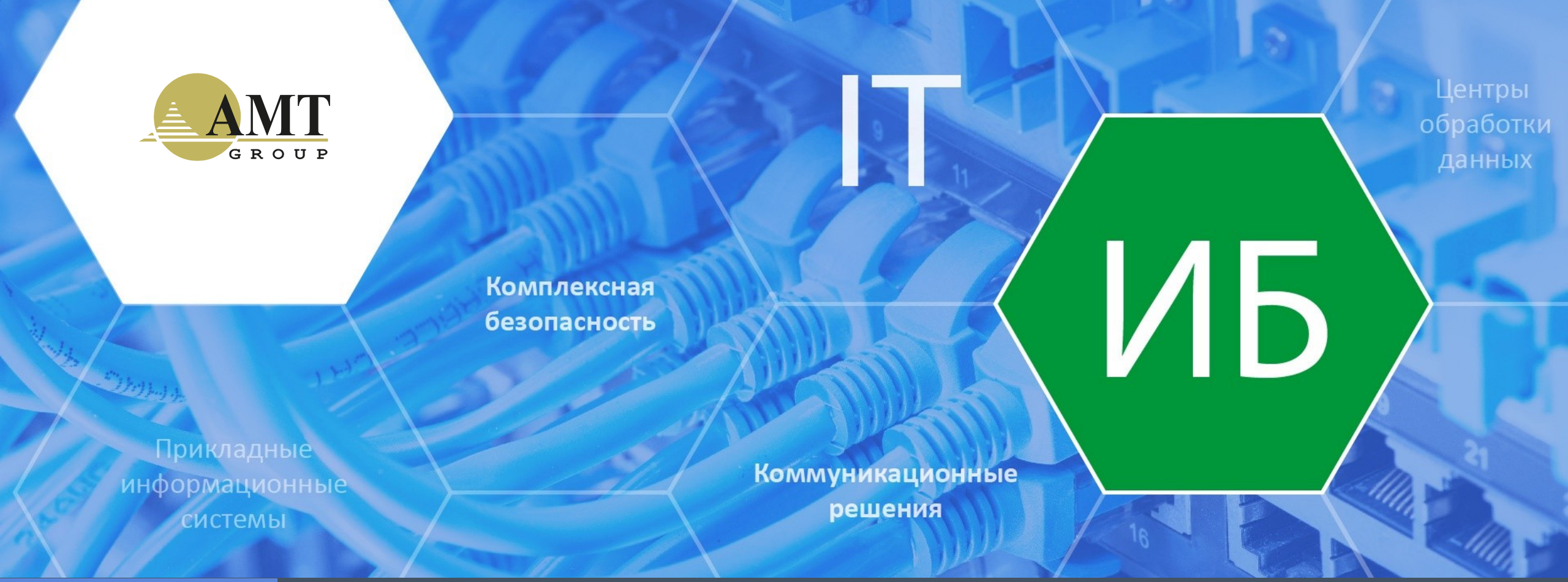


АМТ-ГРУП

Управление сетью МСЭ: быстрее, безопаснее, эффективнее

Кондратьев Илья, зам. директора ДИБ АМТ-ГРУП

Автоматизация процессов ИБ

Проблемы и предпосылки

- Количество и разнообразие средств защиты растет. Угроз тоже
- «Нехватка рук и других частей тела…»
- Многие процессы опираются на бумажные и ручные процедуры
- Ошибки и очепятки при ручном конфигурировании - усилия и время
- IT ушло далеко вперед по пути автоматизации, «облаков» и SDN
- ФЗ 187 - появление средств защиты там, где их раньше не было и вовлечение в процессы ИТ и ИБ новых, «непрофильных» сотрудников

