Фабрика безопасности Fortinet

Алексей Андрияшин
aandriyashin@fortinet.com
+79859996477

УВЕРЕННАЯ ПОЗИЦИЯ НА РЫНКЕ

3.4m
УСТРОЙСТВ БЕЗОПАСНОСТИ

439
ПАТЕНТОВ ПОЛУЧЕНО

291 В ПРОЦЕССЕ

330K
ЗАКАЗЧИКОВ ИСПОЛЬЗУЮТ РЕШЕНИЯ FORTINET

8 ИЗ ТОП 10
FORTUNE КОМПАНИЙ ЕВРОПЫ

9 ИЗ ТОП 10
FORTUNE КОМПАНИЙ АЗИИ

10 ИЗ ТОП 10
FORTUNE ТЕЛЕКОММУНИКАЦИОННЫХ КОМПАНИЙ

9 ИЗ ТОП 10
FORTUNE КОММЕРЧЕСКИХ БАНКОВ И РИТЕЙЛ КОМПАНИЙ

7 ИЗ ТОП 10
АВИА КОМПАНИЙ

GARTNER ENTERPRISE FIREWALL MAGIC QUADRANT
LEADER

НЕПРЕВЗОЙДЁННАЯ СЕРТИФИКАЦИЯ
НЕЗАВИСИМЫХ ЛАБОРАТОРИЙ

О регуляторах: ФСТЭК

- **Сертификат от 16-го марта 2017 и <u>единственный по новым требованиям</u> среди иностранных производителей, лидеров сегмента Enterprise Firewall по версии Gartner**
- Требования к межсетевым экранам ” ФСТЭК России 2016”
- Профиль защиты межсетевых экранов типа А четвёртого класса защиты (ФСТЭК России 2016)
- Профиль защиты межсетевых экранов типа Б четвёртого класса защиты (ФСТЭК России 2016)
- Профиль защиты систем систем обнаружения вторжений уровня сети четвертого класса защиты (ФСТЭК России 2012)
- Требования к системам обнаружения вторжений (ФСТЭК России 2011)
- Классификация по уровню контроля отсутствия недекларированных возможностей – по 4 уровню контроля (Гостехкомиссия России)

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3720

Выдан 16 марта 2017 г.
Действителен до 16 марта 2020 г.

Настоящий сертификат удостоверяет, что **программно-аппаратный комплекс «FortiGate», функционирующий под управлением операционной системы FortiOS 5.4.1**, разработанный компанией Fortinet и производимый ЗАО «Национальный Инновационный Центр» в соответствии с техническими условиями ТУ 5015-003-95561296-15, является программно-техническим средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, соответствует требованиям руководящих документов «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевого экрана типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевого экрана типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011) и «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012).

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ» (аттестат аккредитации от 15.09.2016 № СЗИ.RU.0001.01БИ00.Б010) – техническое заключение от 23.12.2016, и экспертного заключения от 03.02.2017 органа по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: ЗАО «Национальный Инновационный Центр»
Адрес: 121471, г. Москва, Земледельческий пер., д.12
Телефон: (495) 204-2086

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям руководящих документов, указанных в настоящем сертификате, осуществляется испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ».

[illegible] ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

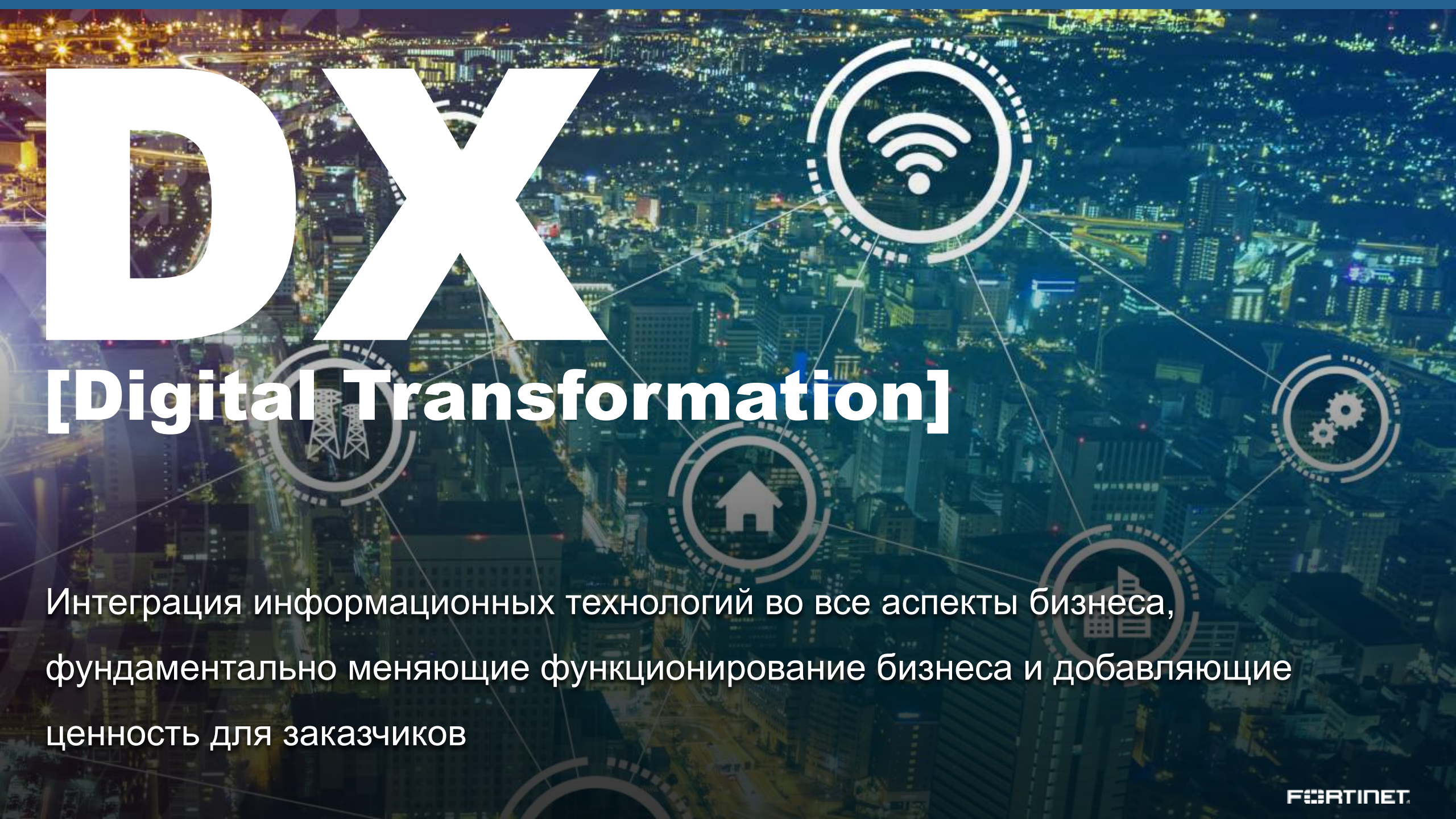
Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
16 марта 2017 г.

Локальное производство “Граница”

