EMA
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

EMA Radar™ for Privileged Access Management (PAM)

Summary Report Spotlighting Broadcom

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

Table of Contents

Executive Summary

Privileged access management (PAM) defines, controls, and manages access to an organization's most sensitive accounts, systems, and applications, meriting it as one of the most critical IT security practices. Related solutions are responsible for centrally defining privileged access policies, governing account creations and changes, recording and auditing privileged activities, and enforcing least privileged access controls. This Enterprise Management Associates® (EMA™) Radar Report™ identifies the 11 leading PAM solution providers on the market today—Amitego, BeyondTrust, Broadcom, CyberArk, Delinea, Devolutions, Keeper Security, One Identity, Netwrix, Saviynt, and Senhasegura—and empirically compares and grades their offered solutions against a broad range of measurements to determine overall product strengths and cost-efficiencies. The goal of the research results is to provide purchasing guidance on the optimal solutions to adopt to meet an organization's unique business requirements. EMA identifies Value Leaders as those that deliver strong products and platform architectures for a comparatively low total cost of ownership.

Understanding Privileged Access Management

Protecting the Most Sensitive Business IT Assets

In the early days of computing when processes were developed for user accounts and permissions, the need for specialized master accounts that enable unmitigated access to all system resources was essential to IT administration. In Unix and Linux, these are known as "root" accounts, while Windows and Macs refer to them as "administrator" accounts. These accounts were necessary to allow authorized individuals to manage and maintain system and security resources (such as kernel, registry, and password files) that should never be accessible to the average user.

Over time, additional features were added to operating systems that allow standard user accounts and custom scripts to have elevated permissions to perform specific tasks. For example, "setuid" scripts, sticky bits, and "sudo" commands can be used to allow users to access privileged files or perform privileged activities. This more granular control allows the designation of access to specific files or executables without needing to grant carte blanche authorization to all system resources.

Unfortunately, the proliferation of elevated user privileges proved to be susceptible to broad misuse and exploitation. Common scenarios in most organizations involved the granting of privileged access in order to enable a user to address a specific need, but failing to remove the permissions and allowing the user's access to persist long after the initial problem was resolved. Among hackers, these standing account privileges are the brass ring of breach events. If a malicious actor gains access to a privileged account or a standard user account with elevated privileges, they gain unfettered access to view, damage, steal, and manipulate the business's most critical IT resources.

Privileged access management (PAM) best practices and solutions were developed specifically to establish control over the provisioning and use of elevated permissions. PAM lies at the core of every modern enterprise IT security strategy. In fact, EMA research confirmed that 79% of organizations consider PAM to be very important or critical to their business operations.[1]

[1] Advancing Privileged Access Management (PAM) to Address Modern Business Requirements

The Scope of Privileged Access Management

The practices associated with PAM vary depending on an organization's security posture and business requirements. For instance, highly regulated organizations—such as government, health care, and financial institutions—require more stringent controls over privileged accounts. Companies with fewer security concerns may be more liberal in assigning access privileges to improve business agility and workforce performance. Regardless of the approach, several key practices should be considered essential to any PAM deployment. These include:

The Identification of Privileged Accounts

Existing privileged accounts and authorizations should be identified for all IT resources the business manages. These include servers, applications, cloud-hosted resources, and endpoint devices.

Onboarding Privileged Users

Users should have the ability to request privileged access to business IT resources. These requests should pass through a formal approval process with designated stakeholders providing written and verifiable authorizations.

Enforcement of Least Privilege Access

The Principles of Least Privilege Access state that users should only be granted privileged access to the resources they absolutely require to perform business tasks. Minimizing access to unnecessary IT resources reduces risk profiles and limits the amount of damage that can be done from a compromised account.

Privileged Access Audits

All privileged activities should be centrally recorded so they can be reviewed to assist with periodic audits and troubleshooting. Privileged actions, including any files that were changed or programmatically created, should be identified and associated with the user that performed them. This also adds a level of accountability and enables the easy acquisition of proof of compliance.

Offboarding Privileged Users

When users no longer require privileged access—such as following an employee termination--their permissions and accounts should be immediately and automatically disabled.

Emerging Changes to the Privileged Access Management Market

Traditionally, enterprises regarded PAM as an independent practice of general identity and access management (IAM), which governs the authentication and access policies of standard user accounts. The two management disciplines involved separate administration processes and tools, with PAM enforcing more stringent monitoring and authorization controls. In recent years, however, the lines between IAM and PAM have substantially blurred. Most enterprise-class IAM platforms now incorporate at least some PAM functionality.

Substantial industry consolidation that saw the merger of respective product sets through acquisitions drove the convergence of PAM and enterprise IAM. Among the many advantages to a unified solution, fully integrated platforms allow organizations to take advantage of consistent and centralized administration consoles and the sharing of a common set of user, system, and contextual information.

Additionally, with converged product sets, IAM solutions can take advantage of features that traditionally were considered PAM functionality. This is most notable with the proliferation of just-in-time (JIT) access, which was developed specifically to establish on-demand access to privileged accounts. Today, however, IAM platforms widely employ JIT solutions to create any on-demand access, such as to cloud-hosed apps.

