ОБЗОР РЕШЕНИЙ

# ANTI-APT

## НА РОССИЙСКОМ РЫНКЕ

**АЛЕКСАНДР РУСЕЦКИЙ,**
руководитель направления
по защите от направленных атак
Центра информационной безопасности
компании «Инфосистемы Джет»

# ВВЕДЕНИЕ

Компания «Инфосистемы Джет» выпускает обзоры решений для защиты от целенаправленных атак и атак нулевого дня с 2016 года. По нашим исследованиям можно проследить динамику развития продуктов класса Anti-APT в России. Так, первый обзор был посвящен анализу 4 продуктов по 33 критериям. Второй вышел в начале 2018 года и включал уже 7 решений, которые были проанализированы по 51 критерию. В новом обзоре количество рассмотренных продуктов было увеличено до 9, а число критериев — до 89[1]. Мы актуализировали информацию о ранее исследованных решениях, добавили новых игроков и расширили критерии с учетом полученной обратной связи от заказчиков и специфики российского рынка Anti-APT.

В отличие от предыдущих обзоров, где фокус был направлен на «песочницы» как базовый инструмент защиты от целенаправленных атак, в новом исследовании мы рассмотрели комплексные подходы к построению защиты от сложных угроз.

Каждый производитель позиционирует свое решение как комплексный продукт с большим набором инструментов и технологий по выявлению новейших угроз и аномалий. В зависимости от вендора, в состав решения, помимо «песочницы», могут входить и сенсоры, и шлюзы (веб и почтовые), и прокси-серверы. При этом внедряемые продукты должны иметь централизованную консоль управления. Комбинированный вариант из нескольких продуктов разных вендоров позволяет построить мультиэшелонированную защиту.

[1] Информация в обзоре актуальна на конец декабря 2019 г. Все обновления продуктов, выпущенные в 2020 г., будут рассмотрены в следующем исследовании.

# ОСОБЕННОСТИ РОССИЙСКОГО РЫНКА ANTI-APT РЕШЕНИЙ

С каждым годом увеличивается количество целевых атак на российские компании.

Если в предыдущие годы российские Anti-APT решения отставали по функциональным возможностям от иностранных аналогов, то сегодня мы наблюдаем уже зрелые отечественные продукты, которые успешно конкурируют с зарубежными.

Последние несколько лет в России наблюдается устойчивый рост количества Anti-APT проектов, несмотря на нежелание многих компаний инвестировать в защиту инфраструктуры, обусловленное уверенностью в том, что они не представляют интерес для злоумышленников.

Для многих иностранных производителей российский рынок не является приоритетным, и, как следствие, ряд продуктов отсутствует на внутреннем рынке ИБ. При этом некоторые зарубежные вендоры подстраиваются под заказчиков из России: открывают локальное производство или проходят сертификацию по продуктам для возможности реализации комплексных проектов.

В отличие от глобального рынка, где растет популярность сервисной модели использования решений, в России по-прежнему остается наиболее востребованным именно внедрение Anti-APT устройств. Несмотря на преимущества сервисного подхода российские компании не готовы передавать трафик на обработку в облако. Более того, многие предпочитают пользоваться «приватной» базой обновлений без передачи данных вовне.

Дефицит ИБ-кадров является не только российской, но и общемировой проблемой, что в ближайшем будущем приведет к росту популярности именно сервисной модели использования Anti-APT решений.

# КОМПЛЕКСНЫЙ ПОДХОД К ПОСТРОЕНИЮ ЗАЩИТЫ ОТ СЛОЖНЫХ УГРОЗ

Казалось бы, основным инструментом борьбы с APT являются специализированные решения класса Breach Detection Systems («песочницы»). Однако их уже недостаточно, чтобы успешно противостоять современным угрозам: социальной инженерии, эксплуатации уязвимостей, комбинациям вредоносного и легитимного программного обеспечения и другим. Тут требуется комплексный подход, предполагающий сочетание «песочниц» с защитой периметра, мониторингом трафика, продвинутой защитой конечных станций и Threat Intelligence. Это значит, что для реализации полноценного проекта Anti-APT требуется набор ИБ-решений. В частности, для достижения максимально высокого уровня предотвращения атак нужны классические инструменты фильтрации распространенных угроз, известных уязвимостей и методов атакующих, для обнаружения и реагирования на киберинциденты — специализированные средства борьбы с неизвестными, продвинутыми угрозами.

# УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

- Да — наличие решения в продуктовой линейке
- Нет — отсутствие решения в продуктовой линейке

## Классификация ИБ-решений в комплексном Anti-APT проекте

| Класс решений / Вендор | Sandbox «Песочница» | EDR Продвинутая защита конечных станций | NGFW Межсетевой экран следующего поколения | IPS/IDS Система предотвращения/обнаружения вторжений | Proxy Прокси-сервер | Anti-spam Антиспам | Honeypot «Ловушки» | NTA Анализ трафика | Mobile Security Защита мобильных устройств | CASB Брокер безопасного доступа в облако | Threat Intelligence Данные кибер-разведки |
|---|---|---|---|---|---|---|---|---|---|---|---|
| FireEye Inc | да | да | нет | да | нет | да | нет | да | нет | нет | да |
| Trend Micro Inc | да | да | нет | да | да | да | нет | да | да | да | да |
| Check Point Software Technologies Ltd | да | да | да | да | да | да | нет | нет | да | да | да |
| Fortinet | да | да | да | да | да | да | да | нет | да | да | да |
| Symantec Enterprise Division of Broadcom | да | да | нет | да | да | да | да | да | да | да | да |
| «Лаборатория Касперского» | да | да | нет | да | да | да | нет | да | да | нет | да |
| Positive Technologies | да | нет | нет | нет | нет | нет | нет | да | нет | нет | да |
| Group-IB | да | да | нет | да | нет | нет | нет | да | нет | нет | да |
| «АВ Софт» | да | нет | нет | да | нет | нет | нет | нет | да | нет | да |

## В ДАННОМ ОБЗОРЕ РАССМАТРИВАЮТСЯ СЛЕДУЮЩИЕ РЕШЕНИЯ:

- **FireEye**
  (FireEye Inc)
- **Trend Micro Deep Discovery**
  (Trend Micro Inc)
- **Check Point SandBlast**
  (Check Point Software Technologies Ltd)
- **Fortinet ATP**
  (Fortinet)
- **Symantec**
  (Symantec Enterprise Division of Broadcom)
- **Kaspersky Anti Targeted Attack**
  («Лаборатория Касперского»)
- **PT Anti-APT**
  (Positive Technologies)
- **Group-IB Threat Detection System**
  (Group-IB)
- **ATHENA**
  («Афина») («АВ Софт»)

## ОСНОВНЫЕ БЛОКИ ОБЗОРА ANTI-APT


## ОБЩАЯ ИНФОРМАЦИЯ О ВЕНДОРЕ

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Компания-вендор** | «Лаборатория Касперского»<br>Россия, Москва<br>www.kaspersky.ru | Positive Technologies<br>Россия, Москва<br>www.ptsecurity.com | Group-IB<br>Россия, Москва<br>www.group-ib.ru | «АВ Софт»<br>Россия, Москва<br>www.avsw.ru | FireEye Inc<br>США, Калифорния<br>www.fireeye.com | Trend Micro Inc<br>Япония, Токио<br>www.trendmicro.com | Check Point Software Technologies Ltd<br>Израиль, Тель-Авив<br>www.checkpoint.com | Fortinet<br>США, Калифорния<br>www.fortinet.com | Symantec Enterprise Division of Broadcom<br>США, Калифорния<br>www.symantec.com |
| **Собственное представи-тельство в России** | да | да | да | да | нет | да | да | да | да |
| **Дистрибьютор в России** | • Axoft<br>• Mont | • Axoft<br>• Mont<br>• OCS | • RRC<br>• Mont | Прямые партнеры | • Axoft<br>• Netwell | • Axoft<br>• Mont | • Mont<br>• RRC<br>• OCS<br>• Fortis | • Marvel<br>• Netwell | • Web Control<br>• Mont<br>• Merlion |

# СОСТАВ РЕШЕНИЙ: ОСНОВНЫЕ И ДОПОЛНИТЕЛЬНЫЕ КОМПОНЕНТЫ

Защита от продвинутых угроз — комплексная задача, для решения которой каждый вендор предлагает целую линейку продуктов. При этом сразу тяжело сориентироваться, какое из решений является основным (базовым), а какое — дополнительным. Мы подошли к их классификации на основе собственного опыта реализации проектов Anti-APT.

**Основные компоненты:**

- «песочница» (локальная/облачная);
- защита почты;
- анализ веб-трафика

(**Внимание!** Устройства с расшифровкой SSL вынесены в раздел «Дополнительные компоненты»);

- защита конечных станций;
- централизованная консоль управления.

**Дополнительные компоненты:**

- все остальные модули.

## Kaspersky Anti Targeted Attack

| НАЗВАНИЕ | КРАТКОЕ ОПИСАНИЕ |
|---|---|
| **ОСНОВНЫЕ КОМПОНЕНТЫ** | |
| Сетевые сенсоры | Анализ почтового и веб-трафика |
| Kaspersky Secure Mail Gateway (KSMG) | Почтовый шлюз |
| Sandbox | «Песочница» |
| Kaspersky EDR (KEDR) | Агенты для рабочих станций, серверов, виртуальных машин, защита конечных станций (антивирус Kaspesky Security для бизнеса (KES) использует один агент с KEDR) |
| Central Node | Центр анализа (механизм оценки и классификации угроз по их уровню критичности, база данных по инцидентам, инструменты визуализации данных и отчетности) |
| **ДОПОЛНИТЕЛЬНЫЕ КОМПОНЕНТЫ** | |
| Kaspersky Private Security Network (KPSN) | Локальная база угроз и центр обмена вердиктами между продуктами |
| Kaspersky Web Traffic Security (KWTS) | Веб-шлюз |
| Kaspersky Security для мобильных устройств | Защита мобильных устройств |
| Kaspersky для виртуальных сред | Защита виртуальных и облачных сред |
| Kaspersky Security для систем хранения данных | Защита систем хранения данных |
| Kaspersky Security для бизнеса | Защита рабочих мест (единый агент с KEDR) |

## PT Anti-APT

| НАЗВАНИЕ | КРАТКОЕ ОПИСАНИЕ |
|---|---|
| **ОСНОВНЫЕ КОМПОНЕНТЫ** | |
| PT Sandbox | «Песочница» (статический и динамический анализ файлов) |
| PT NAD | Решение класса NTA (Network Traffic Analysis) для глубокого анализа трафика, выявления атак и расследования инцидентов |
| **ДОПОЛНИТЕЛЬНЫЕ КОМПОНЕНТЫ** | |
| PT CybSI | Платформа Threat Intelligence (TI) |

## Group-IB Threat Detection System

| НАЗВАНИЕ | КРАТКОЕ ОПИСАНИЕ |
|---|---|
| **ОСНОВНЫЕ КОМПОНЕНТЫ** | |
| TDS Sensor | Анализ сетевого трафика |
| TDS Polygon | Поведенческий анализ файлов |
| TDS Huntpoint | Защита конечных станций |
| TDS Huntbox | Центральный компонент системы, осуществляющий управление компонентами, доступ к информации, ретроспективный анализ и корреляцию событий |
| **ДОПОЛНИТЕЛЬНЫЕ КОМПОНЕНТЫ** | |
| TDS SOC | Внутренний центр обновлений, центр управления сетью устройств, веб-интерфейс, масштабируемое хранилище данных |
| TDS Decryptor | Модуль дешифровки SSL/TLS-трафика в режиме реального времени для дальнейшей подачи на модуль TDS Sensor и другие решения |

## ATHENA

| ОСНОВНЫЕ КОМПОНЕНТЫ |
|---|
| Модуль проверки электронной почты |
| Модуль проверки веб-трафика |
| Подсистема обеспечения сетевой безопасности |
| Подсистема исследования «Песочница» |
| Подсистема анализа и управления |
| **ДОПОЛНИТЕЛЬНЫЕ КОМПОНЕНТЫ** |
| Модуль проверки мобильных устройств |
| Telegram-бот |
| Агенты для ОС Android ATHENA Agent |
| Агенты для рабочих станций (Roadmap Q1 2020) |

