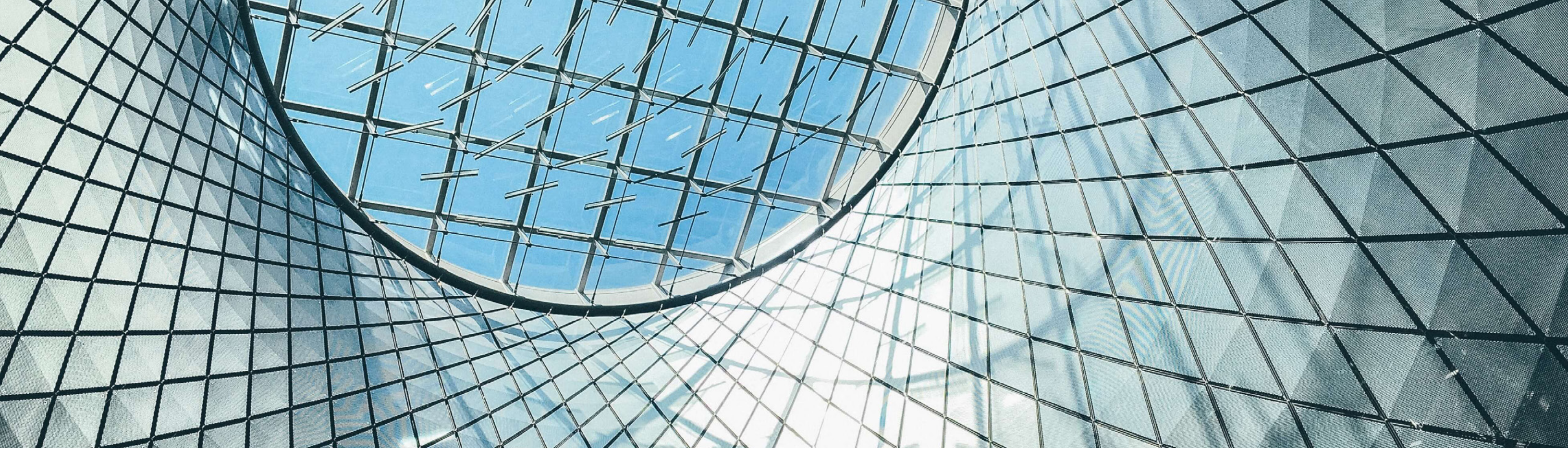


Market Insight Report Reprint

Coverage Initiation: Keeper Security embraces PAM from password manager roots

September 26 2023

by Garrett Bekker

Keeper Security has ventured beyond its enterprise password management roots to build a full cloud-based privileged access management offering with the goal of extending PAM functionality to every user, on every device and from any location.

S&P Global
Market Intelligence

Introduction

According to 451 Research's Voice of the Enterprise survey data, managing passwords, ensuring employees have appropriate access, managing admin accounts and deploying privileged access management (PAM) tools are among the top enterprise pain points (see figure below) when it comes to identity and access management. Keeper Security has ventured beyond its enterprise password management roots to build a full cloud-based PAM offering with the goal of extending PAM functionality to every user, on every device and from any location.

