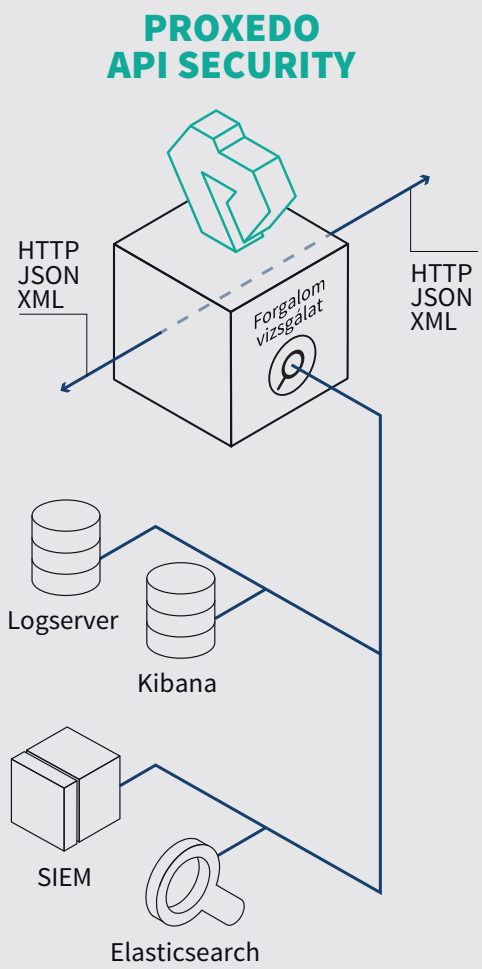
MIÉRT PROXEDO API SECURITY?

1. **Részletes hibakeresési, biztonsági és auditnaplózás**
2. **Testre szabható adatkinyerés az API forgalomból**
3. **Adattovábbítás big data-eszközökhöz, naplóelemzőkhöz és SOC/SIEM-rendszerekhez**
4. **Rugalmas, magasan képzett szenior mérnökcsapat**
5. **A proxy technológia úttörői**
6. **Magyar fejlesztés – 'Tiszta' kódbázis**

PROXEDO
API SECURITY

"2019-ben a Black Friday napján számos nagy online áruház rendszere összeomlott,vagy átmenetileg leállt. A legtöbb ilyen eset hátterében API-hibák álltak. "

AZ API-FORGALOM FELÜGYELETE ÉS ELEMZÉSE



A Proxedo API Security részletesen megvizsgálja az API forgalmat

A kihívás

Vállalata webalkalmazásai is nagy valószínűséggel külső és belső API-kra épülnek. A webes szolgáltatások és a natív alkalmazások is API-kon keresztül bonyolítják a kritikus adatkommunikációt, ezért az API forgalom felügyelete és elemzése az IT biztonsági házirend szerves részét kell hogy képezze.

A biztonsági és üzemeltetési csapatnak információ kell

A naplózás technológiai korlátai miatt a kiterjedt API-infrastruktúrával rendelkező vállalatok komoly kihívásokkal szembesülnek az API-forgalom felügyeletekor. Vállalata IT üzemeltetési és biztonsági csapata csak az API-forgalom proaktív monitorozásával gondoskodhat a biztonságos működésről illetve a fenyegetések észleléséről.

A vállalatok zavaros ügyfeladatokkal dolgoznak

A cégvezetők és üzleti döntéshozók munkáját is megnehezíti, ha nem rendelkeznek megfelelő részletességű jelentésekkel az ügyfelek online viselkedésével kapcsolatban. A minőségi üzleti adatok hiánya alulinformált döntésekhez vezethet, arról nem is beszélve, hogy adatok hiányában a gyanús ügyféltevékenységek azonosítására sincs lehetőség. Ez pedig súlyos adatlopásokhoz vezethet, ahogyan az Egyesült Államok Postahivatalának esetében ez meg is történt.

A fejlesztőknek hatékony hibakeresésre van szüksége

Megfelelő szintű naplózás hiányában a fejlesztők nem képesek az API-k és az alkalmazások teljesítményének mérésére, a tranzakciók követésére, valamint a hibák azonosítására. Mindezek elemzésével és visszacsatolásával jobb kapcsolatot alakíthat ki a fejlesztőkkel, és jobb döntéseket hozhat az alkalmazás-környezetével kapcsolatban.

