



Комплексная безопасность в инфраструктуре DNA

Дмитрий Казаков

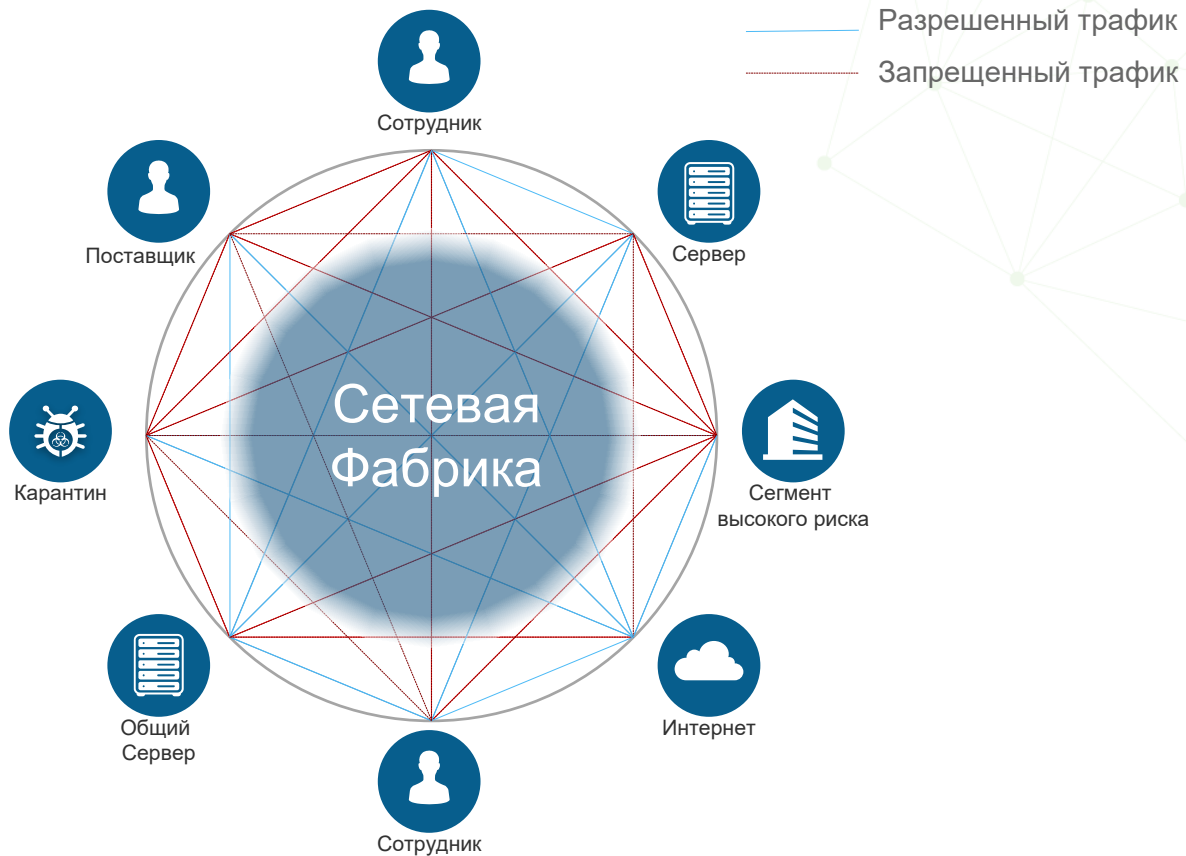
Системный инженер-консультант

CCIE Security, CISSP, СЕН

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

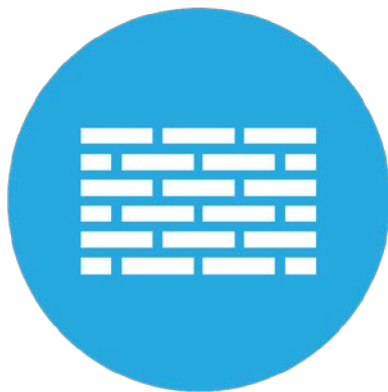


*Инспекция и анализ
действий после
разрешения
доступа*

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



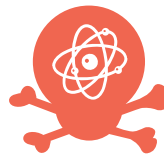
...И защититься от них.



