Apple at Work

Plattformsikkerhet

Sikker fra grunnen av.

Apple er svært opptatt av sikkerhet – for brukerens del og for å beskytte bedriftens data. Vi har bygget avanserte sikkerhetsfunksjoner inn i produktene våre for å gjøre dem sikre fra grunnen av. Og vi har gjort det på en måte som gir en god brukeropplevelse, slik at brukeren får frihet til å arbeide slik de selv ønsker. Det er bare Apple som kan tilby en så omfattende sikkerhetsløsning, for vi utvikler produkter som har maskinvare, programvare og tjenester er integrert.

Maskinvaresikkerhet
Sikker programvare krever et sterkt sikkerhetsgrunnlag som er innebygd i maskinvaren. Det er derfor Apple-enheter – med iOS, iPadOS, macOS, tvOS eller watchOS – har sikkerhetsfunksjoner innebygd i maskinvaren.

Disse omfatter tilpassede prosessorfunksjoner som driver sikkerhetsfunksjoner og maskinvare dedikert til sikkerhetsfunksjoner. Den mest kritiske komponenten er Secure Enclave-koprosessoren i moderne iOS-, iPadOS-, watchOS- og tvOS-enheter og i alle Mac-datamaskiner med Apple T2 Security Chip. Secure Enclave legger grunnlaget for kryptering av arkiverte data, sikker oppstart i macOS og biometri.

Alle moderne iPhone-, iPad- og Mac-enheter med en T2-chip har en dedikert AES-maskinvaremotor for kryptering i linjehastighet når filer skrives eller leses. Dette sørger for at Databeskyttelse og FileVault beskytter brukernes filer uten å eksponere langvarige krypteringsnøkler til prosessoren eller operativsystemet.

Sikker oppstart av Apple-enheter sørger for at programvare på laveste nivå ikke lar seg tukle med, og at kun godkjent operativsystemprogramvare fra Apple lastes inn ved oppstart. På iOS- og iPadOS-enheter begynner sikkerheten i en kode som ikke kan endres, som heter oppstarts-ROM. Denne lages når chipen produseres og er kalt «root of trust» i maskinvaren. På Mac-datamaskiner med en T2-chip begynner godkjenning for sikker oppstart med selve Secure Enclave.

Secure Enclave muliggjør Touch ID og Face ID i Apple-enheter for å gi sikker autentisering samtidig som brukerens biometriske data forblir privat og sikker. Dette gjør at brukerne kan ha sikre, lange og mer komplekse passord med, i mange situasjoner, rask autentisering.

Sikkerhetsfunksjonene i Apple-enheter gjøres mulig av kombinasjonen av silisiumdesign, maskinvare, programvare og tjenester som kun er tilgjengelig fra Apple.

Systemsikkerhet
Systemsikkerheten bygger på de unike funksjonene til Apple-maskinvaren og er designet for å maksimere sikkerheten i operativsystemene på Apple-enheter uten å gå på bekostning av brukervennlighet. Systemsikkerhet omfatter oppstartsprosessen, programvareoppdateringer og driften av operativsystemet.

Sikker oppstart begynner i maskinvaren og bygger en sikkerhetskjede via programvaren, der hvert trinn sørger for at det neste fungerer slik det skal før kontrollen gis videre. Denne sikkerhetsmodellen støtter ikke bare standardoppstarten i Apple-enheter, men også de ulike modusene for gjenoppretting og oppdatering av enheter med iOS, iPadOS og macOS.

De nyeste versjonene av iOS, iPadOS og macOS er de sikreste. Programvareoppdateringer gir ikke bare oppdateringer til rett tid på Apple-enheter, de leverer også bare godkjent programvare fra Apple. Oppdateringssystemet kan til og med forhindre nedgraderingsangrep, slik at enheter ikke kan rulles tilbake til en tidligere versjon av operativsystemet som en metode for å stjele brukerdata.

Apple-enheter har beskyttelse ved oppstart og kjøring, slik at de opprettholder integriteten under drift. Denne beskyttelsen varierer betydelig mellom iOS-, iPadOS- og macOS-enheter basert på de svært ulike settene med funksjoner de støtter, og angrepene de dermed må forhindre.

For å oppnå dette nivået av beskyttelse bruker iOS og iPadOS Kernel Integrity Protection, System Coprocessor Integrity, Pointer Authentication Codes og Page Protection Layer, mens macOS bruker Unified Extensible Firmware Interface-sikkerhet, System Management Mode, Direct Memory Access-beskyttelse og sikkerhet for ekstern firmware.

Kryptering og databeskyttelse
Apple-enheter har krypteringsfunksjoner for å beskytte brukerdata og muliggjøre fjernsletting hvis enheten kommer på avveie eller blir stjålet.

