Microsoft 365

Skydda distansarbetarna

Anpassa säkerhetsstrategin inför förändringar

- Möjliggör fjärråtkomst till appar
- Managera enheter och program
- Skydda företagets resurser

Microsoft 365

Företagen håller på att flytta sina interaktioner med anställda, kunder och partner till virtuella domäner för att kunna skydda personalen och hålla uppe takten i verksamheten – och detta samtidigt som vi måste ta hand om yttre utmaningar och nya sätt att arbeta. För vissa företag kan det här steget innebära att de bygger vidare på saker de redan har infört. För andra kan det innebära ett helt nytt sätt att arbeta.

Om du lyckas göra dessa viktiga interaktioner säkra kan du upprätthålla servicenivåerna för kunderna och göra medarbetarna produktiva. Samtidigt behöver företagen ha säkerhetslösningar som är enkla att använda, utan att de innebär komplexitet eller kostnader för IT-teamen – framför allt nu när IT-teamen håller på att anpassa sig efter de nya arbetssätten.

Om företagen kan se till att dessa viktiga interaktioner är säkra kan de upprätthålla servicenivåerna för kunderna och göra medarbetarna produktiva. Den gamla strategin med skalskydd, som bygger på implementeringar med avskilda data, räcker inte för att hålla data och personal säkra i det här nya virtuella landskapet.

Microsoft 365

Den här guiden är tänkt att visa hur du kan använda dina befintliga investeringar i Microsoft 365 för att snabbt låta personalen övergå till distansarbete, samtidigt som du aktiverar de inbyggda säkerhetskontrollerna för att hjälpa dem att förbli skyddade. I listan till höger kan du identifiera de områden där du behöver hjälp, och du kan använda länkarna för att komma direkt till den informationen.

Utmaningar med fjärråtkomst

- ☐ Hålla jämna steg med det stora antalet distansarbetare som behöver kunna komma åt appar och information.
- ☐ Våra distansarbetare är utspridda över hela världen.
- ☐ Vi måste kunna ge leverantörer och tredje part åtkomst för att de ska kunna göra sina jobb.
- ☐ Vi har blandappar med både lokala resurser och molnresurser, som det för närvarande är svårt att ge obruten tillgång till.
- ☐ Vi är oroade över skalbarheten för VPN.

Börja med:

→ **Möjliggör fjärråtkomst till appar**

Microsoft kan hjälpa dig att snabbt tillhandahålla säker och skalbar åtkomst till dina appar, oavsett om plattformarna är lokala eller finns i molnet.

Utmaningar med enhetsmanagering

- ☐ Hela vår personal distansarbetar, vilket gör manageringen av deras enheter till en utmaning.
- ☐ Vi förväntar oss att vissa kommer att använda sina egna enheter för att göra jobbet.
- ☐ Vi måste snabbt införa och leverera nya enheter till vår distansarbetande personal.
- ☐ Vi kämpar för att kunna managera enhetslivscykeln på distans.

Börja med:

→ **Managera enheter och program**

Microsoft kan hjälpa dig att förenkla manageringen av fjärrenheterna och skydda de appar och företagsdata som finns i dem.

Skyddsutmaningar

- ☐ Vi oroar oss för våra data nu när alla arbetar på distans.
- ☐ Nya cybersäkerhetshot växer snabbt på grund av det ökande distansarbetet – särskilt nätfiske.
- ☐ Risken att konfidentiell information läcker ut ur företaget.
- ☐ Vi har inte koll på all användning av molnresurserna – eller på de potentiella säkerhetsriskerna.

Börja med:

→ **Skydda företagets resurser**

Microsoft kan hjälpa dig att få koll på skyddet för appar och data, nu när arbetet görs på distans, och samtidigt minska besväret med att stoppa nya angrepp.

Microsoft 365

Möjliggör fjärråtkomst till appar

För att lyckas med att koppla upp en distansarbetande personal behöver du säker åtkomst till resurser på ett antal olika nivåer. Detta kan till exempel ske genom att tillhandahålla åtkomst till molnappar och molnresurser för personer utanför företagets nätverk (och eventuellt med deras egna enheter). Eller genom att ge distansarbetarna säker åtkomst till verksamhetskritiska lokala appar. Du kan också behöva se till att det går att fortsätta att samarbeta med externa partner för att kunna upprätthålla arbetstakten på företaget.

