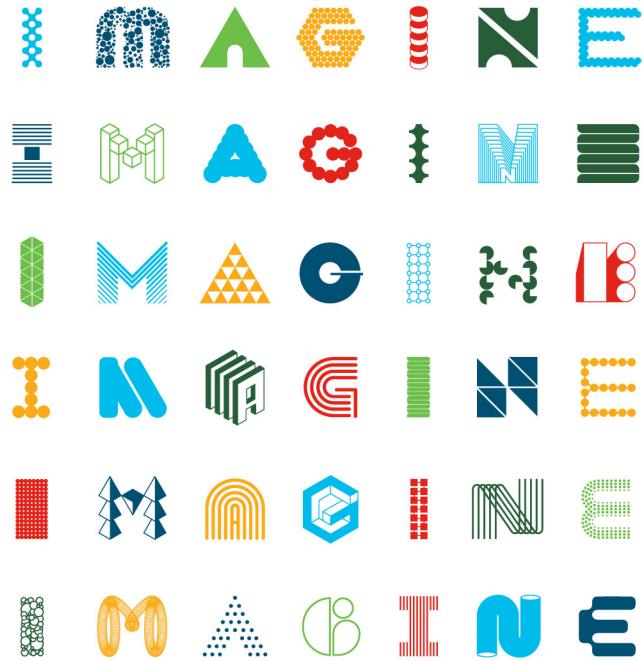




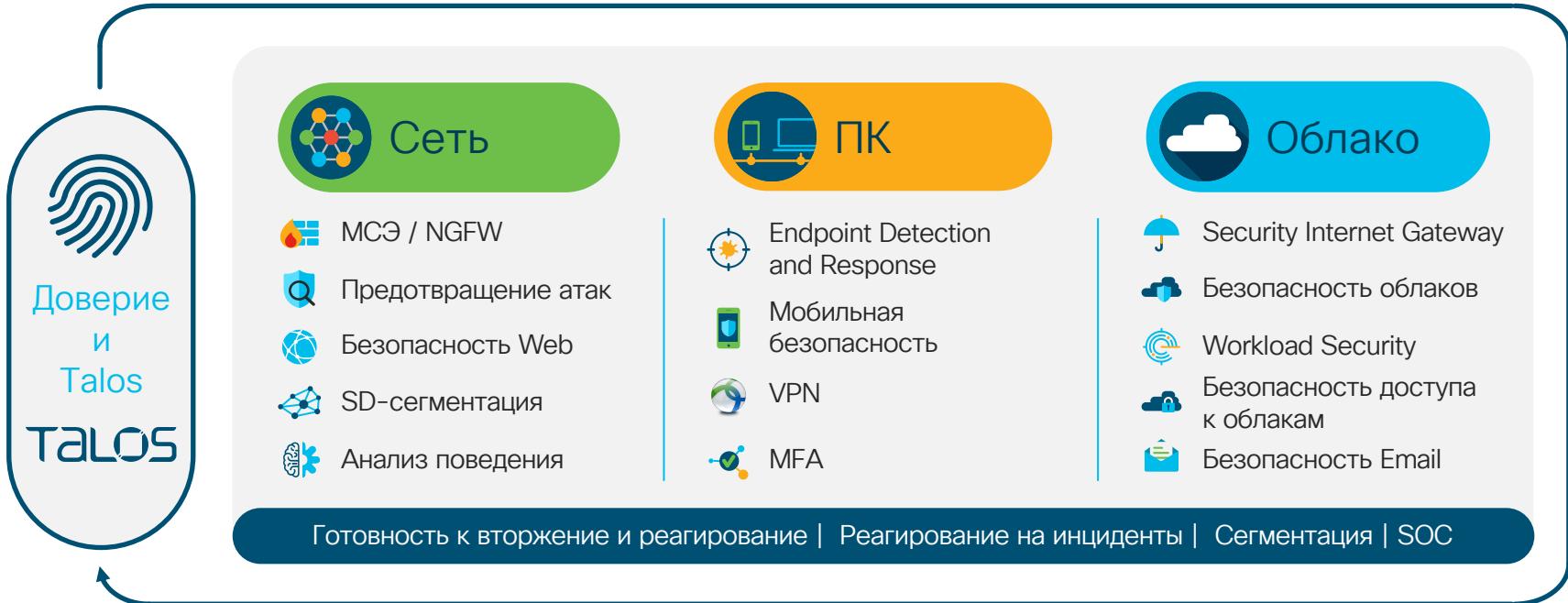
Как превратить вашу сеть в распределенную систему защиты? 7 практических рекомендаций

Лукацкий Алексей, бизнес-консультант по ИБ

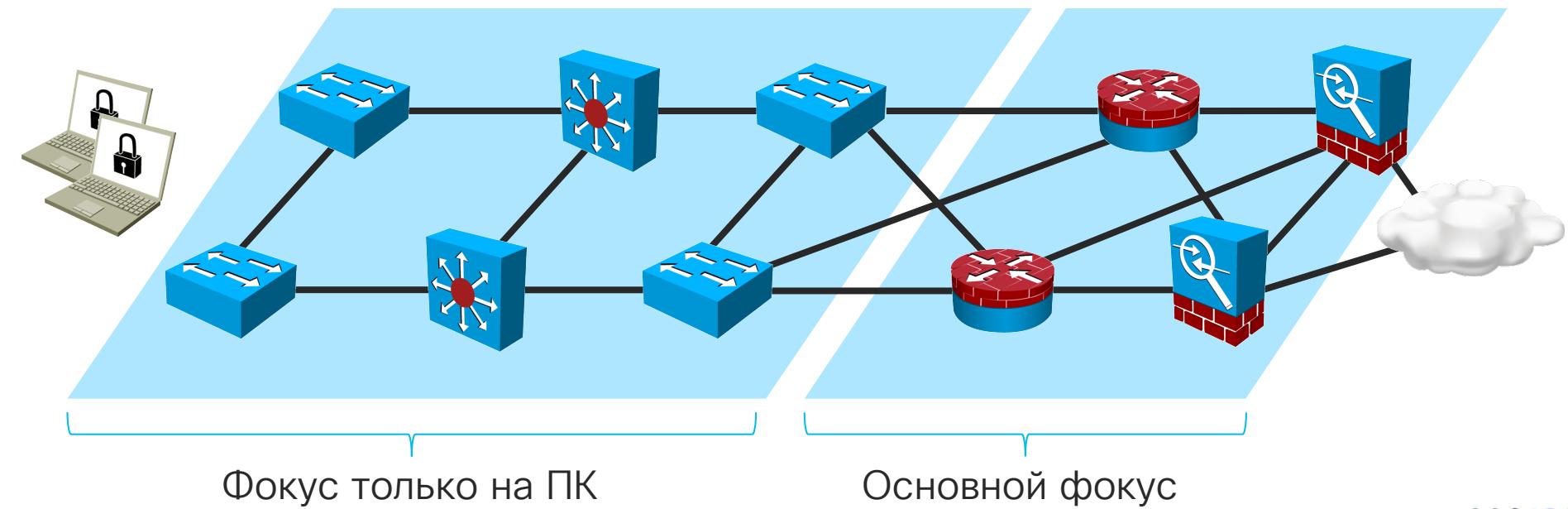


INTUITIVE

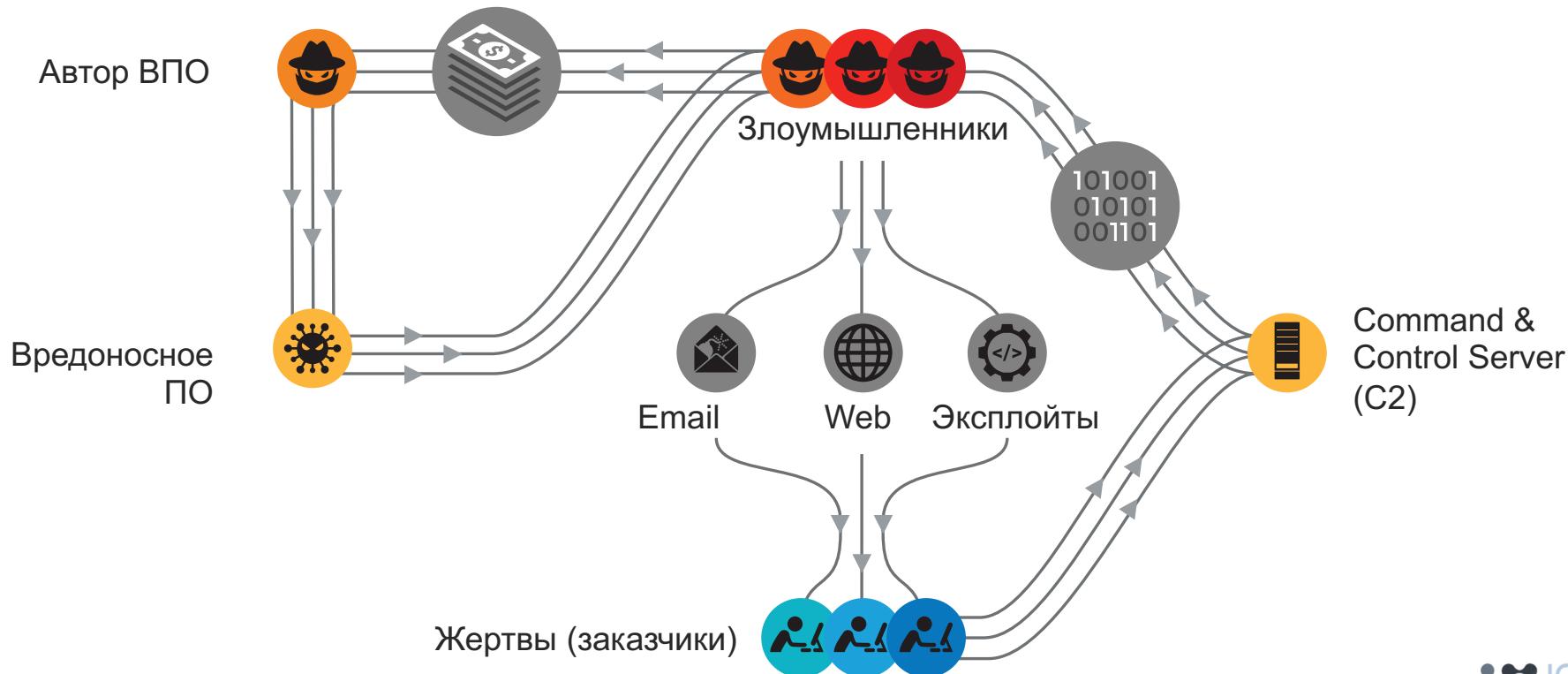
Три направления развития Cisco по ИБ



Как обычно защищается ваша сеть?



