APPWALL – TÖBB MINT WAF

A kibertámadások és a védekezési technikák fejlődését követniük kell a vállalkozásoknak, és a lehető legrövidebbre kell szabniuk a védekezéssel töltött időt.

A vállalkozások a webalkalmazásokra helyezik át az üzletmenet szempontjából kritikus tevékenységeiket annak érdekében, hogy fokozzák a termelékenységüket, javítsák az üzleti agilitásukat és csökkentsék a költségeiket. A webalkalmazásokra történő migráció gazdasági előnyöket biztosít és lehetővé teszi a fokozott üzleti agilitást, ugyanakkor új biztonsági kockázatokat és megfelelőségi elvárásokat is teremt, amelyeket kezelni kell. A támadások komplexitása, gyorsasága, amivel megkerülik az új védekezőeszközöket és technikákat, megkövetel egy olyan robusztusabb és átfogóbb megoldást, amely gyorsabb védekezést és csökkentett karbantartási költségeket kínál.

Az alkalmazási réteg megcélzásával a támadók kimerítik a szerverek és applikációk erőforrásait, és olyan rejtett támadási módszereket használnak, amelyek nem felderíthetők a hagyományos biztonsági eszközökkel. A tét immár nem csak a http flooding és a leállás időtartama. A fejlett módszerek és a többvektoros támadások új kihívásokat támasztanak egy szervezet megvédésében.

AppWall – Magas fokú biztonság webalkalmazások számára

Az AppWall, a Radware webalkalmazás-szintű tűzfala (WAF) a kritikus webalkalmazások gyors, megbízható és biztonságos kézbesítését biztosítja. Az AppWall az ICSA Labs tanúsítványával rendelkező, PCI-kompatibilis WAF, amely teljeskörű védelmet kínál a webalkalmazások elleni, a tartalomelosztó hálózatok (CDN-ek) mögötti webalkalmazásokat megcélzó, a fejlett, HTTP alapú (slowloris, dinamikus flooding), és a bejelentkezési oldalakra irányuló brute force támadásokkal szemben is.

Az AppWall az egyetlen olyan webalkalmazás-szintű tűzfal, amely teljeskörű webalkalmazás biztonságot nyújt. Blokkolja a támadásokat a hálózat határvonalán, valamint biztosítja a kritikus webalkalmazások gyors, megbízható és biztonságos kézbesítését. A legjobban teljesítő alkalmazásbiztonsági megoldást jelenti a webes biztonság, védelem és megfelelés területén.

Átfogó és pontos biztonsági lefedettség

A webalkalmazások tekintetében az AppWall az ismert és ismeretlen veszélyekre egyaránt átfogó és pontos biztonsági lefedettséget nyújt. Teljeskörű és azonnali biztonsági lefedettséget kínál az OWASP top10-es listáján szereplő veszélyekkel szemben, beleértve a cross-site scriptinget (XSS), a cross-site request forgery-t (CSRF), a hibás hitelesítést, az érzékeny információk szivárgását és a munkamenet (session) kezelést. Ugyanakkor az OWASP top10-es listáján kívüli támadásokra és veszélyekre is lefedettséget ad, mint például a webalkalmazás-biztonsági konzorcium (Web Application Security Consortium, WASC) által meghatározott fenyegetettségek.

Az AppWall megszünteti a TCP-kapcsolatokat, és normalizálja a kliens által kódolt forgalmat, hogy blokkolni tudja a különféle megkerülési technikákat, illetve szavatolja, hogy a „dobozos”, tiltás alapú biztonsági megoldások sokkal hatékonyabbak, pontosabbak és kijátszhatatlanabbak legyenek.

Automatizált védelem a nulladik napi webes támadásokkal szemben

A Radware negatív (tiltások definiálása, minden más elfogadása) és pozitív (engedélyek definiálása, minden más elutasítása) biztonsági modelljeinek kombinációja a legjobb biztonsági lefedettséget teszik lehetővé, minimális hatással a legitim forgalomra. A két modell kombinálása utat enged a finomhangolt és pontos policy meghatározásoknak, elkerülve ezáltal a hamis pozitív és a hamis negatív jelzéseket.

