KuppingerCole Report

WHITEPAPER

by Paul Fisher| October2019

Privileged Access Management requirements for Small to Medium Size Businesses (SMB)

Privileged Access Management (PAM) is fast becoming one of the most important areas of Identity and Access Management (IAM). Privileged accounts are given to admins and other users within an organization to access critical data and applications. However, if these are not managed securely, SMBs can find themselves having accounts still open for people who have left or for people who no longer need access or simply giving too many people privileged accounts. Criminals and hackers are becoming more adept at stealing and using credentials for privileged accounts. To reduce this risk, and uphold GRC obligations within an organization, a suitable PAM solution is needed to manage these security challenges.

by **Paul Fisher**
pf@kuppingercole.com
October 2019

Commissioned by Devolutions

Content

Table of Figures

Related Research

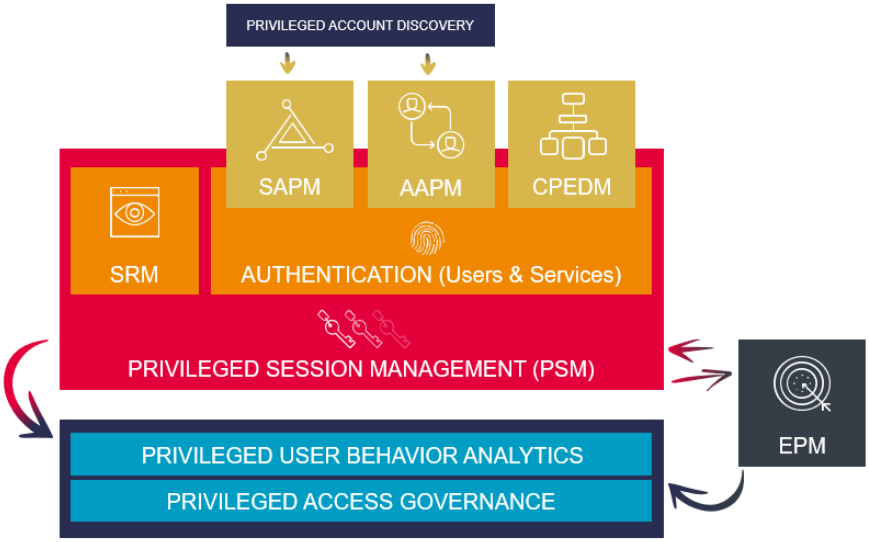
Architecture Blueprint: Access Governance and Privilege Management - 79045

Leadership Compass: Privileged Access Management - 79014

1 Introduction

The pressure on organizations to transform and digitize to create new products and services has meant different processes and technologies are entering the workplace, and some are creeping in without a strategy to manage them. These include trends such as Cloud, AI, Process Automation, IoT, DevOps, and XaaS (Anything as a Service). These trends are not confined to large enterprises but companies of all sizes, including Small to Medium sized Businesses (SMBs).

Taken together, these trends and technologies offer big opportunities for companies and organizations to ensure they remain competitive, but they also need to manage them and ensure they do not increase security and data risks. This is especially true of the massive increase of data and access points offered by these technologies which while enabling the digital change needed, can also increase the risk of access being hijacked by hackers, criminals or hostile state actors.



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)

Figure 1: The key components of a comprehensive PAM solution. SMBs would not necessarily need all of these. (Source: KuppingerCole)

The modern infrastructure therefore requires access be granted to data and IT services to a wide variety and increasing number of stakeholders. These include traditional line employees, admins and managers but now also individuals from partner organizations, contractors and even customers. Some of these will request and need access to critical assets in order to fulfill their roles: these are known as privileged users.

Identity and Access Management (IAM) systems have long been used to manage access to data and services for less critical parts of the business: enabling employee sign on to workstations is one example. From IAM came a subset technology called Privileged Access Management (PAM) which was originally designed simply to manage passwords or two factor authentication (2FA) for critical assets across the organization. Until recently those with privileged access and more basic access were easy to manage as roles and access requests did not change all that much.