Экосистема злоумышленников



Повышение окупаемости инвестиций в решения для обеспечения конфиденциальности данных

Конфиденциальность данных: сравнительное исследование



Исследование
приватности данных и
ПДн в разных странах
для Chief Privacy Officer

cisco.com/go/securityreports

Защита от критических угроз безопасности

Отчет об угрозах, февраль 2019 г.



Анализ тенденций по ту
сторону баррикад за 12
месяцев - для людей,
принимающих решения

В ожидании неизвестного

Работа директоров по информационной
безопасности (CISO): сравнительное
исследование



Ключевые факты и
данные о возможностях
ИБ и реагировании на
инциденты

Сколько
способов
проникновения
в свою сеть вы
знаете?

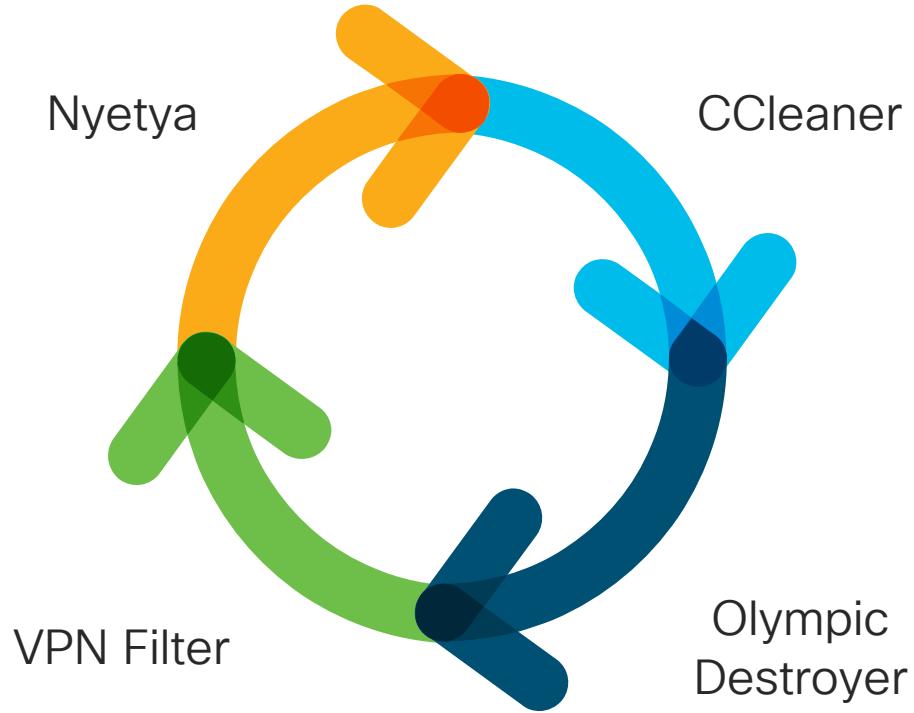


17 каналов проникновения плохих парней в вашу организацию



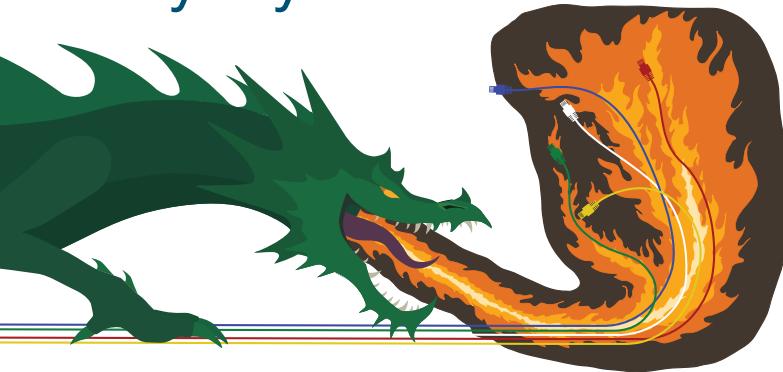
1. E-mail
2. Web
3. Site-to-Site VPN
4. Remote Access VPN
5. Sharing resources
6. USB
7. Wi-Fi
8. Warez
9. BYOD
10. Embedded
11. Клиент-сервер с шифрованием
12. DevOps
13. Подрядчики
14. Уязвимость на портале
15. «Водопой» (Waterhole)
16. DNS
17. Облако

Только четыре живых примера



Примечание: Все 4 примера обнаружены Cisco Talos

Nyetya



Описание

- Продвинутый актор, ассоциированный с государством
- Деструктивная атака маскировалась под Ransomware
- Наиболее дорогой инцидент в истории

Инструменты

- Wormable Ransomware
- Спроектирован для распространения внутри, не снаружи
- Использование Eternal Blue / Eternal Romance и Admin Tools (WMI/PSEexec)



Тактики

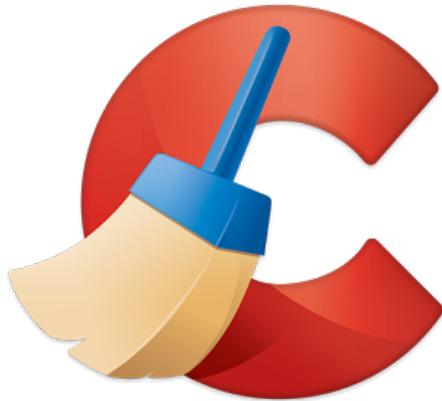
- Цепочка поставок и от жертвы к жертве
- Быстрое распространение
- Разрушение систем / сетей



Процессы

- Разработан для максимально быстрого и эффективного нанесения ущерба
- Похож на вымогателя, но является деструктивным по сути

CCleaner



Описание

- Продвинутый актор, ассоциированный с государством
- Возможность выполнять сложные и длинные операции, фокусированные на краже интеллектуальной собственности

Инструменты

- Целевой фишинг
- Комплексная разведка и профилирование цели
- Кейлогер и вор пользовательских учетных данных



Тактики

- Цепочка поставок и от жертвы к жертве
- Медленная внутренняя разведка
- Сложная многоходовая атака



Процессы

- Высокоточная идентификация жертв через датамайнинг
- Ориентирован на скрытность, рассчитан на долгую «игру»

Olympic Destroyer



Описание

- Targeted Korean Olympics
- US attributes N Korea
- Attempted attribution misdirection

🛠 Инструменты

- PSEXEC / WMI / Creds stealer / Browser stealer
- Использование системных утилит
- Mimikatz и воровство учетных данных



Тактики

- Цепочка поставок
- Расширение плацдарма через WMI и PSEXEC
- Автоматическое расширение плацдарма с украденными учетными данными



Процессы

- Кража учетных данных и расширение плацдарма
- Фокусированная атака, направленная на получение политической выгоды

VPNFilter



Описание

- Ботнет из периметровых сетевых устройств
- Инфицировано свыше 500K устройств

🛠 Инструменты

- Фреймворк для построения собственных ботнетов
- Модульная архитектура для обновления
- Сложная C2 & многоходовая платформа



Тактики

- Направлена на периметровые устройства
- Перенаправляет и изменяет сетевой трафик



Процессы

- Брать все, искать интересующее
- Заразить и закрепиться

Совет №0

Не ограничивайтесь только периметром! Используйте (и выбирайте) сетевую инфраструктуру не только для передачи трафика из точки А в точку Б, но и для решения вопросов кибербезопасности

Три источника данных для мониторинга внутренней сети



Три подхода к мониторингу внутренней сети

«Сырой» трафик для СОВ / СОА

- Самый распространенный и самый очевидный вариант
- Большое количество решений на рынке
- Об этом же говорят регуляторы