## FireEye

| НАЗВАНИЕ | КРАТКОЕ ОПИСАНИЕ |
|---|---|
| **ОСНОВНЫЕ КОМПОНЕНТЫ** | |
| Email Security (EX)<br>Email Threat Prevention (ETP) | Анализ почты |
| Network Security (NX) | Анализ веб-трафика, трафика между серверами |
| Endpoint Security (HX) | Защита конечных станций |
| Central Manager (CM) | Централизованная консоль управления |
| **ДОПОЛНИТЕЛЬНЫЕ КОМПОНЕНТЫ** | |
| File Protection (FX) | Защита файловых серверов |
| Malware Forensic (AX) | Анализ угроз и проведение расследований |
| Network Forensic (PX) | Полный захват трафика |
| FireEye Hellix | Платформа облачного обеспечения безопасности SIEM следующего поколения, оркестрации и анализа угроз |
| Email Security Cloud Edition | Облачный почтовый шлюз безопасности |

## Trend Micro Deep Discovery

| НАЗВАНИЕ | КРАТКОЕ ОПИСАНИЕ |
|---|---|
| **ОСНОВНЫЕ КОМПОНЕНТЫ** | |
| Deep Discovery Email Inspector (DDEI) | Анализ почты |
| Deep Discovery Inspector (DDI) | Анализ пограничного и внутреннего трафика, мультипротокольный анализ |
| Deep Discovery Analyzer (DDAN) | Внешняя «песочница» |
| Apex One | Защита конечных станций |
| Deep Discovery Director (DDD) | Централизованное управление обновлениями и «песочницами», поддержка централизации DDEI для политик и карантина, расширенное расследование инцидентов |
| **ДОПОЛНИТЕЛЬНЫЕ КОМПОНЕНТЫ** | |
| Deep Discovery Web Inspector (DDWI) | Расшифровка SSL и анализ файлов с удержанием объектов до вынесения вердикта |
| Trend Micro Deep Security (DS) | Защита гибридных облачных сред |
| Trend Micro Mobile Security (TM MS) | Защита мобильных устройств |
| Trend Micro Cloud App Security | Защита облачных приложений |

## Check Point SandBlast

| НАЗВАНИЕ | КРАТКОЕ ОПИСАНИЕ |
|---|---|
| **ОСНОВНЫЕ КОМПОНЕНТЫ** | |
| SandBlast | «Песочница» (анализ веб-трафика, почты, файловых сервисов, проверка SSL-трафика) |
| SandBlast Agent | Защита конечных станций |
| Smart Event | Централизованная система сбора и анализа журналов безопасности инфраструктуры Check Point Software Technologies |
| **ДОПОЛНИТЕЛЬНЫЕ КОМПОНЕНТЫ** | |
| SandBlast Mobile | Защита мобильных устройств |
| CloudGuard SaaS | Защита информации в облачных приложениях |
| Check Point Security (NGTX) | Шлюз безопасности с набором блейдов NGTX для интеграции с «песочницей» |

## Fortinet ATP

| НАЗВАНИЕ | КРАТКОЕ ОПИСАНИЕ |
|---|---|
| **ОСНОВНЫЕ КОМПОНЕНТЫ** | |
| FortiMail | Почтовый шлюз |
| FortiSandbox | Универсальная «песочница», поддерживающая широкий набор интеграций с решениями Fortinet или сторонними продуктами. Может полноценно работать без дополнительных решений и компонентов |
| FortiClient | Защита конечных станций |
| **ДОПОЛНИТЕЛЬНЫЕ КОМПОНЕНТЫ** | |
| FortiGate | Шлюз безопасности |
| FortiWeb | Защита и публикация веб-приложений (WAF) |
| FortiEDR | Клиент EDR (состоялся технический релиз, полноценный релиз планируется в Q1 2020) |
| FortiADC | Балансировщик |
| FortiDeceptor | Сетевые «ловушки» (Honeypot) |
| FortiProxy | Выделенный прокси-сервер |
| FortiCASB | Защита облачных приложений |
| FortiIsolator | Комплексная защита браузера |

## Symantec

| НАЗВАНИЕ | КРАТКОЕ ОПИСАНИЕ |
|---|---|
| **ОСНОВНЫЕ КОМПОНЕНТЫ** | |
| Email Security Safeguard | Облачный сервис защиты почты |
| Cynic | Облачная «песочница» |
| SEP / SEP EDR | Защита конечных станций |
| SEPM | Сервер управления конечными станциями |
| **ДОПОЛНИТЕЛЬНЫЕ КОМПОНЕНТЫ** | |
| Content Analysis System (CAS) | Локальная «песочница» |
| Symantec EDR Cloud | Облачная защита конечных станций |
| SEP Mobile | Защита мобильных устройств |
| ProxySG | Прокси-сервер с функцией ETAP или SSL Visibility Appliance — отправка копии расшифрованного веб-трафика на сетевой сенсор EDR |
| Endpoint Hardening | Харденинг конечных точек (AddOn для SEP) |
| Threat Defense for Active Directory (TDAD) | Оценка безопасности и локализация взлома Active Directory |
| Web Isolation | Безопасный просмотр веб-сайтов и загружаемых с них документов в браузерах конечных устройств |
| Email Threat Isolation | Безопасный просмотр ссылок и вложений из почтовых сообщений в браузерах конечных устройств |
| Security Analytics | Аналитическая платформа безопасности |
| Cloud Workload Protection (CWP) | Защита вычислительных ресурсов частных и публичных облаков AWS, Azure и Google Cloud Platform |
| Cloud Workload Protection (CWP for Storage) | Защита облачных хранилищ AWS S3 buckets |
| Cloud Access Security Broker (CASB) | Аудит использования и защита приложений SaaS и IaaS |
| Secure Access Cloud (SAC) | Программно-определяемый периметр (SDP) и реализация принципа zero-trust для доступа к корпоративным ресурсам on-premise и публичных IaaS |
| Symantec Insight for Private Clouds (SIPC) | Локальная база угроз |

## УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

Да — полное соответствие

Пример: критерий реализуется основными компонентами рассматриваемых решений;

Частично — частичное соответствие

Пример: критерий реализуется дополнительными компонентами рассматриваемых решений;

Для реализации критерия требуется выполнить дополнительные операции.

Нет — не соответствует

Пример: для реализации критерия необходимо использовать сторонние средства и продукты, не входящие в состав основных и дополнительных компонентов рассматриваемых решений.

# ВАРИАНТЫ ПОСТАВКИ РЕШЕНИЙ

В зависимости от инфраструктуры, заказчики используют аппаратные решения либо виртуальные платформы. Есть и те, кто работает с облачным сервисом, например, для проверки подписанных хеш-файлов: вердикт по известным файлам выносится сразу, а неизвестные направляются на анализ в облако вендора.

Каждый из перечисленных вариантов имеет преимущества и недостатки. Например, для использования аппаратных устройств в режиме блокировки необходимо предусмотреть их отказоустойчивость, а при превышении пороговых значений (по трафику, количеству анализируемых писем и т.д.) потребуется перейти на более старшую модель, что повлечет дополнительные инвестиции. В случае с виртуальными устройствами нужна поддержка на аппаратном уровне. Недостатки облачных сервисов уже упоминались во введении: мало кто из российских компаний готов использовать облачную консоль, не говоря уже об отправке файлов куда-либо на анализ — и это при более выгодной стоимости таких решений.

Наш опыт подсказывает, что осуществлять эмуляцию файлов целесообразно именно на аппаратной «песочнице». В сравнении с виртуальной она требует минимальных настроек и является более высокопроизводительной. К тому же в этом случае предоставляется поддержка CPU-level detection (подробнее об этом критерии будет рассказано в разделе «Песочницы»). Остальные компоненты, например, шлюз безопасности, сенсор или система управления, могут рассматриваться в виртуальном исполнении. Отметим, что такой функционал поддерживают все решения, включенные в данный обзор.

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Hardware Appliance** | 🟡 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| Комментарии вендоров | Поддерживается опция сборки программно-аппаратного комплекса партнером | | | | | | | | |
| **Virtual Appliance** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟡 | 🟢 | 🟢 |
| Комментарии вендоров | | | | | | | Все компоненты, кроме аппаратной «песочницы» SandBlast | Поддержка гипервизоров VMWare ESXi, KVM, Microsoft Hyper-V и Nutanix | |
| **Software** | 🟢 | 🟢 | 🟢 | 🟢 | 🟡 | 🟡 | 🟡 | 🟡 | 🟡 |
| Комментарии вендоров | | | | | Только HX | Только Apex One, Apex Central, DS, CAS, TMMS | Только SandBlast | Только FortiClient, FortiEDR | Только SEP и SEPM |
| **Cloud** | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |



🟢 да 🟡 частично 🔴 нет

# ПОКРЫТИЕ КАНАЛОВ РАСПРОСТРАНЕНИЯ УГРОЗ

## 1. ПОЧТА

### Протоколы

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **POP3**<br>Комментарии вендоров | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟡<br>Требуется дополнительный компонент Security Analytics |
| **IMAP**<br>Комментарии вендоров | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟡<br>Требуется дополнительный компонент Security Analytics |
| **SMTP**<br>Комментарии вендоров | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟡<br>Требуются дополнительные компоненты Email Security Safeguard и EDR или Security Analytics |

### Основные варианты интеграции с почтой

На сегодняшний день почта остается основным вектором распространения целенаправленных атак. Для анализа почтового трафика можно использовать решения в режиме мониторинга (BCC или SPAN) или блокировки (MTA). В режиме мониторинга анализируются копии электронных писем, отправленных шлюзом MTA или Anti-spam. В режиме блокировки происходит установка решения «в разрыв» между существующим MTA или Anti-spam и внешними корпоративными почтовыми серверами. Письма задерживаются на проверку, после чего они либо пропускаются, либо направляются в карантин.

Все рассматриваемые решения поддерживают возможность блокировки почты напрямую либо через свой почтовый шлюз или антиспам. Мы рекомендуем использовать этот режим работы в продуктиве, так как он препятствует первичному заражению. Практика показала, что задержка в получении почты на время проверки составляет от 3 до 5 минут, что некритично для пользователей.

### Мониторинг

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **BCC**<br>Комментарии вендоров | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟡<br>Требуется дополнительный компонент Security Analytics |
| **SPAN**<br>Комментарии вендоров | 🟢 | 🟢 | 🟢 | 🟡<br>Необходим дополнительный модуль по разбору трафика (например, Microolap EtherSensor или другое ПО с возможностью интеграции по протоколу ICAP или через API системы) | 🟢 | 🟢 | 🟢 | 🟢 | 🟡<br>Требуется дополнительный компонент Security Analytics |

### Блокировка

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **MTA**<br>Комментарии вендоров | 🟢<br>Реализуется при наличии основного компонента KSMG | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢<br>Реализуется при наличии основного компонента FortiMail | 🟡<br>Требуются дополнительные модули Email Security Safeguard и EDR |



🟢 да 🟡 частично 🔴 нет

## 2. ВЕБ

По нашему опыту, использовать решение Anti-APT для анализа только HTTP-трафика нецелесообразно даже на пилоте. При таком подходе не получится увидеть зашифованные обращения к C&C (Command and Control Server), вредоносную нагрузку (payloads) и сами «тела» (объекты), скачиваемые по HTTPS. Необходима расшифровка SSL-трафика и его анализ на скрытые угрозы, тем более что его доля в общем трафике уже превышает 75%, а если говорить о вредоносном трафике, то она значительно выше. Одни решения могут выполнять эту задачу при интеграции со сторонними продуктами, другие сами могут просматривать SSL.

