ПРИЛОЖЕНИЕ

«ПЕСОЧНИЦЫ» ПОД МИКРОСКОПОМ: ОБЗОР РЕШЕНИЙ

JETINFO

№	КРИТЕРИЙ	FIREEYE	TREND MICRO DEEP DISCOVERY	CHECK POINT SANDBLAST	FORTISANDBOX	KASPERSKY ANTI TARGETED ATTACK PLATFORM (KATA)	MULTISCANNER	TDS
	1. ОБЩАЯ ИНФОРМАЦИЯ О ВЕНДОРЕ							
1	**Компания-вендор**	FireEye Inc	Trend Micro Inc	Check Point Software Technologies Ltd	Fortinet	АО «Лаборатория Касперского»	Positive Technologies	Group-IB
	Штаб-квартира	США, Калифорния	Япония, Токио	Израиль, Тель-Авив	США, Калифорния	Россия, Москва	Россия, Москва	Россия, Москва
	Веб-сайт	https://www.fireeye.com/	http://www.trendmicro.com.	https://www.checkpoint.com/	https://www.fortinet.com/	https://www.kaspersky.com/	https://www.ptsecurity.com	https://www.group-ib.ru/
	2. АРХИТЕКТУРА РЕШЕНИЙ							
2	**Варианты исполнения**							
	Hardware Appliance	+	+	+	+	–	+	+
	Virtual Appliance	+	+	–	+	+	+	+
	Software	–	–	–	–	+	+	–
	Cloud	+	+	+	+	–	–	+
	С учетом приобретенного опыта мы рекомендуем осуществлять эмуляцию файлов именно на аппаратной «песочнице». Все рассматриваемые решения готовы предложить такой вариант. С одной стороны, аппаратная «песочница» требует минимальных настроек по сравнению с виртуальной, а с другой — является более высокопроизводительной. Кроме того, в этом случае есть поддержка CPU-level detection (см. критерий ниже). Остальные компоненты, например шлюз безопасности, сенсор, система управления, останутся прежними, могут рассматриваться в виртуальном исполнении.							
3	**Основные варианты интеграции**							
а	**Веб**							
	Мониторинг	TAP/SPAN	TAP/SPAN/ICAP	TAP/SPAN/ICAP	TAP/SPAN/ICAP	SPAN/ICAP	SPAN/ICAP	TAP/SPAN/ICAP
	Блокировка	+	Требуется интеграция с собственным прокси или сторонним прокси/МСЭ *(в RoadMap DD Web Inspector)*	+	Требуется интеграция с FortiGate или FortiWeb	Требуется интеграция с прокси/МСЭ	Требуется интеграция с межсетевым экраном прикладного уровня *(для веб-трафика на портал)* или с любой другой системой, поддерживающей ICAP *(для мониторинга и блокировки пользовательского веб)*	Требуется интеграция с прокси/МСЭ
	С точки зрения анализа веб-трафика мы рекомендуем использовать режим мониторинга. Данный вариант исключает воздействие на бизнес-процессы, так как не вносит задержек. Кроме того, решение не заметно злоумышленникам, при этом оно позволяет обнаруживать угрозы на самых ранних стадиях. Блокировку целесообразно осуществлять на уровне рабочих станций, когда скачиваемые файлы перехватываются и проверяются в «песочнице» до их открытия и запуска, или на уровне сетевого оборудования после вынесения соответствующего вердикта для передачи фидов и создания правил блокировки.							
б	**Email**							
	Мониторинг	BCC/SPAN	BCC/SPAN	BCC/SPAN	TAP/SPAN/BCC	BCC/SPAN/SMTP	MTA/SPAN	BCC/ SMTP from SPAN/SMTP
	Блокировка	MTA	MTA	MTA	Требуется интеграция с FortiMail	Требуется интеграция с KSMG	MTA	MTA
	На сегодняшний день почта остается основным вектором распространения направленных атак. Все рассматриваемые решения поддерживают возможность блокировки почты напрямую или через свой почтовый шлюз/антиспам. Мы рекомендуем использовать данный 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.							
