McAfee™
Together is power.

Как объединить решения разных производителей в единую систему реагирования на инциденты ИБ

Руслан Барбашин,
Аккаунт менеджер McAfee
ruslans_barbasins@mcafee.com

#ProfitSecurityDay

Эпиграф

Любовь это вам не просто так!

Любовью надо заниматься!

Андрей Кнышев

Содержание:

- Адаптивная архитектура безопасности (Gartner)
- Как интегрировать решения разных производителей
- Анонс решений McAfee для ОЦИБ

Зачем нужна интеграция решений ИБ?

- Автоматизация обмена данными
  - Threat Intelligence (TI)
  - телеметрия
  - IOC
- Автоматизация изменения политик
- Уменьшение времени обнаружения (MTTD)
- Уменьшение времени реакции и восстановления (MTTR)

!!! Эффективность ИБ !!!

McAfee™
Together is power.

Адаптивная Архитектура Безопасности

Рекомендации аналитического агентства Gartner

И много будет странствий и скитаний:

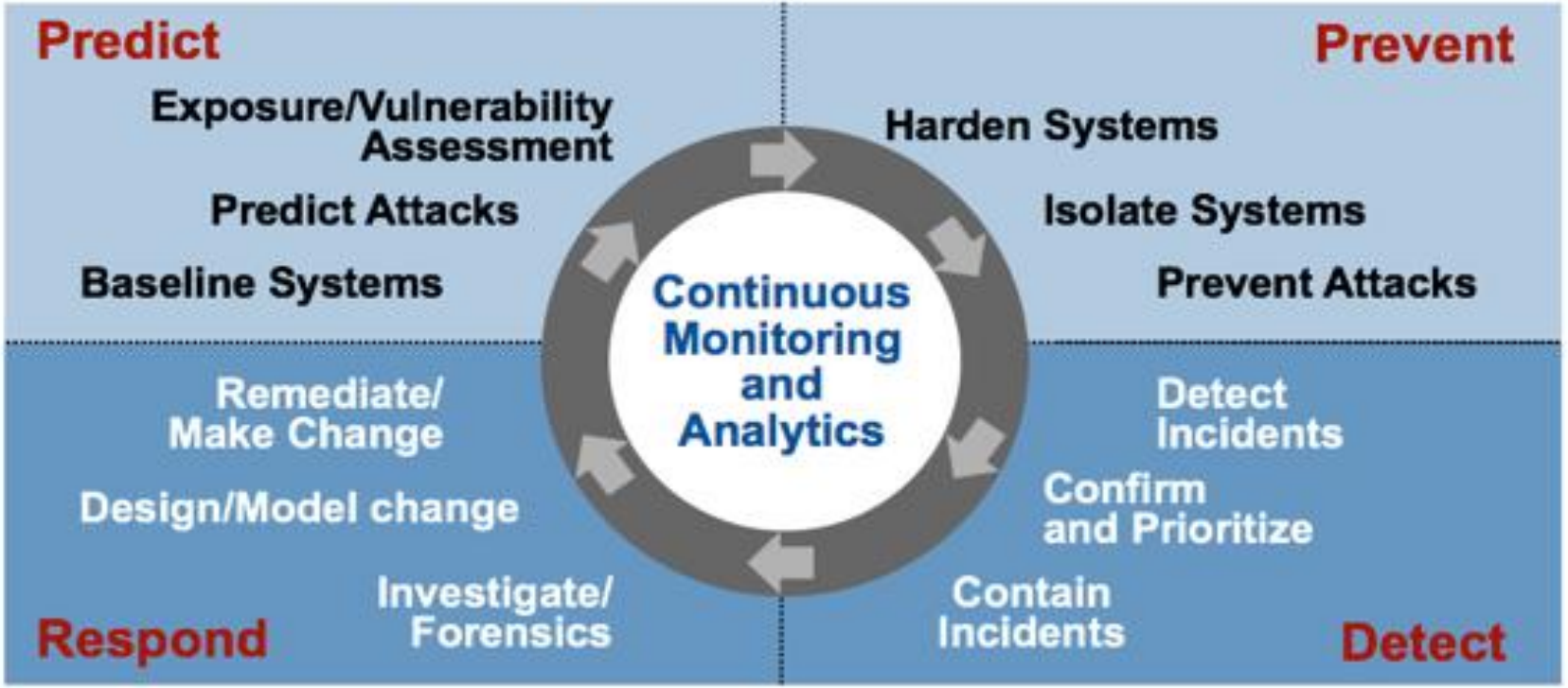
Страна Любви - великая страна!

И с рыцарей своих - для испытаний -

Все строже станет спрашивать она...

Владимир Высоцкий

The Adaptive Security Architecture: Twelve Critical Capabilities of Security



Gartner

Краткие выводы от Gartner:

- Существующих технологий защиты недостаточно для противостояния современным целенаправленным атакам.
- Большинство организаций до сих пор инвестируют средства только в технологии защиты.
- ***Технологии защиты, предотвращения атак, детектирования и расследования/устранения от различных производителей не интегрированы друг с другом, что приводит к дополнительному хаосу, увеличивает затраты и снижает эффективность ИБ.***
- ИБ не хватает постоянной видимости происходящего для детектирования целенаправленных атак.
- Корпоративные системы находятся под постоянными и не прекращающимися атаками, поэтому понятие «Incident Response» больше не подходит.

Рекомендации от Gartner:

- Поменять понятие **«Incident Response»** на **«Continuous Response»,** где предполагается, что системы постоянно скомпрометированы и им необходим непрерывный мониторинг и восстановление.
- Создание **Адаптивной Архитектуры Безопасности** для защиты от целенаправленных атак, используя 12 критических функций от Gartner.
- Направить больше инвестиции на системы обнаружения и быстрого реагирования, и уменьшить на защиту и предотвращение.
- **Отдавать предпочтения производителям, которые предлагают контекстно-ориентированные платформы для сетевой безопасности, безопасности рабочих станций и приложений, а также интегрированный подход к анализу, предотвращению, обнаружению и реагированию на атаки.**
- Развивать **Security Operation Center** (SOC), который позволяет осуществлять постоянный мониторинг и предотвращение атак.
- Осуществлять полный мониторинг на всех уровнях ИТ: сетевых пакетов, сетевых потоков, активности ОС, контента, поведения пользователей.

Экосистема McAfee

А мне приснилось –

Миром правит любовь,

А мне приснилось –

миром правит мечта.

Виктор Цой

Клиент McAfee:

“Мы можем обнаружить атаку в течении 60 секунд, провести анализ и ликвидировать атаку в течении 5 минут”

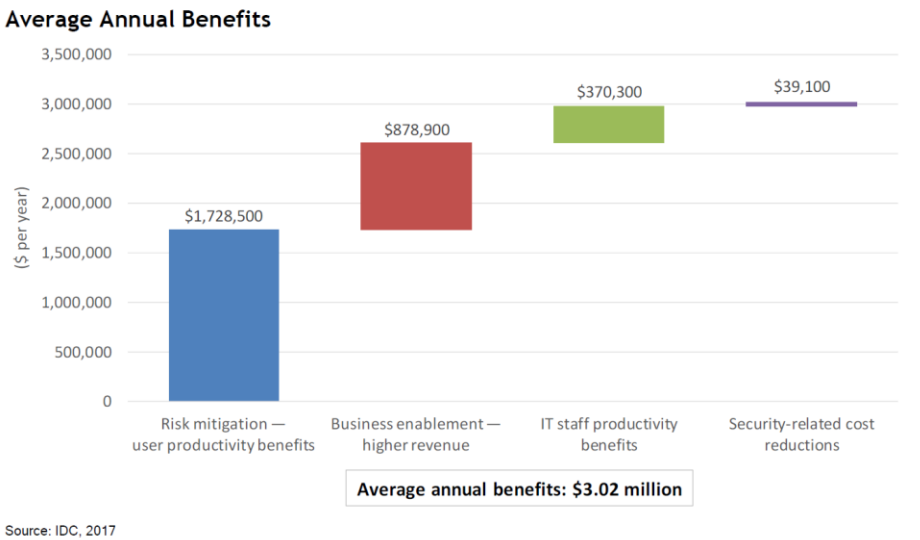
https://www.mcafee.com/enterprise/en-us/assets/case-studies/cs-idc-national-bank.pdf

ExpertROI Spotlight Top 100 US FDIC Bank

“Мы можем обнаружить атаку в течении 60 секунд, провести анализ и ликвидировать атаку в течении 5 минут”

Решения: Endpoint, SIEM, TIE, GTI, ATD, DLP

FIGURE 1



Source: IDC, 2017

- Экономия средств **$3.02 M** в год
- **ROI 208%** в течении 4 лет
- Период окупаемости **20** месяцев
- На **90%** быстрее расследование инцидентов
- На **77%** меньше инцидентов с причиненным ущербом
- На **98%** меньше времени снижение продуктивности из-за инцидентов ИБ
- **$5-10 миллионов** дополнительная прибыль
- Мониторинг всех компонентов на **1-2** консолях

Source: http://idcdocserv.com/US42210917

Содержание:

- Адаптивная архитектура безопасности (Gartner)
- Как интегрировать решения разных производителей
- Анонс решений McAfee для ОЦИБ

KAZAKHSTAN

Межсервисная интеграция до DXL

Для начала интеграция
двух решений

Решение #2

Решение #1

Интеграция решений до DXL

Сначала обмен базовой информацией, host names, credentials, чтобы решения могли начать обмен данными

X Обмен учётными данными

Решение #2

Решение #1

Credentials

Интеграция решений до DXL

Каждый продукт интегрируется с каждым с использованием специализированного API

Решение #2

Решение #1

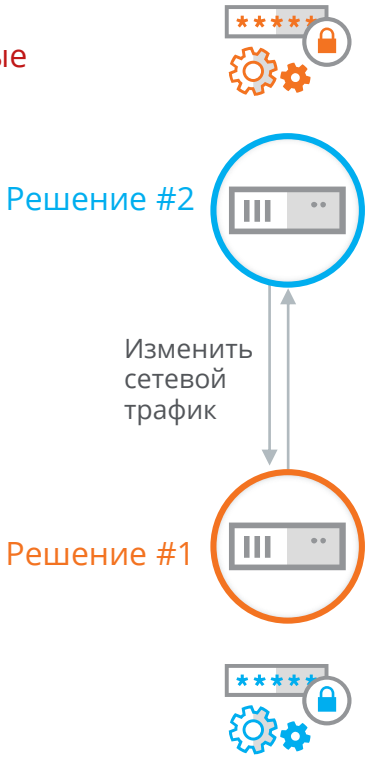
Credentials

API

X	Обмен учётными данными
X	Интеграция на уровне API

Интеграция решений до DXL

Необходимо отрегулировать сетевые политики для разрешения сетевого обмена между решениями (ports, protocols)



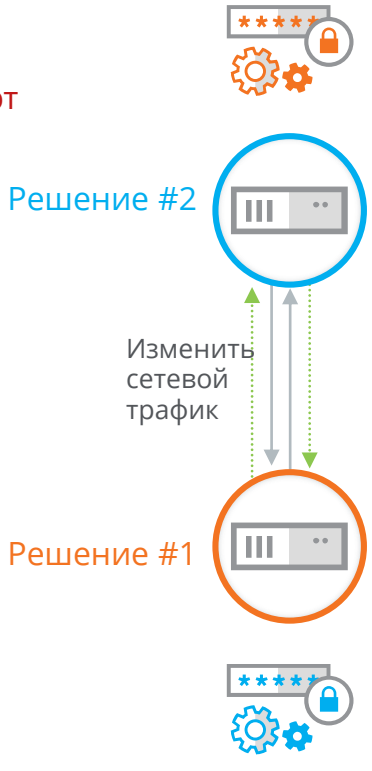
X	Обмен учётными данными
X	Интеграция на уровне API
X	Регулирование сети для портов и протоколов

Credentials

API

Интеграция решений до DXL

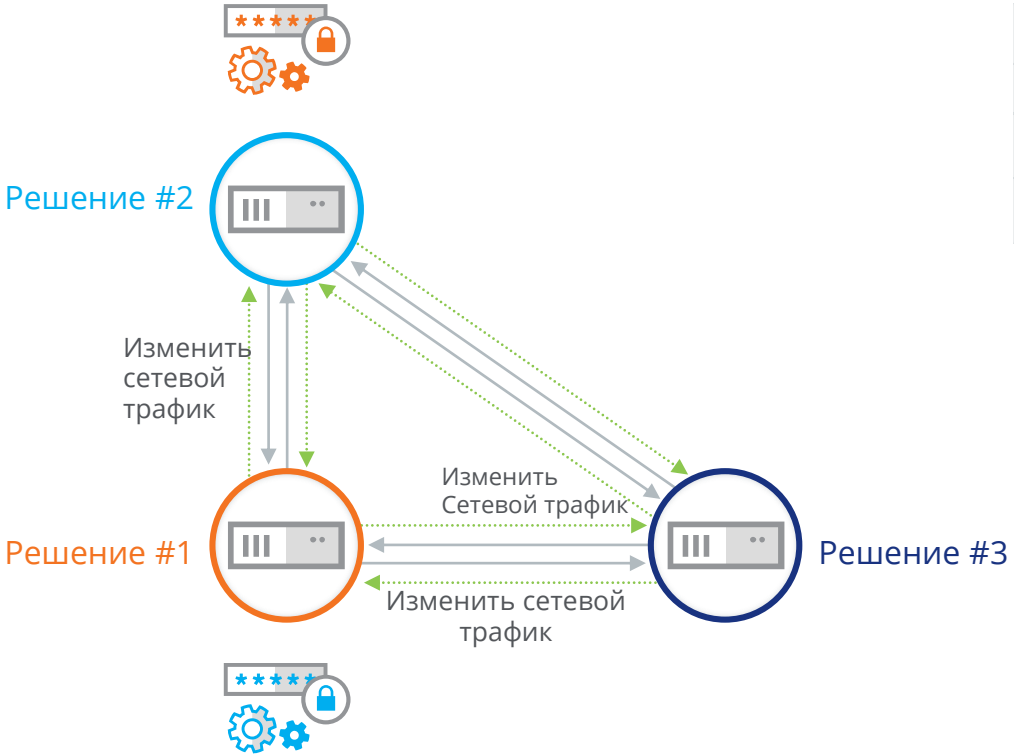
Для получения изменений, решения регулярно опрашивают друг друга