СЕРТИФИКАЦИЯ

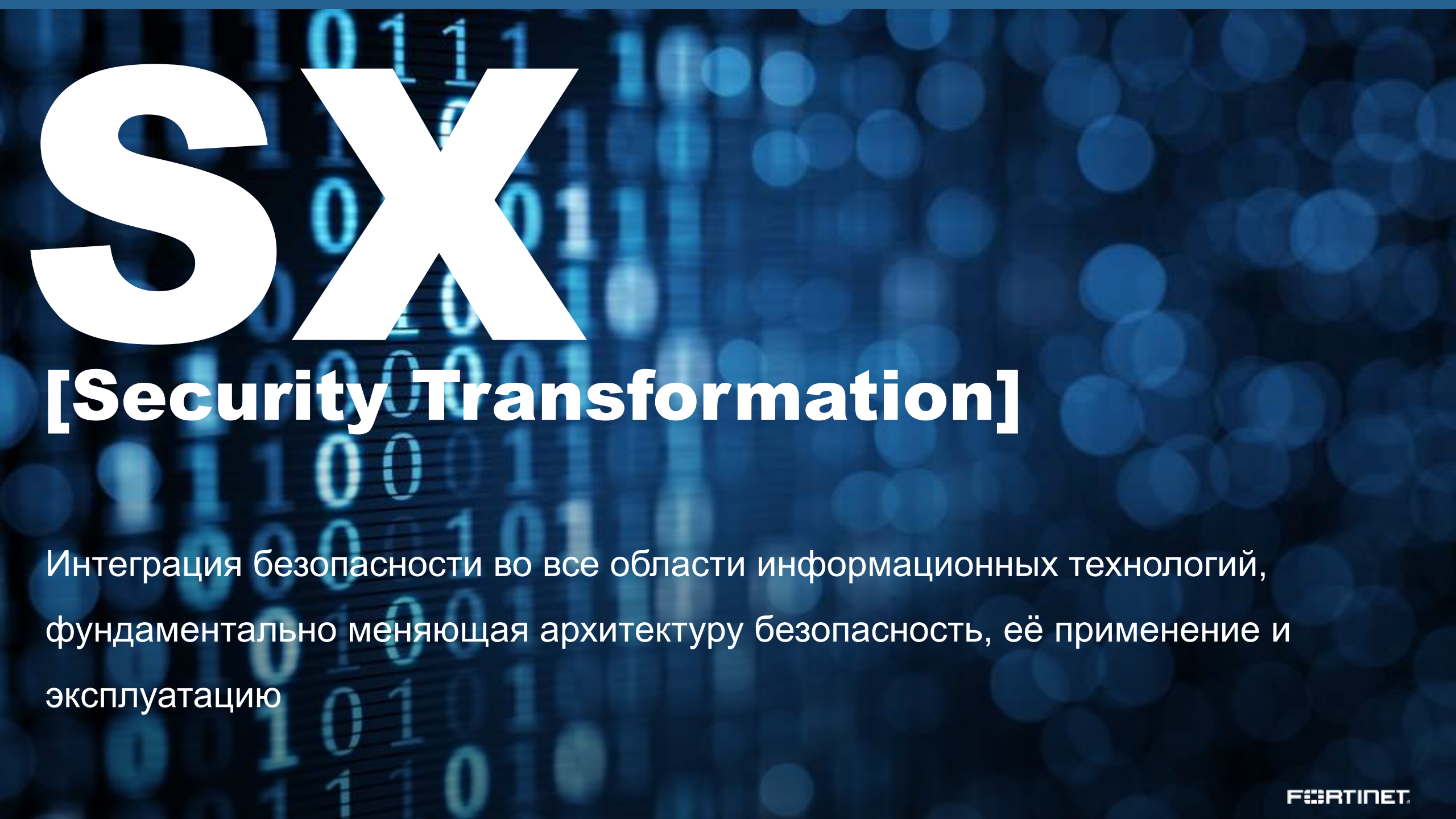
- Сертификат ФСТЭК России на соответствие требованиям «Профиль защиты межсетевого экрана типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ»
- Сертификат ФСТЭК России на соответствие требованиям «Профиль защиты систем обнаружения вторжения уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ»
- Сертификат ФСБ России на соответствие требованиям к средствам криптографической защиты информации по классам КС1, КС2, КС3
- Компоненты продукта внесены в реестр отечественного ПО Минкомсвязи России

	ПАК ГРАНИЦА-30	ПАК ГРАНИЦА-60
Пропускная способность межсетевого экрана (1518 / 512 / 64 byte UDP)	0.95 Gbps	3 / 3 / 3 Gbps
Количество конкурентных сессий	900 000	1.3 Million
Количество новых сессий /с	15 000	30 000
Пропускная способность в режиме контроля приложений	300 Mbps	550 Mbps
Пропускная способность в режиме межсетевого экрана следующего поколения	200 Mbps	250 Mbps
Пропускная способность системы обнаружения вторжений (HTTP / Enterprise Mix)	600 / 240 Mbps	1400 / 350 Mbps
Пропускная способность VPN ГОСТ (UDP1400 / IMIX)	950 / 340 Mbps	950 / 340 Mbps
Максимальное количество ГОСТ туннелей	500	500



Интеграция информационных технологий во все аспекты бизнеса, фундаментально меняющие функционирование бизнеса и добавляющие ценность для заказчиков

FORTINET



Интеграция безопасности во все области информационных технологий, фундаментально меняющая архитектуру безопасность, её применение и эксплуатацию

FORTINET

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПОРЯЖЕНИЕ

от 28 июля 2017 г. № 1632-р

МОСКВА

Утвердить прилагаемую программу "Цифровая экономика Российской Федерации".

Председатель Правительства
Российской Федерации Д.Медведев

Цифровизация экономики

Тинькофф Банк

BELKA CAR

Ростелеком

AEROFLOT

@mail.ru

Место России в мировых рейтингах

№	Страна	Баллы
1	Исландия	8.98
2	Корея	8.95
3	Швейцария	8.74
...		
44	Португалия	7.13
45	Россия	7.07
46	Словакия	7.06

Индекс развития ИКТ (МСЭ) – 2017, 176 стран

№	Страна	Баллы
1	Сингапур	6.0
2	Финляндия	6.0
3	Швеция	5.8
...		
40	Кипр	4,6
41	Россия	4,5
42	Польша	4,5

Индекс готовности к сетевому миру (ВЭФ, INSEAD, Johnson) – 2016, 149 стран

№	Страна	Баллы
1	Швейцария	67.69
2	Швеция	63.82
3	Нидерланды	63.36
...		
44	Греция	38.85
45	Россия	38.76
46	Чили	38.70

INSEAD, Корнельский университет, ВОИС
Глобальный индекс инноваций – 2016, 127 стран

№	Страна	Баллы
1	Сингапур	0.925
2	США	0.919
3	Малайзия	0.893
...		
9	Канада	0.818
10	Россия	0.788
11	Япония	0.786

Глобальный индекс кибербезопасности МСЭ – 2017, 165 стран

№	Страна	Баллы
1	Норвегия	0.949
2	Австралия	0.939
3	Швейцария	0.939
...		
48	Монтенегро	0.807
49	Россия	0.804
50	Румыния	0.802

Индекс человеческого развития (ПРООН) – 2016, 188 стран

№	Страна	Баллы
1	Швейцария	79.90
2	Сингапур	78.42
3	США	75.34
...		
52	Венгрия	44.25
53	Россия	44.22
54	Филиппины	44.17

Глобальный индекс конкурентоспособности талантов (INSEAD, Adecco, Ин-т лидерства в области человеческого капитала) – 2018, 118 стран

https://www.econ.msu.ru/sys/raw.php?o=46780&p=attachment

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ЗНАЧИТЕЛЬНО РАСШИРЯЕТ ПОВЕРХНОСТЬ АТАКИ

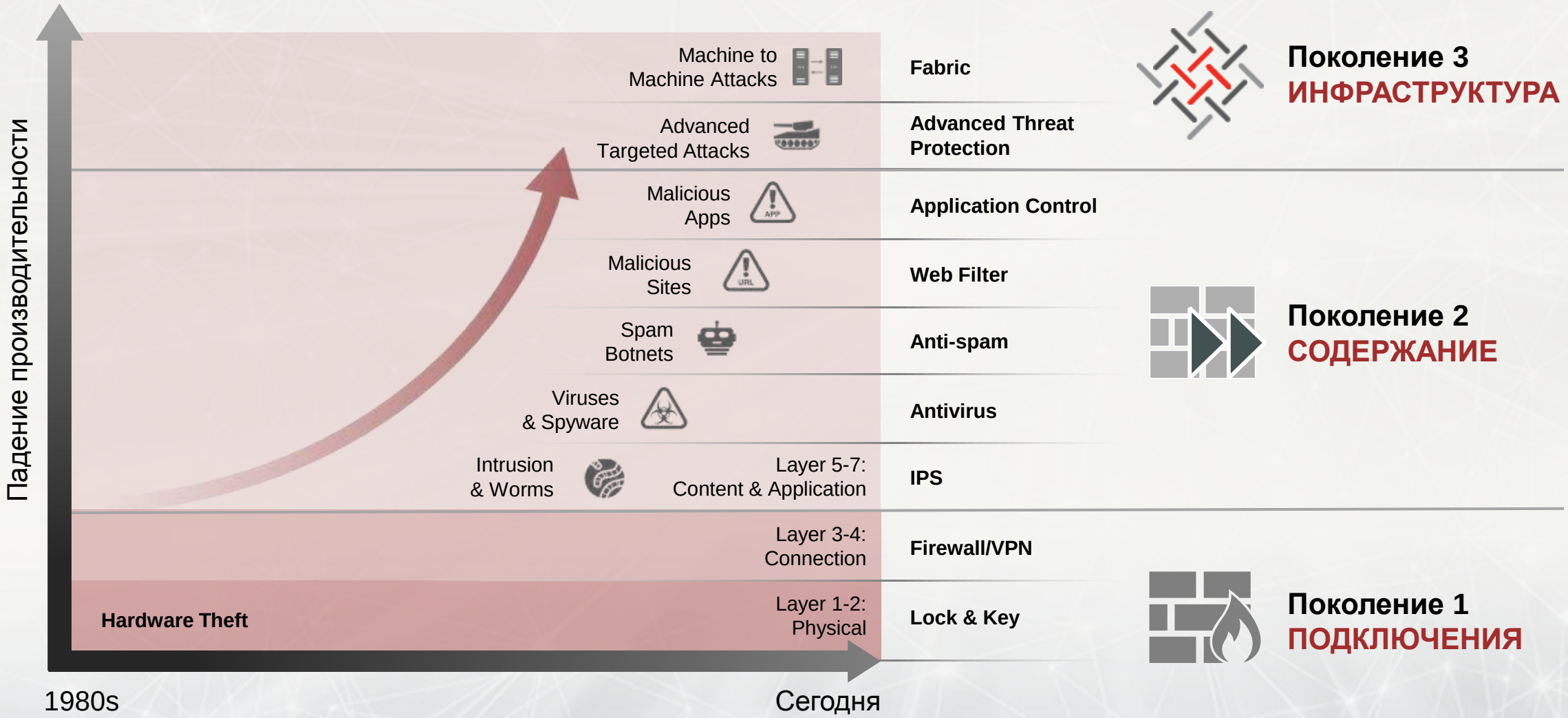
Происходят фундаментальные изменения

DX ⊇ SX

[Security Transformation]