### Протоколы

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| HTTP | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| HTTPS | 🟡 | 🔴 | 🟡 | 🔴 | 🟢 | 🟡 | 🟢 | 🟡 | 🟡 |
| Комментарии вендоров | Осуществляется дополнительным компонентом KWTS | Требуется интеграция со сторонними решениями (A10, F5 и др.) | Осуществляется дополнительным компонентом TDS Decryptor для работы с TLS/SSL-трафиком или при интеграции со сторонними решениями (A10, F5 и др.) | Требуется интеграция со сторонними решениями (A10, F5 и др.) | Осуществляется основным компонентом NX с функцией расшифровки SSL или интеграция со сторонними решениями (A10, F5 и др.) | Требуется дополнительный компонент DDWI или интеграция со сторонними решениями (A10, F5 и др.) | Расшифровка SSL может также осуществляться шлюзом безопасности | При интеграции с дополнительными компонентами FortiGate, FortiClient, FortiWAF FortiWeb, FortiProxy, FortiADC | При интеграции с дополнительными компонентами Symantec ProxySG с функцией ETAP или SSL Visibility Appliance для отправки расшифрованного трафика на сетевой сенсор |

### Основные варианты интеграции с веб

Для анализа веб-трафика также можно использовать режим мониторинга или блокировки. В режиме мониторинга анализу подвергается копия трафика. Это позволяет избежать задержек при передаче данных и исключить воздействие на бизнес-процессы. Кроме того, оставаясь незаметным для злоумышленников, решение помогает обнаруживать угрозы на самых ранних стадиях. В режиме блокировки скачиваемые пользователем файлы перехватываются на уровне рабочей станции и анализируются в «песочнице» до их открытия и запуска.

Также на проверку в «песочницу» могут направляться файлы с прокси-сервера по ICAP. В этом случае блокировка осуществляется на уровне сетевого оборудования после вынесения соответствующего вердикта для передачи фидов и создания правил блокировки. Важный нюанс: **если ICAP способен обрабатывать только исходящий трафик (REQMOD), можно будет увидеть лишь запрашиваемые пользователями URL, а не сами объекты. С точки зрения анализа в «песочнице», такая информация будет бесполезна**.

Варианты использования решений в режиме блокировки Inline различаются, в зависимости от производителя. Например, таким образом можно блокировать подозрительные или вредоносные объекты в режиме реального времени, включая требующие анализа в «песочнице». Речь идет о режиме, который получил названия «задержка объекта» и «исключение первого прохода». Его суть сводится к тому, что пользователь не сможет скачать файл до вынесения вердикта «песочницей». Еще один вариант использования решений — блокировка вредоносного объекта при повторном скачивании (при первом скачивании проводится параллельный анализ в «песочнице»).

### Мониторинг

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| TAP | 🟢 | 🔴 | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| Комментарии вендоров | | | | Требуется интеграция со сторонним прокси-сервером или МСЭ | | | | | |
| SPAN | 🟢 | 🟢 | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| Комментарии вендоров | | Поддержка RSPAN | | Требуется интеграция со сторонним прокси-сервером или МСЭ | | | | | |



🟢 да 🟡 частично 🔴 нет

## Блокировка

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Inline** | 🟡 | 🔴 | 🔴 | 🔴 | 🟢 | 🟡 | 🟢 | 🟡 | 🟢 |
| Комментарии вендоров | Осуществляет дополнительный компонент KWTS | Требуется интеграция с МСЭ прикладного уровня | Требуется интеграция со сторонним прокси-сервером или МСЭ либо интеграция через SIEM | Требуется интеграция со сторонним прокси-сервером или МСЭ | | Осуществляет дополнительный компонент DDWI | | При интеграции с дополнительными компонентами FortiGate, FortiClient, FortiWAF FortiWeb, FortiProxy, FortiADC | |
| **ICAP** | 🟡 | 🟢 | 🟢 | 🟢 | 🟡 | 🟢 | 🟢 | 🟢 | 🟡 |
| Комментарии вендоров | Односторонняя отправка файлов на проверку без обратной передачи фидов | | | | Работа только в режиме мониторинга | | | | Требуется дополнительный компонент CAS |



🟢 да 🟡 частично 🔴 нет

# 3. КОНЕЧНЫЕ СТАНЦИИ

На протяжении последних лет одним из основных способов компрометации ИТ-инфраструктуры для хакеров остается атака на конечные станции. Для их всесторонней защиты недостаточно предотвращения максимального количества известных угроз. Здесь требуется комплексный подход, включающий предотвращение, передовое обнаружение, реагирование, устранение последствий атак и расследование. Обеспечить такую функциональность позволяет совместная эксплуатация решений класса EPP (Endpoint Protection Platform) и EDR (Endpoint Detection and Response). Подробнее о возможностях этих средств можно узнать в нашем обзоре «Продвинутая защита конечных станций»[2].

**NB!** Остановимся подробнее на одном из наиболее распространенных вопросов о защите конечных станций. Как осуществлять вскрытие HTTPS-трафика: на уровне сети (например, на решении F5 SSL Orchestrator или шлюзе безопасности) с дальнейшей отправкой объектов в «песочницу» или на уровне рабочей станции (при наличии EDR)?

Задача «песочницы» — анализировать объекты в трафике, задача EDR — обнаруживать аномальную активность и защищать рабочее место от таргетированных атак. Поэтому хоть EDR и «видит» все уже в расшифрованном виде, этот класс решений не занимается превентивной отправкой всех объектов на анализ в «песочницу». Для этого существует большое количество других механизмов, да и такой сценарий использования решения приведет к его сильной загрузке.

Поэтому, на наш взгляд, необходимо проверять объекты на уровне сети, расшифровывать и перенаправлять трафик на анализ в «песочницу». При этом EDR-агент будет получать алерт и сможет заблокировать объект на уровне станции.

Также рекомендуется установка EDR-агентов на критические станции, в том числе для защиты от других векторов доставки: проприетарных протоколов шифрования и протокола TLS 1.3, который нельзя расшифровать на шлюзе безопасности.

## Интерфейс конечных станций

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **USB**<br>Комментарии вендоров | 🟢 | 🔴<br>Посредством ручной загрузки файлов в веб-интерфейс MultiScanner | 🟢 | 🔴<br>Roadmap Q1 2020 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |

## Анализ поведения на конечных станциях

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Наличие агентского ПО для защиты от угроз нулевого дня**<br>Название агента<br>Комментарии вендоров | 🟢<br>KEDR | 🔴 | 🟢<br>TDS Huntpoint | 🔴<br>Roadmap Q1 2020 | 🟢<br>HX | 🟢<br>Apex One и DS | 🟢<br>SandBlast Agent | 🟢<br>FortiClient | 🟢<br>SEP |
| **Легкий EDR-агент (совместимость со сторонним EPP)**<br>Комментарии вендоров | 🟢 | 🔴 | 🟢 | 🔴<br>Roadmap Q1 2020 | 🟢 | 🟢 | 🟢 | 🟡<br>Реализован только функционал связки с FortiSandbox | 🟡<br>Требуется дополнительный компонент EDR Cloud |
| **Полноценный агент (включает EPP- и EDR-функционал)**<br>Комментарии вендоров | 🟢 | 🔴 | 🟡<br>Реализован только функционал Application&Device Control<br><br>Запрет запуска по hash (prevent) | 🔴<br>Roadmap Q1 2020 | 🟢 | 🟢 | 🟢<br>Доступен в пакетах SandBlast Agent Basic Advanced и Complete | 🟡<br>EDR-функционал предоставляет основной компонент агент FortiEDR (состоялся технический релиз, полноценный релиз планируется в Q1 2020)<br><br>EPP-функционал предоставляет основной компонент FortiClient | 🟢 |

[2] https://jet.su/about/news/19468/

В обзоре «Продвинутая защита конечных станций», опубликованном в начале 2019 года, нет информации об агентах TDS Huntpoint и FortiEDR, так как они были выпущены после его выхода.

🟢 да 🟡 частично 🔴 нет

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Защита от бестелесных атак по поведению на станции**<br><br>Комментарии вендоров | 🟢 | 🟢 | 🟢 | 🔴<br><br>Roadmap Q1 2020 | 🟢 | 🟢 | 🟢 | 🟡<br><br>Реализовано в дополнительном компоненте FortiEDR (состоялся технический релиз, полноценный релиз планируется в Q1 2020) | 🟢 |
| **Защита от вирусов-вымогателей и шифровальщиков по поведению на станции**<br><br>Комментарии вендоров | 🟢 | 🟢 | 🟢 | 🔴<br><br>Roadmap Q1 2020 | 🟢 | 🟢 | 🟢 | 🟡<br><br>Реализовано в дополнительном компоненте FortiEDR (состоялся технический релиз, полноценный релиз планируется в Q1 2020) | 🟢 |
| **Блокировка сетевой активности (изоляция) хоста**<br><br>Изолированный хост лишается сетевого доступа, при этом для рабочей станции доступны, например, консольные команды, позволяющие работать с файлами и процессами<br><br>Комментарии вендоров | 🟢 | 🔴 | 🟢 | 🔴<br><br>Roadmap Q1 2020 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |

## Поддерживаемые платформы

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Windows**<br><br>Комментарии вендоров | 🟢 | 🔴 | 🟢 | 🔴<br><br>Roadmap Q1 2020 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢<br><br>Легкий и полный EDR-агент |
| **Linux**<br><br>Комментарии вендоров | 🟡<br><br>EDR-функционал реализован в дополнительном компоненте KES for Linux<br><br>Roadmap: поддержка полного EDR-функционала | 🔴 | 🔴 | 🔴 | 🟡<br><br>Поддержка части функционала | 🟡<br><br>Поддерживается в дополнительном компоненте DS, в основном компоненте Apex One поддерживается только EDR-функционал | 🔴<br><br>Roadmap 2020 | 🟡<br><br>Только получение обновлений об угрозах (malware package) из FortiSandbox | 🟡<br><br>Поддержка функционала только в дополнительном компоненте Symantec EDR Cloud |
| **MacOS**<br><br>Комментарии вендоров | 🟡<br><br>EPP-функционал реализован только в дополнительном компоненте KES for MacOS<br><br>Roadmap: поддержка EDR-функционала | 🔴 | 🔴 | 🔴 | 🟡<br><br>Поддержка части функционала | 🟢 | 🟢 | 🟢 | 🟡<br><br>Поддержка функционала только в дополнительном компоненте Symantec EDR Cloud |



🟢 да 🟡 частично 🔴 нет

# 4. ФАЙЛОВЫЕ ХРАНИЛИЩА

Файловые хранилища — один из потенциальных векторов распространения угроз. Например, если контрагенты компании подгружают на ее ресурсы какие-либо документы, этим может воспользоваться злоумышленник, поэтому требуется проверка получаемых материалов. Можно запускать сканирование по расписанию или отправлять подозрительные файлы в карантин.

