cpl.thalesgroup.com

THALES
Building a future we can all trust

Protecting O365 and Microsoft Environments with the Thales OneWelcome Identity Platform

White Paper

Contents

Abstract

Organizations are on a cloud migration journey. Many organizations that have implemented various on-premises Microsoft solutions, such as Office suite and AD FS, are now migrating some of these Microsoft solutions – primarily Office 365 – into the cloud. Security of these cloud-based services is of the utmost importance. In this white paper, we'll discuss how OneWelcome Identity Platform, Thales's cloud-based access management and authentication service, can help your organization protect your Microsoft cloud-based services and scale securely in the cloud.

Introduction

Enterprises are abandoning traditional business models and adopting digital transformation at a fast pace. Corporations are moving to cloud, multi-cloud and/or hybrid cloud environments. The adoption rate of cloud applications has been dramatic in recent years, with organizations of all sizes moving to cloud-based delivery models.

While originally it was business needs, such as omnipresence and customer engagement, that pushed towards cloud adoption, nowadays IT services are being migrated to the cloud propelled in large part by the large cloud service providers such as Microsoft, Google and AWS. The majority of orgnizations have already moved their office suite and mail servers to the cloud, adopting Office 365 to cater for new ways of working and enhance employee collaboration. Often, they expand further their cloud footprint by migrating other core IT functions, such as engineering workloads and directory servers.

Despite the growth in adoption of Office 365, use of Microsoft's on-premises Office servers remains almost unchanged. Companies migrating to Office 365 continue to operate in some form of hybrid environment consisting of SaaS such as Office 365, IaaS services such as Azure AD or AWS, and on-premises applications.

As enterprises embrace cloud applications to transform how they collaborate, security is clearly a top concern and businesses worry that it may be a matter of time before something happens to their tenant. As a result, their IT teams are seeking streamlined methods of centrally defining and enforcing access controls to manage security and compliance in a consistent manner across their cloud and on-premises applications.

Access Challenges in Cloud Environments

Leveraging cloud-based applications, such as Office 365, comes with its share of challenges. Indeed, the FBI's 2019 Internet Crime Report has identified Business Email Compromise as one of the year's hottest fraud topics, noting that IC3, its fraud recovery unit received close to 24,000 complaints involving losses of over $1.7billion[1].

Perimeter Security Offers No Protection

This data underlies the fact that by adopting Office 365, users are now accessing the organization's most sensitive resources remotely and beyond the traditional perimeter security. Many organizations secure VPN remote access, but the reality is they haven't moved beyond the concept of "perimeter security".

Login Page is Completely Exposed

Login pages providing access to an organization's critical assets that were once protected within the organization's DMZ or behind a VPN, are now fully exposed to the Internet – accessible to anyone. Office 365 is becoming the platform of choice for malicious attacks. Malevolent actors can easily launch password spraying attacks to gain access to your network resources and start moving laterally to steal sensitive information or cause damage. What is more, this challenge increases the risk of phishing and Man-In-The-Middle (MITM) attacks. Most data breaches could have been thwarted using strong multi-factor authentication.

1 https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

Convenience

By default, cloud apps, such as Office 365, are only protected using weak, static passwords—a reality that jeopardizes the confidentiality of sensitive information and increases the risk of a breach. The abundance of cloud apps requires users to maintain countless usernames and passwords. They are required to authenticate numerous times every day with each application they open, and often resort to security workarounds. This leads to password fatigue—the exhaustion that results from the endless need to create, update and reset passwords for different applications.

Compliance risk

Proving regulatory compliance requires visibility into access events. IT departments need to know who is accessing what application and when. Furthermore, with sensitive data residing in cloud applications, administrators need to know how users' identities are being verified.

