

# JUNIPER NETWORKS CONNECTED SECURITY

Эшелонированная, автоматизированная  
и интеллектуальная архитектура

Павел Живов

системный инженер, [pzhivov@juniper.net](mailto: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  
(ISC<sup>2</sup>)

## IoT РАСШИРЯЕТ ПЛОЩАДЬ АТАК

**75.4 миллиардов** подключенных устройств к 2025  
(Statista)

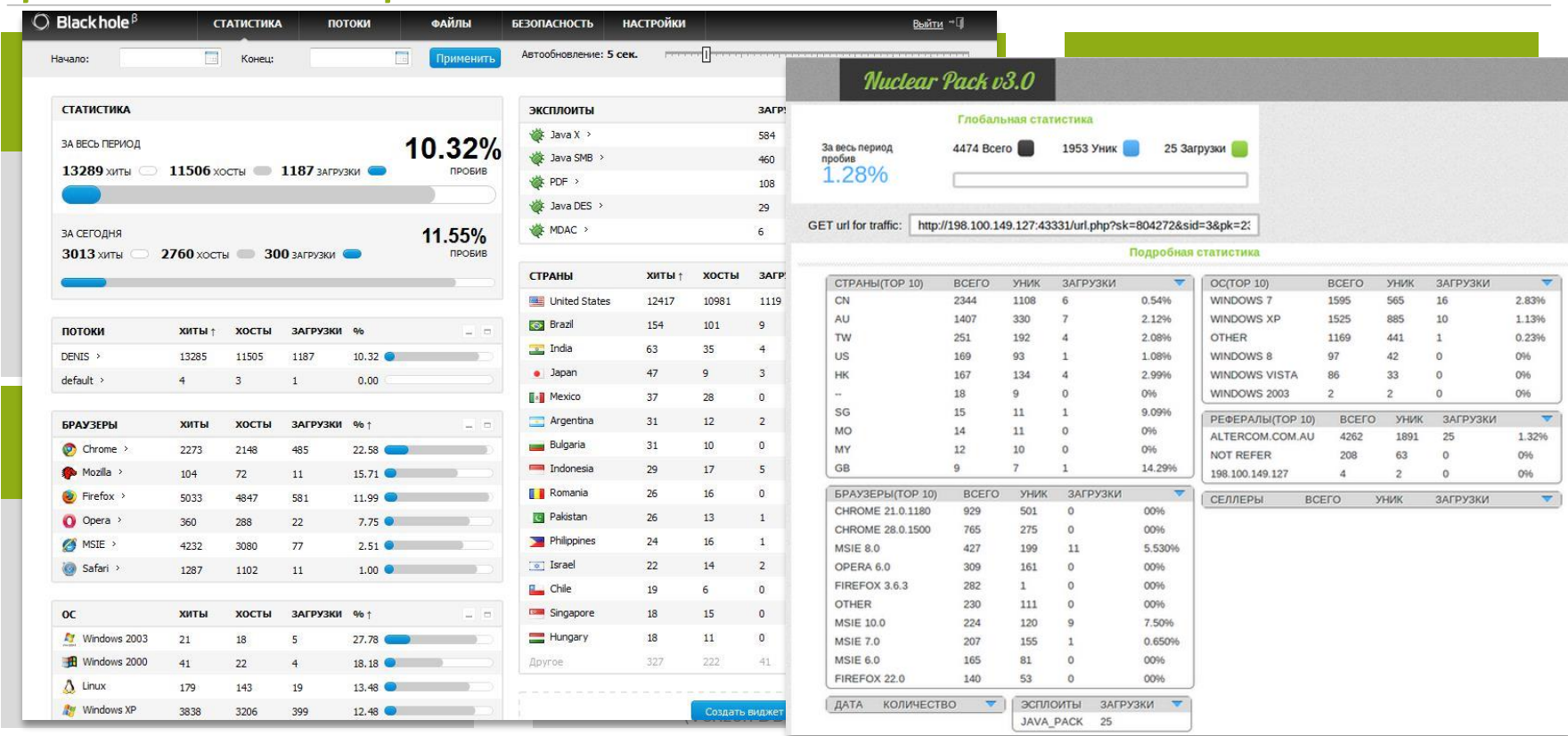
## УГРОЗЫ СТАНОВЯТСЯ БОЛЕЕ ИЗОЦТРЕННЫМИ

**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

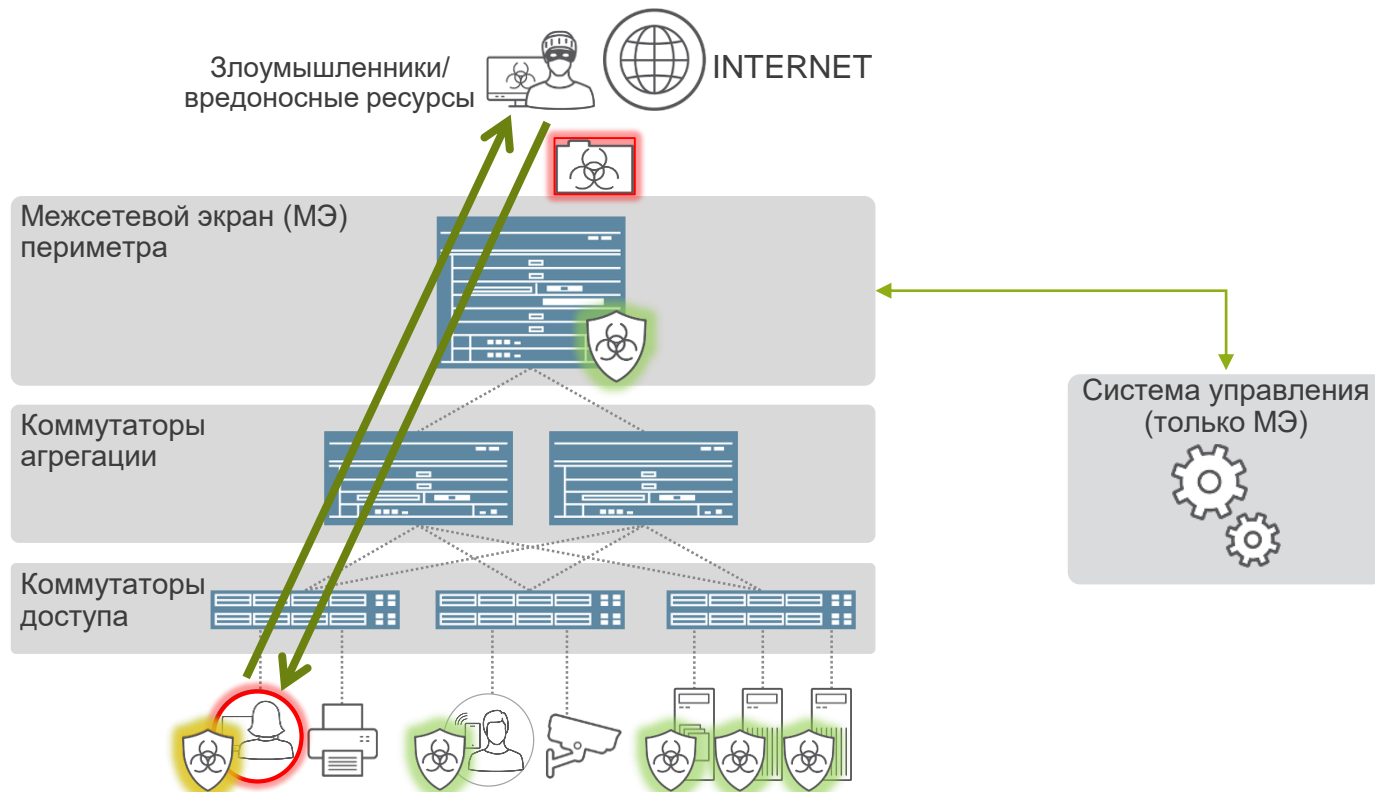


# БЕСФАЙЛОВЫЕ АТАКИ

---

- 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 ВРЕДНОСНЫЙ 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

DEA-1703102203.doc

Analyzed on March 9th 2017 08:00:30 (CEST) running the *Kernelmode* monitor and action script *Heavy Anti-Evasion*  
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1, Office 2010 v14.0.4  
Report generated by VxStream Sandbox v6.20 © Payload Security

malicious

Threat Score: 88/100

AV Multiscan: 16%

Labeled as: Macro.Agent

Sample (109KiB) Downloads VirusTotal Report Re-analyze

Tweet E-Mail

## Incident Response

AV Multiscan: 16%

### Risk Assessment

<b>Persistence</b>	Modifies auto-execute functionality by setting/creating a value in the registry Spawns a lot of processes
<b>Fingerprint</b>	Found a dropped file containing the Windows username (possible fingerprint attempt) Reads the active computer name Reads the cryptographic machine GUID Reads the windows installation date
<b>Evasive</b>	Executes WMI queries known to be used for VM detection
<b>Network Behavior</b>	Contacts 1 host. View the <a href="#">network section</a> for more details.

# БЕСФАЙЛОВЫЙ ВРЕДНОСНЫЙ КОД. ПРИМЕР (2/3)

## Пример атаки. Доставка и запуск




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

SHA256: 12a7898fe5c75e0b57519f1e7019b5d09f5c5cbe49c48ab91daf6cc09ee8a30

File name: court.doc

Detection ratio: 9 / 56

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



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.AgentLAP	20170308
F-Secure	Trojan:W97M/MaliciousMacro.GEN	20170308
Fortinet	WM/Agent.AP!tr.ddd	20170308
Qihoo-360	heur.macro.powershell.x	20170308
ZoneAlarm by Check Point	HEUR:Trojan-Downloader.Script.Generic	20170308

# БЕСФАЙЛОВЫЙ ВРЕДНОСНЫЙ КОД. ПРИМЕР (3/3)

## Пример атаки. Закрепление и исполнение



The screenshot displays a network traffic capture and a debugger. The top window shows a list of network packets, with the selected packet (No. 51) being an HTTPS request to 138.201.75.227:4432. The bottom window shows the debugger's disassembly view for the file 'rch/stage0.hex'. The assembly code includes instructions like 'dec ebp', 'pop edx', 'call \$+5', 'push edx', 'inc ebp', 'push ebp', 'mov ebp, esp', 'add ebx, 177h', 'call ebx', 'add ebx, 0E805h', and 'mov [ebx], edi'. The right side of the image shows a hex editor view of the file's content, displaying hexadecimal data and its corresponding ASCII representation, including headers like 'HTTP/1.1 200 OK' and 'Content-Type: application/octet-stream'.



