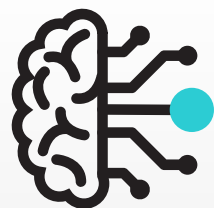


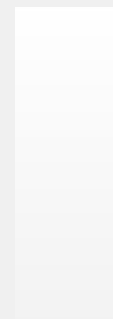
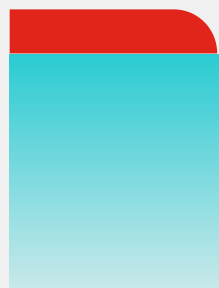
FORTINET®



FortiAI

сверхбыстрый анализ угроз при
поддержке искусственного
интеллекта

Вячеслав Гордеев
FSA, FAI, FML, FWB

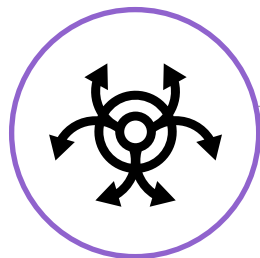


Agenda



01

Видение



02

Эволюция ВПО



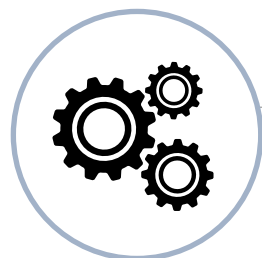
03

FortiAI введение



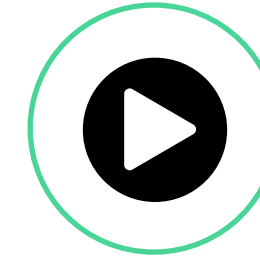
04

Virtual Security Analyst™
Возможности



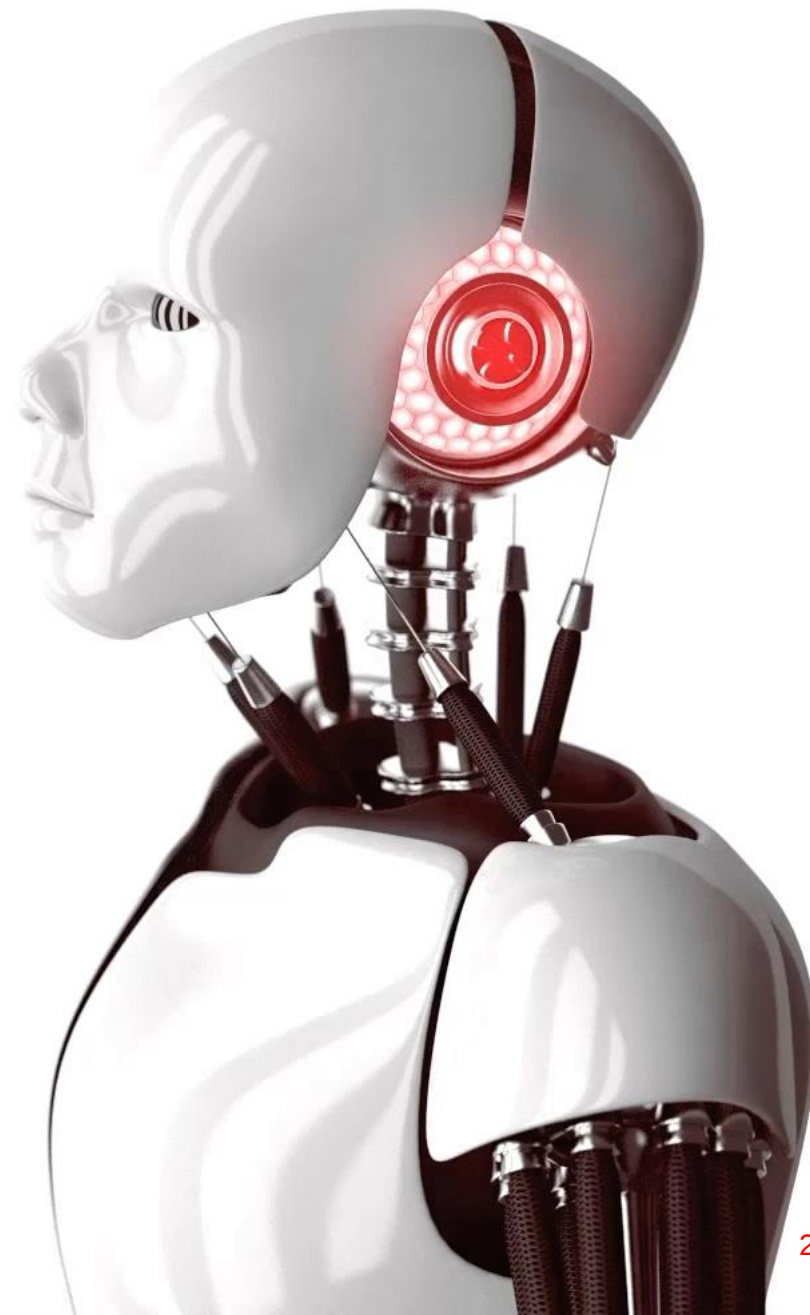
04

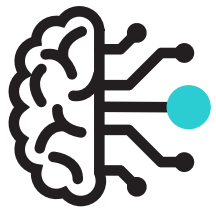
Как работает FAI?



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

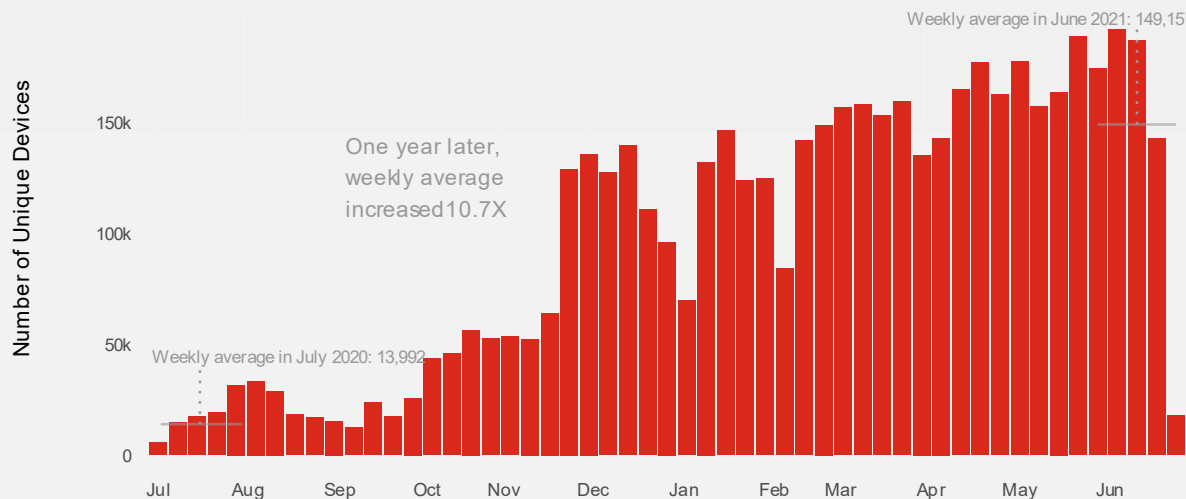


Уменьшение времени обнаружения

Время обнаружения меньше
одной секунды

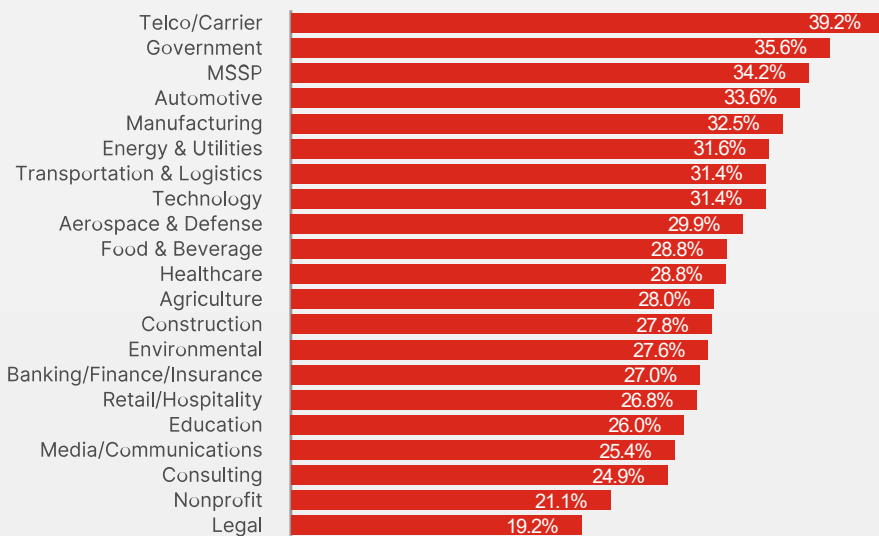
Вызов №1 – Вирусы-вымогатели (Ransomware)

Десятикратный рост активности за год (07.2020-07.2021)