Leveraging cloud apps comes with its share of challenges

Mitigating Cloud-based Access Management Challenges

The real challenge is how to achieve the same level of protection that organizations had when everything was on-premise - in the cloud. That's where access management comes in. CISOs and enterprise IT departments need to simplify the life of their end users, protect their organization in distributed computing environment, and reduce the risk of identity theft with the goal of thwarting data breaches.

Apply Cloud Single Sign-On

Single sign-on (SSO) provides the capability to authenticate once and be subsequently and automatically authenticated when accessing various resources. It eliminates the need to separately log in and authenticate to individual applications and systems, essentially serving as an intermediary between the user and target applications.

Not only does SSO provide convenient and frictionless access for users, but it also makes the administrator's life easier by allowing IT to maintain just one identity per user for all cloud resources. This eliminates the hassle of password resets and the overhead required to troubleshoot users from multiple administration consoles.

Microsoft-based SSO Solutions

Most IT ecosystems are based on Microsoft, so when looking to add single sign-on, most IT departments have considered Microsoft AD FS (Active Directory Federation Services) as the default federation solution. AD FS lets identity information to be shared outside an enterprise's network. It helps reduce the log on burden for end users by assessing claims rules and providing single sign on to applications or cloud services in an organization.

AD FS is a legacy application and its integration may not be sufficient for all your SSO and cloud access management scenarios since it does not offer native MFA or conditional access. Organizations would have to rely on third-party capabilities to implement MFA and policy-based access.

While some organizations who have a more mature cloud model have started migrating their on-premises Active Directory stores to the cloud by adopting Azure AD, many customers are opting to purchase a separate Access Management (AM) platform due to the gaps in functionality for support of non standards-based applications. This is mostly due to the Azure AD focus on cloud environments, which leaves organizations struggling to address on-premises and non-Windows access use cases.

Whether an organization is using Active Directory combined with AD FS for federation services, or has moved partially to Azure AD, a key consideration is how to protect Office 365, non-Microsoft cloud services and on-premises applications with next generation access management, SSO and authentication. As such, IT teams need to take a proactive role in understanding their security risks and take active measures to mitigate them.

Factors to Consider when Assessing an IDaaS Solution

There are several points that CISOs may want to consider when assessing how to best protect their Office 365 tenants.

Considerations in Assessing an SSO Solution	
#1 User Convenience	Does the solution add low friction to user or customer authentication? Can they choose the type of authentication tokens they want?
#2 Security	What assurance levels does your prospective solution offer in terms of multi-factor, conditional and continuous adaptive access?
#3 Cost of ownership	When you calculate the total costs of a solution, do you consider the real hard and soft costs such as licenses, infrastructure, maintenance and consulting? What features does the subscription include?
#4 Administration and set up	What automated workflows, templates and wizards does the prospective solution offer to save you time and effort when provisioning authentication tokens and setting up and maintaining access policies?
#5 Support for your IT environment	Does the solution integrate easily into your IT environment? Can it protect on-premises applications as well as non-Microsoft cloud services? Can it address all use cases?

Protecting Microsoft Cloud-Based Environments with OneWelcome

Enterprises need access management and MFA for Microsoft apps and other cloud services as well as their on-premises applications.

OneWelcome is a cloud-based access management and authentication service that is flexible enough to secure your organization's Microsoft architecture in different ways depending on the deployment architecture and preferences. OneWelcome offers a range of access management and authentication capabilities that fit into varied IT architectures:

- Direct integration with AD FS providing conditional access and MFA for on-premises and cloud services
- Direct integration with O365 via SAML, providing policy-based access and MFA for Office 365, on-premises apps as well as SaaS, PaaS and IaaS services
- Direct integration with Azure AD to secure Office 365, on-premises apps as well as SaaS, PaaS and IaaS services with third party multi-factor authentication=

Scenario 1: Integrating with Existing AD FS Environment

Many organizations are using AD FS as a federation server to bridge Office 365 and Active Directory on-premises. While Microsoft is promoting its cloud services, the reality is that many organizations are still using AD FS and it will likely take a long time for businesses to do away with AD FS.