Recent years also saw a rise in the use of intelligence technologies, including machine learning, cognitive computing, analytics, and language processes. These resources are increasingly employed to aid with risk detection and scoring and vulnerability assessments and to provide recommendations for process improvements.

Points of integration have also accelerated as PAM solutions more broadly enable the acquisition of data points from third-party platforms. In particular, integrations with security information and event management (SIEM) systems and other security solutions have significantly increased the ability of PAM platforms to collect contextual information in support of conditional privileged access policies.

Looking forward, the convergence between PAM and enterprise IAM will continue, with the former likely to be fully absorbed by the latter. In the process, identity governance and administration (IGA) processes will also be more broadly incorporated as the connecting glue between the two disciplines. Ultimately, this is all leading to the availability of truly unified identity management platforms that promise to be easier to manage and more effective at securing business IT assets.

Assessing the PAM Market

Research and Methodology

To assist organizations in identifying PAM solutions that will most effectively meet their requirements for improving security postures while minimizing management efforts and related costs, EMA conducted a formal evaluation of the leading platforms available on the market today. To be clear, EMA defines "value" as the ratio derived from the strength of a product set against its total cost of ownership. Put simply, the more organizations pay for a solution, the greater the advantages they should receive in terms of breadth of functionality and supportability.

EMA's review process began with the determination of critical PAM features and capabilities. This list was used to establish evaluation KPIs that were ranked and weighted to correspond with the current requirements EMA has determined for organizations that have adopted or plan to adopt a PAM platform. The prioritization determinations were based on discussions with IT operations managers, survey-based research responses, and identity security administrator interviews, as well as EMA's own experience and knowledge of enterprise requirements and best practices. Evaluation KPIs focused specifically on supporting PAM functionality with the perspective that the solution would be adopted solely for this purpose, even if the platform supported other identity practices, such as enterprise IAM or IGA.

From these KPIs, a minimum level of functional requirements was established to identify which management platforms qualified for recognition as leading PAM solutions. Minimum requirements included providing support for most or all of the principal PAM practice elements. EMA reviewed more than 30 vendors claiming to offer functionality for monitoring and managing privileged access. Of these, EMA internally identified the leading contenders that were determined to offer sufficient functionality to warrant a detailed review. Each of these vendors was invited to participate in the in-depth evaluation process.

A detailed questionnaire on the capabilities, cost, and supportability of their respective product sets was submitted to each of the selected privileged access management solution providers. More than 400 points of comparison were considered, and all responses were carefully vetted for accuracy. Any vendors who did not participate in providing product information were evaluated based on publicly available sources including documentation, technical writings, video demonstrations, and other published resources. EMA also conducted interviews with vendor customers to confirm product capabilities and indicate customer satisfaction with the product sets.

Scoring of the vendor solutions was mathematically calculated by correlating available features, architectures, pricing, and capabilities with the predetermined KPIs. Some individual feature scores were adjusted based on firsthand customer experiences with the product sets exposed during the interviews. Final scoring of each product set was used in the creation of the product comparison charts and in the determination of award winners.

Notable Absences

Several of the vendors EMA reached out to during the evaluation process either failed to respond or requested not to be included in the review process and final report. EMA urges caution when adopting solutions from vendors that are secretive about their solutions. Notably absent vendors include:

- ARCON – Informed EMA that they were unable to participate due to internal constraints
- Bravura Security - Did not respond to EMA's request for information.
- Okta – Noted that the PAM product set was still in development and key features would not be released until after publication of the report.
- Opal - Did not respond to EMA's request for information.
- WALLIX – Informed EMA they were unable to provide the requested information.

Characteristics of a Preferred Solution

The EMA Radar Report evaluation process standardizes the review of product sets in specific management disciplines by comparing vendors and product characteristics in five distinct categories: architecture and integration, functionality, deployment and administration, cost advantage, and vendor strength. Identified in the following sections are the elements EMA believes are indicative of an ideal privileged access management solution in each of the primary evaluation categories.

Architecture and Integration

The ideal PAM solution is architected to centrally authorize privileged access, monitor their use, and enforce related security and regulatory policies. Scalability of the product set should be achieved by enabling expansion based on increasing enterprise requirements (i.e., a growing number of supported applications, expanded user support needs, etc.). Cloud-hosted services typically have an advantage over on-premises solutions for achieving scalability because they require no additional hardware or software installations to support increased support stack sizes. However, on-premises platforms may comply with policies for on-premises data storage and are often easier to integrate with third-party on-premises applications and servers. Hybrid approaches, incorporating on-premises and cloud components, can sometimes offer the advantages of both platforms. An ideal solution provides multiple deployment options so organizations can choose the architecture that best meets their unique business requirements.

If all or portions of the PAM platform are hosted on cloud services, the service provider should guarantee solution availability. To support requirements for data residency, business data stored on cloud services should be physically hosted within selectable geographic regions. Additionally, cloud platforms should be recognized as having completed and passed any applicable security and reliability assessments, such as with FedRAMP, CSA STAR, or FISMA certifications.