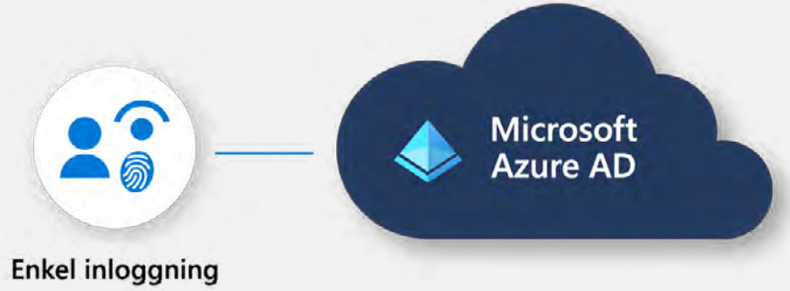
Vi tar en titt på vad som är möjligt.

Säker åtkomst till apparna var som helst ifrån

Manageringen av säker åtkomst, oavsett om det handlar om molnet eller någon annanstans, börjar med att se till att medarbetarna har och behåller säkra identiteter. Microsoft Azure Active Directory (AD) är ett kontrollplan för att managera alla användaridentiteterna, och ger dig en heltäckande plattform för identitets- och åtkomsthantering som en del av din Microsoft 365-prenumeration. Om du inte redan använder det, är detta en mycket bra ställe att börja på.

Azure AD tillhandahåller åtkomstkontroll genom att enkel inloggning används till alla dina appar. Med enkel inloggning behöver användarna bara logga in en gång för att komma åt alla viktiga resurser utan att behöva komma ihåg separata lösenord för varje applikationskonto.

Aktivera enkel inloggning med Azure Active Directory



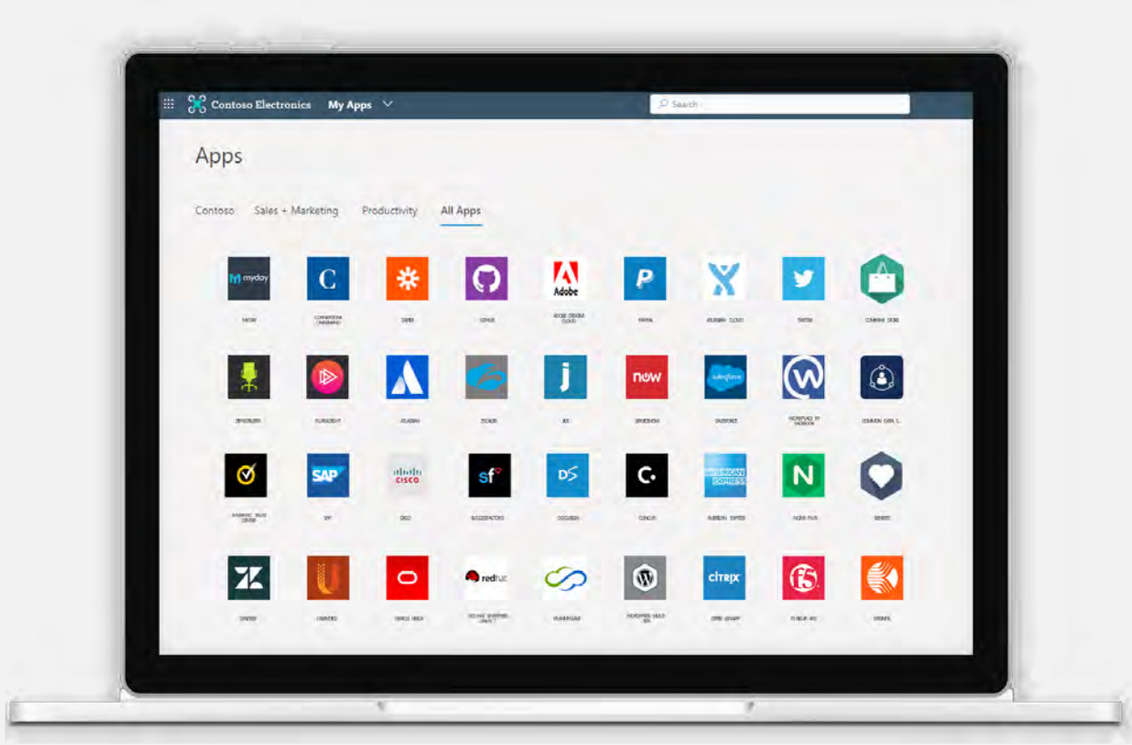
Gör det lättare för slutanvändarna att hitta apparna

