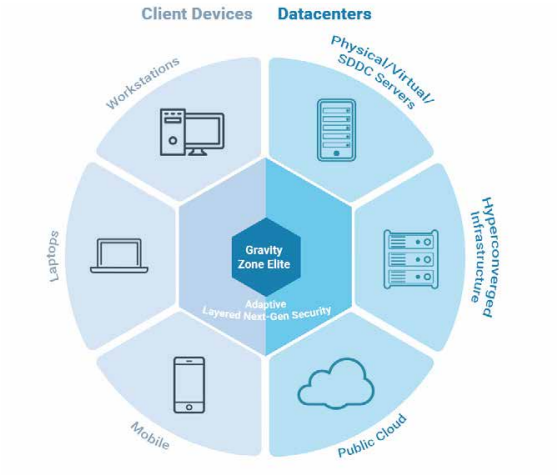
Bitdefender GravityZone Elite Security

Wielowarstwowa Platforma Bezpieczeństwa Nowej Generacji

Pakiet Bitdefender GravityZone Elite został zaprojektowany, aby szybko i skutecznie chronić przedsiębiorstwa przed pełnym spektrum wyrafinowanych zagrożeń cybernetycznych. Elite łączy sprawdzone, warstwowe podejście bezpieczeństwa Bitdefender z narzędziami i technologiami nowej generacji, aby zapewnić wysoką wydajność i ochronę wszystkich punktów końcowych w środowisku przedsiębiorstwa: komputerów stacjonarnych, laptopów, telefonów komórkowych, serwerów fizycznych i wirtualnych.

GravityZone Elite zapewnia spójny poziom bezpieczeństwa całego środowiska informatycznego, ograniczając słabo chronione punkty końcowe, które mogą służyć jako punkt wyjścia dla złośliwych działań przeciwko organizacji. Opiera się na prostej, zintegrowanej architekturze ze scentralizowanym zarządzaniem zarówno punktami końcowymi, jak i centrum danych. Konsole cloud i on-premise pasują zarówno do środowiska w chmurze, jak i do ściśle regulowanych środowisk.



KLUCZOWE CECHY

- Wykrywanie i blokowanie ataków file-less
- Zatrzymywanie ataków opartych na skryptach
- Rozpakowywanie i analizanieznanego złośliwego oprogramowania na etapie przed wykonaniem
- Pojedynczy agent, niewielki rozmiar i niski wpływ na system
- Zintegrowana konsola zarządzania dla fizycznych i wirtualnych punktów końcowych

Ochrona Punktu Końcowego

Bitdefender Endpoint Security HD - komponent bezpieczeństwa punktu końcowego GravityZone Elite - chroni przedsiębiorstwa przed pełnym spektrum zaawansowanych zagrożeń cybernetycznych z szybkością, dokładnością, przy jednoczesnym niskim obciążeniu administracyjnym i minimalnym wpływie na system. To rozwiązanie nowej generacji eliminuje potrzebę uruchamiania wielu rozwiązań zabezpieczających punkty końcowe na jednym komputerze - łączy w sobie kontrole prewencyjne, wieloetapowe techniki wykrywania bez sygnatur i automatyczne reagowanie.

