

# ► KASPERSKY ENDPOINT SECURITY FOR BUSINESS Warstwa 3: Advanced

Szyfrowanie, Konfiguracja systemów, Ochrona mobilna i Kontrola punktów końcowych.

Warstwa 'Advanced' tworzy platformę ochrony i zarządzania, jakiej Twoja firma potrzebuje do wdrożenia polityki bezpieczeństwa IT, oraz chroni użytkowników przed szkodliwym oprogramowaniem i przypadkową utratą danych z powodu kradzieży lub zagubienia urządzeń.

## Możliwości ochrony i zarządzania, jakich potrzebujesz.

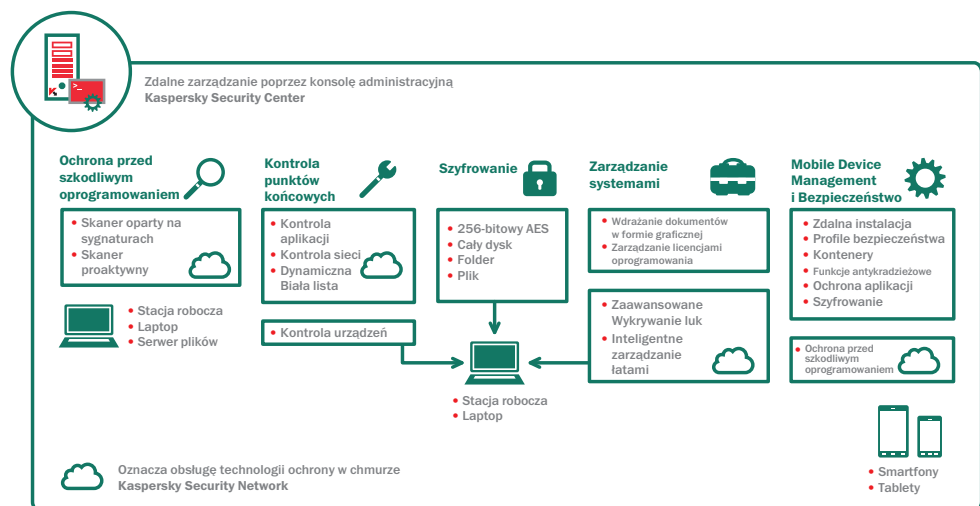
Firma Kaspersky Lab wbudowała potężne funkcje klasy enterprise w cztery progresywne poziomy produktów. Dzięki temu nasza oferta jest nieskomplikowana i przystępna dla każdego rodzaju przedsiębiorstwa.

## Która warstwa jest odpowiednia dla Ciebie?

- CORE
- SELECT
- **ADVANCED**
- TOTAL

### Dostępne funkcje:

- Ochrona przed szkodliwym oprogramowaniem
- Zapora sieciowa
- Ochrona wspomagana przez usługę chmury Kaspersky Security Network
- Kontrola aplikacji
- Biała lista aplikacji
- Kontrola sieci
- Kontrola urządzeń
- Wykrywanie luk
- Ochrona serwerów plików
- Mobile Device Management – zarządzanie urządzeniami mobilnymi
- Mobile Endpoint Security – ochrona mobilnych punktów końcowych (dla tableków i smartfonów)
- Szyfrowanie
- Wdrażanie i konfiguracja systemów
- Zaawansowane Wykrywanie luk
- Zarządzanie łatami



## ► Nasze rozwiązanie to nie podzielony „pakiet”, ale jedyna prawdziwa platforma bezpieczeństwa w branży.

### Jedna Konsola zarządzająca

Z poziomu jednego panelu administrator może przeglądać i zarządzać całym obszarem ochrony — maszynami wirtualnymi, a także urządzeniami fizycznymi i mobilnymi.

### Jedna Platforma bezpieczeństwa

Firma Kaspersky Lab sama opracowała konsolę, moduły ochrony i wewnętrzne narzędzia – nie kupiliśmy tych technologii od innych firm. Oznacza to, że ci sami programiści, pracujący z tą samą bazą kodu, stworzyli technologie, które idealnie współpracują ze sobą. Wynikiem tego jest stabilność, zintegrowane profile, przydatne funkcje raportowania oraz intuicyjne narzędzia.

### Jeden koszt

Wszystkie narzędzia pochodzą od jednego producenta i są dostarczane podczas jednej instalacji — nie musisz więc przechodzić przez nowy proces sporządzania budżetu, aby bezpieczeństwo postawić na równi z celami biznesowymi.

## Szyfrowanie i ochrona danych:

### Szyfrowanie dysku twardego – 256-bitowy AES

Umożliwia wybranie pliku folderu lub całego dysku w celu zabezpieczenia krytycznych informacji firmowych w przypadku kradzieży urządzenia.

### Szyfrowanie urządzenia przenośnego

Zwiększa bezpieczeństwo poprzez profile, które wymuszają szyfrowanie danych na urządzeniach przenośnych.

