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

aws
Azure
ORACLE Cloud Infrastructure
Alibaba Cloud

SECURITY/NETWORK OPERATING CENTER

FortiAnalyzer — Central Log & report
FortiNAC — IoT Access Control
FortiSandBox — File Analysis
FortiWLC — Wireless Controller
FortiDeceptor — Honeypot
FortiSOAR — SOAR

Central Device Mgmt.
User Access Mgmt.
Network Tester
Wireless Manager
SIEM
Client Mgmt. System

FortiManager | FortiAuthenticator | FortiTester | FortiWLM | FortiSIEM | FortiClient EMS

Public Cloud Instances
FTNT Hosted Services

Internet

Security Gateway
FortiGate

L7 D/DOS Mitigator — FortiDDoS
Mail Sec. Gateway — FortiMail
Mail Servers
FortiIsolator
FortiProxy
Browser Isolation
Secure Web Gateway

Remote VPN
2 Factor OTP Token
Endpoint Security
FortiToken
FortiClient
FortiEDR

MOBILE USERS

LAN

Switch — FortiSwitch
Access Point — FortiAP
Surveillance — FortiRecorder
IP PBX — FortiVoice
FortiCamera
FortiFone

DATA CENTER

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

Virtual Appliances
Web App. Firewall — FortiWeb
Load Balancer — FortiADC
Web Servers

3G/4G WAN
FortiExtender
Site-to-site VPN
Secure WiFi Access
FortiWiFi

REMOTE OFFICE

FortiAI 3500F

FortiGate

FORTINET
SECURITY FABRIC

FortiGate

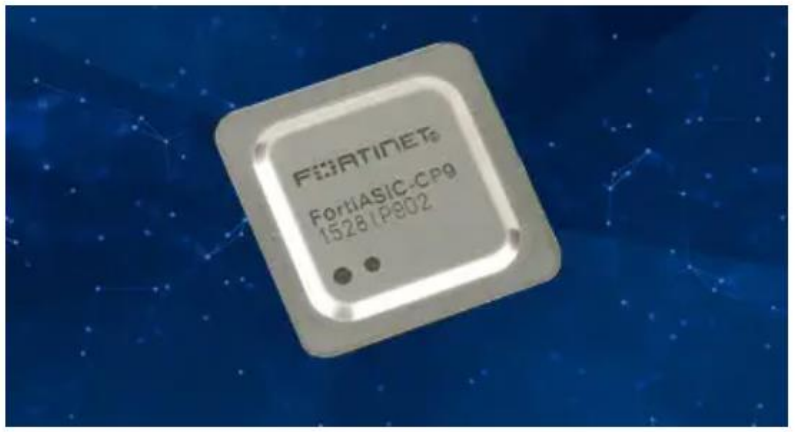
Кластер
High Availability /Load Balancing

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

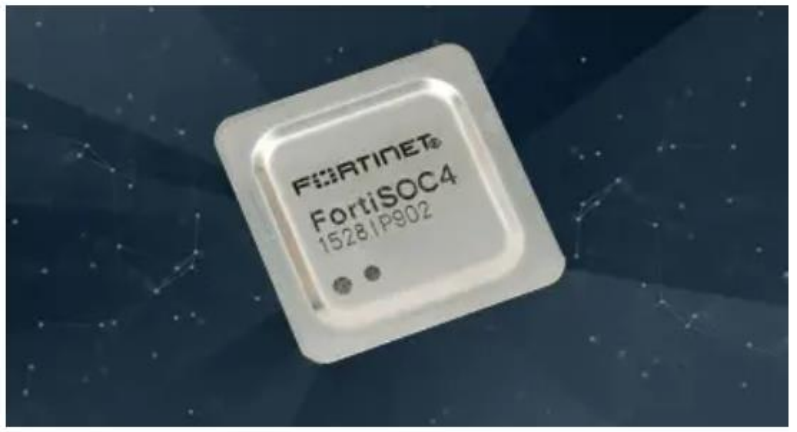
Firewall и Сети

Network Processor 7 (NP7)



