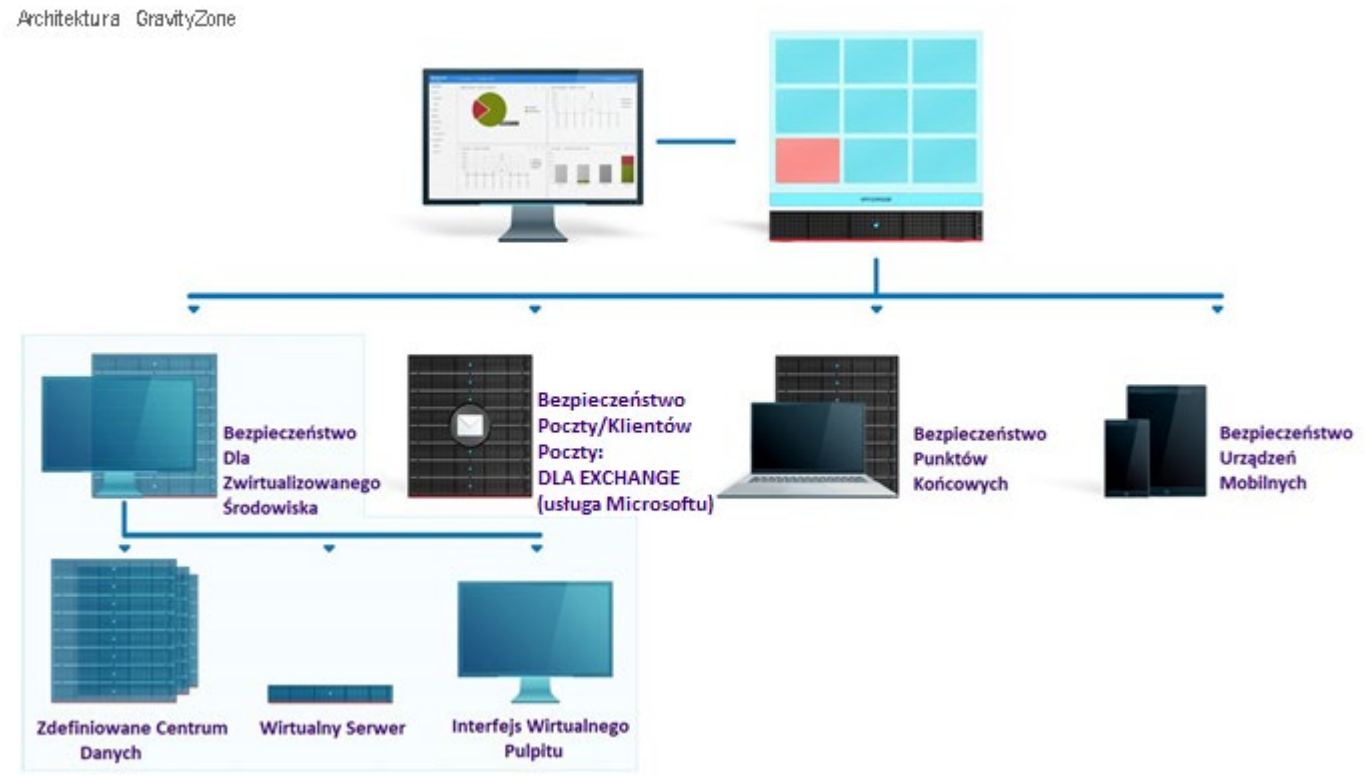
Bitdefender

GravityZone

Bezpieczeństwo dla środowisk wirtualnych

Nie pozwól, aby Twoja ochrona przed wirtualizacją spowalniała infrastrukturę. Bezpieczeństwo i wydajność mogą współistnieć w chmurze i w zwirtualizowanych centrach danych. GravityZone oferuje niskoprofilową usługę bezpieczeństwa, która pomaga firmom zarządzać ryzykiem IT bez utraty korzyści płynących ze skalowalnej infrastruktury.

