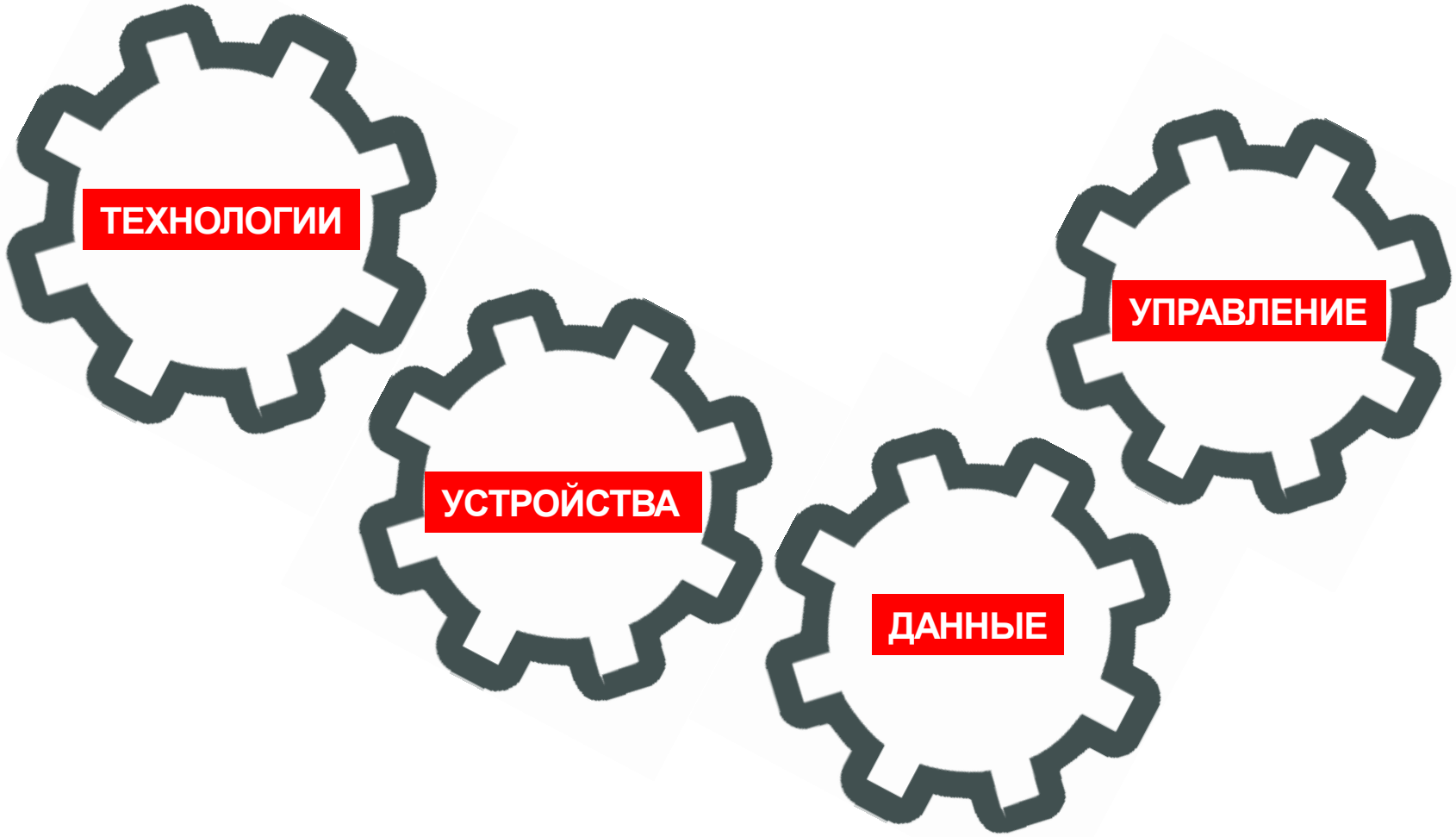
Повышение эффективности процессов ИБ с помощью средств автоматизации Fortinet Security Fabric

