FORTINET SECURITY DAY

VIRTUAL

Платформенный подход к кибербезопасности

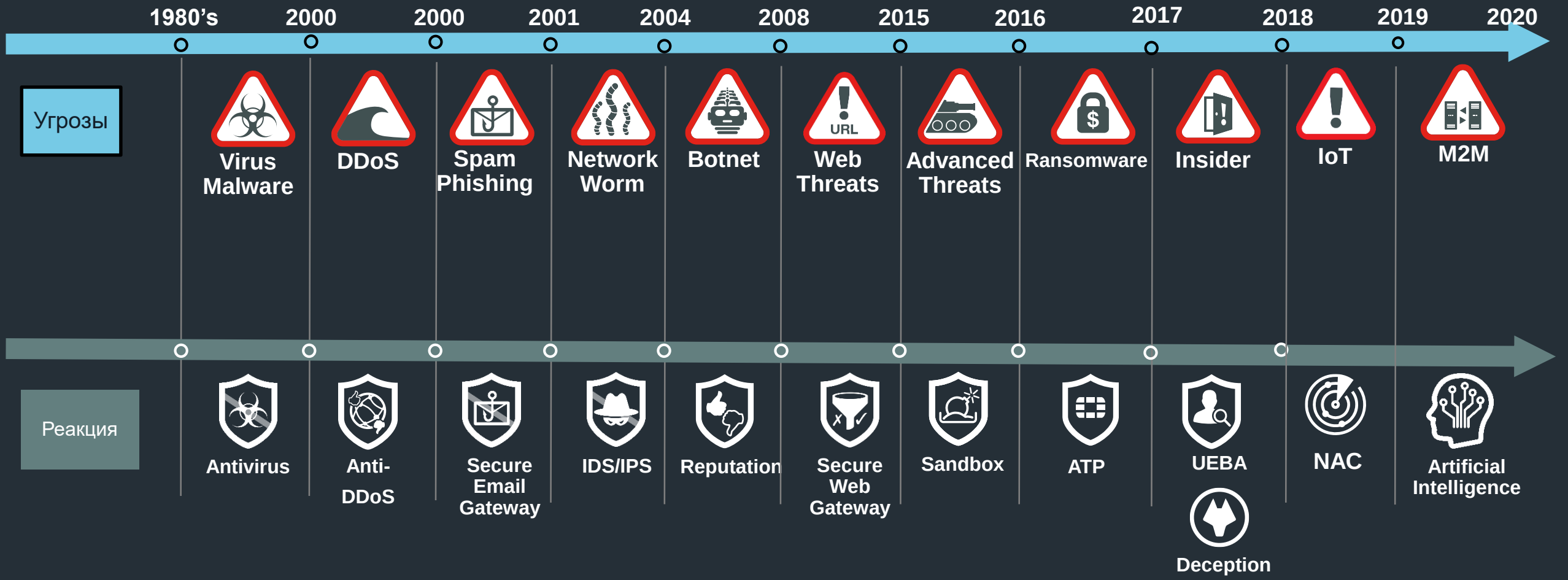
Алексей Андрияшин

aandriyashin@fortinet.com

Технический директор Fortinet в России и странах СНГ

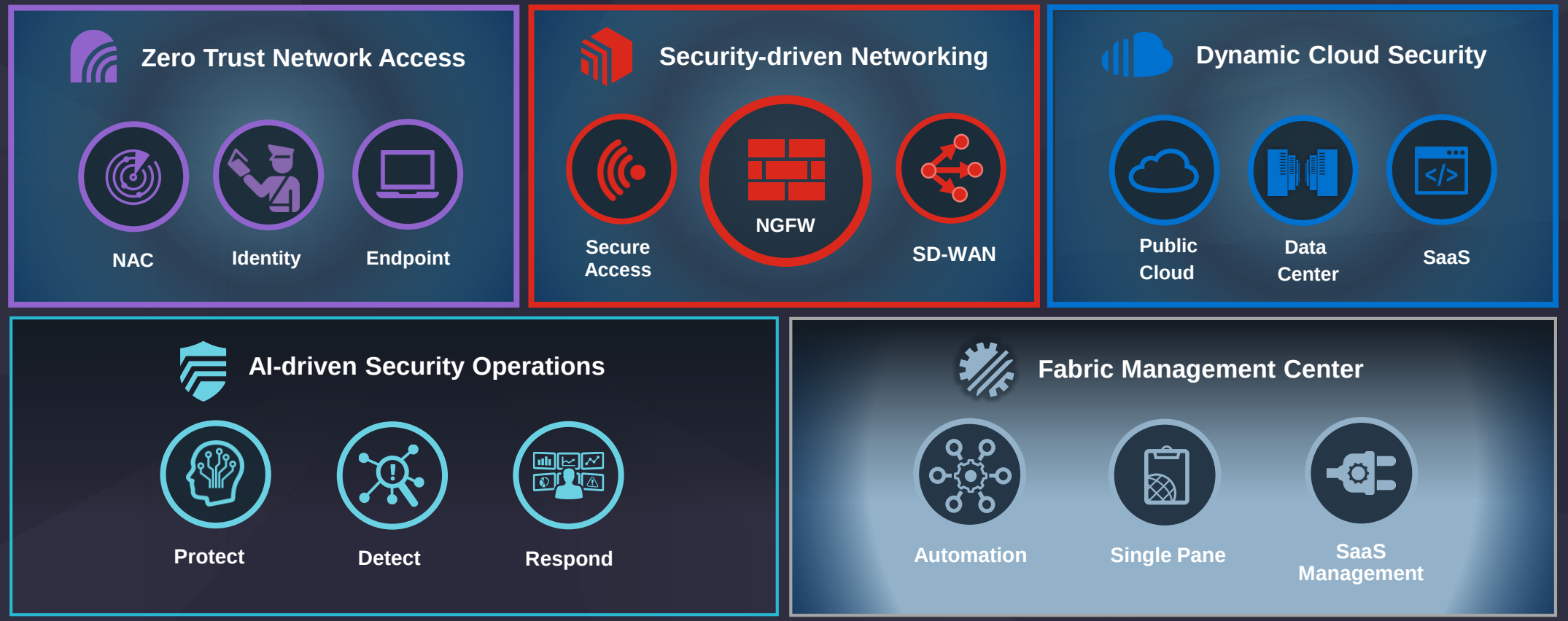
Эволюция угроз

Постоянное расширение поверхности атак




IP Reputation
Machine Learning
Threat Sharing
UEBA
Big Data
User & Device
