BROSZURA DOTYCZĄCA ROZWIĄZANIA

# Sophos Endpoint i EDR

Kompleksowa ochrona punktów końcowych, wykrywanie i reagowanie

## Najbardziej zaawansowane rozwiązanie w branży do ochrony punktów końcowych oparte na sztucznej inteligencji

Sophos Endpoint zapewnia niezrównaną ochronę przed zaawansowanymi cyberatakami dzięki podejściu prevention-first oraz najlepszym w swojej klasie zabezpieczeniom punktów końcowych. Sophos Endpoint Detection and Response (EDR) to kompleksowe rozwiązanie do ochrony, wykrywania i reagowania, które obejmuje Sophos Endpoint i jest przeznaczone dla analityków bezpieczeństwa oraz administratorów IT. Chroń i monitoruj swoje punkty końcowe oraz serwery pod kątem podejrzanej aktywności, niezależnie od tego, czy znajdują się one w biurze, zdalnie, czy w chmurze.

## Podejście do bezpieczeństwa oparte na zapobieganiu

Sophos Endpoint opiera się na podejściu prevention-first, w którym kluczowe znaczenie ma zapobieganie zagrożeniom już na etapie ich powstawania. Rozwiązanie automatycznie blokuje zagrożenia, nie polegając na jednej technice. Modele sztucznej inteligencji oparte na głębokim uczeniu chronią przed znanymi, jak i nowymi atakami. Ograniczanie powierzchni ataku, analiza behawioralna, ochrona przed ransomware, zabezpieczenia przed exploitami oraz inne zaawansowane mechanizmy pozwalają szybko zatrzymać zagrożenia, zanim dojdzie do eskalacji.

## Adaptacyjne mechanizmy obronne

Gdy Sophos Endpoint wykryje atak typu „hands-on-keyboard”, dynamicznie uruchamia dodatkowe zabezpieczenia w modelu „shields up”, aby natychmiast powstrzymać działania przeciwników. Ta pierwsza w branży, unikalna dla Sophos funkcja minimalizuje powierzchnię ataku oraz zakłóca i powstrzymuje atak, ograniczając cyberprzestępcom podejmowanie kolejnych kroków i zapewniając zespołowi cenny czasu na reakcję.

## Uzyskaj wgląd w trudne do wykrycia zagrożenia

Sophos EDR zapewnia wykrywanie zagrożeń z priorytetyzacją opartą na sztucznej inteligencji, które wskazują podejrzaną aktywność wymagającą natychmiastowej uwagi. Analizuj aktywność w czasie rzeczywistym dzięki dostępowi do rozbudowanych danych na urządzeniu oraz telemetrii w jeziorze danych Sophos, w tym historii aktywności, nawet gdy urządzenia są offline.

## Przyspiesz i wzmocnij swój zespół

Sophos EDR jest przeznaczony dla informatyków ogólnych i analityków bezpieczeństwa. Potężne narzędzia umożliwiają zespołowi szybkie i łatwe wykonywanie rozbudowanych zadań operacyjnych związanych z IT dzięki bezpośredniemu i bezpiecznemu połączeniu z urządzeniami. Narzędzia AI ukierunkowane na rezultat usprawniają procesy dochodzenia i reagowania, pozwalające zespołowi szybko i precyzyjnie badać oraz neutralizować podejrzaną aktywność i trudne do wykrycia zagrożenia omijające wymierzone w punkty końcowe i serwery.

## Najważniejsze cechy

- Podejście oparte na zapobieganiu, które zmniejsza powierzchnię ataku i szybko powstrzymuje zagrożenia.
- Ochrona danych przed lokalnymi i zdalnymi atakami ransomware dzięki najlepszej ochronie w swojej klasie.
- Skorzystaj z pierwszych w branży adaptacyjnych mechanizmów obronnych, które automatycznie dostosowują się w odpowiedzi na aktywnych przeciwników oraz ataki typu „hands-on-keyboard”.
- Wykrywanie oparte na sztucznej inteligencji wskazuje obszary, na których zespół powinien się skupić.
- Narzędzia AI ukierunkowane na rezultat usprawniają dochodzenie i reagowanie na podejrzane działania oraz trudne do wykrycia zagrożenia.
- Potężne narzędzia dla informatyków ogólnych i analityków bezpieczeństwa.

