Apple at Work

Alustojen tietoturva

Suunniteltu turvallisiksi.

Sekä käyttäjien että yritystietojen tietoturva on tärkeää Applelle. Suunnittelemme tuotteemme läpikotaisin turvallisiksi käyttäen edistyksellisiä tietoturvaominaisuuksia joka tasolla. Tasapainotamme tämän myös huippuluokan käyttökokemuksen kanssa niin, että käyttäjillä on vapaus työskennellä haluamallaan tavalla. Vain Apple voi tarjota tämän kattavan lähestymistavan tietoturvaan, koska luomme tuotteisiin integroidusti laitteiston, ohjelmiston ja palvelut.

Laitteiston suojaus
Jotta ohjelmisto olisi suojassa, sen täytyy olla suojatuksi rakennetussa laitteistossa. Siksi Applen iOS-, iPadOS-, macOS-, watchOS- ja tvOS-laitteissa on suojausominaisuuksia jo laitteistotasolla.

Näihin ominaisuuksiin kuuluvat räätälöity prosessori, joka mahdollistaa järjestelmän suojausominaisuudet, sekä suojaustoiminnoille varattu lisäsiru. Suojaukseen keskittyvissä laitteistokomponenteissa on periaatteena, että ne tukevat vain rajoitettuja ja erikseen määriteltyjä toimintoja hyökkäysmahdollisuuksien vähentämiseksi. Näitä komponentteja ovat Boot ROM, joka on laitteiston luottamuksen perusta suojatussa käynnistyksessä, tehokkaaseen ja turvalliseen salaukseen ja salauksen purkuun varatut AES-moottorit sekä Secure Enclave.

Secure Enclave on järjestelmäsiru (SoC), joka sisältyy kaikkiin uudempiin iPhone-, iPad-, Apple Watch-, Apple TV- ja HomePod-laitteisiin sekä Apple Siliconilla tai Apple T2 Security -sirulla varustettuun Maciin. Secure Enclave noudattaa SoC:n suunnitteluperiaatetta sisältäen oman erillisen Boot ROM:in ja AES-moottorin. Secure Enclave myös tarjoaa pohjan levossa olevan datan salauksessa tarvittavien avainten luomiselle ja säilyttämiselle ja suojaa ja arvioi Touch ID:stä ja Face ID:stä saatavat biometriset tiedot.

Tallennettujen tietojen salaamisen on oltava nopeaa ja tehokasta. Samalla kuitenkin on tärkeää, että siinä ei paljasteta tietoja (tai avainmateriaalia), joita käytetään salausavainten suhteiden luomiseen. Laitteiston AES-moottori ratkaisee tämän ongelman suorittamalla nopeasti salauksen ja salauksen purkamisen tiedostoja kirjoitettaessa tai luettaessa. AES-moottori saa tarvitsemansa avainmateriaalin Secure Enclavelta erityistä kanavaa pitkin siten, ettei se voi paljastua appeja suorittavalle prosessorille (tai keskusprosessorille) tai käyttöjärjestelmälle. Näin taataan, että Applen tietojen suojaus ja FileVault suojaavat käyttäjien tiedostoja paljastamatta pitkäaikaisia salausavaimia.

Apple on suunnitellut suojatun käynnistyksen suojatakseen ohjelmiston alimpia kerroksia peukaloinnilta ja salliakseen vain Applen luotettavien käyttöjärjestelmä-ohjelmistojen latauksen käynnistämisen yhteydessä. Suojattu käynnistys alkaa muuttumattomasta koodista nimeltä Boot ROM, joka asennetaan Applen järjestelmäsiruun sen valmistuksen aikana. Tämä laitetason RoT-koodi (Root of Trust) on ehdottoman luotettava. T2-sirulla varustetuissa Mac-tietokoneissa macOS:n suojatun käynnistyksen luottamus alkaa T2-sirusta. (Sekä T2-siru että Secure Enclave suorittavat myös omat suojatut käynnistysprosessinsa käyttäen omaa erillistä Boot ROM -koodiaan. Tämä vastaa täsmälleen A-sarjan sirujen ja M1-sirujen suojattua käynnistystä.)