A negatív és a pozitív biztonsági modellek egyidejű használatával, az AppWall eredményezi a legkevesebb hamis pozitív jelzést, minimális üzemeltetési erőfeszítést igényel, ugyanakkor robusztus védelmet biztosít az ismert és nem ismert (nulladik napi) veszélyekkel szemben.

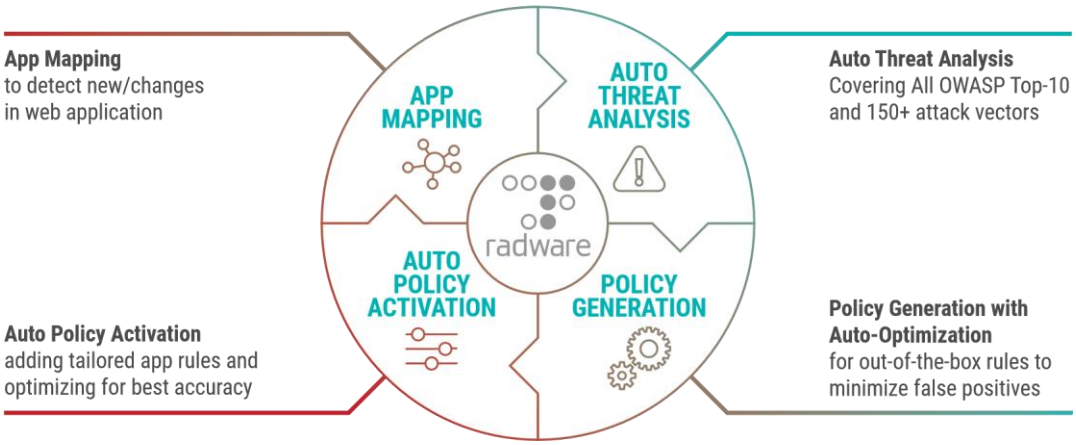
Gépi tanuló algoritmusok használata az automatikus szabálygenerálásban

Az AppWall gépi tanuló algoritmusokat foglal magában annak érdekében, hogy a webes eszközök mindig védve legyenek (még úgy is, hogy az alkalmazások folyamatosan változnak és a veszélyek rohamosan fejlődnek), biztosítva ezáltal a webes biztonság „jövőállóságát”. Az AppWall egyedülálló *Auto Policy Generation* mechanizmusa a védett webalkalmazás számára a legjobb eszközt kínálja a biztonsági policyk automatikus generálásában.

Az *Auto Policy Generation* modul automatikusan igénybe veszi a kellő biztonsági szűrőt, létrehozza a biztonsági szűrés szabályait és aktív módba kapcsolja a biztonsági szűrőket. Ezek a műveletek alapesetben számos kézi hangolást igényelnének.

A gépi tanuló algoritmusok használatával az *Auto Policy Generation*t úgy terveztük, hogy egy webalkalmazást a lehető legautomatizáltabban védjen, kevés vagy korlátozott felhasználói interakcióval; ez a modul továbbá az alábbi előnyöket nyújtja:

- A legrövidebb idő a védelemig; az ismert támadásokhoz csupán egy hetet igényel – **50 százalékkal gyorsabb, mint a többi vezető WAF**
- A legjobb biztonsági lefedettség automatikus veszélyelemzés végrehajtásával, admin beavatkozás nélkül – **több mint 150 támadási vektor figyelése**
- A legkevesebb hamis pozitív jelzés auto-optimalizálás és azonnal használható szabályok révén – **nullához közelítő hamis pozitív jelzés**
- A webalkalmazásokban beállt változtatások automatikus észlelése, biztosítva ezáltal az alkalmazás védelmét a fejlesztési életciklusa teljes idejére – **telepítés utáni problémamentesség**

