beyondtrust
Beyond Traditional Security

PAM Solutions Center
Privileged Account Management Research & Solutions

Market Guide for Privileged Access Management

Establishing controls around privileged access continues to be a focus of attention for organizations and auditors. IAM and security leaders must be prepared to secure, manage and monitor privileged accounts and access. A thriving market provides many options for tools to help with these tasks.

Key Findings

- Prevention of both breaches and insider attacks has become a major driver for the adoption of privileged access management (PAM) solutions, in addition to compliance and operational efficiency.
- The PAM market continues to see strong growth across the board, with new players entering the market.
- Total cost of ownership for PAM products is highly variable and depends on many factors that are not obvious from initial proposals by vendors.
- Adoption of PAM products by organizations is often partial, leaving gaps that translate to risk.
- Product differentiators include Active Directory (AD) to Unix/Linux bridging, built-in high availability, multitenancy, privileged usage and threat analytics, SSH key management, and OCR session transcription.

Recommendations

IAM and security leaders:

- Do not overlook nonhuman service and application accounts – major sources of operational and security risk.
- Ensure a sustainable and fail-safe solution, and scrutinize vendors' high-availability and disaster recovery features, as well as dependencies on external components such as RDBMS.
- Mind the gaps: a partial implementation of PAM tools will leave vulnerabilities and, thus, still leave you exposed. Engage administrative users early. Sell them on the idea that they will have more control over the systems.
- Compare mixed offerings from multiple vendors against comprehensive suites. Adding third-party capabilities such as privileged session management (PSM) can sometimes offer a more suitable solution at a lower price than a suite offering.

Strategic Planning Assumption

By 2017, more stringent regulations around control of privileged access will lead to a rise of 40% in fines and penalties imposed by regulatory bodies on organizations with deficient PAM controls that have been breached.

By 2018, 50% of organizations will use authentication methods other than passwords for administrative access, up from 20% in 2015.

Market Definition

PAM technologies help organizations protect critical assets and meet compliance requirements by securing, managing and monitoring privileged accounts and access. Gartner has renamed PAM, starting with this research, from privileged account management to privileged access management.

PAM tools offer one or more of these features that allow users to:

- Control access to shared accounts (including emergency access using firecall accounts) by either disclosing credentials in the form of passwords, keys and other secrets in a controlled manner or, alternatively, by providing single sign-on (SSO) – without revealing the actual credentials
- Control and filter commands or actions an administrator can execute
- Provide accountability by monitoring and recording privileged access, commands and actions
- Automatically randomize and manage passwords and keys for administrative, service and application accounts, and store them in a secure vault
- Manage SSH keys for accessing systems and applications
- Maintain a comprehensive view of privileged accounts, as well as a view of what users are doing in the IT environment, through dashboards, reporting and analytics
- Integrate with existing IT service and support management (ITSSM) systems and change management workflows for tighter control of administrative access

The tools apply to privileged access spanning a wide range of systems and infrastructure – from operating systems, databases, middleware and applications to network devices, hypervisors and SaaS applications. Although the major focus is on managing privileged access, PAM tools are also used by some organizations to manage shared access to nonadministrative shared accounts.[1] Accounts used by nonhuman users, such as services or applications – whether of an administrative nature or not – are also usually in scope.

Product Categories

Vendors of PAM solutions have offerings in at least one of these categories:

- **Shared account password management (SAPM)**: Manage passwords and control access to shared accounts.
- **Privileged session management (PSM)**: Establish privileged sessions with SSO to multiple systems, and/or monitor and record activity.
- **Superuser privilege management (SUPM)**: Allow fine-grained filtering of commands and actions for administrators.
- **Application-to-application password management (AAPM)**: Eliminate hard-coded passwords used by applications.

Market Direction

Gartner estimates that the size of the PAM market reached $512 Million in 2014. The model for calculating the market size has changed slightly, and some adjustments to 2013 vendor revenue have been made (see Appendix – Vendor Revenue). The market for PAM has continued to grow, with the growth rate for 2014 estimated to have been 32%. We saw extensive activity in this market in 2014. BalaBit, Bomgar, Centrify and Wallix successfully raised capital during that year. In September 2014, BeyondTrust was acquired by Veritas Capital, and CyberArk successfully completed an IPO.

Interest in PAM technology is driven by several factors:

- The risk of 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 an irrefutable trail of evidence for privileged access
- Access to privileged accounts by third parties: vendors, contractors and service providers

Several high-profile breaches and insider attacks have been known to exploit privileged accounts,[2] and this has increased the interest in tools to tighten controls on privileged activity, as well as interest in two-factor authentication for privileged access. While in 2013 the majority of inquiries about PAM tools from Gartner clients were driven by compliance concerns and operational efficiency, a large part is now driven by the desire to mitigate threats of breaches and insider attacks. Gartner expects this trend to continue at least until 2016.

Pricing and bundling remain highly variable within the market (see Appendix – PAM Pricing by Scenario). Gartner has had discussions with organizations that reported receiving surprisingly high-priced offers from vendors to extend the capabilities of a current deployment, which has ultimately led to vendor replacements. Several vendors now bundle multiple capabilities together in their entry-level offerings, and Gartner expects more vendors to follow suit over the next year. Organizations are advised to plan ahead for evolving requirements over the next three to five years, 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:

- **SSH key management for privileged session use between the PAM system and servers or between applications**: Discovery and management of individual (personal) keys for administrative users is another feature that is starting to emerge.
- **Hybrid and purely cloud-based PAM solutions**: For example, Lieberman Software offers its ERPM product in the Azure marketplace, and Thycotic offers Secret Server as a service. Other vendors also indicated that they will start to offer a cloud-based service in 2015.[3]
- **Cloud and hypervisor**: As organizations continue to take up virtualization and cloud infrastructure, PAM tools are expected to continue to build out features to discover and manage infrastructure:
  - Automated discovery and enrolment of hypervisor guests and infrastructure as a service (IaaS) instances
  - Fine-grained authorization of infrastructure management operations (who can create/modify/delete/start/stop individual instances)
- **Privileged usage and threat analytics**: Some vendors offer integrated vulnerability management and correlation or behavioral analytics to calculate risk scores for privileged accounts and users.
- **Multitenancy**: Several vendors have indicated a strong uptake for PAM tools by managed service providers and cloud infrastructure operators. These organizations require multitenancy features within PAM tools, and several vendors are differentiating themselves by catering to this demand.[4]
- **System and privileged account autodiscovery**: 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 account 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 AD) to run an as-is analysis of the current environment, and compare this to the last known state to find changes.
  - 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. An example of this would be Lieberman Software's ERPM.

