



Комплексная безопасность в инфраструктуре DNA

Дмитрий Казаков

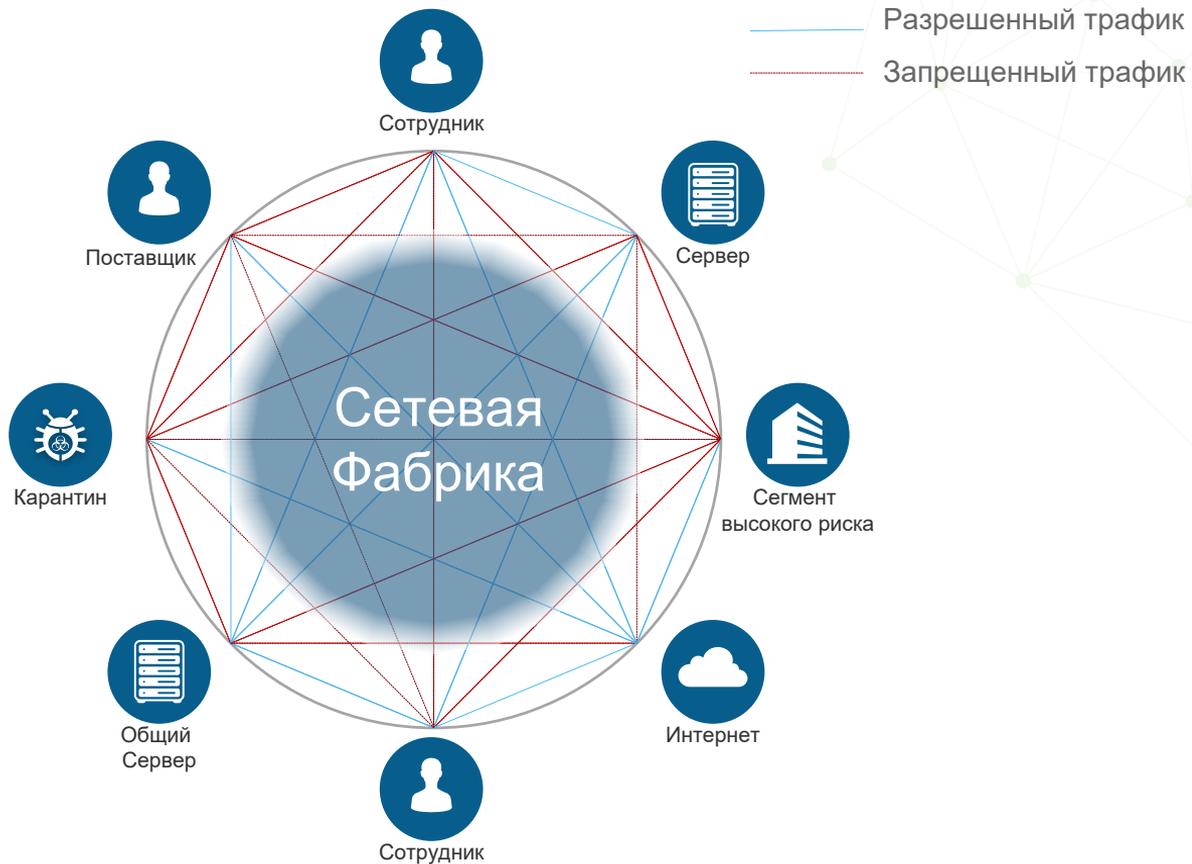
Системный инженер-консультант

CCIE Security, CISSP, CEN

Безопасности нужна видимость контекста и контроль

Четкое понимание потоков трафика с контекстом

Проще создавать и применять политики основанные на контексте



БЕЗОПАСНОСТЬ ДОСТУПА



Пропустить разрешенное и авторизованное

РОЛЕВАЯ СЕГМЕНТАЦИЯ



Логическая сегментация, с использованием динамического контроля угроз

КОНТРОЛЬ КОНТЕНТА



Контроль разрешенного контента

ПОВЕДЕНЧЕСКИЙ АНАЛИЗ

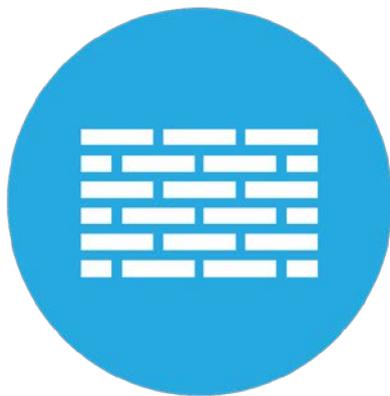


Инспекция и анализ действий после разрешения доступа

Нужно начать с
релевантных рисков,
угроз и требований
ПОЛИТИК ...



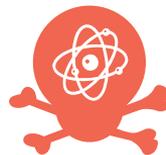
...И защититься от них.



