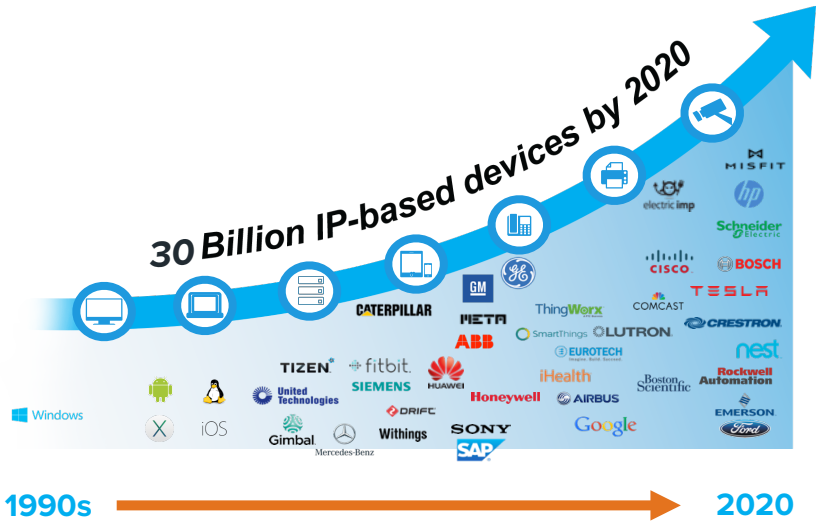
FORESCOUT

Трансформация безопасности через видимость сети™

Даниил Вылегжанин
Product Manager Headtechnology Group
2021

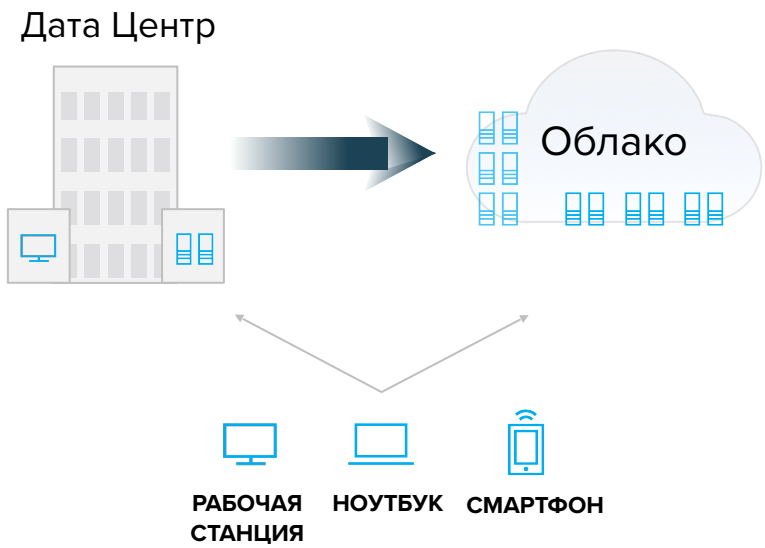
Слияние макро трендов создает проблемы видимости

Рост Количества Устройств и Разнообразие Платформ



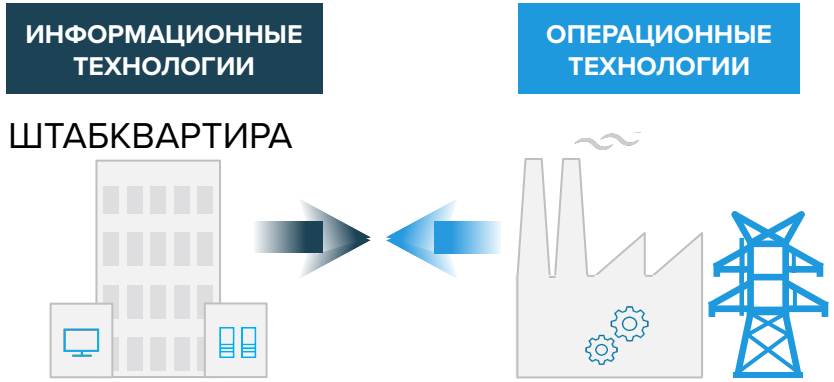
- Бесчисленные вариации операционных систем (ОС)
- Нет возможности устанавливать агентское ПО
- Нет возможности писать агентское ПО для каждой версии ОС