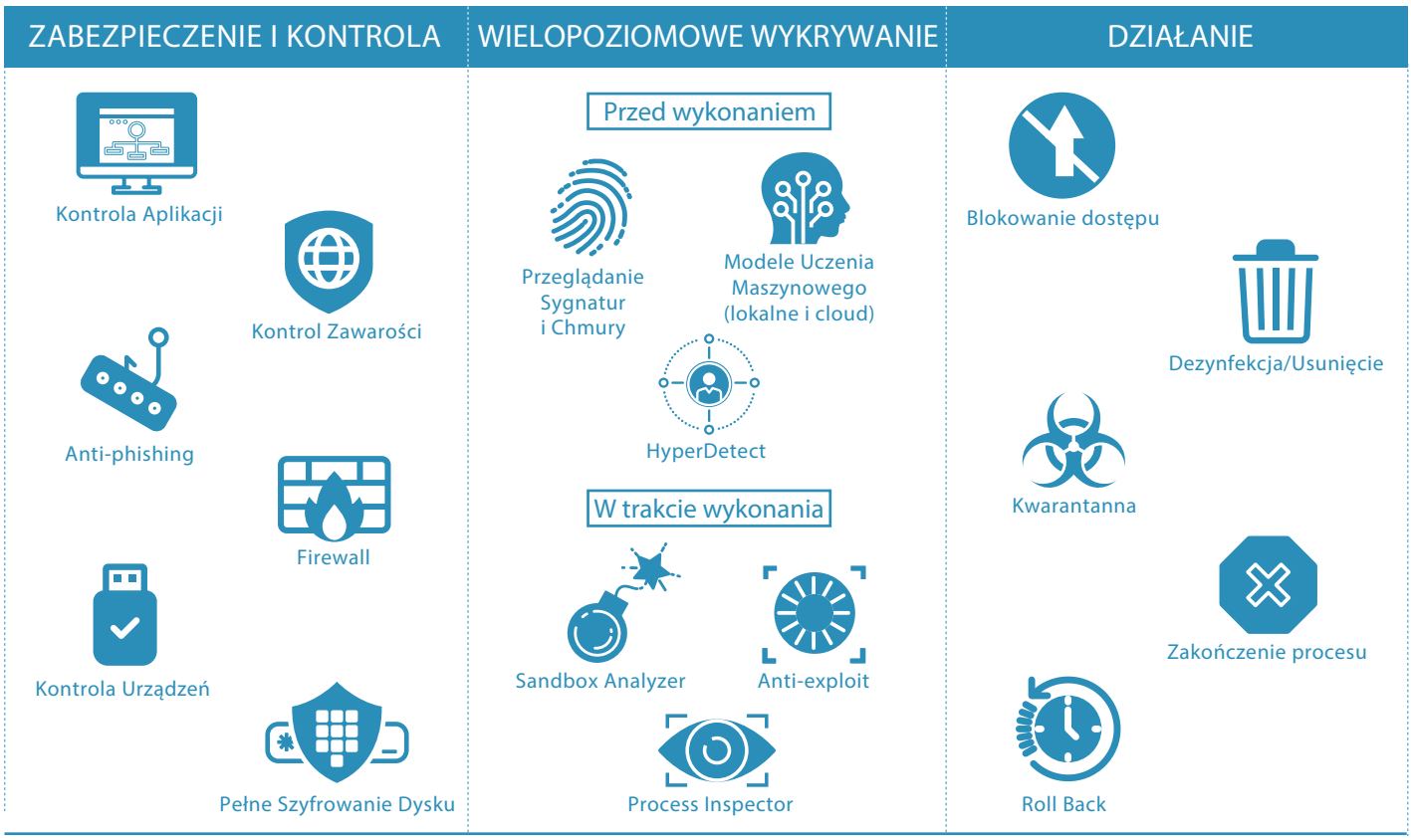
Kluczowe korzyści

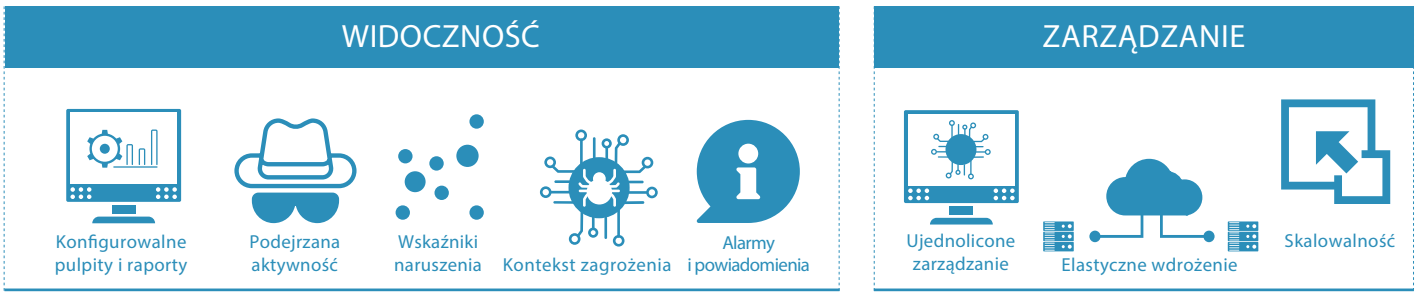
Wykrywanie i zapobieganie całej gamie zaawansowanych zagrożeń i nieznanego złośliwego oprogramowania