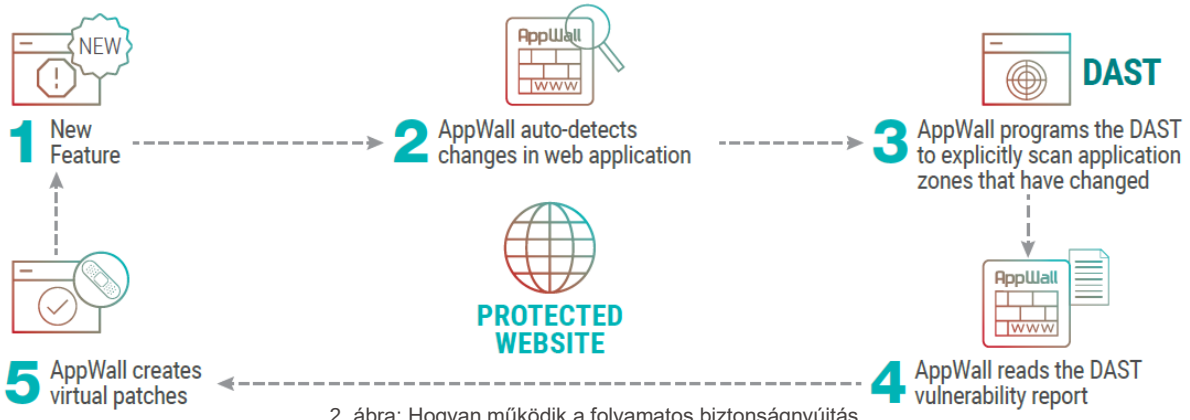


1. ábra: Az AppWall gépi tanuló képességeinek áttekintése

Folyamatos biztonságnyújtás

Az AppWall az első olyan WAF, amely valós idejű patching megoldást kínál webalkalmazások számára a folyamatos alkalmazástelepítési környezetekben. Ez a dinamikus alkalmazásbiztonsági tesztelés (Dynamic Application Security Testing, DAST) megoldásaival történő szoros integráció révén valósul meg.

Ahogy a webalkalmazások folyamatosan új funkciókat és erőforrásokat vezetnek be, a RadWare AppWall automatikusan észlel minden változást a webalkalmazásokban (1) valós időben, majd futtatja (2) a DAST eszközt, hogy az kifejezetten (3) azokat az alkalmazászónákat szkennelje, amelyek megváltoztak. Ez a szkennelés néhány percig tart, szemben az alkalmazás teljes átvizsgálásával, ami órákba telhet. Az AppWall aztán elemzi (4) a DAST sebezhetőségi riportját annak érdekében, hogy automatikusan frissíteni tudja az alkalmazásbiztonsági policyt (5) azáltal, hogy létrehozza a szükséges virtuális patcheket. Ezt követően a második sebezhetőség szkennelés is elindul, hogy ellenőrizni lehessen az alkalmazásbiztonsági javítás sikerességét.



2. ábra: Hogyan működik a folyamatos biztonságnyújtás

IP-agnosztikus eszközujjlenyomat-vétel a botvédelem érdekében

Az AppWall *Device Fingerprinting* és *Activity Tracking* moduljai IP-agnosztikus nyomkövetést kínálnak a fejlett botok (mint például a web scraping, webalkalmazás DDoS, jelszófeltörő és kattintáseltérítő brute force támadások) okozta veszélyek elhárítása érdekében. Az AppWall képes észlelni a dinamikus IP környezetben működő nyomokat és a forrás NAT mögötti aktivitást, mint amilyen a vállalati hálózat vagy proxy. Még ha a bot dinamikusan meg is változtatja az eredeti IP-címét, az ujjlenyomata nem változik meg. Az AppWall nyomon követi az eszközaktivitást, és az idő múlásával egymáshoz viszonyítja a forrás biztonsági kihágásait több munkameneten keresztül.

