FORTINET

Построение архитектуры нулевого доверия

Максим Власюк

Что такое FORTINET?

Fortinet является глобальным лидером на рынке решений в области информационной безопасности

$3.09B
FY2020 Billing
Financially Stable

28B+ Market Cap (as of 2.21.21)
Nasdaq: FTNT
S&P 500

BBB+ Baa1
Security Investment Grade Rating
Leading the Cybersecurity Industry

50
Integrated Fabric Products
Broadest Attack Surface Coverage

500,000+
Customers Worldwide
Massive Customer Input

600,000+
NSE Certifications
WEF Cybersecurity Founders

© Fortinet Inc. All Rights Reserved.

Признанный лидер в категориях Network Firewalls и WAN Edge Infrastructure

2020 Magic Quadrant for Network Firewalls

Fortinet Recognized as a Leader

2020 Magic Quadrant for WAN Edge Infrastructure

Fortinet Recognized as a Leader

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

© Fortinet Inc. All Rights Reserved.

ФСТЭК и новые требования

- Новейший сертификат по новым требованиям
- Профиль защиты межсетевых экранов типа А четвёртого класса защиты
- Профиль защиты межсетевых экранов типа Б четвёртого класса защиты
- Профиль защиты систем систем обнаружения вторжений уровня сети четвертого класса защиты
- Требования к системам обнаружения вторжений
- Специализированная версия OS

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 четвертого 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

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

© Fortinet Inc. All Rights Reserved.

