KuppingerCole Report

EXECUTIVE VIEW

by Anmol Singh | April 2019

BeyondTrust Password Safe

BeyondTrust's portfolio of products provides a well-integrated Privileged Access Management (PAM) suite with a range of capabilities for detection and mitigation of security threats caused by abuse of privileged accounts and access entitlements. BeyondTrust's Password Safe delivers market-leading shared account password management and session management capabilities across a wide range of target systems.

by **Anmol Singh**
asi@kuppingercole.com
April 2019

Content

Related Research

Advisory Note: Real-Time Security Intelligence - 71033

Advisory Note: Security Organization, Governance, and the Cloud - 71151

Architecture Blueprint: Access Governance and Privilege Management - 79045

Executive View: BeyondTrust PowerBroker for Unix & Linux - 70363

Executive View: BeyondTrust PowerBroker PAM - 70725

Executive View: BeyondTrust PowerBroker - 71504

Leadership Brief: Privileged Account Management Considerations - 72016

Leadership Compass: Privilege Management - 72330

Leadership Compass: Privileged Access Management – 79014

1 Introduction

In the age of digital transformation, not only the requirements for IT but also the way IT is done, are constantly evolving. To remain relevant, organizations must reinvent themselves by being agile and more innovative. Emerging technology initiatives such as the digital workplace, DevOps, security automation and the Internet of Things continue to expand the attack surface of organizations as well as introduce new digital risks. To stay competitive and compliant, organizations must actively seek newer ways of assessing and managing security risks without disrupting the business. Security leaders, therefore, have an urgent need to constantly improve upon the security posture of the organization by identifying and implementing appropriate controls to prevent such threats.

Privileged Access Management (PAM) represents the set of critical cybersecurity controls that address the security risks associated with the use of privileged access in an organization. There are primarily two types of privileged users:

1. Privileged Business Users - those who have access to sensitive data and information assets such as HR records, payroll details, financial information, company's intellectual property, etc. This type of access is typically assigned to the application users through business roles using the application accounts.
2. Privileged IT Users – those who have access to IT infrastructure supporting the business. Such access is generally granted to IT administrators through administrative roles using system accounts, software accounts or operational accounts.

The privileged nature of these accounts provides their users with an unrestricted and often unmonitored access across the organization's IT assets, which not only violates basic security principles such as least privilege but also severely limits the ability to establish individual accountability for privileged activities. Privileged accounts pose a significant threat to the overall security posture of an organization because of their heightened level of access to sensitive data and critical operations. Security leaders, therefore, need a stronger emphasis on identifying and managing these accounts to prevent the security risks emanating from their misuse.

Available Identity and Access Management (IAM) tools are purposely designed to deal with management of standard users' identity and access and do not offer the capabilities to manage privileged access scenarios such as the use of shared accounts, monitoring of privileged activities and controlled elevation of access privileges. Privileged Access Management tools are designed to address these scenarios by offering specialized techniques and unique process controls, thereby significantly enhancing the protection of an organization's digital assets by preventing misuse of privileged access.

Privileged Access Management (PAM), over the last few years, has become one of the most relevant areas of Cyber Security closely associated with Identity and Access Management technologies that deal with facilitating, securing and managing privileged access for both IT administrators and business users across an organization's IT environment.

At KuppingerCole, we define PAM solutions to constitute of following key tools and technologies:

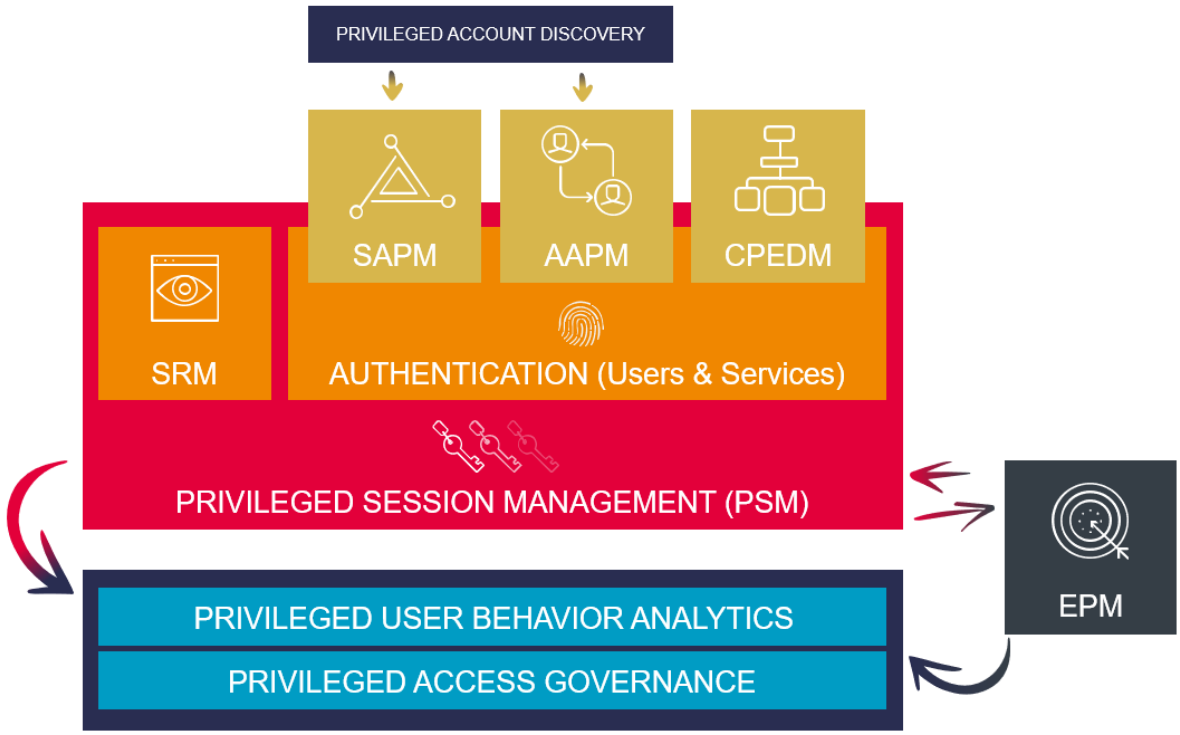

Figure 1: Blueprint of PAM tool and technologies

Privileged Account Discovery and Lifecycle Management (PADLM)
Shared Account Password Management (SAPM)
Privileged Session Management (PSM)
Session Recording and Monitoring (SRM)
Privileged User Behavior Analytics (PUBA)
Controlled Privilege Elevation and Delegation Management (CPEDM)
Application-to-Application Password Management (AAPM)
Endpoint Privilege Management (EPM)
Privileged Access Governance (PAG)

While credential vaulting, password rotation, controlled elevation and delegation of privileges, session establishment and activity monitoring have been the focus of attention for PAM tools, more advanced capabilities such as privileged user analytics, risk-based session monitoring and advanced threat protection are becoming the new norm - all integrated into comprehensive PAM suites being offered. We see a growing number of vendors taking different approaches to solving the underlying problem of restricting, monitoring, and analyzing privileged access and the use of shared accounts.

Among the key challenges that drive the need for privilege management are:

- Abuse of shared credentials
- Abuse of elevated privileges by authorized users
- The hijacking of privileged credentials by cyber-criminals
- Abuse of privileges on third-party systems
- Accidental misuse of elevated privileges by users

Furthermore, there are several other operational, governance and regulatory requirements associated with privileged access:

- Discovery of shared accounts, software and service accounts across the IT infrastructure
- Identifying and tracking of ownership of privileged accounts throughout their life-cycle
- Establishing a Single Sign-on session to target systems for better operational efficiency of administrators
- Auditing, recording and monitoring of privileged activities for regulatory compliance
- Managing, restricting, and monitoring administrative access of IT outsourcing vendors and MSPs to internal IT systems
- Managing, restricting, and monitoring administrative access of internal users to cloud services.

Consequently, multiple technologies and solutions have been developed to address these risks as well as provide better activity monitoring and threat detection. A specific area is the in-depth protection of server platforms such as Unix, Linux, and Windows. These focus on protecting the accounts such as "root" or "admin" on these systems as well as delivering in-depth protection against unwanted privilege elevation, altogether with capabilities of restricting the use, e.g., of specific shell commands. In addition, as more organizations adopt cloud applications or leverage cloud and virtual infrastructure, the PAM technologies must adapt to protect privileged access within these environments too.

For a detailed overview of the leading PAM vendors, please refer to the KuppingerCole Leadership Compass on **Privileged Access Management**[1]**.**

[1] Leadership Compass: Privilege Management (#79014)

2 Product Description

Based in the US, BeyondTrust is a leading vendor of Privileged Access Management, Secure Remote Access, and Vulnerability Management solutions with its headquarters in Atlanta, Georgia. It was founded in 1985 as Symark - a PAM vendor specializing in UNIX solutions, it acquired another software company specializing in Windows IAM solutions in 2009 and adopted its name. BeyondTrust was acquired by Bomgar in late 2018 and the combined entity retains the BeyondTrust brand. The resulting entity remains a privately held company with nearly 800 employees and some 20,000 customers worldwide.

