Top 6 Features SMBs Should Look for in a Privileged Access Management Solution

Devolutions

PAM IS CRITICAL FOR SECURING ORGANIZATIONS OF ALL TYPES AND SIZES

Most Privileged Access Management (PAM) solutions on the market today are designed for large enterprises. While offering a lot of features and much flexibility, they aren't suited to SMBs because of their complexity and cost. But PAM is critical for securing organizations of all types and sizes, and features provided in popular enterprise-grade PAM solutions are also relevant to SMBs. So, when looking for the right PAM solution for your business, make sure that it includes key features that are essential for securing privileged accounts.

In this whitepaper, Devolutions looks at 6 features that SMBs should look for in a PAM product.

1. Ease of deployment and management

Active Directory (AD) is the most widely deployed identity management solution today and all PAM products integrate with it. Microsoft has its own PAM solution based on Windows Server 2016 and Microsoft Identity Manager (MIM). Deploying it requires adding an AD forest to your existing infrastructure and at least one server running MIM. It brings considerable complexity and there are lots of moving parts, making it not only difficult to deploy but it also increases management and administrative costs.

When you are looking for a PAM solution, make sure that it doesn't require changes to your existing Active Directory infrastructure and that it integrates with Azure AD if you use Office 365. There should be the option to separate components across multiple servers to improve performance for larger deployments and simple wizard-driven deployment is preferable, along with a graphical management console that is intuitive to use. Finally, when things go wrong, time is money so make sure that backup and restore of your chosen PAM solution is straightforward.

2. Secure password vault

Passwords are an imperfect solution but like them or not they are still the default means of securing access to IT resources. Over the years, people have found ways to make passwords easier to manage, including writing them down on Post-It notes and sticking them to monitors, and using the same password across multiple sites. Neither of those methods are recommended.

Keeping passwords in multiple stores, like Excel spreadsheets, text files, and remote desktop sessions makes it harder to integrate them into a PAM solution and it leaves accounts more vulnerable to exposure because files aren't designed for managing passwords.

But whether it is an end user that needs to store credentials securely or an organization that wants to secure passwords for granting access to IT resources, a secure password vault gives everyone the confidence that passwords are secure and that they can be retrieved when necessary. Look for a PAM solution that has a secure centralized password vault that can be shared and accessed from anywhere.

3. Logging and reporting

Insight into your IT infrastructure gives you the ability to respond to issues and prevent them. PAM is no exception and it is important to understand how privileged accounts are used in your organization. Any PAM solution you consider should be able to record what, who, when, and where credentials are being used.

But logs are only useful if you can extract the information you need, when you need it. Not only must a

PAM solution record all password-related activity, including login attempts and history, but it should include out-of-the-box reports that let you quickly surface information. And with any system that records lots of data, it's important that you can filter out the noise using advanced search capabilities. The ability to customize reports and export data in different formats is also something you should look for.

4. Built-in two-factor authentication

Irrespective of whether you use a password manager, a secure password vault, and/or follow password security best practices, if credentials are compromised they can be used by an attacker to gain unauthorized access. Two-factor authentication adds an extra layer of protection that requires users to have something in their possession in addition to knowing their password. One of the most popular ways of implementing two-factor authentication is using an authenticator app, like Google Authenticator, which provides a code that users must provide in addition to their password before access is granted to a resource.

Because there are so many ways in which passwords can be compromised, and it is impossible to provide 100% protection, two-factor authentication is an essential tool for securing privileged accounts. You should look for two-factor support that provides a variety of different authentication options, like Google Authenticator, SMS, email, RADIUS, and Yubikey.

5. Brokered Account

A good PAM solution doesn't just securely store passwords and control access to them. It also 'brokers' passwords between the password server and client software so that users never need to know the actual password for a privileged account. This means that password rotation isn't strictly necessary, i.e. automatic generation of a new password each time a credential is checked out, because the password cannot be reused by the user. Nevertheless, password rotation is usually included even when account brokering is present.

Account brokering also prevents users accessing resources outside of a workflow provided by the PAM solution, potentially reducing the potential for credential abuse. Users are often the weakest link in the security chain so look for a PAM product that provides account brokering.

6. Role-based access to credentials

Role-based access control (RBAC) simplifies management by providing a series of 'roles' that can be assigned to users, providing them with access to only the privileged credentials they are authorized to use. RBAC makes it easy for organizations to separate duties and implement other controls to ensure credentials aren't accidently provided to unauthorized users. Defining roles and then configuring finegrained access permissions to sessions is the easiest and safest way to protect privileged credentials and prevent accidental exposure to the wrong people.

As most organizations already use Active Directory, look for a PAM solution that has RBAC and integrates with AD so that you can use existing users and groups. Managing access permissions, users, and groups can get complicated quickly, even in small businesses, so RBAC can help streamline the process and make ongoing management of a PAM solution easier, while also leaving you safe in the knowledge that access to privileged credentials is always properly controlled.

Devolutions Privileged Access Management

Devolutions Privileged Access Management solution provides all the features above and more. It is specifically designed to meet the needs of SMBs, providing enterprise-grade features to bring a level of protection usually only afforded to large organizations while at the same time being simple to deploy and manage. SMBs can reduce the risks from insider threats and data breaches that often originate from credential misuse or compromise; and use Devolutions Privileged Access Management to meet reporting and compliance requirements.

Devolutions' other products integrate with PAM to provide a comprehensive solution for SMBs, including Remote Desktop Manager (RDM), which helps users and IT manage access to remote sessions that require use of privileged credentials.