Privileged Access Management Secures Your Organization's Weakest Link

Privileges gone wild. Passwords running loose. Employees just being "curious." These are just a few ways the human element can jeopardize information security. As several recent breaches have shown, critical data and assets can be compromised with no sophisticated hacking required. What's more, the risk often comes at the hands of the employees, contractors and partners who already have an in to your organization. Today, it's essential to rein in elevated privileges from those who don't need them, while ensuring accountability among those who do.

Fortunately, I have the privilege to share Gartner’s latest "Market Guide for Privileged Access Management" and invite you to learn more about BeyondTrust’s PowerBroker Privileged Access Management solution.

Kevin Hickey, President and Chief Executive Officer, BeyondTrust

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.

BeyondTrust Privileged Access Management Solutions and Trials

BeyondTrust offers an integrated product suite that addresses each of the five solution categories detailed in the Gartner "Market Guide for Privileged Access Management." Our PowerBroker® privileged access management solutions help organizations close the gap between IT security requirements and user enablement. By providing security and IT operations teams with a comprehensive privileged account management solution, deep analytical insights for better decision making, and extensibility across the security landscape, BeyondTrust reduces IT security risks, simplifies compliance and helps maintain user productivity.

» Download a PDF overview of the PowerBroker Privileged Access Management solution

» Request free trials of PowerBroker Privileged Access Management solutions

Shared Account Password Management (SAPM), Application-to-Application Password Management (AAPM), and Privileged Session Management (PSM)

BeyondTrust PowerBroker Password Safe automates privileged password and privileged session management, providing secure access control, auditing, alerting and recording for any privileged account – from local or domain shared administrator, to a user's personal admin account (in the case of dual accounts), to service, operating system, network device, database (A2DB) and application (A2A) accounts – even SSH keys.

Unix & Linux Super-User Privilege Management (SUPM) and Session Monitoring

BeyondTrust PowerBroker for Unix & Linux enables IT organizations to efficiently delegate Unix and Linux privileges and authorization without disclosing passwords for root or other accounts. Record all privileged sessions for audits, including keystroke information. Achieve privileged access control requirements without relying on native tools or sudo.

Windows Super-User Privilege Management (SUPM) and Session Monitoring

BeyondTrust PowerBroker for Windows reduces the risk of privilege misuse on physical and virtual Microsoft Windows servers and desktops. By eliminating Windows administrator privileges, simplifying the enforcement of least-privilege policies, maintaining application access control, and logging
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 access 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 privileged activities, IT closes security gaps, improves operational efficiency and achieves compliance objectives faster.

Active Directory (AD) Bridging
BeyondTrust PowerBroker Identity Services centralizes authentication for Unix, Linux and Mac environments by extending Microsoft Active Directory's Kerberos authentication and single sign-on capabilities to these platforms. By extending Group Policy to these non-Windows platforms PowerBroker provides centralized configuration management, reducing the risk and complexity of managing a heterogeneous environment.

Auditing and Protection
BeyondTrust PowerBroker Management Suite provides centralized real-time change auditing for Active Directory, File Servers, Exchange, SQL and NetApp, the ability to restore Active Directory objects or attributes, and helps to establish and enforce entitlements across the Windows infrastructure. Through simpler administration, IT organizations can mitigate the risks of unwanted changes and better understand user activity to meet compliance requirements.

For more information, please email info@beyondtrust.com or call +1 800-234-9072.