ETT WHITE PAPER FRÅN ATEA – VÅREN 2023

7 steg för att få koll på Mac i din verksamhet

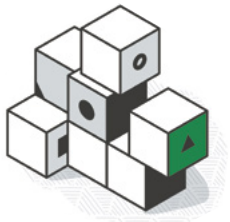
Egentligen är det ganska enkelt. Använd dina befintliga verktyg för att få till både ökad användarvänlighet och en säkrare miljö. Boka in dig på vår workshop och lär dig managera alla enheter i ett och samma verktyg. Vi guidar dig.

STEG 1

Kom i gång med Apple Push Notification Service

I steg ett lär du dig hur du skaffar och hanterar Apple Push Notification Service (APNS) och MDM-certifikat (Mobile Device Management). Apple Push Notification Service är en plattform som gör att tredjeparts-applikationsutvecklare kan skicka meddelanden och uppdateringar till Apple-enheter. Apples MDM-certifikat är kostnadsfritt, men det är också en värdehandling som bör hanteras med stor omsorg. En expert från Atea visar dig hur.

Steg 1 i korthet:
- Registrering av plattformen
- Best practices



STEG 2

Registrera dina Apple-produkter

I steg två går vi igenom hur du registrerar dina Apple-produkter med Automated Device Enrollment som ger dig tillgång till: automatisk aktivering, profilering och möjlighet att pusha ut nya appar och uppdateringar till samtliga enheter. Vi går också igenom registrering och vad du ska tänka på när du aktiverar Apple Device Enrollment och VPP: Volume Purchase Program i din portal. Vi visar Best Practices för Apple Device Enrollment, Apple School Manager och Apple Business Manager.

Steg 2 i korthet:
- Automated Device Enrollment/VPP
- Apple School Manager
- Business Manager
- Registrering

STEG 3

Registrera användare och produkter

I det tredje steget går vi igenom registrering av användare och produkter och hur du skapar automatiserade flöden för uppdateringar och push-installationer. Vår expert visar hur dina medarbetare får access till verksamhetens e-post på ett säkert sätt, vi går igenom scenarios som ger perspektiv och insikter.

Steg 3 i korthet:
- Enrollment/registrering
- User Enrollment
- Automated Device Enrollment
- BYOD (Bring Your Own Device)

STEG 4

Pusha ut appar med script

I steg fyra går vi igenom hur du skickar/pushar ut appar med ett script och hur du automatiserar installationer av appar. Experten/konsulten beskriver volym-köp-apparna, hur it-administratören enklast köper appar och hur du pushar ut dem.

Steg 4 i korthet:
- Applikations-installationer
- Script
- VPP (Volume Purchase Program)
- Agent native distribution

Kryptera diskar på distans

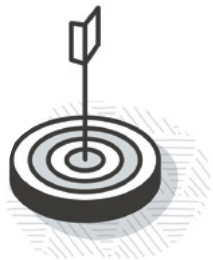
I steg fem går vi igenom konfigurationsprofiler, hur du som jobbar med it krypterar diskar på distans, vilka nätverksinställningar du behöver ha koll på och hur du lägger in restriktioner för användare eller enheter. Om en användare exempelvis ska komma åt iCloud överallt.

Steg 5 i korthet:
- Konfigurationsprofiler
- Diskkryptering
- Nätverk
- Restriktioner

Blås ut ett OS på distans

I steg sex går vi igenom installation, ominstallation – och hur du raderar en hårddisk eller blåser ut ett helt operativsystem på distans. Vi kopplar upp en systemadministratör mot en fiktiv användare och går steg för steg igenom best practices och vad du ska tänka på när du ska göra detta på egen hand.

Steg 6 i korthet:
- Erase & Install
- Ominstallation MAC
- T2 Erase & Install
- ./CreateInstallMedia