Анализ логов сетевых устройств

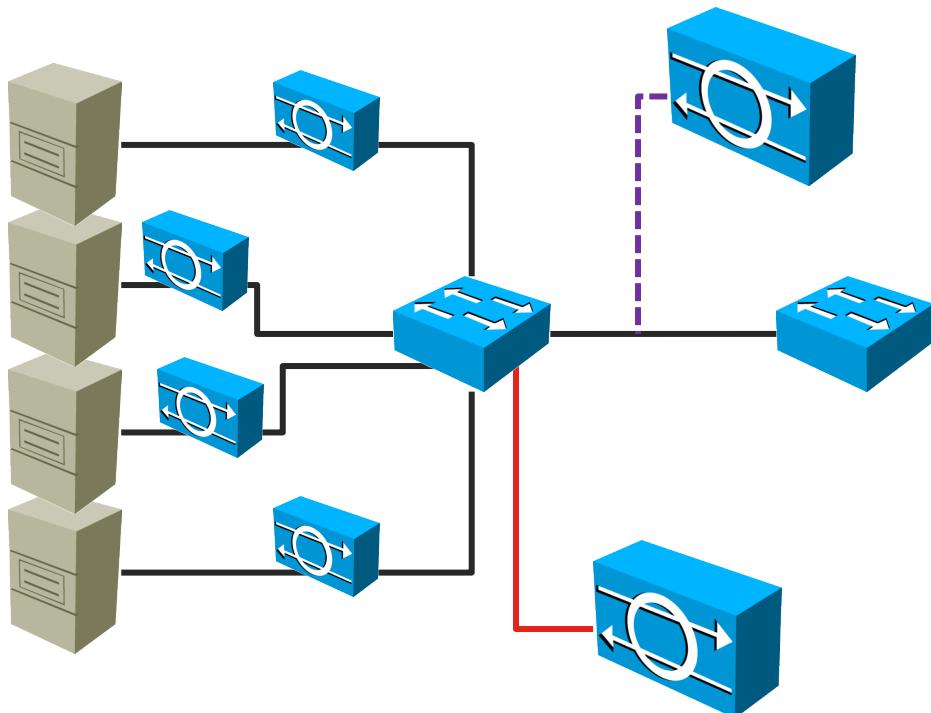
- Самый дешевый вариант
- Зависит от производителя и модели устройства
- Требует анализатора (LM / SIEM)

Потоки трафика

- Защита инвестиций в инфраструктуру
- Зависит от типа протокола Flow
- Требует анализатора (NTA / SIEM)

Примечание: есть еще NBAR2 на ISR/ASR, но ИБ – не его основная задача

Мониторинг с помощью СОВ – самый популярный вариант



Вариант №1
СОВ на каждое
соединение с
сервером



Вариант №2
СОВ на SPAN-порт
(или RSPAN/ERSPAN)



Вариант №3
СОВ на транковое
соединение



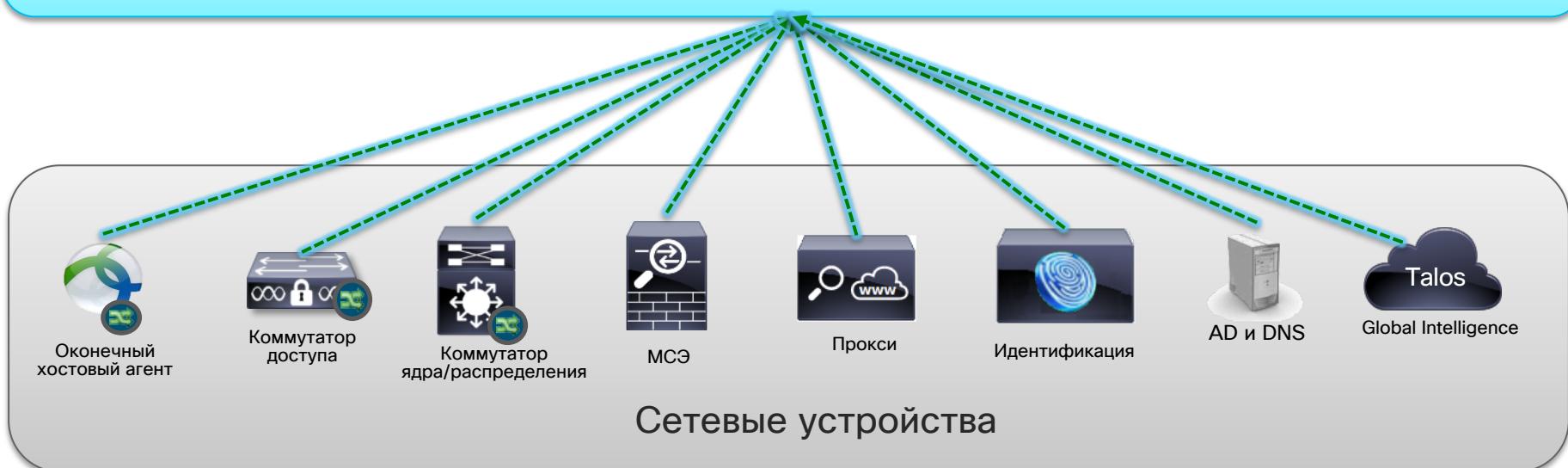
Достоинства и недостатки

Варианты	Достоинства	Недостатки
Вариант №1 СОВ на каждое соединение с сервером	<ul style="list-style-type: none">Полная видимость коммуникаций для каждого сервера	<ul style="list-style-type: none">Избыточная стоимость решенияНаличие разветвителей (для режима IDS)Места в стойках / питание
Вариант №2 СОВ на SPAN-порт (или RSPAN)	<ul style="list-style-type: none">Возможность обойтись меньшим числом сенсоров	<ul style="list-style-type: none">SPAN-порт может быть занятПропускная способность SPAN-порта ниже совокупной пропускной способности контролируемых соединений
Вариант №3 СОВ на транковое соединение	<ul style="list-style-type: none">Низкая стоимость	<ul style="list-style-type: none">Неполная видимость трафика между серверами

Сетевая телеметрия

Телеметрия: процесс автоматизированной коммуникации, при котором измерения и другие данные собираются на удаленных или недоступных точках и передаются на оборудование получателя для анализа и мониторинга.

<https://en.wikipedia.org/wiki/Telemetry>



Сравнение захвата пакетов и анализа потоков

Захват пакетов

- Использование технологий SPAN, RSPAN, ERSPAN или TAP
- Подходит для глубокого анализа конкретной сессии с захватом не только заголовка, но и тела данных
- Может быть использован для хранения доказательной базы

Анализ потоков

- Использование протоколов Netflow, sFlow, IPFIX, NetStream и других
- Сбор метаданных из сетевого трафика
- Первоначально использовался для анализа статистики и поиска проблем в сети
- Применение специальных алгоритмов позволяет использовать для анализа угроз безопасности

Что такое flow в контексте ИБ?

Кто

Когда

Где

Что

Кто

Как

Больше контекста

Flow Detailed Summary: 10.10.18.102

Search Subject Details	Totals	Peer Details
Packets: 285	Packets: 1.44K	Packets: 1.15K
Packet Rate: 2.85pps	Packet Rate: 14.37pps	Packet Rate: 11.52pps
Bytes: 11.49KB	Bytes: 1.63MB	Bytes: 1.62MB
Byte Rate: 117.69bps	Byte Rate: 17.11Kbps	Byte Rate: 16.99Kbps
Percent Transfer: 0.6879458949171267%	Search Subject/Peer Ratio: 0.01	Percent Transfer: 99.31205410508288%
Host Groups: Desktops	TCP Connections: 2	Host Groups: Canada
TrustSec ID: 100	RTT: 2ms	Payload: 200 OK
TrustSec Name: Employees	SRT: 498ms	TrustSec ID: 0
Payload: GET http://crl.entrust.net /2048ca.crl		TrustSec Name: Unknown

Close

- Кто/что, куда, когда и как
- География
- Web-логи
- Active Directory
- Приложения на узле

Сравнение Netflow и sFlow

Функция	NetFlow	sFlow
Захват пакетов	Не захватывает пакетов вообще	Копирует все пакеты и семплирует 1 из N для отправки на коллектор
Поддержка протоколов	Уровень 2 , IP и IPv6	Независим от сетевого уровня
Конфигурируемые поля	Flexible NetFlow – настраиваемые пользователем поля (шаблоны)	Фиксированные поля протокола
Записи потоков	Поддержка записи потоков IPv4, IPv6 для всего трафика	Запись потока не создается, копируется первых N байт пакета
Аппаратное ускорение	Да, записи потоков создаются в «железе» без влияния на data plane	Аппаратное ускорение возможно. Обычно пакеты захватываются ПО
Индустриальный стандарт	IPFIX	sFlow v5
Временные метки потоков (время начала и окончания потока)	Да	Нет
Packet rates (количество пакетов в потоке)	Да	Нет
Подсчет байт (число байт в потоке)	Да	Да (частично)

Совет №1

Используйте Netflow v9 или IPFIX – они дают больше информации в контексте безопасности и позволяют мониторить не только IPv4, но и IPv6, MPLS и т.д.