Внедрение Облаков Создает Новые Проблемы



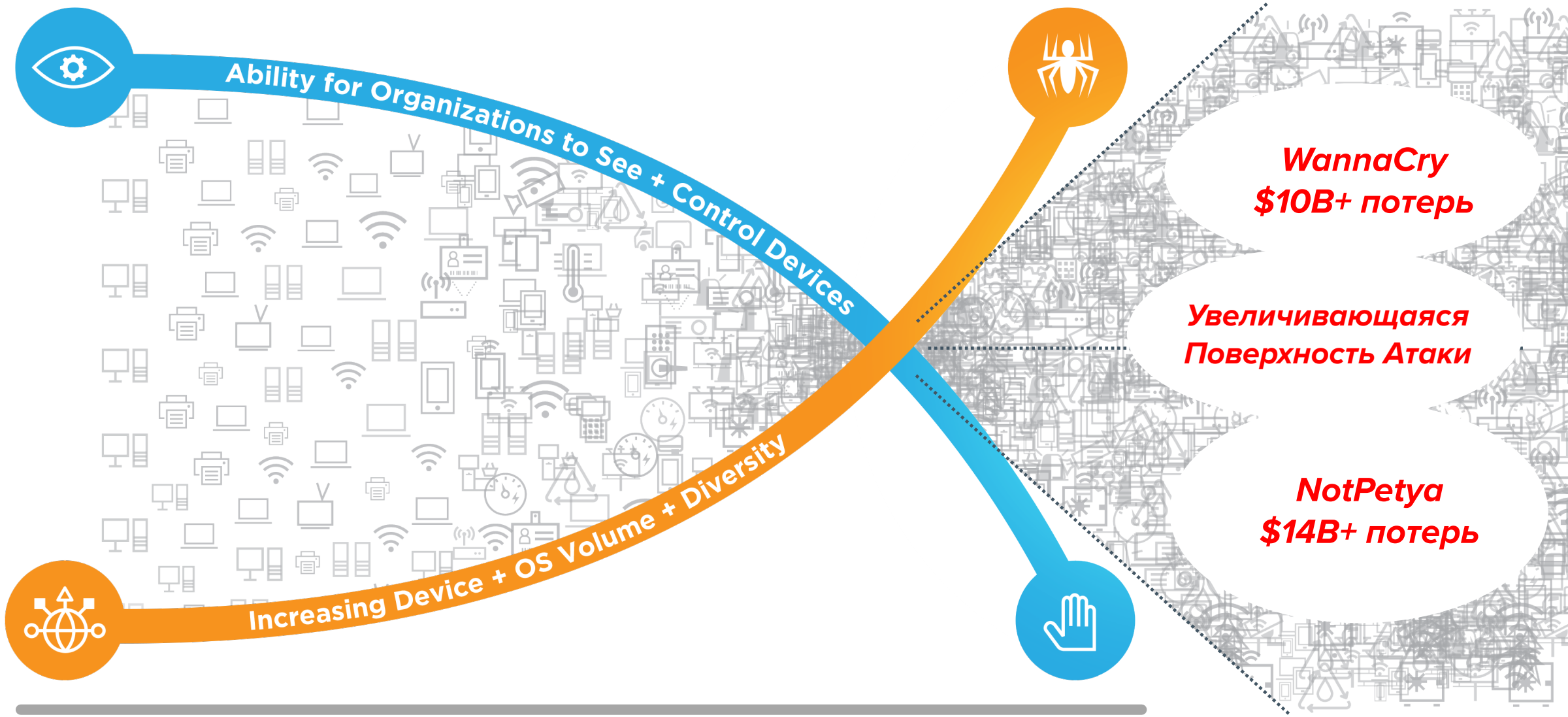
- Множество точек доступа в сеть и распределенность сети
- Гетерогенная среда с множеством вендоров
- Децентрализованное управление

Слияние ОТ и IT Повышает Риски



- ОТ сети теперь не разделены физически
- Угрозы, перемещающиеся между кибер- и физическими измерениями
- Активы очень уязвимы и редко могут быть пропатчены

Вопрос Видимости и Контроля встает все острее



Необходимо, но трудно достигнуть

Способность непрерывно обнаруживать, классифицировать и оценивать каждое IP-подключенное устройство, которое появляется в сети.

