Fortinet Security Fabric -

Основа цифровой трансформации

Олеся Тарабрина
Fortinet SE

FORTINET

$18B+ Market Cap
Nasdaq: FTNT
S&P 500

$2.6B
FY2019 Billings
Fast Growing, Solid Profitability

660+
Patents
Top Innovator

#1 Cybersecurity Company in the World

Leading Every Evolution of Cybersecurity

- ✓ *Most Deployed*
- ✓ *Most Validated*
- ✓ *Most Patented*
- ✓ *Broadest Portfolio*

30%
Global Firewall Shipments
Huge Scale

450,000+
Customers Worldwide
Massive Sensor Network

30+
Cybersecurity Product Lines
Broadest Attack Surface Coverage

Source: Company data, Figures as of December 31, 2019

DX

[Digital Transformation]

Интеграция цифровых технологий во все аспекты бизнеса, приводящая к фундаментальным изменениям в работе бизнеса и в способах донесения ценности до потребителя

FORTINET

SX

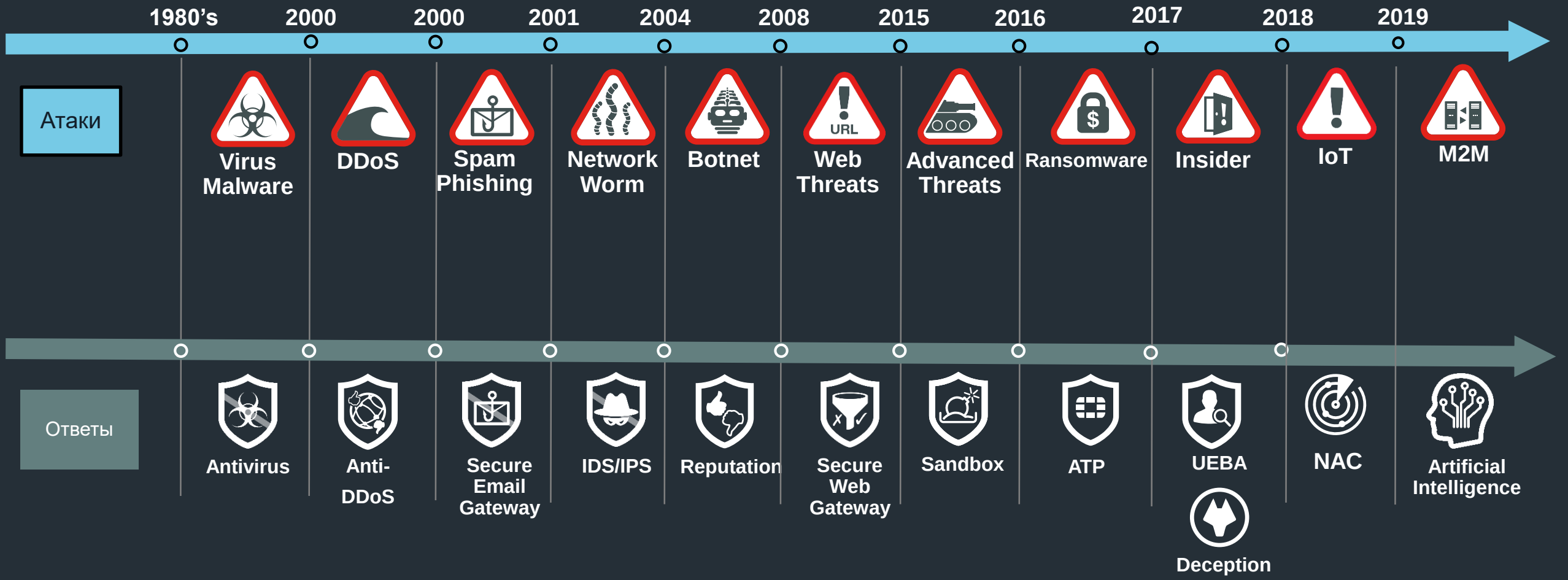
Интеграция безопасности во все аспекты цифровых технологий, приводящая к появлению Архитектуры Безопасности, которая обеспечивает Непрерывную Оценку Доверия.

[Security Transformation]

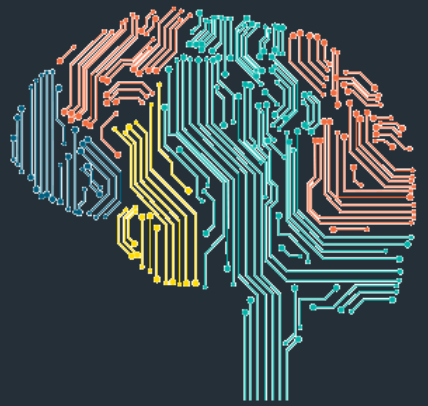
FORTINET

Ландшафт угроз постоянно меняется!

Расширение плоскости атак создает новые вызовы



Технологические проблемы обеспечения ИБ



КОМПЛЕКСНЫЕ
ВЕКТОРЫ АТАК

NOC

АВТОМАТИЗАЦИЯ
ОЦЕНКИ УРОВНЯ ДОВЕРИЯ

ЗАЩИТА ОТ ИЗВЕСТНЫХ УГРОЗ

SOC

БЫСТРОЕ РЕАГИРОВАНИЕ

ИНТЕГРИРОВАННОЕ
ДЕТЕКТИРОВАНИЕ И ЗАЩИТА ОТ НЕИЗВЕСТНЫХ УГРОЗ

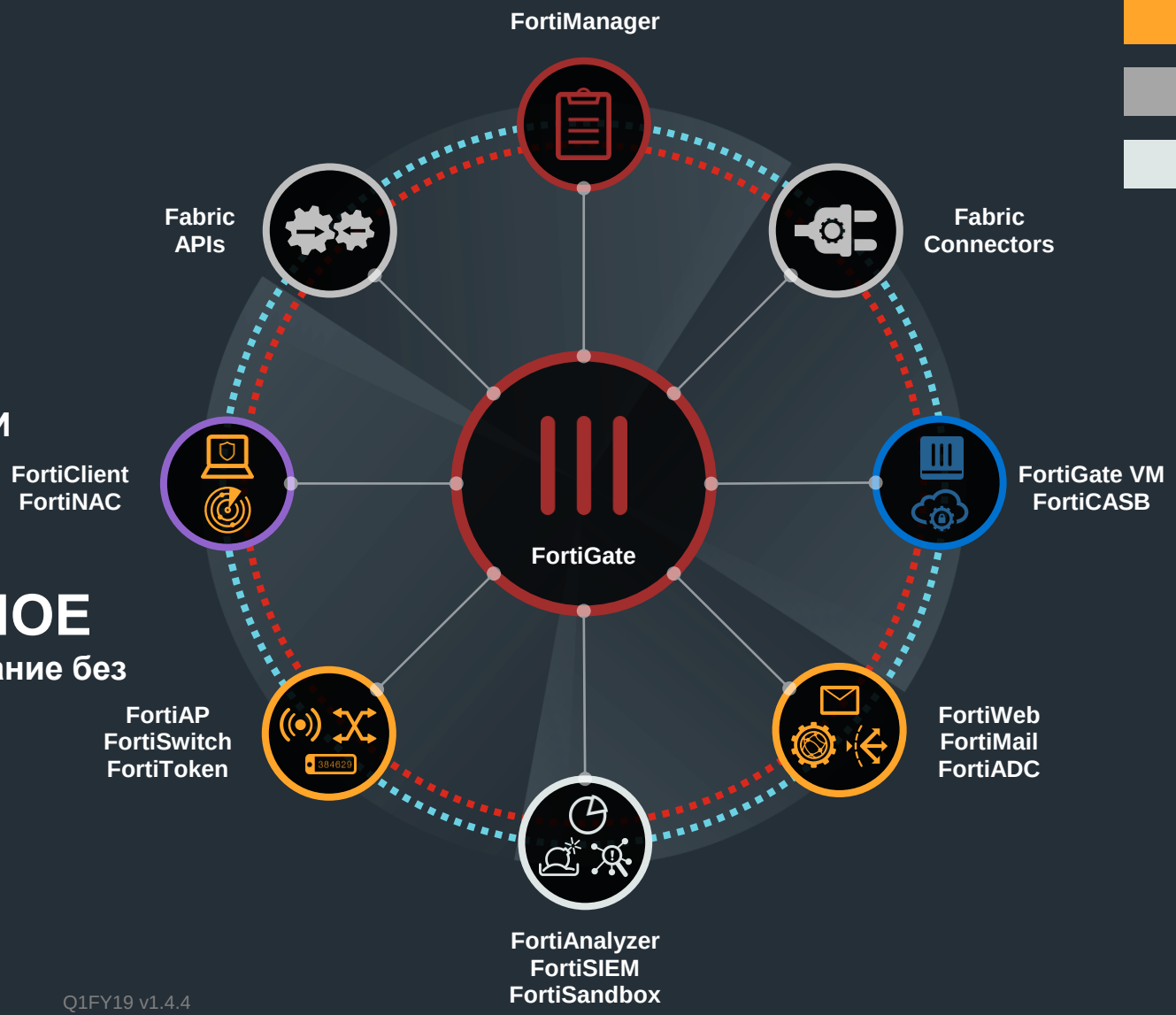
FORTINET

Fortinet Security Fabric

КОМПЛЕКСНОЕ
Видимость и покрытие всех векторов атак

ИНТЕГРИРОВАННОЕ
Предотвращение взлома на основе ИИ в устройствах, сетях и приложениях

