Архитектура обеспечения информационной безопасности. Подход Cisco.

Максим Порицкий

инженер по направлению Cisco, CCIE R&S

m.poritsky@elcoregroup.com

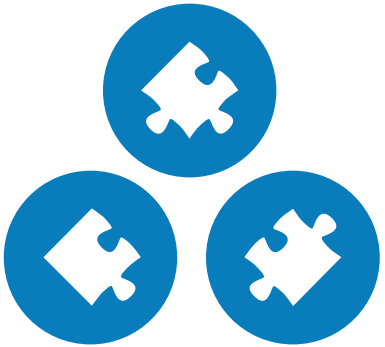
17.10.2017

Проблемы ИБ и задачи

Текущие проблемы ИБ

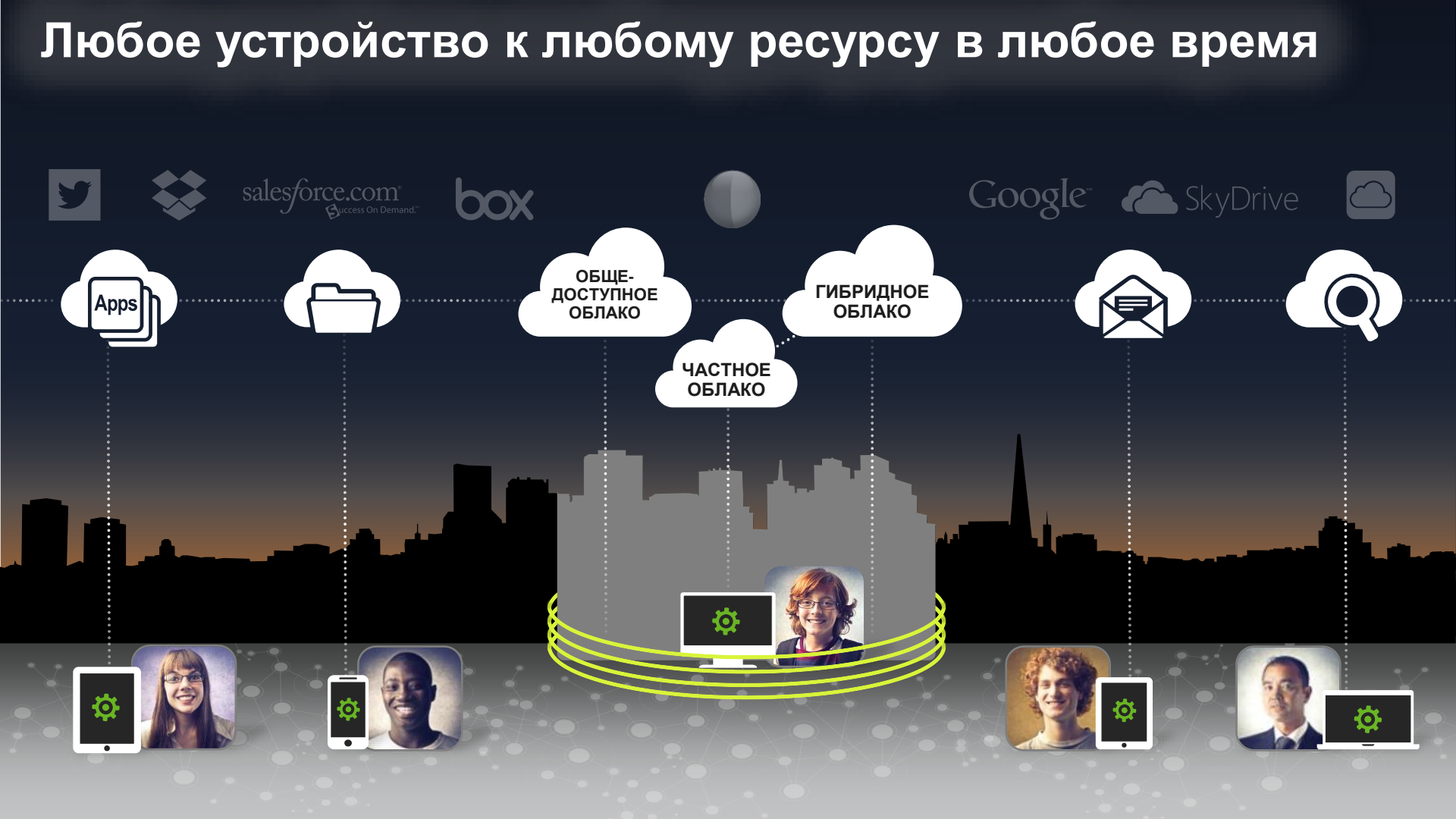
Изменение бизнес-моделей (размытость границ) и роста Интернет сервисов + IoT

Узкая специализированная направленность атак (на приложения, отрасли, компании)



Повышение сложности атак / защиты от них (из-за первых 2 проблем)

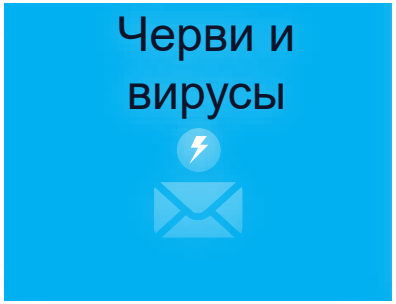
Любое устройство к любому ресурсу в любое время



Всеобъемлющий Интернет и множество IP-сервисов

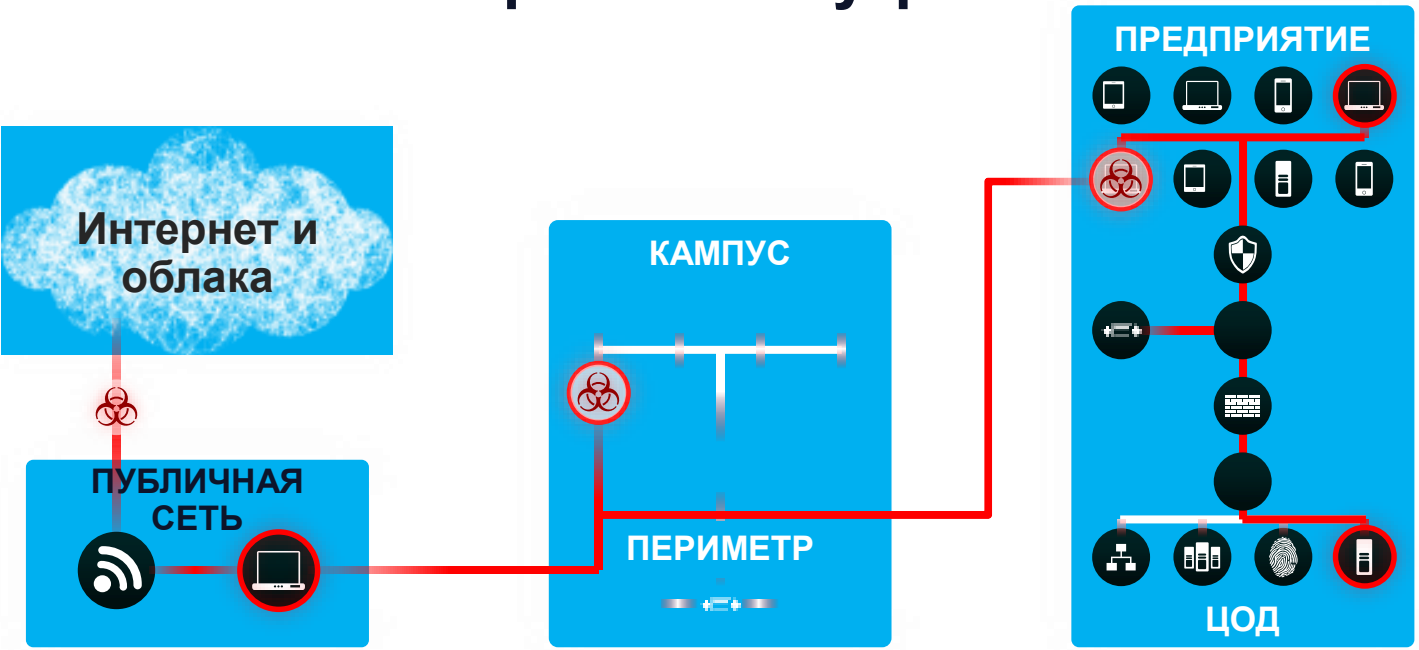
Эволюция угроз

Ответ предприятия	Антивирус (Host-Based)	IDS/IPS (Сетевой периметр)	Репутация (Global) и песочница	Сбор информации и аналитика (Облако)
Угрозы	Черви и вирусы	Шпионское ПО и руткиты	Специализированные угрозы и кибервойны DDOS	сейчас



ЭВОЛЮЦИЯ УГРОЗ

Анатомия современной угрозы



Заражение пользовательского устройства происходит за пределами предприятия

Продвинутые угрозы обходят средства защиты периметра

Угроза распространяется по сети и захватывает как можно больше данных

Периметр – web/email, firewall

1. Untrusted network → our network

2. Старые средства Sec

3. Плохая настройка

4. Уязвимости в hard/soft

5. Нет многоуровневой Sec

Подход Cisco к ИБ

На чем базируется подход Cisco по построению ИБ?

Видимость всего и вся

Интеграция в сеть, широкая база сенсоров, контекст и автоматизация

Фокус на угрозы

Непрерывная защита от угроз, облачное исследование угроз

Платформы

Гибкие и открытые платформы, масштабируемость, всесторонний контроль, управление

Сеть

Оконечные устройства

Мобильные устройства

Виртуальные устройства

Облака

Новая модель ИБ
методологический подход Cisco

Защита широкого диапазона вектора атак

Непрерывность защиты

Портфель решений Cisco

Cisco Talos

5 департаментов

90 МЛРД

DNS-запросов в день

18.5 МЛРД / 1,5 МЛН

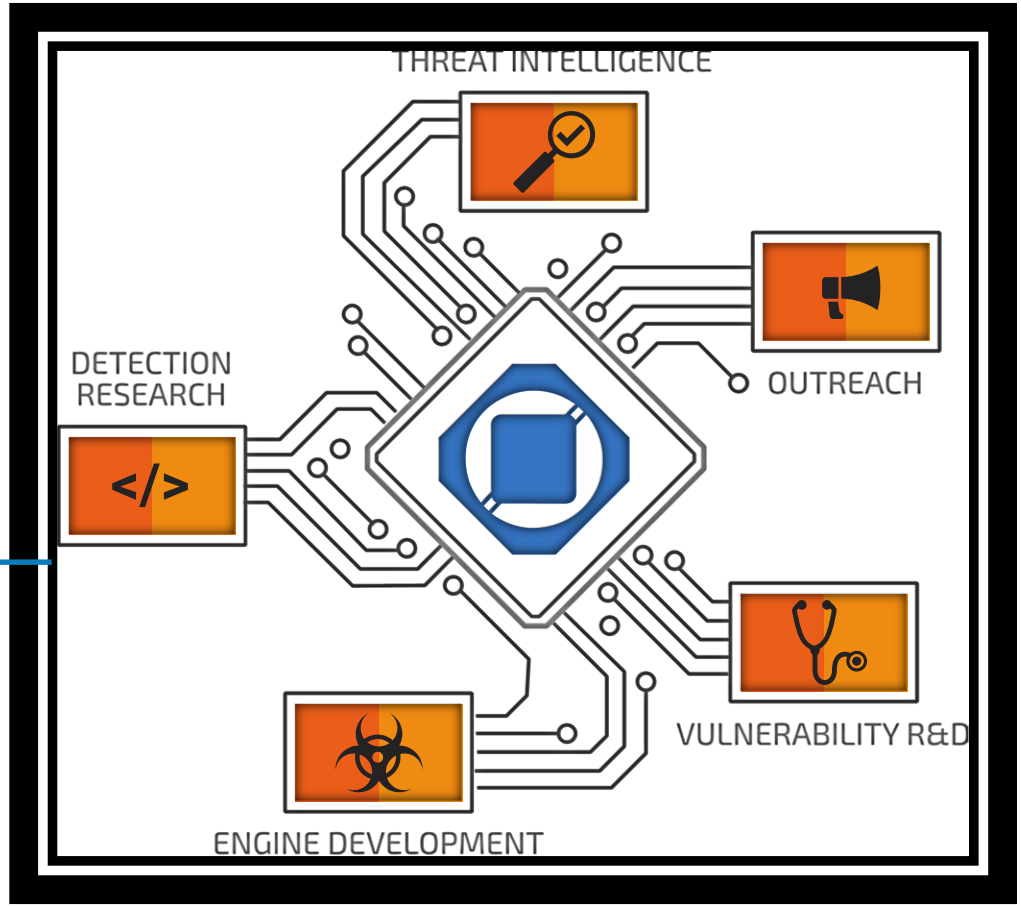
Файлов / семплов в день

16 МЛРД

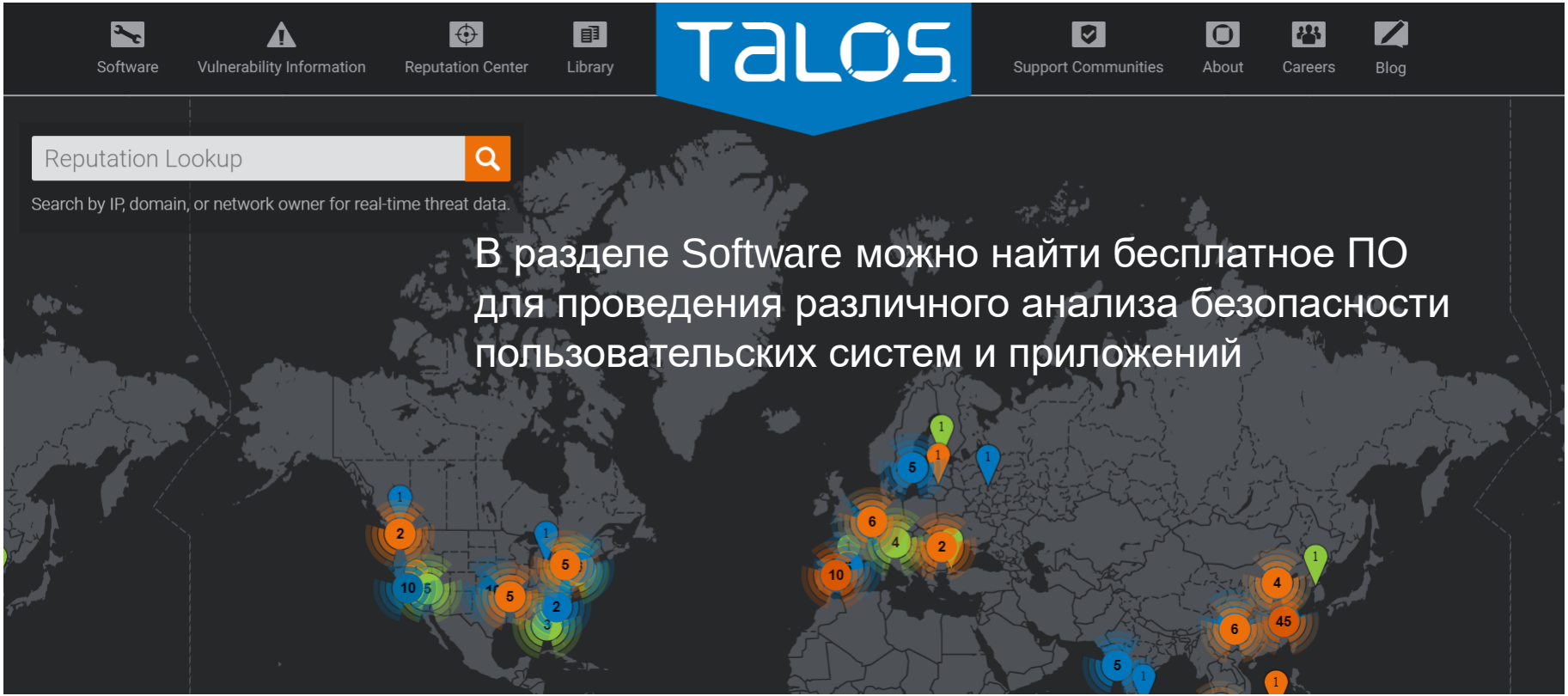
Web-запросов в день

600 МЛРД

сообщений email в день



Cisco Talos



https://www.talosintelligence.com/

“Продукты” Cisco Talos

Разведка

ПК

Сеть

Облака

Email

Web

Open Source

Услуги

ПРОДУКТЫ							
ThreatGrid	AMP ClamAV	FirePower/ASA ISR Meraki	CWS CES OpenDNS	ESA | ClamAV SpamCop SenderBase	WSA CWS	Snort Rules ClamAV Sigs ClamAV	ATA IR
СЕРВИСЫ ОБНАРУЖЕНИЯ							
Cloud & End Point IOCs	Cloud & End Point IOCs	Policy & Control	URL, Domain, IP Reputation	Email Reputation	URL, Domain, IP Reputation	Vulnerability Protection	Cloud & End Point IOCs
Malware Protection	Malware Protection	Malware Protection	Malware Protection	Malware Protection	Malware Protection	Malware Protection	Malware Protection
URL, Domain, IP Reputation	IP Reputation	URL, Domain, IP Reputation	AVC	URL, Domain, IP Reputation	AVC	Policy & Control	URL, Domain, IP Reputation
Network Protection		Vulnerability Protection		Phishing Protection			Vulnerability Protection
				Spoof & Spam Detection			Custom Protection

Внутренняя инфраструктура

Что сеть может сделать для вас?