Integrating OneWelcome with your existing AD FS architecture can benefit organizations by applying flexible access policies and MFA to all their applications, whether they are Microsoft ones, such as Office 365, or non-Microsoft cloud and on-premise applications. Hence, OneWelcome will give organizations, who have AD FS, the ability to offer conditional access combined with MFA. This solution is ideal for organizations who are heavily invested in AD FS but would like to add next-generation policy-based access, conditional access and MFA to their on-premises and cloud services.

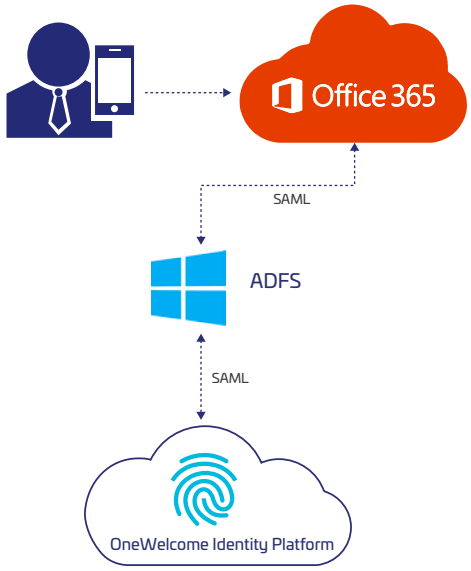


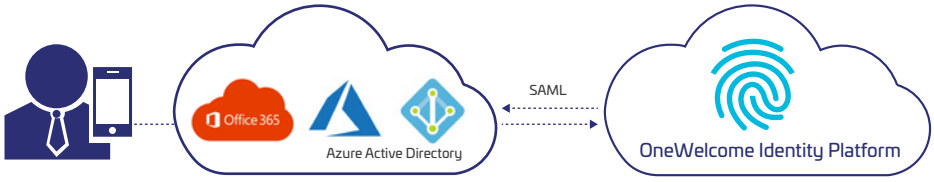
Table 1 below will help you assess the benefits of integrating the OneWelcome Identity Platform with your organization's AD FS architecture.

	OneWelcome	Microsoft AD FS
Single Sign-On	Administrators apply conditional access and different levels of authentication based on the use case. Step up authentication is triggered by the policy.	Offers basic SSO capabilities with no control by IT once the session is opened.
MFA Options	OneWelcome offers a broad range of MFA options including push notifications, hardware tokens, SMS, pattern-based authentication, and PKI credentials, as well as adaptive and risk-based authentication.	AD FS does not include MFA at all and requires the customer to purchase Azure AD license or a 3d party MFA.
Conditional Access	OneWelcome offers conditional access policies based on network, device, location etc. Policy set up is intuitive and user-friendly	AD FS does not support conditional access. Policy configuration uses program scripting and, thus, policies are complex to set up and to update when needed.
Reporting	OneWelcome provides immediate visibility and reporting into who is accessing which application, and how, which is important for achieving regulatory compliance.	AD FS offers limited reporting and visibility into who is accessing what, when and how.
Total Cost of Ownership (TCO)	OneWelcome offers combined access management and MFA with multiple tokens included – including hardware tokens. There is no need for additional infrastructure investments. OneWelcome is scalable to additional applications at no extra cost.	AD FS requires a big investment in on-premise infrastructure plus additional servers for redundancy. Dedicated personnel are required for deployment and ongoing administration and maintenance. Additional Microsoft licenses are required for MFA and additional costs for hardware tokens.

