

GravityZone Smart Centralized Scanning

Cyberbezpieczeństwo dostosowane do potrzeb w zakresie wydajności

Wymagania wielu firm w zakresie cyberbezpieczeństwa rosną ze względu na coraz bardziej wyrafinowane zagrożenia i różnorodność środowisk, którymi przedsiębiorstwa muszą obecnie zarządzać. Centra danych opierają się aktualnie najczęściej na dużych wirtualnych farmach serwerów z rzadka znajdujących się w siedzibie firmy, a częściej w chmurach publicznych i prywatnych. Rośnie także liczba systemów wirtualnych działających na takich serwerach, co z kolei prowadzi do coraz większego zagęszczenia maszyn wirtualnych. Większe zagęszczenie maszyn oznacza większe zapotrzebowanie na procesory, pamięć RAM i przestrzeń do przechowywania cyberzasobów. Środowiska hybrydowe i chmurowe generują różne wyzwania związane z wdrażaniem i zarządzaniem rozwiązaniami z zakresu cyberbezpieczeństwa dla tych zróżnicowanych środowisk. Nie bez znaczenia pozostaje tutaj także kwestia finansów. Firmy niechętnie patrzą na rozwiązania z zakresu cyberbezpieczeństwa, które podnoszą koszty operacyjne, zużywając cenne zasoby.

Rozwiązania w zakresie bezpieczeństwa wciąż ewoluują, aby stawić czoła współczesnym zagrożeniom. Dzięki konsekwentnemu wprowadzaniu nowych funkcji, takich jak uczenie maszynowe, sztuczna inteligencja, szczegółowa analiza ataków, ograniczanie ryzyka i inne, rozwiązania w zakresie bezpieczeństwa mogą czasami wymagać więcej pamięci RAM, mocy obliczeniowej, przestrzeni dyskowej i większej przepustowości do działania. Migrując do chmury, przedsiębiorstwa muszą być świadome kosztów związanych z hostingiem swojej infrastruktury w tej technologii. Wydatki związane z mocą obliczeniową, siecią i przechowywaniem mogą przekładać się na wiele aspektów cyberbezpieczeństwa. Rozwiązania w zakresie cyberbezpieczeństwa muszą być obecnie lżejsze i bardziej skalowalne niż kiedykolwiek wcześniej, oferując jednocześnie najwyższą odporność na zaawansowane ataki cybernetyczne. Aby sprostać tym wyzwaniom, firmy z branży cyberbezpieczeństwa opracowały technologię scentralizowanego inteligentnego skanowania. Technologia ta umożliwia skanowanie wielu systemów z poziomu centralnego serwera w celu odciążenia punktów końcowych, zapewniając przy tym pełną skalowalność. Taka konfiguracja pomaga rozwiązać niektóre problemy związane z ochroną dużych środowisk wirtualnych, ale niesie też za sobą kilka specyficznych trudności. Wdrożenie i zarządzanie takimi rozwiązaniami oraz potencjalne problemy związane z brakiem dostępności serwera mogą przysporzyć zespołom zajmującym się bezpieczeństwem w firmie niepotrzebny ból głowy.

W skrócie

Opatentowane rozwiązanie w zakresie **scentralizowanego skanowania GravityZone** zostało zaprojektowane dla środowisk wirtualnych i obciążeń w chmurze.

Technologia ta znacząco przyczyniła się do sukcesów wielokrotnie nagradzanych rozwiązań w zakresie cyberbezpieczeństwa Bitdefender dzięki konfiguracji umożliwiającej mniejsze zużycie zasobów, co idealnie wpasowuje się w potrzeby centrów danych i obciążeń w chmurze. Firmy nie muszą już wybierać między cyberbezpieczeństwem a wydajnością systemu.

Kluczowe zalety

- Eliminuje problem duplikacji skanowanych plików
 - dwupoziomowe wychwytywanie danych pomaga uniknąć zbędnego skanowania, znacząco zmniejszając wpływ na wydajność systemu. Naprawdę inteligentne skanowanie
 - skanowanie jedynie fragmentów plików zdolnych do wykonania złośliwego kodu poprawia szybkość i efektywność skanowania oraz zmniejsza liczbę IOPS.
- Scentralizowane zarządzanie – integracja ze środowiskami EXSi®, VMWare®, Citrix®, Microsoft Hyper-V®, hostami Nutanix oraz mazon Elastic Compute Cloud (EC2) pozwala na bezproblemowe wdrożenie i zarządzanie.

