Apple at Work

Platformbiztonság

Alaptulajdonsága a biztonság.

Az Apple-nél különösen fontosnak tartjuk a biztonságot – a felhasználó és a vállalati adatok védelme szempontjából egyaránt. Már a kezdetektől fejlett biztonsági megoldásokat építettünk a termékeinkbe, hogy alaptulajdonságuk legyen a biztonság. Mindezt pedig úgy tettük, hogy közben megteremtettük az egyensúlyt a nagyszerű felhasználói élménnyel, és minden felhasználónak lehetővé tettük a szabad, saját stílusban történő munkavégzést. Csak az Apple képes ilyen átfogóan kezelni a biztonságot, mert termékeink integrált hardverekkel, szoftverekkel és szolgáltatásokkal rendelkeznek.

Hardverbiztonság
A biztonságos szoftverekhez biztos alapokon nyugvó hardverbiztonságra van szükség. Ezért rendelkeznek az – iOS, iPadOS, macOS, tvOS vagy watchOS rendszert futtató – Apple-eszközök hardveres biztonsági képességekkel.

Ezek rendszerbiztonsági funkciókat ellátó egyéni processzorképességeken és a biztonsági funkciókhoz dedikált hardvereken alapulnak. A legfontosabb összetevő a modern iOS, iPadOS, watchOS és tvOS rendszerű eszközökben, valamint az Apple T2 biztonsági chippel rendelkező Mac gépekben a Secure Enclave társprocesszor. A Secure Enclave biztosítja a tárolt adatok titkosítását, a macOS biztonságos rendszerindítását és a biometrikát.

Minden T2 chippel rendelkező iPhone, iPad és Mac gép dedikált AES-hardvermotort tartalmaz a fájlok írásának és olvasásának azonnali titkosításának biztosításához. Ez biztosítja, hogy az alkalmazásadatok védelme és a FileVault anélkül gondoskodhasson a felhasználók fájljainak védelméről, hogy megosztaná a hosszú életű titkosítási kulcsokat a processzorral vagy az operációs rendszerrel.

Az Apple-eszközök biztonságos rendszerindítása gondoskodik arról, hogy a legalacsonyabb szintű szoftverek ne legyenek illetéktelenül módosítva, valamint csak megbízható, Apple-től származó operációsrendszer-szoftver töltődjön be indításkor. Az iOS és iPadOS rendszerű eszközök biztonsága a Boot ROM nevű, nem módosítható kódnál kezdődik, amelynek beprogramozása a chipgyártás során történik, és a bizalom hardveres alapjaként ismert. A T2

chippel rendelkező Mac gépeken a biztonságos rendszerindítás iránti bizalom magával a Secure Enclave társprocesszorral kezdődik.

A Secure Enclave teszi lehetővé az Apple-eszközök Touch ID és Face ID funkciójának használatát, amelyek biztonságos hitelesítést nyújtanak, ugyanakkor gondoskodnak a felhasználó biometrikus adatainak bizalmasságáról és biztonságáról. Ez lehetővé teszi, hogy a felhasználók élhessenek a hosszabb és összetettebb kódok és jelszavak nyújtotta biztonsággal, a gyors hitelesítés kényelme mellett.

Az Apple-eszközök biztonsági funkcióit a hardveres tervezés, a hardverek és a szoftverek, valamint a csak az Apple-től elérhető szolgáltatások köre teszi lehetővé.

Rendszerbiztonság
A rendszerbiztonság az Apple-hardverek egyedi képességeire épít, és úgy lett kialakítva, hogy az Apple-eszközök operációs rendszerének biztonságát a használhatóság megőrzése mellett maximalizálja. A rendszerbiztonság a rendszerindítási folyamatot, a szoftverfrissítéseket és az operációs rendszer folyamatos működését foglalja magában.

