thycotic

How CISOs Can Win a Seat with The Board of Directors

Featuring Security Research by Gartner Group

Issue 1

Gartner

CISOs Positioned to Lead at the Executive Table

With major breaches of corporate and government cybersecurity grabbing global headlines, the position of Chief Information Security Officer may appear as a hot seat at the executive table that few would aspire to. Yet, the role of CISO has never presented more challenges—and more opportunities---for leadership than in today's interconnected world.

As an information security leader CISOs have the responsibility to protect their organization's critical assets. But in order to enhance and grow their role as CISO, they are exploring ways to use their knowledge to further the growth of the business rather than simply protecting its information assets.

CISOs today are managing cyber security from an enterprise risk management viewpoint, assessing the impact of security changes on their business as a whole. And to fully earn a place at the executive table, CISOs are rapidly becoming business enablers---finding ways to use secure technologies that support revenue and profit initiatives. That means ensuring the tools and policies they implement will both improve their organization's security posture and promote more efficient business processes---adding value beyond just securing the IT infrastructure.

Cybersecurity Threats Raise the CISO's Visibility—and Leadership Potential

In recent years the responsibilities and functions of the CISO have become much more visible and important to the success of most businesses. That's because critical infrastructure and information have become prime targets for attackers seeking to gain from financial fraud or other criminal activities.

While high profile breaches have raised the visibility of the cybersecurity function and the role of the CISO---sometimes to the board level---the cyber security challenges and potential for leadership by CISOs have grown as well.

With more connectivity through the Internet of Things (IoT), disruptive Ransomware attacks, the disappearing perimeter as employees use multiple devices and social media, cyber threats and risks have multiplied and accelerated. Recent reports indicate that the target for attackers has shifted from perimeter servers/services to end user devices and end user identities. Once an end user device and/or identity has been compromised, the entire organization is at risk. Even worse, it may take weeks or even months before a breach is detected.

According to the 2016 Verizon Data Breaches Investigations Report (DBIR), 63 percent of breaches were the result of weak or stolen credentials, allowing an attacker or insider to use those credentials and act as a trusted user to perform malicious activity or financial crime. IT administrator privileged access is of particular concern as compromising these accounts literally provides an attacker with the "keys to the kingdom" in terms of accessing just about any confidential information within an organization.

10 Questions CISOs must answer to gain a seat on the Board of Directors

Corporate directors play an important role in ensuring their companies have sufficient policies and resources in place to address IT security and to respond in the event that the company suffers a cyber-attack. To gain access to the board of Directors, CISOs must be able to answer the following questions to prove they are fulfilling their oversight role in managing cyber risk.

Questions include:

1.) What are the company's "crown jewels" and are these effectively protected? I.e. privileged account passwords

2.) Has the company effectively allocated resources based on its risk appetite and strategic assets?

3.) What technical capabilities does the company have in place to identify malicious events?

4.) How frequently does the board receive cyber security updates?

5.) What is the company's response plan in the event of an attack?

6.) How often is the response plan tested?

7.) What relationships does the company have or need to develop with government and other organizations to respond effectively to a breach?

8.) What is the security technology roadmap and budget estimates to implement the IT security strategy?

9.) Has the company tested its response plan with a cybersecurity exercise?

10.) How has the company organized itself to approach cybersecurity?

The Path to Improved Implementation of IT Security Technologies

Recent research has identified several leadership qualities exhibited by successful CISOs. These include running IT security like a business, planning security investments around the value they deliver to the business, and effectively working with key stakeholders across the enterprise. Just as important, successful CISOs take the time and effort to ensure the security tools they choose to implement improve both security and business processes as well as improving the productivity of IT staff.

One prime example of this trend focuses on Identity and Access Management (IAM) technologies. Historically, IAM solutions have stood apart from typical security tools because they are much more about "letting the good guys in" than about "keeping the bad guys out." Successful CISOs are recognizing there are solutions available that can effectively do both with less time and effort.

Since hackers increasingly target "insider" accounts (e.g., employees, partners, contractors, consultants, and customers) to get access to networks, servers, applications, and, most importantly data, better IAM has become critical. For most attackers, taking over low-level accounts is only the first step. Their real goal is to capture administrative (i.e., "admin") or privileged accounts so they can escalate their access to applications, data, and key administrative functions. Once accessed, these privileged credentials almost always enable hackers to conceal their activities within the guise of a legitimate administrative user.

This situation often sets up the traditional conflict between IT security professionals and those charged with delivering IT services to keep the business running and growing. IT administrators are understandably "suspicious" about security measures that they see as interfering with their ability to perform tasks that enable the business to function properly. To overcome this conflict, successful CISOs are discovering Privileged Access Management (PAM) security solutions that deliver enhanced security while actually improving the productivity of IT administrative functions.

Thycotic Privileged Account Management and Security Solutions

Thycotic is pioneer in delivering IT security solutions that protect organizations from cyber-attacks which have made their way inside the network perimeter to strike at the heart of the enterprise. Thycotic software solutions are focused on protecting the privileged accounts that have become a prime target in the lifecycle of today's cyber-attacks. Privileged accounts are pervasive and act as the "keys to the IT kingdom," providing complete access to, and control of, all parts of an IT infrastructure and critical business data. Once compromised by an external hacker or malicious insider, privileged accounts allow attackers to take control of and disrupt an organization's IT infrastructures, steal confidential information and commit financial fraud.

Thycotic PAM security solutions are designed to be implemented faster, are easier to use, seamlessly integrate into your environment and can be deployed in traditional on premise data centers or as a cloud solution. IT Admins typically accept and embrace our security solutions because they also make their life easier and more productive.

