Комплексная безопасность в инфраструктуре DNA

Дмитрий Казаков
Системный инженер-консультант
CCIE Security, CISSP, CEH

Безопасности нужна видимость контекста и контроль

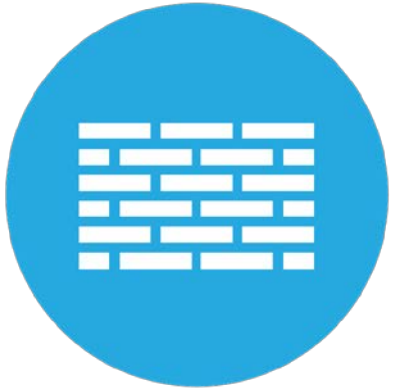
Четкое понимание потоков трафика с контекстом

Проще создавать и применять политики основанные на контексте


БЕЗОПАСНОСТЬ ДОСТУПА
РОЛЕВАЯ СЕГМЕНТАЦИЯ
КОНТРОЛЬ КОНТЕНТА
ПОВЕДЕНЧЕСКИЙ АНАЛИЗ
Пропустить разрешенное и авторизованное
Логическая сегментация, с использованием динамического контроля угроз
Контроль разрешенного контента
Инспекция и анализ действий после разрешения доступа

Нужно начать с релевантных рисков, угроз и требований политик …

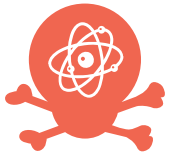
…И защититься от них.



Угрозы

Примеры


Зомби


DDoS


Имперсонализация

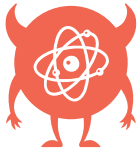

Разрушение


Трояны


Черви


Шпионаж


Command & Control


Zero Days


Внедрение


Внедрение сервиса

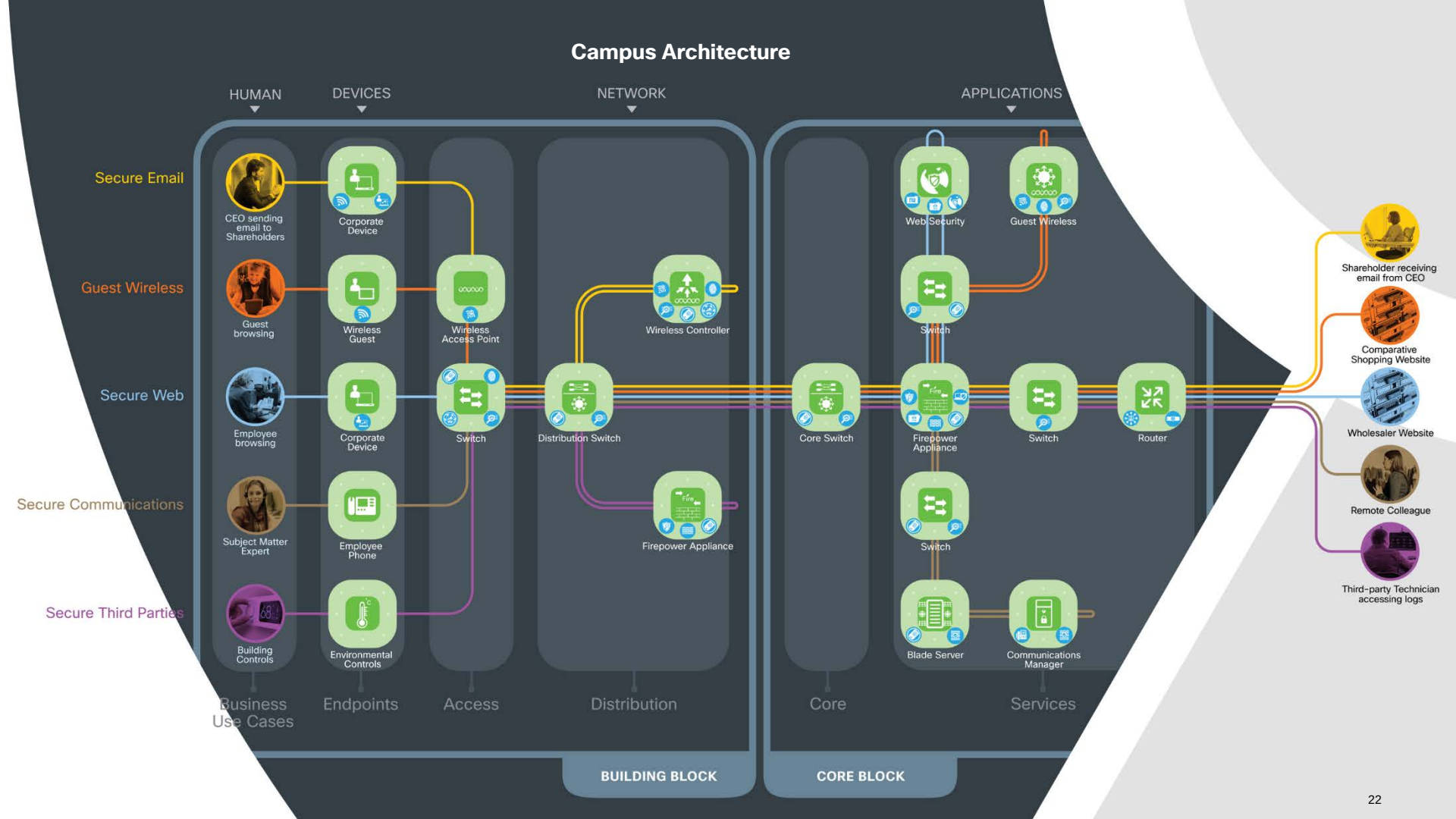

Вывод данных


Шпионское ПО


Вирусы


Сбор данных


HUMAN
DEVICE
NETWORK
APPLICATION
Attack Surface
User
Employees, Third Parties, Customers and Administrators
Device
Client
Voice
Video
Wired
Network
Wireless
Wireless Connection
Analysis
WAN
Public WAN
Cloud
Public/Hybrid Cloud
Application
Application
Security
Identity
Client-Based Security
Posture Assessment
Firewall
Intrusion Prevention
Wireless Rogue Detection
Wireless Intrusion Prevention System
Anti-Malware
Threat Intelligence
Flow Analytics
Web Security
Virtual Private Network (VPN)
Cloud Security
Server-Based Security


Campus Architecture
HUMAN
DEVICES
NETWORK
APPLICATIONS
Secure Email
Guest Wireless
Secure Web
Secure Communications
Secure Third Parties
CEO sending email to Shareholders
Corporate Device
Web Security
Guest Wireless
Guest browsing
Wireless Guest
Wireless Access Point
Wireless Controller
Switch
Employee browsing
Corporate Device
Switch
Distribution Switch
Core Switch
Firepower Appliance
Switch
Router
Subject Matter Expert
Employee Phone
Firepower Appliance
Switch
Building Controls
Environmental Controls
Blade Server
Communications Manager
Shareholder receiving email from CEO
Comparative Shopping Website
Wholesaler Website
Remote Colleague
Third-party Technician accessing logs
Business Use Cases
Endpoints
Access
Distribution
Core
Services
BUILDING BLOCK
CORE BLOCK

Безопасность доступа

Cisco ISE и Anyconnect

Cisco ISE

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

Cisco Anyconnect

Супликант 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

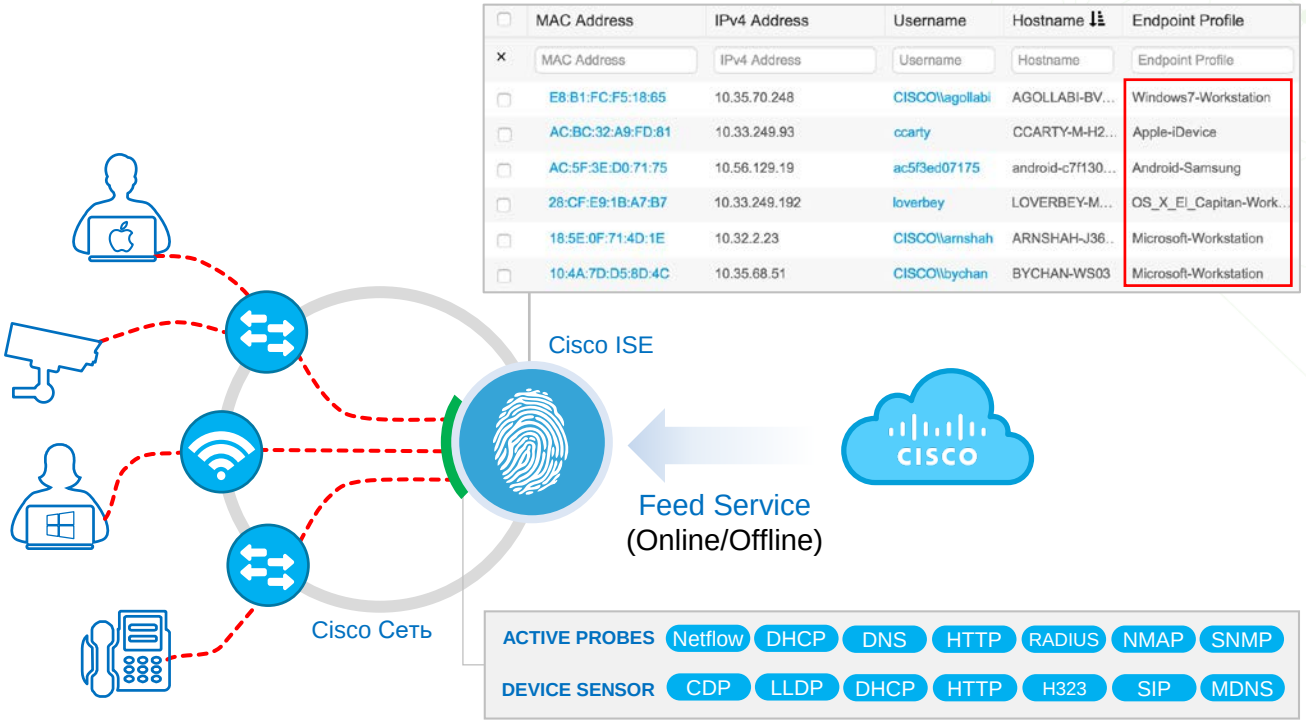
Устройств с ‘50’ атрибутами каждый можно хранить

