JUNIPER NETWORKS CONNECTED SECURITY

Эшелонированная, автоматизированная и интеллектуальная архитектура

Павел Живов

системный инженер, pzhivov@juniper.net

JUNIPER NETWORKS | Summit

ЛАНДШАФТ УГРОЗ ПРОДОЛЖАЕТ ДИВЕРСИФИЦИРОВАТЬСЯ

ОБЛАКА ЗАХВАТЫВАЮТ МИР

50 % Workloads IaaS в облаках к 2020 году
(Gartner)

ЗАТРАТЫ НА ПРОТИВОДЕЙСТВИЕ УГРОЗАМ РАСТУТ

$8 миллиардов
будет потрачено на борьбу с киберпреступностью к 2022
(Исследование Juniper Networks)

ПРОБЛЕМА №1 ПРОВАЛОВ СТРАТЕГИЙ ИБ

3 миллионов
нехватка профессионалов по ИБ по всему миру
(ISC²)

IoT РАСШИРЯЕТ ПЛОЩАДЬ АТАК

75.4 миллиардов
подключенных устройств к 2025
(Statista)

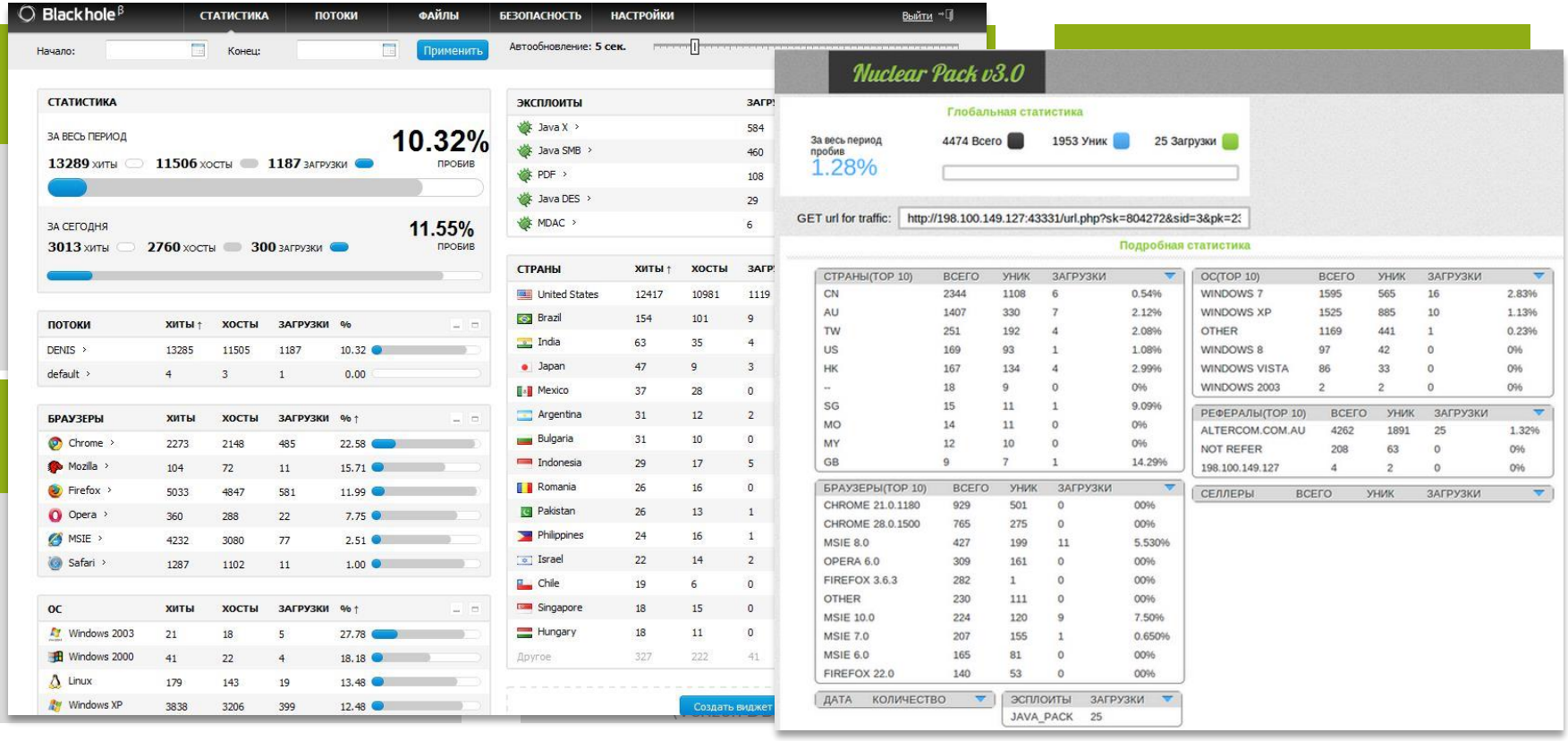
УГРОЗЫ СТАНОВЯТСЯ БОЛЕЕ ИЗОЩРЕННЫМИ

68 %
атак остаются необнаруженными месяцами и даже дольше
(Verizon DBIR 2018)

КИБЕРПРЕСТУПЛЕНИЯ – ЭТО УЖЕ ИНДУСТРИЯ

76 %
атак мотивированы финансово
(Verizon DBIR 2018)

ЛАНДШАФТ УГРОЗ ПРОДОЛЖАЕТ ДИВЕРСИФИЦИРОВАТЬСЯ

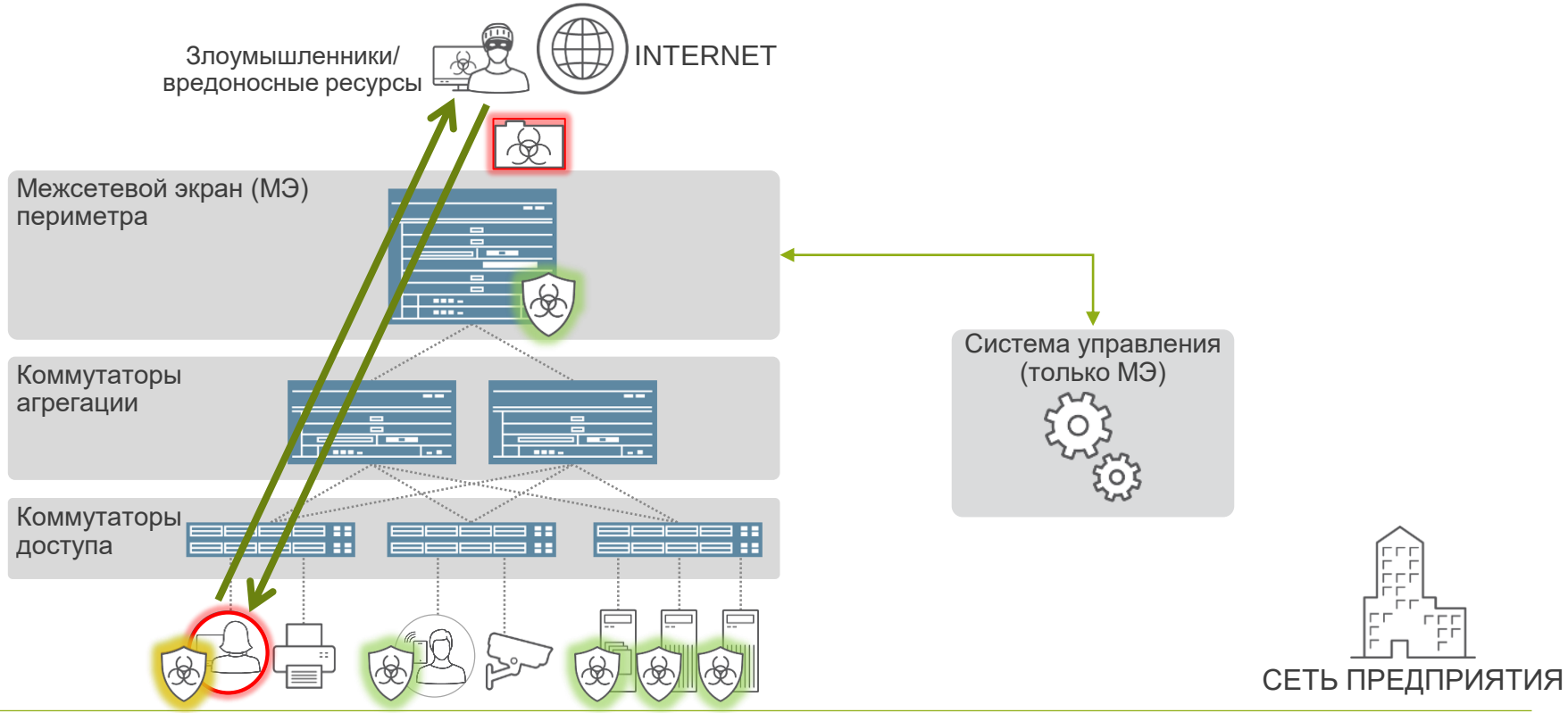


БЕСФАЙЛОВЫЕ АТАКИ

- Poweliks, PhaseBot
- Duqu 2.0, Kovter
- Powersniff, PowerWare, August
- PoshSpy
- Operation Cobalt Kitty
- Ramnit банковский Trojan
- Ursnif Variant
- Sodinokibi

и прочие, прочие, прочие

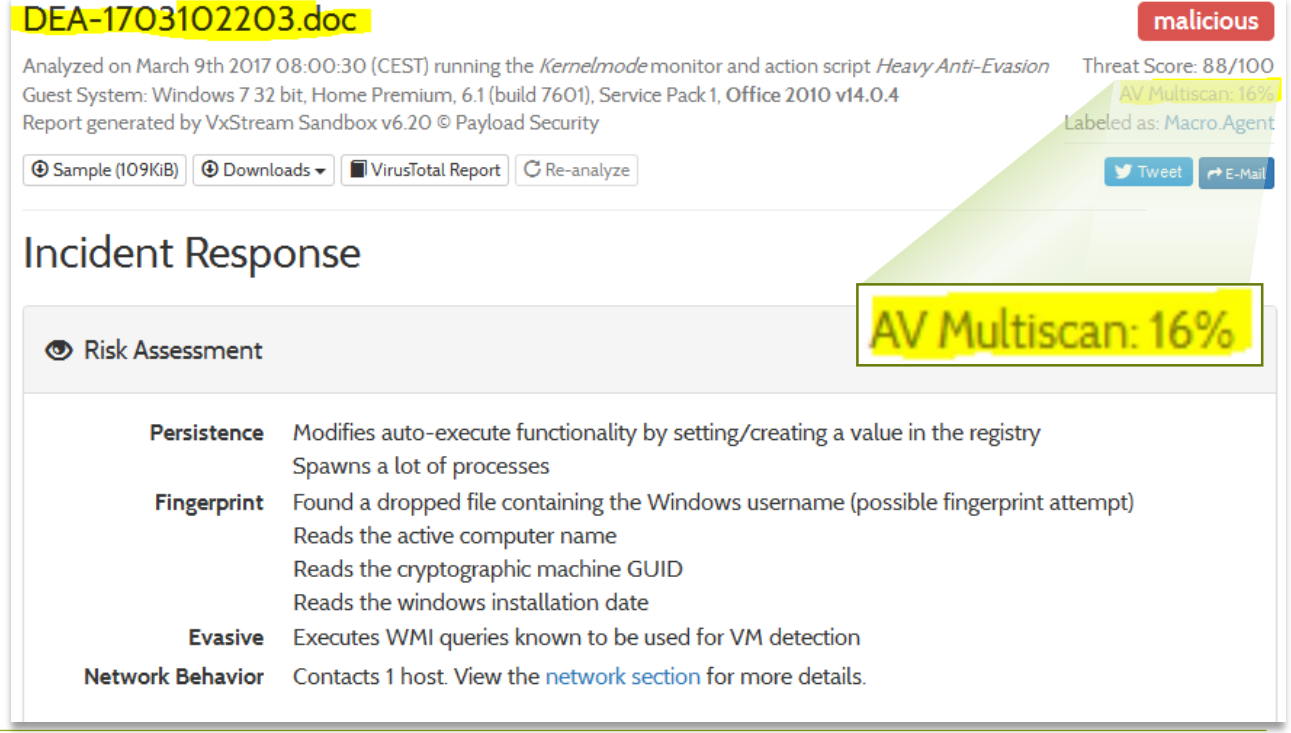
АНТИВИРУСНЫЕ АГЕНТЫ НА УЗЛАХ СПАСАЮТ НЕ ВСЕГДА



БЕСФАЙЛОВЫЙ ВРЕДОНОСНЫЙ КОД. ПРИМЕР (1/3)

Пример атаки. Доставка и запуск

- Пользователь получает фишинговое письмо с документом MS Office, который содержит макрос
- Макрос не имеет явных признаков вредоносного кода и не определяется классическим антивирусом



БЕСФАЙЛОВЫЙ ВРЕДОНОСНЫЙ КОД. ПРИМЕР (2/3)

Пример атаки. Доставка и запуск

- Проверка на VirusTotal показывает, что большинство Антивирусов его тоже не «видят»

SHA256: 12a7898fe5c75e0b57519f1e7019b5d09f5c5cbe49c48ab91daf6fcc09ee8a30

File name: court.doc

Detection ratio: 9 / 56

Analysis date: 2017-03-08 19:14:52 UTC (3 days, 13 hours ago)

