EMA
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

EMA Radar™ for Privileged Access Management (PAM)

Keeper Security Vendor Profile

August 2023
By Steve Brasen, Research Director
Endpoint and Identity Management

KEEPER

Overview

Keeper's patented PAM solution was designed to enable organizations to achieve complete visibility, security, control, and reporting across every privileged user on every device in their organization. The platform incorporates a zero-trust and zero-knowledge security architecture that consolidates three integrated product sets—enterprise-grade password management, secrets management, and privileged connection management—into one unified SaaS platform. KeeperPAM works out of the box with password rotation, passwordless authentication, SSO, SIEM, SDK, MFA, and CI/CD applications. The solution also performs security audits on password strength and reuse in the end-user's vault, and the included BreachWatch features includes a dark web scan to identify compromised credentials.

Headquarters:

Chicago, IL

Territories Supported with a Regional Office:

- North America
- Europe-Middle East-Africa (EMEA)
- Asia Pacific (APAC)

Company Website:

www.keepersecurity.com

Product Name:

KeeperPAM

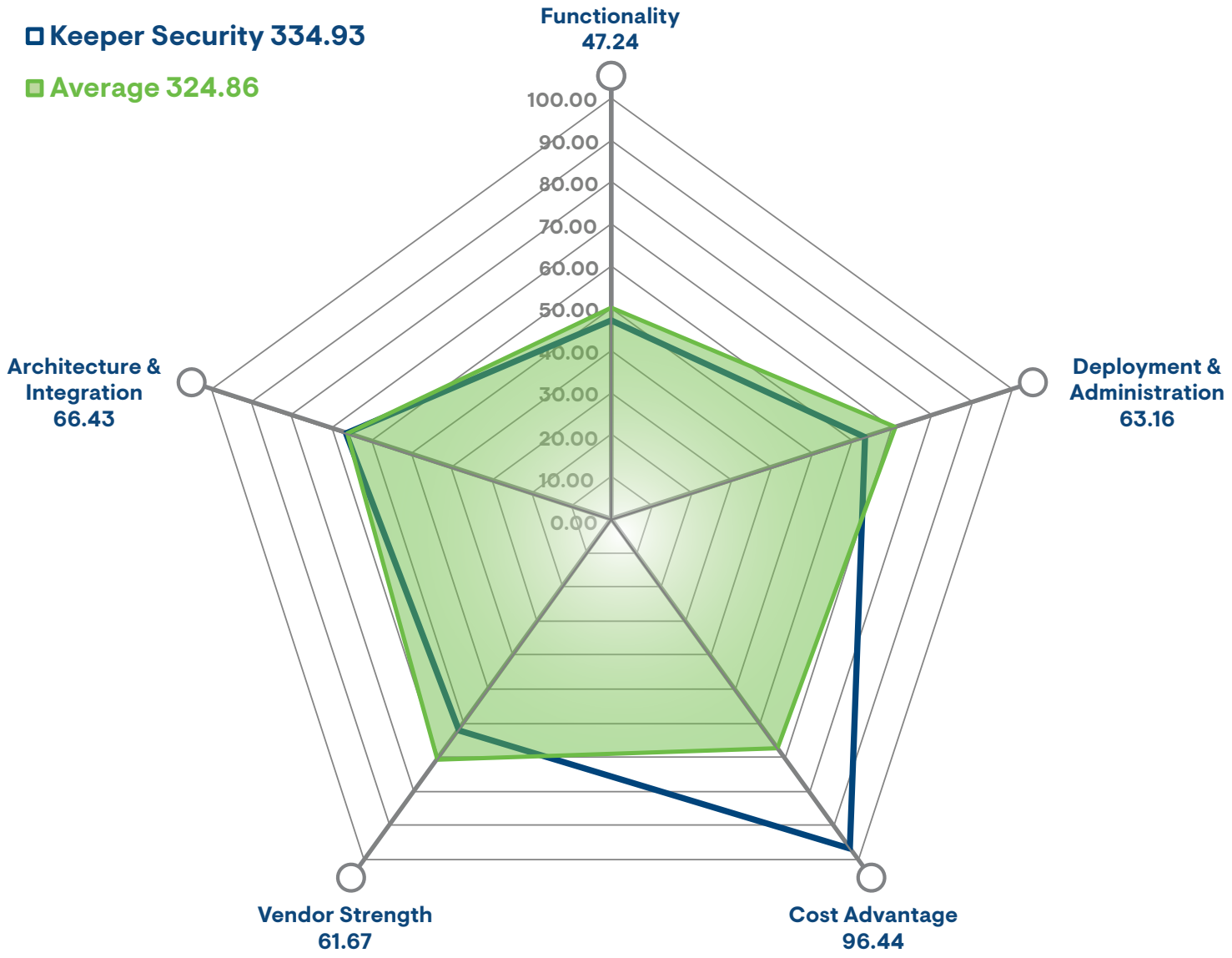
Architecture:

Cloud-based SaaS solution

Notable Features:

- Secure password vault
- Security audit and dark web monitoring
- Clientless and agentless remote access
- SAML-based SSO
- Automated credential rotation
- Secrets management

EMA RADAR


Keeper Security 334.93
Average 324.86
Functionality
47.24
Deployment &
Administration
63.16
Cost Advantage
96.44
Vendor Strength
61.67
Architecture &
Integration
66.43
100.00
90.00
80.00
70.00
60.00
50.00
40.00
30.00
20.00
10.00
0.00

Deployment & Administration

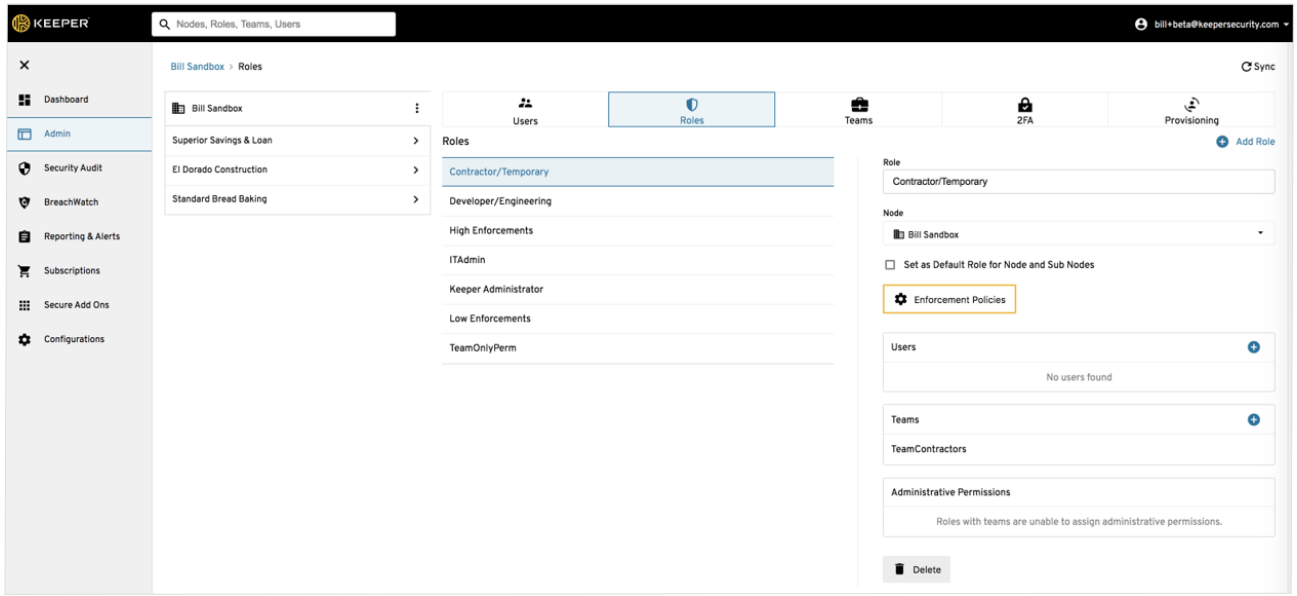
Deployment Complexity	
Ease of Deployment	Outstanding
User/Device Discovery	Solid
Agent Onboarding	Outstanding

Support and Services	
Customer Support	Strong
Community Services	None
Professional Services	Solid

Ease of Administration	
Console Ease of Use	Strong
User and Group Management	Strong
Policy Creation/Orchestration	Limited
Reporting and Dashboarding	Strong

