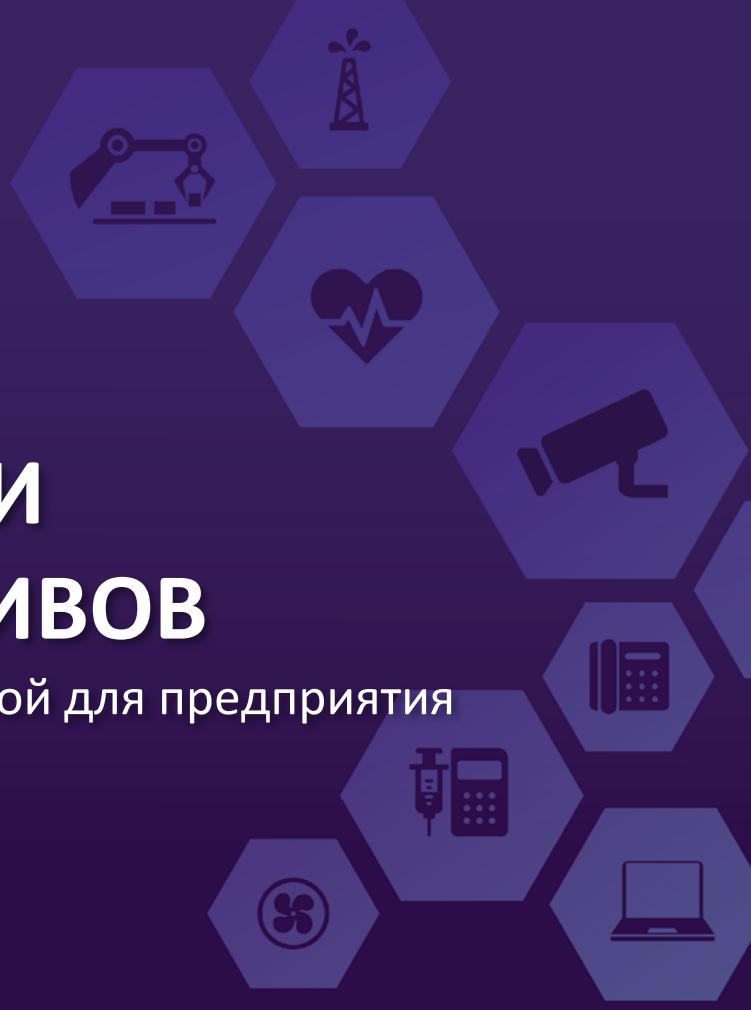
SOFTPROM



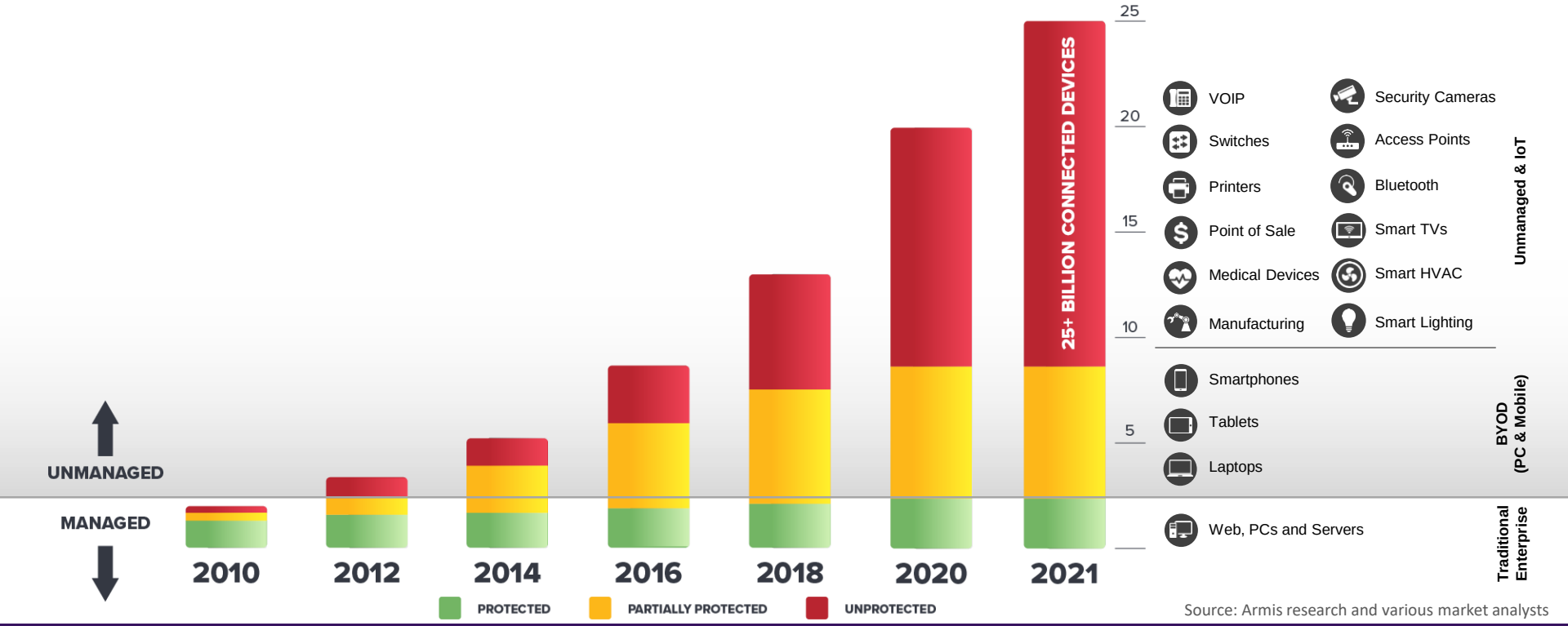
БЕЗАГЕНТНАЯ ЗАЩИТА И ИНВЕНТАРИЗАЦИЯ АКТИВОВ

Делая цифровую трансформацию безопасной для предприятия

ARMIS

Проблематика Традиционной Безопасности Конечных Точек

До 90% устройств будут «безагентными»



Source: Armis research and various market analysts

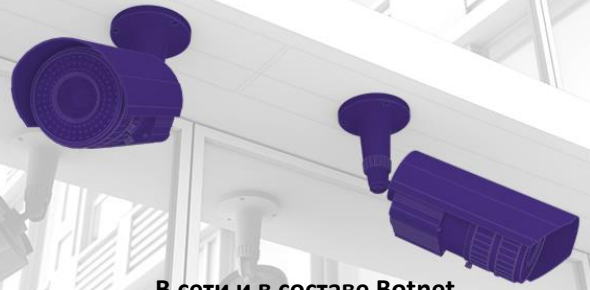
Скомпрометированный планшет

Потоковое видео с камеры из зала заседаний в неизвестное место

Скомпрометированный Smart TV

Заражен вымогателем, пытается атаковать другие устройства, подключенные к нему

Botnet Камера безопасности



В сети и в составе Botnet

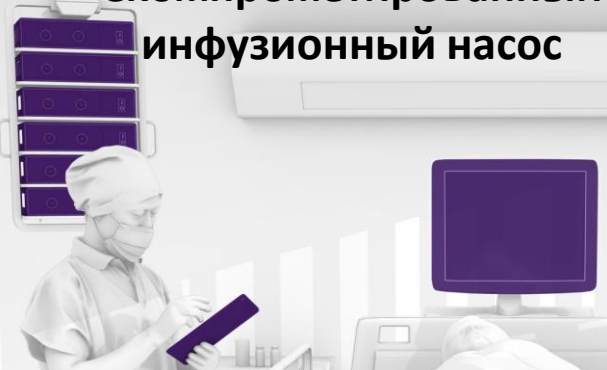
Производство

HMI производственной линии подвергся воздействию программ-вымогателей, перемещающихся по сети

Точка доступа беспроводного принтера

Открытая точка доступа, позволяющая хакерам обойти контроль доступа к сети

Скомпрометированный инфузионный насос



Инфузионный насос скомпрометирован вредоносным ПО при подключении к пациенту.

