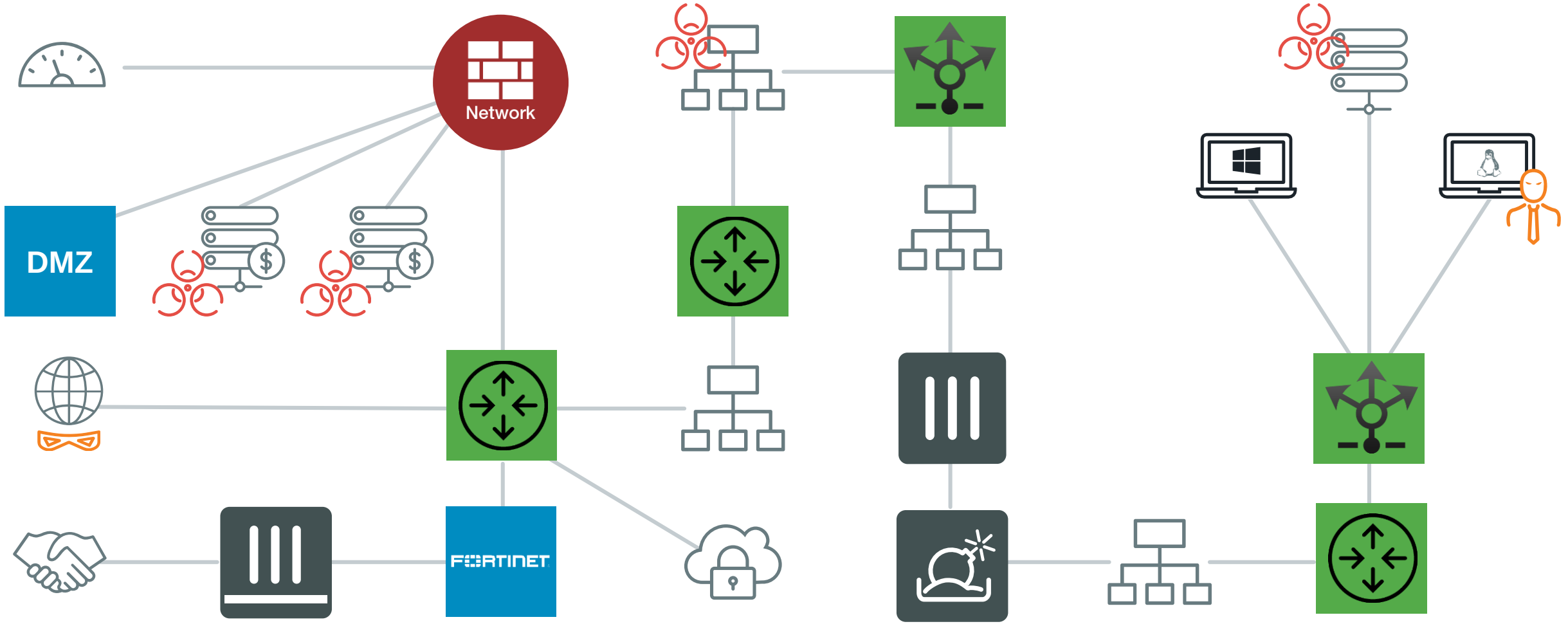
Адаптивная защита Fortinet Security Fabric на основе индикаторов угроз от Skybox Security

Юрий Черкас

20 сентября 2018

SECURITYDAY

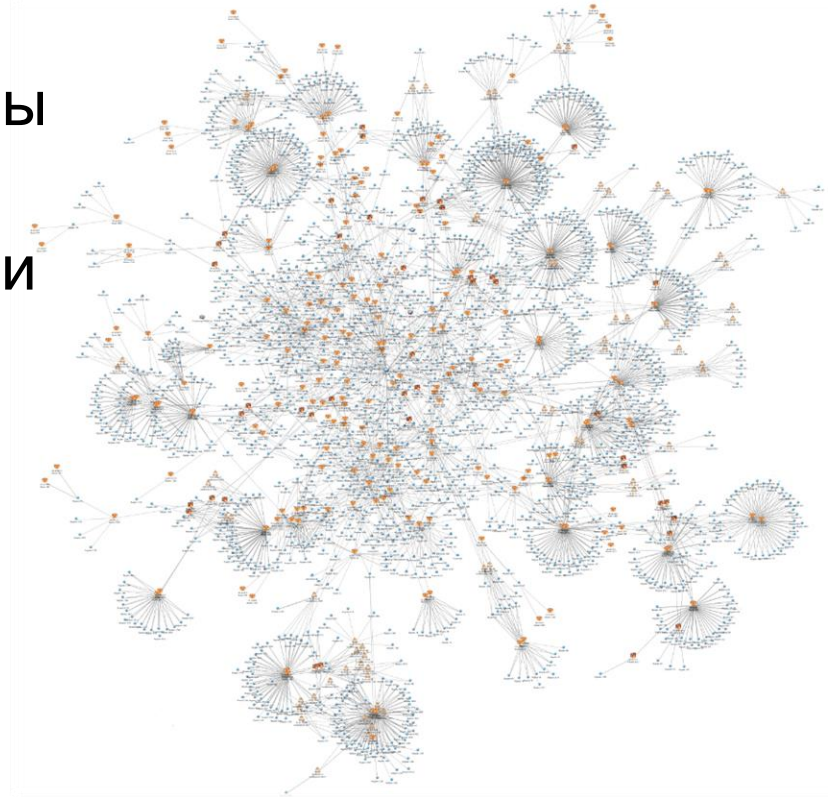
Моделирование вектора атаки



Средства защиты | Топология сети | ИТ-активы | Уязвимости | Источники угроз

Сложности

- Наша цель – защитить ИТ-активы, но:
  - ИТ-инфраструктура динамически меняется и мы не знаем как выглядит наша сеть прямо сейчас
  - Зачастую мы настраиваем защитные механизмы сети без учета уязвимостей на хостах
  - Мы не знаем о новых уязвимостях в период до и между сканированиями
  - Мы учитываем только критичные уязвимости
  - Мы не всегда знаем какие уязвимости достижимы в нашей сети