# ТРАДИЦИОННАЯ ИНФРАСТРУКТУРА СЕГОДНЯ

## Традиционная модель UNTRUST / TRUST

Типичный сценарий для этой модели

Злоумышленники/  
вредоносные ресурсы   INTERNET

Межсетевой экран (МЭ)  
периметра



Коммутаторы  
агрегации



Коммутаторы  
доступа



Система управления  
(только МЭ)



  
СЕТЬ ПРЕДПРИЯТИЯ

# ВРЕДНОС НАУЛЕВОГО ДНЯ ПРОТИВ JUNIPER CONNECTED SECURITY

Злоумышленники/  
вредоносные ресурсы  INTERNET

Межсетевой экран (МЭ)  
периметра



Коммутаторы  
агрегации



Коммутаторы  
доступа



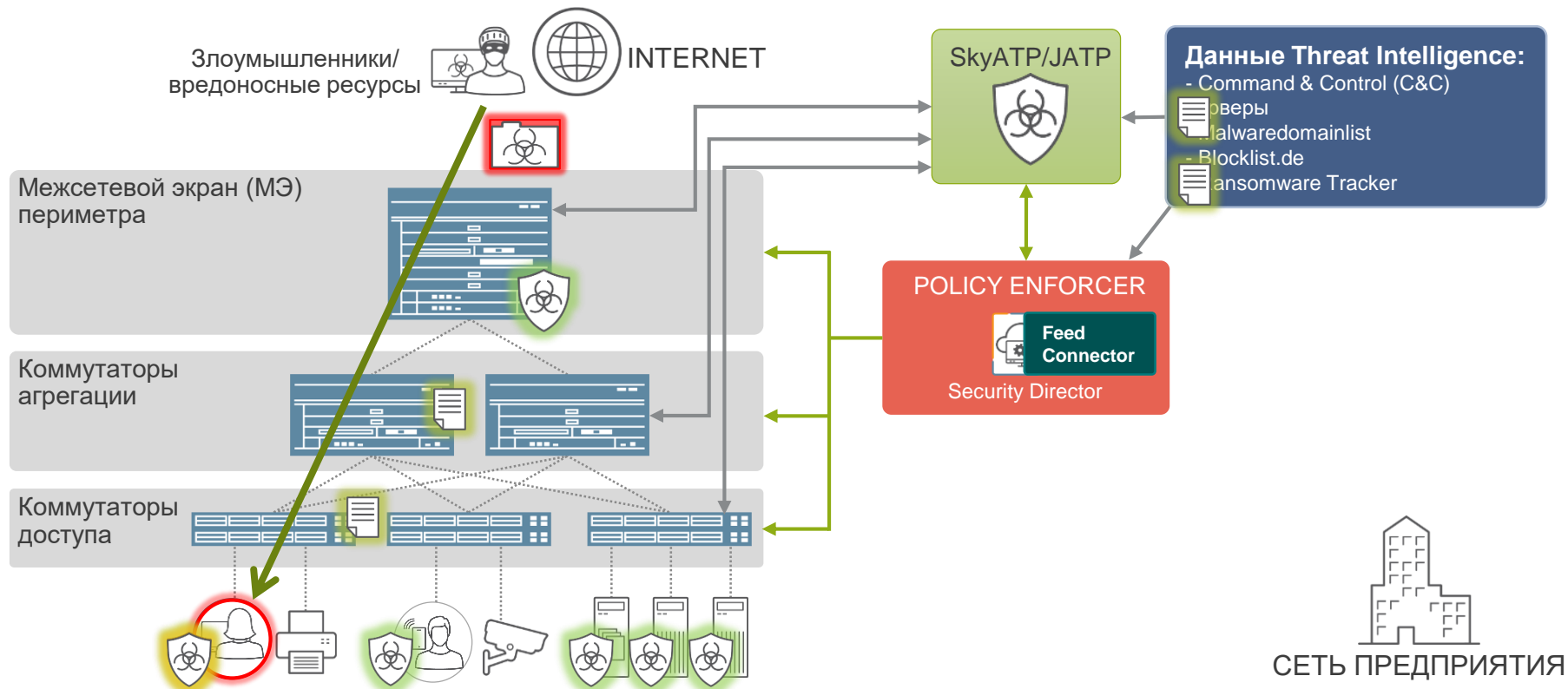
Анализ трафика системой  
предотвращения вторжений

Данные о коммуникациях с С&С  
серверами

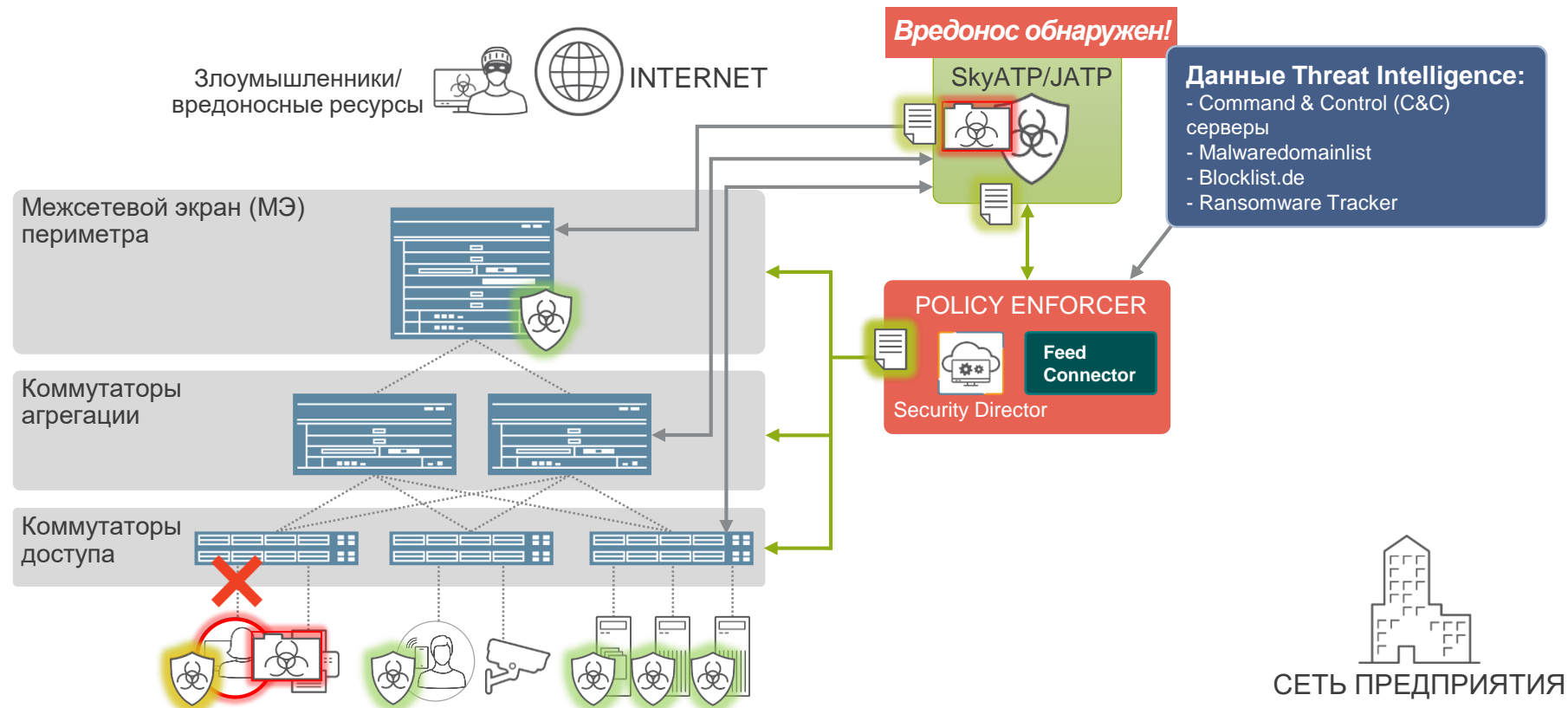
Сбор и анализ данных на уровне сети  
(например, коллектор JATP)