X	Обмен учётными данными
X	Интеграция на уровне API
X	Регулирование сети для портов и протоколов
X	Опрос изменение (simulate real-time events)

Интеграция решений до DXL

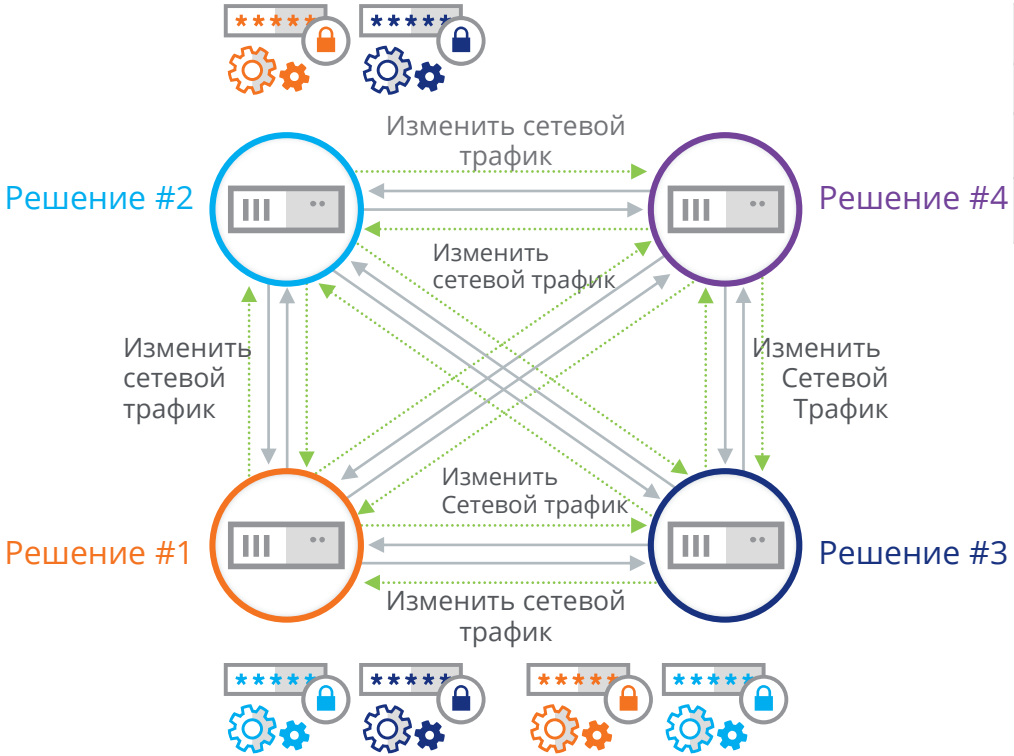
Сложность взаимодействий увеличивается с каждым новым решением



X	Обмен учётными данными
X	Интеграция на уровне API
X	Регулирование сети для портов и протоколов
X	Опрос изменение (simulate real-time events)

Интеграция решений до DXL

По-моему этим
очень сложно
управлять



X	Обмен учётными данными
X	Интеграция на уровне API
X	Регулирование сети для портов и протоколов
X	Опрос изменение (simulate real-time events)

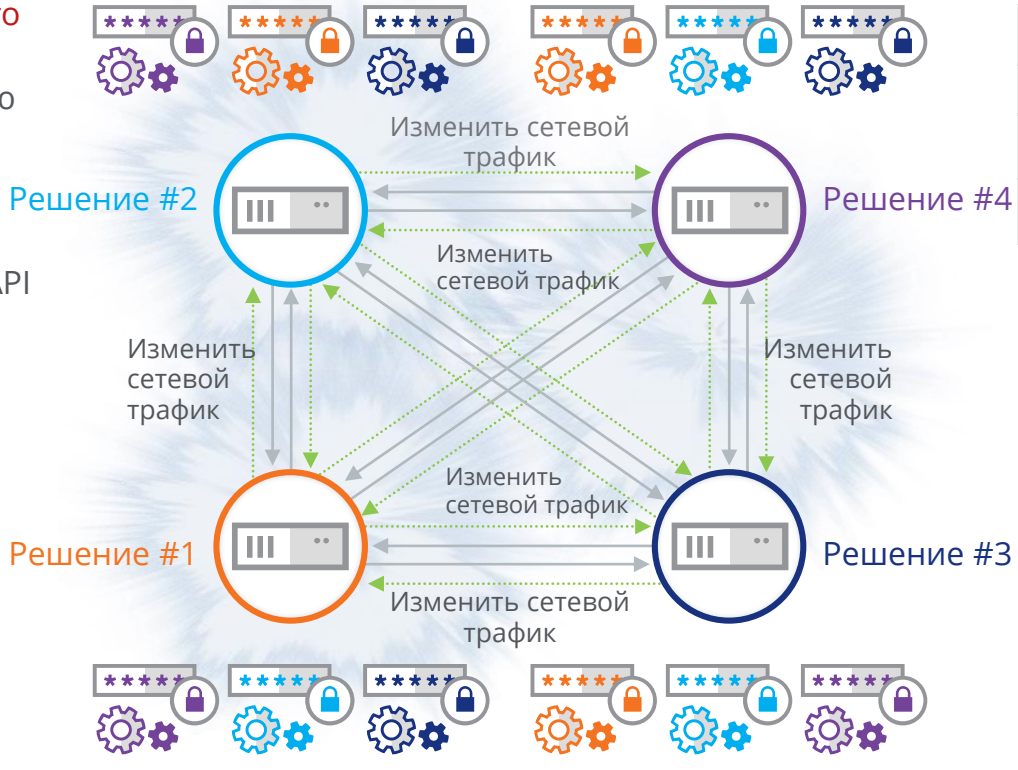
Credentials

API

Интеграция решений до DXL

Затрачено очень много времени и усилий чтобы построить такую сложную систему из нескольких решений.

Когда в одном из продуктов изменитсяAPI (что бывает), всё сломалось начинаем сначала!



X	Обмен учётными данными
X	Интеграция на уровне API
X	Регулирование сети для портов и протоколов
X	Опрос изменение (simulate real-time events)

Credentials

API

McAfee
Together is power.

OpenDXL – возможности интеграционной шины

DXL – Data eXchange Layer

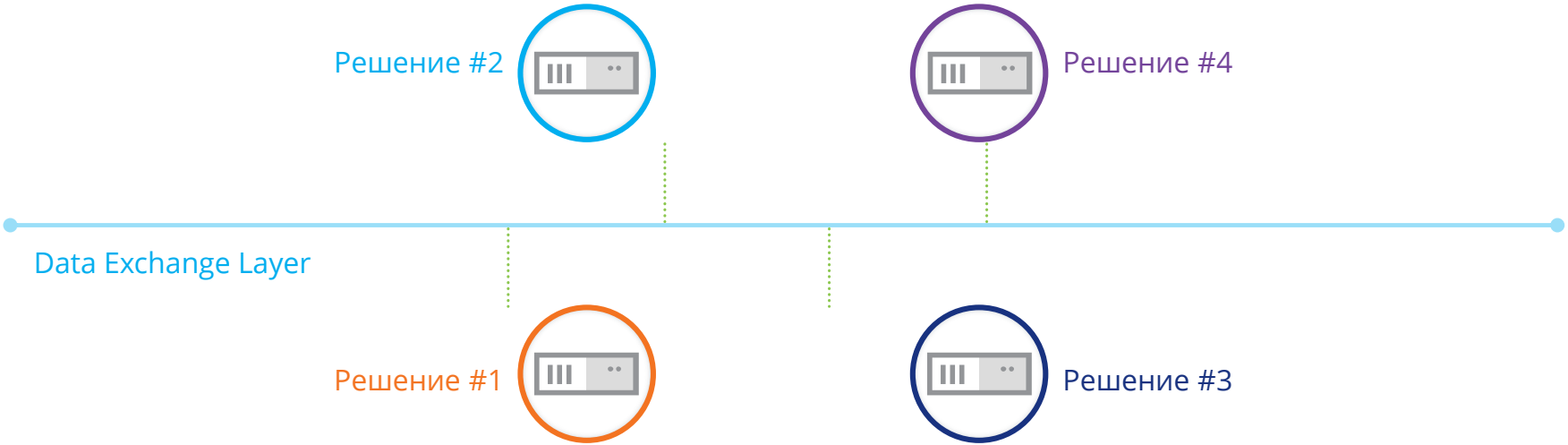
Человек живёт для того, чтобы научиться петь от любви.

Бхакти Вигьяна Госвами

DXL упрощает взаимосвязь

✓ Взаимодействие в рамках единой структуры и протокола

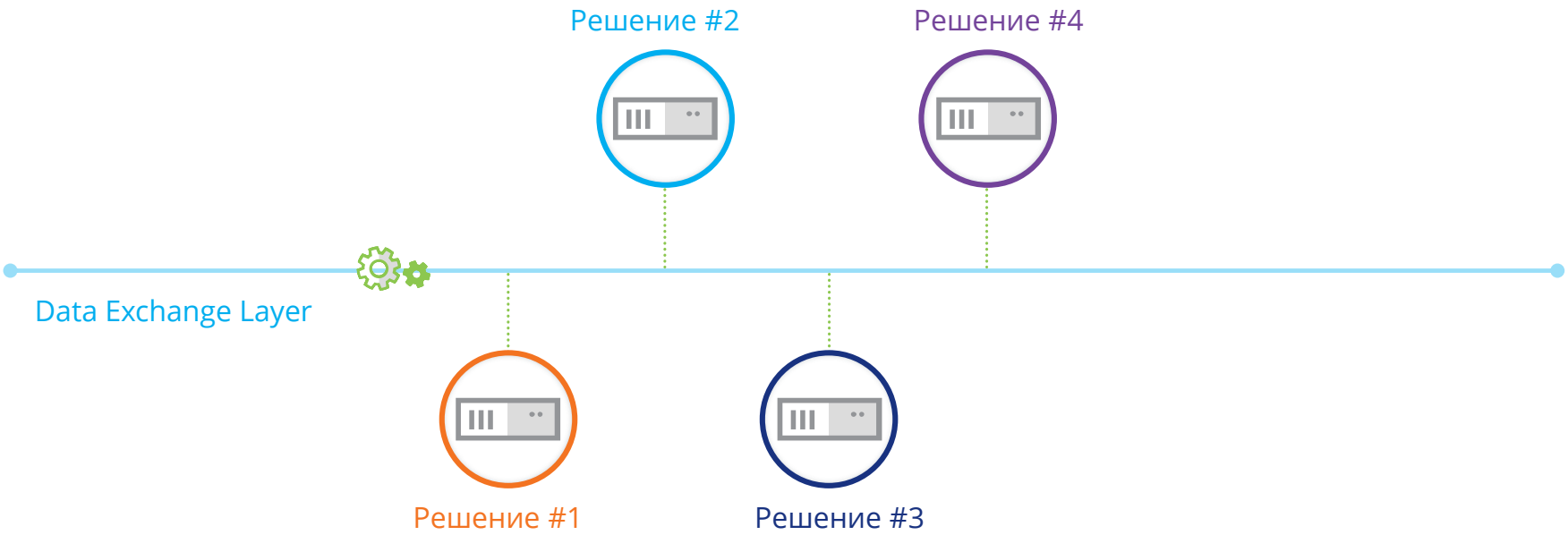
Взаимодействие в рамках единой структуры и протокола



DXL упрощает взаимосвязь

✓	Взаимодействие в рамках единой структуры и протокола
✓	Единый API для всех компонентов (DXL API)

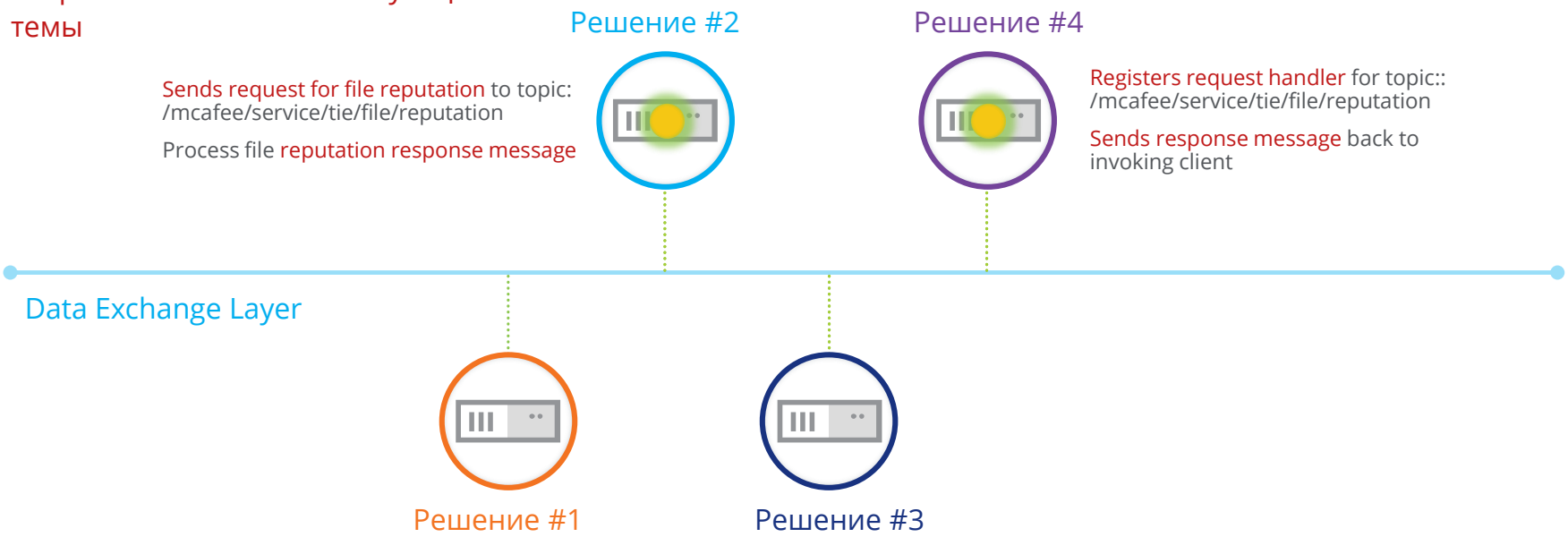
Простой в использовании, единый для всех компонентов API (DXL API)



