KONA SITE DEFENDER

OCHRONA STRON INTERNETOWYCH I APLIKACJI PRZED PRZESTOJAMI I KRADZIEŻĄ DANYCH

Sukces przedsiębiorstwa w dzisiejszym cyfrowym świecie zależy od tego czy jest ono w stanie bez obaw wprowadzać dostępne mu innowacje. Ataki sieciowe takie jak rozproszone ataki Denial-of-Service (DDoS), ataki na aplikacje internetowe i na infrastruktury DNS to dzisiaj największe zagrożenia dla przedsiębiorstw. Ataki te stają się coraz bardziej zuchwałe i dotykają firmy we wszystkich branżach oraz regionach. Powodują przestoje, zwiększają koszty transferu i skutkują utratą poufnych informacji. Mimo ryzyka i wyzwań konsumenci oraz przedsiębiorstwa potrzebują widzieć, słyszeć i działać coraz aktywniej w sieci. Aby odnieść sukces w dzisiejszym cyfrowym świecie, firmy muszą nadal poszerzać swoje oferty internetowe i wprowadzać innowacje bez ciągłej obawy przed intruzami.

Ograniczenia DDoS

Firma Akamai dostarcza ruch internetowy osiągający ponad 80 Tbps. W sieci Akamai ataki mierzone w dziesiątkach a nawet setkach Gbps, są pochłaniane ze względną łatwością. Kona Site Defender chroni przed wszystkimi typami ataków DDoS, atakami direct-to-origin i na aplikacje internetowe – a opcjonalne rozwiązanie firmy Akamai FastDNS ogranicza także ataki na infrastrukturę DNS. Kona Site Defender jest wdrażany na platformie Akamai Intelligent Platform ™, która składa się z ponad 200 000 serwerów rozmieszczonych w ponad 1400 sieciach i więcej niż 110 krajach

Kona Site Defender wykorzystujący inteligentną platformę firmy Akamai, został zaprojektowany w celu udaremniania ataków DDoS poprzez absorbowanie ruchu DDoS skierowanego na warstwę aplikacji, odbijanie całego ruchu DDoS ukierunkowanego na warstwę sieciową np. SYN Floods lub UDP Floods i uwierzytelnianie aktualnego ruchu na granicy sieci.

Ta wbudowana ochrona jest „zawsze włączona" i dozwolony jest ruch wyłącznie na Porcie 80 (HTTP) lub Porcie 443 (HTTPS). Opłaty są ograniczone, dlatego użytkownicy są chronieni przed podwyższonymi kosztami serwisowymi spowodowanymi ruchem DDoS, a elastyczne buforowanie maksymalizuje odciążenie od samego początku.

Inteligentna Platforma Akamai została skonstruowana na skalę masową, w celu ogólnoświatowej dystrybucji po to, by strony internetowe odbiorców zawsze pozostawały dostępne. Ponadto wdrażane są możliwości wprowadzania ograniczeń w ścieżce w sposób natywny, a więc ochrona zapewniona jest nie więcej niż kilka kroków sieciowych od punktu zagrożeni – zatem nie u samego u klienta.

Ochrona warstwy aplikacji

Kona Site Defender zawiera w pełni funkcjonalną ochronę Web Application Firewall (WAF) opartą na prawnie zastrzeżonej technologii, która zapewnia odbiorcom wysoce skalowalną ochronę przed atakami w warstwie aplikacji. Wdrożony Kona Site Defender na globalnie udostępnionej platformie Akamai składającej się z dziesiątek tysięcy serwerów, pomaga wykrywać i usuwać zagrożenia w ruchu HTTP i HTTPS, wydając alerty lub blokując ruch ataku bliżej jego źródła, zanim dotrze do klienta. Ochrona aplikacji webowych Akamai WAF zawiera zestaw reguł Kona Rule Set.

Zestaw Reguł Kona

Kona Site Defender zawiera bogaty zestaw predefiniowanych, konfigurowalnych zasad zabezpieczeń warstw aplikacji (application-layer firewall rules), regularnie aktualizowanych przez firmę Akamai dla różnych kategorii, takich jak: naruszenia protokołu, przekroczenia limitu żądania, naruszenia zasad HTTP, szkodliwych botów, powszechnych ataków i ataków Command Injection, trojany Backdoors i wycieki treści wychodzących (Outbound Content Leakage). Te zasady są łącznie określane jako „Zestaw reguł Kona".

