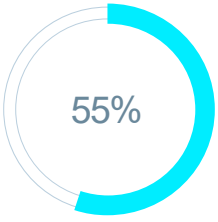
BROSZURA DOTYCZĄCA ROZWIĄZANIA

Sophos Extended Detection and Response (XDR)

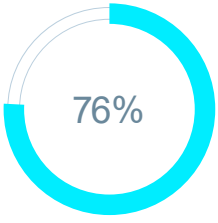
Ochrona przed zaawansowanymi, wieloetapowymi i wielowektorowymi atakami

Szybkie powstrzymywanie ataków ma kluczowe znaczenie. Sophos XDR zapewnia zaawansowane narzędzia oraz informacje o zagrożeniach, które umożliwiają wykrywanie, analizowanie i reagowanie na podejrzane aktywności w całym ekosystemie IT, dostarczane za pośrednictwem adaptacyjnej, natywnie wykorzystującej AI, otwartej platformy Sophos.



W 55% ataków ransomware do penetracji organizacji wykorzystywane są legalne dane uwierzytelniające oraz nieznane luki w zabezpieczeniach. [1]

Ogólna mediana czasu przebywania atakującego w przypadkach badanych przez zespół Sophos Incident Response wynosi 7 dni.[2]



Odrębne narzędzia powodują powstawanie silosów danych oraz ręczny nakład pracy. 76% organizacji doświadczyło w ciągu ostatniego roku wypalenia związanego z cyberbezpieczeństwem.[3]

Oparte na najsilniejszej ochronie

Zespoły IT dysponujące ograniczonymi zasobami mają mniej incydentów do analizowania i rozwiązywania, gdy więcej zagrożeń jest zatrzymywanych na wczesnym etapie. Sophos łączy rozszerzone wykrywanie i reagowanie z najsilniejszą w branży ochroną punktów końcowych, blokując zagrożenia, zanim będą wymagały ręcznej analizy — zmniejszając tym samym obciążenie zespołu.

Uzyskaj pełną widoczność powierzchni ataku

Im więcej widzisz, tym szybciej możesz działać. Nasza otwarta, rozszerzalna architektura zapewnia widoczność całego środowiska IT poprzez integrację informacji o zagrożeniach z istniejących rozwiązań w jednej platformie wykrywania i reagowania. Sophos XDR obejmuje integrację z szeroką gamą narzędzi i technologii.

Przyspiesz działania związane z bezpieczeństwem dzięki GenAI

Zmaksymalizuj efektywność analityków i przyspiesz analizy oraz reagowanie. Narzędzia oparte na sztucznej inteligencji, dostępne w Sophos XDR, usprawniają procesy analizy, zapewniając wgląd w czasie rzeczywistym, kontekstualizując dane dotyczące zagrożeń i oferując jasne rekomendacje.

Otwarta platforma zaprojektowana w celu optymalizacji i ujednolicenia

Skorzystaj z jednego widoku całego ekosystemu IT i skoncentruj działania analityczne na sprawach o wysokim priorytecie, zamiast na nieistotnych, niemożliwych do zrealizowania alertach. Zidentyfikuj najpoważniejsze zagrożenia dzięki priorytetyzacji i analizom opartym na sztucznej inteligencji oraz współpracuj z członkami zespołu, korzystając z solidnych procesów badawczych i narzędzi do zarządzania sprawami.

Najważniejsze informacje

- Zyskaj wgląd w podejrzane działania i trudne do wykrycia zagrożenia we wszystkich kluczowych obszarach powierzchni ataku.
- Otwarta platforma XDR z szeroką gamą integracji w zestawie.
- Uzyskaj większy zwrot z istniejących inwestycji technologicznych.
- Analizuj i reaguj na zagrożenia szybko dzięki priorytetyzowanym wykryciom oraz narzędziom opartym na sztucznej inteligencji.
- Obejmuje wiodącą w branży ochronę punktów końcowych oraz EDR.

Wykrywaj, analizuj i reaguj z maksymalną efektywnością

Sophos XDR zawiera narzędzia i przepływy pracy zaprojektowane w celu zwiększenia wydajności analityków bezpieczeństwa i administratorów IT. Automatycznie generowane sprawy umożliwiają szybkie analizowanie potencjalnych zagrożeń, zrozumienie zakresu oraz przyczyny incydentu, a także skrócenie czasu reakcji.

