Apple at Work

Platformssikkerhed

Designet til sikkerhed.

Hos Apple tager vi sikkerheden meget alvorligt – både for brugernes skyld og for at beskytte virksomhedernes 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 så omfattende en tilgang til sikkerhed, fordi vi skaber produkter med integreret hardware, software og tjenester.

Hardwaresikkerhed
Sikker software kræver, at hardwaren har et robust, indbygget sikkerhedsfundament. Derfor har Apple-enheder – med iOS, iPadOS, macOS, tvOS eller watchOS – sikkerhedsfunktioner, der er tænkt ind i selve chippen.

Det omfatter bl.a. tilpassede CPU-funktioner, der driver funktioner til systemsikkerhed, samt en ekstra chip dedikeret til sikkerhedsfunktioner. Sikkerhedsfokuseret hardware følger princippet om at understøtte begrænsede og separat definerede funktioner for at minimere angrebsfladen. Denne form for komponenter omfatter en Boot ROM, som udgør en tillidsrod for hardwaren til sikker start, dedikerede AES-motorer til effektiv og sikker kryptering og dekryptering samt Secure Enclave.

Secure Enclave er et "system on a chip" (SoC), som er inkluderet i alle de nyeste generationer af iPhone, iPad, Apple Watch, Apple TV og HomePod og på Mac-modeller med Apple Silicon samt enheder med Apple T2 Security-chippen. Secure Enclave følger samme designprincip som SoC og har sin egen separate Boot ROM og AES-motor. Secure Enclave danner også grundlag for sikker generering og opbevaring af de nøgler, der kræves for at kryptere data på enheden, og det beskytter og evaluerer de biometriske data til Touch ID og Face ID.

Lagerkryptering skal være hurtig og effektiv. Samtidig må den ikke afsløre de data (eller det nøglemateriale), den bruger til at etablere kryptografiske nøgleforbindelser. AES-hardwaremotoren løser dette problem ved at udføre hurtig, integreret kryptering og dekryptering, mens filerne bliver skrevet eller læst. En særlig kanal fra Secure Enclave leverer det nødvendige nøglemateriale til AES-motoren uden at afsløre denne information over for applikations-processoren (eller CPU'en) eller det overordnede styresystem. Dermed sikres

det, at Apples databeskyttelse og FileVault-teknologier beskytter brugernes filer uden at afsløre langsigtede krypteringsnøgler.

Apple har designet sikker start, som skal beskytte de laveste niveauer af softwaren mod ændringer og sørge for, at det kun er pålidelig styresystemsoftware fra Apple, der indlæses ved opstart. Sikker start begynder med en uforanderlig kode, den såkaldte Boot ROM, som oprettes ved fremstilling af Apple SoC, og som også kaldes tillidsroden for hardwaren. For Mac-computere med en T2-chip begynder sikker start af macOS med T2-chippen. (Både T2-chippen og Secure Enclave udfører også deres egne processer til sikker start ved hjælp af deres egen separate Boot ROM. Dette er helt analogt med, hvordan chips i A-serierne og M1-chips starter sikkert).

Secure Enclave behandler også fingeraftryk og ansigtsdata fra Touch ID- og Face ID-sensorer i Apple-enheder. Dette giver sikker godkendelse, mens brugerens biometriske data fortsat er private og beskyttede. Det betyder også, at brugerne kan få gavn af sikkerheden i lange og mere komplekse adgangskoder, og at de i mange situationer kan få hurtig godkendelse af adgang eller køb.

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

Systemsikkerhed
Idet den bygger på de unikke funktioner i Apples hardware, er systemsikkerheden ansvarlig for at kontrollere adgang til systemressourcer i Apple-enheder uden at gå på kompromis med brugervenligheden. Systemsikkerhed omfatter startprocessen, softwareopdateringer og beskyttelse af computerens systemressourcer, f.eks. CPU, hukommelse, disk, softwareprogrammer og lagrede data.