AMT GROUP

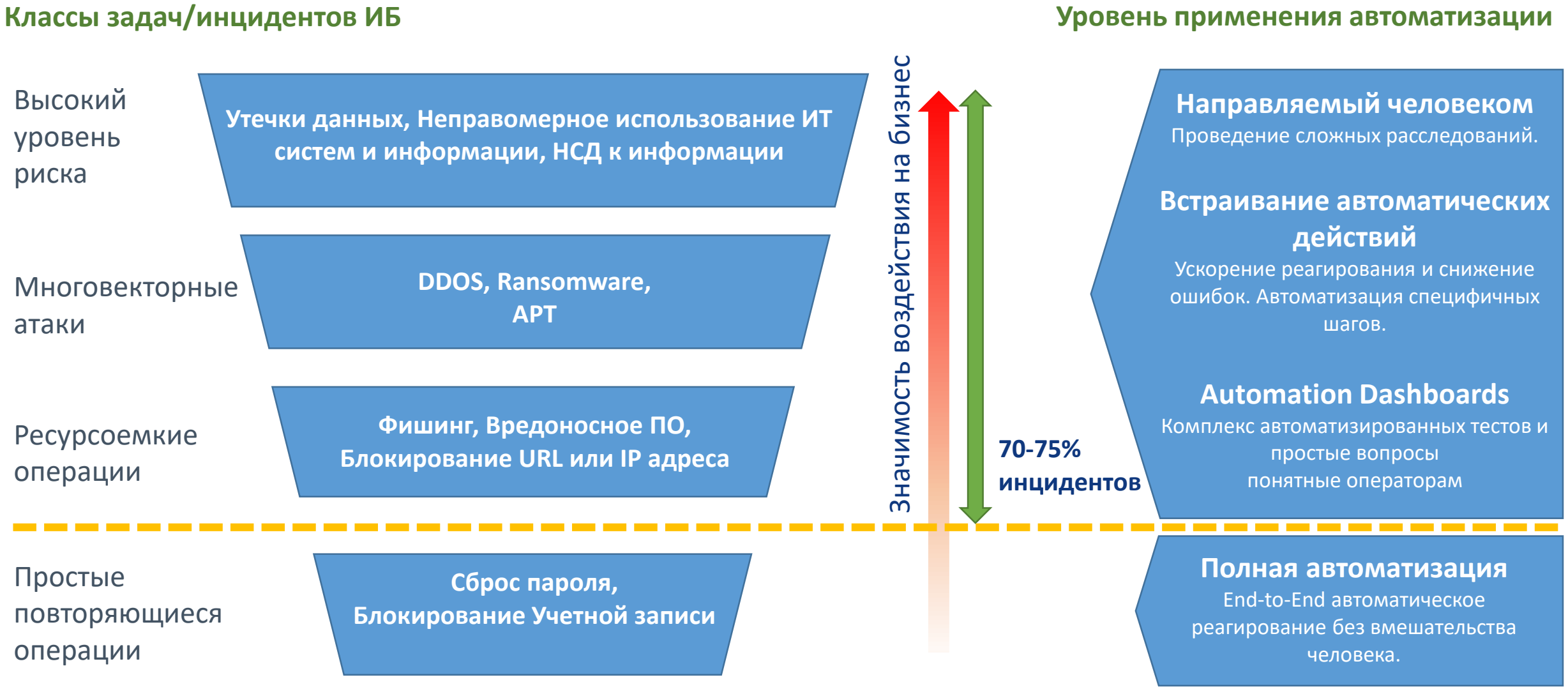
Проблемы и предпосылки

- Чтобы выжить и развиваться организациям нужно повысить скорость в процессах обеспечения ИБ
  - управление правами и доступом
  - управление изменениями
  - инвентаризация и аудит
  - реагирование и расследование
- Дефицит квалифицированных кадров - знание в головах профессионалов(“tribal knowledge”).
- Проблемы сохранения знаний - «единая точка экспертного знания», «смена команды»
- Увеличение количества специалистов может снизить скорость
- Оперативность реагирования играет ключевую роль

AMT GROUP

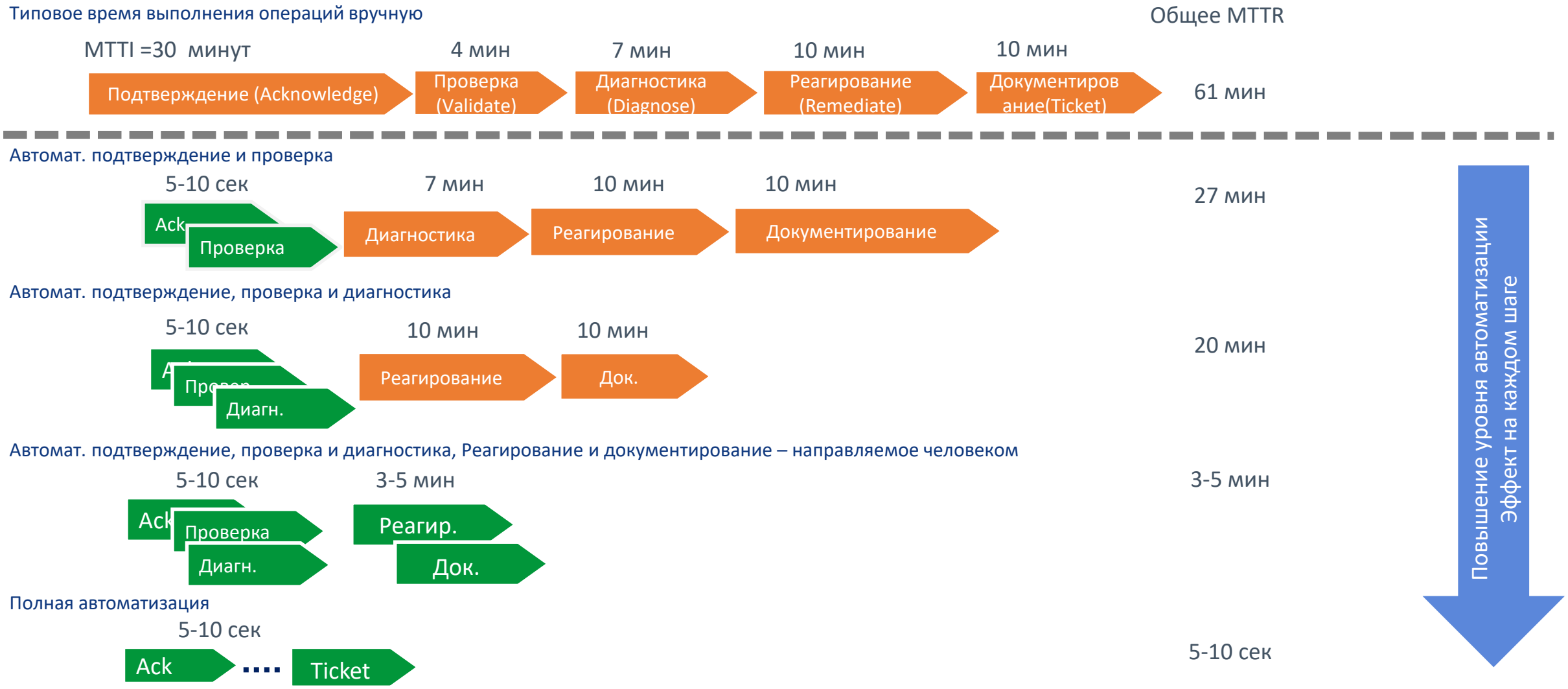
Автоматизация прямо влияет на эффективность

Позволяют справиться со сложными кейсами и быстро адаптироваться



Внедрение поэтапно, эффект сразу

Поэтапное внедрение: автоматизировать где возможно, ускорять операции там где пока нельзя автоматизировать



Автоматизация – это подход, а не продукт

Цели автоматизации

- Скорость изменений и реакции
- Повышение эффективности персонала
- Адекватный ответ современным угрозам

Автоматизируют процессы

- Управление изменениями
- Инвентаризация и аудит
- Диагностика, отчетность и реагирование

Принципы автоматизации

- От простого к сложному
- Измеримость
- Вовлечение ИТ и ИБ специалистов

Что уже автоматизировано

- Сбор и консолидация событий
- Корреляция
- Мониторинг и аналитика

AMT GROUP

Что для этого нужно?

Консоль АИБ, оператора

Playbooks, Scripts, KB

- Процессы – выявить, описать, выстроить/упорядочить.
- Сценарии и «Ролевые игры», База знаний, Case management
- Современные СЗИ и API – хорошо, с Legacy тоже можно работать.
- Ядро – Платформа реализующая автоматизируемые функции

AMT GROUP

Кто это будет делать?

Подход к внедрению – своими силами или позвать на помощь интегратора?