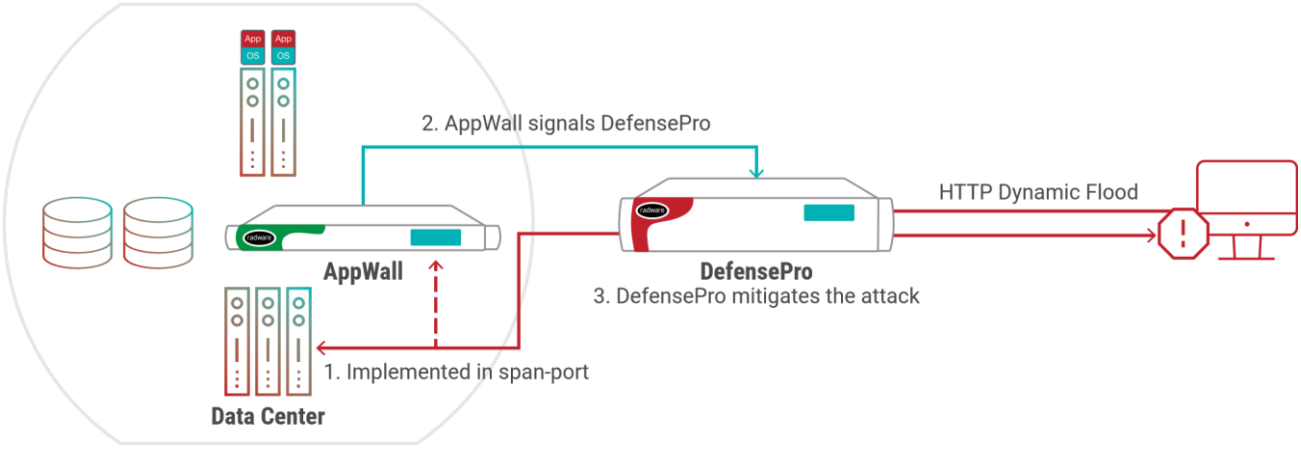
Egyedi 'out-of-path' telepítés teljes vonalsebességű védelemmel

Az AppWall az egyetlen olyan WAF, amely 'out-of-path' módon telepíthető, miközben változatlanul teljeskörű védelmet nyújt. A Radware integrált támadáselhárító megoldása, a *DefenseMessaging*, egy egyedi üzenetküldő mechanizmus, amellyel az AppWall jelezni tud a Radware határvonalvédelmi eszközének, a *DefensePro*-nak, amikor egy webalkalmazás elleni támadást észlel. A *DefensePro* a hálózat határvonalán blokkolja a támadást és megvédi a hálózat többi részét.

Amikor az AppWall észlel egy webes támadást, automatikusan üzenetet küld a hálózat határára telepített *DefensePro*-nak, amely valós időben hárítja el és blokkolja a támadásokat.

Ez az egyedülálló *Defense Messaging* mechanizmus 'in-line' és 'out-of-path' módon telepített AppWall esetén egyaránt használható, hogy biztosítani lehessen a webes támadások elleni vonalsebességű védelmet, minden további látencia, teljesítménycsökkenés vagy kockázat nélkül. További képességek:

- Vonalsebességen történő védelem, legfeljebb 400 Gbps, 330M DDos PPS, 60 mikroszekundumos látenciával.
- A tartalomelosztó hálózatok (CDN) mögötti webalkalmazásokat megcélzó kibertámadások elhárítása.
- Fejlett http alapú DDoS-támadások (Slowloris, dinamikus flooding), bejelentkező oldalak elleni brute force támadások és SSL-alapú támadások blokkolása.
- A támadás forrásának blokkolása a hálózat peremén, mielőtt behatolna a szervezet hálózatába, megvédve így a többi alkalmazást és szolgáltatást.
- Többrétegű észlelés és védelem biztosítása.



3. ábra: 'Out-of-path' észlelés, a hálózat szélén lévő DefensePro értesítése, vonalsebesség

Minden egyben alkalmazáskézbesítés és -biztonság

Mikor az AppWall a Radware alkalmazáskézbesítési vezérlője, az Alteon NG részeként kerül telepítésre, ez a megoldás az elérhetőség, a gyorsulás és a biztonsági szolgáltatások átfogó halmazát nyújtja annak érdekében, hogy gyorsan, megbízhatóan és biztonságosan végezhesse a kritikus webalkalmazások kézbesítését.

Az AppWall példányok erőforrásai dinamikusan allokálhatók a szervezet igényei szerint, továbbá hibaelszigetelést, SLA-biztosítékot és nagy platformsűrűséget kínálnak.

A megoldás egyaránt támogatja az 'out-of-path' és az 'in-line' telepítési módokat, és többfajta platformon is üzembe helyezhető 80 Gbps sebességhatárig.

Teljeskörűen menedzselt webalkalmazás-védelem

Mivel átlátja azokat a kihívásokat, amelyekkel a szervezetek szembesülnek a webalkalmazás-védelmi megoldások menedzselése és üzemeltetése során, a Radware olyan megoldásokat nyújt, amelyeket teljes egészében a Radware biztonsági szakértői kezelnek. A Radware teljeskörűen menedzselt felhőalapú WAF szolgáltatása mellett, a Radware AppWall ügyfelei számára is elérhető a Radware vészhelyzeteket elhárító biztonsági csoportja által nyújtott menedzsment szolgáltatás, az ERT Premium, melybe beletartozik a helyszíni WAF eszköz folyamatos üzemeltetése, felügyelete és konfigurációja.