Table 1: AD FS vs OneWelcome Identity Platform Overview

Scenario 2: OneWelcome Provides 3rd Party MFA to Azure AD

In this scenario, OneWelcome integrates directly with Azure AD and acts as a 3rd party MFA provider. Access management is handled by Azure AD. MFA provided by OneWelcome supports use cases that Azure AD does not, such as Windows Logon or MFA integration for on-premises and non-standards-based applications. In addition, OneWelcome offers hardware tokens not supported by Azure AD for use cases that cannot use mobile phones or pattern-based authentication for contractors. This implementation enables your organization to offer your users a unified authentication experience and a single authentication token for Office 365, Windows Logon, IaaS, PaaS and SaaS services.



OneWelcome provides a powerful MFA solution, as MFA is applied universally and managed centrally for all applications. As a result, it saves the organization from having to deploy different MFA solutions for different use cases. This efficiency adds to the overall user experience, since end users can use the same token for all use cases.

Table 2 below provides an overview of the MFA features offered by OneWelcome.

OneWelcome Identity Platform MFA Features

Use case support	MFA delivered by OneWelcome can secure all applications, whether on-premises or in the cloud.
MFA options	OneWelcome offers extensive MFA options including hardware and software tokens, SMS, pattern-based authentication, FIDO and PKI credentials as well as adaptive and risk-based authentication.
Licensing and business model	OneWelcome has a straightforward licensing policy including tokens, maintenance and support, which makes it easy to plan budget and anticipate costs.
Application support	OneWelcome supports hundreds of applications, including AWS, Salesforce, Google Cloud, BlueCoat, F5 and many others.

Table 2 OneWelcome Identity Platform MFA Features

Scenario 3: OneWelcome Serves as the Identity Provider for Office 365

In this configuration, Office 365 is managed as a cloud application via OneWelcome application manager, exactly like any other cloud application. Integrating and applying policies to accessing Office 365 is only a few minutes away. You can secure Office 365 centrally, along with all your other applications in your environment – including non-standards-based apps, servers on all operating systems including Windows 7, Linux and Mac by applying conditional access and different levels of authentication based on the use case. Furthermore, OneWelcome offers the broadest range of MFA options including push notifications, hardware tokens, SMS, and pattern-based authentication, as well as PKI. In addition, you can have an immediate visibility and powerful reporting into who is accessing all your applications, whether on-premise or in the cloud, when and how.

All these features come at an excellent value. OneWelcome licensing includes combined access management and MFA with multiple tokens offered, including hardware tokens. Your organization is not required to invest in additional infrastructure, while OneWelcome is scalable to additional applications at no extra cost. What is more, there isn't any requirements for dedicated personnel to install, administrate and maintain OneWelcome, since the service is maintained in the cloud.

Table 3 below provides an overview of the benefits of using OneWelcome as an identity provider for Office 365.

OneWelcome Identity Platform as an Identity Provider

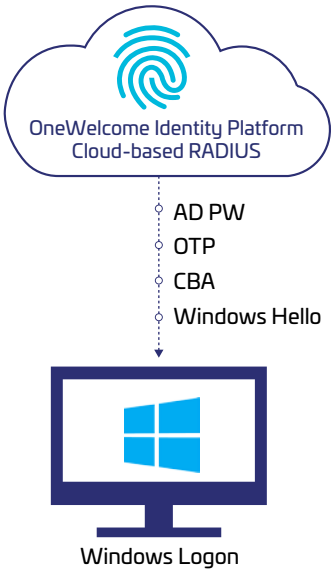
Use case support	Use policy-based access combined with SSO and authentication to secure all applications including non-standards apps, VPN uses cases, RDP VDI, and Windows logon.
MFA options	OneWelcome offers extensive MFA and adaptive authentication options including OTP push notifications, hardware tokens, FIDO, pattern-based authentication, SMS and PKI credentials.
Policy management	OneWelcome offers an attractive GUI and UX which gives customers real-time control and ability to enforce policies at the individual, user, group or application level. Setting up a global policy takes 5 minutes. Setting up a policy to support conditional access and trust elevation would take 10 minutes. Multiple policies are automatically arranged in the correct hierarchical logic
Licensing	OneWelcome is offered as a simple subscription service which includes all the components of an advanced access management solution. It offers SSO, a policy engine and integrated multi-factor authentication – including hardware tokens included in the subscription price - in a simple and transparent per user per month pricing model which allows you to accurately estimate costs over time.
Application support	OneWelcome supports hundreds of applications, including AWS, Salesforce, Google Cloud, BlueCoat, F5 – as well as on-premises applications such as VPNs and servers.

