WHITEPAPER

SECUREAUTH IDP AND OFFICE 365
STRONG AUTHENTICATION AND SINGLE SIGN-ON
FOR THE CLOUD-BASED OFFICE SUITE
EXECUTIVE OVERVIEW

As more and more enterprises move to the cloud, it makes sense that Microsoft would choose to follow them. The corporation has established a new environment in which users can access the well-known and frequently used Office programs (Word, Power Point, Excel, Outlook, etc.) onto the cloud: Office 365.

Users from any device and in any location can utilize Office 365. Enterprises no longer need to manage exchange servers or apply thick clients to individual computers – all applications are web-based and hosted by a virtual server controlled by Microsoft. This enables an easier workflow and less hassle for the company.

The new Office 365 was created to improve the Microsoft experience and alleviate burdens from the enterprise, but with it come new security risks. Applications on the cloud are inherently less secure than internal or network applications because they are out of the company’s control and can be accessed by any external user. In situations like this, enterprises need to rely on more than just a username and password and require a way to regain access control, even if the application is in the cloud.

This white paper will discuss Office 365 from its history to its current standing. The requirements of enterprises due to the faults of the Office 365 model will be examined and the best system for securing the application will be introduced: SecureAuth IdP. The many features and merits of SecureAuth IdP will be exposed, demonstrating how an all-in-one, 2-Factor SSO solution is most apt for Office 365.

TABLE OF CONTENTS
Introduction: Microsoft Office .................................................................3
Microsoft Office to the Cloud ...............................................................3
Problems with Office 365 .................................................................5
SecureAuth IdP: The Solution for Office 365 .........................................6
Single Sign-On with SecureAuth IdP ...................................................9
Customizable Workflow .....................................................................10
Conclusion ..........................................................................................12
INTRODUCTION: MICROSOFT OFFICE

Microsoft Office was created in 1985 for Mac and expanded into Windows versions in 1990. New installments have been released every couple of years, with the latest version, Office 2013 released in October 2012.

Before migrating to the cloud, aspects of Microsoft Office encumbered some enterprises. Though the applications have come to be utilized by the majority of business today, they required extra work that was not keeping up with technology and competitors’ progress.

For example, to operate Microsoft Outlook, the user-friendly email application, companies were forced to house exchange servers that took up space and were difficult to manage. Within these servers was all of the email data from years of communication for each user. Providers began moving to the cloud to remove bulky and arduous hardware from the enterprise to ease the experience and streamline workflow.

Office programs originally required thick clients as well. These are costly, and must be purchased for every 1-5 computers and installed individually. This process severely limits the mobility of business and the freedom of Bring Your Own Device (BYOD) work environments.

Though Microsoft Office is accepted and utilized by many companies in diverse industries, the on-premise requirements and inconveniences has forced enterprises to search for alternative methods. To keep up with the competition and to provide to its customers web-based applications that can be utilized from any device without thick clients or hardware, Microsoft introduced Office 365.

MICROSOFT OFFICE TO THE CLOUD

Office 365 is a subscription-based online office suite, originally released in June 2011. It enables mobile work from numerous users and easy communication for collaboration. No thick clients or servers are required, and all business can be conducted on the cloud.
Small and midsized businesses as well as large enterprises can purchase the suite in different levels from $4.00 a user per month to $20.00 a user per month with an annual commitment. The plans cover 25 users to an unlimited amount, depending on your enterprise requirements.

Each package contains online versions of the applications where users can access the Office applications online and without installations; and some include desktop versions of Word, Excel, PowerPoint, Outlook, OneNote, Access, Publisher, and Lync for up to 5 PCs/Macs per user to enable on and offline work.

Office 365 also includes SharePoint, which enables employees, partners, and customers to work together, share documents, and keep up with the news feed within the enterprise. This is just another feature of Office 365 that improves user experience and streamlines business.
PROBLEMS WITH OFFICE 365

Though Office 365 was created to meet the demands of modern business, the changes have created heightened security risks and generated tedious requirements for enterprises.

Like with any application, moving it from the secure network onto the cloud reduces its protection. Though allowing mobile users to access the suite from any location increases convenience, enabling external access creates vulnerabilities for potential attacks.

With mobile devices, it is essential that security be increased beyond a username and password. Otherwise, an unauthorized user can access corporate resources with a compromised set of credentials.

Another major issue with Office 365 is that it requires an Active Directory (AD) in the cloud. This means that all user data, including names, addresses, passwords, and more are stored and managed on the cloud. Most enterprises have an established directory already on-premise; with Office 365, they require an additional one that resides on the cloud. Though Microsoft is a secure provider, having two data stores with confidential and serious information means that there are two areas that can be violated.

