Bitdefender GravityZone Ultra Suite

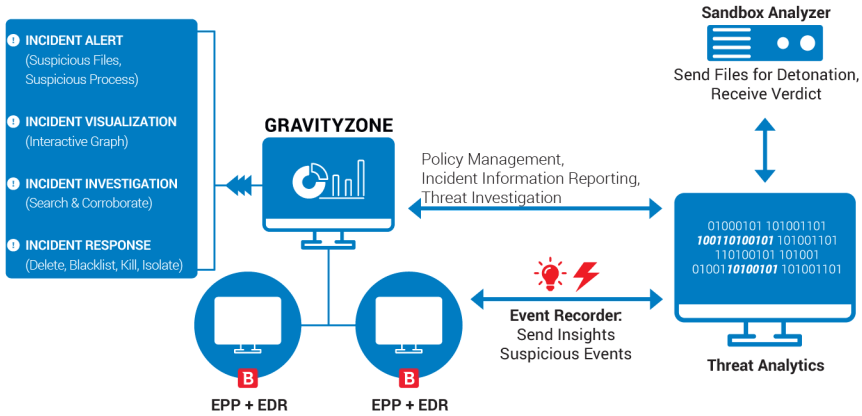
WYKRYWAJ I ZWALCZAJ ZAGROŻENIA SPRAWNIE I PRECYZYJNIE

W przeciwieństwie do produktów EDR, które są zbyt złożone, GravityZone Ultra, wyposażony w Endpoint Security XDR działa płynnie, zapobiegając, wykrywając i reagując na zaawansowane ataki, którym udaje się ominąć tradycyjne rozwiązania anty-malware. Pojedynczy, ujednolicony pakiet zabezpieczeń GravityZone Ultra to:

- Redukcja płaszczyzny ataku (firewall, kontrola aplikacji, kontrola treści i zarządzanie uaktualnieniami)
- Ochrona danych (pełne szyfrowanie dysku)
- Wykrywanie i eliminowanie szkodliwego oprogramowania przed jego wykonaniem (skalowalne uczenie maszynowe, ikontrola procesu w czasie rzeczywistym i analiza sandbox)
- Zautomatyzowane wykrywanie, analiza i naprawa za pośrednictwem nowo wydanego rejestratora zdarzeń punktu końcowego i analiz zagrożeń w Endpoint Security XDR

W rezultacie zyskujemy niezakłócone zapobieganie zagrożeniom, dokładne wykrywanie incydentów i inteligentne reagowanie w celu zminimalizowania ryzyka infekcji i blokowanie naruszeń bezpieczeństwa.

Jako zintegrowany pakiet ochrony punktów końcowych, GravityZone Ultra zapewnia stały poziom bezpieczeństwa dla całego środowiska IT, w którym hakerzy nie będą mieli czego szukać. GravityZone Ultra opiera się na prostej, zintegrowanej architekturze ze scentralizowanym zarządzaniem dla punktów końcowych i centrów danych. Pozwala firmom szybko wdrożyć kompleksowe rozwiązanie ochrony punktów końcowych i wymaga minimalnego wysiłku administracyjnego.



Rysunek 1. Bitdefender XDR: zapobieganie, wykrywanie i reagowanie w jednym agencie, zarządzanym przez konsolę GravityZone

Ułatwione EDR

Dzięki pełnej widoczności wskaźników zagrożeń (IOC) oraz procesom bezpośredniej analizy zagrożeń i reagowania na incydenty, GravityZone Ultra zmniejsza wymagania dotyczące zasobów i kwalifikacji zespołu bezpieczeństwa. Nowy rejestrator danych punktu końcowego jest spójny z istniejącym pakietem ochrony przed zagrożeniami i rejestruje szeroki zakres działań systemu (tworzenie plików i procesów, instalacja programów, ładowanie modułów, modyfikacja rejestru, połączenia sieciowe itp.), pomagając przedsiębiorstwu dokonać wizualizacji łańcucha zdarzeń dotyczących ataku.

