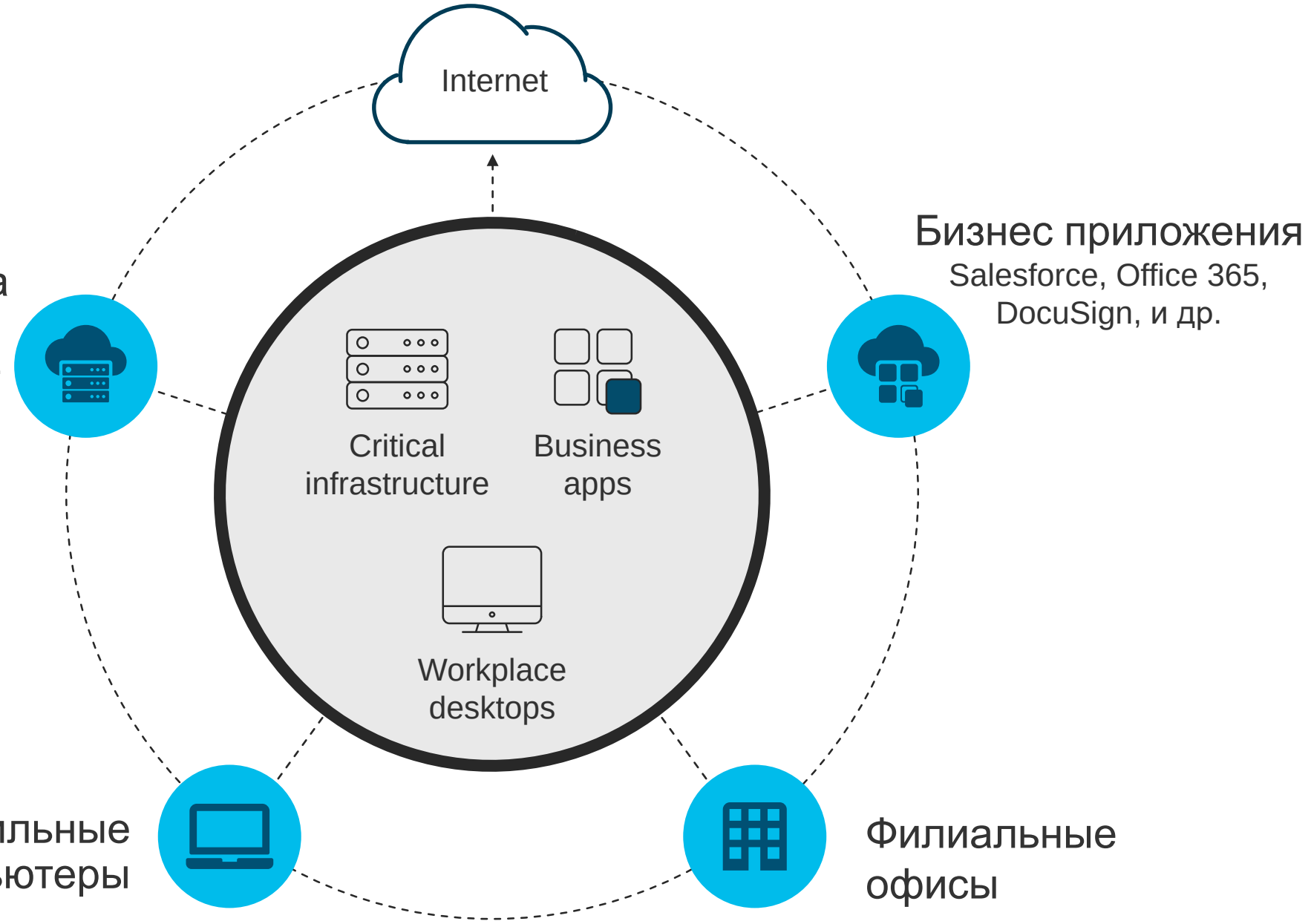
Cisco Umbrella

Безопасный DNS

Гузелия Мошнина
Специалист по информационной безопасности
2018

Как IT строилось ранее

IT Сегодня



Изменилось то как мы работаем...
И наша безопасность

49%
Работников станут мобильными

82%
Предпочитают не включать VPN

70%
Рост использования SaaS

