Управление сетевой безопасностью на основе намерений

Алексей Андрияшин, Технический директор

20.09.2018

SECURITYDAY

Мир сильно изменился…

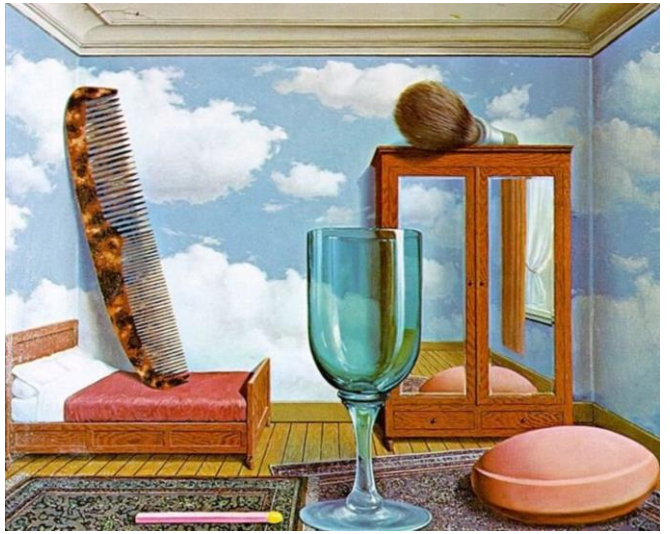
Облачные вычисления

Облака, 1880-е, А.М. Васнецов

Виртуализация

«Thirty» 1937 г. В. Кандинский

Интернет вещей, IoT



«Личные ценности» 1937 г., Р. Магритт

…и продолжает меняться

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ЗНАЧИТЕЛЬНО РАСШИРЯЕТ ПОВЕРХНОСТЬ АТАКИ

Как много производителей могут обеспечивать высокий уровень защиты?

Изучение намерений

Minority Report, 20th Century Fox (North America), DreamWorks Pictures (International), 2002

- Максимальное **исключение** уязвимостей
- Предотвращение угроз **до** их возникновения
- **Адаптация** к изменениям
- Мгновенная **классификация** угроз
- Устойчивое состояние **защищенности**
- Отсутствие **недопустимых** рисков

Предпосылки развития IBNS

- Облачные технологии
- Микросегментация
- DevOPS
- SDN/SDS/SDDC/SDx
- Большие данные
- Agile
- IoT

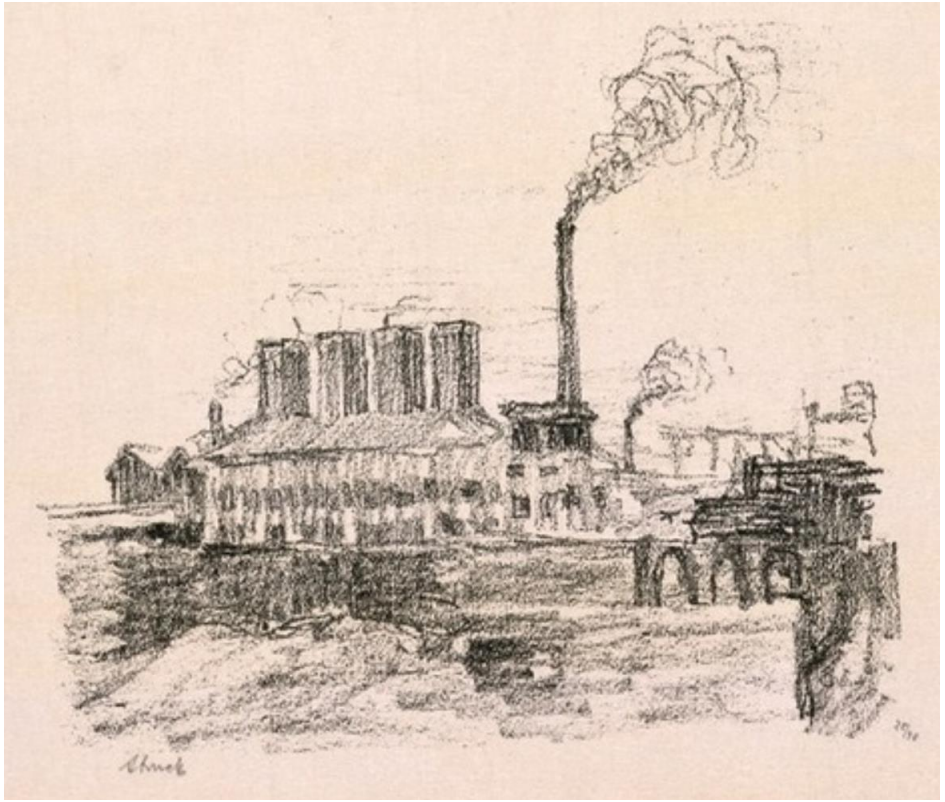
Политики устройств безопасности быстро устаревают и **теряют актуальность**

- https://www.infosecurity-magazine.com/webinars/the-time-for-intentbased-security/

«Сын человеческий» (1964), М.Рене

Гибридные технологии

- Безопасность должна учитывать гибридный принцип построения корпоративных сетей:
  - » SDN (software-defined networking,)
  - » SD-WAN (software-defined, WAN)
  - » Hybrid WAN



