OpenDNS

Безопасность из облака. Опыт зарубежных образовательных учреждений. Cisco OpenDNS

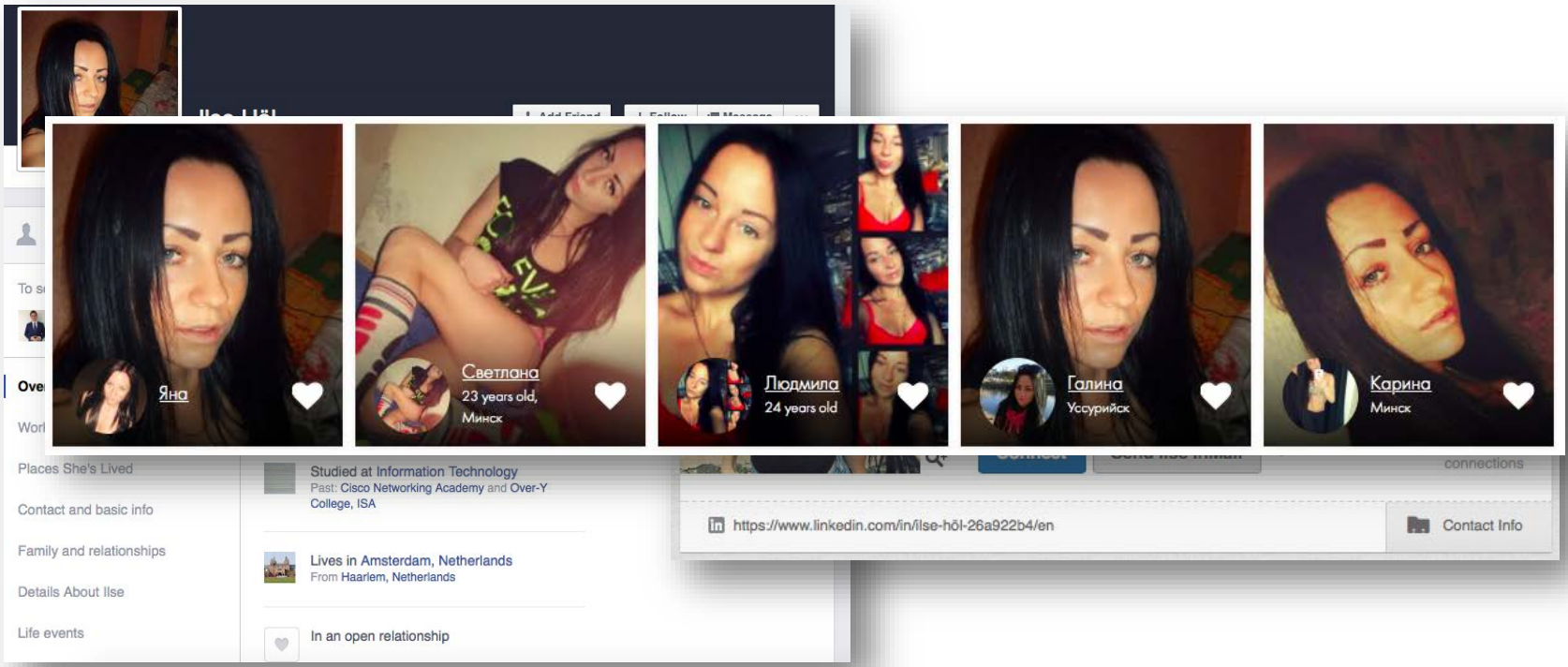
Назим Латыпаев, EMEAR
Системный инженер

OpenDNS is
now part of Cisco.

