# Identifying the security gap in authentication

David Peters, Technical Director, ANSecurity

A big hole in many security frameworks is the user and specifically authentication. Weak passwords and broken credentials are a very real threat and as organisations adopt more cloud services the risk of exposure grows.

Although most people are loathed to admit it, many surveys show that users still keep insecure, or easy to guess passwords which they use across multiple platforms. This has been further validated by leaked passwords from recent hacks of popular online platforms that indicate the same. Even with well enforced strong password policies, some enterprise users still gravitate towards easy to remember, and often easy to guess passwords that are the quickest path for a password that meets the requirements, for example "Password123."

Password theft is also commonplace which means using the same password on multiple platforms becomes a major vulnerability. If a 3rd party social media or online community platform is compromised for example via a phishing, social engineering, malware or hacking attack, this seemingly unrelated to work event can ultimately compromise workplace credentials. The best way to mitigate these risks is to use multiple factors of authentication, a technology presently evolving at a very fast pace with the proliferation of SaaS and cloud platforms to which protection needs to be extended.

Authentication protocols such as SAML offer standards based methods of extending enterprise authentication services, including strong and multi-factor authentication to SaaS platforms. Reducing complexity for the user, ensuring standardised authentication strength for all corporate assets whether on-premises cloud or hybrid and easing administrative burden when revoking credentials.
It is often overlooked but enterprises should be considering options such as federated authentication, protocols used and integration with existing or future multi-factor authentication solutions when evaluating, amongst others, SaaS, Cloud or Remote Access solutions.

Careful consideration about the type of additional factors of authentication used should be taken, the options are wide and varied, each with their own security, complexity and cost considerations. SSL Certificates, Physical tokens, Software tokens, Mobile devices, One Time Passwords (OTP) and the chosen delivery mechanism to name just a few.

Additionally care should be taken around the hardening of authentication platforms, after all locking the castle keep, but leaving the keys lying around won't do! The choice between on-premises or cloud based authentication services also raises many important points and there is generally no 'best' option – it depends on the use case.

Remember you're not alone. Talk to a dedicated security expert who can help clarify the role of integration and well architected solutions that reuse the existing systems and build in new capabilities to deal with today's authentication challenges. The best advice is to consider solutions with sufficient flexibility and scalability to stand the test of time with the fast evolving hybrid IT and cloud.

*The author: David Peters has worked in the IT industry for over 20 years. Initially working on large global email solutions David began specialising in security following the unprecedented growth of email borne viruses that emerged in '99 and 2000. David has been Technical Director at ANSecurity since 2003 David has been closely working with a multitude of security vendors and clients in many industries to help provide the best security possible.*