Content Filter
IPS
Code Emulation
App Ctrl
Pattern Matching
Neural Networks
AntiVirus
Detonation
Sandbox
Primary
FORTINET SECURITY FABRIC
Logging
SIEM
Intent
Auth
Encryption
Threat Score
API
Integration
Automation
Adaptive
Behavior

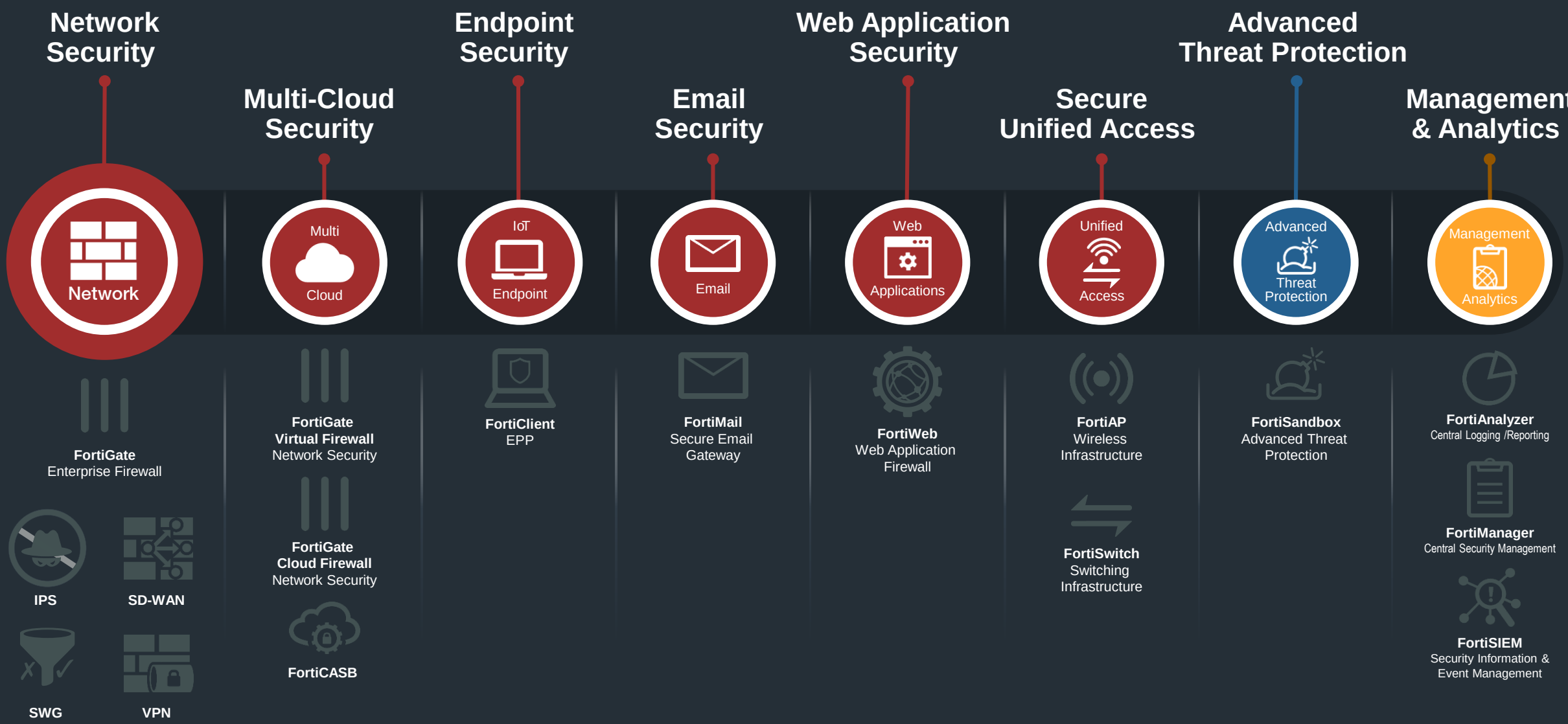
Платформа кибербезопаснсти Fortinet



Appliance | Virtual Machine | Hosted (SaaS) | Cloud | Software (Agent) | Container

