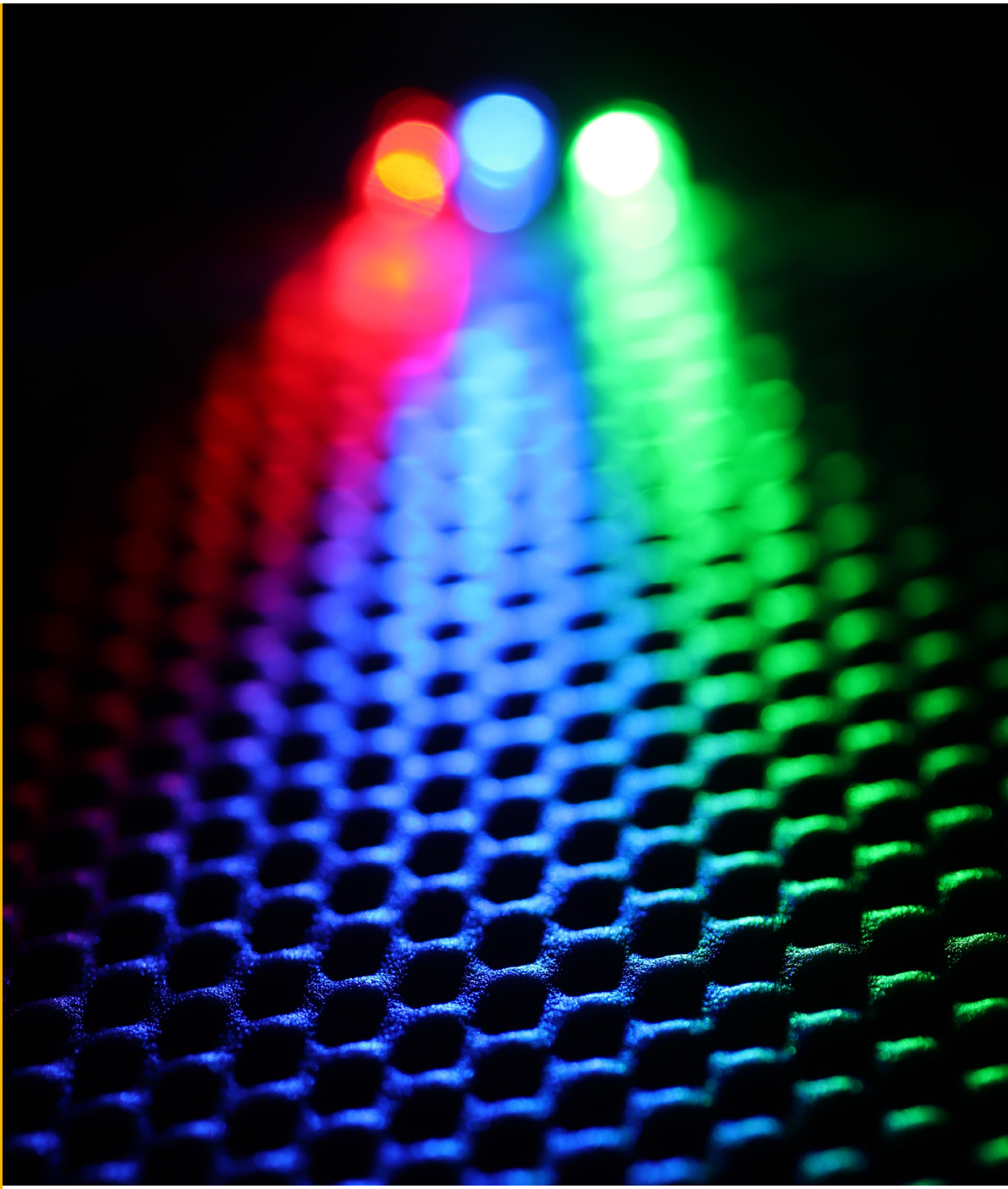
Petri IT Knowledgebase Resource
A BWW Media Group Brand

PETRI
WE GET IT



Petri Whitepaper
November 16, 2021

Must Have Features for a Remote PAM Solution

Sponsored by

Devolutions

Must Have Features for a Remote PAM Solution

Overview

Securing and managing access to privileged accounts is crucial to any organization's security strategy. This is especially true in today's climate of ever-increasing malware attacks, ransomware, and security exposures. The pandemic has certainly contributed to this situation by causing a far larger number of employees to work remotely, which has increased these security exposures and risks. Many businesses are also simultaneously undergoing data modernization efforts.

