Построение адаптивных систем безопасности

Алексей Андрияшин

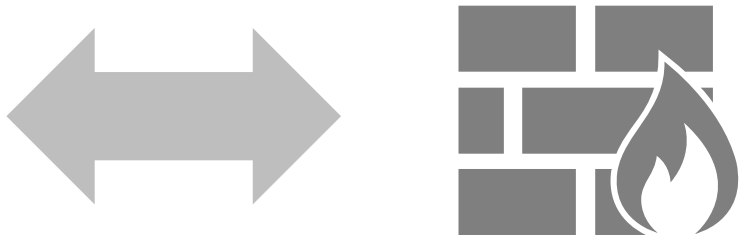
16 Ноября 2017

Безопасность требует нового подхода

Сетевая безопасность первого поколения

1995-2005 **Connection**

Stateful Firewall



SOFTWARE

Безопасность требует нового подхода

Сетевая безопасность второго поколения

2005-2015 **Content**

NGFW/UTM

SOFTWARE

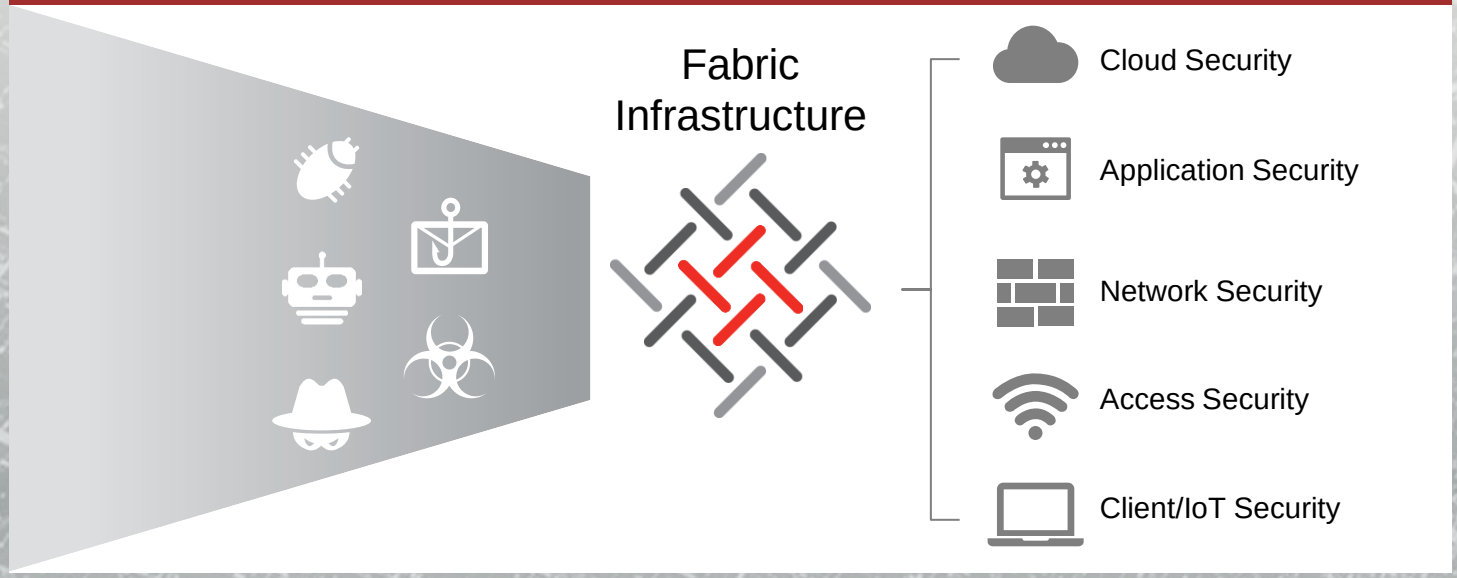
+

SECURITY PROCESSORS

Безопасность требует нового подхода

Сетевая безопасность третьего поколения

2015+ **Borderless**



SOFTWARE

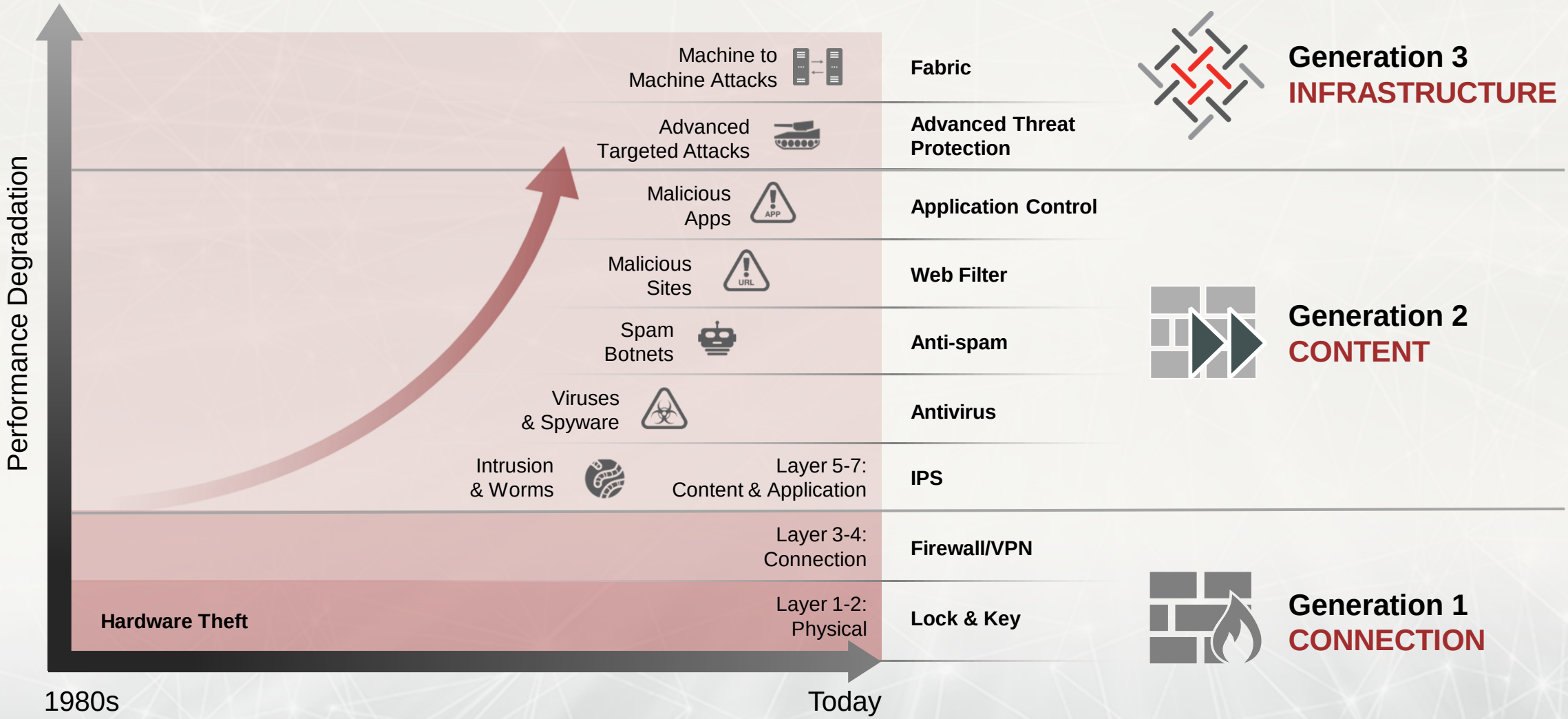
+

SECURITY PROCESSORS

+

FABRIC INFRASTRUCTURE

Угрозы стали более интеллектуальными



Современные тренды – Internet 2 в ближайшее время

Возросшее количество атак

65K инцидентов в отчёте только Verizon DBIR

SDN/NFV

Software-defined everything. SD WAN

Virtualization

80% приложений виртуализированы

Mobile

Не внедрён контроль устройств (BYOD)

SaaS

По статистике около 10 приложений компании размещены в облаке

SSL Traffic Growth

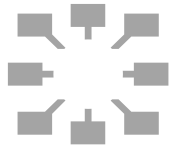
40% всего трафика зашифровано SSL

Social

Рост использования полосы пропускания

IoT

35B устройств подключено к сети



100G

Bandwidth

Wi-Fi достиг скоростей LAN. 100G сети уже построены. Рост бизнес трафика на 20% ежегодно.