# Podejście oparte na zapobieganiu zmniejsza powierzchnię ataku

Wczesne powstrzymanie ataków wymaga mniej zasobów niż monitorowanie i usuwanie ich skutków na późniejszym etapie łańcucha ataku. Sophos Endpoint zawiera zaawansowane technologie ochrony, które blokują najszerszy zakres ataków. Kontrola sieci, aplikacji i urządzeń peryferyjnych zmniejsza powierzchnię ataku i blokuje typowe wektory ataków, ograniczając możliwości penetracji środowiska przez atakujących.

## Ochrona sieci

Przechwytuje wychodzące połączenia przeglądarki i blokuje ruch kierowany do złośliwych lub podejrzanych stron internetowych. Powstrzymuje zagrożenia na etapie dostarczania, uniemożliwiając przekierowanie użytkowników do stron internetowych służących do dystrybucji złośliwego oprogramowania lub phishingu.

## Kontrola sieci

Blokuje dostęp do niepożądanych i nieodpowiednich treści. Egzekwuj akceptowalne zasady korzystania z Internetu w całej organizacji i chroń się przed utratą danych.

## Reputacja pobieranych plików

Analizuje pobierane pliki z użyciem globalnej analityki zagrożeń SophosLabs, aby wydać opinię na podstawie rozpowszechnienia, wieku oraz źródła, zachęcając użytkowników do blokowania plików o niskiej lub nieznanej reputacji.

## Kontrola aplikacji

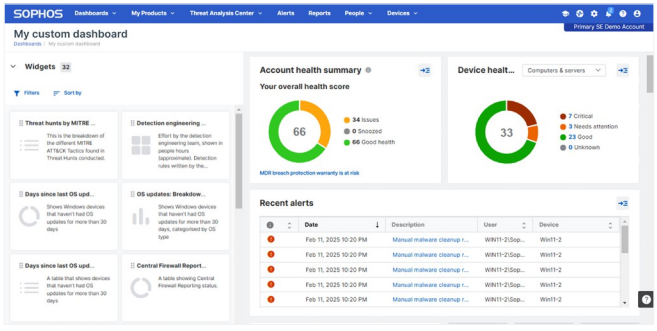
Blokuj aplikacje, które mogą być podatne na zagrożenia, nieodpowiednie dla danego środowiska lub możliwe do wykorzystania w niecnych celach. Sophos udostępnia predefiniowane kategorie do blokowania lub monitorowania aplikacji, eliminując konieczność blokowania pojedynczych aplikacji na podstawie skrótu (hasha).

## Kontrola urządzeń peryferyjnych

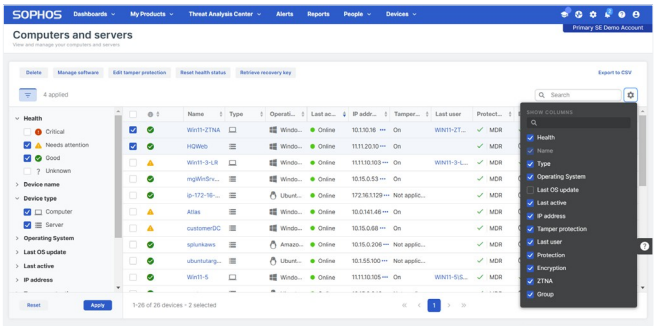
Monitoruje i blokuje dostęp do nośników wymiennych, urządzeń Bluetooth oraz urządzeń mobilnych, aby uniemożliwić niektórym urządzeniom połączenie się z siecią.

