

# FORTINET® SECURITY DAY

VIRTUAL

## Платформенный подход к кибербезопасности

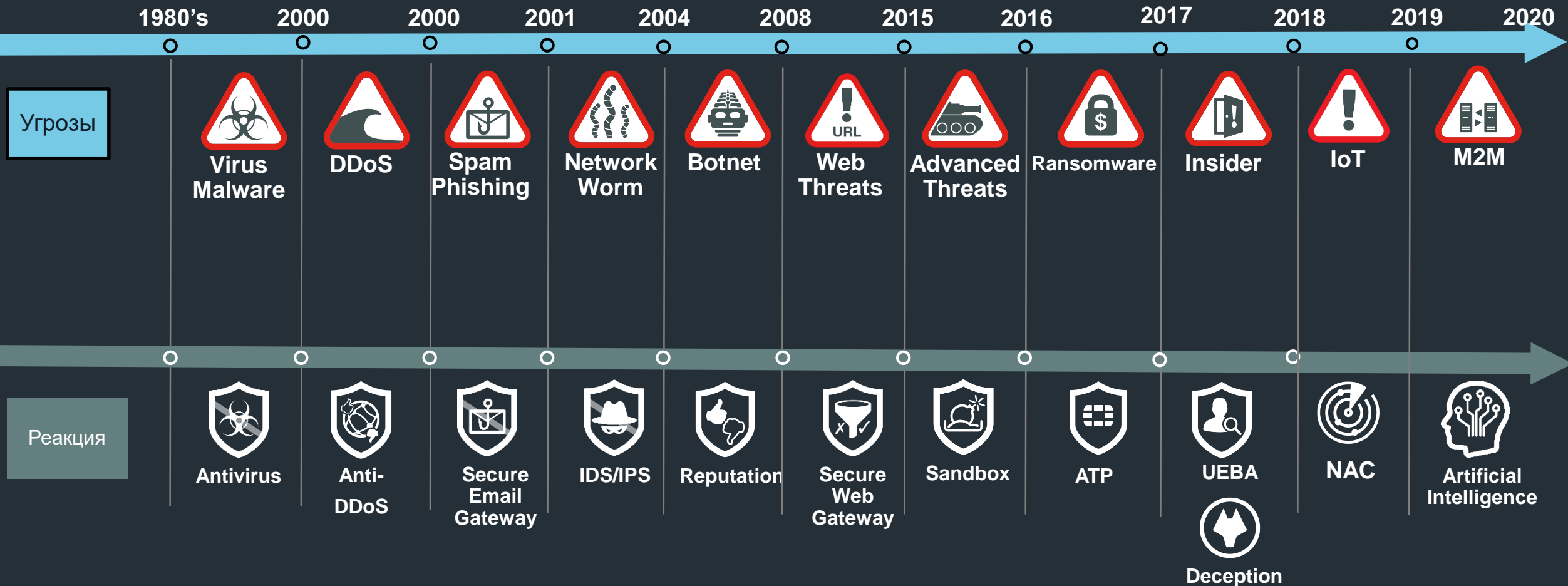
**Алексей Андрияшин**

[aandriyashin@fortinet.com](mailto:aandriyashin@fortinet.com)

