Bevezetés a kiberbiztonságba és biztonságtudatosság

Zero Trust Architecture (ZTA)

Szarvák Anikó

2023. Tavasz

NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Bevezetés

Egy tipikus vállalat infrastruktúrája egyre bonyolultabbá vált.

Egy vállalat több belső hálózatot, saját helyi infrastruktúrával rendelkező távoli irodát, távoli és/vagy mobil egyéneket, valamint felhőszolgáltatásokat üzemeltethet.

Ez az összetettség felülmúlta a határvédelem (perimeter) alapú hálózatbiztonság korábbi módszereit, mivel nincs egyetlen, könnyen azonosítható kerület a vállalat számára.

A határvédelem alapú hálózati biztonság sem bizonyult elégségesnek, mivel amint a támadók áttörik a kerületet, a további oldalirányú mozgás akadálytalan.

Bevezetés (folyt.)

A ZT nem egyetlen architektúra, hanem a munkafolyamat, a rendszertervezés és a műveletek vezérelvei, amelyek segítségével javítható bármilyen alkalmazó biztonsági szintje, helyzete [FIPS199].

A ZTA-ra való átállás egy utazás, arról szól, hogy egy szervezet miként értékeli a kockázatokat küldetése során, és ez nem valósítható meg egyszerűen a technológia cseréjével. Ennek ellenére sok szervezet vállalati infrastruktúrájában már ma is megtalálhatók a ZTA elemei.

A szervezeteknek törekedniük kell a ZTA bizalmi elvek, a folyamatváltozások és a technológiai megoldások fokozatos bevezetésére, amelyek felhasználási esetenként védik adatvagyonukat és üzleti funkcióikat.

A legtöbb vállalati infrastruktúra hibrid zéró bizalom/perem alapú üzemmódban fog működni, miközben továbbra is befektet az IT-korszerűsítési kezdeményezésekbe és javítja a szervezeti üzleti folyamatokat.

Alapvetések

A ZT egy kiberbiztonsági paradigma, amely az erőforrások védelmére összpontosít, és arra az előfeltevésre, hogy a bizalmat soha nem adják meg implicit módon, hanem folyamatosan értékelni kell.

A ZT architektúra a vállalati erőforrás- és adatbiztonság teljes körű megközelítése, amely magában foglalja az identitást (személyes és nem személyi entitások), a hitelesítő adatokat, a hozzáférés-kezelést, a műveleteket, a végpontokat, a tárhely-környezeteket és az összekapcsoló infrastruktúrát.

Arra kell összpontosítani, hogy az erőforrásokat azokra korlátozzák, akiknek csak a küldetés végrehajtásához szükséges minimális jogosultságokat (például olvasási, írási, törlési) kell hozzáférniük és megadniuk.

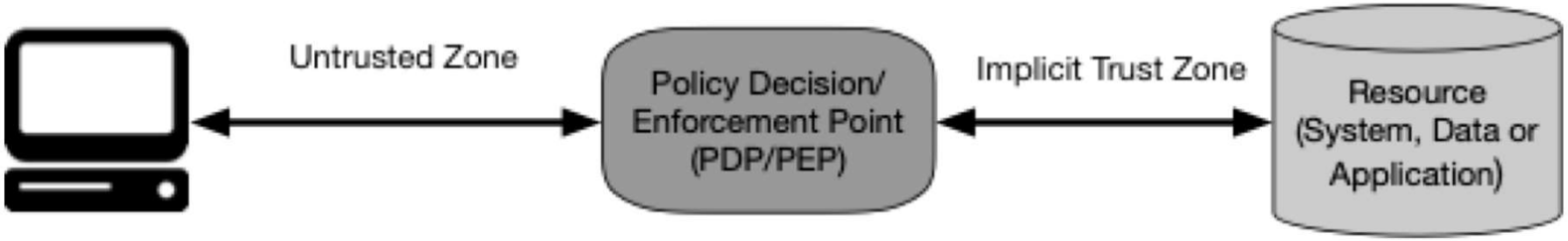

Figure 1: Zero Trust Access

ZTA tételek (folyt.)

1. Minden adatforrás és számítástechnikai szolgáltatás erőforrásnak minősül.

Egy hálózat több eszközosztályból is állhat.

A hálózatnak lehetnek kis helyigényű eszközei is, amelyek adatokat küldenek aggregátoroknak/tárolóknak, szoftvert szolgáltatásként (SaaS), utasításokat küldő rendszereket működtetőknek és egyéb funkciókat.

