EMA
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

2024 PAM Radar Report

Summary Report Spotlighting Broadcom

September 2024
By **Ken Buckler, CASP**, Research Director
Information Security, Risk, and Compliance Management

Table of Contents

Executive Summary

Welcome to the Enterprise Management Associates (EMA) PAM Radar™ report scoring methodology overview. EMA is an industry-leading analyst firm specializing in a wide range of technology areas, including cybersecurity. We are dedicated to providing comprehensive research, analysis, and insights to help organizations make informed decisions about their technology investments.

EMA meticulously crafted the Radar report scoring methodology to address various aspects of cybersecurity vendor offerings, including deployment and administration, cost advantage, architecture and integration, functionality, vendor strength, client market and scalability focus, and more. We understand that every organization has unique needs. The information gathered in this report will enable you to tailor your vendor selection to best align with your specific requirements.

This Radar report combines public user sentiment and analyst analysis with vendors' forward-looking vision to develop a comprehensive, 360-degree profile of a vendor and its product strengths privileged access management (PAM), which is a critical pillar of cybersecurity.

Thank you for your dedication to cybersecurity excellence and your trust in EMA's research and analysis. Let's begin the journey to a more secure future.

Understanding Privileged Access Management

Protecting the Most Sensitive Business IT Assets

In the early days of computing, the development of user accounts and permission processes necessitated the creation of specialized master accounts that enabled unmitigated access to all system resources. In Unix and Linux systems, these are referred to as “root” accounts, while in Windows and macOS, they are known as “administrator” accounts. These accounts were essential for authorized individuals to manage and maintain critical system and security resources, such as the kernel, registry, and password files, which should never be accessible to regular users.

Over time, operating systems introduced additional features that allowed standard user accounts and custom scripts to have elevated permissions to perform specific tasks. For instance, setuid scripts, sticky bits, and sudo commands enable users to access privileged files or execute privileged activities. This granular control permits access to specific files or executables without granting unrestricted authorization to all system resources.

However, the proliferation of elevated user privileges led to widespread misuse and exploitation. A common scenario in many organizations involves granting privileged access to a user for a specific need, but failing to revoke these permissions once the issue is resolved. For hackers, these standing account privileges are highly sought after. If a malicious actor gains access to a privileged account or a standard user account with elevated privileges, they can view, damage, steal, and manipulate the organization’s most critical IT resources.

To address these challenges, privileged access management best practices and solutions were developed to control the provisioning and use of elevated permissions. PAM is a fundamental component of modern enterprise IT security strategies, ensuring robust control and protection of privileged access

The Scope of Privileged Access Management

The practices associated with privileged access management vary according to an organization's security posture and business requirements. Highly regulated sectors—such as government, health care, and financial institutions—demand more rigorous controls over privileged accounts. Conversely, companies with fewer security concerns may adopt a more liberal approach to access privileges to enhance business agility and workforce performance. Regardless of the approach, several key practices are essential for any PAM deployment:

The Identification of Privileged Accounts

Organizations must identify all existing privileged accounts and authorizations across all IT resources, including servers, applications, cloud-hosted resources, and endpoint devices.

Enforcement of Least Privilege Access

The principles of least privilege access dictate that users should only be granted access to the resources they need to perform their tasks. Minimizing access to unnecessary resources reduces risk profiles and limits potential damage from compromised accounts.

Privileged Access Audits

All privileged activities must be centrally recorded to facilitate periodic audits and troubleshooting. Actions, including file changes or programmatic creations, should be linked to the user who performed them, enhancing accountability and providing proof of compliance.

Onboarding Privileged Users

Users should have the ability to request privileged access to IT resources. These requests must go through a formal approval process, with designated stakeholders providing written and verifiable authorizations. When it comes to onboarding, the line between privileged access management and identity governance & administration can sometimes become blurred.

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 viewed PAM as a separate practice from general identity and access management (IAM), which governs the authentication and access policies of standard user accounts. These two management disciplines involved distinct administration processes and tools, with PAM enforcing more stringent monitoring and authorization controls. In recent years, the distinction between IAM and PAM has significantly blurred, with most enterprise-class IAM platforms now incorporating some PAM functionality.

Substantial industry consolidation, including the merger of respective product sets through acquisitions, drove the convergence of PAM and enterprise IAM. A unified solution offers numerous advantages, such as consistent and centralized administration consoles and the sharing of a common set of user, system, and contextual information.

Moreover, with converged product sets, IAM solutions now incorporate features traditionally considered exclusive to PAM. One prominent example is the proliferation of just-in-time (JIT) access, initially developed for on-demand access to privileged accounts. Today, IAM platforms widely use JIT solutions to facilitate any on-demand access, such as to cloud-hosted applications.

In recent years, the adoption of intelligence technologies, including machine learning, cognitive computing, analytics, and natural language processing, has risen. These resources are increasingly employed for identity threat detection and response (ITDR); enhancing risk detection, scoring, and vulnerability assessments; and providing recommendations for process improvements.

Points of integration have also accelerated, with PAM solutions more broadly acquiring data points from third-party platforms. Integrations with security information and event management (SIEM) systems and other security solutions have significantly enhanced PAM platforms' ability to collect contextual information, supporting conditional privileged access policies.

Looking forward, the convergence between PAM and enterprise IAM will likely continue, with IAM eventually fully absorbing PAM. In this process, identity governance and administration (IGA) processes will become more broadly integrated. While not a direct evaluation criterion of this report, IGA will undoubtedly become a key differentiator in future assessments. Ultimately, this evolution will lead to the availability of truly unified identity management platforms that are easier to manage and more effective at securing business IT assets.