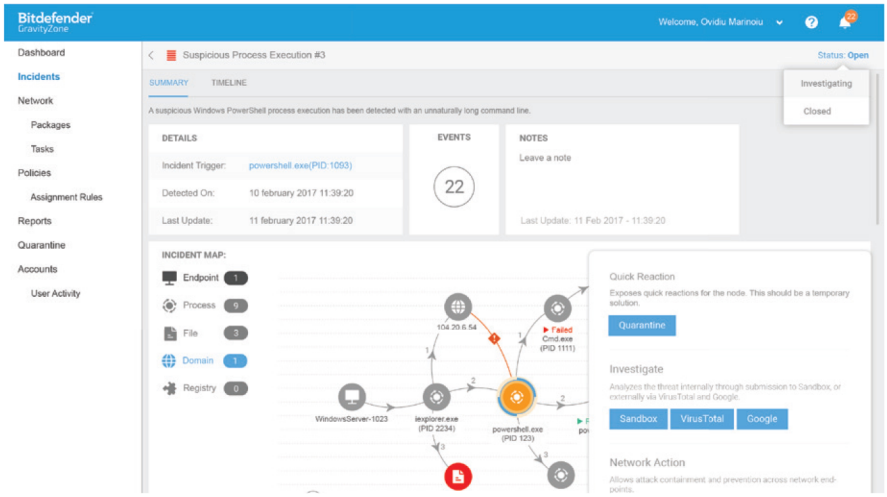
Moduł analizy zagrożeń działa w chmurze i sprawdza zachowanie procesów i ich aktywność w systemie, tworząc uporządkowaną listę przypadków wymagających dodatkowych badań i reagowania.

Kluczowe korzyści

Rozszerzając możliwości poza tradycyjne funkcje EPP, Endpoint Security XDR zapewnia analitykom bezpieczeństwa i zespołom reagowania na incydent narzędzia, których potrzebują do analizowania podejrzanych działań oraz do badania zaawansowanych zagrożeń i odpowiedniego na nie reagowania, takiego jak:

- Wyświetlanie podejrzanych działań

- Analiza zagrożeń przy pomocy jednego kliknięcia
- Klasyfikacja alertów i wizualizacja analizy zdarzeń
- Śledzenie ataków i zmian w systemie
- Natychmiastowa reakcja
- Redukcja przestojów w działaniu poprzez szybkie znajdowanie rozwiązań, zabezpieczanie i naprawę



Rysunek 2. Strona szczegółów zdarzeń zapewnia przejrzysty podgląd zasięgu danego zdarzenia. Umożliwia to weryfikację i podjęcie odpowiednich działań.

Popraw optykę bezpieczeństwa, unikaj męczących alarmów

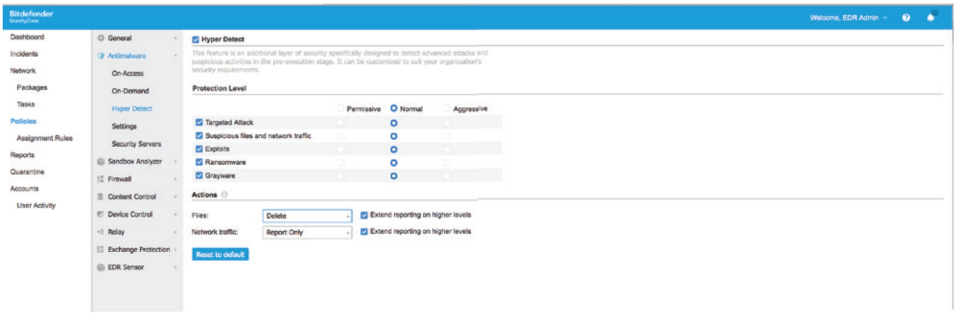
Tylko istotne, skorelowane i ocenione zdarzenia są poddawane ręcznej analizie, a następnie rozwiązywane. Zakłócenia i zbędne informacje są utrzymywane na minimalnym poziomie, ponieważ zdecydowana większość ataków i zaawansowanych ataków jest blokowana na etapie przed lub w trakcie wykonania. Zagrożenia takie jak oprogramowanie fileless, exploity, oprogramowanie ransomware i ukryte złośliwe oprogramowanie są neutralizowane dzięki wysoce skutecznej wielowarstwowej technologii ochrony punktów końcowych nowej generacji oraz dzięki behawioralnemu inspektorowi procesów. Automatyczna reakcja i naprawa eliminują potrzebę interwencji ze strony użytkownika.

Wysokiej jakości wykrywanie pozwala personelowi bezpieczeństwa skupić się tylko na istotnych incydentach i zagrożeniach:

- Minimalizacja zakłóceń spowodowanych fałszywymi alarmami
- Zmniejszenie liczby incydentów dzięki skutecznemu zapobieganiu zagrożeniom
- Eliminacja ręcznego usuwania zablokowanych ataków dzięki automatycznym działaniom naprawczym

