**Check Point upraszcza bezpieczeństwo aplikacji w chmurze dzięki opartemu na sztucznej inteligencji WAFaaS**

**Check Point Software wprowadził CloudGuard WAF-as-a-Service (WAFaaS), czyli oparty na sztucznej inteligencji, zautomatyzowany web application firewall. Rozwiązanie umożliwia kompleksowe zapobieganie zagrożeniom cybernetycznym, chroniąc aplikacje internetowe przed nieautoryzowanym dostępem i naruszeniami danych. To jednocześnie skuteczne zabezpieczanie aplikacji i interfejsów API w chmurze.**

Specjaliści ds. bezpieczeństwa uważają, że rozwiązania WAF wymagają stałej aktualizacji i elastyczności. [Raport](https://www.checkpoint.com/press-releases/rising-cloud-threats-demand-advanced-defenses-check-points-2024-report-highlights-urgent-need-for-ai-and-prevention-first-security-measures/) Check Point dotyczący bezpieczeństwa w chmurze za rok 2024 ujawnił, że przeważająca liczba 96% respondentów zgłosiła obawy dotyczące swojej zdolności do skutecznego zarządzania ryzykiem w chmurze. W pełni zarządzana usługa Check Point CloudGuard WAFaaS eliminuje trudności, związane z utrzymaniem rozwiązań WAF.

- *Nowoczesne operacje w chmurze wymagają prostej i skutecznej ochrony usług sieciowych i interfejsów API, którą CloudGuard WAFaaS zapewnia poprzez niezbędne, zautomatyzowane zabezpieczenia dostarczane przez chmurę* – powiedział Oded Gonda, wiceprezes ds. technologii i innowacji w firmie Check Point Software Technologies. - *CloudGuard WAFaaS upraszcza zabezpieczenia aplikacji dla naszych klientów, oferując najwyższej klasy ochronę przed zagrożeniami w zarządzanym rozwiązaniu, które można wdrożyć w mniej niż pięć minut i skutecznie zapobiega zagrożeniom typu zero-day.*

CloudGuard WAFaaS jest kluczowym elementem rozwiązania zabezpieczającego chmurę od Check Point. Z funkcjami takimi jak wykrywanie zagrożeń oparte na AI, zapobieganie botom wykrywającym API, bezpieczeństwo plików i ograniczanie szybkości, CloudGuard WAFaaS oferuje kompleksowy zestaw ochrony aplikacji i API dla wielu chmur i nowoczesnej architektury oraz obejmuje zapobieganie atakom DDoS i zautomatyzowane zarządzanie certyfikatami.

W ramach [platformy Check Point Infinity](https://www.checkpoint.com/infinity/) do ochrony chmury kluczowe funkcje CloudGuard WAFaaS obejmują:

l **Zapobieganie zagrożeniom:** chroni przed exploitami dnia zerowego, atakami typu Distributed Denial of Service (DDoS) i atakami przeprowadzanymi przez boty, zapewniając kompleksowe bezpieczeństwo bez wpływu na wydajność

l **Analiza kontekstowa:** Precyzyjne wykrywanie, praktycznie bez fałszywych alarmów, uwalnia zespoły ds. bezpieczeństwa od żmudnej konserwacji zapory ogniowej

l **Bezpieczeństwo API:** Skutecznie zmniejsza ryzyko nieautoryzowanego dostępu i naruszeń danych, wykorzystując najnowszą funkcję API Discovery

l **Jednorazowa konfiguracja:** kompleksowy proces wdrożenia można wykonać w ciągu 5 minut

- *W przeciwieństwie do tradycyjnych zapór sieciowych dla aplikacji internetowych, które w dużym stopniu opierają się na ręcznej interwencji i częstych aktualizacjach sygnatur, nasz nowo wydany Check Point CloudGuard WAFaaS wykorzystuje sztuczną inteligencję do dynamicznego dostosowywania się do nowych zagrożeń* – powiedział Brian McHenry, dyrektor ds. inżynierii bezpieczeństwa chmury w Check Point Software. - *Ta funkcja zapewnia organizacjom prewencyjny mechanizm obronny, który ewoluuje wraz z krajobrazem zagrożeń, bez generowania czasochłonnych fałszywych alarmów.*