Analytics

Big Data

Internet 2

100 Gbps и

UHDTV

5G

Wireless

БУДУЩЕЕ

Потребности в анализе SSL растут

SSL данных на данный момент

Более **40%**

Веб-браузинга в HTTPS (SSL)

Источник:
Google Web Performance Labs

Шифрованных вредоносных кодов

Более **50%**

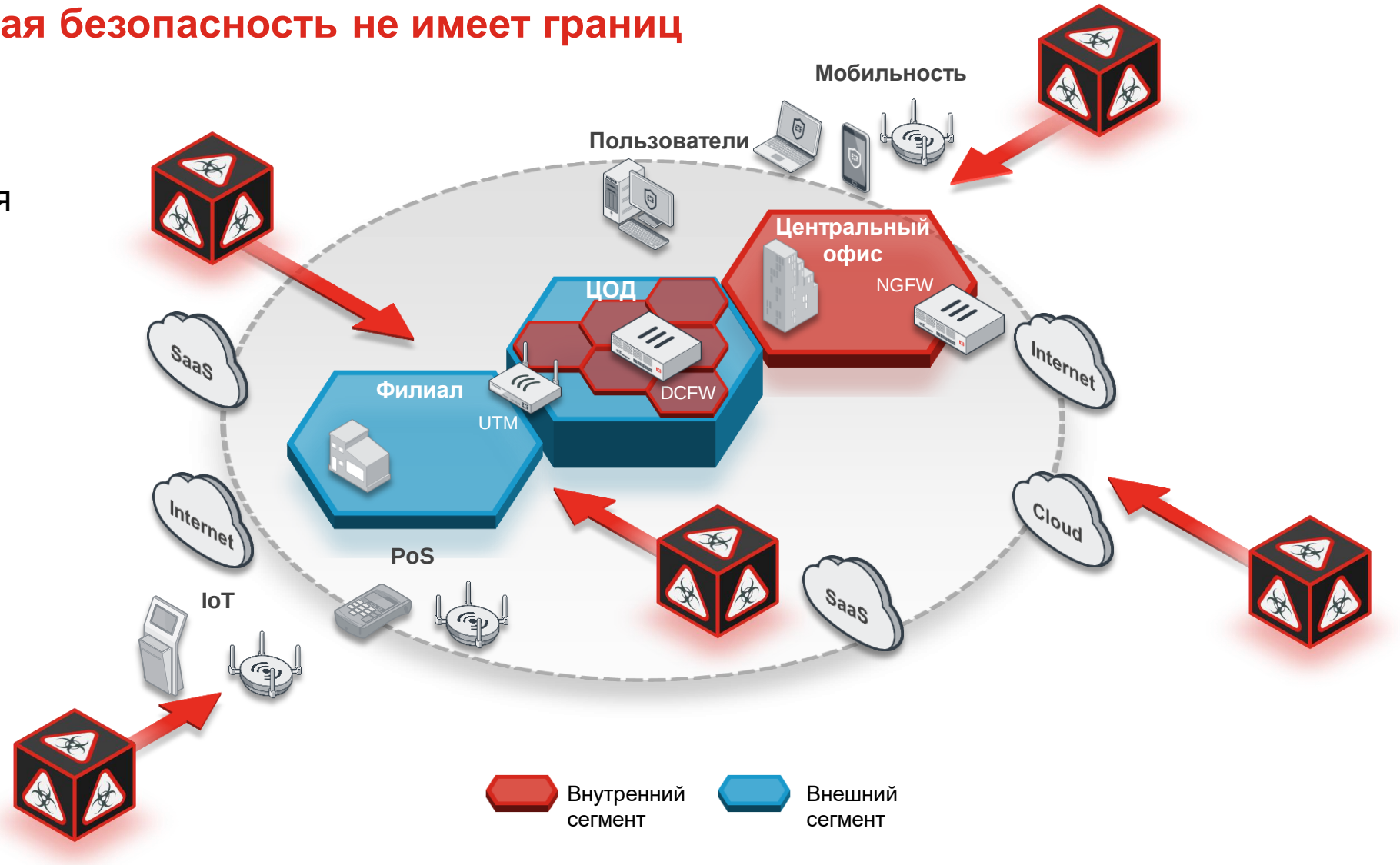
Количество атак с использованием шифрования прогнозируется в 2017*

Источник:
Gartner

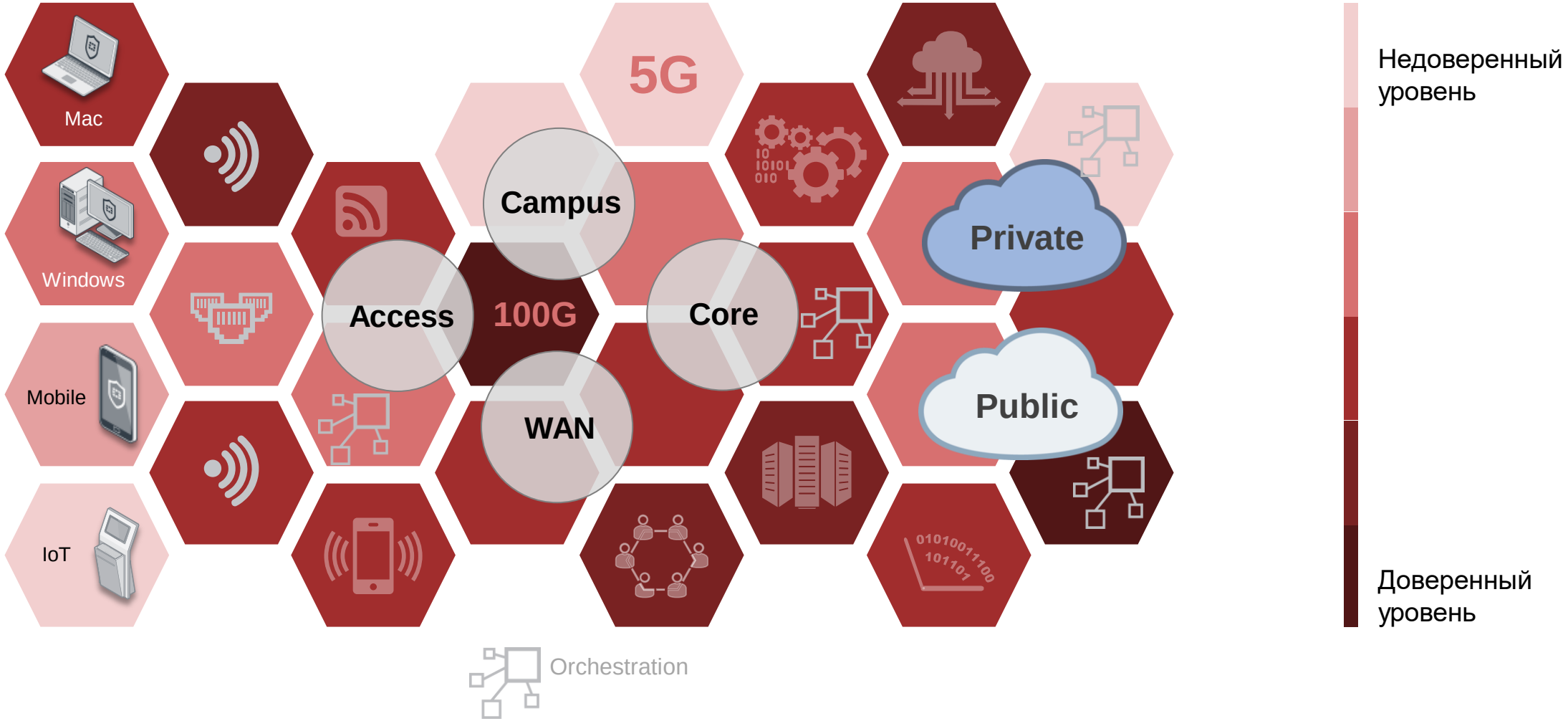
Возможностей для кибер-атак стало больше

