

Решение системы безопасности GravityZone для виртуализированных сред

Не позволяйте процессу виртуализации "тормозить" вашу инфраструктуру. Безопасность и производительность могут сосуществовать в облачных и виртуализированных центрах обработки данных. GravityZone предлагает службу безопасности, которая почти незаметна в работе, но помогает компаниям эффективно управлять ИТ-рисками, не теряя при этом преимуществ масштабируемой инфраструктуры.

Продукт GravityZone полностью создана для виртуализации и облачных сред для предоставления услуг бизнес-безопасности физическим конечным точкам, мобильным устройствам, виртуальным машинам в частных, общедоступных облачных и почтовых серверах Exchange.



ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ПРОДУКТА:

- Поддерживает VMware, Microsoft Hyper-V, Citrix XenServer, Red Hat Enterprise Virtualization (с KVM) и др.
- Защищает виртуальные машины на основе ОС Microsoft и большинства версий Linux.
- Использует NSX в средах VMware для обеспечения максимальной безопасности, специально разработанной для виртуализованных ЦОД.
- Интегрируется с VMware vCenter, позволяя проводить политику управления безопасностью на основе таких объектов, как пулы ресурсов, папки и распределенные сети.
- Постоянно устраняет единичные случаи сбоев систем, обеспечивая при этом беспрецедентную доступность защиты от вредоносных программ.
- Предоставляет зарекомендовавшую себя защиту Bitdefender от вредоносного ПО в файловых системах, памяти, процессах и базе данных реестра, не оставляя без внимания ни единой виртуальной машины.
- Продукт «Безопасность предприятия для виртуализованных сред» (Bitdefender GravityZone Enterprise Security for Virtualized Environments (SVE)) является передовым решением для обеспечения безопасности виртуальных центров обработки данных на рынке, если речь идет о защите от вредоносных программ для виртуальных машин, решение оптимизирует не только консолидационные отношения, но и эксплуатационные расходы.
- Решение GravityZone SVE разработано как корпоративное решение, способное поддерживать крупнейшие центры обработки данных. Однако интеграция в производственную среду очень проста, а преимущества технологии ощущаются в виртуальных средах любого размера.



ОБЗОР ТЕХНОЛОГИИ

Одна из опций продукта GravityZone SVE - предоставление антивирусной защиты с использованием выделенных виртуальных серверов защиты (Security Servers), которые функционируют как централизованные точки высокоинтеллектуальной системы борьбы с вирусами, с тем отличием, что нет необходимости в установке традиционного агента безопасности на каждой виртуальной машине. Обычный агент безопасности требует постоянных обновлений и мониторинга, а кроме того, потребляет значительное количество операционных ресурсов. Каждая виртуальная машина подключается к серверу защиты для выгрузки большинства функций защиты от вредоносных программ, охватывающих файловую систему, память, процессы и проверку реестра.

Продукт GravityZone SVE использует многоуровневый механизм кэширования, который еще более усиливает высокую производительность системы. Во-первых, локальная кеш-память поддерживается внутри каждой виртуальной машины, поэтому объекты сканируются только один раз. Во-вторых, общая кеш-память постоянно обновляется на каждом сервере безопасности, так что объекты, проверенные на одной виртуальной машине, не сканируются на другой. Наконец, серия кэшей уровня файлового блока обеспечивает дедупликацию сканирования вплоть до уровня файловых фрагментов, что означает, что файлы с несколькими различными блоками, представляющими интерес для антивирусных движков на сервере безопасности, не требуют полного повторного сканирования. Чистый результат этих эксклюзивных технологий Bitdefender является главным секретом производительности GravityZone SVE.

Решение Bitdefender GravityZone - это гремячая смесь высокоэффективных технологий обеспечения безопасности, способная справиться с любым видом угрозы - от простейшей атаки вируса до наиболее сложных целевых атак. Благодаря таким технологиям, как Advanced Threat Control, мощному анти-эксплойту, признанной антиспам-системе и точнейшей фильтрации контента, а также многоуровневой защите от вредоносных программ, продукция Bitdefender постоянно занимает первые места в тестированиях независимых организаций, с более чем 99%-вероятностью обнаружения новых или неизвестных угроз.*

Весь арсенал зарекомендовавших себя технологий защиты компании Bitdefender встроен в механизмы безопасности и в архитектуру виртуального устройства. С SVE защита от вредоносных программ более надежна, чем когда-либо, обеспечивая безопасность каждой виртуальной машины, подключенной к центру обработки данных.