Угрозы



Зомби



DDoS



Имперсонализация



Разрушение



Трояни



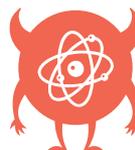
Черви



Шпионаж



Command
& Control



Zero
Days



Внедрение



Внедрение сервиса



Вывод данных



Шпионское ПО

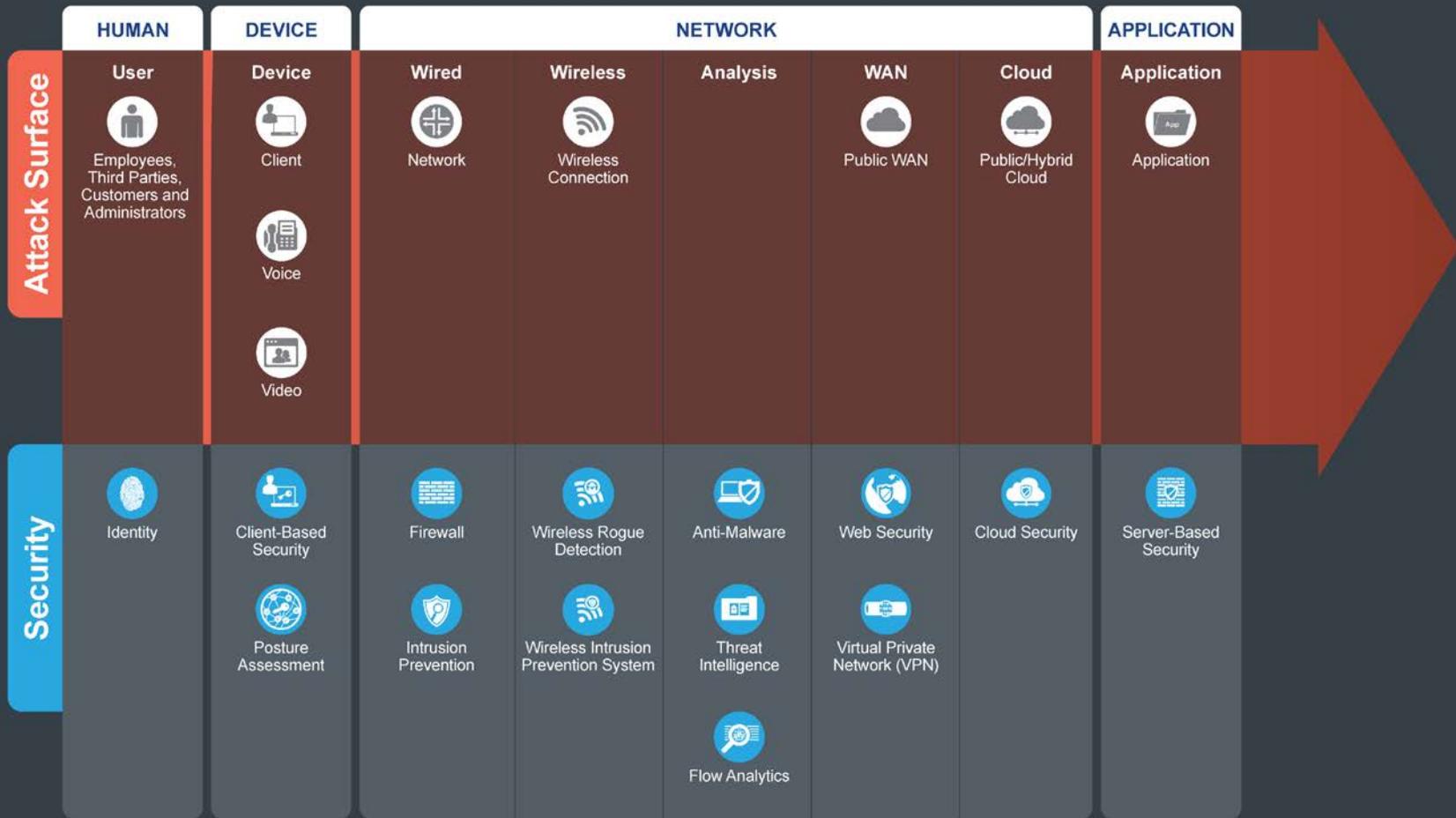


Вирусы

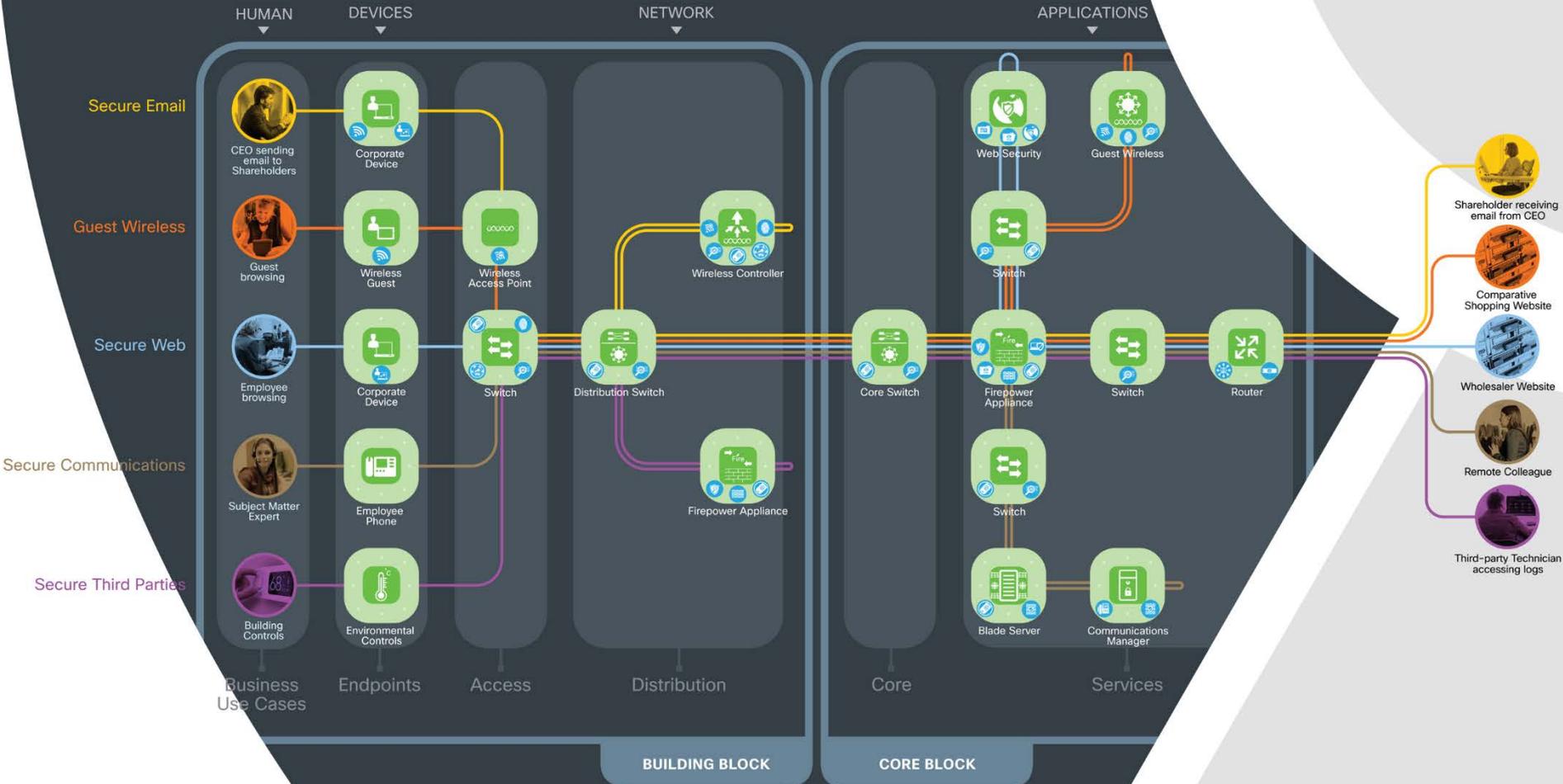


Сбор данных

Примеры



Campus Architecture



Безопасность доступа



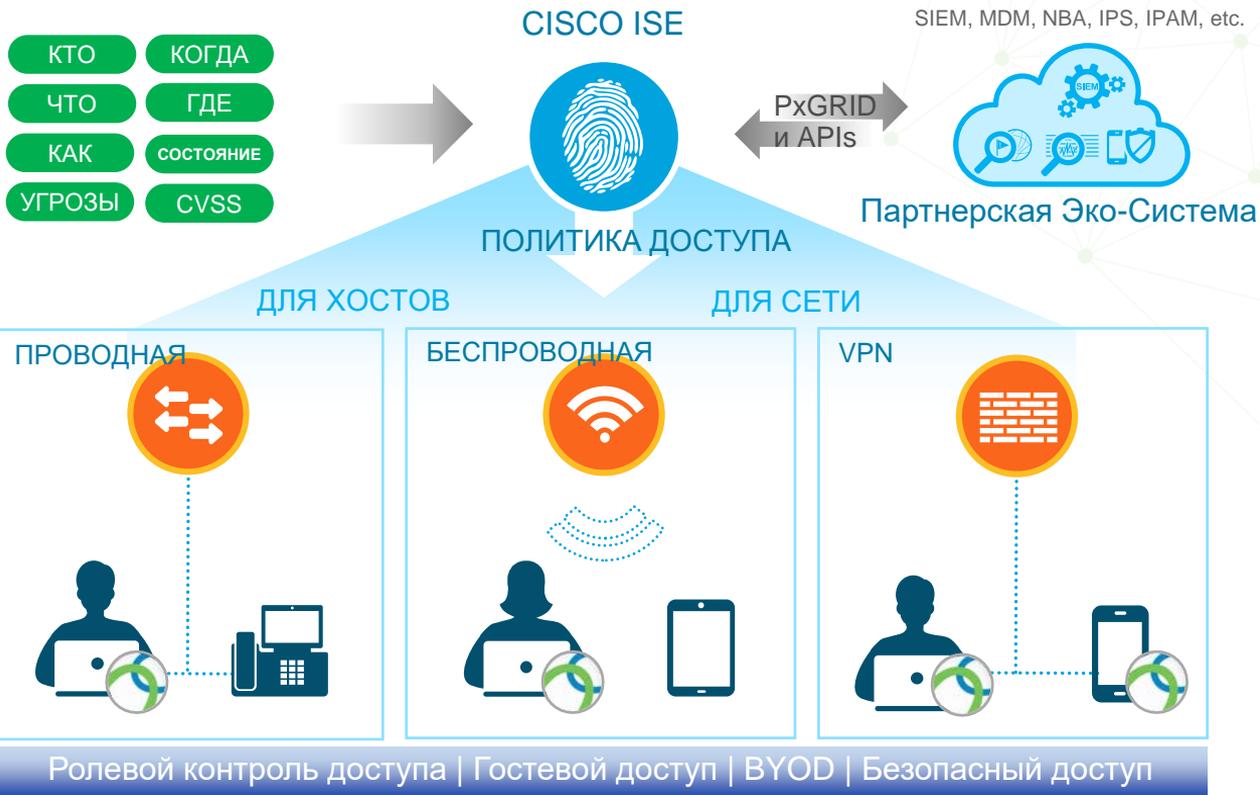
Cisco ISE и Anyconnect

Cisco ISE

Сервис контекстных политик по контролю доступа в проводных, беспроводных и VPN сетях

Cisco Anyconnect

Суппликант для проводного, беспроводного и VPN доступа. Сервис включает: оценку соответствия, Защиту от Malware, Web-безопасность, видимость сети, приложений и другое..



Cisco ISE Профилирование

1.5
МЛН

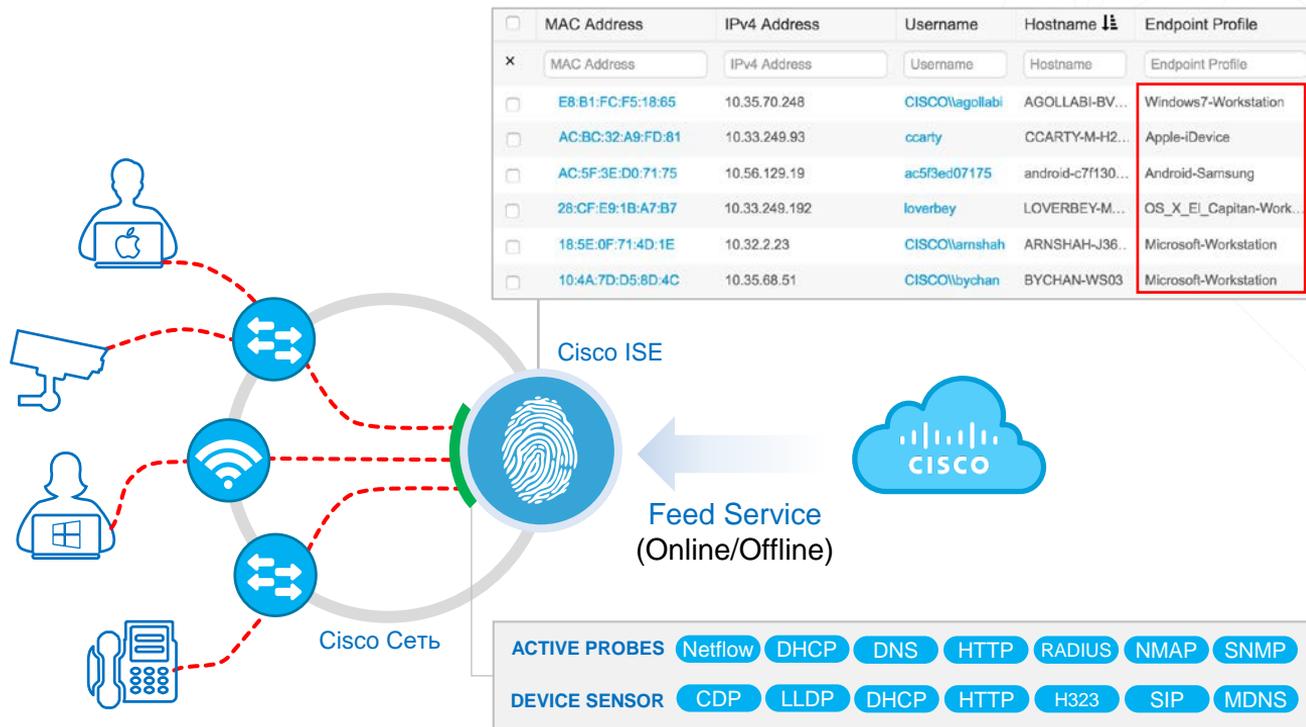
Устройств с '50' атрибутами
каждый можно хранить

550+

Высокоуровневые вложенные
профили.
+Периодические обновления

250+

Профили медицинских
устройств



Видимость групп и пользователей

The screenshot displays the Cisco Identity Services Engine (ISE) interface, focusing on user and endpoint visibility. The interface is divided into several panels:

- Users Panel:** Shows 'Employees' and 'Guest' user lists. A search bar is visible with 'First Name' and 'Dmitry' as input. Below the search bar, a list of users is shown: Alexey, НИКИТА, and ВАДИМ.
- Filters:** 'DEPARTMENT' and 'LOCATION' filters are present, with a 'Refresh' button.
- Endpoint Utilizations:** Two donut charts are shown: 'MANUFACTURERS' (with segments for 'amer... inc.: [5.09%]', 'apple, inc.: [27.27%]', and '... phom... a ltd: [63.64%]') and 'ENDPOINT UTILIZATIONS' (with segments for 'CPU', 'Memory', and 'Disk'). A search bar for 'Devices with over % CPU usage' is also visible.
- Endpoints Panel:** Shows a list of endpoints with a 'Refresh' button. A table below the list displays endpoint details:

MAC Address	BIOS Manufacturer	BIOS Serial Number	BIOS Model	Attached devices	CPU Name
00:0C:29:CC:77:CA	Phoenix Technologies LTD	VMware-56 4d 78 29 46 ba 8f 1...	VMware Virtual Platform	9	
00:22:43:2C:BA:AA	American Megatrends Inc.	SSN12345678901234567	N10E	12	
00:50:56:99:3D:EC	Phoenix Technologies LTD	VMware-42 19 95 7b 4c e3 b5 3...	VMware Virtual Platform	0	
00:50:56:99:D0:C1	Phoenix Technologies LTD	VMware-42 19 e1 87 61 a4 ed d...	VMware Virtual Platform	4	
00:50:56:A4:91:38	Phoenix Technologies LTD	VMware-42 24 29 d0 26 a3 d3 7...	VMware Virtual Platform	0	Intel(R) Core(TM) i7-6700K CPU @ 4.00GHz
00:50:56:A4:D1:02	Phoenix Technologies LTD	VMware-42 24 a3 f1 79 37 4d ce...	VMware Virtual Platform	4	Intel(R) Core(TM) i7-6700K CPU @ 4.00GHz
00:FF:08:43:DB:43	Phoenix Technologies LTD	VMware-42 24 29 d0 26 a3 d3 7...	VMware Virtual Platform	0	Intel(R) Core(TM) i7-6700K CPU @ 4.00GHz