Современная безопасность не имеет границ

- Сети
- Приложения
- Данные
- Люди



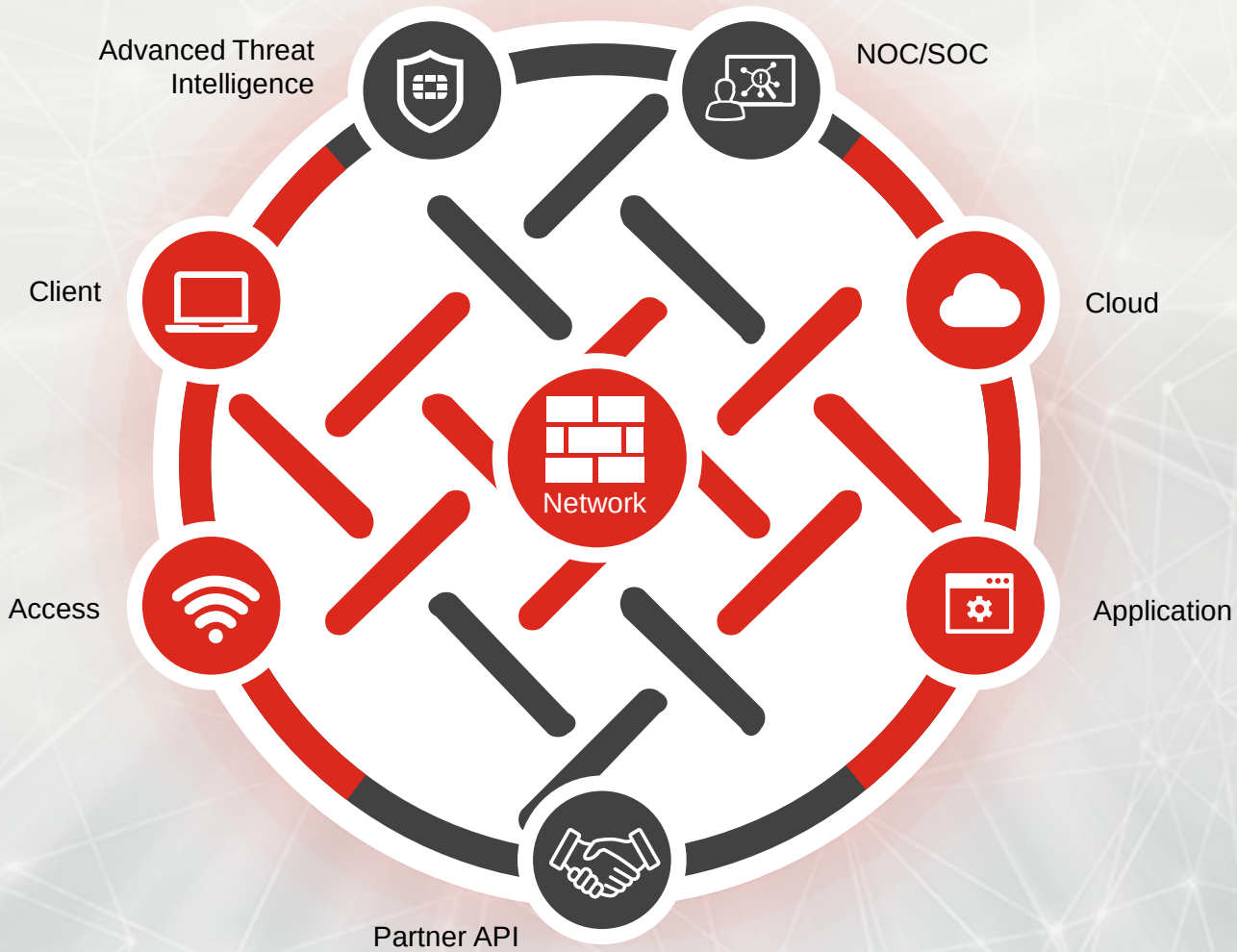
Современные сети не имеют границ – архитектура сетевой сегментации



ФАБРИКА БЕЗОПАСНОСТИ

Фабрика безопасности это концепция, которая обеспечивает безопасность без компромиссов, с ключевыми особенностями:

- ✓ **Безопасность**
- ✓ **Масштабируемость**
- ✓ **Осведомлённость**
- ✓ **Действия**
- ✓ **Открытая**
- ✓ **Всеобъемлющая**



Fortinet “Фабрика Безопасности”

Целый комплекс решений для обеспечения современной безопасности:

ENTERPRISE FIREWALL

FortiGate
- Next-Generation FW
- Data Center FW
- Internal Segmentation FW
- Distributed Enterprise FW

FortiWiFi
FortiManager
FortiAnalyzer
FortiSIEM

FortiCloud

CLOUD SECURITY

ForitGate VM (Virtual FW)
FortiGate VMX (SDN Virtual FW)
FortiGate VM for Public Cloud
- AWS
- Microsoft Azure
- OpenStack

