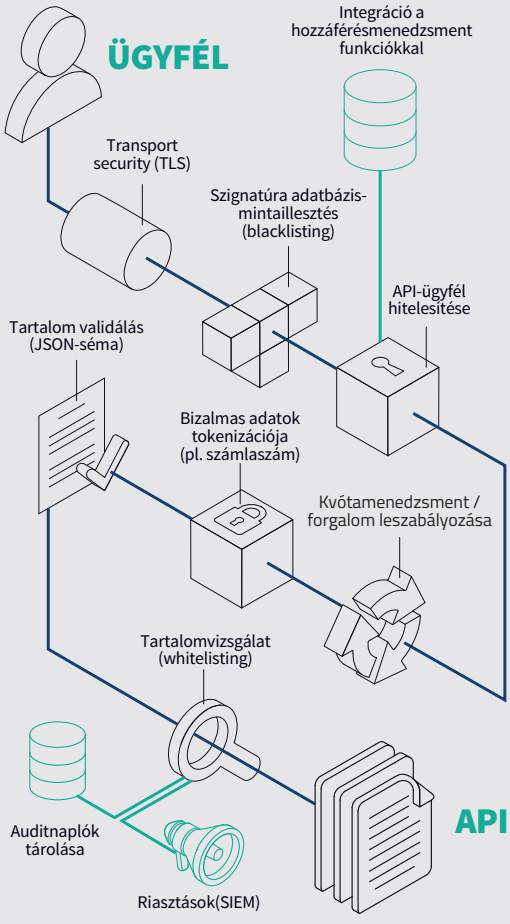
MIÉRT PROXEDO API SECURITY?

1. **API-hívások hitelesítése és validálása**
2. **Részletes hibakeresési, biztonsági és auditnaplózás**
3. **Kikényszerített adattitkosítás**
4. **Rugalmas, magasan képzett szenior mérnökcsapat**
5. **A proxy technológia úttörői**
6. **Magyar fejlesztés – 'Tiszta' kódbázis**

PROXEDO
API SECURITY

A 2019-es Cost of Data Breach című kutatási jelentés szerint a megfelelőségi problémák járulnak hozzá a legnagyobb mértékben az adatlopások okozta költségekhez.

API BIZTONSÁGI MEGFELELŐSÉG ÉS AUDIT



Hatékony API-biztonsági eljárásrend kialakítása

A kihívás

A belső és külső adatkommunikáció egyre nagyobb része API-kon (Application Programming Interface) keresztül zajlik. Ez azt is jelenti, hogy az API-környezetek auditálása és megfelelőségének biztosítása egyre több figyelmet igényel. Minden szabályozásnak egy kulcsfontosságú közös pontja van: a szabályozás alá eső vállalatoknak biztosítaniuk kell az ügyfelek adatainak védelmét a tárolás és a továbbítás során is. Az adatok kiszivárgása súlyos következményekhez vezethet, többek között büntetésekhez, jövőbeli bevételkieséshez, az ügyfelek bizalmának elvesztéséhez, további megfelelőséggel kapcsolatos költségekhez, sőt végső esetben akár csődhöz is.

PSD2

A PSD2 (Revised Payment Services Directive) az Európai Unió pénzforgalmi szolgáltatásokról szóló irányelve, amely az EU-ban, sőt még azon kívül is a feje tetejére állította az egész iparágat. Az irányelv kötelezi a bankokat, hogy tegyék nyitottá API-jaikat a kereskedők és a fintech-szolgáltatók számára. Emellett megköveteli a pénzügyi szolgáltatóktól a nyilvános API-kon keresztül forgalmazott pénzügyi adatok védelmét. A PSD2 követelményeinek való megfelelés kialakítása a régi és új piaci résztvevők részéről is komoly beruházást igényel.

GDPR

Az adatkezelő és adatfeldolgozó vállalatok is használhatnak API-kat a személyes adatok gyűjtéséhez, megosztásához és feldolgozásához. A GDPR értelmében az adatokat kezelő feleknek kötelessége az így továbbított adatok biztonságáról is gondoskodni. A GDPR emellett a továbbított és tárolt bizalmas adatok anonimizálását vagy álnevesítését is megköveteli. Kifejezetten előír bizonyos védelmi intézkedéseket az adatok harmadik féllel való megosztása esetére.