Угрозы



Зомби



DDoS



Имперсонализация



Разрушение



Трояны



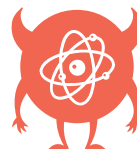
Черви



Шпионаж



Command
& Control



Zero
Days



Внедрение



Внедрение сервиса



Вывод данных



Шпионское ПО

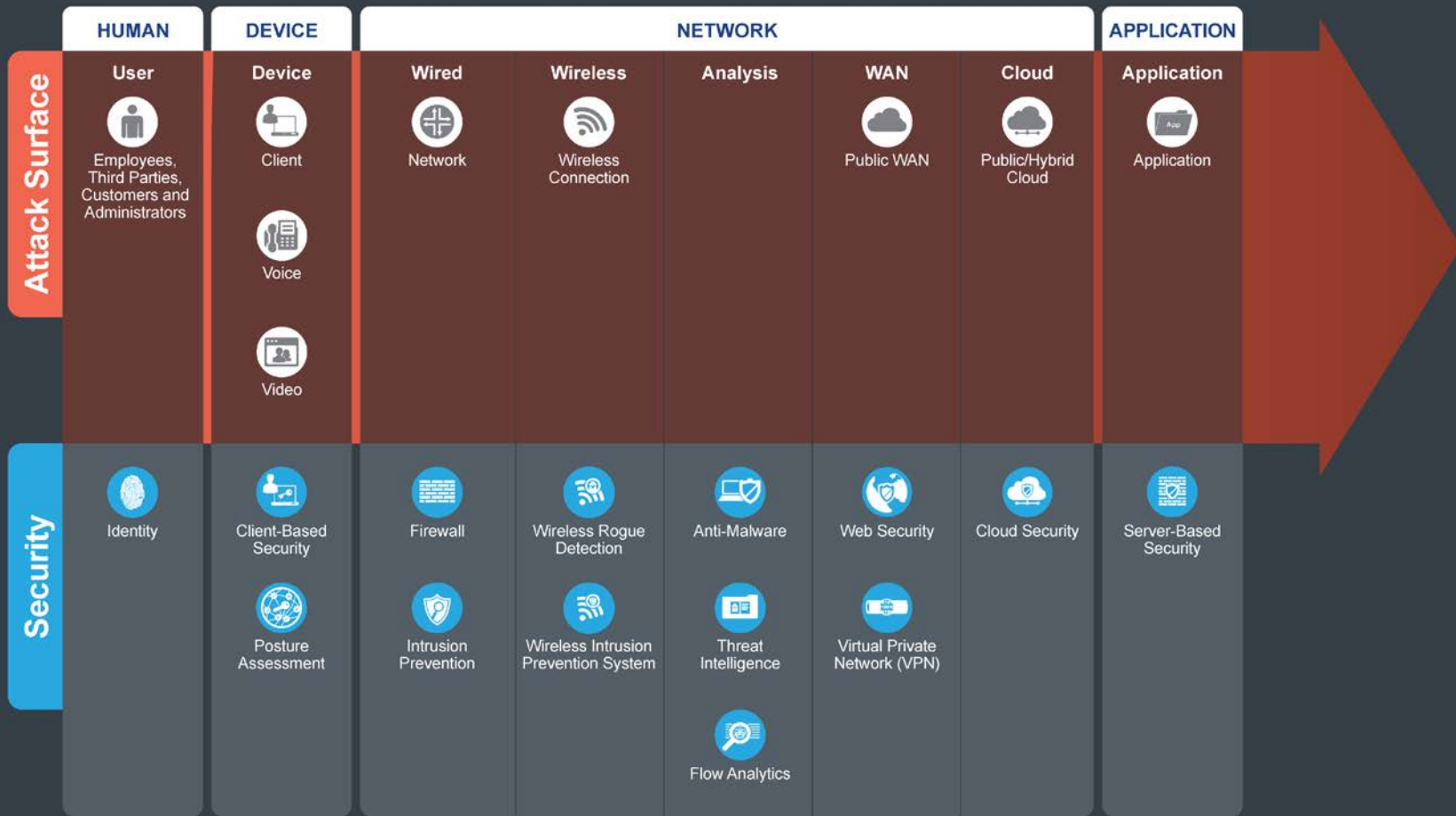


Вирусы



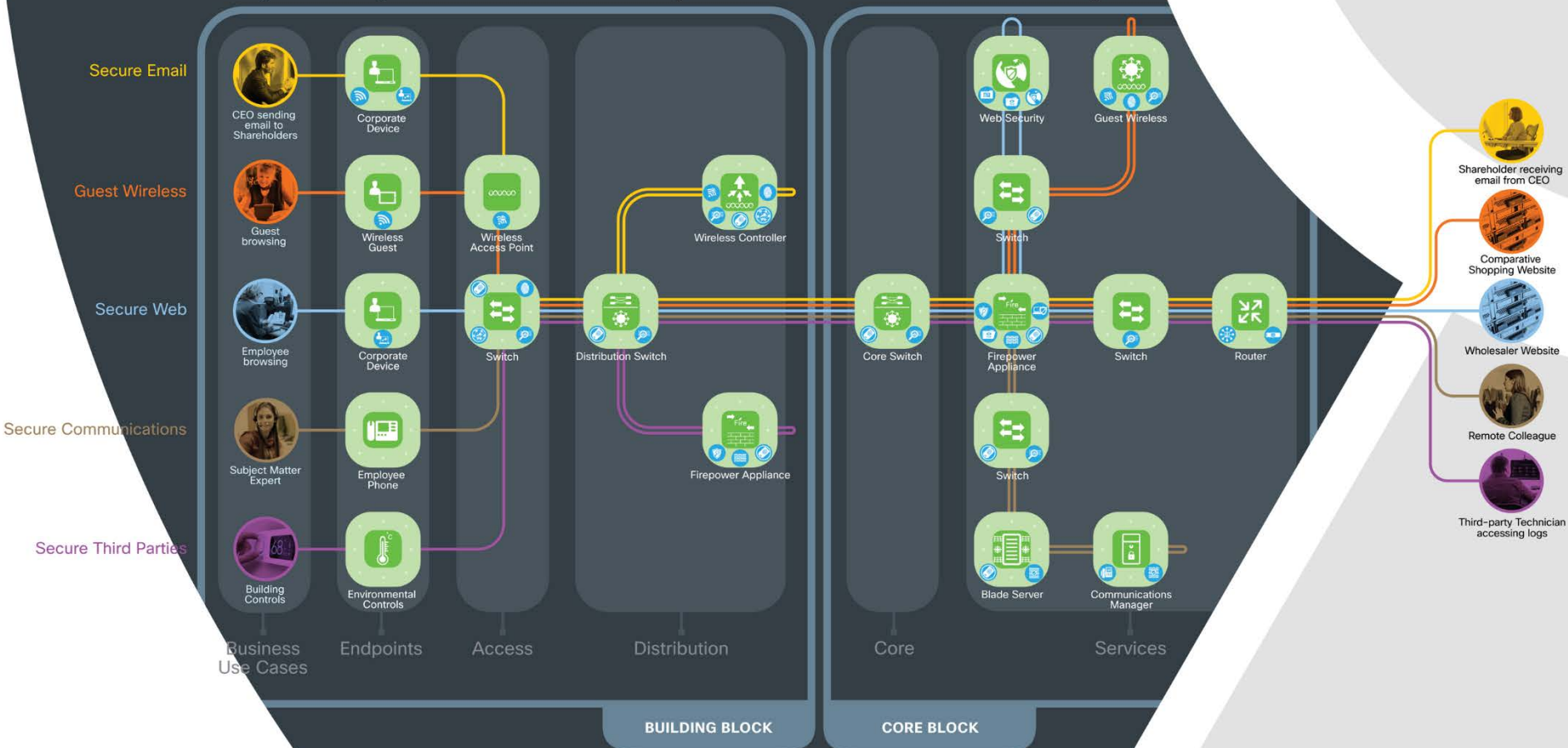
Сбор данных

Примеры

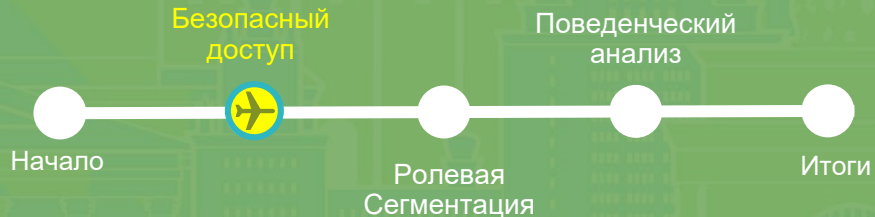


Campus Architecture

HUMAN DEVICES NETWORK APPLICATIONS



Безопасность доступа



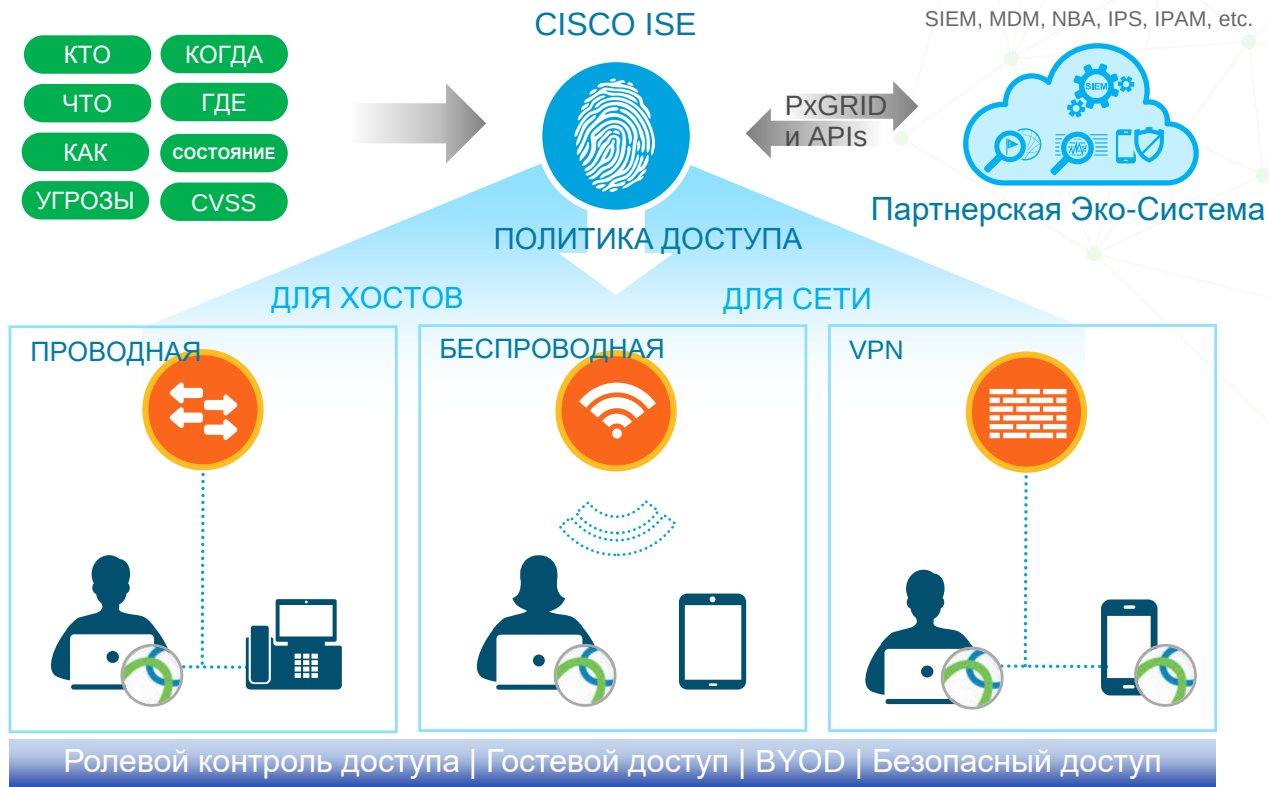
Cisco ISE и Anyconnect

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

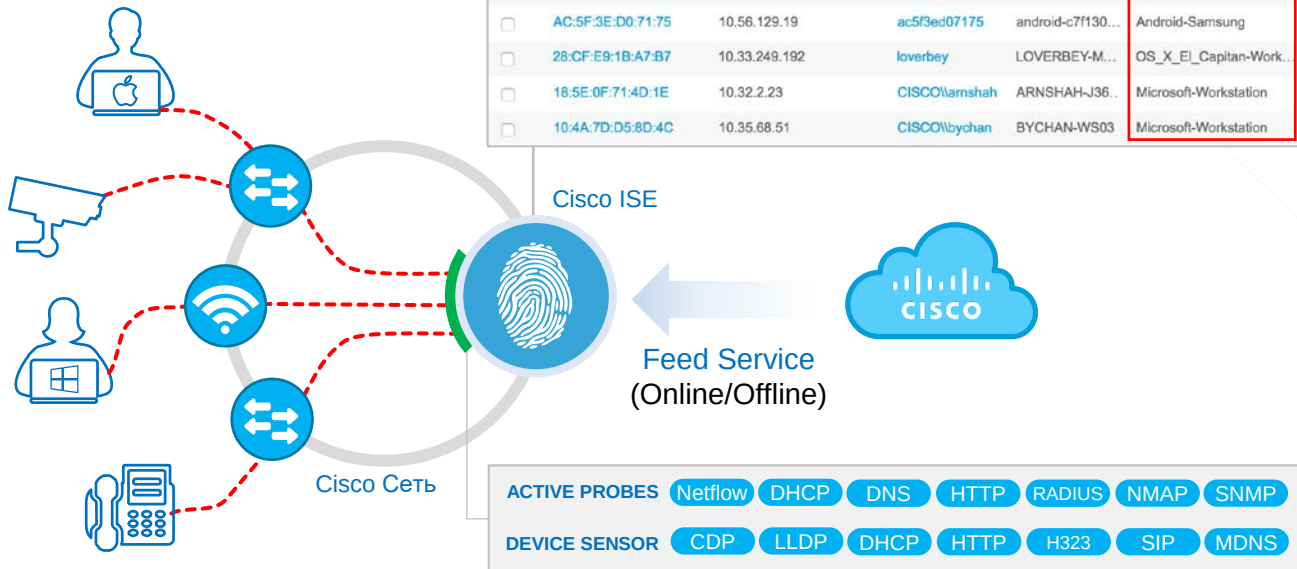
Устройств с '50' атрибутами
каждый можно хранить

550+

Высокоуровневые вложенные
профили.
+Периодические обновления

250+

Профили медицинских
устройств



Видимость групп и пользователей

Identity Services Engine

Home

Context Visibility

Operations

Policy

Administration

Work Centers

Endpoints

Users

Network Devices

Application

Employees

Guest

DEPARTMENT

LOCATION

locat...wired: [5.26%]

locat...ashes: [5.26%]

ENDPOINTS

Type

Profile

workstations: [32.96%]

misc: [55.31%]

Refresh

First Name

MAC Address

Anomalous Behavior

IPv4 Address

Username

00:50:56:A4:F8

192.168.99.22

azaluzhn

win-7-client

Ashes

Windows7-Workstation

VMware, Inc.

OS X

1

00:0C:29:72:66:87

192.168.99.14

azaluzhn

dkazakov-wm

Ashes

Windows7-Workstation

VMware, Inc.

Microsoft Windows Ser...

1

00:50:56:A4:D1:02

192.168.99.18

azaluzhn

lab-pc2

Ashes → Ashe...

Windows7-Workstation

VMware, Inc.

Windows 7 Ultimate 64-bit

1

00:0C:29:CC:77:CA

true

192.168.196.149

dkazakov

DESKTOP-H...

Ashes → Ashe...

Windows7-Workstation

VMware, Inc.

FreeBSD 6.2-RELEASE...

1

00:50:56:A4:80:D0

192.168.200.6

azaluzhn

wannacry-pc1

Ashes → Ashe...

Windows7-Workstation

VMware, Inc.

1

00:50:56:A4:F0:96

192.168.208.5

azaluzhn

DESKTOP-Vi...

Location → All...

Windows7-Workstation

VMware, Inc.