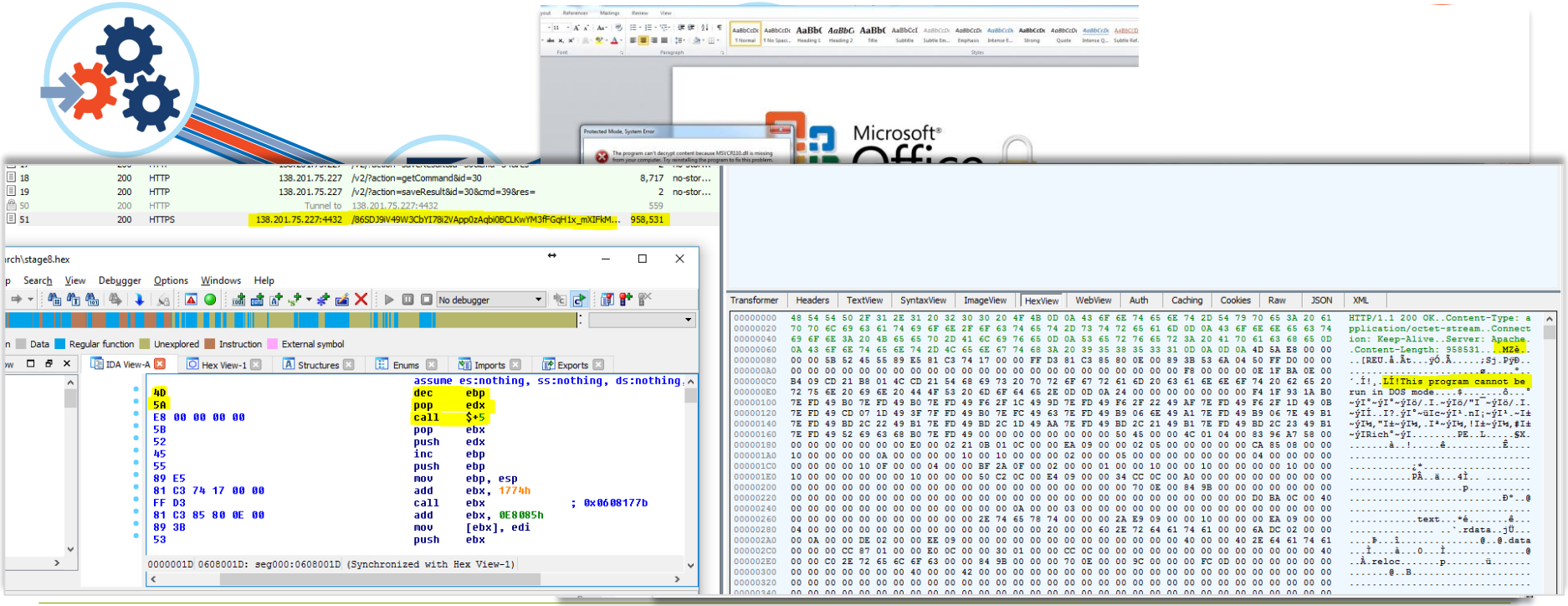
2 0

Analysis | File detail | Additional information | Comments 5 | Votes

Antivirus	Result	Update
AVG	W97M/PWS	20170308
Avast	MO97:Downloader-YI [Trj]	20170308
Avira (no cloud)	HEUR/Macro.Agent	20170308
ClamAV	Win.Trojan.PowerShell-10	20170308
ESET-NOD32	PowerShell/TrojanDownloader.Agent.AP	20170308
F-Secure	Trojan:W97M/MaliciousMacro.GEN	20170308
Fortinet	WM/Agent.AP!tr.dldr	20170308
Qihoo-360	heur.macro.powershell.x	20170308
ZoneAlarm by Check Point	HEUR:Trojan-Downloader.Script.Generic	20170308

БЕСФАЙЛОВЫЙ ВРЕДОНОСНЫЙ КОД. ПРИМЕР (3/3)

