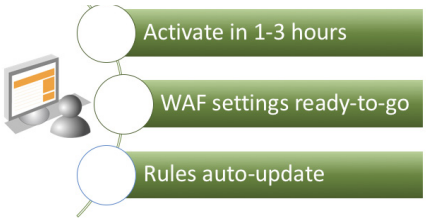
Ochrona Aplikacji Internetowych

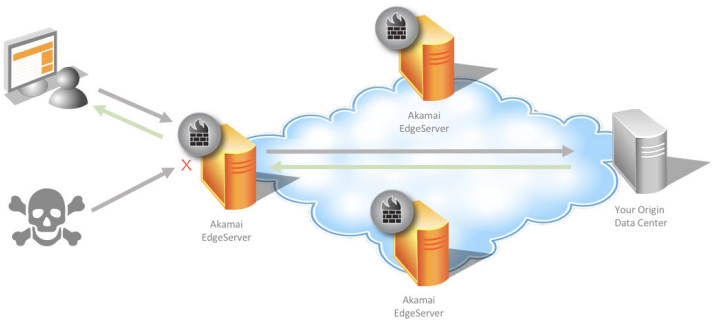
Chroń swoją stronę przed atakami DDoS i atakami na aplikacje internetowe, jednocześnie oszczędzając wysiłek i ogólne koszty. Zapory sieciowe (WAF) są często trudne do wdrożenia i zarządzania, zwłaszcza dla zespołów z ograniczonym personelem ds. bezpieczeństwa. Aplikacja Internetowa Web Application Protector może w tym pomóc oferując prostą konfigurację i zarządzanie jej ustawieniami. Zespół firmy Akamai zajmujący się badaniami nad bezpieczeństwem stale ulepsza dostępne zabezpieczenia, które oferuje produkt, eliminując tym samym potrzebę decydowania o tym, które poszczególne reguły zapory mają zostać uruchomione.

Większość rozwiązań WAF
Wymaga zespołu IT i zespołu obsługi dostawcy

Ochrona Aplikacji Internetowych
Wymaga tylko jednej osoby



Implementacja Web Application Protector jest prosta, a jednocześnie usługa ta zapewnia solidną ochronę, która wykrywa i łagodzi zagrożenia aplikacji w ruchu HTTP i HTTPS, które to próbują przejść przez platformę graniczną Akamai, aby dotrzeć do źródła pochodzenia danych. Platforma specjalizuje się przyspieszonym dostarczaniem treści internetowych zatem należy spodziewać się także znaczącej poprawy prędkości.



Przegląd zabezpieczeń

Usługa ta chroni przed popularnymi exploitami internetowymi bez potrzeby dostrojenia. Jeśli konieczne są poprawki niektórych zabezpieczeń, są one łatwe do zaadaptowania.

Zapora sieciowa

Zapora sieciowa umożliwia blokowanie lub zezwalanie żądania przez adres IP lub lokalizację geograficzną. Akamai dostarcza i utrzymuje listy znanych encji, np. zakres adresów IP popularnych dostawców usług w chmurze, które mogłyby być dodane do białej listy lub adresów IP związanych z niepożądanymi źródłami ruchu, takimi jak The Onion Router (TOR) używanego przez hakerów do ukrycia tożsamości. Geo-blokowanie pozwala odrzucić żądanie z określonych krajów, regionów lub kontynentów.

Ochrona DoS

Web Application Protector zapewnia ochronę przed odmową usługi (DoS) poprzez następujące kontrole.

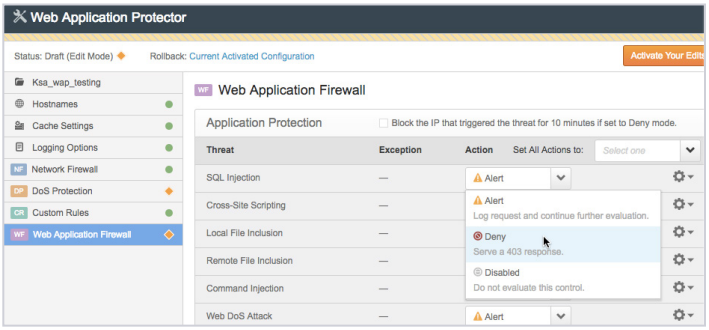
- **Zabezpieczenia warstwy 3 / warstwy 4** sprawdzają pakiety i połączenia sieciowe w celu określenia, które żądania mają być automatycznie blokowane. Ta funkcja jest zawsze włączona dla Twojej ochrony.
- **Ograniczanie natężenia** pozwala ustawić progi, aby oznaczyć żądanie ruchu, które jest zbyt szybkie aby mogło pochodzić od człowieka. Używa się trzech profili, zapewnianych przez firmę Akamai i można stworzyć dwa własne.
- **Slow POST Protection** pozwala złagodzić bardzo powolne żądania, które zużywają zasoby połączenia z serwerem.

Web Application Firewall

Zespół Akamai zajmujący się badaniami bezpieczeństwa śledzi najnowsze zagrożenia internetowe i stale aktualizuje reguły, aby nadążyć za zmieniającym się krajobrazem ryzyka. Web Application Protector zawiera łatwy w zarządzaniu zestaw reguł, który sam się aktualizuje i wdraża. WAF chroni przed sześcioma powszechnymi kategoriami ataku:

- SQL Injection (SQLi)
- Cross-Site Scripting (XSS)
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- Command Injection (CMDi)
- Denial of Service Attack (DoS)

Możesz ustawić działania według kategorii. Na przykład, jeśli przetrwałeś ataki iniekcyjne SQL w przeszłości można określić, że chcesz aby Web Application Protector odrzuciła żądania spełniające kryteria tego rodzaju ataku.



Reguły niestandardowe

Aby poradzić sobie z sytuacjami nieobjętymi przez WAF należy użyć reguł niestandardowych. Możliwe jest zdefiniowanie do 10 takich reguł, na przykład konfiguracja niestandardowej reguły w celu sprawdzenia żądania nagłówka dla określonej wartości i w sytuacji gdy zostanie on odnaleziony, odrzucić żądanie.