DXL упрощает взаимосвязь

✓	Взаимодействие в рамках единой структуры и протокола
✓	Единый API для всех компонентов (DXL API)
✓	Multicast (topic-based) коммуникации

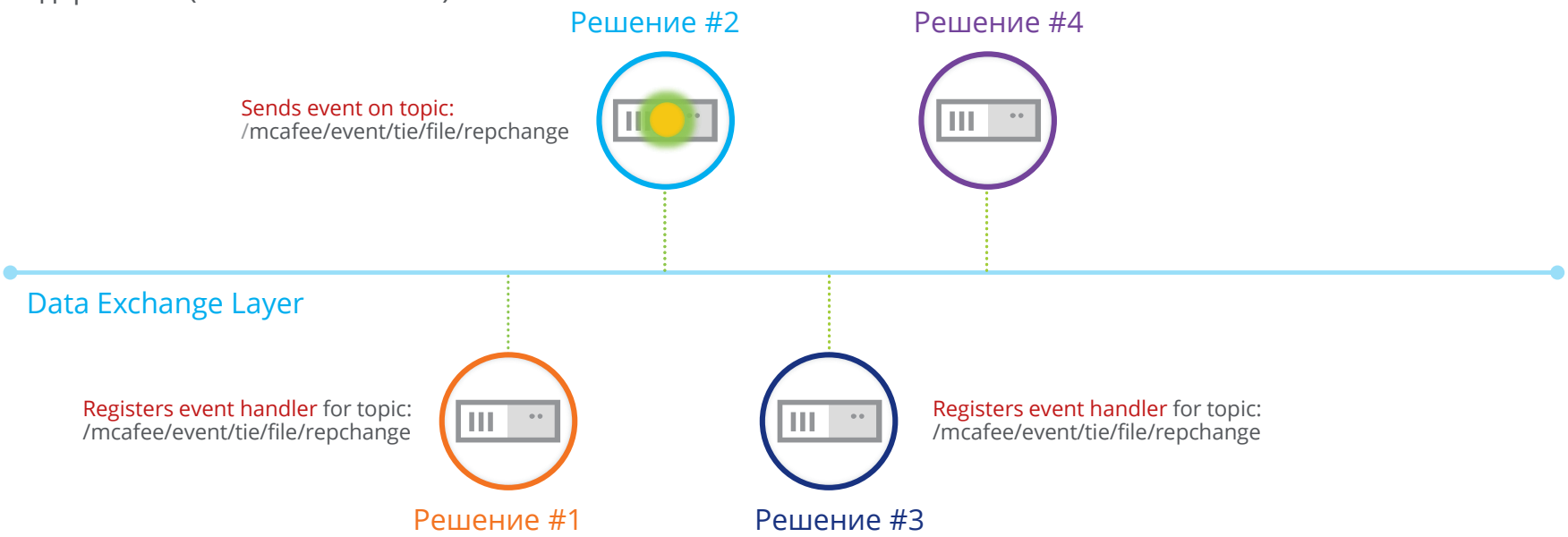
Коммуникация построена по принципу multicast, сообщения отправляются в соответствующие темы



DXL упрощает взаимосвязь

✓	Взаимодействие в рамках единой структуры и протокола
✓	Единый API для всех компонентов (DXL API)
✓	Multicast (topic-based) коммуникации
✓	Почти real-time (без опросная система)

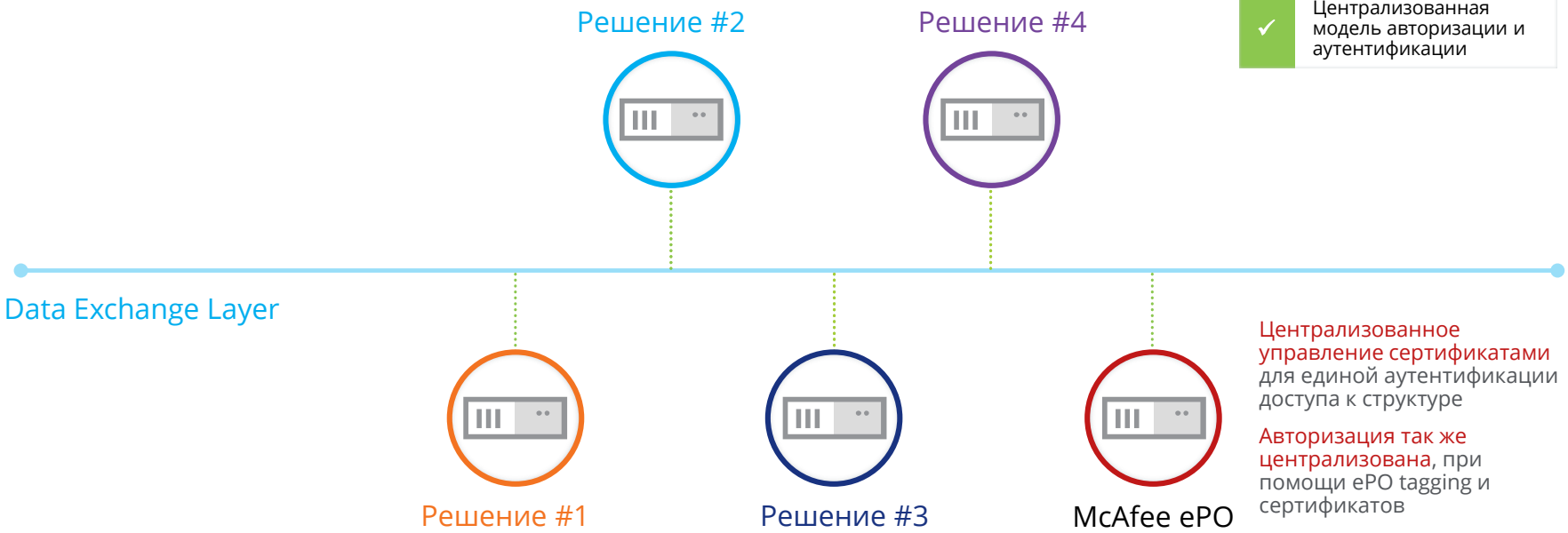
События доставляются ко всем подписчикам темы с минимальными задержками (почти мгновенно)



DXL упрощает взаимосвязь

Централизованная и единая модель аутентификации и авторизации

✓	Взаимодействие в рамках единой структуры и протокола
✓	Единый API для всех компонентов (DXL API)
✓	Multicast (topic-based) коммуникации
✓	Почти real-time (без опросная система)
✓	Централизованная модель авторизации и аутентификации



Централизованное управление сертификатами для единой аутентификации доступа к структуре

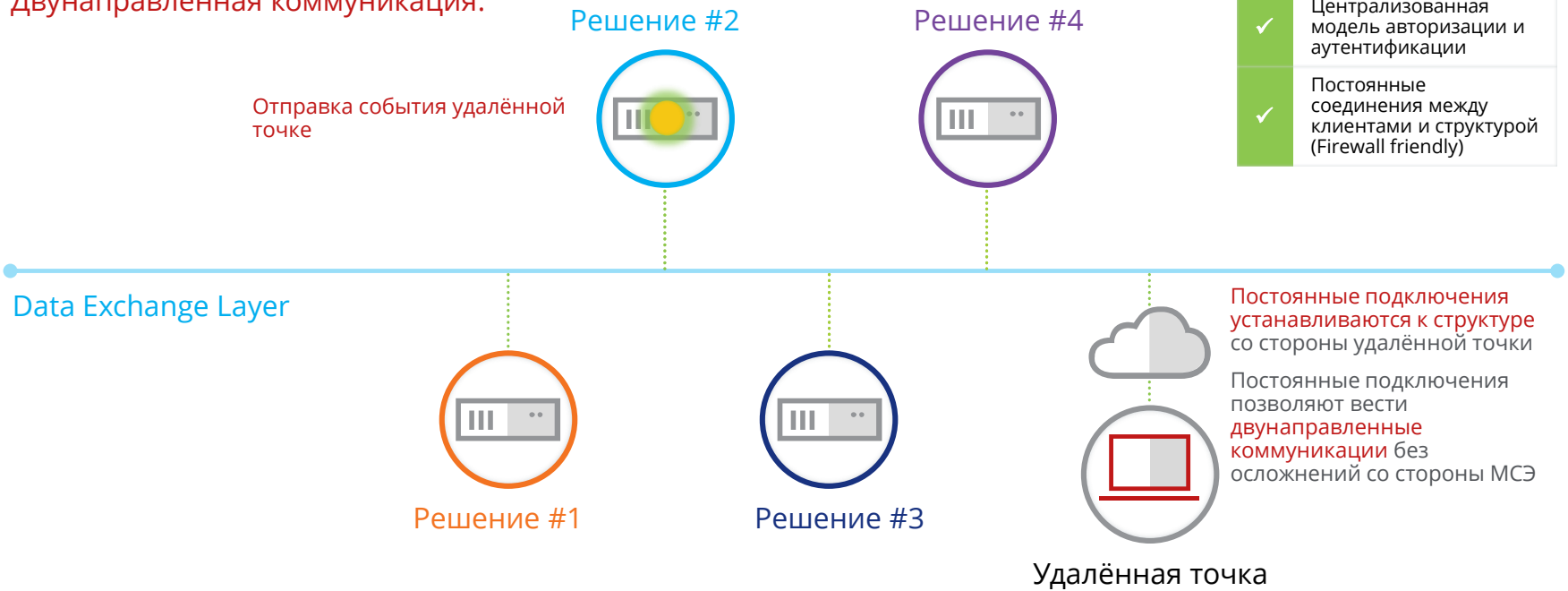
Авторизация так же централизована, при помощи ePO tagging и сертификатов

DXL упрощает взаимосвязь

Постоянные сетевые соединения (client-to-broker).

Двунаправленная коммуникация.

✓	Взаимодействие в рамках единой структуры и протокола
✓	Единый API для всех компонентов (DXL API)
✓	Multicast (topic-based) коммуникации
✓	Почти real-time (без опросная система)
✓	Централизованная модель авторизации и аутентификации
✓	Постоянные соединения между клиентами и структурой (Firewall friendly)



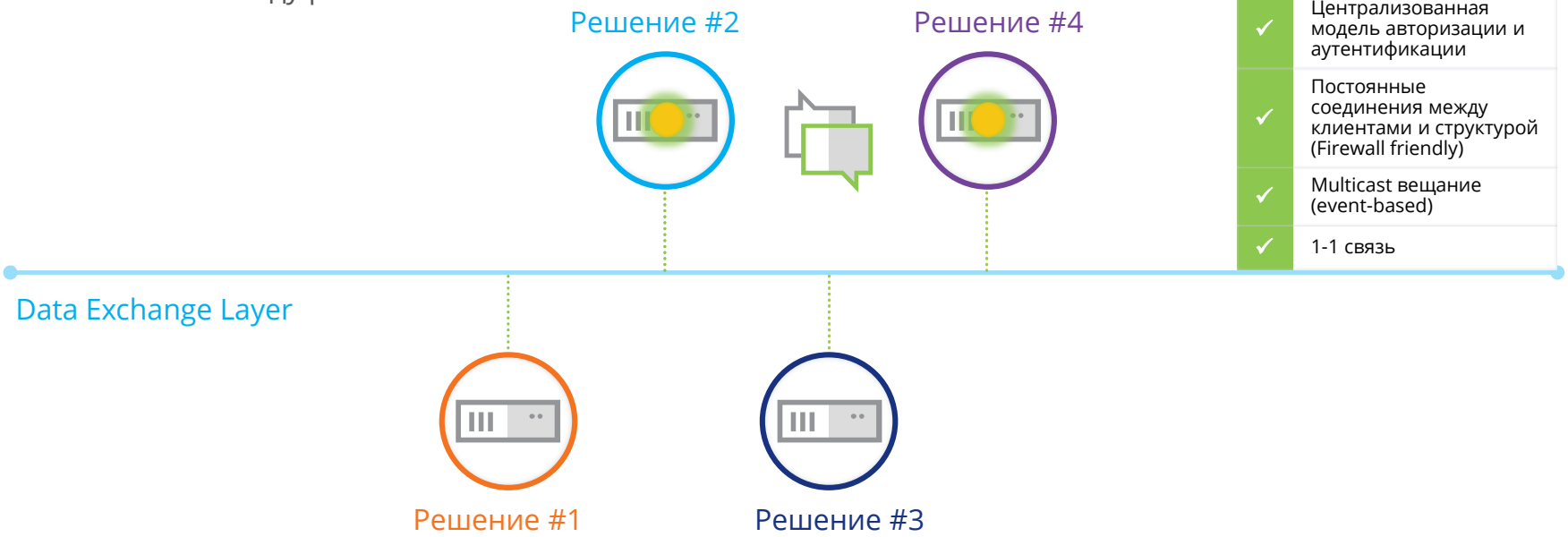
DXL упрощает взаимосвязь

Несколько режимов связи: Multicast event-based сообщения для всех подписчиков

✓	Взаимодействие в рамках единой структуры и протокола
✓	Единый API для всех компонентов (DXL API)
✓	Multicast (topic-based) коммуникации
✓	Почти real-time (без опросная система)
✓	Централизованная модель авторизации и аутентификации
✓	Постоянные соединения между клиентами и структурой (Firewall friendly)
✓	Multicast вещание (event-based)

DXL упрощает взаимосвязь

Multiple Communication modes:
Запрос – Ответ режим общения «точка-точка» между решениями



✓	Взаимодействие в рамках единой структуры и протокола
✓	Единый API для всех компонентов (DXL API)
✓	Multicast (topic-based) коммуникации
✓	Почти real-time (без опросная система)
✓	Централизованная модель авторизации и аутентификации
✓	Постоянные соединения между клиентами и структурой (Firewall friendly)
✓	Multicast вещание (event-based)
✓	1-1 связь

McAfee™
Together is power.