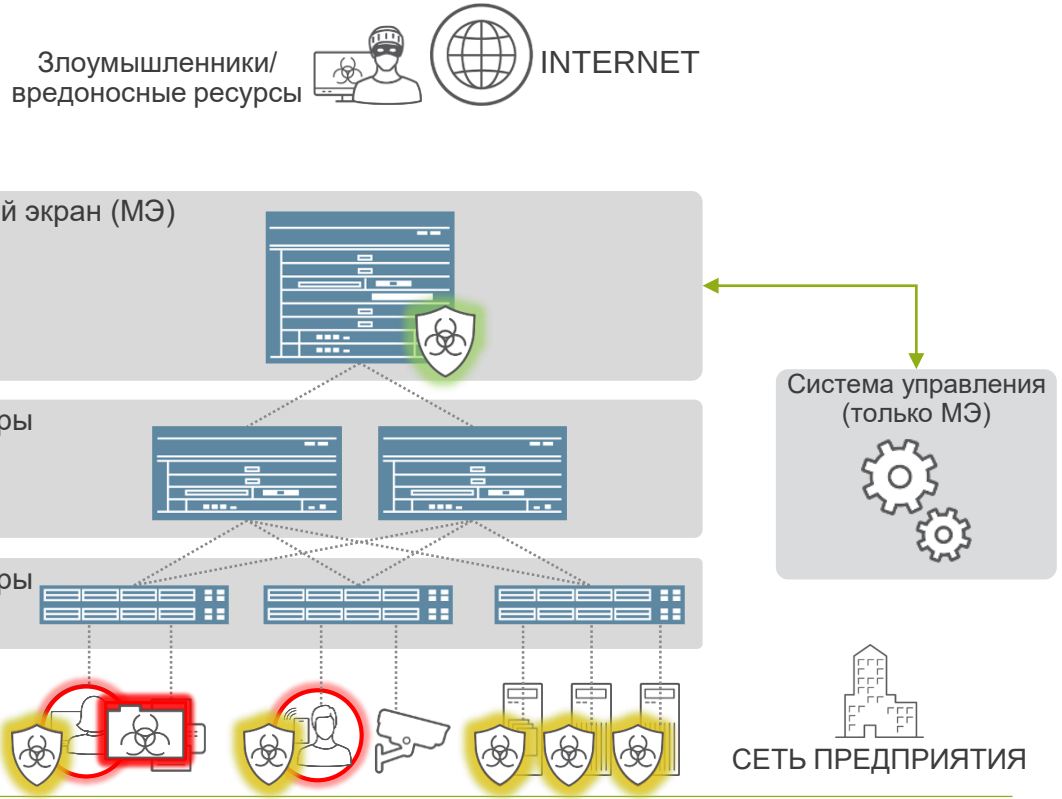
Пример атаки. Закрепление и исполнение



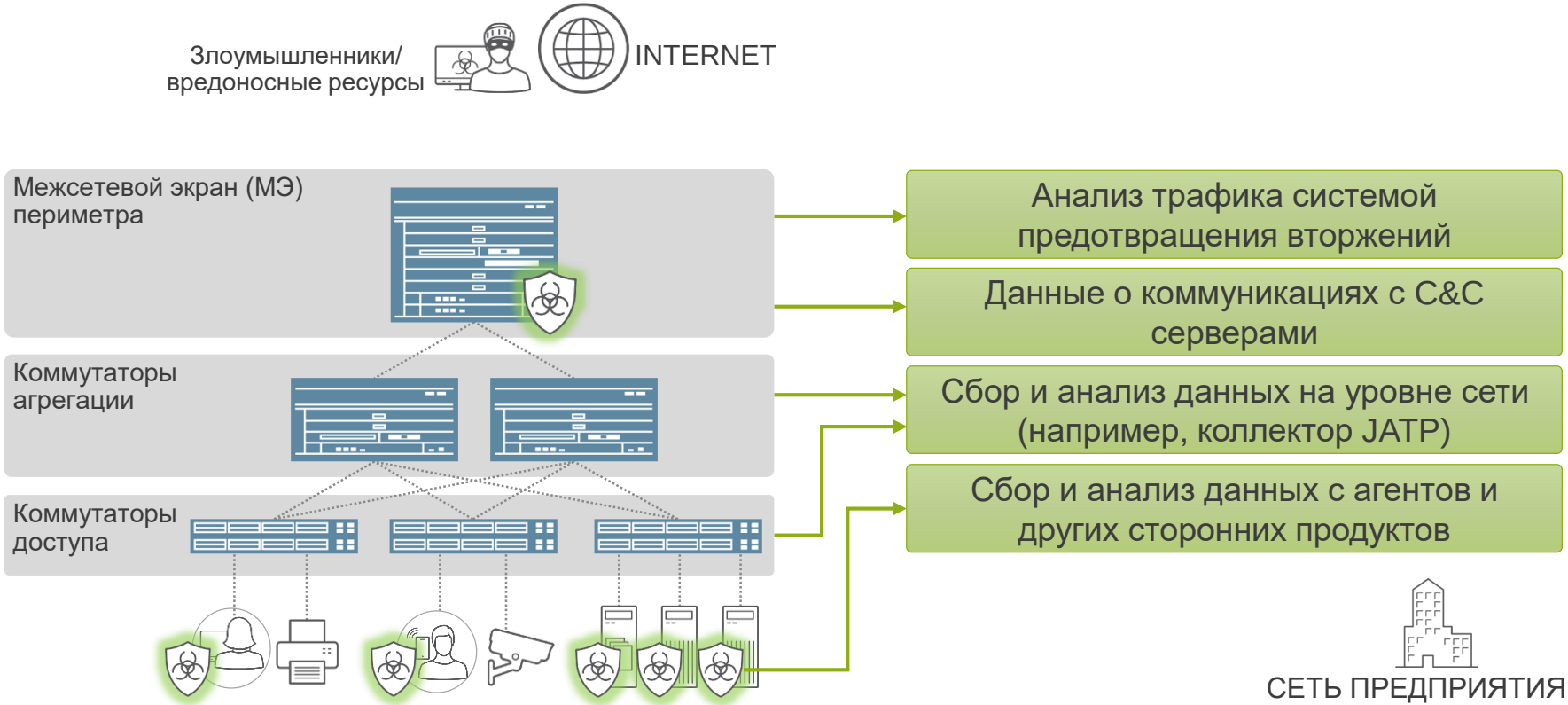
ТРАДИЦИОННАЯ ИНФРАСТРУКТУРА СЕГОДНЯ

Традиционная модель UNTRUST / TRUST

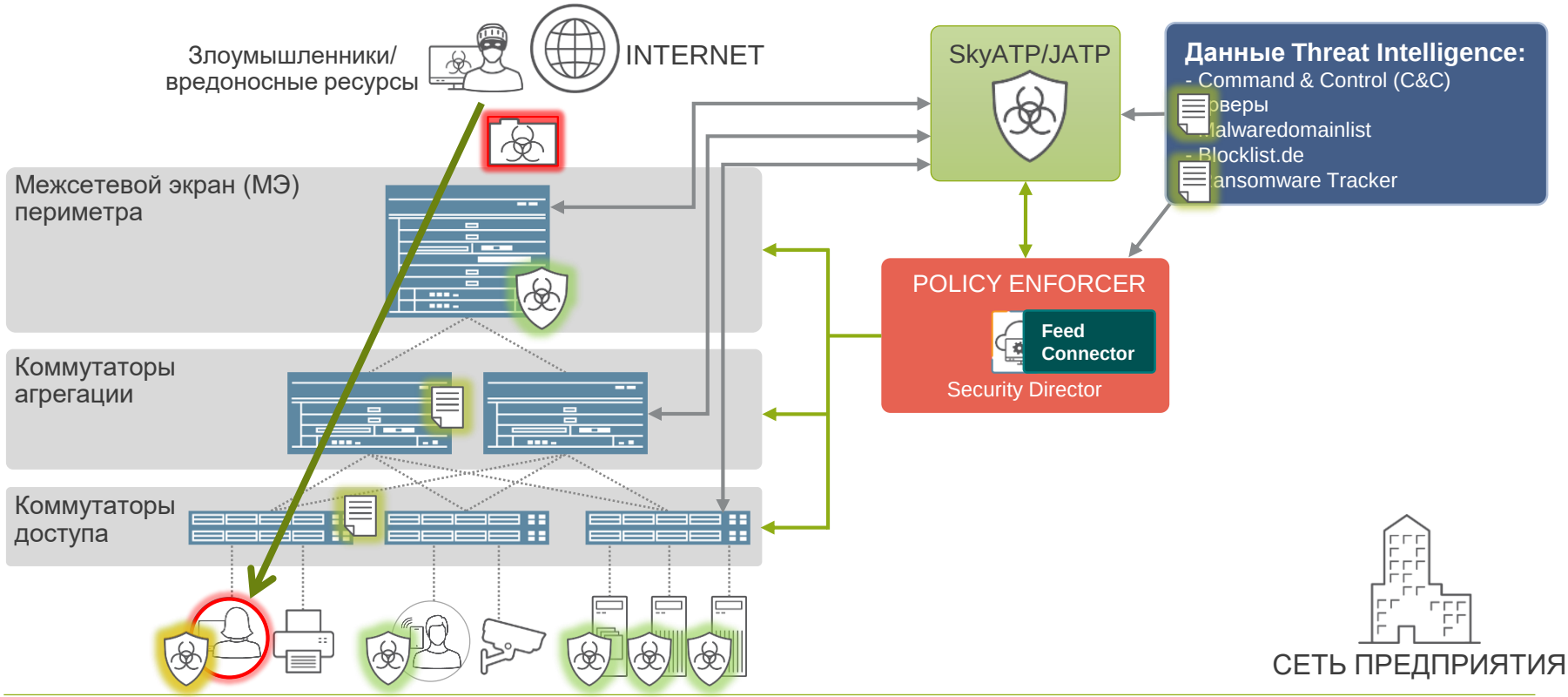
Типичный сценарий для этой модели



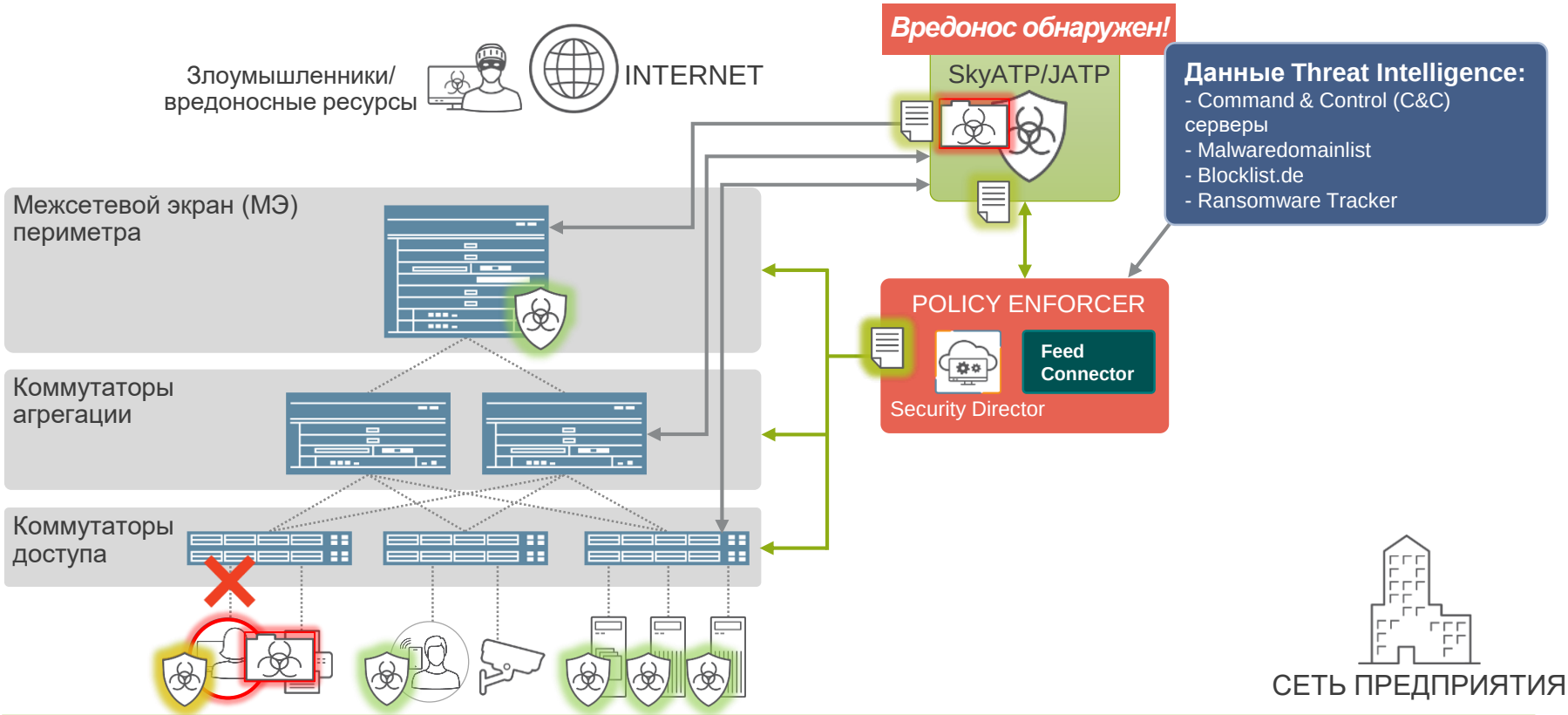
ВРЕДОНОС НУЛЕВОГО ДНЯ ПРОТИВ JUNIPER CONNECTED SECURITY



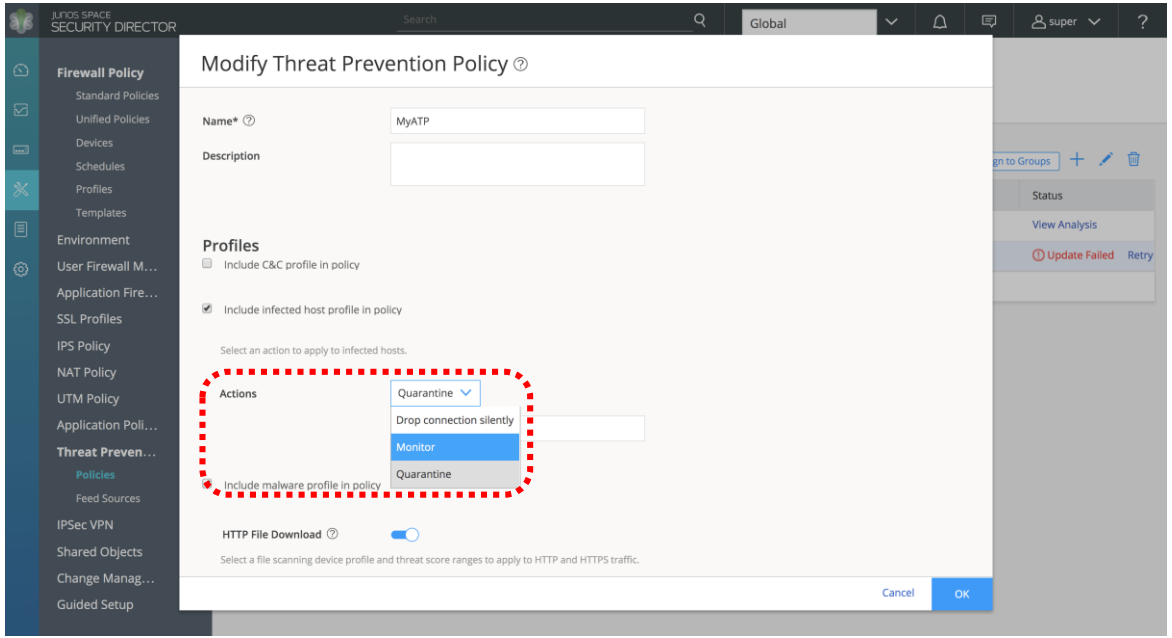
ВРЕДОНОС НУЛЕВОГО ДНЯ ПРОТИВ JUNIPER CONNECTED SECURITY



ВРЕДОНОС НУЛЕВОГО ДНЯ ПРОТИВ JUNIPER CONNECTED SECURITY

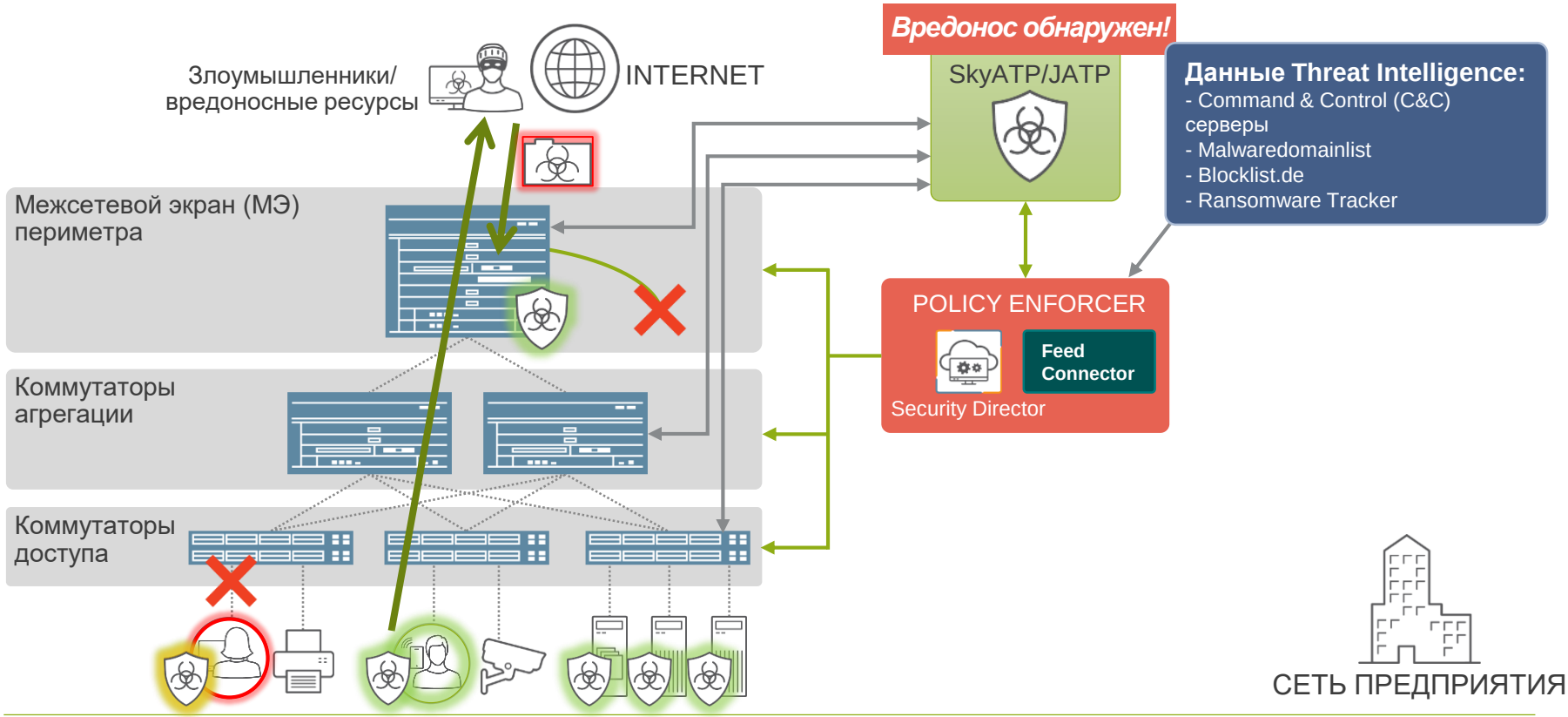


ДЕЙСТВИЯ НАД ИНФИЦИРОВАННЫМИ УЗЛАМИ

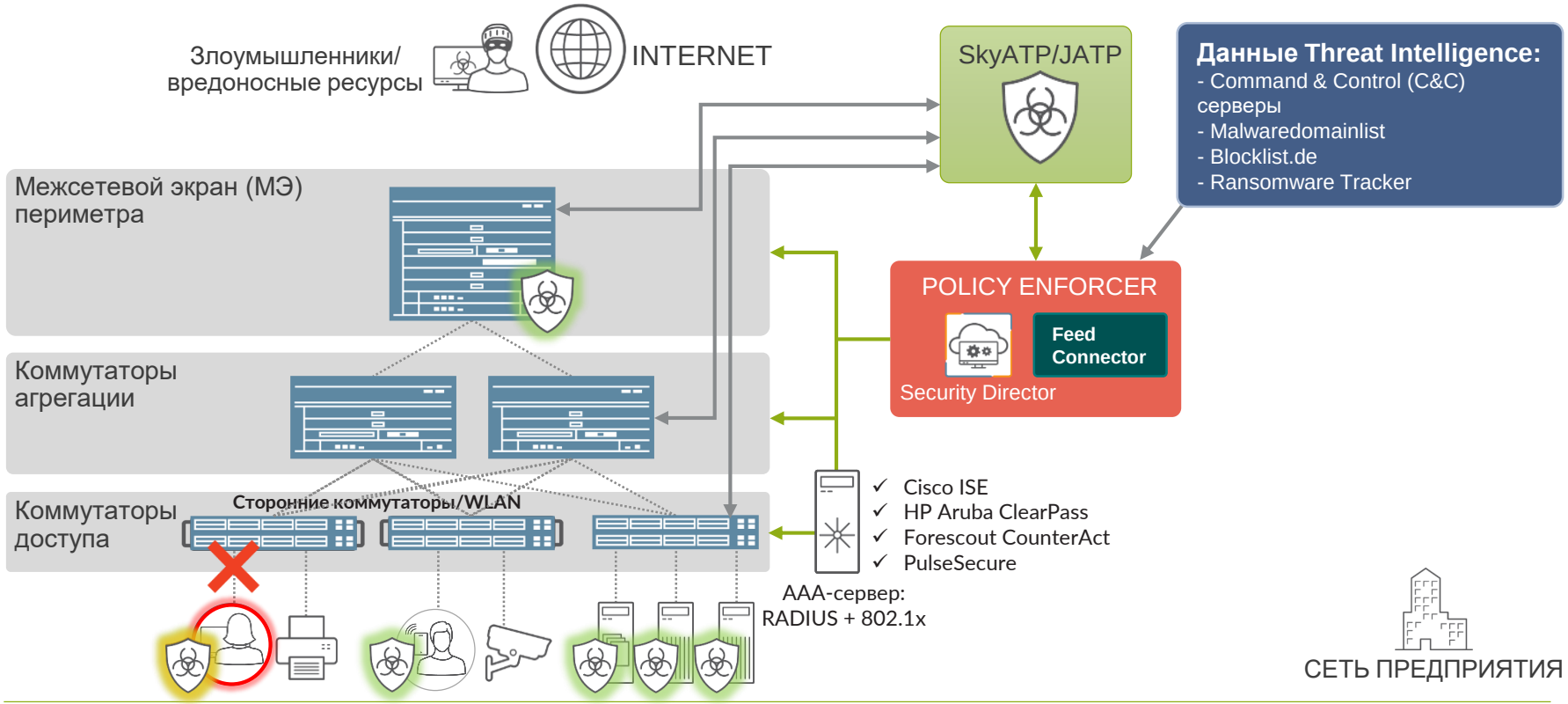


- Блокировать, Переводить в карантин и Мониторить
- Администратор получает уведомление об инфицировании и информацию о точке подключения зараженного узла: порт коммутатора, точка доступа WiFi…
- Режим мониторинга особенно актуален там, где нельзя блокировать узлы, например, роботы на линии сборки или элементы индустриальных сетей

ВРЕДОНОС НУЛЕВОГО ДНЯ ПРОТИВ JUNIPER CONNECTED SECURITY



А ЧТО ЕСЛИ КОММУТАТОРЫ/WIFI НЕ JUNIPER?