Подход Skybox Security

Расчет индикаторов угроз и прогнозирование наиболее вероятных векторов атак

Идея Skybox Security

Построение модели сети

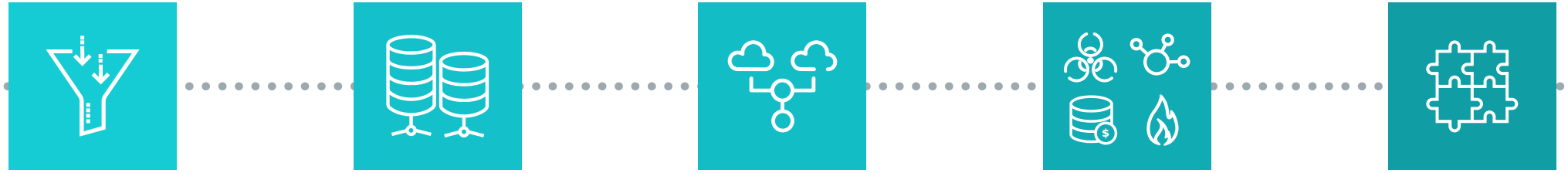
Возможные сценарии

Построение сетевой модели

- Network Assurance – видимость сети

Интерактивная карта сети	Автоматическая проверка соответствия стандартам конфигурирования	Автоматическая проверка соответствия политикам сегментирования

Как Это Работает



1. Сбор и нормализация
2. Моделирование
3. Детальный анализ

Дружба с Fortinet

- Технологическое сотрудничество с 2010 года
- Skybox обязуется поддерживать новые версии Fortinet
- Взаимодействие на уровне разработчиков

FORTINET
Fabric-Ready

Skybox Security and **Fortinet Integration**

Supported Products and Features

FortiGate: Support for versions FGT60B-3.8 and greater

FortiGate Supported Features:

Online:	Fully supported
SSH/Telnet:	Fully supported
SOAP:	Fully supported
Import:	Fully supported
Directory:	Fully supported
Basic:	Fully supported
OS info:	Fully supported
Interfaces:	Fully supported
Routing:	Fully supported
Dynamic routing:	Fully supported
Access:	Fully supported
NAT:	Fully supported
LB:	Fully supported
VRF:	Fully supported
PBR:	Fully supported
Layer 2:	Fully supported
VPN:	Fully supported
Users:	Fully supported
Virtual contexts:	Fully supported
IPS policy signatures:	Fully supported
Change tracking events:	Fully supported
Traffic logs:	Fully supported

FortiManager: Support for versions 5.0.6-build0310 140205 (GA) through 5.4.2

FortiManager Supported Features:

Information extraction via XML API (SOAP) and SSH

Since 2010 Skybox and Fortinet have had a well-established relationship and continue to upgrade and improve connectivity as each company's product line evolve. Fortinet and Skybox are actively involved in reciprocal Technical Alliance Programs.

FORTINET

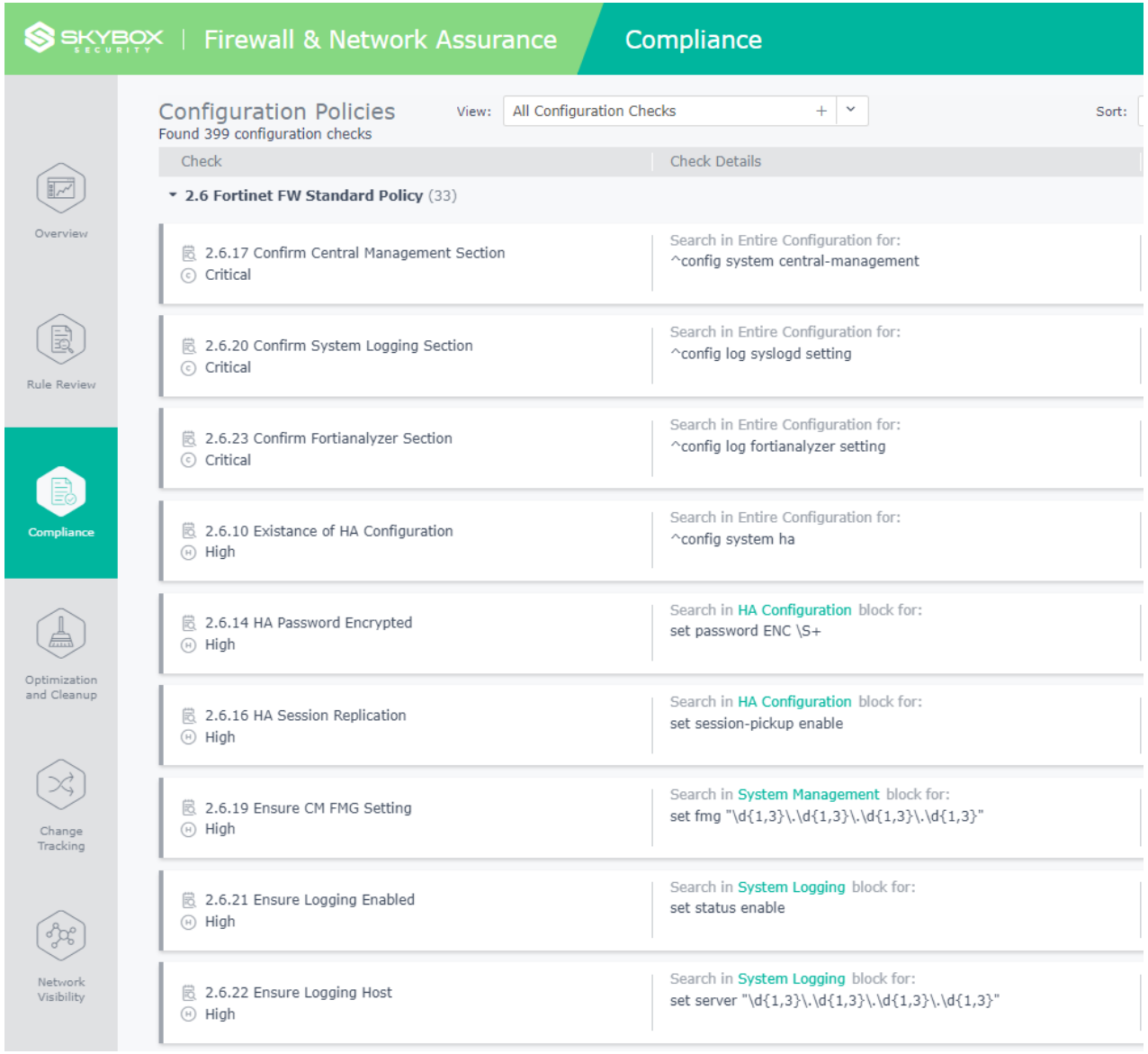
Roadmap Discussions and Information Exchange Between Fortinet and Skybox

Besides being close neighbors in the Silicon Valley, Skybox and Fortinet have had a strong technology relationship since 2010 and are active participants in each other's Technical Alliance Programs. There is continuous mutual support for product lines from both companies.