70%
Филиальных сетей имеют прямой доступ в Интернет

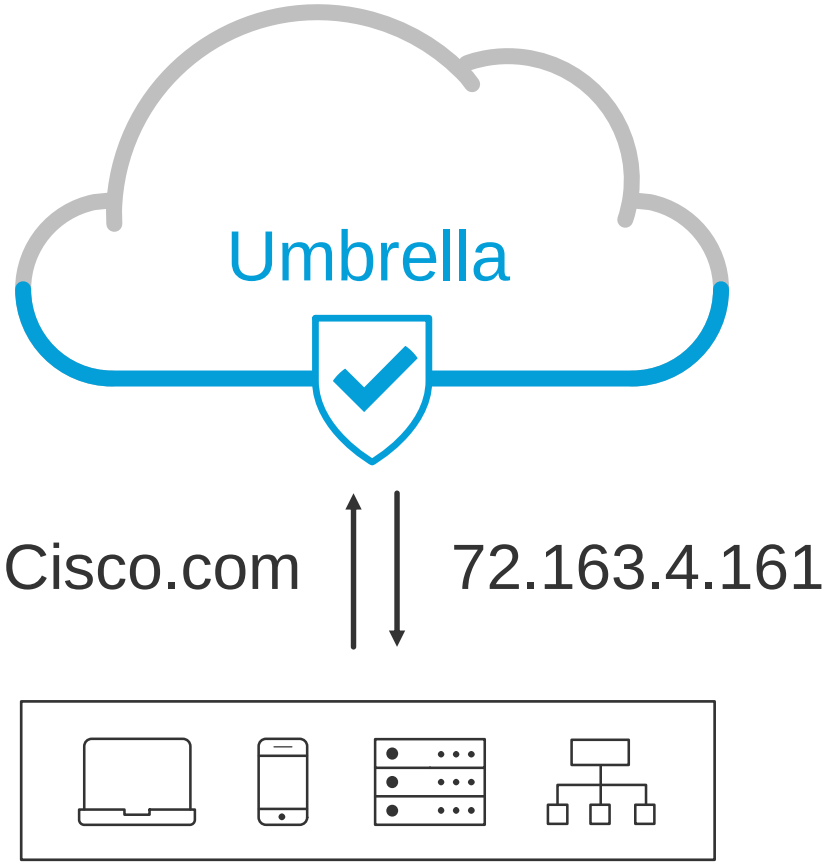
Cisco Umbrella

Защита веб доступа на уровне DNS

Все начинается с DNS

DNS = Domain Name System

- Первый шаг при доступе в интернет
- Предваряет запуск файла и IP соединения
- Использует любые устройства
- Не зависит от портов