## Zapobieganie utracie danych

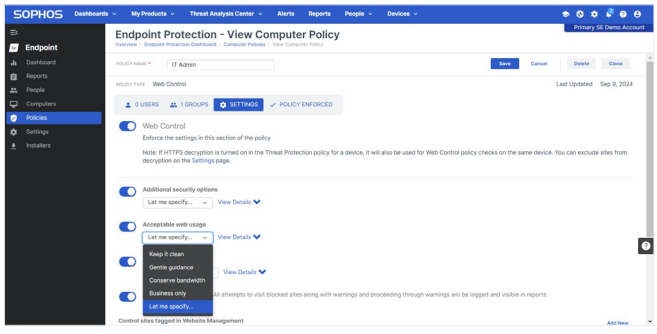
Monitoruj lub ograniczaj przesyłanie plików zawierających poufne dane. Przykładowo, uniemożliwiaj użytkownikom wysyłanie poufnych plików za pośrednictwem poczty elektronicznej opartej na interfejsie webowym.



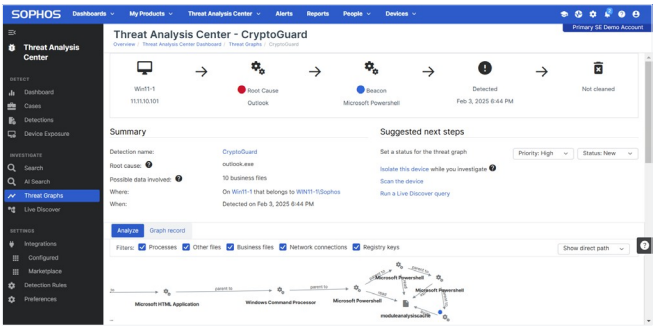

Twórz niestandardowe pulpity nawigacyjne dostosowane do swoich potrzeb.




Zabezpieczenia punktów końcowych, które są łatwe w konfiguracji i zarządzaniu.




Konfigurowalne zasady z domyślnie włączonymi zalecanymi ustawieniami.




Analizuj zagrożenia, aby ustalić ich pierwotną przyczynę.

# Podejście oparte na zapobieganiu pozwala szybko powstrzymać zagrożenia

Wykrywanie i usuwanie zagrożeń na jak najwcześniejszym etapie zmniejsza ryzyko. Sophos Endpoint szybko powstrzymuje zagrożenia, zanim się nasilą, dzięki czemu zespoły IT dysponujące ograniczonymi zasobami mają mniej incydentów do zbadania i rozwiązania. Sophos zapewnia silne funkcje zapobiegania zagrożeniom, potwierdzone konsekwentnymi najwyższymi wynikami w niezależnych testach bezpieczeństwa.

## Kompleksowa ochrona przed ransomware

Zgodnie z reaportem Microsoft „2024 Digital Defense Report", zdalne szyfrowanie występuje obecnie w 70% udanych ataków, z czego 92% pochodzi z niezarządzanych urządzeń w sieci. Sophos Endpoint zapewnia najsilniejszą ochronę punktów końcowych przed lokalnym i zdalnym oprogramowaniem ransomware, wykorzystując zaawansowaną technologię CryptoGuard do wykrywania prób szyfrowania, niezależnie od źródła.

- Blokuje nowe i nieznane wcześniej warianty ransomware.
- Sprawdza zmiany w plikach w czasie rzeczywistym w celu wykrycia złośliwego szyfrowania.
- Zapobiega zdalnemu szyfrowaniu plików przez oprogramowanie ransomware za pośrednictwem sieci.
- Automatycznie przywraca zaszyfrowane pliki do ich pierwotnego, niezaszyfrowanego stanu — przy użyciu autorskiej technologii, która nie opiera się na Windows Shadow Copy Service.
- Chroni wszystkie typy i rozmiary plików przy minimalnym wpływie na wydajność.
- Chroni główny rekord rozruchowy (MBR) przed zaawansowanymi atakami wymierzonymi w dysk twardy.

## Zapobieganie złośliwemu oprogramowaniu oparte na głębokim uczeniu (wykorzystującym sztuczną inteligencję)

Wykrywa i blokuje zarówno znane, jak i nieznane złośliwe oprogramowanie poprzez analizę atrybutów plików i wykorzystanie wnioskowania predykcyjnego do identyfikacji zagrożeń.

## Ochrona przed wykorzystaniem luk w zabezpieczeniach

Chroni integralność procesów poprzez wzmocnienie pamięci aplikacji i zastosowanie zabezpieczeń wykonywania kodu w czasie rzeczywistym. Sophos Endpoint zawiera ponad 60 technik zapobiegania wykorzystywaniu luk w zabezpieczeniach, które są domyślnie włączone i nie wymagają szkolenia ani dostosowywania. Techniki te zapewniają ochronę znacznie przewyższającą ochronę zapewnianą przez system Windows i większość innych rozwiązań zabezpieczających punkty końcowe.

