Bitdefender GravityZone Advanced Business Security

Fragment Raportu

Business Security Report 2017

Język: polski

Sierpień 2017
Data ostatniej aktualizacji: 11.10.2017

www.avcomparatives.org

Wstęp

Przegląd oprogramowania biznesowego AV-Comparatives 2017 dokonuje porównania rozwiązań bezpieczeństwa dla firm korzystających z sieci Microsoft Windows. Raport przygląda się wybranym codziennym zadaniom niezbędnym do funkcjonowania sieci. Szczegółowe informacje o punktach, które sprawdziliśmy dla każdego programu podano poniżej.

Ten raport jest fragmentem raportu Business Security Report1 2017, pokazującym wyniki testu Bitdefender GravityZone Advanced Business Security 6.2. Test został przeprowadzony w sierpniu 2017.

Bitdefender GravityZone Advanced Business Security jest dostępny w dwóch konfiguracjach. Dokonaliśmy przeglądu jego konsoli cloud (chociaż dostępna jest wersja lokalna w postaci wstępnie skonfigurowanej maszyny wirtualnej). Przejrzysta konstrukcja i możliwości konfiguracji sprawiają, że rozwiązanie jest bardzo łatwe w użyciu nawet dla administratorów nie będących ekspertami (w ich przypadku potrzebne jest tylko podstawowe szkolenie).

AV-Comparatives Approved Business Product Award 2017

W ramach certyfikacji produktów bezpieczeństwa biznesowego, przeprowadziliśmy praktyczny test zabezpieczeń, korzystając z naszego Real World Testing Framework.

Aby uzyskać nagrodę Approved Business Product, przeglądane produkty biznesowe musiały osiągnąć współczynnik ochrony wynoszący co najmniej 90%, bez fałszywych alarmów w oprogramowaniu biznesowym.

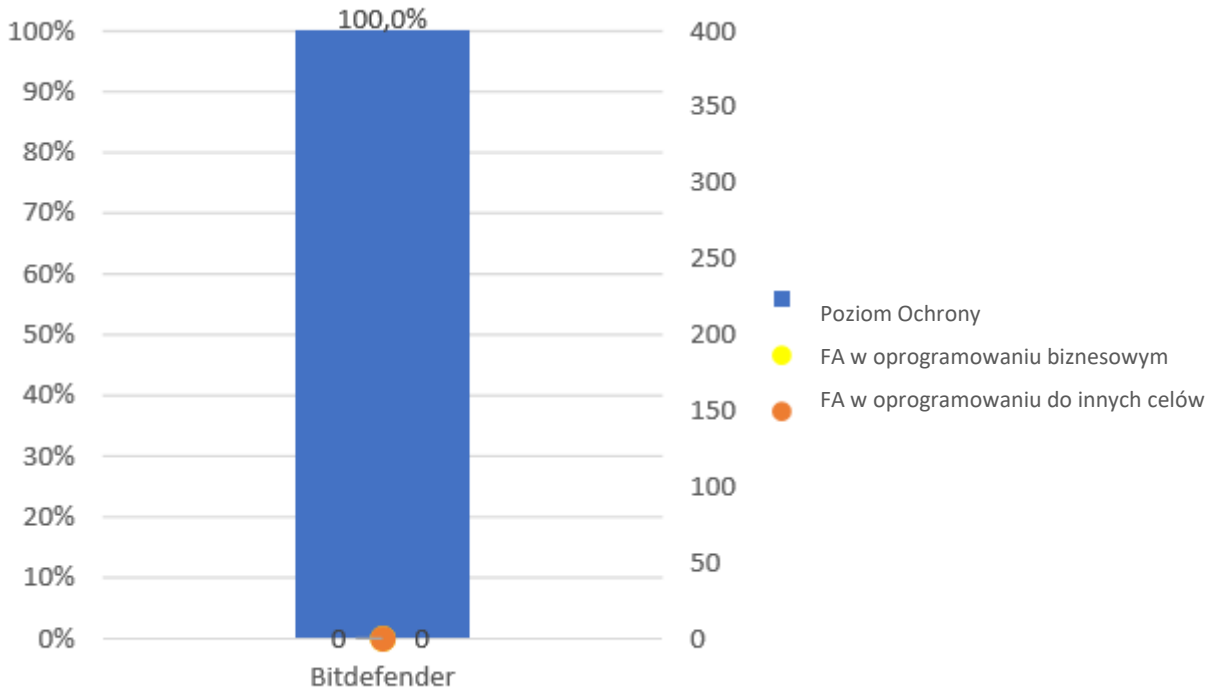
Bitdefender GravityZone Advanced Business Security zdobył nagrodę Approved Business Product. Szczegółowe wyniki można zobaczyć na następnej stronie.

