Malwarebytes

ARKUSZ DANYCH

Malwarebytes Endpoint Protection

Zaawansowana ochrona przed zagrożeniami

FUNKCJE TECHNICZNE

Ochrona sieci Web

Blokuje użytkownikom dostęp do złośliwych stron, sieci reklamowych, sieci scammerów i innych niebezpiecznych środowisk.

Hartowanie aplikacji

Zmniejsza skalę luk w zabezpieczeniach oraz w proaktywny sposób wykrywa próby znakowania plików przez zaawansowane formy ataku.

Ochrona przed wykorzystywaniem luk w oprogramowaniu

W proaktywny sposób wykrywa i blokuje próby wykorzystania luk w oprogramowaniu i zdalnego uruchomienia kodu w punktach końcowych.

Ochrona zachowań aplikacji

Zapobiega wykorzystaniu aplikacji do zainfekowania punktów końcowych.

Wykrywanie anomalii

W proaktywny sposób identyfikuje wirusy i złośliwe oprogramowanie przy użyciu technik uczenia maszynowego.

Analiza zawartości

Identyfikuje całe rodziny znanego (oraz powiązanego z nim) złośliwego oprogramowania w oparciu o zasady heurystyczne i behawioralne.

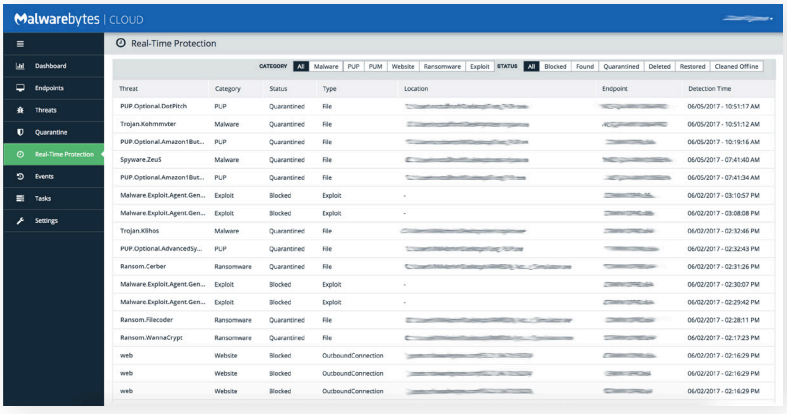
Zapobieganie działaniu oprogramowania ransomware

Za pomocą technologii monitorowania zachowań wykrywa oprogramowanie ransomware i blokuje je.

Podstawą skutecznej strategii ochrony jest zapobieganie, jednak w tym przypadku nie istnieje złoty środek, który zapewni uniwersalne podejście. Eksperci odradzają wręcz poleganie na pojedynczej technice lub technologii do ochrony punktów końcowych firmy. Efektywna ochrona wymaga podejścia opartego o warstwy, zdolnego zapobiegać nie tylko zagrożeniom aktualnym, lecz również tym, które pojawią się w przyszłości.

Malwarebytes Endpoint Protection to zaawansowane rozwiązanie do ochrony punktów końcowych, zbudowane z wielu warstw wykorzystujących różne techniki wykrywania zagrożeń. Takie podejście zapewnia firmom pełną ochronę przed łańcuchem ataku — zarówno w obliczu znanego, jak i nieznanego oprogramowania ransomware, złośliwego oprogramowania i zagrożeń zero-hour. Dzięki ujednoliceniu do postaci pojedynczego agenta Malwarebytes Endpoint Protection ogranicza złożoność i koszty związane zazwyczaj z wdrażaniem wielu pojedynczych rozwiązań.

Skuteczność technik stosowanych przez Malwarebytes Endpoint Protection zwiększa dodatkowo najlepsza w branży telemetria. Malwarebytes wyznacza obecnie standard kompleksowego i dokładnego usuwania zagrożeń w sytuacjach, w których zawodzą inne rozwiązania zabezpieczające. Za dowód naszej skuteczności może posłużyć fakt, że oprogramowanie Malwarebytes pobiera każdego dnia 500 tysięcy firm i klientów indywidualnych. Co więcej, nasze oprogramowanie codziennie wyszukuje i usuwa 3 miliony infekcji. Unikalna telemetria zapewnia także doskonały wgląd w istniejące zagrożenia i techniki, pozwalając w większym stopniu zrozumieć czynniki stojące za sukcesem ataków, a tym samym metody ich skutecznego zwalczania.



