INFORMACJA O PRODUKCIE AKAMAI

App & API Protector

W dzisiejszym połączonym świecie zabezpieczenie aplikacji internetowych i interfejsów API przed szeroką gamą nowych i ewoluujących zagrożeń ma kluczowe znaczenie dla osiągnięcia sukcesu w biznesie. Jednak zabezpieczenie własności cyfrowej w kontekście chmury, nowoczesnych praktyk DevOps i stale zmieniających się aplikacji wprowadza nowe złożoności i wyzwania.

Wdrożenie całościowego rozwiązania do ochrony aplikacji internetowych i interfejsów API poprawia poziom bezpieczeństwa dzięki adaptacyjnemu aktualizowaniu zabezpieczeń i proaktywnemu dostarczaniu informacji na temat wykrytych luk.

Akamai App & API Protector to kompleksowe rozwiązanie, które łączy w sobie wiele technologii bezpieczeństwa, w tym standardową zaporę sieciową (WAF), łagodzenie skutków działania botów, bezpieczeństwo API i ochronę przed DDoS. App & API Protector cieszy się uznaniem jako wiodące rozwiązanie do wykrywania ataków, szybko identyfikujące i mitygujące zagrożenia, których nie można wyeliminować za pomocą standardowej zapory sieciowej, w celu ochrony całych zasobów cyfrowych przed wielowymiarowymi atakami. Platforma jest prosta we wdrożeniu i użytkowaniu, zapewnia pełny obraz sytuacji i automatycznie wdraża aktualne, dostosowane do potrzeb zabezpieczenia za pośrednictwem Akamai Adaptive Security Engine.

Potęga bezpieczeństwa adaptacyjnego

Dzięki App & API Protector zabezpieczenia są stale i automatycznie aktualizowane, a dostosowane zalecenia w zakresie polityki wdrażane jednym kliknięciem. Adaptive Security Engine, technologia stanowiąca fundament rozwiązania App & API Protector, zapewnia nowoczesną ochronę, łącząc uczenie maszynowe, analizę bezpieczeństwa w czasie rzeczywistym, zaawansowaną automatyzację oraz wiedzę pochodzącą od ponad 400 badaczy zagrożeń. Technologia Adaptive Security Engine jest wyjątkowa, ponieważ:

- Analizuje charakterystykę każdego żądania w czasie rzeczywistym na brzegu sieci w celu szybszego wykrywania.
- Uczy się wzorców ataków, wykorzystując zarówno lokalne, jak i globalne dane, aby dostosować ochronę do potrzeb klienta.
- Dostosowuje się do przyszłych zagrożeń, co zapewnia aktualne zabezpieczenia nawet w miarę rozwoju ataków.

Adaptive Security Engine uwalnia od ciężaru czasochłonnego, ręcznego dostosowywania dzięki aktualizacjom bezdotykowym, co oznacza niemal całkowite wyeliminowanie obsługi, dwukrotne zwiększenie wykrywalności i pięciokrotne zmniejszenie liczby fałszywych alarmów. Specjaliści ds. bezpieczeństwa mogą znów stać się bohaterami, mając więcej czasu na skupienie się na umożliwieniu bezpiecznej i przyjaznej klientom cyfrowej działalności biznesowej.

KORZYŚCI BIZNESOWE

Niezawodne wykrywanie ataków.
Podążaj za zmianami w przestrzeni zagrożeń, chroniąc się przed istniejącymi i pojawiającymi się zagrożeniami, takimi jak DDoS, botnety, ataki typu „injection”, ataki API i inne.

Jeden produkt, szeroki zakres ochrony.
Maksymalnie wykorzystaj inwestycję w bezpieczeństwo dzięki rozwiązaniu obejmującemu ochronę aplikacji internetowych i interfejsów API, widoczność i łagodzenie skutków działania botów, ochronę przed DDoS, konektory SIEM, optymalizację stron internetowych, przetwarzanie w chmurze, przyspieszenie interfejsów API itd.