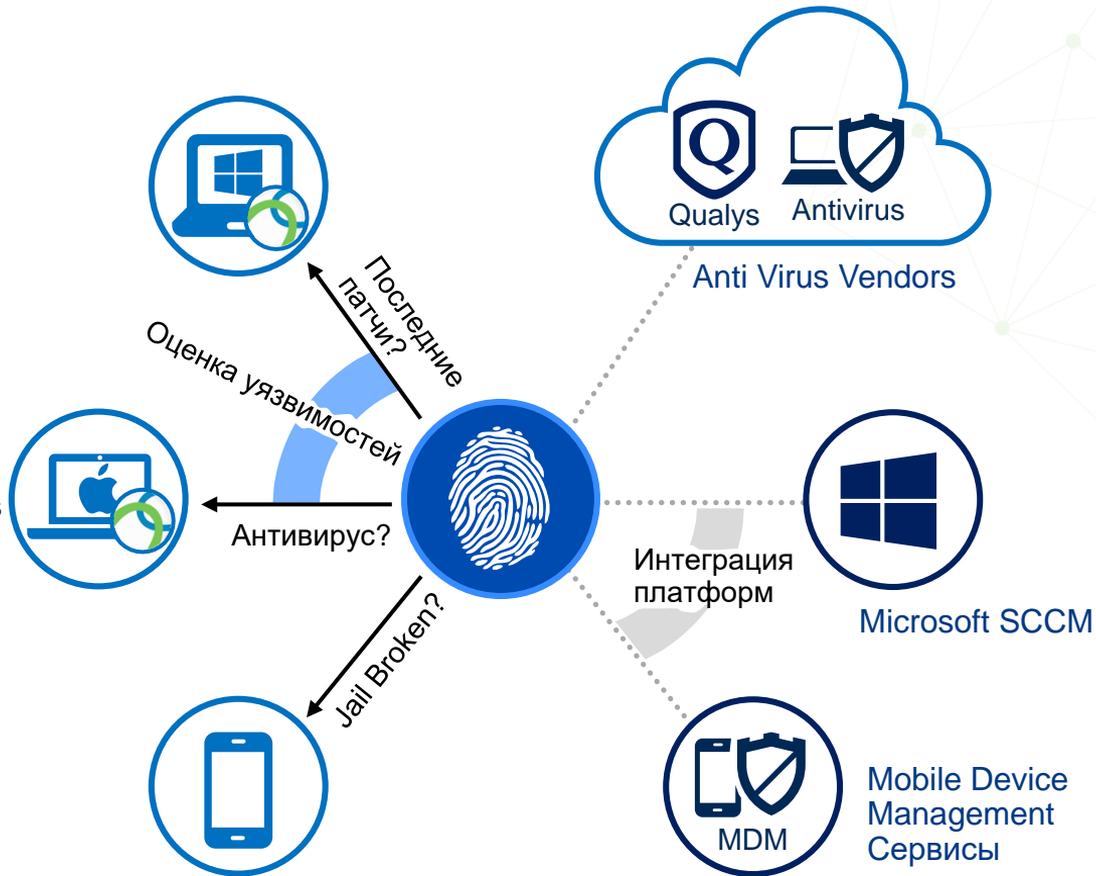
А что с оценкой состояния?

Проверить здоровье хоста

Оценка состояния определяет уровень соответствия с политикой безопасности компании

Оценка состояния процесс:

- ▶ **АУТЕНТИФИКАЦИЯ УСТРОЙСТВА/ПОЛЬЗОВАТЕЛЯ**
Оценка: Неизвестно / Не Соответствует ?
- ▶ **КАРАНТИН**
Ограниченный доступ: VLAN / dACL / SGTs
- ▶ **ОЦЕНКА СОСТОЯНИЯ**
Проверка Hotfix, AV, Pin защита, Jail broken, и тд.
- ▶ **ИСПРАВЛЕНИЕ**
WSUS, Запуск приложения, Скрипты, MDM, и тд.
- ▶ **СМЕНА АВТОРИЗАЦИИ**
Полный доступ – VLAN / dACL / SGTs.



Контекст это всё



НЕИЗВЕСТНО

Отсутствие контекста

IP ADDRESS: 192.168.2.101

НЕИЗВЕСТНО

НЕИЗВЕСТНО

НЕИЗВЕСТНО

НЕИЗВЕСТНО

НЕИЗВЕСТНО

РЕЗУЛЬТАТ

ДОСТУП К IP
(ЛЮБОЕ УСТРОЙСТВО / ПОЛЬЗОВАТЕЛЬ)



Богатый контекст



Дмитрий Казаков (СОТРУДНИК)



WINDOWS WORKSTATION



ЗДАНИЕ-А-ЭТАЖ-13



10:30 AM MSK APR 27



БЕСПРОВОДНАЯ СЕТЬ



НЕТ УГРОЗ / УЯЗВИМОСТЕЙ

РЕЗУЛЬТАТ

РОЛЕВОЙ ДОСТУП



ИЗВЕСТНО

Обмен контекстом

Обогатить контекст (для Политики Доступа)
Угрозы, Уровень уязвимости, MDM атрибуты, др

Кто
Что
Когда
Где
Как
Оценка
Угрозы
Уязвимости

Контекст



Cisco ISE

- SYSLOG
- PXGRID
- REST API



Экосистемные партнеры

Контекстные действия

Политики МСЭ основанные на идентификации,
Доступ в облака со знанием угроз,
Поведенческий анализ с учетом групп/пользователей и др.

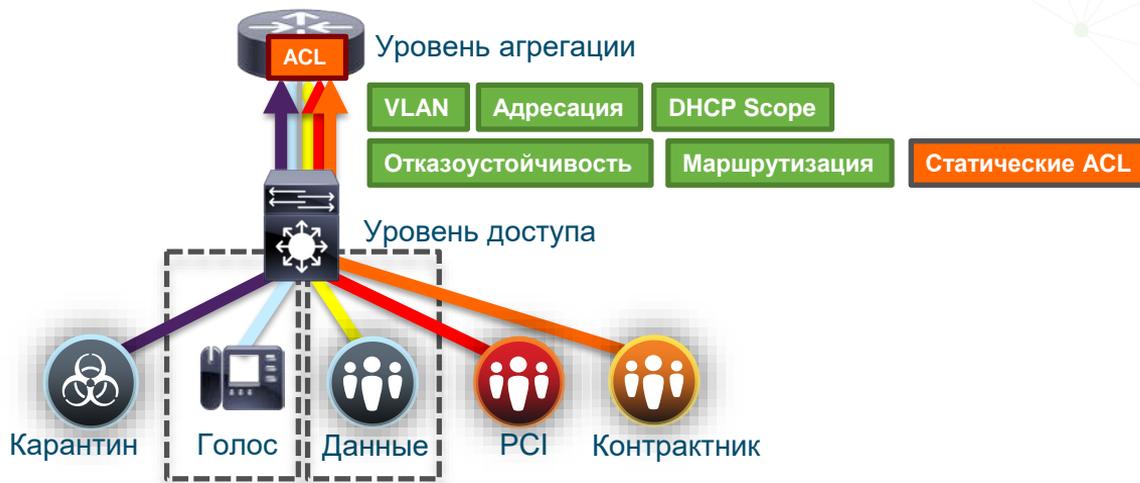
Ролевая сегментация



Традиционная сегментация



Дизайн должен повторяться для этажей, зданий, офисов и других объектов. Затраты могут быть экстремально высоки