KeeperPAM is principally adopted as a cloud-hosted SaaS solution that does not require any on-premises infrastructure deployments. The platform operates agentless and clientless, so no additional software deployments are needed. Users and devices may be automatically discovered in third-party directory services (e.g., Active Directory). The unified console is easily accessible via a web browser or a downloadable app for PC and mobile devices. Policies can be defined for a variety of identities, including employees, service providers, and non-human entities, as well as groups of users based on common job roles, employed devices, or organizational structures. The included Advanced Reporting and Alerts Module provides reports on over 200 event types. Keeper Security provides online product documentation and offers maintenance contracts that provide live help desk support accessible via a web portal. Professional services are also offered to support product implementations, training, and problem remediation.

Keeper Security Management Console



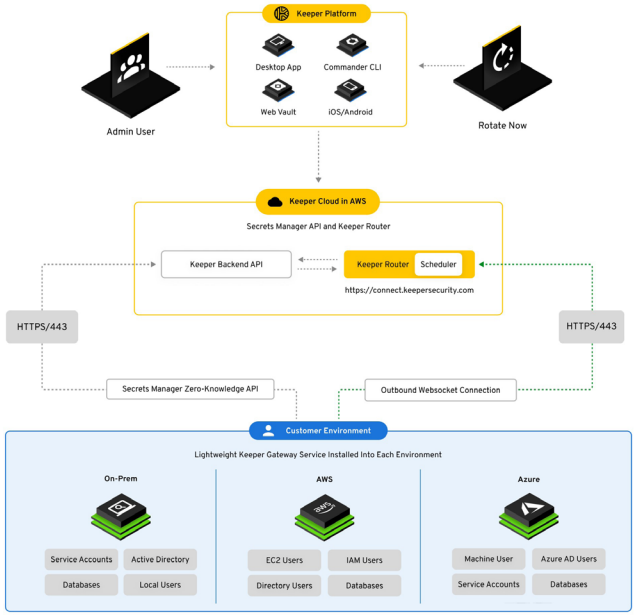
Architecture & Integration

Architecture	
Deployment Flexibility	Solid
Managed Resources	Strong
Directory Architecture	Strong
Data Residency	Strong
Infrastructure Certifications	Strong
Guaranteed Uptime	Strong
Supported Protocols	Strong
Platform Agent Architecture	N/A
Scalability	Strong

Integrations	
Direct (Prebuilt) Integrations	Solid
APIs & SDKs	Outstanding

While most KeeperPAM adopters employ the platform as a vendor-hosted SaaS solution, Keeper Security does offer an optional on-premises deployment of certain solution components to support unique security and business requirements. The solution manages cloud-hosted applications as well as on-premises servers and desktops. Shared secrets and other data are stored on the solution's proprietary SaaS vault and may be collected from third-party directories, such as Active Directory or LDAP, using the on-premises Keeper Gateway. The cloud solution infrastructure includes several certifications, including FedRAMP (moderate), CSA STAR, ITAR, SOC2, ISO27001, and FIMPS 140-2. The service is also StateRAMP authorized and validated by NIST SMVP. Regions supported with data residency include North America, Europe, and Asia-Pacific (APAC). KeeperPAM communicates with cloud-hosted applications using SAML and SCIM protocols. The solution includes several dozen connectors for access to web applications, as well as direct integrations with third-party security, data analysis, password stores, and multi factor authentication solutions. Additional custom integrations may be developed using the provided REST APIs and SDKs.

KeeperPAM System Architecture Diagram



Functionality

Privileged Access Lifecycle Management	
Onboarding	Strong
User Status Change Detection	Strong
Privileged Access Governance	Limited

Authentication and Secrets Management	
Secrets Vaulting/Storage	Outstanding
Password Management	Outstanding
Password Sharing	Outstanding
Non-Human Access Management	Strong
Second-Factor Authenticators	Outstanding
Passwordless Authentication	Strong

Least Privilege Access	
Just-In-Time Access	None
Contextual Awareness	Limited
Adaptive Access	Solid
Continuous Authentication	None

Threat Detection & Response	
Threat Discovery	Strong
Threat Response	Limited
Privileged User/Session Monitoring	Strong

Intelligent Evaluation	
Intelligent Risk Detection	Limited
Risk Scoring	Solid
Group Intelligence	None
Recommendations and Modeling	None

KeeperPAM automatically provisions detected users to managed systems and applications, granting privileges based on developed group policies. Any changes in a user's status, such as with role changes or terminations that are recorded in a directory service, are automatically synchronized with the PAM platform. User accounts may be deactivated without fully removing account information to accommodate a leave of absence and accounts may be fully removed after a defined period.

