Devolutions

Why Passwords Haven't Disappeared Yet & What Organizations Should Do About It

MASSIVE DATA BREACH BREAKS DUE TO WEAK PASSWORDS

123456. Qwerty. Iloveyou. No, these are not exercises for people who are brand new to typing. Shockingly, they are among the most common passwords that end users choose in 2021.

Yes, you read that correctly: in 2021. We are not talking about the dawn of the web in the late 1980s, when people were donning their ultra-cool Sony Walkman. We are talking about 2021, when news of yet another massive data breach breaks on what seems like a daily basis — and 81% of them are due to weak passwords.

And so, this begs the question: Is it time to get rid of passwords once and for all? While the vast majority of IT and InfoSec professionals think this is the way to go, a recent survey found that 85% of them believe that it won't happen in the foreseeable future. Why? Because despite their faults, passwords are highly versatile. They can be used on any device, from any location, and at any time. And at the moment, in most organizations — and across virtually all small and midsize businesses (SMBs) — the infrastructure to support an entirely passwordless landscape does not exist.

Furthermore, old habits die hard — and for billions of people around the world, choosing and using passwords is something they have done for decades. They are familiar with this process, and suddenly switching to a password-less reality would be disconcerting and disorienting. In an interview for WIRED, Andrew Shikiar, the Executive Director of the FIDO Alliance, commented on this dynamic: "It's a learned behavior — the first thing you do is set up a password. So, then the problem is we have a dependence on a really poor foundation. What we need to do is to break that dependence."

But how are organizations supposed to do this? Especially when, as noted earlier, the infrastructure is not in place to support a seamless passwordless user experience? A growing number of experts are advising organizations to take a hybrid approach that significantly reduces the risk, even if it can't eliminate the vulnerabilities rooted in passwords. A hybrid approach is also much more feasible for most organizations since it does not require a complex and costly infrastructure overhaul, as it supports a mix of legacy on-premise systems and private or public cloud-based services.

How a Hybrid Approach Works

In a hybrid approach, accounts — which are tied to the organization's Identity Provider (IdP) — are used to authenticate to a Privileged Access Management (PAM) solution. This enables users to connect to accounts for standalone non-federated assets (e.g., printers, network equipment, specialized machines, etc.).

With a hybrid approach, users only need to know a single password: the one for the IdP. The PAM solution facilitates access to all other accounts. More advanced PAM solutions also allow users to connect to accounts without divulging passwords, which elevates security even more. Advanced controls can also be put in place to limit account access, such as access request requirements and time-based usage (i.e., once users are given permission to access an account, they must do so within a specific time or else the permission will expire).

The Future of Passwords

Eventually, passwords will enter the dustbin of history, and future generations will not be able to comprehend how their ancestors relied on a combination of words, numbers, and symbols to access accounts and devices. In

fact, this passwordless reality may be closer than most people think: Gartner predicts that in the coming months, 60% of large and global enterprises, and 90% of midsize organizations, will implement passwordless methods in more than half of all use cases.

But for the present, passwords will continue to play a significant role across the workplace environment. Adopting a hybrid approach is a strategic, pragmatic, and cost-effective way for organizations to reduce the size of their attack surface, and ultimately lower their security risk. And considering that the average cost of a data breach has surged to $4.24 million (USD) per incident, finding intelligent and sustainable ways to reduce the risk is not just a best practice. Considering what is at stake, it is a fundamental requirement.

How Devolutions Can Help

If your organization is looking to implement a hybrid approach for password management, then Devolutions can help!

Devolutions Server, which is our full-featured, on-premise shared account and password management solution with built-in privileged access components, integrates with Microsoft Active Directory and Microsoft Office365, in order to authenticate each user's unique identity. Devolutions Server also uses rich role-based access control settings (RBAC) to grant permissions based on group membership, thereby enhancing security while reducing administrative burden.

In addition, Devolutions Server pairs seamlessly with **Remote Desktop Manager**, which uses account brokering to inject passwords when users launch remote access technologies; this means that passwords are never exposed.

And if your organization adheres to (or wants to implement) a zero-trust model, you can add the **Devolutions Gateway** component that routes all connections through a secure tunnel. This prevents lateral movement, as it eliminates authentication token re-use across the infrastructure.

Learn More

- Schedule a live demo of Devolutions Server.
- Try Devolutions Server free for 30 days.
- Contact our sales team with any questions : sales@devolutions.net | +1 844 463.0419