Сеть как защитная стена (Network as Enforcer)

Сегментировать сеть надлежащим образом

TrustSec - Secure Group Tagging, VRF, ISE и многое другое

Шифровать трафик для защиты данных в процессе передачи

MACsec (провод), DTLS (беспроводная сеть), IPSec/SSL for WAN и многое другое

Защитить филиалы при прямом доступе в Интернет

IWAN, Cloud Web Security, OpenDNS и многое другое

Что сеть может сделать для вас?
Сеть как защитная стена (Network as Enforcer)

Сеть как защитная стена

Сегментируйте сеть и контролируйте доступ

Сегментация сети

для локализации атак

Ролевой контроль доступа на базе топологии, способа доступа (TrustSec/SGT, ISE)

Сегментация сети (VLAN, TrustSec/SGT, VRF/EVN)

Контроль доступа

для выполнения политик

Контроль доступа пользователей на базе устройства, местоположения, типа сети, времени и других параметров (ISE)

Физические и виртуальные разрешения и запреты (Access Control Lists)

Единая политика для проводного/беспроводного/удаленного доступа (ISE, Unified Access Switches)

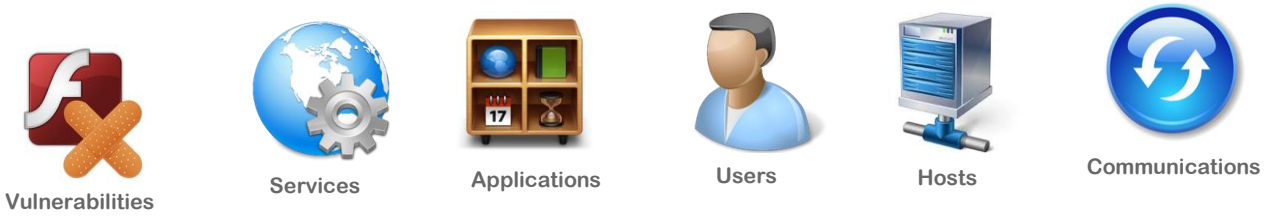
Межсетевые экраны ASA и Firepower

Межсетевые экраны с сервисами безопасности

- Самый популярный межсетевой экран ASA корпоративного класса с функцией контроля состояния соединений + NGFW
- Система гранулярного мониторинга и контроля приложений (Cisco AVC)
- Ведущая в отрасли система предотвращения вторжений следующего поколения (NGIPS) с технологией FirePOWER
- Фильтрация URL-адресов на основе репутации и классификации
- Система Advanced Malware Protection с функциями ретроспективной защиты
- VPN (s2s IPSEC, remote IPSEC/SSL)

Лицензирование на базе подписки

Важность контекста
Понимание своей инфраструктуры



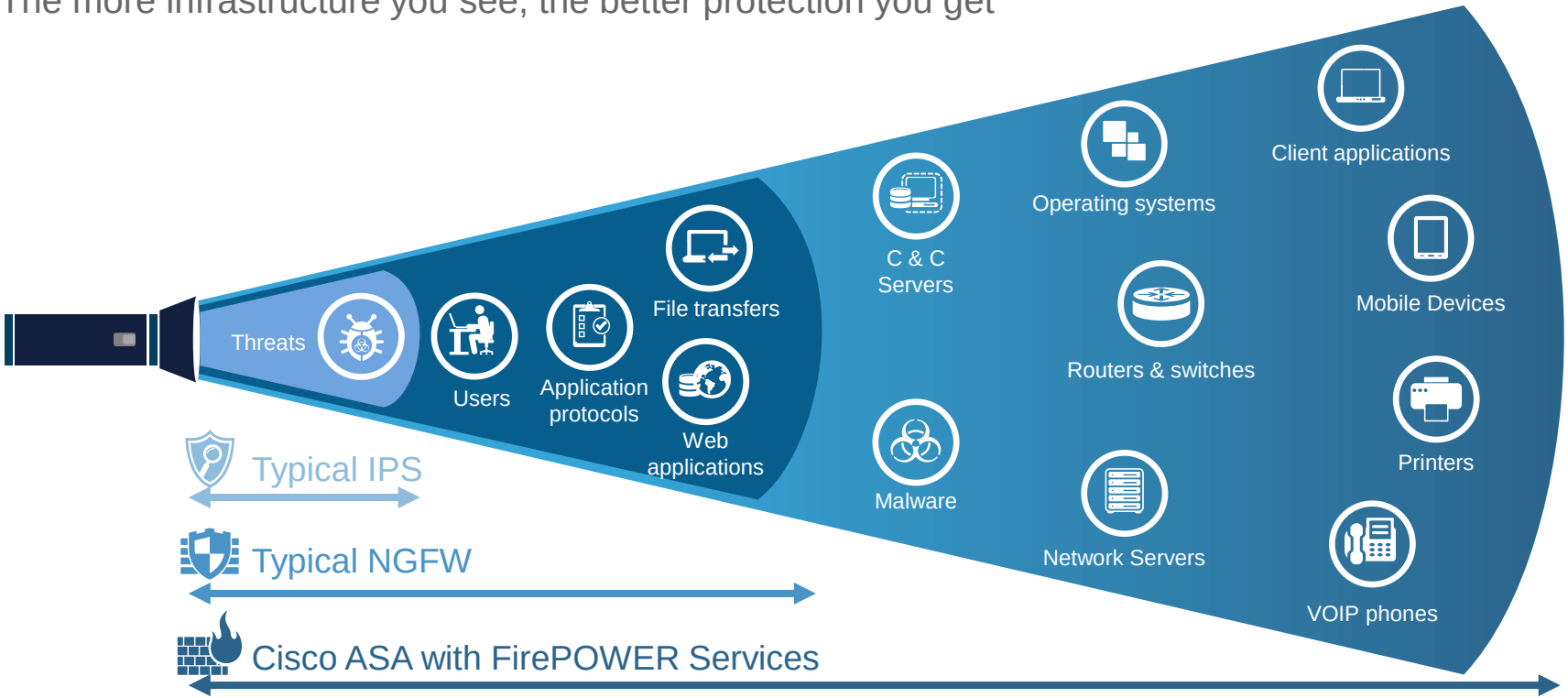
Сенсоры - **ASA**
Пассивное обнаружение

FireSIGHT -
система осведомления,
в режиме реального времени,
информации об инфраструктуре

- The FireSIGHT использует функционал **network discovery** для мониторинга сетевого трафика и построения карты сети
- Управляемые устройства пассивно собирают информацию, распознавая типы узлов, ОС, ПО, открытые порты и т.д. и информируют об этом **FireSIGHT Management Center** (прежнее название — Defense Center)
- **User Agents** на Microsoft Active Directory пересылают информацию об LDAP аутентификации пользователей
- Информация по сбору может быть расширена за счет NetFlow, сканирования и др. методов

No other NGFW offers this level of visibility

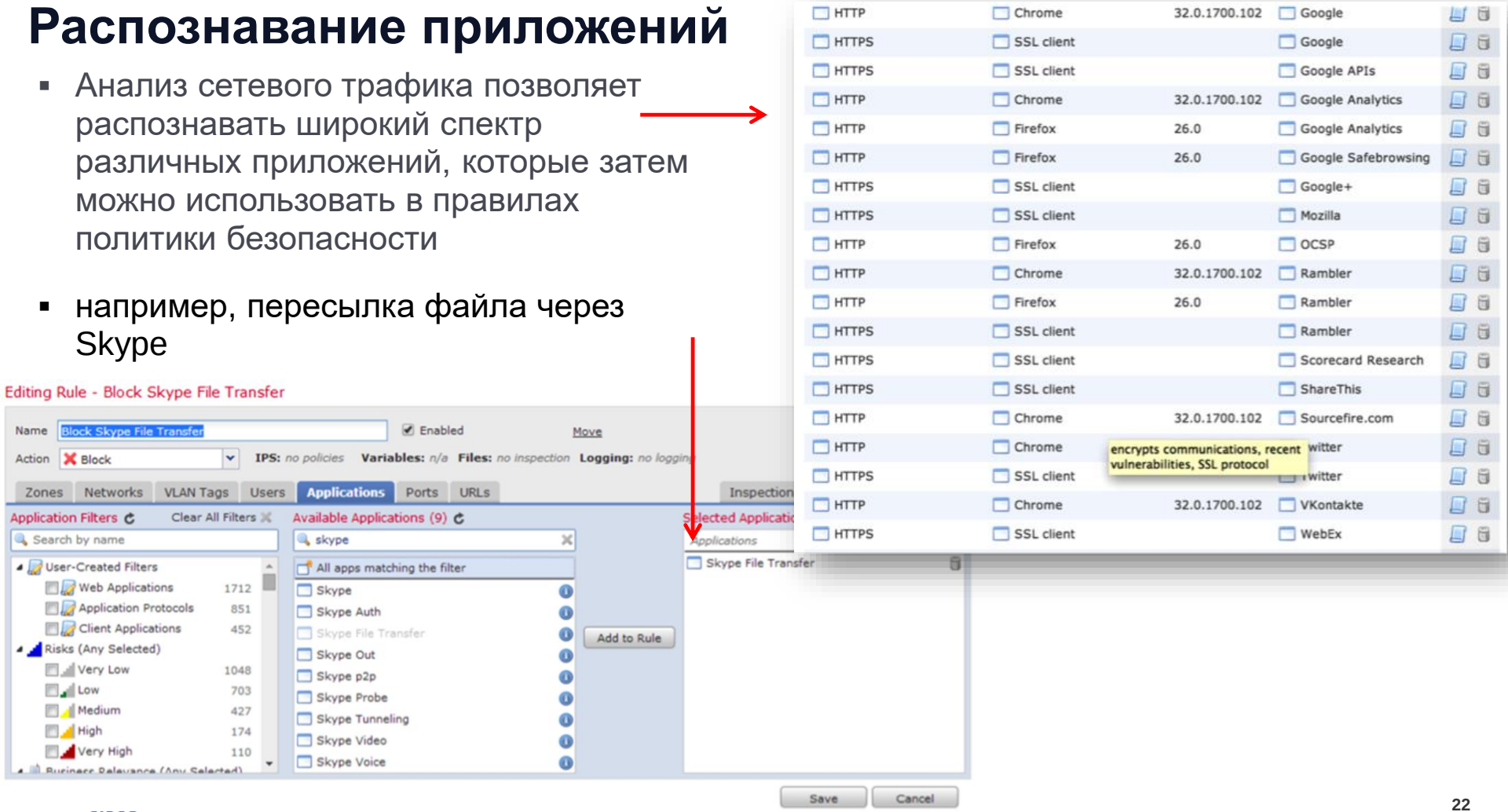
The more infrastructure you see, the better protection you get



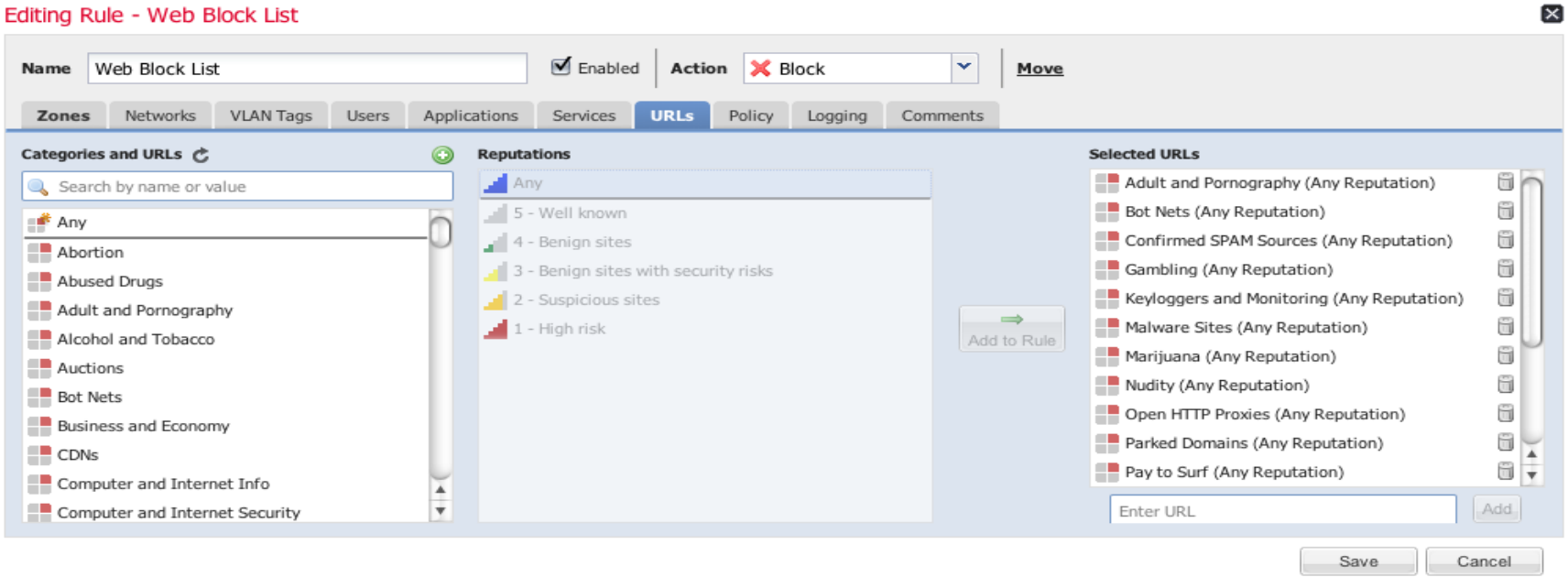
Распознавание приложений

- Анализ сетевого трафика позволяет распознавать широкий спектр различных приложений, которые затем можно использовать в правилах политики безопасности

