БЫСТРЫЙ И НАДЕЖНЫЙ ИНСТРУМЕНТ ПОИСКА И УСТРАНЕНИЯ УГРОЗ

GravityZone Ultra - это комплексное решение Endpoint Security, разработанное с нуля в качестве интегрированного EPP нового поколения и простого в использовании EDR. GZ Ultra предлагает функции предотвращения, обнаружения угроз, автоматического реагирования, обнаружения и устранения вредоносных программ перед исполнением, сортировки инцидентов, расследования, расширенный поиск и легкое управление системой.

Опираясь на высокоэффективные технологии предотвращения и автоматического обнаружения угроз и реагирования, GravityZone Ultra снижает количество инцидентов, требующих ручного анализа, снижая операционные затраты, необходимые для запуска EDR. Облако поставляется и создается с нуля как единое решение для одного агента/единой консоли, его также легко развернуть и интегрировать в существующую архитектуру безопасности.

GravityZone Ultra позволяет корпоративным клиентам защитить цифровые ресурсы даже от самых неуловимых киберугроз и эффективно реагировать на все стадии атаки:

- Сокращение площади атак (с помощью брандмауэра, управления приложениями, контроля содержимого и управления исправлениями).
- Защита данных (с помощью дополнительного модуля полного шифрования диска)
- Предварительное обнаружение и ликвидация вредоносных программ (с помощью настраиваемого машинного обучения, проверки процессов в режиме реального времени и анализа "песочницы").
- Обнаружение угроз в режиме реального времени и автоматическое устранение неисправностей
- Видимость до и после компрометированной атаки (анализ первопричин)
- Быстрая сортировка, расследование и реагирование на инциденты
- Поиск текущих и данных из истории
- «Better-than-before» система безопасности (с помощью дополнительного модуля управления исправлениями)

В результате обеспечивается бесперебойное предотвращение угроз, глубокая видимость, точное обнаружение инцидентов и "умное реагирование" для минимизации воздействия угроз и предотвращения нарушений.

Как интегрированный комплекс средств защиты конечных точек, **GravityZone Ultra** обеспечивает стабильный уровень безопасности для всей ИТ-среды, поэтому злоумышленники не находят достаточное количество незащищенных конечных точек, которые можно было бы использовать в качестве отправной точки для вредоносных действий против вашей компании. **GravityZone Ultra основана** на простой, интегрированной архитектуре с централизованным управлением как для конечных точек, так и для дата-центров**.** Она позволяет компаниям быстро развертывать решение по защите конечных точек и требует меньше усилий по администрированию после внедрения.

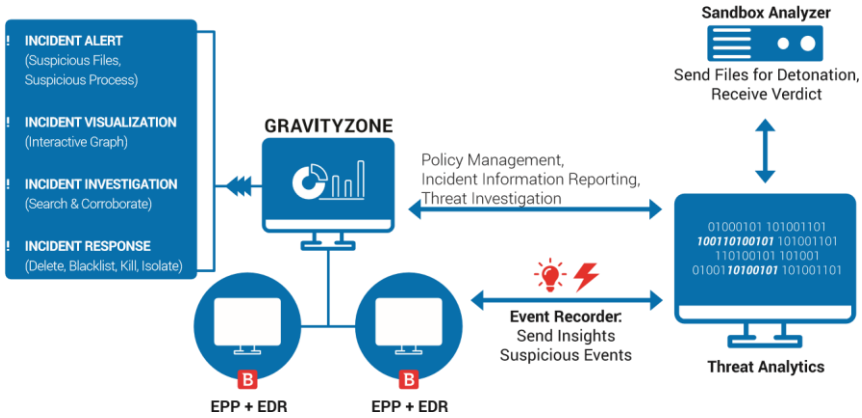


Рисунок 1. Bitdefender Ultra: предотвращение, обнаружение и реагирование в одном агенте, управляемом консолью GravityZone.