GravityZone został zaprojektowany od podstaw i przeznaczony przede wszystkim do wirtualizacji i do zastosowania w chmurze obliczeniowej. GravityZone ma na celu dostarczanie klientowi biznesowemu usług bezpieczeństwa dla fizycznych punktów końcowych, urządzeń mobilnych, maszyn wirtualnych w chmurze prywatnej, publicznej i serwerów pocztowych Exchange.



Bitdefender GravityZone Enterprise Security dla zwirtualizowanych środowisk (SVE) to najbardziej zaawansowane rozwiązanie w sferze bezpieczeństwa wirtualnych centrów danych na rynku, zapewnia ochronę antywirusową maszyn wirtualnych, optymalizuje współczynniki konsolidacji oraz koszty operacyjne. GravityZone SVE został zaprojektowany jako rozwiązanie korporacyjne zdolne do obsługi największych centrów danych. Integracja ze środowiskiem produkcyjnym jest jednak bardzo prosta, a korzyści technologiczne można uzyskać w środowiskach wirtualnych dowolnej wielkości.

Główne zalety

Wsparcie dla VMware, Microsoft Hyper-V, Citrix XenServer, Red Hat Enterprise Virtualization (with KVM) oraz innych.

Chroni maszyny wirtualne z systemem Microsoft i głównymi dystrybucjami Linuksa.

Wykorzystuje NSX we wdrożeniach dla VMware, aby zapewnić najwyższe możliwe bezpieczeństwo, które zostało zaprojektowane i stworzone specjalnie dla Software-Defined Data Center (Centrum Danych Zdefiniowanych przez Oprogramowanie).

Głęboko integruje się z nieograniczoną liczbą wdrożeń VMware vCenter, pozwalając na prowadzenie polityki zarządzania bezpieczeństwem w oparciu o obiekty takie jak pule zasobów, foldery i sieci rozproszone.

Eliminuje pojedyncze przypadki awarii i wąskich gardeł, zapewniając jednocześnie niezrównaną skuteczność ochrony antywirusowej.

Bitdefender zapewnia wielokrotnie nagradzaną ochronę przed złośliwym oprogramowaniem w systemach plików, pamięci, procesach i bazach danych rejestrów, otaczając ochroną każdą wirtualną maszynę.

