Bereitstellungsmodellen unterstützen, von On-Premises-Installationen bis hin zu Private-Cloud- und Hybrid-Cloud-Implementierungen. Darüber hinaus gibt es MSP (Managed Service Provider)-Angebote mit Multi-Mandanten-Fähigkeit. Dadurch haben Kunden eine große Auswahl und Flexibilität bei der Gestaltung dieses Teils ihrer Sicherheitsinfrastruktur.

Keeper EPM bietet eine umfassende Geräteunterstützung, einschließlich Windows-, Linux- und Mac-Endgeräten sowie iOS- und Android-Mobilgeräten und auch der Apple Watch. Außerdem werden alle gängigen Browser unterstützt, darunter Chrome, Safari, Firefox, Opera, IE und Edge. Die Desktop-App bietet darüber hinaus einen "Native App Filler", mit dem Anmeldeinformationen, aber auch Einmalkennwörter (OTPs, One Time Passwords) und andere Daten an ältere Windows-Apps gesendet werden können.

Damit sich Benutzer Client-Komponenten von Keeper EPM authentifizieren können, lässt sich die App mit jedem Identitätsanbieter integrieren, der SAML unterstützt. Das liefert dem Benutzer ein SSO-Erlebnis (Single Sign-On). So können die von diesen IdPs bereitgestellten Funktionen für starke MFA (Multi Factor Authentication) und passwortlose Authentifizierung für den sicheren Zugriff auf Keeper EPM verwendet werden. Zu den unterstützten Identitätsanbietern gehören u.a.

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

- Duo
- OneLogin
- JumpCloud

Zusätzlich besteht die Möglichkeit der Synchronisation mit Microsoft Active Directory oder OpenLDAP unter Verwendung der Keeper AD Bridge.

Wie bei jeder EPM-Lösung ist die Sicherheit von Passwort-Vaults und Passwort-Transfers zu anderen Systemen eines der wichtigsten Unterscheidungskriterien. Keeper Security positioniert seine Lösung sowohl als Zero Knowledge als auch als Zero Trust. Bei Zero Knowledge geht es um die sichere Speicherung und Übermittlung von Passwörtern und anderen Secrets, ohne dass Administratoren oder andere Personen Einblick in die Passwörter erhalten. Der Kunde behält die Kontrolle über die Secrets und kann diese verwalten, während die Passwörter verschlüsselt bleiben. Zero Trust bezieht sich auf die Tatsache, dass die interne Kontrollumgebung des Kunden durch strenge Durchsetzungsrichtlinien bezüglich des Zugangs und der umfassenden Berichterstattung isoliert und geschützt bleibt.

