ОБЗОР РЕШЕНИЙ

ПРОДВИНУТАЯ ЗАЩИТА КОНЕЧНЫХ СТАНЦИЙ

АЛЕКСАНДР РУСЕЦКИЙ,
эксперт Центра информационной безопасности
компании «Инфосистемы Джет»

ВСТУПЛЕНИЕ

На протяжении последних лет одним из основных способов компрометации ИТ-инфраструктуры для хакеров остается атака на рабочие станции. Злоумышленники успешно применяют методы социальной инженерии, эксплуатируя доверчивость и низкую бдительность пользователей, что приводит к захвату контроля над ПК пользователей.

Стратегия большинства организаций по защите конечных станций при этом остается неизменной: многие компании по-прежнему сосредоточены на блокировке атак, применяя традиционные встроенные средства защиты и классические антивирусы, нацеленные на предотвращение первичного заражения.

Такой подход имеет ряд недостатков. Во-первых, невозможно предотвратить все атаки. Во-вторых, офицеры ИБ не всегда могут вовремя среагировать на атаку. Это связано с анализом множества мелких событий и началом расследования только по факту инцидента. И наконец, в-третьих, классические средства защиты не содержат инструменты по устранению последствий атак.

Отметим также, что традиционные средства защиты зачастую не успевают за новыми угрозами и специально кастомизированными для конкретной компании вредоносами. Так, крайне сложно обнаружить и отследить бесфайловые атаки, при которых вредоносное программное обеспечение не размещает никаких файлов на жестком диске, а вместо этого полезная нагрузка загружается непосредственно в оперативную память. Как результат, например, компьютер становится жертвой вируса-шифровальщика, используется для проникновения в корпоративную сеть или майнинга криптовалют в интересах злоумышленников.

Таким образом, для всесторонней защиты конечных станций недостаточно предотвращения максимального количества известных угроз. Здесь требуется комплексный подход, включающий все перечисленные этапы: предотвращение, передовое обнаружение, реагирование, устранение последствий атак и расследование. Обеспечить такую функциональность позволяет совместная эксплуатация решений класса EPP и EDR.

EPP (Endpoint Protection Platform)

Класс решений, предназначенный для предотвращения и блокирования известных угроз, обнаружения вредоносной активности.

Комплексная защита конечных станций, включающая классический антивирус, расширенные технологии безопасности (персональный межсетевой экран, система предотвращения вторжений, контроль приложений, управление съемными носителями и др.) и инструменты расследования и восстановления.

EDR (Endpoint Detection&Response)

Класс решений, предназначенный для обнаружения и реагирования на продвинутые угрозы.

Данный класс решений оперативно выявляет отклонения в поведении приложений и объектов с возможностью их быстрого восстановления в случае подтверждения инцидента офицером безопасности. Системы EDR не опираются на сигнатуры или черные списки.

Зачастую такие решения интегрируются, в том числе, и с сетевыми «песочницами», что значительно повышает эффективность их использования. В этом случае, даже если не удастся спасти конкретный узел, и он, например, станет жертвой шифровальщика, хранимые централизованно детальные логи не будут потеряны, и ИБ-инженер сможет разобраться в причинах заражения и принять необходимые меры для блокирования дальнейшего распространения вредоноса в сети.

На сегодняшний день на рынке представлены также платформы, сочетающие в себе возможности EPP и EDR: они содержат полный набор функций решений обоих классов и при этом имеют единый интерфейс.

Тема продвинутой защиты конечных станций остается дискуссионной. Многие эксперты, игроки рынка, аналитические агентства по-разному позиционируют того или иного производителя, исходя из критериев сравнения и функционала решений.

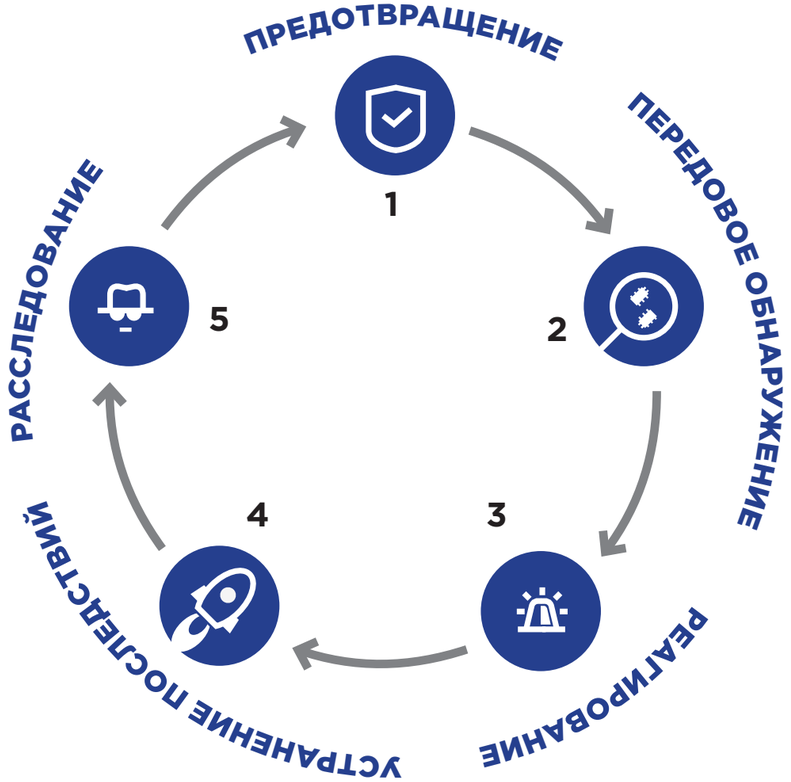
В НАСТОЯЩИЙ ОБЗОР* ВКЛЮЧЕНЫ СЛЕДУЮЩИЕ РЕШЕНИЯ:

- **FireEye HX**
- **CyberBit**
- **Carbon Black Response**
- **Check Point SandBlast Agent**
- **Kaspersky EDR**
- **Symantec EDR**
- **Trend Micro Apex One**

В ОСНОВЕ КРИТЕРИЕВ ОЦЕНКИ ЛЕЖИТ НЕ ТОЛЬКО СТАНДАРТНЫЙ ФУНКЦИОНАЛ РЕШЕНИЙ, НО И КЕЙСЫ ЗАКАЗЧИКОВ, А ТАКЖЕ СОБСТВЕННЫЙ ОПЫТ КОМПАНИИ «ИНФОСИСТЕМЫ ДЖЕТ» В ТЕСТИРОВАНИИ, ЭКСПЛУАТАЦИИ И ВНЕДРЕНИИ ПРОДУКТОВ ДЛЯ ПРОДВИНУТОЙ ЗАЩИТЫ КОНЕЧНЫХ СТАНЦИЙ.

*-Информация в обзоре актуальна на конец декабря 2018 г.

ОСНОВНЫЕ ФУНКЦИОНАЛЬНЫЕ БЛОКИ РЕШЕНИЙ ПО ПРОДВИНУТОЙ ЗАЩИТЕ КОНЕЧНЫХ СТАНЦИЙ



1. ПРЕДОТВРАЩЕНИЕ (PREVENT)

Предотвращение – блокирование общих угроз и защита основных систем для снижения риска продвинутых угроз. Решения включают в себя не только антивирусные технологии, но и технологии репутации, поведенческого анализа, управления приложениями и устройствами, что позволяет блокировать угрозы самым эффективным способом. Данный функционал реализован в решениях класса EPP.