PRZEGLĄD TECHNOLOGII

GravityZone SVE zapewnia ochronę antymalware za pomocą wirtualnych urządzeń zabezpieczających (Serwery Bezpieczeństwa), działających jako scentralizowane punkty inteligencji antywirusowej, bez konieczności instalowania tradycyjnego modułu zabezpieczającego w każdej maszynie wirtualnej. Tradycyjny moduł wymagałby ciągłej aktualizacji i monitorowania oraz zużywałby znaczne zasoby lokalne do działania. Każda maszyna wirtualna łączy się z serwerem bezpieczeństwa w celu odciążenia większości funkcji antymalware, obejmujących skanowanie systemu plików, pamięci, procesów i rejestrów zarówno w systemie Windows, jak i Linux.
GavityZone SVE wykorzystuje wielowarstwowy mechanizm buforowania, który przyczynia się do zwiększenia wydajności. Po pierwsze, lokalna pamięć podręczna jest utrzymywana w obrębie każdej maszyny wirtualnej, więc obiekty są skanowane tylko raz. Po drugie, na każdym serwerze bezpieczeństwa utrzymywana jest współdzielona pamięć podręczna, dzięki czemu obiekty skanowane na jednej maszynie wirtualnej nie są skanowane na drugiej. Wreszcie, seria pamięci podręcznych na poziomie bloków plików sprowadza deduplikację skanowania do poziomu fragmentów plików, co oznacza, że pliki z kilkoma różnymi blokami interesującymi dla silników antywirusowych na serwerze bezpieczeństwa nie są skanowane całkowicie ponownie. W rezultacie użycia unikalnych technologii Bitdefender GravityZone SVE może poszczycić się niezwykłym wzrostem wydajności.
Cały szereg nagradzanych technologii ochrony przed zagrożeniami Bitdefender jest wbudowany w silniki zabezpieczające oraz w architekturę urządzeń wirtualnych. Dzięki SVE ochrona antymalware przed złośliwym oprogramowaniem jest skuteczniejsza niż kiedykolwiek, zapewniając wiodącą ochronę i wysoce dostępną, natychmiastową ochronę dla każdej maszyny wirtualnej w centrum danych.
Bitdefender GravityZone jest wyposażony w potężną kombinację technologii zabezpieczających, które umożliwiają obsługę wszystkich rodzajów zagrożeń, od złośliwego oprogramowania po najbardziej zaawansowane ataki ukierunkowane. Dzięki takim technologiom, jak Zaawansowana Kontrola Zagrożeń, potężny anty-exploit, wielokrotnie nagradzany system antyspamowy i filtrowanie treści, a także wielowarstwową ochronę przed złośliwym oprogramowaniem, Bitdefender zajmuje najwyższe miejsce w niezależnych testach, z ponad 99% wskaźnikiem wykrywania nowych lub nieznanych zagrożeń.
*Cały szereg nagradzanych technologii ochrony przed zagrożeniami Bitdefender jest wbudowany w silniki zabezpieczające oraz w architekturę urządzeń wirtualnych. Dzięki SVE ochrona antymalware przed złośliwym oprogramowaniem jest skuteczniejsza niż kiedykolwiek, zapewniając wiodącą ochronę i wysoce dostępną, natychmiastową ochronę dla każdej maszyny wirtualnej w centrum danych.

BITDEFENDER ENDPOINT SECURITY TOOLS (BEST)- SKANOWANIE CENTRALNE W SKRÓCIE

Aby Security Server (serwer bezpieczeństwa) miał dostęp do systemu plików każdej maszyny wirtualnej, wraz z pamięcią, rejestrem i uruchomionymi procesami oraz innymi wymaganymi funkcjami, do każdej maszyny wirtualnej musi zostać wdrożony zestaw usług pomocniczych, dostarczanych w ramach centralnego skanowania. Skanowanie centralne charakteryzuje się następującymi cechami:

Małe obciążenie systemu:

- Mniej niż 110 MB pamięci masowej w czasie pracy (włącznie z pamięcią podręczną)
- 10-20 MB pamięci lokalnej w czasie pracy (skanowanie w trybie dostępu)
- Szczytowe obciążenie procesora 1-2%, na pojedynczym wirtualnym procesorze dla skanowania dostępowego.

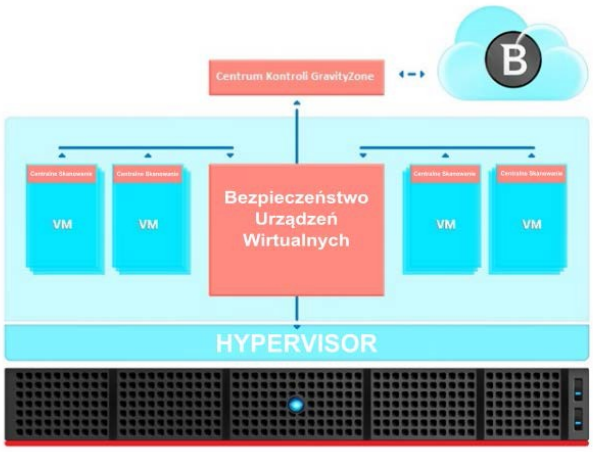
Podstawowe funkcje:

- Ustanawia połączenie z dostępnym autoryzowanym serwerem bezpieczeństwa (urządzeniem wirtualnym), umożliwiającym lokalny dostęp do systemu plików, rejestru, pamięci i procesów.
- Przełącza połączenie na alternatywny serwer bezpieczeństwa w przypadku wolnego czasu reakcji lub nagłej niedostępności.
- Zarządza lokalną dezynfekcją, kwarantanną i blokadą procesów.
- Utrzymuje lokalną pamięć podręczną skanowanych elementów w celu zwiększenia wydajności.
- Działa jako usługa lokalna z usuniętymi wszystkimi uprawnieniami administracyjnymi, chroniącymi przed atakami próbującymi wyłączyć ochronę lokalnie.
- Opcjonalnie zapewnia interfejs użytkownika wewnątrz maszyny wirtualnej z wyskakującymi powiadomieniami na pulpicie.
- Wdrożenie centralnego skanowania (dostępne zarówno w wersji dla systemu Windows, jak i Linux) jest proste i nie wymaga ponownego uruchamiania maszyn wirtualnych, natomiast wdrożenie Security Server nie wymaga ponownego uruchamiania maszyn, hostujących maszyny wirtualne.
- Skanowanie centralne można zapisać w szablonach i obrazach VDI, aby zminimalizować koszty zarządzania.

Unikalny projekt architektoniczny GravityZone ma kilka zalet:

- Wirtualne maszyny nie posiadają lokalnych silników skanujących antymalware i definicji, zawsze będą chronione przez dostępny serwer bezpieczeństwa.
- Eliminuje możliwość wystąpienia zjawiska AV Storms.
- Wielopoziomowe buforowanie na poszczególnych maszynach wirtualnych i serwerach bezpieczeństwa zapewnia, że unikalne pliki są skanowane tylko raz.
- Eliminuje czas uruchamiania i luki w zabezpieczeniach napotykane przy uruchamianiu maszyn wirtualnych.
- Brak pojedynczego punktu przerwania ochrony, ponieważ funkcja Central Scan (Centralne Skanowanie) automatycznie łączy się lub ponownie łączy z dostępnym serwerem bezpieczeństwa, zgodnie z ustalonymi regułami.
- Scentralizowana ochrona bez wąskich gardeł, ponieważ Centralne Skanowanie może automatycznie przełączyć się na inny serwer bezpieczeństwa z szybszym czasem reakcji.
- Nietrwałe (tymczasowe) maszyny wirtualne są automatycznie chronione i podlegają odpowiednim zasadom bezpieczeństwa (gdy Centralne Skanowanie jest zainstalowane na obrazie i polityka bezpieczeństwa jest stosowana do bazy zasobów lub folderu, wówczas maszyna wirtualna przejmie odpowiednią politykę bezpieczeństwa).

* AV-Comparatives Heuristic / Behaviour Tests, Marzec 2015



- Zwiększa zagęszczenie maszyn wirtualnych w wyniku zmniejszenia ilości pamięci, miejsca na dysku, CPU i aktywności I/O.
- Maszyny wirtualne są zawsze chronione przez najnowsze, aktualne technologie, nawet jeśli zostaną przywrócone do starszej wersji snapshot/backup lub uruchomione po dłuższym czasie w trybie offline.
- Po zainstalowaniu centralnego skanowania nie ma potrzeby monitorowania systemów AV na poszczególnych maszynach wirtualnych.

Generowanie niestandardowych i potężnych zapytań (kwerend) do baz danych GravityZone w celu uzyskania zaawansowanej analizy i wglądu w bezpieczeństwo Twojej sieci, jest możliwe za pomocą łatwego w użyciu interfejsu graficznego, który nie wymaga zaawansowanej wiedzy SQL do konfiguracji zapytań (dostępny tylko dla produktów Enterprise Security on-premise).

NIEZRÓWNANA WYDAJNOŚĆ

SVE został zaprojektowany w celu rozwiązania problemów związanych z uruchomieniem AV w środowisku zwirtualizowanym i jest stale ulepszany, z naciskiem na ochronę, prostotę, wydajność i kompatybilność.