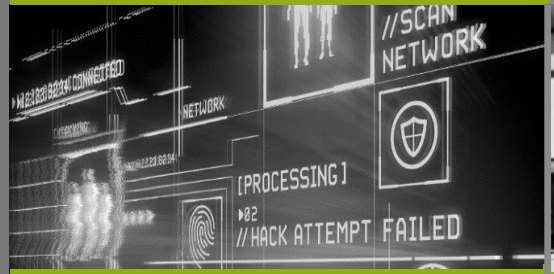


МИНИМИЗИРОВАТЬ РИСК

- Предполагаем, что угроза уже внутри
- Обеспечить детектирование и применение политик в каждой точке сети
- Принять существование уязвимостей в каждом элементе окружения
- Разрозненные продукты безопасности не всегда эффективны

JUNIPER CONNECTED SECURITY

ВИДЕТЬ



- События безопасности и
- данные Threat Intelligence от разных производителей

ВИДЕТЬ

АВТОМАТИЗИРОВАТЬ

- Обнаружение, корреляция и аналитика
- Отделение угроз от информационного шума

ЗНАТЬ

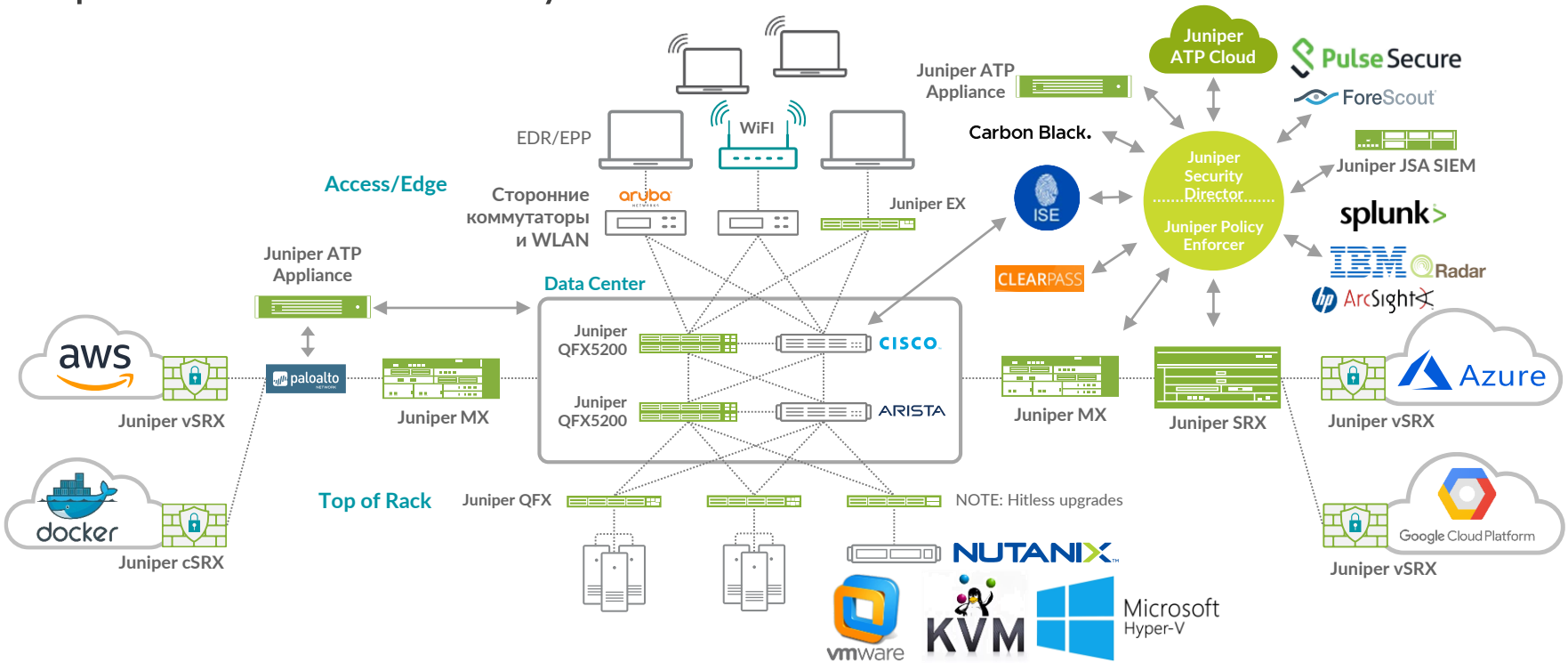
- Изоляция зараженного узла
- Нейтрализация в один клик
- Интеграция с другими вендорами