550+

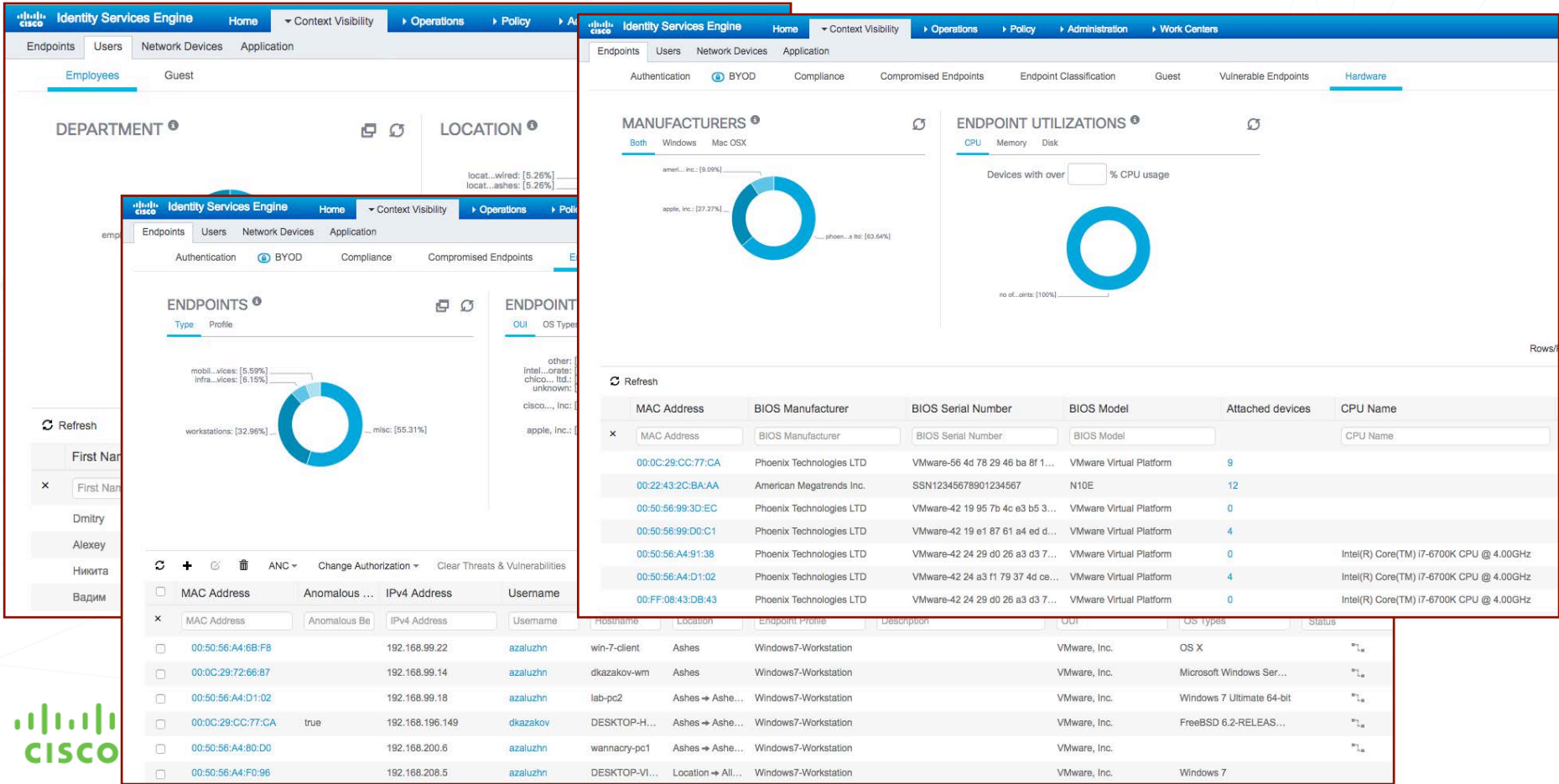
Высокоуровневые вложенные профили.
+Периодические обновления

250+

Профили медицинских устройств



Видимость групп и пользователей



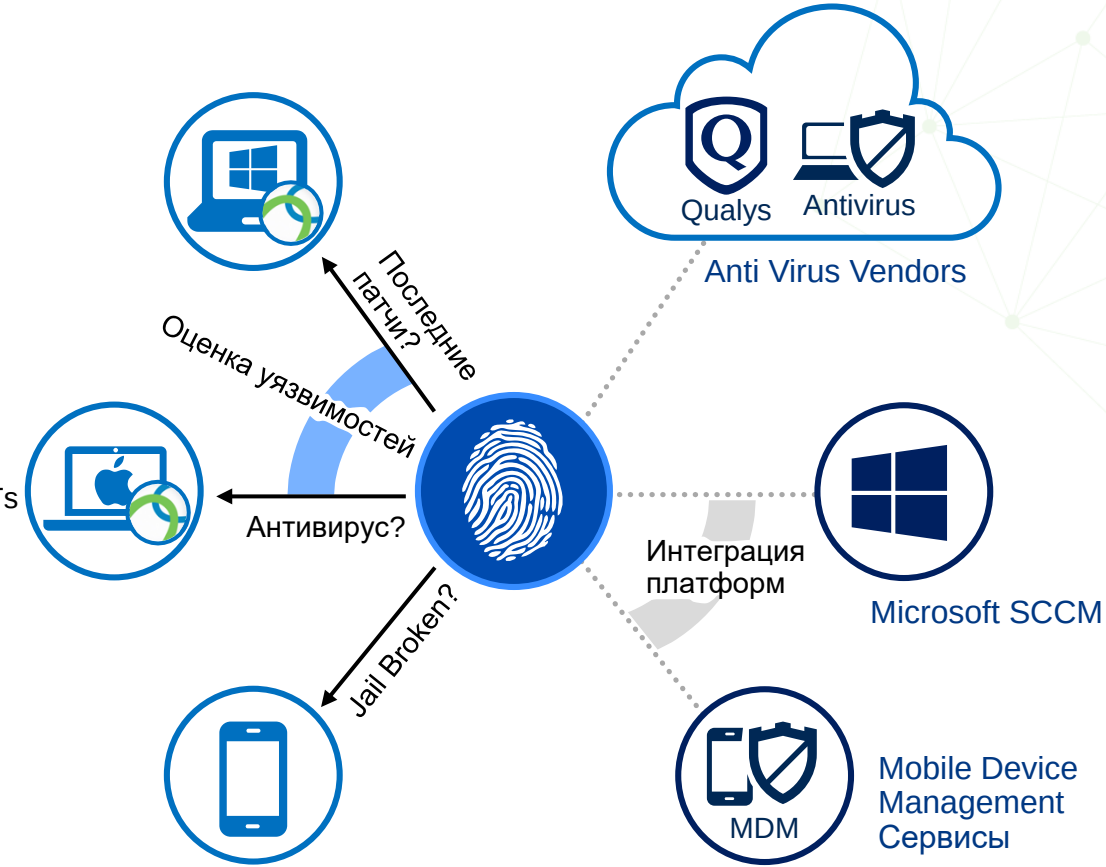
А что с оценкой состояния?

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		Богатый контекст
IP ADDRESS: 192.168.2.101		Дмитрий Казаков (СОТРУДНИК)
НЕИЗВЕСТНО		WINDOWS WORKSTATION
НЕИЗВЕСТНО		ЗДАНИЕ-А-ЭТАЖ-13
НЕИЗВЕСТНО		10:30 AM MSK APR 27
НЕИЗВЕСТНО		БЕСПРОВОДНАЯ СЕТЬ
НЕИЗВЕСТНО		НЕТ УГРОЗ / УЯЗВИМОСТЕЙ

РЕЗУЛЬТАТ	РЕЗУЛЬТАТ
ДОСТУП К IP (ЛЮБОЕ УСТРОЙСТВО / ПОЛЬЗОВАТЕЛЬ)	РОЛЕВОЙ ДОСТУП

ИЗВЕСТНО

Обмен контекстом

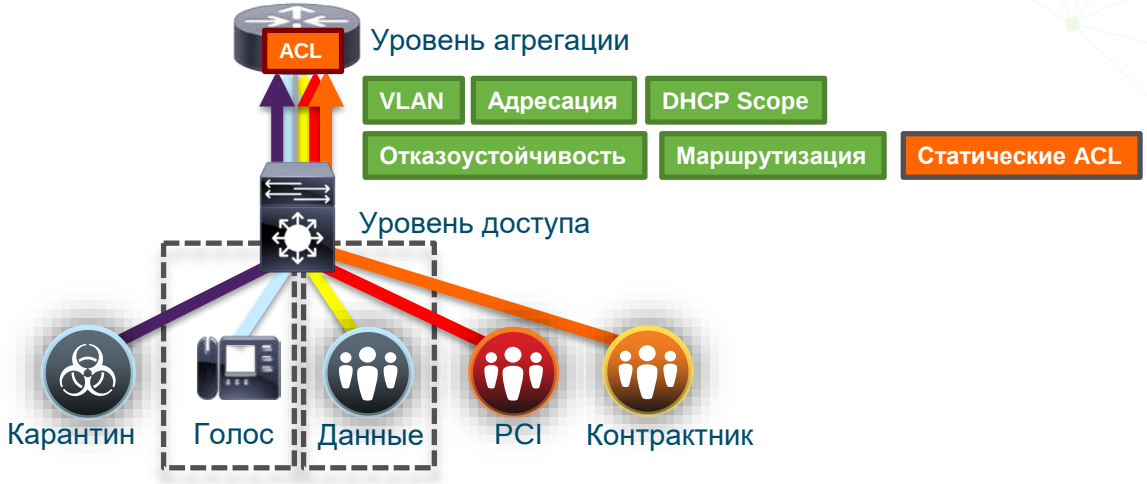
Обогатить контекст (для Политики Доступа)
Угрозы, Уровень уязвимости, MDM атрибуты, др