## Ochrona behawioralna

Monitoruje zdarzenia związane z procesami, plikami i rejestrem w czasie rzeczywistym, aby wykrywać i zatrzymywać złośliwe działania i procesy. Przeprowadza również skanowanie pamięci, sprawdza uruchomione procesy w celu wykrycia złośliwego kodu ujawnionego tylko podczas wykonywania procesu oraz wykrywa osoby atakujące, które umieszczają złośliwy kod w pamięci uruchomionego procesu, aby uniknąć wykrycia.

## Zsynchronizowane zabezpieczenia

Sophos Endpoint udostępnia informacje o stanie i kondycji Sophos Firewall, Sophos Wireless, Sophos Zero Trust Network Access (ZTNA) i innym produktom Sophos, aby zapewnić dodatkową widoczność zagrożeń i wykorzystania aplikacji oraz automatycznie izolować zainfekowane urządzenia.

## Ochrona na żywo

Rozszerza kompleksową ochronę urządzeń dzięki wyszukiwaniu w czasie rzeczywistym najnowszych informacji o zagrożeniach globalnych z SophosLabs w celu uzyskania dodatkowego kontekstu plików, weryfikacji decyzji, eliminacji fałszywych alarmów i reputacji plików. Nasze badania zagrożeń Tier 1 dostarczają dodatkowe bieżących informacji, pochodzących z rozbudowanego portfolio produktów Sophos oraz globalnej bazy klientów.

## Blokada aplikacji

Zapobiega niewłaściwemu użyciu przeglądarki i aplikacji poprzez blokowanie działań, które nie są powszechnie kojarzone z tymi procesami. Przykładowo przeglądarka internetowa lub aplikacja pakietu Office próbująca uruchomić program PowerShell.

## Interfejs skanowania antywirusowego (AMSI)

Interfejs skanowania antywirusowego systemu Windows (AMSI) określa, czy skrypty (np. PowerShell lub makra Office) są bezpieczne, w tym czy są one zaszyfrowane lub generowane w czasie wykonywania, blokując ataki bezplikowe, w których złośliwe oprogramowanie jest ładowane bezpośrednio z pamięci. Sophos posiada również własne rozwiązanie ograniczające skutki złośliwego oprogramowania, które próbuje uniknąć wykrycia przez AMSI.

## Wykrywanie złośliwego ruchu

Wykrywa urządzenia próbujące komunikować się z serwerem dowodzenia i kontroli (C2) poprzez przechwytywanie ruchu z procesów innych niż przeglądarka oraz analizę, czy jest on kierowany do złośliwego adresu.

# Adaptacyjne zabezpieczenia

Sophos Endpoint wykorzystuje pierwsze w branży dynamiczne zabezpieczenia, które automatyzują ochronę, dostosowując się w czasie rzeczywistym do walki z aktywnymi przeciwnikami i atakami typu „hands-on-keyboard”. Adaptacyjne zabezpieczenia blokują działania, które w typowym kontekście mogą nie wydawać się złośliwe, ale mogą być szkodliwe podczas ataku. Dynamicznie reagują na aktywne ataki i zakłócają je, nawet gdy atakujący zdobyli już przyczółek, a wszystko to bez uruchamiania alarmów i polegania na złośliwym kodzie.

## Adaptacyjna ochrona przed atakami

Dynamicznie włącza wzmocnioną ochronę punktu końcowego po wykryciu ataku typu „hands-on-keyboard”, zakłócając działania przeciwnika i dając Ci więcej czasu na reakcję.

## Ostrzeżenie o krytycznym ataku

Powiadamia administratorów o poważnych atakach zachodzących na wielu punktach końcowych, na podstawie wykrytych zagrożeń w całej organizacji.