## Протоколы

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **CIFS** | 🟢 | 🟢 | 🟢 | 🟢 | 🟡 | 🟢 | 🟢 | 🟢 | 🟡 |
| Комментарии вендоров | | | | | Требуется дополнительный компонент FX | | | | Нет автоматической проверки. Требуется установка основного компонента SEP |
| **SMB** | 🟡 | 🟢 | 🟢 | 🟢 | 🟡 | 🟢 | 🟢 | 🟢 | 🟡 |
| Комментарии вендоров | Работает через дополнительный компонент Kaspersky Security для систем хранения данных и обмен вердиктами через KPSN | | | | Требуется дополнительный компонент FX | | Включая поддержку SMB multi-channel | Включая поддержку SMB v3.0 | Нет автоматической проверки. Требуется установка основного компонента SEP |
| **NFS** | 🟡 | 🟢 | 🟢 | 🟢 | 🟡 | 🟢 | 🟢 | 🟢 | 🔴 |
| Комментарии вендоров | Работает через дополнительный компонент Kaspersky Security для систем хранения данных и обмен вердиктами через KPSN | | | | Требуется дополнительный компонент FX | | | Включая поддержку NFS v4.0 | |
| **FTP** | 🟢 | 🟢 | 🟢 | 🟢 | 🟡 | 🟢 | 🟢 | 🟢 | 🔴 |
| Комментарии вендоров | | | | | Требуется дополнительный компонент FX | | | | |
| **Облачные хранилища (Amazon S3, Azure и др.)** | 🟡 | 🔴 | 🟢 | 🟡 | 🟢 | 🟡 | 🔴 | 🟢 | 🟡 |
| Комментарии вендоров | Требуется дополнительный компонент Kaspersky для виртуальных сред | | | Поддержка облачных хранилищ Dropbox, Яндекс.Диск, Google Диск | Amazon S3, OneDrive, SharePoint Online: поддержка WebDAV (Web Distributed Authoring and Versioning), Secure WebDAV | Требуются дополнительные компоненты DS или CAS | | Amazon S3, Azure Blob | Требуется дополнительный компонент CWP for Storage |



🟢 да 🟡 частично 🔴 нет

## Работа с файловыми хранилищами

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Возможность сканирования по расписанию** | 🟡 | 🔴 | 🟢 | 🟢 | 🟡 | 🟢 | 🟢 | 🟢 | 🟡 |
| Комментарии вендоров | Требуется дополнительный компонент Kaspersky Security для систем хранения данных | | | | Требуется дополнительный компонент FX | | | | Сканирование осуществляется SEP |
| **Карантин подозрительных файлов** | 🟡 | 🟢 | 🟢 | 🟢 | 🟡 | 🟢 | 🟢 | 🟢 | 🟡 |
| Комментарии вендоров | Требуется дополнительный компонент Kaspersky Security для систем хранения данных | | | | Требуется дополнительный компонент FX | | | | Сканирование осуществляется SEP |
| **Отправка файлов на анализ посредством API** | 🟡 | 🟢 | 🟢 | 🟢 | 🟡 | 🟢 | 🟢 | 🟢 | 🟢 |
| Комментарии вендоров | Требуется дополнительный компонент Kaspersky Security для систем хранения данных | | | | Требуется дополнительный компонент FX | | | | |
| **Автоматическое перекладывание чистых файлов из одного хранилища в другое** | 🟢 | 🟢 | 🟢 | 🟢 | 🟡 | 🟢 | 🔴 | 🟢 | 🔴 |
| Комментарии вендоров | | | | | Требуется дополнительный компонент FX | | Можно реализовать при помощи API-автоматизации | | |



🟢 да 🟡 частично 🔴 нет

# 5. МОБИЛЬНЫЕ УСТРОЙСТВА

Растет интерес злоумышленников и к личным устройствам работников компаний: мобильным телефонам и планшетам. Результатом их компрометации может стать потеря конфиденциальной информации организации, например, данных для доступа к корпоративному серверу. При этом многие компании до сих пор не контролируют подключение устройств к инфраструктуре. Среди атак на мобильные устройства можно выделить атаки на платформу, сетевые атаки (основной механизм целенаправленных атак) и атаки на приложения (мошеннические, рекламные или нетаргетированные угрозы).

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Защита мобильных устройств**<br>Комментарии вендоров | 🟡<br>Требуется дополнительный компонент Kaspersky Security для мобильных устройств | 🔴 | 🔴 | 🟡<br>Требуется дополнительный компонент ATHENA Agent | 🔴 | 🟡<br>Требуется дополнительный компонент TM MS | 🟡<br>Требуется дополнительный компонент SandBlast Mobile | 🟢<br>Требуется основной компонент FortiClient для мобильных устройств | 🟡<br>Требуется дополнительный компонент SEP Mobile |
| **Единая консоль управления**<br>Комментарии вендоров | 🟢 | 🔴 | 🔴 | 🔴<br>Roadmap Q3 2020 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Поддержка ОС Android** | 🟢 | 🔴 | 🔴 | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Поддержка ОС iOS**<br>Комментарии вендоров | 🟢 | 🔴 | 🔴 | 🔴<br>Roadmap Q4 2020 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Защита от сетевых атак** | 🟢 | 🔴 | 🔴 | 🔴 | 🔴 | 🟢 | 🟢 | 🔴 | 🟢 |
| **Защита от фишинга (включая SMS)**<br>Комментарии вендоров | 🟢 | 🔴 | 🔴 | 🔴<br>Roadmap Q3 2020 | 🔴 | 🟢 | 🟢 | 🔴 | 🟢 |
| **Защита от фишинга с машинным обучением (Machine Learning, ML)**<br>Комментарии вендоров | 🟢 | 🔴 | 🔴 | 🔴<br>Roadmap Q3 2020 | 🔴 | 🟢 | 🟢 | 🔴 | 🟢 |
| **Защита от нелегитимных Wi-Fi, Bluetooth и сотовых сетей**<br>Комментарии вендоров | 🟢 | 🔴 | 🔴 | 🔴<br>Roadmap Q3 2020 | 🔴 | 🟢 | 🟢 | 🔴 | 🟢 |
| **Защита устройства**<br>Комментарии вендоров | 🟢 | 🔴 | 🔴 | 🟡<br>Блокировка вредоносных и непроверенных приложений выполняется. Функции по проверке трафика в Roadmap<br>Roadmap Q3 2020 | 🔴 | 🟢 | 🟢 | 🔴 | 🟢 |



🟢 да 🟡 частично 🔴 нет

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Физическая защита (пароль, шифрование на уровне устройства и т.д.)**<br>Комментарии вендоров | 🟢 | 🔴 | 🔴 | 🔴<br>Roadmap Q3 2020 | 🔴 | 🟢 | 🟢 | 🔴 | 🟡<br>Дополнительный компонент SEP Mobile интегрируется со многими MDM |
| **Обнаружение атак на устройство (эксплойты ОС, подделка системных процессов, изменение профиля и т.д.)**<br>Комментарии вендоров | 🟢 | 🔴 | 🔴 | 🔴<br>Roadmap Q4 2020 | 🔴 | 🟢 | 🟢 | 🔴 | 🟢 |
| **Уязвимости ОС** | 🟢 | 🔴 | 🔴 | 🔴 | 🔴 | 🟢 | 🟢 | 🔴 | 🟢 |
| **Проверка версии и настроек ОС, включая профили и сертификаты**<br>Комментарии вендоров | 🟢 | 🔴 | 🔴 | 🟡<br>Roadmap Q3 2020<br>Настройки проверяются частично в рамках алгоритма работы агента | 🔴 | 🟢 | 🟢 | 🔴 | 🟢 |
| **Защита приложений** | 🟢 | 🔴 | 🔴 | 🔴 | 🔴 | 🟢 | 🟢 | 🔴 | 🟢 |
| **Обнаружение установленных вредоносных приложений на устройствах на базе ОС Android или iOS**<br>Комментарии вендоров | 🟢 | 🔴 | 🔴 | 🟡<br>Только на устройствах на базе ОС Android | 🔴 | 🟢 | 🟢 | 🔴 | 🟢 |
| **Обнаружение вредоносных приложений, установленных из сторонних источников** | 🟢 | 🔴 | 🔴 | 🟢 | 🔴 | 🟢 | 🟢 | 🔴 | 🟢 |
| **Проверка категорий установленных приложений**<br>Комментарии вендоров | 🟢 | 🔴 | 🔴 | 🔴<br>Roadmap Q3 2020 | 🔴 | 🟢 | 🟢 | 🔴 | 🟢 |



🟢 да 🟡 частично 🔴 нет

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Динамический анализ**<br><br>Комментарии вендоров | 🟢 | 🔴 | 🔴 | 🟢 | 🔴 | 🟡<br><br>Только на основе репутационных проверок | 🟢 | 🔴 | 🟢 |
| **Отчетность** | 🟢 | 🔴 | 🔴 | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Уведомления** | 🟢 | 🔴 | 🔴 | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Другое**<br><br>Комментарии вендоров | | | | | | | Защита от ботов, фишинга, включая новые фишинговые сайты без репутации<br><br>Инспекция сетевого трафика непосредственно на мобильном устройстве | Клиент VPN<br><br>Web-filtering<br><br>Compliance (Telemetry) | Комплект для разработки ПО для мобильных приложений SDK (Software development kit) |



🟢 да 🟡 частично 🔴 нет

# 6. ОБЛАЧНЫЕ СЕРВИСЫ

Деятельность компаний все чаще смещается за пределы периметра сети. Многие организации используют облачные сервисы, например, облачную почту Office 365. Это обуславливает необходимость защиты облачной инфраструктуры и хранящихся в ней критически важных для бизнеса данных. Решить эту задачу можно с помощью специализированных продуктов или отдельным классом решений — брокером безопасного доступа в облако (Cloud Access Security Broker, CASB). CASB представляет собой локальное или распределенное программное обеспечение, которое размещается между пользователями и облачными приложениями, отслеживая все действия и обеспечивая соблюдение политик безопасности. Дополнительная защита от внедрения вредоносного кода выполняется путем интеграции с «песочницей».

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Защита облачных сервисов** | 🟡 | 🔴 | 🟢 | 🟢 | 🟢 | 🟡 | 🟡 | 🟡 | 🟡 |
| Комментарии вендоров | Требуется дополнительный компонент Kaspersky для виртуальных сред | | | | | Функционал реализован в дополнительных компонентах DS, CAS или DDWI в зависимости от задачи | Требуется дополнительный компонент Check Point CloudGuard SaaS | Защита Office 365 реализована основными компонентами FortiMail и FortiSandbox<br><br>Защита остальных сервисов реализована с помощью дополнительного компонента FortiCASB | Требуется дополнительный компонент CASB |
| **Защита публичных сервисов (Office 365, Dropbox, Amazon Web Services и др.)** | 🟢 | 🔴 | 🟢 | 🟡 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| Комментарии вендоров | | | | Не все облачные сервисы защищаются | | | | | |
| **Защита «приватных» (собственных) облачных сервисов** | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 | 🟡 | 🟢 | 🟢 |
| Комментарии вендоров | | | | | | | Через API или с помощью дополнительного компонента CloudGuard SaaS | Встроенные в основной компонент FortiSandbox механизмы интеграции | |
| **Защита от фишинга (включая угрозы нулевого дня)** | 🟢 | 🔴 | 🟢 | 🟡 | 🟢 | 🟢 | 🟢 | 🟢 | 🟡 |
| Комментарии вендоров | | | | По ссылкам проверяется только скачиваемый файл<br><br>Проверка загружаемой страницы с целью фишинга данных аутентификации в Roadmap | | | | | Требуется дополнительный компонент Email Security Safeguard |
| **Предотвращение новых вредоносов** | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Другое** | | | Интеграция с любыми поставщиками Cloud Email в режиме Prevent | | Обнаружение по требованию через дополнительный сервис AWS<br><br>Облачные варианты всего портфеля решений | DS покрывает диапазон защиты физических серверов и рабочих станций до бестелесных приложений (HW, VM, VDI, Clouds, Container, Fileless и т.д.) | Защита от перехвата учетных записей | Возможность защиты Outlook 365 полностью облачным или локальным решением | Есть дополнительные компоненты для защиты облачных сервисов CASB, SAC, CWP, CWP for Storage |
| Комментарии вендоров | | | | | | | | | |



🟢 да 🟡 частично 🔴 нет

# 7. ДРУГИЕ КАНАЛЫ РАСПРОСТРАНЕНИЯ УГРОЗ

Общаясь с заказчиками, мы приходим к выводу, что сегодня компании заинтересованы в анализе не только почты и веб-трафика, но и внутренних активностей в корпоративной сети, что подразумевает поддержку широкого спектра протоколов и дополнительных вариантов интеграций. Это позволяет, например, выявить нестандартное использование протоколов, то может использоваться в том числе при сокрытии работы ботнетов.