Происходит интеграция безопасности во все области цифровых технологий, что приводит к фундаментальным изменениям в отношении того, как безопасность оценивается, развертывается и реализуется на практике

Угрозы стали более интеллектуальными



Fortinet Self Evolving Detection System - SEDS

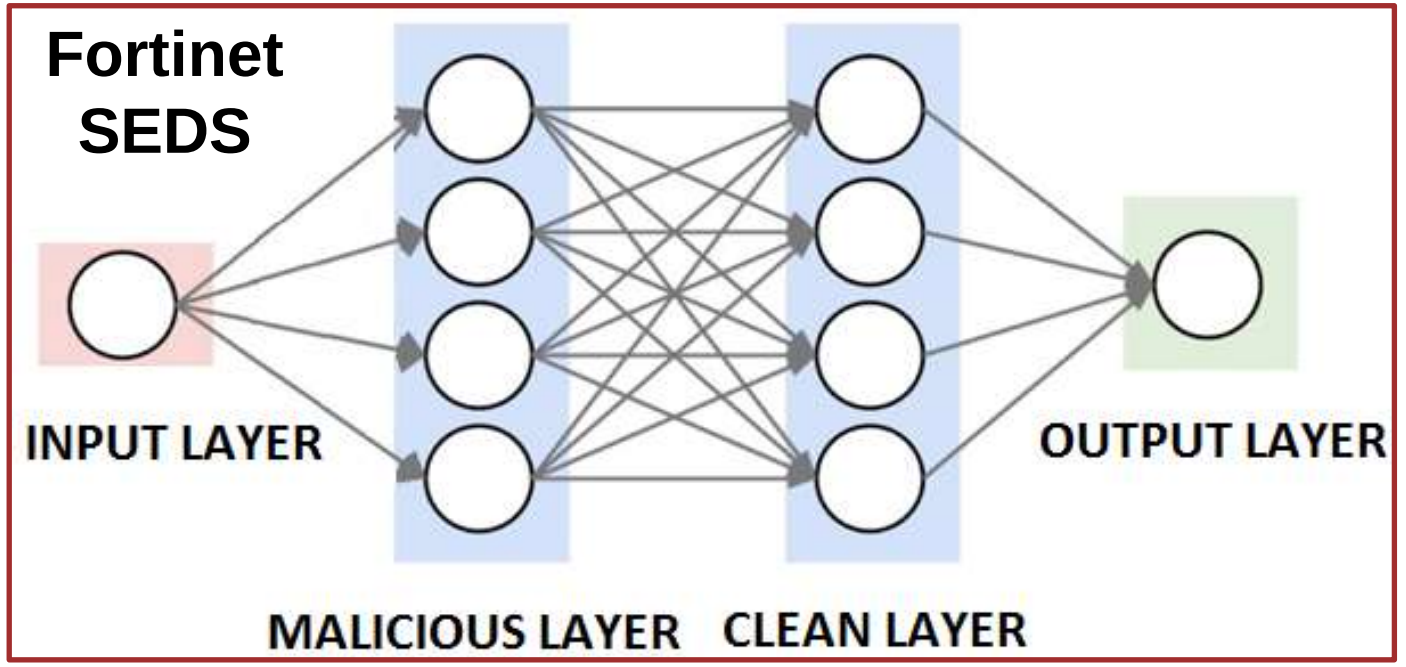
4-уровневая архитектура

1. Обработка входного файла

2. 1,9 миллиарда узлов (нейронов), анализирующих потенциальные вредоносные функции

3. 2,9 миллиарда узлов (нейронов), анализирующих файлы на предмет выполнения безопасных функций

4. Выходной или решающий уровень (1 = вредный , 0 = безопасный)

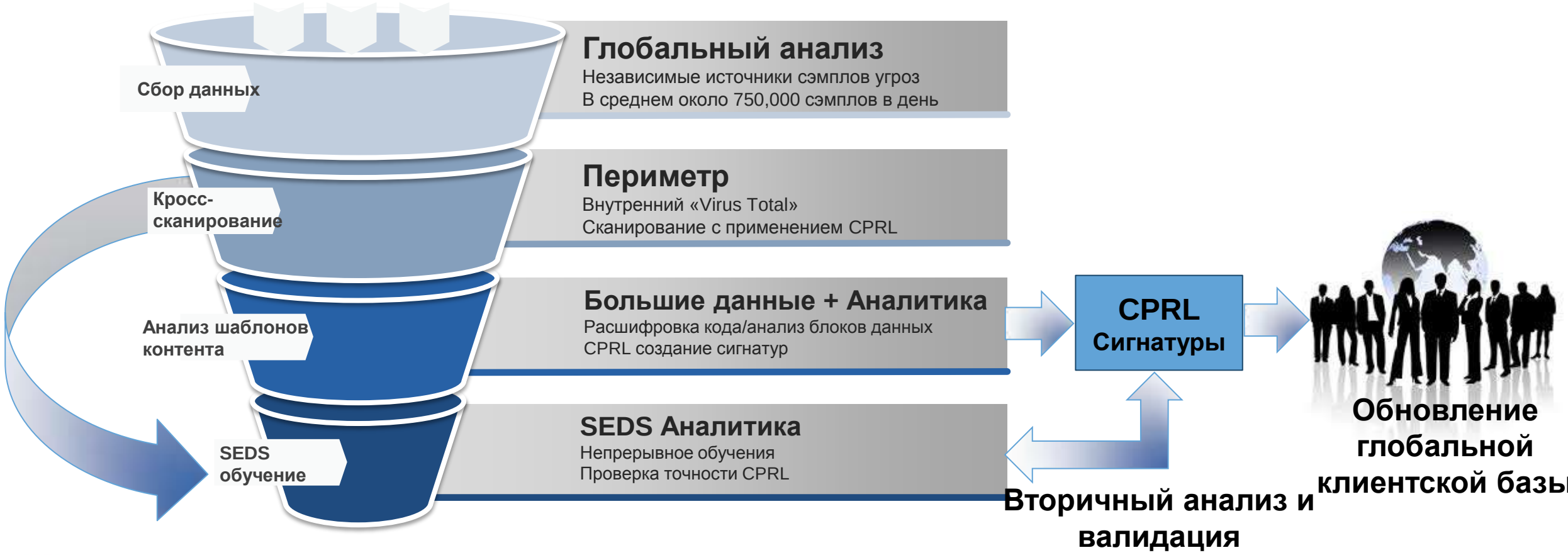


Состоит из отдельных слоев для обработки вредоносных или чистых объектов
Математические модели сравнивают образцы и функции, принимая решение

SEDS – ТЕКУЩИЕ ВОЗМОЖНОСТИ

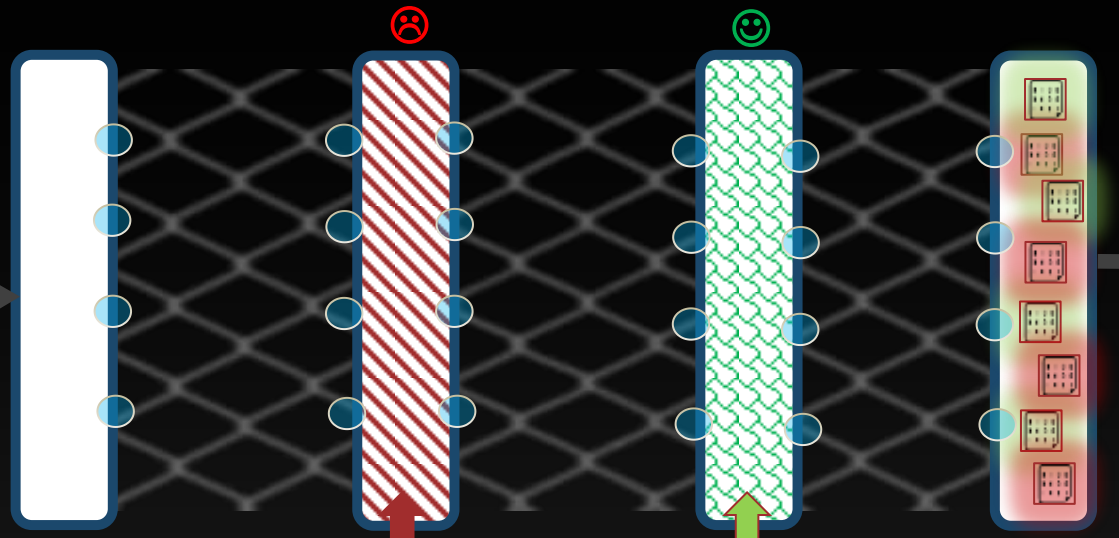
Усовершенствование распознавания образов и автоматическое создание сигнатур