Гордеев Вячеслав

Пути автоматизации



Fortinet Security Fabric

Fabric APIs

Отслеживание всей поверхности атаки

Network Operations

КОМПЛЕКСНОСТЬ

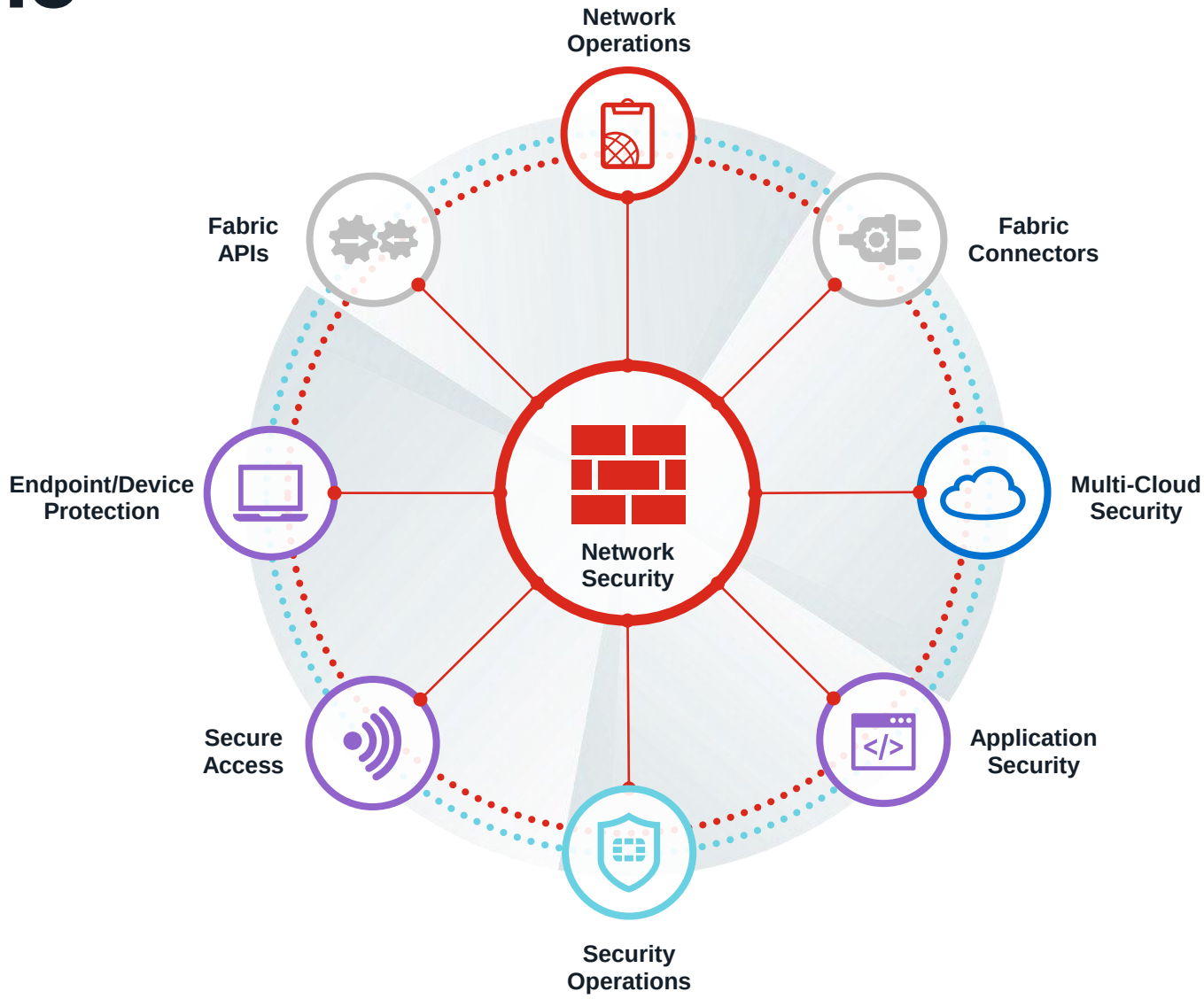
Защита всех устройств, сетей и приложений

Fabric Connectors

АВТОМАТИЗАЦИЯ

Security Operations

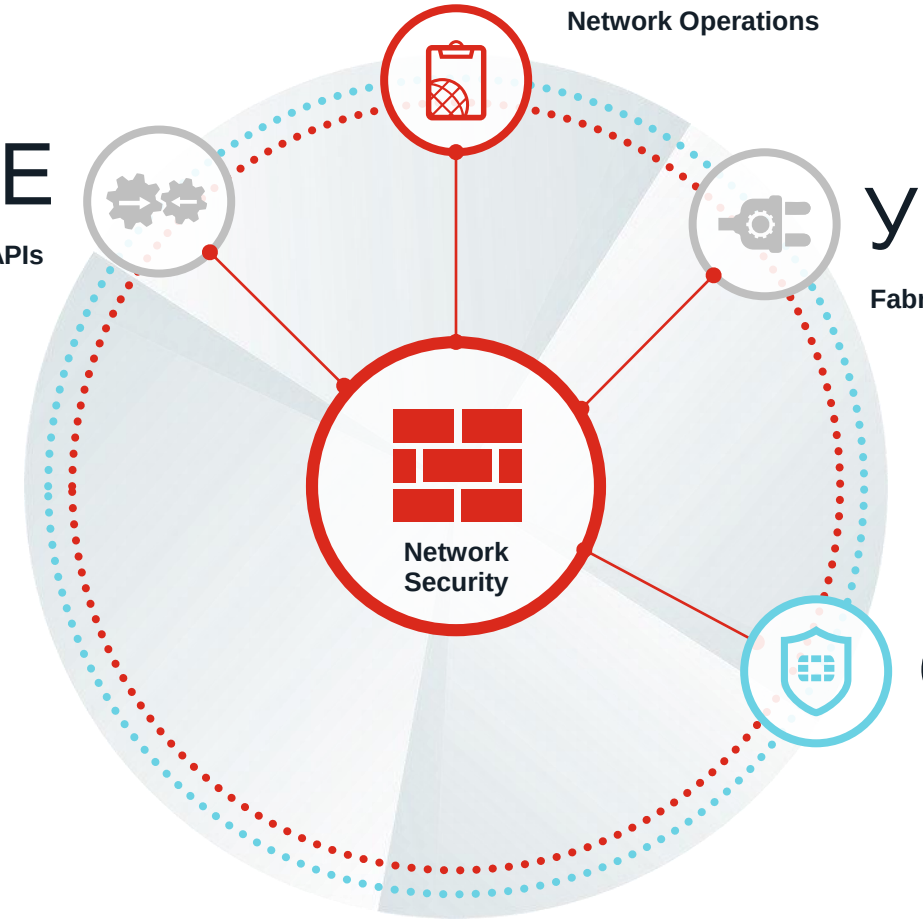
Действия и реагирование на основе машинного обучения



Автоматизация структуры безопасности

РАЗВЕРТЫВАНИЕ
Network Operations

РЕАГИРОВАНИЕ
Fabric APIs



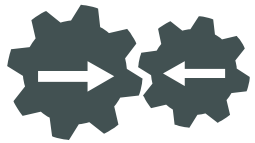
УПРАВЛЕНИЕ
Fabric Connectors

ОБНАРУЖЕНИЕ
Security Operations

Fabric APIs

Реагирование

Открытая экосистема



FABRIC API

- Партнеры Fabric охватывают широкий спектр сетевых технологий от IoT до облаков
- Партнеры пишут код с использованием Fabric API для интеграции с продуктами Fortinet
- Fortinet официально подтверждает поддержку интеграции

