

Cisco Umbrella как облачная платформа защиты от угроз

Дмитрий Казаков

Системный инженер, CISSP, CCIE Security, СЕН

Программа

- **Вступление**
- Что такое Cisco Umbrella
- Архитектура и потоки данных
- Статистические модели
- Заключение



К 2020,
Cisco Global
Cloud Index
оценивает:

92% глобального
трафика ЦОД
будет
приходиться на
облака

К 2021,
Gartner
оценивает:

25%
корпоративного
трафика будет
проходить мимо
периметральной
безопасности

Как IT строилось ранее



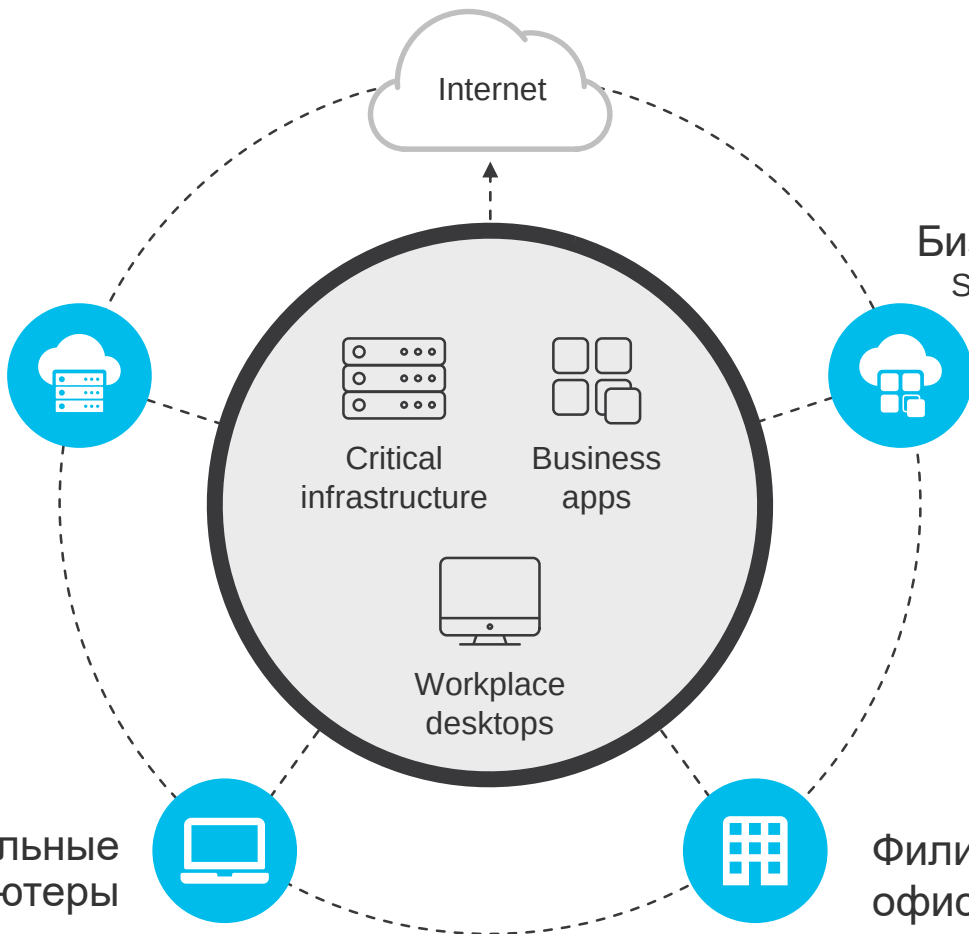
IT Сегодня

Критическая инфраструктура
Amazon, Rackspace, Windows Azure, и др.

Бизнес приложения
Salesforce, Office 365, DocuSign, и др.

Мобильные компьютеры

Филиальные офисы



Изменилось то как мы работаем...

И безопасность также...

49%

Работников
станут
мобильными

82%

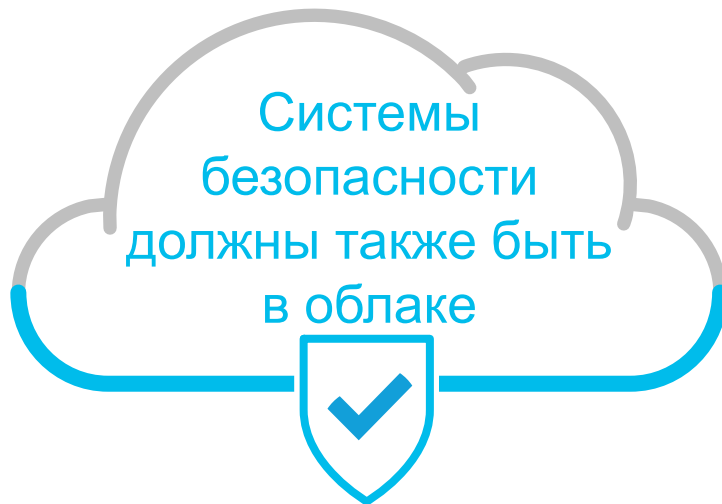
Предпочитают
не включать
VPN

70%

Рост
использования
SaaS

70%

Филиальных
сетей имеют
прямой доступ в
Интернет



Программа

- Вступление
- **Что такое Cisco Umbrella**
- Архитектура и потоки данных
- Статистические модели
- Заключение





Внутри и снаружи
корпоративной сети

Все порты и протоколы

Открытая платформа

Живой интеллект угроз

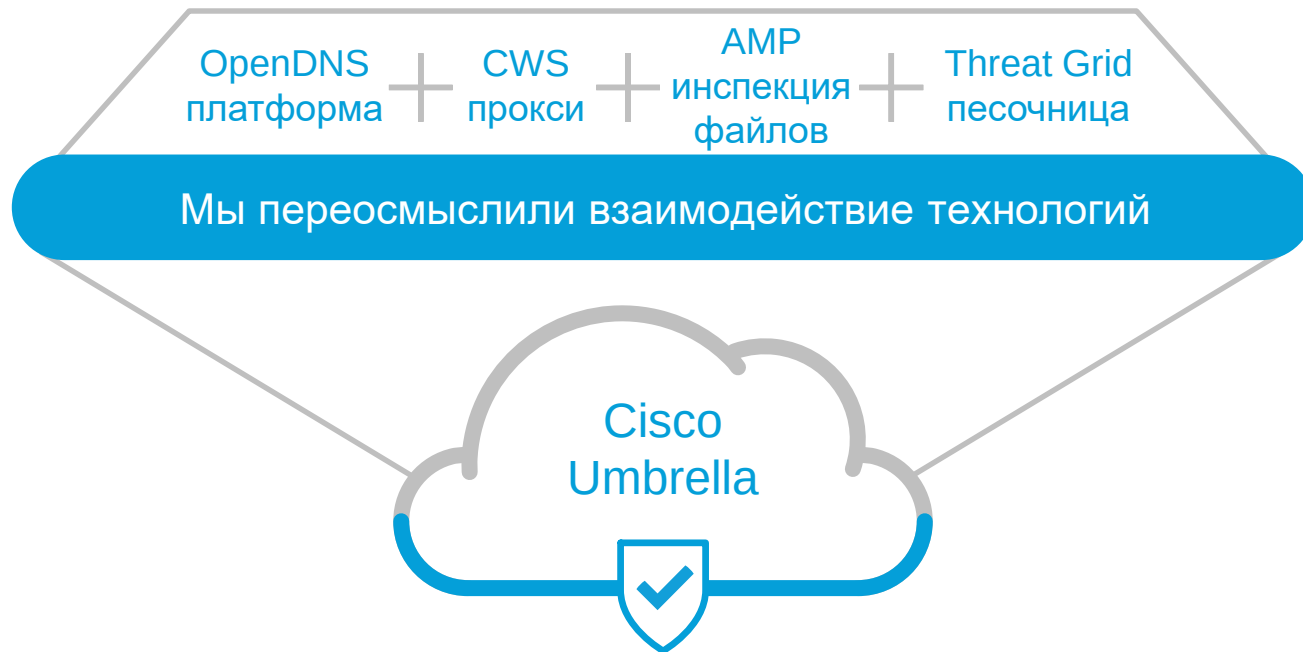
Проксирование и инспекция
файлов

Обнаружение и контроль SaaS



Представляем Cisco Umbrella

Из чего состоит Cisco Secure Internet Gateway



Umbrella отличается от других



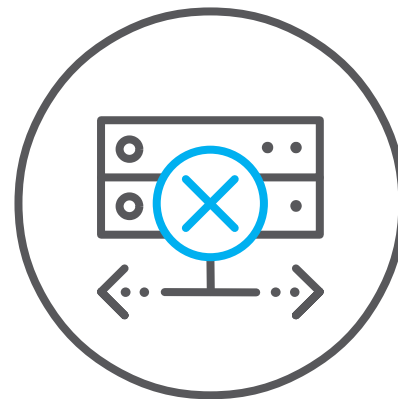
Концентрация на безопасности

Продуктивность не может быть достигнута контролем корпоративной сети



Простота развертывания и управления

Использование DNS и подхода Cisco для простоты развертывания



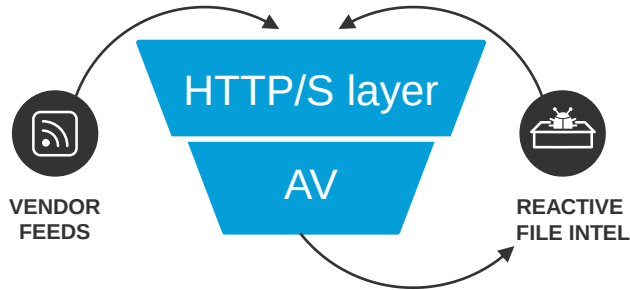
Не нужно проксировать всё

Проксирование всего это проигрыш сражения, только добавляющий задержку

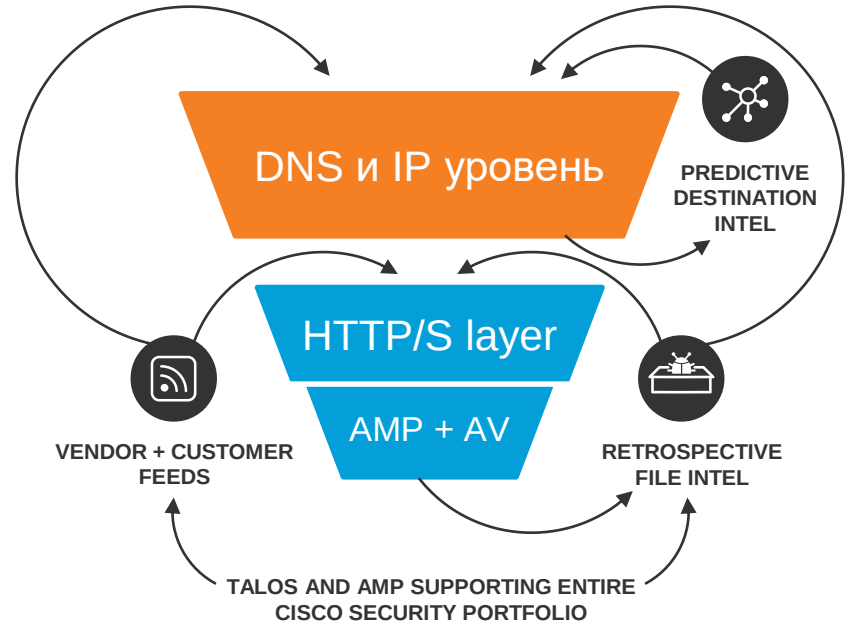
Cisco SIG в сравнении с другими SWG

SWG

Проблема:
Неполное покрытие
направлений и файлов



SIG



Краткий экскурс в историю

OpenDNS

OpenDNS founded

2006

Umbrella global network

2006

Umbrella virtual appliance

2012

Umbrella roaming client

2012

Umbrella statistical models

2013

Umbrella Investigate

2013

Umbrella intelligent proxy

2014

Umbrella API

2014

Umbrella Investigate API

2015

Cisco acquisition

2015

ScanSafe

ScanSafe founded

1999

ScanSafe service launched

2004

Cisco acquires ScanSafe

2009

Integration with ISR G2

2010

Integration with AnyConnect

2010

Integration with ASA

2011

Integration with AMP & CTA

2013

Log Extraction

2015

CWS Secure Browser

2015

Integration with ISR 4K

2016

2016: Cisco
Umbrella запущен!

DNS Обзор



Регистратор доменов

Сопоставляет записи
имен к #S в
“телефонной книге”



Авторитативный DNS

Владеет и публикует
“телефонную книгу”



Рекурсивный DNS

Ищет и хранит
#S для каждого имени



Кто проводит разрешение Ваших DNS запросов?

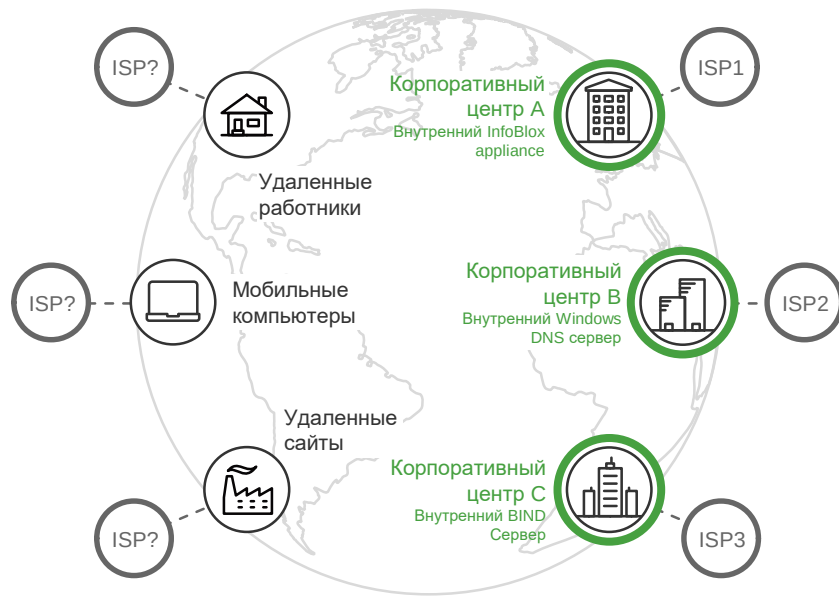
Проблемы

Множество Интернет провайдеров

Прямое подключение филиальных офисов

Пользователи забывают всегда включать VPN

Различные форматы DNS логов



○ Рекурсивный DNS для Интернет доменов

○ Авторитативный DNS для интранет доменов

Umbrella: Единый глобальный рекурсивный DNS Сервис

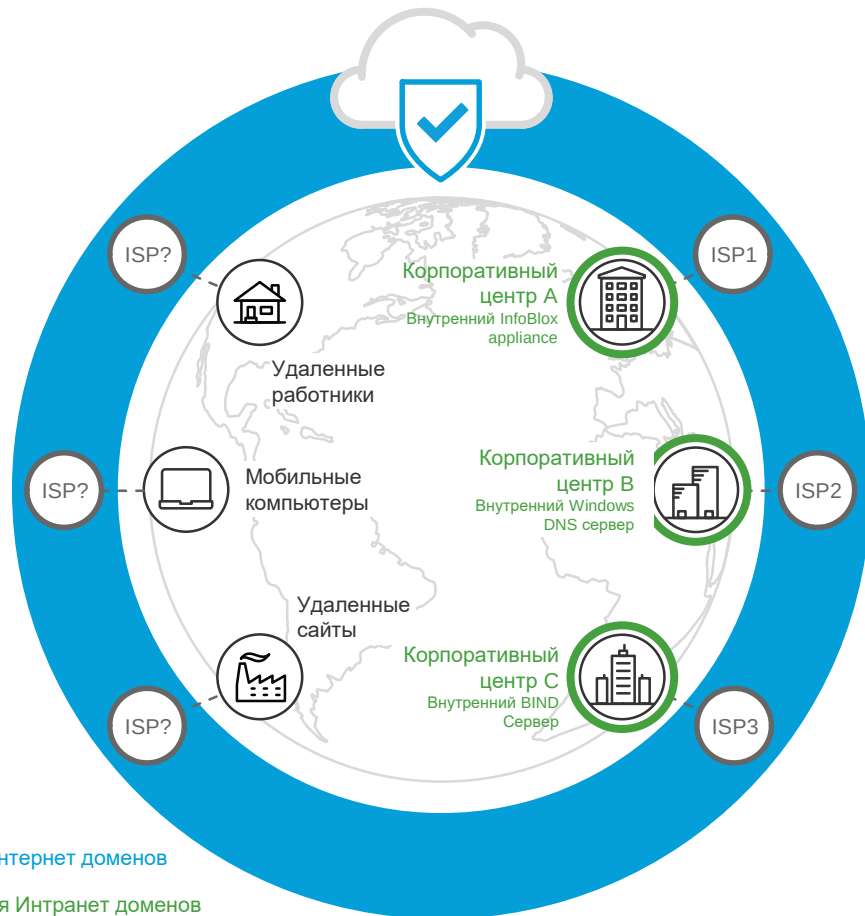
Преимущества

Глобальная видимость Интернет активностей

Сетевая безопасность без добавления задержки

Целостное применение политик

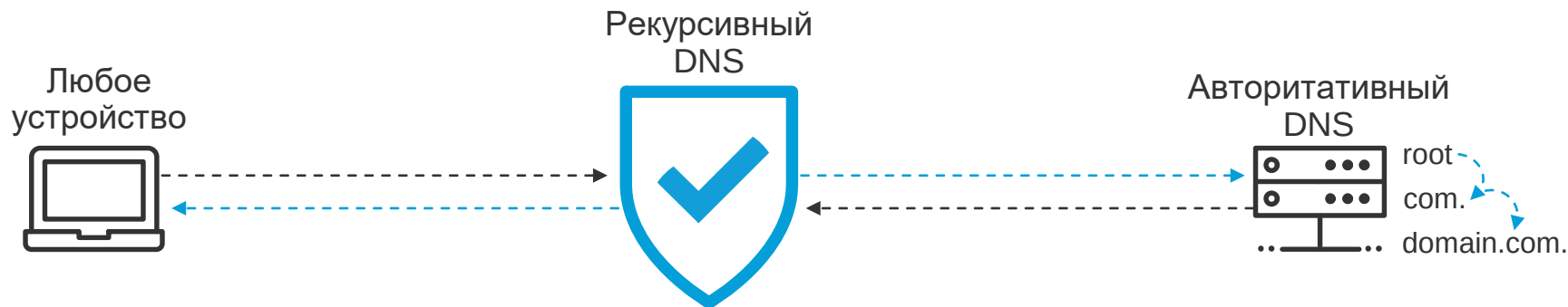
Видимость Интернета из облака



✓ Рекурсивный DNS для Интернет доменов

○ Авторитативный DNS для Интранет доменов

Собирайте данные, усиливайте безопасность на уровне DNS



Шаблоны пользовательских запросов

Используются для обнаружения:

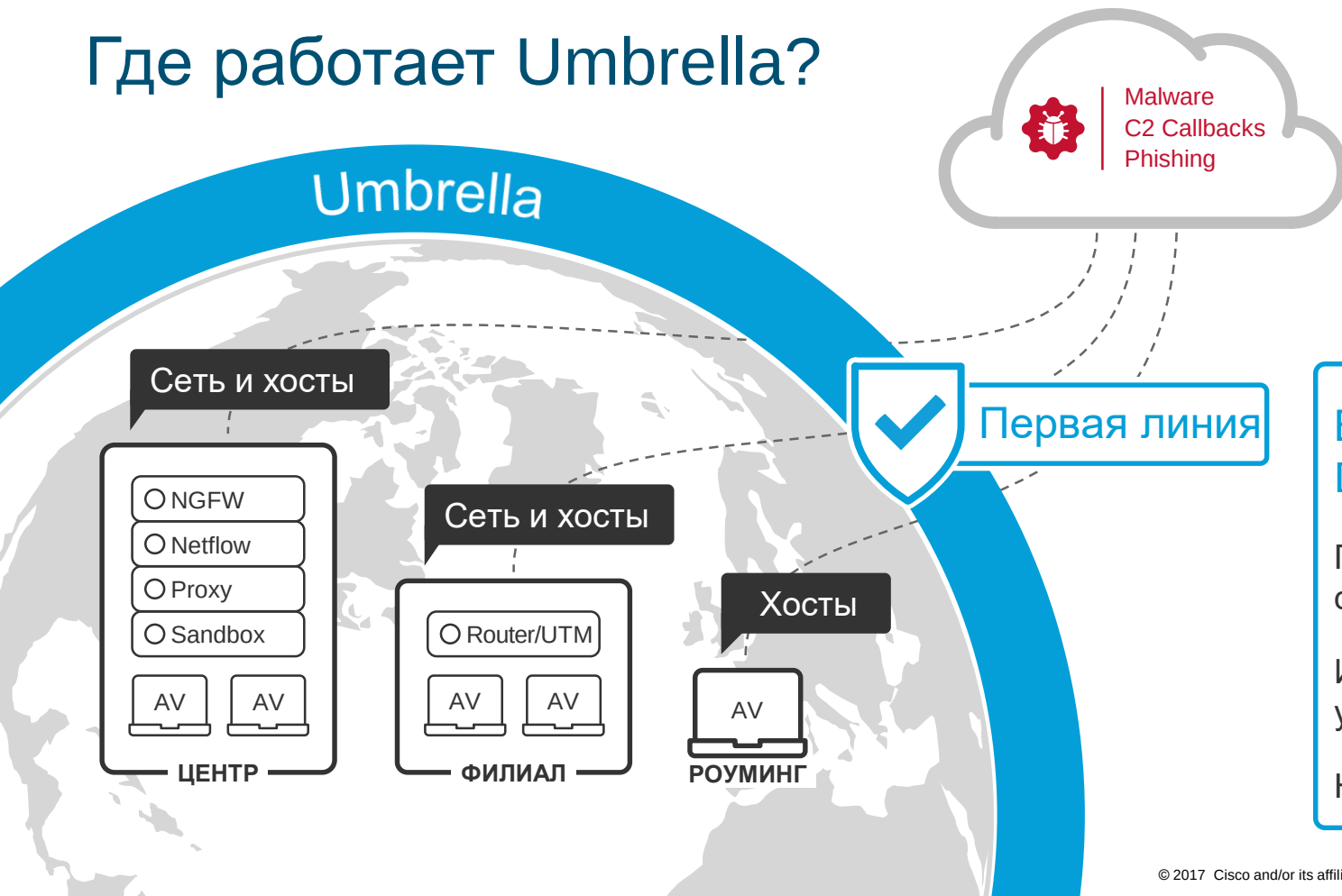
- Скомпрометированных систем
- Запросы на C&C соединения
- Фишинг и распространение Malware
- Доменные имена генерируемые алгоритмом
- Домены совместных запросов
- Свежезарегистрированные домены

Авторитативные DNS логи

Используются для поиска:

- Вновь развертываемых инфраструктур
- Вредоносных доменов, IP, ASN
- DNS перехватов
- Fast flux доменов
- Связанных доменов

Где работает Umbrella?



Всё начинается с DNS

Предвосхищает открытие файлов и IP соединение

Используется всеми устройствами

Не зависит от порта

Видимость Umbrella

100B

Запросов
ежедневно

85M

Активных
пользователей
ежедневно

12K

Корпоративных
заказчиков

160+

Странах
мира

Umbrella Resolver обработка запросов

Направления

Изначально запрошенный ресурсы
или страница блокировки

Контроль безопасности

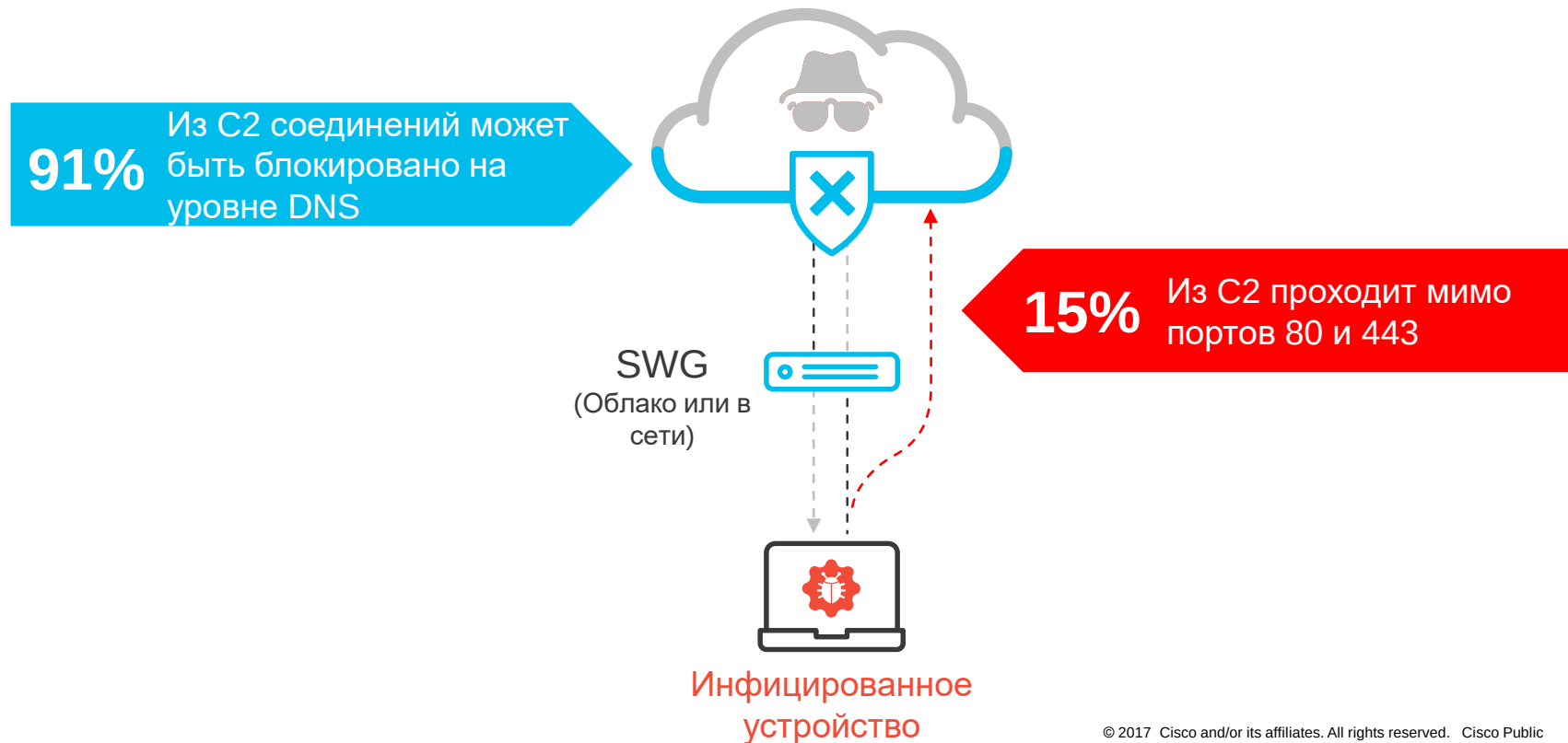
- DNS и IP фильтрация
- Инспекция подозрительных доменов через прокси
- SSL decryption доступен

Интернет трафик

Внутри сети и за её
пределами

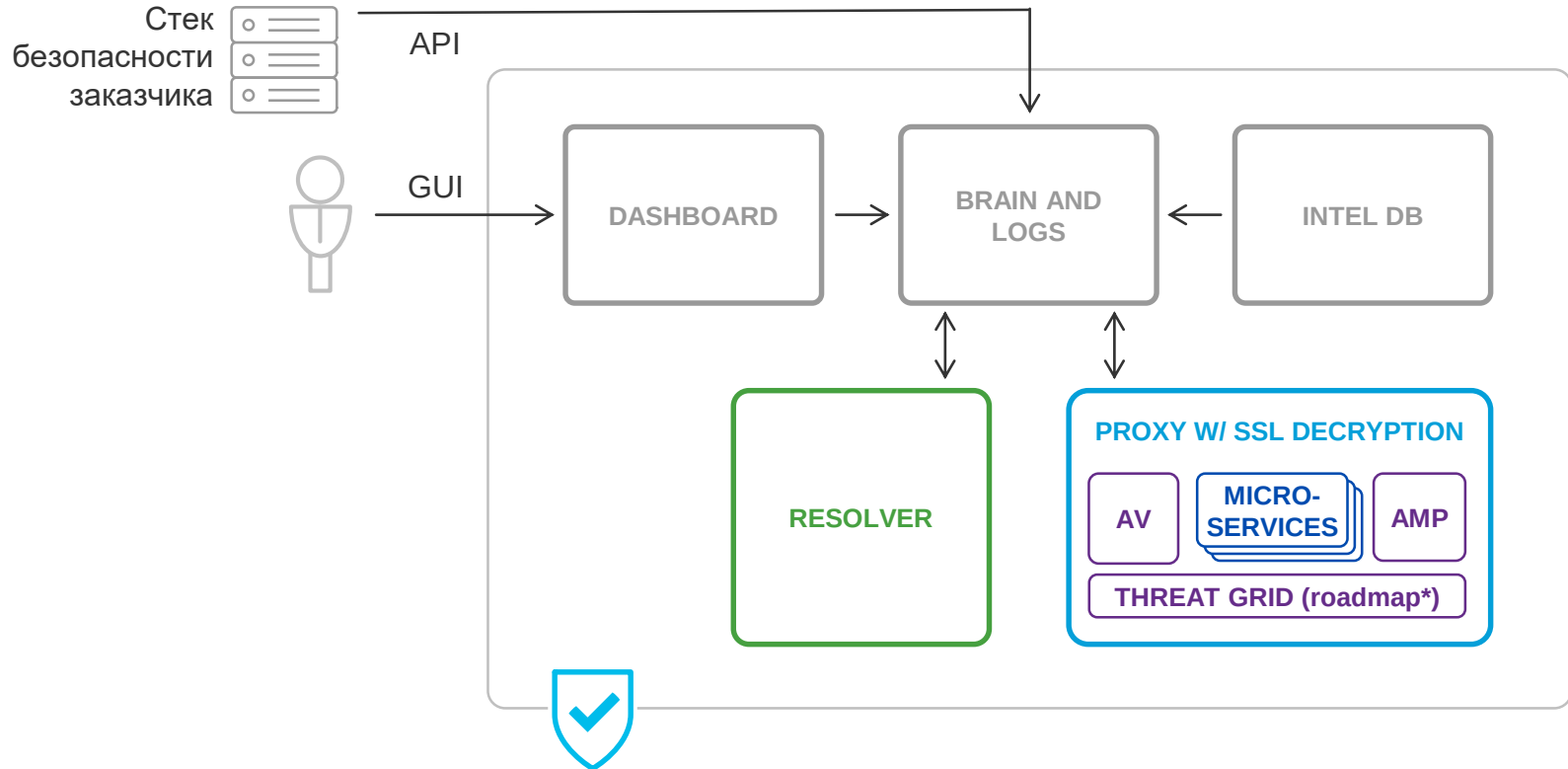


Защита от запросов Command and Control



Umbrella Высокоуровневая архитектура

Что происходит внутри “черного ящика”?



Umbrella опции заказа

		Branch	Roaming	Wireless LAN	Professional	Insights	Platform
		Работает с специфичными решениями Cisco и интеграцией, ограниченный функционал			Работает самостоятельно и в интеграции с Cisco		
Покрытие	On-Network (Любое устройство)	(ISR только)		(LAN только)	✓	✓	✓
	Off-Network (Ноутбуки)		✓		✓	✓	✓
Детальность политик и отчетности	По сети и хосту	(Сеть только)	(Только Хост)	(Сеть только)	✓	✓	✓
	По подсети и пользователю					✓	✓
Фильтрация глубина и покрытие	DNS Layer (domains+IPs)	✓	✓	✓	✓	✓	✓
	IPv4 Layer (non-DNS IPs)					✓	✓
	Proxy (security+IWF URLs)	(IWF только)		✓		✓	✓
	API-Based Integrations						✓
Видимость и интеллект угроз	Basic Logging & Reports	✓	✓	✓	✓	✓	✓
	Advanced Reporting					✓	✓
	Log Management via S3					✓	✓
	Investigate Console						✓

Программа

- Вступление
- Что такое Cisco Umbrella
- **Архитектура и потоки данных**
- Статистические модели
- Заключение



ЦОДы Umbrella располагаются в основных точках обмена (IXP)

Umbrella ЦОДы

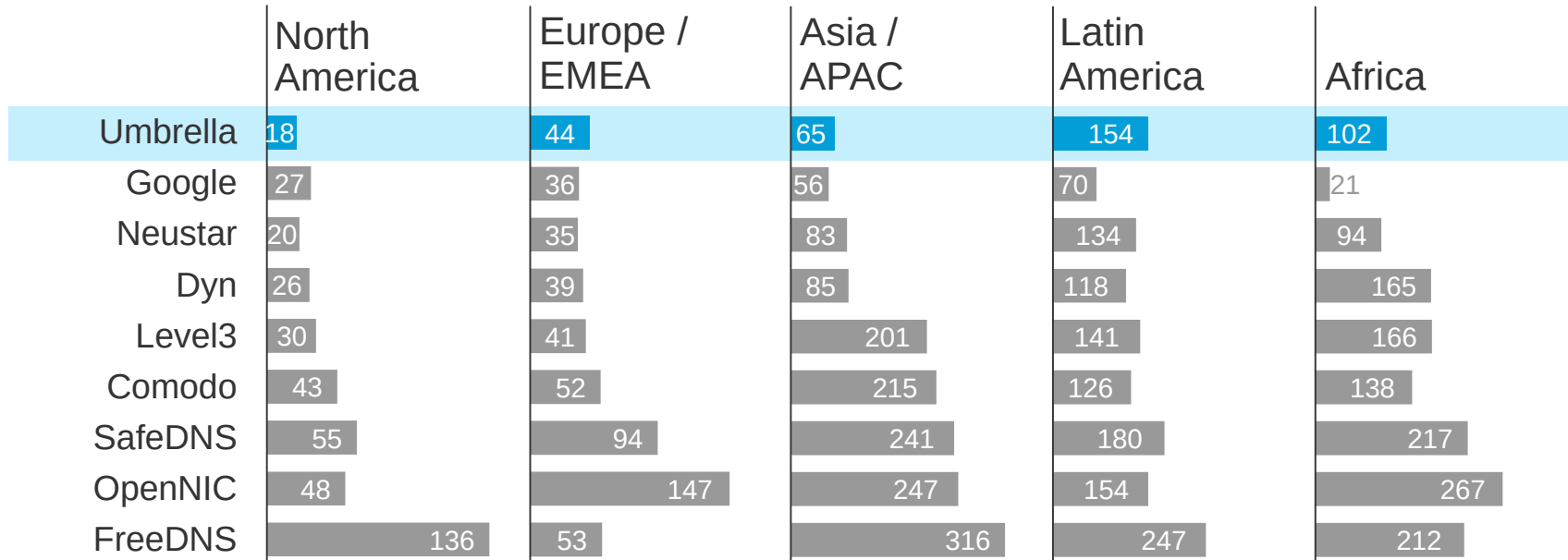
- Amsterdam
- Berlin
- Bucharest
- Chicago
- Copenhagen
- Dallas
- Frankfurt
- Hong Kong
- Johannesburg
- London
- Los Angeles
- Miami
- New York
- Palo Alto
- Paris
- Prague
- Seattle
- Singapore
- Sydney
- Tokyo
- Toronto
- Vancouver
- Warsaw
- Washington DC



BGP Пиринг для скорости



Как быстро Umbrella разрешает DNS запросы?

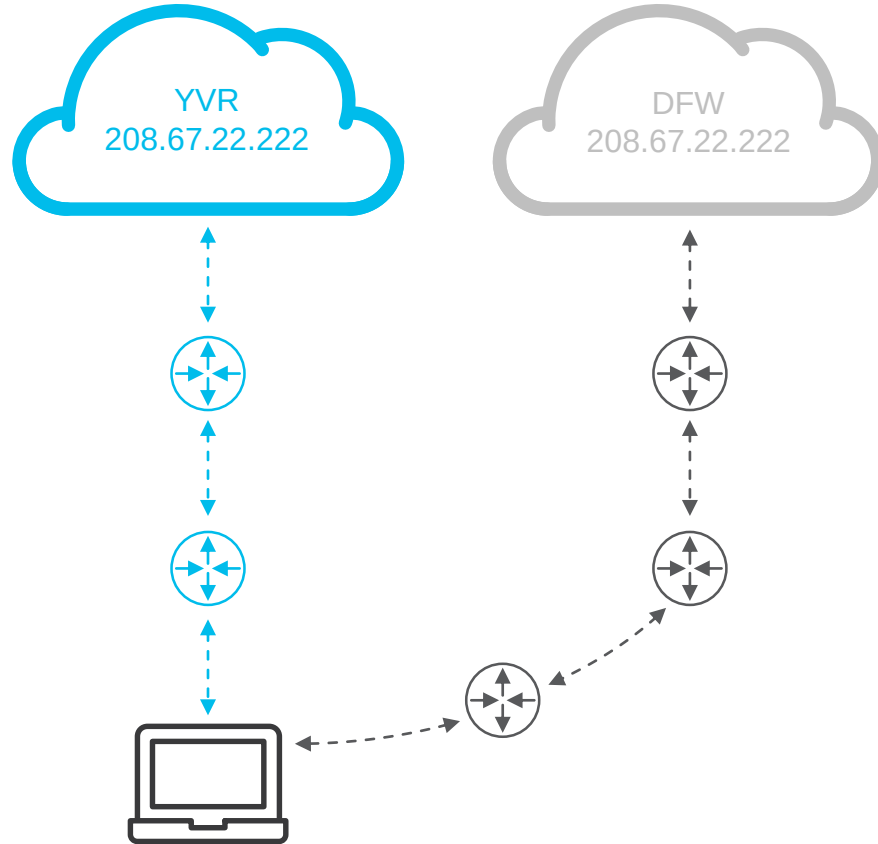


Измерение в Миллисекундах

Источник: MSFT Office 365 Researcher,
ThousandEyes Blog Post, May 2015

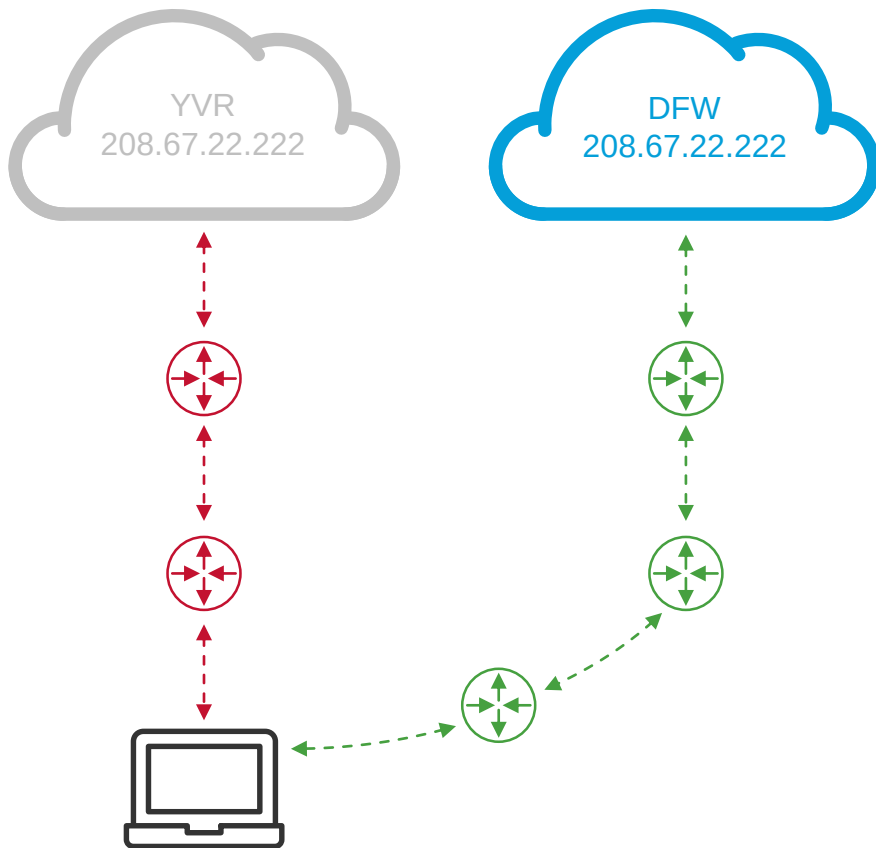
IP Маршрутизация с Anycast для отказоустойчивости

- Все ЦОД анонсируют одинаковые IP адреса
- Запросы прозрачно направляются ближайшему

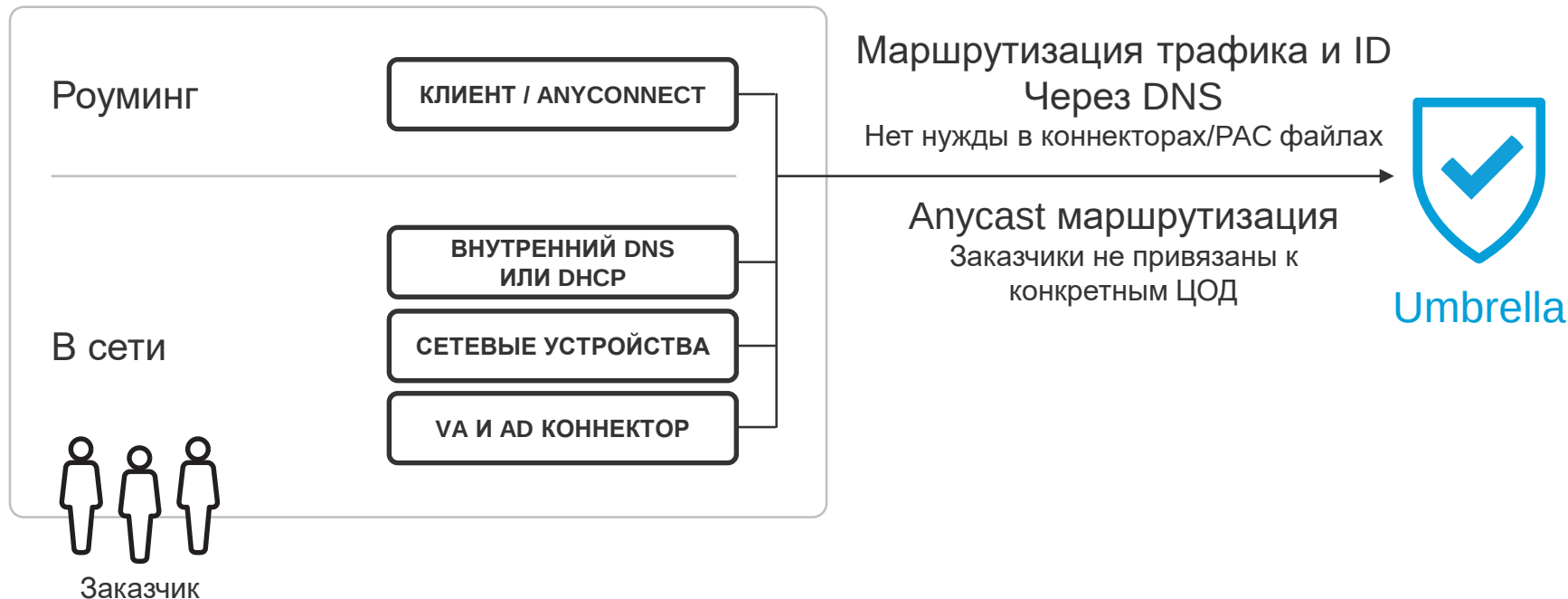


IP Маршрутизация с Anycast для отказоустойчивости

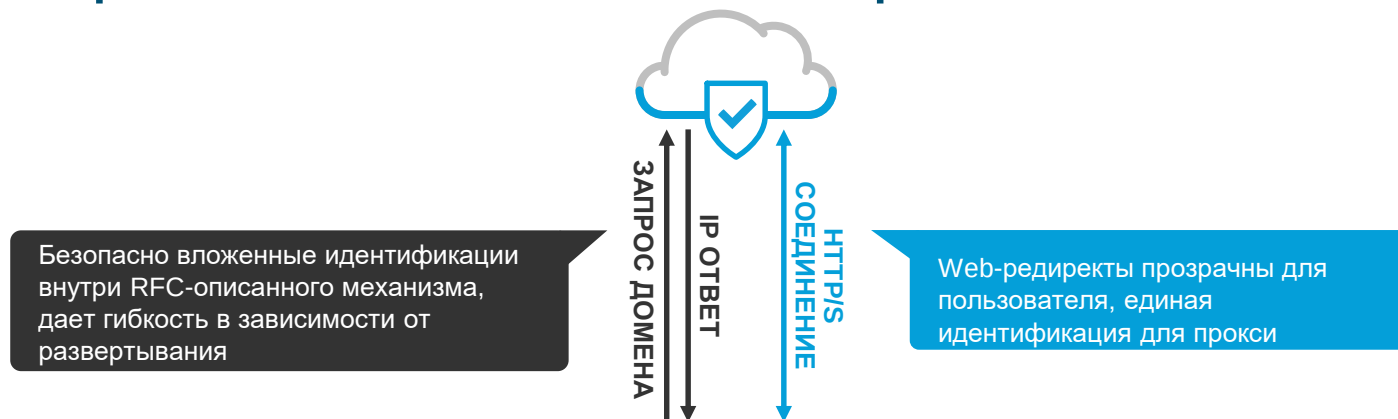
Если отказ произошел по любой из причин, автоматически происходит перемаршрутизация на следующий ближайший



Соединяемся с Umbrella



Фильтрация и видимость с привязкой к объектам



NETWORK VIA EGRESS IP FOR ALL DEPLOYMENTS

Umbrella Развертывания	 DNS или DHCP сервер заказчика	 Umbrella роуминг клиент (RC)	 Umbrella AD Коннектор	 Umbrella виртуальный аплаенс (VA)	 Umbrella API для сетевых устройств
Umbrella Идентификации	N/A	Имя хоста (GA)	Пользователи с группами для RC и VA *	Внутренние IP	Имена сетевых устройств или VLAN ID
		Внутренние IP (LA)		Подсети	
		Имена пользователей* (LA)		Имена пользователей*	

*Показывает идентификацию, получаемую с использованием Umbrella AD Connector

Интеграция с Cisco сетевыми устройствами

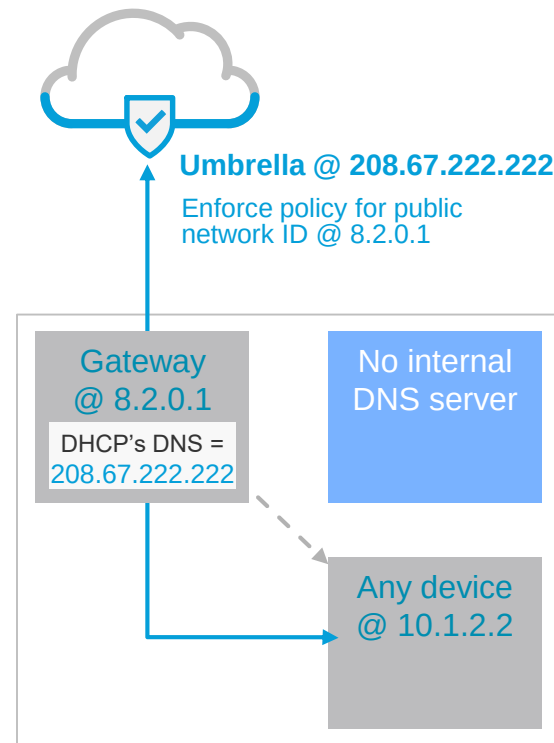
Защита для филиальных устройств и Wi-Fi пользователей



Защита внутри сети

DHCP Сервер – Для локаций без внутреннего домена

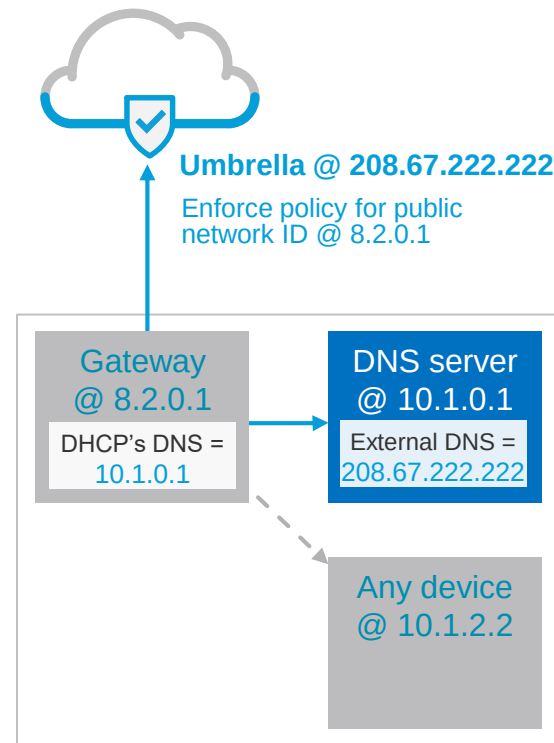
- Использует встроенный DHCP сервер в маршрутизаторе, коммутаторе, Wi-Fi точке, MCЭ, или Windows Сервер
- DNS IP адрес меняется на Umbrella
- Все устройства соединённые к сети будут указывать в DNS запросах на Umbrella
- Работает наилучшим образом если нет внутреннего домена, принтеров или внутренней сети, которой нужен локальное разрешение имен



Защита внутри сети

DNS Сервер – Для локаций где есть локальный домен

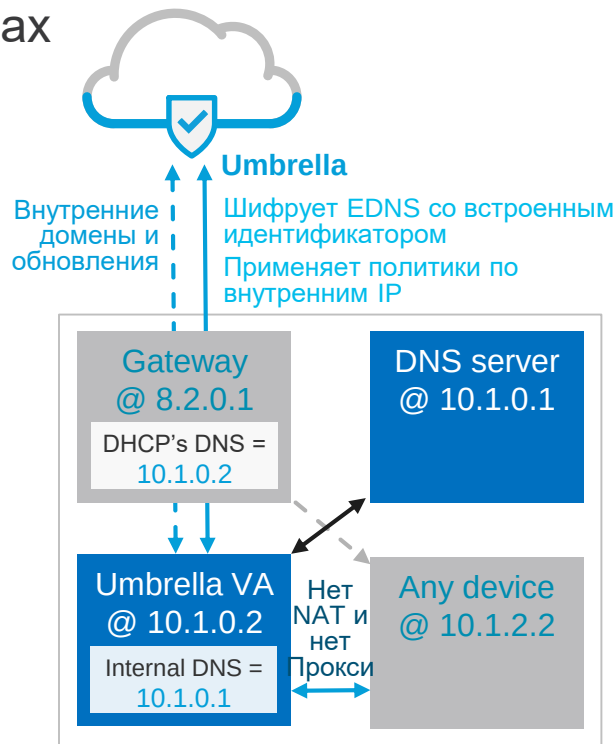
- DNS сервер (или любое устройство делающее разрешение имен) имеется на сети для внутреннего разрешения
- DNS сервер настроен для отправки всех внешних DNS запросов в Интернет домены на Umbrella
- В этом и предыдущем сценарии, политики контроля и видимости все еще ограничены публичным IP адресом сети.



Защита внутри сети

Umbrella Virtual Appliance – Для локаций требующих использования внутренних IP в политиках

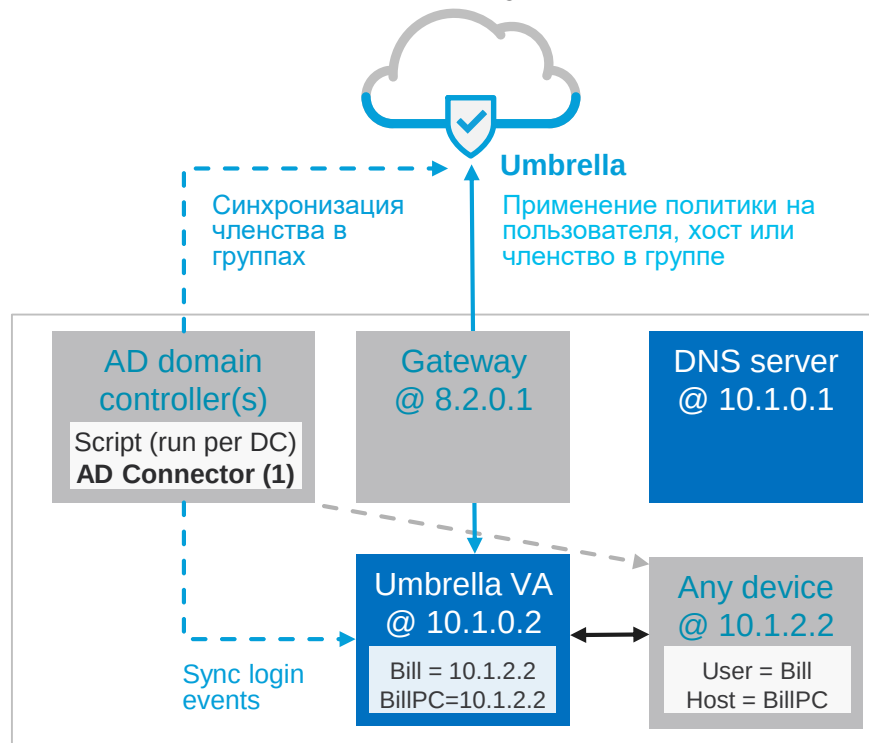
- Поддерживается для VMware и Hyper-V
- Внутренние/Внешние запросы отсылаются в VA
- Внутренние запросы разрешаются локально
- VA упаковывает внутренний IP с использованием RFC-совместимого расширения в DNS



Защита внутри сети

Virtual Appliance + AD Connector – Для детального контроля и глубокой видимости

- Домен-Контроллеры регистрируются на Umbrella
- Сервис коннектора устанавливается на DC/Контроллере:
 1. Синхронизирует членство в группах пользователей и компьютеров в Umbrella
 2. Отсылает соответствие IP->USER на Виртуальные Аплаенсы
- Виртуальный Аплаенс инкапсулирует уникальные идентификаторы, которые Umbrella использует в политиках и отчетах

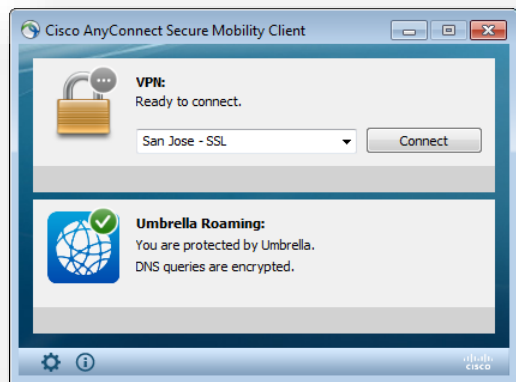


Защита мобильных пользователей

Более не слабое звено...

Если уже используется AnyConnect VPN...

- Установить последнюю версию AnyConnect
- Включить Umbrella Roaming модуль



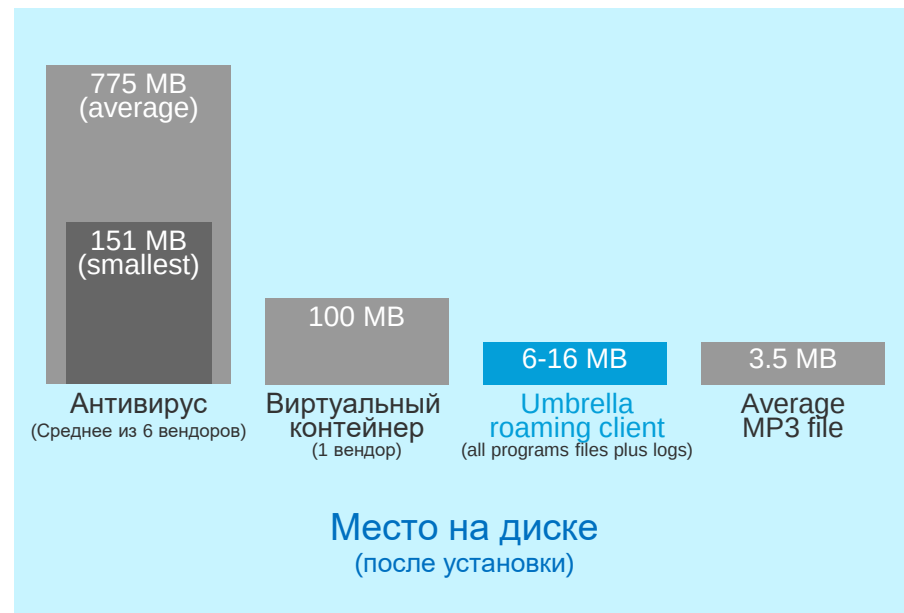
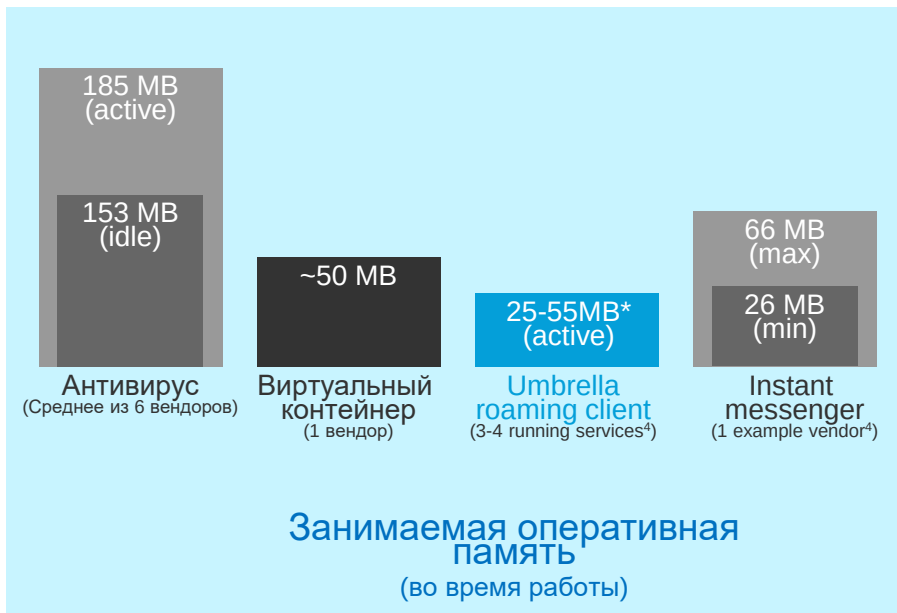
Если не используется AnyConnect...

- Установите Umbrella roaming client
- Отдельный облегченный агент



Umbrella Roaming Клиент

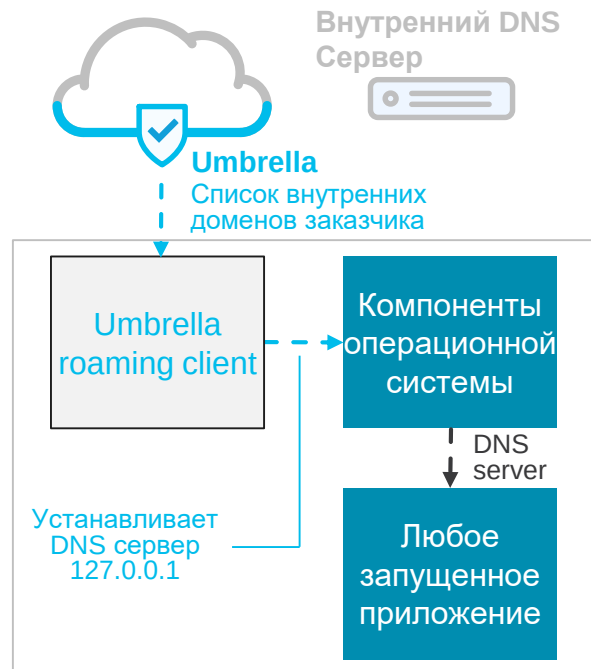
Мобильная защита с облегченным клиентом



Roaming Client

Защита за пределами сети, с использованием и без VPN

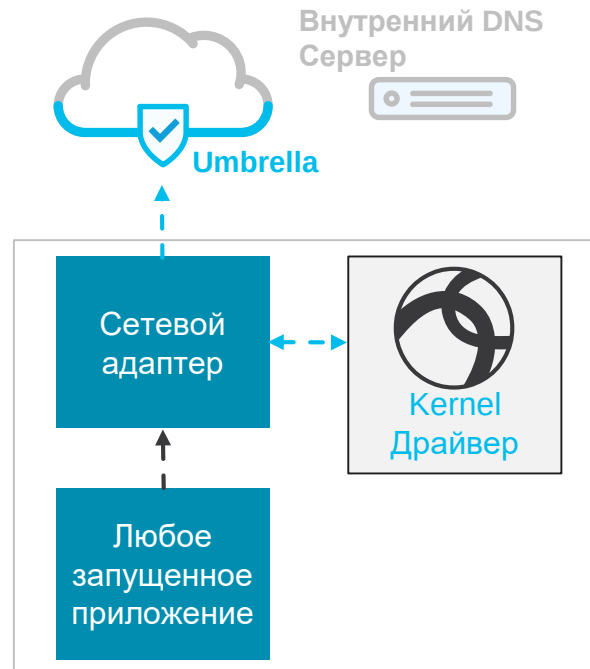
- Клиент наблюдает за изменениями на всех сетевых адаптерах и предоставляет DNS
- Все DNS запросы из любого запущенного приложения направляются на 127.0.0.1
- Клиент понимает какие доменные имена внутренние и их не надо разрешать за пределами сети



AnyConnect

Защита за пределами сети, с использованием и без VPN

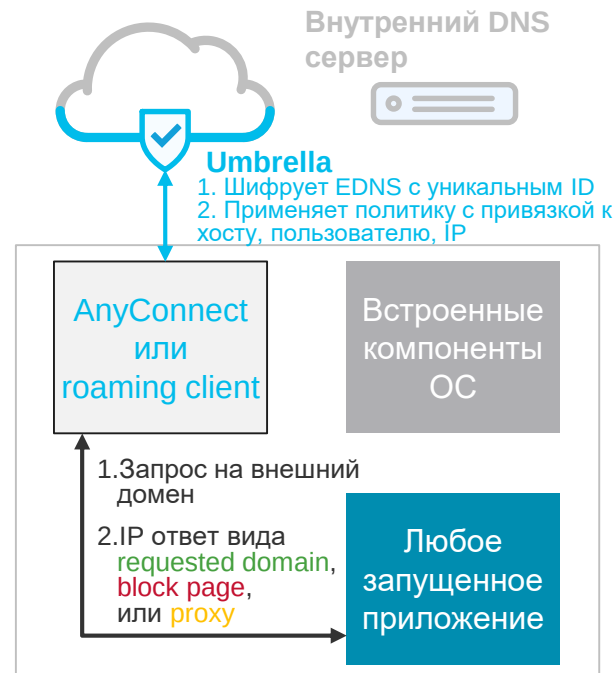
- Захватывает весь локальный трафик DNS прозрачно и перенаправляет от уровня Ядра ОС в Umbrella (Используя AC Kernel драйвер)
- Поддерживается как при включенном, так и при выключенном VPN
- Поддерживает опциональные бинарные обновления (для всех AC модулей) без необходимости в ASA головном устройстве



AnyConnect и Roaming клиенты

Внешние (Интернет) домены разрешаемые в Umbrella

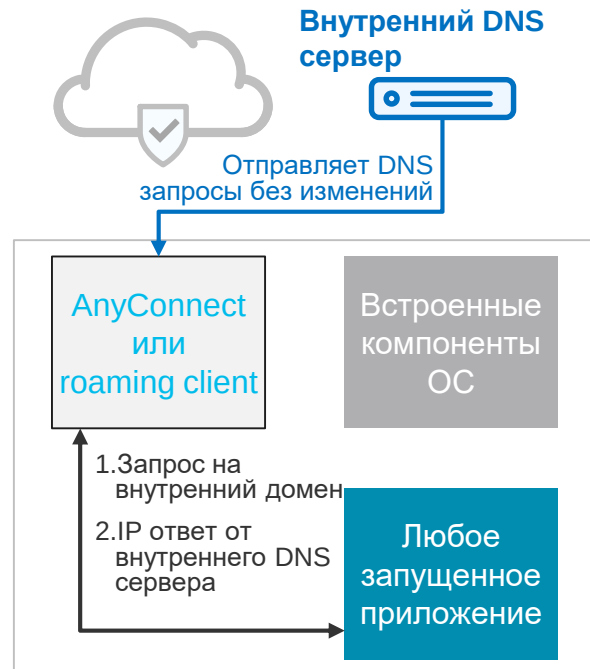
- Для доменного имени из Интернет, клиент включает в DNS запрос уникальный идентификатор клиента, который совпадает с именем запрашивающего хоста
- Клиент также шифрует DNS запрос для предотвращения MITM в публичных сетях (может отключаться при включении VPN до доверенной сети)



AnyConnect и Roaming Client

Внутренние (интранет) домены разрешаются на внутреннем DNS сервере

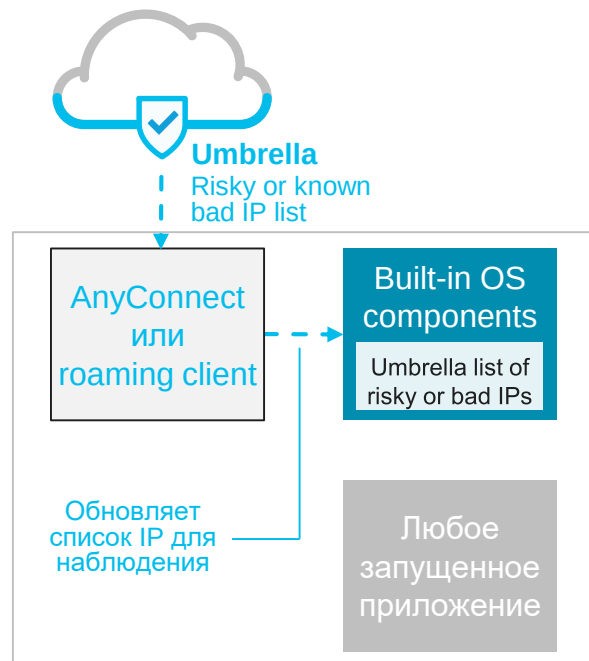
- Запросы на внутренние домены направляются на внутренние DNS сервера DNS без инкапсуляции идентификатора или шифрования запроса
- Клиент не конфликтует с внутренними DNS серверами



Фильтрация на уровне IP

Клиент постоянно получает обновляемые списки IP адресов и ОС наблюдает за подпадающим под критерии трафиком

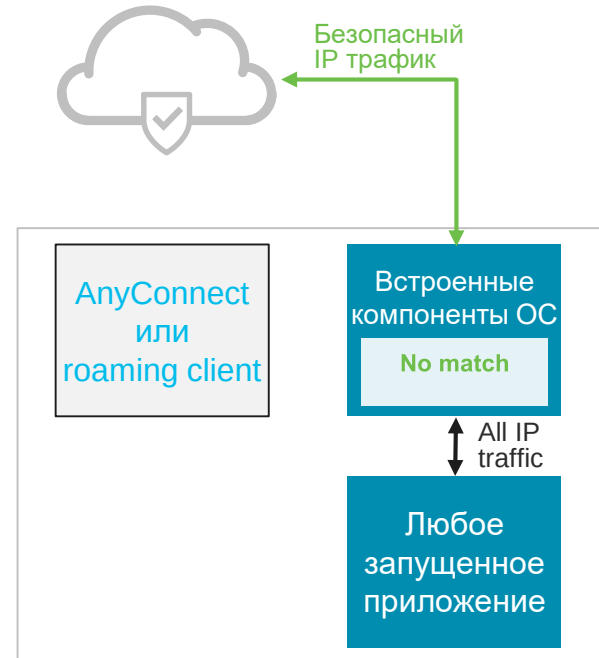
- Umbrella использует roaming client постоянно обновляет список подозрительных IP
- Исследователи Cisco обнаруживали вредоносную активность направленную к данным IP адресам без DNS запросов
- Используя встроенный сетевой стек в ОС, roaming client инструктирует на наблюдение за активностями, направленными к данным адресам



Фильтрация на уровне IP

Большая часть трафика маршрутизируется напрямую в Интернет

- В нормальной ситуации сетевой стек просто отошлет безопасный трафик в Интернет



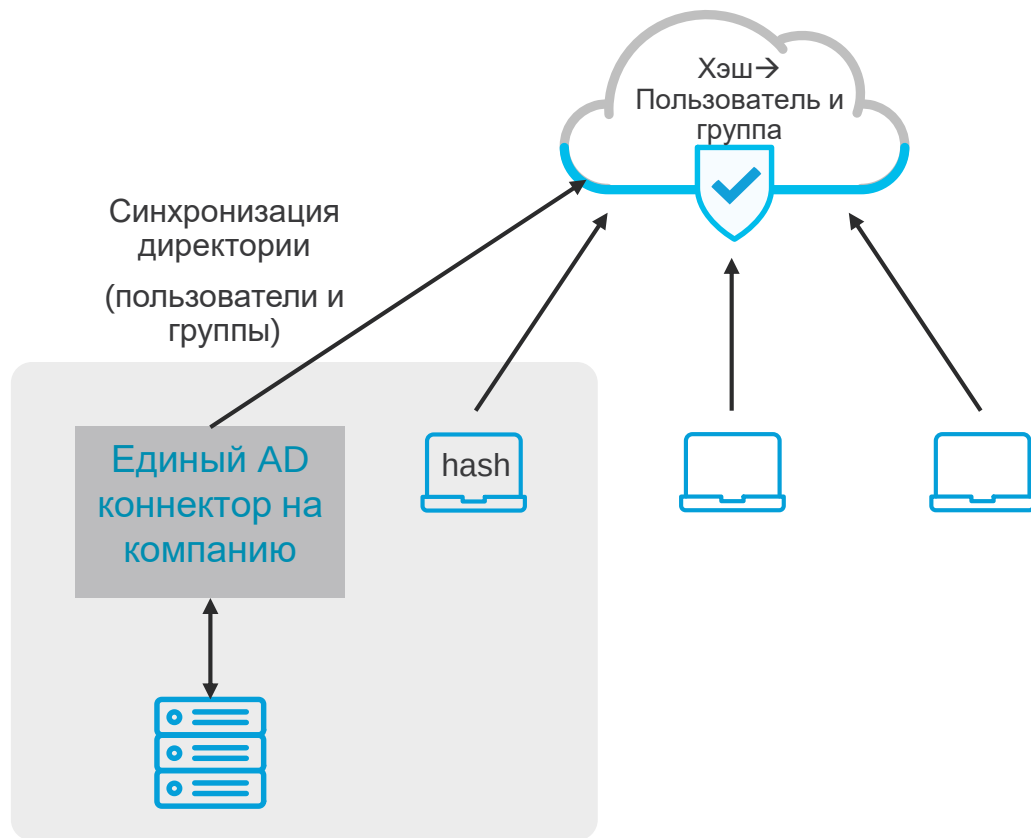
Фильтрация на уровне IP

Часть трафика туннелируется через Umbrella

- Но если срабатывает правило, оно инструктирует клиент мгновенно добавить этот адрес в встроенный IPsec VPN, который туннелирует это соединение в облако Umbrella
- Umbrella либо заблокирует соединение основываясь на IP, или соединение будет проксировано и только плохие URL заблокированы

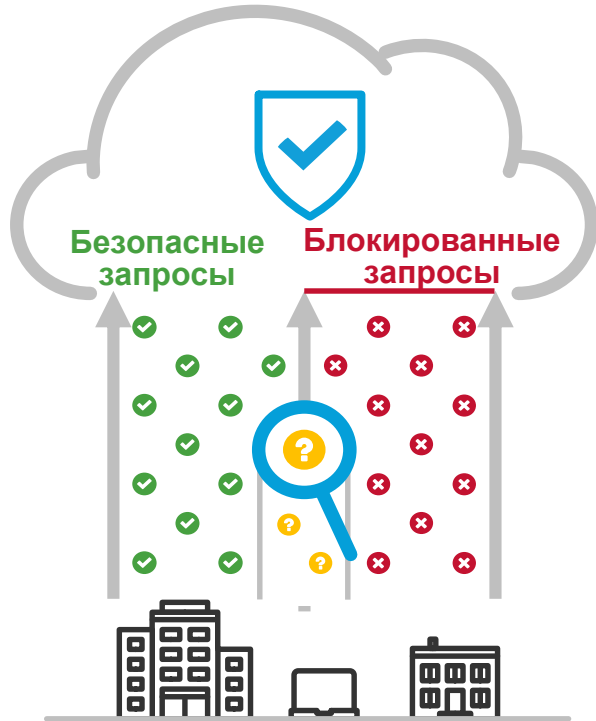


Идентификация пользователя с AC и RC



- AD коннектор синхронизирует информацию о пользователях и группах из AD
- Данные отсылаются в Umbrella
- AC/RC получает имена залогиненных пользователей и добавляет их как зашифрованный хэш в EDNS
- Umbrella сопоставляет имя и добавляет групповые детали
- Тот-же механизм при использовании внутри и снаружи сети

Поток данных - итог



- DNS запрос отсылается в Umbrella
- Для безопасных запросов, которые не блокируются политикой, возвращается корректный IP адрес
- Запросы к вредоносным или запрещенным ресурсам перенаправляются на страницу блокировки (хозящуюся либо в Umbrella либо в компании)
- Запросы в неизвестные направления, или те что были помечены как требующие дополнительной инспекции будут перенаправлены на intelligent проху для дальнейшего анализа

Блокировка на лету, Аналитика офлайн

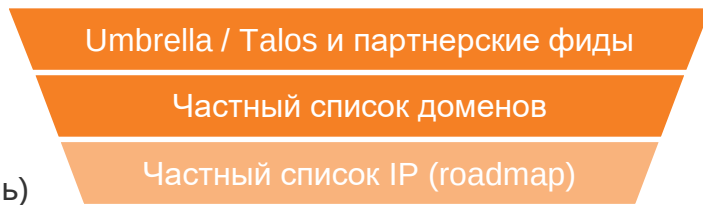
Широта покрытия всех портов и глубина инспекции рискованных доменов

Блокировка на лету

Офлайн аналитика

DNS и IP уровень

- Запрос Домена
- IP ответ (DNS-уровень)
или соединение (IP- уровень)



РАЗРЕШИТЬ, БЛОКИРОВАТЬ ИЛИ PROXY

ПРЕДИКТИВНЫЕ ОБНОВЛЕНИЯ



UMBRELLA
STATISTICAL
MODELS

ТЕЛЕМЕТРИЯ ВСЕГО ИНТЕРНЕТ

HTTP/S уровень

- URL запрос
- Хэш файла



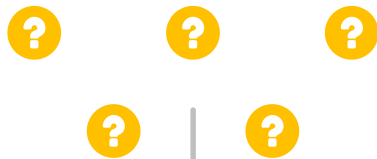
РАЗРЕШИТЬ, БЛОКИРОВАТЬ ИЛИ АНАЛИЗИРОВАТЬ

НЕИЗВЕСТНЫЕ ФАЙЛЫ (ROADMAP)



AMP
THREAT
GRID

Интеллектуальный Прокси



Запросы на “рискованные” домены

URL инспекция

Cisco Talos Фиды
Cisco WBSR
Партнерские фиды

Файловая инспекция

AV Движки
Cisco AMP



Простота и Видимость

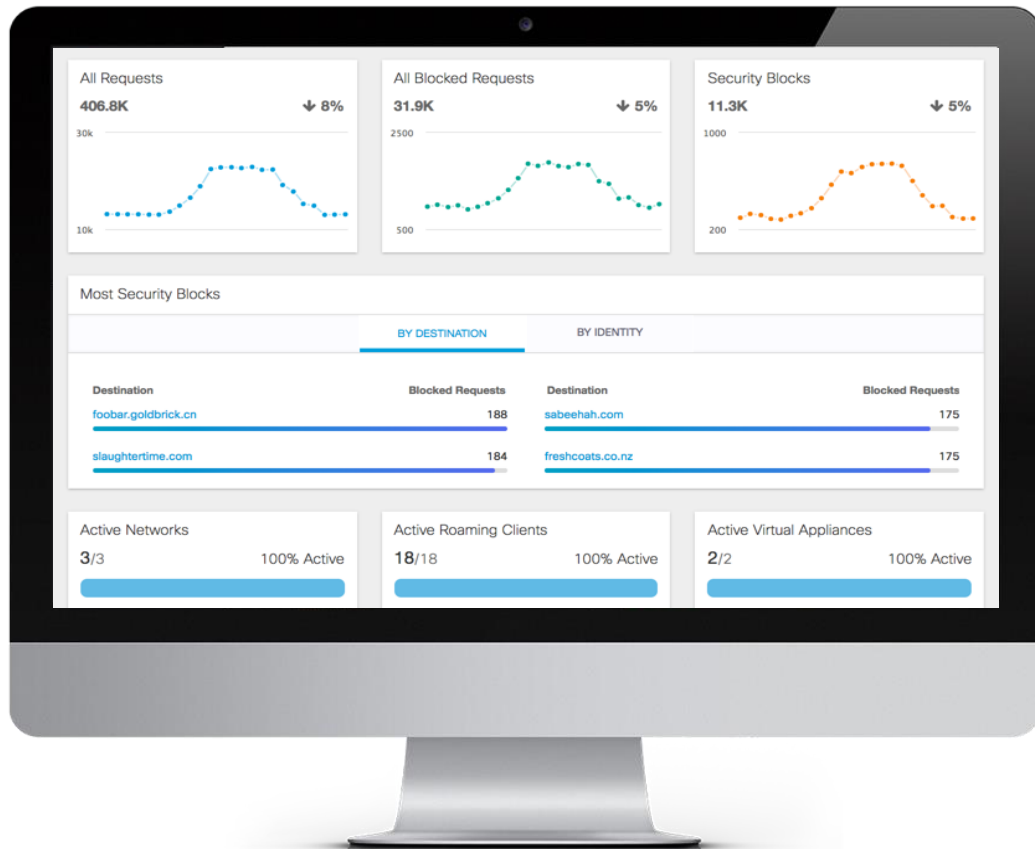
Обзорная страница:

Фокусируемся на недавних событиях безопасности или проблемах развертывания

Отчеты по идентификации и направлениям: Быстрая навигация для большей детализации

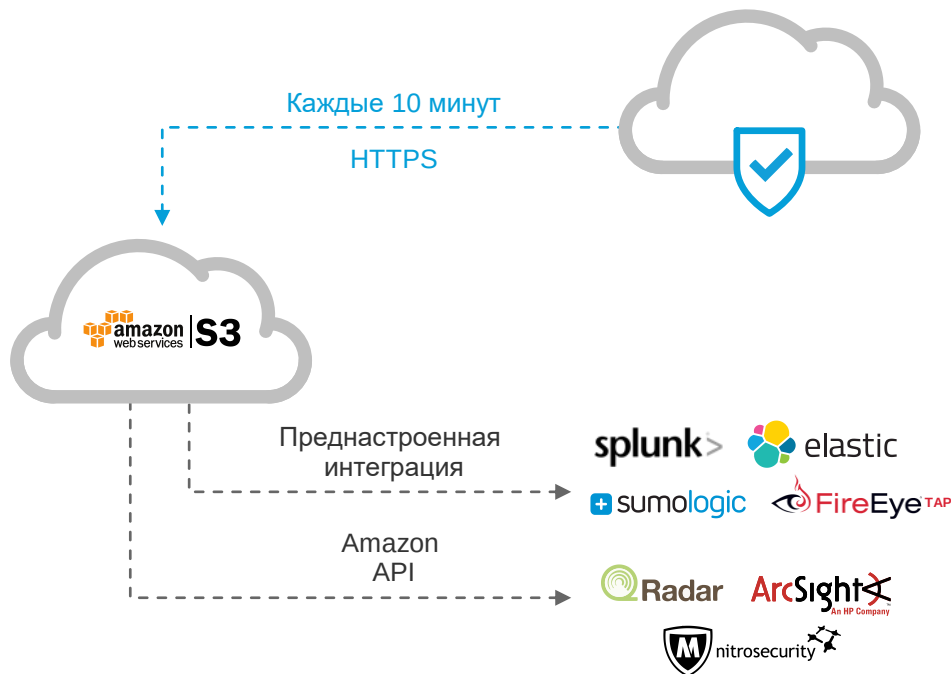
Обзор активностей и событий безопасности:

Показывает еще больше данных (DNS, IP, proxy) с простой фильтрацией запросов



Cloud-to-Cloud хранение логов

С использованием Amazon S3



S3 Преимущества

Тройное резервирование и шифрование хранилища

Преднастроенная интеграция SIEM / log аналитики логов

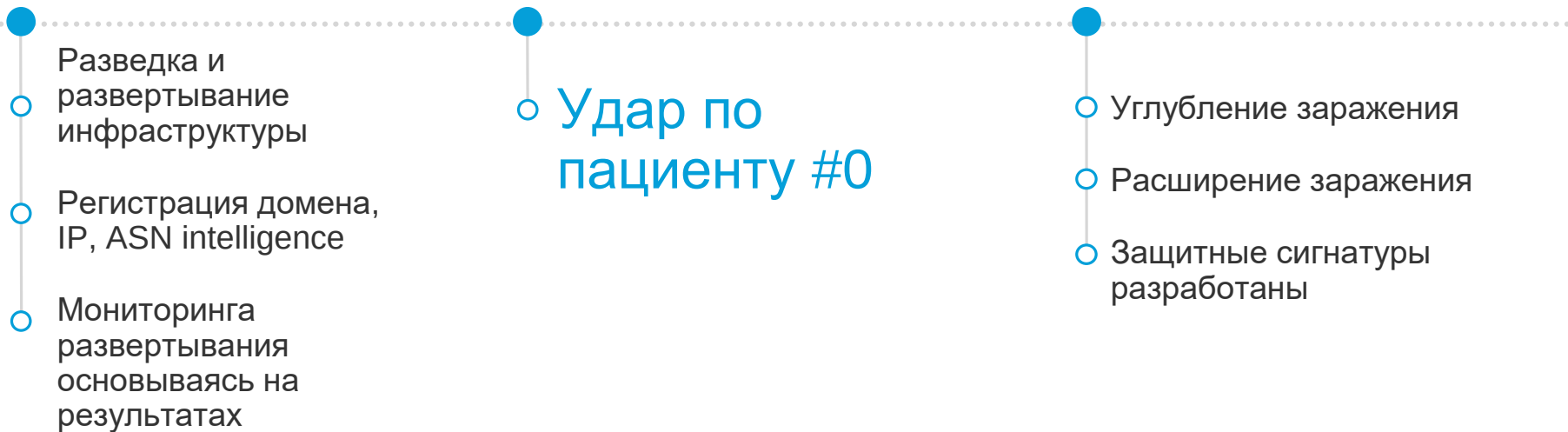
Гибкость: Оплата только за используемое хранилище

Программа

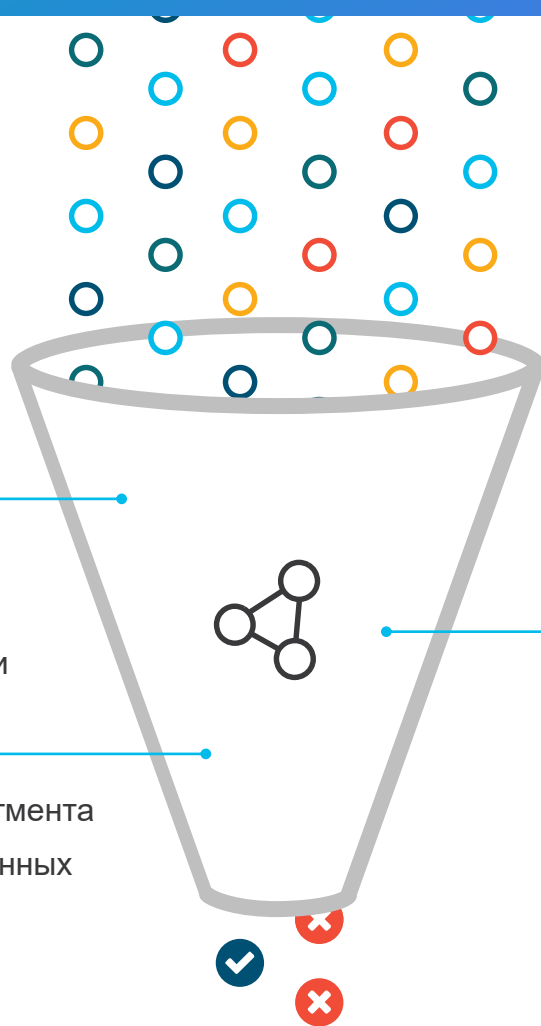
- Вступление
- Что такое Cisco Umbrella
- Архитектура и потоки данных
- **Статистические модели**
- Заключение



Анатомия кибер атаки



Статистическое моделирование



2M+ событий в секунду

11B+ исторических событий

Виновен по поведению

- Модель совместных запросов
- Геолокационная модель
- Модель индекса безопасности

Виновен по связям

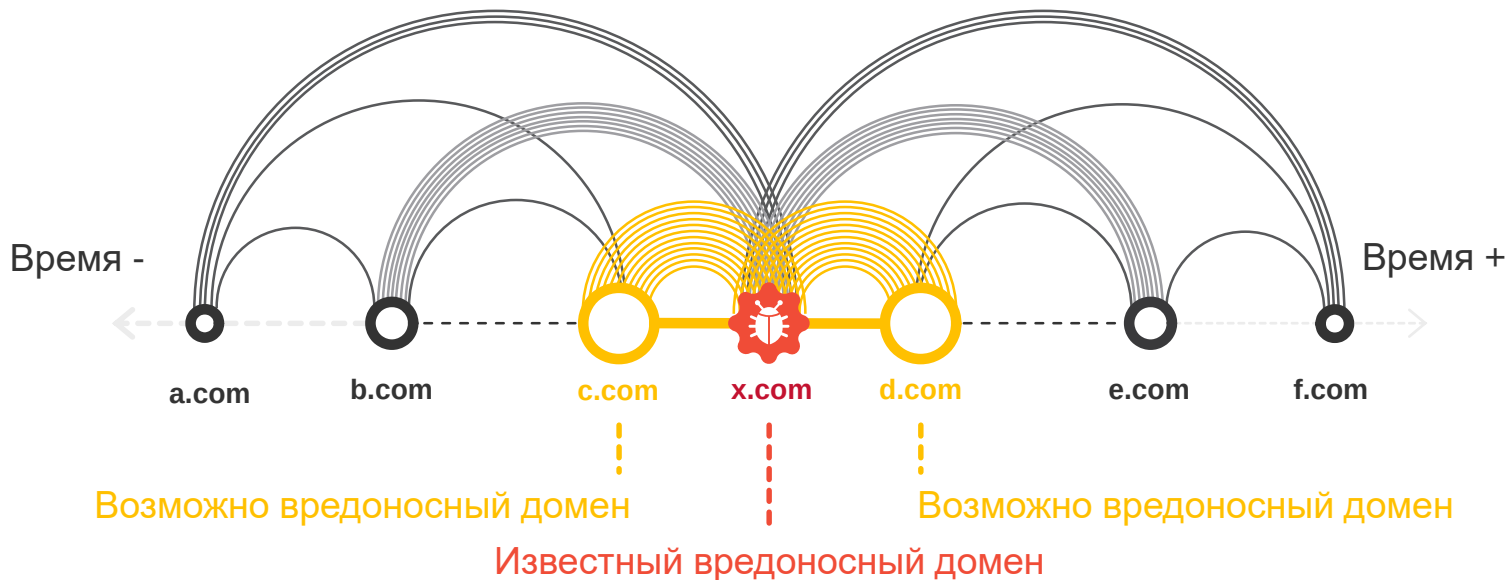
- Модель предсказуемого IP сегмента
- Корреляция DNS и WHOIS данных

Шаблон виновности

- Модель всплесков активности
- Модель оценки языкового шаблона (NLP)
- Обнаружение DGA

Модель совместных запросов

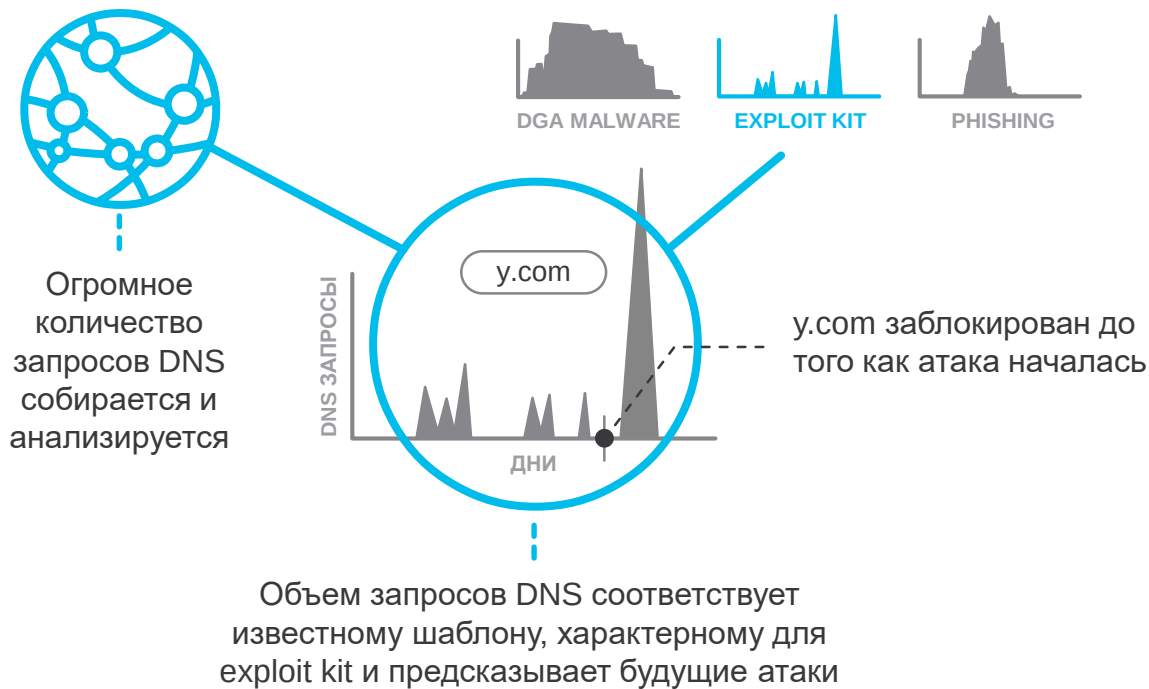
Домены виновные по модели связанных вызовов



Совместное появление доменов означает что статистически значимое количество хостов запросило оба домена одновременно в короткий промежуток времени

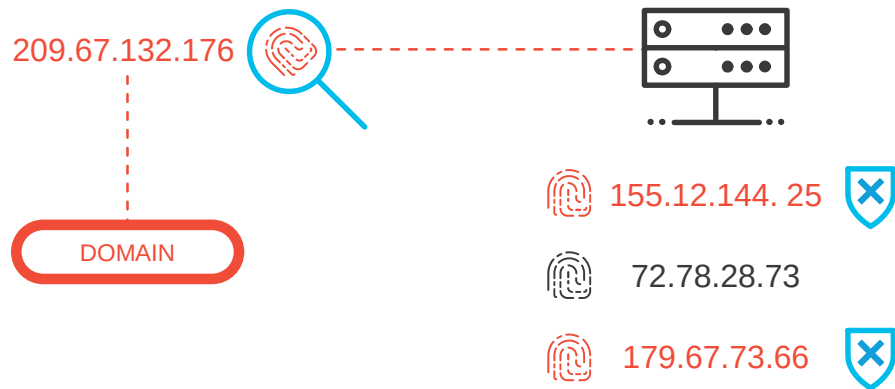
Модель всплесков активности

Шаблоны виновности



Мониторинг предсказуемого IP сегмента

Виновен по ассоциации



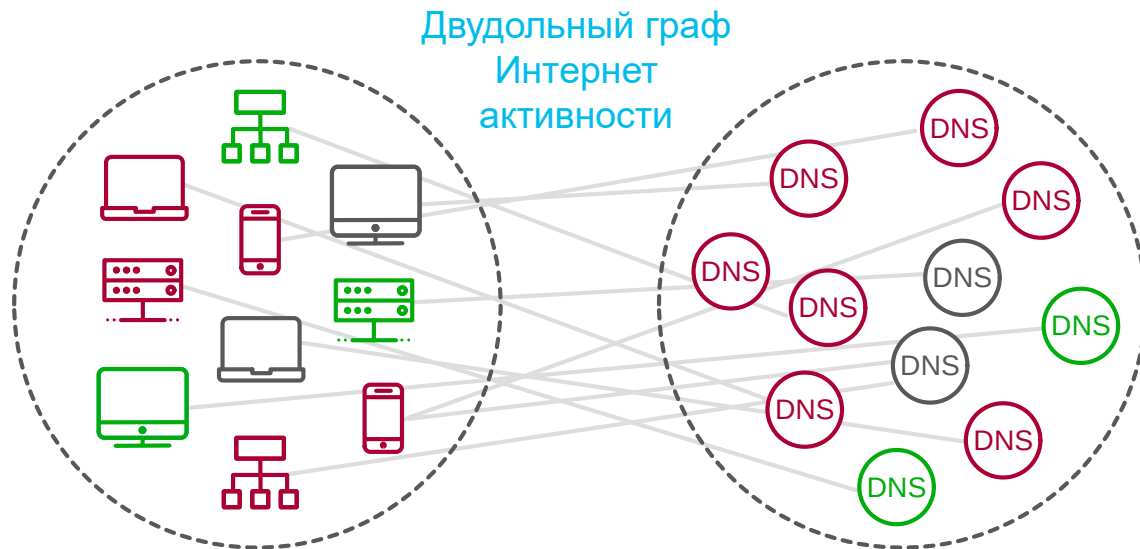
Обнаруживает подозрительные домены, и изучает их IP отпечатки

Идентифицирует другие IP (хотя бы на том же сервере) которые имеют схожие отпечатки

Блокируем эти IP и их ассоциированные домены

Ранжирование по уровню безопасности

Destinations (Домены, IP) Виновные по связям



Хороший, Плохой или Неизвестный
DNS запросы в связи с Идентификацией

Хороший, Плохой или Неизвестный
Репутационный индекс DNS “Соседства”

Модель языкового моделирования (NLPRank)

Идентификация вредоносных доменов и направленных C2 или фишинговых доменов

1

Читаем АРТ отчет



2

Шаблоны в доменах используемых для атаки

- Подлог домена использован для спуфинга
- Частые имена брендов и слово “update”
- Примеры:
update-java[.]net
adobe-update[.]net

3

Проверили данные и подтвердили опасения

- Словарные слова и имена компаний слитно
- Измененные строчные буквы # на символы для сокрытия
- Домены hostятся на ASNaх не ассоциированных с компанией
- Изменённые отпечатки WEB страниц

4

Построили модель и продолжаем подстройку

Обнаружение доменов для фрода:

✗ 1linkedin.net

✓ linkedin.com

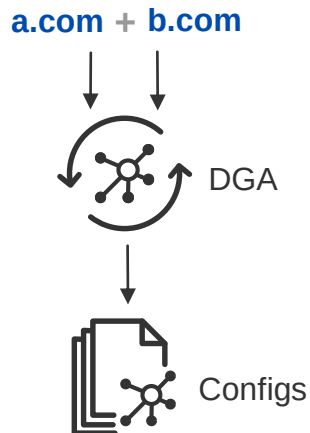
Предугадывание DGA на лету

Автоматизация в большом масштабе



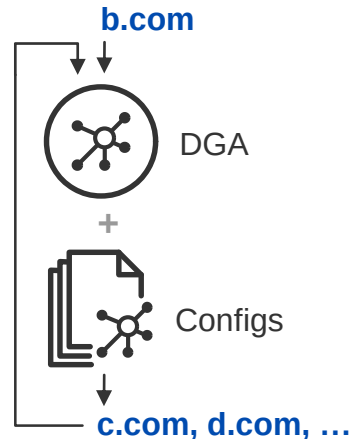
Живой DNS поток логов

Идентификация миллионов доменов, многие используются DGA и не регистрируются



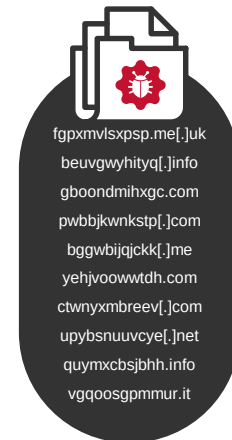
Автоматизированный Реверсинг

Комбинация C2 доменных пар и известных DGA для идентификации неизвестных конфигураций



Предугадать >100,000 будущих доменов

Комбинирование вновь идентифицированных конфигурации DGA с C2 доменами



Автоматическое блокирование пулов C2 доменов

Используется тысячами вредоносных сэмплов сегодня и в будущем

IP ГЕО-локационный анализ

Хостится в более чем 28+ странах



ХОСТ ИНФРАСТРУКТУРА

Расположение сервера
IP адреса связанные с
доменом

Только заказчики из US связываются с .RU
TLD



DNS ЗАПРОШИВАЮЩИЕ ХОСТЫ

Расположение сетевые и вне-сетевые
IP адреса запрашивающих домен

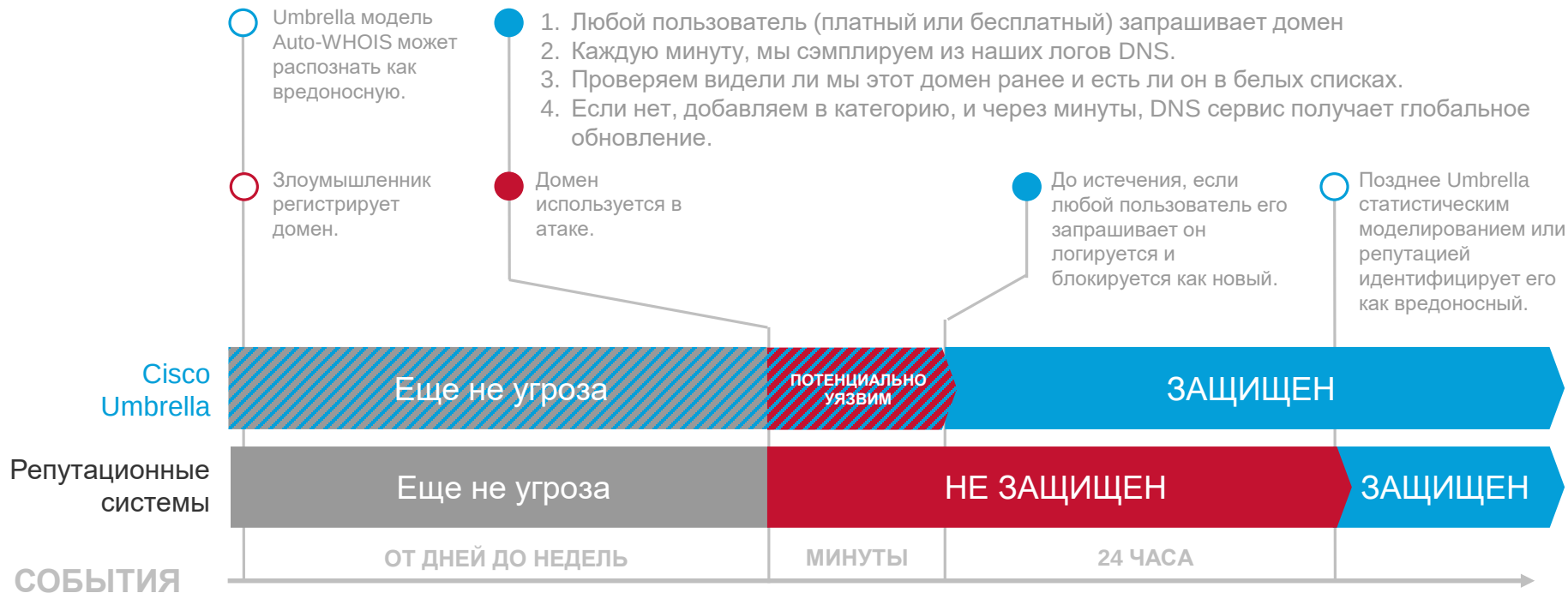
Ранжирование отправителя

Использование анти-спам данных о доменах



‘Newly Seen Domains’ Категория

Уменьшаем риск неизвестного

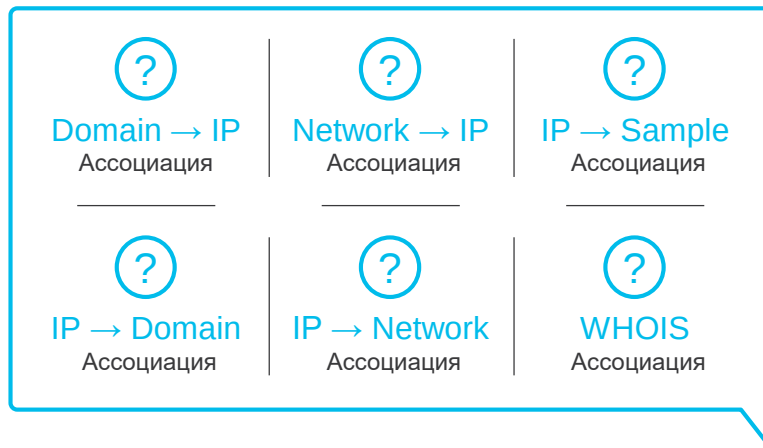


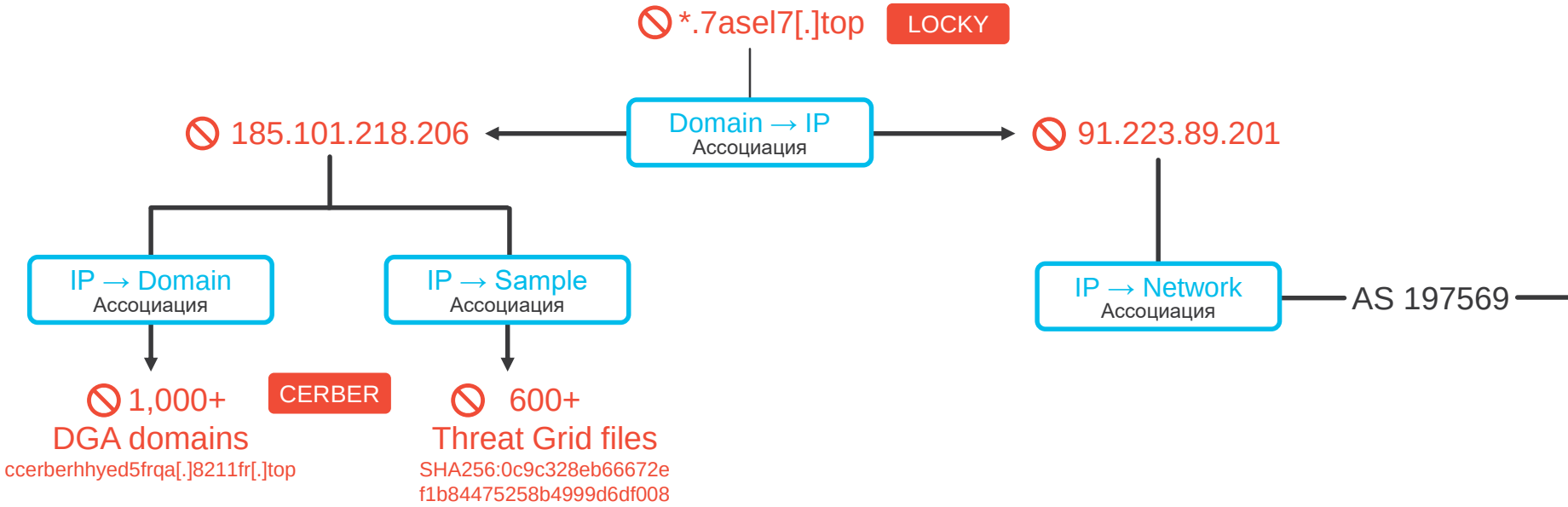
Новые типы Анализа и Категорирования

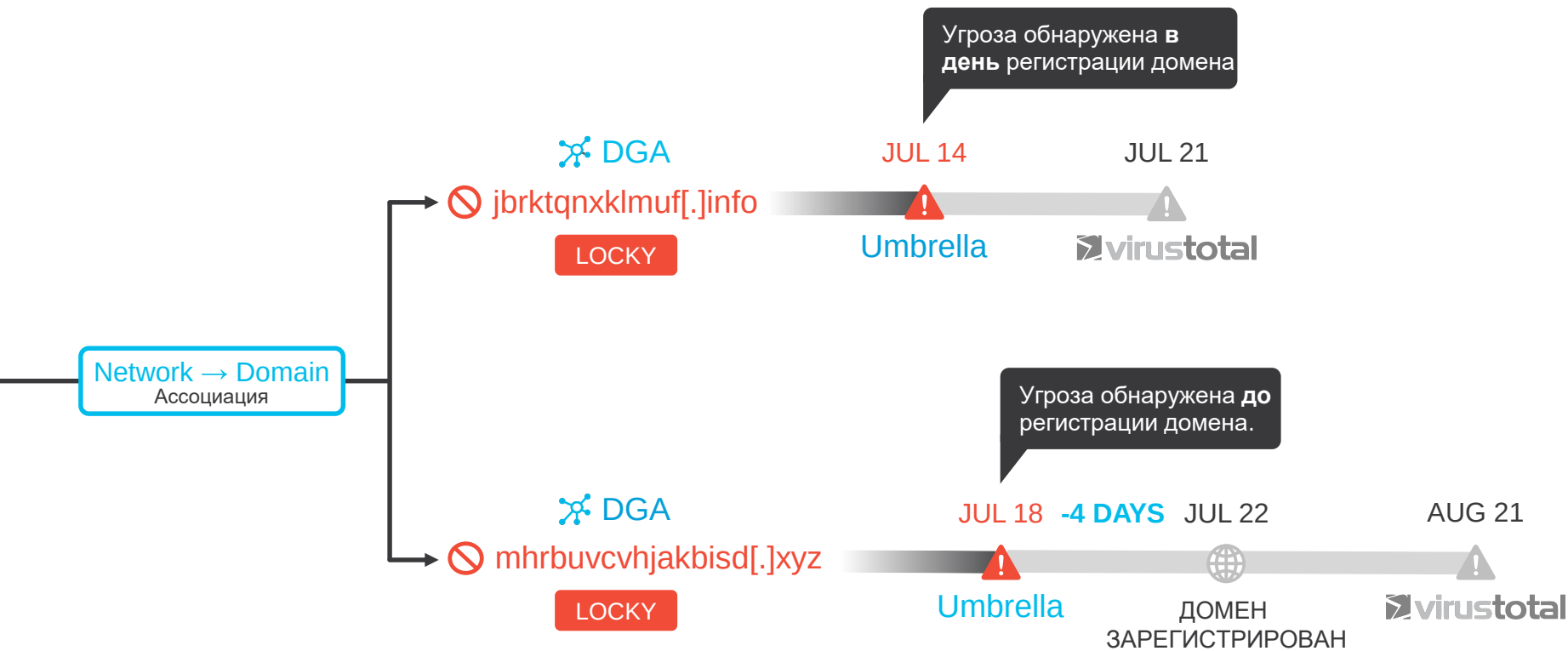
Борьба с DNS туннелированием



Ransomware: обнаружение инфраструктуры злоумышленника







Блокировка вымогателя

Locky: Реальный пример

Загрузка
Malware
URL

Cg3studio.com/87yg756f5.exe

rentmanager.ph

o.dolphin247.com

tadboxxers.com

210.151.131

la0lc9bba29d09fc762866862a43ad4802799a30a2b4a1708c7438ld8a29e16
0b1ld898fice9a980a854296alb3ld9f4b8bel744449d11cd64c792521lf6ea