АВТОМАТИЗИРОВАННОЕ
Управление, оркестрация и реагирование без участия человека



Network Security

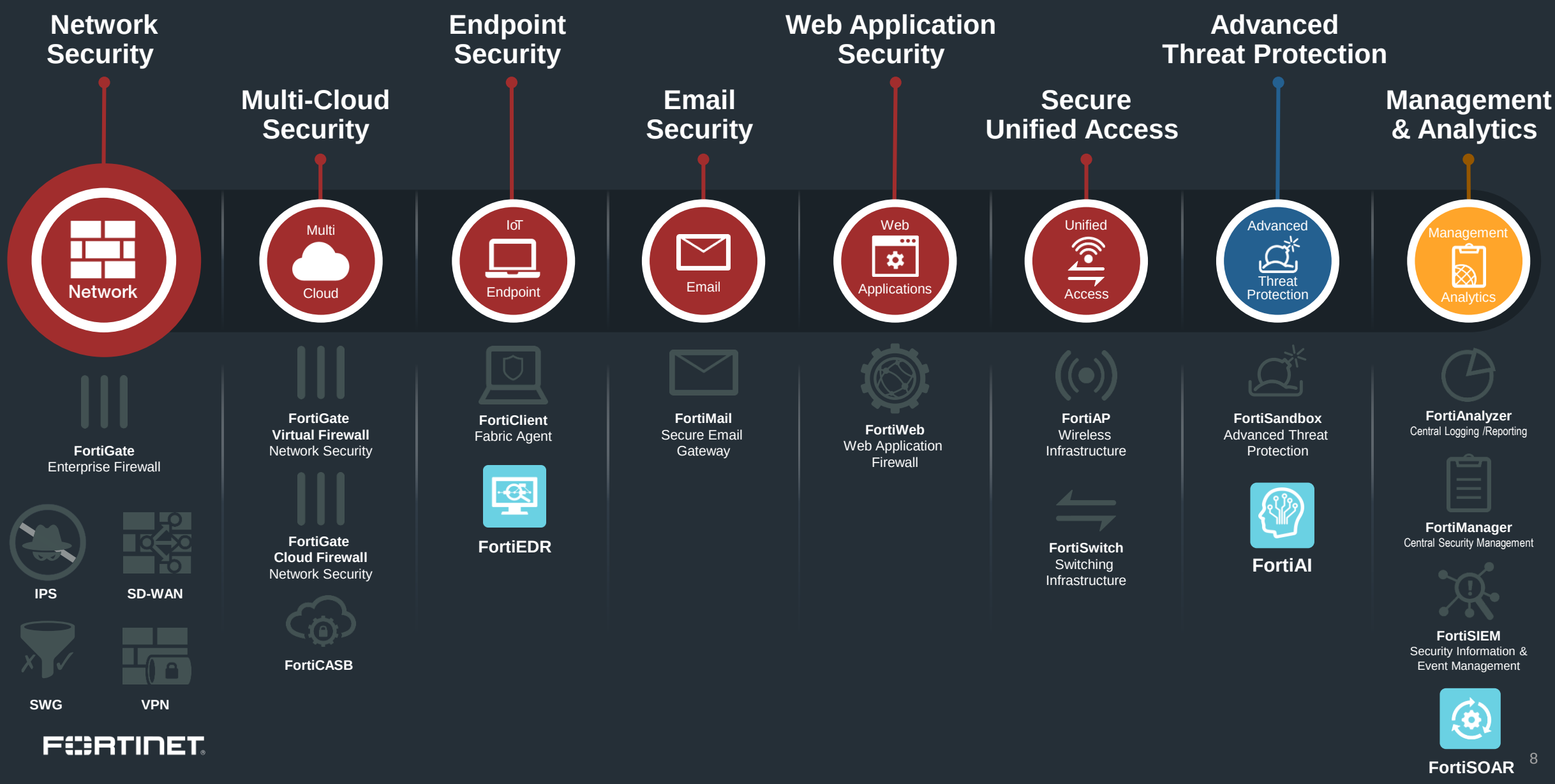
Multi-Cloud Security

Device, Access, and Application Security

Open Ecosystem

Security Operations

Комплексное решение Fortinet



Ключевые технологии Fortinet Security Fabric

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

NP7 — Accelerates Network Traffic

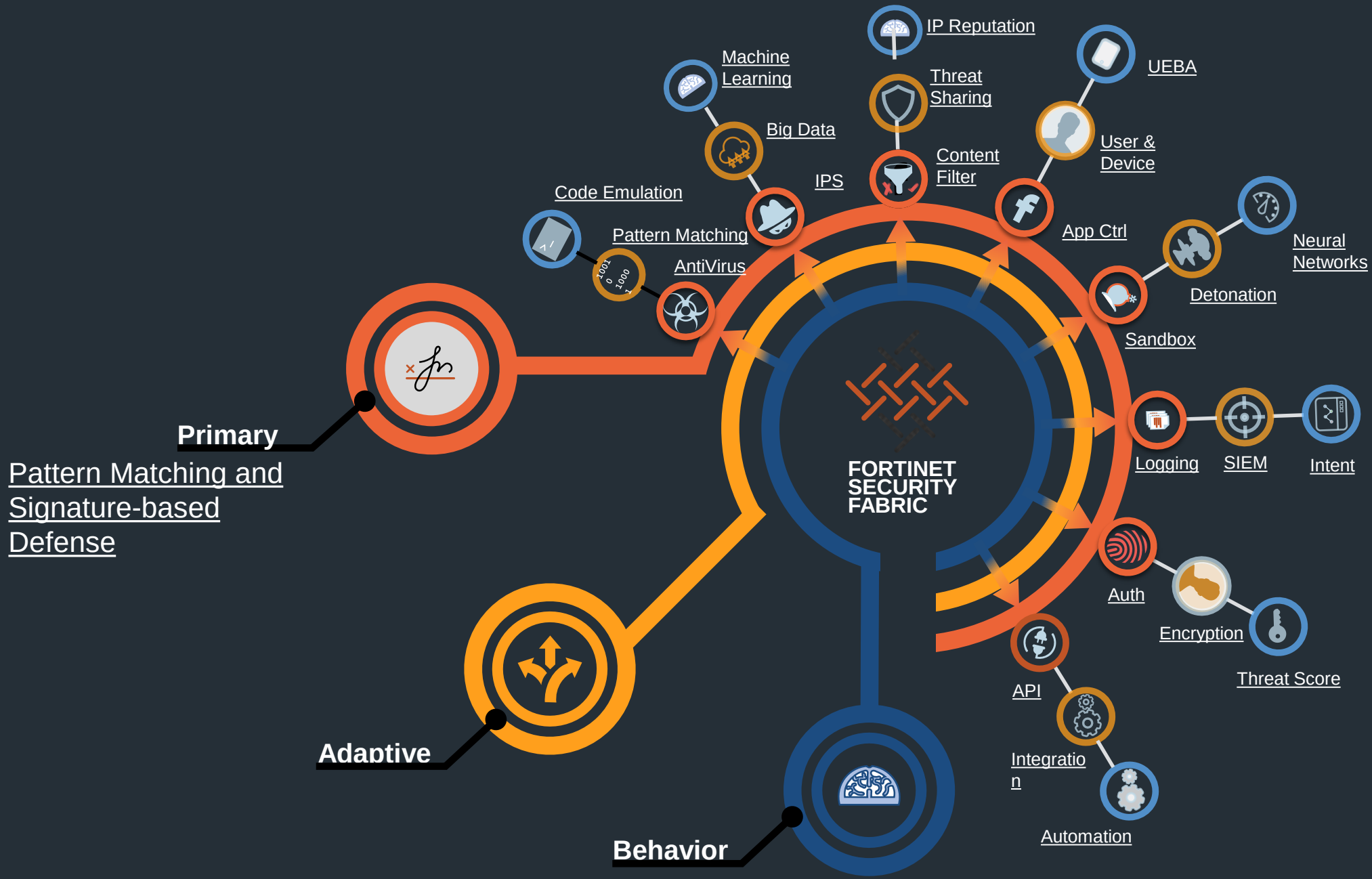
CPU — Flexible Policy

CP9 — Accelerates Content Inspection

SoC4

Optimized for entry-level form factors

- **More Performance**
- **Less Latency**
- **Less Power**
- **Less Space**


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
Pattern Matching and Signature-based Defense
FORTINET SECURITY FABRIC
Logging
SIEM
Intent
Auth
Encryption
Threat Score
API
Integration
Automation
Adaptive
Behavior

Чеклист интеграции Security Fabric

Fabric Integration

Атрибуты Security Fabric

TELEMETRY DEVICE LEVEL API	Могут ли устройства, входящие в Security Fabric общаться друг с другом ?
FORTIVIEW TOPOLOGY MAP	Видно ли все устройства на топологической карте ?
FORTIMANAGER	Возможно ли централизованно управлять и применять политики ?
FORTIANALYZER	Возможно ли централизованно получать отчеты и аналитику ?
SECURITY RATING AUDIT	Возможно ли применять лучшие практики по настройке МСЭ ?
AUTOMATION STITCHES	Возможно ли автоматизировать сценарии рабочих процессов на МСЭ ?
VULNERABILITY SCAN	Возможно ли сканирование уязвимостей конечных узлов ?
ADVANCED THREAT PROTECTION SANDBOX	Возможно ли защититься от угроз нулевого дня ?
FORTISIEM	Возможно ли увидеть и использовать аналитику для устройств “не от Fortinet” ?