Пример использования шины DXL и скриптов openDXL

Помоги, помоги,
я солдат своей
любви..

A’Studio

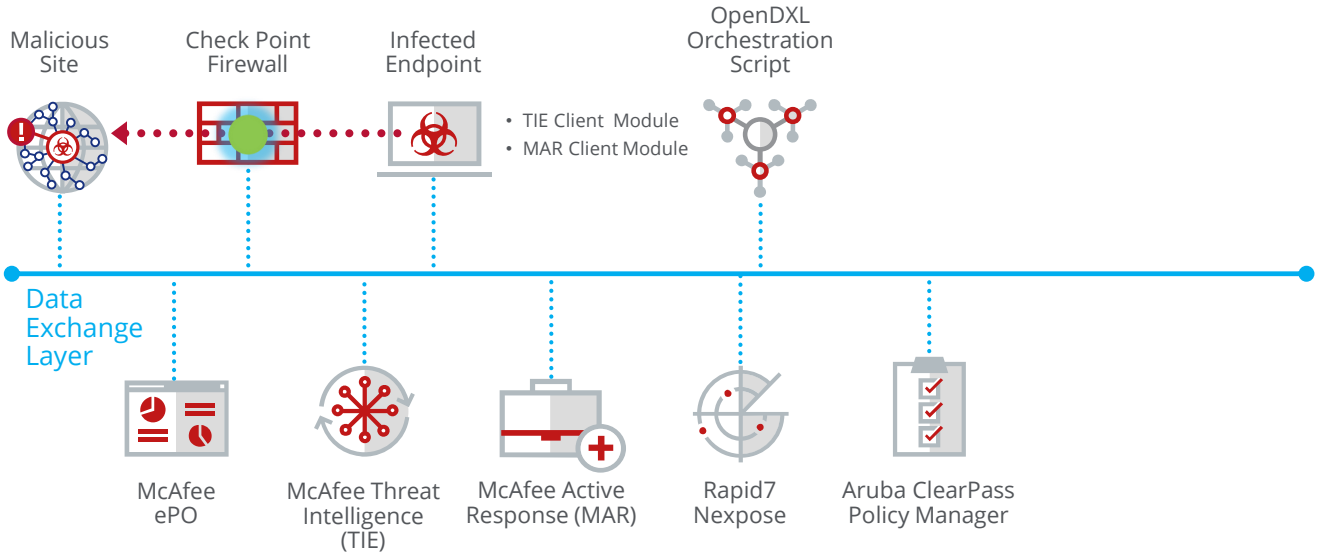
Пример – OpenDXL сценарий

Какие возможности даёт OpenDXL?

✓ Прослушивание событий от Check Point

Зловред инициирован на инфицированном APM, как следствие передача трафика на зловредный сайт

Событие получено OpenDXL хостом

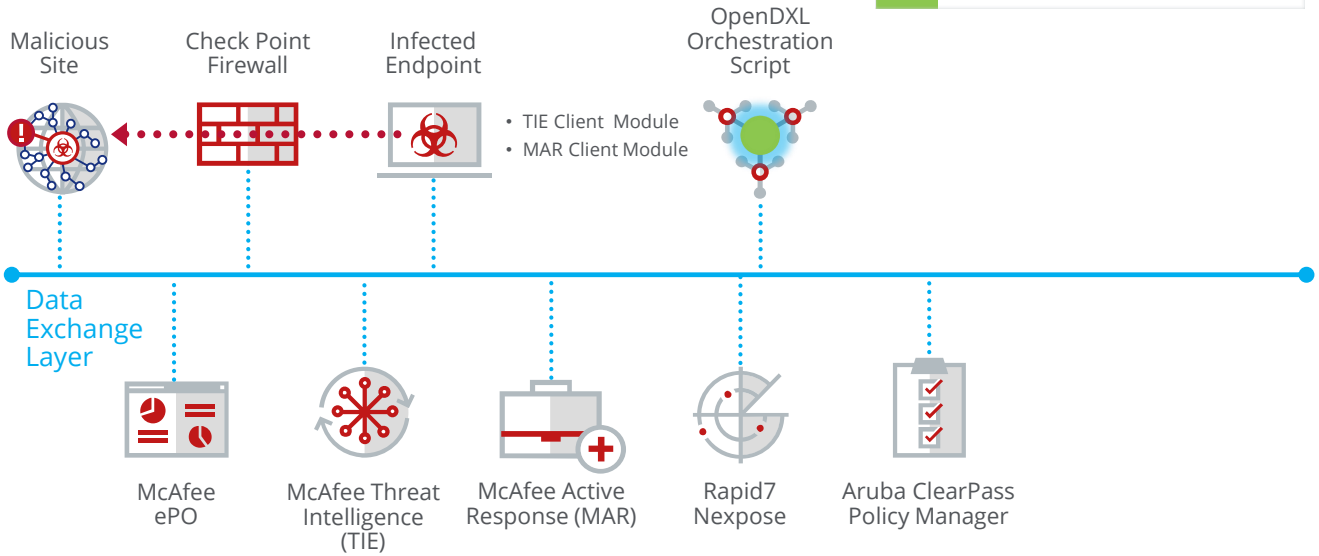


Пример – OpenDXL сценарий

Какие возможности даёт OpenDXL?

Скрип выполняет запрос через DXL к McAfee Active Response (MAR) для определения систем и процессов (хэш сумм) инициирующих подобные соединения

✓	Прослушивание событий от Check Point
✓	MAR для поиска процессов (по совпадению порта и адреса назначения)

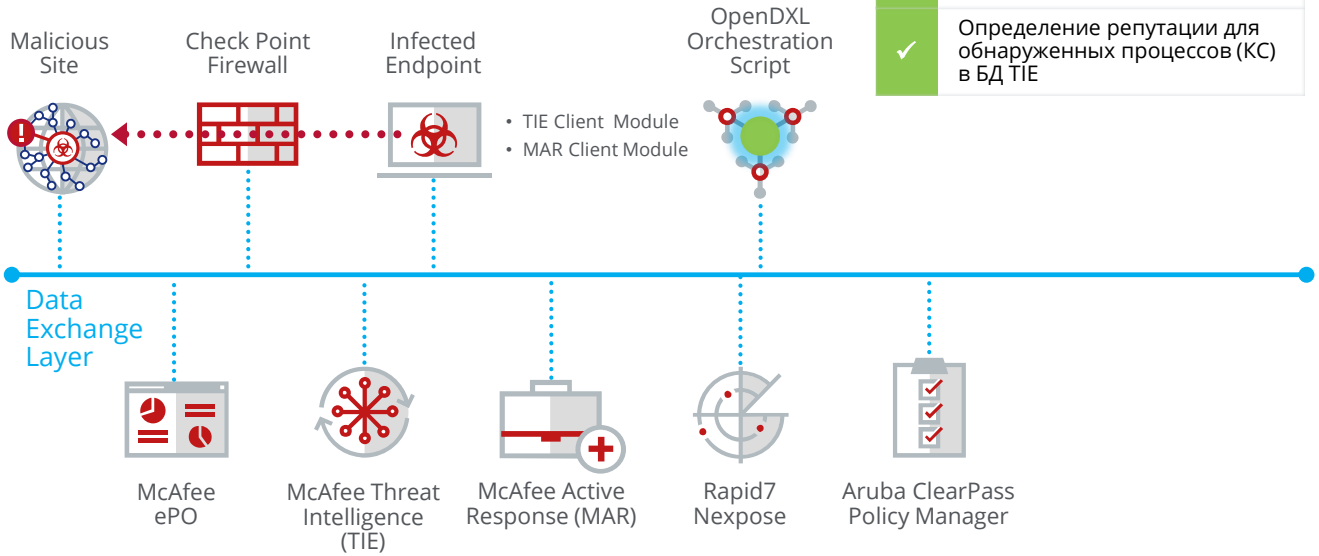


Пример – OpenDXL сценарий

Какие возможности даёт OpenDXL?

Скрипт определяет репутацию в McAfee Threat Intelligence (TIE) как Known Malicious через DXL

Применённая политика TIE приводит к инициализации процедуры уничтожения вредоноса и изоляции бинарных файлов

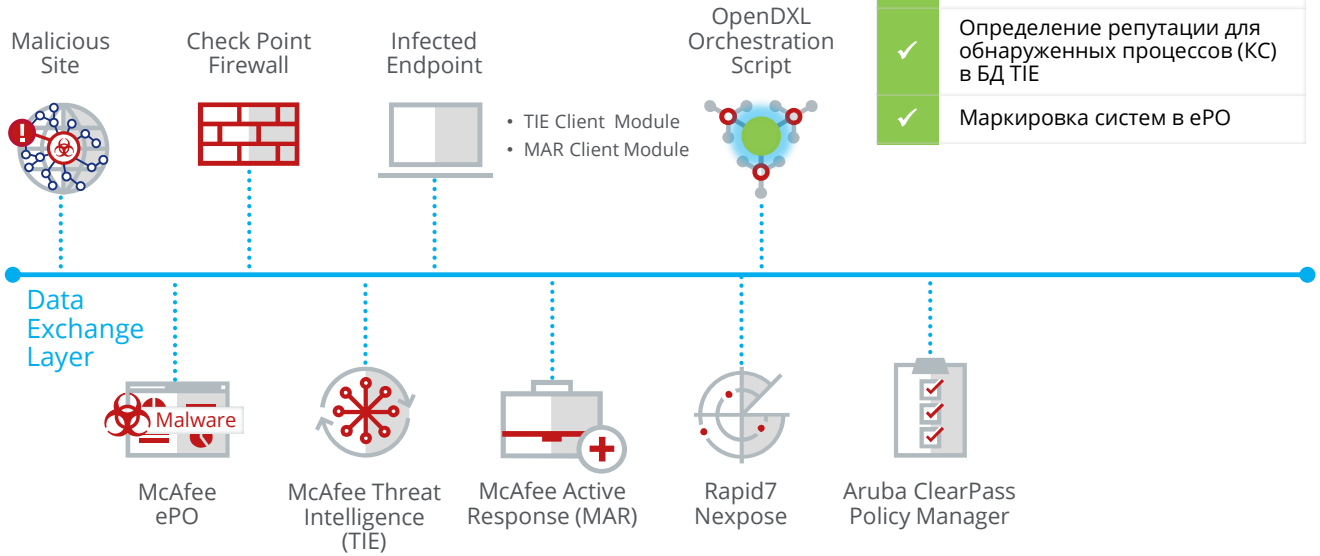


✓	Прослушивание событий от Check Point
✓	MAR для поиска процессов (по совпадению порта и адреса назначения)
✓	Определение репутации для обнаруженных процессов (KC) в БД TIE

Пример – OpenDXL сценарий

Какие возможности даёт OpenDXL?

Скрипт маркирует системы содержащие зловред в ePO через DXL

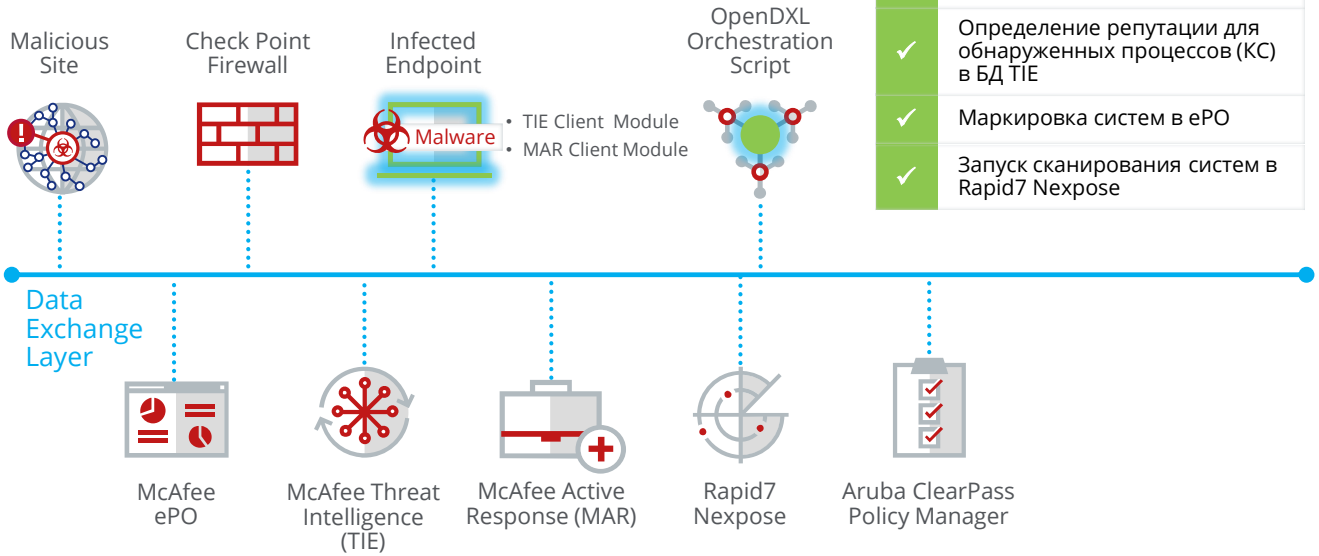


✓	Прослушивание событий от Check Point
✓	MAR для поиска процессов (по совпадению порта и адреса назначения)
✓	Определение репутации для обнаруженных процессов (KC) в БД TIE
✓	Маркировка систем в ePO

Пример – OpenDXL сценарий

Какие возможности даёт OpenDXL?

