

The Fortinet logo is displayed in white, uppercase letters. The letter 'O' is stylized with a red grid pattern. The background features a grid of dark gray squares, some with semi-circular cutouts, and a red horizontal bar at the top left.

FORTINET

AI in Cybersecurity

Mindaugas Ruginis

Systems Engineer MSSP,

Team Lead Baltics

A solid red horizontal bar is located at the bottom left of the slide.

Cyber business

information 748.720 followers online

news · analysis · reports

Does the artificial intelligence algorithm technology and robotics in the near future have a significant impact on employment internet work evolution future of business and deep learning

Message

Message

AI REPORT

complex engineering, medicine, technical

advanced artificial intelligence production

creating images illustrations and videos

dialogue in the natural language

new behavior
algorithms
ChatBo
line learning

DIGITAL REPORT
Artificial neural networks and large server farms
speech recognition and natural language processing
levels of artificial intelligence and high performance computing
machine learning and big data growth potential
artificial general intelligence benefits
for the corporation business and science

DIGITAL REPORT
REPORT serv

DIGITAL REPORT
works and large server farms
and natural language processing
intelligence and high performance computing
and big data growth potential
intelligence benefits
business and science

artificial intelligence

Industry 4.0

machine learning

AI REPORT

Message

TECHNOLOGY REVIEW

forum business economy

online information service

● business ● industry ● trade

work with artificial intelligence decisions
imaging in the absence of all data of all data
industry, trade, factory future of production
chatbot and automation process neural networks

technique
production process neural networks
AI REPORT
videos
online information service

● business ● industry ● trade

intelligence decisions

technology and robotics in the near future
impact on employment internet work
evolution future of business and deep learning

intelligence decisions



Decades of Innovation

FortiGuard & SecOps Driven AI



182

FortiGuard Patents



42

A.I. Patents

FortiGuard
Antivirus
Engine
Heuristics

FortiGuard
Web-Filtering
Category ML

FortiGuard Web-
Filtering Neural
Networks for
Malicious IOCs

FortiGuard AI
for Spam
Signature
Classification

2 Patents
Malware
Detection,
DNS

FortiWeb
AI for
Botnet
Traffic

4 Patents
AV,WiFi, Cellular

FortiAI
Neural
Networks
for Zero-
Day
Malware

18 Patents
IPv6 Load Balance Wifi
Security Fabric, DNS,
Data Exfiltration

FortiNDR AI
for Suspicious
Network
Activity

7 Patents
Kernel Level network
and storage,WiFi,
Adaptative Labeling,
Sandbox

FortiAdvisor
GenAI in
FortiSIEM
and
FortiSOAR

2005

2006

2012

2015

2016

2017

2018

2019

2020

2022

2023

2024

FortiMail
Bayesian
Training

FortiGuard
Malware
Clustering ML to
Identify Botnet
Traffic

FortiGuard
AutoCPRL – AI
Generated
Detections for
Zero-Day
Malware

FortiSandbox AI
for Malware
Behavior
Analysis

FortiGuard
Web-Filtering AI
for Explicit
Content Sites

FortiEDR AI for
Malicious File &
Traffic Behavior

1 Patent
Malware Classification

FortiGuard AI
for Web-
Filtering in
Different
Languages

9 Patents
Malware Classification
and Identification, DNS,
Image Recognition,
Playbook Creation


FortiSOAR
AI for
Playbooks

6 Generations of AI





FortiGuard Labs

Over 50% of the World's
Firewalls Power
FortiGuard Labs 

755,000+ Customers

VISIBILITY

INNOVATION

ACTIONABLE THREAT INTELLIGENCE

Telemetry



Enforcement Partnerships



CERTs



CTA feeds



OSINT



Trusted Partnerships



Darkweb Research



Firewalls (HW/VM/ SASE)

12M+



Web

250M+



Emails

100M+



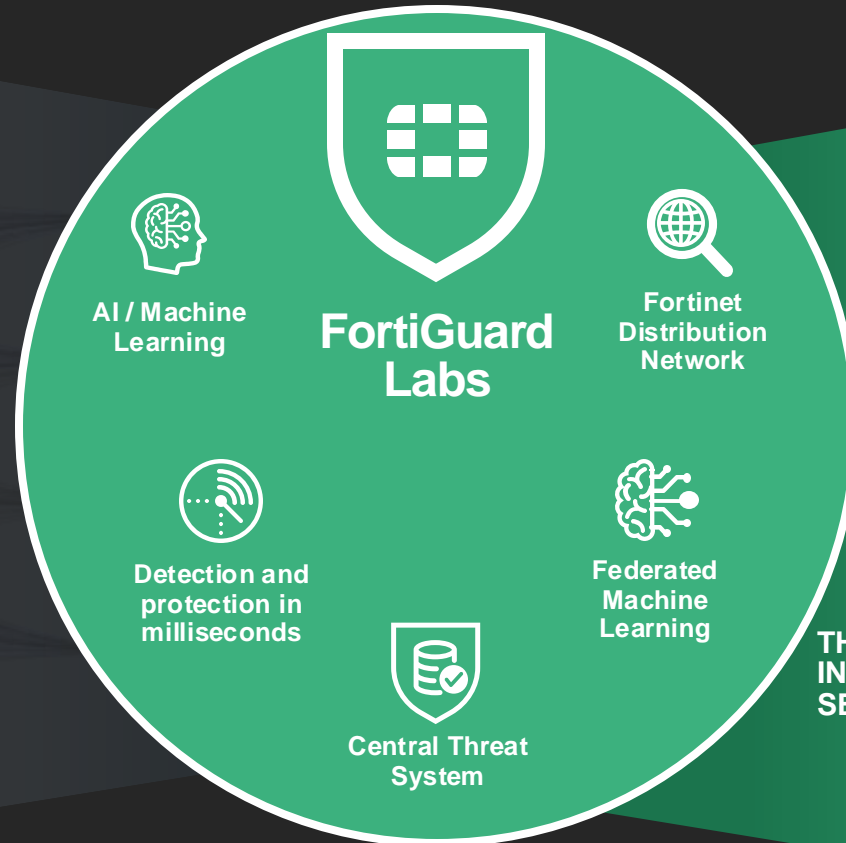
Endpoints

3M+



Sandbox

1M+



SECURITY FABRIC PROTECTIONS



IPS



Application Control



Indicators of Compromise (IoCs)



Phishing



Anti-Spam



Endpoint Vulnerability



PROACTIVE RESEARCH



Adversary Playbooks



Security Blogs



Threat Intel Briefs



Zero Day research



Outbreak Alerts



Virtual Patches

THREAT INTELLIGENCE SERVICES



Penetration Testing



SOCaaS



Incident Response



RedTeam Assessment



Breach and Attack Simulation



Digital Forensics



Architecture Evaluation



Cybersecurity Workshops



FortiRecon

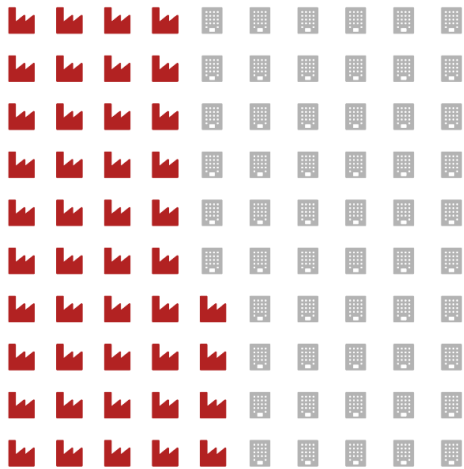


MDR



Ransomware & Wipers

More Targeted to Industry



44% of Global Ransomware Targets OT

Ransomware engagements by industry

Faster Infections



On average new exploits saw attacks in 4.75 days in 2H 2023, 43% faster than 1H 2023

More Levels

Extortion

\$ Encrypt data and hold for ransom

Double Extortion

\$ \$ + threat to release publicly if ransom not paid

Triple Extortion

\$ \$ \$ + threaten to release customer's data if ransom not paid

Quadruple Extortion

\$ \$ \$ \$ + threaten to destroy the data to make it unrecoverable

Increasing pressure to keep paying

For Sale: Initial Access Brokers

Initial Access Brokers



Br0k3r

Selling access to Corporate/Enterprise networks around the world!

⚠ Daily update!

Last update: July 01, 2023

Available networks: 31

Sold networks: 17

Total networks: 48 / ∞

These networks always provided with full domain control privilege. Including Domain Admin credentials, All AD users creds/hashes, DNS zones and objects, Domain trusts... and all other information that may useful for easily network takeover!

You only should plant your beacon/backdoor and start working.

Different countries, Different revenue, Different categories, Different scale and Different price!

The base price is 0.5 and can be changed depending on the network.

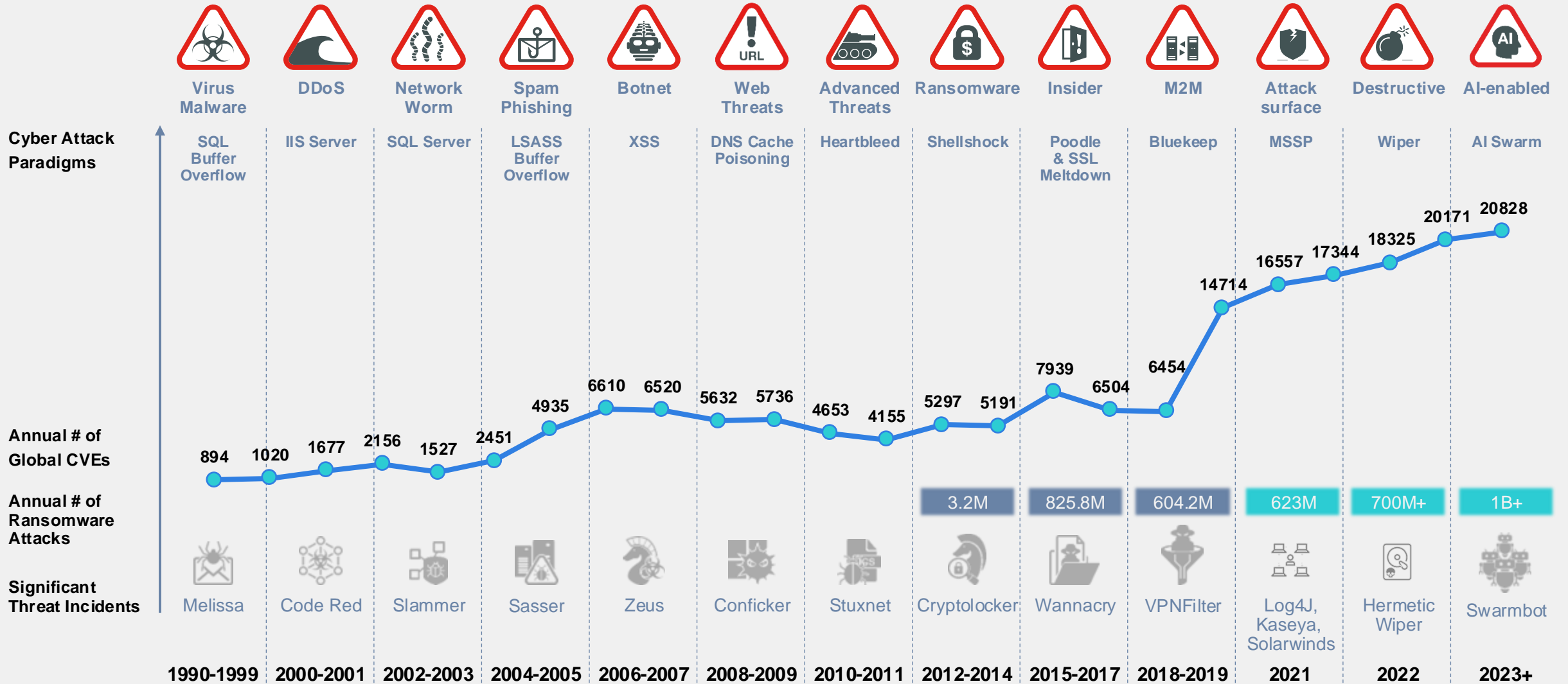
Deal rule: Once you have made your choice, send the desired code, you will receive general information such as internet domain, zoom information and network price. If approved, you will need to share your wallet with enough balance and then we will go to the test phase to prove the existence of the network and you can check the domain admin privilege, access level, network scale, AV/EDR used and other things that may be important to you. Check it out and finally go to pay and make a successful deal!

