Microsoft and Yubico Part 2 - Enterprise Strong Authentication for Cloud Native Organizations

Cloud Native Organization Components

Context

In this scenario a representative Cloud Native Organization:

- May leverage Azure AD as a primary identity provider and for federation.
- May use different MFA controls, sometimes using smart phones with TOTP, push notifications, or SMS. Generally using multiple MFA providers such as Azure MFA, application specific MFA, or third party solutions.
- May utilize SaaS applications for productivity (Office 365), HR, scheduling, CRM, and other Line of Business Applications. Some of these applications are not federated with Azure AD.
- May have deployed custom web applications to the cloud that uniquely address their specific business requirements.

Enabling Strong Authentication

The Cloud Native Organization has a heavy reliance on Web Applications and needs to focus on securing the accounts accessing those web applications. According to Verizon’s 2019 Data Breach Investigations Report, web applications are one of the leading Hacking vectors for breaches in almost every industry and vertical. The report also states that use of stolen credentials was the most frequently used hacking action.
Each component or resource in an organization may need to employ its own strategy to enable strong authentication and transition to passwordless. A Cloud Native Organization is uniquely positioned to take advantage of modern capabilities which are outlined in the following sections.

Enable security keys as an available passwordless authentication method

Microsoft has enabled capabilities in Office 365, Windows 10, and Azure AD federated applications to allow for strong multi-factor credentials to be provided in the form of FIDO2 security keys such as the YubiKey.

Deploying FIDO2 security keys is among the strongest MFA methods available to secure systems and applications. Enabling sign-in with security keys such as the YubiKey not only enhances security but also significantly reduces friction for the employee. The employees no longer need to remember username and password for any application that supports this credential. The YubiKey is now the credential.

If your organization has already federated your applications with your Azure AD tenant, the applications will now instantly be capable of passwordless sign-in. This includes Microsoft applications and services like Office 365, thousands of SaaS applications in the Azure AD Application Gallery, and many other SaaS applications not registered in the Azure AD Application Gallery including your organization’s own custom applications. The Office 365 or Azure AD administrators simply need to enable this capability. Your organization's developers and application administrators do not have to modify their application to enable passwordless sign in if the application is already federated with Azure AD.

As you begin enabling passwordless in your organization, remember that users will have a tendency to use what they are familiar with. You will need to market and sell the features to the employees as it may be second nature to keep using passwords. Teach and encourage users to use passwordless sign-in with their YubiKeys. Show them how it will make sign-ins easier. Don't forget to remind them to register multiple keys to avoid lockouts and reduce Support Desk calls.

During the initial campaign to use passwordless, also encourage users at the same time to register the same YubiKeys as tokens for OATH-TOTP. Monitor the usage of passwordless sign-in as your campaign rolls through the organization. If you aren't seeing a significant adoption of users leveraging passwordless sign-in, then collect feedback from those user populations to understand why users are not adopting passwordless sign-in before you start requiring MFA.
Secure the admins by enforcing MFA

This should be the first step to securing your environment and making sure all critical security controls and Azure AD services are protected. While custom Conditional Access Policies require Premium licenses, enabling MFA for Azure AD Admins can immediately be enabled with free Baseline Policies that are offered to all Azure AD Customers regardless if they have Premium licenses or not. As Information workers, Azure AD Admins will understand and tolerate being the first teams to a new user experience when signing in for admin functions. AAD Admins should protect their accounts with the strongest credentials and use FIDO2 hardware security keys. This will provide them with the strongest credentials that are resistant to phishing, Man-In-The-Middle and remote attacks. It will also improve the user experience by providing them with the least friction during sign-in.

Drive more adoption of passwordless using Conditional Access Policies

Consider using Office 365 as a first candidate for enabling MFA and for driving adoption of passwordless sign-in across the organization.

A chart from the 2019 Verizon DBIR highlights why Office 365 is an important asset to secure.

![Chart from 2019 Verizon DBIR](image)


The 2019 DBIR goes on to say:

"Most often, those compromised credentials were to cloud-based mail servers. There was an uptick in actors seeking these credentials to compromise a user’s email account."

The reasons to enable MFA for Office 365 are clear, while at the same time, the conditions for enabling the application for passwordless are ideal. Office 365 comes federated with Azure AD, it is a web browser based application suite, and is used by different departments.

If Office 365 is not a good candidate for your organization, the next best candidate would be web based, high-value, highly visible Microsoft service or federated application where you can start driving mass adoption of passwordless sign-in using YubiKeys.

Start by requiring MFA for specific groups of users of Office 365. You will be able to selectively choose which applications, groups, or scenarios by configuring Azure AD Conditional Access Policies. Conditional Access Policies allow you to apply fine-grained authentication policies based on a variety of static and dynamic signals. Organizations should resist applying a broad stroke policy that enables MFA for all users and every application. Review all the available signals in Conditional Access Policy configurations. Consider creating policies which require MFA for specific applications, and also create other policies leveraging Azure’s risk engine and Identity Protection features to require MFA for risky sign-ins. By not requiring MFA for every sign-in, users will be less resistant to adopting MFA and which will simplify your MFA deployment.
Enable Windows sign-in with FIDO2 security keys

In addition to web-based application sign-in, many users and organizations may want to leverage passwordless machine sign-in using FIDO2 security keys. If appropriate for your organization's users, Windows 10 PCs can additionally be configured to allow sign-in using YubiKeys.