Сбор и анализ данных с агентов и  
других сторонних продуктов

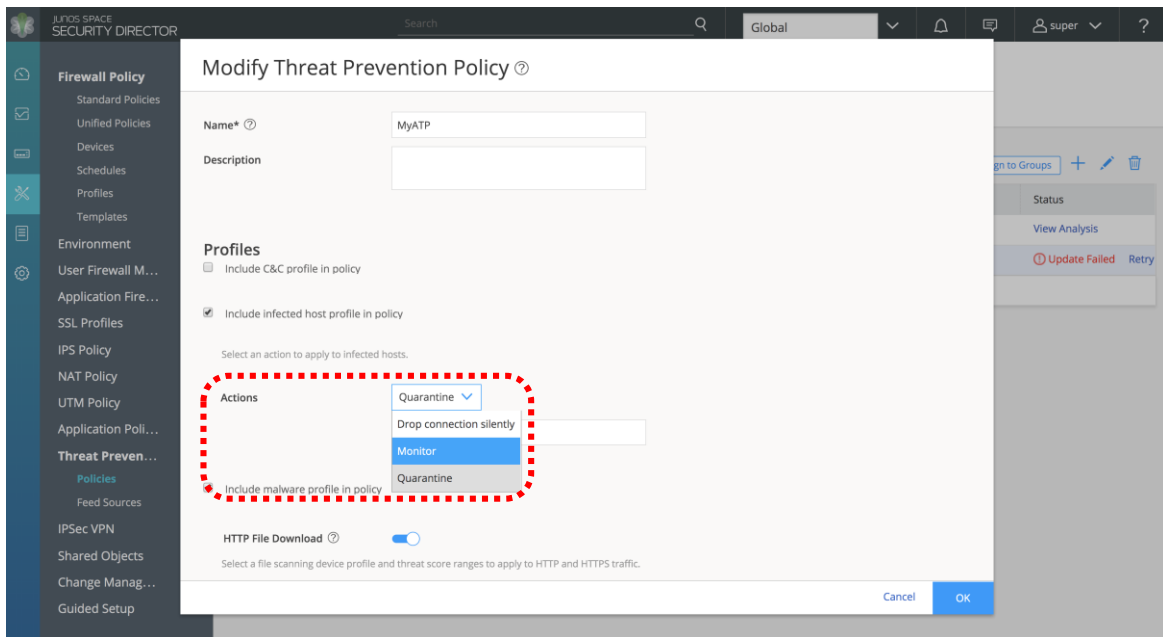
# ВРЕДНОС НУЛЕВОГО ДНЯ ПРОТИВ JUNIPER CONNECTED SECURITY



# ВРЕДНОС НУЛЕВОГО ДНЯ ПРОТИВ JUNIPER CONNECTED SECURITY

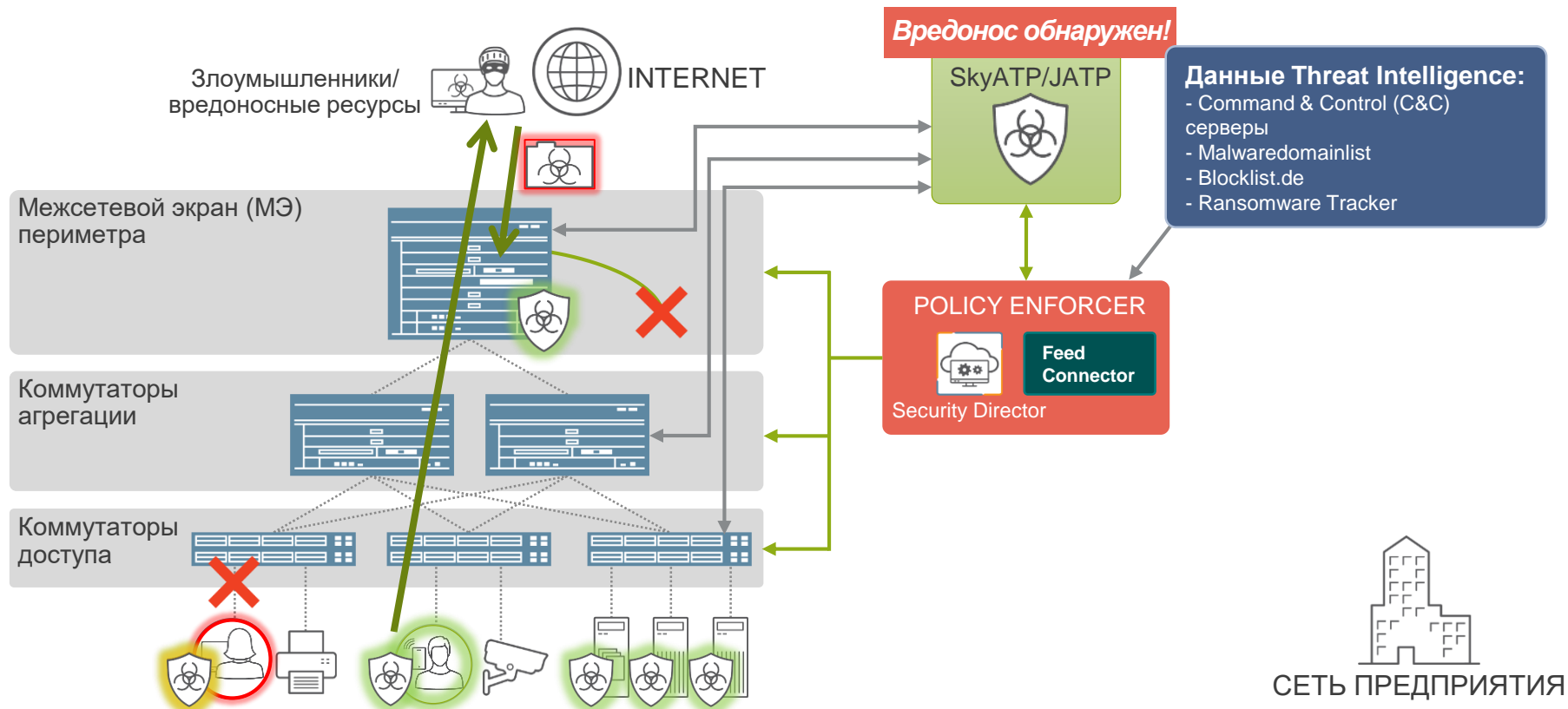


# ДЕЙСТВИЯ НАД ИНФИЦИРОВАННЫМИ УЗЛАМИ

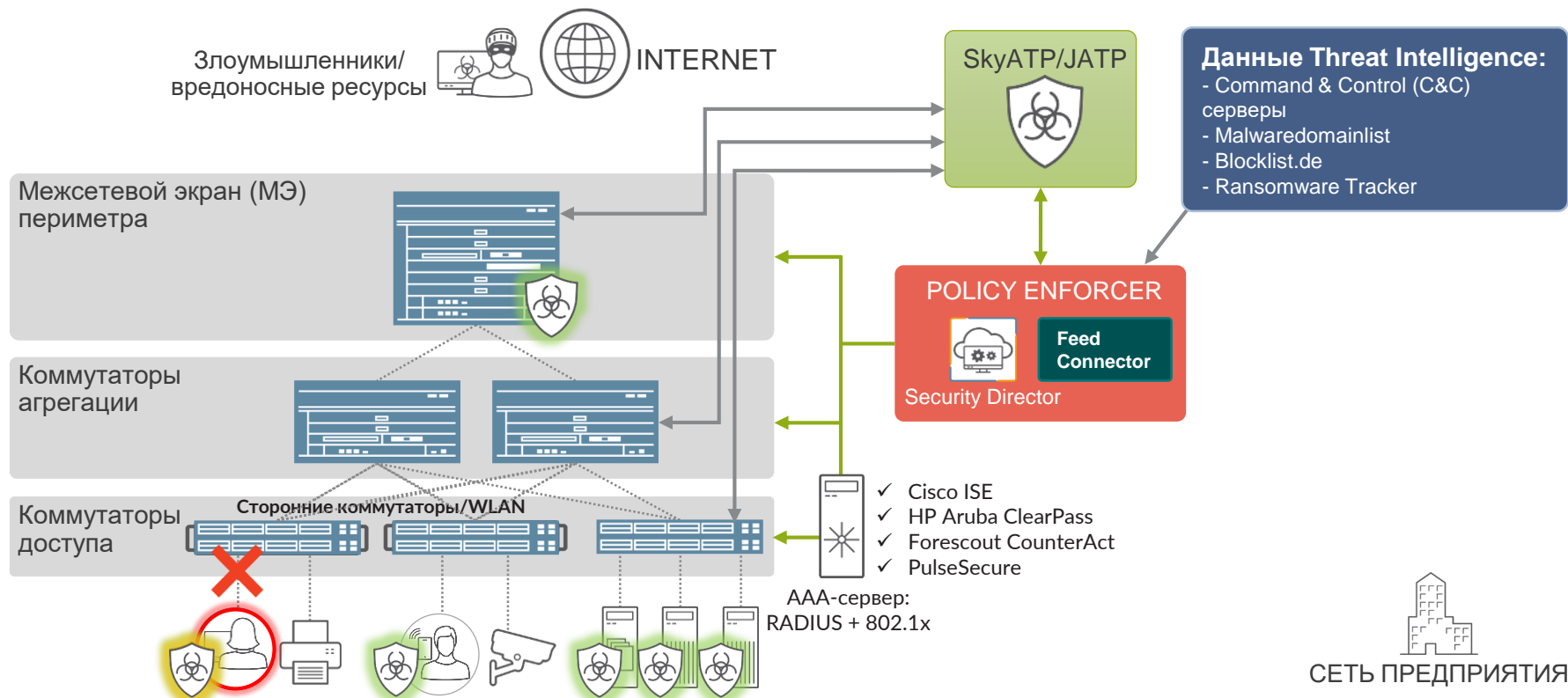


- Блокировать, Переводить в карантин и Мониторить
- Администратор получает уведомление об инфицировании и информацию о точке подключения зараженного узла: порт коммутатора, точка доступа WiFi...
- Режим мониторинга особенно актуален там, где нельзя блокировать узлы, например, роботы на линии сборки или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