Bezobsługowe bezpieczeństwo.
Wyeliminuj czasochłonną ręczną obsługę dzięki automatycznym aktualizacjom i proaktywnym zaleceniom dotyczącym automatycznego dostosowywania.

Łatwa obsługa.
Udoskonalony interfejs użytkownika ułatwia rozpoczęcie pracy i prowadzenie kompleksowych działań w zakresie bezpieczeństwa, w czym pomagają przewodniki dotyczące konfiguracji i rozwiązywania problemów.

Pełny obraz sytuacji.
Kompleksowe rozwiązanie Akamai dostarcza szczegółowych informacji w celu określenia wzorców ruchu i analizowania ataków za pomocą gotowych lub dostosowanych pulpitów i raportów proaktywnego wykrywania.

advatech

Akamai

Więcej niż ochrona aplikacji, zyskaj bezpieczeństwo interfejsów API

Wiodące w branży zabezpieczenia API firmy Akamai zwiększają poziom ochrony, zapewniając wgląd w ruch we wszystkich zasobach cyfrowych, proaktywnie ujawniając luki w zabezpieczeniach, identyfikując zmiany w środowisku i chroniąc przed ukrytymi atakami. Funkcja API Discovery ostrzega zespoły ds. bezpieczeństwa przed nowymi, często niezabezpieczonymi interfejsami API, podłączanymi przez różne linie biznesowe. Akamai App & API Protector automatycznie wykrywa interfejsy API co 24 godziny w oparciu o mechanizm punktacji, który uwzględnia typ zawartości odpowiedzi, charakterystykę ścieżki i wzorce ruchu. API Discovery umożliwia:

- Automatyczne wykrywanie pełnego zakresu znanych, nieznanych i zmieniających się interfejsów API w ruchu internetowym, w tym ich punktów końcowych, definicji i profili ruchu.
- Łatwe rejestrowanie nowo odkrytych interfejsów API za pomocą kilku kliknięć
- Zapewnienie ochrony interfejsów API przed atakami typu denial of service (DoS), złośliwym wstrzyknięciem, nadużyciem danych uwierzytelniających oraz naruszeniem specyfikacji API.
- Kontrolowanie przetwarzania poufnych danych za pomocą funkcji raportowania informacji umożliwiających identyfikację osób w ramach rozwiązania App & API Protector w celu zachowania zgodności z przepisami.

Ale to nie wszystko. Wszystkie żądania API są automatycznie sprawdzane pod kątem złośliwego kodu, niezależnie od tego, czy użytkownik zdecyduje się je zarejestrować, czy nie, co zapewnia wysoki poziom bezpieczeństwa interfejsu API od razu po wdrożeniu App & API Protector. App & API Protector zmniejsza złożoność operacji bezpieczeństwa na poziomie całego przedsiębiorstwa, umożliwiając zespołom ds. bezpieczeństwa lepsze współdziałanie z zespołami programistów, liderami linii biznesowych i kadrą kierowniczą.

Funkcja zapobiegania utracie danych API w App and API Protector pozwala lepiej zabezpieczyć informacje umożliwiające identyfikację osób i inne poufne dane, wykryć miejsca, w których informacje te mogą wyciekać lub być wykorzystywane przez interfejsy API, a także zyskać większą widoczność i kontrolę nad poufnymi danymi w celu zapewnienia bezpieczeństwa organizacji i klientów.

Skuteczne wykrywanie ataków

Wraz z rozwojem cyfrowego otoczenia firmy rośnie również zakres ochrony klienta Akamai. Oprócz automatycznych aktualizacji i adaptacyjnego dostosowania, które zapewnia Adaptive Security Engine, App & API Protector oferuje uznane przez analityków skuteczne wykrywanie różnych wektorów ataków, np. typu DDoS, ataków przeprowadzanych przez boty, złośliwe oprogramowanie itp.