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

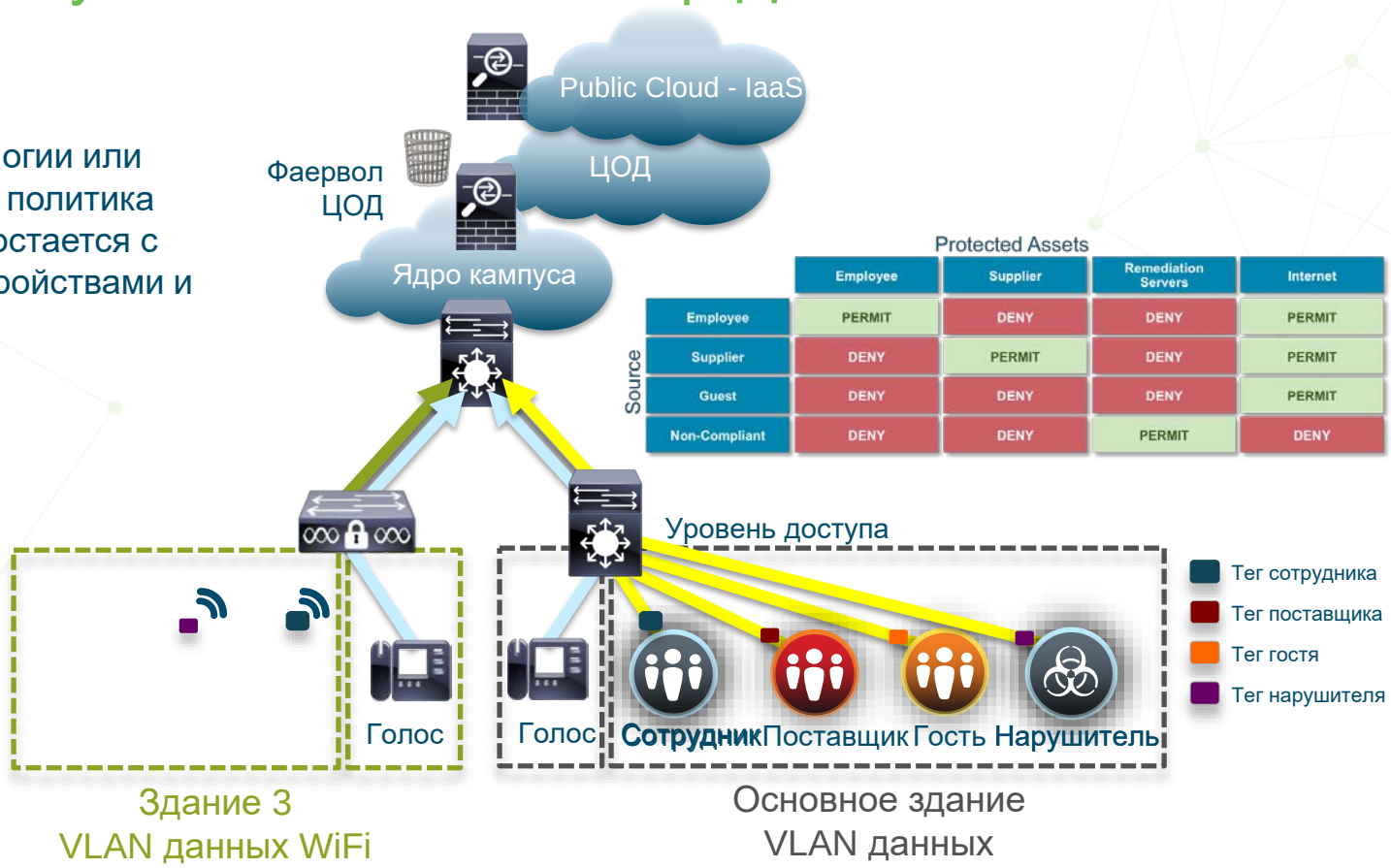


Большая сложность управления VLAN

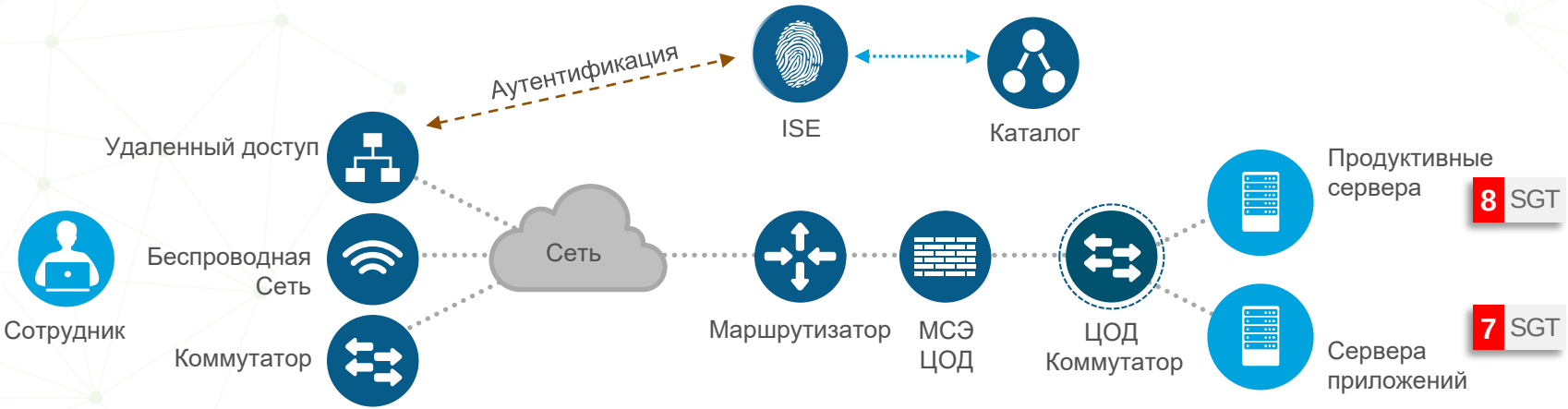
Контроль доступа пользователя в ЦОД с TrustSec

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

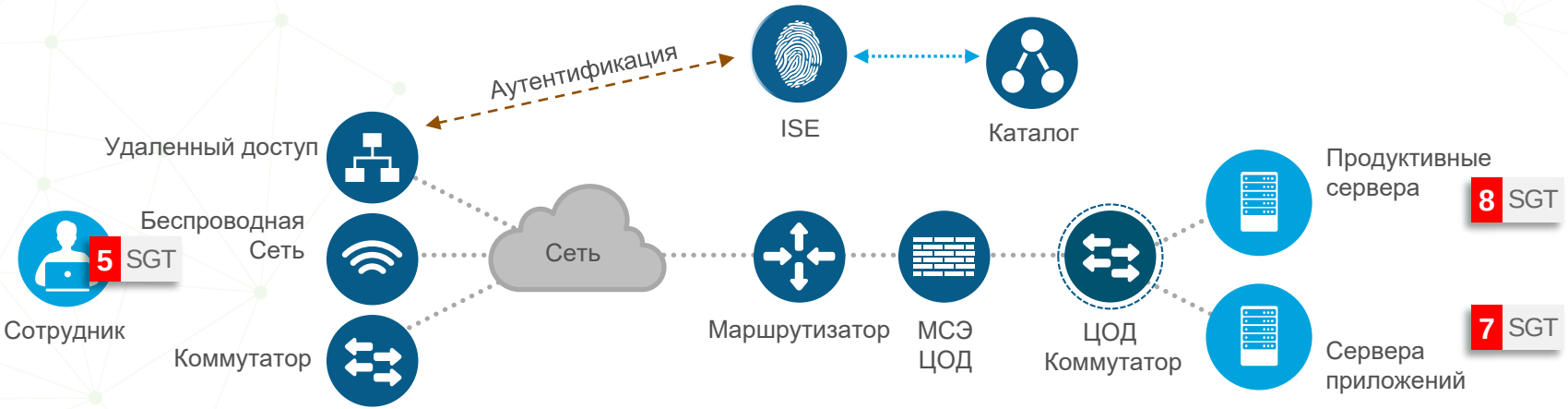
TrustSec упрощает управление ACL для трафика внутри/вне VLAN