Content Processor 9 (CP9)

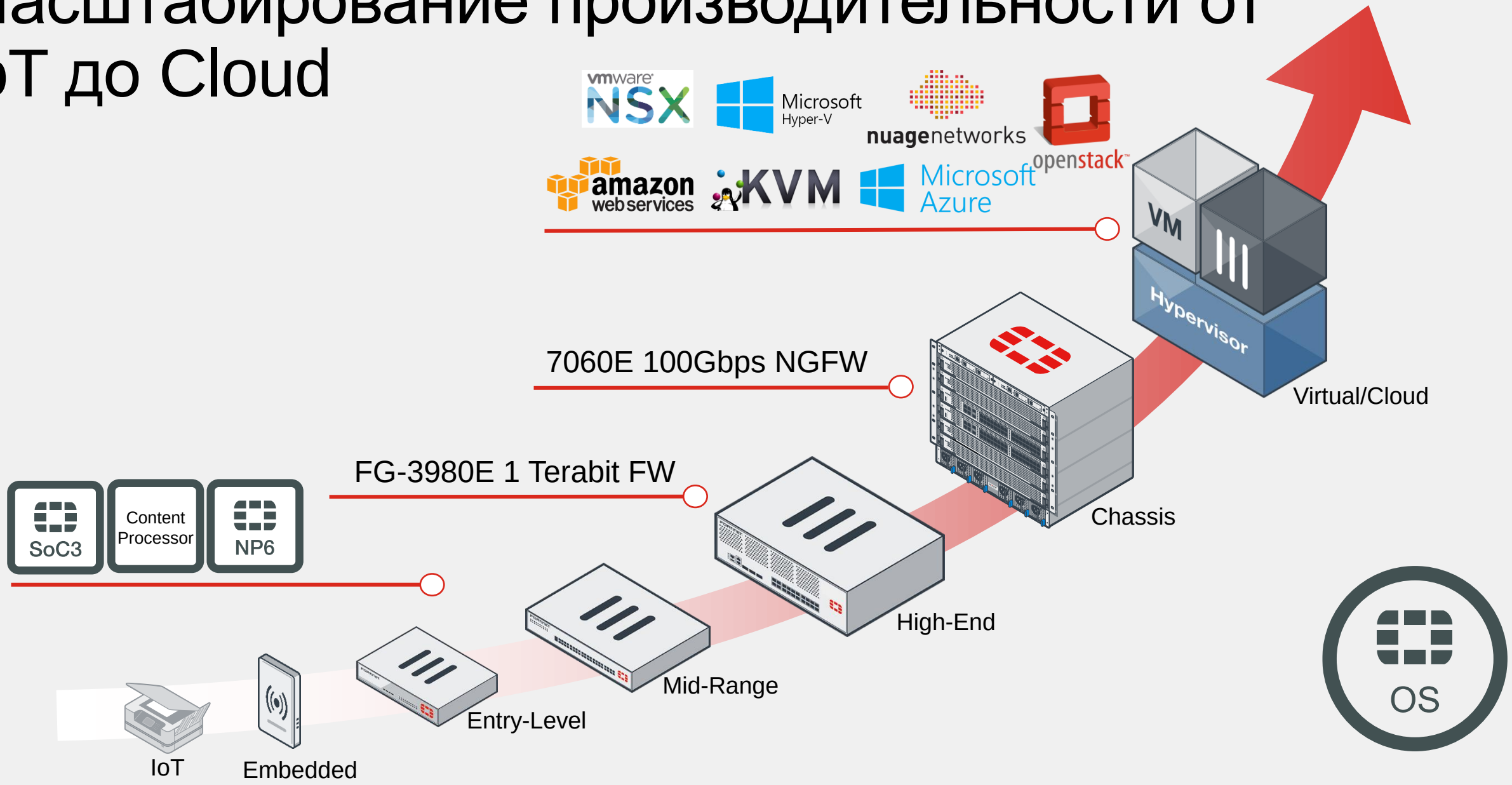
Модули Безопасности



System-on-a-Chip 4 (SoC4)