Nasze szeroko zakrojone testy wydajności dowodzą, że SVE ma najniższy wpływ na wydajność spośród wszystkich głównych rozwiązań AV dostępnych na rynku, a jednocześnie zapewnia wielokrotnie nagradzaną ochronę firmy Bitdefender. Testy dowodzą, że dzięki temu dana firma może odzyskać do 17% mocy obliczeniowej hosta i zmniejszyć opóźnienia w stosunku do dotychczas stosowanego rozwiązania AV, jednocześnie obniżając koszty operacyjne, dzięki radykalnemu ograniczeniu konserwacji i monitorowania.

OPCJONALNIE INTEGRACJA NSX

W przypadku wykorzystania platformy VMware NSX, Bitdefender dostarcza wiodące usługi introspekcji gości, które są tworzone specjalnie dla centrum danych zdefiniowanego przez oprogramowanie, zapewniając ochronę przez dostarczenie bezagentowej ochrony, automatyczne wdrażanie i orkiestrację usług bezpieczeństwa w zwirtualizowanym środowisku.

ELASTYCZNE LICENCJONOWANIE DLA CENTRÓW DANYCH I INDYWIDUALNYCH MASZYN WIRTUALNYCH

GravityZone SVE wprowadza prosty model licencjonowania, według złącza procesora w centrum danych lub opcji zakupu maszyn wirtualnych. Licencjonowanie maszyn wirtualnych jest podzielone na serwery wirtualne i VDI w celu zapewnienia zgodności z dynamiczną i wysoce zwirtualizowaną infrastrukturą.

UJEDNOLICONE ZARZĄDZANIE

GravityZone SVE jest jedną z usług bezpieczeństwa dostarczanych przez ujednoliconą platformę GravityZone Enterprise Security i jest zarządzana poprzez internetowy interfejs "Centrum Kontroli" (Control Centre). Oprócz bezpieczeństwa maszyn wirtualnych, GravityZone Enterprise Security ochroną obejmuje fizyczne stacje robocze i serwery (Windows, Linux, Mac), urządzenia mobilne (Android, iOS) oraz serwery poczty Exchange.
GravityZone składa się z unikalnej architektury opartej na gotowym wirtualnym urządzeniu, które może być klonowane w zależności od obciążenia, przy czym każda z tych aplikacji pełni jedną lub więcej funkcji. Ten prosty, ale potężny model daje GravityZone przewagę skalowania poziomego, aby sprostać wymaganiom największych środowisk jako pojedyncze wdrożenie. Na przykład w San Francisco mogą działać trzy urządzenia wykorzystujące otwartą, chmuro-centryczną bazę danych GravityZone, z czego dwa w Nowym Jorku, podczas gdy podobna liczba serwerów komunikacyjnych jest rozproszona geograficznie tam, gdzie jest to konieczne. Urządzenia wirtualne GravityZone mogą być również skonfigurowane jako kontrolery obciążenia. W miarę rozwoju jednego z punktów geograficznych, niezwykle prostym jest tworzenie kolejnych wirtualnych urządzeń GravityZone, niezwykle prosty jest również wybór odpowiednich funkcji i umożliwienie przepływu obciążenia istniejącego wdrożenia do nowych urządzeń. Ta przełomowa, oparta na chmurze architektura zapewnia klientom szybki i łatwy dostęp do skalowania, konserwacji, monitorowania i raportowania. W rozproszonym geograficznie środowisku GravityZone łączy centra danych, zapewniając kontrolę nad środowiskami zwirtualizowanymi przez heterogeniczne hiperwizory, fizyczne punkty końcowe (laptopy, komputery stacjonarne, serwery) i urządzenia mobilne, jednocześnie.

OCENA NASZEGO ROZWIĄZANIA

GravityZone SVE to niezrównane rozwiązanie zabezpieczające, które można wdrożyć i ocenić we własnym środowisku w ciągu zaledwie kilku godzin, łącznie z czasem potrzebnym na pobranie urządzenia wirtualnego GravityZone. Nie ma potrzeby wykonywania żadnych skryptów, ponieważ cała konfiguracja odbywa się za pośrednictwem CLI urządzenia i intuicyjnego interfejsu internetowego GravityZone. Potwierdza to ponad 85% administratorów, którzy analizowali rozwiązanie Bitdefender SVE, i zarekomendowali jego zakup.

