Windows 11 Pro

Läs färdigt Security Playbook for the Hybrid Workplace

Cybersäkerhet är det allra viktigaste eftersom 88 % av de undersökta små och medelstora företagen svarade att de inte är förberedda på att hantera cyberhot.[1]

Här är några av de sätt som en säker framtidsskyddad IT-infrastruktur hjälper till med att skydda ditt företag mot cyberhot.

Anta nolltolerans

Säkerhetsmodellen nolltolerans minskar riskerna genom att uttryckligen verifiera datapunkter såsom användaridentitet, plats och enhetshälsa för varje åtkomstbegäran utan undantag. När de har verifierats har användare och enheter begränsad åtkomst endast till nödvändiga resurser.

Nolltoleransprincipen är tredelad:

1

Det första steget är att uttryckligen verifiera. Det innebär att alltid autentisera och auktorisera baserat på tillgängliga datapunkter såsom användaridentitet, plats, enhetshälsa, service eller arbetsbörda, dataklassificering och anomalier.

2

Det andra är att använda minsta möjliga åtkomst, vilket begränsar användarens åtkomst just i rätt tid och just tillräckligt, riskbaserade anpassningsbara policyer och dataskydd som hjälper till med att säkra både data och produktivitet.

3

Det tredje steget är att anta att överträdelser sker. Om du antar att överträdelser kommer att ske minimerar du verkningsradien och segmenterar åtkomsten. Verifiera kryptering från slutpunkt till slutpunkt och använd analys för att få insikt i hur det går att förbättra identifieringen av och försvaret mot hot.

För att kunna implementera nolltoleransmåste organisationerna förstå sina egna data och var de lagras.

Företagen bör känna till känslighetsnivån för dessa data och de potentiella riskerna för exponering för att avgöra när nolltolerans är befogat. I allt från molnbaserade lagringmöjligheter och program såsom e-posttjänster och molnlagring är det förnuftigt att upprätta en nolltoleransmiljö och livsviktigt för att undvika risker. Utan detta tillvägagångssätt är företagets lösenord, enheter och känsliga data obönhörligen utsatta för fara.

Implementera avancerade autentiseringsmetoder

En säkerhetsöverträdelse blir mer sannolik om användarnas autentiseringsmetoder äventyras. Obehörig åtkomst till en medarbetares enhet ger oftast en potentiellt dålig aktör åtkomst till en organisations hela nätverk. Att implementera ett säkert sätt för att säkerställa att användarna är de som de utger sig för att vara är nödvändigt i dagens hybrida arbetsmiljö. Multifaktorautentisering kan vara ett stort steg mot att skapa en säkrare miljö. Lösenord räcker inte längre till för att motverka allt mer sofistikerade hot, eftersom de ofta är lätta att knäcka. Tekniker såsom tvåstegsautentisering tillsammans med de biometriska funktionerna som finns tillgängliga på många moderna enheter, såsom Windows Hello för företag, är mycket effektivare på att skydda organisationer och deras nätverk mot cyberattacker, särskilt när de förstärks med säkerhetsstrategin nolltolerans.

