Malwarebytes Incident Response

Scentralizowane wykrywanie zagrożeń i usuwanie ich skutków

FUNKCJE TECHNICZNE

Mechanizm Incident Response
Udostępnia funkcje szybkiego, niezwykle skutecznego skanowania na żądanie w oparciu o harmonogram lub w sposób automatyczny.

Wiele trybów skanowania
Tryby szybkiego, pełnego i niestandardowego skanowania pracują w sposób nieuciążliwy dla użytkowników końcowych.

Mechanizm Linking Engine
Technologia działająca bez sygnatur identyfikuje i dokładnie usuwa wszystkie pozostałości zagrożeń powiązane z pierwotną zawartością.

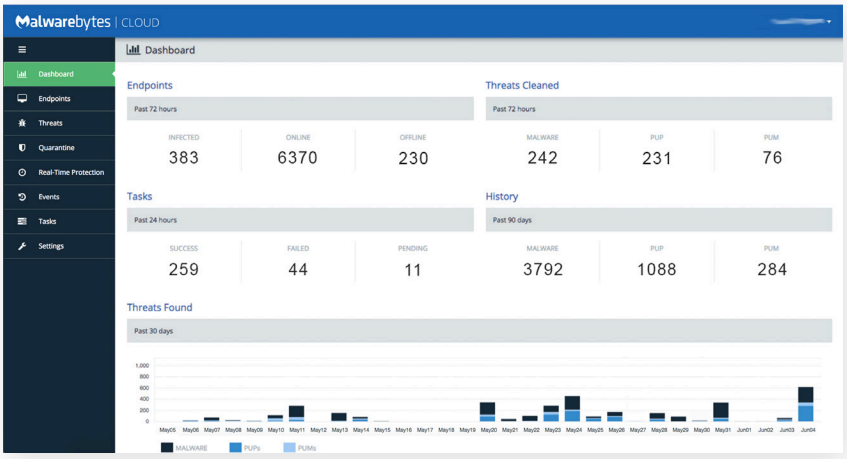
Platforma chmurowa Malwarebytes
Konsola zarządzania oparta o chmurę pozwala na łatwe, scentralizowane zarządzanie zasadami zabezpieczeń, wdrażanie rozwiązań i raportowanie zagrożeń.

Asset Management
Udostępnia przydatne informacje na temat systemów punktów końcowych, w tym ich obiektów pamięci, zainstalowanego oprogramowania, programów uruchamianych przy rozruchu i nie tylko.

Forensic Timeliner
Gromadzi dzienniki zdarzeń systemu Windows i porządkuje je do postaci pojedynczego chronologicznego widoku.

Cyberprzestępcy stosują dziś coraz bardziej wyrafinowane metody dobierania celów, pozyskiwania informacji na temat ofiar i przeprowadzania ataków. Co więcej, złośliwe oprogramowanie nieustannie penetruje zabezpieczenia sieci i punktów końcowych, nawet jeśli firmy, szkoły lub agencje rządowe wydały miliony na wzmocnienie posiadanych stosów zabezpieczeń. Reagowanie na zdarzenia wymaga znacznego czasu i nakładów pracy[1], dlatego usunięcie skutków ataku z jednego punktu końcowego (lub jego przywrócenie z obrazu) może trwać wiele godzin. Zgodnie z wynikami badania przeprowadzonego przez Ponemon Institute wykrycie naruszeń wynikających z obecności złośliwych programów lub działalności przestępców zajmuje średnio 229 dni, a usunięcie ich skutków — 82 dni[2]. Z punktu widzenia firm dostarczenie zespołom maksymalnego wglądu oraz najlepszych środków zaradczych jest dziś niezwykle ważne.

Malwarebytes Incident Response to narzędzie służące do wykrywania zagrożeń i usuwania ich skutków, zbudowane w oparciu o wysoce skalowalną chmurową platformę zarządzania. Oprogramowanie skanuje punkty końcowe połączone z siecią w poszukiwaniu zaawansowanych zagrożeń — w tym złośliwego oprogramowania, potencjalnie niepożądanych programów i oprogramowania adware — a następnie całkowicie je usuwa. Malwarebytes Incident Response podnosi jakość ochrony przed zagrożeniami oraz skraca czas reakcji na ataki. Dodatkowo oferuje wysoką skalowalność, elastyczność i automatyzację.