Возможно пересечение некоторых функций EPP- и EDR-решений.

2. ПЕРЕДОВОЕ ОБНАРУЖЕНИЕ (DETECT)

Передовое обнаружение – постоянный мониторинг, исследование и обнаружение продвинутых угроз. Решения позволяют искать свидетельства взлома во всей сети в режиме реального времени, сопоставлять предупреждения, поступающие из средств управления сетевой безопасностью, с событиями на рабочих местах в режиме реального времени. Для этого используются комбинации различных механизмов и методов детектирования, таких как статический анализ, машинное обучение, ретроспективный анализ и т.д. Данный функционал реализован в решениях класса EDR.

Возможно пересечение некоторых функций EPP- и EDR-решений.

3. РЕАГИРОВАНИЕ (RESPONSE)

Реагирование – управление инцидентом и оперативная нейтрализация атаки для смягчения последствий. Решения сочетают технологии передового обнаружения и реагирования, что позволяет сократить время жизни угроз с нескольких дней или недель до считанных минут. Оперативное реагирование на инциденты обеспечивается за счет корреляции тысяч событий с последующим выделением наиболее подозрительных. Ответные меры могут включать остановку процесса на хосте, запрет запуска исполняемого файла, удаленную модификацию реестра и изоляцию хоста. Оперативная визуализация полной цепочки инцидента, реагирование и остановка атаки занимают несколько минут, что является залогом смягчения последствий угроз. Данный функционал реализован в решениях класса EDR.

Возможно пересечение некоторых функций EPP- и EDR-решений.

4. УСТРАНЕНИЕ ПОСЛЕДСТВИЙ (REMEDIATION)

Устранение последствий – полное удаление инфекции и ее следов с минимальным воздействием на конечных пользователей. Решения включают инструментарий по устранению последствий угроз и позволяют отменить изменения, внесенные зловредным программным обеспечением. В этом случае файлы и реестр возвращаются в первоначальное состояние.

Возможно пересечение некоторых функций EPP- и EDR-решений.

5. РАССЛЕДОВАНИЕ (INVESTIGATION)

Расследование – быстрый сбор и анализ информации, оперативное принятие мер. Решения содержат инструменты комплексного оперативного расследования и глубокого анализа целевой атаки. Данные платформы позволяют аналитикам, ИБ-офицерам, сотрудникам SOC и центрам реагирования быстро собрать и проанализировать информацию в автоматическом или ручном режимах и оперативно принять меры. Важно учитывать, что ручной разбор инцидента занимает продолжительное время и может негативно сказаться на бизнес-процессах при вмешательстве аналитика в работу хоста.

Возможно пересечение некоторых функций EPP- и EDR-решений.

ДОПОЛНИТЕЛЬНЫЕ ФУНКЦИОНАЛЬНЫЕ БЛОКИ

- ЗАЩИТА ОТ ШИФРОВАЛЬЩИКОВ
- ИНТЕГРАЦИЯ
- СООТВЕТСТВИЕ ТРЕБОВАНИЯМ
- РАЗНОЕ

ЗАЩИТА ОТ ШИФРОВАЛЬЩИКОВ

На фоне большого количества атак вирусов-шифровальщиков данный кейс как один из драйверов роста популярности темы защиты конечных станций мы вынесли в отдельный блок. WannaCry и Petya – яркие примеры быстро распространяющегося червя и деструктивного вируса-вымогателя.

Для борьбы с такими видами угроз производители применяют комплекс мер, включающий и поведенческий анализ, и машинное обучение. Например, решения обнаруживают и завершают процессы, которые пытаются манипулировать теневыми копиями, главной загрузочной записью, определенным набором контролируемых файлов на конечной точке. При этом некоторые продукты позволяют проактивно создавать краткосрочные бэкапы «на ходу» и восстанавливать зашифрованные файлы.

Данный функционал входит в базовые возможности некоторых EPP-решений, а также реализован в EDR.

СТОРОННЯЯ ИНТЕГРАЦИЯ

Наличие API позволяет проводить интеграцию системы и сторонних решений. Например, часть решений реализуют проверку подозрительных объектов с хостов в «песочнице» с получением соответствующего вердикта / обратной связи.

Возможно пересечение некоторых функций EPP- и EDR-решений.

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

Решения позволяют организациям достичь соответствия стандартам, требуемым крупными регулирующими органами, например, PCI DSS. В основе соответствия лежат способность постоянного мониторинга активов, отслеживание и применение политик управления изменениями, возможность аудита.

Возможно пересечение некоторых функций EPP- и EDR-решений.

ОБЩАЯ ИНФОРМАЦИЯ О ВЕНДОРЕ

Продукт	FireEye HX	CyberBit	Carbon Black Response	Check Point SandBlast Agent	Kaspersky EDR	Symantec EDR	Trend Micro Apex One
	FireEye Inc США, Калифорния **www.fireeye.com**	**CyberBit** Израиль, Тель-Авив **www.cyberbit.com**	**Carbon Black** США, Уолтем **www.carbonblack.com**	**Check Point Software Technologies Ltd** Израиль, Тель-Авив **www.checkpoint.com**	**АО «Лаборатория Касперского»** Россия, Москва **www.kaspersky.ru**	**Symantec Corporation** США, Калифорния **www.symantec.com**	**Trend Micro Inc** Япония, Токио **www.trendmicro.com**
Собственное представительство в России	🔴	🔴	🔴	🟢	🟢	🟢	🟢
Дистрибьютор в России	• Axoft • Netwell	• ITD Group	• АО «Инфосистемы Джет» (прямой партнер)	• Mont • RRC • OCS	• Axoft • Mont	• Web Control • Mont • Merlion	• Axoft • Mont