ADVANCED THREAT PROTECTION

FortiSandbox
FortiMail
FortiWeb
FortiClient
FortiCloud Sandboxing

APPLICATION SECURITY

FortiMail
FortiWeb
FortiADC
FortiDDoS
FortiDB
FortiWAN

FortiCache

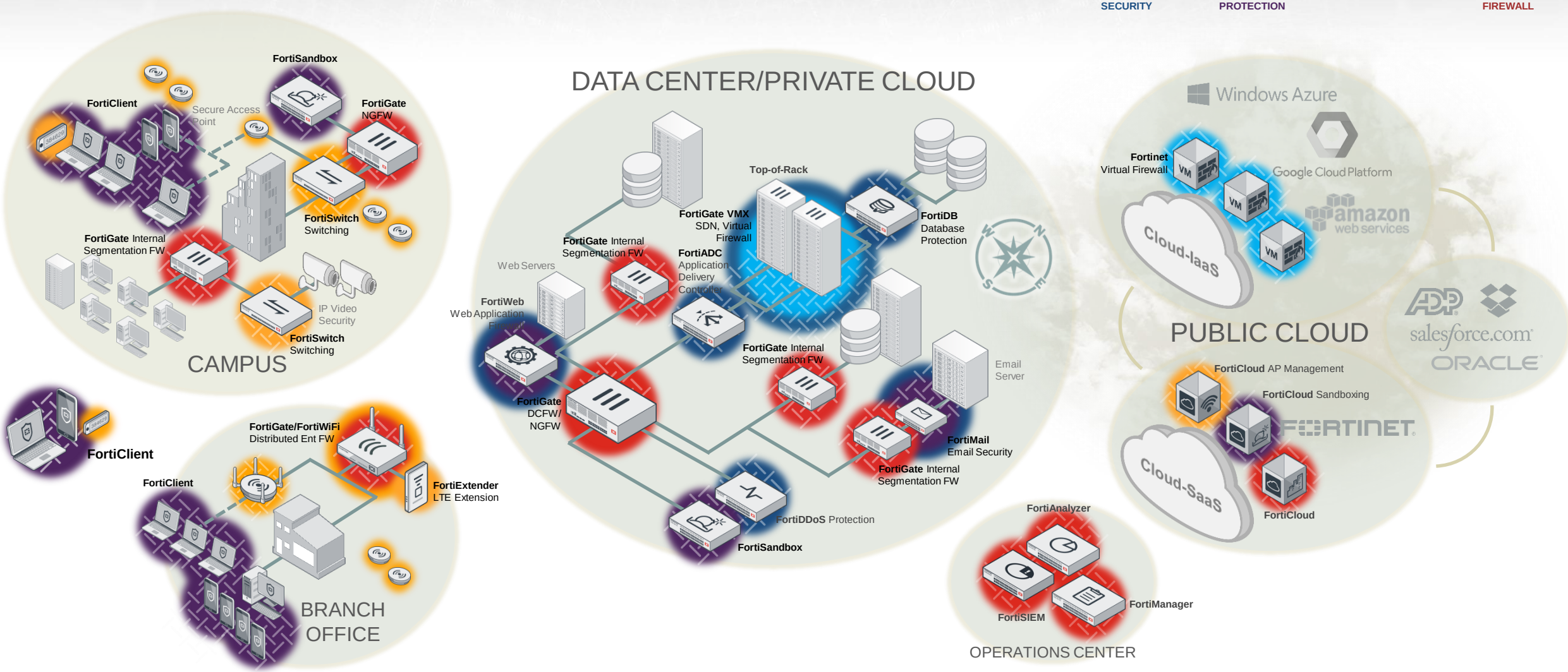
SECURE ACCESS

FortiAP
FortiWiFi
FortiCloud AP Management
FortiSwitch
FortiAuthenticator
FortiToken

FortiExtender

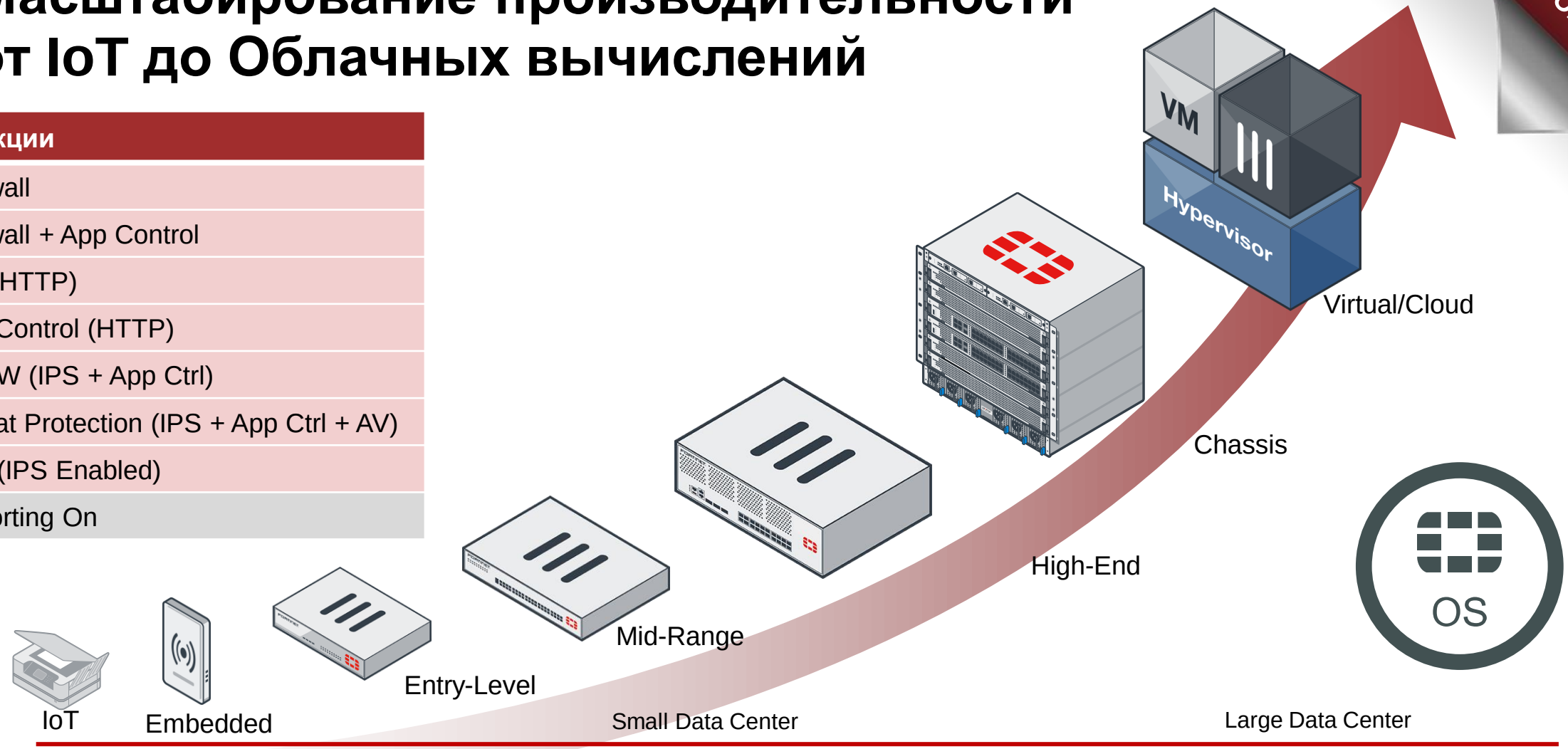
ФАБРИКА БЕЗОПАСНОСТИ

SECURE ACCESS | APPLICATION SECURITY | ADVANCED THREAT PROTECTION | CLOUD SECURITY | ENTERPRISE FIREWALL



Масштабирование производительности от IoT до Облачных вычислений

Функции
Firewall
Firewall + App Control
IPS (HTTP)
App Control (HTTP)
NGFW (IPS + App Ctrl)
Threat Protection (IPS + App Ctrl + AV)
SSL (IPS Enabled)
Reporting On