Finding the Right Solution

It's important to realize that every organization is different, and what works for one organization might not work for another. The primary limitation of any guide such as this one is that it attempts to generalize the product strengths and cost values of solutions without the ability to tailor the evaluation criteria toward specific organizational needs. While the Radar report can be a starting point, it's important to realize that there is no "best" or "worst" choice, and each of the vendors in this report has their own strengths and weaknesses.

While it may be tempting to simply select from the Value Leader segment of this report, consideration and evaluation should be given to Strong Value and even Selective Value contenders. Though our evaluation endeavors to be comprehensive of all features, organizations may not need some features, especially if those features are already available through other tools in which the organization has invested. Even total cost of ownership will vary depending on each organization, with some organizations able to manage certain solutions more efficiently than others. The focus of this report was traditionally enterprise usage, but we find it important to also highlight that some of the solutions that may not be as feature-rich for enterprises are absolutely acceptable for small business usage, and we've done our best to denote as such throughout the report. To use the old cliché, "your mileage may vary."

Assessing the PAM Market

Selection Criteria

Vendors were selected for inclusion in the Radar report based on several factors:

- Interaction with EMA analysts
- Public interest in the vendor (i.e., search engine analytics, social media)
- Availability of public information about their PAM solution

Utilizing this criteria, the top 14 vendors were selected for inclusion in this report.

Research and Methodology

Starting with this year's report, EMA now uses a proprietary analytical engine to gather, process, and analyze scoring for vendor strengths and weaknesses. Utilizing this analytical engine, all vendors were evaluated based on publicly available data, as well as their own responses to our vendor questionnaire. Publicly reviewed data includes, but is not limited to:

- Vendor documentation and public knowledgebase
- Media and news articles
- Social media posts by users of the product/solution
- User sentiment derived from questions and answers on public help forums, including vendor help forums and third-party help forums, such as StackExchange and Reddit

In addition to evaluation based on publicly available data, EMA also offered all selected vendors the chance to provide their own input with an open-ended vendor survey, as well as feedback on our assessment of each solution.

EMA evaluated all responses and scoring based on information revealed within the last several years, utilizing the most up-to-date information possible. EMA evaluated each data point on a weighted scale, with some criteria weighing more heavily on final scoring. The analytical engine, which utilizes public sentiment and vendor responses to generate a holistic, unbiased analysis of vendors and solutions, generated initial scoring. An EMA analyst then adjusted scoring while reviewing the relevant data for accuracy. While this methodology provides a more unbiased approach to evaluating user sentiment, it also does have the limitation that it is only based upon publicly available information. As such, if vendors have not published updates regarding their products in a timely manner, those new or improved features will not be visible to our analytical engine. In addition to this analytical engine, we simplified and standardized evaluation criteria to make reports simpler to understand.

Changes to This Year's Report

In addition to the adoption of our new analytical engine, this year's report seeks to provide a more holistic view of the merits of each vendor's solution. There is no "best" or "worst" vendor, and all vendors in this report should be evaluated based upon their own individual merits, in order to help organizations find the PAM solution that is the right fit for their organization's needs. This year, we even gave an award to a vendor in the Selective Value category.

We added Okta, Microsoft, Akeyless, and ManageEngine to the list of covered vendors. Amitego and Netwrix were omitted in accordance with the selection criteria previously discussed, primarily due to limited public interest in those vendors' PAM solutions

Characteristics of a Preferred Solution

Deployment & Administration

An ideal PAM solution's deployment and administration features would be a seamless blend of speed, flexibility, and user-friendliness. Deployment should be swift and intuitive, with minimal disruption to ongoing operations. The solution should be adaptable to various IT environments, whether on-premises, in the cloud, or hybrid. Administration should be streamlined through automation, reducing manual effort and overhead. The platform should offer a user-friendly interface that is intuitive to navigate and manage, even for less experienced administrators. Key features like role-based access control, automated password management, and granular permissions should be easily configurable and readily accessible. Regular updates and patches should be deployed seamlessly, ensuring security is constantly maintained without disrupting operations. The overall goal is to create a PAM solution that is easy to install, manage, and update, minimizing downtime and maximizing operational efficiency.

Architecture and Integration

An ideal PAM solution boasts a robust and scalable architecture that seamlessly integrates with existing IT environments. This architecture should offer flexibility and speed in deployment and scaling, supporting cloud native, hybrid environments and on-premises deployments. The solution should integrate seamlessly with various identity management systems, directory services, and other enterprise applications, creating a unified and secure ecosystem. This integration should be seamless, minimizing configuration complexities and allowing for a single pane of glass for administrative control. The architecture should adhere to zero trust principles, ensuring that access is granted only on a need-to-know basis and that all activities are rigorously monitored and audited. This holistic approach ensures a secure, adaptable, and efficient PAM solution that can adapt to evolving security needs and organizational growth.

Functionality

An ideal PAM solution provides comprehensive functionality that streamlines the management of privileged credentials, accounts, and secrets while bolstering overall security. It offers a centralized platform for enterprise storage and management of privileged accounts, passwords, keys, secrets such as API keys, and other sensitive information, ensuring they are securely encrypted and accessible only to authorized users. The solution includes robust features for managing privileged accounts, including automated password rotation, access control, and session monitoring, minimizing the risk of unauthorized access and ensuring compliance with security policies. It makes use of just-in-time provisioning, utilizing ephemeral accounts to grant temporary access to specific resources only when needed and revoking it automatically when no longer required. It does this by employing unique, individual privileged accounts and destroying (or removing all permissions from) the privileged account after usage, minimizing the attack surface and enhancing security. The ideal solution also includes sophisticated identity threat detection and response capabilities, leveraging advanced analytics, machine learning, and real-time monitoring to proactively identify potential threats and automatically respond swiftly to security incidents. This combination of features ensures a secure, efficient, and compliant system for managing privileged access, safeguarding sensitive information, and mitigating potential threats. While this year's report does not include identity governance as part of the evaluation requirements, many solutions do include this functionality, and it will likely be included as part of the evaluation criteria for future reports.