🟢 да 🟡 частично 🔴 нет

АРХИТЕКТУРА РЕШЕНИЙ

Продукт	FireEye HX	CyberBit	Carbon Black Response	Check Point SandBlast Agent	Kaspersky EDR	Symantec EDR	Trend Micro Apex One
Основные компоненты	• Агенты • Контроллер	• Агенты • Хранилище больших данных	• Агенты • Хранилище данных	• Агенты	• Агенты • Центр анализа (Central Node) • «Песочница»	• Агенты • База данных • Центр обработки	• Агенты • Хранилище данных
Комментарии вендоров	К основным компонентам опционально относится и DMZ-контроллер.		Дополнительные продукты вендора: • Carbon Black Protection (контроль приложений и защита критической инфраструктуры) • Carbon Black Defense (продвинутый облачный антивирус с функционалом EDR).	В зависимости от количества модулей можно выделить пакеты решений: • SandBlast Agent Anti-Ransomware (в составе только модуль для борьбы с шифровальщиками) • SandBlast Agent (без модуля антивируса) • SandBlast Agent Next Generation AV (NGAV) (с антивирусным модулем) • Endpoint Complete Protection Suite (с максимальным набором модулей, в том числе с шифрованием).	Central Node включает базу данных и вердиктов, механизмы обнаружения, анализатор целевых атак (Targeted Attack Analyzer). Kaspersky EDR (KEDR) поставляется как на базе единого программного агента с Kaspersky Endpoint Security для бизнеса (KES v11), так и как отдельный агент.	Агенты на рабочих местах на базе единого программного агента с Symantec Endpoint Protection (SEP v 14). Центр обработки поставляется в виде физического или виртуального устройства.	Единый программный агент (Office Scan с Endpoint Sensor).
Дополнительные компоненты **Рассматриваемые решения могут работать как автономно, так и в связке с дополнительными компонентами.**	• NX-анализ веб-трафика • EX-анализ почты • AX-платформа для анализа угроз • FX-анализ файловых хранилищ	• SOC3D – платформа реагирования на инциденты информационной безопасности	• Агент Carbon Black Protection • «Песочница»	• «Песочница» Check Point SandBlast • Шлюз безопасности Check Point	• Kaspersky Anti Targeted Attack Platform (передовая защита от сложных угроз и целевых атак на уровне сети) • Kaspersky Private Security Network (локальная копия репутационной базы угроз Kaspersky Security Network)	• Сетевой сканер Advanced Threat Protection for Network (ATP:Network) • Анализ почты Advanced Threat Protection for Email (ATP:Email) использует Email Security Cloud • Локальная «песочница» Content Analysis Service/ Malware Analysis (CAS/MA) • EDR Cloud	• «Песочница» Deep Discovery Analyzer (DDaN)
Единая консоль управления	●	●	●	●	●	●	●
Комментарии вендоров						В состав решения входят две консоли. Одна для управления агентами, другая для обработки и анализа данных.	
Позиционирование продукта	**EDR-агент**	**EDR-агент**	**EDR-агент**	**EPP + EDR**	**EPP + EDR**	**EPP + EDR**	**EPP + EDR**
	Часть решений позиционируется как независимые EDR, поэтому они в качестве легких агентов устанавливаются к текущему продвинутому антивирусу (EPP) на конечной станции. Другие поставляются единым агентом (EPP + EDR).						

● да ● частично ● нет

1. ПРЕДОТВРАЩЕНИЕ (PREVENT)

Продукт	FireEye HX	CyberBit	Carbon Black Response	Check Point SandBlast Agent	Kaspersky EDR	Symantec EDR	Trend Micro Apex One
Наличие антивирусного движка в составе решения	●	●	●	●	●	●	●
Комментарии вендоров			Антивирус есть в отдельном продукте Carbon Black Defense.	Антивирус есть в пакетах SandBlast Agent NGAV, Endpoint Complete Protection Suite.			
Вендор антивирусного движка	Bitdefender	---	---	Kaspersky/Bitdefender	Kaspersky	Symantec	Trend Micro
Комментарии вендоров		Антивирус заявлен в RoadMap.	В дополнительном продукте Carbon Black Defense используется технология, которая может обнаруживать атаки, анализируя действия конечных точек в контексте последовательностей, как они разворачиваются (Streamline Prevention).	В пакетах SandBlast NGAV, Endpoint Complete Protection Suite антивирусный движок Kaspersky (по умолчанию) или BitDefender (на выбор).			
Используемые технологии в антивирусе для предотвращения угроз							
Комментарии вендоров	• Анализ сигнатур • Эвристический анализ	В зависимости от установленного EPP-агента стороннего производителя. В RoadMap заявлен функционал антивируса, включающий сигнатуры и поведенческий анализ.	В зависимости от установленного EPP-агента стороннего производителя.	Сигнатурное сканирование системы, включая файловую систему, съемные носители, сетевые папки, почтовые сообщения, архивы.	• Поведенческий анализ • Машинное обучение • Антикриптор • Эвристический анализ • Обращение в облачную репутационную базу угроз • Защита от вымогателей • Защита от мобильных угроз • Защита от эксплойтов • Механизм восстановления	• Анализ репутации • Эмулятор • Машинное обучение • Анализ сигнатур • Блокировка эксплойтов • Анализ поведения • Сетевой файрвол и IPS • Управление приложениями и устройствами	• Анализ сигнатур • Анализ репутации • Машинное обучение (Predictive Machine Learning) • Поведенческий анализ
1.1. Обнаружение для автоматического блокирования **1.1.1. Выявление активности в ОС на конечной станции**							
Мониторинг запуска исполняемых файлов	●	●	●	●	●	●	●
Мониторинг запуска скриптов (включая bat, ps, js, vbs и т.д.)	●	●	●	●	●	●	●
Мониторинг изменения реестра	●	●	●	●	●	●	●
Контроль целостности файлов	●	●	●	◐	◐	◐	●
Комментарии вендоров	Требуется интеграция с текущим EPP-агентом с соответствующим функционалом.	Требуется интеграция с текущим EPP-агентом с соответствующим функционалом.	Требуется интеграция с отдельным агентом Carbon Black Protection или с текущим EPP-агентом с соответствующим функционалом.	Агент проверяет целостность своих собственных файлов и защищает их от удаления и модификации.	Контроль целостности файлов выполняется в рамках агента Kaspersky Embedded Systems Security (KESS) или Kaspersky Security для Windows Server (KSWS).	Контроль целостности только исполняемых файлов при помощи функционала system lockdown в режиме белого списка.	
Определение пользователя, под которым запускается процесс	●	●	●	●	●	●	●
Определение процесса, запустившего процесс	●	●	●	●	●	●	●

● да ◐ частично ● нет

Продукт	FireEye HX	CyberBit	Carbon Black Response	Check Point SandBlast Agent	Kaspersky EDR	Symantec EDR	Trend Micro Apex One
Определение создания, чтения, изменения произвольных файлов Комментарии вендоров	🟢	🔴 Требуется интеграция с текущим EPP-агентом с соответствующим функционалом.	🟢	🟢	🟢	🟢	🟢
Выявление внедрения произвольного кода в память процесса (code injection)	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Выявление использования системных функций Windows для исполнения произвольного кода (WMI/ PSEXEC) Комментарии вендоров	🟢	🟢	🟢	🟡 Если команды запускаются непосредственно на защищаемой станции (Shell, PowerShell), то они логируются агентом с помощью модуля Forensics. На уровне сети угроза закрывается с помощью шлюзов безопасности Check Point или модулем агента – Endpoint Firewall (доступен во всех пакетах SandBlast Agent).	🟢	🔴	🟢
Выявление использования системных функций Windows для закрепления на хосте – задача в планировщике/ запись в реестре для автозагрузки	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Выявление запуска процесса с повышенными привилегиями Комментарии вендоров	🔴	🟢	🟡 Если процесс уже запущен с повышенными привилегиями, его невозможно идентифицировать.	🟢	🟢	🔴	🟢
Выявление действий по сокрытию вредоносной активности	🟢	🟢	🟢	🟢	🟢	🟢	🟢
1.1.2. Выявление сетевой активности на конечной станции							
Регистрация исходящих сетевых соединений	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Мониторинг DNS-трафика, включая процесс инициатора DNS-обращения Комментарии вендоров	🟢	🔴 Мониторинг DNS-трафика заявлен в RoadMap.	🟢	🔴 Данный функционал реализуется на дополнительном компоненте (шлюзе безопасности Check Point) с помощью модуля Anti-Bot.	🟢	🟢 Используются сигнатуры IPS и custom-IPS, входящие в агент Symantec Endpoint Protection (SEP).	🟢
Выявление аномалий DNS-трафика Комментарии вендоров	🟢 Обнаружение вредоносных доменов.	🔴 Данный функционал заявлен в RoadMap.	🟢 Обнаружение вредоносных доменов.	🔴 Данный функционал реализуется на дополнительном компоненте (шлюзе безопасности Check Point) с помощью модуля Anti-Bot.	🟢	🔴 Для защиты от DNS-туннелирования можно использовать DNS-сервер без доступа ко внешним DNS-зонам и непрозрачный веб-прокси.	🟢