>10x

Рост активности за год



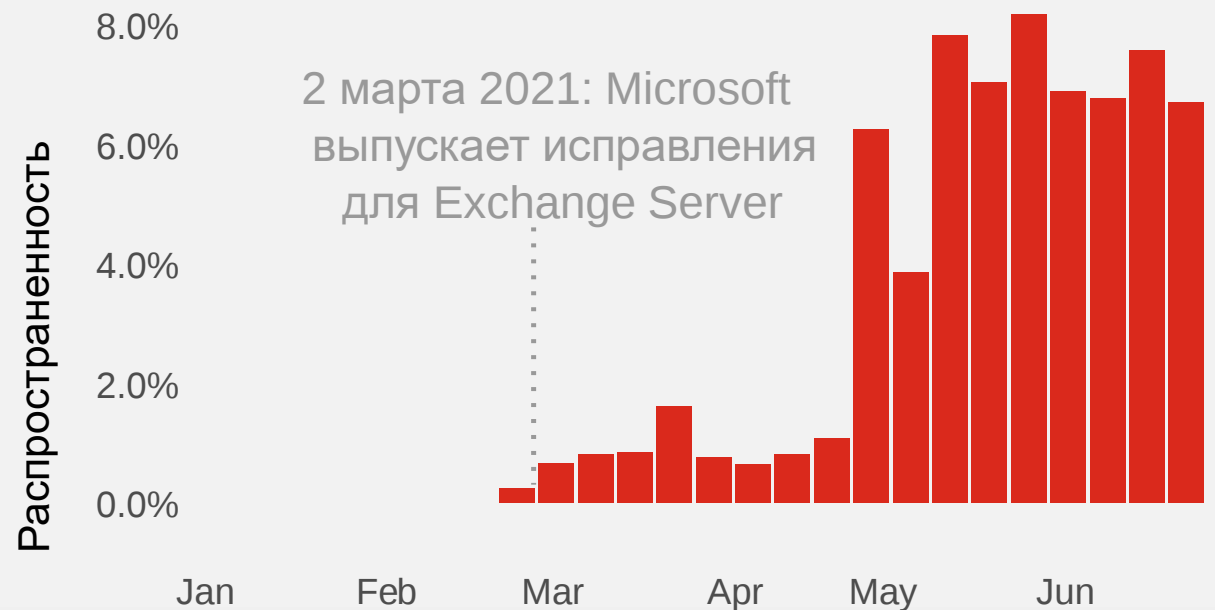
20-40%

Распространенность по секторам экономики

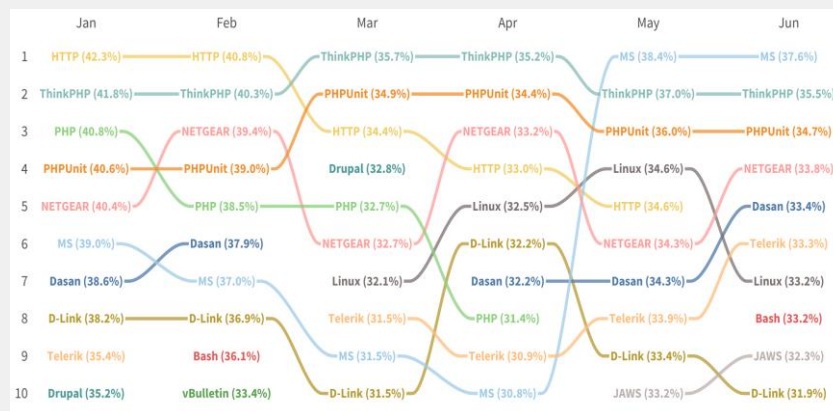


Вызов №2 – Новые уязвимости приложений

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

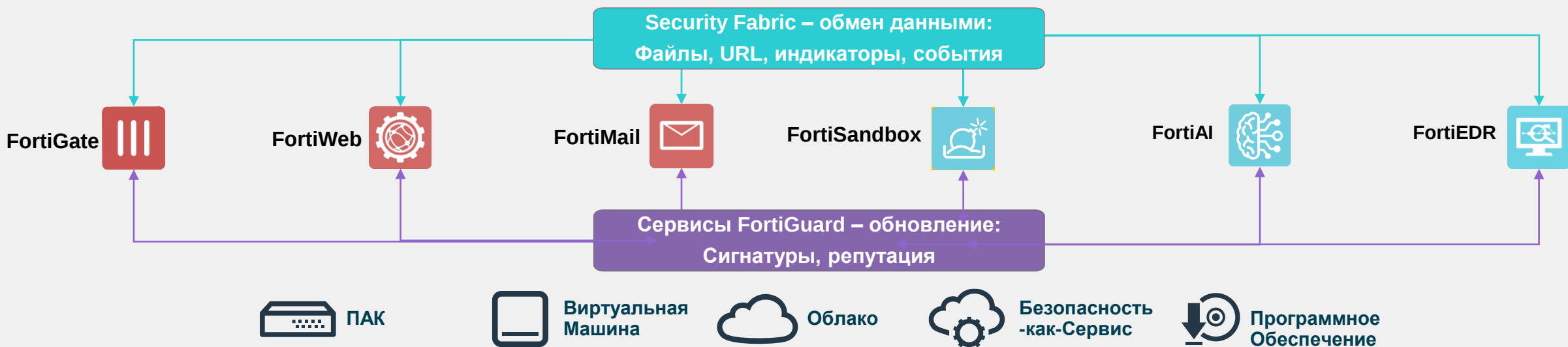


Защита от вирусов-вымогателей средствами Fortinet

Архитектура решения



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



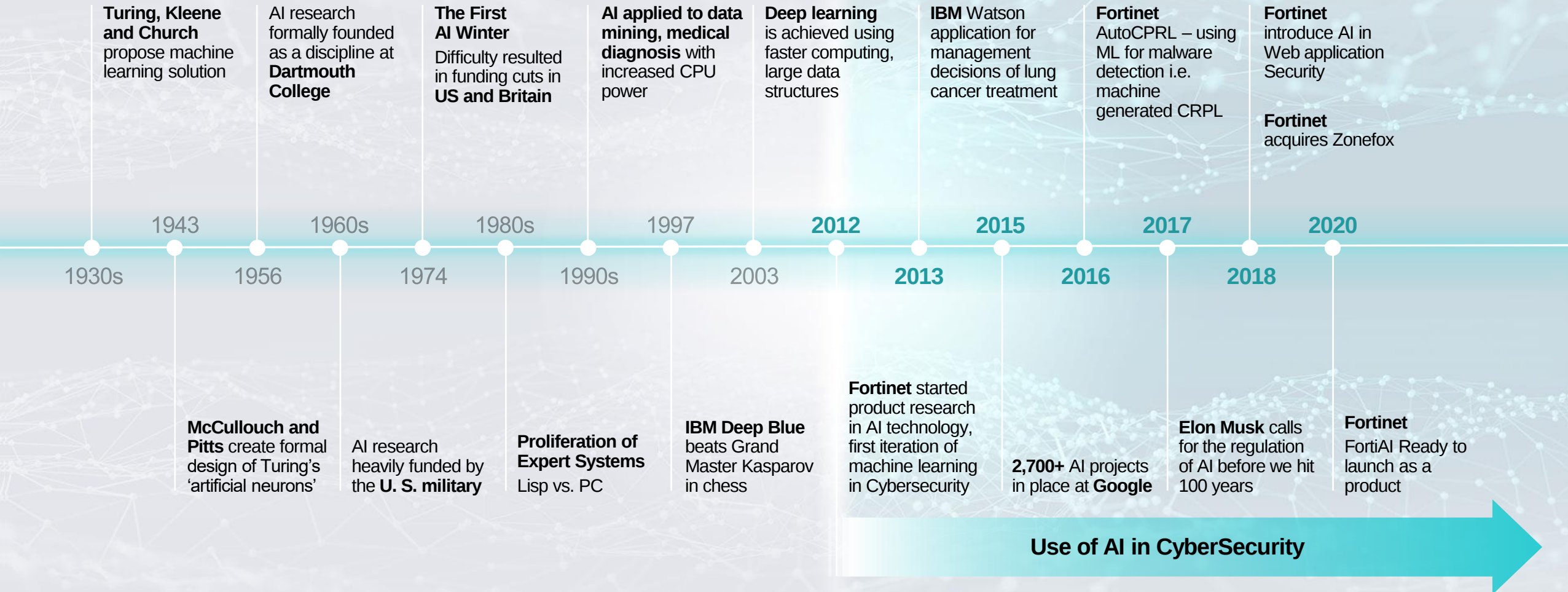


Обзор Эволюции Вредоносного ПО



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

1st
Gen

Signature Based

- Detection Delay
- Intense Compute
- Static Analysis

2nd
Gen

ATP Toolkit

- Malware evolves
- Time to detect – minutes
- Automated malware analysis

3rd
Gen

Artificial Intelligence

- Machine Learning
- Virtual Security Analyst TM
- Sub-second Verdict

Evolution



Malicious Code Detection

Advance Threat Protection (ATP) products at a glance



AV engine

Inspect core of apple...

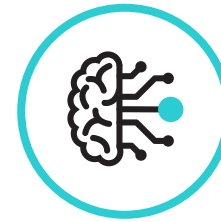
Um, it's bad.



FortiSandbox

Let me take a bite...

Um, it's bad.



FortiAI

Let me describe it -
rotten, smells...

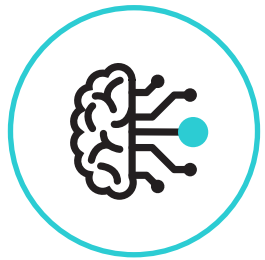
Um, it's bad.



FortiDeceptor

Let me place
more apples...

...with traps.