SOFTPROM

ARMIS

Платформа безопасности безагентных устройств

Инвентаризация активов

- Идентификация и классификация устройства
- Управляемый, неуправляемый и Интернет вещей
- Заполните сканеры уязвимостей и инструменты инвентаризации
- Каждое устройство на каждом сайте (марка, модель, ОС и т. Д.)
- В любой среде и в любой отрасли

Управление рисками

- Пассивная непрерывная оценка уязвимости в реальном времени
- Обширные базы данных CVE и соответствия
- Умная адаптивная оценка рисков
- Риск-ориентированная политика
- Автоматическая сегментация

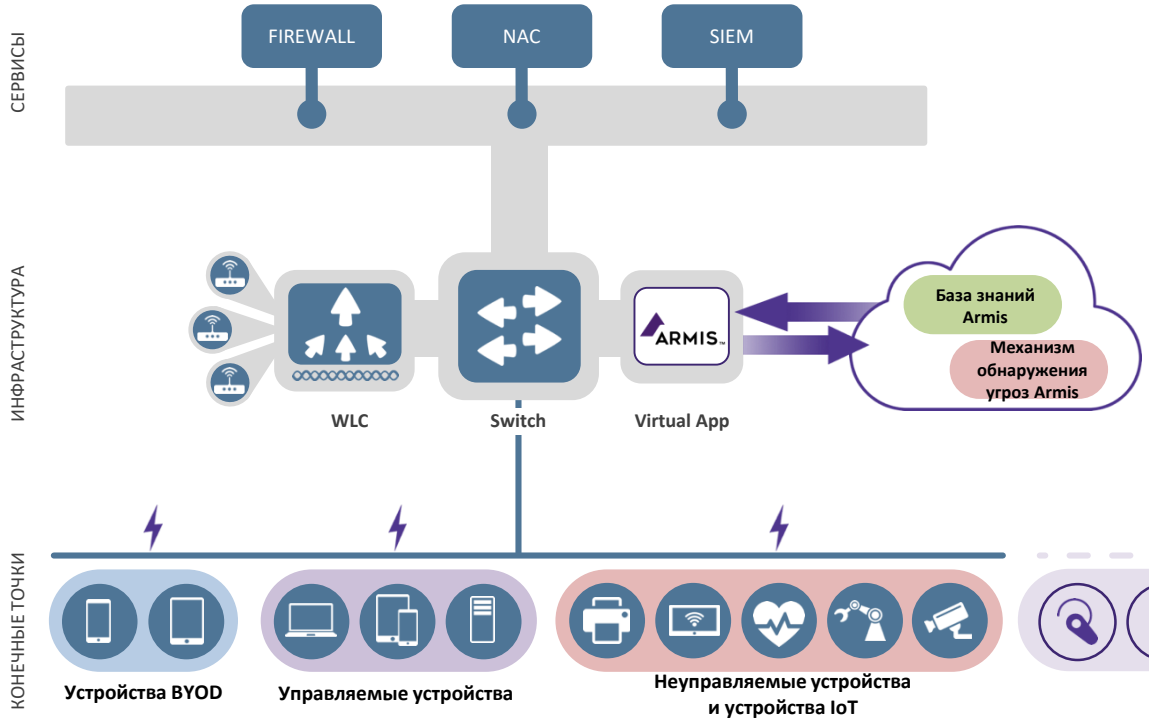
Detection & Response

- Атрибуция действий по устройствам
- Аномалии на основе КВ устройства
- Автоматический ответ на основе политик
- Возможность отключить или поместить в карантин
- Контекст устройства предоставляется каждому инструменту и рабочему процессу SOC (SIEM, Ticketing, Firewall, NAC и т. д.)

