FORTINET

Dual Role of AI in Cybersecurity: Defender of Systems, Guardian of Itself

Dr. Rattipong Putthacharoen, Com. Eng.

Senior Manager, Systems Engineering

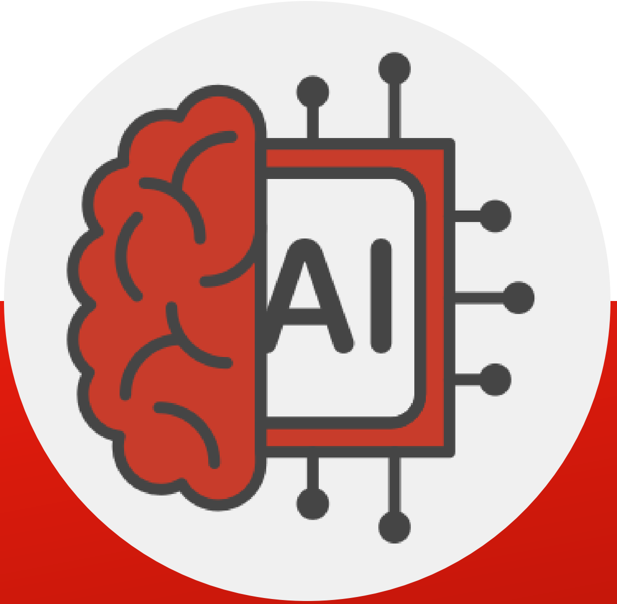
Agenda

1 | AI Threat Landscape

2 | Security powered by AI

3 | AI/LLM Security

4 | About Fortinet



AI Threat Landscape

AI Opportunities & Challenges

Increased use of AI, GenAI is creating opportunities and cybersecurity challenges

AI enables business transformation

Transform business operations, new offerings

Weaponization of AI by adversaries

Attackers using AI for advanced attacks

Vulnerabilities in AI systems

Secure AI Models, prevent LLM data leakage

AI Threat Landscape

Automated Phishing Campaigns

Generative Profiling for Social Engineering

AI-Powered Password Spraying

Deepfake-Assisted Voice Phishing (Vishing)

Enhanced Malware Creation

AI-Generated Misinformation Campaigns

AI Joins the Attacker’s Arsenal

And Most Firms Have Felt It

58%of organizations across Thailand say they have encountered AI-powered cyber threats in the past year.

2X

3X

2X increase reported by 62%

3X increase by 34% of organizations.

AI-powered attacks not just emerging — but already a majority have already experienced/encountered it

AI Joins the Attacker's Arsenal

Fuelling a New Class of Sophisticated, Scalable Attacks

THE TOP 5 AI-DRIVEN THREATS

01 AI-assisted credential stuffing / brute force attacks

02 AI-powered Phishing/ malware (polymorphic/self-evolving)

03 AI-based data poisoning / adversarial AI attacks

04 AI-enhanced reconnaissance (attack surface scanning)

05 AI-driven deepfake impersonation (e.g., BEC)

AI is being used to automate and optimize attacker success rates, rather than simply replacing humans.

AI Joins the Attacker’s Arsenal

Confidence in Tackling AI Threats Remains Worryingly Low

9%

Only Less than **1 out of 10** (9%) of organizations say they are very confident in their ability to defend against AI Powered threats

