FORTINET

FortiAI
сверхбыстрый анализ угроз при поддержке искусственного интеллекта

Вячеслав Гордеев

FSA, FAI, FML, FWB

Agenda

01
Видение

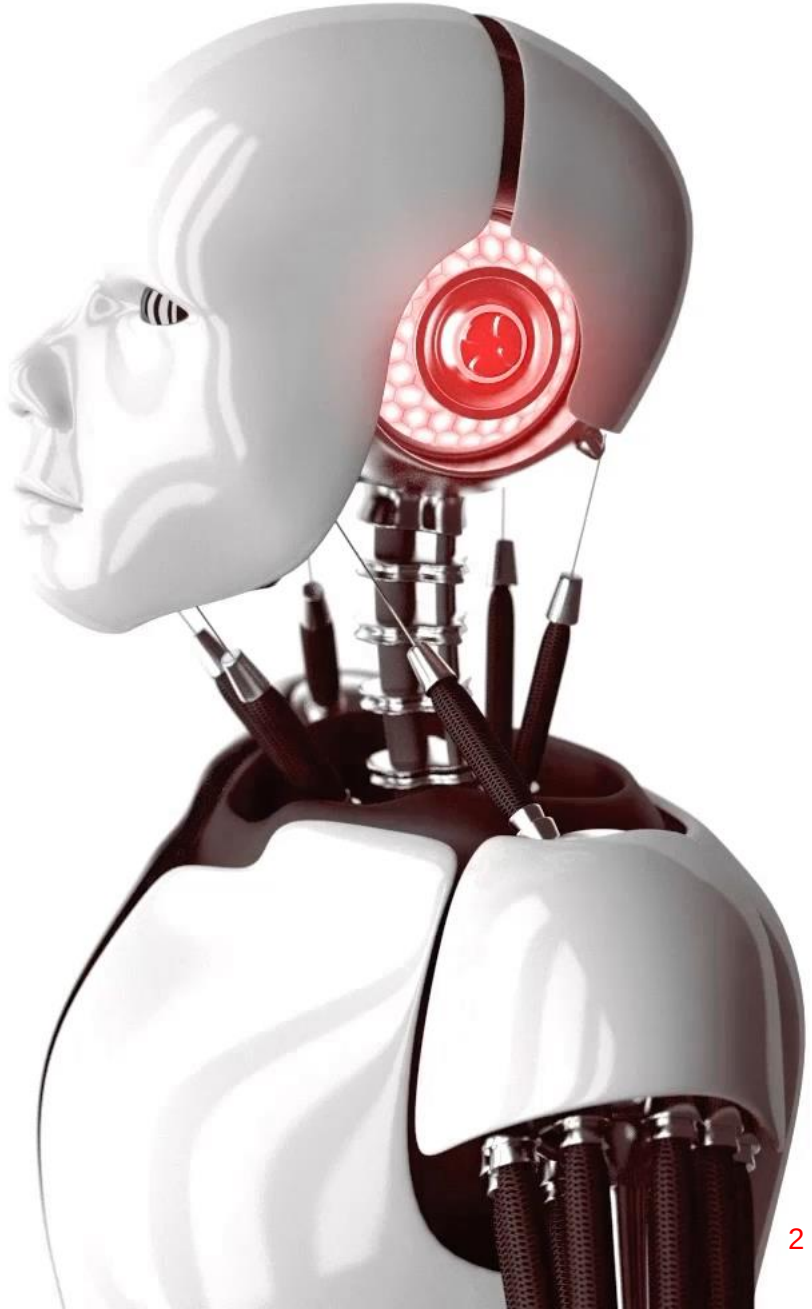
02
Эволюция ВПО

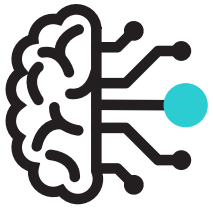
03
FortiAI введение

04
Virtual Security Analyst™
Возможности

04
Как работает FAI?

05
Демо





FortiAI
Видение

FortiAI Product Vision / Goal

*“Использование AI/ML для имитации человеческих возможностей, а **Virtual Security Analyst™** помогает SecOps в расследовании инцидентов.”*

Расследование инцидентов

Использование AI/ML для имитации человеческих возможностей

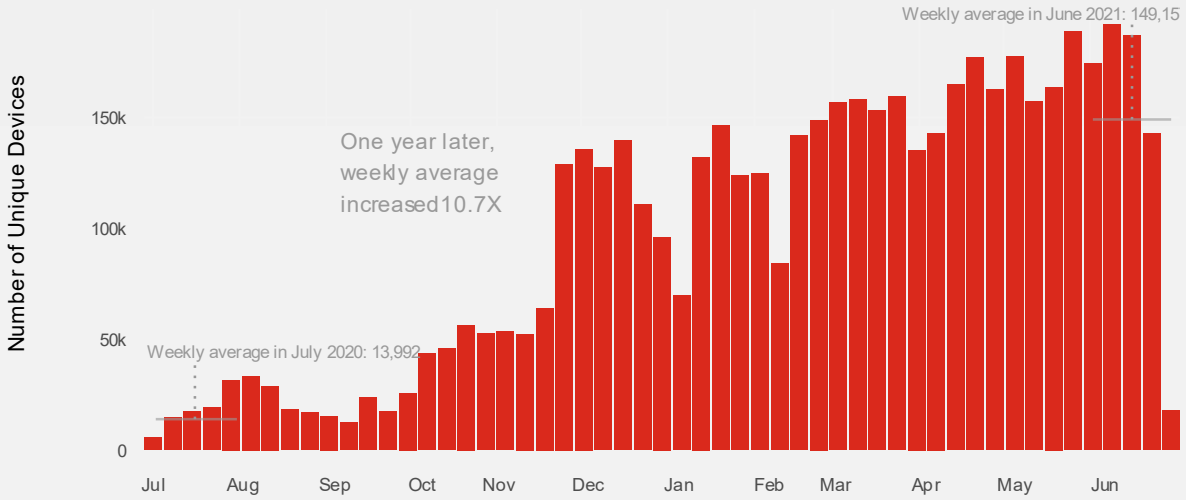
- Incident analysis
- Outbreak Search
- Malware Analyst

Уменьшение времени обнаружения

Время обнаружения меньше одной секунды

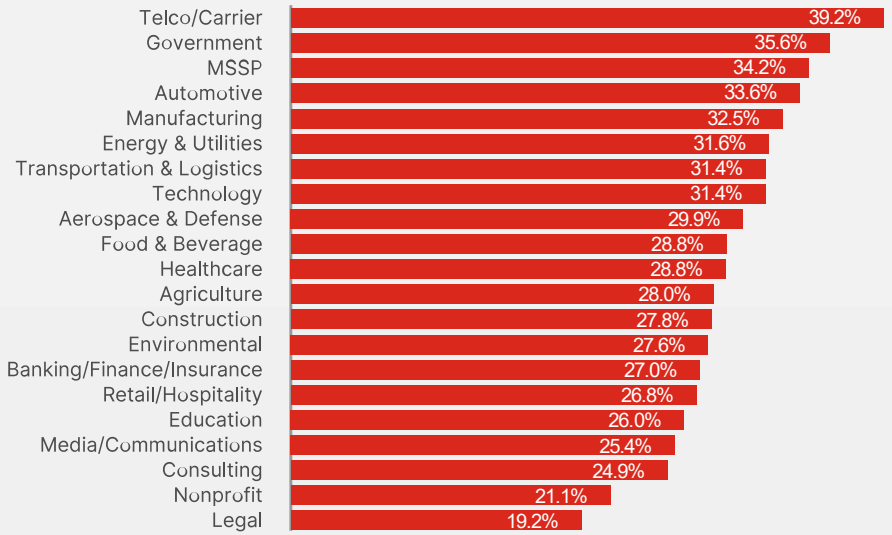
Вызов №1 – Вирусы-вымогатели (Ransomware)

Десятикратный рост активности за год (07.2020-07.2021)



>10x

Рост активности за год

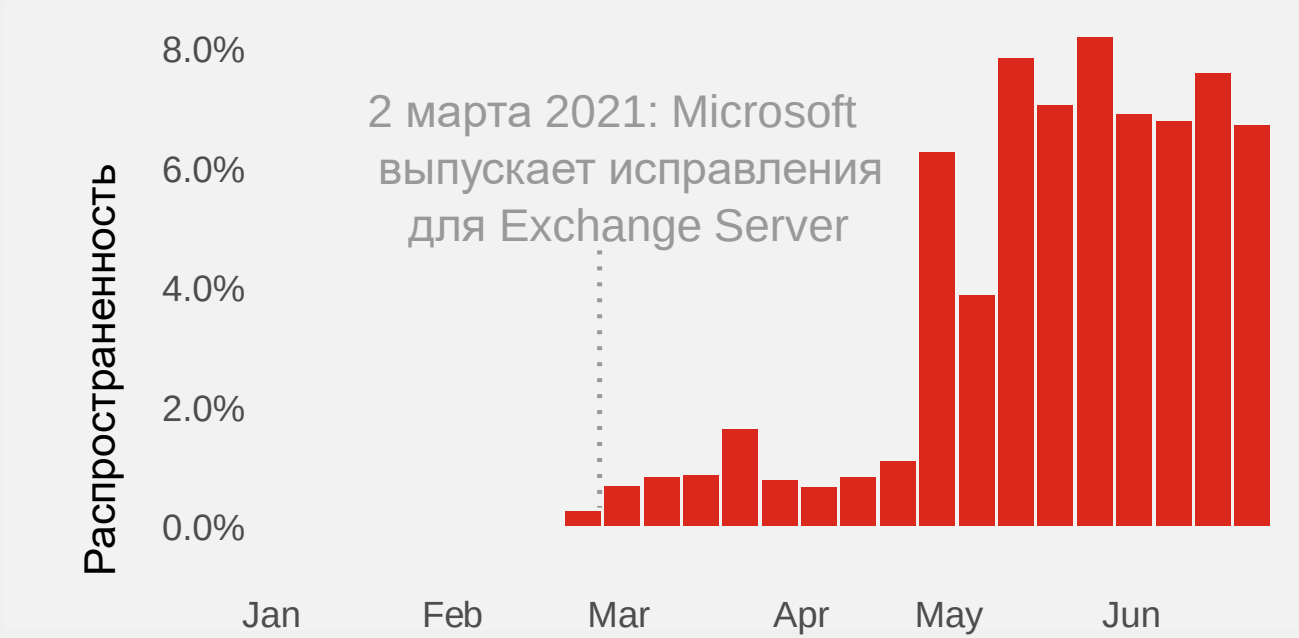


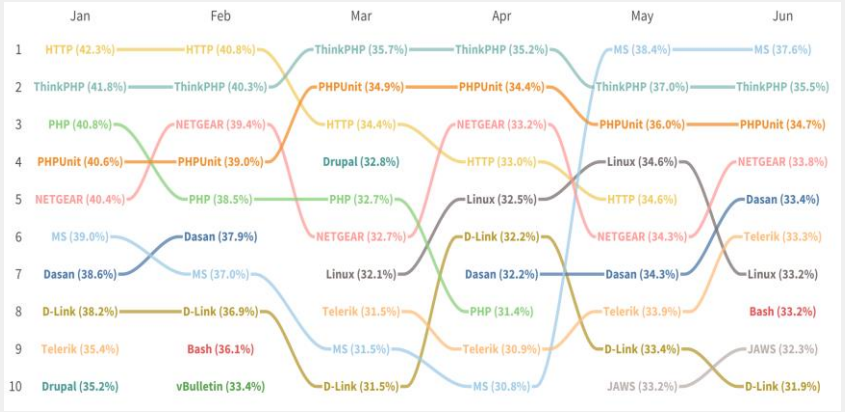
20-40%

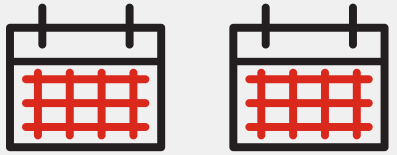
Распространенность по секторам экономики

Вызов №2 – Новые уязвимости приложений

На примере критичной уязвимости в Microsoft Exchange – ProxyLogon







- **Новые критичные уязвимости Microsoft Exchange, риски:**
  - **Доставка вредоносного кода**
  - **Компрометация деловой переписки**

