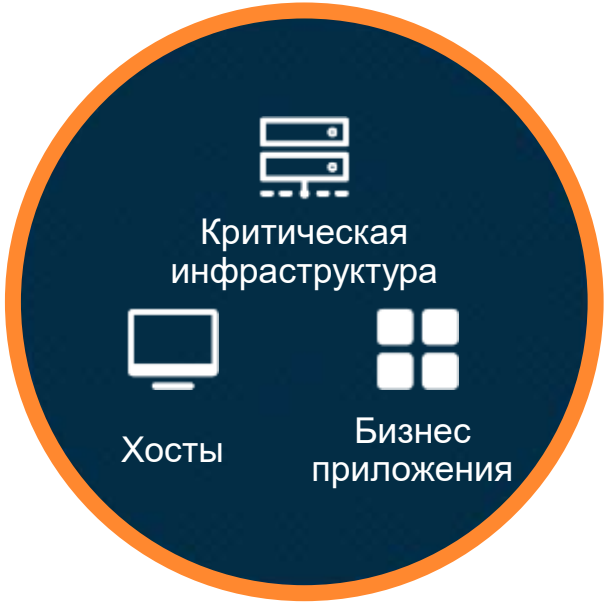
Облачные сервисы на страже безопасности. Cisco Umbrella и Meraki

Владимир Илибман

Cisco Systems

8 декабря 2016

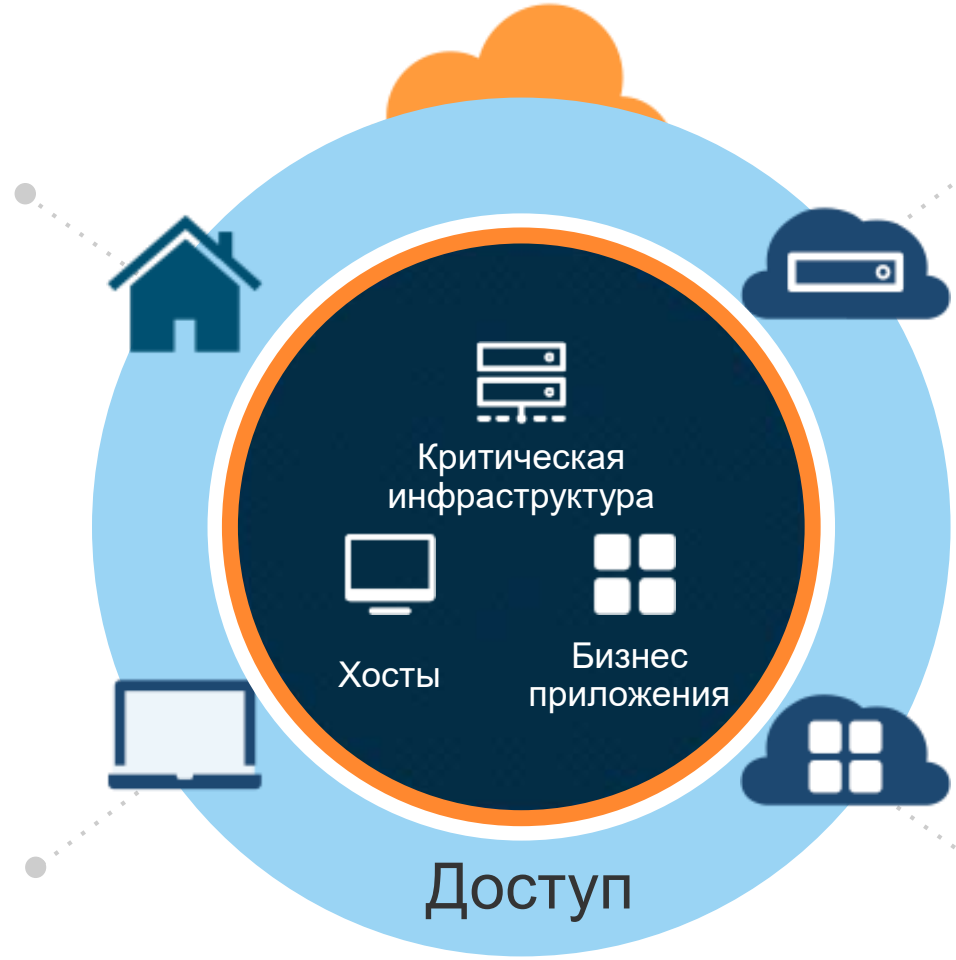
Как мы привыкли работать



Как мы работаем теперь

Удаленные пользователи

Пользователи



Критическая инфраструктура – ***IaaS & PaaS*** (прим:, Amazon, Azure, и др.)

Приложения и данные

Ноутбуки / Планшеты пользователей

Бизнес приложения - ***SaaS*** (прим:., Salesforce, Office365, Google)

Как мы работаем теперь – Расширенный периметр

Удаленные пользователи

Пользователи

Ноутбуки / Планшеты пользователей

Критическая инфраструктура – ***IaaS & PaaS*** (прим:, Amazon, Azure, и др.)

Приложения и данные

Бизнес приложения - ***SaaS*** (прим:., Salesforce, Marketo, Office365, Google)

К 2018, Gartner оценивает:

25% корпоративного трафика данных будет обходить периметральную защиту.

Таким образом к 2018 (или даже быстрее)…

NGFW будут слепы к 25% трафика!

