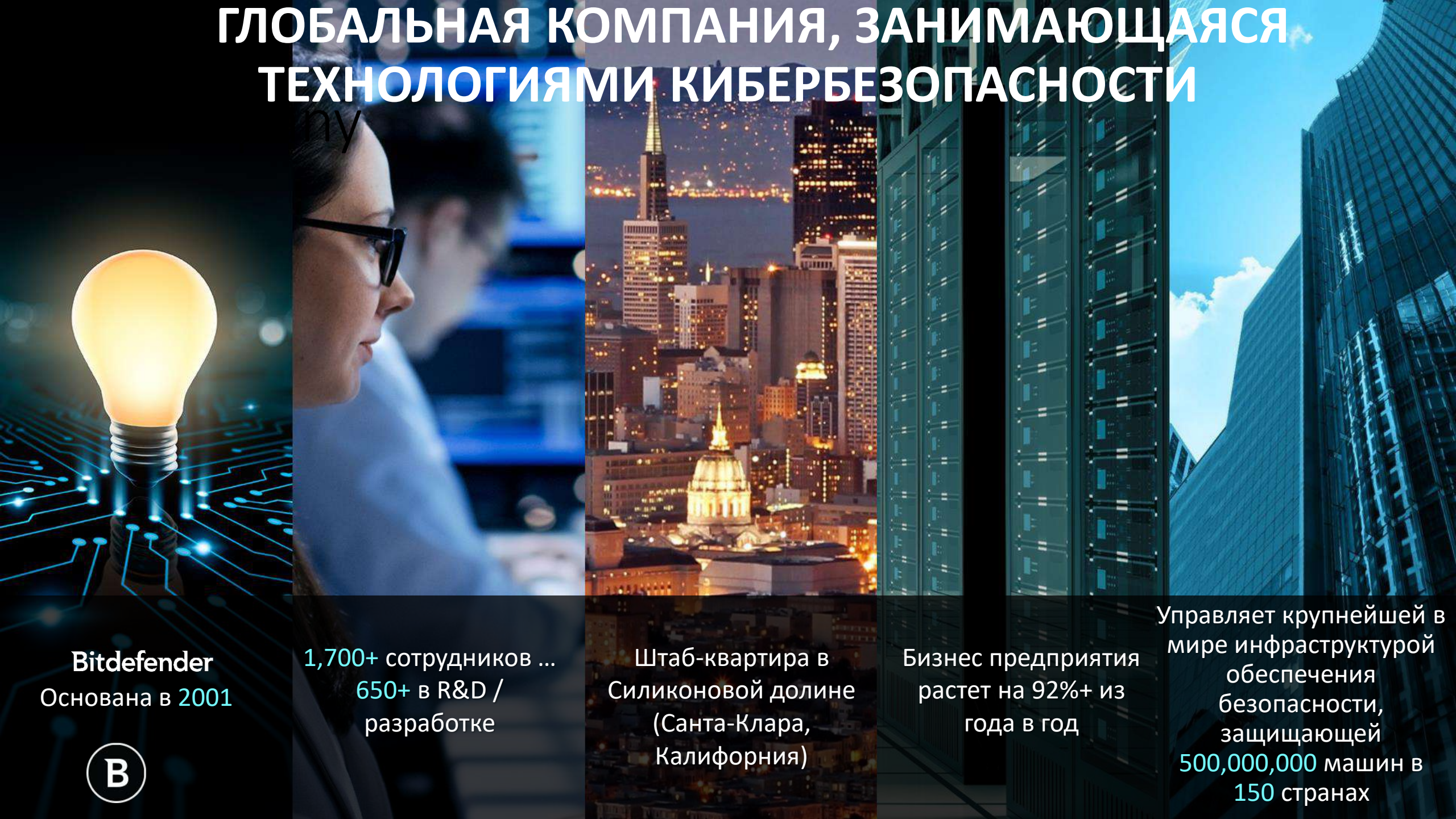
Bitdefender | softico

Bitdefender GravityZone
Многослойная защита следующего поколения



ГЛОБАЛЬНАЯ КОМПАНИЯ, ЗАНИМАЮЩАЯСЯ ТЕХНОЛОГИЯМИ КИБЕРБЕЗОПАСНОСТИ



Bitdefender
Основана в 2001

1,700+ сотрудников …
650+ в R&D / разработке

Штаб-квартира в Силиконовой долине (Санта-Клара, Калифорния)

Бизнес предприятия растет на 92%+ из года в год

Управляет крупнейшей в мире инфраструктурой обеспечения безопасности, защищающей 500,000,000 машин в 150 странах

