WAF
Web Application Firewall

Trustwave®
Security begins with Trust℠

WebDefend

WEB APPLICATION FIREWALL (WAF)
bezpečnost pro webové aplikace a servery

WebDefend od společnosti Trustwave je robustní webový aplikační firewall (WAF), který poskytuje webovým aplikacím v reálném čase neustálou ochranu před útoky a krádežemi dat. Zajišťuje jejich bezproblémový chod a pomáhá upevnit shodu s oborovými standardy jako je např. PCI (Payment Card Industry) DSS (Data Security Standard). Využitím obousměrné analýzy provozu, automatizované profilace chování a vícenásobných detekčních mechanismů identifikuje WebDefend také události mající potenciální vliv na bezpečnost, funkci a dostupnost webové aplikace.

Nejlepší dostupná detekce a prevence útoků

WebDefend poskytuje bezkonkurenčně nejlepší detekci a ochranu proti zranitelnostem a nebezpečným útokům jako je např. „site scraping", „malicious bots", „Google™ hacking", útokům v čase nule a cíleným útokům. Pro dosažení komplexní a přesné ochrany analyzuje WebDefend příchozí i odchozí provoz z webové aplikace, přičemž koreluje data z různých detekčních systémů, např:

⇒ Adaptivní aplikační profilovací systém kontinuálně buduje dynamický bezpečnostní model každé chráněné webové aplikace, který zaručuje, že pouze validní provoz je povolen.

⇒ Systém „ExitControl" analyzuje odchozí provoz z hlediska potenciálního úniku citlivých dat, maskování dat a získávání informací pro řízení bezpečnosti.

⇒ Signatury vyvinuté laboratořemi Trustwave poskytují bezkonkurenčně nejaktuálnější zdroj aplikačních signatur a informací o známých zranitelnostech webových aplikací.

Soubor monitorovacích a blokačních funkcí umožňuje organizacím přizpůsobit reakce WebDefendu. Používá TCP resety, agenty na webových serverech, externí zařízení (firewally,…), logování a uzamykaní uživatelů, atp.

Klíčové přínosy:

⇒ Poskytuje bezkonkurenční ochranu citlivých a důvěrných dat

⇒ Možnost nasazení virtuální appliance do prostředí VMware.

⇒ Flexibilní nasazení:
IN-LINE / **OUT- OF-LINE**

⇒ Umožňuje organizacím identifikovat aplikační události, které ohrožují zisk, snižují důvěru zákazníků a v nepo-slední řadě představují riziko pro datová aktiva

⇒ Poskytuje základ pro kvalitní a včasnou komunikaci mezi odděleními bezpečnosti, vývoje a managementu

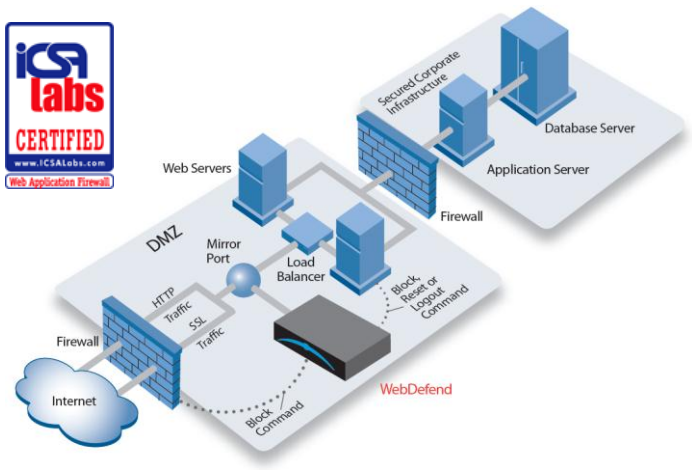
⇒ Výrazně napomáhá udržovat shodu s oborovým standardem PCI DSS – požadavky 2,3,4,5,6,7,8,10,11, 12

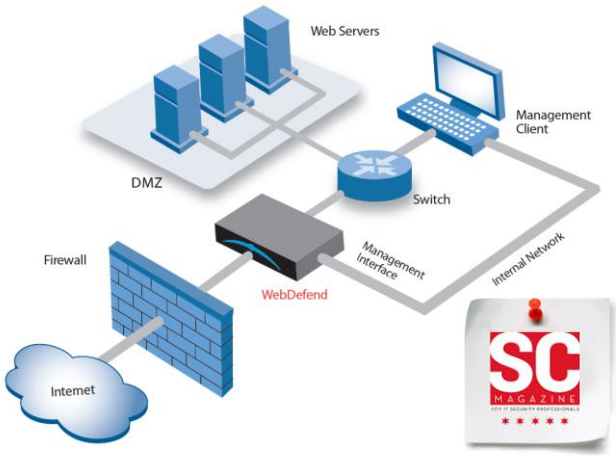
⇒ Podporuje a využívá stávajících investic do infrastruktury (firewally, SIEM)

Trustwave je celosvětovým lídrem v oblasti ochrany webových aplikací

Robustní provedení – snadná instalace

WebDefend je vyvinut pro velké organizace. Jeho architektura umožňuje řídit a chránit více data center najednou. Kterýkoli senzor je možné zapojit v páru pro zajištění vysoké dostupnosti. K dispozici je také centrální správa „WebDefend Manager". **Pro zajištění neintruzivního nasazení v celé distribuované architektuře, může být instalován „out-of-line"** nebo transparentně „in-line", bez potřeby jakéhokoli přenastavení sítě – viz následující obrázky.