# ВРЕДНОС 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

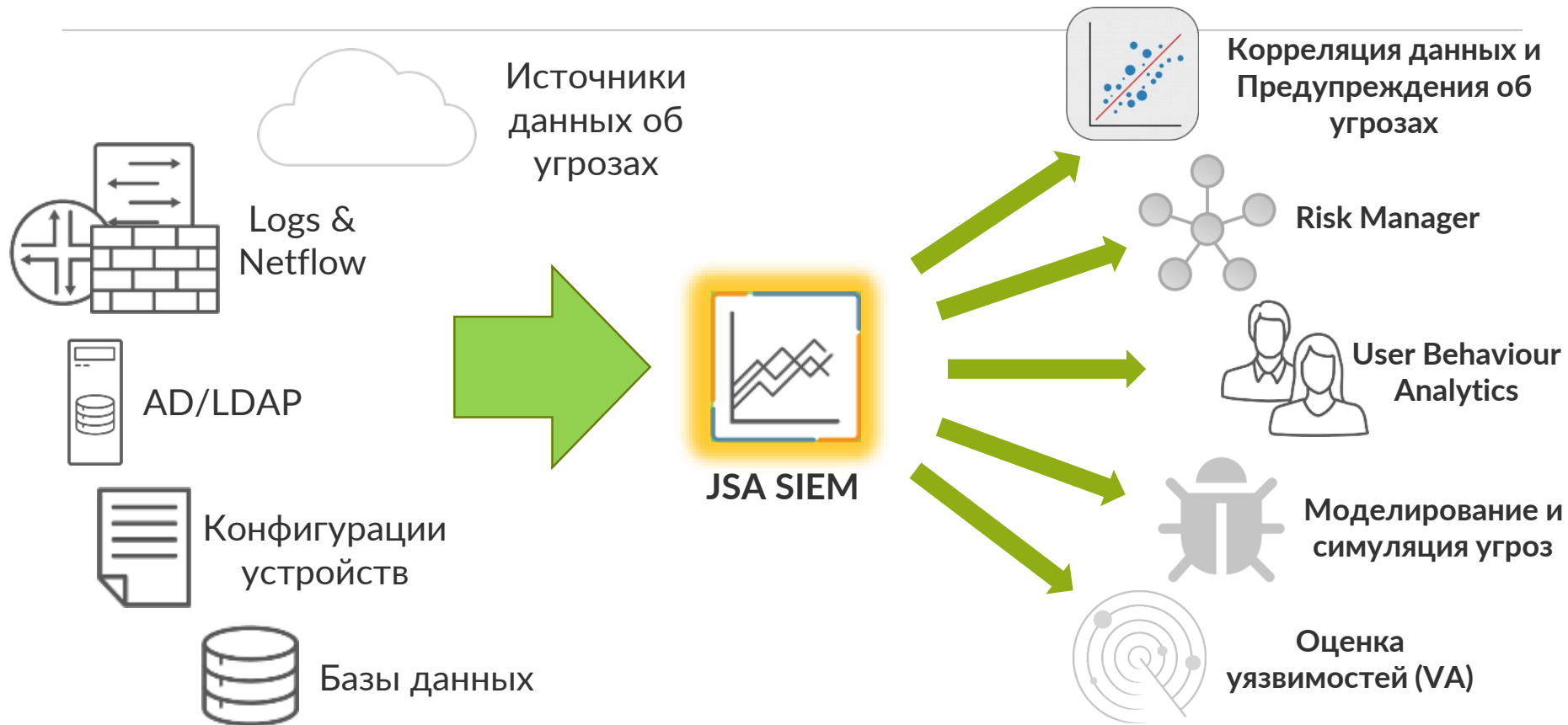






# Видеть и Знать

# 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

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health J-ATP Admin

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Notifications System Profiles Environmental Settings Email Mitigation Settings Firewall Mitigation Settings Asset Value Anti-Virus Configuration Endpoint Integration Settings BlueCoat Configuration Whitelist Rules YARA Rule Upload SNORT Rule Upload Identity Configuration Splunk Configuration External Event Collectors Custom External Collectors

Source Type:  
 Firewall  
 Web Gateway  
 Endpoint AV  
 Endpoint Response

Vendor Name:  
 pan-new  
 PAN Next Gen Firewall

Transport:  
 Log Collector  
Log Source Identifier:  
PA-TEST  
SSL:  
 Enabled  
 Disabled

Default Severity:  
 Max  
 High  
 Med  
 Low  
 Benign

Create Incident:  
 Enabled  
 Disabled

Save

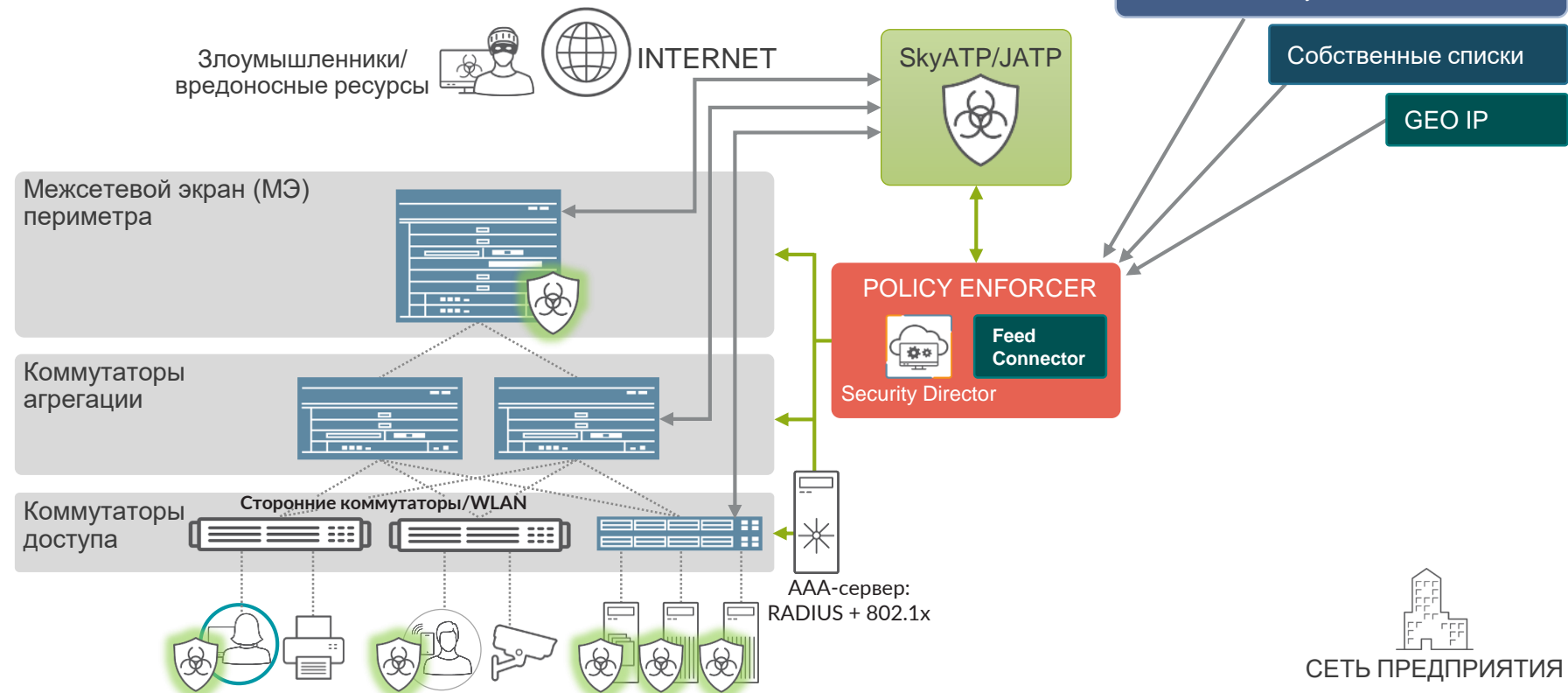
Cancel

Current Third Party Sources

Category	Vendor	Transport	Details	Actions
Firewall	pan-new	Log Collector	Log Source Identifier: PA-TEST	<a href="#">Delete</a> <a href="#">Edit</a> Counters <a href="#">Delete Events</a>
Endpoint AV	ESET	Log Collector	Log Source Identifier: ESETAVENT01.LAD.SANNET.GOV	<a href="#">Delete</a> <a href="#">Edit</a> Counters <a href="#">Delete Events</a>
Endpoint AV	Symantec EP	Log Collector	Log Source Identifier: ATA-SYMANTEC-MANAGER	<a href="#">Delete</a> <a href="#">Edit</a> Counters <a href="#">Delete Events</a>
Firewall	PAN Next Gen Firewall	Log Collector	Log Source Identifier: PA-200	<a href="#">Delete</a> <a href="#">Edit</a> Counters <a href="#">Delete Events</a>