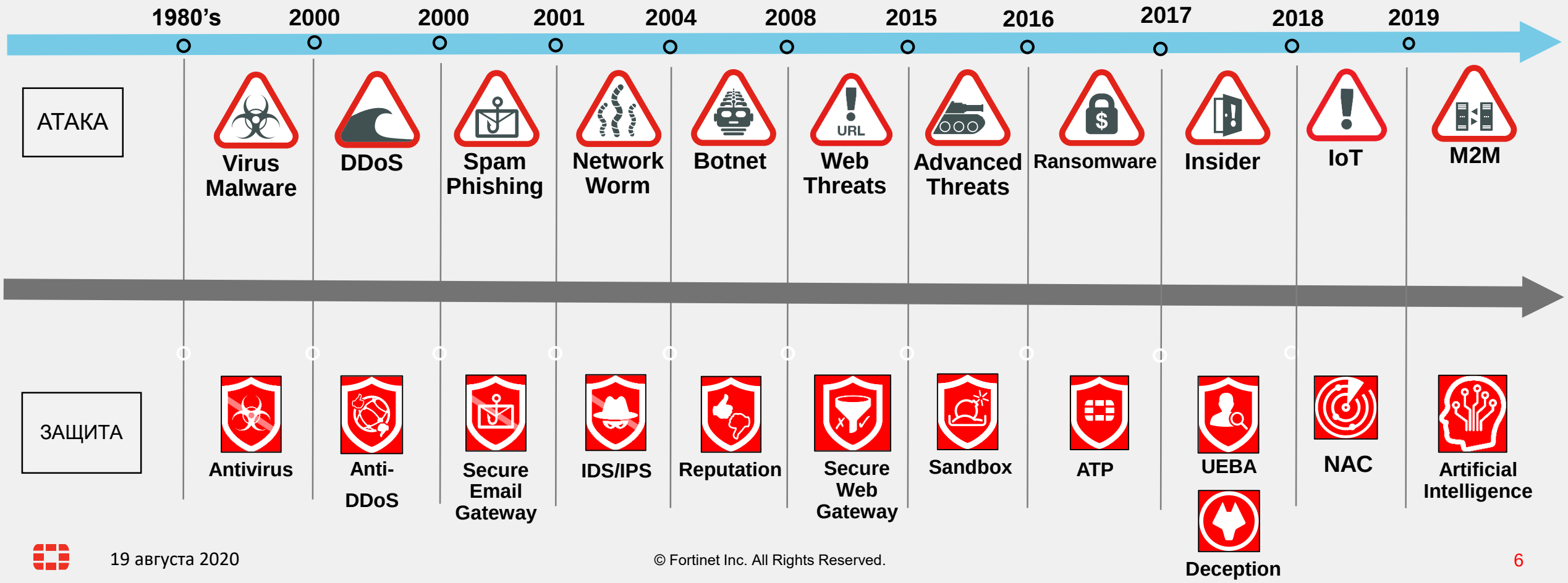
Атаки более не знают границ

Больше возможностей для входа

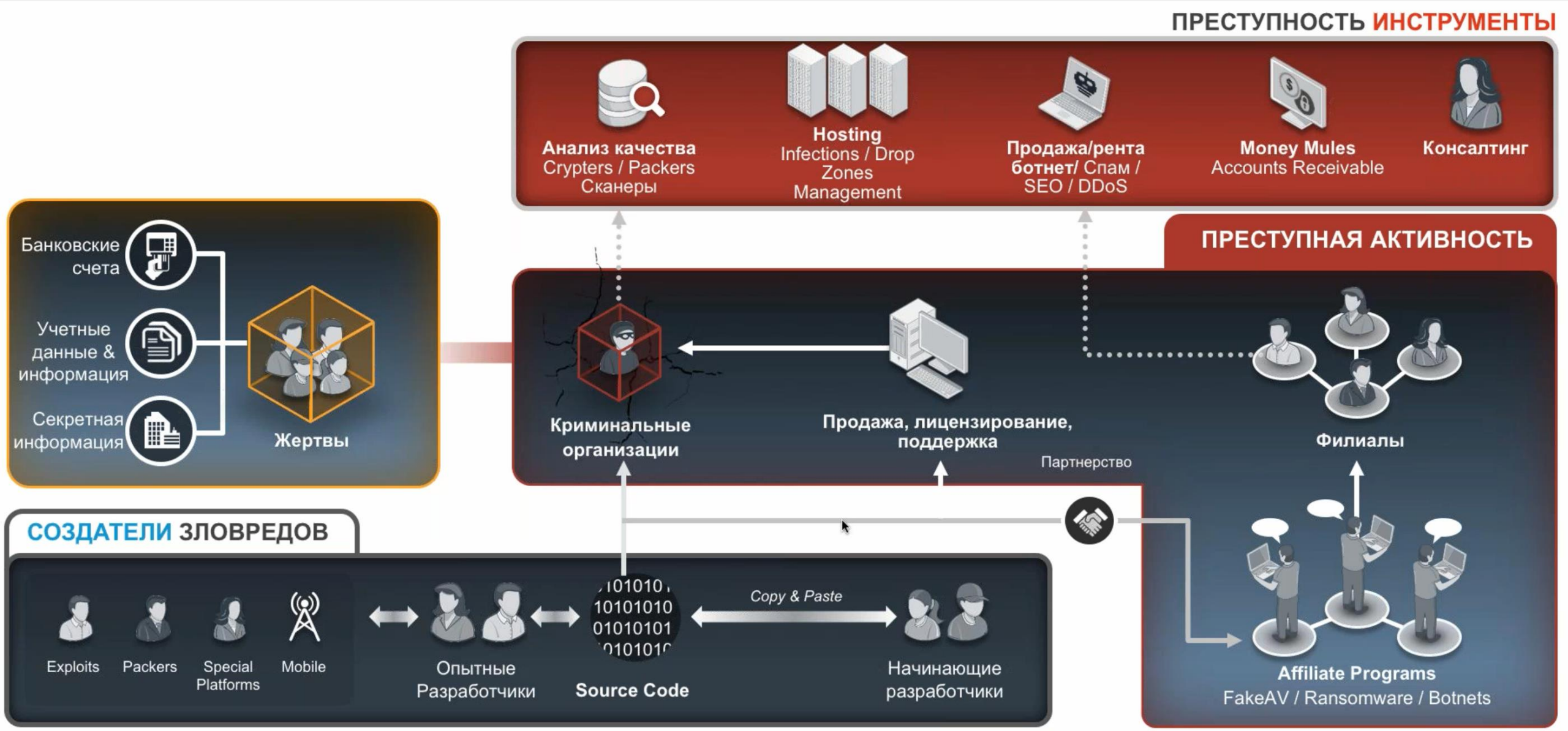
Больше возможностей для выхода

© Fortinet Inc. All Rights Reserved.

Ландшафт угроз



© Fortinet Inc. All Rights Reserved.



© Fortinet Inc. All Rights Reserved.