Скрипт отправляет запрос к DXL службе Rapid7 Nexpose для запуска сканирования систем содержащих зловред

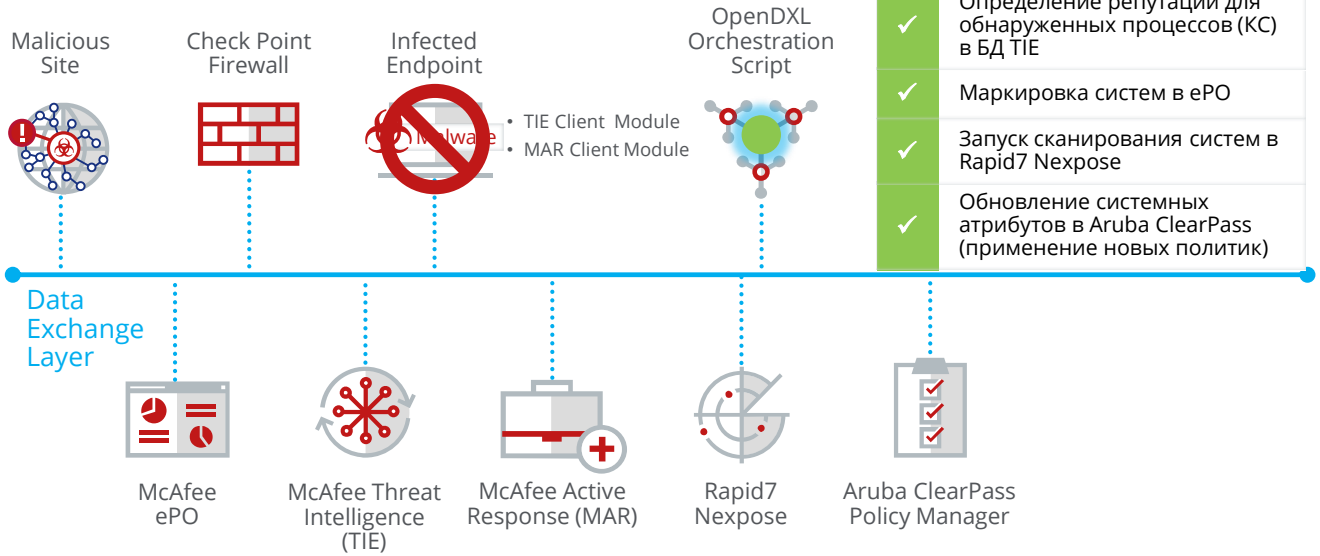


✓	Прослушивание событий от Check Point
✓	MAR для поиска процессов (по совпадению порта и адреса назначения)
✓	Определение репутации для обнаруженных процессов (KC) в БД TIE
✓	Маркировка систем в ePO
✓	Запуск сканирования систем в Rapid7 Nexpose

Пример – OpenDXL сценарий

Какие возможности даёт OpenDXL?

Скрипт отправляет запрос к службе DXL Aruba ClearPass для обновления системных атрибутов систем содержащих зловред с целью применения новых политик



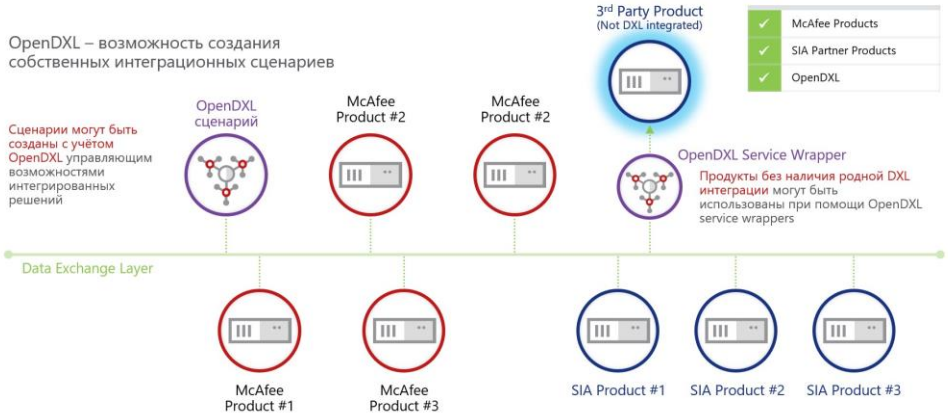
✓	Прослушивание событий от Check Point
✓	MAR для поиска процессов (по совпадению порта и адреса назначения)
✓	Определение репутации для обнаруженных процессов (КС) в БД TIE
✓	Маркировка систем в ePO
✓	Запуск сканирования систем в Rapid7 Nexpose
✓	Обновление системных атрибутов в Aruba ClearPass (применение новых политик)

Пример – OpenDXL сценарий

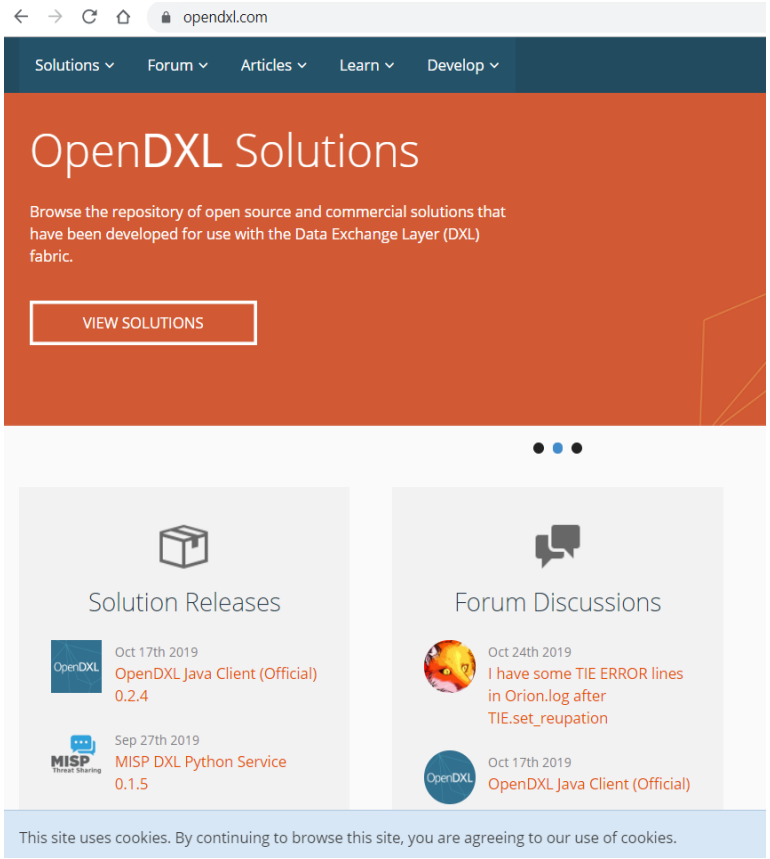
Какие возможности даёт OpenDXL?

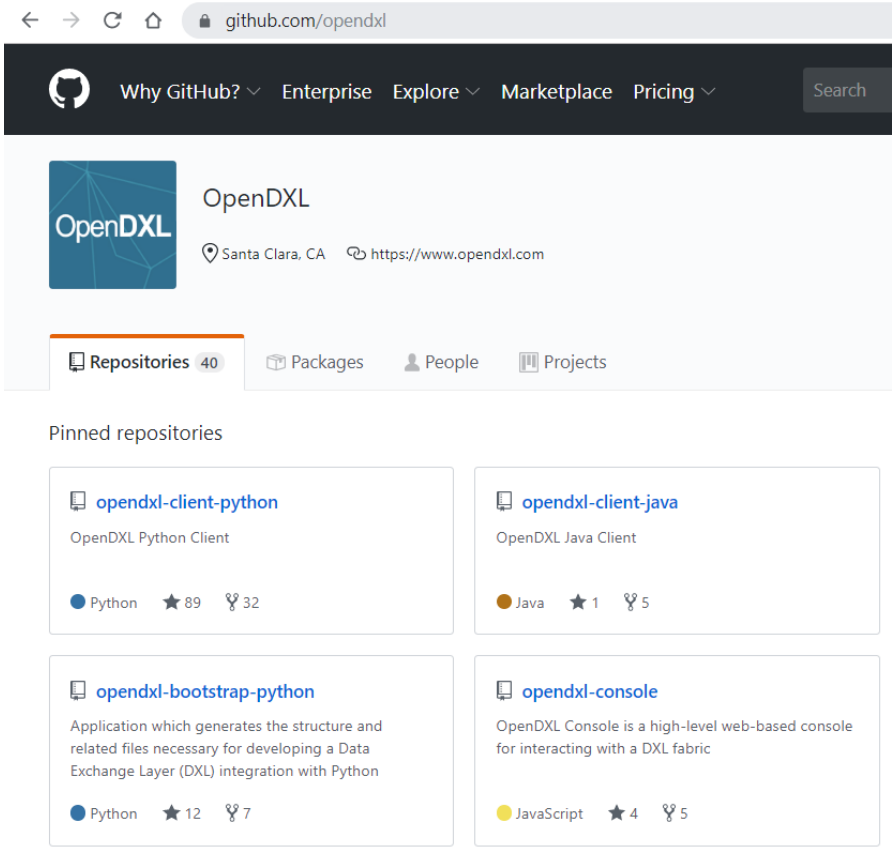
OpenDXL Python клиент был использован для:

- Скрипт оркестрации запускаемый через зарегистрированный DXL Event listener
- Скрипт оркестрации инициировал следующие службы DXL:
  - McAfee Active Response (MAR)
  - McAfee Threat Intelligence Exchange (TIE)
  - McAfee ePolicy Orchestator (ePO)
  - Rapid7 Nexpose
  - Aruba ClearPass
- DXL service wrapper использовался для вызова Rapid7 Nexpose API
- DXL service wrapper использовался для вызова Aruba ClearPass API



GitHub.com и OpenDXL.com



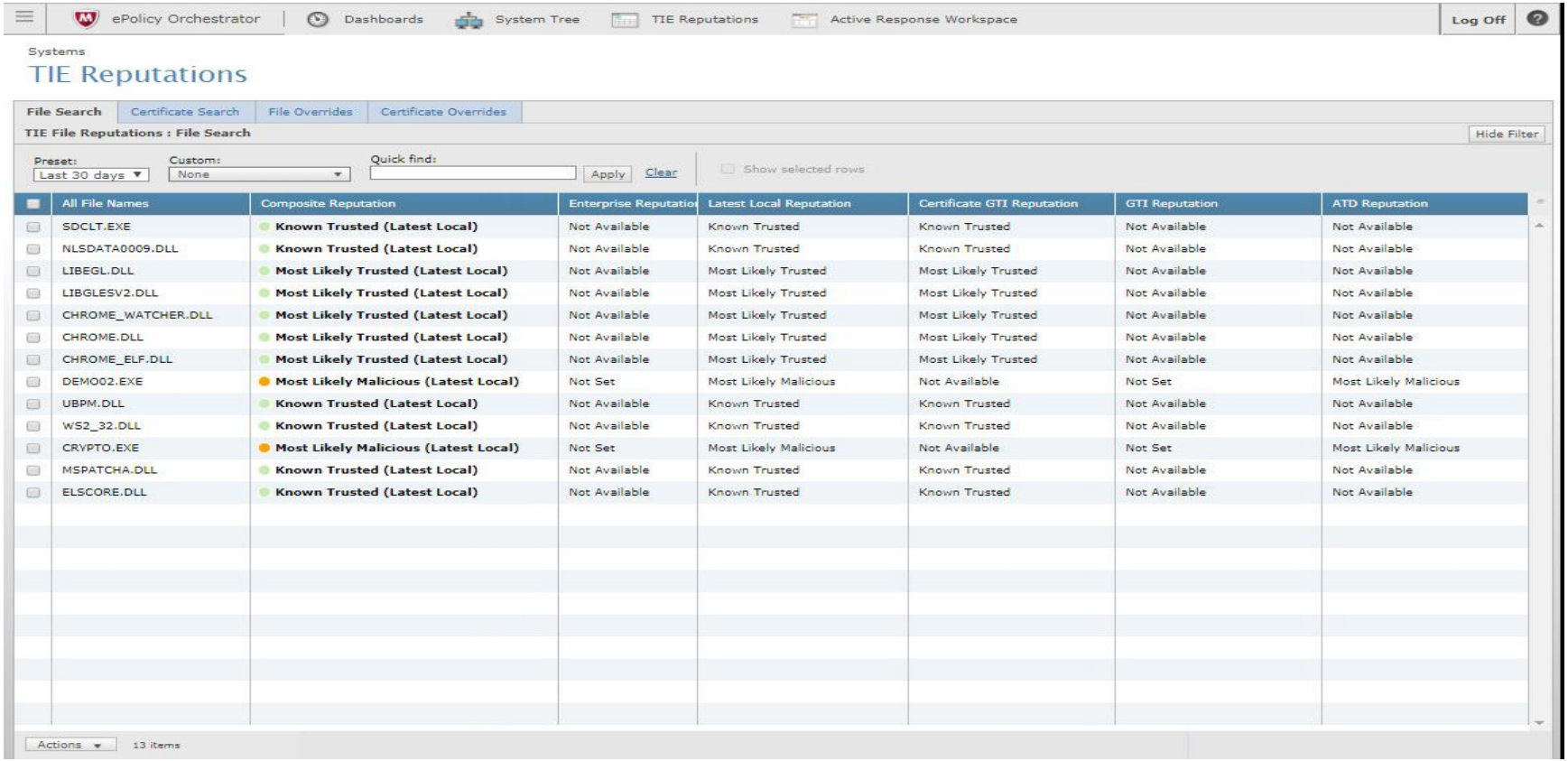


McAfee
Together is power.