FORTINET

Сервисы защиты от киберугроз FortiGuard

FortiGuard Threat Intelligence

Application Control

IP Reputation

Web Filtering

Security Rating

Industrial Control

FortiGuard

Internet Services DB

Antivirus & Mobile Security

Business Aware Tagging

Sandboxing

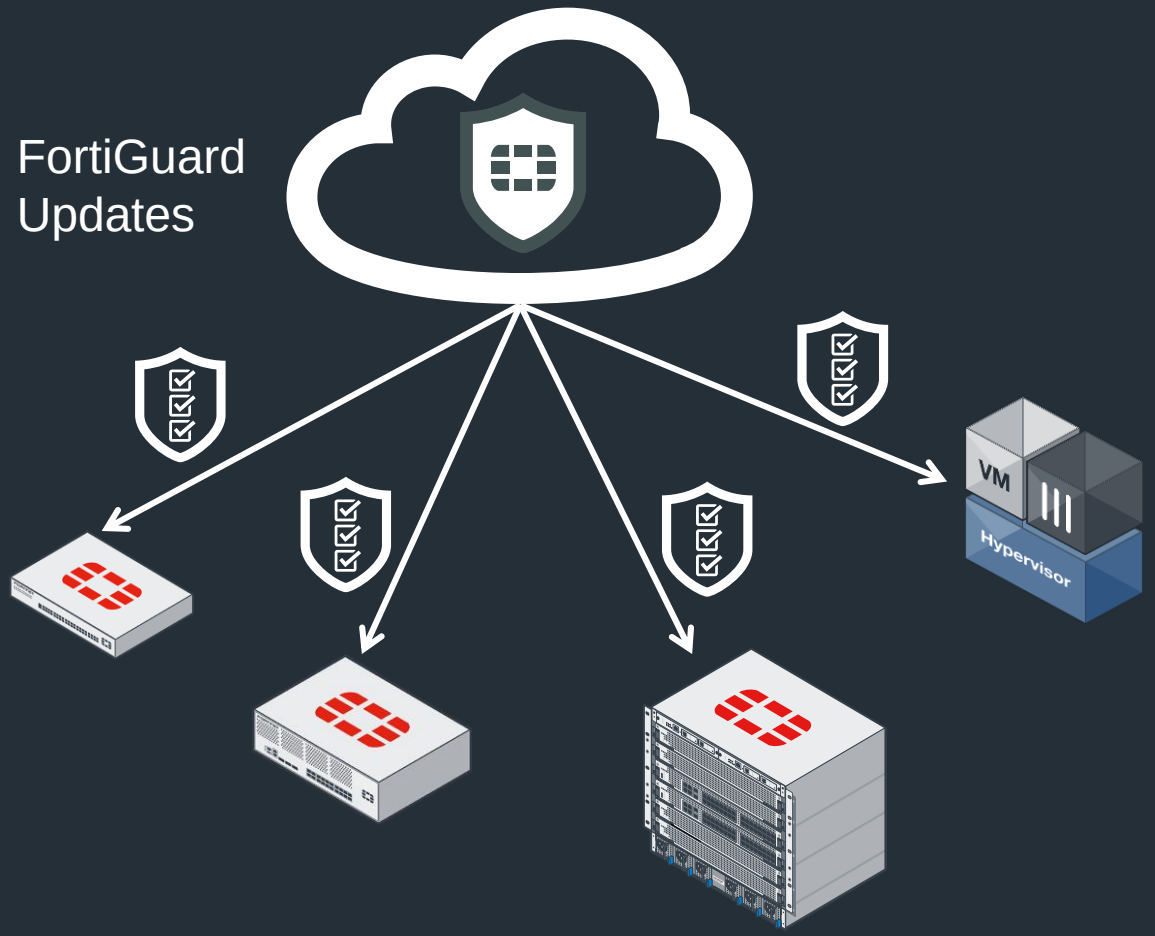
Content Disarm & Reconstruction

Virus Outbreak Service

Security Rating Service

FortiGuard Threat Intelligence

ЛУЧШИЕ МИРОВЫЕ ПРАКТИКИ ПО ИНДУСТРИИ



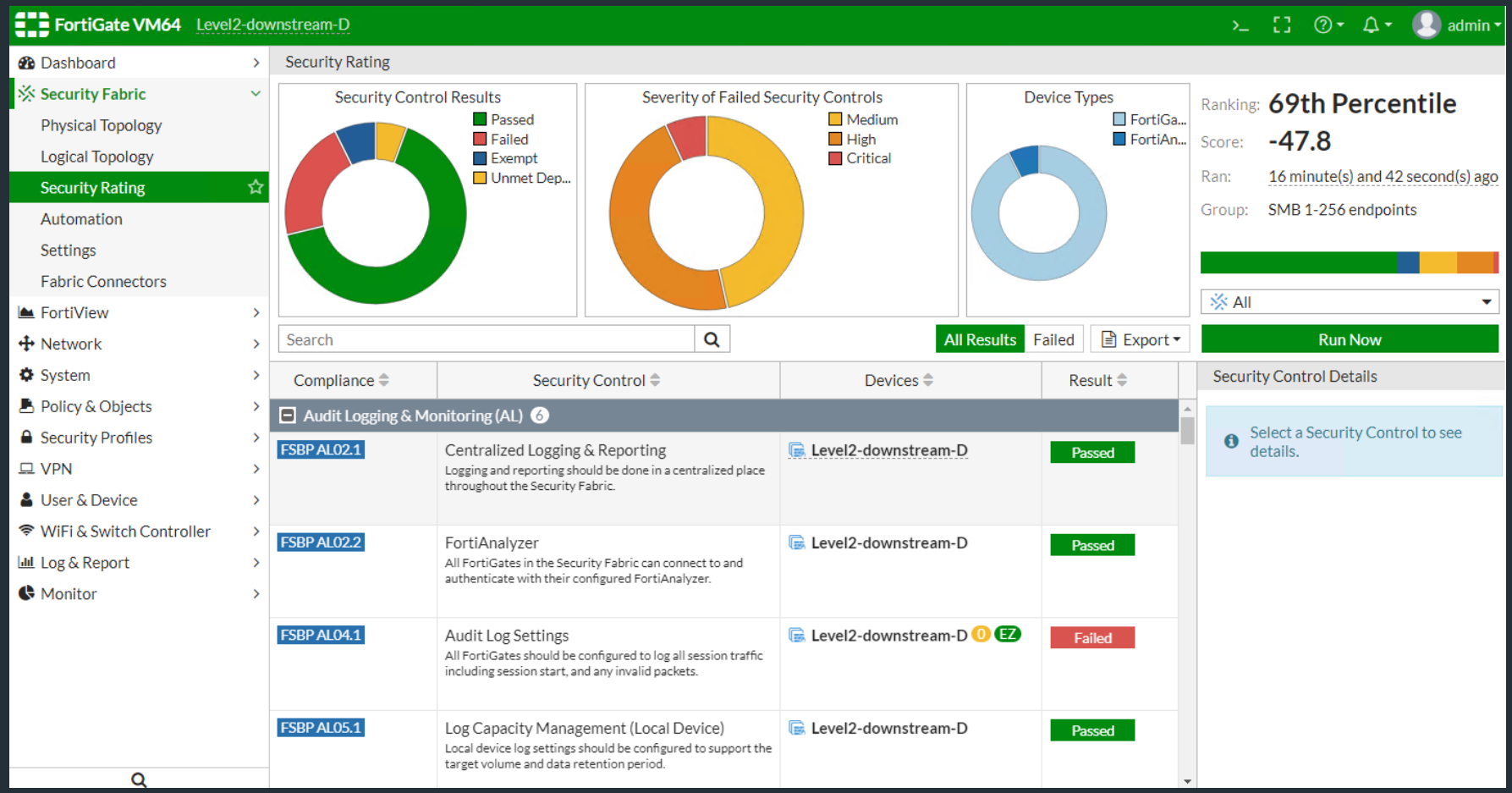
- Коллекция лучших практик от заказчиков
- Примеры
  - Безопасность паролей
  - Пороги срабатывания попыток входа
  - Логирование на FortiAnalyzer
  - Использование 2-х факторной аутентификации
- Система сравнивает соответствие всем лучшим практикам
- Приоритезирует найденное по уровню важности от критической до низкой
- Доступны быстрые пресеты для настройки

354 Passed | 25 Low | 65 Medium | 31 High | 22 Critical

FORTINET

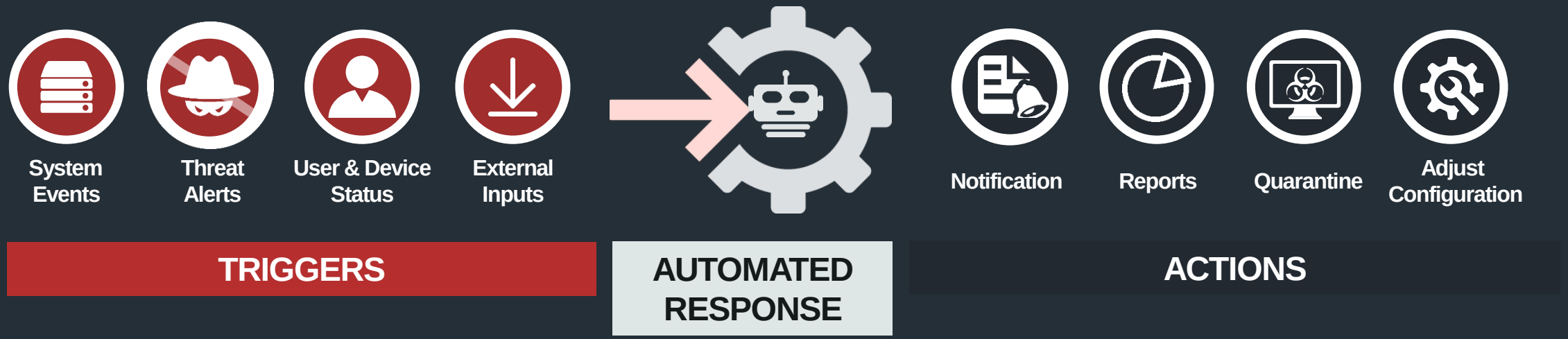
Рейтинг безопасности и сравнительный анализ

- Сравнительный анализ по рейтингу безопасности
  - Сравнение с аналогичными организациями по размеру и индустрии по процентилям
- Представление графика трендов
  - Путем получения исторических данных из FortiAnalyzer