De nyeste versioner af Apples styresystemer er de mest sikre. En vigtig del af Apples sikkerhed er sikker start, som beskytter systemet mod malwareinfektion ved opstart. Sikker start 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 standardopstarten af Apple-enheder, men også de forskellige tilstande til gendannelse og rettidig opdatering af Apple-enheder. Underkomponenter som T2-chippen og Secure Enclave udfører også deres egen form for sikker start, som er med til at sikre, at de kun starter kendt fungerende kode fra Apple. Opdateringssystemet kan endda også forhindre angreb, hvor enhederne går tilbage til en tidligere version af styresystemet (som hackerne ved, hvordan de kan kompromittere) som en metode til at stjæle brugerdata.

Apple-enheder omfatter også beskyttelse ved opstart og ved programafvikling, der bevarer enhedernes integritet under brug. Apple-designede chips på iPhone, iPad, Apple Watch, Apple TV og HomePod og en Mac med Apple Silicon giver en fælles arkitektur til beskyttelse af styresystemets integritet. macOS har også et udvidet og konfigurerbart sæt beskyttelsesfunktioner, der understøtter den særlige databehandlingsmodel i macOS, samt funktioner, der understøttes på alle Mac-hardwareplatforme.

Kryptering og databeskyttelse
Apple-enheder har krypteringsfunktioner til at beskytte brugerdata og tillade fjernsletning, hvis en enhed mistes eller bliver stjålet.

Den sikre startkæde, systemsikkerheden og funktionerne til programsikkerhed er alle med til at bekræfte, at enheden kun kan bruge koder, apps og programmer, der er tillid til. Apple-enheder har yderligere krypteringsfunktioner til at beskytte brugerdata – endda også i situationer, hvor andre dele af sikkerhedsinfrastrukturen er blevet svækket (f.eks. hvis en enhed mistes eller kører kode, der ikke er tillid til). Alle disse funktioner er til gavn for både brugere og IT-administratorer, da de beskytter personlige såvel som virksomhedsoplysninger og omfatter metoder til øjeblikkelig og fuldstændig fjernsletning af enheden, hvis den mistes eller bliver stjålet.

iOS- og iPadOS-enheder bruger en filkrypteringsmetode, der kaldes databeskyttelse, mens data på en Intel-baseret Mac beskyttes ved hjælp af en diskkrypteringsteknologi ved navn FileVault. En Mac med Apple Silicon bruger en hybridmodel, som understøtter databeskyttelse, men med to forbehold: Det laveste beskyttelsesniveau (klasse D) understøttes ikke, og standardniveauet (klasse C) bruger en enhedsnøgle og fungerer på samme måde som FileVault på en Intel-baseret Mac. I alle tilfælde er de primære styringshierarkier rootet i Secure Enclave-chippen, og en dedikeret AES-motor understøtter kryptering med linjehastighed og er med til at sikre, at langvarige krypteringsnøgler ikke afsløres over for kernestyresystemet eller CPU'en (hvor de kan kompromitteres). (En Intel-baseret Mac med en T1-chip eller uden Secure Enclave bruger ikke en dedikeret chip til at beskytte sine FileVault-krypteringsnøgler).

Ud over, at de bruger databeskyttelse og FileVault for at forhindre uautoriseret adgang til data, sørger Apples styresystemkerner også for at gennemtvinge beskyttelse og sikkerhed. Kernen bruger adgangskontroller til sandboxing af programmer (som begrænser, hvilke data en app kan tilgå) og en mekanisme kaldet Data Vault (som begrænser adgangen til en apps data fra alle øvrige anmodende apps frem for at begrænse de opkald, en app kan foretage).

Appsikkerhed

Apps er nogle af de vigtigste elementer i en sikkerhedsarkitektur. Selv om apps giver brugerne enorme fordele, når det gælder produktivitet, kan de også have en negativ indflydelse på systemsikkerhed, stabilitet og brugerdata, hvis de ikke håndteres korrekt.