New technologies, like the Hybrid and Multi Cloud, AI, Process Automation, IoT, DevOps, the Edge, and Analytics offer significant opportunities for businesses to become more flexible and increase their ability to be competitive. However, they also increase complexity and security risks. The rise in remote access and these new digital transformation technologies increase the organization's attack surface, making it more difficult than ever to secure access for your business-critical applications and services.

Challenges in remote access

Some of the main problems that businesses face today are centered around employees and their use or misuse of security credentials and authorizations. Of course, passwords are a major problem. Employees often use weak passwords, plus they tend to reuse these passwords between multiple different sites and applications – often even posting them on yellow sticky pads.

Not surprisingly employees will typically choose productivity over security and protection. In addition, businesses often grant employees with more privileges than they actually need because this can make it a bit easier to do the different tasks that they need to accomplish.

Beyond this, the administrators themselves can also be a security risk – especially in smaller and medium sized businesses. Administrative accounts, like Root for Unix/Linux systems or Administrator for Windows systems, often include high levels of unrestricted access to your servers; including full access to files, directories, and resources with read-write-execute privileges. They can also perform system modifications like shutting down systems, loading device drivers, configuring system and network settings, as well as creating and configuring accounts and even cloud resources.

Worse is the fact that in many cases, these administrators will go ahead and use these highly privileged accounts for everyday application access and other office work - opening the door for malware and ransomware to gain access to your network complete with elevated privileges. There is often no secure way to share privileged credentials, apart from actually divulging account and password information, and there's often no record of highly authorized activity. In addition, businesses can also be vulnerable by having accounts that are still open for people who are no longer with the organization or for people who no longer need privileged accounts.

Cybercriminals, hackers, and malware are all becoming better at stealing and using credentials for unauthorized access to critical business resources and data. Today's increased remote workforce further complicates security and privilege management. Remote employees are often using personal devices and insecure home networks for work related activities. In many cases, these remote workers are your business's weakest security link. This is especially critical for users requiring privileged access. Today's organizations need a strong strategy and tools for managing remote access and privileged accounts to prevent them from becoming vulnerabilities and potential security breaches.

Using Privileged Access Management (PAM) to manage account security

PAM enables you to maintain control and visibility over your organization’s most critical systems and data. PAM is one of the most important areas of Identity and Access Management (IAM). PAM can help discover and prevent data breaches caused by both malicious insiders and external cybercriminals. The threat of unauthorized access is increasing along with the possibility of increased exposure of data and other critical assets.

Privileged access allows security and maintenance functions as well as system-wide configuration changes by providing highly authorized administrator or super user access. Modern PAM solutions are designed to prevent security breaches, as well as provide efficient access to business resources to the personnel that need it. PAM allows you to inject credentials into accounts when they are needed – and more importantly remove them when they are no longer needed.

For instance, employees may need privileged access to complete a certain task and then no longer need it once that task is complete. Likewise, contractors may be onsite or working remotely for a short time and they might need privileged account access for all or part of their assignments. PAM solutions can provide this type of limited access while tracking privileged activity and then ending that access when it is no longer needed.

PAM needs to do more than provide privileged account access. PAM is also capable of monitoring access for local employees as well as contractors and remote workers. Some PAM solutions allow different tiered access of privileges so that line managers can grant access to certain employees and groups. The problems that PAM solutions must address include:

- Weak passwords
- Reusing passwords
- Password rotation
- Too much privileged access
- Using privileged accounts for regular work
- No secure way to share privileged credentials
- No way of delegating security and access from multiple roles
- The need for integration with Active Directory
- No logging of highly authorized activity

It’s important to remember that nowadays securing your business is no longer just about one physical place. Instead your PAM solution needs to be able to be accessible throughout your organization and it needs to be able to secure multiple locations – including today’s remote workforce.

PAM Components

PAM solutions typically consist of the following components:

- **Encrypted Shared Password Vault** – The password vault provides a secure location to store and protect passwords and credentials.
- **Access Manager** – The access manager controls access to employee accounts. It is used to create, add, delete, and manage access for privileged account holders.
- **Session Manager** – The session manager tracks account activity and can provide a record of what privilege account users do. Businesses can use session logs to track suspicious behavior and find potential security vulnerabilities.

