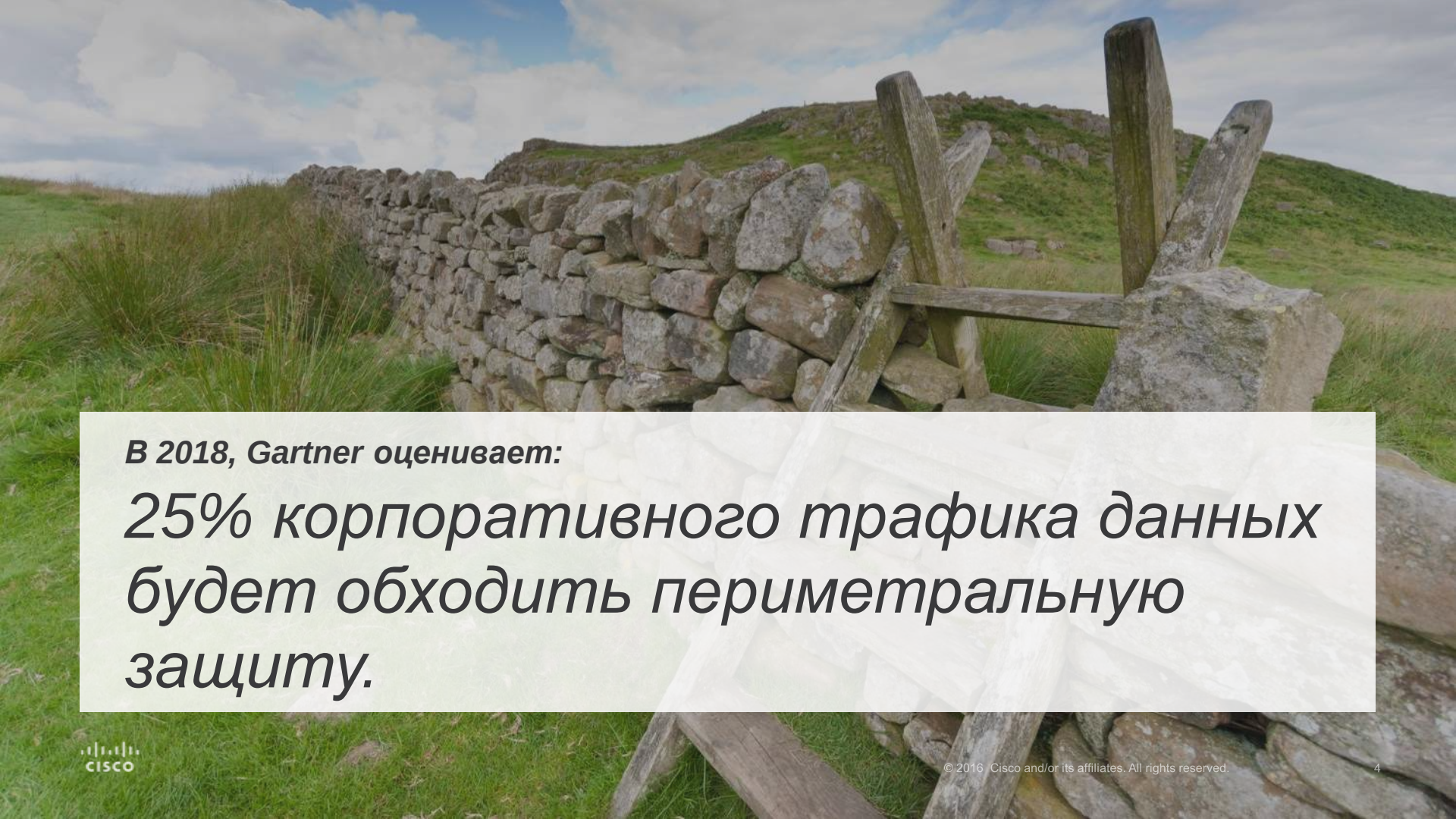

CISCO
SOFTPROM
by ERC
Cisco LabDay 2018
Минск, 26 апреля
#ciscolabday

Под зонтиком безопасности

Владимир Илибман
voilibma@cisco.com

Программа

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



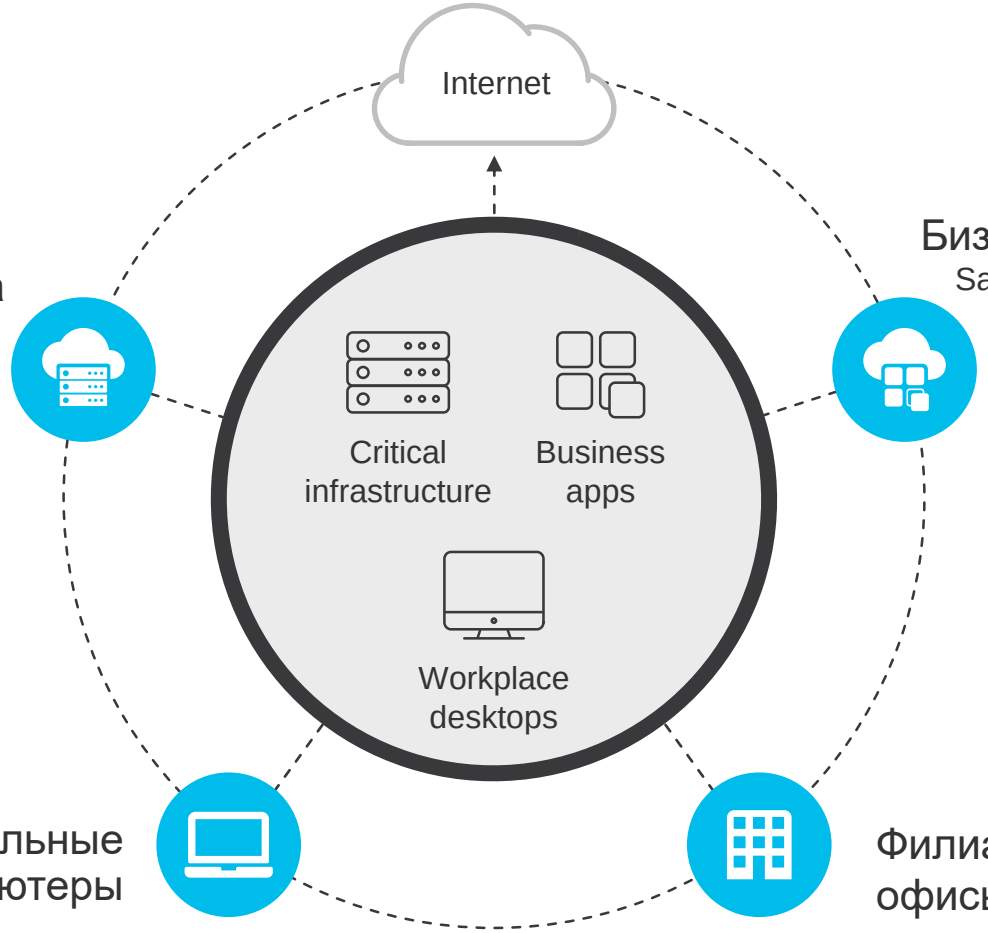
В 2018, Gartner оценивает:

25% корпоративного трафика данных будет обходить периметральную защиту.

Таким образом к 2019 (или даже быстрее)…

NGFW будут слепы к 25% трафика!

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…

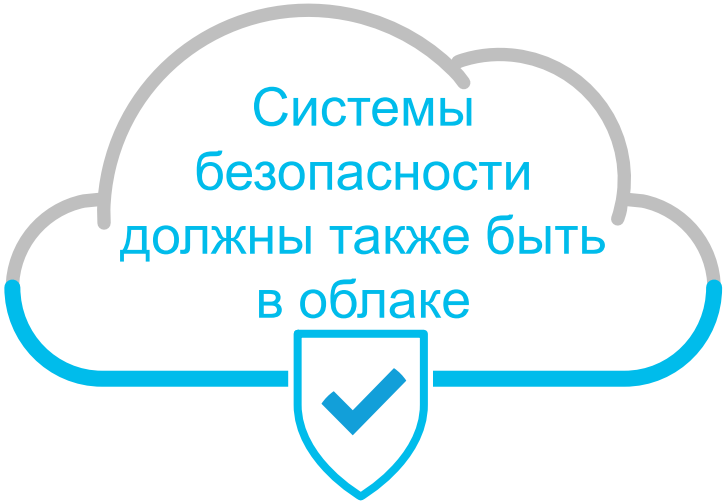
И безопасность также…

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

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

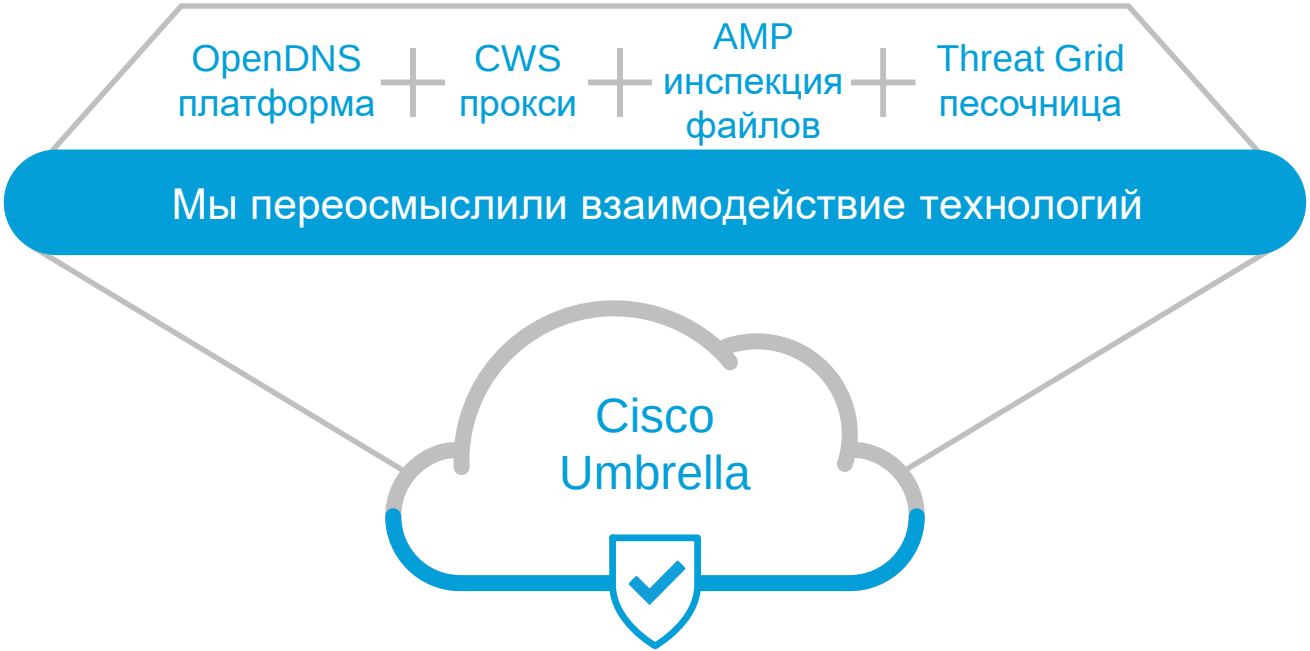
2016: Cisco Umbrella запущен!

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

Представляем Cisco Umbrella

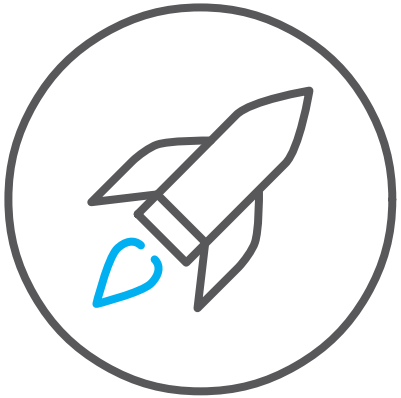
Из чего состоит Cisco Secure Internet Gateway



Umbrella отличается от других

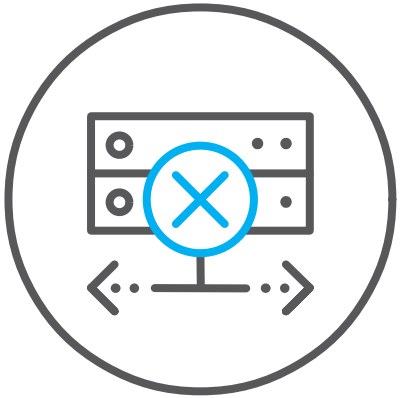
Концентрация на безопасности

Продуктивность не может быть достигнута контролем корпоративной сети



Простота развертывания и управления

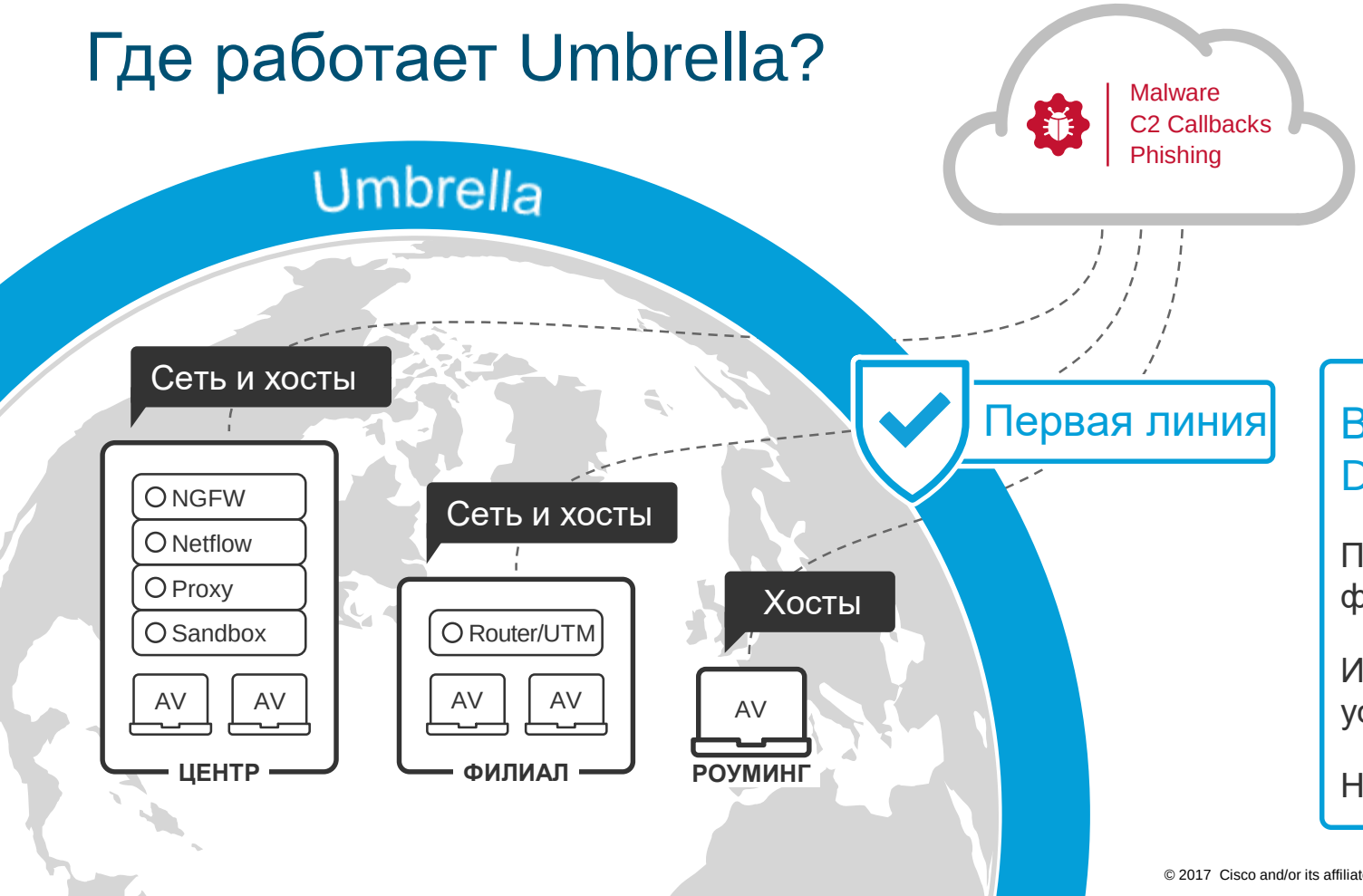
Использование DNS и подхода Cisco для простоты развертывания



Не нужно проксировать всё

Проксирование всего это проигрыш сражения, только добавляющий задержку

Где работает Umbrella?



Всё начинается с DNS

Предвосхищает открытие файлов и IP соединение

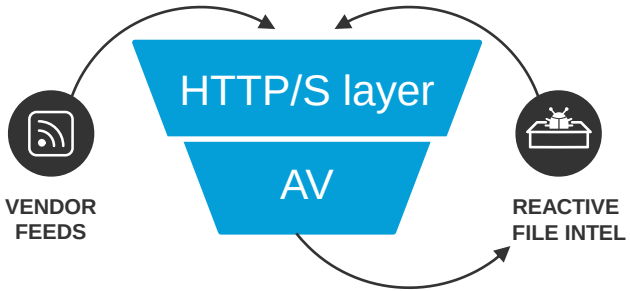
Используется всеми устройствами

Не зависит от порта

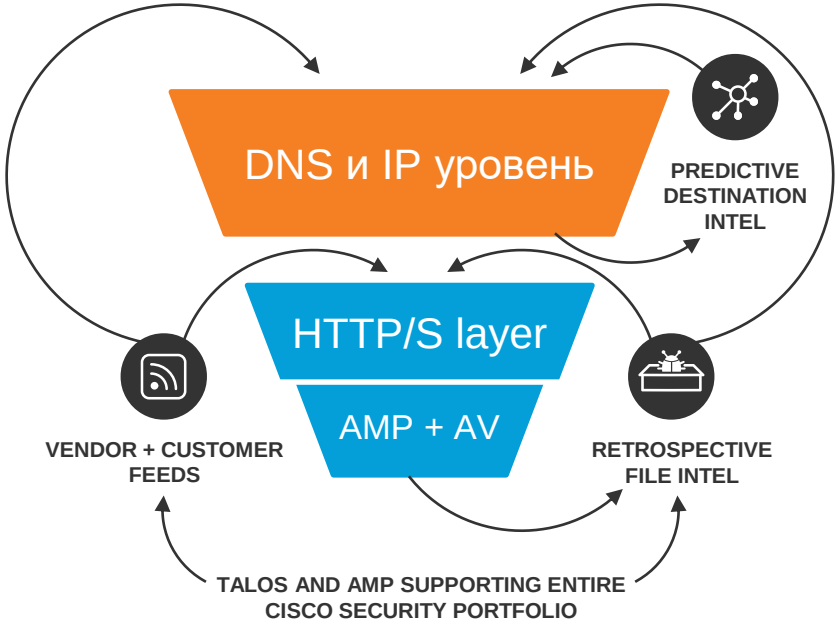
Cisco SIG в сравнении с другими Secure Web Gateway

SWG

Проблема:
Неполное покрытие направлений и файлов



SIG



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

Программа

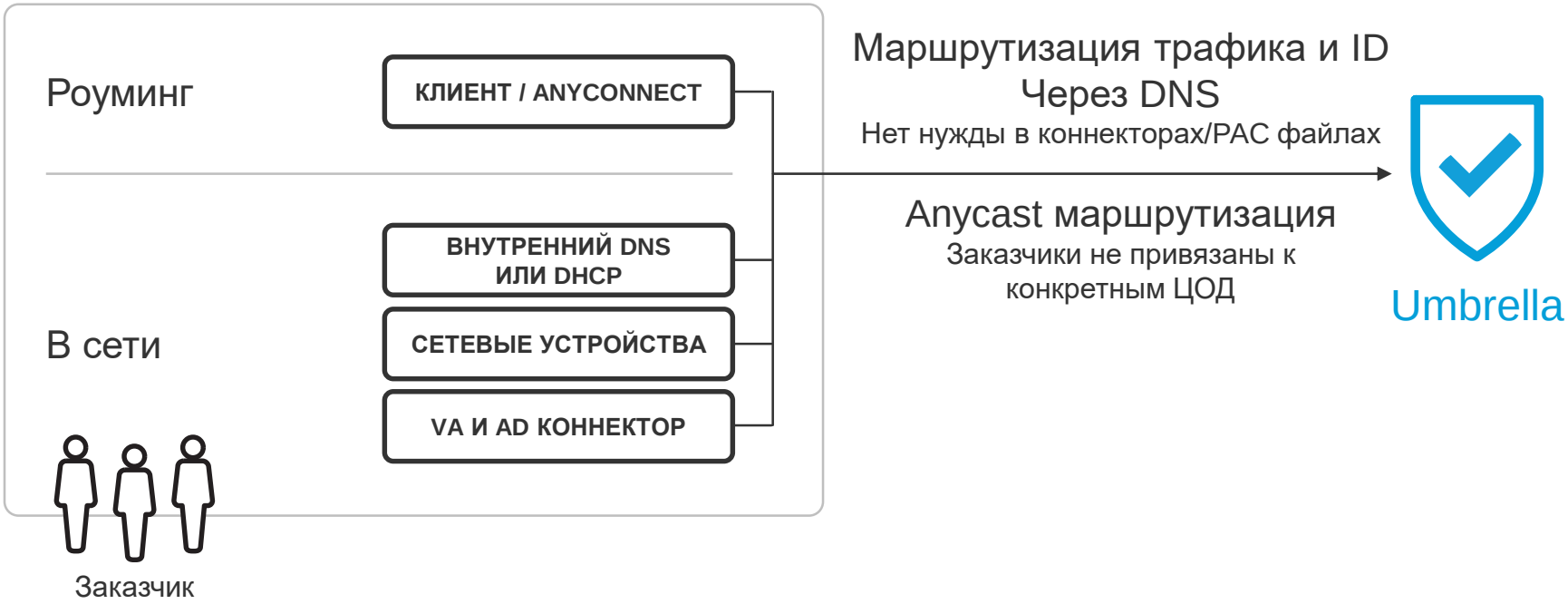
- Вступление
- Что такое Cisco Umbrella
- **Архитектура и потоки данных**
- Статистические модели
- Заключение

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

Соединяемся с Umbrella



Программа

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

Анатомия кибер атаки

- Разведка и развертывание инфраструктуры
- Регистрация домена, IP, ASN intelligence
- Мониторинга развертывания основываясь на результатах

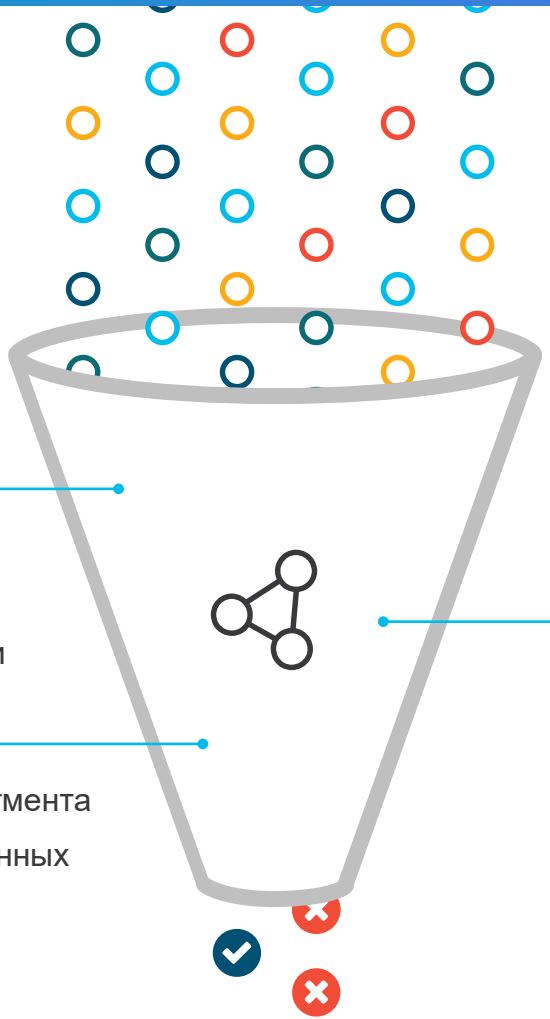
- Удар по пациенту #0

- Углубление заражения
- Расширение заражения
- Защитные сигнатуры разработаны

Видимость Umbrella

100B	85M	12K	160+
Запросов ежедневно	Активных пользователей ежедневно	Корпоративных заказчиков	Странах мира

Статистическое моделирование



2M+ событий в секунду

11B+ исторических событий

Виновен по поведению

- Модель совместных запросов
- Геолокационная модель
- Модель индекса безопасности

