Microsoft Security

Snabbkurs i Azure Active Directory

Den snabba omställningen till att jobba på distans har påskyndat många organisationers arbete med att modernisera arbetsplatsen genom att ge medarbetarna möjlighet att samarbeta på ett säkert och effektivt sätt. IT-avdelningen får fler förfrågningar än någonsin om att ge smidig tillgång till de verktyg och data som användarna behöver, var de än befinner sig och vilka enheter de än använder. För upprätthålla säkerheten på din "nya" arbetsplats måste du skydda dina data effektivt i deras färd mellan många olika platser och program.

0.
Inledning

1.
Vad är Azure AD?

2.
Förbättra användarupplevelsen

3.
Anslut till lokala och molnbaserade appar

4.
Säkra och styr identiteter mer effektivt

0.

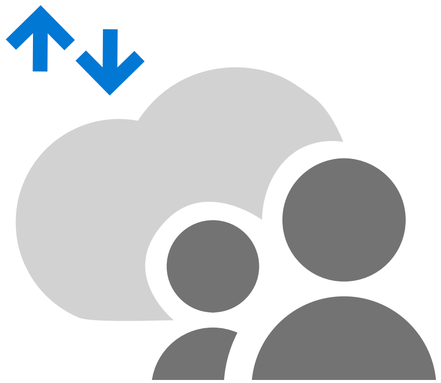
Inledning

En modern metod för identitets- och åtkomsthantering (IAM) kan hjälpa dig att supportera distansmedarbetare på ett säkert sätt.

Kärnan är användningen av Azure Active Directory (Azure AD) för att upprätta en enhetlig identitet samt ge ett enkelt sätt att centralisera autentisering för många typer av program och tjänster. Genom att använda Azure AD kan du förbättra säkerheten och efterlevnaden, medan användarna kan fokusera på innovation och att arbeta effektivt i sina utspridda team. Samtidigt integrerar Azure AD vad som en gång i tiden var olika identitetshanteringsuppgifter för IT-avdelningen och stöder intelligent säkerhet. I den här e-boken tar vi dig med på en snabb rundtur i vad du kan åstadkomma med Azure AD och hur du använder dess fulla potential för att supportera en ny digital arbetsplats på ett säkert sätt.

1.

Vad är Azure AD?



Azure AD är Microsofts molnbaserade katalog- och identitetshanteringstjänst.

I tjänsten kombineras grundläggande katalogtjänster, avancerat identitetsskydd och hantering av appåtkomst. Azure AD ger enkel inloggning (SSO) till lokala och molnbaserade appar, vilket hjälper användarna att vara produktiva. Med Azure AD kan utvecklarna snabbt integrera stark och säker autentisering i sina appar.

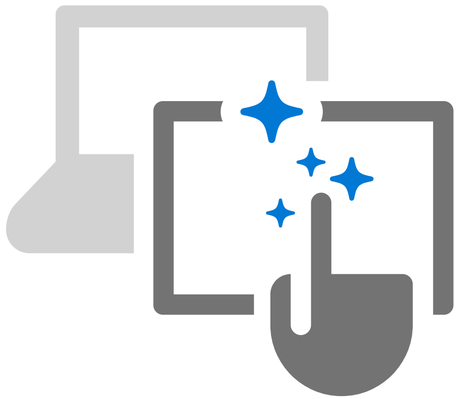
Lösningen erbjuder ett komplett utbud av moderna IAM-funktioner, däribland villkorad åtkomst med multifaktorautentisering (MFA) och inloggning utan lösenord, enkel inloggning, lösenordshantering med självbetjäning, rollbaserad åtkomstkontroll, och funktioner för intelligent säkerhetsövervakning och avisering.

Eftersom tjänsten finns som en fullt hanterad molntjänst är Azure AD den idealiska tjänsten för att kombinera användarkonton till en enda, enhetlig och mycket säker identitet. Tjänsten använder samma lokala Active Directory-teknik (AD) som används av tusentals företag runt om i världen. Den stöder smidig synkronisering från lokala identitetsservrar men med molnets tillgänglighet, skalbarhet och plattformsoberoende funktioner.

Den innehåller lösningar för att autentisera användare för SaaS-appar (programvara som tjänst), lokala appar, webb- och mobilappar med en enhetlig identitet. Denna identitet förenklar också övervakningen och kontrollen av appåtkomst, eftersom alla autentiseringar flödar genom ett enda system. För att maximera värdet av Azure AD bör modellen med en identitet per användare prioriteras.

2.

Förbättra användarupplevelsen



Spara tid och förbättra produktiviteten med enkel inloggning

Personalen använder en mängd olika program under en dag. Att hantera lösenord och logga in om och om igen hindrar dem. Azure AD enkel inloggning (SSO) utökar lokala AD till molnet, så att folk kan använda sin primära företagsidentitet för att logga in på domänanslutna enheter, företagets resurser och i webb- och SaaS-appar.