Secure Enclave prosessoi myös Touch ID- ja Face ID -tunnistimien sormenjälki- ja kasvotiedot Applen laitteissa. Tämä mahdollistaa turvallisen todennuksen, jossa käyttäjän biometriset tiedot pysyvät yksityisinä ja suojattuina. Samalla käyttäjät voivat asettaa turvallisia, pidempiä ja monimutkaisempia pääsykoodeja ja salasanoja, koska he voivat kuitenkin käyttää nopeaa todennusta monissa kirjautumis- tai ostotilanteissa.

Ainoastaan Applen tarjoama sirusuunnittelun, laitteiston, ohjelmiston ja palvelujen yhdistelmä mahdollistaa nämä Applen laitteiden suojausominaisuudet.

Järjestelmän suojaus
Applen laitteistojen ainutlaatuisille ominaisuuksille pohjautuva järjestelmän suojaus hallitsee pääsyä Applen laitteiden järjestelmäresursseihin käytettävyydestä tinkimättä. Järjestelmän suojaus kattaa käynnistysprosessin, ohjelmistopäivitykset sekä suojauksen, joka huolehtii tietokonejärjestelmän resursseista kuten prosessorista, muistista, levystä, ohjelmistoista ja tallennetuista tiedoista.

Applen käyttöjärjestelmien uusimmat versiot ovat kaikkein turvallisimmat. Yksi Applen suojauksen tärkeistä osista on suojattu käynnistys, joka suojelee järjestelmää haittaohjelmilta käynnistyksen aikana. Suojattu käynnistys alkaa laitteistosta ja muodostaa ohjelmistoon luottamusketjun. Siinä jokaisessa vaiheessa varmistetaan, että seuraava toimii oikein, ennen kuin hallinta siirretään. Tämä suojausmalli turvaa Applen laitteiden tavallisen käynnistyksen lisäksi niiden eri palautustiloja ja oikea-aikaista päivittämistä. Alikomponentit, kuten T2-siru ja Secure Enclave, suorittavat myös oman suojatun käynnistyksensä sen varmistamiseksi, että ne käynnistävät vain Applen hyväksi tiedetyn koodin. Päivitysjärjestelmällä voidaan jopa estää heikennyshyökkäyksiä, eli laitteita ei voida palauttaa käyttöjärjestelmän aiempaan versioon (jonka hyökkääjä kykenee vaarantamaan) käyttäjän tietojen varastamista varten.

Käynnistyksen suojaus ja ajonaikainen suojaus turvaavat Applen laitteiden järjestelmän eheyden jatkuvassa käytössä. iPhonessa, iPadissa, Apple Watchissa, Apple TV:ssä ja HomePodissa sekä Apple Siliconilla varustetussa Macissa olevat Applen suunnittelemat sirut muodostavat yhteisen arkkitehtuurin käyttöjärjestelmän eheyden suojaamista varten. macOS:ssä on lisäksi laajennettu ja muokattava joukko suojausominaisuuksia sen erilaista tietojenkäsittelymallia varten sekä kaikilla Mac-laitteistoalustoilla tuettuja ominaisuuksia.

Salaus ja tietojen suojaus
Applen laitteissa on salausominaisuuksia, joilla suojataan käyttäjien tietoja ja mahdollistetaan etätyhjennys, jos laite varastetaan tai se katoaa.

Suojatun käynnistysketjun, järjestelmän suojauksen ja appien suojauksen ominaisuudet auttavat varmistamaan, että laitteessa suoritetaan vain luotettua koodia ja appeja. Applen laitteissa on lisäksi salausominaisuuksia, jotka suojaavat käyttäjän tietoja silloinkin, kun muut suojausinfrastruktuurin osat ovat vaarantuneet (esimerkiksi jos laite katoaa tai jos siinä suoritetaan ei-luotettua koodia). Kaikki nämä ominaisuudet hyödyttävät sekä käyttäjiä että IT-ylläpitäjiä, sillä henkilökohtaiset ja yrityksen tiedot ovat suojattuina, ja jos laite varastetaan tai se katoaa, saatavilla on menetelmiä, joilla se voidaan tyhjentää välittömästi ja täydellisesti etänä.