Digital transformation has changed the landscape. Today data access is lot less binary and much more fluid. Employees and other stakeholders may need privilege access to complete a certain task and then no longer need it. Contractors may be onsite for a short time also needing privilege access accounts, or when working remotely or at a subsidiary site. The increased exposure to data and critical assets has meant the threat of unauthorized access has been elevated, and modern PAM solutions must do as much as possible to prevent security breaches, as well as provide efficient speedy access to those who need it, when they need it – and more importantly deny it when no longer needed. It goes without saying that the digital landscape has made this a much more challenging market for PAM vendors and has transformed PAM into something much more than a simple administration tool. Done well, a PAM investment installation can increase business efficiency and competitiveness for an SMB.

Given the complexity and speed of change of the modern organization any PAM solution must do more than simply provide privileged account access. It needs to be capable of monitoring access from an easy to understand central database and be able to reach into the extended network so that third parties, contractors and remote workers are monitored and given the right access when they need it. The best PAM solution must also go further and allow different tiered access of privilege so that line managers can grant access to certain employees and groups.

While credential vaulting, password rotation, controlled elevation and delegation are important, modern PAM should also offer privileged user analytics, risk-based session monitoring and advanced threat protection. It should also be able to flag suspicious behavior with blocking procedures automatically activated by PAM without need for human intervention, once red flags have been set.

In recent years, the perception of Privilege Management has changed considerably, and many vendors have entered the market. Many obviously target the large enterprise market but the SMB market is now also being catered for. While the scale may be different, smaller businesses are undergoing similar digital changes as bigger companies and in unique ways. Often, they act as the pivot between one organization and another and act as vital partners in digital supply chains. Therefore, they have similar identity and access challenges as they also seek to manage privileged accounts for their own employees, contractors and those of the businesses they are working with. Some SMBs will of course also be serving as managed service providers to bigger organizations, in which case security of data is paramount.

But while the PAM challenges might be similar, the solutions for smaller businesses may need to be different in scale and feature set. This whitepaper sets out why SMBs should now consider PAM, what are the essential components of PAM for SMBs and how new features and trends are making PAM easier for SMBs. It also provides SMB decision makers an overview of best practice in deploying and running a PAM solution that is fit for purpose and scalable.

2 Highlights

- Shows why Privileged Account Management (PAM) should be considered by SMBs
- Looks at how digital transformation is impacting on SMBs and presenting new identity challenges
- Explains why PAM can help defeat cybercriminals and hackers looking to steal credentials and data and why it is now essential for SMBs
- How a good PAM setup for SMBs should automate as many functions as possible, be easy to use and provide real time insights
- Gives an independent overview of Devolutions PAM solutions for SMBs

3 Why SMBs need a PAM solution

SMBs should not think that PAM is only for larger organizations. Even those that may consider their data may not be of interest to criminals or hackers should be aware that they could act as a steppingstone to data they process on behalf of clients or partners. More critically, the digital transformation of business everywhere is something SMBs cannot ignore if they wish to survive. And to survive they must ensure that privilege account access is managed securely as that is crucial to be a successful part of the new IT landscape.

It's a misconception that only large organizations require PAM or indeed IAM solutions. The nature of modern business, which is connected, agile and shifting across traditional boundaries affects smaller organizations as much as larger ones. Data is the lifeblood of any business and secure, on demand access to that data is what creates value for organizations, partners and customers. SMBs are inescapably part of the wider digital ecosystem that is reshaping the business landscape. While those SMBs that control financial or personal data should undoubtedly consider PAM, we would recommend it as an option for almost any SMB that values the integrity of its data and that of its customers - which should be all.

Data and IT services are becoming part of the supply chain, where businesses are consuming new services based on data, and this is changing the way we are dealing and allowing access to data. The positive side is that it enables growth and new revenue streams for SMBs and others when this data is unlocked, but it also means that we need to manage access to greater volumes of data than was traditionally available.