- **Service account discovery**: Many vendors provide account discovery features5 that help organizations face challenges with the scattered and hidden nature of service and application credentials – especially the latter, which may be hard-coded in scripts and application code or stored in configuration files.
- **Privileged identity governance and administration**: Several vendors with IAM offerings, in addition to PAM products, are leveraging synergies between their identity governance and administration (IGA) and PAM products. Other stand-alone PAM vendors have integrated their products with some IGA products from other vendors.

Market Analysis

This is how Gartner defines PAM product categories:

SAPM

Solutions that fall into this category will provide an encrypted and hardened password safe or vault for storing credentials, keys and other secret information. Passwords of administrative, shared and service accounts are managed by changing them at configurable intervals (even, if desired, after every use6) 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.

SAPM tools control administrators' access to shared accounts, allowing authorized users to access. Ideally, these users should not see the actual passwords. Instead, SAPM tools are often tightly coupled with PSM functions or products that will automatically initiate SSO to sessions without disclosing credentials. This helps to comply with the imperative that passwords for shared accounts must not be shared, because this can lead to uncontrolled access (see "Ten Best Practices for Managing Privileged Accounts"). Where this is not possible or impractical, passwords can be disclosed to the user by placing them into the clipboard or copy buffer, or even 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 higher-trust authentication methods. An irrefutable audit trail is kept that documents all privileged account use.

In addition to granting access, SAPM 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 – 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 ITSSM systems out of the box and/or provide APIs to validate administrative access requests by cross-checking them with information from ITSSM systems. SAPM tools also support "break the glass" scenarios for emergency and disaster recovery purposes, including the support for firecall accounts.

SAPM tools, by themselves or in combination with AAPM 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.

PSM

Gartner defines PSM as implementing these features:

- Remote session establishment and control
- Session recording (for later analysis) and real-time monitoring (for dual control or "four eyes" principle)

In some cases, PAM products implement only one of these features. This happens, for example, in SUPM systems that do not control the sessions of regular users, but start recording the session as soon as privilege elevation happens (such as in the situation when a user attempts to execute a command with elevated privileges).

In other cases – especially in PSM modules integrated with SAPM tools – the automatic establishment of privileged sessions happens as part of the credential check-out process. A session is initiated using a well-known protocol (SSH, RDP, ICA, VNC, HTTPS, X11), and the user is automatically logged in. Typically, credential injection happens at this time, leading to the authorized administrator being logged in automatically without revealing the password. The majority of vendors of PSM modules use a gateway (or proxy) approach. 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.

Session recording and transcription is another important aspect of PSM. 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, real differentiators are found in session playback functionality. The most basic PSM systems will support only a 1:1 playback of the entire session. If an administrator pauses for 10 minutes, then the 10-minute pause will also be on the video. Some other PSM 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, many PSM tools can gather metadata events from the session protocol (such as applications executed, Windows opened, text types). For SSH, many PSM tools store input and output streams. A notable feature is full optical character recognition (OCR), scanning entire graphical sessions with extensive protocol support that is provided by several vendors.

Another important aspect of PSM is session monitoring and alerting in real time. This allows for 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 "dual control." A few vendors also provide capabilities to analyze privilege sessions in real time and generate alerts or notifications (via email, text messages or Simple Network Management Protocol [SNMP]) when a suspicious behavior is detected.

Gartner considers a full PSM solution to support complete session management, logging/monitoring supporting of at least Telnet, SSH and RDP protocols, as well as intelligent playback functionality. Partial functionality will support a subset, or will only monitor local sessions through the use of local agents.

SUPM

SUPM tools work by allowing certain commands to be run under elevated privileges, or by restricting commands that can be executed. A common example of a classical SUPM tool is the "sudo" command on many Unix and Linux systems, or the "runas" command for Microsoft Windows. These commands allow a user to run a command under the privilege level of another user (typically, an administrator or superuser). Several SUPM vendors work at the shell level by shipping replacements of a shell, or the sudo command on Unix and Linux systems that integrate with a centralized policy service. In those cases, SUPM tools can log privileged commands or shell sessions.

Other approaches to SUPM are to limit (filter) commands that can be run under elevated privileges in order to limit the scope of what administrators can do or to prevent administrators from carrying out unsafe activities.7 This can happen in order of granularity from coarse to fine:

- Protocol level (via a gateway or proxy)
- Shell level
- Kernel level

Kernel-level granularity allows control at a very fine level, but at a higher cost of administration and performance. On the other end, protocol-level filtering is easiest to implement and maintain, but does not offer the same reliability or granularity.

Context-sensitive command filtering allows SUPM tools to control access based on predefined contextual attributes such as network addresses and/or access client and program, and time and location of access.

Some vendors without a full SUPM offering are offering SUPM-like features such as enabling individual packaged tasks to be executed under privileged credentials in an automated manner by approved users. Examples of these would be selectable items such as "restart the application server" that administrators could launch from a portal without having to log into a particular system.

Gartner considers full SUPM functionality to be delivered by tools that can enforce filtering of commands on a shell level or kernel level. Tools that can filter commands based on session interception through a proxy or gateway have partial functionality.