- например, пересылка файла через Skype



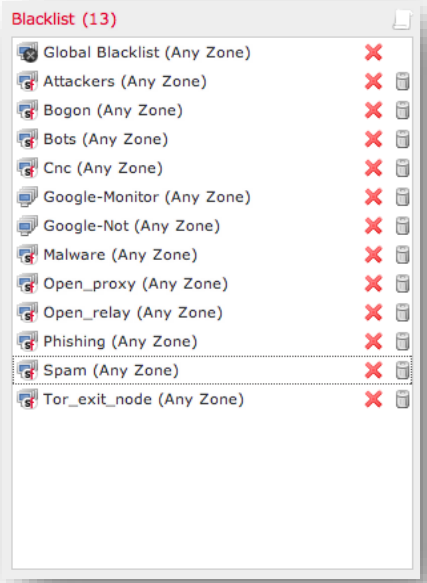
Фильтрация URL

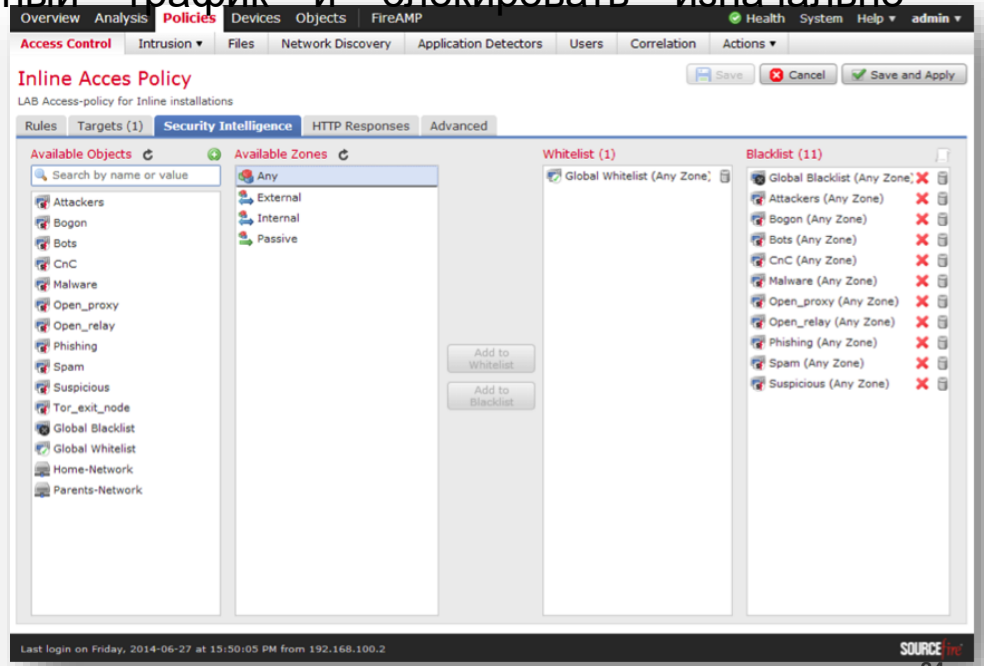


- Фильтрация URL-адресов по репутации и категориям обеспечивает комплексное оповещение и контроль над подозрительным веб-трафиком, а также применение политик для сотен миллионов URL-адресов в более чем 80 категориях

Политики фильтрации – “черные списки”

- можно назначить политику фильтрации Security Intelligence - постоянно обновляемые списки IP адресов спаммеров, центров ботнетов, открытых proxy и т.д.
- выбирать из имеющихся списков, либо загрузить свои собственные списки фильтрации из файла, либо указать системе URL, откуда эти списки забирать
- позволяет не обрабатывать доверенный трафик и блокировать изначально вредоносный

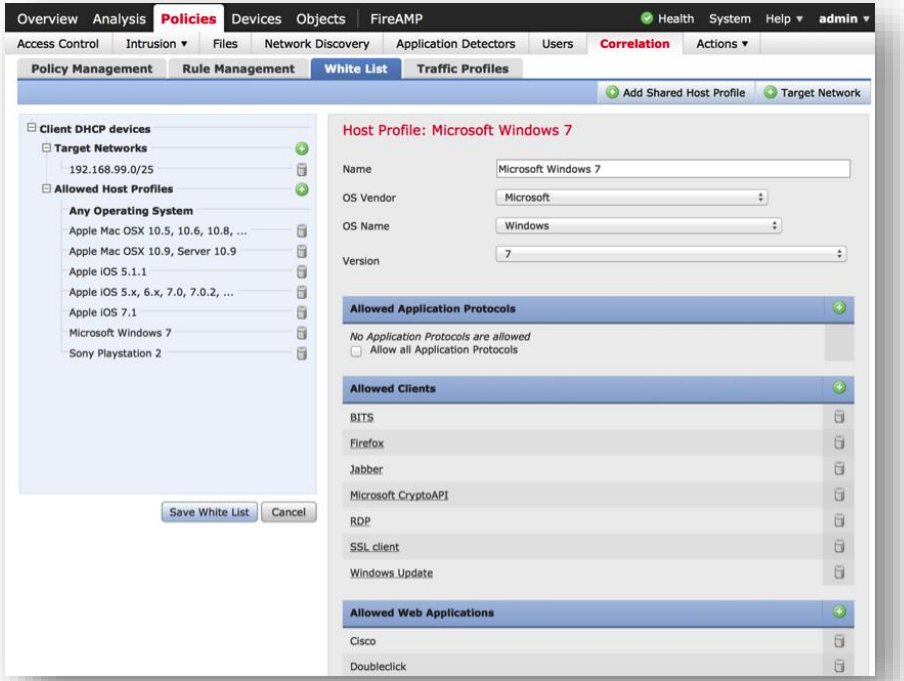




Compliance Whitelist

Создание «белых списков» / «списков соответствия»

- Формирование профиля Compliance
- Разрешенные типы и версии ОС
- Разрешенные клиентские приложения
- Разрешенные Web-приложения
- Разрешенные протоколы транспортного и сетевого уровней
- Разрешенные адреса / диапазоны адресов

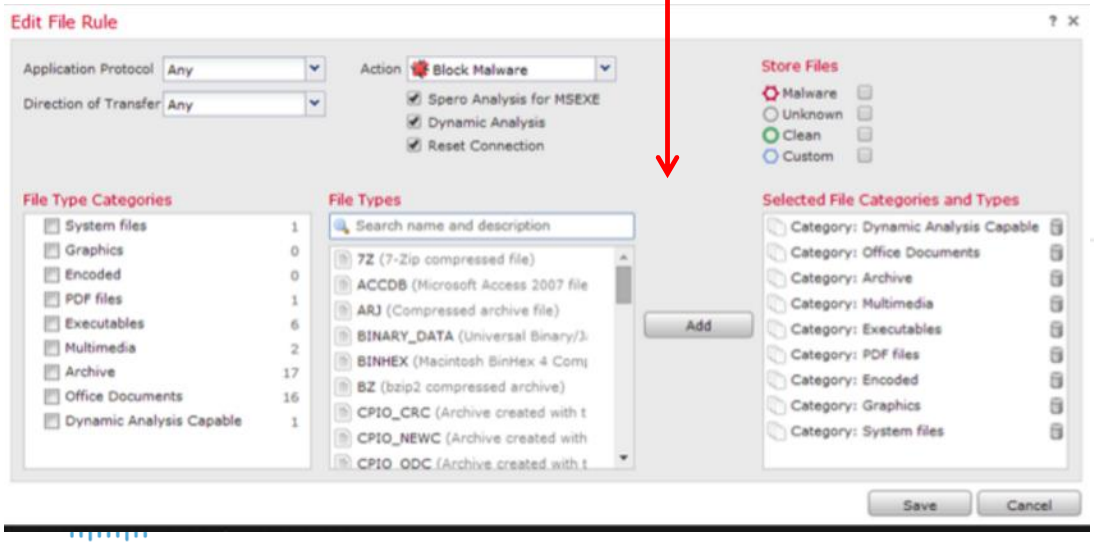


Обнаружение вредоносного кода с помощью AMP

Система анализирует проходящие через устройство файлы указанных в файловой политике форматах и передаваемых посредством указанных типов протоколов

Снимает хэш SHA-256 с файла и отправляет на анализ (облако или on-premises)

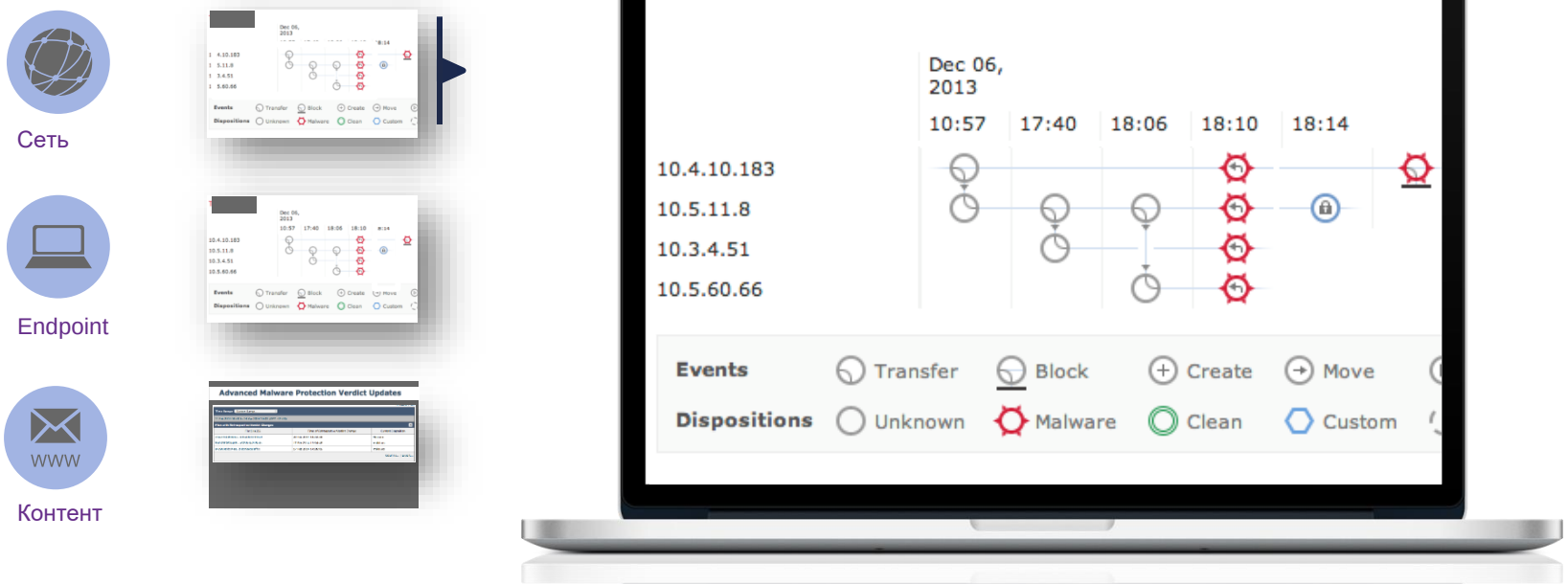
Или в облачную “песочницу” → анализ поведения



Обнаружение вредоносного кода с помощью AMP

- Усовершенствованная система защиты от вредоносного ПО обеспечивает высокую эффективность обнаружения вторжений, низкую стоимость владения и оптимальный уровень защиты, позволяя быстро выявлять, анализировать и предотвращать распространение вредоносного ПО и возникающих угроз, которые могут быть пропущены на других уровнях защиты

Анализ траектории движения вредоносных программ



Сетевая платформа использует индикаторы компрометации, анализ файлов и траекторию движения файла для того, чтобы показать, как вредоносный файл перемещается по сети, откуда он появился, что стало причиной его появления и кто еще пострадал от него

Платформы Cisco NGFW

ASA Cluster 2-16x

Firepower 9300

Firepower 4100

Firepower 2100

ASA 5516-X

ASA 5508-X

ASA 5545-X

ASA 5506-X

ASA 5555-X

ASA 5525-X

NGFWv
(600Mbps NGIPS)

NGIPSv
(600Mbps NGIPS)

SMB/Teleworker

Branch Office

Internet Edge + Campus

Data Center

https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw/datasheet-c78-736661.html

Платформы Cisco NGFW

Firepower Threat Defense для ASA 5500-X	Firepower серии 2100	Firepower серии 4100 и Firepower 9300
		
250 Мбит/с -> 1,75 Гбит/с (сервисы NGFW + IPS)	2 Гбит/с -> 8 Гбит/с (сервисы NGFW + IPS)	41xx = 10 Гбит/с -> 24 Гбит/с 93xx = 24 Гбит/с -> 53 Гбит/с

Все платформы NGFW управляются Firepower Management Center

Производительность Firepower

Features	Cisco Firepower Model											
	2110	2120	2130	2140	4110	4120	4140	4150	9300 with 1 SM-24 Module	9300 with 1 SM-36 Module	9300 with 1 SM-44 Module	9300 with 3 SM-44 Modules
Throughput FW + AVC (Cisco Firepower Threat Defense)[1]	2.0 Gbps	3 Gbps	4.75 Gbps	8.5 Gbps	12 Gbps	20 Gbps	25 Gbps	30 Gbps	30 Gbps	42 Gbps	54 Gbps	135 Gbps
Throughput: FW + AVC + NGIPS (Cisco Firepower Threat Defense)[1]	2.0 Gbps	3 Gbps	4.75 Gbps	8.5 Gbps	10 Gbps	15 Gbps	20 Gbps	24 Gbps	24 Gbps	34 Gbps	53 Gbps	133 Gbps

Simplify management with an easy, unified approach

Firepower Device Manager (FDM)

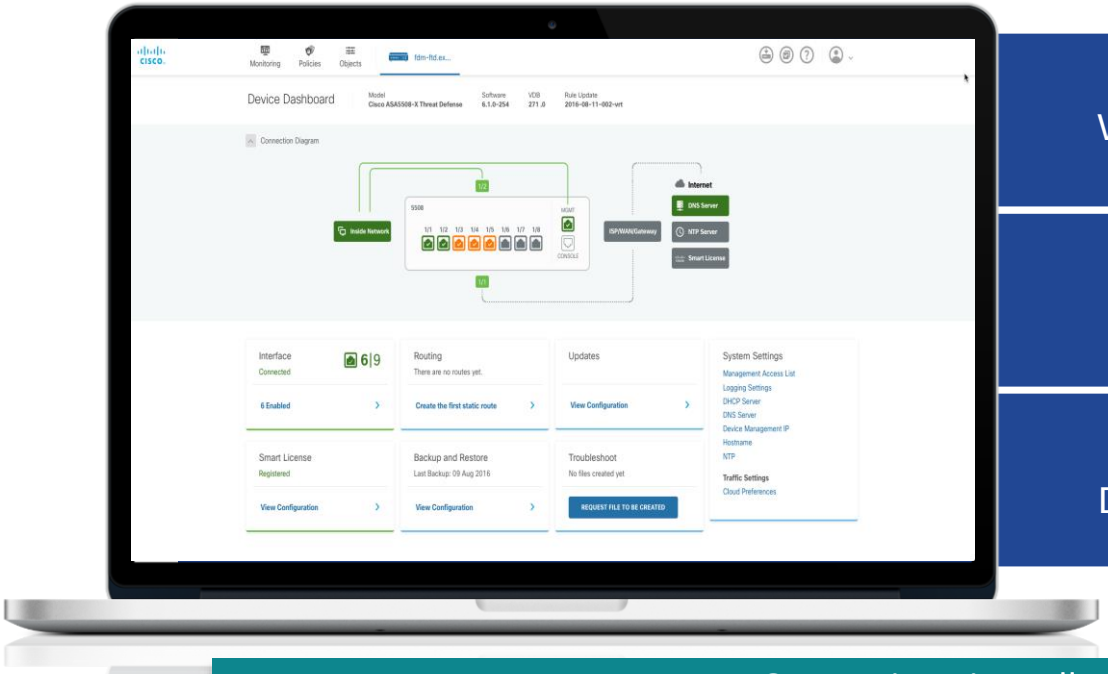
Enables easy on-box management of common security and policy tasks

