**Check Point Horizon XDR/XPR integruje się z Microsoft Defender for Endpoint**

**Usługa Microsoft Defender for Endpoint integruje się z rozwiązaniem rozszerzonego wykrywania i reagowania (XDR) firmy Check Point – Horizon XDR/XPR. Integracja jednym kliknięciem łączy rozwiązanie dla punktu końcowego, a dane telemetryczne są dodawane do silnika korelacji danych, opartego na sztucznej inteligencji XDR/XPR. Rozwiązanie Check Pointa łączy z kolei dane z Defender for Endpoint oraz innymi produktami Check Point oraz firm trzecich, dokonując ich korelacji, aby odkryć ataki, które wcześniej pozostawały niezauważone.**

**Szybsze zapobieganie atakom dzięki XDR/XPR i Defenderowi**

Możliwość automatycznego przeprowadzania analizy AI danych z usługi Microsoft Defender for Endpoint oraz wielu różnych produktów zabezpieczających Check Point i innych firmumożliwia inteligentną korelację, która może wykryć ataki, które obecnie pozostają niewykryte.

Najbardziej niebezpieczni i wyrafinowani napastnicy dużo inwestują w sposoby unikania wykrycia. Wykorzystują fakt, że większość organizacji wdraża swoje rozwiązania bezpieczeństwa w odłączonych silosach. Każde rozwiązanie odpowiada za ochronę określonego wektora (e-mail, ruch sieciowy, punkt końcowy itp.), ale zazwyczaj nie ma między nimi połączenia. Podczas ataku wiele rozwiązań może wykryć drobną aktywność, która sama w sobie nie wymaga ostrzeżenia, ale gdy [Horizon XDR/XPR](https://www.checkpoint.com/horizon/xdr-xpr/) analizuje dane z wielu rozwiązań, jest w stanie znaleźć korelacje i wykryć trwający atak.

**Jak to działa?**

Check Point Horizon XDR/XPR konsoliduje zdarzenia i alerty z całego obszaru zabezpieczeń, aby zapewnić inteligentne powiązania, odkrywać ukryte zagrożenia i podejmować automatyczne działania zapobiegawcze w przypadku ataku. Dzięki Horizon XDR/XPR Twoja firma może cieszyć się:

l **Kompleksową ochroną przed zagrożeniami**

W całym obszarze bezpieczeństwa, wykorzystując integrację z rozwiązaniami Check Point i rozwiązaniami bezpieczeństwa innych firm.

l **Inteligentną korelacją zagrożeń i zdarzeń**

Zapobieganie opiera się na [sztucznej](https://www.checkpoint.com/cyber-hub/cyber-security/what-is-ai-cyber-security/) inteligencji i analizie zagrożeń, łącząc rozwiązanie Check Point i dane stron trzecich.

l **Skonsolidowanymi analizami**

Wgląd w zachowanie, kontekst i obrażenia związane z atakiem. Zrozum, gdzie znajduje się atak w łańcuchu zniszczeń.

Rozwiązanie Check Point Horizon XDR/XPR zostało uznane za lidera w raporcie Frost Radar™ XDR za rok 2023. [Pobierz raport tutaj](https://resources.checkpoint.com/cyber-security-resources/2023-frost-radar-extended-detection-and-response-report) .