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

Umbrella – это подписка на сервис и клиент

Внутри и снаружи корпоративной сети

Все порты и протоколы

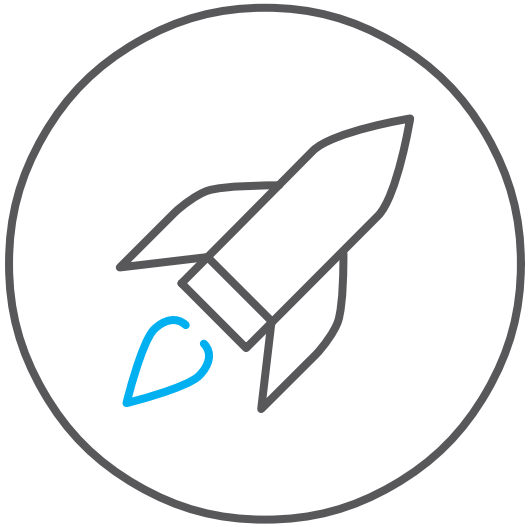
Проксирование и инспекция файлов

Обнаружение и контроль SaaS

Umbrella отличается от других

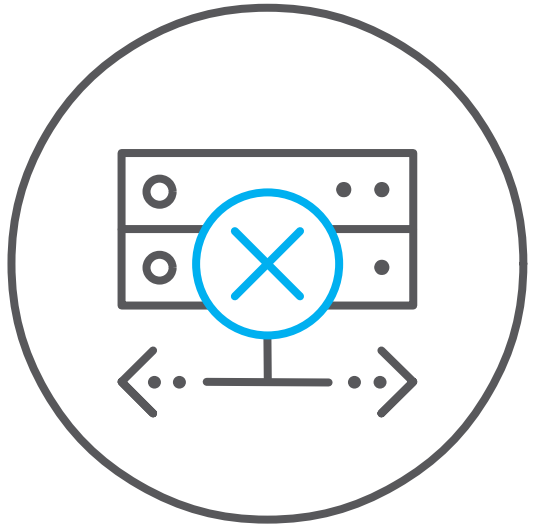
Концентрация на безопасности

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, ухудшающий сражение

Внедрение во всей организации за минуты

Подключение из офиса

Изменение одной настройки

Интегрирован с серией Cisco ISR 4K и Cisco WLAN контроллерами

Удаленные/мобильные пользователи

С помощью интеграции с AnyConnect VPN клиентом

Или с любым VPN используя легкий Umbrella клиент

Блокировка на лету, Аналитика offline

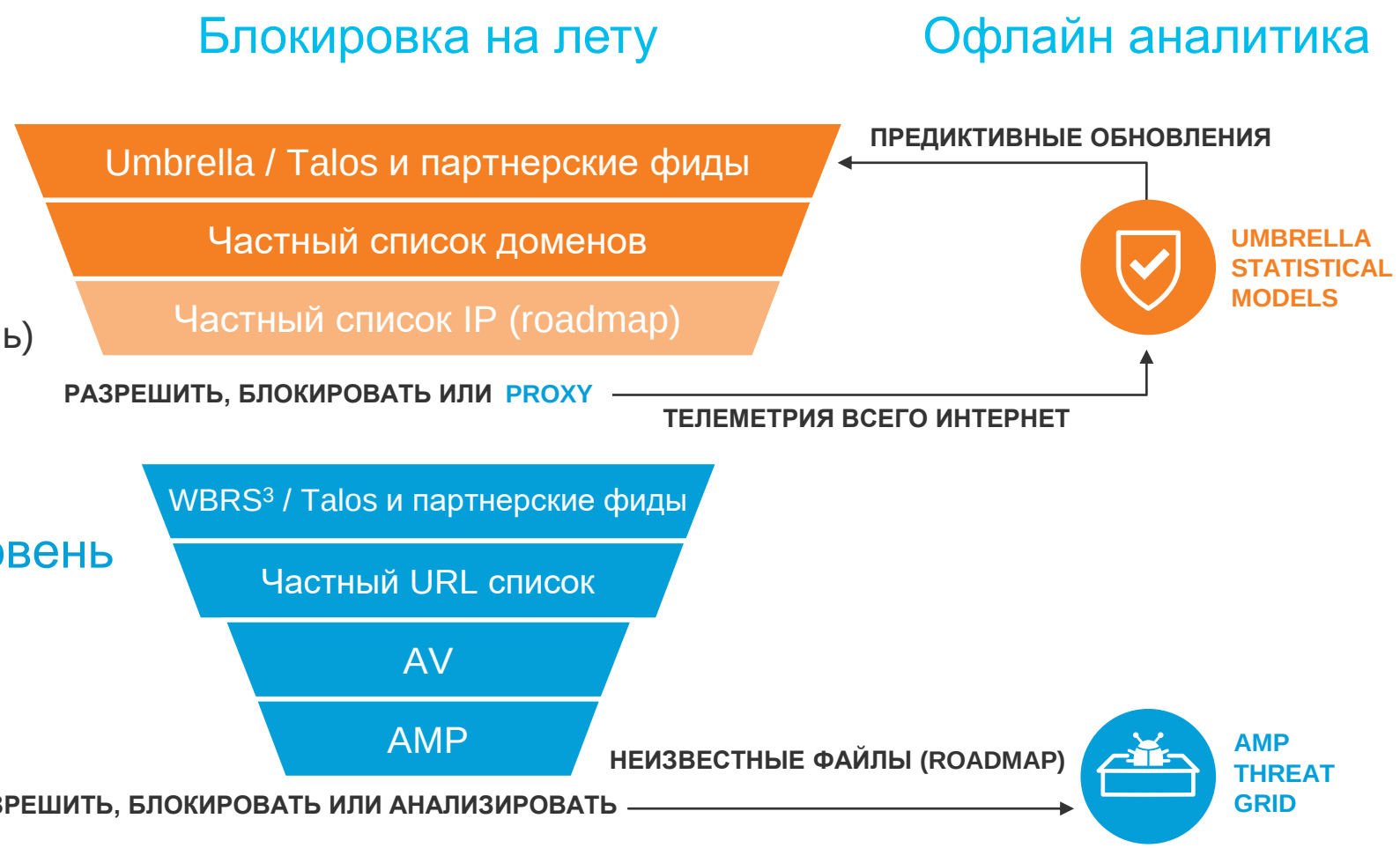
Широта покрытия всех портов и глубина инспекции рискованных доменов