FortiAI

Введение

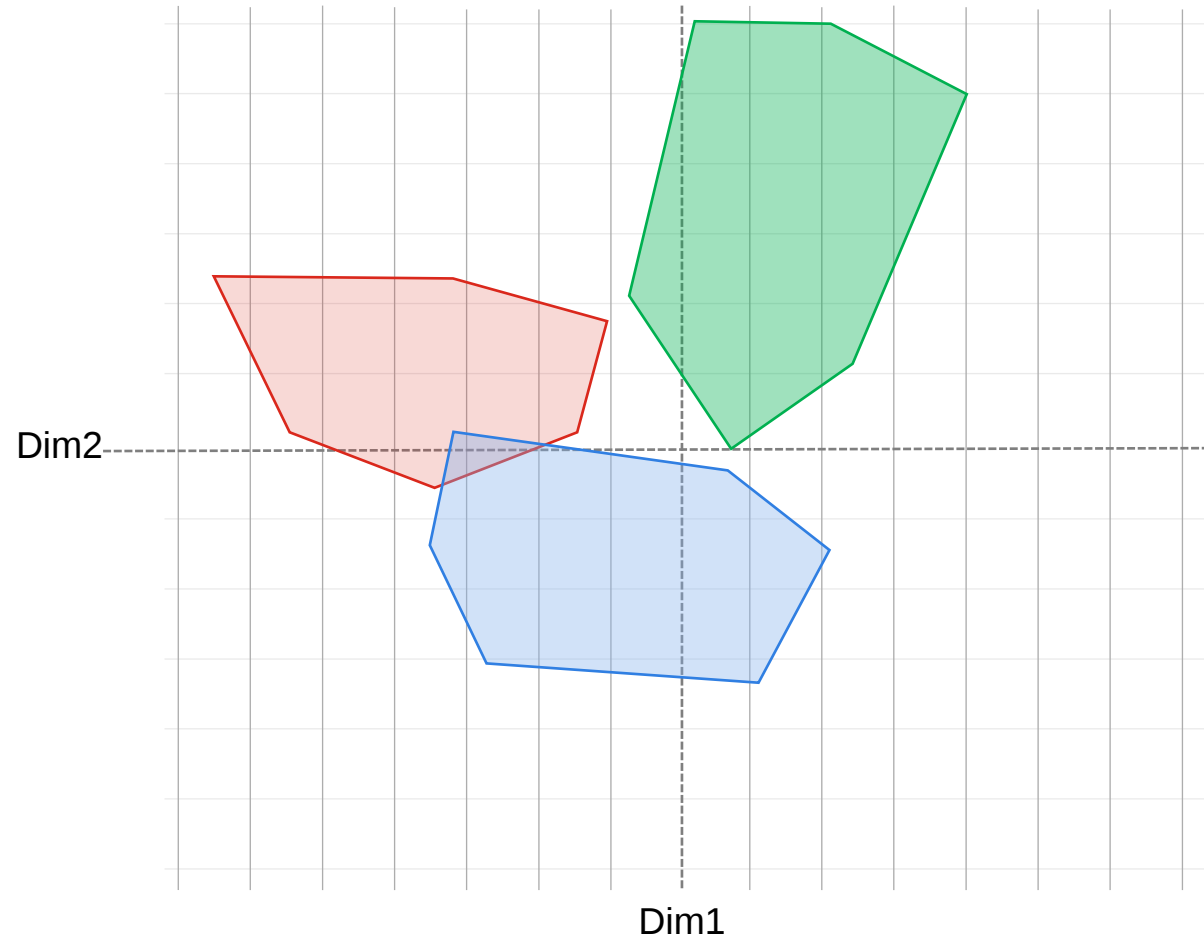


AI / Machine Learning: what do we expect?

- 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

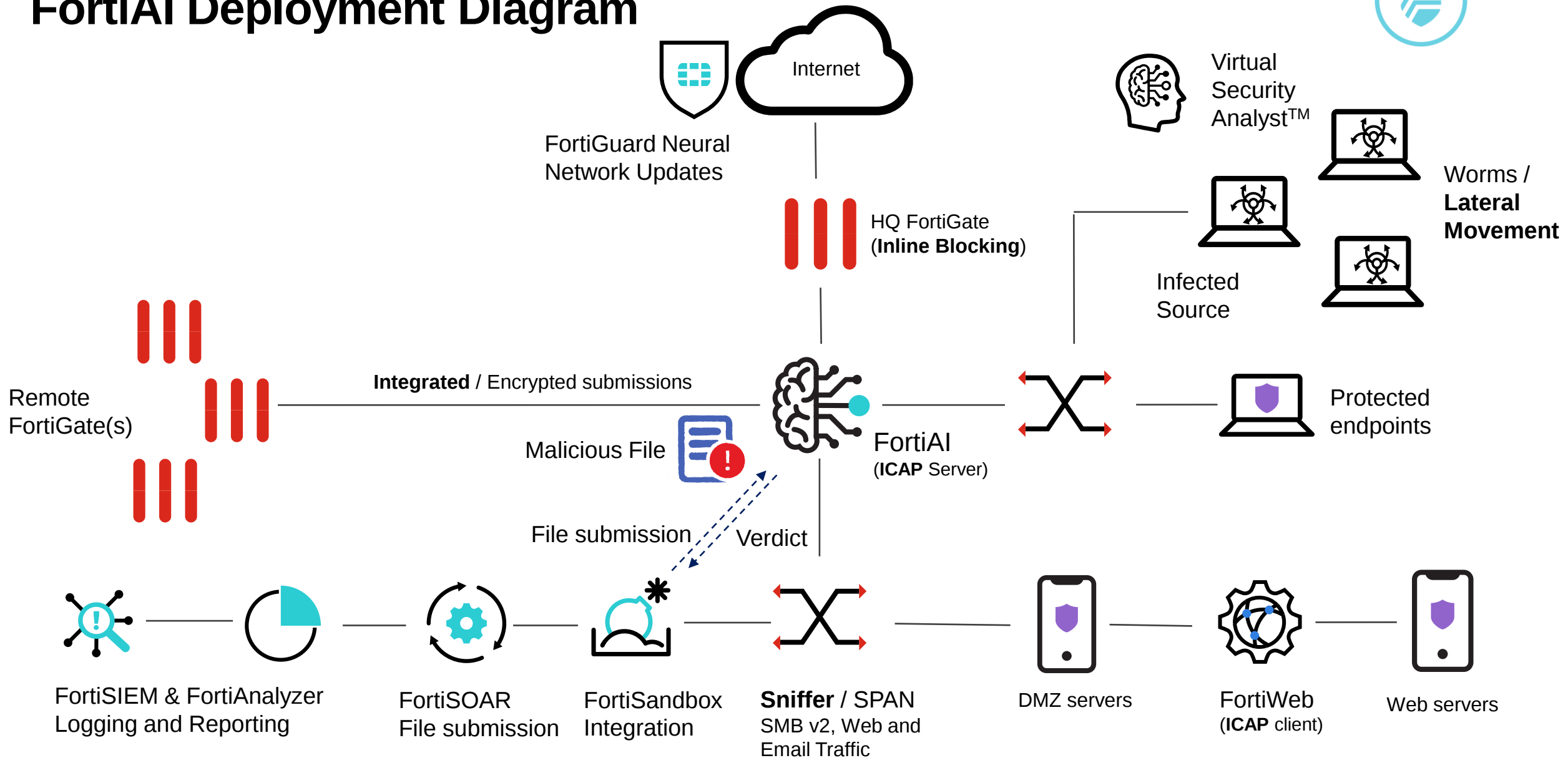
- Sub-second Verdict
- Threat Investigation
- Big Picture analysis
- Attack Scenarios