🟢 да 🟡 частично 🔴 нет

Продукт	FireEye HX	CyberBit	Carbon Black Response	Check Point SandBlast Agent	Kaspersky EDR	Symantec EDR	Trend Micro Apex One
Регистрация удаленных обращений к локальным административным папкам (ADMIN$, C$ и т.п.)	🔴	🟢	🟢	🟡	🟢	🔴	🟢
Комментарии вендоров	Требуется интеграция с дополнительным сетевым компонентом – NX SmartVision.			Контролируются и регистрируются сетевые подключения модулем Endpoint Firewall.		Можно блокировать использование сетевых шар на ПК (модуль Application Control) и детектировать при помощи IPS Symantec Endpoint Protection (SEP).	
Регистрация открытия нового сетевого порта в режиме прослушивания	🔴	🟢	🔴	🟡	🟢	🔴	🟢
Комментарии вендоров				Подключения между процессами внутри машины (127.0.0.1) логируются модулем Forensics. Новый порт должен быть разрешен на модуле Endpoint Firewall, иначе трафик будет заблокирован.			
Выявление исходящего сетевого сканирования – массового обращения к диапазону IP-адресов/ хостов	🔴	🔴	🔴	🟢	🟢	🔴	🟢
Комментарии вендоров		Данный функционал заявлен в RoadMap.					
Выявление входящего сетевого сканирования – массового обращения к диапазону портов хоста с одного источника	🔴	🔴	🔴	🟢	🟢	🟢	🔴
Комментарии вендоров		Данный функционал заявлен в RoadMap.					
1.2. Контроль и автоматическое блокирование							
Межсетевой экран	🔴	🔴	🔴	🟢	🟢	🟢	🟢
Комментарии вендоров	Требуется интеграция с текущим EPP-агентом с соответствующим функционалом.	Требуется интеграция с текущим EPP-агентом с соответствующим функционалом.	Требуется интеграция с текущим EPP-агентом с соответствующим функционалом.	Межсетевой экран доступен в рамках пакетов SandBlast Agent, SandBlast NGAV, EndPoint Complete Protection Suite.			
Предотвращение запуска исполняемых файлов	🔴	🔴	🟢	🟢	🟢	🟢	🟢
Комментарии вендоров	Требуется интеграция с текущим EPP-агентом с соответствующим функционалом.	Требуется интеграция с текущим EPP-агентом с соответствующим функционалом.	Есть черный список хешей. Интеграция с дополнительным агентом Carbon Black Protection позволяет значительно расширить функционал.	Данный критерий выполняется модулем Application Control (доступен во всех пакетах SandBlast Agent).			Требуется встроенный модуль Application Control.
Управление приложениями	🔴	🔴	🔴	🟢	🟢	🟢	🟢
Комментарии вендоров	Требуется интеграция с текущим EPP-агентом с соответствующим функционалом.	Требуется интеграция с текущим EPP-агентом с соответствующим функционалом.	Требуется интеграция с дополнительным агентом Carbon Black Protection или с текущим EPP-агентом с соответствующим функционалом.	Данный критерий выполняется встроенным модулем Application Control (доступен во всех пакетах с SandBlast Agent).			Требуется встроенный модуль Application Control.

🟢 да 🟡 частично 🔴 нет

Продукт	FireEye HX	CyberBit	Carbon Black Response	Check Point SandBlast Agent	Kaspersky EDR	Symantec EDR	Trend Micro Apex One
Проверка цифровой подписи файлов	🔴	🔴	🟢	🟢	🟢	🟢	🟢
Комментарии вендоров	Требуется интеграция с текущим EPP-агентом с соответствующим функционалом.	Требуется интеграция с текущим EPP-агентом с соответствующим функционалом.	Есть черный список хешей. Интеграция с дополнительным агентом Carbon Black Protection позволяет значительно расширить функционал.				
Управление USB/ съемными носителями	🔴	🔴	🔴	🟢	🟢	🟢	🟢
Комментарии вендоров	Требуется интеграция с текущим EPP-агентом с соответствующим функционалом.	Требуется интеграция с текущим EPP-агентом с соответствующим функционалом.	Требуется интеграция с дополнительным агентом Carbon Black Protection или с текущим EPP-агентом с соответствующим функционалом.	Требуется пакет Endpoint Complete Protection Suite или дополнительный модуль Data Protection.		Блокировка любых устройств, не только USB. Отсутствует возможность предоставления доступа к съемному носителю по запросу.	Требуется встроенный модуль Integrated Data Loss Prevention (IDLP).
Защита от уязвимостей (virtual patching)	🔴	🔴	🔴	🟡	🟢	🟢	🟢
Комментарии вендоров	Требуется интеграция с текущим EPP-агентом с соответствующим функционалом.	Требуется интеграция с текущим EPP-агентом с соответствующим функционалом.	Требуется интеграция с дополнительным агентом Carbon Black Protection или с текущим EPP-агентом с соответствующим функционалом.	Модуль Anti-Exploit защищает офисные приложения и браузеры. Модуль Threat Emulation предотвращает и обнаруживает эксплойты в файлах.	Защита от уязвимостей с помощью встроенной технологии Exploit Prevention (EP).		
Защита от кражи учетных записей	🔴	🔴	🔴	🟢	🟢	🔴	🟢
Комментарии вендоров	Требуется интеграция с текущим EPP-агентом с соответствующим функционалом.	Требуется интеграция с текущим EPP-агентом с соответствующим функционалом.	Требуется интеграция с текущим EPP-агентом с соответствующим функционалом.			Защита учетных записей обеспечивается сторонними средствами: двухфакторная аутентификация (Symantec VIP), детектирование MITM (Symantec Endpoint Protection Mobile), веб-защита (Symantec Web Isolation, ProxySG).	
Дополнительные технологии контроля и функциональности	В зависимости от функционала текущего EPP-агента	В зависимости от функционала текущего EPP-агента	В зависимости от функционала текущего EPP-агента	• Шифрование жесткого диска • Шифрование документов — модуль Capsule Docs • Контроль соответствия состояния конечной точки (приложения, обновления ОС, антивируса, ключей реестра и др.) — модуль Compliance • URL-фильтрация соединения с серверами контроля и управления — модуль Anti-Bot. • Выявление новых экземпляров известных семейств вредоносов по поведению непосредственно на конечной станции — модуль Behavioral Guard.	• Контроль веб-приложений • Предотвращение вторжений (HIPS) • Шифрование данных • Защита мобильных устройств • Контроль устройств • System Hardening • Оценка уязвимостей • Patch management • Блокирование сетевых атак (Network Attack Blocker)	Сетевой IPS для входящих и исходящих пакетов	• ПО mutex (mutual exclusion) можно явно прописать для блокирования запуска вредоноса. • UDSO – User-defined suspicious object. Это объект, загруженный пользователем, под который будет сделана специальная сигнатура для последующей блокировки
Комментарии вендоров			Перехват автозапуска исполняемых файлов, вложенных в MS Office с помощью дополнительного агента Carbon Black Protection.				