Cost-Efficiency

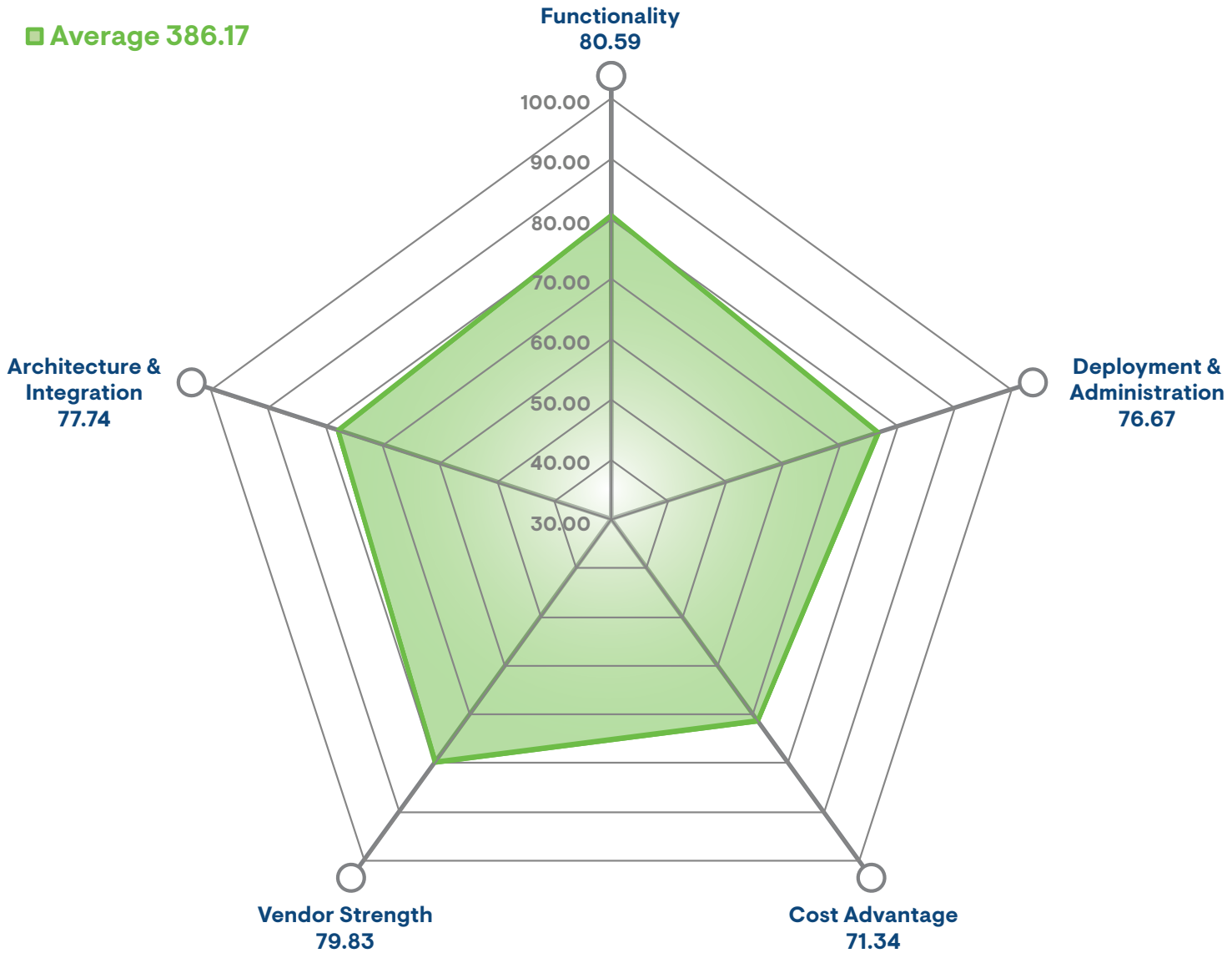
An ideal PAM solution is not only effective, but also cost-efficient, striking a balance between robust security features and affordability. It should offer flexible pricing models that cater to organizations of different sizes and budgets, providing tiered options that scale with their specific needs. The solution should minimize ongoing maintenance and support costs through automation and user-friendly interfaces, reducing the need for extensive technical expertise and support. Moreover, it should offer a compelling return on investment by significantly reducing the risk of security breaches, data loss, and compliance violations, ultimately leading to significant cost savings in the long run. This cost-efficiency should be achieved without compromising on security effectiveness, ensuring organizations receive a robust and reliable PAM solution without breaking the bank.

It's important to note that cost-efficiency is generalized for medium to large enterprises in this report. Organizations with different needs of different sizes will encounter different costs based on their individual needs, and it's important to obtain quotes from multiple vendors, as well as evaluate the total cost of ownership, including the time needed to invest in training employees on utilizing solutions. Additionally, please note that due to the high cost-efficiency of some solutions, the "average" scoring for all solutions may be misleading. Many quality solutions came in "below average" on scoring, but are still likely considered affordable.