Firepower Management Center (FMC)

Enables comprehensive security administration and automation of multiple appliances

Firepower Device Manager
Easily manage individual NGFWs

free local manager for managing single Firepower Threat Defense device



- Web-based OnBox Manager
- Simplified and better user experience
- Workflows, Diagrams and Default configuration options

Manages Next Generation Firewall software
On Cisco ASA 5500-FTD-X Models

FMC Platforms

Virtual (2-10-25)

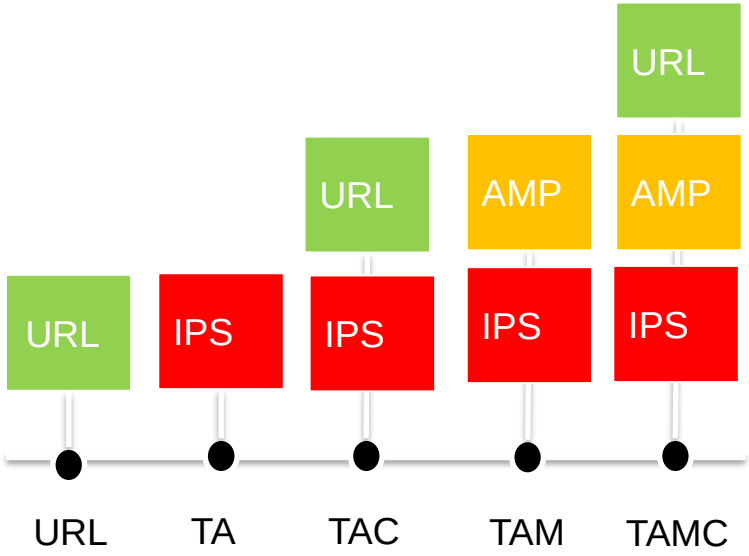
- Up to 25 sensors managed
  10 million maximum events
  250 GB event storage
  Network map up to 50K hosts, 50K users

FMC1000	FMC2500	FMC4500
• Up to 50 sensors managed • 60 million maximum events • 900 GB event storage • Network map up to 50K hosts, 50K users	• Up to 300 sensors managed • 60 million maximum events • 1.8 TB event storage • Network map up to 150K hosts, 150K users	• Up to 750 sensors managed • 300 million maximum events • 3.2 TB event storage • Network map up to 600K hosts, 600K users

https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html

Лицензирование

- FirePower-бандлы (K8, K9)
- 5 вариантов заказа функций безопасности
- Подписка на 1, 3, 5 (включая обновления)
- Функция AVC и NGFW включена по умолчанию
  - ✓ Постоянная лиц., поставляется вместе с устройством
  - ✓ Обновления AVC включены в SMARTnet
- Security Plus Lic (для ASA5506X) – HA, сессии, VLAN
- Security Context Lic (начиная с ASA5508X)
- Promo-подписки (-PR)



Cisco Identity Services Engine (ISE)

Что такое Cisco ISE (Cisco Identity Services Engine) ?

Cisco ISE

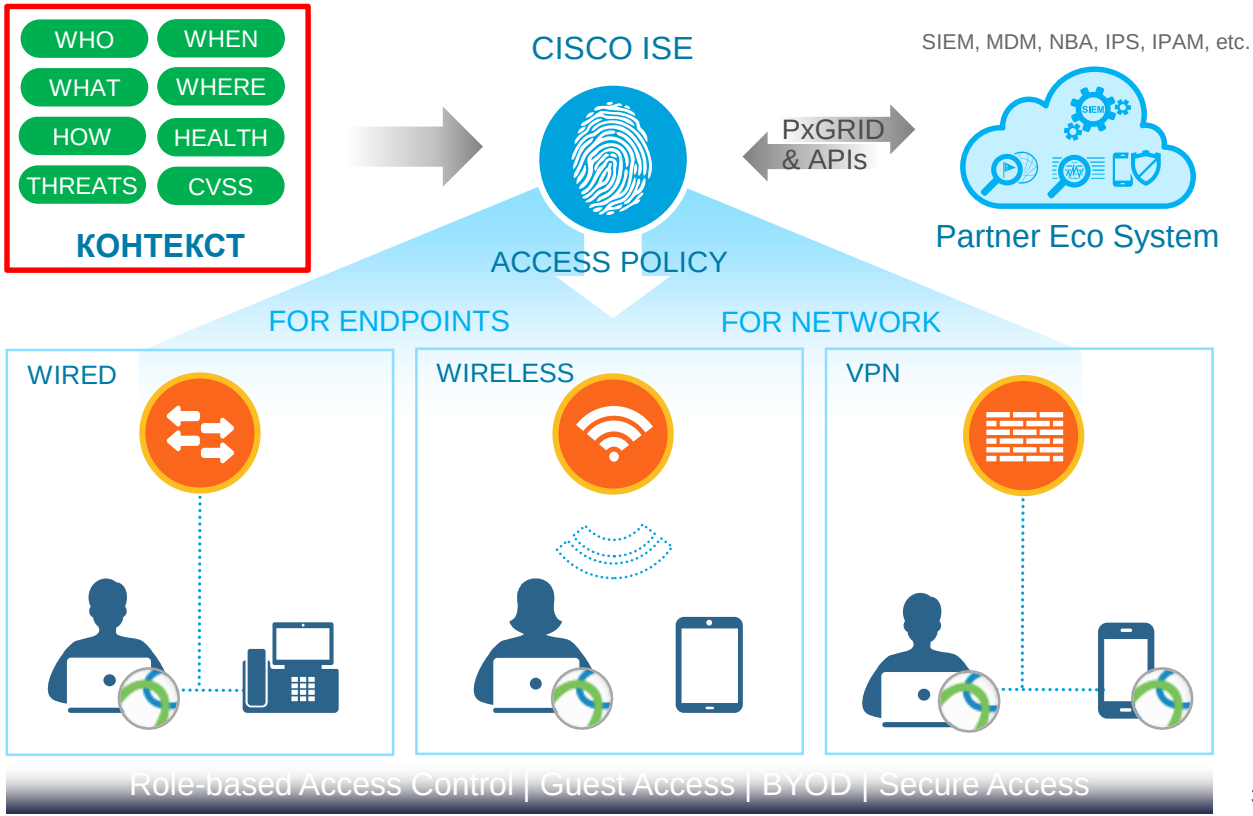
Context aware policy service, to control access and threat across wired, wireless and VPN networks

Cisco Anyconnect

Supplicant for wired, wireless and VPN access.

Services include:

- Posture assessment
- Malware protection
- Web security
- MAC Security
- Network visibility and more



Why Customers Buy ISE

Asset Visibility	Cisco ISE can reach deep into the network to deliver superior visibility into who and what is accessing resources.
Access Control	Consistent access control in to wired, wireless and VPN Networks. 802.1X, MAB, Web Authentication and Easy Connect for admission control.
Guest Access	Fully customizable branded mobile and desktop guest portals, with dynamic visual workflows to easily manage guest user experience.
BYOD Access	Simplified BYOD management with built-in CA and 3rd party MDM integration for on boarding and self-service of personal mobile devices.
Segmentation	Topology independent Software-defined segmentation policy to contain network threats by using Cisco TrustSec technology.
Threat Control	Context sharing with partner eco-system to improve their overall efficacy and accelerate time to containment of network threats.
Device Admin	Cisco ISE supports device administration using the TACACS+ security protocol to control and audit the configuration of network devices.

How Does ISE Get All That Information ?
Cisco ISE Profiling

1.5 million

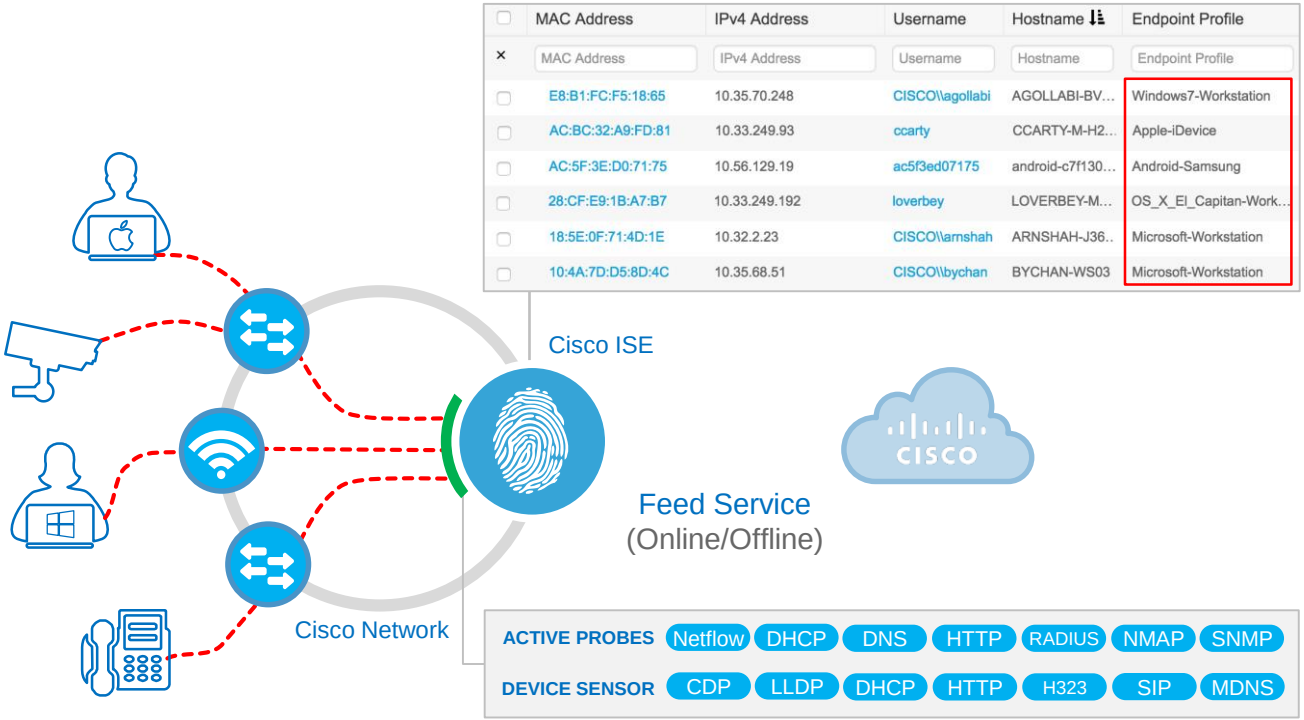
devices with ‘50’ attributes each can be stored

550+

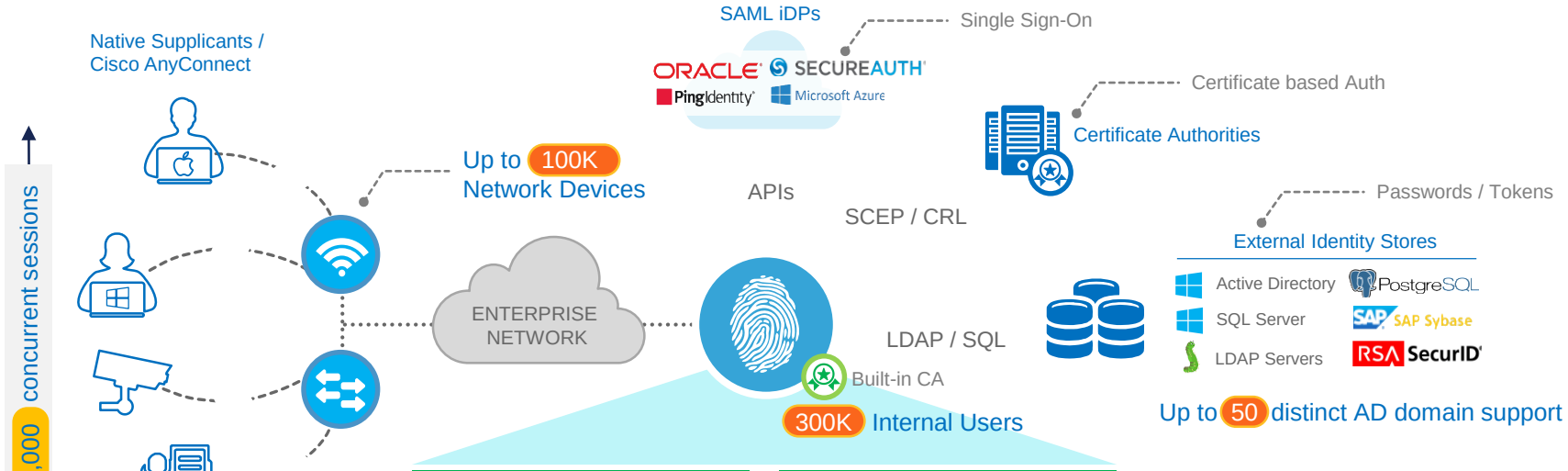
High-level canned profiles. +Periodic feeds

250+

Medical device profiles



Authentications and Authorizations



Authentication Methods

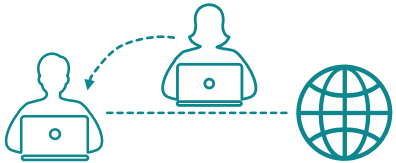
PASSIVE IDENTITY
- **MAC Authentication Bypass**
- **Easy Connect**

ACTIVE IDENTITY
- IEEE 802.1X
- Web Authentication
  - Central WebAuth
  - Local WebAuth

Authorization Options

- **Named ACL / Downloadable ACL (dACL)**
- **Dynamic VLAN Assignment**
- **Security Group Tags (SGT)**
- URL-Redirection (WebAuth, instruction, notification)
- Port Configuration (Auto Smartport macros или Interface Templates)

ISE Is Best for Guest

Hotspot	Self Sponsored	Sponsored Guest Access
		
Immediate, un-credentialed internet access	Self-registration by guests, Sponsors may approve access	Authorized sponsors create account and share credentials