Privileged accounts are used by system administrators, third-party and cloud service providers, applications and business users. They exist in nearly every connected device, server, router, hypervisor, operating system, database, and application throughout the enterprise. Due to the broad access and control they provide, exploiting privileged accounts has become a critical vulnerability that must be addressed to properly secure critical organization assets.

Our Privileged Account Management security solutions proactively protect privileged accounts, limit user privileges and control applications on endpoints and servers. Recognizing that privileged account credentials represent one of the most vulnerable aspects of an organization's IT infrastructure, Thycotic offers comprehensive, affordable PAM security solutions for every level of business enterprise.

To learn more go to www.thycotic.com

Source: Thycotic

Research from Gartner

Market Guide for Privileged Access Management

Privileged access is a major focus for security and I&O leaders looking to prevent and detect breaches, maintain individual accountability, and increase operational efficiency. Products are consolidating around two major patterns: managing privileged passwords and delegating privileged actions.

Key Findings

- Prevention of both breaches and insider attacks remains the major driver for the adoption of privileged access management (PAM) solutions, followed by regulatory compliance and operational efficiency.
- PAM tools allow organizations to comply with high-trust requirements for privileged access by offering or integrating with high-trust two-factor authentication (2FA) capabilities.
- Organizations starting with PAM deployments often struggle to achieve the desired business value due to a mixture of political and cultural issues.
- Emerging use cases for PAM tools are cloud security, anomaly detection and securing the software development life cycle.

Recommendations

Identity and access management (IAM), infrastructure and operations (I&O), and security leaders:

- Don't buy too many tools at once — some of them might be shelfware for a long time. However, plan future extension purchases for the next three years to avoid potential pricing "sticker shocks."
- Use the Market Recommendations section to help choose an approach for selecting the type of PAM tool that fits the most urgent requirements.
- **Small and midsize organizations:** Look for integrated high availability features, bundled 2FA and value-priced bundled offerings. Large organizations: Scrutinize vendors' offerings for 2FA integration support, scalability and autodiscovery features.
- Pay special attention to secure nonhuman service and application accounts — they are major sources of operational and security risk, and most organizations have a significant number of them.
- Engage system and network administrators early, and have them participate in the vendor selection — their support is critical for a successful implementation.

Strategic Planning Assumption

By 2019, 30% of new PAM purchases will be delivered as a service or run in the cloud (up from less than 5% today), reflecting needs to manage virtual infrastructure and cloud services.

Market Definition

PAM technologies help organizations to provide secured privileged access to critical assets and meet compliance requirements by securing, managing and monitoring privileged accounts and access.

PAM tools offer features that allow users to:

- Control access to privileged accounts, including shared and "firecall" (emergency access) accounts.
- Automatically randomize, manage and vault passwords and other credentials for administrative, service and application accounts.
- Provide single sign-on (SSO) for privileged access, so credentials are not revealed.
- Delegate, control and filter privileged operations that an administrator can execute.
- Eliminate hard-coded passwords by making them available on demand to applications.
- Integrate with high-trust authentication solutions to ensure required levels of trust and accountability.
- Audit, record and monitor privileged access, commands and actions.

The tools apply to privileged access spanning a wide range of systems and infrastructure — OSs, databases, middleware and applications, network devices, hypervisors, and cloud services (infrastructure as a service [IaaS], platform as a service [PaaS] and SaaS). Although the major focus is on managing privileged access, PAM tools are also used by some organizations to manage shared access to non-administrative shared accounts, such as an organization's official social media accounts.[1] Accounts used by nonhuman users, such as services or applications — whether of an administrative nature or not — are also in scope.

Market Direction

As the PAM market heads into early maturity, two popular, distinct adoption approaches have evolved as the predominant focus for organizations considering an investment into PAM tools. This has led Gartner to redefine[2] the classification of the PAM market into these two main categories:

- **Privileged account and session management:** Privileged accounts are protected by vaulting their credentials. Access to those accounts is then brokered for human users, services and applications. Password and other forms of credentials for privileged accounts are actively managed (i.e., changed at definable intervals or upon occurrence of specific events).

- **Privilege elevation and delegation management:** Specific privileges are granted on the managed system by host-based agents to users logged in with unprivileged accounts. This includes privilege elevation, in the form of allowing particular commands to be run with a higher level of privileges.

Although managed and cloud-based PAM services are starting to pick up, the overall PAM market is still very much dominated by the sale of on-premises software and appliances. Gartner estimates that the combined revenue of the PAM Market Guide participants in 2015 was $690 million, which represents a 33% growth rate over an adjusted 2014 market size of $521 million (see Appendix — Vendor Revenue section).

As in previous years, the PAM market continued to see extensive activity during 2015 and the first quarter of 2016:

- Bomgar acquired password management technology from Pitbull Software[3] and was acquired by Thoma Bravo.[4]

- CA Technologies acquired Xceedium.[5]

- Osirium[6] and Wallix[7] successfully completed IPOs.

- CyberArk acquired Viewfinity.[8]

- Thycotic successfully raised capital[9] and acquired Arellia.[10]

Interest in PAM technology is driven by several factors:

- The risk of breaches and insider threats

- The existence of malware that specifically targets privileged accounts

- Operational efficiency for administrator access

- Regulation and failed audits, because auditors are paying closer attention to privileged accounts, and regulations are forcing organizations to create a trail of evidence for privileged access

- Access to privileged accounts by third parties: contractors, vendors and service provider technicians

Gartner has noticed a shift in interest over the last year from predominantly large and regulated organizations to smaller, unregulated organizations. Drivers for the investments into PAM technology are primarily the desire to mitigate risks of data breaches and insider abuse. Additionally, we have noticed that some large organizations that bought PAM tools several years ago, mainly for compliance reasons in isolated environments, are now taking another close look at their existing deployments to get more value out of them. This usually leads to extension of PAM deployments. Several organizations are using this opportunity to re-examine the market to evaluate other vendors' offerings as an alternative to purchasing more of the incumbent vendor's solution.