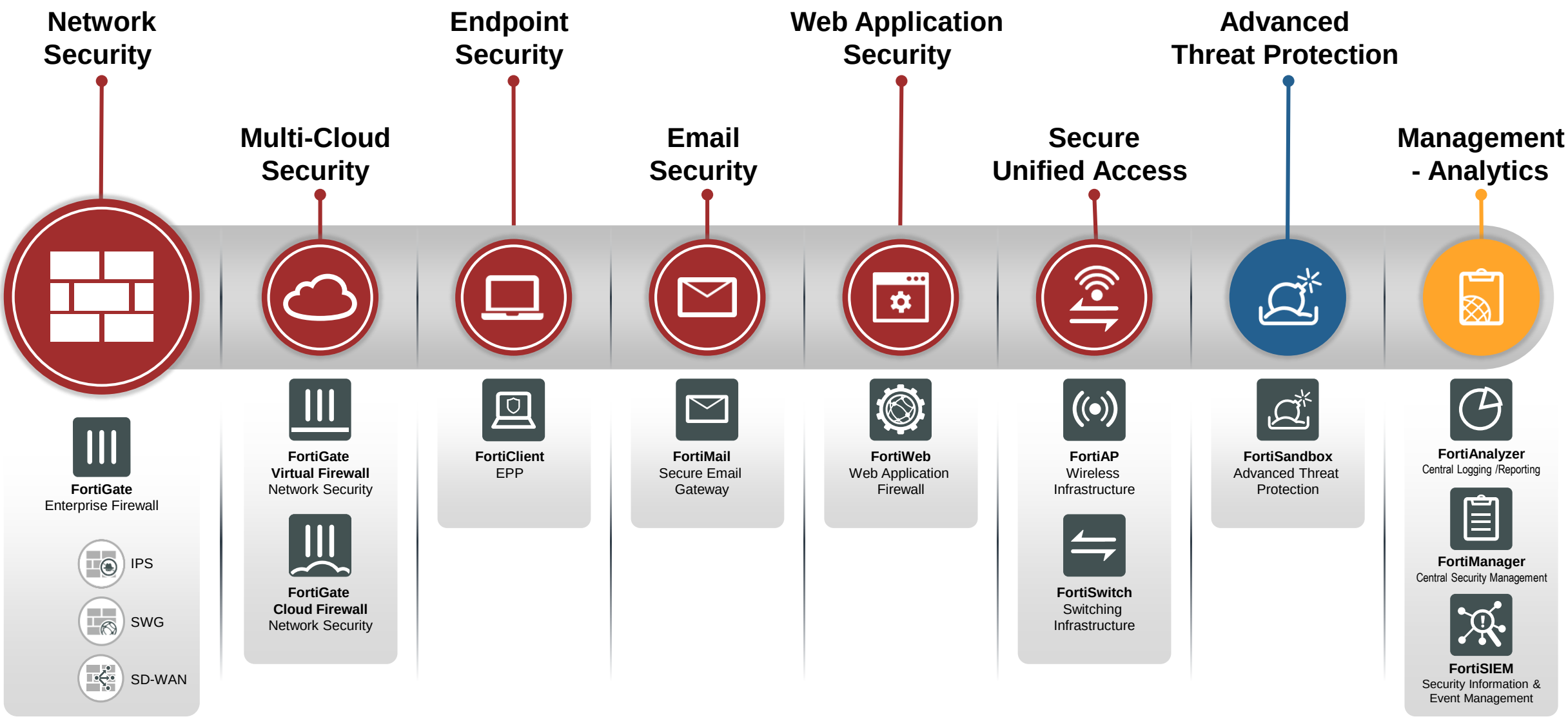
“Нью Йорк, Фабрика”, Г. Штрук

Ключ к построению IBNS

- Определение желаемого уровня защищенности
- Автоматизация процессов для минимизации ручного описания правил, обеспечивающих необходимый уровень безопасности:
  - » в распределённом окружении
  - » в сетях с высокой сегментацией
  - » при высокой мобильности пользователей и устройств