DNS и IP уровень

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

HTTP/S уровень

- URL запрос
- Хэш файла

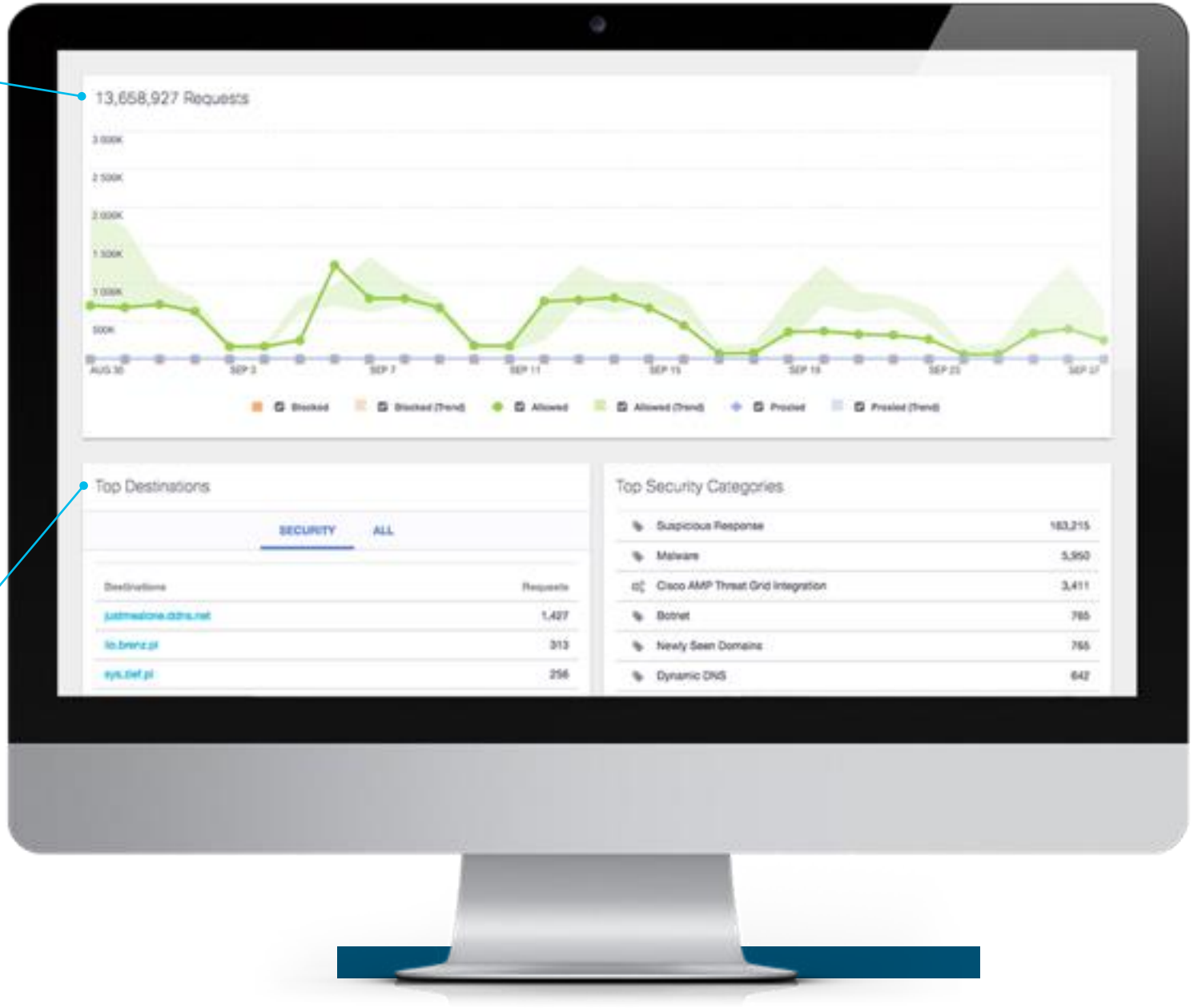


Allowed, blocked, and proxied traffic per device or network

IDENTITY REPORTS

Quickly spot and remediate victims