Ochrona przed DoS/DDoS – App & API Protector, uznawany za wiodące na rynku rozwiązanie DDoS, natychmiast odpiera ataki DDoS w warstwie sieciowej ma brzegu sieci. Zapewnia to ochronę nie tylko przed atakami DDoS, ale także przed gwałtownymi wzrostami ruchu związanymi z atakiem – Akamai DDoS Fee Protection zapewnia kredytowanie wszelkich opłat za przekroczenie limitu, poniesionych w wyniku ataku DDoS.

Widoczność i łagodzenie skutków działania botów – Uzyskaj wgląd w ruch botów w czasie rzeczywistym dzięki dostępowi do obszernego katalogu Akamai zawierającego ponad 1700 znanych botów. Analizuj nieprawidłowości w analityce internetowej, zapobiegaj przeciążeniu źródeł i twórz własne definicje botów, aby umożliwić dostęp do botów stron trzecich i partnerów bez przeszkód. Zwiększ kontrolę nad bezpieczeństwem botów dzięki Akamai Bot Manager Premier, aby zabezpieczyć się przed atakami typu credential stuffing, web scraping, masowym tworzeniem kont, manipulacją zasobami i wyłudzaniem numerów kart płatniczych.

OWASP Top 10

Akamai ogranicza zagrożenia z listy OWASP Top 10 oraz OWASP API Top 10. Dowiedz się więcej o tym, jak App & API Protector i zabezpieczenia Akamai chronią klientów przed dużymi, powszechnymi lub nowymi zagrożeniami.

Pobierz opracowanie, aby dowiedzieć się więcej na temat ochrony zapewnianej przez Akamai przed OWASP Top 10.

Ochrona przed złośliwym oprogramowaniem – Dodatkowy moduł może skanować pliki przed ich przesłaniem w urządzeniach brzegowych, aby wykryć i zablokować złośliwe oprogramowanie przed przedostaniem się do systemów spółki w postaci złośliwych plików. Dzięki temu, że nie jest wymagana żadna dodatkowa aplikacja ani konfiguracja API, oszczędzasz czas, który trzeba by było poświęcić na konfigurację zabezpieczeń w każdym systemie z osobna.

Site Shield – Produkt ten, cieszący się uznaniem klientów, jest teraz dołączony do pakietu App & API Protector i zapobiega omijaniu przez atakujących zabezpieczeń opartych na chmurze i atakowaniu infrastruktury źródłowej. Inne produkty z portfolio zabezpieczeń Akamai, takie jak Page Integrity Manager, Account Protector i Audience Hijacking Protector, mogą rozszerzyć możliwości zabezpieczeń w przeglądarce.

Adaptive Security Engine, technologia stanowiąca fundament rozwiązania App & API Protector, zwiększa wykrywalność dwukrotnie i pięciokrotnie zmniejsza liczbę fałszywych alarmów.

Łatwe w obsłudze kompleksowe narzędzie bezpieczeństwa

Świetne narzędzia bezpieczeństwa działają tylko wtedy, jeśli ich używasz. Akamai koncentruje się na budowaniu całościowej i łatwej w obsłudze platformy gwarantującej efektywność i silne zabezpieczenia.

Kreator rozpoczęcia pracy – App & API Protector udostępnia łatwy w obsłudze kreator rozpoczęcia pracy z właściwościami, wyposażony w procesy integracyjne i konfiguracyjne zaprojektowane w celu usprawnienia i uproszczenia procesu rozpoczęcia pracy z właściwościami i ciągłego uczenia się.

Pulpity nawigacyjne, narzędzia do ostrzegania i raportowania – Uzyskaj dostęp do szczegółowych danych telemetrycznych dotyczących ataków, analizuj zdarzenia związane z bezpieczeństwem, twórz alerty e-mail w czasie rzeczywistym przy użyciu filtrów statycznych i progów,a także wykorzystaj narzędzia do tworzenia raportów dotyczących bezpieczeństwa sieciowego, które stale monitorują i oceniają skuteczność zabezpieczeń.