“Облака” и корпоративная безопасность

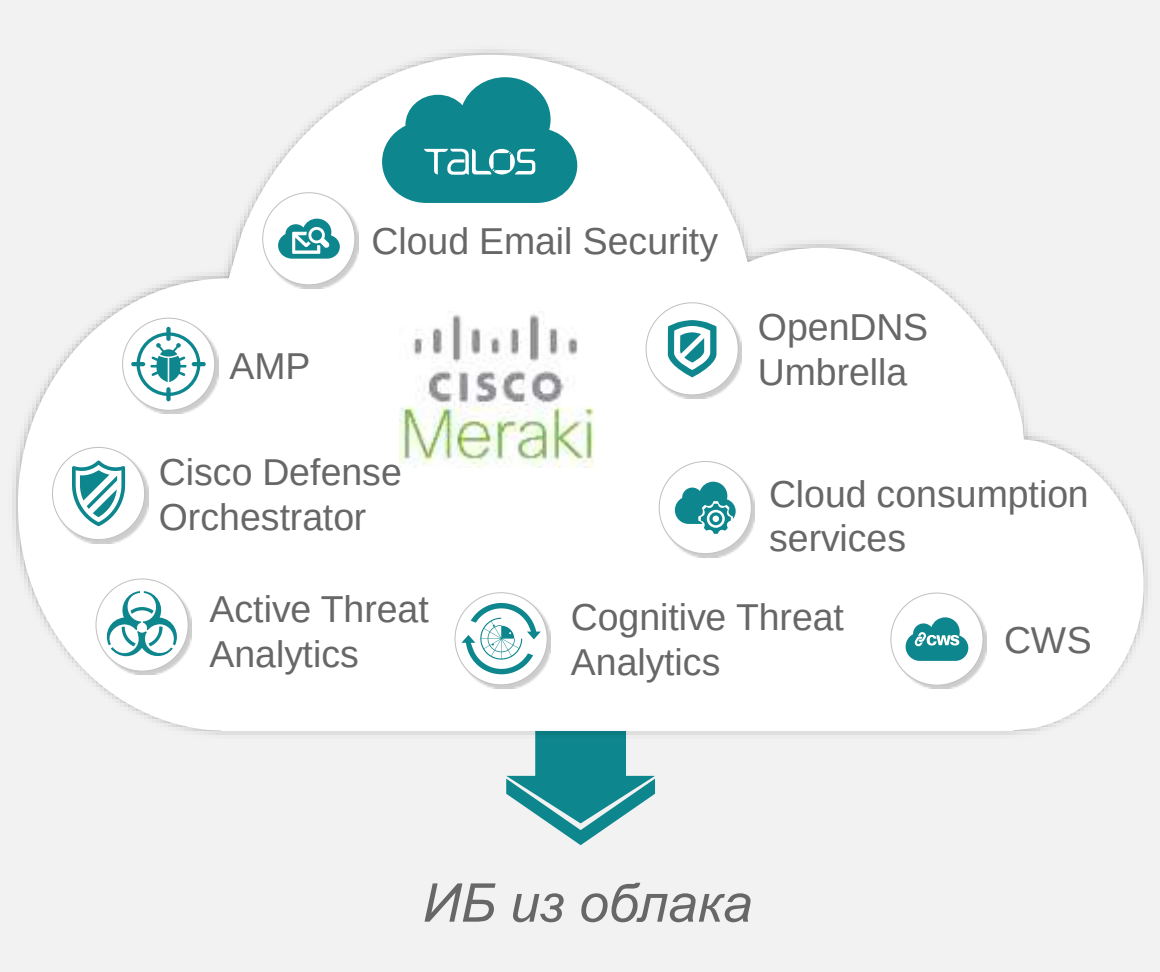
Безопасность из облака

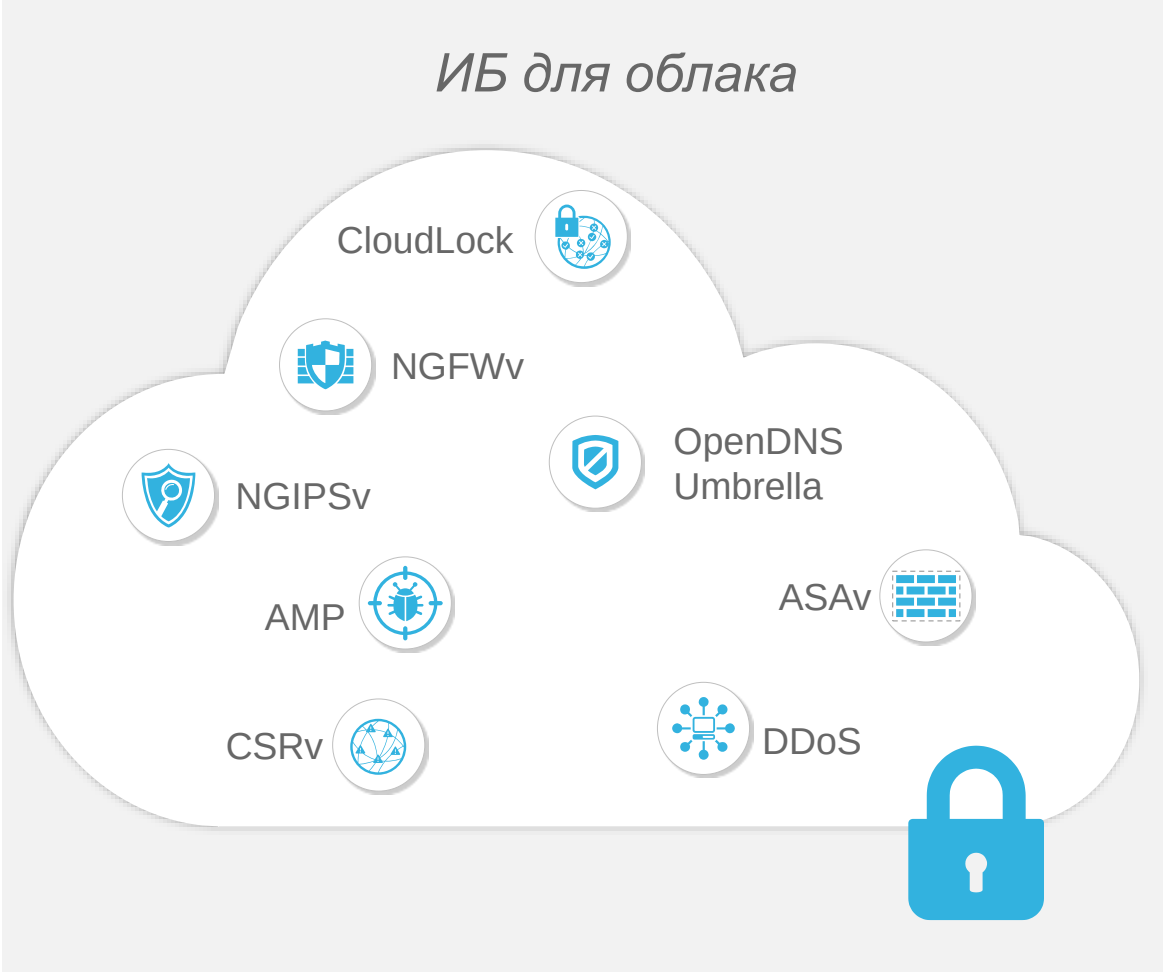
- Использование облачных средств и аналитики из облака для защиты корпоративных ресурсов (включая традиционный периметр)

Безопасность для облака

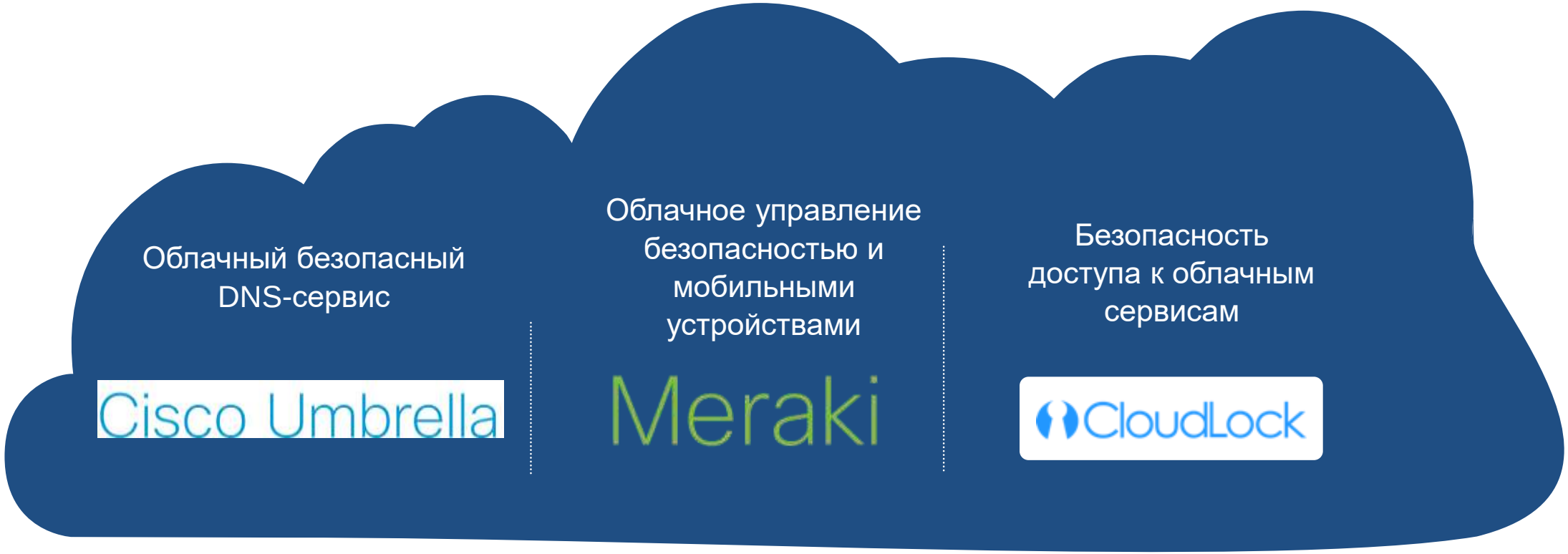
- Защита облачных сервисов, которые используются ИТ-службами или сотрудниками компании