The vaults or directory services used to store shared secrets should be centrally managed within the PAM platform. If secrets are shared with multiple repositories, the PAM solution should federate the data with them to ensure real-time synchronization. Ideal PAM platforms will communicate with third-party directories, IDPs, and applications using a wide variety of protocols, most notably SAML, OAUTH, OpenID Connect, SCIM, RADIUS, and LDAP.

The executions of privileged access controls and the assessment of vulnerabilities and risks require broad visibility into contextual conditions and IT service states. No single PAM platform can be expected to natively collect this rich set of required information across all applications, devices, and hosted IT service supported across business environments. Integration with third-party IT resources, therefore, is an essential capability for any privileged access management solution. PAM platforms that include a broad range of direct integrations are more extensible and easier to deploy and maintain. EMA recognizes “direct integrations” as solutions that federate collected data, employ a common data collection process, enable task executions, and/or store data in a common repository without the need for additional coding or customization. IT management resources for which direct integrations are relevant to PAM solutions include:

- Security management platforms
- Systems management platforms
- Service management platforms
- Configuration management databases (CMDBs)
- Data/log analysis solutions

Since direct integrations cannot be included for all possible IT resources, the availability of robust APIs is essential for the easy establishment of custom integrations. Open APIs are particularly advantageous for allowing third-party solutions to leverage the extent of a PAM platform’s collected data and functionality. Alternatively (or additionally), a PAM platform may offer software developer kits (SDKs) that allow organizations to custom-code integration points or actions that are externally executable.

Functionality

PAM encompasses a broad range of capabilities that are essential for provisioning, monitoring, and governing privileged access. Some product sets include unique features that perform very specialized tasks, so each organization should carefully identify and prioritize which capabilities are most applicable to its business requirements before initiating a product comparison. For the purposes of this evaluation, EMA identified several key functional capabilities for achieving PAM requirements. While no offered platform will comprehensively include all noted capabilities, the number and strength of features supported provide an indication of how well a solution will address essential PAM goals. Evaluated features have been logically organized into five key areas.

Privileged Access Lifecycle Management

- **Onboarding** – Whenever possible, users and devices should be automatically detected and assigned appropriate access permissions based on roles and other characteristics.
- **User Status Change Management** – Whenever users change roles or leave the organization, any associated access privileges must be automatically and instantaneously revised or revoked.
- **Privileged Identity Governance** – To meet regulatory compliance commitments, audit processes and detailed reports should be provided to affirm appropriateness of privileged entitlements, including for attestations and separations of duties.

Authentication and Secrets Management

- **Secrets Vaulting/Storage** – The technology employed to store shared secrets, such as passwords and certificates, directly impacts the effectiveness and reliability of associated authenticators. Commonly, this highly sensitive information is stored in a vault, directory, and/or password manager.
- **Password Management** – Policies should be included that always enforce password complexity, uniqueness, and expiration in support of privileged accounts.
- **Password Sharing** – Organizations that permit the use of common privileged accounts (such as root or administrator accounts) should employ a mechanism that encrypts passwords so they may be utilized but are not visible to authorized users.
- **Non-Human Access Management** – Bots, applications, and other non-human entities that require permissions to perform privileged tasks should be managed by policies that recognize and monitor their autonomous activities.
- **Second-Factor Authenticators** – At least two factors of authentication directly supported by the PAM solution should always support privileged access processes. Common second-factor authentication options include time-based one-time passwords (OTPs) and push notifications.
- **Passwordless Authentication** – Industry standards, such as FIDO and WebAuthn, should be supported to enable the use of passwordless authenticators, such as security keys and biometrics.

Least Privilege Access

- **Just-In-Time Access (JIT)** – Optimal implementation of JIT eliminates the need for standing privileged accounts by temporarily creating accounts or elevating permissions to existing accounts that are disabled after the authorized privileged tasks are performed.
- **Contextual Awareness** – Detailed information on the users, devices, networks, and hosted services is essential to establishing conditional access policies. The richer the contextual dataset, the more granular and precise businesses can make their privileged access policies.
- **Adaptive Access** – Conditional policies should be able to define a variety of responses to contextual states, including forcing password resets, requiring additional factors of authentication, increasing the frequencies of reauthentications, or limiting access to specific files or applications.
- **Continuous Authentication** – To identify any environment changes that could elevate risk levels, contextual conditions should be continuously monitored rather than only during the initial authentication. Suddenly appearing threats should force reauthentication actions or disablement of privileges in real time.

Privileged Identity Threat Detection and Response

- **Threat Discovery** – Ideal PAM solutions should be able to detect identity threats, such as weak/compromised credentials, device vulnerabilities, stale accounts, and suspicious user behaviors.
- **Threat Response** – Detection of risky conditions should immediately trigger automated responses to remediate any deficient states.
- **Privileged User/Session Monitoring** – All privileged sessions should be recorded to ensure accountability and assist with problem investigation by identifying the specific actions that were performed, the individual that performed the actions, and the time the activities took place.