- Выявление, документирование и оптимизация процессов
- Моделирование систем в требуемой среде, разработка НМД
- Облегчение продвижения подхода внутри организации – независимое мнение
- Качественная интеграция разнообразных СЗИ требует экспертных знаний
- Опыт, типовые шаблоны, библиотеки кода – кардинально влияют на сроки
- Инфраструктура для отладки кода и «песочница»
- Поддержка, модификация и адаптация к изменяющимся процессам и процедурам

AMT GROUP

Автоматизация управления МСЭ

Проблемы управления инфраструктурой МСЭ

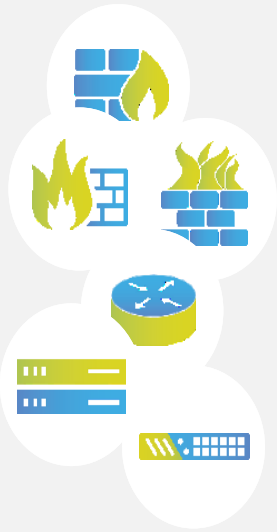
- Маршрутизаторов и МСЭ просто много. Часто от разных производителей
- При объединении сетей требуется анализ и изучение «новой» сети
- Миграция МСЭ других производителей на МСЭ корпоративного стандарта
- «Владельцы» приложений и администраторы говорят на разных языках
- «Безопасное» удаление правил часто непосильная задача
- Ошибки и очепятки при ручном конфигурировании - усилия и время
- Заявки на открытие доступа выполняются долго (до нескольких недель)
- Compliance – PCI DSS, GDPR и др.
- Многие процессы ИБ опираются на бумажные и ручные процедуры

Управление ИТ/ИБ

Ответственные за бизнес приложения

ИТ менеджер
Администраторы сети

Ответственные за ИБ



Бизнес Приложения

Инфраструктура сетевой ИБ

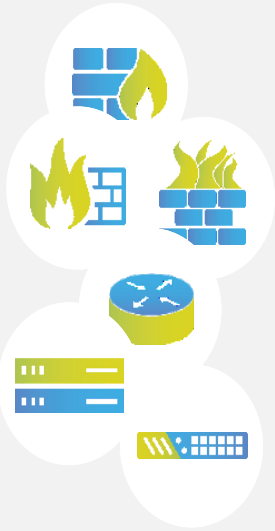
Управление ИТ/ИБ – Algosec AppViz | Tufin Secure App

Ответственные за бизнес приложения

ИТ менеджер
Администраторы сети

Ответственные за ИБ

Платформа управления МСЭ



Бизнес Приложения

Инфраструктура сетевой ИБ

Управление ИТ/ИБ – Algosec AppViz | Tufin Secure App

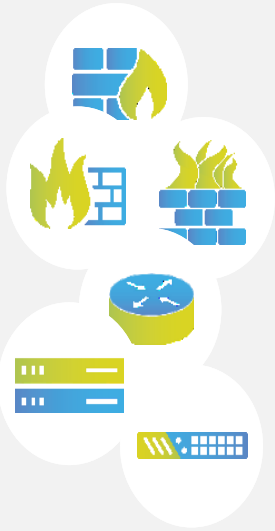
Ответственные за бизнес приложения

ИТ менеджер
Администраторы сети

Ответственные за ИБ

Платформа управления МСЭ

AppViz / SecureApp



Управление политикой ИБ на уровне приложений

- Повышение скорости настроек ИБ для критических и важных бизнес приложений
- Прозрачность требований доступа приложений для повышения управляемости
- «Перевод» требований к доступу в используемые политики ИБ на МСЭ