Windows 7

1

Identity Services Engine

Home

Context Visibility

Operations

Policy

Administration

Work Centers

Authentication

BYOD

Compliance

Compromised Endpoints

Endpoint Classification

Guest

Vulnerable Endpoints

Hardware

MANUFACTURERS

Both

Windows

Mac OSX

amer... inc.: [9.09%]

apple, inc.: [27.27%]

phon... a ltd: [63.64%]

ENDPOINT UTILIZATIONS

CPU

Memory

Disk

Devices with over % CPU usage

no of ants: [100%]

Refresh

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:08:43:0B: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

Hostname

Location

Endpoint Profile

Description

OUI

OS types

Status

win-7-client

Ashes

Windows7-Workstation

VMware, Inc.

OS X

1

dkazakov-wm

Ashes

Windows7-Workstation

VMware, Inc.

Microsoft Windows Ser...

1

lab-pc2

Ashes → Ashe...

Windows7-Workstation

VMware, Inc.

Windows 7 Ultimate 64-bit

1

DESKTOP-H...

Ashes → Ashe...

Windows7-Workstation

VMware, Inc.

FreeBSD 6.2-RELEASE...

1

wannacry-pc1

Ashes → Ashe...

Windows7-Workstation

VMware, Inc.

1

DESKTOP-Vi...

Location → All...

Windows7-Workstation

VMware, Inc.

Windows 7

1

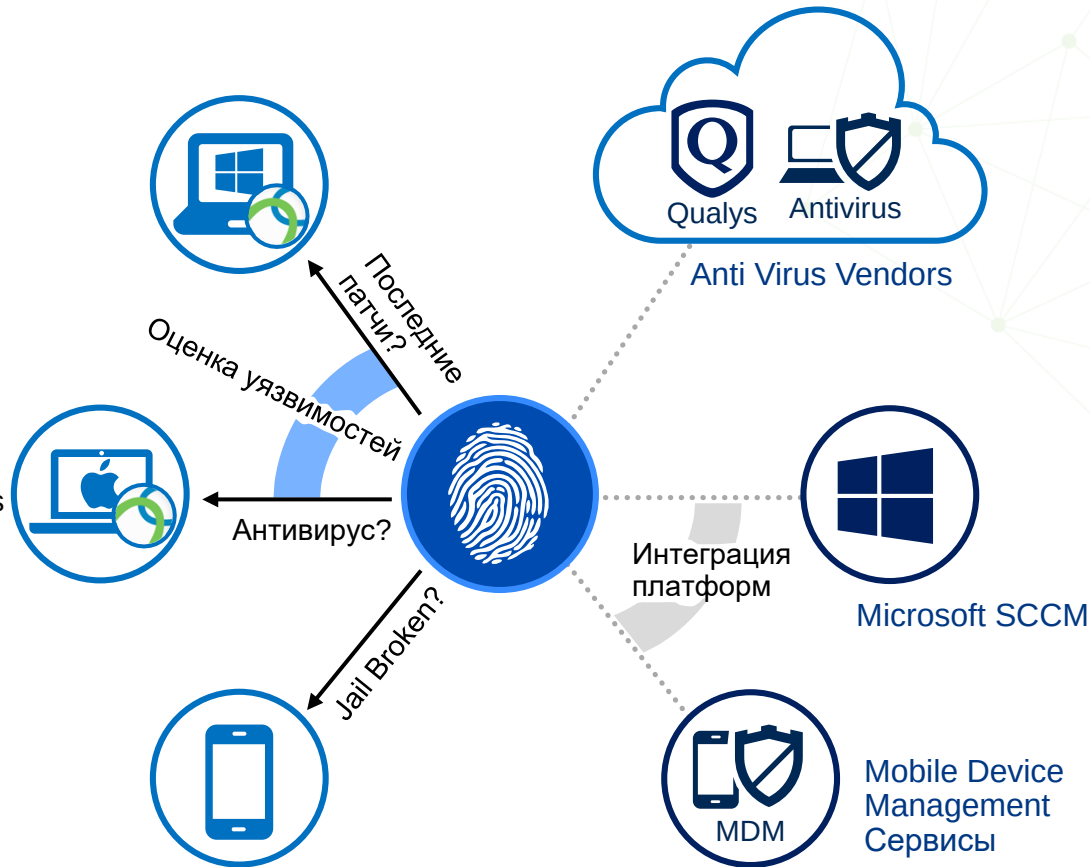
А что с оценкой состояния?