Bitdefender

500 Million

Защищенных клиентов

Крупнейший мировой поставщик решений по обеспечению безопасности

150

Стран

150+

Партнеров



Bitdefender

ИСТОРИЯ ИННОВАЦИЙ

Патентное портфолио:
- 48 получено
- 28 ожидается

2019 Интегрированная аналитика рисков для конечных точек

2018 Многослойные EPP и EDR следующего поколения в одном

2017 Настраиваемое машинное обучение (HyperDetect)

2016 Самоанализ памяти на основе гипервизора (HVI)

2015 IoT безопасность (Bitdefender Box)

2014 Первое использование глубокого обучения для повышения скорости обнаружения

2013 Первый автоматизированный поток обнаружения на о обучения

2011 Интеллектуальное централизованное сканирование

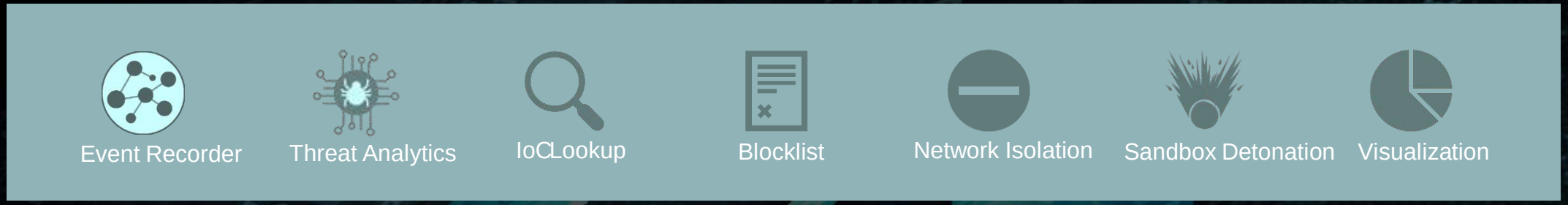
Первыми внедрили машинное обучение в 2008 г.

GRAVITYZONE PRODUCT BUNDLES AND OPTIONS

Функционал	Business Security	Advanced Business Security	Elite	Ultra	Enterprise
Console-Delivery Options	Локально/облачно	Локально/облачно	Локально/облачно	Облачно	Локально
Coverage					
Защита конечных точек	Да	Да	Endpoint Security HD	Endpoint Security XDR	Да
Защита мобильных устройств		Локально	Локально		Да
Защита виртуальной среды	Да	Да	Да	Да	Лицензирование по CPU, виртуальным серверам/машинам
Защита Exchange		Да	Да	Да	Да
Защита на уровне гипервизора (HVI)			Лицензирование по CPU (локально)		Лицензирование по CPU
Security Technologies					
Машинное обучение	Да	Да	Да	Да	Да
Анти-эксплойт	Да	Да	Да	Да	Да
Песочница			Да	Да	Да (Дополнительный модуль)
HyperDetect (Tunable ML)			Да	Да	Да (Дополнительный модуль)
Инспектор процессов (ATC)	Да	Да	Да	Да	Да
Удаление	Да	Да	Да	Да	Да
Централизованное сканирование (Offloaded to an SVA)		Да	Да	Да	Да
Видимость подозрительной активности			Да	Да	Да (Дополнительный модуль)
Контроль приложений	Черный список	Черный список	Черный список Белый список (локально)	Черный список	Черный список Белый список
EDR				Да	
Дополнительные модули					
Patch Management	Да	Да	Да	Да	Да
Лицензирование					

Bitdefender

Интегрированные EDR компоненты



- **Регистратор событий**
Захватывает и хранит информацию о действиях системы, связанных с файлами, процессами, установкой программы, модификацией реестра, сетевыми

- **Аналитика угроз**
Постоянно просеивается через данные регистратора событий, создавая приоритетный список инцидентов для расследования и ответа

- **Индикатор компромиссного поиска**
Предоставляет дополнительные сведения об угрозах и контекст от VirusTotal и Google

- **Блокировка и сетевая изоляция**
Позволяет администраторам системы блокировать вредоносные хэши файлов и предотвращать доступ уязвимой конечной точки к сети для ограничения угрозы

- **Детонация песочницы**
Позволяет ручную детонацию подозрительных файлов в Sandbox Analyzer

- **Визуализация**
Создает карту инцидентов, которая визуализирует события, связанные с подозрительным процессом, чтобы помочь сортировать инциденты

Bitdefender

Усиление и контроль инфраструктуры


Application Contro


Content Control


Anti-Phishing


Firewall


Device Contro


Full-Disk Encryption

- **Управление приложениями**
Поддерживает как «Default Deny», так и «Blacklisting»
Режим аудита или принудительного исполнения
Доверенное обновление

- **Брандмауэр**
Полнофункциональный двухсторонний персональный брандмауэр с контролем и предотвращением вторжений на основе хоста.