4	**Архитектура решения**							
	Основные компоненты	• NX — анализ веб-трафика • EX — анализ почты • HX — защита рабочих станций	• DDI — анализ • пограничного и внутреннего трафика, включая веб и DNS, запросы/отклики + SMB • DDEI — анализ почты • Office Scan — защита рабочих станций	• SandBlast — анализ веб-трафика, почты, проверка SSL трафика • SandBlast Agent — защита рабочих станций	• FortiSandBox— универсальная «песочница», поддерживающая все виды сенсоров • FortiClient — защита рабочих станций	• Сетевые сенсоры • Сенсоры для рабочих станций и серверов • Central Node — центр анализа • Sandbox — «песочница»	• MultiScanner— система анализа веб-трафика, почты, файловых хранилищ	• TDS Sensor — средство анализа сетевого трафика • TDS Polygon — система поведенческого анализа файлов • TDS SOC — внутренний центр обновлений, центр управления сетью устройств, веб-интерфейс, масштабируемое хранилище данных
	Дополнительные компоненты	• FX — защита файловых серверов • AX — анализ и проведение расследований • PX — захват трафика	• DDD *(Director)* — сейчас используется только для централизованного управления обновлениями и «песочницами». В RoadMap — поддержка централизации DDEI для политик и карантина + расширенное расследование инцидентов • DDaN — внешняя «песочница» • InterScan Web Security — прокси-сервер	• Smart Event — централизованная система сбора и анализа журналов безопасности инфраструктуры Check Point • Check Point Security шлюз безопасности с набором блейдов NGTX для интеграции с «песочницей»	• FortiGate-шлюз безопасности • FortiMail-антиспам	• Kaspersky Endpoint Security — сенсор для сетевого решения KATA • Kaspersky Private Security Network (KPSN) — локальная база репутаций для изолированных сетей *(приватная инсталляция решения)* • Kaspersky Secure Mail Gateway (KSMG) — для сбора данных и блокировки вредоносной активности в почте	• HoneyPot — «песочница»	• TDS SOC — внутренний центр обновлений, центр управления сетью устройств, веб-интерфейс, масштабируемое хранилище данных
	Централизованная система управления	+ CM	+ Control Manager	+ Smart Center	+	+	+	– RoadMap
	Почти каждый производитель позиционирует свое решение не как отдельную «песочницу», а как продукт с большим набором дополнительных 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 почта), и прокси. При этом внедряемые решения должны иметь централизованную консоль управления. Внедрение «песочниц» необходимо рассматривать как комплексный проект по информационной безопасности.							
	3. ПОКРЫТИЕ КАНАЛОВ РАСПРОСТРАНЕНИЯ УГРОЗ							
5	**HTTP**	+	+	+	+	+	+	+
6	**HTTPS**	**Требуется интеграция:** • Стороннее решение *(например, A10, F5 и др.)* • Компонент NX с функцией расшифровки SSL *(RoadMap Q1 2018)*	**Требуется интеграция:** • Стороннее решение *(например, A10, F5 и др.)* • ICAP *(DDaN)*	+	**Требуется интеграция:** • Стороннее решение *(например, A10, F5 и др.)* • FortiGate • FortiWeb • ICAP	**Требуется интеграция:** • Стороннее решение *(например, A10, F5 и др.)* • ICAP	**Требуется интеграция:** • Стороннее решение *(например, A10, F5 и др.)* • ICAP	**Требуется интеграция:** • Стороннее решение *(например, A10, F5 и др.)* • ICAP
	Наш опыт показал, что использовать «песочницу» для анализа только HTTP-трафика даже на пилоте нецелесообразно. Необходима расшифровка SSL-трафика и его анализ на скрытые угрозы, ведь его доля уже превышает 50% в общем объеме, а если говорить о вредоносном трафике, она значительно выше.							
7	**Веб-приложения (соцсети, пр.)**	+	+	+ Включая виджеты социальных сетей *(функция NGFW)*	+	+	Требуется интеграция с системой, поддерживающей ICAP	+
8	**Мессенджеры**	+	+	+	+	+	+	+
9	**USB**	**Требуется наличие компонентов:** • HX Альтернатива • Сторонние решения *(например, DeviceLock и др.)*	**Требуется наличие компонентов:** • TrendMicro OfficeScan • скрипты	**Требуется наличие компонентов:** • SandBlast Agent	**Требуется наличие компонентов:** • FortiClient или • Carbon Black	**Требуется наличие компонентов:** • Сенсоры рабочих мест	– Посредством ручной загрузки файлов в веб-интерфейс MultiScanner	–
10	**SMTP**	+	+	+	+	+	+	+
11	**FTP**	+	+	+ Через NGTP/NGTX	+	+	+	+
12	**DNS**	+	+	+ Через NGTP/NGTX	+	+	+	+
13	**IMAP**	+	+	+ Через NGTP/NGTX	+	– RoadMap	+	+
14	**POP3**	+	+	+ Через NGTP/NGTX	+	+	+	+
15	**CIFS**	+	+	+ Через NGTP/NGTX	+	+	+	– RoadMap
16	**Дополнительные протоколы**	TFP, IRC, SMB	Более 100 протоколов	Интеграция со сторонними решениями по API/ при использовании как ICAP Server	NFS	Lotus notes *(через SMTP gateway)*, ICAP	SMB, NFS, ICAP	По запросу
	Сегодня компании заинтересованы в анализе не только почты и веб, но и внутренних активностей в корпоративной сети, что подразумевает поддержку широкого спектра протоколов и дополнительных вариантов интеграций. Это позволяет, например, выявить нестандартное использование протоколов, что может использоваться в том числе при сокрытии работы ботнетов.							