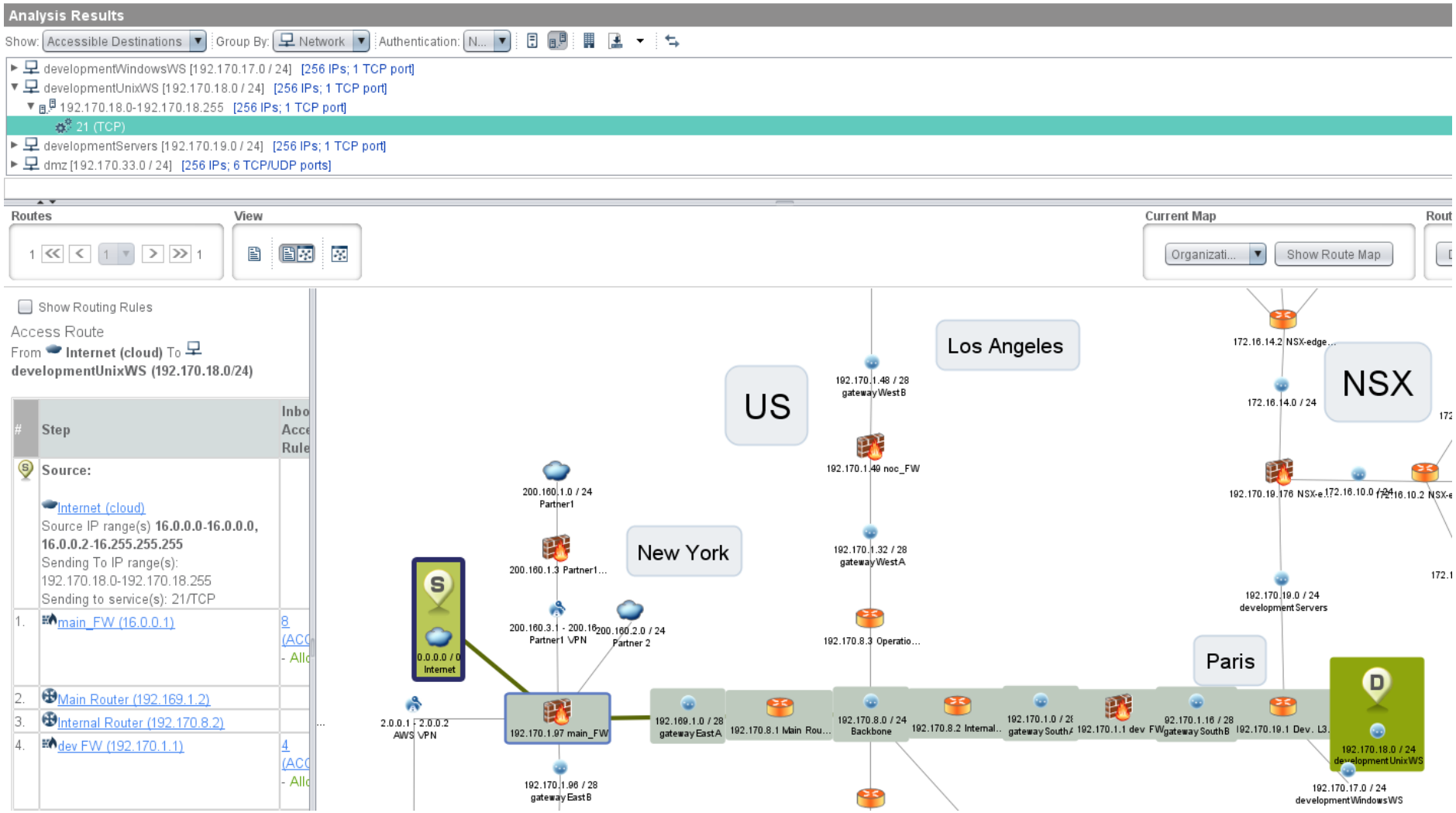
- Skybox is committed to providing support for all future versions. Fortinet is one of the top five leading firewall platforms
- Fortinet shares information via our mutual Technical Alliance relationship
- We have full access to the Fortinet Development Network (FNDN)
- We also have direct access to Fortinet development key engineering personnel, in case escalation is required
- Skybox assesses platform enhancement on an ongoing basis

Проверка конфигураций

- Загружаем конфигурации всех сетевых устройств
- Строим карту сети
- Анализируем корректность конфигураций на:
  - » Соответствие лучшим практикам
  - » Соответствие собственным политикам конфигурирования