- **С мая Microsoft на 1-м месте в статистике IPS по миру**

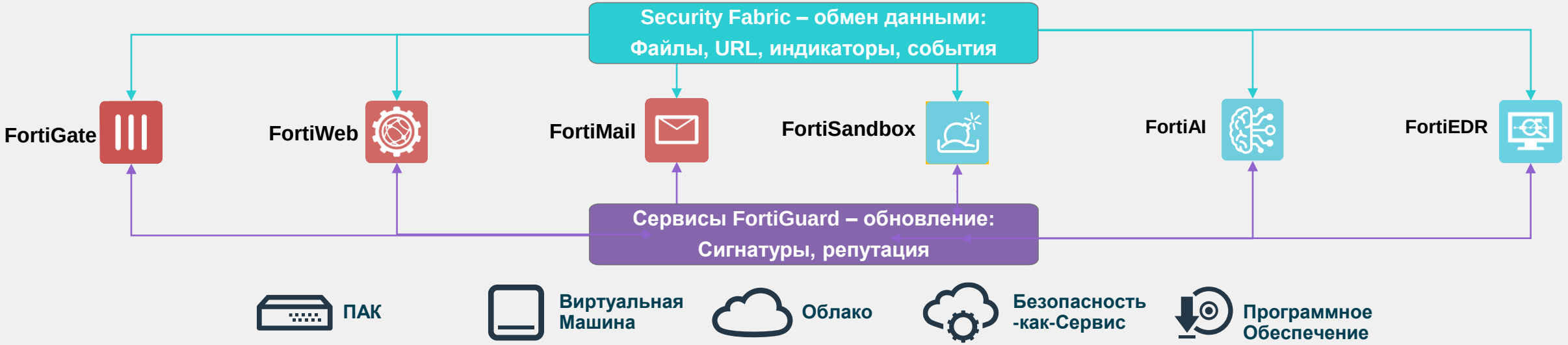
Защита от вирусов-вымогателей средствами Fortinet

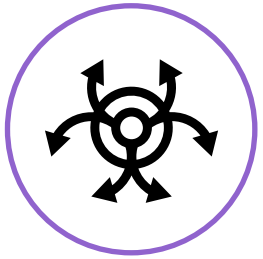
Архитектура решения

Предотвращение доставки

Выявление и подавление подозрительной активности

FortiGate	FortiWeb	FortiMail	FortiSandbox	FortiAI	FortiEDR
Шлюз безопасности (Network Firewall) • Снижение поверхности атаки • Предотвращение распространения вредоносного кода и эксплуатации уязвимостей	**Межсетевой экран веб-приложений (WAF)** • Предотвращение эксплуатации уязвимостей приложений • Защита от загрузки вредоносного кода	**Шлюз электронной почты (SEG)** • Предотвращение доставки вредоносного кода • Предотвращение фишинга • Защита от мошенничества	**Сетевая песочница** • Анализ поведения файлов и ссылок • Формирование индикаторов	**Локальный искусственный интеллект** • Исследование файлов с помощью нейронной сети • Мгновенная реакция, высочайшая производительность	**Anti-APT** • Предотвращение заражения • Обнаружение и подавление действий злоумышленника

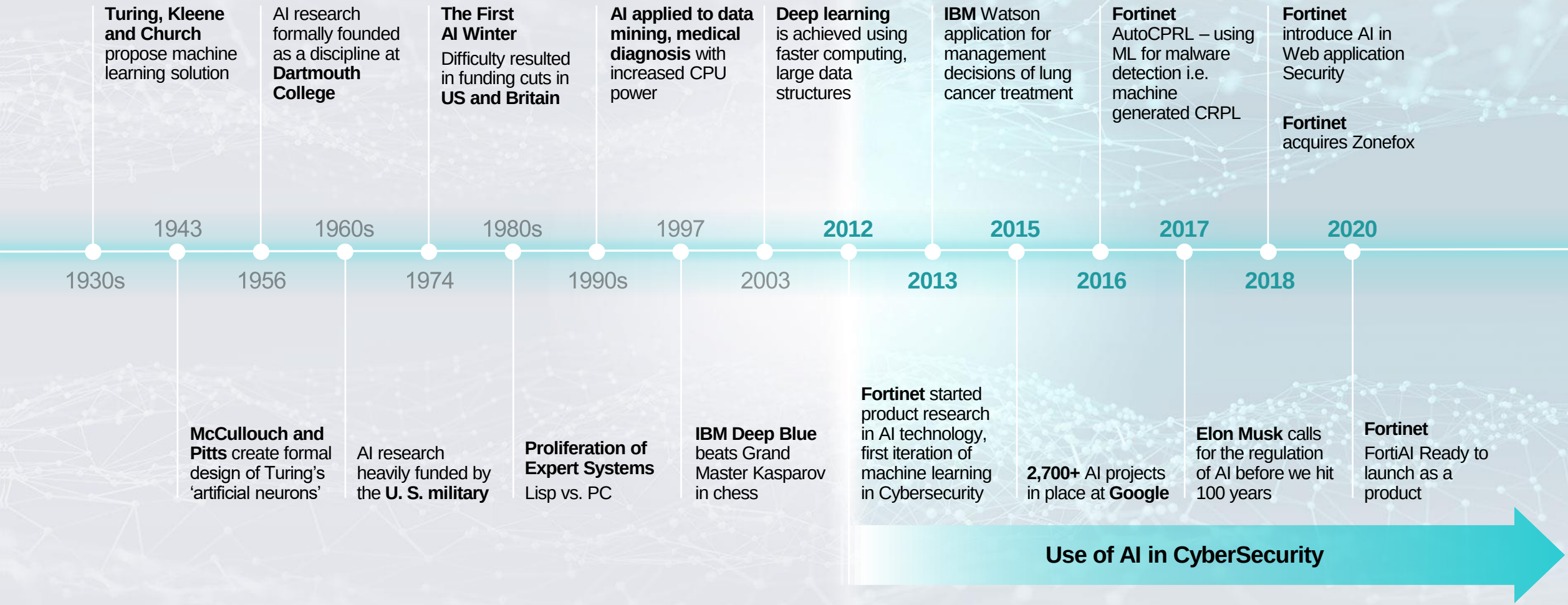




Обзор **Эволюции Вредоносного ПО**

History of Artificial Intelligence

Nearing a Century of AI

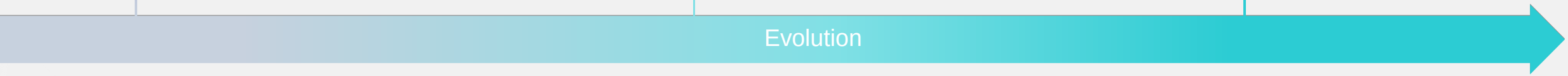


Evolution of Malware Detection

Methods & Problems

"We create new technology *to solve problems that existing technology cannot solve today."*

M. Xie, CTO Fortinet



Malicious Code Detection

Advance Threat Protection (ATP) products at a glance

AV engine

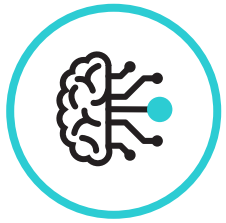
Inspect core of apple…

Um, it's bad.

FortiSandbox

Let me take a bite…

Um, it's bad.



FortiAI

Let me describe it - rotten, smells...

Um, it's bad.

FortiDeceptor

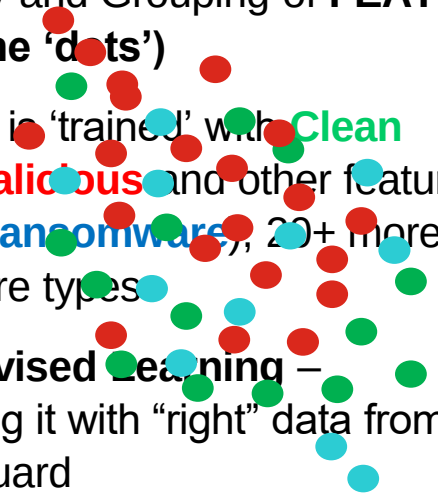
Let me place more apples…

…with traps.

FortiAI
Введение

AI / Machine Learning: what do we expect?

- Machine Learning to find **PATTERN**
- Identify and Grouping of **FEATURES (aka the 'dots')**
- FortiAI is 'trained' with **Clean** and **Malicious** and other features (e.g. **Ransomware**), 20+ more malware types
- **Supervised Learning** – Feeding it with "right" data from FortiGuard



Result

- Patent pending Neural Network for sub-second detection, with analyst logic

FortiAI Key Benefits

Virtual Security Analyst™

- Trace Source on infection
- Outbreak Search
- Personal Malware Analyst
- On Prem Learning

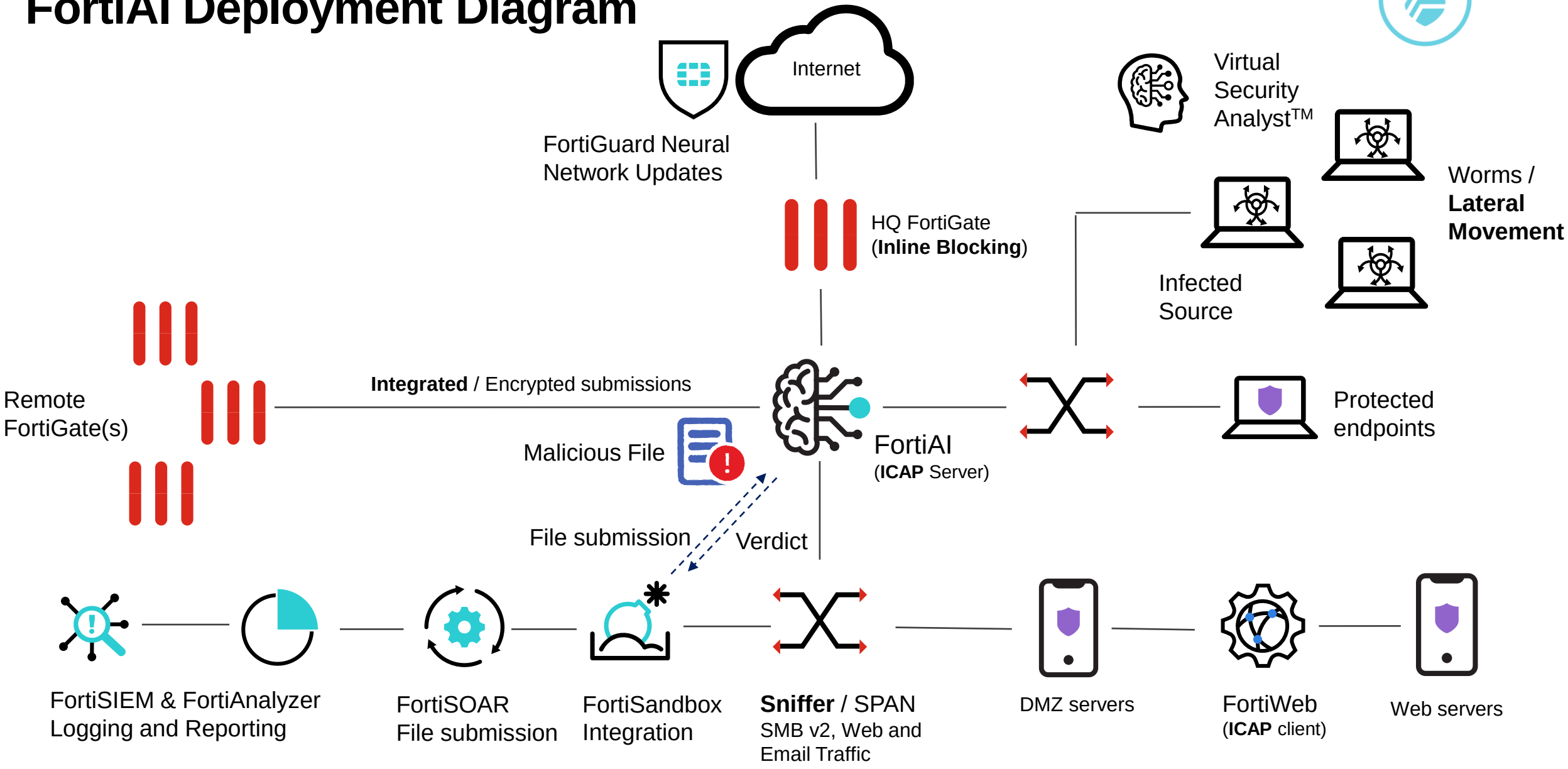
Breach Prevention

- Sub-second Verdict
- Threat Investigation
- Big Picture analysis
- Attack Scenarios

Fabric Integration

- Blocking & Quarantine with FortiGate(s)
- STIXv2 / JSON output
- REST API for submission
- FortiAnalyzer/FortiSIEM support
- FortiSandbox integration (increase coverage)
- SYSLOG / ICAP for 3rd party