ДЕЙСТВОВАТЬ

ЗАЩИЩАТЬ

ИНФРАСТРУКТУРА ГОТОВАЯ ПРОТИВОСТОЯТЬ УГРОЗАМ

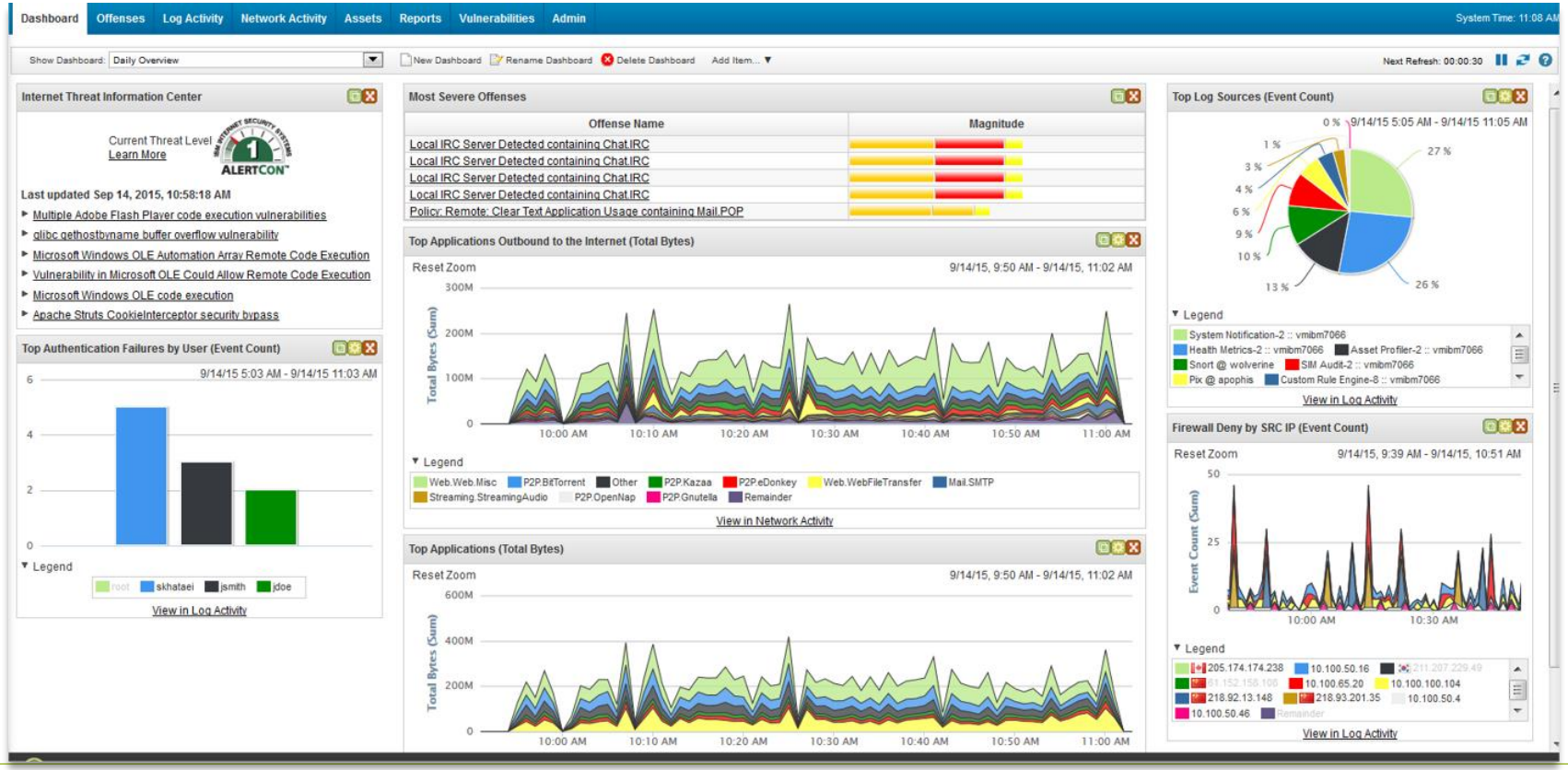
Juniper Connected Security



Видеть и Знать

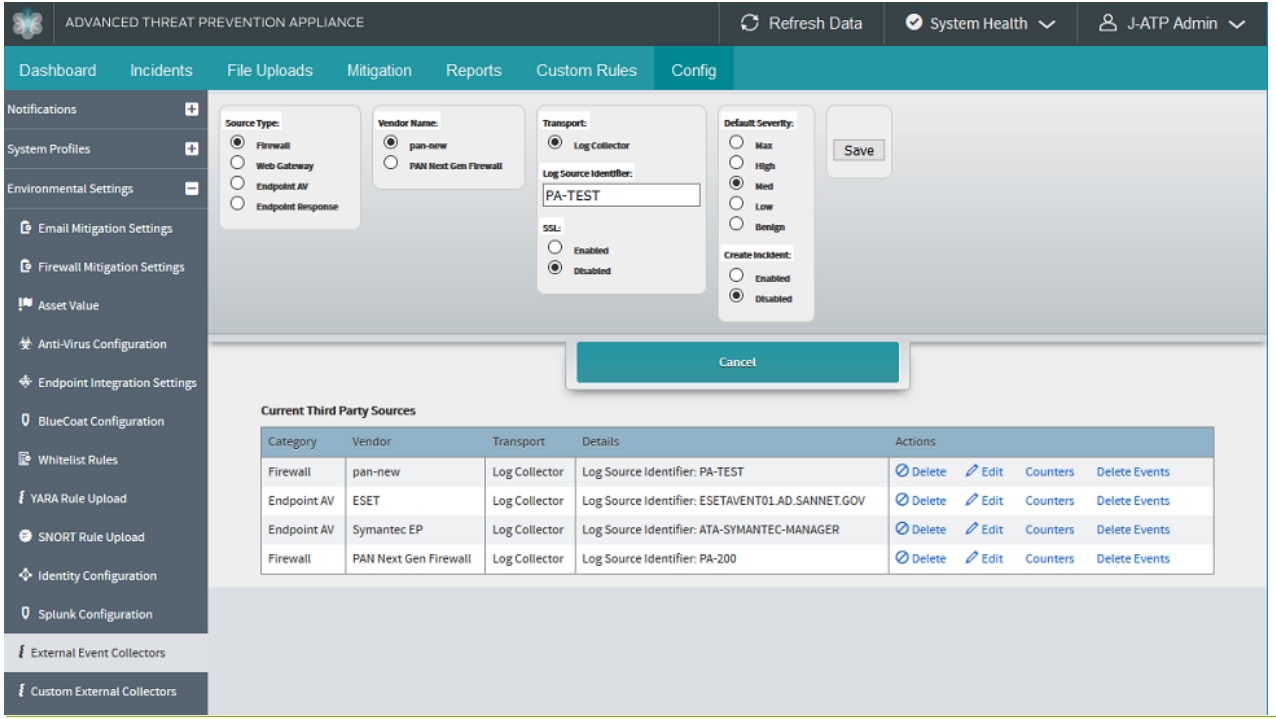
JUNIPER SECURE ANALYTICS SIEM

JUNIPER SECURE ANALYTICS SIEM

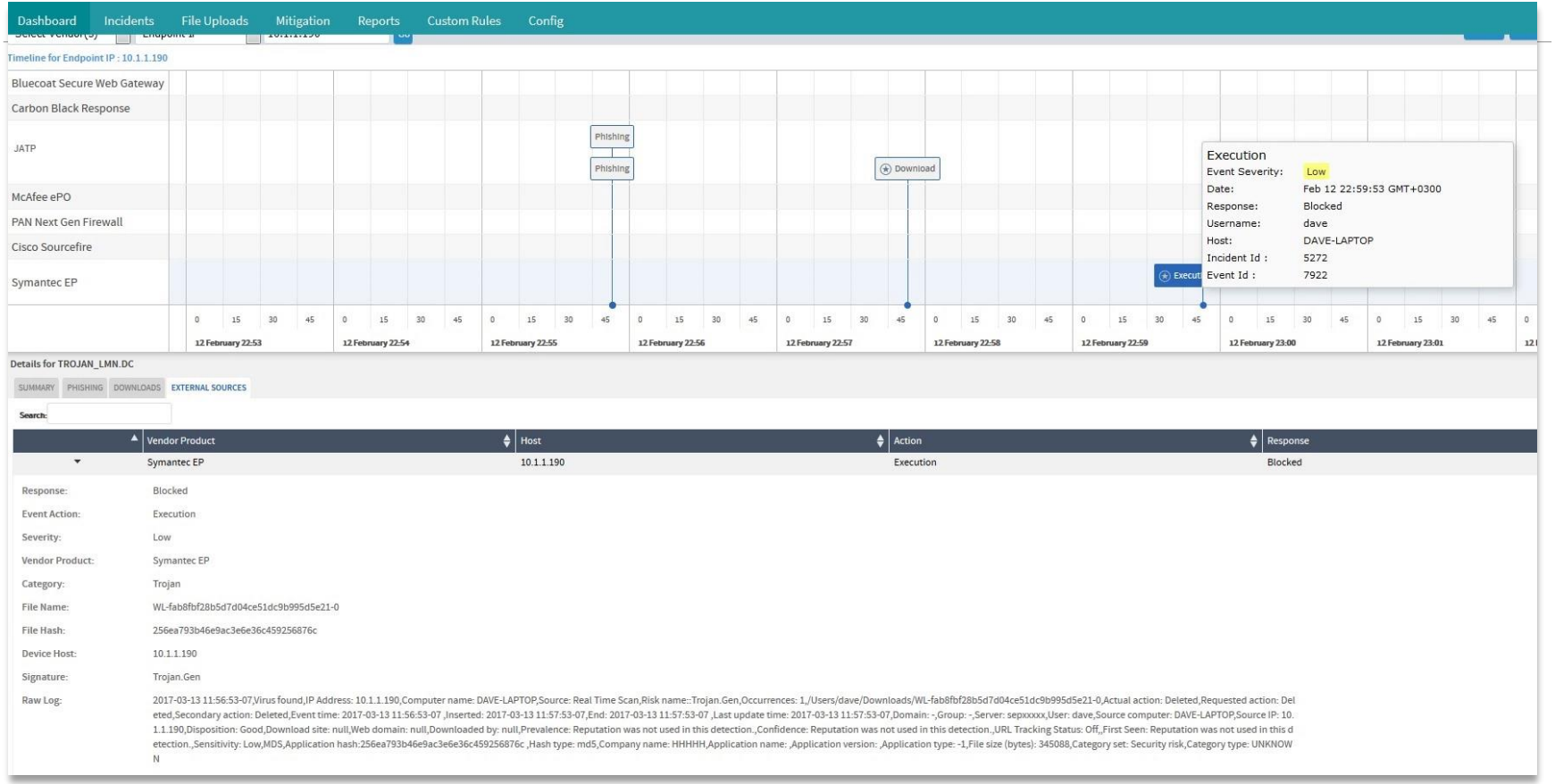


АНАЛИЗ И КОРРЕЛЯЦИЯ СОБЫТИЙ В JATP

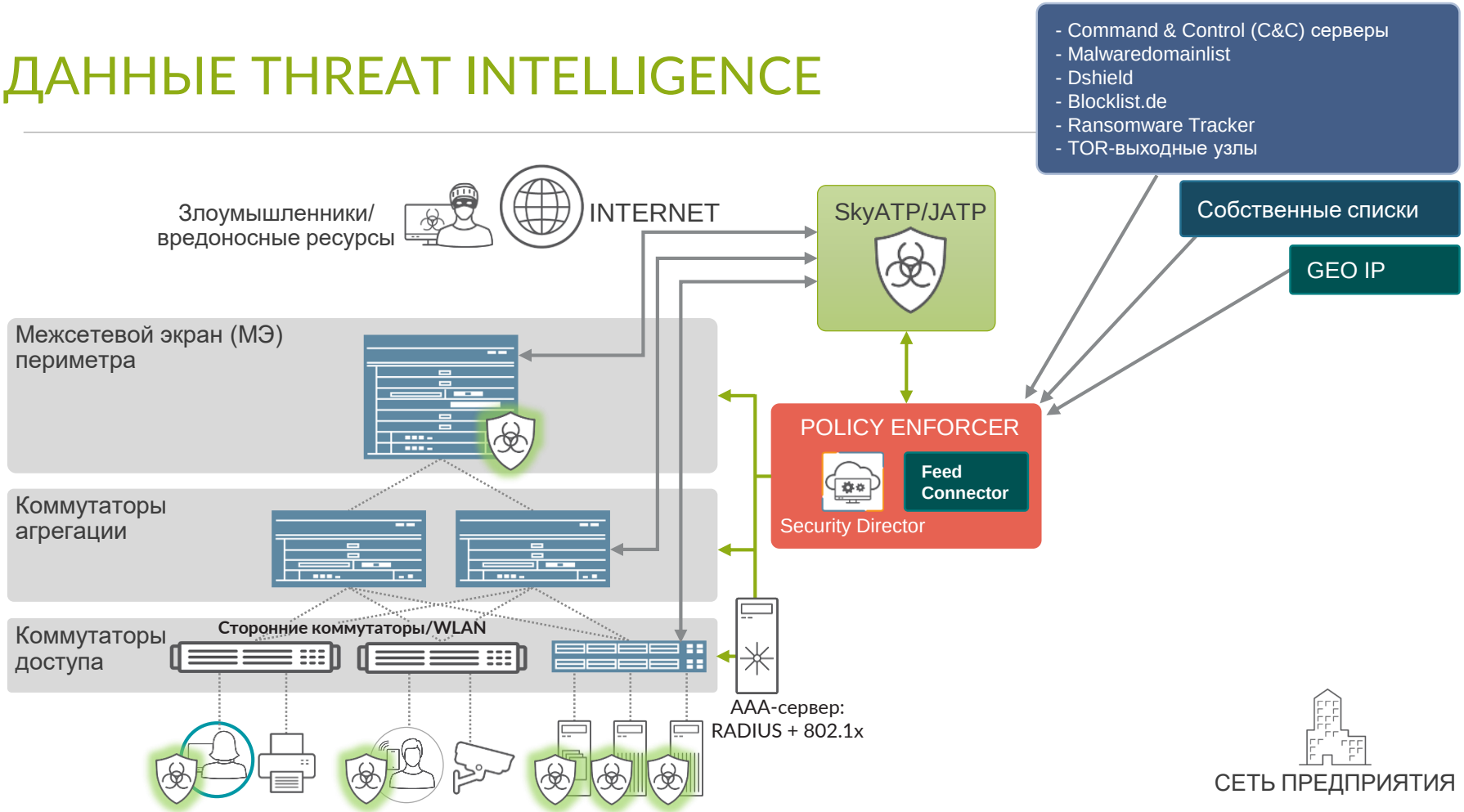
Собирает, анализирует и коррелирует события от любых производителей: парсеры «из коробки» и свои собственные



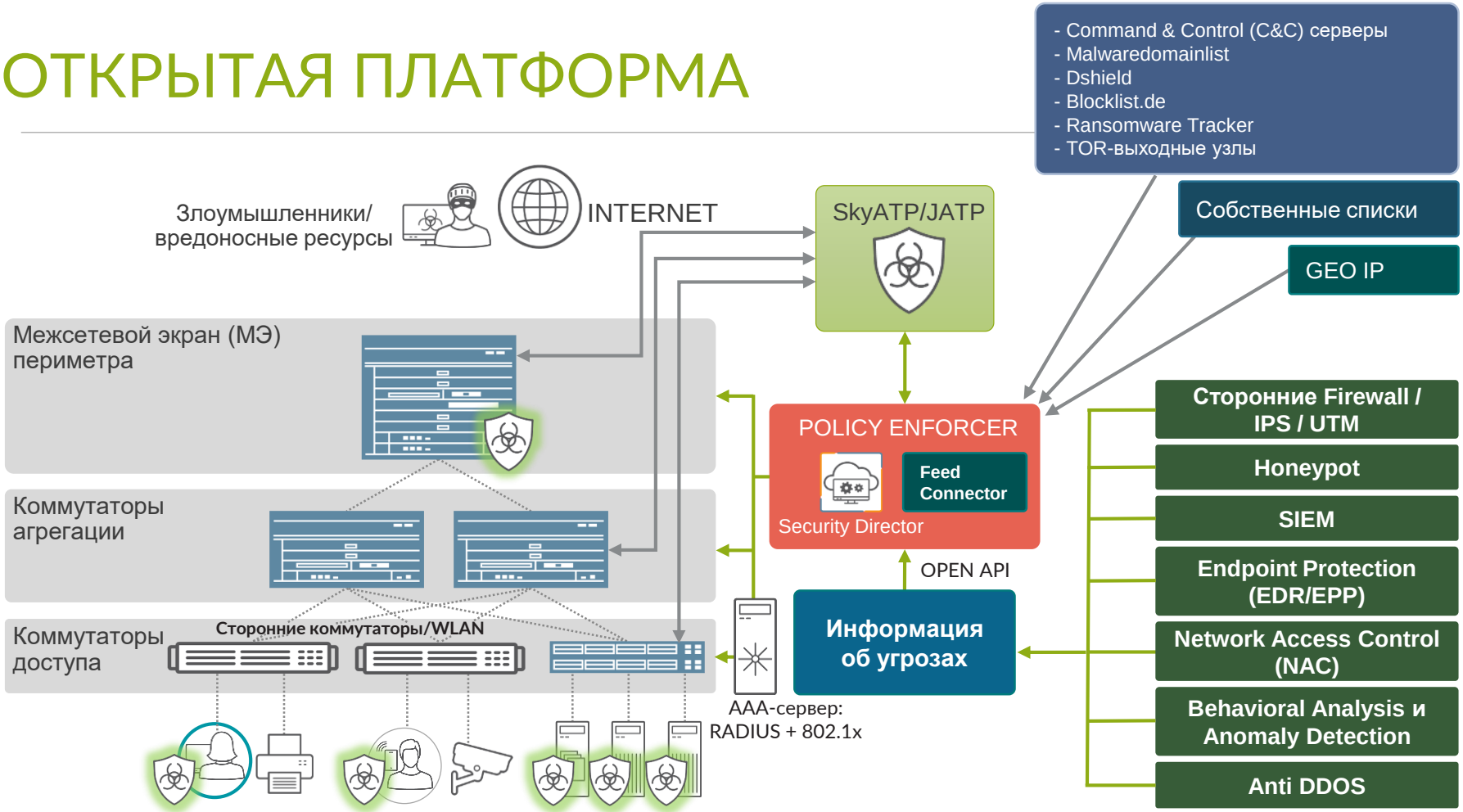
КОРРЕЛЯЦИЯ СОБЫТИЙ В JATP



ДАННЫЕ THREAT INTELLIGENCE



ОТКРЫТАЯ ПЛАТФОРМА



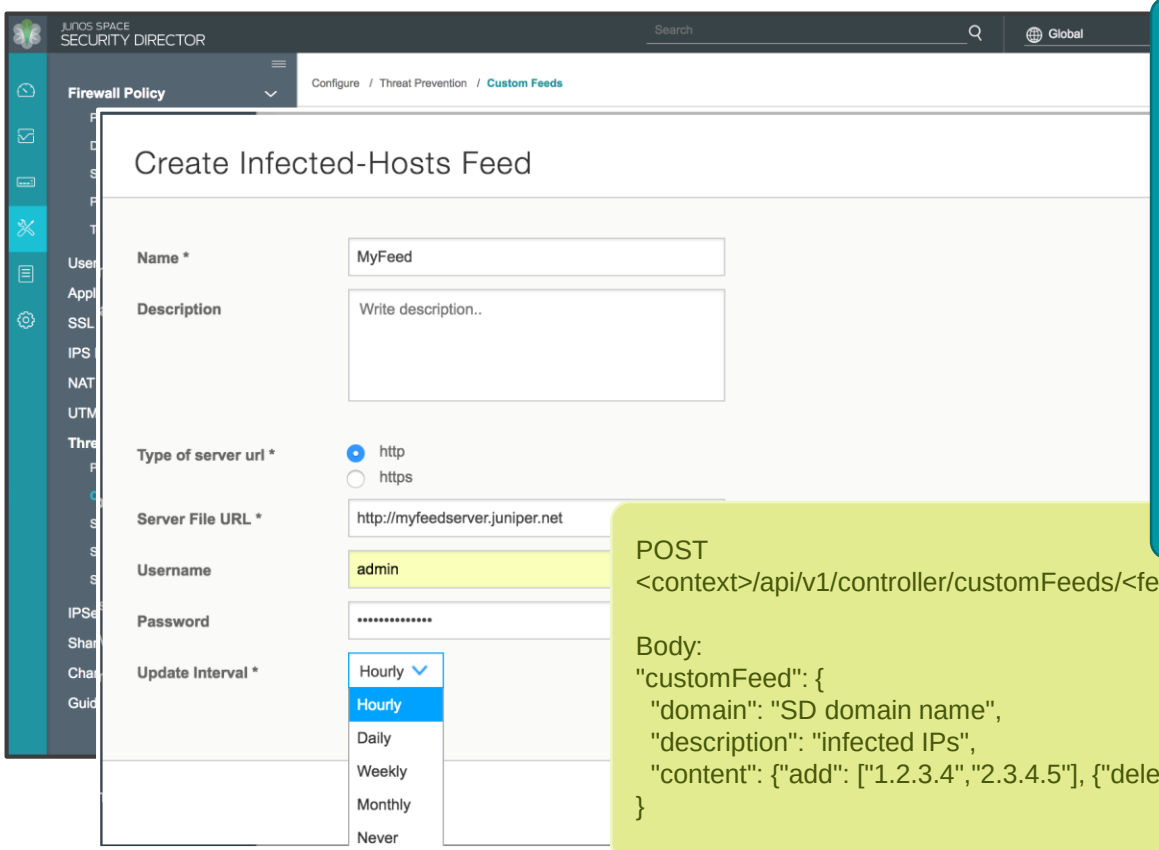
OPEN API FRAMEWORK

RESTful API – стандартные методы включают POST, PATCH, GET, DELETE

Соответствует спецификации Swagger API в формате JSON. API удовлетворяют стандарту OpenAPI Initiative.

Threat Intel API	File/Hash API	Sky ATP API для Черных/Белых списков	Infected Hosts API
• Добавлять/удалять IPv4/v6,URL и FQDN в C&C фиды • До 30 собственных фидов • Черные/белые списки	• Поиск образцов по хэшу • Передача образцов для анализа • Параметры для получения детального отчета	• Доступны также и в UI • Модификация значений через API	• Фид зараженных узлов, которые необходимо заблокировать на уровне сети (доступ, фаерволы, маршрутизаторы)

ДАННЫЕ ОБ УГРОЗАХ ИЗ ЛЮБЫХ ИСТОЧНИКОВ



1. Настройка собственного списка зараженных узлов
2. Список может формироваться из
    1. Локально загружаемого файла,
    2. Файла, загружаемого с удаленного сервера
    3. Загружаться в Policy Enforcer через API

POST
<context>/api/v1/controller/customFeeds/<feedType>/param/<inputType>/<name>

Body:

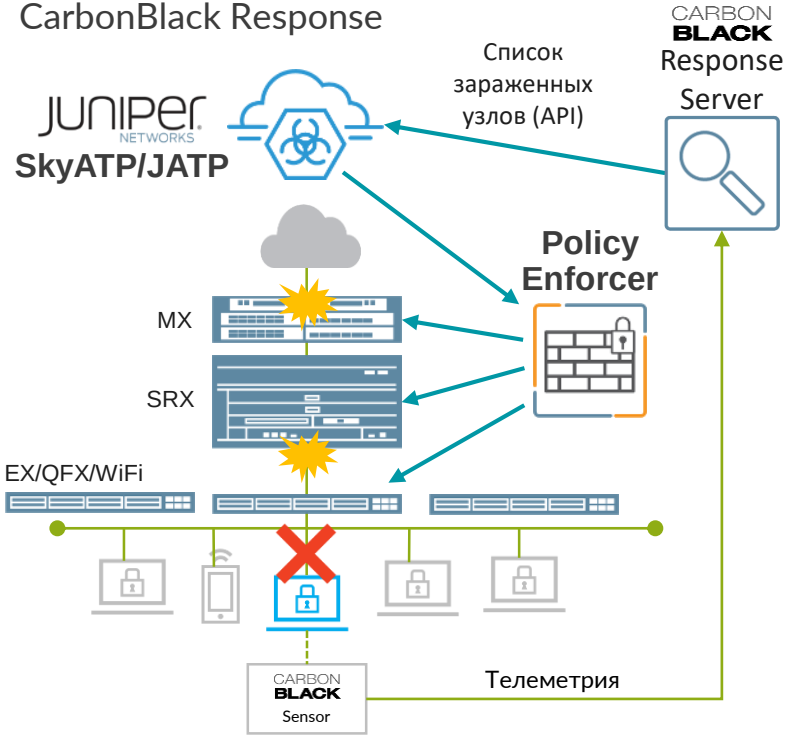
```
"customFeed": {
  "domain": "SD domain name",
  "description": "infected IPs",
  "content": {"add": ["1.2.3.4","2.3.4.5"], {"delete": ["1.3.4.5"]}
}
```