43%

43% admit that AI threats are outpacing their detection capabilities

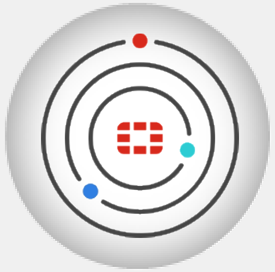
1 out of 4

24% say they have no ability to track these threats at all

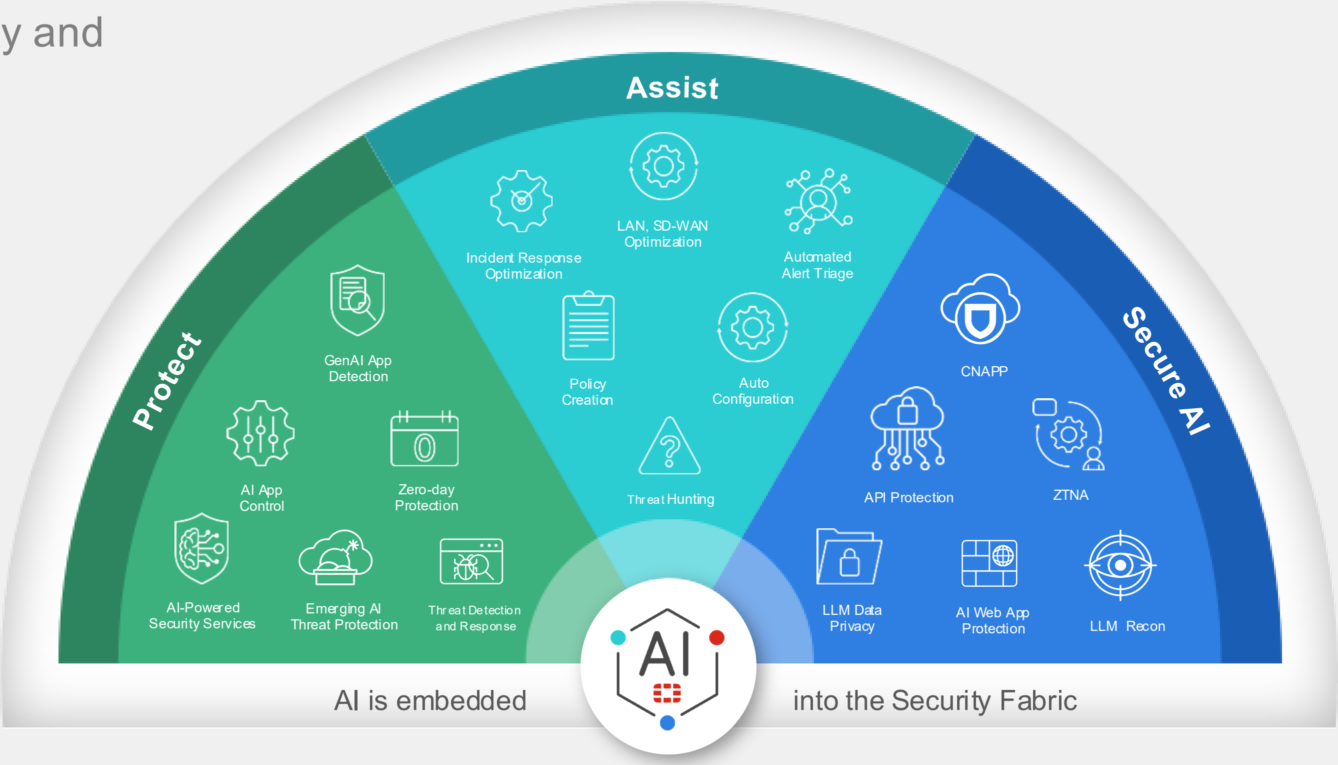
Security powered by AI

AI Use Cases

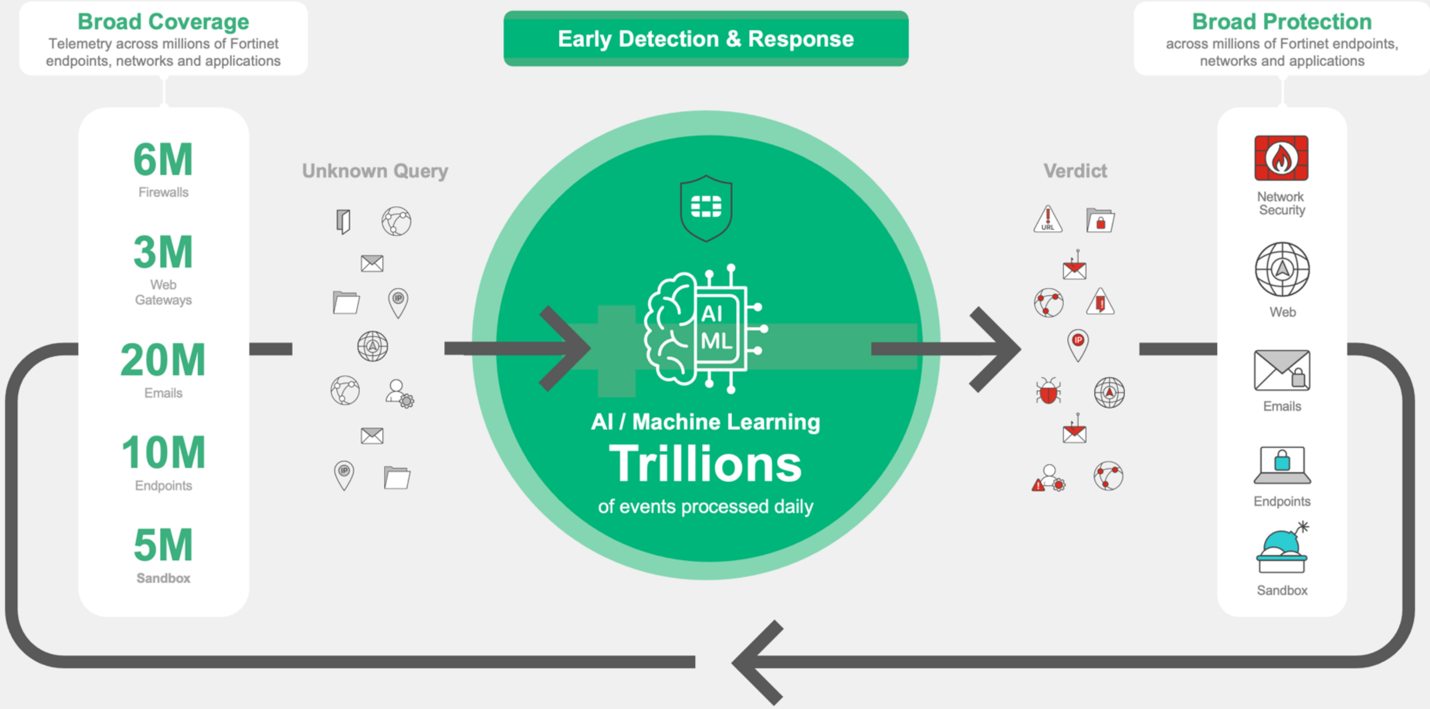
Integrated Security Fabric, AI models for security and Autonomous Operations



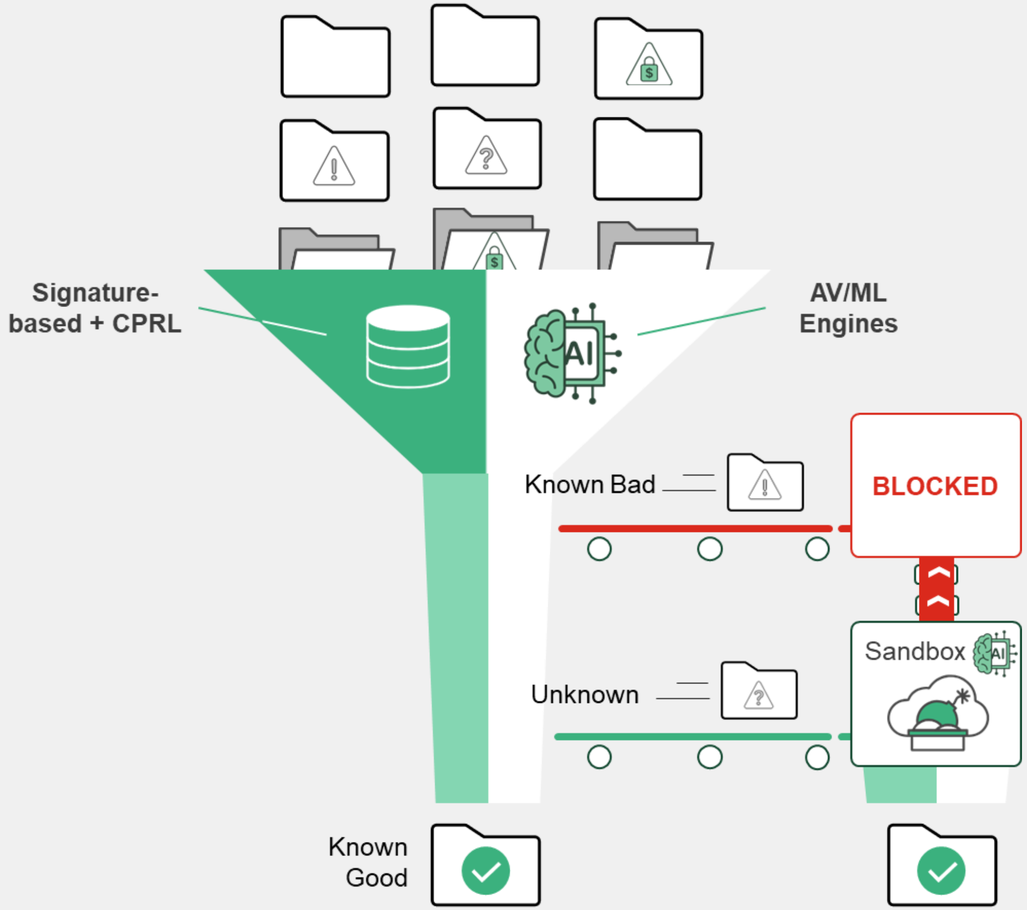
AI is embedded
into the Security Fabric



AI-Powered Threat Intelligence


Broad Coverage
Telemetry across millions of Fortinet endpoints, networks and applications
Early Detection & Response
Broad Protection
across millions of Fortinet endpoints, networks and applications
6M
Firewalls
3M
Web Gateways
20M
Emails
10M
Endpoints
5M
Sandbox
Unknown Query
AI
ML
AI / Machine Learning
Trillions
of events processed daily
Verdict
URL
IP
Network Security
Web
Emails
Endpoints
Sandbox

