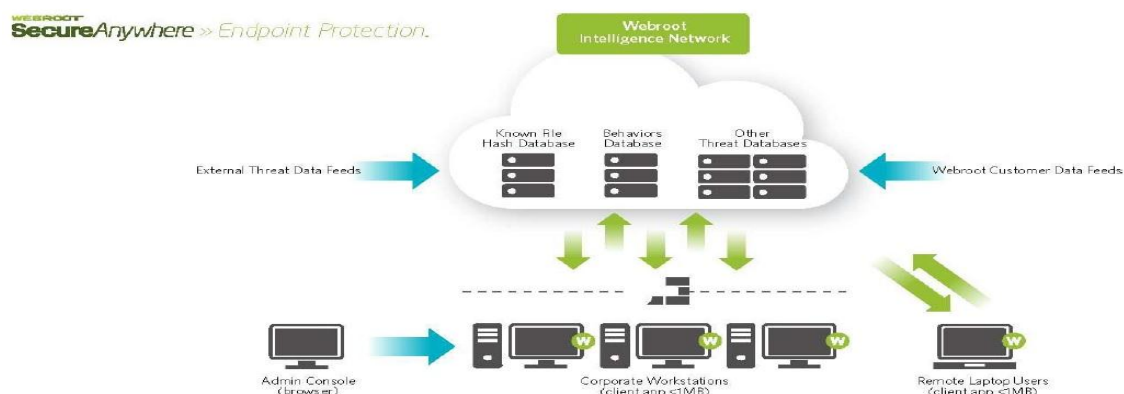


Webroot Secure Anywhere Business – Endpoint Protection

Rewelacyjna ochrona. Niewiarygodna wydajność. Zminimalizowane Zarządzanie.

Wprowadzenie

Webroot® Secure Anywhere Business – Endpoint Protection oferuje rewelacyjne podejście do bezpieczeństwa urządzeń końcowych. Wykorzystuje innowacyjną technologię skanowania plików oraz łączy ją z proaktywną, behawioralną techniką rozpoznawania zagrożeń. Tworzy w ten sposób niezwykle efektywny system, który jest w stanie wykryć nawet najbardziej zaawansowane złośliwe oprogramowanie, chronić przed kodami i atakami typu „zero-day”, wykorzystującymi podatności systemów na nieznane dotąd zagrożenia. Używając najmniejszego, a zarazem najszybszego agenta bezpieczeństwa na świecie, skanowanie trwa niewiarygodnie szybko (w normalnych warunkach mniej niż dwie minuty¹) i nie obciążając przy tym systemu użytkownika. Ponieważ detekcja złośliwego oprogramowania odbywa się w czasie rzeczywistym, jest ona zawsze aktualna i zabezpiecza nawet przed najnowszymi zagrożeniami i atakami bez konieczności codziennego pobierania sygnatur.



SZYBKIE FAKTY:

Najlepsza Ochrona Przed Nieznanym Złośliwym Oprogramowaniem

- Rewelacyjna technologia rozpoznawania wzorów plików i typów zachowania;
- Wbudowana predykcyjna inteligencja właściwie wykrywająca czy aktywność danego pliku może być złośliwa;
- Wirtualna eliminacja tzw. „okna podatności”, czyli czasu, w którym większość producentów zabezpieczeń dopiero tworzy łatki eliminujące występowanie danej podatności, w celu zabezpieczenia klientów przed nowymi „nieznanymi” zagrożeniami.

Niesamowita Szybkość i Łatwość Instalacji

- Najmniejszy na świecie klient do instalacji na końcówce (<700kB)
- Instalacja <6s¹;
- Współdziałanie i brak konfliktów z innym oprogramowaniem bezpieczeństwa.

Brak Wpływu na Szybkość Działania i Efektywność Systemu Produkcyjnego

- Pierwsze skanowanie systemu w czasie < 2 minuty, kolejne poniżej 1 minuty;
- Minimalne obciążenie CPU podczas skanowania;
- Zaawansowane funkcje naprawiania i przywracania chronionych zasobów do ostatniego dobrego stanu bez potrzeby re-instalacji całego systemu.