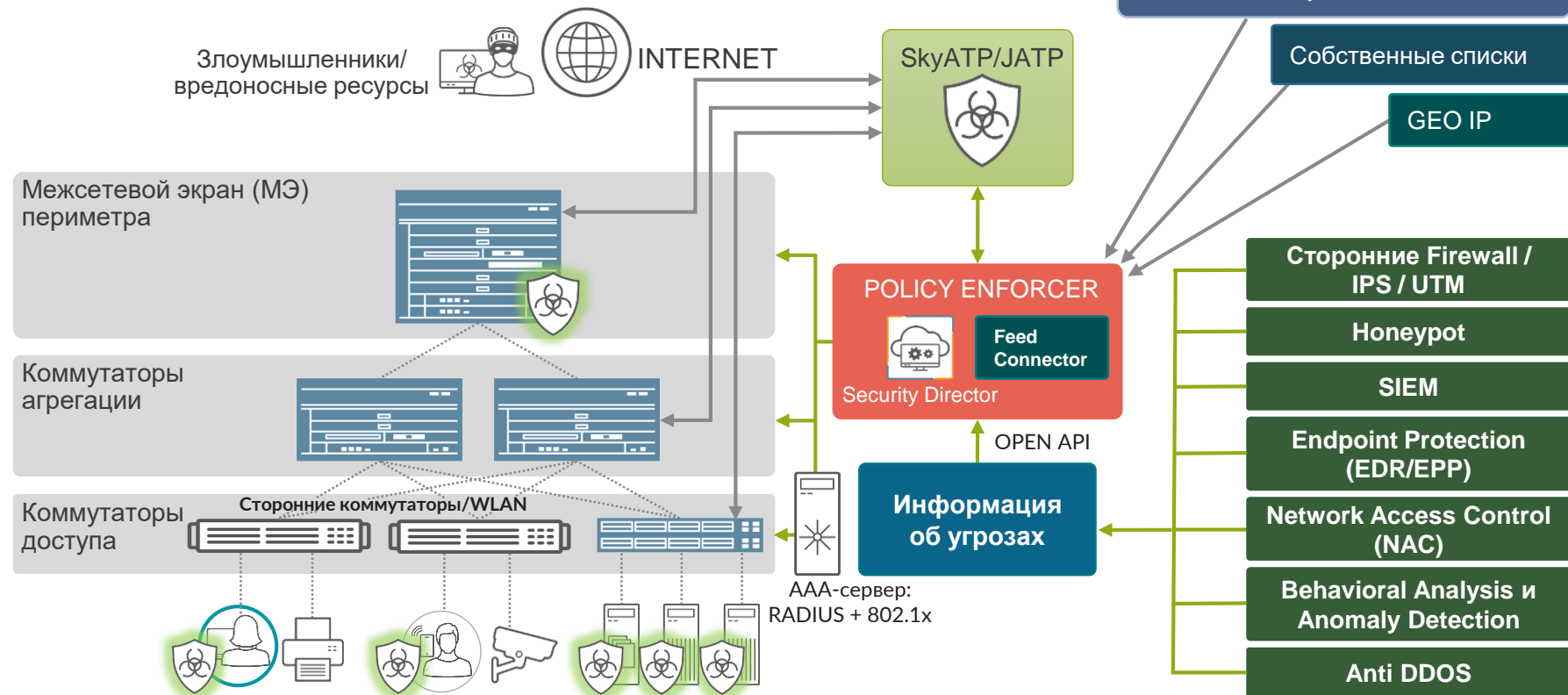


# ДАННЫЕ THREAT INTELLIGENCE





# 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
<ul style="list-style-type: none"><li>• Добавлять/удалять IPv4/v6, URL и FQDN в C&amp;C фиды</li><li>• До 30 собственных фидов</li><li>• Черные/белые списки</li></ul>	<ul style="list-style-type: none"><li>• Поиск образцов по хэшу</li><li>• Передача образцов для анализа</li><li>• Параметры для получения детального отчета</li></ul>	<ul style="list-style-type: none"><li>• Доступны также и в UI</li><li>• Модификация значений через API</li></ul>	<ul style="list-style-type: none"><li>• Фид зараженных узлов, которые необходимо заблокировать на уровне сети (доступ, фаерволы, маршрутизаторы)</li></ul>

# ДАННЫЕ ОБ УГРОЗАХ ИЗ ЛЮБЫХ ИСТОЧНИКОВ

The screenshot shows the 'Create Infected-Hosts Feed' configuration page in the Juniper Security Director. The page is titled 'Create Infected-Hosts Feed' and is part of the 'Custom Feeds' configuration under 'Threat Prevention'. The form includes the following fields:

- Name \***: MyFeed
- Description**: Write description..
- Type of server url \***:  http,  https
- Server File URL \***: http://myfeedserver.juniper.net
- Username**: admin
- Password**: .....
- Update Interval \***: Hourly (selected), Daily, Weekly, Monthly, Never

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>

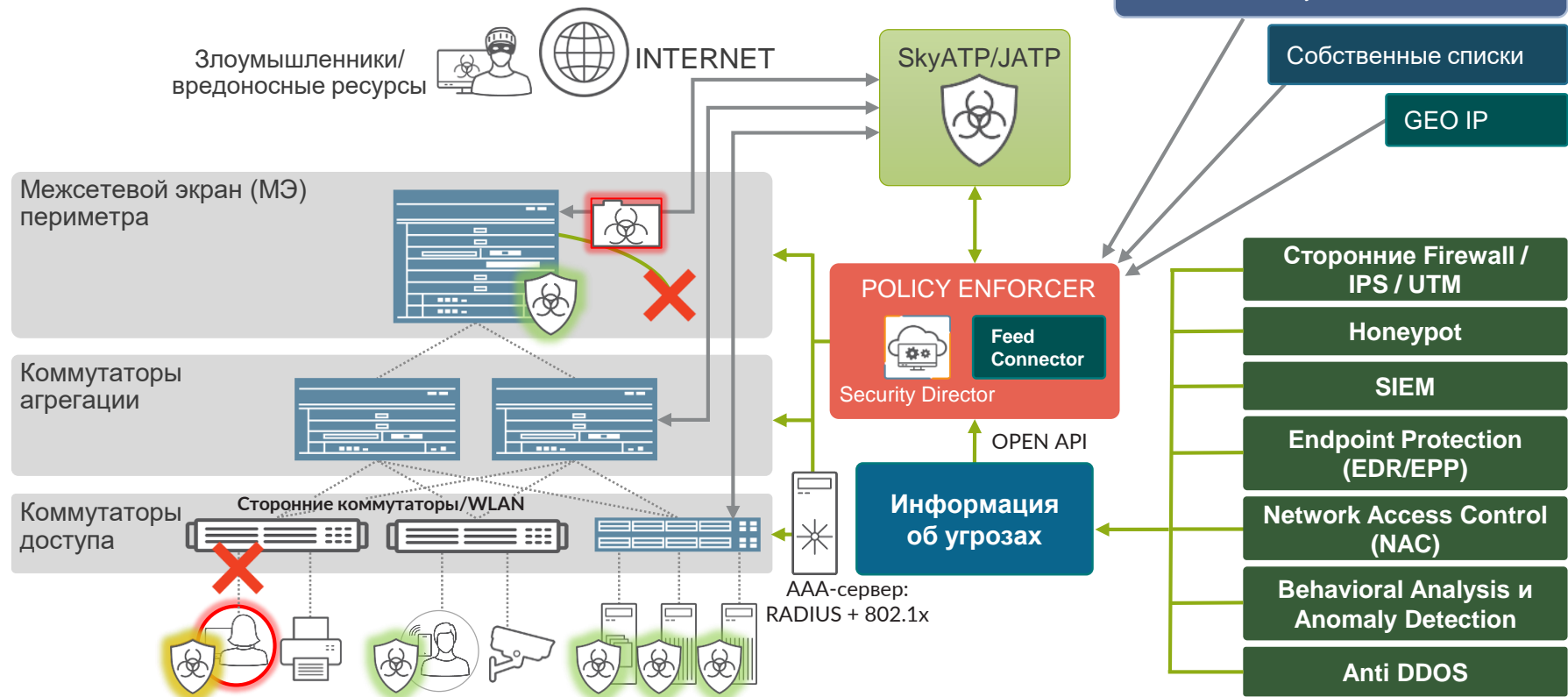
Body:

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



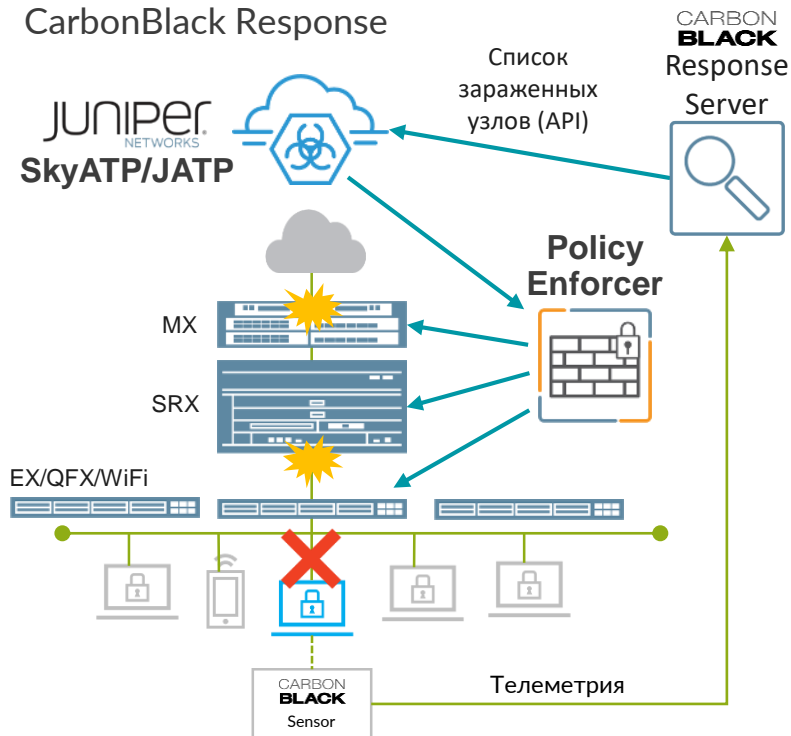
# Действовать и Защищать

# ОТКРЫТАЯ ПЛАТФОРМА



# ИЗОЛЯЦИЯ ЗАРАЖЕННОГО УЗЛА. EDR -> ATP

Использование информации об угрозах из CarbonBlack Response



## Сценарий использования

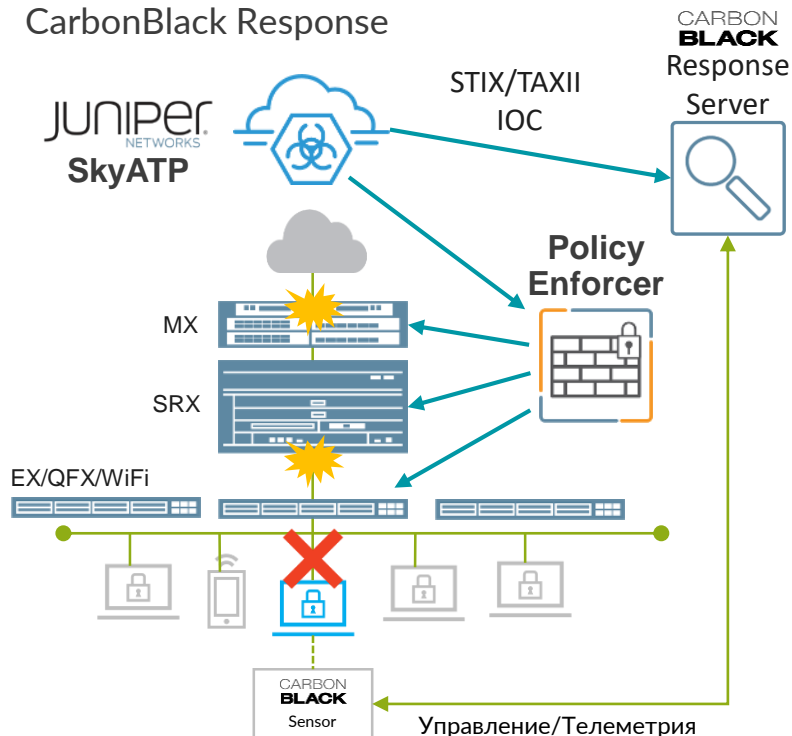
- CB Response детектирует наличие угрозы на оконечном узле и отправляют информацию об IP-адресе в SkyATP/JATP через API,
- SkyATP/JATP добавляет IP-адрес узла в Список зараженных узлов и уведомляет Policy Enforcer,
- Сеть блокирует зараженный узел

