



Демонстрация возможностей Fortinet Security Fabric

Evgenii Puzakov, инженер, epuzakov@fortinet.com

All questions: cis@fortinet.com

Technical questions: cis_se@fortinet.com

Security Fabric / Фабрика безопасности



Сеть & Безопасность



FortiGate Cloud

- FortiGate Mgmt., Log Analysis and Retention
- Bulk Provisioning
- IoC Service

FortiSandbox Cloud

FortiMail Cloud

FortiWeb Cloud

FortiAP Cloud

FortiSwitch Cloud

FortiToken Cloud

FortiVoice Cloud

FortiPresence

FortiCASB

FortiCWP

MOBILE USERS

REMOTE OFFICE

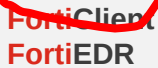


FTNT Hosted Services

Public Cloud Instances



FortiToken



Remote VPN

FortiExtender

Site-to-site VPN

Secure WiFi Access

FortiWiFi



FortiAI 3500F

SECURITY/NETWORK OPERATING CENTER

FortiAnalyzer

Central Log & report

Central Device Mgmt.

FortiNAC

IoT Access Control

User Access Mgmt.

FortiSandbox

File Analysis

Network Tester

FortiWLC

Wireless Controller

Wireless Manager

FortiDeceptor

Honeypot

SIEM

FortiSOAR

SOAR

Client Mgmt. System

FortiManager

FortiAuthenticator

FortiTester

FortiWLM

FortiSIEM

FortiClient EMS

Security Gateway

FortiGate

L7 D/DOS Mitigator

FortiDDoS

Mail Sec. Gateway

FortiMail

FortiIsolator

FortiProxy

Browser Isolation

Secure Web Gateway

DATA CENTER



FortiSwitch



FortiAP



FortiRecorder



FortiVoice

FortiCamera

FortiFone



FortiWeb



FortiADC

Virtual Appliances



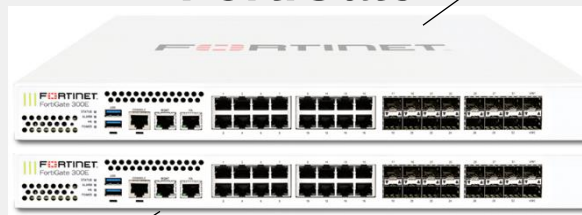
- VMWare
- Citrix Xen
- MS Hyper-V
- KVM
- Nutanix AHV







FortiGate



**Кластер
High Availability /Load
Balancing**



NGFW

Firewall (Межсетевой экран)

Antivirus

IPS (Система против вторжений)

Фильтрация URL и APP control

SSL инспекция

VPN

Ipsec (Site-to-Site / Client-to-Site)

SSL (Tunnel mode / Web Mode)

SD-WAN

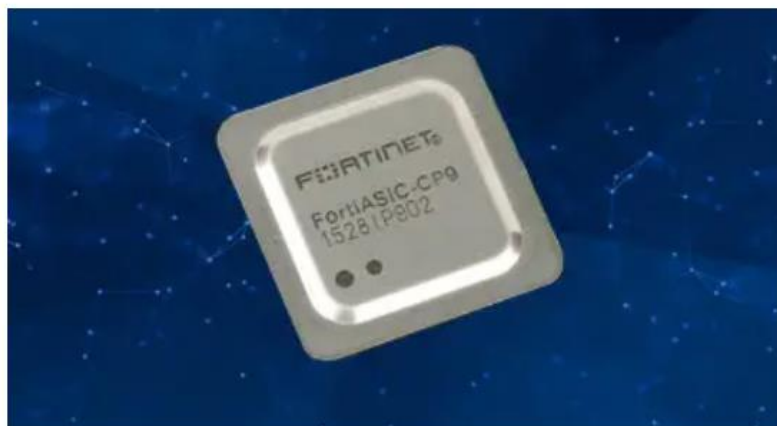
**NGFW в качестве контроллера
для FortiSwitch и FortiAP**

Собственные процессоры

Firewall и Сети



Network Processor 7 (NP7)



Content Processor 9 (CP9)



System-on-a-Chip 4 (SoC4)