Förstärk maskinvarusäkerheten

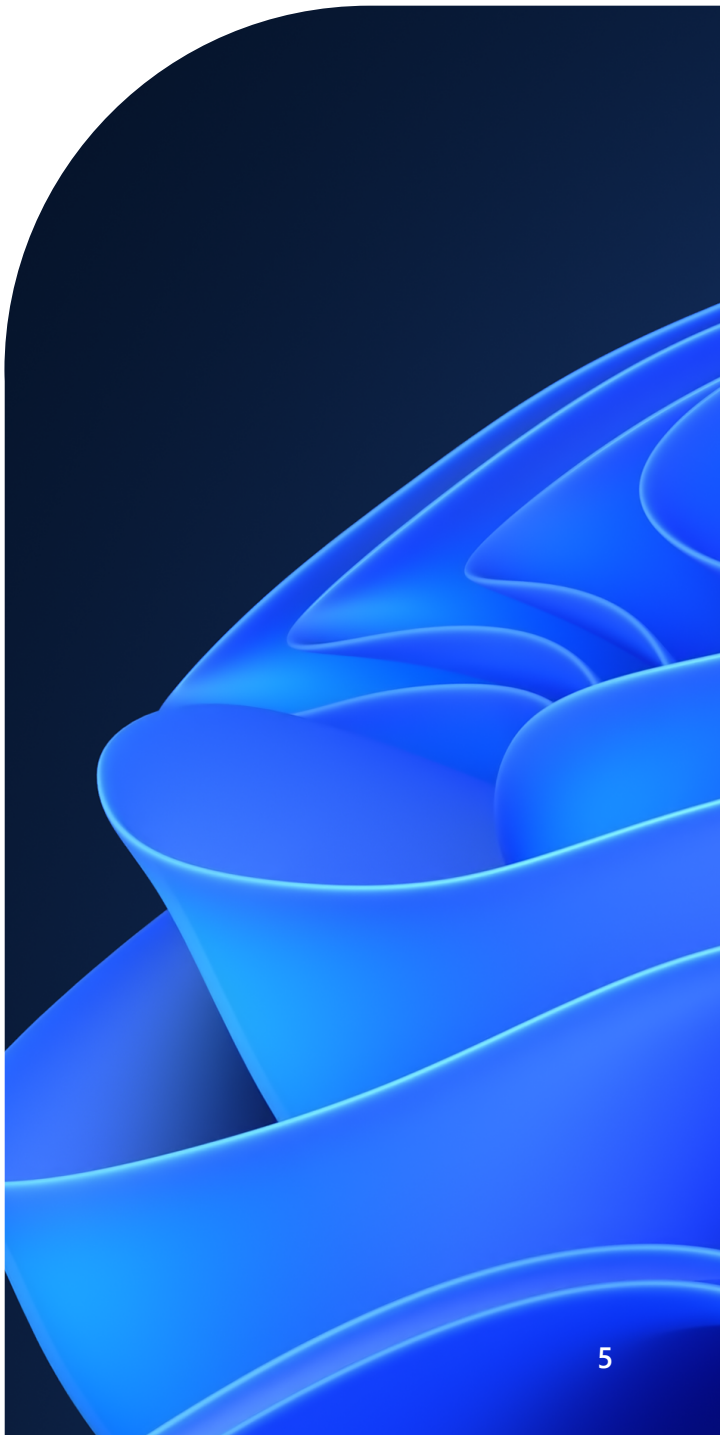
Du kan inte endast lita på att operativsystemet skyddar mot de många olika verktyg och tekniker som it-brottslingar använder sig av för att hacka en dator. När inkräktarna tagit sig in kan de distribuera skadlig kod som är svår att ta bort direkt i enhetens inbyggda programvara eller stjäla känsliga data och viktiga autentiseringsuppgifter. Det kan vara svårt att upptäcka dessa inkräktare när de väl har fått åtkomst. Det behöver finnas en stark koppling mellan maskinvarusäkerheten och de programvarubaserade säkerhetsprogrammen. Moderna hot kräver datormaskinvara som är säker på krets- och processornivå, vilket skyddar känslig företagsinformation direkt där den lagras. En mängd olika svagheter kan undvikas enbart genom att bygga in säkerhetsfunktioner på maskinvarunivå.

Sådana funktioner har till exempel alla Windows 11-datorer med säker kärna. Dessutom kan betydande prestandaförbättringar uppnås jämfört med om endast liknande säkerhetsfunktioner för programvaran distribueras. Det här höjer systemets allmänna säkerhetsläge utan att offra systemets prestanda.

Använd åtkomstkontroller för identitetsbaserat skydd

I molnet kan administratörer kontrollera och hantera identiteter och åtkomst från en plats. Med Microsoft Azure Active Directory (Azure AD) kan de till exempel centralt hantera personalens identiteter samt konfigurera och distribuera policyer för åtkomst till program, sidor och grupper. Administratörer kan bygga in efterlevnadskrav och nya regler kan läggas till när de skapas.

Molnbaserad kontroll ökar säkerheten och stärker efterlevnaden. Forskning från Microsoft visar att multifaktorautentisering på egen hand kan blockera över 99,9 % av hackerattackerna mot konton.[2] Villkorlig åtkomst gör det möjligt för administratörerna att skapa regler baserade på aktivitet eller plats, vilket ytterligare hjälper till med att minska möjligheterna att attackera och utnyttja sårbarheter. Till exempel kan inloggningsförsök från något annat land eller vid konstiga tider avvisas. Dessutom kan administratörer aktivera enkel inloggning, vilket ger användarna säker åtkomst till program varifrån som helst samtidigt som lösenordshanteringen blir enklare för IT-avdelningen.