AAPM

AAPM tools are usually delivered as add-on modules to SAPM tools, and are used to eliminate hard-coded passwords or keys stored in configuration files. Credentials are pulled from the vault using a proprietary interface provided by the PAM vendor. These interfaces are usually in the form of APIs, software developer kits (SDKs) and command line interfaces (CLIs), and require applications or scripts to be modified. The modification is usually simple; however, testing must happen for every application modified, which places a considerable burden on organizations.

AAPM provides functions to pull credentials from the vault; therefore, a trusted session must be established between the application or script and the vault. Differentiators exist in how this session trust is established. In its simplest form, this requires the application to authenticate to the vault with a certificate or another credential. This really does not solve the issue, but, instead, pushes the problem from one side to the other – substituting one stored credential (the original hard-coded or stored credential) with another one (the new credential required to authenticate to the vault). For purposes of differentiation, Gartner does not consider this mechanism to be full AAPM.

Full AAPM tools will *recognize* an application or script, rather than *authenticating* it, by taking multiple factors into account and, thereby, completely eliminating the stored credentials. Examples of these are the "fingerprints" of the application or script and its configuration files and/or the host on which it runs, the user ID that started it, the directory from which it runs, and a one-time password (OTP) value generated from a seed that changes after every invocation. AAPM software that eliminates hard-coded and unencrypted stored credentials altogether embraces the most secure form of delivering credentials to applications or scripts.

Gartner considers a full solution to offer APIs for applications to pull passwords from the vault and eliminate any need to store credentials or private keys, as well as eliminate the need for applications to authenticate to the vault by recognizing them instead. Partial functionality will offer APIs, but still require authentication (to the API) in the form of stored credentials or certificates.

Unified Products

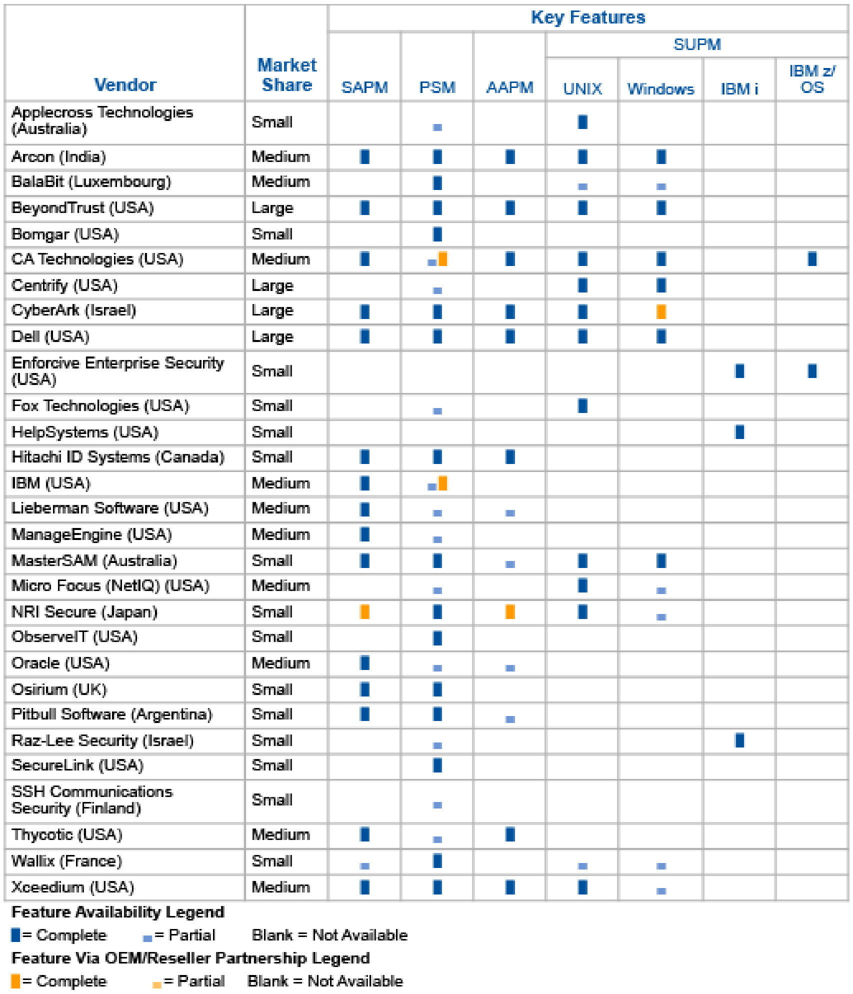
Several – mostly large – PAM vendors offer complete PAM suites, offering capabilities in all four product categories discussed. However, with new and innovative vendors making entry, the market is reshaping to be characterized by privately held small-to-midsize providers that focus on one main product category. Those vendors often deliver unified solutions that contain some capabilities from other adjacent product categories: A common case is SAPM vendors that have added PSM and/or AAPM capabilities. Potential buyers should carefully evaluate unified products with bundled capabilities, versus offers from vendors that license each capability separately, as there is a potential for cost saving.

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.

Figure 1 presents the representative vendors and their key capabilities. 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.

Figure 1. Representative Vendors and Their Key Capabilities



Vendor	Market Share	Key Features						
					SUPM			
		SAPM	PSM	AAPM	UNIX	Windows	IBM i	IBM z/ OS
Applecross Technologies (Australia)	Small		▪		■			
Arcon (India)	Medium	■	■	■	■	■		
BalaBit (Luxembourg)	Medium		■		▪	▪		
BeyondTrust (USA)	Large	■	■	■	■	■		
Bomgar (USA)	Small		■					
CA Technologies (USA)	Medium	■	▪🟧	■	■	■		■
Centrify (USA)	Large		▪		■	■		
CyberArk (Israel)	Large	■	■	■	■	🟧		
Dell (USA)	Large	■	■	■	■	■		
Enforcive Enterprise Security (USA)	Small						■	■
Fox Technologies (USA)	Small		▪		■			
HelpSystems (USA)	Small						■	
Hitachi ID Systems (Canada)	Small	■	■	■				
IBM (USA)	Medium	■	▪🟧					
Lieberman Software (USA)	Medium	■	▪	▪				
ManageEngine (USA)	Medium	■	▪					
MasterSAM (Australia)	Small	■	■	▪	■	■		
Micro Focus (NetIQ) (USA)	Medium		▪		■	▪		
NRI Secure (Japan)	Small	🟧	■	🟧	■	▪		
ObserveIT (USA)	Small		■					
Oracle (USA)	Medium	■	▪	▪				
Osirium (UK)	Small	■	■					
Pitbull Software (Argentina)	Small	■	■	▪				
Raz-Lee Security (Israel)	Small		▪				■	
SecureLink (USA)	Small		■					
SSH Communications Security (Finland)	Small		▪					
Thycotic (USA)	Medium	■	▪	■				
Wallix (France)	Small	▪	■		▪	▪		
Xceedium (USA)	Medium	■	■	■	■	▪		