A vállalat dönthet úgy is, hogy a személyes tulajdonú eszközöket erőforrásként minősíti, ha hozzáfér a vállalati tulajdonú erőforrásokhoz.

ZTA tételek (folyt.)

2. A hálózat helyétől függetlenül minden kommunikáció biztonságos. A hálózati hely önmagában nem jelent bizalmat.

A vállalati tulajdonú hálózati infrastruktúrán (például egy régebbi hálózaton belül) elhelyezkedő eszközökből származó hozzáférési kérelmeknek ugyanazoknak a biztonsági követelményeknek kell megfelelniük, mint a hozzáférési kérelmeknek és a kommunikációnak bármely más, nem vállalati tulajdonú hálózatról. Más szavakkal, a megbízhatóságot nem szabad automatikusan megadni attól függően, hogy az eszköz a vállalati hálózati infrastruktúrán van.

Minden kommunikációt az elérhető legbiztonságosabb módon kell végrehajtani, védeni kell a bizalmasságot és az integritást, és biztosítani kell a forrás hitelesítését.

ZTA tételek (folyt.)

3. Az egyes vállalati erőforrásokhoz való hozzáférés munkamenetenkénti alapon történik.

A kérelmezőbe vetett bizalmat a rendszer a hozzáférés megadása előtt értékeli.

A hozzáférést a feladat elvégzéséhez szükséges legkevesebb jogosultsággal kell biztosítani. Ez csak azt jelentheti, hogy „valamikor mostanában” az adott tranzakcióhoz, és nem fordulhat elő közvetlenül a munkamenet kezdeményezése vagy az erőforrással való tranzakció végrehajtása előtt.

Az egyik erőforrás hitelesítése és engedélyezése azonban nem ad automatikusan hozzáférést egy másik erőforráshoz.

ZTA tételek (folyt.)

4. Az erőforrásokhoz való hozzáférést dinamikus házirend határozza meg – beleértve az ügyfélazonosság, az alkalmazás/szolgáltatás és a kérelmező eszköz megfigyelhető állapotát –, és más viselkedési és környezeti jellemzőket is tartalmazhat.

A szervezet az erőforrások védelmét azáltal védi, hogy meghatározza, milyen erőforrásokkal rendelkezik, kik a tagjai (vagy képesek-e hitelesíteni az egyesített közösségből származó felhasználókat), és milyen erőforrásokhoz van szükségük a tagoknak.

Az erőforrás-hozzáférési és műveleti engedélyek házirendjei az erőforrás/adat érzékenységétől függően változhatnak.

A legkisebb jogosultság elvét alkalmazzák a láthatóság és a hozzáférhetőség korlátozására.

ZTA tételek (folyt.)

5. A vállalat felügyeli és méri az összes tulajdonában lévő és kapcsolódó eszköz integritását és biztonsági helyzetét.

Egyetlen vagyontárgy sem eredendően megbízható.

A vállalat az erőforráskérés értékelésekor értékeli az eszköz biztonsági helyzetét.

A ZTA-t megvalósító vállalkozásnak létre kell hoznia egy folyamatos diagnosztikai és mérséklő (CDM) vagy hasonló rendszert az eszközök és alkalmazások állapotának figyelésére, és szükség esetén javításokat/javításokat kell alkalmaznia.

Ehhez is szükség van egy robusztus megfigyelési és jelentési rendszerre, amely alkalmas adatokat szolgáltat a vállalati erőforrások jelenlegi állapotáról.

ZTA tételek (folyt.)

6. Minden erőforrás-hitelesítés és engedélyezés dinamikus, és a hozzáférés engedélyezése előtt szigorúan betartandó.

Ez a hozzáférés megszerzésének, a fenyegetések vizsgálatának és értékelésének, az alkalmazkodásnak és a folyamatos kommunikációba vetett bizalom folyamatos újraértékelésének állandó ciklusa.

A ZTA-t megvalósító vállalattól elvárható, hogy rendelkezzen Identity, Credential és Access Management (ICAM) és eszközkezelési rendszerekkel.

Ez magában foglalja a többtényezős hitelesítés (MFA) használatát egyes vagy az összes vállalati erőforráshoz való hozzáféréshez.

ZTA tételek (folyt.)

7. A vállalkozás a lehető legtöbb információt összegyűjti az eszközök aktuális állapotáról, a hálózati infrastruktúráról és a kommunikációról, és ezt felhasználja biztonsági helyzetének javítására.