Enterprises are uncomfortable with their profile data residing outside of the network, and having to manage two separate directories is unsafe and tedious. Though Office 365 enables integration and synchronization of the cloud AD and the on-premise directory, it is through a complex process with limited flexibility: Active Directory Federation Services (ADFS).

ADFS enables the synchronization and transference of information between the directories as well as Single Sign On (SSO) from the enterprise AD to Office 365. Though it is a useful tool, the procedures are complicated and the authentication flexibility is minimal.

Office 365 needs a system that enables extended protection for external users, easy and transparent SSO from the enterprise directory, synchronization of the two data stores, and identity and access management that can be controlled internally rather than on the cloud.
SecureAuth IdP is an appropriate solution for Office 365 for numerous reasons. It can be integrated with any enterprise’s existing infrastructure, enable extended protection for mobile users, and assert identities from the network out to the cloud with one set of credentials.

SecureAuth IdP is an all-in-one solution that provides the tools to a company to become its own Identity Provider (IdP). This allows an organization to design its own security, including authentication protocols and SSO options, and to use its
already-established identities. SecureAuth IdP simply provides protected access to permitted users.

Microsoft primarily uses WS-Federation and WS-Trust for application communication. The two act as trusted languages in which applications speak to pass identities from one to another. SecureAuth IdP supports both standards, improving the integration and user experience for Office 365, SharePoint, and other Microsoft programs.

Enterprises that utilize Office 365 most likely have an internal and new, cloud-based AD. SecureAuth IdP can not only integrate with the internal AD and assert identities from there, but it can also use federation to eliminate the AD passwords stored in the cloud-based AD to alleviate the company's burden. In doing so, SecureAuth IdP protects both data stores from unauthorized external users – the internal store through strong authentication options and the external store by eliminating the data store's synchronized passwords.

By assimilating into the enterprise, SecureAuth IdP can enable employees, partners, and customers to utilize their same IDs and passwords that permit access into the network for all applications, including Office 365. Internal users can sign into the company as they already do and immediately receive access into Office 365 without additional logins or unique passwords.

Because Office 365 resides in the cloud, it is likely that employees will use their own mobile devices (laptops, tablets, smartphones, etc.). BYOD environments are growing rapidly in business, and it is no longer feasible for companies to exercise control over the device due to the cost and inconvenience that it creates. SecureAuth IdP enables mobile protection without hardware, thick clients, or enterprise device ownership, but maintains enterprise control of access.

SecureAuth IdP provides 2-Factor Authentication (2FA) for internal and external users. This process requires an extra step after entering the username and password to achieve access into the corporate applications.
SecureAuth offers over twenty different authentication methods from which users can choose:

- SMS OTP
- Telephony One-time Password (OTP)
- Email OTP
- Static PIN
- KBA/KBQ
- Yubikey (USB)
- X.509 Native
- X.509 Java
- Kerberos (IWA)
- NFC Prox Card
- CAC/PIV Card
- Mobile OATH Token (Time-based One-time Password – TOTP)
- Browser OATH Token (TOTP)
- Windows Desktop OATH Token (TOTP)
- Third-Party OATH token (TOTP)
- PUSH Notification
- Help Desk
- Social IDs (Google, Facebook, Twitter, LinkedIn)
- Federated IDs (SAML, WS-Fed, OpenID)
- Device Fingerprinting
- Password
- Symantec VIP

SecureAuth’s 2FA procedure ensures safety but does not encumber user experience. Users are navigated through the process transparently through browser and app interfaces exclusively, quickly and efficiently.

SecureAuth IdP acts a bridge from the AD to the target application. To authenticate users, SecureAuth IdP pulls information from the AD upon receiving the username. This data is held in the IdP only until the authentication process is completed. SecureAuth IdP does not retain any of this user information, which ensures its safety even if the IdP is breached.
Users that wish to access Office 365 from a mobile device would supply their enterprise username and upon recognition, would be redirected to the SecureAuth IdP page. They choose the authentication method to be used (telephony, e-mail, static PIN, etc.), insert the information upon receipt, and then enter their enterprise password. If all of the information collected by SecureAuth IdP matches the data pulled from the enterprise AD, then the user is authenticated and redirected back into Office 365 for use. This all occurs securely and without friction.

**SINGLE SIGN-ON WITH SECUREAUTH IDP**

Systems including ADFS enable SSO from the enterprise AD to Office 365, but the process is more complicated and less effective than SecureAuth IdP SSO.

Due to the ability to integrate with and synchronize the two data stores, SecureAuth can assert authenticated identities to Office 365 as transparently as its 2FA and from any device. No coding is required to enable SSO; administrators need only set preferences through drop-downs in a GUI console.