Сервисы команды FortiGuard

FortiOS Единая операционная система

FortiManager Единая консоль управления

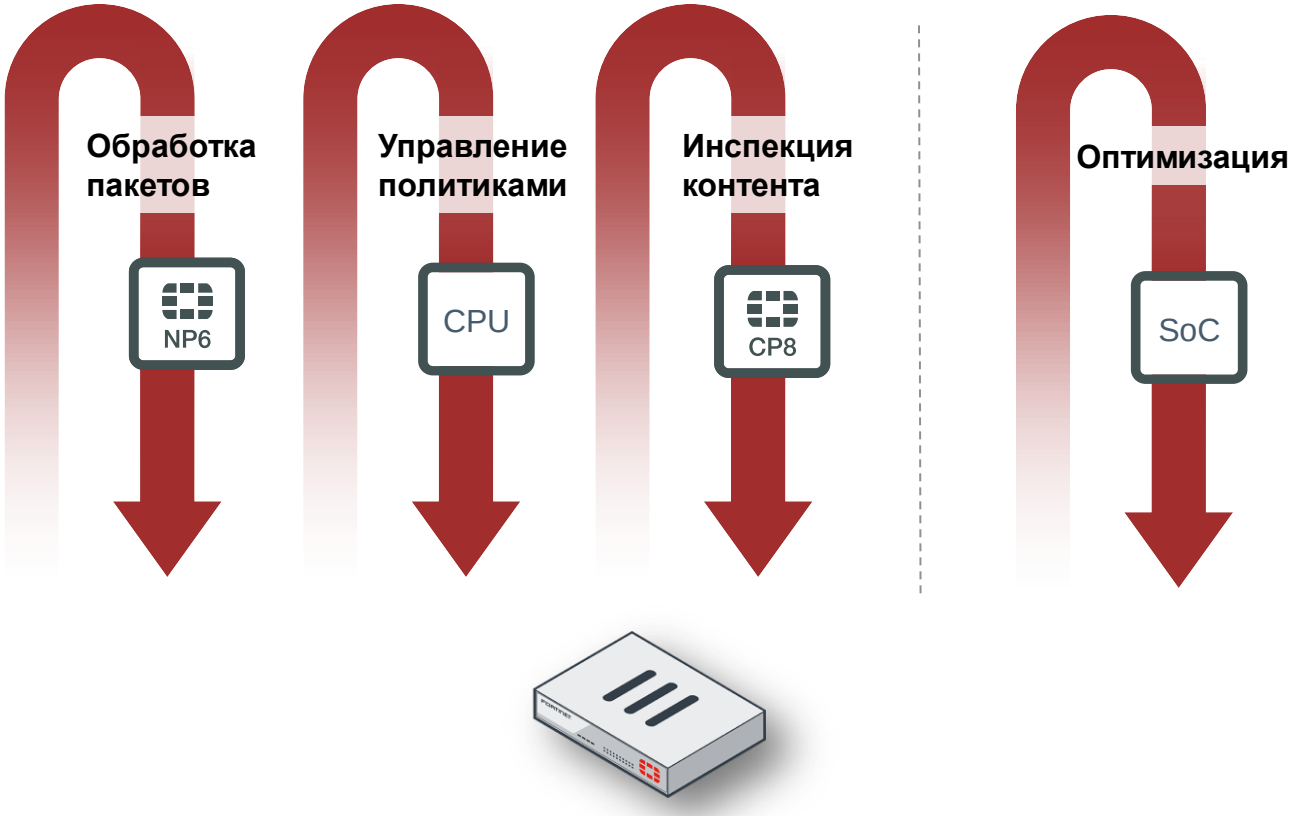
FortiCare and 360° Сервисы поддержки TAC

МОЩНОСТЬ

Параллельная обработка пакетов

Только CPU

Параллельная обработка пакетов (PPP)

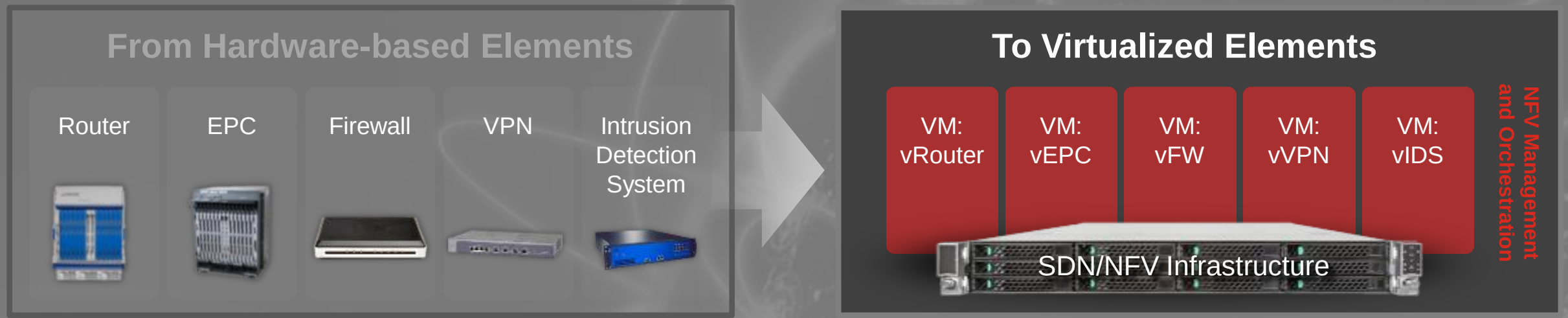


Увеличение производительности

Уменьшение задержки

Уменьшение энергопотребления

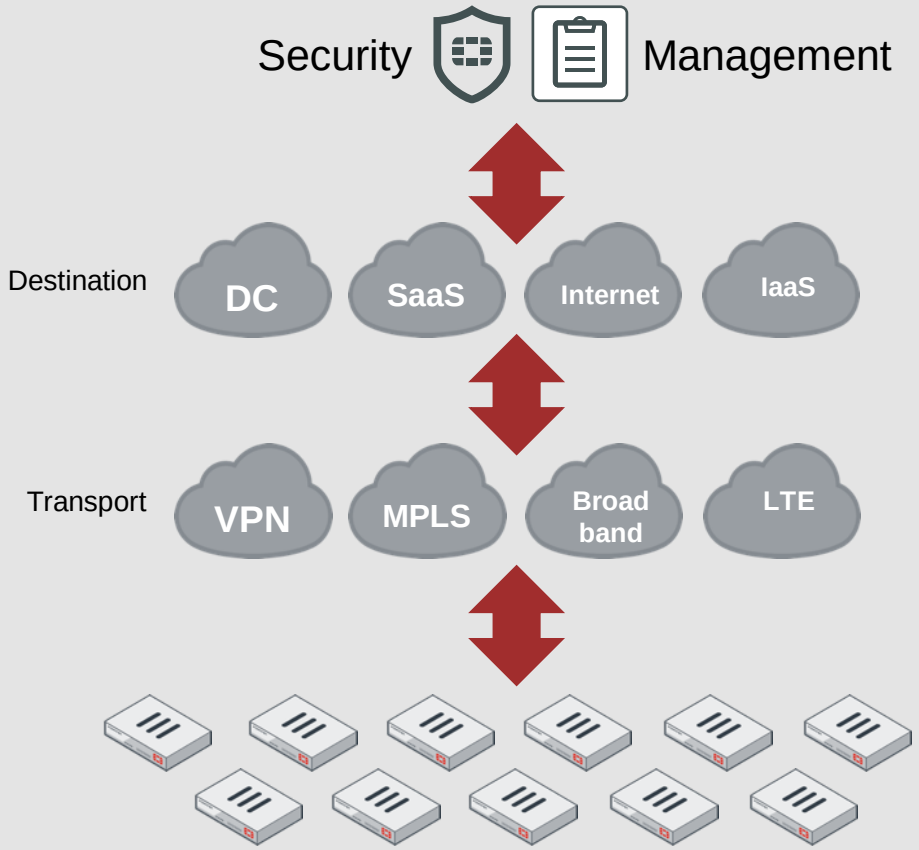
Виртуализация выходит на новый уровень



“WHITE BOX” СТАНОВИТСЯ НОВОЙ СЕРВЕРНОЙ ПЛАТФОРМОЙ

SD-WAN в FOS 5.6

Fortinet Press Release – April 4th



- Centralized Management
- Orchestration (Service Chaining)
- Zero-touch Deployment