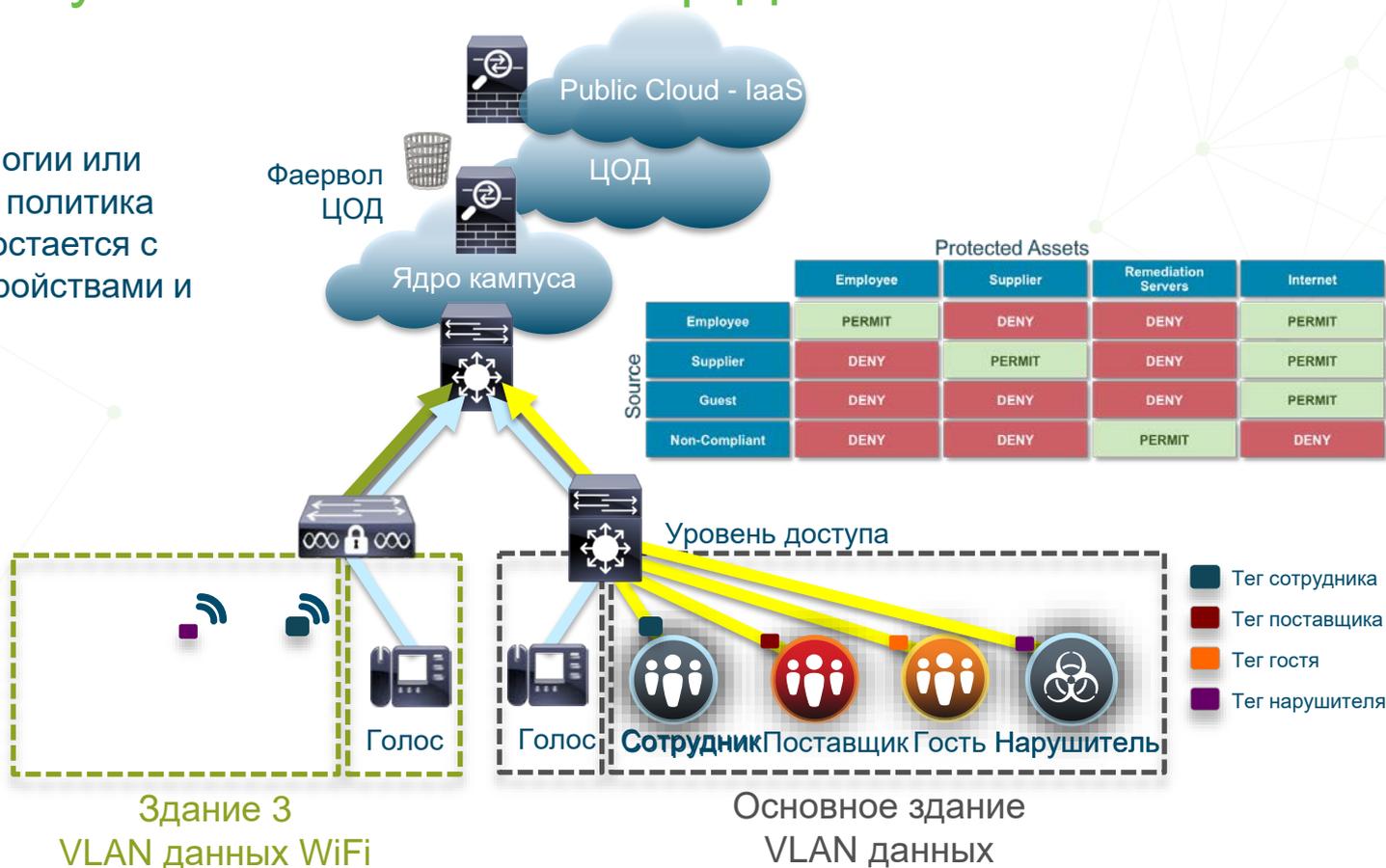


Большая стоимость внедрения VLAN

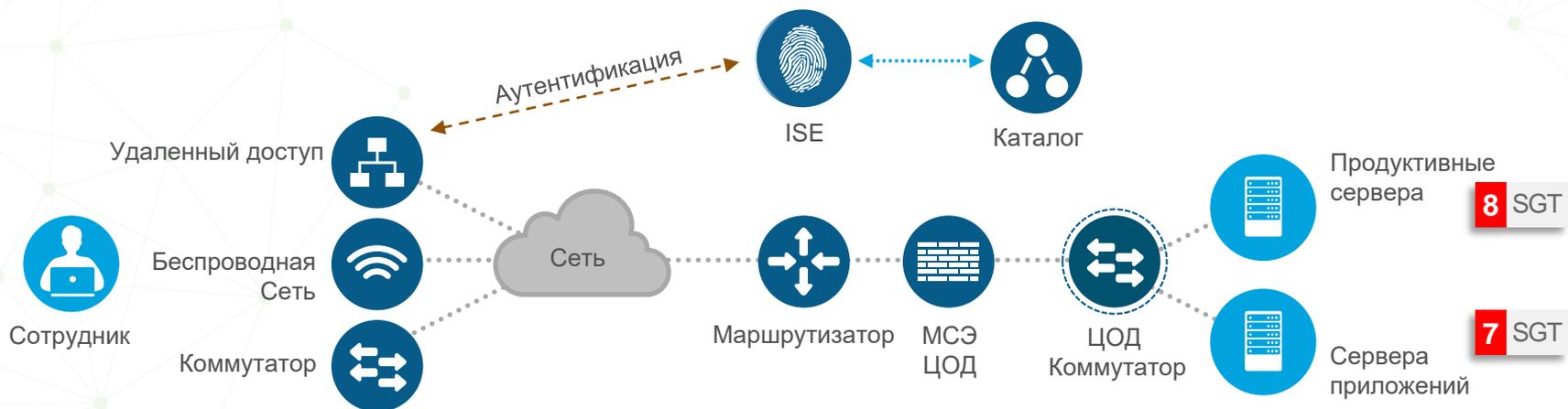
Контроль доступа пользователя в ЦОД с TrustSec

Независимо от топологии или месторасположения, политика (Security Group Tag) остается с пользователями, устройствами и серверами

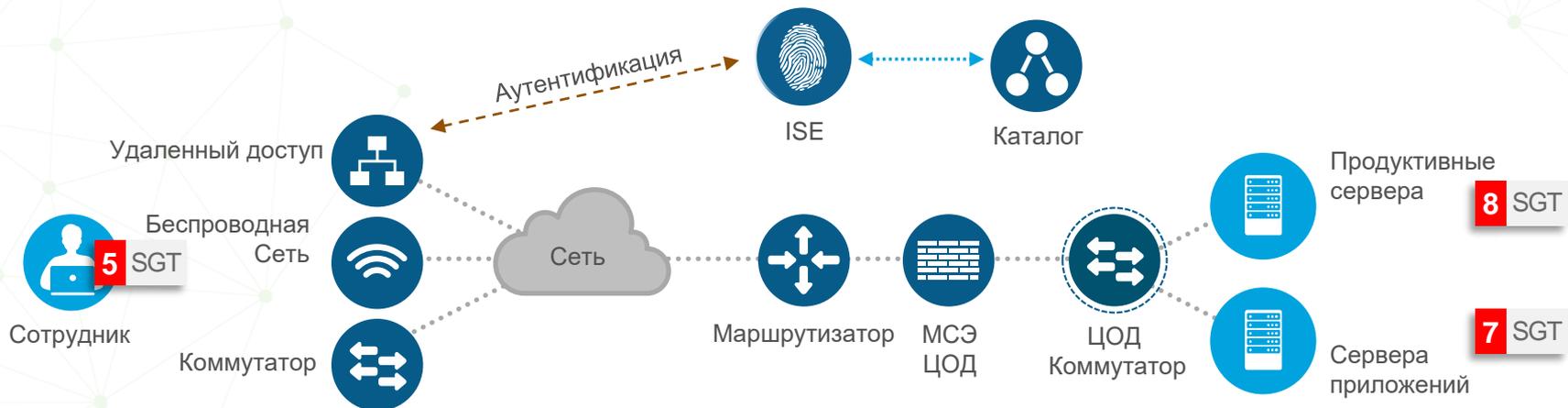
TrustSec упрощает управление ACL для трафика внутри/вне VLAN