	#BR001D23	Hospitality	Revenue \$3B	About 2,600 users and 1,600 Computers
	#US001D23	School district headquartered in Danbury	Revenue \$195M	About 18,000 users and 4,200 Computers
	#GH001D23	Law firm company	Revenue \$10M	About 200 users and 300 computers
	#US005D23	Electricity, Oil & Gas	Revenue \$370M	About 2,200 users and 1,600 computers

Electricity, Oil & Gas Auction at 0.5



Hackers Leveraging AI to Attack



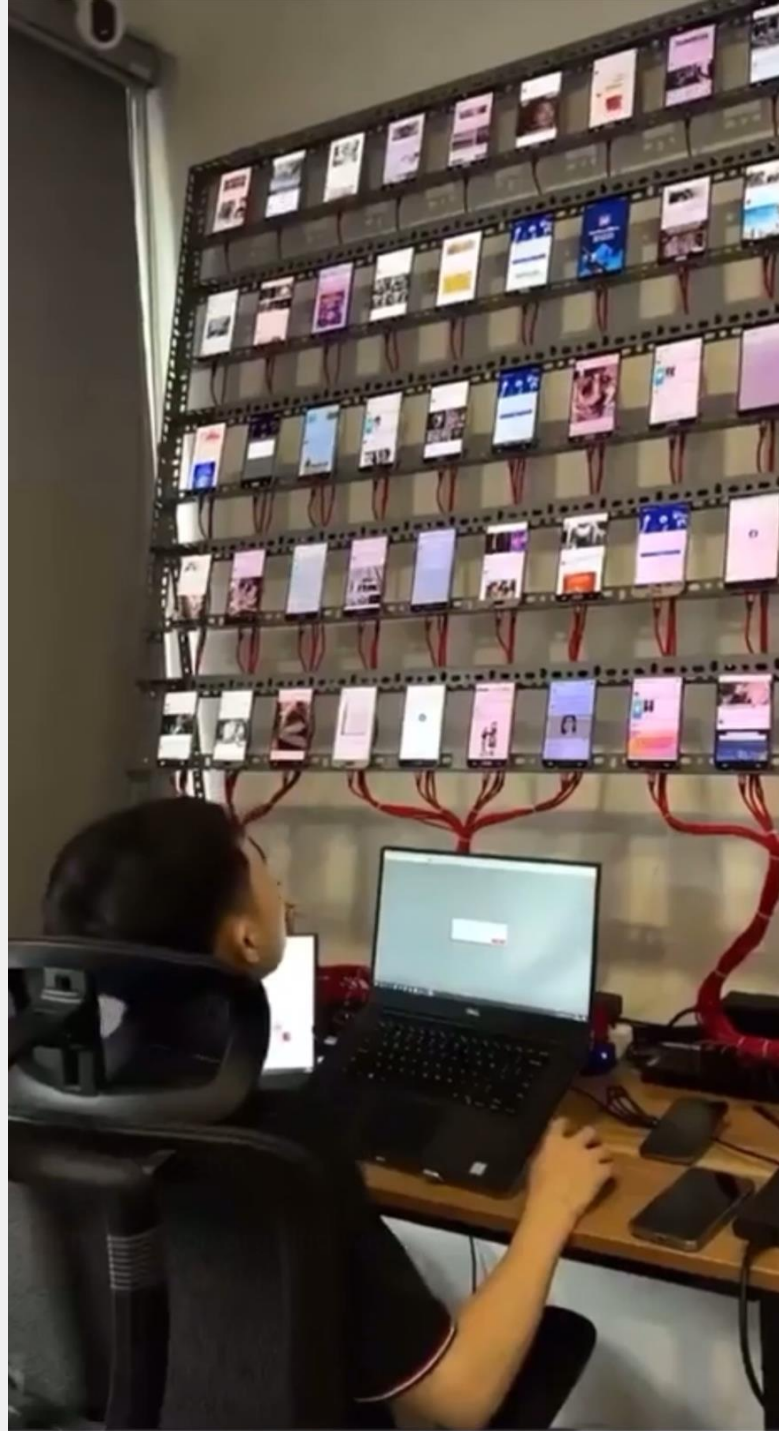
What's wrong?