	4. СРЕДСТВА АНАЛИЗА							
17	**Тип эмулируемого подозрительного контента в «песочнице»**							
	Копия трафика	+	+	+	+	+	+	–
	Отдельные файлы	+	+	+	+	+	+	+
	Скрипты	+	+	+	+	+	+	+
	Макросы	+	+	+	+	+	+	+
	Проверка архивов с паролем в теле письма	+	+	+	+	+	+	+
	Проверка архивов с паролем, подбираемым по словарю	+	+	+	+	+	+	+
	Проверка веб-ссылок в теле письма	+	+	+ С проверкой синтаксиса	+	+	+	+
	Проверка веб-ссылок внутри документа	+	+	+	+	+	– RoadMap	+
	Проверка укороченных ссылок в теле письма	+	+	–	+	+	– RoadMap	+
	Проверка ссылок с перенаправлениями, ведущими на загрузку файлов	+	+	–	+	+	+	+
	Мобильные приложения	+	+	+	+	+	–	–
	По сравнению с вложениями во вредоносном почтовом трафике ссылки набирают все большую популярность . Неслучайно проверка ссылок в теле письма — уже базовый функционал «песочниц». Все решения проверяют прямые ссылки (*.doc, *.pdf и т.п.). С укороченными и перенаправляющими ссылками продукты работают по-разному. Одни решения проверяют такие ссылки. Другие нет, обосновывая это тем, что есть риск выполнить действия от лица пользователя (подписка на рассылку, сброс 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 очень популярно распространение java-скриптов в виде ссылок. Как показала практика, напрямую на шлюзе безопасности они не блокируются. И в этом случае поможет «песочница».							
18	**Кастомизация «песочниц»**	– Образы преднастроены производителем	+	По запросу	+ Возможно создание собственных образов как на основе образов, подготовленных Fortinet, так и с нуля	По запросу	+	По запросу
	Большинство решений поддерживает возможность создания кастомизированных образов ОС. Данный функционал позволяет воссоздать среду, идентичную рабочей (с конкретной ОС, набором ПО и т.д.), чтобы максимально приблизить эмулируемую среду к реальной. Для обеспечения гарантированной производительности и уровня детектирования угроз для некоторых из решений необходимо обратиться в техническую поддержку конкретного вендора. Стоит отметить, что, с одной стороны, кастомизация — полезная функция, позволяющая повысить уровень детектирования угроз, особенно заточенных под конкретную компанию, с другой — при использовании этой функции может возникнуть большое количество ложных срабатываний при некорректной настройке, что приведет к деградации производительности системы.							
19	**Используемые технологии эмуляции**	Собственная платформа	Custom VirtualBox	Собственная платформа	Custom VirtualBox	Custom KVM	KVM, VMWare	Custom Virtual Box
20	**Отслеживание исполнения кода на уровне CPU *(CPU-Level detection)***	+ **MVX (механизм динамического анализа) использует специально созданный гипервизор, где внедрены все инструменты мониторинга. Таким образом, осуществляется отслеживание вызовов между user space, kernel space и CPU from that level.**	–	+	+	+	–	–
21	**Отслеживание исполнения кода на уровне ядра ОС**	+	+	+	+	+	+	+
	Рассматриваемые решения могут отслеживать исполнение кода на уровне CPU и/или на уровне ядра ОС. CPU-Level detection позволяет детектировать эксплойты до того, как они начнут использовать методы обнаружения и обхода «песочниц». 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.							