🟢 да 🟡 частично 🔴 нет

2. ПЕРЕДОВОЕ ОБНАРУЖЕНИЕ (DETECT)

Продукт	FireEye HX	CyberBit	Carbon Black Response	Check Point SandBlast Agent	Kaspersky EDR	Symantec EDR	Trend Micro Apex One
2.1. Автоматическое обнаружение Для продвинутого обнаружения угроз используются дополнительно комбинации различных механизмов и методов детектирования.							
Статический анализ файлов Комментарии вендоров	🟢	🟢	🟢	🟢	🟢	🟡 Статический анализ файлов выполняется в компоненте машинного обучения на агенте. Но результаты можно посмотреть в отчете «песочницы».	🟢
Машинное обучение Большинство решений предлагают передовые возможности обнаружения на основе машинного обучения. Элементы искусственного интеллекта вместе с другими механизмами позволяют детектировать новейшее вредоносное ПО, минимизируя число ложных срабатываний. Комментарии вендоров	🟢	🟢	🔴 Данный функционал реализован в отдельном продукте Carbon Black Defense.	🟢	🟢	🟢	🟢
Глобальная аналитика угроз (репутация файлов)	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Сторонние источники аналитических данных об угрозах	🟢	🟢	🟢	🟢	🟢	🔴	🟢
Выполнение IoC-сканирования и его типы К индикаторам компрометации Indicator of compromise (IoC) относятся данные об угрозе: URL, хеш файла, IP и т.д. Решения позволяют проводить периодическое (или по запросу) IoC-сканирование для выявления артефактов на конечных станциях. Одна из дополнительных возможностей – это использование не только своей аналитики угроз, но и загрузка IoC из сторонних источников, таких как FinCert/ГосСОПКА и т.д. Такой функционал позволяет, с одной стороны, оперативно обнаруживать и реагировать на угрозы, а с другой – создавать правила для их предотвращения. Комментарии вендоров	🟢 • IP • URL • File path • Name • Hash • Registry • DNS entry support for OpenIOC format	🟢 • MD5	🟢 • IP • URL • File path • Name • Hash	🟢 • IP • URL • File path • Name • Hash	🟢 • Open IoC • YARA-правила	🟢 • File (MD5, Sha256, Path, Name) • Process (Module, MD5, Sha256, Path) • Reg_key (Path, Name, Value) • Service (Name, Path) • IoC в формате STIX	🟢 • IP • Port • Domain • DNS • Sha1 hash • File • Name • File path • File type

🟢 да 🟡 частично 🔴 нет

Продукт	FireEye HX	CyberBit	Carbon Black Response	Check Point SandBlast Agent	Kaspersky EDR	Symantec EDR	Trend Micro Apex One
Поддерживаемые варианты IoC-сканирования Комментарии вендоров	Сканирование в реальном времени	Периодическое, по запросу	Периодическое, по запросу	Периодическое, по запросу	Сканирование в режиме реального времени, по расписанию, по запросу Процесс IoC-сканирования инфраструктуры рабочих мест может осуществляться в режиме реального времени или по расписанию, а также поверх базы ретроспективных данных по запросу или расписанию.	Периодическое, по запросу	Периодическое, по запросу
Использование YARA-правил **Часть решений позволяет создавать пользовательские сигнатуры в формате YARA-правил для поиска индикаторов вредоносного ПО на хосте. Другая часть не имеет такого встроенного механизма, но дает возможность реализовать его на дополнительных компонентах.** Комментарии вендоров	🔴 Агент HX не имеет встроенного механизма YARA. Функционал вынесен на сетевые устройства (NX/EX/FX/AX), т.к. он потребляет слишком много ресурсов.	🟢	🟢	🔴 Функционал реализован на уровне дополнительного компонента локальной «песочницы» SandBlast для статического анализа файлов от защищенных станций.	🟢	🔴 Данный функционал реализован на уровне дополнительного компонента локальной «песочницы». Content Analysis Service/ Malware Analysis (CAS/MA).	🟢
Поведенческий анализ	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Поддержка «песочницы» «из коробки» **Часть решений позволяет отправлять файлы в «песочницу» для динамического анализа. По факту вынесения вердикта о вредоносности происходит блокировка на всех конечных станциях, где установлены агенты. Кроме того, решения позволяют получать информацию об угрозах и от других компонентов (например, почтовой или веб-«песочницы») комплексного Anti-APT проекта и осуществлять реагирование или проводить расследование на уровне хостов.** Комментарии вендоров	🔴 Можно провести интеграцию с дополнительным компонентом FireEye AX по API.	🔴 По API поддерживается статический анализ и помещение файла в стороннюю «песочницу».	🔴 Carbon Black Response проводит интеграцию со сторонней «песочницей» по API. Дополнительный агент Carbon Black Protection Protection по умолчанию поддерживает «песочницу» от FireEye, Check Point, Trend Micro, Fortinet.	🟢	🟢	🟢	🟢
Типы передаваемых в «песочницу» файлов Комментарии вендоров	70+ типов файлов.	Любой тип файла. Прием файлов зависит от сторонней «песочницы».	• .exe • Документы Типы передаваемых файлов зависят от их поддержки конкретной «песочницей».	60+ типов файлов, включая: • Документы • Исполняемые файлы • Скрипты • Архивы Список типов передаваемых файлов постоянно увеличивается с обновлением движка «песочницы».	.Exe, .ExeUi, .Dll, .Resource, .Net, .llOnly, .llLibrary, .Bat, .Pdf, .Doc, .Dot, .Docx, .Dotx, .Docm, .Dotm, .Rtf, .Zip, .7z, .Rar, .Vbs, .Xls, .Xlsx, .Xltx, .Xlsm, .Xltm, .Xlam, .Xlsb, .Ppt, .Pptx, .Potx, .Pptm, .Potm, .Ppsx, .Ppsm, .Js, .Html, .Jar, .Dos, .Com, .Java, .Elf, .Msi, .Deb, .Rpm, .Scripts, .MachO, .Bzip2, .Gzip, .Arj, .Dmg, .Xar, .Iso, .Cab, .Msg, .Eml, .Vsd, .Vdx, .Xps, .One, .Onepkg, .Xsn, .Odt, .Ods, .Odp, .Sxw, .Pub, .Swf, .Jpeg, .Gif, .Png, .Tiff, .Chm, .Mht.	.jar, doc, .pdf, .cab, .xls, .ppt, .pptx, .xlsx, .docx, .exe, .dll, а также .zip, .rar, .gz, .7z, .cab, если включают эти типы фалов	• .exe • Документы Нет явных ограничений – можно указать любые типы. Важно, чтобы в «песочнице» было ассоциированное приложение.