Действовать и Защищать

ОТКРЫТАЯ ПЛАТФОРМА

ИЗОЛЯЦИЯ ЗАРАЖЕННОГО УЗЛА. **EDR -> ATP**

Использование информации об угрозах из CarbonBlack Response



Сценарий использования

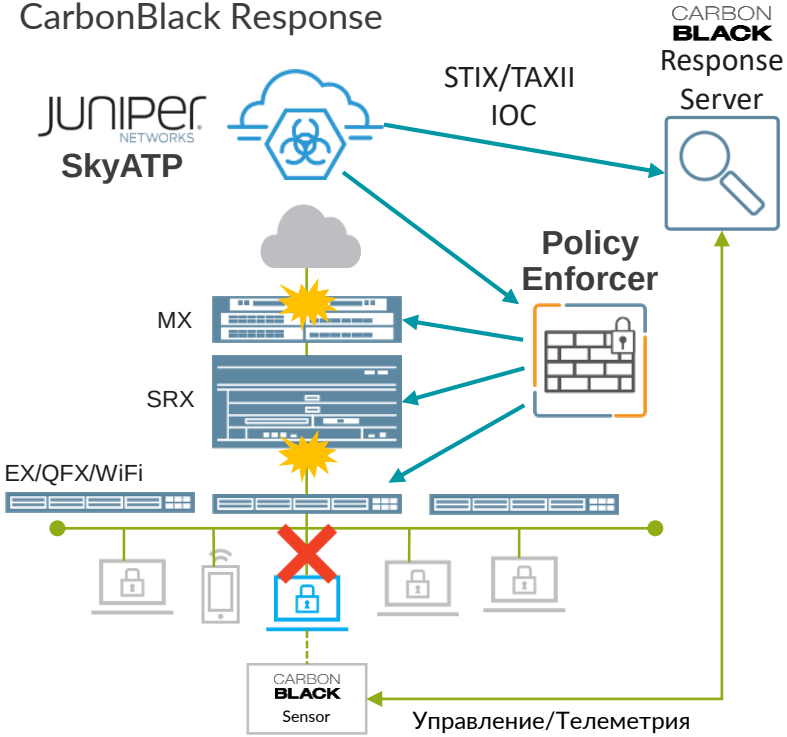
- CB Response детектирует наличие угрозы на оконечном узле и отправляют информацию об IP-адресе в SkyATP/JATP через API,
- SkyATP/JATP добавляет IP-адрес узла в Список зараженных узлов и уведомляет Policy Enforcer,
- Сеть блокирует зараженный узел

Преимущества

- Предотвращение заражения других узлов в сети
- Нейтрализация ранее зараженных узлов (например, заражение произошло с USB-носителя или при подключении к другой сети)

ИЗОЛЯЦИЯ ЗАРАЖЕННОГО УЗЛА. ATP -> EDR

Использование информации об угрозах из CarbonBlack Response



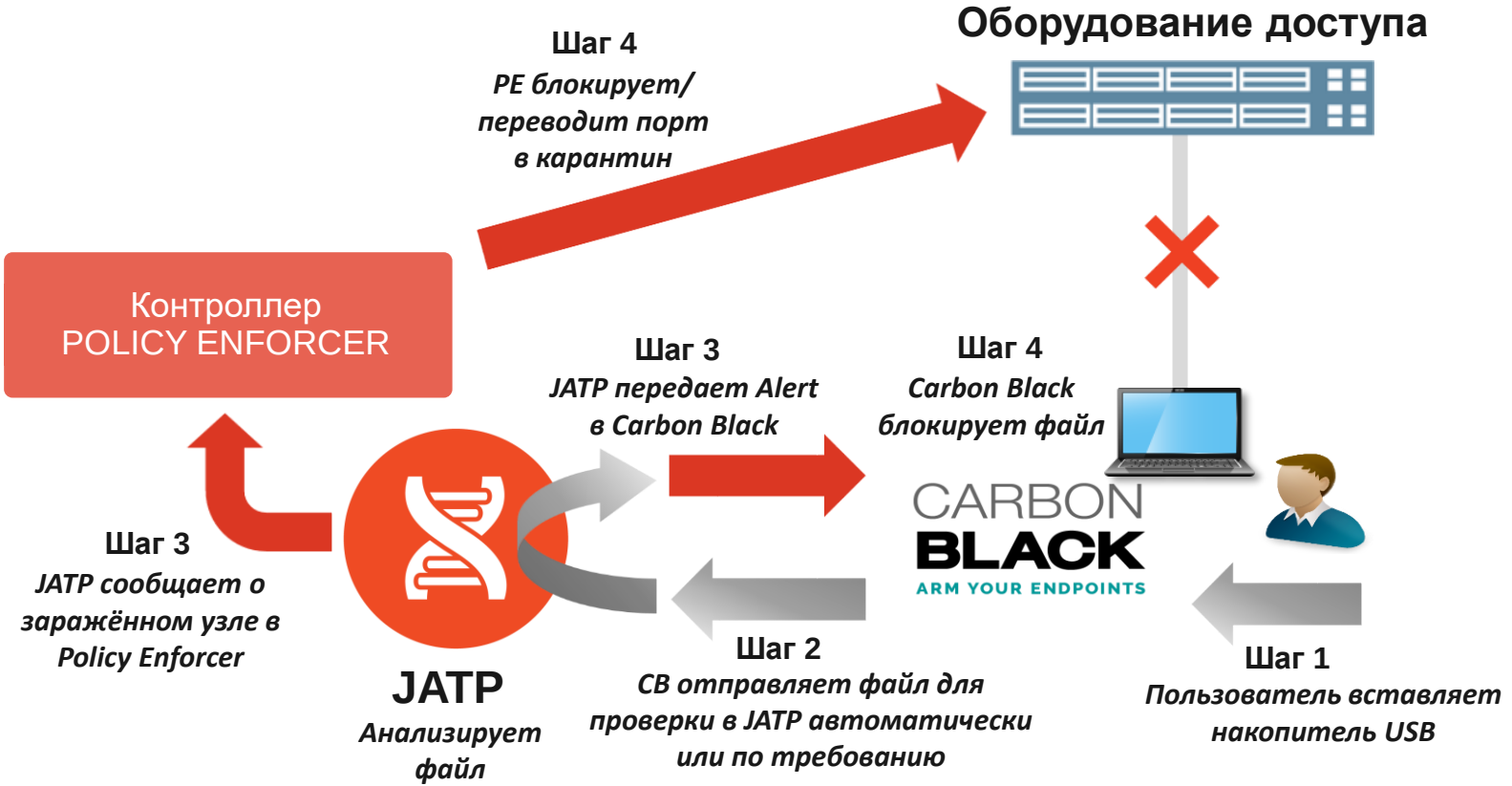
Сценарий использования

- SkyATP детектирует наличие угрозы на оконечном узле и отправляют IOC в CB Response средствами STIX/TAXII,
- SkyATP добавляет IP-адрес узла в Список зараженных узлов и уведомляет Policy Enforcer,
- CB идентифицирует все узлы, подверженные угрозе, и действует (напр. карантин узла)
- Сеть блокирует зараженный узел

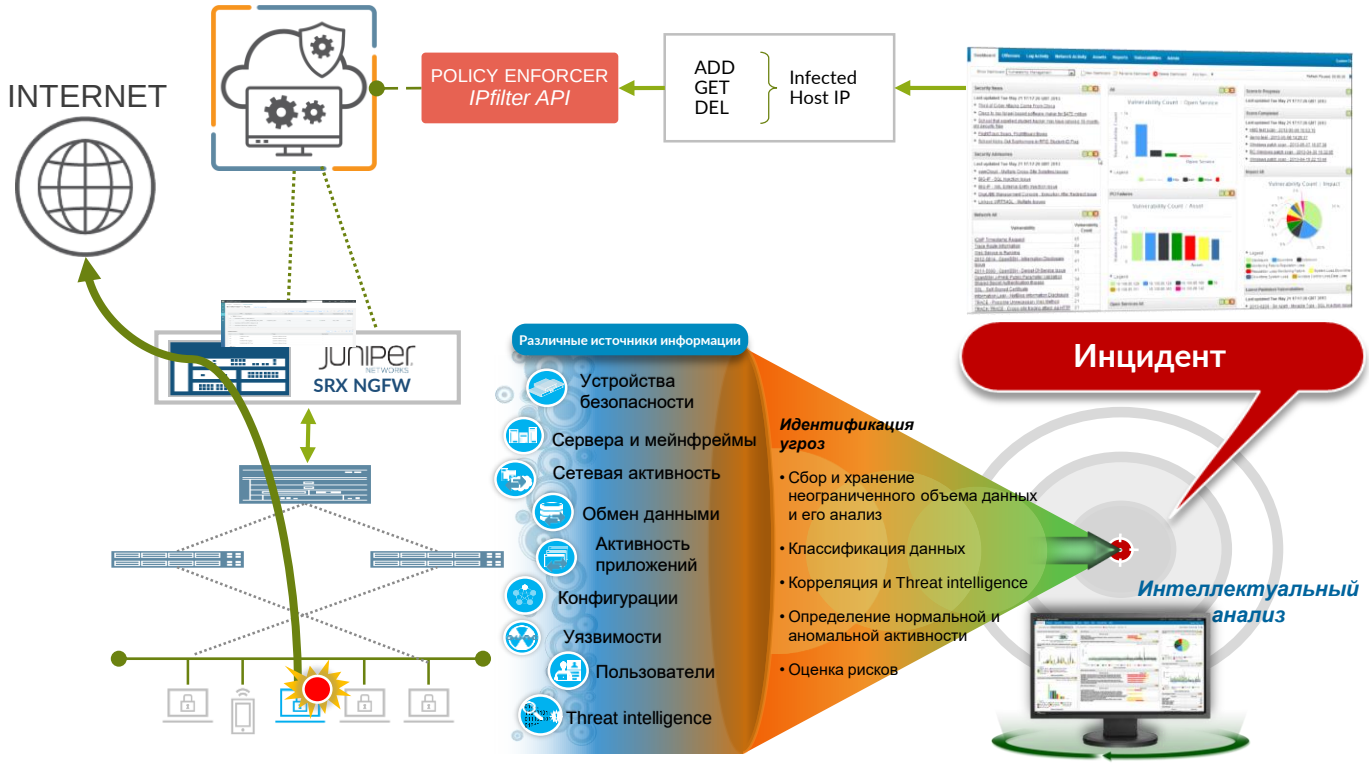
Преимущества

- Предотвращение заражения других узлов в сети
- Совместное использование данных об угрозах для идентификации зараженных узлов и защиты сети
- Данные о состоянии узлов сети

ДЕТЕКТИРОВАНИЕ ВРЕДОНОСНОГО КОДА В ЛОКАЛЬНЫХ ФАЙЛАХ



СЦЕНАРИЙ ВЗАИМОДЕЙСТВИЯ SIEM -> PE



- Подозрительная активность узла
- JSA SIEM коррелирует и анализирует собранные данные о событиях, трафике, поведении
- JSA фиксирует Инцидент
- IP-адрес источника добавляется (вызов API) в IPfilter-фид ‘Suspicious_user’
- PE обновляет динамическую адресную группу в NGFW SRX
- Адрес теперь соответствует политике безопасности в SRX
- Трафик от подозрительного узла теперь подвергается дополнительной проверке: IPS, AV, ATP, URLF, CF и т.д.