FORTINET

Непрерывная цепь решений



Безопасность как основа сети

Базовые решения построения фундамента ИБ

FORTIOS

OS

FABRIC

USE CASES

CONNECTORS

API

AUTOMATION

FABRIC AGENT

CASB

ORCHESTRATION

FORTIGUARD

Security Rating

Threat Intelligence

Web Filtering

FortiSandbox Cloud

Intrusion Prevention

Antivirus

Application Control

IP Reputation

PARALLEL PROCESSING

SPU

NP6

CPU

CP9

Accelerates Network Traffic

Flexible Policy

Accelerates Content Inspection

SoC3

Optimized for entry-level form factors

More Performance

Less Latency

Less Power

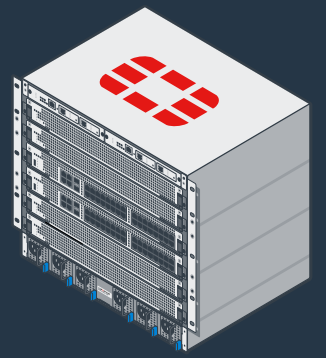
Less Space

FORTINET

Решения сетевой безопасности Fortinet

До 110Gbps SSL инспекции

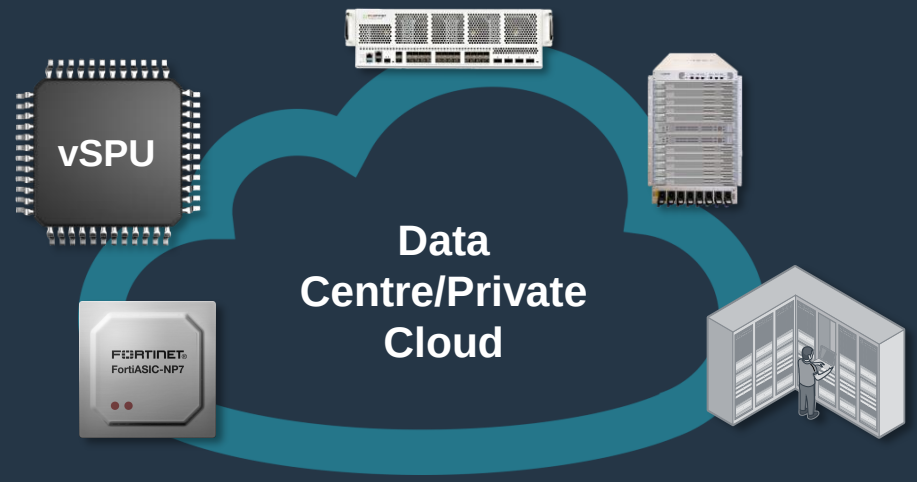
До 100Gbps предотвращения угроз

< 1G	1 - 5G	5 - 20G	10 - 100G	10 - 200G+	FortiGate VM*
FortiGate 30-90	FortiGate 100-900	FortiGate 1000-3000	FortiGate 6000	FortiGate 7000	
					
Entry-Level	Mid-Range	High-End 1	High-End 2	Chassis	Virtual Machine
SoC4	CPU NP6 CP9	N x CPU N x NP6 N x CP9	N x Processor Cards N x DP 3	N x Blades N x DP 3	

*Стороннее оборудование

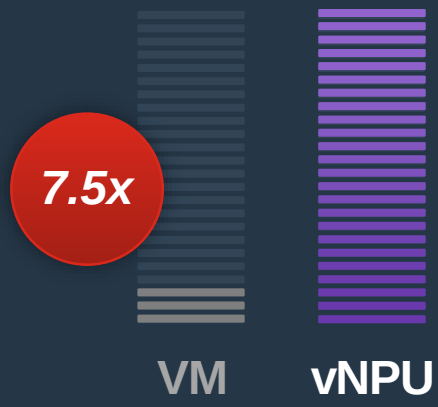
FortiGate-VM

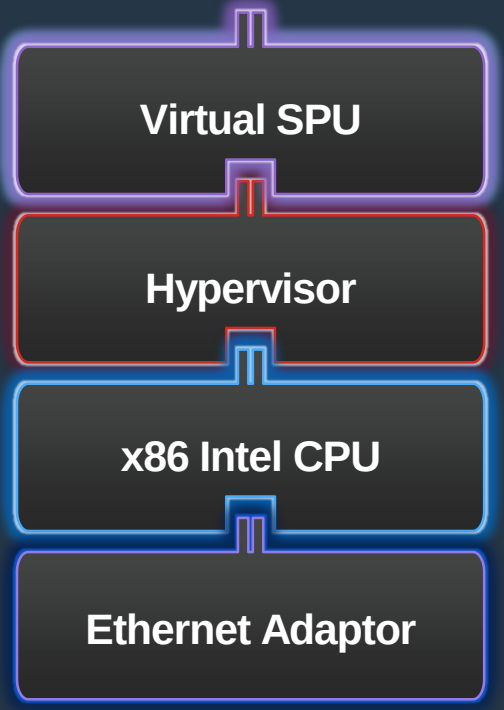
FortiGate VM



8.3 Gbps *@ 512 bytes*

60.4 Gbps *@ 512 bytes*



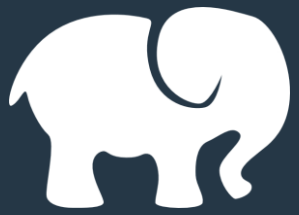


DPDK DATA PLANE DEVELOPMENT KIT | Intel® QuickAssist Technology | SR-IOV | PCI Pass through

Гипермасштабируемые приложения

Невозможно обеспечить защитой традиционными технологиями

Elephant Flows



Low Latency

Dynamic eCommerce

DDoS Protection

UHD TV

5G (CGNAT)

Core Segmentation (VXLAN)

Large VPN

Первый в мире…

…HyperScale ЧИП ускорения

Характеристики

- 28nm литография
- DDR4, PCI4.0/ 3.0
- ~422Млн транзисторов
- 2x 100G Ethernet
- 8x 25/10G Ethernet

FortiGate 4200F Производительность

Турбо ускорение NP7 в действии

Корпорации / ЦОД

45 Gbps
Threat Protection

52 Gbps
IPS

50 Gbps
SSL

210 Gbps
IPSec

Операторы

800 Gbps
Zero CPU Forwarding

7M CPS
Connections/sec (with Hyperscale License)