- **Контроль контента**
Проверяет входящий трафик и электронные письма
Блокирует URL-адреса на основе поведения и машинного обучения
Фильтр веб-категории

- **Управление устройством**
Позволяет администраторам управлять разрешениями для внешних устройств, таких как флэш-накопители USB, устройства Bluetooth и другие

- **Анти-Фишинг**
Блокирует веб-страницы фишинга для предотвращения непреднамеренного раскрытия пользователями частной или конфиденциальной информации.

- **Полное шифрование диска**
Windows BitLocker и Mac OS FileVault для собственного шифрования с централизованным развертыванием, управлением и восстановлением ключей из Центра управления GravityZone

Bitdefender

Предотвращение угроз



Machine Learning



HyperDetect



Sandbox Analyzer



Anti-Exploit



Process Inspector

- Динамическое машинное обучение
Алгоритмы, обученные фильтрации URL-адресов и анализу файлов
на 500M конечных датчиках и триллионах образцов обеспечивают максимальную эффективность при низких ложных срабатываниях

- HyperDetect
Новые модели перестраиваемого машинного обучения и анализа поведения, подготовленные для обнаружения передовых, сложных угроз при предварительном исполнении

- Анализатор песочницы
Автоматическая отправка подозрительных файлов с конечных точек в облачную песочницу для детонации и поведенческого анализа

- Предотвращение использования
Обнаруживает методы эксплойтов и защищает пространство памяти браузеров, просмотр документов, медиаплееров и офисных приложений

Инспектор процессов
Упреждающее динамическое обнаружение неизвестных угроз на основе непрерывного мониторинга и подсчета запущенных процессов и системных событий и пометки подозрительных действий

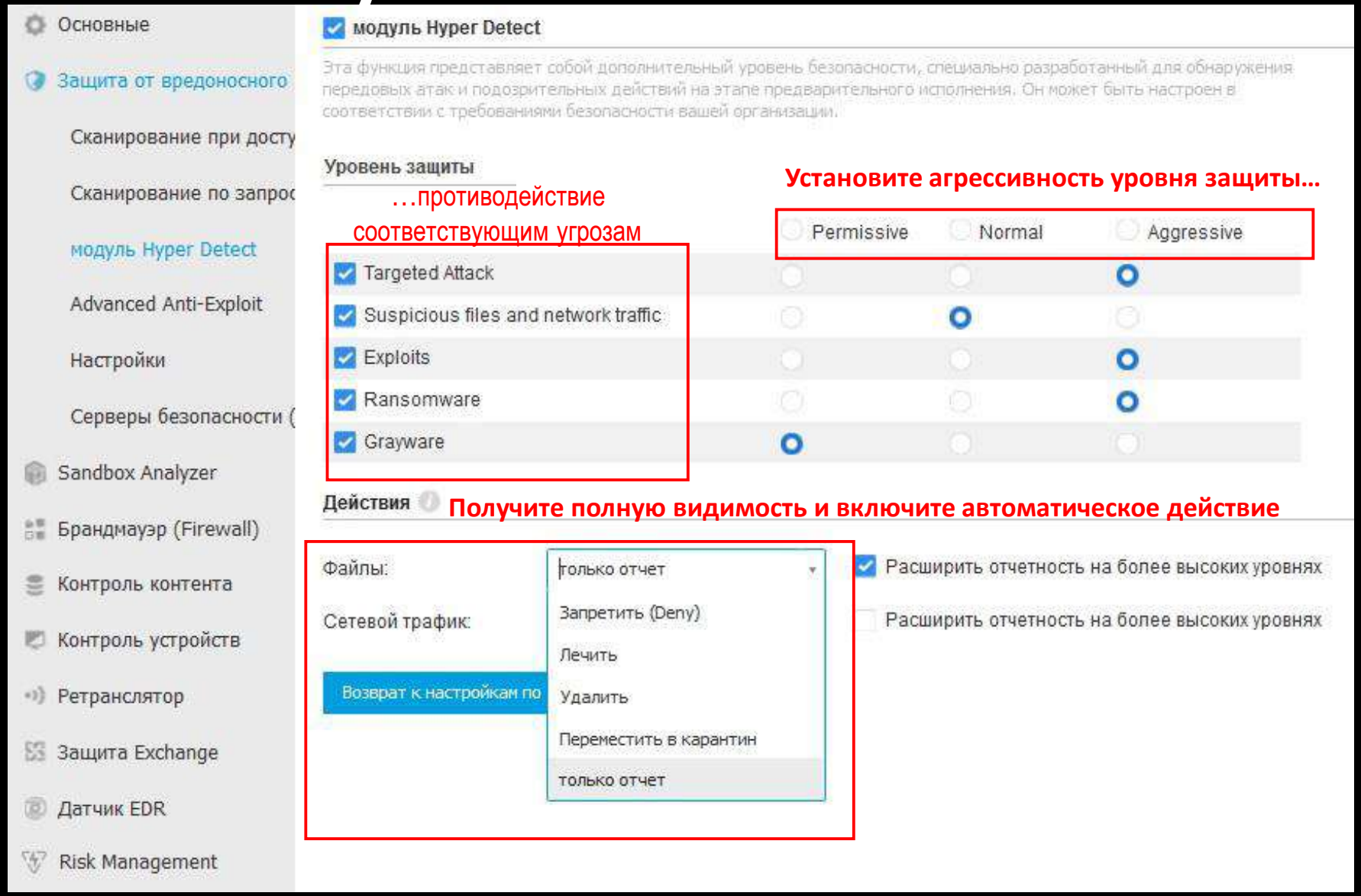
Hyperdetect – Настраиваемое Машинное Обучение