Endpoint Security HD zwalcza zaawansowane zagrożenia i nieznane złośliwe oprogramowanie (w tym ransomware), które potrafią ominąć tradycyjne rozwiązania ochrony punktów końcowych. Zaawansowane ataki, takie jak PowerShell, ataki oparte na skryptach, ataki fileless oraz zaawansowane złośliwe oprogramowanie mogą zostać wykryte i zablokowane przed wykonaniem.

Zatrzymuje ataki makro i ataki oparte na skryptach

W tym przypadku atakującym jest zaufane macro MS Office, które używa narzędzi administracyjnych Windows, takich jak PowerShell, aby uruchamiać skrypty i pobierać złośliwy kod do wykonania ataku. Traktując je jako „zaufane" narzędzia Windows, większość produktów do ochrony punktów końcowych, w tym tzw. dostawcy AV nowej generacji, nie analizuje skryptów, takich jak Powershell, WMI, interpretatory Javascript itp. Bitdefender korzysta z technik Command-line Analyzer (analiza wiersza poleceń) w celu przechwytywania i zabezpieczania skryptów, powiadamiania administratorów i blokowania uruchamiania skryptu, jeśli wykonuje on złośliwe polecenia.





Wykrywanie i powstrzymywanie złośliwego oprogramowania fileless

Ataki oprogramowania fileless wykonują złośliwy kod bezpośrednio w pamięci, dlatego większość rozwiązań AV przeznaczonych do analizy plików nie jest w stanie ich wykryć. Bitdefender wykorzystuje Advanced Anti-Exploit, HyperDetec™ i Process Inspector do wykrywania, blokowania i zatrzymywania ataków fileless.

Przesyła informacje o zagrożeniach w czasie rzeczywistym do GPN (Globalnej Sieci Ochrony), opartej na chmurze usłudze analizy zagrożeń Bitdefender, zapobiegając podobnym atakom na całym świecie.

Zwiększona wydajność operacyjna dzięki pojedynczemu agentowi i zintegrowanej konsoli

Pojedynczy, zintegrowany agent bezpieczeństwa punktów końcowych Bitdefender eliminuje przeciążenie agenta. Modularna konstrukcja zapewnia maksymalną elastyczność i pozwala administratorom określić polityki bezpieczeństwa. GravityZone automatycznie dostosowuje pakiet instalacyjny i minimalizuje wpływ agenta. Zaprojektowany od podstaw dla post-wirtualizacyjnych i post-cloudowych architektur bezpieczeństwa, GravityZone zapewnia ujednoliconą platformę zarządzania bezpieczeństwem w celu ochrony fizycznych, zwirtualizowanych i chmurowych środowisk.

Funkcje

Uczenie Maszynowe

Techniki uczenia maszynowego wykorzystują dobrze wyszkolone modele maszyn i algorytmów do przewidywania i blokowania zaawansowanych ataków. Modele uczenia maszynowego Bitdefender wykorzystują 40 000 statycznych i dynamicznych funkcji i są nieustannie szkolone na miliardach czystych i złośliwych próbek zbieranych z ponad 500 milionów punktów końcowych na całym świecie. To znacznie poprawia skuteczność wykrywania złośliwego oprogramowania i minimalizuje liczbę fałszywych alarmów.