We would recommend PAM as an option for almost any SMB that values the integrity of its data and that of its customers – which should be all.

Just as digital transformation is reshaping the way organizations operate, the explosion of data and distributed computing and cloud has given cyber criminals new opportunities to steal data and gain access to company assets. Many times, these attacks are successful because privileged account credentials have not been properly stored, protected and managed, and hackers are able to take control of them. Not for nothing are privileged credentials called the "keys to the kingdom" as they provide access to the most critical and valuable data in any organization. And yet even now, many SMBs are managing privilege accounts and passwords in unprotected Excel spreadsheets or similar open formats.

Cyber attackers do not differentiate between small or large enterprises, they will always look for the most vulnerable access points to data wherever they are. Often such attacks are preceded by criminal gangs scouting social media for details of employees who have important roles within an organization, those more likely to have privileged access. The tendency for people to reveal so much of themselves on social sites like LinkedIn, including where they work and their job function, has made criminals lives easier.

At the same time criminals will use also malware to actively seek unprotected privilege account credentials within the organization itself – such as password kept in the clear on unprotected documents. Attackers know that SMBs often have less than strict security policies, and employees lack the security awareness and controls found in larger companies

Data is the lifeblood of any business and access to that data is what creates value for organizations, partners and customers.

The rise of ransomware has also led to a growing need for PAM, especially for SMBs who are less able to pay large ransoms and may even be put out of business by a successful ransomware attack. Criminals looking for instant financial gain will use hijacked credentials to access systems and then lock them which can be devastating to a business. Other intruders will seek to Intellectual Property for espionage purposes or simply to damage a company – again this may well be data belonging to a larger business being processed by an SMB.

SMBs do not share the security budgets or resources as larger enterprises, they may not even have dedicated security personnel and therefore must ensure that the security budget is spent effectively (ROI). Given the shift in focus to protecting data and identity management brought on by the digital age, it makes sense to consider a new or replacement PAM solution with urgency, even if some cyber security functions have been outsourced to a Managed Security Services Provider (MSSP). PAM must be used to enhance the basic security functions provided by anti-phishing, anti-malware and firewall technologies.

The increase in threats and criminal activity puts SMBs firmly in sight of attackers. Attackers believe (rightly in many cases) that many SMBs will have not adequately protected their privileged accounts and remote server access and are actively targeting and probing SMBS to see if they are right. SMBs are not immune from prosecution and fines under data regulation such as GDPR and need to prove that they are doing as much as possible to protect personal data for which they act as data controller.

PAM must be used toenhance the basic security functions provided by anti-phishing, anti-malware and firewall technologies and address the limitations of such tools.

SMBs are also as likely to work with third parties such as contractors, freelancers and service providers – often other SMBs providers – thereby extending privilege access further. SMBS may also wish to allow third-party access to brokers to enable legal sharing of data for marketing or other purposes. All of these new opportunities must also be protected. Altogether, the accelerating trends in working practices, outsourcing, cloud and digital transformation -- all of which increase focus on identity and access -- are something that SMBs are part of. The imminent security risks that these changes pose means they must consider access tools such as PAM to mitigate those risks as far as possible.

SMBs do not share the security budgets or resources as larger enterprises, they may not even have dedicated security personnel and therefore must ensure that the security budget is spent effectively (ROI). Given the shift in focus to protecting data and identity management brought on by the digital age, it makes sense to consider a new or replacement PAM solution with urgency, even if some cyber security functions have been outsourced to a Managed Security Services Provider (MSSP). PAM can enhance the basic security functions provided by anti-phishing, anti-malware and firewall technologies and address the limitations of such tools.