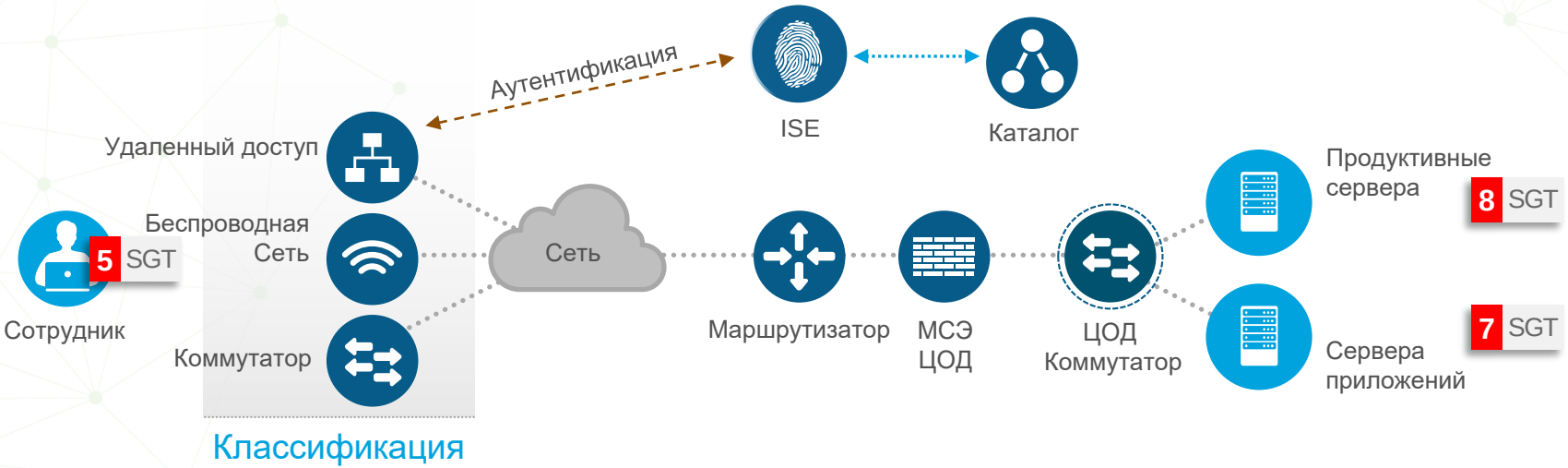
Представляем Cisco TrustSec



Представляем Cisco TrustSec

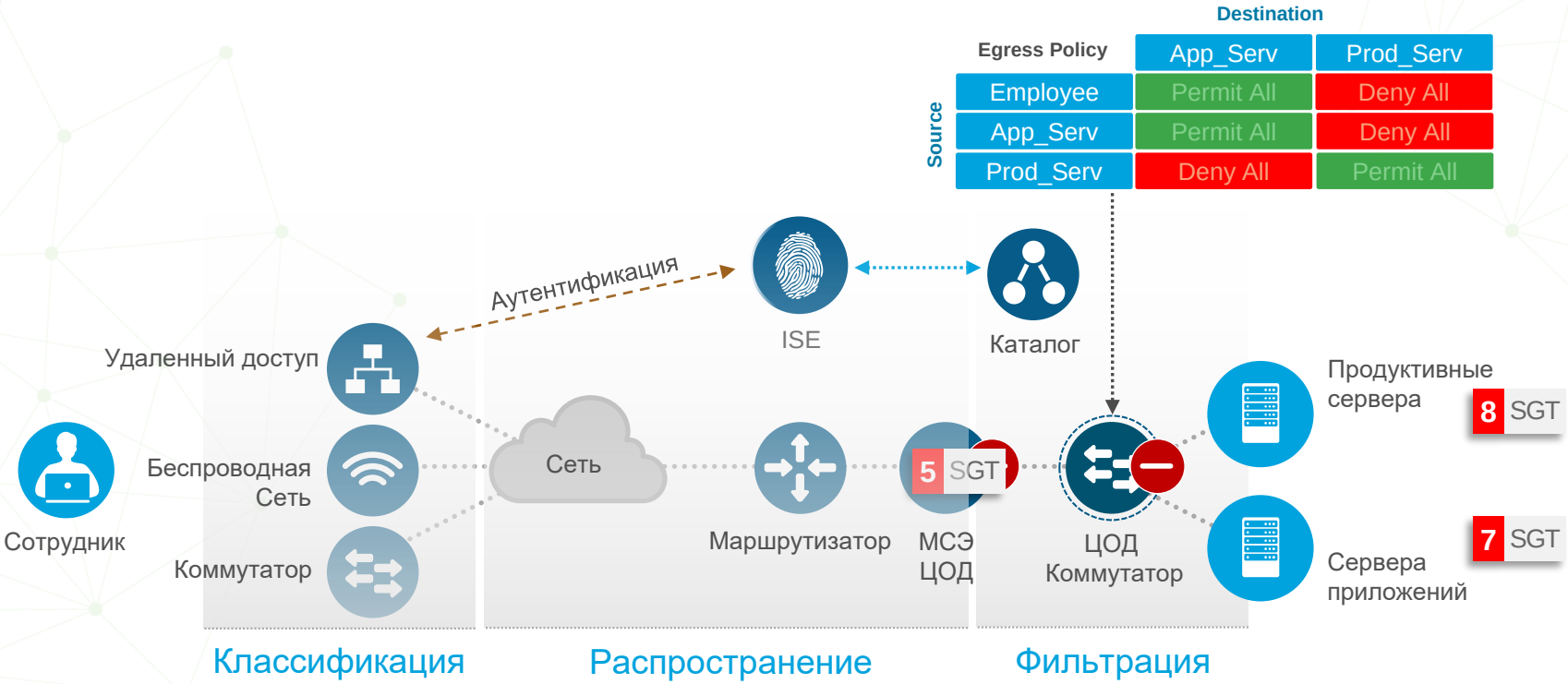


Представляем Cisco TrustSec



Представляем Cisco TrustSec

Представляем Cisco TrustSec

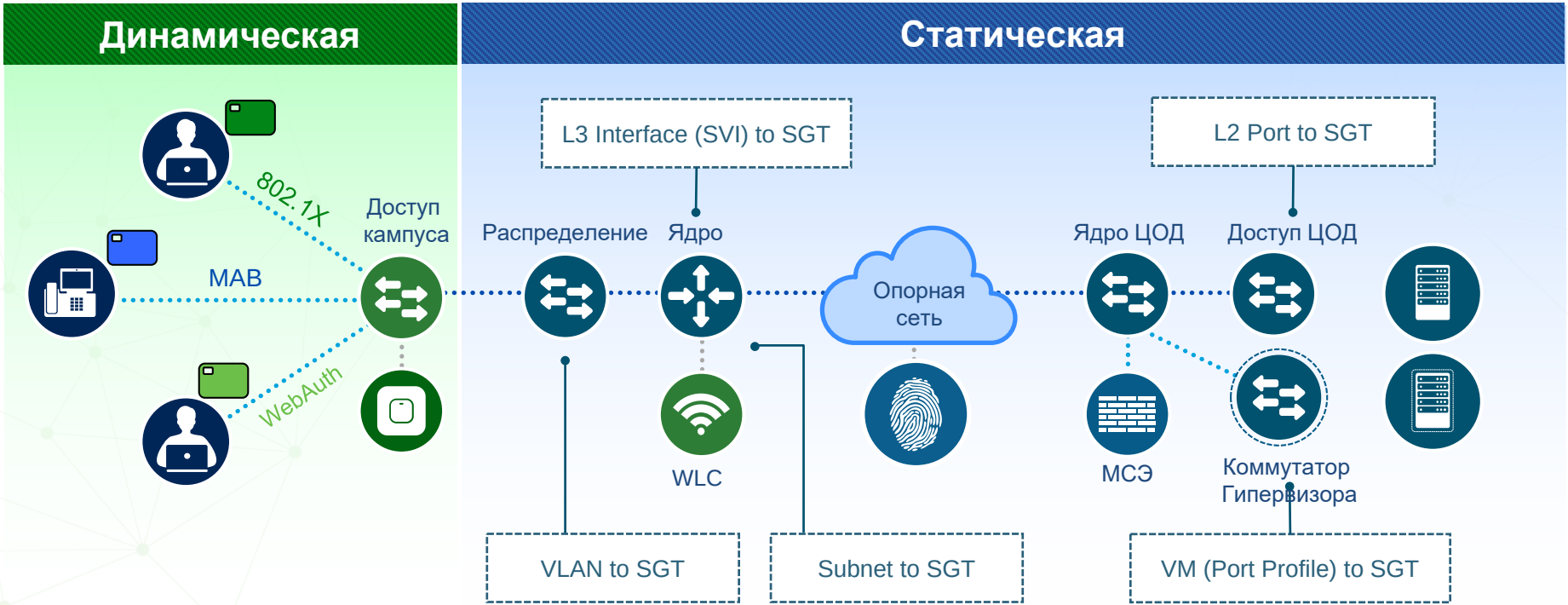


Классификация

Динамическая | **Статическая**

Классификация

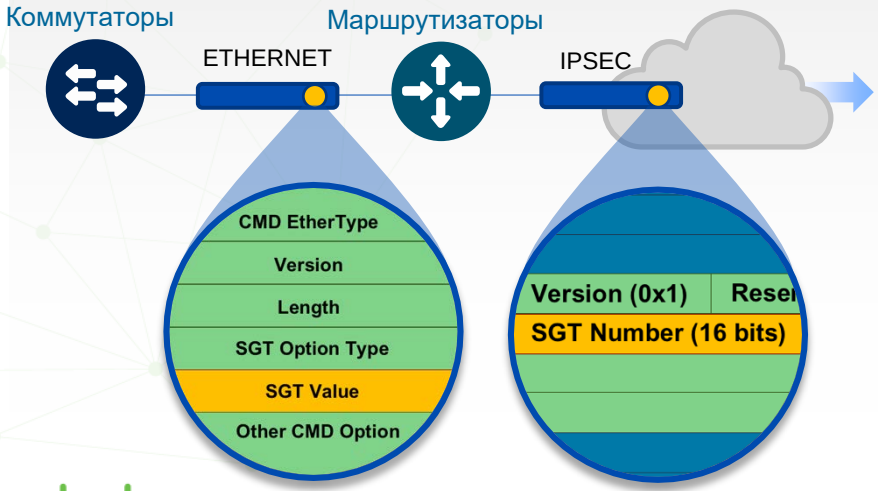
Классификация



Распространение

Тегирование фрейма

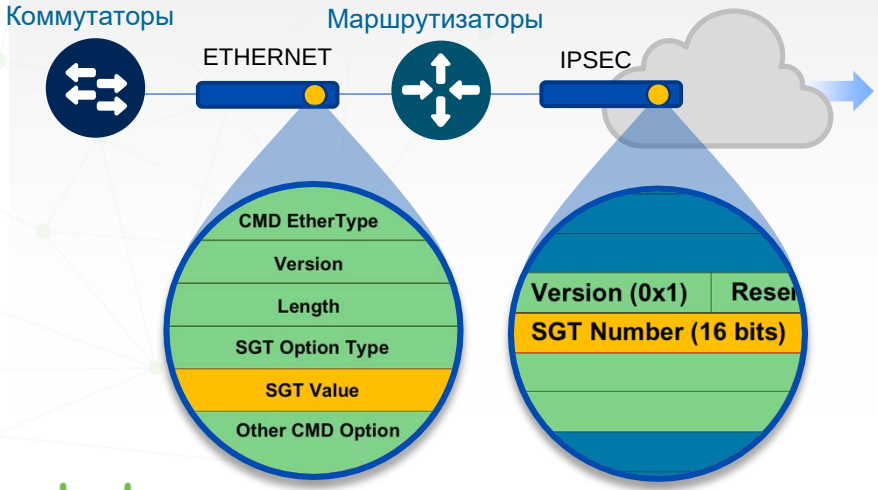
- **Ethernet Inline Tagging:** (EtherType:0x8909) 16-Bit SGT инкапсуляция в Cisco Meta Data (CMD) payload.
- **IPSec / L3 Crypto:** Cisco Meta Data (CMD) использует протокол 99, и включается в начало ESP/AH payload.