McAfee Threat Intelligence Exchange (TIE)

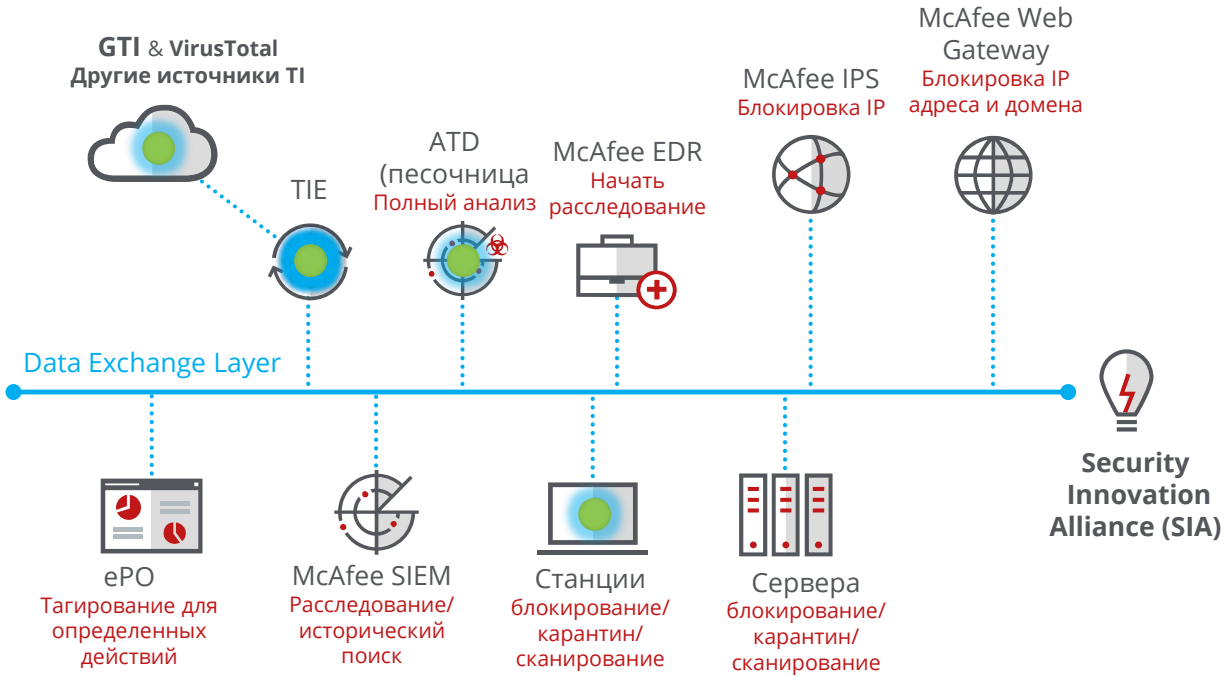
Локальное управление репутациями, IOC

McAfee Threat Intelligence Exchange



McAfee Adaptive Security Architecture

Постоянный обмен репутациями (IOC) по всей экосистеме



Примеры интеграции с openDXL

https://www.cisco.com/c/dam/m/en_us/products/security/technical-alliance-partners/core/assets/pxgrid-mcafee-opendxl-integration-aag.pdf

McAfee™
Together is power.

Адаптивная безопасность для корпораций и государства

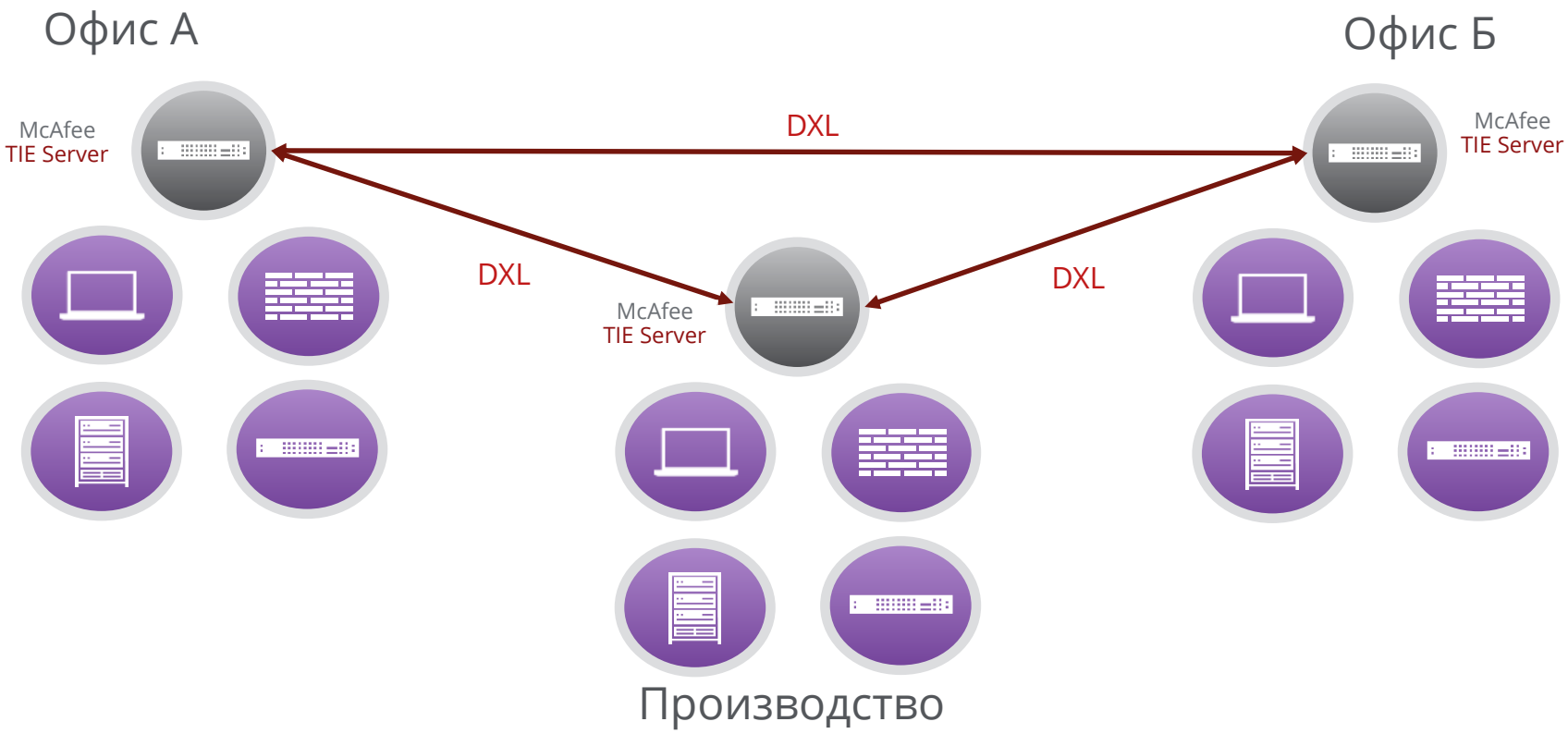
Современный подход

Любить — значит
истину защищать,
Даже восстав против
всей вселенной...

Эдуард Асадов

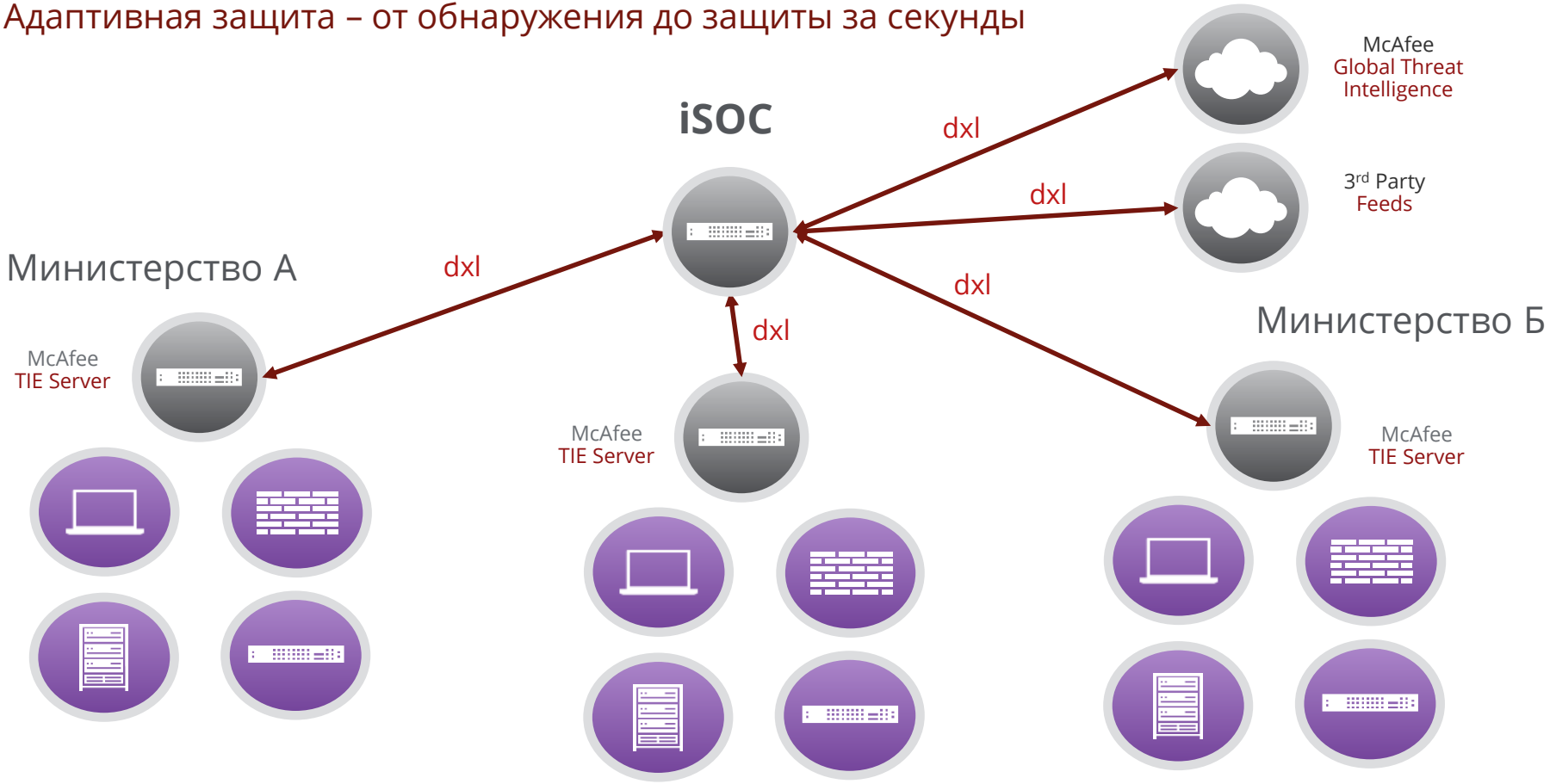
Защита корпорации

Адаптивная защита – от обнаружения до защиты за миллисекунды



Защита для всего государства

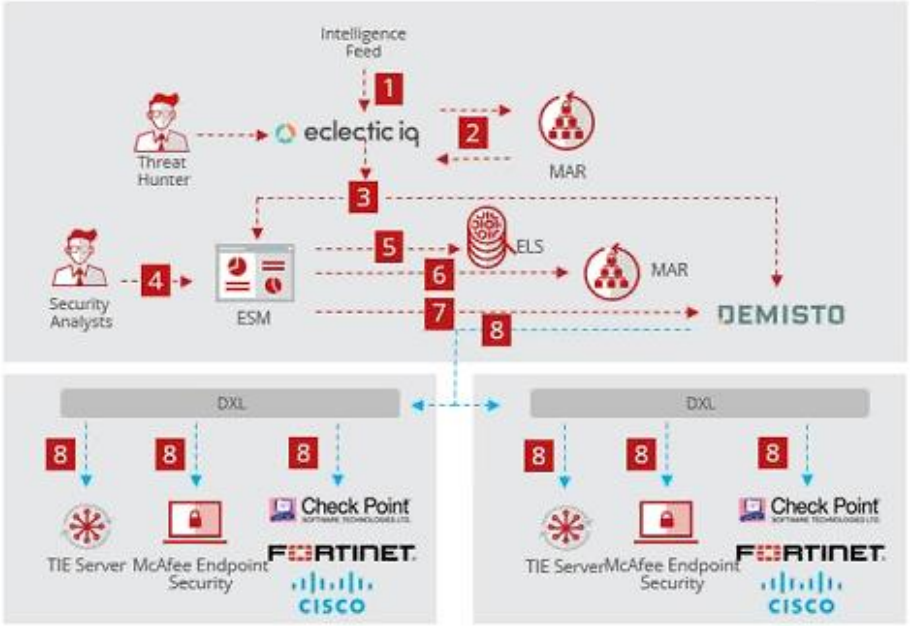
Адаптивная защита – от обнаружения до защиты за секунды



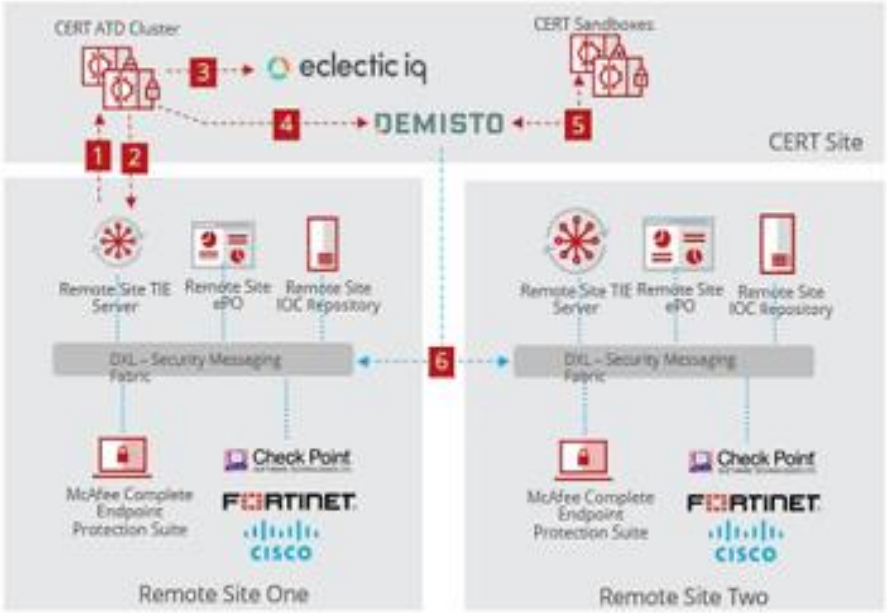
ПРИМЕРЫ АДАПТИВНОЙ АРХИТЕКТУРЫ С DXL

Адаптивная защита – от обнаружения до защиты за секунды

Организация защиты холдинга



Национальный CERT



Содержание:

- Адаптивная архитектура безопасности (Gartner)
- Как интегрировать решения разных производителей
- Анонс решений McAfee для ОЦИБ

McAfee
Together is power.