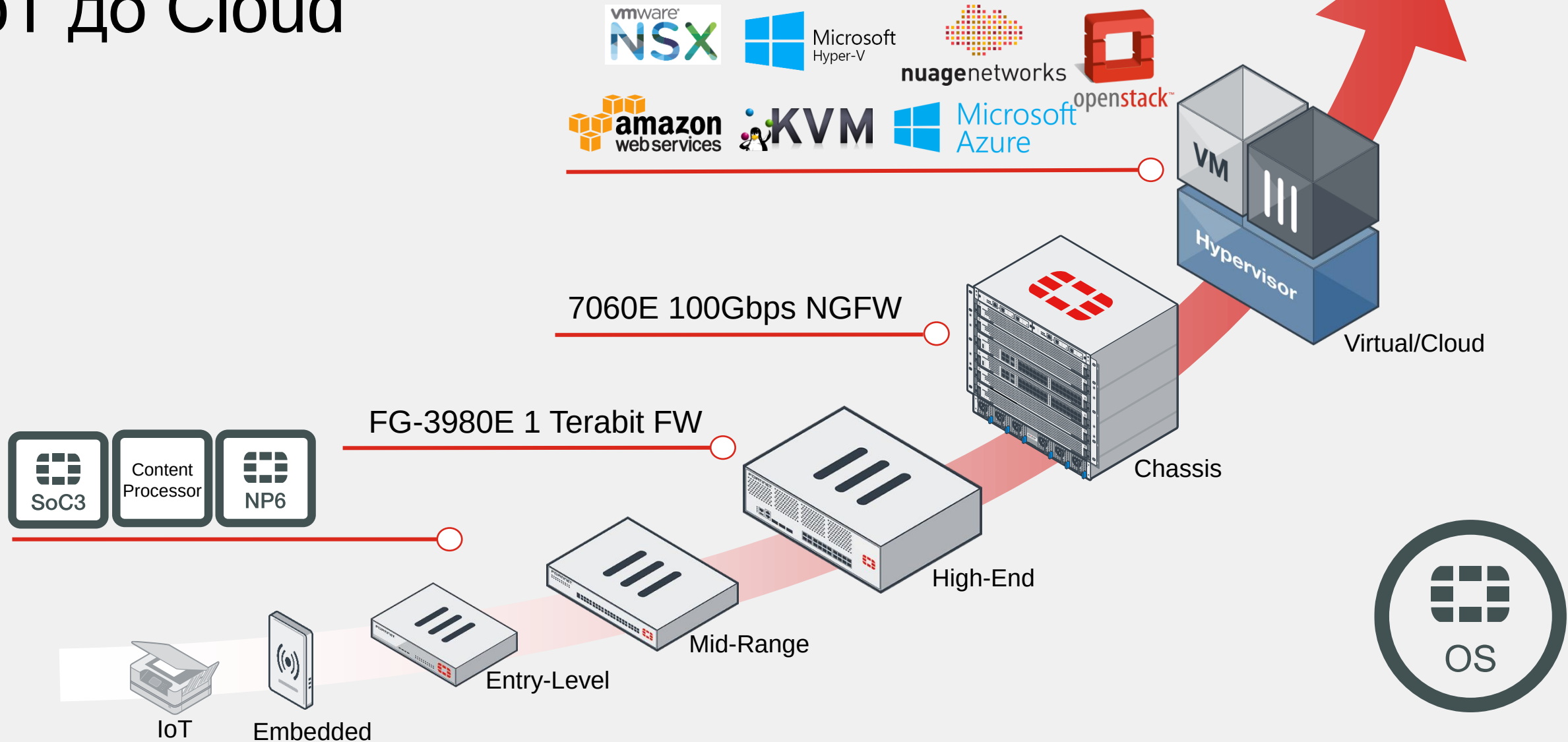


**Модули
Безопасности**



**Модули
Безопасности**

Масштабирование производительности от IoT до Cloud



Лидеры

SD-WAN



NGFW





FortiSandbox



- Физический Appliance
- VM
- В облаке

1. Antivirus
2. FortiGuard cloud
3. Эмуляция файла
4. Взаимодействие с C&C

**Pre-signature
Hash**

FortiGate



FortiGuard



FortiSandbox – ключевое звено в цепочке Operational Threat Intelligence

■ Управление и мониторинг

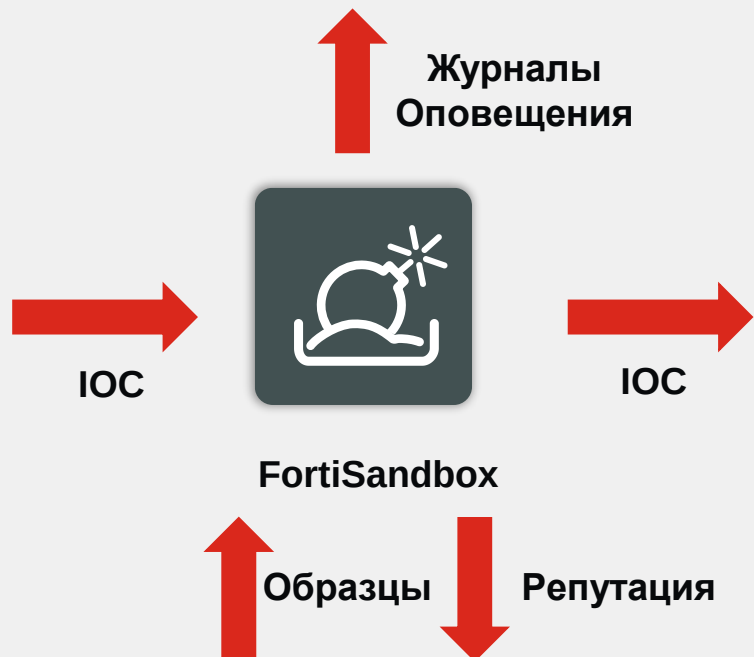
» NOC

» SOC

Журналы
Оповещения

• Генераторы:

- **FortiGuard**
- 3rd party Feeds
- Локальные средства защиты
- Другие «песочницы»



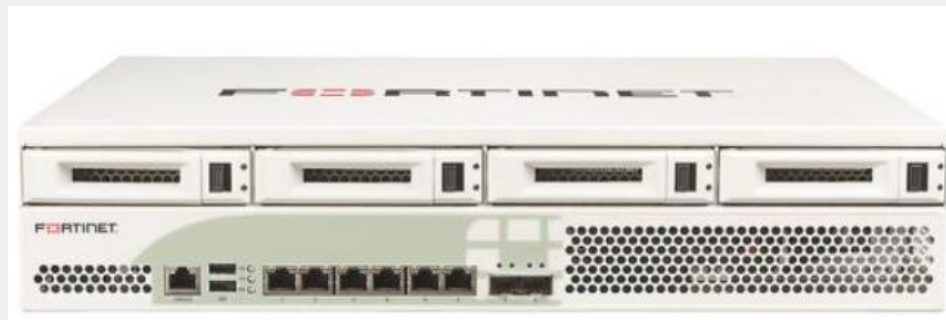
■ Потребители:

- » **FortiGuard**
- » SIEM
- » Локальные средства защиты
- » Другие «песочницы»

■ Средства защиты

- » FortiGate, FortiMail, FortiWeb, FortiClient
- » Сторонние: ICAP-клиенты, API, Bit9 Carbon Black,
- » Общие: сетевые папки, копия трафика

FortiSandbox	FSA-500F	FSA-1000F/-DC	FSA-2000E	FSA-3000E	FSA-VM
VM Sandboxing (Files/Hour)	120	280	480	1,120	Hardware Dependent
Sandbox Pre-Filter (Files/Hour)	4,500	7,500	12,000	15,000	Hardware Dependent
Number of VMs	2+4 optional	2+12 optional	4+20 optional	8 + 48 optional	Total: 1 to 54
Interfaces	4x GE RJ45 ports	4x GE RJ45 ports, 4x 10GE SFP+ slots	4x GE RJ45 ports, 2x 10GE SFP+ slots	4x GE RJ45 ports, 2x 10GE SFP+ slots	Hardware Dependent



FortiSandbox – Advanced Pre-filter

FortiAI

FortiAI Settings

☒ Enable

Server IP: 10.59.26.252

Token:

Rating Timeout (Se

Uploading Timeou

Maximum File Size

Scan Profile

Pre-Filter

VM Association

Advanced

Process the following selected file types.

Executables

PDF documents

Office documents

Flash files

Web pages

Compressed archives

Android files

Mac files

Linux files

URL detection

User defined extensions

Notes: The file type prefiltering applies to submission via sniffer, adapters and Fabric devices (except FortiMail). Files from OnDemand, FortiMail and Network Share are always processed.