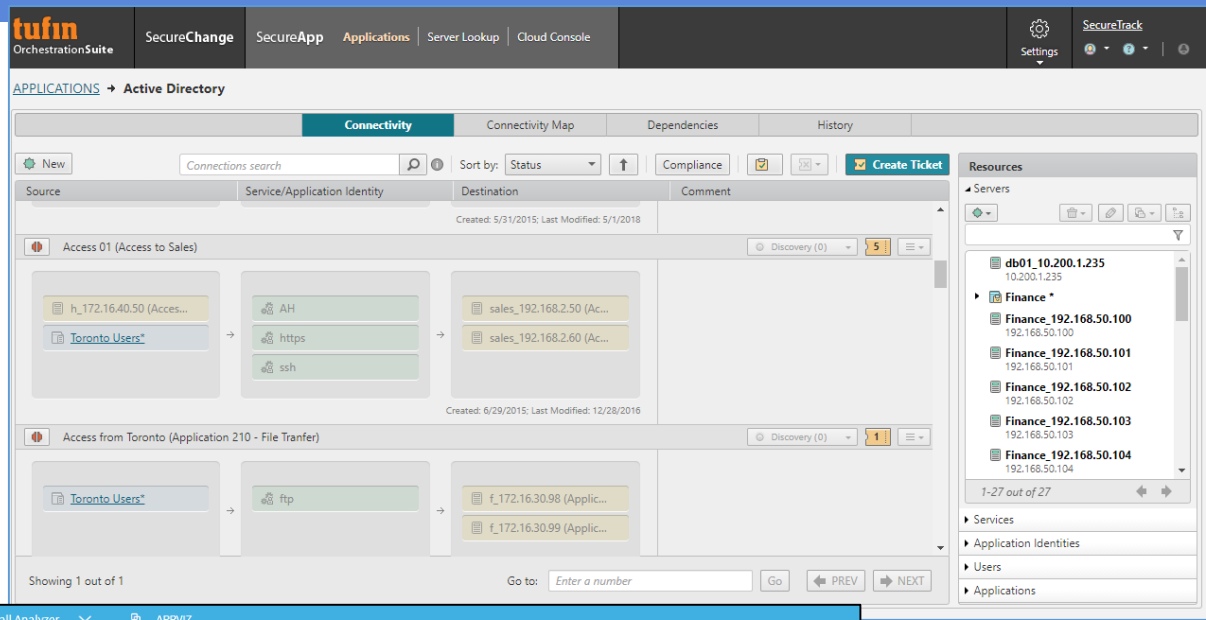
Бизнес Приложения

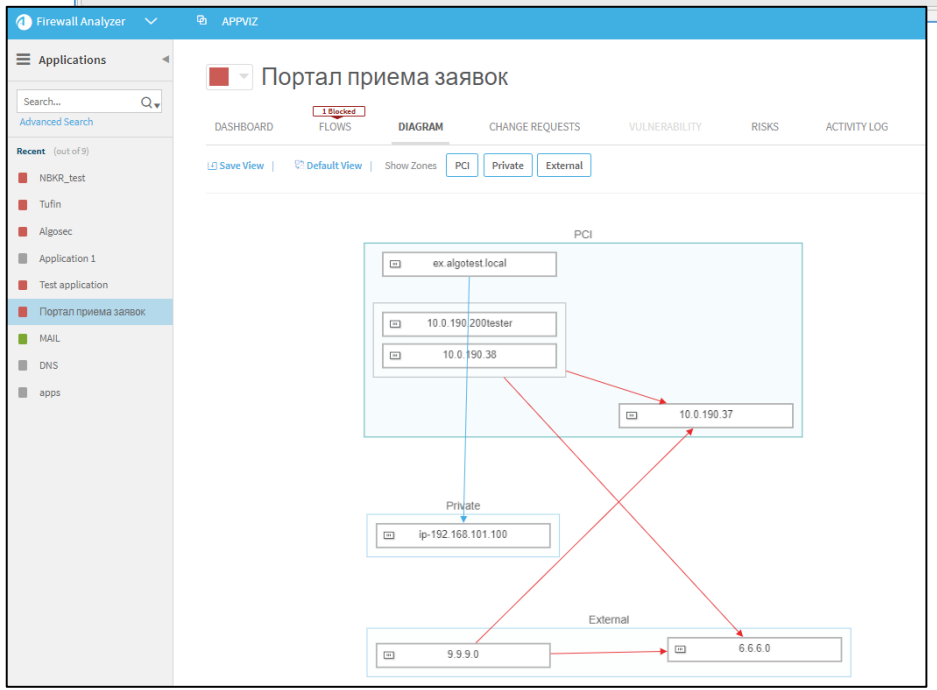
Инфраструктура сетевой ИБ

Управление ИТ/ИБ – AlgoSec AppViz | Tufin SecureApp

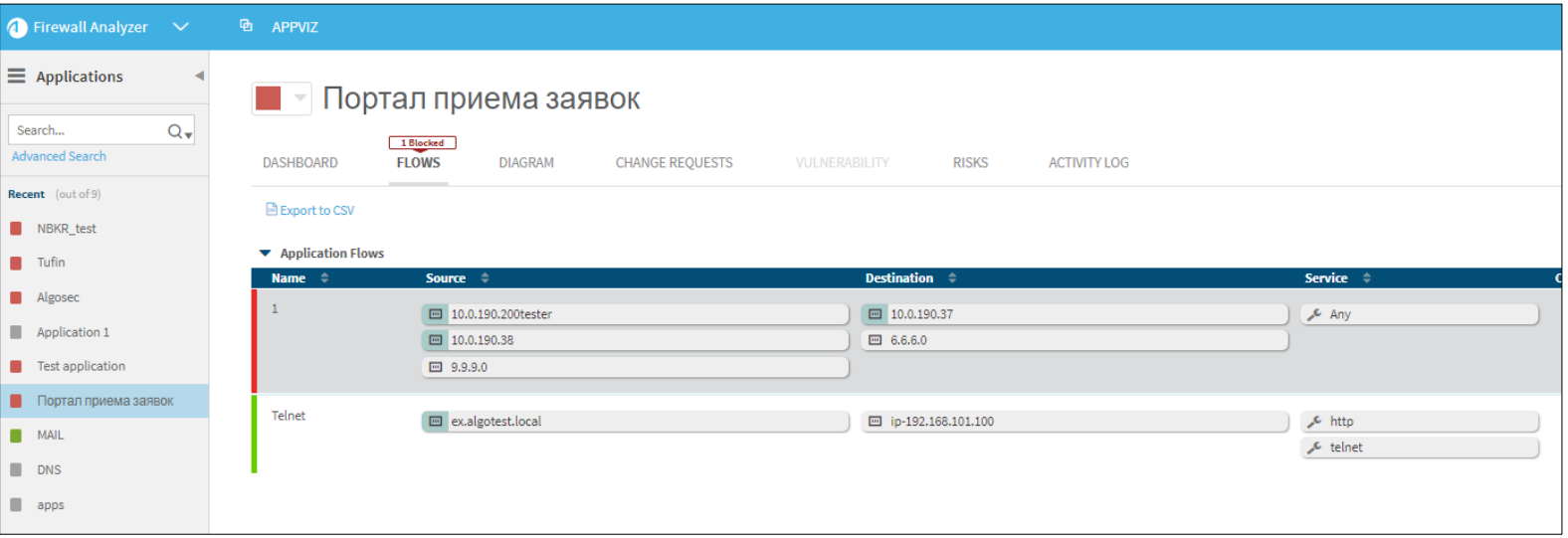
Управление взаимосвязью приложений и услуг с правилами фильтрации трафика в МСЭ и роутерах

- Центральная, обновляемая база данных требований бизнес приложений и услуг к сетевым услугам и соединениям, с возможностью углубиться on-line в данные до уровня правила в МСЭ
- Автоматический перевод заявок на подключение услуг и бизнес приложений в технические детали для изменений в МСЭ
- Автоматический расчет влияния изменений топологии и конфигурации СПД на приложение/услугу (к примеру миграция сервера).
- Безопасное удаление правил в МСЭ, в которых нет больше потребности (к примеру в результате вывода приложения из эксплуатации).
- Интеллектуальное соотношение (mapping) правил и политик МСЭ с бизнес услугами и приложениями.
- Полный аудит соединений бизнес-услуг и приложений (connectivity audit trail)