## Протоколы

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **DNS** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟡 |
| **Другие протоколы**<br><br>Комментарии вендоров | | Определение более 50 протоколов, глубокий разбор более 30 протоколов до L7 | HTTP, HTTPS, SMB, CIFS, POP3, SMTP, S7COMM, OPC UA, MODBUS, IEC104, DELTAV, UMAS, ERSPAN, MPLS, GRE, FTP, DCE/RPC, SSH, ENIP/CIP, DNP3, NFS, NTP, TFTP, RDP | Требуется интеграция со сторонним прокси-сервером или МСЭ | TFP, IRC | Более 105 протоколов<br><br>Поддержка протоколов SCADA-систем: MODBUS и IEC104 | Протоколы АСУ ТП | Возможность защиты веб-приложений Microsoft Exchange (OWA, ActiveSync, MAPI) от загрузки в почтовую систему вредоносных вложений | DPI для более 2800 приложений<br><br>Поддержка SCADA |
| **Веб-приложения (соцсети и т.д.)**<br><br>Комментарии вендоров | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟡<br><br>Требуется дополнительный компонент Security Analytics |
| **Мессенджеры**<br><br>Комментарии вендоров | 🟢 | 🟢 | 🟢 | 🟡<br><br>Дополнительный модуль системы «Telegram-бот» позволяет проверять файлы в мессенджере Telegram<br><br>Для проверки файлов других мессенджеров и веб-приложений необходима интеграция со сторонним МСЭ, позволяющим извлекать файлы из трафика приложений и передавать их в систему по протоколу ICAP или через API | 🟢 | 🟢 | 🟢 | 🟢 | 🟡<br><br>Требуется дополнительный компонент Security Analytics |
| **Другое**<br><br>Комментарии вендоров | | | | | | | Защита от фишинга и кражи учетных записей, включая новые фишинговые сайты без репутации | Возможность приоритизации сканирования для разных источников и типов файлов | |



🟢 да 🟡 частично 🔴 нет

# СРЕДСТВА АНАЛИЗА

Каждый из рассматриваемых вендоров предлагает компоненты (перечислены в разделе «Состав решений: основные и дополнительные компоненты») для анализа почты, веб-трафика, конечных станций и файловых хранилищ, а также технологии детектирования (механизмы обнаружения). Ниже приведена унифицированная информация по механизмам обнаружения.

## Механизмы обнаружения угроз и аномалий

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Статический анализ** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Антивирусный движок**<br><br>Комментарии вендоров | ● | ●<br><br>До 7 антивирусных движков | ● | ●<br><br>20 антивирусных движков | ● | ● | ● | ● | ● |
| **Технологии искусственного интеллекта (Artificial Intelligence)** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Машинное обучение (Machine Learning)** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Поведенческий анализ** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Глобальная аналитика угроз** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Сторонние источники аналитических данных об угрозах** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **IoC-сканирование**<br><br>Индикаторы компрометации (Indicators of compromise, IoC) — перечень данных об угрозе: URL, хеш файла, IP и т.д.<br><br>Автоматически генерируются в результате динамического анализа или предоставляются сервисом вендора | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **IoA-сканирование**<br><br>Индикаторы атаки (Indicators of attack, IoA) фокусируются на выявлении действий злоумышленника во время атаки<br><br>Примеры IoA: обращения хостов к командному центру, сканирование внутренних узлов сети | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Динамический анализ («песочница»)** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Другие механизмы**<br><br>Комментарии вендоров | | Обнаружение DGA-доменов<br>Обнаружение вредоносного поведения в шифрованном трафике без его расшифрования | Детонация полезной нагрузки и извлечение глубинных индикаторов | Глубокий статический анализ файлов популярных форматов | Система предотвращения вторжений (Intrusion Prevention System, IPS) | | Динамический анализ по поведению на станции<br><br>«Приманки» (Honeypot) для шифровальщиков | Обмен IoC между «песочницами» Forti-Sandbox | Функционал Deception реализован в SEP<br><br>Дополнительный компонент TDAD |



● да ● частично ● нет

# БАЗОВЫЙ ИНСТРУМЕНТ ANTI-APT — «ПЕСОЧНИЦА»

Являясь базовым компонентом проекта Anti-APT, «песочница» содержит набор виртуальных машин («песочниц»), максимально точно воссоздающих реальную среду, в которой работают пользователи. Это дает возможность посмотреть, как ведет себя тот или иной файл в реальных условиях, и оценить степень его деструктивного воздействия.

Решение о том, является ли файл вредоносным, выносится по совокупности нескольких критериев:

- обращения к опасным и зараженным ресурсам;
- изменения конфигурации конечных точек (реестр, файловая система);
- загрузка дополнительных элементов в фоновом режиме.

Помимо вредоносных вложений, «песочницы» анализируют и ссылки в почтовом трафике. Все решения проверяют прямые ссылки (*.doc, *.pdf и т.п.), а вот с укороченными и перенаправляющими ссылками продукты работают по-разному. Производители решений, которые такие ссылки не проверяют, объясняют это стремлением нивелировать риск выполнения действий от лица пользователя: подписки на рассылку, сброса пароля и т.п. Кроме того, для проверки ссылок с перенаправлениями, ведущими на загрузку файлов, часть вендоров наряду с почтовой используют веб-версию «песочницы». В последнее время набирает обороты распространение JavaScript в виде ссылок. Как показала практика, напрямую на шлюзе безопасности они не блокируются, и в этом случае поможет «песочница».

Еще одна возможность рассматриваемых решений — защита от вредоносных URL-адресов в сообщениях электронной почты в момент щелчка. Когда эта функция включена, происходит перезапись подозрительных ссылок в email-сообщениях для дальнейшего анализа. Решения анализируют перезаписанный URL-адрес при каждом щелчке и разрешают либо блокируют переход по нему на основе уровней риска URL-адресов.

### Тип эмулируемого подозрительного контента в «песочнице»

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Анализ всех веб-объектов (веб-страниц, flash, PDF, офисных документов и EXE)**<br>Комментарии вендоров | ● | ●<br>Анализ только PDF, Office, EXE<br>Остальные в Roadmap | ● | ● | ● | ● | ● | ● | ● |
| **Анализ отдельных файлов** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Скрипты** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Макросы** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Архивы** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Проверка запароленных архивов подбором паролей из тела письма**<br>Комментарии вендоров | ● | ●<br>Roadmap | ● | ● | ● | ● | ● | ●<br>Поддержка всех распространенных форматов, включая ZIP, 7-ZIP, RAR | ● |
| **Проверка запароленных архивов подбором паролей из словаря** | ● | ● | ● | ● | ● | ● | ● | ● | ● |



● да ● частично ● нет

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Пополнение словарной базы для подбора паролей к зашифрованным архивам на основе автоматически извлеченных паролей из тела письма**<br><br>Комментарии вендоров | 🟢 | 🔴<br><br>Roadmap | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🔴 |
| **Пополнение словарной базы для подбора паролей к зашифрованным архивам на основе произвольных пользовательских паролей**<br><br>Комментарии вендоров | 🟢 | 🟢 | 🟡<br><br>При загрузке файла в ручном режиме можно указать пользовательский пароль<br><br>Добавление паролей для всех архивов в Roadmap | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🔴 |
| **Проверка многотомных архивов**<br><br>Комментарии вендоров | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🟡<br><br>Архивом будет считаться только первый том, остальные считаются обычными бинарными объектами и не вскрываются | 🟢 | 🟢 | 🔴 |
| **Проверка веб-ссылок в теле письма**<br><br>Комментарии вендоров | 🟢 | 🔴<br><br>Roadmap | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Проверка веб-ссылок внутри документа**<br><br>Комментарии вендоров | 🟢 | 🔴<br><br>Roadmap | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Проверка веб-ссылок внутри документа формата TXT**<br><br>Комментарии вендоров | 🟢 | 🔴 | 🟢 | 🟢 | 🔴 | 🔴 | 🟢<br><br>Закрывается на уровне защиты в браузере с помощью основного компонента SandBlast Agent | 🟢 | 🟢 |
| **Проверка укороченных ссылок в теле письма**<br><br>Комментарии вендоров | 🟢 | 🔴<br><br>Roadmap | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |



🟢 да 🟡 частично 🔴 нет

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Проверка ссылок в момент нажатия (time of click)** | 🟢 | 🔴 | 🟡 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| Комментарии вендоров | | Roadmap | | Roadmap Q2 2020 | | | Включая проверку в облаке CloudGuard SaaS | При интеграции с основным компонентом FortiMail или с дополнительным компонентом FortiIsolator | |
| **Проверка ссылок с перенаправлениями, ведущими на загрузку файлов** | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| Комментарии вендоров | | Roadmap | | | | | При использовании механизма перезаписи ссылок | | |
| **Проверка мобильных приложений** | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Другое** | | | | | | Проверка ссылок с выдачей объекта через meta-refresh | | Контейнер для ОС Android | |
| Комментарии вендоров | | | | | | | | | |
| **Используемые технологии эмуляции** | Custom KVM | Xen | Custom VirtualBox | Custom KVM | Собственная платформа | Custom VirtualBox | Собственный стек технологий | Custom VirtualBox | KVM |
| Комментарии вендоров | | | | | | | | | |

## Варианты отслеживания исполнения кода

Рассматриваемые решения могут отслеживать исполнение кода как на уровне CPU, так и на уровне ядра операционной системы. CPU-Level detection позволяет детектировать эксплойты до того, как они начнут использовать методы обнаружения и обхода «песочницы». Отслеживается каждая инструкция, исполняемая вредоносом, а не только вызовы ОС. При этом CPU-Level detection требует большей производительности оборудования. Отслеживание кода на уровне ядра ОС подразумевает динамический анализ в виртуальных машинах, логирование и анализ всех активностей.

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Отслеживание исполнения кода на уровне CPU** | 🟢 | 🔴 | 🟢 | 🟡 | 🟢 | 🔴 | 🟢 | 🔴 | 🔴 |
| Комментарии вендоров | | | | На уровне CPU проверяется часть инструкций преимущественно с целью маскировки среды виртуализации | MVX (механизм динамического анализа) использует специально созданный гипервизор, где внедрены все инструменты мониторинга | | | | |
| **Отслеживание исполнения кода на уровне ядра ОС** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |



🟢 да 🟡 частично 🔴 нет

## Противодействие механизмам обнаружения работы в виртуальной среде

Производители по-разному подходят к созданию «песочниц»: одни используют собственные платформы, другие — существующие. В первом случае «песочницы» не имеют стандартных признаков виртуализации, свойственных современным гипервизорам, во втором — приобретают некоторые признаки виртуальных машин. Чтобы вредоносное ПО не могло использовать эти особенности решений, все «песочницы» обладают различным функционалом по автоматическому обнаружению и противодействию техникам их обхода (Anti-VM evasion, Sandbox evasion).

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Система сокрытия работы в виртуальной среде (Anti-VM evasion protection)**<br>Комментарии вендоров | ● | ● | ●<br>Собственная технология | ● | ●<br>Собственная технология | ● | ● | ●<br>Собственная технология (специальный движок, оповещение в отчетах) | ● |
| **Противодействие проверкам сервисов, присущим для VMware (vmicheatbeat, VMTools, vmxnet)**<br>Комментарии вендоров | ● | ● | ● | ● | ●<br>Собственная технология | ● | ● | ● | ● |
| **Противодействие проверкам наличия уникальных файлов VMware (vmmouse.sys)** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Противодействие определению наличия порта VMX, используемого VMware для связи с виртуальными машинами**<br>Наличие порта может использоваться вредоносным ПО для предотвращения обнаружения | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Другое**<br>Комментарии вендоров | | | | Прохождение проверок Pafish и Al-Khaser | | | | | Добавление собственных правил детектирования проверок |



● да ● частично ● нет

## Противодействие техникам обхода «песочниц»

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Система противодействия техникам обхода «песочницы» (Sandbox evasion)** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Имитация щелчка «мышкой»**<br>Противодействие технике ВПО по обнаружению «песочницы» путем поиска действий «щелчка» мышкой как признака взаимодействия пользователя до выполнения вредоносного кода | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Имитация движения «мышкой»**<br>Противодействие технике ВПО по обнаружению «песочницы» по изменениям положения курсора | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Режим ожидания (замирание на определенное время)**<br>Противодействие технике ВПО по обнаружению «песочницы» по тайм-аутам в анализе объектов<br>Комментарии вендоров | ● | ● | ● | ● | ● | ● | ● | ● | ●<br>Через скрипт на Python |
| **Временный триггер (запуск в определенное время)**<br>Противодействие технике ВПО по обходу «песочницы» путем запуска в определенное время<br>Комментарии вендоров | ● | ● | ● | ● | ● | ● | ● | ● | ●<br>Через скрипт на Python |
| **«Прокрутка»**<br>Противодействие технике ВПО по обходу «песочницы» путем внедрения глубже в документ в ожидании прокрутки пользователем до страницы с кодом<br>Комментарии вендоров | ● | ● | ● | ● | ● | ● | ● | ● | ●<br>Через скрипт на Python |



● да ● частично ● нет

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Исполнение после перезагрузки**<br><br>Противодействие технике ВПО по обходу «песочницы» путем ожидания выполнения вредоносных действий до перезагрузки решения | 🟢 | 🔴 | 🟢 | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🔴 |
| **Другое**<br><br>Комментарии вендоров | | | Эмуляция отложенных задач, задач после рестарта и User Activity. Собственный механизм детонации вредоносной нагрузки во время исполнения | | | Использование параметров окружения, отличных от стандартных с точки зрения идентификации компонентами ВПО (например, диапазон MAC-адресов и значения реестра)<br><br>Использование файлов-приманок, типичных для каждодневной работы пользователя<br><br>Использование сервисов-заглушек (например, веб-сервер) для отработки запросов при недоступности целевых сервисов при переходе по ссылкам | История недавно открытых документов, непустой буфер обмена и др. | Запатентованный движок anti-evasion | |

## Поддерживаемые ОС в образах виртуальных машин «песочниц»

Для проверки действий ВПО можно выбрать «песочницы» на основе разных ОС. Все вендоры поддерживают Windows XP, 7, 8 и 10, что удовлетворяет потребностям большинства компаний. Также можно выбрать решения с поддержкой серверных платформ и мобильных ОС.