Wykrycia priorytetyzowane przez AI

Łatwo identyfikuj podejrzaną aktywność wymagającą natychmiastowej uwagi. Sophos XDR automatycznie priorytetyzuje wykrycia na podstawie ryzyka, zapewniając pełny kontekst.

Mapowanie struktury MITRE ATT&CK

Wykrycia i sprawy są automatycznie mapowane do taktyk MITRE ATT&CK, co pozwala łatwo zidentyfikować luki w zabezpieczeniach i ustalić priorytety usprawnień.

Szybka analiza i wykrywanie zagrożeń

Wyszukiwanie oparte na sztucznej inteligencji w języku naturalnym oraz gotowe szablony zapytań umożliwiają szybkie odnajdywanie informacji potrzebnych do przeprowadzenia analizy, bez konieczności posiadania wiedzy eksperckiej z zakresiu języka SQL.

Zautomatyzowane reakcje

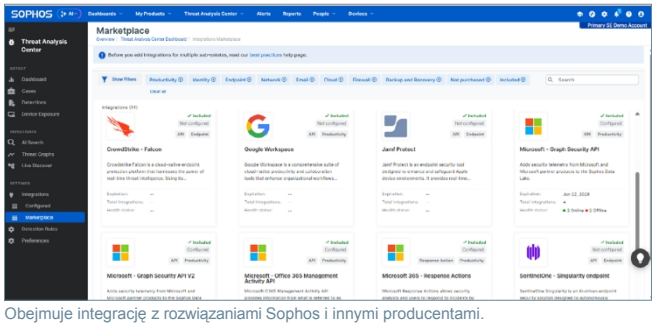
Zautomatyzowane działania, takie jak zakończenie procesu, cofanie skutków ransomware, izolacja sieci oraz adaptacyjna ochrona przed atakami, pozwalają szybko ograniczać zagrożenia i oszczędzać cenny czas zespołu.

Wspólne zarządzanie sprawami

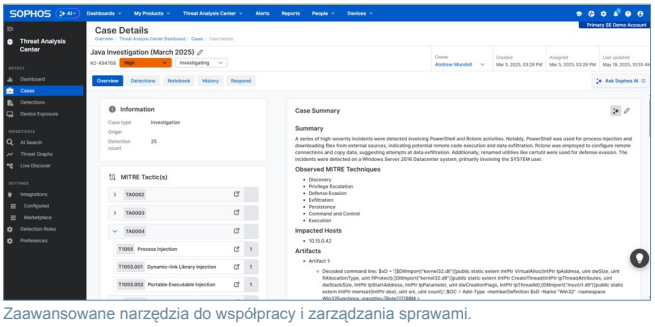
Automatyczne tworzenie spraw umożliwia szybką analizę, a kompleksowe narzędzia do zarządzania sprawami ułatwiają współpracę z innymi członkami zespołu.

Działania podejmowane przez analityków

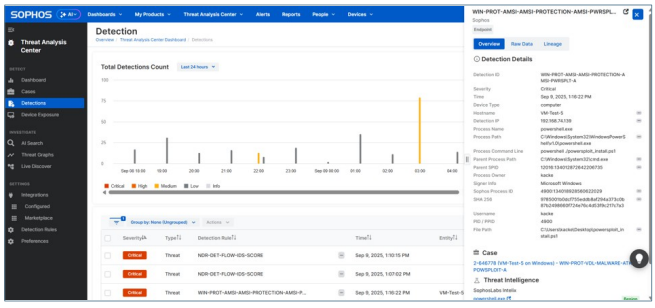
Wykonuj szeroki zakres działań reakcyjnych, aby szybko ograniczyć i zneutralizować zagrożenia, również w środowiskach Microsoft 365.



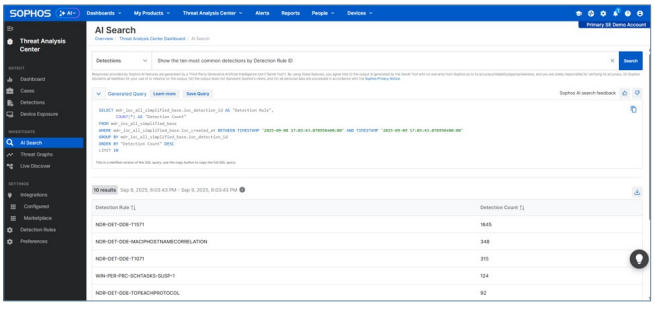
Obejmuje integrację z rozwiązaniami Sophos i innymi producentami.