Распространение

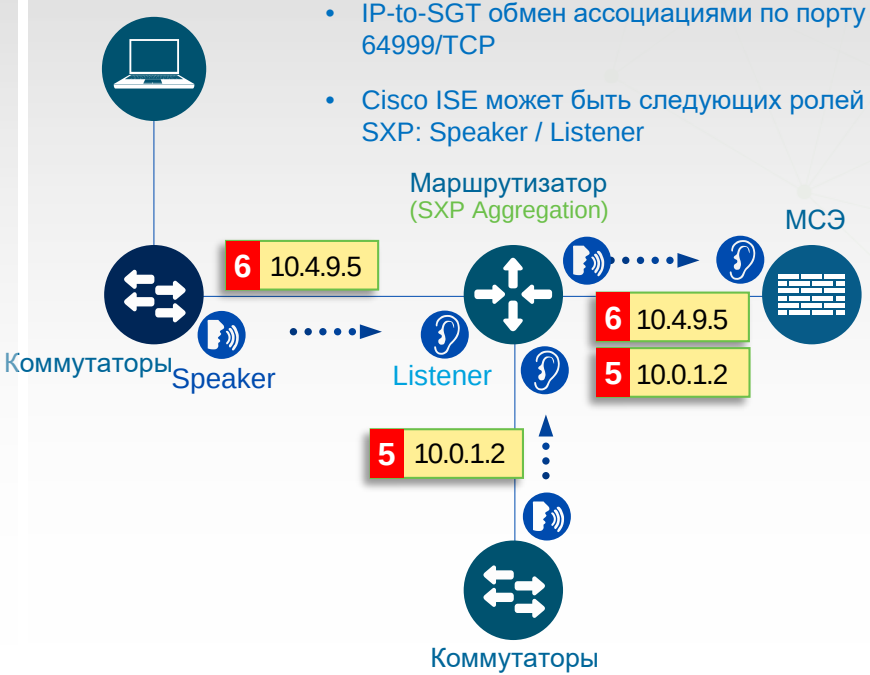
Тегирование фрейма

- **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.

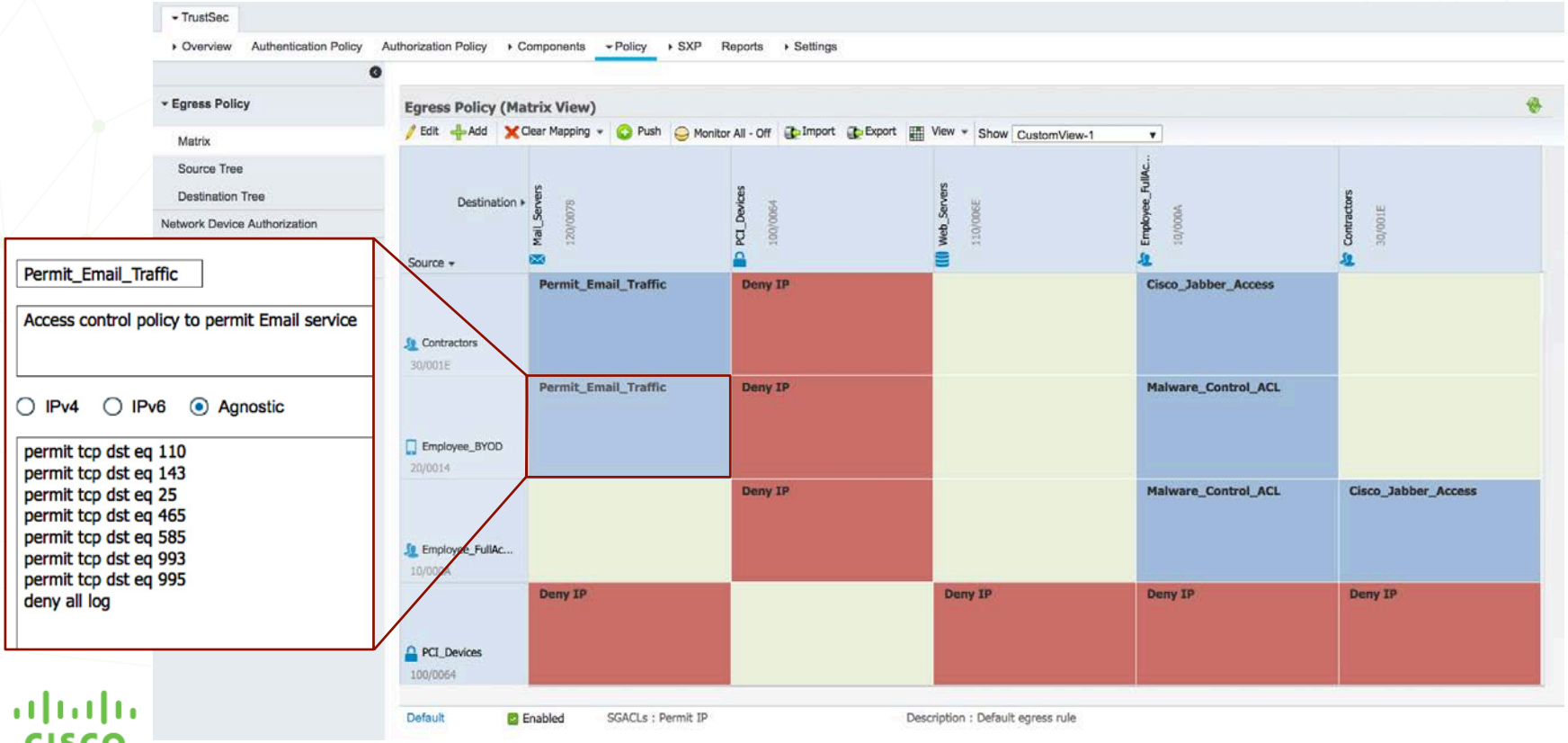


SGT Exchange Protocol (SXP)

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

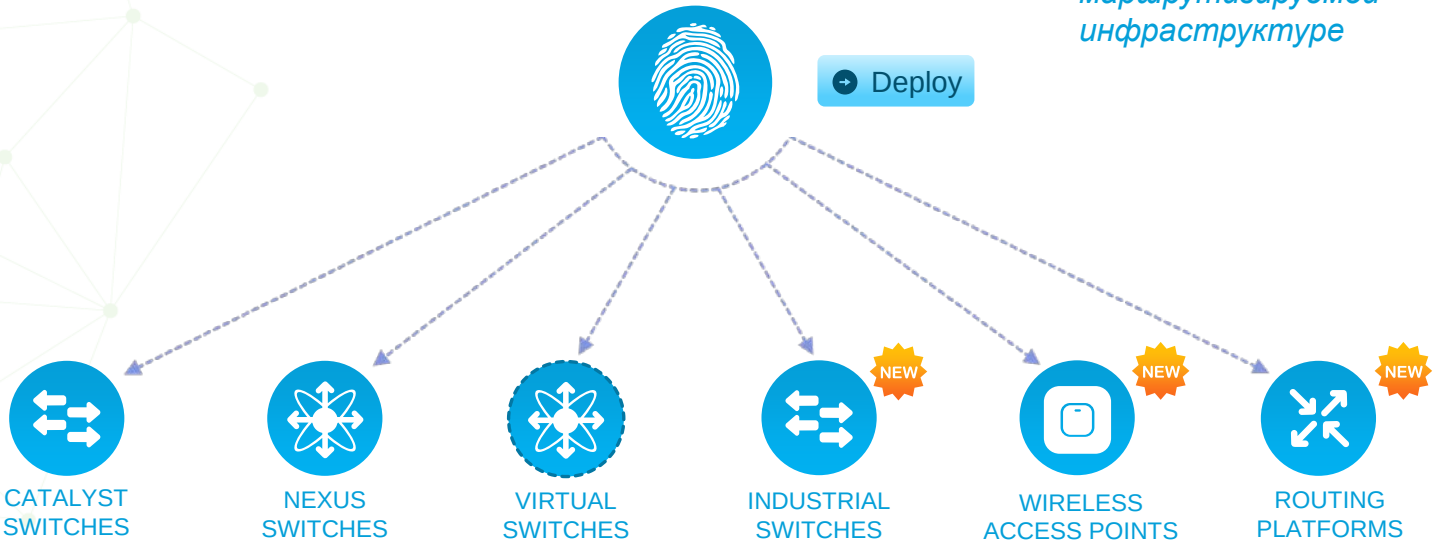


TrustSec политика фильтрации



Целостное применение политики

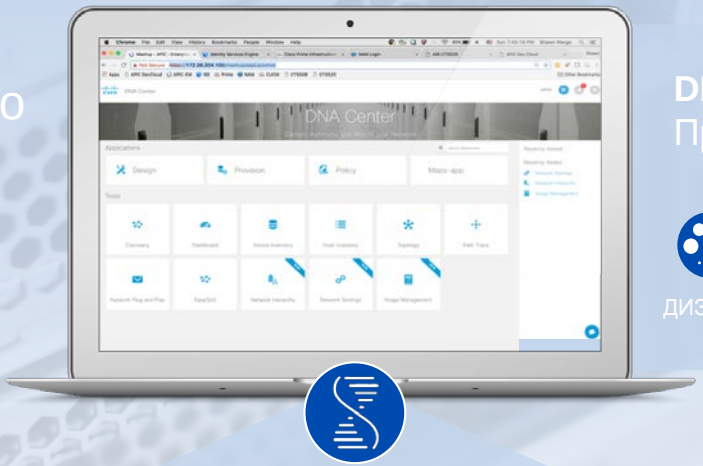
Отправляйте и разворачивайте TrustSec политики целостно в коммутируемой, беспроводной и маршрутизируемой инфраструктуре