A vállalatnak adatokat kell gyűjtenie az eszközök biztonsági helyzetéről, a hálózati forgalomról és a hozzáférési kérelmekről, fel kell dolgoznia ezeket az adatokat, és minden megszerzett betekintést fel kell használnia a szabályzat létrehozásának és betartatásának javítására.

Ezek az adatok felhasználhatók arra is, hogy kontextust biztosítsanak az alanyok hozzáférési kérelmeihez.

ZTA Hálózati nézete

1. A teljes vállalati magánhálózat nem tekinthető implicit bizalmi zónának.

Az eszközöknek mindig úgy kell viselkedniük, mintha támadó lenne jelen a vállalati hálózaton, és a kommunikációt a lehető legbiztonságosabb módon kell végezni (lásd a fenti 2. tételt).

Ez olyan műveletekkel jár, mint az összes kapcsolat hitelesítése és az összes forgalom titkosítása.

ZTA Hálózati nézete (folyt.)

2. Előfordulhat, hogy a hálózaton lévő eszközök nem lehetnek a vállalat tulajdonában és nem konfigurálhatók.

A látogatók és/vagy a szerződéses szolgáltatások tartalmazhatnak nem vállalati tulajdonú eszközöket, amelyeknek hálózati hozzáférésre van szükségük szerepük ellátásához.

Ebbe beletartoznak a „hozd saját eszközöd” (BYOD) házirendek, amelyek lehetővé teszik a vállalati alanyok számára, hogy nem vállalati tulajdonú eszközöket használjanak a vállalati erőforrásokhoz.

ZTA Hálózati nézete (folyt.)

3. Egyetlen erőforrás sem eleve megbízható.

Minden eszköz biztonsági helyzetét PEP segítségével ki kell értékelni, mielőtt egy vállalati tulajdonú erőforráshoz adnak egy kérelmet.

Ennek az értékelésnek folyamatosnak kell lennie mindaddig, amíg az ülés tart.

A vállalati tulajdonú eszközök tartalmazhatnak olyan melléktermékeket, amelyek lehetővé teszik a hitelesítést, és magasabb megbízhatósági szintet biztosítanak, mint a nem vállalati tulajdonú eszközökről érkező kérés.

Az alany hitelesítő adatai önmagukban nem elegendőek az eszköz hitelesítéséhez egy vállalati erőforráshoz.

ZTA Hálózati nézete (folyt.)

4. Nem minden vállalati erőforrás található a vállalati infrastruktúrán.

Az erőforrások közé tartoznak a távoli vállalati témák, valamint a felhőszolgáltatások.

Előfordulhat, hogy a vállalati tulajdonú vagy kezelt eszközöknek a helyi (azaz nem vállalati) hálózatot kell használniuk az alapvető csatlakozásokhoz és hálózati szolgáltatásokhoz (például DNS-feloldáshoz).

ZTA Hálózati nézete (folyt.)

5. A távoli vállalati alanyok és eszközök nem bízhatnak teljes mértékben a helyi hálózati kapcsolatukban.

A távoli személyeknek feltételezniük kell, hogy a helyi (azaz nem vállalati tulajdonú) hálózat ellenséges.

Az eszközöknek feltételezniük kell, hogy az összes forgalmat figyelik és potenciálisan módosítják.

Minden csatlakozási kérelmet hitelesíteni és engedélyeztetni kell, és minden kommunikációt a lehető legbiztonságosabb módon kell végrehajtani (azaz biztosítani kell a bizalmas kezelést, az integritás védelmét és a forráshitelesítést).

ZTA Hálózati nézete (folyt.)

6. A vállalati és nem vállalati infrastruktúra között mozgó eszközöknek és munkafolyamatoknak következetes biztonsági politikával és helyzettel kell rendelkezniük.

Az eszközöknek és a munkaterheléseknek meg kell őrizniük biztonsági helyzetüket, amikor a vállalati tulajdonú infrastruktúrába vagy onnan költöznek.

Ez magában foglalja azokat az eszközöket, amelyek a vállalati hálózatokból nem vállalati hálózatokba lépnek át (azaz távoli felhasználók).

Ez magában foglalja a helyszíni adatközpontokból a nem vállalati felhőpéldányokba migráló munkaterheléseket is.

Házirend motor (PE)

Ez a komponens felelős a végső döntésért, hogy hozzáférést biztosítanak-e egy adott téma erőforrásához.