Not only will the passwordless sign-in make the desktop available to the user, all Azure AD federated web applications will leverage the same session for access. This eliminates the need for yet another sign-in when they access their organization's applications. This applies for both web and desktop applications such as Outlook that are taking advantage of modern authentication.

Federate your SaaS applications with Azure AD

Your organization likely has one or more SaaS applications that maintain its own identity store. Focus on centralizing all applications to use the same identity provider. By federating all applications with Azure AD, the sprawl of identity islands will be reduced, providing a single place of governance and control for identities' complete lifecycle. In addition to the central point of control, the users will have a single credential that is used for accessing all the federated applications. When users have many credentials to access their various applications, password management hygiene tends to degrade. By federating the SaaS applications, both the users and the organization will benefit while making passwordless for these applications an available option.

Azure AD has a large gallery of thousands of applications where all the work is done to facilitate the federation of commonly used applications. Applications that are not officially registered in the Azure AD Application Gallery can also be federated as long as they support one of the modern authentication protocols. Azure AD supports all the modern authentication protocols such as WS-Federation, SAML, and OpenID Connect. Most modern web applications will support one of these protocols making it easy to federate.

Enable alternate MFA options for applications that don't support passwordless

Until FIDO2 passwordless sign-in support is added across all applications and platforms, you will encounter scenarios where passwordless sign-in will not function. You might find lacking support from mobile devices, OS versions or browsers that haven't been upgraded yet. This will lead you to find alternate MFA options to secure your application until all the prerequisites can be met that are needed to support passwordless. For a Cloud Native Organization, MFA options are generally in the form of One Time Passcodes using SMS, or using an authenticator app to generate OATH-TOTP codes. While these common MFA solutions have well-known weaknesses, this is sometimes the best or the only available option. Microsoft published an interesting blog titled 'All your creds are belong to us' about MFA weaknesses, acknowledging which MFA solutions are susceptible to different attacks. As you encounter systems that won't support FIDO passwordless, keep this information in mind and also keep it in context that an immediate short-term imperfect MFA solution may still reduce the likelihood of compromise to 0.1% of the general population.

Keep the long-term vision in mind. Evaluate solutions that will be familiar to your users and can later be easily migrated to a passwordless solution when it is available. This can be done by leveraging the same investments in YubiKeys that you already made for enabling passwordless. YubiKeys support many authentication protocols including both OATH TOTP, OATH HOTP, and FIDO U2F.
Leveraging the one YubiKey to open up many doors provides a lot of flexibility, uniformity, and opportunity to start establishing behaviors in your users to use the same key to access all applications across all systems and devices. This prepares a more seamless transition for users towards passwordless while avoiding the need for additional licensing, support costs, software, and infrastructure.

**Enable Azure MFA OTP**

Azure AD supports a variety of MFA options. One common option is to use OATH TOTP tokens. The YubiKey can be setup to support Azure MFA requirements as an OATH TOTP token. This will allow you to enable strong authentication for all the scenarios that won't support passwordless sign-in yet. Unlike other TOTP solutions leveraging a TOTP software authenticator app, the YubiKey TOTP solution stores the secure secrets in a crush and water resistant, hardware key, and not in software living on a fragile mobile phone. This allows for a more portable and secure solution - allowing a single TOTP registration to work across all your devices and platforms.

**Non-federated SaaS Applications**

Earlier we discussed the benefits of federating your SaaS applications with Azure AD. Inevitably there will be some applications that are unable to be federated for some technical, compliance or business reasons. Your enterprise should apply discipline and enforce all SaaS applications to be federated with your primary identity provider. If there is a legitimate policy or business reason for not federating the applications your organization should immediately secure the app with MFA. You may want to investigate the capabilities that are native to the SaaS application. Many SaaS applications will allow users to secure the sign-in using OTP codes generated by authenticator apps, or they might support FIDO standards like U2F or WebAuthn. For these solutions, your users can benefit from using the same YubiKeys that they are using for passwordless sign-in.

**Summary**

At this stage in the Cloud Native Organization's journey to passwordless, they are beginning to gain traction and focusing on federating all possible SaaS applications with Azure AD so that they can leverage the investments that the big technology companies are making in FIDO2. Today many of their applications and devices will support passwordless sign-in but support isn’t everywhere. As the corners of the FIDO2 ecosystem become fully featured and gain support, this Cloud Native Organization will soon be ready to leverage passwordless everywhere. In the meantime, while they wait for that future to arrive, the organization is simultaneously securing their applications while beginning the transition. They put YubiKeys in the hands of their users so they can start using the same keys that are capable of passwordless and using the keys for TOTP, WebAuthn, and U2F MFA controls. The organization will soon begin to see less need for using the keys as OTP tokens and start seeing more and more use for FIDO2 passwordless sign-in.

Continue reading the series with: Microsoft and Yubico Part 3 - Enterprise Strong Authentication for On-Premises and Cloud Organizations