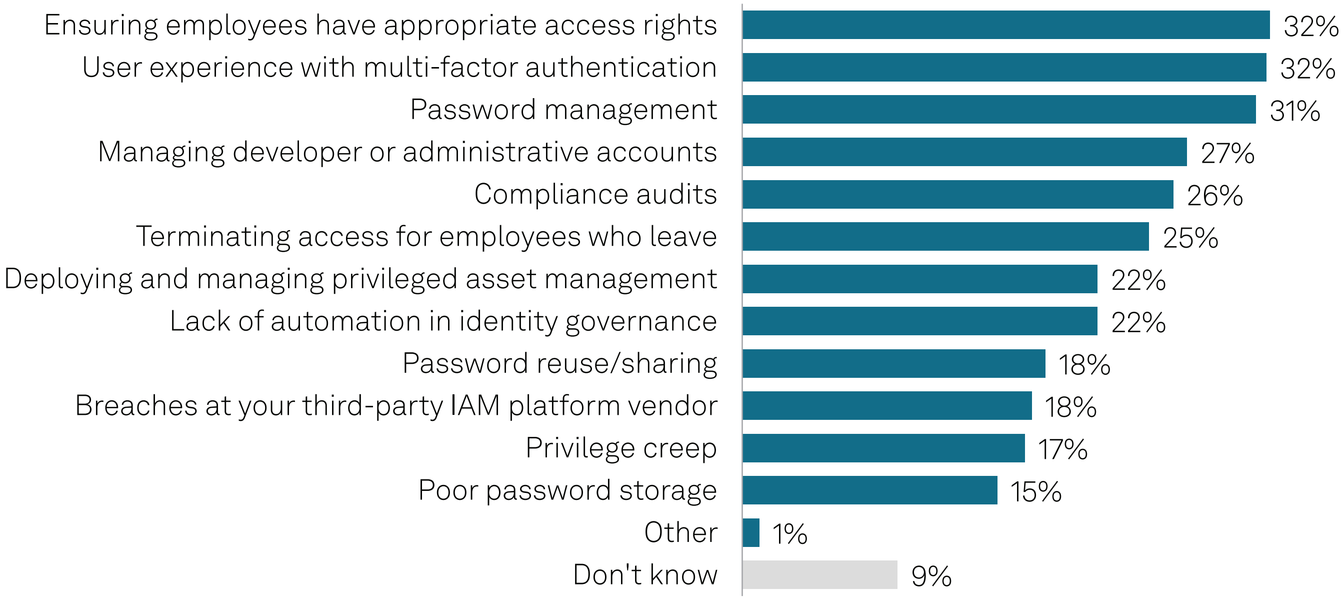
THE TAKE

There is a reason why PAM deployments trail other security tools — they are traditionally complex, expensive and hard to deploy. Keeper's overall goal is to make it easier to deploy PAM, and its fully cloud-based, distributed architecture could provide opportunities with organizations that do not have the resources (or patience) to deal with legacy PAM deployments. The company has strong growth equity funding, with a highly disciplined and focused go-to-market model that ranges from consumers and small office/home office accounts to large enterprises and government agencies with complex PAM needs. That said, Keeper is fairly new to the PAM game, and has less market awareness than more established PAM vendors. It is also entering one of the more competitive markets in security.

Context

Keeper Security was founded in 2011 by CEO Darren Guccione and CTO Craig Luney. The company is headquartered in Chicago, with additional offices in California, Japan, Ireland and the Philippines. It has roughly 350 employees, 90% of whom work remotely. Keeper started with a business-to-consumer focus, but business to business is now 65% of revenue, and B2C makes up the remaining 35%. Keeper did not take outside equity until it hit $40 million ARR, and is now funded by growth equity investors Insight Partners (Mike Triplett and Thomas Crain) and Summit Partners.

Figure 1: Identity management and governance pain points



Q. What are your organization's key pain points when it comes to identity management or governance? Please select all that apply.

Base: All respondents (n=479).

Source: 451 Research's Voice of the Enterprise: Information Security, Identity Management 2022.

Products

Keeper offers three main products: its Enterprise Password Manager (EPM), as well as the more recent Keeper Secrets Manager (KSM) and Keeper Connection Manager (KCM). Collectively, these three products comprise what Keeper calls its “next-gen PAM” platform, KeeperPAM. The offering is built on zero-trust and zero-knowledge security principles (the company’s employees can never view unencrypted data, which is encrypted and decrypted locally on the user’s device).

EPM is Keeper’s flagship product, and still accounts for the majority of revenue. EPM provides standard capabilities, such as the ability to discover, share and rotate passwords. It is also useful for applications that do not support modern authentication protocols like SAML or OIDC. EPM can store shared passwords and TOTP (time-based one-time password) codes. In addition to EPM, KeeperMSP is a modern, multi-tenant hosted SaaS password manager built specifically for managed service providers.

KSM was launched a year and a half ago, after Keeper saw demand for the same vaulting, logging and reporting capabilities for DevOps environments as it had for human credentials. Keeper Vault is a secrets manager that can store secrets (API keys, database credentials, certificates, logins or generic encryption keys) — Keeper calls them record types — for applications, servers, databases or other resources. Record types can also attach files and be customized to store things such as access keys for cloud providers like AWS or Azure. Keeper also provides custom templates in the vault that can store structured data.