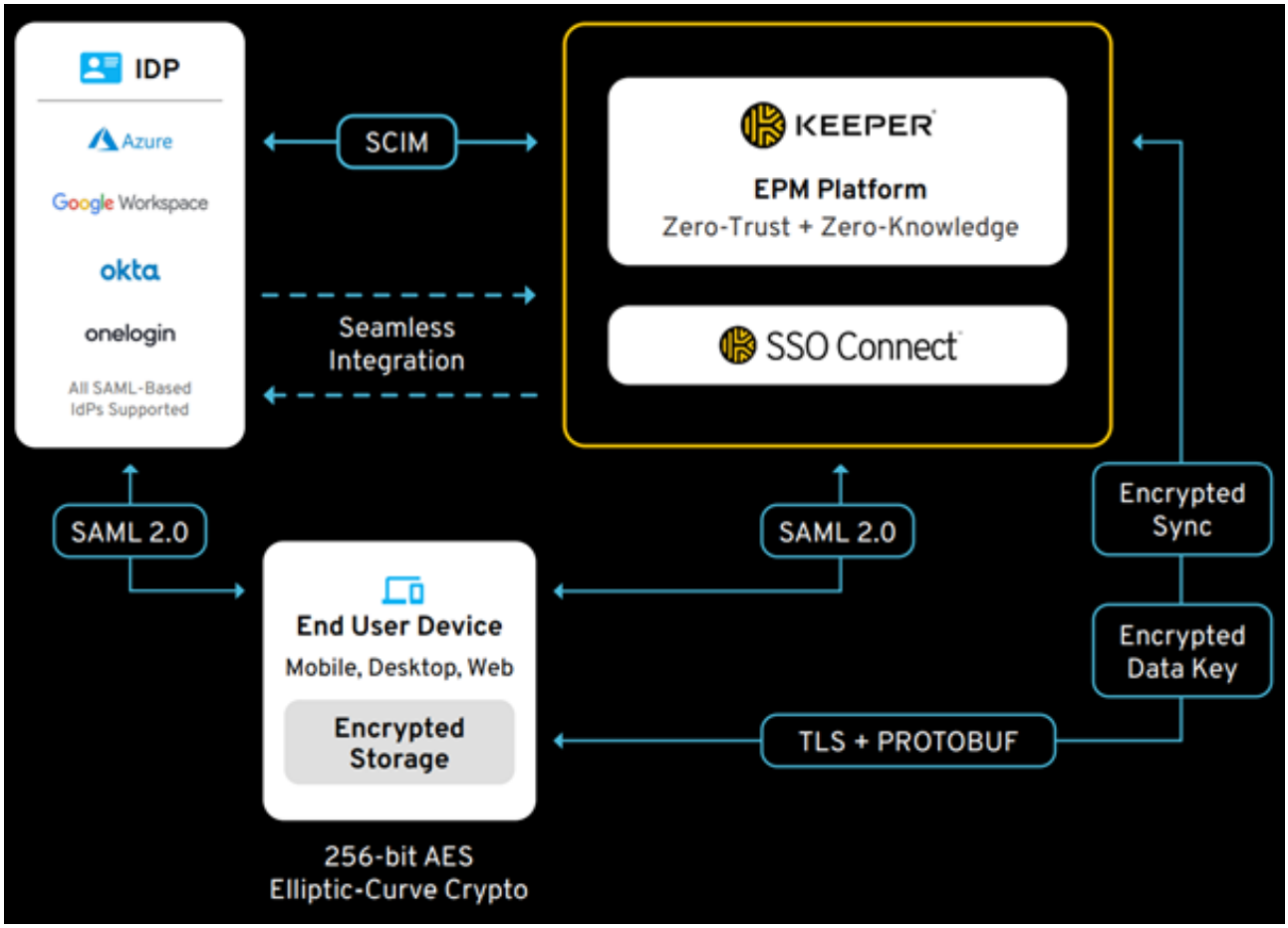

Abbildung 1: Die hochgradige sichere Architektur von Keeper Enterprise (Quelle: Keeper Security).

Wie bereits ausgeführt, lässt sich Keeper EPM am Backend mit verschiedenen IdPs integrieren. Die Benutzerverwaltung wird dabei über den SCIM-Standard (System for Cross-Domain Identity Management) unterstützt, der die Bereitstellung und das Deprovisionieren von Benutzern über den IdP ermöglicht. Die Benutzer können sich dann über das SAML 2.0-Standardprotokoll authentifizieren, wobei die Keeper-Endbenutzerkomponenten bei dieser Authentifizierung als vertrauende Partei/Dienstanbieter fungieren. SAML 2.0 wird daher für die Authentifizierung von Endpunkten gegenüber den Keeper Enterprise Backend-Services verwendet.

Keeper bietet native MFA-Unterstützung für Kunden, die keinen Identitätsanbieter besitzen, und stellt einen einfachen Weg für die Multi-Faktor-Authentifizierung bereit, der E-Mail, Text, KeeperPush, OTP, Biometrie etc. unterstützt. Die mobile Anwendung unterstützt FIDO 2 WebAuthn und ermöglicht somit die Verwendung von Yubikeys und Gerätebiometrie als Authentifizierungsfaktoren.

Auf dem Gerät werden die Daten verschlüsselt gespeichert, indem starke kryptographische Algorithmen (AES 256-Bit, elliptische Kurve) verwendet werden. Keeper verwendet mehrere Verschlüsselungsebenen, bei denen jeder einzelne Datensatz seinen eigenen Schlüssel hat. Ebenso ist die Kommunikation zwischen dem verschlüsselten Speicher und den zentralen Modulen von Keeper Enterprise verschlüsselt und geschützt. Basierend auf dem Zero-Knowledge-Prinzip speichert Keeper nur einen Hash des Datensatzes

und hat keinerlei Zugriff auf die Anmeldedaten oder Secrets der Benutzer.

Keeper Enterprise unterstützt zudem die automatische Rotation von Passwörtern im Backend. Auf Grundlage der Keeper Commander SDK können Administratoren und Entwickler die Passwortsicherheit für eigenen Code und Backend-Systeme verbessern, von Windows- und Linux-Servern bis hin zu Datenbanken und AWS-Passwörtern.

Der Rollout der Komponenten auf die Endgeräte ist unkompliziert. Sie kann unter anderem per E-Mail mit Links erfolgen, bei denen die Verifizierung auf der Domäne des Unternehmens basiert. Die Client-Komponenten verfügen dabei über eine moderne Benutzeroberfläche, die einen reibungslosen Zugriff und die Verwaltung der Anmeldedaten und anderer Secrets des Benutzers ermöglicht. Die Kontrolle der Secrets der Benutzer kann flexibel über zentrale Richtlinien verwaltet und eingeschränkt werden. Bei der Verwaltung verfolgt Keeper Enterprise einen rollenbasierten Ansatz der Zugriffskontrolle.

Die zentrale Verwaltungskonsole bietet sowohl Verwaltungsfunktionen für die verschiedenen Endpunkte und Benutzer als auch einen Einblick in den aktuellen Status. Dies ermöglicht eine Sicherheitsüberwachung in Echtzeit und versetzt die Administratoren in die Lage, sofortige Maßnahmen ergreifen zu können. Die Dashboards liefern dabei Risikobewertungen und detaillierte Einblicke. Für eine effiziente Verwaltung verfügt Keeper Enterprise über vorkonfigurierte Richtlinien zur Einhaltung von Vorschriften und Compliance-Berichten wie HIPAA, DPA, GDPR, SOX etc. Richtlinien können somit flexibel mit einer Vielzahl von Funktionen konfiguriert werden, z. B. mit MFA oder Whitelisting von IP-Adressen. Keeper BreachWatch integriert auch die Überwachung des Dark Web, um geleakte Passwörter zu identifizieren, die im Dark Web verkauft werden.