Zaawansowane narzędzia do współpracy i zarządzania sprawami.



Wykrywanie priorytetowe oparte na sztucznej inteligencji we wszystkich kluczowych obszarach ataku.



Wyszukiwanie oparte na sztucznej inteligencji w języku naturalnym — nie jest wymagana znajomość języka SQL.

Przyspiesz działania związane z bezpieczeństwem dzięki GenAI

Rozbudowane możliwości generatywnej sztucznej inteligencji w Sophos XDR umożliwiają Twojemu zespołowi podejmowanie inteligentnych decyzji i szybsze neutralizowanie przeciwników, zwiększając zarówno zaufanie analityków, jak i biznesu. Funkcje GenAI są automatycznie dostępne do Sophos XDR.

Asystent AI

Prowadzi użytkowników o różnych poziomach kompetencji przez każdy etap analizy sprawy, maksymalizując efektywność w celu szybkiego zatrzymywania zagrożeń.

Wyszukiwanie AI

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

Podsumowanie sprawy AI

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

Analiza poleceń AI

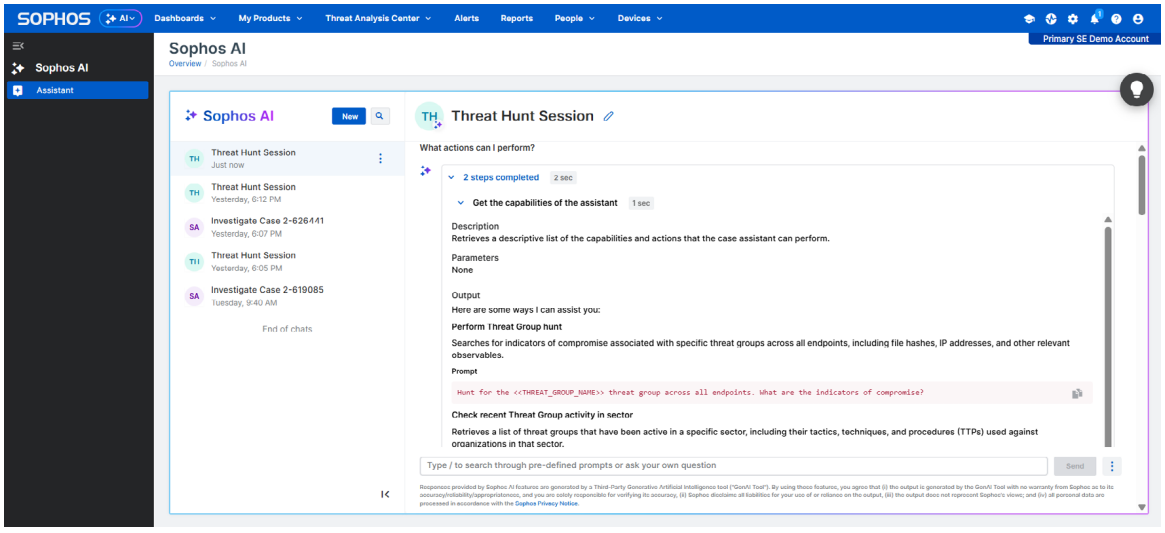
Analizuje złożone argumenty wiersza poleceń, aby odkryć ich intencje i wpływ, wraz z wyjaśnieniami w prostym języku.

Sophos AI Assistant

Asystent Sophos AI ułatwia wszystkim użytkownikom — od informatyków ogólnych po analityków SOC poziomu 3 — uzyskanie informacji potrzebnych do prowadzenia dochodzeń dotyczących zagrożeń oraz szybkiego neutralizowania przeciwników.