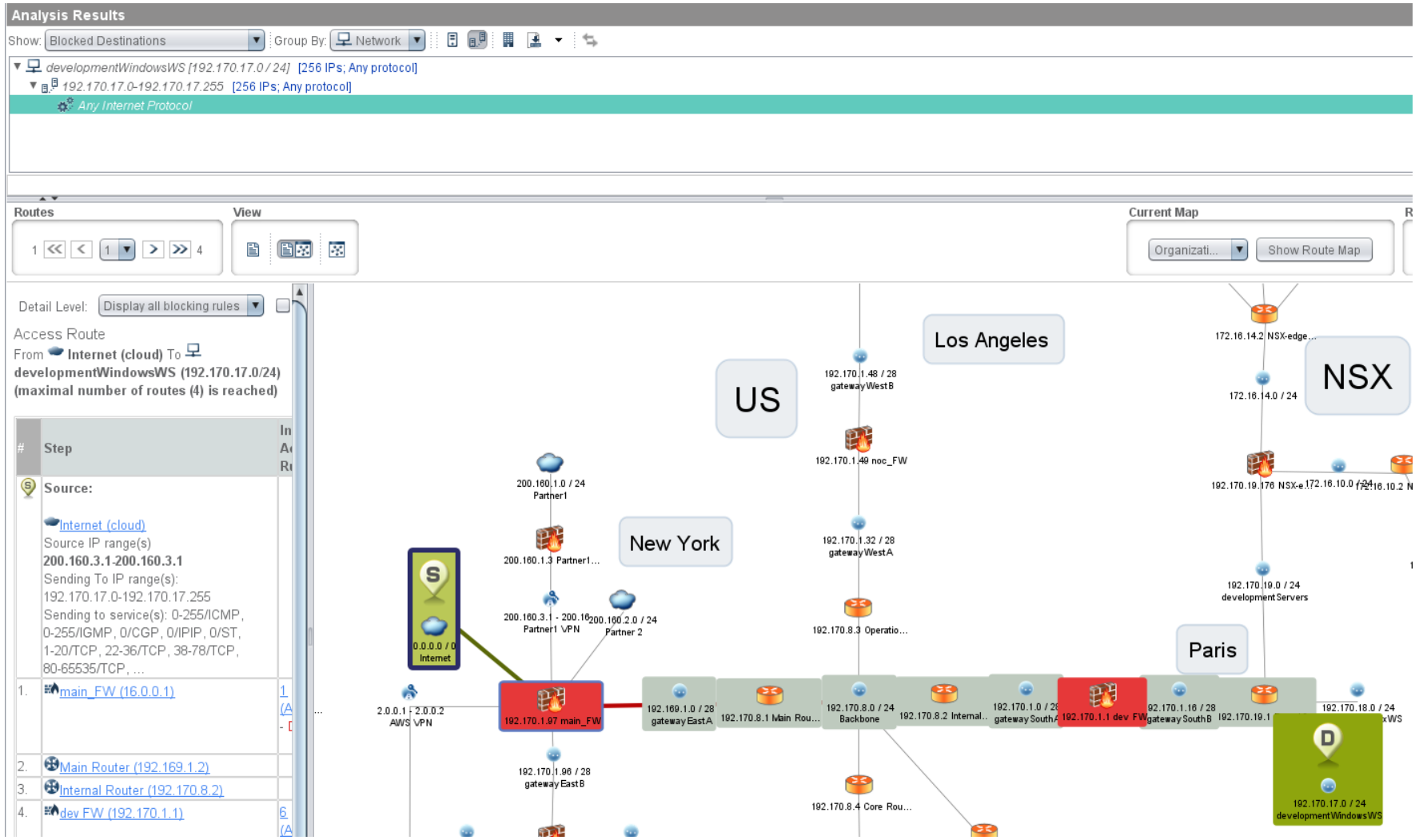


Проверка доступа на лету



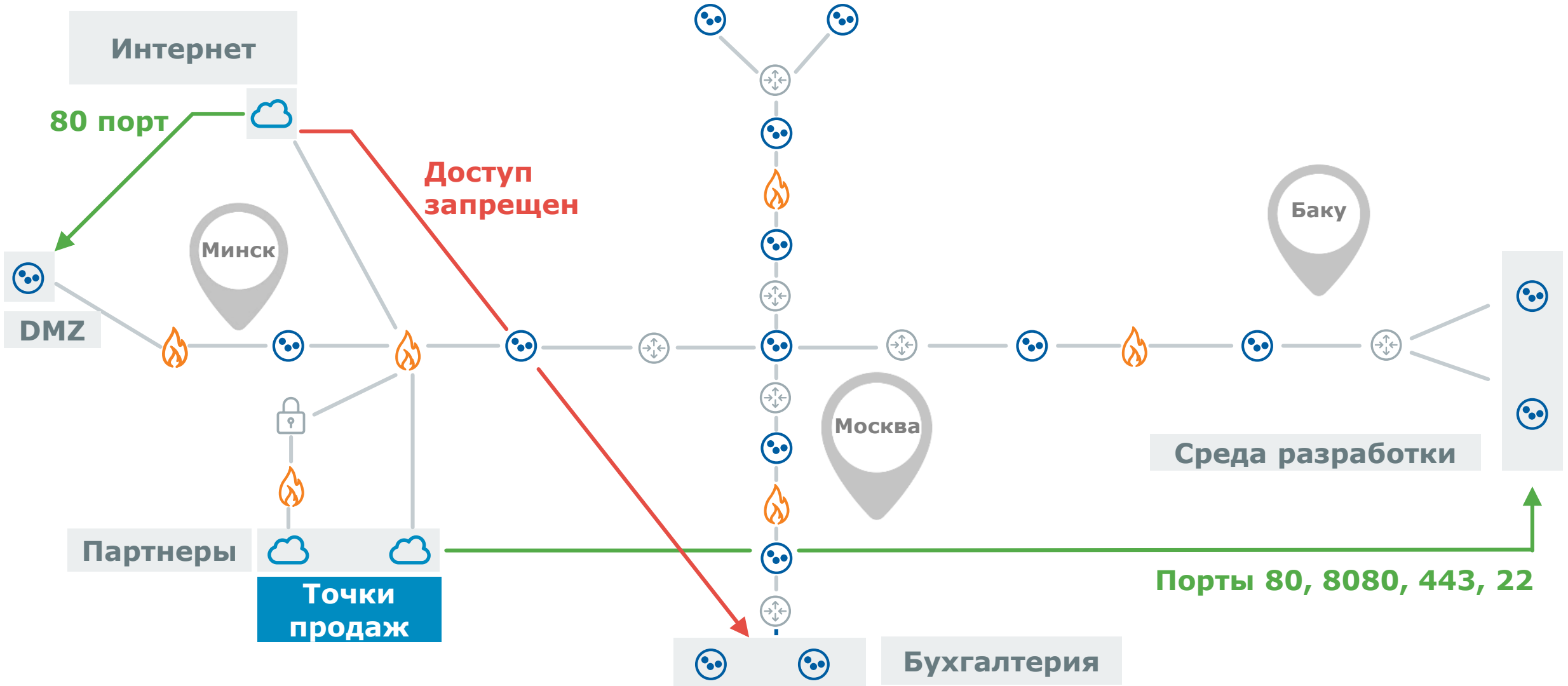
Проверяем наличие доступа в 2 клика

Проверка доступа на лету

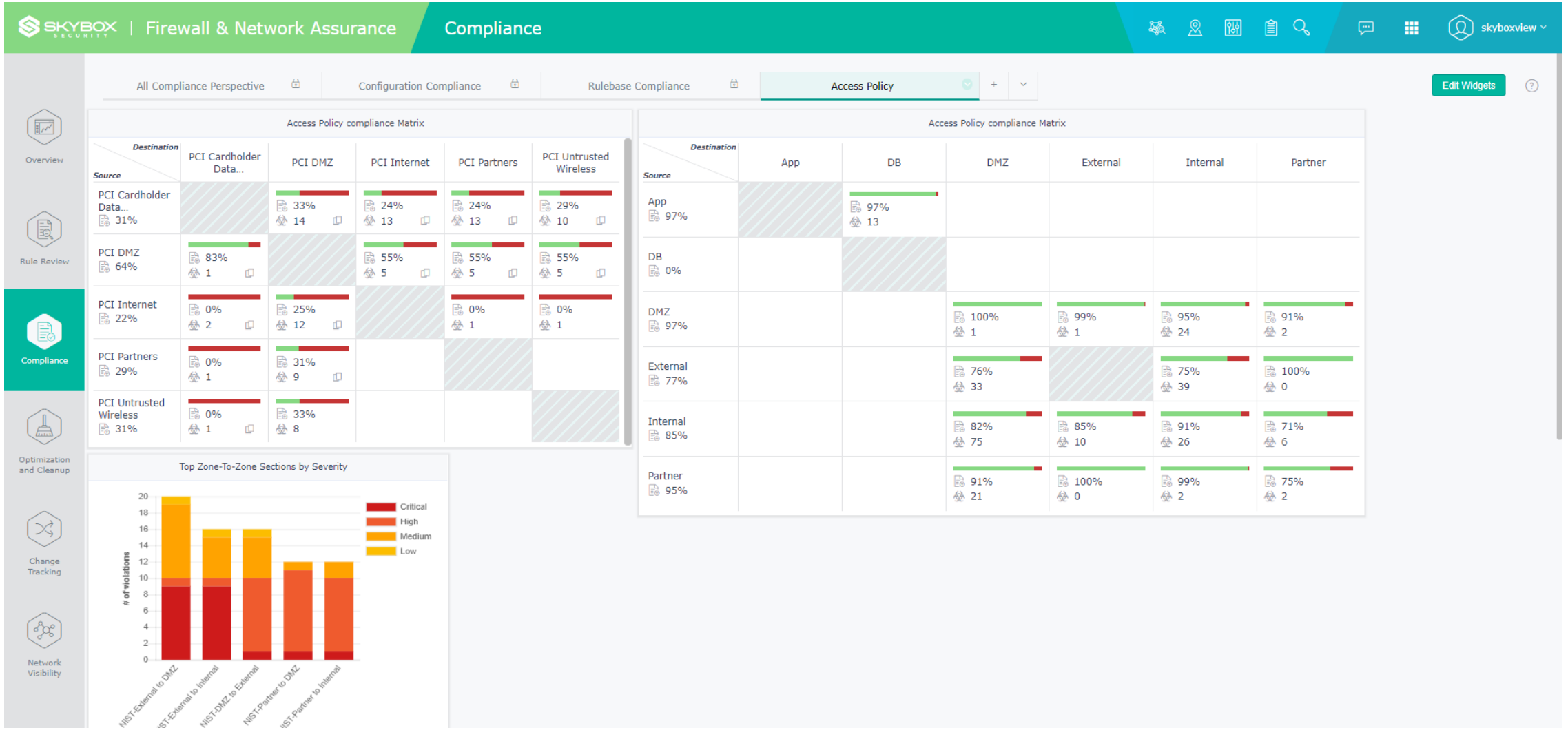


Проверяем отсутствие доступа в 2 клика

Контроль политик сетевого доступа



Соответствие политикам сетевого доступа



Работа с уязвимостями