Технический директор Fortinet в России и странах СНГ

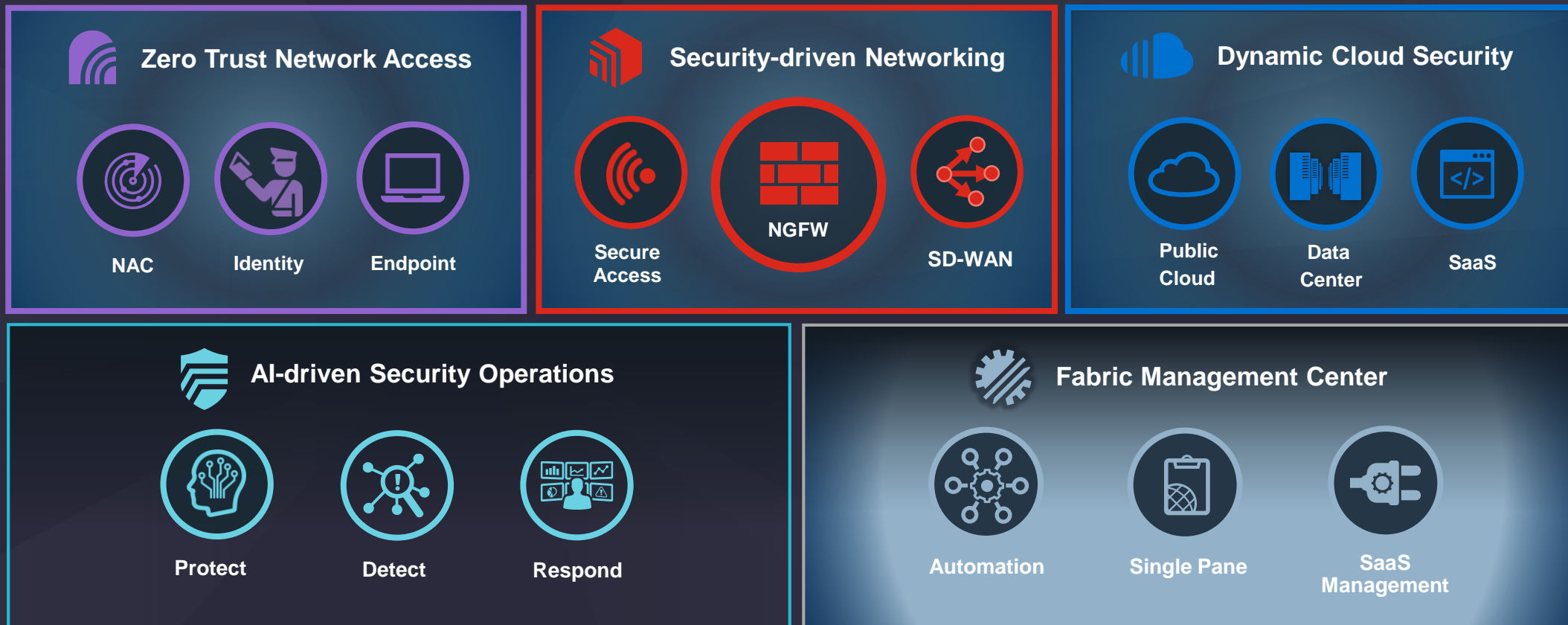
# Эволюция угроз

Постоянное расширение поверхности атак

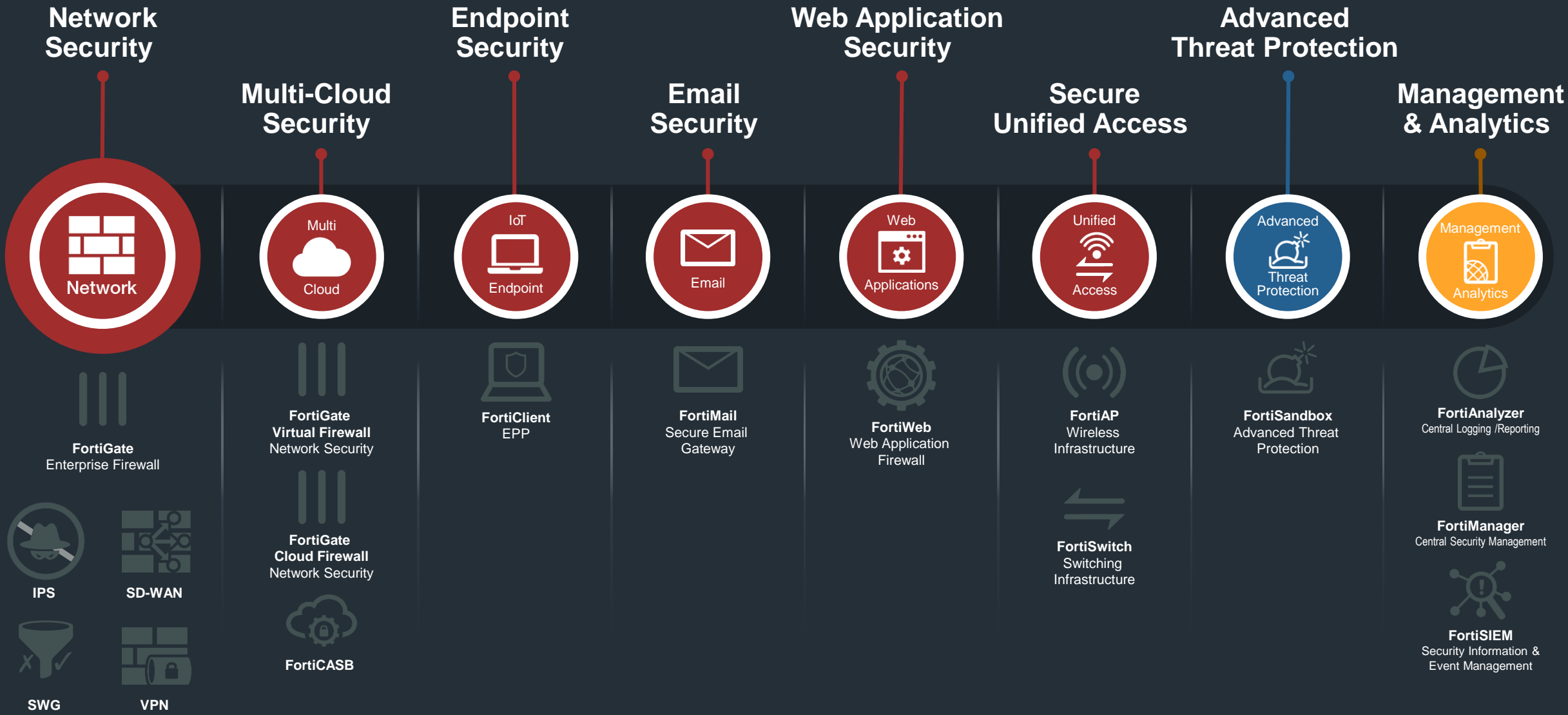




# Платформа кибербезопасности Fortinet



# Непрерывная цепь решений



# Безопасность как основа сети



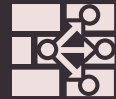


# Базовые решения построения фундамента ИБ

## FORTIOS



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



Accelerates  
Network  
Traffic