FortiAI Deployment Diagram



Virtual Security Analyst ™
Възможности

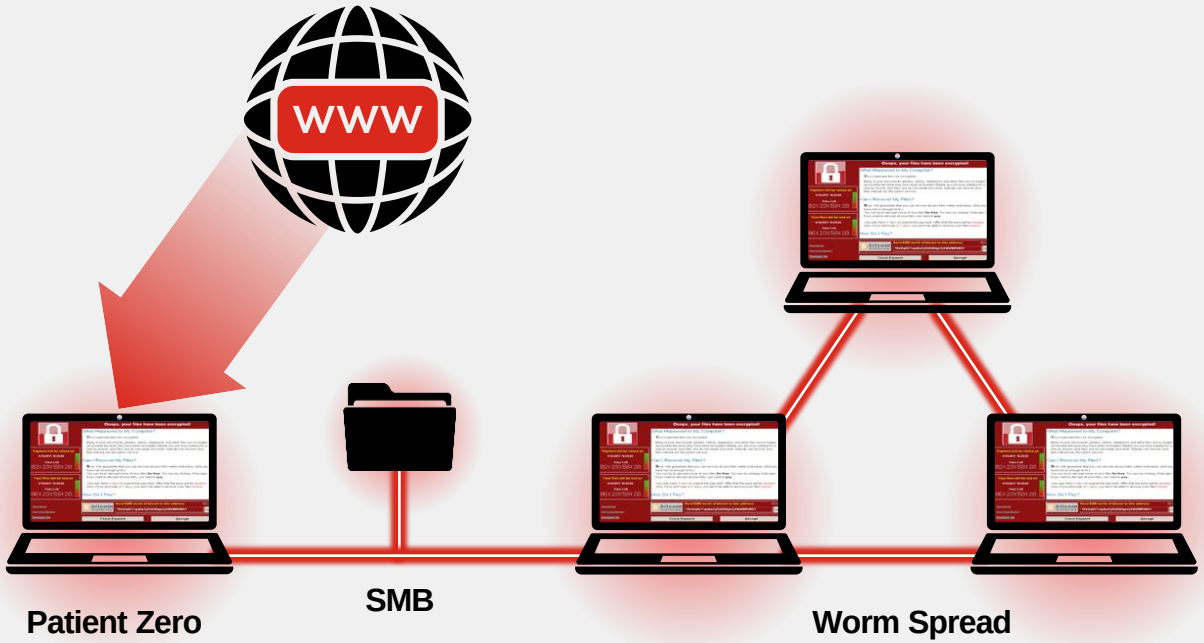
FortiAI Virtual Security Analyst ™

Tracing the source of attack

Attack Scenario

- How malware was spread through the network
- Scenario **Finding "Patient Zero"** based engine linking infections by time
- Sub-second verdict
- Ability to quarantine with FortiGates

FAI GUI: kill chain analysis

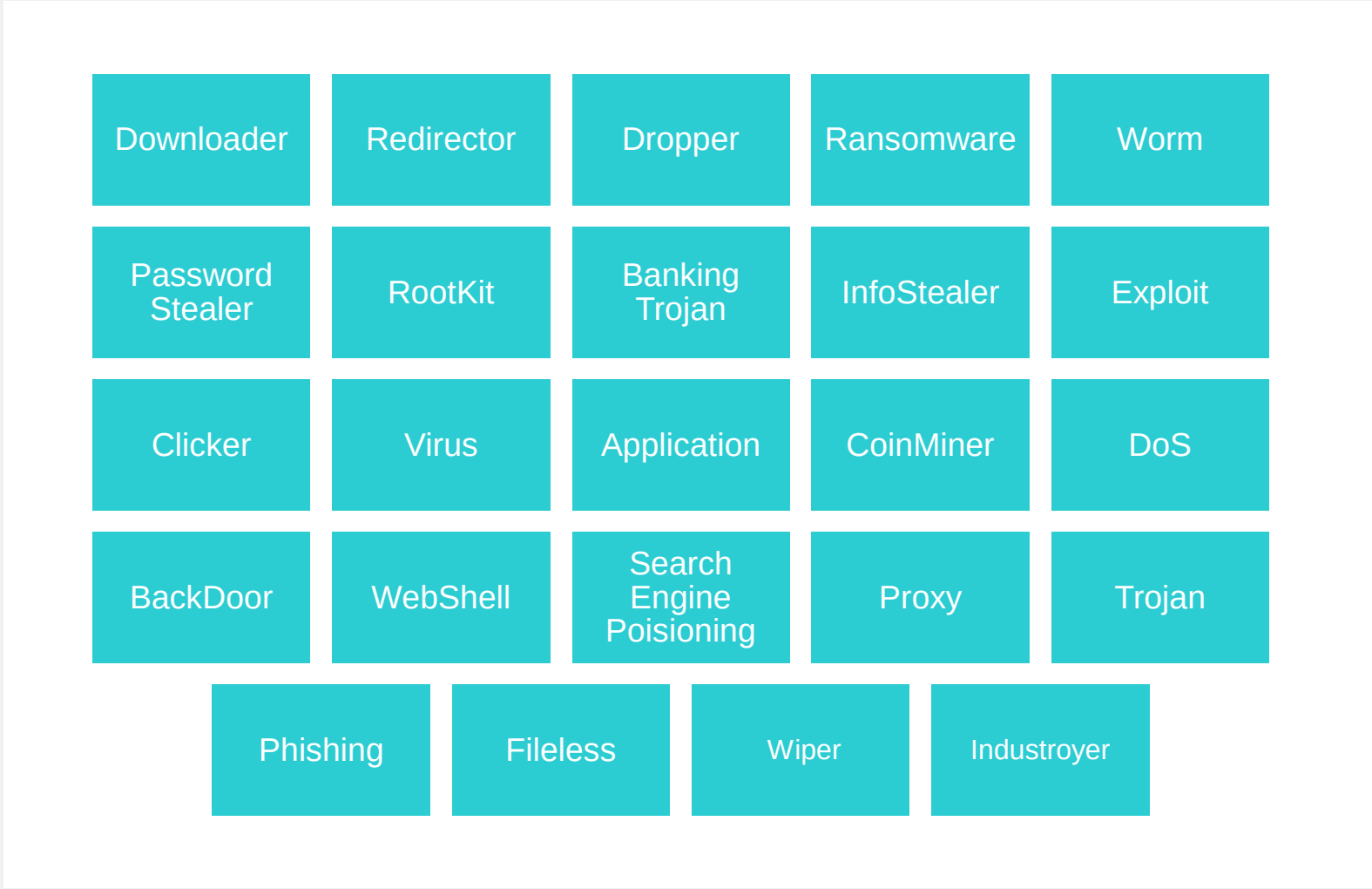


FortiAI Virtual Security Analyst ™

Malware Analyst Function

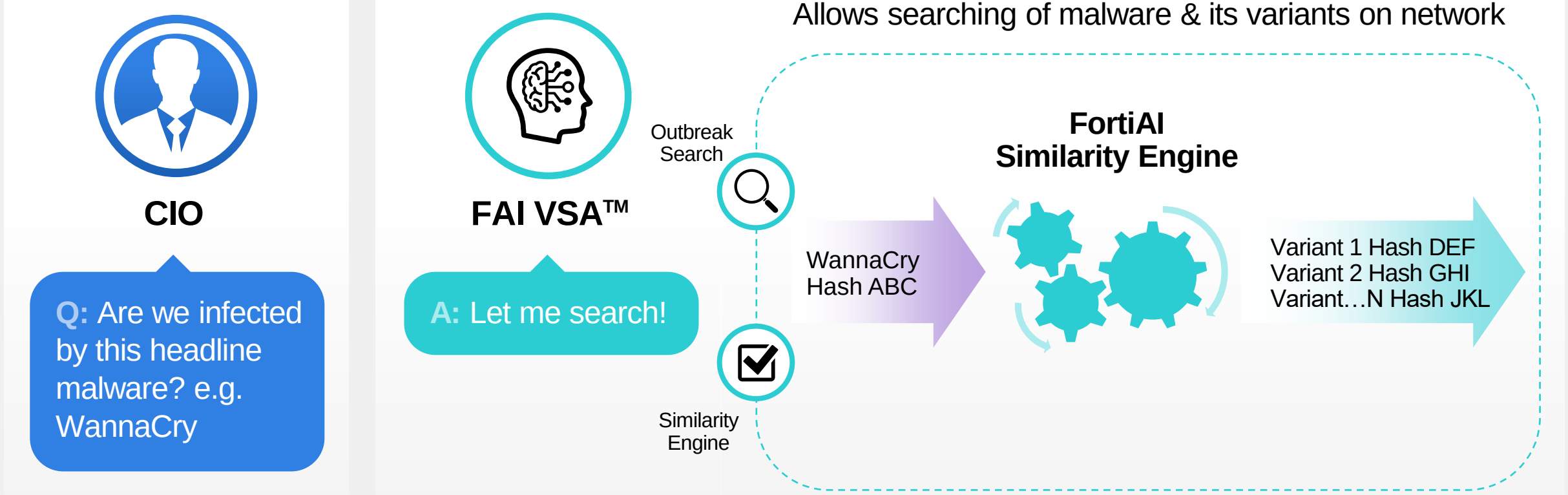
Your malware analyst – identify 20+ Attack Scenarios

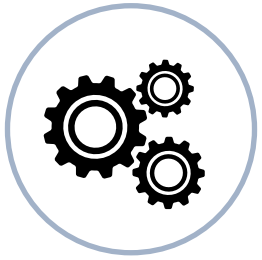
- Such as Ransomware, Dropper, PWS
  (Password Stealing Trojan), CoinMiner,
  Banking Trojan, Fileless attack etc
- Answers the questions:
  - What type of malware attacks am I under?
  - What is the intent of malware?
  - Why is it malicious?
- Feature “Tagging” in logs



FortiAI Virtual Security Analyst ™

Outbreak Search & Similarity Engine





Более пристальный взгляд на то, как **Как работает FAI**

FortiAI - Under the Hood

Patent pending # U.S. Serial No.: 16/053,479

Single Layer of Neural Network

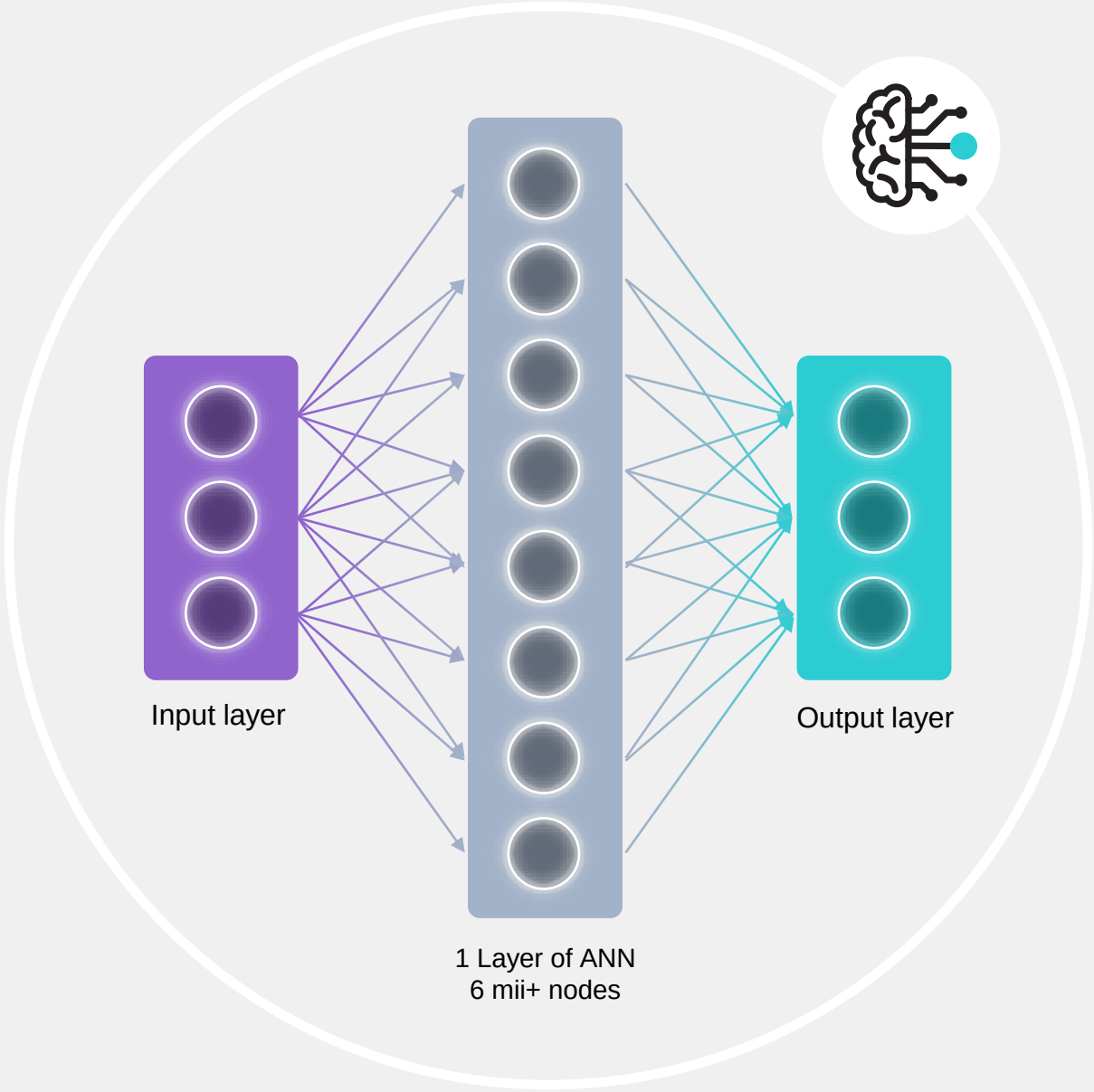
- Pre-trained with 20mil+ clean and malicious files
- Billions of clean and malicious features learnt

Each node (middle circles) represents an “Analyst”

- Job function - to determine if they match a single malware feature
- Current features DB consists:
  - PE features (Portable Executables) & Non-PE features
  - Via techniques such as file analysis of registry values, stack status, execution flow etc.