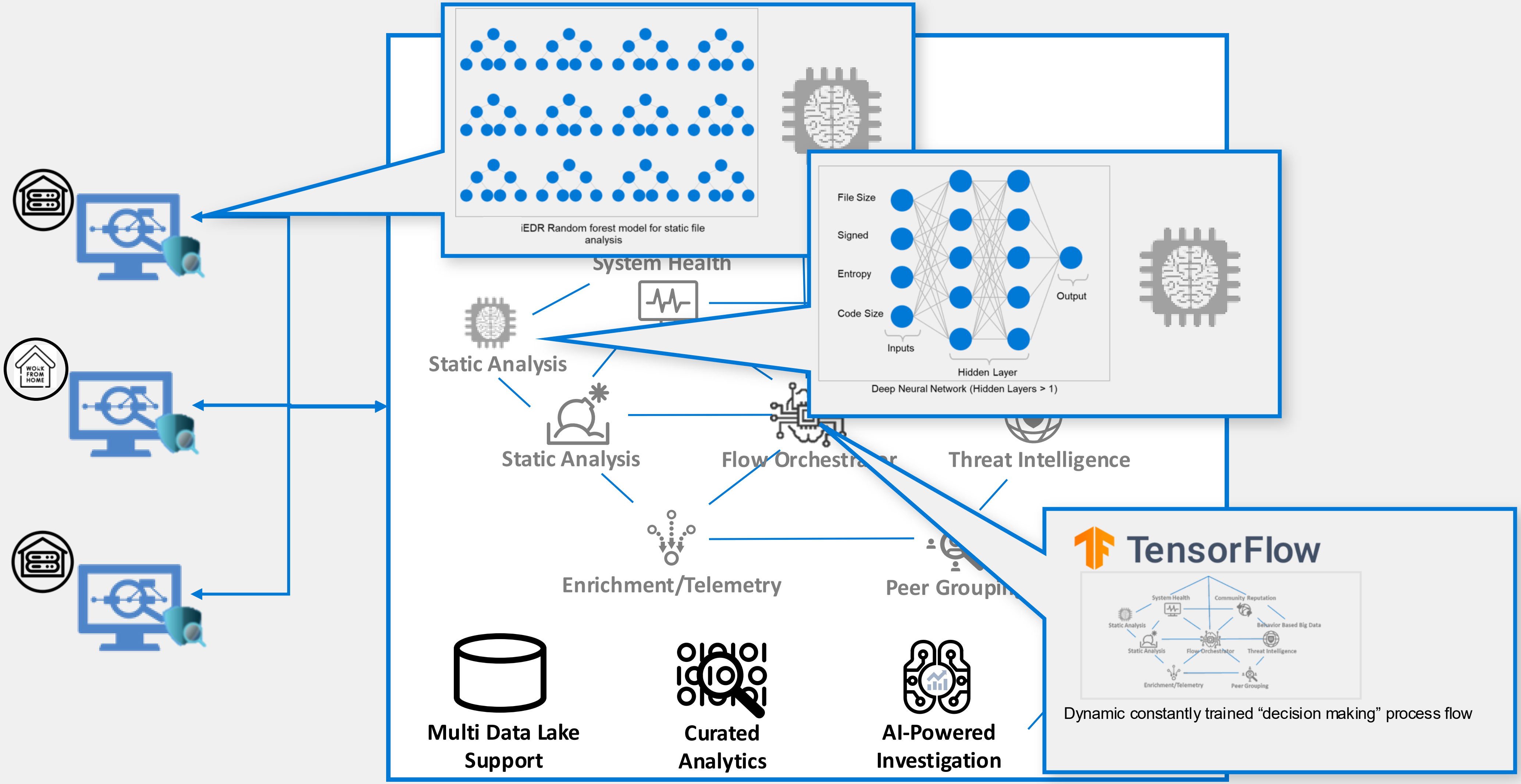
Global Intelligence Network (GIN) learns and processes Trillions events daily, make the Threat Intelligence Services



AI-enhanced capabilities as part of threat intelligence formulation

Endpoint Detection with AI

Teaching to ML NGAV to Investigate—Static File Classification



iEDR Random forest model for static file analysis

File Size
Signed
Entropy
Code Size
Inputs
Hidden Layer
Output

Deep Neural Network (Hidden Layers > 1)

System Health
Static Analysis
Static Analysis
Flow Orchestrator
Threat Intelligence
Enrichment/Telemetry
Peer Grouping

TensorFlow

System Health
Community Reputation
Static Analysis
Behavior Based Big Data
Static Analysis
Flow Orchestrator
Threat Intelligence
Enrichment/Telemetry
Peer Grouping