Защищает от:
- Вирусов-вымогателей
- Эксплойтов

* Атаки без файлов
* Атаки на основе сценариев

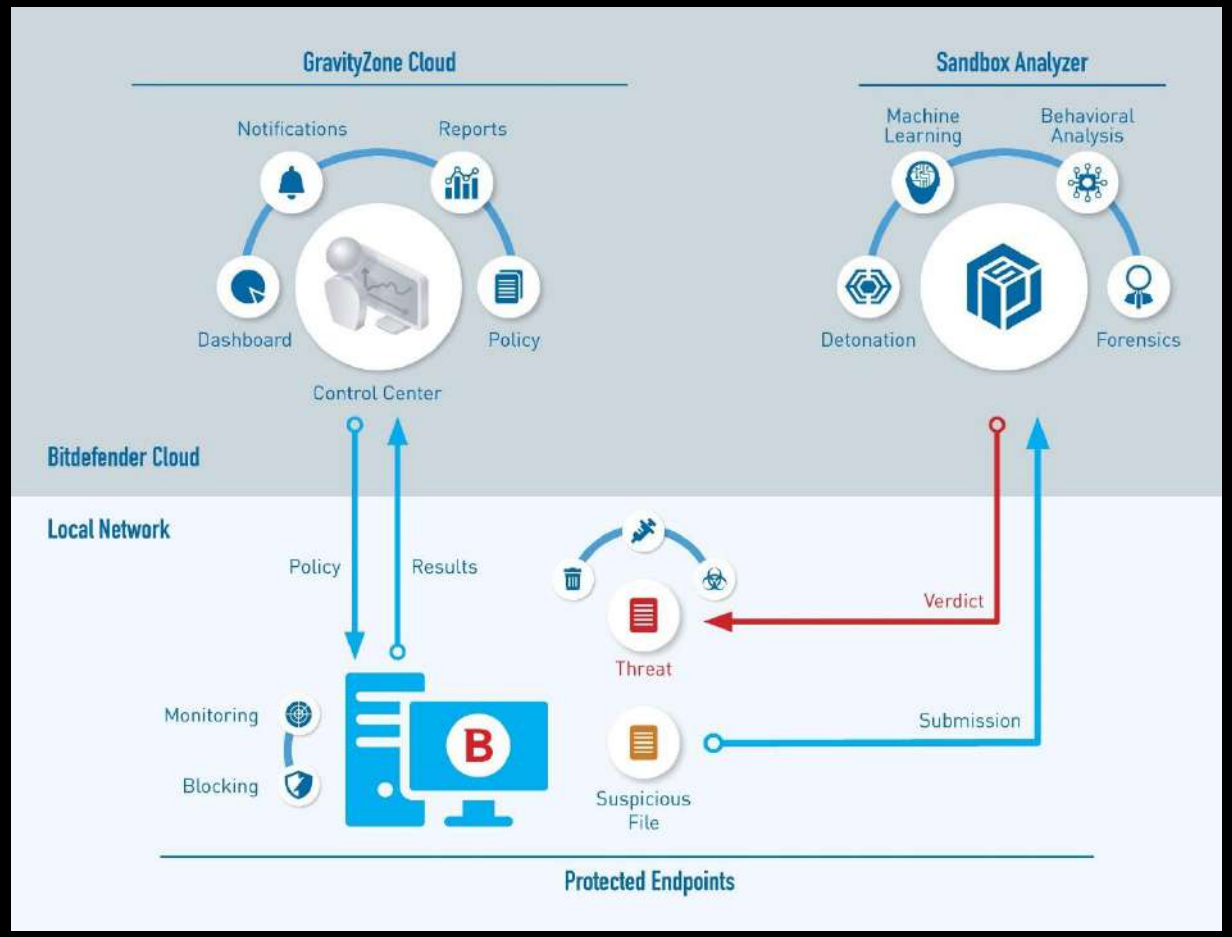
Обеспечивает максимальную точность обнаружения без ложных срабатываний