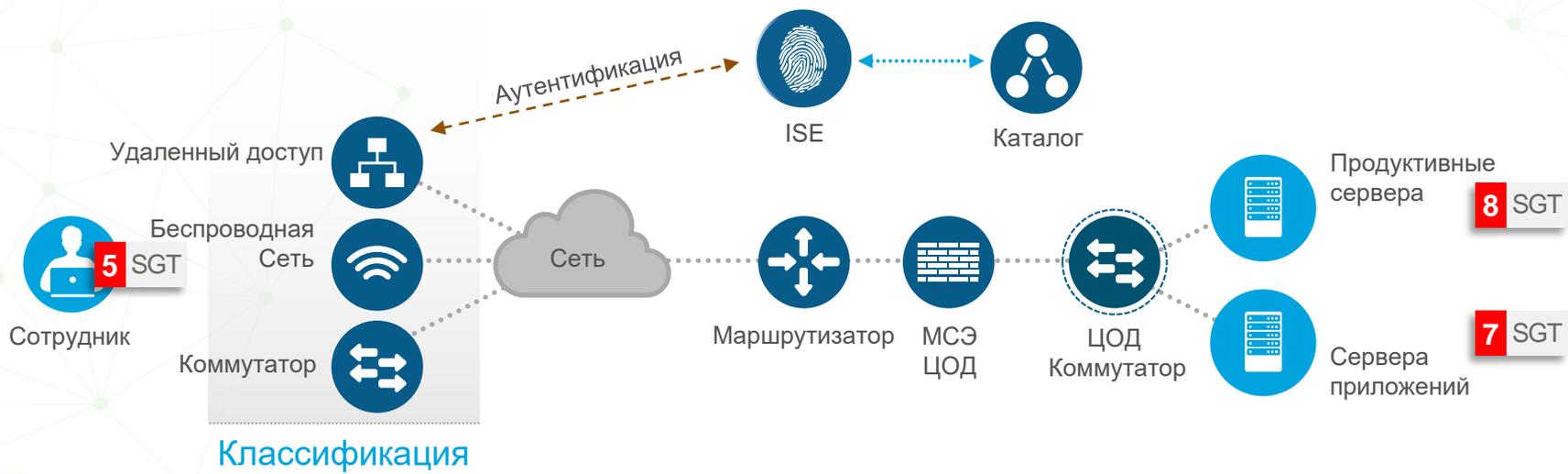
Представляем Cisco TrustSec



Представляем Cisco TrustSec



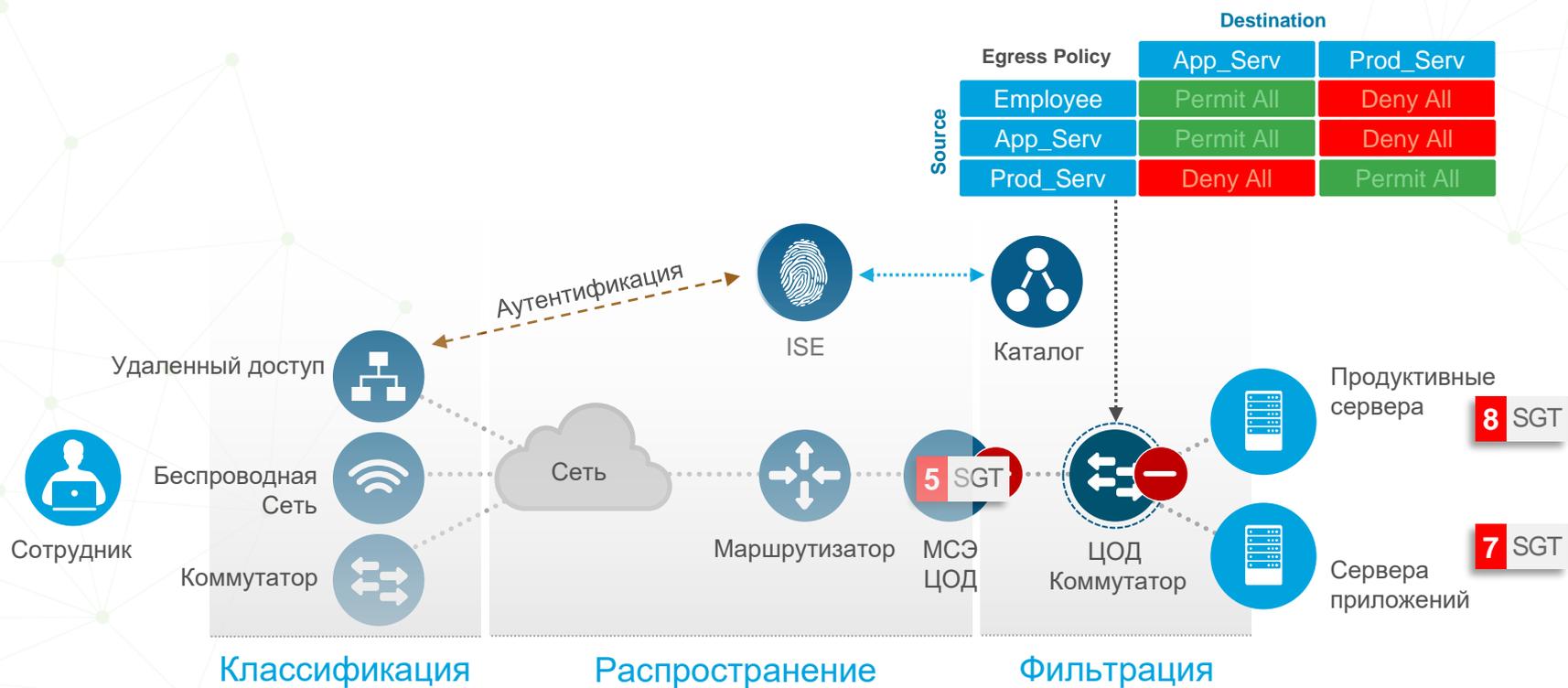
Представляем Cisco TrustSec



Представляем Cisco TrustSec



Представляем Cisco TrustSec



Классификация

Динамическая

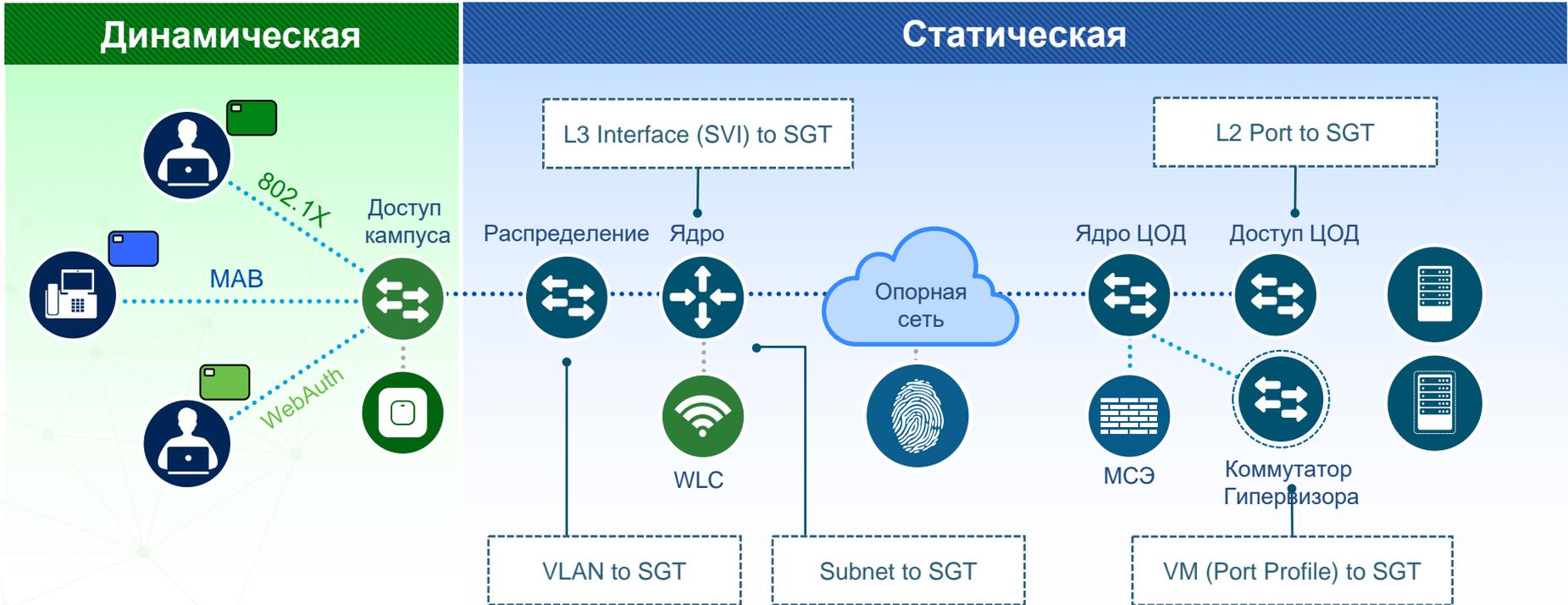
Статическая



Классификация



Классификация

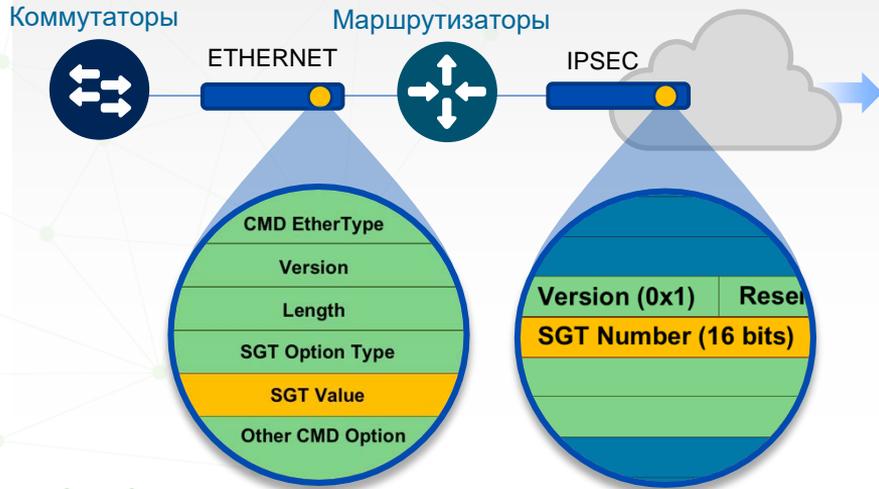




Распространение

Тегирование фрейма

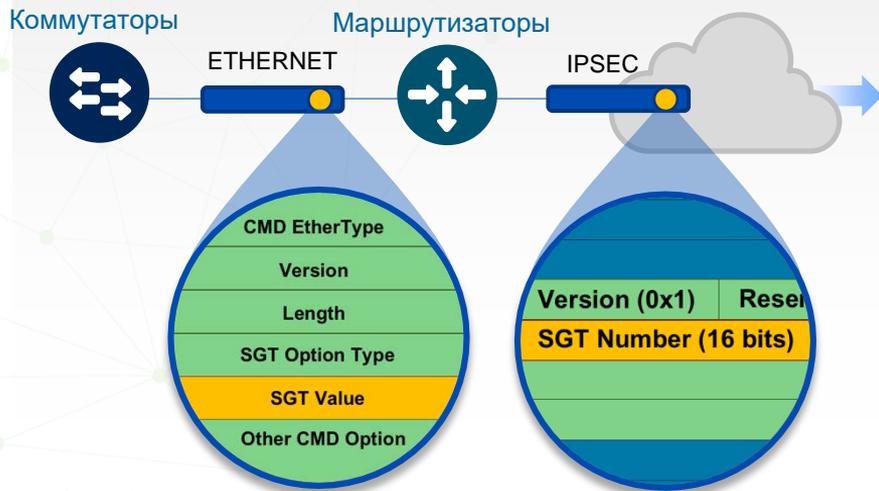
- **Ethernet Inline Tagging:** (EtherType:0x8909) 16-Bit SGT инкапсуляция в Cisco Meta Data (CMD) payload.
- **IPSec / L3 Crypto:** Cisco Meta Data (CMD) использует протокол 99, и включается в начало ESP/AH payload.



Распространение

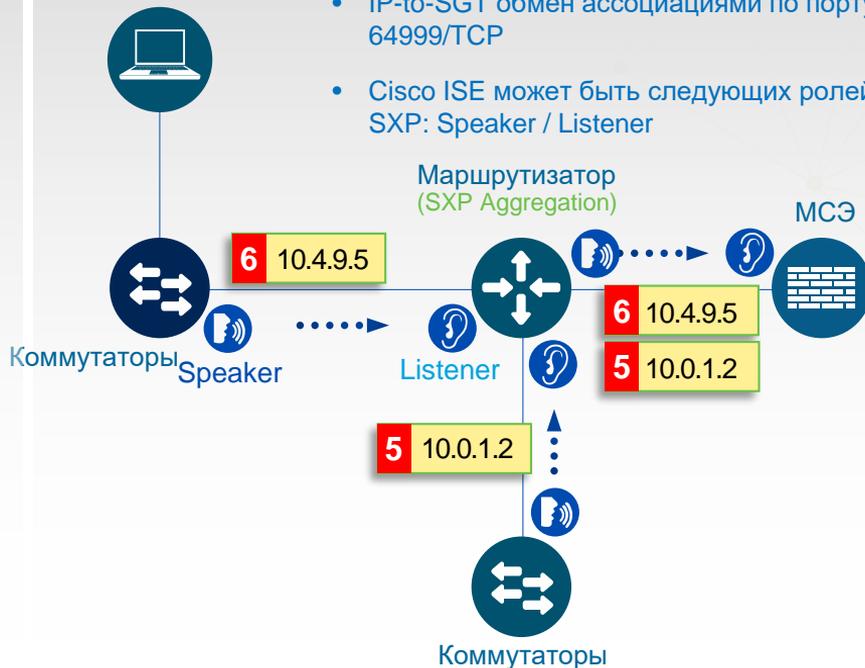
Тегирование фрейма

- **Ethernet Inline Tagging:** (EtherType:0x8909) 16-Bit SGT инкапсуляция в Cisco Meta Data (CMD) payload.
- **IPSec / L3 Crypto:** Cisco Meta Data (CMD) использует протокол 99, и включается в начало ESP/AH payload.



SGT Exchange Protocol (SXP)

- IP-to-SGT обмен ассоциациями по порту 64999/TCP
- Cisco ISE может быть следующих ролей SXP: Speaker / Listener



TrustSec политика фильтрации

TrustSec

Overview Authentication Policy Authorization Policy Components Policy SXP Reports Settings

Egress Policy

Matrix

Source Tree

Destination Tree

Network Device Authorization

Egress Policy (Matrix View)

Edit Add Clear Mapping Push Monitor All - Off Import Export View Show CustomView-1

Source	Mail_Servers 120/0078	PCI_Devices 100/0064	Web_Servers 110/000E	Employee_FullAc... 10/000A	Contractors 30/001E
Mail_Servers 120/0078	Permit_Email_Traffic	Deny IP		Cisco_Jabber_Access	
Contractors 30/001E	Permit_Email_Traffic	Deny IP		Malware_Control_ACL	
Employee_BYOD 20/0014		Deny IP		Malware_Control_ACL	Cisco_Jabber_Access
Employee_FullAc... 10/000A					
PCI_Devices 100/0064	Deny IP		Deny IP	Deny IP	Deny IP

Default Enabled SGACLs : Permit IP Description : Default egress rule

Permit_Email_Traffic

Access control policy to permit Email service

IPv4 IPv6 Agnostic

```

permit tcp dst eq 110
permit tcp dst eq 143
permit tcp dst eq 25
permit tcp dst eq 465
permit tcp dst eq 585
permit tcp dst eq 993
permit tcp dst eq 995
deny all log
    
```

Целостное применение политики

TRUSTSEC МАТРИЦА ПОЛИТИК

	✓	—	—	—
	✓	✓	✓	✓

Отправляйте и разворачивайте TrustSec политики целостно в коммутируемой, беспроводной и маршрутизируемой инфраструктуре