CPU

Flexible  
Policy



Accelerates  
Content  
Inspection



Optimized for entry-level  
form factors



More Performance



Less Latency



Less Power



Less Space

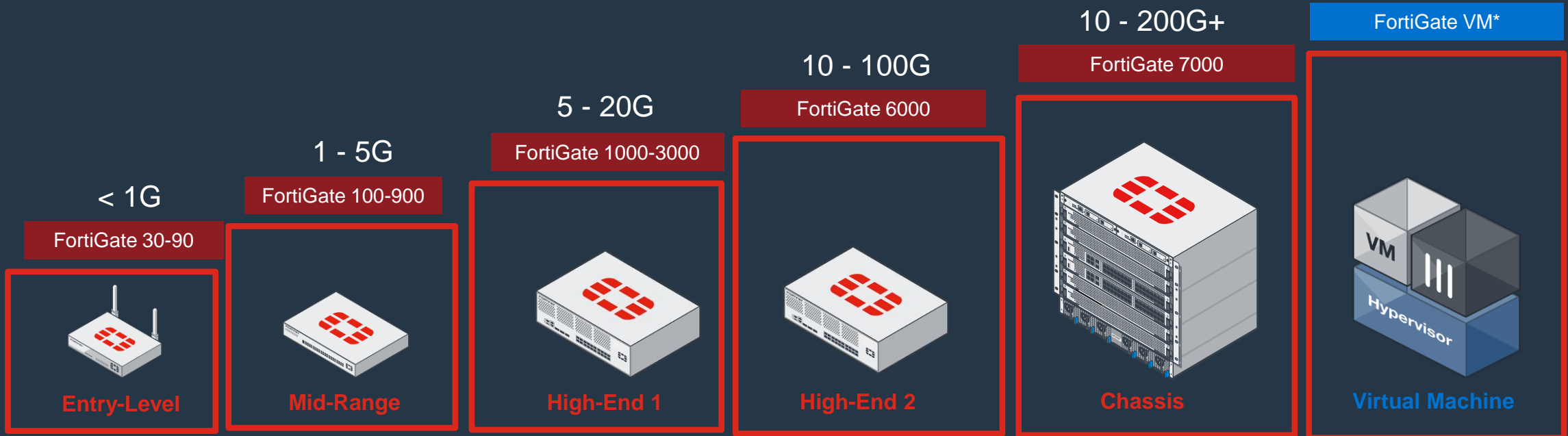
# Решения сетевой безопасности Fortinet



До 110Gbps SSL инспекции



До 100Gbps предотвращения угроз



N x



N x



N x



N x



N x



N x



N x

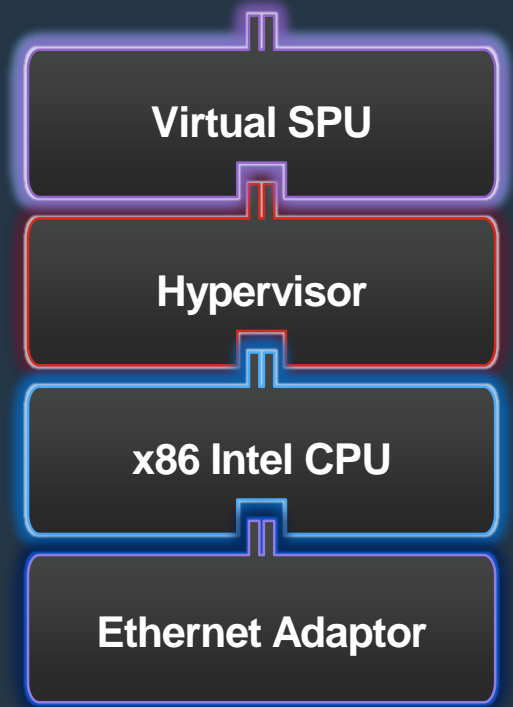
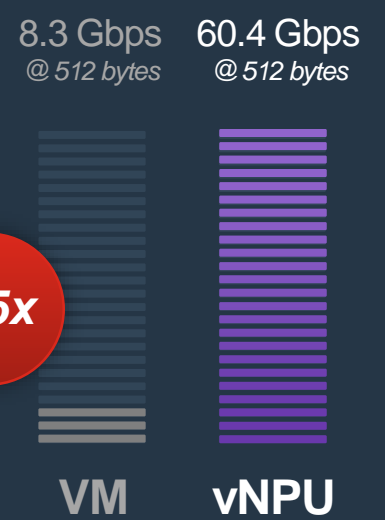
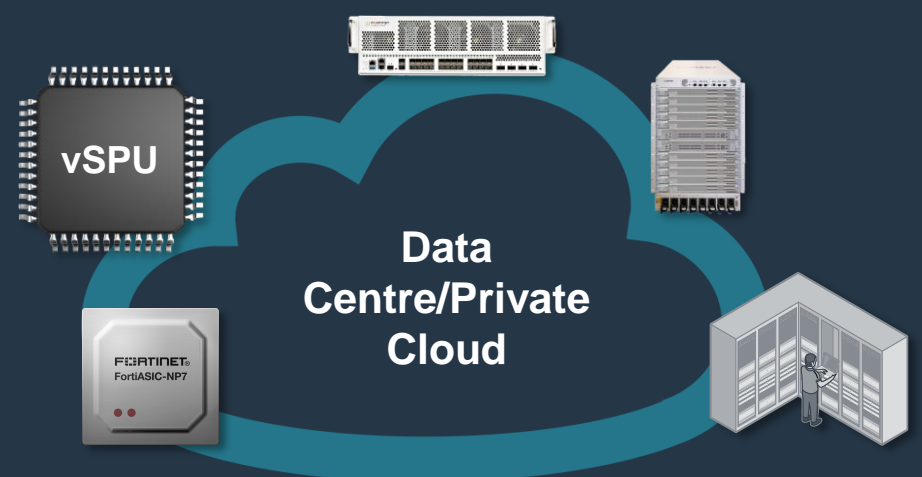