### Ochrona danych, które znajdują się w ruchu

Oznacza, że użytkownicy mogą łatwo tworzyć zaszyfrowane i samorozpakowujące się pakiety w celu zapewnienia ochrony danych podczas współdzielenia z użyciem urządzeń mobilnych, wiadomości e-mail, sieci firmową lub internetu.

### Technologia niewidoczna dla użytkowników

Rozwiązanie szyfrowania Kaspersky Lab jest niewidoczne dla użytkowników i nie ma negatywnego wpływu na efektywność pracy.

## Kontrola punktów końcowych:

### Kontrola aplikacji

Umożliwia administratorom IT definiowanie polityk zezwalających, blokujących lub regulujących aktywność aplikacji (lub kategorii aplikacji).

### Kontrola sieci

System kontroli śledzi działania użytkownika – niezależnie od tego czy znajduje się w sieci firmowej, czy poza nią.

### Kontrola urządzeń

Umożliwia użytkownikom definiowanie, planowanie i wymuszenie polityk obsługi danych dla nośników przenośnych i innych urządzeń peryferyjnych — podłączonych poprzez USB lub inny typ magistrali.

### Dynamiczna Biała lista

Współczynnik reputacji plików dostarczany w czasie rzeczywistym przez Kaspersky Security Network zapewnia, że zatwierdzone przez Ciebie aplikacje nie zawierają szkodliwych programów, a także pomagają zmaksymalizować produktywność.

## Ochrona antywirusowa punktów końcowych:

### Częste aktualizacje i ochrona oparta na sygnaturach

Sprawdzająca się w branży tradycyjna metoda wykrywania zagrożeń oparta na sygnaturach.

### Ochrona w chmurze

Usługa Kaspersky Security Network (KSN) zapewnia o wiele szybszą reakcję na zagrożenia niż tradycyjne metody ochrony. Testy firm trzecich pokazują, że czas reakcji KSN wynosi zaledwie 0,02 sekundy!

## Konfiguracja systemów i zarządzanie łaćami:

### Zarządzanie łaćami

Zaawansowane szczegółowe skanowanie w poszukiwaniu luk połączone z zautomatyzowaną instalacją łać.

### Przesyłanie obrazów systemu operacyjnego i aplikacji

Łatwe tworzenie, przechowywanie i przesyłanie obrazów systemu z głównej lokalizacji. Idealne do migracji na system Microsoft® Windows® 8.

### Zdalna instalacja oprogramowania

Zdalna instalacja oprogramowania na komputerach klienckich, a nawet na tych, które znajdują się w innych oddziałach firmy.

### Narzędzia służące do rozwiązywania problemów

Zdalna łączność z systemem komputera klienckiego w celu naprawienia błędów — z poziomu tej samej konsoli administracyjnej.

### Kontrola licencji, sprzętu i oprogramowania

Raporty inwentaryzacji sprzętu i oprogramowania pomagają kontrolować zobowiązania licencjonowanie użytkowanego w firmie oprogramowania. Możesz zaoszczędzić na kosztach eliminując niewykorzystywane licencje lub przydzielając je tam, gdzie są bardziej potrzebne.

## Kaspersky Security for Mobile:

### Innowacyjne technologie ochrony przed szkodliwym oprogramowaniem

Wynikiem połączenia wykrywania opartego na sygnaturach z modułem proaktywnym i chmurą jest ochrona działająca w czasie rzeczywistym. Funkcje takie jak bezpieczna przeglądarka, ochrona przed spamem oraz bezpieczne, odizolowane środowisko (sandbox) dla aplikacji jeszcze bardziej zwiększają bezpieczeństwo.

### Technologia instalacji Over The Air (OTA)

Możliwość zdalnej prekonfiguracji i instalacji aplikacji przy pomocy SMS-a, wiadomości e-mail i komputera.

### Zdalne narzędzia modułu Anti-Theft (ochrona przed kradzieżą)

Technologie takie jak SIM-Watch, zdalne blokowanie, usuwanie i odnajdywanie eliminują możliwość uzyskania nieautoryzowanego dostępu do danych firmowych w przypadku zgubienia lub kradzieży urządzenia mobilnego.

### Kontrola aplikacji dla urządzeń mobilnych

Monitoruje aplikacje zainstalowane na urządzeniu mobilnym zgodnie z predefiniowanymi politykami grupowymi. Zawiera grupę „Aplikacje obowiązkowe”.

### Obsługa urządzeń pracowników

Aplikacje i dane firmowe są odizolowane w zaszyfrowanych kontenerach, które są niewidoczne dla użytkownika. Dane te mogą zostać usunięte oddzielnie.

**NIE WSZYSTKIE FUNKCJE SĄ DOSTĘPNE NA WSZYSTKICH PLATFORMACH.**

Więcej informacji jest dostępnych na stronie [www.kaspersky.pl](http://www.kaspersky.pl)