An Office in the Clouds

Jay Kelley, 2016-21-09

Microsoft Office is one of the most deployed and widely used business productivity software suites ever. It remains core to businesses worldwide despite increasing competitive pressure from a host of “born-in-the-cloud” SaaS productivity solutions to replace it.

Office has been available as a service for some time in the form of Office 365. Over the past couple of years, Microsoft has made huge leaps forward in the functionality, security, and management capabilities of Office 365. This has led businesses all over the world to make the leap from the relative comfort of the on-premises solution to the cloud-based offering. All signs point to Microsoft retaining its business productivity leadership mantle as Office 365 momentum in the enterprise continues to accelerate at a record breaking pace.

But why?

Some organizations migrate to Office 365 because of user familiarity with Microsoft Office applications. This familiarity limits the need for training, help desk calls, and more; that saves time and expense.

For others, it's that Office 365 enhances collaboration, regardless of where users are in the world, through cloud-based, market-leading solutions like SharePoint Online and Skype for Business. Office 365 makes it easier for co-workers to share information and content while working in real time across locations and devices.

For many organizations, it's a simple fact that Microsoft Office 365 increases user productivity. Office 365 enables users to work anytime, anywhere, from nearly any device. This ability helps the organization as well as the user, since they no longer need to be tethered to a desk, an office, a hardwired network connection, or even their own data center. They can finally have that office in the cloud.

As with anything, though, there are challenges.

One of the first challenges an organization is likely to confront once they decide to migrate to Office 365 is to determine the best architecture and deployment model to meet (and hopefully exceed) the needs of their users and organization. Should they move completely to the cloud? Or, alternatively, would a hybrid solution be the best approach, with the organization maintaining some Office functionality on premises, such as Microsoft Exchange and user email, while implementing Office 365 for anytime, anywhere user productivity.

Companies also need to find the right balance between usability and security. As organizations migrate to Office 365, their control over data—even critical and sensitive data—can be diminished. Their data is now traversing back and forth to the cloud from user devices that may be anywhere over nearly any network, including insecure public Wi-Fi.

One constant challenge, though, is maintaining organizational control over user identity and access, the entry points to cloud-based applications. An organization may wish to enable simple, seamless single sign-on (SSO) for their users accessing Office 365 from an on-site location. However, when that same user is outside the confines of their office, an organization may want to institute a multi-factor authentication (MFA) checkpoint, based on user location, device type, connection, and other attributes, ***before*** they are allowed to access Office 365.

Microsoft offers three different identity models for Office 365:

1. **Cloud Identity** enables the creation and management of a user in Office 365, with the user’s identity stored in and their password verified by Microsoft Azure Active Directory**.**
2. **Synchronized Identity** manages user identity from an on-premises server, allowing the user to enter the password on premises, with the user account and password hashes synchronized to Office 365, where their

password is verified in Azure Active Directory.

3. **Federated Identity**, the most popular method for secure access to Office 365, is similar to Synchronized Identity, but the user password verification is conducted by an on-premises identity provider without synchronizing the password hash to Azure Active Directory. This allows secure control over user credentials. With Federated Identity, the threat of lost or stolen credentials is mitigated, and integration with new or existing MFA methods is greatly simplified.

One of the main reasons for the popularity of Federated Identity is that most organizations are very reluctant to share their user credential store—essentially the keys to an organization's identities, and therefore data—outside of the organization and its secure data center. Most organizations feel the need to maintain complete control of their users' credentials. They would much rather manage user identity from an on-premises server and even avoid sending hashed user account data and passwords outside of their secure perimeter. They would rather opt to have users' passwords verified by an on-premises SAML identity provider (IdP), such as a third-party IdP, or Microsoft Active Directory Federation Services (ADFS).

Stay tuned for our next blog on Office 365, which will discuss whether Microsoft ADFS is the right IdP for your organization, and learn more about securing Office 365 access with F5

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | wwww.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com