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

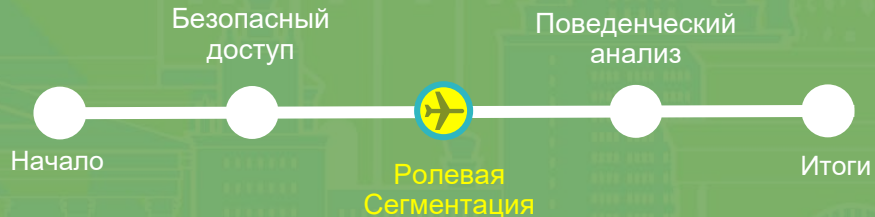


Экосистемные партнеры

Контекстные действия

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

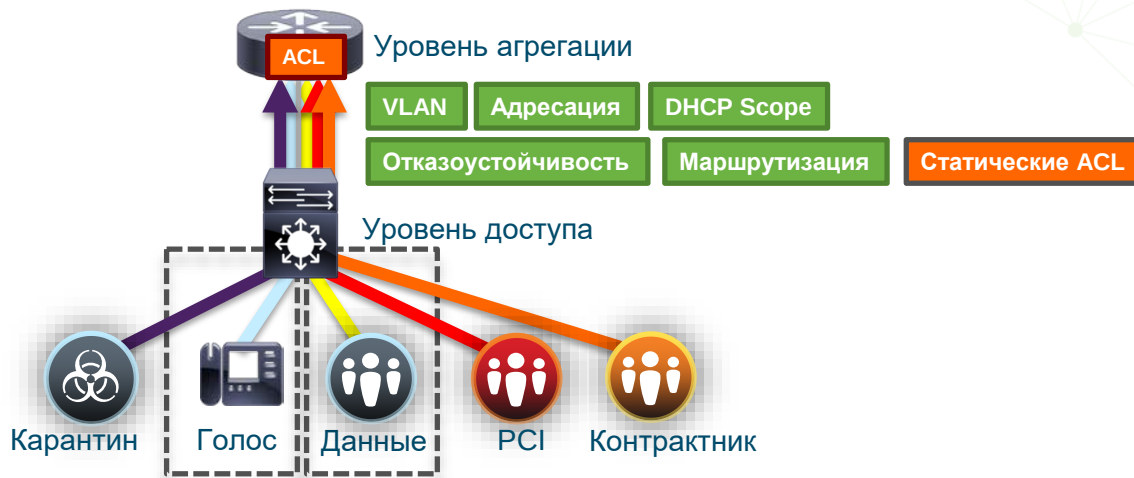
Ролевая сегментация



Традиционная сегментация



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

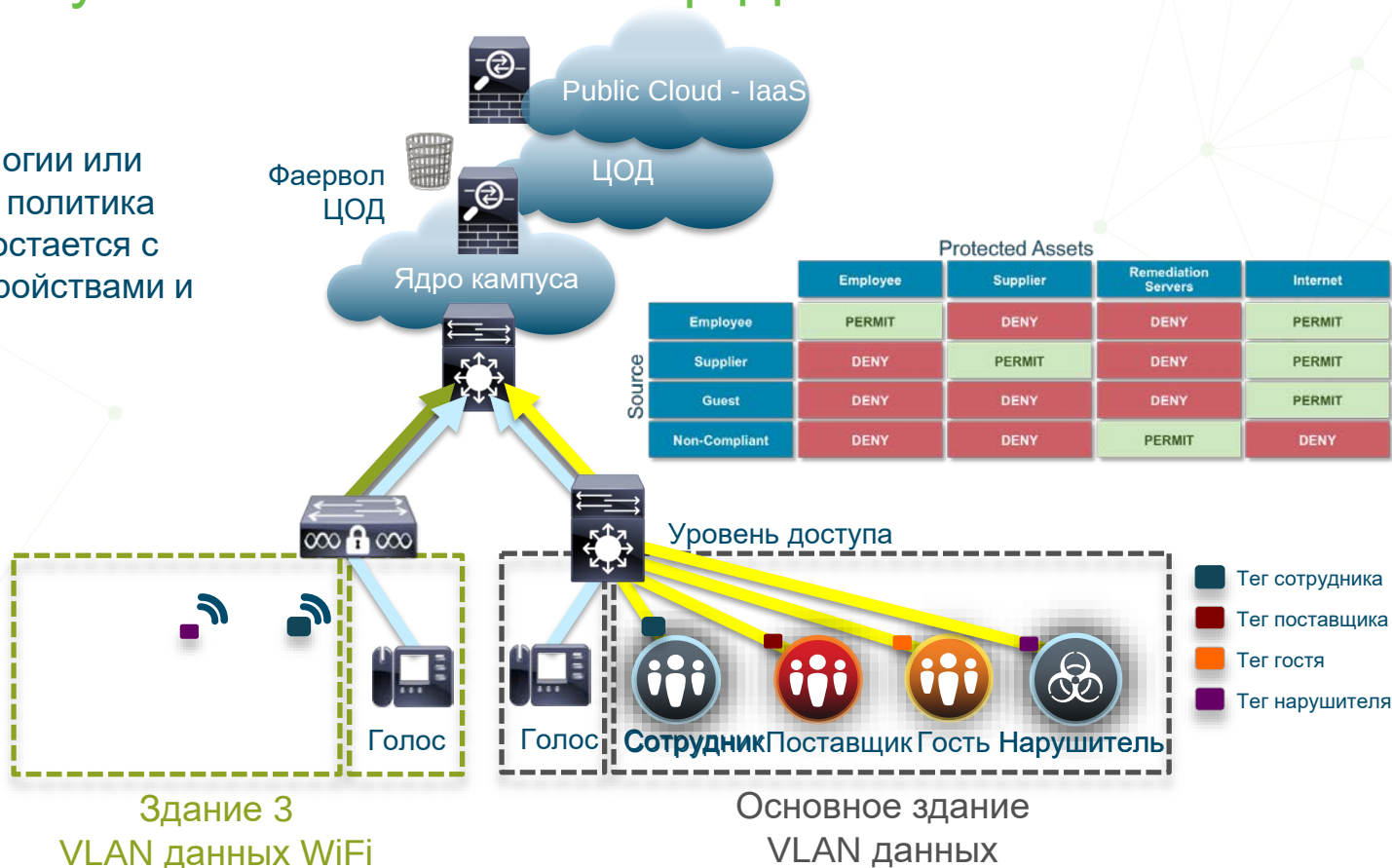


Большинство сегментов создается на уровне VLAN

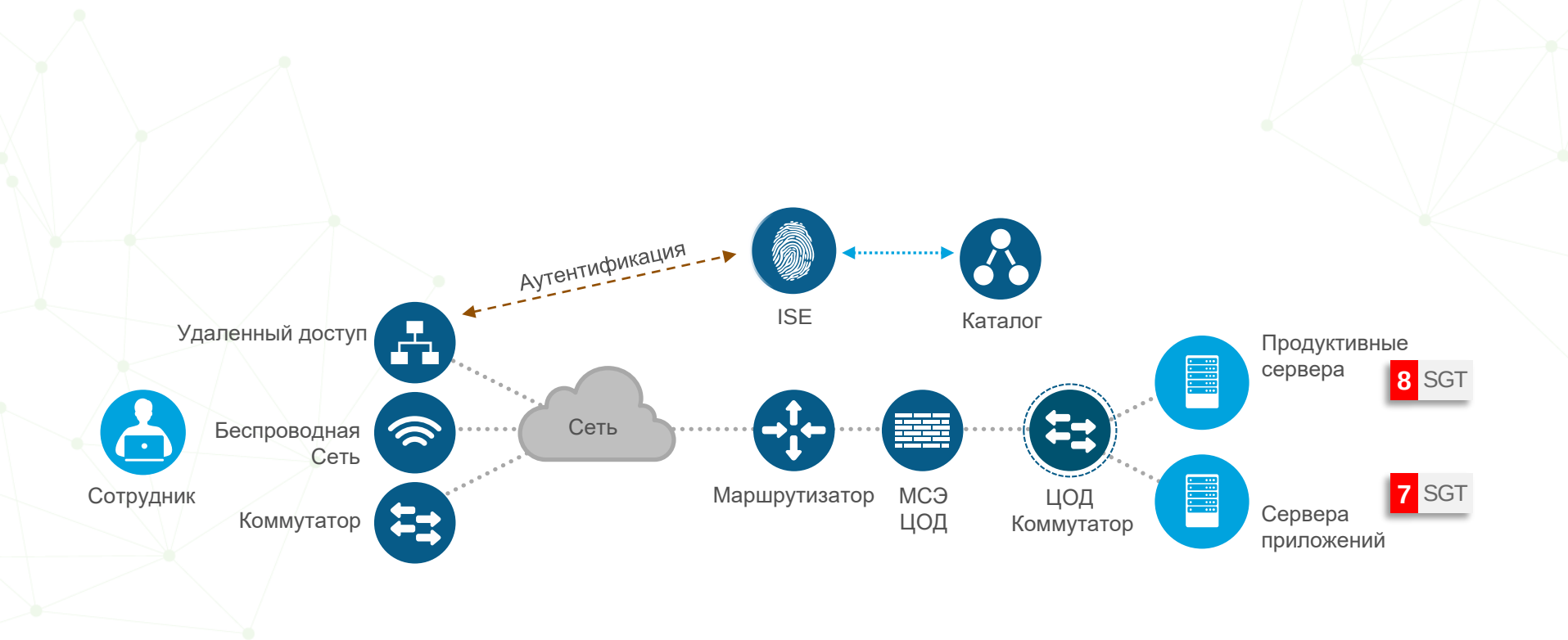
Контроль доступа пользователя в ЦОД с TrustSec

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

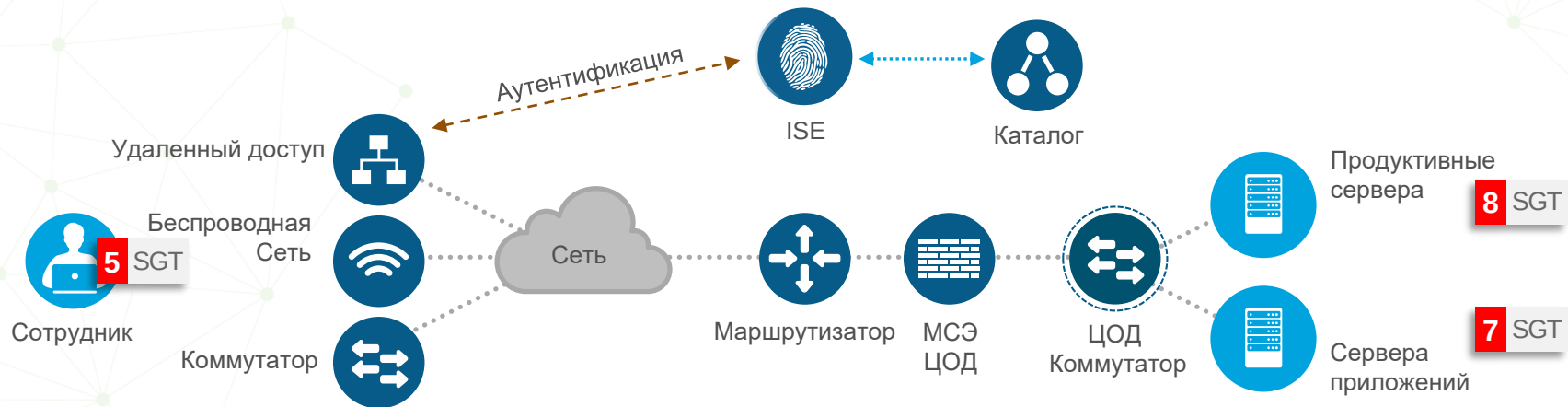
TrustSec упрощает управление ACL для трафика внутри/вне VLAN