В реальном времени и непрерывно

ORACLE · Mondelēz International · Allergan · Sysco · PerkinElmer · MATTRESSFIRM

Как работает Armis

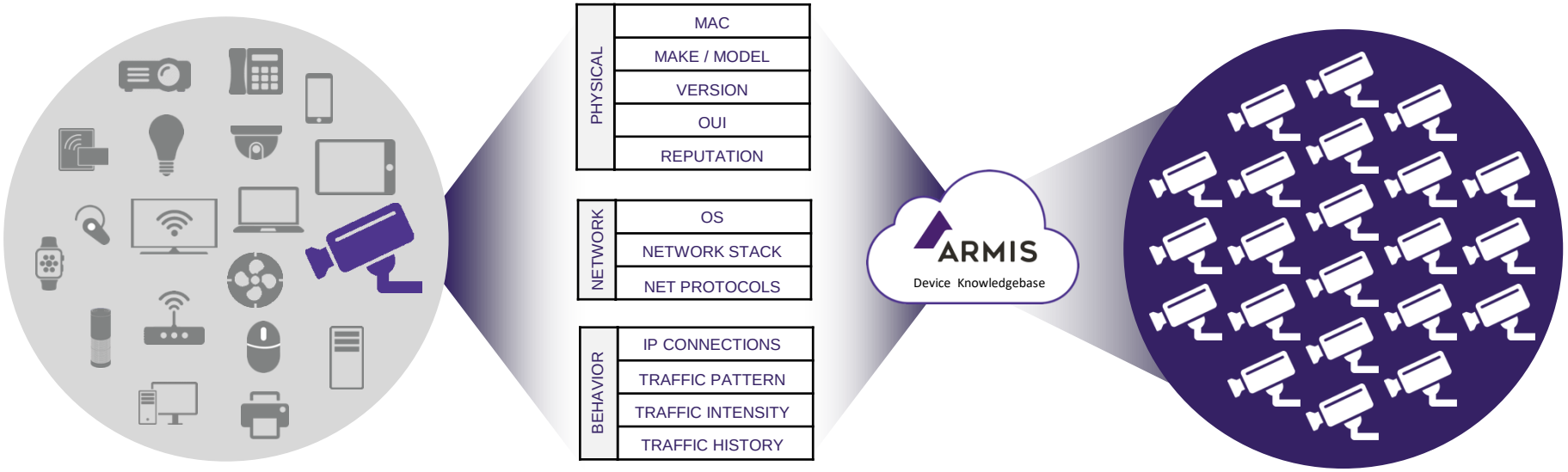


Легкость развертывания

- Нет агентов
- Развертывается от минут до часов
- Интегрируется с существующими решениями безопасности
- Нет влияния на сеть

SOFTPROM
ARMIS

Идентификация и отслеживание устройств без агента



Источники данных

- WLC - метаданные устройства, состояния подключения и т. д.
- AP - пакетный трафик, данные радиосигнала
- Switch - Span-порт или система захвата пакетов (например, Gigamon)
- Другое - Сеть / инфраструктура безопасности (например, брандмауэр для SYSLOG, наборы правил)