Hitelesítési átjáró

Az AppWall felhasználóhitelesítési és egyszeri bejelentkezési (SSO) megoldása a webalkalmazások előtt elhelyezkedő autentikációs szintként funkcionál. Kétlépcsős hitelesítést alkalmaz, engedélyezi és végrehajtja a Web Access Control policyt, és a vállalati hálózaton kívülről biztosít hozzáférést a helyszínen futó alkalmazásokhoz. Különféle hitelesítési sémákat támogat, köztük az FBA-t (űrlap alapú hitelesítés), az NTLM-et és a KCD-t (Kerberos által korlátozott delegálás).

ÜZLETI ÉRTÉKEK

A legjobb biztonsági lefedettség

- **Támadások elhárítása a teljesítmény csökkenése vagy további kockázatok nélkül**
- **Webalkalmazások biztonságos elérhetősége**
- **Auditálásra kész és alkalmazásbiztonsági láthatóság**
- **Adatvesztés megelőzése**

A leggyorsabb üzembe helyezés

- **Kritikus webalkalmazások gyors, megbízható és biztonságos kézbesítése**

Védett és folyamatos webalkalmazás-kézbesítést tesz lehetővé

- **DAST-integráció a valós idejű webes biztonsági patchelés érdekében**

A legegyszerűbb üzemeltetés

- **Alacsony üzemeltetési költségek és telepítés utáni problémamentesség**
- **Hatékonyabb kockázatkezelés**

Többvektoros, szerepalapú biztonsági policy

Az AppWall hitelesítés és SSO használatával az egyes alkalmazásbeli vagy szervezeti webes szerepkörök (alkalmazottak, partnerek, ügyfelek stb.), valamint a biztonsági policyk (mint például az alkalmazáshoz történő hozzáférés, adatok láthatósága és webes biztonság) érvényesíteni tudják a feladatok elkülönítését, ami biztosítja, hogy az adatokhoz való hozzáférés üzleti igények alapján történjen.

Megfelelőség

Az AppWall képessé teszi a szervezeteket, hogy teljes egészében megfeleljenek a PCI DSS 6.6-odik szakasz követelményeinek, és magában foglalja a legrészletesebb grafikus jelentéseket az alkalmazásbiztonság és az észlelt támadások vizuális megjelenítésére. Az AppWall szintén részletes PCI-megfelelőségi jelentése elemzi a biztonsági policykat, valamint közli az automatikus megfelelés státuszát és a kötelező megfelelőségi akciótervet.

A Radware-ról

A Radware® (NASDAQ: RDWR) globális vezető a kiberbiztonsági és alkalmazáskézbesítési megoldások területén, fizikai, felhőalapú és szoftver által definiált adatközpontok számára. Megoldásainak díjnyertes portfoliója biztosítja a digitális élményt azáltal, hogy globálisan infrastruktúra-, alkalmazás- és céginformatikai védelmet kínál a vállalkozásoknak. A Radware megoldásai világszerte több mint 12 500 vállalati és szállítmányozási ügyfelet tesz képessé arra, hogy gyorsan alkalmazkodjon a piaci kihívásokhoz, fenntartsa az üzleti folytonosságot és maximális termelékenységet érjen el a költségek alacsonyan tartása mellett. A további információkért, kérjük, látogasson el a www.radware.com weboldalra.

A Radware arra biztatja Önt, hogy csatlakozzon a közösségünkhöz, és kövessen minket a következő felületeken: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app iPhone®-ra, illetve a DDoSWarriors.com biztonsági központunk, amely átfogó elemzést közöl DDoS eszközökről, trendekről és veszélyekről.

Certainty Support

A Radware a *Certainty Support* programján keresztül műszaki támogatást kínál minden termékére. A program minden szintje négy elemből áll: telefonos támogatás, szoftverfrissítések, hardverkarbantartás és helyszíni támogatás. Továbbá a Radware elkötelezett mérnökgárdája szakmai szolgáltatás alapon segít az ügyfeleknek az összetett projektek megvalósításában.