OPIS ROZWIĄZANIA

Sophos Endpoint

Zapobieganie naruszeniom bezpieczeństwa, atakom ransomware i utracie danych dzięki zabezpieczeniom opartym na sztucznej inteligencji

Sophos Endpoint zapewnia niezrównaną ochronę przed zaawansowanymi cyberatakami dzięki najlepszym w swojej klasie zabezpieczeniom punktów końcowych. Kompleksowe, wielowarstwowe podejście do ochrony — obejmujące ochronę przed oprogramowaniem ransomware o zamkniętej, spójnej architekturze (airtight ransomware protection) — automatycznie zatrzymuje najszerszy zakres zagrożeń, zanim wpłyną one na systemy. Narzędzia wykrywania i reagowania oparte na sztucznej inteligencji umożliwiają zespołowi szybkie i precyzyjne analizowanie oraz neutralizowanie podejrzanych działań i zaawansowanych zagrożeń wymierzonych w punkty końcowe i serwery.

Przykłady zastosowań

1 | PODEJŚCIE OPARTE NA ZAPOBIEGANIU

Pożądany rezultat: blokowanie większej liczby zagrożeń na wczesnym etapie w celu minimalizacji ryzyka i zmniejszenia obciążenia zespołu.

Rozwiązanie: Sophos Endpoint stosuje kompleksowe podejście do bezpieczeństwa typu prevention-first, automatycznie blokując zagrożenia bez polegania na jednej technice. Modele sztucznej inteligencji oparte na głębokim uczeniu chronią przed znanymi i nowymi atakami. Kontrola sieci, aplikacji i urządzeń peryferyjnych ogranicza powierzchnię ataku i blokuje typowe wektory ataków. Analiza behawioralna, ochrona przed oprogramowaniem ransomware, ochrona przed exploitami i inne zaawansowane technologie szybko powstrzymują zagrożenia, zanim dojdzie do ich eskalacji, dzięki czemu zespoły IT o ograniczonych zasobach mają mniej incydentów do zbadania i rozwiązania.

2 | ADAPTACYJNE ZABEZPIECZENIA

Pożądany rezultat: powstrzymanie aktywnych przeciwników dzięki dynamicznej ochronie, która automatycznie dostosowuje się wraz z rozwojem ataku.

Rozwiązanie: Gdy Sophos Endpoint wykryje atak typu „hands-on-keyboard”, dynamicznie uruchamia dodatkowe mechanizmy obrony stosując podejście „shields up”, aby natychmiast zatrzymać działania przeciwników. Ta pierwsza w branży funkcja, unikalna dla Sophos, minimalizuje powierzchnię ataku oraz zakłóca i ogranicza atak, uniemożliwiając cyberprzestępcom podejmowanie dalszych działań i zapewniając zespołowi cenny czas na reakcję.

3 | UPROSZCZONE ZARZĄDZANIE

Pożądany rezultat: koncentracja na zagrożeniach zamiast na administracji.

Rozwiązanie: Sophos Central to oparta na chmurze, natywnie wykorzystująca AI platforma zarządzania cyberbezpieczeństwem, która łączy wszystkie rozwiązania bezpieczeństwa nowej generacji Sophos. Silne ustawienia polityk domyślnych zapewniają, że organizacja natychmiast uzyska zalecaną ochronę bez konieczności dodatkowego szkolenia lub dostosowywania. Funkcja sprawdzania kondycji konta Sophos Central identyfikuje problemy konfiguracyjne i umożliwia ich proste rozwiązanie za pomocą jednego kliknięcia, wzmacniając poziom bezpieczeństwa organizacji.

4 | WYKRYWANIE I REAGOWANIE

Pożądany rezultat: Neutralizacja ataków, których nie można powstrzymać wyłącznie za pomocą technologii.

Rozwiązanie: Potężna funkcja wykrywania i reagowania na zagrożenia na punktach końcowych (EDR) umożliwia identyfikację, analizowanie i reagowanie na podejrzane działania w obrębie punktów końcowych i serwerów. Rozszerzone wykrywanie i reagowanie Sophos (XDR) rozszerza mozliwości EDR, zapewniając widoczność całej powierzchni ataku poprzez integrację informacji o zagrożeniach pochodzących z istniejących i przyszłych inwestycji w rozwiązania bezpieczeństwa. Organizacje dysponujące ograniczonymi zasobami wewnętrznymi mogą skorzystać z zarządzanych usług wykrywania i reagowania Sophos (MDR), realizowanych przez globaln zespół ekspertów ds. cyberbezpieczeństwa, którzy monitorują środowisko użytkownika pod kątem zagrożeń 24/7.

Gartner

Lider w raporcie Gartner® Magic Quadrant™ 2025 dla platform ochrony punktów końcowych – po raz 16. z rzędu

Gartner Peer Insights Customers' Choice 2025

Wyróżnienie „Customers' Choice” w raporcie Gartner® Voice of the Customer 2025 dla platform ochrony punktów końcowych.

SE Labs

Wiodące w branży wyniki w niezależnych testach ochrony prowadzonych przez zewnętrzne podmioty

#1

Najbardziej rozbudowana ochrona punktów końcowych typu zero-touch (bez konieczności interwencji użytkownika) przed zdalnym ransomware

Dowiedz się więcej i rozpocznij bezpłatny okres próbny:

sophos.com/endpoint

2025-09-17 SB-EN (NP)