## 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



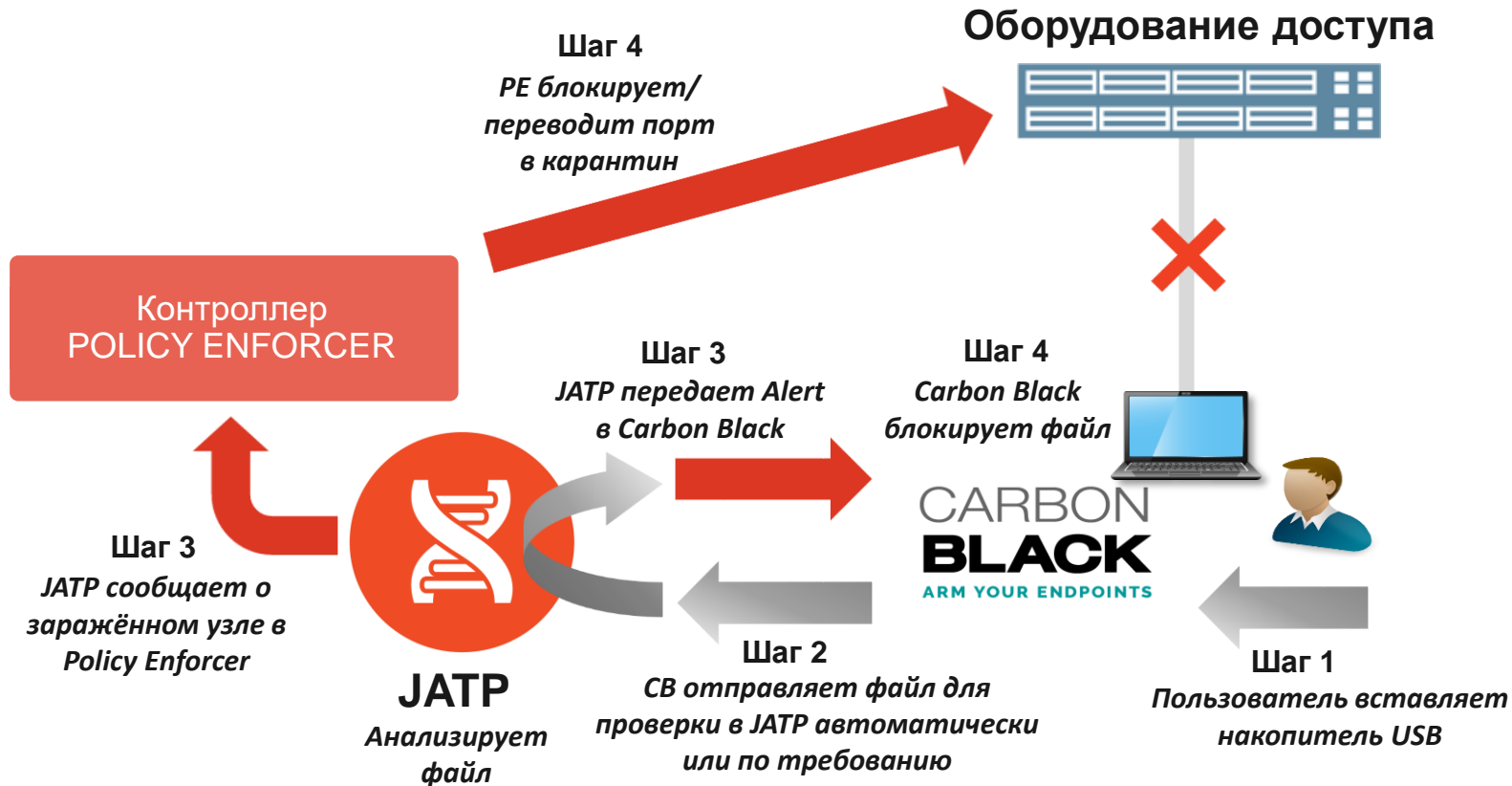
## Сценарий использования

- SkyATP детектирует наличие угрозы на конечном 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

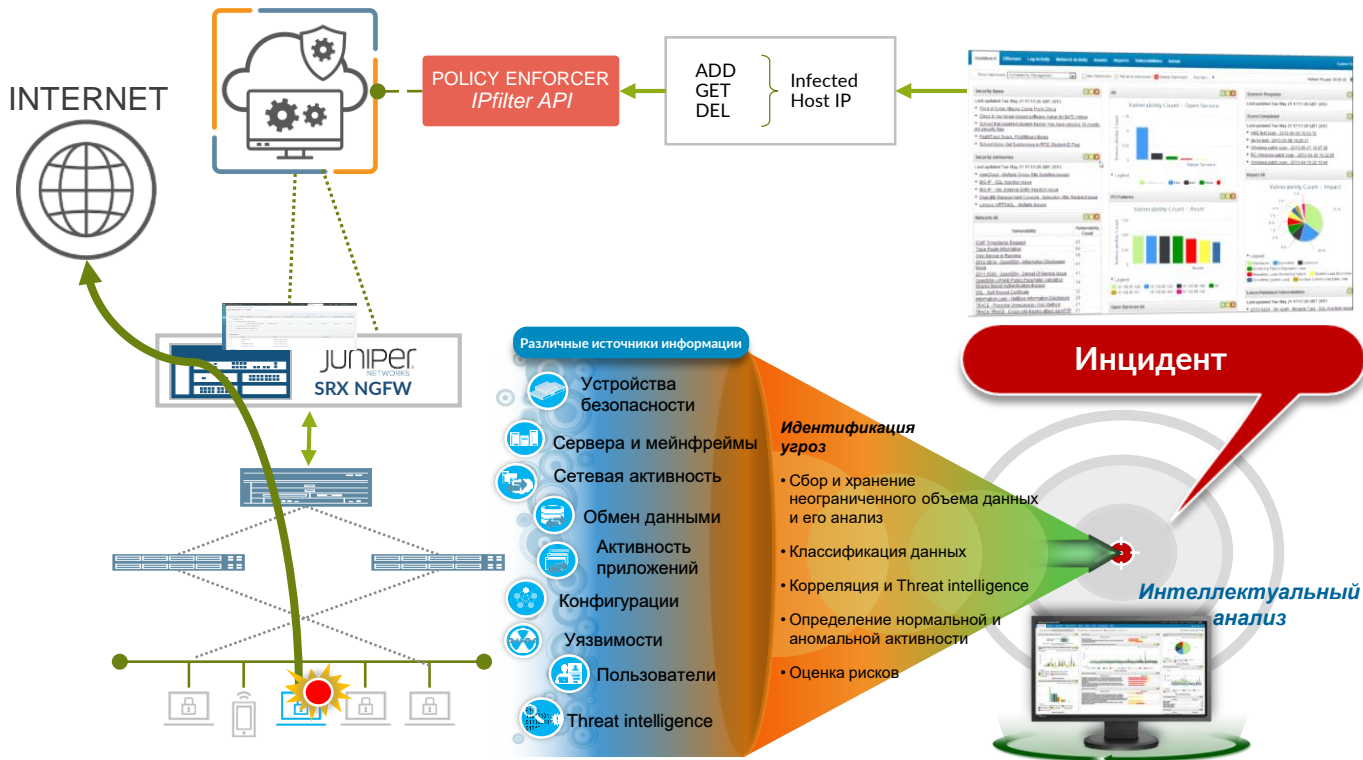
- Предотвращение заражения других узлов в сети
- Совместное использование данных об угрозах для идентификации зараженных узлов и защиты сети
- Данные о состоянии узлов сети

# ДЕТЕКТИРОВАНИЕ ВРЕДНОСНОГО 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 МХ КАК УСТРОЙСТВА ПЕРИМЕТРА В SECURE FABRIC

## Преимущество

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

## Как это работает

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

Add Enforcement Points ⓘ

Assigning a device to the site will cause a change in the device configuration.

Specify the enforcement points to assign to the site. The site cannot contain both switches and connectors.