Integracje DevOps – Umożliwiają szybkie rozpoczęcie pracy, spójne zarządzanie politykami bezpieczeństwa, centralizację wdrażania w infrastrukturach chmurowych oraz usprawnienie współpracy między zespołami DevOps i bezpieczeństwa w ramach przepływu pracy GitOps, aby zabezpieczenia zawsze nadążały za dzisiejszymi szybkimi zmianami. Interfejsy API Akamai, dostępne również w formie wrappera z pakietem Akamai CLI lub Terraform, umożliwiają zarządzanie App & API Protector za pomocą kodu. Każde działanie dostępne w UI jest dostępne poprzez programowalne interfejsy API.

Integracje SIEM – Dostępne są również interfejsy API do zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem (SIEM), przy czym gotowe konektory do Splunk, QRadar, ArcSight i innych rozwiązań są automatycznie dołączane do App & API Protector.

Dołączone funkcjonalności – Aby zwiększyć widoczność i wydajność, App & API Protector oferuje teraz wiele z najbardziej docenianych przez klientów Akamai produktów, w tym:

- **mPulse Lite**
  Dogłębny wgląd w zachowanie użytkowników, rozwiązywanie problemów z wydajnością w czasie rzeczywistym i analiza wpływu zmian cyfrowych na przychody.
- **EdgeWorkers**
  Poznaj korzyści płynące z przetwarzania bezserwerowego, w tym skrócenie czasu wprowadzania na rynek i wykonywanie logiki jak najbliżej użytkowników końcowych.
- **Image & Video Manager**
  Inteligentna optymalizacja obrazów i filmów z idealną kombinacją jakości, formatu i **rozmiaru.**
- **API Acceleration**
  Zwiększ wydajność interfejsu API poprzez łatwe zarządzanie dostępem, skalowanie w przypadku nagłych wzrostów zapotrzebowania oraz poprawę bezpieczeństwa interfejsu API.

Oferty na poziomie darmowym mogą mieć ograniczenia w użytkowaniu. Aby uzyskać więcej informacji, skontaktuj się z Akamai.

Zaawansowane zarządzanie bezpieczeństwem

Opcjonalny moduł Advanced Security Management oferuje automatyzację i elastyczność konfiguracji dla tych, którzy mają bardziej złożone środowiska aplikacji i zaawansowane potrzeby w zakresie bezpieczeństwa. Wprawdzie zalecane są aktualizacje automatyczne, ale ta opcja udostępnia ręczny tryb pracy, który umożliwia granularne działania i możliwość aktywowania aktualizacji w razie potrzeby. Można również użyć Trybu oceny do testowania nowych aktualizacji równolegle z obecnymi zabezpieczeniami, aby zapoznać się z ulepszeniami w zakresie dokładności przed wdrożeniem. Opcja Advanced Security Management obejmuje również w formie gotowych rozwiązań dodatkowe konfiguracje, kontrolę szybkości, polityki, niestandardowe reguły, pozytywne zabezpieczenia API oraz dostęp do analiz zagrożeń związanych z reputacją IP (Client Reputation).

Zarządzane usługi bezpieczeństwa

Wszyscy klienci Akamai mają zapewnione standardowe wsparcie przez całą dobę, 7 dni w tygodniu, 365 dni w roku. Oprócz profesjonalnych usług doradczych na żądanie czy prac nad pojedynczymi projektami, Akamai oferuje dwa poziomy usług zarządzanych – w pełni zarządzaną ochronę aplikacji internetowych i API oraz zarządzane wsparcie w zakresie ataków.

Aby dowiedzieć się więcej, odwiedź stronę akamai.advatech.pl lub skontaktuj się bezpośrednio z:

Daniel Wysocki
Kierownik Działu Cybersecurity

+48 539 526 218,
dwysocki@advatech.pl

akamai.advatech.pl