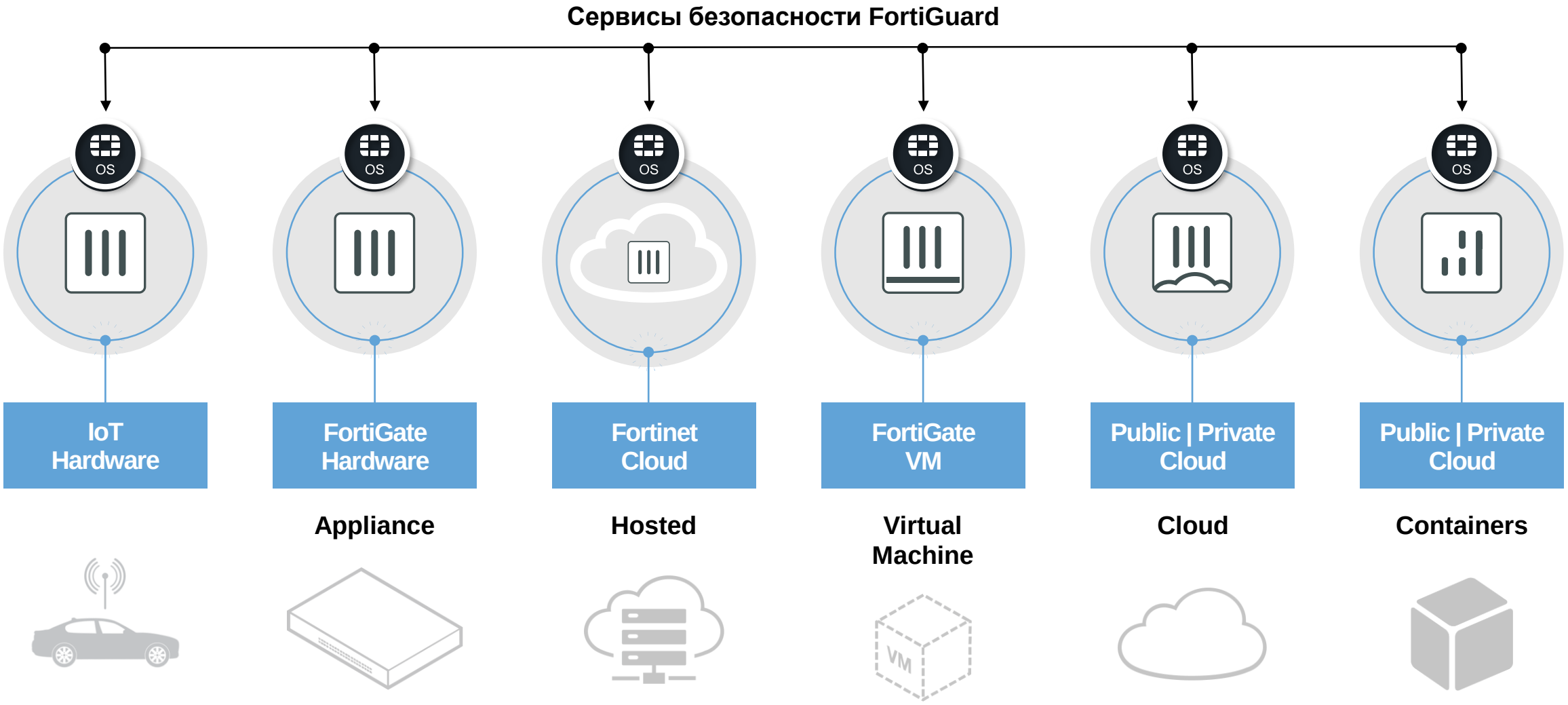
Н. Клюшник “Ключи”, 2014

2018 Fortinet – Фабрика безопасности

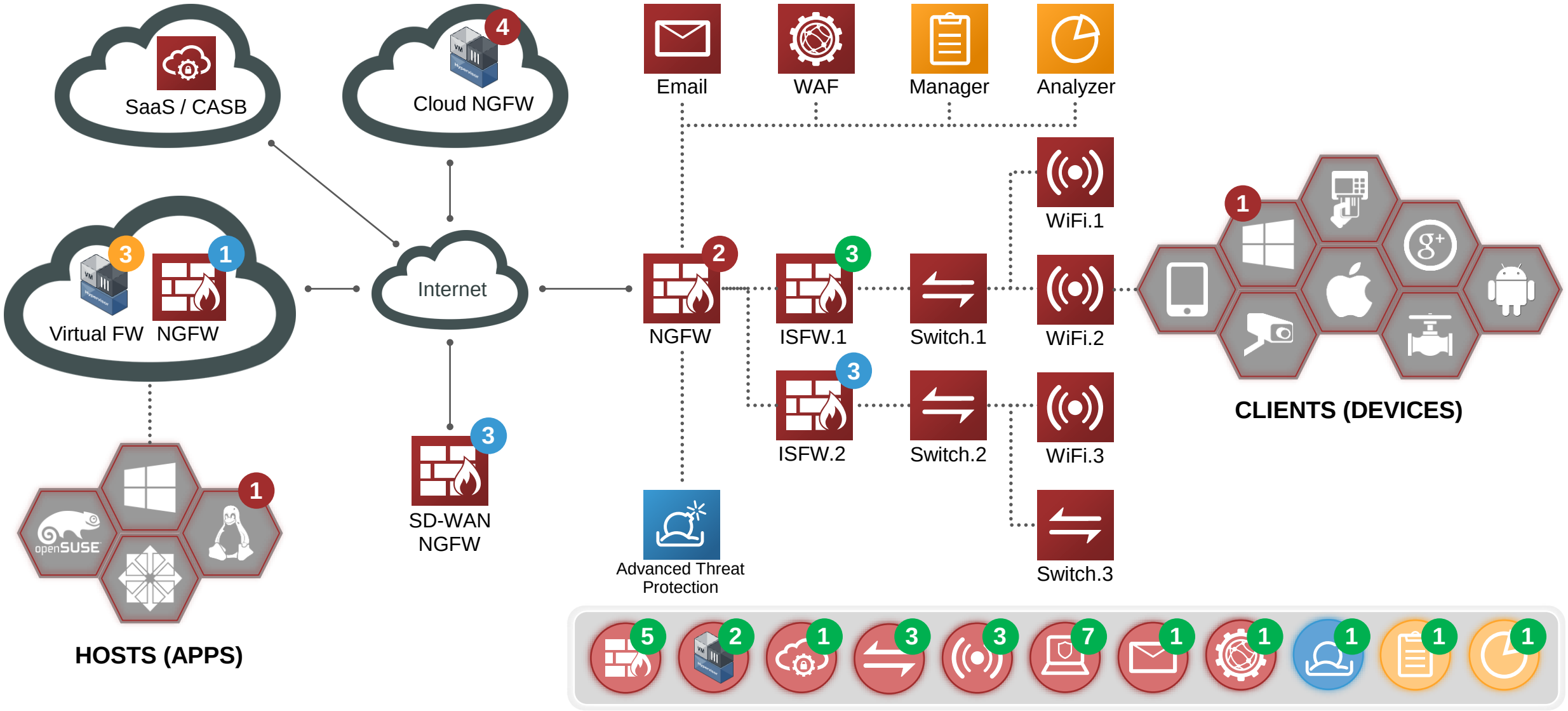


Адаптивная архитектура безопасности

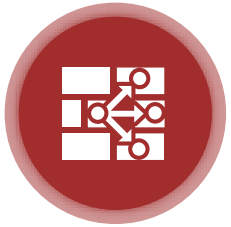
Оборудование + Программное обеспечение + Сервисы



Фабрика безопасности (топология)