\*Стороннее оборудование



# FortiGate-VM

FortiGate VM



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

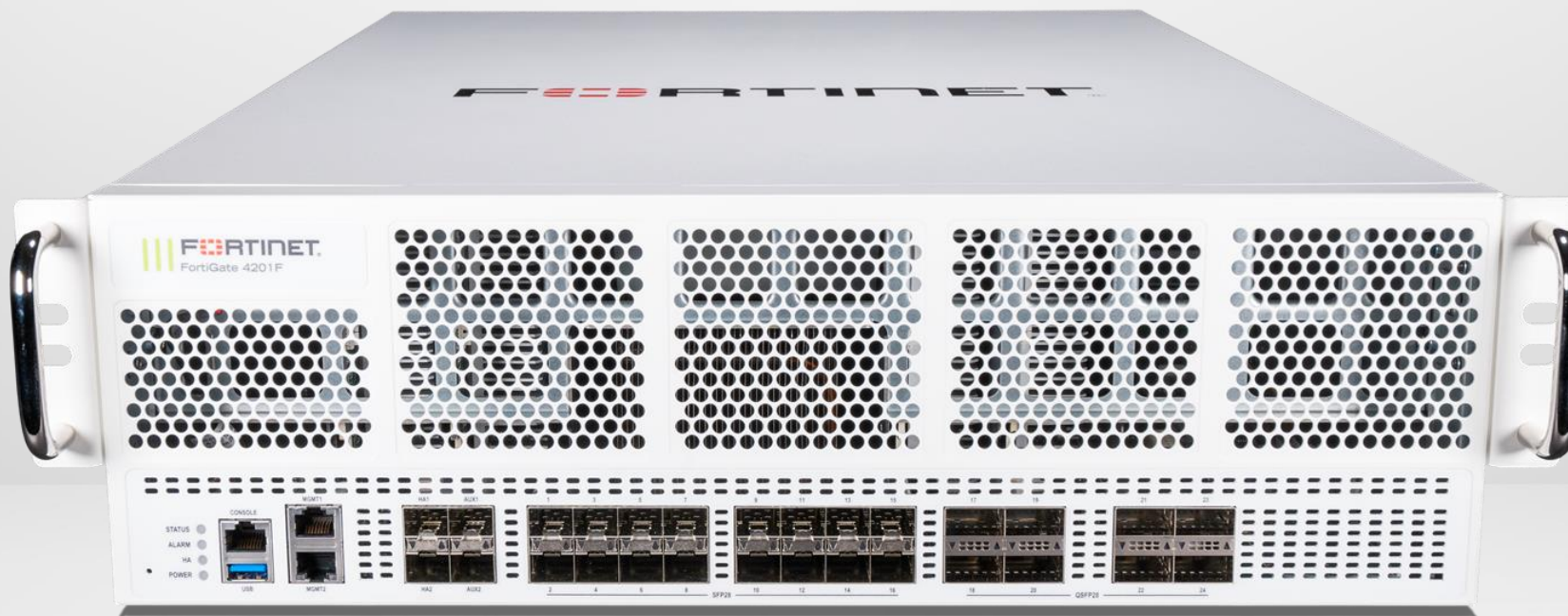
### Характеристики

- 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

800 Gbps



Zero CPU Forwarding

7M CPS

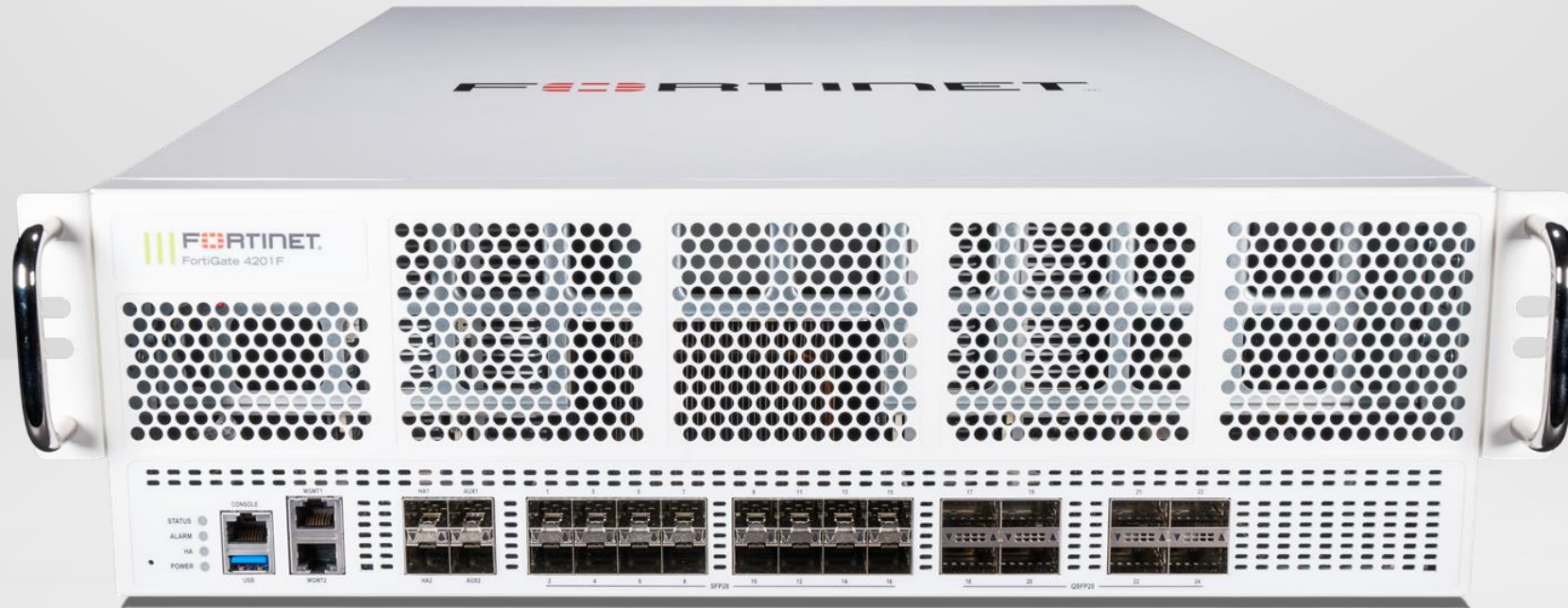


Connections/sec  
(with Hyperscale License)