Модули Безопасности

Масштабирование производительности от IoT до Cloud



Лидеры

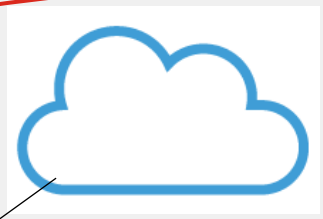
SD-WAN

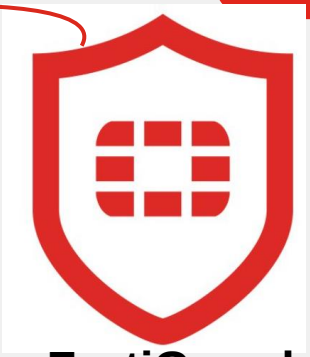
NGFW

Source: Gartner (November 2020)

FortiSandbox

FORTINET SECURITY FABRIC





FortiGuard

FortiSandbox

- Физический Appliance
- VM
- В облаке

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

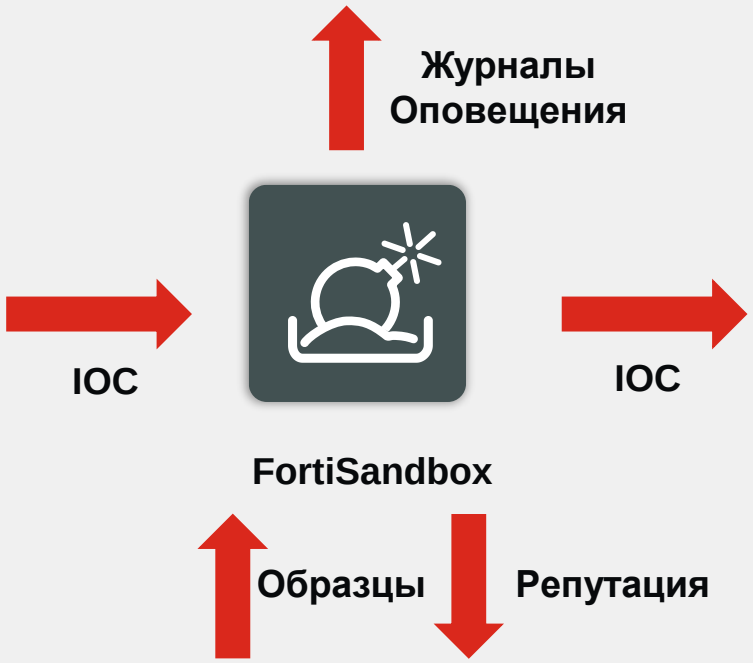
Pre-signature
Hash

FortiGate

FortiSandbox – ключевое звено в цепочке Operational Threat Intelligence

- **Управление и мониторинг**
  - » NOC
  - » SOC

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

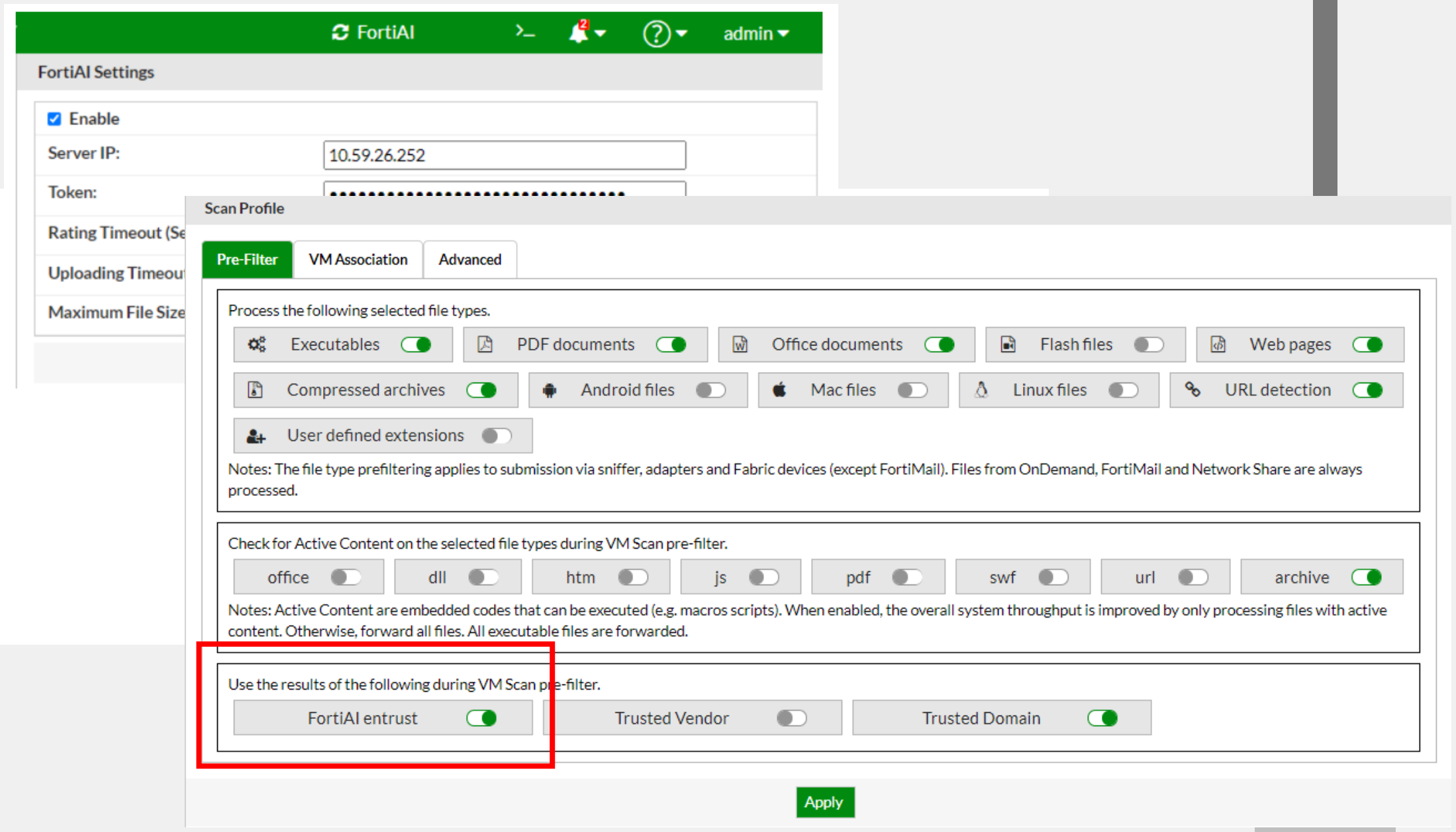


- **Потребители**:
  - » **FortiGuard**
  - » SIEM
  - » Локальные средства защиты
  - » Другие «песочницы»