SD WAN

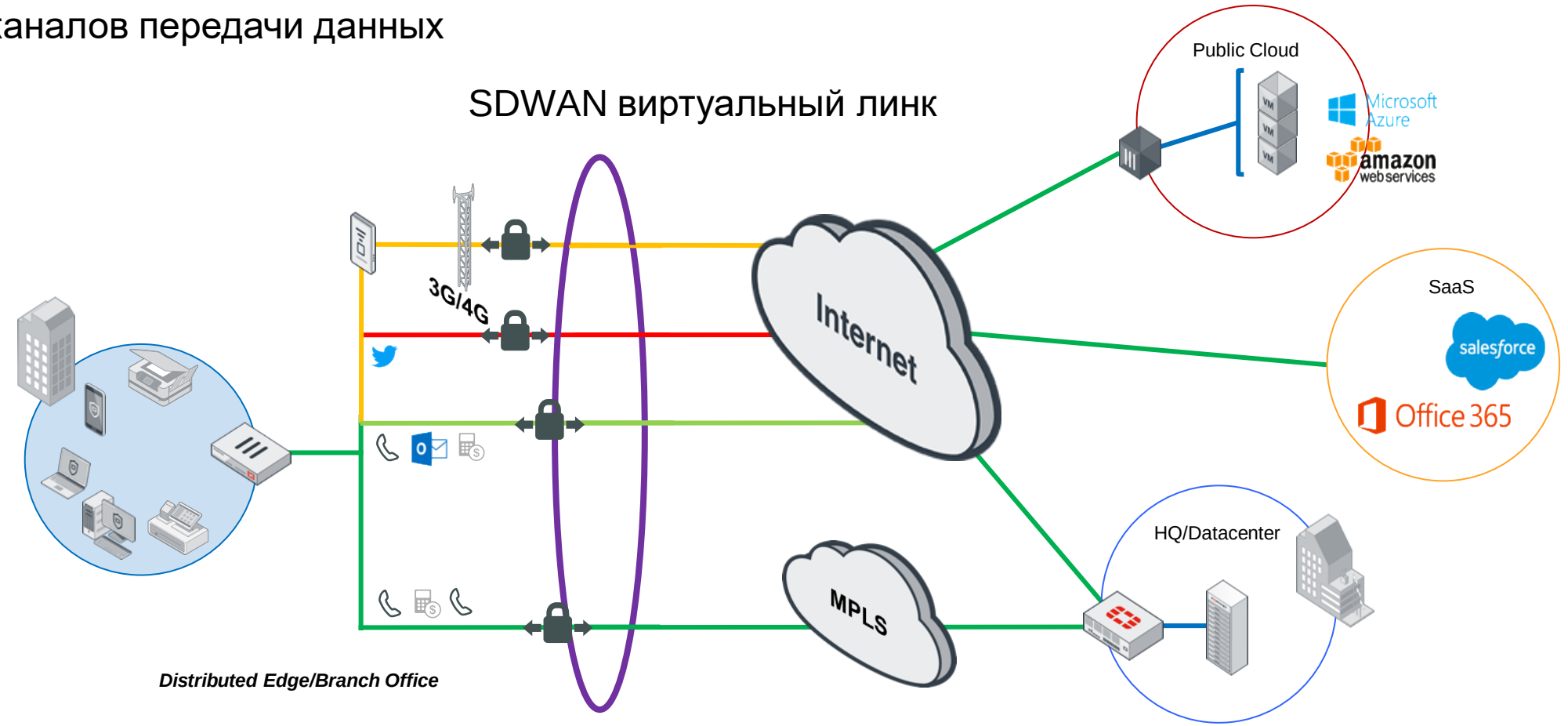
- Link Path Controller and Health Monitoring
- Dynamic SaaS Application Database
- IPSec VPN Tunneling
- Prioritized Business Applications (Traffic Shaping)

- Security Processor-powered Appliance
- Hybrid Appliance for vCPE
- Virtual Machine

SDWAN – Оценка качества каналов связи

- Маршрутизация на основе качества каналов связи
- Поддержка заданного уровня доступности приложений
- Учет стоимости каналов передачи данных