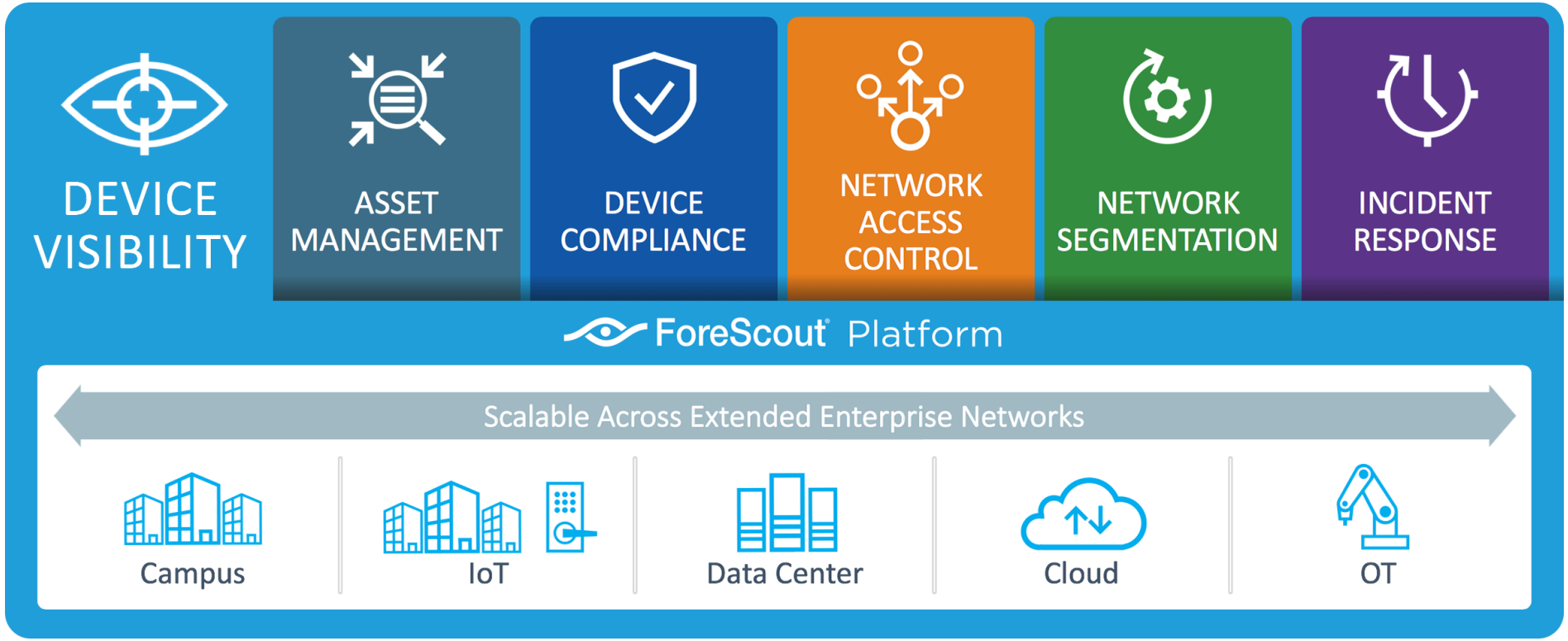
Challenges for Business:

- В среднем, компании имеют на **~30% больше подключенных к сети устройств**, чем они предполагают
- Даже когда предприятия знают о подключении устройств, они часто не знают, **что они такое** и должны ли они вообще быть в сети
- **Аудиты** устройств часто сложные и часто **провальные**.

