

Link do produktu: <https://softtechnika.pl/eset-endpoint-encryption-essential-p-116.html>



ESET Endpoint Encryption Essential

Cena	78,87 zł
Dostępność	Dostępny
Czas wysyłki	24 godziny
Producent	ESET
Rodzaj licencji	ESD

Opis produktu

ESET Endpoint Encryption (dawniej DESLock+) to niezbędne w każdej firmie narzędzie, przeznaczone do szyfrowania danych, zapobiegające negatywnym skutkom wycieków danych. ESET Endpoint Encryption jest intuicyjny w obsłudze i niewidoczny dla pracowników chronionego przedsiębiorstwa. Umożliwia szyfrowanie całych powierzchni dysków (FDE) oraz zabezpieczanie tylko wybranych plików, folderów czy wiadomości e-mail.

Dlaczego warto wybrać ESET Endpoint Encryption?

NARUSZENIA DANYCH

Coraz częściej media donoszą o cyberatakach na firmy i instytucje rządowe. W tego typu sytuacjach, jeśli w zaatakowanych organizacjach nie stosowano szyfrowania danych, niemal pewnym jest, że prócz samego przełamania zabezpieczeń, doszło także do wycieku danych. Nie każda firma dostrzega niebezpieczeństwa związane z tego typu sytuacjami. Każde przedsiębiorstwo musi jednak mieć na uwadze, że posiada i przechowuje dane, które nie mogą zostać ujawnione, tj. dane osobowe, informacje dotyczące klientów czy pracowników. Wdrażając rozwiązanie szyfrujące w firmie, odczytanie danych przez nieuprawnioną osobę jest niemożliwe.

OCHRONA ZDALNYCH PRACOWNIKÓW

Praca zdalna oraz częste podróże pracowników stały się codziennością wielu współczesnych firm. Praca w biegu, w kawiarni, czy na lotnisku, zwiększa ryzyko zgubienia lub kradzieży firmowych komputerów lub nośników danych. To także wyzwanie dla firm, które zaczynają wymagać błyskawicznej możliwości odcinania pracownika zdalnego od kluczowych dla firmy danych, w sytuacji zwolnienia go z obowiązku świadczenia pracy. W przeciwieństwie do konkurencyjnych rozwiązań, ESET Endpoint Encryption pozwala zdalnie wyłączyć służbowego laptopa, blokując dostęp do firmowych danych. Wszystko to następuje w kilka sekund po nawiązaniu przez komputer połączenia z Internetem, bez konieczności zestawiania dedykowanego tunelu VPN.

WYMOGI PRAWNE

Istnieją regulacje prawne, które wymagają od firm zabezpieczania swoich danych poprzez stosowanie rozwiązań szyfrujących. Do takich regulacji należą m.in. RODO, PCI-DSS, HIPAA, SOX oraz GLBA. Warto podkreślić, że rozwiązania szyfrujące przestały być dodatkiem do antywirusa, a stały się kluczowym zabezpieczeniem firmy i jej danych.

ZARZĄDZAJ Z DOWOLNEGO MIEJSCA

Dzięki ESET Endpoint Encryption możesz zarządzać firmowymi urządzeniami z każdego miejsca na świecie, bez konieczności korzystania z VPN lub tworzenia wyjątków na firewallu. Zarządzanie jest możliwe dzięki wykorzystaniu połączenia HTTPS, realizowanego przez serwer proxy. Takie podejście eliminuje potrzebę zezwalania na ryzykowne połączenia przychodzące. Dzięki temu zarządzanie szyfrowaniem jest bezpieczne i proste dla firmy każdej wielkości. Wszystkie połączenia klienta i serwera są szyfrowane za pomocą protokołu SSL, z kolei polecenia i dane są szyfrowane za pomocą algorytmu AES lub RSA.

PRACA BEZ ZAKŁÓCEŃ Wdrożenie ESET Endpoint Encryption jest całkowicie niezauważalne dla pracowników i nie wymaga z ich strony żadnych dodatkowych działań. Nie generuje również dodatkowych kosztów po stronie działu IT i nie wiąże się z koniecznością realizacji specjalistycznych szkoleń dla pracowników.

