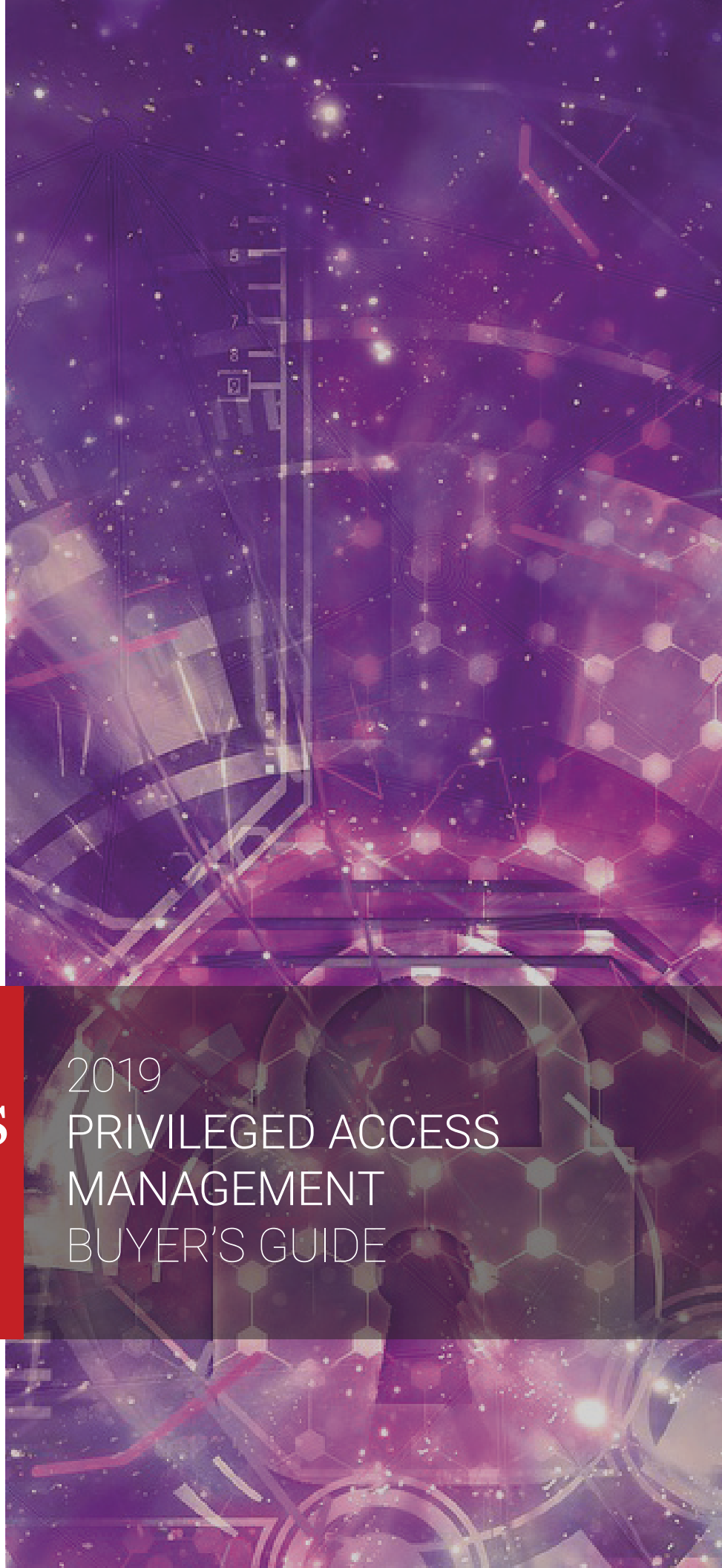

Solutions Review

2019 PRIVILEGED ACCESS MANAGEMENT BUYER'S GUIDE

MARKET OVERVIEW

If anything could be considered a hacker's or insider threat's prime target—the golden goose which they wish to plunder—it would be your enterprises' privileged identities.

The reason why is simple: unmanaged, unmonitored privileged accounts are both easy and lucrative targets for both external attacks and malicious insiders. In fact, according to the Verizon 2018 Data Breach Investigations Report, 80% of security breaches were the result of weak or stolen passwords. Moreover, 80% of security breaches involve privileged credentials, according to Forrester Research.

