**Potrójne zabezpieczenie z Check Point SASE: Nowa ochrona cyfrowej granicy**

**Bezpieczeństwo współczesnych sieci korporacyjnych stało się bardziej złożone niż kiedykolwiek. Dane firmowe migrują do chmury, aplikacje typu SaaS stały się standardem, a pracownicy coraz częściej pracują zdalnie. Ochrona tych dynamicznych środowisk wymaga nowego podejścia, które wykracza poza tradycyjne metody i mierzy się z realiami nowej granicy firmowej. Oto Secure Access Service Edge (SASE).**

Tradycyjne modele bezpieczeństwa sieci koncentrowały się na zabezpieczeniu biur i zasobów lokalnych. Jednak z uwagi na przejście na pracę zdalną i aplikacje oparte na chmurze, te modele wymagają modyfikacji. SASE oferuje rozwiązanie, skupiając się na zabezpieczaniu użytkowników i ich dostępu do aplikacji na zasadzie potrzeby. Dzięki temu możliwe jest stosowanie bardziej szczegółowych kontroli bezpieczeństwa, co ułatwia ochronę zasobów firmowych w zdecentralizowanym środowisku.

Rozwiązania SASE są zaprojektowane tak, aby monitorować ruch użytkowników i stosować podejście "zero trust" (brak zaufania) do każdego żądania dostępu. Każda próba dostępu jest dokładnie sprawdzana, a dostęp przyznawany jest tylko na podstawie uzasadnionych próśb. Istnieje jednak jeden obszar, w którym SASE ma braki: widoczność w przeglądarce, która jest głównym narzędziem interakcji pracowników z zasobami firmy.

**Znaczenie bezpieczeństwa przeglądarki**

Przeglądarka jest centralnym elementem współczesnej pracy, umożliwiając dostęp do aplikacji krytycznych dla biznesu, współpracę w czasie rzeczywistym oraz zarządzanie przepływami pracy. Niezależnie od tego, czy jest to Google Docs, Salesforce, czy Office 365, przeglądarka jest bramą do cyfrowych zasobów firmy.

Jednak ta wygoda wiąże się z istotnymi wyzwaniami w zakresie bezpieczeństwa. Przeglądarki zostały zaprojektowane tak, aby wykonywać kod z różnych źródeł, co czyni je priorytetowym celem dla cyberataków. Złośliwi aktorzy mogą wykorzystywać luki w przeglądarkach, aby uzyskać dostęp do sieci firmowych, często poprzez pozornie nieszkodliwe działania, takie jak pobieranie pliku lub kliknięcie w reklamę stron trzecich.

Z tego względu kluczowe jest, aby rozwiązania SASE zawierały wbudowane mechanizmy zabezpieczające przeglądarki. Bez nich, nawet najbardziej zaawansowane systemy obrony sieciowej mogą zostać ominięte przez dobrze zaplanowane ataki skierowane na przeglądarki.

**Wprowadzenie Check Point SASE: Potrójna warstwa ochrony**

Check Point SASE rozwiązuje ten krytyczny problem, oferując kompleksowe podejście zabezpieczające w trzech warstwach: agent stacjonarny, chmura oraz przeglądarka. To hybrydowe podejście zapewnia ochronę sieci przed nowymi zagrożeniami w każdym możliwym punkcie styku – niezależnie od tego, czy Twój zespół korzysta z zasobów firmy, przegląda internet, czy pracuje w aplikacjach chmurowych.

1.  **Agent dla urządzenia:** Pierwsza linia obrony na urządzeniu użytkownika. Check Point. Agent jest wyposażony w zaawansowane funkcje zapobiegania zagrożeniom, w tym ochronę przed ransomware, keyloggerami i zagrożeniami zero-day.

2.  **Bezpieczeństwo chmury:** Druga warstwa ochrony zapewniana jest przez globalną sieć Check Point z ponad 70 punktami obecności (PoP). Te punkty oferują bezpieczne, szybkie połączenia z aplikacjami w chmurze i zasobami lokalnymi, blokując dostęp dla złośliwych aktorów.

3.  **Bezpieczeństwo przeglądarki:** Trzecia i ostatnia warstwa skupia się na samej przeglądarce. Rozwiązanie Check Point SASE w zakresie zabezpieczeń przeglądarki oferuje funkcje takie jak kontrola schowka, bezpieczne wyszukiwanie, ochrona haseł firmowych, wykrywanie zagrożeń, sanityzacja plików, ochrona przed phishingiem i wiele innych.

Podejście Check Point do SASE zapewnia kilka kluczowych korzyści:

l **Elastyczne bezpieczeństwo**: Potrójna warstwa ochrony gwarantuje kompleksowe zabezpieczenie na poziomie stacjonarnym, w chmurze i w przeglądarce.

l **Szybsze połączenia**: Bezpieczny dostęp do internetu jest dwukrotnie szybszy niż w przypadku tradycyjnych metod, co pozwala na zwiększenie produktywności bez kompromisów w zakresie bezpieczeństwa.

l **Dostosowywana sieć**: Pełna sieć mesh umożliwia dostosowanie Check Point SASE do Twoich specyficznych potrzeb, zapewniając płynne połączenia między użytkownikami a zasobami.

l **Zintegrowane zarządzanie**: Całą infrastrukturą zabezpieczeń sieciowych można zarządzać z jednego intuicyjnego panelu – Check Point Infinity Portal.