Table 3 OneWelcome Identity Platform as an Identity Provider Overview

Scenario 4: Securing Office 365 and Windows Logon

Many organizations are using MFA to ensure strong user authentication for their Windows domains. OneWelcome can offer a single solution to secure Office 365, cloud applications and Windows domains, including legacy Windows domains, with access management and MFA. Applying a universal MFA solution to all on-premises and cloud applications and using Windows domain credentials in access policies provides a better user experience. Step up authentication, with a broad range of MFA options, is activated only when needed.

Overall, OneWelcome is a universal solution that protects legacy Windows OS and Windows 10. For Windows 10 environments, users can use the same authentication method for multiple use cases instead of having to use Windows Hello and a 3rd part MFA solution for cloud applications, VPN and on-premises applications. Organizations invested in certificate-based authentication and that have mixed Windows OS environment can also use a combined certificate-based / FIDO token for Windows Logon and remote access use cases.

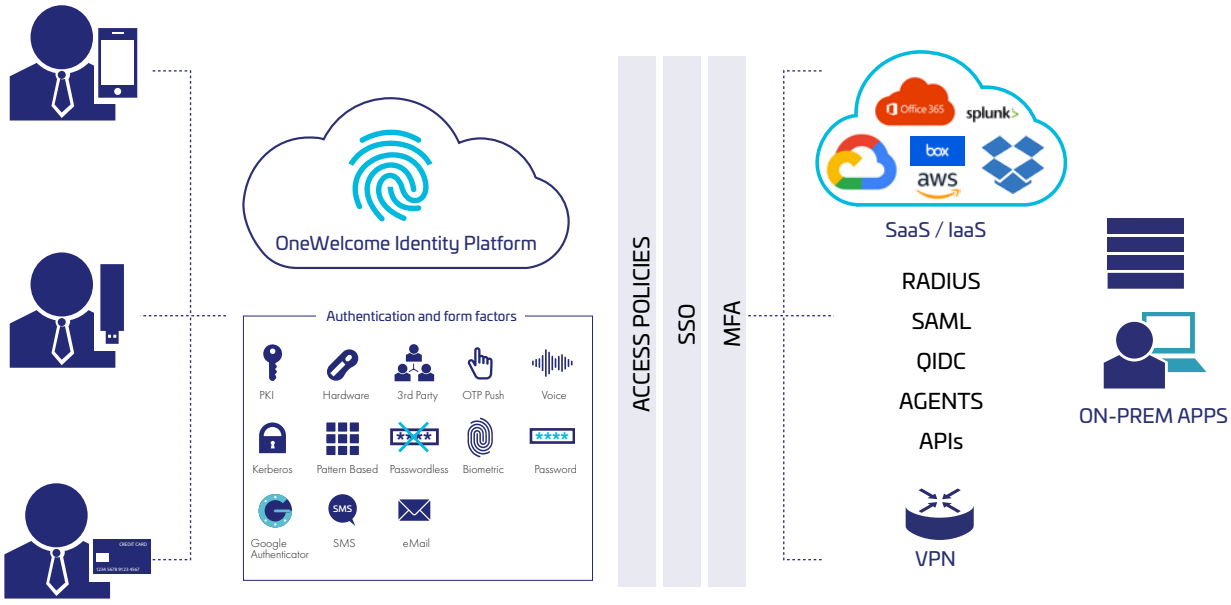


OneWelcome Added Value

Organizations will face several factors regarding cloud application adoption, now and in the future: compliancy, growing number of cloud apps, appropriate risk management and the overall operational costs involved in setting up and managing cloud access.

