

MIÉRT PROXEDO API SECURITY?

- 1 | Az API forgalom mélységi ellenőrzése
- 2 | Egyéni biztonsági házirendek kikényszerítése
- 3 | Alkalmazások adatforgalmának egyedi elemzése
- 4 | Rugalmas, magasan képzett szenior mérnökcsapat
- 5 | A proxy technológia úttörői
- 6 | Magyar fejlesztés – 'Tiszta' kódbázis

ADDITIONÁLIS BIZTONSÁGI RÉTEG A WAF ÉS AZ API-MENEDZSMENT FÖLÖTT

A kihívás

A WAF-ok korlátai

A webes alkalmazás-tűzfalak (WAF) feladata a webalkalmazások bejövő és kimenő HTTP-forgalmának szűrése, monitorozása és - szükség esetén - blokkolása. A WAF-ok jellemzően nem képesek a célzott API-támadások megelőzésére, mivel nem az API-forgalom részletes vizsgálatára vannak optimalizálva. A WAF-termékek általában a HTTP-forgalom szignatúra adatbázis-alapú szűrésére vannak tervezve. Az API-forgalomba ágyazott adatfolyam ellenőrzésére kevésbé alkalmasak. Hiányzik továbbá az API forgalom validálása, részletes naplózása, valamint a testre-szabott biztonsági házirendek implementálásának képessége. A kiterjedt API infrastruktúrával rendelkező, hagyományos WAF-al rendelkező vállalatoknak egy speciális API-biztonsági célmegoldásra is szüksége van, amely kifejezetten a fenti problémák kezelésére képes.

Az API-menedzsment eszközök korlátai

Az API-menedzsment eszközök legfontosabb funkciója az API-k létrehozása, üzembe helyezése és kezelése. Az API biztonság nem tartozik a főbb funkcionális szempontok közé. Az API-menedzsment eszközök általában az alábbi feladatokra fókuszálnak:

- API-életciklus-menedzsment
- API-ügyfelek hitelesítése, engedélyezése és a felhasználói fiókok kezelése
- API-forgalom vezérlése, optimalizálása és terheléelosztása
- Leírók és dokumentáció

PROXEDO API SECURITY

Pozitív biztonsági modell

OpenAPI-sémák
(Swagger)