Dynamic constantly trained "decision making" process flow

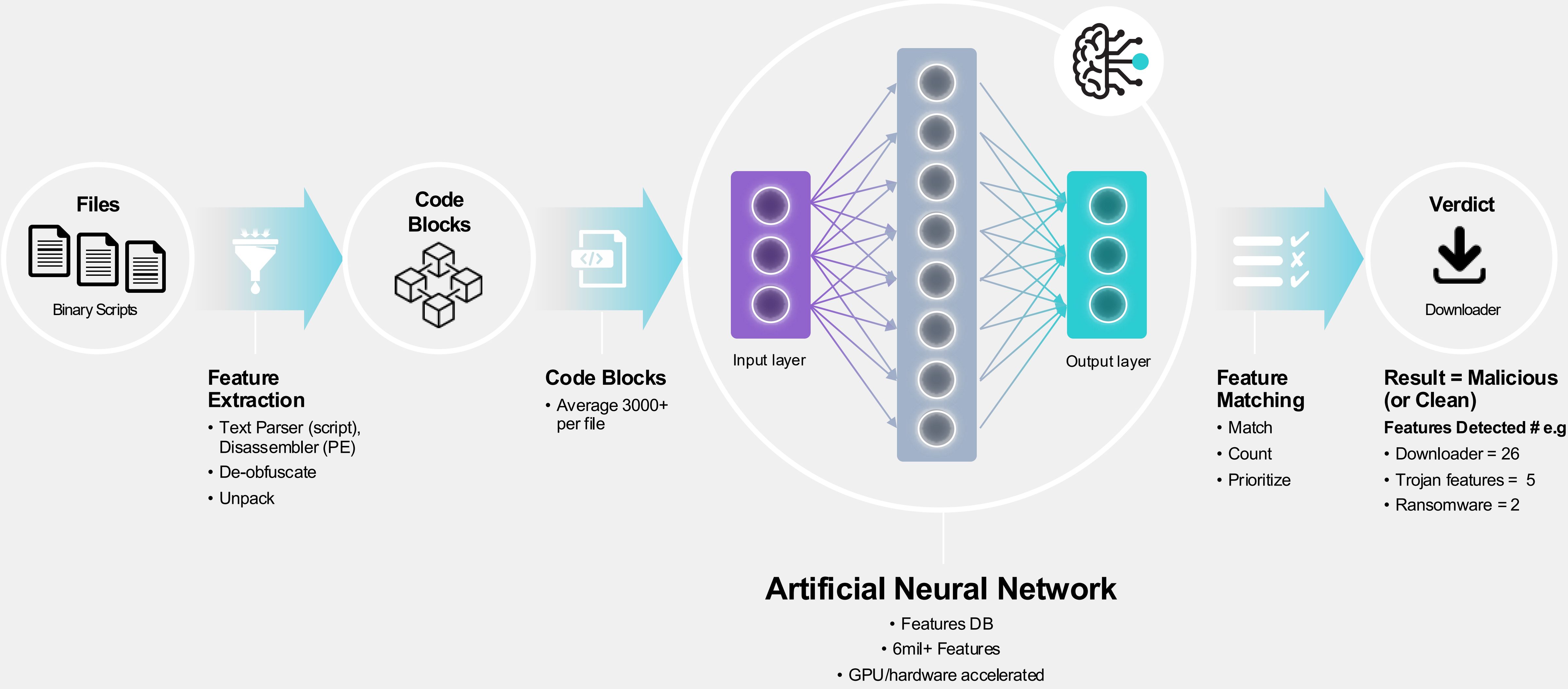
Multi Data Lake Support

Curated Analytics

AI-Powered Investigation

Network Detection with Artificial Neural Network

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



Feature Extraction

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

Code Blocks

- Average 3000+ per file

Artificial Neural Network

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

Feature Matching

- Match
- Count
- Prioritize

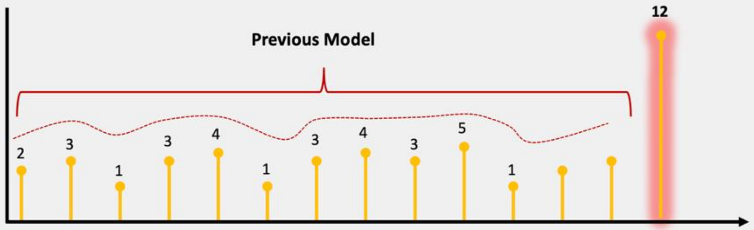
Result = Malicious (or Clean)

Features Detected # e.g.

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

UEBA with ML

Use Entity and Behavior Analytics (UEBA)



SIEM integrates broad, advanced technology for effective UEBA defence

SIEM

Integrated UEBA Capabilities

Anomaly Detection Rules

- Sudden user location change
- Sudden user login pattern change
- Sudden increase in user login volume
- Mean and Standard deviation profiling

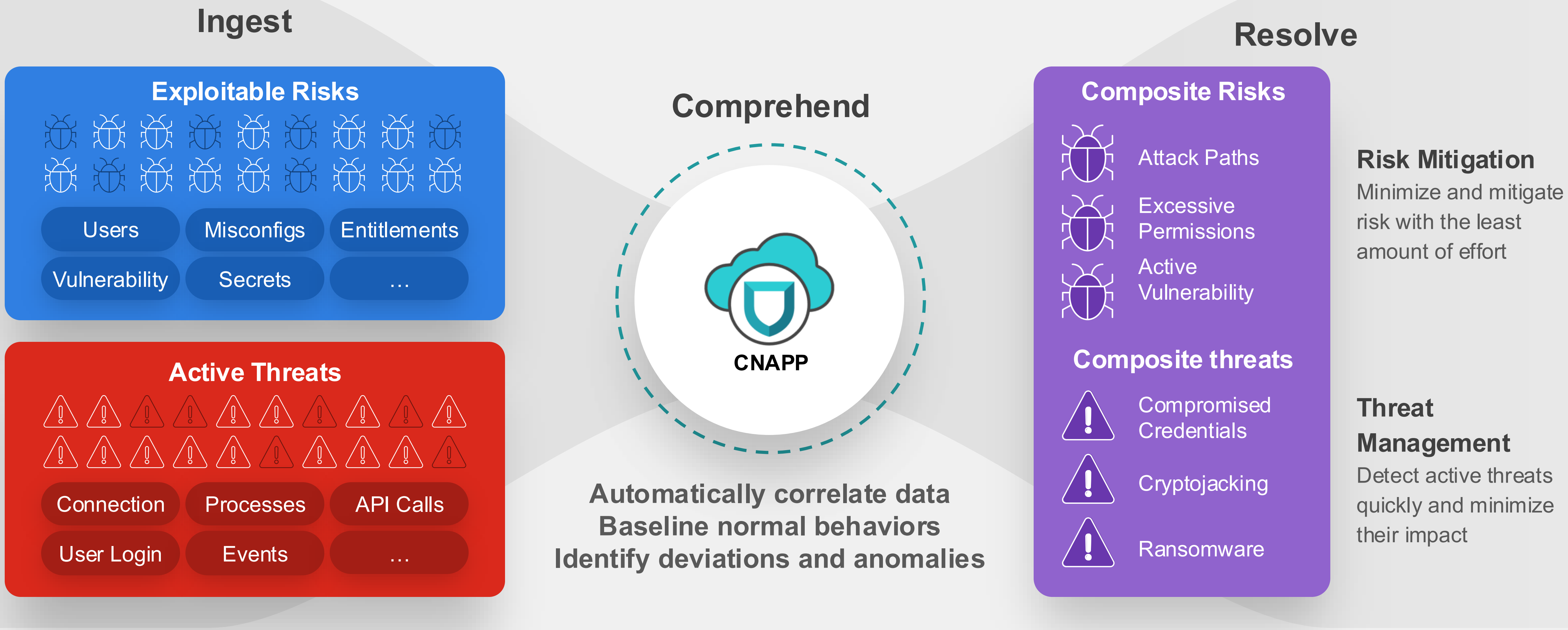
Machine Learning

- ML Framework – no code
  - Anomaly Detection
  - Classification
  - Clustering
  - Forecasting
  - Regression
- SIEM UEBA – pre-defined model
  - Rich endpoint telemetry
- User and Entity Risk Scoring

- Correlation Rules
- Baseline lists

AI Based Cloud-Native Application Protection

Single platform that understands your environment from code to cloud



Ingest

Exploitable Risks

Users | Misconfigs | Entitlements

Vulnerability | Secrets | …

Active Threats

Connection | Processes | API Calls

User Login | Events | …

Comprehend

Automatically correlate data
Baseline normal behaviors
Identify deviations and anomalies

