KEEPER
Cybersecurity Starts Here™

Privileged Access Management, Single Sign-On and Enterprise Password Managers

Choosing the Right IAM Solution for Your Business

TABLE OF CONTENTS

BACKGROUND

Password security plays a fundamental role in Identity and Access Management (IAM). The easiest way for cybercriminals to breach an enterprise network is to obtain a set of legitimate login credentials. This allows them to bypass firewalls, intrusion detection systems and other technical security solutions. Once inside, they can remain undetected for some time. The average "dwell time," the period between the initial breach and the time a company discovers it, is a staggering 101 days.[1] The cybercriminals behind the infamous Marriott Starwood breach were inside the company's system for four years before being discovered.[2]

A study of global small-and medium-sized businesses (SMBs) conducted by the Ponemon Institute in conjunction with Keeper Security found that SMBs worldwide are struggling to keep employee passwords secure. Surveyed SMBs cited their top two pain points as employee passwords being stolen or compromised (70%) and use of weak passwords (61%).

Nearly half (47%) of cyberattacks against surveyed SMBs in the previous 12 months involved compromised employee passwords. Half of respondents have no employee password policy, and over half (54%) have no visibility into employee password practices.[3]

From proprietary IAM solutions offered as a native part of public cloud providers' services to provisioning software and identity repositories, there's no shortage of IAM tools on the market. There are so many tools that even tech companies may be uncertain as to which one(s) they need. However, in the end, most IAM solutions fall into one of three categories: Privileged Access Management, Single Sign-On and Enterprise Password Management. In this paper, we'll explain what each of these solutions does, examine their pros and cons and outline typical use cases.

SINGLE SIGN-ON (SSO)

Purpose

Single Sign-On, or SSO, allows end users to log in to multiple websites or cloud applications using one set of login credentials. SSO is session-based; once a user logs into the SSO, they don't have to log in again during that session. It is used by both individuals and businesses. Most people have seen SSO in action when using their Google, LinkedIn, Twitter or Facebook credentials to log into a third-party website or application, such as a mobile game.

Some SSO services use protocols such as Kerberos, SAML or OAuth. There are also smart card-based SSO systems that require users to present a card encoded with their login credentials.

Advantages & Disadvantages

The biggest advantage to SSO is user convenience. Instead of having to remember multiple passwords, users memorize only one. Once logged into the SSO system, users can access multiple sites and apps without having to re-enter their login credentials during that session; this enhances productivity and also minimizes IT help desk tickets for missing passwords.

However, SSO is not a silver bullet. All that convenience can come with security risks, particularly if the SSO doesn't utilize end-to-end encryption, isn't augmented with two-factor authentication (2FA) and identity governance. SSO only controls access to systems, not individual user access levels within the target application. If the user forgets their password, they're locked out of multiple sites and apps instead of just one; conversely, if a cybercriminal steals their password, they can access multiple systems instead of just one. SSO also doesn't prevent employees from reusing passwords from the workplace for their personal accounts.

Moreover, SSO does not solve all productivity issues with passwords. Not all apps and systems support SSO -- or at least not the SSO protocol your enterprise is using -- resulting in major security gaps. If your company uses the SAML protocol, and your employees need to access apps that support OAuth, they're out of luck. Employees will have to separately track passwords for sites and apps that don't support your SSO. Moreover, SSO does not protect mission-critical non-password credentials, such as cloud infrastructure, API keys, SSH keys and digital certificates.

Typical Use Case

Cloud-first or cloud-only businesses with users who need to access a known and finite number of applications, such as companies that use the Microsoft 365 ecosystem.

PRIVILEGED ACCESS MANAGEMENT (PAM)

Purpose

Privileged Access Management (PAM) is used to restrict and monitor access to an organization's most critical and sensitive systems while also abiding by regulatory and industry compliance requirements. Privileged users are typically IT and security admins, C-level executives and other high-level individuals. In addition to preventing cybercriminals from stealing privileged users' credentials, PAM systems prevent these users from misusing their access. Typical features of a PAM system include password vaulting, session logging and tracking, 2FA and automated provisioning and deprovisioning.

Advantages & Disadvantages

Unlike SSO, which only governs user access, PAM enables granular permissions and role-based access control (RBAC). It generates comprehensive reports and audit trails to enhance security and support stringent IT compliance standards and it alerts administrators to suspicious behavior that might indicate misuse or a stolen password.