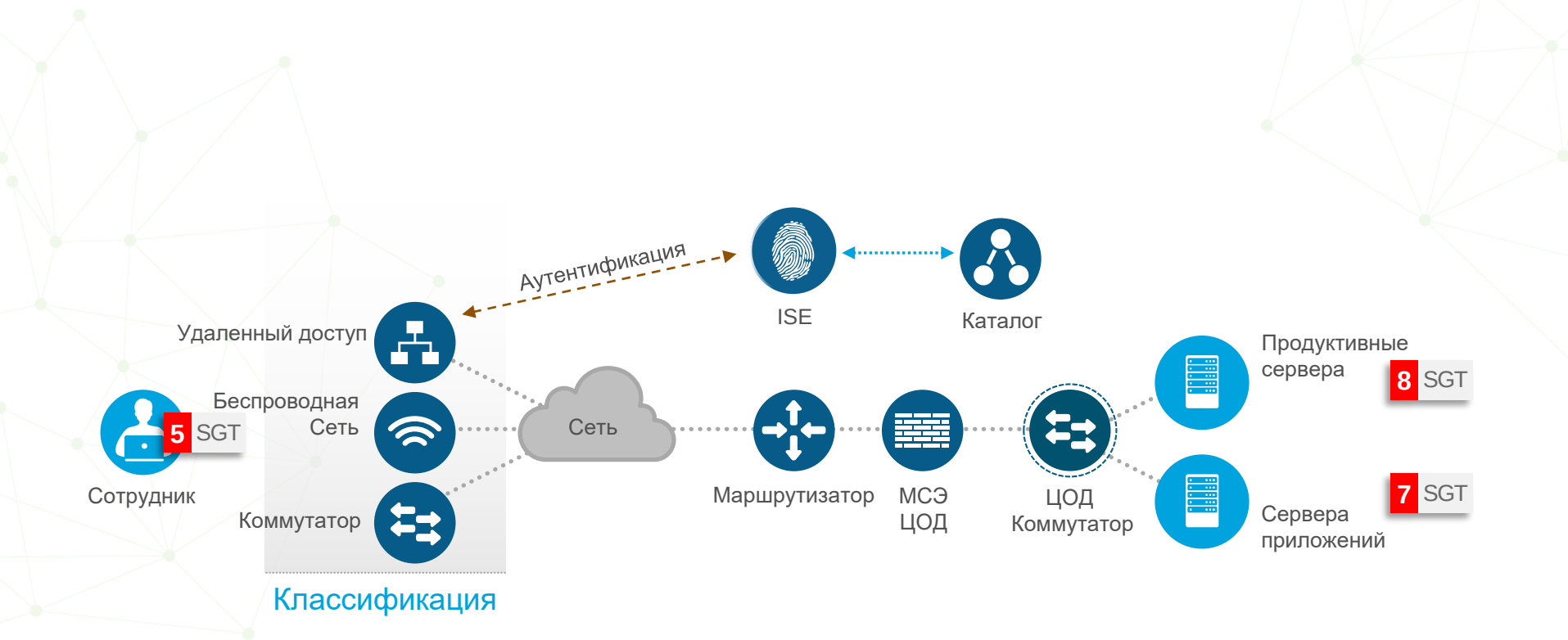
Представляем Cisco TrustSec



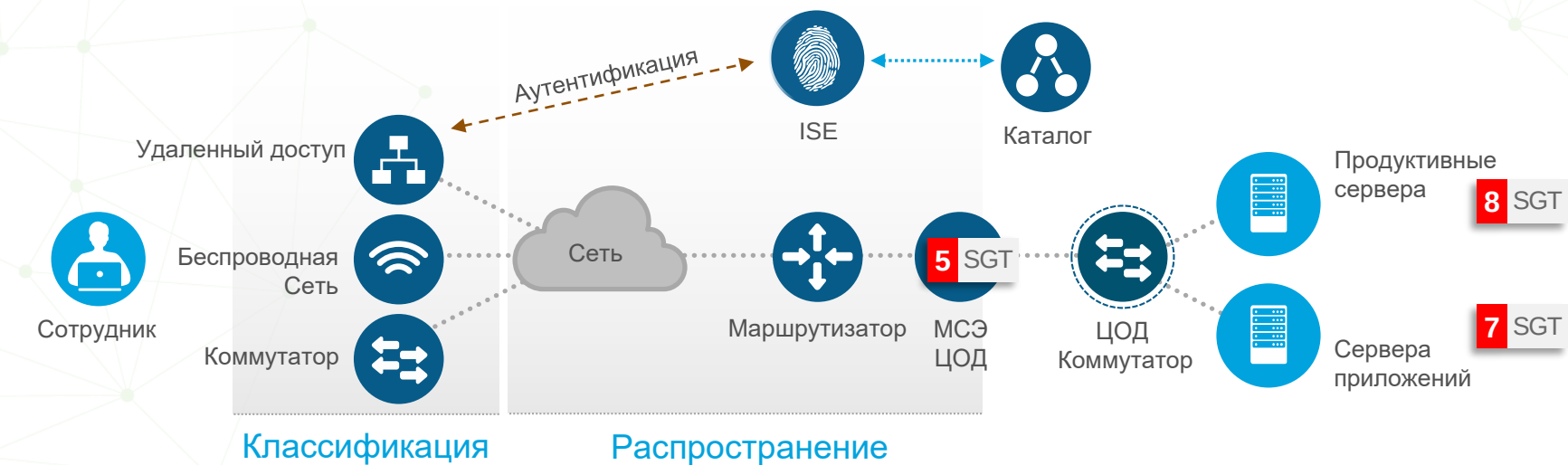
Представляем Cisco TrustSec



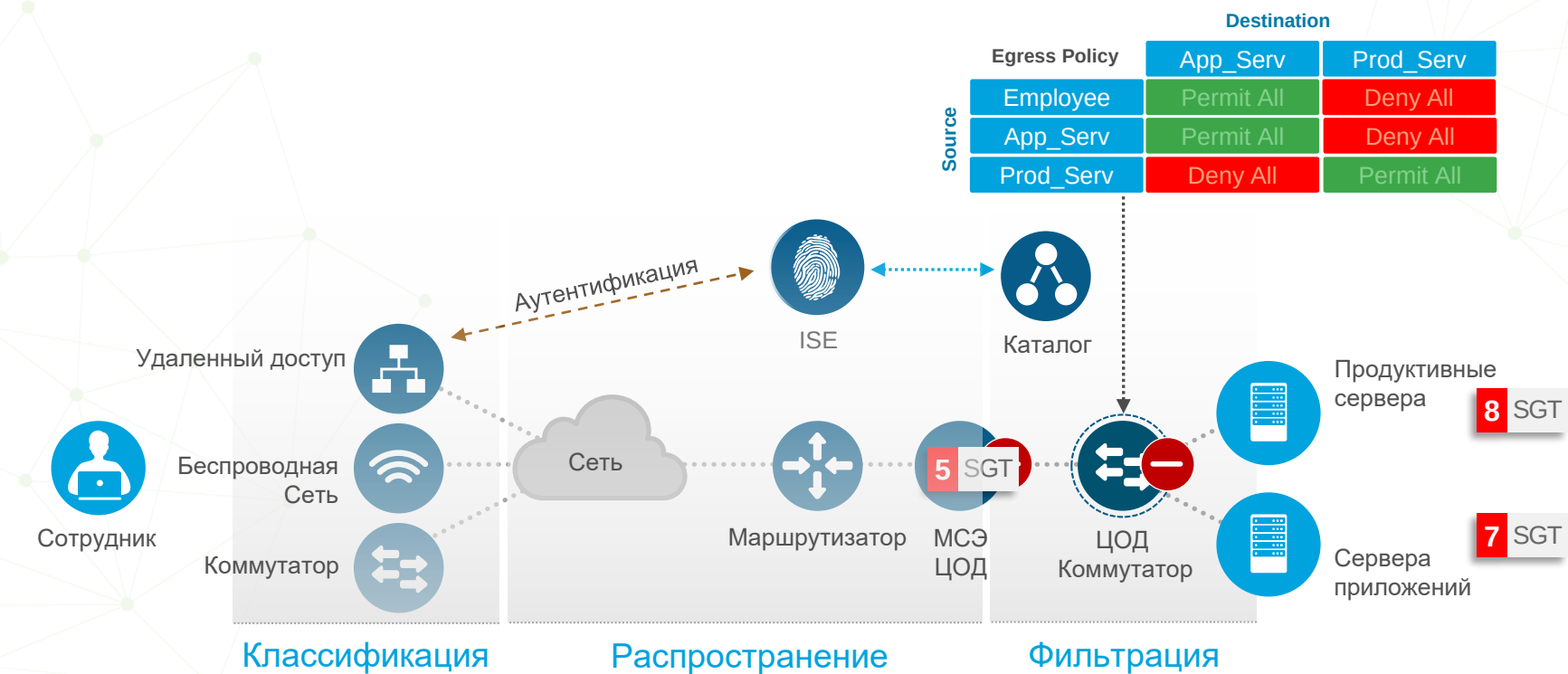
Представляем Cisco TrustSec



Представляем Cisco TrustSec



Представляем Cisco TrustSec



Классификация

Динамическая

Статическая



Классификация



Классификация



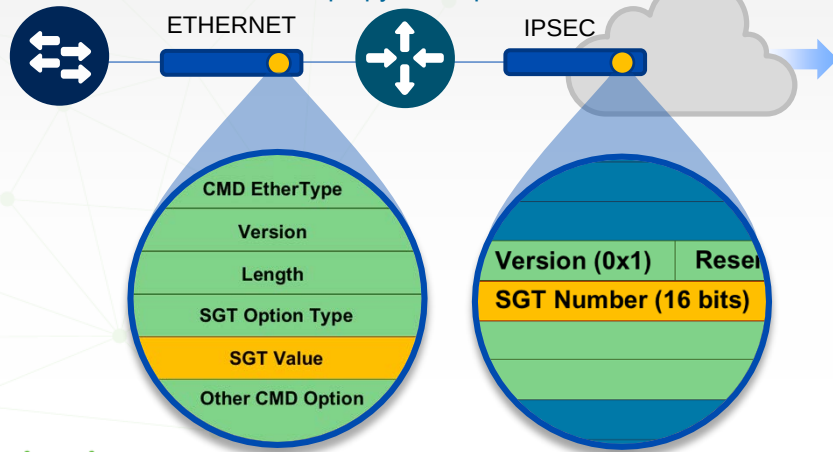
Распространение

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.

Коммутаторы

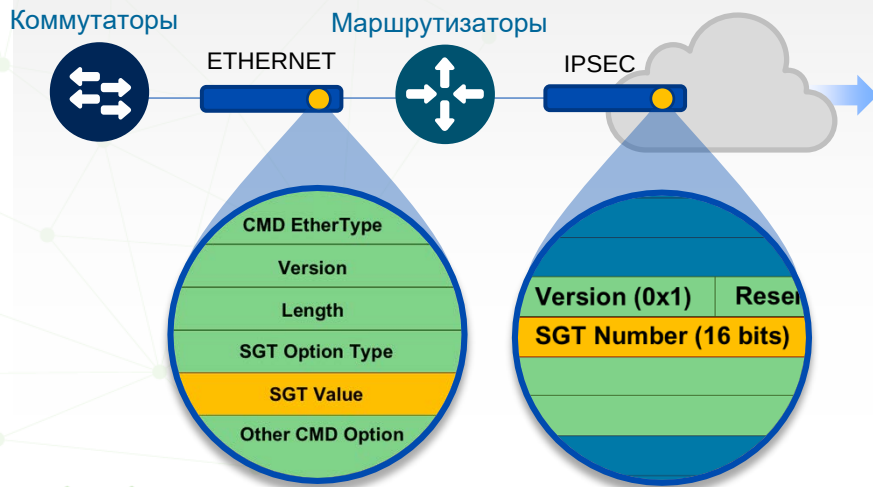
Маршрутизаторы



Распространение

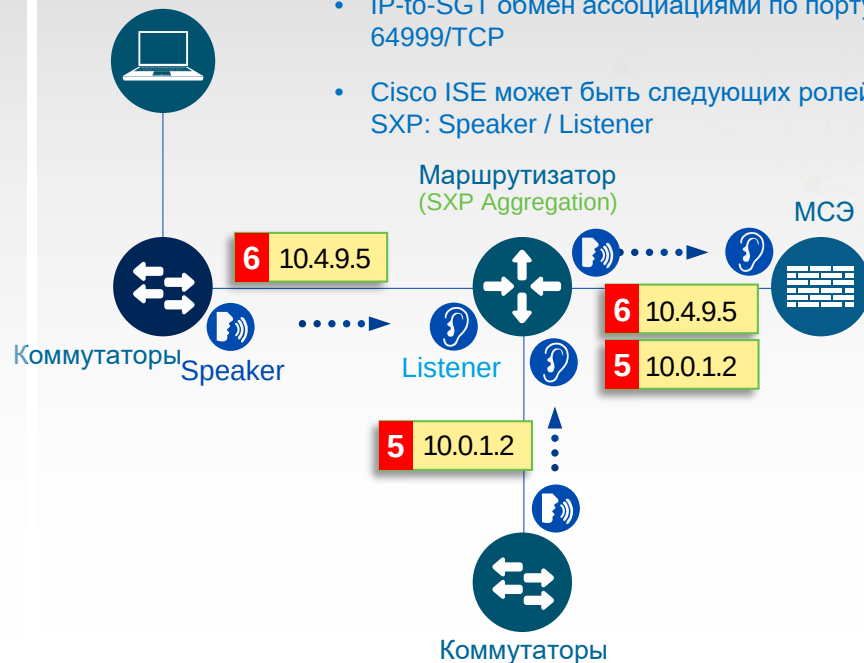
Тегирование фрейма

- **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

The screenshot displays the TrustSec Egress Policy Matrix View. The left sidebar shows the navigation menu with 'TrustSec' expanded, and 'Egress Policy' selected. The main area shows the 'Egress Policy (Matrix View)' with a table of source-destination pairs and their associated policies.