Latency = 25 ms
Jitter = 1 ms
Packet Loss = 0 %
BW = 200 Mbps

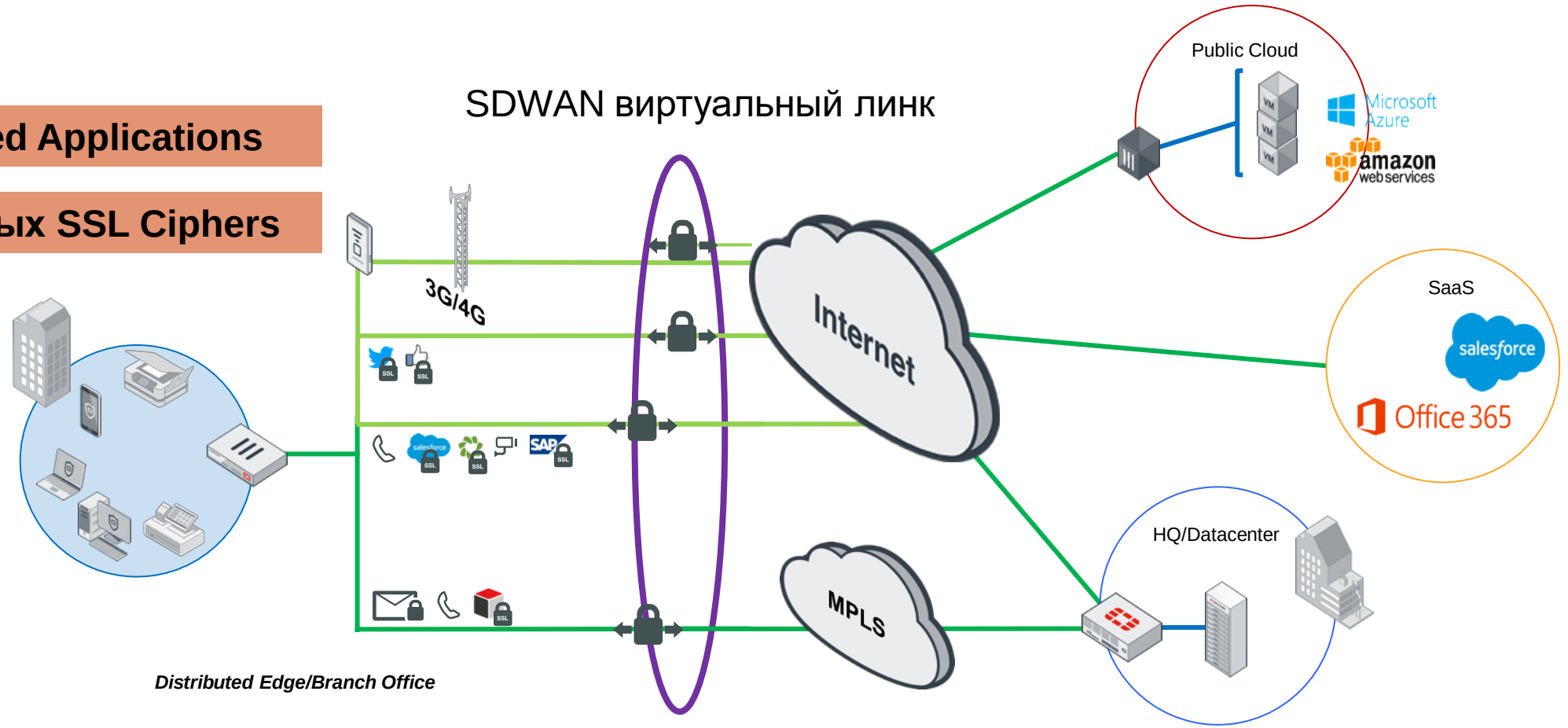


Детальный анализ трафика приложений

- Обеспечение работы бизнес-критичных приложений
- SSL-анализ трафика приджений

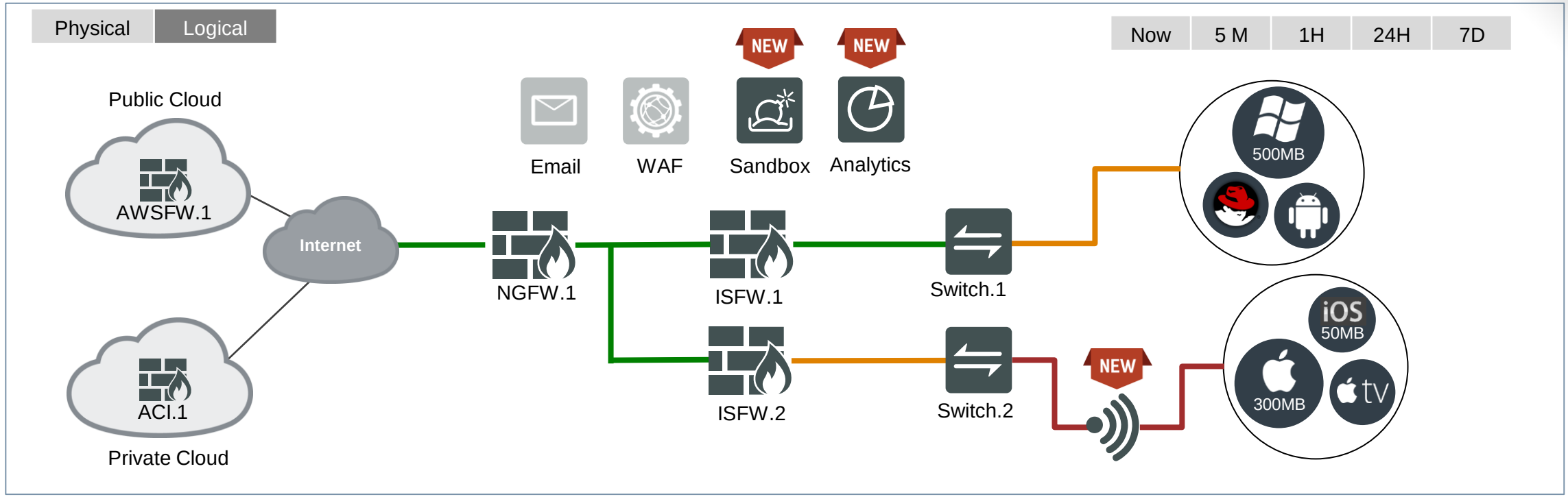
Более 3000 Supported Applications

Поддержка различных SSL Ciphers



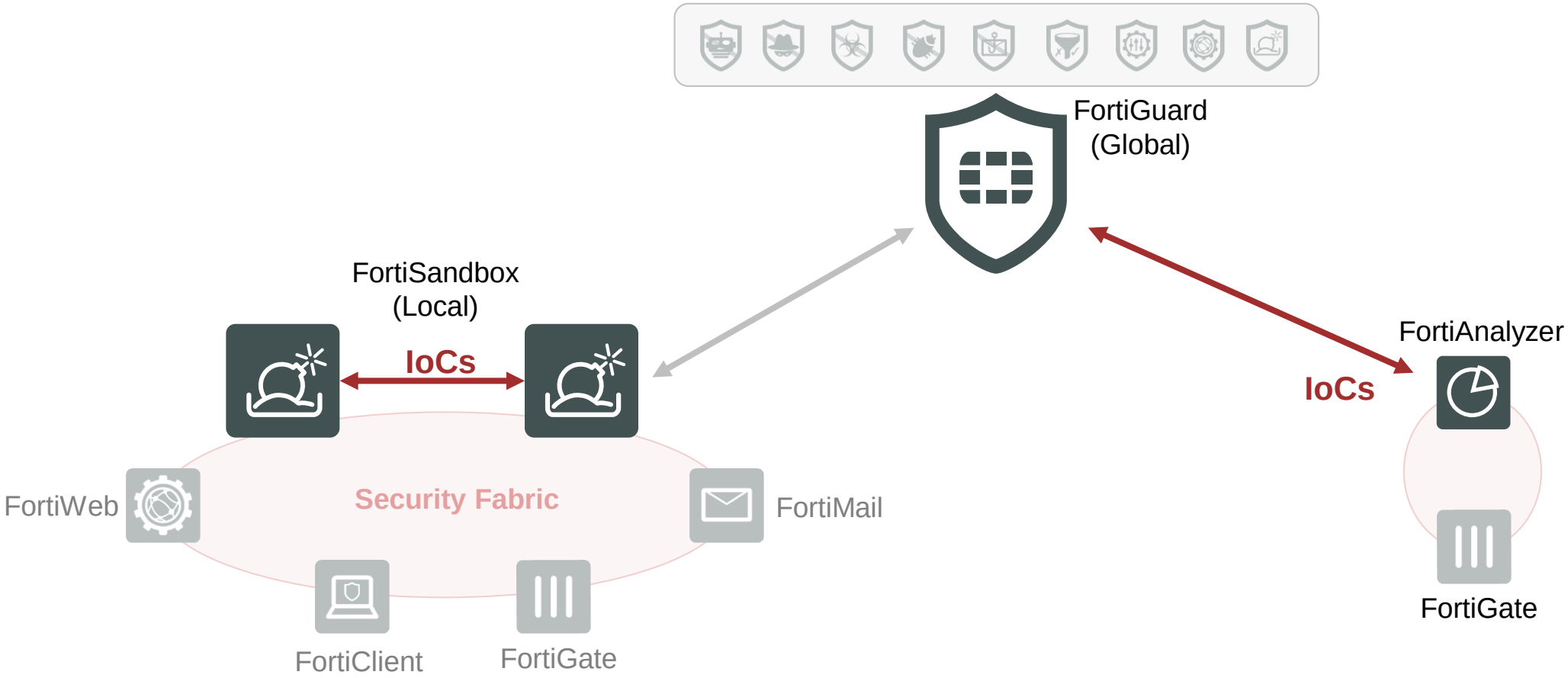
Большая Визуализация устройств безопасности упрощает задачу сегментации

ШИРОТА



Новые устройства и определение статуса	Новый механизм определения трендов
Новый инструмент визуализации FortiView	Новый механизм подавления атак и карантин

Быстрый доступ к анализу локальных и глобальных угроз



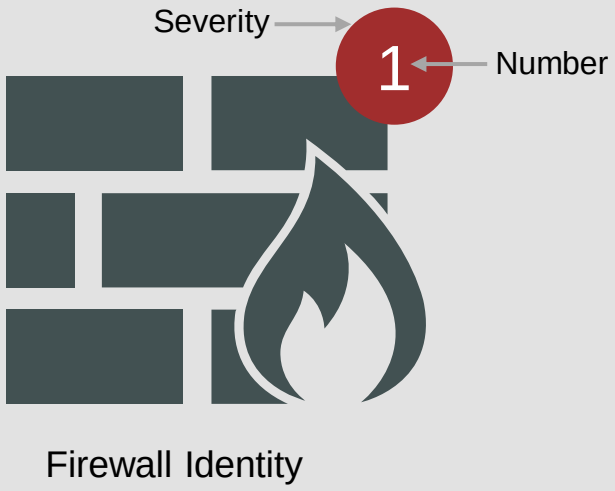
Кластерный анализ угроз распределенный по Фабрике безопасности обеспечивает высокую скорость реакции