Resolve

Composite Risks

- Attack Paths
- Excessive Permissions
- Active Vulnerability

Composite threats

- Compromised Credentials
- Cryptojacking
- Ransomware

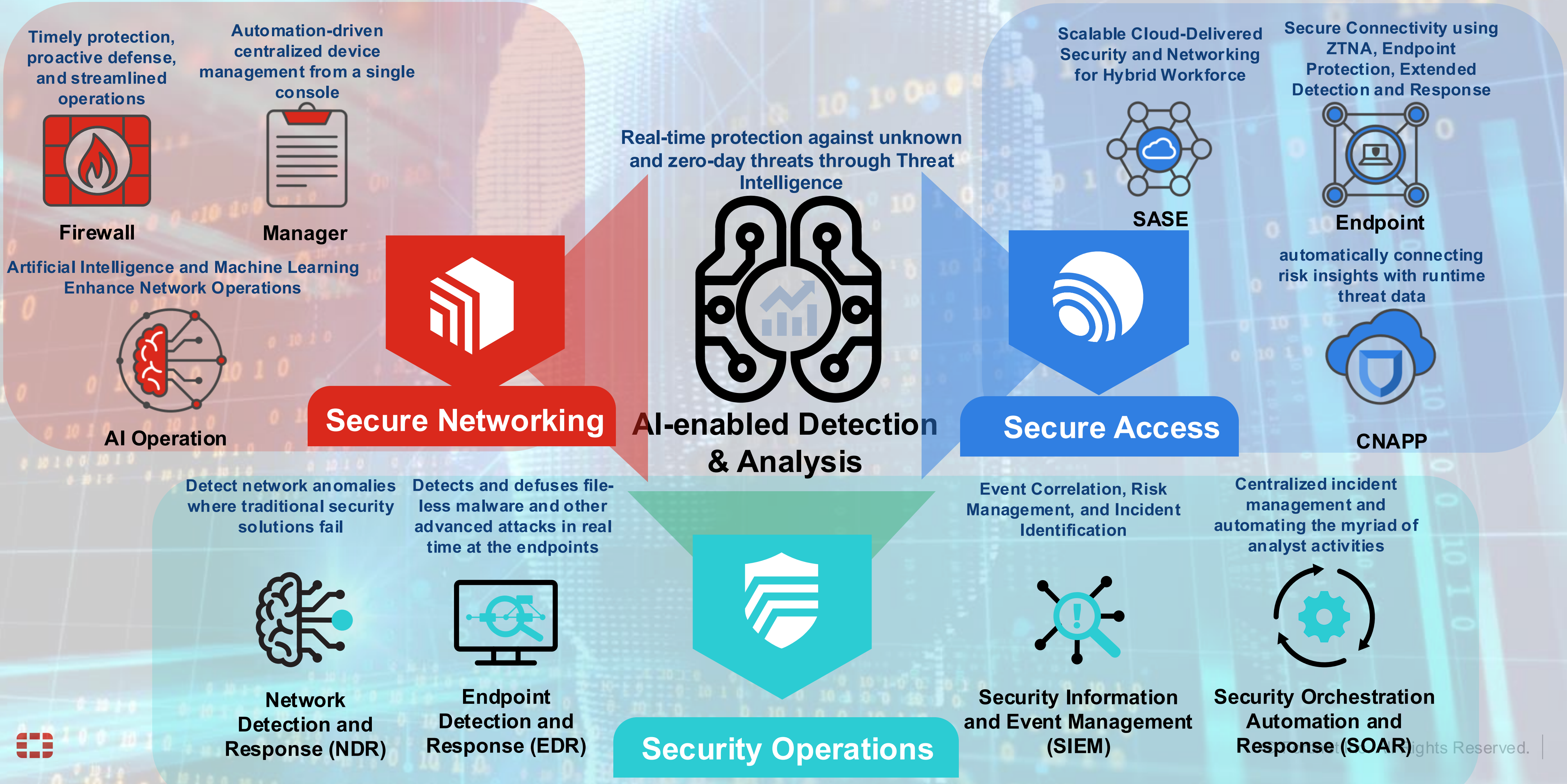
Risk Mitigation

Minimize and mitigate risk with the least amount of effort

Threat Management

Detect active threats quickly and minimize their impact

Security powered by AI



Secure Networking

Firewall

Timely protection, proactive defense, and streamlined operations

Manager

Automation-driven centralized device management from a single console

AI Operation

Artificial Intelligence and Machine Learning Enhance Network Operations

AI-enabled Detection & Analysis

Real-time protection against unknown and zero-day threats through Threat Intelligence

Secure Access

SASE

Scalable Cloud-Delivered Security and Networking for Hybrid Workforce

Endpoint

Secure Connectivity using ZTNA, Endpoint Protection, Extended Detection and Response

CNAPP

automatically connecting risk insights with runtime threat data

Security Operations

Network Detection and Response (NDR)

Detect network anomalies where traditional security solutions fail

Endpoint Detection and Response (EDR)

Detects and defuses file-less malware and other advanced attacks in real time at the endpoints

Security Information and Event Management (SIEM)

Event Correlation, Risk Management, and Incident Identification

Security Orchestration Automation and Response (SOAR)

Centralized incident management and automating the myriad of analyst activities

GenAI Augmented SecOps

OpenAI Gemini

1 Augments GenAI Intel

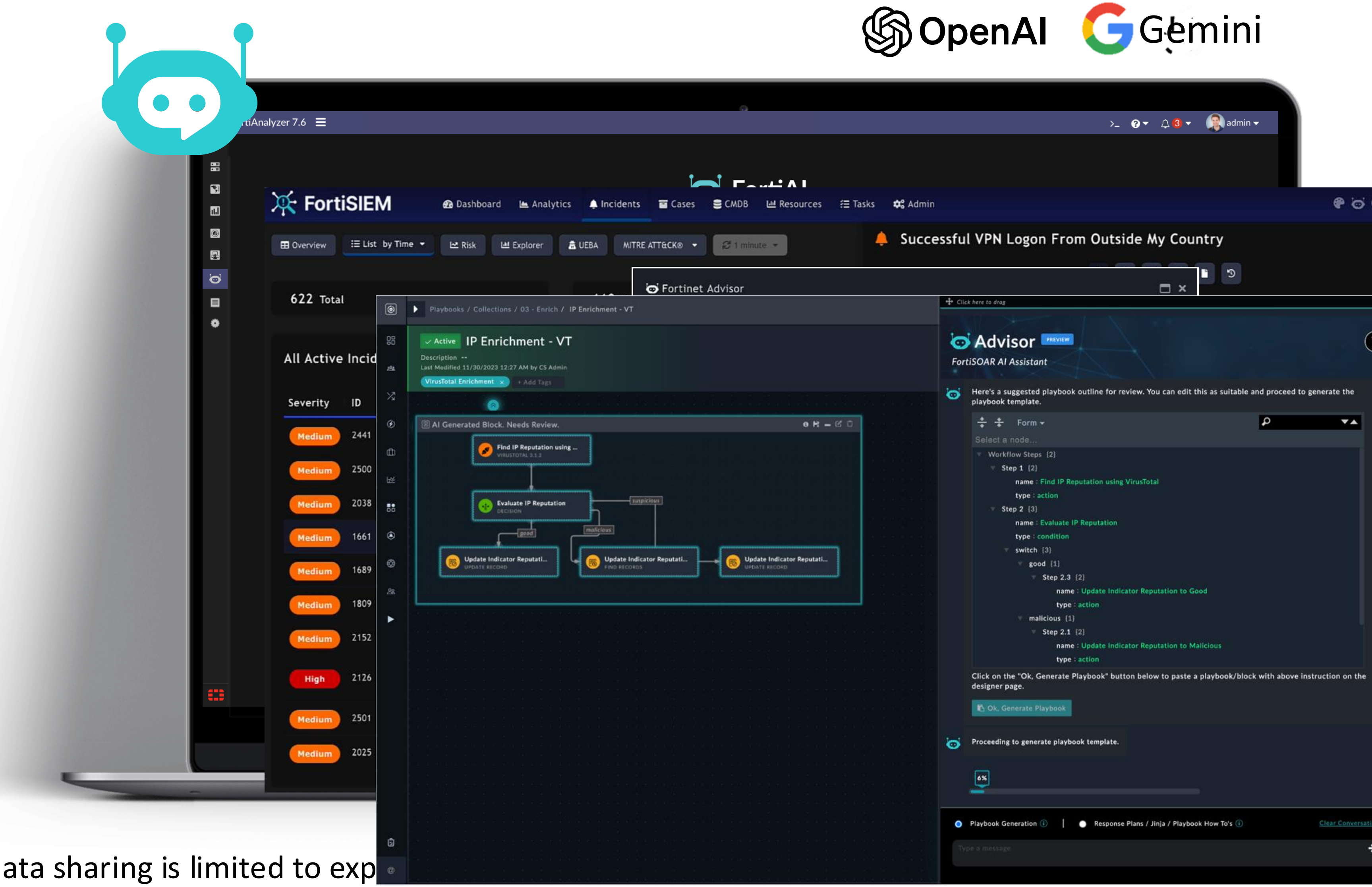
Provides DB of Vendor Threat intel, product detail, and examples to augment the AI engine

2 Transforms Queries

Adds complete query detail needed to elicit an accurate contextual AI response

3 Shapes Responses

Builds out a complete, relevant, and actionable user response



Successful VPN Logon From Outside My Country

622 Total

All Active Incid

Severity	ID
Medium	2441
Medium	2500
Medium	2038
Medium	1661
Medium	1689
Medium	1809
Medium	2152
High	2126
Medium	2501
Medium	2025

Playbooks / Collections / 03 - Enrich / IP Enrichment - VT

Active IP Enrichment - VT

Description --

Last Modified 11/30/2023 12:27 AM by CS Admin

VirusTotal Enrichment + Add Tags

AI Generated Block. Needs Review.