UNIKALNY SYSTEM KLUCZY SZYFRUJĄCYCH

Korzystanie z centralnie zarządzanych, współdzielonych kluczy szyfrujących, eliminuje problem korzystania ze wspólnych haseł lub kluczy publicznych, wykorzystywanych przez inne rozwiązania szyfrujące. System, używany przez ESET Endpoint Encryption, działa na podobnych zasadach jak fizyczne klucze, służące do otwierania konkretnych zamków w domach, mieszkaniach czy samochodach. Warto podkreślić, że mechanizm współdzielonych kluczy szyfrujących, zarządzanych z poziomu konsoli zdalnego zarządzania, jest nie tylko praktyczny, ale także bezpieczny.

ZABEZPIECZENIE NOŚNIKÓW WYMIENNYCH

Kontrola i ochrona nośników wymiennych w bezpiecznym środowisku sieciowym firmy może okazać się nie lada wyzwaniem. ESET Endpoint Encryption chroni nośniki każdej wielkości, tworząc na nich szyfrowaną przestrzeń, która może być powiększana lub zmniejszana, w zależności od potrzeb. Dzięki temu dowolny nośnik służbowy może być bezpiecznie wykorzystywany bez przeszkód na terenie firmy. Z kolei urządzenia będące własnością pracowników nadal mogą być przez nich wykorzystywane w celach prywatnych, bez konieczności tworzenia dodatkowych białych list.

ZDALNE WYŁĄCZANIE URZĄDZEŃ

Coraz więcej firm posiada pracowników, realizujących swoje zadania zdalnie, poza siedzibą firmy - w domu, na lotniskach, czy też w kawiarniach. Nie dziwi zatem, że te organizacje zgłaszają potrzebę posiadania możliwości zdalnego wyłączenia i blokowania urządzenia, w razie jego zgubienia lub kradzieży. Program ESET Endpoint Encryption daje taką możliwość administratorom bez konieczności otwierania dodatkowych portów firewalla, wykorzystywania połączeń VPN i najważniejsze - bez jakiegokolwiek aktywności ze strony użytkownika. Jeśli urządzenie jest podłączone do sieci i otrzyma zdalne polecenie usunięcia kluczy szyfrujących, dostęp do systemu zostanie zablokowany.

WSPARCIE DLA RÓŻNYCH TYPÓW SZYFROWANIA

Szyfrowanie całych powierzchni dysków (FDE), plików/ folderów, nośników USB oraz wiadomości e-mail.

W PEŁNI ZWERYFIKOWANY

ESET Endpoint Encryption spełnia standard szyfrowania FIPS 140-2, wykorzystując 256-bitowy algorytm szyfrujący AES.

ALGORYTMY I STANDARDY

Wykorzystywane algorytmy: AES 256-bitowy, AES 128-bitowy, SHA 256-bitowy, SHA1 160-bitowy, RSA 1024-bitowy, Triple DES 112-bitowy, Blowfish 128-bitowy.

Produkt posiada dodatkowe opcje:

Okres licencjonowania: bezterminowa , 1 rok , 2 lata , 3 lata

Porównanie Wersji

	EEE Essential	EEE Standard	EEE Pro
Szyfrowanie całej powierzchni dysku	-	-	+
Szybka i transparentna autoryzacja w fazie pre-boot.			
Szyfrowanie dysków wymiennych	-	+	+
Szyfrowanie nośników wymiennych w oparciu o konkretne polityki tworzone w konsoli centralnego zarządzania.			
EEE Go - szyfrowanie nośników wymiennych	-	+	+
- Dostęp do zaszyfrowanych danych na stacjach bez			

zainstalowanego programu
ESET Endpoint Encryption
Essential.

Szyfrowanie plików i folderów - Dodatkowa ochrona wrażliwych danych.	+	+	+
Szyfrowanie poczty i załączników (wtyczka dla MS Outlook) - Przesyłanie zaszyfrowanych wiadomości wraz z załącznikami przy użyciu programu MS Outlook.	+	+	+
Szyfrowanie tekstu oraz schowka - Szyfrowanie tekstu całych dokumentów lub ich dowolnej części.	+	+	+
Dyski wirtualne i skompresowane archiwa - Tworzenie dodatkowo zaszyfrowanych woluminów oraz archiwów samorozpakowujących.	+	+	+
Kompatybilność z centralnym zarządzaniem - Zarządzanie zaszyfrowanymi stacjami, użytkownikami oraz kluczami szyfrującymi.	+	+	+

Pojedyncza instalacja dla wszystkich typów licencji. Uaktualnienie (upgrade) i odnowienie nie wymaga reinstalacji systemu.