Enforcement Points

15 Available

Name	IP	Model
<input type="checkbox"/> vsrx-06	172.19.101.166	VSRX
<input type="checkbox"/> SRX210H	172.19.100.239	SRX240H
<input type="checkbox"/> vsrx-04	172.19.101.128	VSRX
<input type="checkbox"/> tmetestsw01	172.19.100.33	EX4300-48P
<input type="checkbox"/> vsrx-srini-187.D...	10.92.82.187	VSRX
<input type="checkbox"/> skunk	172.19.100.27	MX80-T

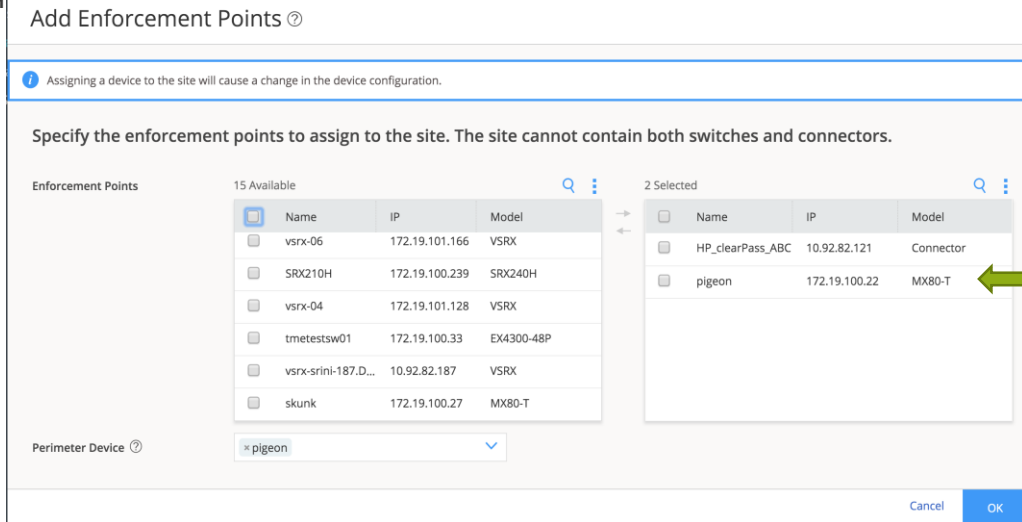
2 Selected

Name	IP	Model
<input type="checkbox"/> HP_clearPass_ABC	10.92.82.121	Connector
<input checked="" type="checkbox"/> pigeon	172.19.100.22	MX80-T

Perimeter Device ⓘ

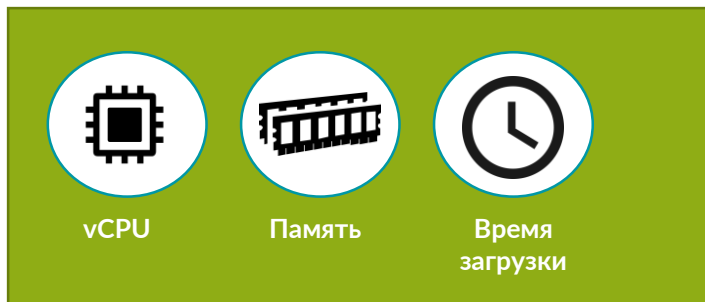
x pigeon

Cancel OK



# ВИРТУАЛЬНЫЕ СРЕДЫ И ОБЛАКА

## Скорость развертывания и размер



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

### vSRX 2.x

- Вложенная 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



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)

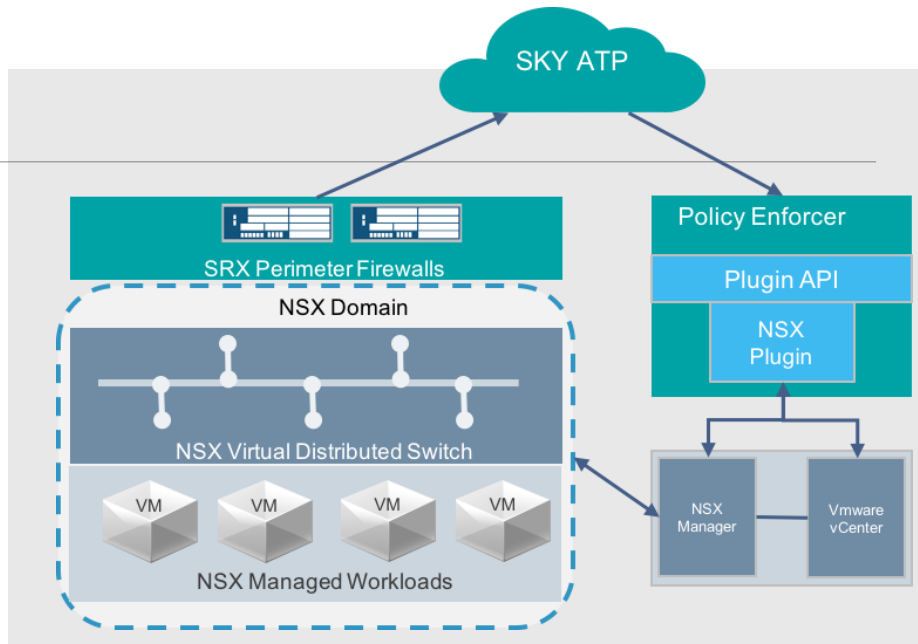
### Threat Prevention Policy

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

### Сертифицировано VMWare

## Ключевой функционал

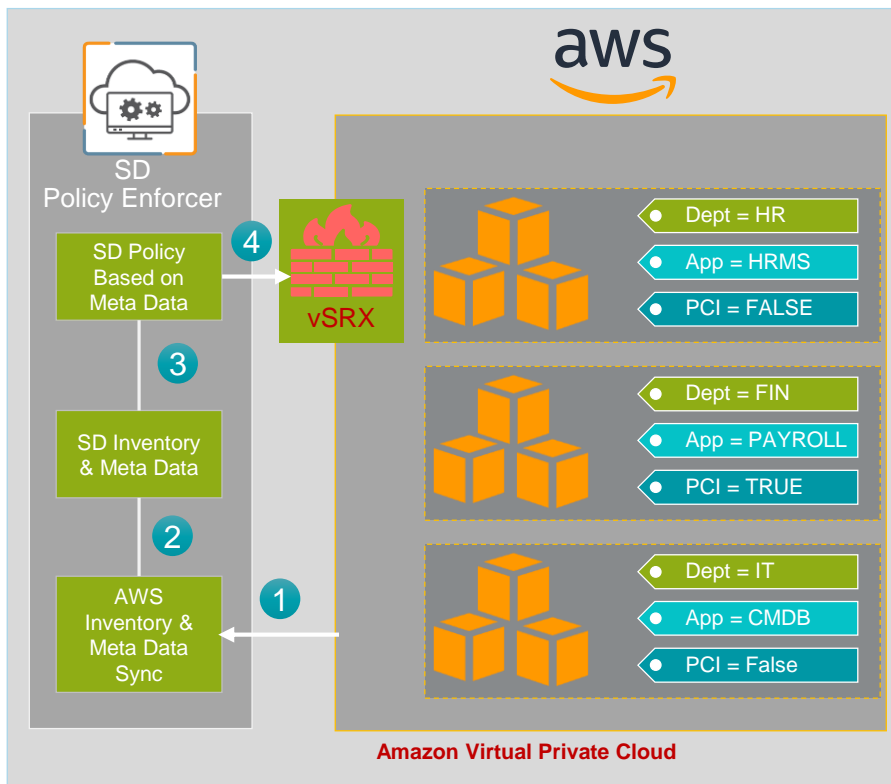
- Security Fabric включает хосты домена NSX
- Синхронизация Групп Безопасности (Security Group)  
Группы безопасности NSX и членство хостов в группах синхронизируется с Security Director "Dynamic Address Groups"
- Политика Security Director для трафика Север-Юг и Восток-Запад  
SD задает L7/IPS/ATP политику 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



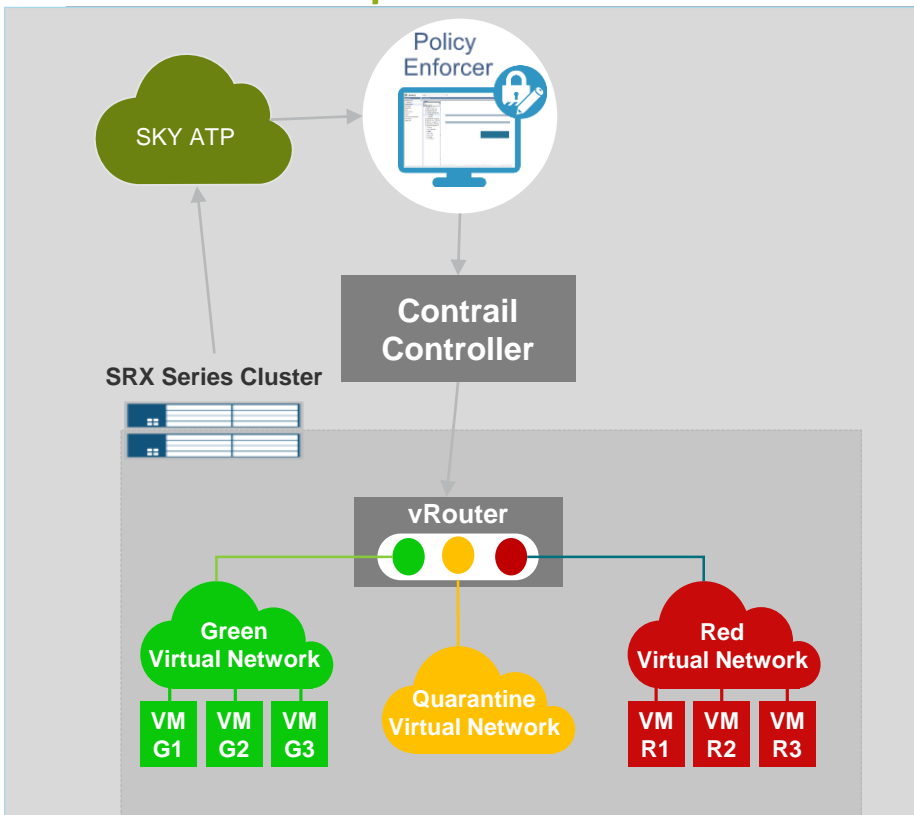
## Решаемые задачи

- 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 безопасности

## Микро-сегментация

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

# ДИНАМИЧЕСКИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ

Срабатывание правил позволяет динамически изменять настройки политик безопасности

Configuration / Firewall Policy / Policies

## Policies

Save Discard Publish Update Shared Objects More

Seq.	Hit Count	Rule name	Source Zone	Source Address	Source ID	Destination Zone	Destination Address	Service	Condition	Action	Advanced Security
▼ ZONE TRUST TO UT1 (10 rules)											
1	1.5k	Rule-1	Untrust	Any	767	Untrust	Any	Any	[ConditionName]	Deny	-
2	3.5k	Rule-2	GOLD	172.22.33.11 172.22.33.12 172.22.33.13	-	GOLD	172.22.33.13	http http-8080 https tcp-5100 tcp-7091 tcp-8101	[Condition_001] [Condition_002] [Condition_003] [Condition_004] -	Permit Deny Deny Permit Permit	IPS: ON - - IPS: ON, UTM: wf-policy -
3	2k	Rule-3	Untrust	Any	767	Untrust	Any	Any	-	Deny	-