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

DNA Solution

Cisco Enterprise Portfolio



DNA Center

Простота имплементации

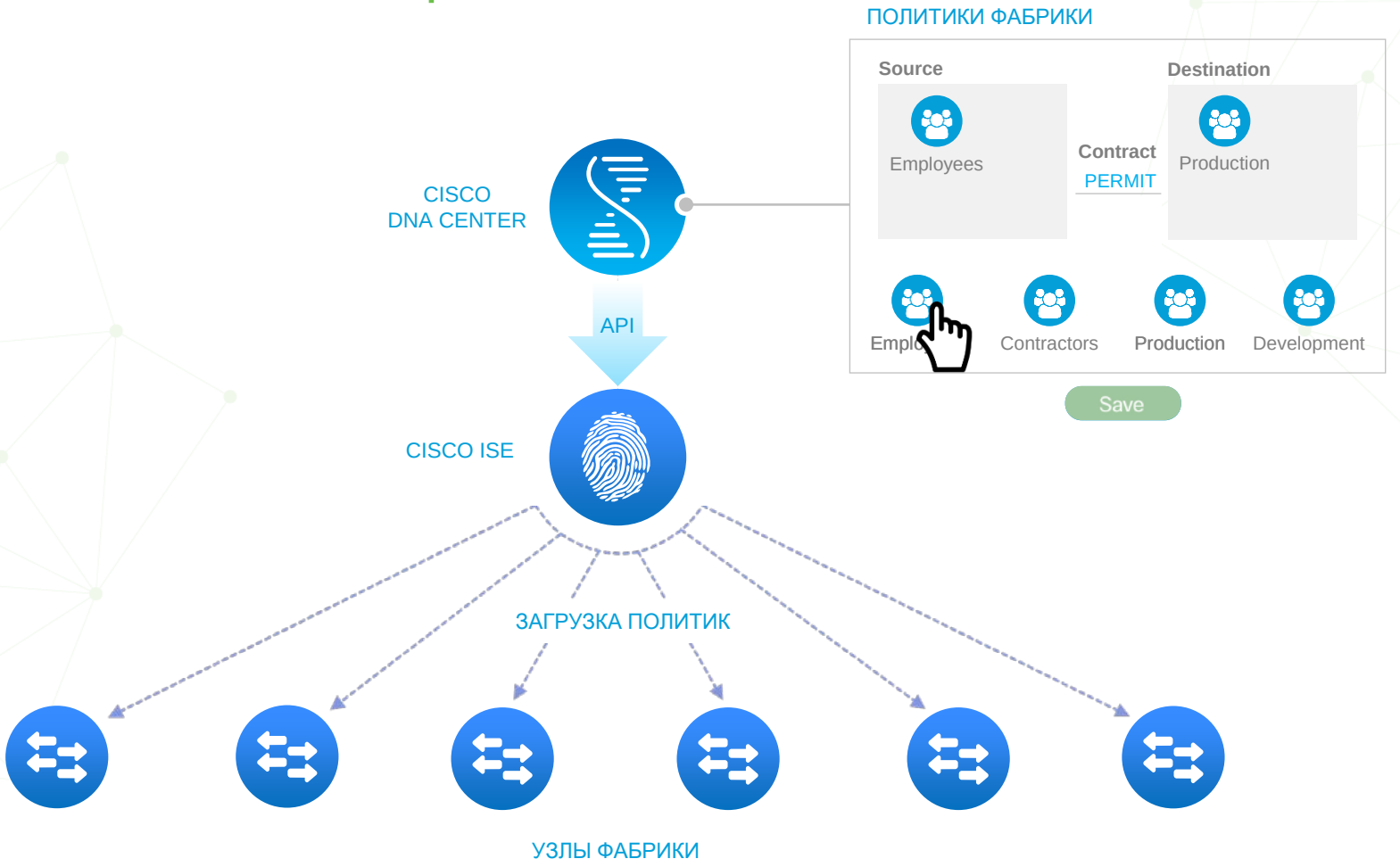
ДИЗАЙН — РАЗВЕРТЫВАНИЕ — ПОЛИТИКА — АНАЛИТИКА

DNA Center

Identity Services Engine — **Network Controller Platform** — **Network Data Platform**

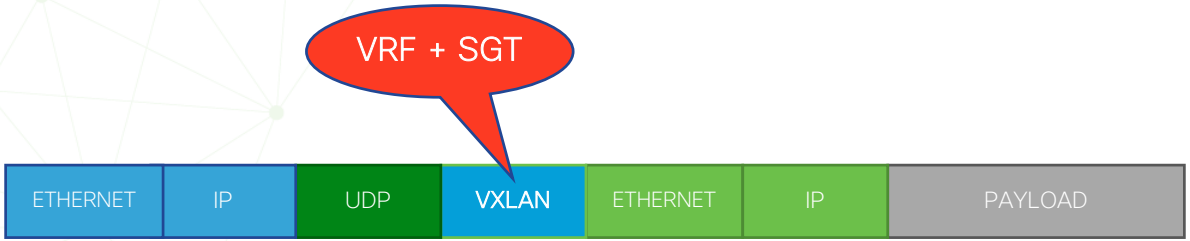
МАРШРУТИЗАТОРЫ | **КОММУТАТОРЫ** | **БЛВС КОНТРОЛЛЕРЫ** | **ТОЧКИ ДОСТУПА**

SD Access – ISE/DNAC применение политики



Что уникального в SD Access (Кампусной фабрике)?

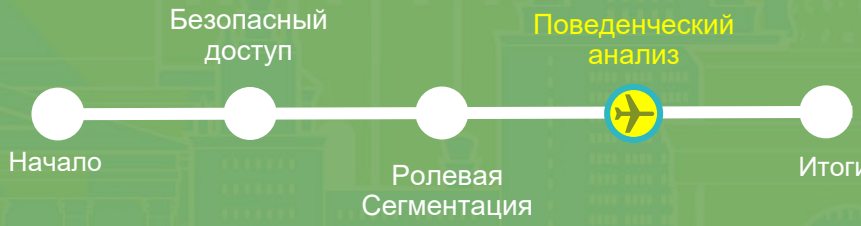
1. **Основанный на LISP Control-Plane**
2. **Основанный на VXLAN Data-Plane**
3. **Интегрированный SGT/SGACL**



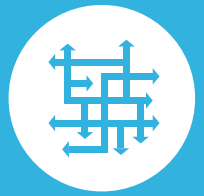
Virtual Routing & Forwarding

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)

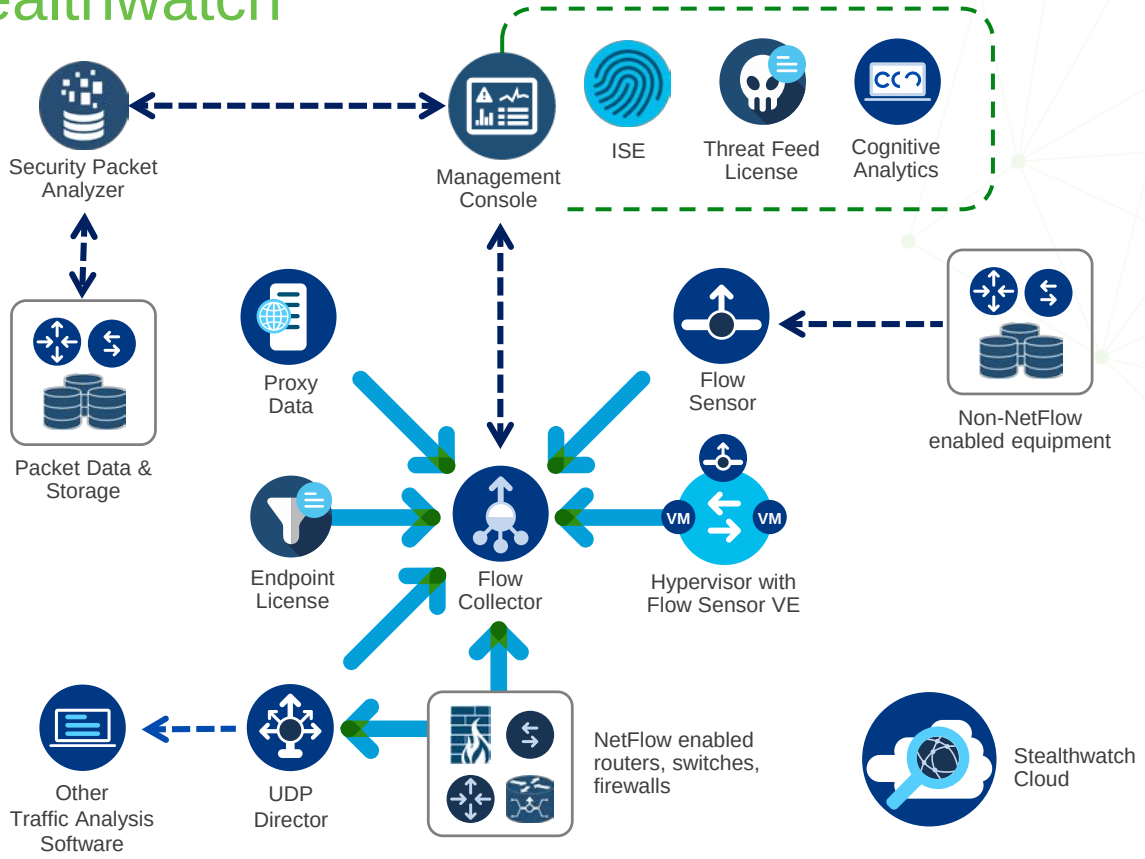
Лучше понимание возможности реагирования на IOC

Записи всех коммуникаций хост-хост

cisco

Система Cisco Stealthwatch

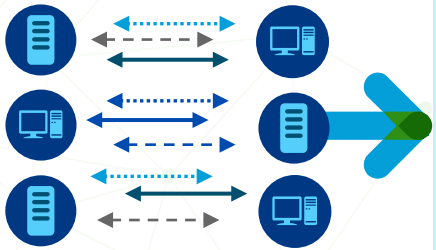
Комплексная **безопасность** и сетевой **мониторинг**



Модель поведенческого анализа и обнаружения аномалий

Поведенческие алгоритмы применяются для генерации “Событий безопасности”

Сбор и анализ Потоков



Потоки

События безопасности

Addr_Scan
..
Bad_Flag_ACK**
Beaconing Host
Bot Infected Host - Successful
Brute Force Login
Fake Application
Flow_Denied
..
ICMP Flood
..
Max Flows Initiated
Max Flows Served
..
Suspect Data Hoarding
Suspect Data Loss
Suspect Long Flow
..
UDP Received

Категории тревог

- Concern
- Recon
- C&C
- Exploitation
- Data hoarding
- Exfiltration
- DDoS target