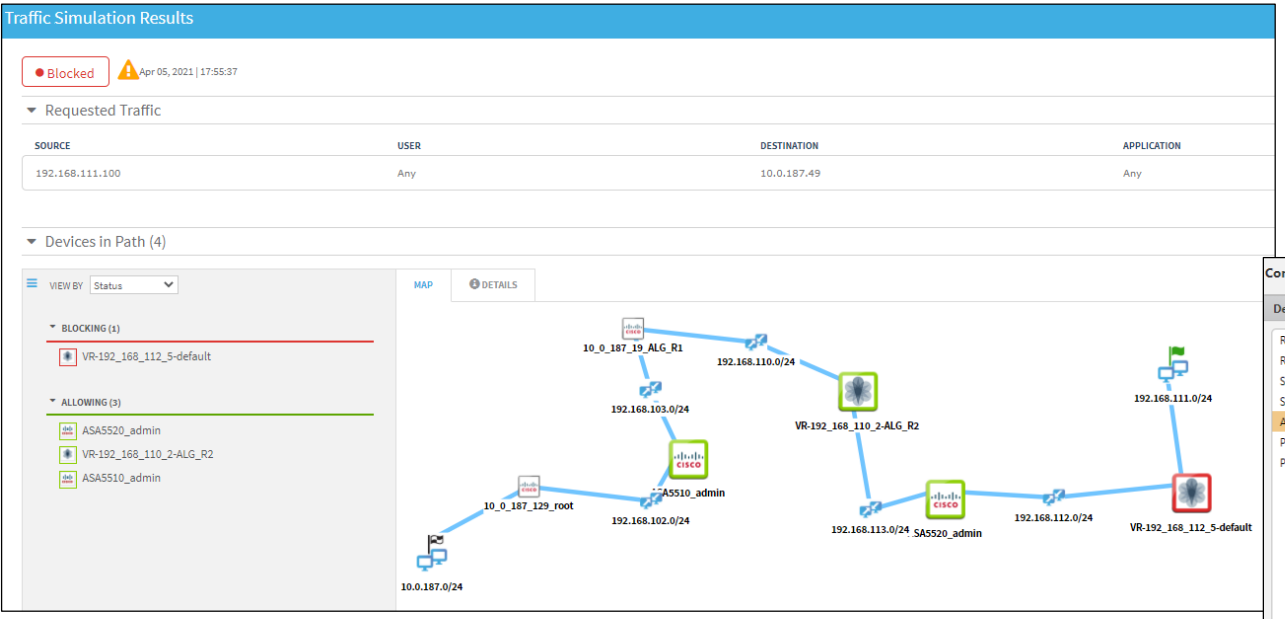




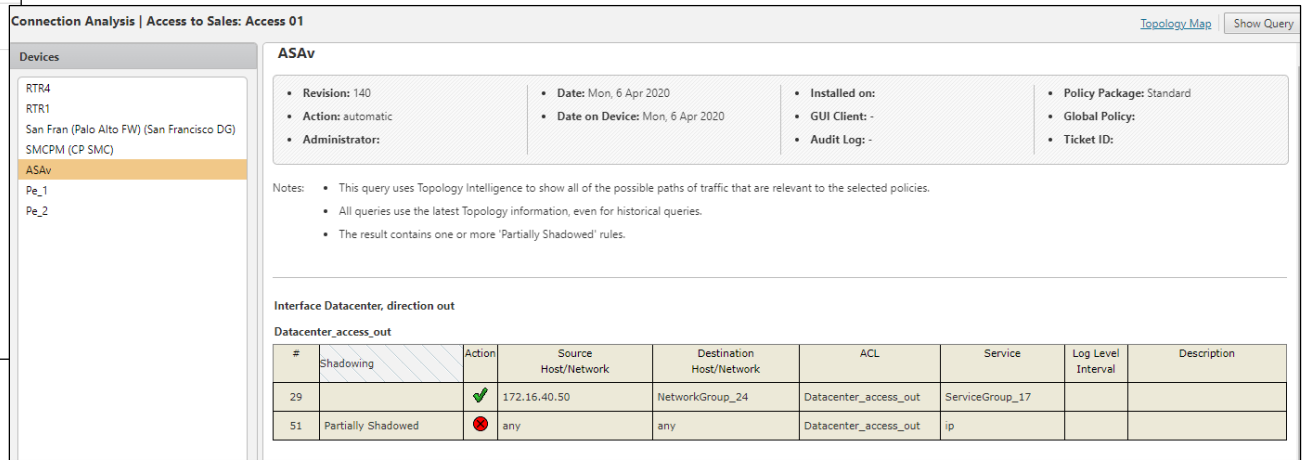
Управление ИТ/ИБ – Algosec AppViz | Tufin SecureApp



- Анализ рисков до модификации правил
- Интеграция с тикетинговой системой
- Учет и автоматизация зависимостей
- Миграция серверов упрощается



- Автоматическая проверка достижимости
- Учет уязвимостей на серверах
- Описание трафика приложения/сервиса отдельно от сетевой топологии



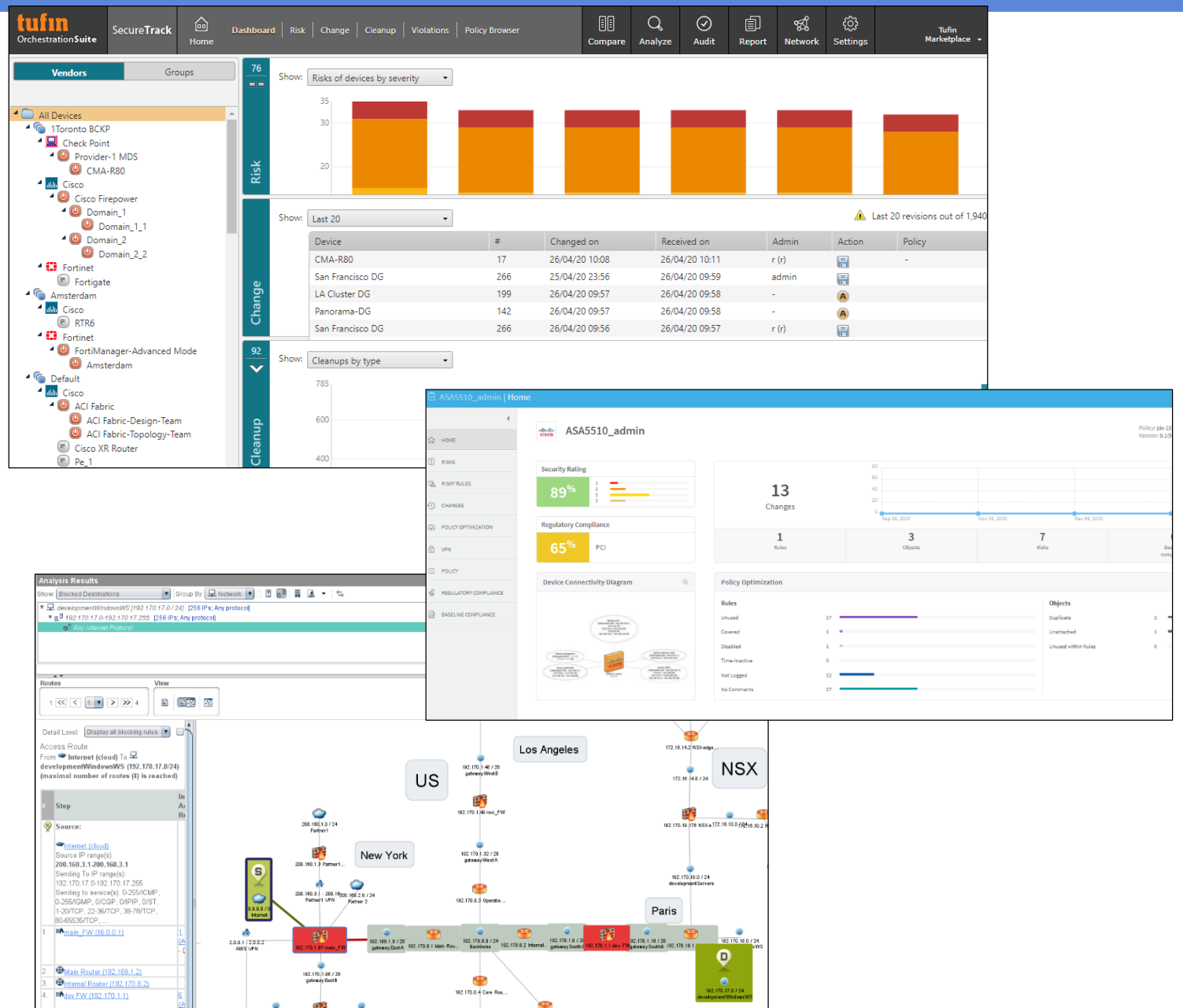
Управление ИБ – Algosec | Tufin | Skybox