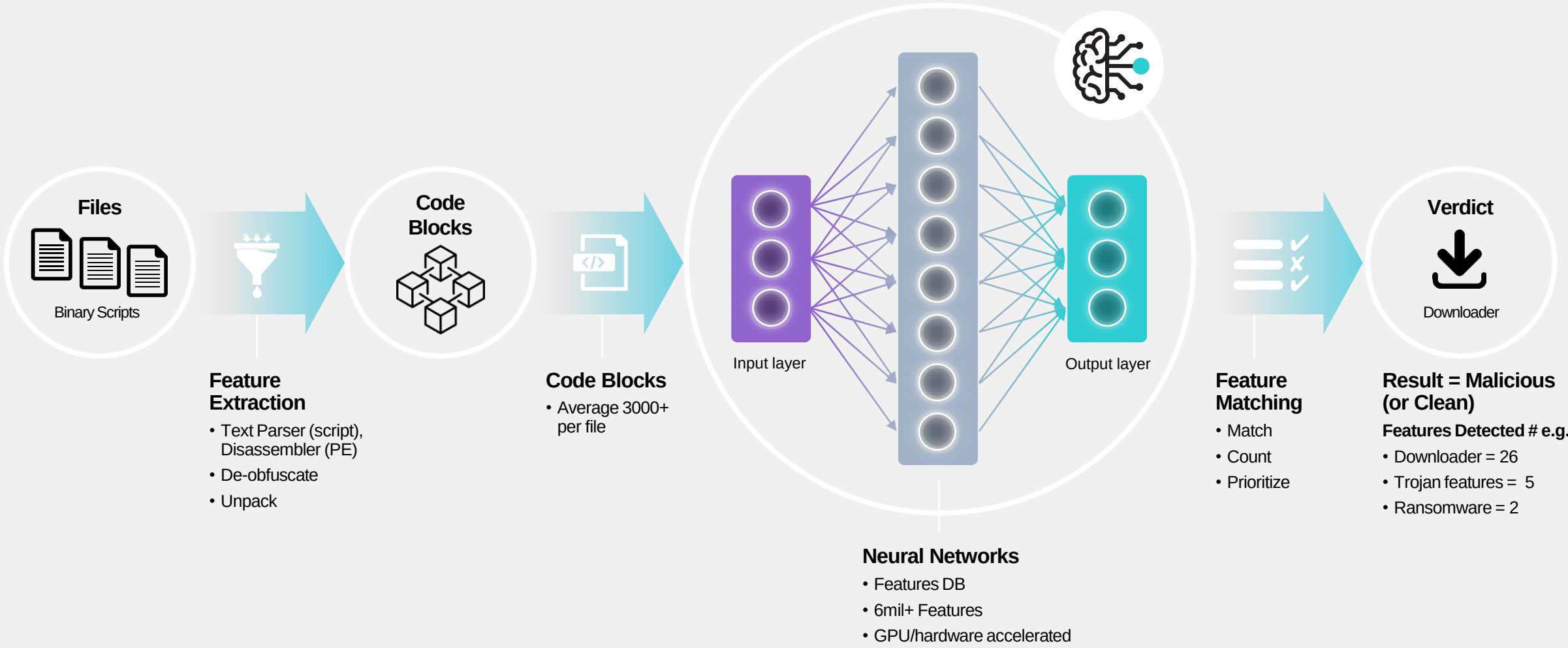
Does not require to ‘run’ the file (vs Sandboxing)

- hence speed (sub-second)
- Identify good/bad instantly



FortiAI

Malware Detection Workflow



Feature Extraction

- Text Parser (script), Disassembler (PE)
- De-obfuscate
- Unpack

Code Blocks

- Average 3000+ per file

Neural Networks

- Features DB
- 6mil+ Features
- GPU/hardware accelerated

Feature Matching

- Match
- Count
- Prioritize

Result = Malicious (or Clean)

Features Detected # e.g.

- Downloader = 26
- Trojan features = 5
- Ransomware = 2

Training in Action – Human vs Machines

Human vs Machines detection over training period

FortiAI Artificial Neural Network

- Pretrained before ship

Training phase(s) Goal

- Highest detection rate
- Lowest false +ve rate

FortiGuard Updates

- ANN update
- Keep up with latest threats

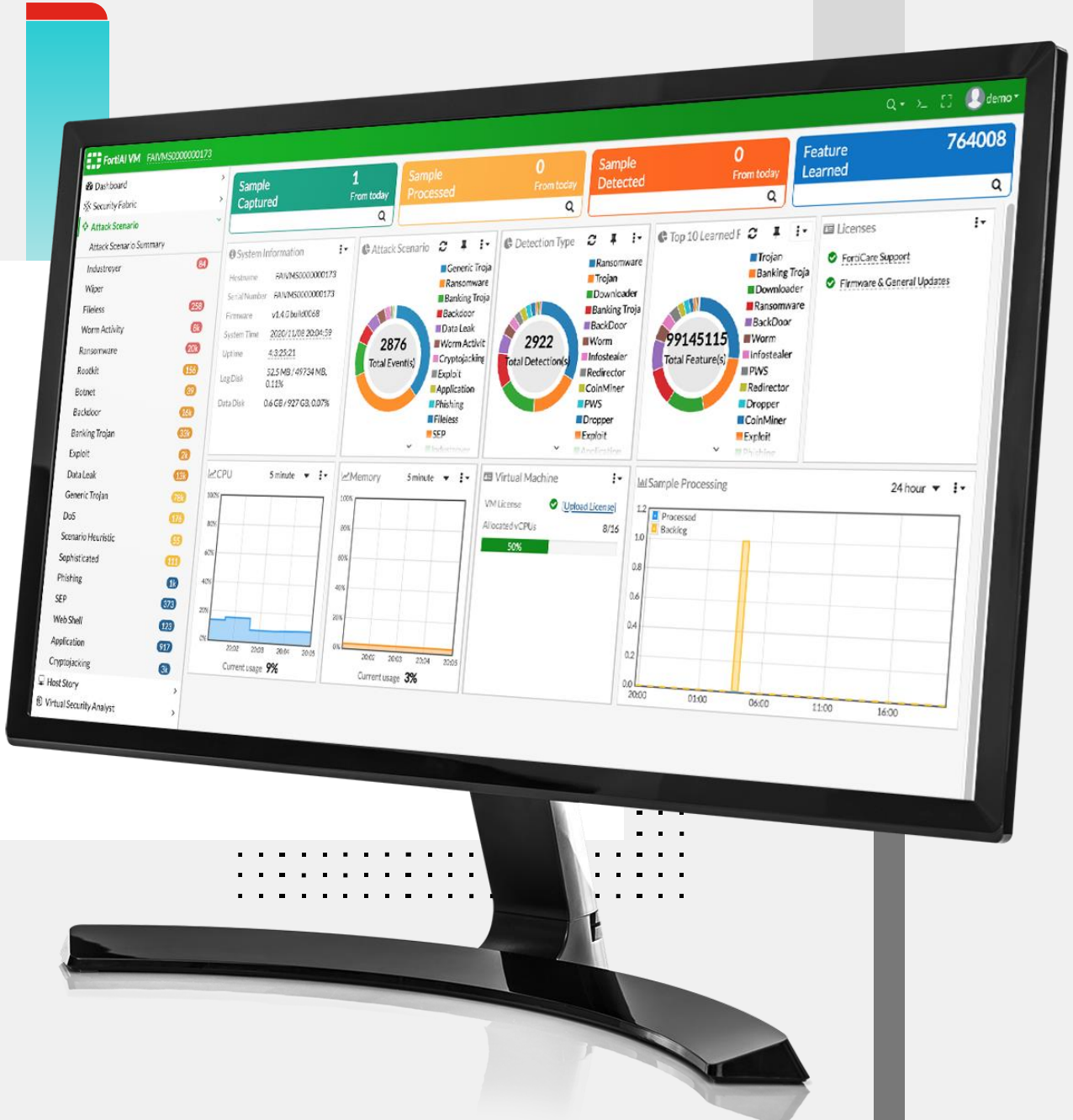
Further learning

- On Customer Premises

*Detection Rate on FortiGuard QA samples

FortiAI
demo

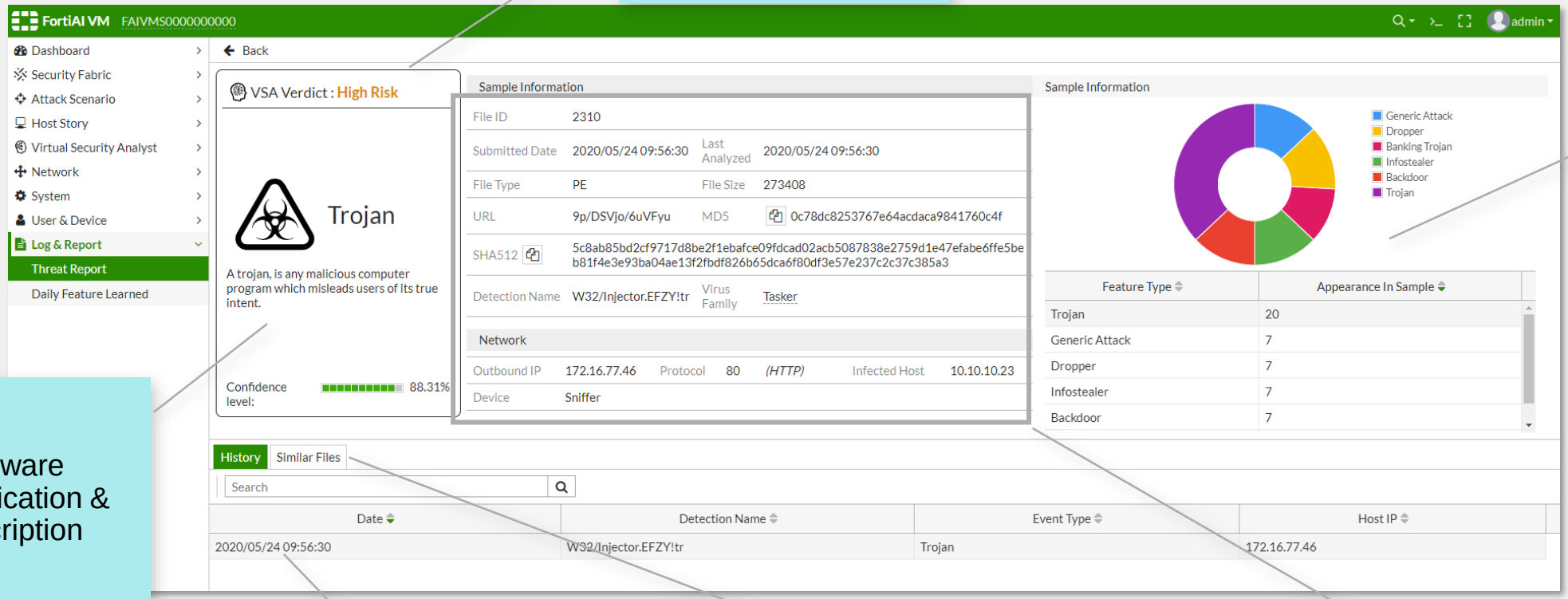
https://fortiai.fortidemo.com
demo / demo



Virtual Security Analyst™ Report

V1.3

Verdict & Confidence Level



Feature Breakdown

Malware Classification & Description

Appearance on Network (History)