McAfee Enterprise Security Manager (ESM)

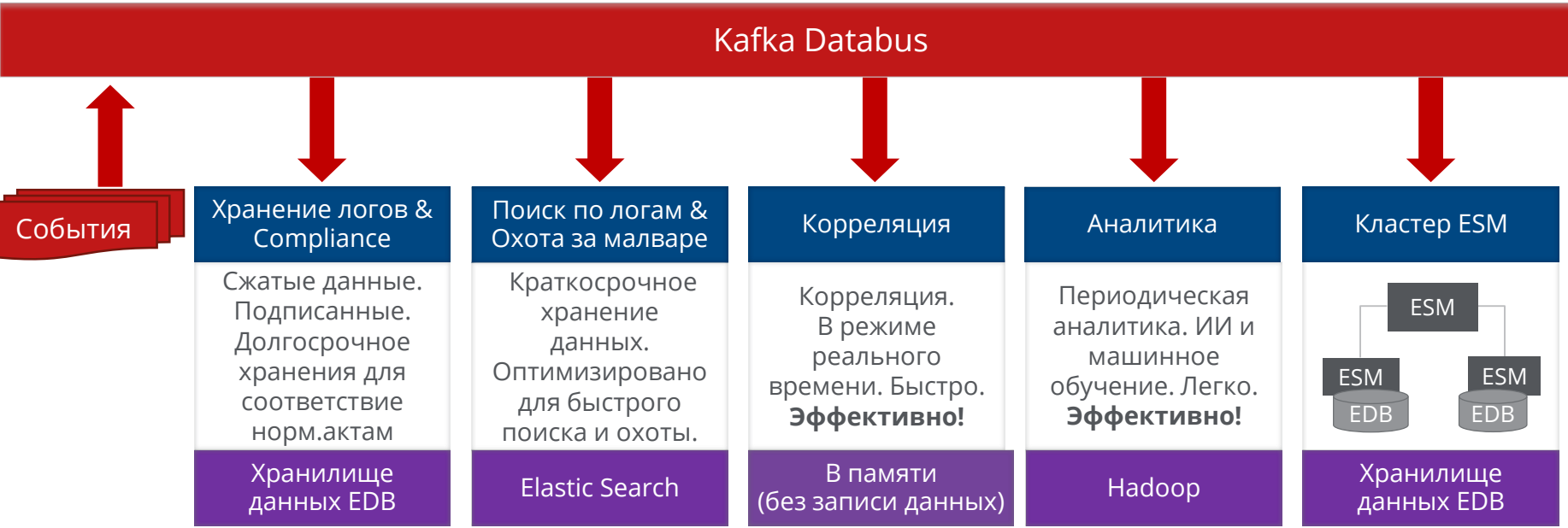
Высокопроизводительная SIEM платформа для построения интеллектуального SOC

8 лет в квадранте Лидеров Гартнер

- McAfee has implemented a modern SIEM architecture that leverages big data technologies, such as Kafka and Elasticsearch. The open nature of the data tier allows organizations looking to feed data into or out of ESM to have flexible options.
- User behavior capabilities are available through several options. In addition to basic user monitoring via a content pack for ESM, McAfee offers MBA as a UEBA/analytics offering, plus support for numerous third-party UEBA integrations.
- Application support is strong across databases, ERP solutions, OT and IoT, either leveraging native capabilities or enhanced through the use of its ADM and DAM solutions.
- MI (an add-on subscription product in the Security Operations product portfolio) provides guided incident investigation support for analysts, including context/evidence collection and recommended actions.

McAfee SIEM - Платформа для обработки Big Data –

ESM 11 = Никаких компромиссов. Высокая производительность. Низкая стоимость владения



McAfee
Together is power.

MVISION EDR

Мощный инструмент для расследования инцидентов ИБ

Я искал в этом городе женщину, ту единственную, свою...

Григорий Лепс

Рабочие станции и сервера генерируют большое количество данных

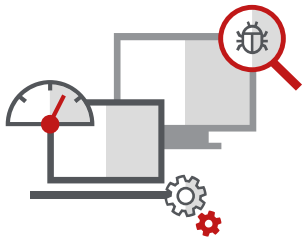
Сегодня, инструменты EDR требуют **высококвалифицированных аналитиков**

Почему?

- Множество данных - трудно «иголку в стогу сена»
- Множество оповещений и алертов
- Высокая квалификация специалистов – **обычно они в дефиците** – для расследования и интерпретирования алертов

Что такое MVISION EDR?

McAfee Active Response



Мониторинг рабочих станций и серверов, сбор данных

Детектирование подозрительного поведения

Быстрый поиск

Быстрый ответ

Улучшения

Простая облачная архитектура

Расширенный сбор данных и их обновление

MITRE ATT&CK™ методология расследования

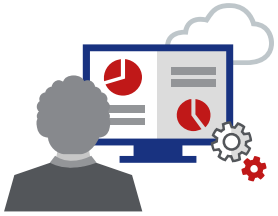
McAfee Investigator

Динамический гид по расследованиям

Автоматизированный анализ

Сбор данных по всей организации

MVISION EDR



Мощное средство для детектирования, расследований и ответной реакции – в простом виде

Обнаружение и устранение угроз – быстрее и проще

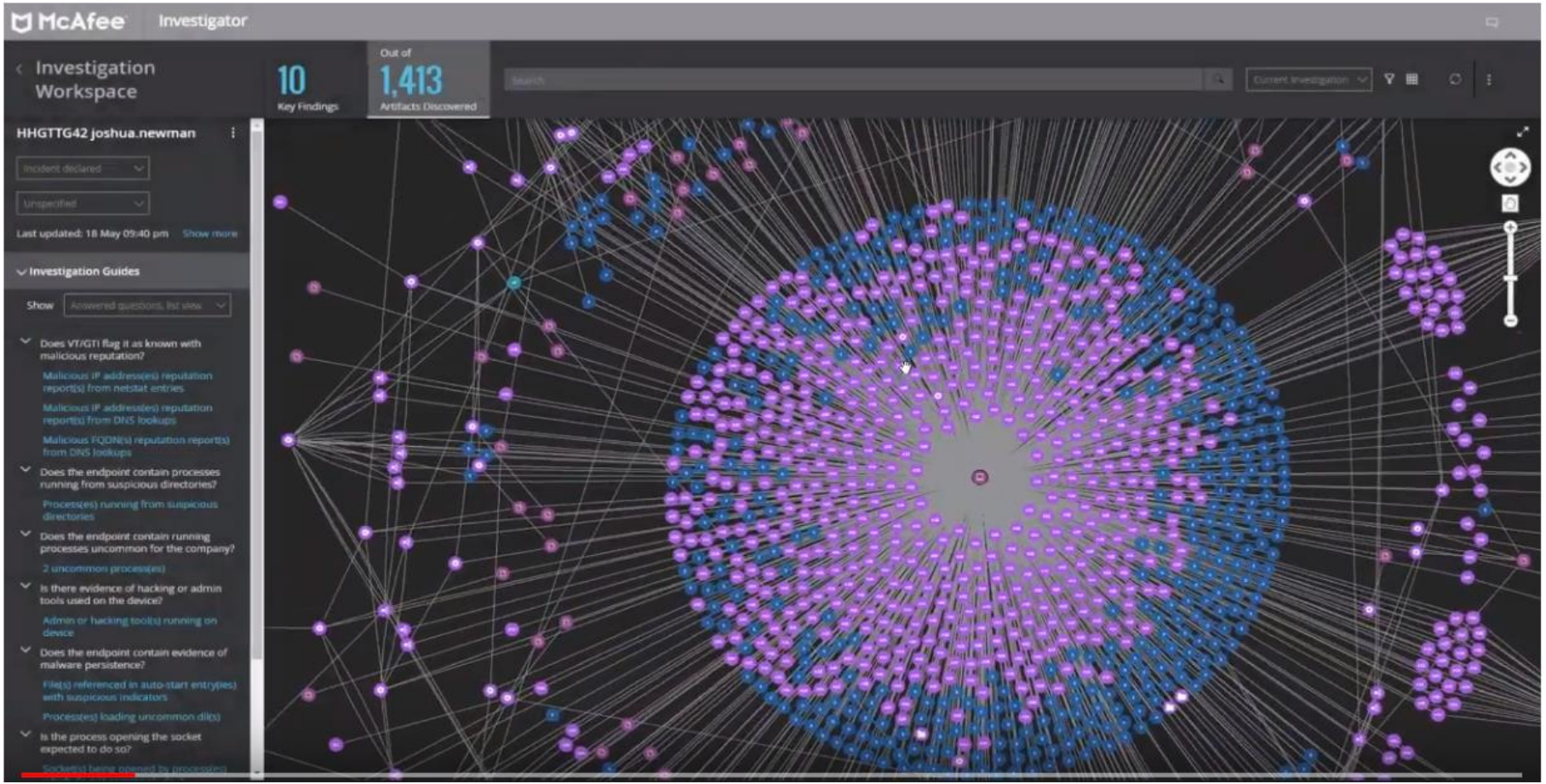
- Поведенческий анализ
- Файловые и безфайловые атаки
- Работает с любыми вендорами
- Быстрое внедрение новых аналитических алгоритмов

- Детектирование основанное на стандарте MITRE ATT&CK™
- Скоростной и постоянный процесс позволяющий определять фазу атаки, связанные с атакой риски и приоритет противодействий
- Расстановка приоритетов оповещений позволяет аналитикам понять степень риска и опасности
- Визуализация данных позволяет аналитикам быстро понять почему система выделила данное событие. Дальнейшее действие : игнорировать, ответное действие, *расследование*.