# 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



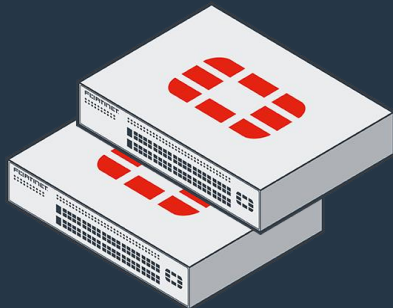
# Сетевая безопасность: NGFW



Сегментация

FortiGate

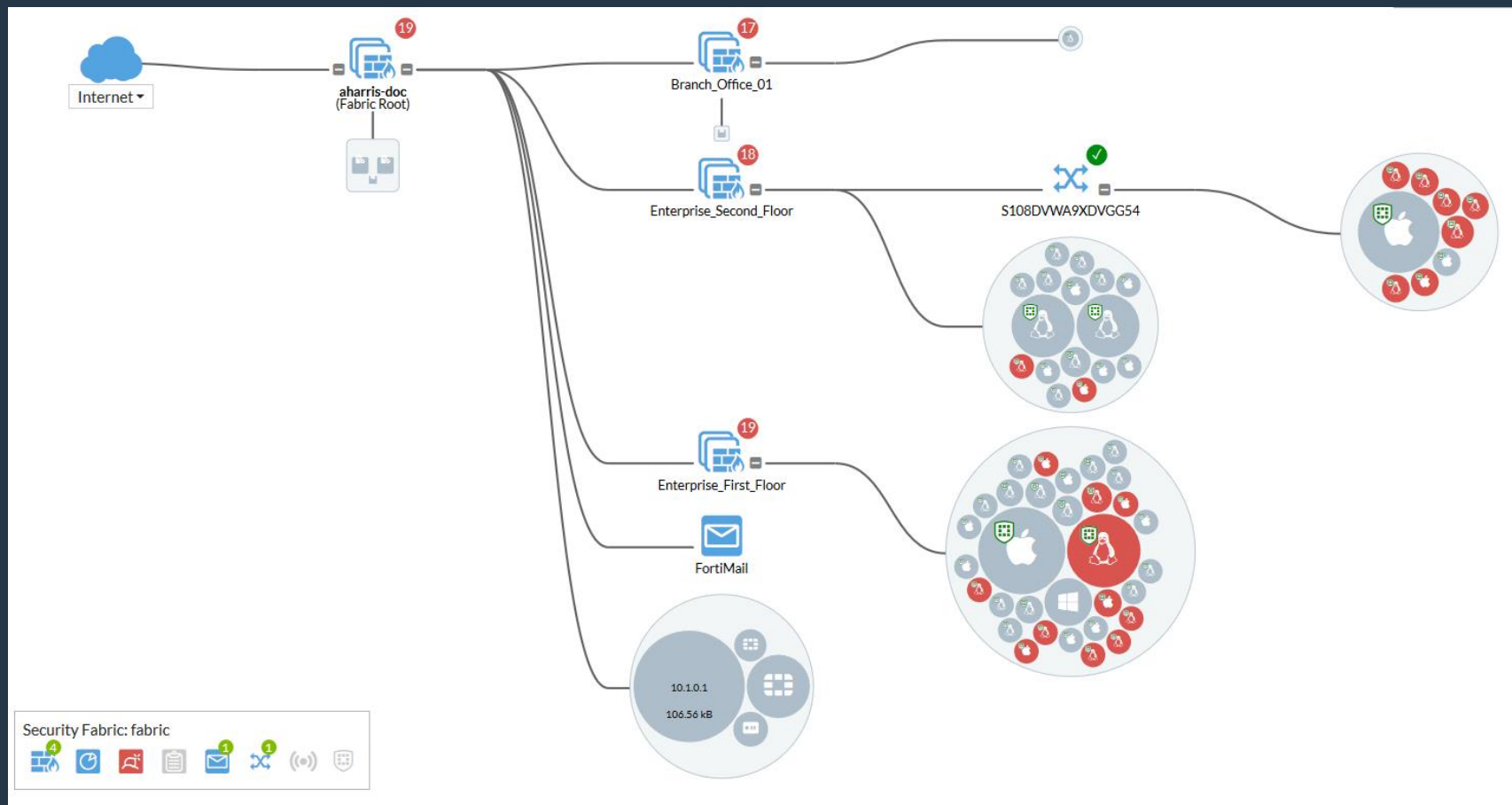
NGFW



## FortiGate

FortiGate 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

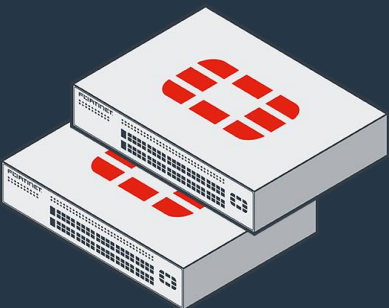
## NGFW

## SD-WAN



Масштабируемость и легкость развертывания

Беспрецедентная интеграция и видимость



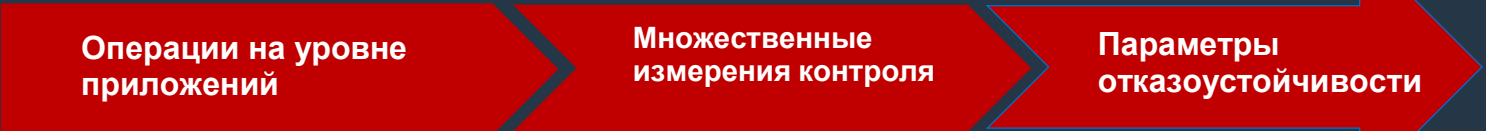
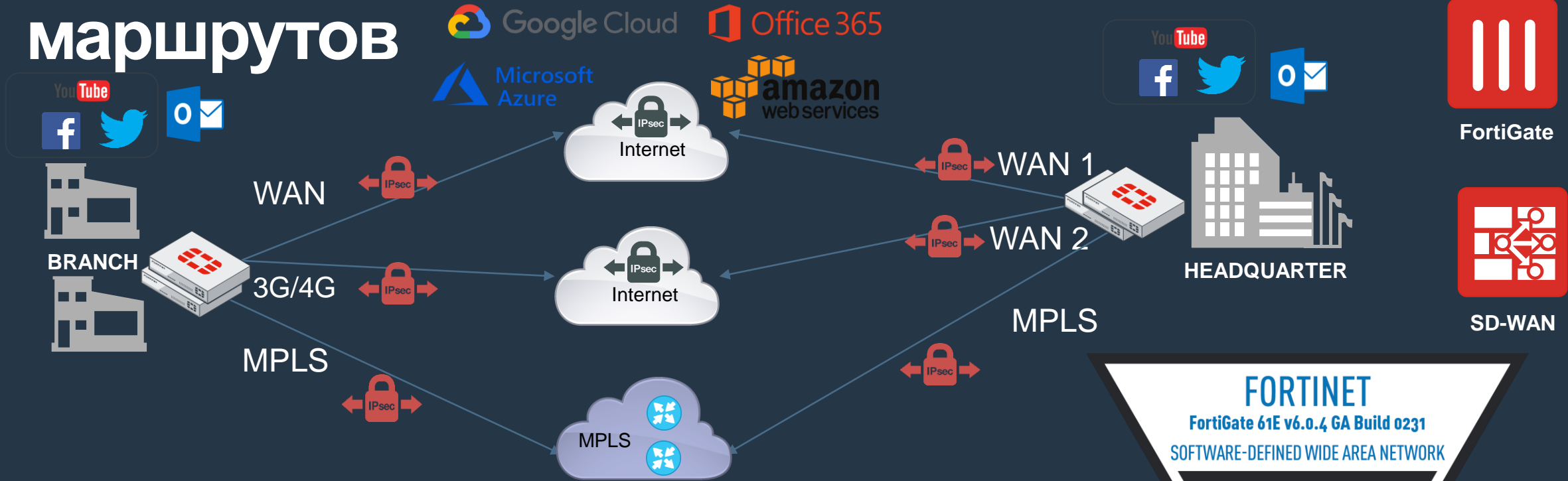
FORTINET