22	**Система сокрытия работы в виртуальной среде (Anti-VM evasion protection)**	+ Собственная технология	+ За счет гибкой настройки образов VM. API Hooking используется для перехвата запросов вредоносных приложений и возврата ложных значений относительно среды работы. + разные MAC адреса + возможность использовать адресацию корпоративной сети и многое другое	+	+ Собственная технология	+ **Сокрытие:** противодействие обнаружению исполнения в «песочнице». **Детектирование:** evasion-техник как отдельный набор детектов	+	+ Собственная технология
23	**Поддерживаемые ОС**							
	Windows XP	+	+	+	+	+	+	+
	Windows 7	+	+	+	+	+	+	+
	Windows 8/8.1	+	+	+	+	–	+	+
	Windows 10	+	+	+	+	–	+	+
	Windows Server	–	+ Win *2003, 2008, 2012, 2016*	–	+ Win *2003, 2008, 2012*	–	+	–
	Mac OS X	+ Модельный ряд ограничен	+ Облако	–	+	–	–	–
	Android	+ Облако	+ Облако	+ SandBlast Mobile	+	+/– Реализовано в виде технологии Risk Score для анализа apk-объектов *(в RoadMap VM Android)*	–	–
	IOS	+ Облако	–	+ SandBlast Mobile	–	–	–	–
24	**Поддерживаемые языки в ОС**							
	Английский	+	+	+	+	+	+	+
	Русский	+	+	По запросу	+ Любой язык на выбор	– RoadMap	+	+
25	**Лицензии на Windows/ Office в составе решения**	+	–	+	Опционально *(лицензии заказываются у Fortinet для готовых образов; лицензии предоставляются заказчиком для собственных образов)*	–	– Только на пилот	–
26	**Поддерживаемые типы файлов**							
	Исполняемые	+	+	+	+	+	+	+
	Офисные	+	+	+	+	+	+	+
	Архивы	+	+	+	+	+	+	+
	Скрипты	+	+	+	+	+	+	+
	Аудио/видео	+	+/– Без эмуляции в «песочнице»	+/– Частично *(статический анализ)*	+	+/– Проверка осуществляется в составе антивирусного ядра	+	–
	Графические	+	+ Без эмуляции в «песочнице»	+/– Частично *(статический анализ и конвертация в безопасную версию)*	+	+ Проверка осуществляется в составе антивирусного ядра	+	–
	Мобильные приложения	+	+ облако	+ облако	+	+	–	–
	Другие	Все PE, файлы Microsoft Office, медиафайлы, PDF, Flash и ZIP/RAR/TNEF архивы, vCard	Всего более 50 типов	Flash-анимация с учетом контекста для детектирования сложных составных атак. В RoadMap дополнительные файлы	Любые типы файлов по усмотрению администратора	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, .Mach0, .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, если установлен необходимый для открытия софт	Более 70 различных форматов: .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
27	**Ретроспективный анализ событий**	+	+	+	+	+	+	+
	Ретроспективный анализ событий относится к процедуре расследования инцидентов. Решения позволяют узнать, как зловред попал в сеть компании, какой хост стал жертвой атаки, какие соединения инициировались и т.д. Часть решений позволяет напрямую проводить такой анализ, часть — через отчеты в агентах на рабочих станциях. Осуществляется поддержка сервиса индикаторов компрометации для ретроспективного выявления скомпрометированных узлов.							
28	**Противодействие режиму сна**	+ Ускорение системного времени, имитация работы пользователя	+	+ Ускорение системного времени, имитация работы пользователя	+	+ Ускорение системного времени, имитация работы пользователя	+	+
29	**Возможность масштабирования по производительности (кластеризация)**	+	+	+	+	+	+	+
	5. КАСТОМИЗАЦИЯ ПРОЦЕССА АНАЛИЗА							
30	**Самостоятельная настройка критериев для анализа файлов/ трафика в «песочнице»**	+ YARA-правила	+ Порядка 4000 правил и их регулярное обновление/ пополнение	–	+ YARA-правила	+ Настройка работы «песочницы» в режиме без активного анализа трафика и без интернета или с доступом к интернету с активным анализом посредством IDS-правил. Настройка VIP-групп и белых списков для кастомизированного анализа. YARA-правила	+	По запросу
	Часть решений позволяет самостоятельно настраивать критерии для анализа файлов в «песочнице», например, создание пользовательских сигнатур в формате YARA-правил. Другие производители считают, что такая настройка не нужна, ведь в продукте уже есть множество различных критериев, а кастомизация со стороны пользователя только увеличит число ложных вердиктов.							