С EDR проще

Благодаря четкой видимости индикаторов компрометации (IOCs) и рабочих процессов по расследованию угроз и реагированию на инциденты одним щелчком мыши, GravityZone Ultra снижает требования к ресурсам и навыкам для групп безопасности. Новый регистратор данных конечных точек является удобным дополнением к существующему стеку защиты от угроз и выполняет широкий набор действий системы (файлы и процессы, установка программ, загрузка модулей, модификация реестра, сетевые подключения и т.д.) для визуализации всей корпоративной цепочки событий, связанных с атакой.

Ключевые преимущества

Расширяя традиционные функции EPP, GravityZone Ultra предоставляет аналитикам по безопасности и группам реагирования инструменты, необходимые для анализа подозрительной деятельности, расследования и адекватного реагирования на современные угрозы:

- Обнаружение в режиме реального времени и автоматическое устранение неисправностей
- Быстрая сортировка, расследование и реагирование на инциденты
  - Обнаружение подозрительной деятельности
  - Проверка подозрительной деятельности и сортировка по степени опасности
  - Реагирование на инцидент одним щелчком мыши

- КРасследование до и после компрометации (анализ первопричин)
- Поиск текущих данных и из истории на основе:
  - IOCs
  - MITRE tags
  - Процессы, файлы, записи реестра или другие параметры

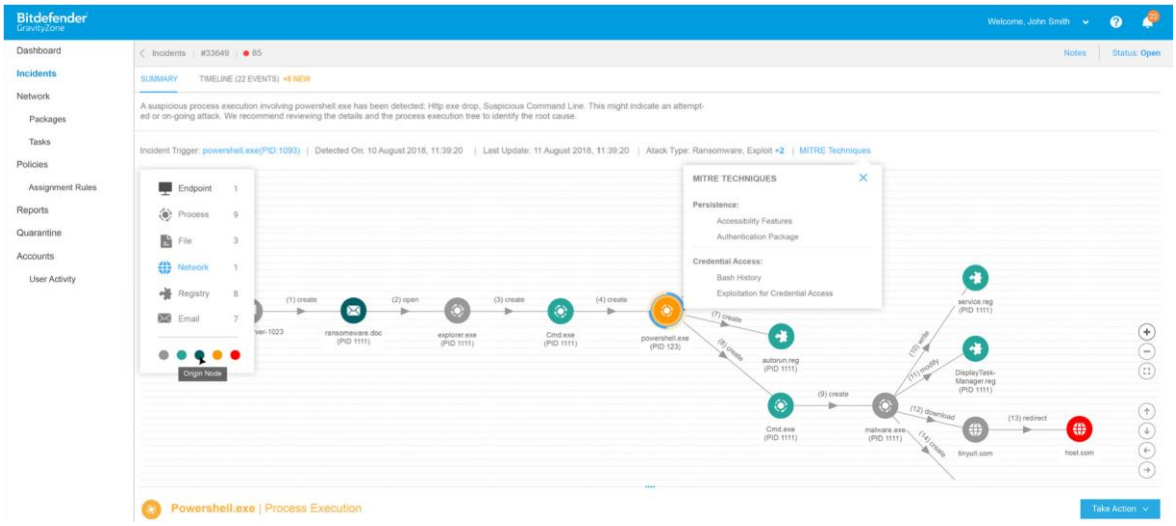


Рисунок 2. Страница сведений об инцидентах предоставляет четкий обзор «области поражения» инцидентов

Высококачественное обнаружение

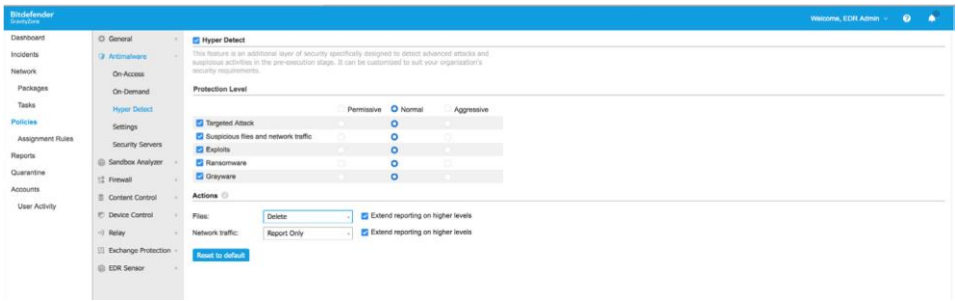
Для анализа и разрешения вручную представляются только релевантные, коррелированные и классифицированные по степени тяжести события. Шум и избыточность информации сведены к минимуму, так как подавляющее большинство атак и продвинутых атак блокируются на этапе до или во время исполнения. Элевантные угрозы, включая безфайловые вредоносные программы, эксплойты, программы выкупа и замаскированные вредоносные программы, нейтрализуются высокоэффективными многоуровневыми технологиями защиты конечных точек нового поколения и инспектором процессов на основе поведения во время выполнения. Автоматическое реагирование и восстановление исключают необходимость вмешательства человека в блокированные атаки.