Inteligentne reagowanie to lepsza profilaktyka

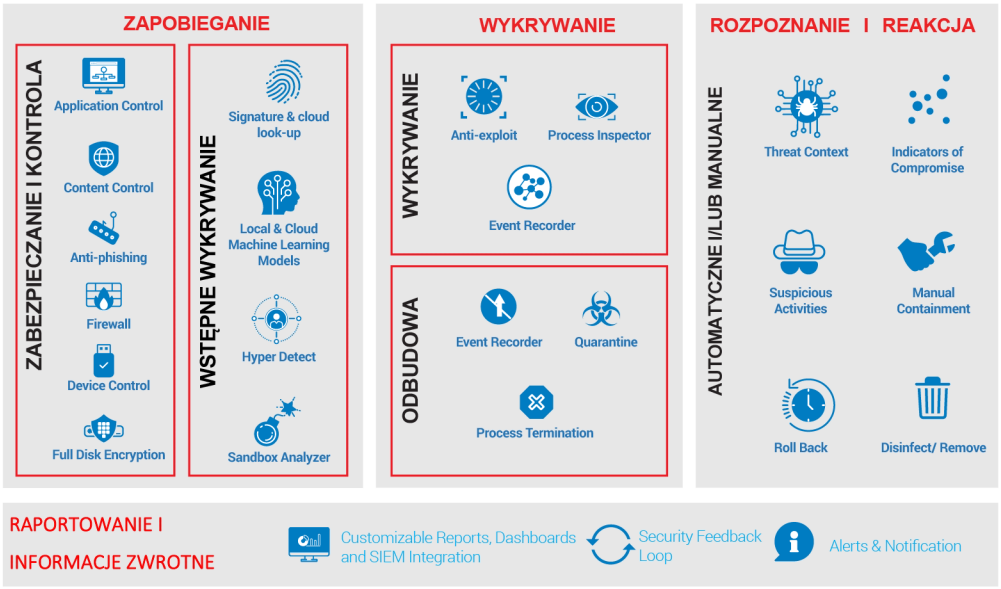
GravityZone Ultra jest zintegrowanym rozwiązaniem zapobiegającym, wykrywającym oraz naprawczym. Umożliwia ono szybką reakcję i przywracanie punktów końcowych do stanu jeszcze lepszego niż przed interwencją. Wykorzystując informacje o zagrożeniach zebrane z punktów końcowych podczas procesu sprawdzania, pojedynczy interfejs zapewnia narzędzia do natychmiastowego dostosowania luki w polityce i uaktualnieniach, dzięki czemu zapobiega przyszłym incydentom, poprawiając bezpieczeństwo środowiska.



Kompleksowa platforma bezpieczeństwa punktów końcowych w jednym agencie i konsoli

GravityZone Ultra posiada wszystkie zabezpieczenia i kontrole zawarte w Endpoint Security HD i pakiecie GravityZone Elite:

- Minimalizacja narażenia systemu na zagrożenia dzięki silnej profilaktyce
- Uczenie maszynowe i wykrywanie oparte na modelu behawioralnym powstrzymuje nieznane zagrożenia na etapie wstępnych i kolejnych działań
- Wykrywanie i blokowanie złośliwych skryptów, podejrzanego, niestandardowego złośliwego oprogramowania oraz oprogramowania fileless, wraz z automatyczną naprawą
- Ochrona pamięci w celu zapobiegania exploitom
- Redukcja płaszczyzny ataku dzięki kontroli bezpieczeństwa IT
- Zintegrowana zapora sieciowa, kontrola urządzeń, filtrowanie treści WWW, kontrola aplikacji, zarządzanie uaktualnieniami i wiele więcej

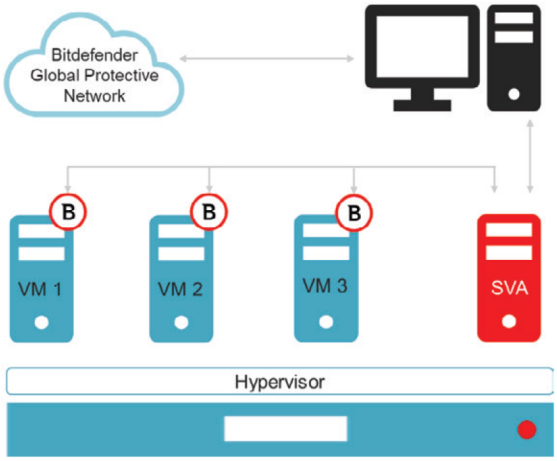


Rysunek 3. Bitdefender XDR: Kompleksowa platforma bezpieczeństwa końcowego

Ochrona Bazy Danych

Security for Virtualized Environments (SVE) to w pełni integrujący się z Bitdefender Endpoint Security XDR komponent Ochrony Danych pakietu GravityZone Elite. Jest to najbardziej zaawansowane rozwiązanie do ochrony wirtualizacji centrów danych na rynku ochrony przed złośliwym oprogramowaniem dla maszyn wirtualnych, optymalizujące nie tylko stopień konsolidacji, ale także koszty operacyjne. GravityZone SVE to rozwiązanie dla przedsiębiorstw, które może obsługiwać nawet największe centra danych. Integracja w środowisku produkcyjnym jest prosta, a z technologii mogą korzystać srodowiska wirtualne dowolnej wielkości.