- **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

Самообучающаяся система AI

8+ ЛЕТ
Обучения AI

Более 6 млн
Признаков
идентификации
зловредов

Менее 100 ms
На
расследование

10 GB
Пропускная
способность

FortiAI 3500F

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

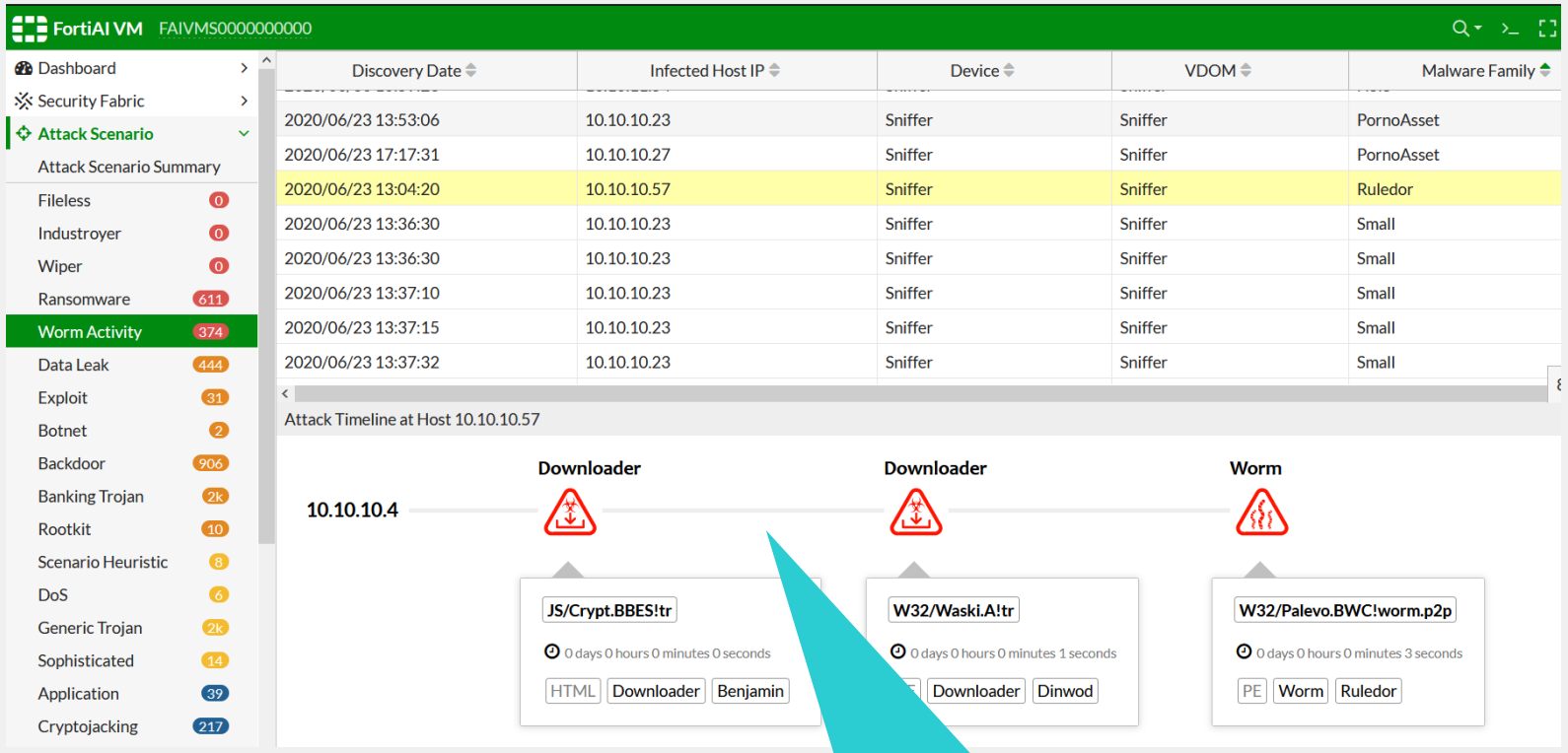
1

1 **Иденцифирует**

Останавливает угрозы в считанные секунды

Решает

SecOps встречают огромное кол-во 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 иденцифирует , **классицифирует**, и расследует сложные атаки и блокирует их