Vendor Strength

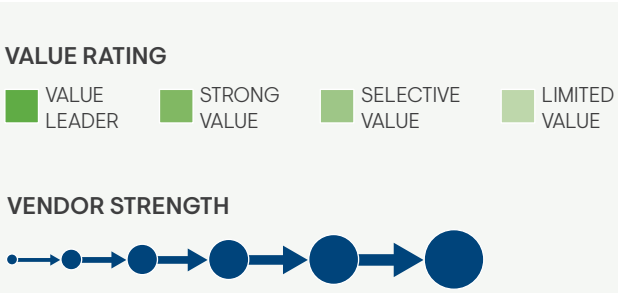
An ideal PAM solution comes from a vendor demonstrating a strong track record of innovation, reliability, and customer satisfaction. They should be a trusted leader in the cybersecurity space, known for their expertise in identity and access management. The vendor should offer a comprehensive suite of PAM solutions, catering to various organizational needs and complexities. Their team should be highly responsive and knowledgeable and provide excellent customer support and proactive guidance in navigating the ever-evolving landscape of cybersecurity threats. They should prioritize transparency and ethical practices, adhering to industry standards and continuously investing in research and development to stay ahead of emerging security challenges. A vendor with these strengths builds trust and confidence to ensure organizations have a reliable partner to navigate the complexities of securing their privileged access. Community support, as well as contribution to the open-source community and open standards, is essential to continue innovation.

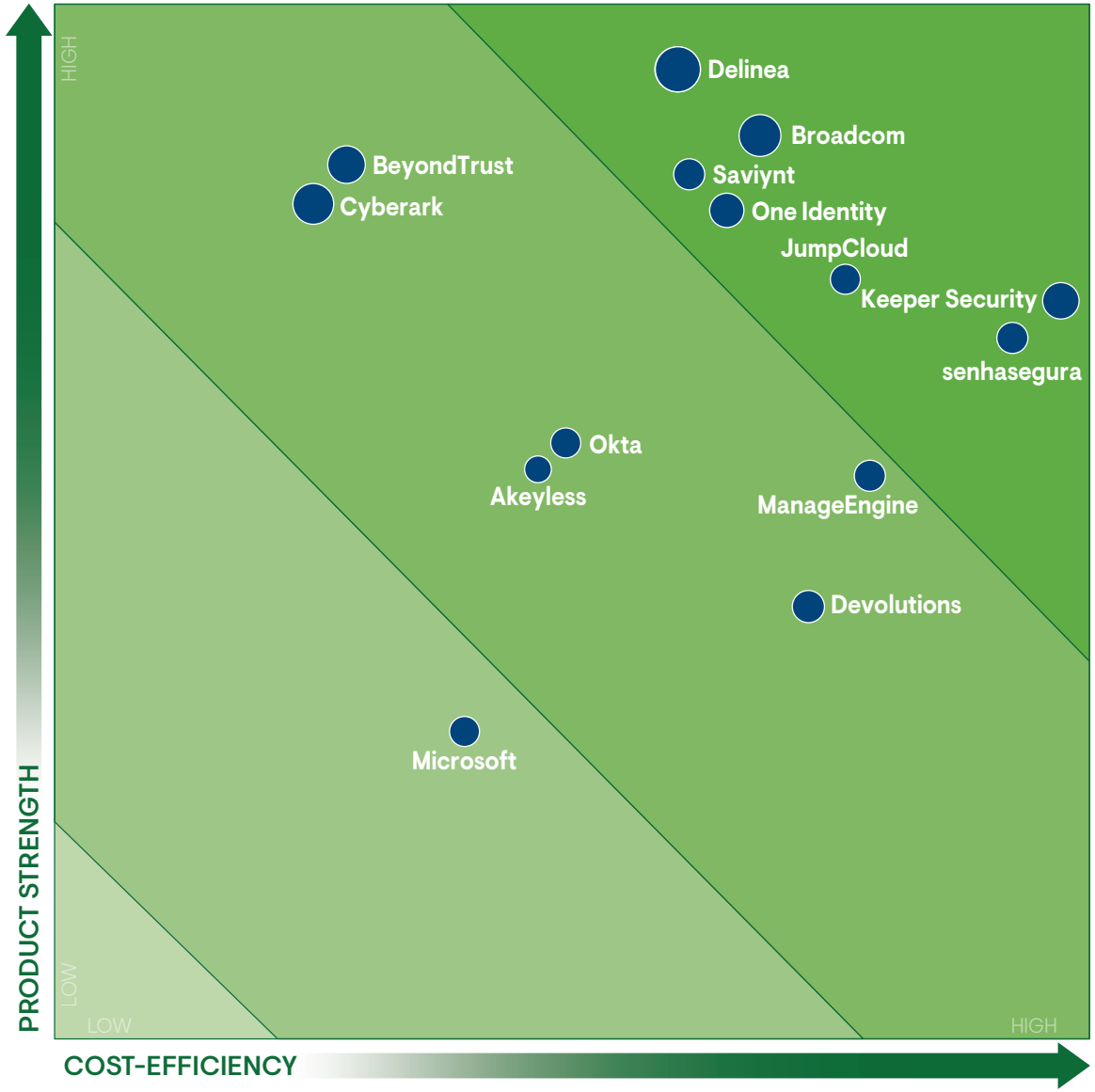
Vendor strength is also generalized in this report for medium and large enterprises. Some vendors specialize in the needs of smaller enterprises, and this is also noted in the report where applicable.


Average 386.17
Functionality
80.59
100.00
90.00
80.00
70.00
60.00
50.00
40.00
30.00
Deployment &
Administration
76.67
Cost Advantage
71.34
Vendor Strength
79.83
Architecture &
Integration
77.74

On the EMA Radar™

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

Broadcom PAM offers a straightforward deployment process with comprehensive documentation. Support is responsive, mitigating critical impacts. The professional services provide thorough training. Administrative overhead is reduced through robust features. Security is strong with automated password management. Reporting is user-friendly with detailed logs and data analytics provide real-time insights. The architecture is robust and scalable and integration is secure. JIT provisioning is efficient. Identity threat detection and response offer advanced analytics. What differentiates Broadcom from other vendors is its robust scalability and strong integration capabilities with existing infrastructure, making it ideal for large enterprises.