3 Stärken und Herausforderungen

Keeper Enterprise ist eine ausgereifte Lösung für EPM mit einer modernen Benutzeroberfläche und unterstützt die aktuellen Standards in den Bereichen Authentifizierung, Identitätsbereitstellung und Verschlüsselung. Das Produkt verfügt über eine breite Unterstützung für Endgeräte. Die lokalen Komponenten lassen sich einfach implementieren. Die Sicherheitskonzepte sind gut durchdacht, die Administrationsoberfläche ist leistungsstark und liefert Echtzeiteinblicke in passwortbezogene Bedrohungen.

Die Lösung zeichnet sich durch insgesamt starke Integrationsfähigkeiten aus, sowohl zu IdPs für Authentifizierung und Benutzerverwaltung als auch zu Backends und unterstützenden Systemen, wie HSMs. Die Bereitstellung funktioniert äußerst flexibel und die Einführung der Client-Komponenten ist unkompliziert. Keeper Enterprise ist darauf ausgelegt, in bestehende IT-Umgebungen gut integrierbar zu sein, z.B. für eine integrierte Authentifizierung, und bietet auch integrierte MFA-Funktionen. Da Keeper Enterprise ein EPM ist, das sich auf Webanwendungen und Backend-Integration über ein SDK konzentriert, ist die integrierte Unterstützung für die passwortbasierte Anmeldung bei älteren Windows-Anwendungen (Fat Client-Anwendungen) begrenzt. Keeper Enterprise ist daher kein vollständiger Ersatz für E-SSO-Lösungen.

Mit seinem breiten Spektrum an Funktionen zählt Keeper Enterprise zu den führenden EPM-Plattformen. Angesichts der Tatsache, dass die meisten Unternehmen nach wie vor eine große Anzahl von Passwörtern verwalten und schützen müssen, bietet Keeper Enterprise eine wichtige Ergänzung des Portfolios an Cybersecurity-Tools. Wir empfehlen daher, Keeper Enterprise zu evaluieren, wenn Sie nach einer EPM-Lösung suchen.

Stärken

- Starke Sicherheitskonzepte
- Unterstützung für die meisten modernen und sicheren kryptographischen Algorithmen
- Flexible, breite und standardbasierte Integration in IdPs für starke Authentifizierung
- Moderne Benutzeroberfläche für Endanwender und Administratoren
- Dashboard für Administratoren, das einen Einblick in aktuelle Risiken bietet
- Flexible, richtlinienbasierte Sicherheitskonfiguration
- Out-of-the-Box-Unterstützung für gängige Vorschriften wie HIPAA
- Flexible Bereitstellungsmodelle
- Umfassende Endpunktunterstützung für Desktops und mobile Geräte
- SDK für Backend-Integration und automatische Passwortrotation

Herausforderungen

- Auch wenn wichtige Informationen für die Offline-Nutzung lokal zwischengespeichert werden, handelt es sich um einen Cloud-Dienst.
- Vergleichsweise niedrige Kosten, aber dennoch eine zusätzliche Investition im Vergleich zu kostenlosen Passwortspeicherfunktionen in Browsern und anderen Geräten.
- Viele Bereitstellungsoptionen, aber noch kein QR-Code-basierter Ansatz für die einfache Bereitstellung.

4 Verwandter Research

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

Abbildungsverzeichnis

Copyright

KuppingerCole unterstützt IT-Experten mit herausragender Expertise bei der Definition von IT-Strategien und in relevanten Entscheidungsprozessen. Als führendes Analyseunternehmen bietet KuppingerCole aus erster Hand herstellerneutrale Informationen. Unsere Dienstleistungen ermöglichen es Ihnen, sich bei Entscheidungen, die für ihr Unternehmen unerlässlich sind, wohl und sicher zu fühlen.

KuppingerCole, gegründet im Jahr 2004, ist eine globale, unabhängige Analyseorganisation mit Hauptsitz in Europa. Wir sind darauf spezialisiert, herstellerneutrale Beratung, Expertise, Thought Leadership und praktische Relevanz in den Bereichen Cybersicherheit, digitale Identität & IAM (Identitäts- und Zugriffsmanagement), Cloud-Risiko und -Sicherheit und künstliche Intelligenz sowie für alle Technologien, die die digitale Transformation fördern, anzubieten. Wir unterstützen Unternehmen, Unternehmensanwender, Integratoren und Softwarehersteller dabei, sowohl taktische als auch strategische Herausforderungen zu meistern und bessere Entscheidungen für den Erfolg ihres Unternehmens zu treffen. Die Aufrechterhaltung eines Gleichgewichts zwischen sofortiger Umsetzung und langfristiger Lebensfähigkeit ist das Herzstück unserer Philosophie.

Für weitere Informationen wenden Sie sich bitte an clients@kuppingercole.com.