

Webroot®

Ochrona stacji końcowych dla przedsiębiorstw

Intuicyjne narzędzie do poprawy cyberbezpieczeństwa w firmie.



Zarys

W dzisiejszych czasach firmy każdej wielkości są nieustannie atakowane. Część ataków zdarza się okazjonalnie, ale wiele z nich jest bardzo ukierunkowanych i precyzyjnych. Ze względu na ich różnorodność i szybkość, istotne jest używanie zabezpieczeń o szerokim spektrum. Rozwiązania te powinny też współpracować z innymi systemami ochronnymi i powstrzymywać złośliwe oprogramowania (ransomware, phishing, cryptomining). Wyzwania związane z bezpieczeństwem są takie same, niezależnie od wielkości firmy.

Webroot® Business Endpoint Protection wspiera przedsiębiorstwa w rozwiązywaniu tych i wielu innych problemów. Oferuje wielokrotnie nagradzaną¹, intuicyjną konsolę zarządzania. Dzięki interfejsowi RESTful API mamy możliwość integracji z ponad 40 aplikacjami innych firm. Kompleksowa strategia ochrony pozwala na zautomatyzowane wykrywanie, zapobieganie, ochronę i likwidację zagrożeń na stacjach końcowych i środowiskach serwerowych. Webroot w unikalny sposób wykorzystuje możliwości chmury obliczeniowej i uczenia maszynowego w czasie rzeczywistym, aby stale monitorować i dostosowywać ochronę.

Dzięki opatentowanemu, proaktywnemu i predykcynemu podejściu do bezpieczeństwa, Webroot Business Endpoint Protection oferuje wysoce skuteczną ochronę przed współczesnymi zagrożeniami cybernetycznymi.

Unikalne podejście Webroot

Webroot® Business Endpoint Protection diametralnie różni się od innych rozwiązań zabezpieczających punkty końcowe. Oparte na chmurze rozwiązanie jest dostępne w postaci usługi (SaaS) i oferuje szereg korzyści:

Bezproblemowe wdrażanie

Instalacja niewielkiego (<5MB) agenta trwa średnio 3 sekundy², a sam agent dobrze współpracuje z innymi systemami bezpieczeństwa. Taka kompatybilność sprawia, że wdrażanie Webroot i zastępowanie nim starszego oprogramowania jest znacznie szybsze i łatwiejsze. Administratorzy nie muszą już się martwić o negatywny wpływ wdrożenia na wydajność użytkowników.

W pełni zdalne zarządzanie i kontrola punktów końcowych

Oparta na chmurze konsola nie wymaga instalacji na serwerze w siedzibie klienta. Umożliwia łatwe testowanie, wdrażanie i zarządzanie innymi rozwiązaniami producenta, takimi jak Webroot® DNS Protection i Webroot® Security Awareness Training. Zapewnia wgląd i kontrolę nad każdym urządzeniem, na którym zainstalowany jest agent Webroot. Pozwala zarządzać wieloma jednostkami i lokalizacjami oraz daje możliwość efektywnego wykorzystania agenta, dzięki zdalnym poleceniom akcji.

Uproszczona obsługa

Webroot® Business Endpoint Protection zaprojektowano od podstaw tak, aby był łatwy do wdrożenia, zarządzania i utrzymania. Możesz korzystać z predefiniowanych szablonów polityk lub w prosty sposób modyfikować je, tworząc własne. Nie ma potrzeby aktualizowania sygnatur ani definicji, ponieważ ochrona przed zagrożeniami odbywa się za pośrednictwem chmury w czasie rzeczywistym. Aktualizacje agenta są samoistne i trwają zazwyczaj 3 sekundy², pozostając całkowicie nieodczuwalnymi dla użytkownika. Ostrzeżenia o zagrożeniach i środki naprawcze są zautomatyzowane, co pomaga zaoszczędzić czas działom bezpieczeństwa.

Ochrona w trybie online i offline

Webroot wykorzystuje opatentowaną technologię do monitorowania, rejestrowania i powstrzymywania ataków, również gdy urządzenie znajduje się w trybie offline. Podobnie, dane systemów i użytkowników są chronione w tym trybie.

Światowej klasy rozwiązanie oparte na analizie zagrożeń w czasie rzeczywistym

Wszystkie rozwiązania Webroot są wspierane przez własną platformę, która integruje ten sam globalny system Webroot BrightCloud® Threat Intelligence, której zaufało ponad 100 producentów. Użyte algorytmy uczenia maszynowego analizują ponad pół biliona niebezpiecznych obiektów dziennie.