Deploy



CATALYST SWITCHES



NEXUS SWITCHES



VIRTUAL SWITCHES



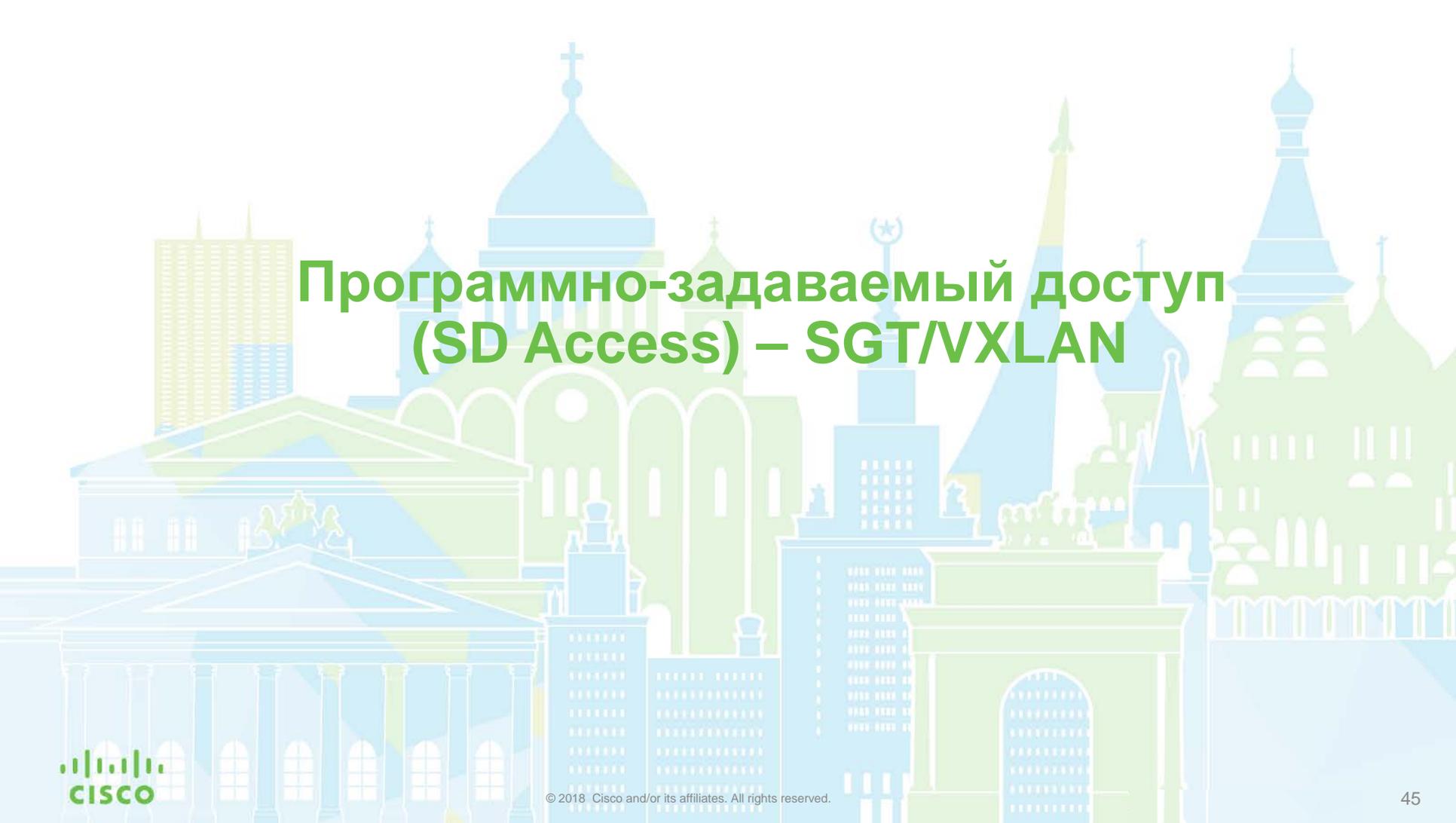
INDUSTRIAL SWITCHES



WIRELESS ACCESS POINTS



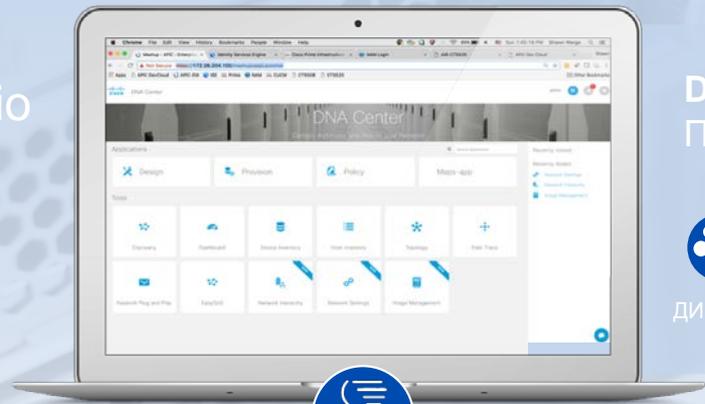
ROUTING PLATFORMS



Программно-задаваемый доступ (SD Access) – SGT/VXLAN

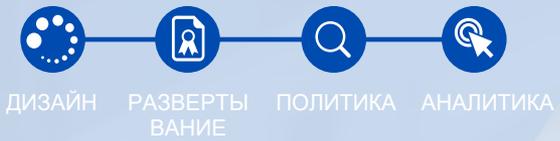
DNA Solution

Cisco Enterprise Portfolio



DNA Center

Простота имплементации



DNA Center



Identity Services Engine



Network Data Platform

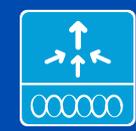
Network Controller Platform



МАРШРУТИЗАТОРЫ



КОММУТАТОРЫ



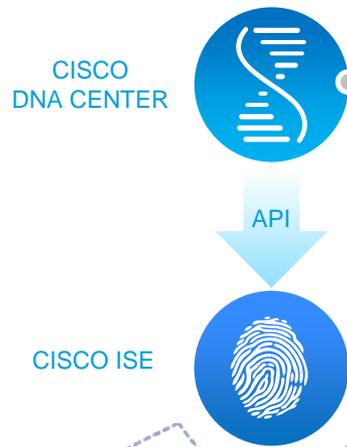
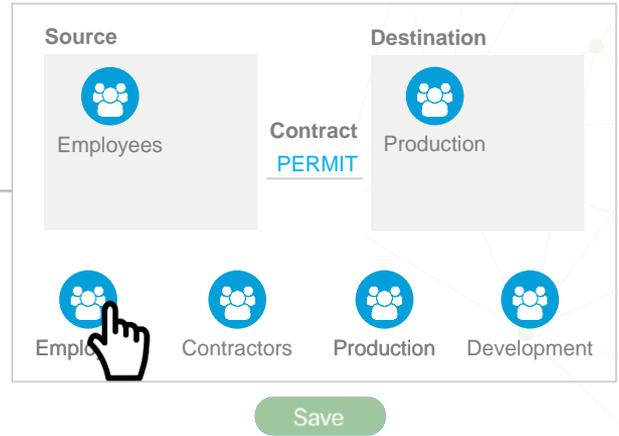
БЛВС КОНТРОЛЛЕРЫ



ТОЧКИ ДОСТУПА

SD Access – ISE/DNAC применение политики

ПОЛИТИКИ ФАБРИКИ



ЗАГРУЗКА ПОЛИТИК

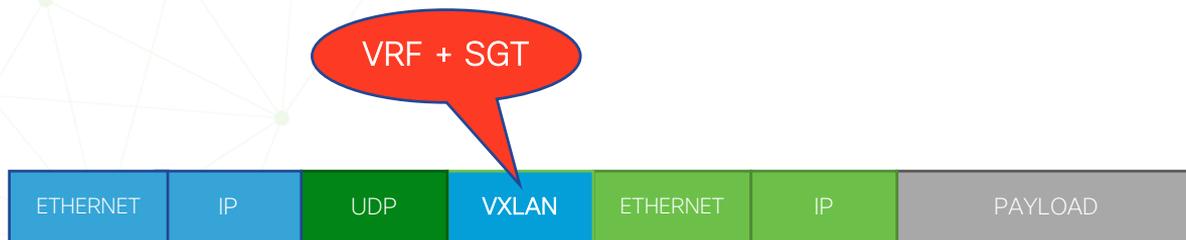


УЗЛЫ ФАБРИКИ



Что уникального в SD Access (Кампусной фабрике)?

1. Основанный на LISP Control-Plane
2. Основанный на VXLAN Data-Plane
3. Интегрированный SGT/SGACL



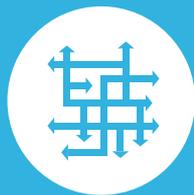
Virtual Routing & Forwarding
Scalable Group Tagging



Поведенческий анализ



Аналитика, которую предоставляет StealthWatch



Обнаружение

Идентификация бизнес-критичных приложений и сервисов в сети



Идентификация дополнительных IOС

Политика и Сегментация
Аномалии сетевого поведения (NBAD)