Управление ИБ – Algosec | Tufin | Skybox

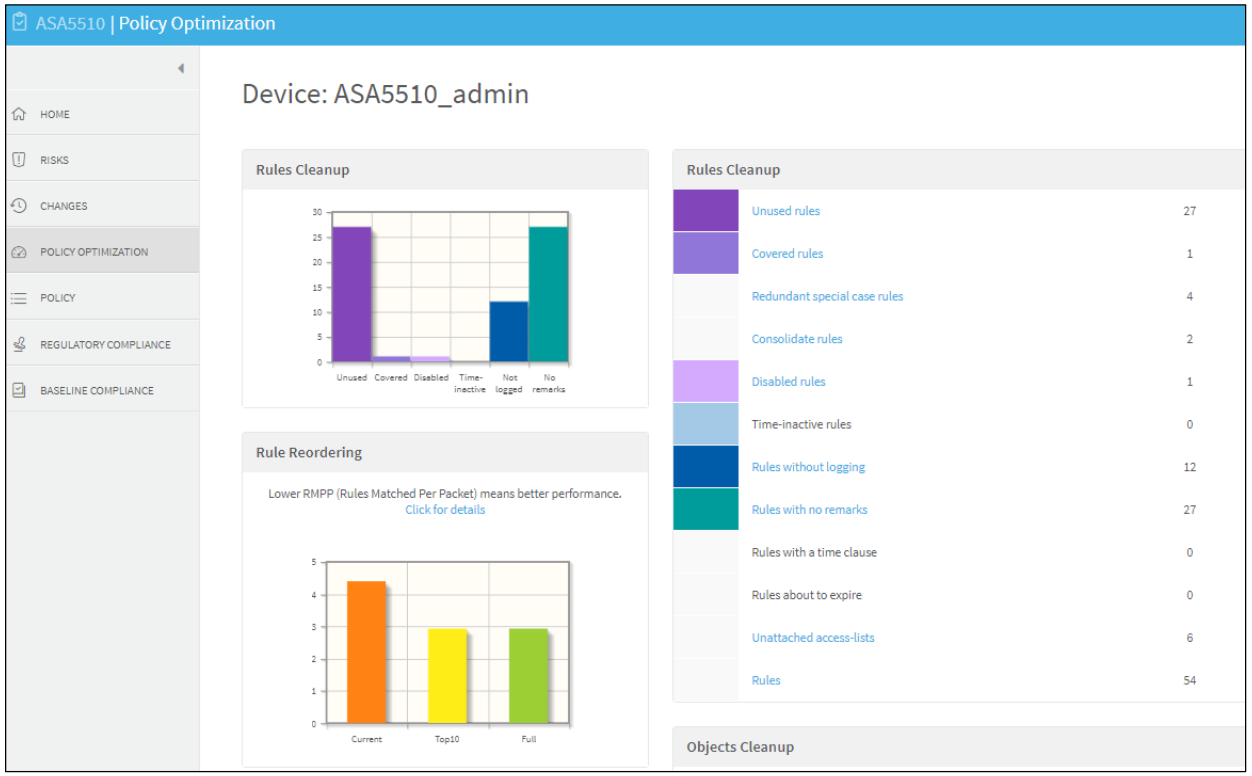
Управление ИБ - AlgoSec | Tufin | Skybox

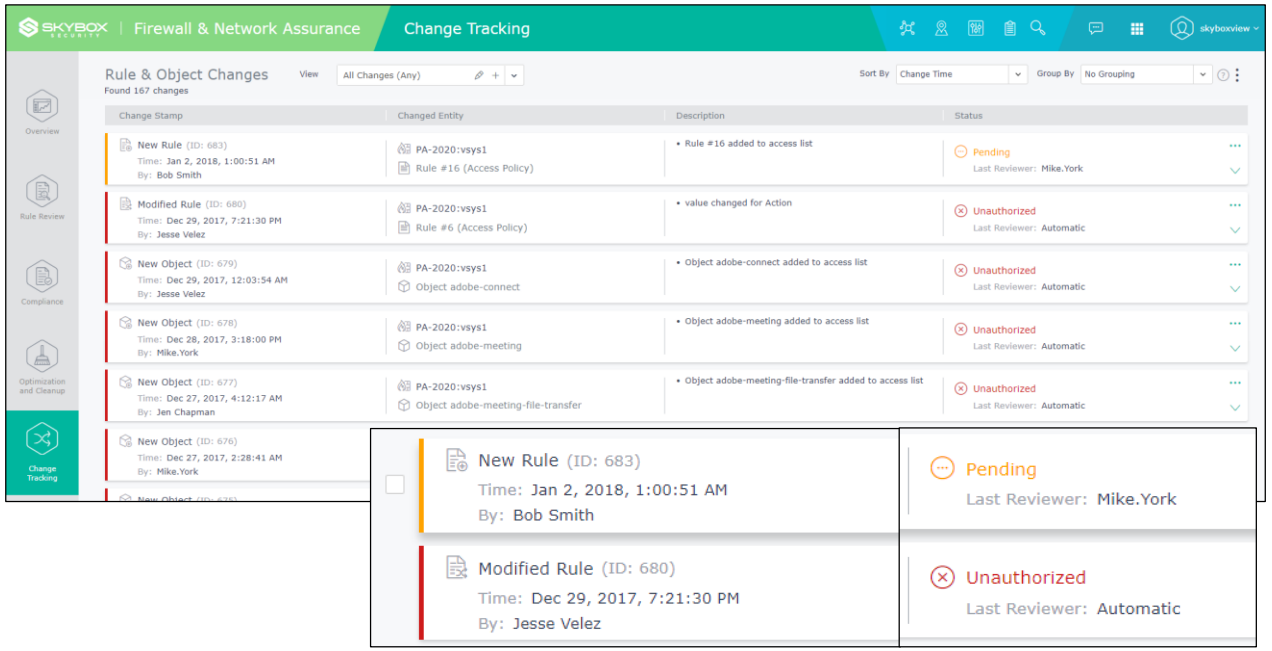
Интеллектуальный анализ политики и правил ИБ