Возможные сценарии

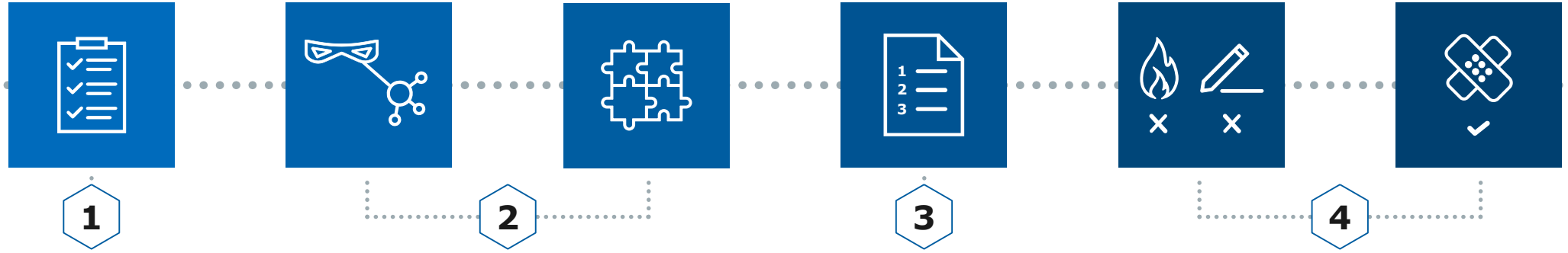
Принцип работы

Выявление уязвимостей в период до и между сканированиями

Расчет векторов атак в контексте сети

Расчет приоритетов и реагирование

Как Это Работает



1 Выявление

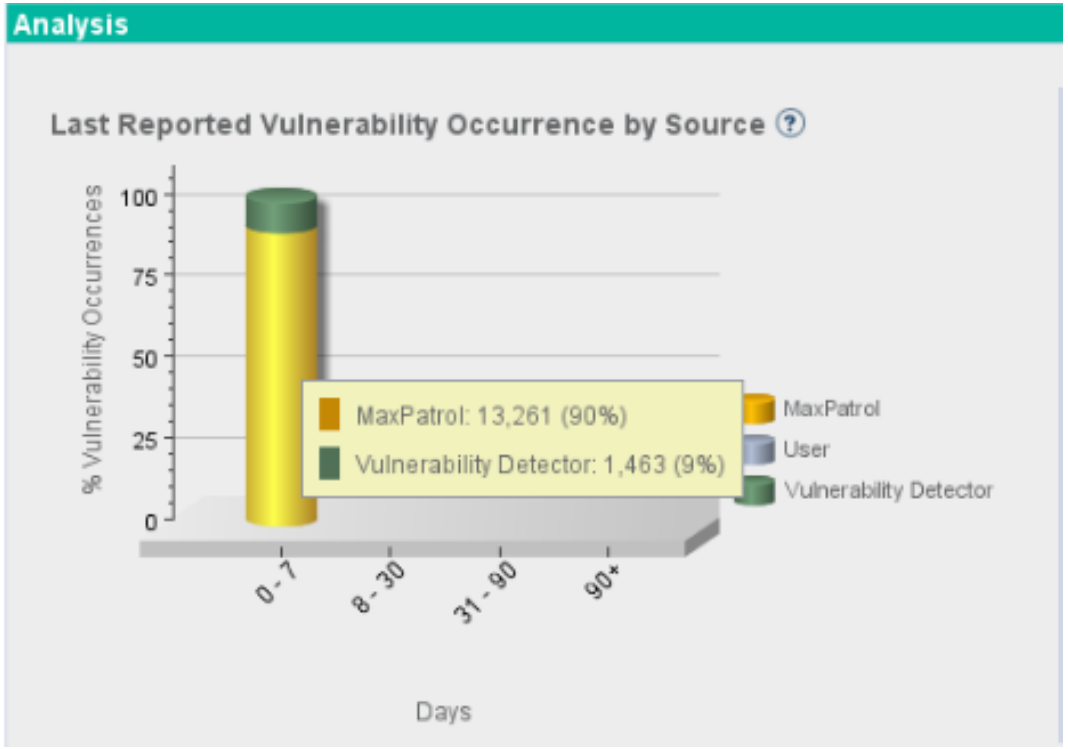
2 Анализ

3 Приоритезация

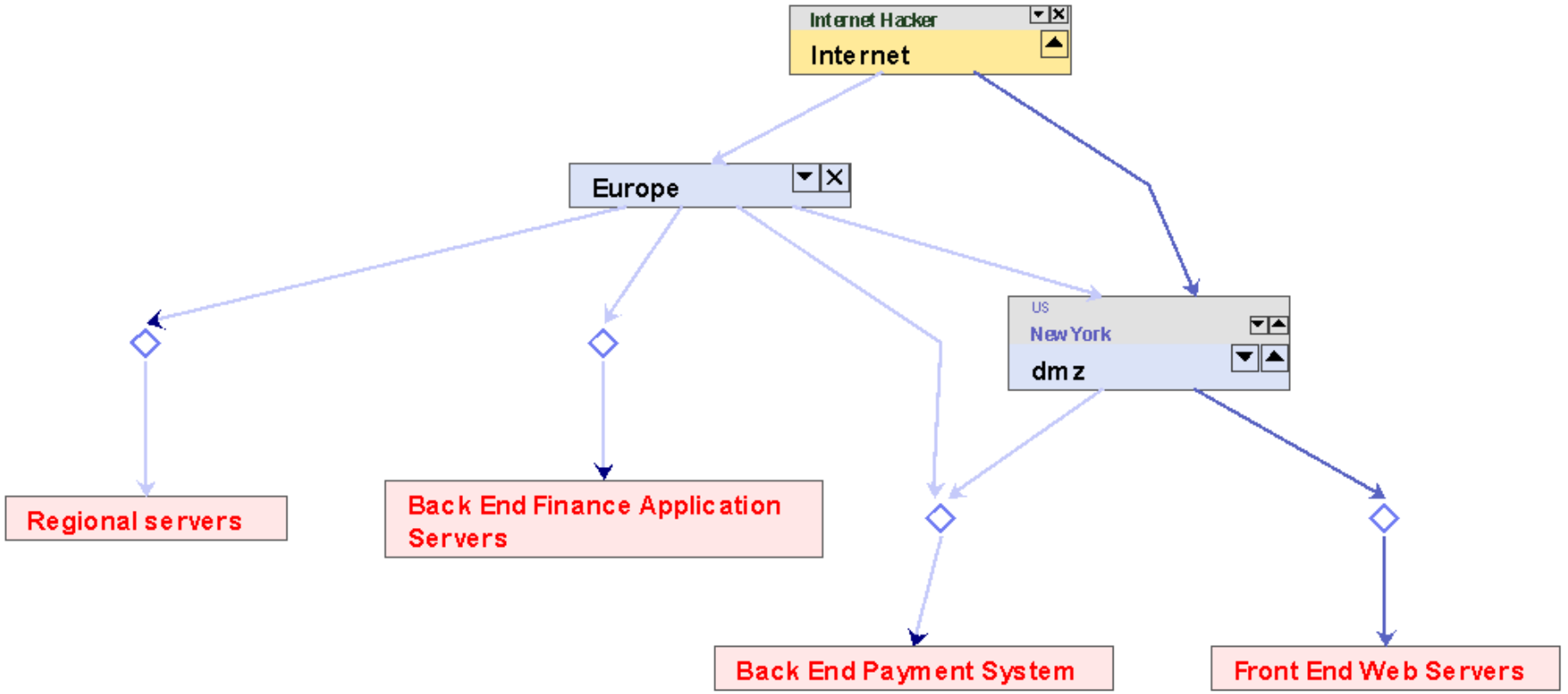
4 Реагирование

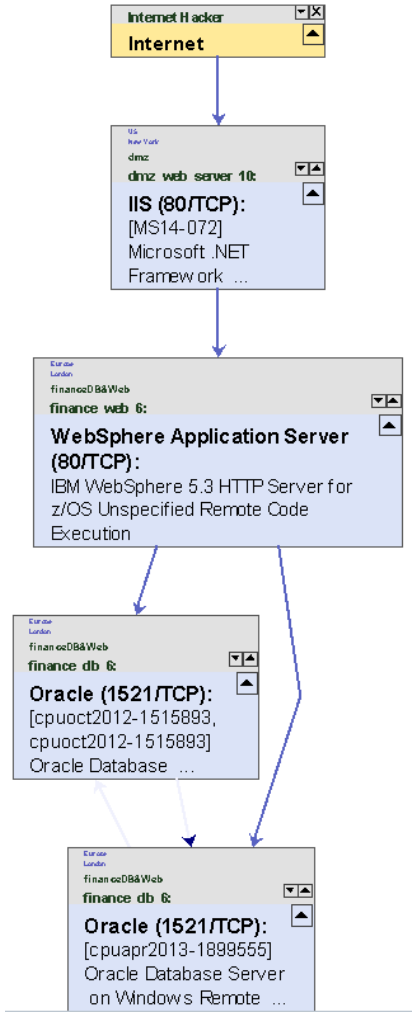
Выявление уязвимостей

- Как это работает:
  - » Загрузка отчетов сканеров
  - » Загрузка отчетов систем инвентаризации SCCM, WSUS и др.
  - » Ежедневное «пассивное» сканирование
- Результат:
  - » Актуальный список всех известных уязвимостей (обновляемая база Skybox из 25+ источников)
  - » актуальный список уязвимостей для IT-активов