- **Wykonuj szeroki zakres zadań SecOps:** Analizuj podejrzane polecenia, twórz listy wskaźników IOC, wzbogacaj dane o informacje wywiadowcze dotyczące zagrożeń, twórz szczegółowe raporty i nie tylko.
- **Zadawaj pytania, używając języka potocznego** lub skorzystaj z gotowych podpowiedzi przygotowanych przez ekspertów Sophos ds. zagrożeń. Skorzystaj z przejrzystych podsumowań i zaleceń dotyczących dalszych działań.
- **Zaprojektowany we współpracy z analitykami bezpieczeństwa Sophos:** korzystaj z rzeczywistych przepływów pracy oraz doświadczenia ekspertów Sophos MDR.
- **Ciągła aktualizacja w oparciu o aktualny stan zagrożeń:** zapewnia dostęp do najnowszych technik analizy oraz informacji wywiadowczych o zagrożeniach pochodzących z Sophos X-Ops.

To nie jest po prostu kolejne narzędzie AI — to specjalistyczna wiedza zespołu stojącego za wiodącą na świecie usługą Managed Detection and Response, zawarta w inteligentnym agencie.



Integracje produktów Sophos „gotowych do XDR”

Rozwiązania Sophos płynnie współpracują ze sobą, zapewniając najlepsze możliwe wyniki w zakresie bezpieczeństwa. Nasza szeroka gama wielokrotnie nagradzanych produktów, w tym Endpoint, Firewall, NDR, ZTNA, Email, Cloud i Mobile, jest w pełni zintegrowana z platformą XDR — a najlepsza w swojej klasie ochrona Sophos Endpoint jest automatycznie dołączona.

SOPHOS ENDPOINT

Blokuj zaawansowane zagrożenia na punktach końcowych i serwerach, w tym wyrafinowane ataki ransomware.

W zestawie z Sophos XDR

SOPHOS EDR

Wykrywaj, analizuj i reaguj na podejrzaną aktywność oraz zagrożenia trudne do wykrycia, wymierzone w punkty końcowe.

W zestawie z Sophos XDR

SOPHOS ITDR

Monitoruj swoje środowisko pod kątem zagrożeń związanych z tożsamością i uzyskaj informacje z dark web na temat naruszonych danych uwierzytelniających.

Produkt sprzedawany oddzielnie; zintegrowany bez dodatkowych opłat

SOPHOS FIREWALL

Monitoruj i filtruj przychodzący oraz wychodzący ruch sieciowy, aby zatrzymywać zaawansowane zagrożenia, zanim zdążą wyrządzić szkody.

Produkt sprzedawany oddzielnie; subskrypcja Xstream Protection wymagana; zintegrowany bez dodatkowych opłat

SOPHOS NDR

Ciągle monitoruj aktywność wewnątrz sieci w celu wykrywania podejrzanych działań zachodzących pomiędzy urządzeniami, które w innym przypadku pozostałyby niewidoczne.

Produkt sprzedawany oddzielnie; zintegrowany bez dodatkowych opłat. Zgodny z dowolną siecią dzięki mirroringowi portów SPAN.

SOPHOS ZTNA

Zastąp zdalny dostęp VPN dostępem z minimalnymi uprawnieniami, aby bezpiecznie połączyć użytkowników z aplikacjami sieciowymi.

Produkt sprzedawany oddzielnie; zintegrowany bez dodatkowych opłat

SOPHOS MOBILE

Chroń swoje urządzenia z systemem iOS i Android oraz dane przed najnowszymi zagrożeniami mobilnymi.

Produkt sprzedawany oddzielnie; zintegrowany bez dodatkowych opłat

SOPHOS EMAIL

Chroń swoją skrzynkę odbiorczą przed złośliwym oprogramowaniem dzięki zaawansowanej sztucznej inteligencji, która powstrzymuje ukierunkowane ataki typu phishing i podszywanie się pod inne osoby.