Zawsze Aktualna Ochrona

- Brak konieczności wykonywania codziennych aktualizacji definicji sygnatur wysycających przepustowość sieci;
- Ochrona użytkowników pozostających off-line bez potrzeby wykonywania aktualizacji;
- Natychmiastowa ochrona wszystkich użytkowników przed nowymi zagrożeniami.

Łatwość Zarządzania

- Scentralizowane zarządzanie przez konsolę www dla wszystkich użytkowników;
- Zautomatyzowane zarządzanie i raportowanie;
- Brak konieczności posiadania serwera i oprogramowania;
- Pełne zarządzanie politykami bezpieczeństwa i urządzeniami chronionymi poprzez zdalny dostęp.

Ochrona Online i Offline

- Oddzielna kontrola i zarządzanie urządzeniami użytkowników pracujących w trybie off-line;
- Możliwość zarządzania portami i urządzeniami takimi jak: USB, CD, DVD.

¹ PassMark Software „Webroot SecureAnywhere vs. Traditional Antivirus, February 2012”

Kluczowe korzyści

Rewolucyjne Podejście do Bezpieczeństwa

Podejście do zagadnień bezpieczeństwa firmy Webroot, jest oparte w dużej mierze na zasobach chmury obliczeniowej. Pozwala to, na wyeliminowanie okna podatności, które istnieje w przypadku większości pozostałych rozwiązań bezpieczeństwa urządzeń końcowych opartych o sygnatury. Dostarcza ochrony w czasie rzeczywistym przeciwko wszystkim typom złośliwego oprogramowania.

- Eliminacja czasu podatności systemu na zagrożenia, występującego od momentu utworzenia złośliwego kodu aż do czasu jego wykrycia i wytworzenia aktualizacji, która chroni przed nim użytkownika.
- Unikalna technologia rozpoznawania wzorów plików i typów zachowania, wykrywająca czy aktywność danego urządzenia jest odpowiednia czy też może stanowić zagrożenie.
- Ciągła kontrola nowych i ulegających zmianie plików i procesów w ramach „Webroot® Intelligence Network” – bazy danych w chmurze Webroota, zawierającej ponad 75 TB inteligentnych danych by zrozumieć zachowania wszystkich plików, a także śledzić i określać ich intencje i cele.

Zaawansowana inteligencja rozpoznawania ataków umożliwia wyselekcjonowanie znanych i nieznanych zagrożeń tak, by efektywnie chronić użytkownika przed znanymi złośliwymi kodami jak i atakami typu zero-day.

- Ochrona off-line - zabezpieczająca końcówki, które nie są połączone z siecią Internet, wykorzystująca zaawansowane mechanizmy heurystyczne oraz możliwość zarządzania portami i urządzeniami takimi jak USB, CD i DVD.
- „Webroot Intelligence Network” - zbierając w sposób ciągły informacje o nowych, potencjalnie groźnych plikach z całej sieci Internet oraz od użytkowników Webroot’a na całym świecie. Współdzieląc te informacje w czasie rzeczywistym poprzez chmurę obliczeniową, zapewnia natychmiastowo efektywną ochronę.
- Brak konieczności codziennej aktualizacji bazy danych sygnatur lub/i plików na urządzeniu końcowym.

Niewiarygodna Wydajność



Webroot SecureAnywhere Business – Endpoint Protection ustanawia nowe standardy w zakresie czasu wdrożenia, prędkości skanowania i całkowitego obciążenia systemu tak, aby zaoszczędzić Twój czas i pieniądze.

- Ultralekki klient – najlżejszy na świecie, zajmuje mniej niż 700KB;
- Pobranie, instalacja i wdrożenie liczone w sekundach¹;
- Minimalne użycie CPU, aby zapobiec spowolnieniu środowiska pracy użytkownika;
- Minimalne zajęcie pamięci dyskowej – brak potrzeby posiadania lokalnej bazy danych sygnatur zagrożeń;

- Szybkie skanowanie, poniżej dwóch minut², porównując często do godzin u innych dostawców oprogramowania;
- Znikomy wpływ na wydajność PC, nawet stacji o minimalnych wymaganiach systemowych;
- Możliwość działania wraz z innymi produktami bezpieczeństwa IT, co eliminuje potrzebę odinstalowywania obecnych rozwiązań przed migracją;
- Maksymalizacja bezpieczeństwa i produktywności.