🟢 да 🟡 частично 🔴 нет

Продукт	FireEye HX	CyberBit	Carbon Black Response	Check Point SandBlast Agent	Kaspersky EDR	Symantec EDR	Trend Micro Apex One
Размер файлов							
Комментарии вендоров	До 1024 Мб.	Ограничений нет. Зависит от сторонней «песочницы».	В зависимости от «песочницы».	• До 15 Мб при перехвате в браузере • До 40 Мб при отправке в «песочницу» из файловой системы • 150+ Мб при антивирусной проверке.	До 100 Мб.	10 Мб.	50 Мб.
Антивирусный модуль	🟢	🔴	🔴	🟢	🟢	🟢	🟢
Антивирусный модуль в совокупности с другими механизмами служит для выявления сложных угроз (у решений класса EPP антивирус выступает в режиме блокировки).							
Комментарии вендоров	Движок BitDefender.	Антивирусный модуль заявлен в RoadMap.	Данный функционал реализован в отдельном продукте – Carbon Black Defense.	Антивирус есть в пакетах SanbBlast NGAV, Endpoint Complete Protection Suite.	Антивирусный модуль доступен в Central Node и на рабочих местах.		
Ретроспективный анализ	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Срок хранения ретроспективных данных							
Срок хранения данных может быть фиксирован или настраиваться индивидуально в зависимости от объема дискового пространства, выделенного для хранения.							
Комментарии вендоров	Зависит от активности хоста, кеша агента, настраивается от 10 до 500 Мб.	Конфигурируемый, рекомендуемый – 2-4 недели.	Зависит от объема хранилища.	Зависит от активности рабочей станции. Локальное хранилище от 1 до 4 Гб на каждой станции. 1 Гб логов обеспечивает в среднем 1 месяц истории на офисной станции.	30 дней.	Определяется размером базы на конечных точках, на сервере с центром обработки размер базы ограничен размером диска.	Настраивается индивидуально в зависимости от объема дискового пространства, выделенного для хранения данных.
Варианты хранения данных							
Часть решений хранят данные на отдельном сервере, часть непосредственно на конечных станциях. Необходимо проработать вопрос восстановления или сохранения детальных логов в случае выхода из строя хранилища или рабочей станции.							
Централизованно	🟢	🟢	🟢	🟡	🟢	🟢	🟢
Комментарии вендоров				Централизованный вариант хранения данных для файлов в карантине.			
На рабочих местах	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Комментарии вендоров	Кеш агента до 500 Мб.	В случае проблем с сетевым соединением с серверной частью данные хранятся на агенте на конечных станциях.	На рабочем месте данные хранятся в автономном режим.				

🟢 да 🟡 частично 🔴 нет

3. РЕАГИРОВАНИЕ (RESPONSE)

Продукт	FireEye HX	CyberBit	Carbon Black Response	Check Point SandBlast Agent	Kaspersky EDR	Symantec EDR	Trend Micro Apex One
Получение списка процессов на хосте Комментарии вендоров	🟢	🟢	🟢	🟡 Получение только списка процессов, связанных с инцидентом.	🟢	🔴	🟢
Белые/черные списки файлов Комментарии вендоров	🔴 Требуется интеграция с текущим EPP-агентом с соответствующим функционалом. В белый список можно добавить файл, чтобы система не срабатывала на него. Как таковых черных списков (с автоматическим блокированием файла) в системе нет. Можно создать индикатор, который будет мониторить определенные файлы по названию или по md5-сумме. При обнаружении таких файлов в системе создастся Alert, по которому администратор может заблокировать сетевую активность на ПК пользователя.	🟢	🟢	🟢 Данный функционал реализуется через модуль Threat Emulation созданием исключений по папкам и хешам, а также модулями Application Control и Compliance.	🟢	🟢	🟢 Функционал реализован через систему управления Control Manager.
Снятие дампа памяти Комментарии вендоров	🟢	🟢	🟢	🔴 Снимаются только логи об активности процесса.	🟡 Есть собственная встроенная утилита kldumper.exe	🔴	🟢
Остановка целевого процесса на хосте Комментарии вендоров	🟡 Модуль Exploit Guard позволяет остановить процесс, в котором был найден эксплойт. Остановить любой процесс в ручном режиме сейчас нельзя. Данный функционал заявлен в RoadMap.	🟢	🟢	🟢 В ходе восстановления станции после атаки автоматически срабатывает модуль Forensics.	🟢	🔴	🟢
Запрет запуска исполняемого файла Комментарии вендоров	🟡 Модули MalwareGuard и MalwareProtection позволяют переместить зараженный исполняемый файл в карантин и заблокировать его запуск. Запретить запуск любого исполняемого незараженного файла в ручном режиме нельзя.	🟢	🟢 Есть черный список хешей. Интеграция с дополнительным агентом Carbon Black Protection позволяет значительно расширить возможности.	🟢 Данный функционал выполняется встроенным модулем Application Control.	🟢	🟢	🟢 Данный функционал поддерживается встроенным модулем Application Control.
Блокировка сетевой активности (изоляция) хоста **Изолированный хост лишается сетевого доступа. При этом для этой рабочей станции доступны, например, консольные команды, позволяющие работать с файлами и процессами.** Комментарии вендоров	🟢 VPN не требуется для пользователей вне сети компании.	🟢	🟢	🟢	🟢	🟢	🟢

🟢 да 🟡 частично 🔴 нет

Продукт	FireEye HX	CyberBit	Carbon Black Response	Check Point SandBlast Agent	Kaspersky EDR	Symantec EDR	Trend Micro Apex One
Отправка в карантин и восстановление Комментарии вендоров	🟢	🟢	🟢	🟢 Отправка в карантин выполняется автоматически встроенным модулем Forensics в ходе восстановления станции после атаки. Восстановление из карантина по запросу локально или централизованно.	🟢	🟢	🟢
Выполнение произвольных команд на хосте Комментарии вендоров	🔴	🔴 Требуется интеграция с дополнительным компонентом CyberBit SOC3D.	🟡 Ограниченный набор основных возможных команд.	🔴	🟢	🔴 Требуется интеграция с дополнительным модулем Host Integrity.	🟢
Удаленная модификация реестра Windows Комментарии вендоров	🔴	🟢	🟢	🟢 Автоматически выполняется встроенным модулем Forensics в ходе восстановления станции после атаки.	🟢	🔴	🟢
Скачивание с хоста или загрузка на хост произвольного файла Комментарии вендоров	🟡 Есть возможность загрузить файл или весь жесткий диск с компьютера, где установлен агент FireEye. Загрузка произвольного файла на компьютер с агентом не поддерживается.	🟢	🟢	🟡 Данный функционал поддерживается только для файлов в карантине.	🟢	🟡 Осуществляется скачивание только исполняемого файла, загрузка на хост невозможна.	🟢
Удаление файла Данный функционал заявлен в RoadMap.	🔴	🟢 Удаление файла осуществляется посредством карантина.	🟢	🟢 Автоматически выполняется встроенным модулем Forensics в ходе восстановления станции после атаки.	🟢	🟢	🟢
Отправка хеша файла на сервис VirusTotal Комментарии вендоров	🔴 Из «коробки» это не выполняется. Возможность интеграции через API FireEye HX и API VirusTotal.	🟢	🟢	🟢	🟢	🟢	🟡 Выполняется через бесплатный дополнительный модуль Deep Discovery Director.