Privileged access management may be the most sensitive aspect of IT and identity security, matched by a security field that has rapidly matured to meet its demands. Administrative accounts with privileged access can make sweeping and fundamental changes to the IT systems on which your business may depend. Fail to protect those accounts, and you may as well hand intruders to keys to your proprietary or customers' data.

Furthermore, with administrative access, an intruder can move laterally through your business's network causing massive damage and evading detection for even longer, inflicting new security threats and compliance violations and tarnishing the reputation of your business over the long term.

Oftentimes, hackers and internal threat actors don't even need to steal the privileged credentials they seek. They can instead locate and exploit the orphaned accounts—the accounts left behind during an employee's offboarding or enterprise role change—lingering on your network. By exploiting these accounts, hackers can conceal themselves even more and extend their dwell time.

To address these unique identity security threats, enterprises must improve the management of their privileged access accounts, limit the amount of data system administrators and superusers can access, restrict some of privileged activities on the network, and close all of their orphaned accounts.

This can be a tall order, but it is a necessary one to prevent hackers from exploiting the most powerful credentials in your network. Enter the Privileged Access Management (PAM) solution.

A good PAM solution protects the identities of individuals and applications that have the power to create accounts, delete accounts, or edit account privileges. But it goes further than that; it can help ensure regulatory compliance, maintain business integrity and responsible commercial processes, tackle security risks inside and outside your organization, and even reduce the total cost of your IT operations.

Enter this Buyer's Guide. Here we have listed the top Privileged Access Management solutions providers with individual profiles, key features, and capability references for each.

The Editors at Solutions Review cut through the rhetoric to provide an unbiased rundown of these unique vendors to unearth the technical capabilities of each. We provide the Bottom Line: our take on what makes the featured providers unique, distinctive, or exceptional.

This is the first step on an important journey.

Ben Canner, Editor
Solutions Review

80%

80 percent of data breaches involve the use of privileged credentials.[1]

62%

62% of enterprises fail to provision for privileged access accounts.[2]

51%

51% fail to enact secure logins for privileged access accounts.[2]

70%

70% of enterprises fail to discover all of the privileged access accounts in their networks.[2]

55%

55% fail to revoke permissions after a privileged employee is removed.[2]

63%

63% don't have security alerts in place for failed privileged access account login attempts.[2]

65%

65% of enterprises allow for the unrestricted, unmonitored, and shared use of privileged accounts.[3]

Sources:

1 The Forrester Wave: Privileged Identity Management, July 2016

2 Thycotic "2018 Global State of Privileged Access Management (PAM) Risk & Compliance"

3 Gartner "Best Practices For Privileged Access Management"

5 Key Capabilities To Consider When Evaluating A Privileged Access Management Solution

Two-Factor or Multifactor Authentication

Two-factor and Multifactor Authentication add additional steps to the privileged authentication process. Typically, these additional factors involve pairing something the user knows, such as a username and password combination, with an action or something the user has, such as an SMS message to their phone, a secure email, or a token. It is imperative for small-to-midsized businesses (SMBs) and large enterprises to move past the single-factor username/password paradigm which can be easily compromised.

Single Sign-On

Through Single Sign-On (SSO), regular and privileged users can log onto a single platform that gives them automatic login access to multiple application, databases, and communications for a set period of time. This allows users to present only one set of credentials for their everyday work processes. Single Sign-On is designed to eliminate certain kinds of passwords and can be restricted on privileged access accounts to protect proprietary databases.

Role-Based Access Controls

PAM solutions can allow your enterprise to operate according to the principles of least privileges, giving your employees just enough privileges and permissions to do their jobs effectively, ensuring limited network and data damage if their credentials are abused. In addition, they often provide granular, role-based access controls that allow administrators to regulate privileges and entitlements based on a user's individual role. Additional privileges via self-service requests and can be approved or denied directly.

Limit Lateral Access

PAM solutions can also limit the authority of privileged access users over their assigned enterprise systems and the commands they can enter into those systems. This is designed to prevent employees or hackers from escalating privileges without security team or administrator permission or move laterally within the network into systems they should not have control over or authority within. Your IT team can set access policies and adjust them to determine the lateral movement capabilities of your employees.

Monitoring Privilege Use

PAM solutions provide your enterprise security team the capabilities to monitor, record, and audit privileged accounts' activity on your corporate network. This not only serves as a secondary layer of protection against insider threats and hackers, but it is also often a crucial part of regulatory compliance protocols for almost all industries. This allows IT administrators to review privileged accounts in the event of an incident, and determining what actions occurred, allowing for rapid threat response.