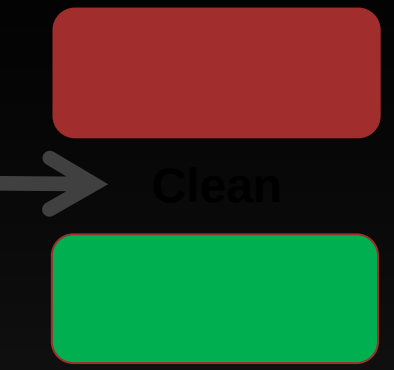
Непрерывное обучение и усовершенствование функций - повышение точности системы



FortiGuard (SEDS) Самообучающаяся система обнаружения угроз

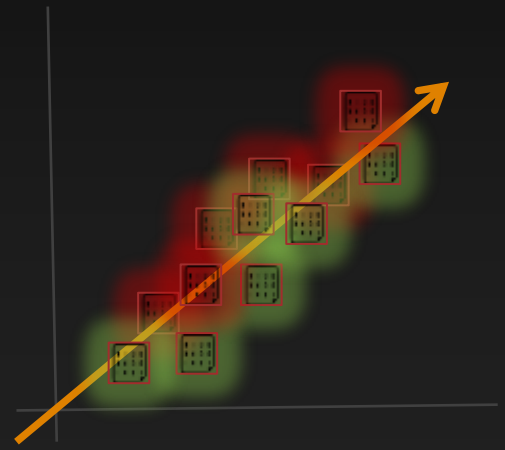
Образцы





Расширение функций – Качество, Стабильность, Количество, расстановка весов

Непрерывное повышение точности и уровня доверия



FortiGuard в числах


THREAT
LANDSCAPE
REPORT
Q1 2018

Инфраструктурные тренды

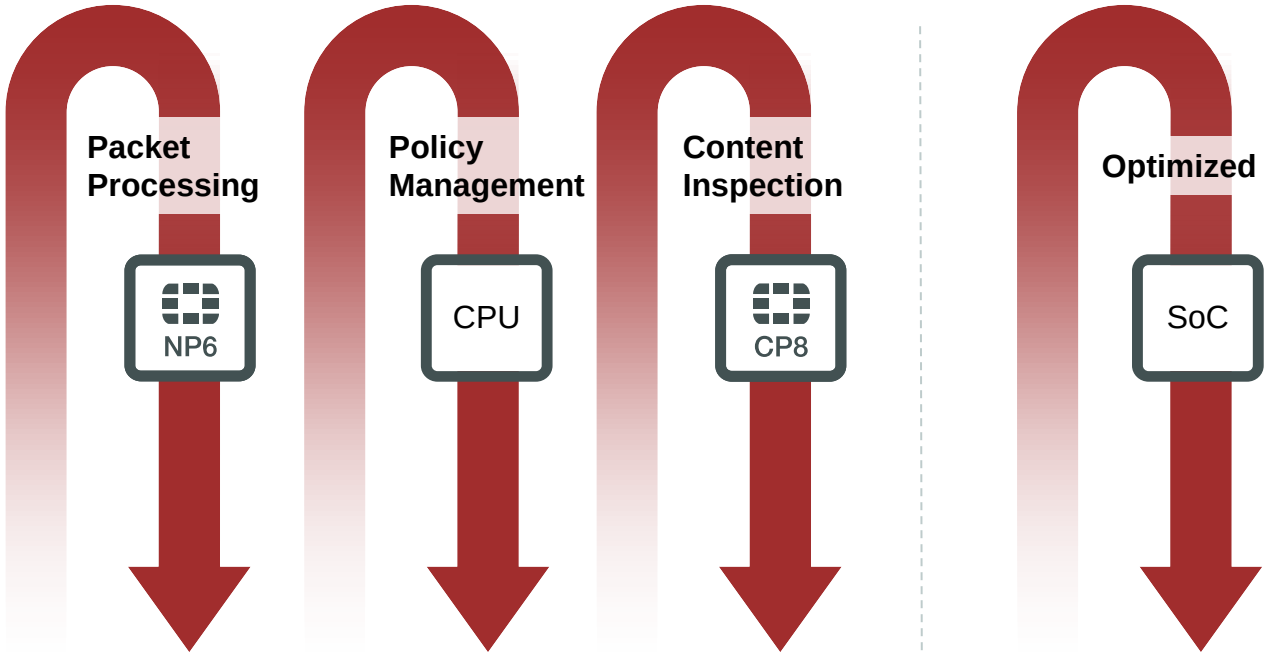
	Q1 2016	Q2 2016	Q3 2016	Q4 2016	Q1 2017	Q2 2017	Q3 2017	Q4 2017
Daily bandwidth	6.3G	7.7G	7.3G	8.5G	8.5G	6.4G	8.9G	10.6G
HTTPS ratio	52.5%	49.8%	52.4%	50.8%	54.9%	57.3%	55.4%	58.5%
Daily Total Apps	216	215	211	211	195	187	195	202
SaaS apps	33	35	35	36	33	28	32	37
IaaS apps	26	22	23	27	29	25	26	28
RAS apps	4	4	4	4	4	4	4	4
Proxy apps	4	4	4	5	4	4	4	3
P2P apps	1	2	2	1	1	1	1	1
Social apps	14	19	17	17	14	13	14	15
Streaming apps	17	24	21	20	16	14	15	15
Gaming apps	2	3	3	3	2	2	2	2
Daily website visits	600	590	571	595	502	411	404	364

Преимущества использования SPU FortiASIC

CPU Only «классический подход»

Большинство производителей оборудования

Архитектура Fortinet Parallel Path Processing (PPP)



Решения Fortinet

- Больше производительность
- Меньше задержка
- Меньше места в стойках
- Энергоэффективность

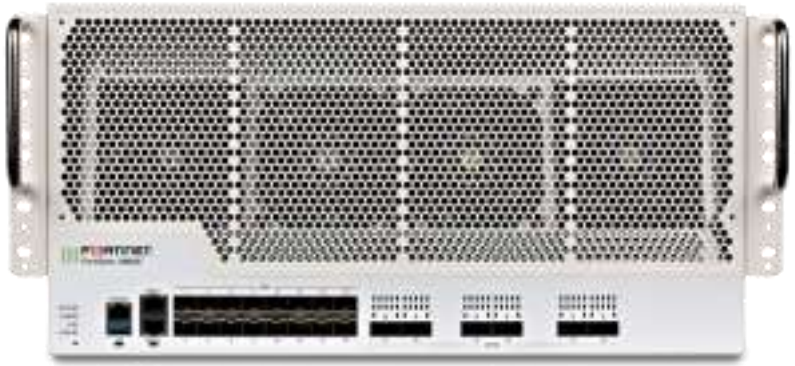
Платформы High-end FortiGate

FortiGate 3960E and 3980E

- Основные сферы применения:
  - Построение распределенного ЦОД
  - Высокопроизводительный Firewall, VPN
  - Операторы/провайдеры