Policy Configuration (Left Panel):

- Policy Name:** Permit_Email_Traffic
- Description:** Access control policy to permit Email service
- Protocol:** ☐ IPv4 ☐ IPv6 ☒ Agnostic
- Rules:**

```

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

```

Egress Policy Matrix (Main View):

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

Footer: Default Enabled SGACLs : Permit IP Description : Default egress rule

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

NEW



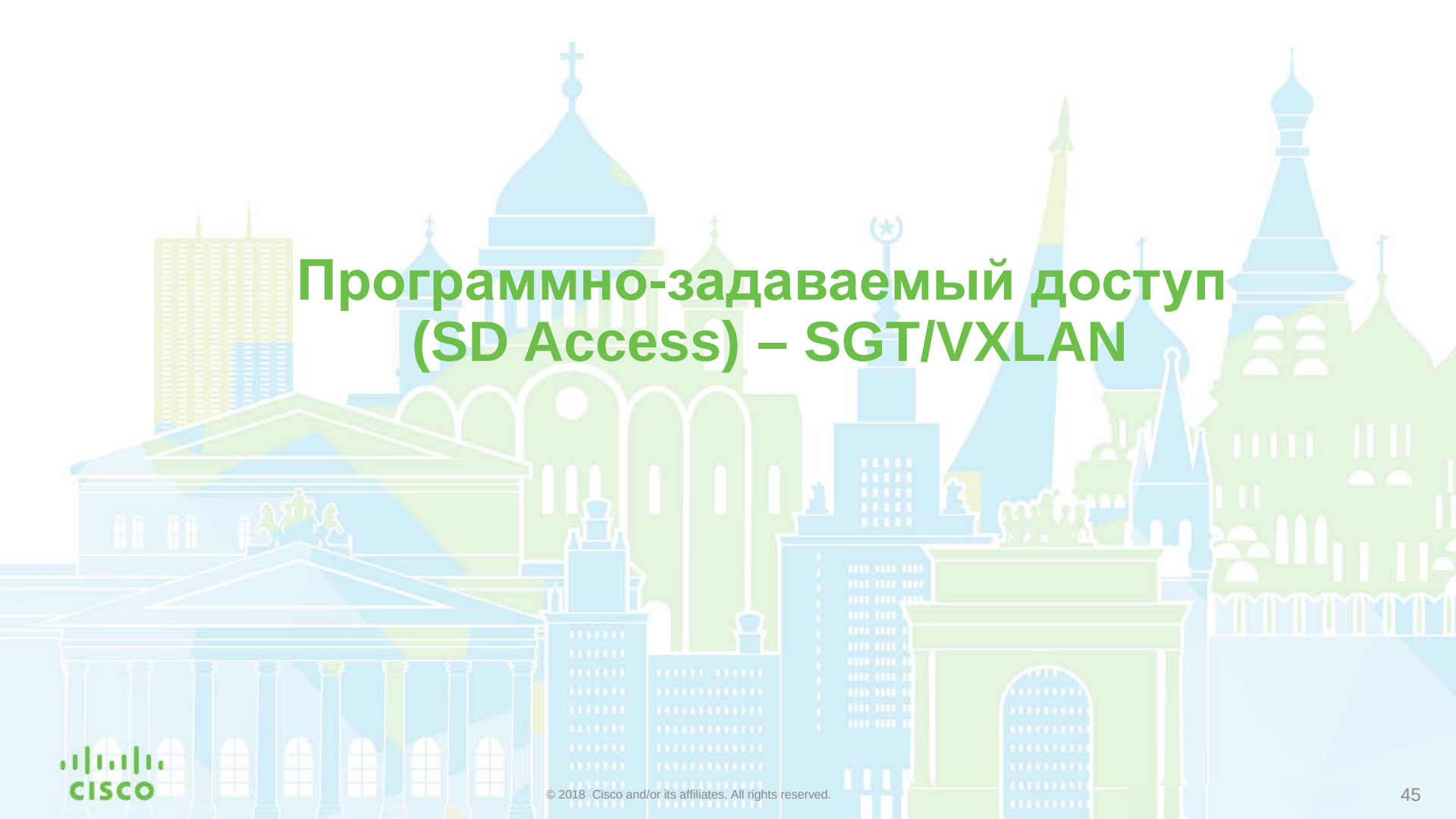
WIRELESS ACCESS POINTS

NEW



ROUTING PLATFORMS

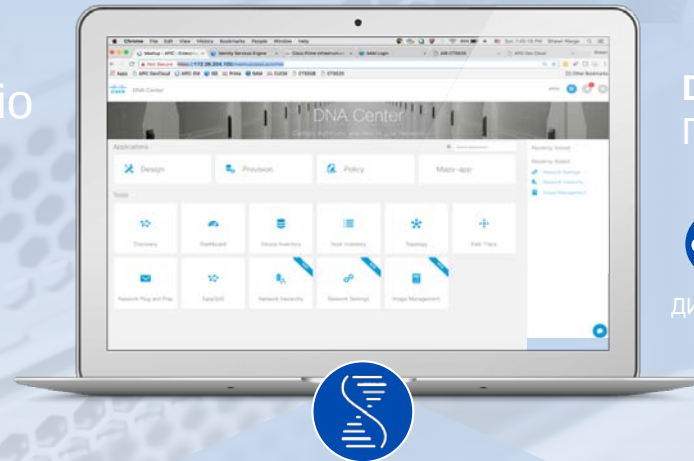
NEW



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

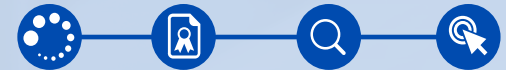
DNA Solution

Cisco Enterprise Portfolio



DNA Center

Простота имплементации



ДИЗАЙН РАЗВЕРТЫВАНИЕ ПОЛИТИКА АНАЛИТИКА



DNA Center



Identity Services Engine



Network Data Platform

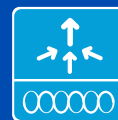
Network Controller
Platform



МАРШРУТИЗАТОРЫ



КОММУТАТОРЫ

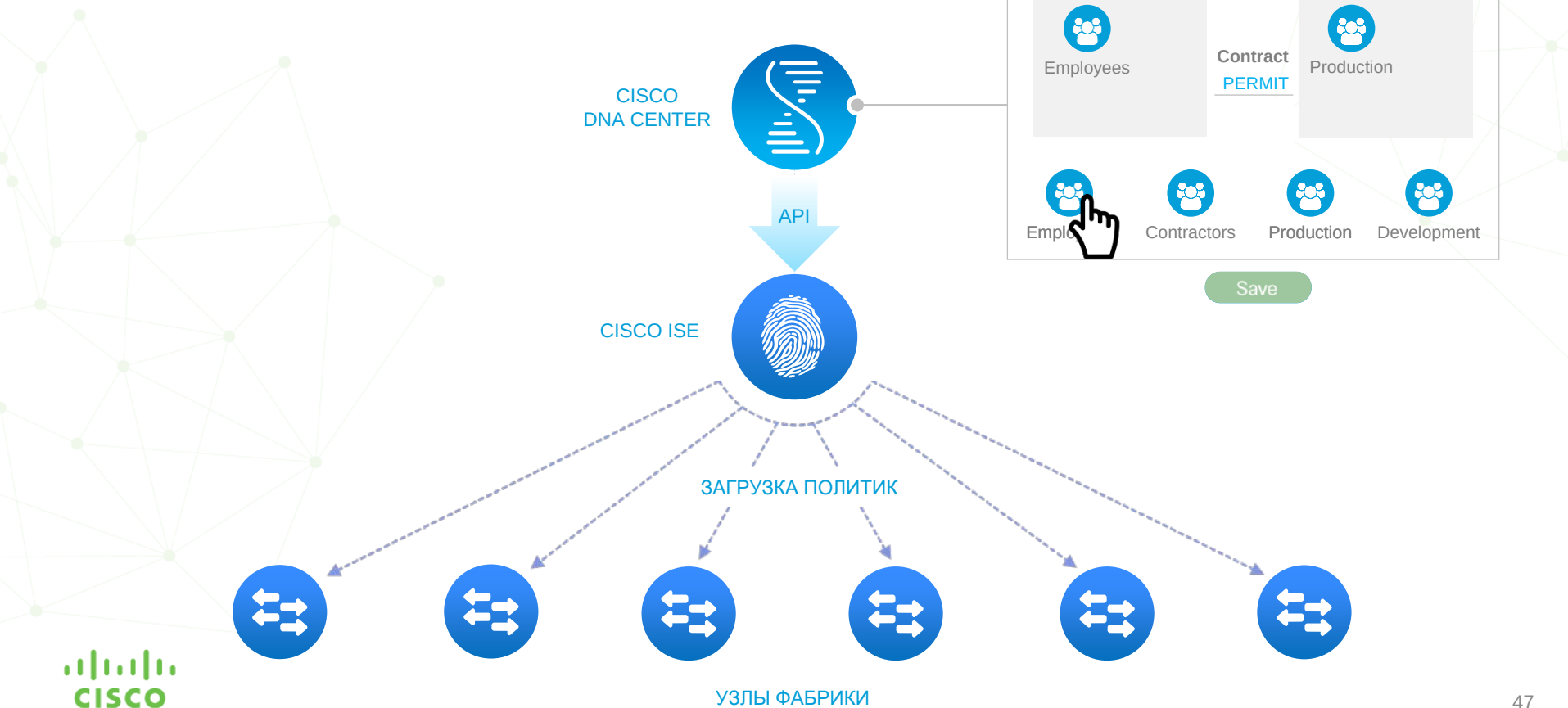


БЛВС КОНТРОЛЛЕРЫ



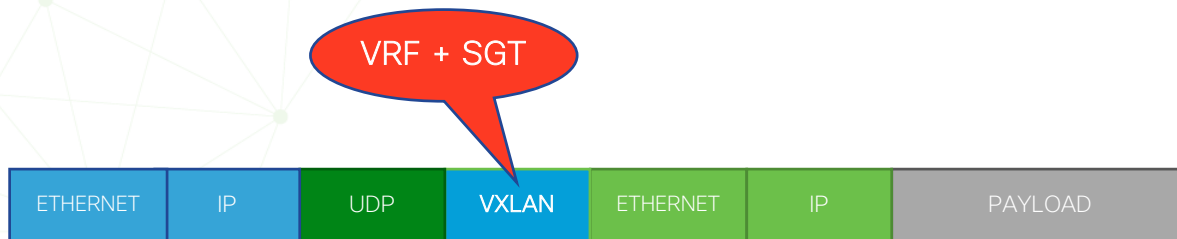
ТОЧКИ ДОСТУПА

SD Access – ISE/DNAC применение политики



Что уникального в SD Access (Кампусной фабрике)?