In terms of geographical distribution, Gartner sees considerable interest from North America,[11] followed by Europe[12] and Asia.[13] In addition, we notice increased adoption in Gulf Cooperation Council countries due to the introduction of several national regulatory frameworks[14] targeting critical infrastructure industries.

Pricing and bundling remain highly variable within the market and underline the need to shop around. Some Gartner clients have indicated that they have selected a vendor based on specific features that they ultimately end up not using, or buy additional modules that end up as "shelfware." Many vendors now bundle more capabilities together in their entry-level offerings; however, other vendors have split up their offerings into multiple editions, or unbundled newer capabilities that are sold as separate modules.

Vendors use multiple distinct pricing metrics (per named user, per system, per concurrent session), and adding to the confusion is that some vendors use distinct pricing metrics for different modules of their products! Organizations are advised to plan ahead for evolving requirements over the next three to five years by forcing vendors to provide pricing for expected future scenarios, and Gartner clients are encouraged to use inquiries to discuss these plans with an analyst.

The market remains very competitive. Most vendors are working to extend current capabilities, add competitive features and introduce new delivery mechanisms:

- **DevOps:** Some organizations are now looking to use PAM tools to enable their DevOps initiatives by automating the management and delivery of keys and credentials for continuous integration/deployment frameworks.
- **Cloud and hypervisor:** As organizations continue to take up virtualization and cloud infrastructure, PAM vendors continue to build out features to discover and manage infrastructure:
  - Automated discovery and enrollment of hypervisor guests and IaaS instances
  - Fine-grained authorization of infrastructure management operations (that can create/modify/delete/start/stop individual instances)
  - Password vaulting and shared account password management for SaaS (overlapping with some identity and access management as a service [IDaaS] vendors' offerings)
- **Cloud-based PAM solutions:** In 2015, Centrify launched its cloud-based privileged account and session management (PASM) solution exclusively as a service for managing on-premises and cloud-hosted infrastructure. Other vendors, such as Arcon and Thycotic, offer their solution as a service in addition to other delivery options. Other vendors also offer their solution as a virtual image on the Amazon Web Services (AWS) marketplace and Azure marketplace.
- **Privileged usage analytics:** Some vendors, such as Balabit, CyberArk and ObserveIT, are using behavioral analytics on privileged account usage to detect and flag anomalies.
- **Vulnerability management:** Some vendors, such as BeyondTrust, are leveraging synergies between privileged command delegation and vulnerability management to detect and prevent unsafe operations on potentially compromised or vulnerable systems. Vulnerability assessments can also be correlated with privileged activity for risk scoring.
- **System and privileged account discovery:** Identifying all systems and the corresponding privileged accounts is important, because every privileged account is a potential source of risk. However, this is a major challenge, as it is easy for privileged or default system accounts to be forgotten and left out. This is exacerbated by virtualization and hybrid environments that include cloud infrastructure. In such a dynamic environment, systems and accounts can easily fall through the cracks of privileged access management. Autodiscovery capabilities attempt to automate the discovery of currently unmanaged systems and accounts, and come at different levels:
  - **Ad hoc discovery** requires running a separate task to scan the network and associated information (such as in Active Directory [AD]) to run an as-is analysis of the current environment, and compare this to the last known state to find changes. Most vendors that offer autodiscovery fall into this category.

- **Concurrent discovery** works on a continuous basis where changes in AD, as well as to hypervisors, are detected as they happen and can trigger automatic enrolment workflows within the PAM solution. Lieberman Software's ERPM is the best-known example of this.

- **Secure Shell (SSH) key discovery and mapping.** Vendors, such as SSH Communications Security and Venafi, provide the capability to discover and map SSH keys to accounts and/or users. This covers both human and nonhuman entities.

- **Privileged identity governance and administration:** Several vendors with identity governance and administration (IGA) as well as PAM products are leveraging synergies between them to track and manage account ownership and privileged entitlement life cycles. Other stand-alone PAM vendors have integrated their products with some IGA products from other vendors.

Market Analysis

Most PAM vendors provide tools that fall into one or both of the categories described in the Market Direction section:

- Privileged account and session management

- Privileged elevation and delegation management

The difference between the two approaches is that the first case controls access to individual accounts with always-on privileges, whereas the second case is more granular, controlling the invocation of a specific privilege in the form of executing a command with elevated privileges on a case-by-case basis. Both of these approaches complement each other, and many organizations will ultimately deploy technology to address both approaches. However, attempting to deploy both types of tools at the same time is rarely feasible — organizations should start with one type of tool first, before attempting to roll out the other[15] (see the Market Recommendations section to help choose an approach for selecting the type of tool that fits the most urgent requirements).

Privileged Account and Session Management

Solutions that fall into this category will provide an encrypted and hardened vault for storing account passwords, keys, other credentials and other secret information. Passwords of administrative, shared and service accounts are managed by changing them at configurable intervals or upon occurrence of specific events (even, if desired, after every use16) according to definable policies. Reconciliation features verify that passwords have not been changed through any other mechanism, and password history is available to support restores from earlier backups. Comprehensive reporting features provide detailed information on privileged accounts, access rights, approvals and activity.

