**Barracuda uruchamia platformę Cloud Application Protection 2.0, która chroni aplikacje internetowe przed ewoluującymi wektorami ataku**

*Platforma blokuje ataki na łańcuchy dostaw, używa uczenia maszynowego w celu powstrzymywania botów, dodaje kontenerową wersję zapory WAF do ochrony aplikacji wdrażanych w kontenerach*

**Najważniejsze informacje:**

* Usługa Client-Side Protection automatyczne tworzy i wdraża zabezpieczenia przed skimmingiem oraz atakami na łańcuchy dostaw, takimi jak MageCart.
* Nowe opcje wdrożeniowe pozwalają stosować mechanizm zabezpieczający znany z Barracuda WAF i WAF-as-a-Service w kontenerach.
* Usługa Cloud Application Protection wykorzystuje uczenie maszynowe, skanowanie i usuwanie luk w zabezpieczeniach oraz zaawansowaną ochronę przed zagrożeniami, aby zapewnić inteligentną analizę zagrożeń.
* Mechanizm autokonfiguracji automatycznie dopasowuje ustawienia bezpieczeństwa do bieżących zagrożeń.

Firma Barracuda, zaufany partner i czołowy dostawca rozwiązań w zakresie bezpieczeństwa chmury, poinformowała dziś o nowych, ważnych funkcjach swojej [platformy Cloud Application Protection](https://www.barracuda.com/cap), które zapewniają dodatkowy poziom ochrony i ułatwiają organizacjom zabezpieczanie aplikacji w świecie po transformacji cyfrowej. Zaprezentowane usługi i rozwiązania obejmują ochronę po stronie klienta, możliwość wdrażania kontenerowych węzłów WAF oraz mechanizm autokonfiguracji. Ponadto platforma Cloud Application Protection wykorzystuje uczenie maszynowe, skanowanie i usuwanie luk w zabezpieczeniach oraz zaawansowaną ochronę przed zagrożeniami, aby zapewnić inteligentną analizę zagrożeń, a przez to skuteczniejszą ochronę.

Cloud Application Protection to platforma firmy Barracuda do ochrony aplikacji internetowych i interfejsów API (Web Application and API Protection, WAAP). Według firmy Gartner „do 2023 r. ponad 30 proc. dostępnych publicznie aplikacji i interfejsów API będzie chronionych przez usługi WAAP, które łączą ochronę przed rozproszonymi atakami blokady usług (DDoS), ograniczanie aktywności botów, ochronę API oraz zapory aplikacji internetowych (WAF). Oznacza to wzrost w porównaniu z niespełna 15 proc. obecnie”.1

„W firmie Barracuda nieustannie pracujemy nad upraszczaniem rozwiązań zapewniających bezpieczeństwo, a Cloud Application Protection 2.0 zapewnia klientom ochronę aplikacji klasy korporacyjnej w połączeniu z łatwością użycia – **powiedział** **Tim Jefferson, SVP, Engineering for Data, Networks and Application Security w firmie Barracuda**. – Nowe zaawansowane funkcje rozwiązują problemy z bezpieczeństwem aplikacji, które obecnie budzą największe obawy organizacji, a także zapewniają ochronę przed nadchodzącymi zagrożeniami”.

Firma Barracuda [niedawno przeprowadziła sondaż wśród setek osób odpowiedzialnych za systemy IT](https://www.barracuda.com/appsec-report-2021) w organizacjach na całym świecie, a pięcioma najczęściej wskazywanymi problemami związanymi z bezpieczeństwem aplikacji były boty, ataki na łańcuchy dostaw, wykrywanie luk w zabezpieczeniach, bezpieczeństwo interfejsów API oraz wolniejsze tworzenie aplikacji wskutek konieczności dodawania zabezpieczeń.