4 Choosing the right PAM for SMBs: key capabilities and functionalities

The key to choosing the right PAM solution is to consider needs, budgets of the organization and match to features available from the vendor. Not all SMBs will need enterprise level features and resources but at the very minimum a PAM solution should offer an Access Manager, Shared Password Vault and Session Manager to manage privileged accounts on premises, in the cloud and for employees and contractors. As well as these a minimum level of auditing and analytics is needed to meet compliance standards.

We have established that PAM makes a good security investment choice for SMBs so what should they look for when deciding on the right solution? There is a broad and complex spectrum of technologies on the market and the sometimes-complex deployment requirements is not always well-suited to the specific needs of SMBs. Some smaller businesses involved in high-risk and targeted sectors such as financial services or critical infrastructure may need features closer to enterprise level, while others will need a less comprehensive set of security tools and settings.

To make the right decision SMBs should ask some key questions:

- What is your budget and how can you maximise ROI and features?
- Are you managing resources in a private or public cloud?
- What specific IT environments and data need protection?
- Who are your privileged users and what are their roles and responsibilities?
- Have you done an audit of privileged users?

At KuppingerCole we believe that a PAM installation should have the following critical features as standard:

- An Access Manager to control access to privileged accounts. For SMBs this should be an easy to configure dashboard style application through which an admin or security manager can create, add delete and update access for privileged account holders. Added controls in the Access Manager can automate access duration so that contractors' access is switched off and ex-employees' credentials are revoked.

- An encrypted Shared Password Vault is essential to protect passwords and credentials from both hackers and employees. The vault prevents employees from knowing their passwords and so cannot share them. Ideally it is best stored on premises or in a private cloud.

- A Session Manager is necessary for compliance and incident response purposes. By having a complete record of what privilege account users do, companies can track suspicious behavior or find potential vulnerabilities. This may not be available for some PAM solutions aimed at SMBs.