Feature Availability Legend

■= Complete ▪= Partial Blank = Not Available

Feature Via OEM/Reseller Partnership Legend

🟧= Complete 🔸= Partial Blank = Not Available

Note: More marks does not signify a better product
Source: Gartner (May 2015)

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

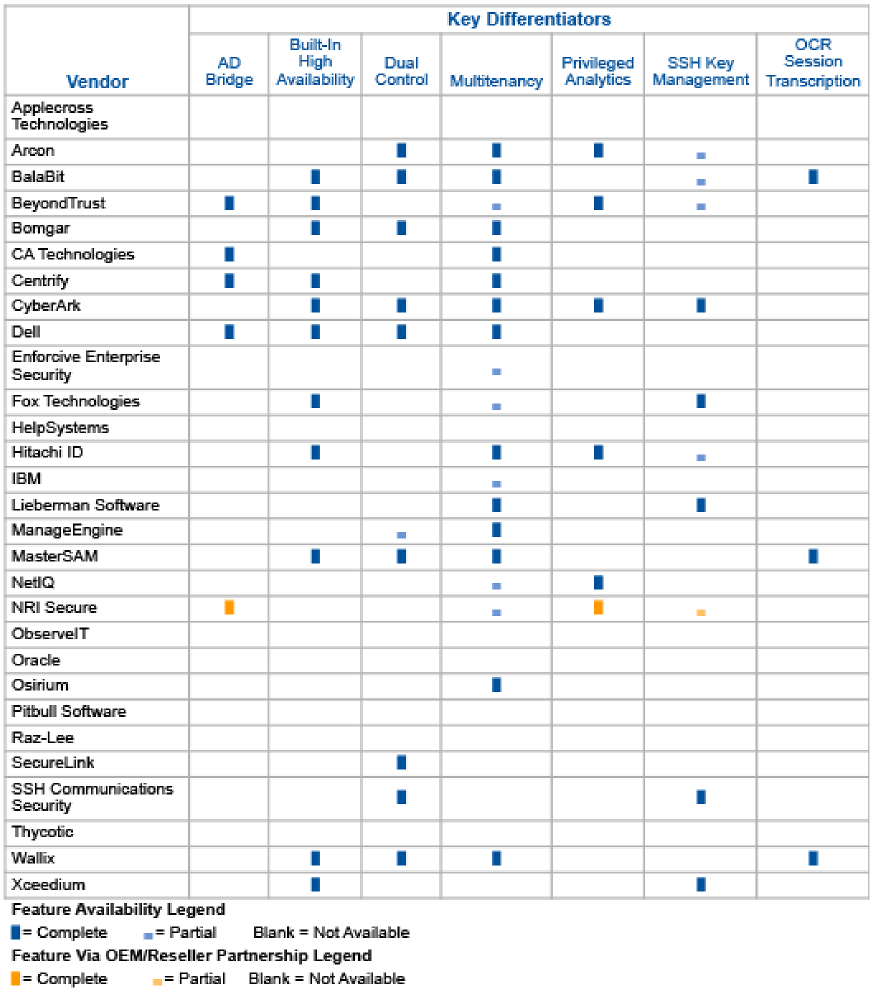
Key Differentiators

Key differentiators for PAM solutions are shown based on these definitions (see Figure 2):

- **AD bridge**: Allowing users to log into Unix using their AD accounts through an agent that extends users, groups and some GPOs from Microsoft AD to Unix and Linux. Some vendors will support smart-card login for consistency within the Windows environment.
- **Built-in high availability**: Integrated configuration features to allow a simple and rapid deployment of an active-active or active-passive, high-availability configuration without the need to configure a highly available RDBMS.
- **Dual control**: Mandate the participation of a second person for concurrent session access, and allow that second person to take over or terminate the session.

- **Multitenancy**: Specific features to allow use of the same PAM platform by multiple different parties in complete isolation, all managing a different set of credentials.
- **Privileged analytics**: Calculate risk scores for privileged accounts and users through behavioral analytics and/or correlation of privileged activity with vulnerability information.
- **SSH key management**: Partial features include the management of keys for accessing privileged accounts by the PAM system. Full features denote discovery and management of user keys on managed systems.
- **OCR session transcription**: Analysis of privileged sessions and generation of searchable textual metadata from graphical sessions that document what was done by an administrator during the session.

Figure 2. Representative Vendors and Their Key Differentiators



	Key Differentiators						
Vendor	AD Bridge	Built-In High Availability	Dual Control	Multitenancy	Privileged Analytics	SSH Key Management	OCR Session Transcription
Applecross Technologies							
Arcon			■	■	■	▪	
BalaBit		■	■	■		▪	■
BeyondTrust	■	■		▪	■	▪	
Bomgar		■	■	■			
CA Technologies	■			■			
Centrify	■	■		■			
CyberArk		■	■	■	■	■	
Dell	■	■	■	■			
Enforcive Enterprise Security				▪			
Fox Technologies		■		▪		■	
HelpSystems							
Hitachi ID		■		■	■	▪	
IBM				▪			
Lieberman Software				■		■	
ManageEngine			▪	■			
MasterSAM		■	■	■			■
NetIQ				▪	■		
NRI Secure	🟧			▪	🟧	🔸	
ObserveIT							
Oracle							
Osirium				■			
Pitbull Software							
Raz-Lee							
SecureLink			■				
SSH Communications Security			■			■	
Thycotic							
Wallix		■	■	■			■
Xceedium		■				■	

