Accelerate your Zero Trust journey with the top five use cases for Microsoft

Recognized as global leaders in cybersecurity and delivering solutions purpose-built to bring their customers to Zero Trust, Yubico and Microsoft are FIDO Alliance members committed to providing phishing-resistant authentication solutions based on FIDO2 and certificate-based authentication standards.

Reference these use cases to understand how your organization, whether public or private sector, can block any sign-in attempt that does not use CBA and ensure your users are protected by leveraging secure, phishing-resistant, multi-factor authentication solutions with a passkey.

Secure enterprises with passwordless authentication

Use cases: All. Remote workforce, privileged access, mobile restricted environments, shared workstations, consumers

Industries: All including Public Sector, Retail & Hospitality, Manufacturing, Financial services, Healthcare, Cyber insurance, Telecoms, and more.

Login without a password using phishing-resistant FIDO2 authentication to Microsoft products and applications. The Surface Pro 10 for Business is equipped with a built-in NFC reader to sign in passwordlessly with a FIDO2 passkey such as those that reside in the YubiKey 5 NFC and YubiKey 5C NFC.

Login to Windows 10/11 workstations, native apps, web applications and remote desktops with a FIDO2 YubiKey to increase efficiency in your organization and authenticate in seconds. These keys are also supported as PIV-compliant smart cards out-of-the-box with Microsoft Entra ID or with your on-premises infrastructure.

Certificate-based Authentication (CBA)

Use cases: Mobile restricted environments, shared workstations

Industry: Federal government and enterprises that interact with federal governments

CBA enables organizations with existing smart card and public-key-infrastructure (PKI) deployments to authenticate to Microsoft Entra ID (formerly Azure AD) without a federated server.

Use the same YubiKey as a smart card with Entra ID enabling you to migrate away from on-premises authentication solutions like ADFS as part of your Zero Trust and cloud strategies.

CBA on iOS and Android for federal government and enterprises

Use cases: remote workforce

Industry: Federal government and enterprises that interact with federal governments

Provides users with the same convenient smart card authentication method on mobile devices that they have on their desktops.

CBA has been a staple of governments and high security environments for decades, long before the invention of FIDO U2F and FIDO2, mostly due to its reliability and effectiveness in physical environments.

The YubiKey is currently the only external device that supports CBA on Android and iOS. Plus, the YubiKey is the only FIPS-certified, phishing-resistant solution available for Entra ID on mobile.

yubico | Microsoft

Conditional Access Authentication Strengths: Enforced FIDO or CBA

Use cases: All. Remote workforce, privileged access, mobile restricted environments, shared workstations

Industries: All including Public Sector, Retail & Hospitality, Manufacturing, Financial services, Healthcare, Cyber insurance, Telecoms, and more.

Fight phishing attacks by implementing specific user authentication policies.

Leverage YubiKeys for phishing-resistant MFA for FIDO-based passwordless (FIDO2/WebAuthn) or CBA to enforce that YubiKeys are the only authentication solution allowed.

Restrict authentication to an organization's requirements.

Eliminate an entire attack vector for your most privileged users and safeguard your most critical assets by configuring Entra ID to require YubiKeys for phishing-resistant authentication.

Azure Virtual Desktop (AVD) and Remote Desktop adds support for FIDO and CBA

Use cases: Remote workforce, privileged access

Industries: All including Public Sector, Retail & Hospitality, Manufacturing, Financial services, Healthcare, Cyber insurance, Telecoms, and more.

Connect to a personal workstation in the cloud with the same security and work experience no matter where you are. Native clients and web clients allow you to connect to your virtual desktop in the cloud from both desktops and mobile devices.

FIDO-based passwordless or Certificate-based authentication with AVD enables users to sign-in with their YubiKey and Entra ID passwordless credentials or when they sign into an application inside their virtual desktop session.

> "As the threat of sophisticated cyberattacks continues to rise, ensuring our customers have access to phishing-resistant MFA methods like YubiKeys while using our products and platforms is critical, Thanks to our collaboration with Yubico, we're thrilled that our federal government and enterprise customers can now use Entra ID CBA on iOS and Android devices to comply with the Executive Order on improving the Nation's Cybersecurity that directs the use of phishing-resistant MFA on all device platforms."

Natee Pretikul
Principal Product Management Lead | Microsoft Security division

Learn more about how Yubico and Microsoft are stronger together

FIND INTEGRATIONS
yubi.co/wwyk

CONTACT US (AMERICAS)
channels@yubico.com

LEARN MORE
yubi.co/msft-365-mfa

CONTACT US (OUTSIDE AMERICAS)
sales@yubico.com

YUBICO IN THE AZURE MARKETPLACE
yubi.co/msftam

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, the gold standard in phishing-resistant multi-factor authentication (MFA), and a creator and contributor to FIDO open authentication standards. The company is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries. For more information, visit: www.yubico.com.