Apple at Work

Alustojen suojaus

Suunniteltu turvalliseksi.

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

Laitteiston suojaus
Suojattu ohjelmisto vaatii pohjalleen suojausta, joka on sisäänrakennettu laitteistoon. Siksi Applen laitteissa, joissa on iOS, iPadOS, macOS, tvOS tai watchOS, on suojausominaisuuksia aivan laitteistotasolla.

Näitä ovat prosessorin muokatut ominaisuudet, jotka mahdollistavat järjestelmän suojausominaisuudet ja suojaustoiminnoille tarkoitetun sirun. Tärkein komponentti on Secure Enclave -apuprosessori moderneissa iOS-, iPadOS-, watchOS- ja tvOS-laitteissa ja kaikissa Mac-tietokoneissa, joissa on Apple T2 Security -siru. Secure Enclave luo pohjan tietojen salaukselle levossa, suojatulle käynnistykselle macOS:ssä ja biometrisille tiedoille.

Kaikissa moderneissa iPhone- ja iPad-laitteissa sekä Mac-tietokoneissa, joissa on T2-siru, on erillinen AES-laiteohjelma, joka mahdollistaa mahdollisimman nopean salauksen, kun tiedostoja kirjoitetaan tai luetaan. Tämä takaa, että tietojen suojaus ja FileVault suojaavat käyttäjien tiedostoja paljastamatta pitkäaikaisia salausavaimia prosessorille tai käyttöjärjestelmälle.

Apple-laitteiden suojattu käynnistys varmistaa, että ohjelmiston alimpia tasoja ei ole peukaloitu ja että vain Applen luotettu käyttöjärjestelmäohjelmisto latautuu käynnistyksessä. iOS- ja iPadOS-laitteissa tietoturva alkaa Boot ROM -nimisestä muuttumattomasta koodista, joka asennetaan sirun valmistuksen aikana ja joka tunnetaan laitteiston luottamuksen perustana. Mac-tietokoneissa, joissa on T2-siru, suojatun käynnistyksen luottamus alkaa itse Secure Enclavesta.

Secure Enclaven ansiosta Applen laitteiden Touch ID ja Face ID voivat tarjota suojatun todentautumisen. Samalla ne pitävät käyttäjän biometriset tiedot yksityisinä ja suojattuina. Tämän ansiosta käyttäjät voivat hyödyntää pidempien ja monimutkaisempien pääsykoodien ja salasanojen tarjoamaa tietoturvaa sekä monissa tilanteissa nopean todentautumisen kätevyyttä.

Applen laitteiden suojausominaisuudet mahdollistaa vain Applelta saatavilla oleva yhdistelmä sirun suunnittelua, laitteistoa, ohjelmistoa ja palveluja.

Järjestelmän suojaus
Applen laitteiston ainutlaatuisille ominaisuuksille pohjautuva järjestelmän suojaus on suunniteltu maksimoimaan Applen laitteiden suojaus käytettävyydestä tinkimättä. Järjestelmän suojaukseen sisältyvät käynnistysprosessi, ohjelmistopäivitykset ja käyttöjärjestelmän jatkuva toiminta.

Suojattu käynnistys alkaa laitteistosta ja muodostaa ohjelmistoon luottamusketjun. Siinä jokaisella vaiheella varmistetaan, että seuraava toimii oikein, ennen kuin hallinta siirretään. Tämä suojausmalli tukee Apple-laitteiden oletuskäynnistyksen lisäksi iOS-, iPadOS- ja macOS-laitteiden eri palautus- ja päivitystiloja.

iOS:n, iPadOS:n ja macOS:n uusimmat versiot ovat kaikkein turvallisimmat. Ohjelmiston päivitysmekanismi ei ainoastaan tarjoa oikea-aikaisia päivityksiä Applen laitteisiin, vaan se tarjoaa myös ainoat luotetut ohjelmistot Applelta. Päivitysjärjestelmä voi myös estää heikennyshyökkäyksiä, jotta laitteita ei voida palauttaa käyttöjärjestelmän aiempaaan versioon käyttäjätietojen varastamisen keinona.

Apple-laitteet sisältävät käynnistyksen ja ajonaikaisen suojauksen, jotta ne säilyttävät eheytensä jatkuvan toiminnan aikana. Nämä suojaukset vaihtelevat merkittävästi iOS-, iPadOS- ja macOS-laitteiden välillä, koska ne tukevat eri ominaisuuksia, jolloin niiden täytyy estää erilaisia hyökkäyksiä.

Jotta voidaan saavuttaa tämä suojauksen taso, iOS:ssä ja iPadOS:ssä on käytössä kernelin eheyden suojaus (KIP), järjestelmän apuprosessorin eheyden suojaus (SCIP), PAC-koodit (Pointer Authentication Codes) ja sivun suojauskerros (PPL). macOS:ssä on puolestaan käytössä seuraavat: UEFI-suojaus (Unified Extensible Firmware Interface), järjestelmänhallintatila (SSM), suoran muistin käytön (DMA) suojaukset ja oheislaitteiden laiteohjelmiston suojaus.

