

Cisco Umbrella

Felhő-alapú biztonsági platform

ÁTTEKINTÉS

A Cisco Umbrella egy felhő-alapú security megoldás, amely a védelem első vonalát jelenti a felhasználók számára csatlakozzanak bárhol is az Internetre. A Cisco globálisan telepített infrastruktúrája 100 milliárd kérést szolgál ki nap mint nap, amelyeket a gyártó folyamatosan elemez, és építi saját tudásbázisát, hogy akár már a legelső támadás előtt is védeni tudja ügyfeleit.

LEGFONTOSABB ELŐNYÖK

- A védelem első vonala az online támadások ellen
- Vizibilitás és védelem csatlakozási helytől függetlenül
- Meglévő rendszerekkel való integráció
- SIEM-integráció

A Cisco felismertem, hogy a vállalati hálózatok decentralizációjával, valamint a végfelhasználók SaaS alkalmazásokhoz történő közvetlen csatlakozásával az IT biztonsági megoldásoknak is publikus felhő-alapú szolgáltatások irányába kell elmozdulnia. Az így létrejövő megoldások új termék kategóriaként Secure Internet Gateway (SIG) néven jelentek meg a piacon.

Secure Internet Gateway

A SIG biztonságos Internetelérést biztosít bárhol is legyenek a felhasználók a világban, még akkor is, ha VPN nélkül csatlakoznak az Internetre.

Már a célszerverhez történő első hálózati csatlakozás előtt a biztonságos kommunikációt a SIG biztosítja. Függetlenül attól, hogy a végfelhasználó hol helyezkedik el, illetve hogy hova csatlakozik, a hálózati forgalom a SIG-en keresztül megy keresztül először. A SIG felhő-alapú platformját elérve a Cisco megoldása különböző csomagvizsgálatokat végez, és csak a biztonságosnak ítélt tartalom után engedi a további kommunikációt kliens és szerver között.

Cisco Umbrella

A Cisco Umbrella minden eszközt véd (legyen az akár managed akár nem managed), köztük az okoskészülékeket és IoT eszközöket is.

Felhő-alapú szolgáltatás

A SIG által nyújtott szolgáltatások csak abban az esetben nyújthatók megfelelő szolgáltatási szinten, amennyiben az teljes egészében a gyártó felhőjében fut, Software-as-

a-Service szolgáltatásként. Publikus szolgáltatásként kialakítva biztosítja a Cisco, hogy a világ bármely pontján csatlakozva az Internetre képes a kompromisszum nélküli SLA biztosítására.

A Cisco Umbrella nem igényel a nagyvállalat által üzemeltetni szükséges hardware-t vagy software-t, és tetszőleges mérethez képes skálázódni. Az Umbrella a DNS-t szolgáltatást használja, hogy az eszközökről induló összes adatforgalmat a Cisco felhőjébe irányítsa. A megoldás emellett szorosan integrálódik a Cisco végfelhasználói és hálózati megoldásaihoz is (AnyConnect, ISR, Wireless LAN vezérlők.)

Proxy-alapú web forgalom és fájl vizsgálat

A SIG számára elengedhetetlen, hogy egy felhő proxyval rendelkezzen, amely mélységeiben képes vizsgálni a web forgalmat, különösképpen a kockázatosnak ítélt webportálokról. Kiemelten fontos, hogy a SIG a proxy segítségével a hálózaton utazó fájlokat is vizsgálja vírusvédelmi szempontból.

Az Umbrella intelligens proxy komponense csak azokat a csomagokat küldi mélyebb vizsgálatra, amelyek kockázatosnak ítélt forrásokból érkeznek, így javítva a rendszer performancia mutatóit. A Cisco proxy architektúrája microszolgáltatásokból épül fel, amelyek – a növekvő terhelés hatására – automatikusan képesek skálázódni.

A Cisco Umbrella a hálózaton küldött fájlokat Anti-Virus enginen és a Cisco Advanced Malware Protection fájl reputációs megoldásán is átfuttatja, mielőtt biztonságosnak ítéli.

A megoldás üzembe állítása

Egy nagyvállalat számára fontos szempont, hogy felhasználói számára transzparens legyen a megoldás, illetve komplex telepítési folyamatok nélkül terjeszthető és konfigurálható legyen. VPN, GRE, IPSec csatornák és PAC fájlok beállítása nem ideális út egy ezres felhasználószámú vállalat számára.

A Cisco Umbrella telepítése gyors és egyszerű folyamat, mindössze a hálózati DNS szolgáltató címét szükséges megváltoztatni, ezáltal percek alatt akár a legnagyobb cégek is védelem alá tudják vonni alkalmazottaikat.