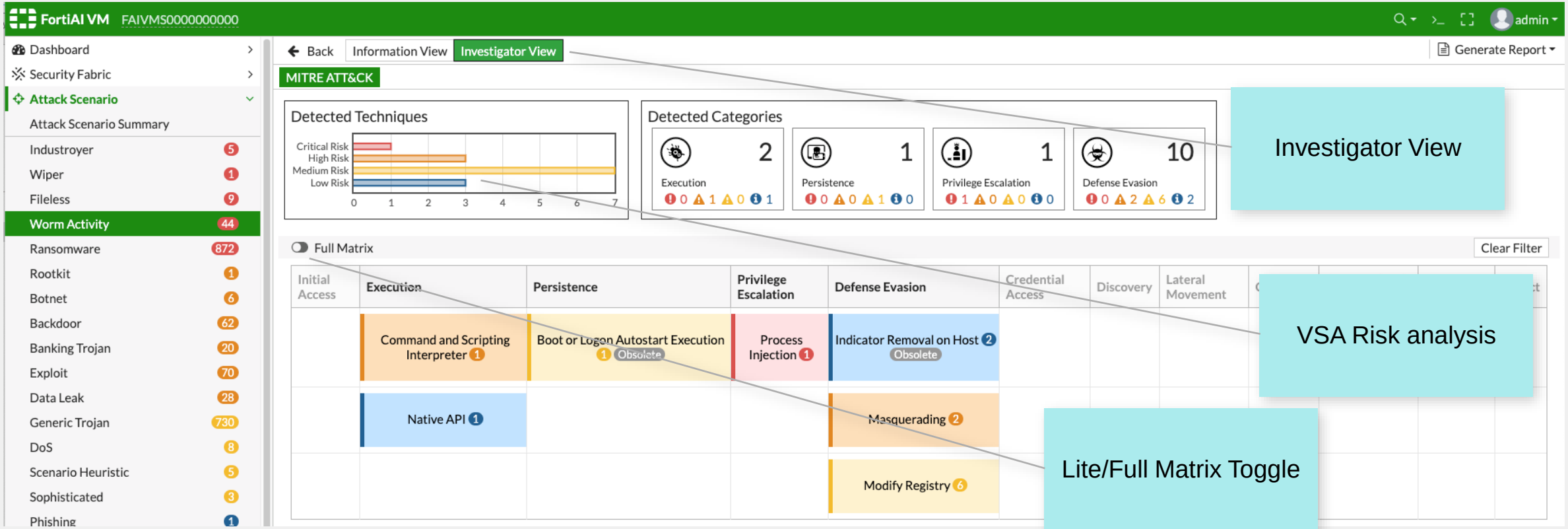
Similarity Engine Search

Hash / Type / Time / Virus Family / Source

FortAI - AI-driven Security Operations

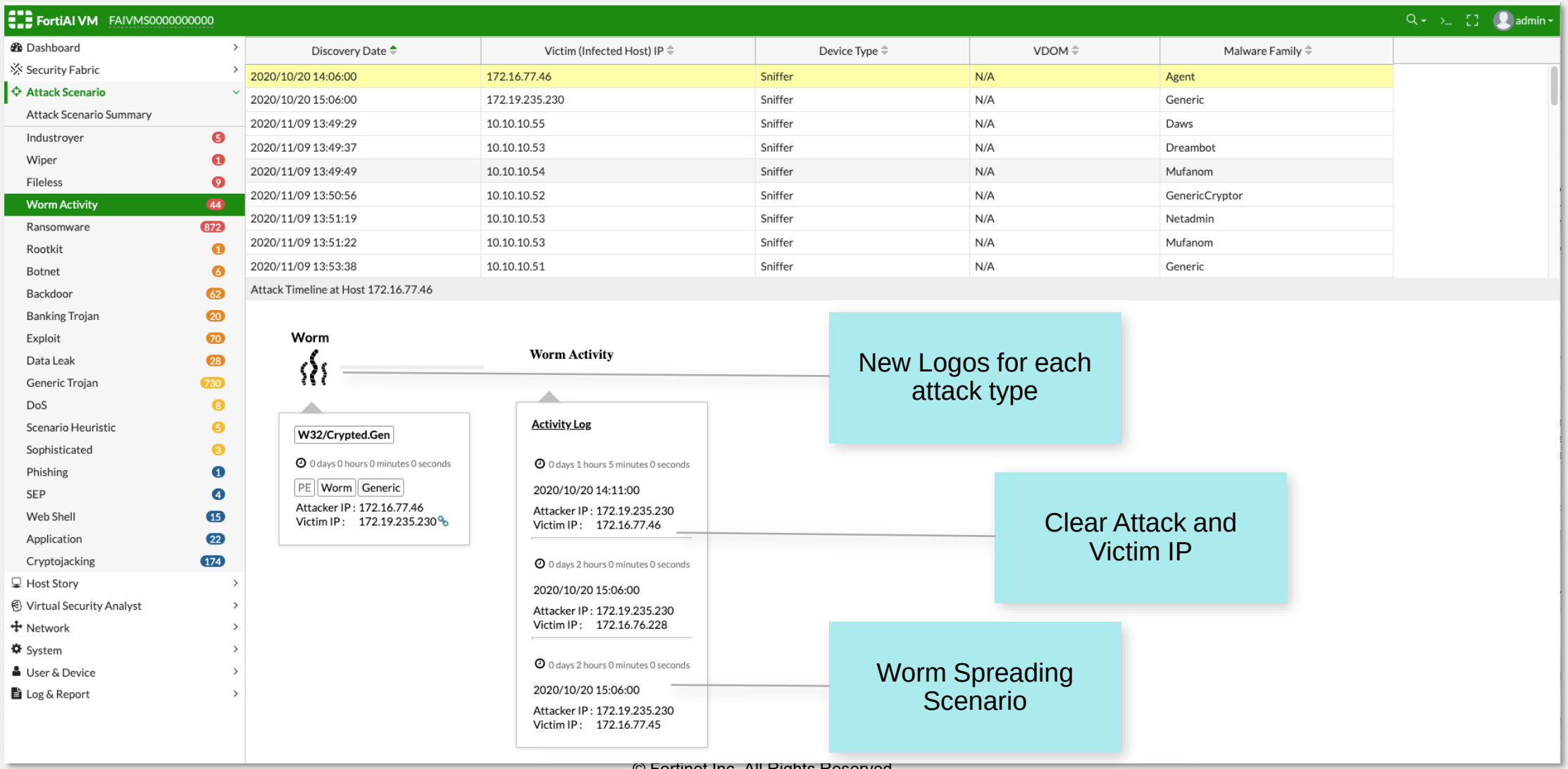
MITRE ATT&CK Mapping

- Investigator View
- Map malware into MITRE ATT&CK Tactics Techniques and Procedures (TTPs)
- Click any to Filter



FortiAI - AI-driven Security Operations

Enhanced Attack Timeline

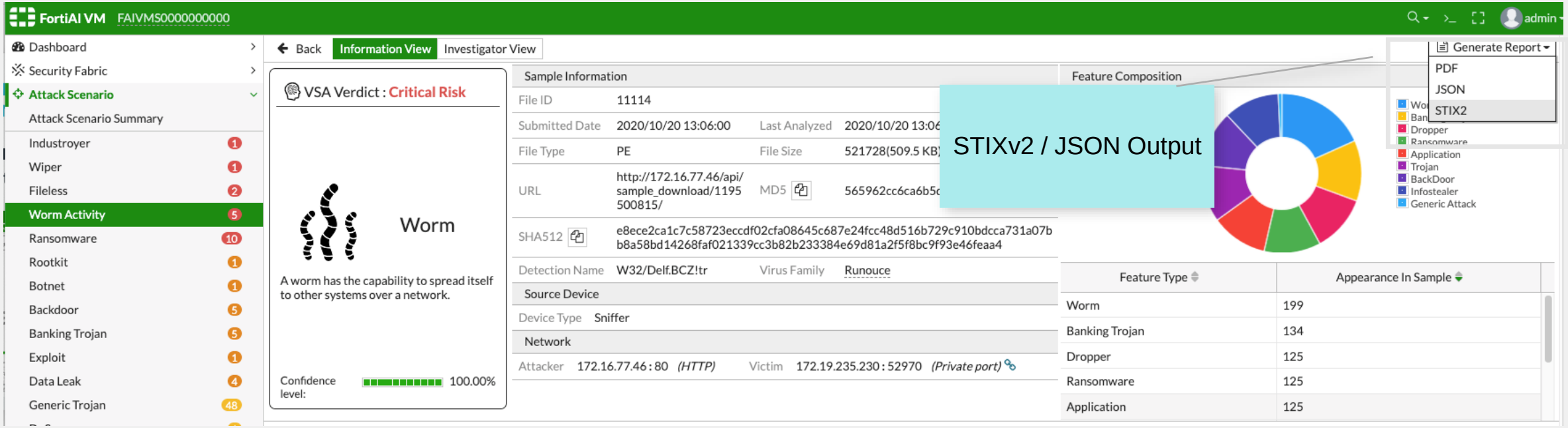


FortiAI - AI-driven Security Operations

STIX v2 and JSON support

3rd Party Threat Intelligence platform integration

- STIX v2 Output
- JSON Output



AI-driven Security Operations

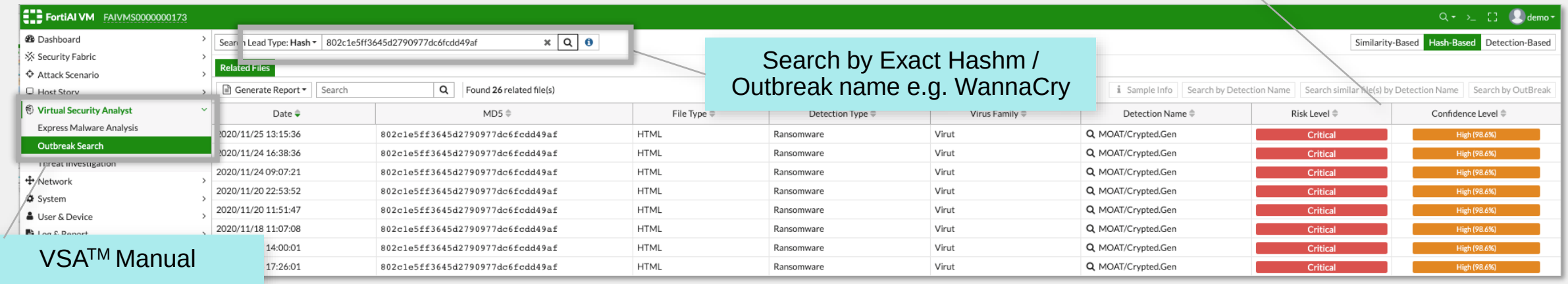
V1.3

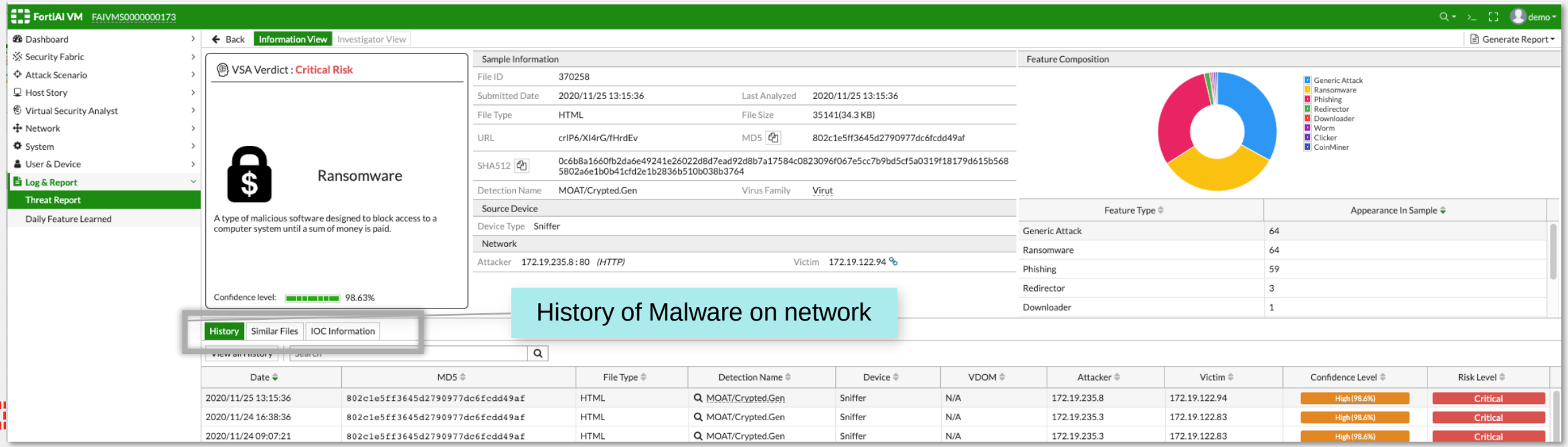
FortiAI Outbreak Search

Search by Exact Hash or Similar files (variants)