COMGUARD
security & networking

COMGUARD s.r.o.
Sochorova 38, CZ 616 00 Brno
tel. +420 513 035 400
info@comguard.cz | www.comguard.cz

WAF
Web Application Firewall

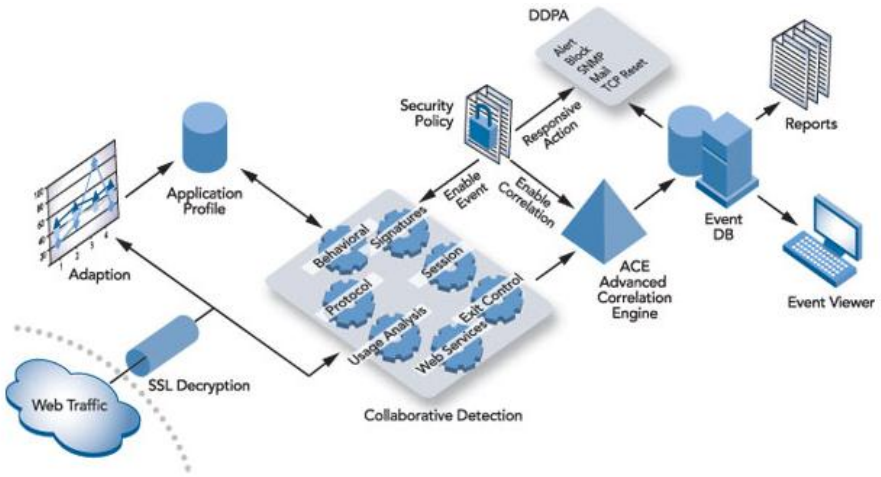
Trustwave®
Security begins with Trust℠

Out-of-the-Box shoda se standardem PCI

WebDefend obsahuje přednastavené „PCI" politiky a reporty pro organizace, které chtějí vyhovět požadavkům standardu PCI DSS. Tyto politiky zaručují správnou konfiguraci pro prevenci útoků a logování v souvislosti s užíváním systémů pro platební katy. Specifické reporty poskytují okamžitý přehled o shodě a používání citlivých dat pro auditní účely.

Okamžitá detekce bezpečnostních událostí

WebDefend provádí kontinuální vyhodnocování každé chráněné aplikace tak, aby identifikoval události, které mohou ovlivnit bezpečnost aplikace, její funkčnost a dostupnost. Události zahrnují programátorské chyby, selhání aplikace a nebezpečné kódování. Když je taková událost zjištěna, WebDefend zajistí všechny požadavky a reakce stejně jako náhled události skrz prohlížeč tak, aby mohl být problém jednoduše pochopen a rychle vyřešen.



Intuitivní / instruktivní konzole

Snadno použitelná WebDefend Management konzole poskytuje z jednoho místa konfiguraci i monitoring. Je velmi intuitivní, a proto nevyžaduje žádné školení k tomu, aby administrátor rychle pochopil architekturu a bezpečnost webové aplikace. Umožňuje chápat události v kontextu, což vede k rychlému řešení problémů. Každá detekovaná událost je detailně popsána, přičemž je zdůrazněno jádro problému. Konzole poskytuje několik pohledů na událost s podrobným rozpadem informací. Snadno a rychle jsou k dispozici informace o hlavní příčině, celých transakcích i chybových hlášeních předložených návštěvníkům stránky. Vše doplňuje sofistikovaný reportovací nástroj.

E-mailový tiketovací systém usnadňuje vývoj webových aplikací

WebDefend umožňuje bezpečnostním týmům vytvářet tikety pro vývojové a testovací týmy, a to jednoduše kliknutím pravým tlačítkem na danou událost v seznamu detekovaných událostí a chyb. Tiket obsahuje podrobný popis události, detailní popis řešení, link pro získání dalších informací a vzorek požadavku a odezvy pro demonstraci události. Tyto kompletní informace je možné komunikovat v běžném jazyce, což šetří čas a zkvalitňuje výstupy v podobě oprav a nových verzí webové aplikace.

SSL dešifrace

WebDefend replikuje a dešifruje SSL streamy bez terminace původních šifrovaných spojení. Okamžitě po dešifraci WebDefend důkladně kontroluje provoz příchozí i odchozí v rámci webového prostředí, přičemž zachovává plnou viditelnost i detekovatelnost útoků bez kompromitace provozu.

Distribuovaná detekční / prevenční architektura

Unikátní detekční / prevenční architektura WebDefendu poskytuje centrální bod inteligence s flexibilní distribuovanou prevencí tak, aby mohly organizace plně využít stávajících investic do infrastruktury. Řešení lze integrovat se síťovými firewally, webovými servery, produkty typu SIEM (Security Information and Event Management), což ve výsledku umožňuje organizacím řídit bezpečnost webových aplikací tak, jak řídí samotné aplikace.

Modelová řada WebDefend	TX30i System	TX60i System	TX110i System	TX120i System
CPU	1 x Quad Core 2.4 GHz	1 x Quad Core 2.0 GHz	2 x Quad Core 2.0 GHz	2 x Quad Core 2.4 GHz
Síť	Silicon Dual Port Copper Bypass	Silicon Dual Port Copper Bypass	Silicon Quad Port Copper Bypass	Silicon Quad Port Copper Bypass
Počet transakcí / sec	7000	9000	13000	20000
Max počet webových stránek (unikátní IP & Port combo)	30	60	200	200
Propustnost (všechny prvky aktivní)	50Mb/s (40% SSL)	100Mb/s (50% SSL)	600Mb/s (50% SSL)	1000+Mb/s (50% SSL)
Možnosti nasazení	In-line / Out-of-Line	In-line / Out-of-Line	In-line / Out-of-Line	In-line / Out-of-Line

COMGUARD
security & networking

COMGUARD s.r.o.
Sochorova 38, CZ 616 00 Brno
tel. +420 513 035 400
info@comguard.cz | www.comguard.cz