Apple at Work

Platformssikkerhed

Designet til sikkerhed.

Hos Apple tager vi sikkerheden meget alvorligt – både for brugernes skyld og for at beskytte virksomhedens data. Vi har bygget avanceret sikkerhed ind i vores produkter fra bunden, så de er designet til sikkerhed. Og det har vi gjort på en måde, der er i balance med en fantastisk brugeroplevelse, som giver brugerne frihed til at arbejde, som de vil. Kun Apple kan levere et omfattende udvalg af sikkerhedsfunktioner, fordi vi skaber produkter med integreret hardware, software og tjenester.

Hardwaresikkerhed

Sikker software kræver, at hardwaren har et robust, indbygget sikkerheds-fundament. Derfor har Apple-enheder – som kører iOS, iPadOS, macOS, tvOS eller watchOS – sikkerhedsfunktioner, der er bygget ind i selve kernen.

Det omfatter brugerdefinerede CPU-funktioner, der driver systemsikkerheds-funktioner, samt en dedikeret chip til sikkerhedsfunktioner. Den vigtigste komponent er Secure Enclave-hjælpeprocessoren på nyere iOS-, iPadOS-, watchOS- og tvOS-enheder samt alle Mac-computere med Apple T2 Security-chippen. Secure Enclave danner sikkerhedsgrundlag for kryptering af data i hvile, sikker opstart i macOS og biometriske data.

Alle nyere iPhones og iPads samt Mac-computere med en T2-chip indeholder et dedikeret AES-modul i hardwaren, der muliggør hurtig kryptering, når filer skrives eller læses. På denne måde beskytter databeskyttelse og FileVault brugernes filer uden at afsløre langsigtede krypteringsnøgler for CPU'en eller styresystemet.

Apple-enheders sikre opstart sørger for, at der ikke ændres i de laveste niveauer af softwaren, og at det kun er pålidelig styresystemsoftware fra Apple, der åbnes ved opstart. Sikkerheden for enheder med iOS og iPadOS starter med en uforanderlig kode, den såkaldte Boot ROM, som oprettes, når chippen fremstilles, og som også er kendt som en hardwarebaseret "root of trust". For Mac-computere med en T2-chip begynder sikker opstart med selve Secure Enclave.

Secure Enclave muliggør Touch ID og Face ID i Apple-enheder, så brugerne kan bruge en sikker godkendelsesmetode, hvor de ikke behøver afsløre deres biometriske data. De kan dermed drage fordel af sikkerheden ved længere og mere komplekse adgangskoder og, i mange tilfælde, foretage en hurtig godkendelse.

Sikkerhedsfunktionerne på Apple-enheder er gjort mulige gennem en kombination af chips, hardware, software og tjenester, der kun tilbydes af Apple.

Systemsikkerhed
Systemsikkerheden bygger på de unikke funktioner i Apples hardware og er designet til at maksimere sikkerheden i Apple-enheders styresystemer uden at gå på kompromis med brugervenligheden. Begrebet systemsikkerhed omfatter startprocessen, softwareopdateringer og styresystemets kontinuerlige drift.

Sikker opstart begynder i hardwaren og bygger en kæde af tillid gennem softwaren, hvor hvert trin sikrer, at det næste trin fungerer korrekt, før processen fortsætter. Denne sikkerhedsmodel understøtter ikke kun standardopstart af Apple-enheder, men også forskellige tilstande til gendannelse og opdatering af enheder med iOS, iPadOS og macOS.

De nyeste versioner af iOS, iPadOS og macOS er de mest sikre. Software-opdateringsmekanismen indebærer, at Apple-enhederne opdateres regelmæssigt, men også at de kun opdateres med Apples pålidelige software. Opdateringssystemet forhindrer endda angreb, hvor enhederne går tilbage til en tidligere version af styresystemet som en metode til at stjæle brugerdata.

Sidst, men ikke mindst, har Apple-enheder beskyttelse ved opstart og ved programafvikling, der beskytter enhedernes integritet under brug. Typen af beskyttelse varierer betydeligt mellem enheder med iOS, iPadOS og macOS grundet de forskellige funktioner, de understøtter, og de angreb, de dermed skal kunne afværge.

For at yde beskyttelse på dette niveau bruger iOS og iPadOS Kernel Integrity Protection, System Coprocessor Integrity, PAC-koder (Pointer Authentication Codes) og Page Protection Layer, og macOS bruger UEFI-sikkerhed (Unified Extensible Firmware Interface), SMM (System Management Mode), DMA-beskyttelse (Direct Memory Access) og ekstern firmware-sikkerhed.

Kryptering og databeskyttelse
Apple-enheder har krypteringsfunktioner, der beskytter brugerdata og tillader fjernsletning, hvis en enhed bliver stjålet, eller I mister den.