Feature Availability Legend

■ = Complete ▪ = Partial Blank = Not Available

Feature Via OEM/Reseller Partnership Legend

🟧 = Complete 🔸 = Partial Blank = Not Available

Note: More marks does not signify a better product.
Source: Gartner (May 2015)

Applecross Technologies (www.applecrosstech.com) offers its Privileged User Manager (PUM) on a subscription basis as software or virtual appliance. The solution provides privileged access to Unix/Linux and consists of Web UI, RESTful API and native modules. Administrative users can access shared accounts through supported SSH clients or via a Web interface with an embedded SSH client and the ability to control several accounts at once. A sudo replacement module is also available, providing centralized management and logging.

Arcon (www.arconnet.com) provides the Access and Root Control Solution (ARCOS). The solution is delivered as a set of different modules that are licensed separately and provided as software, appliance (physical or virtual) and as a service in a private cloud. The high-availability module is licensed separately. ARCOS is unique in that it can provide a very fine-grained control over database privileged activity through delivery of specialized client agents. Also, its multitenancy capabilities are deep, which should make the solution appeal to organizations with complex environments requiring a high degree of flexibility.

BalaBit (www.balabit.com) offers Shell Control Box delivered as a physical or virtual appliance. The product is primarily a PSM solution that supports an extensive list of network protocols and can act as a gateway or transparent proxy. It features protocol-based command and application filtering for privileged sessions and can work in conjunction with an external password vault (provided by other vendors) to provide SSO. BalaBit can also store passwords but does not manage them on other systems. Organizations that require deep PSM capabilities should evaluate BalaBit's offering, in addition to SAPM tools from other vendors, and even as an alternative to other vendors' separately priced PSM modules.

BeyondTrust (www.beyondtrust.com) provides a comprehensive range of PAM products under its PowerBroker label. The products are delivered as software or as an appliance (physical or virtual) and can be bundled in the BeyondInsight platform or licensed separately. BeyondTrust is one of very few vendors covered in this report that has a native product for kernel-based Windows SUPM. It also offers privileged analytics, included free as part of its BeyondInsight IT risk management platform. Organizations looking for a comprehensive and cost-effective solution will appreciate that BeyondTrust's SAPM and SUPM products include PSM and AAPM capabilities at no extra charge.

Bomgar (www.bomgar.com) offers a PSM solution called Bomgar Privileged Access Management as a physical or virtual appliance or as a service. The solution allows an organization to control access to privileged sessions according to policies. Organizations looking for a VPN-free solution that allows managing third-party access by vendors, integrated with session monitoring and recording, will appreciate Bomgar's strong collaboration capabilities, including support for session monitoring and control from remote tablets and smartphones.

CA Technologies (www.ca.com) offers a comprehensive solution of PAM products under the CA Privileged Identity Manager brand (previously ControlMinder) that are licensed separately. The solution includes SUPM for the hypervisor for virtual environments (CA Privileged Identity Manager for Virtual Environment, delivered as a virtual appliance) that is based on technology from HyTrust. CA Technologies is one of few vendors that can provide SUPM for Unix/Linux on a very fine-grained level through the use of kernel agents. It also offers a flexible deployment model through multiple tiers that can be individually load-balanced for high scalability. SAPM includes AAPM for no additional cost. Both CA ACF2 for z/OS (and z/VM) and CA Top Secret for z/OS (z/VM and z/VSE) offer full superuser privilege management through the use of standard system authorization facility (SAF) calls.

Centrify (www.centrify.com) offers its Centrify Server Suite as software that provides SUPM for Unix/Linux and Windows in the form of command control. Command control is possible in two modes: always-on (restricted shell for Unix/Linux and privileged Windows desktop), and on-demand (elevating privileges by invoking a special tool). Centrify's solution uses a native agent for Unix/Linux to extend AD users and groups to those systems; for systems that cannot be fitted with a native agent, a special network information service (NIS) or LDAP proxy service can be made available. Organizations looking for an AD bridge with command control functionality will appreciate Centrify's capabilities in this area. Centrify has an extensive global network of reseller partnerships.

CyberArk (www.cyberark.com) offers a comprehensive range of PAM products that are licensed separately and delivered as software or appliance (physical or virtual). SUPM for Windows is provided as technology licensed through an OEM agreement with Avecto. CyberArk also offers a subscription model for managed service providers, and multitenancy features permit the vault to contain separate "safes" that can be individually assigned without a common administrator. CyberArk has a global footprint and a strong market presence in North America and EMEA.

Dell (www.dell.com) provides a comprehensive PAM solution, delivered as a physical appliance (SAPM, PSM, AAPM) and software for all other components. SUPM for Unix/Linux is sold in two editions: Dell Privilege Manager for Unix includes remote host command execution and restricted privileged shells. Dell Privilege Manager for Sudo extends the Unix/Linux sudo command with centralized keystroke logging and policy management and is more moderately priced but does not include those two features. AAPM is included within the license for SAPM.

Enforcive Enterprise Security (www.enforcive.com) provides several software products to manage security on IBM i and IBM z. Several of these tools fall into the category of PAM. Application Access Control is part of the Enforcive Enterprise Security (ES) for IBM i product suite and selectively restricts privileged users' remote command execution based on policy and elevates sessions by swapping to privileged accounts. Elevated sessions are monitored for command execution and file access, and privileged activity can be correlated and analyzed. Other modules within the suite provide functionality for distributing administration functions through role-based configuration of different functions for different administrators. Enforcive/Security for CICS has functionality for monitoring security officer activity and for distributing administration functions by defining different functions and control for different administrators.

