KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Technologia szyfrowania

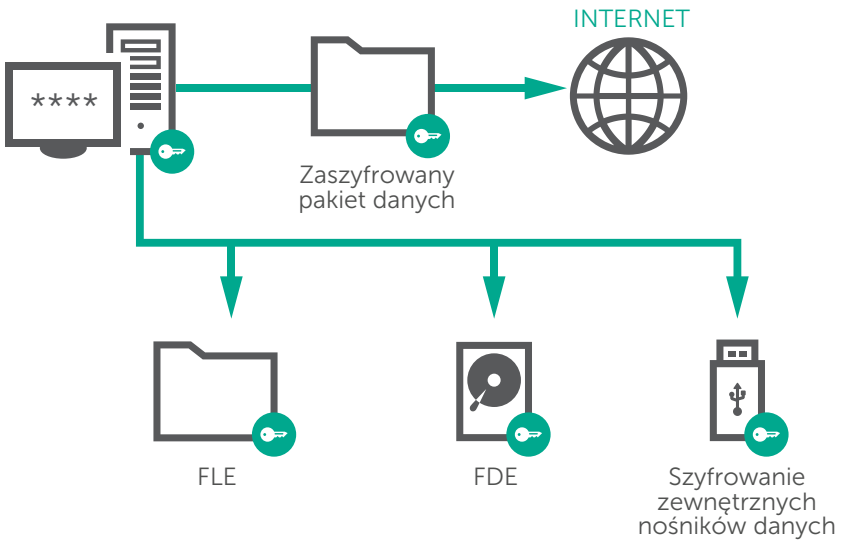
Proaktywna ochrona danych i zgodność z globalnymi oraz krajowymi wymogami bezpieczeństwa.

Technologia szyfrowania opracowana przez Kaspersky Lab chroni cenne dane firmowe przed nieautoryzowanym dostępem do danych w wyniku zgubienia i kradzieży urządzeń lub działania szpiegowskich szkodliwych programów. Dzięki integracji autorskich technologii, Kaspersky Lab oferuje możliwość zarządzania szyfrowaniem z poziomu tej samej konsoli, która jest stosowana do kontrolowania ochrony punktów końcowych w firmowej infrastrukturze IT (Kaspersky Security Center).

Rozwiązanie Kaspersky Lab pozwala na szyfrowanie:

- całych dysków (FDE)
- wybranych plików/folderów (FLE)
- zewnętrznych nośników danych

WSZYSTKO JEST ZARZĄDZANE Z POZIOMU POJEDYNCZEJ KONSOLI ADMINISTRACYJNEJ



MECHANIZMY KRYPTOGRAFICZNE ZGODNE Z RYNKOWYMI STANDARDAMI

Rozwiązanie Kaspersky Lab korzysta z algorytmu szyfrującego Advanced Encryption Standard (AES) z 256-bitwym kluczem. Obsługiwana jest technologia Intel® AES-NI oraz platformy UEFI i GPT.

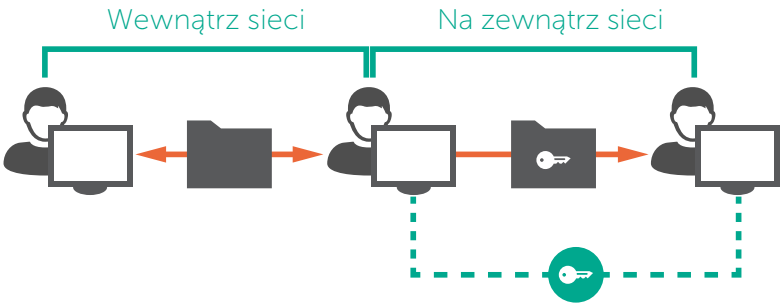
PEŁNA ELASTYCZNOŚĆ

Rozwiązanie Kaspersky Lab pozwala zarówno na szyfrowanie pełnych dysków (FDE) jak i pojedynczych plików i folderów (FLE). Chronione mogą być dane przechowywane na dyskach twardych oraz na nośnikach zewnętrznych. Specjalny 'tryb przenośny' pozwala na korzystanie z danych oraz przenoszenie nowych informacji na zaszyfrowany nośnik zewnętrzny (np. pendrive), nawet gdy na danym komputerze nie zainstalowano rozwiązania szyfrowania. Daje to możliwość bezpiecznego korzystania z danych firmowych nawet na komputerach znajdujących się poza infrastrukturą przedsiębiorstwa.

