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

Chraňte své aplikace pomocí jedné jednoduché platformy

Začněte s flexibilními a výkonnými řešeními WAF.

Řešení Barracuda Web Application Firewall (WAF) jsou k dispozici jako zařízení (hardwarová nebo virtuální), která lze implementovat v prostorách společnosti nebo hostovat v cloudu, jako kontejner a prostřednictvím inovativního řešení SaaS, které kombinuje pokročilé funkce se snadným nasazením a správou. Webový aplikační firewall Barracuda v kontejneru lze nasadit a spravovat pomocí řešení SaaS, což poskytuje možnost používat jedno nebo obě řešení podle vašich potřeb.

S oběma modely nasazení získáte kompletní zabezpečení aplikací, včetně ochrany před **10 nejčastějšími hrozbami OWASP** pro web a API a mnoha dalšími zranitelnostmi a automatizovanými hrozbami, spolu s automatickou detekcí a nápravou. V porovnání s mnoha konkurenčními řešeními je nasazení, konfigurace a správa řešení Barracuda WAF pozoruhodně jednoduchá, a to díky funkcím, jako je například automatická konfigurace založená na strojovém učení.

Barracuda Active Threat Intelligence shromažďuje data o hrozbách z rozsáhlé instalované sítě senzorů a provozu zákazníků. Tato data jsou zpracovávána pomocí strojového učení téměř v reálném čase a okamžitě rozesílána připojeným jednotkám, což umožňuje rychlou detekci nových hrozeb a útočníků.

Barracuda Active Threat Intelligence obsahuje několik komponent. Barracuda Vulnerability Manager a Remediation Service poskytují možnosti skenování a nápravy. Barracuda Advanced Threat Protection je cloudový sandbox, který skenuje a identifikuje pokročilé trvalé hrozby v odeslaných souborech. Barracuda Active Threat Intelligence také obsahuje cloudovou vrstvu strojového učení pro Advanced Bot Protection a Auto Configuration Engine. Auto Configuration Engine je služba, která prověřuje veškerý provoz aplikací z připojených jednotek a poskytuje doporučení konfigurace specifické pro danou aplikaci, čímž snižuje čas a úsilí spojené s režijními náklady na správu.

Zastavte nejpokročilejší škodlivé roboty současnosti.

Hackeři vytvářejí sofistikované roboty, kteří mohou napodobovat lidské uživatele a provádět ničivé útoky. Výzvou je nejen rozlišit legitimní a škodlivé boty, ale také rozlišit skutečné lidské uživatele od nejpokročilejších botů.

Pokročilá ochrana proti botům Barracuda využívá umělou inteligenci a strojové učení, aby neustále zlepšovala svou schopnost odhalovat a blokovat špatné boty a zároveň umožnit legitimnímu lidskému a botovému provozu pokračovat s minimálním dopadem.

Nedovolte, aby útoky DDoS srazily vaši firmu na kolena.

Útoky DDoS (Distributed Denial-of-Service) jsou stále vážnou hrozbou pro podniky všeho druhu. Tím, že znemožní používání vašich aplikací nebo je znepřístupní legitimním uživatelům, mohou efektivně zastavit provoz vaší firmy na delší dobu, což může být nesmírně nákladné. Řešení Barracuda pro zabezpečení aplikací zahrnují výkonnou a plno-spektrální ochranu proti DDoS. Tato schopnost, která pokrývá provoz na 3. až 7. vrstvě a blokuje jak objemové, tak aplikační DDoS útoky, zajišťuje, že vaše kritické obchodní aplikace zůstanou dostupné, přístupné a efektivní bez přerušení.

Ochrana před nebezpečnými útoky v dodavatelském řetězci.

Útočníci využívají skripty třetích stran k provádění digitálních skimmingových útoků na straně klienta, jako je Magecart, ke krádeži osobních a finančních údajů přímo z prohlížeče. Tyto útoky je obtížné odhalit, protože tyto skripty jsou načítány přímo prohlížečem a útočníci používají sofistikované techniky, aby se vyhnuli odhalení pomocí skenerů a podobných obranných metod.

Barracuda Web Application Firewall nabízí funkci Client-Side Protection, která automatizuje konfiguraci CSP a SRI, čímž snižuje režijní náklady správce a chyby v konfiguraci. Kromě těchto funkcí poskytuje vrstva Barracuda Active Threat Intelligence vizualizaci a reporting těchto konfigurací, čímž poskytuje správcům hlubší přehled o používání těchto skriptů.

Kontrolujte, kdo co může vidět.

Kromě obrany proti nejrůznějším kybernetickým hrozbám je také důležité zajistit, aby k zázemí aplikace a datům měli přístup pouze oprávnění pracovníci. Zabezpečení aplikací Barracuda brání tomu, aby se data dostala do nepovolaných rukou, a to díky integraci s AD, LDAP a RADIUS, která vám umožní granulární kontrolu nad tím, kteří uživatelé a skupiny mohou přistupovat k jakým datům.