Check for Active Content on the selected file types during VM Scan pre-filter.

office

dll

htm

js

pdf

swf

url

archive

Notes: Active Content are embedded codes that can be executed (e.g. macros scripts). When enabled, the overall system throughput is improved by only processing files with active content. Otherwise, forward all files. All executable files are forwarded.

Use the results of the following during VM Scan pre-filter.

FortiAI entrust

Trusted Vendor

Trusted Domain

Apply





Самообучающаяся система AI

8+ ЛЕТ
Обучения AI

Более 6 млн
Признаков
идентификации
зловредов

Менее 100 ms
На
расследование

10 GB
Пропускная
способность



FortiAI 3500F

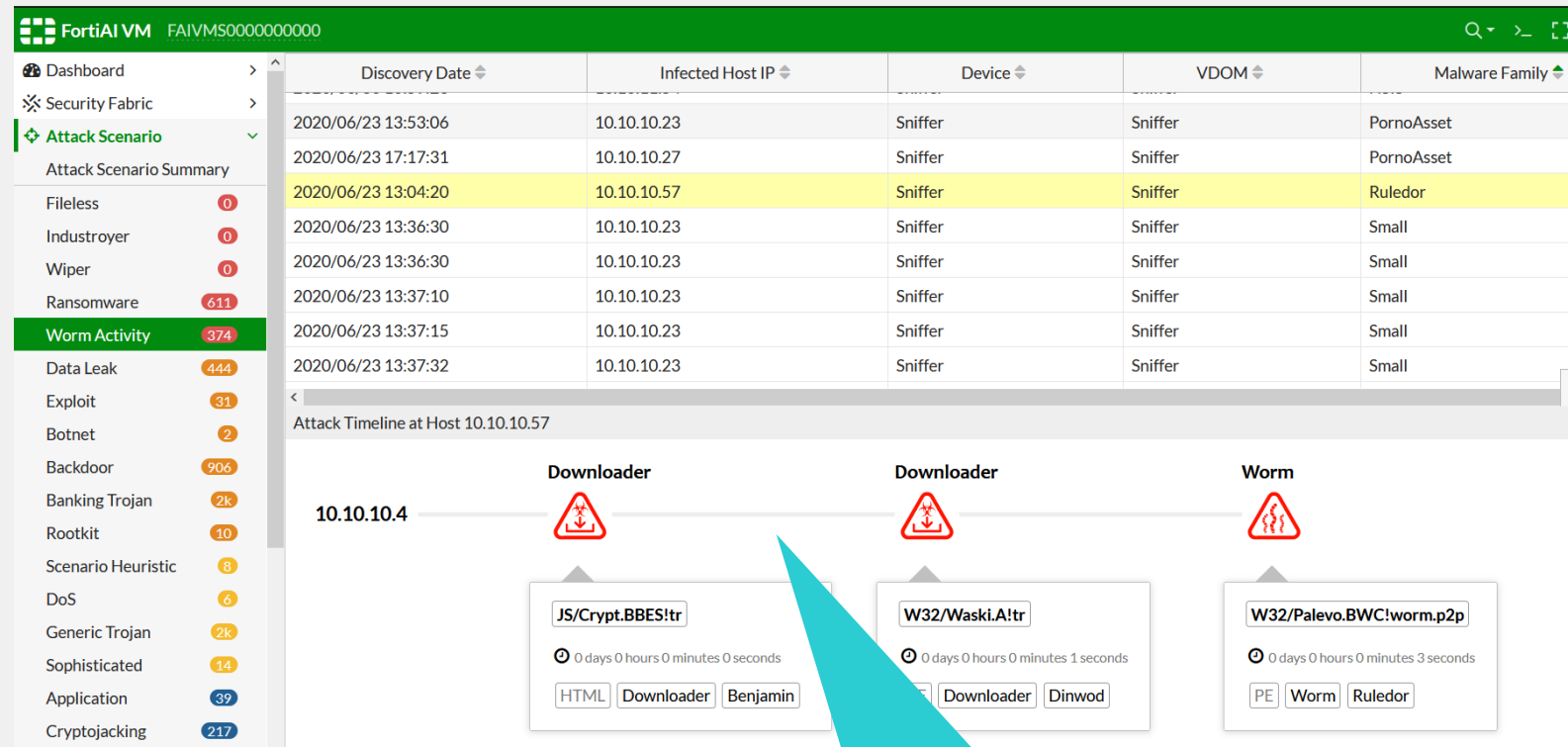




1 Virtual Security Analyst™ оснащённый Deep Neural Networks, который **идентифицирует**, классифицирует, и расследует сложные атаки и блокирует их