3 Privileged Access Management Questions You Must Answer Before Selecting Your Solution

Who Has Privileged Access In your Enterprise?

Privilege creep can result in users having permissions they no longer need as they move throughout roles in your enterprise. Additionally, discrepancies in the onboarding process can bestow unnecessary access. This means your ordinary users might have privileges unknown to your security teams (and even to them)…and which can prove devastating in the wrong hands. This also means figuring out how many orphaned accounts are hidden on your network.

What Access Do Your Privileged Credentials Have?

Not all superusers are or should be created equal in terms of digital permissions. Instead, your enterprise should look to enforce the principle of least privileges throughout all of your users' identities. The principle of least privileges dictates users should have the least amount of permissions possible. Ideally, superusers should only have the access they need to accomplish their daily tasks. Ex. The superusers associated with your HR department should not have access to your financial department's databases.

What Privileged Access Management Tools Do You Have?

Legacy solutions are inadequate to handle the demands of modern enterprise's users and privileges. Your enterprise needs a next-generation solution. There is no way around it. According to One Identity, 31% of enterprises use outdated or manual methods like pen and paper to manage their superuser's credentials. But writing down passwords invites the unscrupulous to steal passwords or for those passwords to end up in the wrong hands.

Solution Provider Profiles

One of the most recognized names on the privileged access management market, Arizona-based BeyondTrust focuses on eliminating insider privilege abuse and increasing application visibility. Their Least Privilege Management and Server Privilege Management solutions offer app-to-app password management capabilities and broad support for PIV-based authentication. BeyondTrust offers machine learning and predictive analytics which analyzes privileged password, user, and account behaviors. BeyondTrust also features an established global partner network and recognized cybersecurity talent. With its 2018 acquisition by Bomgar, BeyondTrust now carries capabilities designed to eliminate manual user password changes and provide quick time to value and deployment.

BeyondTrust
5090 North 40th St
Phoenix, AZ
United States
+1 (480) 405-9131
www.beyondtrust.com

Key Features

Least Privilege Management

BeyondTrust allows enterprise security teams visibility into applications and endpoints alike and can assign privileges to apps and tasks rather than users to prevent credentials abuse. They also offer privileged session recording capabilities to facilitate privilege evaluations and possible rescinding when necessary.

Enterprise Password Management

BeyondTrust grants security teams the power to discover, profile, and manage all known and unknown assets as well as shared, user, and service accounts to gain control over credentials both regular and privileged. Also allows for the whitelisting, blacklisting, and greylisting of applications to ensure network safety.

Server Privilege

Through BeyondTrust's capabilities, users can control access to Unix, Linux, and Windows servers with fine-grained policy control. BeyondTrust also offers integration and behavioral analysis to identify security anomalies and improve their overall server security while simplifying their privileged access management deployments.

Bottom Line

BeyondTrust offers customizable privileged session management capabilities, which can provide companies with a versatile solution. BeyondTrust is ideal for companies with many different operating systems in their network and therefore mobile or digitally transforming workforces. It does support personal identity verification (PIV)-based authentication which will appeal to enterprises with high-risk data. Its 2018 merger with Bomgar (and thus also technology from Lieberman Software) has added new automation capabilities appealing to SMBs. BeyondTrust was named a Leader in the Forrester Wave for Privileged Access Management in 2018.

CA Technologies provides an end-to-end Identity Management portfolio with its Identity Suite, Single Sign-On, Advanced Authentication, and Privileged Access Management Capabilities. The corporation became a player in PAM services in late 2016 following its acquisition of Xceedium and their XSuite PAM solution. CA Technologies provides contextual/adaptive access to its Advanced Authentication product, and offers CA API Management—a full-life-cycle API management product. CA Technologies also features identity governance and administration to round out its PAM tools. Their capabilities include web single sign-on, authentication, identity and password self-service, and permissions provisioning for both cloud and on-premises applications.

CA Technologies
One CA Plz
Islandia, NY
United States
+1 (800) 225-5224
www.ca.com

Key Features

Privileged Access Management

CA Technologies enables customers to control and monitor their privileged users' access and activity, detecting and preventing the threat of internal and external attacks through user behavior analysis and through diverse authentication factors.