Автоматизация процессов

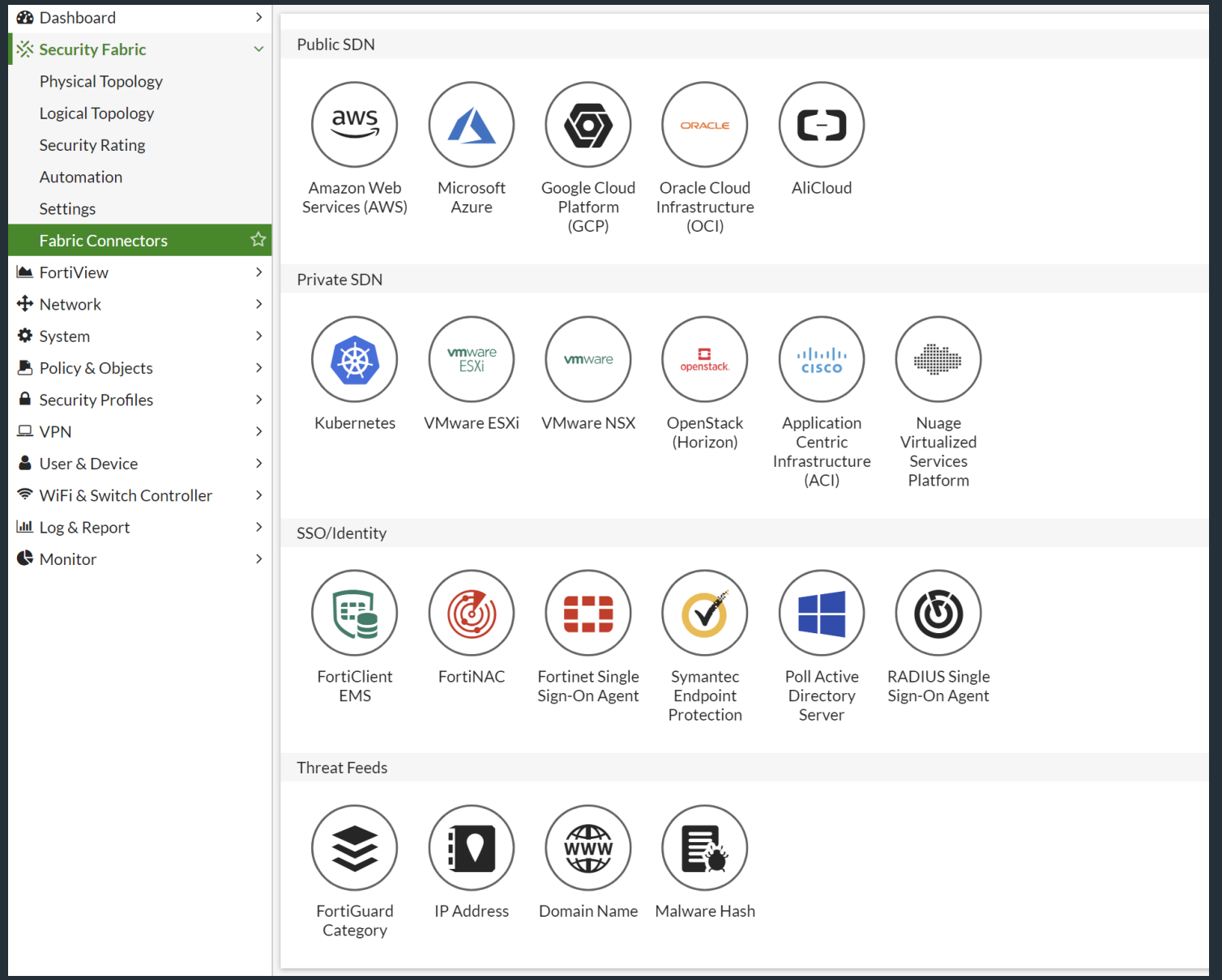
Automation



- Автоматизированные операции (stitches) используют триггеры для выполнения действий
  - » Легко создаются с помощью графических помощников (wizard)
  - » Работают с компонентами внутри Security Fabric

Глубокая интеграция с помощью Fabric Connectors

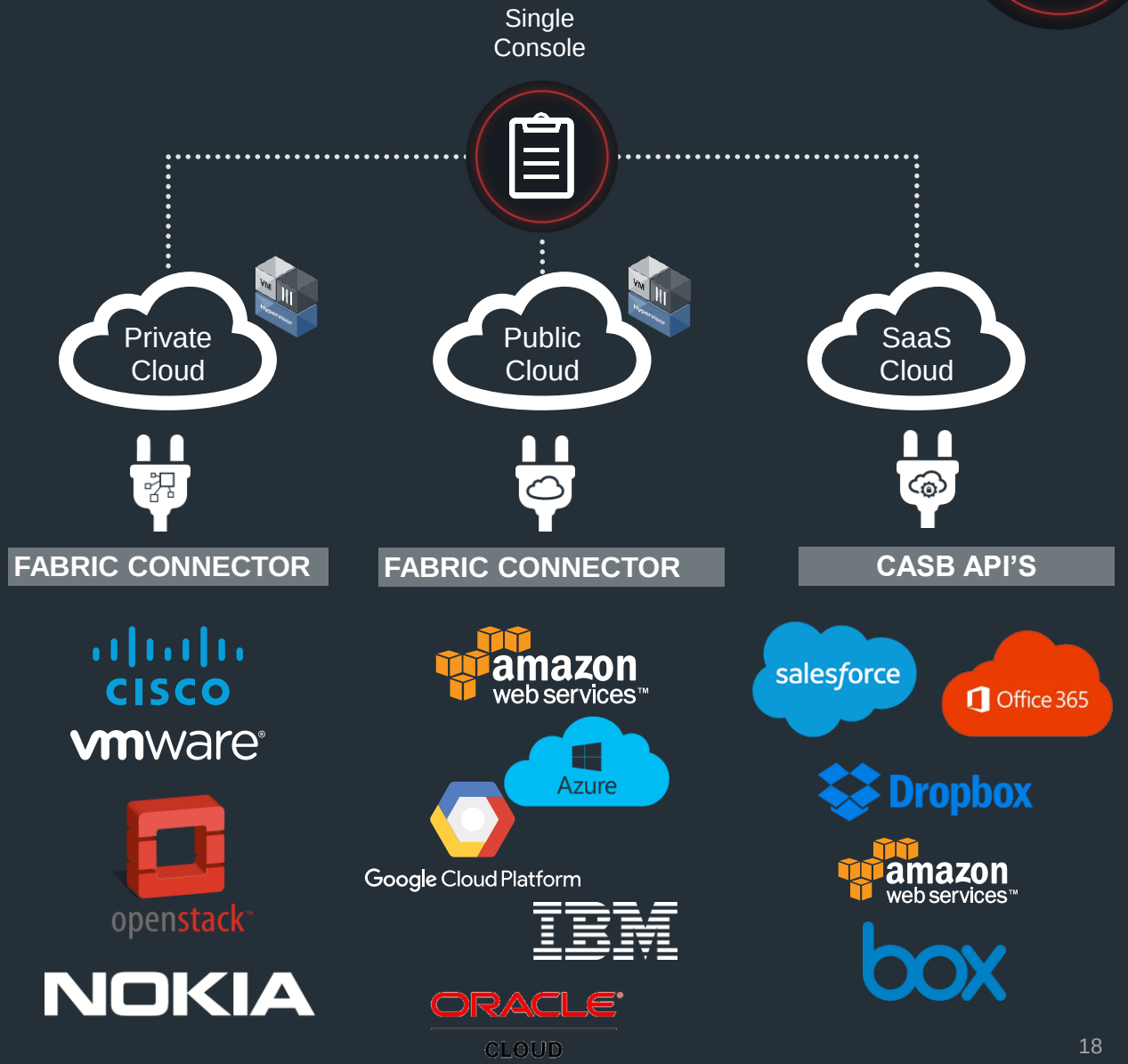
- Fabric Connectors обеспечивают глубокую интеграцию
- Существуют разные типы Fabric Connectors
- Все они доступны через GUI



Мультиоблачные коннекторы безопасности

Connectors

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



FORTINET

Партнерство в программе Fabric Ready

Fabric Ready Partners

CLOUD

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

SDN

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

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 CONTINUOUS SECURITY
- 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