Since 2009, BeyondTrust has made several strategic acquisitions, including eEye Digital Security and Blackbird Group. These acquisitions have allowed BeyondTrust to expand its technology portfolio and consolidate its products into an integrated risk intelligence suite - the BeyondInsight IT Risk Management Platform. By combining its Privileged Access Management Suite with its Vulnerability Management platform, BeyondTrust is able to deliver privileged access intelligence with information about endpoint and web application vulnerabilities, thereby offering a risk-based approach for managing corporate users as well as assets including on-premise, mobile and cloud-based resources.

Bomgar, on the other hand, with its recent acquisitions of Lieberman Software and Avecto has built a good portfolio of PAM technologies over time that includes some market-leading secure remote access, shared account password management and endpoint privilege management capabilities. While the BeyondTrust acquisition creates some functional overlap of technologies, the nature of acquisition puts BeyondTrust ahead of conventional value-creation activities in the PAM market by starting to acquire competitive targets for profit building and supporting economies of scale – depicting a leap forward for BeyondTrust, the BeyondInsight IT Risk Management Platform remains a modular and integrated family of products for Privileged Access Management that includes entitlement, password and credentials management for Unix/Linux, Windows, and MacOS systems to offer management of and required visibility into administrative privileges across an organization's IT infrastructure including servers and endpoints.

Password Safe remains BeyondTrust's flagship Shared Account Password Management (SAPM) product offering a mature password vaulting and credential management solution in addition to privileged session management features that include auditing, monitoring and recording of privileged activities. Password Safe provides leading Shared Account Password Management (SAPM) capabilities targeted at managing account passwords across the range of target systems including local and domain administrative accounts, named (non-generic) and shared (generic) administrative accounts, operating system accounts, application to application (A2A) accounts and cloud as well as social media accounts. It also provides discovery and rotation of SSH keys. Password management for the accounts includes secure password vaulting, password propagation to target systems and policy-based password rotation, synchronization and recovery.

Password Safe also provides password request management capabilities that offer self-service capabilities for administrators and end-users to request access to passwords, approval of password requests and provisions for management of passwords by system and application owners throughout the account's lifecycle. Password Safe offers a user interface that is administrator friendly

and abstracts password management functionalities in an effective and user-intuitive fashion. Emergency access and break-glass scenarios are supported by configuring automated approval workflows for password release.

Password Safe supports application to application (A2A) and application to database (A2DB) password management by eliminating hardcoded passwords in scripts, application code and configuration files by replacing them with either API or CLI for the purpose of retrieving passwords from the vault. Password Safe offers a REST interface that allows for programmatic retrieval of passwords via API. The interface may be wrapped in a variety of languages including C/C++, Perl, .NET or Java as well as CLI and PowerShell.

Wherever a username/password combination is used in an application or script, it can be simply substituted by the API call to retrieve the password dynamically from the Password Safe. For enhanced security, Password Safe authenticates the application or service making the password retrieval request using PKI (x.509) certificates and several other optional systems or application attributes such as hostname, IP address (including X-Forwarded-For), registered key, program signature, etc.

Privileged session management (PSM) capabilities offered by Password Safe include session establishment as well as activity auditing, monitoring and recording across the range of target systems. PSM capabilities from Password Safe are uniquely positioned in the market as it allows administrators to launch sessions directly from their standard toolsets without the need for logging onto the administration web console. Administrators can simply add a connection string to the administrative tools that they are accustomed to in order to launch sessions without the need for explicitly changing administrative behaviour. Offering session recording in DVR-style, Password Safe also supports live session search and role-based activity review and replay. Besides allowing provisions for conditional masking of data, Password Safe can also be configured to limit concurrent privileged sessions to target systems.

Password Safe integrates with BeyondTrust's BeyondInsight IT Risk Management platform to offer comprehensive logging, auditing, reporting and threat analytics capabilities across the BeyondTrust PAM products. The license for BeyondInsight IT Risk Management platform is included at no additional cost. The integration combined with BeyondTrust's Vulnerability Management product allows for asset and account discovery, profiling and classification of known and unknown assets such as shared and service accounts, SSH keys, PKI certificates and other credentials across an organization's IT infrastructure. By analyzing privileged password, user and account behaviour, Vulnerability Management assigns threat levels to the user, requested asset and the application launched. The use of threat and vulnerability intelligence combined with behavioural analytics allows it to uncover emerging risks in the environment by identifying and reporting on the type of activities that might be at risk. The integration with Password Safe further allows the platform to undertake remedial measures to proactively eliminate the potential threats such as session termination or heightened logging, auditing and review for the privileged session.

