

- 1 | API-támadások megelőzése
- 2 | API forgalom felügyelete és elemzése
- 3 | API biztonsági megfelelés és audit
- 4 | Legacy alkalmazások védelme
- 5 | WAF-ok és API-menedzsment eszközök biztonsági kiegészítése

„A Gartner szerint, míg a vállalatok 70%-a a digitális átalakulás egyik központi elemének tartja az API-kat, azzal is tisztában vannak, hogy ezen a téren a biztonság jelenti a legnagyobb kihívást”

# PROXEDO API SECURITY

## RUGALMAS VÉDELEM API-TÁMADÁSOK ELLEN

A **Proxedo API Security (PAS)** egy transzparens, alkalmazásszintű átjáró, amely a világ első, 20 éves fejlesztői múltú visszatekintő, moduláris proxy technológiájára épül.

## A támadók figyelme az API-kra összpontosul

Az API-kon (Application Programming Interface) keresztül továbbított bizalmas adatok mennyisége robbanásszerűen növekszik, ezáltal az API-k egyre inkább a támadók elsődleges célpontjává válnak. A közelmúltban történt nagyobb adatlopások közül sok esetben az API-k sebezhetőségét használták ki gondoljunk csak a Salesforce.com, a T-Mobile, az US Post, vagy a Verizon incidensekre. Az API-támadások célzottak, amelyek könnyedén megkerülhetik a hagyományos védelmi rendszereket. Ezeket a betöréseket a webes alkalmazás-tűzfalak (WAF-ok) sem tudják észlelni, mivel képességeik nem az API-adatforgalom mélységi vizsgálatára vannak optimalizálva.

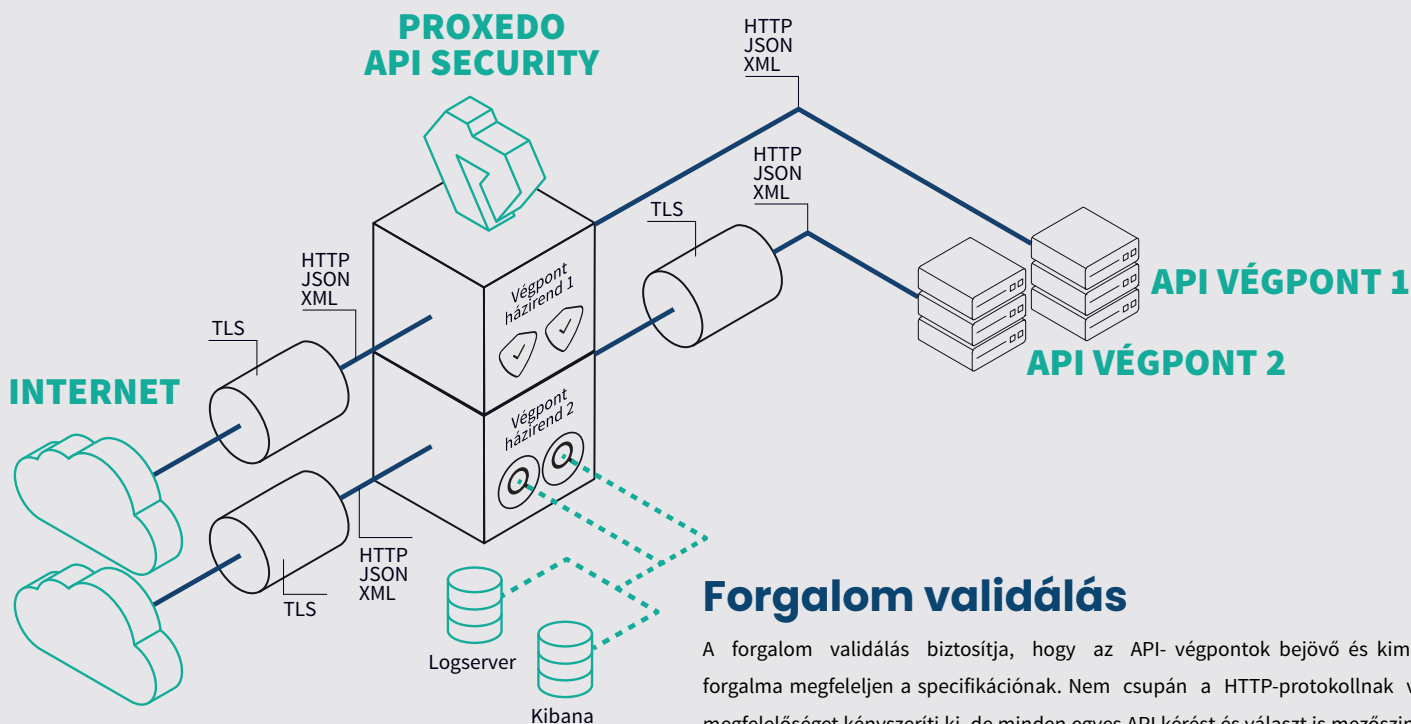
## Az API fejlesztők számára nem a biztonság az elsődleges