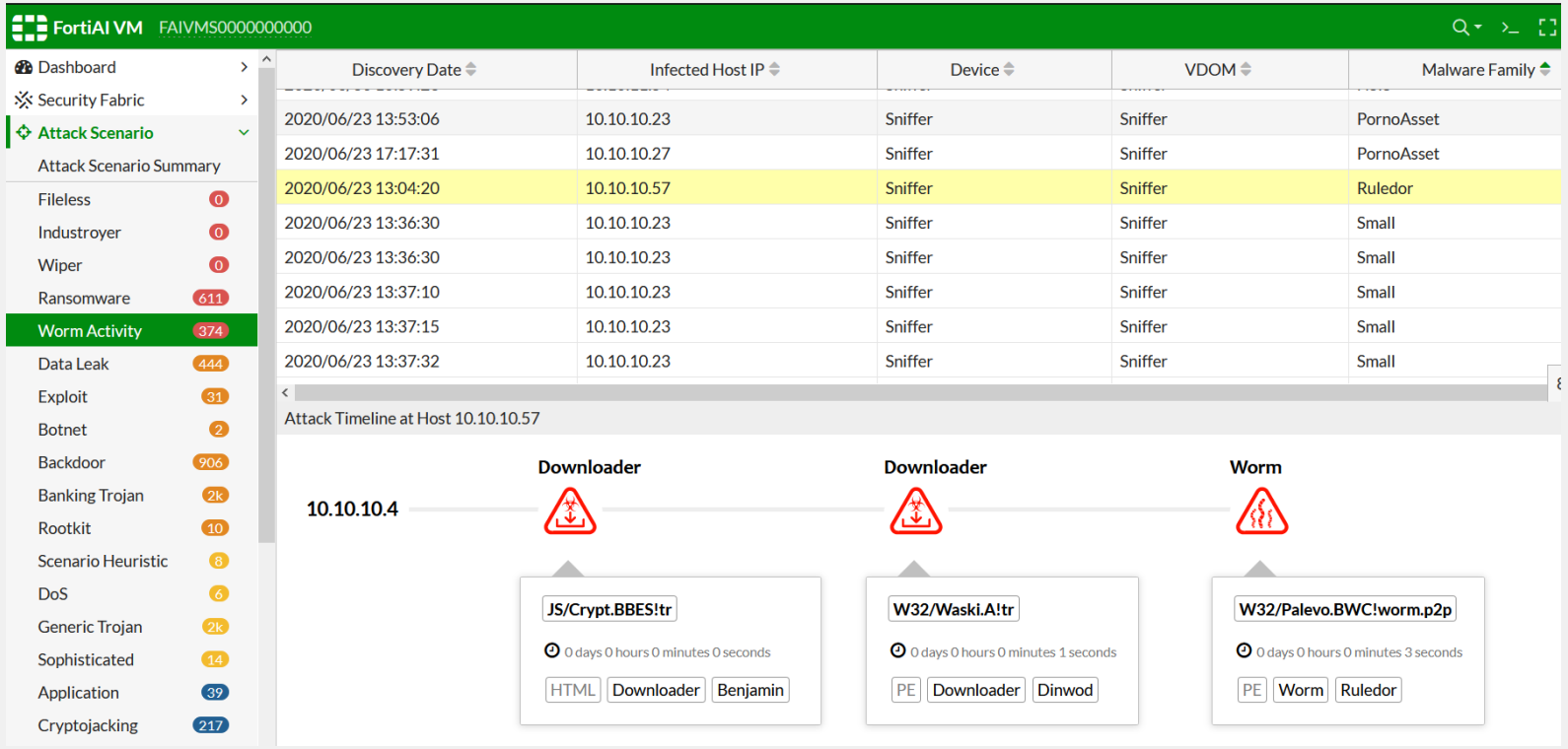
2

2 Классифицирует

Распознает класс угрозы и их действия в системе

Решает

Угрозы, которые скрываются засчёт скрывания своей зловредной активности



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

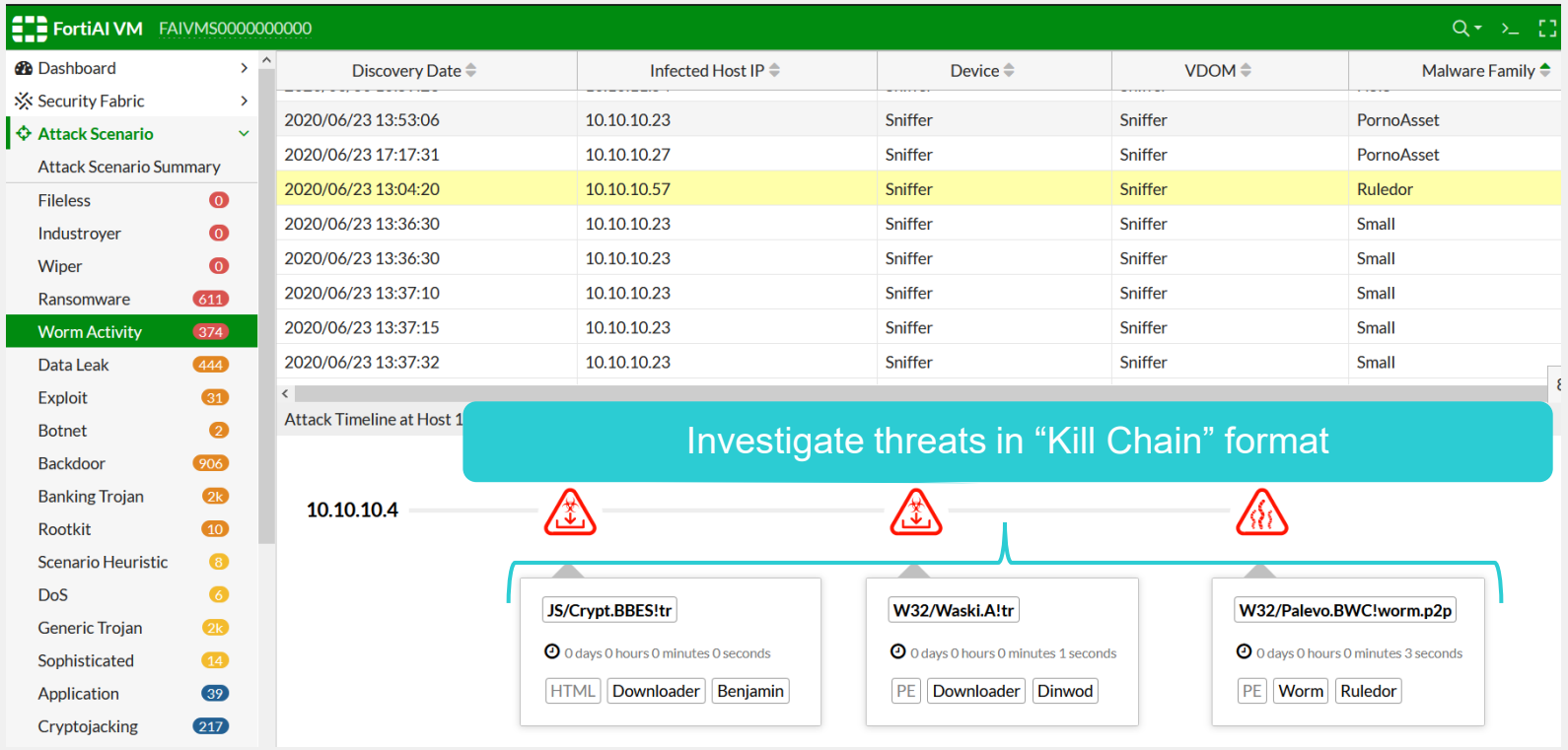
3

3 **Расследует**

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

Решает

Распознает горизонтальное и вертикальное распространение



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