cisco

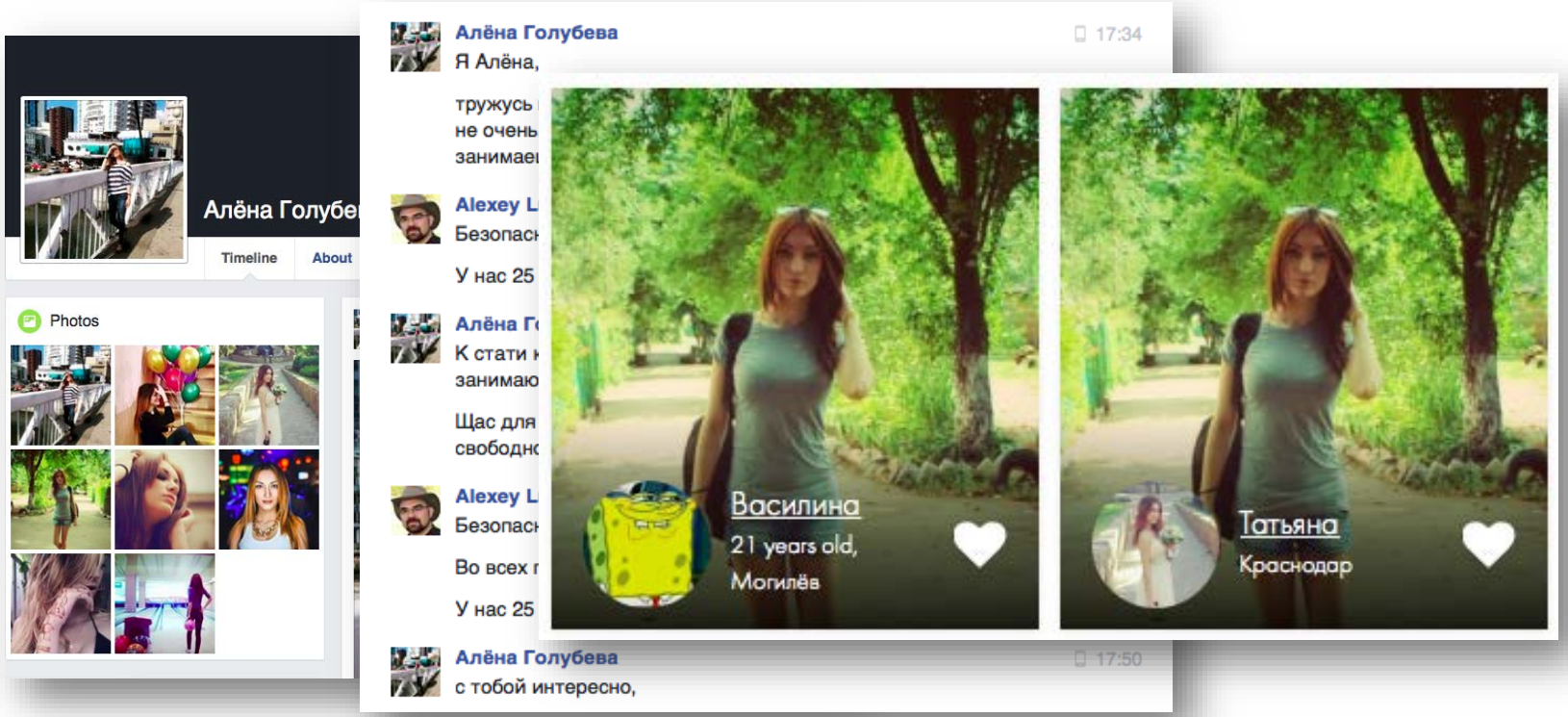
Как злоумышленник проводит разведку вашей сети?

Красивая приманка

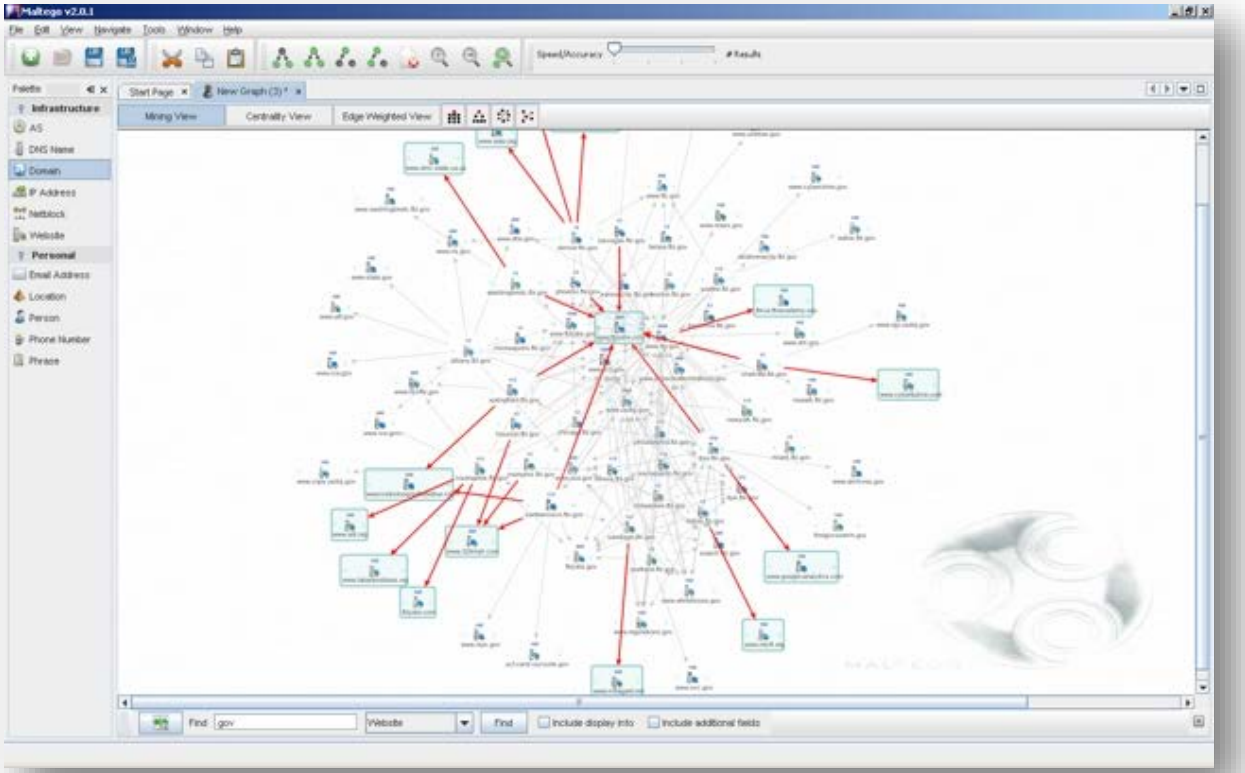


OpenDNS

Не только через почту, но и через соцсети



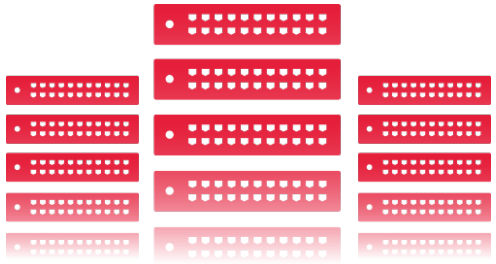
OSINT (Open-source intelligence): Maltego



OpenDNS

DNS: слепая зона для безопасности

Популярный протокол, который используют злоумышленники для управления, утечки данных и перенаправления трафика



91,3%

Вредоносного ПО использует DNS

68%

Организаций **не** мониторят его

Какие протоколы используют вымогатели?

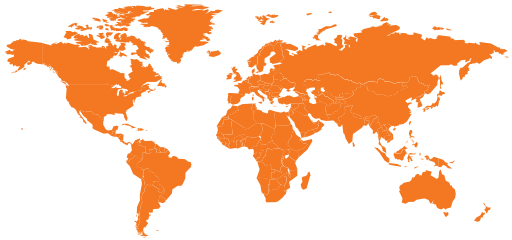
	Шифрование C&C				Шантаж
ИМЯ	DNS	IP	NO C&C	TOR	ОПЛАТА
Locky	●	●			DNS
SamSam			●		DNS (TOR)
TeslaCrypt	●				DNS
CryptoWall	●				DNS
TorrentLocker	●				DNS
PadCrypt	●				DNS (TOR)
CTB-Locker	●			●	DNS
FAKBEN	●				DNS (TOR)
PayCrypt	●				DNS
KeyRanger	●			●	DNS

Почему OpenDNS?

DNS-службы - для самой большой в мире платформы по обеспечению безопасности

ГЛОБАЛЬНАЯ СЕТЬ

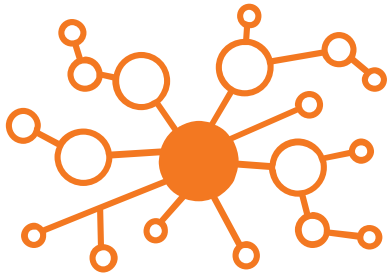
- более 80 млрд DNS-запросов в день
- более 65 млн корпоративных и частных пользователей
- 100%-ная бесперебойная работа
- любой порт, протокол, приложение



+

УНИКАЛЬНАЯ АНАЛИТИКА

- исследовательская группа по безопасности
- автоматическая классификация
- обмен между одноранговыми узлами BGP
- механизм 3D-визуализации



=

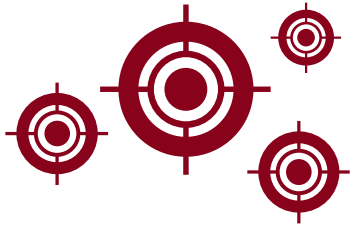
более 80 млн

вредоносных запросов блокируется ежедневно

Общие проблемы обеспечения безопасности

50% компьютеров — мобильные
70% офисов — удаленные

Большинство мобильных и удаленных сотрудников не всегда включают VPN, большинство филиалов не обеспечивают обратный транзит трафика, а большая часть новых оконечных устройств только обнаруживают угрозы



70-90% вредоносного ПО уникально для каждой организации

Средства на основе сигнатур, реактивный интеллектуальный анализ угроз и отдельное применение политик безопасности не могут опередить атаки

Недостаток квалифицированных специалистов в сфере безопасности

Для многих средств требуется больше ресурсов, чем имеется для выполнения работы

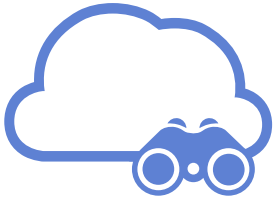
Проблемы, которые мы решаем

Защита от вторжений и вредоносного ПО

Предотвращение утечки данных и дискредитации систем с помощью блокировки обратных отзывов C2 и вредоносных сайтов

Мониторинг по всему Интернету

Ускорение реагирования на инциденты с актуальной, обновляемой в реальном времени
картиной Интернета



Веб-фильтрация и мониторинг облака и «Интернета вещей»

Внедрение приемлемого использования, просмотр используемых облачных служб и устройств «Интернета вещей»
и обеспечение безопасности гостевого Wi-Fi

менее 30

МИНУТ ДЛЯ ГЛОБАЛЬНОГО ОХВАТА

Использование DHCP или AP-контроллеров, защита тысячи устройств и местоположений

более чем в 2 раза

ОПРЕДЕЛЕННЫХ ДИСКРЕДИТИРОВАННЫХ СИСТЕМ

В сравнении с традиционными системами безопасности сети/оконечных устройств или другими средствами защиты от сложных угроз

в 10 раз

СНИЖЕНИЕ ЛОЖНЫХ УВЕДОМЛЕНИЙ

Благодаря интеграции нашего стратегического анализа угроз в ваши процессы SIEM и IR через наши API-интерфейсы

1 и более

СОТРУДНИКОВ БЕЗОПАСНОСТИ ОБСВОБОЖДАЕТСЯ

Снижение затрат на эксплуатацию и обслуживание, меньшее количество зараженных устройств, которых необходимо восстанавливать, и более эффективное реагирование на инциденты

ДОБАВЛЕННАЯ ИЗМЕРЯЕМАЯ ЦЕННОСТЬ

OpenDNS

ПРОДУКТЫ И ТЕХНОЛОГИИ

UMBRELLA

Применение

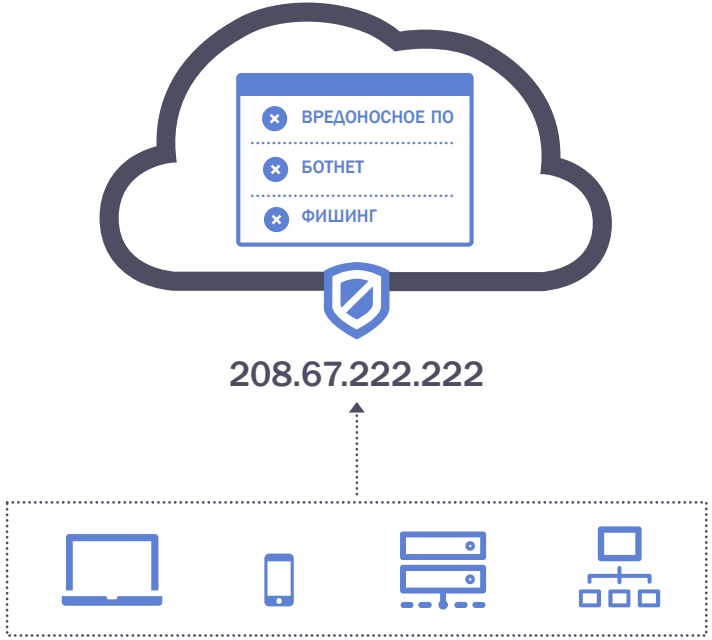
Служба сетевой безопасности защищает любое устройство, в любом месте

INVESTIGATE

Аналитика

Обнаружение и прогнозирование атак до того, как они происходят

OpenDNS UMBRELLA



Новый уровень защиты от вторжений с мониторингом по всему Интернету внутри или вне сети

Расширение ATD (FireEye) за пределы периметра и выполнение незамедлительных действий на IOC (Cisco)

Определение целенаправленных атак путем сравнения вашей активности с мировой практикой

Исследование атак с помощью графиков Интернет-активности в реальном времени

OpenDNS

Интеграция «под ключ» на базе API-интерфейсов

Работа с уже имеющимся ПО

ВЫЯВЛЕНИЕ УГРОЗ

FireEye Check Point SOFTWARE TECHNOLOGIES LTD. + ДРУГИЕ

АНАЛИЗ УГРОЗ И ИНТЕЛЛЕКТУАЛЬНЫЕ ИСТОЧНИКИ ДАННЫХ

cisco ZEROFOX + ДРУГИЕ

ИНТЕЛЛЕКТУАЛЬНЫЕ ПЛАТФОРМЫ ПО БОРЬБЕ С УГРОЗАМИ

THREATQUOTIENT THREATCONNECT + ПОЛЬЗОВАТЕЛЬСКИЕ

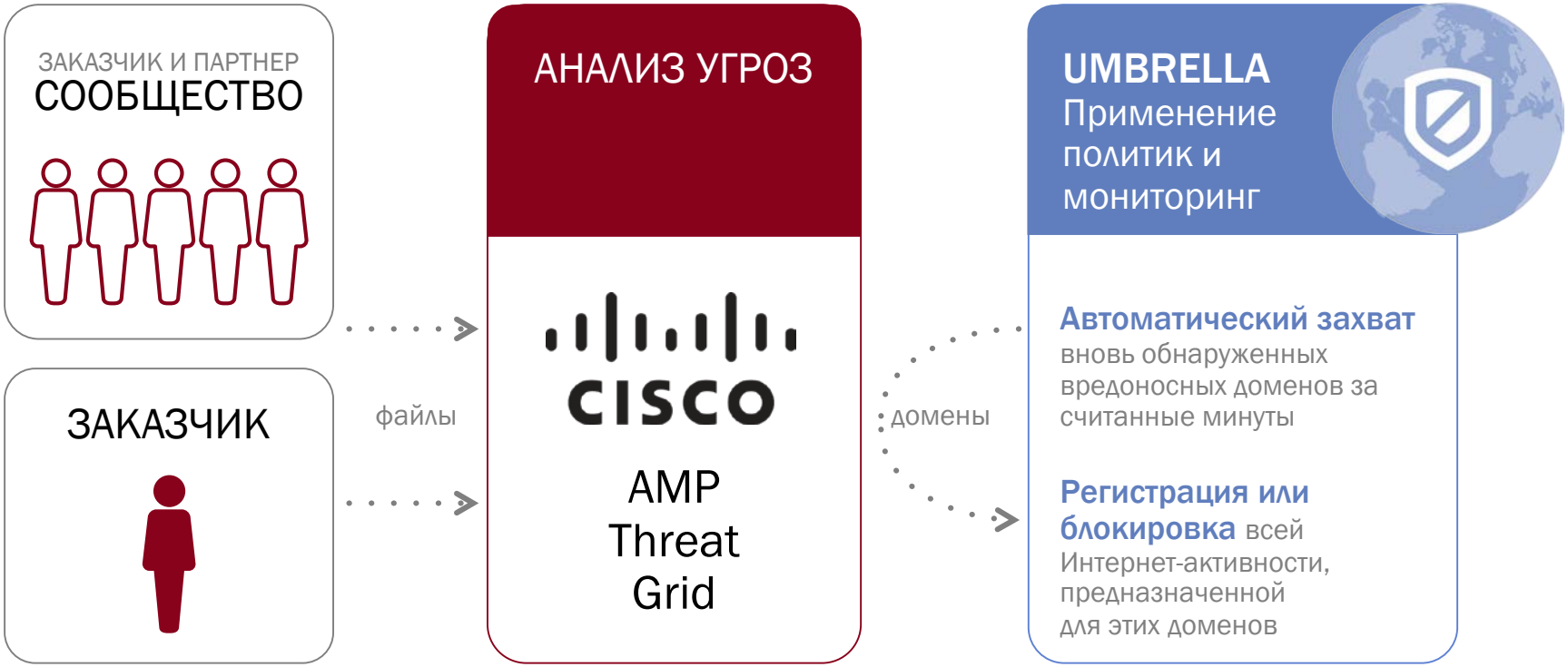
Индикаторы компрометации

UMBRELLA

Применение политик и мониторинг

Регистрация или блокировка доменов, отправленных партнером или пользовательскими системами

Автоматизация защиты для снижения времени реакции на атаку



OpenDNS

Новый уровень защиты от вторжений

UMBRELLA

Применение политик

Предотвращение угроз
Не просто обнаружение угроз

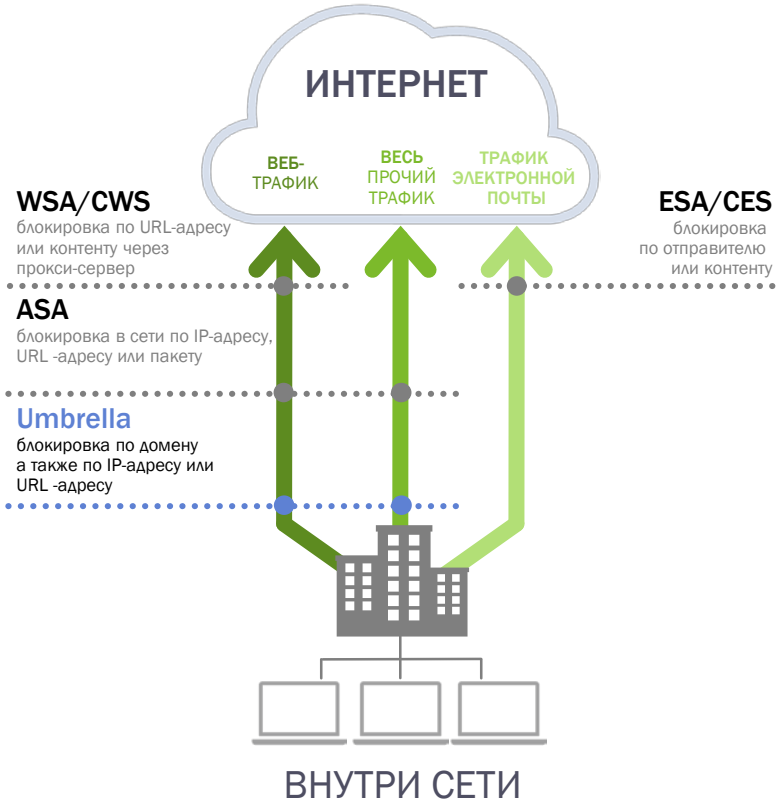
Защита внутри и вне сети
Не ограничивается устройствами, передающими трафик через локальные устройства

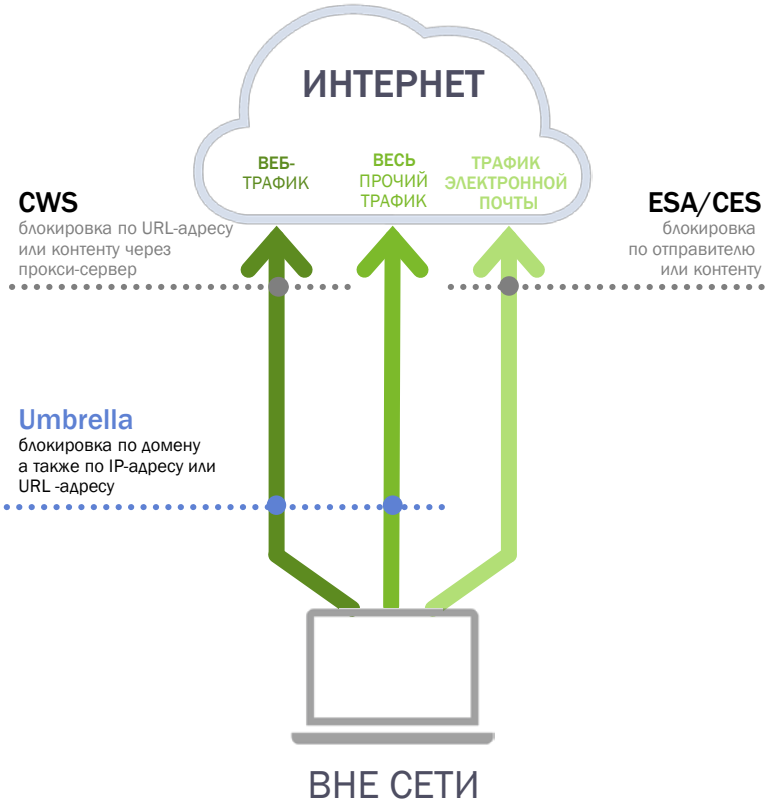
Постоянное обновление
Устройству не нужно обращаться к VPN на локальном сервере для получения обновлений

Блокировка каждого домена для всех портов
Не только IP-адреса или домены только через порты 80/443

Интеграция с партнерским и пользовательским ПО
Не требует услуг профессионалов при настройке