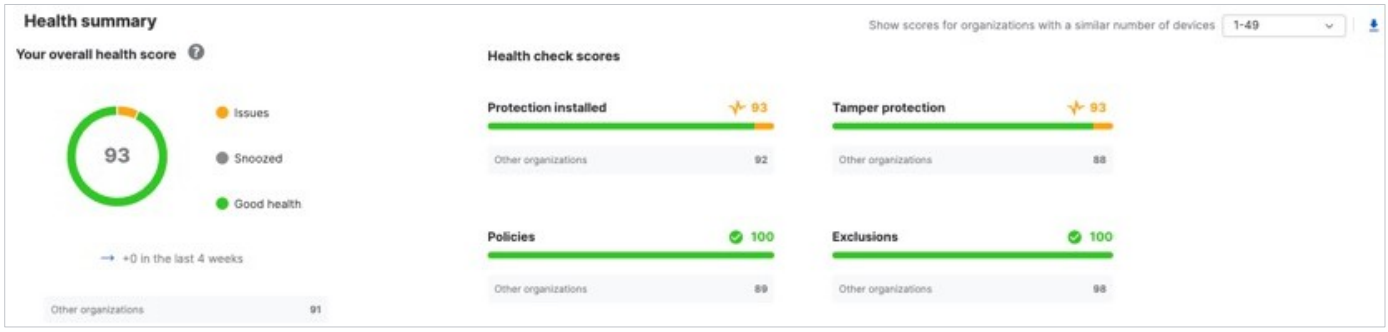
| | OCHRONA BEZPIECZEŃSTWA | ADAPTACYJNA OCHRONA PRZED ATAKAMI | OSTRZEŻENIE O KRYTYCZNYM ATAKU |
|---|---|---|---|
| ZAKRES | POJEDYNCZE URZĄDZENIE | POJEDYNCZE URZĄDZENIE | CAŁA INFRASTRUKTURA |
| KORZYŚCI | Silnik behawioralny zatrzymuje aktywne ataki przeciwników na wczesnym etapie | Zwiększa czułość ochrony, aby zapobiegać atakom | Ostrzega o ataku wymagającym natychmiastowej reakcji |
| WYZWALACZ | Reguły behawioralne | Wykryte zestawy narzędzi hakerskich | Wskaźniki aktywnych ataków o dużym wpływie, w tym korelacje na poziomie organizacji i progi |
| ANALOGIA | „OCHRONA WŁĄCZONA!” | „WŁĄCZ OCHRONĘ!” | „CZERWONY ALARM!” |

Adaptacyjne zabezpieczenia w Sophos Endpoint

# Silne domyślne zasady i identyfikowanie odchyleń w poziomie bezpieczeństwa

Domyślnie Sophos Endpoint jest wyposażony w zalecane przez nas technologie ochrony, które zapewniają natychmiastową, najsilniejszą ochronę. Nie ma potrzeby skomplikowanej konfiguracji ani dostosowywania. Jeśli jednak zajdzie taka potrzeba, można również skorzystać z opcji bardziej szczegółowej kontroli.

Nieprawidłowo skonfigurowane ustawienia zasad, wykluczenia i inne czynniki mogą zagrozić bezpieczeństwu. Funkcja sprawdzania stanu konta identyfikuje odchylenia od stanu bezpieczeństwa i konfiguracje wysokiego ryzyka oraz umożliwia usunięcie problemów za pomocą jednego kliknięcia.




Kontrola stanu konta

## Przyspiesz wykrywanie, badanie i reagowanie

Sophos EDR to kompleksowe rozwiązanie do ochrony, wykrywania i reagowania, zaprojektowane z myślą o informatykach ogólnych i analitykach bezpieczeństwa. Sophos EDR zmniejsza ryzyko związane z bezpieczeństwem, umożliwiając reagowanie na trudne do wykrycia zagrożenia i ograniczając potencjalny wpływ na działalność firmy. Sophos Endpoint jest dołączony do Sophos EDR i natywnie zintegrowany z tym rozwiązaniem.

### Wykrywanie oparte na sztucznej inteligencji

Łatwo identyfikuj podejrzane działania, które wymagają natychmiastowej uwagi. Sophos EDR automatycznie nadaje priorytet wykryciom w oparciu o ryzyko, zapewniając pełny kontekst.