SD-WAN



Поддержка приложений

Видимость более чем 3500 приложений

Управление трафиком приложений для соблюдения SLA

Сетевая гибкость

Динамический выбор маршрута соответствующего SLA

Отказоустойчивость подключений на уровне ISP

Несколько ISP

Независимый транспорт с поддержкой Ethernet, 3G/4G

Объединение нескольких интерфейсов в один логический SD-WAN

Эффективное управление

Один клик для подключения нескольких филиалов к центру обработки данных

Минимальное количество ресурсов для подключения удаленной точки

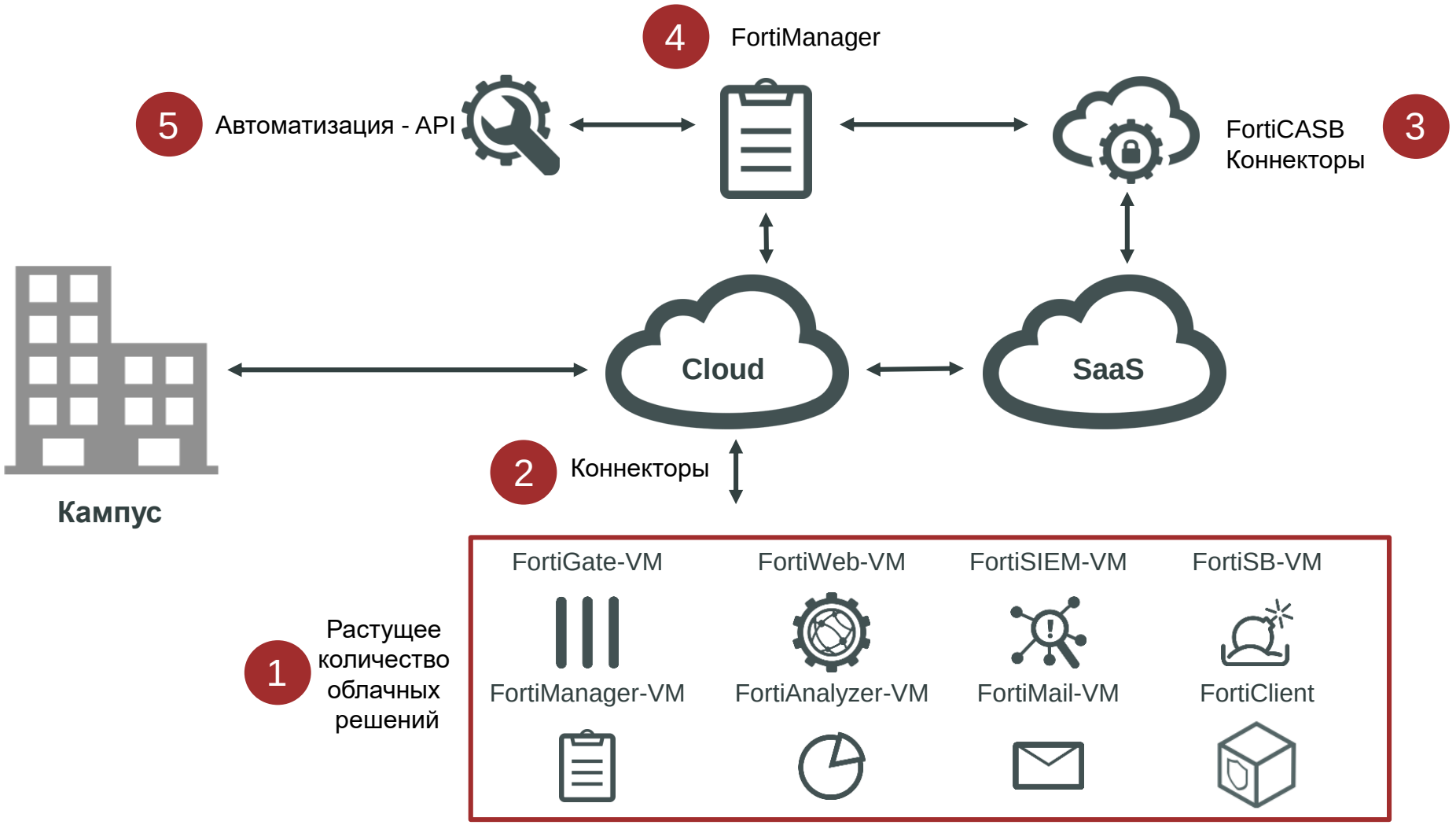
Проверенные решения

Проверено NSS Lab и многими сторонними компаниями

Высокая производительность, обеспеченная аппаратными Security Processor

Облачные решения Fortinet

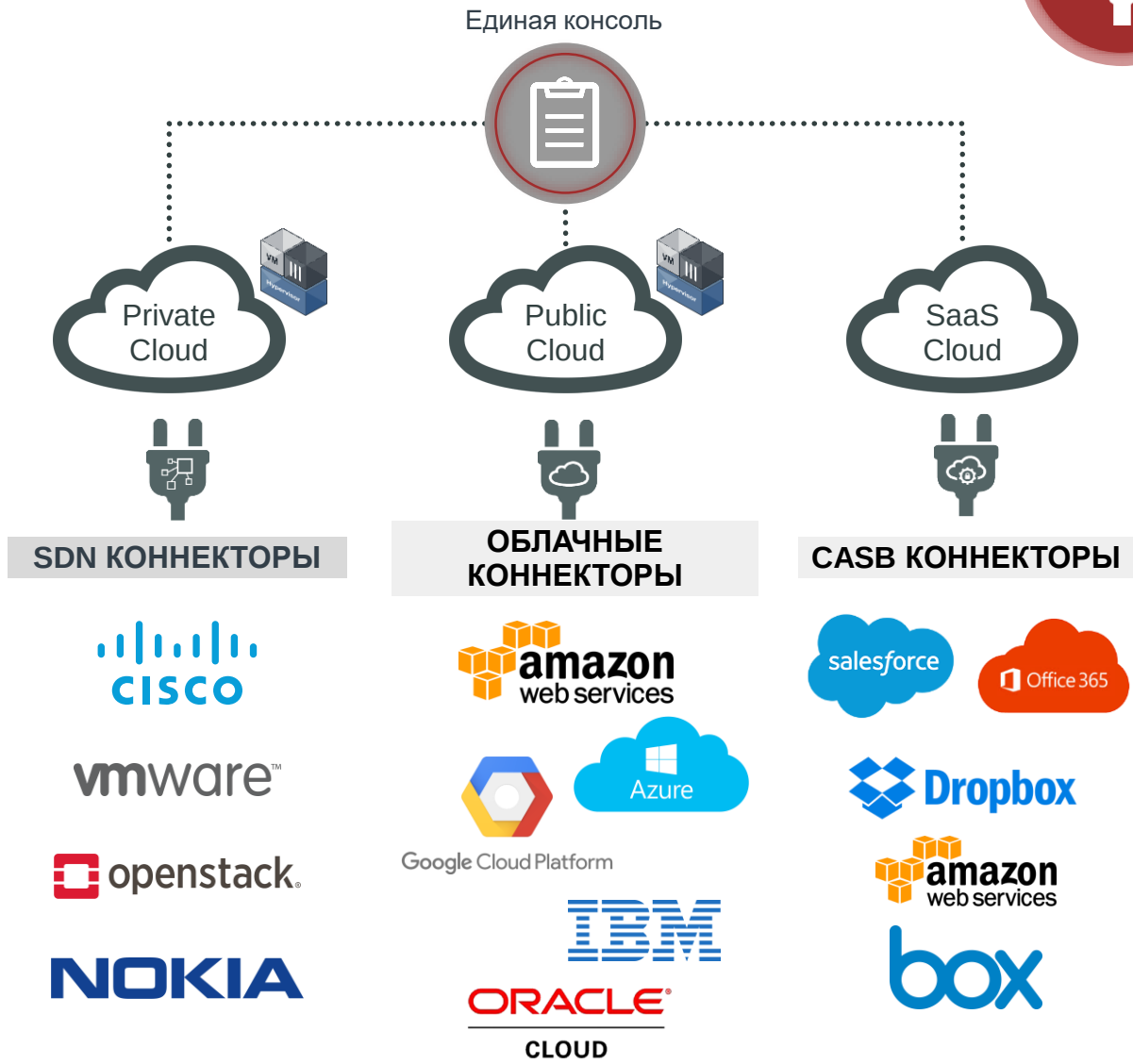
Коннекторы



Облачные коннекторы

Коннекторы

Virtual Security	Cloud Security	API
Applications	Applications	Applications
Data	Data	Data
O/S	O/S	O/S
Virtualization	Virtualization	Virtualization
Servers	Servers	Servers
Networking	Networking	Networking