Search by Exact Hashm / Outbreak name e.g. WannaCry

VSA™ Manual



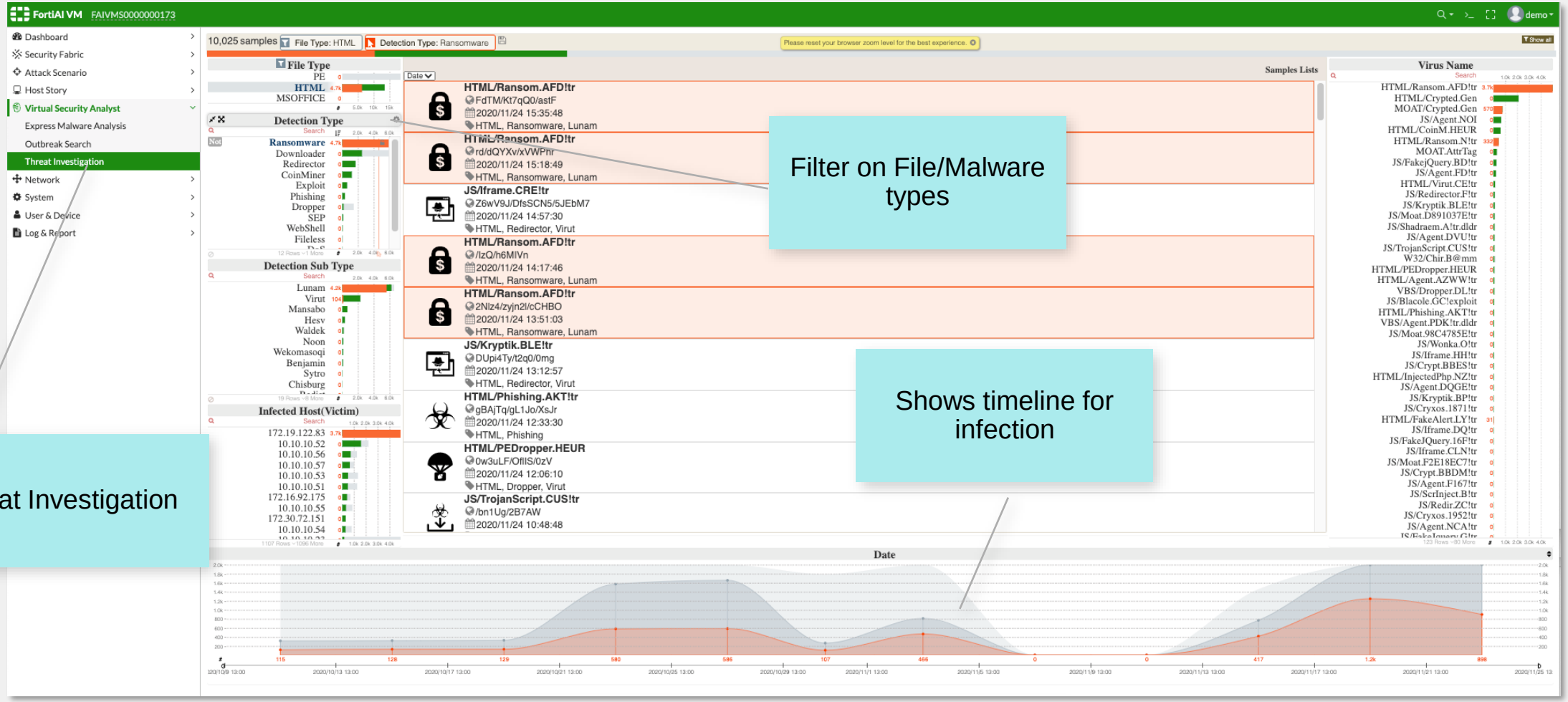


History of Malware on network

VSA™

V1.3

Threat Investigation – “Big Picture” analysis

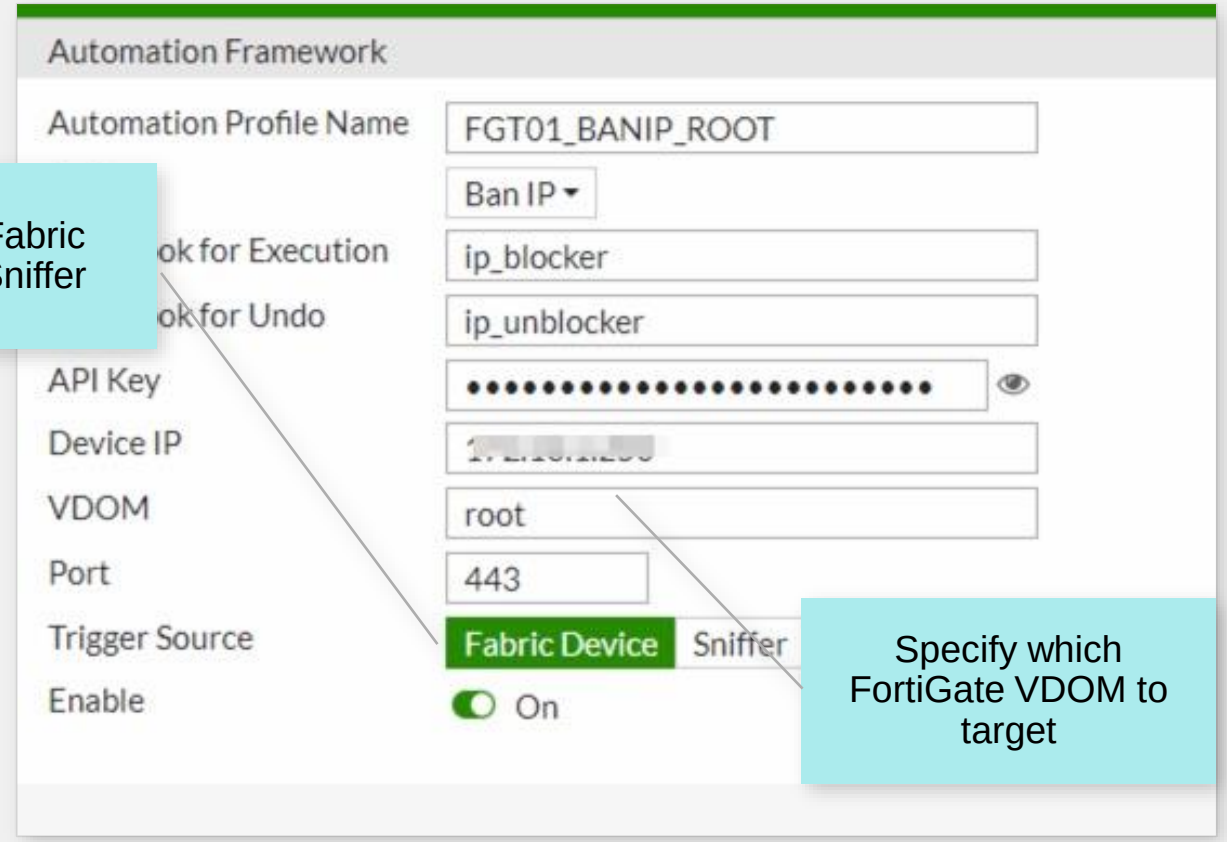


AI-driven Security Operations

Security Fabric Integration – FortiGate Quarantine

V1.3

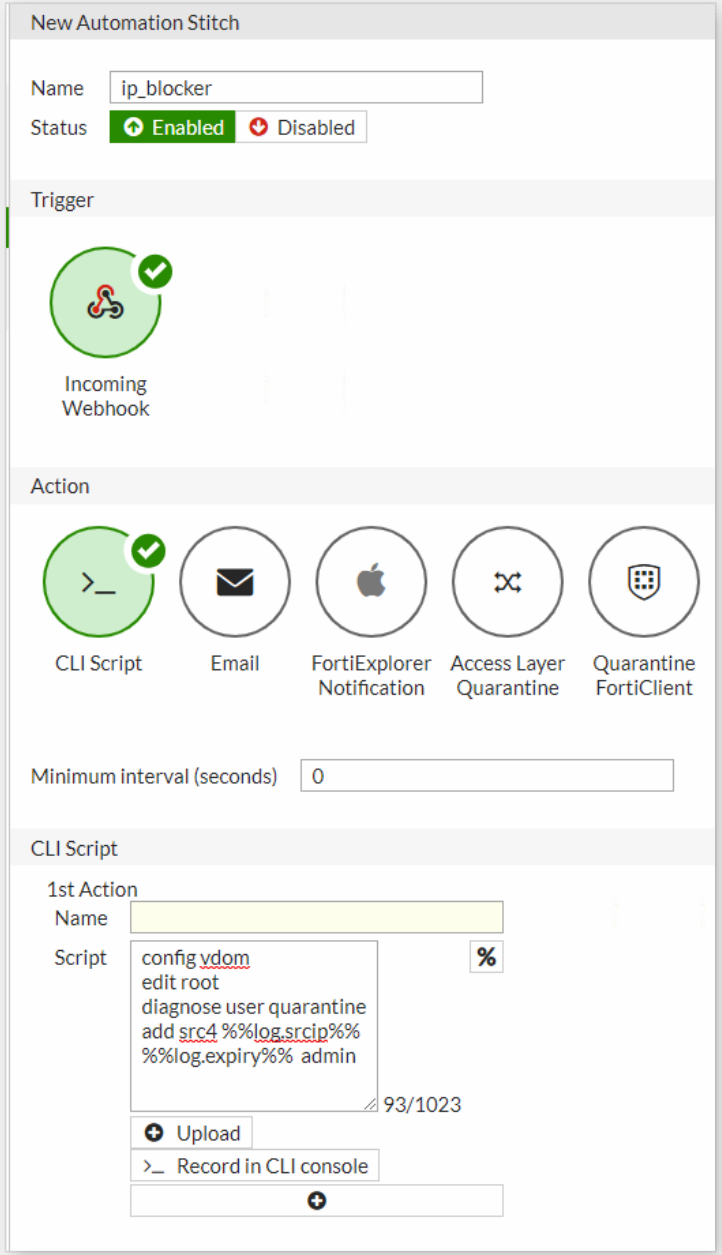
FortiAI Security Fabric Configuration:



Source of Fabric Device or Sniffer

Specify which FortiGate VDOM to target

FortiGate Configuration

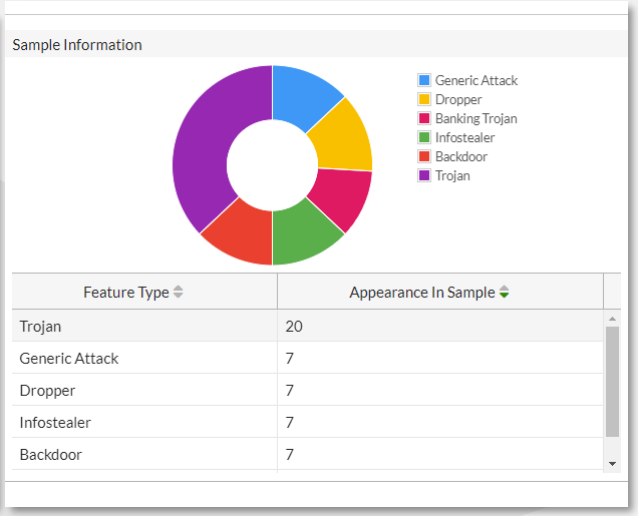


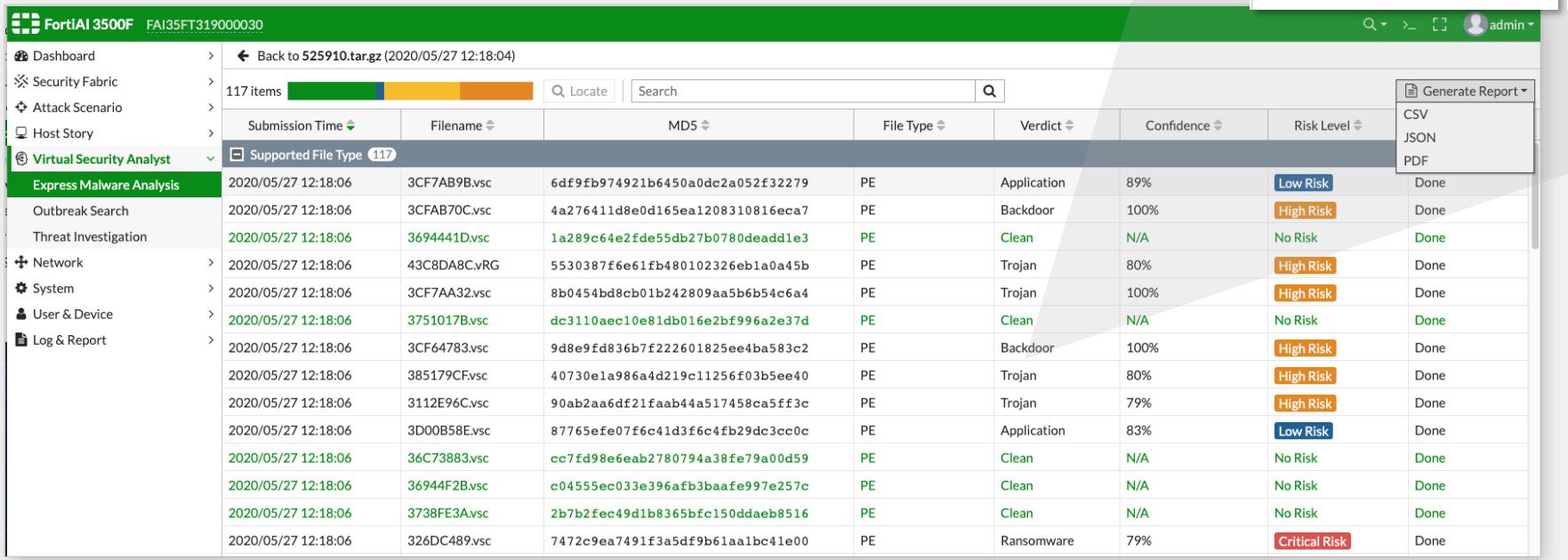
AI-driven Security Operations

Express Malware Analysis – Manual & API Upload

V1.3

- REST API upload & Manual GUI Upload
- Compress File Support (tar, gz, tgz, zip, bz2, rar)
- Password Support (e.g. infected)
- VSATM Sub-Second verdict