¹ G2.com. "Usability Index for Endpoint Protection Suites" (Fall 2019)

² PassMark Software. "Webroot SecureAnywhere® Business Endpoint Protection vs. Eight Competitors." (March 2019)

Niskie koszty systemowe (porównanie z niezależnego benchmarkingu)

Kluczową zaletą koncepcji opartej na chmurze jest to, że intensywne przetwarzanie danych związanych z wykrywaniem i analizą złośliwego oprogramowania odbywa się bez konieczności zajmowania przestrzeni dyskowych w infrastrukturze klienta. Niezależne testy przeprowadzone przez PassMark Software wykazały, że ochrona Webroot charakteryzuje się najniższym całkowitym zużyciem zasobów systemowych wśród wiodących produktów konkurencyjnych². Pełne zaplanowane skanowanie jest niezauważalne dla użytkowników, a wykorzystanie procesora systemowego i pamięci RAM jest nieznaczne i nie obciąża zasobów.

Innowacyjna technologia wykrywania

W przeciwieństwie do tradycyjnych metod, tj. rozwiązań bazujących na sygnaturach, ochrona Webroot działa wieloetapowo. Po pierwsze zapobiega przenikaniu złośliwego oprogramowania do systemu. Następnie uniemożliwia uruchomienie oprogramowania i nieznanego plików, jeśli wykazują one szkodliwe zachowanie. Ta wieloetapowa strategia jest nie tylko bardziej skuteczna w walce z nowoczesnymi zagrożeniami, ale również zmniejsza prawdopodobieństwo wystąpienia fałszywych alarmów.

Webroot® Business Endpoint Protection w skrócie

- **Bezpieczna i odporna architektura rozproszonej chmury**
Wykorzystuje centra danych na całym świecie, aby zapewnić klientom i użytkownikom kompleksową obsługę.

- **Wielowarstwowa ochrona użytkowników i urządzeń**
Powstrzymuje również ataki, które wykorzystują socjotechniki, a nie tylko te ukierunkowane na luki w zabezpieczeniach urządzeń.

- **Wykrywanie i blokowanie złośliwego oprogramowania**
Typu: trojany, phishing, ransomware, spyware, ataki oparte na przeglądarce, cryptojacking, złośliwe oprogramowanie wykradające dane uwierzytelniające, ataki oparte na skryptach oraz wiele innych zagrożeń.

- **Ochrona przed złośliwymi skryptami**
Opatentowana technologia Webroot® Evasion Shield wykrywa, blokuje i usuwa (poddaje kwarantannie) ataki z wykorzystaniem skryptów, niezależnie od tego, czy są one oparte na plikach, bez plików, zamaskowane lub zaszyfrowane. Zapobiega również uruchamianiu złośliwych aktywności w językach PowerShell, JavaScript i VBScript.

- **Obsługa wielu systemów operacyjnych, wirtualizacji, serwerów terminalowych i Citrix**
Obsługuje urządzenia z systemem MacOS®, komputery i serwery z systemem Windows®, wirtualizację, serwery terminali i środowiska Citrix.

- **Ochrona tożsamości i prywatności użytkowników**
The Identity Shield (izolowanie przeglądarek i aplikacji) jest zaufanym narzędziem wykorzystywanym przez największe banki na świecie do powstrzymywania ataków takich jak DNS poisoning, keylogging, screen grabbing, cookie scraping, clipboard grabbing oraz przechwytywanie przeglądarek i sesji przez złośliwe oprogramowanie.

- **Biała i czarna lista**
Zapewnia bezpośrednią kontrolę nad aplikacjami.

- **Inteligentny firewall**
Monitoruje system oraz aplikacje, uzupełnia firewall Windows® chroniąc użytkowników zarówno w sieciach firmy jak i poza nimi.

- **Pełna ochrona w trybie offline**
Zatrzymuje ataki bez dostępu do sieci i umożliwia administratorom tworzenie oddzielnych polityk dotyczących przetwarzania plików na dyskach lokalnych, USB, CD i DVD.

- **Bezpłatna, wielokrotnie nagradzana pomoc telefoniczna**
Wewnętrzny zespół pomocy technicznej Webroot jest gotowy do rozwiązywania problemów, a wskaźnik zadowolenia klientów wynosi 95%.

- **Przejrzyste użytkowanie i rozliczanie**
Portale Webroot My Usage i My Billing w konsoli zarządzania sprawiają, że dostęp do płatności jest przejrzysty i intuicyjny.

Jakich wyników można się spodziewać

Webroot® Business Endpoint Protection pomaga firmom podwyższyć poziom bezpieczeństwa zapewniając zaawansowaną ochronę przed stale rosnącą i ewoluującą falą nowoczesnych ataków. Dzięki wysoce zautomatyzowanemu i skutecznemu zabezpieczeniu punktów końcowych nie trzeba już korzystać z dedykowanych zasobów i ekspertów ds. bezpieczeństwa IT. Dzięki maksymalnie zredukowanej liczbie infekcji i ataków, uwaga administratorów nie będzie rozproszona problemami związanymi z bezpieczeństwem.

CEEcloud Services Distribution Sp. z o.o.

Autoryzowany dystrybutor Datto w Polsce

Skontaktuj się z nami:

www.ceecloud.pl | kontakt@ceecloud.pl | +48 12 340 90 30



in @CEEcloud
f @CEEcloud
Bakotech Poland&CEE