Microsoft lanserade nyligen allmänt tillgängligt säkerhetsstöd för flera moln. Nu kan företag implementera resurser från flera moln till Azure Security Center, såsom Google Cloud Platform (GCP) och Amazon Web Services (AWS), samtidigt som de skyddar servrarna med Azure Defender för servrar baserad på Azure Arc.

Skydda fjärrenheter

Microsoft-molnet gör det lättare att hantera enheter och program. Med Microsoft Intune kan till exempel enhetsdistribution hanteras säkert och på distans samtidigt som program enkelt kan skalas för att svara på efterfrågan.

Microsoft Windows Autopilot utnyttjar säkerhetsinställningarna och andra kontroller för att skydda enheter innan en medarbetare ansluter sig till en resurs.

Säkra program

Få bättre skydd mot osäkra källor genom att öppna filer och webbplatser i en isolerad behållare med Windows Defender Application Guard. Den molnorienterade designen gör det enkelt att utöka med Microsoft 365, Microsoft Defender for Cloud och Microsoft Defender for Endpoints.[3]

Effektivisera säkerhetshanteringen på olika platser och utöka säkerheten till molnet. Hjälp till att skydda enheter, data, appar och identiteter var som helst. Distribuera med tillförsikt, förvissad om att 99,6 % av alla applikationer är kompatibla med Windows 11.[4]

Automatisera säkerhetsunderhållet

Molnbaserad teknik gör det möjligt för IT-administratörer att automatiskt göra uppdateringar, korrigeringar och säkerhetskopior på olika system och enheter. Det minskar antalet installationsfel och begränsar driftstopp samtidigt som system skyddas mot nya hot. Rutinuppgifter kan automatiseras, vilket ger administratörerna tid för att fokusera på viktigare saker som verkligen kräver deras expertis.

Skydda ditt företag med Windows 11 Pro-enheter

Att förändra din organisations säkerhetsläge borde prioriteras och att utrusta din arbetsstyrka med säkra enheter är en av grundpelarna till hur du lyckas med det. Nya Windows 11 Pro-enheter tillsammans med Microsoft 365 är gjorda för säkert hybridarbete.

- Skydda dina medarbetare mot skadlig kod, virus, nätfiskeförsök, skadliga länkar och hjälp till med att skydda företagskritiska data.

- Få lager med kraftfull säkerhet för enheter, data, identiteter, program och i molnet.

- Strömlinjeforma IT:n med enhetliga molnbaserade verktyg för slutpunktshantering såsom Microsoft Endpoint Manager, Azure Active Directory och Windows Autopilot. Ställ in och genomdriv IT-policyn på distans, hantera program och identiteter och distribuera företagsfärdiga enheter på ett enkelt sätt.

- Övervinn utmaningarna för samarbete på distans med en helhetslösning med videokonferens, produktivitetsappar, fildelning och mycket mer. Se till att medarbetarna har säker åtkomst till viktiga jobbappar och -information via en enhetlig samarbetslösning.

- För personer i datakänsliga branscher och företagsmiljöer: Datorer med säker kärna är de säkraste Windows-enheterna och har alla avancerade säkerhetsfunktioner hos Windows 11 aktiverade.

Minska risken för cyberattacker avsevärt genom att ersätta gamla datorer med nya, moderna enheter optimerade för säkerhet och hybridarbete. Windows 11 Pro och Microsoft M365 sammanför maskinvara och programvara för kraftfullt, direkt skydd för dina enheter, data, applikationer, identiteter och tjänster.

Windows 11 Pro

[1] *https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity*

[2] *https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/*

[3] *Säljs separat*

[4] *App Assure-programdata från oktober 2018 till februari 2022. Sedan 2018 har App Assure jobbat med tusentals kunder och utvärderat fler än 1,1 miljoner appar med en kompabilitetsfrekvens för appar på 99,6 procent. För att lära dig mer går du till App Assure-webbplatsen och läser Windows IT Pro-blogginlägget om App Assure*