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Windows XP**<br><br>Комментарии вендоров | 🟢 | 🔴 | 🟢 | 🔴<br><br>Roadmap Q1 2020 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Windows 7** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Windows 8/8.1** | 🔴 | 🟢 | 🟢 | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🔴 |
| **Windows 10** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Win Server 2003**<br><br>Комментарии вендоров | 🔴 | 🔴 | 🔴 | 🔴<br><br>Roadmap Q1 2020 | 🔴 | 🟢 | 🔴 | 🟢 | 🔴 |
| **Win Server 2008** | 🔴 | 🔴 | 🔴 | 🟢 | 🔴 | 🟢 | 🔴 | 🟢 | 🔴 |
| **Win Server 2012** | 🔴 | 🔴 | 🔴 | 🟢 | 🔴 | 🟢 | 🔴 | 🟢 | 🔴 |
| **Win Server 2016** | 🔴 | 🔴 | 🔴 | 🟢 | 🔴 | 🟢 | 🔴 | 🟢 | 🔴 |



🟢 да 🟡 частично 🔴 нет

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **MacOS** | 🔴 | 🔴 | 🔴 | 🔴 | 🟢 | 🟢 | 🔴 | 🟢 | 🔴 |
| Комментарии вендоров | | | | Roadmap Q3 2020 | | В облаке | Roadmap Q1 2020 | | |
| **Linux** | 🔴 | 🔴 | 🔴 | 🟢 | 🟢 | 🔴 | 🔴 | 🟡 | 🔴 |
| Комментарии вендоров | Roadmap | Roadmap | | Поддерживает Ubuntu, Debian, CentOS, Red Hat Linux, SUSE Linux, RedOS, Astra Linux | | | Roadmap Q2 2020 | Ubuntu 18 | |
| **Android** | 🟢 | 🔴 | 🔴 | 🟢 | 🔴 | 🟡 | 🟡 | 🟢 | 🟢 |
| Комментарии вендоров | В облаке | | | | | Только репутационные проверки | Только в дополнительном компоненте SandBlast Mobile | | |
| **iOS** | 🔴 | 🔴 | 🔴 | 🔴 | 🟢 | 🟡 | 🟡 | 🔴 | 🟢 |
| Комментарии вендоров | | | | Roadmap Q3 2020 | | Только репутационные проверки | Только в дополнительном компоненте SandBlast Mobile | | |
| **Другие** | | | | | | | | | |
| Комментарии вендоров | | | | | | | | Специализированные ОС ICS (Industrial Control Systems) и OT (Operational Technology) с поддержкой протоколов TFTP, MODBUS, S7COMM, HTTP, SNMP, BACNET, IPMI | |

## Поддерживаемые языки в ОС

Поддержка русского языка в ОС сокращает возможности запуска некоторого вредоносного ПО.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Английский** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Русский** | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟡 | 🟢 | 🟢 |
| Комментарии вендоров | Roadmap | | | | | | По запросу | Любой язык на выбор | |

## Поддерживаемые версии MS Office в образах виртуальных машин «песочниц»

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **MS Office 2003** | 🟢 | 🟢 | 🟢 | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 |
| **MS Office 2007** | 🟢 | 🟢 | 🟢 | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 |
| **MS Office 2010** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **MS Office 2013** | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **MS Office 2016** | 🔴 | 🟢 | 🟢 | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 |
| Комментарии вендоров | | Поддержка MS Office 2019 | | | | | | | |



🟢 да 🟡 частично 🔴 нет

## Лицензии в составе решения

Часть вендоров предлагают лицензии на Windows или Office в составе решения, в других случаях необходимо подгружать собственные.

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Лицензии на ОС Windows и MS Office в составе решения**<br>Комментарии вендоров | 🟢 | 🔴<br>Только для проведения пилотного тестирования | 🔴 | 🔴 | 🟢 | 🔴 | 🟢 | 🟢<br>Опционально<br>Лицензии заказываются у Fortinet для готовых образов<br>Лицензии предостав-ляются заказчиком для собственных образов | 🟡<br>Только для ОС Windows |

## Поддерживаемые типы файлов

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Windows XP** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Офисные**<br>Комментарии вендоров | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟡<br>Требуется дополнительный компонент CAS |
| **Архивы**<br>Комментарии вендоров | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟡<br>Требуется дополнительный компонент CAS |
| **Скрипты**<br>Комментарии вендоров | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟡<br>Требуется дополнительный компонент CAS |
| **Аудио и видео**<br>Комментарии вендоров | 🟡<br>Проверка осуществляет-ся в составе антивирус-ного ядра | 🟢 | 🔴 | 🟢 | 🟢 | 🟡<br>Без эмуляции в «песочнице» | 🟡<br>Частично (статический анализ) | 🟢 | 🟡<br>Требуется дополнительный компонент CAS |
| **Графические**<br>Комментарии вендоров | 🟡<br>Проверка осуществляет-ся в составе антивирус-ного ядра | 🟢 | 🔴 | 🟢 | 🟢 | 🟡<br>Без эмуляции в «песочнице» | 🟡<br>Частично (статический анализ и конвертация в безопасную версию) | 🔴 | 🟡<br>Требуется дополнительный компонент CAS |
| **Мобильные приложения**<br>Комментарии вендоров | 🟢 | 🔴 | 🟢 | 🟢 | 🔴 | 🟢<br>В облаке | 🟢<br>В облаке | 🟢 | 🟡<br>Требуется дополнительный компонент CAS |



🟢 да 🟡 частично 🔴 нет

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Другие типы файлов**<br><br>Комментарии вендоров | 70+ типов файлов<br><br>EXE, EXEUI, DLL, RESOURCE, NET, ILONLY, ILLIBRARY, 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 | Любые типы файлов при установленном ПО для их открытия | 110+ типов файлов, включая 7Z, ACE, AR, ARJ, BAT, BZ2, BZIP2, CAB, CMD, COM, CPL, CSV, DOC, DOCM, DOCX, DOT, DOTM, DOTX, EML, EXE, GZ, GZIP, HTA, HTM, HTML, ISO, JAR, JS, JSE, LNK, LZ, LZH, LZMA, LZO, MHT, MSI, PDF, POTM, POTX, PPS, PPSM, PPSX, PPT, PPTM, PPTX, PS1, RAR, REF, RTF, SCR, SVG, TAR, TAZ, TB2, TBZ, TBZ2, TGZ, TLZ, TXZ, TZO, URL, UUE, VBE, VBS, WSF, XAR, XLS, XLSM, XLSX, XML, XZ, Z, ZIP и др. | | 100+ типов файлов<br><br>Все PE, файлы MS Office, медиафайлы, PDF, flash и архивы ZIP, RAR, TNEF, vCard | Всего более 50+ типов файлов для полноценной эмуляции<br><br>200+ типов файлов для предпроверки | 81 тип файлов, включая PDF, файлы MS Office, исполняемые, скрипты, PowerShell, архивы, MacOS и т.д.<br><br>Flash-анимация с учетом контекста для детектирования сложных составных атак<br><br>В Roadmap дополнительные файлы | Любые типы файлов по усмотрению администратора | Любые типы файлов в локальной «песочнице» CAS |
| **Максимальный размер анализируемого файла**<br><br>Комментарии вендоров | 100 Мб | 8 Гб | 50 Мб | 300 Мб по умолчанию<br><br>Настраиваемый параметр | 1024 Мб | 100 Мб | 100 Мб | 1024 Мб<br><br>Настраиваемый параметр | 10 Мб при анализе в основном компоненте Cynic<br><br>100 Мб при анализе в дополнительном компоненте CAS |
| **Автоматическое восстановление виртуальных машин в исходное состояние** | ● | ● | ● | ● | ● | ● | ● | ● | ● |

## Результаты анализа

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Визуализация обнаруженных угроз** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Отчет** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Кастомизированный отчет** | ● | ● | ● | ● | ● | ● | ● | ● | ● |

## Формат отчета

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **PDF** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **CSV** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **STIX**<br><br>Комментарии вендоров | ● | ●<br><br>Roadmap | ● | ●<br><br>Roadmap Q1 2020 | ●<br><br>Через плагин STIX в отдельном решении вендора FireEye Security Orchestrator | ● | ●<br><br>Только импорт | ● | ● |
| **JSON**<br><br>Комментарии вендоров | ●<br><br>Поддержка в отдельном решении вендора Research Sandbox | ●<br><br>Roadmap | ● | ● | ● | ● | ● | ● | ● |



● да ● частично ● нет

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Отчет в соответствии с MITRE ATT&CK**<br>Комментарии вендоров | ● | ● | ●<br>Roadmap | ●<br>Roadmap Q1 2020 | ● | ● | ● | ● | ● |
| **Безопасная выгрузка семпла** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Выгрузка файла PCAP**<br>Комментарии вендоров | ● | ● | ● | ● | ● | ● | ● | ● | ●<br>Требуется дополнительный компонент CAS |
| **Скриншот активности семпла**<br>Комментарии вендоров | ● | ● | ● | ● | ● | ● | ● | ● | ●<br>Требуется дополнительный компонент CAS |
| **Видеоактивности семпла**<br>Комментарии вендоров | ● | ● | ● | ● | ●<br>Требуется дополнительный компонент FireEye AX | ● | ● | ● | ● |
| **Ретроспективный анализ событий**<br>В части решений реализуется напрямую, в части — через отчеты в агентах на рабочих станциях<br><br>Осуществляется поддержка сервиса индикаторов компрометации для ретроспективного выявления скомпрометированных узлов | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Возможность нотификации через почту (оповещение администратора или офицера ИБ об обнаруженных инцидентах ИБ)** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Возможность масштабирования по производительности** | ● | ● | ● | ● | ● | ● | ● | ● | ● |



● да ● частично ● нет

## Обеспечение отказоустойчивости и распределения нагрузки

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Active/Active**<br>Комментарии вендоров | ● | ● | ● | ● | ● | ● | ● | ● | ●<br>Требуется внешний балансировщик |
| **Active/Standby** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Балансировщик нагрузки** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Поддержка выхода «песочниц» в сеть Интернет для более глубокого анализа определенных видов ВПО**<br>Комментарии вендоров | ● | ● | ● | ● | ● | ● | ●<br>Эмуляция сети Интернет<br>Roadmap Q2 2020 | ● | ● |
| **Поддержка выхода «песочниц» в сеть Интернет через прокси-сервер для более глубокого анализа определенных видов ВПО**<br>Комментарии вендоров | ● | ● | ● | ● | ● | ● | ●<br>Эмуляция сети Интернет<br>Roadmap Q2 2020 | ● | ● |
| **Мониторинг состояния решения** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Ролевое разграничение доступа** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Возможность проведения аудита действий администраторов и отслеживания вносимых изменений** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Необходимые права доступа для запуска файлов в «песочнице»**<br>Комментарии вендоров | Admin | Admin | Admin | Admin или User | Admin | Admin | Admin | Admin | Произвольно через скрипт Python |
| **Язык интерфейса**<br>Комментарии вендоров | Русский, Английский | Русский, Английский | Русский, Английский | Русский, Английский | Английский | Английский | Английский | Английский | Английский |



● да ● частично ● нет

# КАСТОМИЗАЦИЯ ПРОЦЕССА АНАЛИЗА

Кастомизация процесса анализа объектов в «песочнице» позволяет повысить уровень детектирования угроз, особенно адаптированных под конкретную компанию. Тем не менее, важно помнить, что ее некорректная настройка может привести к возникновению большого количества ложных срабатываний и, как следствие, деградации производительности системы. Рассмотрим, какие возможности по кастомизации предоставляют исследованные решения.