A PE vállalati szabályzatot, valamint külső forrásokból (pl. CDM-rendszerekből, alább ismertetett fenyegetés-felderítő szolgáltatásokból) származó bemenetet használ egy megbízhatósági algoritmus bemeneteként az erőforráshoz való hozzáférés megadására, megtagadására vagy visszavonására.

A PE párosítva van a házirend-rendszergazda összetevővel.

A házirend-motor hozza meg és naplózza a döntést (jóváhagyva vagy elutasítva), a házirend-adminisztrátor pedig végrehajtja a döntést.

Házirend-adminisztrátor (PA)

Ez az összetevő felelős az alany és az erőforrás közötti kommunikációs útvonal létrehozásáért és/vagy leállításáért (a megfelelő PEP-ekhez küldött parancsokon keresztül).

Ez létrehozna minden munkamenet-specifikus hitelesítési és hitelesítési tokent vagy hitelesítő adatot, amelyet az ügyfél a vállalati erőforrás eléréséhez használ.

Szorosan kötődik a PE-hez, és annak döntésére támaszkodik, hogy végül engedélyezi vagy megtagadja a munkamenetet.

- Ha a munkamenet engedélyezett, és a kérés hitelesített, a PA konfigurálja a PEP-t, hogy lehetővé tegye a munkamenet elindítását.
- Ha a munkamenetet megtagadják (vagy egy korábbi jóváhagyást ellensúlyoznak), a PA jelzi a PEP-nek a kapcsolat leállítását.

Egyes megvalósítások a PE-t és a PA-t egyetlen szolgáltatásként kezelhetik; itt fel van osztva annak két logikai komponens.

Irányelv-végrehajtási pont (PEP)

Ez a rendszer felelős az alany és a vállalati erőforrás közötti kapcsolatok engedélyezéséért, figyeléséért és esetlegesen megszüntetéséért.

A PEP kommunikál a PA-val a kérelmek továbbítása és/vagy az irányelv-frissítések fogadása érdekében.

Ez egyetlen logikai komponens a ZTA-ban, de két különböző összetevőre bontható: a kliens (pl. ügynök a laptopon) és az erőforrás oldal (pl. a hozzáférést vezérlő erőforrás előtti átjáró komponens) vagy egyetlen portálkomponens, amely működik. mint a kommunikációs utak kapuőre.

A PEP-n túl található a vállalati erőforrást kiszolgáló bizalmi zóna.