BeyondTrust Password Safe also integrates with several access governance solutions available in the market, notably SailPoint IdentityIQ, to provide automated provisioning, entitlements cataloguing and access certification for privileged accounts, thereby enabling privileged access governance. This bi-directional integration includes feeding privileged entitlements data for privileged and non-privileged access across the managed assets into SailPoint IdentityIQ for certification purposes. The changes to user's access entitlements as a result of access certification are automatically synchronized into the Password Safe.

Password Safe also integrates OOTB (out-of-the-box) with IT Service Management (ITSM) systems from CA, BMC Software and ServiceNow to regulate and review privileged access for administrators based on incident and change management policies within the organization.

Password Safe integrates with other products from BeyondTrustsuch as Endpoint Privilege Management for Windows and Unix/ Linux to offer a comprehensive and well-integrated PAM platform. It also integrates with BeyondTrust's AD bridging solution Active Directory Bridge. In addition, integration into BeyondTrust's Secure Remote Access solutions (formerly from Bomgar) allows for sessions to be instantiated using injected credentials directly from Password Safe without ever exposing them to the end user or administrator. This application to application approach extends the BeyondInsight platform to other solutions in the BeyondTrust portfolio.

Configurable in Active-Passive failover configuration for distributed nodes, Password Safe allows for near real-time replication of data and password changes across the nodes to support high availability. Password Safe also offers an Active-Active configuration providing linear scaling and resilience for Enterprise implementations.

BeyondTrust plans to work on expanding the Password Safe feature set to accommodate the specialized needs of Lieberman Privileged Identity customers and enable a migration path for them in the mid-to-long term. Password Safe will be positioned as the primary password vaulting solution for Remote Support and Privileged Remote Access solutions in the long term.

3 Strengths and Challenges

BeyondTrust Password Safe is a market leading password vaulting solution offering integrated shared account password management (SAPM), application to application password management (AAPM) and privileged session management (PSM) capabilities. Offering a simple and straightforward UI, Password Safe enhances the operational and administrative experience of the users.

Available in physical and virtual appliance formats, Password Safe is deployable on public cloud-delivered from Azure, Google and AWS marketplaces. This will also offer better integration with cloud-based services and applications in addition to integration with host-based components to manage passwords across on-premises systems.

Technology maturity and market understanding remain the primary strengths of BeyondTrust as a key and long-established player in the Privileged Access Management market. Offering a comprehensive PAM suite, Password Safe comes with enhanced integration across the products within the BeyondTrust family.

The host-centric approach for privileged access management offers more granular control and better management of target platforms and resources than the proxy-based approach. While the approach may be seen by some as an architecture shortcoming that is associated with additional maintenance overhead for certain deployment scenarios, it may be instrumental in environments requiring better integration, granular control of target systems and detailed auditing and logging of privileged activities. Password Safe has positioned itself as a leading password vaulting solution within BeyondTrust's family of PAM products that represent one of the most comprehensive PAM solutions in the market today.

Strengths	Challenges
• Technology maturity and market understanding • Large market share owing to a strong, well-established global partner ecosystem • Supports both proxy, host-based and hybrid deployments • Offers improved and deep integrations across the BeyondTrust product portfolio • Offers integration with third-party access governance products for privileged access governance • Deep integration and granular controls into target platforms due to the host-centric approach	• Longer development cycles for integrating Bomgar Privileged Remote Access and Privileged Identity (Lieberman ERPM) with Password Safe • Some functionality overlaps with Bomgar's PAM portfolio • Threat analytics requires additional Vulnerability Management purchase

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a leading Europe-based analyst company for identity focused information security, both in classical and in cloud environments. KuppingerCole stands for expertise, thought leadership, and a vendor-neutral view on these information security market segments, covering all relevant aspects like Identity and Access Management (IAM), Governance, Risk Management and Compliance (GRC), IT Risk Management, Authentication and Authorization, Single Sign-On, Federation, User Centric Identity Management, eID cards, Cloud Security and Management, and Virtualization.

For further information, please contact **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstraße 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com