Not only can SecureAuth IdP assert identities to Office 365 via WS-Federation and WS-Trust, but it can also assert the same identities into other applications that communicate differently, such as with SAML.

SecureAuth IdP includes Security Token Services (STS), which accept the identity and then translate it into appropriate artifacts (WS-*, SAML, etc.). Many application protocols are supported by SecureAuth IdP, facilitating access into thousands of applications with one username and one password. For Office 365 users, this means that not only can SecureAuth IdP provide frictionless SSO from...
the enterprise AD into Office 365, but also SSO to other network, web, cloud, and mobile applications, including *native mobile apps*.

SSO with SecureAuth IdP is simple to apply and to use. Users are no longer burdened with the responsibility of remembering numerous, unique passwords that they will inevitably lose or forget. Just one set of credentials can enable access into all enterprise resources, and with 2FA, companies can confidently assume that the access is being granted to only authorized users.

**CUSTOMIZABLE WORKFLOW**

SecureAuth IdP provides infallible protection and also strives to maintain a friendly user experience. Not only are the 2FA and SSO processes completely transparent and require no coding, Identity Access Management (IAM) is enabled with SecureAuth IdP that allows enterprises to create the workflow that their users undergo.

2FA is enabled specifically for mobile users; however, if the organization so chooses, 2FA can be required for all employees, including those in the office. Admins can determine the time duration of an authentication registration to eliminate the need for subsequent authentication. This period is determined by the company and can be anything: one session, one day, one month, three months, etc. SecureAuth IdP also provides 1-Touch Revocation, which enables an admin to expire a user or device authentication at any point with a single-click action.

Step-up authentication is also available with SecureAuth IdP, allowing the enterprise to make the authentication easier or more difficult based on risk factors. If the company wishes, 3-Factor Authentication can be applied for specific users or applications; or simply 1-Factor Authentication (username/password) can be the only requirement. Authentication preferences can be set based on users, access groups, applications, or devices individually.

A revolutionary mechanism included in SecureAuth IdP’s workflow is **Device Fingerprinting**. Mobile users that register their identities on their personal devices can link those devices to their enterprise profile after one authentication to remove subsequent authentication. Each mobile device that is used by the
user is logged and connected to him/her, and future use does not require 2FA within the allotted time duration. This also enables quick revocation if needed, as admins can look up devices by user and swiftly remove the authentication.

SSO can also be determined based on individual aspects, and can be modified at any time.

Because SecureAuth IdP integrates with the AD, profile management is also simple and effective. All profile changes can be made in the admin console, including removal. By simply disabling the user’s profile, all access and allocations are immediately ceased so enterprises need not stress about previous employees’ continued access. All access control remains with the company internally, rather than on the cloud.

SecureAuth IdP also enables user self-management, which includes profile registration and modification, password reset, and self or device revocation. Companies save hundreds of thousands of dollars a year with self-password reset. Users can recreate their lost or compromised passwords quickly and without any assistance, which saves the enterprise time and money that was previously wasted.
With SecureAuth IdP, organizations that utilize Office 365 can continue to use their ADs (enterprise and cloud-based) and enterprise identities without complicated transfer/syncing processes, implement 2FA to ensure secure mobile access, assert identities through SSO to Office 365 and other applications, and manage profiles and control access through a simple-to-use SecureAuth admin console. Companies can work on Office 365 through SecureAuth IdP without any hardware, thick clients, coding, or third-party tools to produce a streamlined and effective workflow.

**CONCLUSION**

Office 365 has enabled enterprises to move their business onto the cloud with the same applications and programs that they already know and utilize. And with the inclusion of SharePoint in the suite, users are able to collaborate from any device more than ever.
Moving applications to the cloud improves user experience but also heightens security risks. By allowing users to access the corporate resources virtually, unauthorized users could achieve access with compromised enterprise credentials. Companies require a solution that protects their data without sacrificing user experience.

SecureAuth IdP works best for Office 365 due to its safeguarding capabilities and its focus on user experience. The solution integrates with the enterprise AD and can synchronize it with the cloud-based data store, provides frictionless 2FA for external users, and enables transparent SSO from the enterprise out to Office 365 and other network, web, cloud, and mobile applications.

SecureAuth IdP is easy to configure and can be designed to create a streamlined workflow based on risk and accessibility. With easy-to-use IAM tools and user self-management, controlling access without impeding the end-user experience is accomplished. No hardware, thick client, or coding is required by the enterprise so the Office 365 experience can remain completely virtual.

Office 365 enables companies to continue conducting business without being burdened by exchange servers or installations, and employing SecureAuth IdP to protect corporate resources maintains that same convenience.