Access Control for Shared Accounts

PASM tools support privileged account sharing by controlling authorized administrators' access to accounts. Administrators will log on to the PASM tools using high-trust 2FA — usually through a web portal — and can then request access to a shared account on a particular system.

PASM tools often implement workflow features for administrative users to request access, and for authorized approvers to grant this access. In some cases, this can also be automated by including external data sources — for example, service desk tickets that contain change control authorizations, or incident reports that document outages or anomalies that need to be rectified. Most products integrate with some IT services support management (ITSSM) systems out of the box and/or provide APIs to validate administrative access requests by cross-checking them with information from ITSSM systems. Buyers should look to leverage existing integrations to link privileged access with change management processes. PASM tools also support "break the glass" scenarios for emergency and disaster recovery purposes, including the support for firecall accounts.

As a general rule, users of privileged accounts should not be allowed to see or access the actual passwords for these accounts, because they could reuse them or pass them on, therefore eroding the usage control of the accounts. Instead, most of these tools will automatically initiate SSO to sessions without disclosing credentials. A session is initiated using a well-known protocol (SSH, Remote Desktop Protocol [RDP], Independent Computing Architecture [ICA], Virtual Network Computing [VNC], HTTPS, X11), and credential injection happens at this time (see next section).

This helps to comply with the imperative that passwords for shared accounts must not be shared, which can lead to uncontrolled access. When

the only practical way forward is to disclose a password to the user, it can be placed into the clipboard or copy buffer, or even by displaying them followed by an automated password reset as soon as the current password's use has concluded. Access to shared accounts can be contingent on additional workflow approvals and/or high-trust authentication methods. An audit trail documents all privileged account use.

Some PASM tools also support the notion of preconfigured tasks, which allow an authorized user to execute a specific batch of commands using a shared account. In some specific and simple use cases, preconfigured tasks can provide an alternative to controlled privilege elevation and delegation (PEDM) tools (discussed in the Privilege Elevation and Delegation Management section).

Privileged Session Management

While single sign-on to privileged sessions for administrators is a standard feature for today's PASM tools, some vendors offer additional privileged session management (PSM) capabilities, either built into the standard version of the product or as an additional licensable module:

- Real-time monitoring (for dual control or "four eyes" principle/session shadowing)
- Protocol-based command filtering for sessions to either restrict what an administrator can do, or to raise an alert on suspicious or dangerous activity
- Session recording (for later analysis)
- Application session separation: Launching interactive local applications (mostly Windows-based) in a remote, contained environment (such as a terminal server), rather than permitting administrators to run them on potentially compromised endpoints

A small number of vendors, such as Balabit, ObserveIT and NRI Secure Technologies, specialize in delivery of these PSM features in a stand-alone manner, without offering broader PASM capabilities around credential management.

The majority of vendors use a gateway (or proxy) approach for session management and recording. With this approach, all traffic passes through one or more control points. Another approach is to initiate direct connections from the administrator's workstation to the target systems, and to inject credentials into the session on the workstation using a local control. Recording then happens on the administrator's workstation and is forwarded to a collector. While this can be beneficial in the case where a system is accessed at a remote location that has only very limited bandwidth, one major disadvantage is that the approach requires a high level of reliance on trust and integrity in the administrator's workstation in order to rule out that a compromised workstation will ultimately compromise session control and recording. Achieving this level of assurance on third-party-owned workstations, compared to workstations operating internally, presents new challenges that IAM and security leaders need to account for.

With respect to session recording and transcription, features range from a simple searchable key or input/output (I/O) logging to "over-the-shoulder" video recording of graphical sessions. For the latter, most tools provide very efficient compression, but real differentiators are found in the session playback functionality: The most basic tools will support only a 1:1 playback of the entire session. Some other tools will take regular screenshots of a session every few seconds. More advanced playback features allow automatic skipping forward and backward, based on user activity. When protocols such as RDP are used, some tools can gather additional metadata events, such as applications executed, windows opened, text typed. For SSH, many tools store input and output streams. More vendors are now supporting full optical character recognition (OCR), scanning entire graphical sessions with extensive protocol support.

In addition to session recording, some tools support session monitoring and alerting in real time. This allows live monitoring of privileged sessions by administrators or managers, who can intervene or even terminate the session if necessary. This feature is also known as the "four eyes principle" or "session shadowing." Some tools can also analyze privilege sessions in real time and generate alerts or notifications when a suspicious behavior is detected. These can be sent to a security information and event management (SIEM) system, or supervisors can be alerted.

Brokering Privileged Credentials to Applications

PASM tools also manage passwords and other credentials for nonhuman access, such as service or application accounts. These are accounts used by automated services or applications for accessing other applications, data or systems.

An important aspect of PAM is to broker access to accounts used by nonhuman users (i.e., applications and services). Most PASM tools will have functionalities to manage service and application accounts by one or more of the following methods:

- Rotating credentials and changing them in situ — that is, in the place where they are held by the system, application or service. Examples are Windows services that run under local or domain service accounts — whenever the password is changed, the services require that their service configuration is updated on each local system where the services run.
- Allowing an application to retrieve the password from the vault through a network-protocol-based API.
- By use of application-to-application password management (AAPM) agents that are installed on local systems and allow applications to access credentials using host-based access control mechanisms, described in the next section.

Application-to-Application Password Management

AAPM tools are agents that allow applications or scripts to gain access to application credentials through proprietary software development kits (SDKs) and command line interfaces (CLIs). These tools are available as additional modules to PASM solutions and, in some cases, are even available stand-alone, although sometimes these modules are already included in the license of the base product at no additional charge (such as in the case of BeyondTrust and Hitachi ID Systems).