Denne sikre startkæde, systemsikkerheden og appsikkerhedsfunktionerne er alle med til at sikre, at enheden kun kan bruge koder og apps, der er tillid til. Apple-enheder har yderligere krypteringsfunktioner, der beskytter brugerdata, selv f.eks. i situationer, hvor andre dele af sikkerhedsinfrastrukturen er blevet svækket – f.eks. hvis en enhed mistes eller kører upålidelig kode. Alle disse funktioner er til gavn for både brugere og IT-administratorer, da de konstant beskytter både personlige og virksomhedsoplysninger og muliggør øjeblikkelig og fuldstændig fjernsletning af enheden, hvis I mister den, eller den bliver stjålet.

iOS- og iPadOS-enheder bruger en filkrypteringsmetode, der kaldes databeskyttelse, mens data på Mac-computere beskyttes ved hjælp af en disk-krypteringsteknologi ved navn FileVault. Begge modeller har lignende hierarkier for nøglehåndtering, der er forankret i den dedikerede chip i Secure Enclave på enheder med SEP. Derudover bruger begge modeller et dedikeret AES-modul, der muliggør hurtig kryptering og sikrer, at langsigtede krypteringsnøgler aldrig eksponeres for styresystemkernen eller CPU'en, hvor de kan kompromitteres.

App-sikkerhed

Apps er blandt de vigtigste elementer i en moderne sikkerhedsarkitektur. Apps giver brugerne enorme fordele, når det gælder produktivitet, men kan også have en negativ indflydelse på systemsikkerhed, stabilitet og brugerdata, hvis de ikke håndteres korrekt. Apple giver forskellige lag af beskyttelse for at sikre, at apps er fri for kendt malware, og at der ikke er blevet manipuleret med dem. Der er også andre sikkerhedsforanstaltninger, der kontrollerer adgangen til brugerdata fra apps og overvåger processen omhyggeligt.

Indbyggede sikkerhedsfunktioner bidrager til en stabil, sikker platform til apps, hvor tusinder af udviklere kan levere hundredtusindvis af apps til iOS, iPadOS og macOS helt uden at påvirke systemets integritet. Slutbrugere kan få adgang til disse apps fra deres Apple-enheder, og der er kontrolfunktioner på plads, der beskytter mod virus, malware eller uautoriserede angreb.

På iPhone, iPad og iPod touch downloades alle apps fra App Store, og alle apps er "sandboxed", hvilket giver den bedst mulige kontrol. På Mac-computere hentes mange programmer fra App Store, men Mac-brugere downloader også programmer fra internettet. macOS har yderligere kontrollag, der gør downloadning fra internettet sikkert. For det første skal alle Mac-programmer bekræftes af Apple, før de kan starte (standard i macOS 10.15 og nyere). Dette krav sikrer, at disse programmer ikke indeholder skadelig malware, selvom de ikke kommer fra App Store. macOS indeholder dernæst antivirusbeskyttelse efter branchestandard, der blokerer malware og fjerner den om nødvendigt.

Sandboxing udgør en ekstra kontrolforanstaltning mellem platforme og hjælper med at forhindre uautoriseret adgang til brugerdata fra programmer. Data i kritiske dele af macOS isoleres fra alle programmer, uanset om de programmer, der kræver adgang, selv er blevet isoleret eller ej. Det giver brugerne mulighed for at kontrollere adgangen til filer i mapperne Skrivebord, Dokumenter, Overførsler og andre områder.

Sikre tjenester

Apple har opbygget et robust sæt af tjenester til at hjælpe brugerne med få mere ud af og være mere produktive med deres enheder. Disse tjenester omfatter Apple ID, iCloud, Log ind med Apple, Apple Pay, iMessage, FaceTime, Siri og Find. Tjenesterne tilbyder effektive funktioner til lagring i skyen og synkronisering, godkendelse, betaling, beskeder, kommunikation og meget mere, mens de samtidig beskytter brugernes anonymitet og deres data.

Partner-økosystem

Apple-enheder fungerer med almindelige sikkerhedsværktøjer og -tjenester for virksomheder for at sikre, at enhederne og de data, de indeholder, opfylder kravene. Hver platform understøtter VPN-standardprotokoller og sikre Wi-Fi-forbindelser, der beskytter netværkstrafikken, og kan forbindes sikkert til almindelige virksomhedsinfrastrukturer.

Apples partnerskab med Cisco tilbyder forbedret sikkerhed og produktivitet, når de to virksomheders teknologier bruges sammen. Cisco-netværk byder på øget sikkerhed gennem Cisco Security Connector, og virksomhedsapps prioriteres på Cisco-netværk.

Få mere at vide om Apple-enheder og sikkerhed.

apple.com/dk/business/it

apple.com/macos/security

apple.com/dk/privacy/features

apple.com/dk/security