



Společnost **Barracuda Networks**, sídlící v Silicon Valley, působí celosvětově s více než 1 500 zaměstnanci a nabízí špičková, komplexní a cenově dostupná řešení v oblasti zabezpečení IT. Ve více než 225 000 organizací po celém světě, od malých a středních podniků po velké společnosti, pomocí inovativních řešení zabezpečuje ochranu e-mailů, chrání firemní aplikace a cloudová řešení, zabezpečuje sítě a chrání firemní data.

Barracuda Networks je partnerem Amazon Advanced Technology Partner a **Microsoft Partner of the Year Winner** (cena za řešení ISV s certifikací Microsoft Azure) a pomohla desítkám tisíc zákazníků bezpečně přejít na Office 365 a Azure.

Společnost **Barracuda Networks** získala ocenění Comparably za **Best Company Culture** a byla také zařazena do seznamu do seznamu 25 nejžhavějších společností CRN 2021 **Edge Security Computing 100**.

Více na stránkách výrobce www.barracuda.com

Web Application Firewall

Zabezpečení aplikací je stále složitější. Barracuda to zjednodušuje. Barracuda Web Application Firewall je součástí Barracuda Cloud Application Protection, integrované platformy, která spojuje komplexní sadu interoperabilních řešení a funkcí pro zajištění kompletního zabezpečení aplikací.

- Zajištění ochrany před webovými útoky a DDoS.
- Zastavte špatné roboty v jejich stopách.
- Chraňte své rozhraní API a mobilní aplikace.
- Umožněte granulární řízení přístupu a bezpečné doručování aplikací.
- Automatizujte a orchestrujte zabezpečení.
- Report.

Zajištění ochrany před webovými útoky a DDoS.

Brána Barracuda Web Application Firewall chrání aplikace, rozhraní API a backendy mobilních aplikací před různými útoky, včetně útoků podle seznamu OWASP Top 10, hrozby typu zero-day, úniku dat a útoků typu DoS (denial of service) na aplikační vrstvě. Kombinací zásad založených na signaturách a pozitivním zabezpečení s robustními funkcemi detekce anomálií dokáže Barracuda Web Application Firewall porazit nejsložitější útoky, které dnes cílí na vaše webové aplikace.

Barracuda Active DDoS Prevention - doplňková služba pro Barracuda Web Application Firewall - filtruje volumetrické DDoS útoky dříve, než se vůbec dostanou do vaší sítě a poškodí vaše aplikace. Chrání také před sofistikovanými aplikačními DDoS útoky bez administrativních a zdrojových nákladů tradičních řešení, aby se eliminovaly výpadky služeb a zároveň se udržely přijatelné náklady pro organizace všech velikostí.

Pokročilá ochrana proti botům.

Sofistikovaní škodliví boti napodobují lidské uživatele, aby se vyhnuli standardní detekci botů. Moderní ochrana proti botům tedy musí rozlišovat jak mezi legitimními a škodlivými boty, tak mezi lidskými uživateli a pokročilými boty. Barracuda Web Application Firewall nabízí pokročilou ochranu proti botům, která využívá strojové učení k neustálému zlepšování své schopnosti odhalovat a blokovat špatné boty a boty napodobující lidi.

Chraňte své rozhraní API a mobilní aplikace.

Barracuda Web Application Firewall chrání rozhraní REST API a aplikací založených na API. Ochrana XML zabezpečuje rozhraní REST a WSDL proti otravě schémat a WSDL. Ochrana JSON skenuje užitečná zatížení, aby zajistila, že budou propouštěny pouze legitimní požadavky. Funkce API Discovery využívají vaše soubory s definicemi API k automatickému vytvoření požadovaných sad pravidel pro API, čímž snižují režii správce.

Umožňuje granulární řízení přístupu a bezpečné doručování aplikací.