Minimalizacja Zarządzania

Zarządzanie oparte na konsoli webowej, pozwala łatwo administrować politykami dla końcowych użytkowników poprzez intuicyjny interfejs. Oferujący w zamian kompletne zarządzanie urządzeniami końcowymi wraz z możliwością stworzenia centralnego administrowania politykami bezpieczeństwa, wglądu w szczegółowe raporty i logi, zarządzanie białymi i czarnymi listami oraz nadpisywaniem plików.

Inne zalety zarządzania przez konsolę to:

- Brak potrzeby posiadania serwera i oprogramowania, eliminując koszty zakupu, instalacji i utrzymania;
- Konfigurowalne, domyślne szablony polityk;
- Łatwe administrowanie alarmami i powiadomieniami;
- Raportowanie ad-hoc bądź też według określonych harmonogramów z użyciem logów w czasie rzeczywistym;
- Automatyczne definicje zagrożeń i aktualizacje oprogramowania z chmury;
- Automatyczne aktualizacje klienta bez wpływu na przepustowość sieci i wydajność urządzenia;
- Zarządzanie PC, laptopami, serwerami, urządzeniami mobilnymi i tabletami z jednej konsoli.



² Po skanowaniu inicjacyjnym, kolejny pełny skan systemu zajmuje zwykle około 2 minut lub mniej

Główne cechy

Wysoka Wykrywalność Złośliwego Oprogramowania

Dostarcza najbardziej zaawansowaną ochronę urządzeń końcowych w czasie rzeczywistym przeciwko znanym i nieznanym zagrożeniom eliminując „okno podatności” pomiędzy czasem utworzenia złośliwego kodu a czasem jego wykrycia.

Ochrona Offline

Zapobiega atakom w czasie, kiedy urządzenie jest offline, z oddzielną polityką wykonywania plików dla lokalnego dysku, USB, CD czy stacji DVD. Również zawiera możliwość zablokowania urządzeń oraz portów.

Silna Heurystyka

Ustawienia heurystyk mogą być dostosowane w zależności od tolerancji ryzyka dla wykonania pliku. Ustawienia heurystyk obejmują kategorie:

- „Advanced” Zaawansowana analiza nowych plików pod kątem przewidywanych akcji, które są typowe dla złośliwego oprogramowania.
- „Age” Zaawansowana analiza nowych plików na bazie informacji o czasie, w jakim podobne pliki pojawiały się wśród użytkowników Webroot’a.
- „Popularity” Zaawansowana analiza nowych plików pod kątem tego, jak często dany plik jest używany wśród użytkowników Webroot’a.

Malware Remediation

Wszechstronny silnik detekcji i usuwania znanych oraz nieznanych zagrożeń, zawierających niebezpieczne rootkity i fragmenty złośliwego oprogramowania. Usuwać te pliki z systemu użytkownika.

Remediation Rollback

Bezpieczny mechanizm dający możliwość przywrócenia stanu danego programu lub/i ustawień systemu bądź rejestru z czasu sprzed infekcji do poprzedniego stabilnego stanu.

Webroot Intelligence Network

Wykrywanie zagrożeń i ich analiza w czasie rzeczywistym, zapewniona dzięki największej na świecie bazie danych obiektów w chmurze, składającej się z 250 milionów plików i powiązanych z nimi charakterystyk behawioralnych.

Natychmiastowe Wdrożenie

Odbytujące się poprzez pakiet instalacyjny MSI, konfigurowalne narzędzie do instalacji lub link z plikiem wykonywalnym do pobrania.

Kompatybilność Oprogramowania

Rozwiązanie kompatybilne z innym oprogramowaniem, obejmującym również rozwiązania bezpieczeństwa urządzeń końcowych, umożliwiające łatwe wdrożenie obok istniejącego już systemu.