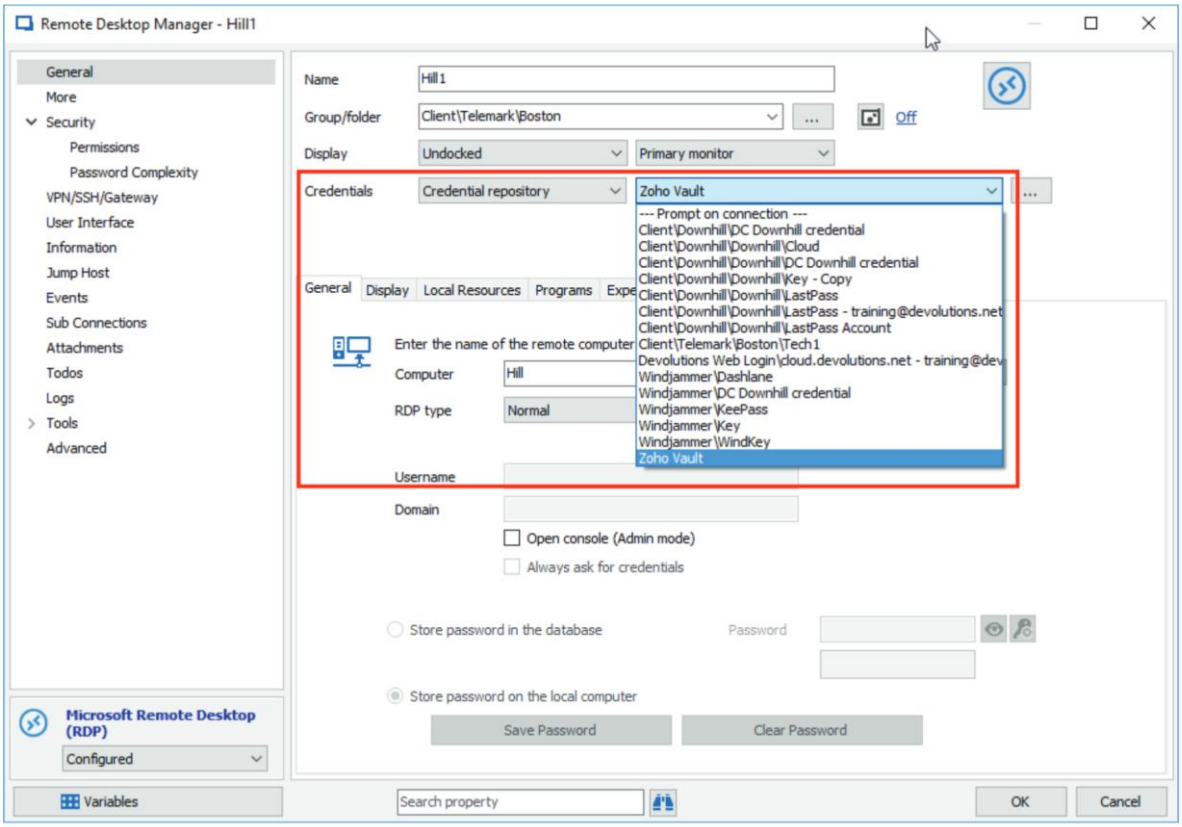


Figure 2: Granting remote access and storing credentials to external users (Source: Devolutions)

A solution that fulfills these will provide a first line of defence against the threats mentioned earlier. However, while SMBs may share similar characteristics in terms of size and budgets, their sector or data requirements may affect their eventual choice of PAM solution. For example, an SMB may work within the defense or government sector in which case the data protection requirements are likely to be far more stringent than a small engineering firm. Another SMB may act as a service provider in which case its account management tools will need to address access by its own employees and those of its customers, and will need a scalable, agile and flexible PAM solution. A software business may need to accommodate fast changing session requests to enable rapid development and upgrades of its products in a competitive market. Before any investment decisions can be made the organization needs to look carefully at how it conducts business and what kind of data it has access to.

An SMB may work within the defense or government sector in which case the data protection requirements are likely to be far more stringent than a small engineering firm.

So, while the access management needs of SMBs can be as daunting and critical as those for a larger enterprise, they remain small businesses and should look for PAM solutions from vendors that consider their operational needs. A "lite" or cut down version of an enterprise system may not be appropriate. An enterprise PAM is likely to demand a much higher level of upfront technical knowledge on behalf of its administrators and users. SMBs do not necessarily have resources for traditionally qualified security or data protection personnel and will rely on adequate and trustworthy levels of automation in the product.

SMBs should look for PAM solutions from vendors that consider their operational needs. A "lite" or cut down version of an enterprise system may not be appropriate.

Automated password and session management of all privilege accounts means that those SMBs with no or few security admins can be assured that the PAM solution will take care of this important task. A rules-based policy of least privilege – where users are given only the least amount of access, they need to get their jobs done, should be easily set and maintained via a dashboard. The same should be available for control and accountability.

For larger or SMBs that are involved in critical industry sectors, more advanced operational, governance and regulatory features that may be needed include.

- Discovery of shared accounts, software and service accounts across the IT infrastructure
- Identification and continuous tracking of ownership of privileged accounts throughout their lifecycle
- 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

- Managing and monitoring privileged access of business users and IT administrators to cloud infrastructure and applications
- Privileged Single Sign On (SSO) capability to multiple sessions

While a PAM solution for SMBs may not offer the most granular levels of analytics, without any it is hard for companies to understand how data is accessed and how threat actors may exploit this, so any level of analytics is highly desirable. The same should be said of auditing capability, ideally in-line with common auditing and security standards such as ISO 27001. Automation of scanning, patching and reporting of vulnerable systems is recommended as is automatic update of the PAM solution itself. Dashboard style, out of the box reporting is highly recommended making it easy for resource-light smaller companies keep on top of security analytics and reporting.

