

Breach ModSecurity Pro™ M1000 Appliance



Produktový list

ModSecurity Pro™ M1000 Appliance

*Breach Security, Inc. je lídrem na dynamicky se rozrůstajícím trhu inteligentních řešení ochrany web serverů. **Produkty společnosti chrání více než 10000 web serverů** po celém světě. Appliance M1000 v sobě integrují řešení potřeb firemních sítí s legislativními normami a standardy. Svým pojetím jsou předurčeny k ochraně kritických systémů a podílejí se tak na zajištění kontinuity podnikání. Toto poslání naplňují díky kombinaci nejnovějších detekčních a preventivních technologií, které jsou schopny ochránit citlivé web systémy před cílenými útoky na aplikační úrovni.*

BREACH™
Nekompromisní
ochrana web
serverů

Ochrana na aplikační vrstvě:

- ✓ **Ochrana proti útokům na webové servery na aplikační vrstvě** jako jsou:
 - SQL Injections
 - Cross-site Scripting (XSS)
 - OS Command Execution
 - Remote Code Inclusion
 - Buffer Overflows
- ✓ **Automatická detekce nebezpečných aktivit:**
 - Detekce Botů, Crawlerů, Scannerů
- ✓ **Detekce nedodržení RFC u HTTP/S protokolů** a lokálně definovaných politik užití
- ✓ **Ochrana proti ztrátě citlivých informací**
 - Blokuje odesílání citlivých dat v odchozím provozu a detekuje útoky Trojských koní

Flexibilní technologie ModSecurity

Jejím hlavním posláním je detekovat a preventivně chránit web servery před útoky na aplikační úrovni v příchozím provozu a blokovat citlivá data v odchozím provozu. Dále dokáže filtrovat šifrovaný SSL provoz a je také velmi platným nástrojem jako auditovací zařízení pro HTTP, jelikož dokáže uchopit všechny požadavky na provoz. Dalšími důležitými funkcemi systému ModSecurity jsou:

- **Session Management** – ModSecurity dokáže vystopovat a monitorovat uživatelská spojení, což přináší ochranu před útoky typu session hijacking a podporu pro detekci anomálií navázaných spojení.
- **Korelace událostí** – umožňuje detekci širokého spektra útoků zahrnující DoS útoky, útoky hrubou silou, stejně jako „průzkumnické“ útoky. Tato funkce pak nedovolí hackerům provést skutečný nebezpečný útok.
- **Engin pro pokročilé analýzy:** - velmi podrobná pravidla se umožňují zaměřit na analýzu specifických HTTP komponent. Příklad: vyhledávání signatur v hlavičkách odpovědí.

Klíčové charakteristiky ModSecurity Pro™ M1000 Appliance:

- ✓ **Ochrana na aplikační úrovni před známými i neznámými útoky** - negativní i pozitivní bezpečnostní modely
- ✓ **Virtuální záplatování** web aplikací
- ✓ **Out-of-the-Box ochrana** - ModSecurity Pro M1000 poskytuje okamžitou ochranu na aplikační úrovni, která se velmi snadno nasazuje do každé sítě
- ✓ **Certifikovaný předdefinovaný set pravidel** – tato pravidla představují velmi rychlou a efektivní ochranu před útoky na známé zranitelnosti a zároveň přináší jistotu vyhovění specifickým bezpečnostním normám a standardům.
- ✓ **Speciální pravidla pro ochranu Microsoft™ Outlook web Access (OWA)**
- ✓ **ModSecurity GUI Management Console** – administrace probíhá přes web rozhraní. Předností je snadné použití a umožnění rychlého přehledu o stavu systému.
- ✓ **Shoda s PCI** – v roce 2004 byly sjednoceny bezpečnostní požadavky na provoz karetních platebních systémů na webu, které jsou známy jako Payment Card Industry (PCI) Data Security Standard. Vznikly za spolupráce mezi společnostmi Visa a MasterCard. Jedním z požadavků tohoto standardu je instalace firewallu chránícího web servery platebních systémů až po aplikační úroveň.
- ✓ **Reverzní Proxy** - pracující jako inline reverzní proxy host, provádí M1000 appliance široké spektrum kontrol, monitorování provozu a reakce na útoky v reálném čase. Reverzní proxy jsou nasazeny před web servery, kde poskytují další úroveň bezpečnosti.

Breach ModSecurity Pro™ M1000 Appliance



Produktový list

ModSecurity je extrémně flexibilní technologie, která dokáže chránit jakoukoli web aplikaci včetně originálně vyvíjených vlastních aplikací a to přesto, že se u nich neumí automaticky učit jejich funkce. Dovoluje totiž zadávat vlastní pravidla a tím posílit celkovou ochranu o pozitivní modely zabezpečení systémů. Pro komplexnost nabízí Breach Security pro webové stránky využívající formuláře a interaktivní stránky profesionální služby pro analýzu a tvorbu vlastních pravidel.