ZTA elemei

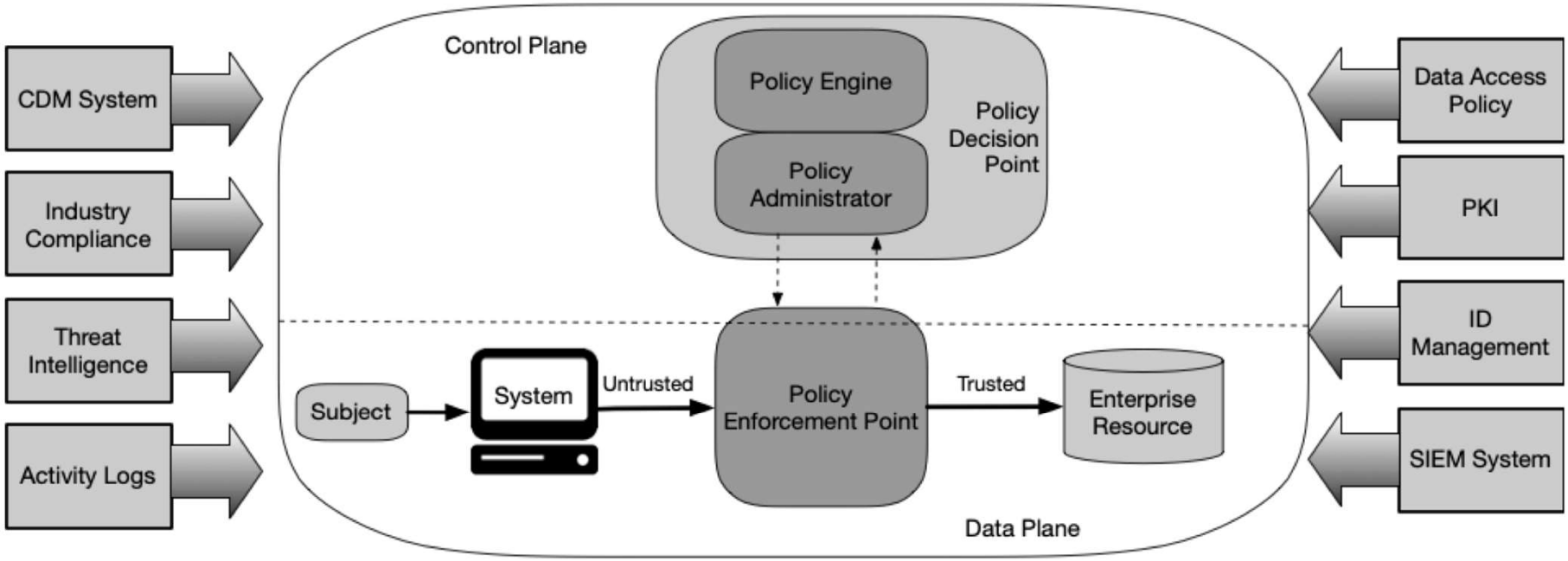

Figure 2: Core Zero Trust Logical Components

Folyamatos diagnosztikai és kockázatcsökkentő (CDM) rendszer

Ez információkat gyűjt a vállalati eszköz aktuális állapotáról, és frissítéseket hajt végre a konfigurációs és szoftverösszetevőkre.

A vállalati CDM-rendszer információkat nyújt a házirend-motor számára a hozzáférési kérelmet benyújtó eszközről, például arról, hogy fut-e a megfelelő javított operációs rendszer (OS), a vállalati jóváhagyott szoftverösszetevők integritása vagy a nem jóváhagyott összetevők jelenléte és hogy az eszköznek van-e ismert sebezhetősége.

A CDM-rendszerek felelősek a házirendek egy részhalmazának azonosításáért és esetleges érvényesítéséért is a vállalati infrastruktúrán aktív, nem vállalati eszközökön.

Iparági megfelelőségi rendszer

Ez biztosítja, hogy a vállalkozás továbbra is megfeleljen minden olyan szabályozási rendszernek, amely alá eshet (pl. FISMA, egészségügyi vagy pénzügyi ágazat információbiztonsági követelményei).

Ez magában foglalja az összes szabályzatot, amelyet a vállalat a megfelelés biztosítására dolgoz ki.

Fenyegetés-információs hírfolyam(ok)

Belső vagy külső forrásokból származó információkat biztosít, amelyek segítik a házirend-motort a hozzáférési döntések meghozatalában.

Ezek több szolgáltatás is lehetnek, amelyek belső és/vagy több külső forrásból vesznek adatokat, és információkat szolgáltatnak az újonnan felfedezett támadásokról vagy sebezhetőségekről.

Ez magában foglalja a szoftverben újonnan felfedezett hibákat, az újonnan azonosított rosszindulatú programokat és az egyéb eszközök elleni jelentett támadásokat is, amelyekhez a házirend-motor meg akarja tagadni a hozzáférést a vállalati eszközöktől.

Hálózati és rendszertevékenységi naplók

Ez a vállalati rendszer összesíti az eszköznaplókat, a hálózati forgalmat, az erőforrás-hozzáférési műveleteket és egyéb eseményeket, amelyek valós idejű (vagy közel valós idejű) visszajelzést adnak a vállalati információs rendszerek biztonsági helyzetéről.

Adathozzáférési szabályzatok

Ezek a vállalati erőforrásokhoz való hozzáférésre vonatkozó attribútumok, szabályok és szabályzatok.

Ez a szabálykészlet kódolható (a felügyeleti felületen keresztül) vagy dinamikusan generálható a házirend-motor által.

Ezek a házirendek jelentik az erőforrásokhoz való hozzáférés engedélyezésének kiindulópontját, mivel alapvető hozzáférési jogosultságokat biztosítanak a vállalati fiókokhoz és alkalmazásokhoz/szolgáltatásokhoz.

Ezeknek a politikáknak a szervezet meghatározott küldetési szerepein és igényein kell alapulniuk.

Vállalati nyilvános kulcsú infrastruktúra (PKI)

Ez a rendszer felelős a vállalat által erőforrásoknak, alanyoknak, szolgáltatásoknak és alkalmazásoknak kiadott tanúsítványok létrehozásáért és naplózásáért.

Ez magában foglalja a globális tanúsító hatóság ökoszisztémáját és a szövetségi PKI-t is,4 amely lehet integrálva a vállalati PKI-vel, de lehet, hogy nem.

Ez egy olyan PKI is lehet, amely nem X.509-tanúsítványokra épül.