Обеспечивает полную видимость подозрительных действий



Песочница (sandbox analyzer)

Защищает от:
* Расширенных целевых атак
* Пользовательских вредоносных программ
* Неизвестных упаковщиков



Использует машинное обучение и поведенческий анализ для оценки подозрительных файлов

Работает в режиме блокировки или мониторинга

Обеспечивает вердикт в режиме, близком к реальному времени, и принимает меры по исправлению ситуации на основе настроек политики

Предоставляет подробные отчеты о поведении вредоносных программ

Bitdefender

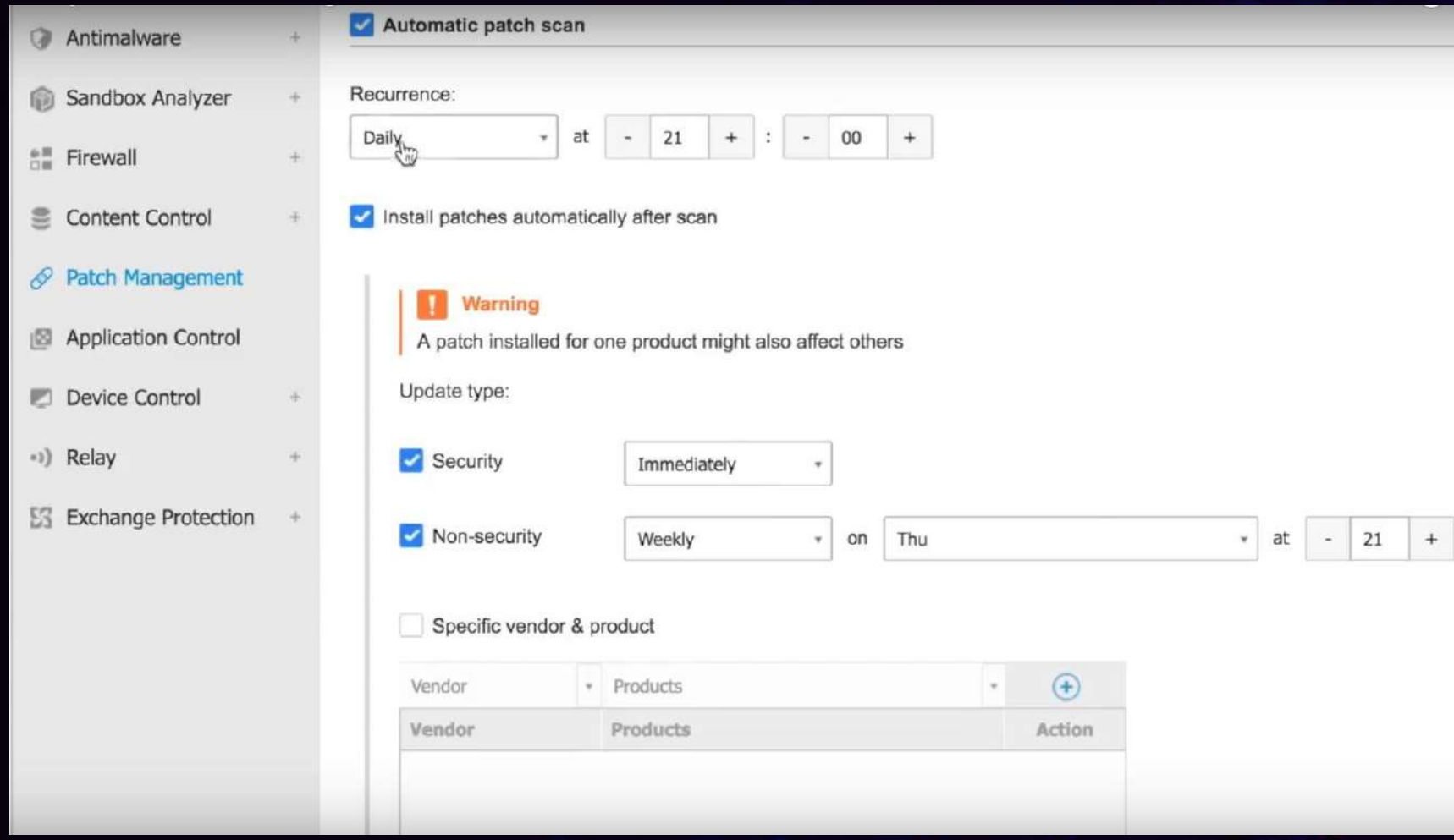
PATCH MANAGEMENT ADD-ON

Помогает улучшить состояние безопасности за счет оперативного обнаружения и устранения уязвимостей