Top activity and categories per device or network

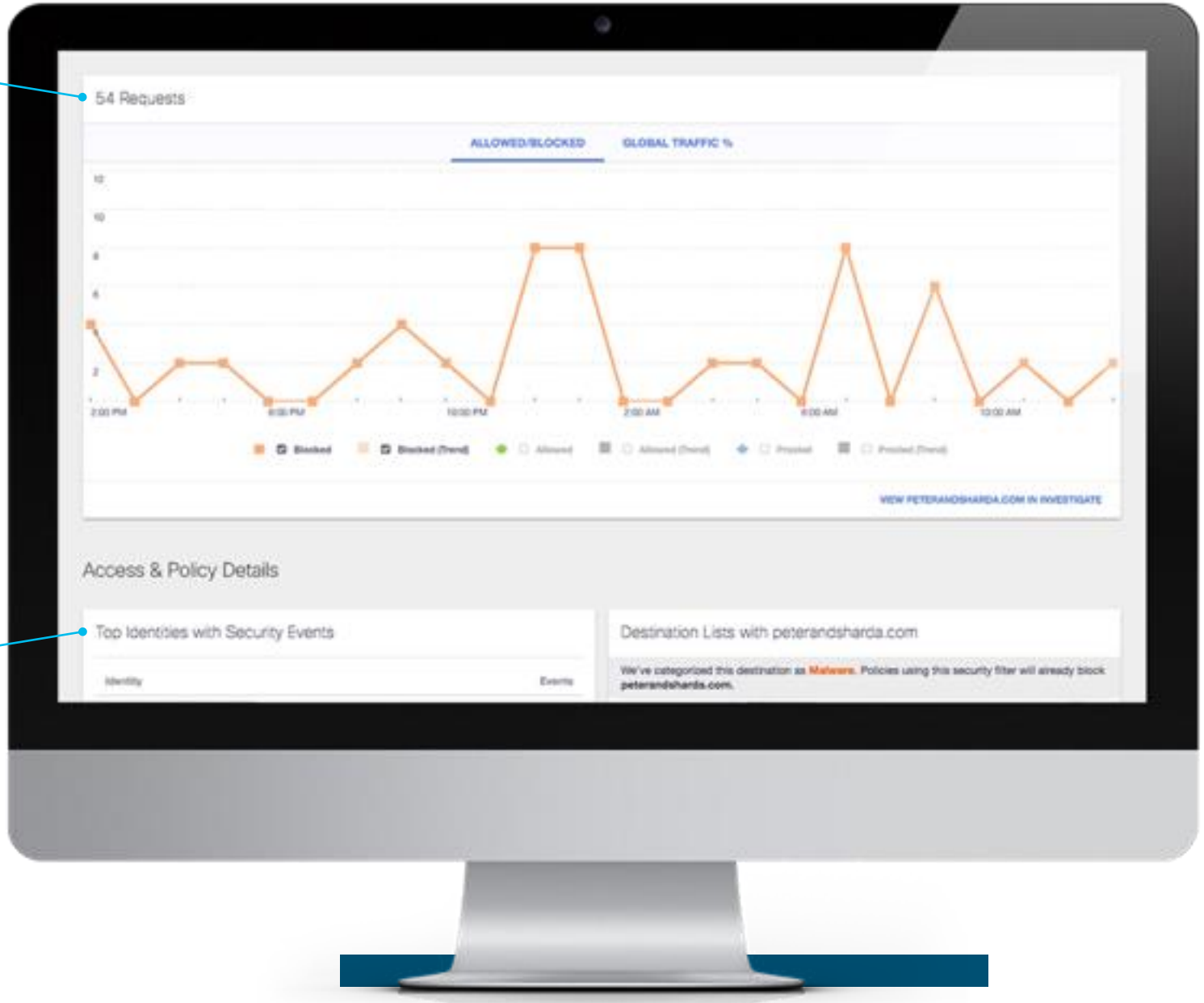


Local vs. global trends for malicious domains

DESTINATION REPORTS

Quickly assess extent of exposure

Top identities associated with malicious activity