FortiGate 4200F Производительность

Турбо ускорение NP7 в действии

Копорации

45 Gbps Threat Protect
Excellent IPSec VPN
DDOS Protection in hardware
Elephant flows

Сервис-провайдеры

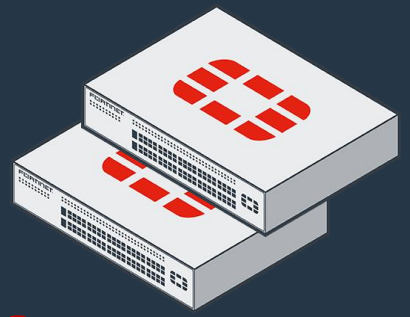
Hardware CGNAT & logging
Suite B Support
Fragment reassembly in hardware
GTP TEID Distribution

ЦОД

Ultra High Connections per second and hardware logging
Elephant Flow support
VXLAN and GRE Acceleration

Сетевая безопасность: NGFW

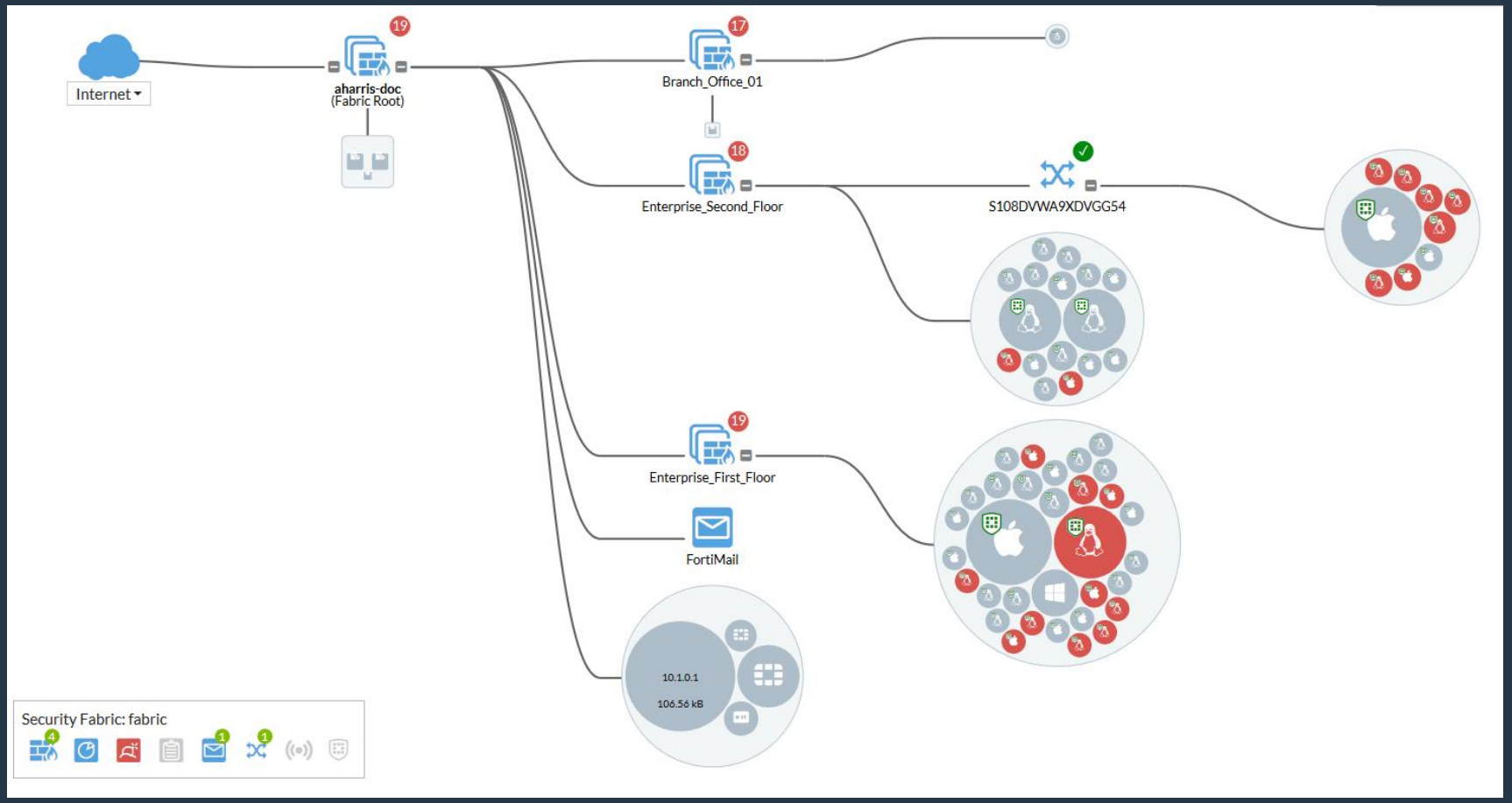
Сегментация FortiGate NGFW



FortiGate

FortiGtae предоставляет возможности межсетевого экрана нового поколения для средних и крупных предприятий, для развертывания в кампусе или филиале предприятия. Защита от киберугроз с помощью процессора безопасности, обеспечивающего высокую производительность, эффективность и глубокую видимость процессов

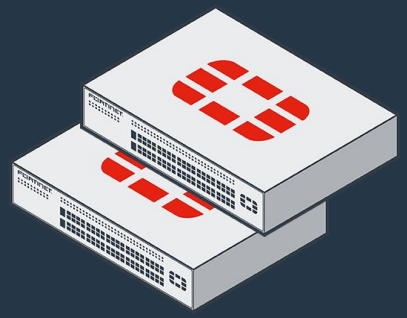
Security Fabric Топология



FortiGate NGFW с интеграцией SD-WAN

SD-WAN использует Интернет, что требует большей безопасности в каждом филиале

90% SD-WAN производителей предлагают только stateful FW



Secure SD-WAN

NGFW

SD-WAN

SD-WAN + Traffic Shaping + VPN (IPsec) + App Control + Intrusion Prevention + Antivirus + URL Filtering + Sandboxing + SSL Inspection (SSL)