iOS- ja iPadOS-laitteissa käytetään tietojen suojaukseksi kutsuttua tiedostojen salausmenetelmää. Intel-pohjaisten Mac-tietokoneiden tiedot puolestaan suojataan FileVault-nimisellä taltionsalausteknologialla. Apple Siliconilla varustettu Mac käyttää hybridimallia. Se tukee tietojen suojausta, joka kuitenkin eroaa muiden laitteiden tietojen suojauksesta kahdella tavalla: alinta suojaustasoa (D-luokka) ei tueta ja oletustaso (C-luokka) käyttää taltioavainta ja toimii samalla tavalla kuin Intel-pohjaisen Macin FileVault. Kaikissa tapauksissa avaintenhallintahierarkioiden juurihakemisto on Secure Enclaven erillisessä sirussa, ja erillinen AES-moottori tukee linjanopeudella toimivaa salausta ja auttaa varmistamaan, että pitkäaikaiset salausavaimet eivät paljastu kernelin käyttöjärjestelmälle tai prosessorille (missä ne voisivat vaarantua). (Intel-pohjaisessa Macissa, jossa on T1-siru tai jossa ei ole Secure Enclavea, ei käytetä erillistä sirua FileVault-salausavainten suojaamiseen.)

Sen lisäksi, että luvatonta tietojen käyttöä torjutaan tietojen suojauksella ja FileVaultilla, myös Applen käyttöjärjestelmän kernelit huolehtivat osaltaan suojauksesta ja tietoturvasta. Kernel käyttää pääsynhallintaa appien sandbox-eristykseen (mikä rajoittaa apin käytössä olevia tietoja) sekä tietosäiliöksi kutsuttavaa mekanismia (joka rajoittaa pääsyä apin tietoihin kaikilta muilta pääsyä pyytäviltä apeilta sen sijaan, että rajoitettaisiin pyyntöjä, joita appi voi tehdä).

Appien suojaus
Apit ovat suojausarkkitehtuurin kriittisimpiä elementtejä. Ne tarjoavat käyttäjille merkittävää hyötyä työskentelyssä, mutta saattavat myös vaikuttaa vahingollisesti järjestelmän suojaukseen, vakauteen ja käyttäjän tietoihin, jos niitä ei käsitellä oikein.

Tämän takia Apple käyttää useita suojaustasoja, jotta voidaan varmistaa, ettei apeissa ole tunnettuja haittaohjelmistoja eikä niitä ole peukaloitu. Lisäksi suojauksilla pidetään huoli siitä, että appien pääsy käyttäjien tietoihin on tarkasti rajoitettu. Nämä suojaukset takaavat vakaan ja turvallisen alustan apeille sekä mahdollistavat sen, että tuhannet kehittäjät voivat tarjota satojatuhansia appeja iOS:lle, iPadOS:lle ja macOS:lle järjestelmän eheyttä vaarantamatta. Käyttäjät voivat käyttää näitä appeja Applen laitteissaan pelkäämättä turhaan viruksia, haittaohjelmistoja tai luvattomia hyökkäyksiä.

iPhonessa, iPadissa ja iPod touchissa kaikki apit hankitaan App Storesta, ja ne kaikki eristetään omaan sandbox-ympäristöön mahdollisimman tiukan suojauksen varmistamiseksi.

Macissa monet apit hankitaan App Storesta, mutta lisäksi Mac-käyttäjät lataavat ja käyttävät internetistä peräisin olevia appeja. macOS tarjoaakin enemmän suojaustasoja internet-latauksia varten. Oletuksena macOS 10.15:ssä tai uudemmissa versioissa kaikkien Mac-appien on oltava Applen oikeiksi todistamia, jotta ne voidaan käynnistää. Tämä vaatimus auttaa varmistamaan, että näissä

apeissa ei ole tunnettuja haittaohjelmistoja, mutta ei kuitenkaan edellytä, että apit hankitaan aina App Storen kautta. Lisäksi macOS sisältää huippuluokan virustorjunnan, joka estää ja tarvittaessa poistaa haittaohjelmistoja.