KORZYŚCI

Korzyści biznesowe:

- **Mniejsze ryzyko** przestojów, defacement - zamazywania i kradzieży danych.
- **Ochrona przychodów** lojalność klientów i kapitał marki.
- **Utrzymanie wydajności** w czasie ataku.
- **Mniejsze koszty** związane z obsługą przepięć związanych z ruchem podczas ataku.
- **Mniejsze wydatki** związane z bezpieczeństwem sprzętu i oprogramowania.

Korzyści techniczne:

- **Prosta integracja** z istniejącą infrastrukturą IT.
- **Maksymalizacja czasu nieprzerwanego działania i dostępności** w trakcie ataku DDoS.
- **Obrona** infrastruktury aplikacji internetowych.
- **Ochrona** przed atakami Direct-to-Origin.
- **Poprawa** dostępności infrastruktury DNS.
- **Skalowanie na życzenie.**
- **Dostęp** do najlepszej w swojej klasie eksperckiej aplikacji bezpieczeństwa.

Kona Site Defender

Kona Rule Set obejmuje swoim działaniem najnowsze zagrożenia i ataki z jakimi mogą się spotkać tysiące naszych klientów. Zasady te są regularnie aktualizowane przez Zespół ds. Zagrożeń i są dostępne dla wszystkich odbiorców Kona Site Defender. Chronią przed atakami takimi jak: Low Orbit Ion Cannon, High OrbitIon Cannon, HULK, Dirt Jumper, Havij SQL Injection Tool, Netsparker, ApacheBench, Webhive i inne.
Zasady Kona obejmują:

- Punktację anomalii, przy czym każda reguła przyczynia się do ogólnej oceny ryzyka. Decyzje o alercie lub blokadzie są podejmowane na podstawie całkowitego wyniku.
- Umożliwienie kontroli nagłówków zapytań/odpowiedzi HTTP oraz kontroli zapytań/odpowiedzi HTTP POST poprzez szereg kaskadowych reguł REGEX w celu ochrony przed atakami takimi jak SQL Injections i Cross-Site Scripting.
- Różnorodność funkcji ułatwiających zasady aktualizacji:
  - » Kreator aktualizacji, który umożliwia obecnym klientom aktualizację WAF do najnowszej wersji reguł Kona.
  - » Tryb oceny, który umożliwia klientom zachowanie starszych reguł i zabezpieczeń przy jednoczesnym wprowadzeniu nowych reguł KRS.
  - » Funkcja wersjonowania reguł, która umożliwia klientom przyjęcie nowej lub zmodyfikowanej reguły zgodnie z obowiązującym procesem kontroli zmian.

Kontrole warstw sieci umożliwiają przedsiębiorstwom egzekwowanie zdefiniowanych przez klienta białych i czarnych list adresów IP. Aktualizacje są rozpowszechniane w globalnej sieci Akamai w ciągu kilku minut, umożliwiając szybką reakcję na atak. Inne funkcje obejmują możliwość ograniczenia zapytań z określonych adresów IP w celu ochrony klienta przed atakami na warstwach aplikacji i wdrożenie geo-blokowania. Obsługiwanych jest do 10 000 wpisów CIDR - w tym nazwane listy, takie jak węzły wyjściowe Tora (Tor exit nodes). Białe i czarne listy mogą również być podawane automatycznie przez API blokujące IP.

Kontrole natężenia zapewniają ochronę przed atakami DDoS na warstwie aplikacji przez monitorowanie i kontrolowanie liczby zapytań do serwerów Akamai i klienta. Kona Site Defender może reagować na pojawiające się zapytania w ciągu kilku sekund.

KSD (Kona Site Defender) zapewnia ochronę przed atakami Man-in-the-Middle (MITM) dla jakiegokolwiek ruchu na porcie 443 (SSL lub TLS) i sprawdza ruch plików XML pod kątem niebezpiecznych treści, umożliwiając blokowanie lub ostrzeganie o ryzykownych treściach.

