FŐ KÉPESSÉGEK

PROXEDO NETWORK SECURITY

- Biztonságos azonosítás és jogosultságkezelés
- Hálózati forgalom mélységi vizsgálata
- Örökségrendszer felügyelet és kontrol
- Zero Trust hálózati mikroszegmentáció
- Részletes audit naplózás és riasztások

PROXEDO NETWORK SECURITY

- Kritikus infrastruktúra rendszerek szeparálása
- Hozzáféréskezelés bármilyen rendszerhez
- Részletes naplózás, felügyelet és audit
- Zero Trust hálózati architektúra
- Adatvédelem és titkosítás kikényszerítése
- Remote site üzemeltetés
- Központi konfiguráció management
- On-prem és virtualizáció támogatás

Többfunkciós hálózatvédelem

A Proxedo Network Security egy rugalmas, többfunkciós tűzfalmegoldás, mely lehetővé teszi vállalatok számára, hogy megerősítsék a kibervédelmi fenyegetésekkel szembeni rezilienciájukat és teljesítsék a NIS2 előírásait.

A Proxedo személyre szabható szabályrendszerének és folyamatosan fejlődő, kibervédelmi eszköztárának köszönhetően több, mint 20 éve biztosítja kritikus infrastruktúrák, pénzügyi szolgáltatók, egészségügy, telekommunikáció, államigazgatás és ipari szereplők hálózatbiztonságát.

Hálózati forgalom mélységi vizsgálata

A Proxedo tűzfal Deep Packet Inspection technológiát alkalmaz, hogy teljeskörű betekintést adjon a védett rendszerek forgalmába, a Proxedo tartalom alapú szabályainak köszönhetően egy eszközzel kikényszeríthető a biztonság, teljesítmény és folyamatos felügyelet.

A 15+ IT és OT protokoll proxyjával és az egyedi proxyk létrehozására szolgáló eszközkészlettel bármilyen rendszer forgalmára kiterjeszthető felügyeletet kínál, legyen az modern-, egyedi-, vagy örökségrendszer.