Monitoring Systemu / Firewall Aplikacyjny

Zaawansowany firewall oparty na rozwiązaniach w chmurze chroni Twoich użytkowników nawet, gdy są poza siecią korporacyjną, zwiększając funkcjonalność firewalla Microsoft® Windows® by zaoferować pełną kontrolę zarówno dla połączeń wychodzących jak i przychodzących bez konieczności dodatkowego drenowania wydajności urządzeń końcowych. Poprzez zarządzanie i monitorowanie całego ruchu zewnętrznego, firewall chroni przed złośliwymi atakami typu „phone-home” i daje pewność, że tylko aplikacja spełniająca wymogi polityki bezpieczeństwa ma zapewnioną komunikację z siecią. Firewall potrafi również automatycznie rozpoznawać „dobre” i „złe” programy, więc użytkownicy nie są niepokojeni pojawiającymi się oknami typu pop-up, które często zmuszają ich do podjęcia decyzji dotyczącej danej aplikacji w sytuacji, kiedy nie posiadają oni dostatecznych informacji dla jej podjęcia.

SafeStart Sandbox

Nieznane pliki mogą być otwierane tylko w chronionym środowisku typu „sandbox”, w celu oceny ich zachowania. Pomaga to upewnić się, że nieznanne aplikacje i pliki nie zainfekują systemu użytkownika.

Wsparcie dla Serwerów i Maszyn Wirtualnych

Poza wspieraniem środowisk fizycznych typu Windows PC, Webroot SecureAnywhere może również wspierać środowiska typu Windows Server oraz środowiska wirtualne.

Ochrona Urządzeń Mobilnych i Tableatów

Webroot SecureAnywhere Business – Mobile Protection jest również dostępny dla urządzeń z systemem Android i iOS firmy Apple, zarówno dla smartfonów jak i tableatów.

Niezawodność Rozproszonej Architektury w Chmurze

Składa się z wielu globalnych centrów danych, dostarczających wsparcia dla lokalnych użytkowników poprzez najbliższe data center w powiązaniu z niezwykłą efektywnością, odpornością i redundancją.

Wymagania Systemowe:

Dostęp do Konsoli Zarządzającej:

- Internet Explorer® wersja 7, 8, 9, 10
- Mozilla® Firefox® wersja 3.6 i wyżej
- Chrome 11 i 12
- Safari 5
- Opera 11

Wspierane Platformy PC

- Windows® XP Service Pack 2 i 3, 32 i 64bit
- Windows Vista®, 32 i 64bit
- Windows 7, 32 i 64bit
- Windows 8, 32 i 64bit

Wspierane Platformy Serwerowe

- Windows Server 2003 Standard, Enterprise, 32 i 64bit
- Windows Server 2008 R2 Foundation, Standard, Enterprise
- Windows Small Business Server 2008, 2011 i 2012

Wspierane Platformy Serwerów Wirtualnych

- VMware vSphere 4 (ESX/ESXi3.0, 3.5, 4.0, 4.1, plus Workstation 6.5, 7.0, Server 1.0, 2.0)
- Citrix XenDesktop 5 i XenServer 5.0, 5.5, 5.6
- Microsoft Hyper-V Server 2008, 2008 R2.6

Wspierane Mobilne Systemy Operacyjne

- Android operating system wersja 2.1 lub wyższa
- Android – smartfon lub tablet z 3MB wolnego miejsca na dysku
- Apple iOS 4.2 lub wyższy
- Kompatybilne z iPhone, iPod Touch i iPad

Firmie

Webroot został założony w 1997 roku, jako przedsiębiorstwo prywatne. Ma swoją główną siedzibę w Colorado. Firma posiada swoje oddziały i operuje na terytorium Ameryki Północnej, Europy oraz regionu Azji i Pacyfiku. Zapraszamy do kontaktu

Webroot International Limited
6th Floor, Block A 1 George's Quay Plaza
George's Quay, Dublin 2 Ireland

Telephone: +44 (0) 870 1417 070

Webroot Poland
SOFTIL s.c.
Ul. Derdowskiego 8/17, 71-178 Szczecin
E-mail: info@softil.pl
Telefon: + 48 91 434 15 44