Cisco DNA
Catalyst 9k

Наиболее интересные кейсы применения технлогий Cisco

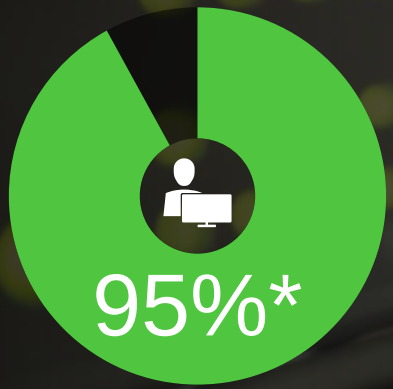
Andrew Ovrashko
System Engineer

18th April 2018

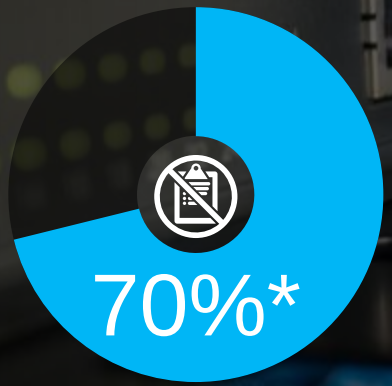
Корпоративные сети сегодня – сложные …

Управление множеством VLAN	Работа с различными сетями	Работа с множеством разных политик - LAN, WLAN, WAN, ЦОД	Масштабирование увеличивает сложность эксплуатации

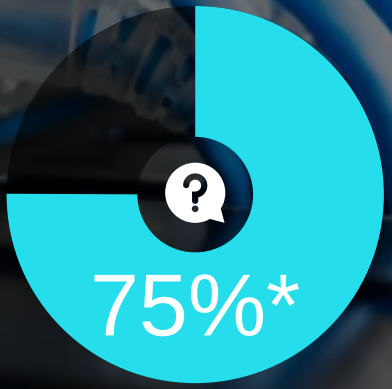
…и имеют множество эксплуатационных проблем



доля ручного труда при внесении изменений



нарушений политик и правил из-за человеческих ошибок



Операционных расходов приходится на поиск неисправностей и диагностику

Традиционные сети НЕ ГОТОВЫ к быстрым темпам развития потребностей бизнеса

Сеть и жизнь

управление и мониторинг

- **Сетку админят руками** (telnet/ssh/CLI/Cisco_IOS)
  - 95% (глобальная статистика!!) – управление коробками по CLI
  - Статичные и **простые** конфигурации
  - Сложность внедрения изменений, особенно в динамике (особенно безопасность)
  - Безопасность, QoS, типовые конфиграции, Central auth для RBAC – дополнительная сложность
- **Мониторинга сети зачастую очень базовый** (Nagios / Zabbix / Cacti / PRGT)
  - Syslog – поиск иголки в стоге сена
  - NetFlow некоторые собирают с Cisco (но ценности особой не видят без корреляции и ML)
  - «Кесарю – кесарево!» У безопасников свои «мониторилки» (сеть?) у ИТ свои (безопасность?)
  - «Куили SIEM» (но нормально не внедрили) – типовой сценарий ☺
- **Средства автоматизации управления и мониторинга**
- **Интеграция сети и безопасности**

Сеть и жизнь

сегментация

- **Сегментация = VLAN** (иногда правила на Firewall)
  - Сегментация сети обычно, есть но очень базовая (не достаточно для безопасности)
  - Больше сегментов = больше VLAN-ов, сложнее контроль доступа между VLAN
  - В реальности VLAN – сегмент, но не ролевая группа
  - Статичные и **простые** конфигурации со списками контроля доступа (ACL)
  - Нет единого окна мониторинга ACL (насколько полно решают задачу?)
  - Нет инструмента поиска устаревших правил во множестве ACL
  - Абсолютно не решает задачи контроля трафика пользователей одного VLAN/подсети
- **Микросегментация**
  - Предполагает ролевой досутп к сети (RBAC) = интеграция NAC (**ISE**) с MS Active Directory
  - Добавляет динамику
  - Предполагает совместимое оборудование (SGT enforcement)
- **Макросегментация**
  - Возможность объединять микросегменты в макрогруппы
  - Возможность растянуть сегментацию на всю сеть с полной автоматизацией внедрения

Что изменилось за последнее время?

IT = поддержка бизнеса **–> основа ведения бизнеса**

Сети стали сложнее: Wired + Wireless + Virtual + Remote Access.

Сложность поддержки единых политик по всей сети

Понятие «периметр сети» изменилось.

Больше требований к безопасности. **Сложнее реализация.**

Сетевые сервисы стали сложнее: BYOD, App experience, user mobility.

Значительно возросла нагрузка на IT подразделения.

Что изменится в ближайшее время?

IT персонала меньше, задач больше.

Требования к унификации и единому подходу.

От частных насроек к единым политикам.

IT SECURITY = MUST HAVE!!

Сложнее угрозы ИБ. Всё больше шифрованного трафика.

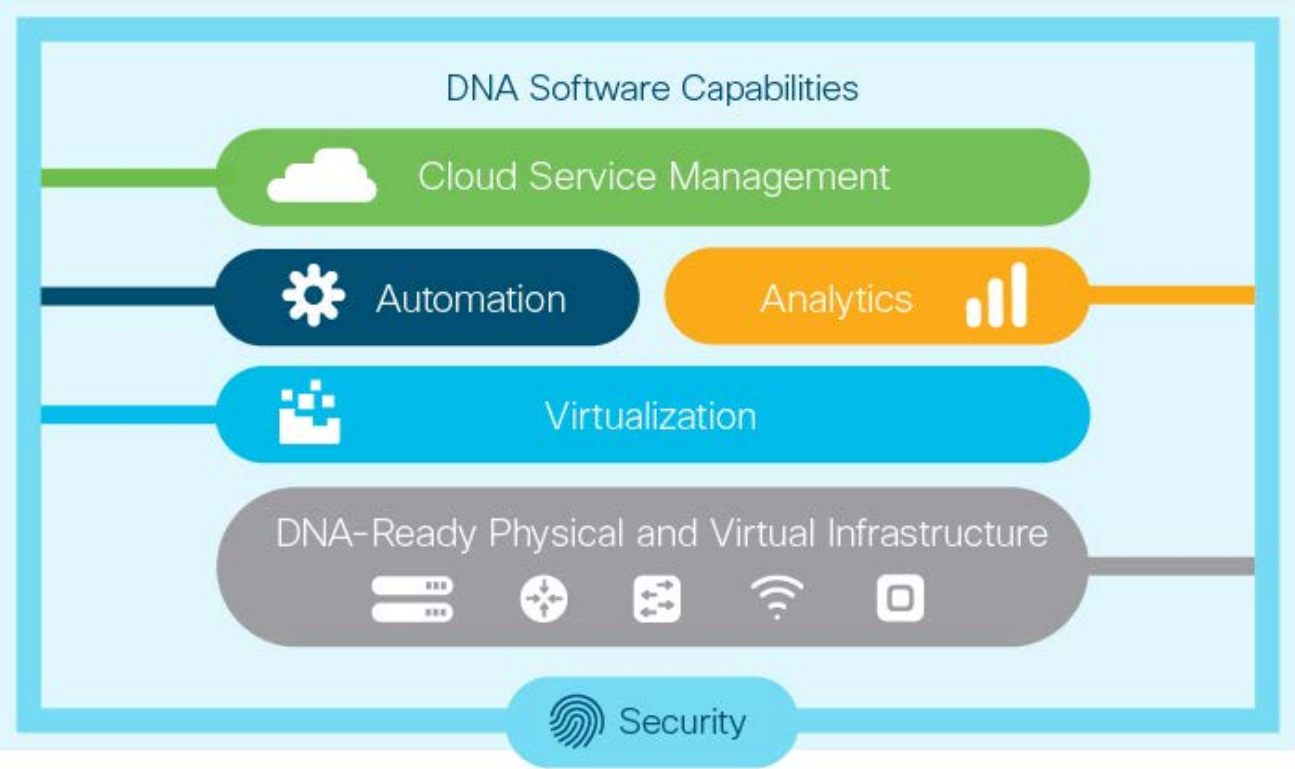
Многомерные сети: App, Device, User, Network, Segmentation, IoT, Cloud

Новые подходы к построению сетей: SDN, network Fabric, NaaS/E

Challenges

- **Implementation Complexity**
- **Network segmentation**
- **Access control policies**
- **User & device onboarding**
- **Slow issue resolution.**

Cisco Digital Network Architecture (DNA)