[1] Pełny raport można znaleźć tutaj:
https://www.av-comparatives.org/wp-content/uploads/2017/10/avc_cor_2017_en.pdf

Wyniki Testu Praktycznego Real-World Protection

Wyniki są oparte na zestawie testowym **389** aktywnych szkodliwych adresów URL. Wektory infekcji są wektorami, z którymi na co dzień mają do czynienia typowi użytkownicy. Wykorzystane przypadki testowe obejmują szeroki zakres aktualnych złośliwych witryn i zapewniają wgląd w ochronę zapewnianą przez produkt.

Produkt	Poziom Ochrony	Fałszywe Alarmy w oprogramowaniu biznesowym	Fałszywe Alarmy w oprogramowaniu do innych celów
Bitdefender GravityZone	100.0%	0	0



Podsumowanie

Za dużą zaletę uznaliśmy fakt, że strona Pulpitu może być łatwo dostosowana do wyświetlania różnych alertów lub pozycji statusu, a okno dialogowe opcji instalacji, które jest (opcjonalnie) wyświetlane po zalogowaniu, sprawia, że wdrażanie oprogramowania klienta jest bardzo proste. Oprogramowanie klienta jest również bardzo przejrzyste i pozwala użytkownikom wykonywać kluczowe codzienne zadania.

W tym roku do konsoli GravityZone zostały wprowadzone dwie nowe funkcje bezpieczeństwa: Hyper Detect i Analizator Sandbox. HyperDetect pozwala administratorom dostosować ochronę poprzez dostrojenie lokalnych modeli uczenia maszynowego i stosowanie zaawansowanej heurystyki, które są wyspecjalizowane w wykrywaniu narzędzi hakerskich, exploitów i technik zaciemniania złośliwego oprogramowania. Dzięki temu możliwe jest blokowanie zagrożeń przed ich wykonaniem, wykrywanie technik ich dostarczania i witryn zawierających zestawy exploitów oraz blokowanie podejrzanego ruchu internetowego.

Dzięki opcji "Tylko zgłoś" administratorzy zabezpieczeń mogą ustawiać i monitorować swoją nową politykę bezpieczeństwa przed jej wprowadzeniem. W połączeniu z wysoką widocznością i blokowaniem zagrożeń, użytkownicy mogą ustawić HyperDetect na blokowanie na poziomie "Normalnym" lub "Dopuszczalnym", przy czym mogą nadal raportować na poziomie "Agresywnym", wykrywającym wczesne wskaźniki zagrożeń.

Analizator Sandbox automatycznie przesyła podejrzane pliki do analizy w zamkniętym wirtualnym środowisku hostowanym przez Bitdefender, analizuje ich zachowanie i zgłasza złośliwe zamiary. Funkcja automatycznego przesyłania pozwala administratorom bezpieczeństwa korporacyjnego wybrać tryb "Monitoruj" lub "Blokuj", który uniemożliwia dostęp do pliku do momentu otrzymania wyniku. Administratorzy mogą również ręcznie przesyłać pliki do analizy. Obszerny zakres informacji kryminalistycznych Analizatora Sandbox pozwala administratorom uzyskać czytelny kontekst zagrożeń i pomaga zrozumieć ich zachowanie.

