



Apple at Work

Plattformssäkerhet

Säkert i grunden.

Apple tar säkerheten på största allvar, både för användaren och när det gäller att skydda företagsdata. Vi bygger in avancerade säkerhetsfunktioner i våra produkter för att skydda dem och vi gör det på ett sätt som varken stör den enastående användarupplevelsen eller begränsar människors frihet att arbeta som de vill. Endast Apple kan leverera denna omfattande säkerhet, eftersom vi skapar produkter där hårdvara, mjukvara och tjänster är integrerade med varandra.

Säkerhet och hårdvara

Säker mjukvara kräver att hårdvaran har en robust inbyggd säkerhetsgrund. Därför har Apple-enheter som kör iOS, iPadOS, macOS, tvOS eller watchOS integrerade kretsar med inbyggda säkerhetsfunktioner.

Här ingår specialanpassade processorfunktioner som driver funktioner för systemsäkerhet samt dedikerade chip med säkerhetsfunktioner. Den allra viktigaste komponenten är Secure Enclave-coprocessorn som finns i moderna iOS-, iPadOS-, watchOS- och tvOS-enheter samt i alla Mac-datorer med Apple T2 Security-chip. Secure Enclave utgör grunden för kryptering av lagrade data, säker start i macOS samt biometriska data.

Alla moderna iPhone- och iPad-modeller samt Mac-datorer med T2-chip har en dedikerad AES-hårdvarumotor som möjliggör snabb kryptering när enheten skriver eller läser filer. På så sätt kan dataskyddet och FileVault skydda användarnas filer utan att exponera långlivade krypteringsnycklar för processor eller operativsystem.

Den säkra startsekvensen garanterar att den mest grundläggande mjukvaran inte har manipulerats samt att det endast är betrodda operativsystem från Apple som startar. Säkerheten hos enheter med iOS och iPadOS utgår från oföränderlig kod, så kallad start-ROM, som finns inbyggd i chipet och som även kallas för hårdvarans betrodda rot. Hos Mac-datorer med T2-chip utgår säker start från Secure Enclave.

Secure Enclave möjliggör säker inloggning på Apple-enheter med Touch ID och Face ID samtidigt som användarens biometriska data förblir skyddade. På så sätt kan användaren utnyttja säkerheten hos längre och mer komplexa lösenkoder och lösenord och samtidigt dra fördel av snabb autentisering i många olika lägen.

Säkerhetsfunktionerna hos Apples enheter möjliggörs av en kombinationen av kretsdesign, hårdvara, mjukvara och tjänster som bara Apple kan erbjuda.

Systemsäkerhet

Systemsäkerheten bygger på de unika egenskaperna hos Apples hårdvara och är utformad för att maximera säkerheten i operativsystemen i Apples enheter utan att kompromissa med funktionaliteten. Begreppet systemsäkerhet omfattar startprocessen, mjukvaruuppdateringar och operativsystemet kontinuerliga drift.

Säker start tar avstamp i hårdvaran och bygger en förtroendekedja genom mjukvaran, där varje steg säkerställer att nästa steg fungerar som det ska innan processen går vidare. Den här säkerhetsmodellen används inte bara för standardstart av Apple-enheter utan även för olika lägen för återställning och uppdatering av enheter med iOS, iPadOS och macOS.

De senaste versionerna av iOS, iPadOS och macOS är de säkraste. Mekanismen för mjukvaruuppdatering innebär att Apple-enheterna uppdateras regelbundet, men även att de bara uppdateras med betrodd mjukvara från Apple. Uppdaterings-systemet kan rentav förhindra nedgraderingsattacker, så att enheter inte kan återställas till en tidigare version av operativsystemet i syfte att stjäla användardata.

Sist men inte minst har Apple-enheter säkerhetsfunktioner vid start samt under körning som skyddar enheternas integritet vid användning. Skyddet varierar avsevärt mellan enheter med iOS, iPadOS och macOS utifrån de olika funktioner som enheterna stöder och de attacker som de därmed måste kunna avvärja.

För att kunna erbjuda skydd på den här nivån använder iOS och iPadOS Kernel Integrity Protection, System Coprocessor Integrity, PAC-koder (Pointer Authentication Codes) och Page Protection Layer. macOS använder UEFI-säkerhet (Unified Extensible Firmware Interface), SMM (System Management Mode), DMA-skydd (Direct Memory Access) och peripheral firmware security.

Kryptering och dataskydd

Apple-enheter har krypteringsfunktioner som skyddar användardata och möjliggör fjärradering om en enhet blir stulen eller tappas bort.