BitDefender Endpoint Security Tools

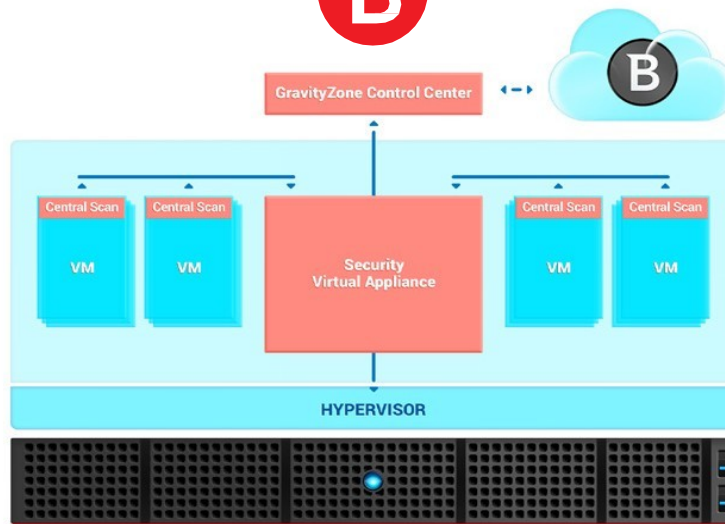
Чтобы Security Server получал доступ к файловой системе каждой виртуальной машины, а также к памяти, реестру и запущенным процессам и другим необходимым функциям, поддерживающий набор сервисов, поставляемых в виде централизованного сканирования, должен быть развернут для каждой виртуальной машины. Характеристики Централизованного сканирования.

Низкое воздействие на работоспособность системы:

- Использует менее 110 МБ RAM (включая runtime cache);
- 10-20 МБ локальной памяти;
- Пиковая загрузка процессора 1-2% для одной виртуальной машины при сканировании по доступу.

Основные функции:

- Устанавливает соединение с доступным авторизованным сервером безопасности (виртуальное устройство), позволяя локальный доступ к файловой системе, реестру, памяти и процессам;
- подключается к альтернативным серверам безопасности в случае медленного времени отклика или внезапной недоступности сервера;
- Управляет локальным сканированием, карантином и блокировкой процессов;
- Поддерживает локальный кеш сканируемых объектов для повышения производительности;
- Запускается как локальная служба без прав администратора, защищая от атак, пытающихся локально выключить защиту;
- Опционально предоставляет пользовательский интерфейс внутри виртуальной машины с всплывающими уведомлениями на рабочем столе;
- Процесс внедрения централизованного сканирования (доступно как для Windows, так и для Linux) прост и не требует перезагрузки виртуальных машин, а внедрение сервера безопасности также не требует перезагрузки компьютеров, на которых размещены виртуальные машины;
- Центральное сканирование также может использоваться в шаблонах и образах VDI для уменьшения загрузки инфраструктуры.



Уникальный дизайн архитектуры GravityZone дает несколько преимуществ:

- У виртуальных машин нет локальных антивирусных программ, но они всегда будут защищены доступным сервером безопасности
 - Устраняет возможность AV Storms.
 - Многоуровневое кэширование отдельных виртуальных машин и сервера безопасности гарантирует, что один и тот же файл не будет сканироваться многократно
 - устраняет замедление загрузки и уязвимости, возникающие при запуске виртуальных машин
 - Пробелы в защите невозможны, поскольку Центральное Сканирование автоматически подключается или переключается к доступному серверу безопасности, как это определено политикой.
 - Централизованная защита не имеет проблемных узких мест, поскольку Центральное сканирование может автоматически переключиться на другой сервер безопасности с более быстрым временем отклика.
 - постоянно работающие виртуальные машины автоматически защищаются за счет соответствующей политики безопасности (когда на виртуальной машине установлено центральное сканирование, и политика безопасности применена к пулу ресурсов или папке, виртуальная машина наследует соответствующую политику)
- * AV-Comparatives Heuristic / Behaviour Tests, Март 2015
- позволяет создать больше виртуальных машин в следствие экономии объема памяти, дискового пространства, расхода ресурсов процессора и уменьшения количества операций ввода-вывода;
 - виртуальные машины всегда защищены новейшими технологиями, даже если были восстановлены из старого бэкапа или запущены после длительного перерыва в работе;
 - нет необходимости в установке антивируса на каждую виртуальную машину, если было настроено централизованное сканирование;
 - позволяет создавать гибкие запросы в базе данных GravityZone для получения данных по расширенной аналитике и понимания структуры вашей сети с помощью простого графического интерфейса, который не требует дополнительных знаний SQL для настройки дополнительных параметров (доступно только для продуктов Enterprise Security on-premise).



Непревзойденная производительность

Решение SVE было разработано для решения проблем, связанных с запуском AV в виртуализованной среде, и постоянно совершенствуется, акцентируя свое внимание на защите, простоте, производительности и совместимости.

Наши обширные тесты производительности подтверждают, что SVE имеет самое низкое влияние на все основные AV-решения на рынке, а также обеспечивает отмеченную наградами систему защиты от Bitdefender. Таким образом, вы сможете восстановить до 17% вычислительной мощности вашего хоста и сократить время ожидания по сравнению с вашим текущим AV-решением, одновременно сокращая эксплуатационные расходы из-за радикального сокращения обслуживания и мониторинга.

ДОПОЛНИТЕЛЬНО: ИНТЕГРАЦИЯ NSX

При использовании платформы VMware NSX, Bitdefender обеспечивает высокоэффективный анализ посещений, разработанный специально для датацентров, предоставляя безагентную защиту, автоматическое развертывание и организацию служб безопасности в виртуализованной среде.

Гибкое лицензирование датацентров и личных VMS

Продукт GravityZone SVE предоставляет простую модель лицензирования как для каждого сокета процессора в центрах обработки данных, так и для виртуальных компьютеров. Лицензирование VM разделено между виртуальными серверами и VDI, чтобы соответствовать динамическим и высоко виртуализованным инфраструктурам.

УНИФИЦИРОВАННОЕ УПРАВЛЕНИЕ

Решение GravityZone SVE – это один из продуктов компании, направленных на обеспечение безопасности, относящихся к единой платформе GravityZone Enterprise Security, управление происходит через веб-интерфейс. В дополнение к защите VM, GravityZone Enterprise Security защищает физические рабочие точки и серверы (на базе Windows, Linux, Mac), мобильные устройства (на базе Android, iOS), и почтовые сервисы Exchange.

Решение GravityZone обладает уникальной архитектурой, основанной на готовом виртуальном устройстве, которое в случае необходимости может быть скопировано. Каждый экземпляр может играть одну или несколько ролей. Эта простая, но мощная модель делает GravityZone передовым продуктом, удовлетворяющим требованиям самых больших инфраструктур посредством единоразового внедрения.

Например, три устройства, работающие с облачной средой с открытым исходным кодом и облачная централизованная база данных, входящие в состав GravityZone, могут работать в Сан-Франциско, имея еще две точки в Нью-Йорке, в то время как аналогичное количество серверов связи географически распределяется там, где это необходимо. Виртуальные устройства GravityZone также могут быть настроены как балансировщики нагрузки. В случае добавления географически удаленного объекта нужно просто добавить больше виртуальных устройств GravityZone, выбрать необходимые роли и обеспечить возможность распространения существующих параметров развертывания на новые устройства. Данная новаторская облачная архитектура обеспечивает клиентам быстрый и легкий доступ к масштабированию, обслуживанию, мониторингу и отчетности.

В географически разбросанной среде GravityZone объединяет датацентры в одно целое и позволяет управлять неоднородными виртуализованными средами, состоящими из гипервизоров, серверов, ПК, ноутбуков и мобильных устройств.