5 Running PAM for SMBs: deployment, organization and operation lifecycle

Deciding on a PAM solution is only a start. SMBs need to apply correct lifecycle management to the solution to ensure that it remains fit for purpose and is configured for changing operations and personnel changes. Crucial to this is the Review and Audit stage that enables modifications to be made to privilege accounts, passwords and serves as an audit of data trails and security risks.

Having decided that a PAM solution is necessary for the organization, and we would recommend that any SMB should consider it, it must be set up for the most effective lifecycle. While most PAM solutions on the market may be suitable for an SMB, it is logical to ensure that it can be configured for the varied requirements of SMBs and their business needs.

One task a PAM solution cannot do is decide which users should be privileged and which should not. This is a relatively easy to discover in a smaller SMB with fewer employees, but for larger it will involve an audit of job roles and functions – including those of contractors or temporary workers. This, however, must be the first step in setting up PAM in any organization, whatever the size.

Depending on workload, this may be a task that can be completed in house with available resources or it may need outside help but however it is completed it's essential that privilege accounts are classified in alignment with business goals and risks. For example, a contractor or temp may need access to certain high-level data to complete a task or collaborate on a project on which product development or new services may depend. Ordinarily a contract worker would be considered a higher risk for privileged accounts but, in this case, access must be granted for the good of the business.

One task a PAM solution cannot do is decide which users should be privileged and which should not. This is a relatively easy to discover in a smaller SMB with fewer employees, but for larger it will involve an audit of job roles and functions.

The advantage of well configured PAM solution is that such access can be identified, controlled and managed so that the contractor only gets as much access as they need for no longer than is required This process known as least privilege is fundamental to the successful implementation of PAM and all privilege account holders should be subject to it. A dashboard that highlights how privileged accounts are being used can help identify security risks and alert admins or managers to attempts at accessing privileged accounts by non-authorized users.

SMBs should follow a lifecycle management structure for PAM installation and usage. A well-designed and deployed PAM solution will be scalable as well as easily configured to accommodate changes in an organization. By having a strict lifecycle management policy for a PAM changes can easily be detected and implemented. This lifecycle can be identified by the following steps.

Define

Define and classify privileged accounts in the organization in alignment with business goals and risk. It's a good idea to educate users on the importance of data security and why only certain people can have access to data and IT services. Once this step is completed, the PAM solution can be configured to set the controls for the identified privilege accounts.

Manage and monitor

Businesses grow, and organizations mature; therefore, any PAM solution must respond to these changes by being able to discover and manage privileged accounts. This is essential to avoid privileged account "creep" or abandoned or unused accounts left open undetected. Depending on the features of the PAM solution it may also track any account abuse by employees or attempts by outsiders to infiltrate. It is also important that the same checks and balances are applied to admin accounts as these are highly targeted by criminals and hackers. The concept of least privilege must be strictly applied to admin accounts

Any PAM solution must respond to changes by being able to discover and manage privileged accounts. This is essential to avoid privileged account "creep".

Control passwords

Passwords must be managed in an encrypted vault or multiple vaults allowing secure storage and administration of passwords. Password management can be configured so that users do not know their passwords and cannot reset passwords without authorization. It is important to schedule password rotation and delete passwords at the first sign of malicious activity. Integration with SIEM products enables users to log suspicious activity to prevent similar attacks occurring.

Review and audit

Privileged account activity must be continually reviewed. Continuously monitoring privileged account usage via audits and reports helps identify unusual behaviors. This should be a constant process. No matter how well a PAM solution is featured, it cannot adapt automatically to business changes. This requires human involvement by acting on activity reports produced by PAM solutions. Reviews and audits can be used to improve the performance and security of the organization.

6 The Devolutions approach to PAM for SMBs

Devolutions offers a PAM solution that is targeted at SMBs that aims to offer the best of enterprise level solutions with an ease of use favored by smaller organizations. It offers essential features such as a central password and credentials vault which can integrate with Microsoft Active Directory. It also offers account discovery and secure remote access. The remote access capabilities are broad and support various types of access patterns across a variety of target operating systems. It also 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

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 finally 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 size of business, because every company 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 functionality going well-beyond what most SMBs require, and in their deployment and operations.