Технологические проблемы обеспечения ИБ

КОМПЛЕКСНЫЕ
ВЕКТОРЫ АТАК

NOC

АВТОМАТИЗАЦИЯ
ОЦЕНКИ УРОВНЯ ДОВЕРИЯ

ЗАЩИТА ОТ ИЗВЕСТНЫХ УГРОЗ

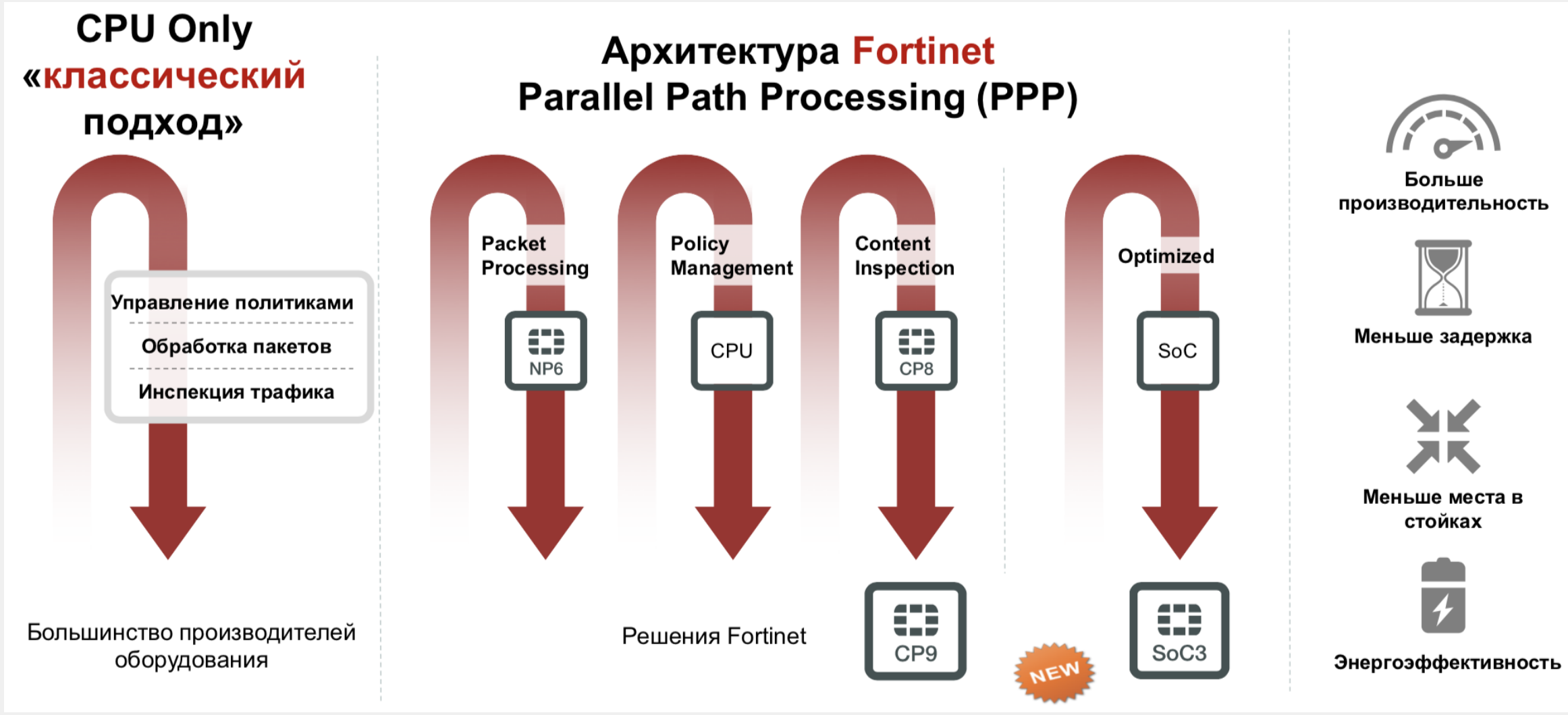
SOC

БЫСТРОЕ РЕАГИРОВАНИЕ

ИНТЕГРИРОВАННОЕ
ДЕТЕКТИРОВАНИЕ И ЗАЩИТА ОТ НЕИЗВЕСТНЫХ УГРОЗ

© Fortinet Inc. All Rights Reserved.

Архитектура решения



© Fortinet Inc. All Rights Reserved.

