Devolutions

World Password Day: A Closer Look at Cloud-Based vs. On-Premises Password Management Solutions

AN OPPORTUNITY TO PROMOTE BETTER PASSWORD HYGIENE

May 6th is World Password Day. This annual occasion, which falls on the first Thursday in May, is an opportunity to promote better password hygiene, which unfortunately is something that many businesses need to do right away — especially SMBs.

Devolutions' State of Cybersecurity in SMBs in 2020/2021 Survey revealed that while some SMBs are taking steps to strengthen password security, others are not rising to the occasion — and consequently they are putting their employees, customers, organization, and reputation at risk. For example:

- **47% of SMBs still allow end users to re-use passwords across personal and professional accounts.**
- **29% of SMBs rely on human memory for storing passwords.**
- **15% of SMBs do not use any tools whatsoever to protect or manage passwords.**

The bad news is that this is not the kind of problem that "fixes itself" over time. On the contrary, it only grows bigger and becomes more dangerous. Research has found that 81% of data breaches are caused by compromised, weak or re-used passwords. Even more alarming is that the average cost of a data breach for SMBs has surpassed $200,000 per incident (for large organizations and enterprises the price tag has skyrocketed to $3.6 million per incident), and 60% of SMBs go out of business within six months of getting hacked.

However, there is some good news as well: the worldwide password management solution marketplace is booming, and is estimated to be worth a whopping $2.05 billion by 2025. This means business of all sizes — including SMBs that have historically been ignored by many service providers — have an increasing number of products to choose from.

To help your business make the right choice — if you are implementing a password management solution for the first time, or if you want to replace your current solution — **we invite you to explore the following overview of cloud-based and on-premises solutions:**

Deployment

- **Cloud:** Contrary to what some non-IT people believe, cloud password management solutions are not hosted somewhere "in the air." Rather, they are hosted by a service provider. Customers, however, can access those resources as often as they want, and from any internet-enabled device.
- **On-Premises:** On-premises password management solutions are deployed in-house, and within a business's infrastructure. Unlike a cloud model, the business rather than the service provider is responsible for maintaining the solution and all associated processes.

Control

- **Cloud:** With cloud password management solutions, the service provider maintains control — not because

they are trying to wrestle it away from customers, but because (as discussed above) they are responsible for hosting and maintaining the solution. As such, they require control in order to keep things operational and secure.

- **On-premises:** With on-premises password management solutions, businesses keep all resources in-house and are in total control. While this is an advantage for some businesses, it can be a drawback for others — especially SMBs — that lack the infrastructure and specialized employees to continuously optimize and secure the solution.

Security

- **Cloud:** In the past, concern regarding security was the number one reason businesses hesitated to adopt cloud apps, resources, and solutions (including but not limited to cloud password management solutions). However, in recent years cloud security has dramatically improved. For example, cloud password management service providers monitor security 24/7, implement multiple types of security, and conduct ongoing penetration testing. This is a level of deep, ongoing protection that many SMBs cannot achieve due to limited budgets and lack of cybersecurity specialists.
- **On-premises:** Since on-premises password management solutions are hosted, maintained, and controlled within a business's IT infrastructure, they are inherently more secure than cloud solutions. Note that this does not mean that cloud solutions are insecure. Rather, it simply means that on-premises solutions provide an enhanced layer of security. For some businesses, this enhanced layer is important or may be essential for compliance reasons (more on this in the next section). For other businesses, this enhanced layer is not required, and as such choosing a cloud solution may be more practical and affordable.

Compliance

- **Cloud:** When it comes to compliance, businesses need to ensure that the cloud password management solution service provider they choose adheres to relevant compliance standards such as SOC 2 Type II and ISO 27001:2013. In addition, service providers should use cryptographic design in their solution.
- **On-premises:** Some businesses in certain industries, such as healthcare, may be required to maintain full in-house control of their data (i.e. their data cannot be stored outside their environment with a third-party service provider). In this case, choosing an on-premises password management solution is necessary.