### Reakcje analityków bezpieczeństwa

Twój zespół może izolować punkt końcowy, ręcznie włączyć adaptacyjną ochronę przed atakami podczas badania podejrzanej aktywności i nie tylko.

### Podsumowanie przypadku AI

Zapewnia łatwy do zrozumienia przegląd wykrytych zagrożeń i zalecanych dalszych kroków, pomagając w szybkim podejmowaniu trafnych decyzji.

### Zautomatyzowane reakcje

Zautomatyzowane działania, takie jak zakończenie procesu, cofnięcie oprogramowania ransomware, izolacja sieci i adaptacyjna ochrona przed atakami, szybko powstrzymują zagrożenia i oszczędzają cenny czas Twojego zespołu.

### Wyszukiwanie AI

Wykorzystuje język naturalny, aby przyspieszyć codzienne zadania i obniżyć barierę technologiczną w zakresie operacji związanych z bezpieczeństwem.

### Analiza poleceń AI

Analizuje złożone argumenty wiersza poleceń, aby odkryć ich intencje i wpływ, wraz z wyjaśnieniami w prostym języku.

## Reakcja na żywo

Sophos EDR umożliwia informatykom ogólnym i analitykom bezpieczeństwa wykonywanie zadań operacyjnych związanych z IT oraz szybkie i precyzyjne usuwanie zagrożeń. Bezpośrednie, bezpieczne i kontrolowane połączenie z punktami końcowymi i serwerami w celu zbadania i usunięcia ewentualnych problemów bezpośrednio z konsoli Sophos.

### Zdalny dostęp do urządzeń w celu

- Instalowania i odinstalowywania oprogramowania
- Uruchamiania skryptów i programów
- Edytowania plików konfiguracyjnych
- Wyłączania/restartowania
- Uruchamiania narzędzi kryminalistycznych innych producentów
- I wiele więcej

### Ekspozycja urządzenia

Szybko identyfikuj ryzykowne, nieaktualne i podatne na ataki urządzenia w swoim środowisku. Funkcja ekspozycji urządzeń dostarcza informacji o tym, które urządzenia są najbardziej podatne na zagrożenia, i umożliwia podjęcie działań w przypadku urządzeń, na których od dłuższego czasu nie przeprowadzono aktualizacji systemu operacyjnego.

## Co zawiera Sophos Endpoint i Sophos EDR

| | Sophos Endpoint | Sophos EDR |
|---|---|---|
| **Ochrona punktów końcowych nowej generacji**<br>Zapobieganie złośliwemu oprogramowaniu oparte na głębokim uczeniu (AI), ochrona przed oprogramowaniem ransomware, analiza behawioralna, ochrona przed exploitami i wiele więcej. | ✓ | ✓ |
| **Adaptacyjne zabezpieczenia**<br>Adaptacyjna ochrona przed atakami, ostrzeganie o krytycznych atakach | ✓ | ✓ |
| **Ograniczenie narażenia punktów końcowych na zagrożenia**<br>Ochrona sieci, kontrola sieci, kontrola urządzeń peryferyjnych, kontrola aplikacji, utrata danych i zapobieganie | ✓ | ✓ |
| **Wykrywanie i reagowanie na zagrożenia w punktach końcowych (EDR)**<br>Wykrywanie, badanie i reagowanie na ataki wymierzone w punkty końcowe i serwery | | ✓ |
| **Reagowanie na żywo i narażenie urządzeń**<br>Potężne narzędzia dla informatyków ogólnych i analityków bezpieczeństwa | | ✓ |
| **Dane dotyczące wykrywania przechowywane w jeziorze danych Sophos**<br>Standardowo 30 dni | | ✓<br>(Możliwość przedłużenia do 1 roku) |
| **Sophos Endpoint dla starszych platform**<br>Kompleksowe zabezpieczenia dla starszych i nieobsługiwanych systemów operacyjnych Windows i Linux | Opcjonalny dodatek | Opcjonalny dodatek |
| **Sophos Device Encryption**<br>Scentralizowane zarządzanie natywnym szyfrowaniem dysków w urządzeniach z systemem Windows i macOS | Opcjonalny dodatek | Opcjonalny dodatek |
| **Usługi reagowania na incydenty (IR) Sophos**<br>Elitarny zespół ekspertów gotowy do działania w przypadku naruszenia bezpieczeństwa | Opcjonalny dodatek | Opcjonalny dodatek |