Области применения Umbrella





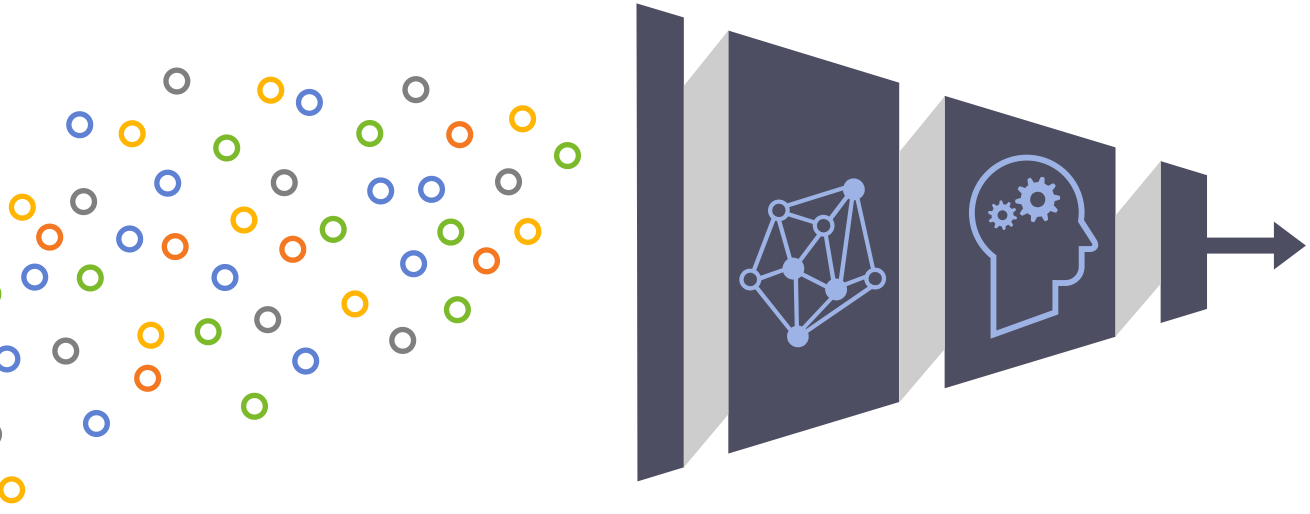
OpenDNS

Как работает наша классификация безопасности

Прием
миллионов точек ввода данных в секунду

Применение
статистических моделей и человеческого интеллекта

Идентификация
возможных вредоносных сайтов



Стратегия Cisco

OpenDNS обеспечивает дополнительную облачную сетевую безопасность

Платформа SaaS
и глобальная сеть

Быстрое развертывание
и применение технологии
для многих решений

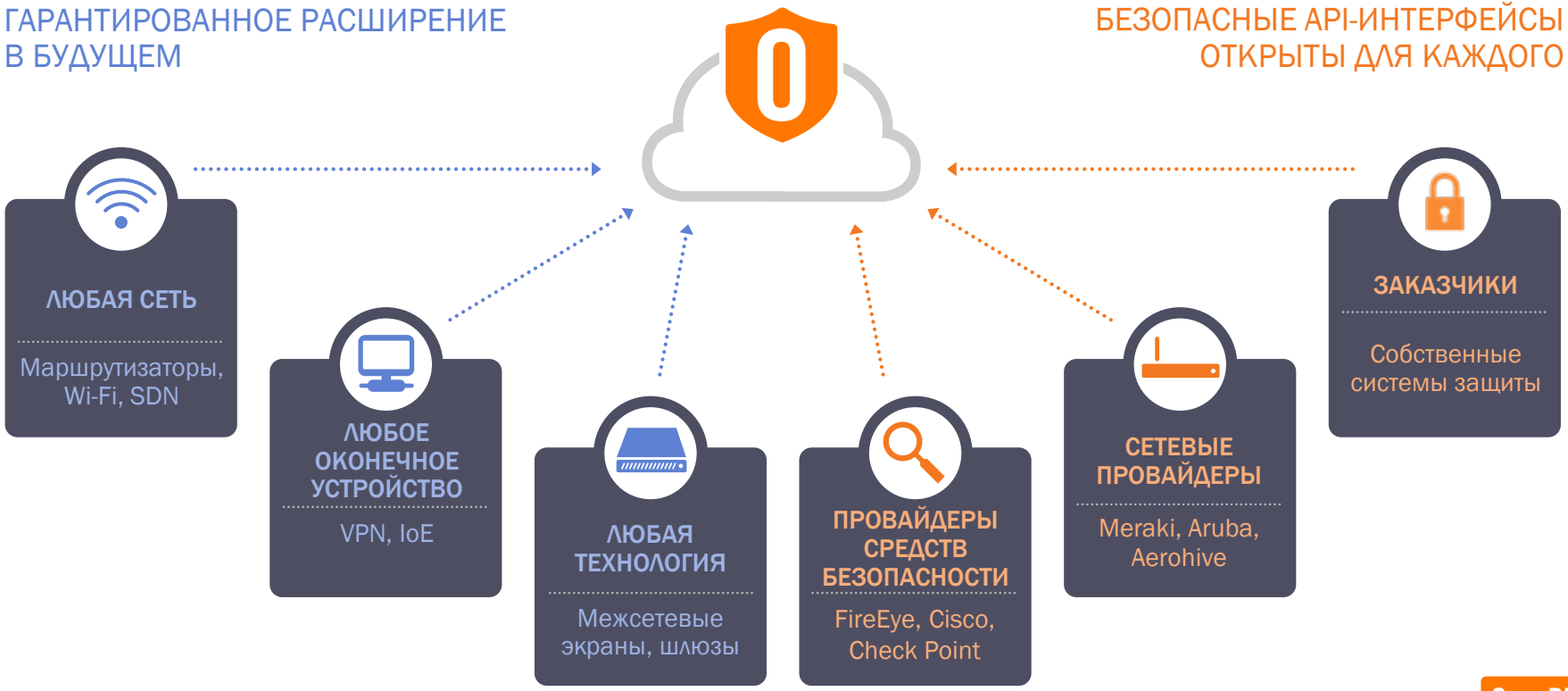
Анализ угроз
мгновенно
превращается
в предотвращение
угроз