# SD-WAN интеллектуальный выбор маршрутов

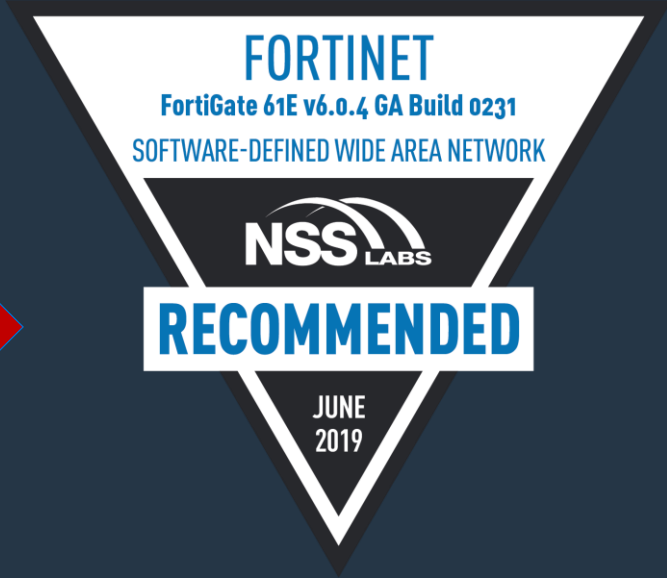
## маршрутов



- Операции на уровне приложений
- Latency < 200ms
  - Latency < 100ms
  - AND
  - Packet Loss < 1%
  - AND
  - Jitter < 30ms

- Множественные измерения контроля
- Ping
  - HTTP
  - TCP Echo
  - UDP Echo
  - TWAMP

- Параметры отказоустойчивости
- Check Interval
  - Failure before inactive
  - Success before restore



# 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

Figure 1. Magic Quadrant for WAN Edge Infrastructure



As of September 2020 © Gartner, Inc

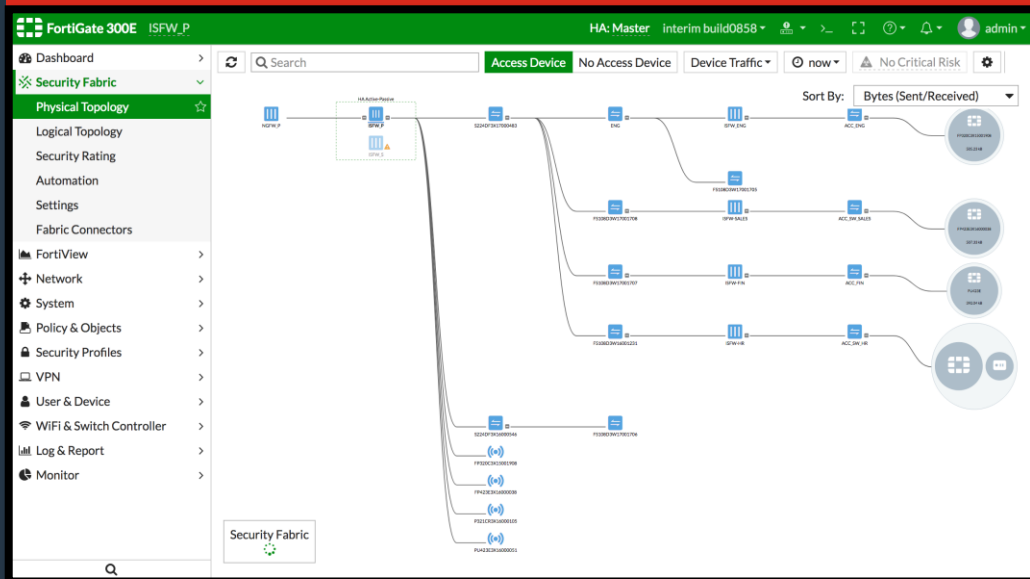
Source: Gartner (September 2020)

# 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

Access Point	Connected Via	SSIDs	Channel	Clients	OS Version	AP Profile
FP320C3X140078	192.168.10.101	Radio 1: Radio 2: 136	Radio 1: 1 Radio 2: 1	Radio 1: 0 Radio 2: 1	FP320C-v5.6-build04	
PS323C3U150004	192.168.4.100	Radio 1: Radio 2: 165	Radio 1: 1 Radio 2: 0	Radio 1: 0 Radio 2: 0	PS323C-v5.6-build03	
FP320C3X140120	192.168.107.100	Radio 1: Radio 2: 132	Radio 1: 11 Radio 2: 1	Radio 1: 0 Radio 2: 1	FP320C-v5.6-build04	
FP320C3X150019	192.168.101.2	Radio 1: Radio 2: 20	Radio 1: 1 Radio 2: 0	Radio 1: 0 Radio 2: 0	FP320C-v6.0-build00	
FP423E3X160000	192.168.103.2	Radio 1: Radio 2: 144	Radio 1: 1 Radio 2: 0	Radio 1: 0 Radio 2: 0	FP423E-v6.0-build00	
P321CR3X160001	192.168.104.3	Radio 1: Radio 2: 0	Radio 1: 0 Radio 2: 0	Radio 1: 0 Radio 2: 0	P321CR-v5.4-build01	
PU423E3X160000	192.168.102.1	Radio 1: Radio 2: 149	Radio 1: 1 Radio 2: 0	Radio 1: 0 Radio 2: 0	PU423E-v5.4-build00	
FP221B3X130102	20.20.20.22	Radio 1: Radio 2: 11	Radio 1: 36 Radio 2: 1	Radio 1: 0 Radio 2: 0	FP221B-v5.4-build03	
FP320B3X130031	20.20.20.23	Radio 1: Radio 2: 1	Radio 1: 0 Radio 2: 1	Radio 1: 0 Radio 2: 1	FP320B-v5.0-build06	
FP320C3X140098	20.20.20.21	Radio 1: Radio 2: 149	Radio 1: 11 Radio 2: 1	Radio 1: 0 Radio 2: 1	FP320C-v5.6-build04	

