KuppingerCole Report

EXECUTIVE VIEW

by Martin Kuppinger | September 2019

Devolutions PAM Solution

Devolutions provides a PAM solution targeted at SMB customers that provides a good baseline set of PAM capabilities and easy to deploy and operate. The solution comes with a password vault, account discovery capabilities, and strong remote access features. While some of the more advanced capabilities of the leading-edge PAM solutions are lacking, the product fits well to the target group of SMBs.

by **Martin Kuppinger**
mk@kuppingercole.com
September2019

Content

Related Research

Architecture Blueprint: Access Governance and Privilege Management - 79045
Advisory Note: Privilege Management - 70736

Leadership Compass: Privileged Access Management
Buyer's Guide: Consumer Identity and Access Management Solution – 80111
Architecture Blueprint: Hybrid Cloud Security – 72552

1 Introduction

Privileged Access Management (PAM), over the past few years, has become one of the most relevant areas of Cyber Security associated with IAM (Identity and Access Management) that deals with identifying, securing and managing privileged credentials and the resulting access across an Organization's IT environment. Once considered a technology option for optimizing administrative efficiency by managing passwords and other secrets, PAM has evolved into a set of crucial technologies for preventing security breaches and credential thefts. PAM today concerns Security and Risk Management leaders as well as Infrastructure and Operation (I&O) leaders across the industries for several security and operational benefits.

Privileged Access Management represents the set of critical cybersecurity controls that address the security risks associated with privileged users and 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 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 stronger emphasis on identifying and managing these accounts to prevent the security risks emanating from their misuse.

Among the key challenges that drive the need for managing privileged access are:

- Abuse of shared credentials
- Abuse of elevated privileges by authorized users
- Hijacking of privileged credentials by cyber-criminals
- Abuse of privileges on third-party systems, and
- 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
- Identification and continuous tracking of ownership of privileged accounts throughout their life-cycle
- Establishing and managing privileged session to target systems for enhanced operational efficiency of administrators
- Auditing, recording and monitoring of privileged activities for regulatory compliance
- Managing and monitoring administrative access of IT outsourcing vendors and MSPs to internal IT systems, and
- Managing and monitoring privileged access of business users and IT administrators to cloud infrastructure and applications

Consequently, multiple technologies and solutions have been developed to address these risks, as well as provide better activity monitoring and threat detection.

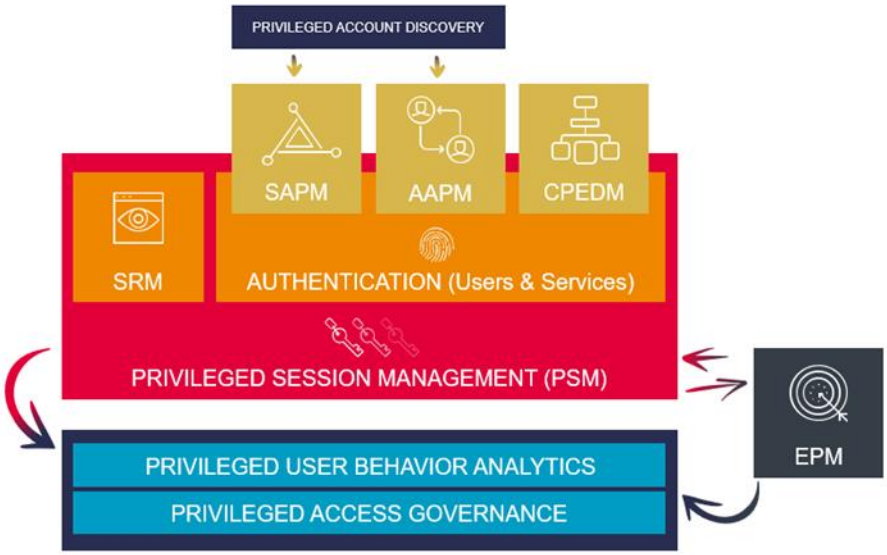

Figure 1: Architecture Blueprint of PAM tools and technologies

PAM is essential to all types of companies, well-beyond the large businesses. On the other hand, the broad and complex spectrum of technologies within the PAM market segment and the sometimes complex deployment are not always well-suited specifically for SMBs (small/medium businesses). While they need PAM, their focus (unless being high-risk businesses, e.g. in a critical infrastructure industry) must be on some essential capabilities, which specifically include

- Managing credentials securely, specifically for shared passwords (Shared Account Password Management)
- Providing secure remote access whenever required, as a baseline Privileged Session Management
- Account Discovery to move this into protection

Devolutions focuses on specific PAM solutions for the SMB market, covering remote access, shared account password management for various types of accounts, and is about to add account discovery.

2 Product Description

Devolutions has a set of products that are centered around managing remote access to systems and securing passwords of users. These cover various use cases, from individual user's Password Management to Remote Connection Management and Remote Access, and last but not least Privileged Access Management (PAM). Furthermore, Devolutions also integrates their Remote Access solutions into other vendor's PAM solutions.