### Sophos XDR

Rozszerzone wykrywanie i reagowanie Sophos (XDR) zapewnia widoczność wykraczającą poza punkty końcowe i serwery. Zapewnia potężne narzędzia i informacje o zagrożeniach, które umożliwiają wykrywanie, badanie i neutralizowanie zagrożeń w całym ekosystemie IT, dostarczane za pośrednictwem adaptacyjnej, natywnej dla sztucznej inteligencji, otwartej platformy Sophos.

Nasza otwarta, rozszerzalna architektura zapewnia widoczność całego obszaru ataku poprzez integrację informacji o zagrożeniach pochodzących z istniejących i przyszłych inwestycji w zabezpieczenia. Sophos XDR obejmuje gotowe integracje z rozbudowanym ekosystemem rozwiązań w zakresie punktów końcowych, zapór sieciowych, sieci, poczty elektronicznej, tożsamości, kopii zapasowych, bezpieczeństwa w chmurze i produktywności.

Więcej informacji można znaleźć na stronie Sophos.com/XDR.

### Sophos MDR

Niezależnie od tego, na jakim etapie jesteś w swojej podróży ku bezpieczeństwu, nasze usługi Sophos Managed Detection and Response (MDR) zapewniają Ci przewagę nad przeciwnikami. Łączymy łatwą w użyciu technologię opartą na sztucznej inteligencji z światowej klasy ekspertami ds. bezpieczeństwa, którzy monitorują, zapobiegają, wykrywają i reagują na zagrożenia 24 godziny na dobę, 7 dni w tygodniu.

Wybierz spośród szerokiej gamy poziomów usług i trybów reagowania na zagrożenia, aby dopasować je do swoich potrzeb. Sophos MDR integruje informacje o zagrożeniach pochodzące z istniejących i przyszłych inwestycji w zabezpieczenia.

Więcej informacji można znaleźć na stronie Sophos.com/MDR

# Dowiedz się, dlaczego klienci wybierają Sophos Endpoint

Sophos jest uznanym liderem w dziedzinie bezpieczeństwa punktów końcowych, co potwierdzają branżowe wyróżnienia.

Gartner

Sophos został uznany za lidera w raporcie Gartner® Magic Quadrant™ 2025 dotyczącym platform ochrony punktów końcowych w 16 kolejnych raportach.

SE Labs

Sophos konsekwentnie osiąga wiodące w branży wyniki w niezależnych testach bezpieczeństwa punktów końcowych.

G2 Lider

Sophos jest jedynym dostawcą, który został uznany za lidera w raportach G2 Spring 2025 Overall Grid® dotyczących pakietów zabezpieczeń punktów końcowych, EDR, XDR, oprogramowania firewallowego i MDR.

IDC

Sophos został uznany za lidera w raporcie IDC MarketScape 2024 dotyczącym nowoczesnych zabezpieczeń punktów końcowych dla małych i średnich przedsiębiorstw na całym świecie.

Gartner Peer Insights Customers' Choice 2025

Sophos jest dostawcą wyróżnionym tytułem „Customers' Choice" w raporcie Gartner® Peer Insights™ „Voice of the Customer" z 2025 r. w kategorii platform ochrony punktów końcowych.

## Wypróbuj teraz za darmo

Zarejestruj się, aby skorzystać z bezpłatnej 30-dniowej wersji próbnej na stronie sophos.com/endpoint

Sprzedaż w Wielkiej Brytanii i na całym świecie Tel.: +44 (0)8447 671131
E-mail: sales@sophos.com

Sprzedaż w Ameryce Północnej
Bezpłatny numer: 1-866-866-2802
E-mail: nasales@sophos.com

Sprzedaż w Australii i Nowej Zelandii
Tel.: +61 2 9409 9100
E-mail: sales@sophos.com.au

Sprzedaż w Azji
Tel.: +65 62244168
E-mail: salesasia@sophos.com



2025-09-17 BR-EN (NP)

SOPHOS