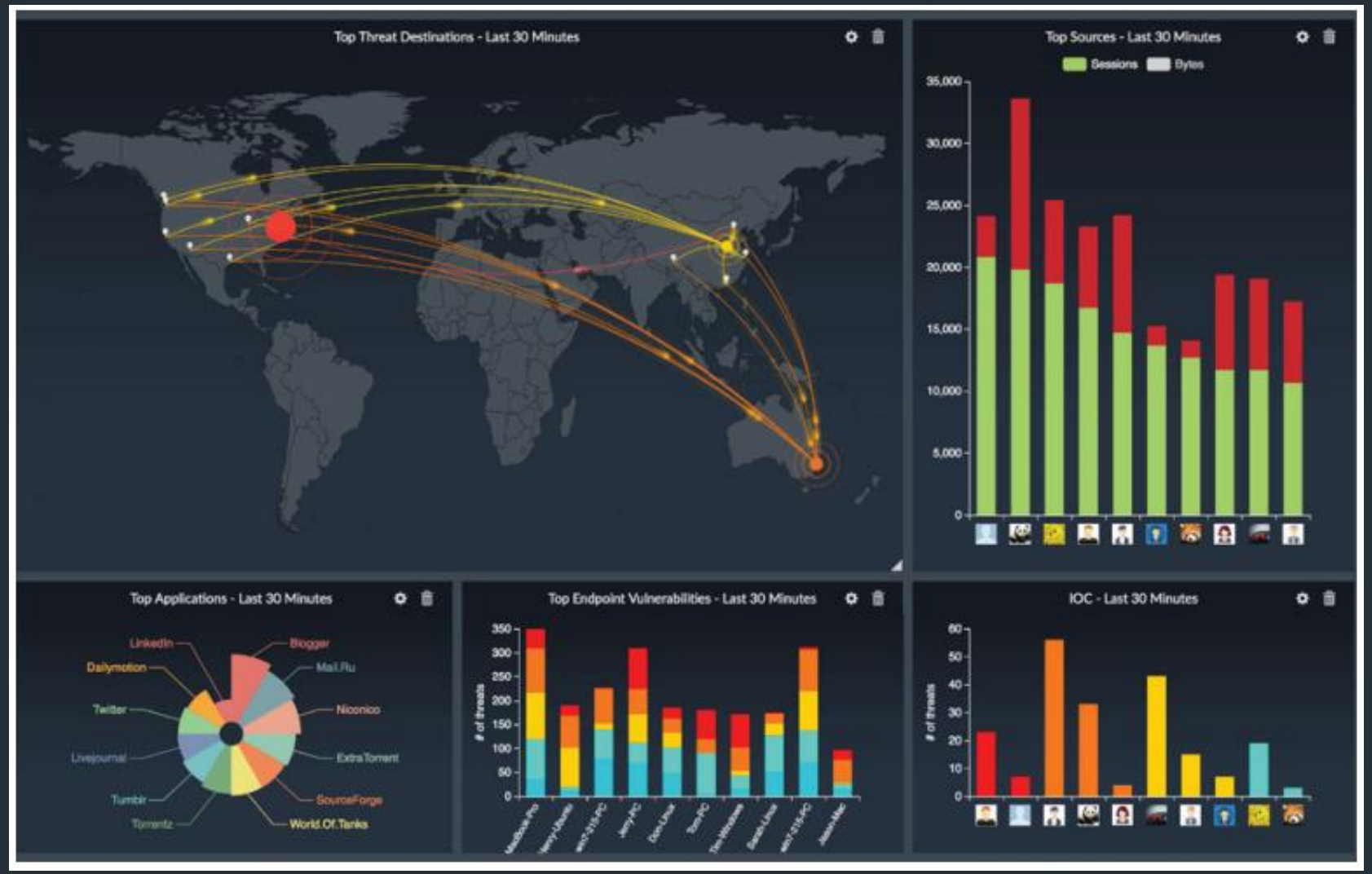
TECHNOLOGY

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

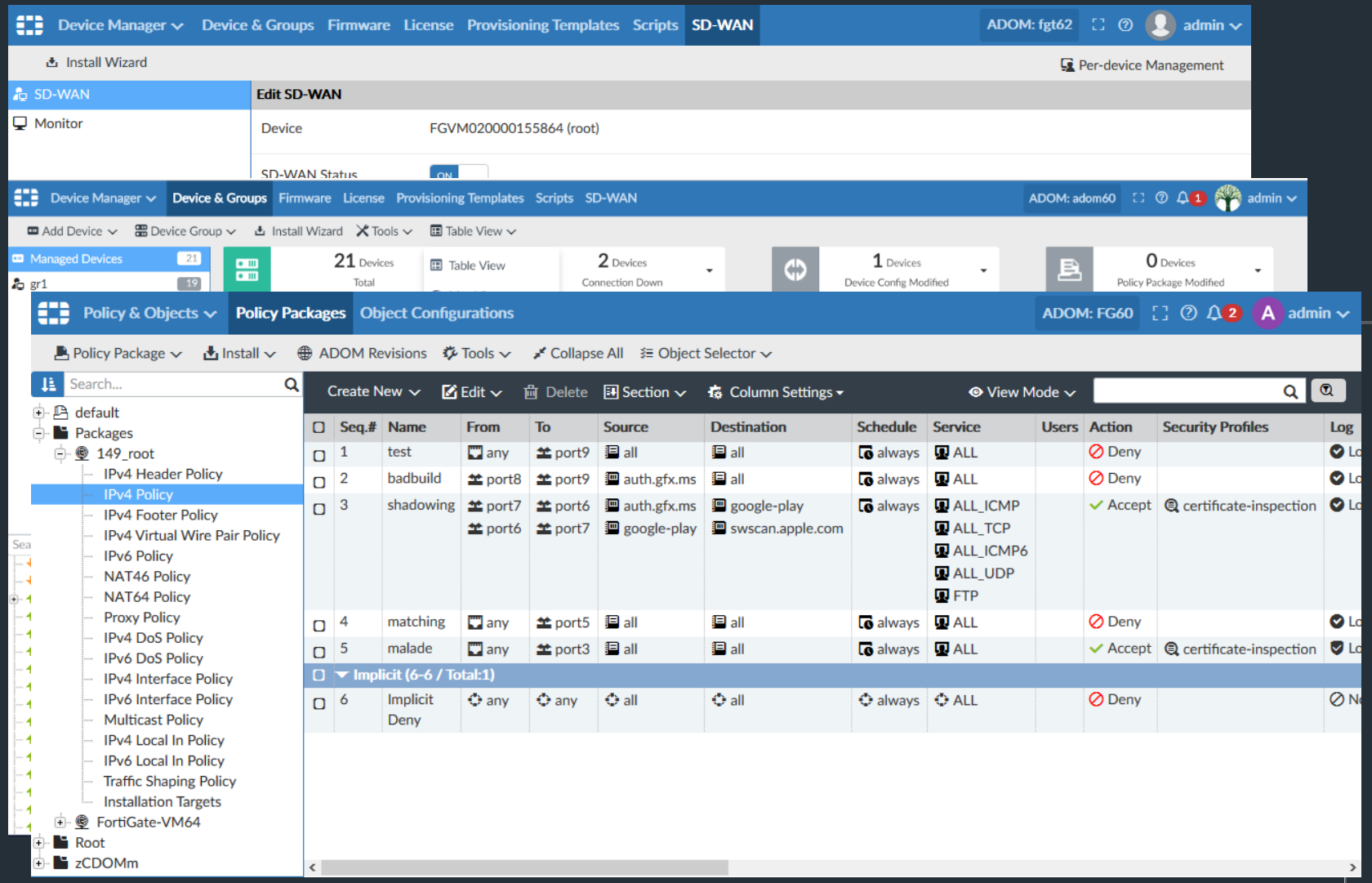
FORTINET

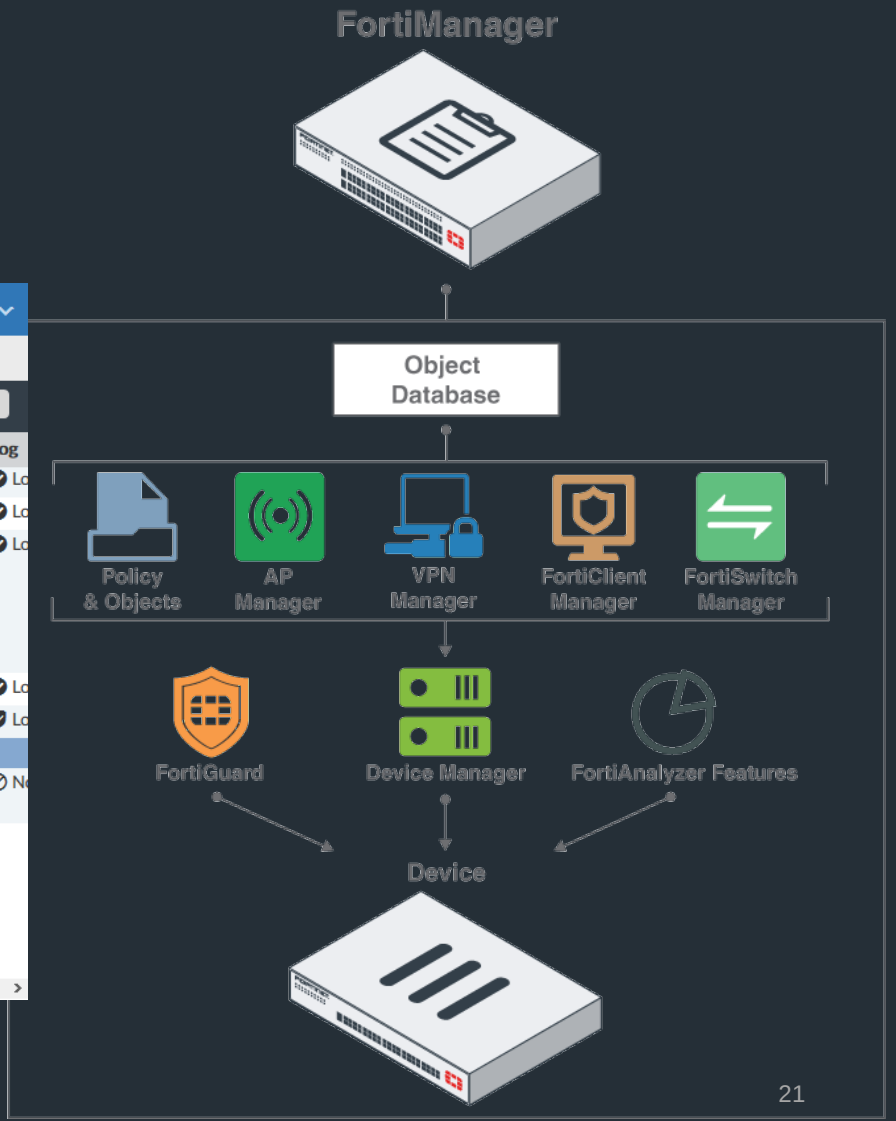
FortiAnalyzer – Сбор логов и анализ в Security Fabric

- Автоматизированное управление логами и анализ угроз в real-time
- Упрощение расследования инцидентов, ускорение реагирования на инциденты