Применение
статистических
моделей
на массивном
и разнообразном
наборе данных

OpenDNS работает со всеми вашими программами

ГАРАНТИРОВАННОЕ РАСШИРЕНИЕ
В БУДУЩЕМ

БЕЗОПАСНЫЕ API-ИНТЕРФЕЙСЫ
ОТКРЫТЫ ДЛЯ КАЖДОГО



OpenDNS

OpenDNS добавляет преимущества портфелю решений Cisco для обеспечения безопасности

до, во время и после атаки

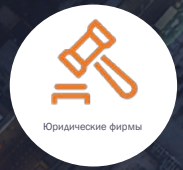
опережение будущих атак с помощью блокировки вредоносных доменов, IP-адресов и ASN

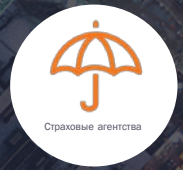
блокировка обратных вызовов и утечки с любого порта, протокола или приложения на уровне DNS и IP

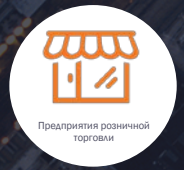
анализ угроз на основе запросов в реальном времени всех доменов и IP-адресов в Интернете

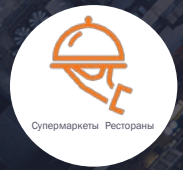
OpenDNS

Предприятия по всему миру используют OpenDNS









OpenDNS

Учебные заведения по всему миру используют OpenDNS

https://www.opendns.com/enterprise-security/customers/#filter=higher-education

Запуск через 30 секунд...Правда!

1

ОБЛАЧНЫЕ СЛУЖБЫ С ПОЛНЫМ ЦИКЛОМ ИСПЫТАНИЙ ПРИ ВВОДЕ В ЭКСПЛУАТАЦИЮ

Отслеживание DNS-трафика из одного места без ПО или оборудования и без изменения топологии сети или конфигурации устройств.

2

ПОКРЫТИЕ ВНЕ СЕТИ И МОНИТОРИНГ КАЖДОГО УСТРОЙСТВА

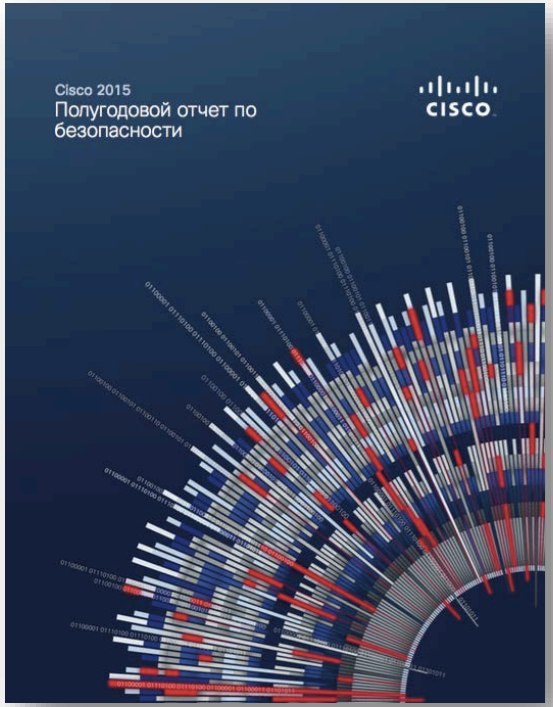
Защита наиболее слабых звеньев и определение, какое конкретное устройство (или пользователь) является целью атак; требуется ПО с самостоятельным обновлением

3

РАСШИРЕННАЯ ЗАЩИТА И ОБОГАЩЕНИЕ ДАННЫМИ ЧЕРЕЗ API-ИНТЕРФЕЙСЫ

Помощь группам SOC в извлечении большей ценности из существующих инвестиций, таких как FireEye, и группам реагирования на инциденты для ускорения расследований угроз

Дополнительная информация про угрозы



OpenDNS

OpenDNS is
now part of Cisco.