Must have features for remote PAM

Today's PAM solutions need to meet both the needs of both local as well as an ever increasing number of remote users. To be an effective solution for a remote work force your PAM solution needs to focus on three key areas: a secure password store, an efficient way to securely access applications, and a secure way to share passwords with colleagues.

Secure password store

While some organizations have begun to move away from passwords, there's no doubt that passwords are still the default means of securing access to IT resources. Unfortunately, today users must often deal with a multitude of passwords with different requirements. And to do so, they often resort to a number of different and highly insecure ways of dealing with passwords including writing them down on Post-It notes and sticking them to monitors, reusing the same password across multiple sites, and storing passwords in various unsecured documents like Excel spreadsheets and text files.

A Google survey found that at least 65% of people reuse passwords across multiple, if not all, sites. These makeshift solutions aren't designed for managing passwords and they leave accounts vulnerable to exposure. The Verizon Data Breach Investigations Report revealed that compromised passwords are responsible for 81% of hacking-related security exposures.

An encrypted Shared Password Vault is essential to protect passwords and credentials for both regular employees and administrators. A secure password vault provides users with a convenient central and secured location to store their passwords. For administrative access, PAM solutions take privileged account credentials and store them in that secure repository. This repository can be either local or it can be stored in the cloud.

Administrators need to go through the PAM system to access these privileged credentials. They can check out the credentials at which point they are authenticated to the application, service, or site that they need to use, and their access is logged. When they are finished, the credentials are checked back in and automatically rotated. Then the next time they want to use those credentials, they once again need to go through the PAM system. Security is much stronger as employees don't have to resort to simplistic do-it-yourself solutions. Passwords are not exposed and an encrypted Shared Password Vault gives you the knowledge that your organization's passwords are secure and that they can be easily retrieved on-demand.

In addition to providing a secure shared storage location for passwords, PAM solutions can also offer several other password management capabilities. They can provide password templates and enforce customizable password rules with a variety of complexity specification and requirements. They can also generate strong passwords on demand as well as providing automatic password randomization and automatic password regeneration and renewal.

Efficiently secure access for applications and services

Providing the right level of access to your applications and services is vital for an effective remote PAM solution. Managing access permissions for different users and groups can get complicated even in smaller businesses. Support for Role-Based Access Control (RBAC) can help streamline ongoing management of a PAM solution. The ability to delegate authority simplifies management by assigning users to different sets of roles that provide them with access to only the privileged credentials they are authorized to use. RBAC makes it easier for organizations to separate duties and ensure credentials aren't accidently provided to unauthorized users. It's also important for a PAM solution with RBAC to be able to integrate with Active Directory so that you can use existing users and groups.

Next, you want to be sure that your administrators are not using elevated access to execute normal applications like Office, email or web browsing. When you're using a PAM solution, system administrators need to go through the PAM system to access their credentials. Highly privileged credentials are essentially checked in when they're in use, accounts are authenticated, and their access is logged and finally checked out when that use is finished. The PAM solution should be able to record what, who, when, and where credentials are being used as well as being able to record all password-related activity, including login attempts and history as well as providing reports that provide visibility into highly privileged account activity.

Securely sharing passwords

Sharing passwords – especially administrative passwords – can be a real security risk for most businesses. This is especially true for sharing passwords with remote personnel because the passwords are often communicated through unencrypted emails which can be easily compromised. If the account is an Active Directory administrative account, this can be a huge potential security exposure for the entire organization.

By centralizing privileged credentials in one place, PAM systems ensure a high level of security for privileged access. However, some PAM solutions don't just securely store passwords and control access to them. They also securely transmit credentials between the password server and client software so that users never need to know the actual password for a privileged account. This ability takes PAM to another level of security by enabling administrators to access and share highly authorized credentials without ever needing to see the passwords. This type of account brokering lets users and administrators launch remote connections to servers, applications, and websites without ever needing to know the passwords that are being used, enabling secure password and credentials sharing between employees.