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 lisäsalausominaisuuksia, 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 aina suojattuina, ja jos laite varastetaan tai se katoaa, saatavilla on menetelmiä, joilla se voidaan tyhjentää välittömästi kokonaan etänä.

iOS- ja iPadOS-laitteissa käytetään tietojen suojaukseksi kutsuttua tiedostojen salausmenetelmää. Mac-tietokoneiden tiedot puolestaan suojataan FileVault-nimisellä taltionsalausteknologialla. Molempien mallien avaintenhallintahierarkian juurihakemisto on samalla tavalla Secure Enclaven erillisessä sirussa laitteissa, joissa on SEP. Molemmat mallit hyödyntävät erillistä AES-ohjelmaa tukeakseen linjanopeaa salausta ja varmistaakseen, että pitkäaikaisia salausavaimia ei koskaan tarvitse tarjota kernelin käyttöjärjestelmälle tai prosessorille, jossa ne voisivat vaarantua.

Appien suojaus

Apit ovat modernin suojausarkkitehtuurin kriittisimpiä elementtejä. Apit tarjoavat käyttäjille merkittäviä tuottavuusetuja, mutta saattavat vaikuttaa myös negatiivisesti järjestelmän suojaukseen, vakauteen ja käyttäjätietoihin, jos niitä ei käsitellä oikein. Apple tarjoaa useita tasoja suojaa, jotta voidaan varmistaa, ettei apeissa ei ole tunnettuja haittaohjelmistoja eikä niitä ole peukaloitu. Muut suojaustoimenpiteet estävät pääsyn käyttäjän tietoihin appien kautta ja valvovat prosessia huolellisesti.

Sisäänrakennetut suojausrajoitukset tarjoavat vakaan ja suojatun alustan apeille sekä mahdollistavat sen, että tuhannet kehittäjät voivat tarjota satoja tuhansia appeja iOS:lle, iPadOS:lle ja macOS:lle vaikuttamatta järjestelmän eheyteen. Käyttäjät voivat käyttää näitä appeja Applen laitteillaan rajoitusten auttaessa suojautumaan viruksilta, haittaohjelmilta tai luvattomilta hyökkäyksiltä.

iPhonessa, iPadissa ja iPod touchissa kaikki apit hankitaan App Storesta, ja ne kaikki eristetään mahdollisimman tiukan suojauksen varmistamiseksi. Macissa monet apit hankitaan App Storesta, mutta lisäksi Mac-käyttäjät lataavat ja käyttävät appeja internetistä. macOS tarjoaa internet-latausta varten lisähallintaa suojaukseen. Oletuksena macOS 10.15:ssä tai uudemmissa versioissa kaikkien Mac-appien on oltava Applen oikeiksi todistamia, jotta ne voidaan käynnistää. Tällä vaatimuksella varmistetaan, että näissä apeissa ei ole tunnettuja haittaohjelmistoja edellyttämättä, että apit tarjottaisiin App Storen kautta. Lisäksi macOS:ään sisältyy alan standardien mukainen virusturva, joka estää ja tarvittaessa poistaa haittaohjelmat.

Sandbox-eristys toimii lisäsuojana alustoilla ja auttaa suojaamaan käyttäjätietoja siltä, että apit käyttäisivät niitä ilman lupaa. macOS:ssä kriittisten alueiden tiedot on eristetty, mikä takaa, että käyttäjillä on pääsy Työpöytä-, Dokumentit- ja Lataukset-kansioiden sekä muiden alueiden tiedostoihin kaikista apeista riippumatta siitä, onko pääsyä yrittäviä appeja eristetty vai ei.

Palveluiden suojaus

Applella on laaja valikoima palveluita, joiden avulla käyttäjät saavat laitteistaan irti enemmän hyötyä ja tuottavuutta. Näitä palveluita ovat esimerkiksi Apple ID, iCloud, Kirjaudu sisään Applella, Apple Pay, iMessage, FaceTime, Siri ja Missä on…? Nämä palvelut tarjoavat tehokkaita ominaisuuksia pilvitallennukseen ja synkronointiin, todentamiseen, maksamiseen, viestintään ja muuhun suojaten samalla käyttäjien yksityisyyttä ja tietoja.

Kumppaniekosysteemi

Applen laitteet toimivat yhdessä yrityksen yleisten tietoturvatyökalujen ja -palveluiden kanssa varmistaen laitteiden ja niissä olevien tietojen vaatimustenmukaisuuden. Kukin alusta tukee yleisiä protokollia VPN:ää ja turvallista Wi-Fiä varten suojaten verkkoliikenteen ja muodostaen turvallisen yhteyden yrityksen yleiseen infrastruktuuriin.

Applen kumppanuus yhdessä Ciscon kanssa tarjoaa parannetun suojauksen ja tuottavuuden. Ciscon verkot tarjoavat parannetun suojauksen Cisco Security Connectorin kautta ja antavat etusijan Ciscon verkkojen yrityskäytölle.

Tutustu Applen laitteiden suojaukseen:

apple.com/fi/business/it

apple.com/macos/security

apple.com/privacy/features

apple.com/fi/security