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™

Возможности



FortiAI Virtual Security Analyst™

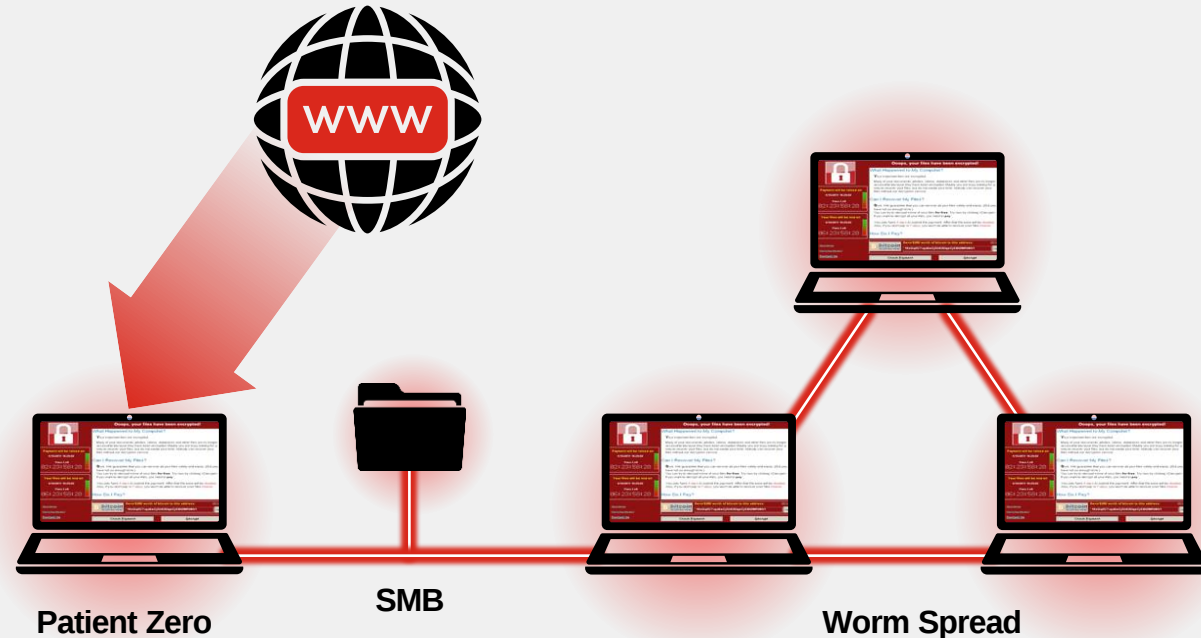
Tracing the source of attack

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



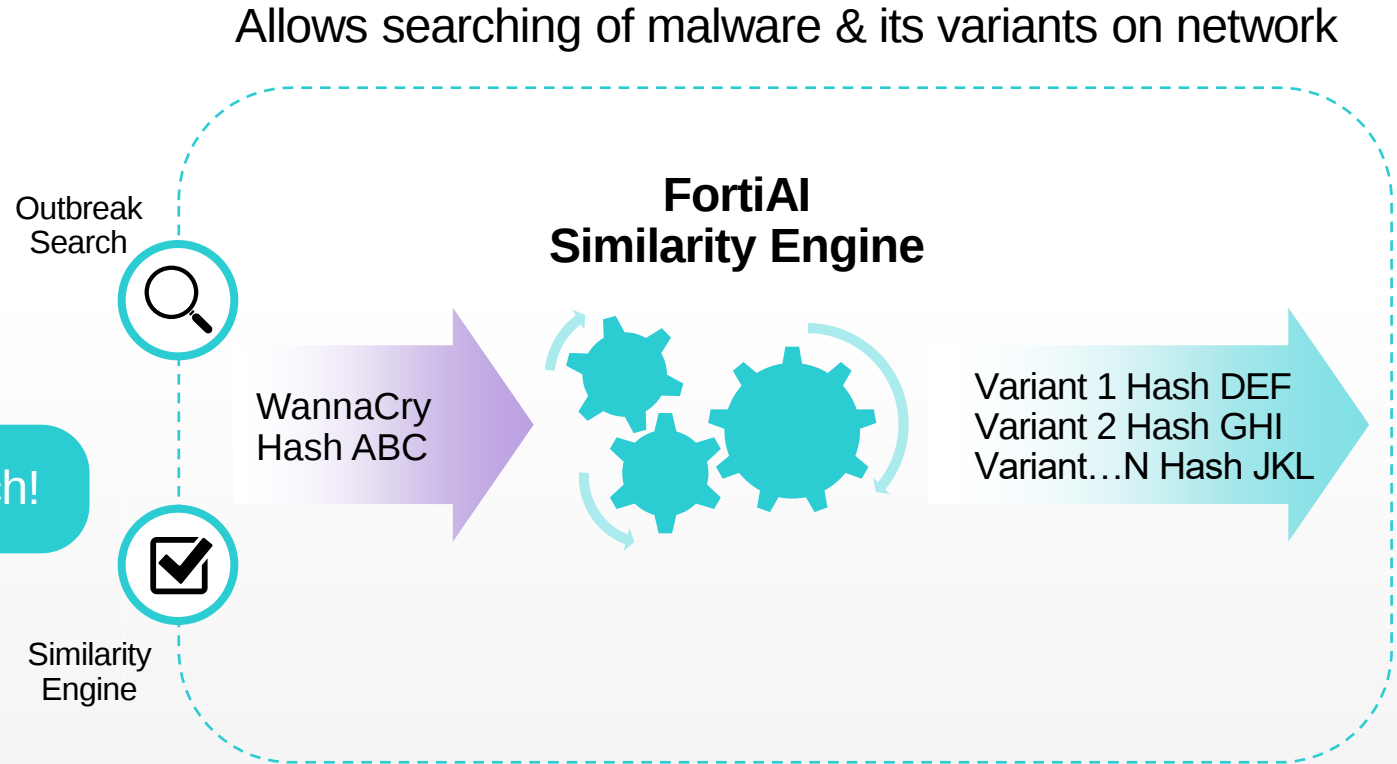
CIO

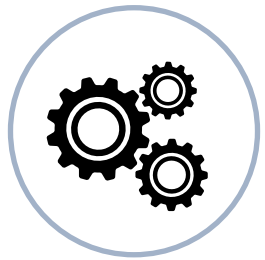
Q: Are we infected by this headline malware? e.g. WannaCry



FAI VSA™

A: Let me search!





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

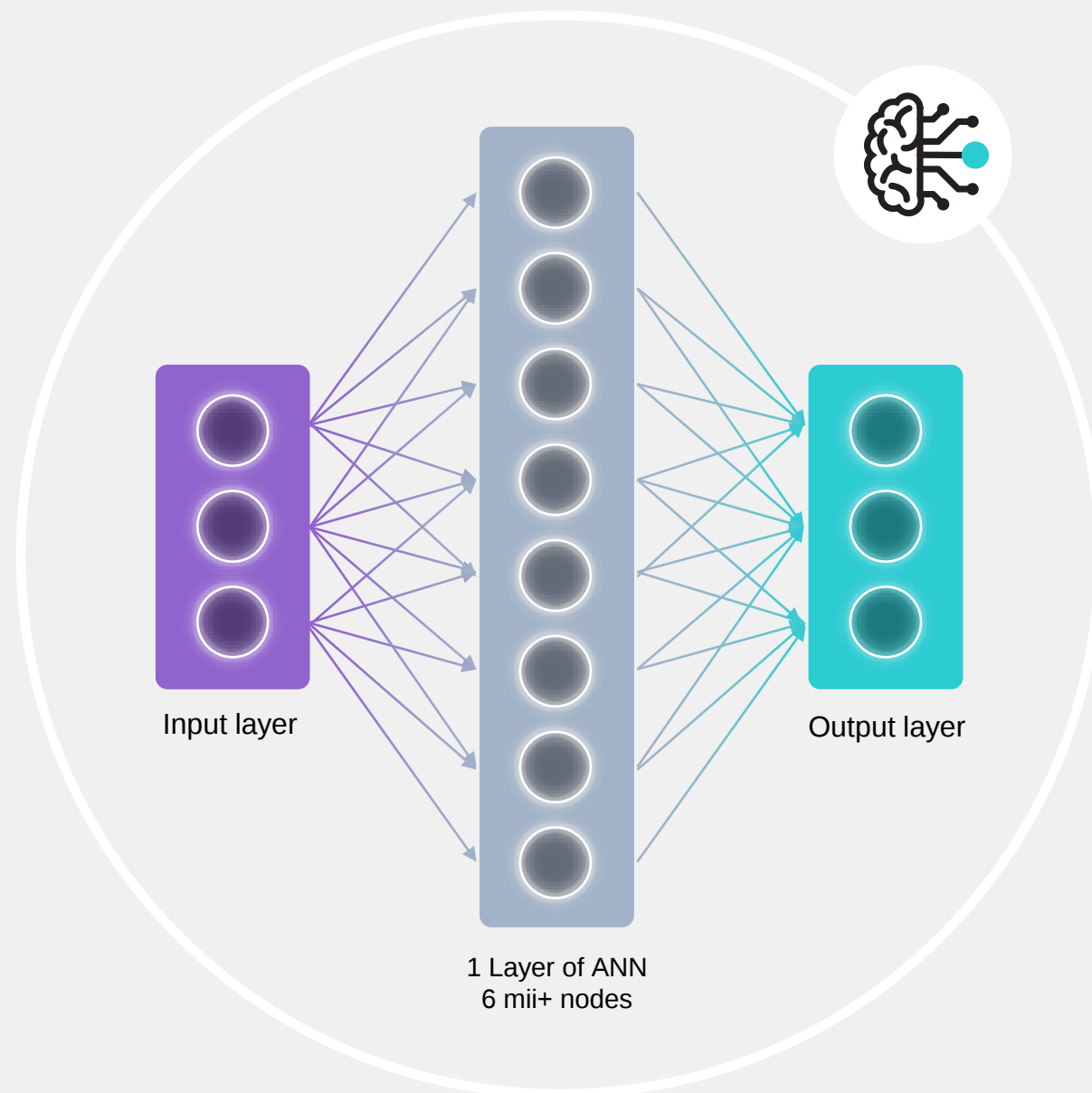
- Pre-trained with 20mil+ clean and malicious files
- Billions of clean and malicious features learnt

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.

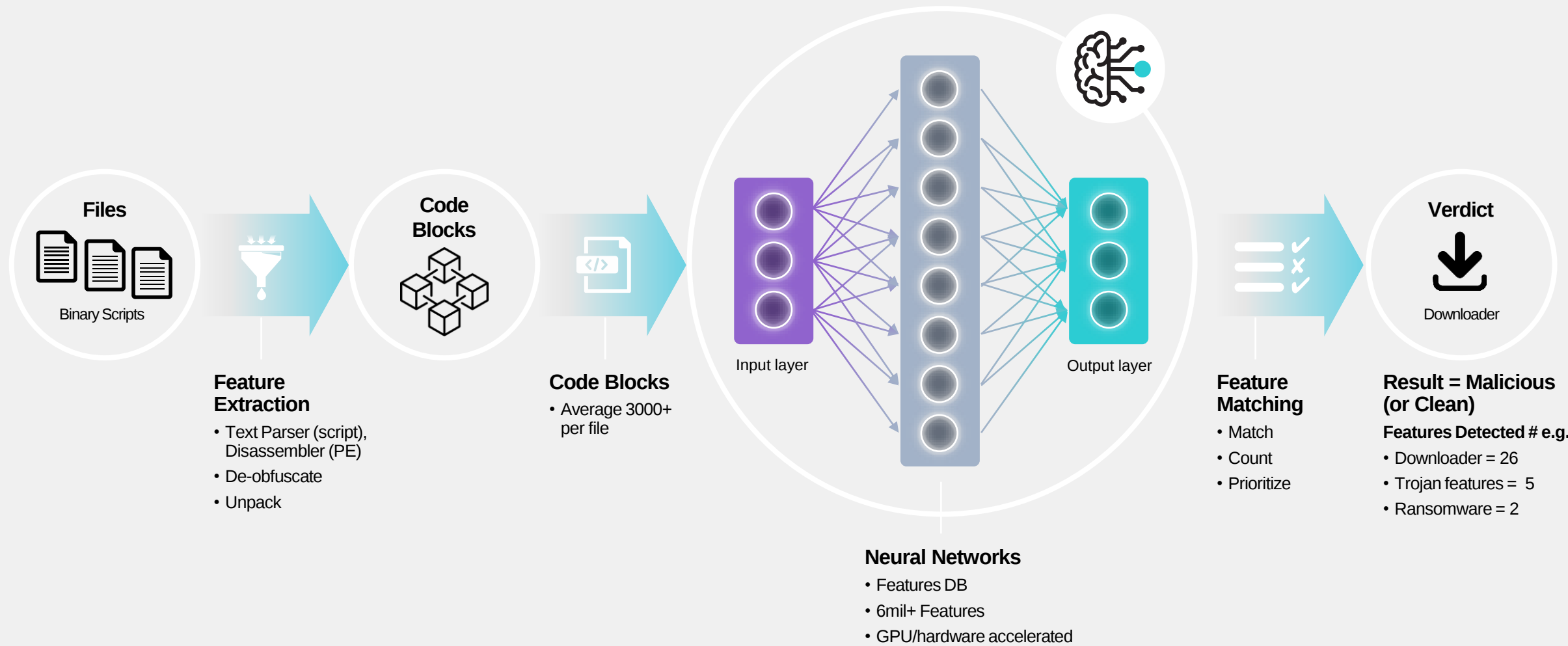
Does not require to ‘run’ the file (vs Sandboxing)