Intelligent Evaluation

- **Risk Detection** – Intelligence technologies, such as machine learning, cognitive computing, and analytics, should be employed to evaluate contextual information to assess risks in real time. These include the detection of suspicious login activities and user behaviors, as well as the identification of segregation of duties violations.
- **Risk Scoring** – Intelligent technologies should use conditional states and detected risks to calculate a numerical risk score. The risk score may be used as a simple metric in conditional policies to determine if privileged access should be authorized, limited, or denied.
- **Group Intelligence** – Intelligent peer group analysis identifies the distribution of privileged accounts in relation to organizational structures and user roles. This helps determine whether access privileges have been overprovisioned and determines any outliers that may have been inappropriately granted permissions.
- **Recommendations and Modeling** – Information should be provided to administrators on environmental changes that will improve privileged access security and mitigate potential threats. Hypothetical modeling proactively determines the impact of planned changes or conditions for privileged access authorizations and security.

Deployment and Administration

The ease with which a solution can be deployed is directly related to the complexity of the infrastructure supporting it. The more hardware and software elements need to be installed, the more challenging the deployment will likely be. An ideal solution will employ automation for enabling a turnkey deployment process, rapidly installing software components (such as databases, reporting engines, and console interfaces) and automatically detecting the mobile endpoints that will be supported. While cloud-hosted platforms typically do not require any on-premises software or hardware installation, organizations sometimes have the option of installing an on-premises staging area to host software elements, such as data repositories, to meet compliance and business requirements. If agents need to be deployed on managed devices, they should be automatically pushed from the console server or made available for download by the end user from a publicly available source (such as a web portal or app store).

Administration is simplified with an intuitive and customizable console interface that consolidates all PAM processes, dashboards, and reports. A mobile application or HTML5-based web interface that enables console access is advantageous for IT administrators who need to provide remote or out-of-hours support. The processes for collecting configuration and status data from applications and devices should be automated, requiring little or no administrative interaction. Dashboard views should be customizable and graphically display easily-digestible information, including aggregated risk scores, historical trends, and the status of privileged access certifications. Dashboard views and administration actions should adapt to individual roles.

PAM solutions should be able to manage all identity types, including employees, service providers, and non-human entities (applications, bots, and other automated IT services). Privileged access policies and reports should be easy to create and customize with prebuilt templates and workflow design engines.

Vendors must also display a commitment to supporting the PAM platform and its user community. Maintenance contracts should be offered that deliver responsive and continuously available live support, as well as timely product updates. Vendors should offer professional services staffed with support professionals who are knowledgeable about their solution set and management processes to assist customers with training, problem solving, environment optimization, and the initial product deployment. Vendors should also engage the user community by hosting online forums and regular conferences or meetings to educate organizations on the effective use of their platforms and on PAM best practices.

Cost Advantage

Pricing models for PAM platforms should be simple to understand and easy to calculate. PAM solution providers may offer one-time perpetual licenses or recurring subscription fees. Maintenance contracts, which provide access to platform updates and the vendor's help desk, are typically included with subscription licensing for no additional cost, but incur a recurring (e.g., annual) fee with perpetual licenses. Additionally, cost considerations should include any infrastructure expenses, such as for on-premises servers, appliances, databases, vaults, directories, gateways, virtual instances, or private cloud services.

Vendor Strength

Consumers should always be aware of a vendor's stability and its commitment to a platform prior to adopting the solution to be sure of its long-term viability. A vendor that is financially strong with high revenue and vast equity is more likely to continue to support a management platform. Solution providers that invest heavily in research and development will also be assured of maintaining continual value in the platform's architecture and feature set. Strategic and channel partnerships also increase vendor relevance in the marketspace, and customer loyalty provides visible credibility of the platform's favorability. Additionally, a vendor's vision and strategy for development, innovation, and foresight of future requirements indicates whether a management solution will maintain optimal value in constantly changing marketplaces.

Evaluation Criteria

Feature Eligibility

For a product set to be credited with a feature or capability in EMA's evaluation, it was required to meet three strict criteria.

1. The features needed to be generally available with the solution set at the time of the evaluation. Any features that were in beta testing or were scheduled to be included in later releases of the management suite were not eligible for consideration.
2. All features needed to be self-contained within the included package sets. Any features not natively included in the evaluated package sets, but available separately from the same vendor or third-party vendors for an additional cost, did not qualify.
3. All reported features needed to be clearly documented in publicly available resources (such as user manuals or technical papers) for verification of their existence and to ensure they are supported.

Financial Evaluation

To enable product license cost comparisons that are as fair as can possibly be attained through analytical processes, EMA developed six sample support models and applied vendor pricing to each. Pricing included subscription costs for all products, add-ons, and modules necessary to achieve the functionality credited in all other sections of this evaluation. Additionally, expenditures were added to account for any additional hardware and/or software infrastructure costs necessary for the platform to operate, and maintenance costs (if applicable) were calculated for the time specified in each model. The results for each of the six models were empirically rated on a pricing scale (i.e., rated from 1-10 with a two-decimal point level of accuracy). Ratings for all six models were then averaged to provide the final scoring reported in this evaluation. The six models used in EMA's evaluation are as follows:

- **Short-Term Small Business Model** – supporting 20 users over 3 years
- **Long-Term Small Business Model** – supporting 20 users over 7 years
- **Short-Term Medium Business Model** – supporting 250 users over 3 years
- **Long-Term Medium Business Model** – supporting 250 users over 7 years
- **Short-Term Large Business Model** – supporting 1,000 users over 3 years
- **Long-Term Large Business Model** – supporting 1,000 users over 7 years

Vendors that offer multiple product licensing and/or deployment models were evaluated across all potential scenarios, and the best scores achieved were calculated in the final tabulation.