GravityZone posiada funkcje potrzebne do obsługi większych sieci, będąc jednocześnie prostym i łatwym w użytkowaniu rozwiązaniem, zwłaszcza dla firm nie posiadających pełnoetatowych pracowników IT.

Bitdefender GravityZone Advanced Business Security

Przegląd

Wersja produktu

Bitdefender Endpoint Security 6.2.22.923

Obsługiwany system operacyjny Windows

Klienci: Windows XP, Vista, 7, 8/8.1, 10

Serwery: Windows Server 2003/R2, 2008/R2, 2012/R2; Windows Small Business Server 2003, 2008, 2011.

W naszym teście, Bitdefender Endpoint Security działał bez zarzutu z Windows Server 2016.

O produkcie

Bitdefender GravityZone jest wyposażony w konsolę cloud do zarządzania oprogramowaniem zabezpieczającym dla systemów operacyjnych Windows, Mac i Linux. Konsola Bitdefender GravityZone jest również dostępna w wersji lokalnej. Do testu użyto konsoli cloud.

Funkcje EDR

W odniesieniu do funkcji EDR, Bitdefender podaje: "W ostatnim kwartale 2017 roku Bitdefender wprowadzi "Bitdefender xDR ", który łączy w jednym rozwiązaniu funkcje zapobiegania zagrożeniom, wykrywania zagrożeń i reagowania na zagrożenia. "Bitdefender xDR" zapobiega znanym i nieznanym atakom, wykrywa podejrzane działania na urządzeniu, bada te działania w celu zrozumienia wpływu i potwierdzenia obecności wskaźników naruszenia. Ataki są sprawdzane przez Analizator Sandbox Bitdefender i Bitdefender Global Protective Network. Akcje reagowania na incydenty obejmują: usunięcie IOC, poddanie kwarantannie systemów podlegających usterce oraz dostrojenie polityk bezpieczeństwa tak, aby automatycznie zapobiegać przyszłym atakom "

Informacje o produkcie na stronie internetowej dostawcy

https://bitdefender.pl/biznes/oprogramowanie-antywirusowe-dla-firm/gravityzone-advanced-business-security

Wsparcie online

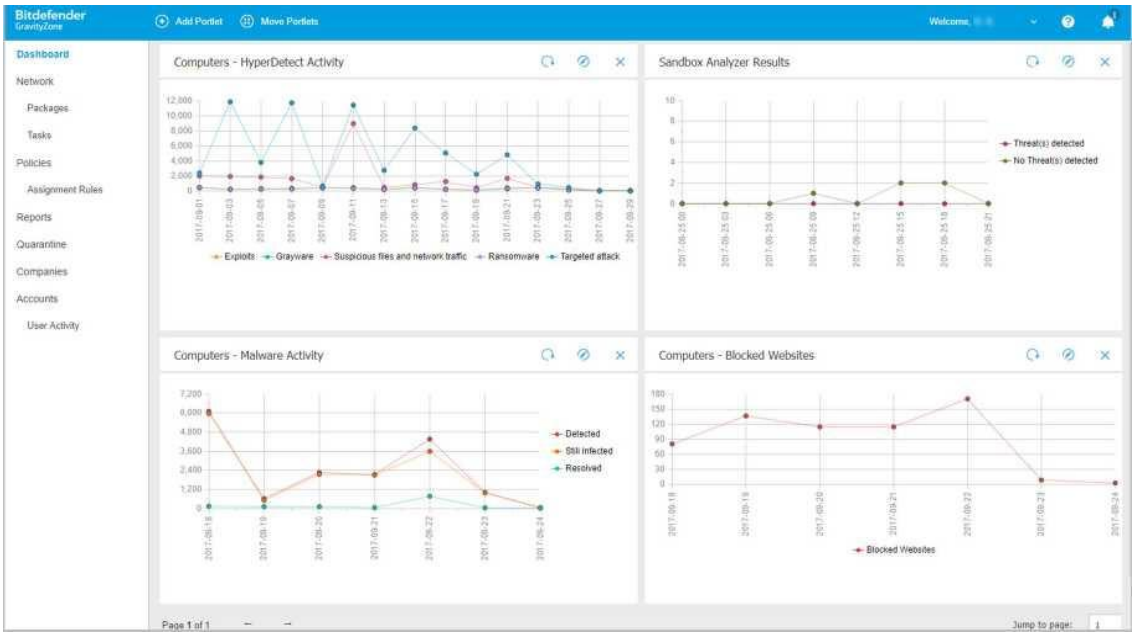
https://bitdefender.pl/biznes/uzyteczne-linki/wsparcie-techniczne