DEVOPS

- Созданные в Fortinet скрипты DevOps, автоматизируют обеспечение безопасности через FortiManager
- Полная автоматизация функциональных возможностей FortiGate и управление конфигурацией
- Легко выполняются, доступны в FNDN & GitHub

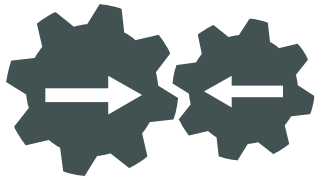
FABRIC CONNECTORS

- Fabric Connectors обеспечивают глубокую интеграцию с компонентами экосистемы клиента, где критически важна автоматизация безопасности
- Существуют различные типы Fabric Connectors – список постоянно пополняется
- Активируются простым нажатием на GUI

Типы партнерских интеграций

Fabric-Ready (Fabric APIs)

- Партнер разработал решения для интеграции с продуктами FTNT
- На основе существующих API и / или стандартных протоколов (RADIUS, SYSLOG, SSH и т. д.)
- (Обычно) отсутствие написанного кода со стороны FTNT
- FTNT тестирует решение, чтобы убедиться, что интеграция работает

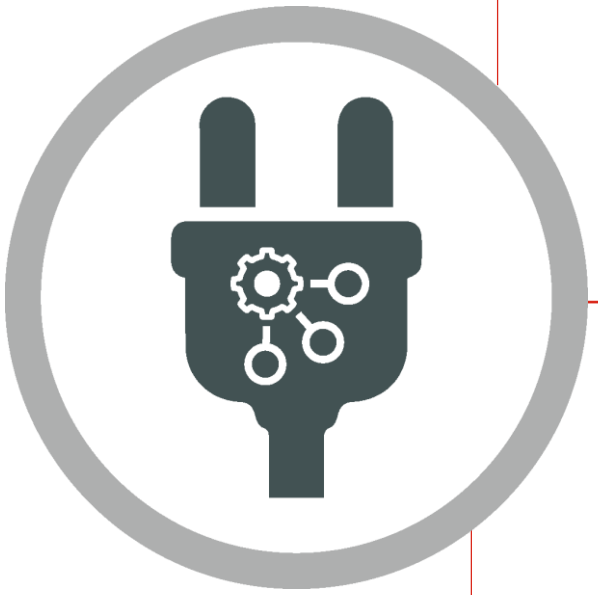


Fabric Connectors

- Fortinet пишет специализированный код
- Управляется через GUI / CLI
- В основном на базе API
- Разработка функциональных возможностей по интеграции производится FTNT
- Может потребоваться совместное тестирование с партнером

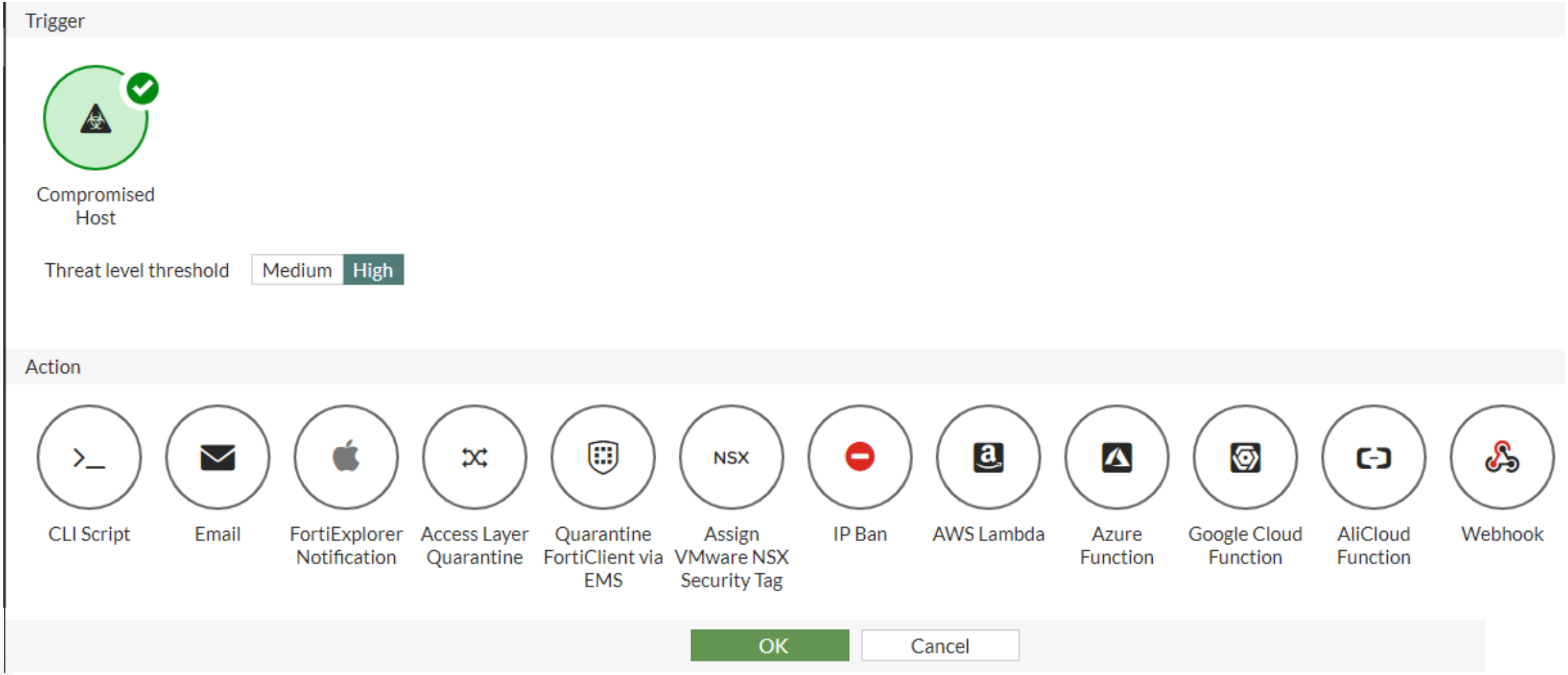
Автоматизация реагирования

AUTOMATION ENGINE



- Отправка HTTP запроса
- Автоматизация оповещений SOC
- API / script response

Правила автоматизации



Automation (& dev-ops)

- Пример карантина:
  - Любой триггер
  - Любое действие

https://github.com/**Fortinet**

Fortinet Developer Network

Триггер

Действие

КАРАНТИН

В целом, мне нужна ***эффективность и автоматизация***

Эксплуатационные расходы намного превышают любые первоначальные затраты на продукт ... более быстрое устройство, без применения средств автоматизации - ничего не значит.

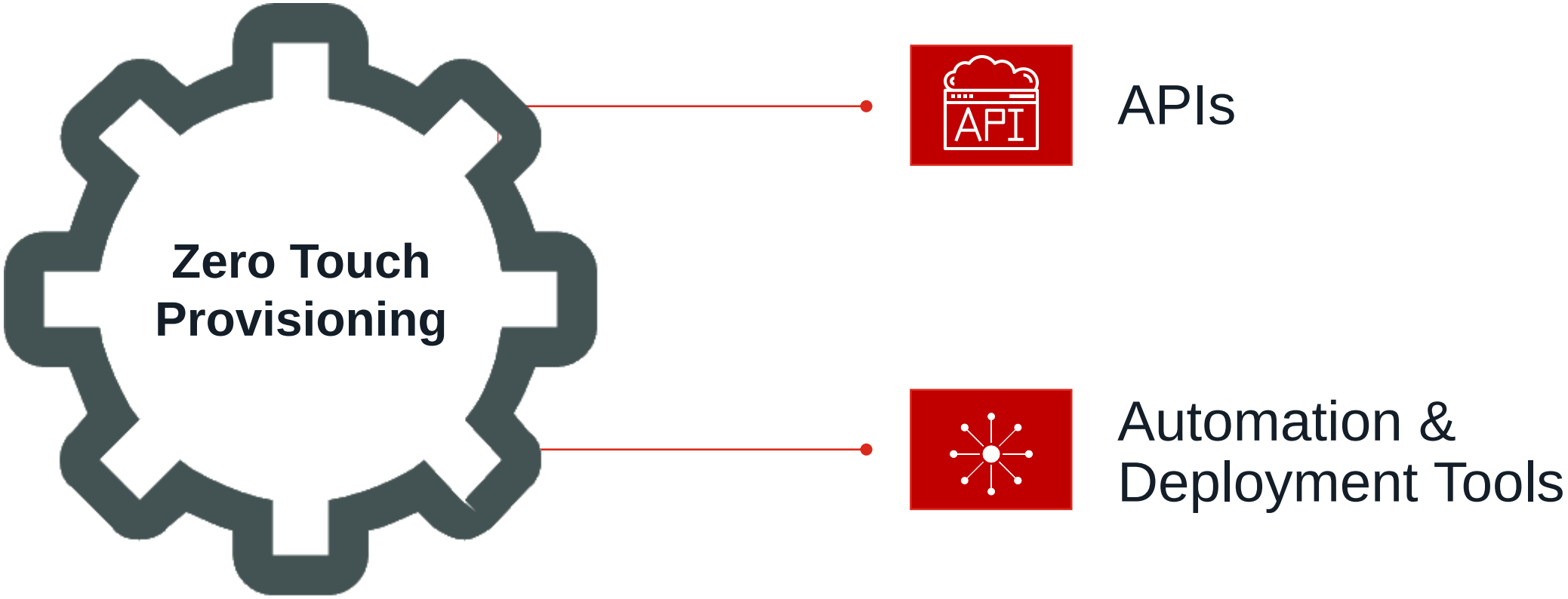
Гибкие функции		
• Switch VLAN	• Host (EMS)	• NSX
• AP VLAN	• FortiNAC	• Webhook
• Captive Portal	• AWS Lambda	• ServiceNow