PCI DSS

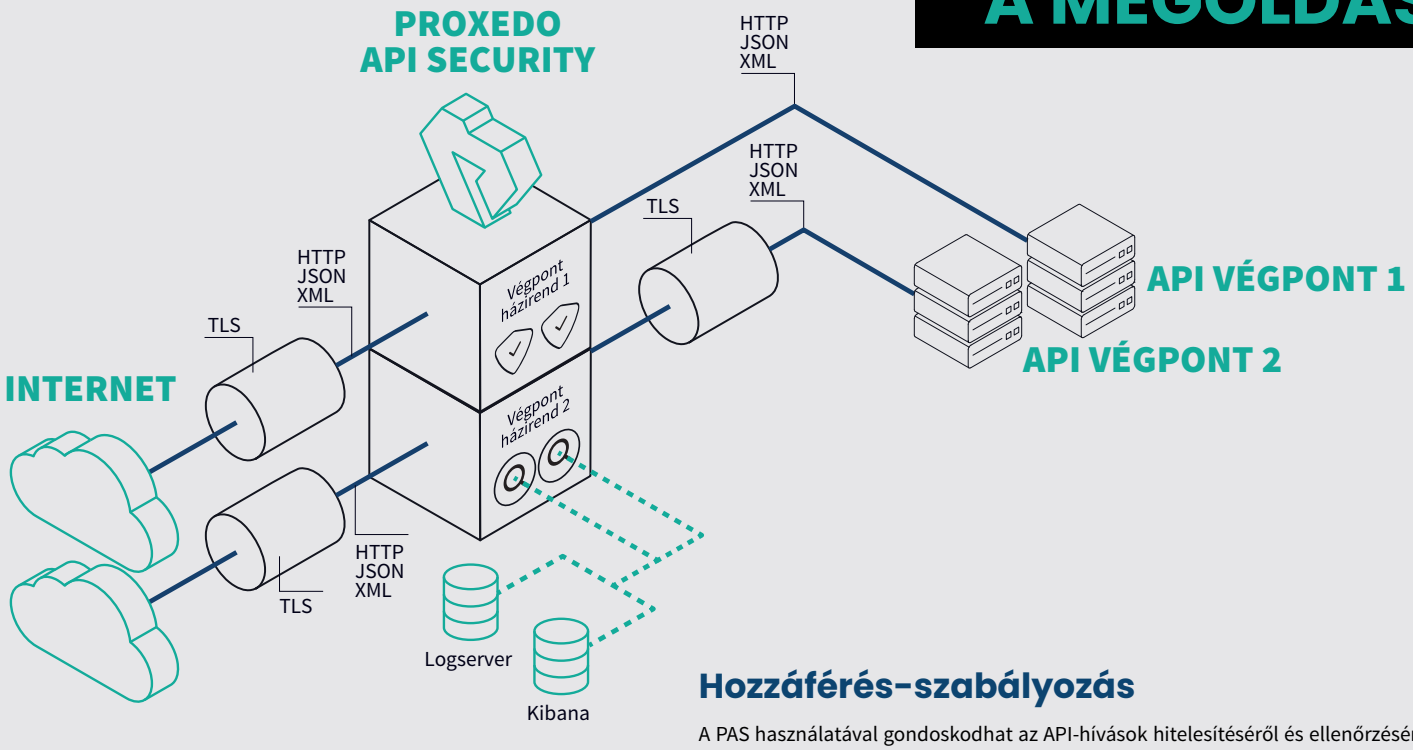
A PCI DSS kötelezi a pénzügyi szolgáltatókat és a kereskedőket a kártyaadatok publikus hálózatokon történő továbbításának titkosítására. Ha az API-kon bármilyen kártyás fizetéssel kapcsolatos információ halad keresztül, akkor az adott vállalatnak és a szóban forgó API-kat támogató összes technológiai partnerének rendelkeznie kell PCI-tanúsítvánnyal, és meg kell felelnie a vonatkozó kártyaadat-biztonsági feltételeknek.

BALASYS

info@balasys.hu

A MEGOLDÁS

Proxedo API Security (PAS) mintaarchitektúra



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.

ELŐNYÖK

Minden szabályozói előírásnak egy kulcsfontosságú közös pontja van: a szabályozás alá eső vállalatoknak biztosítaniuk kell az ügyfelek adatainak védelmét a tárolás és a továbbítás során is. A Proxedo API Security átfogó hozzáférés-szabályozási, titkosítási és naplózási képességei révén könnyebbé teszi a megfelelőség biztosítását az API infrastruktúrájában.

Proxedo API Security Termékoldal

Próbaverzió kérése

BALASYS

Hozzáférés-szabályozás

A PAS használatával gondoskodhat az API-hívások hitelesítéséről és ellenőrzéséről. A forgalom validálása révén biztosíthatja, hogy az API-végpontok bejövő és kimenő forgalma megfeleljen az arra vonatkozó követelményeknek. Biztosíthatja, hogy csak az engedélyezett adatok juthassanak át az átjárón, és megakadályozhatja, hogy a nem megfelelő vagy potenciálisan rosszindulatú hívások elérjék a kiszolgálót, illetve hogy a bizalmas adatok kiszivárogjanak.

A PAS emellett egy szignatúra adatbázis alapján is vizsgálja a HTTP(S)-forgalmat, és azonosítja az ismert támadási mintázatokat. A fenti funkciók birtokában a már ismert és az ismeretlen fenyegetésektől is megvédheti webalapú szolgáltatásait.

Titkosítás

A Proxedo API Security képes a TLS protokoll (a HTTP biztonsági rétegének) átfogó kezelésére, ezáltal biztosítja a titkosítás olyan háttérrendszerek előtti egységes megvalósítását, amelyek nem feltétlenül támogatják a TLS-t. Így a titkosítási házirendeket rugalmasan, a kommunikáció különböző résztvevői számára testreszabottan konfigurálhatja.

A Proxedo adatmanipulációs képessége lehetővé teszi a bizalmas adatok anonimizálását, ami szükséges a GDPR és más adatvédelmi szabványoknak való megfeleléshez. Az adatok névtelenül továbbíthatók a külső partnerekhez.

Naplózás és felügyelet

A legtöbb informatikai biztonsági szabályozás szigorú elvárásokat fogalmaz meg a bizalmas adatokat tartalmazó kommunikáció naplózására vonatkozóan. A Proxedo API Security hatékony naplólétrehozási és -gyűjtési képességekkel rendelkezik. Megoldásunk minden adathozzáférést képes naplózni, amely a vállalata API-jain keresztül történik. Az elkészült naplófájlokat biztonságosan tárolja, időbélyegzővel látja el, indexeli, és szükség esetén a hatóságok számára azonnal elérhetővé teszi. A biztonsági naplókat akár SIEM/SOC-rendszerekbe is továbbíthatja, ezzel is javítva szervezete biztonság felügyeleti képességét.