Dane aktualne na dzień: 02-12-2022 08:20

Link do produktu: http://midinet.pl/f-secure-adv-protection-service-for-businesssss-p-15.html

F-SECURE Adv Protection Service for BusinessSSS

Cena	**145,00 zł**
Dostępność	**Dostępny**
Czas wysyłki	**24 godziny**

Opis produktu

KORZYŚCI

Software Updater
• Zautomatyzowana funkcja zarządzania poprawkami, która jest w pełni zintegrowana z klientami F-Secure Workstation Security. Nie trzeba instalować oddzielnych agentów, serwerów zarządzania czy konsol.
• 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 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).

Funkcja DeepGuard
• Łączy najbardziej zaawansowane technologie zabezpieczeń. Jest to ostateczna i najważniejsza warstwa zabezpieczeń przed nowymi zagrożeniami — nawet takimi, które atakują wcześniej nieznane luki w zabezpieczeniach.
• 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.

Usługa F-Secure Security Cloud
• System analizy zagrożeń działający w chmurze. Korzysta ona z technologii Big Data i uczenia maszynowego oraz innych technologii, aby stale powiększać bazę wiedzy o zagrożeniach cyfrowych. Usługa Security Cloud jest stale w kontakcie z systemami klientów, co pozwala na wykrywanie nowych zagrożeń, gdy tylko się pojawią, i zapewnianie ochrony w ciągu minut.
• Usługa analizy zagrożeń działająca w chmurze ma wiele zalet w porównaniu z tradycyjnymi rozwiązaniami.
Zbiera informacje o zagrożeniach z setek tysięcy węzłów obsługujących wielu klientów, dzięki czemu otrzymuje obraz globalnej sytuacji zagrożeń w czasie rzeczywistym. Ta wiedza pozwala w ciągu minut opracować rozwiązania chroniące klientów.
• Jeśli na przykład analiza heurystyczna i analiza działania funkcji DeepGuard zidentyfikują atak typu „zero-day", informacje na ten temat zostaną udostępnione wszystkim chronionym urządzeniom za pomocą usługi F-Secure Security Cloud, dzięki czemu ten zaawansowany atak stanie się nieskuteczny w ciągu minut po jego wykryciu.

Ochrona przed złośliwym oprogramowaniem
Składnik zabezpieczeń komputera korzysta z naszej platformy zabezpieczeń obejmującej wiele aparatów do wykrywania i blokowania złośliwego oprogramowania. Oferuje on znacznie lepszą ochronę niż tradycyjne technologie oparte na sygnaturach:
• Wykrywa szerszy zakres złośliwych funkcji, wzorców i trendów, co pozwala na bardziej niezawodne i dokładniejsze wykrywanie zagrożeń — nawet nieznanych wcześniej wersji złośliwego oprogramowania.
• Korzystanie z usługi F-Secure Security Cloud w czasie rzeczywistym umożliwia szybszą reakcję na nowe i powstające zagrożenia oraz zmniejsza zużycie zasobów.
• Emulacja pozwala na wykrywanie złośliwego oprogramowania, które używa technik zaciemniania i oferuje dodatkową warstwę zabezpieczeń przed uruchomieniem pliku.

Ochrona przeglądania

• 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.
• Dzięki Ochronie przeglądania użytkownicy końcowi nie zostaną na przykład nakłonieni do wejścia na pozornie nieszkodliwe witryny wyłudzające informacje, nie klikną łącza w wiadomości e-mail prowadzącego do złośliwej witryny ani nie zostaną zainfekowani przez złośliwe reklamy na niegroźnych stronach.
• Ta funkcja pobiera najnowsze wyniki sprawdzania reputacji witryn internetowych i plików z usługi F-Secure Security Cloud na podstawie różnych danych, takich jak adresy IP, słowa kluczowe w adresach URL czy zachowanie strony.
• Nie jest zależna od przeglądarki, ponieważ działa na poziomie sieci. Dzięki temu funkcja ta zapewnia ochronę nawet wtedy, gdy użytkownik końcowy nie korzysta z przeglądarki zatwierdzonej przez firmę.

Ochrona ruchu internetowego
• Zapobiega wykorzystywaniu luk w aktywnej treści, takiej jak Java czy Flash, które są używane w większości ataków internetowych. Te składniki są blokowane automatycznie na nieznanych i podejrzanych stronach na podstawie ich reputacji. Administratorzy mogą określać wyjątki, dodając witryny do listy zaufanych witryn. Jest to przydatne na przykład w przypadku stron firmowego intranetu, dla których F-Secure nie ma żadnych danych na temat reputacji.
• Skanuje ruch HTTP w czasie rzeczywistym za pomocą wielu uzupełniających się silników przeciw złośliwemu oprogramowaniu i funkcji sprawdzania reputacji. Dzięki temu złośliwe oprogramowanie i luki w zabezpieczeniach są znajdowane i blokowane na etapie ruchu sieciowego, zanim dane zostaną zapisane na dysku twardym. Zapewnia to dodatkową ochronę przed bardziej zaawansowanym złośliwym oprogramowaniem — na przykład takim, które znajduje się tylko w pamięci urządzenia.

Web Content Control
• Kontrola nad zawartością internetową pozwala ograniczyć bezproduktywne i nieodpowiednie korzystanie z Internetu. Za pomocą tej funkcji możesz ograniczyć pracownikom możliwość przeglądania stron internetowych, blokując dostęp do witryn niezwiązanych z pracą, na przykład serwisów społecznościowych czy portali dla dorosłych, aby zwiększyć wydajność ich pracy i uniknąć infekcji ze złośliwych witryn.
• Kontrola nad zawartością internetową zmniejsza straty w produktywności, zużycie przepustowości sieci i ryzyko problemów prawnych powstałych z powodu przeglądania przez pracowników nieodpowiedniej lub rozpraszającej zawartości internetowej. Ta funkcja znacznie zmniejsza też ryzyko kontaktu pracownika ze złośliwą zawartością.
• Administratorzy IT mogą stosować lokalne wyjątki zastępujące wymuszone kategorie. Jeśli na przykład blokowane są portale społecznościowe, możesz dodać serwis Linkedin.com do listy zaufanych witryn jako wyjątek.

Kontrola połączeń
• Warstwa zabezpieczeń, która znacznie zwiększa ochronę kluczowych czynności w firmie, takich jak korzystanie z intranetu lub poufnych usług w chmurze (na przykład systemów CRM).
• Gdy pracownik otworzy witrynę, która wymaga dodatkowej ochrony, Kontrola połączeń automatycznie zwiększy poziom zabezpieczeń dla tej sesji. W tym okresie Kontrola połączeń zamyka połączenia sieciowe z punktu końcowego do wszystkich nieznanych witryn. Użytkownicy mogą nadal korzystać ze stron internetowych zweryfikowanych przez F-Secure jako bezpieczne, aby nie obniżać produktywności pracowników.
• Dzięki blokowaniu niezaufanych połączeń konie trojańskie wyłudzające informacje bankowe oraz inne złośliwe programy nie mogą wysyłać przestępcom poufnych danych firmy, takich jak dane logowania użytkowników czy informacje z chmury. Zabezpieczenia wracają do normalnego poziomu, gdy dany proces przeglądarki zostanie zakończony lub użytkownik zakończy sesję