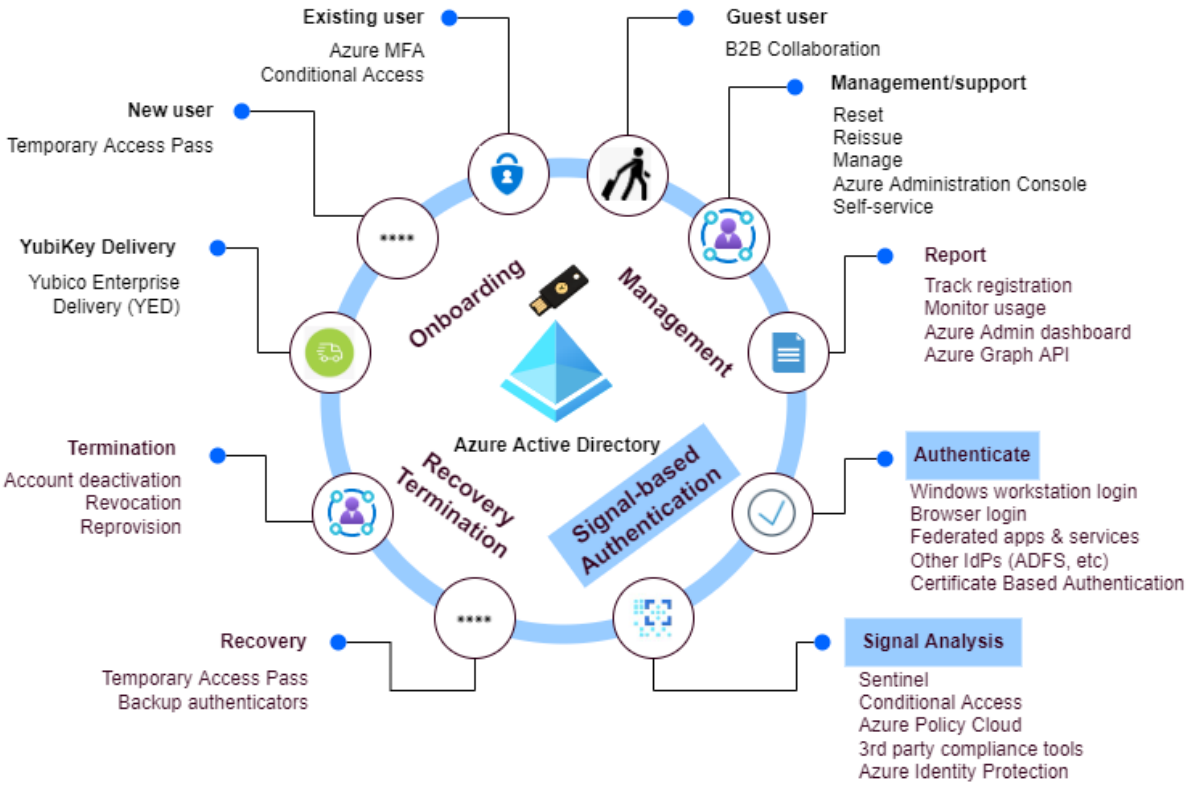
YubiKey Lifecycle Management Best Practices with Microsoft Azure AD Passwordless - Signal-based Authentication



This component has to do with the use of YubiKeys in the field. Users authenticate to get access to different resources and services according to policies designed by the organization to enforce the security requirements. Some of these policies require tracking of specific behaviors or situations (signals) that can be collected by specialized systems and used to create rules that enforce the desired policies.

Authentication

YubiKeys provide strong authentication that eliminates passwords and delivers a more secure and frictionless login experience. It is important to educate end users on the risks of less secure authentication and how that can negatively impact the organization. Informing users of the improved security impact of phishing-resistant login with YubiKeys can empower users to be a part of protecting the overall organization. In addition, explaining to end users the improved experience of no longer having to remember or frequently change passwords, or use a personal device to access work applications, will increase adoption. The more users understand the benefits, the easier it will be to gain their buy-in.

With Microsoft Azure AD it is possible to implement phishing-resistant authentication in different ways--for workstation login or web browser access to applications (including those provided by the organization or by third parties through federation). It is also possible to implement digital certificates to authenticate users.

The effort required for this step includes: phishing-resistant authentication configuration, Azure AD federation configuration with the required applications and services, creation of guides and user training.

Signal Analysis

Signal Analysis provides useful information that can be used to perform additional authentication steps, sometimes called adaptive authentication, which is an emerging trend in identity and access technology. It uses a range of factors from the user (their behavior, devices they're using and other variables) to determine whether a user is performing potentially dangerous activities or engaging in risky behavior.

Using Signal Analysis it is possible to do risk-based authentication, which identifies potentially risky or fraudulent authentication attempts by silently analyzing user behavior and the device of origin. An assessment is done by calculating a risk score using a combination of factors that reflect a specific risk scenario. The calculation may be done using metrics based on a set of static rules and/or data analytics processes that take into account behavioral and historical aspects related to the interaction of a given user with the system in question. Based on the value of the risk score, the user is presented with a number of challenges with the goal of reducing the risk of having a malicious user successfully perform a risky action.

Microsoft provides a number of tools and services that work with Azure AD to help organizations implementing signal analysis and adaptive step-up authentication. Among these services are: Microsoft Defender for Cloud, Azure Conditional Access, and Azure AD Identity Protection. It also provides a powerful SIEM tool in Microsoft Sentinel, that can be integrated with several Azure components. For governance compliance, Azure AD can be integrated with third party solutions like SailPoint and Saviynt.

The effort required for this step includes: signal analysis system configuration and integration with Azure AD and the required applications and services, definition and documentation of step-up authentication policies, and user training.