Эти домены
Вызываются
поочередно

INVESTIGATE Visualize Back to top

CO-OCCURRENCES

tadboxxers.com (100.00)

RELATED DOMAINS

No info to display

soumya101@gmail.com

Email адрес
зарегистров
ан за доменом
инфраструктуре

2.215

ns-1418.awsdns-49.org

cg3studio.com

allinfo.xyz

sapanboon.com

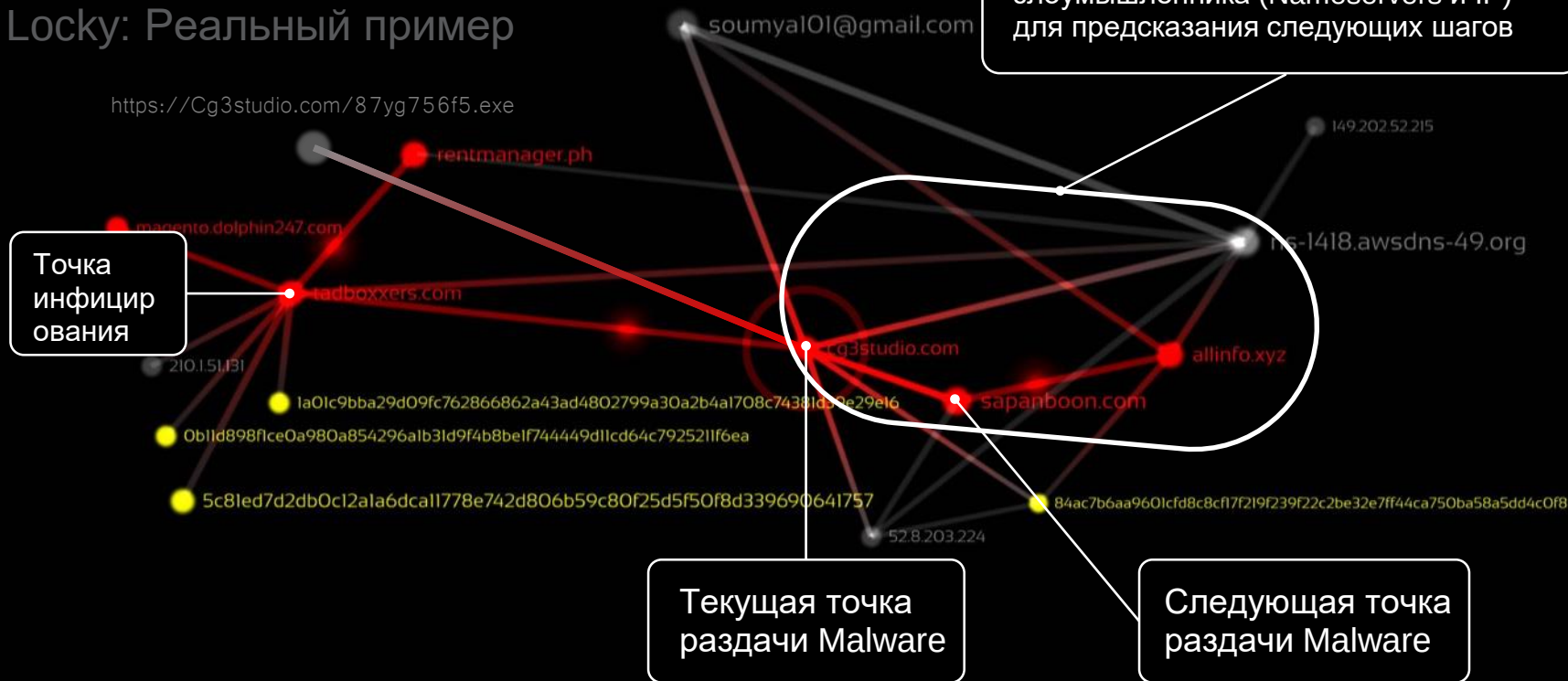
757

52.8.203.224

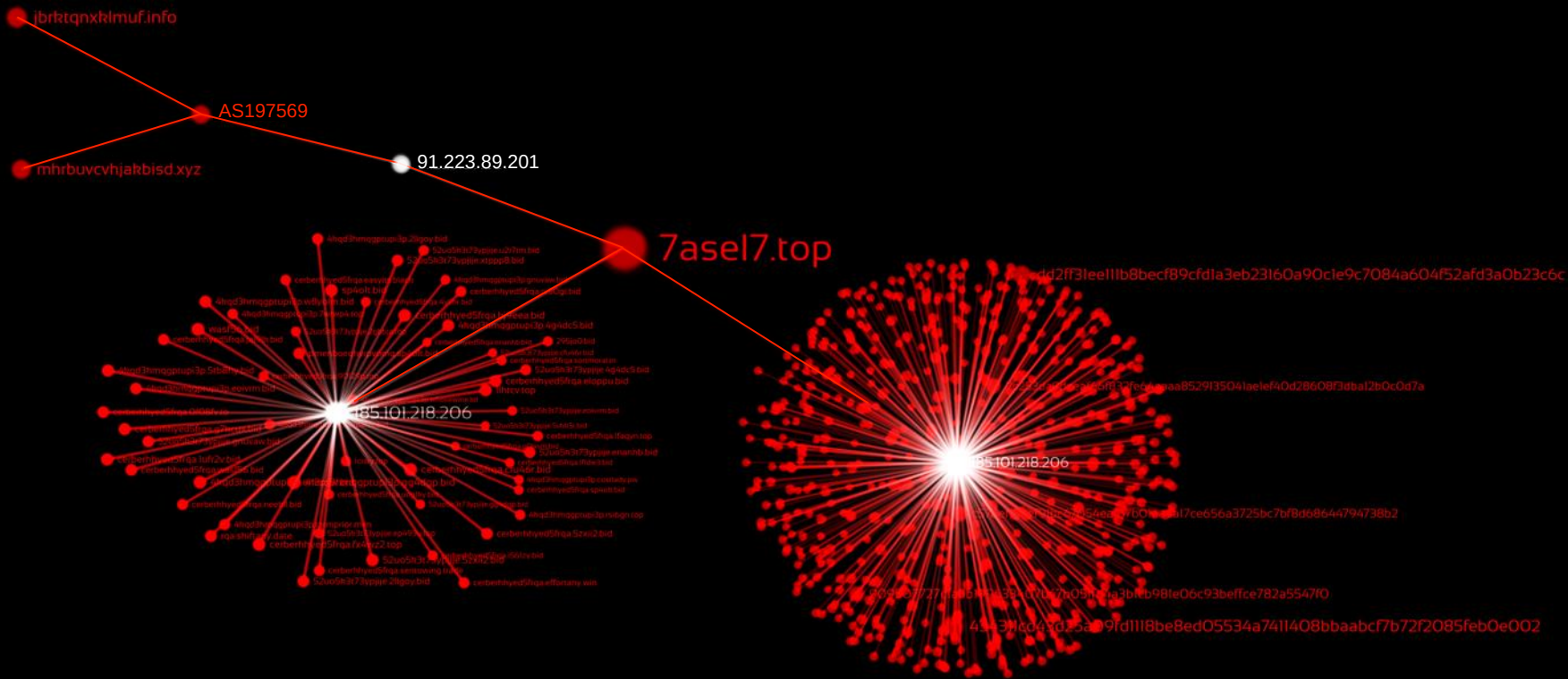
Домены красные
автоматически
блокируются
Хэш вредоносных
файлов загружаемых
с этих доменов
Umbrella

Локу: Реальный пример

Изучена инфраструктура
злоумышленника (Nameservers и IP)
для предсказания следующих шагов



Визуализация инфраструктуры нападающего



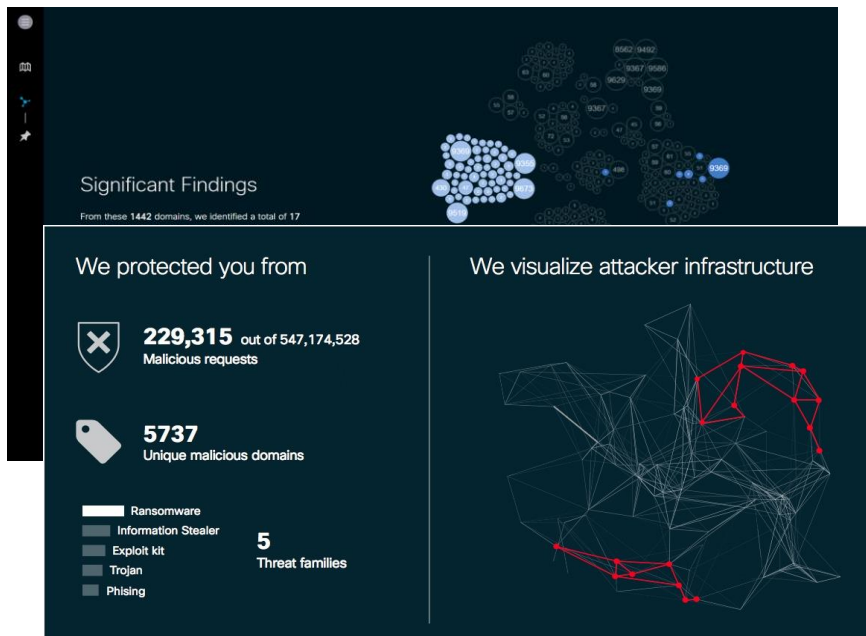
Программа

- Вступление
- Что такое Cisco Umbrella
- Архитектура и потоки данных
- Статистические модели
- **Заключение**



Самое простое тестирование из тех что Вы делали

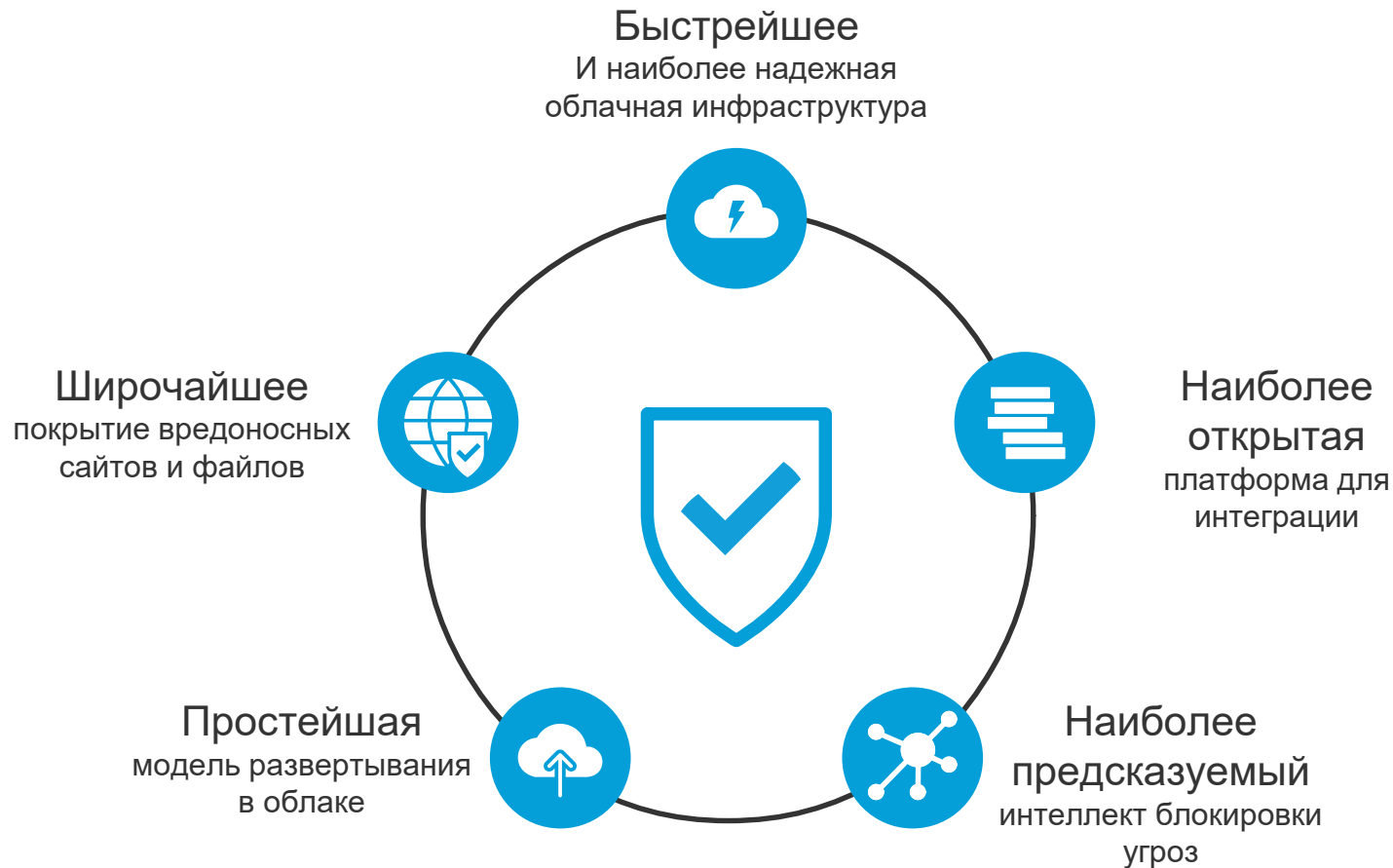
1. Подписаться 2. Указать DNS 3. Готово.



После тестирования вы получаете отчет, помогающий ответить на вопросы:

- Насколько эффективно данное решение?
- Как его можно сравнить (или добавить) к существующим решениям?
- Является ли оно эффективным инструментом экономящим время и приносящим пользу?

Umbrella Итоги





Спасибо!