1 Идентифицирует
Останавливает угрозы в считанные секунды

Решает
SecOps встречают огромное количество угроз, в том числе False Positive (на что уходит очень много времени)



Распознает угрозы менее, чем за секунду





Virtual Security Analyst™ оснащённый Deep Neural Networks, который идентифицирует, классифицирует, и расследует сложные атаки и блокирует их

2

2 Классифицирует

Распознает класс угрозы и их действия в системе

Решает

Угрозы, которые скрываются за счёт скрывания своей зловредной активности

FortiAI VM FAIVMS0000000000

Dashboard > Security Fabric > Attack Scenario > Attack Scenario Summary

Fileless 0
Industroyer 0
Wiper 0
Ransomware 611
Worm Activity 374
Data Leak 444
Exploit 31
Botnet 2
Backdoor 906
Banking Trojan 2k
Rootkit 10
Scenario Heuristic 8
DoS 6
Generic Trojan 2k
Sophisticated 14
Application 39
Cryptojacking 217

Discovery Date	Infected Host IP	Device	VDOM	Malware Family
2020/06/23 13:53:06	10.10.10.23	Sniffer	Sniffer	PornoAsset
2020/06/23 17:17:31	10.10.10.27	Sniffer	Sniffer	PornoAsset
2020/06/23 13:04:20	10.10.10.57	Sniffer	Sniffer	Ruledor
2020/06/23 13:36:30	10.10.10.23	Sniffer	Sniffer	Small
2020/06/23 13:36:30	10.10.10.23	Sniffer	Sniffer	Small
2020/06/23 13:37:10	10.10.10.23	Sniffer	Sniffer	Small
2020/06/23 13:37:15	10.10.10.23	Sniffer	Sniffer	Small
2020/06/23 13:37:32	10.10.10.23	Sniffer	Sniffer	Small

Attack Timeline at Host 10.10.10.57

10.10.10.4

Downloader

JS/Crypt.BBES!tr

0 days 0 hours 0 minutes 0 seconds

HTML Downloader Benjamin

Downloader

W32/Waski.A!tr

0 days 0 hours 0 minutes 1 seconds

PE Downloader Dinwod

Worm

W32/Palevo.BWC!worm.p2p

0 days 0 hours 0 minutes 3 seconds

PE Worm Ruledor





Virtual Security Analyst™ оснащённый Deep Neural Networks, который идентифицирует, классифицирует, и **расследует** сложные атаки и блокирует их

3

3 Расследует

Расследует угрозу в реальном времени, сохраняет её следы и делает это без задержек

Решает

Распознает горизонтальное и вертикальное распространение

The screenshot displays the FortiAI VM interface. On the left, a sidebar lists various attack scenarios with their counts: Fileless (0), Industroyer (0), Wiper (0), Ransomware (611), Worm Activity (374), Data Leak (444), Exploit (31), Botnet (2), Backdoor (906), Banking Trojan (2k), Rootkit (10), Scenario Heuristic (8), DoS (6), Generic Trojan (2k), Sophisticated (14), Application (39), and Cryptojacking (217). The main area shows a table of attack scenarios with columns for Discovery Date, Infected Host IP, Device, VDOM, and Malware Family. The table lists several attacks, with the third row highlighted in yellow: 2020/06/23 13:04:20, 10.10.10.57, Sniffer, Sniffer, Ruledor. Below the table, a section titled 'Attack Timeline at Host 1' shows a 'Kill Chain' diagram. The diagram illustrates the progression of an attack from a source IP (10.10.10.4) through three stages: 1. JS/Crypt.BBES!tr (HTML, Downloader, Benjamin), 2. W32/Waski.A!tr (PE, Downloader, Dinwod), and 3. W32/Palevo.BWC!worm.p2p (PE, Worm, Ruledor). Each stage includes a timestamp and a status indicator.