🟢 да 🟡 частично 🔴 нет

4. УСТРАНЕНИЕ ПОСЛЕДСТВИЙ (REMEDIATION)

Продукт	FireEye HX	CyberBit	Carbon Black Response	Check Point SandBlast Agent	Kaspersky EDR	Symantec EDR	Trend Micro Apex One
Восстановление объекта	🟢	🔴	🔴	🟢	🟢	🟢	🟢
Комментарии вендоров	Реализуется антивирусным движком.	Данный функционал заявлен в RoadMap.				Восстановление файла из карантина (из консоли системы управления агентами).	В том числе восстановление зашифрованных объектов.
Восстановление реестра	🟢	🟢	🟢	🟢	🟢	🔴	🔴
Комментарии вендоров	Реализуется антивирусным движком.		Восстановление реестра осуществляется с помощью встроенного модуля Live Response.				Данный функционал заявлен в RoadMap.
Детальный список задач по устранению последствий	🔴	🟡	🟢	🟢	🟢	🔴	🔴
Комментарии вендоров		Есть ограниченный список инструментов для реакции.	Показывает действия вредоносного файла, очистка выполняется вручную.				Данный функционал заявлен в RoadMap.

🟢 да 🟡 частично 🔴 нет

5. РАССЛЕДОВАНИЕ (INVESTIGATION)

Продукт	FireEye HX	CyberBit	Carbon Black Response	Check Point SandBlast Agent	Kaspersky EDR	Symantec EDR	Trend Micro Apex One
Threat hunting С помощью данного функционала и инструментария EDR аналитики или офицеры ИБ могут не только реагировать, но и осуществлять проактивный поиск и обнаруживать, например, скрытые продвинутые угрозы.	●	●	●	●	●	●	●
Расследования по следам оповещений Данный функционал позволяет оперативно выявить, как произошел инцидент, как его остановить, какие объекты были затронуты и как избежать такой ситуации.	●	●	●	●	●	●	●
Сохранение хеш-сумм исполняемых файлов	●	●	●	●	●	●	●
Сохранение хеш-сумм скрипт-файлов (.ps, .vbs, .bat, .js и т.д.)	●	●	●	●	●	●	●
Сохранение копий исполняемых файлов, включая .exe и .dll Комментарии вендоров	●	●	● Все новые загруженные бинарные файлы, .dll хранятся на центральном сервере Carbon Black Response.	● Сохранение копий исполняемых файлов в локальном или централизованном карантине.	●	● Осуществляется вручную и автоматически для подозрительных файлов.	● Данный функционал доступен только при срабатывании задачи отправки в «песочницу».
Сохранение копий скрипт-файлов (.ps, .vbs, .bat, .js и т.д.) Комментарии вендоров	●	●	● Эти файлы не сохраняются автоматически. Однако, если включен встроенный модуль Live Response, то можно собирать любой файл от конечных точек.	● Локальный или централизованный карантин.	●	●	● Данный функционал доступен только при срабатывании задачи отправки в «песочницу».
Визуализация распространения угрозы	●	●	●	●	●	●	●
Визуализация дерева запущенных процессов	●	●	●	●	●	●	●
Визуализация параметров запуска	●	●	●	●	●	●	●
Визуализация операций, выполненных запущенными процессами Комментарии вендоров	●	●	●	●	●	● Возможно с помощью отдельного решения Symantec EDR Cloud.	●

● да ● частично ● нет

Продукт	FireEye HX	CyberBit	Carbon Black Response	Check Point SandBlast Agent	Kaspersky EDR	Symantec EDR	Trend Micro Apex One
Создание forensic-отчетов **Подробный анализ и отчет по событиям, лежащим в основе исходной причины инцидента. Например, визуализация цепочки событий, которые привели к запуску процесса.**	●	●	●	●	●	●	●
Запись всех событий Комментарии вендоров	●	●	●	◐ Запись всех событий, кроме большинства системных.	●	●	●
Сервисы от вендоров Многие вендоры предлагают тренинги, дополнительные сервисы по поиску, мониторингу событий и реагированию на инциденты. Кроме того, предоставляется доступ к порталу знаний об индикаторах угроз и их взаимосвязи.							
Тренинги Комментарии вендоров	●	●	●	● Три центра обучения в Москве и Санкт-Петербурге.	● Kaspersky Security Training: цифровая криминалистика, анализ вредоносного ПО, реагирование на инциденты, эффективная работа с YARA, администрирование KEDR и пр.	○	●
Активный поиск угроз и мониторинг событий Комментарии вендоров	●	●	●	● Облачный сервис проактивного анализа логов.	● Kaspersky Threat Hunting: Kaspersky Targeted Attack Discovery, Kaspersky Managed Protection.	●	● Managed Detection and Response (MDR).
Реагирование на инциденты Комментарии вендоров	●	●	●	● Сервис Incident Response (IR).	● Kaspersky Incident Response.	●	● Managed Detection and Response (MDR).
Доступ к Threat Intelligence (TI) Комментарии вендоров	●	○ Возможна интеграция только со сторонними TI.	●	● При подключении TI к шлюзам и агентам.	● Kaspersky Threat Intelligence Portal – портал базы знаний о вредоносных файлах, легитимных объектах, индикаторах угроз и их различных взаимосвязях. Поддержка облачной «песочницы».	●	● Managed Detection and Response (MDR).

● да ◐ частично ○ нет

ЗАЩИТА ОТ ШИФРОВАЛЬЩИКОВ

Продукт	FireEye HX	CyberBit	Carbon Black Response	Check Point SandBlast Agent	Kaspersky EDR	Symantec EDR	Trend Micro Apex One
Способы обнаружения	Машинное обучение	Поведенческий анализ	Модель события для предварительного обнаружения активности шифровальщика	Постоянный мониторинг специфических признаков поведения шифровальщиков и ханипоты	**Комбинация технологий:** • Network filtering (остановка распространения шифровальщиков по сети) • Cloud-enabled content filtering (блокировка вредоносного контента, связанного с шифровальщиками в веб-трафике) • Port controls (предотвращение заражения шифровальщиком через внешние устройства) • Behavioral analysis (Exploit prevention, Encryption action detection) • Execution privilege control (отсутствие возможности шифровать контролируемые документы) • Automated rollback (возможность отката действий шифровальщика после обнаружения)	• Машинное обучение • Эмулятор • IPS • Анализ поведения	Идентификация по характерным признакам
Способы предотвращения Комментарии вендоров	Карантин	Требуется интеграция с текущим EPP-агентом с соответствующим функционалом Данный функционал заявлен в RoadMap.	Требуется интеграция с дополнительным агентом Carbon Black Protection или с текущим EPP-агентом с соответствующим функционалом Данный функционал также доступен в отдельном продукте Carbon Black Defense. Используется технология предотвращения потоковой передачи.	Проактивное создание краткосрочных бэкапов и остановка всех вредоносных процессов в момент обнаружения	Бэкап файлов и восстановление	• Блокировка • Изоляция • Поиск IoC	• Резервирование объектов • Инжектирование легитимных процессов для мониторинга и предотвращения
Восстановление зашифрованных файлов Комментарии вендоров	🔴	🔴 Данный функционал заявлен в RoadMap.	🔴	🟢	🟢	🔴	🟢