Produkt sprzedawany oddzielnie; zintegrowany bez dodatkowych opłat

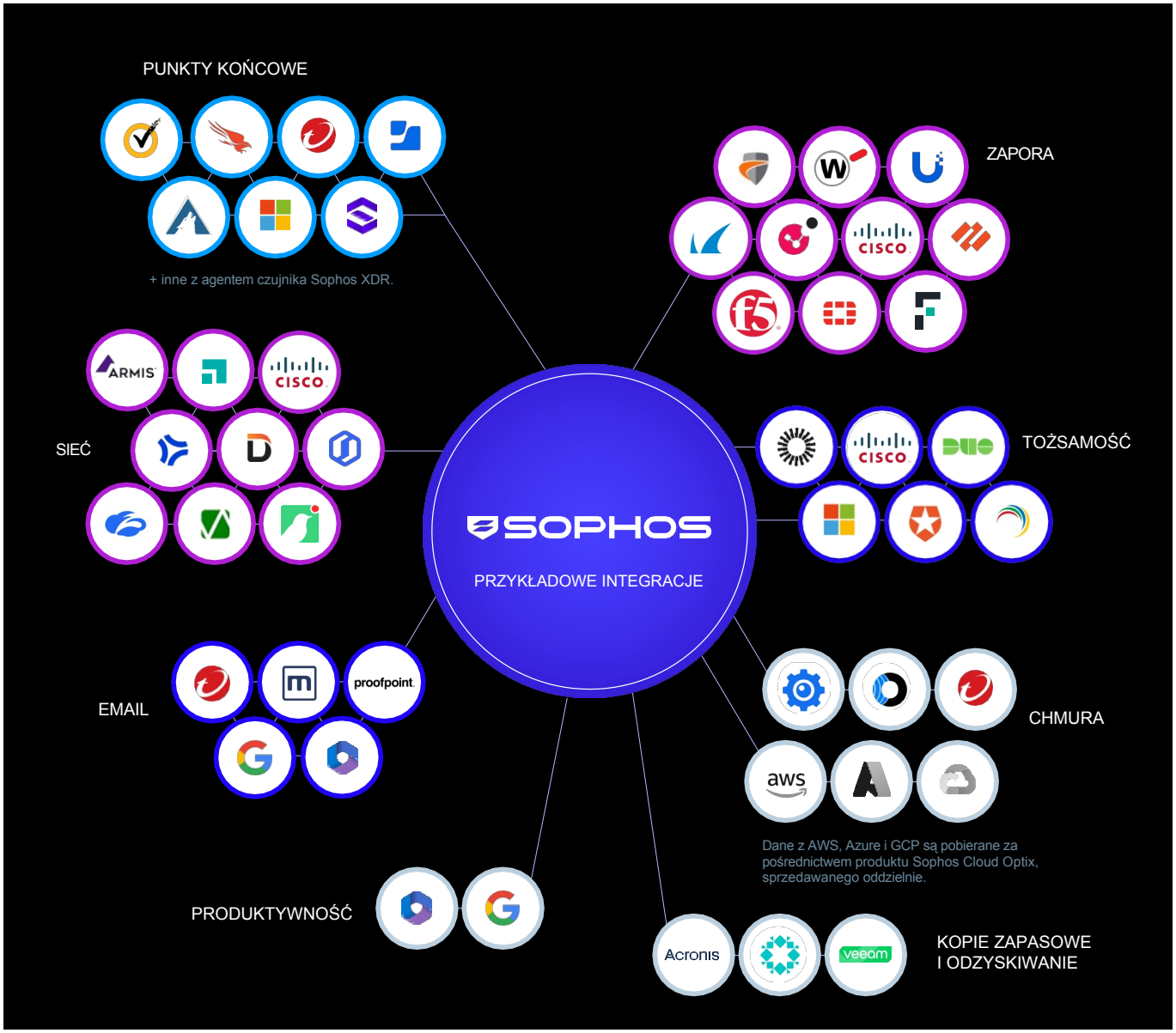
SOPHOS CLOUD OPTIX

Zapobiegaj naruszeniom bezpieczeństwa w chmurze i uzyskaj wgląd w kluczowe usługi chmurowe, w tym AWS, Azure i GCP.

Produkt sprzedawany oddzielnie; zintegrowany bez dodatkowych opłat

Wykorzystaj inwestycje w technologie inne niż Sophos

Zwiększ zwrot z inwestycji w narzędzia zabezpieczające, z których korzystasz obecnie, integrując je z naszą otwartą platformą. Sophos XDR obejmuje gotowe integracje z rozbudowanym ekosystemem zewnętrznych narzędzi do ochrony punktów końcowych, zapór sieciowych, sieci, poczty elektronicznej, tożsamości, tworzenia kopii zapasowych, bezpieczeństwa w chmurze i produktywności, w tym Microsoft 365.



Powyższe informacje stanowią reprezentatywny przykład integracji technologii innych niż Sophos zawartych w Sophos XDR.

