kaspersky AKTYWUJ PRZYSZŁOŚĆ

Kaspersky Endpoint Security for Business

Select

Rozwiązanie Kaspersky Endpoint Security for Business Select to wykorzystująca technologię HuMachine™ ochrona szerokiego wachlarza platform – w tym serwerów i punktów końcowych opartych na Linuksie. Wielowarstwowa ochrona wykrywa podejrzane zachowanie i blokuje zagrożenia, łącznie z ransomware. Wykorzystujące chmurę narzędzia kontroli zmniejszają ekspozycję na ataki, a funkcje zarządzania urządzeniami mobilnymi pomagają chronić znajdujące się na nich dane.

Poziom ochrony i zarządzania, jakiego potrzebujesz

We wszystkich warstwach naszych produktów zastosowaliśmy wszechstronne funkcje klasy korporacyjnej. Zadbaliśmy o to, aby korzystanie z tych technologii było łatwe i elastyczne dla wszystkich firm, bez względu na ich rozmiar.

Ochrona wielowarstwowa dla:
- systemu Windows, Linux oraz macOS,
- serwerów Windows i Linux,
- kontenerów Windows Server,
- urządzeń mobilnych,
- pamięci przenośnych.

Najlepsza ochrona przed:
- exploitami dla oprogramowania,
- ransomware,
- mobilnymi szkodliwymi programami,
- zaawansowanymi zagrożeniami,
- zagrożeniami bezplikowymi,
- atakami wykorzystującymi skrypty i PowerShell,
- zagrożeniami pochodzącymi z internetu.

Dostępne funkcje:
- Ochrona przed szkodliwym oprogramowaniem
- Zarządzanie lukami
- Doradca ds. polityki bezpieczeństwa
- Izolacja procesów
- Ochrona przed exploitami i cofanie zmian
- Zarządzanie zaporą sieciową i zaporą sieciową systemu operacyjnego
- Ochrona wykorzystująca chmurę
- Pełna integracja z Kaspersky EDR Optimum NOWOŚĆ
- Pełna integracja z Kaspersky Sandbox NOWOŚĆ
- Integracja z systemami SIEM za pośrednictwem Syslog
- Kontrola aplikacji
- Kontrola sieci i urządzeń
- Ochrona dla serwerów i kontenerów
- Zdalne wymazywanie danych NOWOŚĆ
- Ochrona przed zagrożeniami mobilnymi
- Generowanie raportów
- Konsola chmurowa NOWOŚĆ
- Konsola wykorzystująca sieć i MMC

Szczegółowe informacje znajdują się na naszych stronach.

Zaawansowana ochrona i kontrola

Elastyczna ochrona adaptacyjna

Rozwiązanie Kaspersky Endpoint Security for Business Select powstało z myślą o zabezpieczaniu dowolnego środowiska IT. Szeroki wachlarz innowacyjnych technologii o udowodnionej skuteczności chroni nawet przed zaawansowanymi i nieznanymi zagrożeniami, zmniejszając poziom narażenia na nie i zabezpieczając przed nimi organizację, dane i użytkowników.

Prosta integracja z nowymi rozwiązaniami Kaspersky EDR Optimum i Kaspersky Sandbox ułatwia rozszerzanie ochrony o automatyczne wykrywanie i reagowanie.

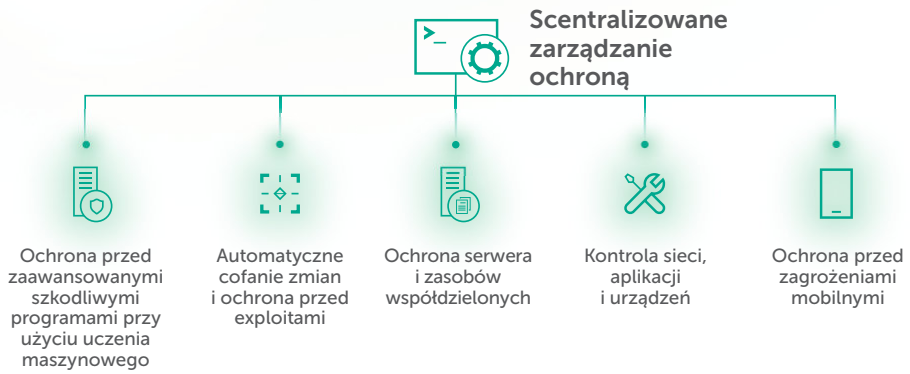
Jedna konsola zarządzania to najlepsze połączenie dwóch światów

Wolisz rozwiązanie w postaci usługi w chmurze, wdrożenia lokalnego czy obie wersje? W każdym przypadku nasza firma oferuje ujednolicone zarządzanie za pośrednictwem konsoli w chmurze lub tradycyjnej konsoli lokalnej, w środowiskach chmurowych AWS lub Azure.

Bez względu na to, którą opcję wybierzesz, nasza prosta w użyciu konsola umożliwia szybkie i bezproblemowe wdrożenie polityk wybranej ochrony na każdym punkcie końcowym, a także upraszcza funkcje zarządzania takie jak wdrożenie systemu operacyjnego i oprogramowania oraz udostępnianie licencji.

Najczęściej testowana, najczęściej nagradzana ochrona

Rok po roku nasze produkty wykazują najlepsze wyniki w niezależnych testach i raportach. Jesteśmy dumni z tych niesamowitych wyników, dzięki którym cieszymy się uznaniem w całej branży. Ponadto ogromnie cieszy nas to, że nasi Klienci niezmiennie wyrażają swoje zadowolenie w kwestii wydajności i skuteczności naszych produktów.