Delinea

Delinea offers a broad range of identity security, protection, and governance capabilities. Traditionally a PAM pure-play vendor, Delinea has expanded its portfolio to include CIEM, identity threat detection and response, IGA, separation of duties (SOD), and AI-driven auditing to reduce staff workloads and improve enterprise risk exposure. The Delinea Platform is a fully modernized, cloud native solution that enables users to quickly integrate new feature sets. Emphasizing intelligent authorization, organizations discover all identities, assign appropriate access levels, detect irregularities, and immediately respond to identity threats in real time.

JumpCloud

JumpCloud's focus is on small and medium enterprises, and deployment is quick and flexible for those organizations. Disruptions are minimized with streamlined IT operations, but for larger organizations with complex use cases, setup challenges exist. Support is responsive and expert, though occasional communication issues arise. JumpCloud recently added Customer Success Managers and Professional Services to specifically help support larger and more complex organizations. Staff training emphasizes detailed onboarding and self-learning modules. Automation reduces administrative overhead. Security features are comprehensive with seamless updates. Reporting is robust and data analytics offer detailed insights. The architecture uses modern protocols with robust security, but works best as an all-in-one IAM and device platform rather than a best-of-breed solution. Integration is centralized with versatile support. Vendor lock-in is minimized with flexible integration capabilities. JIT provisioning is efficient. Identity threat detection includes real-time monitoring and customization is versatile. What differentiates JumpCloud is its cloud native Directory as a Service, which allows centralized identity, access, and device management from a single unified console, providing enhanced flexibility and administrative efficiency.

Keeper Security

Keeper Security excels in swift deployment and platform compatibility. Deployment disruptions are minimal and have quick resolutions. Support is robust, with extensive comprehensive training. Staff training is comprehensive. Automation is high, with user-friendly interfaces, and security has strong role-based controls. Reporting is user-friendly and offers customizable options. Data analytics are comprehensive, with multi-device sync. The zero-knowledge security architecture is robust. Integration is user-friendly and includes strong encryption. JIT provisioning minimizes risks. Identity threat detection includes dark web monitoring. Customization is versatile. What differentiates Keeper Security is its specialization in robust password management solutions with strong encryption and user-friendly features, making it an ideal choice for organizations prioritizing password security and ease of use.

One Identity

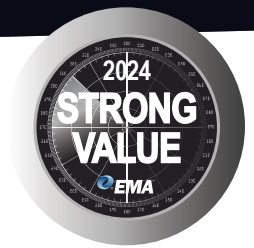
One Identity Safeguard PAM offers quick deployment with a modular architecture. Deployment is robust, with detailed documentation. Support is comprehensive and staff training is well organized. Automation streamlines onboarding. Security features include granular controls and regular updates with detailed reporting. Data analytics are robust. The architecture is comprehensive with user-friendly interfaces. Integration supports various platforms, and JIT provisioning reduces attack surfaces and is built into Safeguard. Identity threat detection uses machine learning. Customization is adaptable. Management is intuitive and is one of the areas in which the product excels. One Identity shines in providing a unified approach to identity security by integrating PAM with identity governance, making it an ideal choice for organizations seeking a comprehensive and cohesive identity security solution.

Saviynt

Saviynt ensures efficient deployment with comprehensive documentation. Deployment disruptions are minimal, with responsive, extensive support. Training programs are detailed and structured. Automation includes robust password management and session recording. Security features are strong, with regular updates, and reporting capabilities are user-friendly with preconfigured options. Data analytics provide thorough monitoring. The architecture supports high availability. Integration is generally seamless and vendor lock-in is minimized through extensive documentation. JIT provisioning is efficient and user-friendly. Identity threat detection includes continuous monitoring. Customization is flexible and centralized management is effective. In addition to its PAM capabilities, Saviynt is known for its identity governance and administration capabilities, focusing on compliance and security, making it a standout choice for organizations prioritizing comprehensive identity management and regulatory compliance.

senhasegura

senhasegura ensures quick deployment with document-backed installation. Deployment disruptions are minimal, with responsive support. Support is comprehensive, but needs more localized options, and though staff training is structured, it requires role-specific customization. Automation includes password vaulting and session recording and features a user-friendly interface. Security features are robust, with regular updates. Reporting is user-friendly with preconfigured options, but customization is required for maximum effectiveness. Data analytics offer comprehensive monitoring. The architecture is modular, with high availability, and integration is seamless. Vendor lock-in is minimized, with strong documentation and open connectors. JIT provisioning is real-time and user-friendly. Identity threat detection includes continuous monitoring. Management solutions are centralized and highly customizable.



Akeyless

Akeyless provides a PAM solution with straightforward deployment backed by comprehensive documentation. Deployment disruptions are rare, thanks to efficient support. The support network is extensive, and training is detailed and structured. Automation features, including password vaulting and session monitoring, are robust. Security is top-notch with regular updates. Reporting is thorough, with preconfigured options. Data analytics offer detailed monitoring, and the architecture is modular and supports high availability. Integration is generally seamless. Vendor lock-in is minimized through extensive documentation. JIT provisioning is efficient and user-friendly. Identity threat detection includes continuous monitoring with flexible customization. Centralized management is effective. What differentiates Akeyless from other vendors is its zero trust architecture, which provides robust secrets management and secure remote access with an emphasis on minimizing risk through strong encryption and real-time monitoring.

BeyondTrust

BeyondTrust offers a PAM solution with smooth deployment aided by comprehensive documentation, supported by responsive customer service. The support network is extensive, and training is detailed and structured. Automation features, including password vaulting and session monitoring, are robust. Security is top-notch with regular updates. Reporting is thorough, with preconfigured options. Data analytics offer detailed monitoring. The architecture is modular and supports high availability. Integration is generally seamless and vendor lock-in is minimized through extensive documentation. JIT provisioning is efficient and user-friendly. Identity threat detection includes continuous monitoring with flexible customization. Centralized management is effective. What differentiates BeyondTrust from other vendors is its comprehensive endpoint privilege management capabilities, providing granular control and robust security across diverse IT environments.