Here's a suggested playbook outline for review. You can edit this as suitable and proceed to generate the playbook template.

```
Workflow Steps [2]
  Step 1 [2]
    name : Find IP Reputation using VirusTotal
    type : action
  Step 2 [3]
    name : Evaluate IP Reputation
    type : condition
    switch [3]
      good [1]
        Step 2.3 [2]
          name : Update Indicator Reputation to Good
          type : action
      malicious [1]
        Step 2.1 [2]
          name : Update Indicator Reputation to Malicious
          type : action
```

Click on the "Ok, Generate Playbook" button below to paste a playbook/block with above instruction on the designer page.

Proceeding to generate playbook template.

FortiAnalyzer FortiSIEM FortiSOAR

Security & Privacy

Cloud AI engine data sharing is limited to exp
Sensitive information can be automatically masked before sharing.
GenAI Advisor does not itself share or provide access to customer data.

AI/LLM Security

Emerging Security Challenges In the AI Era

While GenAI has made remarkable progress, it also raises significant privacy and confidentiality concerns

Training Data Leak

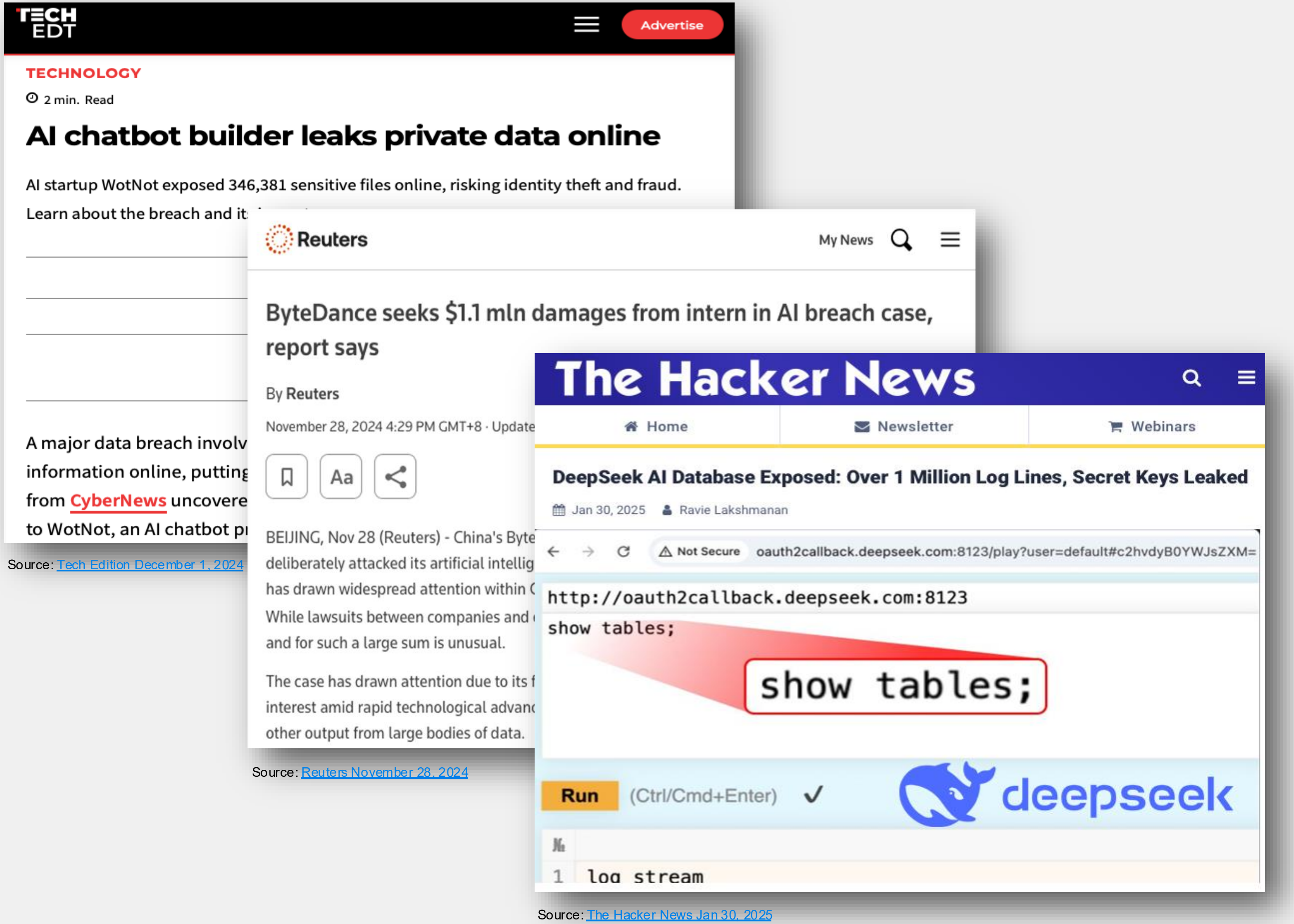
An Indian AI startup that helps businesses build custom AI chatbots has leaked almost 350,000 sensitive files after the data was left unsecured on the web.

Chat Records

Chinese AI startup DeepSeek, has publicly exposed two databases containing sensitive user and operational information.

AI Breach Surging

AI agents, with their extensive data repositories, are vulnerable to breaches. Unauthorized access or input manipulation can compromise model integrity and expose sensitive information.



TECHNOLOGY

2 min. Read

AI chatbot builder leaks private data online

AI startup WotNot exposed 346,381 sensitive files online, risking identity theft and fraud. Learn about the breach and it

A major data breach involv
information online, putting
from CyberNews uncovere
to WotNot, an AI chatbot p

ByteDance seeks $1.1 mln damages from intern in AI breach case, report says

By Reuters

November 28, 2024 4:29 PM GMT+8 · Update

BEIJING, Nov 28 (Reuters) - China's Byte
deliberately attacked its artificial intellig
has drawn widespread attention within C
While lawsuits between companies and
and for such a large sum is unusual.

The case has drawn attention due to its f
interest amid rapid technological advanc
other output from large bodies of data.