Сервисы безопасности FortiGuard

FortiGuard

Baseline Protection

- IP Reputation
- Internet DB
- Certificate & Domain White List
- Application Control
- Antispam

+

Threat Protection

- Antivirus
- Intrusion Prevention

Unified Protection

- Web Filtering
- Antivirus
- Intrusion Prevention

Enterprise Protection

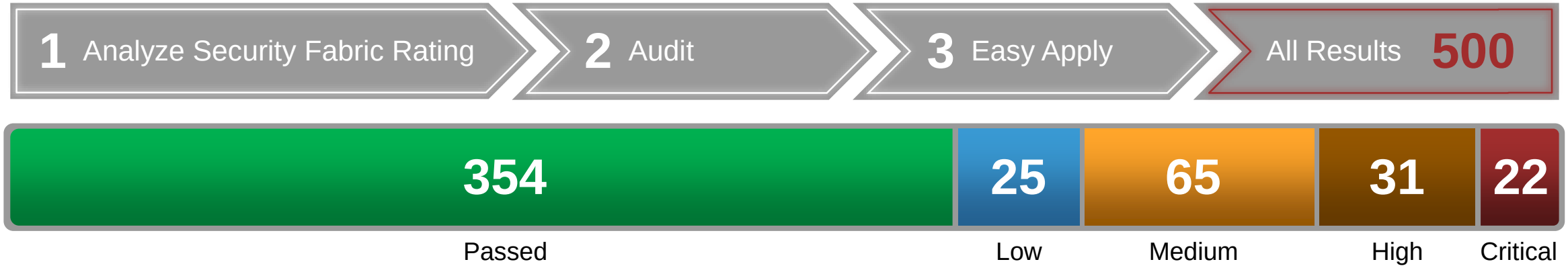
- **Virus Outbreak Service**
- **Content Disarm & Reconstruction**
- FortiSandbox Cloud
- Web Filtering
- Antivirus
- Intrusion Prevention

Industrial Security Service

Security Audit Service

Адаптивный анализ защищенности

Security Rating



Агенты безопасности и защита конечных точек

Поддержка хостов и конечных точек

Fabric Agent

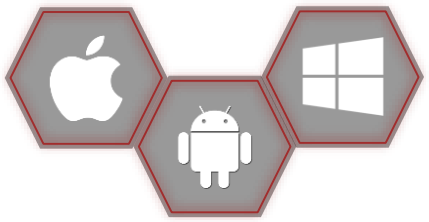
ЗАЩИТА КОНЕЧНЫХ ТОЧЕК

VPN АГЕНТЫ

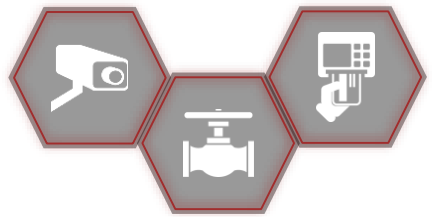
АГЕНТЫ ФАБРИКИ БЕЗОПАСНОСТИ – Сетевая телеметрия

БАЗА ДАННЫХ УСТРОЙСТВ

ХОСТЫ (ПРИЛОЖЕНИЯ)



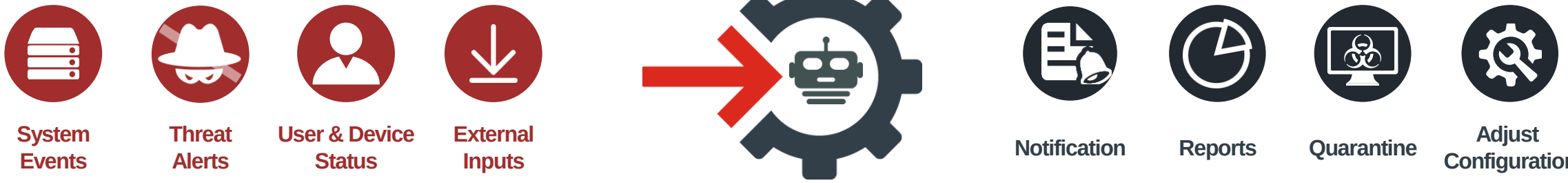
КОНЕЧНЫЕ ТОЧКИ (УСТРОЙСТВА)



IOT (УСТРОЙСТВА)