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



FortiAI

Malware Detection Workflow



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 Comparison*





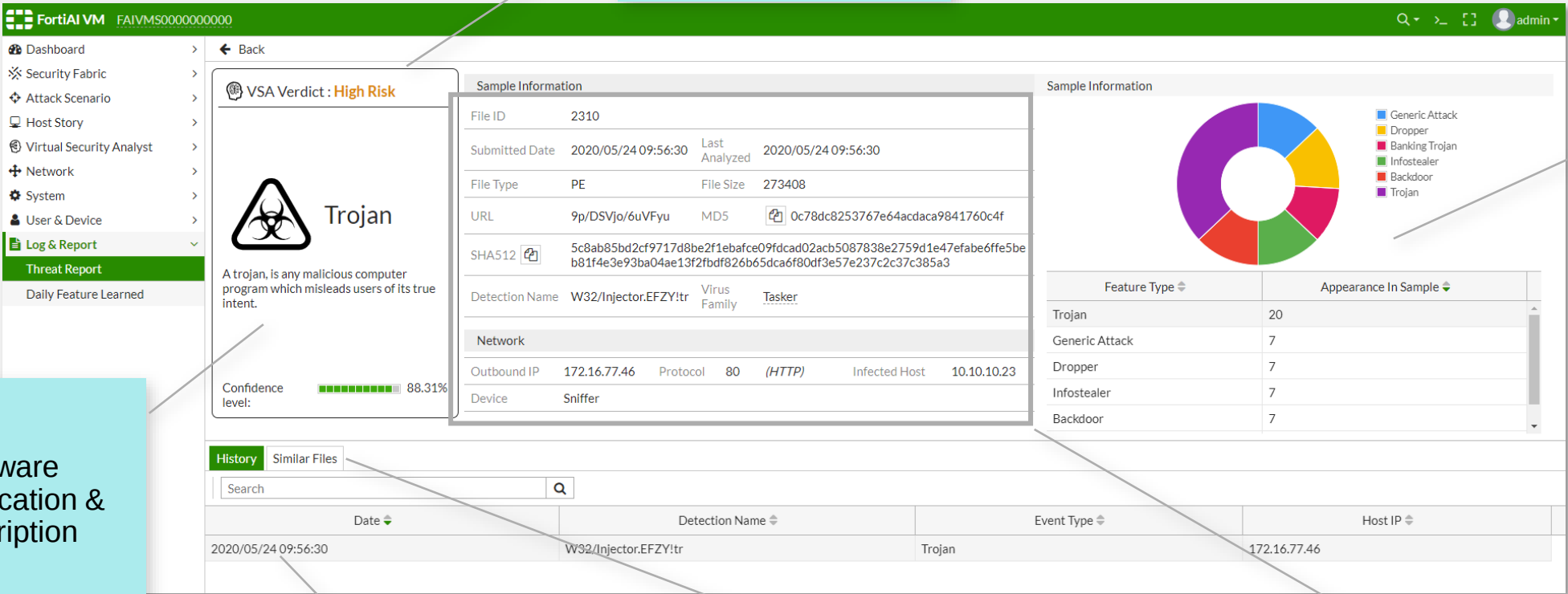
FortiAI demo

<https://fortiai.fortidemo.com>

demo / demo



Virtual Security Analyst™ Report



Verdict & Confidence Level

Feature Breakdown

Malware Classification & Description

Appearance on Network (History)

Similarity Engine Search

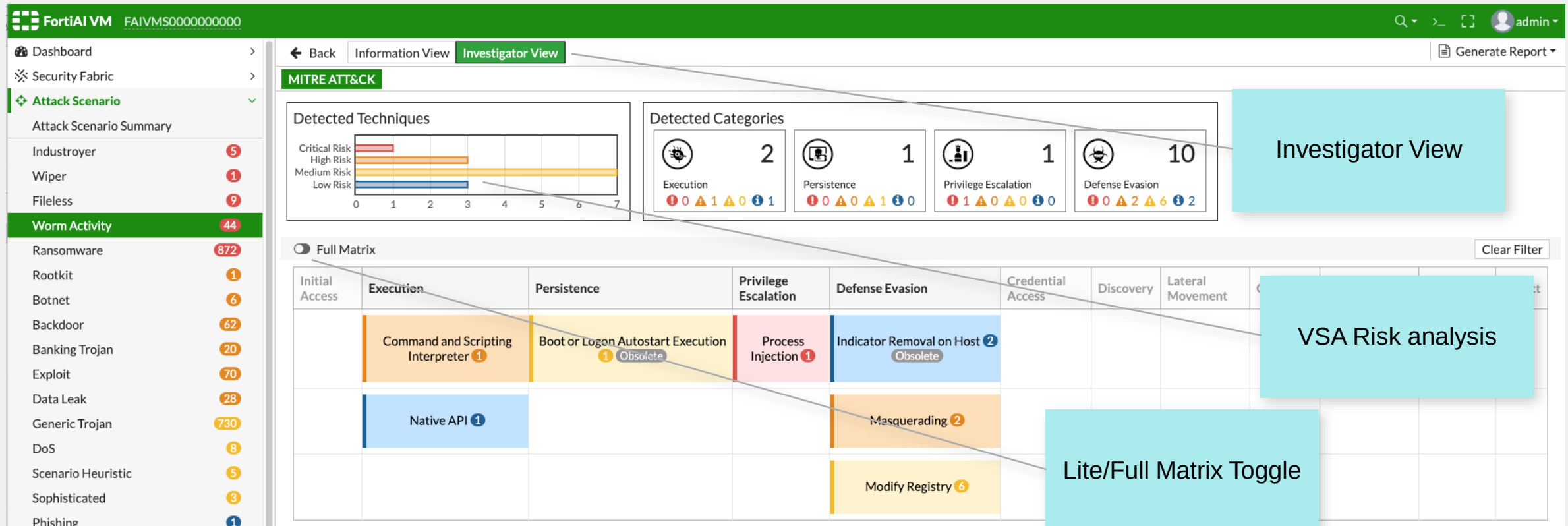
Hash / Type / Time / Virus Family / Source



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 VM FAIVMS0000000000

admin

Dashboard > Security Fabric > **Attack Scenario** > Attack Scenario Summary

	Discovery Date	Victim (Infected Host) IP	Device Type	VDOM	Malware Family
Industroyer	2020/10/20 14:06:00	172.16.77.46	Sniffer	N/A	Agent
Wiper	2020/10/20 15:06:00	172.19.235.230	Sniffer	N/A	Generic
Fileless	2020/11/09 13:49:29	10.10.10.55	Sniffer	N/A	Daws
	2020/11/09 13:49:37	10.10.10.53	Sniffer	N/A	Dreambot
	2020/11/09 13:49:49	10.10.10.54	Sniffer	N/A	Mufanom
Worm Activity	2020/11/09 13:50:56	10.10.10.52	Sniffer	N/A	GenericCryptor
Ransomware	2020/11/09 13:51:19	10.10.10.53	Sniffer	N/A	Netadmin
Rootkit	2020/11/09 13:51:22	10.10.10.53	Sniffer	N/A	Mufanom
Botnet	2020/11/09 13:53:38	10.10.10.51	Sniffer	N/A	Generic

Attack Timeline at Host 172.16.77.46

Worm

Worm Activity

W32/Crypted.Gen

0 days 0 hours 0 minutes 0 seconds

PE Worm Generic

Attacker IP: 172.16.77.46

Victim IP: 172.19.235.230

Activity Log

0 days 1 hours 5 minutes 0 seconds

2020/10/20 14:11:00

Attacker IP: 172.19.235.230

Victim IP: 172.16.77.46

0 days 2 hours 0 minutes 0 seconds

2020/10/20 15:06:00

Attacker IP: 172.19.235.230

Victim IP: 172.16.76.228

0 days 2 hours 0 minutes 0 seconds

2020/10/20 15:06:00

Attacker IP: 172.19.235.230

Victim IP: 172.16.77.45

New Logos for each attack type

Clear Attack and Victim IP

Worm Spreading Scenario



FortiAI - AI-driven Security Operations

STIX v2 and JSON support

3rd Party Threat Intelligence platform integration

- STIX v2 Output
- JSON Output

FortiAI VM FAIVM500000000000

Dashboard > Security Fabric > **Attack Scenario** > Attack Scenario Summary

Industroyer 1, Wiper 1, Fileless 2, **Worm Activity 5**, Ransomware 10, Rootkit 1, Botnet 1, Backdoor 5, Banking Trojan 5, Exploit 1, Data Leak 4, Generic Trojan 48

VSA Verdict: Critical Risk

Worm

A worm has the capability to spread itself to other systems over a network.

Confidence level: 100.00%

Sample Information			
File ID	11114		
Submitted Date	2020/10/20 13:06:00	Last Analyzed	2020/10/20 13:06:00
File Type	PE	File Size	521728(509.5 KB)
URL	http://172.16.77.46/api/sample_download/1195500815/ MD5 565962cc6ca6b5c		
SHA512	e8ece2ca1c7c58723eccdf02cfa08645c687e24fcc48d516b729c910bdcca731a07b b8a58bd14268faf021339cc3b82b233384e69d81a2f5f8bc9f93e46feaa4		
Detection Name	W32/Delf.BCZ!tr	Virus Family	Runouce
Source Device			
Device Type	Sniffer		
Network			
Attacker	172.16.77.46:80 (HTTP)	Victim	172.19.235.230:52970 (Private port)

Feature Composition	
Feature Type	Appearance In Sample
Worm	199
Banking Trojan	134
Dropper	125
Ransomware	125
Application	125

Generate Report

- PDF
- JSON
- STIX2**

STIXv2 / JSON Output

AI-driven Security Operations

FortiAI Outbreak Search

V1.3

Search by Exact Hash or Similar files (variants)

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

VSA™ Manual

FortiAI VM FAIVMS0000000173

Search Lead Type: Hash 802c1e5ff3645d2790977dc6fcdd49af

Similarity-Based Hash-Based Detection-Based

Generate Report Search Found 26 related file(s)