FortiManager – Централизованное управление и развертывание

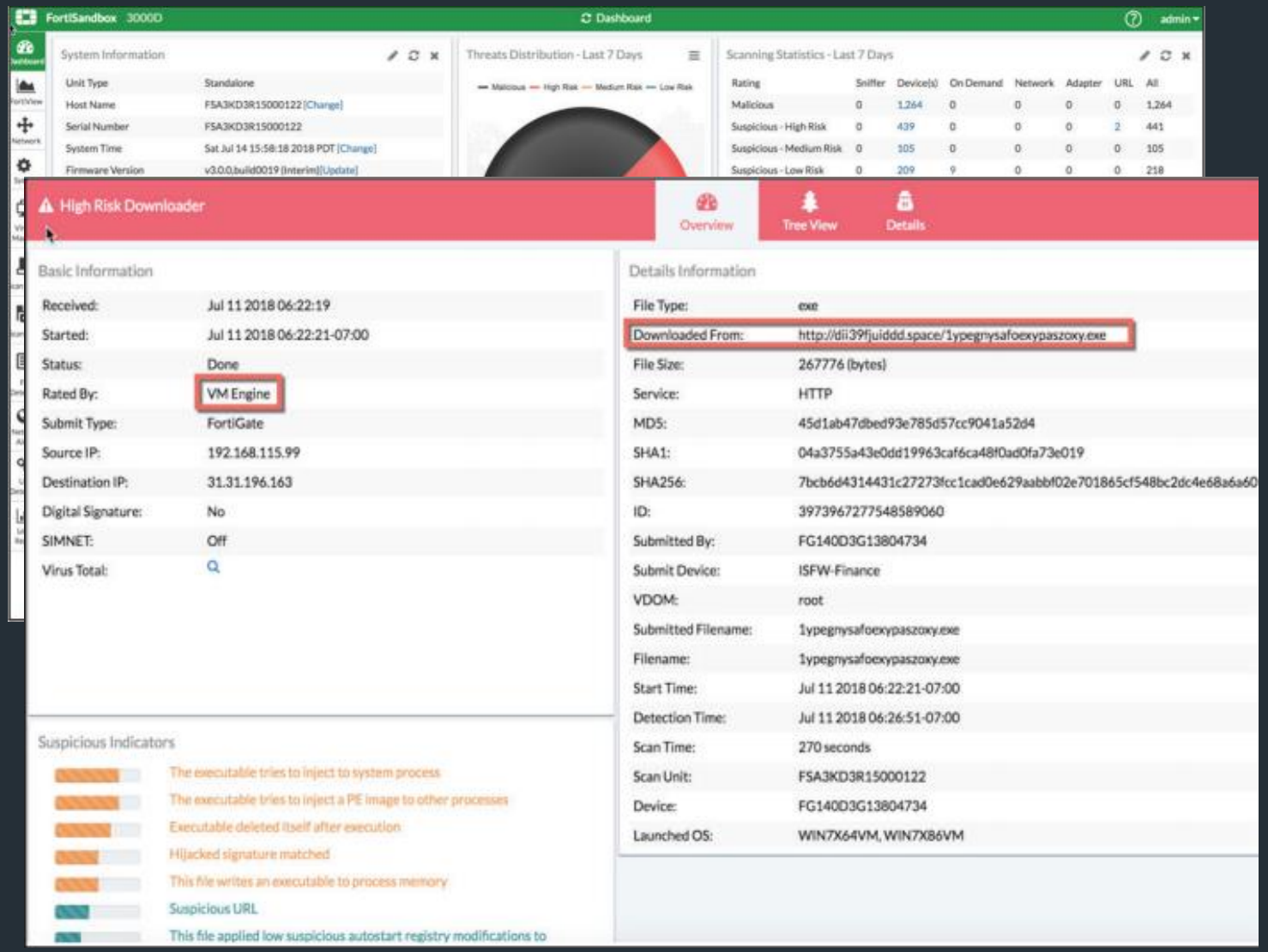




FortiSandbox – Защита от угроз нулевого дня топ-уровня !

Автоматизированное обнаружение и подавление угроз нулевого дня

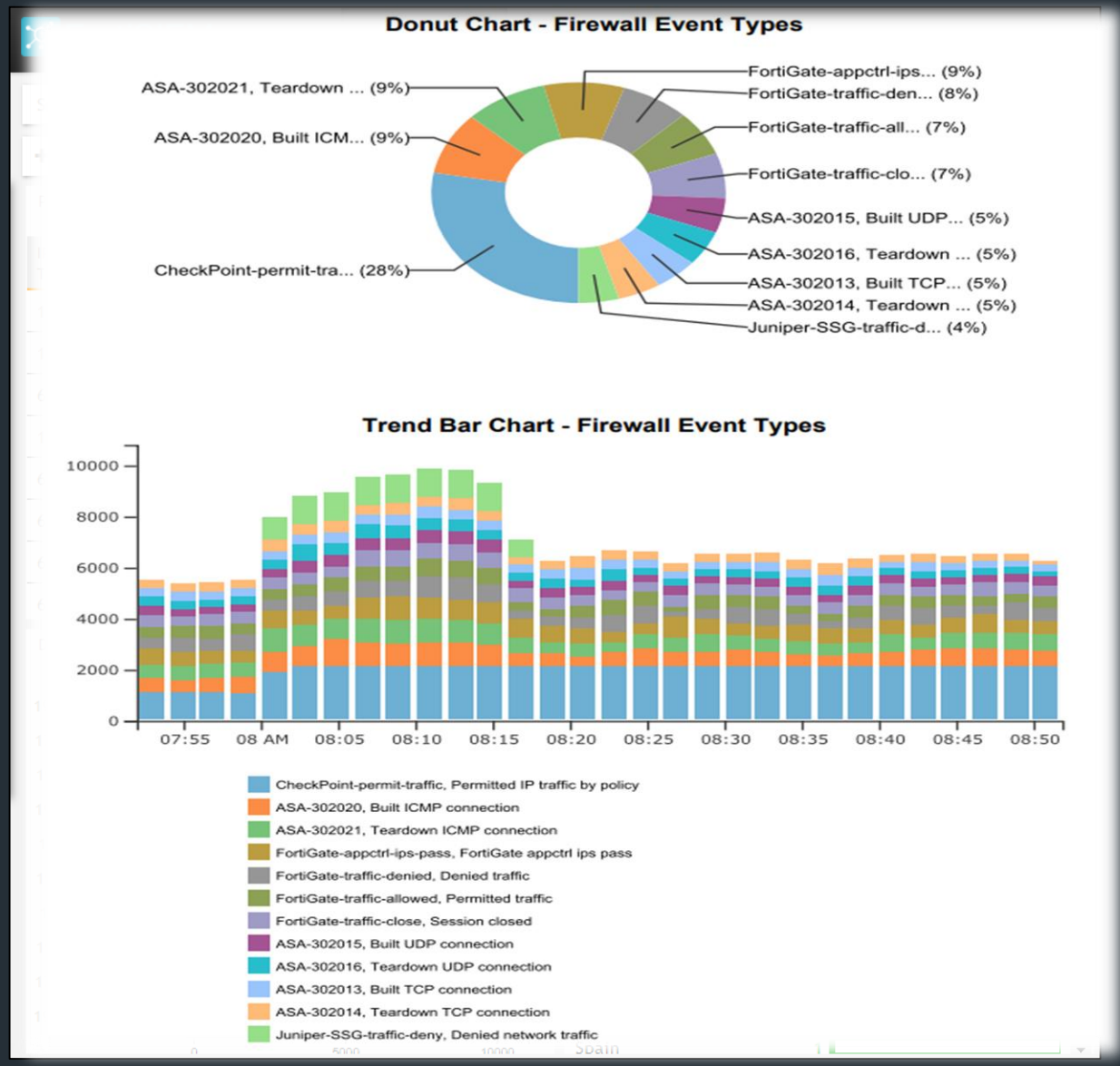
- Родная интеграция и наличие открытого API
- Проверка объектов от Security Fabric и сторонних устройств
- Возможность поделиться информацией об обнаруженных угрозах в реальном времени для незамедлительного реагирования с целью предотвращения атаки