AAPM tools usually provide a caching function that is kept in sync with the main PASM vault. They implement local (host-based) access controls for applications that attempt to fetch credentials, such as:

- Application fingerprinting or checksum verification of the application, its configuration and other dependent files to prevent tampering
- Environment verification, such as the user ID or process under which the application is started, from which directory it is started, and so on
- One-time password mechanisms, where after every invocation the next sequence password is generated from a seed, stored and verified upon subsequent invocation

AAPM tools allow elimination of hard-coded and unencrypted stored credentials altogether and present the most secure form of delivering credentials to applications or scripts, when no other mechanisms exist to safeguard locally stored credentials, at the cost of modifying the application. The modification is usually simple; however, testing must happen for every application modified, which places a considerable burden on organizations.

Privilege Elevation and Delegation Management

PEDM tools are local agents that allow certain commands to be run under elevated privileges, or by restricting or replacing commands that can be executed. The tools use policies to limit the scope of what administrators can do, or to prevent administrators from carrying out unsafe activities that could be a vector for malware or that potentially could do great damage.[17] The difference to the approach of PASM tools is that PEDM will elevate individual commands, but not give access to an unrestricted privileged session. PEDM tools also monitor and record privileged activity on the systems — either upon login, or during execution of privileged commands.

On Windows systems, PEDM agents are kernel-based. Apart from being able to tightly control who can run which privileged commands, these tools are also an important level of protection from Pass-the-Hash attacks.[18] For this reason, Windows PEDM tools are not only deployed to establish controls for system administrators, but many organizations have also deployed Windows PEDM tools pervasively on endpoints for purposes other than privileged access management, such as application control.

On Unix and Linux systems, many PEDM vendors integrate at the shell level by shipping replacements of shell and other common commands, such as text editors (to prevent shell escapes). Other vendors, such as CA Technologies, offer kernel-based PEDM tools for Unix and Linux as an additional option. Some vendors ship a replacement or extension to the popular Unix "sudo" command. Unix PEDM tools are often combined with, or include, Active Directory bridging tools that allow authorized users to log in to Unix and Linux systems using their Windows domain account.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Tables 1 and 2 below present the representative vendors and their key capabilities for PASM and PEDM, respectively. Each mark indicates that the vendor in question has an offering within the particular capability. The existence of more marks for a particular vendor must not be interpreted to mean a better or more appropriate product! Depth of features and functionality differ widely within every capability. Some vendors that only address one or few capabilities are very good at what they do. Keep in mind that some products from different vendors can work together to create a best-of-breed solution at a more attractive price.

Vendors With PASM Solutions

Table 1 denotes capabilities that are available in a vendor's solution, either as an integral part of the basic solution or as an optional licensable component:

- A vendor may have multiple "editions" of a main product. In Table 1, features that exist in the basic (lowest-priced) edition are market with the block symbol (Đ), whereas features only existing in higher priced editions are marked with the dollar sign ($).
- A vendor may offer individual feature or capabilities as separate products that need to be licensed separately.

The "Product Name(s)" column lists all components that would need to be acquired to deliver the functionality indicated:

- Every vendor listed must have a solution that is able to actively manage (i.e., change) credentials for privileged accounts on multiple systems, network devices and applications. Solutions must include a vault, and allow access to privileged accounts according to specific policies. Single sign-on features must exist that allow a privileged session to be automatically established using a protocol such as SSH, RDP or HTTP without revealing credentials to the user. Vendors that do not deliver this functionality, or can only deliver this functionality in combination with other products, are not listed in Table 1.
- Command filtering: The ability to limit commands or operations using an agentless approach by filtering the underlying network protocol (SSH, HTTP, and so on).
- Built-in HA: Integrated high-availability features that do not require an organization to deploy and operate an external highly available relational database management system (RDBMS; such as database clustering or database replication). Vendors that are not listed with this feature support high availability in combination with external components, such as database clustering.
- AAPM: Agent-based application-to-application password management capability, as described in the Market Analysis section.

Here's how Gartner defines PAM market share segments:

- Small: Less than $10 million
- Medium: Between $10 million and $30 million
- Large: Greater than $30 million

Vendors With PEDM Solutions

Table 2 denotes capabilities for agent-based controlled privileged elevation and delegation on multiple platforms. The "Product Name(s)" column lists all components that would need to be acquired to deliver the functionality indicated:

- Unix/Linux, Windows, IBM i, IBM z/OS: Denotes support for the respective operating system.
- Unix/Linux AD Bridging: The vendor offers an agent-based Active Directory bridge for multiple Unix and Linux systems. Vendors that provide Unix/Linux AD bridges without PEDM solutions are not listed in this table.