Предоставляет самый широкий спектр исправлений безопасности для операционных систем, сторонних приложений и образов

Охватывает физические, виртуальные локальные и облачные конечные точки и серверы на базе Windows

Развертывается и управляется с консоли GravityZone и интегрируется в его агент



Bitdefender

BITDEFENDER GravityZone: ключевые преимущества

Простота и легкость использования: Администрирование из GravityZone Control Center, с отдельными видами и конкретными наборами политик для каждой из трех служб безопасности.

Одна платформа защиты для всех регионов: Архитектура позволяет защищать в глобальном масштабе организационные единицы в распределённых регионах. GravityZone может быть подключена и управляться централизованно из различных местных развертываний по всему миру.

Развертывание под ключ на одном виртуальном устройстве : Облегчение администрирования - начальная настройка из командной строки и конфигурация сканирования, без необходимости установки и настройки других компонентов.

Гибкое модульное лицезирование: Каждая служба безопасности лицензируется отдельно и может быть активирована при необходимости с ростом бизнеса. Лицензирование по процессорным разъёмам обеспечивает еще большую гибкость для компаний с VDI инфраструктурой.

Bitdefender Email security (защита Office 365)



Bitdefender

softico

Bitdefender Email Security

- Высокая точность категоризации электронной почты
- Блокирует вредоносную электронную почту
- Допускает законные электронные письма
- Классификация репутации (высокий/средний/низкий)
- Большинство почтовых продуктов используют один движок
- Bitdefender Email Security имеет более 10000 алгоритмов
- Анализирует 137 атрибутов каждого письма за 0,2 секунды.
- Полностью интегрирован с Bitdefender Sandbox (входит в комплект)
- Использует механизмы сканирования вредоносных программ Bitdefender (в комплекте)
- Сканирование каждого перенаправления.
- Некоторые вредоносные программы используют 128 перенаправлений