620 Gbps FW

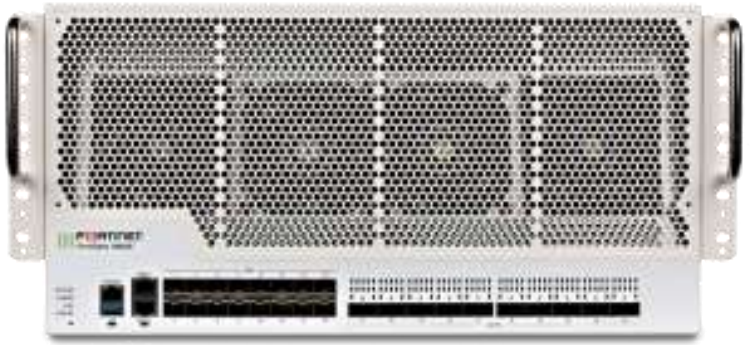
280 Gbps VPN



FortiGate 3960E

1 Tbps FW

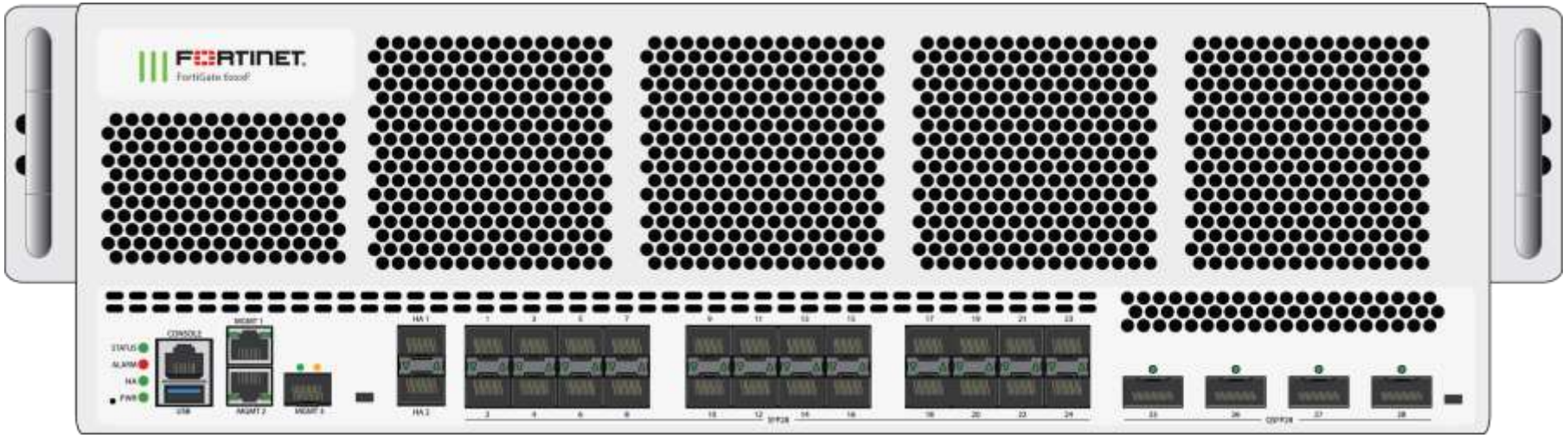
400 Gbps VPN



FortiGate 3980E

FortiGate Ultra High End – FG-6300F и FG-6500F

Новая линейка High End Next Generation Firewall

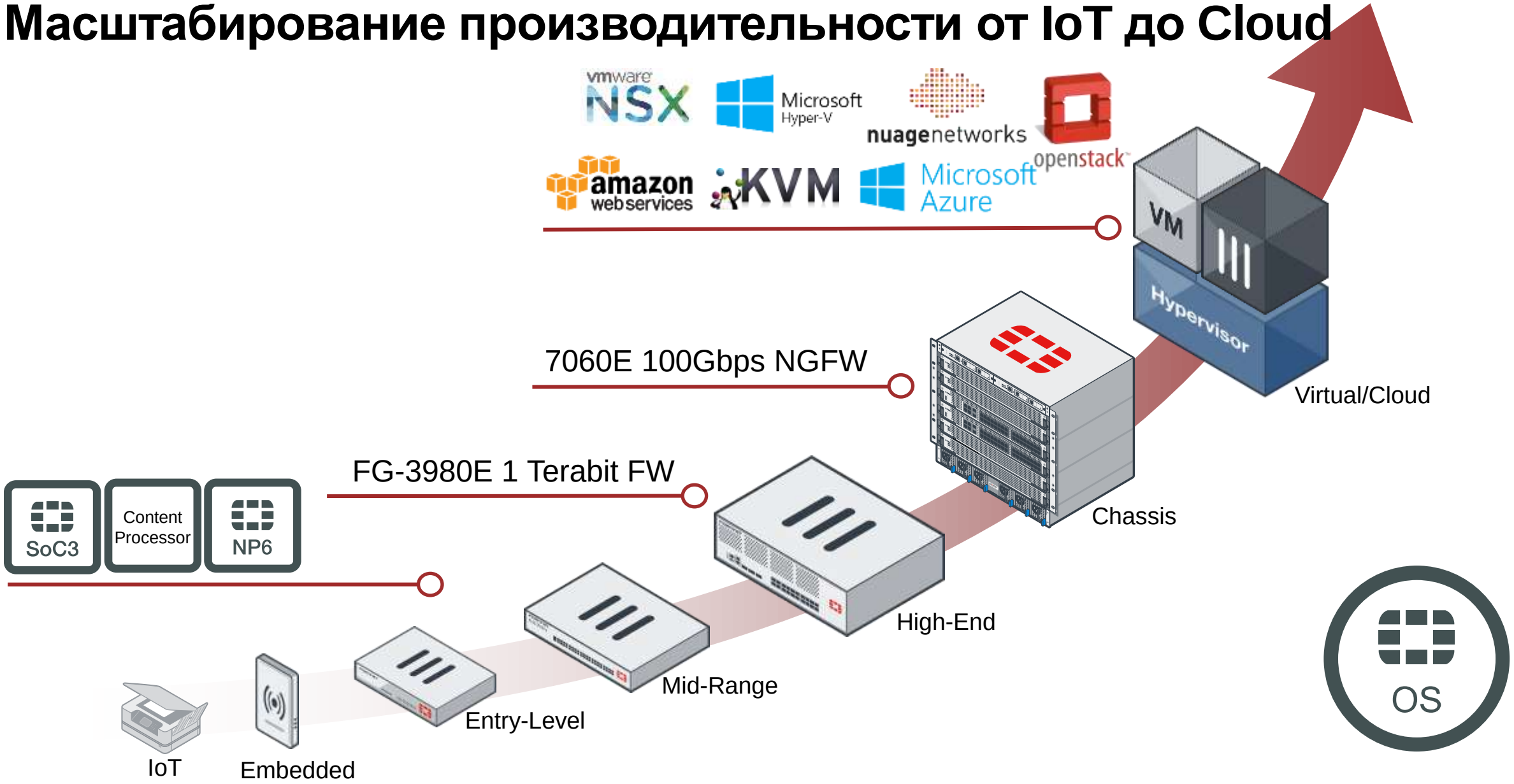


6000 серия

- **3 RU форм-фактор**
- **Резервные блоки питания с «горячей заменой»**
- **2TB SSD локальный диск**

- **Ultra-high Performance Compact NGFW** – до 100 Гбит/с производительности по показателю Threat Protection
- **Industry's Highest SSL Inspection Performance** – инспекция SSL-трафика на огромных скоростях
- **Flexible Network Interfaces** – широкий выбор сетевых интерфейсов 10G/25G/40G и 100G, поддержка современных архитектур, миграция с 10GE на 100GE
- **Out of Band Logging –** журналирование через выделенный интерфейс 10G SFP+ OOB

Масштабирование производительности от IoT до Cloud



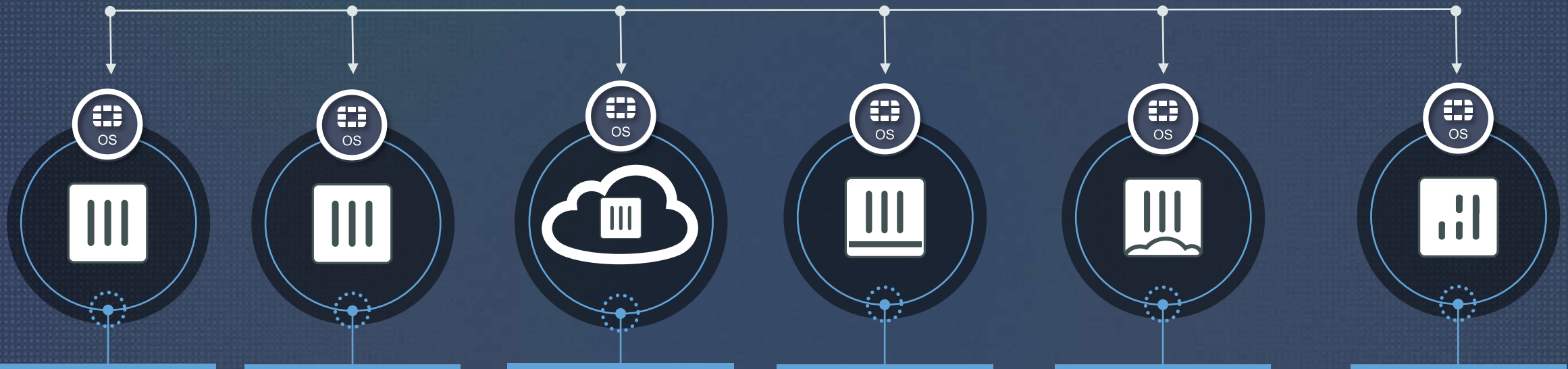
FORTIOS 6.0


Fabric Integration
Tagging
SD-WAN
Certs
Fabric Ready Partners
Automation
Connectors
OS
Developers Network API
CASB
Fabric Agent
FortiGuard
SecurityRating

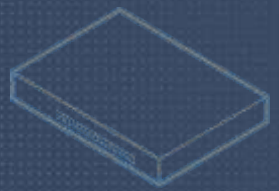
АРХИТЕКТУРА АДАПТИВНОЙ БЕЗОПАСНОСТИ

ОБОРУДОВАНИЕ + ПО + СЕРВИСЫ

Обновления FortiGuard



IoT Hardware	FortiGate Hardware	Fortinet Cloud	FortiGate VM	Public | Private Cloud	Public | Private Cloud
	ПАК	Хостинг	Виртуальная Машина	Облако	Контейнеры



СЕРВИСЫ ЗАЩИТЫ FORTIGUARD

FortiGuard

Baseline Protection

- IP Reputation
- Internet service DB
- Certificate & Domain white list
- Application Control
- Anti-Spam