Dodatkowo wykrywa techniki dostarczania złośliwego oprogramowania i witryny, które obsługują zestawy exploitów oraz blokuje podejrzany ruch internetowy.
HyperDetect pozwala administratorom zabezpieczeń dostosować ochronę, aby jak najlepiej przeciwdziałać zagrożeniom, na jakie narażona jest organizacja. Dzięki opcji „Tylko raportuj" administratorzy bezpieczeństwa mogą tworzyć i monitorować nową politykę bezpieczeństwa przed rozpoczęciem wdrożenia, eliminując tym samym przerwy w działalności firmy. Duża widoczność i blokowanie zagrożeń pozwalają użytkownikom ustawić HyperDetect na blokowanie na normalnym lub dopuszczalnym poziomie, pozostawiając raportowanie na poziomie agresywnym, dzięki czemu ujawniane są wczesne wskaźniki naruszenia.

HyperDetect

Ta nowa warstwa ochrony działająca na etapie przed wykonaniem obejmuje lokalne modele uczenia maszynowego i zaawansowaną heurystykę, przeszkoloną do wykrywania narzędzi hakerskich, exploitów i technik zaciemniania złośliwego oprogramowania w celu blokowania zaawansowanych zagrożeń przed ich wykonaniem.

Zintegrowany z agentem GravityZone Endpoint, Sandbox Analyzer automatycznie przesyła podejrzane pliki do analizy. Jeśli plik analizowany w Sandboxie okazuje się złośliwy, Endpoint Security HD automatycznie blokuje go na wszystkich systemach w całym przedsiębiorstwie. Funkcja automatycznego przesyłania pozwala administratorom bezpieczeństwa wybrać tryb „monitorowania" lub „blokowania", który uniemożliwia dostęp do pliku do czasu otrzymania wyniku analizy. Administratorzy mogą również manualnie przesyłać pliki do analizy. Bogata baza analityczna Sandbox Analyzer daje jasny kontekst zagrożeń i pomaga zrozumieć ich zachowanie.

Zaawansowany Anti-Exploit

Technologia zapobiegania exploitom chroni pamięć i podatne na ataki aplikacje, takie jak przeglądarki, czytniki dokumentów, pliki multimedialne i runtime (np. Flash, Java). Zaawansowane mechanizmy monitorują procedury dostępu do pamięci w celu wykrywania i blokowania technik exploit, takich jak weryfikacja połączeń API, stack pivot, return-oriented-programming (ROP) i inne.

Inspektor Procesów

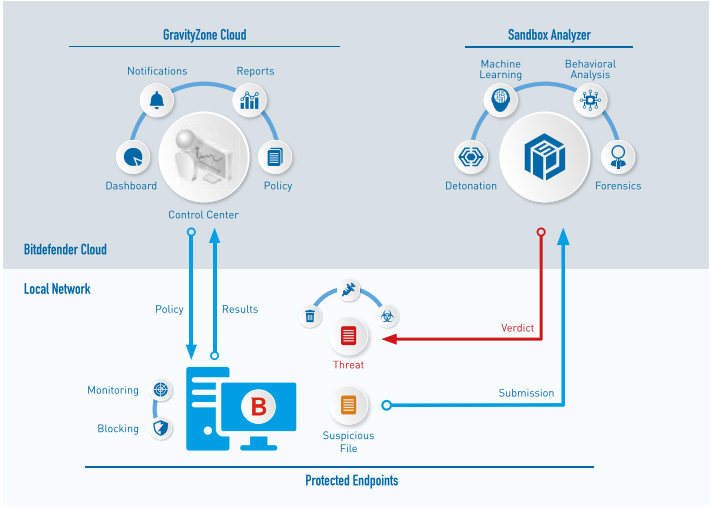
Inspektor Procesów działa w trybie zerowego zaufania, stale monitorując wszystkie procesy uruchomione w systemie operacyjnym. Wyszukuje podejrzane działania lub nietypowe zachowania procesów, takie jak próby ukrycia typu procesu, wykonanie kodu w obszarze innego procesu (przejęcie kontroli nad pamięcią procesu w celu zwiększenia uprawnień), replikowanie, upuszczanie plików, ukrywanie się przed aplikacjami numerującymi procesy i więcej. Podejmuje odpowiednie działania naprawcze, w tym zakończenie procesu i cofnięcie zmian wprowadzonych przez proces. Jest bardzo skuteczny w wykrywaniu nieznanego, zaawansowanego złośliwego oprogramowania, w tym ransomware.