Идеи, заложенные в Cisco DNA

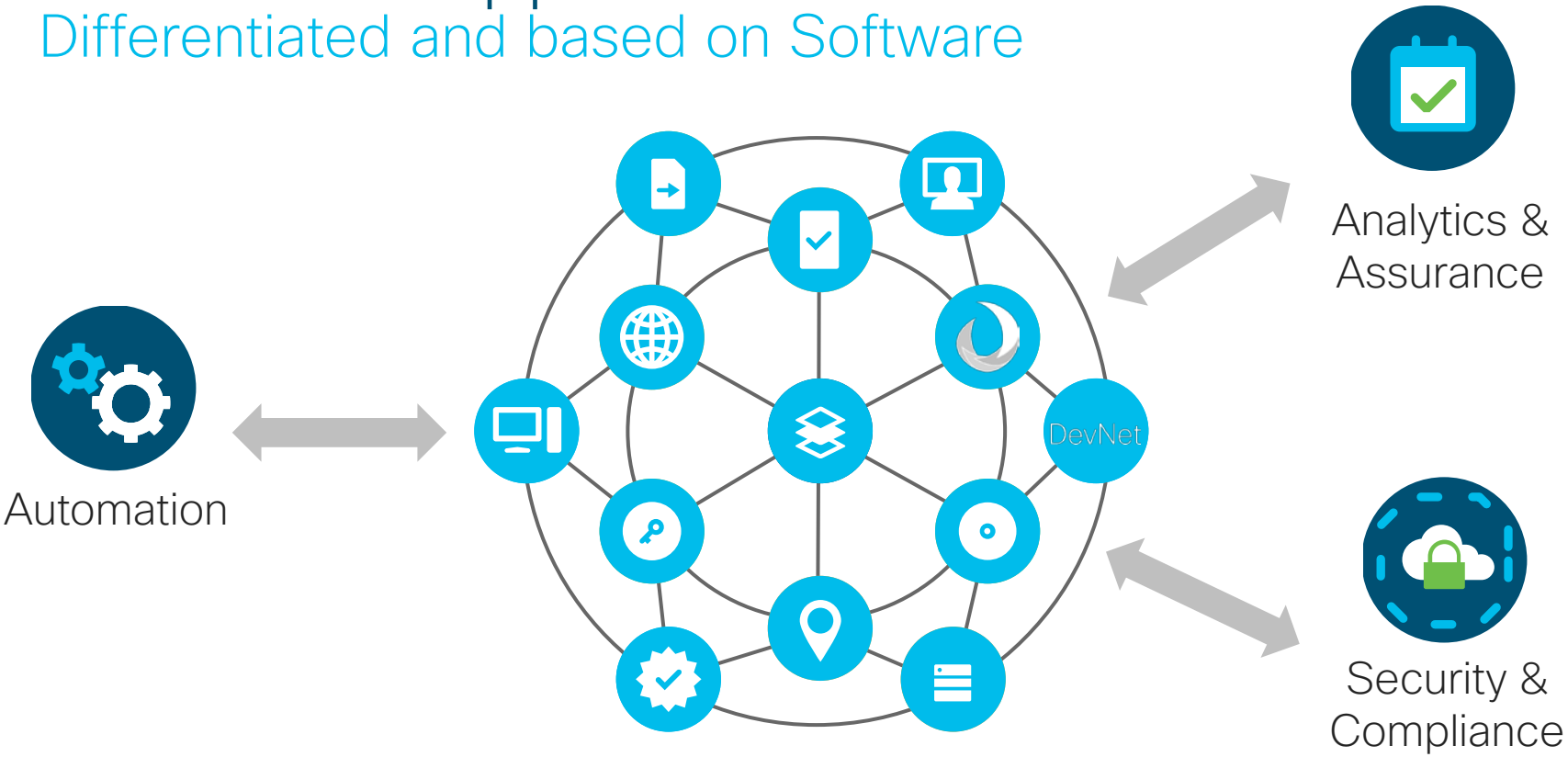
1. **Любое повторяемое и хорошо описанное действие можно автоматизировать.**
2. Автоматизация на сети предполагает превращение сети в единый организам (абстракция).
3. В идеале автоматизация – программно управляемая (SDN).
4. **Любая автоматизация требует обратной связи (аналитика).**
5. Имея готовую аналитику есть смысл её переиспользовать (ИБ, планирование, работа с клиентами и тп.).
6. **Виртуализация сетевых функций даёт возможность разворачивать сервисы по требованию (Enterprise NfV).**
7. **Потребление сетевых услуг в идеале должно быть «как из облака» (сервисный портал).**
8. **Безопасность должна быть учтена везде от А до Я.**

Cisco is rewriting the network playbook

Traditional network	The Network. Intuitive.
Hardware centric	Software driven
Manual	Automated
Fragmented security	Built-in security
Network data	Business insights

Powered by Cisco DNA™

A Platform Approach:
Differentiated and based on Software



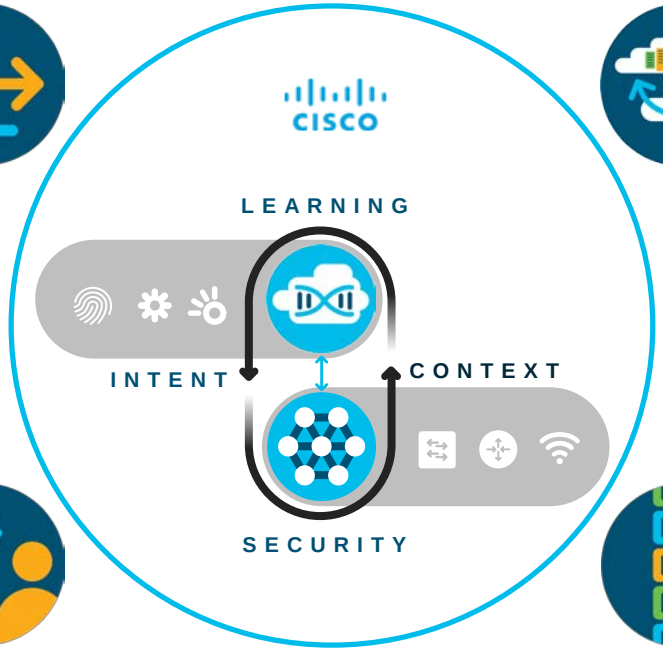
Intent-based network for

WAN

Optimize and secure application performance over any connection to the cloud.

Cloud Edge

Securely connect and protect workloads moving into the cloud and between clouds.



Access

Segment your network and secure user access from the edge to the cloud

Data Center

Run any traditional or cloud native application across any environment

Наиболее полезные сценарии использования технологий Cisco и их преимущества для бизнеса

Сценарии использования Cisco и Business Impact

Безопасность

- Ролевой доступ к сети (Network Access Control).
- Сегментация сети (микро- и макро-) в зависимости от роли.
- Полная интеграция Cisco сети и Cisco безопасности + eco-partners.

Мониторинг

- Продвинутый мониторинг агрегированной сетевой статистики (NetFlow) с машинным обучением и множеством готовых шаблонов.
- Обнаружение malware в шифрованном трафике.
- Network Data Platform как часть Cisco DNA Center.

Автоматизация

- Простота внедрения сети любого масштаба
- Многомерные инструменты (network, user, app, compliance) траблшутинга
- Business insights

Сценарии использования Cisco и Business Impact

#1 TrustSec with Scalable Group Tag (SGT)

Case / issue:

- Сотрудники ждут очереди для перехода между командами, потому что Helpdesk перегружен запросами

Root cause:

- Текущие списки доступа (ACL) привязаны к IP-адресации
- Каждый сайт – свой уникальный IP-pool, количество сетей – мультипликатор политик доступа (ACL)

[45 групп сотрудников] X [20 сайтов] = **900 разных ACL (!!!)**

Group Policy based segmentation

Solution:

- Переход на SGT даст возможность иметь всего 45 ACL (по одной для группы)
- Возможно частичное и/или стадийное внедрение с сохранением текущей парадигмы с ACL
- Возможны гибридные схемы со старым и сторонним оборудованием (есть ограничения и нюансы)