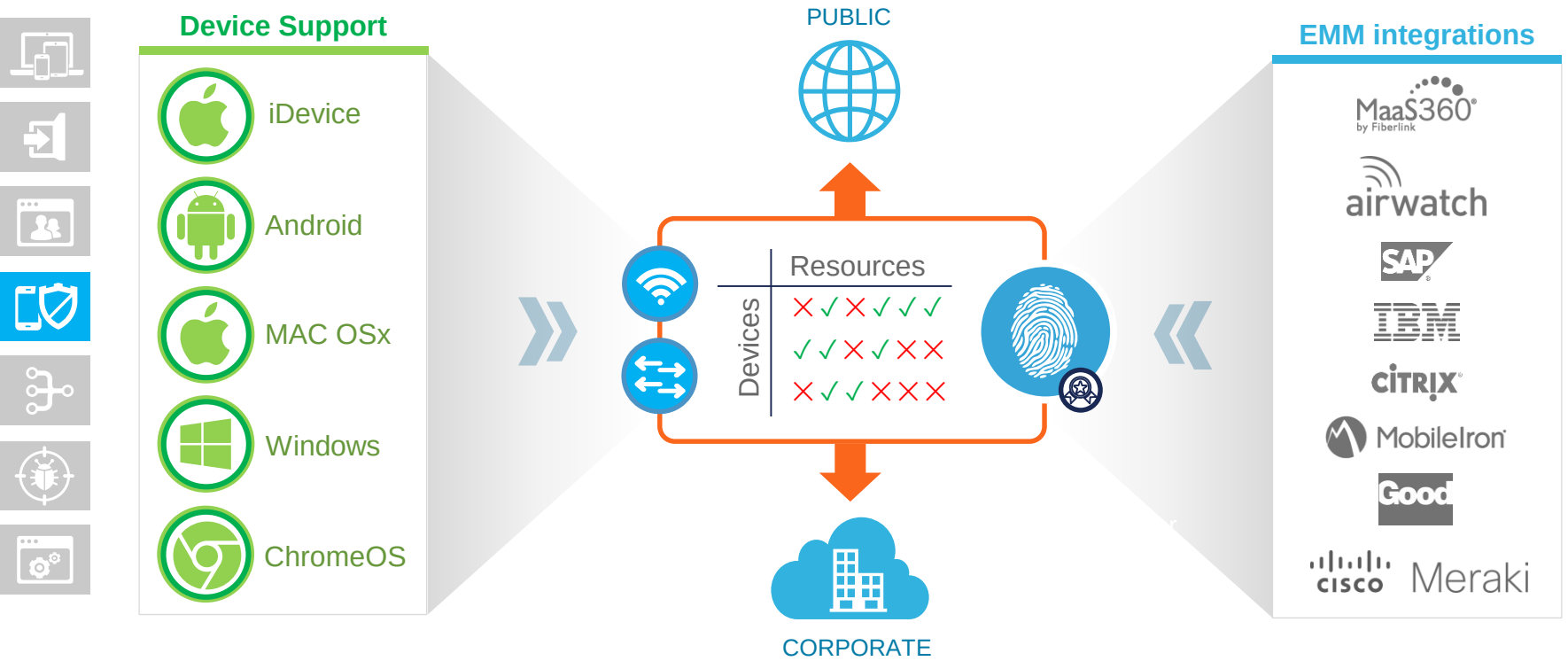
# of supported Guest accounts

Guest account notification options

Portal language customization

Manage guest accounts via REST

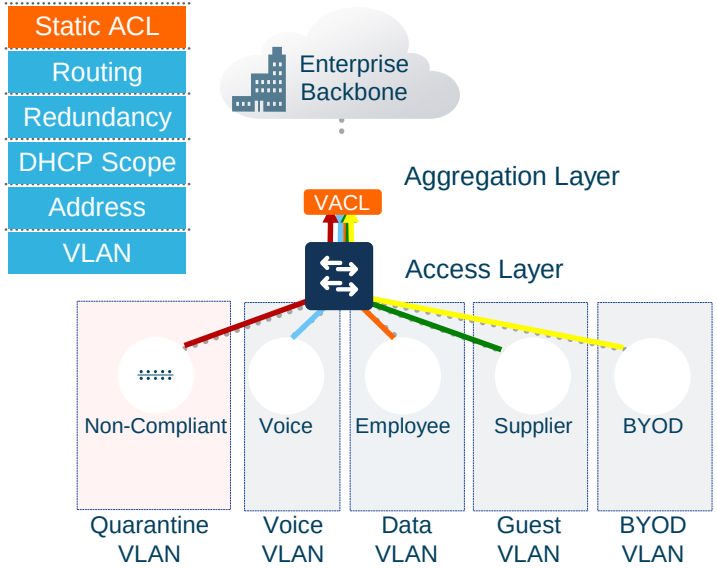
Bring Your Own Device



EMM: Enterprise Mobility Management | MDM: Mobile Device Management

ISE simplifies segmentation with TrustSec

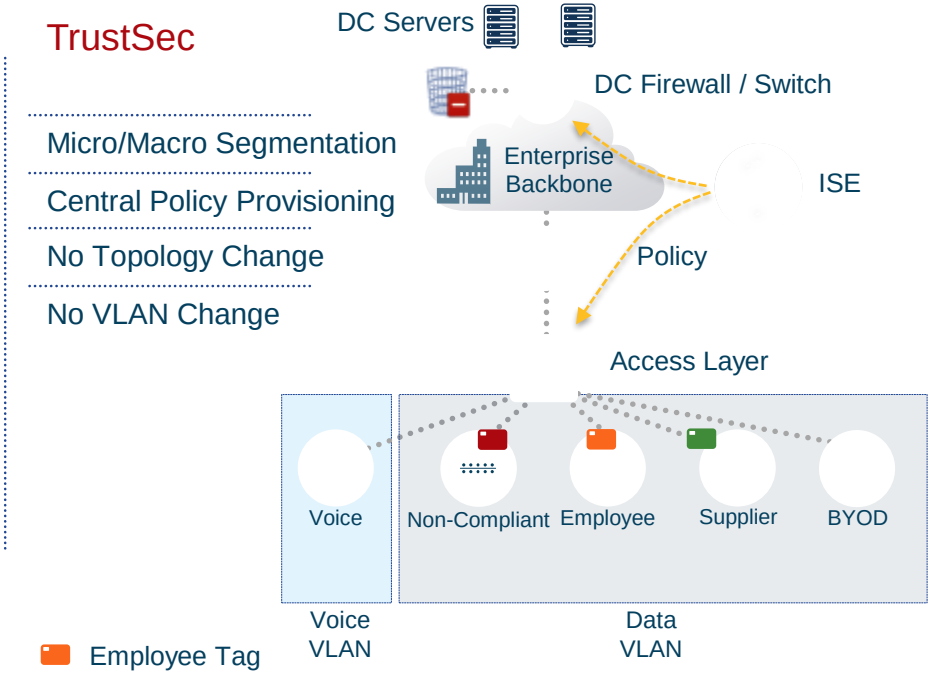
Traditional Segmentation



Security Policy based on Topology
High cost and complex maintenance

TrustSec

- Micro/Macro Segmentation
- Central Policy Provisioning
- No Topology Change
- No VLAN Change



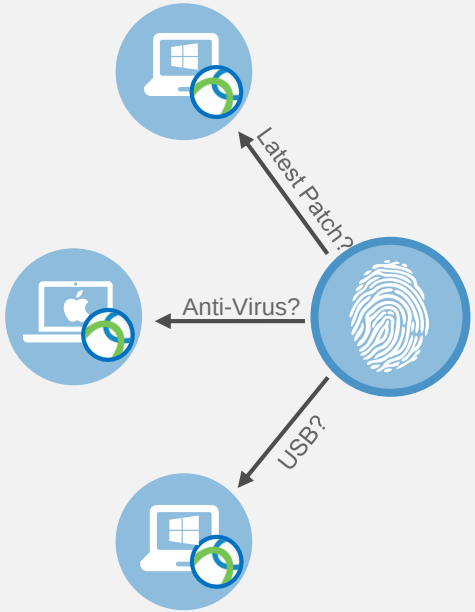
Use existing topology and automate security policy to reduce OpEx

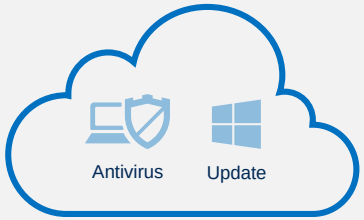
Always-on Policy Compliance

Posture defines the state of compliance with the company's security policy

Posture Flow

- **Authenticate User/Device**
  Posture: Unknown/Non-Compliant ?
- **Quarantine**
  Limited Access: VLAN/dACL/SGTs
- **Posture Assesment**
  Check Hotfix, AV, Pin lock, USB Device, etc.
- **Remediation**
  WSUS, Launch App, Scripts, MDM, etc.
- **Authorization Change**
  Full Access – VLAN/dACL/SGTs.





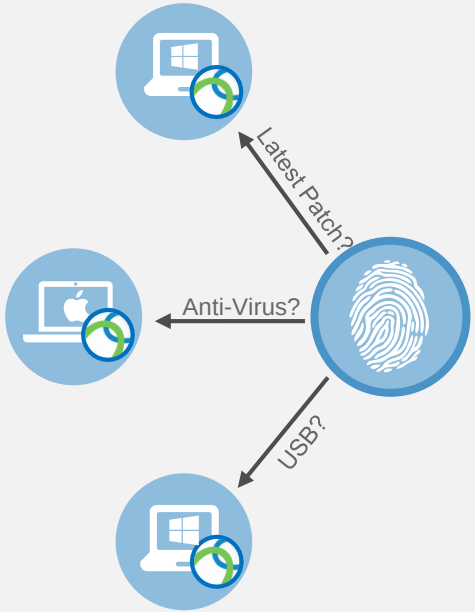
- Posture
  - Remediation Actions
    - Anti-Malware Condition
    - Anti-Spyware Condition
    - Anti-Virus Condition
    - File Remediations
    - Launch Program Remediations
    - Link Remediations
    - Patch Management Remediations
    - USB Remediations
    - Window Server Update Server
    - Windows Update Remediations

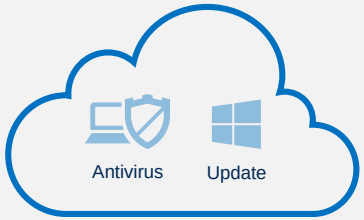
Always-on Policy Compliance

Posture defines the state of compliance with the company's security policy

Posture Flow

- **Authenticate User/Device**
  Posture: Unknown/Non-Compliant ?
- **Quarantine**
  Limited Access: VLAN/dACL/SGTs
- **Posture Assesment**
  Check Hotfix, AV, Pin lock, USB Device, etc.
- **Remediation**
  WSUS, Launch App, Scripts, MDM, etc.
- **Authorization Change**
  Full Access – VLAN/dACL/SGTs.





- Posture
  - Remediation Actions
    - Anti-Malware Condition
    - Anti-Spyware Condition
    - Anti-Virus Condition
    - File Remediations
    - Launch Program Remediations
    - Link Remediations
    - Patch Management Remediations
    - USB Remediations
    - Window Server Update Server
    - Windows Update Remediations

Cisco Annyconnect

Современные требования к системам удаленного подключения сотрудников

Однообразный доступ

Одинаковый функционал защиты
В любое время
Из любого места

Видимость контекста

“Видимость” пользовательского поведения и состояния устройства

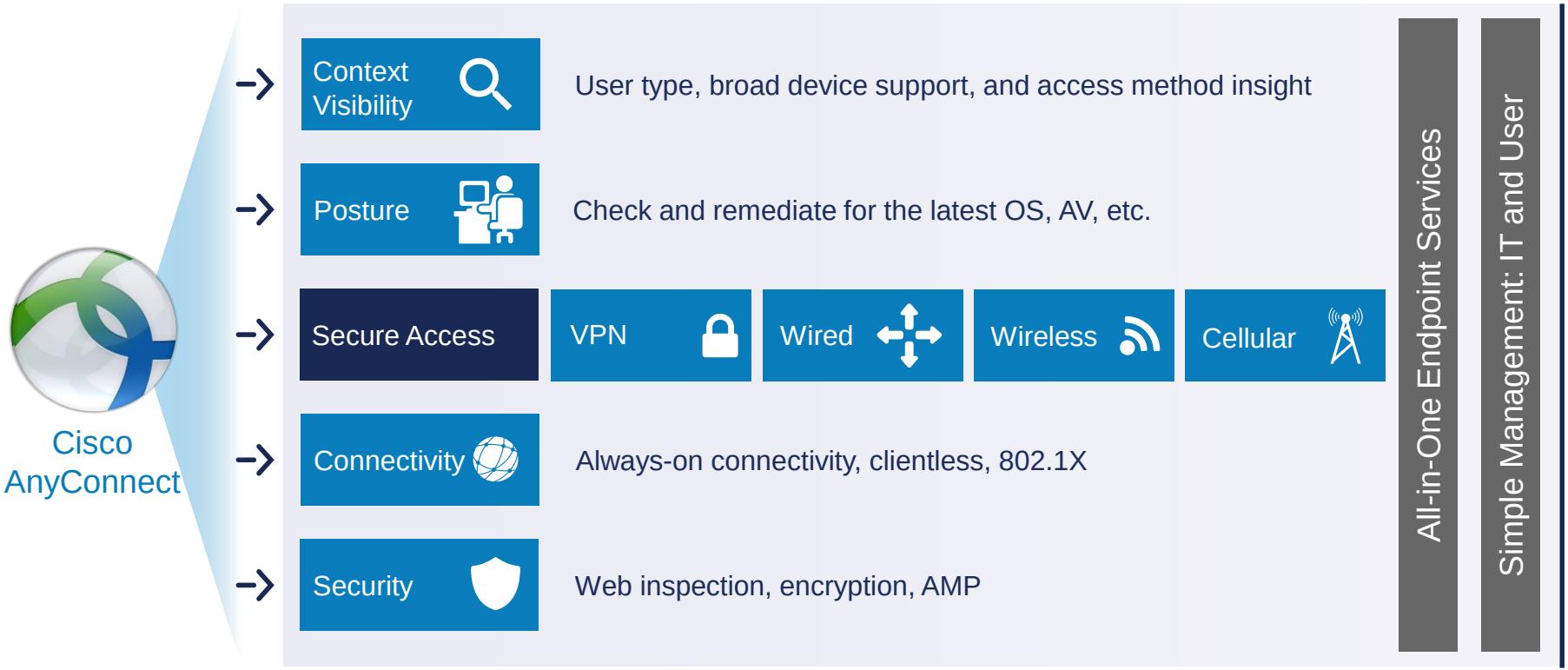
Удобство и компромисс

Компромисс между легкостью поддержки со стороны IT и разнообразными возможностями пользователя (user experiences)

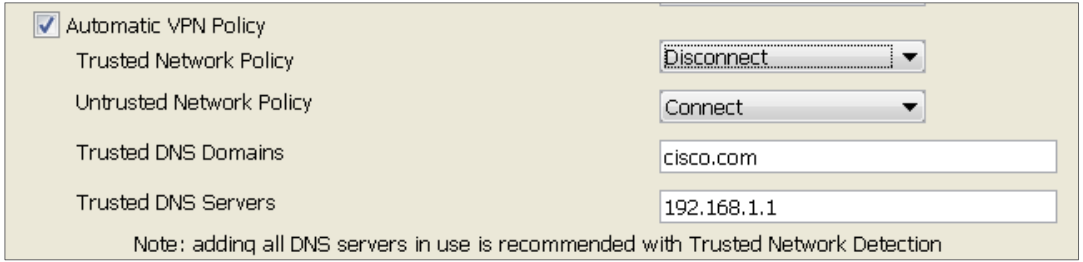
Всесторонняя безопасность

Обеспечение всесторонней постоянной защиты (always-on protection)

