Apple at Work

Plattformsikkerhet

Designet for sikkerhet.

Apple er svært opptatt av sikkerhet – for brukerens del og for å beskytte bedriftens data. Vi har innarbeidet avanserte sikkerhetsfunksjoner i produktene våre for å gjøre dem sikre fra grunnen av. Og vi har gjort det på en måte som tar hensyn til brukeropplevelsen, slik at brukerne får mulighet til å jobbe på sin egen måte. Det er bare Apple som kan tilby en så omfattende tilnærming til sikkerhet, fordi vi utvikler produkter som integrerer maskinvare, programvare og tjenester.

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 integrert i maskinvaren.

Disse omfatter tilpassede prosessorfunksjoner som driver sikkerhetsfunksjoner og maskinvare dedikert til sikkerhetsfunksjoner. Maskinvare med fokus på sikkerhet følger prinsippene om å støtte begrenset og separat definerte funksjoner for å redusere den potensielle angrepsflaten. Disse komponentene inneholder en oppstart-ROM som former en maskinvarebasert root of trust for sikker oppstart, dedikerte AES-motorer for effektiv og sikker kryptering og dekryptering, og en Secure Enclave.

Secure Enclave er et system på en chip (SoC) som er inkludert på alle nye iPhone-, iPad-, Apple Watch-, Apple TV- og HomePod-enheter, på Macer med Apple-chipen og på de med Apple T2 Security Chip. Secure Enclave følger de samme designprinsippene som SoC, inneholder sin egen separate oppstart-ROM og AES-motor. Secure Enclave legger også grunnlaget for en sikker enhetsgenerasjon og kryptering av arkiverte data, og beskytter og evaluerer biometriske data for Touch ID og Face ID.

Lagringskryptering må være rask og effektiv. Samtidig kan den ikke eksponere data (eller nøkkelmaterialet) den bruker til å etablere kryptografiske nøkkelforhold. Den maskinvarebaserte AES-motoren løser problemet ved å utføre rask og direkte kryptering og dekryptering etter hvert som filene skrives eller leses. En unik kanal fra Secure Enclave leverer det nødvendige nøkkelmaterialet til AES-motoren uten å eksponere denne informasjonen for applikasjonsprosessoren (eller prosessoren)

eller hele operativsystemet. Dette sørger for at Databeskyttelse og FileVault beskytter brukernes filer uten å eksponere langvarige krypteringsnøkler.

Apple har utviklet en sikker oppstart for å beskytte grunnleggende programvare fra å bli tuklet med, og for at kun programvare som er godkjent av Apples operativsystem lastes inn ved oppstart. Sikker oppstart begynner i en kode som ikke kan endres, som heter oppstarts-ROM. Denne lages når Apples SoC produseres og er kalt «root of trust» i maskinvaren. På Mac-datamaskiner med en T2-chip begynner godkjenning for sikker oppstart av macOS med T2-chipen. (Både T2-chipen og Secure Enclave utfører også sine egne prosesser for sikker oppstart med sin separate oppstart-ROM – dette er en nøyaktig parallell til hvordan A-serien og M1-chipene starter opp på en sikker måte.)

Secure Enclave registrerer også fingeravtrykks- og ansiktsdata fra Touch ID- og Face ID-sensorene i Apple-enhetene. Dette gir sikker autentisering samtidig som brukerens biometriske data forblir privat og sikker. Det gjør det også mulig for brukerne å få fordelen av sikre, lange og mer komplekse koder og passord, og i mange situasjoner rask autentisering for tilgang eller kjøp.

Disse sikkerhetsfunksjonene i Apple-enheter er mulige gjennom kombinasjonen av silisiumdesign, maskinvare, programvare og tjenester som bare er tilgjengelige fra Apple.

Systemsikkerhet

Systemsikkerheten bygger på de unike funksjonene til Apple-maskinvaren og er designet for å kontrollere tilgang til systemressurser i Apple-enheter uten å gå på bekostning av brukervennlighet. Systemsikkerhet omfatter prosessen for sikker oppstart, programvareoppdateringer og beskyttelse av datamaskinens systemressurser, slik som prosessor, minne, disk, programvareprogrammer og lagrede data.

De nyeste versjonene av Apples operativsystemer er de sikreste. En viktig del av Apples sikkerhet er sikker oppstart, som beskytter systemet mot skadelig programvare under selve oppstarten. 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 Apple-enheter. Underkomponenter som T2-chipen og Secure Enclave utfører også en egen sikker oppstart for å sikre at bare godkjent kode fra Apple starter opp. Oppdateringssystemet kan til og med forhindre nedgraderingsangrep, slik at enheter ikke kan rulles tilbake til en tidligere versjon av operativsystemet (som en angriper vet hvordan de kan bruke) som en metode for å stjele brukerdata.