Cost

- **Cloud:** With a cloud password management solution, businesses do not need to purchase software or hardware. Instead, they purchase a license or a subscription and access the solution over-the-web. The type of access they are entitled to depends on what kind of license/subscription they have. For example, some solutions provide access to specific machines, while others provide access to specific users. This latter model is much more business-friendly, because it enables end users to access the solution from wherever they are, and through any device.
- **On-premises:** On-premises password management solutions are typically more costly than cloud solutions. This is because it is necessary for businesses to implement the required IT infrastructure and processes, while also covering ongoing operating and maintenance costs. Many SMBs lack the budget and the personnel to meet these requirements, and therefore focus on cloud solutions instead.

Implementation

- **Cloud:** Cloud password management solutions "should" be easy to implement. We emphasize "should" because unfortunately this is not always the case. Some cloud solutions are straightforward and deploy rapidly, while others are highly (and needlessly) complex, and they require significant configuration and testing. Businesses that opt for a cloud solution need to ensure that implementation is smooth rather than stressful. Examining credible reviews and taking advantage of a free trial are good ways to verify this.
- **On-premises:** On-premises password management solutions are inherently more complex to implement than cloud solutions because they are hosted and maintained in-house. As such, they must be configured and integrated with the environment. Businesses that choose an on-premises option should ensure that the service provider has resources and programs to make the implementation experience as fast and trouble-free as possible.

Additional Considerations

In addition to the above, **there are some other factors that businesses should consider** regardless of whether they choose a cloud or on-premises password management solution. **These include:**

- **Expert Technical Support:** The service provider should provide responsive support from qualified experts before, during, and after implementation.

- **Upgrades and Updates:** The service provider should continuously upgrade their solution (with cloud solutions, updates are typically automatic; with on-premises solutions, updates need to be implemented by the in-house IT team).
- **Companion Tools:** The service provider should provide a growing roster of companion tools to enhance useability and value.

And the Winner Is…

Some overviews that explore two types of solutions are about finding the "best" one. **However, that approach does not apply here**. Neither cloud nor on-premises password management solutions are inherently superior. As highlighted above, each has advantages and limitations.

Ultimately, the right choice is the one that improves (and for some businesses, dramatically improves) password management hygiene. Because given the costs and consequences of a data breach, keeping credentials away from the bad guys these days is tougher — and more important — than ever.

From the Desk of Our CSO Martin Lemay:

The never-ending debate between cloud and on-premises solutions strikes again when it comes to password management solutions. However, in my opinion, the discussion should revolve around what the specific password management needs are for the organization. These needs may vary according to multiple factors, such as (but not limited to):

- User location and roles
- Availability requirements
- IT environment size and complexity
- Value of data to protect
- Compliance and security requirements

In some cases, hybrid deployments that combine elements of both cloud and on-premises solutions could solve distinct needs, instead of selecting only one more restrictive product. Furthermore, one solution could be deployed multiple times to address problems such as segregation of duties. Regardless of what you choose — on-premises, cloud, free, or paid — ensure that you clearly define all of your needs before shopping for technology, and while you obviously need to address today's needs, you'll need to anticipate future requirements as well.

Explore Our Solutions

At Devolutions, we proudly offer a cloud password management solution called **Password Hub Business**, and an on-premises password management solution called **Devolutions Server**.

Password Hub Business is a secure and cloud-based password manager for teams. It empowers SMBs to securely vault and manage business-user passwords — along with other sensitive information like building alarm codes and corporate credit card numbers — through a user-friendly web interface that can be quickly, easily, and safely accessed via any browser. Simply put, Password Hub Business is the perfect balance of security and useability. To request a free trial, click here.

Devolutions Server is a full-featured shared account and password management solution, with built-in privileged access components created to meet the ever-expanding security requirements of SMBs. It is fast to deploy and easy to implement, and it has all the basic features required for a PAM solution, while remaining very affordable. When used in combination with our centralized remote connection and management solution, Remote Desktop Manager, Devolutions Server forms a robust, privileged account and session management tool that supports over 150 integrations and technologies. To request a free trial, click here.