Řešení Barracuda WAF dokáže zabezpečit všechny služby, které se spoléhají na AD FS. Podpora SAML poskytuje bezproblémové jednotné přihlášení (SSO) napříč lokálními i cloudovými aplikacemi. Dvoufaktorové ověřování dále zvyšuje zabezpečení a integruje se s oblíbenými službami, jako jsou RSA SecureID, SMS PASSCODE, Duo a další.

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.

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.

- Zajistěte ochranu 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.
- Získejte hluboký přehled o útocích a vzorcích provozu.

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 nejsofistikovanější 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.

Zastavte roboty

Sofistikovaní zákeřní roboti napodobují lidské uživatele, aby se vyhnuli standardní detekci botů. Blokování legitimních robotů však může poškodit vaši firmu. Moderní obrana proti botům tedy musí rozlišovat mezi legitimními a škodlivými roboty a mezi lidskými uživateli a pokročilými roboty. Barracuda Web Application Firewall nabízí pokročilou ochranu botů, která využívá strojové učení k neustálému zlepšování své schopnosti odhalovat a blokovat špatné roboty a roboty napodobující člověka – a přitom umožňuje legitimní provoz mezi lidmi a roboty s minimálním dopadem.

Řešení Barracuda Web Application Firewall využívají Barracuda Vulnerability Manager a Remediation Service, aby vám umožnili opravit zranitelnost aplikací jediným kliknutím a nasadit nové a aktualizované aplikace s plnou jistotou. Barracuda Web Application Firewall také podporuje mnoho nástrojů pro skenování zranitelnosti třetích stran, jako je IBM AppScan, Rapid7, Immuniweb, HPE Security WebInspect a další, aby vám poskytl úplnou svobodu a kontrolu nad zmírněním zranitelnosti.

WAF jako služba

Získejte úplné zabezpečení aplikace v pěti snadných krocích. Barracuda WAF jako služba vám dává plnou kontrolu. Díky průvodci nasazením v pěti krocích a předkonfigurovaným sadám pravidel můžete snadno a rychle zahájit provoz. Případně můžete využít praktičtější přístup a vytvořit, doladit a použít vlastní sady pravidel pro konkrétní aplikace, které si vyberete. Ať tak či onak, WAF jako služba vám poskytne kompletní sadu funkcí a možností pro zajištění celkové bezpečnosti aplikací.

Moderní aplikace jsou stále více propojené, což vystavuje útokům více rozhraní API. Barracuda WAF-as-a-Service chrání celý povrch útoků, včetně rozhraní REST API a aplikací založených na API. Funkce API Discovery využívají vaše soubory s definicemi API k automatickému vytvoření požadovaných sad pravidel pro API, což snižuje režijní náklady na správu. Barracuda WAF-as-a-Service nabízí ochranu pro rozhraní API XML i JSON, včetně ochrany před parserovými a DDoS útoky.

Získejte pokročilou ochranu proti DDoS bez dalších poplatků.

Funkce neměřené ochrany proti DDoS vám poskytnou naprostý klid a zablokují celý rozsah hrozeb aplikací - mnohem více než jen deset nejzranitelnějších míst podle OWASP. A na rozdíl od jiných řešení poskytuje WAF jako služba také plnospektrální ochranu DDoS na 3. až 7. vrstvě, aby byla zajištěna nepřetržitá dostupnost aplikací.

Automatické vyhledávání a odstraňování zranitelností.

Složitá nasazení, časté aktualizace aplikací a rychlé nasazení nových aplikací mohou snadno přinést zranitelnosti. Barracuda WAF-as-a-Service využívá náš pokročilý skener zranitelností k neustálému monitorování celého nasazení na zranitelnosti. Můžete je automaticky nebo jediným kliknutím opravit.

Od nuly k zabezpečení během několika minut. Stačí jen 5 kroků a můžete snadno a rychle začít zmírňovat útoky na aplikace.

WAF jako služba 30 denní trial

Load Balancer (rozložení zátěže)

Barracuda Load Balancer ADC je ideální pro optimalizaci výkonu aplikací. Odlehčuje serveru výpočetně náročné transakce SSL, čímž šetří prostředky pro aplikace. Kromě toho optimalizační funkce, jako je ukládání do mezipaměti, komprese a sdružování TCP, umožňují rychlejší doručování aplikací a zajišťují škálovatelnost.

Barracuda Load Balancer ADC, který je k dispozici v hardwarových, virtuálních a cloudových instancích, poskytuje pokročilé vyvažování zátěže na 4. a 7. vrstvě s funkcemi SSL Offloading a Application Acceleration. Vestavěný modul Global Server Load Balancing (GSLB) umožňuje nasadit aplikace na více geograficky rozptýlených místech. Modul Application Security zajišťuje komplexní ochranu webových aplikací, včetně ochrany proti útokům OWASP Top 10 a Application DDoS, a zároveň monitoruje odchozí provoz pro Data Loss Prevention.