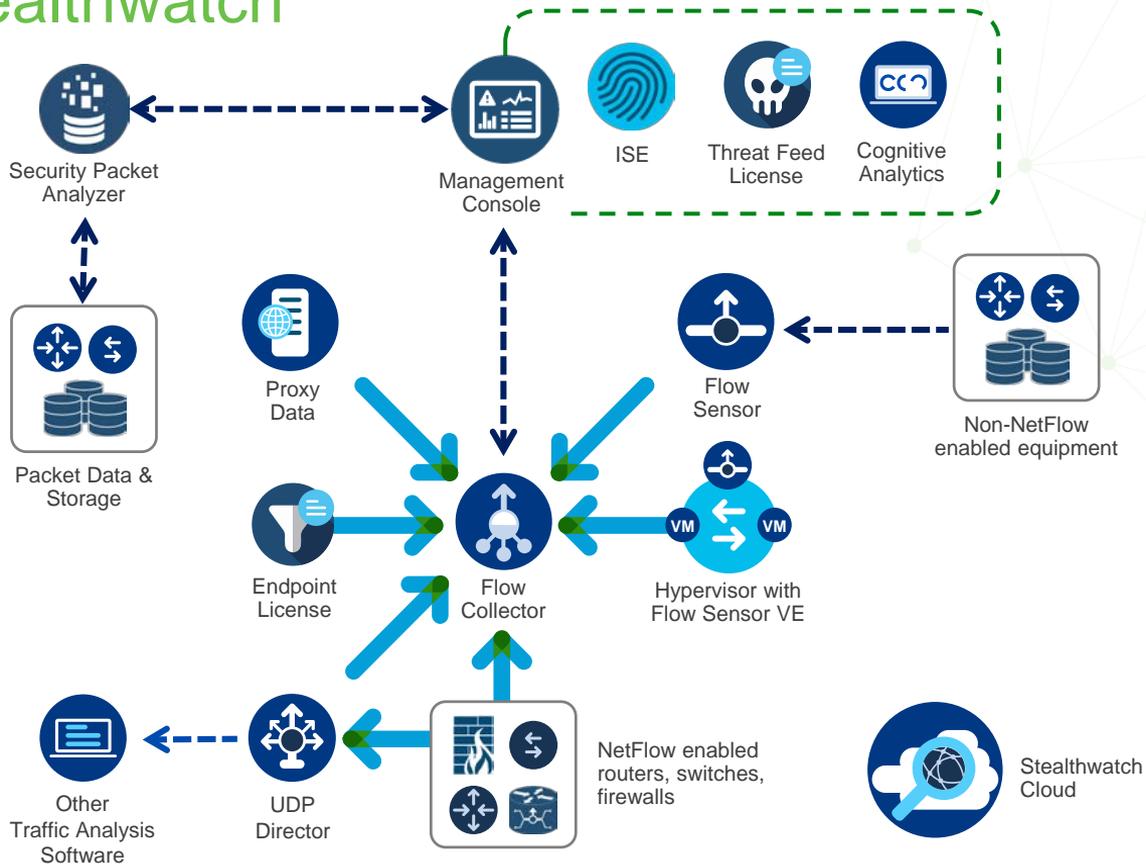


Лучше понимание возможности реагирования на IOС

Записи всех коммуникаций хост-хост

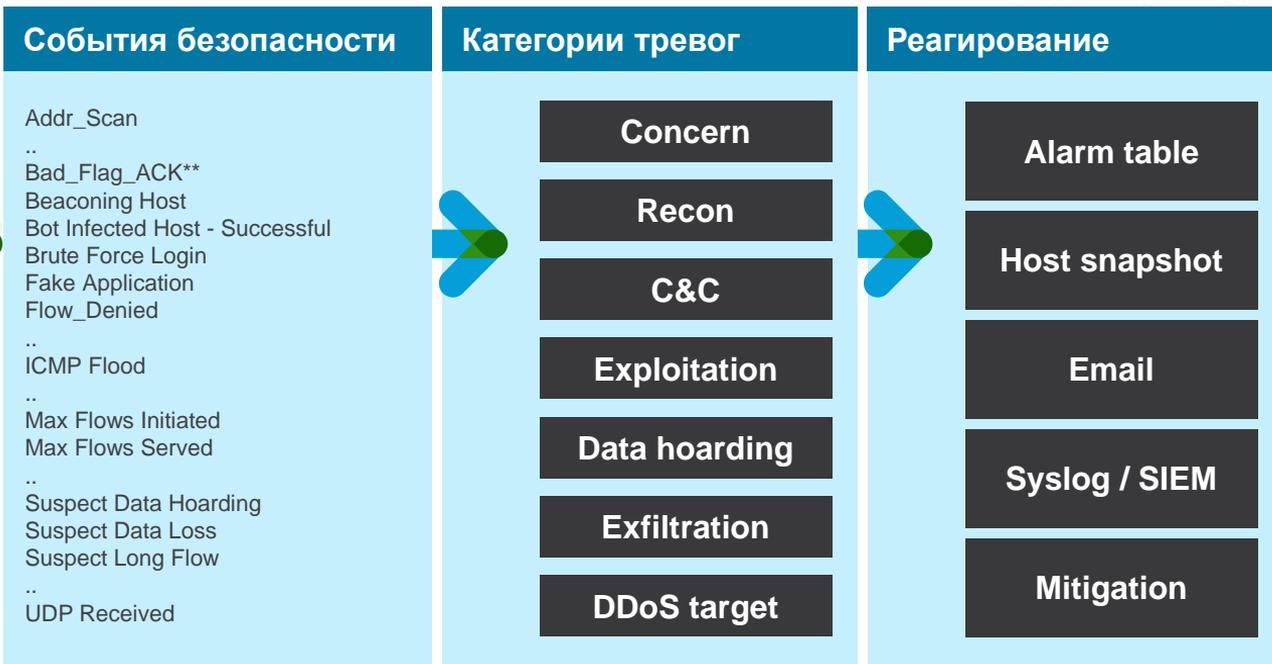
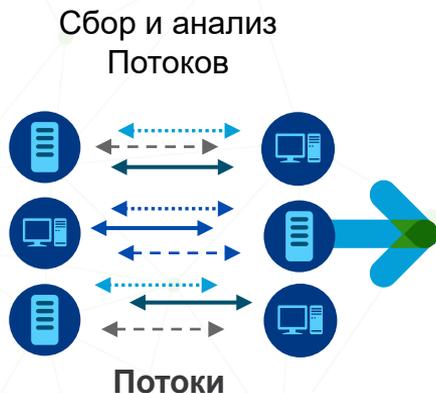
Система Cisco Stealthwatch

Комплексная
безопасность и
сетевой мониторинг



Модель поведенческого анализа и обнаружения аномалий

Поведенческие алгоритмы применяются для генерации “Событий безопасности”



Мощь многоуровневого машинного обучения



Расширенная видимость и поведенческий анализ

- Получение дополнительной видимости и контекста из глобального и локального трафика от TALOS
- Использовать машинное обучение и статистическое моделирование для продолжительной идентификации угроз



Продвинутое обнаружение угроз

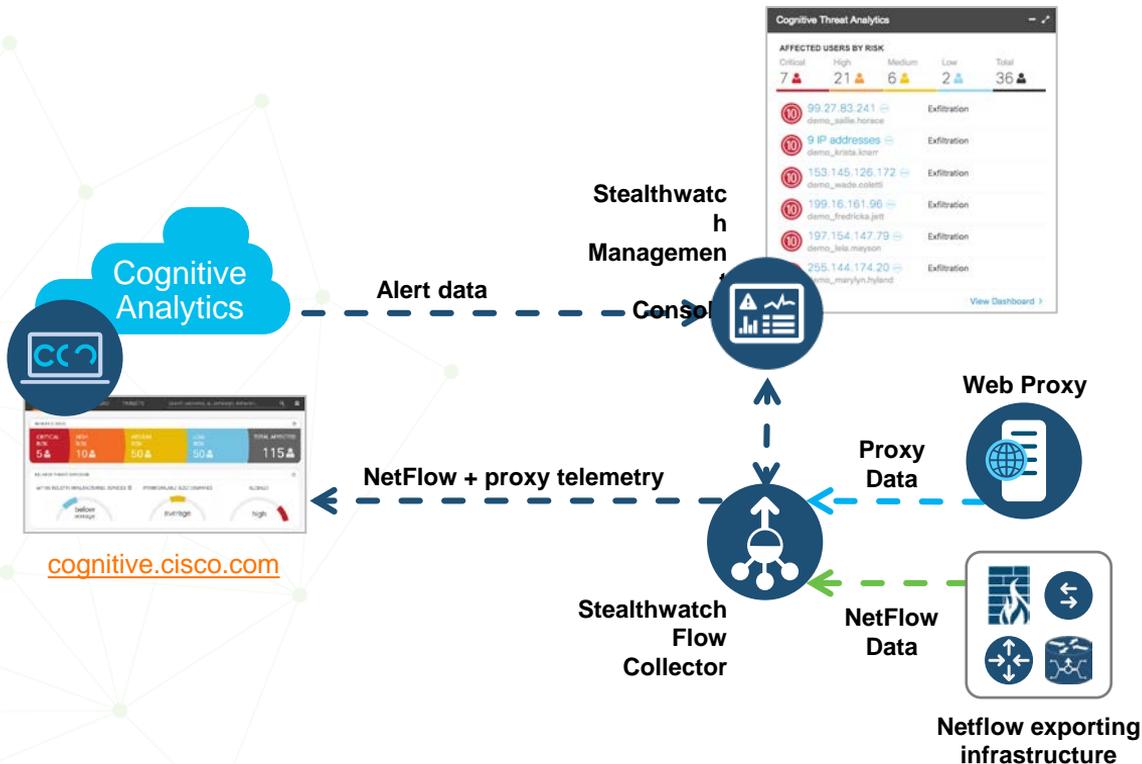
- Обнаружить угрозы, которые обошли текущие механизмы контроля
- Идентификация вывода данных, обнаружение command and control (C2) коммуникаций



Аналитика зашифрованного трафика

- Обнаружить вредоносные шаблоны в зашифрованном трафике
- Понять характеристики шифрования и убедиться в соответствии требованиям

Stealthwatch и Cognitive Analytics



Расширенная видимость и поведенческий анализ



Продвинутое обнаружение угроз



Аналитика зашифрованного трафика

Мощь многоуровневого машинного обучения

Повысить точность определения используя лучшую в классе аналитику безопасности

10,000,000,000
запросов в день



Global Risk Map
Threat Grid, TALOS



Обнаружение аномалий



Моделирование доверия



Классификация событий



Модели объектов



Моделирование взаимосвязей

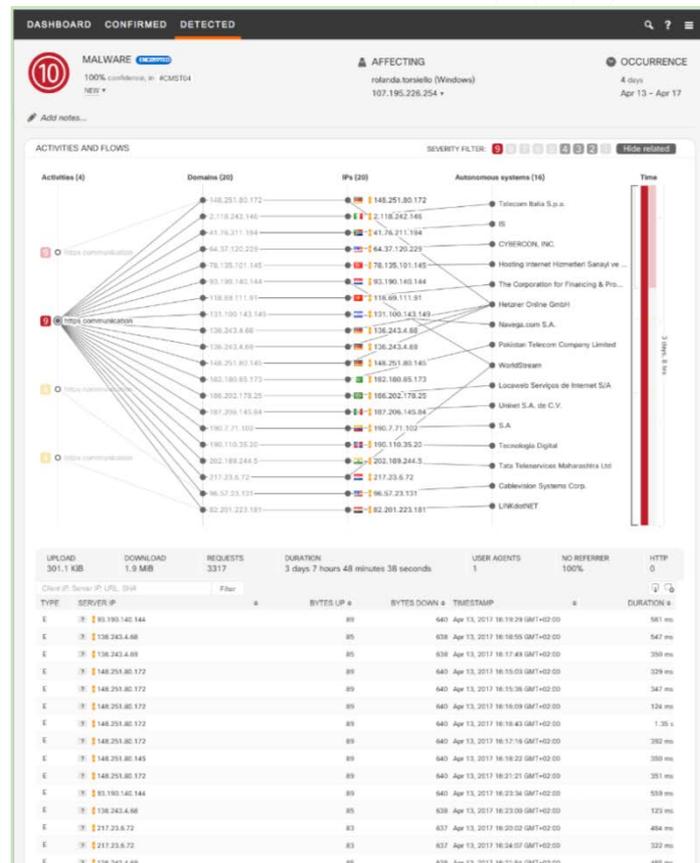
50,000
Инцидентов в день

Аномальный
Трафик

Вредоносные
события

Инциденты
угроз

Дополнительный уровень аналитики в наблюдаемом трафике



Обнаруженные инциденты с обогащенной атрибуцией

DASHBOARD CONFIRMED DETECTED

10 #CMST04 100% confidence 7

AFFECTING
7 users , Windows
20+ users in < 5 companies 

OCCURRENCE
35 days
Jul 6 - Aug 9

TRIASG INVESTIGATING REMEDIATING RESOLVED

10 risk #CMST04 last seen Aug 9, 2016 for 35 days

9 risk #CRMN01 last seen Aug 18, 2016 for 85 days

8 risk #CDCH01 last seen Aug 16, 2016 for 25 days

8 risk #CSAL01 last seen Jul 18, 2016 for 2 days

7 risk

AFFECTED USERS
7 users affected by this threat during the last 45 days with unresolved incidents.

adena.batie aleen.eisenbarth cindie.janas
haywood.nagel tiffany.brent victor.castiglione

GLOBAL INTELLIGENCE: AMP THREAT GRID

The following statistics are based on **85** samples of threat artifacts from AMP Threat Grid that show network behaviors related to this CONFIRMED CTA threat category.