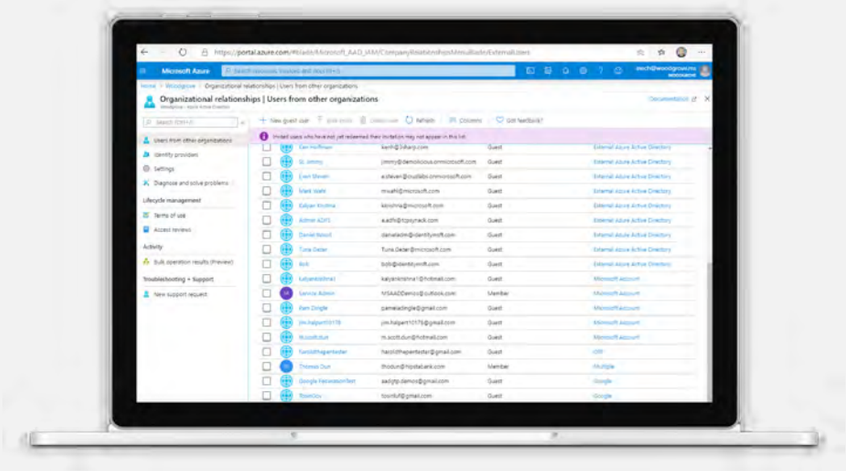
Azure Active Directory har ett appgalleri med tusentals SaaS-appar från tredje part för att förenkla enkel inloggning för dina användare. Oavsett om det gäller Salesforce, Workday , Marketo, Adobe eller flera andra kan du använda Azure AD för att tillhandahålla en central skyddspunkt för dina medarbetare.

Om du redan använder Microsoft 365 och Office-portalen kommer alla appar som är anslutna till Azure AD att visas i Office-portalen. Om du inte använder Office-portalen online kan du få samma upplevelse av portalen Mina appar i Azure AD. Med portalen Mina appar är det enkelt att distribuera nya appar i hela organisationen eller till specifika grupper av medarbetare, till exempel nyanställda som behöver bli produktiva på en gång.

Om du dessutom använder Microsoft Endpoint Manager kan användarna hitta och införa alla installerade appar och webb/molnklientdelar på ett och samma ställe, Microsoft Company Portal. Om ni distribuerar appar med hjälp av Microsoft Endpoint Manager via Company Portal kan ni dessutom använda säkerhets-och dataskyddspolicyer på MDM-registrerade enheter och SDK-försedda enheter i scenarier där enbart MAM används.

Hjälp dina medarbetare att hitta sina appar på ett och samma ställe





Samarbeta säkert med externa partner, för alla appar

Du kan också använda Azure AD för att förenkla samarbetet med externa parter, till exempel affärspartner, distributörer och leverantörer, eller med andra som behöver ha tillgång till specifika appar som en del av den dagliga affärsverksamheten.

Med Azure AD kan du

- Ge medarbetarna möjligheten att bjuda in sina externa partner att komma åt interna resurser.
- Ge affärspartners möjlighet att begära åtkomst.
- Ansluta dina externa partner till dina appar i SharePoint Online och Office 365, samt till eventuella andra SaaS-appar eller specialanpassade lokala affärsappar.

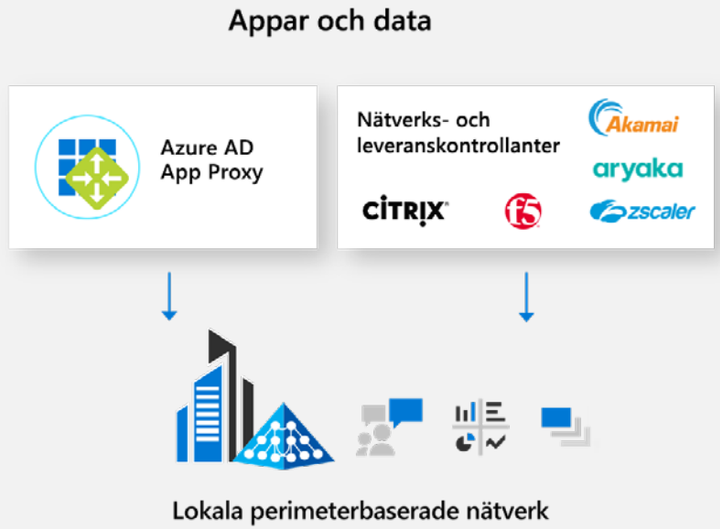
Aktivera extern åtkomst i Azure AD

Säker åtkomst till verksamhetskritiska lokala appar för distansanvändare

Många företag har även äldre lokala program att managera (appar som inte kanske är så lätta att modernisera). För att göra det enklare att ansluta alla program till Azure AD kan du använda lösningar som Azure AD App Proxy och integrationer med nätverkssäkerhetsföretag – Akamai, Arayaka, Citrix, F5 och Zscaler.