Discovery Date	Infected Host IP	Device	VDOM	Malware Family
2020/06/23 13:53:06	10.10.10.23	Sniffer	Sniffer	PornoAsset
2020/06/23 17:17:31	10.10.10.27	Sniffer	Sniffer	PornoAsset
2020/06/23 13:04:20	10.10.10.57	Sniffer	Sniffer	Ruledor
2020/06/23 13:36:30	10.10.10.23	Sniffer	Sniffer	Small
2020/06/23 13:36:30	10.10.10.23	Sniffer	Sniffer	Small
2020/06/23 13:37:10	10.10.10.23	Sniffer	Sniffer	Small
2020/06/23 13:37:15	10.10.10.23	Sniffer	Sniffer	Small
2020/06/23 13:37:32	10.10.10.23	Sniffer	Sniffer	Small

Attack Timeline at Host 1

Investigate threats in "Kill Chain" format

10.10.10.4

- JS/Crypt.BBES!tr
0 days 0 hours 0 minutes 0 seconds
HTML Downloader Benjamin
- W32/Waski.A!tr
0 days 0 hours 0 minutes 1 seconds
PE Downloader Dinwod
- W32/Palevo.BWC!worm.p2p
0 days 0 hours 0 minutes 3 seconds
PE Worm Ruledor





Virtual Security Analyst™ оснащённый Deep Neural Networks, который идентифицирует, классифицирует, и расследует сложные атаки и **блокирует** их

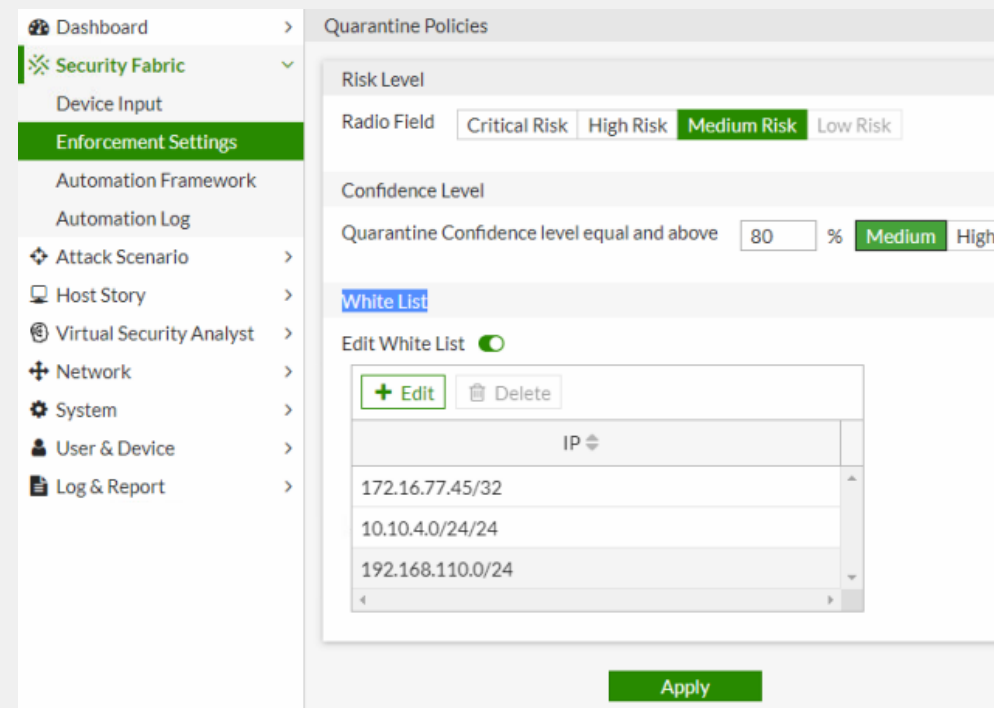
4

4 Automated Response

Засчет интеграции с FortiGate – блокирует угрозы в реальном времени.

Решает

Сценарии по устранению угрозы в реальном времени



FortiGate quarantine based on FortiAI risk & confidence levels



FortiGuard

FortiSan

File Types and Protocols

- 32bit and 64bit Portable Executables (PE) files including DLLs and self-extracting ZIP files
- Web based, text, and PE files such as HTML, PDF, JS, VBS, VBA, ELF, HWP (Hancor), 32 & 64bits PE files including DLLs, MSOFFICE, DEX, PHP, XML, POWERSHELL, Archive files including ZIP, TAR, XZ, GZIP, BZIP, BZIP2, RAR, LZH, LZW, ARJ, CAB, and 7Z

00 – 100 тыс.