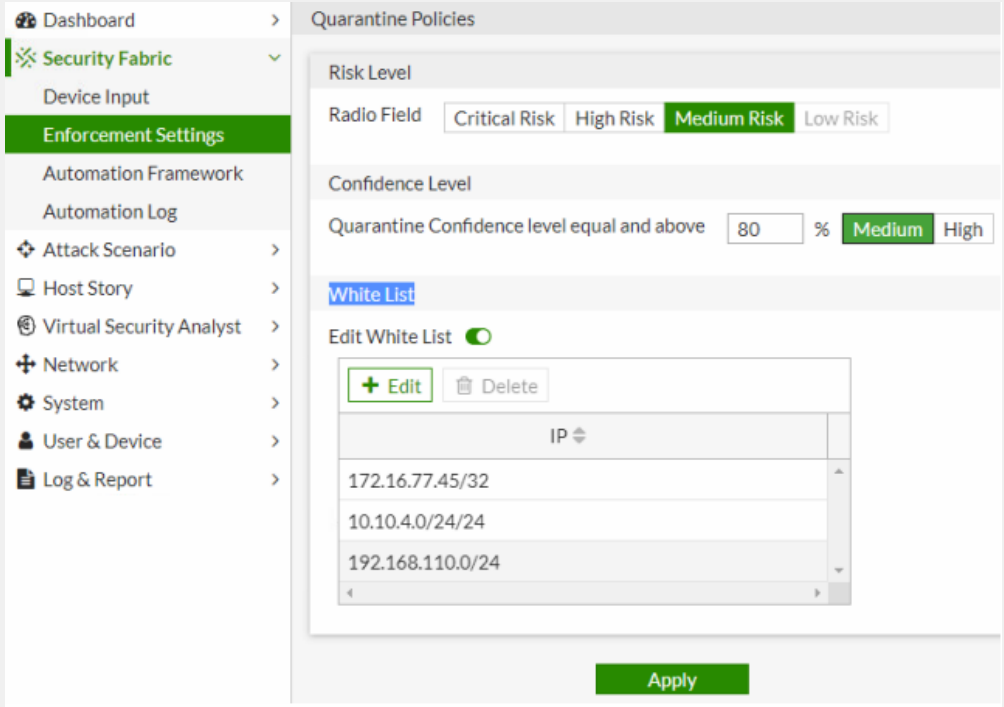
4

4 **Automated Response**

Зассчет интеграции с FortiGate – блокирует угрозы в реальном времени.

Решает

Сценарии по устранению угрозы в реальном времени



FortiGate quarantine based on FortiAI risk & confidence levels

FORTINET SECURITY FABRIC

FortiGuard

FortiSar

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 (Hancom), 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

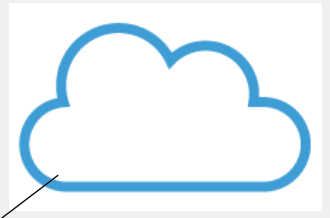
4) Ручная загрузка файлов

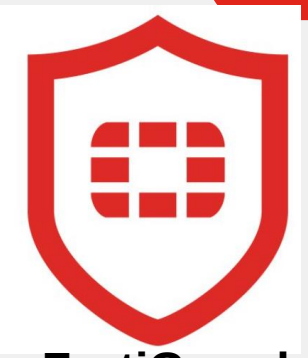
FortiAI 3500F

Inline blocking (v7.0.1)

Практические сценарии

Топология сети





FortiGuard

FortiSandbox

172.16.10.100

FortiAI
172.16.10.177

FortiGate

172.16.10.1

192.168.30.1

Attacker
192.168.30.30

Switch

Windows_Client
172.16.10.2

FORTINET SECURITY FABRIC

Наши контакты:

по общим вопросам cis@fortinet.com
по техническим вопросам cis_se@fortinet.com