Najważniejsze funkcje platformy Cloud Application Protection 2.0 to:

* **Client-Side Protection.** Ta nowa usługa automatycznie tworzy i wdraża zabezpieczenia przed skimmingiem oraz atakami na łańcuchy dostaw, takimi jak MageCart. Ataki tego typu przeprowadza się poprzez infekowanie witryny skryptem, który jest wczytywany bezpośrednio przez przeglądarkę, co oznacza, że zapory WAF nie są w stanie go wykryć. Cloud Application Protection 2.0 dodaje zarówno ochronę przed takimi atakami, jak i ich raportowanie.
* **Kontenerowe wdrożenia WAF.** Ta nowa opcja wdrożeniowa oferuje ten sam mechanizm bezpieczeństwa, który jest używany w rozwiązaniach Barracuda WAF oraz WAF-as-a-Service, ale w formie kontenerowej Coraz więcej aplikacji jest wdrażanych w kontenerach, a teraz również ich bezpieczeństwo może być oferowane w analogicznym modelu
* **Mechanizm autokonfiguracji.** Mechanizm autokonfiguracji wykorzystuje modele uczenia maszynowego do badania wzorców ruchu organizacji i rekomendowania skuteczniejszych ustawień bezpieczeństwa, zmniejszając nakład pracy administracyjnej.
* **Active Threat Intelligence.** Ta chmurowa usługa oparta na uczeniu maszynowym zapewnia analizę zagrożeń w czasie zbliżonym do rzeczywistego, aby na bieżąco wykrywać i powstrzymywać nowe zagrożenia. Barracuda Active Threat Intelligence łączy rozwiązania Barracuda Vulnerability Manager, Barracuda Vulnerability Remediation Service, Barracuda Advanced Threat Protection oraz chmurową warstwę Barracuda Advanced Bot Protection w jedną usługę, która zapewnia wszystkie funkcje od wykrywania do eliminowania zagrożeń.

Oprócz nowych funkcji w Cloud Application Protection 2.0 dodano integrację z usługą Azure Sentinel, która pozwala szybko obejrzeć najważniejsze informacje w konkretnym kontekście, co umożliwia szybką reakcję. Klienci mogą również utworzyć reguły

Azure Sentinel w celu przeprowadzania zadań konfiguracyjnych z wykorzystaniem WAF API, aby domknąć pętlę sprzężenia zwrotnego na wypadek wykrycia nowego ataku.

Szablon konfigurujący przestrzeń roboczą Azure Sentinel z konsolą zarządzającą dla Barracuda WAF lub WAF-as-a-Service jest obecnie dostępny w portalu Azure, więc administratorzy mogą bezproblemowo przeprowadzić tę integrację.

**Wypowiedź klienta**

„Barracuda Cloud Application Protection łączy funkcje i wydajność, której potrzebujemy, z łatwością użycia, na której nam zależy – **powiedział Zach Peer, dyrektor ds. technologii i hostingu zarządzanego w One North.** – Jako wieloletni klienci jesteśmy pewni, że rozwiązanie to zapewnia najlepszą możliwą ochronę przed wszystkimi najnowszymi zagrożeniami.”

## Zasoby:

Więcej informacji o platformie Barracuda Cloud Application Protection 2.0: <https://www.barracuda.com/cap>

Więcej informacji o Barracuda WAF-as-a-Service: <https://www.barracuda.com/waf-as-a-service>

Przeczytaj raport: The state of application security in 2021: <https://www.barracuda.com/appsec-report-2021>

1 Gartner, „Magic Quadrant for Web Application Firewalls”, Jeremy D'Hoinne, Adam Hils, Rajpreet Kaur, John Watts, 19 października 2020 r.

**O firmie Barracuda**

W firmie Barracuda staramy się uczynić świat bezpieczniejszym. Uważamy, że każde przedsiębiorstwo zasługuje na dostęp do najwyższej klasy rozwiązań bezpieczeństwa, przystosowanych do współpracy z chmurą, które można łatwo zakupić, wdrożyć i eksploatować. Chronimy pocztę elektroniczną, sieci, dane i aplikacje korzystając z innowacyjnych rozwiązań, które rozwijają się i dostosowują do bieżących potrzeb naszych klientów. W kwestii bezpieczeństwa firmie Barracuda zaufało już ponad 150 000 organizacji z całego świata. Dzięki wysokiej skuteczności naszych rozwiązań mogą one nawet nie być świadome zagrożeń, co pozwala im w pełni skoncentrować się na rozwoju swojej działalności. Więcej informacji można uzyskać na stronie barracuda.com.

Barracuda Networks, Barracuda i logo Barracuda Networks są znakami handlowymi należącymi do firmy Barracuda Networks, Inc., które mogą być zarejestrowane w Stanach Zjednoczonych i w innych państwach.