Azonosítókezelő rendszer

Ez felelős a vállalati felhasználói fiókok és identitásrekordok létrehozásáért, tárolásáért és kezeléséért (pl. könnyű címtárelérési protokoll (LDAP) szerver).

Ez a rendszer tartalmazza a szükséges tárgyinformációkat (pl. név, e-mail cím, tanúsítványok) és egyéb vállalati jellemzőket, például szerepkört, hozzáférési attribútumokat és hozzárendelt eszközöket.

Ez a rendszer gyakran más rendszereket (például PKI-t) használ a felhasználói fiókokhoz társított műtermékekhez.

Ez a rendszer egy nagyobb szövetségi közösség része lehet, és nem vállalati alkalmazottakat vagy nem vállalati eszközökre mutató hivatkozásokat tartalmazhat az együttműködés érdekében.

Biztonsági információ- és eseménykezelő (SIEM) rendszer

Ez biztonsági központú információkat gyűjt a későbbi elemzéshez.

Ezeket az adatokat azután a házirendek finomítására és a vállalati eszközök elleni lehetséges támadásokra való figyelmeztetésre használják.

Példa ZTA

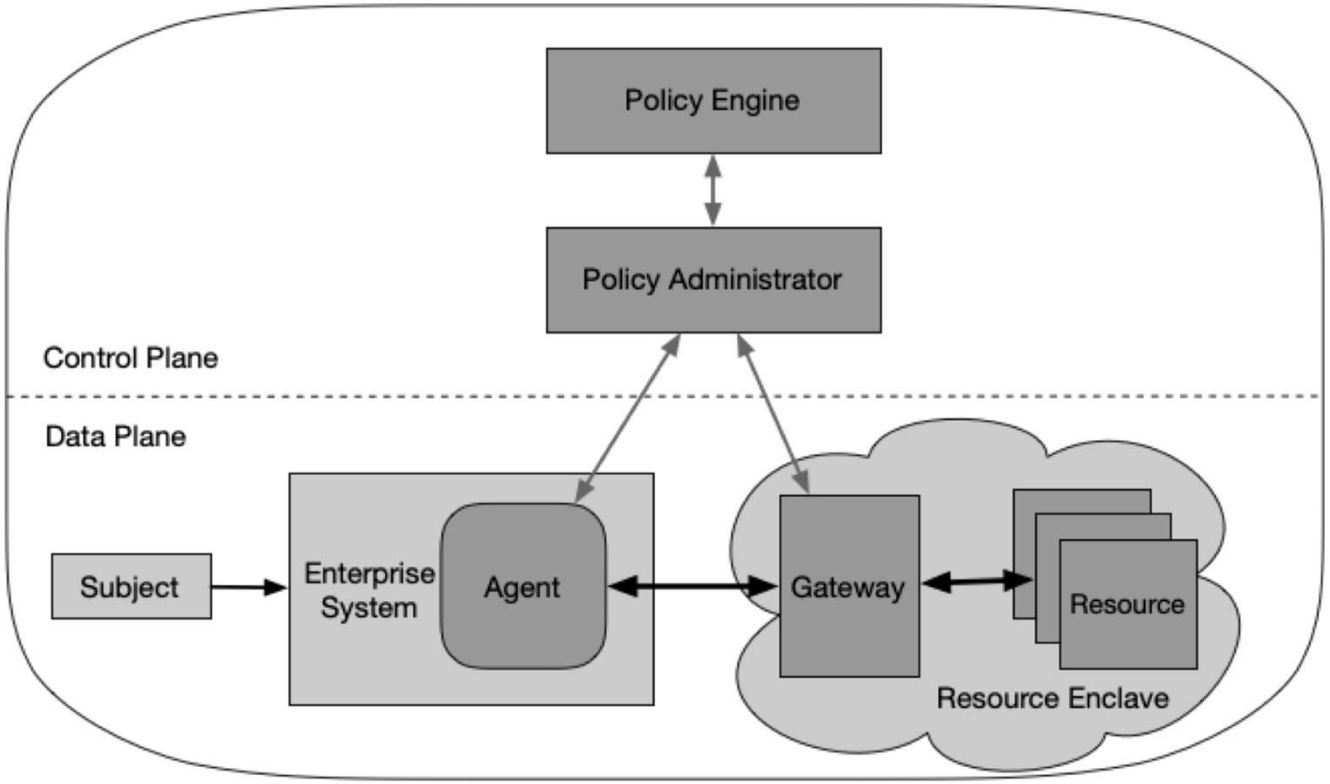

Figure 4: Enclave Gateway Model