Azure AD App Proxy är en funktion i Azure AD som har stöd för enkel inloggning, och som gör det möjligt för användare att komma åt lokala webbprogram från en fjärransluten klient, vilket innebär att det inte behövs något VPN eller en omvänd proxy.

Använd Azure AD App Proxy

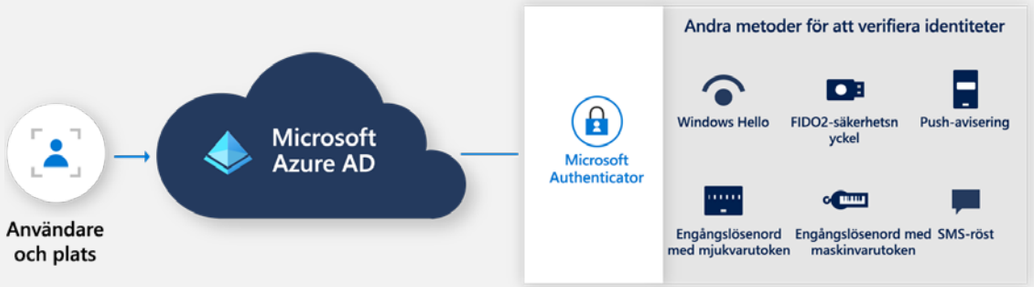


Använd stark autentisering

För att skydda dina medarbetare när de arbetar på distans bör du också se till att slutanvändarautentiseringen är säker. Lösenorden är den svagaste länken i säkerhetskedjan, och om inga ytterligare kontroller används så är de en enskild felkälla. Autentisering med flera faktorer (MFA) kan dock minska risken för intrång med 99,9 %. Om du bara ska göra en enda sak för att skydda dina medarbetare, så ska du införa MFA på företaget.

Du kan ytterligare stärka säkerheten genom att använda Azure AD Conditional Access för att distribuera finjusterade adaptiva åtkomstpolicyer som bygger på riskinformation per användarkontext, enhet, plats och session. Med Conditional Access kan du definiera specifika villkor för hur användare ska autentisera och kunna komma åt era appar och data.

Använda MFA



Åtgärder som du kan vidta i dag för att komma igång

- Ansluta din lokala infrastruktur till molnet.
- Ansluta alla appar till Azure AD för att aktivera enkel inloggning.
- Aktivera MFA med Conditional Access.

En mer detaljerad genomgång som hjälper dig att komma igång med säker fjärråtkomst till dina appar finns i guiden Application management with Azure AD på Microsoft Docs.

Microsoft 365

Managera enheter och program

Manageringen av enheter och appar är en viktig del av arbetet med att skydda den distansarbetande personalen. Men på grund av att övergången till distansarbete under denna kris har gått så snabbt har företagen inte haft tid att hitta den bästa metoden för att managera alla de enheter som fjärransluter till appar och data.

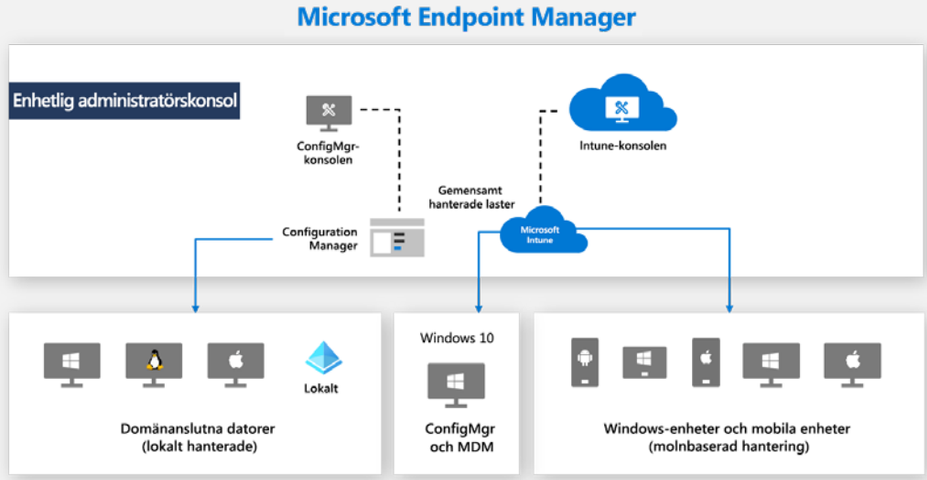
Många medarbetare använder kanske en blandning av företagets produkter och egna produkter. Samtidigt kämpar dina IT-team kanske för att hinna införa och distribuera de nya enheterna på distans. Du behöver ett sätt att på ett säkert sätt managera appar, flera typer av enheter och virtuella skrivbordsupplevelser under hela livscykeln.