Анализ семплированной телеметрии в контексте кибербезопасности

Несемплированная

- Экспорт Netflow/IPFIX зависит от активного/неактивного таймера и может приводить к задержкам до 30 минут
- Полная видимость всего трафика
- Позволяет обеспечивать расследование инцидентов

Семплированная

- Данные передаются в реальном времени
- Хорошо подходит для обнаружения массированных DoS/DDoS-атак
- Пропуск «многопакетных» атак, непопавших в семплированный трафика
- Пропуск «атомарных» атак
- Не подходит для расследования инцидентов

Семплирование трафика – все равно, что
оценка книги по одной странице из ста 😞

Скорость канала	Уровень семплирования
10 Мбит/сек	1 из 200
100 Мбит/сек	1 из 500
1 Гбит/сек	1 из 1000
10 Гбит/сек	1 из 2000

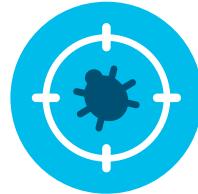
Совет №2

Используйте
несемплированный flow-
протокол – он дает больше
информации для
обнаружения угроз.
Например, Netflow или IPFIX

Пример анализатора потоков: Cisco Stealthwatch

Осведомленность в реальном времени на ПК, филиалах, ЦОДах и облаках

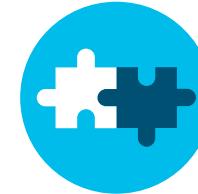
Расширенная
защита



Ускоренное
реагирование



Простая
сегментация



Stealthwatch Enterprise

Корпоративная сеть

Stealthwatch Cloud

Частное облако

Публичное облако

Аналитические движки

Stealthwatch “On Box”

- Поведенческий анализ
- Обнаружение аномалий через статистическое обучение
- Обучение без учителя
- Выставляемый пользователем анализ поведения

Top Alarming Hosts	
HOST	CATEGORY
10.201.3.149 ⓘ	DH RC CI EX
End User Devices	
10.201.3.18 ⓘ	DH RC
End User Devices	
10.201.0.23 ⓘ	DH EX
Terminal Servers	
10.150.1.200 ⓘ	RC DH EX CI
WebHostedApp	
10.10.101.24 ⓘ	EP
End User Devices	

Cognitive Analytics

- Облачный
- Многоуровневый движок машинного обучения
- Обнаружение аномалий через статистический анализ
- Обучение с учителем
- Классификация вредоносов



Классификатор хостов

- Многоуровневое машинное обучение
- Классификация по правилам
- Управляется настройками пользователя

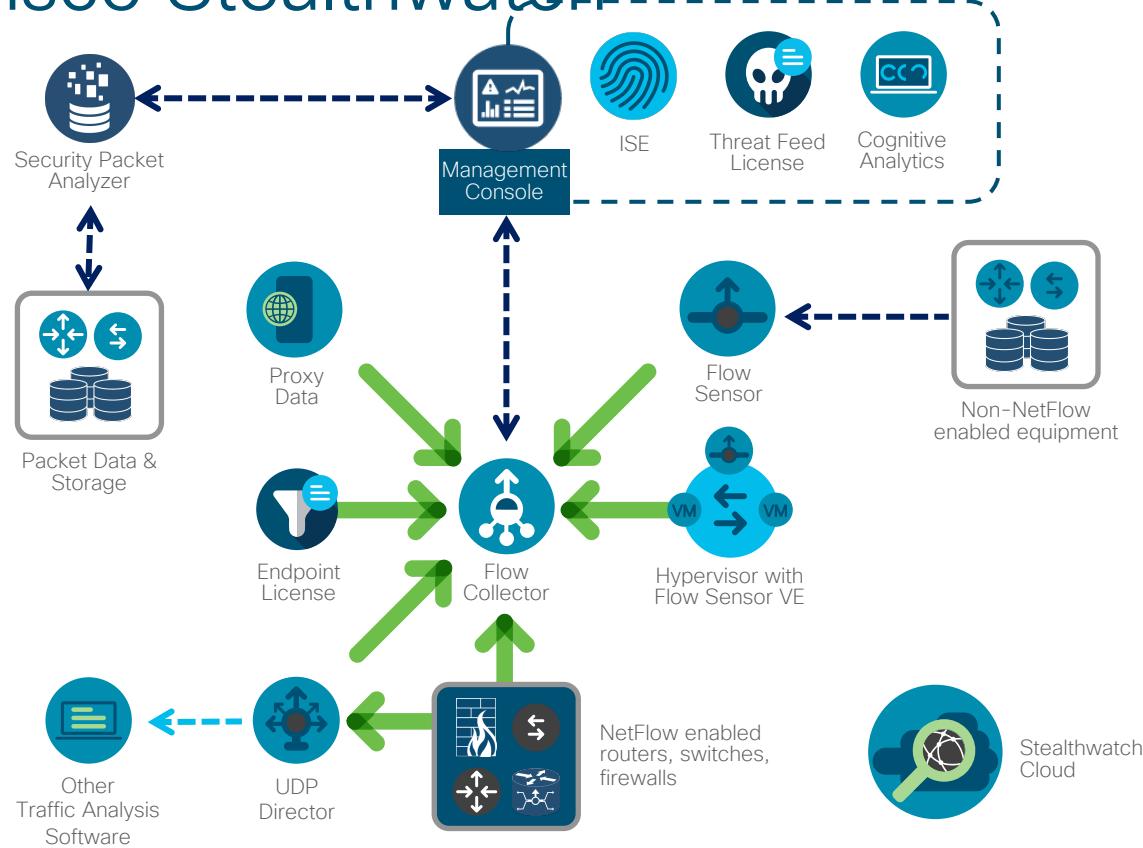
Classification Searches

SUGGESTED

NTP Server	100
Web Server	100
DHCP Server	100
DNS Server	100

Архитектура Cisco Stealthwatch

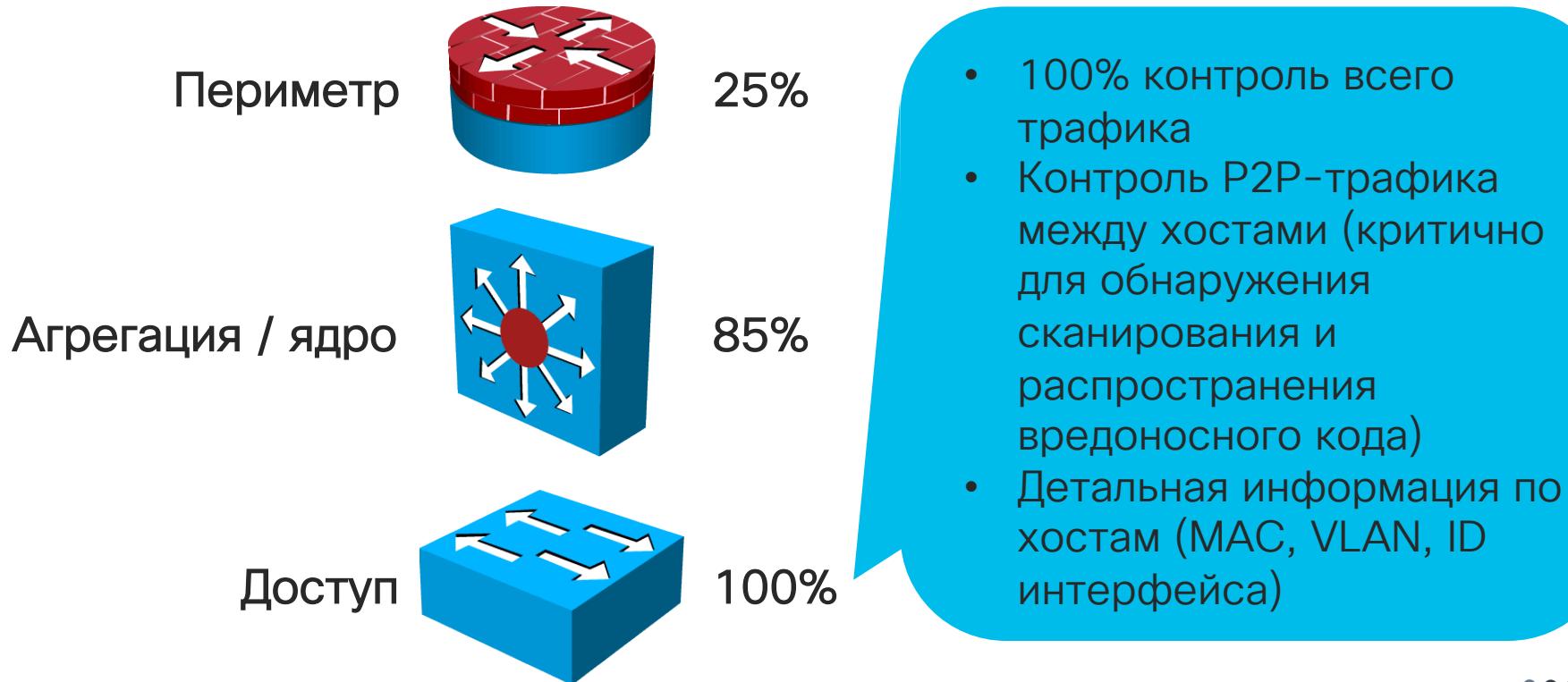
**Комплексная
безопасность
и сетевой
МОНИТОРИНГ**



Совет №3

Проверьте загрузку вашего сетевого оборудования – возможно оно не справится с обработкой еще и flow-протокола. Тогда продумайте применение виртуальных сенсоров или Netflow Generation Appliance

Где размещать?



Что вы можете увидеть?

