**Korzystanie z GenAI może być bezpieczne dzięki nowej usłudze Check Point Software**

**Aplikacje generujące sztuczną inteligencję, takie jak ChatGPT i Gemini ugruntowały swoją pozycję na rynku. Niestety, jak to czasem bywa, znacznie ułatwiając życie użytkownikom, utrudniają życie firmom, w szczególności w obszarze bezpieczeństwa. Chociaż niektóre organizacje całkowicie zakazały aplikacji GenAI, według badania Check Point i Vason Bourne 92% organizacji pozwala swoim pracownikom na korzystanie z narzędzi GenAI, ale obawia się bezpieczeństwa i wycieku danych.**

Szacuje się, że aż [55](https://www.forbes.com/sites/davidbalaban/2024/04/04/gen-ai-and-its-malicious-impact-on-the-cyber-physical-threat-landscape/)% przypadków wycieku danych jest bezpośrednim skutkiem użycia GenAI. Konwencjonalne rozwiązania w zakresie ochrony danych nie są przeznaczone do wykrywania i zapobiegania wyciekom danych w aplikacjach generatywnej sztucznej inteligencji, ponieważ opierają się na statycznych, predefiniowanych słowach kluczowych i wzorcach. Nie rozumieją kontekstu nieustrukturyzowanych danych, typowego dla podpowiedzi GenAI, które z natury mają charakter konwersacyjny.Okazuje się, że aby zaradzić [zagrożeniom związanym z GenAI](https://blog.checkpoint.com/artificial-intelligence/top-genai-threats-and-why-zero-trust-ai-access-is-the-future/) , potrzebne jest rozwiązanie oparte na GenAI.

[**https://www.youtube.com/watch?v=A244uSbP4zQ&t=4s**](https://www.youtube.com/watch?v=A244uSbP4zQ&amp;amp;t=4s)

**Check Point pozwala bezpiecznie zastosować generatywną sztuczną inteligencję**

Rozwiązanie zabezpieczające GenAI firmy Check Point instaluje się w ciągu kilku minut, aby wykryć usługi GenAI używane w organizacji, ocenić związane z nimi ryzyko i zastosować przełomową ochronę danych opartą na sztucznej inteligencji, dzięki czemu możesz korzystać z najnowszych usług bez dodatkowego ryzyka.

**Rozwiązanie wykorzystuje transformacyjną analizę danych opartą na sztucznej inteligencji, aby dokładnie klasyfikować dane konwersacyjne w ramach podpowiedzi. Przełomowa technologia klasyfikacji, opracowana przez Check Pointa, rozumie kontekst danych, aby zapewnić precyzyjną widoczność i kontrolę, jednocześnie unikając konieczności definiowania uciążliwych typów danych.**

Korzystając z technologii DLP opartej na GenAI, rozwiązanie może rozróżnić treści niskiego ryzyka, takie jak zakup nowego domu, od treści wysokiego ryzyka, takich jak potencjalne przejęcie firmy.

- *Generatywna sztuczna inteligencja zwiększa produktywność przedsiębiorstw, zapewniając pomoc sztucznej inteligencji w marketingu, analizie danych, a nawet opracowywaniu kodu. Niestety, pracownicy narażają przedsiębiorstwa na ryzyko cybernetyczne poprzez utratę danych i kradzież własności intelektualnej, włączając poufne informacje do aplikacji GenAI. CISO szukają sposobów bezpiecznego zarządzania wykorzystaniem aplikacji GenAI w całym przedsiębiorstwi*e – powiedział Frank Dickson, wiceprezes grupy ds. bezpieczeństwa i zaufania [w IDC](https://www.idc.com/). - *Dzięki sztucznej inteligencji i automatyzacji nowy GenAI Protect firmy Check Point umożliwia przedsiębiorstwom bezpieczne wdrażanie generatywnych narzędzi AI poprzez wykrywanie, w jaki sposób aplikacje GenAI są wykorzystywane, analizowanie udostępnianych danych, stosowanie polityki bezpieczeństwa zapobiegającej utracie danych w czasie rzeczywistym oraz zapewnianie widoczności i raportowanie pod kątem zgodności.”*

**#1 Odkryj i oceń użycie GenAI w przedsiębiorstwie**

[Rozwiązanie zabezpieczające GenAI firmy Check Point](https://www.checkpoint.com/solutions/genai-security/) umożliwia wykrywanie zarówno zatwierdzonych, jak i ukrytych aplikacji GenAI oraz zapewnia wgląd w najważniejsze przypadki użycia GenAI, takie jak kodowanie i marketing, dzięki czemu możesz podejmować świadome decyzje dotyczące zarządzania GenAI. Zabezpieczenie odkrywa także źródła danych skopiowanych/wklejonych do podpowiedzi i zapewnia ocenę ryzyka w celu ustalenia priorytetów działań łagodzących.

**#2 Zapobiegaj utracie danych w czasie rzeczywistym i rozwiązuj problemy związane z prywatnością**

Rozwiązanie pozwala egzekwować konfigurowalne zasady zapobiegające wyciekom danych i stosować zapobieganie utracie danych oparte na sztucznej inteligencji, aby zatrzymać udostępnianie wrażliwych danych nieustrukturyzowanych. Umożliwia nawet egzekwowanie ograniczeń kopiowania/wklejania, aby zapobiec pobieraniu repozytoriów kodu źródłowego, narzędzi CRM, firmowej poczty e-mail i innych wrażliwych aplikacji.

**#3 Spełniaj zasady dzięki widoczności na poziomie korporacyjnym**

Nowe rozwiązanie bezpieczeństwa GenAI firmy Check Point zapewnia szczegółowe monitorowanie i widoczność, co ułatwia realizowanie przepisów współczesnego i przyszłego prawa. Zapewnia wgląd w ryzykowne monity użytkownika i aplikacje AI wysokiego ryzyka (w oparciu o analizę zagrożeń charakterystyczną dla aplikacji), a nawet określa, dlaczego monit jest oznaczony jako niebezpieczny.

**Czym różni się rozwiązanie firmy Check Point?**

W odróżnieniu od innych rozwiązań Check Point umożliwia:

l Start w kilka minut, wymagający jedynie prostego rozszerzenia przeglądarki, aby odkryć aplikacje GenAI i rozpocząć tworzenie polityk.

l Odkrycie najważniejszych przypadków użycia GenAI (np. kodowanie, marketing i poczta elektroniczna) aby móc podejmować świadome decyzje dotyczące zarządzania GenAI

l Wykorzystywanie klasyfikacji danych opartej na GenAI, aby dokładnie identyfikować i blokować wrażliwe dane w monitach AI

Dzięki swojej najnowszej ofercie Check Point po raz kolejny zwiększa bezpieczeństwo przedsiębiorstwa, wykorzystując moc sztucznej inteligencji, dodając [AI Copilot](https://www.checkpoint.com/ai/copilot/), który służy jako osobisty asystent bezpieczeństwa GenAI, [AI Cloud Protect](https://www.checkpoint.com/ai/cloudprotect/) do ochrony rozwoju sztucznej inteligencji w chmurze oraz [ThreatCloud AI](https://www.checkpoint.com/ai/threatcloud/) do zerowego dzienne zapobieganie zagrożeniom.