However, PAM is highly complex and costly to set up, and it requires substantial time, money and expertise to maintain. It's not a realistic option for budget-minded SMBs. Additionally, PAM isn't meant to be a comprehensive IAM solution; it is designed to secure only a small subset of credentials belonging to a small number of high-level employees.

Typical Use Case

Large enterprises or multinationals with substantial budgets and in-house IT resources, especially businesses operating in high-risk industries, such as finance, that are subject to very strict regulations and IT compliance mandates.

ENTERPRISE PASSWORD MANAGEMENT (EPM)

Purpose

A password manager, such as Keeper's solutions for businesses, is a software application that allows users to securely store all of their login credentials in one centralized, private, encrypted repository. Similar to SSO, users memorize only one "master password," which is used to access all of the credentials in the repository. However, unlike SSO, password managers aren't session-based; they work with all websites, applications and systems and include additional features, such as strong password generators and password auto-fill. Robust password managers also include advanced features such as: support for 2FA; secure storage of other confidential information such as access credentials, metadata, documents and media files; the ability to share with family, friends and colleagues; and warning users if they are duplicating passwords across multiple accounts.

Advantages & Disadvantages

Password managers are cost effective, easy to set up and maintain and easy to use, even by non-technical employees. They cover all employees, websites and apps, including employees' personal accounts. They simplify and enforce password best practices, such as strong passwords and not reusing passwords across multiple websites and applications.

However, like any cybersecurity solution, password managers aren't a panacea. For best results, they must be paired with 2FA, Role-Based Access Control (RBAC) and other security measures, such as network logging and monitoring.

Typical Use Case

Password managers are a particularly good solution for SMBs that don't have large IT budgets or extensive, in-house security expertise. However, even the largest enterprises benefit from using password managers. They can be used alongside SSO, PAM and other IAM and security solutions and, in fact, augment them with an additional layer of protection.

CHOOSING THE RIGHT IAM SOLUTION FOR YOUR BUSINESS

A comprehensive IAM strategy is a layered approach that combines SSO, PAM and a password manager with 2FA, RBAC and other security measures, such as monitoring end user behavior for unusual login activity. This approach is out of reach for most SMBs -- but that shouldn't discourage them, especially since a password manager and 2FA may cover the overwhelming majority of their needs.

Large enterprises and multinationals with highly complex data environments and expansive security budgets should utilize a comprehensive SSO/PAM/Enterprise Password Manager (EPM) solution. SMBs must balance their budget and internal resources with the needs of their IT department and the needs of their end users. There are two choices.

SSO & Password Manager Together

If your organization already uses an SSO solution or is thinking of implementing one, you should pair it with a password manager. An SSO by itself has major functional and security gaps. First, they only cover SSO-compliant, cloud-based applications and second, they perform authentication, not end-to-end encryption. When an SSO and Enterprise Password Management solution is used together, they cover secure authentication and end-to-end encryption across every cloud application, native application and further, the protection of metadata and files in a ubiquitous digital vault.

Password Manager Alone

If you can choose only one IAM solution, go with a password manager and pair it with 2FA and RBAC. Password managers provide great security coverage and value. They're also easy to set up and maintain, and they're user-friendly even for non-technical staff.

WHY KEEPER?

Not all password managers are created equal. Some are more difficult to set up and maintain, particularly when integrating them with SSO or 2FA.

Keeper's business and enterprise password management solutions help thousands of companies all over the world prevent password-related data breaches, improve productivity and enforce compliance with industry-leading features such as:

Exclusive, proprietary zero-knowledge security architecture

Three-in-one solution for small businesses; use Keeper as your password manager, SSO and PAM

Ease of use for both IT admins and end users; rapid deployment on all devices with no upfront equipment or installation costs

Personalized onboarding and 24/7 support and training from a dedicated support specialist

Support for RBAC, 2FA, auditing, event reporting and multiple compliance standards, including HIPAA, DPA, FINRA and GDPR

Seamless integration with SSO; no need for separate logins

Secure storage for sensitive files, documents, photos and videos on unlimited devices