+

Threat Protection

- Antivirus
- Intrusion Prevention

Unified Protection

- Web Filtering
- Antivirus
- Intrusion Prevention

Enterprise Protection

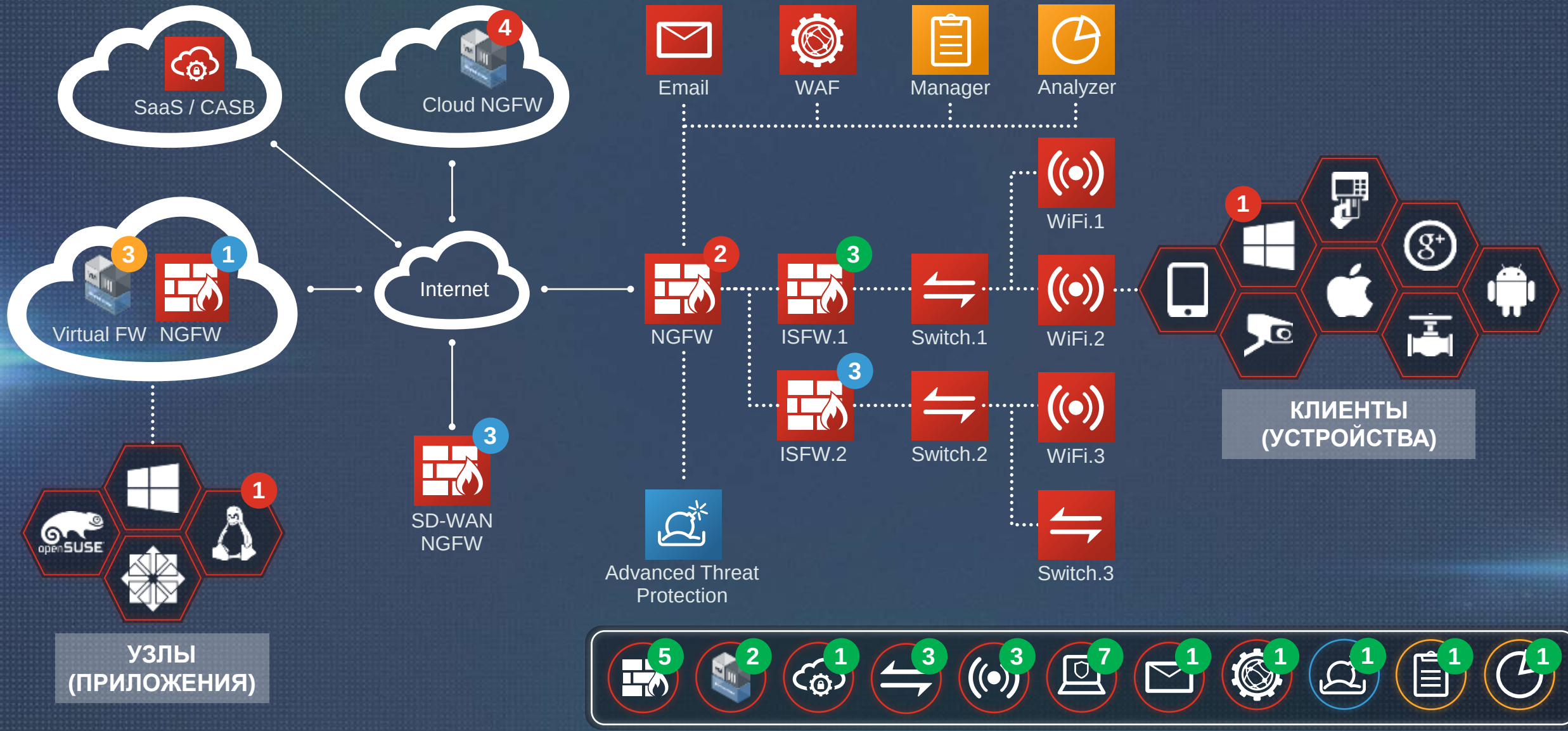
- Virus Outbreak Service
- Content Disarm & Reconstruction
- FortiSandbox Cloud
- Web Filtering
- Antivirus
- Intrusion Prevention

Industrial Security Service

Security Audit Service

FORTINET SECURITY FABRIC - ТОПОЛОГИЯ

Fabric Integration



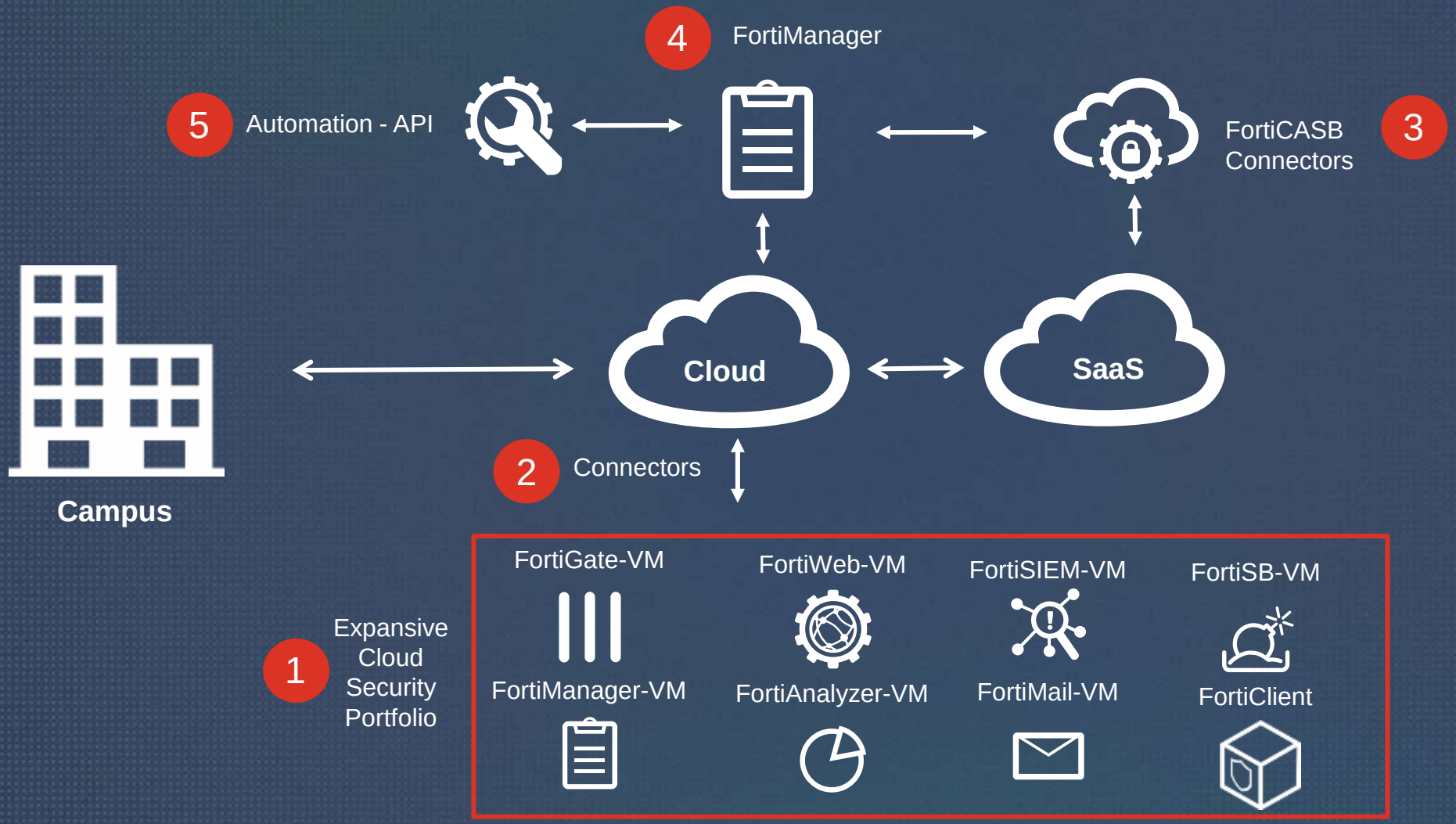
КОНТРОЛЬНЫЙ СПИСОК ИНТЕГРАЦИЙ SECURITY FABRIC

Fabric Integration

	NETWORK	ENDPOINT	UNIFIED ACCESS		EMAIL	WEB APPS		MULTICLOUD
	FORTIGATE	FORTICLIENT	FORTISWITCH	FORTIAP	FORTIMAIL	FORTIWEB	FORTIADC	FORTICASB
TELEMETRY DEVICE LEVEL API	✓	✓	✓	✓	✓	✓	✓	2018
FORTIVIEW TOPOLOGY MAP	✓	✓	✓	✓	2018	✓	✓	
FORTIMANAGER	✓	✓	✓	✓		✓		
FORTIANALYZER	✓	✓		✓	✓	✓	2019	Q1 2018
SECURITY RATING AUDIT	✓			✓	2019	2018		
AUTOMATION STITCHES	✓	✓	✓	2018	2018	✓		
VULNERABILITY SCAN		✓				✓		
ADVANCED THREAT PROTECTION SANDBOX	✓	✓			✓	✓	✓	
FORTISIEM	✓	✓	2018	✓	✓	✓	2018	