"Dla nas kluczem do zaliczenia zadania będzie test wydajności produktu w naszym zwirtualizowanym środowisku, to, w jakim stopniu produkt wpłynie lub nie wpłynie na produktywność użytkowników i na reakcję profesjonalnego zespołu serwisowego." Mikael Korsgaard Jensen, Server Manager, Herning Kommune, Dania

"Ponieważ Bitdefender jest Partnerem VMware Technology Alliance, integrującym się z vShield i vCenter, pozwala nam to zarówno zwiększyć naszą przewagę konkurencyjną, jak i wyróżnić hostowaną usługę VDI poprzez połączenie jej z najlepszym w swojej klasie bezpieczeństwem hostowanego środowiska VDI". Jose Uribe, COO, Webhosting.net, USA

ZAKRES SYSTEMÓW OPERACYJNYCH
NAJSZERSZY ZASIĘG WIRTUALIZACJI I SYSTEMÓW OPERACYJNYCH DZIĘKI PARTNERSTWU TECHNOLOGICZNEMU

VMware vSphere 4.1, 5.0, 5.1, 5.5, 6.0 z VMware vCenter Server 4.1, 5.0, 5.1, 5.5, 6.0
VMware View 5.0, 5.1, 5.2, 5.3
VMware Workstation 8.0.6, 9.x, 10.x, 11.x
VMware Player 5.x, 6.x, 7.x
ESXi 4.1 (build 433742 lub nowszy), 5.0 (build 474610 lub nowszy), 5.1, 5.5, 6.0
vCenter Server 4.1, 5.0, 5.1, 5.5, 6.0
vCloud Networking and Security 5.5.1, 5.5.2, 5.5.3, 5.5.4
vShield Manager 5.0, 5.1, 5.5
vShield Endpoint
VMware Tools 8.6.0 build 446312 albo nowszy

Pełna integracja z VMware NSX:

- ESXi 6.0 lub nowszym dla każdego serwera
- vCenter Server 6.0 lub późniejszy
- NSX Manager 6.2.4 lub późniejszy
- VMware Tools 10.0.9 lub późniejszy

Integracja z Citrix:
Citrix XenServer 5.5, 5.6, 6.0, 6.2, 6.5, 7.0 (wliczając Xen Hypervisor)
Citrix XenDesktop 5.0, 5.5, 5.6, 7, 7.1, 7.5, 7.6, 7.7, 7.8, 7.9,
Citrix XenApp 6.5, 7.5, 7.6, 7.8, 7.9,
Citrix VDI-in-a-Box 5.x

Microsoft: Hyper-V Server 2008 R2, 2012, 2012 R2 lub Windows Server 2008 R2, 2012, 2012 R2 (wliczając Hyper-V Hypervisor)
Linux: Red Hat Enterprise Virtualization 3.0 (wliczając KVM Hypervisor)
Oracle: VM 3.0

OBSŁUGA SYSTEMÓW OPERACYJNYCH

Windows
Workstation Operating Systems: Windows Vista (SP1, SP2), 7, 8, 8.1, 10, 10 TH2
Server operating systems: Windows Home Server, Small Business Server (SBS) 2008, 2011, Windows Server 2008, 2008 R2, 2012, 2012 R2

Linux:
Red Hat Enterprise Linux / CentOS 5.6 albo nowszy
Ubuntu 12.04 LTS albo nowszy
SUSE Linux Enterprise Server 11 albo nowszy
OpenSUSE 11 albo nowszy
Fedora 16 albo nowszy
Debian 7.0 albo nowszy
Oracle Solaris 11, 10 (tylko w środowiskach VMware vShield)
Oracle Linux 6.3 albo nowszy

Oracle Solaris 11, 10 (tylko w środowiskach VMware vShield)