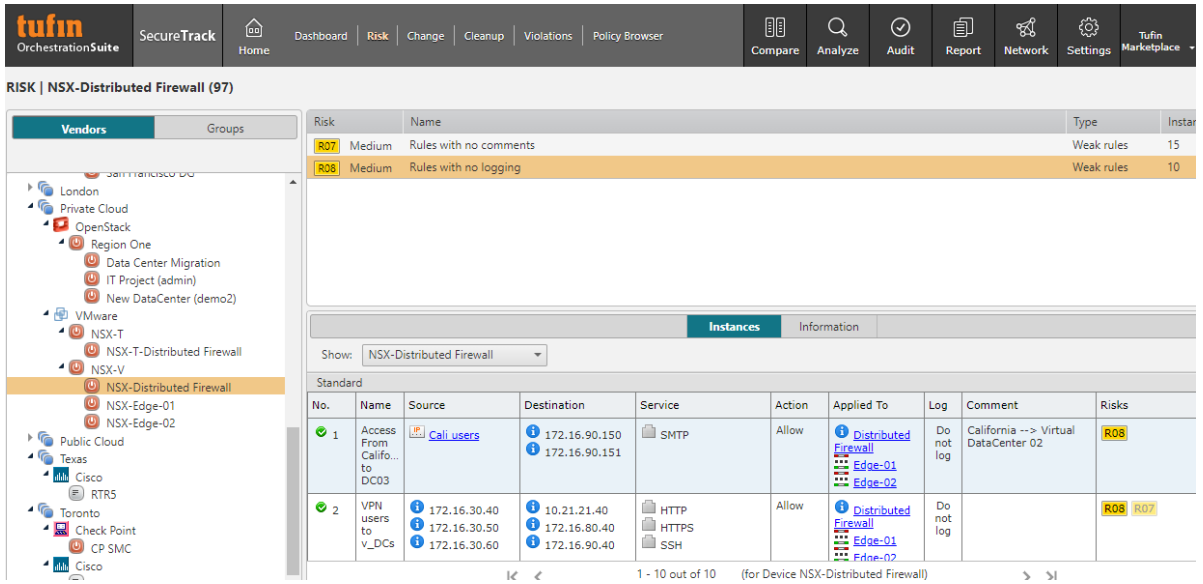
- Определение и анализ топологии сети и зон ИБ (сегментация)
- Контроль изменений политик и правил МСЭ
- Анализ достижимости (Simulation)
- Анализ рисков
- Проверка соответствия требованиям стандартов
- Автоматический сбор и анализ конфигураций («зоопарк» приветствуется)



Управление ИБ – анализ рисков, аудит, оптимизация

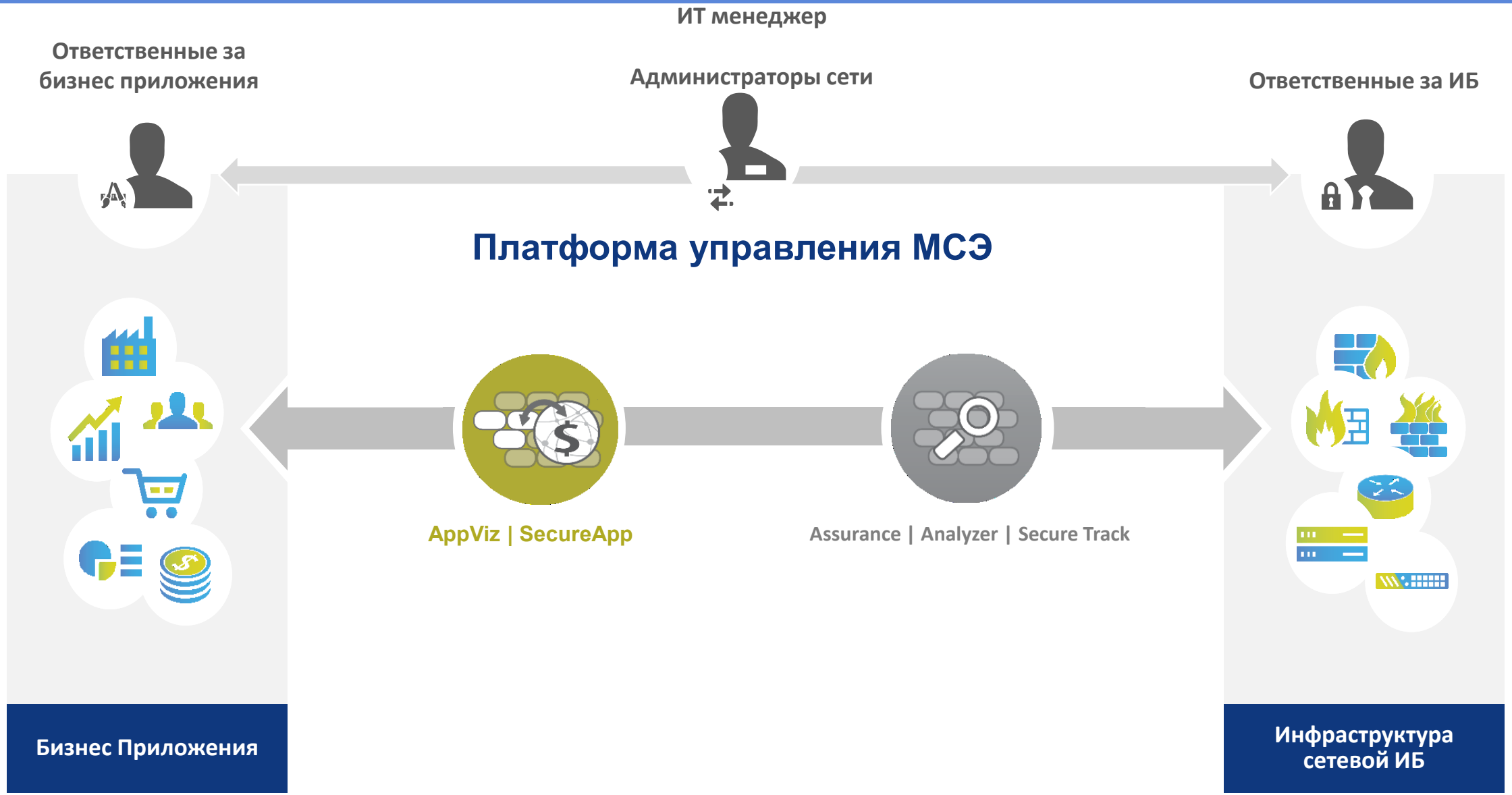






- Выявление несанкционированных изменений
- «Чистка» и оптимизация политик и правил МСЭ
- Анализ рисков с учетом уязвимостей на серверах
- Compliance
- Контроль базовой конфигурации МСЭ и устройств ИБ
- Документирование правил – единая база