It is worth noting that Keeper has cloud integrations that allow KSM to be used either as a replacement for a cloud provider’s key management system or as a “single source of truth” that will sync to an organization’s various cloud key management systems. Current integrations allow developers to hook directly into GitHub Actions, Ansible and Docker, and publish infrastructure without potentially leaking hard-coded credentials, to reduce or eliminate secret sprawl. Keeper does not have a hardware security module, but since all encryption is local and not on Keeper’s infrastructure, organizations can still meet FIPS requirements. Keeper also has FIPS-certified encryption libraries. KSM also provides a command line interface and software development kits in many languages in order to pull keys on the fly.

KCM is an agentless desktop gateway for privileged session management based on technology acquired from Glyptodon in 2021. Glyptodon had a commercial version of Apache Guacamole that was retooled, integrated into the Keeper platform and renamed Keeper Connection Manager early in 2022. Users can log into KCM via single sign-on and, once launched, jump straight into a target resource (Linux terminal, Windows instance, etc.) or other asset without logging into a VPN, just connecting via the organization’s identity provider (IDP) such as Okta or Microsoft Azure AD (now Entra). KCM supports all modern connection protocols like SSH, RDP and VNC, and has also build some app-specific protocols. The sessions can hide the passwords, so the user does not know the secrets in these privileged sessions. Privileged sessions can also be recorded and replay the history of everything that has taken place in a session.

Keeper’s admin console has a full audit and reporting engine for all event types — policy changes, logins, accessing records — that can also be safely pushed to third-party tools like Datadog or Elastic, since it contains no secrets. Breach Watch is a relatively new capability included in Keeper Vault that allows records to be scanned against Dark Web data breaches to see if any have been exposed. The intent is to identify records that may be at risk of an account takeover attack. Breach Watch can alert customers to records that might be at risk, and also evaluate password reuse and password strength.

In terms of architecture, Keeper is built on a cloud-based node architecture with delegated administration that allows customers to set up different organizational units or IDPs in the same console with their own respective policies.

Strategy

One of Keeper's key differentiators, in our view, is its detailed and focused go-to-market strategy, which has been informed by Insight Partners' and Summit's experience and leadership. Keeper's strategy rests on high-velocity demand generation with quick turns, similar to SolarWinds. SMB deals can be closed in 10 days, or 75 days for midmarket or enterprise deals. As noted earlier, the company started in 2011 with a B2C focus, but B2C is now about 35% of ARR, while the remaining 65% is B2B.

In terms of company focus, Keeper targets all company sizes, from a five-person doctor's office for basic password management to a 25,000-seat large enterprise with complex PAM requirements. SMB remains the biggest segment in terms of the number of customers. The company also does substantial business in midmarket enterprises, which have the same complex needs as large enterprises but are simply smaller. Keeper competes on ease of use and deployment, particularly for complex workloads. The company also targets the public sector (federal, state and local government and higher education) and is both FedRAMP and StateRAMP authorized. To best address each segment, it has dedicated teams for marketing, demand generation, content and sales for each market segment. The product can be tailored specifically to each segment, and scaled up or down accordingly. Keeper recently expanded internationally, with a new Asia-Pacific headquarters in Tokyo that opened in March.

Competition

In its core password management segment, Keeper is most likely to encounter the likes of LastPass, BitWarden and 1Password. The PAM space is more hotly contested, with roughly 40 vendors all-in, including market leaders such as CyberArk Software Ltd., BeyondTrust and Delinea (formerly Thycotic Centrify). Additional PAM vendors include cloud-native-focused newcomers HashiCorp and Akeyless, as well as Senhasegura, Teleport, StrongDM, Manage Engine, One Identity, Netwrix (via the StealthBits and Remediant acquisitions), ARCON, Wallix, Devolutions, EmpowerID, Fudo Security, OnionID and Imprivata (Xton).

SWOT Analysis

STRENGTHS

Keeper has a fully cloud-based architecture and strong backing from Insight and Summit Partners, with a highly disciplined and focused go-to-market model.

WEAKNESSES

Keeper is fairly new to the PAM game and has less market awareness than more established PAM vendors.

OPPORTUNITIES

PAM deployments tend to trail other security tools, in part due to the challenge of deploying and managing PAM products. Keeper will likely use EPM as a wedge in the door to upsell Secrets Manager and Connection Manager.

THREATS

PAM is one of the more competitive markets in security with over 40 participants, ranging from established legacy PAM vendors with substantial installed bases to newer vendors with specific expertise in cloud-native environments.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively, S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers, (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global Market Intelligence does not endorse companies, technologies, products, services, or solutions.

S&P Global keeps certain activities of its divisions separate from each other in order to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain non-public information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its websites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.