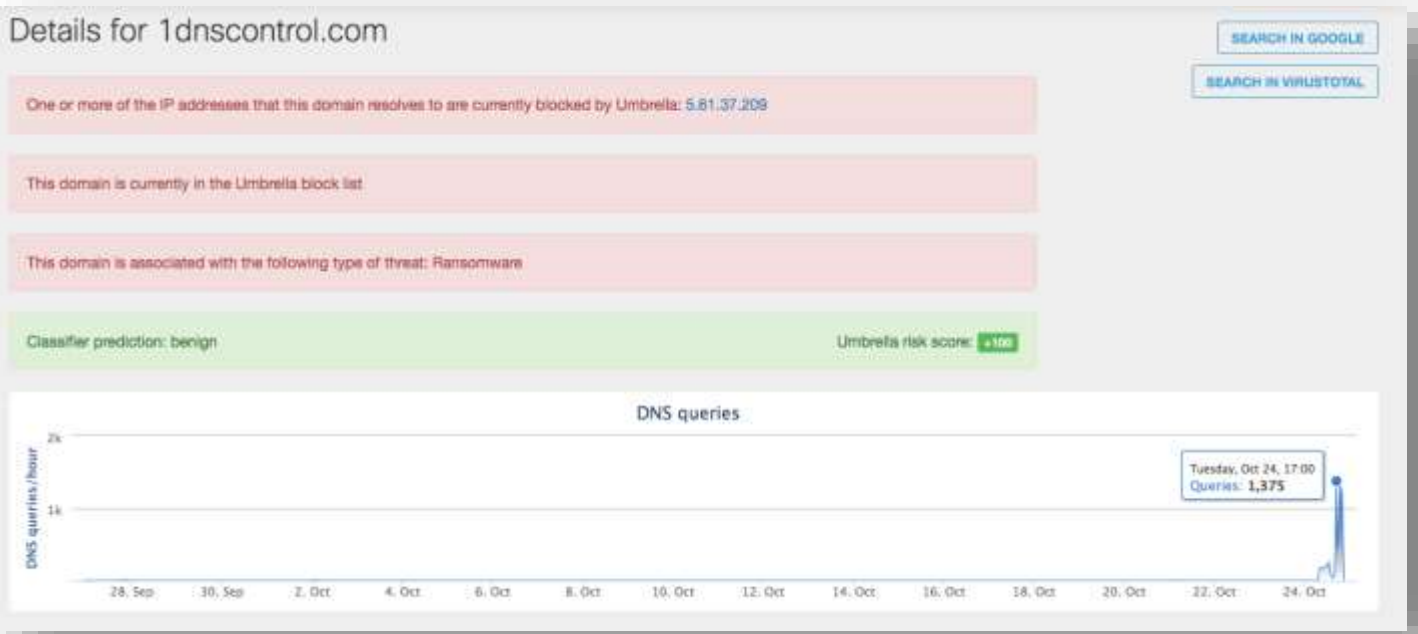
Виновен по связям

- Модель предсказуемого IP сегмента
- Корреляция DNS и WHOIS данных

Шаблон виновности

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

Следуй за «Плохим кроликом»

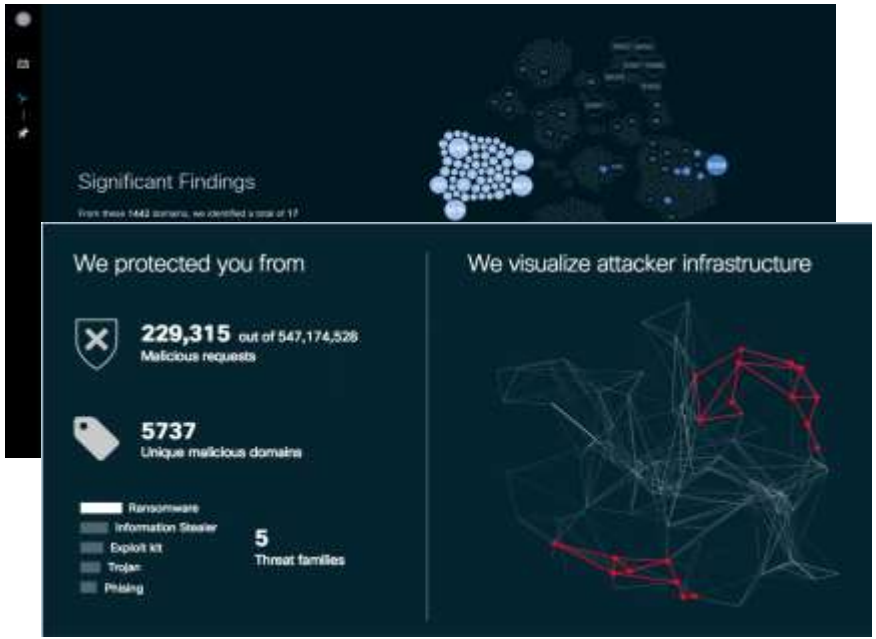


Программа

- 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.

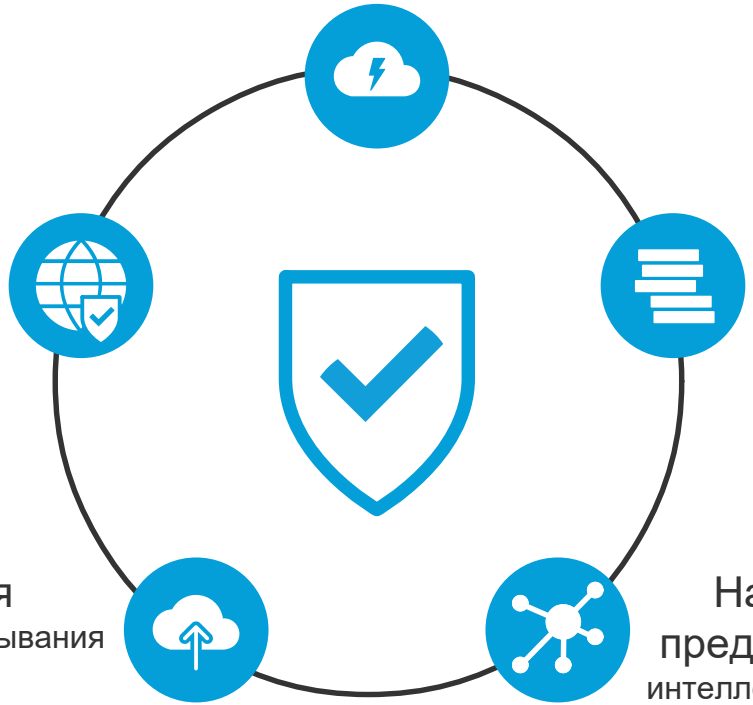


После тестирования вы получаете отчет, помогающий ответить на вопросы:

- 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

Быстрая
И наиболее надежная
облачная инфраструктура



Широчайшее
покрытие вредоносных
сайтов и файлов

Открытая
платформа для
интеграции

Простая
модель развертывания
в облаке

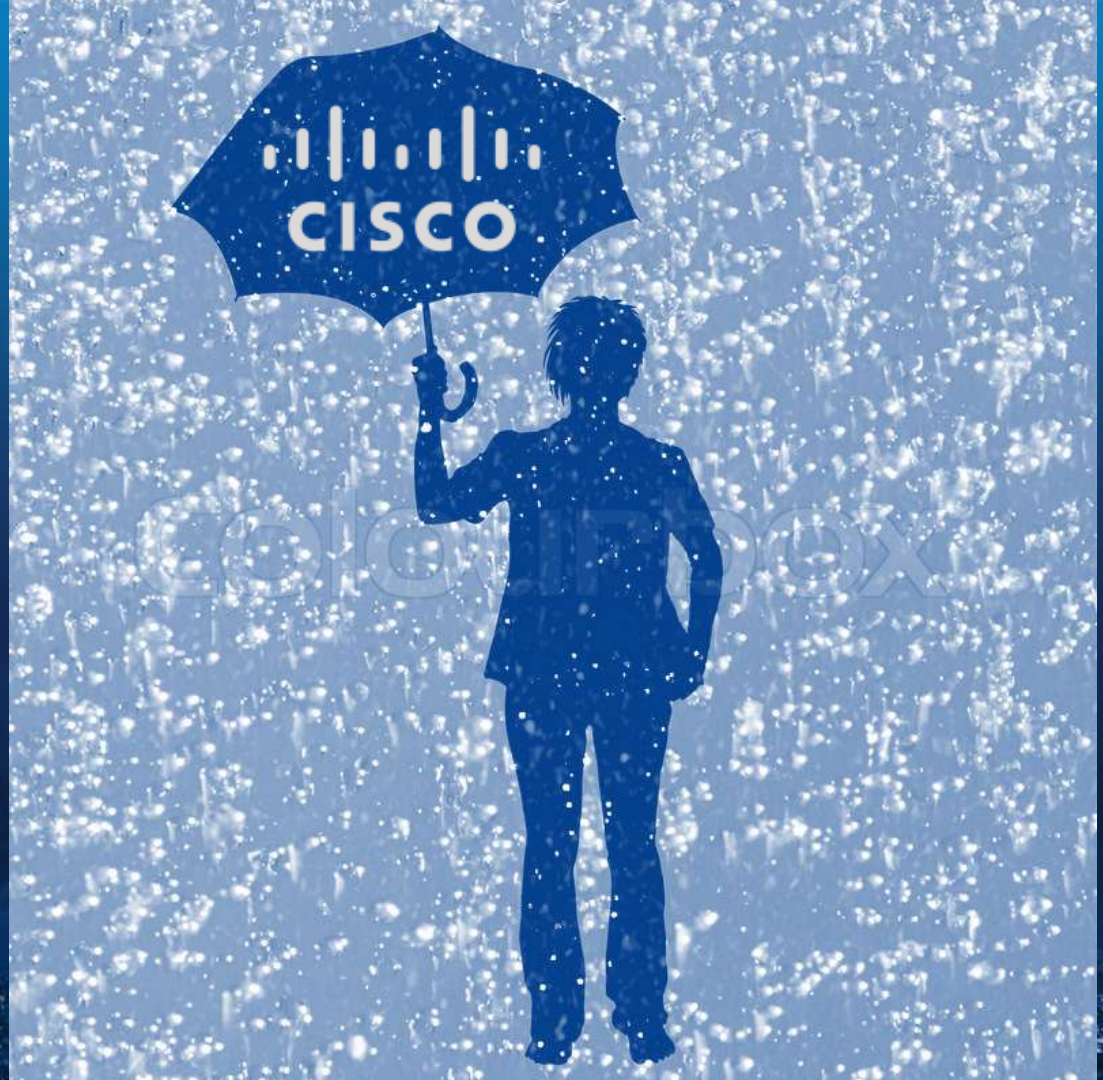
Наиболее предсказуемый
интеллект блокировки
угроз

С чего начать

Протестировать у заказчиков

Использовать дома

Сдать экзамены и начать использовать в офисе


CISCO


CISCO
SOFTPROM
by ERC
Cisco LabDay 2018
Минск, 26 апреля
#ciscolabday