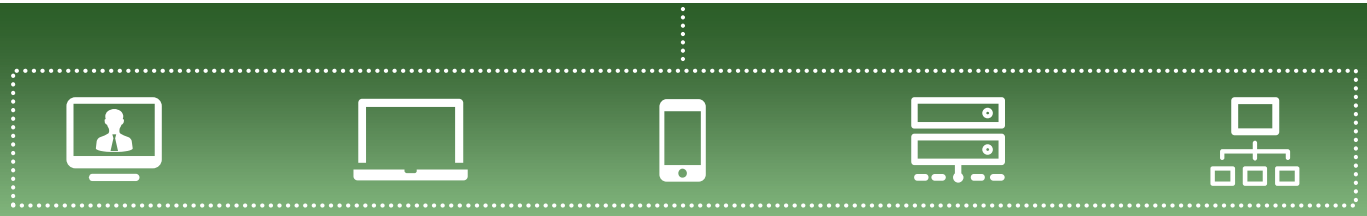
Объединяя ИБ из облака и для облака





Платформа Cisco Cloud Security

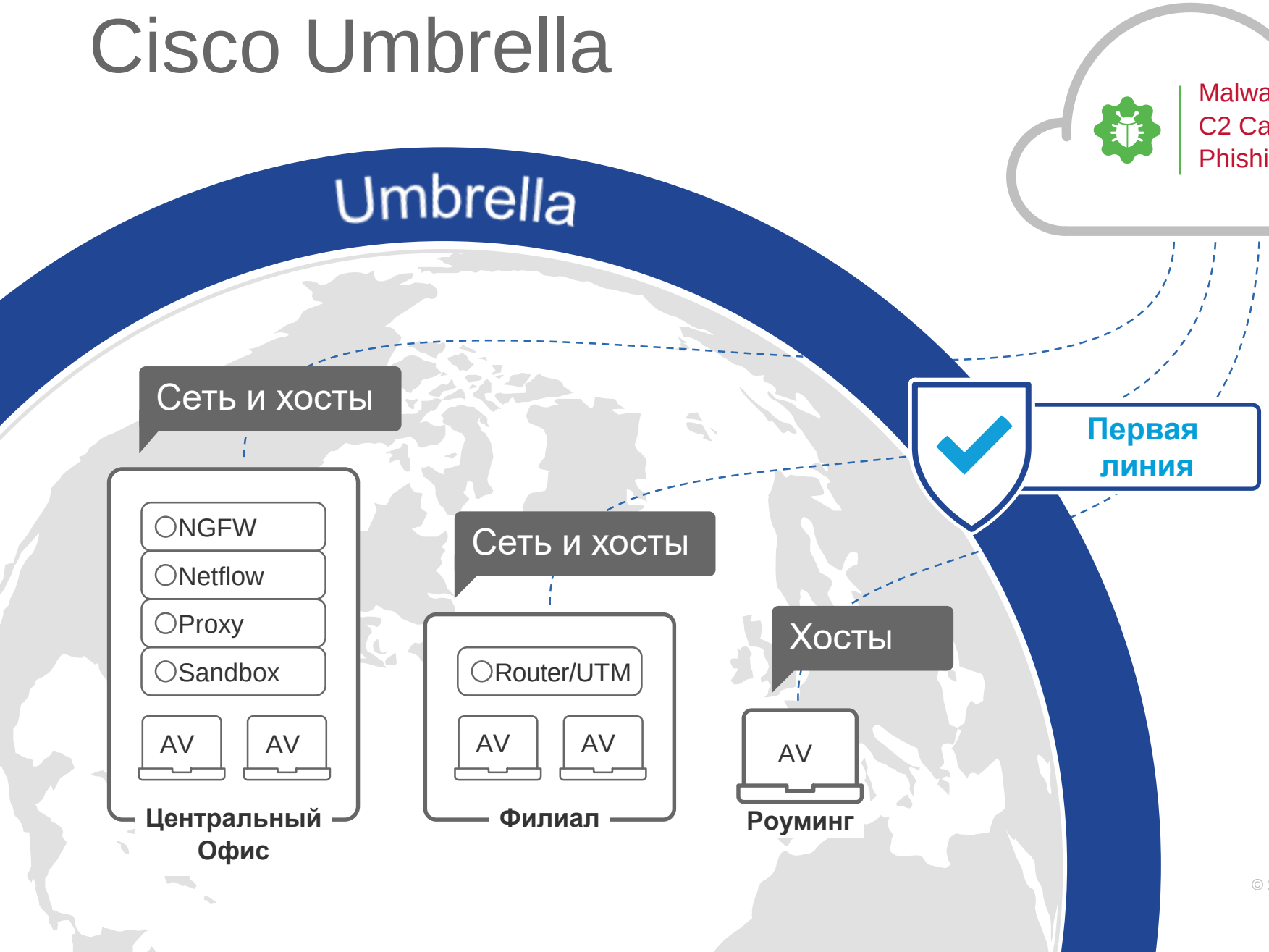




Устройства и сети
Подключение отовсюду

Cisco Umbrella

Cisco Umbrella



Всё начинается с DNS

Предшествует открытию файлов и установлению IP соединения

Используется всеми устройствами

Независимо от порта

Cisco Umbrella – сервис безопасного DNS

Встроен в саму основу Интернет

Интеллект позволяющий видеть угрозу до атаки

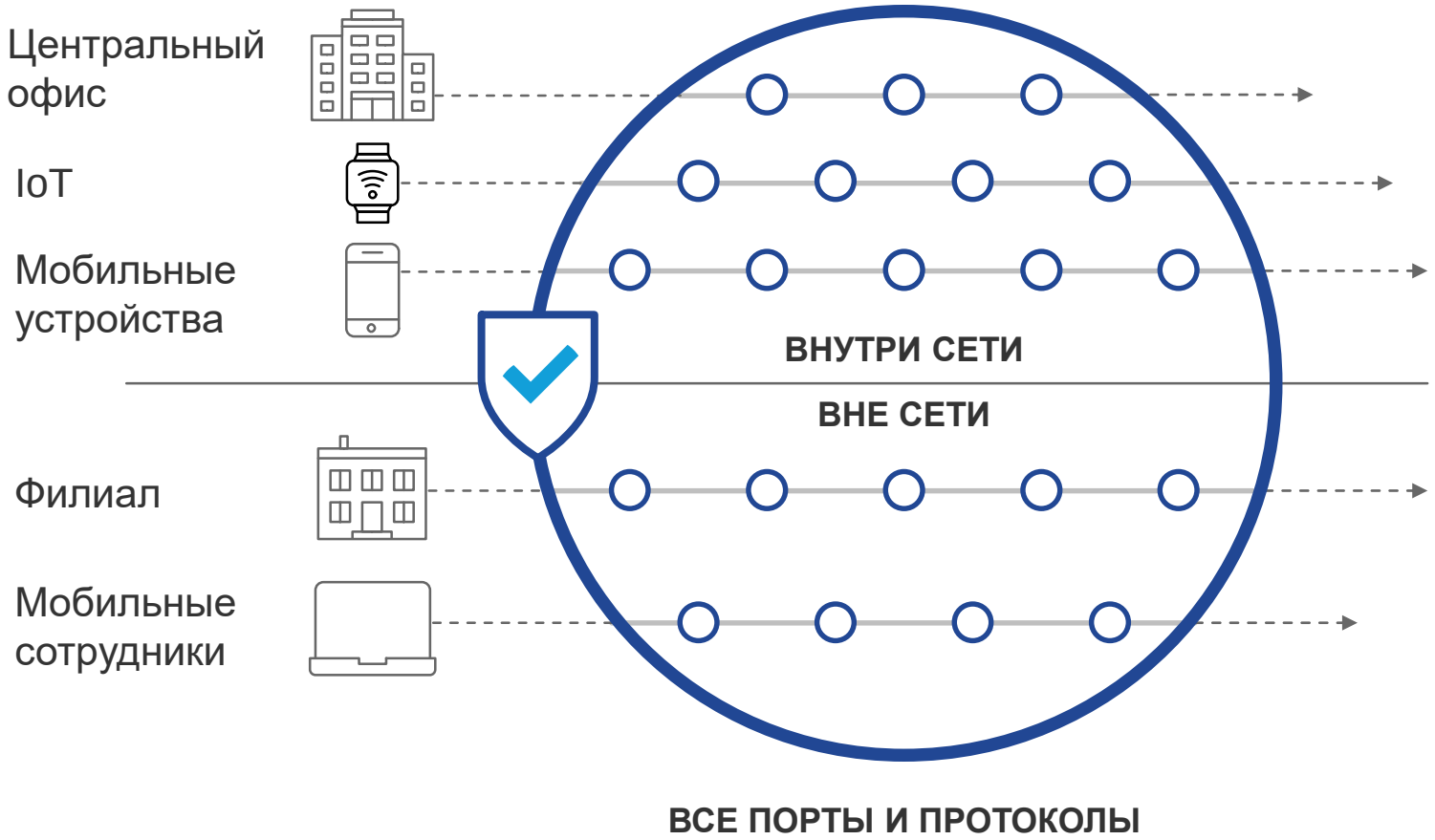
Видимость и защита везде

Развертывание на всю сеть за минуты

Интеграция для расширения текущих возможностей

Доступен со всех платформ и устройств

Umbrella



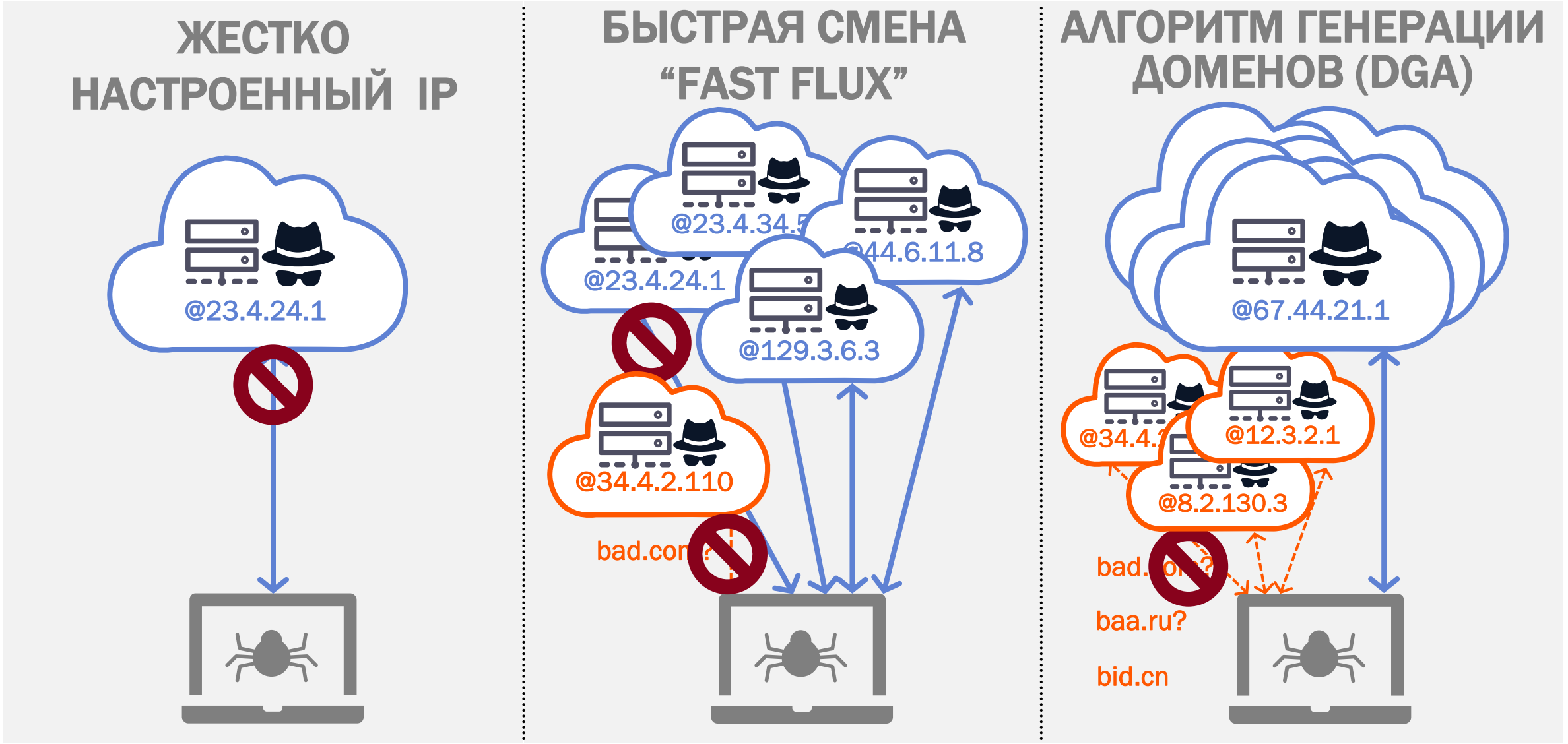
Все офисные локации

Любое устройство в сети

Мобильные хосты

Каждый порт и протокол

Эволюция Command & Control отзвонов

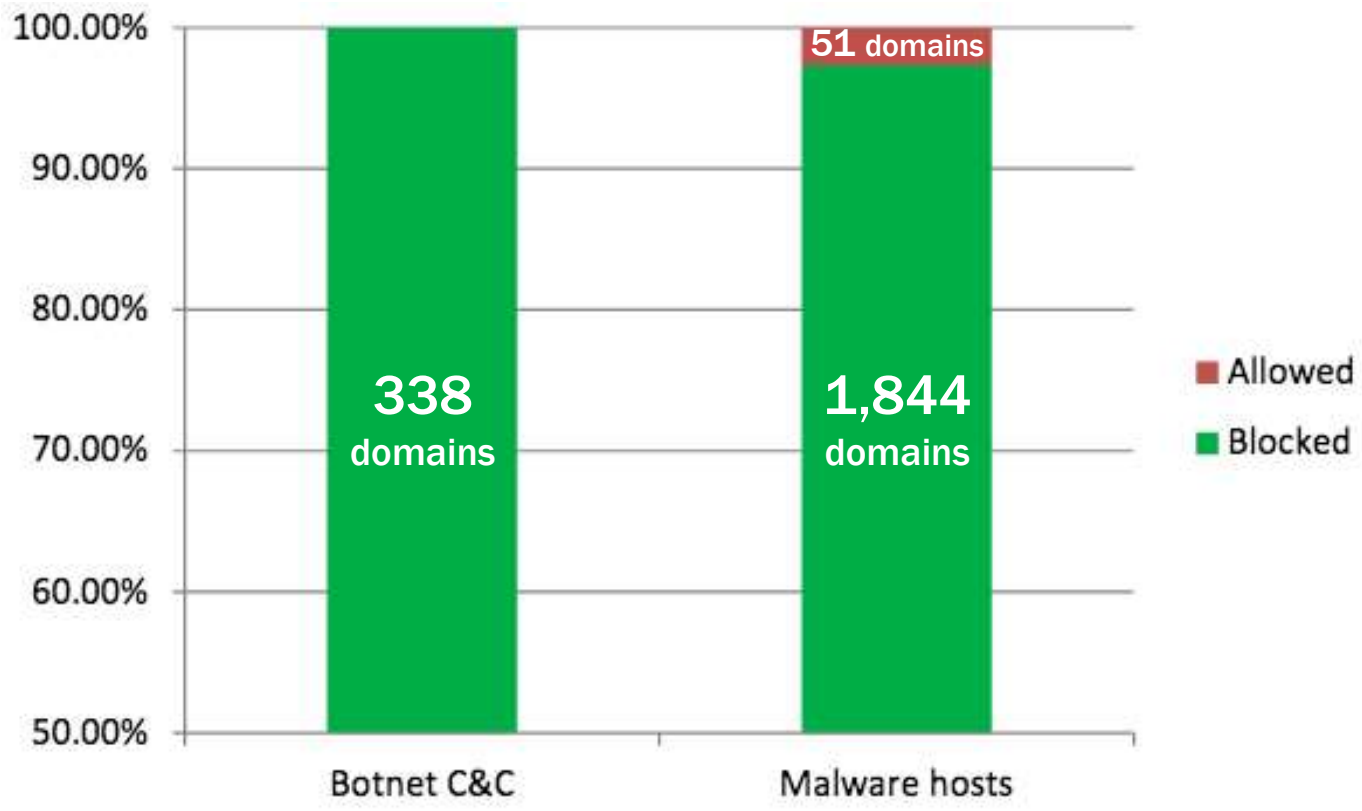


“ OpenDNS смог классифицировать и блокировать 100% тестированных 338 C&C серверов. ”

AV-TEST

Тестировалось 4 Мая 2015

“Ввиду своего уникального подхода к защите хостов на уровне DNS он также не несет никакой нагрузки на производительность.”



Видение Интернет от OpenDNS / Umbrella

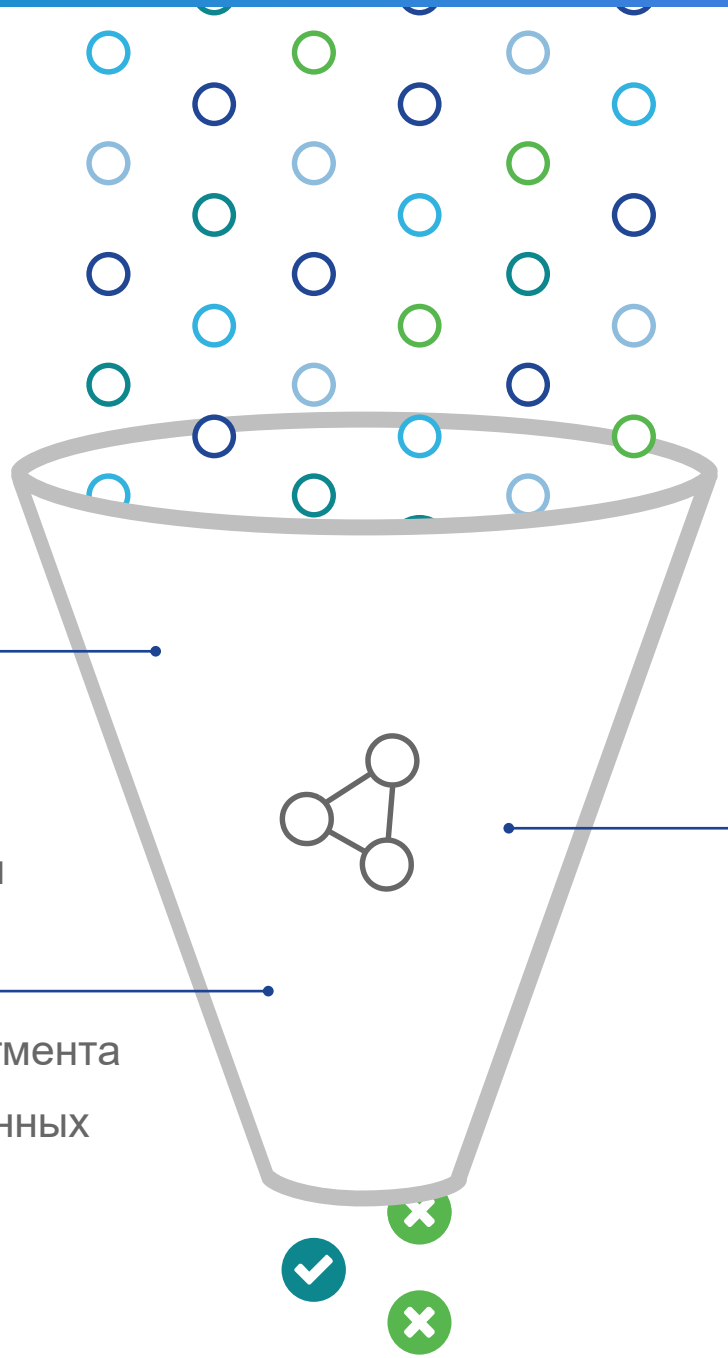
80
МЛРД.
Запросов в день

65
МЛН.
Активных пользователей ежедневно

12
ТЫС.
Корпоративных заказчиков

160+
Стран по всему миру

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

Наша эффективность

Обнаружение

3M+

Новых доменных имен в день

Идентификация

60K+

Вредоносных доменов в день

Защита от

7M+

Активных вредоносных сайтов и адресов

ЦОД расположены в основных точках обмена трафиком

25

ЦОД по всему миру

Сценарии развертывания Cisco Umbrella

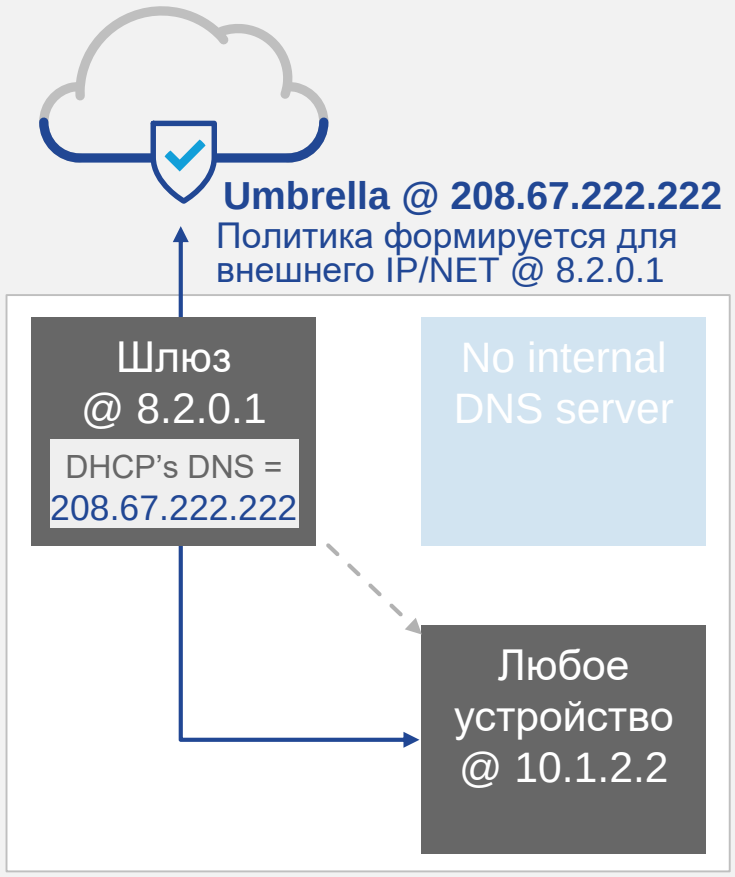
Простейший способ защитить любое устройство в сети

Направить внешний DNS трафик в Umbrella

Внутри сети: Просто указать внешний DNS без клиентов

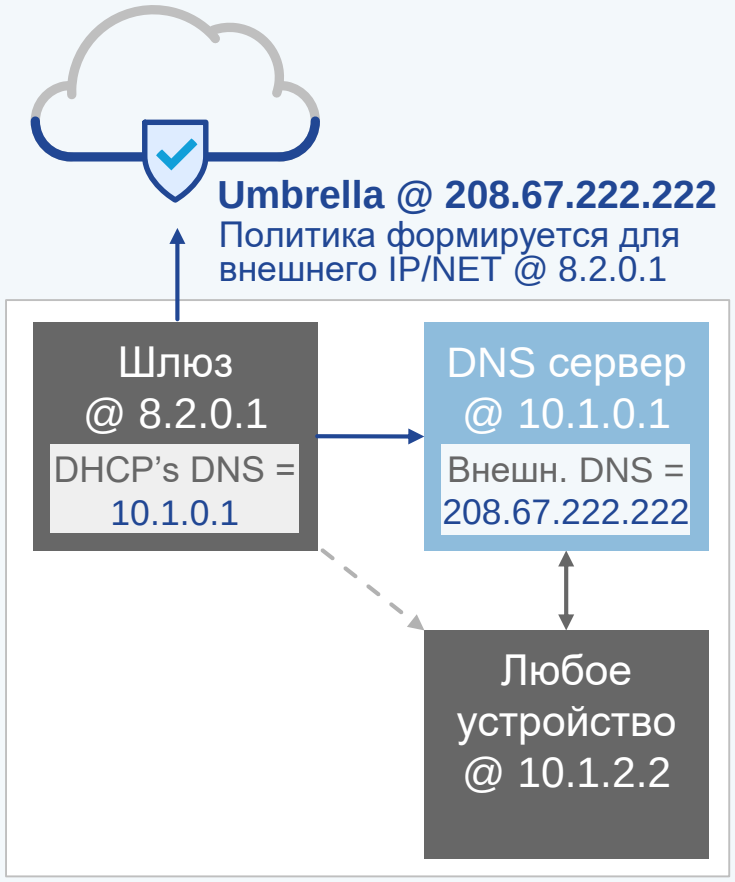
DHCP сервер

Просто для мест без внутренних доменов



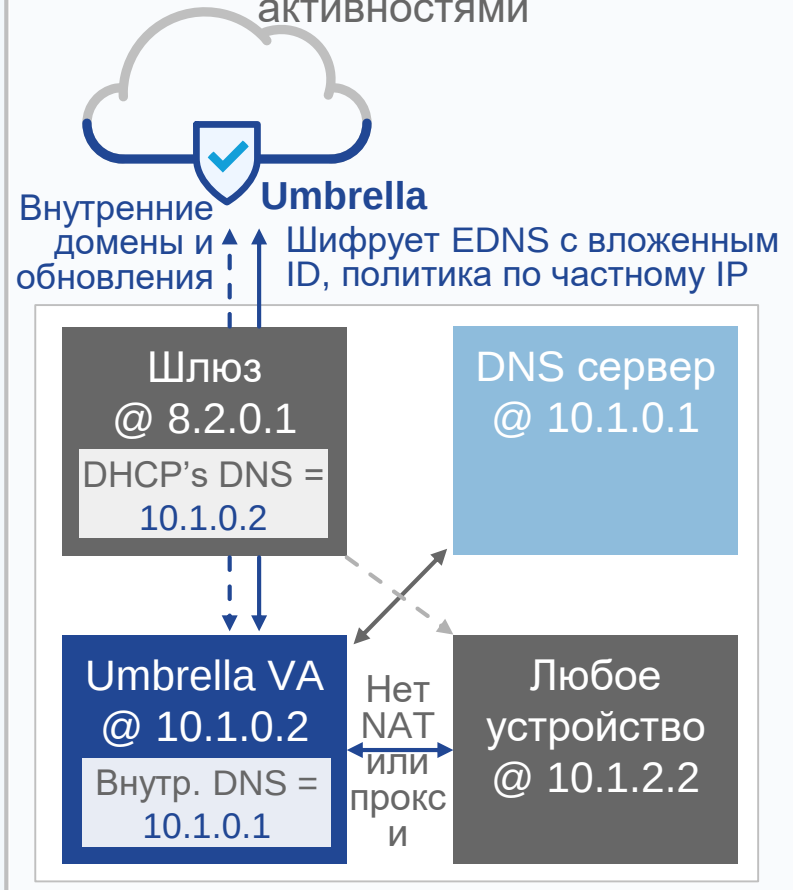
DNS server

Просто для мест где есть внутренний домен



Virtual appliance

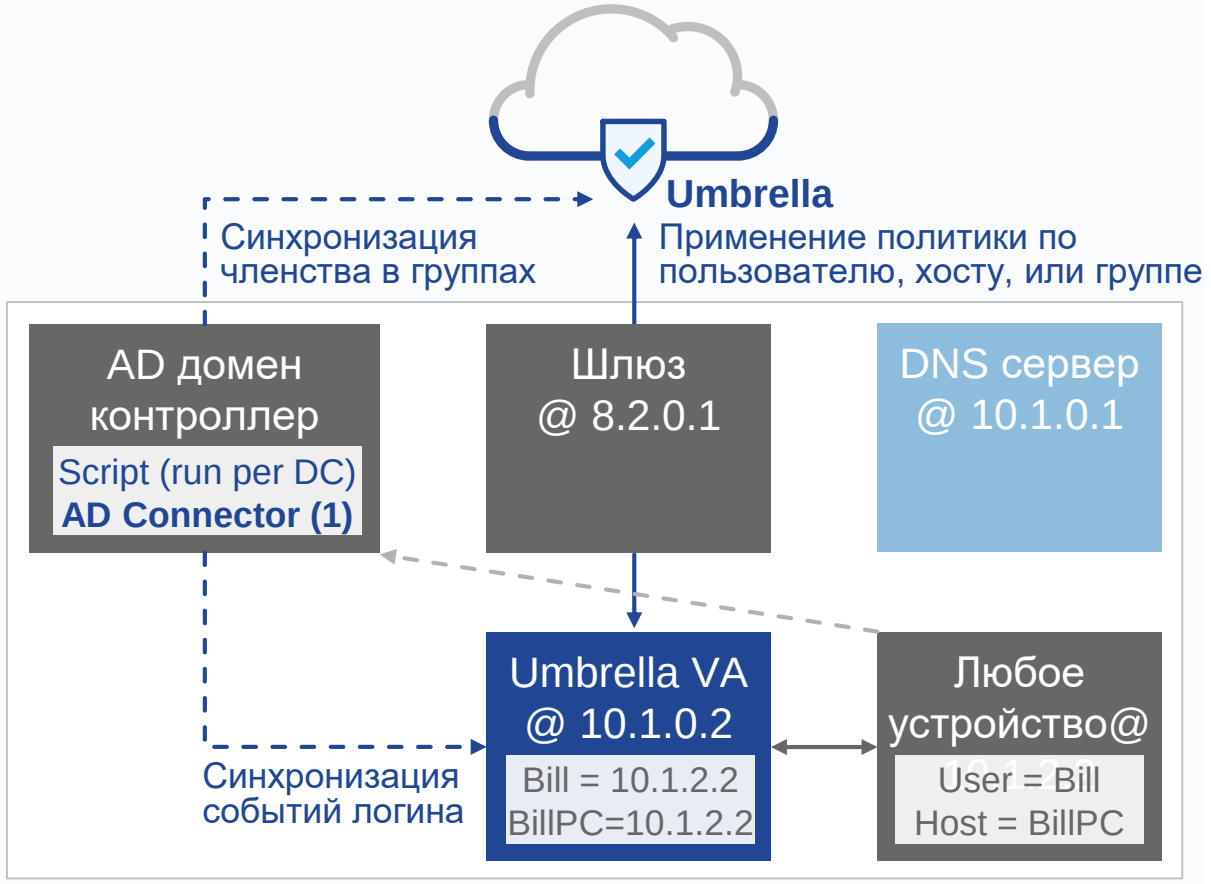
Лучшее для офисов которым нужен детальный контроль за активностями



Внутри сети: Добавление политик по пользователям без агентов

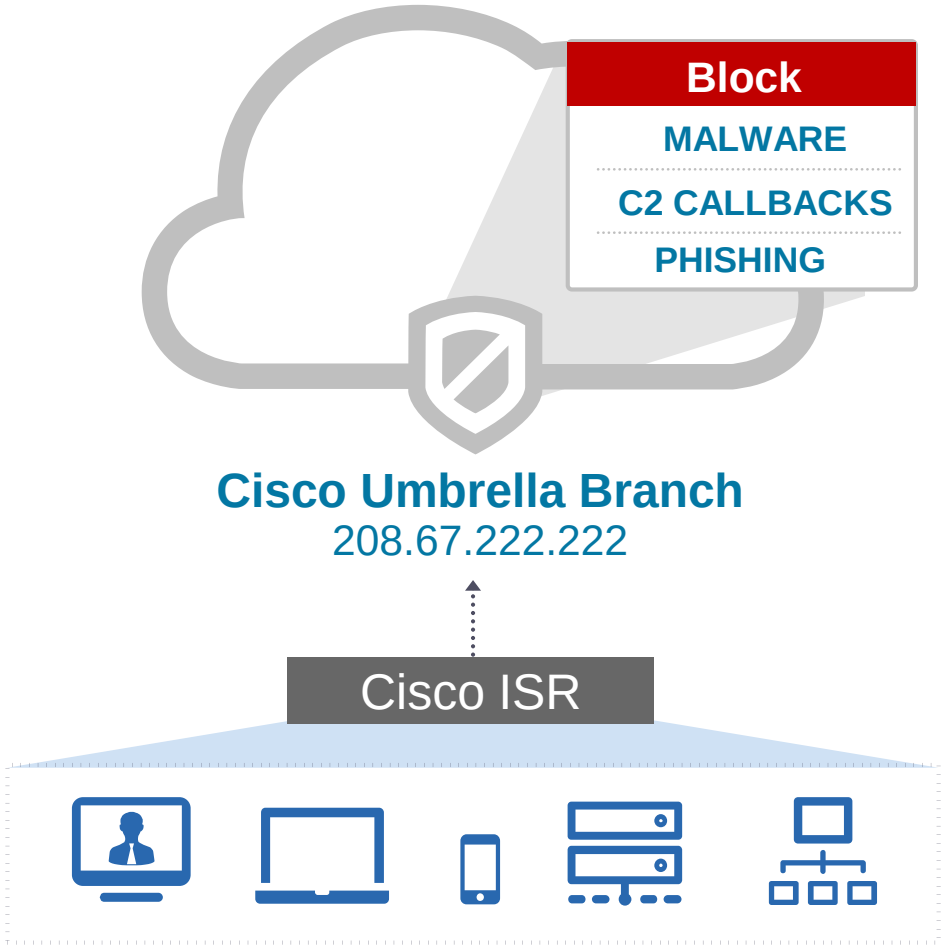
Виртуальный аплаенс + Коннектор

Лучшее для тех кому нужен детальный контроль и видимость интегрированная с AD



Cisco Umbrella Branch

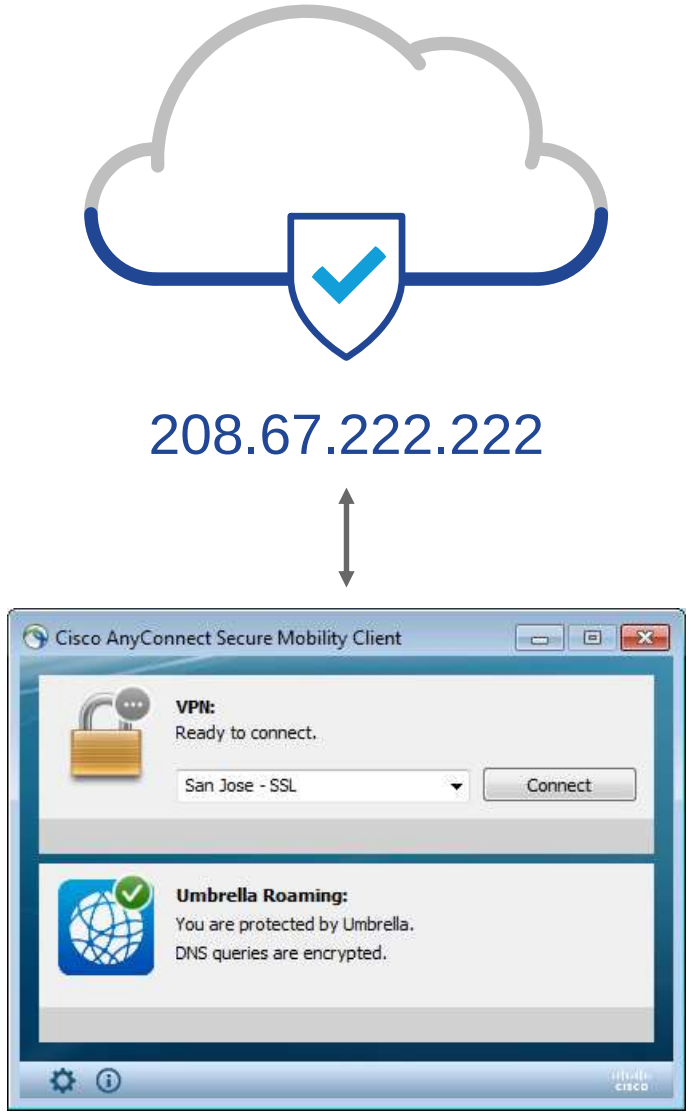
Ваш первый уровень защиты для филиала



- Видимость и фильтрация на уровне DNS
- Блокировка запросов к вредоносным доменам и IP
- Контентная фильтрация для гостей и корпоративных пользователей

Cisco AnyConnect модуль

1. Включить модуль роуминга
2. Настроить политику роуминга в Umbrella
3. Увидеть интернет активности и детальные логи для разбора инцидентов



Модель лицензирования

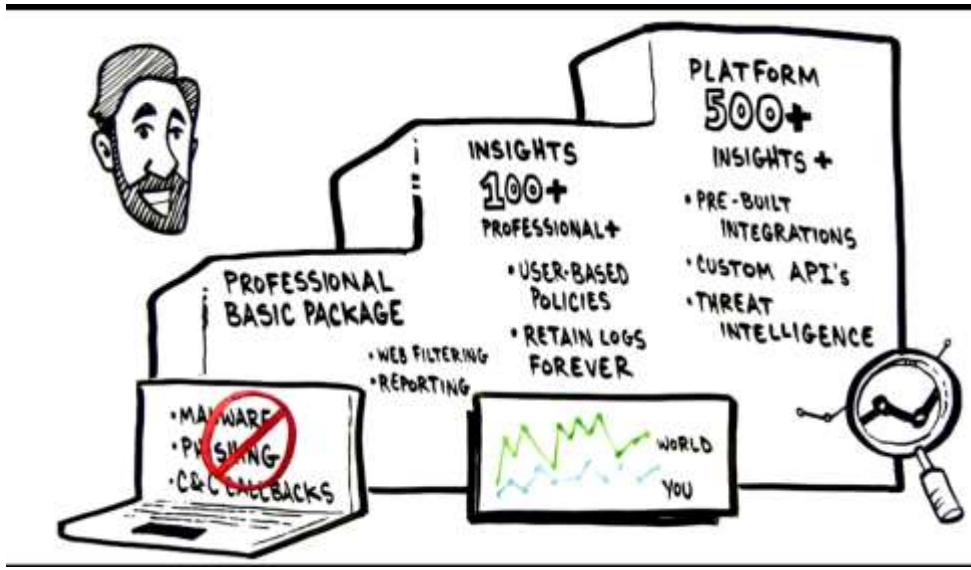
OpenDNS для дома

Фильтрация опасных сайтов
- 208.67.222.222
- 208.67.220.220

Блокировка взрослого контента
- 208.67.222.123
- 208.67.220.123

Premium DNS

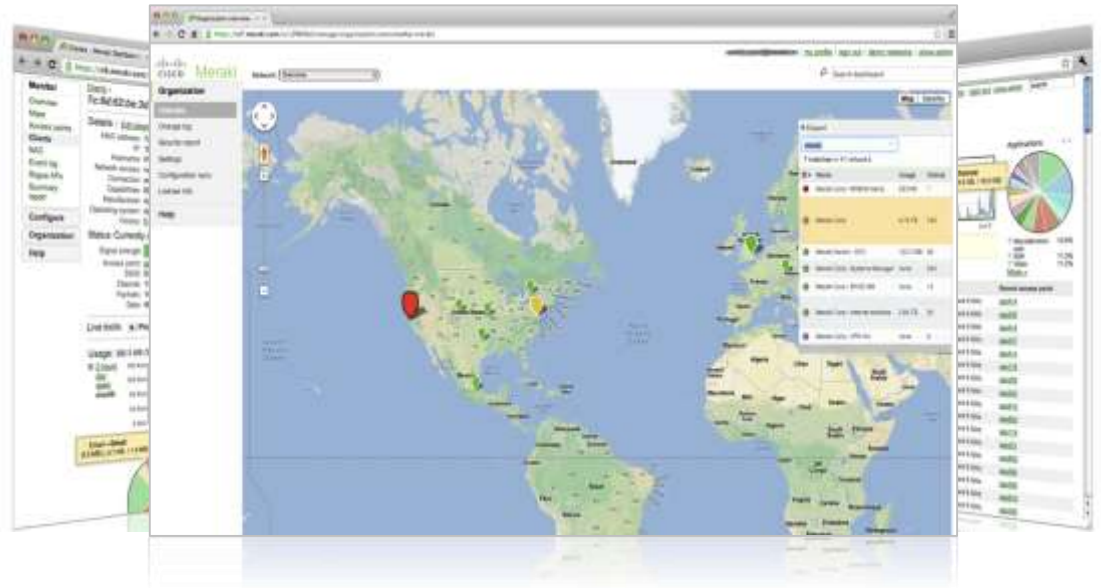
Umbrella для бизнеса



Cisco Meraki
Безопасность и управление мобильными устройствами из облака

Cisco Meraki: портфолио

- Сетевое решение с полностью облачным управлением
  - Беспроводное оборудование
  - Коммутаторы
  - Безопасность
  - MDM
- Признания за инновации
  - Gartner Magic Quadrant
  - InfoWorld Technology of the Year
  - CRN Coolest Technologies



Wireless LAN

Enterprise Security

Access & Aggregation Switching

Mobile Device Management

Cisco Meraki UTM

Безопасность
NG Firewall, IPS, Client VPN, Site to Site VPN

Сетевые сервисы
NAT/DHCP, Routing, Link Balancing

Контроль приложений
WAN Optimization, Traffic Shaping, Content Filtering

Cloud Managed

Auto VPN

Application Firewall

WAN Optimization

Application Control

Content Filtering

Smart Link Bonding

Bonjour Gateway

Mobile Device Manager

Задачи по управлению служебными и личными мобильными устройствами

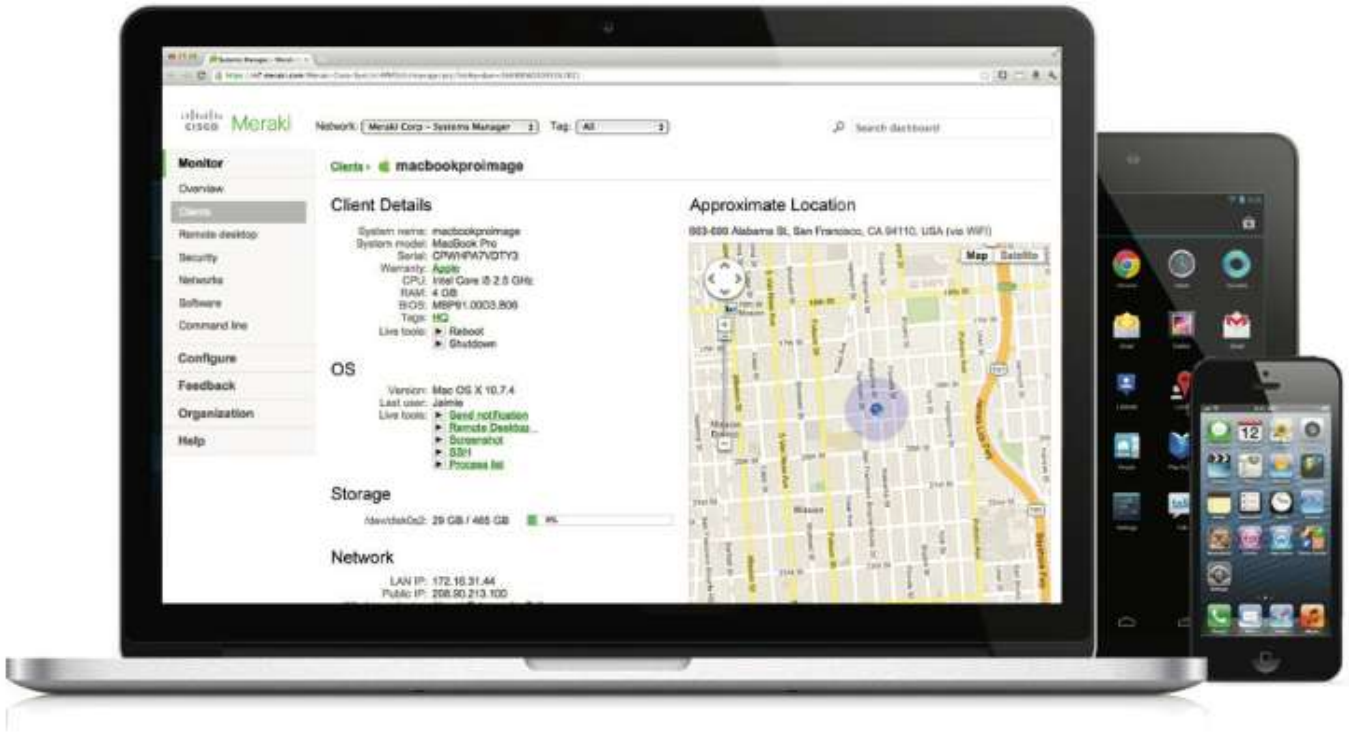
- Применить политику“принеси свое устройство” bring your own device (BYOD)
- Обеспечить защиту мобильных данных
- Внести инновации в работу через мобильные приложения
- Усилить политики управления мобильными устройствами (MDM)

Что делает Cisco Meraki MDM (Systems Manager)

Управляет устройствами

Смартфоны, планшеты, ноутбуки, десктопы

- Apple iPad, iPod Touch, iPhone, Apple TV
- Android 4.0+ (Android for Work 5.0+)
- macOS 10.7+
- Windows 10, 8.1, 8, 7,
- Windows Phone 10, 8.1
- Windows Server 2016, 2012, 2008 R2
- Chrome



Инвентаризация устройств

Работает в любой сети

Простое, единое лицензирование для всех платформ и операционных систем

Что делает Cisco Meraki MDM (Systems Manager)

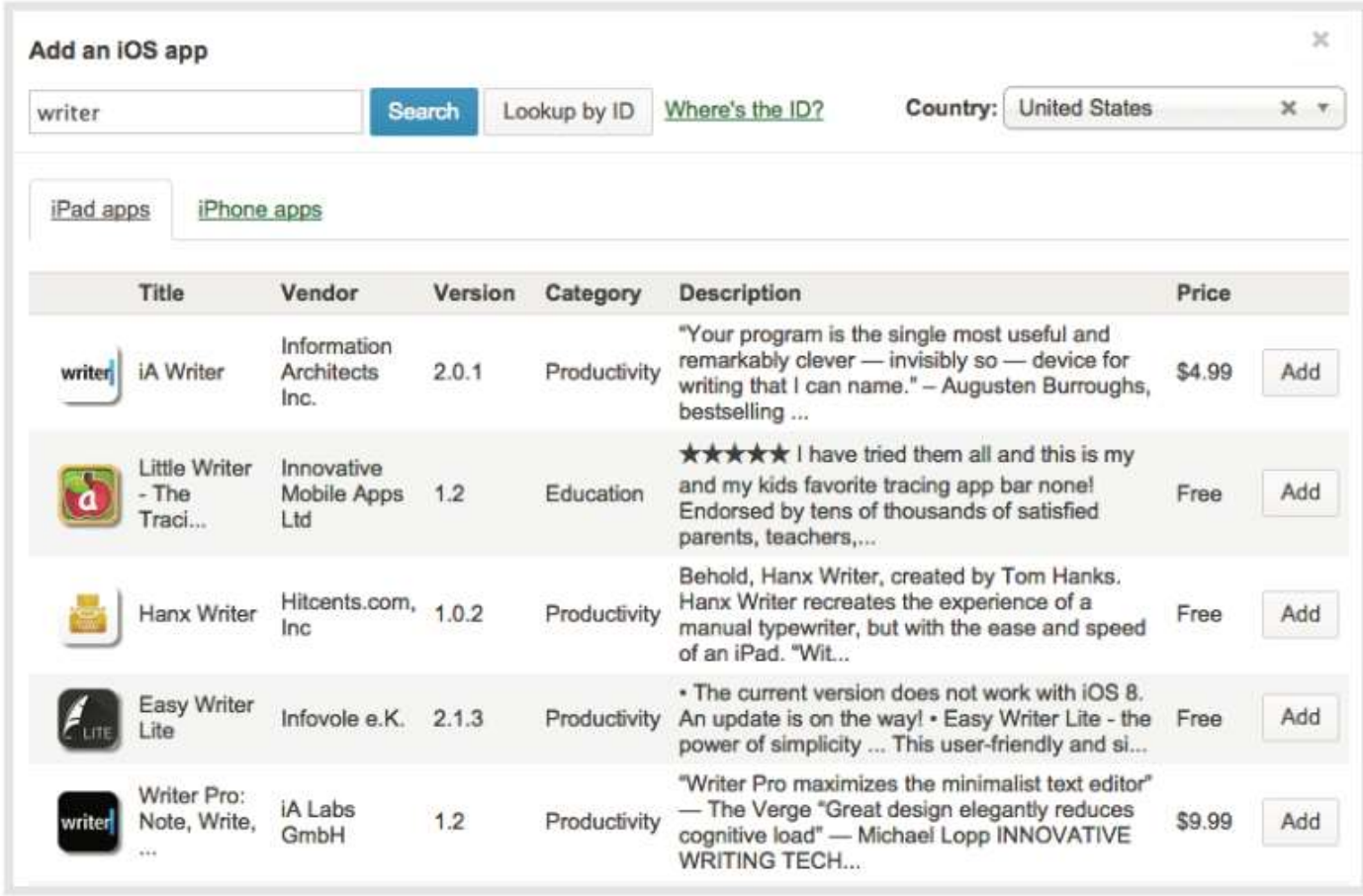
Управляет приложениями

Установка и удаление приложений и контента, блокирование приложений

Интеграция с Apple Store и Google Play, корпоративный магазин приложений

Поддержка Android for Work (рабочий “контейнер”)

На PC и Mac распространение приложений через MSI и PKG файлы



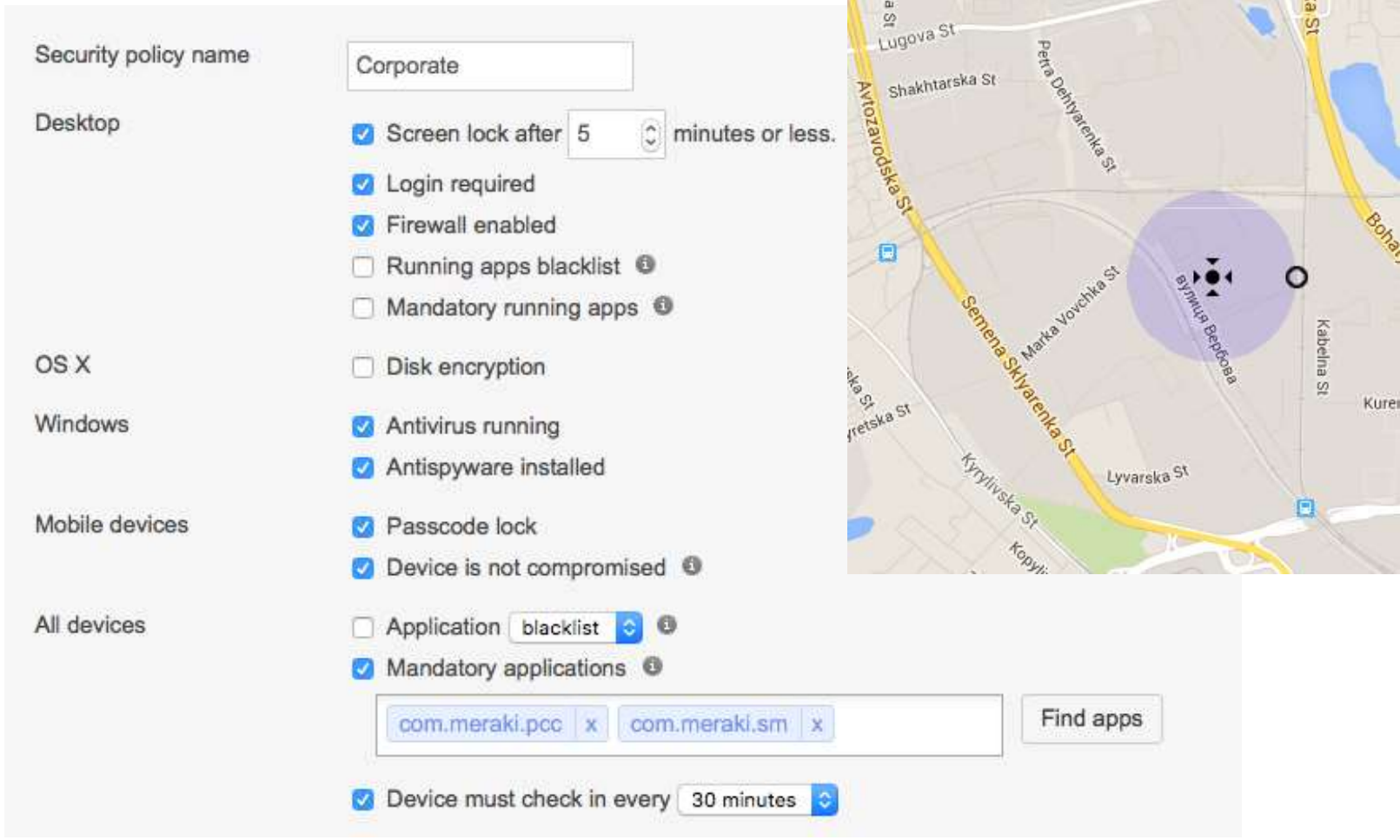
Что делает Cisco Meraki MDM (Systems Manager)

Усиливает безопасность

Парольные политики, ограничение доступа

Защита данных, удаление и избирательное удаление данных

Локация устройства и применение политик на основании местонахождения



Что делает Cisco Meraki MDM (Systems Manager)

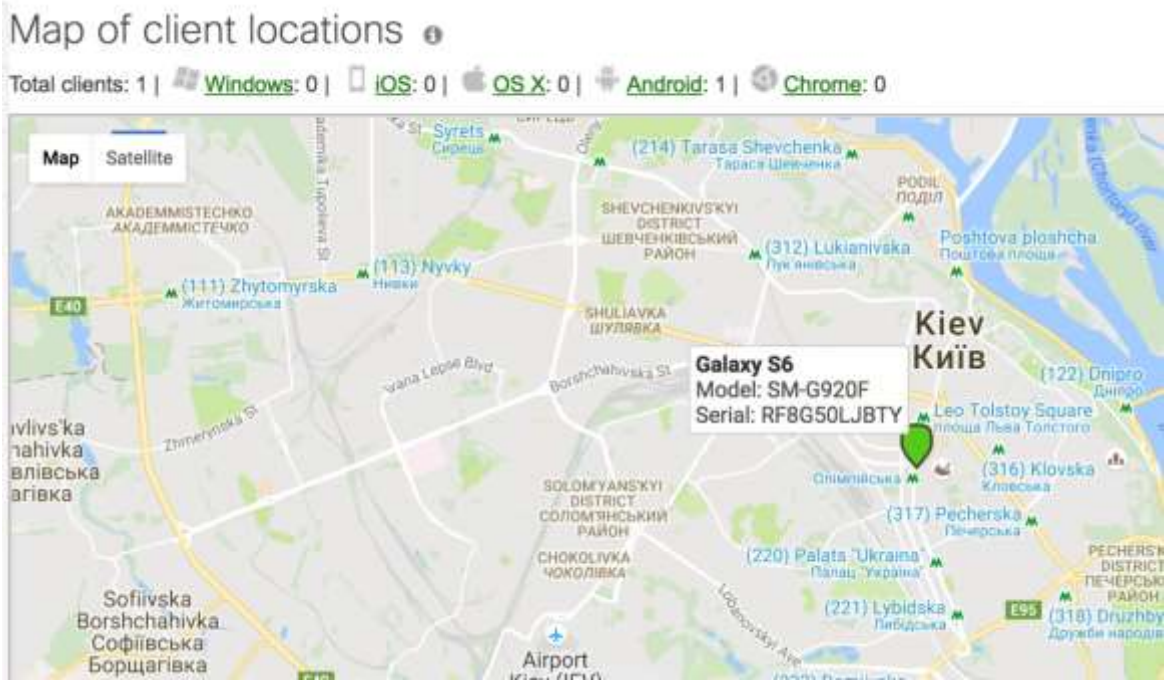
Экономит время и помогает в обслуживании

Автоматическая регистрация и профилирование устройств, динамическое управление политиками, интеграция с AD

Распространение настроек WiFi, VPN, почты

RDP, удаленный ребут и выключение

Уведомления о событиях администраторах (выход за пределы территории, изменения в приложениях, удаление профиля итд.)



Status	Name	Notes	Model	OS	Connected	Connectivity	Disk % used	Battery	Managed?	Carrier network	Geofencing status
	vikaphone		iPhone 5c	iOS 9.2.1	Apr 20 2016 11:10		100%	100%	Yes	Kyivstar	
	tandiberg@gmail.com		A9	Android 4.1.1	now		24%	12%	Yes	-	
	VikaMac		MacBook Air	OS X 10.11.3	now		97%	-	No	-	
	EUGENE-PC		-	Windows 7 Œ ª á¨¬ «ì ï (64-bit)	now		53%	-	No	-	5 days

CloudLock защита данных и приложений в публичных облаках

Что кампания хочет защитить в облаке

Пользователей/ Аккаунты

- Кто чем занимается в моих облачных приложениях?
- Как понять что аккаунты скомпрометированы?
- Есть ли внутренние злоумышленники выводящие информацию?