Single Sign-On Access

CA technologies enables single sign-on access and federated identity for privileged users, spanning the hybrid enterprise infrastructure across endpoints, cloud environments, or hybrid IT architectures.

Privileged User Governance

CA Technologies ensure that all users with privileged accounts gain and maintain the appropriate level of access corresponding to their roles both permanent and temporary. It also serves to prevent entitlement and access creep.

Bottom Line

Compared to their competitors, CA Technologies' PAM services are still quite new to the market. They have been working to innovate and expand their product, which accommodates most endpoints and integrates with IGA, SIEM, and Security Analytics solutions. They are also ideal for enterprises with a hybrid on-premises/cloud environment. CA Technologies does offer a global footprint and support infrastructure, but the recent acquisition by Broadcom has provoked some questions about what the future holds for this solution provider. However, the vendor is as strong as ever.

California's Centrify has transformed into an almost exclusively PAM-as-a-service solution provider in 2018. It offers their Privileged Access Security solution through a cloud architecture. Centrify's capabilities include single sign-on, user-provisioning, mobile device management (MDM), and multi-factor authentication (MFA). Centrify is particularly notable for its integrated MDM capabilities, which are some of the strongest in the market and match the capabilities of many MDM vendors. Centrify provides a broad set of user authentication methods including out of band (OOB) push mode and mobile endpoint biometric modes with remote access that supports different use cases including privileged users.

Centrify
3300 Tannery Way
Santa Clara, CA
United States
+1 (669) 444-5200
www.centrify.com

Key Features

Federated Privilege Access

Centrify enables secure remote access for outsourced IT administrators and third-party developers to your enterprise's digital infrastructure through federated authentication. It also secures thousands of apps and enables access to network cloud and on-premises through consolidated login parameters.

Enterprise-wide Multifactor Authentication

Centrify prevents compromised credentials by implementing multi-factor authentication across every user and every IT resource, bypassing the password weaknesses inherent in single factor authentication and due to password reuse or fatigue.

Automated Account Management

Centrify allows administrators to manage their employees' access to all their applications from any source: Active Directory, LDAP, Cloud Directory or external identity. It also secures and manages the privileged accounts used to access cloud and mobile application databases.

Bottom Line

In 2018, Centrify separated into two separate solutions providers: Centrify for privileged access management and privileged identity management and Idaptive for IDaaS offerings. This will allow Centrify to focus exclusively on improving their privilege management capabilities, which has been praised and noted by Gartner, Forrester, and KuppingerCole. Their solutions remains lightweight and well-suited to enterprises' mobile endpoint security. Enterprise customers of all sizes praise Centrify's technical and customer service. Centrify has proven to be continual innovators in their password vaulting and forwarding capabilities.

Founded in Israel and based out of Massachusetts, CyberArk commands a large share of the modern PAM market. The solution provider's Privileged Account Security Solutions offer enterprise-grade, policy-based solutions that secure, manage, and log privileged accounts and activities for both protection and evaluation. CyberArk also uses behavioral analytics on privileged account usage to detect and flag potential anomalies from insider and external threats. Key components of CyberArk's PASS include an SSH Key Manager, Privileged Session Manager, Privileged Threat Analytics, and Endpoint Privilege Manager. They also offer the CyberArk Privilege Cloud as a cloud-delivered PAM solution to simplify the storage and rotation of credentials and monitoring privileged access.

CyberArk
60 Wells Ave
Newton, MA
United States
+1 (888) 808-9005
www.cyberark.com

Key Features

Enterprise Password Vault

CyberArk secures, rotates and controls access to privileged credentials in accordance with your enterprise's privilege credentials policies to prevent unauthorized access to superuser accounts. It also features detailed audit reporting to prepare a clear view of privileged user activity.

Privileged Session Manager

CyberArk's PAM capabilities isolates, controls, and monitors privileged user access on critical Unix, Linux, and Windows-based systems, databases, and virtual machines. It also includes risk-based session review and the automation of privileged tasks. It further offers compliance demonstration tools.

On-Demand Privileges Manager

CyberArk eliminates unneeded root privileges and allows privileged users to run authorized administrative commands from native sessions. They also allow enterprises to detect, alert, and respond to attacks on privileged accounts in real-time with privileged threat analytics.

