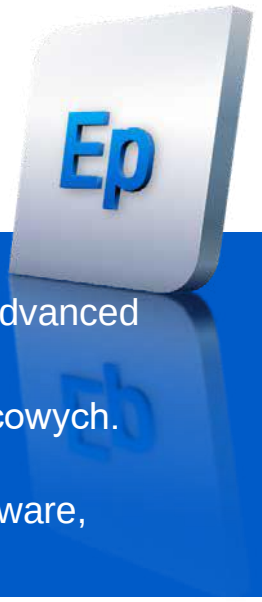
Intercept X



Intercept X Advanced, Intercept X Advanced z EDR, Intercept X Advanced z XDR, Intercept X Advanced z MTR

Sophos Intercept X to najlepsza na świecie ochrona punktów końcowych. Powstrzymuje najnowsze zagrożenia cyberbezpieczeństwa dzięki połączeniu uczenia głębokiego AI, ochrony przed atakami ransomware, zapobieganiu wykorzystaniu exploitów i innych technik.

Sophos Intercept X stosuje kompleksowe, dogłębne podejście do ochrony punktów końcowych, zamiast polegać na jednej, podstawowej technice zapewniania bezpieczeństwa. To wielowarstwowe rozwiązanie łączy techniki nowoczesne i tradycyjne, aby powstrzymać jak najszerszy zakres zagrożeń.

Blokowanie nieznanych zagrożeń

Techniki uczenia głębokiego AI w Intercept X pozwalają wykryć i zablokować złośliwe oprogramowanie, nawet jeśli wcześniej nie było ono znane. W tym celu AI analizuje atrybuty plików pochodzące z setek milionów próbek, co umożliwia zidentyfikowanie zagrożenia bez konieczności posiadania sygnatur.

Blokowanie ataków Ransomware

Intercept X posiada zaawansowane funkcje ochrony przed atakami ransomware, które wykrywają i blokują złośliwe szyfrowanie wykorzystywane w tych atakach. Pliki, które zostały zaszyfrowane, zostaną zabezpieczone i przywrócone do poprzedniego stanu, co minimalizuje wpływ ataku na działanie firmy.

Zapobieganie wykorzystaniu exploitów

Technologia ochrony przed wykorzystaniem exploitów pozwala zablokować metody wykorzystywane przez cyberprzestępców do złamania zabezpieczeń urządzeń, kradzieży danych uwierzytelniających i rozsyłania złośliwego oprogramowania. Blokując techniki używane w całym łańcuchu ataków, Intercept X chroni każdą firmę przed atakami typu fileless i zero-day.

Wielowarstwowa ochrona

Oprócz potężnych, nowoczesnych funkcjonalności, Intercept X wykorzystuje również sprawdzone podejście tradycyjne. Przykładowe funkcje obejmują blokowanie aplikacji, kontrolę sieci, zapobieganie utracie danych i wykrywanie złośliwego oprogramowania na podstawie sygnatur. Połączenie nowoczesnych i tradycyjnych technik zmniejsza możliwość ataku i zapewnia najlepszą ochronę na wielu poziomach.

Synchronizacja funkcji zapewniania bezpieczeństwa

Rozwiązania Sophos doskonale ze sobą współpracują. Na przykład Intercept X i Sophos Firewall udostępniają sobie dane, co pozwala automatycznie odizolować zainfekowane urządzenia, a następnie przywrócić dostęp do sieci po zneutralizowaniu zagrożenia. Wszystko bez potrzeby interwencji administratora.

Najważniejsze funkcje

- Pozwala zablokować nieznane dotąd zagrożenia dzięki technikom uczenia głębokiego AI
- Blokuje ataki ransomware i przywraca bezpieczeństwo zaatakowanych plików
- Zapobiega wykorzystaniu exploitów w całym łańcuchu ataków
- Reaguje na krytyczne operacje IT i pytania związane z wykrywaniem zagrożeń za pomocą EDR
- Zapewnia bezpieczeństwo 24/7/365, jako w pełni zarządzalną usługę
- Analizuje i wykorzystuje firewall, e-mail i inne źródła danych* dzięki XDR

Rozwiązanie łatwe do wdrożenia, konfiguracji i utrzymania nawet w zdalnych środowiskach pracy