Kluczowe Korzyści



Sprawność

SVE umożliwia automatyzację bezpieczeństwa w całym cyklu życia centrum danych podczas wdrażania, jak również podczas codziennych operacji bezpieczeństwa w bardzo dynamicznym środowisku wirtualnym. Integruje się z VMware (vCenter, vShield, NSX), Citrix XenCenter i Nutanix Enterprise Cloud Platform i umożliwia szybkie automatyczne przydzielanie zasobów.

Wydajność operacyjna

Zunifikowana konsola zarządzania GravityZone Control Center upraszcza wdrażanie, obsługę i aktualizacje zabezpieczeń, zapewniając scentralizowaną widoczność na wszystkich wirtualnych i fizycznych serwerach oraz stacjach roboczych. Obsługuje scentralizowane tworzenie i automatyczne administrowanie politykami bezpieczeństwa w celu usprawnienia operacji IT przy jednoczesnym zwiększeniu ich zgodności.

Lepsze wykorzystanie infrastruktury

Scentralizowane skanowanie i niepochłaniający dużej ilości zasobów agent znacznie zmniejszają wykorzystanie pamięci, miejsca na dysku, procesora i operacji I/O na serwerach hosta, zwiększając gęstość maszyn wirtualnych i zwrot z inwestycji w infrastrukturę IT.

Zunifikowana kompatybilność
Kompatybilne ze wszystkimi wiodącymi platformami hypervisor (VMware ESXi, Microsoft Hyper-V, Citrix Xen, Red Hat KVM i Nutanix AHV) oraz systemami operacyjnymi Windows i Linux.

Nieograniczona skalowalność liniowa
Gdy centrum danych się rozrasta i tworzonych jest coraz więcej maszyn wirtualnych, aby zwiększyć wydajność skanowania można wykorzystać większą ilość urządzeń SVA (Security Virtual Appliance). Gdy istniejące SVA osiągają pewien próg obciążenia, można wdrożyć kolejne. Dodatkową korzyścią z wdrożenia wielu SVA jest poprawa odporności i współdzielenia obciążenia: obciążenie z nieudanej/przeciążonej SVA może zostać przejęte przez inną aktywną lub mniej obciążoną SVA.

Wielowarstwowa ochrona nowej generacji
GravityZone Security for Virtualized Environments zawiera wszystkie kluczowe warstwy zabezpieczeń Endpoint Security, w tym HyperDetect, Sandbox Analyzer i metody wykrywania fileless, które zapewniają wiodącą ochronę zasobów cyfrowych przedsiębiorstwa przechowywanych lub przetwarzanych w centrum danych

Funkcje

- Zaprojektowany, aby umożliwić transformację centrów danych: SDDC, hiperkonwergencja i chmura hybrydowa
- Kompleksowa integracja z VMware, Nutanix, Citrix, AWS i Microsoft w celu ochrony inwestycji, automatyzacji wdrażania oraz zarządzania zasobami i licencjami
- Obsługa wielu środowisk wirtualizacji i chmury już od pierwszego wdrożenia
- Widoczność i scentralizowane zarządzanie w chmurze hybrydowej
- Wydajna, odporna i skalowalna architektura oparta na architekturze SVA obsługującej wszystkie hipervisory
- Zmaksymalizowana gęstość maszyn wirtualnych, minimalne opóźnienie rozruchu i optymalna wydajność aplikacji
- Zaawansowane warstwowe zabezpieczenia obejmujące chmurę hybrydową

GravityZone Control Center

GravityZone Control Center to wielofunkcyjne narzędzie do scentralizowanego zarządzania bezpieczeństwem, w tym bezpieczeństwem punktów końcowych, bezpieczeństwem centrum danych, zabezpieczeniami Exchange i zabezpieczeniami urządzeń mobilnych. Może być hostowany w chmurze lub wdrażany lokalnie. Centrum zarządzania GravityZone obejmuje wiele ról i zawiera bazę danych serwera, serwer aktualizacji i konsolę internetową. Centrum sterowania jest dostarczane jako urządzenie wirtualne i można je wdrożyć w ciągu zaledwie 30 minut.
W przypadku większych przedsiębiorstw możliwe jest korzystanie z wielu urządzeń z wbudowanym modułem równoważenia obciążenia w celu zapewnienia lepszej skalowalności i wysokiej dostępności.

Szczegółowe wymagania systemowe można znaleźć na stronie www.bitdefender.com/business/ultra-security

BD-NGZ-Nov.14-2017-TH
Bitdefender-NGZ-UltraSuite-Datasheet-creat2199-A4-en_EN