Distribuera och managera enheter och virtuella skrivbord

En av de största utmaningarna med att managera en brokig blandning av produkter är de olika ”fönsterrutor” som krävs. Microsoft Endpoint Manager sammanför alla dina slutpunkter och appar under en och samma fönsterruta, och kombinerar de lokala funktionerna i Microsoft Configuration Manager och de molnbaserade fördelarna med Microsoft Intune i Microsoft 365 Admin Center.

Med Microsoft Endpoint Manager kan du distribuera och managera alla dina appar och slutpunkter, bygga på den lokala infrastrukturen med molnsäkerhet och på ett säkert sätt aktivera BYO för åtkomst till resurser. Du kommer också att kunna automatisera distributionen av alla enheter direkt från tillverkaren till användaren, och automatisera införandet av användarinställningar, konfigurationer och appar.

Kom i gång nu med Microsoft Endpoint Manager



Förutom enheterna, så kan företagen också välja att ge användarna åtkomst via virtuella skrivbord. Azure Windows Virtual Desktop tillhandahåller en virtualiseringsinfrastruktur som en managerad tjänst, så att du kan distribuera och managera virtuella maskiner i Azure-prenumerationen och managera upplevelser med verktyg som ConfigMgr och Intune.

Lär dig mer om Windows Virtual Desktop

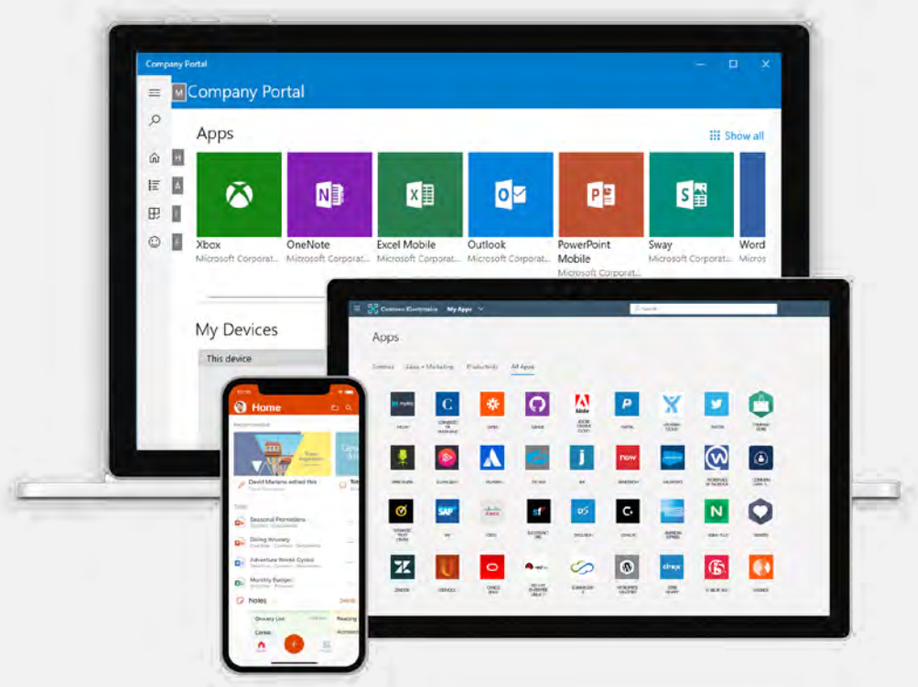
Distribuera och managera appar på valfri enhet

Vissa företag vill ha mer kontroll över manageringen av enheterna och de appar som finns i dem. Andra kan ha infört BYO-policyer. Microsoft erbjuder två metoder för att skydda de appar och de data som finns på mobila enheter.