FORTINET

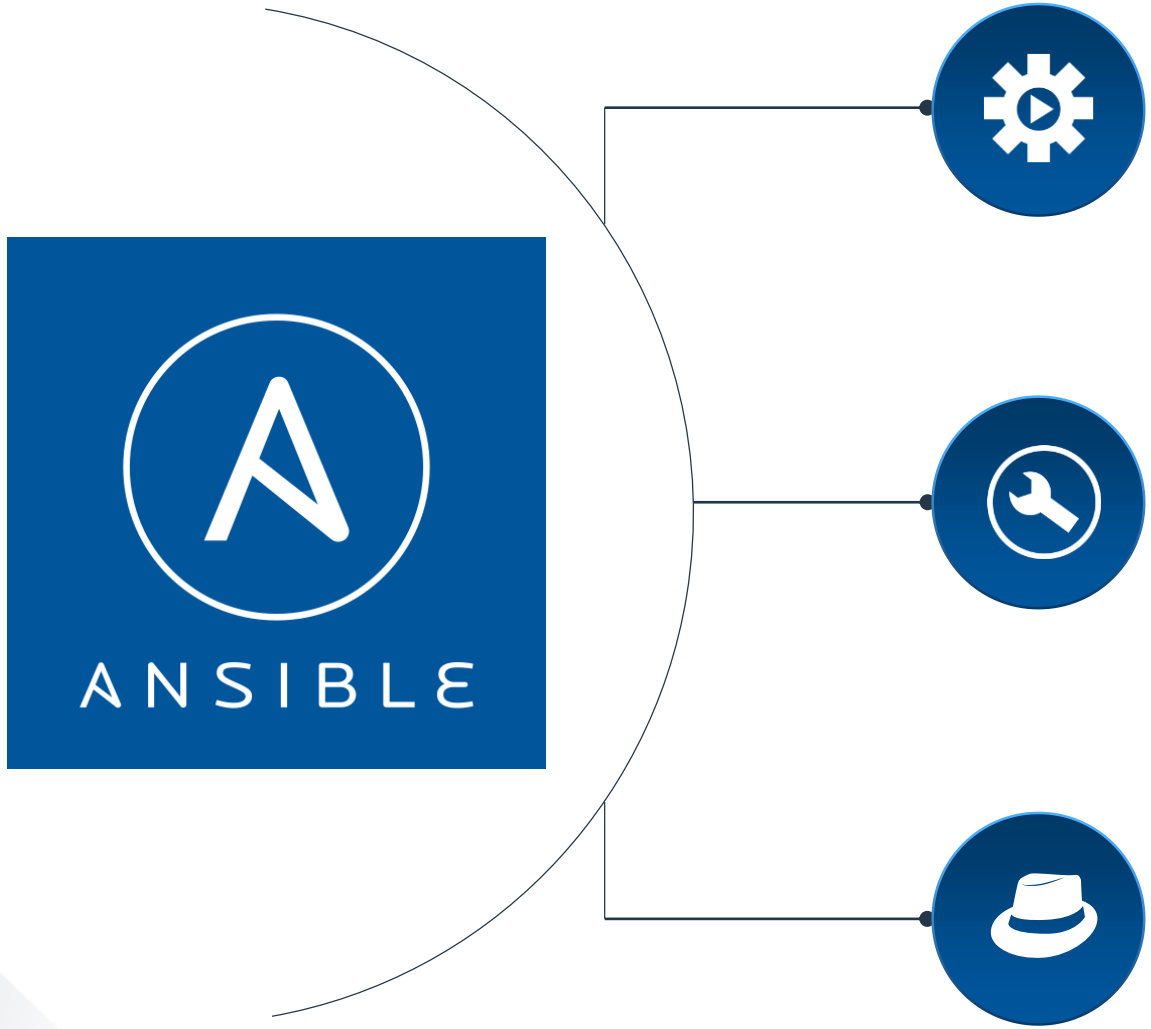
Network Operations

Развертывание

Автоматизация развертывания



Автоматизация развертывания - Ansible



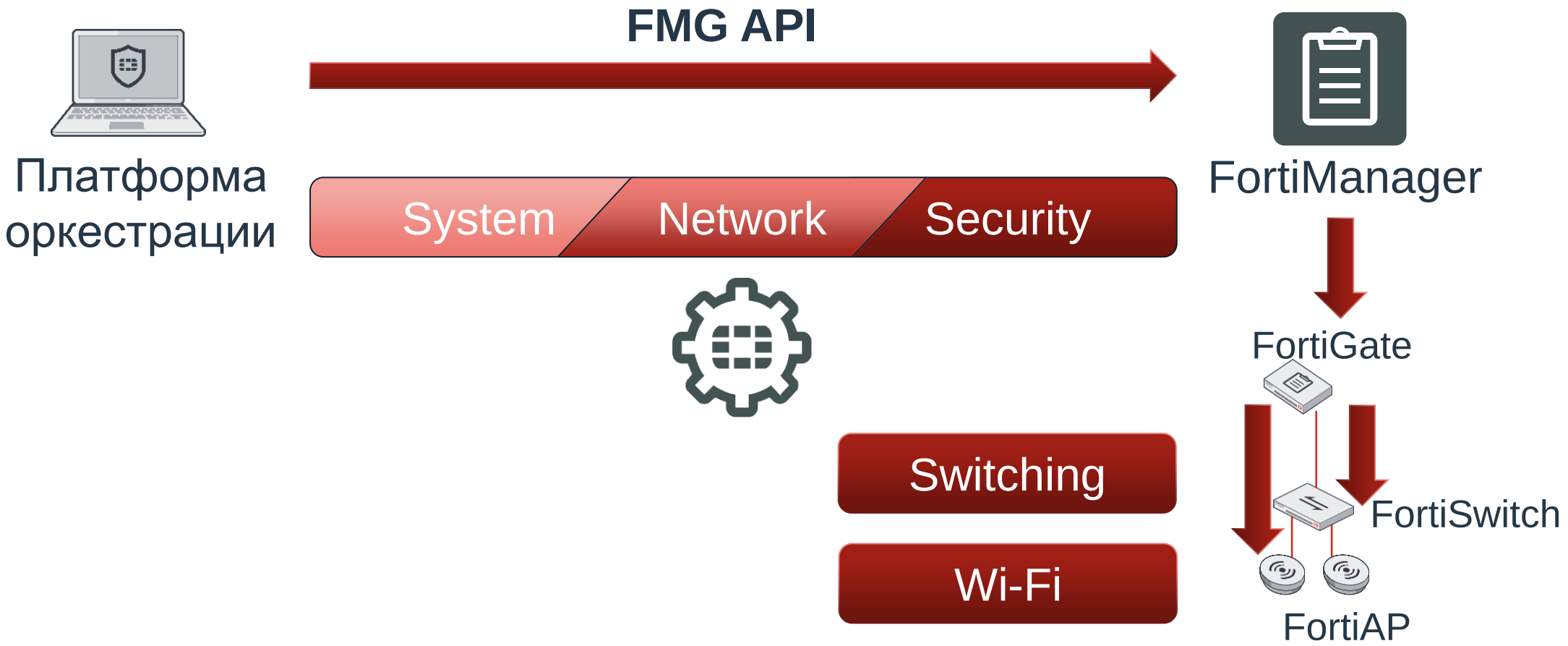
Это утилита для автоматизации ИТ

А также для ИТ оркестрации

Настраивает и администрирует вашу ИТ-инфраструктуру