W raporcie 'Forrester Wave Endpoint Encryption, 2015' organizacja badawcza Forrester Research Inc. oceniła Kaspersky Lab jako silnego gracza w branży rozwiązań szyfrowania punktów końcowych.

Jakość doceniona przez branżowych ekspertów.

POJEDYNCZE LOGOWANIE; PEŁNA PRZEZROCZYSTOŚĆ DLA UŻYTKOWNIKA KOŃCOWEGO



Odkonfiguracjipocodzienneużytkowanie-technologia szyfrowania Kaspersky Lab działa przezroczyście we wszystkich zastosowaniach, bez negatywnego wpływu na produktywność pracowników chronionej firmy. Mechanizm pojedynczego logowania zapewnia, że szyfrowanie działa przez cały czas.

Rozwiązanie Kaspersky Lab pozwala na bezpieczne przenoszenie danych miedzy pracownikami znajdującymi się wewnątrz i poza firmową siecią.

FUNKCJE SZYFROWANIA

PEŁNA INTEGRACJA Z TECHNOLOGIAMI BEZPIECZEŃSTWA KASPERSKY LAB

Wszystkie technologie stosowane w rozwiązaniach Kaspersky Lab są opracowywane wewnątrz firmy, dzięki czemu możliwa jest ich całkowita integracja, przy zachowaniu najwyższej wydajności oraz łatwego zarządzania. To oznacza, że ustawienia szyfrowania mogą być stosowane - w całej firmowej sieci lub na wybranych urządzeniach - z użyciem tych samych profili, które zarządzają ochroną przed szkodliwym oprogramowaniem, kontrolą urządzeń i innymi aspektami bezpieczeństwa IT. Nie ma potrzeby generowaniawyspecjalizowanychprofilianiwdrażania oddzielnych rozwiązań. Kompatybilność sprzętowa jestsprawdzanaautomatycznieprzeduruchomieniem szyfrowania. Rozwiązanie obsługuje platformy UEFI oraz GPT.

KONTROLA DOSTĘPU W OPARCIU O ROLE

Rozwiązanie pozwala na oddelegowanie zarządzania szyfrowaniem do konkretnych użytkowników, co może byćprzydatnewdużychorganizacjach,gdzieinfrastrukturą IT zarządza wieloosobowy zespół.

UWIERZYTELNIANIE PRZED STARTEM SYSTEMU (PBA)

Podanie danych uwierzytelniających jest wymagane jeszcze przed uruchomieniem systemu operacyjnego, co zapewnia dodatkową warstwę ochrony. Istnieje także możliwość zastosowania pojedynczego logowania - użytkownik podaje dane uwierzytelniające tylko raz, co daje mu dostęp do systemu operacyjnego i zaszyfrowanych danych.

UWIERZYTELNIANIE Z UŻYCIEM KART INTELIGENTNYCH I TOKENÓW

Rozwiązanie Kaspersky Lab obsługuje uwierzytelnianie dwuskładnikowe,obejmującezastosowaniepopularnych kart inteligentnych i tokenów, co eliminuje konieczność zapamiętywania dodatkowych loginów i haseł, a tym samym zwiększa komfort użytkowania.

ODZYSKANIE DANYCH W RAZIE AWARII

Administratorzy mogą odszyfrować dane na wypadek awarii sprzętu lub oprogramowania. Odzyskiwanie hasła użytkownika przebiega z użyciem prostego mechanizmu typu pytanie-odpowiedź.

OPTYMALIZACJA WDROŻENIA I MOŻLIWOŚĆ DOSTOSOWANIA USTAWIEŃ

W celu zapewnienia łatwego wdrożenia ustawienia szyfrowania zostały wstępnie skonfigurowane przez ekspertówzKasperskyLab,jednakmogązostaćdowolnie zmodyfikowane przez klienta.

Jak kupić

Technologia szyfrowania opracowana przez Kaspersky Labniejestdostępnajakoindywidualnyprodukt-wchodzi w skład warstw 'Advanced' oraz 'Total' rozwiązania Kaspersky Endpoint Security for Business. W celu dokonania zakupu lub rozszerzenia posiadanej ochrony prosimy o kontakt z działem sprzedaży Kaspersky Lab Polska: sprzedaz@kaspersky.pl.