Devolutions remote PAM solutions

Devolutions Server addresses these critical PAM requirements for local and remote connections. It provides enterprise-grade features in a platform that is easy enough to use for the small and medium sized businesses (SMB). Devolutions Server provides a level of protection that is usually only available to large organizations, yet it is easy to deploy and manage. Devolutions Server directly addresses the primarily remote PAM requirements with the following capabilities:

Secure Password Vault

At the core of Devolutions Server is the secure Password Vault. The vault protects credentials as well as other privileged information like certificates, secret keys, files, images, license keys, credit cards, and access to privileged accounts using AES 256-bit encryption. It can be deployed either on-premises or in your private Azure cloud. The Password Vault provides the ability to automatically scan and discover privileged accounts. It can also be used to supply employees with their very own personal user vault to store both private and other business-related passwords and information.

Secure privileged sessions management

Devolution's PAM solution has the ability to perform account brokering where credentials are injected directly into remote sessions without ever exposing them to the user. Privileged accounts are requested for checkout, which automatically notifies administrators for approval and begins logging account activity. This ability to broker accounts enables you to share credentials without ever exposing or even needing to know the passwords behind highly privileged accounts.

It also enables you to add additional security by enforcing time limits on privileged sessions. This ensures they are not left unattended where they could be potentially exposed. It can also enforce password rotation every time you check in a privileged account, which changes both the system and Devolutions Server's credentials. This type of password maintenance automation removes the burden of administrators from having to manually edit accounts on a schedule. Devolutions Server can also be combined with Devolutions Remote Desktop Manager for remote system access. You can launch remote sessions from the web browser using credentials from the shared password vault.

Password management and two-factor authentication

Devolutions Server also provides different levels of password protection. First, it enables you to establish and enforce a wide variety of password rules with multiple customizations. You have the ability to employ specific password templates that allow you to meet your own custom password policy requirements. There is the ability to generate strong passwords using the built-in password generator. It also offers account discovery and secure remote access. The remote access capabilities are broad and there is support for various types of remote access across a variety of systems.

Two-factor authentication can be implemented system-wide or on a per-user basis. Devolutions Server can be integrated with a variety of two-factor and multi-factor authentication solutions including: Office 365, SMS, Email, Devolutions Workspace, Duo, Google Authenticator, Yubikey, Radius Server, Azure Multi-Factor, and SafeNet.

Role-Based Access Control and Active Directory integration

The RBAC in Devolutions Server enables flexible management of access rights with the ability to delegate different levels of permissions. You can assign granular permissions controlling who has access to view, edit, and delete vaults, folders, and entries in the Password Vault. The ability to delegate these responsibilities removes some of the management burden from security administrators. Devolutions Server can also integrate with Microsoft Active Directory. Both users and groups can be synchronized with Active Directory to reflect your existing user infrastructure.

Logging and session recording

As you saw earlier, visibility into the activity of privileged accounts is vital for ensuring they are not misused. Devolutions Server provides privileged account transparency by keeping track of all privileged account, password, and session related actions. You can monitor how accounts were used, when they were used, and who accessed them. In addition, it logs privileged access and can send the Syslog file to external tools for reporting and auditing purposes. Devolutions Server allows you to save remote session recordings and to access those recorded remote sessions for playback and review. It also offers account reporting capabilities that provide information about the use of accounts, successful and failed login attempts, login histories per user and accounts.

Devolutions Server editions

There are three Devolutions Server editions that are designed for different sized businesses. All of the editions support users, groups and RBAC, two-factor authentication, Active Directory and Microsoft 365 integration, password history, connection history, connection logs, email notifications, and event subscriptions.

The three editions of Devolutions Server are:

- **Team** – 15 users, 1 data source, 1 domain - $499.99
- **Enterprise** – 50 users, 3 data sources, 1 domain - $1,999.99
- **Platinum** – Unlimited users, data sources, domains – Per sales contact

Devolutions Server solves remote PAM challenges

In this age of ever-increasing security threats, ransomware, and security breaches, PAM has become an essential technology for businesses of all types and sizes to protect their vital information and resources. Today's distributed remote workforce adds to these security risks. PAM solutions, like Devolutions Server, can close your organization's security gaps and give you control over the use of your privileged accounts for both local and remote users.

Additional Information

For more detailed information about SMB cybersecurity challenges and solutions, be sure to check out Devolutions State of Cybersecurity in SMBs in the 2021 report.

Devolutions