Технические Трудности:

- Агенты не поддерживаются и/или не разворачиваются на всех устройствах
- Практически нет информации об атрибутах устройств для классификации и оценки подключенных устройств
- Нет единого источника достоверных данных для всех подключенных устройств

ForeScout - это не просто NAC



DEVICE VISIBILITY

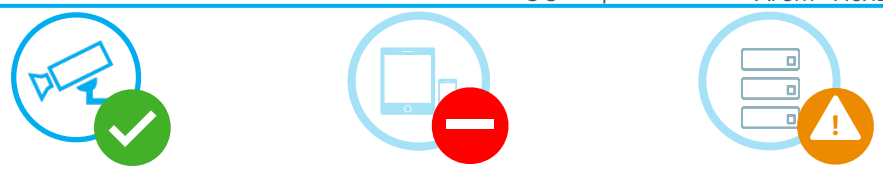
ЧТО мы делаем и КАК мы это делаем?

Что Мы Делаем

ОБНАРУЖИВАЕМ все IP-адресуемые устройство в момент их подключения к сети

КЛАССИФИЦИРУЕМ каждое устройство и категорируем соответственно

ОЦЕНИВАЕМ устройства по



Как Мы Это Делаем

Без агентов

- ✓ Не требуется агентов на устройстве
- ✓ Использование активных и пассивных техник

Гетерогенные сети

- ✓ Интеграция с 100+ моделями сетевого оборудования
- ✓ Покрываем все – ДЦ, Облака, АСУТП

Интеллектуально

- ✓ Device Cloud ~1500 клиентов предоставляют 12M профилей
- ✓ Обширная таксономия устройств в IT и OT

Непрерывно

- ✓ В режиме реального времени, поэтому нет необходимости планировать сканирование
- ✓ Механизм политик постоянно оценивает состояние устройств

ASSET MANAGEMENT

Challenges for Business:

- Большинство систем управления активами **заполняются людьми**, и поддержание данных в актуальном состоянии является сложной задачей
- Многие системы управления активами **не хранят данные** с неуправляемых машин, таких как IoT и OT
- Часто заказчики нанимают **дорогих консультантов**, чтобы те в ручную проводили инвентаризацию

ForeScout CounterACT

- **Автоматизировать** инвентаризацию активов, подключенных к IP, в сетях IT & OT
- **Точно определить** местоположение в режиме реального времени всех IP-подключенных устройств
- **Непрерывная** и точная оценка всех IP-подключенных устройств

Расширить/ Автоматизировать

- Актуализировать CMDB полной инвентаризацией устройств и контекстом
- **Информирование** UEM об устройствах BYOD, подключенных к корпоративной сети

CMDB

servicenow

UEM

IBM MobileIron vmware

DEVICE COMPLIANCE

Challenges for Business:

- **Ограниченные и устаревшие** данные о состоянии машины
- **Бреши в комплаенсе** для нетрадиционных устройств (например, огромные белые списки MAC)

ForeScout CounterACT

Отчет о состоянии патчинга для Microsoft Windows и Apple OSX

Определить за секунду, где расположены совместимые и несовместимые устройства

Сканирование определенных устройств на соответствие требованиям SCAP

Расширить/ Автоматизировать

Запуск системы управления уязвимостями для сканирования и обновления устройств, пропущенных при запланированных проверках.