CONFIRMED INCIDENTS

anomaly detection + global feature cache + IOCs

- ad injector
- anonymization software
- banking trojan
- click fraud
- cryptocurrency miner
- exfiltration
- exploit kit
- information stealer
- malicious advertising
- malicious content distribution
- malware distribution
- maney scam
- PUA
- ransomware
- scareware
- spam botnet
- spam tracking
- trojan

10 - 3

DETECTED INCIDENTS

risk

- 10 cryptowall
- 9 ramnit
- 8 sality
- 8 botnet
- 8 c&c
- 8 - 6 SMB service discovery
- 7 DNS sinkhole
- 7 suspicious file download
- 7 ICMP burst
- 6 unexpected DNS usage
- 6 SSH cracking
- 5 torrent
- 5 excessive communication
- 5 vulnerability scanning tool
- 5 phishing
- 4 TOR

Совет №4

Реализуйте контроль в первую очередь на уровне доступа – это даст вам возможность видеть 100% всего трафика

А что
российские
вендоры
сетевого
оборудования?



Cisco Stealthwatch будет работать с большинством российских сетевых вендоров

NSG	Полигон	Элтекс	Зелакс
<ul style="list-style-type: none">• Нет поддержки flow• Нет SPAN	<ul style="list-style-type: none">• Нет поддержки flow• SPAN, RSPAN	<ul style="list-style-type: none">• sFlow (в планах)• SPAN, RSPAN	<ul style="list-style-type: none">• sFlow• SPAN
Натекс	QTech	Рустелетех	Крафтвей
<ul style="list-style-type: none">• sFlow• SPAN	<ul style="list-style-type: none">• sFlow• SPAN, RSPAN	<ul style="list-style-type: none">• sFlow• SPAN	<ul style="list-style-type: none">• Нет поддержки flow• SPAN

Stealthwatch поддерживает sFlow, Netflow, IPFIX, cFlow, jFlow, NetStream

Совет №5

Если вы выбираете российское сетевое оборудование, то выбирайте то, которое поддерживает flow-протоколы или имеет SPAN/RSPAN-порты

Cisco Stealthwatch

ETA

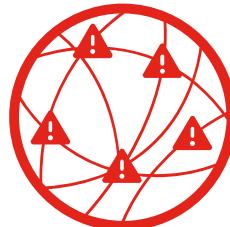
Анализ
зашифрованного
трафика во внутренней
корпоративной сети



Не требует
перестройки сети
для мониторинга
внутренних угроз

ROI

Защита сделанных
инвестиций в
сетевую инфраструктуру и
возможность использования
решения для ИТ и ИБ

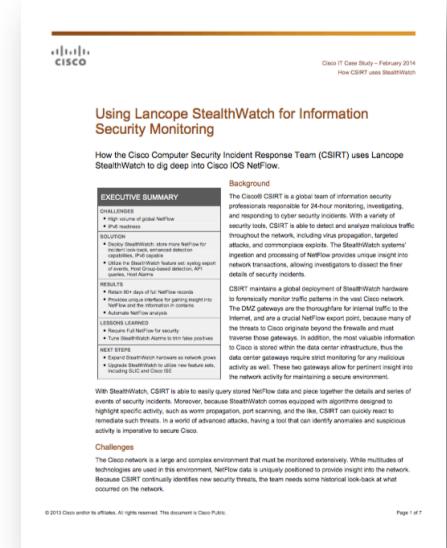
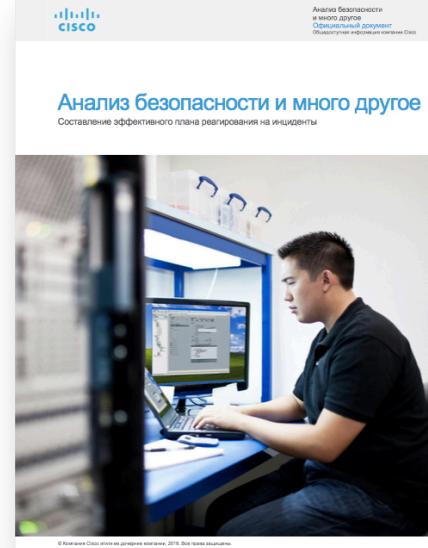


Мониторинг
инфраструктуры
Cisco и не только
(IPFIX, cFlow, jFlow,
sFlow, SPAN/RSPAN)

Варианты применения анализаторов потоков

Понимание контекста	Обнаружение угроз	Реагирование на инциденты	Планирование и диагностика сети	Мониторинг пользователей
<ul style="list-style-type: none">Активности сети, приложений и пользователейМониторинг ИБ, используя сеть как сенсор	<ul style="list-style-type: none">APTИнсайдерыDDoSУтечки данныхВредоносное ПОDGAC2	<ul style="list-style-type: none">Анализ потоков данных при криминалистической экспертизе и сборе доказательствРепозиторий информации по ИБ	<ul style="list-style-type: none">Сегментация сети для профилирования трафика приложений / устройствПланирование пропускной способностиМониторинг сбоевАнализ приложений	<ul style="list-style-type: none">Cisco ISEМониторинг привилегированного доступаРеализация политик

Cisco CSIRT о своей практике использования анализаторов потоков



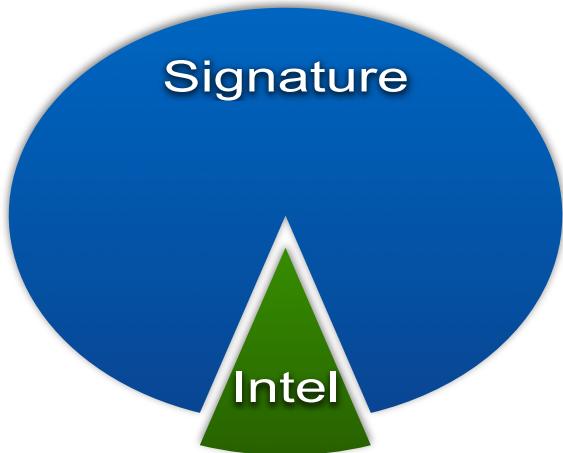
<https://youtu.be/FEmAmsajBtl>

Сравнение Netflow и NGIPS

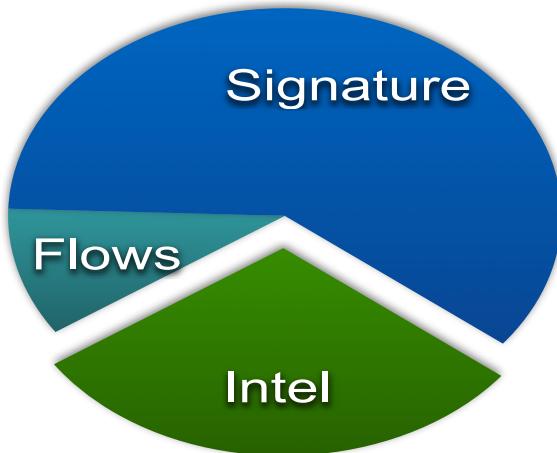
Параметр	Анализ NetFlow	Next-Gen IPS
Метод работы	Анализ потоков	Захват пакетов
Размещение	Коллектор обычно размещается в центре. Сенсоры посылают потоки через UDP	Внутри защищаемого сегмента
Инспекция	Широкая (на базе метаданных)	Глубокая (до уровня файлов)
Приватность	Анализ только заголовков. Пользовательские данные не анализируются	Инспектирование файлов и приложений
Хранилище	Информация о потоках легковеснее и может быть сохранена на месяцы и годы для расследования	Хранение каждого пакета нецелесообразно. Только логи могут храниться долго
Анализ зашифрованного трафика	Возможен при использовании машинного обучения (независимо от используемого алгоритма и протокола)	Возможен только в схеме «Man in the Middle», исключая протокол TLS 1.3