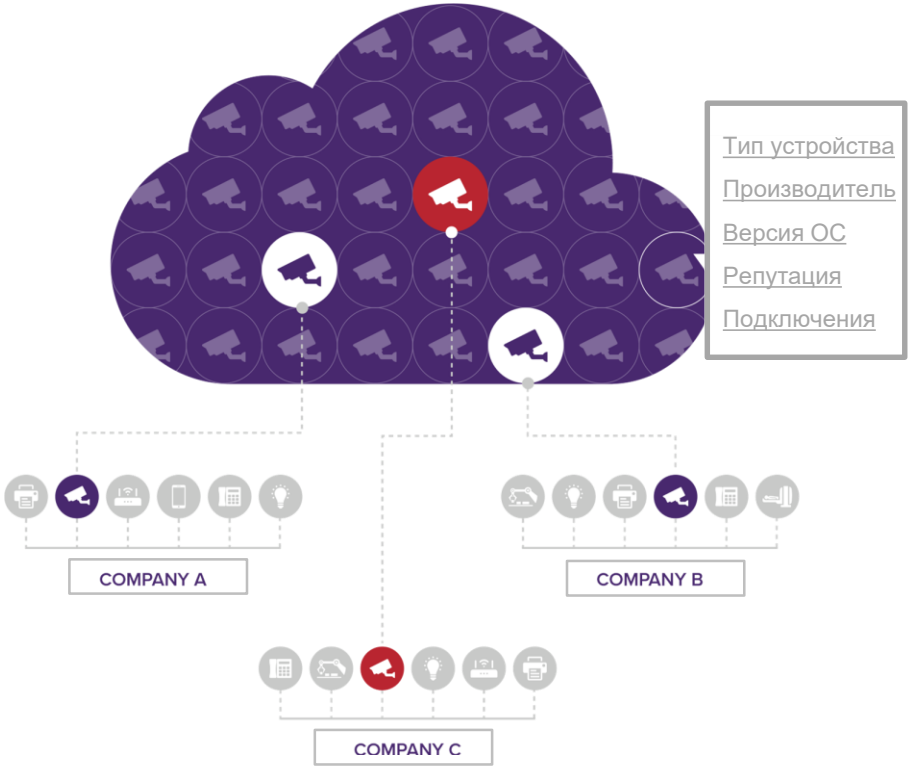
Атрибуты устройства

- Физический
- Сеть
- Поведенческий

Процесс классификации

- Отслеживание 280 млн устройств
- Сравните с порогами класса для результата ID
- Расширенные возможности аналитики угроз для оценки рисков устройств
- Непрерывный мониторинг для обнаружения поведенческих аномалий