SPU

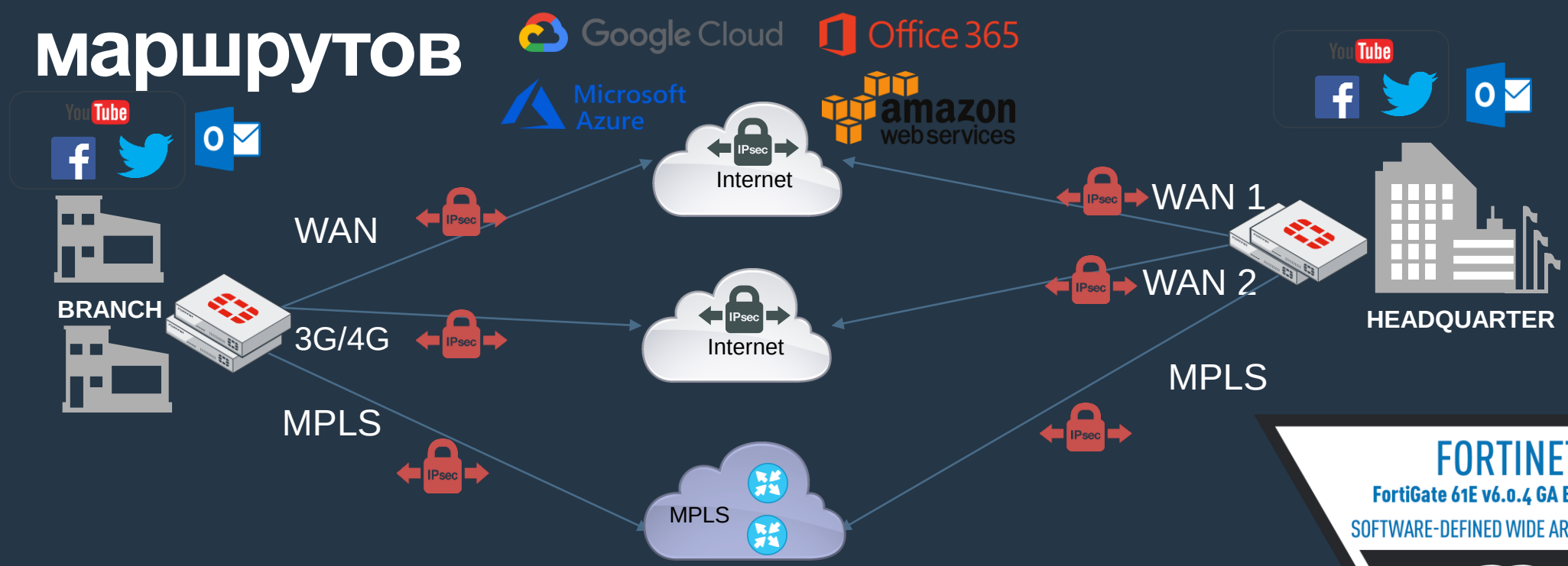
Масштабируемость и легкость развертывания

FORTINET SECURITY FABRIC

Беспрецедентная интеграция и видимость

FORTINET

SD-WAN интеллектуальный выбор маршрутов



FortiGate

SD-WAN

Операции на уровне приложений → **Множественные измерения контроля** → **Параметры отказоустойчивости**

Latency < 200ms
Latency < 100ms
AND
Packet Loss < 1%
AND
Jitter < 30ms

- ❑ Ping
- ❑ HTTP
- ❑ TCP Echo
- ❑ UDP Echo
- ❑ TWAMP

- ❑ Check Interval
- ❑ Failure before inactive
- ❑ Success before restore

FORTINET
FortiGate 61E v6.0.4 GA Build 0231
SOFTWARE-DEFINED WIDE AREA NETWORK
NSS LABS
RECOMMENDED
JUNE 2019

FORTINET

Инфраструктура: Защищенный доступ

Расширение защиты до уровня доступа

Простота

- Гибкая архитектура, масштабируемая по мере изменения потребностей
- Видимость управления и аналитика по проводной, беспроводной сети и безопасности

Защита

- Порты FW и коммутатора одинаково защищены, SSID напрямую привязаны к политикам FW
- Контролируется безопасность на уровне сетевых портов и WLAN

Низкая стоимость владения

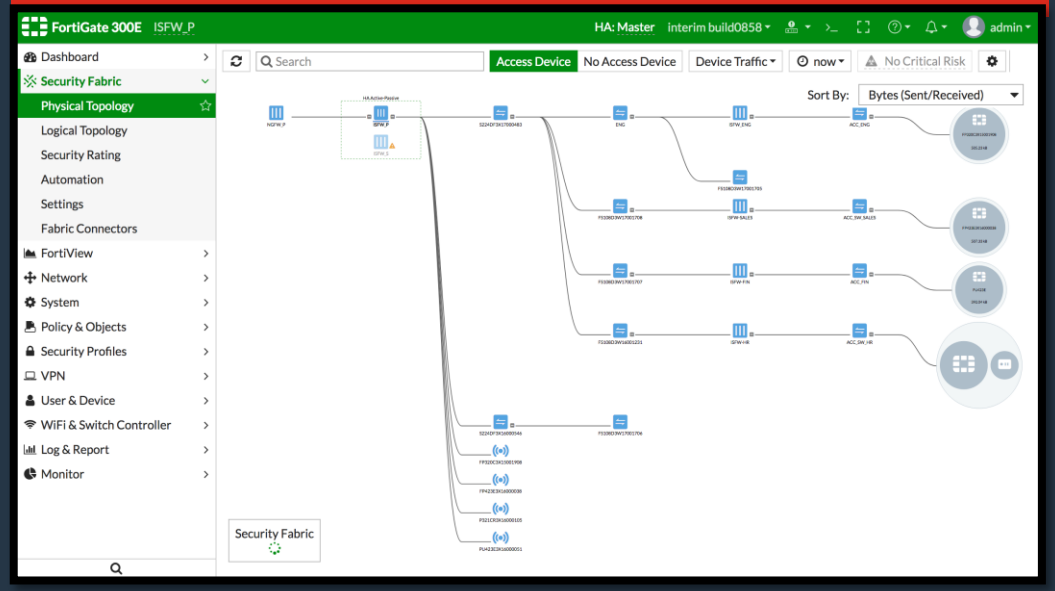
- Управление доступом в SD-Branch не требуют доп. лицензий

FORTINET

Инфраструктура: Защищенный доступ

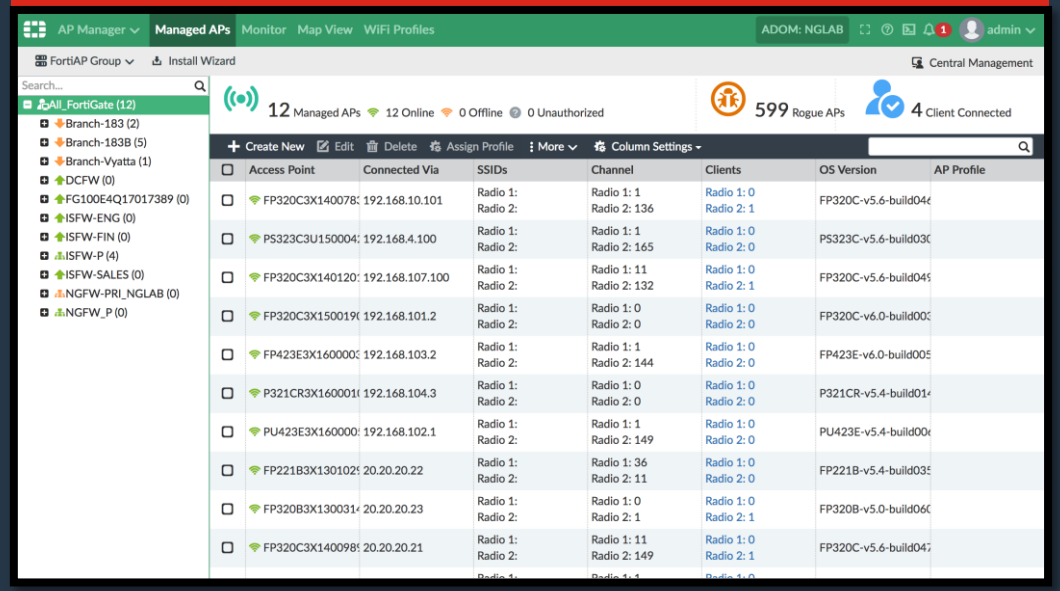
Расширение защиты до уровня доступа

FortiGate Interface



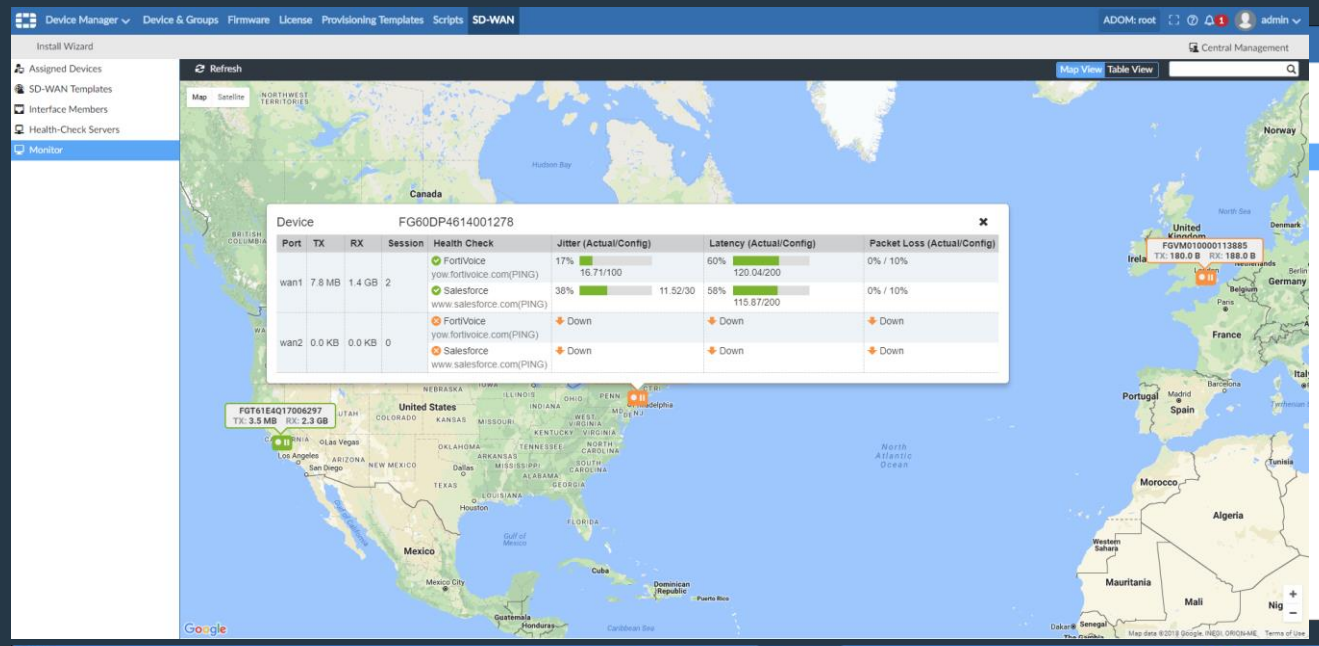
- Идеально подходит для небольших или одиночных развертываний
- Обеспечивает настройку и управление SD-WAN
- Управляйте безопасностью, доступом к сети и WAN из единого интерфейса