Опыт Cisco: комбинируйте методы обнаружения

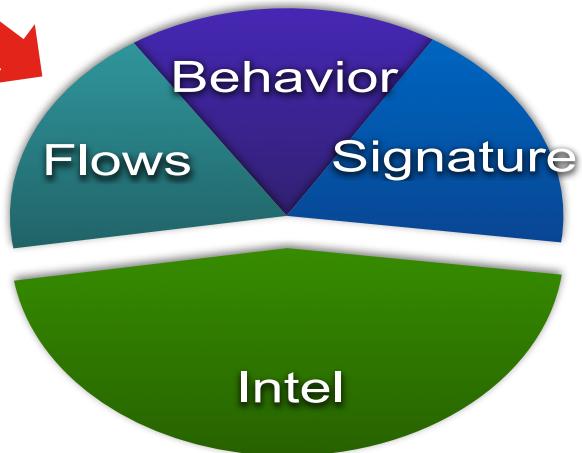
В прошлом



2012

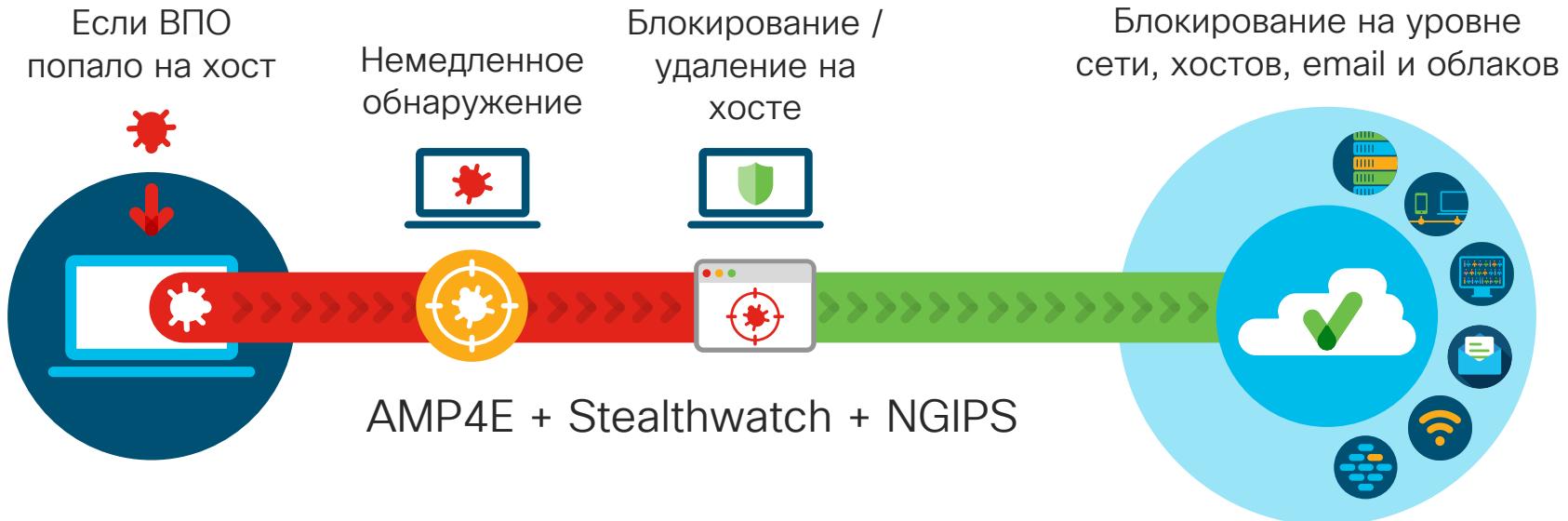


2013+



Необходимо использовать различные способы изучения угроз
Сетевые потоки | Поведение | Сигнатуры | Исследования

Автоматизация обнаружения атак на уровне сети и хостов



Совет №6

Комбинируйте системы обнаружения/
предотвращения вторжения/атак на границах и системы анализа потоков во внутренней сети (в том числе и в облаках)

На периметре вы
обычно ставите
МСЭ (FW) и СОВ
(IDS)!

- Если Cisco Stealthwatch – это система обнаружения атак во внутренней инфраструктуре, то есть ли у Cisco внутренний межсетевой экран?
- И чтобы он задействовал внутреннюю инфраструктуру!
- И чтобы он был прост в управлении!
- И чтобы он интегрировался с периметром!

Опыт Cisco говорит о нежелании многих заказчиков внедрять межсетевые экраны во внутренние сети. Они отдают приоритет интегрированной безопасности



А почему не
межсетевой
экран?



Типовые зоны / сегменты корпоративной сети

Название сегмента	Предназначение
Корпоративные пользователи	Доверенные бизнес-пользователи
Разработчики	Недоверенные бизнес-пользователи
ДМЗ	Сервера с web-сервисами, доступные для недоверенных пользователей
Партнеры	Сервисы и данные для бизнес-партнеров
Привилегированные пользователи	Доверенные бизнес-пользователи с привилегированным доступом или информацией ограниченного доступа
Публичная зона	Любая система за пределами корпоративного периметра
Нормативная зона	Сервисы и данные, попадающие под регулирование (PCI DSS, 382-П)
АСУ ТП	Промышленные системы
Air Gap	Секретная информация или критические сервисы

В современных предприятиях данным, приложениям и пользователям разрешено перемещаться между...



Любыми
пользователями

- ✓ Сотрудники
- ✓ Контрактники
- ✓ Партнеры



Любыми
устройствами

- ✓ Корпоративные
- ✓ Собственные
- ✓ IoT



Любыми
приложениями

- ✓ ЦОД
- ✓ Мультиоблачо
- ✓ SaaS



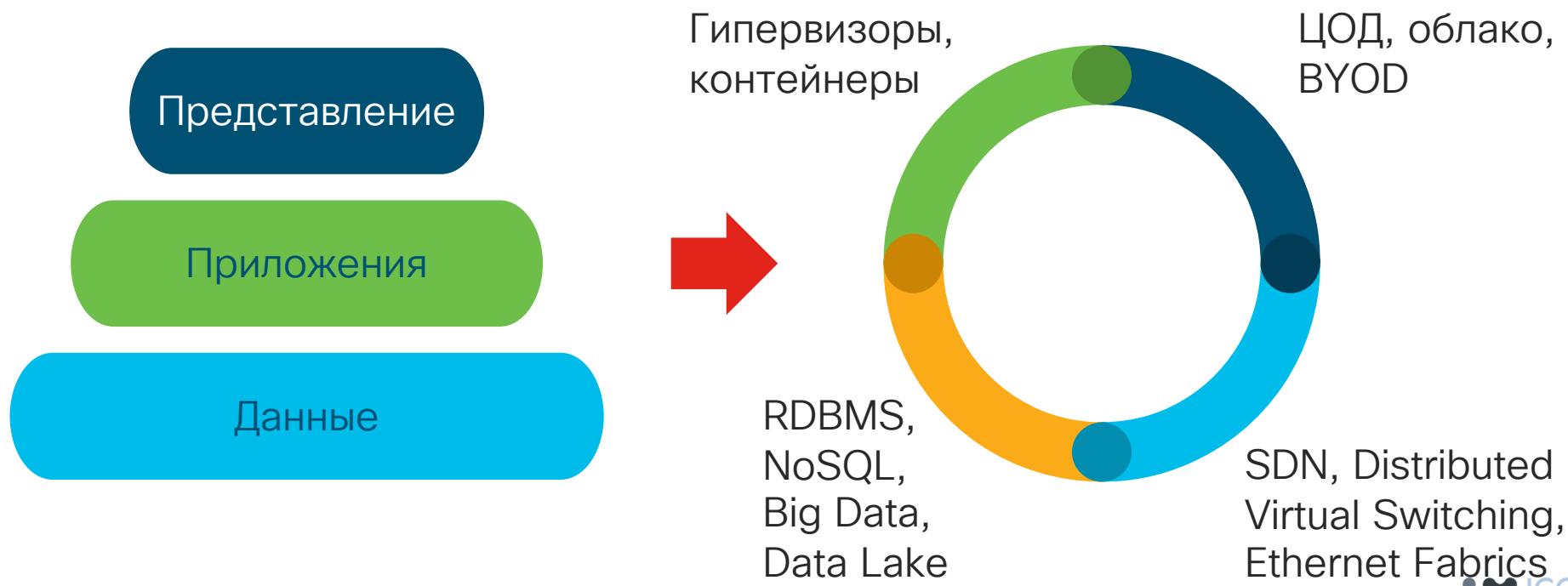
В любых
местах

- ✓ Внутри сети
- ✓ Через VPN
- ✓ Вне сети

Ethernet

SGT SD-Access
Google Cloud iSCSI ACL Hard / Soft Zoning
Public Cloud Amazon AWS Internet of Things
Data Lake Microsoft Azure SD-WAN
MPLS Scalable Group Tag
VLAN NoSQL VXLAN Big Data SDN ICS Kubernetes
Storage Area Network Software Defined Network Hypervisor
Distributed Virtual Switching Application Container Zero Trust
Cloud Access Security Broker Ethernet Fabric
LUN Masking Air Gap Controller Area Network
Software-as-a-Service

Современное зонирование



Может вам
нужна точка
принятия
решений о
доступе?



Совет №7

Думайте о зонировании не в контексте межсетевого экранования, а в контексте коммуникаций узлов и пользователей. А для этого используется сеть!

Что лежит в
основе всех
коммуникаций?



Добавьте контекст



НЕИЗВЕСТНО



ИЗВЕСТНО

Отсутствие контекста

IP АДРЕС: 192.168.2.101



НЕИЗВЕСТНО



НЕИЗВЕСТНО



НЕИЗВЕСТНО



НЕИЗВЕСТНО



НЕИЗВЕСТНО



РЕЗУЛЬТАТ

ДОСТУП К IP
(ЛЮБОЕ УСТРОЙСТВО / ПОЛЬЗОВАТЕЛЬ)



Богатый контекст

Алексей Лукацкий (СОТРУДНИК)