Bottom Line

One of the most recognized PAM solutions providers in the market, CyberArk offers strong capabilities in an intuitive package. Customers praise them for their excellent technical support, their proactive assistance, and their mitigation of privileged account risks. Overall, they are known to be secure, compliant with most regulatory institutions, and possessing strong password vaulting capabilities. Indeed, CyberArk was named a Leader in the 2018 Forrester Wave Report for Privileged Identity Management because of its password vaulting capabilities.

Ekran System is an insider threat protection platform that provides proper security control over your enterprise's privileged accounts. It offers lightweight software agents for all kinds of endpoints, supporting any access scheme and network architecture, including hybrid. Agents combine access management functionality with comprehensive activity monitoring, recording, and alerting and enable essential incident response capabilities. Ekran System's solution serves to enhance third-party vendor management, remote and on-site employee control, and other security tasks.

Ekran System
3500 South DuPont Hwy
Dover, DE
United States
+1 (952) 217-7041
www.ekransystem.com

Key Features

PASM Toolset for Jump Servers

Ekran System enables a full set of privileged account and session management features with its jump server software clients and centralized secure password vault. The Ekran System jump server client allows your security team to control a whole segment of your infrastructure via unlimited concurrent sessions.

One-time Passwords and Manual Login Approval

Ekran System provides one-time password functionality to protect critical endpoints, provide access to third-party vendors, and handle emergency access scenarios. These credentials may be generated by security administrators or requested by a user and manually approved by an administrator. Once access is granted, a security administrator may connect to the session and follow it in real time.

Multi-factor Authentication and Secondary Authentication

Ekran System clients enable multi-factor authentication on protected endpoints. They also support secondary authentication, identifying users of shared accounts with individual credentials.

Bottom Line

Ekran System is a flexible software platform supporting a wide range of operating systems, virtual and physical infrastructures, servers, and desktops. Offering a combination of clients with various configurations, Ekran System can fit your enterprise's infrastructure and security requirements. All parts are managed via a single web-based control center, enabling easy maintenance and multi-tenant and high-availability deployments. Ekran System deliver powerful activity monitoring and session recording capabilities, allowing supervisors to control security after access is granted. It also integrates well with other SIEM and ticketing systems.

ManageEngine is primarily based out of California and is the IT management division of the Zoho Corporation. Their privileged identity management solution incorporates their Password Manager Pro product, which can discover, store, control, audit, and monitor privileged accounts. ManageEngine also offers ease-of-use with an intuitive user interface for their PAM solutions which supports approval workflows and real-time alerts on password access. ManageEngine's discovery engine is capable of discovering and enumerating Windows local and domain accounts on the enterprise network, virtual environment, and on Linux devices with equal efficiency. The Manager Pro product acts as a centralized credentials vault and can manage shared accounts across operating systems.

ManageEngine
4141 Hacienda Dr
Pleasanton, CA
United States
+1 (925) 924-9500
www.manageengine.com

Key Features

Password Manager Pro

This can centralize password storage, and automate frequent password changes in critical systems to improve IT productivity. It can also control access to IT resources and applications based on roles and job responsibilities.

Key Manager Plus

This allows for the discovery of all SSH keys and SSL certificates in your network and then consolidate them in a secure, centralized repository. It can also create and deploy new key pairs on target systems and rotate them periodically.

Password Manager Pro MSP

For enterprises with stretched cybersecurity talent and resources, this can securely store and manage clients' privileged accounts from a centralized console, backed with multi-tenant architecture for clear data segregation.

Bottom Line

The ManageEngine Password Manager Pro is a solution best suited to small to mid-sized businesses. According to customer feedback, it is reportedly easy to install and configure, relieving the burden on enterprise's IT helpdesks. Overall its implementation is described as easy and the solution as having a strong feature set. ManageEngine will work well in hybrid systems, which may be ideal for enterprises undergoing their digital transformation or unable to completely break away from on-premises environments. The 2018 Forrester Wave report named ManageEngine a Contender.

One Identity's Privileged Password Manager solution lets enterprises enable secure automated control and auditing on their privileged accounts. The Privileged Password Manager offers session management features, as well as active directory bridge between different operating systems across the enterprise network. One Identity's products are offered via a modular and integrated approach, allowing customers to add new capabilities quickly by building on existing investments; as an example, by integrating their Identity Manager Solution with Privileged Password Manager, users can request, provision, and attest to privileged and general-user access within the same console. In 2018, One Identity acquirted Balabit specifically to boost their PAM capabilities.