🟢 да 🟡 частично 🔴 нет

СТОРОННЯЯ ИНТЕГРАЦИЯ

Продукт	FireEye HX	CyberBit	Carbon Black Response	Check Point SandBlast Agent	Kaspersky EDR	Symantec EDR	Trend Micro Apex One
Поддержка API	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Легкий агент (совместимость со сторонним EPP) **Легкий EDR-агент устанавливается к текущему EPP-агенту.** Комментарии вендоров	🟢	🟢	🟢	🟢	🟢	🔴 Возможно использование только дополнительных компонентов Advanced Threat Protection for Network (ATP:Network) и Advanced Threat Protection for Email (ATP:Email).	🟢 Встроенный модуль Endpoint Sensor поддерживает совместимость со сторонним EPP.
Полноценный агент (в составе EPP) **Полноценный агент уже включает в себя EPP- и EDR-функционал.** Комментарии вендоров	🟡 Поддержка с помощью движка BitDefender.	🔴 Данный функционал заявлен в RoadMap.	🔴 Данный функционал доступен в отдельном продукте Carbon Black Defense.	🟢 Доступен в пакетах SandBlast NGAV или Endpoint Complete Protection Suite.	🟢	🟢	🟢
Интеграция с «песочницей»							
Локальная «песочница» Комментарии вендоров	🟢 Интеграция с FireEye AX по API.	🟢 По API поддерживается статический анализ и помещение файла в стороннюю «песочницу».	🟢 Carbon Black Response через API. Дополнительный агент Carbon Black Protection по умолчанию поддерживает «песочницу» от FireEye, Check Point, Trend Micro, Fortinet.	🟢	🟢	🟢	🟢
Облачная «песочница» Комментарии вендоров	🔴	🔴	🔴 Данный функционал доступен в отдельном продукте Carbon Black Defense.	🟢	🟢	🟢	🟢 Для SaaS-версии.
Интеграция с другими платформами того же вендора Комментарии вендоров	🟢	🟢	🟢	🟢 Интеграшия со шлюзом безопасности.	🟢 Интеграция с Threat Intelligence (TI), Kaspersky Security Center (KSC), Kaspersky Private Security Network (KPSN), Kaspersky Anti Targeted Attack Platform (KATA).	🟢 Интеграция с Advanced Threat Protection for Network (ATP:Network) и Advanced Threat Protection for Email (ATP:Email).	🟢 Интеграция через систему управления Control Manager.
Интеграция с SIEM Комментарии вендоров	🟢	🟢	🟢	🟢	🟢	🟢 Интеграция со Splunk, IBM QRadar, Symantec ICDx, отправка событий и инцидентов на любой syslog-сервер.	🟢

🟢 да 🟡 частично 🔴 нет

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

Продукт	FireEye HX	CyberBit	Carbon Black Response	Check Point SandBlast Agent	Kaspersky EDR	Symantec EDR	Trend Micro Apex One
Основные требования PCI DSS (v3.2)	🟢	🔴	🟢	🟢	🟢	🟢	🟢
Комментарии вендоров		Выполнение требований PCI DSS на уровне антивируса, а не EDR.					
Защита инфраструктуры конечных точек с повышенными требованиями к изоляции	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Комментарии вендоров	Локальная база угроз.	Требование выполняется. Доступ к облаку не требуется.	Локальная база угроз. Также требование выполняется дополнительным модулем Carbon Black Protection.	Локальная база угроз: Private Threat Cloud.	Локальная база угроз: запатентованная технология Kaspersky Private Security Network (KPSN), локальная «песочница».	Локальная база доступна только для системы управления агентами Symantec Endpoint Manager (SEPM), требуется дополнительный компонент Symantec Insight for Private Cloud (SIPC).	Локальная база Control Manager.

🟢 да 🟡 частично 🔴 нет

РАЗНОЕ

Продукт	FireEye HX	CyberBit	Carbon Black Response	Check Point SandBlast Agent	Kaspersky EDR	Symantec EDR	Trend Micro Apex One
Самозащита агента от удаления	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Защита паролем	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Защита от модификации исполняемых модулей агента Комментарии вендоров	🔴	🟢	🟢	🟢 Файлы подписаны на основе электронно-цифровой подписи и защищены от записи и удаления сторонними процессами.	🟢	🟢	🟢
Защита от остановки процесса агента	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Поддерживаемые платформы							
Windows	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Linux Комментарии вендоров	🟡 Поддержка части функционала.	🟢	🟢	🔴	🟡 Только функциональность EPP – Kaspersky Endpoint Security (KES) for Linux. В RoadMap поддержка EDR-функциональности.	🟢	🔴 Поддержка реализована для отдельного продукта – Trend Micro Deep Security для защиты серверов.
Mac OS Комментарии вендоров	🟡 Поддержка части функционала.	🔴 Функционал заявлен в RoadMap.	🟢	🟢 Дистрибутив представляется по запросу.	🟡 Только функциональность EPP – Kaspersky Endpoint Security (KES) for MacOS. В RoadMap поддержка EDR-функциональности.	🟢	🟢
Создание пользователей с разными правами доступа к решению	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Мониторинг состояния решения	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Язык интерфейса	Английский	Английский	Английский	• Русский • Английский • Китайский • Французский • Испанский • Японский	• Русский • Английский • Китайский	• Русский (только для Symantec Endpoint Manager (SEPM) и агента Symantec Endpoint Protection (SEP)) • Английский	• Английский

🟢 да 🟡 частично 🔴 нет

АКТУАЛЬНОСТЬ ТЕМЫ ПРОДВИНУТОЙ ЗАЩИТЫ ПК ПОЛЬЗОВАТЕЛЕЙ НАБИРАЕТ ОБОРОТЫ. МНОГИЕ КОМПАНИИ, КОТОРЫЕ РАНЕЕ ТОЛЬКО ИНТЕРЕСОВАЛИСЬ ДАННЫМ НАПРАВЛЕНИЕМ, СЕГОДНЯ УЖЕ НАЧИНАЮТ ВНЕДРЯТЬ ТАКОГО РОДА РЕШЕНИЯ. ПО НАШЕМУ ОПЫТУ, МАКСИМАЛЬНУЮ ПОЛЬЗУ В ПРОТИВОДЕЙСТВИИ СОВРЕМЕННЫМ УГРОЗАМ НА УРОВНЕ КОНЕЧНЫХ СТАНЦИЙ ДАЕТ КОМПЛЕКСНЫЙ ПОДХОД, ПРЕДПОЛАГАЮЩИЙ СОЧЕТАНИЕ ФУНКЦИЙ EPP И EDR. ОТВЕЧАЯ НА ЗАПРОСЫ РЫНКА, ПРОИЗВОДИТЕЛИ СТРЕМЯТСЯ СОВЕРШЕНСТВОВАТЬ СВОИ РЕШЕНИЯ. СЕГОДНЯ ВО МНОГИХ РЕШЕНИЯХ КЛАССА EPP ПОЯВЛЯЮТСЯ ФУНКЦИИ EDR И НАОБОРОТ. О ТОМ, КАК БУДЕТ РАЗВИВАТЬСЯ НАПРАВЛЕНИЕ В ДАЛЬНЕЙШЕМ, МЫ РАССКАЖЕМ В СЛЕДУЮЩИХ ОБЗОРАХ.

ИНФОСИСТЕМЫ ДЖЕТ

127015, г. Москва, ул. Большая Новодмитровская,
д. 14, стр. 1, 2-я проходная, офисный центр
«Новодмитровский»

Телефон: +7 (495) 411-76-01, 411-76-03

Email: antiapt@jet.su