Date	MD5	File Type	Detection Type	Virus Family	Detection Name	Risk Level	Confidence Level
2020/11/25 13:15:36	802c1e5ff3645d2790977dc6fcdd49af	HTML	Ransomware	Virut	Q MOAT/Crypted.Gen	Critical	High (98.6%)
2020/11/24 16:38:36	802c1e5ff3645d2790977dc6fcdd49af	HTML	Ransomware	Virut	Q MOAT/Crypted.Gen	Critical	High (98.6%)
2020/11/24 09:07:21	802c1e5ff3645d2790977dc6fcdd49af	HTML	Ransomware	Virut	Q MOAT/Crypted.Gen	Critical	High (98.6%)
2020/11/20 22:53:52	802c1e5ff3645d2790977dc6fcdd49af	HTML	Ransomware	Virut	Q MOAT/Crypted.Gen	Critical	High (98.6%)
2020/11/20 11:51:47	802c1e5ff3645d2790977dc6fcdd49af	HTML	Ransomware	Virut	Q MOAT/Crypted.Gen	Critical	High (98.6%)
2020/11/18 11:07:08	802c1e5ff3645d2790977dc6fcdd49af	HTML	Ransomware	Virut	Q MOAT/Crypted.Gen	Critical	High (98.6%)
14:00:01	802c1e5ff3645d2790977dc6fcdd49af	HTML	Ransomware	Virut	Q MOAT/Crypted.Gen	Critical	High (98.6%)
17:26:01	802c1e5ff3645d2790977dc6fcdd49af	HTML	Ransomware	Virut	Q MOAT/Crypted.Gen	Critical	High (98.6%)

FortiAI VM

FAIVMS0000000173

Dashboard

Security Fabric

Attack Scenario

Host Story

Virtual Security Analyst

Network

System

User & Device

Log & Report

Threat Report

Daily Feature Learned

Back

Information View

Investigator View

VSA Verdict : Critical Risk

Ransomware

A type of malicious software designed to block access to a computer system until a sum of money is paid.

Confidence level: 98.63%

Sample Information

File ID370258

Submitted Date2020/11/25 13:15:36Last Analyzed2020/11/25 13:15:36

File TypeHTMLFile Size35141(34.3 KB)

URLcriP6/Xl4rG/fHrdEvMD5802c1e5ff3645d2790977dc6fcdd49af

SHA5120c6b8a1660fb2da6e49241e26022d8d7ead92d8b7a17584c0823096f067e5cc7b9bd5cf5a0319f18179d615b5685802a6e1b0b41cfd2e1b2836b510b038b3764

Detection NameMOAT/Crypted.GenVirus FamilyVirut

Source Device

Device TypeSniffer

Network

Attacker172.19.235.8 :80 (HTTP)Victim172.19.122.94

Feature Composition

Generic Attack

Ransomware

Phishing

Redirector

Downloader

Worm

Clicker

CoinMiner

Feature Type

Appearance In Sample

Generic Attack64

Ransomware64

Phishing59

Redirector3

Downloader1

History

Similar Files

IOC Information

View all history

Search

Date

MD5

File Type

Detection Name

Device

VDOM

Attacker

Victim

Confidence Level

Risk Level

2020/11/25 13:15:36

802c1e5ff3645d2790977dc6fcdd49af

HTML

Q MOAT/Crypted.Gen

Sniffer

N/A

172.19.235.8

172.19.122.94

High (98.6%)

Critical

2020/11/24 16:38:36

802c1e5ff3645d2790977dc6fcdd49af

HTML

Q MOAT/Crypted.Gen

Sniffer

N/A

172.19.235.3

172.19.122.83

High (98.6%)

Critical

2020/11/24 09:07:21

802c1e5ff3645d2790977dc6fcdd49af

HTML

Q MOAT/Crypted.Gen

Sniffer

N/A

172.19.235.3

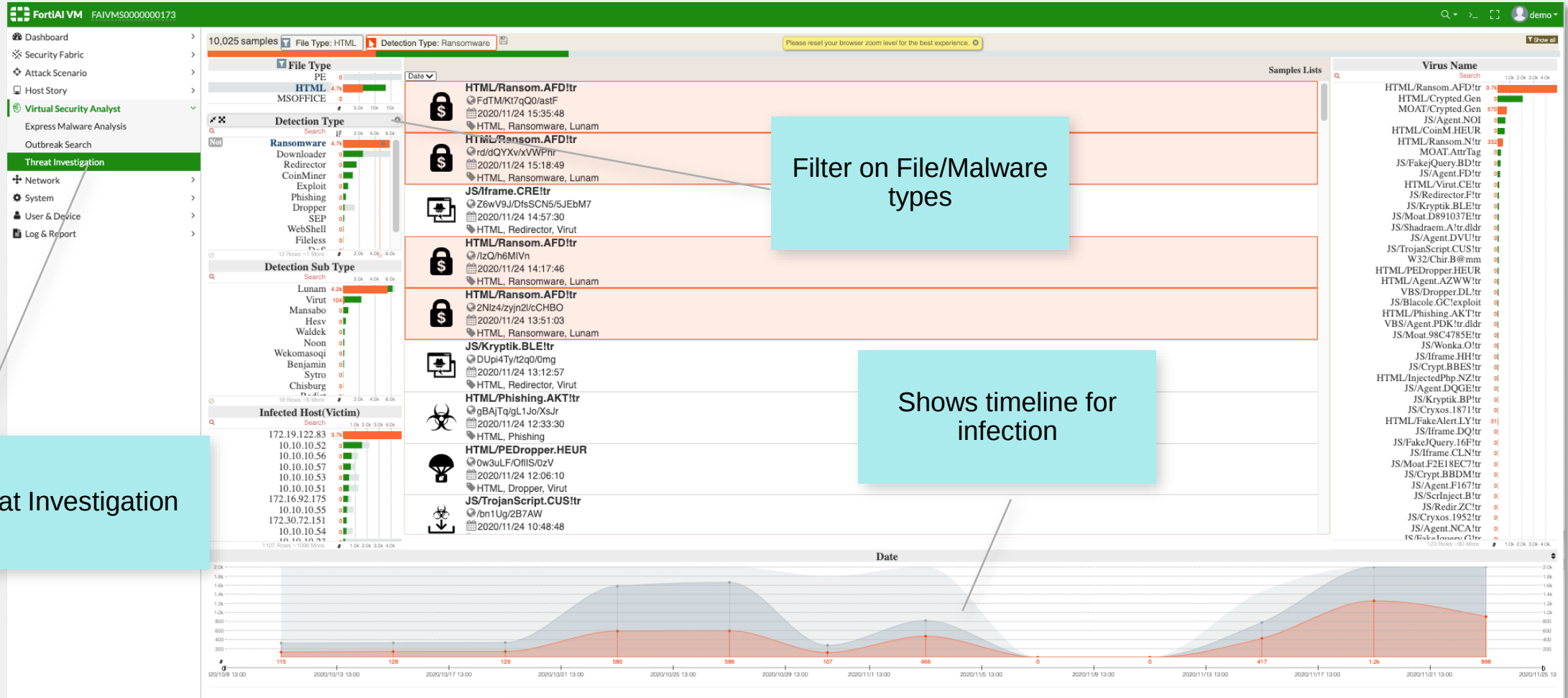
172.19.122.83

High (98.6%)

Critical

History of Malware on network

Threat Investigation – “Big Picture” analysis



AI-driven Security Operations

Security Fabric Integration – FortiGate Quarantine

V1.3

FortiAI Security Fabric Configuration:

Automation Framework

Automation Profile Name: FGT01_BANIP_ROOT

Automation Profile Type: Ban IP

Trigger Source: ip_blocker

Trigger Source: ip_unblocker

API Key: [Redacted]

Device IP: 172.16.1.250

VDOM: root

Port: 443

Trigger Source: **Fabric Device** Sniffer

Enable: ☒ On

Source of Fabric Device or Sniffer

Specify which FortiGate VDOM to target

FortiGate Configuration

New Automation Stitch

Name: ip_blocker

Status: ☒ Enabled ☐ Disabled

Trigger

Incoming Webhook

Action

CLI Script ☒ Email ☐ FortiExplorer Notification ☐ Access Layer Quarantine ☐ Quarantine FortiClient

Minimum interval (seconds): 0

CLI Script

1st Action Name: [Redacted]

Script: config vdom
edit root
diagnose user quarantine
add src4 %%log.srcip%%
%%log.expiry%% admin