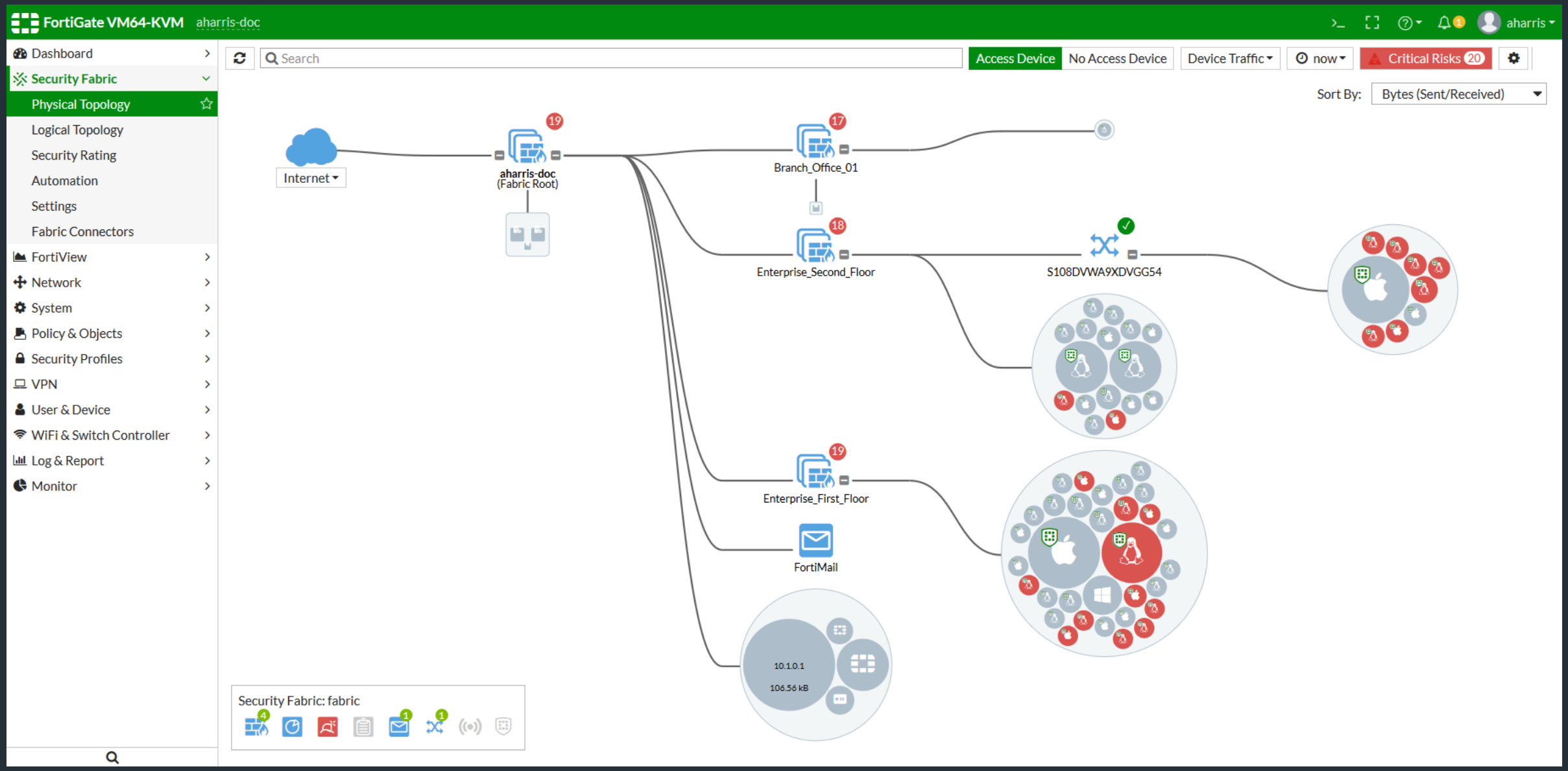
FortiSIEM - Security Information and Event Management

Унифицированная корреляция событий и инцидентов, управление рисками для современных сетей

- Быстрое обнаружение и реагирование на инциденты
- Управление и мониторинг безопасности, производительности и соответствия требованиям



Security Fabric Topology View



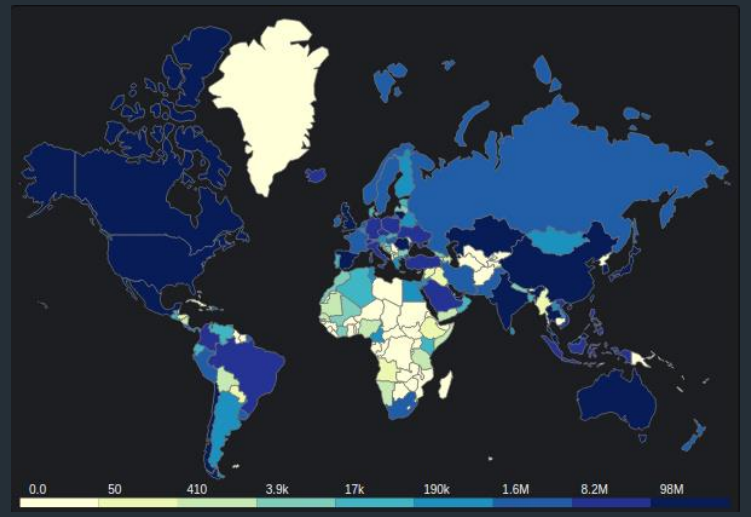

FortiGuard
Threat Intelligence
Service

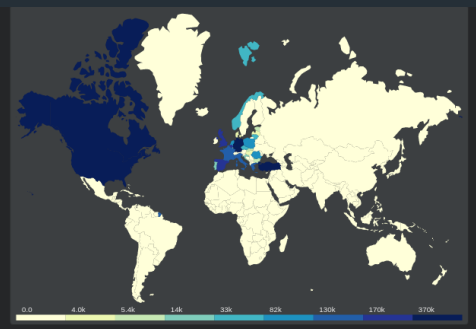
FortiGuard Threat Research & Response

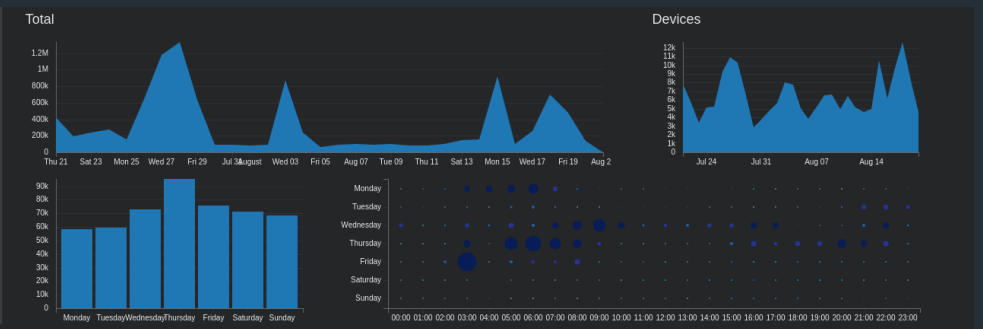
Глобальный центр исследования и реагирования киберугроз

Глобальная видимость

- Глобальная сеть сенсоров
- 4.4 M устройств в сети сенсоров !
- Глобальная сеть раннего предупреждения







Region Name	FG Count	Total
Asia	37,908	9,486,462
North America	38,388	8,070,291
Europe	11,471	3,187,615
Africa	521	461,738
South America	1,487	305,924
Oceania	802	177,982
Region 1	759	169,107

Top Countries — Count: 28

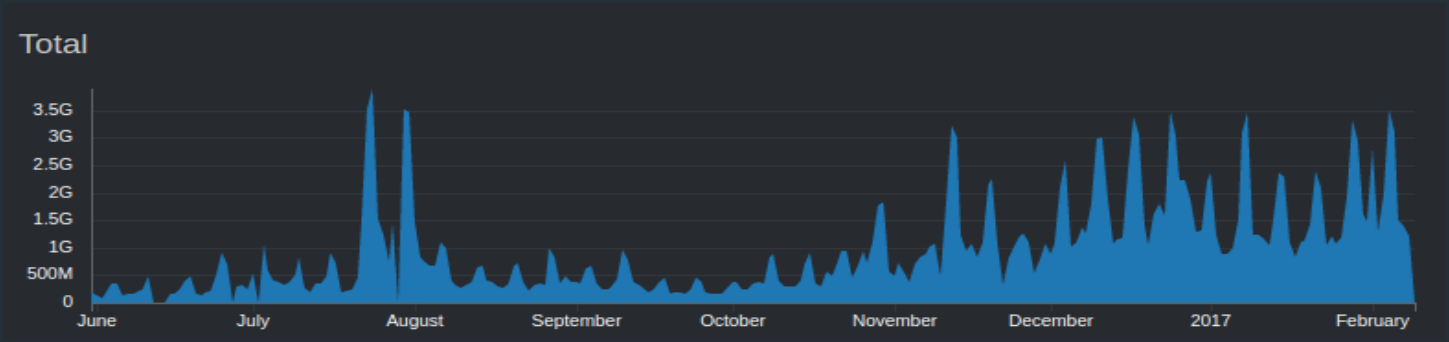
Country Code	Country	FG Count	Total
US	United States	38,156	7,165,008
TR	Turkey	1,183	611,604
CA	Canada	1,375	409,926
DE	Germany	1,558	365,218
ES	Spain	736	261,270
BE	Belgium	556	231,435
GB	United Kingdom	802	172,319
GR	Greece	109	161,592
IT	Italy	733	130,122
FR	France	1,145	129,444

Top Names — Count: 4,989

Name	FG Count	Total
JS/Nemucod.ANO!tr	4,229	1,222,870
JS/Nemucod.AOT!tr	6,873	854,760
WM/Agent.BJC!tr.dldr	10,340	851,746
WM/Agent.BOJ!tr.dldr	6,945	765,617
HTML/Refresh.BC!tr	6,917	670,939
JS/Nemucod.DRY!tr.dldr	4,845	610,478
JS/Nemucod.25A0!tr.dldr	5,525	552,970
WM/Agent!tr	5,731	518,566
JS/Nemucod.0971!tr	2,548	367,988
Adware/AdExchange	7,893	230,832