Site Shield (osłona witryny Site Shield) - Kona Site Defender ma możliwość maskowania (ukrywania) pochodzenia klienta w publicznym Internecie. Mapy osłony Site Shield mogą być konfigurowane za pomocą profesjonalnych serwisów lub przy pomocy Luna oraz za pośrednictwem interfejsów API. Osłona witryny ma na celu wsparcie istniejącej infrastruktury i zapobieganie atakom u źródła.

Monitoring bezpieczeństwa Kona Site Defender zapewnia wgląd w incydenty bezpieczeństwa w czasie rzeczywistym, a także daje możliwość wniknięcia w alerty ataku, aby uzyskać szczegółowe informacje o tym, kto atakuje, co atakuje, jakie zdolności obronne wywołał atak a co konkretnie było widoczne w żądaniach, które wywołały mechanizmy ochronne witryny. Monitoring bezpieczeństwa obejmuje możliwość przeglądania szczegółów nagłówka zapytania/odpowiedzi w celu dopasowania reguł i rozpoznania źródła ataku.

Usługa aktualizacji zasad profesjonalny zespół firmy Akamai zapewnia przeglądy konfiguracji Kona Site Defender i WAF'a (Web Application Firewall). Obejmują one false-positive analizę logowań do Kona Security Monitor, rekomendacje dotyczące Kona Site Defender, dostrajanie i optymalizacje konfiguracji.

Szybka ochrona serwera nazw domen FastDNS zapewnia solidne, niezawodne i skalowalne rozwiązanie stworzone, aby zapewnić użytkownikom końcowym bezpośredni dostęp do ich stron internetowych. FastDNS firmy Akamai wykorzystuje dodatkowe autorytatywne nazwy serwerów rozpowszechniane globalnie za pomocą Inteligentnej Platformy Akamai. Nie wymaga to dokonywania zmian w istniejących procesach administrowania DNS i zapewnia niesamowicie solidną, niezawodną, skalowalną i bezpieczną rozdzielczość DNS.

Reputacja Klienta (moduł opcjonalny). Moduł ten uzupełnia Kona Site Defender o wgląd i dodatkową warstwę ochrony przed destrukcyjnymi zjawiskami. Client Reputation zapewnia ochronę skupiając się na źródle zagrożenia. Innymi słowy, moduł ten koncentruje się na klientach internetowych w odróżnieniu od wektorów zagrożeń. Akamai widzi miliardy adresów IP co kwartał. Moduł Client Reputation wykorzystuje zaawansowane algorytmy danych zebranych od klientów internetowych w celu identyfikacji złośliwych zjawisk. Złośliwi klienci sieciowi są punktowani według prawdopodobieństwa zaangażowania w trzy różne typy złośliwego zachowania: skanowanie strony internetowej, ogólne ataki sieciowe i ataki DoS.

Ekosystem Akamai

Dzięki firmie Akamai Internet jest szybki, niezawodny i bezpieczny. Nasze kompleksowe rozwiązania są oparte na globalnie dystrybuowanej platformie Akamai Intelligent Platform ™, zarządzanej przez ujednolicone, konfigurowalne Centrum Sterowania Luna (Luna Control Centre) dla uzyskania maksymalnej widoczności i kontroli. Nasza platforma wspierana jest przez ekspertów, którzy w razie potrzeby i w miarę rozwoju strategii pomogą i zainspirują do wykorzystywania innowacyjnych rozwiązań.

Akamai FASTER FORWARD

As the global leader in Content Delivery Network *(CDN)* services, Akamai makes the Internet fast, reliable, and secure for its customers. The company's advanced web performance, mobile performance, cloud security, and media delivery solutions are revolutionizing how businesses optimize consumer, enterprise, and entertainment experiences for any device, anywhere. To learn how Akamai solutions and its team of Internet experts are helping businesses move faster forward, please visit *www.akamai.com* or *blogs.akamai.com*, and follow *@Akamai* on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers, and contact information for all locations are listed on *www.akamai.com/locations*.