Konsola chmurowa Malwarebytes — ochrona w czasie rzeczywistym

Najważniejsze korzyści

Warstwy technik wykrywania zagrożeń

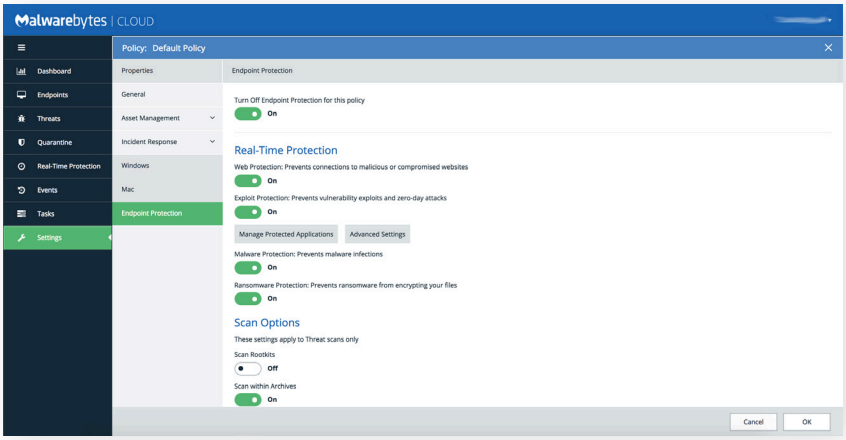
Malwarebytes Endpoint Protection wykorzystuje wiele technik identyfikowania i ochrony na wszystkich etapach łańcucha ataku. Dzięki efektywnemu połączeniu warstw technologii dopasowywania oraz technologii działających bez udziału sygnatur jest w stanie podejmować działania zarówno przed, jak i po wystąpieniu ataku. Najlepsza w branży telemetria nieustannie doskonali techniki wykrywania ataków przed ich uruchomieniem, pozwalając na wykrywanie zagrożeń na wczesnych etapach łańcucha infekcji.

Dokładne i kompleksowe usuwanie zagrożeń

Malwarebytes Endpoint Protection korzysta z opracowanego przez nas mechanizmu Linking Engine, aby usuwać nie tylko główną zawartość zagrożenia, lecz także wszystkie ślady infekcji i ich pozostałości. Stosowanie podejścia działającego bez sygnatur przyspiesza skanowanie i zapewnia znaczną oszczędność czasu, który w innych przypadkach należałoby poświęcić na czyszczenie punktów końcowych i przywracanie ich z obrazów.

Zarządzanie w oparciu o chmurę

Malwarebytes Endpoint Protection to rozwiązanie dostarczane za pośrednictwem platformy zarządzania punktami końcowymi Malwarebytes opartej o chmurę obliczeniową. Zastosowanie platformy chmurowej zmniejsza złożoność, ułatwiając wdrażanie Malwarebytes Endpoint Protection i innych rozwiązań Malwarebytes oraz zarządzanie nimi — niezależnie od liczby posiadanych punktów końcowych. Co więcej, scentralizowana konsola działająca w chmurze eliminuje konieczność pozyskiwania i utrzymywania sprzętu w sposób lokalny.



Ustawienia zasad zabezpieczeń Malwarebytes Endpoint Protection

WYMAGANIA SYSTEMOWE

Zawarte komponenty

- Platforma chmurowa Malwarebytes
- Malwarebytes Endpoint Protection (trwały agent systemu Windows)
- Wsparcie e-mail i telefoniczne

Wymagania sprzętowe

System Windows

Procesor: 1 GHz

Pamięć RAM: 1 GB (klienty); 2 GB (serwery)

Dostępne miejsce na dysku: 100 MB (program + dzienniki)

Aktywne połączenie internetowe

Obsługiwane systemy operacyjne

Windows 10® (32-, 64-bitowy)

Windows 8.1® (32-, 64-bitowy)

Windows 8® (32-, 64-bitowy)

Windows 7® (32-, 64-bitowy)

Windows Vista® (32-, 64-bitowy)

Windows XP® z dodatkiem SP3 (tylko 32-bitowy)

* Windows Server 2016® (32-, 64-bitowy)

* Windows Server 2012/2012R2® (32-, 64-bitowy)

* Windows Small Business Server 2011

* Windows Server 2008/2008R2® (32-, 64-bitowy)

* Windows Server 2003® (tylko 32-bitowy)

Należy zwrócić uwagę, że serwery Windows, w których jest wykorzystywany proces instalowania Server Core, są specjalnie wykluczone.

** Integracja z Centrum akcji systemu Windows nie jest obsługiwana w systemach operacyjnych Windows Server.*

malwarebytes.com corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes jest nowoczesną firmą zajmującą się cyberbezpieczeństwem, której zaufały miliony użytkowników na całym świecie. Malwarebytes aktywnie chroni firmy i użytkowników indywidualnych przed zagrożeniami takimi jak złośliwe oprogramowanie, programy ransomware i programy wykorzystujące luki w zabezpieczeniach, których nie są w stanie wykryć tradycyjne rozwiązania antywirusowe. Flagowy produkt firmy łączy zaawansowane heurystyczne wykrywanie zagrożeń z bezsygnaturowymi technologiami wykrywania cyberataków i przeciwdziałania im jeszcze przed wystąpieniem strat. Ponad 10 000 firm na całym świecie wykorzystuje, ufa i poleca Malwarebytes. Firma została założona w 2008 roku. Jej siedziba główna znajduje się w Kalifornii, a jej filie znajdują się w Europie i Azji. Firma dysponuje także globalnym zespołem badaczy i ekspertów w dziedzinie zabezpieczeń.