Allt ljus på säkerhet

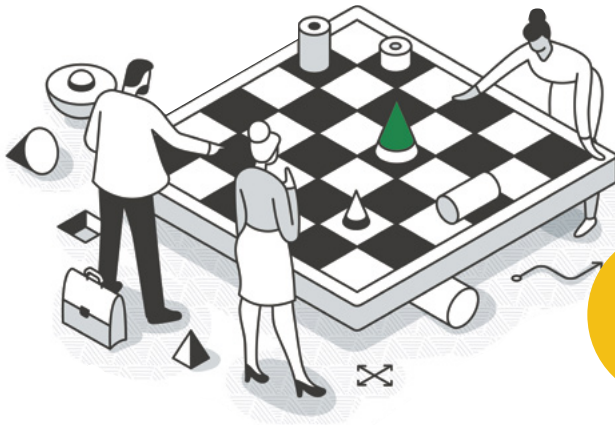
I det sjunde och sista steget sätter vi allt ljus på säkerhet. Här går vi igenom vad du som lokal it-administratör ska tänka på, hur du sätter upp riktlinjer/policys för access och hur de viktigaste apparna för iOS och iPadOS beter sig i Microsoft Intune jämfört med JAMF Pro. Vårt mål är att användare som valt att jobba på Mac eller iPad ska ha en lika bra eller bättre upplevelse jämfört med dem som valt datorer från andra tillverkare.

Steg 7 i korthet:
- Säkerhet
- Lokal administratör
- Antivirus
- CIS Benchmarks (Center for Internet Security) Conditional Access

👉

Yes! Jag vill få koll på Mac!

Klicka här om du vill bli kontaktad av en rådgivare om workshopen.



Se Apples fullständiga handbok kring säkerhet här

Så säkrar du Mac i din verksamhet

Apples produkter är populära tack vare hög prestanda, pålitlighet och användarvänlighet. Men precis som andra plattformar kan Apples produkter utsättas för säkerhetsrisker om de inte hanteras på rätt sätt.

Så ökar du Mac-säkerheten i din verksamhet!

- **Uppdatera regelbundet:** Se till att Mac-datorerna i företaget är uppdaterade med den senaste versionen av operativsystemet och programvaran. Uppdateringar innehåller ofta säkerhetsförbättringar som kan förhindra angrepp.
- **Använd kryptering:** Kryptering kan skydda data från att läsas av obehöriga. Se till att all data på företagets Mac-datorer är krypterad, inklusive hårddiskar, USB-enheter och molnlagring.
- **Implementera starka lösenord och ”Single Sign On”:** Använd starka lösenord för att skydda Mac-datorer och programvaror från obehöriga åtkomstförsök. Se till att anställda förstår vikten av att använda starka lösenord och att de ändrar dem regelbundet. Säkerställ att ni använder Single Sing on på samtliga system och webbplatser där det är möjligt. Användarvänligheten ökar samt säkerheten.
- **Kontrollera användarbehörigheter:** Säkerställ att användaren har den behörighet på sitt lokala konto som krävs för att kunna utföra sitt arbete. Kom ihåg att lokal administratörs behörighet på en Mac skiljer sig ifrån en PC. Lokal Administratör motsvarar ”Power User” på en PC plattform. Om ni måste begränsa adminrättighet säkerställ att ni har en metod för användarna att begära det under en begränsad tid.
- **Börja använda klassificering av dokument och applikationer:** Med hjälp av den så detta kan du sätta regelverk kring när och var användarna har åtkomst till filer och applikationer.
- **Använd säkerhetsprogramvara:** Använd säkerhetsprogramvaror till att få åtkomst till säkerhetsrelaterade event på en Mac plattform. Se till att integrera dessa loggar med exempelvis en CERT funktionalitet. Säkerställ att ni agerar på larm och event ifrån både maskinen och användaren.
- **Använd brandvägg:** Aktivera brandväggen på Mac-datorerna för att blockera oönskad trafik från internet och andra nätverk. Konfigurera brandväggen så att den tillåter nödvändig trafik för företagets arbete.
- **Konfigurera VPN:** VPN säkerställer att trafiken vid distansarbete är krypterad och minskar risken för avlyssning vid publika nätverk.

Utgå ifrån er befintliga säkerhetspolicy

Upprätta en säkerhetspolicy för användning av Mac-datorer inom företaget som linjerar med befintlig säkerhetspolicy. Säkerhetspolicyn bör beskriva vilka säkerhetsåtgärder som är nödvändiga och hur anställda kan hjälpa till att säkra företagets data.

Genom att implementera dessa säkerhetsåtgärder kan företagets Mac-datorer skyddas från en rad olika säkerhetsproblem. Det är viktigt att ha en helhetssyn på säkerhet och att ha en plan för hur man ska hantera säkerhetsincidenter om de inträffar.

ILLUSTRATION: ISTOCKPHOTO