As outlined above, PAM is a challenge for virtually every businesses, because every business is a potential target of attackers and internal fraud. The challenge for SMBs is the complexity of many of the leading PAM solutions, both in their functional breadth going well-beyond what most SMBs require, and in their deployment and operations.

Devolutions focuses on a more light-weight PAM approach that builds on the set of capabilities they have developed over the past years, plus adding additional features. The main addition is in network discovery, focusing on identifying privileged (and specifically shared) accounts across the various systems in a network and putting them under control.

Together with the ability for remotely managing target systems running various operating systems such as MacOS, Windows, and Linux, and the password vaulting and management capabilities, this forms a PAM solution covering the essential capabilities required by SMBs, while remaining lean and easy-to-use. Providing a lean PAM is essential for success in SMB organizations, because these are rarely able to deploy and maintain complex infrastructures.

The Devolutions offering comes with a central password vault that stores credentials and provides them to the users when required, or in the background when launching remote sessions. Access to these credentials and sessions can be centrally managed, based on folders that group various systems. It integrates with Microsoft Active Directory, allowing to use Active Directory groups for implementing a role-based access control model for managing access to credentials and remote sessions. Based on the password management capabilities, automated password changes are also supported. There is an automated password generators available for creating strong passwords on the fly, as well as the password history can be tracked, if required.

Aside of the central password vaults, there is also an option of having user-specific, private vaults that are only accessible to individual users, for their privileged accounts.

In conjunction with the new discovery capabilities, the managed accounts can be automatically identified across the network. Once added to the list of systems and grouped into folders, these accounts can be fully protected by the Devolutions PAM solution.

Notably, Devolutions PAM is focused on running in a single instance. However, there is support for multiple vaults, providing high scalability and also the ability to distribute vaults across locations if required. While there are some limitations in supporting complex, geographically dispersed environments, there is good support for scalability and distributed vaults. That is adequate for the target group of SMBs, where IT commonly is managed and operated from one central location.

Due to the integration with the established remote access capabilities of Devolutions, there is broad support for running remote sessions on target systems via different protocols and different networks. Protocols include, amongst others, SSH and RDP (Remote Desktop Protocol). The product supports various types of connections such as via VPNs. Credentials can be injected into these sessions, thus hiding the password from the administrators. The solution also supports mobile access, which can be of high importance specifically for SMBs, when administrators are called outside of their working hours and must quickly access systems.

Access to remote sessions can be based on two-factor authentication (2FA), with broad support of 2FA options. Amongst the supported two factor capabilities we find Office 365/Azure Active Directory, SMS, Email, Duo Security, Google Authenticator, Yubikey, RADIUS Server, VASCO, AuthAnvil, and SafeNet. An interesting capability is that 2FA can be activated individually per user or centrally for all users.

While Devolutions provides good remote access features, there is no session monitoring and recording implemented yet. However, these capabilities are anyway very extensive in operations, with massive man-power required for monitoring or for analyzing session recordings. While this is of high relevance for high risk use cases, it is rarely adequate for SMBs.

Devolutions' PAM solution comes with good reporting capabilities that provide information about the use of accounts, successful and failed login attempts, login histories per user and accounts, and other information. There is also a view on the currently connected users. The solution also provides a real-time Email notification passed on defined events per session, user, or role. Again, these capabilities are adequate to the target group of SMBs.

3 Strengths and Challenges

The Devolutions PAM solution is targeted at SMB customers, even while it comes with several enterprise-grade capabilities, thus also being attractive for larger organizations looking for a baseline PAM solution that is quickly to implement and easy to operate.

The solution covers the baseline features required in PAM such as account discovery, password vaulting, and secure remote access. The remote access capabilities are broad and support various types of access patterns across a variety of target operating systems.

Being focused on the entry-level of the PAM market, certain more advanced capabilities are lacking, including elaborated session monitoring and recording. Furthermore, the solution is still an on premises-only offering. Devolutions, as of now, does not offer a cloud variant of the product, which would be attractive specifically to SMBs.

In sum, Devolutions PAM is an interesting offering that is well-targeted at the SMB companies, where it provides a good baseline set of PAM features that can be rolled out and managed easily. We recommend looking at this solution as an alternative to the established players for that type of companies.

Strengths	Challenges
• Clear focus on SMB requirements on PAM, delivering good baseline capabilities • Simple deployment and operations • Strong remote access and remote session capabilities, supporting multiple protocols and remote access patterns • Support discovery of accounts in the network • Broad support for two factor authentication • Multiple vaults supported	• Focused on core PAM capabilities, lack of support for extended PAM features such as session monitoring and recording or Privileged User Behavior Analytics • No cloud deployment option available • Relatively small vendor with small partner ecosystem and no global reach yet

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
Wilhelmstr. 20-22
65185 Wiesbaden | Germany

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