Sandbox-eristys toimii lisäsuojana kaikilla alustoilla ja auttaa suojaamaan käyttäjän tietoja siltä, että apit käyttäisivät niitä ilman lupaa. macOS:ssä on myös suojattu kriittisten alueiden tiedot. Tämä suojaus auttaa varmistamaan, että käyttäjät hallitsevat kaikkien appien pääsyä Työpöytä-, Dokumentit- ja Lataukset-kansioiden sekä muiden alueiden tiedostoihin riippumatta siitä, onko pääsyä yrittävät apit sandbox-eristetty vai ei.

Palveluiden suojaus
Applella on laaja valikoima palveluita, joiden avulla käyttäjät saavat vielä enemmän hyötyä laitteistaan. Ne tarjoavat tehokkaita ominaisuuksia pilvitallennukseen, synkronointiin, salasanojen tallennukseen, todennukseen, maksamiseen, viestintään ja muuhun suojaten samalla käyttäjien yksityisyyttä ja tietoja.

Näihin palveluihin kuuluvat iCloud, Kirjaudu sisään Applella, Apple Pay, iMessage, Yrityschat, FaceTime, Missä on…? ja Jatkuvuus, ja ne saattavat vaatia Apple ID:n tai hallitun Apple ID:n. Joissakin tapauksissa hallittua Apple ID:tä ei voida käyttää tietyssä palvelussa, kuten Apple Payssa.

Huomaa: Kaikki Applen palvelut ja sisältö eivät ole saatavilla kaikissa maissa tai kaikilla alueilla.

Verkkoliikenteen suojauksen yleiskatsaus
Apple käyttää sisäänrakennettuja suojausominaisuuksia Applen laitteisiin tallennettujen tietojen suojaamiseen. Niiden lisäksi organisaatiot voivat käyttää monenlaisia keinoja suojatakseen laitteisiin saapuvia ja niistä lähteviä tietoja. Kaikki nämä suojausominaisuudet ja keinot kuuluvat verkkoliikenteen suojaukseen.

Käyttäjillä on oltava mahdollisuus käyttää yritysverkkoja kaikkialta maailmasta. On siis tärkeää varmistaa, että heillä on valtuutus tähän ja että heidän tietonsa suojataan siirron aikana. Luotettaviksi osoittautuneet teknologiat ja uusimmat standardit sekä Wi-Fi- että mobiilidataverkkojen yhteyksille mahdollistavat näiden tietoturvan vaatimusten toteuttamisen iOS:ssä, iPadOS:ssä ja macOS:ssä. Siksi käyttöjärjestelmämme käyttävät standardien mukaisia verkkoprotokollia todennettuun, valtuutettuun ja salattuun viestintään ja tarjoavat kehittäjillekin pääsyn niihin.

Tutustu tarkemmin Applen laitteiden tietoturvaan:

apple.com/fi/business/it

apple.com/macos/security

apple.com/privacy/features

apple.com/security

Kumppaniekosysteemi
Applen laitteet toimivat yhdessä yritysten yleisten tietoturvatyökalujen ja -palveluiden kanssa varmistaen laitteiden ja niissä olevien tietojen vaatimustenmukaisuuden. Kukin alusta tukee tavallisia VPN-protokollia (mukaan lukien iOS ja iPadOS 14:n tilikohtaiset VPN-yhteydet) ja turvallisia Wi-Fi-protokollia, jotka suojaavat verkkoliikenteen ja muodostavat tietoturvallisen yhteyden yrityksen yhteiseen infrastruktuuriin.

Applen tekee yhteistyötä Ciscon kanssa, jotta ne voivat voimansa yhdistämällä tarjota parempaa suojausta ja työtehoa. Ciscon verkot tarjoavat parannetun suojauksen Cisco Security Connectorilla ja priorisoivat yritysapit etusijalle.