Konsola Zarządzania

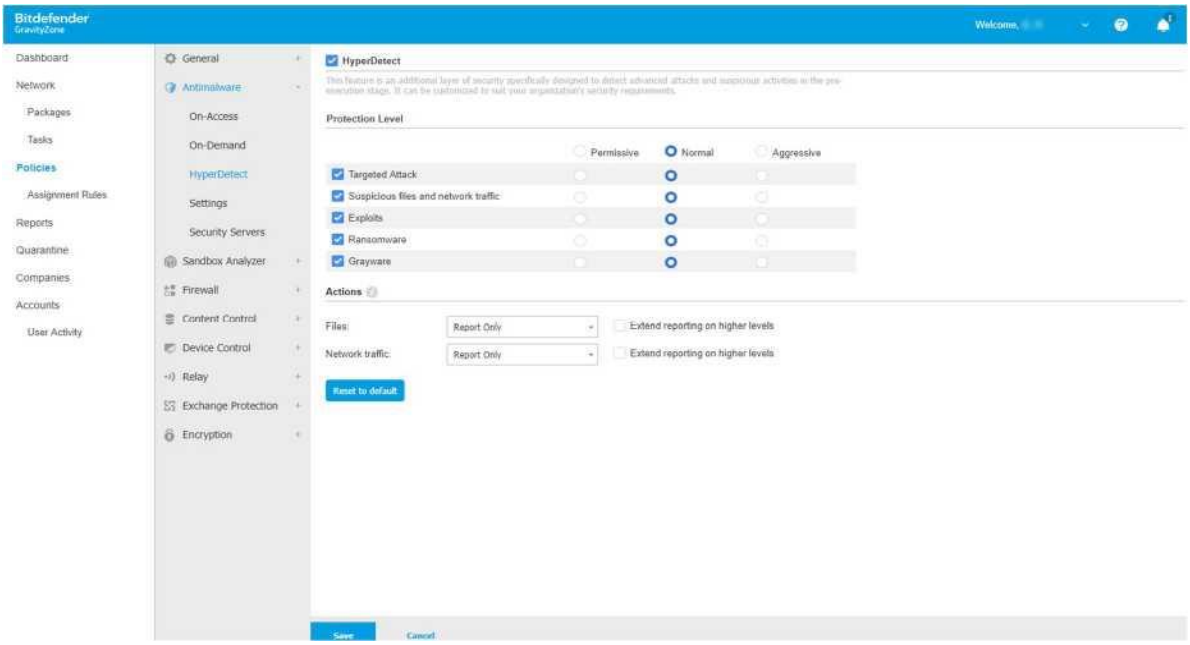
Instalacja i Konfiguracja

Konsola jest oparta na chmurze, więc nie wymaga konfiguracji.

Układ



Układ konsoli jest prosty i przejrzysty. Kolumna menu po lewej stronie umożliwia administratorowi przełączanie między Pulpitem, Siecią, Politykami, Raportami, Kwarantanną i Kontami.