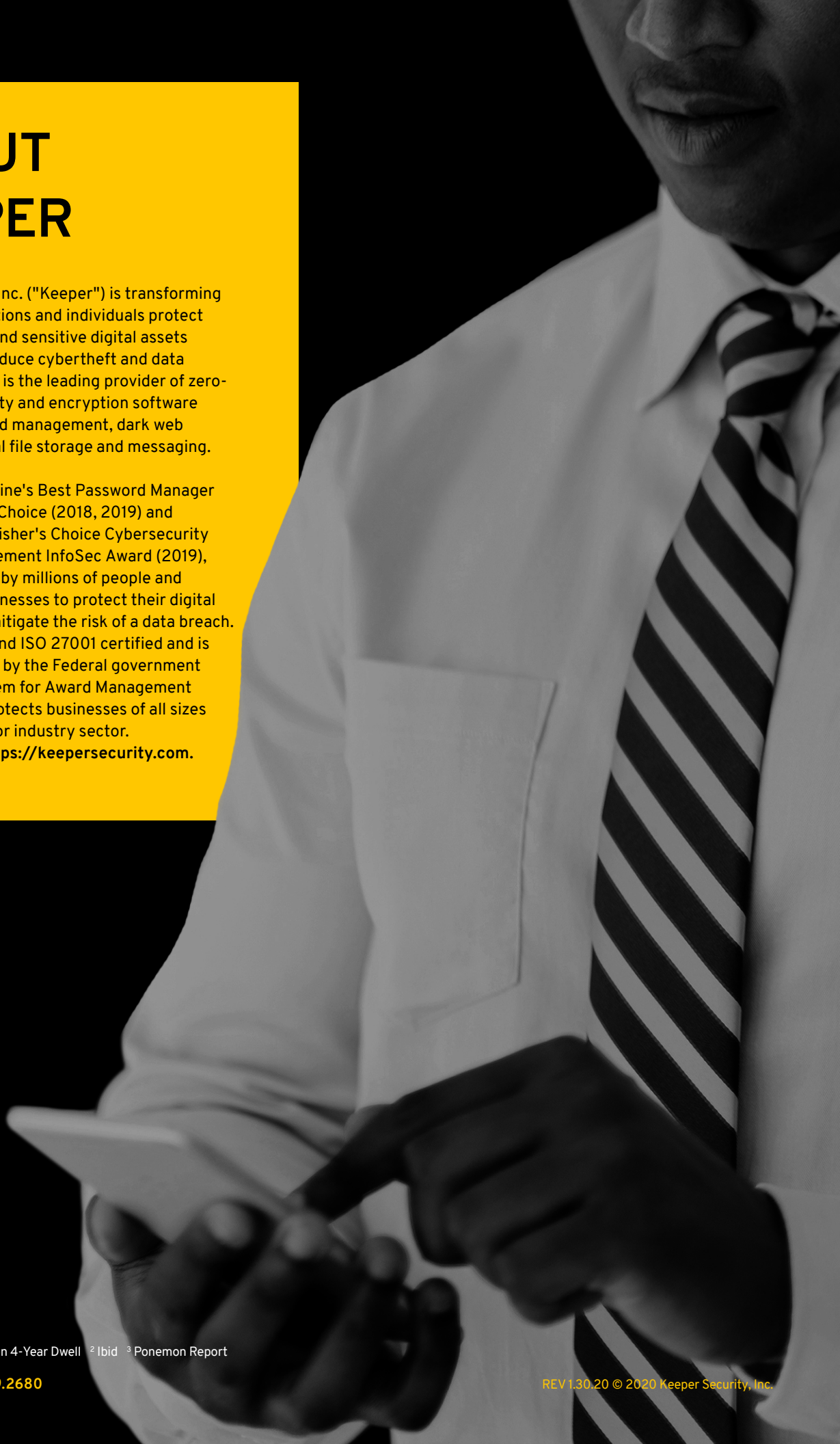
Private vaults for each employee, plus shared folders, subfolders and passwords for teams

Complete flexibility; whether your organization is a tiny startup or a multinational enterprise, Keeper scales to the size of your business

ABOUT KEEPER

Keeper Security, Inc. ("Keeper") is transforming the way organizations and individuals protect their passwords and sensitive digital assets to significantly reduce cybertheft and data breaches. Keeper is the leading provider of zero-knowledge security and encryption software covering password management, dark web monitoring, digital file storage and messaging.

Named PC Magazine's Best Password Manager (2018) & Editors' Choice (2018, 2019) and awarded the Publisher's Choice Cybersecurity Password Management InfoSec Award (2019), Keeper is trusted by millions of people and thousands of businesses to protect their digital assets and help mitigate the risk of a data breach. Keeper is SOC2 and ISO 27001 certified and is also listed for use by the Federal government through the System for Award Management (SAM). Keeper protects businesses of all sizes across every major industry sector.
Learn more at **https://keepersecurity.com.**



Sources:
[1] Starwood Breach Reaction Focuses on 4-Year Dwell [2] Ibid [3] Ponemon Report