Publish Poisoned Dataset
MITRE AML.T0019



Mobile Phone Farms



Machine Learning Quiz



Animal



Mammal



Four Legs



Gray Fur



Around 5 kg



Short Tail



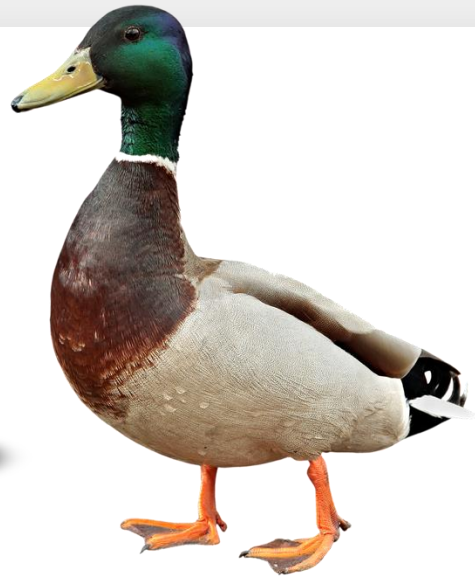
Long Ears



TARGET



Artificial Intelligence - Challenges





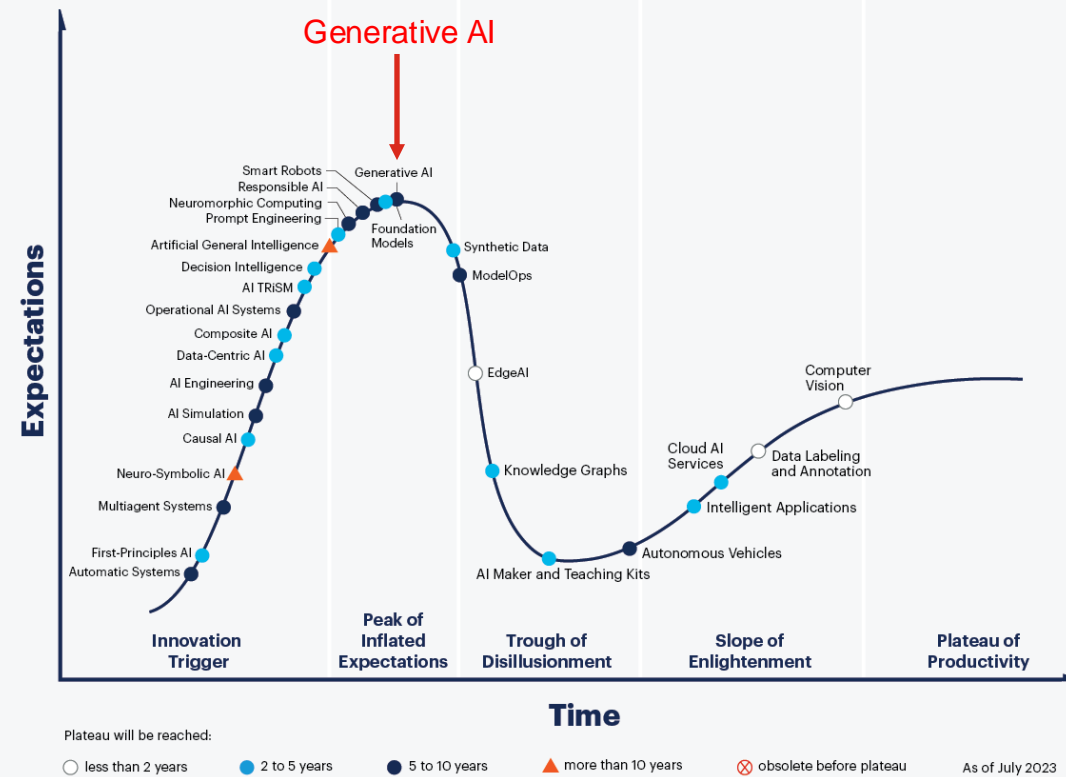
Beyond the Hype

Harnessing AI for greater value and efficient services



2023 Gartner Hype Cycle for AI

Hype Cycle for Artificial Intelligence, 2023



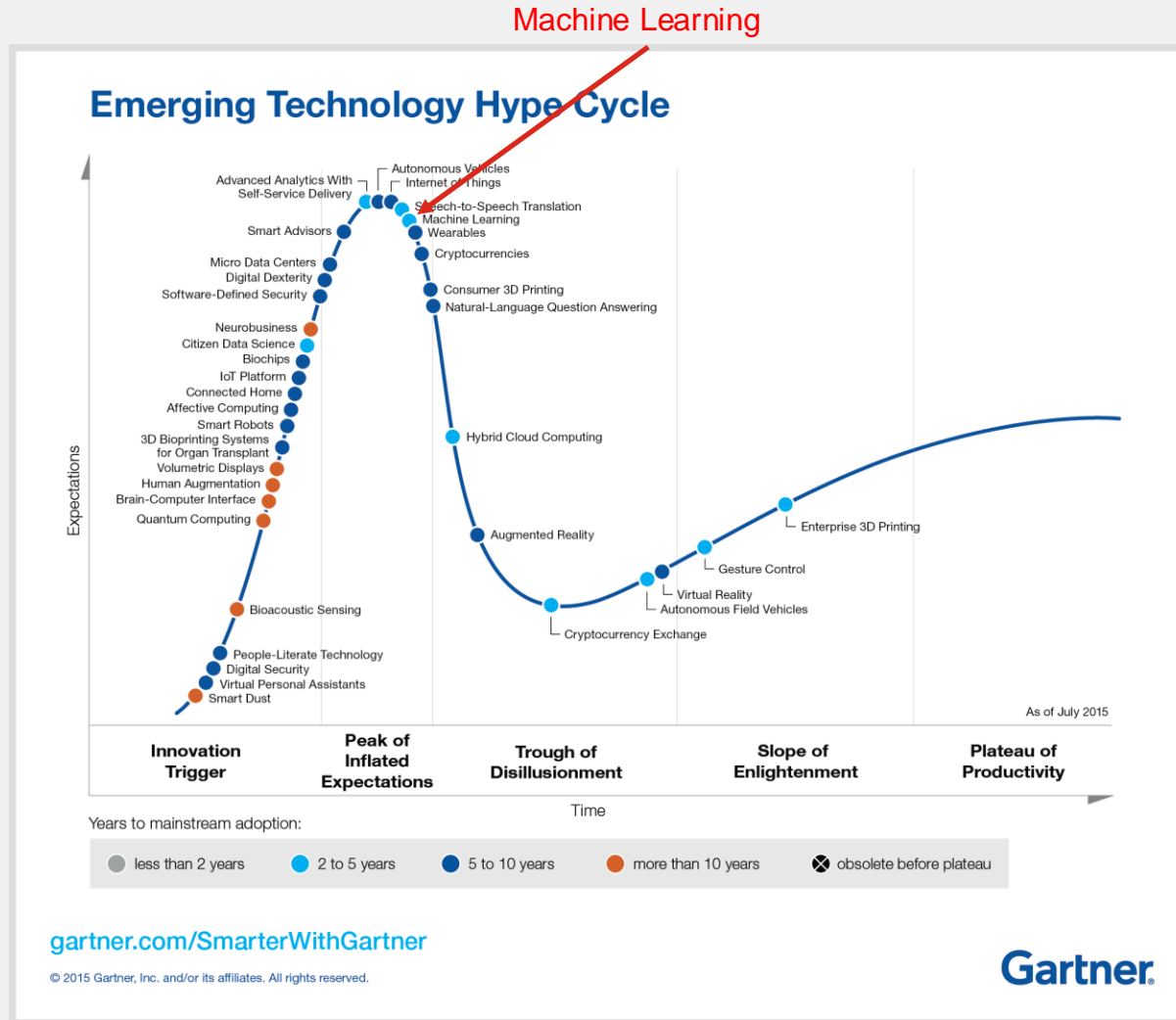
[gartner.com](https://www.gartner.com)

Source: Gartner
© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. 2079794

Gartner.



2015 Gartner Hype Cycle

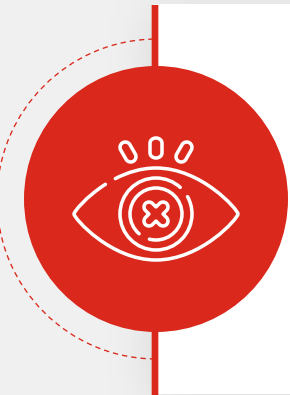


Machine Learning



Supervised machine learning

- Train using “labelled” data
- System learns to identify objects



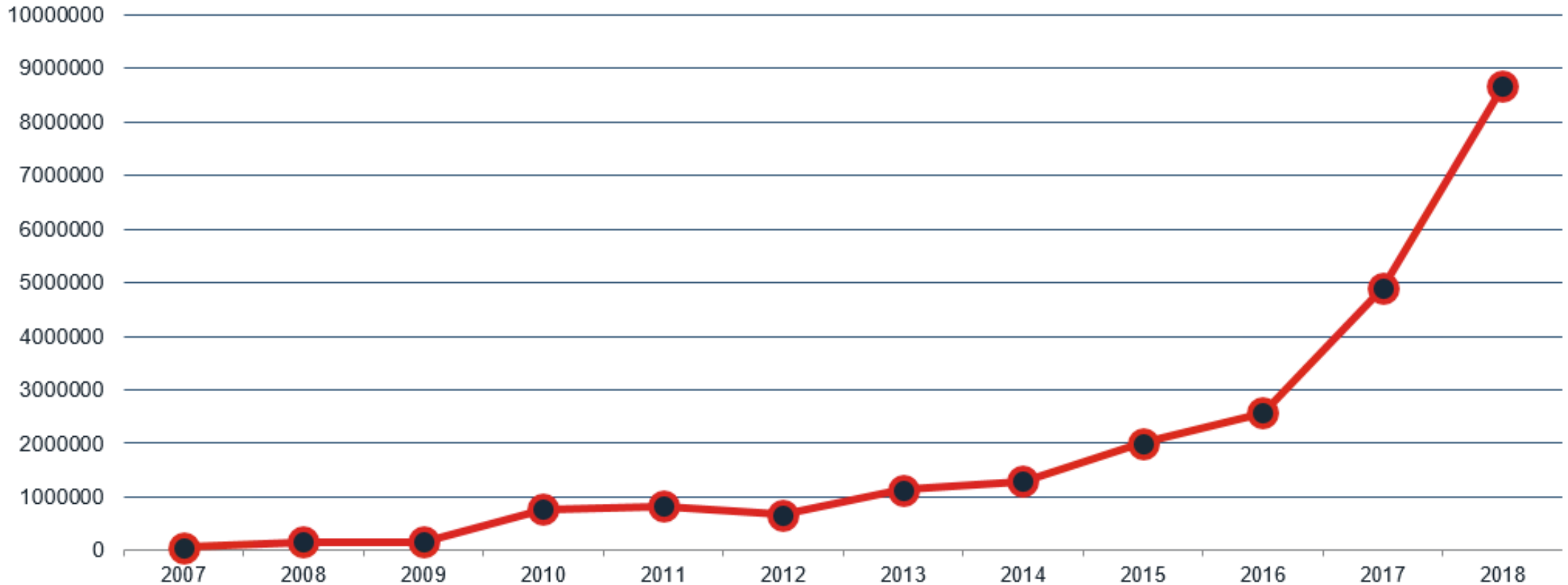
Unsupervised learning

- Establish a baseline behaviour
- Trigger when behaviour does not conform to baseline