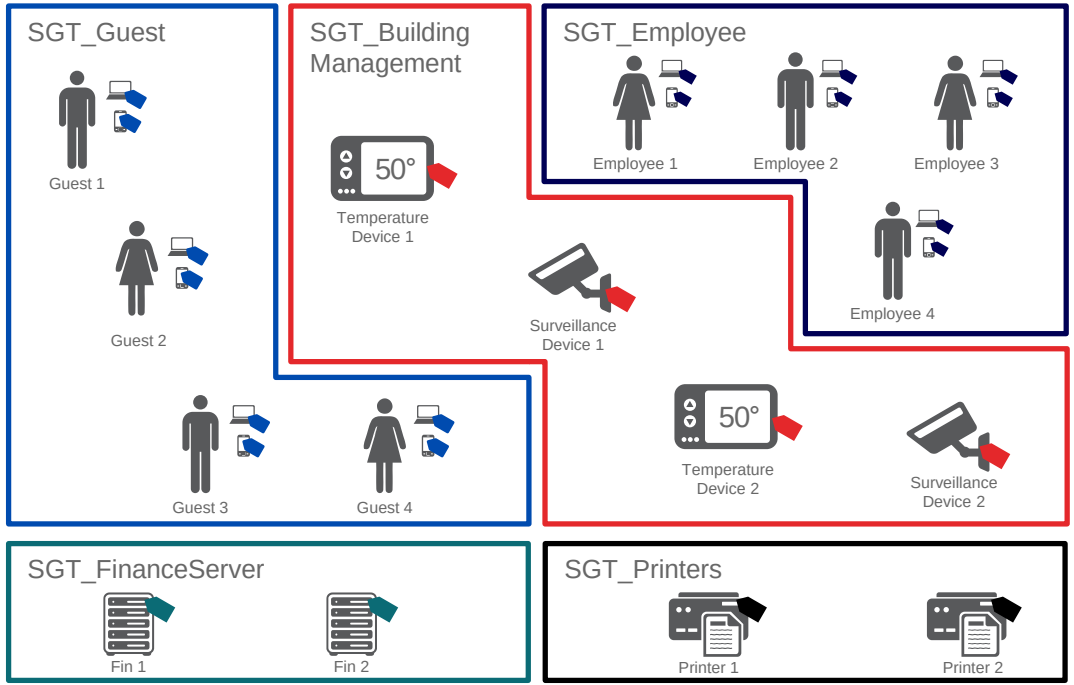
Business impact: **HIGH**

- Agile IT
- Повышение общего уровня информационной безопасности
- Полная наблюдаемость сетевых взаимодействий, простота поддержки и аудита
- Однозначно определённая политика безопасности

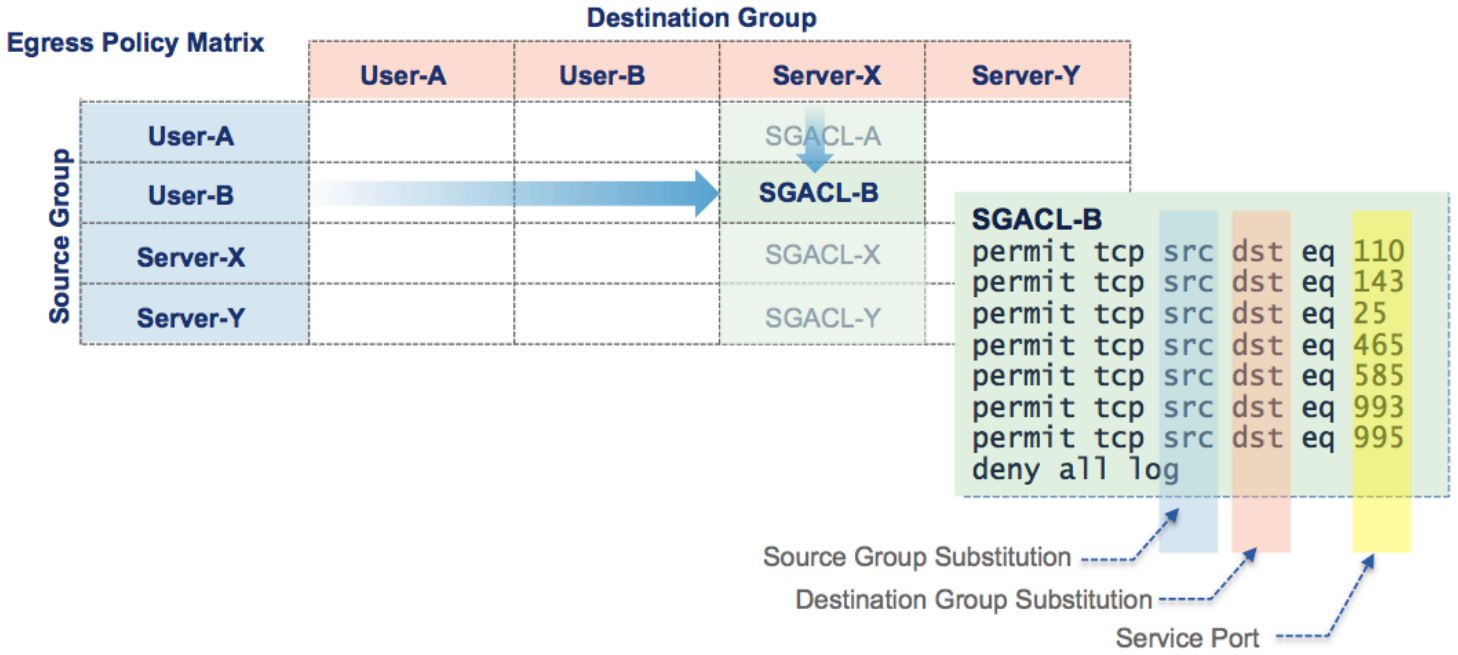
Decoupling policy from subnet

ISE обеспечивает **сегментацию** сети

- Для любых пользователей и устройств
- В качестве инструмента могут быть **любые сетевые устройства** (файерволы, коммутаторы, маршрутизаторы, WiFI…)



Security Group Access Control Lists



Сценарии использования Cisco и Business Impact

#2 DEFence rediness CONditions (DEFCON) with Scalable Group Tag (SGT)

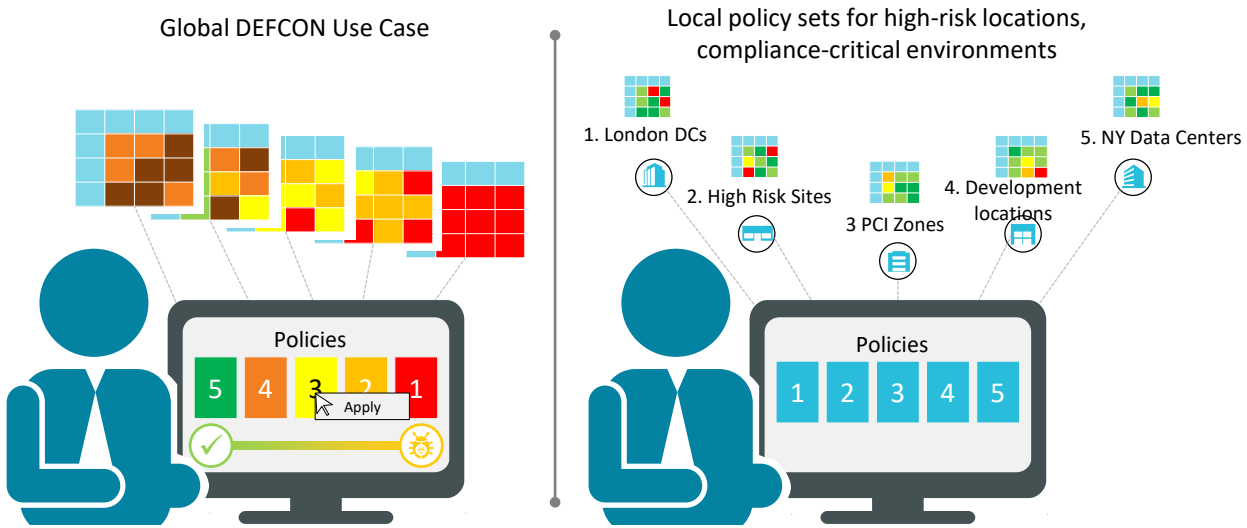
Case / issue:
Необходимо быстро (почти мгновенно) изменить права доступа по всей сети, например в случае вирусной эпидемии, но в текущих реалиях это невозможно, так как требует изменения множества ACL

Root cause:
- Текущие списки доступа (ACL) привязаны к IP-адресации
- Каждый сайт – свой уникальный IP-pool
- Нет единой, полностью детерминированной, матрицы доступа

Solution:
- Политики доступа по SGT привязаны к единой (!) матрице доступа между группами
- DefCon подход предусматривает, что таких «единых матриц» доступа может быть несколько – каждая для своего случая.
- Переключение между матрицами доступа «мирного времени» и «состояния войны» практически мгновенное
- Интеграция с эко-партнёрами по pxGrid (McAfee, Splunk etc.)