Apple-enheter har beskyttelse ved oppstart og kjøring, slik at de opprettholder integriteten under drift. Apple-utviklet silisium på iPhone, iPad, Apple Watch, Apple TV og HomePod og en Mac med Apple-chipen leverer en vanlig arkitektur for beskyttelse av operativsystemets integritet. macOS har også et utvidet og konfigurerbart sett med beskyttelsesmuligheter som støtter forskjellige datamodeller samt funksjoner som støttes på alle Mac-maskinvareplattformer.

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 avveier eller blir stjålet.

iOS- og iPadOS-enheter bruker en filkrypteringsmetode som heter Databeskyttelse, mens dataene på Intel-baserte Macer beskyttes med en volumkrypteringsteknologi som heter FireVault. En Mac med Apple-chip bruker en hybridmodell som støtter Databeskyttelse, med to forbehold: Det laveste beskyttelsesnivået (klasse D) støttes ikke, og standardnivået (klasse C) bruker en volumtast og oppfører seg som FileVault på en Intel-basert Mac. I alle tilfeller er nøkkeladministrasjonshierarkier basert i det dedikerte silisiumet i Secure Enclave, og en dedikert AES-motor støtter kryptering i linjehastighet og bidrar i å sikre at langvarige krypteringsnøkler ikke eksponeres for kjerneoperativsystemet eller prosessoren (der de kan bli kompromittert). (En Intel-basert Mac med en T1-chip eller som mangler Secure Enclave bruker ikke dedikert silisium til å beskytte FileVault-krypteringsnøkler.)

I tillegg til å bruke Databeskyttelse og FileVault til å forhindre uautorisert tilgang, sørger Apples operativsystemkjerner for beskyttelse og sikkerhet. Kjernen bruker tilgangskontroller til å kjøre apper i et sandkassesystem (som begrenser hvilke data en app får tilgang til) og en mekanisme som kalles Datahvelv (som begrenser tilgang til data i en app fra alle andre apper som ber om tilgang i stedet for å begrense hva en app kan gjøre).

Appsikkerhet
Apper er ett av de mest kritiske elementene i en sikkerhetsarkitektur. Selv om apper gir brukerne utrolig mange fordeler når det gjelder produktivitet, kan de også påvirke systemsikkerhet, stabilitet og brukerdata negativt hvis de ikke håndteres riktig.

Apple har derfor 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. Disse sikkerhetskontrollene gir en stabil og sikker plattform for apper, og de gjør det mulig for tusenvis av utviklere å levere mange hundre tusen apper for iOS, iPadOS og macOS uten å påvirke systemintegriteten. Og brukere kan bruke disse appene på Apple-enhetene sine uten å være bekymret for virus, skadelig programvare eller autoriserte angrep.

Alle apper til iPhone, iPad og iPod touch hentes fra App Store – og de kjøres i en sandkasse – for å gi strengeste kontroll.

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. macOS kommer også med høyteknologisk antivirusbeskyttelse for å blokkere, og om nødvendig 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 beskyttet, 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 av tjenester for å hjelpe brukerne med å få enda mer nytte og produktivitet ut av enhetene. Disse tjenestene har kraftige funksjoner for nettskylagring og -synkronisering, autentisering, betaling, meldinger, kommunikasjon og annet, samtidig som de ivaretar brukernes personvern og beskytter dataene.

Disse tjenestene omfatter iCloud, Logg på med Apple, Apple Pay, iMessage, Spør bedriften, FaceTime, Hvor er? og Kontinuitet, og kan kreve en Apple ID eller en administrert Apple ID. I noen tilfeller kan ikke en administrert Apple ID brukes med en bestemt tjeneste, som Apple Pay.

Merk: Ikke alt av Apple-tjenester og -innhold er tilgjengelig i alle land og områder.

Oversikt over nettverkssikkerhet

I tillegg til de innebygde sikkerhetsløsningene Apple bruker til å beskytte data som er lagret på Apple-enheter, finnes det mange løsninger som organisasjoner kan ta i bruk for å sikre informasjonen mens den overføres til eller fra en enhet. Alle disse sikkerhetsmekanismene og løsningene havner under nettverkssikkerhet.

Brukere må ha tilgang til bedriftsnettverk fra hele verden, så det er viktig å sikre at de er godkjente, og at dataene er beskyttet under overføringen. For å tilby denne sikkerheten integrerer iOS, iPadOS og macOS anerkjent teknologi og de nyeste standardene for både Wi-Fi- og mobilnettilkoblinger. Det er derfor operativsystemene våre bruker, og gir utviklere tilgang til, standard nettverksprotokoller for autentisert, autorisert og kryptert kommunikasjon.

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 – inkludert Per Account VPN-tilkoblinger på iOS og iPadOS 14 – 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 kompatibilitet med Apple-enheter.

apple.com/no/business/it

apple.com/no/macos/security

apple.com/no/privacy/features

apple.com/no/security