FortiGuard Malware Processing Cycle

New malware from all sources per week



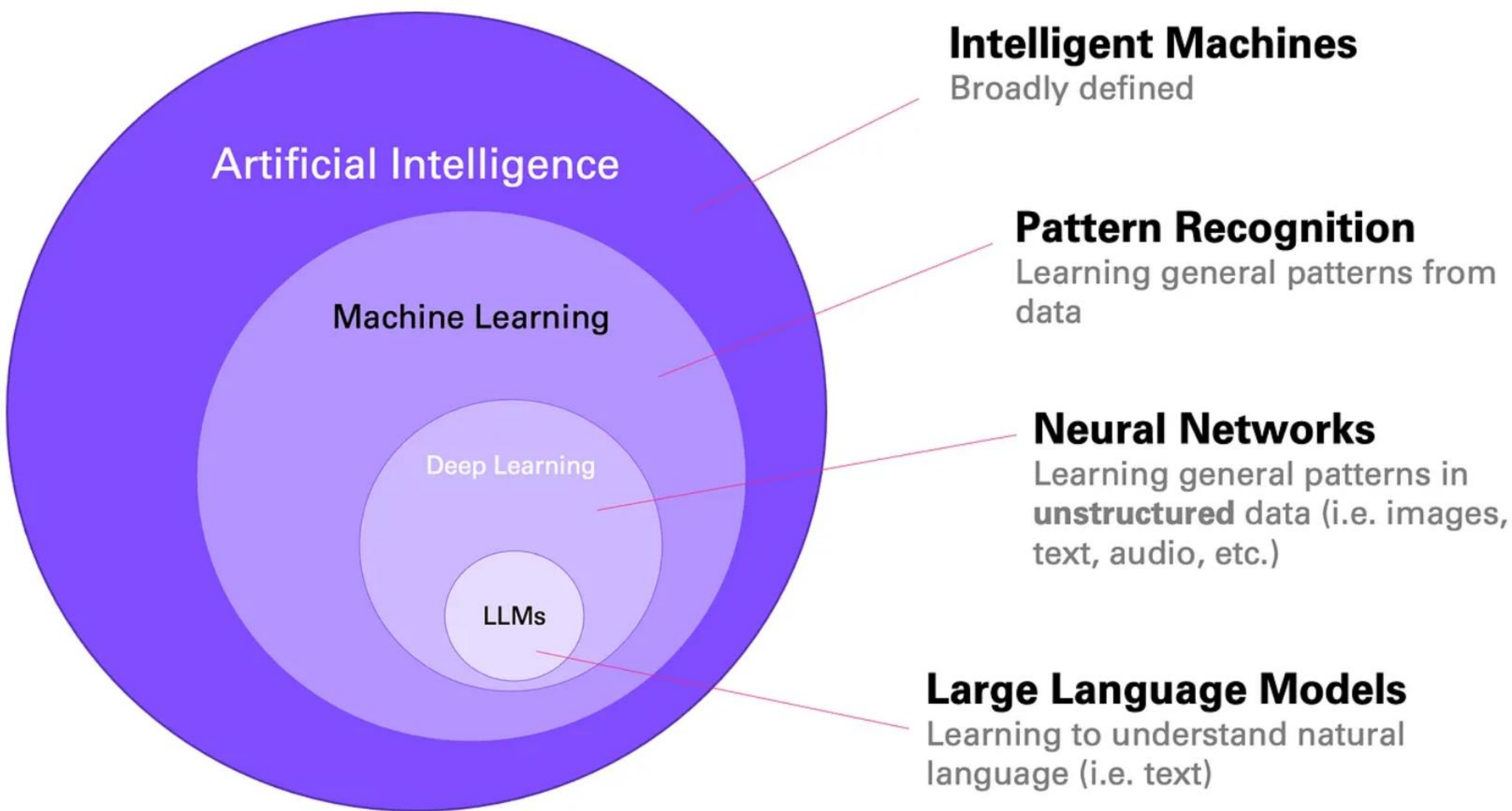
Source: FortiGuard Labs



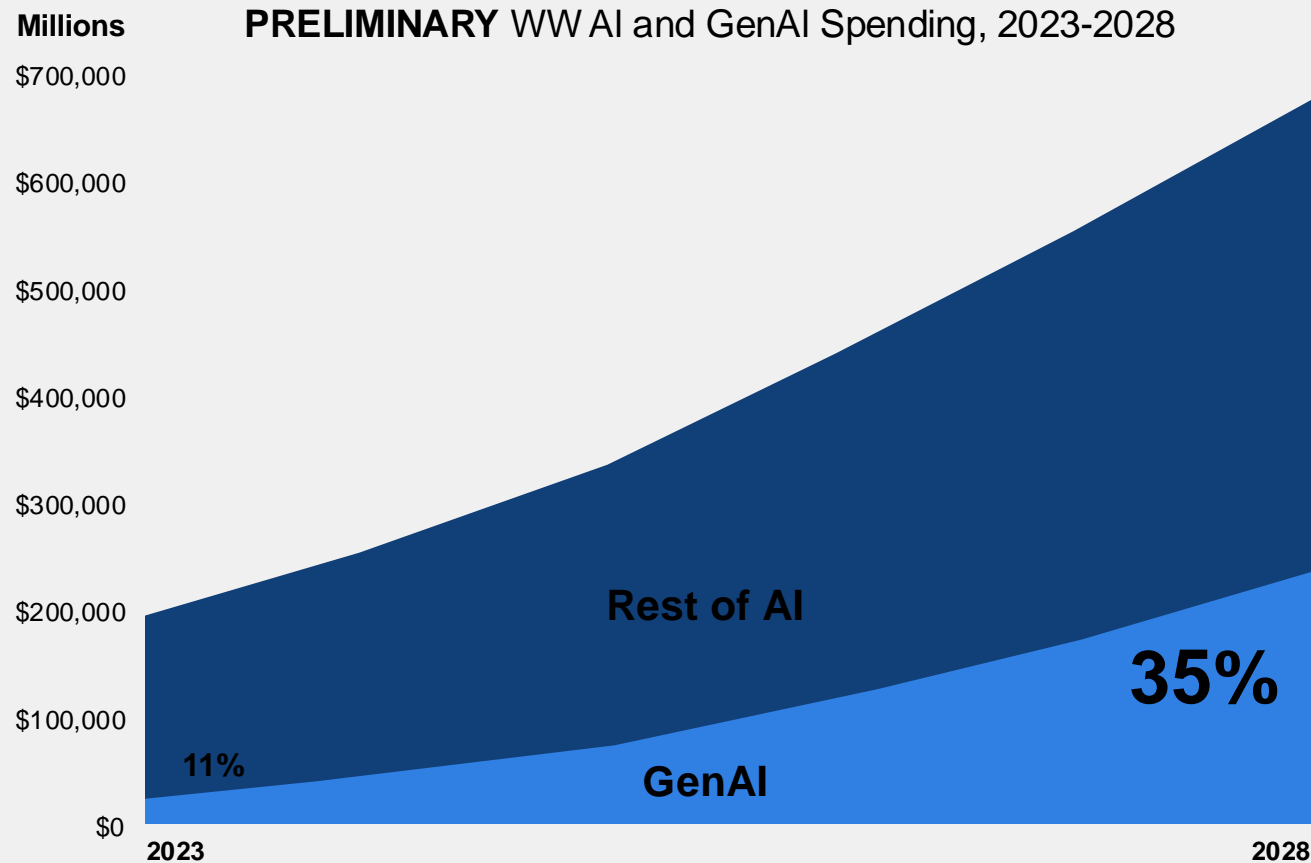
The background features a dark grey gradient with several abstract geometric elements: a red horizontal bar at the top left, a large grey rounded rectangle on the left, a red horizontal bar at the top right, a grey vertical bar on the right, a cyan rounded rectangle at the bottom right, a grey vertical bar on the bottom left, a red horizontal bar at the bottom left, and a grid of small white dots in the lower-left quadrant.

Beyond Machine Learning





GenAI Is a Small, but Growing, Segment of a Much Bigger Opportunity



In 2028

\$625 billion

total WW AI market

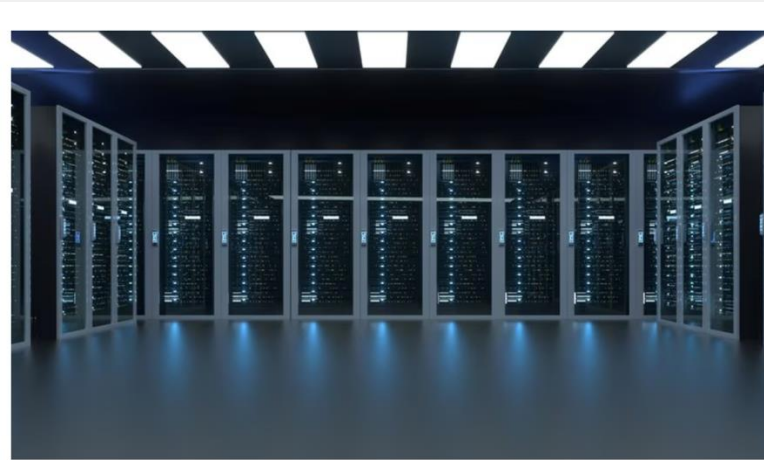
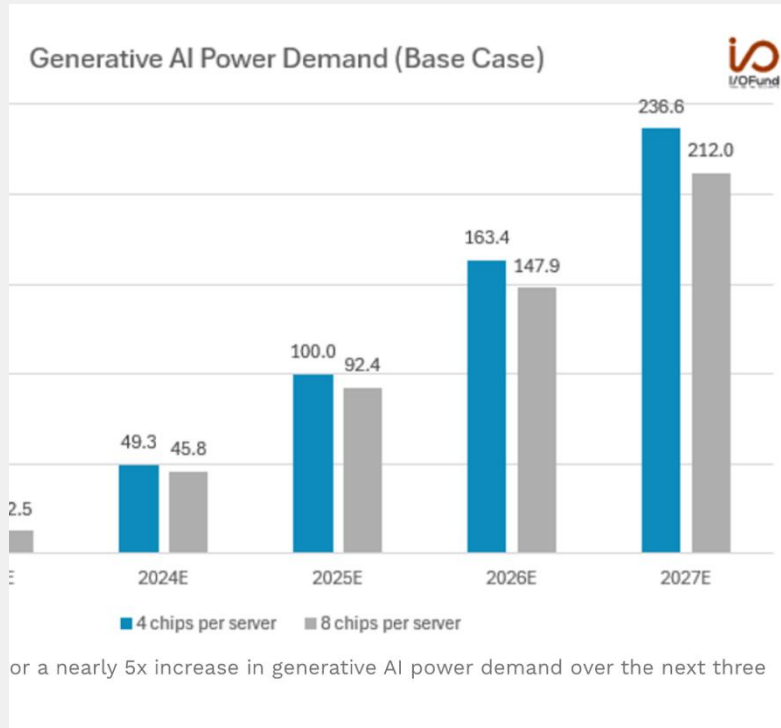
of which

\$215 billion

will be GenAI



AI comes with cost



On average, a ChatGPT query needs nearly 10 times as much electricity to process as a Google search. In that difference lies a coming sea change in how the US, Europe, and the world at large will consume power — and how much that will cost.

Forbes

AI Power Consumption: Rapidly Becoming Mission-Critical

Beth Kindig Contributor @
Free stock tips and stock research newsletter at <https://io-fund.com> [Follow](#)

Jun 20, 2024, 04:13pm EDT

Big Tech is spending tens of billions quarterly on AI accelerators, which has led to an exponential increase in power consumption. Over the past few months, multiple forecasts and data points reveal soaring data center electricity demand, and surging power consumption. The rise of generative AI and surging GPU shipments is causing data centers to scale from tens of thousands to 100,000-plus accelerators, shifting the emphasis to power as a mission-critical problem to solve.

FortiWeb

MACHINE LEARNING



API Discovery and Protection

API Discovery using URL clustering with schema awareness, automatic schema generation, schema enforcement



Threat Analytics

Analyze millions of events using ML to identify common characteristics and patterns and group them into meaningful security incidents



Web Protection

Zero-day attack protection using two-layer solution, Anomaly verification, continuous learning

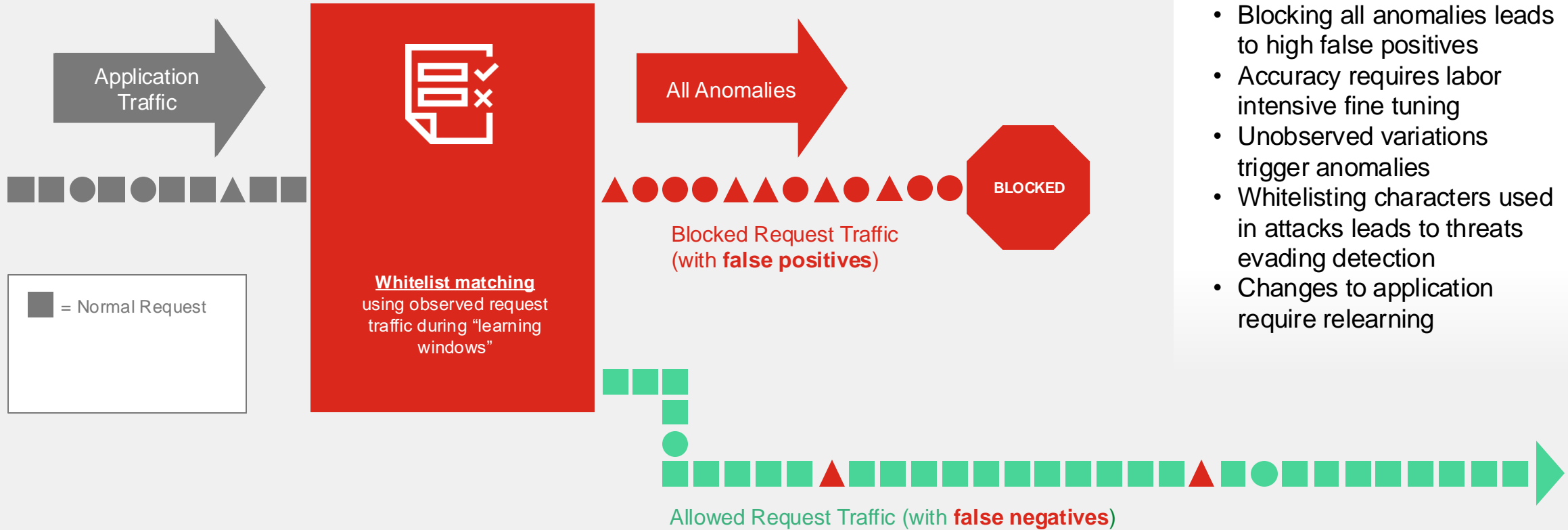


Bot mitigation

Behavioral learning using based on different traffic dimensions, automated verification using training samples