MACOS WORKSTATION



ЗДАНИЕ-4-ЭТАЖ-3



13:30 AM MSK ИЮН 21



БЕСПРОВОДНАЯ СЕТЬ



НЕТ УГРОЗ / УЯЗВИМОСТЕЙ

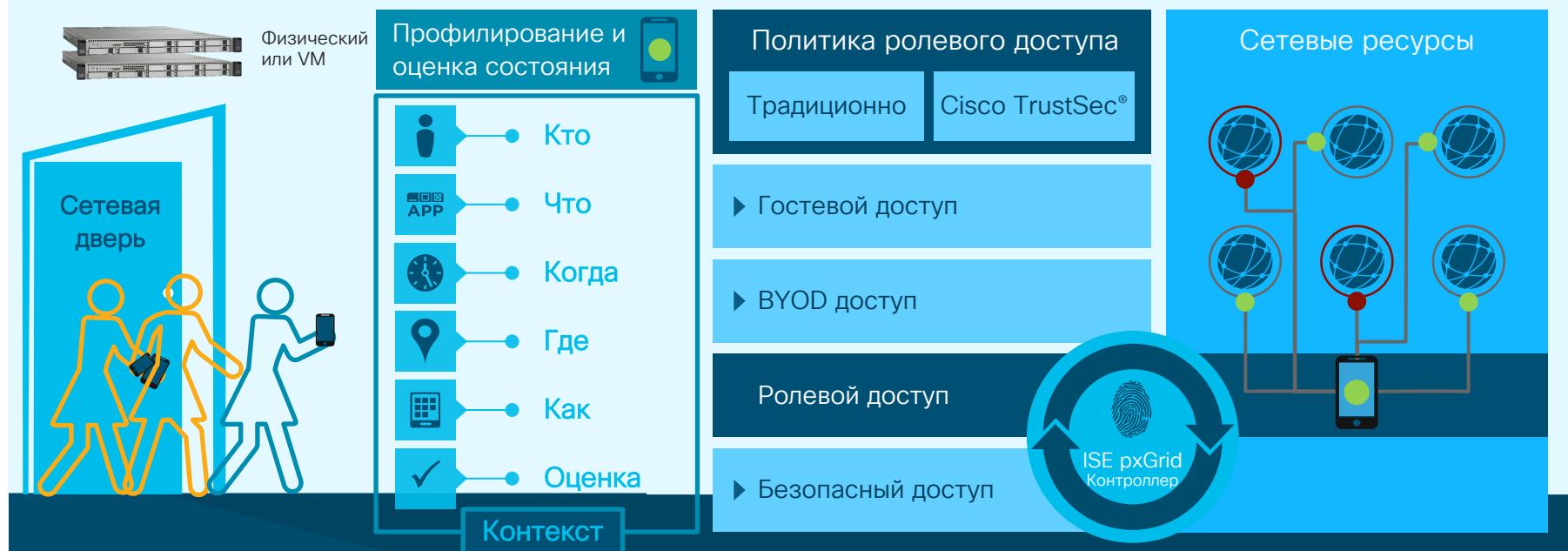
РЕЗУЛЬТАТ

РОЛЕВОЙ ДОСТУП

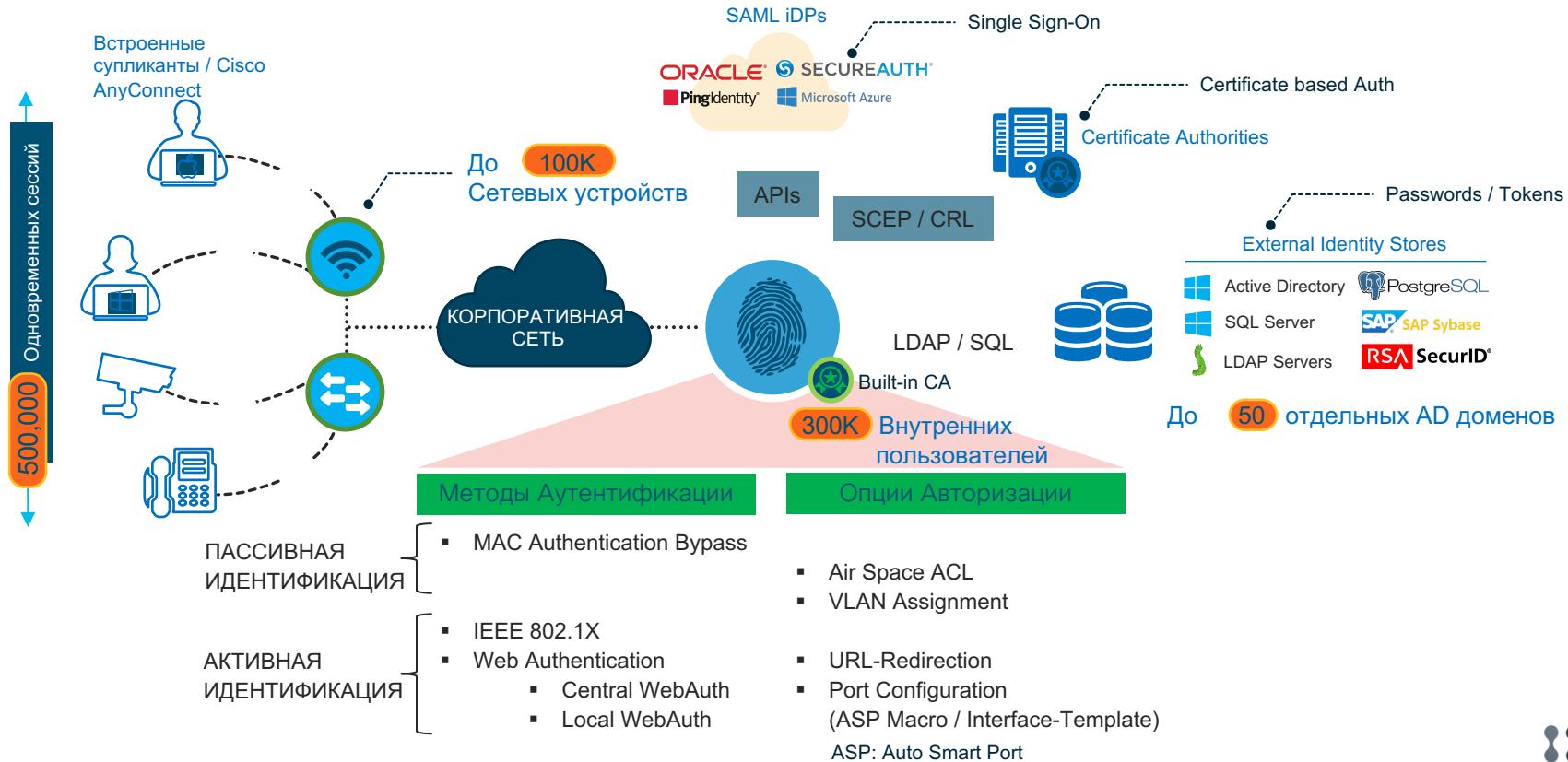


Пример оркестратора: Cisco Identity Services Engine

Централизованное решение для автоматизации контекстно-задаваемых политик доступа к сетевым ресурсам и обмена контекстом



Контроль доступа внутри и снаружи



Варианты авторизации

DACL или Named ACL

Загружаемые ACL (Провод) или
Именованные ACL (Провод + БЛВС)



VLAN

Динамическое назначение VLAN



Security Group Tags

Cisco TrustSec



Для российских вендоров тоже

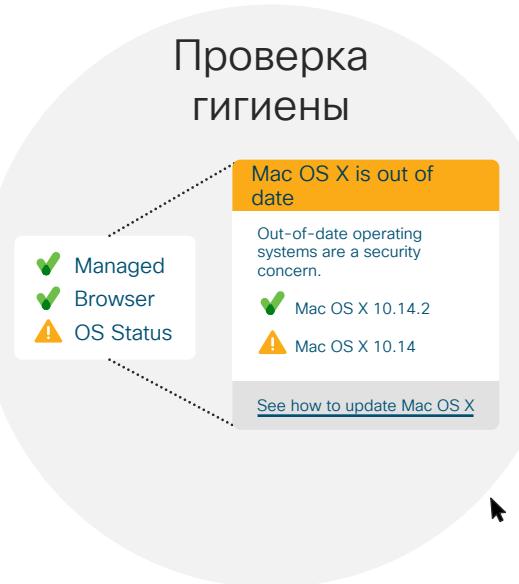
Автоматизация доверенного доступа

Доступ
нормальных
приложений



Проверка
идентичности

Проверка
гигиены



Блокирование
доступа



Доступ
разрешен



Cisco pxGrid позволяет создать экосистему

40+ интеграций партнерских продуктов и 12 технологических областей



pxGrid-работающее партнерство с ISE:

- RTC: Cisco FirePower, Cisco Stealthwatch, Attivo, Bayshore, E8, Elastica, Hawk, Huntsman, Infoblox, Intelliment, LemonFish, LogRhythm, NetIQ, Rapid7, Redshift, SAINT, Splunk, Tenable, ThreatTrack, TrapX
- Firewall: Check Point, Infoblox, Bayshore
- DDI: Infoblox
- Cloud: Elastica, SkyHigh Networks, Netskope
- Net/App: Savvius
- Network Visibility: Lumeta
- SIEM/TD: Splunk, Lancope, NetIQ, LogRhythm, FortScale, Rapid7
- IAM: Ping, NetIQ, SecureAuth, Situational
- UBA: Fortscale, Niara
- Vulnerability: Rapid7, Tenable, SAINT
- IoT Security: Bayshore Networks
- P-Cap/Forensics: Emulex
- Cisco: WSA, FirePower, ISE, Stealthwatch