Данные

- Хранят ли пользователи запрещенную и регулируемую информацию в облаке?
- Как обнаружить нарушение политики?
- Как автоматизировать исправление состояния при инцидентах?

Приложения

- Как я могу следить за использованием приложения и рисками?
- Имеются ли сторонние подключенные к инфраструктуре приложения?
- Как отключить рискованные приложения?

Технология Информационной безопасности #1 в 2016 году

CASB

Cloud Access Security Broker

Источник: Gartner, 2016

Платформа CloudLock

CASB для SaaS

Защищенное использование **Бизнес приложений** в облаке

CASB для IaaS/PaaS

Защищенное использование **критической инфраструктуры** в облаке

Cloud Security Orchestration

Включите облака в **процессы ИБ**

CloudLock **Cloud Security Fabric™**

CloudLock платформа

Защищенное использование **Бизнес приложений** в облаке

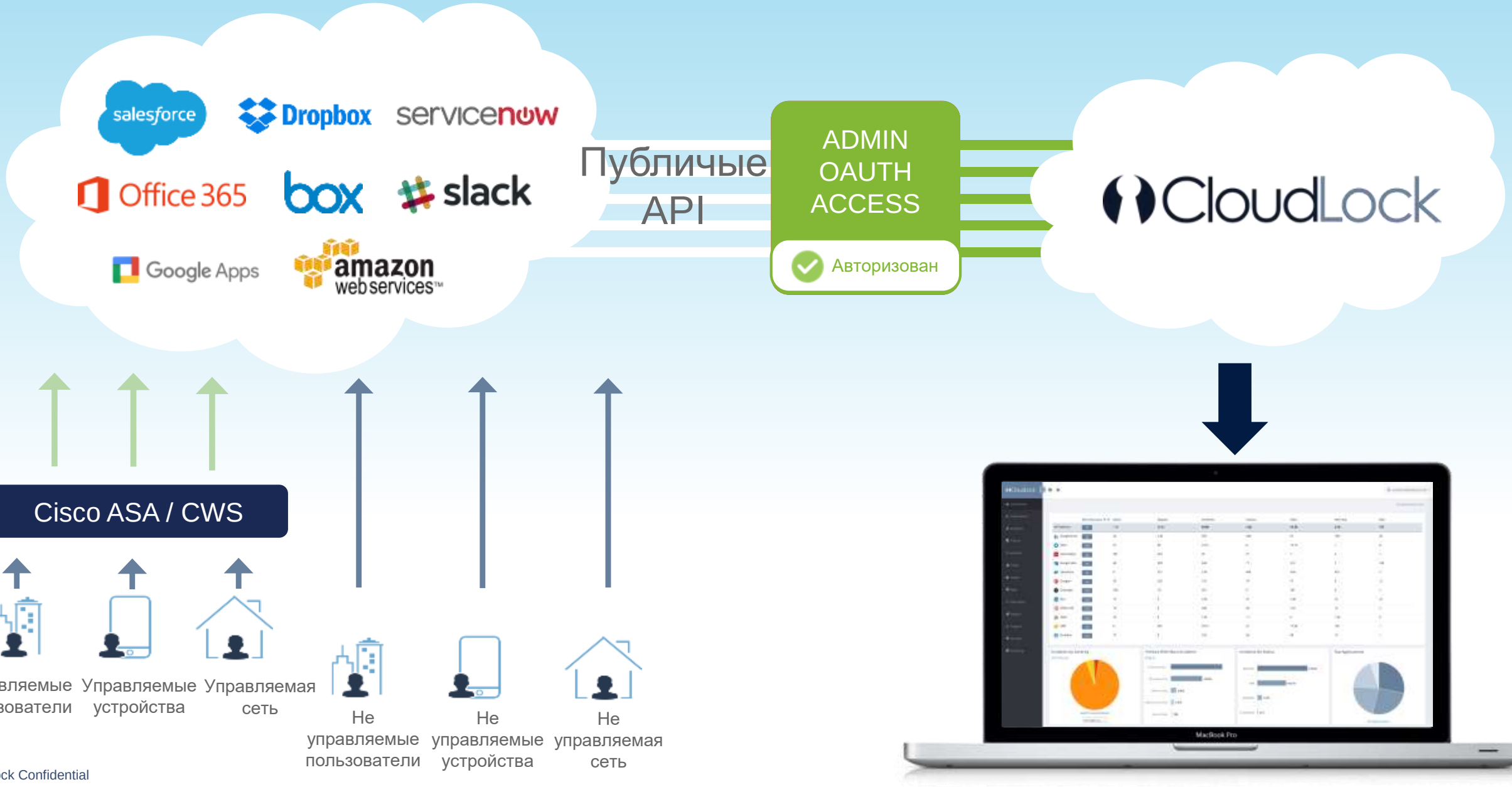
Защищенное использование **критической инфраструктуры** в облаке

Включите облака в **процессы ИБ**

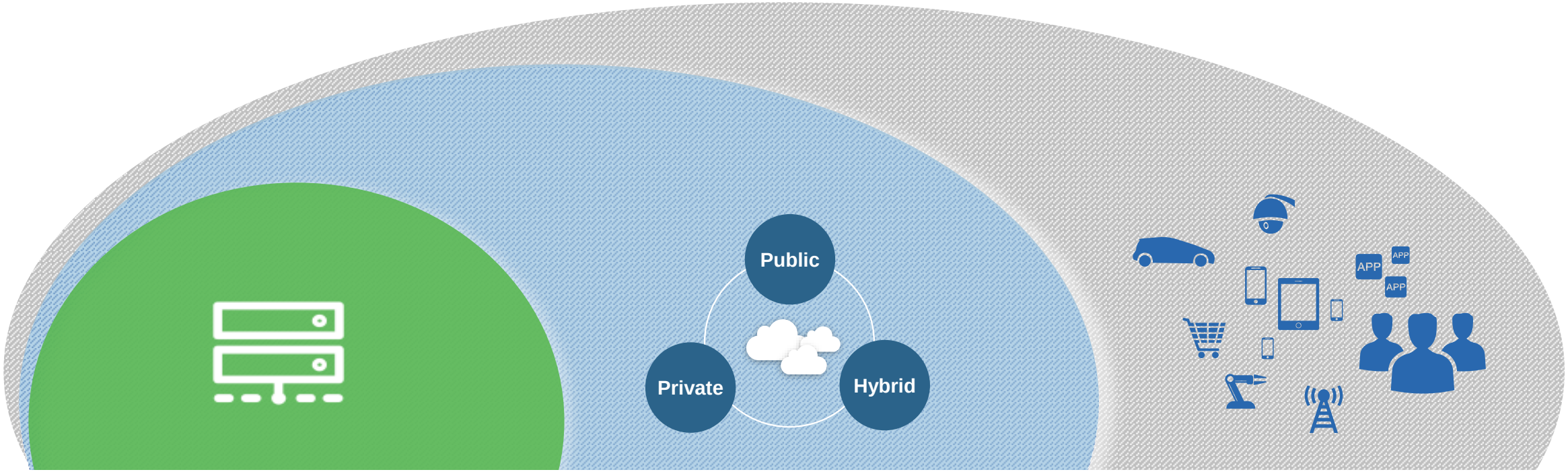
CloudLock **Cloud Security Fabric™**

- Анализ поведения пользователей
- Прикладной МСЭ
- DLP
- Управление шифрованием
- Безопасность конфигурации
- Централизованный аудит

CloudLock: контроль облака из облака



Обеспечение кибербезопасности должно быть целостным

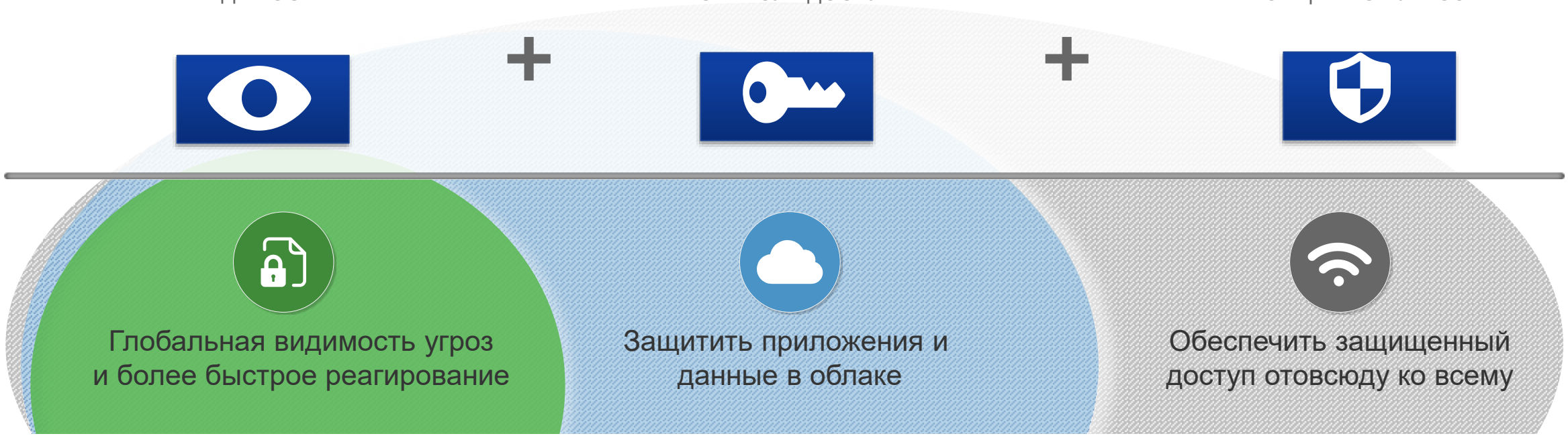


Корпоративный периметр **Облако** **Пользователи/устройства**

Повсеместная безопасность

Облачная безопасность

ВИДИМОСТЬ + КОНТРОЛЬ ДОСТУПА + ЗАЩИТА ОТ УГРОЗ



Корпоративный периметр **Облако** **Пользователи/устройства**

Безопасность из облака

Безопасность для облака

CISCO

Начните день с Cisco Secure Cloud

Все описанные технологии и решения можно протестировать

1. Попробовать **Cisco Umbrella** можно здесь
2. По прежнему бесплатен **OpenDNS Premium DNS** и OpenDNS Home
3. **Meraki MDM** (бесплатно до 100 мобильных устройств)
4. Записаться на тест **CloudLock**
5. Бесплатная оценка безопасности использования облачных технологий в Вашей организации **CloudLock Security Assessment**

Больше информации http://www.cisco.com/c/en/us/solutions/cloud/security.html

Спасибо