Business impact: **HIGH**
- Уменьшение влияния брешей ИБ (минимизация охвата поражения в результате реализации угроз ИБ)
- Business continuity (возможность изолировать LoB приложения от источников угроз)
- Скорость реализации экстренной реакции [переход на «План Б» за считанные минуты]

Политики безопасности с учетом уровня угрозы



DEFCON (аббревиатура, англ. *DEFense readiness CONdition* — готовность обороны) — шкала готовности вооружённых сил Соединённых Штатов Америки. Стандартный протокол в мирное время — DEFCON 5. DEFCON 1 соответствует ожиданию немедленной полномасштабной атаки

Политики DefCon для сети

Multiple levels of policy sets
Applied globally

Standard Policy

Source \ Destination	LoB 1 Employee	LoB 2 Employee	Partner 1	Partner 2	PCI Server	Shared Apps	LoB 1 Apps	LoB 2 Apps
LoB 1 Employee	✓	–	–	–	–	✓	✓	–
LoB 2 Employee	–	✓	–	–	–	✓	–	✓
Partner 1	–	–	✓	–	–	✓	–	–
Partner 2	–	–	–	✓	–	✓	–	–
POS Terminal	–	–	–	–	✓	–	–	–

Ограничение распространения

DEFCON3 Policy

Source \ Destination	LoB 1 Employee	LoB 2 Employee	Partner 1	Partner 2	PCI Server	Shared Apps	LoB 1 Apps	LoB 2 Apps
LoB 1 Employee	–	–	–	–	–	✓	✓	–
LoB 2 Employee	–	–	–	–	–	✓	–	✓
Partner 1	–	–	✓	–	–	–	–	–
Partner 2	–	–	–	✓	–	✓	–	–
POS Terminal	–	–	–	–	✓	–	–	–

Сценарии использования Cisco и Business Impact

#3 Rapid Threat Containment (RTC)

Case / issue:
Необходимо быстро и автоматически изолировать заражённых пользователей (например, при выявлении обращения к командным центрам бот-нетов)

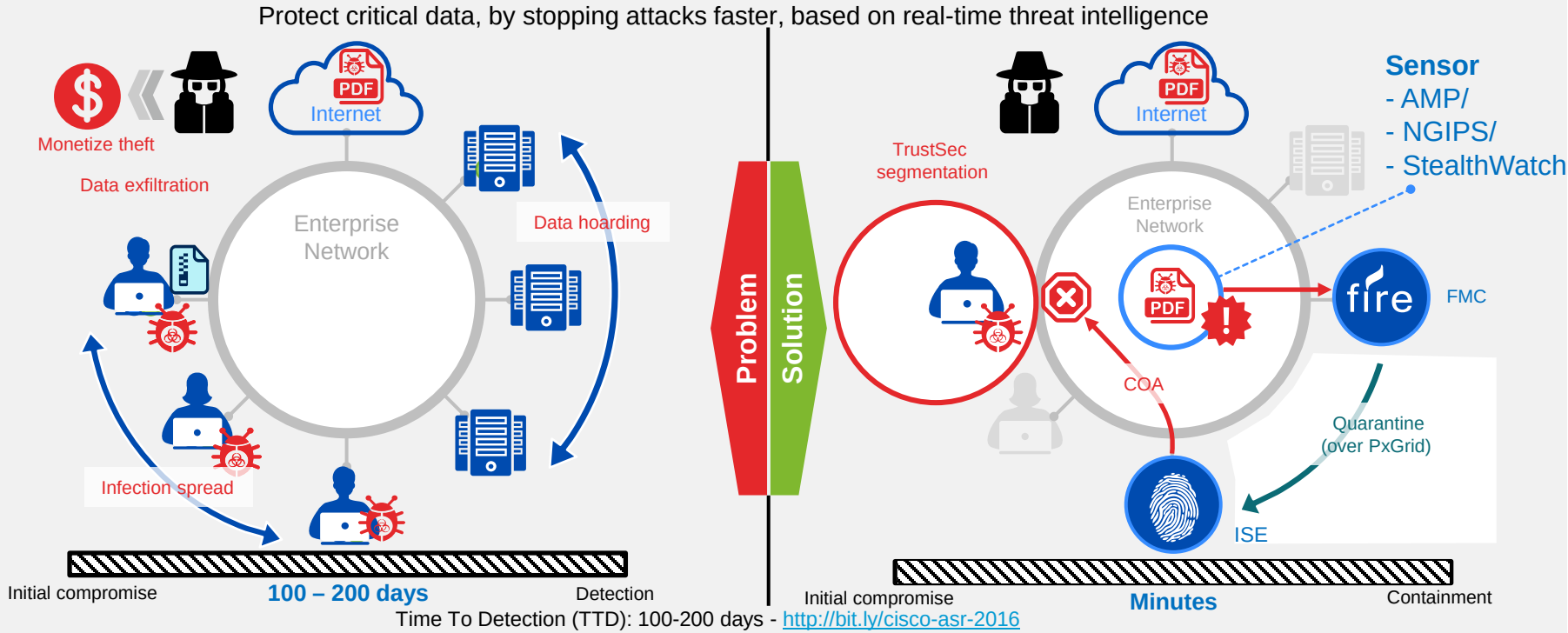
Root cause:
- Продукты ИБ и контроль сетевого доступа не связаны
- Множество клиентов без каких либо агентов на ОС (виртуалки, BYOD, *nix OS)
- Множество клиентов сети не в домене (виртуалки, BYOD, *nix OS)

Solution:
- Автоматизация взаимодействия инструментов ИБ и систем контроля доступа к сети (RTC)
- Реакция на события от продуктов ИБ Cisco (AMP, StealthWatch, FirePower)
- Интеграция с эко-партнёрами по pxGrid (McAfee, Splunk и многие другие.)

Business impact: **HIGH**
- Уменьшение влияния брешей ИБ (минимизация охвата поражения до единичного хоста)
- Business continuity (точечная изоляция/карантин)
- Не требует вмешательства администратора (24X7)
- Дополнительная ценность от уже купленных продуктов ИБ и мониторинга

Объединяем все вместе Rapid Threat Containment (RTC)

Быстрое реагирование



Сценарии использования Cisco и Business Impact

#4 Encrypted Traffic Analytics (ETA) with StealthWatch

Encrypted Traffic Analytics

Case / issue:

- В сети множество шифрованного трафика и его доля растёт из года в год
- Это слепая зона для всех продуктов безопасности

Root cause:

- Malware зачастую использует шифрованные коммуникации (SSL/TLS).
- Без расшифровки трафика понять malware или не-malware трафик в текущих реалиях нет возможности
- Поставить агентское ПО (чтобы увидеть трафик до шифрования) на каждый хост (VMs, BYOD) нет возможности
- SSL offload адресует только часть трафика (много SSL/TLS шифрования, трафик malware)

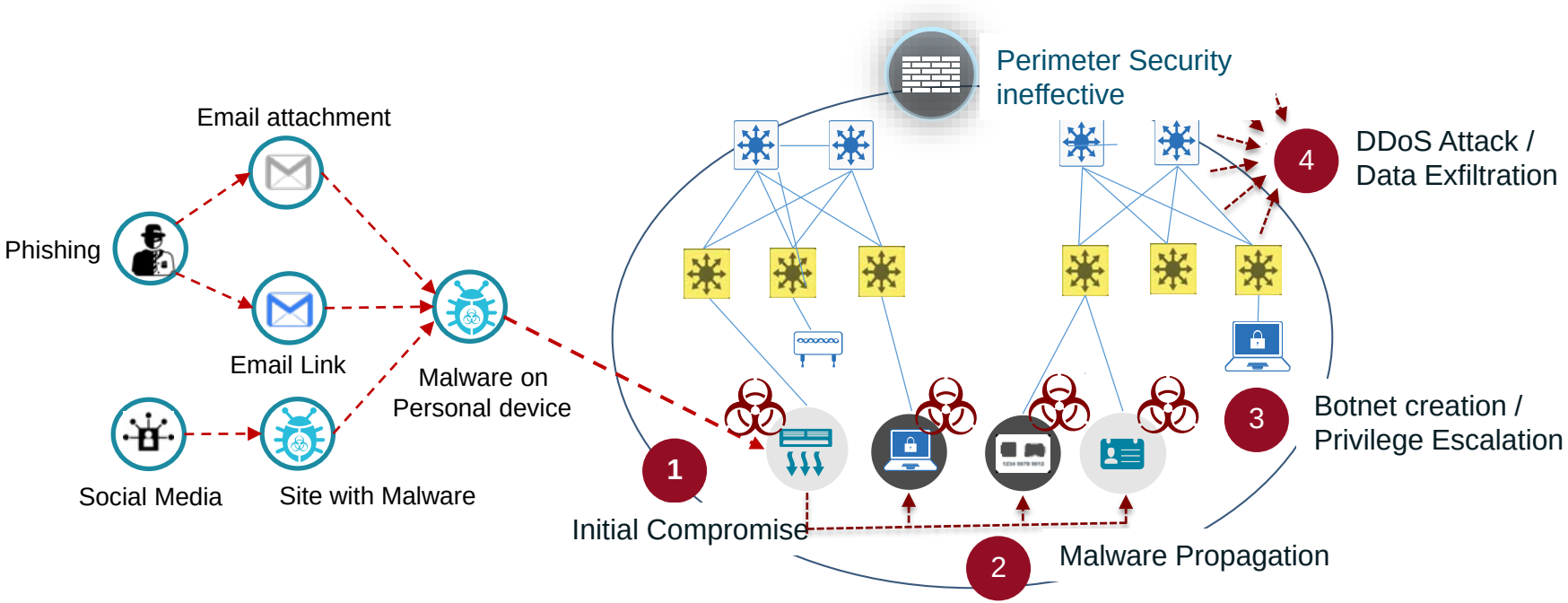
Solution:

- Переход на свичи, которые могут экспортровать NetFlow в Stealthwatch
- Переход на свичи с поддержкой ETA (не все NetFlow устройства поддерживают ETA)
- Управление автоматической реакцией через ISE - Rapid Threat Containment (RTC)

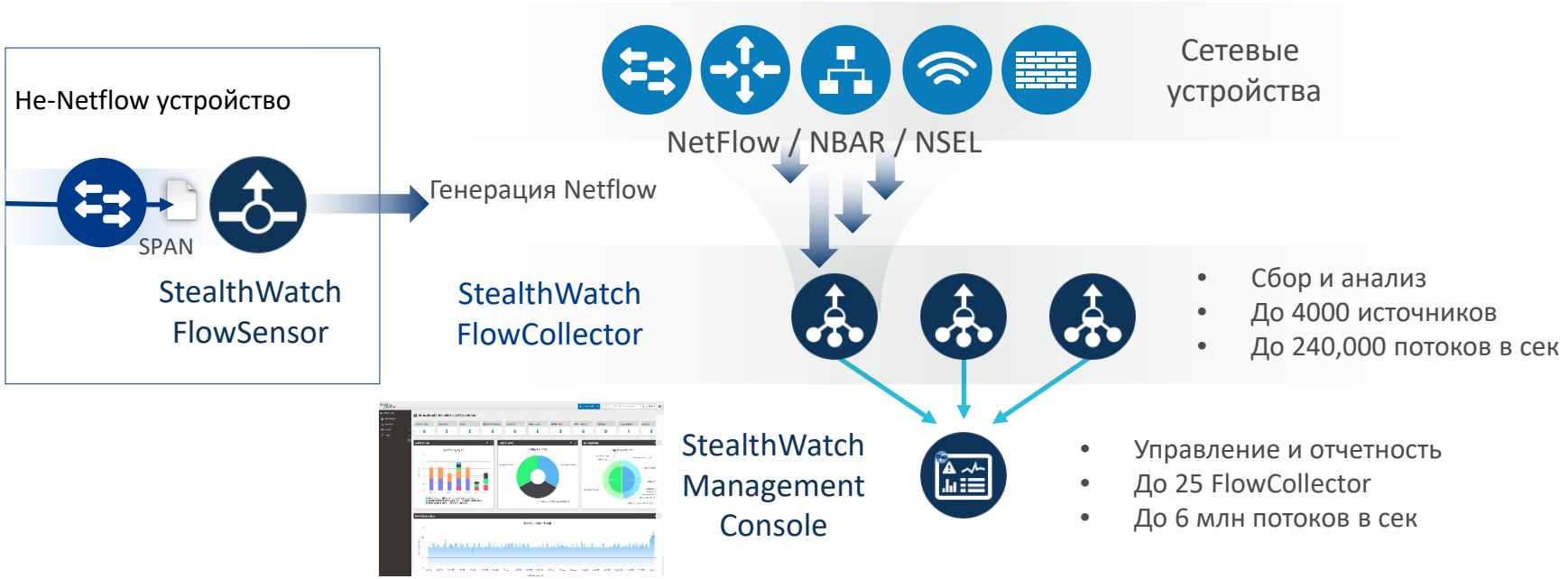
Business impact: **HIGH**

- Бесклиентская защита сети
- Полная наблюдаемость **всех** сетевых endpoint (виртуалок, устройств за хабами и тп)
- Операционная эффективность (нет необходимости заставлять пользователей вводить виртуалки в домен или вручную ставить агентское ПО)
- Обнаружение malware там, где раньше его нельзя было обнаружить **с эффективностью более 99% (!!) и false positive <0.1%**

Надежного периметра уже недостаточно



Обзор системы StealthWatch



Что позволяет обнаруживать NetFlow?

Сканирование сети

Сканирование TCP, UDP, портов по множеству узлов

Обнаружение ботнетов

Когда внутренний узел общается с внешним сервером C&C в течение длительного периода времени

Отказ в обслуживании

SYN Half Open; ICMP/UDP/Port Flood

Фрагментированные атаки

Узел отправляет необычный фрагментированный трафик

Изменение репутации узла

Потенциально скомпрометированные внутренние узлы или получение ненормального скана или иные аномалии

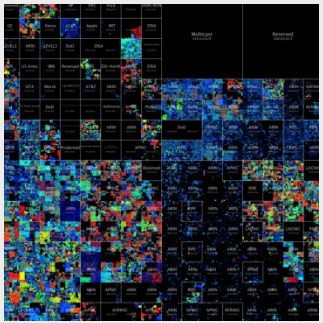
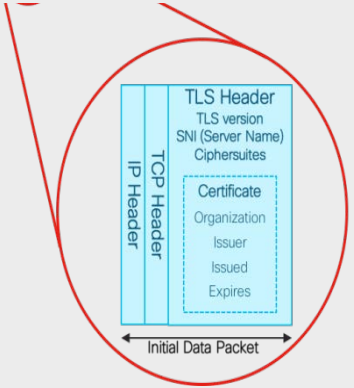
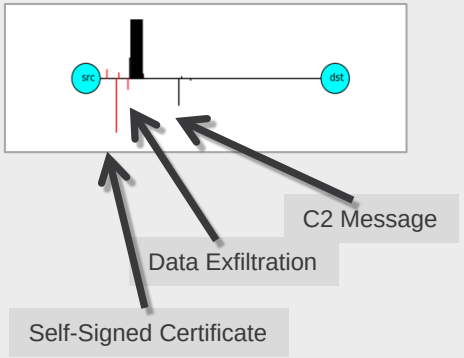
Распространение червей

Инфицированный узел сканирует сеть и соединяется с узлами по сети; другие узлы начинают повторять эти действия

Утечки данных

Большой объем исходящего трафика VS. дневной квоты

How do we inspect encrypted traffic?

Global risk map	Initial Data Packet	Sequence of Packet Lengths and Times
Who's who of the Internet's dark side	**Make the most of the unencrypted fields**	**Identify the content type through the size and timing of packets**
 Broad behavioral information about the servers on the Internet.		

Encrypted Traffic Analytics

cognitive.cisco.com

Network Sensors

NetFlow

Telemetry for Encrypted Malware Detection and Crypto Compliance

Stealthwatch Flow Collector(s)

Enhanced NetFlow

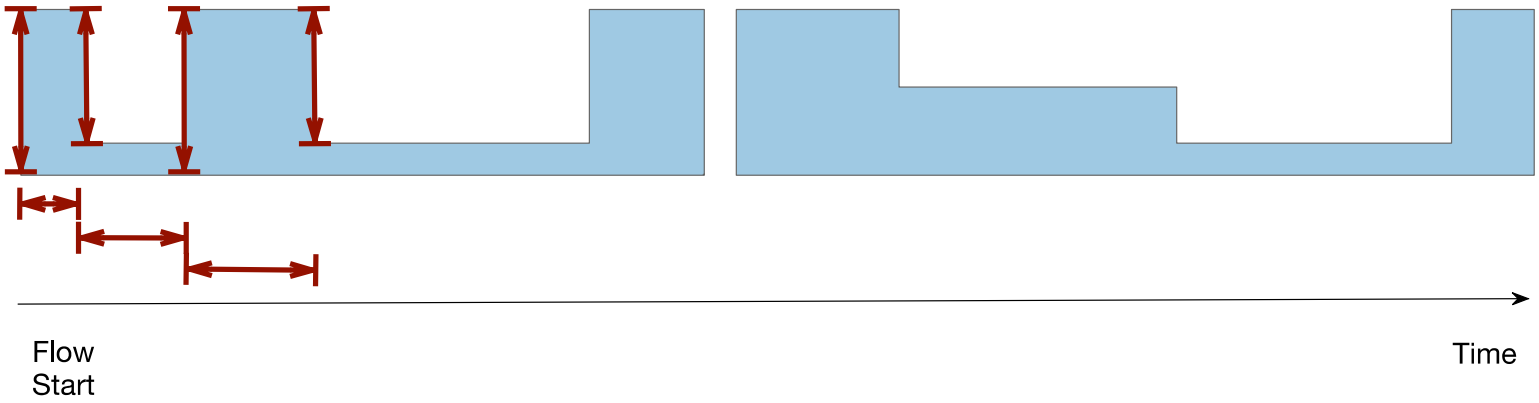
https

Enhanced NetFlow with encrypted traffic analytics from Cisco's newest switches and routers