Автоматизация процессов ИБ

Автоматизация

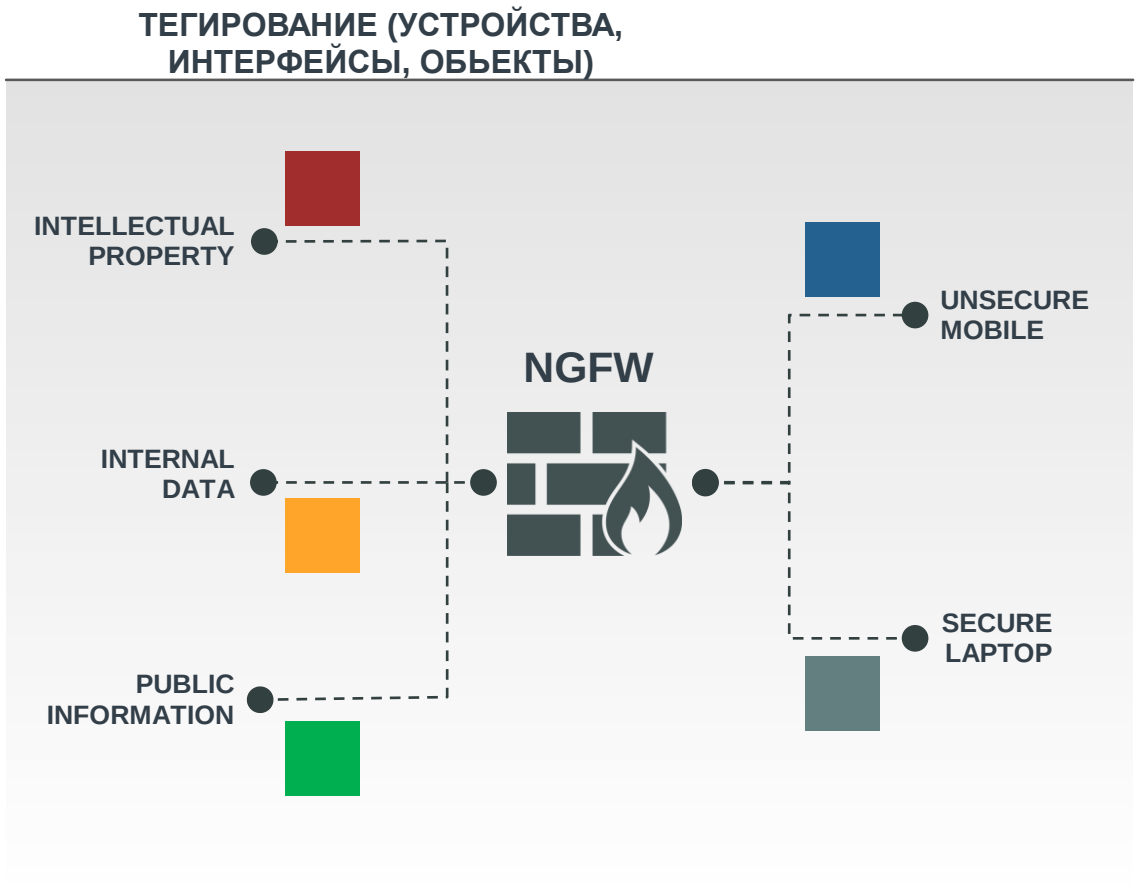


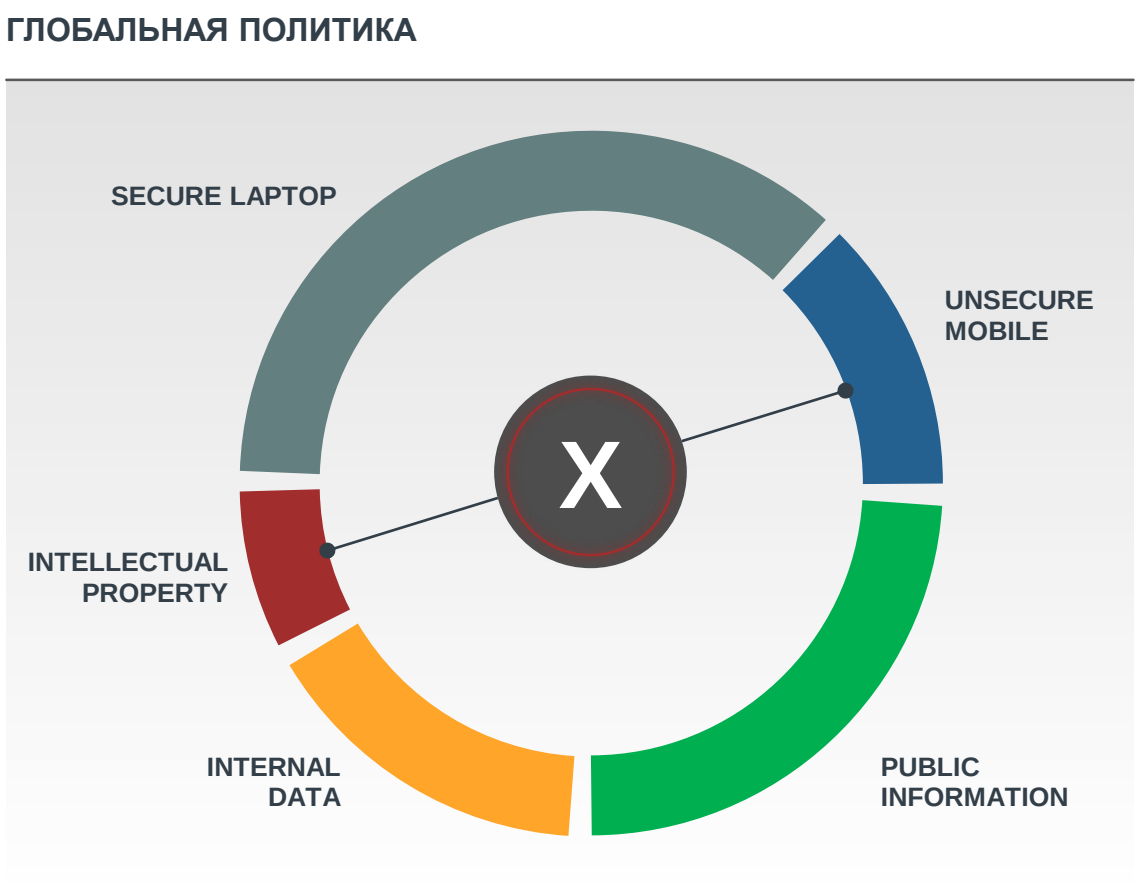
Автоматизация процессы безопасности с использованием триггеров для выполнения соответствующих действий