Řešení Barracuda Web Application Firewall se integrují s AD, LDAP a RADIUS, abyste zajistili, že k backendům aplikací a datům budou mít přístup pouze oprávnění pracovníci, což vám umožní granulární kontrolu nad tím, kteří uživatelé a skupiny mohou přistupovat k jakým datům. Zabezpečují také všechny služby, které se spoléhají na ADFS. Podpora SAML poskytuje bezproblémové jednotné přihlášení (SSO) napříč lokálními i cloudovými aplikacemi. Dvoufaktorové ověřování dále zvyšuje zabezpečení díky integraci s RSA SecureID, SMS PASSCODE, Duo a dalšími.

Brána Barracuda Web Application Firewall je vybavena zabezpečeným zásobníkem SSL/TLS, který poskytuje bezpečný front end HTTPS pro vaše aplikace. Díky předpřipraveným šablonám můžete okamžitě a snadno nastavit bezpečné šifry a protokoly TLS pro zajištění shody se standardy.

Vestavěný modul pro doručování aplikací umožňuje vyrovnávání zátěže HTTP, směrování obsahu, ukládání do mezipaměti a kompresi. Modul směrování obsahu lze použít k nasměrování provozu na různé aplikace na základě charakteristik příchozího provozu – například jiný server pro PC a jiný pro mobilního klienta. Funkce sdružování připojení, ukládání do mezipaměti a komprese urychlují doručování provozu a zlepšují uživatelský komfort snížením zatížení serveru a snížením latence.

Automatizace a orchestrace zabezpečení.

Barracuda Web Application Firewall se integruje s mnoha oblíbenými nástroji DevOps třetích stran, aby byly procesy CI/CD plně automatizovány. Plnohodnotné rozhraní REST API se bezproblémově integruje s aplikacemi Puppet, Chef, Ansible, Terraform, Azure ARM, AWS CloudFormation a dalšími. Modul směrování obsahu navíc dále umožňuje možnosti nasazení CI/CD, jako je modrozelené nasazení, kanárkové nasazení a A/B testování. Rozhraní REST API brány Barracuda Web Application Firewall je postaveno na specifikacích OpenAPI, což usnadňuje vytváření automatizačních skriptů, a na oficiální stránce GitHub jsou k dispozici ukázky kódu pro populární platformy a případy použití.

Řešení Barracuda Web Application Firewall využívají služby Barracuda Vulnerability Manager a Remediation Service, které umožňují odstraňovat zranitelnosti aplikací jediným kliknutím a s plnou důvěrou nasazovat nové a aktualizované aplikace. Barracuda Web Application Firewall také podporuje mnoho nástrojů třetích stran pro skenování zranitelností, jako jsou IBM AppScan, Rapid7, Immuniweb, HPE Security WebInspect a další, abyste měli úplnou svobodu a kontrolu nad odstraňováním zranitelností.

Získejte hluboký přehled o útocích a vzorcích provozu.

Brána Barracuda Web Application Firewall je vybavena podrobným řídicím panelem, který prezentuje obrovské množství dat v podobě praktických informací, které vám pomohou přijímat informovaná rozhodnutí. Stav a využití systému, vzorce provozu, stav předplatného, výkon systému, statistiky útoků a místa jejich původu a mnoho dalšího je rozvrstveno do přehledného ovládacího panelu, který umožňuje snadnou interpretaci a použití. Barracuda Web Application Firewall podporuje také mnoho externích SIEM a nástrojů pro správu protokolů, jako jsou Azure Sentinel, Loggly, Sumologic, HPE ARCSight, IBM QRadar, Splunk a mnoho dalších.

Otestujte si webové aplikace na zranitelnosti ještě dnes.

[Free Web App Vulnerability Scan](#)

Ocenění: Produkt byl oceněn v recenzi prestižního magazínu pro IT bezpečnostní experty SC Magazine hodnocením „Best Buy“ za jednoduchou instalaci, kvalitní funkcionality a také nízkou cenu. Ve všech testovaných kategoriích získal plný počet bodů, přičemž redakce nezjistila žádné slabiny produktu.

Distributor pro ČR a SR:

atlantis telecom spol. s r.o. | Štěrboholská 1427/55 | 102 00 Praha 10 - Hostivař
Telefon: +420 271 004 208 | <http://www.atlantis.cz> | networking@atlantis.cz