Stealthwatch enhanced analytics and machine learning reduces threat investigation time

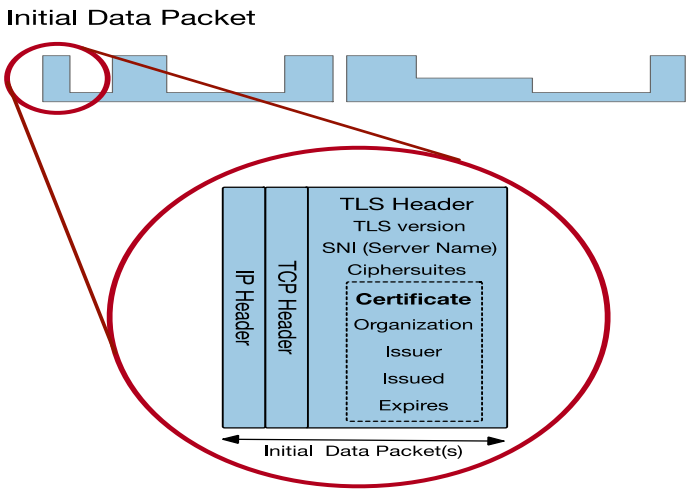
Global-to-local knowledge correlation results in higher precision of threat findings

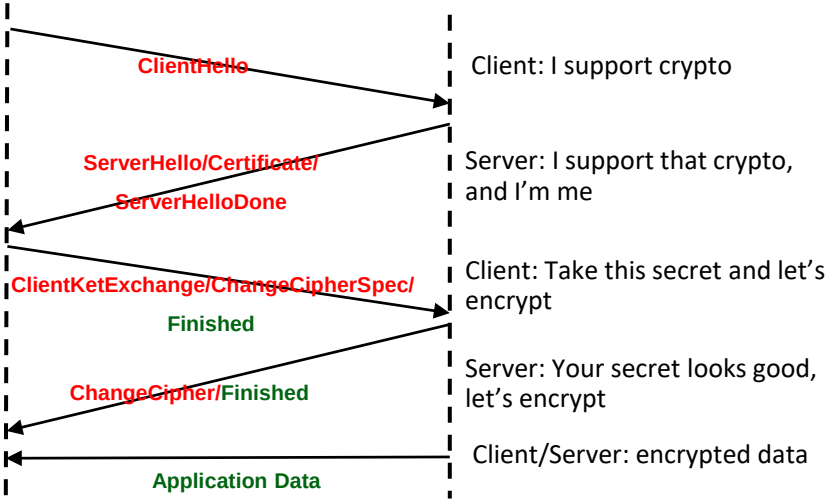
Sequence of Packet Lengths and Times (SPLT)



Malware Behavior	Network Behavior
Communication with command control server	Sequence of packet lengths
Write to the disk	Time interval between packet

Initial Data Packet

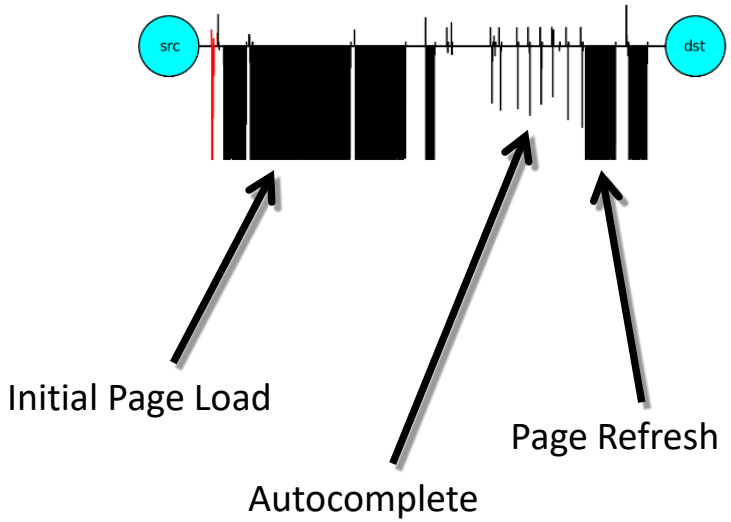




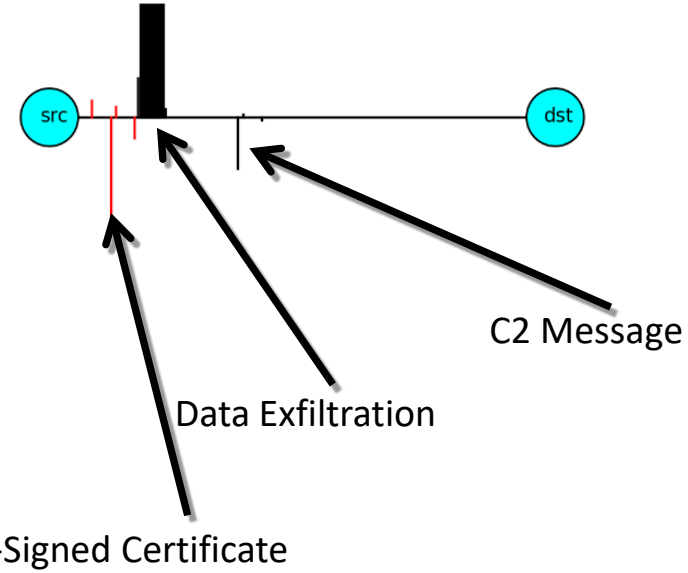
TLS field (in ClientHello)	Inference
Offered Cyphersuites	Browsers prefer heavy weight and more secure encryption algorithms, Mobile applications prefer efficient encryption
Extensions	

Behavioral Patterns w.r.t. Packet Lengths/Times

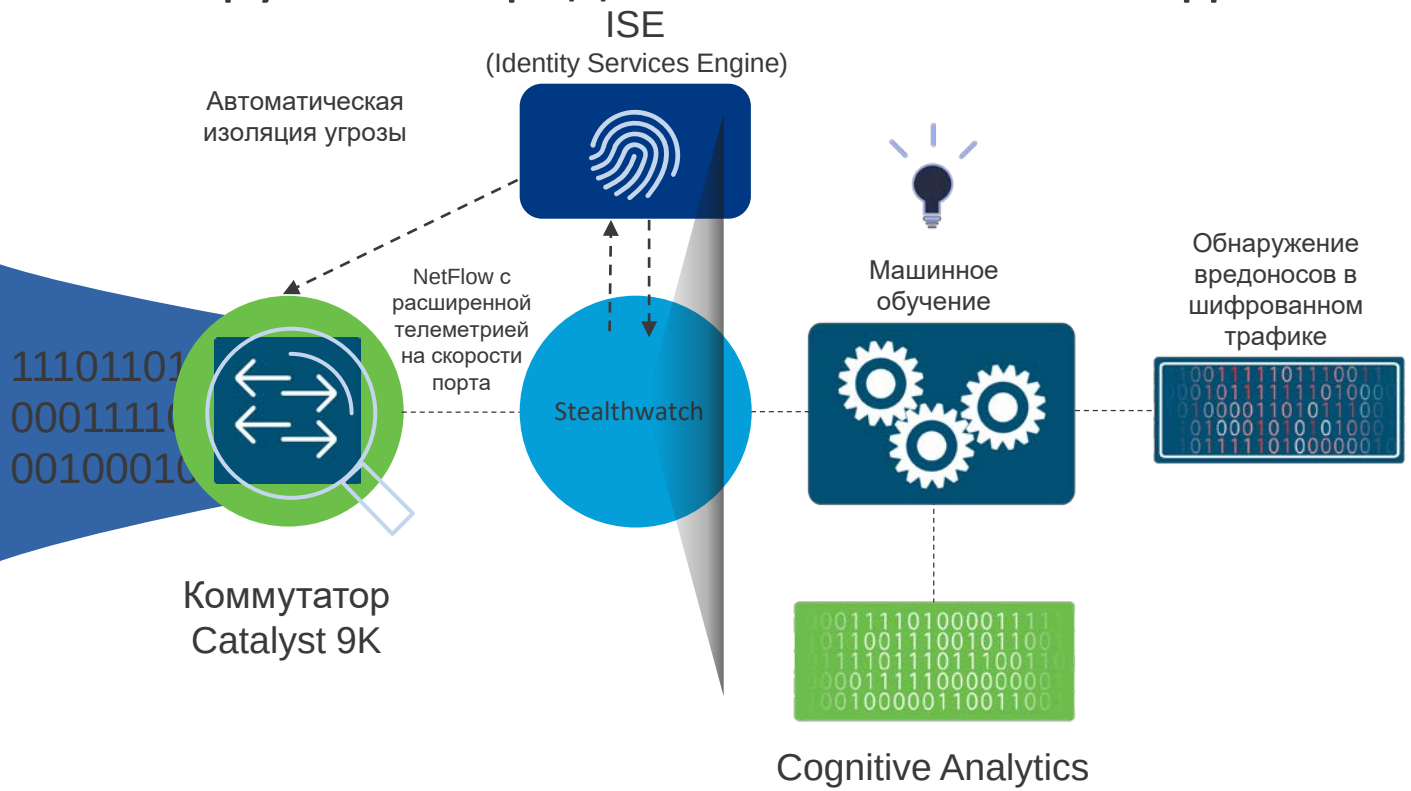
Google Search



Bestafera



Развитие решения Cisco «Сеть как Сенсор»
Обнаружение вредоносного ПО в зашифрованном трафике



