1. **API-támadások megelőzése**
2. **API-forgalom felügyelete és elemzése**
3. **API biztonsági megfelelőség és audit**
4. **Legacy alkalmazások védelme**
5. **Extra biztonsági réteg a WAF és az API-menedzsment fölött**

PROXEDO
API LIFECYCLE PLATFORM

„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 LIFECYCLE PLATFORM API SECURITY

NE ENGEDJE, HOGY AZ API-JAI ÖN ELLEN FORDULJANAK

Az **API Security** egy transzparens, alkalmazás-szintű átjáró, amely a világ első, 20 éves fejlesztői múltra visszatekintő, moduláris proxy technológiájára épül. Az API Security a Proxedo API Lifecycle Platform központi modulja.

A támadók figyelme az API-kra összpontosul

Az API-kon (Application Programming Interface) keresztül továbbított bizalmas adatok mennyisége robbanásszerűén 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, a US Post, vagy a Verizon incidensekre. Az API-támadások célzottak, így 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 gondolkoznak. 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.

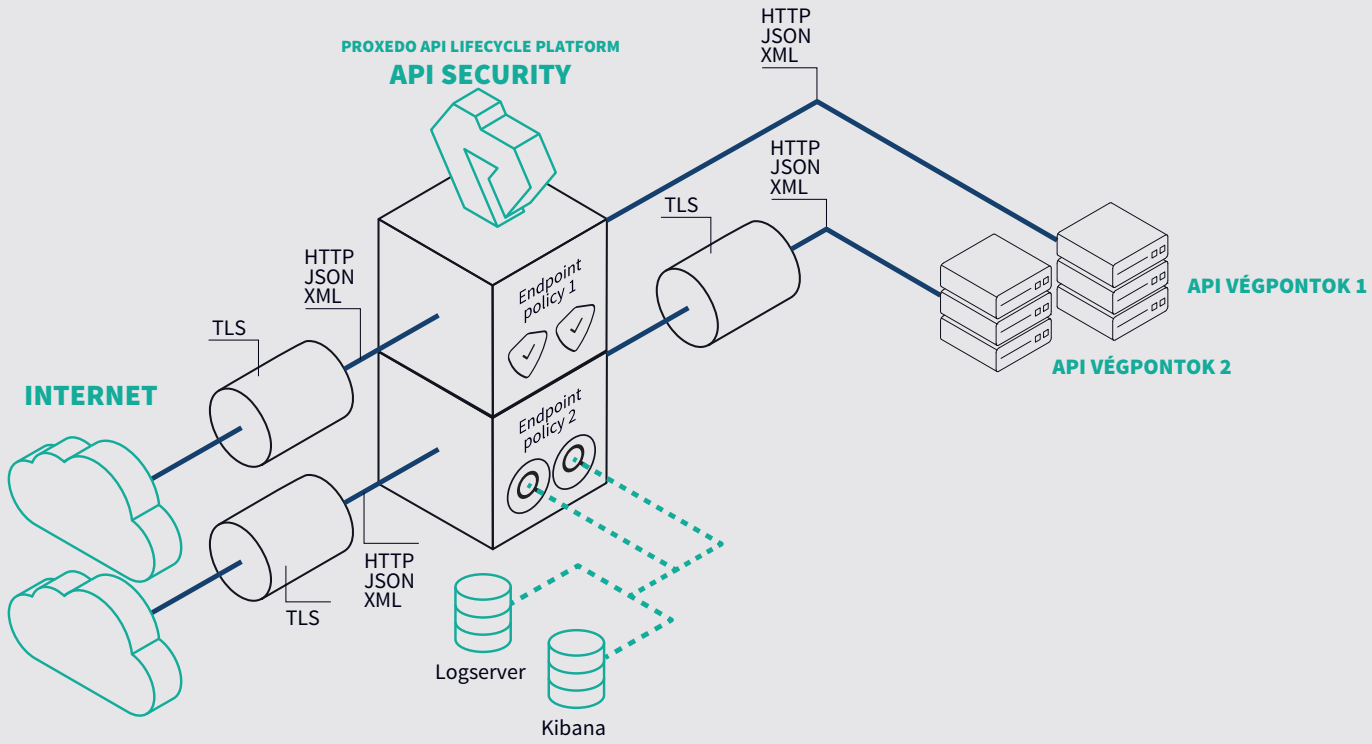
API-biztonság a WAF-on túl

Az 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 API-forgalmát, mindezt kiegészítve egy szignatúra adatbázis-alapú védelemmel. Rugalmas architektúrájának köszönhetően vállalata kompromisszumok nélküli, egyedi API biztonsági házirendet kényszeríthet ki. Az API Security kifejezetten az API-biztonságra összpontosít, így remekül kiegészíti a hagyományos WAF és API-menedzsment eszközöket is.

BALASYS

info@balasys.hu

API Security mintaarchitektúra



Forgalomtitkosítás

Az API Security 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.

MIÉRT API SECURITY

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

Proxedo API Lifecycle Platform főoldal

Próbaverzió igénylése

BALASYS

Forgalomvalidálás

A forgalomvalidálás biztosítja, hogy az API-végpontok bejövő és kimenő forgalma megfeleljen a specifikációnak. Nem csupán a HTTP-protokollnak való megfelelőséget 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 szivárogjanak ki.

Forgalomelemzés

Az API Security 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.

Forgalomszabályozás

A háttérrendszerek előtt elhelyezkedő API Security terheléselosztóként 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.

Proxedo API Lifecycle Platform

A Proxedo API Lifecycle Platform olyan moduláris megoldás, amellyel nemcsak kezelheti, de meg is védheti API-jait. Végpontok közötti APIbiztonsági eszközkészletével vállalata elháríthatja az API-specifikus fenyegetéseket, automatizált támadásokat, APT-ket és csalási kísérleteket. A megoldás központi eleme, az API Security modul egy speciális biztonsági átjáró, amely részletesen szabályozza az alkalmazásforgalmat. Az API-biztonság mellett portfóliónk webalkalmazás tűzfalat, valamint API-menedzsment és csalásmegelőzési szolgáltatásokat is kínál.