ПОРТФЕЛЬ FORTINET ДЛЯ ЗАЩИТЫ ОБЛАКОВ

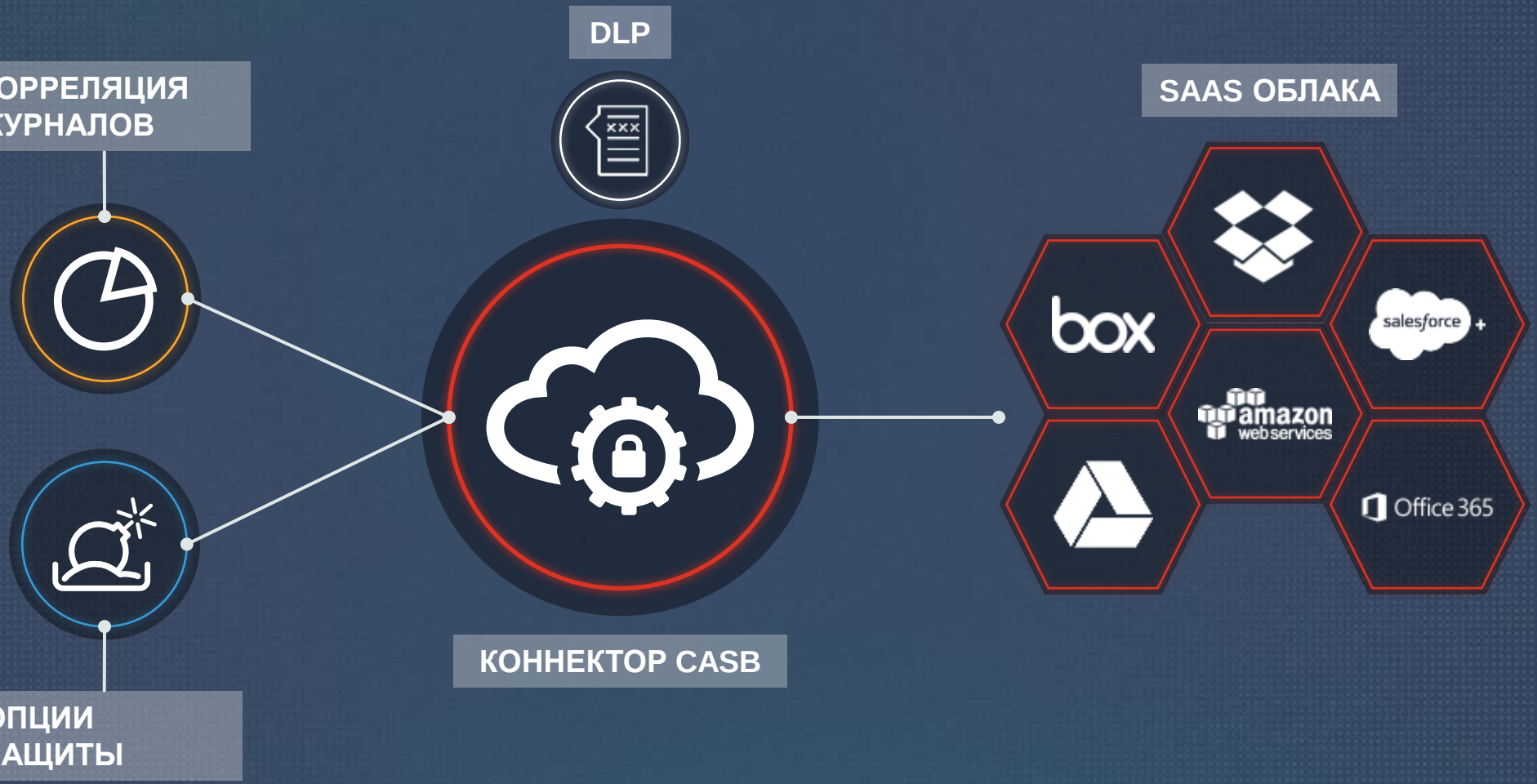
Connectors



CASB – КРИТИЧЕСКИЙ КОМПОНЕНТ ЗАЩИТЫ СЕТИ

FORTICASB 1.2

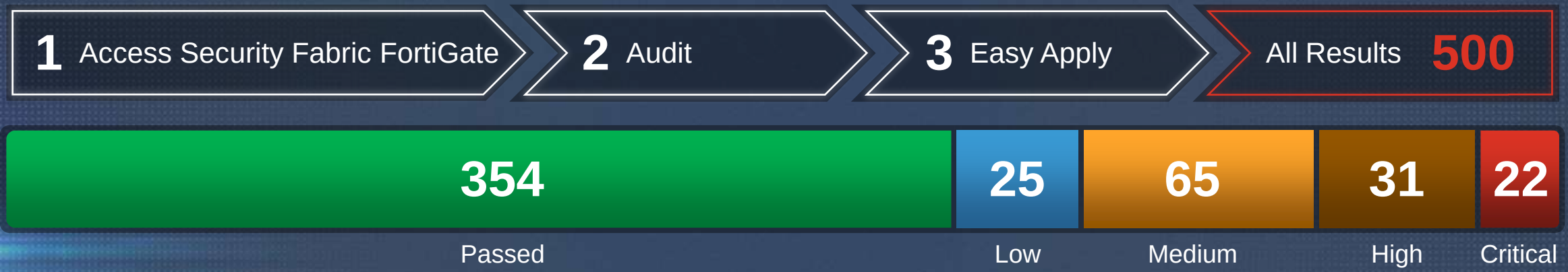
CASB



SECURITY RATING SERVICE

VULNERABILITY SCAN

Security Rating



9,564 Passed

569 Low

126 Medium

27 High

6 Critical

FABRIC АГЕНТ И ЗАЩИТА УЗЛОВ

ПОДДЕРЖКА СЕРВЕРОВ И АРМ

Fabric Agent

Защита от угроз

Агент VPN

Агент фабрики – сетевая телеметрия

HOSTS (APPS)

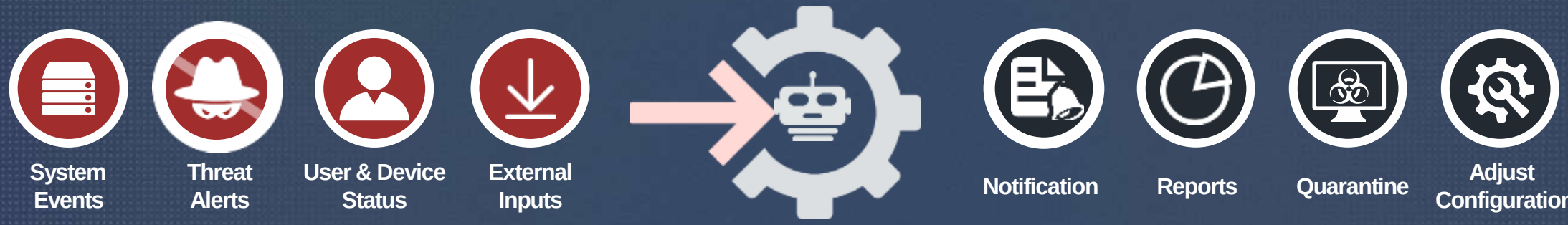
ENDPOINT (DEVICES)

БД Устройств

IOT (DEVICES)

WORKFLOW - АВТОМАТИЗАЦИЯ

Automation



Триггеры | **Автоматизация реагирования** | **Действия**

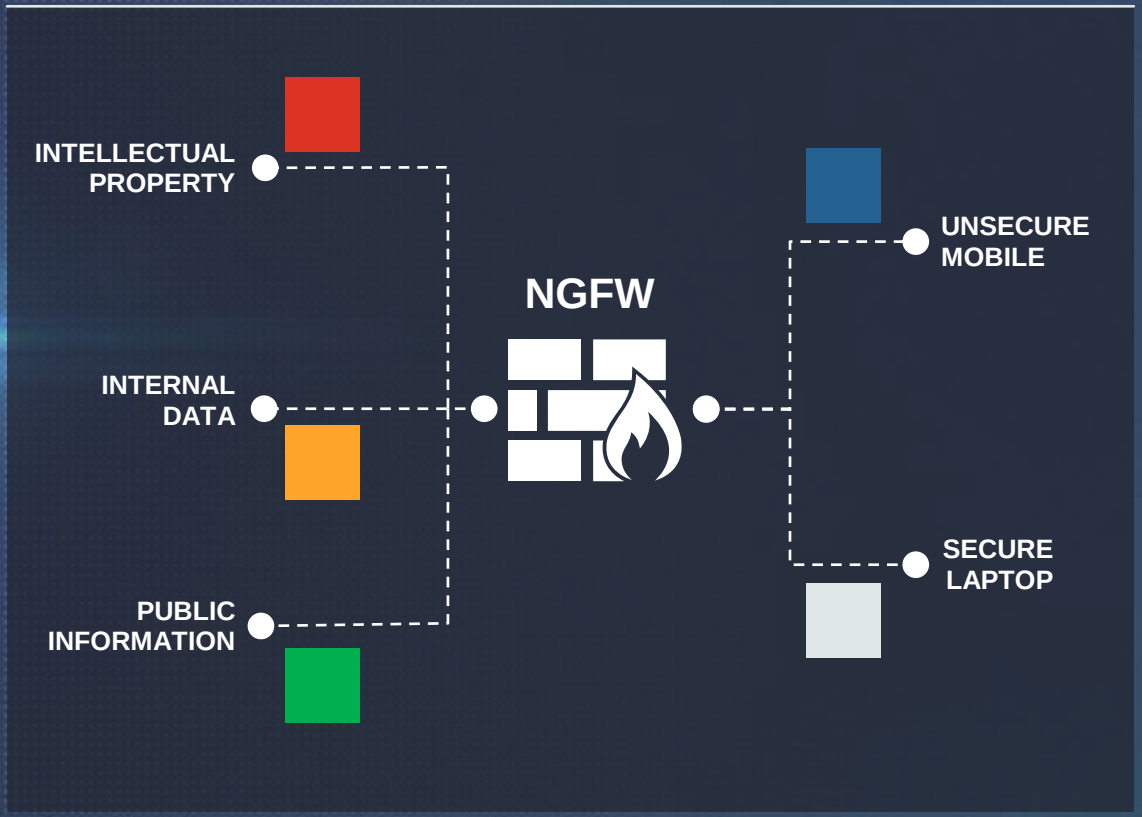
Автоматизация позволяет предпринять соответствующие действия без вовлечения администраторов (например, помещение в карантин)

