Why your business needs a secure digital vault

Password management solutions evolve to accommodate needs of individuals and businesses in one highly secure setting

WHITE PAPER

TABLE OF CONTENTS

Both individual users as well as entire businesses cannot be blamed for upping their efforts to protect sensitive data with secure, comprehensive password management solutions. After all, as one major cybersecurity study revealed, nearly two-thirds (63%) of confirmed data breaches involved weak, default or stolen passwords.[1] What the data doesn't reveal are the tremendous financial losses and hardships resulting from the password-enabled breaches.

Password management solutions for individuals have soared in popularity, in part because most of them are free downloads. Very often these same individuals utilize their own solutions in the workplace. This can have negative consequences because IT administrators need and want to have a transparent look into the password practices of employees. Another major study found that nearly 60% of small and mid-sized businesses (SMBs) have no visibility into employees' password management practices.[2]

That is precisely why a secure vault can be an ideal solution that gives businesses and individuals the best of both worlds. Individuals can securely store passwords and all digital credentials within the secure vault. Business leaders meanwhile gain vision into password practices, but never at the expense of the privacy that individual users seek in the first place.

1 "2017 Data Breach Investigations Report, 10th Edition." Verizon, 2017.

2 "2017 Ponemon Institute Study Finds Huge Target for Hackers." PR Newswire, September 2017.

Devolutions

Devolutions Server

TechTarget | Custom Media

WHAT IS A SECURE VAULT?

In brief, a secure vault is a repository that allows both individual employees and teams of workers and associates to centralize passwords and digital credentials in one place. As an all-in-one solution designed to streamline password management, a secure vault is a key element of a comprehensive password management solution. Using a secure vault enables the management of user security rights and access; reduces help desk support calls (up to 50% of which are related to password resets); and greatly bolsters overall network security by generating near-bullet proof, unique passwords that users don't need to remember.

Most importantly, a secure vault allows individual end users to be issued accounts that are specifically for their own personal use, such as accessing social media sites or other servers, and a separate account for all business-related usage. IT administrators get the much sought after vision into the password habits and usage of individual employees. A secure vault may not necessarily allow these administrators to see or know the actual passwords being used. But at a minimum, they can tell whether the passwords are strong, or whether employees are using the same passwords over and over again for different access and authentication.

Thus, a secure vault is effectively a two-for-one solution giving end users the freedom and privacy to maintain their own passwords and credentials while at the same time giving IT and administrators the password management they seek across the entire organization.

SECURE VAULTS NOT JUST FOR PASSWORDS

Secure vaults are not only great for generating and storing passwords, but they are also an ideal location for storing just about any digital credential. Included among these are credit cards and the various user names and passwords associated with them; alarm codes; software keys; email account information; and certificates and associated key material such as those stored in PKCS#12 and PKCS#15 (which defines an archive file format for storing many cryptography objects as a single file.)

SECURE VAULTS, THE PERFECT BITCOIN STORAGE SOLUTION

The cryptocurrency Bitcoin has come a long way since, in 2010, an early user bought a couple of pizzas from Papa John's—one of the first known commercial transactions using the then-nearly valueless currency. The cost was 10,000 Bitcoin. Today, Bitcoin prices fluctuate wildly between $7,000 and $20,000 apiece, attracting millions of small investors. And as a Bitcoin is really nothing other than an IP address, anyone in possession of that IP address can use the Bitcoin associated with it. Thus, questions of where and how to store Bitcoin abound.

Some are stored in electronic wallet files, which contain a private key for a specific Bitcoin address. However, even if the wallet file is encrypted, the security of the information stored in the wallet file could be compromised if a weak password is used. There are online wallet service providers, too. But they may well not be very secure because the private keys for online wallets are accessible to the operators of the online wallet service. Not only that, but they are also high value targets for hackers. And some people just write down or print out the IP addresses, which has obvious potential problems.

By contrast, many users are discovering the relative safety of storing Bitcoin in a secure digital vault. They offer the convenience of an online wallet with the security of an offline system, like a safe or bank safety deposit box for storing hard copy of private keys. Getting to the keys is as simple as logging into the vault, attaching the wallet file as an attachment to a secure record, and that is that. It takes less than a minute.

WHY EVERY ORGANIZATION NEEDS A COMPREHENSIVE SECURE VAULT PASSWORD MANAGEMENT SYSTEM

Many organizations today have their own systems and means for managing internal passwords. They often use single sign-on vendors and cloud access security brokers to manage employees' access to online sites and services. But very often these solutions do not cover all accounts employees use for work. And few cover what employees are doing to manage access to personal sites, such as social media. This is particularly risky given the tendency of many employees to reuse the same passwords, resulting in business credentials winding up being the same as those used on random websites.

According to one major study, 56% of organizations had no single sign-on available at all.[3] What's worse, SMBs seldom have the money to afford such a solution. The study found further that of the top domains employees typically use in the workplace, 50% or more are popular personal solutions. There is clearly a need for a comprehensive solution that unites the personal uses of employees with their work as business users, and that solution is a secure vault.

WHAT TO LOOK FOR IN A SECURE VAULT SOLUTION

With multiple vendors selling various secure vault solutions, there is some confusion among individuals as well as businesses as to what to look for in the 'right' solution. Below are several criteria inherent in a comprehensive secure vault solution.

- An interface for end users and sysadmins that is demonstrably user friendly, intuitive and powerful
- True ease of deployment and ease of integration into most any business IT environment
- Supports a broad array of mobile devices for ubiquitous access to the vault
- Encryption approved by the highest authorities, such as the Federal government
- Ability to easily import into the vault the credentials currently in any number of free password management solutions tailored for individual users
- Ability to manage virtually all digital credentials (bank and credit card information; alarm codes; software keys; email account information; cryptocurrency IP addresses, and so on)
- Ability to manage documents as attachments or secure notes
- Allows for seamless yet highly secure sharing of data entries and passwords among multiple users
- Automatically fills in Web forms

A SMART SOLUTION FROM DEVOLUTIONS

The **Devolutions Server** from Devolutions offers individuals and entire organizations a powerful, streamlined, all-in-one password management solution. It allows individuals or an entire team to centralize passwords and digital credentials into a single, highly secure repository. In doing so, the Devolutions Server allows for simplified management of user security rights and access while reducing help desk calls and strengthening overall network security in generating only very strong passwords. A hallmark of the Devolutions solution is its highly intuitive and easily customizable dashboard.

Other features of the Devolutions Server include:

- U.S. Government-approved encryption
- The ability to reduce help desk calls by 25-40%, given the number of such calls today seeking password resets or other lost password help
- Capability to import passwords and credentials from a broad spectrum of password management tools favored by individuals
- A highly intuitive interface appreciated by individual users and system administrators alike

With Devolutions Server, Devolutions provides a highly secured vaulted password management solution that can control access to your privileged accounts, while also improving overall network visibility for sysadmins and providing a seamless experience for end users.

Click here for more information on Devolutions and its unique secure vault solution.

3 "Most IT Execs Have Zero Control Over Password Hygiene." Infosecurity Magazine, January 2018.