**Cloud Optix i Sophos Mobile będą dostępne już wkrótce*

SOPHOS

Wykrywanie i reagowanie w punktach końcowych - *Endpoint Detection and Response* (EDR)

Zaprojektowany dla administratorów IT i specjalistów ds. cyberbezpieczeństwa Sophos EDR jest odpowiedzią na potrzeby związane z krytycznymi operacjami IT i wykrywaniem zagrożeń. Pozwala, na przykład, zidentyfikować urządzenia mające problemy z wydajnością lub podejrzane procesy próbujące nawiązać połączenie z niestandardowymi portami, a następnie umożliwia zdalny dostęp do urządzenia w celu podjęcia działań naprawczych.

Zarządzalne reagowanie na zagrożenia - *Managed Threat Response* (MTR)

Dostępna 24/7/365 usługa wykrywania i reagowania na zagrożenia świadczona przez zespół ekspertów Sophos. Analitycy Sophos reagują na potencjalne zagrożenia, szukają wektorów ataku (*indicators of compromise*) i udostępniają szczegółową analizę zdarzeń, w tym tego, co się wydarzyło, gdzie, kiedy i dlaczego.

** Integracja Sophos Cloud Optix i Sophos Mobile XDR będzie dostępna wkrótce*

Rozszerzone wykrywanie i reagowanie - *Extended Detection and Response* (XDR)

Wykorzystanie firewalla, poczty e-mail i innych źródeł danych*, pozwala spojrzeć szerzej, niż tylko na same punkty końcowe i serwery. Uzyskuje się w ten sposób ogólny wgląd w stan cyberbezpieczeństwa firmy oraz możliwość zagłębiania się w nawet najdrobniejsze zagadnienia. Podejście to pozwala, na przykład, wykryć problemy związane z działaniem biurowej sieci i stwierdzić, jaka aplikacja je powoduje.

Proste zarządzanie

Intercept X jest zarządzany z poziomu Sophos Central, platformy do zarządzania w chmurze dla wszystkich rozwiązań Sophos. To jedna konsola dla wszystkich urządzeń i produktów, ułatwiająca wdrażanie, konfigurowanie i zarządzanie środowiskiem nawet w przypadku rozwiązań zdalnych.

Specyfikacje techniczne

Intercept X obsługuje wdrożenia w systemach Windows i macOS. Informacje dotyczące tych zagadnień podane zostały w Wymaganiach systemowych Windows oraz Arkuszu danych dla komputerów Mac.

Licencje

Funkcje	Intercept X Advanced	Intercept X Advanced z EDR	Intercept X Advanced z XDR	Intercept X Advanced z MTR Standard	Intercept X Advanced z MTR Advanced
Ochrona podstawowa (w tym kontrola aplikacji, wykrywanie zachowań i nie tylko)	✓	✓	✓	✓	✓
Ochrona nowej generacji (w tym techniki głębokiego uczenia, ochrona przed atakami ransomware, ochrona przed atakami fileless i nie tylko)	✓	✓	✓	✓	✓
EDR (*Endpoint detection and response* - wykrywanie i reagowanie w punktach końcowych)		✓	✓	✓	✓
XDR (*Extended detection and response* - rozszerzone wykrywanie i reagowanie)			✓		Patrz komentarz*
Managed Threat Response (Zarządzalne reagowanie na zagrożenia - MTR – usługa wykrywania i reagowania na zagrożenia 24/7/365)				✓	✓
MTR Advanced (wykrywanie, dedykowany kontakt i nie tylko)					✓

* Uwaga: zespół MTR będzie miał możliwość wykorzystania danych i funkcji XDR w przypadku klientów MTR Advanced. Jednak klienci MTR będą ograniczeni do funkcji EDR konsoli Sophos Central, chyba że wybiorą licencję XDR

Wypróbuj teraz, za darmo

Zarejestruj się na stronie sophos.com/intercept-x i skorzystaj z bezpłatnego, 30-dniowego okresu testowego

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

Sprzedaż na terenie Ameryki Północnej
Bezpłatny numer: 1-866-866-2802
E-mail: nasales@sophos.com

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

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

21-04-26 DS-EN (PS)