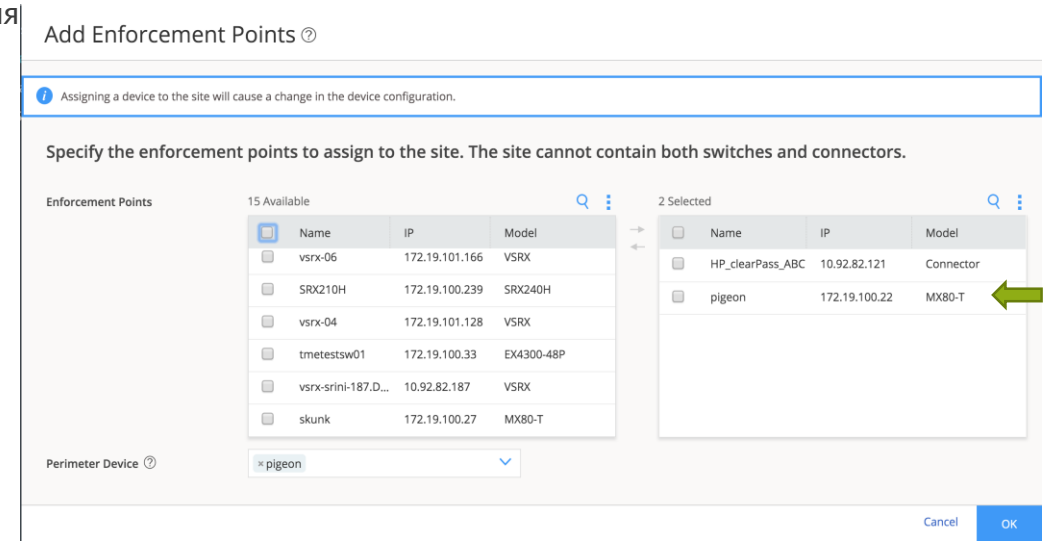
МАРШРУТИЗАТОРЫ СЕРИИ MX КАК УСТРОЙСТВА ПЕРИМЕТРА В SECURE FABRIC

Преимущество

- Маршрутизаторы MX также могут работать для защиты от продвинутых угроз когда развернуты как граничные устройства
- Маршрутизаторы MX умеют блокировать трафик к/от Command & Control-серверам

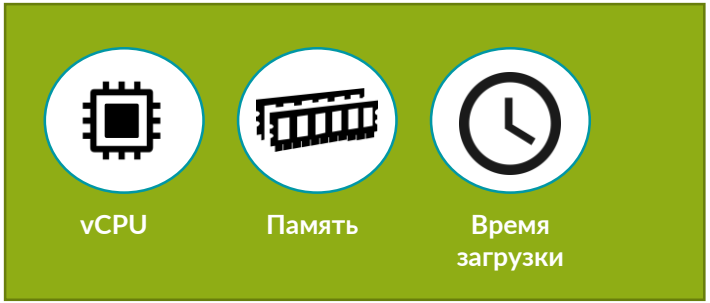
Как это работает

- Устройства MX добавляются как «Enforcement points» в Secure Fabric
- MX использует динамические ACL
- Контроллер Policy Enforcer передает списки C&C-серверов в MX для этих ACL
- Поддерживаются Command & Control и GeoIP фиды IP-адресов



ВИРТУАЛЬНЫЕ СРЕДЫ И ОБЛАКА

Скорость развертывания и размер



СТОИМОСТЬ ПОЛЬЗОВАНИЯ ОБЛАЧНОЙ ИНФРАСТРУКТУРОЙ ЗАВИСИТ ОТ ПОТРЕБЛЯЕМЫХ РЕСУРСОВ.
МЕНЬШЕ РЕСУРСОВ – НИЖЕ TCO

vSRX 2.x

- Вложеная виртуализация (Junos in KVM)
- Значительное время загрузки и место на диске

vSRX 3.0

- Без вложенной виртуализации
- Время загрузки в 7 раз меньше, чем раньше

cSRX

- Контейнерный фаерволл. Время загрузки – секунды, крошечный размер

ПОДДЕРЖКА ПЛАТФОРМ

Сервера и гипервизоры

SDN

IaaS

ФАЕРВОЛ ВНЕДРЯЕТСЯ В СУЩЕСТВУЮЩУЮ ИНФРАСТРУКТУРУ, А НЕ НАОБОРОТ

ГИПЕРВИЗОРЫ

- VMware ESXi 5.x, 6.0, 6.5, 6.7
- KVM – Centos, Ubuntu & RHEL
- Microsoft – Hyper-V
- Nutanix - AHV

КОНТЕЙНЕРЫ

- Docker for cSRX
- Contrail + K8s

ПЛАТФОРМЫ ЧАСТНЫХ ОБЛАКОВ

- VMware NSX
- Open Stack
- Contrail

ПУБЛИЧНЫЕ ОБЛАКА

- Amazon AWS
- Microsoft Azure
- Google Cloud Platform

ИНТЕГРАЦИЯ С NSX

Пример: Микро-сегментация с NSX & vSRX

Реализация политик

Микро-сегментация в доменах NSX в частных облачных ЦОД

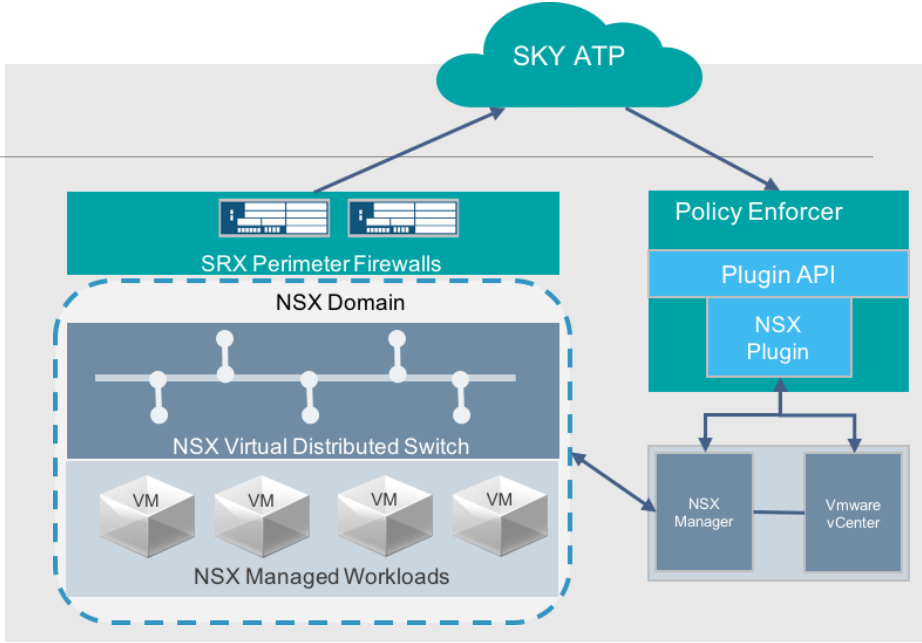
- AppSecure (Layer-7 Application Firewall)
- IPS

Интеграция управления (Policy Enforcer <–> NSX Manager)

Threat Prevention Policy

- Sky ATP, JATP
- UTM (Web Filtering, Anti-Virus, Anti-Spam, Content-Filtering)

Сертифицировано VMWare



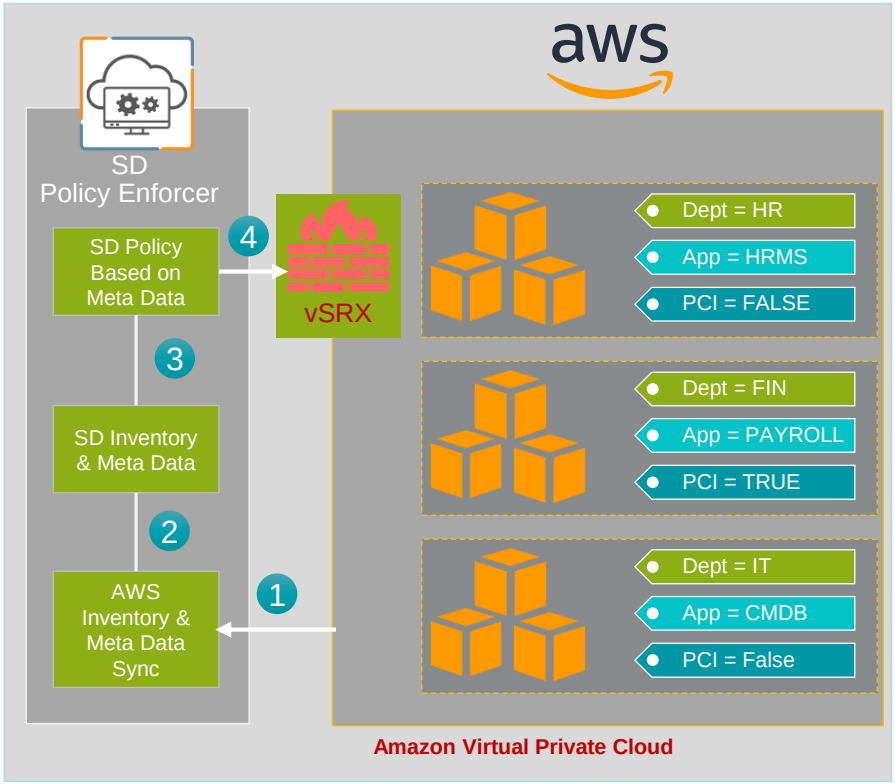
Ключевой функционал

- Security Fabric включает хосты домена NSX
- Синхронизация Групп Безопасности (Security Group)
  Группы безопасности NSX и членство хостов в группах синхронизируется с Security Director “Dynamic Address Groups”
- Политика Security Director для трафка Север-Юг и Восток-Запад
  SD задает L7/IPS/ATP политику для проверки трафика С-Ю и В-З
  Логи/Отчеты включают имена виртуальных машин для задач аудита и поиска неисправностей

Преимущества для конечного пользователя

Авто-развертывание vSRX на узлы NSX
Продвинутая проверка (L7 Firewall, IPS, Sky ATP, JATP) для любых маршрутов трафика
Единая политика управления для трафика Север-Юг и Восток-Запад

ИНТЕГРАЦИЯ С AMAZON WEB SERVICES



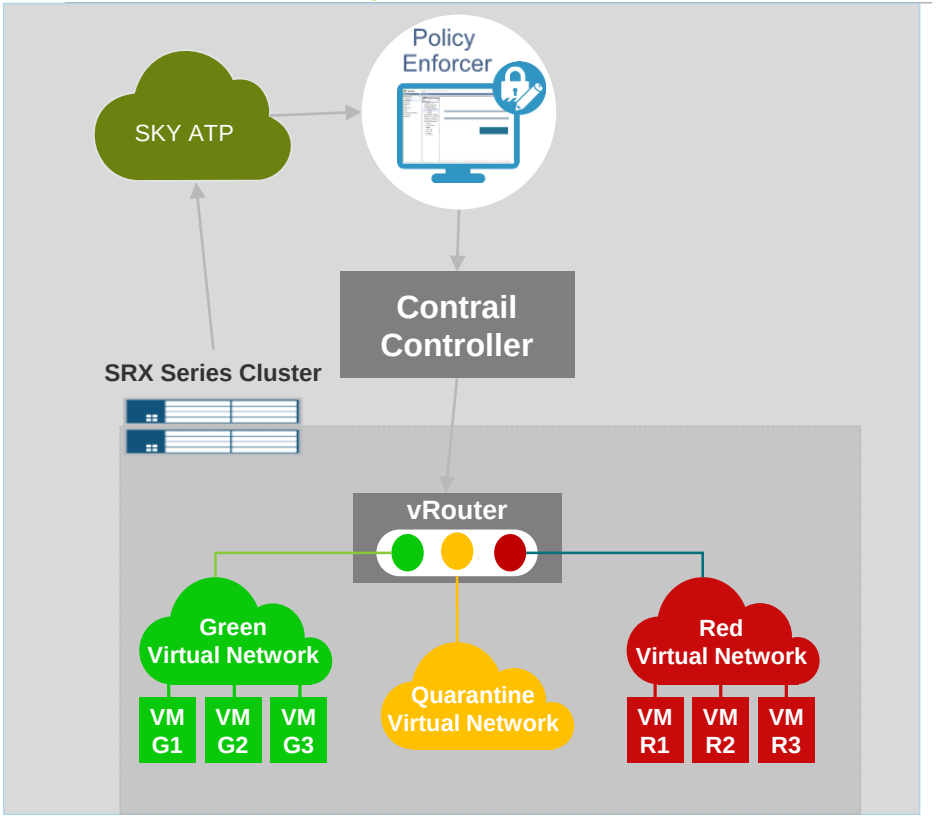
Решаемые задачи

- Политика безопасности должна поспевать за изменяющимся окружением в облаке
- Соответствие процессам в Amazon Virtual Private Cloud
- Горизонтальный трафик в Amazon VPC

Juniper Connected Security

- Синхронизация inventory и мета-данных из AWS в Security Director
- Policy Enforcer поддерживает политики на основе мета-данных для быстроменяющихся сетевых условий
- Сервисы L3, L7 FW, IPS и Threat Prevention Policies на основе мета-данных
- Блокировка угроз: Зараженные машины AWS помещаются на карантин путем перемещения их в заданную Группу Безопасности AWS

ИНТЕГРАЦИЯ С CONTRAIL



Блокировка угроз

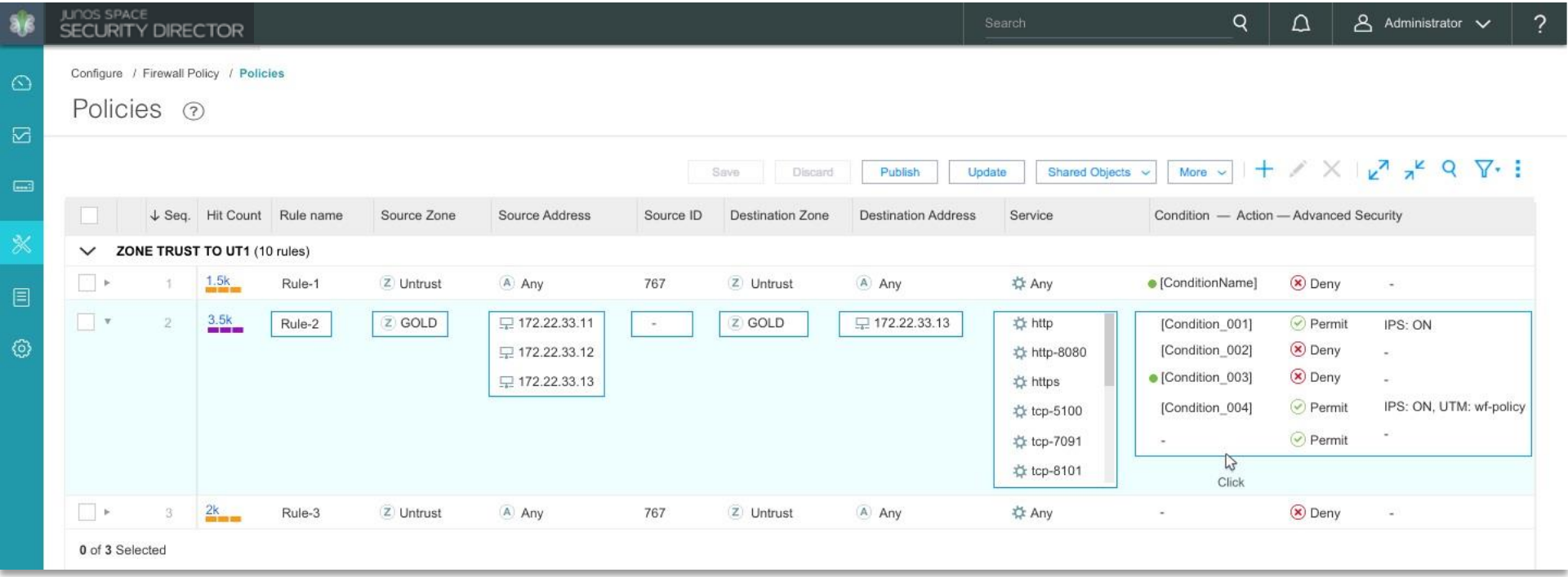
- Например, перевод в Quarantine Virtual Network
- Блокировка доступа к сети
- Изменение групп безопасносности