Открытая экосистема

400+ интегрированных решений

Fortinet-developed deep integration automating security operations and policies

Fabric Connectors

aws · aruba · cisco · Google Cloud · IBM Cloud · Microsoft Azure · ORACLE · servicenow · Symantec

Partner-developed integration using Fabric APIs providing broad visibility with end-to-end solutions

Fabric APIs

EQUINIX · Guardicore · DELL · DRAGOS · ARISTA · SIEMENS Ingenuity for life · ordr · NVIDIA · tufin

Community-driven DevOps scripts automating network and security provisioning, configuration, and orchestration

Fabric DevOps

aws · Google Cloud · HashiCorp · Microsoft Azure · openstack · ORACLE · RED HAT ANSIBLE Automation · TIGERA · vmware

Integrations with threat sharing initiatives and other vendor technologies

Extended Ecosystem

CYBER THREAT ALLIANCE · MITRE · STIX · INTERPOL · OT CSA · Firewalls · Switching · Wireless · Endpoint Security

And many more…

© Fortinet Inc. All Rights Reserved.

Note: Logos are a representative subset of the Security Fabric Ecosystem

FortiGuard Lab.

- **Аналитический и исследовательский департамент** высококвалифицированных экспертов-аналитиков и инженеров
- **Задача – обеспечить сервисы безопасности** на устройствах Fortinet наиболее актуальной информацией для защиты от известных и неизвестных угроз
- **Постоянно анализируются** большие объемы данных, используя машинное обучения, элементы искусственного интеллекта, моделирование для разработки высокоточных сигнатур
- **Взаимодействие и партнерство** с сотнями компаний в области аналитики безопасности

© Fortinet Inc. All Rights Reserved.

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

© Fortinet Inc. All Rights Reserved.

Ключевые компоненты

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 Inc. All Rights Reserved.