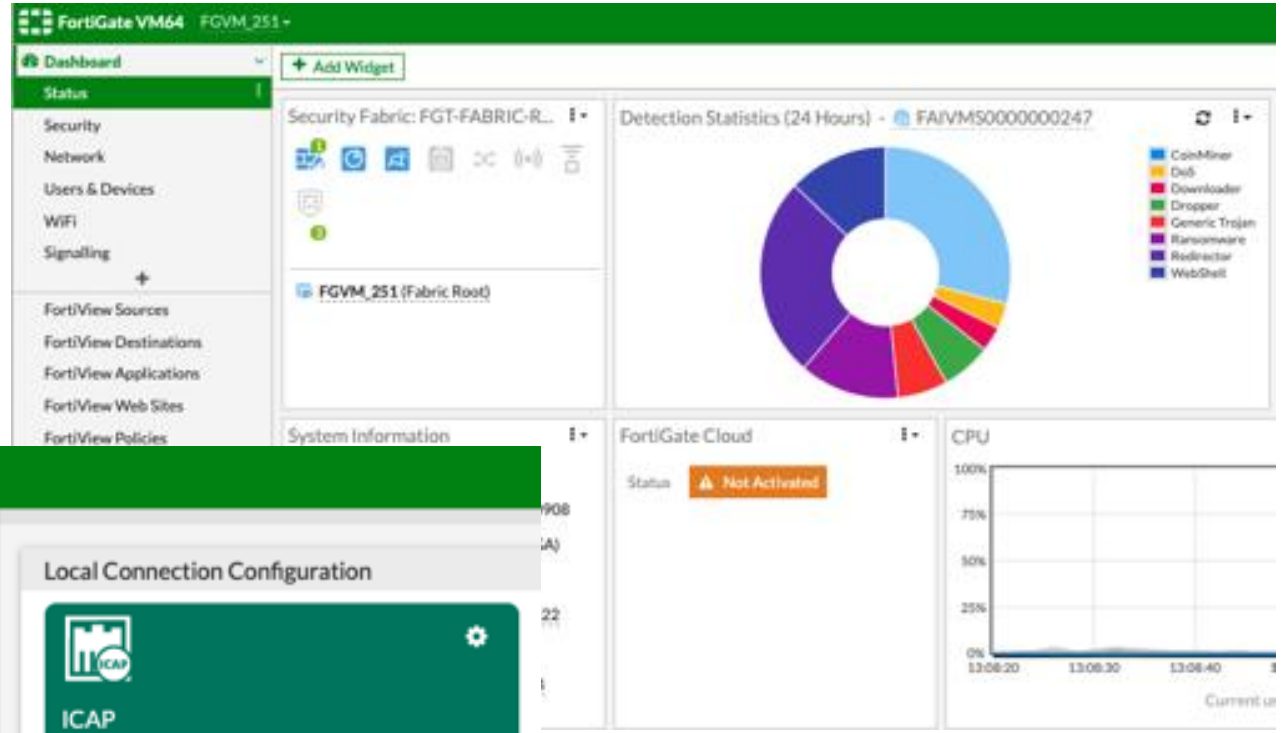
FortiAI - What's New v1.5.1

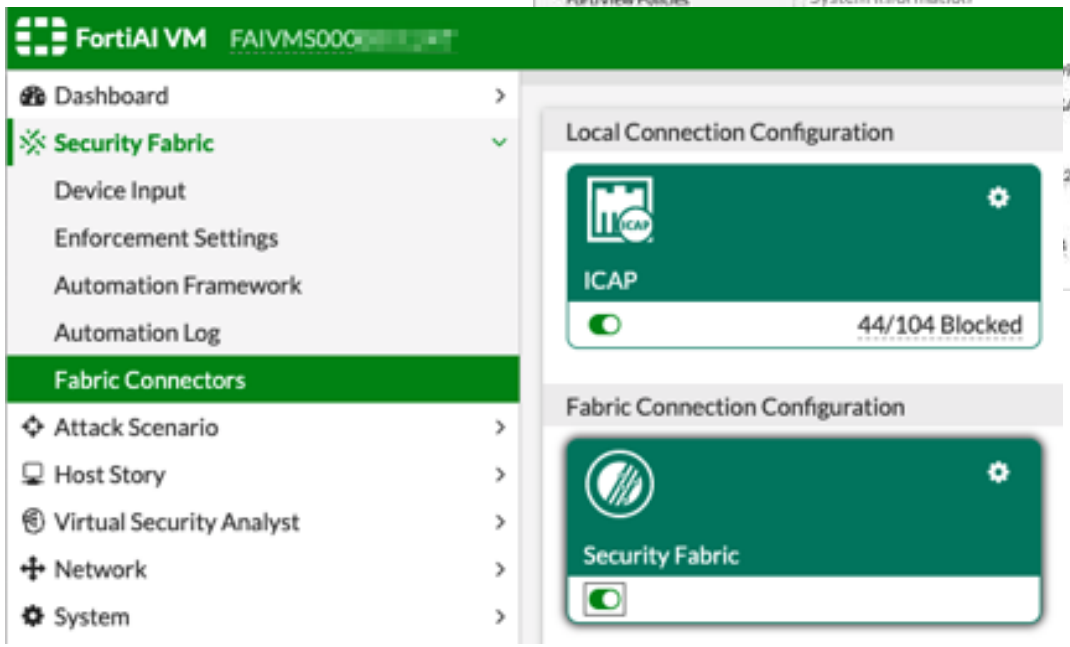
FortAI - AI-driven **Security Operations**

V1.5

Security Fabric Pairing

- Appears in FortiOS topology
- FOS widgets to display type of malware on network (e.g. Ransomware, Banking Trojan)
- FortiAI Security Fabric Connector





FortAI - AI-driven **Security Operations**

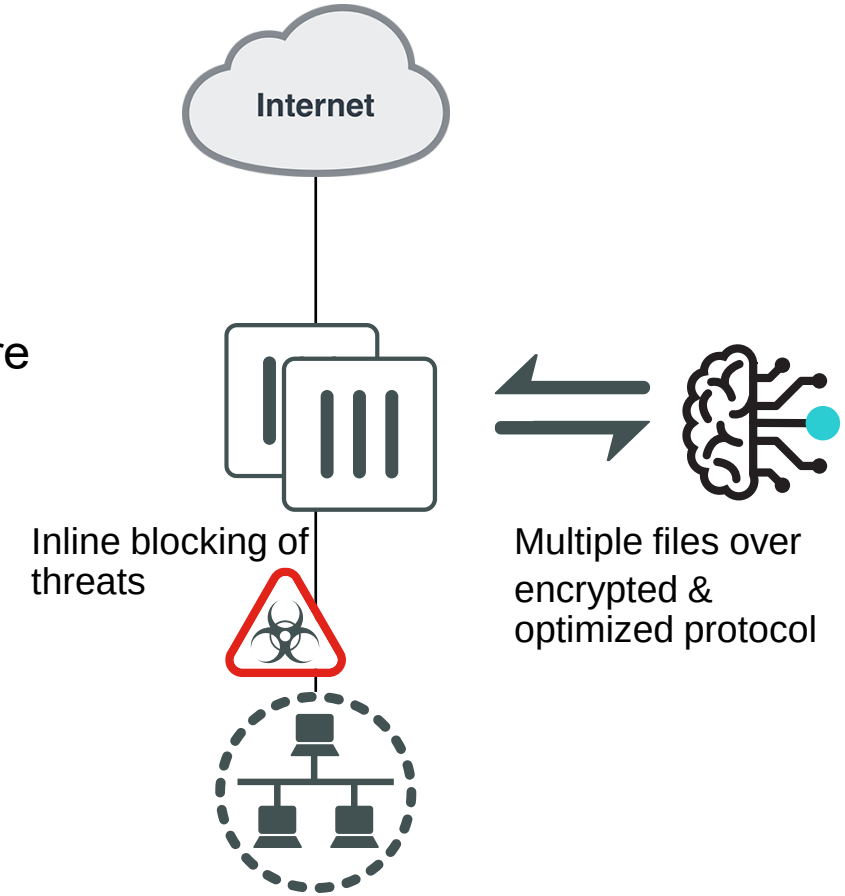
FOS 7.0.1

Background:

- FAI v1.4 uses ICAP and OFTP (FortiSandbox Field) with FOS integration (FOS v6.4)
- Customer cannot run FSA/FAI at same time

What's New:

- In FOS 7.0.1 / FortiAI v1.5.1 will have 'inline' blocking feature, where web/email traffic's session will 'hold' and wait for FAI's verdict
- Goal of this is to block "patient zero", utilizing FortiAI's sub-second verdict
- This is configured under FortiGate AV profile (CLI, not FSA field)
- FortiAI is "one of" the AV profile scanning options. E.g. AV engine and/or FortiAI verdict

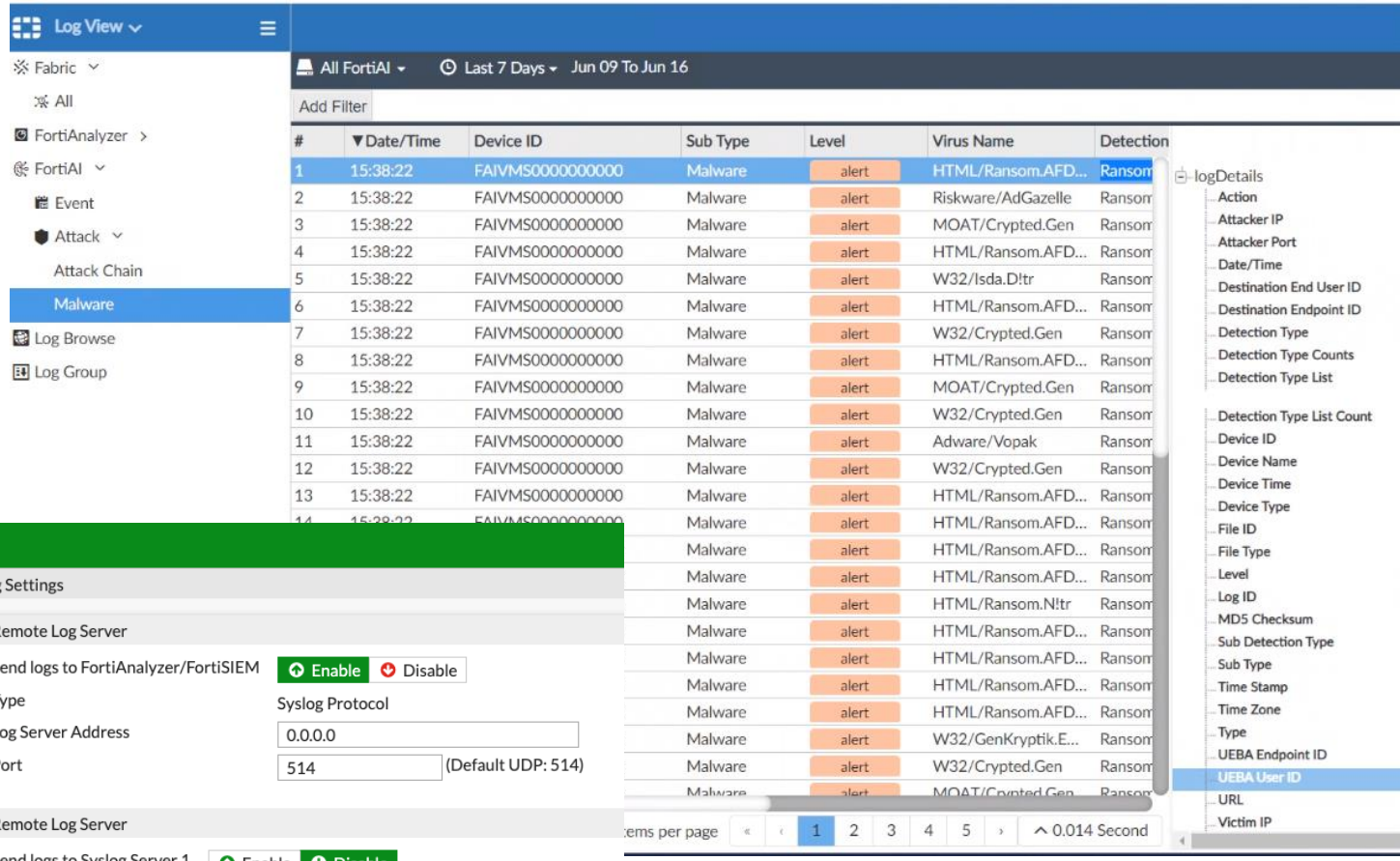


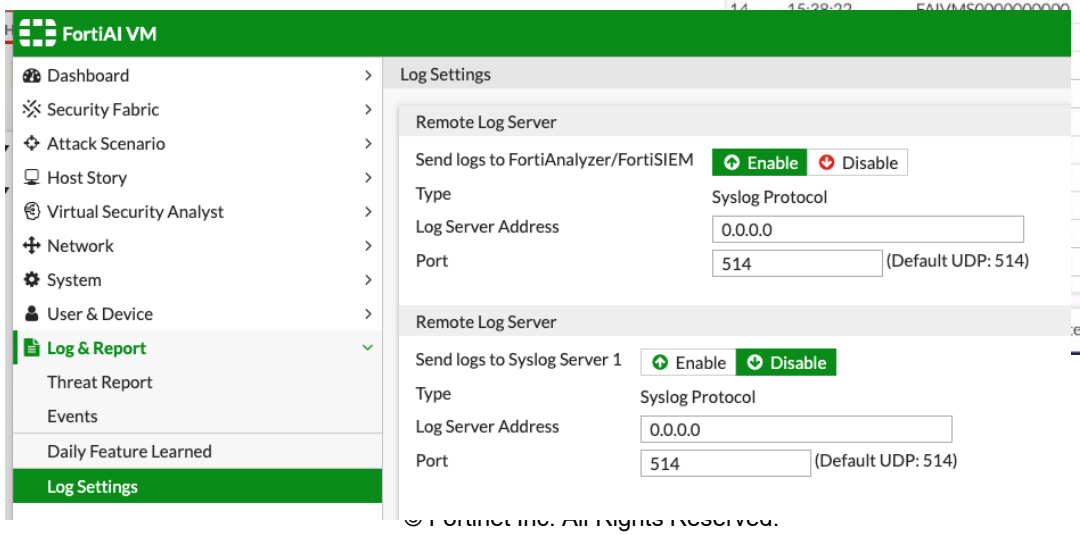
FortiAI - AI-driven **Security Operations**