Oparte na najlepszej na świecie ochronie punktów końcowych

Skup działania analityczne na właściwych incydentach, zatrzymując większą liczbę naruszeń, zanim do nich dojdzie. Większość rozwiązań XDR zmusza analityków do poświęcania cennego czasu na analizę incydentów, które powinny zostać zablokowane przez mechanizmy ochrony. Sophos łączy XDR z najsilniejszą w branży ochroną punktów końcowych, blokując zagrożenia, zanim będą wymagały ręcznej analizy — zmniejszając obciążenie zespołu.

Subskrypcje Sophos XDR obejmują Sophos Endpoint, zapewniając zaawansowaną ochronę przed ransomware i exploitami, ochronę przed złośliwym oprogramowaniem opartą na AI oraz adaptacyjne mechanizmy obronne, które dynamicznie zwiększają poziom ochrony w odpowiedzi na aktywny atak.

Więcej informacji można znaleźć na stronie sophos.com/endpoint

Wykrywanie i reagowanie jako w pełni zarządzana usługa

Możesz samodzielnie wykrywać i badać zagrożenia za pomocą Sophos XDR lub odciążyć swoich pracowników, korzystając z kompleksowej usługi zarządzanej dostępnej 24/7. Dzięki Sophos Managed Detection and Response (MDR) nasz doświadczony zespół analityków może zapewnić Ci natychmiastowy dostęp do centrum operacji bezpieczeństwa, obejmującego pełne możliwości reagowania na incydenty.

Więcej informacji można znaleźć na stronie sophos.com/mdr

W zestawie z subskrypcjami Sophos XDR

	Sophos XDR
Oceny zagrożeń generowane przez sztuczną inteligencję i wykrywania z priorytetami	✓
Zarządzanie sprawami, współpraca i działania reagujące	✓
Zaawansowane narzędzia wyszukiwania w języku naturalnym do wykrywania i badania zagrożeń	✓
Funkcje XDR oparte na sztucznej inteligencji: Asystent AI, podsumowanie sprawy AI, analiza poleceń AI, wyszukiwanie AI	✓
W zestawie Sophos Endpoint (lub możliwość korzystania z istniejącego rozwiązania innego niż Sophos)	✓
Dane wykrywania przechowywane w jeziorze danych Sophos (standardowo przez 90 dni)	✓
Dostępna roczna retencja danych	Opcjonalny dodatek
Natywna integracja z rozwiązaniami Sophos: Sophos Endpoint, Sophos Mobile, Sophos Firewall, Sophos ZTNA, Sophos Email, Sophos Cloud Optix	✓
Integracja z rozwiązaniami innymi niż Sophos w zakresie punktów końcowych, zapór sieciowych, sieci, poczty elektronicznej, chmury, tożsamości, kopii zapasowych, Microsoft 365 i Google Workspace	✓
Sophos Network Detection and Response (NDR)	Opcjonalny dodatek
Sophos Identity Threat Detection and Response (ITDR)	Opcjonalny dodatek

Dowiedz się, dlaczego klienci wybierają Sophos XDR

Sophos jest uznanym liderem w dziedzinie rozszerzonego wykrywania i reagowania, co potwierdza uznanie branży.

Gartner

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

Gartner Peer Insights Customers' Choice 2025

„Wybór klientów" w raporcie Gartner® Voice of the Customer 2025 w kategorii rozszerzonego wykrywania i reagowania.

Lider

Lider w raporcie G2 Spring 2025 Overall Grid® dotyczącym rozszerzonego wykrywania i reagowania.

MITRE | ATT&CK® Evaluations

Sophos XDR osiąga bardzo dobre wyniki w testach MITRE ATT&CK dla produktów dla przedsiębiorstw.

SE Labs

Sophos konsekwentnie osiąga najlepsze w branży wyniki w zakresie ochrony w niezależnych testach bezpieczeństwa przeprowadzanych przez SE Labs.

1 Raport Sophos dotyczący stanu oprogramowania ransomware w 2025 r.
2 Raport Sophos dotyczący aktywnych przeciwników 2025
3 Raport Sophos — Jak radzić sobie z wypaleniem zawodowym w cyberbezpieczeństwie w 2025 r.

Wypróbuj teraz za darmo

Zarejestruj się, aby uzyskać bezpłatną 30-dniową wersję próbną na stronie sophos.com/xdr

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

2025-09-15 DS-EN (NP)

SOPHOS