Top Serials — Count: 45,875

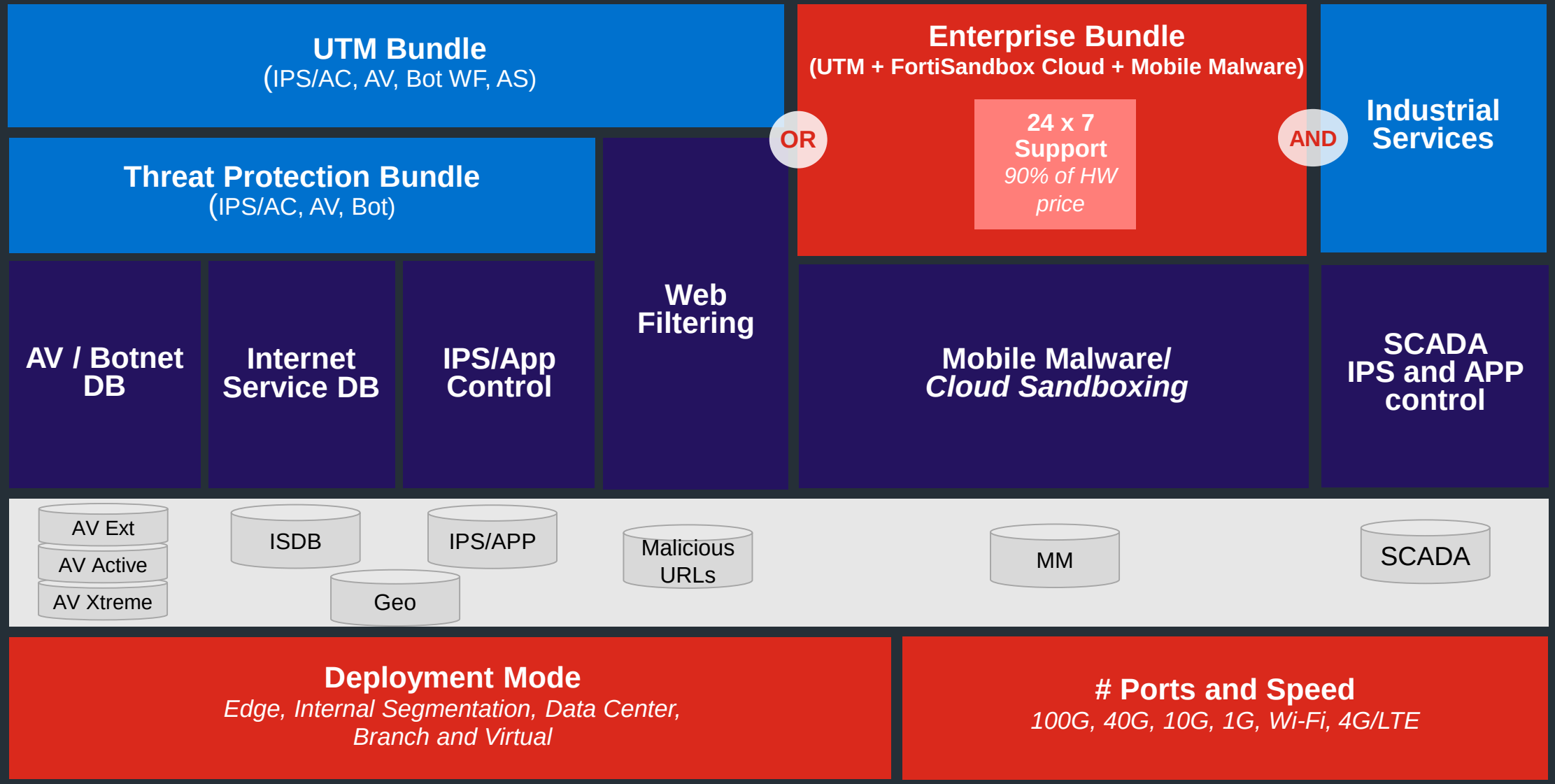
Serial ID	Unique Names	Total
11914	288	158,740
16851	30	150,668
44597	6	112,456
1683036	21	110,820
16741	8	108,568
220740	7	106,719
686	17	103,348
1712873	8	101,867
13025	12	101,853
13922	9	100,723



Партнерство FortiGuard Threat Intelligence

CISCP
& NCCIC

Сервисы FortiGuard Services для FortiGate



Подписки FortiGuard для FortiGate (2020Q1 Bundles)

1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 6.2

	Advanced Threat Protection (ATP)	Unified Protection (UTM)	Enterprise Protection (ENT)	360 Protection
FortiManager Cloud [2]				✓
FortiAnalyzer Cloud [2]				✓
SD-WAN Cloud Assist Monitoring [2]				✓
SD-WAN One Click VPN Overlay [2]				✓
FortiConverter Service				✓
Industrial Security Service			✓	✓
FortiGuard Security Rating Service			✓	✓
FortiCASB			✓	✓
FortiGuard Anti-Spam Service		✓	✓	✓
FortiGuard Web Filtering Service		✓	✓	✓
FortiGuard Advanced Malware Protection (AMP) - Antivirus, Botnet IP/Domain Service, Mobile Malware Security, FortiSandbox Cloud, Virus Outbreak Protection Service and Content Disarm & Reconstruct	✓	✓	✓	✓
FortiGuard IPS Service	✓	✓	✓	✓
FortiCare (incl. Internet Service DB, Client ID DB, IP Geography DB, Malicious URL DB, URL Whitelist DB) + Application Control	*24x7*	*24x7*	*24x7*	*ASE [1]*

FORTINET

Сертификация по требованиям ФСТЭК России

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4222

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
11 февраля 2020 г.

Выдан: 11 февраля 2020 г.
Действителен до: 11 февраля 2025 г.

Настоящий сертификат удостоверяет, что **программно-аппаратный комплекс «FortiGate», функционирующий под управлением операционной системы FortiOS версии 6.X**, разработанный компанией Fortinet и производимый АО «НИЦ», является программно-аппаратным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции системы обнаружения вторжений и межсетевого экрана, соответствует требованиям по безопасности информации, установленным в документах «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Б четзертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012) при выполнении указаний по эксплуатации, приведенных в формуляре ЦТНВ-26.20.40.140-011 ФО.

Сертификат выдан на основании технического заключения от 18.12.2019, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО «ИИАТ» (аттестат аккредитации от 27.02.2018 № СЗИ RU.0001.01БИ00.Б027), и экспертного заключения от 27.12.2019, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

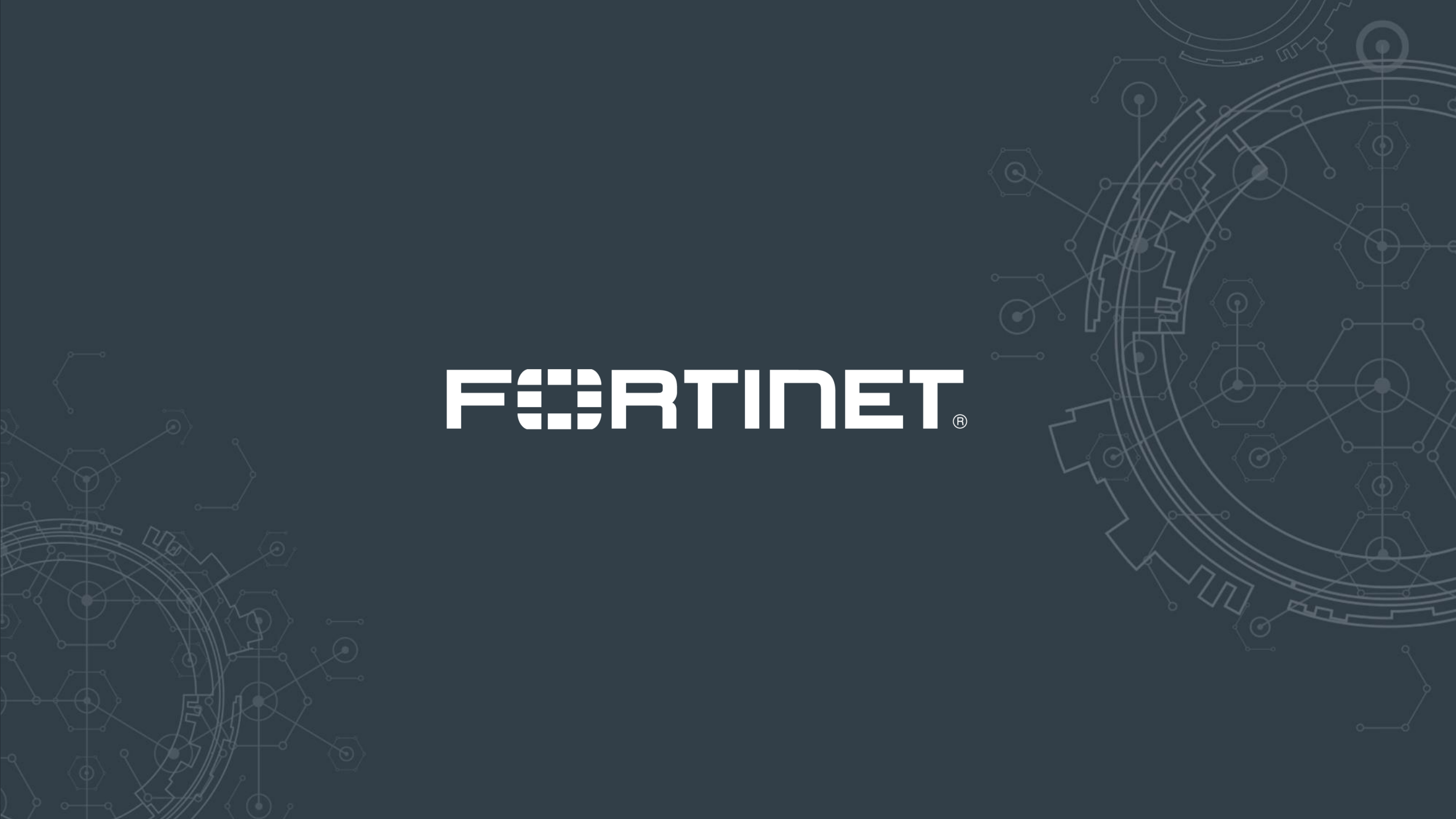
Заявитель: АО «НИЦ»
Адрес: 117246, г. Москва, Научный проезд, д. 6, эт. 1, пом. 1, ком. 32
Телефон: (495) 204-2086

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Модельный ряд:

- FortiGate-30E-LENC
- FortiGate-60E-LENC
- FortiGate-100E-LENC
- FortiGate-301E-LENC
- FortiGate-501E-LENC
- FortiGate-1500D-LENC
- FortiGate-2500E-LENC
- FortiGate-3960E-LENC
- FortiGate-3980E-LENC
- FortiGate-6301F-LENC
- FortiGate-6501F-LENC


FORTINET