Påskynda er Zero Trust resa med de fem främsta användningsfallen

Yubico och Microsoft är erkända som globalt ledande inom cybersäkerhet och tillhandahåller lösningar som är byggda för att ge deras kunder tillgång till nolltillitslösningar. Yubico och Microsoft är medlemmar av FIDO Alliance och är engagerade i att tillhandahålla lösningar för phishing-resistent autentisering som är baserade på FIDO2 och certifikatbaserade autentiseringsstandarder.

Läs de här användningsfallen för att få mer information om hur din organisation, oavsett om du bedriver verksamhet inom den offentliga eller privata sektorn, kan blockera alla inloggningsförsök som inte använder certifikatbaserad autentisering och se till att dina användare är skyddade genom att använda säkra phishing-resistenta multifaktorautentiseringslösningar med lösenordsnyckel (passkeys).

Skydda företag med hjälp av lösenordsfri autentisering

Användningsfall: alla, distansarbetare, privilegierad åtkomst, begränsade mobila miljöer, delade enheter, konsumenter.

Branscher: alla, inklusive den offentliga sektorn, detaljhandel, hotell och restauranger, tillverkning, finansiella tjänster, hälso- och sjukvård, cyberförsäkringar, telekommunikation m.m.

Logga in utan lösenord med phishing-resistent FIDO2-autentisering på Microsoft-produkter och -program. Surface Pro 10 för företag har en inbyggd NFC-läsare för lösenordsfri inloggning med en FIDO2-lösenordsnyckel, som de som finns på YubiKey 5 NFC och YubiKey 5C NFC.

Logga in på Windows 10-/11-enheter, inbyggda appar, webbapplikationer och fjärrskrivbord med hjälp av FIDO2-YubiKey-nycklar för att öka effektiviteten och autentisera er på några sekunder.

Certifikatbaserad autentisering (CBA)

Anvädningsfall: begränsade mobila miljöer, delade enheter.

Bransch: myndigheter och företag som interagerar med myndigheter.

Certifikatbaserad autentisering gör det möjligt för organisationer med befintliga smartkort och infrastruktur för offentliga nycklar att autentisera sig till Microsoft Entra ID (tidigare Azure AD) utan någon förenad server.

Genom att använda samma YubiKey-nyckel som smartkort med Entra ID kan ni slippa lokala autentiseringslösningar som ADFS som del av era nolltillits- och molnstrategier.

Certifikatbaserad autentisering på iOS och Android för myndigheter och företag/organisationer

Användningsfall: distansarbetare.

Bransch: myndigheter och organisationer som interagerar med myndigheter.

Ge användarna tillgång till samma behändiga autentiseringsmetod med smartkort på deras mobila enheter som de har på sina stationära datorer.

Certifikatbaserad autentisering har använts på statsnivå och i miljöer med hög säkerhet i årtionden, långt innan FIDO U2F och FIDO2 uppfanns, framförallt på grund av dess tillförlitlighet och effektivitet i fysiska miljöer.

YubiKey-nycklar är för närvarande de enda externa enheterna med stöd för certifikatbaserad autentisering på Android och iOS. Dessutom är YubiKey-nycklar den enda FIPS-certifierade phishing-resistenta lösningen för Entra ID på mobiler.

yubico | Microsoft

Styrkor för autentisering med villkorlig åtkomst: tvingad FIDO-autentisering eller certifikatbaserad autentisering

Användningsfall: alla, distansarbetare, privilegierad åtkomst, begränsade mobila miljöer, delade enheter.

Brancher: alla, inklusive den offentliga sektorn, detaljhandel, hotell och restauranger, tillverkning, finansiella tjänster, hälso- och sjukvård, cyber-försäkringar, telekommunikation m.m.

Bekämpa phishingattacker genom att implementera specifika policyer för användarautentisering.

Använd YubiKey-nycklar för phishing-resistent multifaktorautentisering för FIDO-baserad lösenordsfri (FIDO2/WebAuthn) eller certifikatbaserad autentisering för att se till att YubiKey-nycklar är den enda tillåtna autentiseringslösningen.

Begränsa autentiseringen efter organisationens krav.

Undvik en hel attackvektor för era mest privilegierade användare och skydda era viktigaste tillgångar genom att konfigurera Entra ID för att kräva YubiKey-nycklar för phishing-resistent autentisering.

AVD (Azure Virtual Desktop) och Fjärrskrivbord innehåller nu stöd för FIDO-autentisering och certifikatbaserad autentisering

Andvändningsfall: distansarbetare, privilegierad åtkomst.

Brancher: alla, inklusive den offentliga sektorn, detaljhandel, hotell och restauranger, tillverkning, finansiella tjänster, hälso- och sjukvård, cyberförsäkringar, telekommunikation m.m.

Anslut till personliga enheter i molnet med samma säkerhets- och arbetsgränssnitt oavsett var ni befinner er. Använd inbyggda klienter och webbklienterill att ansluta er till virtuella skrivbord i molnet från stationära och mobila enheter.

Användare kan använda FIDO-baserad lösenordsfri autentisering eller certifikatbaserad autentisering med AVD, vilket innebär att de kan logga in med sina lösenordsfria YubiKeys och Entra ID-inloggningsuppgifter eller när de loggar in på applikationer i sin virtuella skrivbordssession.

> Eftersom hotet från avancerade cyberattacker fortsätter öka är det viktigt att se till att våra kunder har tillgång till phishing-resistenta multifaktorautentiseringsmetoder, som YubiKey-nycklar, när kunderna använder våra produkter och plattformar. Tack vare vårt samarbete med Yubico är vi mycket glada över att våra myndigheter och företagskunder nu kan använda certifikatbaserad Entra ID-autentisering på iOS- och Android-enheter.”

Natee Pretikul
Principal Product Management Lead | Microsoft Security division

Läs mer om hur Yubico och Microsoft är starkare tillsammans

HITTA INTEGRERINGAR
yubi.co/wwyk

LÄS MER
yubi.co/msft-365-mfa

YUBICO PÅ AZURE MARKETPLACE
yubi.co/msftam

KONTAKT
sales@yubico.com