- 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**

Device: FG60DP4614001278

Port	TX	RX	Session	Health Check	Jitter (Actual/Config)	Latency (Actual/Config)	Packet Loss (Actual/Config)
wan1	7.8 MB	1.4 GB	2	<ul style="list-style-type: none"> <li>FortiVoice: 17% (16.71/100)</li> <li>Salesforce: 38% (11.52/30)</li> </ul>	60% (120.04/200) <td>0% / 10%</td>	0% / 10%	
wan2	0.0 KB	0.0 KB	0	<ul style="list-style-type: none"> <li>FortiVoice: Down</li> <li>Salesforce: Down</li> </ul>	Down	Down	Down

SLA by Application

Application	Port	Jitter	Latency	Packet Loss
FTNT-FortiGuard	INT (WAN 1)	0.32 ms	0.62 ms	0.00%
MS-Office 365	INT (WAN 1)	0.21 ms	0.51 ms	0.00%
MS-Skype	INT (WAN 1)	0.12 ms	0.62 ms	0.00%
Google-Gmail	INT (WAN 1)	0.43 ms	0.24 ms	0.00%
Amazon-Web	MPLS (WAN 2)	0.14 ms	0.17 ms	0.00%

Top Application by Bandwidth

Application	Upstream	Downstream
MS-Office 365	210/113 B/s	46/86 B/s
MS-Skype	104/89 B/s	35/15 B/s
Amazon-Web	78/54 B/s	27/45 B/s
Google-Gmail	33/65 B/s	16/54 B/s
FTNT-FortiGuard	27/52 B/s	12/46 B/s

Application Bandwidth

Application Bandwidth Usage (24 hours)

Device	SD-WAN	Rules					Upstream		Downstream	
		FTNT-FortiGuard	MS-Office 365	MS-Skype	Google-Gmail	Amazon-Web	80%	29%	102/350 B/s	462/550 B/s
Ottawa Office	INT (WAN 1)	Green	Green	Green	Green	Green	80%	29%	473/550 B/s	102/350 B/s
	MPLS (WAN 2)	Green	Green	Green	Green	Green	67%	84%	347/350 B/s	462/550 B/s
Las Vegas HR	INT (WAN 1)	Green	Green	Green	Green	Yellow	65%	55%	174/260 B/s	143/260 B/s
	MPLS (WAN 2)	Green	Green	Green	Green	Red	43%	74%	210/350 B/s	140/350 B/s
Porland Lab2	INT (WAN 1)	Green	Green	Green	Green	Green	78%	89%	497/828 B/s	265/828 B/s
	MPLS (WAN 2)	Green	Green	Green	Green	Green	29%	22%	143/275 B/s	140/275 B/s
New York	INT (WAN 1)	Green	Green	Green	Green	Green	65%	34%	153/221 B/s	180/263 B/s
	IPSec-DC	Green	Green	Green	Green	Red				





# Мониторинг состояния сети

SOC FortiView Monitors
ADOM: Fabric-ADOM
S satish

+ Add Widget Dashboard All Devices Last 1 Hour 10:02:23 - 11:02:23
Refresh Day Night Ocean

### Top Sources Today

Total 3,031,221 traffic sessions (1,610,682 Allowed / 1,420,539 Blocked) discovered

IP Address	Allowed	Blocked
10.88.210.32	595,716	91,316
10.88.120.100	173,577	147,550
fe80::115:d706:cc0d:c44c	0	296,130
10.88.110.101	161,705	130,210
10.88.120.104	164,323	126,677
10.88.120.103	139,898	110,272
172.30.72.168	0	130,596
fe80::280:a3ff:feb0:6726	0	87,543
172.30.142.6	32,767	40,876
172.30.142.5	60,115	10,245
10.88.210.50	69,748	67
0.0.0.0	0	57,642
119.76.28.40	0	50,442
10.88.12.254	4	40,688
172.30.72.39	40,048	0

### Top Cloud Applications

#	Application	Category	Risk	Login IDs	Sessions (Blocked/Allowed)	File (Up/Dow...)	Videos Played	Bytes (Sent/Recei...)
1	Dropbox	Storage.Bac	Medium	0	13	0	0	0.0 KB/0.0 KB
2	OneDrive	Storage.Bac	Medium	0	2	0	0	0.0 KB/0.0 KB
3	Facebook	Social.Medi	Medium	0	49	0	0	0.0 KB/0.0 KB