Управляется RedHat и поддерживается сообществом Open Source

Полностью автоматизированное развертывание – SD-WAN



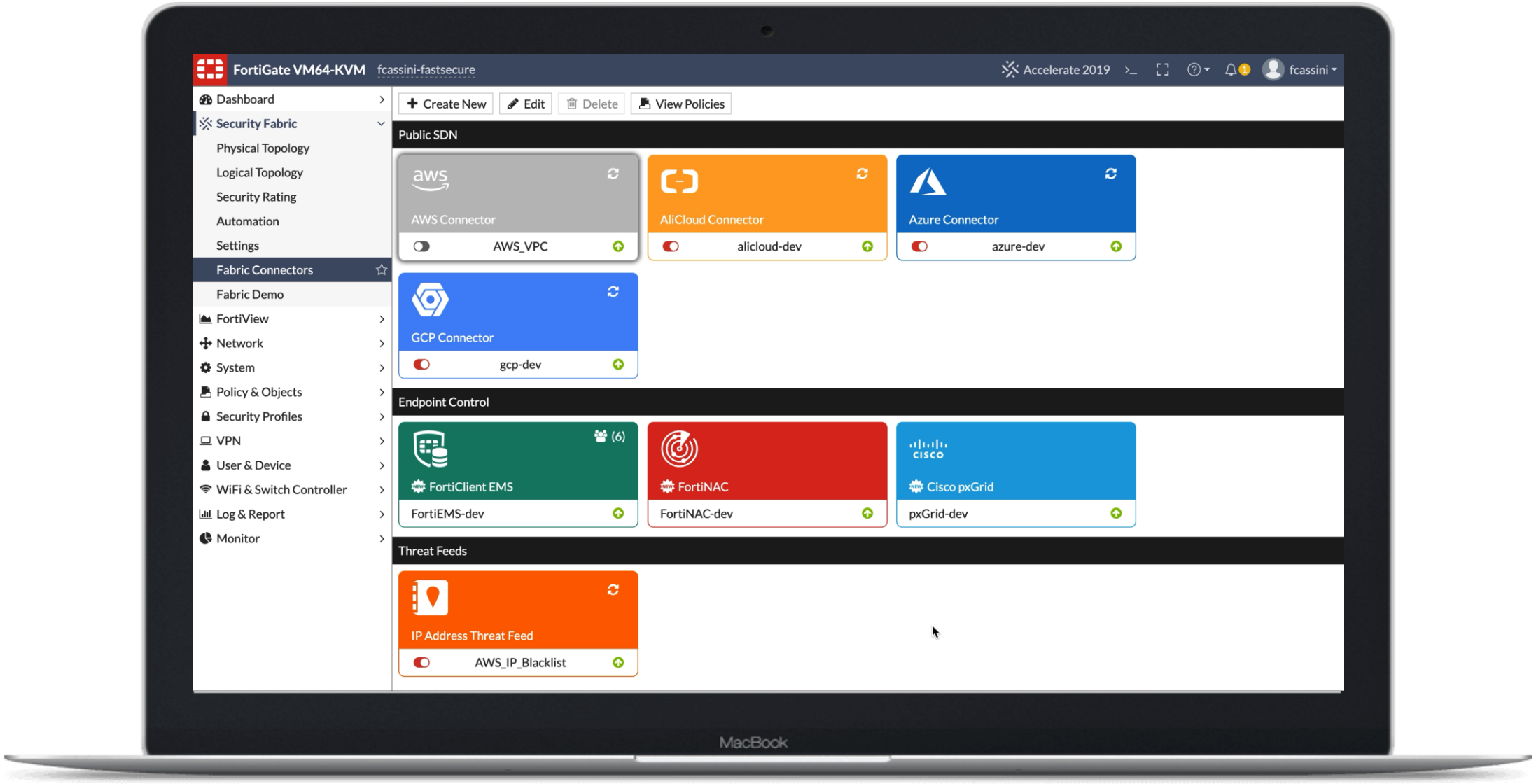
Fabric Connectors

Управление

Fabric Connectors

- Private SDN
- Public SDN
- IaaS Visibility
- Automation Action
- ITSM
- Threat Feeds
- SSO/Identity
- Endpoint CVE
- REST API