Cisco AnyConnect
расширенный функционал в одном клиентском ПО



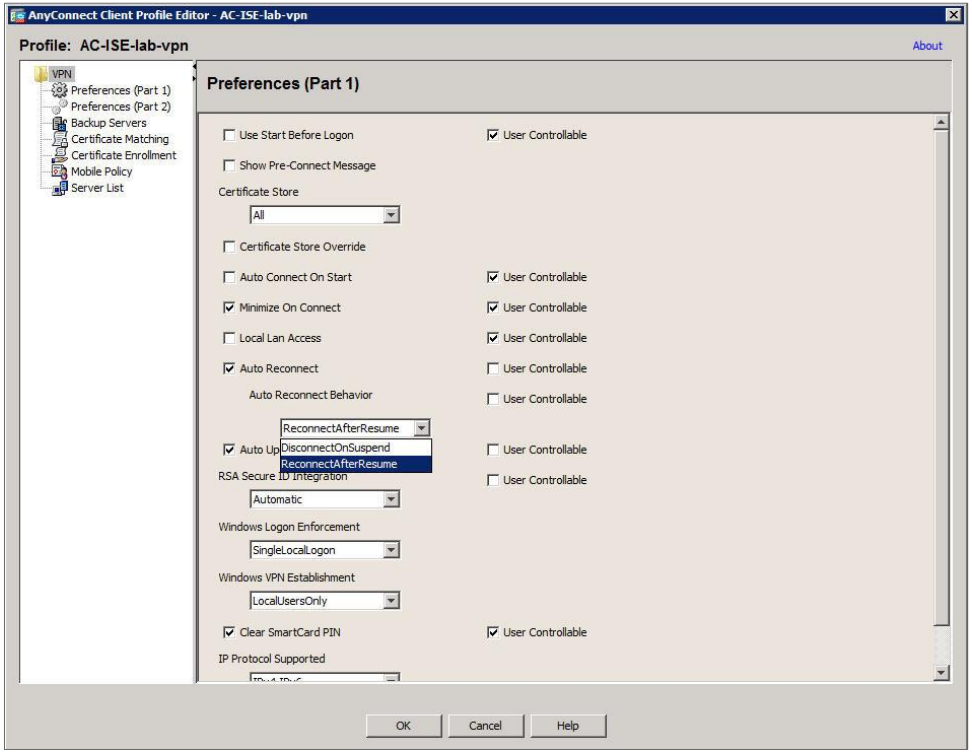
Trusted Network Detection



- Цель – автоматизировать процесс установления или обрыва VPN подключения
- Auto-disconnect inside office
- Auto-connect when out of office
- Based on default domain name or DNS server IP
- Настраивается в ASDM Profile Editor или в отдельном AnyConnect Profile Editor for Windows*

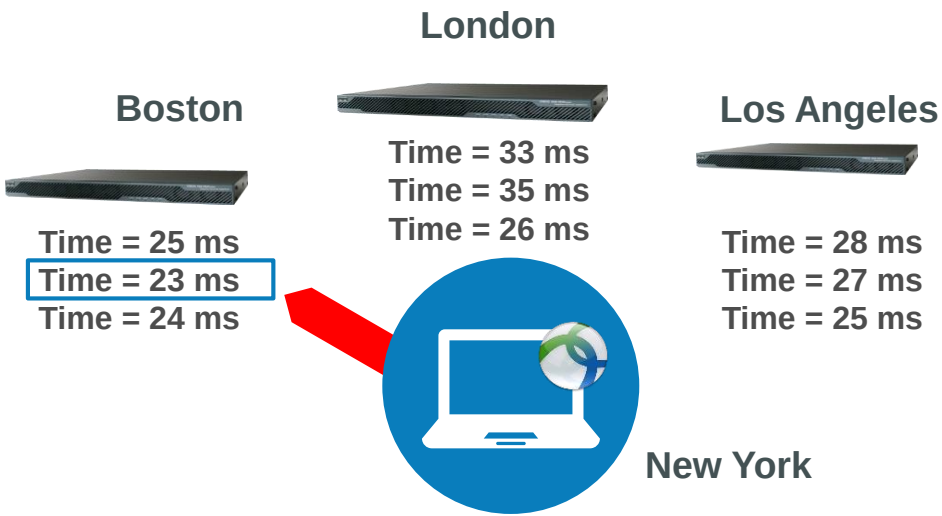
* Download the anyconnect-profileeditor-win-<version>-k9.exe from Cisco.com

Always-ON и Session Persistence



- Цель – предотвратить доступ в к Интернет ресурсам (until in untrusted network) без установление VPN туннеля
- Auto- established a VPN session (until in untrusted network)
- Auto-reconnect
- No re-authentication

Оптимальный выбор head-end
На основе round trip delay



- Цель – автоматический выбор оптимального (с точки зрения сетевых задержек) head-end для установление VPN туннеля
- Интеграция с механизмами резервирования head-end (список возможных head-end узлов)
- Повышение производительности работы

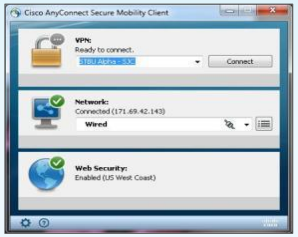
Web Security
на базе Cisco Cloud Web Security*

Выбор CWS proxy with the fastest response time

Cisco AnyConnect for Cloud Web Security

Cisco ScanCenter is the management portal for Cisco Cloud Web Security

Internet-Bound Web Communications

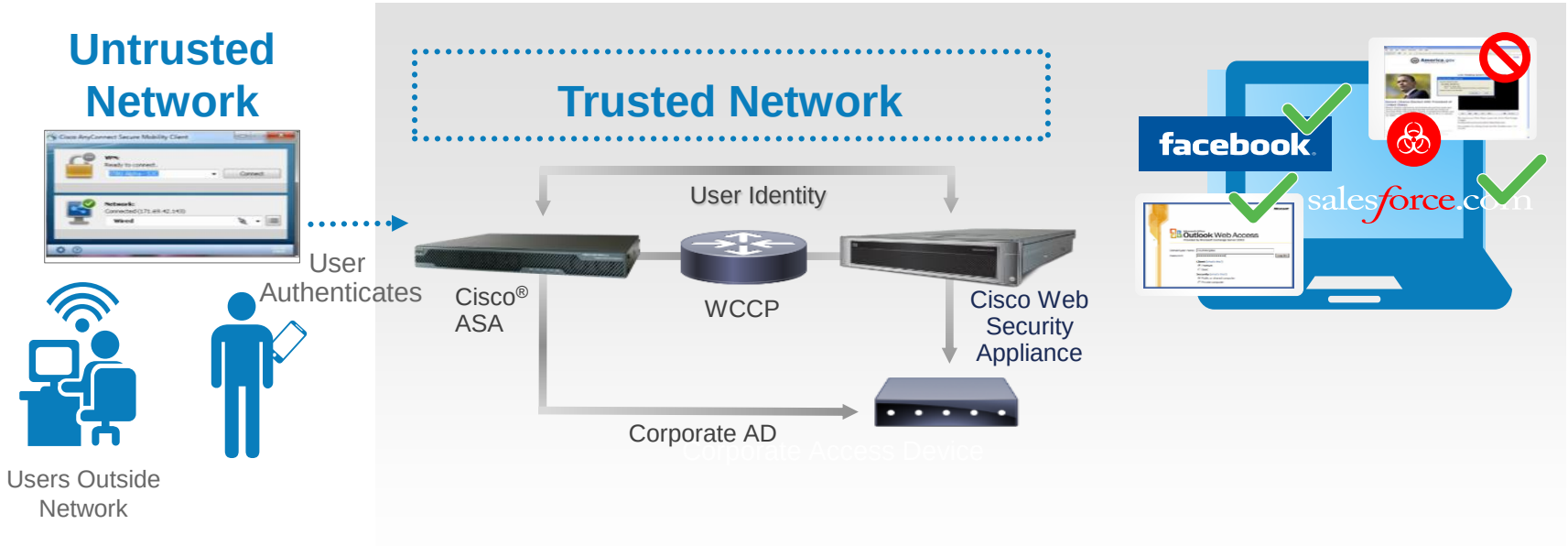


Cisco AnyConnect Secure Mobility Client

Internal Communications

* Лицензии для CWS приобретаются отдельно

Web Security
на базе Cisco Web Security Appliance*



* Лицензии для WSA приобретаются отдельно

Network Visibility Module (NVM)
модуль сбора телеметрической информации

- Цель – сбор телеметрической (контекстной) информации об устройстве для дальнейшей визуализации этих данных (решение задач - планирование, аудит, compliance, безопасность)

  - The device - the endpoint, irrespective of its location
  - The user - the one logged into the endpoint
  - The application - what generates the traffic
  - The location - the network location the traffic was generated on
  - The destination - the actual FQDN to which this traffic was intended

- Дополнительный программный модуль к AnyConnect

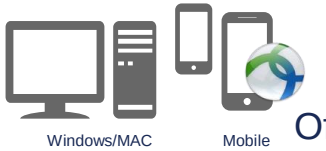
- Сбор телеметрических данных в trusted or untrusted network

- In trusted network, AnyConnect NVM exports the flow records to a collector → IPFIX → (a third-party vendor such as Lancope* or LiveAction)

* Компания Lancope приобретена Cisco

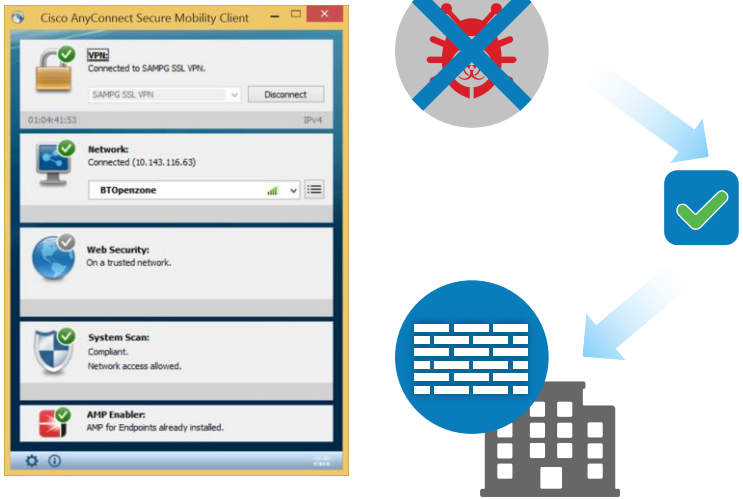
Advanced Malware Protection (AMP) Enabler*
расширение защиты пользовательского устройства

- Цель – защитить удаленного пользователя от вредоносного кода и угроз безопасности, путем проверки трафика на наличие вредоносного кода
- Дополнительный программный модуль к AnyConnect
- AMP for Endpoint лицензионная подписка (FP-AMP-LIC=) на 1, 3, 5 лет приобретается отдельно
- Поддержка – Windows, MAC (see Release Notes)



Off Premise

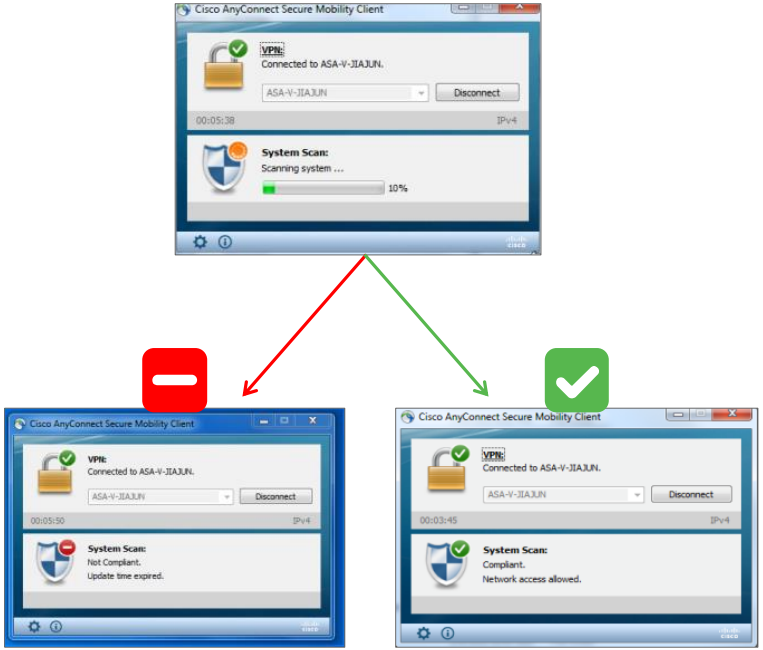
More Security



* AMP for Endpoints licensed separately

Endpoint Compliance
проверка на соответствие

- Цель – обеспечить аудит узла на соответствие корпоративным политикам безопасности при подключении к корпоративной сети и гарантировать доступ только тем, кто успешно прошел проверку
- 2 варианта: ASA HostScan Module (separate from AC v4) и ISE Posture Module (integrate with AC)
- ISE Apex лицензионная подписка (L-ISE-APX-S-zzzz=) на 1, 3, 5 лет приобретается отдельно
- Поддержка – Windows, MAC, Linux (see Release Notes)



Новое лицензирование в Cisco AnyConnect 4.0

2 типа лицензий

Лицензия Plus

- VPN (вкл. IP phone VPN)
- Сторонние VPN клиенты (IPsec IKEv2)
- Мобильный VPN по приложениям (Per-app VPN)
- Менеджер сетевого подключения (NAM)
- Веб-безопасность (CWS и WSA)*
- Cisco AMP for Endpoints Enabler*

* Specific licenses are required

Лицензия Apex

- Функции Plus
- Network Visibility модуль
- Соответствие устройств (Unified Endpoint Compliance and Remediation (Posture))*
- “Без-клиентский” (clientless) доступ (browser-based)
- Криптография Suite B

* ISE Apex licenses are required

Лицензия по пользователям (с любым кол-вом устройств)

Cisco Web Security

Why Web Security?