Fox Technologies (www.foxt.com) provides BoKS Server Control for Unix and Linux, delivered as software. The solution takes a different approach from most others covered in this report. It uses a management server (BoKS Master), in combination with a set of local agents on Unix and Linux servers, to manage security configurations across all systems. Included are a modified version of OpenSSH, a centralized sudo replacement, SSH key distribution and a password vaulting feature. Integration with LDAP, AD and other directories (via a Web-services interface) is also featured. The combined system provides central and contextual control of all access and privilege escalation, and general access control for user sessions by enforcing access rules. The solution should appeal to organizations that require a comprehensive, centrally managed security solution for Unix and Linux systems that includes user management.

HelpSystems (www.helpsystems.com) provides security products for IBM i through multiple brands. Several of these tools fall into the category of PAM. Safestone Powerful User Passport and PowerTech Authority Broker allow temporary elevation to a higher level of authority by swapping and providing a full audit log of activities. Safestone Multiple System Administrator (MSA) establishes a centralized administration of multiple servers and partitions through a single point of control. PowerTech Authority Broker can record all screens for swapped users and allow administrators to monitor activity, as well as send real-time alerts when swapping occurs.

Hitachi ID Systems (www.hitachi-id.com) offers a unified PAM solution called Hitachi ID Privileged Access Manager. The solution is offered as software or as a virtual appliance. SUPM features are not offered; however, the solution can temporarily add a user ID to a security group for the duration of a session. Potential customers will appreciate the fact that all of the solution's capabilities, including active-active clustering for high availability are included in the product. These three factors provide the potential to significantly lower the total cost of ownership.

IBM (www.ibm.com) provides the IBM Security Privileged Identity Manager (ISPIM) as a virtual appliance. PSM is provided through two options. A basic PSM module works by providing regular screen shots of graphical sessions and input/output logging for textual sessions. Both its AAPM and PSM solutions are sold as add-on products to the base ISPIM server. Additionally, agent-based PSM technology from ObserveIT is available as an additional option. IBM's SAPM shares technology with several other IBM security products (including IBM Security Identity Manager) and, thus, comes with a rich set of application connectors. Organizations that already leverage other products within IBM's security portfolio can profit from synergies between those products and IBM's PAM solution.

Lieberman Software (www.liebsoft.com) offers Enterprise Random Password Manager (ERPM), available as software, or in the cloud through the Azure Marketplace. Some PSM features are available through a separately licensed launch server app that utilizes Windows Terminal Server and records sessions. ERPM is highly scalable through its multitier architecture, which can use zone processors to change passwords on a massively parallel fashion. It is also one of few vendors that supports concurrent (not just ad hoc) discovery of privileged accounts and systems, including from hypervisors. This makes the solution particularly attractive to very large organizations. Smaller organizations will appreciate the fact that ERPM's AAPM features are included at no additional cost.

ManageEngine (www.manageengine.com) offers Password Manager Pro (PMP) as a unified PAM solution in three editions. PMP is available as software, either for purchase or as a subscription-based model. Sessions are initiated with an HTML5-compatible browser, and can be recorded and shadowed. Managed service providers that need a PAM solution for multiple customers will appreciate the fact that a special MSP edition is available with multitenancy features. Also, due to its low price relative to other offers, PMP is of particular interest to organizations without complex requirements looking for a rightsized PAM solution available at one of the most affordable pricing options in the market.

MasterSAM (www.mastersam.com) offers a PAM solution through multiple products that are licensed separately. The solution has multiple overlapping components that allow PSM and SUPM capabilities to be delivered as a gateway/proxy or, alternatively, as a host-based solution. MasterSAM's SUPM capabilities are offered at the most affordable pricing option in the market. The solution should appeal to organizations based in the Asia/Pacific region that want full flexibility in terms of deployment options or a hybrid between host-based and gateway/proxy.

Micro Focus (NetIQ) (www.netiq.com) offers the NetIQ Privileged User Manager (PUM) that is available as software or as a service. The solution provides a framework manager to manage agents on Unix/Linux. Users will then log into the framework manager to execute commands on target systems. Access to other (non-Unix/Linux systems) can be provided through a gateway that uses RDP relaying or SSH key management to provide remote access, and can filter commands. Video and keystroke recording for session is supported. Existing NetIQ customers can take advantage of synergies provided between PUM and other NetIQ products such as NetIQ Identity Manager for password management (but no vaulting) and NetIQ Sentinel for log analysis.

NRI Secure Technologies (www.nri-secure.com) provides SecureCube Access Check as software. Its clients often integrate SecureCube Access Check to extend PowerBroker Password Safe from BeyondTrust or iDoperation IM for Access Check by NTT Software Corporation (only available in Japan). The solution acts as a gateway/proxy-based system that can filter commands in multiple protocols, and alerts can be generated upon detection of specific activity. Sessions can be logged and audited. Policies and workflow capabilities are available for session management and for ensuring auditing through sign-off on specific sessions. The product is especially interesting for companies that require a wider range of supported protocols: In addition to common interactive session protocols such as SSH and RDP, SecureCube Access Check can also monitor and log file transfers via SFTP and FTP and CIFS protocol, as well as database sessions, to Oracle RDBMS systems using the TNS protocol.

ObserveIT (www.observeit.com) offers a software PSM solution that works as an agent for Windows and Unix/Linux (a gateway-based mode is also available, but less common). The solution provides detailed, fully searchable recording of all user activity. Logging can be configured on a granular basis, up to the level of individual system calls. ObserveIT will appeal to organizations that are interested in session recording capabilities that go beyond those found in mainstream PAM products.

Oracle (www.oracle.com) offers Oracle Privileged Account Manager (OPAM). The solution is delivered as software and has SAPM, PSM and partial AAPM capabilities. It shares technology with Oracle Identity Governance Suite (OIG) and thus comes with a rich set of application connectors. PSM capabilities are provided by the OPAM Session Manager (OPM) that acts as a proxy for the SSH protocol and supports input/out recording. OPAM will appeal especially to existing Oracle customers that can add OPAM to an existing IGS deployment to take advantages of synergies such as integrated privileged account governance and a familiar connector and administration framework.