Metody wdrażania oprogramowania zabezpieczającego punkt końcowy

- Pobieranie i instalowanie lokalnie przez klienta
- Wysyłanie linku instalacyjnego na email użytkownika
- Zdalna instalacja od pierwszego preinstalowanego klienta

Monitorowanie sieci

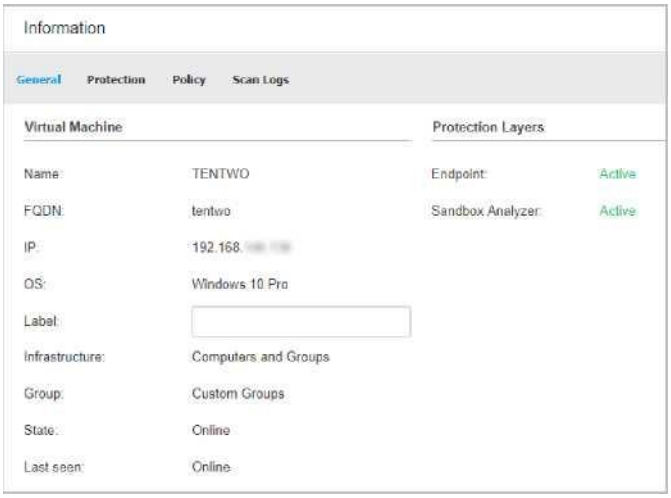
Status i powiadomienia

Są one wyświetlane na Pulpicie (strona główna) konsoli i składają się z Aktywności Złośliwego Oprogramowania,

Statusu Złośliwego Oprogramowania, 10 Najczęściej Wykrywanych Złośliwych Programów i Statusu Ochrony Punktów Końcowych.

Wersja Programu

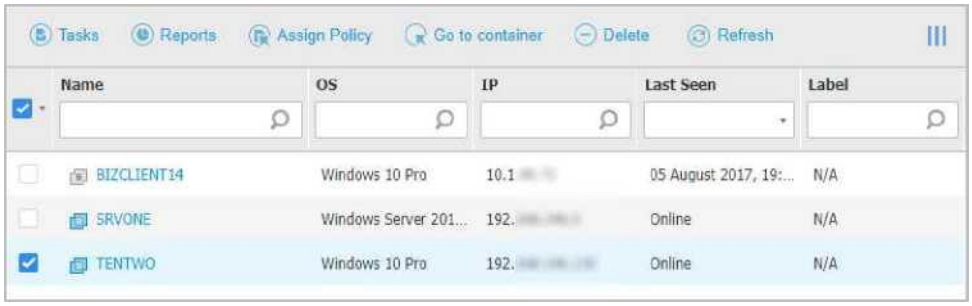
Wyświetlana jest na stronie Informacje:



Zarządzanie siecią

Skanowanie, planowanie skanów, aktualizowanie i usuwanie urządzeń z konsoli

Na stronie Sieci administrator może wybierać komputery, przypisywać zadania takie jak aktualizacje i skany lub przypisywać polityki:

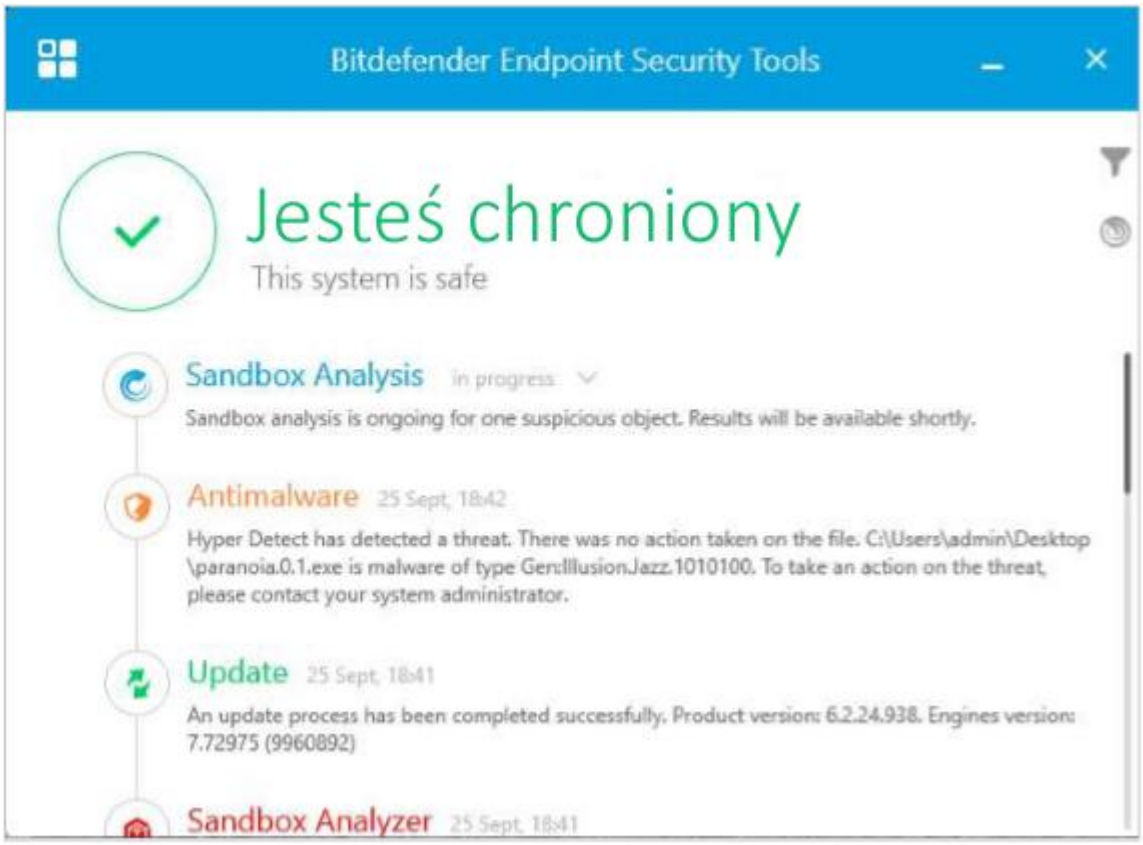


Kontrolowanie dostępu użytkownika do oprogramowania zabezpieczającego punkt końcowy

Domyślnie, użytkownicy nie mają uprawnień do wyłączania komponentów ochrony.

Oprogramowanie zabezpieczające punkty końcowe dla klientów Windows

Oprogramowanie klienta posiada graficzny interfejs użytkownika z widocznym wyświetlaniem statusu oraz przyciski funkcji i ustawień:



Zadanie dostępne dla użytkowników

Użytkownicy mogą uruchamiać szybkie, pełne lub niestandardowe skanowanie i sprawdzać dostępność aktualizacji.

Centrum Zabezpieczeń Systemu Windows / Windows Defender

Narzędzia Bitdefender Endpoint Security są zarejestrowane jako programy antywirusowe i zapory w Centrum Zabezpieczeń systemu Windows. Windows Defender i Zapora systemu Windows są wyłączone.

Powiadomienia

Jeśli plik testowy EICAR zostanie pobrany, zostanie on zablokowany, a w oknie przeglądarki zostanie wyświetlone poniższe powiadomienie:

Działania ze strony użytkownika nie są wymagane.

Jeśli ochrona w czasie rzeczywistym jest wyłączona, w obszarze stanu głównego okna programu wyświetlane jest ostrzeżenie:

Domyślnie komponenty można włączać i wyłączać tylko z poziomu konsoli.

Oprogramowanie zabezpieczające punkty końcowe Windows Server

Można je uznać za identyczne z oprogramowaniem klienta, chociaż nie są zainstalowane niektóre składniki (zapora, kontrola zawartości)

Prawa autorskie i klauzula zrzeczenia się odpowiedzialności

Aby uzyskać więcej informacji na temat AV-Comparatives i metodologii testowania, odwiedź naszą stronę internetową.

(Październik 2017)