Корреляция глобальных IoCs и сетевых журналов событий определяют новые угрозы

Аудит фабрики безопасности

АВТОМАТИЗАЦИЯ

Индикаторы визуального аудита



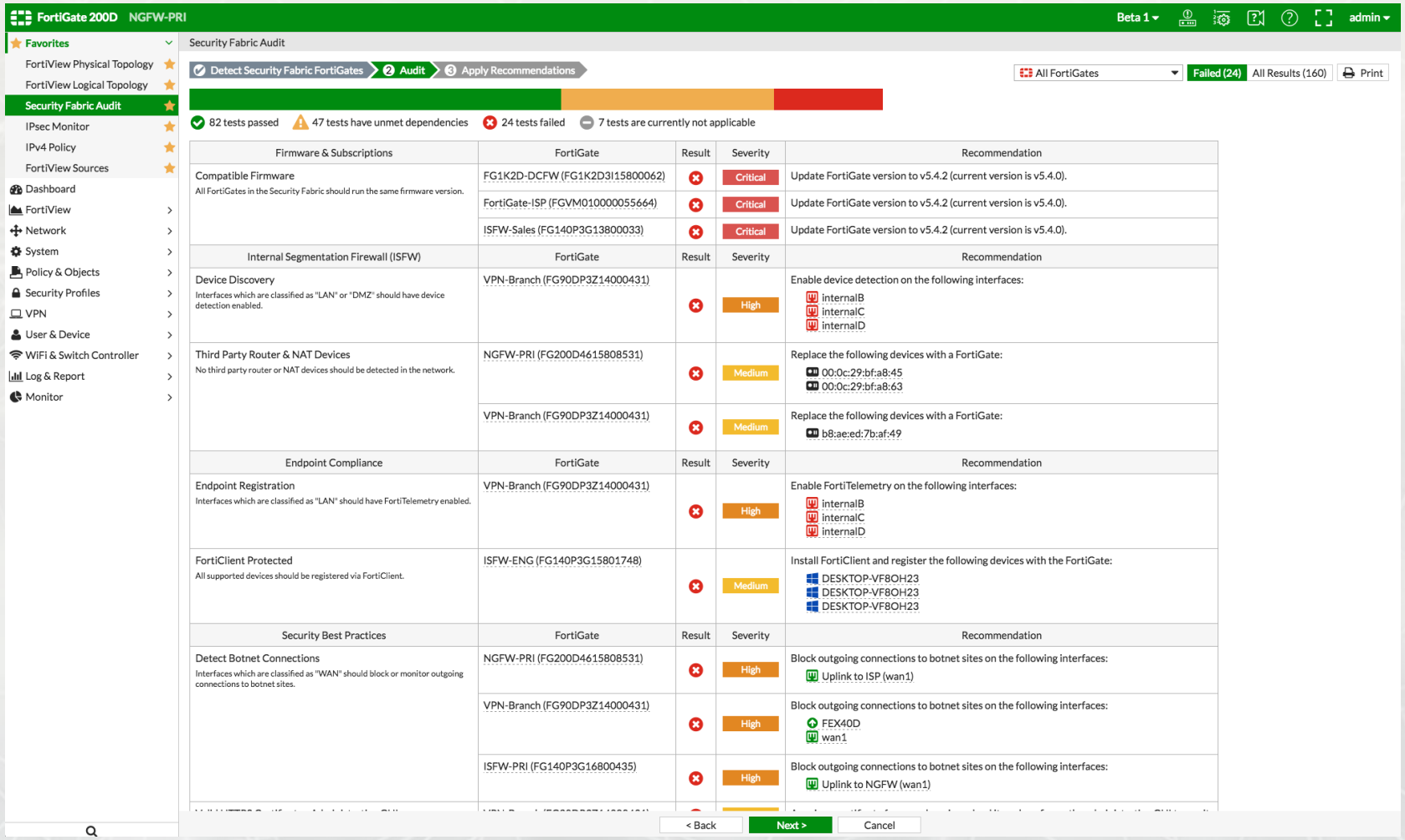
Запуск аудита
(Priority-based)

Priority	Element	Severity	No.
1.	ISFW.2	Critical	1
2.	ISFW.1	High	2
3.	NGFW.1	Low	6
4.	AWSFW.1	Low	1

Выполнение рекомендаций

- Лучшие практики
  - ✓ Административный доступ
  - ✓ Текущая прошивка и подписки
  - ✓ Оценка работы журналов событий …….
- Отчетность
- Шаблоны соответствия

Автоматизация Аудит и рекомендации



FORTINET SECURITY FABRIC

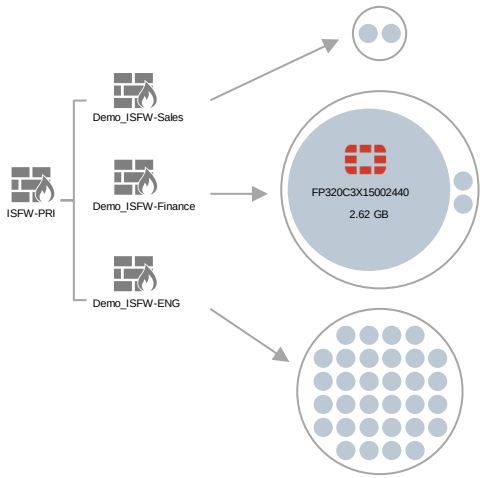
Автоматизация и осведомлённость
Быстрая и скоординированная реакция на угрозы

Глобально и локально

Известные угрозы
FortiGuard

Неизвестные угрозы
FortiSandbox

Аудит и рекомендации



Координация

Открытость – Фабрика позволяет интегрироваться с другими средствами безопасности

FORTINET SECURITY FABRIC

Virtualization & SDN/NFV

- Fortinet Fabric Ready: Brocade
- Fortinet Fabric Ready: nuagenetworks
- Fortinet Fabric Ready: vmware NSX
- Arista
- NEC
- Ericsson
- big switch networks
- Citrix
- Corsa

CLOUD

- Fortinet Fabric Ready: VERISIGN
- Fortinet Fabric Ready: HPE Helion
- amazon web services
- Microsoft Azure
- NTT
- IBM Cloud

ENDPOINT & IoT

- Fortinet Fabric Ready: CARBON BLACK ARM YOUR ENDPOINTS
- Fortinet Fabric Ready: NOZOMI NETWORKS
- Attivo NETWORKS
- Fortinet Fabric Ready: ziften
- Fortinet Fabric Ready: Pulse Secure

MANAGEMENT

- Fortinet Fabric Ready: QUALYS CONTINUOUS SECURITY
- Fortinet Fabric Ready: tufin
- Fortinet Fabric Ready: WhiteHat SECURITY
- Fortinet Fabric Ready: Centrify
- algosec
- Gigamon
- BRADFORD NETWORKS
- gemalto security to be free
- Kiana Analytics
- FIREMON
- skybox Security
- Extreme Connect Beyond the Network

SIEM

- Hewlett Packard Enterprise
- IBM Security
- splunk>

SYSTEMS INTEGRATOR

- Hewlett Packard Enterprise
- IBM Security
- Capgemini CONSULTING.TECHNOLOGY.OUTSOURCING
- dimension data
- NTT Communications
- accenture High performance. Delivered.


FORTINET