The Keeper vault is able to store any type of confidential information by leveraging Keeper's proprietary zero-knowledge and encryption technology. Passwords are checked for complexity, uniqueness, and whether they have been compromised and posted on the dark web. Policies can define settings for password expiration, password resets, account locking, and endpoint screen locking. Several effective methods are provided for users and teams to securely share passwords and other sensitive information. The solution can also manage authentications from non-human entities, such as applications and IoT devices. Second-factor authenticators are natively provided supporting one-time passwords and push notifications, and broad passwordless authentication is enabled with FIDO2 support.

Policies can be created to authorize or deny access based on the physical location of the user and networks over which they are communicating. Additionally, the solution can natively integrate with third-party SIEMs and security solutions to identify risky conditions. The included Keeper Connection Manager provides secure, VPN-less remote access and enables full session recordings, capturing videos of user displays and logs of privileged user actions.

Cost-Efficiency

Pricing Model	
License Costs	$
Maintenance Costs	$$
Infrastructure Costs	None (SaaS) $$$ (on-premises)

$ = Very inexpensive
$$ = Somewhat inexpensive
$$$ = Moderately priced
$$$$ = Somewhat expensive
$$$$$ = Very expensive

KeeperPAM components are principally offered for annual subscription licenses priced by number of users. The Secrets Management with Password Rotation module is a metered service priced by the number of API calls per month. While software maintenance is included with subscriptions, customers incur an additional charge (priced as a percentage of the total purchase cost) for platinum help desk support, onboarding, and training. The solution is most commonly adopted as a cloud-hosted SaaS platform, requiring no additional infrastructure purchases. However, the vendor also offers an optional on-premises software edition that would necessitate the deployment of a hosting server, virtual instance, or private cloud instance.

Vendor Strength

Pricing Model	
Vision	Strong
Strategy	Strong
Financial Strength	Solid
Research and Development	Solid
Partnerships and Channels	Strong
Market Credibility	Solid

Keeper Security's vision for its PAM platform is to provide zero-trust and zero-knowledge security and compliance by delivering full visibility, security, control, and reporting across every user on every device. The vendor's strategy is to deliver a low-cost and easy-to-deploy platform that includes broad functionality, including password management, dark web monitoring, secure file and secrets storage, compliance reporting and alerting, session monitoring, and secure messaging. Keeper Security is privately owned, and backed by Insight Partners and Summit Partners. The company does not publicly disclose financial information; however, EMA was informed that it is profitable and growing. Keeper Security is committed to a 100% channel model in EMEA markets, operating through distribution and reseller networks.

Special Award – Best Password Sharing

KeeperPAM natively includes advanced functionality for enabling administrators to securely share privileged account passwords for individuals and groups—including root and administrator accounts—without exposing clear text credentials. Three unique methods for password sharing include Shared Folders, providing the ability to share permissions for accessing records and subfolders with specified users and teams; Direct Sharing, enabling the sharing of an individual record with another Keeper user; and One-Time Share, securely sharing a record or file with a hyperlink to users outside the organization who may or may not be a Keeper user. Policies can be created to govern password sharing access based on user roles, and authorized teams can be created within the administration console through the Active Directory Bridge or via SCIM synchronization with cloud identity providers. Sharing uses Elliptic Curve (EC) and AES-256 bit encryption technology to preserve zero knowledge and ensure that shared record recipients can only decrypt the credentials and data they are provisioned. EMA's evaluation of the PAM market space indicates that Keeper Security provides the most comprehensive and easy-to-use methods for securely sharing privileged access passwords.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at **www.enterprisemanagement.com** You can also follow EMA on **Twitter** or **LinkedIn**

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com**

4307.082823-Keeper Security