- **Mobile Device Management** (MDM) ger dig möjligheten att managera enheterna på enhetsnivå. Med MDM kan du använda villkorlig åtkomst för att begränsa åtkomsten till och från den managerade enheten.
- **Mobile Application Management** (MAM) är idealiskt för BYO-scenarier. Du sköter manageringen på appnivån, utan att behöva registrera enheten i MDM. Med hjälp av MAM kan du till exempel tillhandahålla säker åtkomst till Office-appar och tillhörande data på personliga enheter. Dessa data är skyddade, och du kan ta bort dem från enheten utan att personliga data eller appar påverkas. Du kan tillämpa informationsskyddspolicyer för att styra hur det ska gå till att komma åt och använda dessa data.

Du kan också erbjuda användarna en central mötesplats där de kan hitta och komma åt sina jobbappar genom att använda Mina appar, företagsportalen eller Office 365-portalen.

Läs mer om Intune-appmanagering.



Managera uppdateringar, korrigering och policyer proaktivt

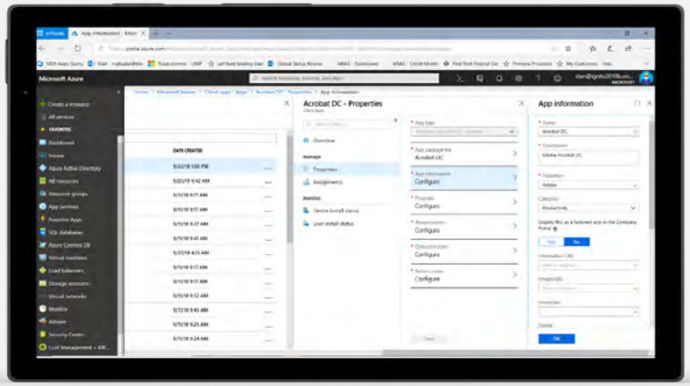
Eftersom hela företag nu arbetar på distans kan det vara svårt att fjärrmanagera livscykeln för enheter och appar för att se till att alla enheter och appar hålls aktuella med nödvändiga uppdateringar, korrigeringar och policyer.

Du kan konfigurera sammanageringsfunktioner i Endpoint Configuration Manager och Intune för en mer flexibel och centraliserad upplevelse vid managering av fjärrenheter och appar.

Du kommer till exempel att kunna:

- Managera uppdateringar av operativsystemet på Windows-datorer och macOS, och ställa in uppdateringspolicyer för iOS och iPad-enheter i övervakningsläge.
- För Windows 10-datorer har du möjlighet att konfigurera uppdateringar som är omedelbara, automatiserade eller där användaren får en uppmaning.
- För iOS-och iPadOS-enheter kan du uppdatera appar och ställa in programuppdateringspolicyer för övervakningsläget.

Läs mer om hur sammanageringsfunktioner fungerar



Åtgärder som du kan vidta i dag för att komma igång

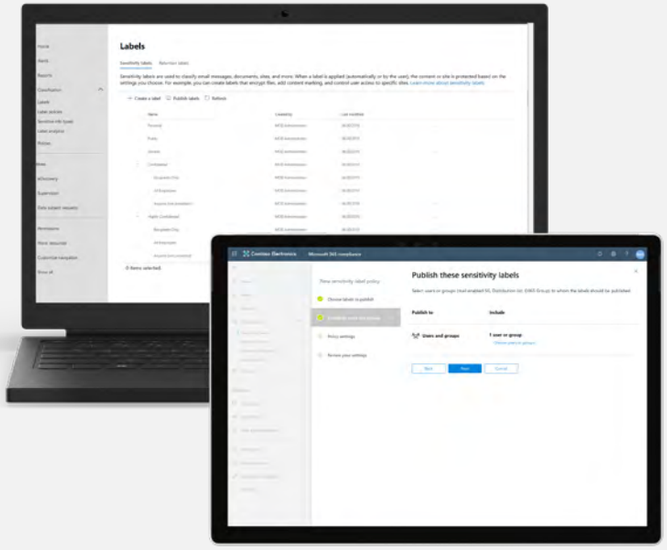
- **Införa och distribuera nya enheter på distans.**
- **Tillämpa åtkomstpolicyer på ej managerade enheter med Intune.**
- **Distribuera och managera virtuella skrivbord.**

Microsoft 365

Skydda företagets resurser

Nu när nästan alla arbetar på distans har det blivit svårare att skydda företagets resurser. Tyvärr vet vi också att illasinnade aktörer kommer att utnyttja situationen. Det är av största vikt att skydda data, appar och slutpunkter mot hot och säkerhetsrisker.