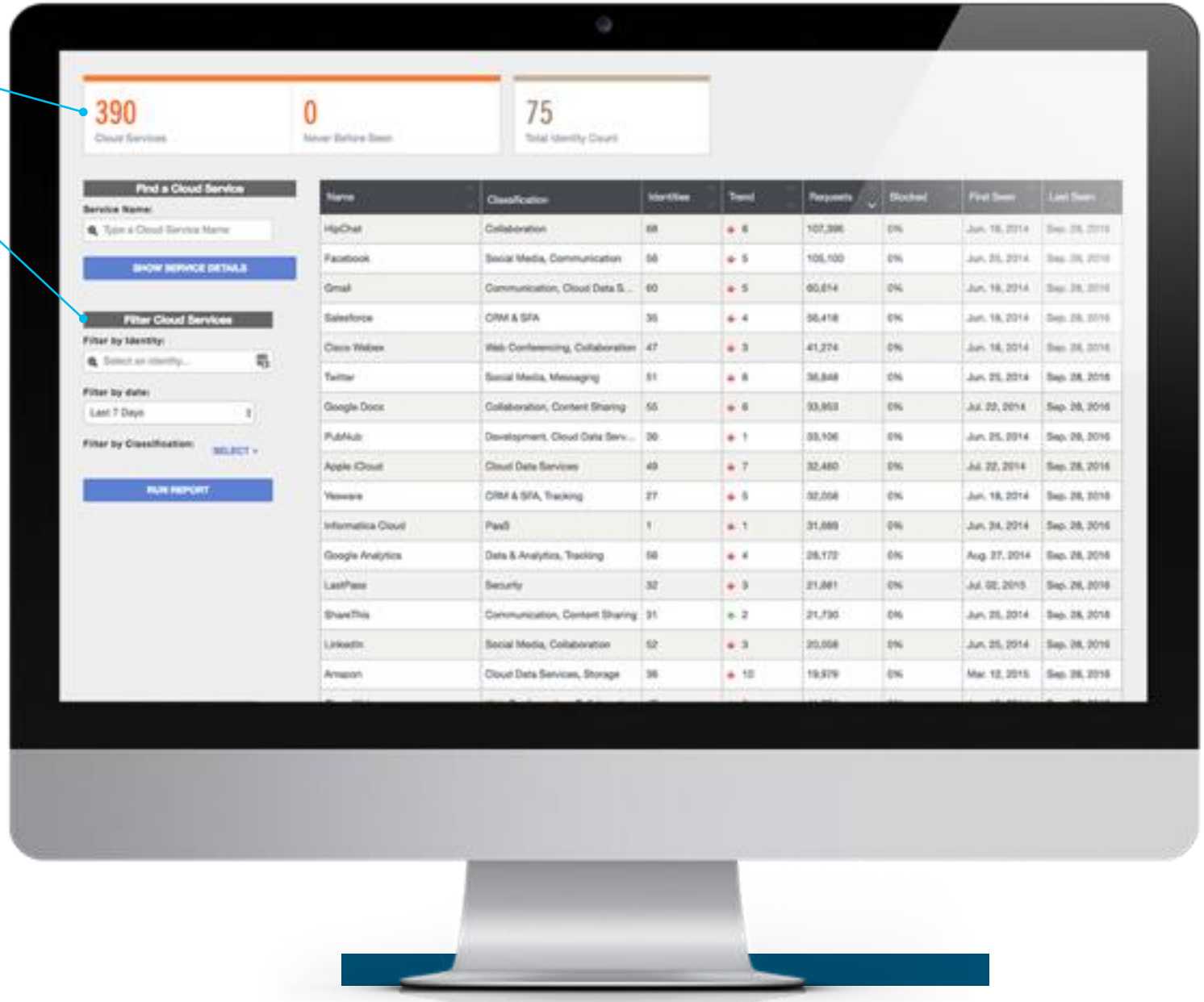


Total and newly seen cloud services

Cloud apps by classification and traffic volume

CLOUD SERVICES REPORT

Effectively combat shadow IT



Самое простое ИБ решение

1. Подпишитесь
2. Направьте ваш DNS
3. Готово