Password Manager vs. Privileged Access Management (PAM) vs. Single Sign-On (SSO)

Devolutions

THE RIGHT SOLUTION IS CRITICAL TO PROTECT YOUR ORGANIZATION AGAINST BOTH EXTERNAL HACKERS AND INTERNAL ROGUE USERS.

It's been said that in life, it's the simple things that really matter — like watching a lovely sunset or playing with your cat. But sometimes life gets complicated, like when you're trying to figure out whether your organization should invest in a password manager, a Privileged Access Management (PAM) solution, or a Single Sign-On (SSO) solution.

The right solution is critical to protect your organization against both external hackers and internal rogue users. Fortunately, you don't have to be like Homer Simpson and play "Eeny, meeny, miny, moe". Instead, you can use the following advice to help your organization make the right choice.

SOLUTION: PASSWORD MANAGER

Typical Use Case: Your organization has a limited budget and needs to protect all user accounts in a secure and centralized vault, while also increasing password security awareness. Your organization does not need to manage privileged accounts or privileged users.

Description: Password managers like Dashlane, Devolutions Password Server, Zoho Vault, and others in the marketplace enable your organization to save and securely store all credentials and other sensitive information in a centralized vault, which users can access with a master password. As such, users don't have to remember multiple strong passwords or insecurely store passwords on spreadsheets, sticky notes, and so on. It's also important to note that unlike SSO solutions, password managers aren't session-based, and they don't work with all user accounts and all cloud applications.

Password Manager Advantages:

- User-friendly solution
- Cost-effective for SMBs
- Protects against outside threats
- Enforces password best practices

Password Manager Disadvantages:

- If not available out-of-the-box, organizations need to add a 2FA tool to establish a second layer of security for specific accounts
- Does not support privileged user and privileged account management
- Does not monitor the system
- Is not designed to meet stringent compliance requirements

SOLUTION: PRIVILEGED ACCESS MANAGEMENT (PAM)

Typical Use Case: Your organization has a substantial security budget, and you need to monitor and manage privileged accounts and privileged users. You also need to automatically create audit logs and meet stringent compliance requirements (e.g. GDPR, ISO 27001, NIS, HIPAA, PCI-DSS, SOC 2, etc.).

Description: A PAM solution – Devolutions Password Server, CyberArk, BeyondTrust, Thycotic – enables your organization to control, manage and monitor privileged access to critical systems, while also helping you meet compliance requirements. A good PAM solution will help you achieve three important goals. First, it lets you isolate the use of privileged accounts to reduce the risk of accidental or intentional misuse of credentials. Second, it gives you more control and awareness of your IT environment. Third, it proactively warns administrators if changes are made to specific accounts, or if unusual user behavior is detected.

PAM Advantages:

- Designed for controlling, managing and monitoring privileged access to critical systems
- Supports a granular protection system defined by a role-based access control
- Generates full and detailed reporting and automatically creates a comprehensive audit trail
- Meets stringent compliance requirements and standards

PAM Disadvantages:

- Requires substantial IT resources to setup, maintain and manage
- Costly and may exceed SMB security budgets
- Not user-friendly to setup or manage — in-house or third-party expertise is required

SOLUTION: SINGLE SIGN-ON (SSO)

Typical Use Case: Your organization needs to secure business accounts for all users who access specific cloud applications.

Description: An SSO solution like onelogin, Okta or JumpCloud, allows your users to access multiple cloud-based services and resources, but without having to enter new login credentials each time they switch applications (or switch back to previous applications). Unlike a password manager that only protects user passwords, an SSO solution can protect all privileged accounts.

SSO Advantages:

- Logs user activities and monitors accounts (including privileged accounts)
- Eliminates time-consuming credential re-authentication
- Improves productivity
- Minimizes phishing
- Improves compliance through a centralized database

SSO Disadvantages:

- Not suitable for systems requiring guaranteed access — when users lose credentials to one system, they lose access to all systems
- Can increase risk exposure — if hackers steal a user's credentials they have access to multiple apps instead of just one
- Cannot add MFA if the option is not supported by the SaaS app
- Does not cover all cloud applications

A NOTE FROM OUR CSO:

When it's time to select a technology to prevent unauthorized access to organization's information, it is necessary to exercise caution to understand which threats it addresses, and which risks it might induce. Advantages and disadvantages of technologies described in the article are great hints to identify those risks. However, I would like to share a broader perspective with these questions: Will a Password Manager be accepted and used appropriately by all your end users? Will an SSO solution cover effectively all intended services? Does upper management understand the need for such control? Answers to such questions will most likely impact the technology selection process and avoid disastrous negative impacts such as: improper coverage of the solution, loss of end-user buy-in to corporate security policies, and lack of budget. I truly believe that a broader view will lead to a balanced, combined, use of all those technologies (Password Manager, PAM and SSO) that will optimize investment, improve security and maintain user buy-in. There are integrated solutions available on the market that make use of all those technologies and that will ease the required efforts to deploy and maintain them for your IT and security staff.

There you go folks! Hopefully this advice will point your organization towards the password manager, PAM solution, or SSO solution (or maybe a combination) that you need to protect your data, your customers and your reputation.

As always, please let us know your thoughts by using the comment feature of the blog. You can also visit our forums to get help and submit feature requests, you can find them here.