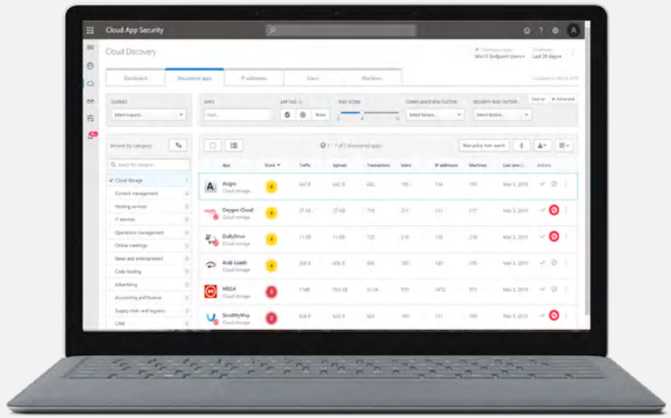
Vi tittar närmare på några områden där du kan hålla personalen produktiv och se till att appar och slutpunkter är säkra.



Skydda data när den distansarbetande personalen samarbetar

På grund av alla bestämmelser om att hålla sig hemma samarbetar medarbetarna nu ofta med digitala verktyg som Microsoft Teams. Övergången till sådana verktyg har hjälpt dem att vara produktiva samtidigt som informationen är skyddad, eftersom mycket av den kommunikation och det innehåll som delas finns i samarbetsmiljön i Teams. Samtidigt måste du se till att all den kommunikation som sker inom Teams, Office-produkterna och andra produktivitetsverktyg från tredje part följer alla relevanta branschförordningar.

Med hjälp av Microsoft Information Protection kan du skydda era känsliga data var de än förvaras och förflyttas. Ett exempel är systemet för dataförlustsskydd (DLP) för Teams, som automatiskt blockerar meddelanden som innehåller känslig information. Microsoft Information Protection innehåller från start över 90 definitioner för känslig information som du kan använda för att identifiera vanliga datatyper, till exempel kreditkortsnummer.



Skydda data i molnappar och molnresurser

De flesta organisationer använder sig av molnbaserade appar, oavsett om det handlar om SaaS-appar eller appar som har molnet som värd. Nu, när det sker en snabb övergång till distansarbete, letar personerna på ditt företag kanske efter nya verktyg och appar som kan fylla luckorna och låta dem få saker gjorda på distans. Att hålla koll på vilka molnappar och molnresurser som används, och hur de används, är avgörande för att kunna skydda sig mot risker.

Med Microsoft Cloud App Security kan du upptäcka och kontrollera åtkomsten till dina molnappar och molnresurser. Verktyget gör att du kan övervaka och kontrollera webbsessioner i realtid, och skydda dem från hot som nedladdning av känsliga filer från ej managerade enheter. Du får också insyn och kontroll över användningen av molnappar. Du kan till exempel upptäcka att en app används som inte uppfyller företagets policyer och då blockera den appen.

Skydda er mot nätfiske och angrepp med skadlig programvara

Före pandemin stod e-post med nätfiske och angrepp med skadlig kod högst på listan över cybersäkerhetshot. Nu försöker angriparna slå mynt av vår rädsla och dra nytta av denna tid av osäkerhet och förändringar. Nätfiske och angrepp med skadlig kod är på uppgång, och många av dessa har nu lockbeten som är relaterade till COVID-19. På grund av de omständigheter vi lever i fortsätter dessa hot att vara några av de mest betydande riskerna för företagen.

Med Microsoft Office 365 Advanced Threat Protection (ATP) kan du skydda företaget från dessa hot, och samtidigt hjälpa säkerhetsteamen att vara mer produktiva tack vare de funktioner för automatisering och AI som ingår i Office 365 ATP.

Här följer några rekommendationer om hur du skyddar er mot nätfiske och angrepp med skadlig kod:

1. **Aktivera Säkra länkar och bilagor**, som ger ett skydd för webbadresser vid den tidpunkt då någon klickar på dem. Säkra bilagor har en detonationsfunktion för bilagor.
2. **Använd Recommended Configuration Analyzer.** Cirka 20 % av allt nätfiske som levereras till användarnas brevlådor beror på felaktiga konfigurationer. Granska konfigurationerna och se till att dina policyer är aktuella.
3. **Visualisera hoten mot företaget**. Med hjälp av Office 365 ATP kan du visualisera och förstå angreppen, och hur de har förhindrats.

Läs mer om hur du kan skydda din organisation mot nätfiske och angrepp med skadlig kod.