CyberArk

CyberArk's PAM solution ensures efficient deployment with robust documentation. Disruptions during deployment are minimal with responsive support. The support network is extensive, and training is comprehensive and structured. Automation includes password vaulting and session recording. Security features are strong and regularly updated. Reporting is user-friendly, with preconfigured options. Data analytics provide comprehensive monitoring. The architecture is modular with high availability and integration is seamless. Vendor lock-in is minimized with strong documentation. JIT provisioning is real-time and user-friendly. Identity threat detection includes continuous monitoring. Customization is tailored and management is centralized. What differentiates CyberArk from other vendors is its unparalleled focus on securing privileged accounts with advanced security measures and comprehensive session monitoring, making it a top choice for organizations with stringent security requirements.

Devolutions

Devolutions' remote desktop solution offers flexible deployment options that accommodate various business needs. Their support team is highly responsive and backed by an extensive knowledge base. Automation through their centralized platform significantly reduces overhead. Security updates are frequent and adhere to industry best practices, ensuring robust protection for remote connections. Reporting capabilities are comprehensive, and data analytics tools are detailed. The architecture focuses on security and management efficiency. Integration with other systems is thorough. Just-in-time provisioning offers real-time resource allocation, enhancing operational flexibility. Identity threat detection includes continuous monitoring. Overall, Devolutions is a unique solution that focuses on remote desktop, as well as leveraging PAM as a productivity tool instead of the more traditional approaches to PAM other vendors use.

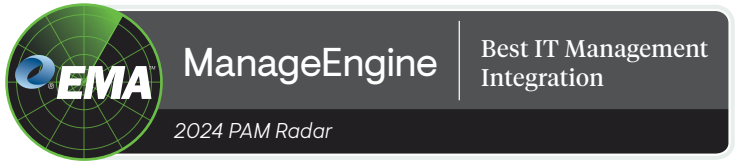
ManageEngine

ManageEngine PAM360 offers fast deployment with flexible configurations. Deployment is reliable. Support is responsive and knowledgeable, and staff training provides extensive resources. Automation reduces overhead. Security features are strong, with frequent updates. Reporting is comprehensive. Data analytics provide real-time monitoring. The architecture is robust and integration is seamless within ManageEngine products. JIT provisioning enhances security. Identity threat detection is strong and customization is extensive. Management is intuitive. What differentiates ManageEngine is its broad range of IT management tools, including PAM, with a focus on affordability and comprehensive feature sets. It's an ideal choice for organizations looking for cost-effective and robust IT management solutions.

Okta

Okta's PAM solution offers quick deployment supported by detailed documentation. Deployment disruptions are minimal, with responsive support, which is comprehensive. Training programs are structured and automation features, such as password management and session recording, are robust. Security features are advanced with regular updates. Reporting is user-friendly, with preconfigured options. Data analytics offer thorough monitoring. The architecture supports high availability. Integration is generally seamless and vendor lock-in is minimized through strong documentation. JIT provisioning is efficient and user-friendly. Identity threat detection is continuous and proactive. Customization is extensive and centralized management is effective. With a launch date of December 2023, Okta's PAM offering has the potential to be a serious contender in the space as the product evolves. What differentiates Okta is its excellence in identity management and single sign-on (SSO) solutions, which provide strong user authentication and access controls, making it an ideal choice for organizations seeking robust and reliable identity solutions.

Awards



ManageEngine – Best IT Management Integration

ManageEngine's PAM360 is expertly positioned as the premier choice for organizations seeking seamless integration with a comprehensive IT management tool suite. PAM360 is designed to integrate effortlessly with ManageEngine's extensive range of IT management solutions, including ServiceDesk Plus, OpManager, ADManager Plus, and Log360. This unified approach allows organizations to manage privileged access alongside other critical IT functions within a single, cohesive platform. PAM360 enhances security and compliance by providing detailed audit trails, real-time monitoring, and automated workflows, all while maintaining a user-friendly interface. Its ability to centralize and streamline privileged access management within the broader IT ecosystem makes ManageEngine's PAM360 the optimal solution for organizations looking to maximize efficiency and security in their IT operations.

Devolutions – Best Remote Desktop Experience

Devolutions is strategically positioned as a leading provider of remote desktop services, offering robust and comprehensive solutions tailored for IT professionals and teams. Their flagship product, Remote Desktop Manager (RDM), centralizes all remote connections, passwords, and credentials into a single, secure platform, significantly enhancing efficiency and security. RDM supports a wide range of remote connection protocols and integrates seamlessly with numerous third-party tools and services, providing flexibility and compatibility in diverse IT environments. Its user-friendly interface and powerful features, such as session recording, granular access controls, and real-time monitoring, make it an invaluable tool for managing remote access.

Microsoft – Best Azure AD Integration

While Microsoft is only highlighted as a Selective Value in this year's report, we felt it was important to highlight the strength behind Microsoft's ability to integrate within the Microsoft ecosystem. Microsoft's privileged access management (PAM) solutions are exceptionally positioned for seamless integration with Azure Active Directory (Azure AD), offering unparalleled ease of use and comprehensive security. Azure AD Privileged Identity Management (PIM) is a built-in solution that simplifies the management of privileged roles through just-in-time access, approval workflows, and detailed activity logging. Its deep integration with the Microsoft ecosystem, including Office 365 and other Azure services, ensures a unified and cohesive approach to identity and access management. The user-friendly Azure portal facilitates straightforward configuration and monitoring, while extensive documentation and support resources further streamline deployment and management. This makes Microsoft PAM an ideal choice for organizations seeking basic PAM capabilities without any non-windows devices.