Vendor Profile Feature Scorings

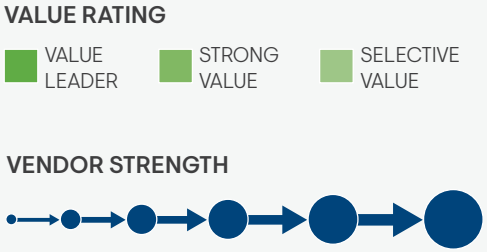
The scoring of solution features was achieved by comparing product and vendor characteristics against EMA's predetermined KPIs defining an optimal PAM solution. To bring visibility to EMA's evaluation results, the full vendor profiles included in this report provide indications on how EMA rated support in each reviewed category. Feature ratings are defined as follows:

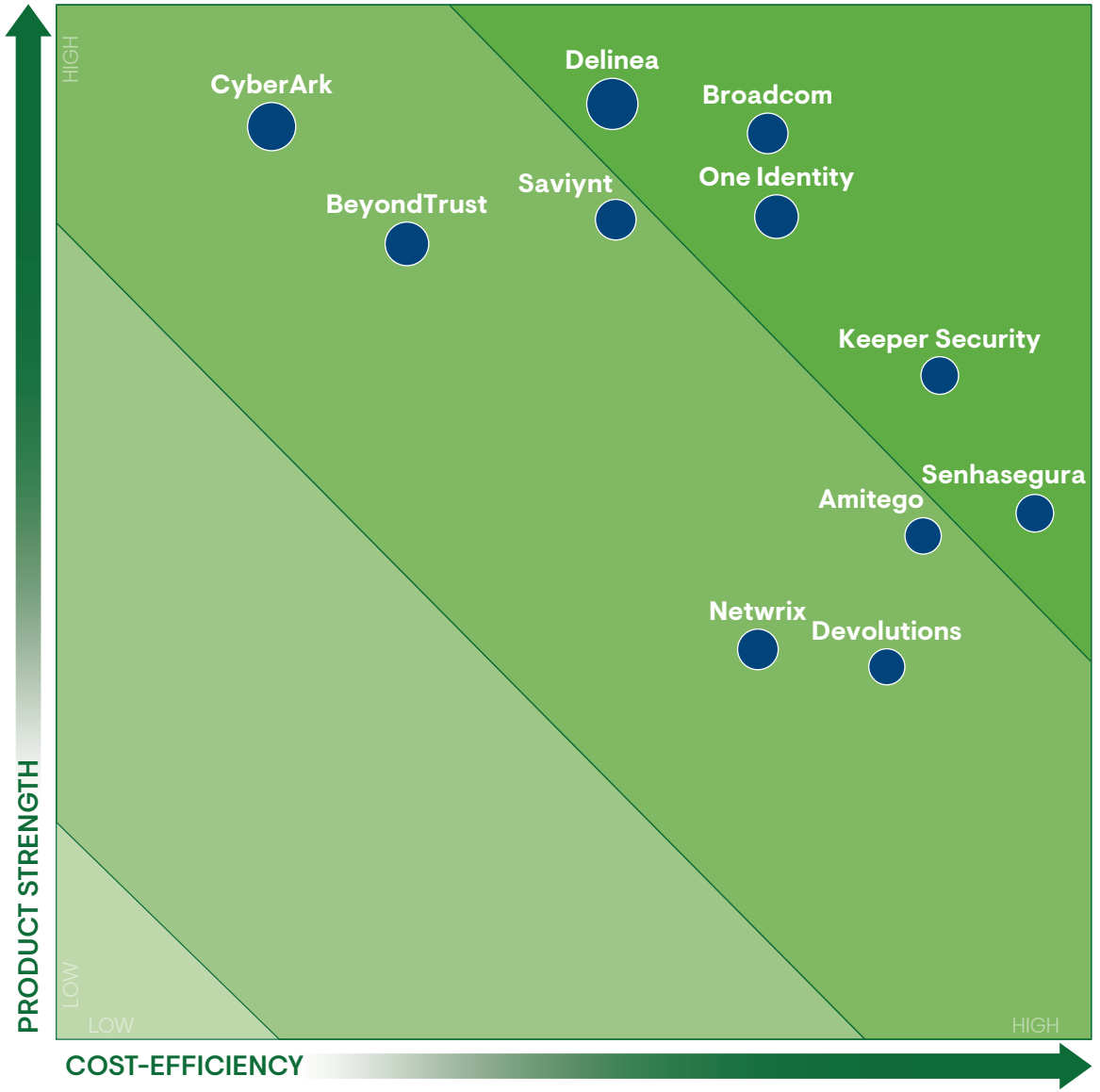
- **None** – The platform offers no features in this category
- **Limited** – The platform supports only a few EMA-defined requirements in this category
- **Solid** – The platform supports a moderate number of EMA-defined requirements in this category
- **Strong** – The platform supports most EMA-defined requirements in this category
- **Outstanding** – The platform features in this category exceed EMA-defined requirements