Bitdefender NTSA

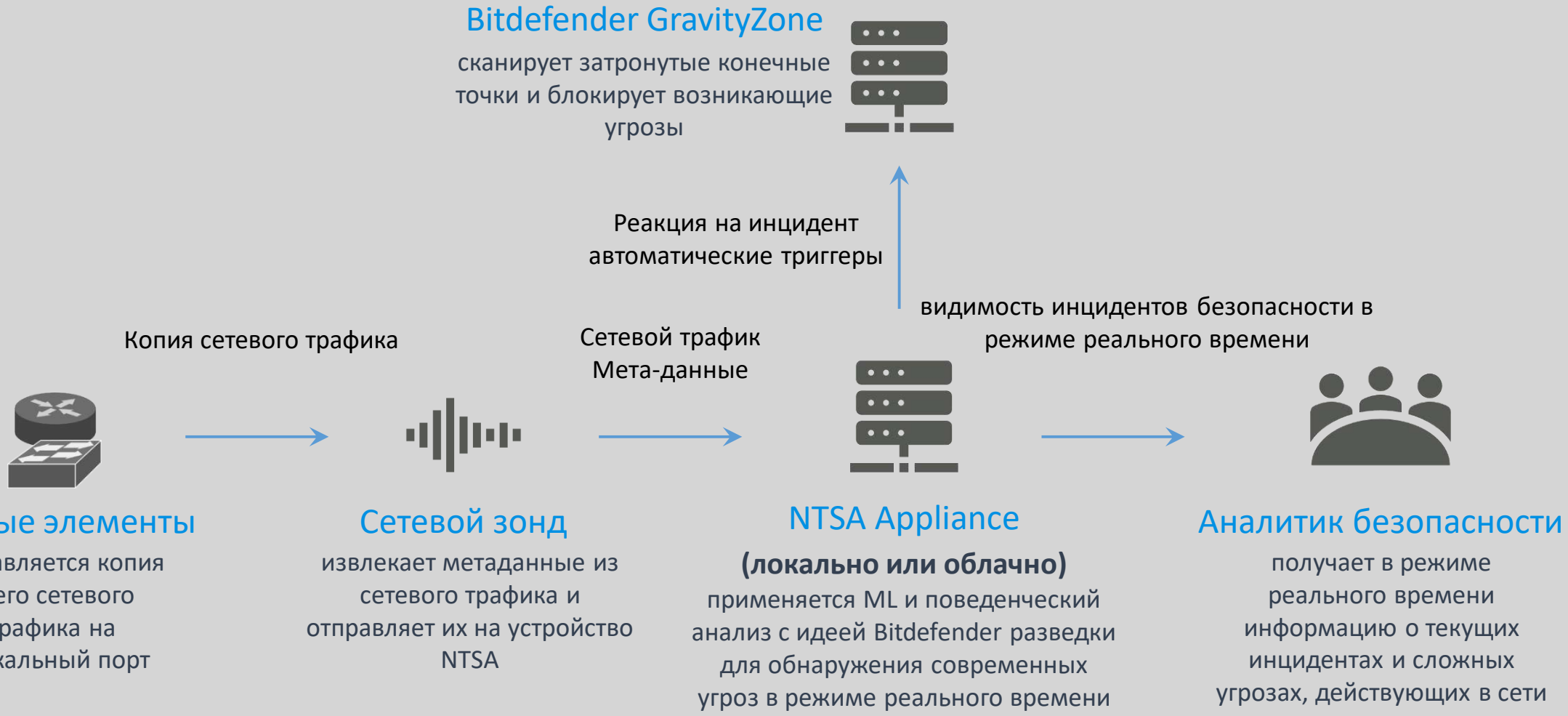


Bitdefender

softico

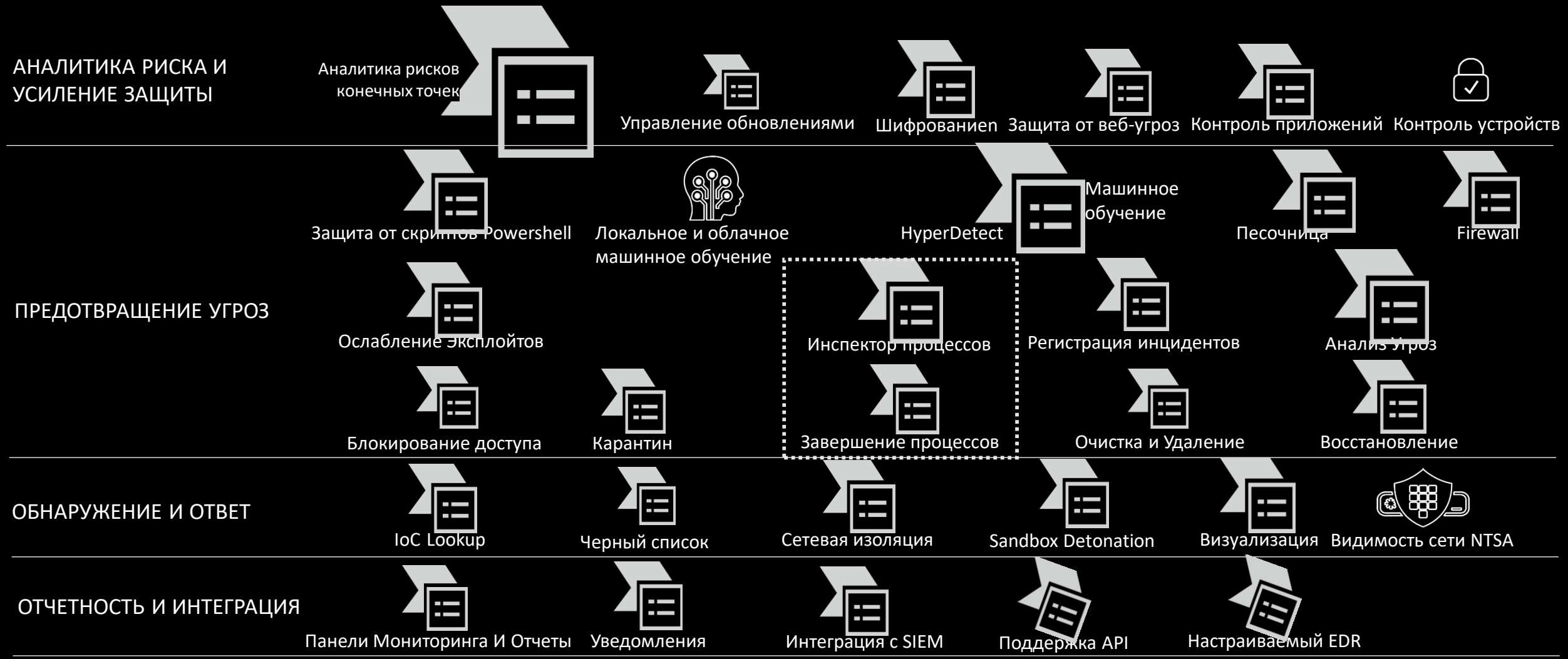
Обнаружение расширенных угроз в режиме реального времени

КАК РАБОТАЕТ NTSA?