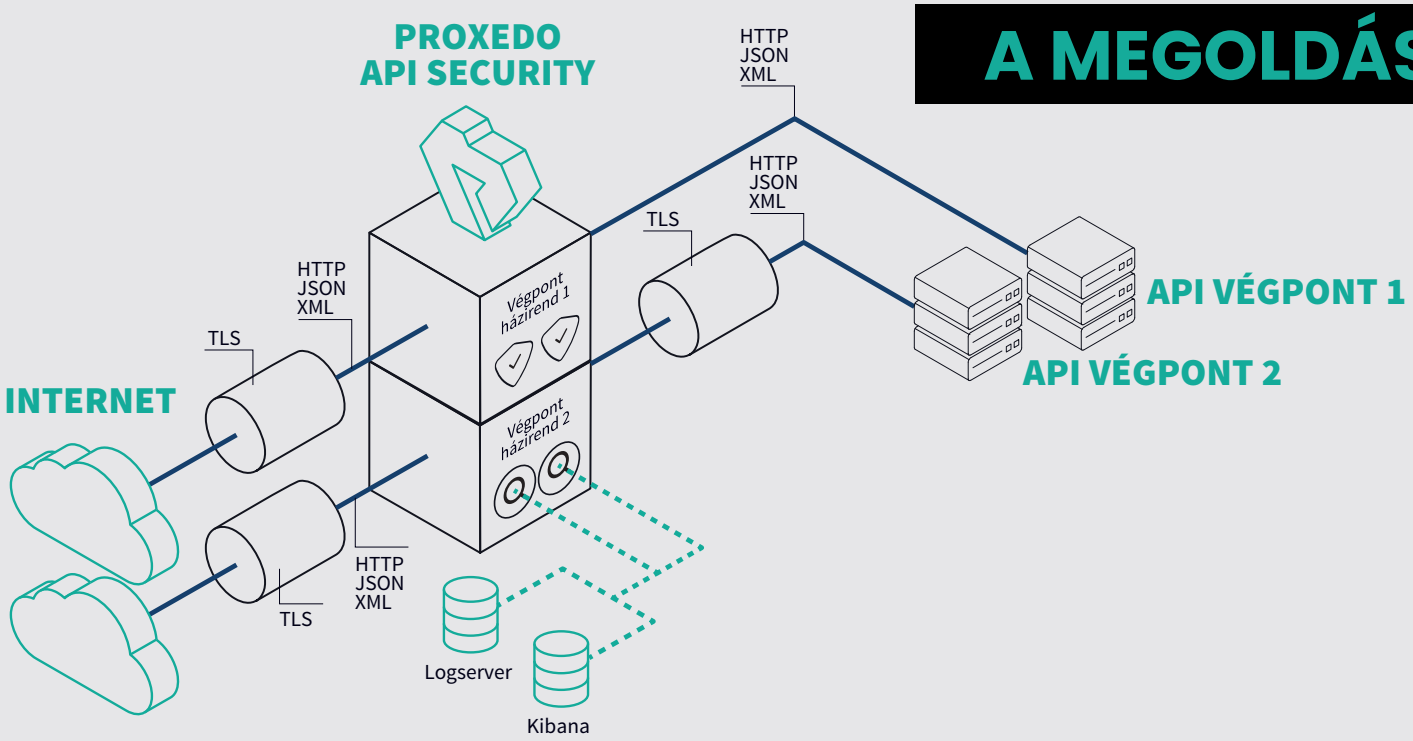
Az API-hibák üzletkritikusak

2019-ben a Black Friday napján számos online áruház rendszere összeomlott, vagy átmenetileg elérhetetlenné vált – főként API-hibák következtében. Néhány esetben az összeomlás külső szolgáltatók rendszerében történt. Például a fizetéskezelő átjáró API-ja hibásodott meg, jelentős veszteségeket okozva az érintett webáruházaknak. Egy vállalat dollármilliókat veszíthet, ha a csúcsidőben nem képes kezelni az online tranzakciókat.

BALASYS

info@balasys.hu

Proxedo API Security (PAS) mintaarchitektúra



A 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.

ELŐNYÖK

A Balasys Proxedo API Security megoldásával átláthatóvá teheti az API-kon áthaladó forgalmat. A biztonsági csapata tovább fejlesztheti a biztonság felügyeleti képességeit, ezáltal hatékonyabban szállhat szembe a fenyegetésekkel. Az informatikai üzemeltetési csapat alaposabban elemezheti az API-k használatát, illetve azok tovább fejlesztési lehetőségeit. Az API-fejlesztők nyomon követhetik az API-k teljesítményét. Az üzleti döntéshozók pedig elemezhetik az API-tranzakciókat, ezáltal megalapozottabb döntéseket hozhatnak.

A Proxedo API Security használatával az alkalmazások leállása esetén is könnyedén helyreállíthatja üzletmenetét, azonosíthatja a rosszindulatú szereplőket, illetve felismerheti a felhasználói viselkedés változását. Emellett nyomon követheti API-programja sikerét, és megtervezheti a kapcsolódó jövőbeli beruházásokat.

Proxedo API Security Termékoldal

Próbaverzió kérése

BALASYS

Forgalomelemzés

A Proxedo API Security egyedülálló eszközkészletet kínál az adatok API-forgalomból történő kinyeréséhez, és külső elemző eszközökhöz való továbbításához. Az API-hívások részletes értelmezése és a rugalmas konfiguráció révén minden releváns adatot kinyerhet, és csak azokat, amelyekre szüksége van, mindezt valós időben, közvetlenül a forrásból.

Biztonság felügyelet és audit

A PAS részletes biztonsági és auditnaplózási funkciókat nyújt. SIEM- vagy SOC-rendszereibe megbízható és releváns adatokat küldhet, ezzel javíthatja biztonság monitorozási és riasztási képességeit. Az API-tranzakciók részletes naplózása az alkalmazások auditálását is segíti, emellett a megfelelőség kialakítása érdekében tett erőfeszítéseket is támogatja.

Üzleti adatok elemzése

A PAS támogatja a naplófájlok big data eszközökhöz és data lake-ekhez való továbbítását (pl. Kibana, Elasticsearch, Kafka). Előszűrt és minőségi adatokat küldhet az említett rendszerekbe részletes üzleti elemzés céljából.

Hibakeresés

A részletes hibakeresési naplók segítik a fejlesztőket az API-kal kapcsolatos problémák elhárításában. Ez csökkenti az API-k biztonsági réseinek számát, és növeli az alkalmazásai biztonságát a fejlesztési folya- mat során, valamint a kiadást követően. A releváns naplók az informatikai üzemeltetési csapat számára is hasznosak, és segítenek a webalkalmazások üzembiztonságának növelésében. Emellett a HTTP-kérések nem böngésző típusú alkalmazásokból, például mobil-alkalmazásokból, történő lekérdezésére is lehetőséget nyújtanak.

Forgalomszabályozás

A háttérrendszerek előtt elhelyezkedő Proxedo 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.