kaspersky AKTYWUJ PRZYSZŁOŚĆ

Gotowy na RODO

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

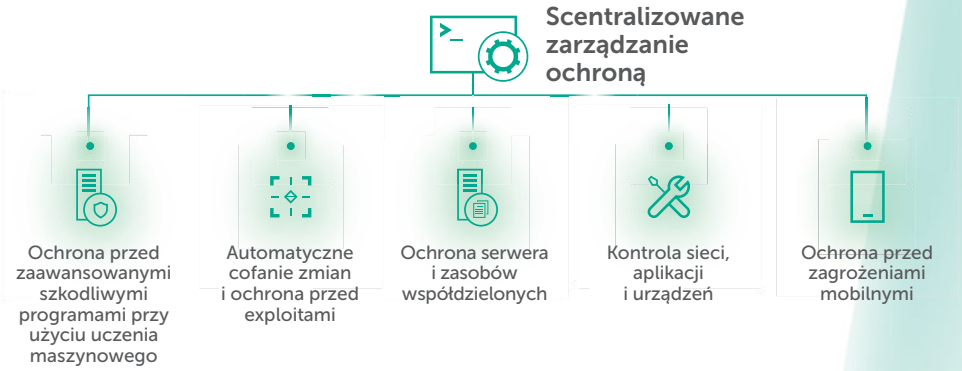
We wszystkich warstwach naszych produktów zastosowaliśmy wszechstronne funkcje klasy korporacyjnej. Zadbaliśmy o to, aby korzystanie z tych technologii było łatwe i elastyczne dla wszystkich firm, bez względu na ich rozmiar.

Który produkt jest najlepszy dla Ciebie?
- **SELECT**
- ADVANCED
- TOTAL

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 Ulepszono
- Zarządzanie lukami
- Doradca ds. polityki bezpieczeństwa
- Uczenie wykorzystujące sztuczną inteligencję
- Obsługa AMSI Nowość
- Skanowanie ruchu szyfrowanego Nowość
- Izolacja procesów
- Ochrona przed exploitami i cofanie zmian
- Zarządzanie zaporą sieciową i zaporą sieciową systemu operacyjnego
- Ochrona wykorzystująca chmurę
- Zintegrowany agent EDR
- Integracja z systemami SIEM za pośrednictwem Syslog Nowość
- Kontrola aplikacji
- Kontrola sieci i urządzeń
- Ochrona dla serwerów i kontenerów Ulepszono
- Obsługa podsystemu Windows w systemie Linux Nowość
- Ochrona przed zagrożeniami mobilnymi Ulepszono
- Generowanie raportów



Ochrona nowej generacji i narzędzia kontroli dla każdego puntu końcowego

Jedna konsola zarządzania

Dzięki jednej konsoli zarządzania administratorzy widzą cały krajobraz ochrony i mogą nią zarządzać, a na każdym punkcie końcowym w firmie mogą stosować inną politykę zabezpieczającą. Pomaga to sprawnie dostosowywać ochronę i wymaga jedynie minimalnej przerwy w działaniu, a dodatkowo dostępnych jest wiele wstępnie skonfigurowanych scenariuszy.

Elastyczna ochrona

Produkt może działać w każdym środowisku IT i stosuje wszystkie technologie nowej generacji o udowodnionej skuteczności. Wbudowane sensory i integracja z produktem Endpoint Detection and Response (EDR) umożliwia przechwytywanie i analizę dużych ilości danych w celu wykrywania nawet najbardziej zamaskowanych, wyrafinowanych cyberataków.

Satysfakcja klienta gwarantowana

Dzięki dużym nakładom na badania i rozwój nasze produkty zapewniają ochronę, jakiej potrzebujesz. Osoby decyzyjne w firmach konsekwentnie wskazują, że są zadowolone z efektów korzystania z naszych produktów, co regularnie potwierdzają niezależne badania i raporty.

Szczegółowe informacje znajdują się na naszych stronach.

Kluczowe funkcje

Kluczowe funkcje

Ochrona przed exploitami
Blokuje szkodliwym programom możliwość uruchamiania się i wykorzystywania oprogramowania, zapewniając dodatkową warstwę ochrony przed nieznanymi zagrożeniami dnia zerowego.