Traditional WAF Application Learning Detection

THREAT DETECTION

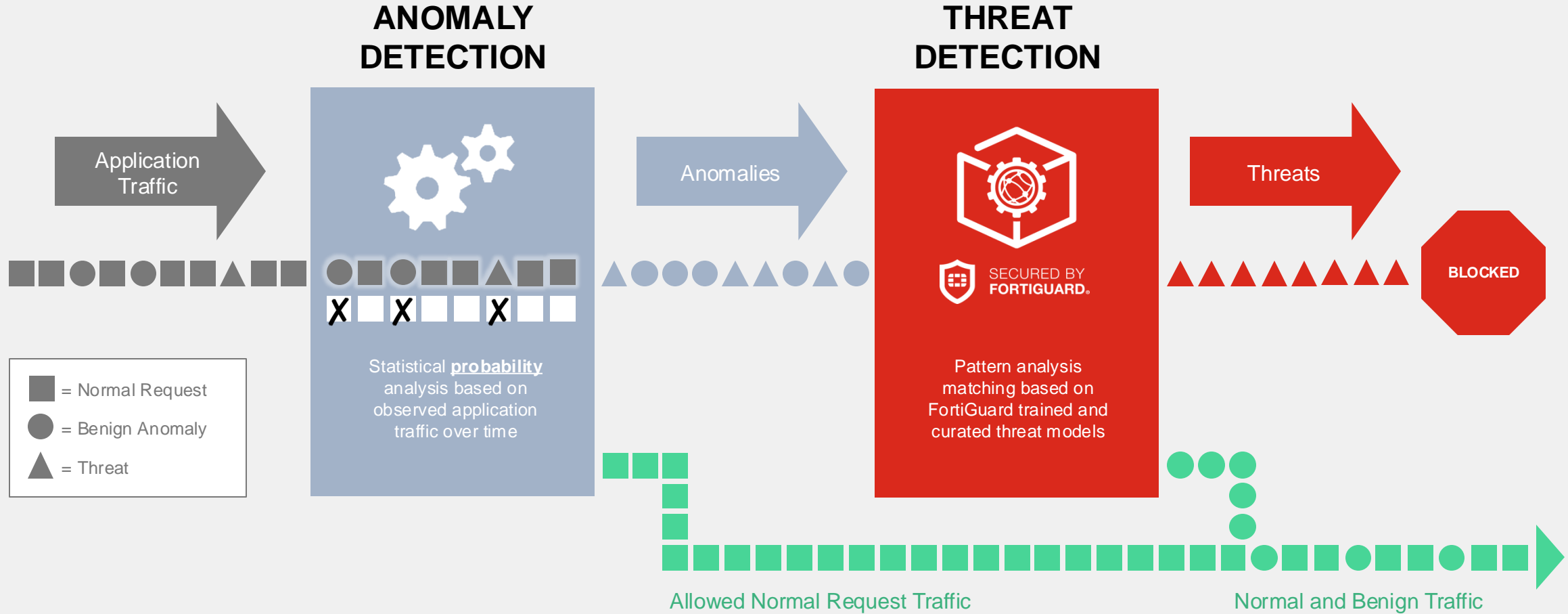


Known Issues/Limitations

- Blocking all anomalies leads to high false positives
- Accuracy requires labor intensive fine tuning
- Unobserved variations trigger anomalies
- Whitelisting characters used in attacks leads to threats evading detection
- Changes to application require relearning



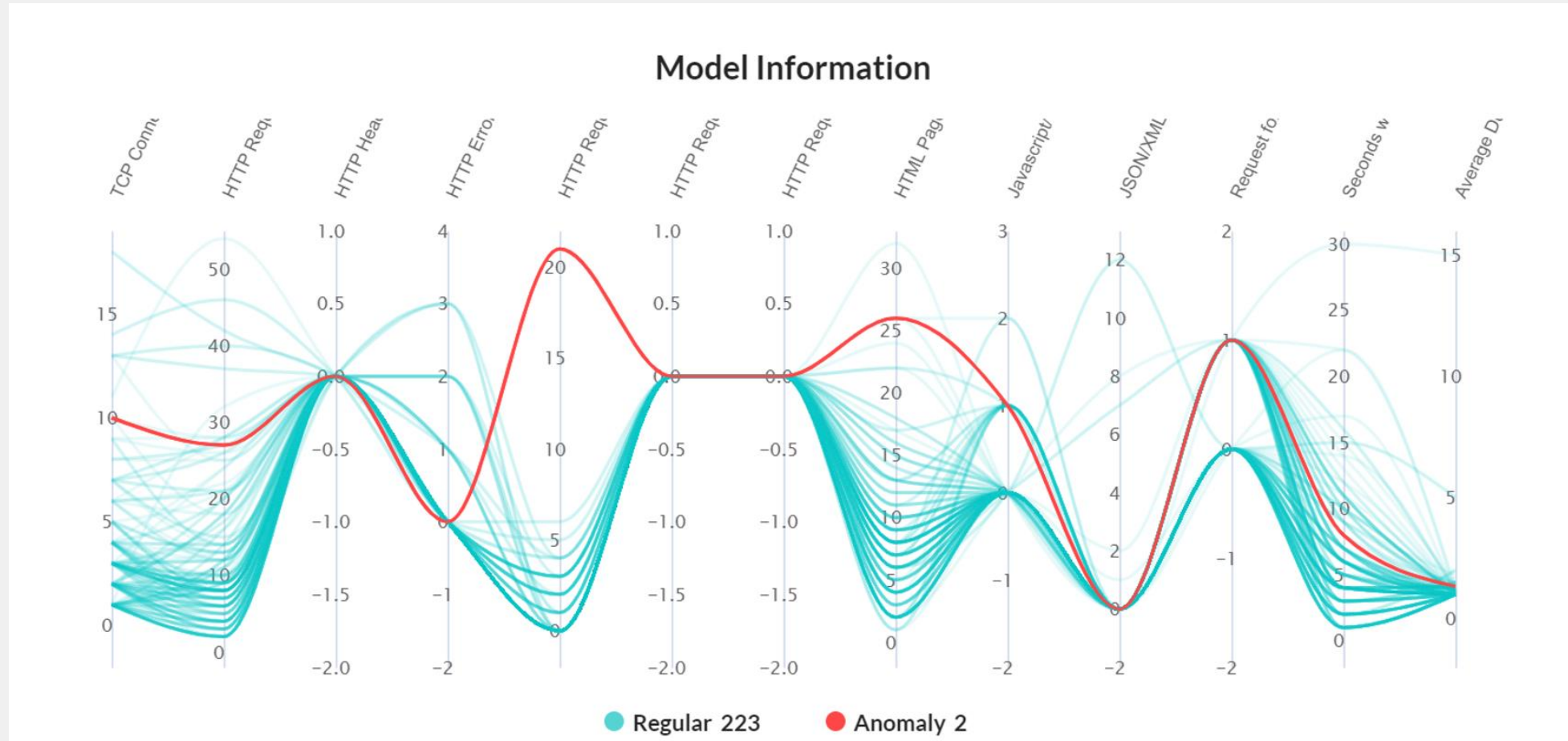
FortiWeb Employs Two Layers of Machine Learning



Reduce friction when deploying web applications!



ML – Machine Learning





FortiGuard Advanced Bot Protection

“To detect and mitigate sophisticated bots using behavioral analysis and deep learning algorithms.”



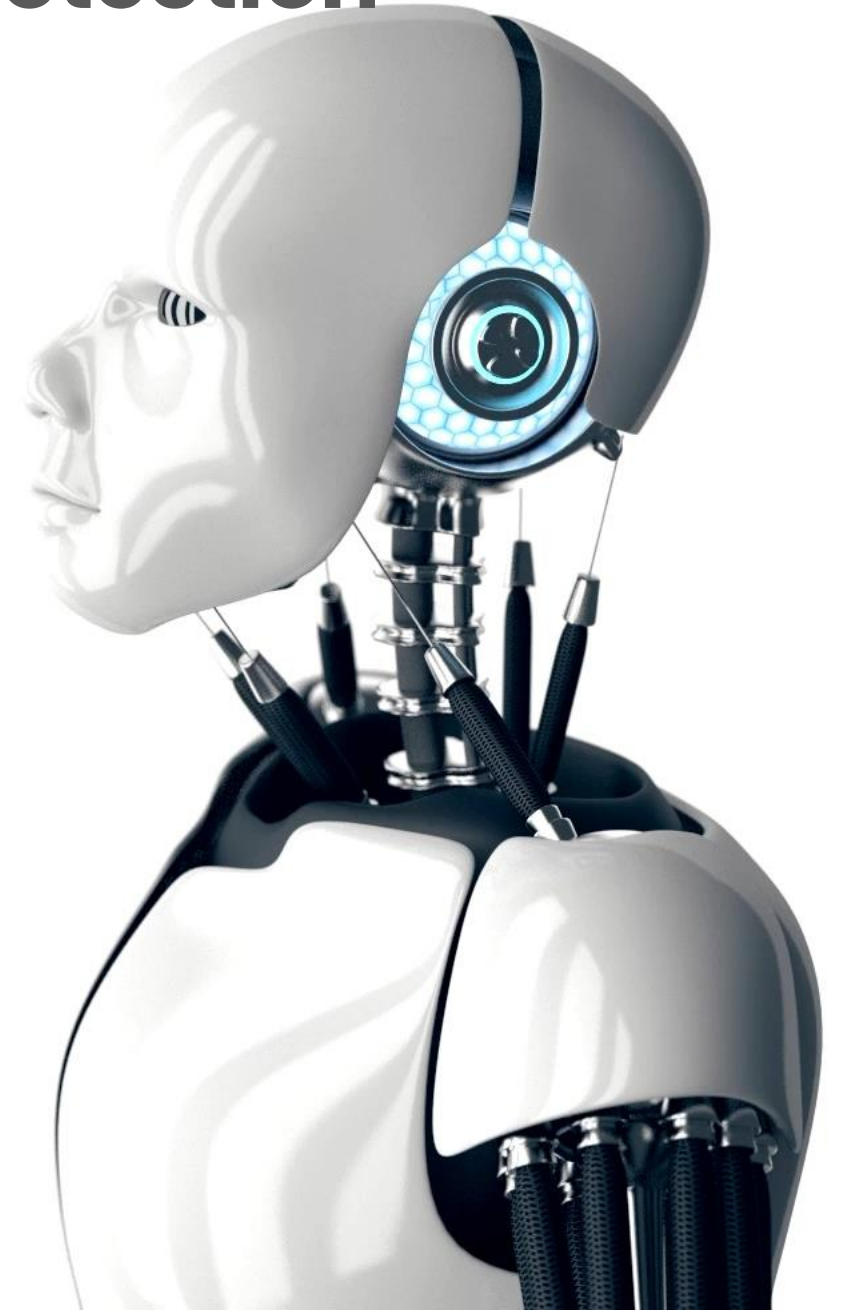
Threats:

- Fraud
- Data theft/ ATO
- Spam
- Web Scraping
- Denial of Service



Unwanted Outcomes

- Negative brand image
- Financial losses
- Regulatory fines
- Customer churn



Bot Attacks Cost, Immediately!

What's On ▶ Music & Nightlife ▶ In The News

Taylor Swift fans fume as 'bot message' leaves them unable to access ticket sale

Multiple fans have taken to social media to complain after being denied access to the AXS website when they tried to buy tickets after being 'identified as a potential bot'

This article contains affiliate links, we will receive a commission on any sales we generate from it. [Learn more](#)

WHAT'S ON By [Catherine Addison-Swan](#)

13:08, 18 JUL 2023 | UPDATED 14:56, 2 AUG 2023

Find things to do

In YourArea

▼ All events

▼ All dates

📍 Location

Search



Nike Shoe Bot

<https://www.nikeshoebot.com>

[NikeShoeBot](#) | [Sneaker Bot](#) | [Shoe Bot](#) | [Automatically Buy ...](#)

Having been in this game for over 8 years, we know that a sneaker bot is the only way to get limited-edition sneakers at retail. NSB is the first sneaker bot to ...

[Best Nike Bots](#) · [Nike Bot Protection](#) · [How Much Do Sneaker Bots...](#) · [Proof It Works](#)

Bookm...