ОЦЕНКА НАШЕГО РЕШЕНИЯ

Решение GravityZone SVE - это уникальное решение для обеспечения безопасности, которое вы можете установить и оценить в своей собственной среде всего за несколько часов, включая время, необходимое для загрузки виртуального устройства GravityZone. Никаких сценариев не требуется, так как все конфигурации выполняются через CLI устройства и интуитивно понятный веб-интерфейс GravityZone. В итоге - более 85% пользователей нашей программы положительно оценили решение Bitdefender SVE, и впоследствии приобрели ее.

«Для нас ключом к прохождению теста была производительность продукта в нашей виртуализованной среде, насколько продукт будет или не будет влиять на производительность конечных точек пользователей и каково будет мнение команды поддержки». Микаэль Корсгард Йенсен, сервер-менеджер, Хернинг Коммуны, Дания

«Поскольку Bitdefender является партнером VMware Technology Alliance, интегрирующимся с vShield и vCenter, он позволяет нам как увеличить наши конкурентные преимущества, так и дифференцировать нашу размещенную VDI-услугу, объединив ее с лучшим в своем классе средством защиты размещенной среды VDI». Хосе Урибе, управляющий директор, Webhosting.net, США

ПОКРЫТИЕ ОС НАИБОЛЕЕ ШИРОКОЕ ПОКРЫТИЕ СИСТЕМ ВИРТУАЛИЗАЦИИ И ЭКСПЛУАТАЦИИ БЛАГОДАРЯ ТЕХНОЛОГИЯМ ПАРТНЕРСТВА

VMware vSphere 4.1, 5.0, 5.1, 5.5, 6.0 с центральным сервером 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 или выше), 5.0 (версия 474610 или выше), 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 версия 446312 или выше

Интеграция с VMware NSX Requirements:

- ESXi 6.0 или более поздняя версия для каждого сервера
- vCenter Server 6.0 или более поздняя версия
- NSX Manager 6.2.4 или более поздняя версия
- VMware Tools 10.0.9 или более поздняя версия

Интеграция с Citrix:

Citrix XenServer 5.5, 5.6, 6.0, 6.2, 6.5, 7.0 (включая 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 or Windows Server 2008 R2, 2012, 2012 R2 (включая Hyper-V Hypervisor)
Linux: Red Hat Enterprise Virtualization 3.0 (включая KVM Hypervisor)
Oracle: VM 3.0

ПОКРЫТИЕ ОПЕРАЦИОННЫХ СИСТЕМ

Windows

ОС рабочих станций: Windows Vista (SP1, SP2), 7, 8, 8.1, 10, 10 TH2
ОС серверов: 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 или выше
Ubuntu 12.04 LTS или выше
SUSE Linux Enterprise Server 11 или выше
OpenSUSE 11 или выше
Fedora 16 или выше
Debian 7.0 или выше
Oracle Solaris 11, 10 (только в средах VMware и vShield)
Oracle Linux 6.3 или выше

Oracle Solaris 11, 10 (только в средах VMware и vShield)

Пробная версия продукта на: <http://www.bitdefender.ru>

Образцы для России - обращайтесь по телефону: 8 800 350 4560



Bitdefender предоставляет технологии безопасности в более чем 100 стран через передовую сеть компаний-представителей, дистрибьюторов и партнеров-посредников. С 2001 года Bitdefender последовательно выпускает ведущие на рынке технологии для бизнеса и потребителей и является одним из ведущих поставщиков услуг по виртуализации и облачным технологиям. Bitdefender подобрал свои отличные награды технологии с альянсами продаж и партнерствами и укрепил свои позиции на мировом рынке благодаря стратегическим союзам с некоторыми из ведущих в мире поставщиков виртуализации и облачных технологий.

Все права защищены. © 2015 Bitdefender. Все товарные знаки, торговые наименования и продукты, упомянутые в настоящем документе, являются собственностью их соответствующих владельцев. Для ДОПОЛНИТЕЛЬНОЙ ИНФОРМАЦИИ - сайт: enterprise.bitdefender.com