**Sztuczna inteligencja i kryptografia post-kwantowa w nowym rozwiązaniu Check Pointa. To odpowiedź na 75% wzrost ataków.**

**Organizacje mierzą się z aż 75% wzrostem cyberataków na całym świecie, nic więc dziwnego, że firmy technologiczne szukają sposobów na bardziej skuteczną walkę z cyberprzestępcami. Odpowiedzią na współczesne wyzwania cybernetyczne ma być m.in. oparte na sztucznej inteligencji nowe oprogramowanie Check Point Quantum Firewall R82. Oferuje ono nowe silniki AI, szyfrowanie post-kwantowe, przyspieszone DevOps i większą prostotę obsługi centrów danych.**

Zaprezentowane przez Check Pointa rozwiązania pomagają zapobiegać zagrożeniom typu zero-day, w tym phishingowi, złośliwemu oprogramowaniu i atakom na systemy nazw domen (DNS). To również zmiany architektoniczne i innowacje, które zwiększają zwinność DevOps w obszarze operacji centrów danych, przy jednoczesnej prostocie obsługi i możliwej skalowalności.

*- Zagrożenia nadal mnożą się wykładniczo, a organizacje potrzebują inteligentnych rozwiązań, które pozwolą im być o krok przed nimi. Nasz zestaw narzędzi prewencyjnych opartych na sztucznej inteligencji nie tylko wprowadza innowacje światowej klasy, ale także koncentruje się na prostocie i rezyliencji systemów* — powiedziała Nataly Kremer, dyrektor ds. produktów w Check Point Software Technologies.

Quantum Software R82 oferuje klientom korporacyjnym [ponad 50 nowych możliwości, w tym:](https://blog.checkpoint.com/security/the-best-security-simplicity-and-scale-just-got-better/)

l **Wiodąca w branży oparta na sztucznej inteligencji funkcja zapobiegania zagrożeniom**, która [blokuje 99,8%](https://www.checkpoint.com/press-releases/check-point-software-technologies-triumphs-in-miercoms-2024-next-generation-firewall-benchmark-report/) zagrożeń typu zero-day. Wprowadza cztery nowe silniki AI, aby znaleźć ukryte relacje oraz wzorce i zablokować ponad 500 tys. dodatkowych ataków miesięcznie, chroniąc przed wyrafinowanymi kampaniami phishingowymi i złośliwym oprogramowaniem typu zero-day.

l **Zwinne operacje centrum danych** przyspieszające rozwój aplikacji dzięki automatycznej integracjipolityki bezpieczeństwa. Dzięki radykalnie uproszczonej wirtualizacji zapory sieciowej, organizacje osiągają 3-krotnie szybsze dostarczanie systemów wirtualnych dla wielodostępności oprogramowania i sprawnego rozwoju aplikacji, co przynosi korzyści DevOps.

l **Prostota operacyjna,** która zapewnia bezproblemową skalowalność dla sieci każdej wielkości, automatycznie dostosowując się do wzrostu biznesu i skoków ruchu. Organizacje mogą osiągnąć odporność dzięki wbudowanemu współdzieleniu obciążenia i klastrowaniu (ElasticXL), jednocześnie korzystając z trzykrotnie szybszego zapewnienia środków realizacji (provisioning) i zarządzania zaporą sieciową.

l **Kryptografia postkwantowa (PQC)** ma zapewnić najnowszą, zatwierdzoną przez NIST, kryptografię Kyber (ML-KEM) do bezpiecznego szyfrowania kwantowego, gwarantując, że dzisiejsze zaszyfrowane dane nie staną się jutro skarbem dla cyberprzestępców.

Nowe możliwości opierają się na niedawno wydanym przez firmę Check Point pakiecie innowacji w zakresie zapobiegania zagrożeniom, opartych na sztucznej inteligencji:

l **Check Point** [Infinity AI Copilot](https://www.checkpoint.com/ai/copilot/) - responsywny asystent oparty na sztucznej inteligencji, którego celem jest automatyzacja i przyspieszenie zarządzania bezpieczeństwem oraz rozwiązywania zagrożeń.

l **Check Point** [GenAI Protect](https://www.checkpoint.com/solutions/genai-security/) - pionierskie rozwiązanie umożliwiające bezpieczne wdrożenie generatywnej sztucznej inteligencji w przedsiębiorstwach.

l **Check Point Infinity** [External Risk Management](https://www.checkpoint.com/infinity/soc/external-risk-management/) **(ERM)** - zapewniający ciągły monitoring i zapobieganie zagrożeniom w czasie rzeczywistym, uzupełnione o usługi zarządzane przez ekspertów. Chroni to klientów przed szerszym wachlarzem zewnętrznych zagrożeń, od zagrożeń dla poświadczeń i wykorzystywania luk w zabezpieczeniach po ataki phishingowe i oszustwa.

*- Zauważyliśmy wyraźny wzrost wydajności i wartości operacyjnej dzięki za sprawą aktualizacji do wersji Quantum Firewall Software R82. Nowe oprogramowanie Quantum Firewall pozwala nam zabezpieczać i zarządzać naszym szyfrowanym ruchem łatwiej niż kiedykolwiek wcześniej* — powiedział Jeff Burgess, Manager IT Enterprise, Aviation Technical Services.

Firma Check Point został niedawno uznana za lidera w raportach [The Forrester Wave™: Enterprise Firewalls, Q4 2024](https://www.checkpoint.com/press-releases/check-point-software-named-a-leader-in-enterprise-firewall-solutions-evaluation-according-to-independent-research-firm/) oraz The Forrester Wave™: Zero Trust Platform Providers, Q3 [2023.](https://www.checkpoint.com/press-releases/check-point-software-technologies-named-a-leader-in-latest-zero-trust-platform-providers-report-by-independent-research-firm/)