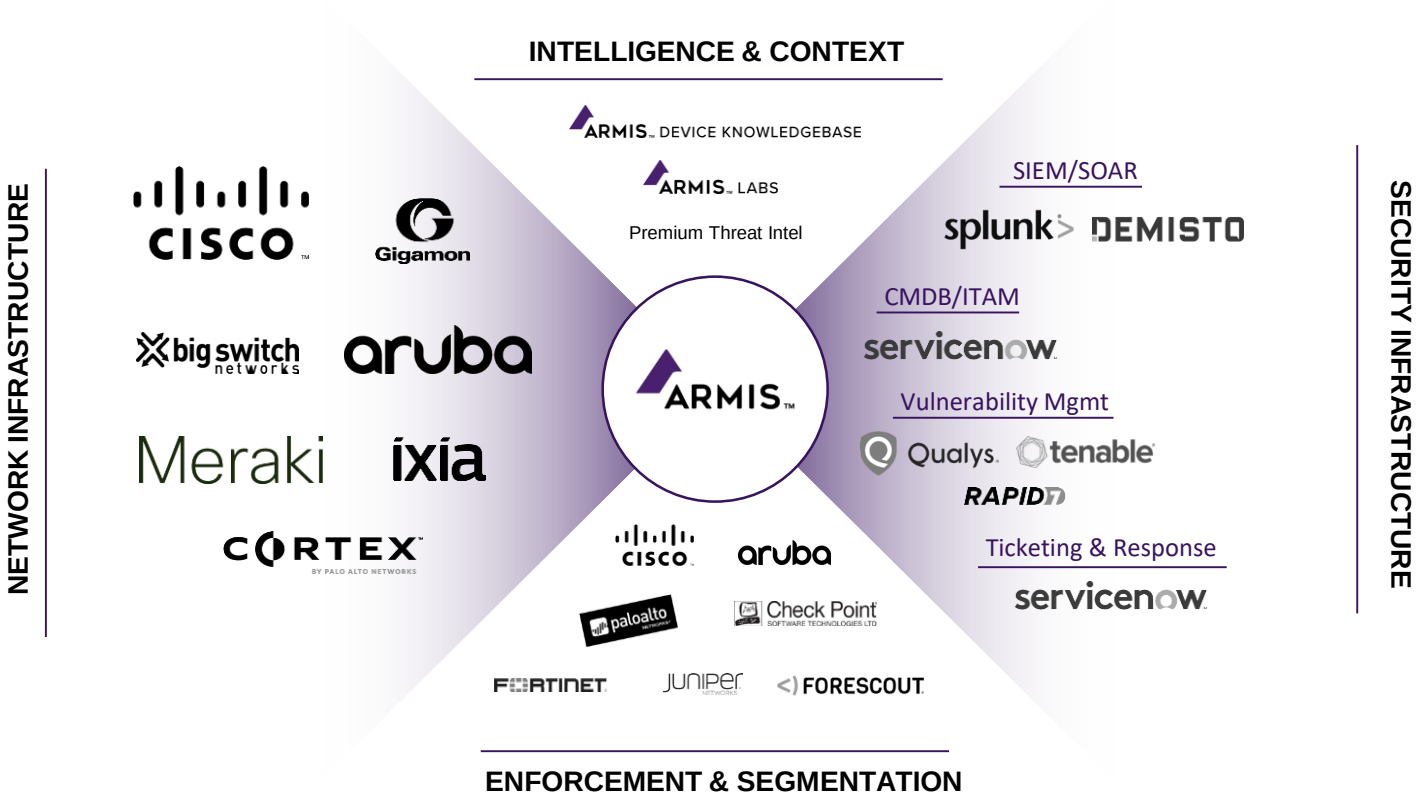
База знаний Armis



Контекст имеет значение

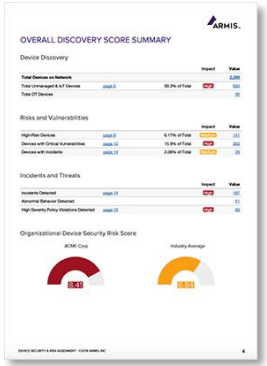
- 300 млн.+ отслеживаемых устройств (и их количество растет)
- 15 млн. профилей устройств
- Крупнейшая облачная, краудсорсинговая база знаний об устройствах
- Сравнивает поведение устройства в реальном времени с «заведомо исправными» базовыми показателями.
- Выявляет нарушения политик, неправильную конфигурацию или ненормальное поведение
- Быстрое развертывание и ввод в эксплуатацию

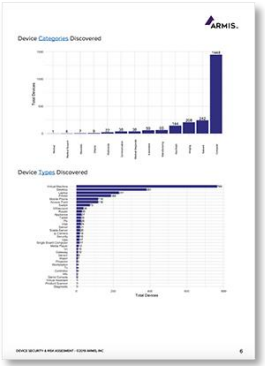
Простая и легкая интеграция

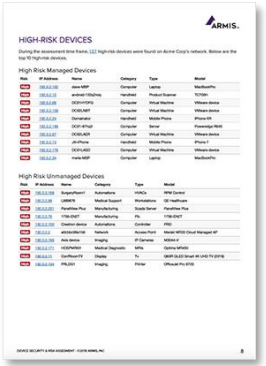


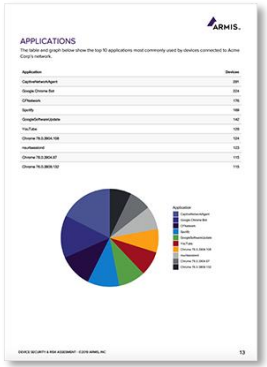
Позвольте нам это доказать

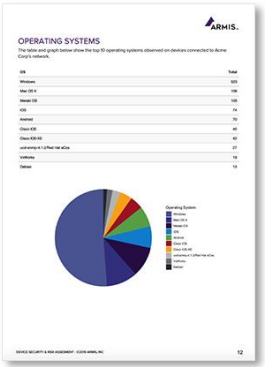
- Инвентаризация активов и оценка рисков
- Настройка от минут до часов
- Определение устройств, рисков, воздействия
- Предоставление полного отчета

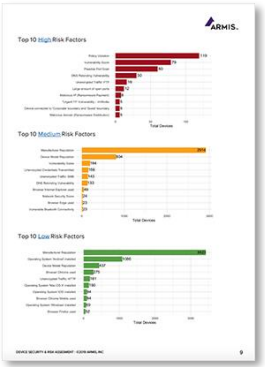


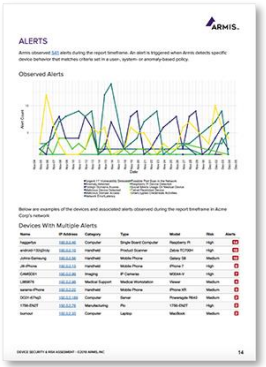












THANK YOU

SOFTPROM

ARMIS