Analizator Sandbox
Dane Techniczne

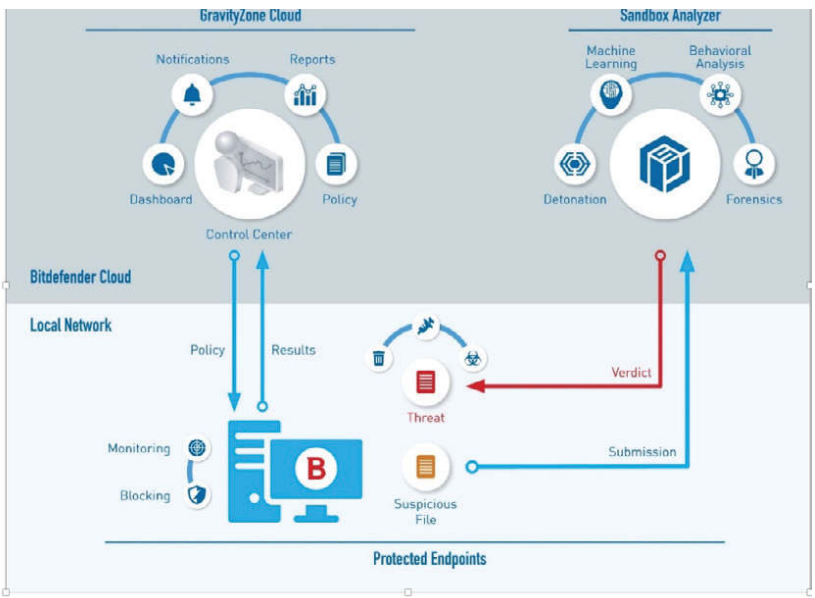
Przegląd

W obecnym krajobrazie cyberbezpieczeństwa, przedsiębiorstwa są stale narażone na działanie złośliwego oprogramowania, zakłócenia, naruszenia bezpieczeństwa danych oraz szereg innych incydentów wpływających na poprawne funkcjonowanie firmy. Dzieje się tak, ponieważ cyberprzestępcy stają się coraz bardziej profesjonalni w swojej dziedzinie, udoskonalają swój warsztat przestępczy i nieustannie zmieniają taktykę działania. Platforma Bitdefender GravityZone Endpoint Security chroni punkty końcowe przed pełnym zakresem zaawansowanych ataków cybernetycznych, zapewniając wysoką efektywność, niewielki wpływ na użytkowników końcowych i niskie koszty administracyjne. Składa się ona z wielowarstwowej ochrony, która stanowi dla hakerów nie lada wyzwanie. Każda z warstw ma na celu zablokowanie określonych typów zagrożeń, narzędzi lub technik ataków.
Bitdefender Sandbox Analyzer jest częścią platformy GravityZone Endpoint Security. Zapewnia wykrywanie ataków jeszcze przed ich wykonaniem, poprzez automatyczne wysyłanie podejrzanych plików do dalszej analizy w chmurze Sandbox i podejmowanie działań naprawczych.

Etap Wykrywania	Typ Technologii	Zasięg Zagrożenia
Wstępne działania	Detonator (Sandbox)	APT, Ataki Celowane, Techniki Unikania, Zaciemnione Złośliwe Oprogramowanie, Niestandardowe Złośliwe Oprogramowanie, Ransomware

Znaczenie Analizatora Sandbox

Cyberprzestępcy wykorzystują istniejące już zagrożenia i wprowadzają drobne modyfikacje kodu, próbując ominąć mechanizmy obronne oparte na sygnaturach. Wiele z dzisiejszych narzędzi bezpieczeństwa jest już w stanie wykryć niektóre z tych polimorficznych zagrożeń. Jednak napastnicy, którzy są bardziej zdeterminowani, cierpliwi i wykwalifikowani, inwestują swój czas i pieniądze, aby cały czas tworzyć zupełnie nowe, nieznane dotąd zagrożenia. Zagrożenia te mogą celować w branżę, organizację czy, w niektórych przypadkach, w jednostkę. Analizator Sandbox został zaprojektowany tak, aby wykrywać, zatrzymywać ale również zapobiegać naruszeniom zanim złośliwy plik zostanie uruchomiony na punkcie końcowym. Wszystko dzięki opartej na chmurze technologii sandbox. Za każdym razem, gdy użytkownik końcowy uzyskuje dostęp do nieznanego przenośnego pliku wykonywalnego (PE), Bitdefender stosuje uczenie maszynowe i technologię HyperDetect, aby określić, czy plik ten jest złośliwy. Jeśli pliki wymagają dalszej analizy, Bitdefender wysyła je do sandboxa w chmurze.