Derfor bruger Apple flere lag af beskyttelse som hjælp til at sikre, at apps er fri for kendt malware, og at der ikke er foretaget ændringer i dem. Yderligere beskyttelse sørger for, at adgang til brugerdata fra apps kontrolleres nøje og gennemføres korrekt. Disse 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. Og brugere kan få adgang til disse apps på deres Apple-enheder uden at skulle bekymre sig unødigt om virus, malware eller uautoriserede angreb.

På iPhone, iPad og iPod touch downloades alle apps fra App Store – og alle apps er "sandboxed" – for at give den bedst mulige kontrol.

På Mac-computere hentes mange programmer fra App Store, men Mac-brugere downloader også programmer fra internettet. For at understøtte downloads fra internettet på sikker vis har macOS også yderligere kontrollag. For det første er det standard i macOS 10.15 og nyere versioner, at alle Mac-programmer skal bekræftes af Apple, før de kan starte. Dette krav er med til at sikre, at disse programmer ikke indeholder kendt malware, selvom de ikke nødvendigvis kommer

fra App Store. Desuden har macOS en yderst avanceret antivirusbeskyttelse, som blokerer – og om nødvendigt fjerner – malware.

Sandboxing udgør en ekstra kontrolforanstaltning mellem platforme og er med til at forhindre, at apps og programmer får uautoriseret adgang til brugerdata. Og i macOS er data i kritiske dele beskyttede – det er med til at sikre, at brugerne fortsat kan styre adgangen til filer i Skrivebord, Dokumenter, Overførsler og andre dele af systemet fra alle programmer, uanset om de programmer, der kræver adgang, selv er sandboxed eller ej.

Sikre tjenester

Apple har opbygget et robust sæt af tjenester, der kan hjælpe brugerne med at få endnu mere ud af deres enheder på mere produktive måder. Disse tjenester tilbyder effektive funktioner til lagring i skyen, synkronisering, lagring af adgangskode, godkendelse, betaling, beskeder, kommunikation og meget mere, mens de samtidig beskytter brugernes anonymitet holder deres data sikre.

Tjenesterne omfatter iCloud, Log ind med Apple, Apple Pay, iMessage, Virksomhedschat, FaceTime, Find og Kontinuitet og kan kræve Apple-id eller administreret Apple-id. I nogle tilfælde kan et administreret Apple-id ikke bruges til en bestemt tjeneste, f.eks. Apple Pay.

Bemærk: Nogle Apple-tjenester og noget Apple-indhold er ikke tilgængelige i alle lande eller områder.

Oversigt over netværkssikkerhed

Ud over de indbyggede sikkerhedsfunktioner, Apple bruger til at beskytte data lagret på Apple-enheder, er der mange foranstaltninger, som organisationer kan træffe for at beskytte oplysninger, der sendes mellem enheder. Alle disse sikkerhedsfunktioner og foranstaltninger falder ind under netværkssikkerhed.

Brugere skal kunne få adgang til virksomhedens netværk fra et hvilket som helst sted i verden, så det er vigtigt at sikre, at brugerne er autoriserede, og at deres data er beskyttet under overførslen. For at opfylde disse sikkerhedsmål integrerer iOS, iPadOS og macOS gennemprøvede teknologier og de nyeste standarder for forbindelser både via Wi-Fi- og mobildatanetværk. Det er derfor, vores styresystemer bruger – og giver udviklere adgang til – standardnetværksprotokoller til godkendt, autoriseret og krypteret kommunikation.

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/security

Partner-økosystem

Apple-enheder fungerer sammen med almindelige sikkerhedsværktøjer og -tjenester til virksomheder for at sikre, at enhederne og de data, de indeholder, opfylder kravene. Hver platform understøtter VPN-standardprotokoller – inklusive kontobaserede VPN-forbindelser i iOS og iPadOS 14 – og sikre Wi-Fi-forbindelser for at beskytte netværkstrafikken og kan forbindes med almindelige virksomhedsinfrastrukturer på sikker vis.

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