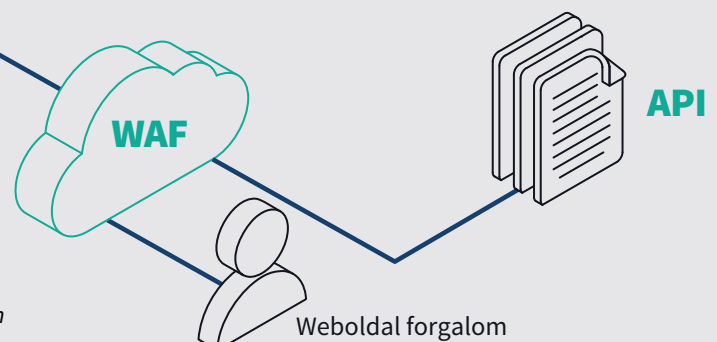
Legitim
API-hívások

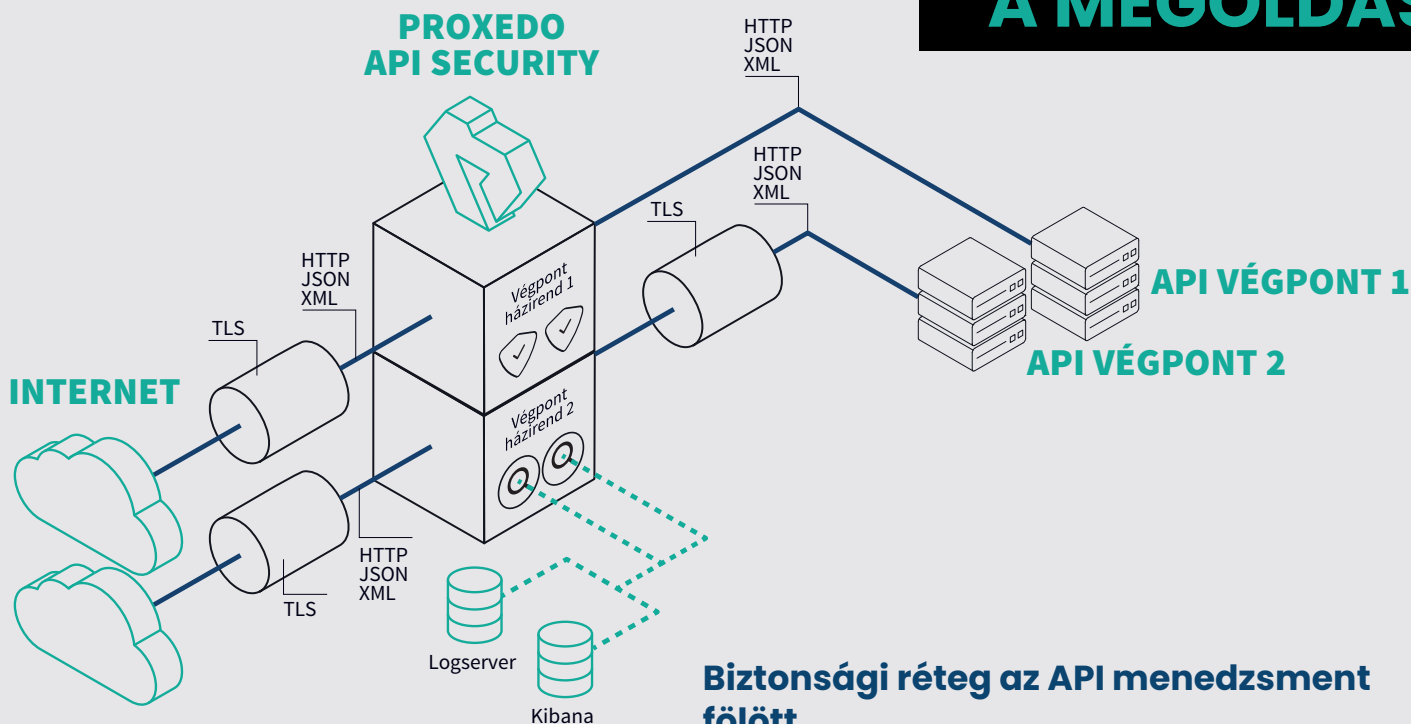


Rosszindulatú
API-hívások



API támadások védelme WAF-al integrált környezetben





API biztonság a WAF-on túl

A Proxedo API Security egy speciális webes alkalmazás-tűzfal (WAF), amelyet az API-végpontok védelmére fejlesztettek ki. Egy rugalmas hálózatbiztonsági célmegoldás, amellyel szabályozhatja alkalmazásai adatforgalmát az API-támadások megelőzése érdekében. A Deep Packet Inspection (DPI) technológiának köszönhetően részletesen ellenőrizheti, titkosíthatja, és elemezheti az API forgalmát, mindezt kiegészítve egy szignatúra adatbázis-alapú védelemmel. Rugalmas architektúrájának köszönhetően vállalata kompromisszumok nélküli, egyedi API biztonsági házirendet kényszeríthet ki. A Proxedo API Security kifejezetten az API biztonságra összpontosít, így remekül kiegészíti a hagyományos WAF és API menedzsment eszközöket is.

Biztonsági réteg az API menedzsment fölött

A Proxedo API Security NEM menedzsment eszköz, hanem egy biztonság fókuszú célmegoldás. Ellentétben az API-menedzsment szolgáltatókkal, ahol a biztonság csak egy kiegészítő funkció, a Proxedo API Security kizárólag az API-kommunikáció biztonságára összpontosít, az API forgalom ellenőrzésének, titkosításának és elemzésének optimális kombinációját kínálva. Erőteljes biztonsági funkcionálitása révén a Proxedo API Security az API-menedzsment megoldásokkal együtt alkalmazva hozzáadott értéket képvisel.

Adicionális biztonsági rétegeként a PAS az alábbiakat támogatja:

- API-forgalom validálása
- Testre szabható forgalom titkosítás
- Egyéni API-biztonsági házirendek
- Részletes, adatszintűnaplózás és elemzések
- Kapcsolódás autentikációs szolgáltatásokhoz

Webalkalmazás tűzfalak

Csak a webalkalmazások védelmére fókuszál

Vizsgálat csak a HTTP-protokoll rétegén

Nincs DPI (Deep Packet Inspection)

Nincs API-hívás validálás

Korlátozott naplózási képességek

Nincs rugalmas házirend-konfigurálás

Mintaillesztés URL-adatbázis alapján („blaclisting”)

Proxedo API Security

A webalkalmazások és a vállalatok közötti (B2B) alkalmazásintegráció védelméről is gondoskodik

Vizsgálat az API-protokoll rétegén

Fejlett DPI

API-hívások validálása

Testre szabható forgalom- és biztonsági naplózás

Házirendek rugalmas konfigurálása

Mintaillesztés és szabályok implementálása a védett szolgáltatás alapján („whitelisting”)