On the EMA Radar™

Privileged Access Management Market Overview

EMA defines value in any solution as a comparison of the strength of the platform against its total cost of ownership. The EMA Privileged Access Management Market Landscape Chart provides a graphical representation of evaluated industry leader positioning in relation to both critical axes. The "Product Strength" axis combines evaluation scores for Functionality with Architecture & Integration. "Cost-Efficiency" is calculated by adding the scores achieved for Cost Advantage and Deployment & Administration. The size of each bubble indicates the Vendor Strength as quantified in their individual profiles.





BROADCOM

Overview

Broadcom's Symantec Privileged Access Management is comprised of four product sets that may be purchased individually or together as a bundled offering. Privileged Access Management is a self-contained physical or virtual appliance for on-premises or cloud (AWS or Azure) deployment, supporting credential management, session management, access control, and application-to-application password management (AAPM). Users may optionally purchase AAPM separately as a software solution with the Privileged App-to-App Manager. Privileged Access Manager Server Control is a software-based solution that enforces access control over host servers. Also included with the base platform is Threat Analytics, a virtual appliance that continuously monitors privileged activity to detect unusual behaviors and assess risk.

Headquarters:

San Jose, CA

Territories Supported with a Regional Office:

All regions worldwide

Company Website:

https://www.broadcom.com

Product Name:

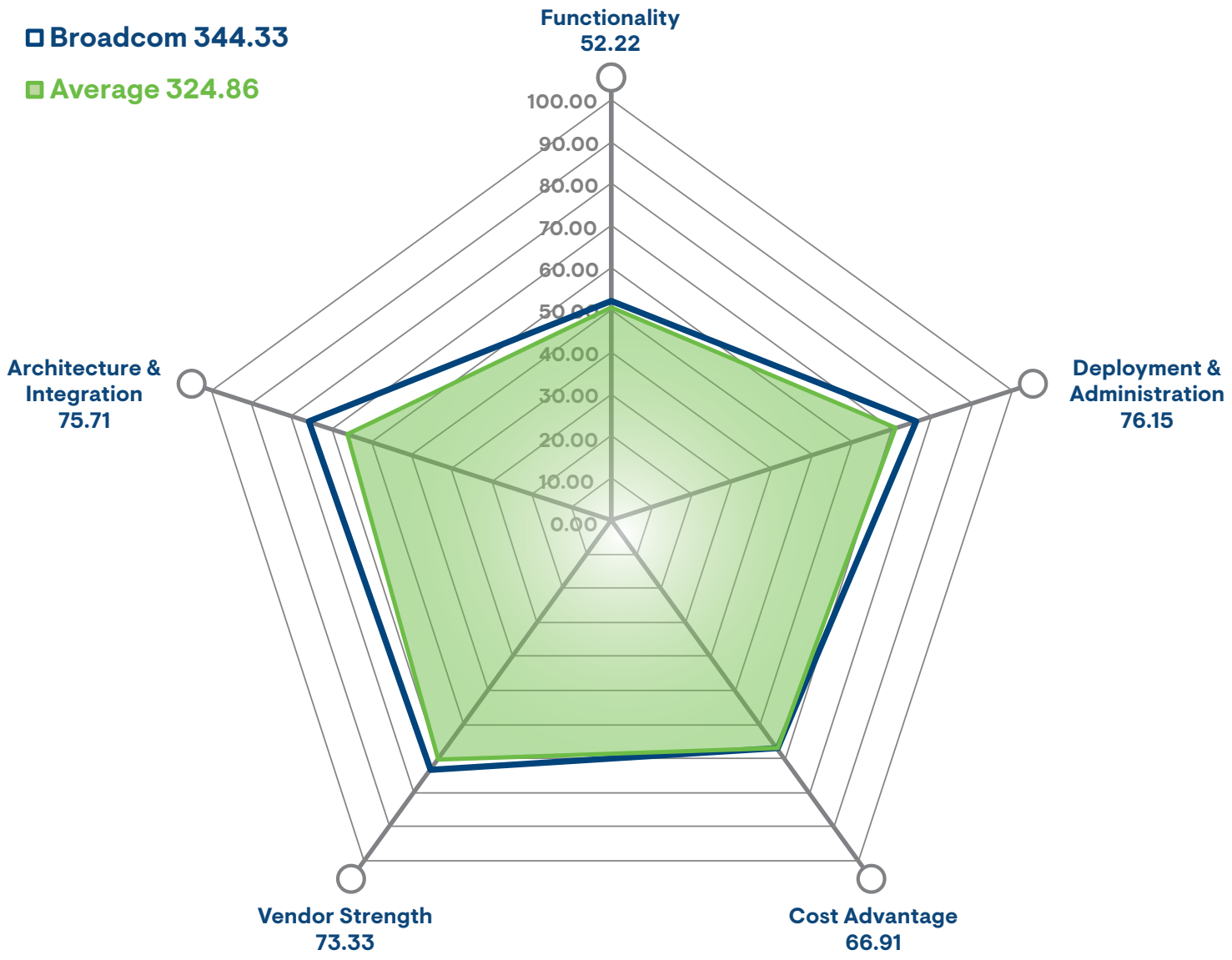
Symantec Privileged Access Management

Architecture:

Physical or virtual appliance

Notable Features:

- "All-inclusive" appliance model for deployment
- API-driven management
- Fine-grained access control
- Just-in-time privileged elevation
- SSH certificate authentication
- PIV pass-through authentication
- Programmatic access scalability
- NIST FIPS 140 encryption certification


Broadcom 344.33
Average 324.86
Functionality
52.22
Deployment &
Administration
76.15
Cost Advantage
66.91
Vendor Strength
73.33
Architecture &
Integration
75.71
100.00
90.00
80.00
70.00
60.00
50.00
40.00
30.00
20.00
10.00
0.00

Deployment & Administration

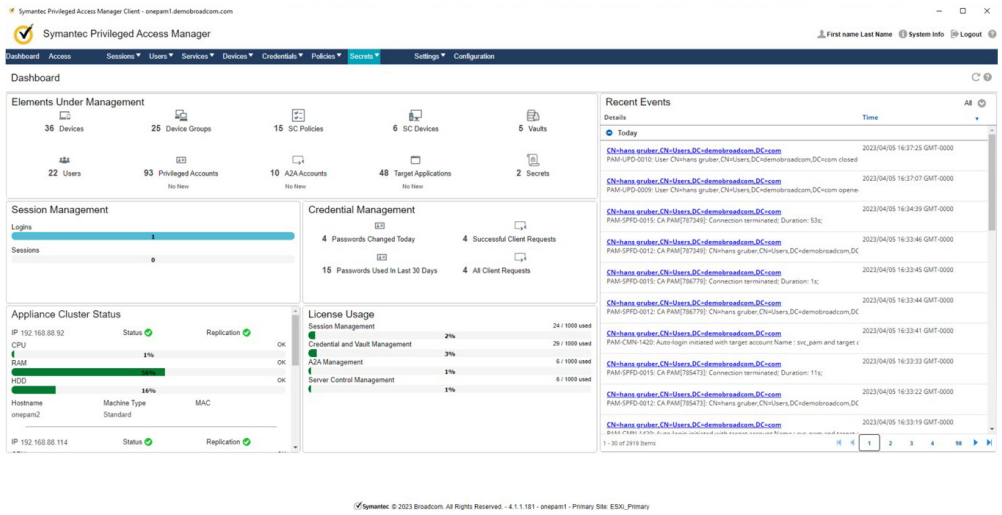
Deployment Complexity	
Ease of Deployment	Strong
User/Device Discovery	Outstanding
Agent Onboarding	Strong

Support and Services	
Customer Support	Strong
Community Services	Strong
Professional Services	Strong

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

Symantec Privileged Access Management is principally deployed as a self-contained physical or virtual appliance. While the physical appliance is a turnkey solution that does not require any additional infrastructure, the virtual instances are provisioned on preexisting VMware OVA, AWS AMI, or Azure VHD environments. Virtual instances may be hosted on-premises, on a private cloud, or in a hybrid configuration. Users and devices are discovered automatically from managed networks, devices, applications, and directory services. Implementations requiring only credential and secrets management can operate agentlessly, while more advanced functionality—such as fine-grained access control and session management—require the deployment of an endpoint agent. The centralized management console supports role-based access and includes several prebuilt reports and dashboard visualizations. Broadcom offers 24x7 live help desk support via phone, email, chat sessions, and web portal. The vendor hosts an online community forum and periodic meetings to engage customers. Broadcom also offers professional services to assist with platform design, implementation, training, and problem diagnosis. The Applixure Feedback module includes a variety of prebuilt and customizable survey templates, and the Applixure Workflow module enables the creation of custom data views.