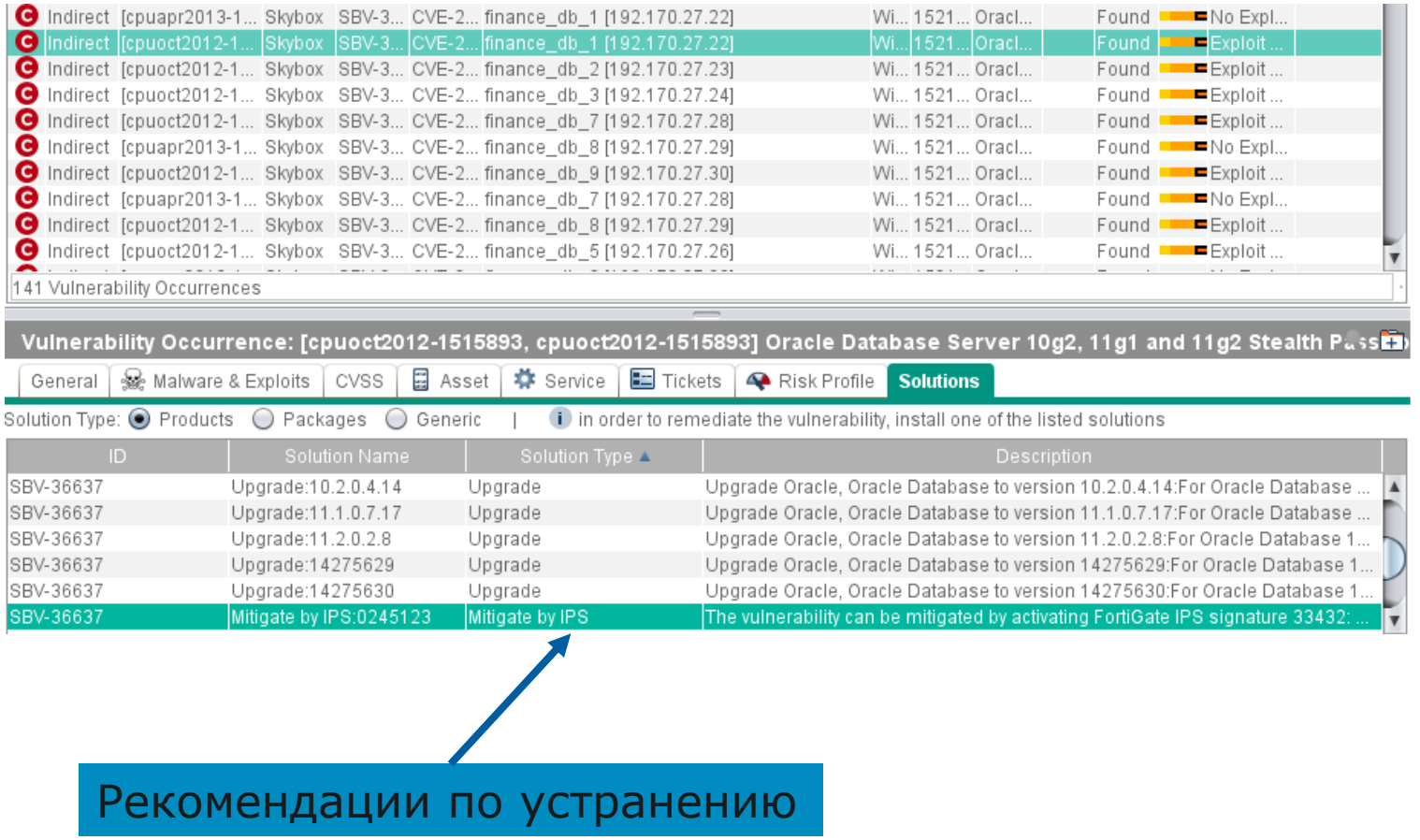
Визуализация вектора атаки





Индикаторы угроз и приоритезация уязвимостей

- Учитываются:
  - Критичность
  - Достижимость (наличие доступа)
  - Уровень злоумышленника
  - Ценность актива
  - Наличие готового эксплойта
  - Статистика атак с использованием конкретной уязвимости