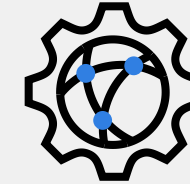
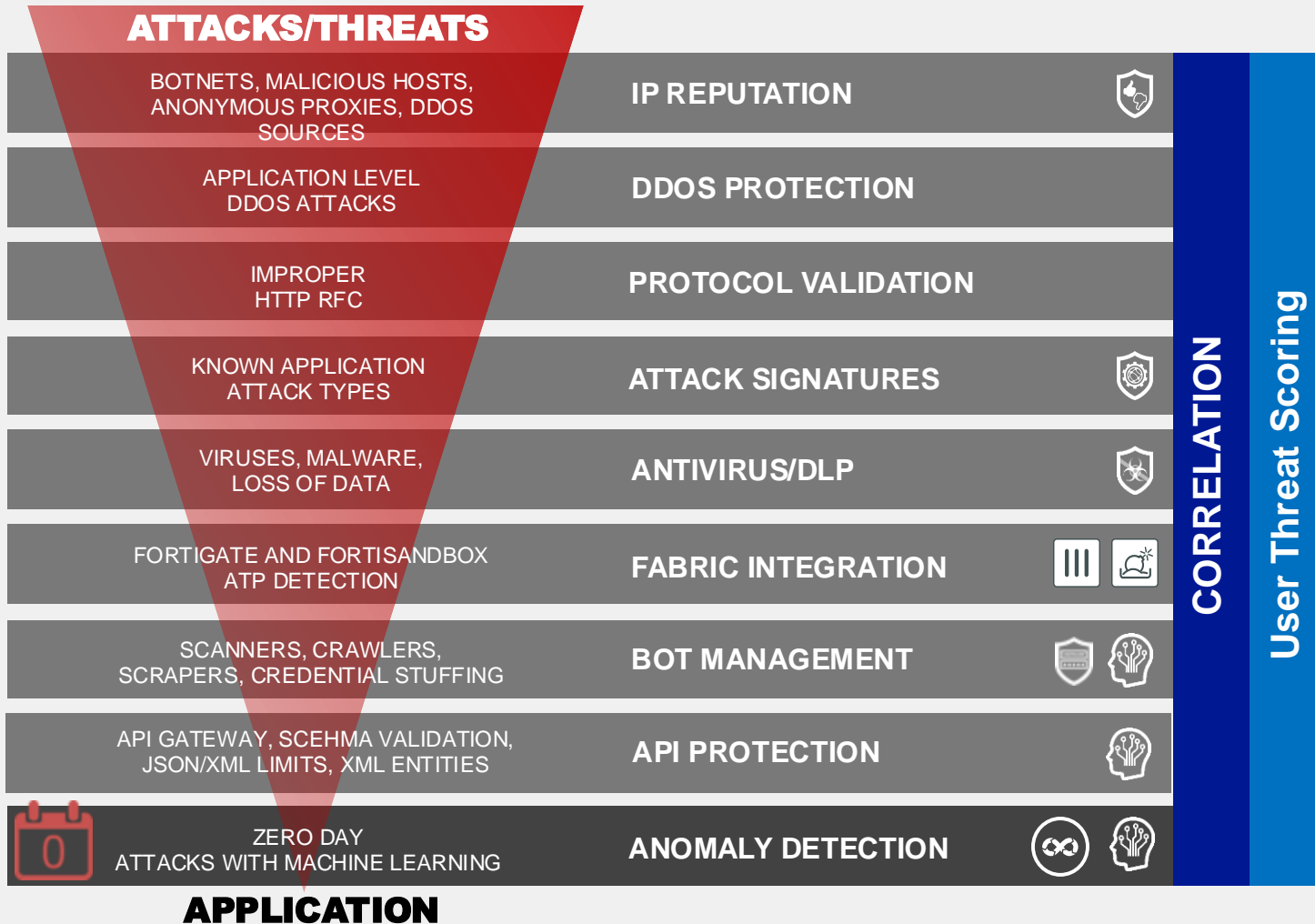
Around 600,000 of the supermarket's 12 million loyalty program members have been warned about a cyberattack.

U.K. supermarket giant Tesco is warning on a **credential-stuffing attack** that potentially affects 600,000 members of its Clubcard loyalty program.

It said that it detected cybercriminals trying out different name and password combos, gleaned from a database of stolen usernames and passwords for other services, on Clubcard accounts. The efforts were partially successful, it said, so out of an abundance of caution, it is replacing cards and requiring shoppers to set up new credentials.



Machine Learning for Anomaly Detection







Machine Learning based anomaly detection learns how your users interact with your application, delivering both improved threat detection and reducing the false positives that drive administrative overhead.





FortiAI

Why work harder when you can work smarter?



Generative AI

The image shows a screenshot of the Fortinet FortiView interface. A central teal callout box contains the text "Show me the top websites by bandwidth". To the right, a white box displays a SQL query for filtering traffic by bandwidth. The background shows the FortiView dashboard with various charts and a sidebar menu.

Show me the top websites by bandwidth

```
select coalesce(natcliip(hostname), ipser('dsip')) as domain, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log-traffic where $filter and (logflag&1>0) and (countweb>0 or ((logver is null or logver<502000000) and (hostname is not null or utmevent in ('webfilter', 'banned-word', 'web-content', 'command-block', 'script-filter')))) group by domain having sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0))>0 order by bandwidth desc### t group by domain order by bandwidth desc
```



FortiAI: Generative AI and More

What MITRE techniques does this threat actor employ? F

The Dragonfly (Energetic Bear) group is known to use a variety of MITRE ATT&CK techniques. Here is a list of some common techniques that they have been reported to use:

1. Spear-Phishing Attachment (T1566.001): Using targeted phishing emails with malicious attachments to gain initial access.
2. Exploit Public-Facing Application (T1190): Attacking vulnerabilities in internet-facing systems to gain entry into a network.
3. Valid Accounts (T1078): Using legitimate credentials to maintain access and move laterally within the network.
4. External Remote Services (T1133): Using remote services such as VPNs to maintain access.
5. PowerShell (T1059.001): Using PowerShell scripts for execution of various tasks.
6. Credential Dumping (T1003): Acquiring user credentials to further compromise systems and maintain access

What blocking actions will help contain this incident? F

Show me the latest known vulnerabilities F

Create a report of events per critical incident for the last 30 days. F

Type a message



Fortinet AI: Applies AI where They Fit Best

Leverage multiple AI technologies. Leverage the large threat landscape. Leverage Fortinet platform and fabric integrations



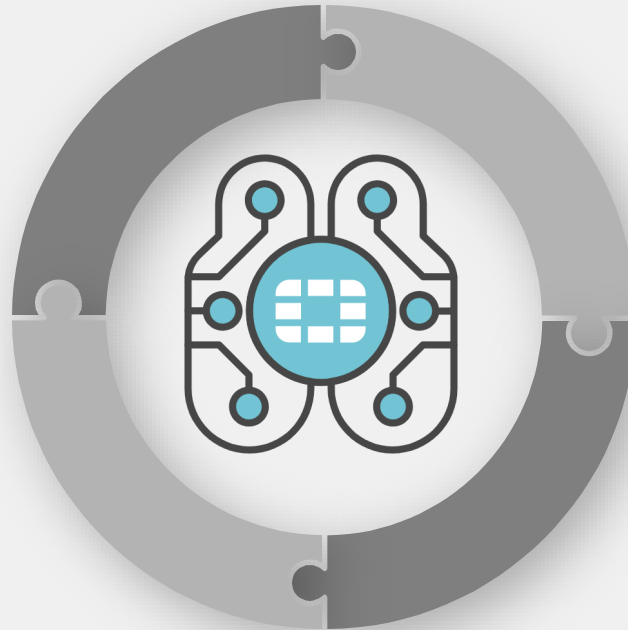
AI for Threat Detection

AI and ML to continuously train the models to improve accuracy and speed in threat detection



AI for Networking

Moving towards a self-healing network model.



AI For Data Protection

Detect and prevent data leakage when Large Language Model (LLM) deployed in cloud applications,



AI for NoC and SoC

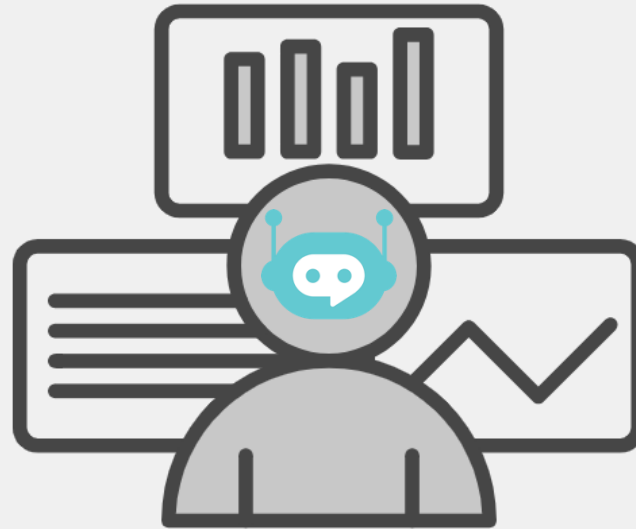
Harness network and security operation with FortiAI Advisor in FortiSIEM, FortiSOAR, FortiManager and FortiAnalyzer