Палитра решений для обеспечения безопасности

FortiGuard Security Services

SOC & NOC

- Content Security
- Web Security
- Advanced SOC/NOC

User Security

- User Security
- Device Security

Fabric Management Center - SOC

Endpoint

- FortiEDR
- FortiXDR

Breach

- FortiSandbox
- FortiDeceptor
- FortiAI

Incident Response

- FortiAnalyzer
- FortiSIEM
- FortiSOAR
- FortiGuard MDR Service

Fabric Management Center - NOC

- FortiManager
- FortiCloud
- FortiMonitor

Open Ecosystem

- Connector
- Fabric API
- DevOps
- Extended Fabric Ecosystem

Zero Trust Access

- FortiClient
- FortiNAC
- FortiToken
- FortiAuthenticator

Security-Driven Networking

LAN Edge

- FortiAP
- FortiSwitch

WAN Edge

- FortiGate SD-WAN
- FortiExtender

DC Edge

- FortiGate
- FortiProxy

Cloud Edge

- FortiSASE
- FortiIsolator

Adaptive Cloud Security

Network

- FortiGate VM
- Cloud Networking
- FortiDDos
- FortiSegment

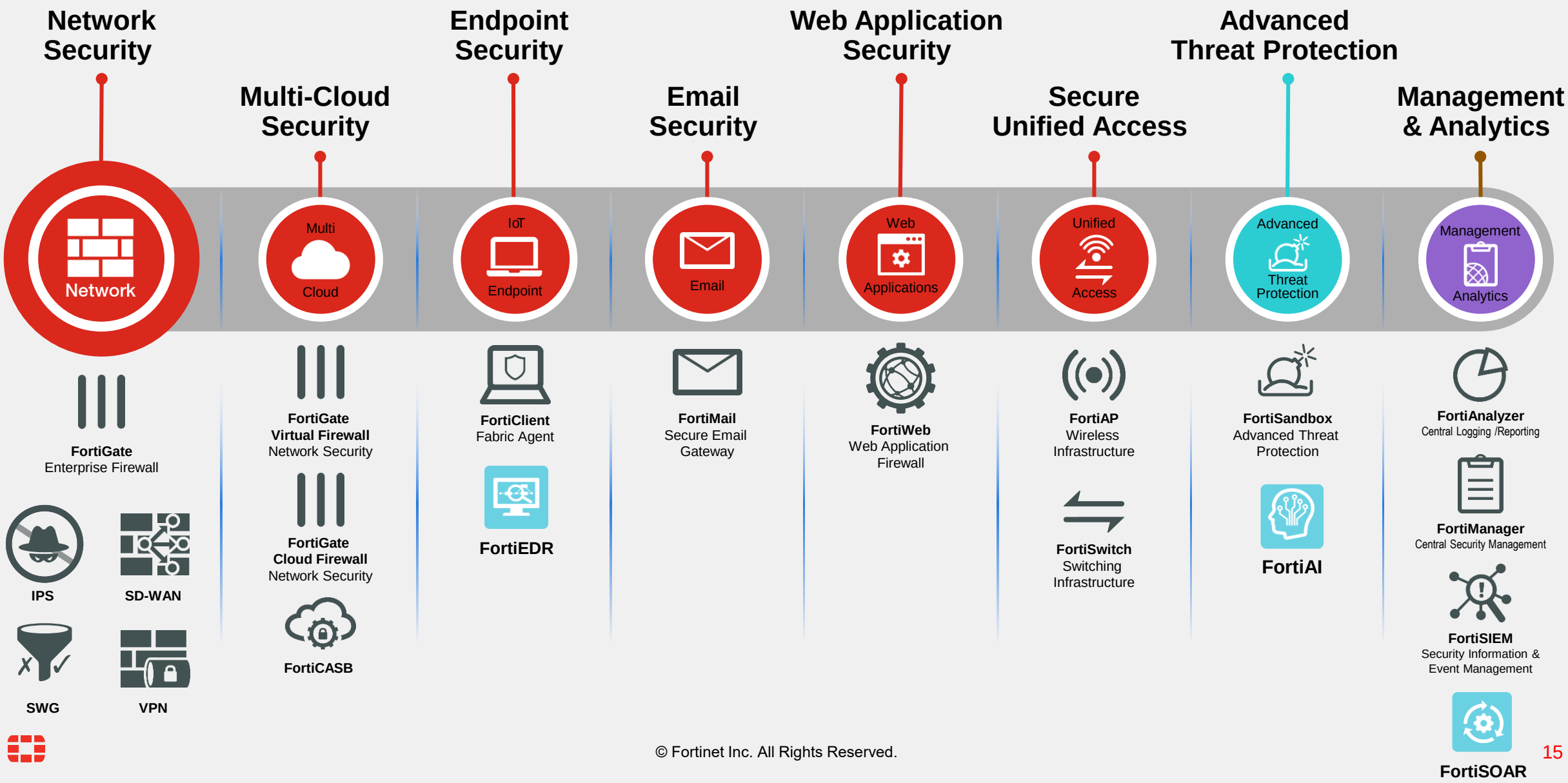
Platform

- FortiCASB
- FortiCWP
- AWS Native
- Azure Native

Applications

- FortiWeb
- FortiMail
- FortiADC
- FortiGSLB

© Fortinet Inc. All Rights Reserved.



© Fortinet Inc. All Rights Reserved.

Консолидация сервисов в SD-Branch

© Fortinet Inc. All Rights Reserved.

Unparalleled 3rd Party Validation

■ Recommended / Certified □ Neutral ■ Caution O Undisclosed X – did not participate

CERTIFICATION	Fortinet	Check Point	Cisco	Palo Alto Networks	Juniper	FireEye
NSS Next-Gen Firewall	■	■	O	■	O	x
NSS DC Security Gateway	■	x	■	■	■	x
NSS Next-Gen IPS	■	x	O	■	O	x
NSS DC IPS	■ ■	x	■	x	x	x
NSS Breach Detection	■	x	■	x	x	■
NSS Breach Prevention	■	■	■	■	■	x
NSS WAF	■	x	x	x	x	x
NSS Advanced Endpoint	■	■	■	O	x	x
NSS SD-WAN	■	x	x	x	x	x
ICSA ATD – Sandbox	■	x	x	x	■	x
ICSA ATD – Email	■	x	x	x	x	x
ICSA Network Firewall	■	■	x	■	x	x
ICSA Network IPS	■	x	x	x	x	■
ICSA Anti-malware Network	■	x	x	x	x	x
ICSA WAF	■	x	x	x	x	x
Virus Bulletin 100	■	x	x	x	x	■
Virus Bulletin Spam	■	x	x	x	x	x
Virus Bulletin Web	■	x	x	x	x	x
Common Criteria	■	■	■	■	■	■
FIPS	■	■	■	■	■	■
UNH USGv6/IPv6	■	■	■	■	■	x

© Fortinet Inc. All Rights Reserved.

Полезные ссылки

Бесплатные курсы NSE:

https://www.fortinet.com/training/cybersecurity-professionals?utm_source=pr&utm_campaign=2020-q2-keyword#free-trainings

Лабораторные работы **Fast Track**:

https://go.fortinet.com/l/872291/2021-01-05/3t3nm

Вебинары:

https://secure.fortinet.com/LP=6011

Документация:

https://docs.fortinet.com/

© Fortinet Inc. All Rights Reserved.


FORTINET