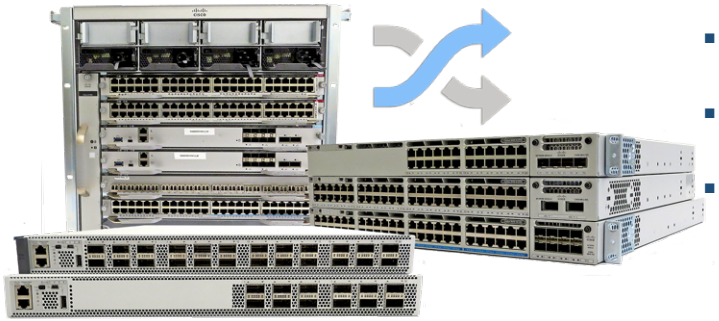
Encrypted Traffic Analytics

99%
точность обнаружения угроз*

0.01%
ложных срабатываний*

*Source : Identifying Encrypted Malware Traffic with Contextual Flow Data, Oct 2016

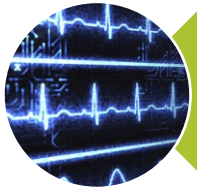
Эксклюзивная поддержка ETA на Catalyst 9K



Специализированная телеметрия

- **Netflow Data:** SrcIP, DstIP, SrcPort, DstPort, Proto, #Bytes, #Packets
- **Intraflow Data:** Sequence of Packet Lengths & Times (SPLT), Byte Distribution, …
- **TLS Metadata:** Extensions, Ciphersuites, SNI, Certificate Strings, …

Основная задача



Обнаружение угроз в зашифрованном трафике

Вторичная задача

Аудит использования криптографии

Сценарии использования Cisco и Business Impact

#5 VLAN per MAC

Case / issue:

- Разработчики используют виртуальные машины на лаптопах. Необходимо разделить доступ корпоративной ОС и виртуалке (которая не в домене и без агента ИБ)

Root cause:

- 802.1x классически подразумевает VLAN per port (точнее data VLAN и voice VLAN)
- Порт подключения пользователей не транковый
- Раньше не было возможности выделить VLAN на MAC

Solution:

- Переход на свичи с поддержкой VLAN per MAC
- Управление политикой через ISE

Segmentation
VLAN per MAC

Business impact: **HIGH**

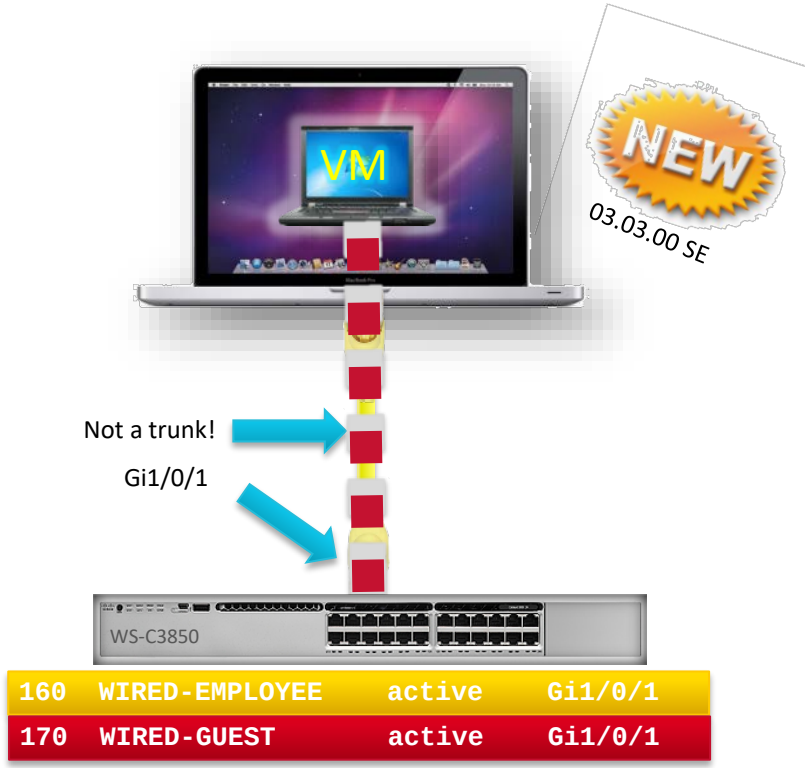
- Бесклиентская защита сети
- Полная наблюдаемость **всех** сетевых endpoint (виртуалок, устройств за хабами и тп)
- Операционная эффективность (нет необходимости заставлять пользователей вводить виртуалки в домен или вручную ставить агентское ПО)

Per MAC per VLAN Assignment

"MAC based VLANs"

- Before Cat3850 / Cat3650: One port, one VLAN per access port (1:1)
- Exception: Voice (one Data Device untagged, one Voice Device tagged w/ VVLAN)
- Later: Allowing VLAN assignment on multi-authentication ports, but first device 'rules' the port.
- **Now with Catalyst 2960X, 3850 & 3650: Each session can have individual VLAN assigned**
  - 2960X → 15.2(2)E
  - C3850 → 03.03.00SE
  - C3650 → 03.03.00SE

And now it is available on Catalyst 9k



Сценарии использования Cisco и Business Impact

#6 MACSec

Case / issue:

- Обеспечить защиту трафика (конфиденциальность), который проходит по оптике по недоверенной территории, например, между зданиями и этажами зданий

Root cause:

- Необходимо обеспечить шифрование трафика
- Шифрование средствами VPN (IPSec) дорого, не производительно и сложно в поддержке
- VPN технологии имеют целый ряд ограничений (например, непрозрачность для сетевого трафика)

Solution:

- Переход на свичи с поддержкой MACSec на всех портах
- Применение прозрачного шифрования wire speed с поддержкой современных протоколов шифрования (AES-256)

Business impact: **MEDIUM**

- Защита конфиденциальности корпоративных данных
- Защита данных заказчиков (минимизация возможностей утечки данных через съём с изгибов оптики)
- Простота использования и поддержки

Сценарии использования Cisco и Business Impact

#7 Sofware Defined Access (SDA)

Case / issue:

- Скорость открытия нового офиса – недели, так как требуется настройка оборудования
- Бизнес хочет открывать офисы по требованию, как можно быстрее

Root cause:

- Настройка оборудоавния на каждом сайте – рутинный процесс, требущий времени
- Требуется привлечение высококвалифицированных специалистов, занятых другой работой (планирование)
- Кроме простого connectivity требуется настройка продвинутых функций (безопасность, сегментация, QoS)
- Классический (не SDN) подход не способен обеспечить такой скорости

Solution:

- Переход на свичи с SDA
- Переход на SDA по мере необходимости (перспектива, не учтено в предложении, но оборудование готово к SDA)

Business impact: **HIGH (перспективно)**

- Agile IT
- Перспективные технологии обеспечивающие полный жизненный цикл сети: Design, Policy, Provisioning, Assurance
- Операционная эффективность
- Стандартизация подходов к развитию сети
- Возможность менять дизайн сети по требованию внешних приложений (Software Defined Network)
- Повышение уровня информационной безопасности

SD Access Use Cases

1. **Security and segmentation**
2. **User mobility**
3. **Guest access**
4. **IoT integration**
5. **Monitoring and troubleshooting**
6. **Cloud/data center integration**
7. **Branch integration**

SD Access. Собираем всё вместе

Как снизить стоимость владения SDA?