A biztonságos rendszerindítás a hardverrel kezdődik, majd bizalmi láncot alakít ki a szoftveren keresztül, ahol az egyes lépések a vezérlés átadása előtt megbizonyosodnak arról, hogy a következő lépés megfelelően működik. A biztonsági modell nemcsak az Apple-eszközök alapértelmezett rendszerindítását támogatja, hanem az iOS, az iPadOS és a macOS rendszerű eszközök különböző helyreállítási és frissítési módjait is.

Az iOS, az iPadOS és a macOS legújabb verziói a legbiztonságosabbak. A szoftverfrissítési mechanizmus nemcsak időszerű frissítéseket biztosít az Apple-eszközöknek, hanem csak az Apple-től származó, megbízható szoftvereket is. A frissítési rendszer még a visszaállítási támadásokat is képes megakadályozni, így az eszközöket nem lehet visszaállítani az operációs rendszer korábbi verziójára a felhasználói adatok ellopása érdekében.

Végezetül az Apple-eszközök rendszerindítási és futásidejű védelmi mechanizmusokkal is rendelkeznek, így képesek megőrizni az integritásukat a folyamatban lévő műveletek során. Ezek a védelmi mechanizmusok jelentősen eltérnek az iOS, iPadOS és macOS rendszerű eszközök között a nagymértékben eltérő támogatott képességektől és az elhárítandó támadásoktól függően.

Az ilyen szintű védelem elérése érdekében az iOS és az iPadOS kernelintegritási védelmet, rendszertársprocesszor-védelmet, mutatóhitelesítési kódokat és lapozóvédelmi réteget használ, míg a macOS egységes bővíthető firmware-felületi biztonságot, rendszer-felügyeleti módot, közvetlen memória-hozzáférési védelmi mechanizmusokat és a perifériaeszközök firmware-védelmét használja.

Titkosítás és adatvédelem
Az Apple-eszközök titkosítási funkciókkal rendelkeznek a felhasználói adatok védelme, valamint az eszköz ellopása vagy elvesztése esetén az adatok távoli törlése érdekében.

A biztonságos rendszerindítási lánc, a rendszerbiztonság és az alkalmazásbiztonsági képességek mind segítenek annak biztosításában, hogy csak megbízható kódok és alkalmazások futhassanak az eszközön.

Az Apple-eszközök további titkosítási funkciókkal is rendelkeznek a felhasználói adatok védelme érdekében, még akkor is, ha a biztonsági infrastruktúra más részei sérültek – például ha az eszköz elveszett, vagy nem megbízható kódot futtat. Ezek a funkciók mind a felhasználók, mind az informatikai rendszergazdák számára hasznosak, mivel folyamatosan védik a személyes és vállalati adatokat, és olyan lehetőségekkel szolgálnak, amelyekkel azonnal és teljes mértékben törölhetők az adatok az eszköz ellopása vagy elvesztése esetén.

Az iOS és az iPadOS rendszerű eszközök az alkalmazásadatok védelméről gondoskodó fájltitkosítási módszert használják, míg a Mac gépeken lévő adatokat a FileVault nevű kötettitkosítási technológia védi. A két modell mindegyike a Secure Enclave dedikált hardverében tárolja a kulcsfontosságú felügyeleti hierarchiákat a SEP-et tartalmazó eszközökön. Emellett mindkét modell dedikált AES-motort használ az azonnali titkosítás támogatásához és annak biztosításához, hogy a hosszú életű titkosítási kulcsokat soha ne kelljen megadni az operációs rendszer vagy processzor rendszermagjának, ahol illetéktelenül módosíthatnák őket.

Alkalmazásbiztonság
A modern biztonsági architektúrák egyik legsérülékenyebb elemét az alkalmazások jelentik. Bár az alkalmazások nagyszerű előnyöket biztosítanak a termelékenység terén, a rendszerbiztonság, a stabilitás és a felhasználói adatok negatív befolyásolására is képesek nem megfelelő kezelés esetén. Az Apple által biztosított többrétegű védelem gondoskodik arról, hogy az alkalmazásokat ne fertőzzék meg az ismert kártevők, és ne módosítsák őket illetéktelenül. Az alkalmazások által tárolt felhasználói adatokhoz való hozzáférésre további védelmi mechanizmusok vonatkoznak, amelyek minden ponton támogatják a folyamatot.