„Dzięki temu, że GravityZone ogranicza zużycie zasobów do minimum, nie wywiera najmniejszego wpływu na czas odpowiedzi punktu końcowego ani opóźnienia. Ponieważ nasz zespół IT znajduje się w siedzibie IRSAP, często korzystamy z możliwości centralnego i zdalnego zarządzania wszystkimi naszymi fizycznymi i wirtualnymi punktami końcowymi. W ogólnym rozrachunku zarządzanie bezpieczeństwem stało się bardziej wydajne.”

Marco Broetto,
IT Manager, IRSAP

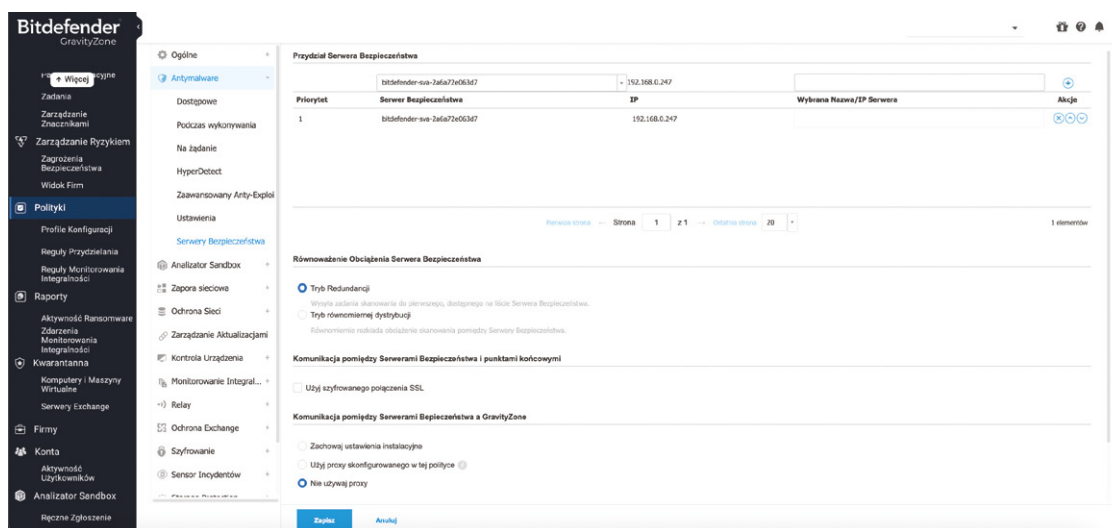
Ochrona dużych środowisk wirtualnych niesie za sobą specyficzne trudności.

- Wdrożenie rozwiązań opartych na technologii scentralizowanego skanowania i zarządzanie nimi oraz większe wymagania z tym związane mogą przysporzyć zespołom zajmującym się bezpieczeństwem w firmie dodatkowej pracy.
- Rosnące potrzeby w zakresie bezpieczeństwa, jakimi obciążone są obciążenia w chmurze, mogą znacząco podnieść koszty operacyjne.
- Starsze rozwiązania w zakresie cyberbezpieczeństwa mogą negatywnie wpływać na wydajność i pracę systemów. Rozwiązania w zakresie scentralizowanego skanowania mogą nie odpowiadać pod względem redundancji potrzebom środowisk produkcyjnych.

Krótki opis rozwiązania

Rozwiązanie Security for Virtualized Environments GravityZone zostało opracowane specjalnie z myślą o współczesnych wymagających centrach danych i środowiskach wykorzystujących obciążenia w chmurze. Dzięki naszej opatentowanej technologii jesteśmy w stanie wyeliminować problemy związane ze zużyciem zasobów i ochroną punktów końcowych oraz obciążen w chmurze. Technologia inteligentnego scentralizowanego skanowania wykorzystywana przez rozwiązanie GravityZone Endpoint Protection pomaga odciążać standardowe intensywne procesy skanowania maszyn przy pomocy wirtualnego urządzenia z funkcjonalnością „serwera bezpieczeństwa”. Taka konfiguracja sprawia, że fizyczne i wirtualne punkty końcowe nie są nadmiernie obciążane przez rozwiązania z zakresu cyberbezpieczeństwa wymagające dużych zasobów. Ta unikalna koncepcja może służyć do ochrony środowisk wyposażonych zarówno w fizyczne, jak i wirtualne stacje robocze, serwery, kontenery danych, desktopy i inne punkty końcowe działające na systemach Windows, MacOS i Linux.