Для выявления вредоносного содержимого производители используют в решениях различные скоринговые модели анализа контента. Суть подхода заключается в начислении анализируемым файлам штрафных очков за каждое подозрительное действие и классификации их как вредоносных при превышении порогового значения. Однако не все производители предоставляют возможность самостоятельной донастройки этих моделей.

Часть решений поддерживают возможность создания кастомизированных образов операционной системы «из коробки»: это позволяет воссоздать среду, идентичную рабочей — с конкретной ОС, набором ПО и т.д. Для обеспечения гарантированной производительности и уровня детектирования угроз некоторых решений необходимо обращаться в техническую поддержку вендора.

Продукты ряда производителей позволяют самостоятельно настраивать критерии анализа файлов в «песочнице», например, создавать пользовательские сигнатуры в формате YARA-правил. Ряд вендоров считают этот функционал ненужным из-за риска увеличения ложных вердиктов.

Некоторые решения поддерживают автоматическую конвертацию файлов в безопасный формат в почтовом и веб-трафике, что позволяет очищать объекты от опасного содержимого и мгновенно доставлять их пользователю. Как результат можно избежать очередей на эмуляцию в часы высокой нагрузки и не прибегать к порогам на отказ от проверки после длительного нахождения письма в очереди.

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Кастомизация «песочницы» «из коробки»** | 🔴 | 🟢 | 🔴 | 🟢 | 🟡 | 🟢 | 🔴 | 🟢 | 🟢 |
| Комментарии вендоров | Только в рамках профессионального сервиса | | Только в рамках профессионального сервиса | | Только настройка гостевых образов | | Только в рамках профессионального сервиса | Возможно создание собственных образов как на основе образов, подготовленных Fortinet, так и с нуля | |
| **YARA-правила** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| Комментарии вендоров | | | | | | Порядка 4000 правил и их регулярное обновление и пополнение | | | |
| **Автоматическая конвертация файлов в безопасный формат в почтовом трафике** | 🔴 | 🔴 | 🔴 | 🟢 | 🔴 | 🔴 | 🟢 | 🟢 | 🟡 |
| Комментарии вендоров | | | | | | | | Поддерживается основным комонентом FortiMail | Требуется интеграция с основным компонентом Email Security Safeguard и дополнительным компонентом Email Threat Isolation |
| **Автоматическая конвертация файлов в веб-трафике** | 🔴 | 🔴 | 🔴 | 🟢 | 🔴 | 🔴 | 🟢 | 🟡 | 🟡 |
| Комментарии вендоров | | | | | | | | Требуется интеграция с дополнительным компонентом FortiGate | Требуется интеграция с дополнительным компонентом Web Isolation |
| **Принудительная передача файлов на анализ в ручном режиме** | 🟢 | 🟢 | 🟢 | 🟢 | 🟡 | 🟢 | 🟢 | 🟢 | 🔴 |
| Комментарии вендоров | | | | | Требуется дополнительный компонент AX или облачный вариант (загрузка по требованию) | | | | |



🟢 да 🟡 частично 🔴 нет

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Принудительное определение файлов как вредоносных в ручном режиме** | 🟢 | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🟡 | 🟢 | 🔴 |
| Комментарии вендоров | YARA-правила, гибкий язык поиска, использование локальной базы вердиктов KPSN, а также путем ручного добавления IoC | | | | YARA-правила, «черные» и «белые» списки | Через хеши, YARA, STIX | Частично (по хешам на уровне шлюза или «песочницы»)<br><br>На уровне агента Threat Hunting | YARA-правила, «черные» списки (MD5, SHA1, SHA256, regex, управление доменами) | |

## КАЧЕСТВО ОБНАРУЖЕНИЯ

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Анализ сетевого трафика на аномалии, выявление бот-сетей** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Анализ HTTP-сессий целиком (JavaScript, XSS, уязвимости в flash)** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Поддержка динамического анализа одновременно в нескольких ОС локально на устройстве (Multi-Version)** | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟡 |
| Комментарии вендоров | Исполнение каждого объекта одновременно в 3 разных версиях ОС | Roadmap | | | | | | | Требуется дополнительный компонент CAS |
| **Поддержка динамического анализа одновременно с несколькими версиями прикладного ПО локально на устройстве (Multi-Version)** | 🟢 | 🟡 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟡 |
| Комментарии вендоров | Файл запускается в нескольких ОС и на разных версиях ПО | Только последовательно | | | | | | | Требуется дополнительный компонент CAS |
| **Выявление использования утилит администраторов (PsExec, WMI, PowerShell)** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |



🟢 да 🟡 частично 🔴 нет

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Выявление многовекторных атак (Multi-Vector Attack)**<br><br>Предполагается не только отслеживание атаки через несколько векторов, но и обмен информацией между компонентами системы для защиты от угроз такого типа | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Обнаружение сложных составных атак с доставкой вредоносного кода по частям с разных внешних ресурсов (Multi-Flow Attack)**<br><br>В зависимости от производителя, детектирование таких видов угроз осуществляется на уровне сети или агента на рабочей станции | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Выявление активностей с использованием Tor**<br><br>Комментарии вендоров | ● | ● | ● | ● | ● | ● | ● | ● | ●<br><br>Требуется дополнительный компонент ProxySG |
| **Выявление попыток соединения с центрами управления ботнетами (C&C)** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Threat Hunting**<br><br>Функционал позволяет аналитикам и офицерам ИБ не только реагировать, но и детектировать скрытые продвинутые угрозы на ранних этапах до нанесения ущерба компании<br><br>Рассматриваемые решения предлагают функционал как в рамках текущих продуктов, так и в рамках дополнительных сервисов или услуг | ● | ● | ● | ● | ● | ● | ● | ● | ● |



● да ● частично ● нет

# ВАРИАНТЫ ИНТЕГРАЦИИ

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Поддержка API**<br><br>Возможность интеграции собственных сторонних решений<br><br>Часть заказчиков реализует свои сервисы автоматизированной проверки объектов в «песочнице» с получением обратной связи | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Использование IoC вендора** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Добавление IoC вручную**<br><br>Комментарии вендоров | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟡<br><br>Только поиск по IoC |
| **Экспорт IoC** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Поддержка формата JSON**<br><br>Комментарии вендоров | 🔴<br><br>Поддержка в отдельном продукте вендора Research Sandbox | 🟡<br><br>Только в дополнительном компоненте PT CybSI | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Импорт IoC** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **OpenIOC**<br>(открытый стандарт описания индикаторов компрометации)<br><br>Комментарии вендоров | 🟢 | 🟡<br><br>Только в дополнительном компоненте PT CybSI | 🔴 | 🟢 | 🟢 | 🟢 | 🔴 | 🔴 | 🔴 |
| **STIX**<br>(стандарт предоставления унифицированной информации о киберугрозах)<br><br>Комментарии вендоров | 🟢 | 🟡<br><br>Только в дополнительном компоненте PT CybSI | 🔴 | 🔴<br><br>Roadmap Q1 2020 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **TAXII**<br>(стандарт унификации способов обмена сведениями о киберугрозах по протоколу HTTPS, описанных с помощью STIX)<br><br>Комментарии вендоров | 🔴 | 🟡<br><br>Только в дополнительном компоненте PT CybSI | 🔴 | 🔴<br><br>Roadmap Q1 2020 | 🔴 | 🟢 | 🟡<br><br>При наличии дополнительного компонента Check Point Threat Cloud | 🔴 | 🔴 |



🟢 да 🟡 частично 🔴 нет

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Threat Intelligence в составе решения** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Отправка хеша файла на сервис VirusTotal**<br><br>Комментарии вендоров | 🟢 | 🔴 | 🟢 | 🟢 | 🟡<br><br>Доступен только через Helix, через API продуктов FireEye и API VirusTotal | 🟡<br><br>Только в ручном режиме | 🟢 | 🟢 | 🟢 |
| **Прямая интеграция с сетевыми системами (прокси, МСЭ, IDS/IPS)**<br><br>Комментарии вендоров | 🟡<br><br>В виде коннектора, реализуемого силами вендора<br><br>Посредством API в Roadmap | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟡<br><br>Требуется дополнительный компонент CAS, поддерживается ICAP и API |
| **Интеграция с WAF (Web Application Firewall)**<br><br>Может быть реализована для проверки в «песочнице» контента, поступающего в веб-приложение<br><br>Комментарии вендоров | 🟡<br><br>Интеграция производится силами вендора<br><br>Посредством API в Roadmap | 🟢 | 🔴 | 🟢 | 🟢<br><br>Интеграция с WAF от Imperva и F5 | 🟡<br><br>Поддержка только части форматов данных для обработки | 🟢<br><br>Интегрируется с WAF от Positive Technologies | 🟢 | 🟢 |
| **Интеграция с Honeypot**<br><br>Решения сигнализируют о сборе и анализе информации атакующими и скрытом распространении ВПО в корпоративной сети с целью обнаружения наиболее ценных активов<br><br>Могут отправлять в «песочницу» обнаруженные исполняемые файлы на анализ, взаимодействовать с решениями EDR для оперативного реагирования<br><br>Комментарии вендоров | 🟢<br><br>Через API | 🟡 | 🟢<br><br>Через API | 🟢 | 🟢 | 🟢<br><br>Через API | 🟢<br><br>Через API<br><br>Реализована интеграция с TrapX | 🟢 | 🟢 |



🟢 да 🟡 частично 🔴 нет

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Интеграция с CRM**<br><br>Позволяет организовать проверку семплов, загружаемых из внешних источников и с рабочих станций пользователей в корпоративные ИС (системы документооборота, CRM, корпоративный портал, чат и т.д.)<br><br>Комментарии вендоров | 🟢 | 🟢<br><br>Через API | 🟢<br><br>Через API | 🔴<br><br>Roadmap Q1 2020 | 🟢 | 🟢<br><br>Через API | 🟢 | 🟢 | 🟢 |
| **Интеграция с MDM, EMM, UEM**<br><br>Решения позволяют управлять конечными и в том числе мобильными устройствами (или службами) через единую консоль, что не только повышает уровень ИБ, но и значительно сокращает затраты на эксплуатацию<br><br>Комментарии вендоров | 🟢 | 🔴 | 🟢<br><br>Через API | 🔴<br><br>Roadmap Q1 2020 | 🟢 | 🟡<br><br>Частично | 🟢 | 🟢 | 🟢 |
| **Интеграция с SIEM** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Поддержка CEF-формата** | 🟢 | 🔴 | 🟢 | | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Интеграция с SOAR (Security Orchestration, Automation and Response)**<br><br>Инструмент обобщения сведений об угрозах безопасности, поступающих из различных источников с помощью коннекторов; служит для автоматизации процессов управления ИБ | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |



🟢 да 🟡 частично 🔴 нет

# СЕРВИСЫ

Российский рынок Anti-APT постепенно приходит к выводу, что при работе с решениями требуется экспертный анализ. Большинство вендоров предлагают тренинги, сервисы по мониторингу и реагированию на инциденты ИБ, предоставляют доступ к порталам знаний об индикаторах компрометации и их взаимосвязи.