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



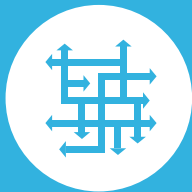
Virtual Routing & Forwarding
Scalable Group Tagging



Поведенческий анализ



Аналитика, которую предоставляет StealthWatch



Обнаружение

Идентификация бизнес-критичных приложений и сервисов в сети



Идентификация дополнительных IOC

Политика и Сегментация
Аномалии сетевого поведения (NBAD)

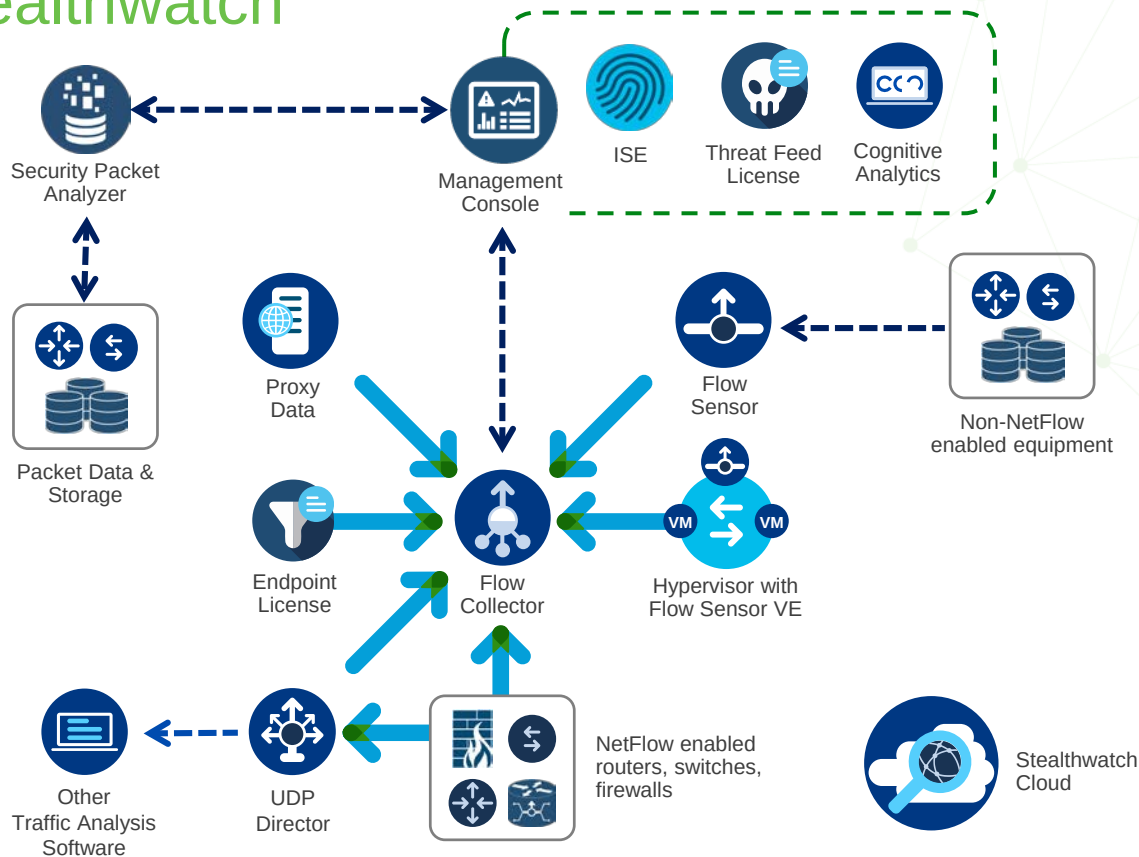


Лучше понимание возможности реагирования на IOC

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

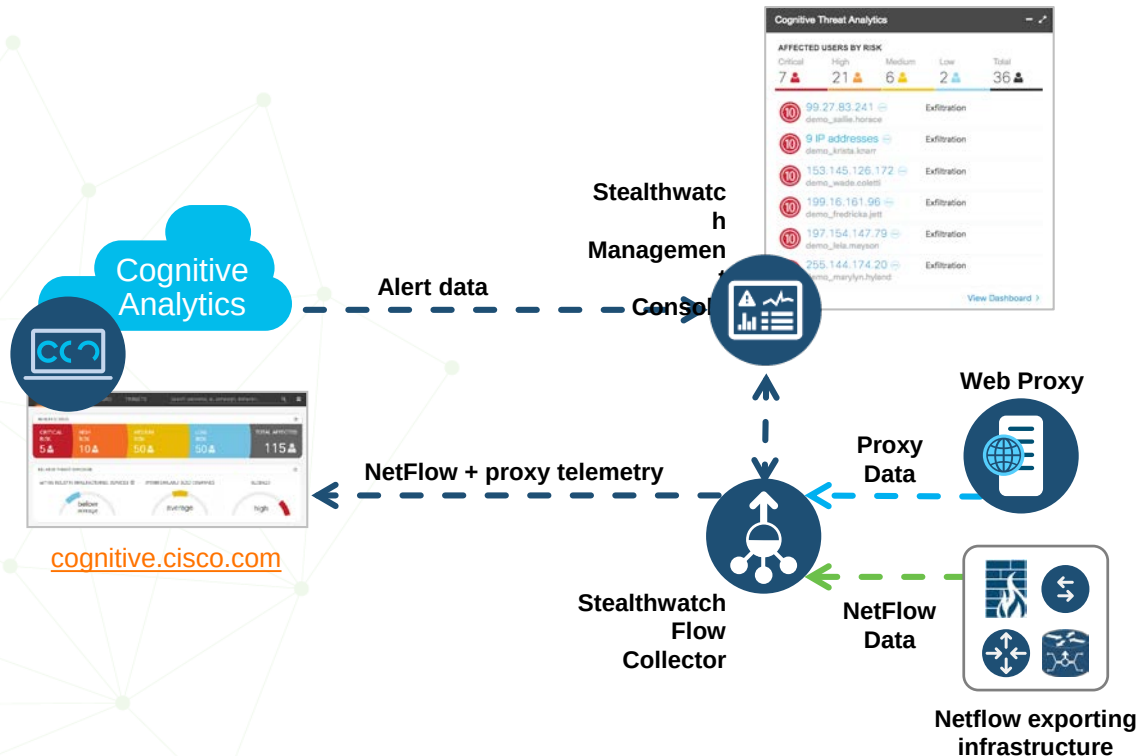
- Обнаружить угрозы, которые обошли текущие механизмы контроля
- Идентификация вывода данных, обнаружение command and control (C2) коммуникаций



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 шифрованного 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

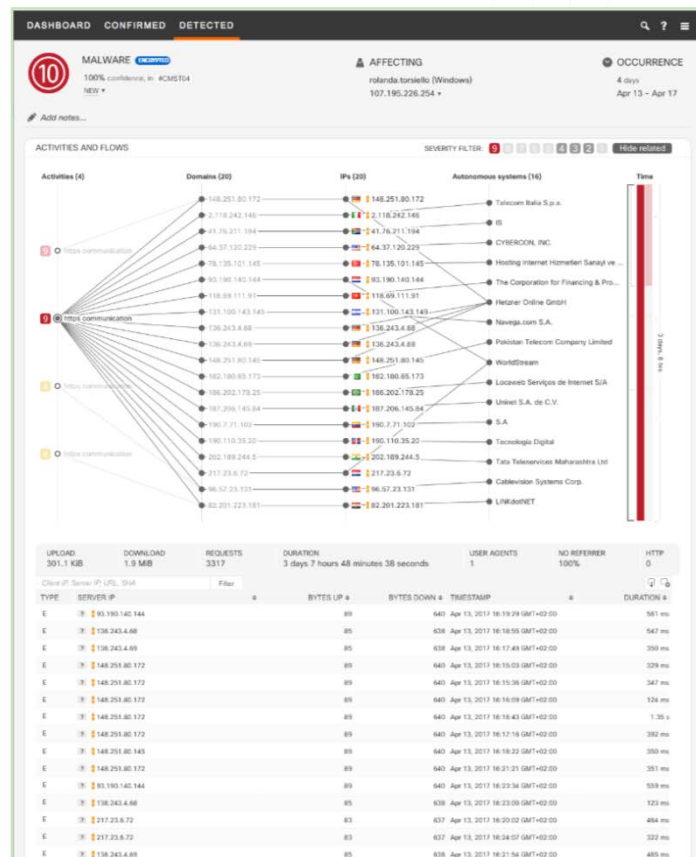
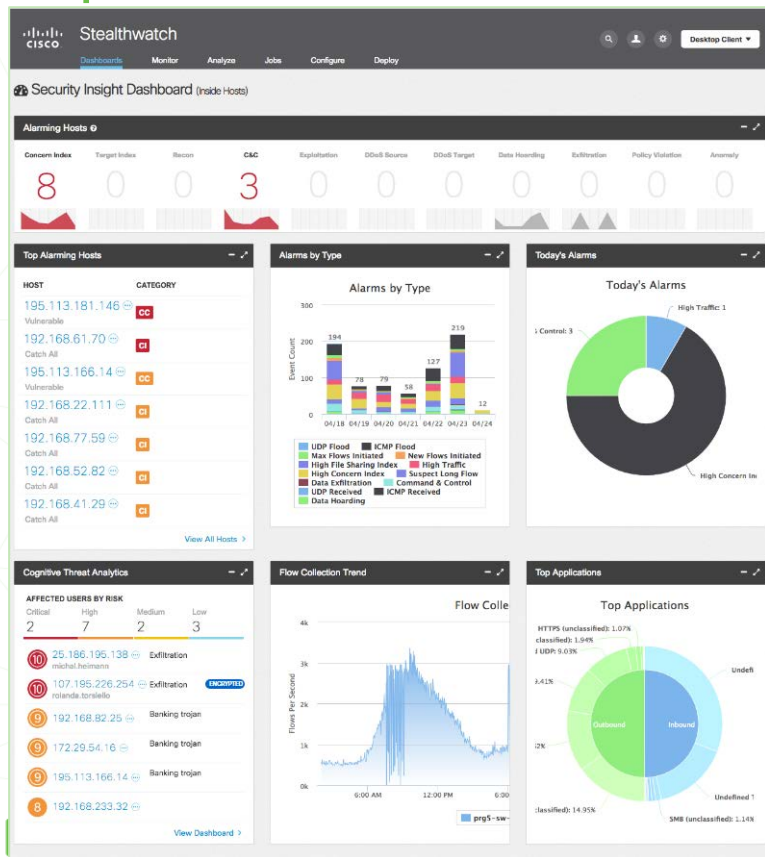
Аномальный
Трафик