Table 1. Representative PASM Vendors and Their Key Capabilities

Vendor	Market Share	Key Features					Product Name(s)
		Session Recording	Command Filtering	Built-In HA	AAPM	Form Factor	
Applecross Technologies (Australia)	Small	■				$	Privileged User Manager
Arcon (India)	Medium	$	$	■	$	H, S, Svc, V	ARCOS (Access and Root Control Solution) Enterprise Privileged Account Management, Privileged Session Logging, Hardcoded Password Management
BeyondTrust (U.S.)	Large	■		■	■	H, S, V	PowerBroker Password Safe
Bomgar (U.S.)	Small	$	$		$	H	Privileged Access Management
CA Technologies (U.S.)	Large	■	■	■	$	H, V	CA Privileged Access Manager, CA Privileged Access App to App Manager
Centrify (U.S.)	Large	■		■	■	Svc	Centrify Privilege Service
CyberArk (Israel)	Large	$	$	$	$	H, S	Enterprise Password Vault, Privileged Session Manager, Enterprise High Availability Module, Application Identity Manager

continue

Dell (U.S.)	Large	$	$	$	$	H	Privileged Password Manager, Privileged Session Manager
Hitachi ID Systems (Canada)	Small	■		■	■	S, V	Privileged Access Manager
IBM (U.S.)	Medium	$	$		$	V	IBM Security Privileged Identity Manager, IBM Security Privileged Identity Manager Session Recorder, IBM Security Privileged Identity Manager for Applications
Iraje (India)	Small	■	■	■		H	Privileged Identity Management
Kron (Turkey)	Small	■	■				Single Connect
Lieberman Software (U.S.)	Medium	$	$			S	Enterprise Random Password Manager, Application Launch Server
ManageEngine (U.S.)	Medium	$		$	$	S, V	Password Manager Pro (Multiple Editions)
MasterSAM (Australia)	Small	$	$	■		S	Privileged Management System, Analyst, Integrated Gateway, App Gateway
Micro Focus (NetIQ) (U.K.)	Medium	■	■	■		S	Privileged Account Manager
MT4 (Brazil)	Small	■	■	■	■	H, V	Senha Segura

continue

Novasys (Argentina)	Small	■				S	SATCS
Onion ID	Small	■	■	■		Svc, V	Onion ID
Oracle (U.S.)	Medium	■	■			S	Oracle Privileged Account Manager
Osirium (U.K.)	Small	■		■		V	Osirium
Thycotic (U.S.)	Medium	$	$		$	S, Svc	Secret Server (Multiple Editions), Privilege Manager for Unix
Wallix (France)	Small	$	$	■		H, Svc, V	WAB Access Manager, WAB Password Manager, WAB Session Manager
Wheel Systems (Poland)	Small	$	$	■	$	H, V	Fudo Privileged Session Manager, Fudo Secret Manager, Fudo Application to Application Password Manager

Feature Availability Legend:
■ = Included in base product
$ = Available as an option or higher-priced edition
Blank = Not Available
S = Software; **H** = Hardware Appliance; **V** = Virtual Appliance; **Svc** = Cloud-based Service
Feature via OEM/Reseller Partnership Legend:
$ = Available as an option
Note: More marks do not signify a better product. Built-in high availability is included as a criterion based on an increased interest shown by small and midsize organizations.

Source: Gartner (August 2016)

Table 2. Representative PEDM Vendors and Their Key Capabilities

Vendor	Market Share	Key Features					Product Name(s)
		Unix/ Linux	Unix/ Linux AD Bridging	Windows	IBM i	IBM z/ OS	
Applecross Technologies (Australia)	Small	■					Privileged User Manager
Arcon (India)	Medium	■		■			ARCOS Privileged Account Access Control
Avecto (U.K.)	Medium			■			Defendpoint
BeyondTrust (U.S.)	Large	■	■	■			PowerBroker for Unix/Linux, PowerBroker Identity Services, PowerBroker for Windows
CA Technologies (U.S.)	Medium	■	■	■		■	CA Privileged Access Manager Server Control, CA ACF, CA Top Secret
Centrify (U.S.)	Large	■	■	■			Centrify Server Suite
CyberArk (Israel)	Large	■		■			On-Demand Privileges Manager, Viewfinity
Dell (U.S.)	Large	■	■	■			Privileged Access Suite for Unix, Privilege Manager Pro
Enforcive Systems (U.S.)	Small				■	■	Enterprise Security for IBM i, Enforcive/ Security for CICS
Fox Technologies (U.S.)	Medium	■	■				BoKS ServerControl

continue

HelpSystems (U.S.)	Small				■		Safestone Powerful User Passport, PowerTech Authority Broker, Safestone Multiple System Administrator
MasterSAM (Australia)	Small	■		■			Privilege Management System, Analyst, Secure@Unix/ Linux, Secure@ Windows
Micro Focus (NetIQ) (U.K.)	Medium	■		■			Privileged Account Manager
Raz-Lee Security (Israel)	Medium				■		iSecurity Software Suite
Thycotic (U.S.)	Medium			■			Application Control Solution

Feature Availability Legend
■ = Available; Blank = Not Available
Note: More marks do not signify a better product.

Source: Gartner (August 2016)