DeepSeek AI Database Exposed: Over 1 Million Log Lines, Secret Keys Leaked

Jan 30, 2025 Ravie Lakshmanan

oauth2callback.deepseek.com:8123/play?user=default#c2hvdyB0YWJsZXM=

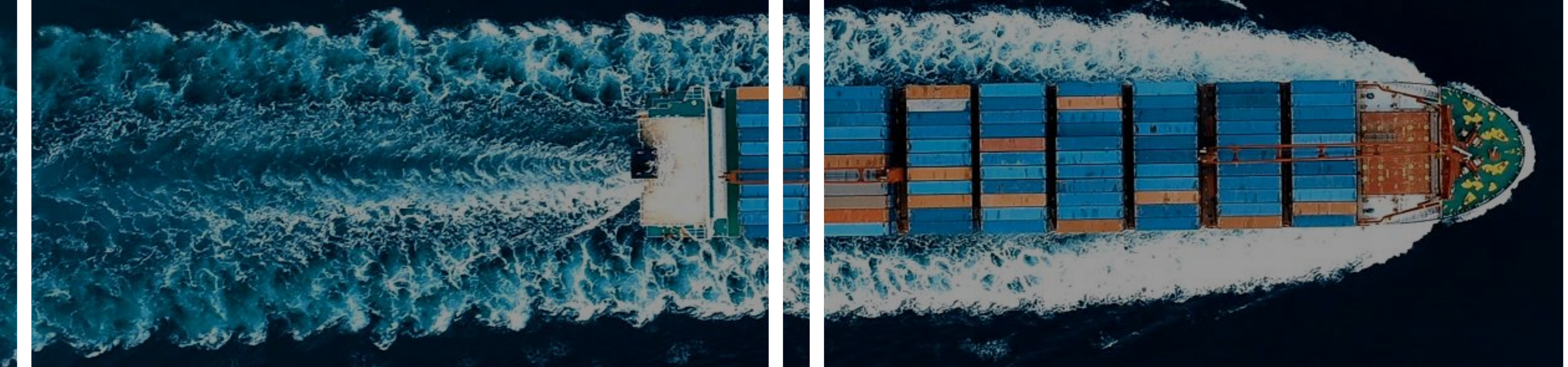
```
http://oauth2callback.deepseek.com:8123
show tables;
```

```
log_stream
```

Source: Tech Edition December 1, 2024

Source: Reuters November 28, 2024

Source: The Hacker News Jan 30, 2025



1

NIST AI RMF

The NIST AI 100 framework, officially known as the NIST Artificial Intelligence Risk Management Framework (AI RMF), was published by the NIST in January 2023. It serves as a voluntary resource designed to help organizations manage risks associated with AI systems.

2

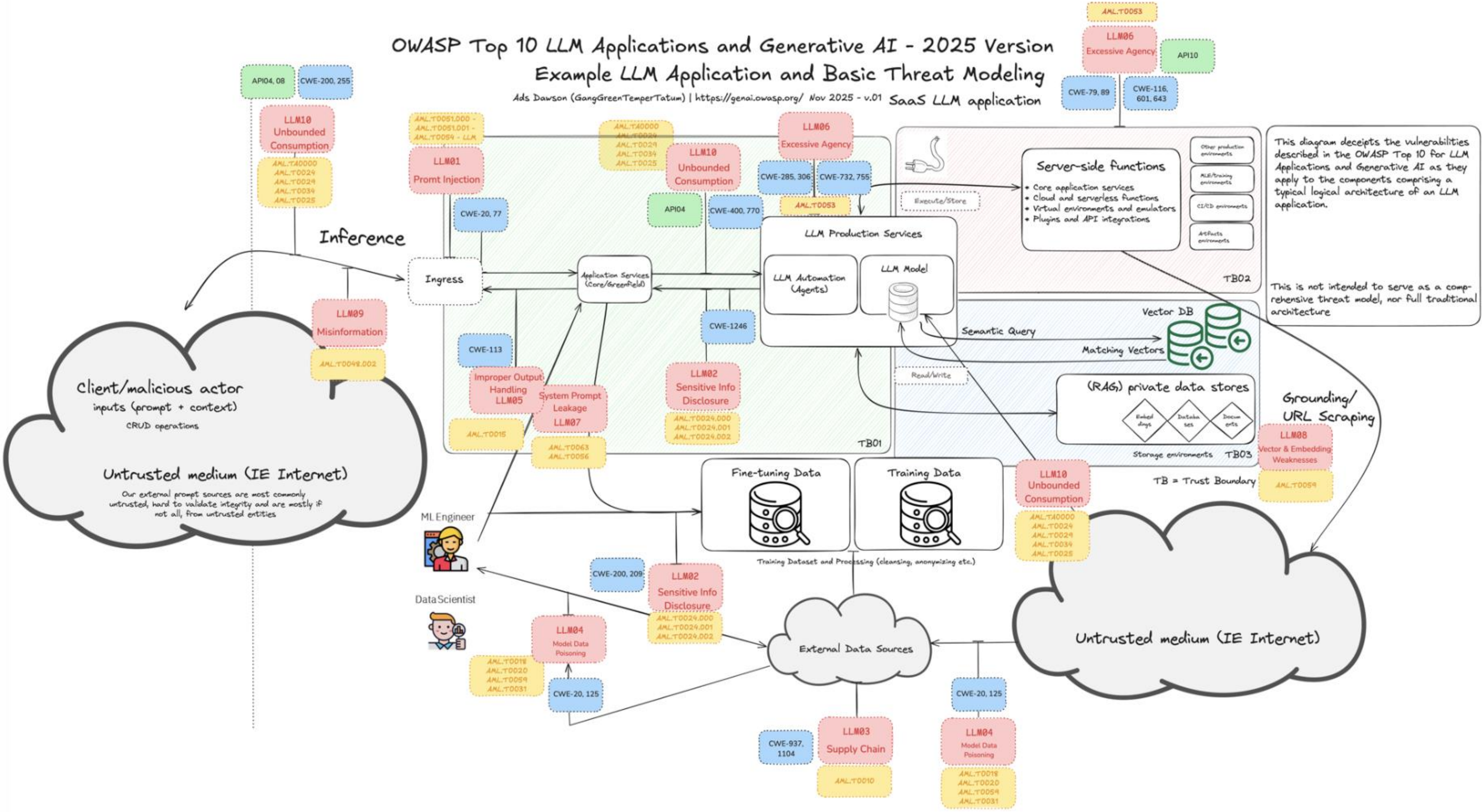
GenAI Governance Framework

Generative AI (GenAI) Governance Framework proposes a systematic and balanced approach to address the risks and ethical concerns of generative AI, by emphasizing principles like accountability, transparency, and fairness.

3

OWASP AI Exchange

The OWASP AI Exchange is an open-source collaborative project aimed at advancing the development of AI security standards and regulations. It provides a comprehensive overview of AI threats, vulnerabilities, and controls, serving as a valuable resource for professionals.