31	**Принудительная передача файлов на анализ в ручном режиме**	Требуется наличие компонента AX или FX	Требуется наличие компонента DDaN	+ через Threat Prevention API или команду в CLI	+ поддерживается видеозапись процесса анализа и возможность подключения администратора к ВМ для выполнения действий в процессе анализа	+ через веб-интерфейс, через скрипты	+	+ через API
32	**Принудительное определение файлов как вредоносных в ручном режиме**	+ YARA-правила, методы исключения	+ YARA-правила или интеграция с Application Control посредством использования черных списков файлов	+/– частично *(по хешам на уровне шлюза)*	+ YARA-правила, черные списки	+ YARA-правила, гибкий язык поиска, использование локальной базы вердиктов KPSN, а также путем ручного добавления IoC	+	–
	6. КАЧЕСТВО ОБНАРУЖЕНИЯ							
33	**Анализ сетевого трафика на аномалии, выявления бот-сетей**	+	+	+	+	+	Требуется интеграция с PT NAD	+
34	**Анализ http-сессий целиком** *(java script, XSS, уязвимости в flash)*	+	+	+	+	+	Требуется интеграция с PT NAD	+
35	**Поддержка динамического анализа одновременно в нескольких ОС локально на устройстве** *(Multi-Version)*	+	+	+	+	+ исполнение каждого объекта одновременно в 3 разных версиях ОС	+	+
36	**Поддержка динамического анализа одновременно с несколькими версиями прикладного ПО локально на устройстве** *(Multi-Version)*	+	+	+	+	+ файл запускается в нескольких ОС и на разных версиях ПО	+ только последовательно	+
37	**Выявление использования утилит администраторов** *(PsExec/WMI/ PowerShell)*	+ подозрительное поведение с использованием этих средств	+	+	+	+	+ при наличии YARA-правил	+
	Данные инструменты очень распространены в контексте атак. Например, в одном из проектов было выявлено использование WMI с определенной учетной записью из определенного сетевого сегмента, для которого это запрещено, в направлении критического сетевого ресурса заказчика.							
38	**Выявление многовекторных атак — Multi-Vector Attack**	+	+	+ с использованием SmartEvent	+	+	+	–
	Так называемые Multi-Vector Attack (многовекторные атаки) очень распространены. Например, часто используется вариант фишингового письма с веб-ссылкой. Предполагается не только отслеживание атаки через несколько векторов, но и обмен информацией между компонентами системы для защиты от угроз такого типа.							
39	**Обнаружение сложных составных атак с доставкой вредоносного кода по частям с разных внешних ресурсов — Multi-Flow Attack**	+	+	+	+	+	+	+
	Так называемые Multi-Flow Attack (составные атаки) также очень распространены в последнее время. Доставка вредоносного кода по частям осуществляется с разных внешних ресурсов, в том числе с использованием обфускации и стеганографии. В зависимости от производителя, детектирование таких видов угроз осуществляется на уровне сети или агента на рабочей станции.							
40	**Анализ поведения на рабочих станциях**							
	Наличие агентского ПО для защиты от угроз «нулевого дня»	+	+	+	+	+	–	–
	Легкий агент	+	+	+	+	+	–	–
	Полноценный AV-агент	+/– частично *(поддержка с помощью Bitdefender движка)*	+	+	+	+	–	–
	EDR агент	+	+ Remediation требует наличия полноценного AV-агента	+	Требуется интеграция с Carbon Black	+	–	–
	Возможность изоляции скомпрометированной рабочей станции	+	+	+	+	+ в ручном режиме после решения оператора через единый интерфейс путем отправки исполняемой команды на удаленный АРМ	–	Требуется интеграция с внешней системой
	Наряду с анализом почты и веб заказчики все чаще и чаще обращают внимание на защиту рабочих станций. Большинство рассматриваемых решений имеют в своей линейке агентское ПО для защиты от угроз «нулевого дня». При этом можно выделить так называемые легкие агенты, совместимые с текущим антивирусом заказчика, и полноценные AV-агенты. В последнее время все большую популярность набирают EDR (Endpoint Detection and Response) агенты, которые позволяют выявлять, изолировать и устранять сложные устойчивые угрозы на уровне рабочих станций. Данный класс решений оперативно выявляет отклонения в поведении приложений и объектов с возможностью быстрого восстановления в случае подтверждения инцидента офицером безопасности.							