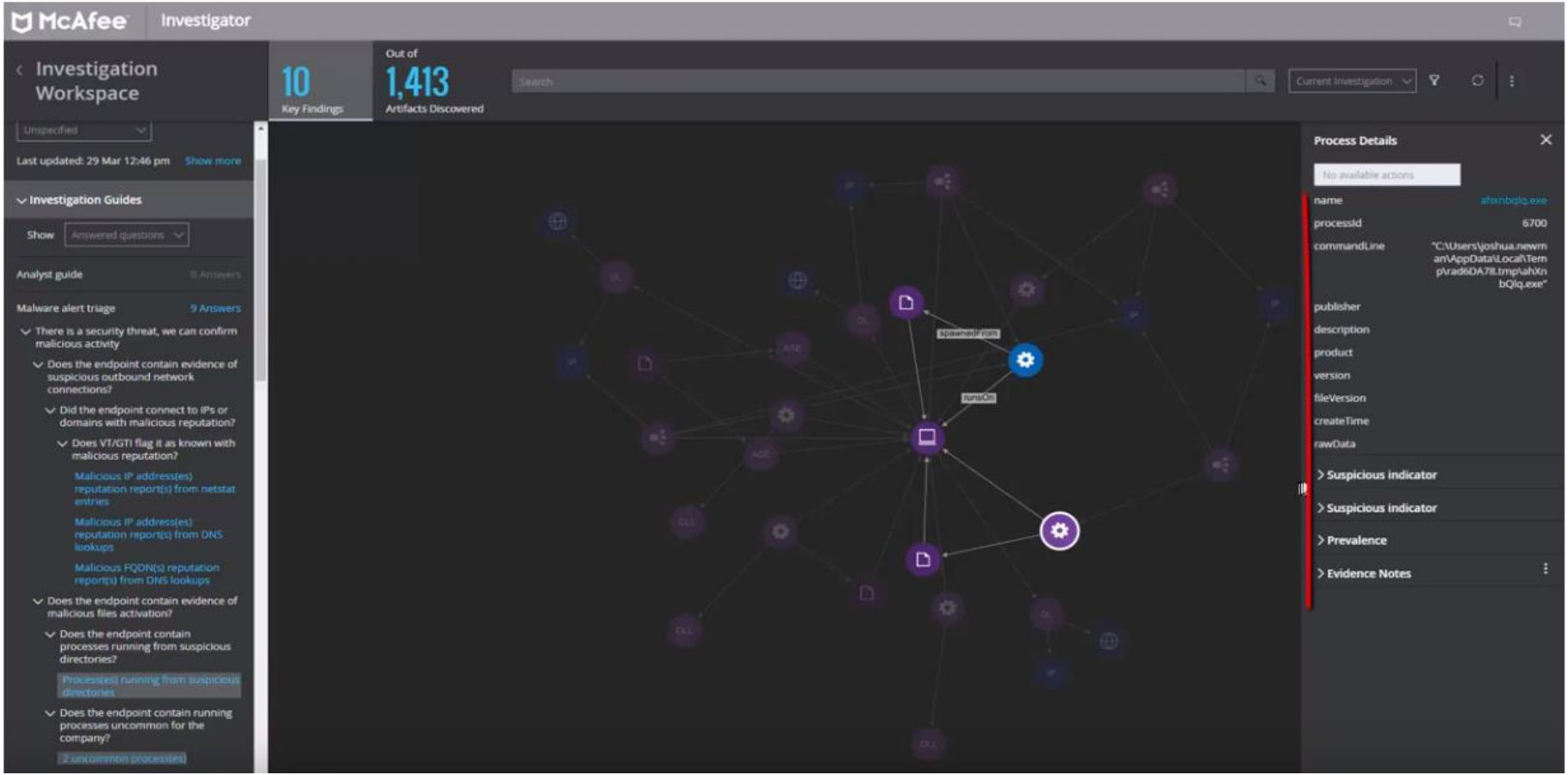
Новый подход McAfee к задачам EDR

Скоростное разрешение с высокой долей вероятности

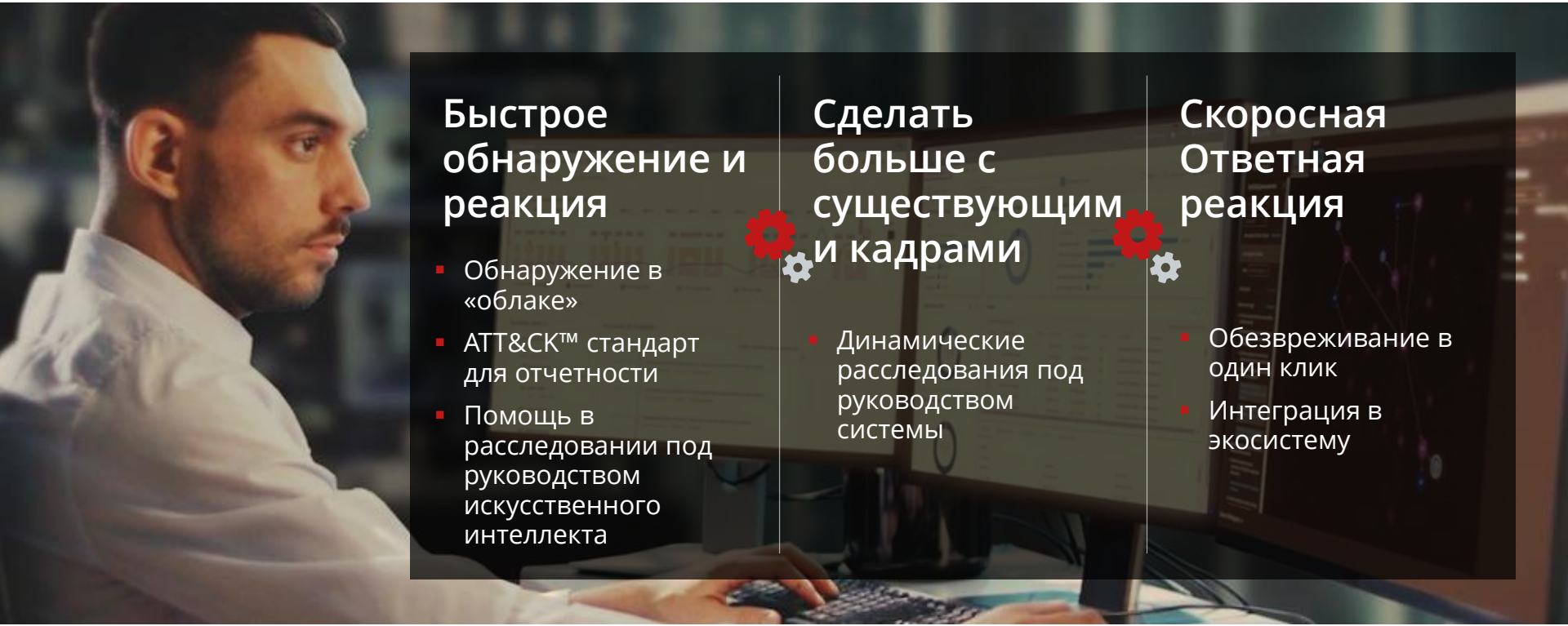
Панель расследования MVISION EDR



Панель расследования MVISION EDR



Change the Game with MVISION EDR



Быстрое обнаружение и реакция

- Обнаружение в «облаке»
- ATT&CK™ стандарт для отчетности
- Помощь в расследовании под руководством искусственного интеллекта

Сделать больше с существующим и кадрами

- Динамические расследования под руководством системы

Скоросная Ответная реакция

- Обезвреживание в один клик
- Интеграция в экосистему

McAfee
Together is power.

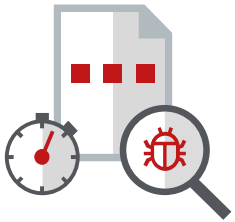
McAfee Advance Threat Defense

Обнаружение сложных целенаправленных атак

McAfee Advanced Threat Defense Advanced Analysis

Песочница + Глубокий анализ вредоносных программ

Стандартные средства

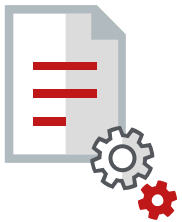


Использование **сигнатур**, **репутаций**, **эмуляций**— для быстрого выявление известных атак и вредоносных файлов.

Анализ большего числа файлов.

Быстрые результаты

Динамический анализ



Запуск файла в “**защищенной**” и **контролируемой** среде.

Наблюдение за исполнением программы файла и поиск вредоносного **поведения.**

Статический Анализ кода (Искусственный интеллект)

Убрать «шелуху» и **найти** выполняемый код.

Анализ **ВСЕХ** атрибутов и инструкций для выявление действий вредоносного кода.

Нахождение к какому **семейству вредоносного кода** относиться файл

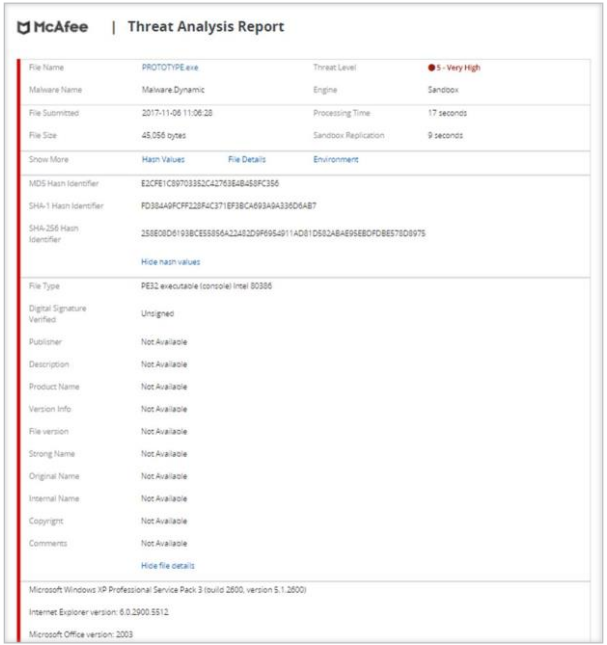
Нейронные сети (Машинное обучение)

Обнаружение шаблонов кода скрытых угроз.

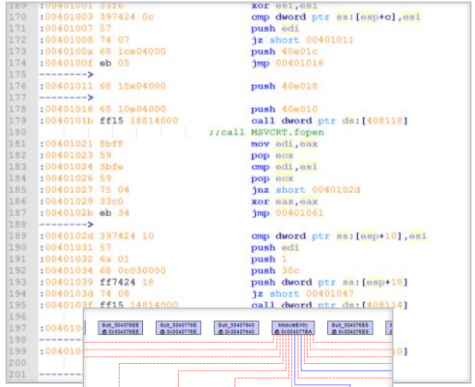
Анализ **типичного поведения** вредоносных программ.

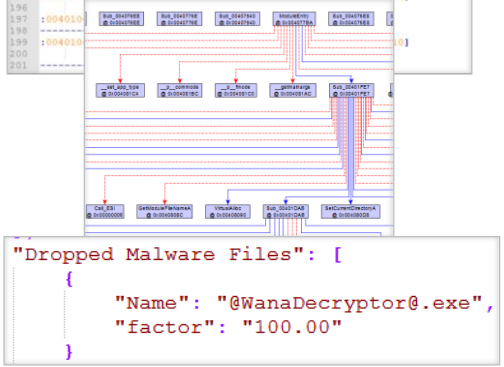
Детализированные отчеты и выдача их в стандартизированном виде

Threat Analysis Report



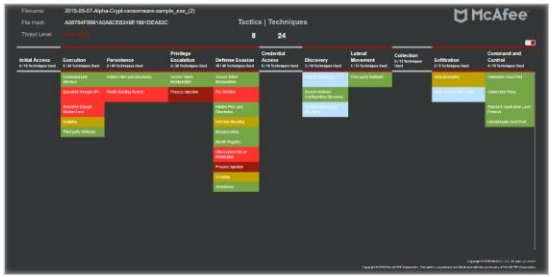
Assembly Code, Graph Analysis, and Indicators of Compromise





```
"Dropped Malware Files": [
    {
        "Name": "@WanaDecryptor@.exe",
        "factor": "100.00"
    }
```

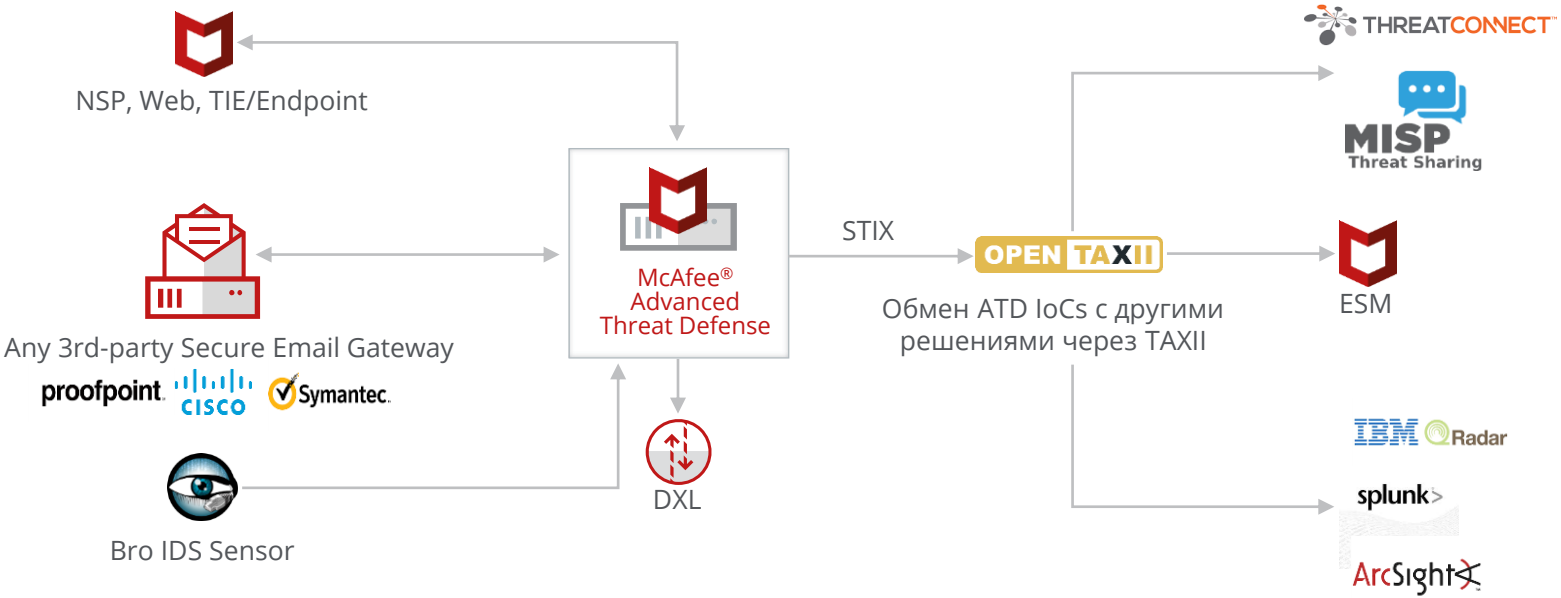
MITRE ATT&CK™ mapping



Threat Timeline

Открытая платформа, интеграция с другими решениями ИБ

Автоматизация действий по защите и детектированию и интеграция через открытую платформу



All you need is
All you need is
All you need is
LOVE is all you need!

John Lennon

Бренд McAfee

Мы верим в то, что ни один человек, продукт или организация не может защитить цифровой мир в одиночку.

Поэтому мы переделали McAfee беря во внимание совместную работу: Люди работают вместе. Решения работают вместе. Организации работают вместе.

Наша цель – вдохновить на совместную работу наших клиентов, партнеров, и даже конкурентов – сделав этот мир более защищенным.

McAfee. Together is power.
Вместе - сила.

McAfee. The device-to-cloud cybersecurity company.

Мы работаем для Вашего успеха и всегда готовы помочь и предоставить консультации по вопросам информационной безопасности!
Будем рады Вашим запросам!

Наши контакты:

Руслан Барбашин, McAfee
Территориальный менеджер
+7 727 350 5498
Ruslans_Barbasins@mcafee.com

Присоединяйтесь в соц.сетях:
www.facebook.com/ruslans.barbasins
www.linkedin.com/in/ruslansbarbasins/

Кирилл Креккер, Монт
McAfee Product Manager

Mobile: +7(702) 216-05-90;
Office: +7(727) 355-60-05, int. 161
kkrekker@mont.com