By clearly defining business and security goals and assessing them against the factors outlined in this paper, CISOs, IT managers and risk management professionals have the power to make an informed decision about the Access Management and MFA solution that best meets their current and future needs.

The value OneWelcome brings is by providing an environment agnostic Access Management and MFA for all applications, whether they are on-premises, or cloud based. Many organizations start their migration to the cloud journey with Office 365 and rapidly add additional cloud applications. OneWelcome provides a single solution that protects the entire environment, allows businesses to scale infinitely and protect additional cloud applications at no extra cost.



Flexibility and Superb User Experience: OneWelcome offers MFA for a wide variety of cloud and non-standard applications. Many organizations are not totally dependent on Microsoft suites and have mixed IT environments. In this type of mixed environment, the ability to integrate seamlessly into a broad range of apps and services is key to ensuring a standardized unified access framework, as well as a consistent authentication experience for end users.

Policy set up and Reporting: OneWelcome makes it easier to keep control of your policies and maintain and prove compliance. OneWelcome offers flexible access management through a simple to use policy engine that gives customers real-time control over the ability to enforce policies at the individual user, group or application level. The policy engine supports a broad range of authentication methods, including ones already deployed, allowing organizations to leverage their current investments and use them to secure cloud and web-based services. The admin console provides simple UX for keeping track of access management visualizing the hierarchy of policies, preventing conflicts between policies and users being blocked out of their applications. Furthermore, OneWelcome offers powerful reporting capabilities with more than 40 pre-configured MFA reports providing visibility into all access events through the respective dashboards. Data-driven insights into access events enable organizations to fine-tune their access policies and ensure regulatory compliance.

Low Total Cost of Ownership (TCO): All OneWelcome capabilities are included in one license, without any hidden costs. Support is included free in the license as are multiple tokens – including hardware tokens. The license also includes cloud-based RADIUS and, therefore, there is no need to maintain a separate on-premises RADIUS server. The licensed solution provides automation and eliminates the requirements for implementing custom integrations.

Agnostic Security Solution: While Microsoft offers numerous security products, these products can be costly if indiscriminately acquired and may not make a difference if not applied appropriately. Businesses can avoid vendor lock-in by doing a comprehensive examination of their security risks and adopting an agnostic security solution which proactively addresses security threats most relevant to them. There are many benefits with choosing an agnostic security solution but the biggest is that it allows to own data protection, data optimization, and recovery across all environments: physical, virtual, cloud, and hybrid cloud environment.

Conclusion

Cloud-based applications play a vital role in fulfilling productivity, operational and infrastructure needs in the enterprise. However, the burden of managing users' multiple cloud identities grows as more cloud apps are used. Most enterprises have a hybrid environment consisting of SaaS such as Office 365, IaaS services such as Azure AD or AWS, and on-premises applications.

As enterprises embrace cloud applications, they are seeking streamlined methods of centrally defining and enforcing access controls to manage security and compliance in a consistent manner across their cloud and on-premises applications. The real challenge is how to achieve the same level of protection that organizations had when everything was on premise - in the cloud. CISOs and enterprise IT departments need an access management and MFA solution for Microsoft installations and other cloud services as well as their on-premises applications which can simplify the life of their end users, protect their organization in a perimeter-less environment, and reduce the risk of identity theft with the goal of thwarting data breaches.

OneWelcome is a cloud-based access management and authentication service that combines the convenience of smart cloud SSO with policy-based access security. OneWelcome is flexible enough to secure your organization's Microsoft architecture in different ways depending on the deployment architecture and preferences. OneWelcome offers a range of access management and authentication capabilities that fit into varied IT architectures and can help organizations prevent data breaches and comply with regulations, allowing them to migrate to the cloud simply and securely.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <