Dane aktualne na dzień: 17-05-2024 12:36

Link do produktu: https://sklep.cnet.com.pl/webroot-secureanywhere-business-endpoint-protection-edugovnp-1-rok-przedzial-stanowisk-1000-5000-esd-p-89.html

Webroot SecureAnywhere Business Endpoint Protection EDU/GOV/NP 1 rok przedział stanowisk 1000-5000 ESD

Cena brutto	**61,99 zł**
Cena netto	**50,40 zł**
Dostępność	**Dostępny**
Czas wysyłki	**24 godziny**
Producent	**WEBROOT**

Opis produktu

- Solidna ochrona wykorzystująca potencjał największej na świecie bazy zagrożeń WIN
- Niewiarygodnie szybki silnik skanujący – skanowanie w mniej niż 2 minuty
- Zintegrowany pakiet dostępny już w podstawowej wersji – ochrona prywatności, firewall oraz ochrona antyphishingowa
- Zarządzanie zdalne przez konsolę administracyj

Nowatorska konsola WEB

- Całkowicie zautomatyzowane zarządzanie wszystkimi końcówkami bez względu na to czy są w sieci lokalnej czy też nie.
- Bezproblemowe zarządzanie komputerami firmowymi z każdego miejsca na ziemi**.**
- **Całkowity brak potrzeby posiadania własnego serwera**

Lekkość i bezkonfliktowość

Webroot SecureAnywhere Endpoint Protection to jedyne oprogramowanie, którego wdrożenie nie pociąga za sobą nieprzewidzianych konsekwencji. Instalacja trwa kilka sekund, obciążenie dla systemu jest niezauważalne. Specjalne polityki pozwalają administratorowi na ustawienie własnych czarnych i białych list. Instalacja oprogramowania Webroot nie powoduje przestojów w firmie czy też nieoczekiwanych konfliktów.

Bezpieczeństwo na miarę XXI wieku

W dobie kiedy każdego dnia pojawia się około 70 000 nowych wirusów tradycyjne metody detekcji nie zdają egzaminu. Webroot dostarcza całkowicie nowatorskie metody wykrywania zagrożeń oparte na 3 filarach:

- sygnatury
- zachowanie aplikacji
- reputacja aplikacji i stron www

Nawet jeśli nie istnieje sygnatura dla danego zagrożenia Webroot jest w stanie zdefiniować szkodliwy plik na podstawie jego zachowania.

Zainstaluj i zapomnij

Webroot to jedyne oprogramowanie, które nie ściąga sygnatur lokalnie. Po zainstalowaniu ochrona działa w czasie rzeczywistym w chmurze. Administrator nie musi martwić się o aktualizację gdyż całe działanie programu opiera się na strukturze funkcjonującej w chmurze obliczeniowej.

Technologia PREVX

Ta technologia to badanie reputacji plików i stron w sieci pozwala na unikanie infekcji przez odwiedzenie szkodliwych stron lub ściągnięcie zainfekowanych danych. Wszystkie te procesy mają miejsce w chmurze bez zbędnego obciążenia stacji końcowej użytkownika

Innowacje w bezpieczeństwo

TRADYCYJNY ANTYWIRUS

WEBROOT CLOUD

Niesamowita lekkość

Oprogramowanie tradycyjne zajmuje nawet do 100 razy więcej miejsca na dysku Twojego komputera. Należy pamiętać iż do samego programu trzeba załadować sygnatury które potrafią być olbrzymie. WEBROOT wyznaczył nową jakość. Klient zajmuje zaledwie 700 kb i nie pobiera sygnatur wiec oszczędza tak cenne w dzisiejszych czasach zasoby.

Szybka instalacja

Dzięki temu, że Agent Webroota jest tak mały, około 99% mniejszy niż

konkurencyjne rozwiązania instaluje się w około 2 sekundy. Konkurencyjne rozwiązania mogą instalować się nawet 45 minut. Po zakończonym procesie rozpoczyna się pobieranie sygnatur które trwa kolejne kilka lub kilkanaście minut. Gdy liczy się prędkość nie ma kompromisów – WEBROOT oszczędza Twój czas.

Głębokie skanowanie

Głębokie skanowanie w przypadku oprogramowania Webroot SecureAnywhere trwa zazwyczaj około 2 minuty. Można je przeprowadzać w każdej chwili gdyż nie ma absolutnie żadnego obciążenia dla stacji końcowej. Przy niewiarygodnej szybkości skanowanie Webroota jest niebywale efektywne.

Brak obciążenia

WEBROOT dzięki chmurze obliczeniowej WIN na serwerach AMAZON redukuje obciążenie Twojego PC o około 99% Dlatego nawet nie zauważysz kiedy przeprowadza takie działania jak skanowanie czy konserwację systemu. Czy wiesz ze WEBROOT jest najlżejszym i najszybszym rozwiązaniem an świecie wg. niezależnej organizacji certyfikującej AV Comparatives?

Wyeliminowanie konieczności posiadania sygnatur

Codzienne aktualizowanie sygnatur spowalnia pracę na komputerze i ogranicza przepustowość sieci. Webroot oferuje diametralnie inne podejście. Ochrona w czasie rzeczywistym działająca w chmurze niweluje tewszystkie niedogodności. W czasie rzeczywistym każdy użytkownik korzysta z ogromnej bazy zagrożeń w chmurze. Jest to obecnie ponad 80TB i średnio dziennie przybywa kolejne 200GB nowych danych.

Zapobieganie konfliktom

Obszerne i przeładowane niepotrzebnymi funkcjami oprogramowanie bardzo często powoduje konflikty z wieloma aplikacjami. Agent Webroota jest bezkonfliktowym i ultra-lekkim rozwiązaniem kompatybilnym z każdym oprogramowaniem.

Blokowanie zagrożeń dnia zerowego

Ochrona oparta na sygnaturach sprawia, że od momentu ukazania się wirusa do opublikowania jego sygnatury użytkownik pozostaje bezbronny. Webroot blokuje nieznane zagrożenia na

podstawie ich zachowania a w wypadku wykrycia niebezpiecznego pliku po kilku sekundach każdy użytkownik na świecie jest przed nim chroniony 2012.

Zaawansowana analiza oraz odwracanie szkodliwych zmian

Tradycyjne oprogramowanie nie analizuje działania wirusów. Tym bardziej nie potrafi odwracać wyrządzonych przez nie szkód. Webroot szczegółowo analizuje każdy proces i z niespotkaną skutecznością odwraca szkodliwe zmiany 2012.

Niezależna kontrola nad plikami

Po zdefiniowaniu zagrożenia w przypadku tradycyjnego oprogramowania upływa długi okres czasu do momentu kiedy użytkownik jest w pełni zabezpieczony. Webroot zapewnia natychmiastową reakcję na zagrożenia opartą na inteligentnej analizie zachowania.

Ochrona w czasie rzeczywistym

WEBROOT dzięki stałemu dostępowi do bazy w chmurze obliczeniowej jest w stanie ochronić użytkownika nawet przed najnowszymi zagrożeniami. Analiza behawioralna dodatkowo monitoruje plik, które nie są znane i wychwytuje szkodliwe zachowania.

Błyskawiczne naprawianie szkód

W przypadku standardowego oprogramowania najczęstszą metodą naprawy jest całkowita reinstalacja systemu. Webroot dzięki zaawansowanej technologii raportowania i odwracania zmian jest w stanie przywrócić komputer do odpowiedniego stanu bez potrzeby przeinstalowania systemu. Dzieje się to automatycznie i bez konieczności udziału administratora.

Nieustannie rosnąca ilość zagrożeń

Obecnie ilość nowych zagrożeń jest tak ogromna, że producenci nie mają szans na opublikowanie wszystkich sygnatur na czas. Webroot zmienił podejście do zwalczania wirusów przez zastosowanie kompleksowej oraz inteligentnej detekcji opartej na analizie zachowań. Dzięki temu odnajduje zagrożenia, które jeszcze nigdy się nie pojawiły obserwując ich zachowanie.

Zapobieganie wykradaniu danych

Obecnie oprogramowanie malware staje się coraz bardziej wyrafinowane a ataki są nakierowane bardzo precyzyjnie w celu uzyskania konkretnych danych. Webroot oferuje strukturalną ochronę danych opartą na zaawansowanych modułach ochrony prywatności. Dzięki temu prywatne dane oraz operacje bankowe online są całkowicie bezpieczne.