Technologia **GravityZone Smart Centralized Scanning** jest idealna dla firm, które chcą zapewnić bezpieczeństwo środowisk fizycznych, wirtualnych i obciążen w chmurze. Umożliwia ona zespołom zajmującym się cyberbezpieczeństwem bezproblemowe wdrożenie rozwiązania GravityZone w całej firmie dzięki centralnej konsoli do zarządzania. W przypadku środowisk VMware VSphere GravityZone oferuje ochronę bez agenta poprzez integrację z vShield Endpoint™.



Rys. 1.1: Z pomocą ustawień polityki GravityZone zespoły zajmujące się cyberbezpieczeństwem w firmie mogą konfigurować punkty końcowe w taki sposób, aby zapewnić ich płynną komunikację z kilkoma różnymi wirtualnymi urządzeniami z funkcjonalnością „serwera bezpieczeństwa” w trybie redundantnym, który umożliwi pracę systemu w sytuacjach awaryjnych lub w trybie równej dystrybucji pozwalającym na harmonijne rozłożenie obciążenia.

Technologia inna niż wszystkie


Zespoły ds. cyberbezpieczeństwa używające Gravity Zone mogą z łatwością pobrać wirtualne urządzenie Security Server Virtual Appliance, a następnie wykorzystać je jako centralną stację skanowania z poziomu konsoli do zarządzania GravityZone. Wirtualne urządzenie z funkcjonalnością „serwera bezpieczeństwa” Security Server Virtual Appliance jest dostępne dla hostów EXSi® standalone, VMware® VSphere, Citrix® Xen servers™, Microsoft Hyper-V® i Nutanix Prism® i oferuje możliwość integracji

ze środowiskami Amazon Elastic Compute Cloud (EC2). Security Server Virtual Appliance może następnie zostać wprowadzone po prostu jako kolejna wirtualna maszyna. Wystarczy kilka prostych kroków konfiguracji komunikacji sieciowej, aby zespoły ds. cyberbezpieczeństwa były gotowe do skonfigurowania ochrony punktów końcowych do komunikacji z wdrożonymi wirtualnymi urządzeniami Security Servers.

Konsola do zarządzania GravityZone umożliwia zespołom zajmującym się cyberbezpieczeństwem utworzenie lekkiego pakietu agenta skonfigurowanego do pracy z naszą opatentowaną technologią inteligentnego scentralizowanego skanowania. Agent, mimo niewielkich rozmiarów, zachowuje kluczowe komponenty, takie jak rozwiązanie do zarządzania aplikacjami Application Control, funkcja ochrony przed zagrożeniami sieciowymi Web Threat Protection, opcja do zarządzania aktualizacjami, technologia Process Inspector, funkcja Ransomware Mitigation służąca do ograniczania zagrożeń atakami ransomware i zaawansowana ochrona przed exploitami, jednocześnie odciążając zadania wymagające intensywnego przetwarzania danych, np. skanowanie i aktualizacje produktów. Pozwala on również na współpracę z wirtualnym urządzeniem GravityZone Security Server, co umożliwia korzystanie z funkcjonalności HyperDetect i Sandboxing.

Większa gęstość maszyn wirtualnych

W przeciwieństwie do tradycyjnych rozwiązań GravityZone zostało od podstaw zaprojektowane z myślą o optymalizacji pod kątem serwerów i obciążeń roboczych w chmurze. Technologia **Smart Centralized Scanning** minimalizuje wpływ rozwiązania na bezpieczeństwo infrastruktury, wykorzystując w tym celu dwupoziomowy mechanizm wychwytywania danych, który pomaga uniknąć duplikacji skanowanych plików. Wirtualne urządzenie z funkcjonalnością „serwera bezpieczeństwa” Security Server Virtual Appliance sprawdza każdy plik tylko raz, nawet jeśli pojawia się on w kilku punktach końcowych. Pomaga to uniknąć zbędnego skanowania, znacząco zmniejszając tym samym obciążenie procesora, pamięci RAM, infrastruktury i sieci. Wirtualne urządzenie z funkcjonalnością „serwera bezpieczeństwa” Security Server Virtual Appliance można skonfigurować do pracy w dwóch trybach: redundantnym i równej dystrybucji. Co więcej, automatycznie wykrywa ono utworzenie nowej maszyny wirtualnej, a także przeniesienie oraz usunięcie istniejącej. Rozwiązanie Security Server może następnie zastosować wyznaczoną politykę bezpieczeństwa do dowolnej maszyny, kierując się przydziałem w ramach puli zasobów, podziałem na grupy lub sieci, do których dana maszyna jest przypisana.