Osirium (www.osirium.com) provides Osirium Enterprise, with SAPM and PSM capabilities. The solution is delivered as a virtual appliance that acts as a proxy, and a desktop client that must be installed on every administrator workstation. The PSM module works by providing regular screen shots of graphical sessions, as well as input/output logging for textual sessions. Session shadowing is also supported. The solution also has multitenancy features. It is sold mostly through subscription.

Pitbull Software (www.pitbullsoftware.net) offers its Pitbull KeyHolder product as software and virtual appliance and as a service. Session recording supports input/output for SSH and video recording for RDP and SQL Server Management Studio, although there are no advanced/rapid playback functions for videos. High availability is built into the product, supporting both active-active, as well as active-passive mode; however, a Microsoft SQL Server RDBMS must be provided in a replicated environment for a highly available solution. Pitbull KeyHolder is one of the most affordable products covered in this report and, therefore, very attractive for organizations without complex requirements looking for a rightsized PAM solution that is simple to deploy.

Raz-Lee Security (www.raz-lee.com) provides the iSecurity software suite, a security, auditing and compliance solution of 20 tools for IBM i. Several of these tools fall into the category of PAM. The audit tool reports the security status and activity based on the system journal (QAUDJRN). The Action tool can trigger automated alerts. Authority on Demand is used to provide firecall access. The Command tool controls the validity of system and user CL commands and parameters.

SecureLink (www.securelink.com) provides a specialized, 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. When an end-user organization using SecureLink for Enterprises links up with a vendor that already uses SecureLink for Vendors, the vendor's users are available immediately and can be granted access.

SSH Communications Security (www.ssh.com) offers a PAM solution with PSM capabilities that takes a different approach from most others covered in this report. The solution is based on two products. Universal SSH Key Manager is delivered as software and provides a centralized management platform for SSH keys and access. It provides automated life cycle management, including discovery, creation, removal and rotation of SSH keys on each endpoint. CryptoAuditor is a physical or virtual hardware appliance that can intercept and decrypt SSH sessions using managed keys. The sessions can then be recorded, and filtering can occur on a subprotocol level (that is, disabling tunneling capabilities within sessions or preventing specific file transfers).

Thycotic (www.thycotic.com) offers its Secret Server product in several editions as software or as a service. PSM and AAPM capabilities are available in the Enterprise Plus edition. Access to shared accounts for SAPM can be configured through templates. Ad hoc discovery is available in several editions. The solution will appeal to small and medium enterprises that are looking for a rightsized affordable solution that is easy to deploy and manage.

Wallix (www.wallix.com) provides Wallix AdminBastion (WAB) as a physical or virtual appliance using a proxy/gateway approach. An extensive list of network protocols is supported. The solution can manage administrator credentials on other systems, but not for service accounts. It can also integrate with the vault from other vendors' SAPM tools in order to fetch credentials from the vault and provide SSO to privileged sessions. Dual control and network-based command filtering are supported. Organizations that require deep PSM capabilities should evaluate Wallix's offering, especially as an alternative to other vendors' separately priced PSM modules.

Xceedium (www.xceedium.com) offers its Xsuite solution as a physical and virtual appliance. Its SUPM capabilities utilize protocol-based command filtering. Apart from SSH sessions, Xsuite also supports socket filters that can filter sessions on target systems and require an agent on those systems. A notable feature of Xsuite is its additional ability to create ephemeral (temporary) accounts on the fly for dynamic systems such as virtualization and cloud management consoles. These accounts can be created with a specific calculated set of permissions and allow granular and flexible management of privileges for a particular session. All features except for AAPM are included in the same product and do not need to be licensed separately.

Market Recommendations

PAM tools cover a wide spectrum of capabilities and will help address significant gaps around the control of privileged account usage. Based on interactions with users of PAM technology and vendors, Gartner made the following observations:

- SAPM and gateway-based PSM tools are the easiest to deploy, and 82% of customer references indicated that they deployed those tools without the help of an integrator.
- Installation of SAPM tools can typically be achieved in weeks, or sometimes even days. However, be aware that getting systems covered by those tools can be a challenge:
  - Organizational silos, lack of communication and political issues cause ownerships issues to get in the way of bringing particular systems under SAPM coverage and, therefore, cause gaps. Several organizations have indicated that IT operations and the networking group are often separate and struggle to agree to use a common system. The networking group does tend to come around once the group sees the benefits of the solution, but this takes time. Executive sponsorship and early stakeholder engagement help.
  - Discovery of privileged accounts and their use continues to be a major challenge for organizations, and is expected to take a considerable effort.[8]
- Host-based PSM tools offer more detailed information, but require agents to be installed on systems, increasing deployment time and maintenance cost.
- Host-based SUPM tools offer the most fine-grained command-filtering capabilities, but are also most complex to deploy and manage.[9]

Gartner advises potential customers to shop around, because pricing for PAM solutions varies widely (see Appendix – PAM Pricing by Scenario). Specifically, organizations considering an investment into PAM technology should:

- Plan for the next three years in terms of systems and functionality covered, and get a pricing commitment not just for the initial phase, but for subsequent phases as well. Some Gartner customers have indicated unexpectedly expensive proposals when extending an initially purchased license.
- Include estimates for access by third parties such as vendors or outsourcing. This can make a significant difference in terms of licensing.
- Keep in mind that several vendors offer functionality in one package or bundle capabilities together, while other vendors charge separately for every capability.
- Understand that several vendors require the use of an externally managed RDBMS system that needs to be deployed to cater to replication and high availability. This can add to the overall cost of the solution.

While PAM suites are available that cover a broad range of capabilities, point solutions exist and can, in some cases, supplement existing gaps, or be used in combination for those that favor a best-of-breed approach. Evaluate multiple vendors for capabilities and pricing because of the large range in pricing between vendors. Gartner clients are encouraged to make use of inquiries for guidance on pricing and capabilities.

Additional analysis provided by Mark Diodati and Neil Wynne.