Anti-phishing i filtrowanie zabezpieczeń sieci Web

Filtrowanie zabezpieczeń sieci Web umożliwia skanowanie przychodzącego ruchu sieciowego w czasie rzeczywistym, w tym ruchu SSL, http i https, aby zapobiec pobieraniu złośliwego oprogramowania na punkt końcowy. Ochrona antyphishingowa automatycznie blokuje phishing i fałszywe strony internetowe.

Sandbox Analyzer zintegrowany z punktem końcowym

Potężna warstwa ochrony przed zaawansowanymi zagrożeniami dogłębnie analizuje podejrzane pliki, detonuje ładunki w zamkniętym środowisku wirtualnym hostowanym przez Bitdefender, analizuje ich zachowanie i zgłasza złośliwe ich zamiary.



Sandbox Analyzer zintegrowany z punktem końcowym

Potężna warstwa ochrony przed zaawansowanymi zagrożeniami dogłębnie analizuje podejrzane pliki, detonuje ładunki w zamkniętym środowisku wirtualnym hostowanym przez Bitdefender, analizuje ich zachowanie i zgłasza złośliwe ich zamiary.

Pełne Szyfrowanie Dysku

Zarządzane przez GravityZone Pełne Szyfrowanie Dysku używające Windows BitLockera i Mac FileVault bazuje na technologiach wbudowanych w systemy operacyjne.

Zabezpieczenie i kontrola punktów końcowych

Kontrola punktów końcowych bazująca na politykach obejmuje zaporę sieciową, kontrolę urządzeń przy użyciu skanowania USB oraz kontrolę zawartości sieci przy pomocy kategoryzacji adresów URL.

Reagowanie i powstrzymywanie zagrożeń

GravityZone oferuje najlepszą na rynku technologię oczyszczania. Automatycznie blokuje/powstrzymuje zagrożenia, zabija złośliwe procesy i wycofuje zmiany.

Ochrona Centrum Danych

GravityZone Security for Virtualized Environments (SVE) wykorzystuje warstwowe zabezpieczenia nowej generacji - Bitdefender Endpoint Security HD, aby zapewnić przedsiębiorstwom najlepszą w swojej klasie ochronę dla serwerów, VDI i obciążeń w chmurze, jednocześnie maksymalizując wydajność infrastruktury i wydajność operacyjną. GravityZone SVE został zaprojektowany jako rozwiązanie biznesowe będące w stanie wspierać nawet największe centra danych.

Kluczowe Korzyści

Elastyczność

SVE umożliwia automatyzację zabezpieczeń centrów danych w całym ich okresie użytkowania - podczas wdrożenia, jak i podczas codziennych operacji z zakresu bezpieczeństwa w mocno dynamicznym środowisku wirtualnym. Integruje się z VMware (vCenter, vShield, NSX), Citrix XenCenter i Nutanix Enterprise Cloud Platform oraz umożliwia szybkie zautomatyzowane udostępnianie.

Wydajność Operacyjna

Ujednolicona konsola zarządzania GravityZone Control Center upraszcza wdrażanie, obsługę i aktualizację zabezpieczeń, zapewniając scentralizowaną widoczność wszystkich wirtualnych i fizycznych serwerów i stacji roboczych. Obsługuje scentralizowane tworzenie i automatyczne administrowanie zasadami bezpieczeństwa, aby usprawnić operacje IT przy jednoczesnej poprawie zgodności.

