Dane aktualne na dzień: 29-07-2026 12:32

Link do produktu: https://esklep.pcservice-pabianice.info/f-secure-computer-protection-protection-service-for-business-licencja-biznesowa-p-1456.html

F-Secure COMPUTER PROTECTION - Protection Service for Business (licencja biznesowa)

Dostępność	**Dostępność - 3 dni**
Czas wysyłki	**24 godziny**
Kod producenta	**Mobile Protection FfB**
Producent	**F-Secure**

Opis produktu

F-Secure COMPUTER PROTECTION - Protection Service for Business (PSB) - to kompletna usługa chmurowa do zabezpieczenia jednostek komputerowych (Windows i Mac) w firmie, zarządzana za pośrednictwem panelu administratora.

RODO:
Jednostki komputerowe z dostępem do służbowej poczty, usług lub informacji są podatne na naruszenie bezpieczeństwa danych. Na mocy ogólnego Rozporządzenia o Ochronie Danych Osobowych, od maja 2018 r. będzie to grozić karą w wysokości 20 milionów euro albo 4 proc. rocznego obrotu.

F-Secure PSB pozwala zabezpieczyć i kontrolować wszystkie jednostki komputerowe w firmie.

Licencja wykupywana jest na ilość stanowisk. Nie jest przypisywana na sztywno do jednostki komputerowej. Umożliwia to w pełni dowolne zarządzanie licencjami stanowiskowymi. (zmiana komputera nie generuje potrzeby dokupowania licencji). Wszystko jest zarządzana z pod konsoli on-line. Konsola wskazuje wszystkie podpięte jednostki komputerowe, ich stan ochrony, brakujące aktualizacje innych aplikacji klienckich zainstalowanych w systemie, bieżący update systemu itp.

Główne funkcje usługi:

Funkcja Software Updater automatyzuje zarządzanie poprawkami. Jest w pełni zintegrowana z klientami F-Secure Workstation Security.
Software Updater to krytyczny składnik zabezpieczeń. Jest to pierwsza warstwa ochrony przed złośliwą zawartością atakującą punkty końcowe i może zapobiec nawet 80% ataków, po prostu dbając o aktualność oprogramowania zabezpieczeń. Wyszukuje ona brakujące aktualizacje, tworzy na ich podstawie raport o lukach w zabezpieczeniach, a następnie pobiera i wdraża aktualizacje automatycznie albo ręcznie. Poprawki zabezpieczeń obejmują aktualizacje oprogramowania firmy Microsoft i ponad 2500 aplikacji innych firm, na przykład Flash, Java, OpenOffice czy innych programów często wykorzystywanych do przeprowadzania ataków (z powodu ich popularności i dużej liczby luk w zabezpieczeniach).

Każde naruszenie bezpieczeństwa jest sygnalizowane mailowo na koto administratora.
Funkcja DeepGuard to analiza heurystyczna i analiza działania. Jest to ostateczna i najważniejsza warstwa zabezpieczeń przed nowymi zagrożeniami — nawet takimi, które atakują wcześniej nieznane luki w zabezpieczeniach. DeepGuard obserwuje działanie aplikacji i przechwytuje potencjalnie szkodliwe działania, zanim wyrządzą szkody. Skupiając się na wzorcach szkodliwego działania, a nie na typowych charakterystykach, funkcja DeepGuard może zidentyfikować i zablokować złośliwe oprogramowanie, zanim jego próbka zostanie pobrana i zbadana. Podczas pierwszego uruchomienia nieznanego lub podejrzanego programu funkcja DeepGuard tymczasowo opóźnia jego wykonanie, aby sprawdzić reputację i częstotliwość występowania pliku, następnie uruchamia go w ograniczonym środowisku (piaskownicy), a na koniec uruchamia go w celu analizy działania i przechwytywania prób wykorzystania luk w zabezpieczeniach.

Opcjonalna funkcja Funkcja F-Secure DataGuard ma zastosowanie do wybranych folderów o wysokim ryzyku i kluczowym znaczeniu (dane osobowe, aplikacje, bazy danych, poczta itp. Funkcja chroni przed atakami typu ransomware oraz nieznanymi i złośliwymi aplikacjami, które mogą próbować zniszczyć dane lub manipulować nimi. Funkcja chroni przed zaszyfrowaniem folderów.
(***Funkcja F-Secure DataGuard jest dostępna w produkcie Computer Protection Premium***)

Usługa F-Secure Security Cloud to system analizy zagrożeń działający w chmurze. Korzysta z technologii Big Data i uczenia maszynowego oraz innych technologii, aby stale powiększać naszą bazę wiedzy o zagrożeniach cyfrowych. Usługa Security