Реагирование

- Alarm table
- Host snapshot
- Email
- Syslog / SIEM
- Mitigation

cisco

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

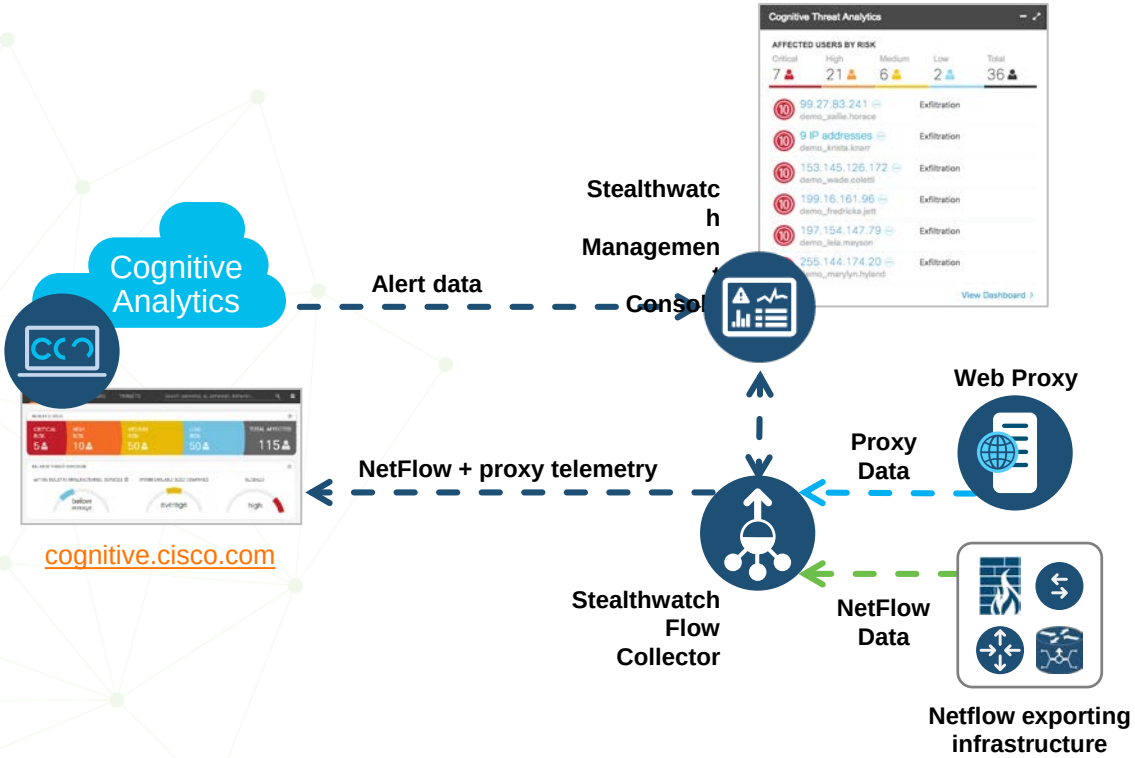
- Обнаружить угрозы, которые обошли текущие механизмы контроля
- Идентификация вывода данных, обнаружение command and control (C2) коммуникаций

Аналитика шифрованного трафика

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

cisco

Stealthwatch и Cognitive Analytics



Расширенная видимость и поведенческий анализ

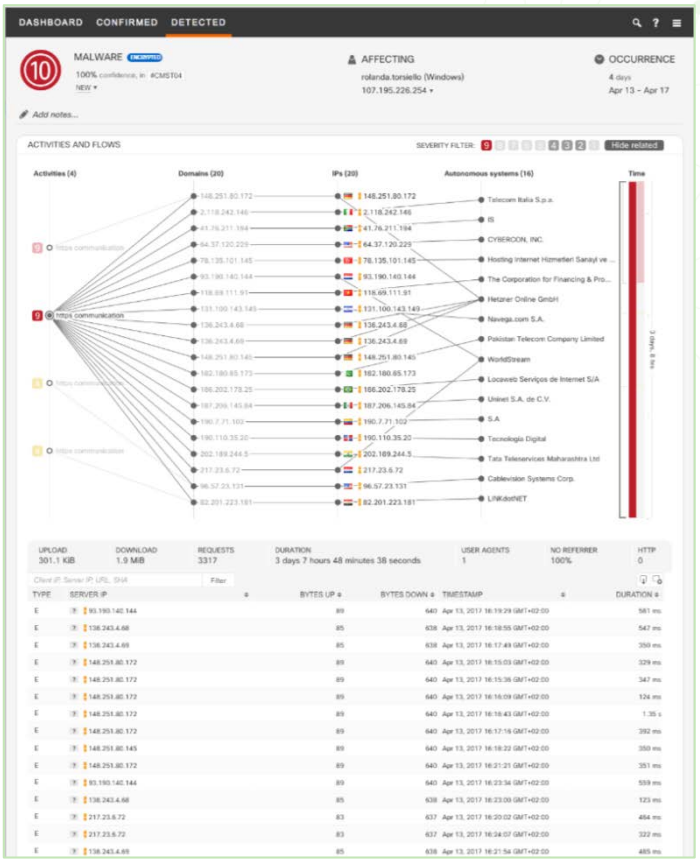
Продвинутое обнаружение угроз

Аналитика шифрованного трафика

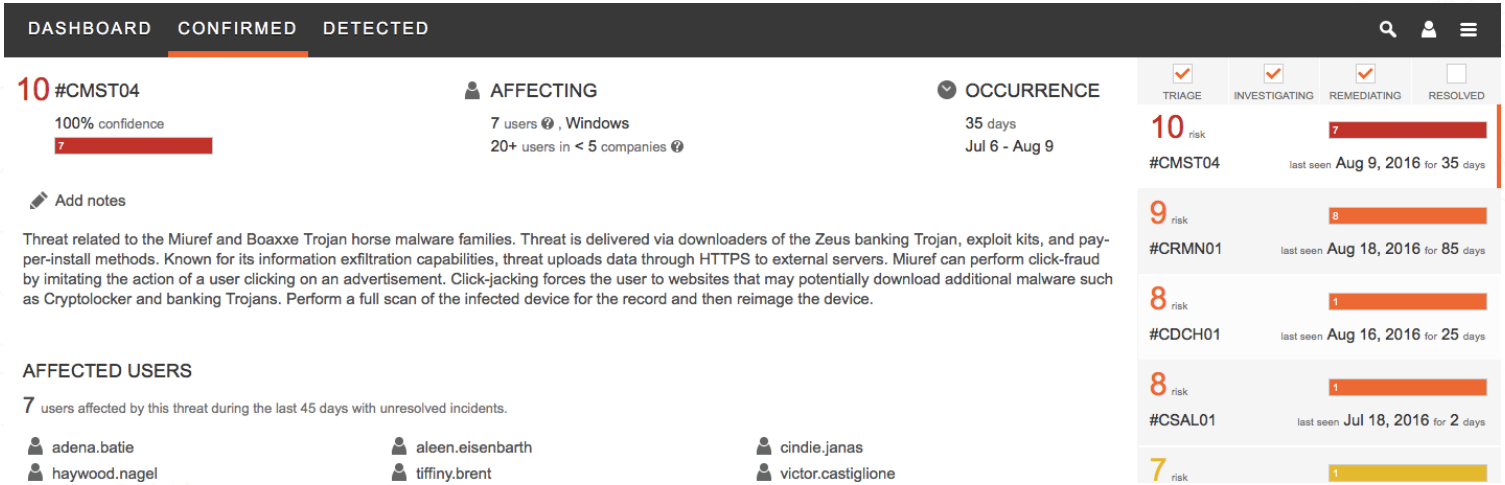
Мощь многоуровневого машинного обучения

Повысить точность определения используя лучшую в классе аналитику безопасности

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

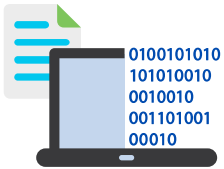
- /Users/Administrator/AppData/Local/Temp/KKOTHS51OX.exe
- /Users/Administrator/AppData/Local/Temp/a20Pm4SnPg/FnBxKdIO/Setup.exe
- /Users/Administrator/AppData/Local/Temp/QT4731FXGB.exe

+ 606 more paths

Encrypted Traffic Analytics

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

Вредоносы в шифрованном трафике



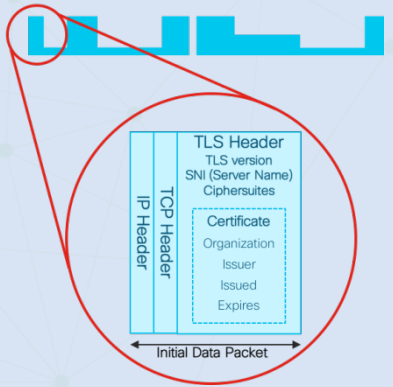
Криптографическое соответствие

cisco

Как мы можем инспектировать шифрованные данные?

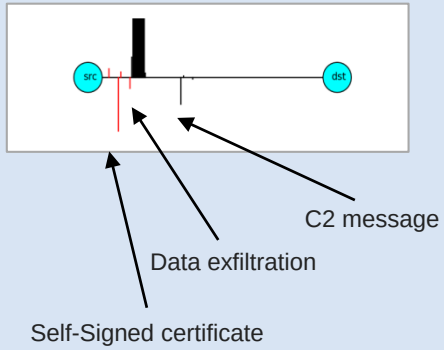
Первый пакет данных

Получите максимум от нешифрованных полей



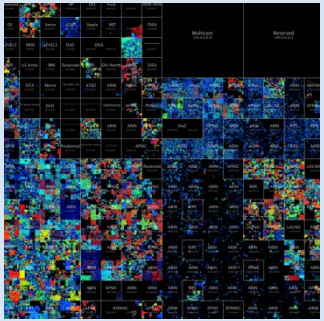
Последовательность длин пакетов и времен