One Identity
+1 (800) 306-9329
www.oneidentity.com

Key Features

Self Service Access Portal

Reduces IT effort via a customizable online intuitive "shopping cart" portal, which enables users to request access to network resources, physical assets, groups and distribution lists. It also controls access rights and permissions for their entire identity lifecycle while leveraging predefined approval processes and workflows.

Risk Reducer

Facilitates better security decisions by combining security information and policies from multiple expert sources and intelligence networks to reduce identity and personal information exposure and eliminate information silos in the enterprise network.

Privilege Safe and Privilege Account Governance

One Identity can automate granting privileged credentials, via established policies and approvals. It can also simplify privilege management via defined roles and access approval workflows.

Bottom Line

One Identity appears to be refocusing on their privileged access management (PAM) capabilities through both internal PAM solutions updates and their January 2018 acquisition of privileged access solution provider Balabit. One Identity's Privileged Password Manager is ideal for organizations focused on the password management side of privileged access. One Identity is offered in 13 languages and enjoys a strong popularity in overseas markets. As a result of its broad international support makes the One Identity Privileged Password Manager particularly attractive to global enterprises.

Since merging with Core Security in 2018, SecureAuth has supplemented their multifactor authentication use cases with more identity governance and privileged access management capabilities. SecureAuth offers specific industry solutions for healthcare, energy, and retail. SecureAuth's solutions allow customers to manage privileged access to applications in the cloud or on-premise through provisioning user access changes, certifying user access, remediating access violations, and generating audit and compliance reports. Their specific use cases include 25 multifactor authentication methods to supplant password-oriented and two-factor authentication and options to protect Microsoft Office 365 in particular.

SecureAuth
8845 Irvine Center Dr
Irvine, CA
United States
+1 (949) 777-6959
www.secureauth.com
inside-sales@secureauth.com

Key Features

Multi-Factor Authentication

SecureAuth designs its multifactor authentication to only interupt users if they find sufficient risk through multiple checks, preventing a disruption of the user experience unless absolutely necessary. The provider also offers plenty of flexible factor options to provide different levels of authentication security.

Self-Service Across Enterprise Systems

Allows for rapid deployment policies and modular architecture deploys quickly, without a substantial investment in prerequisite systems that may deter small to medium sized businesses or enterprises looking for easier deployments.

Single Sign-On

The single sign-on capability is designed to provide a smooth user experience by enabling users to present their credentials once and thus gain access to many applications. It also supports a wide breadth of federation protocols.

Bottom Line

Core Security and SecureAuth were both highly recognized in the identity security marketplace before their 2018 merger was made official. Now that they have completed their merger, SecureAuth has worked to solidify their market share as one of the largest solutions providers. SecureAuth is widely utilized in highly-regulated industries and should be considered for enterprises operating in industries operating in fields such as healthcare, banking, and natural resources. They support privileged access to major cloud environments, and they also automate credential access and usage.

Simeio Solutions provides a vendor-neutral view with Simeio Identity Intelligence Center (IIC). Founded in 2007, Atlanta-based Simeio Solutions provides a comprehensive Identity Management portfolio with solutions addressing Identity Governance, Access Management & Federation, Identity Administration, Privileged Identity Management, Data Security & Loss Prevention, Core Directory Services, Security and Risk Intelligence, and Cloud Security. Simeio Solutions can help with privileged access management for customers via on-prem, cloud, or hybrid environments with solutions designed to scale.

Simeio
55 Ivan Allen Jr. Blvd
Atlanta, GA
United States
+1 (844) 2-SIMEIO
www.simeiosolutions.com

Key Features

Risk Reduction

Simeio Solutions protects sensitive access to critical devices and systems where users are susceptible to compromises in their confidential information, change transactions, and removal of audit trails.

Policy Improvement

Simeio Solutions' Privileged Identity Management (PIM) enables continuous and sustainable policy enforcement over administrative and root accounts across an organization guaranteeing established business and security policies are continuously enforced.

Visibility Improvement

Privileged Identity Management allows for the detection, identification, and monitoring of privileged accounts and their usage. This detection improves the audit process and assists in meeting compliance guidelines.

Bottom Line

Simeio Solutions' Privileged Identity Management (PIM) automates compliance reporting with integration to existing access governance and multi-factor authentication infrastructure. Simeio offers enterprise PIM technologies with 24/7 monitoring and support, requiring no hardware or capital investments. Simeio can help mitigate serious and rapidly changing security threats while reducing the friction between business processes or employees.