Высокоточное обнаружение позволяет сотрудникам службы безопасности сосредоточиться только на реальных инцидентах и угрозах:

- Минимизация ложных тревог
- Сокращение количества инцидентов при эффективном предотвращении угроз
- Исключение ручного устранения блокированных атак с помощью автоматического устранения неисправностей

Простое расследование инцидентов и умное реагирование для усовершенствованной защиты

Интегрированное решение GravityZone Ultra, предназначенное для предотвращения обнаружения и обнаружения неисправностей, позволяет быстро реагировать и восстанавливать конечные точки до уровня «Better-than-before». Инструменты расследования инцидентов, такие как анализ первопричин и отчеты песочницы, помогают группам безопасности проверять подозрительную деятельность и адекватно реагировать на киберугрозы. Расширенный поиск текущих и исторических данных на основе меток IOC, MITRE и других релевантных артефактов позволяет быстро идентифицировать угрозы, которые могут скрываться в инфраструктуре конечных точек.



Используя данные, собранные с конечных точек в ходе расследования, интерфейс управления предоставляет инструменты для немедленной корректировки политики и/или исправления выявленных уязвимостей с целью предотвращения будущих инцидентов, повышения безопасности вашей среды.

Комплексная платформа безопасности конечных точек в одном агенте и консоли

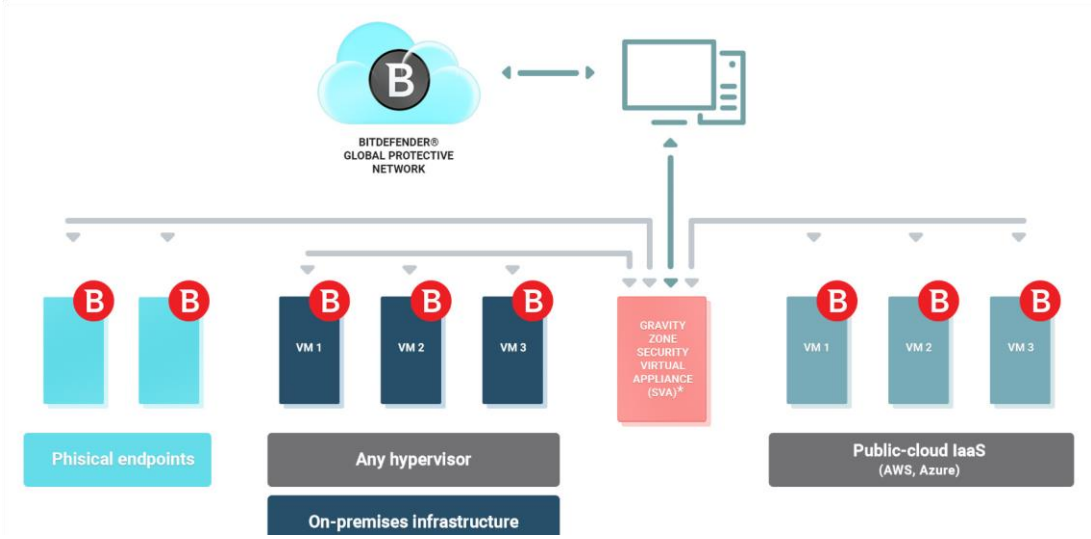
GravityZone Ultra унаследовала все элементы защиты, входящие в комплект GravityZone Elite:

- Минимизация воздействия с помощью усиленной профилактики
- Машинное обучение и обнаружение на основе поведения блокируют неизвестные угрозы перед и во время запуска
- Обнаружение и блокирование безфайловых, замаскированных и пользовательских вредоносных программ на основе сценариев с автоматическим исправлением.
- Защита памяти для предотвращения эксплойтов
- Уменьшение области поражения, с помощью средств управления ИТ-безопасностью.
- Интегрированный клиентский брандмауэр, управление устройствами, фильтрация веб-контента, управление приложениями и многое другое.
- Дополнительные модули: Полное шифрование диска, управление исправлениями
-

Рисунок 3. Bitdefender GravityZone Ultra: комплексная платформа EPP + EDR, Endpoint Security

Защита ЦОД и облачной инфраструктуры

Неотъемлемой частью GravityZone Ultra, GravityZone Security for Virtualized Environment является компонент безопасности серверов и VDI, разработанный для обеспечения гибкости, операционной эффективности и сдерживания расходов на инфраструктуру в программных, гиперконвергентных и гибридных облачных средах.



*** - Also, agentless deployments are supported with VMware® vShieldTM or NSXTM**

Ключевые преимущества

Повышение эксплуатационной эффективности и маневренности
Совместимость с несколькими облачными платформами и всеми гипервизорами (например, VMware® ESXiTM, Citrix® XenServer®, Microsoft® Hyper-V, Nutanix® AHV, KVM),
RedHat® Enterprise Virtualization (или их комбинация), GravityZone помогает оптимизировать ИТ и операции по обеспечению безопасности, улучшая при этом соответствие нормативным требованиям. Унифицированная консоль управления GravityZone упрощает развертывание и администрирование системы безопасности, обеспечивая автоматизированное обеспечение безопасности, централизованное внедрение политик и прозрачность одной панели стекла в неоднородных и распределенных средах. Интеграция с инструментами управления виртуализацией (например, vCenter Server, XenServer и Nutanix Prism) позволяет GravityZone в режиме реального времени получать информацию об операционном контексте инфраструктуры, включая глобальную опись виртуальных машин (VM). Следовательно, GravityZone может автоматически применять соответствующие ВМ политики безопасности, которые следуют за рабочими нагрузками, независимо от того, где они находятся в гибридном облаке, позволяя ИТ-отделам заказчиков в считанные часы развернуть тысячи защищенных ВМ.

Лучшая производительность и использование инфраструктуры
Запатентованные алгоритмы безопасности GravityZone и их эффективная конструкция, устраняющая необходимость использования ресурсоемких агентов внутри каждой виртуальной машины, позволяют увеличить плотность виртуализации до 35% и скорость отклика приложений по сравнению с конкурентами на 17%, обеспечивая лучшее использование инфраструктуры и превосходный опыт конечного пользователя.

Неограниченная линейная масштабируемость
Модульная и гибкая архитектура GravityZone обеспечивает масштабируемость для обеспечения безопасности развертывания операторского класса. Платформа может расширяться по требованию линейно и эффективно, добавляя виртуальные устройства безопасности или при необходимости увеличивая роли сервера центра управления.

Универсальная совместимость
Совместимость со всеми ведущими гипервизорными платформами (VMware ESXi, Microsoft Hyper-V, Citrix Xen, Red Hat KVM и Nutanix AHV) и гостевыми ОС Windows и Linux.

Центр управления GravityZone

GravityZone Ultra Control Center представляет собой интегрированную и централизованную консоль управления, которая предоставляет обзор всех компонентов управления безопасностью, включая безопасность конечных точек, центра обработки данных, "облачной" безопасности и защиты Exchange-сервера. Для GravityZone Ultra доступна только консоль с облачным хостингом. Центр управления GravityZone включает в себя несколько ролей и содержит сервер баз данных, коммуникационный сервер, сервер обновлений и веб-консоль.

GravityZone Ultra доступен с консолью облачных вычислений**.** Он защищает настольные компьютеры, серверы и почтовые ящики Exchange. Доля серверов должна составлять менее 35% от общего количества единиц.

Подробные системные требования см. на сайте www.bitdefender.com/business/enterprise-products/ultra-security

Bitdefender is a global security technology company that provides cutting edge end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on. More information is available at http://www.bitdefender.com.

Bitdefender