Wykrywanie niebezpiecznego zachowania i automatyczne wycofywanie zmian
Identyfikuje i chroni przed zaawansowanymi zagrożeniami, w tym ransomware, atakami bezplikowymi i przechwytywaniem kont administratorów. Moduł Wykrywanie zachowań blokuje ataki, a Automatyczne wycofywanie zmian unieważnia wszelkie dokonane zmiany.

Ochrona przed szyfrowaniem dla folderów współdzielonych
Unikatowy mechanizm potrafi blokować próby szyfrowania plików znajdujących się w zasobach współdzielonych, podejmowane przez szkodliwy proces działający na innym sprzęcie w tej samej sieci.

Ochrona przed zagrożeniami pochodzącymi z internetu
Szkodliwe programy mogą wywoływać przepełnienia bufora, aby modyfikować proces, który już działa w pamięci, i uruchamiać szkodliwy kod. Moduł Ochrony przed zagrożeniami sieciowymi identyfikuje i blokuje ataki pochodzące z internetu.

Konsola internetowa
Aby zwiększyć tolerancję błędów, możesz zainstalować naszą konsolę sieciową umożliwiającą zarządzanie centralne zarówno fizycznymi, jak i wirtualnymi maszynami znajdującymi się w środowiskach chmury Amazon i Microsoft Azure.

Funkcje ochrony mobilnej

Innowacyjne technologie chroniące przed szkodliwymi programami
Połączenie opartego na uczeniu maszynowym, proaktywnego i wykorzystującego chmurę wykrywania zapewnia ochronę w czasie rzeczywistym, którą zwiększa bezpieczna przeglądarka, skanowanie na żądanie lub zgodnie z harmonogramem.

Instalacja bez połączenia przewodowego (Over the Air, OTA)
Funkcja ta umożliwia wstępne skonfigurowanie i instalację aplikacji z jednego miejsca przy użyciu wiadomości SMS, e-mail czy komputera PC.

Narzędzia zdalne do ochrony przed kradzieżą
Funkcja SIM Watch, zdalne blokowanie, usuwanie i odnajdywanie zapobiegają uzyskiwaniu nieautoryzowanego dostępu do danych firmowych, gdy urządzenie mobilne zostanie zgubione lub skradzione.

Kontrola aplikacji dla urządzeń mobilnych
Moduł Kontrola aplikacji gromadzi dane na temat zainstalowanych programów i umożliwia administratorom wymuszenie instalacji określonych aplikacji czy korzystanie z nich.

Narzędzia do kontroli punktów końcowych wykorzystujące chmurę

Kontrola aplikacji
Zmniejsza ryzyko ataku, dając całkowitą kontrolę nad tym, jakie oprogramowanie może być uruchamiane na komputerach PC, przy wsparciu ze strony technologii Dynamiczne tworzenie białych list tworzonej w wewnętrznym laboratorium Kaspersky. Dostępne scenariusze obejmują tryb domyślnej akceptacji i domyślnej odmowy.

Dynamiczne tworzenie białych list
Aby lepiej kategoryzować oprogramowanie, moduł Kontrola aplikacji może korzystać z dynamicznie tworzonej białej listy, generowanej przez Kaspersky na drodze gromadzenia informacji o legalnym oprogramowaniu.

Kontrola urządzeń
Umożliwia konfigurację, planowanie i wymuszanie stosowania polityk obejmujących dane, regulujących pamięci przenośne i inne urządzenia peryferyjne podłączane do dowolnego złącza (np. USB).

Zapobieganie włamaniom (HIPS)
Reguluje dostęp do wrażliwych danych i urządzeń nagrywających obraz oraz dźwięk przy wykorzystaniu lokalnych i chmurowych baz danych zawierających informacje na temat reputacji (Kaspersky Security Network), nie wpływając przy tym na szybkość działania autoryzowanych aplikacji.

Serwis i pomoc techniczna

W 34 biurach zlokalizowanych w ponad 200 krajach na całym świecie pracownicy pomocy technicznej Kaspersky pomagają klientom w pełni wykorzystać możliwości ochrony. W Polsce pomoc jest dostępna, działa 24 godziny na dobę i 7 dni w tygodniu.

Przekonaj się

Sprawdź, na czym polega prawdziwe cyberbezpieczeństwo! Aby skorzystać z 30-dniowej wersji testowej produktu Kaspersky Endpoint Security for Business, wejdź na tę stronę.

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.