	7. СТОРОННЯЯ ИНТЕГРАЦИЯ							
41	**Поддержка API**	+	+	+	+	– RoadMap *(текущие проекты по интеграции осуществляются силами вендора. Open API – в процессе формирования)*	+	+
	Наличие API позволяет проводить интеграцию собственных и сторонних решений производителя. Например, часть заказчиков реализует свои сервисы автоматизированной проверки объектов в «песочнице» с получением соответствующего вердикта/обратной связи.							
42	**Работа с файловыми хранилищами**							
	Возможность сканирования по расписанию	+	+	+ SandBlast Agent с блейдом AV	+	+	–	Требуется интеграция с внешней системой через API
	Карантин подозрительных файлов	+	+	+ SandBlast Agent с блейдом AV	+	+	+	Требуется интеграция с внешней системой через API
	Отправка файлов на анализ посредством API	+	+	+ SandBlast Agent с блейдом AV	+	– RoadMap *(присутствует возможность отправки файлов вручную или по ICAP)*	+	+
	Автоматическое перекладывание чистых файлов из одного хранилища в другое	+/– частично (есть возможность очистки архивов)	+ Сторонний скрипт	–	+	–	+	Требуется интеграция с внешней системой через API
	Файловые хранилища — один из потенциальных векторов распространения угроз. Например, контрагенты заказчика подгружают документы на ресурс компании, чем может воспользоваться злоумышленник, поэтому требуется проверка получаемых материалов. Есть возможность запускать сканирование по расписанию и отправлять подозрительные файлы в карантин.							
43	**Работа с индикаторами компрометации (IoC)**							
	Использование IoC вендора	+	+	+	+	+	+	+
	Добавление IoC вручную	+	+	+	+	+	+	–
	Экспорт IoC	+	+	+	+	+	+	–
	Импорт IoC	+	+	+	+	+	+	По запросу
	Indicator of compromise (IoC) — перечень данных об угрозе (URL, хеш (контрольная сумма) файла), IP и т.д.). IoC автоматически генерируются в результате динамического анализа или предоставляемым сервисом вендора. Есть возможность заведения собственного IoC с помощью дополнительных правил. Для многих заказчиков важна возможность импорта IoC-подписок. У решений есть возможность отдавать выявленные IoC, например, через алерты системы. В этом случае заказчик может добавить отправителей в антиспам, черные списки на почтовом сервере или осуществить IP-блокировку на сетевом шлюзе.							
44	**Threat Intelligence в составе решения**	+	+	+	+	+	+	+
	В состав решений входит репутационная база Thrreat Intelligence. Осуществляется обмен с глобальными платформами о ландшафте угроз.							
45	**Прямая интеграция с сетевыми системами** *(прокси, МСЭ, IDS/IPS)*	+ Есть несколько готовых вариантов интеграции, например, с Bluecoat ProxyNG, ForeScout NAC, Infoblox, OpenDNS	+	+	+ FortiGate ICAP-клиент FortiMail	+ В виде коннектора, реализуемого силами вендора. Посредством API в RoadMap	+	+
46	**Интеграция с WAF**	+ Есть несколько готовых вариантов интеграции, например, с Imperva и F5	–	+ с Positive Technologies Application Firewall PT AF	+ с FortiWeb	+ Интеграция производится силами вендора. Посредством API в RoadMap	+ с PT AF	–
47	**Интеграция с SIEM**	+	+	+	+	+	+	+
	«Песочницы» могут выступить в роли важного источника для SIEM-системы заказчика. Все решения, представленные в обзоре, позволяют выгружать логи инцидентов и логи работы «песочниц».							
	8. Разное							
48	**Решение в реестре отечественного ПО**	–	–	– планируется локальное производство в 2018 г.	–	+	+	– в процессе включения в список
50	**Сертификация ФСТЭК/ФСБ**	–	–	– в процессе получения	–	+/– сертификат ФСБ *(СОВ 2017 г.)/ФСТЭК (СОВ, Anti-APT)*	– в процессе получения	– в процессе получения
50	**Сертификация МО**	–	–	– в процессе получения	–	– в процессе получения	+ 2-й уровень контроля отсутствия недекларированных возможностей	– в процессе получения
51	**С какими правами файлы запускаются в «песочнице»?**	Admin	Admin	Admin	Admin	Admin	Admin	Admin