Важность приоритезации

ОПРЕДЕЛЕНИЕ ВСЕХ ИЗВЕСТНЫХ УЯЗВИМОСТЕЙ

ВСЕГО: 70K
Skybox Vulnerability Database

Потенциальная угроза

ОПРЕДЕЛЕНИЕ СУЩЕСТВУЮЩИХ УЯЗВИМОСТЕЙ

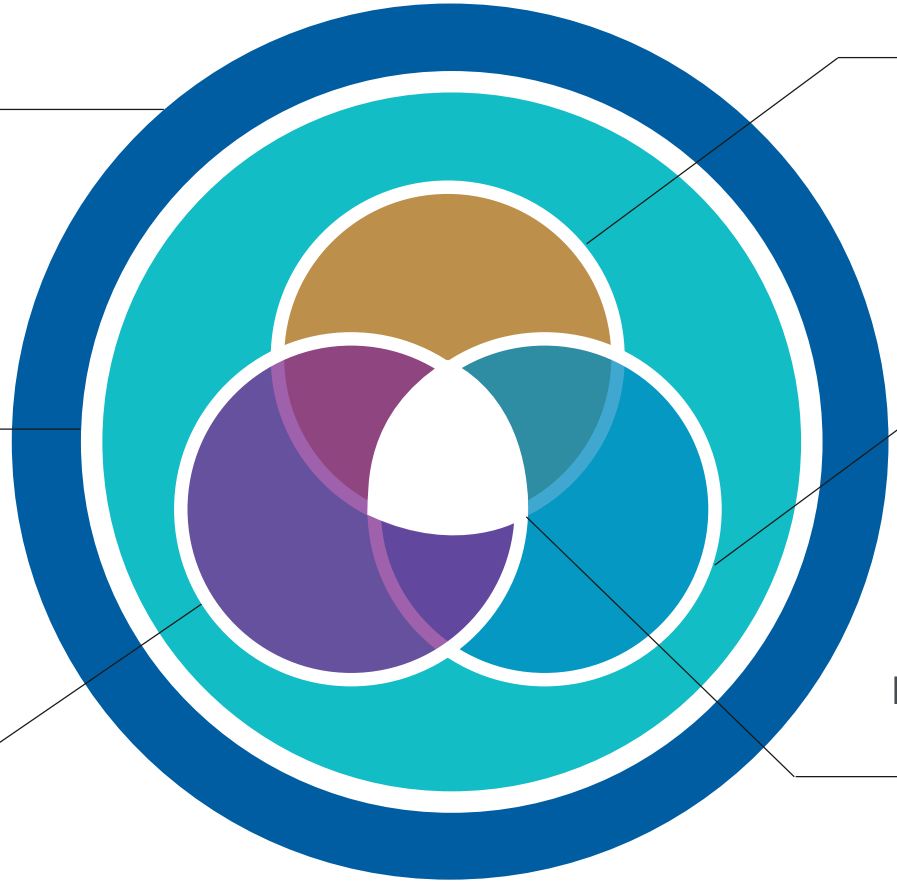
ВСЕГО НАЙДЕНО: 7122
Сканеры защищенности,
Skybox Vulnerability Detector

Потенциальная угроза

НАЛИЧИЕ ЭКСПЛОЙТОВ

ВСЕГО ОПРЕДЕЛЕНО: 1105
Skybox Research Lab real-time threat intelligence

Потенциальная угроза



КОРРЕЛЯЦИЯ С CVSS

ВСЕГО КРИТИЧНЫХ: 3578
CVSS scoring

Потенциальная угроза

ДОСТУПНЫЕ В СЕТИ УЯЗВИМОСТИ

ДОСТУПНО В СЕТИ: 141
Анализ векторов атак

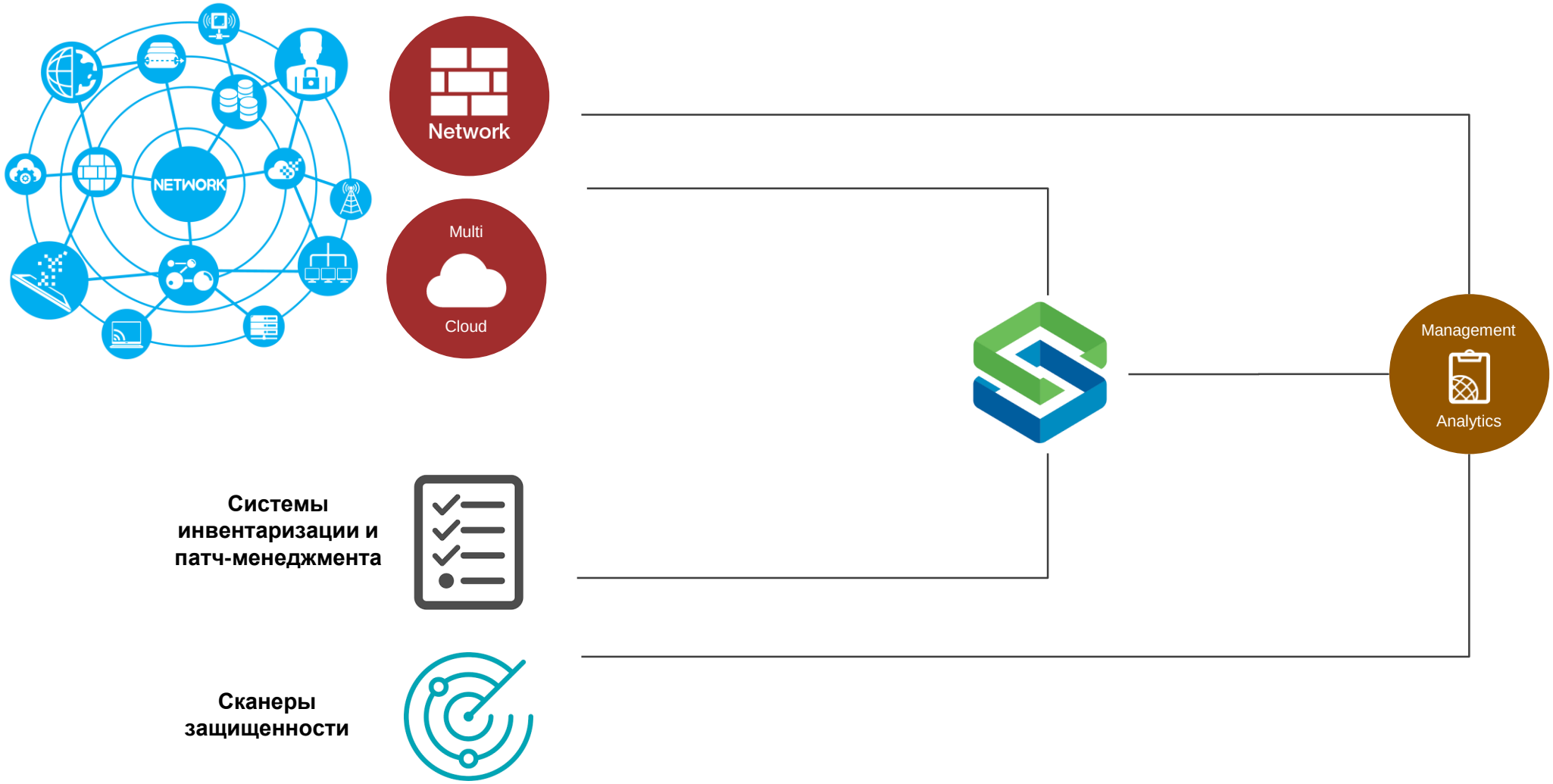
Вероятная угроза

ВЫДЕЛЕНИЕ УЯЗВИМОСТЕЙ С МАКСИМАЛЬНЫМ РИСКОМ

ВСЕГО: 13
Skybox Vulnerability Control Prioritization Center

Вероятная угроза

Fortinet Security Fabric + Skybox Security



FORTINET®

SKYBOX SECURITY

+7 (800) 511 08 28

Sales.Russia@skyboxsecurity.com