Top 5 Reasons to Unify Your Microsoft Credentials

Azure AD is Microsoft's preferred identity provider for the cloud and slated to replace the on-premises offering – Microsoft AD – over time. Windows Hello for Business is a credential that leverages a PIN or a biometric. However, these powerful identity components are siloed. Here are the Top 5 reasons to unify your Microsoft credentials.

1 Improve the end user experience significantly

A recent study concluded nearly a third of workers in the 18 to 24 age range have tried to circumvent security controls due to the perception that they "wasted time".[1] Azure AD, Microsoft AD, and Windows Hello for Business credentials should be unified into a single, efficient and ideally passwordless authentication approach. This approach would save end users a significant amount of time, minimize security bother, and prevent circumvention of security.

2 Expedite migration to Azure AD and efficiently run hybrid on-premises and cloud

Azure AD is embracing Certificate-Based Authentication (CBA) that is a different infrastructure than previous Azure AD and Microsoft AD approaches. Having up to three authentication infrastructures is difficult to manage and expensive. A unified authentication approach would speed the migration to Azure AD and enable efficient hybrid operations for as long as needed.

3 Map group and user need to the appropriate authentication level

With siloed authentication, end users in the same group either have different authentication methods or must use multiple authentication methods based on the confidentiality of the task or information. With a unified authentication approach, a single authentication process could adapt to the confidentiality of the task. The net result is higher security, less friction.

4 Enable efficient management due to capabilities for codifying authentication lifecycle

Password-reliant Multi Factor Authentication (MFA) loses programmability due to having user dependencies in the stream. With passwordless authentication, the entire authentication process – and the entire lifecycle – can be programmed. This enables the development of efficient, programmatic management tools and workflows.

5 Get more life out of existing Microsoft investments

As Microsoft solidifies Azure AD as the backbone of its offerings, organizations may need to replace most if not all of their existing Microsoft-based authentication approaches. A unified authentication approach ensures that existing investments in Microsoft AD and Windows Hello for Business can be supported efficiently for some time. This freedom both gets more life out of existing investments and improves security by eliminating siloes and gaps.

Learn more about authentication best practices in our blog.

[1] Townsend, Kevin, "CISOs Faced With Friction, Resistance From Remote Workers Over Security Controls", Security World, 9/13/21.