Detta gör att användarna slipper hantera flera inloggningar och gör det möjligt för organisationerna att ge eller återkalla åtkomst baserat på medarbetarens roll. Azure AD hanterar användarens livscykel dynamiskt. Det är integrerat med personalavdelningens kontroller och ger automatisk åtkomst till de appar som användarna behöver utifrån team och roll. När användare går med, flyttar eller ger sig av anpassas åtkomsten utifrån förinställda policyer. Med SSO kan du hantera användaråtkomst till SaaS, lokala och anpassade appar direkt från Azure-portalen och delegera beslutsprocesser och godkännanden av ansökningar om appåtkomst till alla i organisationen för ökad produktivitet. Inbyggd övervakning och rapportering av användaraktivitet hjälper din organisation att identifiera och minimera obehörig åtkomst. Azure AD-appgalleriet har tusentals SaaS-appar med inbyggda integrationer, vilket gör det enkelt för IT-avdelningen att ansluta nya appar för användarna. Med Mina appar eller Office-portalen kan användarna hitta, filtrera och publicera sina appar från en central, webbaserad portal.

Använd inloggning utan lösenord säkert och enkelt

Att hålla koll på lösenord kan vara besvärligt för användarna, vilket får dem att skriva ner autentiseringsuppgifter i icke-krypterade format – och öppna dörren för säkerhetsöverträdelser. Azure AD tillhandahåller inloggningsalternativ utan lösenord som gör autentisering enklare för användare och säkrare för företag. Med hjälp av appen Microsoft Authenticator kan anställda till exempel logga in genom att få en avisering på sin mobiltelefon. På en domänansluten Windows 10-enhet, där IT-avdelningen har integrerat en enhet med Azure AD, kan Windows Hello låsa upp både enheten och apparna genom att känna igen en PIN-kod, ett smartkort eller biometri som ett fingeravtryck eller ett ansikte. Om en användare inte kan komma åt sin kontorsdator eller mobila enhet kan de använda en FIDO2-säkerhetsnyckel för att logga in på sitt Azure AD-konto.

Ge användarna en konsekvent upplevelse genom att lägga till företagets varumärke

Tillämpa ditt företags utseende och känsla på inloggningssidan för Azure AD, som visas när användare loggar in i appar som använder Azure AD som identitetsleverantör. Det här alternativet kan konfigureras i Azure AD administratörscenter.

Förenkla lösenordshanteringen med självbetjäning av lösenordsåterställning i Azure AD

Din IT-avdelning bör få prioritera strategiskt och verksamhetskritiskt arbete, i stället för att spendera tid och resurser på att återställa lösenord. Med Azure AD Self Service Password Reset (SSPR) kan du göra det möjligt för användare att ändra sina lösenord och låsa upp sina konton utan att kontakta helpdesken. När en användare skapar eller hanterar sina autentiseringsmetoder, till exempel mobilapp, e-post eller säkerhetsfrågor, kan du aktivera SSPR för att förmå dem att registrera samma säkerhetsinformation för MFA, vilket underlättar för slutanvändaren.

3.

Anslut till lokala och molnbaserade appar

Integrera lokala och molnbaserade kataloger med Azure AD Connect

Om du använder Active Directory lokalt kan du enkelt dra nytta av Azure AD genom att synkronisera de två med Azure AD Connect. Genom att tillhandahålla en enda, gemensam identitet för åtkomst till både molnbaserade och lokala resurser kan du förbättra användarupplevelsen, stödja produktiviteten och aktivera avancerade säkerhetsfunktioner. Flera lokala katalogscenarier är möjliga, antingen till en enda AD-skog eller till många isolerade AD-skogar som skapas av komplexa organisationsstrukturer eller sammanslagningar och förvärv. Azure AD Connect kan fungera med Active Directory Federation Services (AD FS) för att hantera komplexa driftsättningsscenarier som domänanslutna SSO. Med Azure AD Connect kan du ta liten plats lokalt samtidigt som du integrerar komplexa kataloger i molnet. Azure AD Connect innehåller också Azure AD Connect Health som hjälper dig att övervaka och rapportera om din katalogmiljö. Det hjälper dig att säkerställa att användarna på ett tillförlitligt sätt kan komma åt alla resurser de behöver med hjälp av en enkel Azure AD Connect Health-agent.