### Resource Usage Average

#	Device	R...	CPU Usa...	Memory Usage	Disk ...	Logs Per Second	Security I	Concurrent...	Bandwidth (Sent/ New Sessi...)
1	FGR60D4		9.17%	29.83%	0%	1.19		101.25	40 kbps   0.17
2	NGFW-D		1.5%	18.25%	1%	40.7		2610.25	5,193 kbps   28.00
3	FORTIDE		1%	23%	0%	0.17		129.42	118 kbps   0.00
4	FORTIDE		1%	24.25%	0%	6.93		2245.75	11,992 kbps   10.33
5	Demo-ISF		0.42%	20%	0%	8.78		573.92	1,829 kbps   5.25
6	Demo-DC		0.17%	15%	1%	37.31		3440.42	2,962 kbps   28.67
7	Demo-ISF		0.15%	20%	0%	17.31		1481.69	2,800 kbps   13.54
8	Demo-ISF		0.08%	20%	0%	0.53		65.33	50 kbps   0.33
9	NGFW-D		0%	17%	1%	0.08		284.50	163 kbps   0.00
10	FortiGate		0%	27%	1%	0.9		124.92	7 kbps   0.00
11	FG_VM-C		0%	20%	2%	3.72		110.25	29 kbps   0.08

### Top Policy Hits

#	Policy	Policy Type	Source Interfa...	Destination Inter...	Device Name	VDOM	Hit Count	Bytes (Sent/Re...	Last Used
1	Outbound policy		DC-SERVERS	port1	Demo-DCFW	root	167,190	121.9 MB/598.8 MB	2019-09-06
2	VLAN-ISF policy		ENG_VLAN	wan1	Demo-ISFW-E	root	41,857	38.9 MB/551.0 MB	2019-09-06
3	FSA-DMZ policy		FSA-DMZ2	port36	NGFW-DEMC	root	6,351	19.9 MB/495.5 MB	2019-09-06
4	LAN-NGF policy		ENG,FIN,SALES	port1	FORTIDEMO	root	42,154	339.2 MB/3.0 MB	2019-09-06
5	VLAN-W. policy		VLAN_FIN	wan1	Demo-ISFW-F	root	120,906	36.7 MB/209.8 MB	2019-09-06

# 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 (ТИ), включая российских

# Фабрика безопасности Fortinet

- Network Security
- Multi-Cloud Security
- Device, Access, and Application Security
- Open Ecosystem
- Security Operations

## ШИРОТА

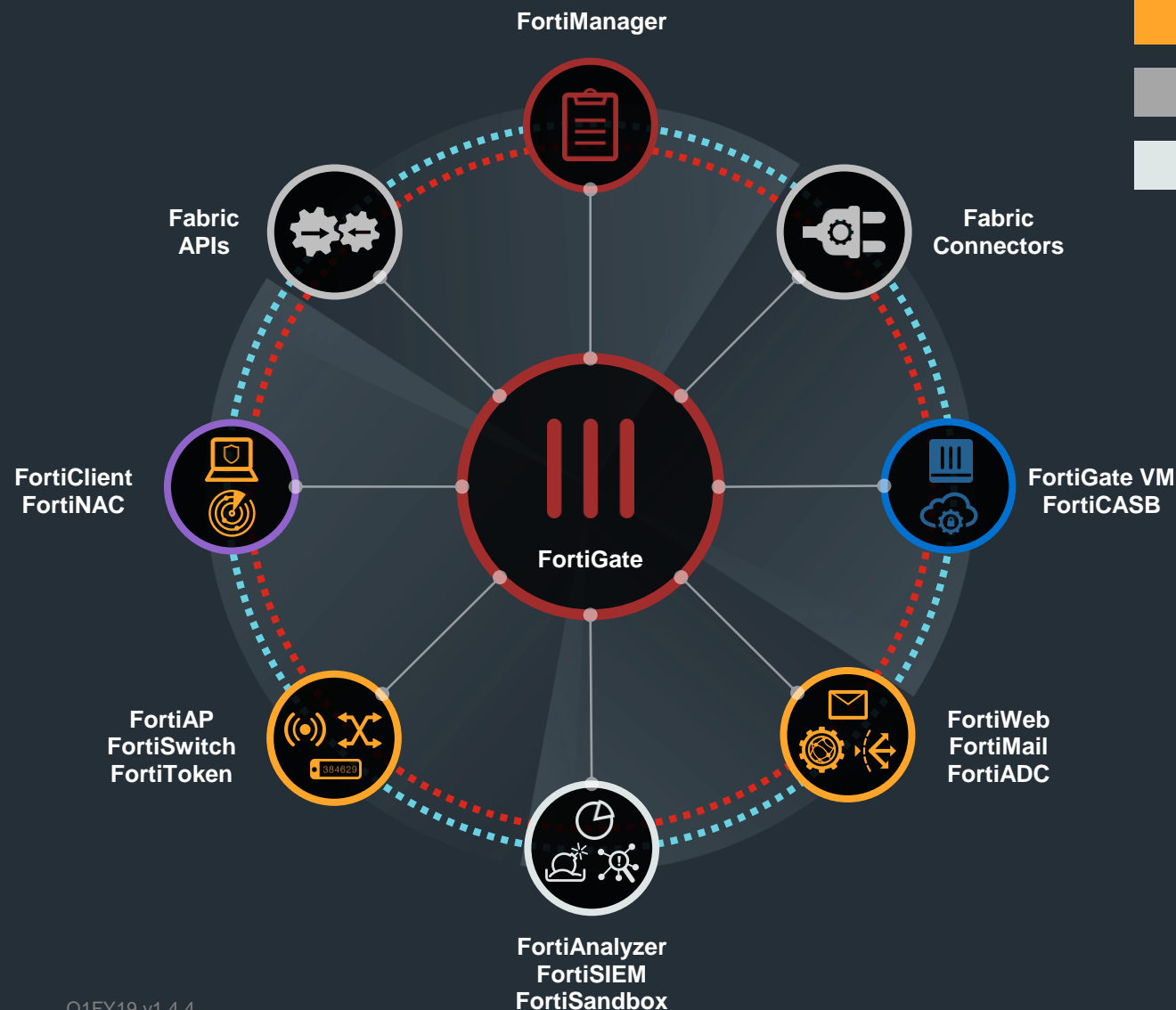
Визуализация всей площади атаки

## ИНТЕГРАЦИЯ

AI- предотвращение угроз для устройств, сетей, приложений

## АВТОМАТИЗАЦИЯ

Операции, управление и ответ





**FORTINET**<sup>®</sup>