TOP 10 REASONS TO LEVERAGE A FEDERATED IDENTITY SOLUTION WITH OFFICE 365

Microsoft's cloud-based productivity suite, Office 365, is quickly replacing on-premises solutions. Businesses welcome the easy access it provides to corporate resources, regardless of user location or device, but managing that access for a large, dispersed workforce can get pretty complex. To address this challenge, Office 365 offers the option to implement federated identity solutions that simplify management and leverage authentication controls such as single sign-on (SSO). Here are the top 10 reasons to implement a federated identity solution with Office 365.

#1

CENTRALIZED ADMINISTRATION: Identity management and user authentication can get chaotic in mixed environments with on-premises and cloud-based resources. By leveraging federated identity solution support in Office 365, you can set up a single administration interface for user authentication, identity federation and directory synchronization. Regardless of where users seek access to corporate resources, everything is controlled from a central location.

#2

COMPLETE VISIBILITY: Centralized management is a proven remedy for complexity. It keeps things simple and gives administrators visibility across the entire identity landscape from a single pane. This demystifies identity management while plugging security holes that tend to occur when resources aren't centralized, and instead, run from different administrative dashboards in multiple locations.

#3

FEWER PASSWORDS: Most users have forgotten passwords at one time or another. In the past, this would trigger a helpdesk call for a reset. But even though resets are mostly automated now, users are required to remember too many passwords—typically somewhere around 201. This causes frustration and hurts productivity. A federated identity solution enables SSO for all your applications, on-premises and in the cloud, allowing users to remember only one password for all of their applications, websites and systems.

#4

IDENTITY STORE COMPATIBILITY: Businesses sometimes resist IT upgrades because they fear compatibility issues with existing resources, which can lead to further expenses. With a federated identity solution, there's no need to fear. You synchronize your existing directories with Azure AD, so you don't have your identities stored in multiple places with multiple passwords. This interoperability adds administrative convenience, eases user adoption and helps eliminate costly password resets.

TOP 10 REASONS TO LEVERAGE A FEDERATED IDENTITY SOLUTION WITH OFFICE 365 (CONT.)

#5

MULTI-FACTOR AUTHENTICATION: You can add an extra layer of security to identity management with multi-factor authentication (MFA). This requires users to confirm their identity by providing additional data (factors) through a mobile app, hard token or one-time passcode delivered via text message or email before accessing an application or website. A good MFA approach adds security without adversely affecting usability.

#6

HYBRID APPLICATION SUPPORT: Many organizations are choosing to deploy applications in a hybrid public and private cloud environment while also leveraging SaaS applications. A federated identity solution not only centralizes identity management but also lets you control authentication and authorization for resources regardless of where they're hosted.

#7

SIGN-ON AUDIT: Keeping track of who is accessing which applications, websites or services is a challenge when managing a dispersed workforce. You need audit capabilities to determine when a user's account is at risk or has been compromised. With a federated identity solution, you can audit sign-on activities and immediately disable accounts if an unauthorized user seizes them, or when someone leaves the company or moves to a different position.

#8

LIFECYCLE MANAGEMENT: A federated identity solution supports lifecycle management for all of your user identities and authentication protocols. This includes onboarding and offboarding users as well as the enforcement of password policies that control when passwords are issued and reset. It doesn't force you to replace or change existing identity policies. It just gives you a better way to manage and automate them.

#9

STRONGER POLICY ENFORCEMENT: Some businesses need to restrict access to critical assets based on user location, business hours and other criteria. A federated identity solution lets you manage access restrictions based on the client in use, whether users are within or outside network walls when signing on, or whether they try to do so during off hours. An advanced federated identity solution also lets you manage access according to rules such as user role and group privileges, ensuring your organization remains compliant with both corporate and industry policies and regulations.

#10

SUPPORT FOR OPEN STANDARDS: A federated identity solution is built on and leverages open standards such as SAML (Security Assertion Markup Language) and OpenID Connect. SAML is the gold standard for providing users with SSO to web applications. OpenID Connect is the next-generation standard that builds on OAuth 2.0, providing authentication and access management for web, mobile and APIs.