19.7 Billion

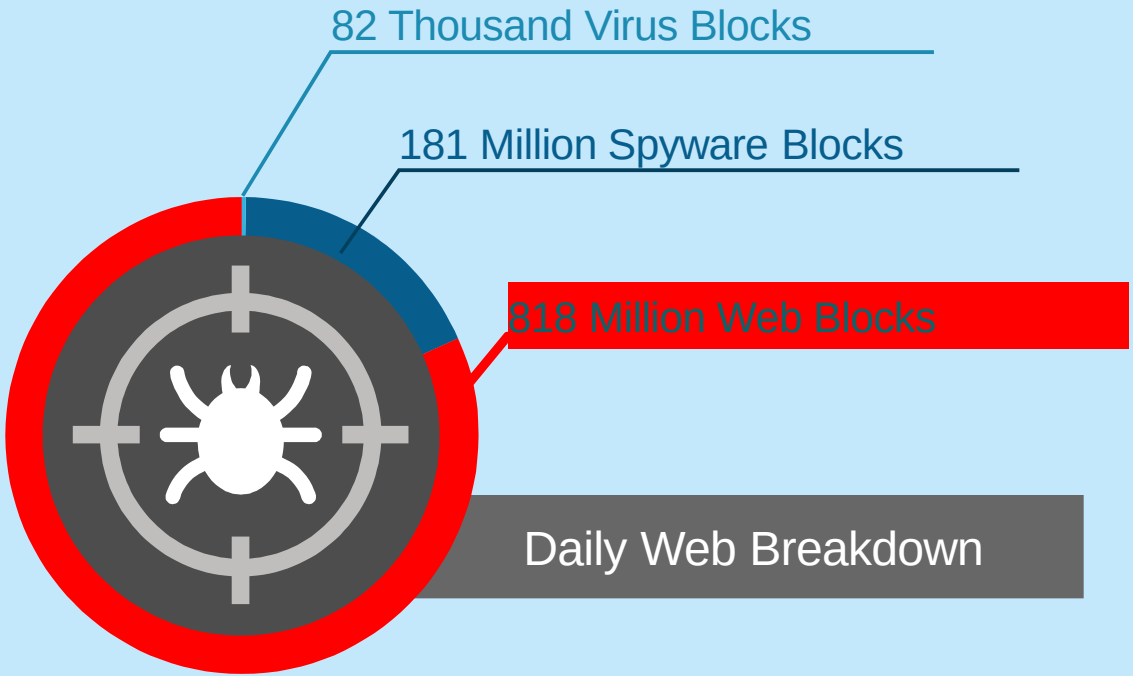
Total Threat Blocks

Daily

=

7.2 Trillion

Yearly



Cisco Web Security Protects the Web Vector While Supporting Your Business

Comprehensive Defense

Advanced Threat Protection

Superior Flexibility

Cisco Web Security Appliance (WSA)

Cisco Cloud Web Security (CWS)

It Starts with Usage Control and Active Defense

Web Filtering
Block over 50 million known malicious sites, 75 categories

Web Reputation
Restrict access to sites based on assigned reputation score (more 50 site's parameters)

Dynamic Content Analysis
Categorize webpage content and block sites automatically

Outbreak Intelligence
Identify unknown malware and zero-hour outbreaks in real time (how each component behaves)

Application Visibility and Control
Regulate access to website components and apps

DLP Integration
Prevent confidential information from leaving your network

Time and Bandwidth Quotas
Set controls for users in terms of time on social media sites as well as bandwidth usage

Roaming User Protection
Protect users while away from the corporate network (Using Cisco AnyConnect)

Available only on WSA/WSAv

Available only on CWS

Cisco Web Security Combats Evolving Threats

Cisco Advanced Malware Protection (AMP)

File Reputation

Increase the accuracy of threat detection by examining every aspect of a file

File Sandboxing

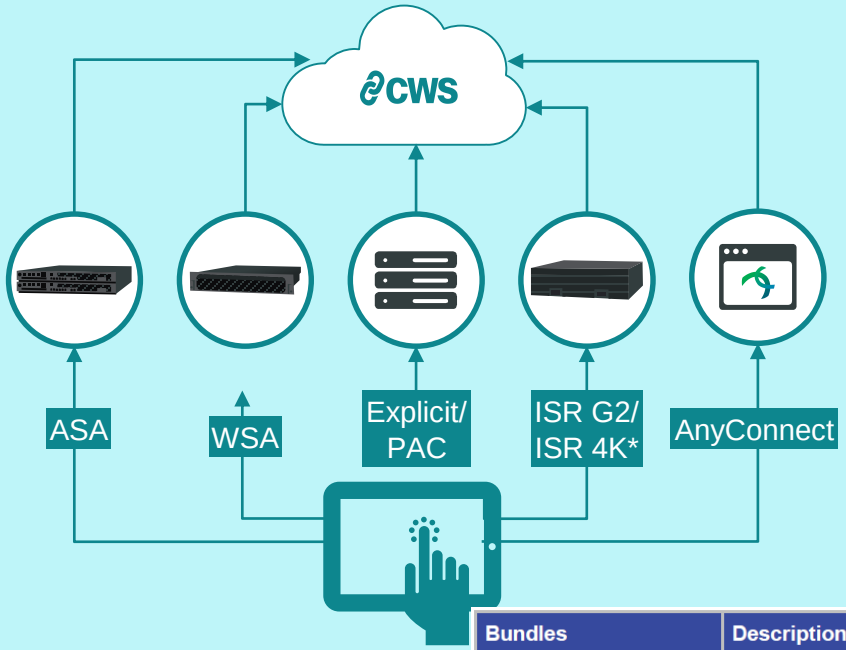
Determine the malicious intent of a file before it enters the network

File Retrospection

Identify a breach faster by tracking a file's disposition over time

Ordering

CWS Traffic Redirectors



WSA Models

Physical Appliance

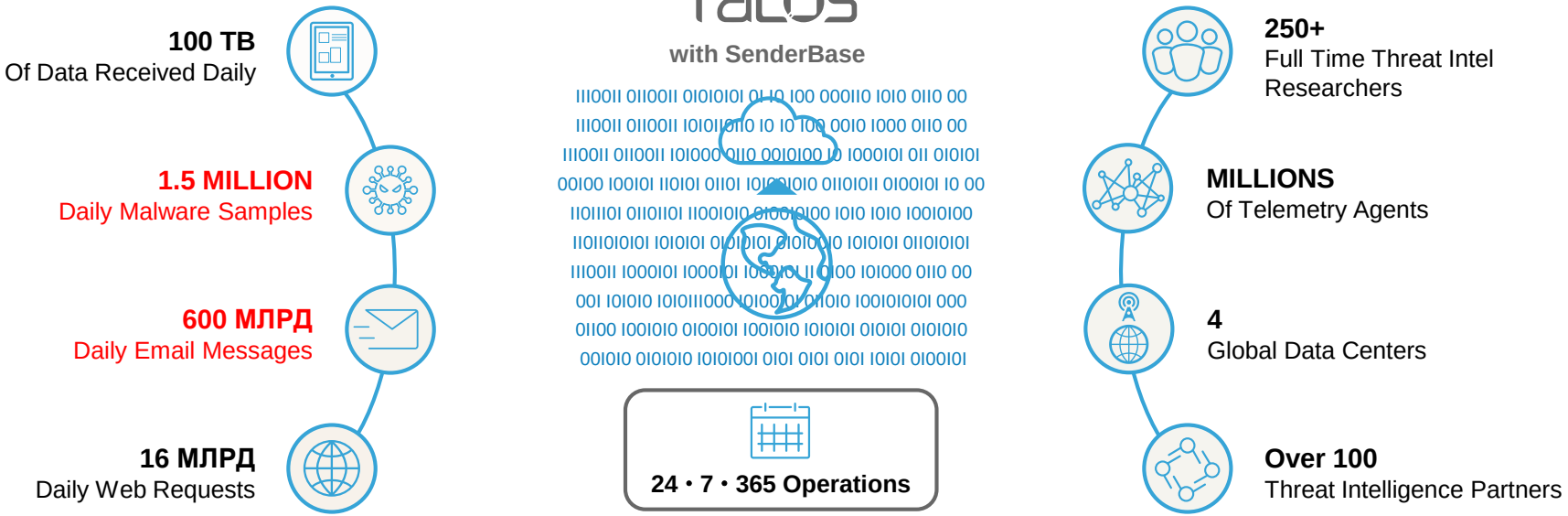
Perfect for small business branches	Perfect for mid-size offices	Perfect for large enterprises
WSA-S190	WSA-S390	WSA-S690/690X

Virtual Appliance (WSAv)

Bundles	Description	Top-Level SKU
Cisco Web Security Essentials	Provides protection and control of an organization's web traffic using Web Usage Controls (URL Filtering and AVC) and Web Reputation technologies. Includes software subscription support and a license for the Web Security Virtual Appliance.	WSA-WSE-LIC=
Cisco Web Security Antimalware	Combines Cisco Web Reputation with Sophos Anti-malware, Webroot Anti-malware. Includes software subscription support and includes license for the Web Security Virtual Appliance.	WSA-WSM-LIC=
Cisco Web Security Premium	Combines the features of "Cisco Web Security Essentials" bundle and "Cisco Web Security Antimalware" bundle.	WSA-WSP-LIC=

Cisco Email Security

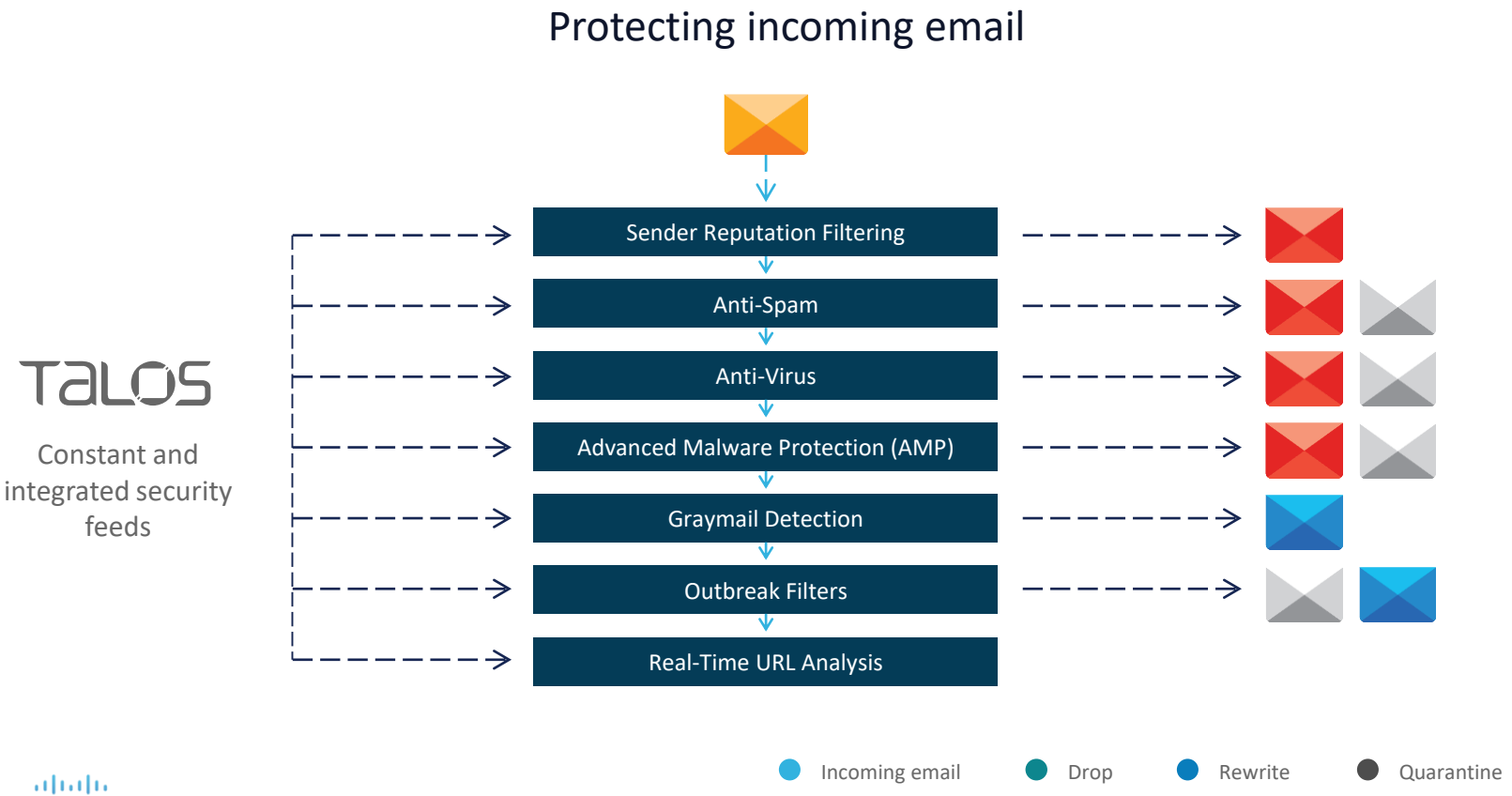
Cisco Email Security is backed by unrivaled global threat intelligence



Deploy the world's largest email traffic monitoring network

Leverage industry-leading threat analytics

Talos on Cisco Email Security



It’s built with industry-leading spam protection

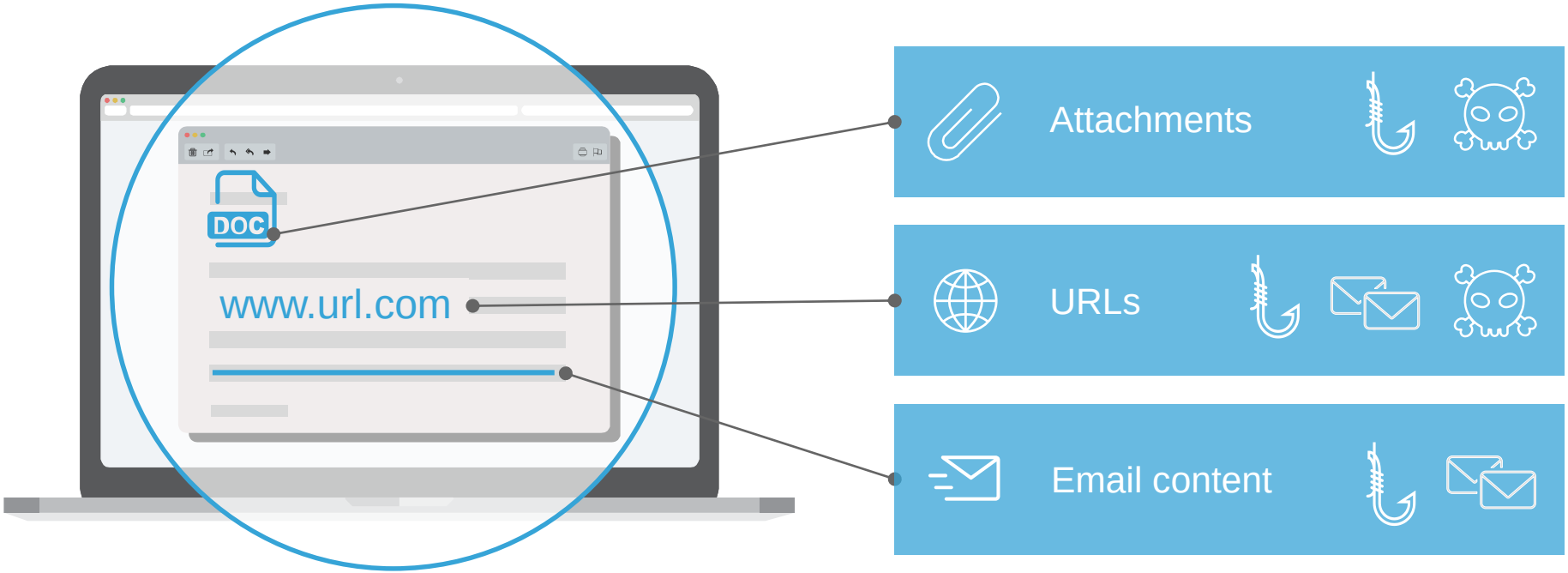
Anti-spam processing / Context Adaptive Scanning Engine (CASE)

Review sender reputation, URL reputation, and message content

Block spam with 99% accuracy with fewer than 1:1M false positives

Quarantine suspicious messages for additional review

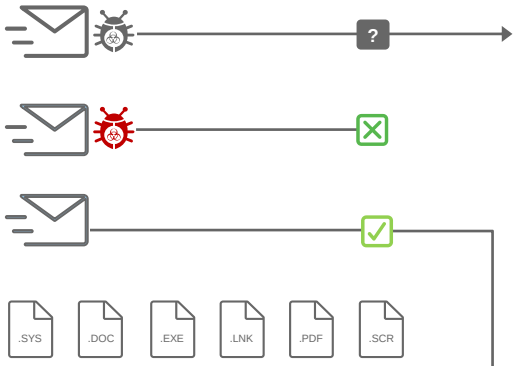
And reduces your exposure to the three main components of an email attack