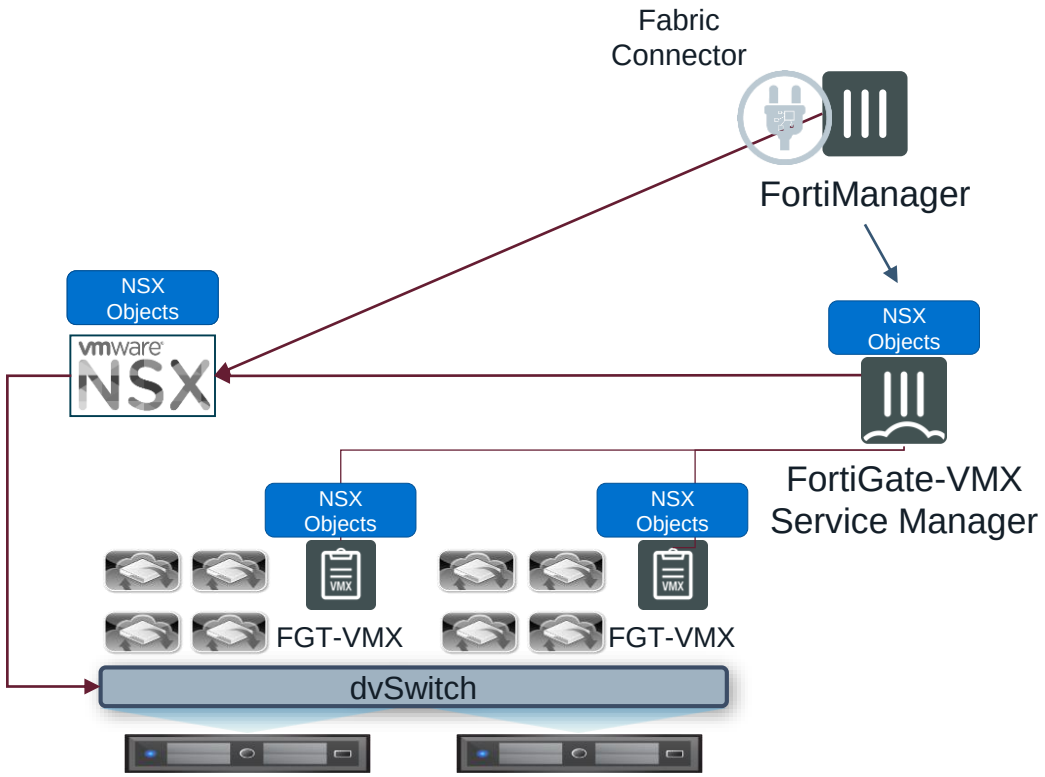
Автоматизация правил безопасности



Fabric Connector: VMware NSX

Private SDN

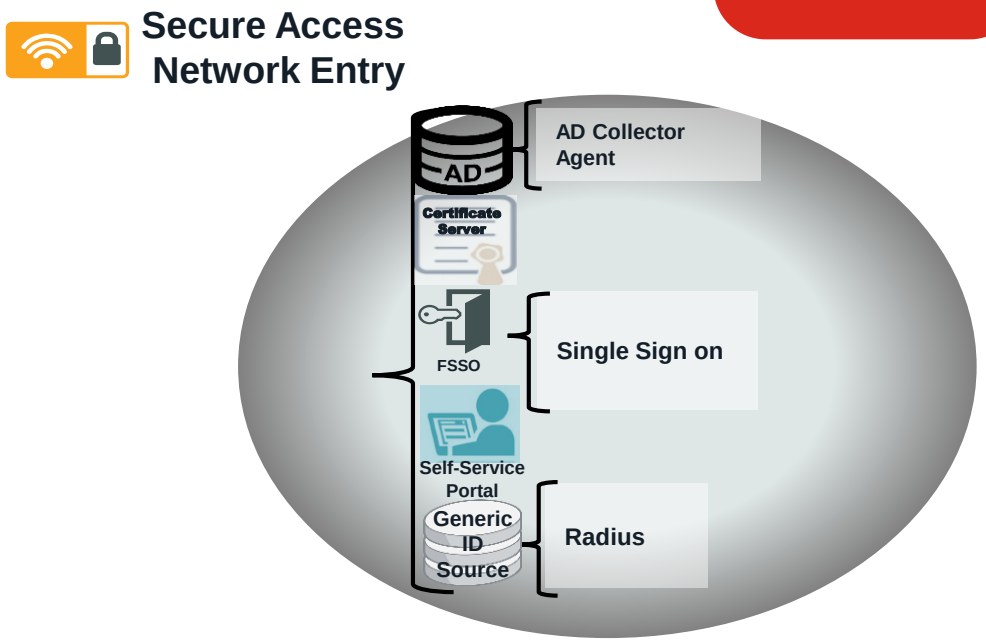
- Автоматизированное развертывание виртуальной машины и управление оркестровкой
- Динамические объекты (теги NSX) автоматически импортируются с помощью Fabric Connector без необходимости разбираться в сложных процессах управления
- Мониторинг, микросегментация и безопасность L4 - L7 для виртуального трафика East-West

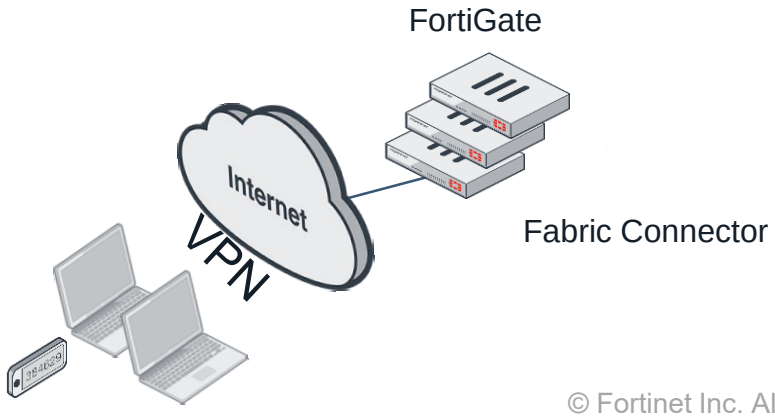


Fabric Connectors: Active Directory, Radius

SSO/Identity

- SSO в FortiGate проверяет подлинность пользователей в соответствии с правилом МЭ, не запрашивая имя пользователя и пароль
- Fabric Connector получает информацию с разных источников – систем централизованной аутентификации
- При этом автоматически применяются профили защиты, назначаемые каждому пользователю