Sandbox analizuje pliki, wykorzystując specjalnie zaprojektowane, zaawansowane algorytmy uczenia maszynowego, wabiki, techniki anty-unikowe i anty-exploit oraz analizy agresywnego zachowania. W związku z tym, że plik jest analizowany w środowisku sandbox, Bitdefender GravityZone może przeprowadzić dogłębną analizę bez obawy o wpływ na wydajność, eliminując jednocześnie ryzyko związane z uruchomieniem potencjalnie złośliwego pliku na punkcie końcowym. Bitdefender zezwoli lub zablokuje wykonanie pliku na punkcie końcowym na podstawie polityki administracyjnej. Jeśli werdykt okaże się złośliwy, Bitdefender zaktualizuje również Globalną Sieć Ochrony (usługa Bitdefender do wykrywania zagrożeń w chmurze). Zapewni to ochronę przed nowo zidentyfikowanym zagrożeniem wszystkim klientom Bitdefender.

Funkcje

- Automatyczne przesyłanie plików z punktu końcowego do analizy Sandbox. Dodatkowe warstwy zapobiegawcze Bitdefender GravityZone - Wykrywanie Zagrozen oparte na Uczeniu Maszynowym i HyperDetect dbaja o to, aby tylko pliki wymagajace dalszej analizy były przesłane do sandboxa.
- Automatyczna naprawa w oparciu o wynik analizy: blokowanie nowo wykrytych zagrożeń w całym przedsiębiorstwie
- Specjalnie zaprojektowane, zaawansowane algorytmy Uczenia Maszynowego, analiza agresywnych zachowań, techniki anty-unikowe oraz porównanie zrzutów pamięci
- Szeroki zakres typów plików: Microsoft Office, aplety Adobe Flash, Adobe Reader, aplety Java, przenośne pliki wykonywalne (PEF).
- Powiadomienie użytkownika końcowego o przeprowadzanej analizie sandbox
- Obsługa trybu "Monitorowania" i "Blokowania"
- Możliwość ręcznego przesyłania plików
- Wczesne wykrywanie wskaźników kompromisu (IOC)
- Wnikliwe raporty na temat zachowań szkodliwych programów
- Wsparcie dla fizycznych i wirtualnych punktów końcowych (Bitdefender Gravity Zone - Security for Virtualized Environments (SVE)

Korzyści

- Wczesne wykrywanie zaawansowanych ataków i zapobieganie naruszeniom, redukcja kosztów oraz wysiłku związanego z reagowaniem na incydenty
- Redukcja obciążenia spowodowanego wykrywaniem zagrożeń
- Zwiększenie wykrywalności nieuchwytnych zagrożeń, dzięki Sandbox Analyzer na etapie przed ich wykonaniem, w tym APT, ataków ukierunkowanych, technik unikania, zaciemnionego złośliwego oprogramowania, niestandardowego złośliwego oprogramowania, ransomware
- Automatyczne przesyłanie przenośnych plików wykonywalnych z punktów końcowych do opartych na chmurze usług sandbox radykalnie zmniejsza obciążenia administracyjne związane z technologią sandbox
- Potężne technologie uczenia maszynowego i wykrywania zachowań od Bitdefender gwarantujące, że tylko pliki wymagające dalszej analizy są przesyłane do sandboxa
- Szczegółowe sprawozdania zapewniające administratorom bezpieczeństwa wgląd w zachowanie szkodliwego oprogramowania
- Obsługa trybu "Monitoruj" i "Blokuj" dająca administratorom bezpieczeństwa niezbędną elastyczność
- Jest częścią jednego, zintegrowanego agenta bezpieczeństwa punktów końcowych i platformy centralnego zarządzania, co redukuje obciążenia administracyjne Klienci nie muszą już wdrażać mieszanki rozwiązań bezpieczeństwa punktów końcowych

www.bitdefender.pl | www.marken.com.pl | Marken Systemy Antywirusowe | tel: 58 573 51 51 | ul. Jana Hieronima Derdowskiego 7, 81-369 Gdynia