

Password Reset: the Time Vampire of the IT Universe

Passwords Are Dead? Really?

If you were to search for recent articles on passwords, you would find that the majority of them are focused on new methods of credentialing. They treat passwords as if they were already a thing of the past. Everyone, from analysts to the media, is turning their attention to sexier topics like multi-factor authentication and biometrics. Even at Micro Focus, we're guilty of declaring passwords dead.

Despite the avalanche of articles to the contrary, passwords are still one of the most important authentication methods. Take a moment and think about the systems that you log on to—for work, social media, banking, financial and so on. Do any of them use a form of authentication other than passwords? Then think about any major security breach in the news. There's a good chance it resulted from some kind of stolen credentials, involving a password. The truth is passwords are still very much a part of our daily lives.

The reasons we're all so keen to move beyond passwords are simple. They're either insecure or they waste time—or both. Security can suffer because users often have poor password hygiene: they write them down, use the same one for everything, or choose an obvious phrase because it's easy to remember. In an effort to increase their security, organizations can implement password policies that require frequent changes with a high degree of password complexity and uniqueness. But this increase in password difficulty is usually an



organizational time waster because users forget the password they chose and then call IT to reset their password, impacting both their own productivity and the productivity of the help desk. In fact, anecdotal evidence suggests that between one-sixth and one-third of all help desk calls still focus on passwords.

Making Passwords Self-Service: a Quick Win for Everybody

In today's era of ROI, everyone is expected to keep productivity high and limit wasted time. Given the emphasis on ROI, it may come as a surprise that many organizations overlook a relatively simple means of saving time and money. According to Gartner, calls for basic password resets can constitute 20% or more of calls to the average service desk, making self-service automated reset an obvious choice to reduce service desk call volume and costs.



Choose the Right Solution:

There are quite a few solutions out there, and picking the right one can be a real challenge. Evaluate your choices and look for options that:

- Are truly self-service—the system should reset the password without any IT intervention.
- Allow users to change the password for all the systems they use in a single interface.
- Enforce password complexity requirements across all systems.
- Allow ample tools and options for end-user verification, like challenge-response questions.
- Work on modern mobile platforms and embrace the dynamic and changing nature of remote access.