Table 3. Vendors With Their Product Name(s) and Description

Vendor	Product Name(s) and Description
Balabit (Luxembourg)	Shell Control Box (delivered as a physical or virtual appliance) is a stand-alone PSM solution that supports an extensive list of network protocols, and can act as a gateway or transparent proxy. Balabit also offers Blindspotter, a user behavior analytics engine that can identify suspicious privileged activity.
Conjur (U.S.)	Secrets Management (delivered as software) enables organizations to centralize management of all secrets, such as encryption keys, credentials, API keys and so on. Role-based access control policies manage authorization between systems and/or code. Particularly noteworthy is Conjur's experience and support of integrating DevOps processes, such as continuous integration and deployment.
HashiCorp (U.S.)	Vault (delivered as software) stores, manages and grants access to credentials and other secrets through APIs. Vault is delivered in two editions: free open-source, and commercially supported Enterprise version with additional features.
Microsoft (U.S.)	Privileged Access Management is a solution based on Microsoft Identity Manager (MIM). It works by using MIM's access request user interface and workflow capabilities to broker temporary membership in privileged security groups.
NRI SecureTechnologies (Japan)	SecureCube Access Check (delivered as software) is a stand-alone PSM solution that integrates to extend PowerBroker Password Safe from BeyondTrust or iDoperation IM for Access Check by NTT Software (available only in Japan). Apart from extensive PSM capabilities, SecureCube Access Check can also monitor and log file transfers and database sessions to Oracle RDBMS systems.
ObserveIT (U.S.)	ObserveIT (delivered as software) is a PSM solution that works as an agent for Windows and Unix/Linux (a gateway-based mode is also available, but is less common). The solution provides detailed, fully searchable recording of all user activity and user behavior analytics.
Red Hat (U.S.)	Red Hat offers two software solutions: Commercially supported Red Hat Identity Management (IdM) and free, open-source FreeIPA (both delivered as software) address authentication, user management and privilege management and elevation for Linux and can integrate with Active Directory through Kerberos.
SecureLink (U.S.)	SecureLink is a cloud-based PSM service to control privileged access by third parties, such as vendors. The service is sold in two editions: SecureLink for Enterprises provides an environment in which an organization can control remote support access to multiple vendors. SecureLink for Vendors is the counterpart for service providers or vendors that provide remote service or maintenance to a variety of customers. Both modules can be used independently, but they can be linked to provide synergies in terms of integrated user management.
SSH Communications Security (Finland)	CryptoAuditor (delivered as a hardware or virtual appliance) is a stand-alone PSM appliance with a built-in privileged account credential vault. Some organizations are also using the company's Universal SSH Key Manager (delivered as software or virtual appliance) for managing privileged access for humans and applications based on a centralized management platform for SSH keys and access.
Venafi (U.S.)	Venafi Trust Protection Platform (delivered as software) offers centralized SSH and key management capabilities, used by some organizations to also manage privilege access for humans and applications. Venafi also includes features for DevOps automation through integration with continuous integration tools.

Source: Gartner (August 2016)

Other PAM Solutions

Several vendors offer solutions that do not entirely fall into the main categories of PASM or PEDM, yet those solutions have been deployed successfully by clients. The vendors described in Table 3 provide an alternative way to mitigate risks around privileged access, or provide a set of specific and deep capabilities to augment existing PAM deployments.

Market Recommendations

Organizations considering PAM tools should keep in mind that both types of tools (PASM and PEDM) are complementary, and some organizations eventually deploy both of them to address most risks associated with privileged access. However, we advise against attempting deployment of both types of tools at the same time, because of the significant cultural change and integration involved. To choose a starting point for a PAM tool, Gartner recommends the following methodology:

- Most organizations will want to start by first deploying PASM tools to manage shared and service accounts. PASM technology has the advantage that it applies to different types of systems, including network appliances and even SaaS or applications, therefore allowing an organization to manage privileged access across platforms — although at a lower granularity. High-trust 2FA authentication must be enabled for access to the PASM tools, and session recording and monitoring should be activated. Shared account access to Windows systems should leverage local privileged accounts rather than domain admin accounts. Federal agencies that are required to use multifactor personal identity verification (PIV)-based authentication for privileged users as part of HSPD-12 and Cybersecurity Strategy and Implementation Plan (CSIP) directives[19] should look out for vendors that offer native support for Common Access Card (CAC) and PIV smartcards. CA Technologies (Privileged Access Manager, formerly Xceedium Xsuite) and BeyondTrust offer broad support for PIV-based authentication.

- Organizations should first look toward Windows PEDM tools for use pervasively if they are predominantly Windows-based, already have high-trust 2FA authentication in place and currently allow administrators to use accounts with domain admin privileges. These organizations should eliminate usage of accounts with domain admin privileges except for very specific and extreme situations, such as rebuilding, reconfiguring or patching Active Directory domain controllers. Instead, administrators should elevate privileges from their regular user accounts.

- PEDM for Unix/Linux is good start for organizations that are already using individual named accounts for users on Unix or Linux systems, and require these users to execute limited privileged operations on these systems. Organizations that also want to extend Active Directory over Unix and Linux systems to allow certain users to log into Unix and Linux systems using their AD accounts should focus on PEDM for Unix/Linux with Active Directory bridging functionality.

Some vendors sell PASM tools as different modules (vaulting plus password management, PSM, and AAPM); others sell "mini-suites" or combined PASM products. When deploying PASM tools, vaulting plus password management and PSM can easily be deployed at the same time, whereas deployment of AAPM requires additional focus that can cause distractions when attempted at the same time.

When selecting tools from vendors, organizations should keep in mind that:

- Small and midsize organizations should closely look at solutions that have **built-in high availability features** as alternatives to solutions that require the use of an external RDBMS system that needs to be configured for replication and high availability.

- High-trust authentication, such as **two-factor authentication** (2FA), should always be used in conjunction with PAM tools. Most vendors provide native support for integration with Active Directory and Lightweight Directory Access Protocol (LDAP)-compliant directories, as well as authentication systems such as RADIUS. Some vendors ship embedded 2FA solutions, which is attractive for small and midsize companies that do not have a 2FA solution in place. Organizations that already have a third-party user authentication solution in place should ensure that shortlisted PAM vendors provide the required integration support — for example, some vendors integrate with offerings from Duo Security and SecureAuth to support a wider range of authentication methods.

- **A2A credential brokering:** Some operating systems (specifically Windows) offer a mechanism to safeguard service account credentials, and organizations can use PASM to rotate and update those credentials in situ. Having applications retrieve credentials from the vault through a network-protocol-based API requires authentication to the vault, which requires the use of a HSM or other secure credential storage mechanisms. When this is not practical, AAPM tools should be strongly considered.