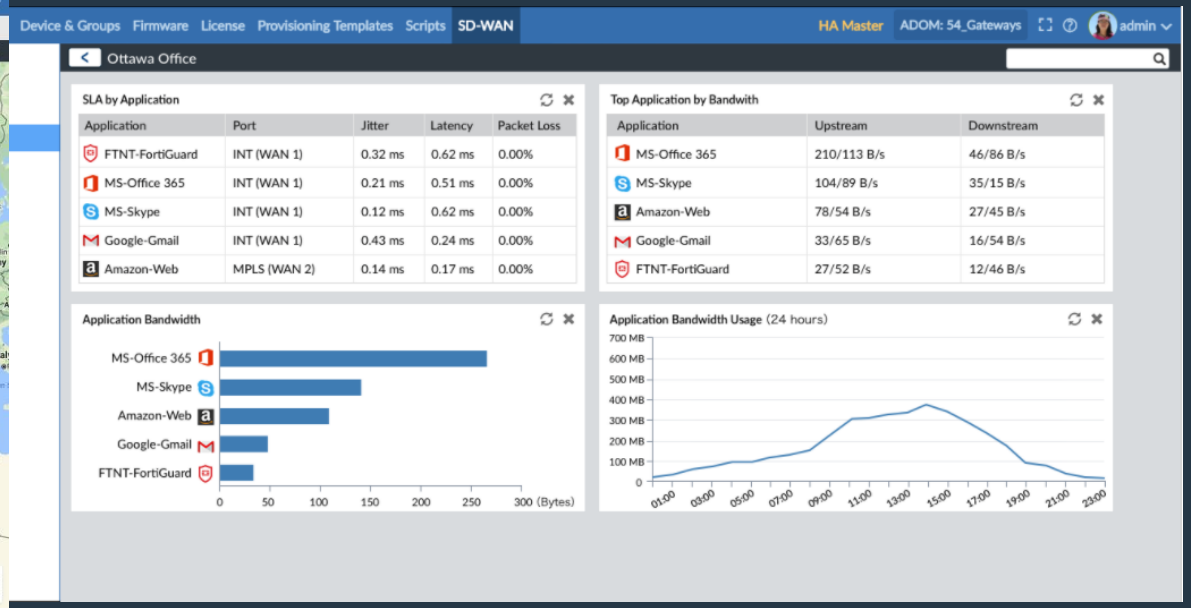
FortiManager



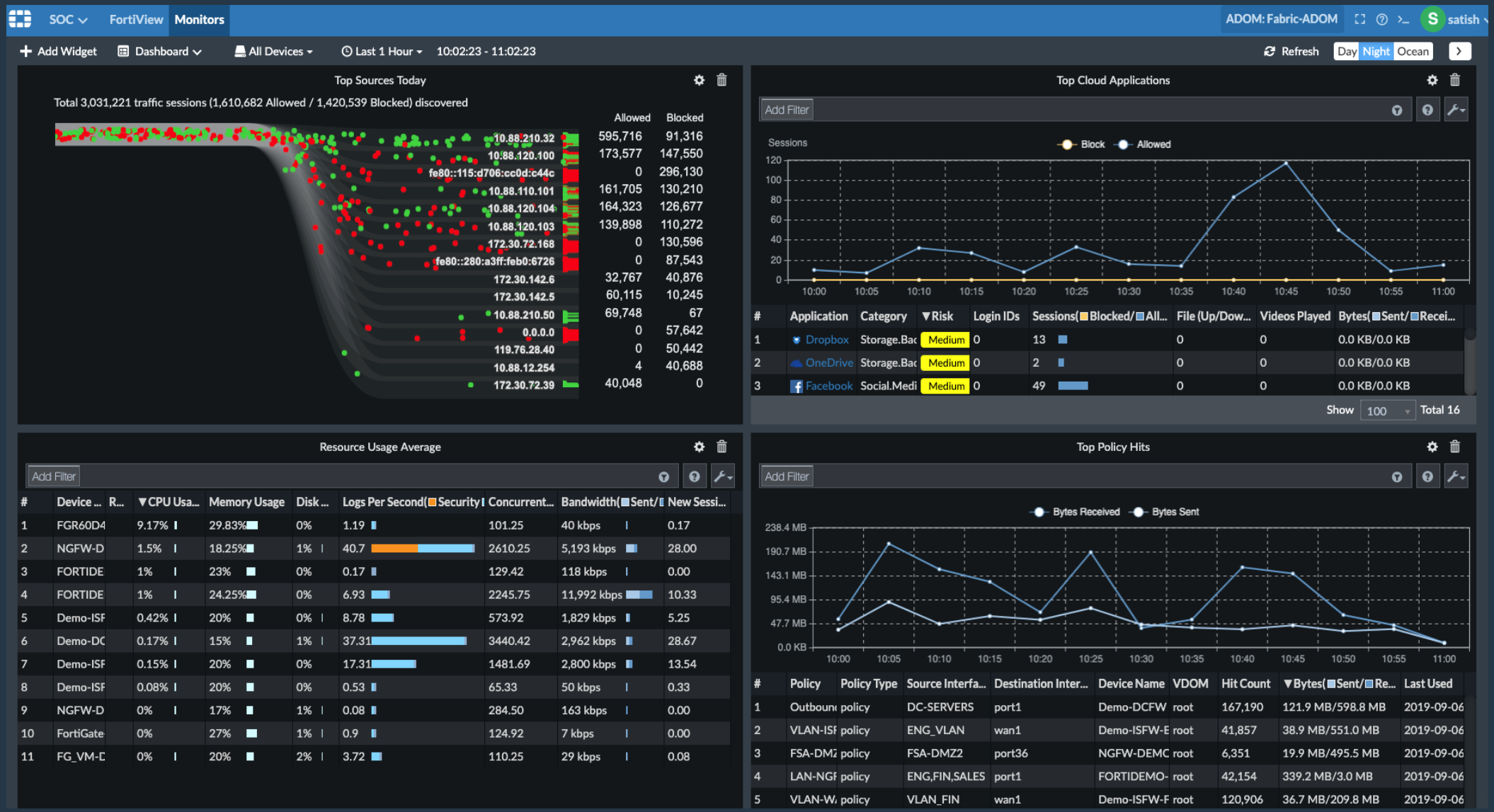
- Масштабируемое управление
- Обеспечивает настройку и управление SD-WAN
- Поддерживает оперативное развертывание Zero Touch
- Управление SD-WAN, безопасностью и доступом из единого интерфейса