A beépített biztonsági vezérlők stabil, biztonságos platformot biztosítanak az alkalmazásoknak, így lehetővé teszik, hogy fejlesztők ezrei alkalmazások százezreit hozzák létre az iOS, iPadOS és macOS rendszerhez – mindezt a rendszer integritásának befolyásolása nélkül. A felhasználók a vezérlők működése mellett férhetnek hozzá ezekhez az alkalmazásokhoz az Apple-eszközeiken, amelyek segítenek a vírusokkal, kártevőkkel és más illetéktelen támadásokkal szembeni védekezésben.

Az iPhone, iPad és iPod touch minden alkalmazása az App Store áruházból származik – és mindegyik munkapéldányosított – a legszigorúbb vezérlők biztosítása érdekében. A Mac gépeken számos alkalmazás származik az App Store áruházból, azonban a Mac-felhasználók az internetről is letölthetnek és használhatnak alkalmazásokat. Az internetes letöltés biztonságos támogatása érdekében a macOS rétegzi a további vezérlőket. Először is a macOS 10.15-ös és újabb verzióin az Apple-nek alapértelmezés szerint hitelesítenie kell a Mac-alkalmazásokat a futtatáshoz. Ez a követelmény gondoskodik arról, hogy az alkalmazások az ismert kártevőktől mentesek legyenek, azonban nem teszi kötelezővé, hogy az alkalmazások az App Store áruházból származzanak. Emellett a macOS iparági szabványoknak megfelelő vírusvédelmet biztosít a kártevők kivédéséhez, és ha szükséges, eltávolításához.

A munkapéldányosítás a platformok további vezérlőjeként segít megvédeni a felhasználói adatokat az alkalmazások általi illetéktelen hozzáféréstől. A macOS rendszerben a kritikus területek adatai munkapéldányosítva vannak, ami biztosítja, hogy az íróasztalon, a dokumentumokban, a letöltésekben és más területeken található adatokhoz való hozzáférés szabályozása a felhasználó kezében maradjon – függetlenül attól, hogy a hozzáférést megkísérlő alkalmazások munkapéldányosítva vannak-e vagy sem.

Szolgáltatásbiztonság

Az Apple hatékony szolgáltatásokkal segíti a felhasználókat, hogy még jobban ki tudják használni az eszközeiket, és még nagyobb termelékenységet érhessenek el. Ezek a szolgáltatások az Apple ID, az iCloud, a Bejelentkezés az Apple-lel, az Apple Pay, az iMessage, a FaceTime, a Siri és a Lokátor. Ezek a szolgáltatások hatékony képességeket nyújtanak a felhőalapú tárolás és szinkronizálás, a hitelesítés, a fizetés, az üzenetkezelés, a kommunikáció és sok más terület számára, mindezt a felhasználó személyes adatainak biztonságának megőrzése mellett.

Partner-ökoszisztéma

Az Apple-eszközök együttműködnek a gyakori vállalati biztonsági eszközökkel és szolgáltatásokkal, így biztosítják az eszközök és az azokon tárolt adatok megfelelőségét. Minden platform támogatja a szabványos VPN- és biztonságos Wi-Fi-protokollokat a hálózati forgalom védelme és az általános vállalati infrastruktúrához történő biztonságos csatlakozás érdekében.

Az Apple és a Cisco együttes használata esetén továbbfejlesztett biztonság és termelékenység érhető el. A Cisco hálózatai továbbfejlesztett biztonságot nyújtanak a Cisco Security Connectorral, és elsőbbséget biztosítanak a Cisco hálózatain lévő üzleti alkalmazásoknak.

További információk az Apple-eszközök biztonságáról.

apple.com/hu/business/it

apple.com/macos/security

apple.com/privacy/features

apple.com/hu/security