- **Discovery** of privileged accounts and their use continues to be a major challenge for organizations. Clients should expect this to take a considerable effort and realize that it may not necessarily provide adequate results or value.[20]

- **Shop around:** Pricing and feature bundling is highly variable between vendors, and is exacerbated by the fact that some vendors even apply distinct licensing mechanisms for their individual tools or modules. Plan for the next three years in terms of systems and functionality covered, and get a pricing commitment not only for the initial phase, but also for subsequent phases. Gartner clients should use inquiry privileges for pricing reviews.

Appendix

Vendor Revenue

Among medium and large PAM vendors that provided revenue information, revenue growth through 2015 was in the range of 8% to 56%, with an average growth rate of 33% per vendor (see Table 4).

Avecto, Microsoft, Red Hat and Venafi are not counted toward the total PAM revenue because the majority of revenue is generated for use cases that are not strictly considered to be PAM (in the case of Avecto and Venafi), or because the solution is available for free, or part of another solution outside of PAM (in the case of Microsoft and Red Hat).

Evidence

This research has been informed by vendor surveys, inquiries with Gartner clients and secondary research.

[1]Some organizations are using PAM tools to put controls around access to shared social networking accounts used for marketing purposes, although this may not be as effective as tools specifically tailored for this use case such as Adobe Social, Bitium, Falcon.io, Hootsuite, Spredfast and Shoutlet. In addition to multilevel review and approval workflows for content publication, these tools also support social analytics, engagement and CRM integration (see "Market Guide for Social Marketing Management").

[2]Previously, Gartner defined four categories of PAM tools: shared account password management (SAPM), superuser privilege management (SUPM), privileged session management (PSM) and application-to-application password management (AAPM). In the new classification, PASM = SAPM + PSM + AAPM, whereas PEDM = SUPM.

[3]See "Bomgar Acquires Password Management Technology From Pitbull Software."

Table 4. Vendor Revenue by Market Share

Vendor Revenue 2015	Number of Vendors in the Category	2015 Total Revenue Share	2015 Total Revenue Size
Small: Less than $10 million	18	8%	$52.6 million
Medium: Between $10 and $30 million	11	26%	$179.5 million
Large: More than $30 million	5	66%	$457.7 million
Total	34	100%	$689.8 million

Source: Gartner (August 2016)

[4]See "Thoma Bravo Acquires Bomgar, Strengthens Security Software Portfolio."

[5]See "CA Technologies Completes Acquisition of Xceedium, Inc."

[6]See "London Stock Exchange Welcomes Osirium Technologies to AIM."

[7]See "Euronext: Wallix."

[8]See "CyberArk Completes Acquisition of Viewfinity, Inc."

[9]See "Thycotic Receives Significant Investment from Insight Venture Partners to Meet Growing Demand for Privileged Account Management Solutions."

[10]See "Thycotic Completes Acquisition of Arellia."

[11]While many potential buyers from North America are mentioning the desire to achieve compliance with frameworks such as PCI-DSS, NIST 800-53, ISO 2700x, HIPAA or SOX, compliance is not always the primary driver for PAM technology purchases. Gartner has advised many PAM buyers in 2015 whose primary drivers were good practices around security effectiveness and operational efficiency.

[12]Potential buyers from Europe that have spoken to Gartner indicated good security practices, rather than regulatory compliance, as the main driver for their purchases.

[13]Mostly driven by compliance with regulation such as technology and risk management guidelines from the Monetary Authority of Singapore.

[14]Such as Qatar's National ICS Security Standard and regulation from the UAE's National Electronic Security Authority (NESA).

[15]Although PAM tools are typically simple to install, using them pervasively requires a change to an organization's processes and culture, and therefore require buy-in from all parties that require privileged access. That can be a lengthy exercise for one tool alone. Yet a significant minority of proposals from PAM vendors reviewed by Gartner includes both types of tools for simultaneous purchase. As a consequence, Gartner has learned from organizations that struggle to fully deploy all tools — leading to "shelfware," where only some tools are deployed, and other tools incur annual support and maintenance costs while "waiting in the wings."

[16]This is recommended when passwords are revealed to an administrator. If the passwords are not changed (automatically) after use, the password is no longer controlled; it could be revealed to another party and thus undermine policy. On the other hand, when single sign-on is used to establish sessions for administrators, the password is not revealed. In this case, passwords do not need to be changed after every use. In fact, changing passwords that have not been revealed after every use can be counterproductive, as it increases the load on the PAM solutions, and Gartner hears from customers that this can be a problem for less scalable PAM solutions.

[17]For example, administrators must avoid executing any commands that could serve as a vector for malware, such as running browsers or email clients within sessions with administrative privileges, or executing unknown code.

[18]See "Microsoft Security Intelligence Report."

[19]See "Best Practices for Privileged User PIV Authentication."

[20]Some vendors differentiate themselves by offering features to scan for — and discover — accounts in a programmatic way. This can greatly reduce the time and effort. But remember that this is an inexact science, and many privileged accounts will likely fall through the cracks of autodiscovery and will need to be discovered through other mechanisms (see "How to Manage Authentication and Credentials for Software Accounts").

Gartner Research Note G00279025, Felix Gaehtgens, Anmol Singh, 2 August 2016

Contact Us

WASHINGTON DC HQ

1101 17th Street NW, Suite 1102
Washington DC 20036
United States
+1-202-802-9399 (phone)
+1-202-315-3315 (fax)

UNITED KINGDOM

69 Old Broad Street
London EC2M 1QS
United Kingdom
+44-1777-712603

AUSTRALIA

83 King William Road
Unley 5061
South Australia
+61-28015-2090