Pulpit nawigacyjny konsoli chmurowej Malwarebytes

Odniesienia

[1] Reagowanie na zdarzenia oznacza stosowanie przez organizacje narzędzi, procesów i umiejętności w celu przeciwdziałania cyberatakom i usuwania ich skutków po ich zidentyfikowaniu.

[2] Źródło: Ponemon Institute, 2016 Cost of Data Breach Study, czerwiec 2016.

Najważniejsze korzyści

Automatyzacja

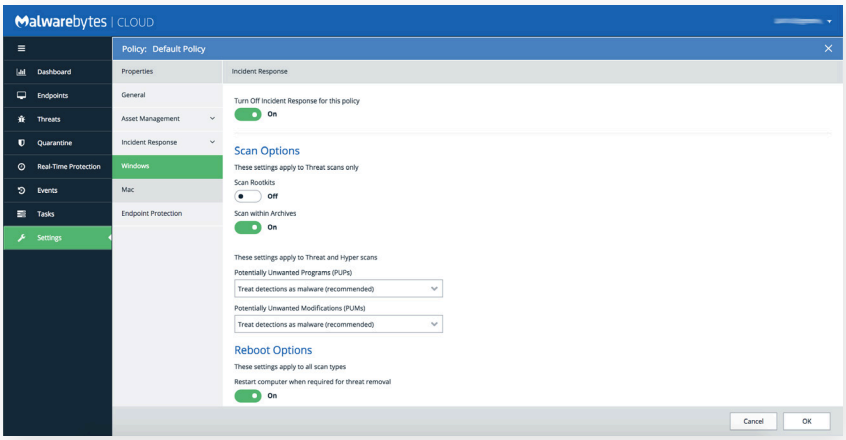
Wstępne wdrożenie Malwarebytes Incident Response na punktach końcowych pozwala korzystać z funkcji wykrywania i usuwania zagrożeń za pomocą jednego przycisku. Integracja z istniejącymi systemami zarządzania punktami końcowymi, SIEM i narzędziami do wykrywania zagrożeń pozwala także w automatyczny sposób reagować na alerty o zdarzeniach. Co więcej, automatyzacja procesu reagowania na zagrożenia pozwala firmom przyspieszyć działanie przepływów reakcji, skracając przy tym czas obecności zagrożeń na punktach końcowych.

Elastyczność

Malwarebytes Incident Response korzysta zarówno z ujednoliconego agenta trwałego, jak i agentów nietrwałych (Breach Remediation). Dzięki temu udostępnia elastyczne opcje wdrażania, dopasowane do różnorodnych środowisk informatycznych. Rozwiązanie pozwala na łatwą integrację z istniejącym stosem zabezpieczeń,spełniając jednocześnie wymogi systemów operacyjnych (Windows i Mac OS X), jak i infrastruktury.

Skalowalność

Malwarebytes Incident Response to rozwiązanie dostarczane za pośrednictwem nowej platformy zarządzania punktami końcowymi Malwarebytes opartej o chmurę obliczeniową. Zastosowanie platformy chmurowej Malwarebytes zmniejsza złożoność, ułatwiając wdrażanie Malwarebytes Incident Response i innych rozwiązań Malwarebytes oraz zarządzanie nimi — niezależnie od tego, czy dysponujemy jednym czy milionem punktów końcowych. Co więcej, scentralizowana konsola działająca w chmurze eliminuje konieczność pozyskiwania i utrzymywania sprzętu w sposób lokalny.



Ustawienia zasad zabezpieczeń Malwarebytes Incident Response

WYMAGANIA SYSTEMOWE

Zawarte komponenty

- Platforma chmurowa Malwarebytes
- Malwarebytes Incident Response (trwałe agenty systemów Windows i Mac OS X)
- Breach Remediation (nietrwałe agenty: wiersz poleceń systemu Windows oraz interfejs graficzny i wiersz poleceń dla komputerów Mac)
- Forensic Timeliner (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

Komputery Mac
Dowolne urządzenie Apple Mac ze wsparciem dla systemu Mac OS X (w wersji 10.10 lub nowszej)
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)

Mac OS X (10.10 lub nowszy)

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.