NAGŁÓWEK	SEGMENTY MOŻLIWE DO WYKONANIA	ROZSZERZENIE PLIKU
		
ROZSZERZENIE PLIKU		
• Pełny rozmiar pliku		25 MB
• Rozmiar segmentów zdolnych do wykonania (tj. obszary plików podlegające inspekcji)		2,5 MB
• Zaoszczędzone zasoby		22,5 MB

Rys. 2.1: GravityZone korzysta z bardzo efektywnej techniki skanowania, która sprawdza tylko fragmenty plików zdolne do wykonania złośliwego kodu, co eliminuje konieczność przesyłania całych plików z maszyny wirtualnej na urządzenie wirtualne pełniące funkcję serwera, znacząco redukując w ten sposób obciążenie procesora, pamięci RAM, infrastruktury i sieci.

Naprawdę inteligentne skanowanie

Optymalizacja w naszym wydaniu nie kończy się na eliminacji duplikacji skanowania. Funkcja **GravityZone Smart Centralized Scanning** dodatkowo zmniejsza przepustowość i zasoby potrzebne do identyfikacji zagrożeń poprzez przesyłanie do urządzenia wirtualnego Security Server tylko fragmentów plików zdolnych do wykonania złośliwego kodu. Fragmenty takie przekazywane są za pośrednictwem bezpiecznego portu TCP/IP z punktów końcowych na wirtualne urządzenie Security Server. Po dotarciu do urządzenia fragmenty plików są skanowane, a w razie wykrycia złośliwego kodu, cały plik zostaje oznaczony jako wymagający działania: odrzucenia, poddania kwarantannie albo usunięcia - w zależności od wybranej polityki bezpieczeństwa.

Brak konieczności skanowania całego pliku w celu identyfikacji zagrożeń oferowany przez rozwiązanie **GravityZone Smart Centralized Scanning** umożliwia wydajniejszą ochronę punktów końcowych i minimalny wpływ na pracę systemu nawet podczas skanowania dużych ilości danych.

Idealne rozwiązanie dla centrów danych i obciążeń w chmurze

Technologia inteligentnego scentralizowanego skanowania GravityZone przyspiesza identyfikację zagrożeń, jednocześnie nie obciążając systemu większym zużyciem jego zasobów. To sprawia, że jest doskonałą opcją dla centrów danych i środowisk korzystających z obciążeń w chmurze z licznymi rozproszonymi punktami końcowymi o różnych konfiguracjach sieci. Polityki GravityZone, obejmujące tryb redundantny i równej dystrybucji, umożliwiają konfigurację wielu wirtualnych urządzeń Security Server oraz ich błyskawiczne włączanie i wyłączenie.

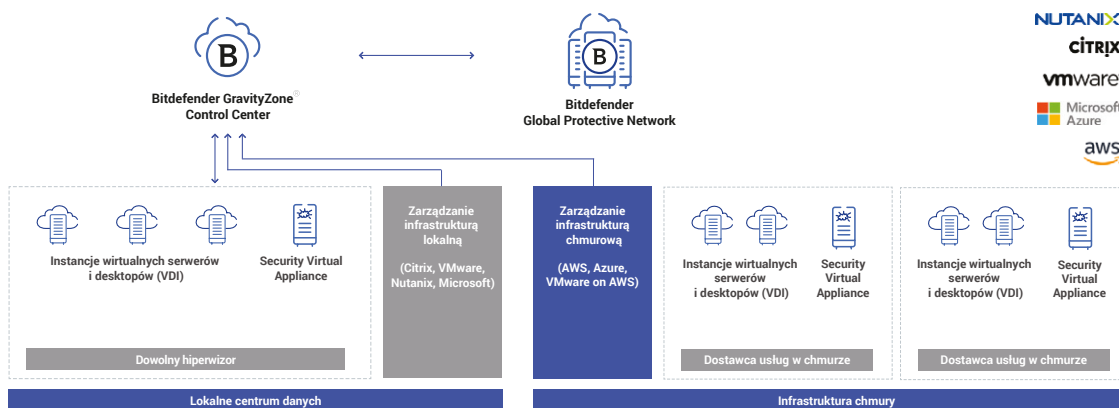
Opcja integracji z rozwiązaniami VMware vCenter, Citrix XenServer oraz Amazon Elastic Compute Cloud (EC2) umożliwia zespołom zajmującym się cyberbezpieczeństwem zarządzanie wszystkimi maszynami za pomocą jednolitego, prostego w obsłudze interfejsu. Przy jego pomocy pracownicy mogą przeglądać zdarzenia, przypisywać polityki oraz inicjować działania we wszystkich zarządzanych systemach – tych na miejscu oraz tych w chmurze. Konsola GravityZone zapewnia wszechstronny dostęp do wszystkich najważniejszych funkcji – od wyświetlania szczegółowych raportów na temat filtrowania zawartości stron internetowych, poprzez izolowanie hostów podczas prowadzonych dochodzeń i konfigurowanie powiadomień o wykrytych zagrożeniach, aż do planowania cyklicznych kontroli bezpieczeństwa. Rozwiązanie GravityZone Smart Centralized Scanning zapewnia maksymalną elastyczność i skalowalność niezależnie od wielkości firmy.