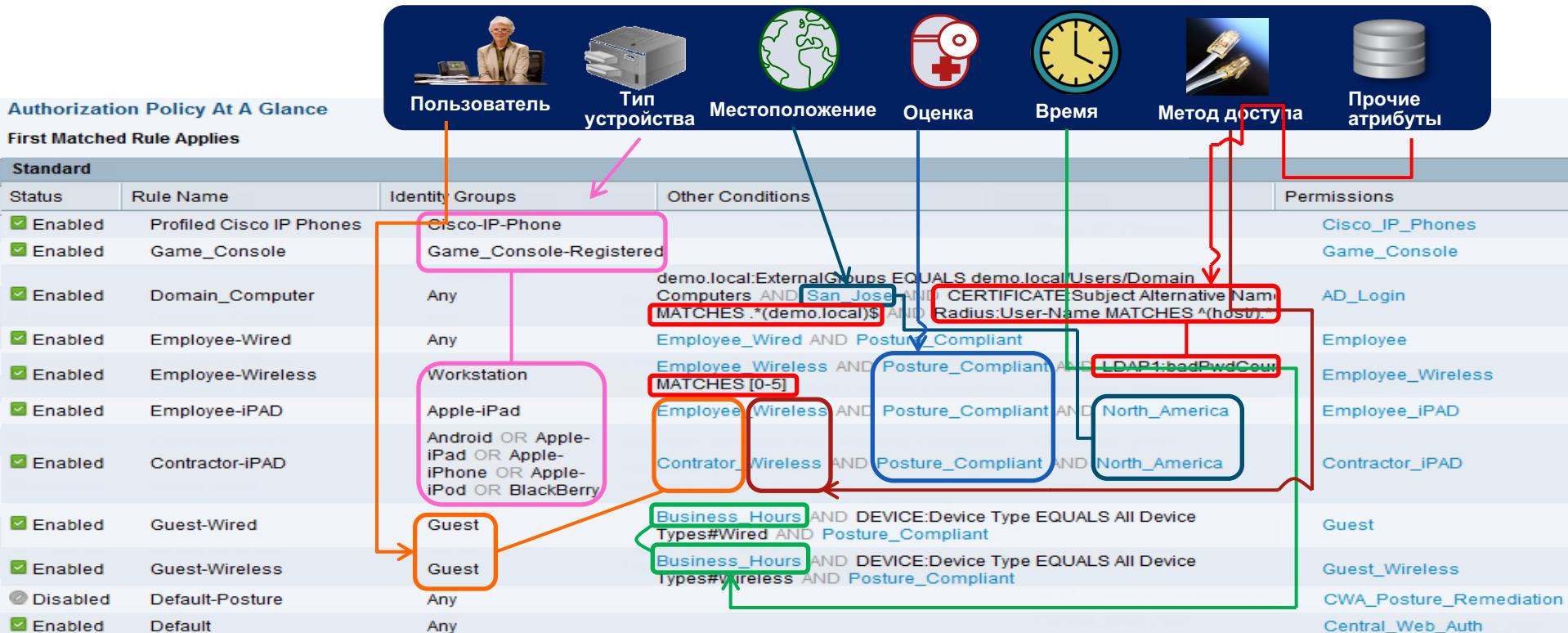
Другие ISE Партнеры:

- SIEM/TD: ArcSight, IBM QRadar, Tibco LogLogic, Symantec
- MDM/EMM: Cisco Meraki, MobileIron, AirWatch, JAMF, SOTI, Symantec, Citrix, IBM, Good, SAP, Tangoe, Globo, Absolute
- Threat Centric NAC: Cisco AMP, Qualys

Опыт использования контекста в Cisco

Кто? Известные пользователи (Сотрудники, продавцы, HR) Неизвестные пользователи (Гости)	Что? Идентификатор устройства Классификация устройств (профиль) Состояние устройства (posture)	Как? Проводное подключение Беспроводное подключение VPN-подключение
Где / куда / откуда? Географическое местоположение Департамент / отдел SSID / Порт коммутатора	Когда? Дата Время	Другие? Пользовательские атрибуты Статус устройства / пользователя Используемые приложения

Опыт Cisco: контроль доступа с Cisco ISE



Автоматизация сетевой сегментации



Совет №8 (бонус)

Автоматизируйте обмен
данными между средствами
мониторинга сети и
контроля сетевого доступа

Эффективная безопасность зависит от общей видимости



ЗНАТЬ
Каждый хост



ВИДЕТЬ
Каждую сессию



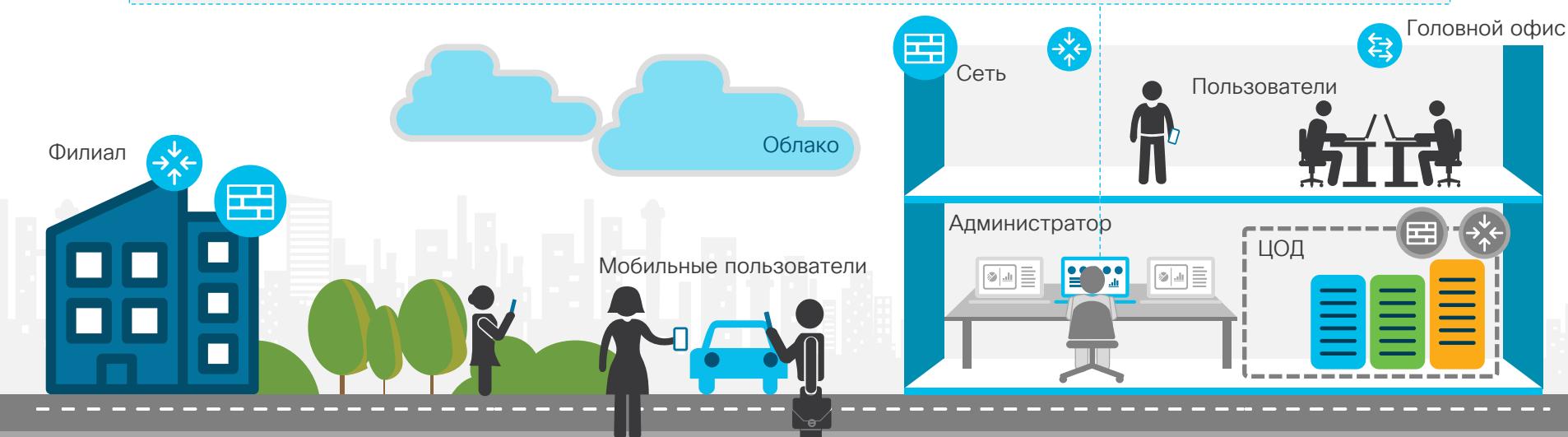
Понимать что
есть **НОРМА**



Быть предупрежденным
при **ИЗМЕНЕНИИ**



Реагировать на
УГРОЗЫ быстро



Совет №9 (бонус)

Посмотрите на свою сеть в перспективе 3-5 лет.
Средства мониторинга и контроля сетевого доступа должны учитывать новые технологии (облака, виртуализацию, контейнеры и т.п.)

Сеть может делиться данными для лучшей видимости и контроля

Сетевые данные и аналитика позволяют...



Обнаруживать аномалии



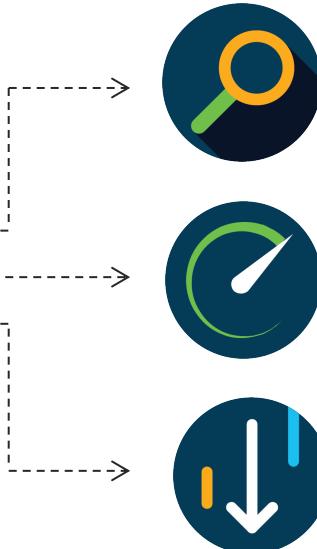
Управлять политиками доступа



Расследовать инциденты

И упростить операции без снижения продуктивности

Интегрированный подход
позволяет...



Обеспечить ситуационную
осведомленность и принятие решений

Упростить сегментацию

Снизить операционные издержки

Превратите свою сеть в распределенную систему безопасности

Обнаружение и корреляция сетевой телеметрии

Установление эталона для поведения сети позволяет вам отслеживать использование, злоупотребление и нарушение в сети



Видеть и обмениваться данными пользователей

Лучший контроль через обогащенную контекстную информацию, включая улучшенный мониторинг угроз и уязвимостей

Кто	Леха, контрактор
Что	BYOD планшет; iOS 9.3.2
Когда	11:00 AM EST on April 10 th
Где	Здание 200, 2 nd этаж
Как	Wireless
Соответствие	Да. PIN-lock включен
Угроза	Distracting
Уязвимость	CVSS score of 6

Резюме

- 0 Не ограничивайтесь периметром
- 1 Используйте Netflow или IPFIX
- 2 Используйте несемплированный Netflow
- 3 Проверьте загрузку оборудования
- 4 Начните с уровня доступа
- 5 Если российское, то с поддержкой flow
- 6 Комбинируйте NTA и СОВ/СОА
- 7 Думайте о зонировании, а не о МСЭ
- 8 Интегрируйте средства мониторинга сети и контроля сетевого доступа
- 9 Учитывайте стратегию развития своей сети

Почему Cisco?



5K
специалистов
по ИБ



Крупнейшая
сеть обнаружения атак



100x
Быстрее
обнаружение
инцидентов



19.7B
угроз блокируется
ежедневно



99%
Эффективность
безопасности



250K
заказчиков



30%
снижение
издержек



170+
экосистемных
партнеров



\$2+ Billion
доходы от
направления ИБ



88%
Fortune 100
использует наши
решения

Где вы можете узнать больше?



Пишите на security-request@cisco.com



Быть в курсе всех последних новостей вам помогут:



<http://www.facebook.com/CiscoRu>



<http://twitter.com/CiscoRussia>



<http://www.youtube.com/CiscoRussiaMedia>



<http://www.flickr.com/photos/CiscoRussia>



<http://vkontakte.ru/Cisco>



<http://blogs.cisco.ru/>



<http://habrahabr.ru/company/cisco>



<http://linkedin.com/groups/Cisco-Russia-3798428>



<http://slideshare.net/CiscoRu>



<https://plus.google.com/106603907471961036146/posts>



<http://www.cisco.ru/>





Спасибо!

security-request@cisco.com



INTUITIVE



INTUITIVE