Kedjan vid säker start, systemsäkerheten och appsäkerheten bidrar alla till att garantera att bara betrodd kod och appar körs på en enhet. Apple-enheter har ytterligare krypteringsfunktioner som skyddar användardata om andra delar av säkerhetsinfrastrukturen skulle komprometteras, till exempel om en enhet tappas bort eller kör otillförlitlig kod. Alla dessa funktioner gynnar såväl användare som it-administratörer eftersom de ständigt skyddar både personliga data och företagsdata och möjliggör omedelbar och fullständig radering av enheten om den skulle bli stulen eller komma bort.

iOS- och iPadOS-enheter använder en metod för filkryptering som går under benämningen dataskydd, medan data på Mac-datorer skyddas med volymkrypteringstekniken FileVault. Båda modellerna har liknande hierarkier för nyckelhantering med roten i de dedikerade kretsarna för Secure Enclave på enheter med Secure Enclave Processor. Båda modellerna använder dessutom en dedikerad AES-motor som möjliggör snabb kryptering och ser till att långlivade krypteringsnycklar aldrig exponeras för operativsystemskärnan eller processorn, där de kan komprometteras.

Appsäkerhet

Apparna är bland de mest kritiska komponenterna i en modern säkerhetsarkitektur. Apparna erbjuder enorma fördelar i fråga om produktivitet, men kan även påverka systemsäkerhet, stabilitet och användardata negativt om de inte hanteras på rätt sätt. Apple tillhandahåller olika skyddslager för att säkerställa att appar är fria från känd skadlig mjukvara och inte har manipulerats. Det finns även andra skyddslösningar som styr åtkomsten till användardata från appar och överser processen noga.

Inbyggda säkerhetskontroller bidrar till en stabil, säker plattform för appar där tusentals utvecklare kan leverera hundratusentals appar för iOS, iPadOS och macOS helt utan att det påverkar systemintegriteten. Användare kan öppna dessa appar från sina Apple-enheter och det finns kontroller på plats som skyddar mot virus, skadlig mjukvara och ovälkomna attacker.

På iPhone, iPad och iPod touch hämtas alla appar från App Store och alla appar körs i en sandlåda vilket bidrar till bästa tänkbara kontroll. På Mac hämtas många av apparna från App Store, men Mac-användare laddar även ner appar från internet. macOS har därför ytterligare kontrollager som skyddar vid nedladdning från internet. Först av allt måste alla Mac-appar attesteras av Apple innan de kan startas (standard i macOS 10.15 och senare). Det här kravet garanterar att apparna är fria från känd skadlig mjukvara utan att apparna för den skull måste komma från App Store. macOS innehåller dessutom antiviruskydd av branschstandard som blockerar skadlig mjukvara och tar bort den vid behov.

Sandlådan utgör en extra kontroll mellan plattformar och bidrar till att förhindra att obehöriga appar ger åtkomst till användardata. Data i kritiska delar av macOS isoleras från alla appar, oavsett om de appar som kräver åtkomst i sin tur är isolerade eller inte. På så sätt kan användare kontrollera åtkomsten till filer i mapparna Skrivbord, Dokument, Hämtade filer med mera.

Säkra tjänster

Apple har skapat en kraftfull uppsättning tjänster som hjälper användarna att få ut ännu mer av sina enheter i fråga om funktionalitet och produktivitet. Här ingår Apple ID, iCloud, Logga in med Apple, Apple Pay, iMessage, FaceTime, Siri, Hitta med flera. Tjänsterna erbjuder kraftfulla funktioner för molnlagring och synk, autentisering, betalning, meddelanden, kommunikation med mera samtidigt som de skyddar användarnas integritet och deras data.

Ekosystem för partner

Apple-enheter fungerar med vanliga säkerhetsverktyg och säkerhetstjänster för företag som garanterar att enheterna och de data som de innehåller uppfyller gällande krav. Varje plattform stöder standardprotokoll för VPN och säkra wifi-anslutningar till skydd för nätverkstrafik och kan på ett säkert sätt anslutas till vanlig företagsinfrastruktur.

Apples samarbete med Cisco erbjuder utökad säkerhet och produktivitet. Ciscos nätverk bidrar till ökad säkerhet via Cisco Security Connector och företagsappar prioriteras i Ciscos nätverk.

Ta reda på mer om Apple-enheter och säkerhet.

apple.com/se/business/it

apple.com/macOS/security

apple.com/se/privacy/features

apple.com/se/security