FortiAnalyzer 7.0.1 Log View

V1.5.1

- FAZ 7.0.1 Support (Fabric ADOM) Log View
- Event Log (including performance, file summary statistics)
- Attack Log (including kill chain logs)
- Default dataset and reports in future release



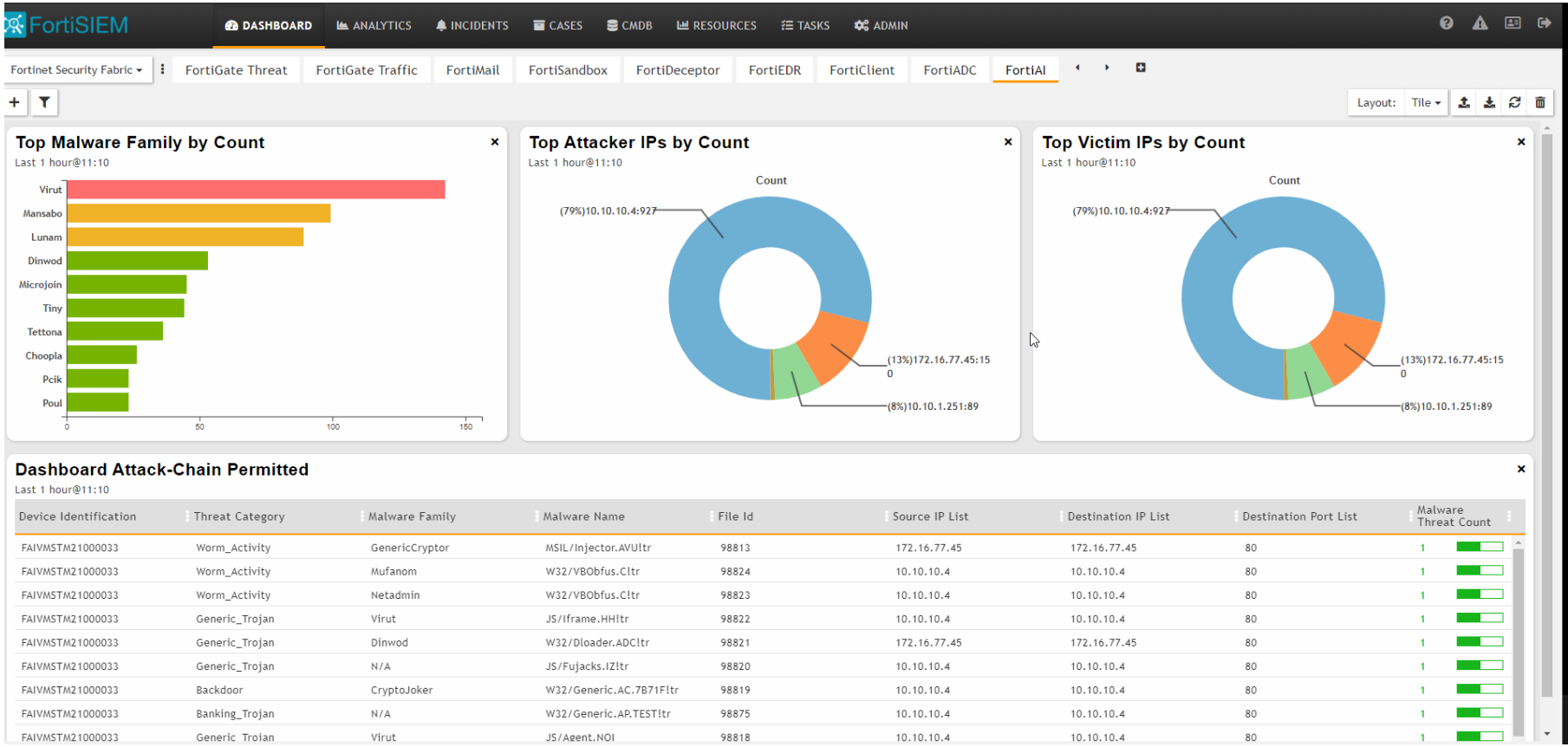


FortiAI - AI-driven Security Operations

V1.5.1

FortiSIEM Integration

- FortiSIEM v6.3 support
- Log Parsing
- FortiAI Dashboard
- New prefilter rule – attack killchain – block
- Shows victim IP/Malware family



FortiAI - AI-driven **Security Operations**

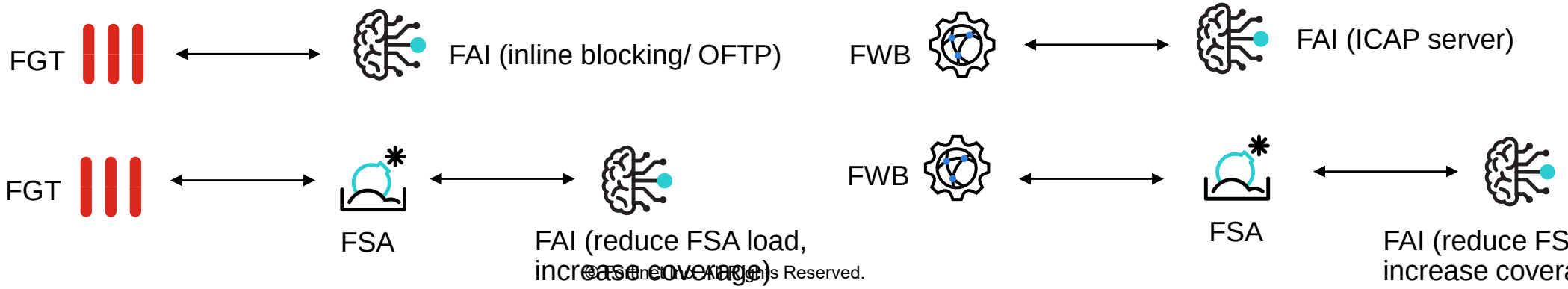
V1.5.1

FortiSandbox Integration (FSA v4.0.1)

- **Goal 1**: To reduce load for FSA dynamic scan (VM)
- **How**: FortiAI returns verdict of ‘absolute clean’ back to FSA, FSA “entrust FAI” and optionally skip dynamic (VM) scan

- **Goal 2**: Add coverage & context of malware
- How: Utilise both technology to increase coverage of malware detection. FortiAI provides features and malware type (e.g. Banking Trojan) back to FSA’s report

- **Goal 3**: Flexible integration options
- How: Allow existing FSA customers and new customers options for integration. E.g.



FortiAI - AI-driven **Security Operations**

V1.5.1

FortiSandbox Integration (FSA v4.0.1) - Configuration

1. Generate FAI user token (CLI or GUI)
2. Configure FSA <-> FAI pairing
3. Configure FSA Scan profile
4. View results in FAI logs / Device Input *

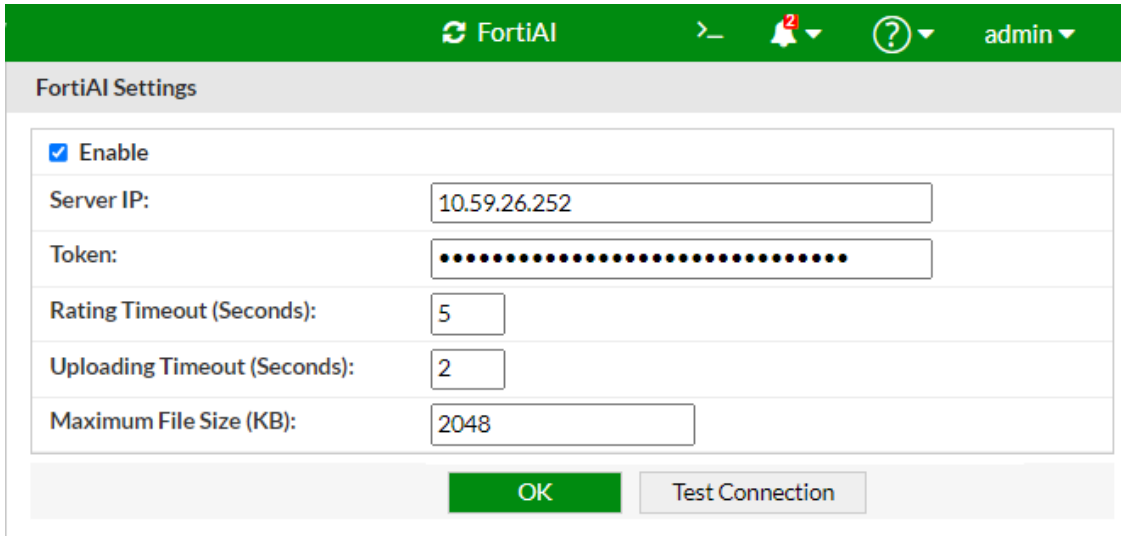
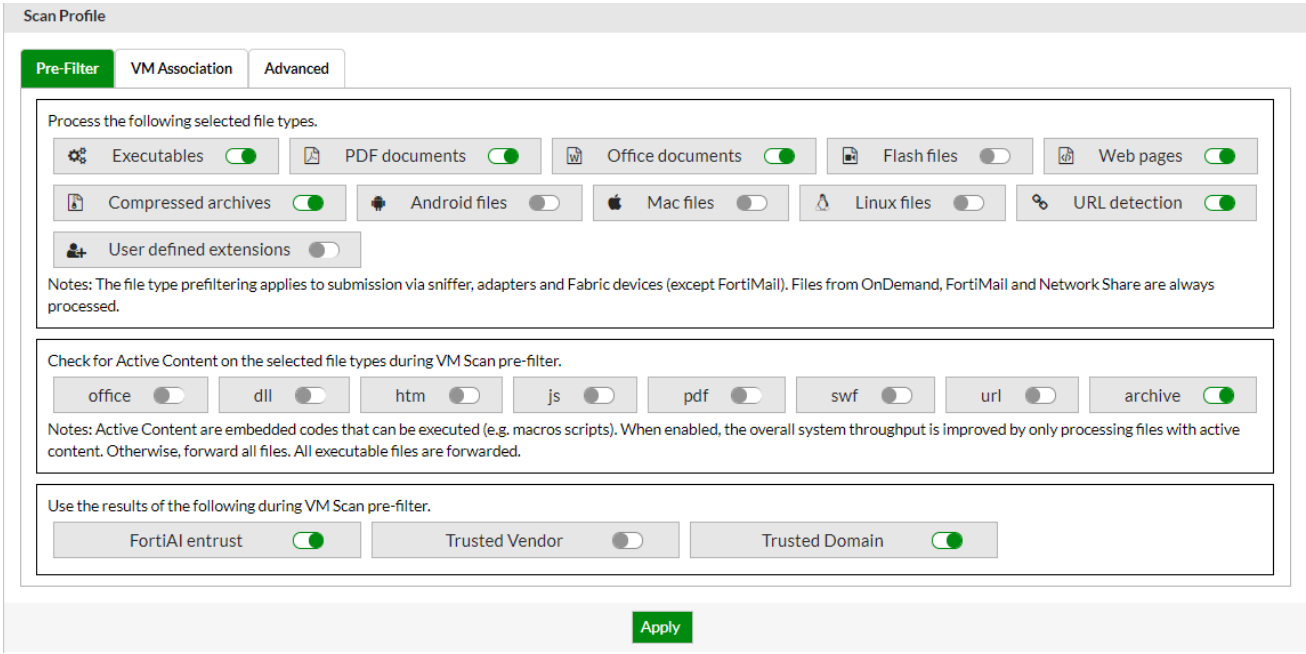


Figure – FSA FortiAI system settings

Figure – FSA Scan profile with “FortAI entrust”



* FSA device only appears after file is submitted


FORTINET