Keep tabs on all emails admitted into the environment after analysis

Advanced Malware Protection (AMP)

File Reputation



File Sandboxing

- Advanced Analytics
- Dynamic analysis
- 560+ indicators

File Retrospection

Block known malware

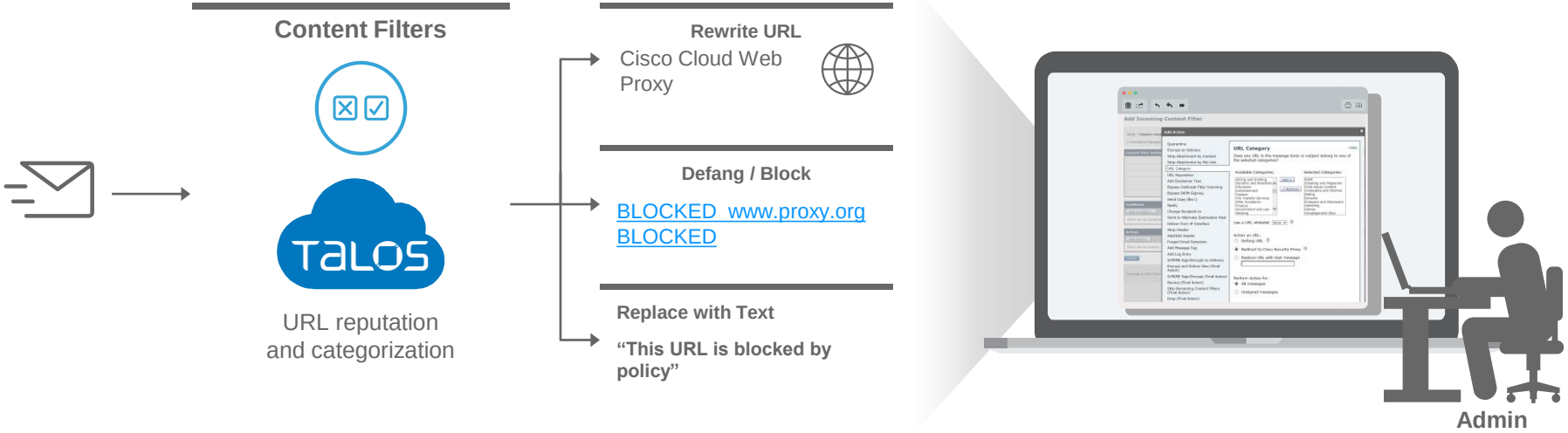
Investigate files safely

Auto-remediate threats in O365

Gain visibility into messages trying to enter the network

Control which emails cross the network

Content Filters

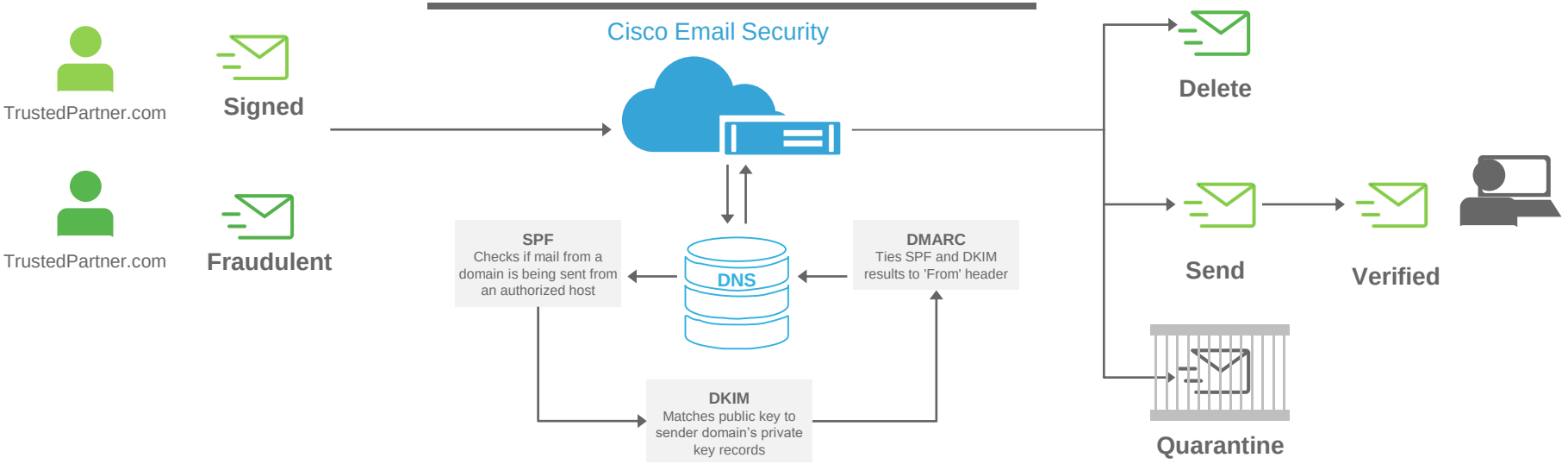


Customize filters in three different ways for additional security

Easily enforce business and compliance policies

Block fraudulent senders

DMARC, DKIM and SPF



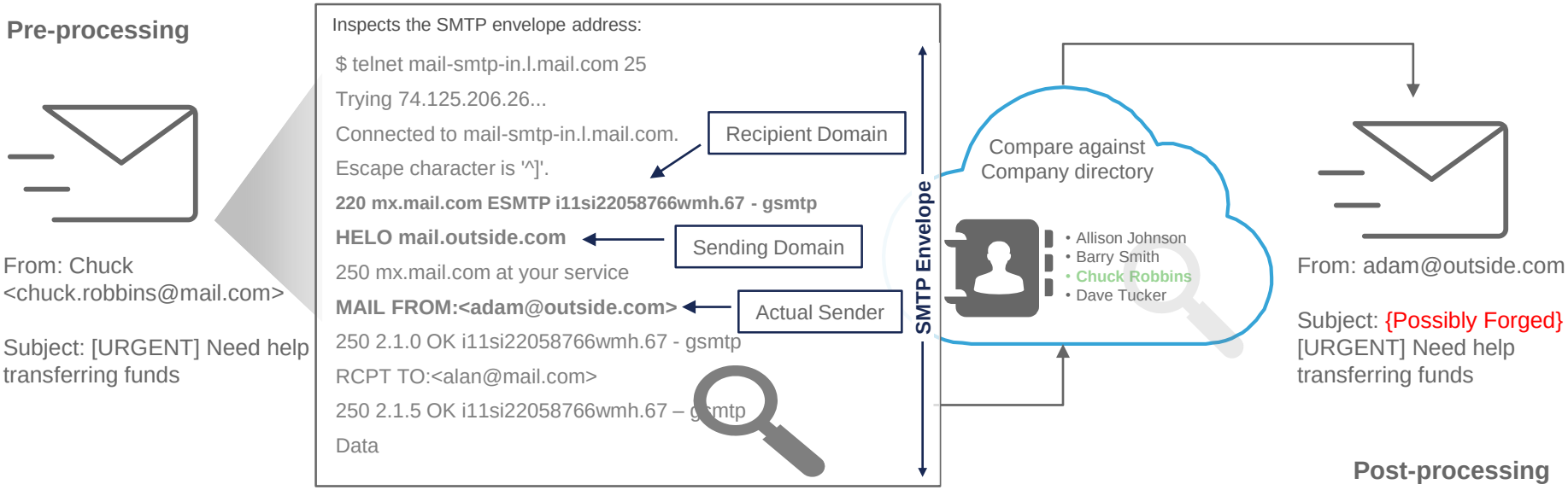
Determine whether a sender is reputable

Inspect sender details on inbound messages

Block invalid senders and identify next steps

Protect against spoofing attacks

Forged Email Detection



Inspect SMTP envelope for sender address

Match sender address against company directory

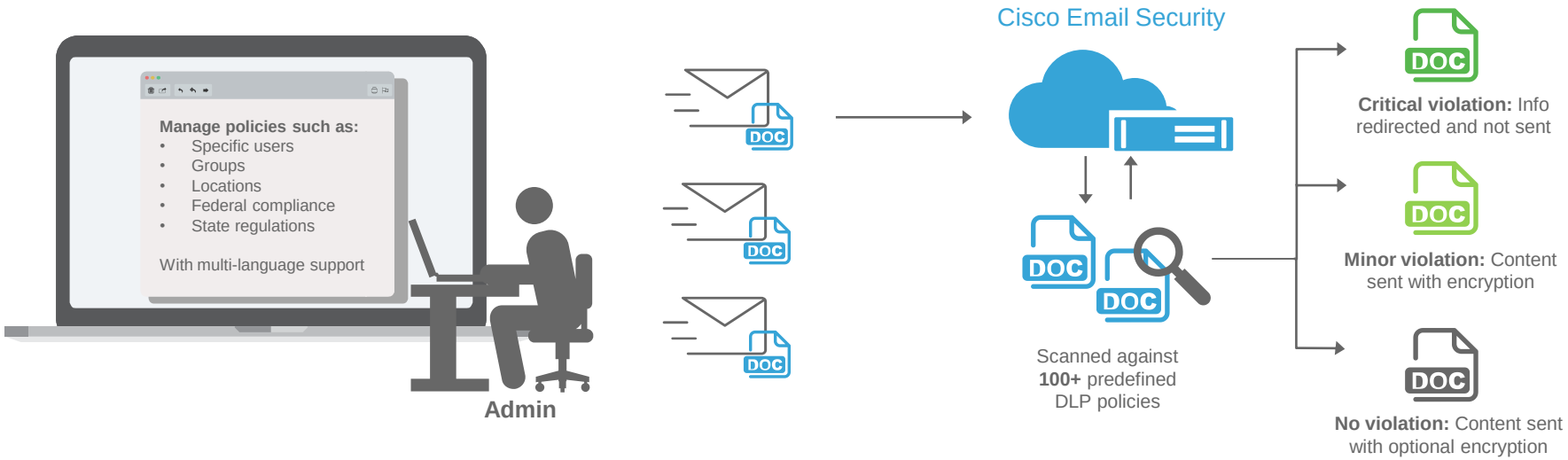
Send appended mail to warn users of potential forgery

Record a log of attempts and actions taken

Cisco catches critical data before it leaves the network

Protect personal information and IP

Data Loss Prevention (DLP)



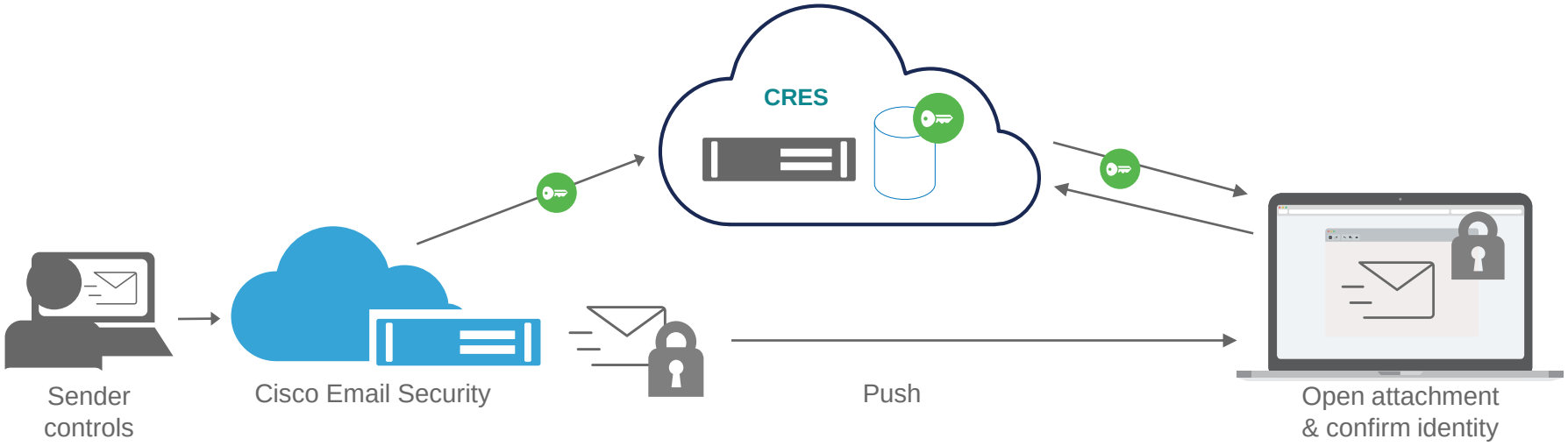
Control what leaves the network and customize policies

Scan email content for sensitive information

Prevent data exfiltration automatically

Extend security to external communications

Cisco Registered Envelope Service (CRES)

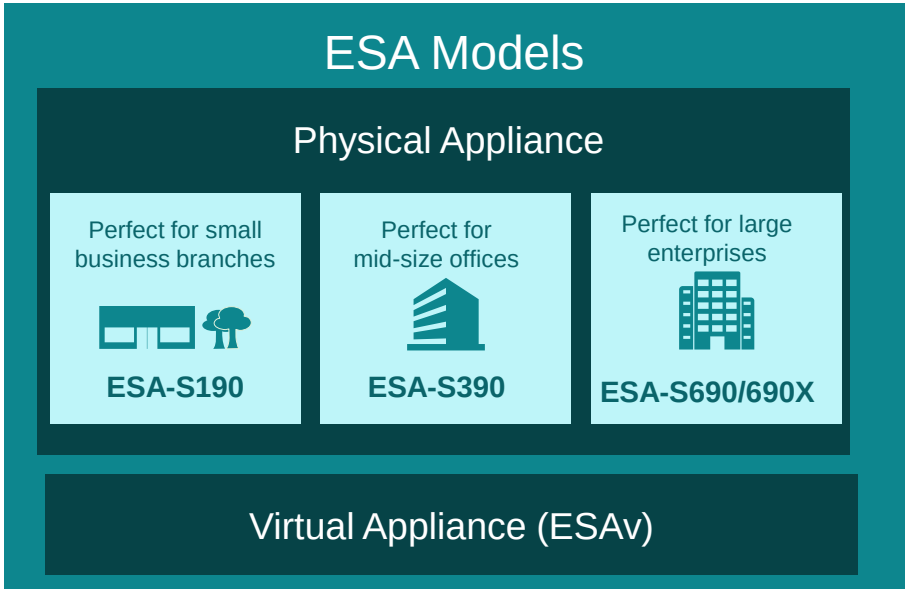


Scan messages for keywords, policies, and sender

Apply authentication mechanisms to access encryption keys

Maintain control over your sent messages

Ordering



Bundles	Description	Top-Level SKU
Cisco Email Security Inbound	Protects an organization's mailboxes against spam, viruses, and targeted attacks (Antispam + Antivirus + Outbreak Filters + Forged Email Detection); includes license for the Email Security Virtual Appliance	ESA-ESI-LIC=
Cisco Email Security Outbound	Helps satisfy compliance requirements by providing easy-to-use encryption and DLP solutions (DLP + Encryption); includes license for the Email Security Virtual Appliance	ESA-ESO-LIC=
Cisco Email Security Premium	Combines Inbound and Outbound protection to provide a complete email security solution (Inbound + Outbound); includes license for the Email Security Virtual Appliance	ESA-ESP-LIC=

Спасибо за внимание!

Максим Порицкий

инженер по направлению Cisco, CCIE R&S

m.poritsky@elcoregroup.com

17.10.2017