Cloud ogólnie ujmując weryfikuje zawartość jak ma trafić z internetu na jednostkę komputerową. Za w czasu blokuje szkodliwe jej części i dopuszcza tylko te prawidłowe. Usługa blokuje niebezpieczne strony internetowe, oraz pobierane aplikacje, tak że nie trafiają one do systemu. Dzięki czemu system nie jest obciążany i działa sprawniej, bardziej wydajnie.
Ochrona przeglądania to kluczowa warstwa zabezpieczeń, która nie pozwala użytkownikom końcowym na odwiedzanie złośliwych witryn internetowych. Jest to bardzo skuteczne, ponieważ wczesna interwencja pozwala zminimalizować kontakt ze szkodliwą treścią, a więc ograniczyć ataki. Ochrona działa na poziomie sieci , nie jest zależna od używanej przeglądarki, czy programu pocztowego. Niechciana lub szkodliwa poczta jest blokowana, zanim zostanie dostarczona do aplikacji (wiadomość dochodzi, jednak np. ma poblokowane załączniki czy ukryte linki do nie pożądanych stron).

Administratorzy oczywiście mogę ustawiać wyjątki co do odwiedzanych stron i uruchamianych aplikacji.

Funkcja blokowanie ruchu internetowego (a czasami udziałów LAN) podczas obsługi banku internetowego, lub portali o wysokim priorytecie bezpieczeństwa. Charakteryzuje się to tym, iż na czas trwania sesji bankowej pozostałe zakładki są odłączone od internetu, a połączenia sieciowe nieznanych aplikacji są blokowane. Oczywiście istnieje możliwość wykluczenia stron z blokady (np. aplikacja webowa oprogramowania księgowego z którego pobieramy dane do banku)

Funkcja Device Control zapobiega przenikaniu zagrożeń do systemu za pośrednictwem takich urządzeń, jak pamięci USB, napędy CD-ROM i kamery internetowe.
W sytuacji podłączenia zabronionego urządzenia, funkcja Device Control wyłączy je, aby uniemożliwić użytkownikowi dostęp. Można definiować reguły, które zezwalają na korzystanie z konkretnych urządzeń, jednocześnie blokując wszystkie inne urządzenia tej samej klasy. Można zabronić aplikacjom dostępu do USB, napędów DVD, oraz wyłączyć automatyczne uruchamianie, przypadkowe wykonywanie lub wczytywanie modułów z nośników wymiennych. Można zezwolić na dostęp do napędów w trybie tylko do odczytu. Zablokować klasę urządzeń z wyjątkami dla konkretnych urządzeń

Funkcja Application Control,która powstrzymuje zagrożenia przed wykonywaniem i uruchamianiem skryptów, nawet jeśli ominęły one inne warstwy ochrony. Zmniejsza to ryzyka stworzone przez szkodliwe, nielegalne lub nieautoryzowane oprogramowanie w firmowym środowisku.

Zapora F-Secure wykorzystuje domyślny mechanizm Windows do realizacji reguł zapory. Znacznie zwiększa to kompatybilność z innymi aplikacjami i urządzeniami. Ekspercki zestaw reguł F-Secure, który zawiera reguły zwalczające takie zagrożenia, jak propagacja złośliwego oprogramowania i ruch boczny, jest dodawany do standardowego zestawu reguł Windows. Administrator ma możliwość definiowania tych reguł.

OBSŁUGIWANE PLATFORMY:
Windows, Mac.

Jesteśmy autoryzowanym partnerem handlowym firmy F-Secure. Od lat sami stosujemy wybrane produkty i śmiało je możemy polecać.

UWAGA!!!
Program sprzedawany tylko w wersji cyfrowej. Płatność z góry.
Po złożeniu zamówienia kontaktujemy się celem zweryfikowania wersji aplikacji, ilości szt. itp.
Zamówienie realizujemy dopiero po otrzymaniu wpłaty. (wystawiamy FV, po której opłaceniu dosyłamy klucz licencyjny)

Prosimy o wcześniejszy kontakt celem przedstawienia oferty cenowej.
Koszt licencji jest zależny od ilości stanowisk, oraz marży partnera.

Składając zapytanie cenowe prosimy podać dane firmy (nazwa, NIP).

Składając ofertę przydzielamy Państwu opiekuna.
Pierwsze zapytanie cenowe jest przypisane do dealera, opiekuna i najczęściej zawiera ono najkorzystniejszą ofertę cenową.
(kolejne zapytanie cenowe, np. u innego dealera generuje wyższe oferty cenowe, gdyż ta jest już zarezerwowana u pierwszego). Zachęcamy więc wpierw do składania zapytań cenowych w Naszej Firmie :), gdyż gwarantujemy rzetelną i sprawną obsługę wdrożeniową. Zapewniamy outsourcing IT w latach następnych.