Appendix

Vendor Revenue

Among the PAM vendors that provided revenue information (representing around 80% of the total estimated market size), revenue growth per vendor through 2014 was in the range of 7.7% to 211%, with an average growth rate of 43% per vendor.

License revenue in 2014 grew at a rate of 35%, compared to subscription revenue growth of 102% (although the latter started from a small base). Vendors that volunteered revenue information reportedly closed a total of 30,000 deals related to PAM products and services (including renewals and expansions) during 2014. Average contract value per vendor for PAM-related deals varies widely across the included vendors, from a low of $15,000 to a high of $300,000 in 2014.

We classified the market players into three broad categories based on their annual revenue (see Table 1).

Table 1. PAM Vendor Revenue by Market Share

2014 Total Revenue/Vendor	**2014 Revenue by Market Share**	**Revenue Share, 2014**
Small: Less than $10 Million	$56 Million	11.0%
Medium: $10 Million to $30 Million	$171 Million	33.4%
Large: More than $30 Million	$285 Million	55.6%
Total	**$512 Million**	**100%**

Source: Gartner (May 2015)

PAM Pricing by Scenario

PAM vendors offer vastly diverse pricing models, based on varying metrics – from number of privileged users, managed target systems and accounts, number of simultaneous sessions to delivery options (physical or virtual appliance, SaaS), as well as deployment types (host- or gateway-based). Some vendors bundle functionality together; others sell different modules separately. Several vendors also offer different metrics for features like SAPM, SUPM, AAPM, PSM or AD bridging – sometimes one module is based on a per-privileged-user basis, and another is based on a per-managed-target-system basis. Some vendors charge extra for high-availability and load-balancing capabilities.

Pricing models for PAM tools largely include perpetual licenses for on-premises deployments in the form of software and physical or virtual appliances, with a few vendors now offering subscription-based pricing models for private-hosted or SaaS-based solutions. We expect a shift from perpetual licensing to subscription and usage-based licensing models for PAM products as adoption of virtualization, SaaS and cloud-based infrastructure grows across the industry verticals.

SAPM pricing typically consists of a base server or appliance license price, combined with the number of systems to be managed, or the number of human administrators (not physical accounts) that will use the systems. Per-system licensing price may differ based on the type of system (such as firewall, router, Windows or Unix) and the number of systems. Some vendors offer password vault as an add-on module and charge for it separately, but most offer it as part of the base license.

AAPM is usually priced based on the number of application ID instances or nodes connecting to the password vault. For some vendors, AAPM is included in the SAPM pricing. Similarly, while PSM is typically charged based on the number of user endpoints or concurrent sessions allowed to connect to target systems, some vendors are including it as part of a SAPM or SUPM license.

We asked vendors to provide information on their pricing models for the various PAM features offered across SAPM, AAPM, SUPM and PSM segments. Here, we provide guidance on relative pricing expectations derived from the information gathered on three deployment scenarios. The average prices indicated in Table 2 for the three deployment scenarios are perpetual license prices and include support and maintenance charges for the first year.

Table 2. Estimated Pricing Based on Deployment Sizes

	Average Price			
Deployment Sizes	**SAPM**	**AAPM**	**SUPM**	**PSM**
100 Systems **25 Administrators** **500 Admin/Service Accounts** **1 Data Center With High Availability**	32,400	38,350	102,400	41,200
1,000 Systems **100 Administrators** **5,000 Admin/Service Accounts** **2 Data Centers With High Availability**	119,400	141,200	490,000	190,000
10,000 Systems				

350 administrators 50,000 Admin/Service Accounts 4 Data Centers With High Availability	2,041,500	648,900	4,417,000	885,500

Source: Gartner (May 2015)

Among all the deployment scenarios we studied, SUPM implementations, on average, are 200% more expensive than SAPM deployments for the same sample deployment size. For small-scale deployments, SAPM, AAPM and PSM are priced in a close range ($32,000 to $42,000); however, for large-scale deployments, SAPM on average costs nearly three times more than AAPM's or PSM's relative license costs.

Evidence

This report 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 Social, 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] The full list is too extensive to list here, but during inquiries, customers have specifically mentioned the Snowden affair (abuse of privileged accounts), and breaches at eBay, Target, Home Depot and Sony. These breaches involved the abuse, compromise and exploitation of privileged accounts.

[3] Centrify announced its Centrify Privileged Service (CPS), a SAPM solution delivered as a service, on April 22 (after research for this Market Guide was already concluded).

[4] Last year, we expected most vendors without those features to catch up by the end of 2015. Since then, it seems that we may have been too optimistic in our expectation; however, we have seen BeyondTrust and IBM add partial multitenancy capabilities and Wallix add full multitenancy.

[5] Account discovery works by periodically scanning systems and applications for newly provisioned/created accounts. Most vendors' offerings primarily focus on Windows systems because they are easier to scan due to common approaches for service account use on these systems. On Unix/Linux systems, some vendors offer features that scan all files in order to find patterns that look like credentials stored in configuration files. However, these features are not 100% reliable and cannot discover every account. Other measures are needed to identify accounts that may not be caught by discovery features (see "How to Manage Authentication and Credentials for Software Accounts").

[6] 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 PSM tools are used to automatically sign administrators on to shared accounts, 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 SAPM system, and Gartner hears from customers that this can be a problem for less scalable PAM solutions.

[7] 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.

[8] 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").

[9] SUPM can be used in a preventative or detective mode. In preventative mode, command control is used to limit administrator actions. While this looks promising, it is very difficult to carry out in practice to its fullest extent. It requires a delicate balance of allowing an administrator to have just the right set of commands to carry out the required work, versus not foreseeing or disallowing commands that may still be needed less frequently. Analytics tools to help create and maintain SUPM policies, blacklists and whitelists are lacking. Given the cost of SUPM tools, organizations should weigh the possibility of deferring an investment into command control tools unless they have a clear idea on how to create and maintain SUPM policies.

Source: Gartner Research G00271722, Felix Gaehtgens, Anmol Singh, 27 May 2015

Return to Home