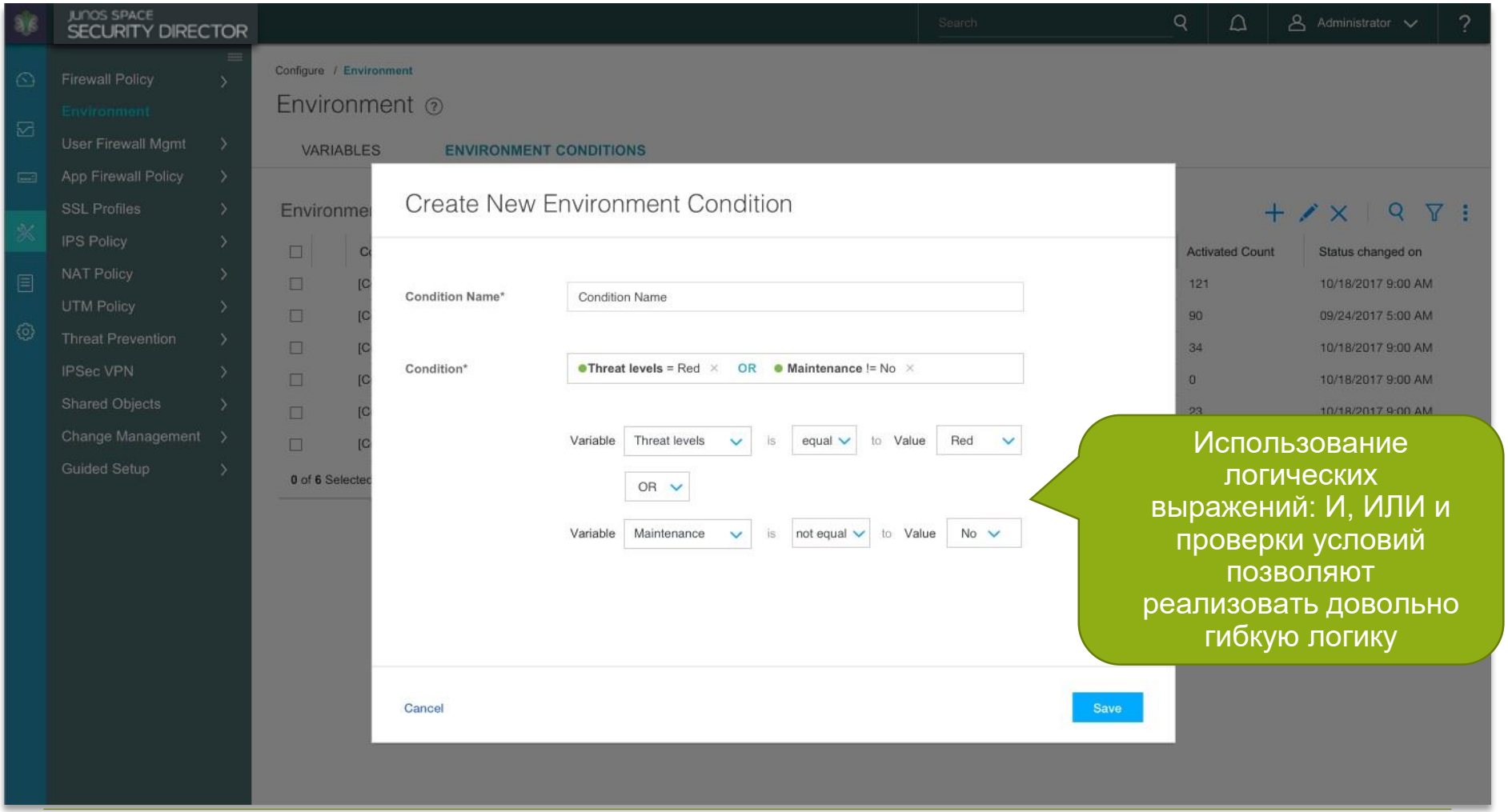
Микро-сегментация

- Синхронизация инвентори и тэгов безопасности в Contrail с vSRX
- Политики безопасности vSRX на основе тэгов (мета-данных)
- Политики безопасности в SDSN для vSRX (L7, IPS и т.д.)

ДИНАМИЧЕСКИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ

Срабатывание правил позволяет динамически изменять настройки политик безопасности

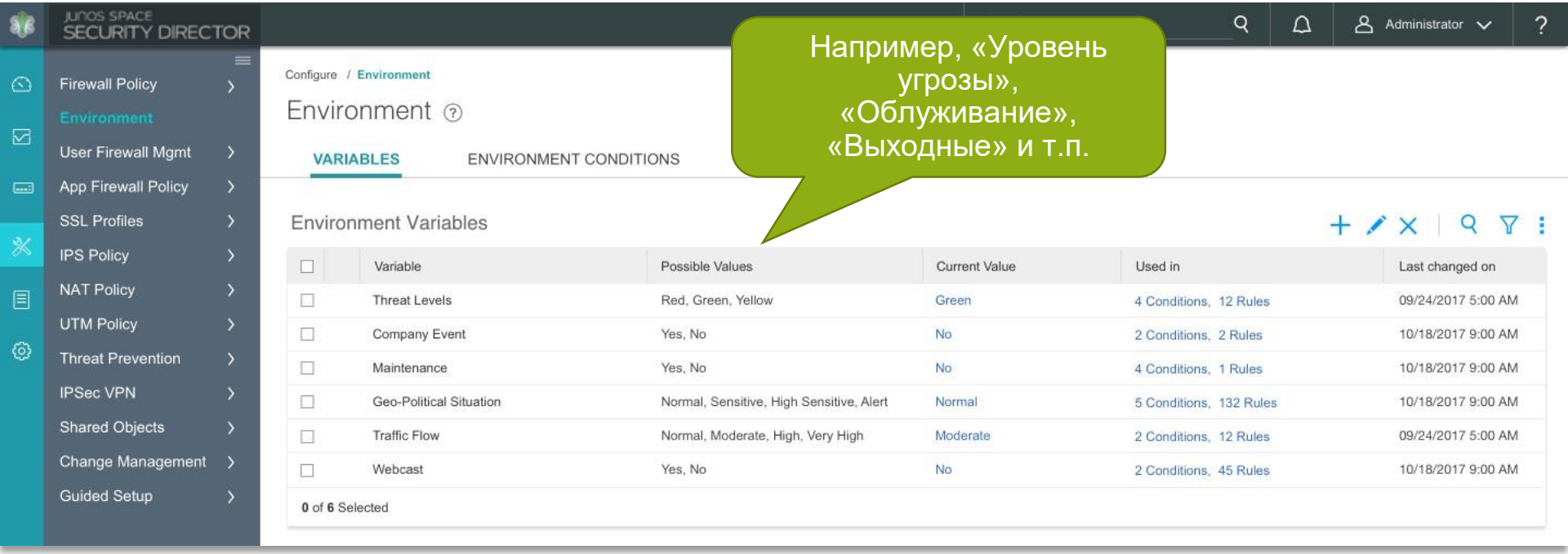




ДИНАМИЧЕСКИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ

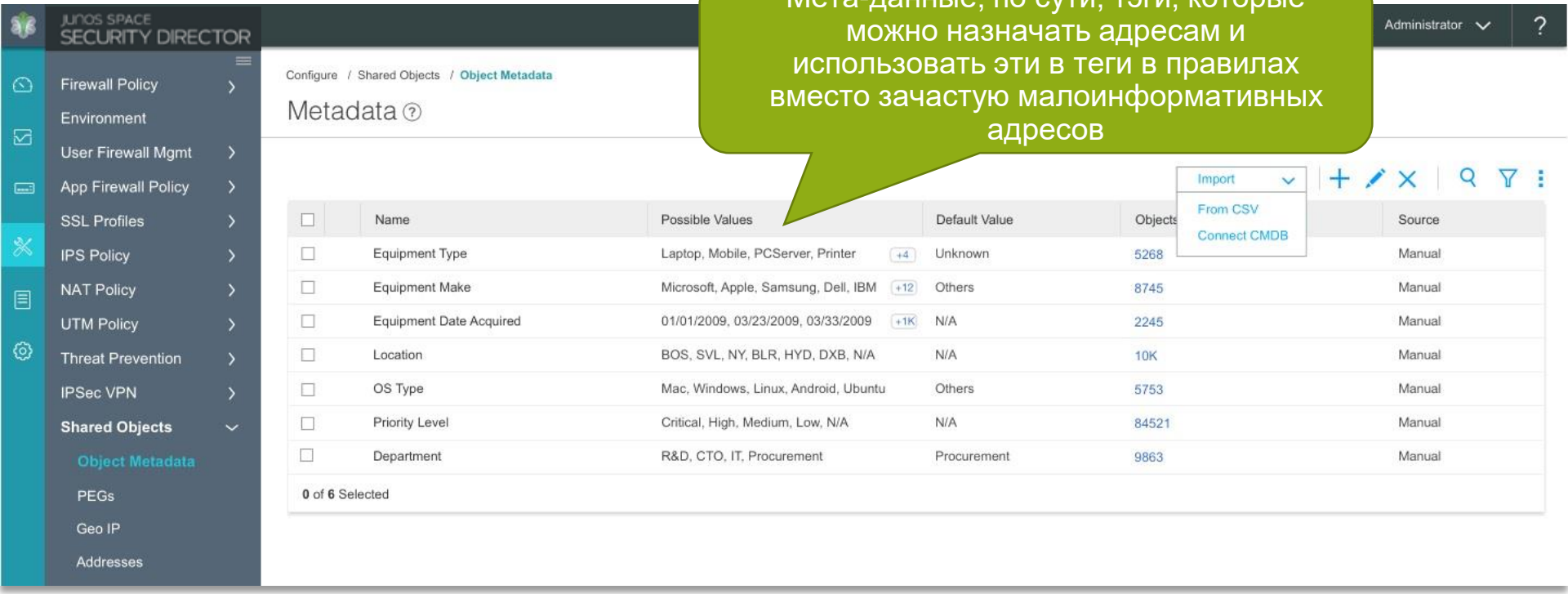
Администратор имеет возможность создать собственные переменные (на слайде примеры).

Изменение значений переменных: вручную или автоматизировано (API)

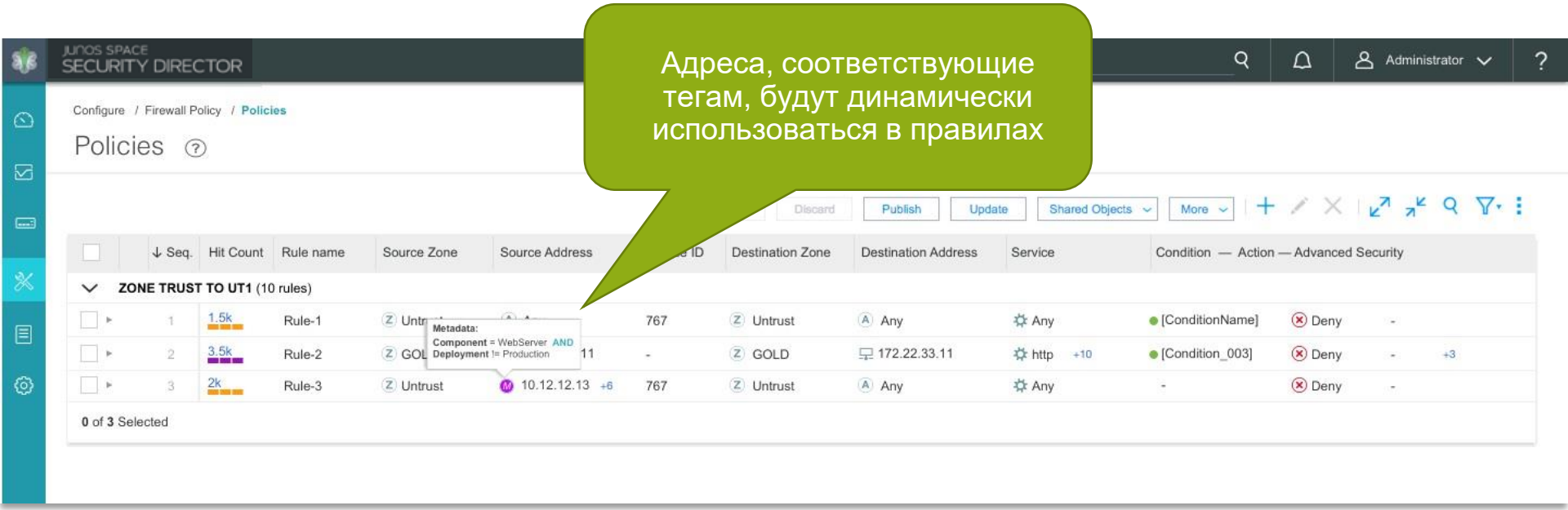


АДРЕСНЫЕ КНИГИ НА ОСНОВЕ МЕТА-ДАННЫХ

Мета-данные, по сути, тэги, которые можно назначать адресам и использовать эти в теги в правилах вместо зачастую малоинформативных адресов



АДРЕСНЫЕ КНИГИ НА ОСНОВЕ МЕТА-ДАННЫХ



Заключение

JUNIPER NETWORKS CONNECTED SECURITY

АНАЛИТИКА, ДЕТЕКТИРОВАНИЕ & НЕЙТРАЛИЗАЦИЯ

- Оперативная защита пользователей, приложений и инфраструктуры от угроз нулевого дня и продвинутых атак
- Анализ угроз на протяжении их жизненного цикла
- Автоматическая/автоматизированная нейтрализация в один клик
- Целостная картина происходящего в традиционной и мультиоблачном окружении
- Данные о том, кто и что находятся в Вашей сети и гранулярный контроль всех точек подключения
- Сквозной контроль и реализация политик безопасности
- Открытая архитектура и набор доступных API

СПАСИБО!

Наш канал на Youtube

JUNIPER NETWORKS | Engineering Simplicity