Devolutions focuses on a more lightweight PAM approach that builds on the set of capabilities they have developed over the past years. 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 to remotely manage 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.

Devolutions focuses on a more lightweight PAM approach that builds on the set of capabilities they have developed over the past years, plus adding additional features. 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 generator available for creating strong passwords on the fly, and 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.

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

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.

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 SMBsbut the Password Server can be hosted by a third-party cloud provider of the customer's choosing.

In sum, Devolutions PAM is an interesting offering that is well-targeted at 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 this type of companies.

Notably, Devolutions PAM is focused on running in a single instance. However, there is support for multiple vaults, providing high scalability and 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.

Devolutions provides good remote access features, and is session monitoring and recording is available on the local client should the customer need it. However, such capabilities are labour intensive, with large manpower required for monitoring and analyzing session recordings. While this is of high relevance for high risk use cases, it is not always needed needed 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 on defined events per session, user, or role. Again, these capabilities are adequate for the target group of SMBs.

7 Recommendations

Privileged Account Management is highly recommended for SMBs even if they currently feel they are not big enough or do not yet process the kind of data that needs this kind of protection. Many SMBs would discover, through a careful audit of data usage and access that they may well be exposing the company to risks without realizing through poorly managed privileged accounts. Even if we lived in a world without cyber-attacks, the efficiency and operational benefits that a well set up PAM solution delivers should be attractive to any business. These also reduce the threat of ex-employees or temporary workers retaining access to systems and helps keep SMBs on the right side of compliance and audit legislation.

Given the aggressive threat landscape, stringent regulatory frameworks and the connected infrastructures of digital transformation, we would highly recommend any SMB to investigate a Privileged Account Management solution. It is almost inevitable that smaller businesses will at some point find the need to give certain individuals access to critical data, whether belonging to the organization itself, a partner, on premises or in the cloud. It may even be then case that the SMB does not even classify data and allows uncontrolled access to all data, which is not a good security posture. We would highly recommend any SMB to conduct a data audit to establish its data access situation and type of PAM solution needed.

The results of the audit or self-assessment should be considered against other factors that will influence the choice of PAM solution. It is recommended that the organization considers its budget, the resources

available to set up, run and modify a PAM solution and what level of features are needed. Not all SMBs will have the same requirements for their type of business and how they access data.

SMBs would be advised to investigate those SMB solutions that are geared towards an SMB and not simply cut down version of enterprise grade solutions. It is unlikely that SMBs will have the technical resources or personnel in house to configure a full-service PAM solution designed for enterprises.

Ease of use and configuration should therefore be a primary consideration. This is important for administrators and for end users who need to access data quickly to get tasks completed. A dashboard style interface is almost an essential requirement for a PAM solution aimed at SMBS, as it enables quick access to accounts and allows rapid configuration and changes without deep knowledge. That said, training for any PAM solution is recommended and we would favour any vendor that offers training set up and support as part of its service offering.

It is recommended that SMBs use PAM as a tool for measuring risk and security posture for the company. A good PAM solution will offer insight from activity recorded in the Session Manager. If the PAM can generate reports easily and on demand this will enable the SMB to adapt to access demand changes and audit data trails across the organization. At the heart of a PAM is the Password Vault where passwords are stored in an encrypted shell. As this is fundamental to the security of the organization, we recommend that some time is spent considering the type of encryption used and the management of passwords within the vault. While not all features will be available in any PAM solution aimed at SMBS, buyers should endeavour to find that which provides as many core functionalities and balance this against cost, ease of use and scalability.

8 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 global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

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

KuppingerCole Analysts AG
Wilhelmstr. 20-22
65185 Wiesbaden | Deutschland

Telefon +49 (211) 23 70 77 - 0
Fax+49 (211) 23 70 77 - 11
www.kuppingercole.com