Безопасность на основе намерений (IBNS)

Бизнес логика при реализации политик безопасности

Тегирование





УПРАВЛЕНИЕ

Удобство мониторинга и отчетности

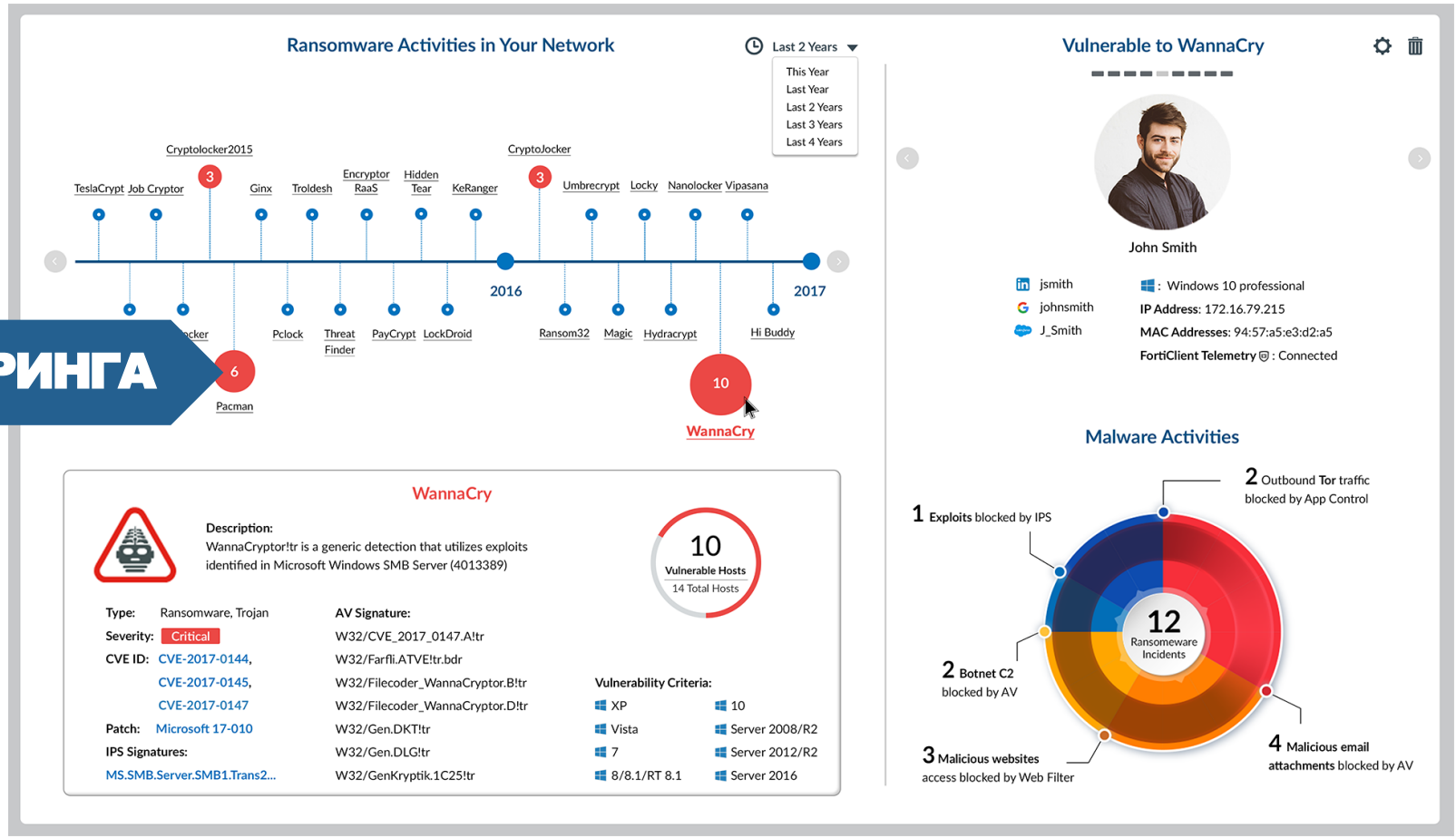
ОТЧЕТЫ БЕЗОПАСНОСТИ

Новые шаблоны отчетов для менеджмента / C-уровня и аудиторов

Удобство мониторинга и отчетности

ВИДЖЕТЫ ДЛЯ МОНИТОРИНГА

Дополнительные виджеты мониторинга в FAZ



russia@fortinet.com


FORTINET®