A legtöbb alkalmazásfejlesztési projektnél leginkább a funkcionalitást, a felhasználói élményt és a határidőket tartják szem előtt. A fejlesztők tehát nem a támadók fejével gondolkodnak. Ebből kifolyólag a nyilvános API-kban számos biztonsági rés lehet, ez pedig kockázatot jelent az üzlet számára és lehetőséget kínál a támadóknak. Szerencsére azonban erre is van megoldás.

## 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.





## Forgalom validálás

A forgalom validálás biztosítja, hogy az API- végpontok bejövő és kimenő forgalma megfeleljen a specifikációnak. Nem csupán a HTTP-protokollnak való megfelelést kényszeríti ki, de minden egyes API kérést és választ is mezőszinten validál az API-t leíró OpenAPI séma alapján. Ezáltal biztosítja, hogy csak az engedélyezett adatok jussanak át az átjárón, és megakadályozza, hogy a nem megfelelő vagy potenciálisan rosszindulatú adatok elérjék a háttérrendszereket, illetve, hogy bizalmas információk szivároghassanak ki.

## Forgalomelemzés

A PAS részletes hibakeresési, biztonsági- és auditnaplózási funkciókat kínál. Páratlan eszköztárat biztosít a releváns adatok kinyerésére az API forgalomból. A kinyert adatokat továbbíthatja SIEM/SOC rendszerekbe, big data és analitikai eszközökbe. Az API-hívások részletes értelmezése és a rugalmas konfiguráció révén minden érdekes adatot kinyerhet, és csak azokat, amelyekre szüksége van. Mindezt valós időben, közvetlenül a forrásból.

## Forgalomtitkosítás

A PAS képes a TLS protokollt (a HTTP biztonsági rétegét) kezelni, ezáltal biztosítja a forgalom titkosítását olyan háttérrendszerek előtt is, amelyek nem feltétlenül támogatják a fejlett titkosítást. A TLS-t rugalmasan konfigurálhatja a kommunikáló felek igényeinek megfelelően.

## Forgalomszabályozás

A háttérrendszerek előtt elhelyezkedő Proxedo API Security terheléelosztóként is működik a kiszolgálók számára. Mély ellenőrzési képességeinek köszönhetően az átjáró nem csupán az alapértelmezett tiltás („default-deny”), hanem részletes biztonsági házirendek kikényszerítésére is képes.

## Szignatúra-alapú védelem

A PAS egy szignatúra adatbázissal folyamatosan összehasonlítja a HTTP(S) forgalmat, hogy azonosítsa a támadási mintákat. Ezzel megvédheti webes szolgáltatásait az ismert internetes fenyegetésekkel szemben.

# MIÉRT

# PROXEDO API SECURITY

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



Proxedo API Security Termékoldal  
Próbaverzió kérése