BeyondTrust – Best Endpoint Privilege Management

BeyondTrust is a market leader in endpoint privilege management (EPM), offering a comprehensive and robust solution that enforces the principle of least privilege, ensuring users operate with the minimum necessary rights to reduce the attack surface and mitigate risks. With its advanced application control, real-time privilege elevation, and centralized management capabilities, BeyondTrust provides granular control and flexibility tailored to organizational needs. Its broad support for various operating systems and seamless integration with other IT and security tools further solidify its position. Recognized for its user-friendly interface, advanced threat protection, and compliance features, BeyondTrust stands out as a top choice for organizations seeking to enhance endpoint security and manage privileged access effectively.

BROADCOM

Overview

Broadcom PAM offers a straightforward deployment process with comprehensive documentation, though it can be complex for those without prior PAM experience. Support is responsive, mitigating critical impacts despite occasional communication issues. The professional services provide thorough training, which is comprehensive, but can be technical. Administrative overhead is reduced through robust features, though initial setup can be complex. Security is strong, with automated password management. Reporting is user-friendly with detailed logs, though customization may be needed. Data analytics provide real-time insights, but integration with third-party tools could be streamlined. The architecture is robust and scalable, though the user interface could be improved. Integration is secure, but complex. Vendor lock-in is a concern due to the proprietary nature of the product. JIT provisioning is efficient, but the setup can be complex. Identity threat detection and response offer advanced analytics, though setup can be significant.

Broadcom excels in scaling solutions for large enterprises, offering robust integration capabilities with existing infrastructure.

EMA RADAR

Headquarters:
San Jose, California, USA

Territories Supported with a Regional Office:
North America, Europe, Asia-Pacific

Company Website:
broadcom.com

Product Name:
Symantec Privileged Access Manager

Architecture:
On-premises, cloud, hybrid

Notable Features:

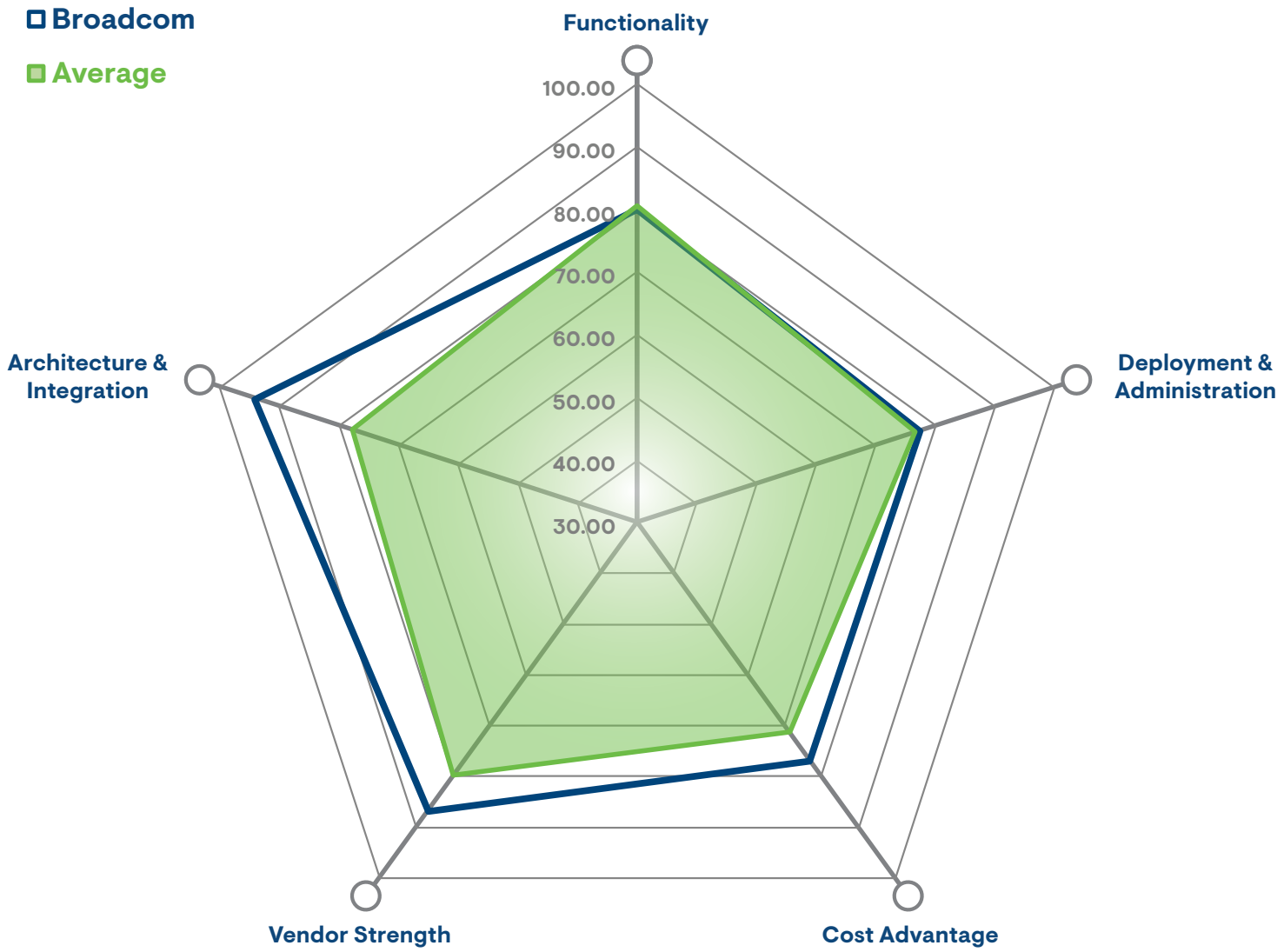
Privileged Credential Vault
Protect and manage administrative credentials in an encrypted database.

Secrets Management
Secure communication by eliminating hard-coded passwords.