Sikker oppstartssekvens, systemsikkerhet og funksjoner for appsikkerhet bidrar alle til å sikre at bare godkjent kode og godkjente apper kan kjøre på en enhet. Apple-enheter har ekstra krypteringsfunksjoner for å beskytte brukerdata, selv når andre deler av sikkerhetsinfrastrukturen har blitt kompromittert, for eksempel hvis en enhet kommer på avveie eller kjører kode som ikke er godkjent. Alle disse funksjonene er til nytte for både brukere og IT-administratorer, og de beskytter personlig informasjon og bedriftsinformasjon til enhver tid, med muligheter for umiddelbar og fullstendig fjernsletting hvis enheten kommer på avveie eller blir stjålet.

iOS- og iPadOS-enheter bruker en filkrypteringsmetode som heter Databeskyttelse, mens dataene på Mac-datamaskiner beskyttes med en volumkrypteringsteknologi som heter FireVault. Begge modellene baserer sine nøkkeladministrasjonshierarkier i det dedikerte silisiumet i Secure Enclave på enheter som har en SEP. Begge modellene benytter også en dedikert AES-motor til å støtte kryptering i linjehastighet og for å sikre at langvarige krypteringsnøkler aldri må gis til kjerneoperativsystemet eller prosessoren, der de kan bli kompromittert.

Appsikkerhet

Apper er ett av de meste kritiske elementene i en moderne sikkerhetsarkitektur. Apper gir riktignok brukerne utrolig mange fordeler når det gjelder produktivitet, men de kan også påvirke systemsikkerhet, stabilitet og brukerdata negativt hvis de ikke håndteres riktig. Apple har flere beskyttelseslag for å sikre at apper ikke inneholder kjent skadelig programvare, og at de ikke har blitt tuklet med. Ekstra beskyttelse kontrollerer tilgangen til all brukerdata fra apper og håndterer denne prosessen nøye.

Innebygde sikkerhetskontroller gir en stabil og sikker plattform for apper, og gjør det mulig for tusenvis av utviklere å levere hundretusenvis av apper for iOS, iPadOS og macOS – alt uten å påvirke systemintegriteten. Og brukerne har tilgang til disse appene på Apple-enhetene sine med kontroller på plass som hjelper til med å beskytte mot virus, skadelig programvare eller uautoriserte angrep.

På iPhone, iPad og iPod touch hentes alle apper fra App Store – og alle apper kjøres i en sandkasse – for å gi de strengeste kontrollene. På Mac hentes mange apper fra App Store, men Mac-brukere laster også ned og bruker apper fra internett. macOS har ekstra kontroller i flere lag for å støtte nedlasting fra internett på en sikker måte. Som standard på macOS 10.15 eller nyere må alle Mac-apper attesteres av Apple for å kunne startes. Dette kravet sørger for at disse appene ikke inneholder kjent skadelig programvare uten å kreve at appene må tilbys gjennom App Store. I tillegg har macOS standard antivirusbeskyttelse for å blokkere og, ved behov, fjerne skadelig programvare.

Som en ekstra kontroll på tvers av plattformer hjelper sandkasseteknologi med å beskytte brukerdata fra uautorisert tilgang fra apper. Og i macOS blir data i kritiske områder selv kjørt i en sandkasse, noe som sikrer at brukerne har kontroll over tilgang til filer på skrivebordet, i dokumenter og nedlastinger og andre områder – fra alle apper, uansett om appene som forsøker å få tilgang selv kjøres i en sandkasse eller ikke.

Tjenestesikkerhet

Apple har bygd et robust sett med tjenester for å hjelpe brukerne med å få enda mer utbytte av og produktivitet ut av enhetene. Disse tjenestene omfatter Apple ID, iCloud, Logg på med Apple, Apple Pay, iMessage, FaceTime, Siri og Hvor er?. Disse tjenestene har kraftige funksjoner for nettskylagring og -synkronisering, autentisering, betaling, meldinger, kommunikasjon og annet, alt mens de ivaretar brukernes personvern og beskytter dataene.

Partnerøkosystem

Apple-enheter fungerer sammen med vanlige sikkerhetsverktøy og -tjenester i bedrifter og sørger for samsvar med enhetene og de tilhørende dataene. Hver plattform støtter standardprotokoller for VPN og sikker Wi-Fi for å beskytte nettverkstrafikk, og kobles til vanlige bedriftsinfrastrukturer på en sikker måte.

Apples samarbeid med Cisco gir forbedret sikkerhet og produktivitet når de kobles sammen. Cisco-nettverk gir forbedret sikkerhet via Cisco Security Connector og prioriterer bedriftsapplikasjoner på Cisco-nettverk.

Finn ut mer om sikkerhet med Apple-enheter.

apple.com/no/business/it

apple.com/macos/security

apple.com/no/privacy/features

apple.com/no/security