Informacje o rozwiązaniu EDR Optimum NOWOŚĆ
(do kupienia oddzielnie)

Możliwości oferowane przez technologię EDR są już dostępne w rozwiązaniu Kaspersky Endpoint Security for Business i można je rozszerzyć za pomocą nowego rozwiązania Kaspersky EDR Optimum. W efekcie otrzymujesz pełną widoczność oraz możliwość przeprowadzania analiz dotyczących podstawowych przyczyn w celu uzyskania dokładnych informacji na temat stanu firmowej ochrony przed zaawansowanymi zagrożeniami. Specjalista ds. ochrony IT w Twojej firmie otrzymuje informacje i obraz sytuacji potrzebne do skutecznej analizy oraz szybkiej i stosownej reakcji na incydenty, zanim wystąpi jakakolwiek szkoda, jak również podstawowe możliwości rozpoznawania zagrożeń (skanowanie w poszukiwaniu oznak włamania).

Informacje o rozwiązaniu Kaspersky Sandbox NOWOŚĆ
(do kupienia oddzielnie)

Kaspersky Sandbox automatycznie chroni przed zaawansowanymi zagrożeniami, których zadaniem jest omijanie ochrony na punkcie końcowym. W oparciu o technologię dynamicznej emulacji zagrożeń rozwiązanie Kaspersky Sandbox używa naszych najlepszych praktyk w zwalczaniu kompleksowych zagrożeń i ataków na poziomie APT, zapewniając zautomatyzowane reagowanie na wszystkich punktach końcowych.

Kluczowe funkcje

Ochrona najważniejszych obszarów

Nasze komponenty ochrony przed zagrożeniami tworzą filar skutecznej ochrony przed powszechnymi zagrożeniami. Należą do nich: **Ochrona plików, poczty i sieci, Zapora sieciowa, Ochrona przed zagrożeniami z internetu, Ochrona przed atakami typu BadUSB** oraz **AMSI Protection Provider**.

Zaawansowana ochrona przed zagrożeniami wykorzystująca uczenie maszynowe

Zaawansowane komponenty ochrony, takie jak **HIPS, Kaspersky Security Network, Wykrywanie zachowań**, Ochrona przed ransomware czy Ochrona przed exploitami, potrafią wykrywać i blokować nawet nowe i nieznane zagrożenia. Wspierana zarówno statycznym, jak i dynamicznym uczeniem maszynowym funkcja Wykrywanie zachowań analizuje aktywność procesów w czasie rzeczywistym w celu wykrywania najbardziej wyrafinowanych zagrożeń, takich jak bezplikowe szkodliwe programy czy ataki wykorzystujące skrypty. Po zidentyfikowaniu i oflagowaniu szkodliwego procesu jego aktywność zostaje wstrzymana, a Silnik korygujący wycofuje wszelkie dokonane zmiany.

Chmurowe narzędzia kontroli pomagające we wzmacnianiu polityk i zapobieganiu włamaniom

System **Host Intrusion Prevention** oraz scentralizowane narzędzia do **kontroli sieci, urządzeń i aplikacji** zmniejszają powierzchnię narażenia na atak oraz pomagają w zachowaniu bezpieczeństwa i produktywności użytkowników. Firma Kaspersky ma własne laboratorium Dynamicznego tworzenia białych list, w którym przechowywane są nieustannie monitorowane i aktualizowane bazy danych zawierające ponad 2,5 miliarda zaufanych programów.

Elastyczne i kompleksowe zarządzanie

Kaspersky Security Center to konsola zarządzania scentralizowanego, która ułatwia administratorom konfigurowanie wdrożenia ochrony, a także aktualizowanie i zarządzanie nią. Rozwiązanie to upraszcza stosowanie zadań grupowych, polityk i ich profili, jak również generowanie raportów. Dostępne są trzy opcje zarządzania:

- Konsola Kaspersky Security Center MMC
- Konsola sieciowa Kaspersky Security Center
- Konsola chmurowa Kaspersky Security Center NOWOŚĆ

Dla systemów Windows, Mac i Linux

Do zarządzania ochroną dla punktów końcowych i serwerów z systemem Windows i Linux, a także dla stacji roboczych Mac, służy ta sama konsola, a takie podejście idealnie nadaje się do środowisk mieszanych.

Zarządzanie i ochrona urządzeń mobilnych

Wszechstronna ochrona przed szkodliwymi programami wraz z wykorzystującą chmurę analizą zagrożeń, kontrolą sieci i ochroną przed phishingiem, oferująca możliwość zarządzania urządzeniami mobilnymi i integracji z systemami EMM.

Integracja umożliwiająca zaawansowany poziom zapobiegania, wykrywania i reagowania NOWOŚĆ

Rozwiązanie Kaspersky Endpoint Security for Windows powstało z myślą o integracji z produktami **Kaspersky Sandbox** i **Kaspersky EDR Optimum** w celu zaawansowanego i automatycznego wykrywania i reagowania.

Informacje o cyberzagrożeniach: securelist.pl
Informacje ze świata bezpieczeństwa IT: kaspersky.pl/blog
Ochrona IT dla MŚP: kaspersky.pl/biznes
Ochrona IT dla korporacji: kaspersky.pl/korporacje

www.kaspersky.pl

Jesteśmy skuteczni. Jesteśmy niezależni. Jesteśmy transparentni. Zobowiązaliśmy się do budowania bezpieczniejszego świata, w którym technologia czyni nasze życie lepszym. Dlatego go chronimy, aby każda osoba wszędzie mogła korzystać z jego nieskończonych możliwości. Aktywuj cyberbezpieczeństwo dla lepszego jutra.

Dowiedz się więcej na stronie kaspersky.pl/future

Sprawdzony.
Transparentny.
Niezależny.