Gravity Zone

Предотвращение, профилактика, обнаружение, реагирование и анализ рисков



Дополнительные преимущества Bitdefender

- Полноценная БЕСПЛАТНАЯ поддержка в Украине, специалисты которой сертифицированы вендором, и имеют многолетний опыт по настройке, развертыванию и поддержке.
- Наличие технических отчетов по результатам исследований кибератак, направленных против Украинских компаний, что свидетельствует об осведомленности специалистов вирусной лаборатории о состоянии киберугроз в УКРАИНЕ.
- Исследование подозрительных файлов или анализ журналов, осуществляются специалистами технической поддержки в Украине без пересылки в другие страны.
- Возможность бесплатно привлечь технических специалистов разработчика к работам по анализу инфраструктуры, настройки автоматизированной системы.
- Возможность бесплатно пригласить технических специалистов разработчика для участия во внутренних конференциях по информационной безопасности, с целью информирования о современных угрозах и методах противостояния путем внедрения необходимых настроек существующей инфраструктуры.
- Возможность заказать для системных администраторов бесплатные учебные курсы, которые будут проведены техническими специалистами разработчика, как в представительстве разработчика в Киеве, так и на базе клиента.
- Возможность использования антивирусных продуктов при условии, что управление ими будет осуществляться существующими имеющимися серверами
- Возможность устанавливать актуальные версии антивирусных продуктов на все версии ОС Windows, начиная с Windows XP SP2
- Наличие в вирусной лаборатории специального подразделения, занимающегося мониторингом и исследованием сложных угроз, таких как целенаправленные атаки, шифровальщики, и тому подобное. Результаты опытов дают возможность добавлять необходимые DNA-сигнатуры таких угроз к вирусной базе еще до того, как они начали свою активность, то есть не постфактум, а заранее.

• BITDEFENDER Експертний висновок Держспецзв'язку



ЕКСПЕРТНИЙ ВИСНОВОК

Програмний комплекс захисту інформаційних ресурсів «Bitdefender GravityZone Advanced Business Security» версії 6.x

виробництва компанії Bitdefender SRL (Румунія)

Зареєстровано в Адміністрації Державної служби спеціального зв'язку та захисту інформації України

"13" грудня 2019 р. за № **1062**
Дійсний до "13" грудня 2022 р.

Результати експертизи свідчать, що

програмний комплекс захисту інформаційних ресурсів «Bitdefender GravityZone Advanced Business Security» версії 6.x,
(назва засобу ТЗІ)

який наданий на експертизу **ТОВ «СОФТІКО ЮА»,**
найменування організації (підприємства,

м. Київ, вул. Борисоглібська, буд. 15-в,
установи) – власника (розпорядника), місцезнаходження)

відповідає
(відповідає/не відповідає)

вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених в документі «Програмний комплекс захисту інформаційних ресурсів «Bitdefender GravityZone Advanced Business Security» версії 6.x. Технічні вимоги щодо захисту інформації від несанкціонованого доступу».

Вимоги до умов експлуатації та сфери використання об'єкта експертизи визначені у відповідних розділах Експертного висновку.

Директор
ТОВ «ІВМАР УКРАЇНА» **В.С. Кузнєцов**
ініціали, прізвище



ЕКСПЕРТНИЙ ВИСНОВОК

Програмний комплекс Bitdefender GravityZone Elite Security версії 6.x

виробництва компанії Bitdefender SRL (Румунія)

Зареєстровано в Адміністрації Державної служби спеціального зв'язку та захисту інформації України

"23" квітня 2019 р. за № **946**
Дійсний до "23" квітня 2022 р.

Результати експертизи свідчать, що

програмний комплекс захисту інформаційних ресурсів Bitdefender GravityZone Elite Security версії 6.x,
(назва засобу ТЗІ)

який наданий на експертизу **ТОВ «СОФТІКО ЮА»,**
найменування організації (підприємства,

м. Київ, вул. Борисоглібська, 15-В,
установи) – власника (розпорядника), місцезнаходження)

відповідає
(відповідає/не відповідає)

вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у документі «Програмний комплекс захисту інформаційних ресурсів Bitdefender GravityZone Elite Security версії 6.x. Технічні вимоги щодо захисту інформації від несанкціонованого доступу».

Вимоги до умов експлуатації та сфери використання об'єкта експертизи визначені у відповідних розділах Експертного висновку.

Директор
ТОВ «ІВМАР УКРАЇНА» **В.С. Кузнєцов**
ініціали, прізвище

Bitdefender

СПАСИБО!



Александр Бутусов
Head of Information Security Solutions Department
Тел. (044) 383-44-10 (вн.947)
Тел. (099) 712-76-58
email: abt@softico.ua

PROTECTING **500 MILLION USERS** WORLWIDE

softico