Headquartered in Washington D.C. and with offices in London and Australia, Thycotic offers its Privilege Manager and Protect Windows Privilege Access products as enterprise-level privileged access management tools. Their solutions include Enterprise Password Management and Least Privilege Policy, in addition to their anti-malware solutions. Thycotic's solutions offer two-factor authentication support, integration with SIEM and CRM software, and even automated databases for disaster recovery. Thycotic offers a speedy deployment time, which can be as low as 15 minutes in Windows environments. They also offer deny-first whitelisting, least privilege strategies, and privileged behavior analytics as well as specific tools for on-premises and cloud IT environments.

Thycotic
1101 17th St NW
Washington, DC
United States
+1 (202) 802-9399
www.thycotic.com

Key Features

Secret Server Cloud

Thycotic's Secret Server Cloud is designed for instant deployment of privileged access capabilities with no infrastructure requirements and can be configured rapidly. It also offers PAM-as-a-service for no management overhead.

Least Privilege Policy

Thycotic's Least Privilege Policy automatically removes privileges and adds policy-based controls so people can use tools without needing to call on an overstretched enterprise Help Desk.

Product Integration and Application Control

Thycotic controls application download permissions and manages privilege within applications both on-premises and off. Thycotic's solution integrates with interior products such as Secret Server to enforce multi-layered protection of privileged credentials.

Bottom Line

Thycotic's quick privileged access management deployment times and strong identity and basic password management capabilities make it a good solution for small to midsized businesses looking for a no-frills, low-stress password management tool. Thycotic is often described as responsive to their customers' needs and very knowledgeable in their deployment and management support. Their least privilege policies are designed to avoid interfering with administrator and employee productivity and user experience. Thycotic was named a Leader in Privileged Identity by Forrester Research.

Located just outside of Philadelphia, Xton Technologies is a new face in the privileged access management market with experienced professionals behind it. Formed by enterprise software security experts, Xton Technologies has the express goal to provide simple and affordable PAM software to enterprises. Their XT Access Manager Solution offers multifactor authentication controls, can store and share security keys with users and superusers, delegate the execution of privileged commands, and lock down privileged accounts with suspicious activity. Xton Technologies also provide solutions to combat social engineering attacks and limit the internal attack surface. They also provide a free trial option with easy deployment and integration.

Xton
1210 Northbrook Dr
Trevose, PA
United States
+ 1 (844) 402-8708
info@xtontech.com
www.xtontech.com

Key Features

Privileged Session Management

Xton Access Manager establishes a secure, interactive session to remote Windows, Unix or Mainframe endpoints, Network Devices like Cisco, Juniper or Palo Alto, and Websites or Web Management Portals to monitor privileged access activity.

Privileged Account Management

With Xton Access Manager, access (passwords, keys, certificates, documents and more) to privileged accounts are kept safe, secure and out of the reach of threats, both internal and external.

Privileged Job Management

Xton Access Manager reduces the number of privileged accounts in the network and controls access to active privileged accounts. This enables the appropriate people or processes to perform work on critical computers and devices at the right time.

Bottom Line

Xton Access Manager is deliberately designed to be an affordable enterprise-class PAM solution that is easy to install, deploy, and manage. Enterprises of all sizes seeking out a PAM solution without complex implementation, configuration, and ongoing maintenance demands may want to consider Xton Access Manager. However, due to its relative youth in the privileged access management market, it is not as customizable as other solutions. On the other hand, they have innovated heavily in the managed services provider marketplace, offering privileged access management to such providers to help secure their client base.

ABOUT SOLUTIONS REVIEW

Solutions Review is a collection of technology news sites that aggregates, curates, and creates the best content within leading technology categories. Solutions Review's mission is to connect buyers of enterprise technology with the best solution sellers.

Over the past four years, Solutions Review has launched ten technology buyer's guide sites in categories ranging from cybersecurity to wireless 802.11, as well as mobility management, business intelligence and data analytics, data integration, and cloud platforms.

Information for this report was gathered via a meta-analysis of available online materials and reports, conversations with vendor representatives, and examinations of product demonstrations and free trials. Solutions Review does not endorse any vendor, product or service depicted in this publication and does not advise technology users to base their vendor selection entirely on this research. Solutions Review disclaims all warranties, expressed or implied, regarding this research, including any warranties of merchantability or fitness for a particular purpose.