93/1023

Upload

>_ Record in CLI console



AI-driven Security Operations

Express Malware Analysis – Manual & API Upload

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

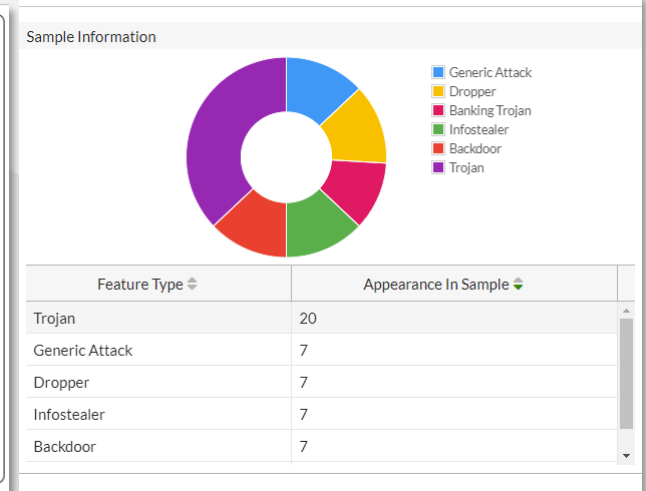
FortiAI 3500F FAI35FT319000030								
Dashboard	Back to 525910.tar.gz (2020/05/27 12:18:04)							
Security Fabric	117 items Locate Search							
Attack Scenario								
Host Story								
Virtual Security Analyst	Supported File Type 117							
Express Malware Analysis	2020/05/27 12:18:06	3CF7AB9B.vsc	6df9fb974921b6450a0dc2a052f32279	PE	Application	89%	Low Risk	Done
Outbreak Search	2020/05/27 12:18:06	3CFAB70C.vsc	4a276411d8e0d165ea1208310816eca7	PE	Backdoor	100%	High Risk	Done
Threat Investigation	2020/05/27 12:18:06	3694441D.vsc	1a289c64e2fde55db27b0780deadd1e3	PE	Clean	N/A	No Risk	Done
Network	2020/05/27 12:18:06	43C8DA8C.vRG	5530387f6e61fb480102326eb1a0a45b	PE	Trojan	80%	High Risk	Done
System	2020/05/27 12:18:06	3CF7AA32.vsc	8b0454bd8cb01b242809aa5b6b54c6a4	PE	Trojan	100%	High Risk	Done
User & Device	2020/05/27 12:18:06	3751017B.vsc	dc3110aec10e81db016e2bf996a2e37d	PE	Clean	N/A	No Risk	Done
Log & Report	2020/05/27 12:18:06	3CF64783.vsc	9d8e9fd836b7f222601825ee4ba583c2	PE	Backdoor	100%	High Risk	Done
	2020/05/27 12:18:06	385179CF.vsc	40730e1a986a4d219c11256f03b5ee40	PE	Trojan	80%	High Risk	Done
	2020/05/27 12:18:06	3112E96C.vsc	90ab2aa6df21faab44a517458ca5ff3c	PE	Trojan	79%	High Risk	Done
	2020/05/27 12:18:06	3D00B58E.vsc	87765efe07f6c41d3f6c4fb29dc3cc0c	PE	Application	83%	Low Risk	Done
	2020/05/27 12:18:06	36C73883.vsc	cc7fd98e6eab2780794a38fe79a00d59	PE	Clean	N/A	No Risk	Done
	2020/05/27 12:18:06	36944F2B.vsc	c04555ec033e396afb3baafe997e257c	PE	Clean	N/A	No Risk	Done
	2020/05/27 12:18:06	3738FE3A.vsc	2b7b2fec49d1b8365bfc150ddaeb8516	PE	Clean	N/A	No Risk	Done
	2020/05/27 12:18:06	326DC489.vsc	7472e9ea7491f3a5df9b61aa1bc41e00	PE	Ransomware	79%	Critical Risk	Done

VSA Verdict : **High Risk**

 Trojan

A trojan, is any malicious computer program which misleads users of its true intent.

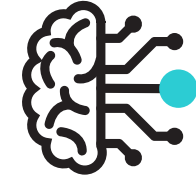
Confidence level: 88.31%





FortiAI - What's New v1.5.1

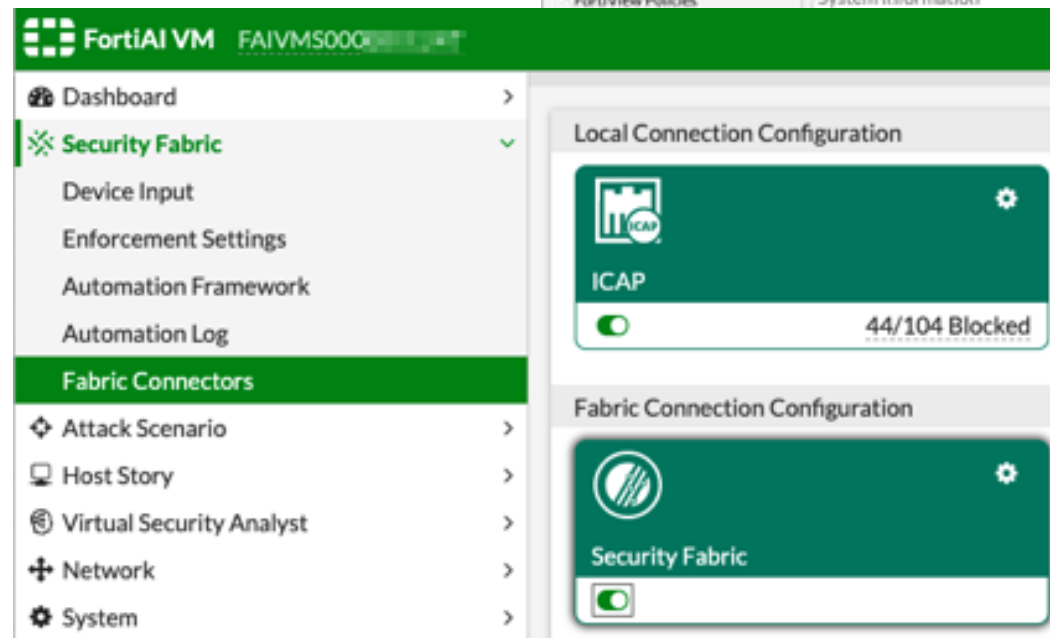
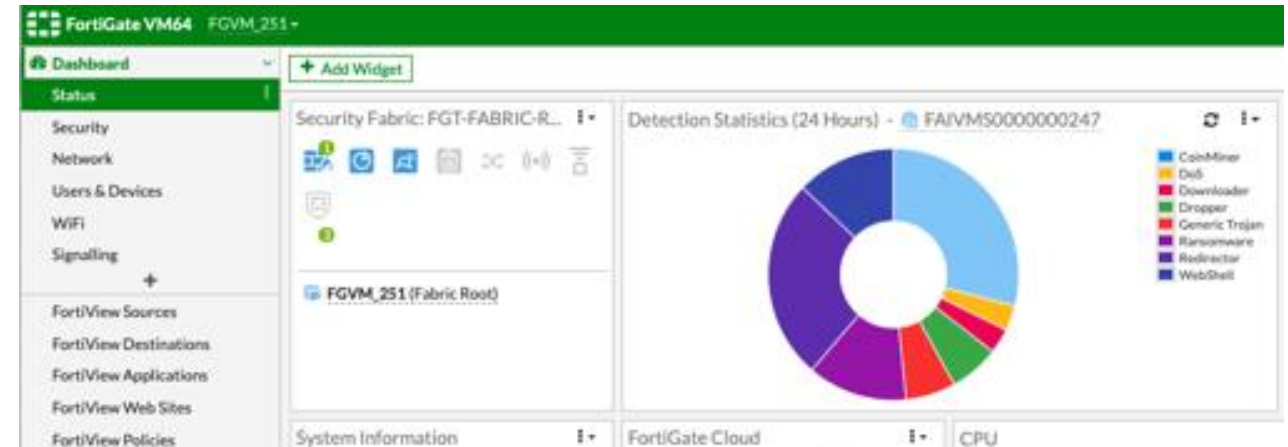
FortAI - AI-driven Security Operations



V1.5

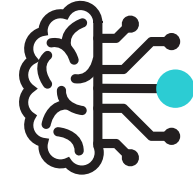
Security Fabric Pairing

- 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

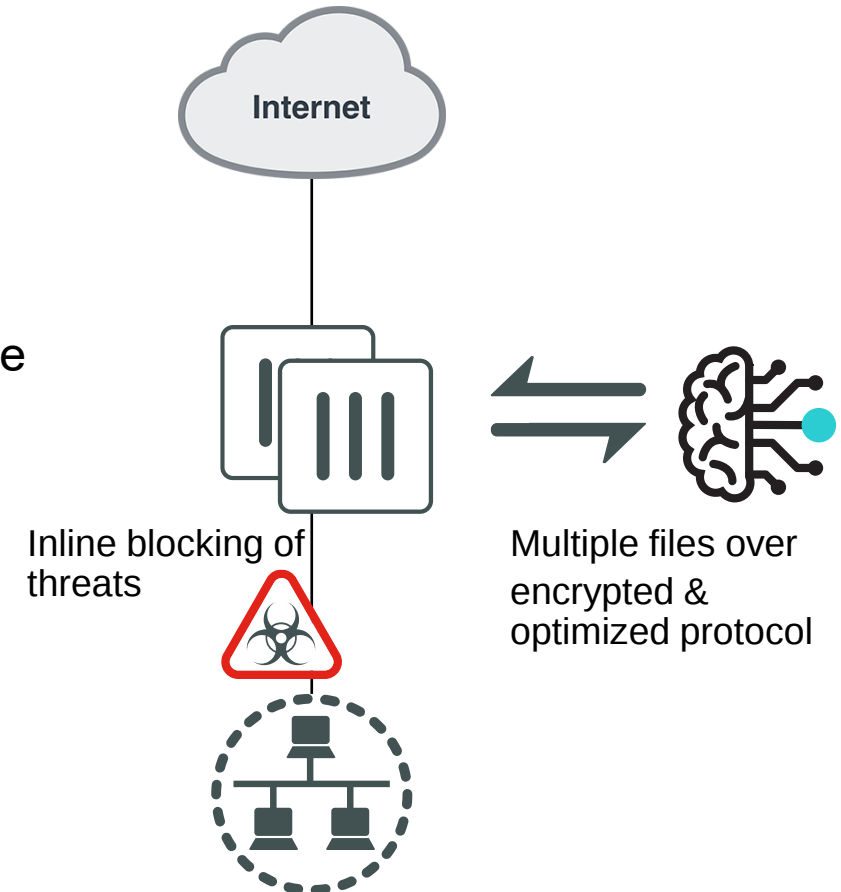


Background:

- 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:

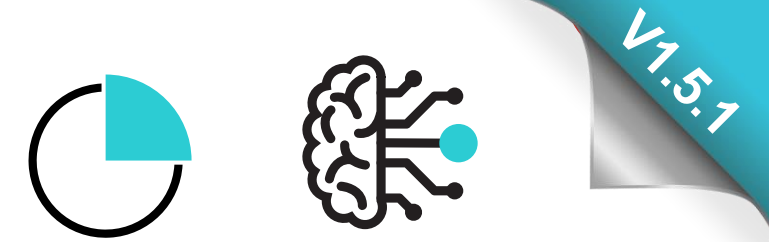
- In FOS 7.0.1 / FortiAI v1.5.1 will have 'inline' blocking feature, where web/email traffic's session will 'hold' and wait for FAI's verdict
- Goal of this is to block "patient zero", utilizing FortiAI's sub-second verdict
- This is configured under FortiGate AV profile (CLI, not FSA field)
- FortiAI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

- 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



The screenshot displays two interfaces from the FortiAI system. The top interface is the 'Log View' page, showing a table of security events. The bottom interface is the 'Log Settings' page, showing configuration options for log servers.