0 of 3 Selected



JUNOS SPACE SECURITY DIRECTOR

Configure / Environment

## Environment ?

VARIABLES ENVIRONMENT CONDITIONS

### Create New Environment Condition

Condition Name\*

Condition\* ● Threat levels = Red × OR ● Maintenance != No ×

Variable  is  to Value

Variable  is  to Value

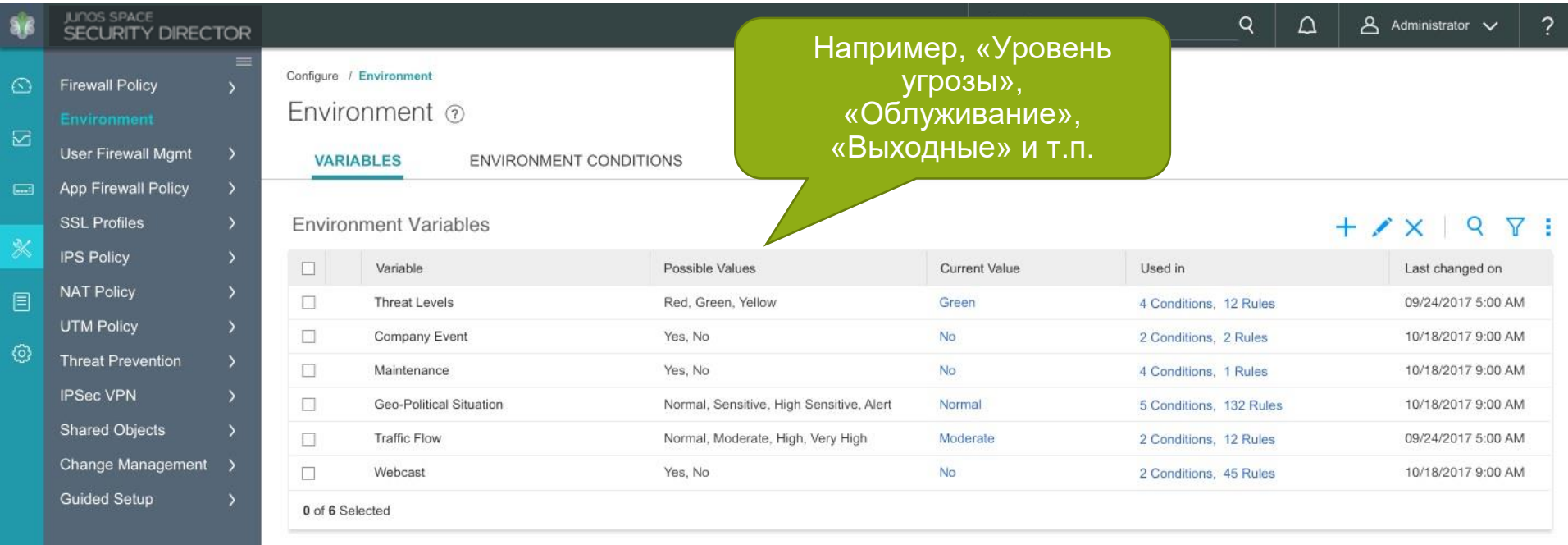
Activated Count	Status changed on
121	10/18/2017 9:00 AM
90	09/24/2017 5:00 AM
34	10/18/2017 9:00 AM
0	10/18/2017 9:00 AM
23	10/18/2017 9:00 AM

Использование логических выражений: И, ИЛИ и проверки условий позволяют реализовать довольно гибкую логику

# ДИНАМИЧЕСКИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ

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

Изменение значений переменных: вручную или автоматизировано (API)



Environment Variables

<input type="checkbox"/>	Variable	Possible Values	Current Value	Used in	Last changed on
<input type="checkbox"/>	Threat Levels	Red, Green, Yellow	Green	4 Conditions, 12 Rules	09/24/2017 5:00 AM
<input type="checkbox"/>	Company Event	Yes, No	No	2 Conditions, 2 Rules	10/18/2017 9:00 AM
<input type="checkbox"/>	Maintenance	Yes, No	No	4 Conditions, 1 Rules	10/18/2017 9:00 AM
<input type="checkbox"/>	Geo-Political Situation	Normal, Sensitive, High Sensitive, Alert	Normal	5 Conditions, 132 Rules	10/18/2017 9:00 AM
<input type="checkbox"/>	Traffic Flow	Normal, Moderate, High, Very High	Moderate	2 Conditions, 12 Rules	09/24/2017 5:00 AM
<input type="checkbox"/>	Webcast	Yes, No	No	2 Conditions, 45 Rules	10/18/2017 9:00 AM

0 of 6 Selected

# 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

Configuration / Shared Objects / Object Metadata

## Metadata ?

<input type="checkbox"/>	Name	Possible Values	Default Value	Objects	Source
<input type="checkbox"/>	Equipment Type	Laptop, Mobile, PCServer, Printer <span>+4</span>	Unknown	5268	Manual
<input type="checkbox"/>	Equipment Make	Microsoft, Apple, Samsung, Dell, IBM <span>+12</span>	Others	8745	Manual
<input type="checkbox"/>	Equipment Date Acquired	01/01/2009, 03/23/2009, 03/33/2009 <span>+1K</span>	N/A	2245	Manual
<input type="checkbox"/>	Location	BOS, SVL, NY, BLR, HYD, DXB, N/A	N/A	10K	Manual
<input type="checkbox"/>	OS Type	Mac, Windows, Linux, Android, Ubuntu	Others	5753	Manual
<input type="checkbox"/>	Priority Level	Critical, High, Medium, Low, N/A	N/A	84521	Manual
<input type="checkbox"/>	Department	R&D, CTO, IT, Procurement	Procurement	9863	Manual

0 of 6 Selected

Import  
From CSV  
Connect CMDB

# АДРЕСНЫЕ КНИГИ НА ОСНОВЕ МЕТА-ДАННЫХ

The screenshot displays the Junos Space Security Director interface. The top navigation bar includes 'Configure / Firewall Policy / Policies'. The main content area shows a table of firewall rules under the heading 'ZONE TRUST TO UT1 (10 rules)'. A callout box points to the 'Source Address' column of the first rule, 'Rule-1', which is 'Untrust'. The callout text reads: 'Адреса, соответствующие тегам, будут динамически использоваться в правилах' (Addresses corresponding to tags will be dynamically used in rules). A tooltip for the 'Untrust' zone shows metadata: 'Component = WebServer AND Deployment != Production'. The table below shows three rules with their respective hit counts, source and destination zones, addresses, services, and actions.

	Seq.	Hit Count	Rule name	Source Zone	Source Address	Source ID	Destination Zone	Destination Address	Service	Condition	Action	Advanced Security	
▼	ZONE TRUST TO UT1 (10 rules)												
<input type="checkbox"/>	1	1.5k	Rule-1	Z Untrust		767	Z Untrust	A Any	Any	[ConditionName]	Deny	-	
<input type="checkbox"/>	2	3.5k	Rule-2	Z GOLD		11	Z GOLD	172.22.33.11	http +10	[Condition_003]	Deny	+3	
<input type="checkbox"/>	3	2k	Rule-3	Z Untrust	10.12.12.13 +6	767	Z Untrust	A Any	Any	-	Deny	-	

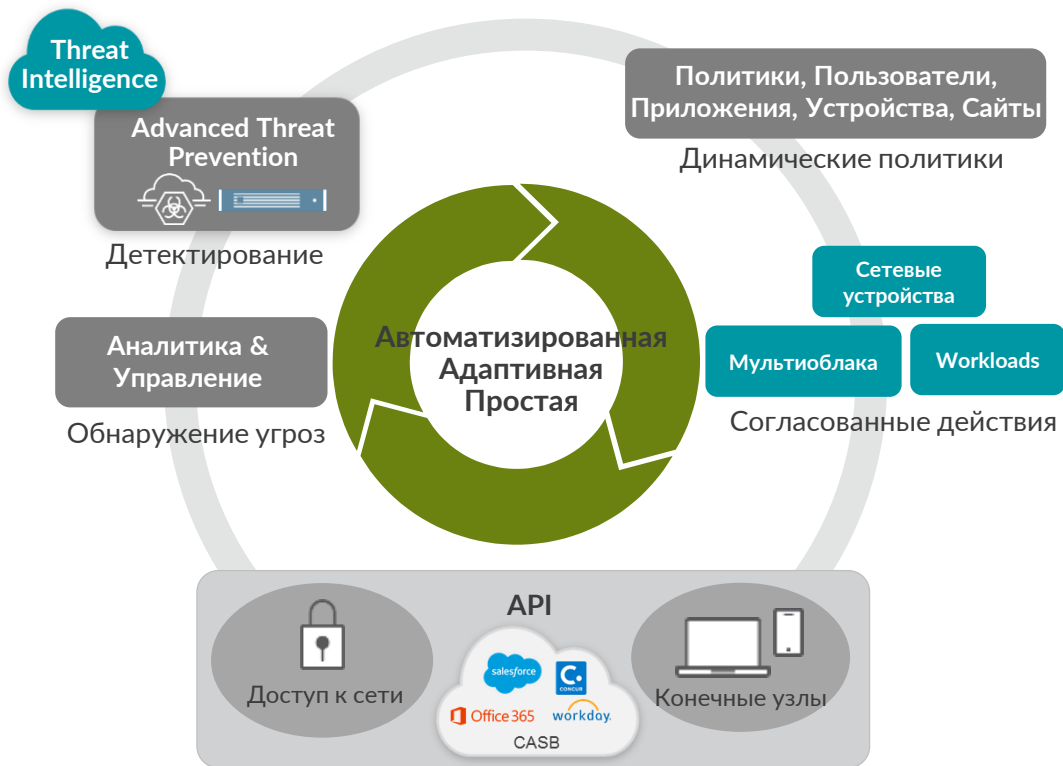
0 of 3 Selected



# 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