Вредоносные
события

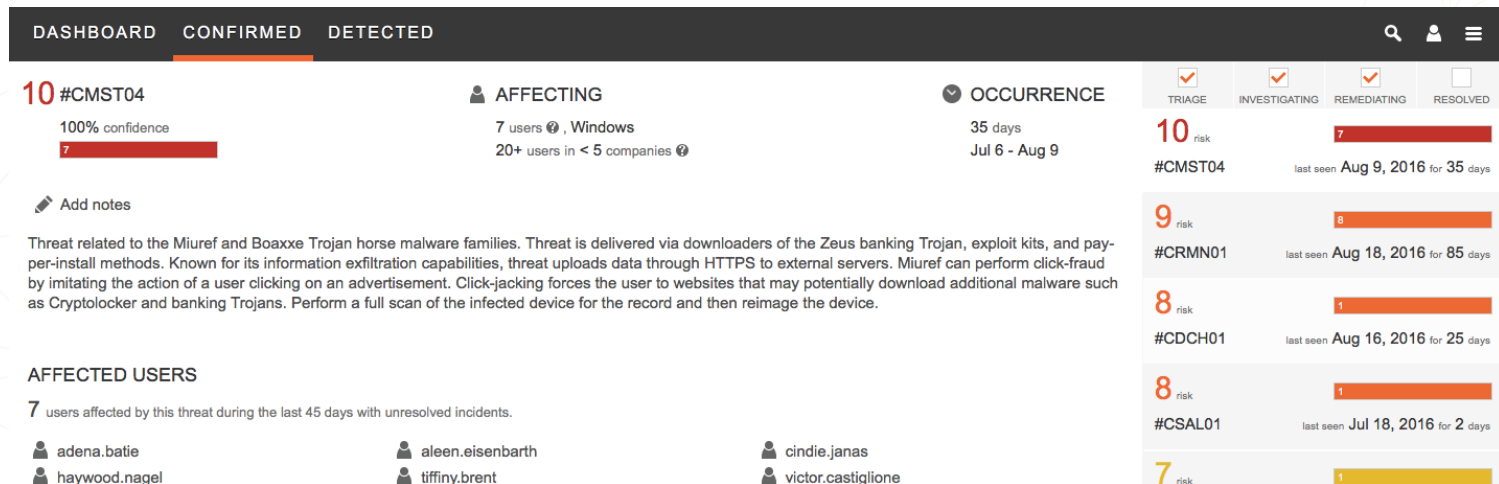
Инциденты
угроз

50,000
Инцидентов в день

Дополнительный уровень аналитики в наблюдаемом трафике



Обнаруженные инциденты с обогащенной атрибуцией



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

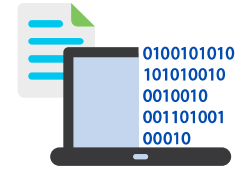
- /Users/Administrator/AppData/Local/Temp/KK0THS510X.exe
- /Users/Administrator/AppData/Local/Temp/a20Pm4SnPg/FnBxKdIO/Setup.exe
- /Users/Administrator/AppData/Local/Temp/QT4731FXGB.exe
- + 606 more paths

Encrypted Traffic Analytics

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



Вредоносы в зашифрованном трафике

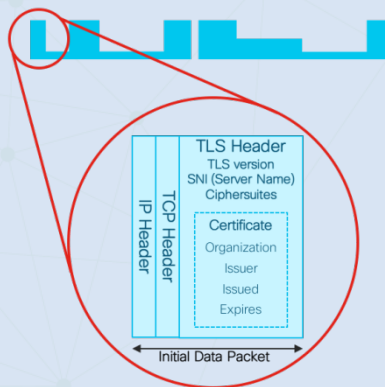


Криптографическое соответствие

Как мы можем инспектировать зашифрованные данные?

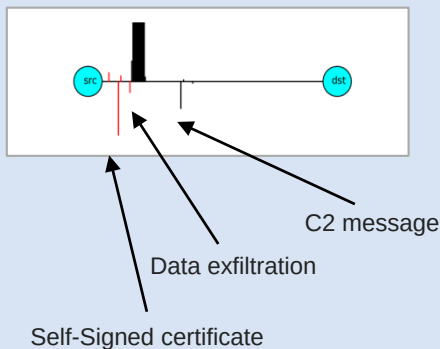
Первый пакет данных

Получите максимум от
нешифрованных полей



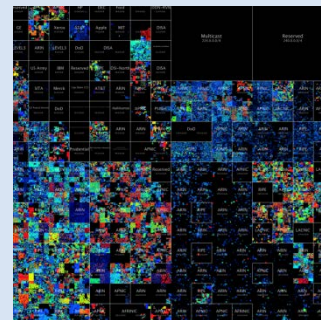
Последовательность длин пакетов и времен

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



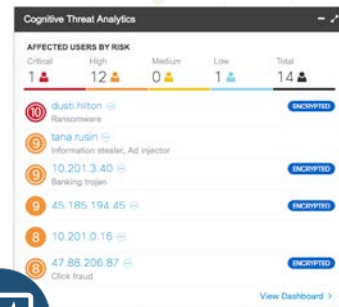
Alert data

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

Stealthwatch

Dashboards Monitor Analyze Jobs Configure Deploy

Flow Search Results (90)

Edit Search Last Hour (Time Range) 2,000 (Max Records)

Subject: 10.201.3.51 Either (Orientation)

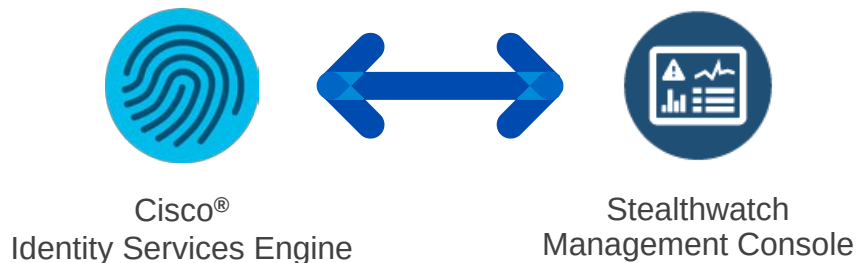
Connection: 443/Tcp (Port / Protocol) All (Flow Direction)

100% Complete Delete Search

Save Search Save Results Start New Search

START	DURATION	SUBJECT POR...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	ENCRYPTION T...	ENCRYPTION K...	ENCRYPTION A...	ENCRYPTION A...	ENCRYPTION ...	PEER PORT/PR...	PEER BYTES	ACTIONS
Ex. 06/09/21	Ex. <=50min40s	Ex. 57100/UDP	Ex. <=50M	Ex. *Corporate...	Ex. <=50M	Ex. 1.0	Ex. ECDH	Ex. ECDSA	Ex. AES_256_GCM	Ex. SHA384	Ex. 2055/UDP	Ex. <=50M	
Nov 9, 2017 10:52:... (46min 19s ago)	54s	49286/TCP	125.67 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	29.96 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	49269/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



Постановка и снятие с карантина
через pxGrid

Host Summary

 *Host IP*
10.201.3.149 ...

Flows Classify History

Status: Active

Hostname: workstation-149

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

Location: RFC 1918

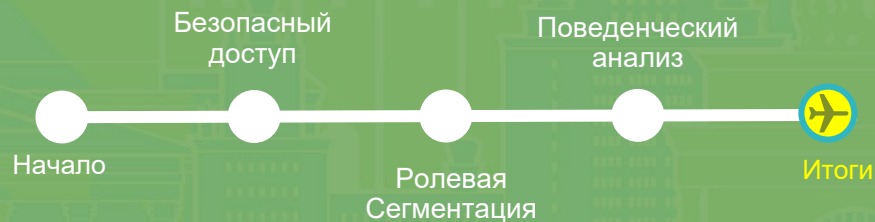
Last Seen: 1/9/17 10:25 AM

Policies: [Host-specific Policy],Inside

MAC Address: --

Quarantine Unquarantine

Заключение



Digital Network Architecture для корпоративной безопасности

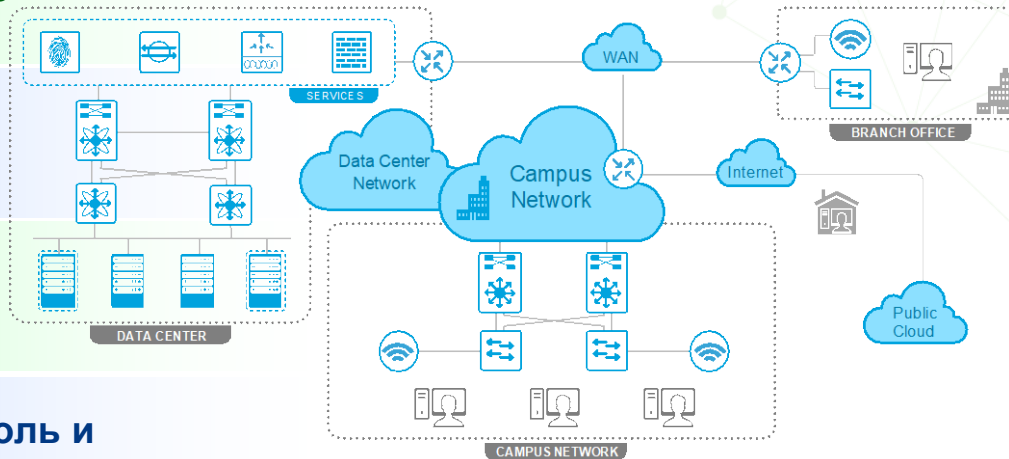
Видимость и контроль повсеместно

Интегрированная в сеть
безопасность

Быстрая реакция на угрозы

Централизованная политика, контроль и
отчетность

‘Инфраструктура’ для защиты ‘Информации’





Спасибо за
внимание!