Log View Table:

#	Date/Time	Device ID	Sub Type	Level	Virus Name	Detection
1	15:38:22	FAIVMS0000000000	Malware	alert	HTML/Ransom.AFD...	Ransom
2	15:38:22	FAIVMS0000000000	Malware	alert	Riskware/AdGazelle	Ransom
3	15:38:22	FAIVMS0000000000	Malware	alert	MOAT/Crypted.Gen	Ransom
4	15:38:22	FAIVMS0000000000	Malware	alert	HTML/Ransom.AFD...	Ransom
5	15:38:22	FAIVMS0000000000	Malware	alert	W32/Isda.D!tr	Ransom
6	15:38:22	FAIVMS0000000000	Malware	alert	HTML/Ransom.AFD...	Ransom
7	15:38:22	FAIVMS0000000000	Malware	alert	W32/Crypted.Gen	Ransom
8	15:38:22	FAIVMS0000000000	Malware	alert	HTML/Ransom.AFD...	Ransom
9	15:38:22	FAIVMS0000000000	Malware	alert	MOAT/Crypted.Gen	Ransom
10	15:38:22	FAIVMS0000000000	Malware	alert	W32/Crypted.Gen	Ransom
11	15:38:22	FAIVMS0000000000	Malware	alert	Adware/Vopak	Ransom
12	15:38:22	FAIVMS0000000000	Malware	alert	W32/Crypted.Gen	Ransom
13	15:38:22	FAIVMS0000000000	Malware	alert	HTML/Ransom.AFD...	Ransom
14	15:38:22	FAIVMS0000000000	Malware	alert	HTML/Ransom.AFD...	Ransom

Log Settings Page:

Log Settings

Remote Log Server

Send logs to FortiAnalyzer/FortiSIEM ☒ Enable ☐ Disable

Type Syslog Protocol

Log Server Address 0.0.0.0

Port 514 (Default UDP: 514)

Remote Log Server

Send logs to Syslog Server 1 ☒ Enable ☐ Disable

Type Syslog Protocol

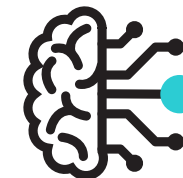
Log Server Address 0.0.0.0

Port 514 (Default UDP: 514)



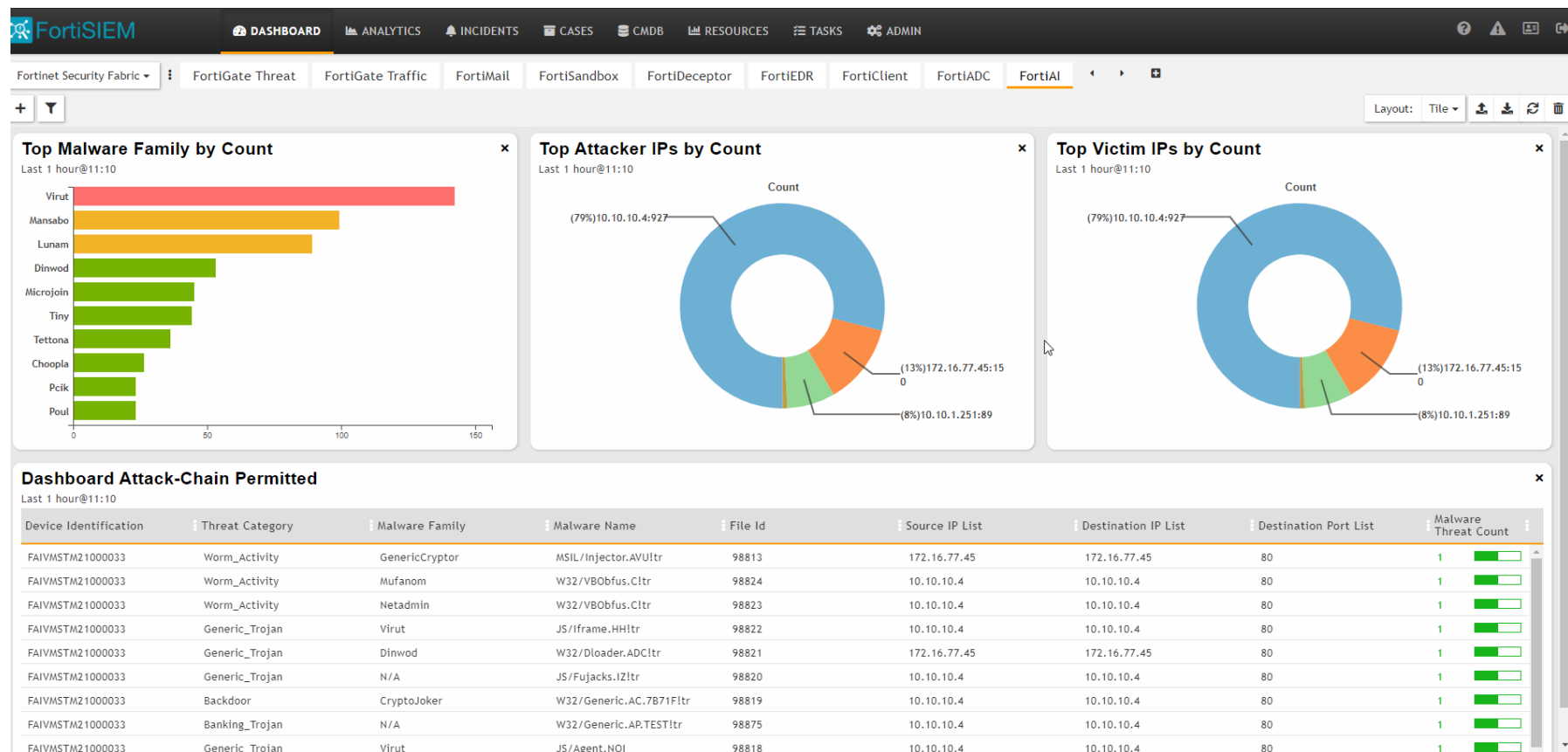
FortiAI - AI-driven Security Operations

FortiSIEM Integration



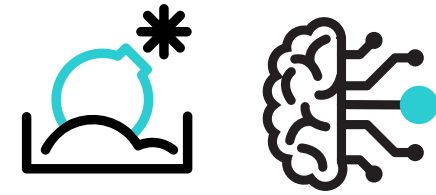
V1.5.1

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



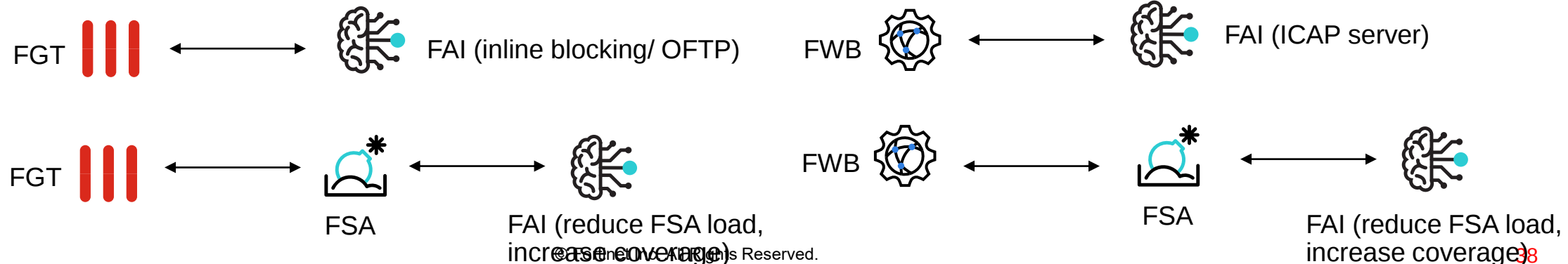
FortiAI - AI-driven Security Operations

FortiSandbox Integration (FSA v4.0.1)



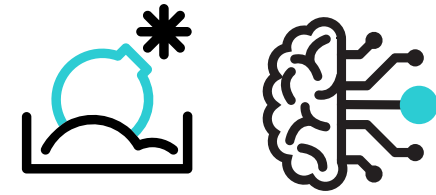
V1.5.7

- **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

FortiSandbox Integration (FSA v4.0.1) - Configuration



V1.5.1

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 *

A screenshot of the FortiAI Settings page. The page has a green header with the FortiAI logo and navigation icons. Below the header, there's a section titled "FortiAI Settings". It contains a list of settings: "Enable" (checked), "Server IP:" (10.59.26.252), "Token:" (a masked token), "Rating Timeout (Seconds):" (5), "Uploading Timeout (Seconds):" (2), and "Maximum File Size (KB):" (2048). At the bottom, there are "OK" and "Test Connection" buttons.

FortiAI Settings

☒ Enable

Server IP: 10.59.26.252

Token:

Rating Timeout (Seconds): 5

Uploading Timeout (Seconds): 2

Maximum File Size (KB): 2048

OK Test Connection

Figure – FSA FortiAI system settings

Figure – FSA Scan profile with “FortAI entrust”

A screenshot of the FSA Scan Profile configuration page. The page has a header with "Scan Profile" and tabs for "Pre-Filter", "VM Association", and "Advanced". The "Pre-Filter" tab is selected. It contains a section "Process the following selected file types." with various file type toggles: Executables, PDF documents, Office documents, Flash files, Web pages, Compressed archives, Android files, Mac files, Linux files, and URL detection. Below this is a "Notes" section. The next section is "Check for Active Content on the selected file types during VM Scan pre-filter." with toggles for office, dll, htm, js, pdf, swf, url, and archive. Another "Notes" section follows. The final section is "Use the results of the following during VM Scan pre-filter." with toggles for FortiAI entrust, Trusted Vendor, and Trusted Domain. An "Apply" button is at the bottom right.

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

* FSA device only appears after file is submitted



FORTINET®