Управление изменениями - FireFlow | SecureChange | Change Manger

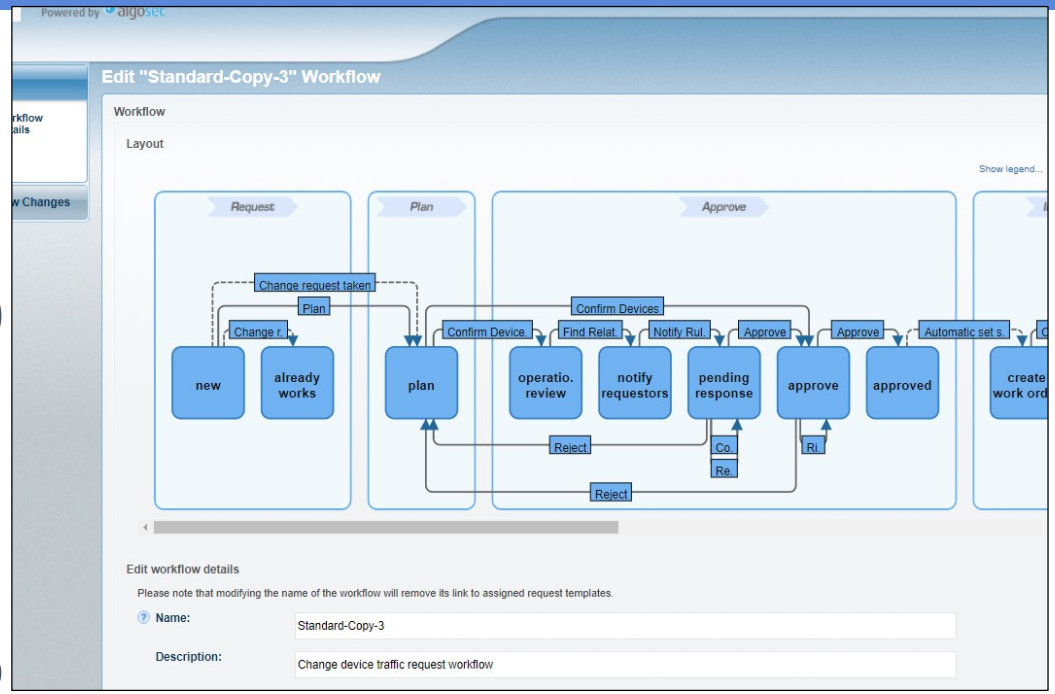


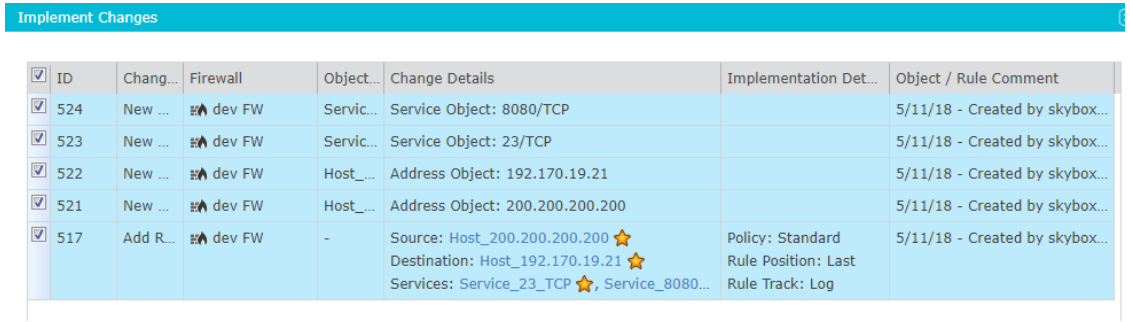
Управление изменениями - FireFlow | SecureChange | Change Manger

Управление изменениями - FireFlow | SecureChange | Change Manger

Интеллектуальная автоматизация управления изменениями в МСЭ и устройствах ИБ

- Кастомизируемые автоматические процессы работ (workflows)
- Интеллектуальная симуляция и анализ влияния исполнения заявки на работу сети и элементов ИБ
- Проактивная проверка влияния изменений на риски и соответствие стандартам
- Автоматическая установка изменений политик и правил в МСЭ
- Полный аудит изменений в устройствах ИБ
- Контроль качества выполнения заявок/заказов (SLA)
- Интеграция с существующими системами (BMC, HP, CA)





Результаты

- 40 - 50% существующих правил на МСЭ можно удалить (в среднем)
- 20 % заявок не требуют внесения изменений
- Продление жизни существующим МСЭ – до 20%.
- До 80% снижения в трудоемкости подготовки и проведения аудита МСЭ
- Настройки ИБ производятся в 2-4 быстрее
- Проверка наличия доступа в большой сети занимает секунды
- Схема L3 топологии сети поддерживается автоматически - всегда актуальна
- Правила фильтрации соответствуют запрошенным доступам
- Повышение устойчивости к кибератакам благодаря более правильным настройкам МСЭ

Реальный кейс

Российский холдинг: >200 МСЭ и >1000 сетевых L3-устройств

Сотни криптографических шлюзов

Правила МСЭ часто добавляются и практически не удаляются

Документация правил слабая, единая карта сети отсутствует

Заявки на изменения в правила МСЭ выполняются до 2 недель

Процесс управления изменениями в явном виде не документирован

Тысячи приложений и ИТ-сервисов

Аудит правил МСЭ занимает месяцы и поэтому теряет смысл

Реальный кейс. Продолжение

Процесс управления изменениями на МСЭ документирован и адаптирован с учетом средств автоматизации

>40% правил МСЭ могут быть перекрываются и могут быть удалены

Около 20 % заявок на сетевой доступ не требуют выполнения

Время внесения изменений сокращается на 50%. Проверка изменений автоматизирована

SOC получил инструмент для оценки достижимости ИТ-активов с зараженных хостов

Владельцы ИТ-систем получили инструмент для моделирования изменений и упрощения миграции между площадками

Отечественные криптошлюзы подключены к системе для полноты сетевой карты. Выявлен ряд ошибок маршрутизации

Аудит правил МСЭ проводится автоматически

СПАСИБО ЗА ВНИМАНИЕ!