Unified by FortiAI - Autonomous Cyber Defense

FortiAI: Built-in GenAI capabilities for the simplified NoC and proactive SoC

NOC

Simplify configuration & changes
Quick troubleshooting
Automate enforcement



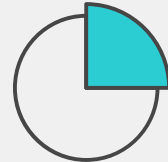
SOC

Save time on complex tasks
Make optimal decisions
Rapidly respond to threats

Guide, simplify, and automate



FortiManager



FortiAnalyzer



FortiSIEM



FortiSOAR

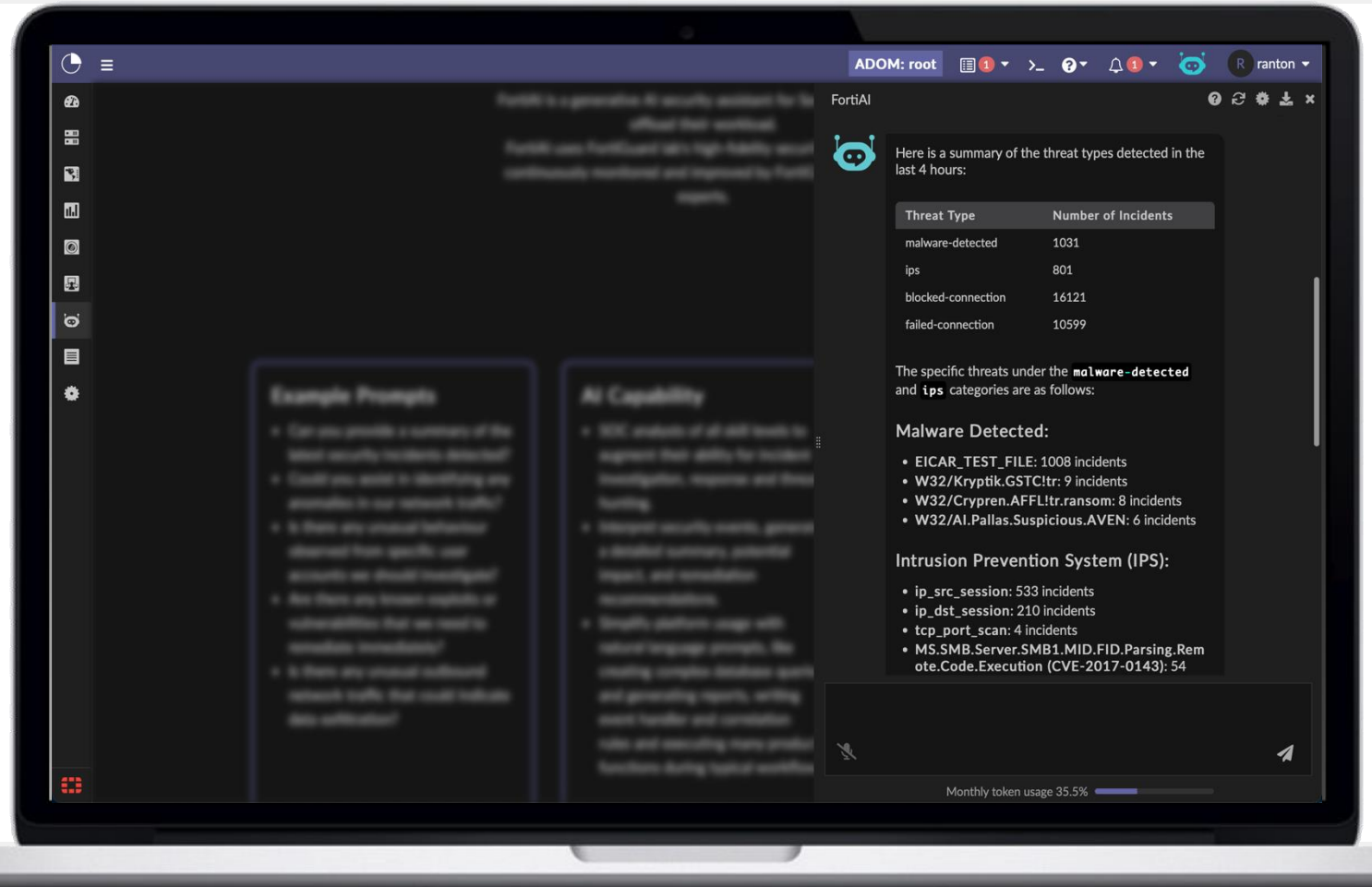


FortiAI GenAI Assistance in FortiAnalyzer & FortiManager

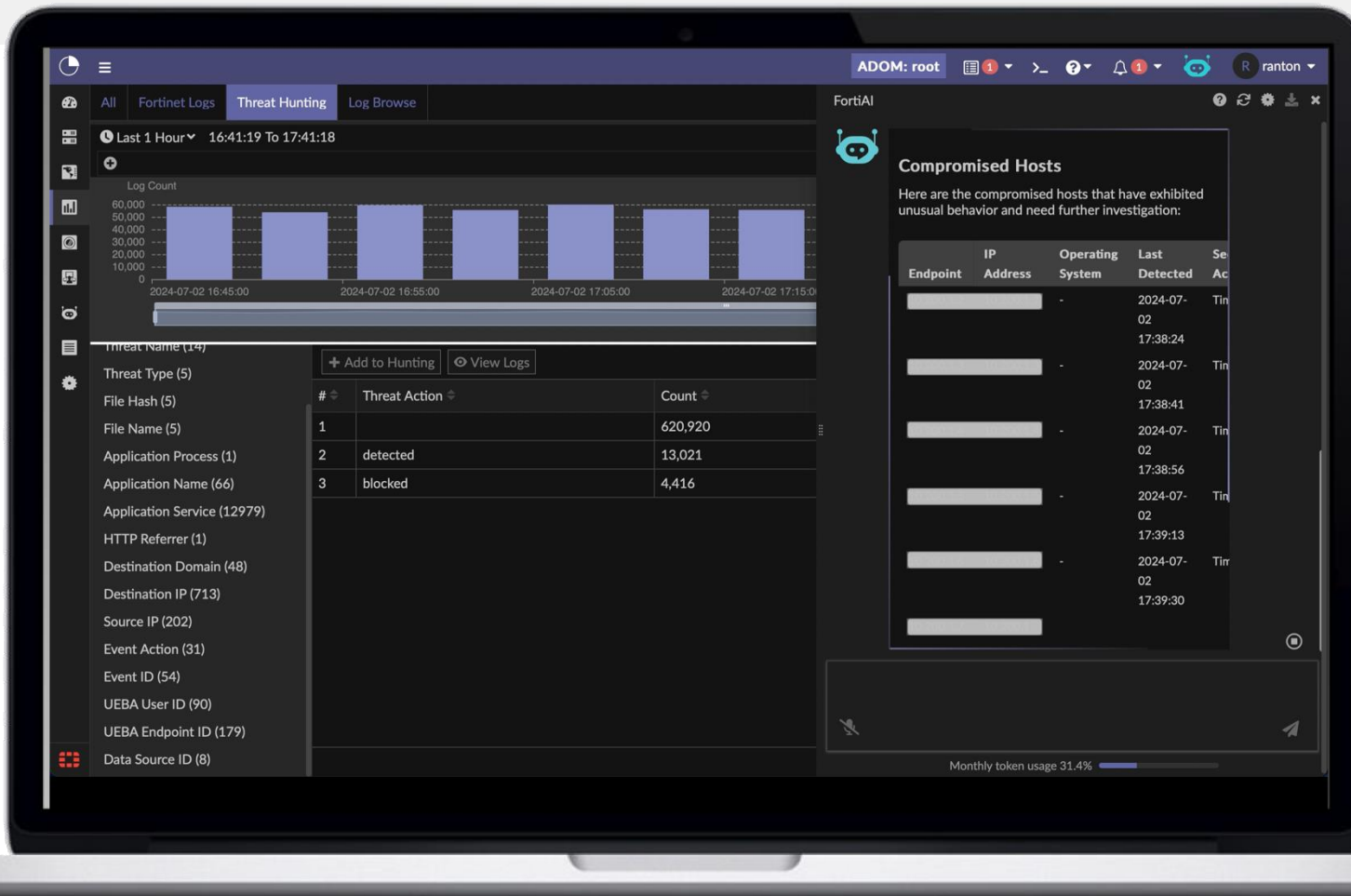


GenAI IoT Security Assistant

Increase analyst productivity and narrow the skills gap with Gen-AI assistance built into the user experience.



Threat Hunting with FortiAnalyzer's GenAI Assistant FortiAI



Telemetry Analysis Turns Data into Action

Analysts can use natural language queries to retrieve log statistics based on specified filters, groupings, and time ranges.

- *"Show me threats without blocking happening on risky destinations"*
- *"Give me the statistics of malware activities detected today by threat name"*



FortiAI GenAI Assistance in FortiAnalyzer



Visualize with Graphical Representations

Benefit from graphical representations and charts to make sense of log data using voice commands.

- *"Render a pie chart for blocked threats by destination IP" or "Show a bar chart of malware activities by threat type"*



The screenshot shows the FortiAnalyzer interface with a log table and a bar chart. The log table has columns for #, Date/Time, Device ID, Action, Source, Service, and Destination IP. The bar chart shows the number of blocked threats by destination IP, with two bars for 10.100.91.2 and 2.1.1.2. The FortiAI assistant is overlaid on the right side of the screen, displaying a message and a list of available log fields.

#	Date/Time	Device ID	Action	Source	Service	Destination IP	V
1							Ei
2							Ei
3							Ei
4							Ei
5							Ei
6							Ei
7							Ei
8							Ei
9							Ei
10							Ei
11							Ei
12							Ei
13							Ei

FortiAI

I will redirect you to the logview page for Antivirus logs to proceed with chart creation for a Malware Report.

Let's continue.

We are now on the Antivirus logview page and ready to create the chart. Here are the available log fields:

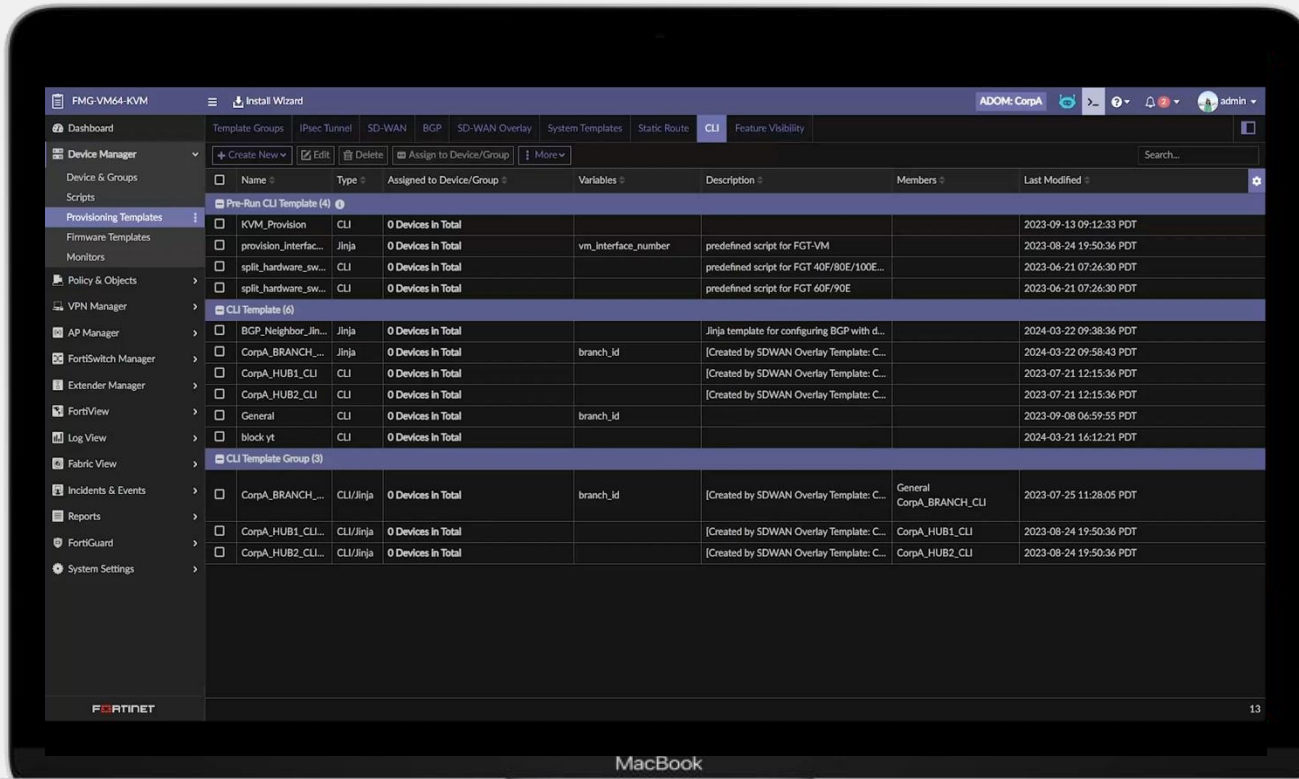
- Device ID
- Action (blocked, passthrough, monitored, analytics, monitor, content-disarmed, infection-removed, attachment-removed)
- Source

Monthly token usage 34.1%



FortiAI on FortiManager

Unleash the Potential of FortiManager and Transform Network Operation



Day 0-1: Quicker Configuration with Consistency:

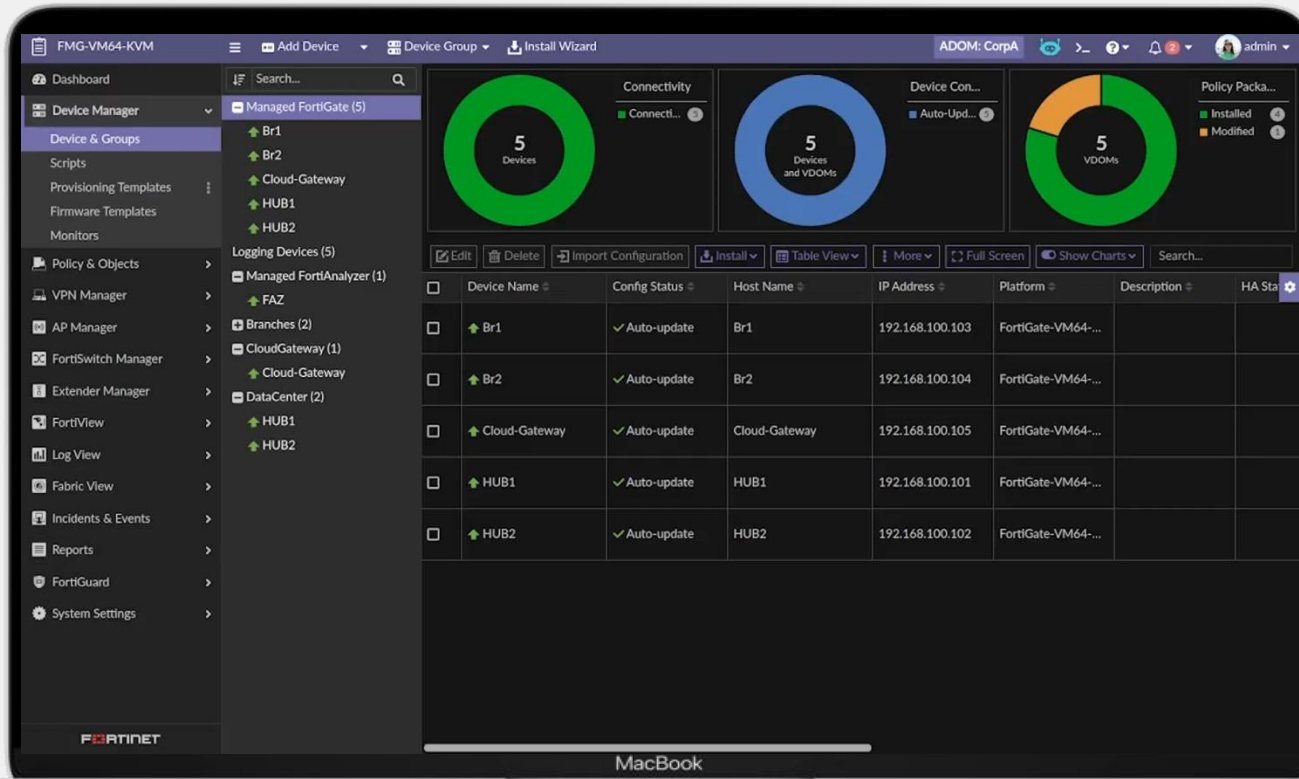
- GenAI-Assisted Scripting
- CLI, Jinja and VPN Advisor
- Syntax Validation and inline editing
- Save scripts and template for execution





FortiAI on FortiManager

Unleash the Potential of FortiManager and Transform Network Operation

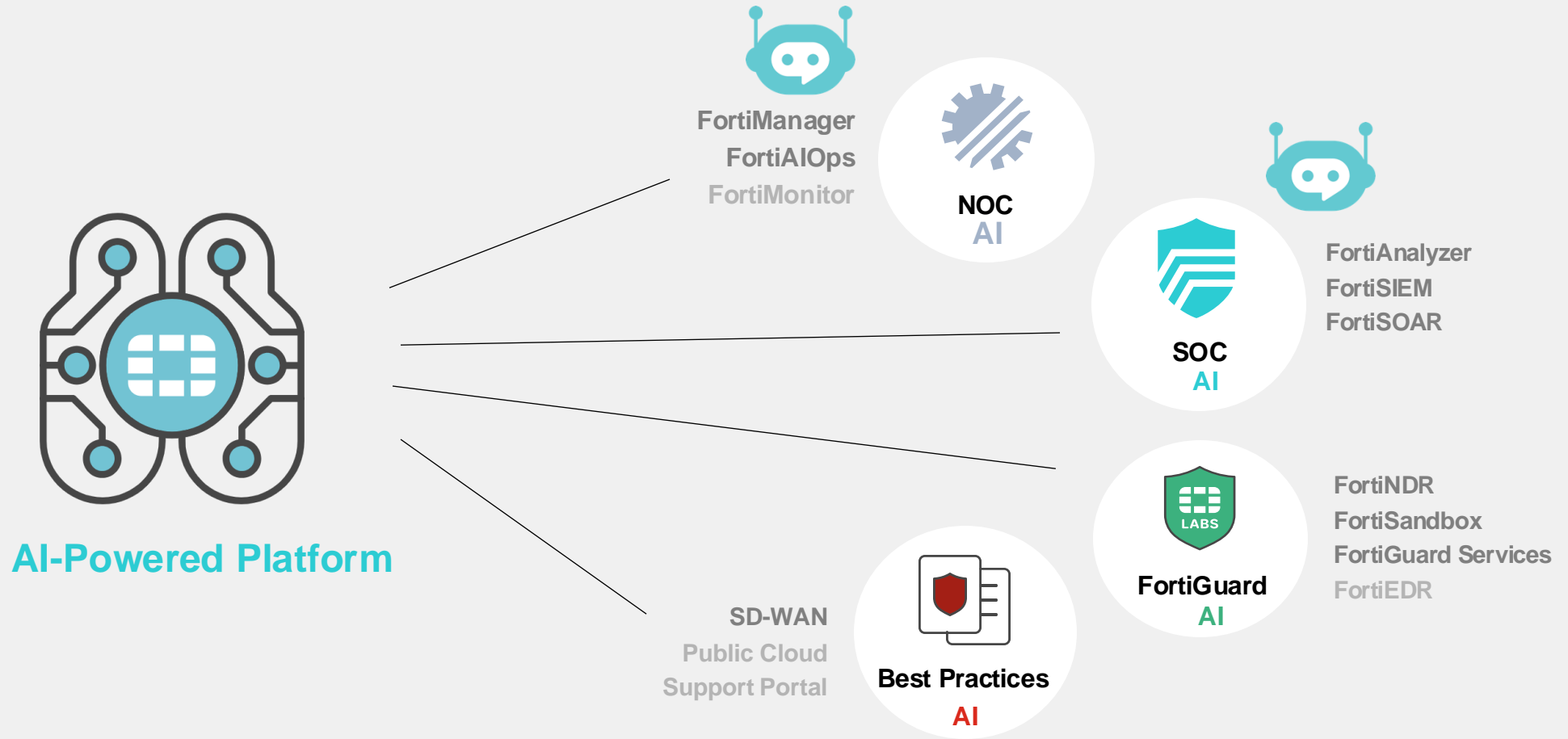


Day 2: From Re-Active to Proactive:

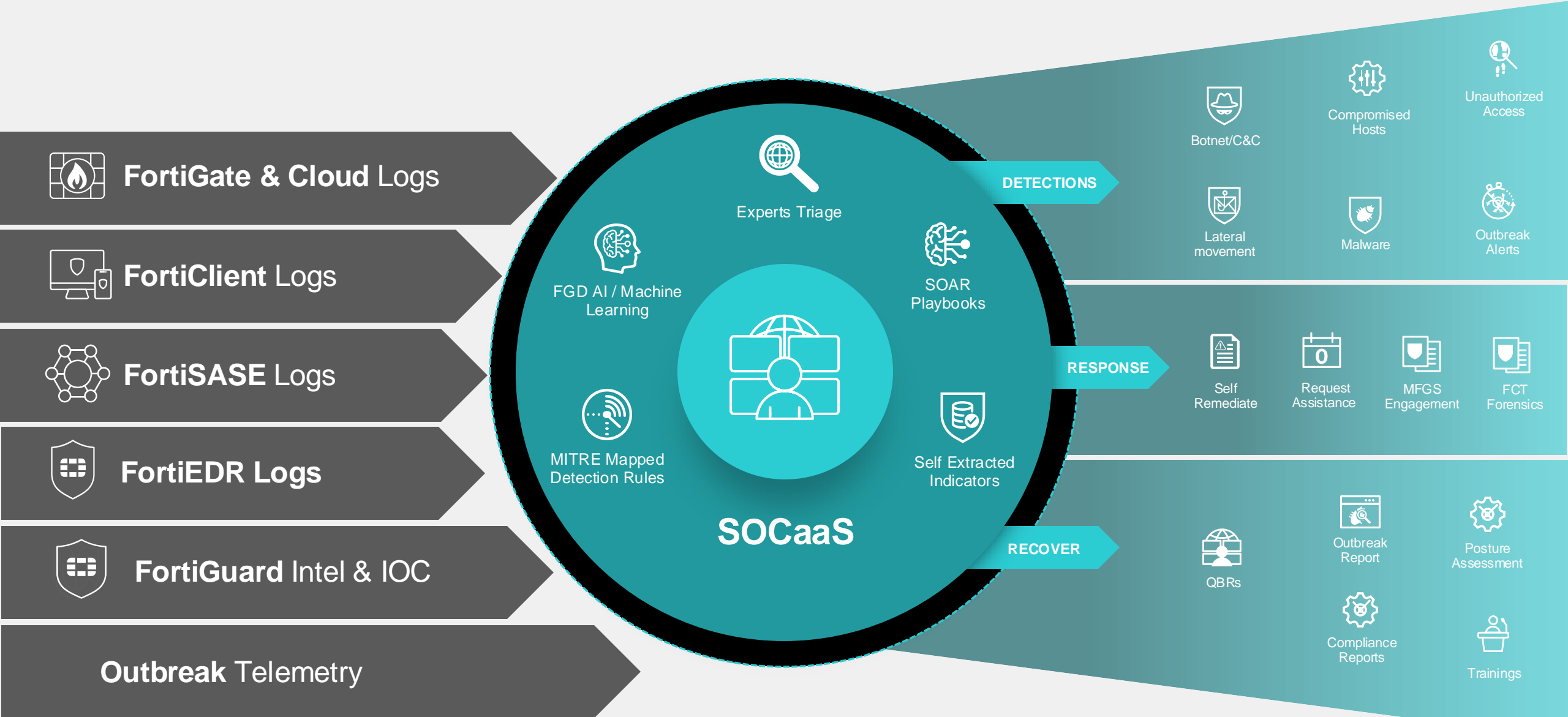
- IoT Device Assistant
- Drill-down on Vulnerabilities
- Recommended actions
- Reporting



Fortinet AI is a Holistic Fabric Play



What is SOCaaS?



FORTINET

