**IoT Protect od Check Pointa odpowiedzią na bezpieczeństwo Internetu Rzeczy**

**Firma Check Point wprowadziła na rynek rozwiązanie Internet of Things Protect, do zabezpieczania sieci IoT, inteligentnych budynków, służby zdrowia czy środowisk infrastruktury krytycznej przed zagrożeniami VI generacji. Rozwiązanie zapewnia funkcje zapobiegania zagrożeniom i zarządzania bezpieczeństwem, aby blokować nawet nieznane ataki cybernetyczne zarówno na poziomie sieci IoT, jak i urządzeń IoT, wykorzystując analizę zagrożeń i innowacyjne usługi bezpieczeństwa specyficzne dla IoT.**

Większość organizacji z sektorów komercyjnego, przemysłowego, opieki zdrowotnej i użyteczności publicznej wdrożyła rozwiązania IoT i technologie operacyjne (OT), co znacznie zwiększyło ich ryzyko cybernetyczne – wiele urządzeń IoT ma luki w zabezpieczeniach, których nie można załatać. Ponadto organizacje dysponują różnymi zasobami urządzeń od różnych dostawców, z wieloma urządzeniami-cieniem, które są niezarządzane i podłączone do sieci bez autoryzacji, więc organizacje mają ograniczoną widoczność i kontrolę nad nimi, co potęguje ryzyko. Wyniki ankiety przeprowadzonej przez Check Point potwierdzają te problemy: 90% respondentów zgłosiło, że ich organizacje mają w swoich sieciach ukryte urządzenia IoT, a 44% stwierdziło, że co najmniej połowa ich urządzeń IoT była połączona bez wiedzy zespołów IT lub bezpieczeństwa. Tylko 11% respondentów stwierdziło, że w pełni wdrożyło rozwiązanie zabezpieczające IoT, a 52% nie ma w ogóle wdrożonych zabezpieczeń IoT.

W rezultacie [67% przedsiębiorstw](https://www.armis.com/resources/analyst-reports/forrester-state-of-enterprise-iot-security-in-north-america-unmanaged-and-unsecured-tlp/) i [82% firm opieki](https://www.hipaajournal.com/82-of-healthcare-organizations-have-experienced-a-cyberattack-on-their-iot-devices/) zdrowotnej doświadczyło incydentów związanych z IoT. Rosnące ataki na urządzenia i sieci IoT, w połączeniu z szybkim przejściem do pracy zdalnej wymuszonej przez pandemię Covid-19, wymagają najbardziej zaawansowanej, wszechstronnej struktury bezpieczeństwa, która może zidentyfikować wrażliwe urządzenia IoT, zastosować ochronę i powstrzymać inteligentne cyberzagrożenia.

IoT Protect firmy Check Point zapewnia bezpieczeństwo na poziomie sieci oraz zarządzanie politykami bezpieczeństwa wraz z bramami Check Pointa i nano-agentami IoT Protect, które zapewniają ochronę w czasie rzeczywistym, na podłączonym urządzeniu. IoT Protect integruje się z wiodącymi w branży platformami wykrywania zasobów IoT w sektorach opieki zdrowotnej, przemysłowej, inteligentnych biur i inteligentnych budynków, aby zabezpieczyć setki tysięcy urządzeń IoT. Rozwiązanie zapewnia:

l  **Pełną widoczność urządzeń IoT, wraz z analizą ryzyka:** identyfikuje i klasyfikuje urządzenia IoT w dowolnej sieci poprzez integrację z wiodącymi silnikami wykrywania w celu ujawnienia zagrożeń, takich jak słabe hasła, przestarzałe oprogramowanie układowe i znane luki w zabezpieczeniach.

l  **Zmniejszanie luk w zabezpieczeniach i zapobieganie zagrożeniom typu zero-day nawet na urządzeniach, których nie można zaktualizować:** urządzenia IoT można „wirtualnie załatać”, aby naprawić luki w zabezpieczeniach, nawet te z nieaktualnym oprogramowaniem układowym lub starszymi systemami operacyjnymi. IoT Protect obejmuje 60 usług bezpieczeństwa specyficznych dla IoT, które identyfikują i zatrzymują nieautoryzowany dostęp i ruch do i z urządzeń i serwerów oraz zapobiegają atakom złośliwego oprogramowania ukierunkowanym na IoT. Unikalny Nano-Agent IoT Defense może być również osadzony na urządzeniach, aby zapewnić wbudowaną ochronę przed zagrożeniami zero-day.

l  **Intuicyjna segmentacja i zarządzanie siecią Zero Trust:** rozwiązanie stosuje i egzekwuje szczegółowe reguły bezpieczeństwa w całej strukturze sieci IoT w oparciu o atrybuty urządzeń, zagrożenia i protokoły oraz obsługuje całościowe zarządzanie polityką bezpieczeństwa w jednym okienku zarówno dla sieci IT, jak i IoT .

IoT Protect oferuje największy w branży ekosystem wykrywania IoT, który zabezpiecza setki tysięcy urządzeń IoT. Check Point utrzymuje otwartą strukturę partnerów technologicznych – takich jak Armis, MediGate, Claroty i Ordr - specjalizujących się w wykrywaniu i klasyfikowaniu urządzeń IoT w różnych branżach. Z częścią z nich podpisano umowy, które pozwalają klientom Check Point uzyskać prawdziwie kompleksowe rozwiązanie.

IoT Protect obsługuje ponad 1600 protokołów IoT i technologii operacyjnych (OT), aplikacji i poleceń bezpośrednio po wyjęciu z pudełka, zapewniając jednocześnie najlepsze praktyki zgodności z przepisami, w tym HIPAA, NERC CIP, RODO i wielu innych. Rozwiązanie jest wspierane przez Check Point ThreatCloud, największą na świecie i najpotężniejszą bazę danych o zagrożeniach.