Mniejsze wydatki na bezpieczeństwo

Technologia inteligentnego scentralizowanego skanowania pomaga ograniczyć wydatki na bezpieczeństwo, minimalizując wpływ rozwiązania GravityZone na zużycie firmowych zasobów. Ta wyjątkowa koncepcja ogranicza potrzeby w zakresie modernizacji drogiego sprzętu w przypadku środowisk lokalnych i hybrydowych, a także zmniejsza koszty operacyjne (związane z mocą obliczeniową i siecią) w przypadku modeli PaaS, IaaS i SaaS.

Bezkompromisowe cyberbezpieczeństwo

Firmy nie muszą już wybierać między cyberbezpieczeństwem a wydajnością systemu. Technologia inteligentnego scentralizowanego skanowania daje zespołom zajmującym się cyberbezpieczeństwem potężne skalowalne narzędzie, które jest łatwe do wdrożenia i zarządzania we wszystkich środowiskach, niezależnie od ich wielkości. Opatentowana technologia pozwala ograniczyć wpływ nagradzanego rozwiązania Bitdefender na wydajność infrastruktury firmy, zapewniając bezpieczeństwo jej systemów i doskonałą funkcjonalność.



Rys. 3.1: GravityZone Smart Centralized Scanning odciąża zasobochłonne zadania skanowania danych z maszyn fizycznych i wirtualnych, posiłkując się wsparciem wirtualnego urządzenia GravityZone Security Server. Powoduje to znaczny wzrost wydajności w porównaniu do starszych konfiguracji rozwiązań w zakresie cyberbezpieczeństwa. Zespoły zajmujące się cyberbezpieczeństwem mogą wdrażać różne funkcje maszyn fizycznych i wirtualnych i zarządzać nimi z poziomu jednej kontroli do zarządzania GravityZone.

Bitdefender[®]
BUILT FOR RESILIENCE

Centrala

Siedziba przedsiębiorstwa – Santa Clara, California, USA
Centrala technologiczna – Bukareszt, Rumunia

Przedstawiciel marki Bitdefender w Polsce

Marken Systemy Antywirusowe
Tel: 58 667 49 49
E-mail: kontakt@marken.com.pl
www.bitdefender.pl

Bitdefender jest światowym liderem w dziedzinie cyberbezpieczeństwa, dostarczając najwyższej klasy rozwiązania do zapobiegania, wykrywania i reagowania na zagrożenia. Wybrany przez miliony konsumentów, firm i instytucji państwowych, Bitdefender jest jednym z najbardziej zaufanych ekspertów w branży w zakresie eliminacji zagrożeń, ochrony prywatności i danych oraz wzmocnienia cyberodporności. Dzięki dużym nakładom na badania i rozwój, Bitdefender Labs co minutę odkrywa 400 nowych zagrożeń i sprawdza 40 miliardów zapytań o zagrożenia dziennie. Będąc pionierem przełomowych innowacji w dziedzinie zabezpieczeń, bezpieczeństwa IoT, analityki behawioralnej i sztucznej inteligencji, dostarcza licencji technologicznych ponad 150 najbardziej rozpoznawalnym firmom technologicznym na świecie. Założony w 2001 roku Bitdefender ma klientów w ponad 170 krajach i biura na całym świecie.

Więcej informacji na stronie <https://www.bitdefender.com>

Wszelkie prawa zastrzeżone. © 2022 Bitdefender.

Wszystkie znaki handlowe, nazwy handlowe i produkty wymienione w niniejszym dokumencie są własnością ich właścicieli.