FortiManager – централизованное управление и видимость





Мониторинг состояния сети



Крупнейшая в отрасли экосистема кибербезопасности

250+ Партнеров по экосистеме Security Fabric

Fabric Connector

» Глубокая интеграция, автоматизирующая операции и политики безопасности

Fabric API

» Разработанная партнерами интеграция с использованием API-интерфейсов Fabric, обеспечивающая сквозную совместимость

Fabric DevOps

» Скрипты DevOps, управляемые сообществом, автоматизирующие обеспечение сети и безопасность, настройку и оркестровку

Расширенная экосистема

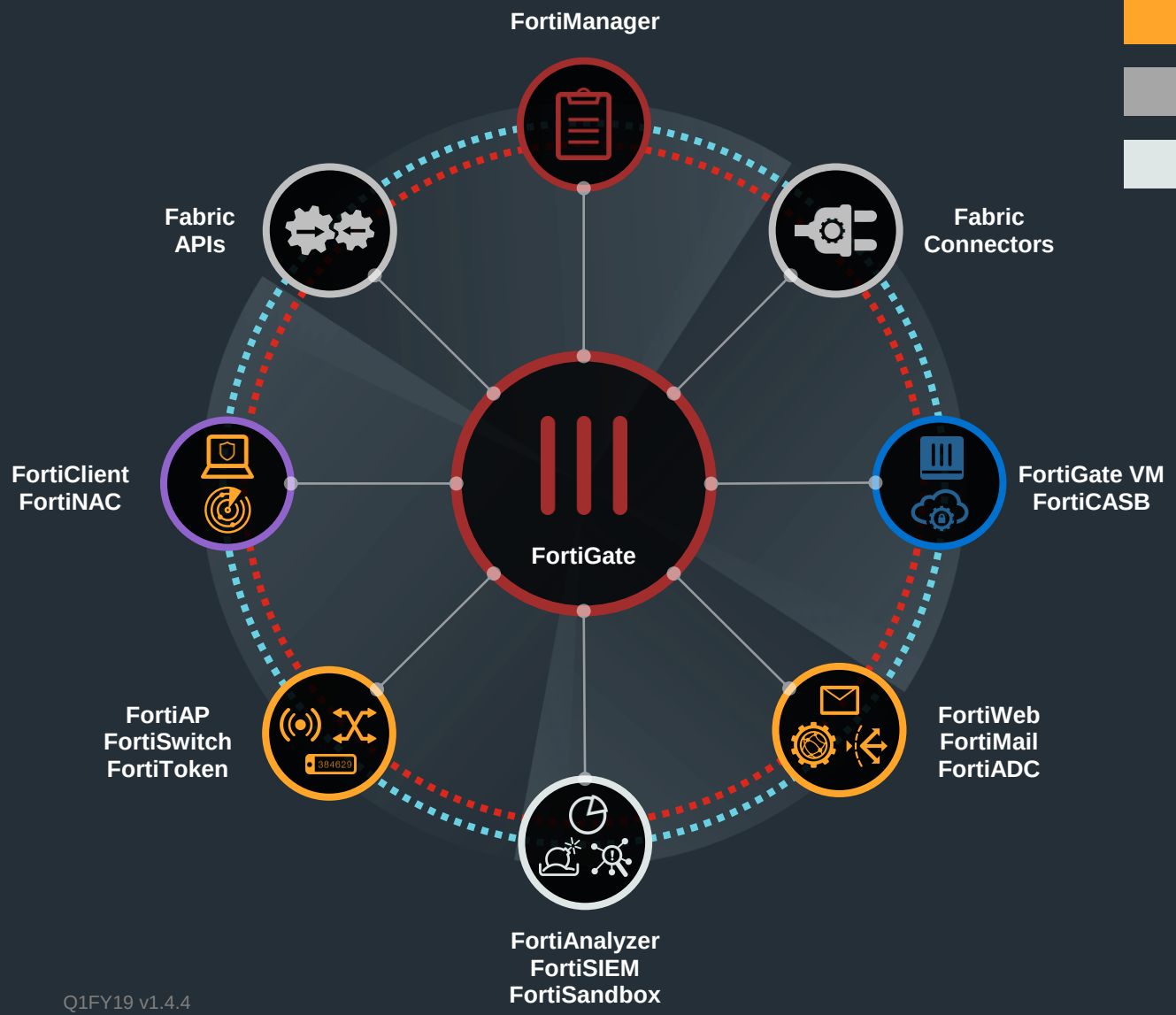
» Обмен информацией об угрозах с другими производителями и технологическими партнерами (TI), включая российских

Фабрика безопасности Fortinet

ШИРОТА
Визуализация всей площади атаки

ИНТЕГРАЦИЯ
AI- предотвращение угроз для устройств, сетей, приложений

АВТОМАТИЗАЦИЯ
Операции, управление и ответ




FORTINET