Exploring 4 Aspects of Password Management

Devolutions

SMARTER AND SAFER WAYS TO PROTECT DATA

With the headlines full of data breach stories, most organizations (and it should really be ALL organizations!) are looking for smarter and safer ways to protect data. Clearly, **robust password management is an essential part of this solution**. In their research, Gartner focuses on four key aspects of password management:

1. Policy, Standards & Guidelines
2. Password Management Tools
3. Privileged Access Management (PAM)
4. Personal Password Managers

Let's briefly look at each aspect to appreciate how they differ, and also how they overlap and work together as part of a comprehensive enterprise password management program.

Policy, Standards & Guidelines

These critical elements establish the framework and responsibilities for password usage and administration. Mandatory requirements typically include:

- Passwords must be unique **for each app and device** (i.e. end users cannot have the same credentials for more than one login).
- Passwords must be **suitably strong and complex, but not to the point that confused or frustrated** end users undermine security by writing down passwords or storing them in text files or spreadsheets.
- End users must **never share their passwords with anyone**. For example, an end user who urgently needs a file cannot ask a colleague to log in on their behalf and send it to them.
- Password reset processes must **guard against snooping or social engineering**.

In addition, it's important for organizational leadership to ensure that end users are familiar with applicable password management policies, standards and guidelines (and receive coaching/ training as needed). With that being said, it must be clearly understood that **while strong password management governance can mitigate risk, it is not a standalone method** — especially with regard to sensitive and high-profile accounts.

Password Management Tools

These tools, which can exist independently or embedded in various identity administration solutions, enable two critical functions:

- **Allow end users to securely reset their account(s)**. An increasing number of organizations are mandating 2FA/MFA alongside (or instead of) traditional authentication methods like answering security questions.
- **Synchronize passwords for end users across numerous systems**, which make things more

  efficient for users. It can also improve security, since users who must remember multiple passwords sometimes (as noted above) store them in alarmingly unsafe ways!

Privileged Access Management (PAM)

PAM technologies enable organizations to establish secure access to critical assets. They also **help organizations monitor, record and audit privileged accounts to ensure compliance**. In the 2017 Market Guide for Privileged Access Management, Gartner highlights two types of PAM solutions that should be required across the infrastructure (IaaS, PaaS and SaaS):

- Privilege account and session management (PASM) solutions, which protect accounts by vaulting their credentials.

- Privilege elevation and delegation management (PEDM) solutions, in which specific privileges are granted on managed systems by host-based agents.

Devolutions is part of a small list of select vendors that Gartner (in the above-noted Market Guide) has deemed effective at delivering an alternative way to **mitigate the risks around privileged access, or providing a set of specific and deep capabilities** to augment existing PAM deployment. As noted by Gartner analysts: "Devolutions offers Devolutions Server, Password Vault Manager and Remote Desktop Manager. The combination of these products offers capabilities for vaulting administrative passwords, account sharing and session management."

Personal Password Managers

As Sysadminotaur amusingly covers here, end users are often the weakest link in the password management chain. Personal password managers help close the gap by giving users a **secure yet easy-to-access method of storing and retrieving passwords,** along with other sensitive information (e.g. credit card numbers, etc.).

A variety of personal password managers are available in the marketplace, including those that store data locally or in the cloud. While it is safer to store data on-premise, some end users find it more convenient to use the cloud so they can access their password manager from anywhere.

The Bottom Line

Developing, executing and optimizing a robust password management program that embraces all 4 elements described above will go a long way **to ensuring organizations stay safe**. That way, if they make the headlines, it will be to announce some good news instead of having to make excuses for yet another data breach!