ЗАЩИТА СЕТИ НА ОСНОВЕ НАМЕРЕНИЙ

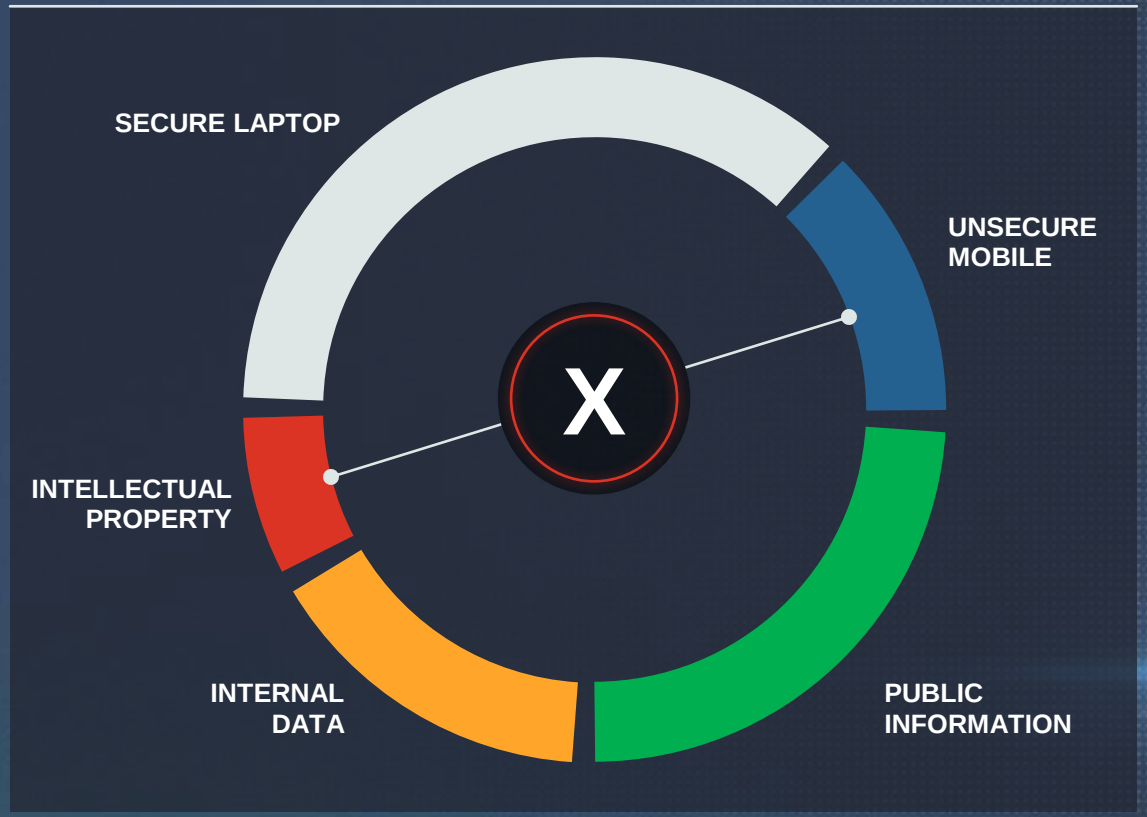
ТЕГИРОВАНИЕ АКТИВОВ

Tagging

TAGGING (DEVICES, INTERFACES, OBJECTS)



GLOBAL POLICY



FABRIC READY - ЭКОСИСТЕМА

Fabric Ready Partners

CLOUD

- amazon web services
- Google Cloud Platform
- ORACLE
- Microsoft Azure
- IBM

SDN

- BROCADE
- cisco
- nuagenetworks
- NEC
- openstack
- vmware

ENDPOINT

- Attivo NETWORKS
- CARBON BLACK ARM YOUR ENDPOINTS
- McAfee Together is power.
- SentinelOne
- Symantec
- ziften

MANAGEMENT

- algosec
- FIREMON
- servicenow
- tufin
- BACKBOX BACKUP RECOVERY AUTOMATION

Security/SIEM

- QUALYS
- IBM Security
- Hewlett Packard Enterprise
- CYBERARK
- MICRO FOCUS
- cyglass
- WhiteHat SECURITY
- Phantom

IOT/OT/NAC

- BRADFORD NETWORKS
- ForeScout
- NOZOMI NETWORKS
- Pulse Secure

IDENTITY

- Centrify
- CLOUDIFY
- CYBERARK

TECHNOLOGY

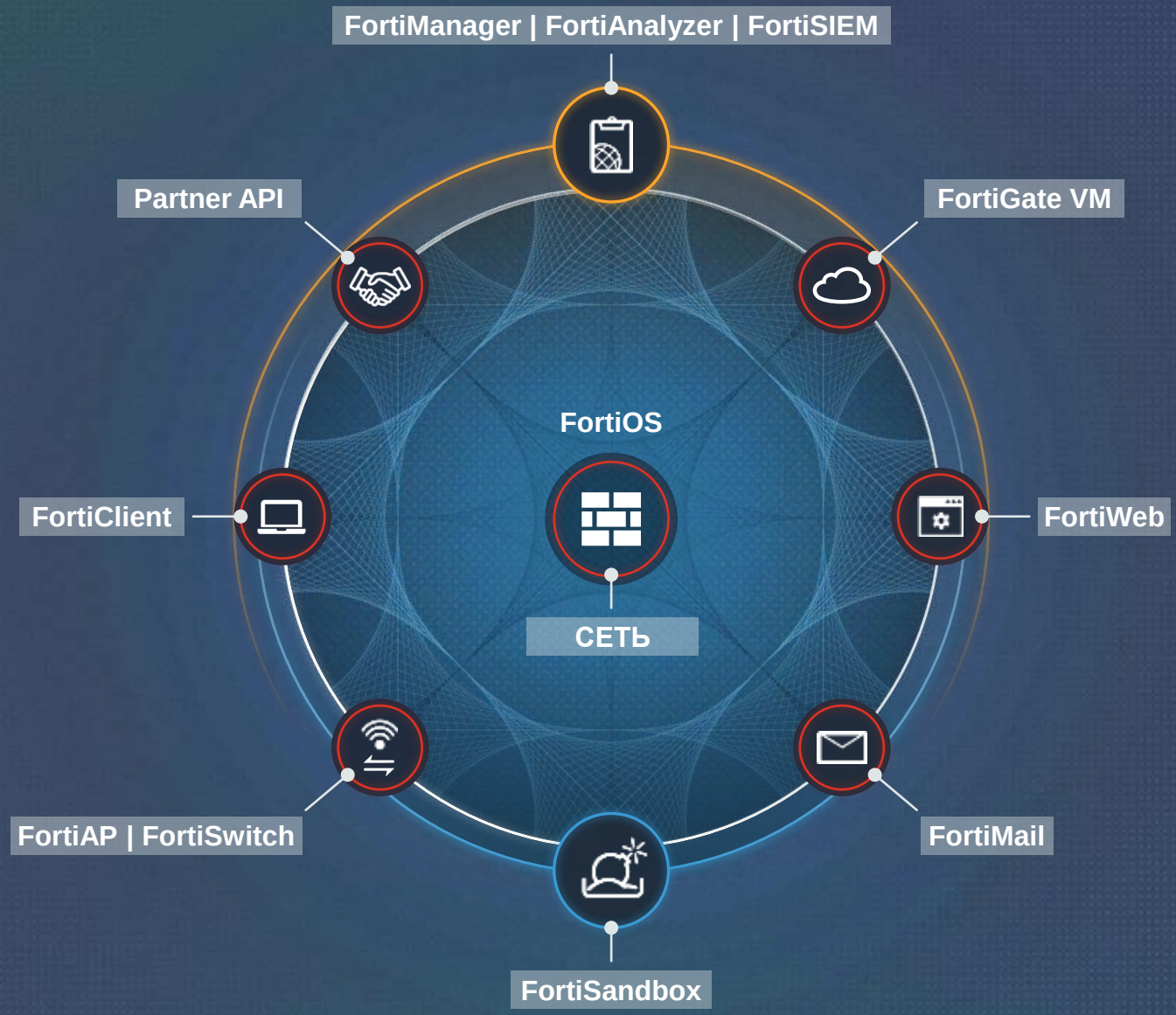
- ADVA Optical Networking
- HUGHES
- intel
- Sonus Cloud communications made smarter
- VERISIGN

2018 FORTINET SECURITY FABRIC

ШИРОТА

ИНТЕГРАЦИЯ

АВТОМАТИЗАЦИЯ




FORTINET