Access Control
Enforce policy-based access control for least privilege access.

Audit and Monitoring
Comprehensive monitoring and logging of privileged activities for compliance.

Just-in-Time Access
Dynamic access provisioning to reduce standing privileges.


Broadcom
Average
Functionality
100.00
90.00
80.00
70.00
60.00
50.00
40.00
30.00
Deployment & Administration
Cost Advantage
Vendor Strength
Architecture & Integration

Deployment & Administration

Ease of Deployment	
Deployment Time & Flexibility	Outstanding
Deployment Disruption	Strong

Support and Services	
Professional Services & Cust. Support	Outstanding
Staff Training	Outstanding

Ease of Administration	
Administrative Overhead & Automation	Solid
Administrative Security & Update Impact	Strong

Reporting	
Out-of-the-Box Reporting	Solid
Data Analytics & Accessibility	Solid

Broadcom PAM offers a relatively straightforward deployment process with comprehensive documentation and support. Its architecture is flexible, supporting both on-premises and cloud environments. However, initial setup and configuration can be complex, particularly for organizations lacking experience with privileged access management systems. This complexity might require a steeper learning curve, potentially impacting deployment time and administrative overhead. Broadcom PAM does feature robust automation capabilities aimed at reducing manual workload and streamlining administrative tasks. However, initial configuration and complexity of implementation might make it less accessible for smaller organizations or those without dedicated IT resources, despite its strong administrative security and update impact.

Broadcom PAM offers a relatively straightforward deployment process with comprehensive documentation and support.

Architecture & Integration

Architecture	
Data Collection & Performance	Outstanding
Data Retention, Privacy & Protection	Outstanding

Integration	
Data Feeds to Other Products	Outstanding
Data Ingestion from Other Products	Outstanding

Vendor Lock-In	
Data Import	Strong
Data Portability	Strong

Broadcom's PAM architecture is robust and scalable, designed to support a wide range of IT environments. It offers comprehensive features like session recording, multifactor authentication, and granular access controls, ensuring that privileged accounts are managed with a high level of security. The architecture also integrates well with existing IT infrastructure, supporting a wide range of operating systems, databases, and applications. This seamless integration makes it easier for organizations to deploy and manage the solution across their entire IT landscape. Broadcom's PAM solution prioritizes logging and auditing, providing detailed records of user activities and access attempts, which are crucial for compliance and security investigations. While the architecture is strong, there is room for improvement in areas like user interface design and ease of use, which could further enhance the overall user experience.

This seamless integration makes it easier for organizations to deploy and manage the solution across their entire IT landscape.

Vendor Strength

Industry Vision (Thought Leadership)	Strong
Product Vision	Outstanding
Strategy	Strong
Financial Strength	Outstanding
Research & Development	Strong
Partnerships and Channel	Solid
Community Support & Open Source	Outstanding

Functionality

Core Features	
Management of Privileged Accounts, Secrets, and Credentials	Outstanding
Just-in-Time Provisioning	Outstanding
Identity Threat Detection and Response/Integration	Solid

Configuration & Updates	
Configurable for Business Needs	Solid
Updates do not Impact Core Functionality/Downtime	Solid

Management	
Ease of Management	Strong

Ease of Use	
Roles Supported	Strong
Reporting	Strong

Cost-Efficiency

Pricing Model	
Licensing Costs	$$$
Licensing Model/Flexibility	Strong
Support and Training Costs	$$
Infrastructure Costs & Management Costs	$$

Broadcom PAM offers a robust and comprehensive solution for managing privileged accounts across various IT environments. It is known for its strong security features, including session recording, multi-factor authentication, and granular access controls. Broadcom PAM excels in its ability to automate many administrative tasks, including password management, session recording, and compliance reporting, thus reducing manual workloads and streamlining operations. The solution integrates well with existing IT infrastructure and supports extensive logging and auditing, which are crucial for meeting compliance requirements and ensuring security.

Broadcom PAM excels in its ability to automate many administrative tasks, including password management, session recording, and compliance reporting, thus reducing manual workloads and streamlining operations.

EMA Perspective and Opportunities for Improvement

The PAM market has seen significant improvement over the past few years in providing efficient privileged account management, secrets management, and management of sensitive credentials. Now that management of these aspects of privileged access has matured, vendors should increasingly focus on identity threat detection and response, as well as better just-in-time integration and identity governance & administration.

Identity threat detection and response (ITDR)

Most vendors have started to implement ITDR features focused on automated detection and manual reactive response. The ideal approach is to leverage ITDR for not only proactive response, but also automated response. Recent advancements in artificial intelligence are showing great promise in this area, especially for anomaly detection and automated triage. Automated response technology is still in its infancy and needs to prove itself to the market before widespread adoption.

Just-in-time (JIT) integration

Most vendors now support some form of JIT integration. However, the largest concern with current implementation is that most vendors are relying on time-gated access to privileged accounts instead of dynamic account creation and removal. To truly leverage JIT integration for a "principle of least privilege" and "zero trust" perspective, vendors should create and remove accounts for maximum protection. After all, an attacker can't access a compromised privileged account if that account does not exist after the session is completed.

Identity governance & administration (IGA)

While not a criterion for evaluation in this year's report, IGA has the potential to become a driving force in the evolution of PAM solutions. With many vendors already including IGA features in their PAM solutions, it is highly likely that IGA will become a cornerstone of evaluation in future iterations of this report. IGA will also play a pivotal role in enabling better JIT access control.

The PAM market continues to evolve for the better, and we believe that most vendors are moving in the right direction with the evolution of their solutions. We look forward to further advancement of PAM solutions over the coming years.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT analyst research firm that specializes in going "beyond the surface" to provide deep insight across the full spectrum of IT 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 its clients achieve their goals. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.

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