Common signatures

Endpoint content security signatures associated with similar threats seen in AMP Threat Grid.

W32S.Adware.RelevantKnowledge-6

Win.Adware.Agent-1343801

Win.Adware.Agent-60025

Common files EXPAND ALL

Files appearing in threat samples that may be present at the endpoint.

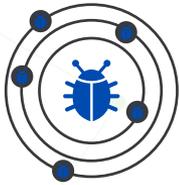
24% chance that malware created or modified files with the following pattern:

severity **100** N/A 

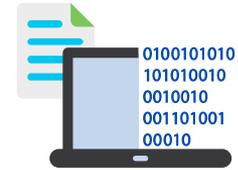
- /Users/Administrator/AppData/Local/Temp/KK0THS510X.exe
 - /Users/Administrator/AppData/Local/Temp/a20Pm4SnPg/FnBxKdI0/Setup.exe
 - /Users/Administrator/AppData/Local/Temp/QT4731FXGB.exe
- + 606 more paths

Encrypted Traffic Analytics

Единственное решение, которое предоставляет видимость и обнаружение вредоносной активности трафика без его расшифровки



Вредоносы в зашифрованном трафике

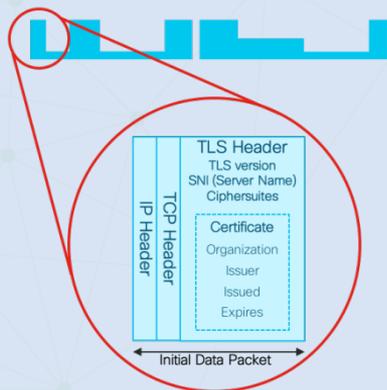


Криптографическое соответствие

Как мы можем инспектировать зашифрованные данные?

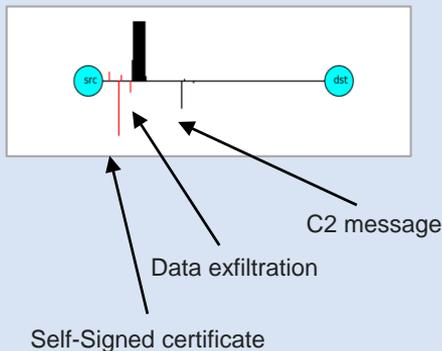
Первый пакет данных

Получите максимум от нешифрованных полей



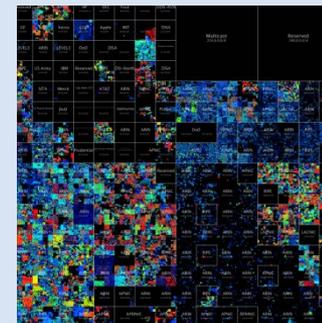
Последовательность длин пакетов и времен

Идентификация типа контента через размер и тайминг пакетов



Карта угроз

Кто есть кто на черной стороне Интернета



Широкая поведенческая база о серверах в Интернет



Encrypted Traffic Analytics



Корреляция знаний Глобальных-Локальных результатов с высокой точностью нахождения угроз



Stealthwatch улучшенная аналитика и машинное обучение уменьшает время расследования инцидентов



Улучшенный NetFlow с аналитикой шифрованного трафика от новейших коммутаторов и маршрутизаторов Cisco



cognitive.cisco.com



Alert data

NetFlow + proxy telemetry

NetFlow

Enhanced NetFlow
Crypto Audit Telemetry



Stealthwatch Management Console предоставляет агрегированные данные аналитики Cognitive по обнаружению Malware

Flow Collector(s)

Криптографическое соответствие требованиям

The screenshot displays the Cisco Stealthwatch interface. At the top, the Cisco logo and 'Stealthwatch' name are visible. Below the navigation menu, the 'Flow Search Results (90)' section is active. Search filters include 'Last Hour (Time Range)' with '2,000 (Max Records)', 'Subject: 10.201.3.51', and 'Connection: 443/Tcp (Port / Protocol)'. A table of search results is shown below, with a red box highlighting the encryption-related columns. The table has columns for START, DURATION, SUBJECT POR..., SUBJECT BYTES, APPLICATION, TOTAL BYTES, ENCRYPTION T..., ENCRYPTION K..., ENCRYPTION A..., ENCRYPTION A..., ENCRYPTION ..., PEER PORT/PR..., PEER BYTES, and ACTIONS. The highlighted columns contain encryption details such as TLS 1.2, ECDHE, RSA, ECDSA, AES_128_GCM/128, and SHA256.

START	DURATION	SUBJECT POR...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	ENCRYPTION T...	ENCRYPTION K...	ENCRYPTION A...	ENCRYPTION A...	ENCRYPTION ...	PEER PORT/PR...	PEER BYTES	ACTIONS
Nov 9, 2017 10:52... (46min 19s ago)	54s	49286/TCP	125.07 K	HTTPS (unclassified)	14.21 M	TLS 1.2	ECDHE	RSA	AES_128_GCM/128	SHA256	443/TCP	14.09 M	
Nov 9, 2017 11:33:3... (5min 17s ago)	1min 40s	49233/TCP	225.66 K	HTTPS (unclassified)	7.34 M	TLS 1.2	ECDHE	ECDSA	AES_128_GCM/128	SHA256	443/TCP	7.12 M	
Nov 9, 2017 10:52... (45min 52s ago)	27s	49315/TCP	130.65 K	HTTPS (unclassified)	1.47 M	TLS 1.2	ECDHE	RSA	AES_128_GCM/128	SHA256	443/TCP	1.36 M	
Nov 9, 2017 10:52... (46min 5s ago)	17s	49298/TCP	37.88 K	HTTPS (unclassified)	1.25 M	TLS 1.2	ECDHE	RSA	AES_128_GCM/128	SHA256	443/TCP	1.21 M	
Nov 9, 2017 10:52... (46min 14s ago)	7s	49291/TCP	16.88 K	HTTPS (unclassified)	264.89 K	TLS 1.2	ECDHE	RSA	AES_128_GCM/128	SHA256	443/TCP	248.02 K	
Nov 9, 2017 11:33:3... (5min 9s ago)	1min 21s	49241/TCP	29.90 K	HTTPS (unclassified)	119.34 K	TLS 1.2	ECDHE	ECDSA	AES_128_GCM/128	SHA256	443/TCP	69.38 K	
Nov 9, 2017 11:33:5... (4min 57s ago)	1min 3s	49254/TCP	23.57 K	HTTPS (unclassified)	84.39 K	TLS 1.2	ECDHE	RSA	AES_128_GCM/128	SHA256	443/TCP	60.82 K	
Nov 9, 2017 11:33:5... (4min 55s ago)	1min 2s	49255/TCP	19.88 K	HTTPS (unclassified)	77.74 K	TLS 1.2	ECDHE	ECDSA	AES_128_GCM/128	SHA256	443/TCP	57.67 K	
Nov 9, 2017 11:33:5... (4min 51s ago)	57s	49265/TCP	23.85 K	HTTPS (unclassified)	68.19 K	TLS 1.2	ECDHE	RSA	AES_128_GCM/128	SHA256	443/TCP	44.34 K	
Nov 9, 2017 11:33:5... (4min 54s ago)	1min 2s	49259/TCP	19.63 K	HTTPS (unclassified)	58.91 K	TLS 1.2	ECDHE	RSA	AES_128_GCM/128	SHA256	443/TCP	30.28 K	

Rapid Threat Containment



Cisco®
Identity Services Engine



Stealthwatch
Management Console

Постановка и снятие с карантина
через pxGrid

Host Summary

 *Host IP*
10.201.3.149 ⋮

Status: Active

Hostname: workstation-149

Host Groups: [End User Devices, Desktops, Atlanta, Sales and Marketing](#)

Location: RFC 1918

Last Seen: 1/9/17 10:25 AM

Policies: [Host-specific Policy], Inside

MAC Address: --

Заключение



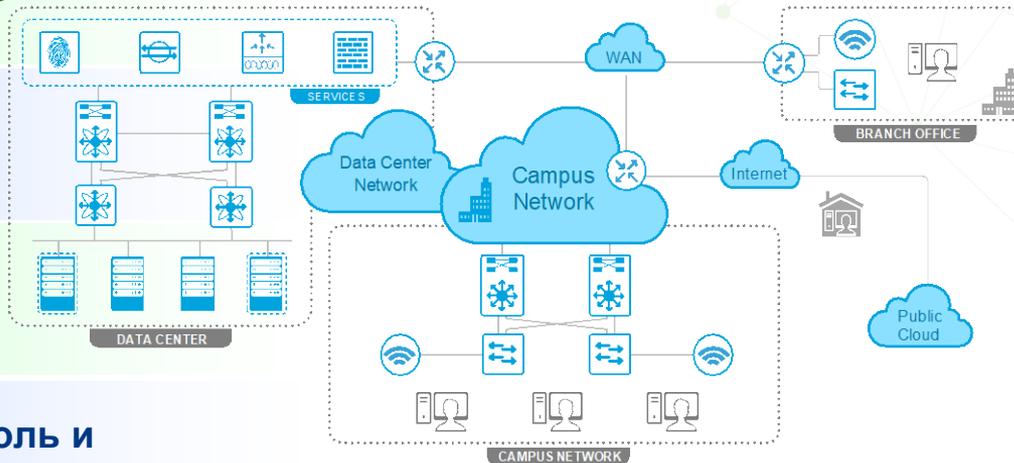
Digital Network Architecture для корпоративной безопасности

Видимость и контроль повсеместно

Интегрированная в сеть безопасность

Быстрая реакция на угрозы

Централизованная политика, контроль и отчетность



‘Инфраструктура’ для защиты ‘Информации’



Спасибо за
внимание!