Skydda era slutpunkter

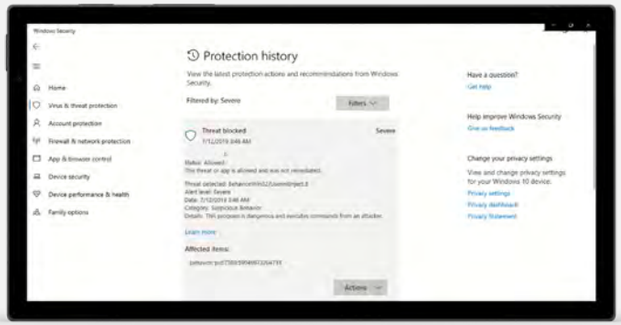
Nu när det mesta arbetet sker på distans är det svårare än någonsin tidigare att se till att alla medarbetarnas slutpunkter är skyddade. På samma gång fortsätter hotbilden att utvecklas.

Med Microsoft får du ta del av våra branschledande funktioner för hot och skadlig kod, funktioner som är inbyggda i Windows och som ger ett beteendebaserat realtidsskydd som till exempel blockerar skadlig kod (både i och utanför filer) och stoppar skadlig aktivitet (från både betrodda och ej betrodda appar). Microsoft Defender Advanced Threat Protection (ATP), vår enhetliga säkerhetslösning för slutpunkter, ger dig en integrerad uppsättning funktioner som kan användas både före och efter ett intrång, och som hjälper säkerhetsteamen att anpassa skalan och fungera effektivt under rådande omständigheter.

Några av de viktigare funktionerna är

- **Managering av hot och sårbarheter** för att upptäcka, prioritera och åtgärda sårbarheter på slutpunkter.
- **Minskning av angreppsytan** för att förstärka systemen och reglera åtkomsten till potentiellt skadliga IP-adresser, domäner och webbadresser.
- **Automatisk utredning och avhjälpning** för att minska risken för att många varningar och falsklarm stjäl all kraft och för att kunna reagera snabbt på hot.

Läs mer om hur du kan skydda den distansarbetande personalen med Microsoft Defender ATP



Åtgärder som du kan vidta i dag för att komma igång

- **Aktivera policyerna för skydd mot dataförlust i Microsoft Teams.**
- **Skydda webbsessionerna med Microsoft Cloud App Security.**
- **Aktivera säkra länkar och säkra bilagor.**
- **Dra nytta av den inbyggda slutpunktssäkerheten.**

Microsoft 365

Kom igång med att skapa ett säkrare distansarbete

Vi vet att alla företag har olika behov och har kommit olika långt med arbetet att göra distansarbetet säkert. Råden i den här e-boken är några av de åtgärder som oftast rekommenderas, och som kan ge betydande säkerhetsfördelar för ditt företag. Vi har sammanfattat de viktigaste stegen inom varje prioritetsområde, så att du kan komma igång redan i dag.

Aktivera säker fjärråtkomst

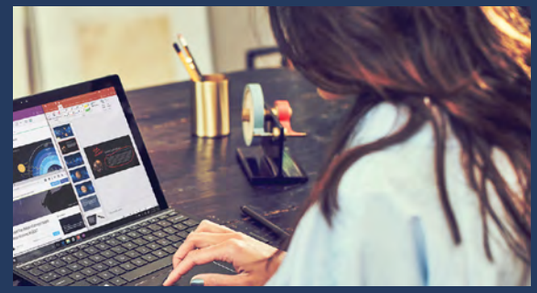
De viktigaste åtgärderna

1. Ansluta din lokala infrastruktur till molnet.
2. Ansluta alla appar till Azure AD för att aktivera enkel inloggning.
3. Aktivera MFA med Conditional Access.

Managera enheter och program

De viktigaste åtgärderna

1. Införa och distribuera nya enheter på distans.
2. Tillämpa åtkomstpolicyer på ej managerade enheter med Intune.
3. Distribuera och managera virtuella skrivbord.



Skydda företagets resurser

De viktigaste åtgärderna

1. Aktivera policyerna för skydd mot dataförlust i Microsoft Teams.
2. Skydda webbsessionerna med Microsoft Cloud App Security.
3. Aktivera säkra länkar och säkra bilagor.
4. Dra nytta av den inbyggda slutpunktssäkerheten.

Microsoft 365

Fortsätta samtalet

Praktiskt program

Få kostnadsfri hjälp med distributionen med Microsoft FastTrack.

Praktiska resurser

Dra nytta av självbetjäningsvägledningen för distribution.

Om du vill veta mer kan du besöka vår webbplats om säkert distansarbete.