Symantec Privileged Access Management Administrative User Main Dashboard



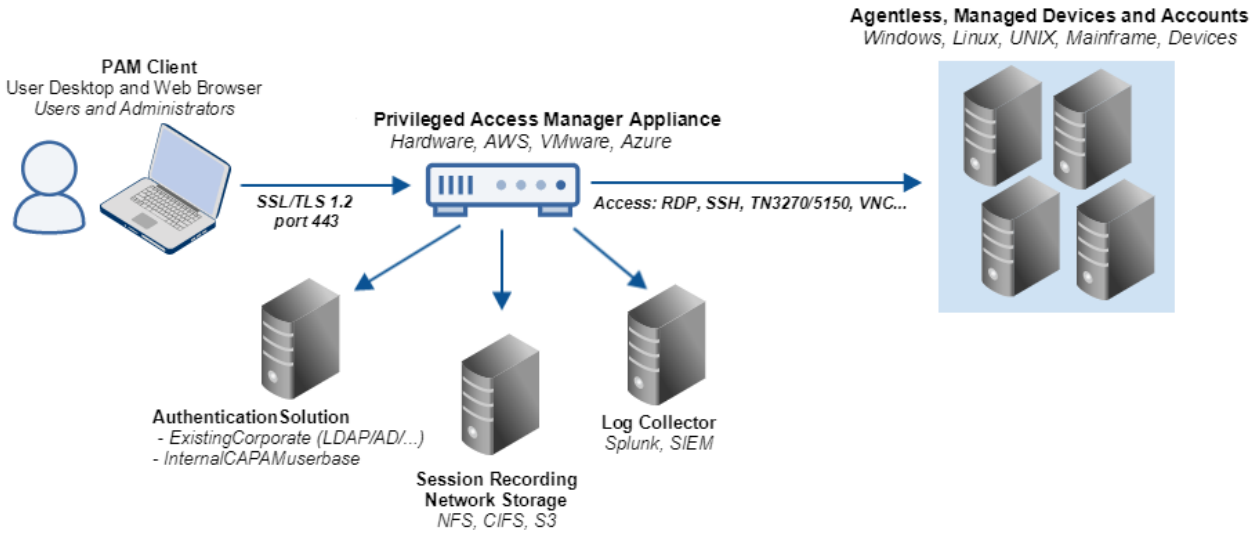
Architecture & Integration

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

Integrations	
Direct (Prebuilt) Integrations	Solid
APIs & SDKs	Strong

Broadcom's Symantec PAM platform manages privileged access across a broad range of on-premises and remote resources, including servers, endpoints, web apps, and SaaS apps. The solution connects to remote resources using SCIM, SAML, RADIUS, LDAP, and TACACS+ protocols. A proprietary vault is natively included for centrally storing policy secrets and, optionally, may federate data collection with third-party directory services, such as Active Directory and LDAP. Third-party penetration testing and automated scans are regularly performed on the latest supported release. Endpoint agents run persistently, autonomously, and when the devices are disconnected from the network. Direct integrations are included with service management platforms—including ServiceNow, BMC Remedy, HP Service Desk Manager, CA Service Desk Manager, and Salesforce Service Cloud. Other direct integrations are provided for network routers (Cisco and Palo Alto), data analysis (Splunk, QRadar, Logstash), and Broadcom's risk intelligence platform, Symantec Threat Analytics. REST, SOAP, and RPC APIs are provided for establishing custom integrations. Additionally, a Custom Connector Framework is provided to establish remote connections to resources that are not available out of the box and a Swagger document is included to define the structure of APIs.

Symantec Privileged Access Management Advance Architecture



Functionality

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

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

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

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

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

Users can create policies in Symantec PAM to automatically grant privileged access to discovered users based on their business role or other common attributes. Account privileges are provisioned to managed applications with provided connectors, standards-based APIs, or manual fulfillment. Administrators can configure how frequently changes in a user's status are detected in directory services, and managed accounts are automatically deactivated upon detection of an employment termination. Privileged identity governance features include access approvals, attestations, certification campaigns, segregation of duties control, and entitlement reconciliation.

Shared secrets (such as credentials, certificates, and encryption keys) are stored in the platform's included vault. Passwords are checked for uniqueness and complexity and granular policies can be set for password expirations, resets, and deactivations. Second-factor authentication is supported with email and SMS one-time passwords or push notifications. The platform's Shared Accounts Management (SAM) feature allows individual administrators to check in and check out shared privileged accounts to ensure transparency and accountability. Policies can also be created to manage privileged access for non-human identities.

Temporary privileged accounts can be created on servers, applications, and databases to support just-in-time access. Symantec PAM analytically monitors user behaviors and other contextual conditions to determine and score levels of risk. On detection of risky states, the solution can automatically deny users access, force reauthentications, or change authentication methods. Session recordings capture full video of user activities during privileged access events, as well as details such as usernames and files accessed.

Cost-Efficiency

Pricing Model	
License Costs	$$$
Maintenance Costs	$$
Infrastructure Costs	$$$

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

Broadcom offers several licensing options for the Symantec Privileged Access Management platform. Customers may purchase the base platform as a hardware appliance, virtual appliance, or cloud appliance. For each implementation option, customers may purchase perpetual licenses or monthly subscription licenses. Broadcom also offers a Portfolio License Agreement that gives customer entitlements to its entire Identity Management Security (IMS) portfolio, which includes the PAM platform and is charged per usage. While annual maintenance is included in subscription licenses, an annual fee is charged for perpetual licenses, which is calculated as a percentage of the purchase price.

Vendor Strength

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

Broadcom is a publicly-traded multinational semiconductor and infrastructure software provider. It offers its PAM solution under its Symantec Enterprise Security product line. The company's annual report for fiscal year 2022 discloses $33 billion in total net revenue, indicating a 17% increase over the preceding year. However, revenue attainment specifically for the Symantec PAM was not disclosed. Broadcom Software has approximately 22,000 partners and resellers worldwide. The company contributes to the NIAP PAM Protection Profile Technical Committee standards body. Broadcom's vision for Symantec PAM is delivering enterprise scalability, fast time to value, low total cost of ownership, and advanced functionality. The vendor's long-term strategy is to migrate to a microservice-centric architecture for all components supported on-premises or in the cloud.

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**