Lepsze wykorzystanie infrastruktury

Scentralizowane skanowanie i niewielki rozmiar śladu generowanego przez agenta w znaczący sposób zmniejszają użycie pamięci, przestrzeni dyskowej, procesora i aktywność urządzeń wejścia / wyjścia na serwerach hosta, zwiększając gęstość wirtualizacji i ROI na infrastrukturze IT.

Uniwersalna kompatybilność

Kompatybilny ze wszystkimi platformami wirtualizacji (takimi jak VMware® ESXiTM, Microsoft® Hyper-VTM, Citrix® XenServer®, Red Hat® Enterprise Virtualization®, KVM i Nutanix® Acropolis), Microsoft Active Directory oraz systemami operacyjnymi gości Windows® i Linux®. GravityZone upraszcza wdrażanie, wykrywanie punktów końcowych i zarządzanie politykami.

Warstwowa ochrona nowej generacji

GravityZone Security for Virtualized Environments zawiera wszystkie kluczowe warstwy zabezpieczeń Endpoint Security, w tym HyperDetect, Sandbox Analyzer i metody wykrywania ataków file-less. Zapewnia wiodącą ochronę cyfrowych zasobów przedsiębiorstwa przechowywanych lub przetwarzanych w centrum danych.

Ochrona urządzeń mobilnych z systemem iOS i Android

Rozwiązanie zostało zaprojektowane tak, aby umożliwić kontrolowaną adaptację koncepcji bring-your-own-device (BYOD) poprzez konsekwentne egzekwowanie polityk bezpieczeństwa na wszystkich urządzeniach użytkownika. Dzięki temu urządzenia są pod kontrolą, a znajdujące się na nich poufne dane firmowe są chronione. Aktualizowanie statusu zgodności/niezgodności urządzeń znacznie redukuje obciążenia administracyjne.

Ochrona serwerów Exchange

Zapewnia wielowarstwową ochronę wiadomości: antyspam, antyphishing, antywirus i antymalware z analizą behawioralną i ochroną przed zagrożeniami zero-day oraz filtrowaniem ruchu email, w tym filtrowaniem załączników i treści. Skanowanie antymalware może być wyładowywane z chronionych serwerów pocztowych do scentralizowanych serwerów bezpieczeństwa. Zarządzanie i raportowanie są scentralizowane, co umożliwia stosowanie ujednoliconych zasad dotyczących punktów końcowych i przesyłania wiadomości.

GravityZone Control Center

GravityZone Control Center to zintegrowana i scentralizowana konsola zarządzania, która zapewnia wgląd we wszystkie komponenty zarządzania bezpieczeństwem, w tym bezpieczeństwo punktu końcowego, bezpieczeństwo centrum danych, bezpieczeństwo Exchange i bezpieczeństwo urządzeń mobilnych. Może być hostowany w chmurze lub wdrożony lokalnie. Centrum zarządzania GravityZone obejmuje wiele ról i zawiera serwer bazy danych, serwer komunikacyjny, serwer aktualizacji i konsolę internetową. Dla większych przedsiębiorstw istnieje możliwość konfiguracji wielu urządzeń wirtualnych z wieloma instancjami określonych ról z wbudowanym balansem obciążenia dla skalowalności i wysokiej dostępności.

Szczegółowe wymagania systemowe znajdują się na:

https://bitdefender.pl/gravityzone-elite-security/

Bitdefender

Bitdefender jest światowym dostawcą zabezpieczeń, który zapewnia najnowocześniejsze kompleksowe rozwiązania bezpieczeństwa ponad 500 milionom użytkowników w ponad 150 krajach. Bitdefender od 2001 roku tworzy nagradzane technologie zabezpieczeń dla firm i konsumentów oraz dostarcza rozwiązania z zakresu bezpieczeństwa infrastruktury hybrydowej i ochrony punktów końcowych. Dzięki R&D, współpracy i partnerstwu, Bitdefender ma wiodącą pozycję na rynku, zapewniając niezawodne zabezpieczenia, na których można polegać. Więcej informacji znajduje się na stronie: http://www.bitdefender.com.