Ochrana zranitelností – virtuální záplatování

Fixace a záplatování zranitelností web aplikací vždy vyžaduje určitý čas a jelikož mají organizace zřídka kdy přístup ke zdrojovým kódům, jsou prakticky vydány na milost výrobcům. Musí čekat na příslušnou opravu. Dokonce i v případě, kdy mají ke zdrojovému kódu přístup, uplyne nějaký čas, než je patch vyvinut a úspěšně aplikován.

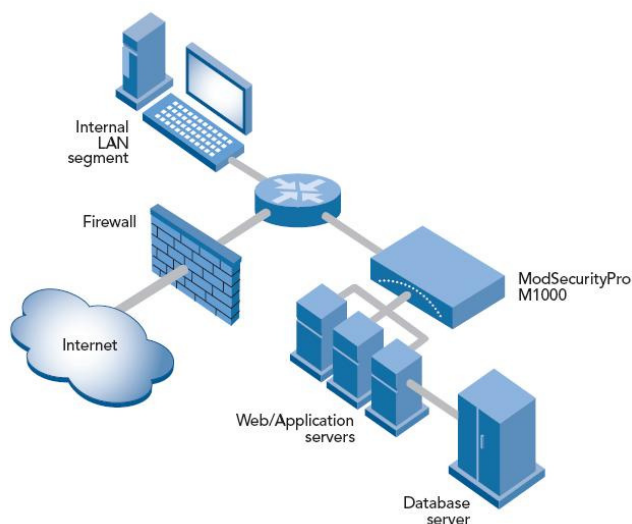
Externí záplatování (nazývané také „just-in-time záplatování“ nebo „virtuální záplatování“) je jedním ze zásadních přínosů web aplikačních firewallů. Jakmile WAF (web application firewall) obdrží požadavek na spojení, prozkoumá jeho bezpečnost a jednoduše ho zahodí v případě, že jde o útok. Toto je nejsnazší cesta jak „záplatovat“ známé zranitelnosti web aplikací.

Díky novým a novým zranitelnostem vznikají vždy okna příležitostí pro útoky na ně. Elegance řešení pomocí WAF spočívá v tom, že je problém vyřešen externě. Vytvoření pravidla na WAF, které chrání specifickou zranitelnost totiž obvykle nepředstavuje velký problém, většinou to může být otázka pouhých 15 minut. Výsledkem je však opětovné nabytí kontroly nad web aplikací a riziko je maximálním způsobem eliminováno.

Kompatibilita s Payment Card Industry Data Security Standard (PCI DSS)

ModSecurity je nejlepší volbou pro organizace požadující nákladově efektivní řešení pro ochranu web aplikací a shodu se standardy jako je Payment Card Industry Data Security Standard (PCI DSS).

ModSecurity Pro M1000 spolu s množinou pravidel PCI poskytuje ochranu proti útokům na webové aplikace, které jsou definovány ve standardu DSS. Navíc, nasazení ModSecurity Pro M1000 zajišťuje splnění shody s článkem 6.6 zmíněného standardu, což dovoluje chránit aplikace systémem ModSecurity Pro M1000 podstatně snadněji, než podrobování se nákladnému a čas konzumujícímu bezpečnostnímu revidování kódu při každém updatu vlastní aplikace. Breach Security je členem rady pro PCI Standard a tím je pro koncové uživatele zaručena jistota dlouhodobého vývoje a kompatibility s PCI standardem.



Profesionální podpora kontinuity služeb

Breach Security nabízí možnost záložní „cold spare“ appliance, která je připravena k nasazení v případě, že primární selže. Alternativně lze nastavit u některých firewallů konfiguraci automatické redirekce provozu na pasivní appliance, když má primární výpadek.

Breach Security nabízí pro všechny komerční uživatele ModSecurity Pro:

Technické specifikace:

- NIC 10/100/1000
- Podpora RSA autentizace a algoritmu výměny klíčů
- FIPS 140-2 Level 2 and 3 vyhovující uložení klíčů
- Podpora všech běžných šifrovacích a MAC klasifikačních algoritmů jako je: DES, Triple-DES, RC4, RC2, MD5, SHA, SHA1

- | | |
|--|--|
| ✓ 24 x 7 telefonická a emailová podpora | ✓ Ladění logování a updaty do system level bugs |
| ✓ Základní asistence při nasazení a instalaci | ✓ Asistence u updatů na novější verze |
| ✓ Přístup ke všem ModSecurity system level updatům | ✓ Záruka na hw formou výměny (pouze pro ModSecurity Pro M1000) |
| ✓ Asistence u analýz Audit logů | ✓ Rozšířený balíček pravidel |