Экспертные сервисы предлагают и сервис-провайдеры, специализирующиеся на услугах аутсорсинга информационной безопасности. Например, Центр мониторинга и реагирования на инциденты ИБ Jet CSIRT компании «Инфосистемы Джет», помимо услуг традиционного SOC, предоставляет сервисы по эксплуатации средств защиты информации, управлению уязвимостями, киберкриминалистике, киберучениям, OSINT и другие.

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Обучение от вендора** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **SOC вендора** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🔴 | 🟢 | 🟢 |
| Комментарии вендоров | Kaspersky Managed Protection and Incident Response Services | PT Expert Security Center | | | | XDR | Roadmap | FortiGuard | Managed EDR Service |
| **Сервис вендора по мониторингу и реагированию на инциденты ИБ** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| Комментарии вендоров | | PT Expert Security Center | | | | Managed Detection and Response (MXDR) | | | |
| **Доступ к Threat Intelligence** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **MSSP-модель** MSSP (Managed Security Service Provider) — предоставление услуг по управлению ИБ по модели Security as a Service | 🟢 | 🟢 | 🟢 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |



🟢 да 🟡 частично 🔴 нет

# СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Решение в реестре отечественного ПО**<br>Комментарии вендоров | ● | ● | ● | ● | ● | ● | ●<br>Разработка ведется в Израиле | ● | ● |
| **Сертификация ФСТЭК, ФСБ**<br>Комментарии вендоров | ● | ●<br>PT NAD — сертификат ФСТЭК, PT Sandbox — в процессе получения | ● | ●<br>В процессе получения | ● | ●<br>Сертификат ФСТЭК есть у дополнительного компонента DS и основного компонента Apex One | ●<br>В процессе получения | ● | ● |
| **Сертификация МО**<br>Комментарии вендоров | ● | ●<br>2 уровень контроля отсутствия НДВ | ●<br>В процессе получения | ●<br>В процессе получения | ● | ● | ●<br>В процессе получения | ● | ● |
| **Наличие локального производства в России** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Защита инфраструктуры с повышенными требованиями к изоляции** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **«Приватная» база обновлений**<br>Комментарии вендоров | ●<br>Kaspersky Private Security Network (KPSN) | ● | ●<br>TDS Huntbox | ● | ●<br>Central Manager (CM)<br>Доступен автономный режим | ●<br>Apex Central, Deep Discovery Director (DDD) | ●<br>Check Point Private Threat Cloud (PTC) | ●<br>FortiManager | ●<br>Symantec Insight for Private Clouds (SIPC) |



● да ● частично ● нет

# КРИМИНАЛИСТИЧЕСКАЯ ЛАБОРАТОРИЯ

Наши заказчики все чаще используют решения Anti-APT как криминалистическую лабораторию для безопасного запуска семплов, обнаружения и анализа ВПО и продвинутых угроз. Такие «песочницы» отличаются от стандартных расширенным журналированием и углубленной отчетностью о поведении файла. Решения могут применяться аналитиками вредоносных программ, аналитиками SOC или CERT и другими квалифицированными специалистами, которые отвечают за анализ угроз и реагирование на инциденты информационной безопасности.

## Вариант решения

| Продукт | Research Sandbox | PT CybSI | Group-IB TDS Huntbox, TDS Polygon | ATHENA | FireEye AX | DDAN | Check Point SandBlast, SandBlast Agent | FortiSandbox | Symantec Security Analytics с локальной «песочницей» CAS |
|---|---|---|---|---|---|---|---|---|---|
| **Локальное**<br>Комментарии вендоров | 🟡<br>Предрелизная версия<br>Релиз запланирован в Q2 2020 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Облако**<br>Комментарии вендоров | 🟢 | 🔴<br>PT Expert Security Center | 🟢 | 🟢 | 🟢 | 🟡<br>Только для двух основных компонентов: виртуального DDI и облачного Apex One | 🟢 | 🟢 | 🔴 |

## Варианты использования

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Ручная загрузка семплов** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Автоматическая загрузка семплов** | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Интеграция с внешними системами**<br>Комментарии вендоров | 🔴<br>Roadmap | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Личные кабинеты аналитиков**<br>Комментарии вендоров | 🟢 | 🔴<br>Roadmap | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🔴 |
| **Гибкая настройка справочников**<br>Комментарии вендоров | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🔴 | 🟢 | 🟡<br>Возможность создавать только YARA-правила, «черные» списки (MD5, SHA1, SHA256, regex, управление доменами) | 🔴 |
| **Создание своей базы знаний ВПО**<br>Комментарии вендоров | 🟢 | 🟢 | 🔴 | 🟢 | 🔴 | 🟡<br>Только на уровне индикаторов компрометации разных форматов | 🟢 | 🟢 | 🔴 |
| **Создание собственных шаблонов исследований**<br>Комментарии вендоров | 🟢 | 🔴<br>Roadmap | 🔴 | 🟢 | 🟢 | 🔴 | 🟢 | 🟢 | 🔴 |



🟢 да 🟡 частично 🔴 нет

| Продукт | Research Sandbox | PT CybSI | Group-IB TDS Huntbox, TDS Polygon | ATHENA | FireEye AX | DDAN | Check Point SandBlast, SandBlast Agent | FortiSandbox | Symantec Security Analytics с локальной «песочницей» CAS |
|---|---|---|---|---|---|---|---|---|---|
| **Сравнение исследований**<br>Комментарии вендоров | ● | ●<br>Roadmap | ●<br>Roadmap | ● | ● | ● | ● | ● | ● |
| **Возможность повторной загрузки файла с той же контрольной суммой (например, с другим расширением) для повторного анализа** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Экспертный анализ ВПО с использованием углубленных аналитик** | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Средство удаленного контроля за ходом исполнения анализируемого объекта**<br>Пример реализации: свободно распространяемое средство Guacamole Remote Control<br>Комментарии вендоров | ● | ● | ● | ● | ● | ●<br>Слайд-шоу со сменой кадров каждые 5 секунд | ●<br>Используется VNC | ●<br>Возможность создания видеозаписи | ● |
| **Дополнительные возможности**<br>Комментарии вендоров | | | | Анализ результатов динамического анализа с помощью Python-скриптов | | | Автоматическое создание детальных отчетов форензики SandBlast Agent | | |



● да ● частично ● нет

# РАЗНОЕ

| Продукт | Kaspersky Anti Targeted Attack | PT Anti-APT | Group-IB Threat Detection System | ATHENA | FireEye | Trend Micro Deep Discovery | Check Point SandBlast | Fortinet ATP | Symantec |
|---|---|---|---|---|---|---|---|---|---|
| **Результаты тестов независимых лабораторий** | Radicati Group, 2018:<br>Kaspersky Anti Targeted Attack<br><br>ICSA Labs:<br>Kaspersky Anti Targeted Attack<br><br>SE Labs: BREACH<br><br>RESPONSE TEST:<br>Kaspersky Anti Targeted Attack<br><br>MITRE Round2 (APT29) Evaluation:<br>Kaspersky Anti Targeted Attack | | IMDA SG (Singapore) Certified:<br>TDS<br><br>Gartner:<br>TI | | AV Comparatives, 2018:<br>HX<br><br>ICSA Labs Endpoint Anti-Malware:<br>HX<br><br>Forrester MITRE ATT&CK Evaluation:<br>FireEye<br><br>The Forrester New Wave™: External Threat Intelligence Services,<br>The Forrester Wave™: Cybersecurity Incident Response Services:<br>TI FireEye | NSS Labs Breach Detection System, 2014-2019: DDI<br><br>NSS Labs. BPS (Breach Prevention System), 2019: TP, DDAN, OSCE (Apex One) | NSS Labs Breach Prevention System 2019: шлюз безопасности, «песочница», агенты<br><br>Gartner MTD 2019, Miercom MTD 2019: защита мобильных устройств | NSS Labs Breach Prevention System, 2019 (Recommended):<br>Шлюз безопасности, «песочница», агент<br><br>BDS 2018 (Recommended):<br>«песочница», агент<br><br>ICSA ATD Certified с 2015 года:<br>шлюзы, «песочница», агенты | RADICATI, Endpoint Security Market Quadrant, 2018:<br>агенты |
| **Лицензирование**<br><br>Комментарии вендоров | По пропускной способности канала; по количеству сенсоров; по числу пользователей или устройств: KEDR, Kaspersky Security для бизнеса, Kaspersky для мобильных устройств, Kaspersky Security для систем хранения данных<br><br>По количеству виртуальных машин, CPU: Kaspersky для виртуальных сред | По объему анализируемого трафика, количеству почтовых ящиков, использованию дополнительных источников | По пропускной способности канала и количеству модулей:<br>TDS Sensor<br><br>По количеству уникальных файлов в час: TDS Polygon<br><br>По количеству агентов:<br>TDS Huntpoint | По количеству уникальных файлов в час, количеству пользователей | По количеству пользователей почты: EX<br><br>По пропускной способности канала: NX<br><br>По количеству уникальных файлов в час:<br>AX, FX<br><br>По количеству агентов:<br>HX | По количеству пользователей: DDEI, DS, TM MS, CAS, Apex<br><br>По пропускной способности: DDI, DDWI<br><br>По количеству устройств: DDAN | По количеству уникальных файлов в час: сайзинг «песочницы»<br><br>По количеству ядер: виртуальные шлюзы<br><br>По количеству защищаемых пользователей или устройств: SandBlast Agent, SandBlast Mobile, CloudGuard SaaS | По количеству обрабатываемых файлов, без ограничения по количеству пользователей и устройств: подбор «песочницы»<br><br>По производительности: FortiMail<br><br>По количеству агентов: FortiClient | По устройствам: CAS, Security Analytics<br><br>По пользователям: все остальное |
| **Актуальные killer-feature решений**<br><br>Комментарии вендоров | Kaspersky Sandbox: автоматическая отправка неизвестных файлов с антивируса KES на проверку в «песочницу»<br><br>Автоматическая блокировка без привлечения вирусного аналитика или офицера ИБ | Глубокий анализ сетевого трафика<br><br>Возможность хранения «сырого» трафика | Услуги по глубокому криминалистическому расследованию<br><br>Страховка от киберрисков | Физическая «песочница»<br><br>Поддержка отечественных ОС (Astra Linux, RedOS, ALT Linux, ROSA Linux) | Решение класса BAS (Breach and Attack Simulation) для симуляции атак и взломов<br><br>Инструментальная платформа Verodin Security позволяет выполнять реальные атаки и симуляции проникновения с непрерывным опросом существующего стека безопасности, включая олицетворение субъектов угроз APT | При невозможности вскрыть вложенный файл, защищённый паролем, система может поместить письмо в карантин с возможностью последующей перепроверки путём ввода пароля в карантинной зоне. Пароль может быть получен как от целевого получателя письма, так и в самой системе (в виде скриншота письма, попавшего в карантин). Кейс в последнее время очень актуален для наших заказчиков, когда, например, приходит SMS с паролем от контрагента, и у «песочницы» есть возможность перепроверить содержимое архива | Проверка дополнительных протоколов SCP, SFTP и SMBv3, протоколов АСУ ТП | Прямая интеграция FortiSandbox с большим портфелем решений по информационной безопасности Fortinet (от периметровой защиты до SIEM) | Возможность изоляции веб-трафика и загружаемых файлов (Web Isolation) без применения терминальных серверов и агентов на конечных устройствах |

На рынке Anti-APT продолжается переход от превентивных технологий к обнаружению, реагированию и прогнозированию инцидентов с привлечением как собственных аналитиков, так и специалистов вендоров или интеграторов в рамках подписочных и сервисных моделей. Вопросы ближайшей перспективы — что делать с зараженными репозитариями: библиотеками, Docker-образами и т.п.? О том, как будет развиваться направление решений для защиты от целенаправленных атак и атак нулевого дня, 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