Информирование внешних платформ об устаревших агентах и файлах сигнатур, а затем автоматическое исправление по мере необходимости

Управление Уязвимостями

RAPID7 Qualys. tenable

UEM/EPP/EDR/PAM

IBM MobileIron vmware Carbon Black. CROWDSTRIKE Symantec. McAfee CYBERARK

NETWORK ACCESS CONTROL

Challenges for Business:

- **Занимает годы, чтобы развернуть**
- Обычно требуется **дорогостоящее** обновление сети
- **Отсутствие поддержки гетерогенной** сетевой инфраструктуры
- **Зависимость** от агентов (802.1 x) ограничивает видимость устройств

ForeScout CounterACT

- **Взаимодействие** с более чем со 100 моделями сетевого оборудования позволяет избежать дорогостоящего обновления парка оборудования
- 802.1x **опционален**
- **Изолировать** несовместимые или зараженные устройства без изменения конфигурации сетевой инфраструктуры
- **Непрерывный** контроль гигиены устройства и автоматическое принятие мер, когда это необходимо

Расширить/ Автоматизировать

- **Сосуществование** с решениями 802.1 x на основе агентов

NAC

aruba a Hewlett Packard Enterprise company

cisco

FORTINET

NETWORK SEGMENTATION

Challenges for Business:

- Практически не существует механизмов для автоматизации процесса обновления многочисленных политик по мере **изменения и перемещения устройств**
- Большинство сетей большие и плоские и зачастую не имеют механизмов блокировки злоумышленников, когда **они уже попали во внутрь сети**
- **Разрастание политик сегментации из-за множественных решений**, обслуживающих различные части корпоративной сети
- **Ограниченное понимание** шаблонов трафика между устройствами

ForeScout CounterACT

- Автоматическое **создание** традиционных и виртуальных ACL- ов
- Динамически **назначать** объекты зонам на основе типа устройства, приложения, пользователя и местоположения

Расширить/ Автоматизировать

- **Предоставление** полной контекстной информации об устройстве и пользователе ведущим в отрасли поставщикам NGFW для обеспечения динамической сегментации
- **Обмен** контекстом с ведущими платформами виртуализации, микро-сегментации и облаков

NGFW

Check Point SOFTWARE TECHNOLOGIES LTD.

paloalto NETWORKS

FORTINET

Micro-segmentation

aws

vmware NSX

INCIDENT RESPONSE

Challenge for Business:

- Проблемы реагирования на инциденты при подключении новых устройств к сети в отсутствие их видимости
- Большинство IR команд не готовы к **инцидентам с IoT и OT**
- **Длительное среднее время реагирования** обеспечивает широкое горизонтальное распространение атак
- Неспособность **правильно расставить приоритеты** предупреждений и оценить критичность инцидентов

ForeScout CounterACT

- **Определение** устройств с высоким риском
- **Выполнение** предопределенного исправления для несоответствующих устройств во время подключения для уменьшения MTTR
- **Поиск** потенциально уязвимых устройств
- **Просмотр** из единого дашборда, отображающего общую работоспособность устройств на всем предприятии

Расширить/ Автоматизировать

- **Поиск** уязвимостей, IoC-ов и других атрибутов, предоставляемых ведущими решениями по обнаружению угроз, управлению уязвимостями и SIEM
- **Выполнение** действий реагирования, как требуют ведущие SOAR вендоры.

ATD / EDR

FireEye, paloalto NETWORKS, Check Point SOFTWARE TECHNOLOGIES LTD., Carbon Black., CROWDSTRIKE

SIEM

IBM, splunk>, ArcSight

Наше Видение Продукта

СТАНДАРТ ДЛЯ **ВИДИМОСТИ УСТРОЙСТВ** НА ВСЕМ ПРЕДПРИЯТИИ

Офис

IoT

Дата Центр

Облако

Операционные технологии

Почему Выбирают ForeScout

Видимость

В среднем обнаруживаем на 30% больше устройств

Оркестрация

Увеличение стоимости существующих инвестиций
Сокращение MTTR с помощью автоматизации

12M+ Профилей в Device Cloud

2M+ Устройств в одной инсталляции

85M+ Всего лицензий продано

FORESCOUT

3800+

Заказчиков в более чем 80 странах

Во всех основных отраслях промышленности, Правительства, Финансов, Здравоохранения, Телекома и Ритейла

Time-to-Value

65 дней – среднее время завершения проекта

83

Net Promoter Score

FORESCOUT

Спасибо за внимание

Даниил Вылегжанин
Product Manager Headtechnology Group
d.vylegzhanin@headtechnology.com