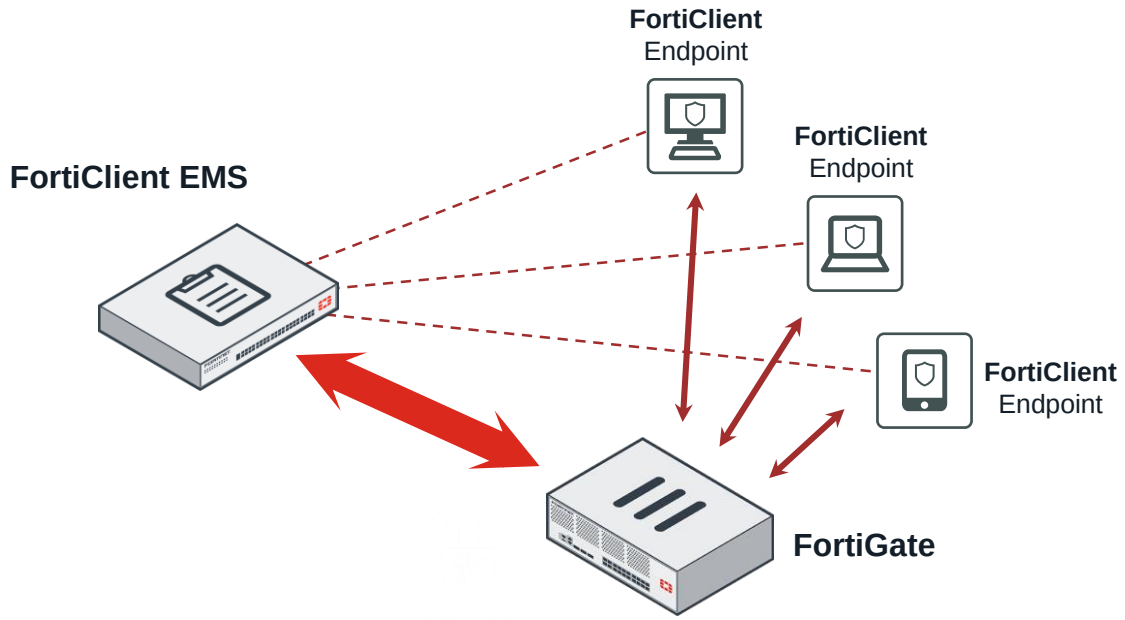




Fabric Connector: FortiClient Quarantine

Automation Action

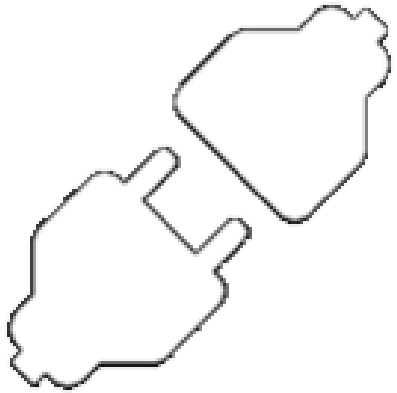
- Вызов Fabric Automation Action для помещения рабочей станции с FortiClient в карантин
- Когда FortiGate подозревает IOC, он запускает автоматический карантин скомпрометированных или зараженных конечных точек
- Рабочие станции в карантине отображаются в логической топологии фабрики безопасности



Fabric Connector: REST API

REST API

- REST API сторонних производителей для пользовательских сценариев использования
- Автоматизирует безопасность для пользовательских приложений и платформ
- Простота развертывания, снижение сложности, управление разными поставщиками средств защиты



Примеры использования клиентами:
- Threat Feeds
- Automation Action
- SSO/Identity
- Other

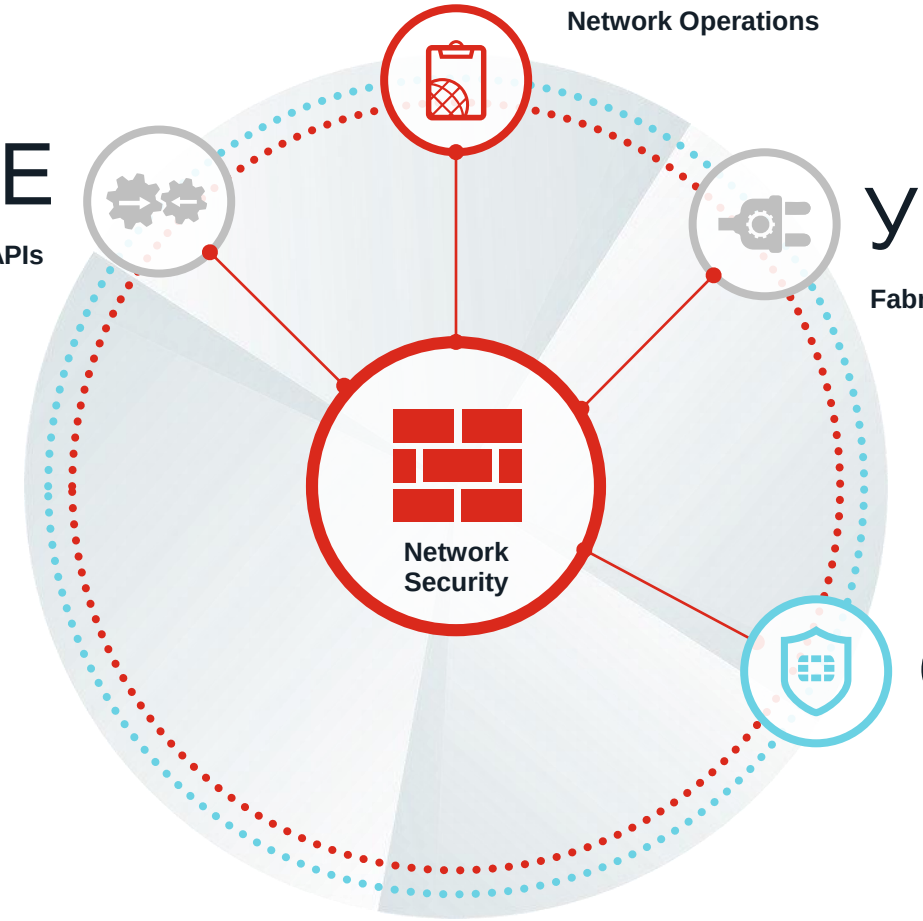
Автоматизация выполнена!

РАЗВЕРТЫВАНИЕ

Network Operations

РЕАГИРОВАНИЕ

Fabric APIs



УПРАВЛЕНИЕ

Fabric Connectors

ОБНАРУЖЕНИЕ

Security Operations


FORTINET