Usuwanie nieznanych zagrożeń

Tradycyjne oprogramowanie okazuje się bezradne w wypadku nieznanych programów pozwalając im na nieograniczoną ingerencję w systemie. Webroot pozwala nieznanym programom na swobodne uruchamianie się w bezpiecznym wirtualnym środowisku a w przypadku gdy okaże się ono szkodliwe natychmiast je blokuje i odwraca wszystkie dokonane przez nie zmiany.

Zredukowanie możliwości wycieku danych

Tradycyjne oprogramowanie rzadko kiedy sprawdza się w wypadku nieznanego oprogramowania szpiegującego. Webroot zapobiega utracie danych dzięki inteligentnemu firewallowi opartemu na analizie podejrzanych zachowań, który nie dopuści do nieodwracalnych akcji takich jak przesłanie danych bez kontroli użytkownika.

Skalowalne ustawienia wykrywalności

Webroot zastępuję przestarzałą heurystykę, która sprowadzała się do zwykłego zgadywania wyrafinowanym i skalowalnym systemem analizyzachowań. Heurystyka Webroota to w pełni zarządzalny moduł prewencyjnej analizy zachowawczej.

Bezproblemowe i błyskawiczne wsparcie techniczne

Czasochłonne czekanie w kolejkach telefonicznych i męczące objaśnianie problemu to już przeszłość. Webroot oferuje profesjonalne wsparcie opartena logach i kompleksową diagnostykę dzięki przejrzystości działaniaprogramu w chmurze.

Skład pakietu bezpieczeństwa

- Zintegrowany Firewall

- Konsola zarządzająca WEB
- System Analyser (analizuje podzespoły systemu i ich sprawność)
- System Cleaner (czyści system i rejestr z śmieci systemowych)
- Ochrona prywatności (ochrona haseł oraz prywatności)
- Głębokie skanowanie komputera ok 1 min bez obciążania systemu
- Brak pobierania sygnatur z internetu
- Bezkonkurencyjny poziom ochrony, ponad 80TB sygnatur chmury Amazon EC2
- 100% skuteczności w przypadku nowych zagrożeń
- Funkcja Rollback – unikalne rozwiązanie, które odwraca zmiany dokonane przez infekcję
- W pełni funkcjonalna ochrona w trybie offline

Wymagania systemowe

Konsola administratora

- Internet Explorer® wersja 7, 8, 9 i 10 (Październik 2012)
- Mozilla® Firefox® wersja 3.6 lub wyższa
- Chrome 11 oraz 12
- Safari 5
- Opera 11

Systemy operacyjne

- Microsoft® Windows® XP 32- oraz 64-bit SP2, SP3
- Windows Vista® 32-bit (wszystkie edycje), Windows Vista SP1, SP2 32- oraz 64-bit (wszystkie edycje)
- Windows 7 32- oraz 64-bit (wszystkie edycje), Windows 7 SP1 32- oraz 64-bit (wszystkie edycje)
- Windows 8 32-oraz 64-bit

Minimalne wymogi sprzętowe

- Intel®Pentium®/Celeron® family, or AMD® K6/Athlon™/Duron™ family, lub inny kompatybilny procesor
- 128 MB RAM (minimum)
- 10 MB HDD
- Microsoft® Internet Explorer® 7.0 alub wyższa, Mozilla® Firefox® 3.6 lub wyższa
- Google Chrome™ 10.0 lub wyższy
- Apple® Safari® 5.0.1 lub wyższy
- Dostęp do internetu

Wspierane platformy serwerowe

- Windows Server 2003 Standard, Enterprise, 32 oraz 64-bit
- Windows Server 2008 R2 Foundation, Standard, Enterprise
- Windows Small Business Server 2008 oraz 2011
- Windows Small Business Server 2012 (Listopad 2012)

Wspierane wirtualne platformy serwerowe

- VMware vSphere 4 (ESX/ESXi3.0, 3.5, 4.0, 4.1), oraz Workstation 6.5, 7.0, i Server 1.0, 2.0
- Citrix XenDesktop 5 oraz XenServer 5.0, 5.5, 5.6
- Microsoft Hyper-V Server 2008, 2008 R2