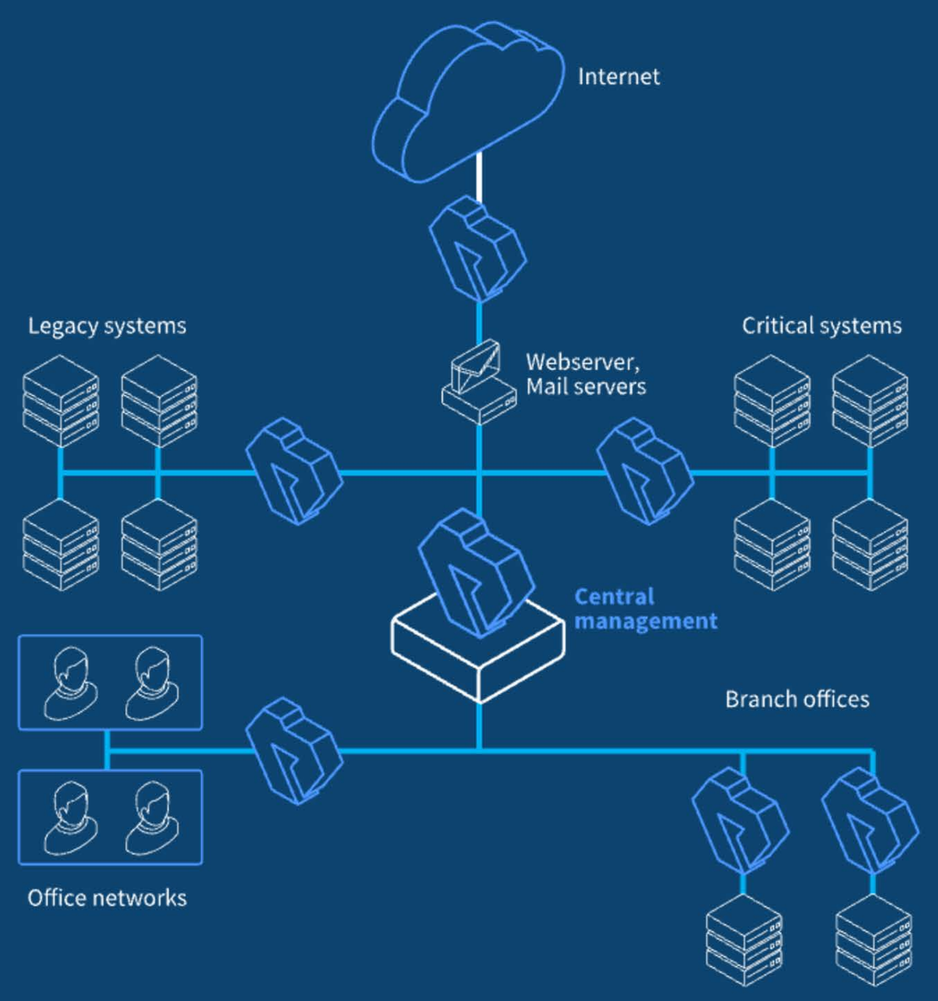
Adatvédelem és titkosítás

A PNS tűzfaltechnológia lehetővé teszi titkosított csatornák kiépítését, VPN és azonosítás beépítését a kommunikációba, valamint a forgalom folyamatos naplózását.

A egyedileg konfigurálható szabályok lehetővé teszik mind az ügyfél-, mind a backend oldali titkosítási szabályok kezelését, valamint a tanusítványkezelést és a TLS titkosított forgalom átvizsgálását anélkül, hogy bármilyen módosítást kellene végrehajtani a védett alkalmazáson.

BALASYS

info@balasys.hu
Balasys IT Zrt. Minden jog fenntartva.



HÁLÓZAT SZINTŰ JOGOSULTSÁG KEZELÉS

FORGALOMMANIPULÁCIÓ SZŰRÉS ÉS TITKOSÍTÁS

RÉSZLETES AUDIT NAPLÓZÁS ÉS FELÜGYELET

KRITIKUS RENDSZEREK ÉS HÁLÓZATOK SZEPARÁLÁSA

LEGACY RENDSZER TÁMOGATÁS ÉS VÉDELEM

EGYEDI SZABÁLYRENDSZEREK KIKÉNYSZERÍTÉSE

TECHNIKAI ELŐNYÖK

- 15+ protokoll proxy
- “Best-match” alapú szabály ellenőrzés
- LDAP/AD, Kerberos és RADIUS hozzáféréskezelés
- Erős authentikáció (S/Key, SecurID, X.509, …)
- License- és certificate management
- Titkosítás kikényszerítése TLS 1.3 támogatással
- IPSec és OpenVPN támogatás
- GeoIP, Blacklist, Whitelist
- WAF, AV, sandboxing és URL-szűrő
- IDS/IPS, DLP, MFA & SIEM integráció

Tudjon meg többet

Látogasson el balasys.hu oldalra további információkért a Proxedo megoldásokról

BALASYS

Zero Trust Architektúra

A Proxedo Network Security a NIST Zero Trrust Architektúra alapelveit alkalmazza a támadási felületek minimalizálására, valamint a támadók laterális mozgásának megakadályozására és az incidensek által érintett rendszerek teljeskörű behatárolására.

A Proxedoval a NIST ZTA kialakítása, a meglévő infrastruktúra elemeivel valósul meg, anélkül, hogy le kellene cserélni akár az elavult, vagy alacsony kibervédelmi érettségi szinttel rendelkező rendszereket, mivel ezek kommunikációjában a legmodernebb standardeknek megfelelő védelem folyamatos megkövetelését biztosítja.

Részletes naplózás

A forgalom mélyégi vizsgálatának köszönhetően, a PNS eszköztára lehetővé teszi a hálózat folyamatos naplózását, valamint egyedi igényeknek megfelelő riasztások és jelentések készítését.

A Proxedo kiterjeszti az IT és OT felügyeleti eszközök és kibervédelmi folyamatok látóterét az összes védett rendszerre, legyen az modern- vagy örökségrendszer, harmadik fél szolgáltatása, vagy egyedi protokol.

A Proxedo képes továbbítani a kinyert, vagy általa generált információkat a napló management, SIEM, SoC, DLPS és Big Data Analitika rendszerek felé, támogatva azokat, a teljes infrastruktúrára kiterjedő adatforrásként.

Bármilyen környezetben alkalmazható

A Proxedo Network Security a VM és hardveres környezetben egyaránt üzemeltethető, támogatott platformok széles választékával.

A skálázhatóságának és robusztus központi management képességeinek köszönhetően a PNS lehetővé teszi akár világszerte több száz telephely harmonizált üzemeltetését és felügyeletét.