Модульные коммутаторы Catalyst 9400 вместо 9300

Подписки DNA Advantage на 5/7 лет вместо 3 лет

ISE на всю сеть (снижение цены от к-ва)

C1-DNA-Adv особенно для StealthWatch

Бандлы, промо, case study

Сценарии использования Cisco и Business Impact

#8 Application Visibility and Control (AVC)

Case / issue:

- Необходимо понимание трафика уровня приложений (Application Visibility)
- Необхоимо приоритизировать трафик бизнес критических приложений и настроить баланс для работы остальных

Root cause:

- Множество приложений используют общие протоколы как транспорт (HTTP), “IP_addr:port” не определяет приложение
- NG-FW, которые могут распознавать трафик приложений, обычно стоят на периметре сети
- Маршрутизаторы Cisco (AVC), которые понимают трафик приложений, стоят на границе сети
- Фактически средств набюдения трафика приложений и управления трафиком приложений внутри сети раньше не хватало.

Solution:

- Cisco Application Visibility and Control
- Обработка сетевого трафика с пониманием приложений и их особенностей
- Возможность строить системы мониторинга сети и безопасности с пониманием трафика приложенй (Flexible NetFlow)

Business impact: **HIGH (перспективно)**

- Business Continuity. Понимание работоспособности бизнес-критических приложений.
- Бизнес релевантность сетевых данных
- Операционная эффективность

Сценарии использования Cisco и Business Impact

#9 Reediness for innovations

Case / issue:

- Необходимо иметь надёжную платформу с длительным циклом жизни и перспективой развития
- Множество потенциальных требований: Smart Lightning, Smart Building, IoT, Wi-Fi next-gen.

Root cause:

- Планируя сеть как платформу для бизнеса на 5-7 лет тяжело предугадать требования бизнеса
- Повсеместная автоматизация и прорыв в тренде IoT (интернет вещей)
- Громадный потенциал технологий Smart Building с предсказуемым ROI
- Рост потребления питания по витой паре (PoE), новые стандартов Wi-Fi и появление всё новых «умных» устройств

Solution:

- Новая линейка коммутаторов с использованием проверенной и отлаженной архитектуры + средства автоматизации
- Програмируемые ASIC – возможность дописывать аппаратную поддержку новых функций «на лету»
- Аппаратная готовность к **60**-100Вт/порт (**UPoE**) и новым скоростям по витой паре **mGig** (**1G –> 2.5G –> 5G –> 10G –>** 25G)
- Поддержка IoT стандартов (CoAP, CoAP Proxi, Containers и прочих)
- Подписка на функционал как способ получения инноваций во время жизни сети

Business impact: **MEDIUM (перспективно - HIGH)**

- Investment protection. Переиспользование сетевого оборудования в перспективных сценариях от безопасности до Smart XX.
- Готовность к концепции «офис будущего» для нужд бизнеса, ИТ, ИБ, ФизБ, HR.
- Ongoing access to innovation. Готовность к новым стандартам и технологиям, возможность получения инноваций по подписке.

X86 Architecture

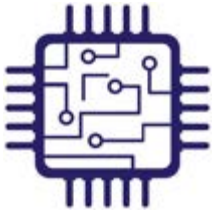
Modular Software

Patchability

Containers

Storage

Analytics



Programmable ASIC

Data Modeling

NETCONF/ YANG/Python

Threat Detection

Controller based networking

60W UPoE

Uninterrupted Power

Multi Gig Density

AVB

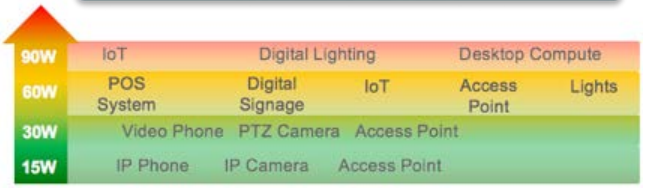
802.11ax. UPoE, 5G / 25G Uplinks

Сеть готовая к инновациям

More Agile & Flexible

- ✓ True SDN with Software Defined Access
- ✓ Programmable & Flexible Hardware & Software

More Power



More Density

- ✓ 48 x mGig Ports – Hardware Leadership; Deployment Flexibility

5G/25G transition

More Secure

- ✓ Encrypted Malware detection/mitigation, Distributed FW Scale
- ✓ Host Best of the Breed Security Apps

More Bandwidth

- ✓ Faster wireless standard needs larger backhaul pipe

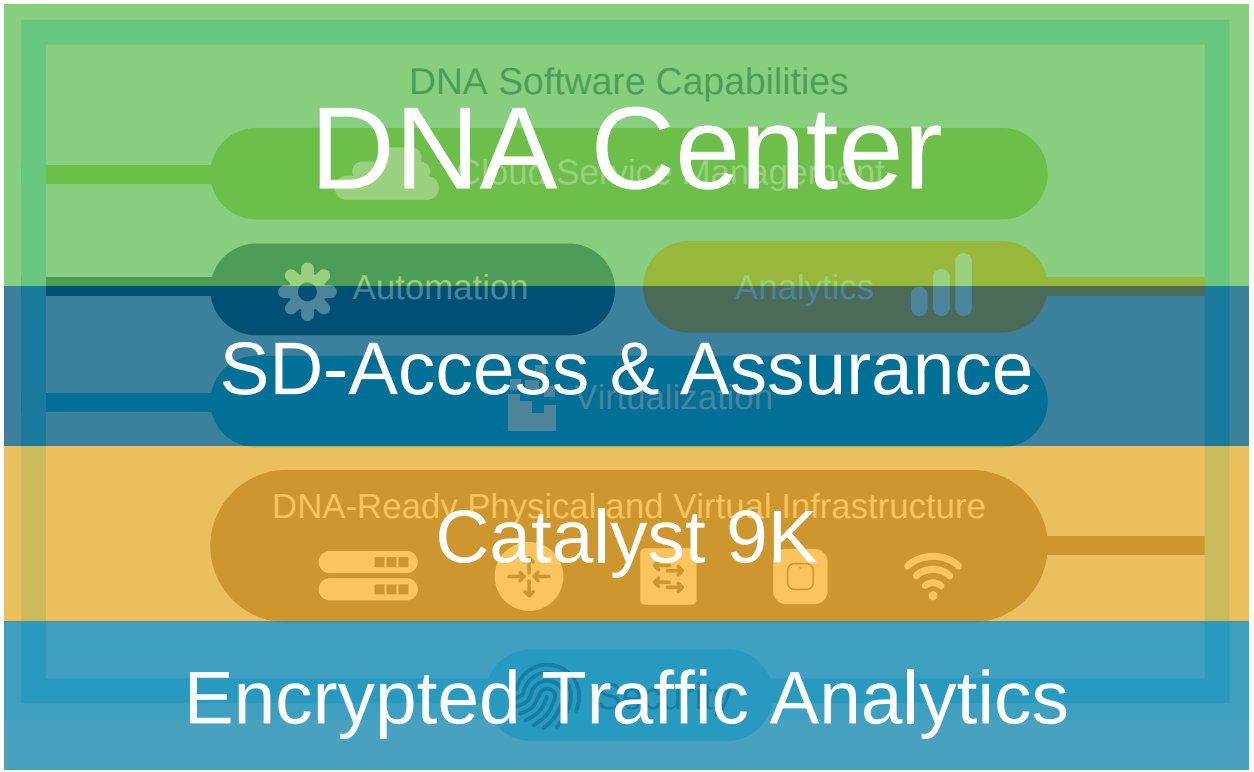
Cisco Catalyst 9300/9400 offer UPoE (and support for upcoming powering standard .3bt) & Offers all ports with mGig capabilities to support future data hungry devices

Бизнес преимущества решения Cisco

- ✓ **Investment Protection.** Простота миграции с существующей Cisco сети с сохранением преемственности конфигураций и парадигмы управления.
- ✓ **Time to Market.** Ускорение перемещения сотрудников между командами за счет использования Cisco TrustSec (SGT).
- ✓ **Security.** Значительное повышени информационной безопасности. Защита данных на скорости порта (MACSec).
- ✓ **Human Factor Mitigation.** Уменьшение влияния человеческого фактора на состояние ИБ.
- ✓ **Compliance.** Простота прохождения внутренних и внешних аудитов.
- ✓ **Business Continuity.** Близкая к мгновенной автоматизированная изоляция инцидентов ИБ в режиме 24/7 без остановки всей сети.
- ✓ **IT Agility.** Быстрое изменение сети под требования бизнеса.
- ✓ **Access to Innovations.** Возможность запуска новых технологий и сетевых сервисов, включая ETA, SD Access, mGig, UPOE, RTC.
- ✓ **Operational Efficiency.** Нет нужно заставлять пользователей вводить тестовые VMs в домен или требовать устанавливать на них агентское ПО
- ✓ **Financial Impact.** Сокращение операционных затрат на 80% и дополнительное сокращение операционных издержек на 61%** после перехода на SD Access

** SD – Access Overview and TCO Analysis. White Paper – доступно по NDA

Digital Network Architecture – What's New




CISCO