Идентификация типа контента через размер и тайминг пакетов



Карта угроз

Кто есть кто на черной стороне Интернета



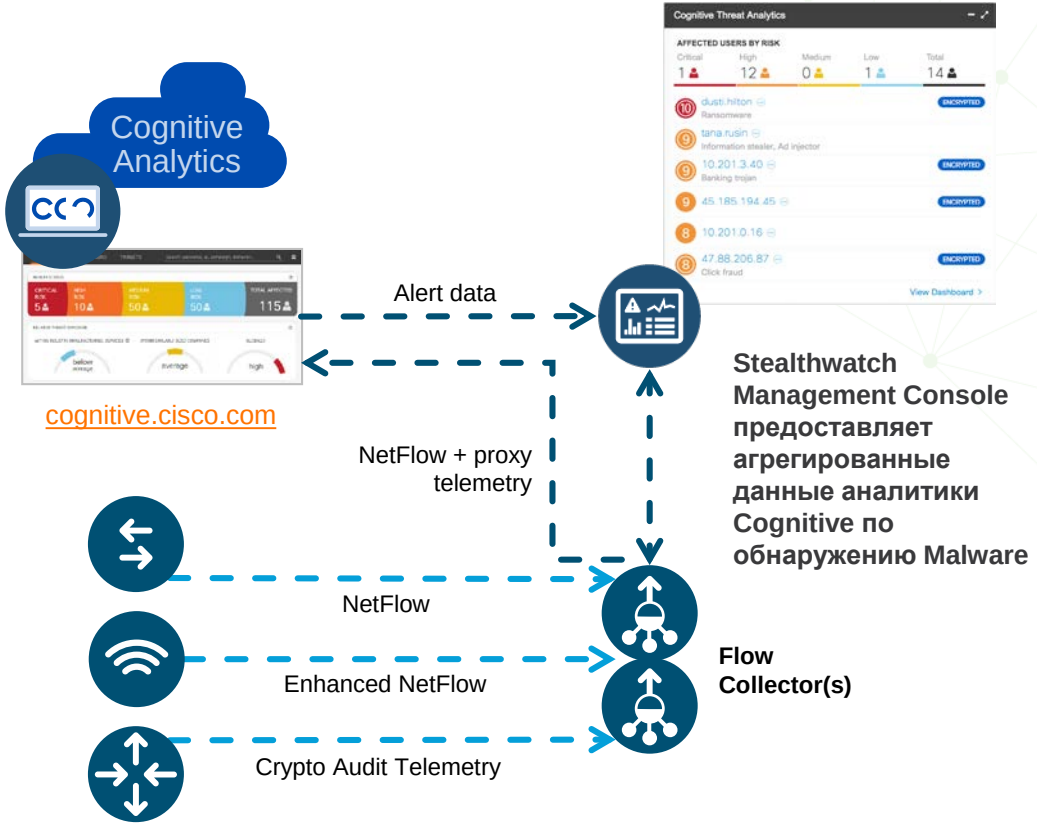
Широкая поведенческая база о серверах в Интернет

Encrypted Traffic Analytics

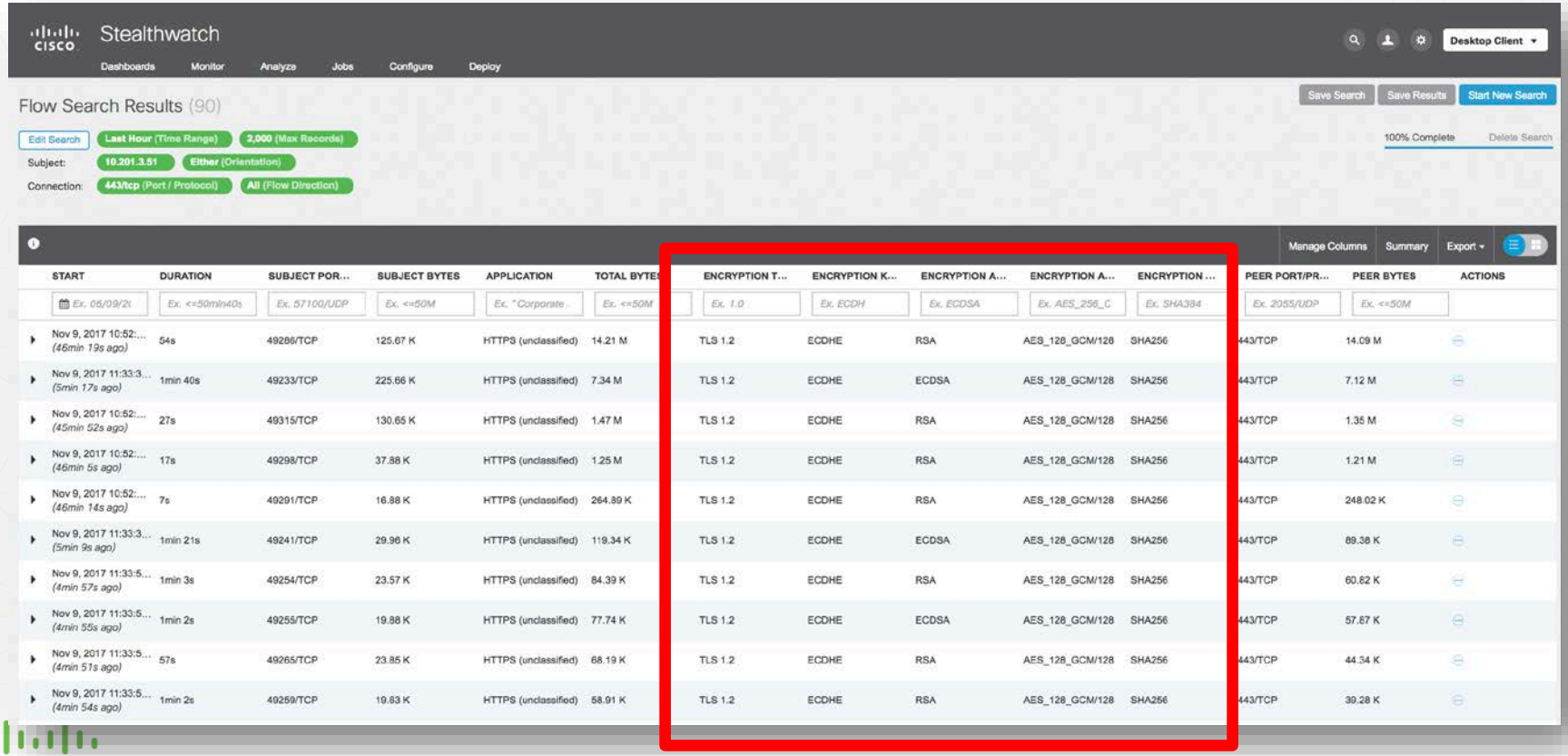
Корреляция знаний Глобальных-Локальных результатов с высокой точностью нахождения угроз

Stealthwatch улучшенная аналитика и машинное обучение уменьшает время расследования инцидентов

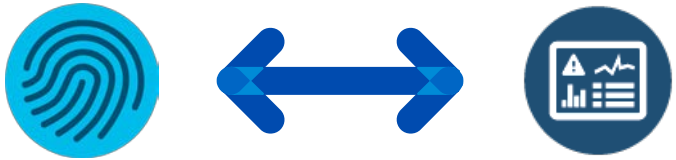
Улучшенный NetFlow с аналитикой шифрованного трафика от новейших коммутаторов и маршрутизаторов Cisco



Криптографическое соответствие требованиям



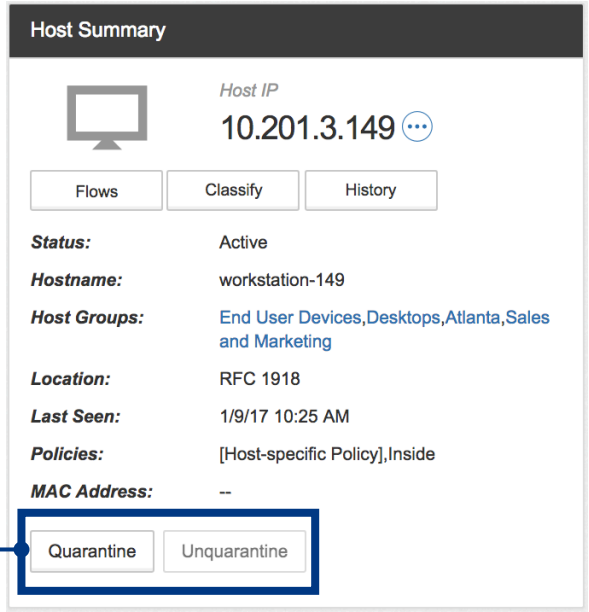
Rapid Threat Containment



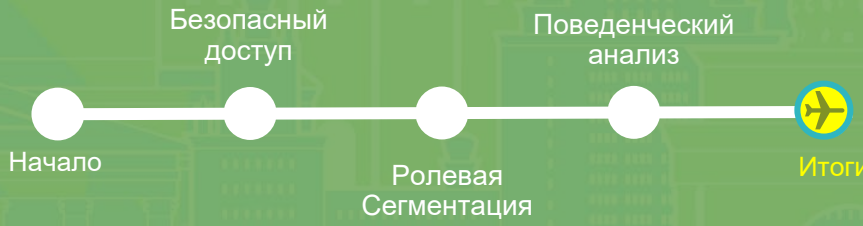
Cisco®
Identity Services Engine

Stealthwatch
Management Console

Постановка и снятие с карантина
через pxGrid



Заключение



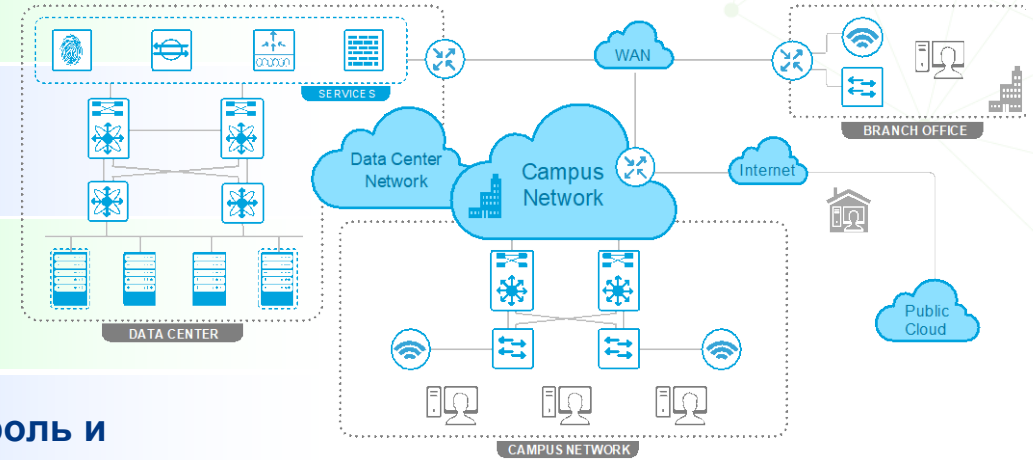
Digital Network Architecture для корпоративной безопасности

Видимость и контроль повсеместно

Интегрированная в сеть безопасность

Быстрая реакция на угрозы

Централизованная политика, контроль и отчетность



‘Инфраструктура’ для защиты ‘Информации’

cisco

Спасибо за внимание!