час

22 тыс. файлов

FortiGate

4) Ручная загрузка
файлов

FortiAI 3500F

Inline blocking (v7.0.1)

© Fortinet Inc. All Rights Reserved.

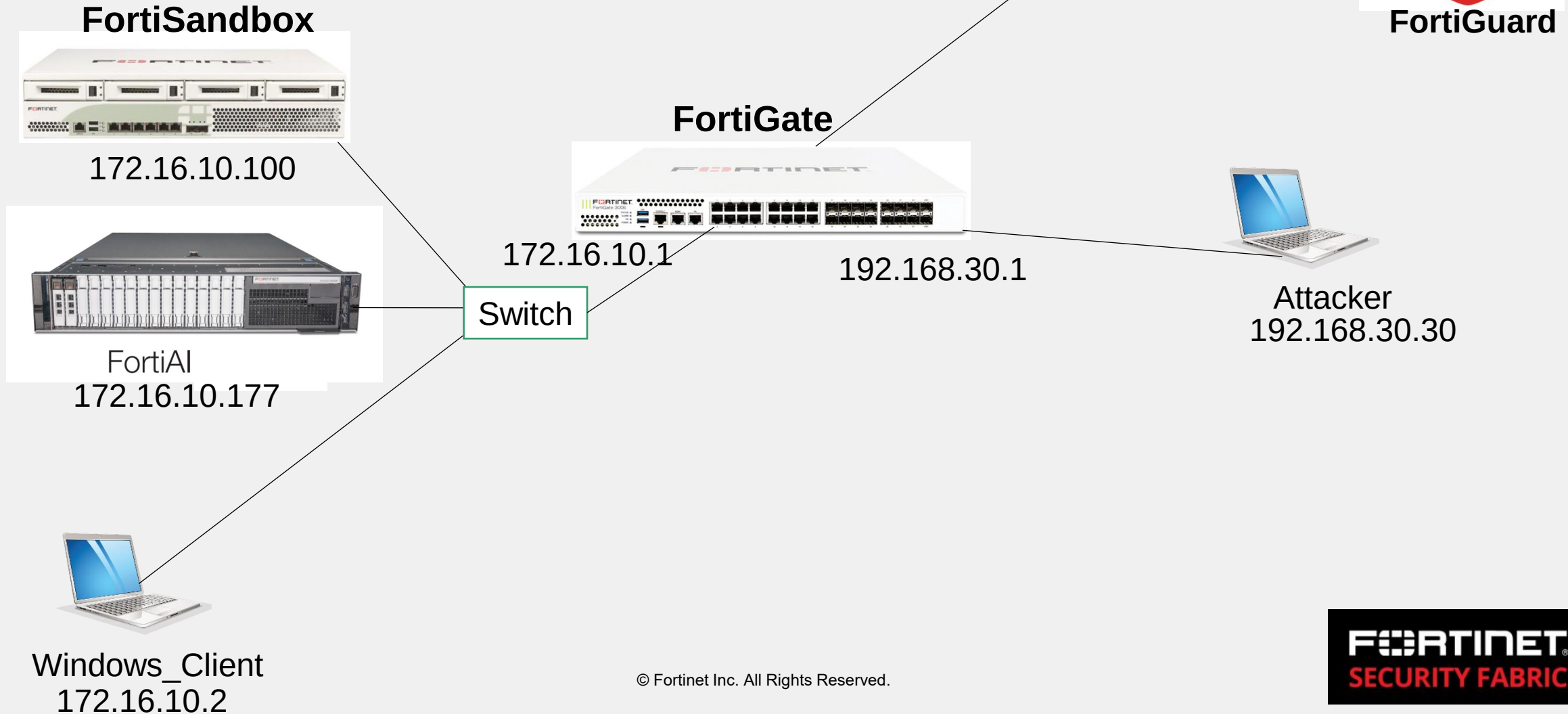




Практические сценарии



Топология сети





Наши контакты:

по общим вопросам cis@fortinet.com

по техническим вопросам cis_se@fortinet.com