Aktivera säker fjärråtkomst till lokala program

När du ger dina anställda möjlighet att arbeta på sina egna enheter med åtkomst till lokala program var som helst ifrån, kan du avsevärt förbättra produktiviteten. Vissa traditionella åtkomstmetoder för distansarbetare – till exempel virtuella privata nätverk (VPN) och demilitariserade zoner (DMZ) – kan vara komplicerade och svåra att skydda och hantera. En enkel agent är allt som krävs för att Azure AD Application Proxy ska kunna aktivera enkel inloggning och säker fjärråtkomst för lokala webbappar, t.ex. SharePoint-webbplatser, Outlook Web Access på Exchange Server eller andra affärsappar. Du kan också para ihop skalbarheten och säkerheten hos Azure AD med app-plattformar som redan finns i din infrastruktur, till exempel F5, Oracle, SAP och Zscaler.

Interagera mer effektivt med dina kunder med B2B-samarbete

De anställda är inte de enda som behöver säker tillgång till ditt programekosystem. Du kan också behöva ansluta till leverantörer, partner, dotterbolag eller andra externa enheter. Med hjälp av Azure AD B2B-samarbete kan du ge gästanvändare enkel inloggning till appar som du väljer, med kraftfulla autentiseringspolicyer som hanteras av Azure AD. Gästanvändare kan till och med använda sitt eget företags identitetsleverantör för autentisering och ändå komma åt de godkända apparna och resurserna i organisationens nätverk.

Om du tillhandahåller en enda, gemensam identitet för gästanvändare, kan de komma åt både molnbaserade och lokala resurser. Du underlättar för företagets gäster och ser till att de kan vara produktiva samtidigt som identiteterna förblir säkra.

4.

Säkra och styr identiteter mer effektivt

Förbättra säkerheten med Azure AD:s villkorsstyrda åtkomst och MFA

I en värld med växande cyberhot räcker det helt enkelt inte med lösenord för att skydda känslig information, men du vill inte heller riskera att minska produktiviteten. Azure AD:s villkorsstyrda åtkomst förenklar multifaktorautentisering så att det bara krävs när förhållandena utgör en risk. Villkorad åtkomst ger ett riskbaserat resultat baserat på flera kriterier om den användare, enhet och plats som används för att logga in för att avgöra om MFA, lösenordsåterställning eller begränsade funktioner i appen ska tillämpas. Med Azure MFA kan du lägga till enhetsbaserad eller biometrisk säkerhet samtidigt som användarna får en effektiv inloggningsprocess. Du kan använda telefonsamtal, sms eller appbaserad verifiering som sekundär autentiseringsmetod. Om du väljer Microsofts autentiseringsapp som din metod får du MFA utan kostnad!

Identifiera och minimera intrång med Azure AD Identity Protection

Om en angripare stjäl en användares identitet kan hen få åtkomst till kritiska system och data – även om identiteten har minimala behörigheter. Azure AD Identity Protection hjälper dig att identifiera identitetssårbarheter, undersöka och minimera den misstänkta åtkomsten, samt konfigurera automatiserade svar på potentiella identitetsintrång. Med Azure AD Identity Protection kan du skydda alla identiteter oavsett deras behörighetsnivå och proaktivt förhindra att komprometterade identiteter missbrukas.

Lösningen använder adaptiva algoritmer för maskininlärning och heuristik för att upptäcka avvikelser och suspekta incidenter som indikerar potentiellt komprometterade identiteter. Med hjälp av dessa data genererar Azure AD Identity Protection rapporter och varningar som gör att du kan utvärdera de problem som upptäckts och vidta lämpliga åtgärder för begränsning eller reparation. Du kan också konfigurera automatiserade svar på potentiella identitetsintrång, inklusive automatisk blockering eller reparationsåtgärder för att till exempel återställa lösenord eller upprätthålla MFAi.

Delegera administrativa kontroller och styr åtkomstefterlevnad med Azure AD Identity Governance

Azure AD Identity Governance styr identitets- och åtkomstlivscykler genom att säkerställa att rätt användare kommer åt rätt resurser. Inrätta konton till nyanställda med personalavdelningens verktyg så att de kommer i gång direkt, och uppdatera användarnas åtkomst om deras roller förändras. Välj vilka interna användare och gästanvändare som får begära åtkomst till resurser och samla ihop åtkomst till paket för bättre skalbarhet. Azure AD-åtkomstgranskningar hjälper dig att regelbundet utvärdera den aktuella åtkomststatusen samt dynamiskt automatisera åtkomst- och gruppmedlemskap utifrån identitetsattribut. Azure AD Privileged Identity Management hjälper dig att minska risken för överdriven eller onödig utvidgning av roller och åtkomstbehörigheter.

Se dokumentationen om Azure Active Directory om du vill veta mer om Azure AD >

Microsoft Security

Upptäck fördelarna med molnbaserad identitet

Det bästa sättet att uppleva möjligheterna med Azure AD är att testa själv.

Starta din kostnadsfria utvärderingsperiod nu

Kontakta oss