OWASP Top 10 LLM Applications and Generative AI - 2025 Version
Example LLM Application and Basic Threat Modeling

Ads Dawson (GangGreenTemperTatum) | https://genai.owasp.org/ Nov 2025 - v.01

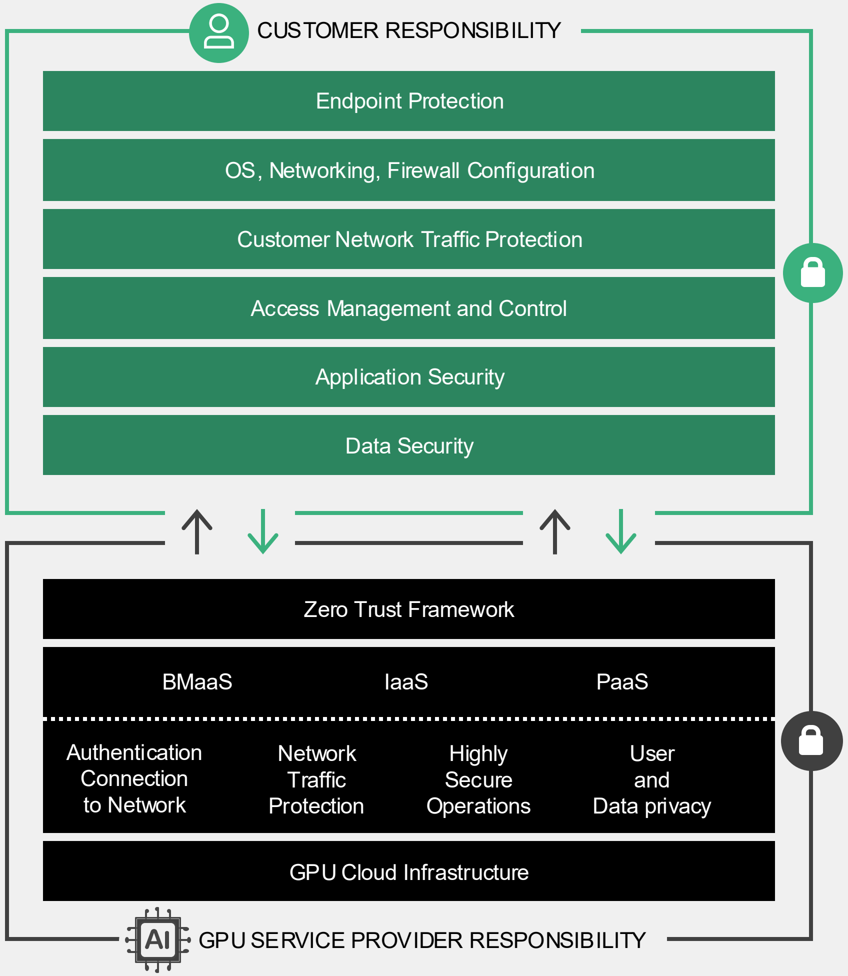
SaaS LLM application

This diagram deceipts the vulnerabilities described in the OWASP Top 10 for LLM Applications and Generative AI as they apply to the components comprising a typical logical architecture of an LLM application.

This is not intended to serve as a comprehensive threat model, nor full traditional architecture

AI Cloud Infrastructure and Shared Responsibility

Challenges

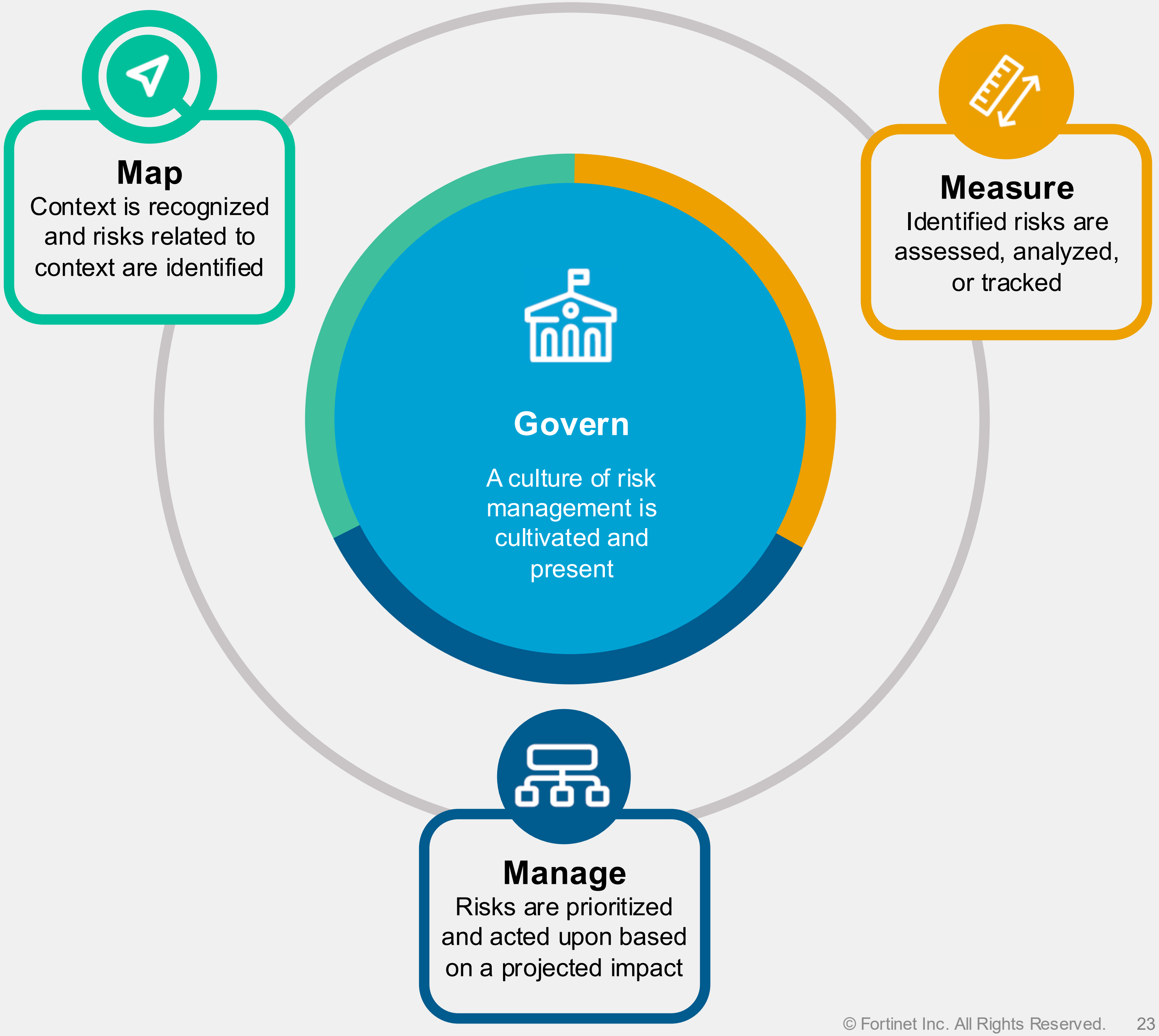

CUSTOMER RESPONSIBILITY
Endpoint Protection
OS, Networking, Firewall Configuration
Customer Network Traffic Protection
Access Management and Control
Application Security
Data Security
Zero Trust Framework
BMaaS
IaaS
PaaS
Authentication Connection to Network
Network Traffic Protection
Highly Secure Operations
User and Data privacy
GPU Cloud Infrastructure
AI
GPU SERVICE PROVIDER RESPONSIBILITY

- **Security become increasingly complex**: Security is becoming more and more complex as artificial intelligence (AI), 5G, cloud, the Internet of Things (IoT) and other disruptive technologies broaden the threat landscape — while regulations call for ever more stringent security measures
- **GPU infra built-in security features**: Alone is not enough to handle all business security needs and enterprise must take responsibility for covering many aspects of security
- **Security skills gap**: Some enterprises may not have the skills in-house to keep up with the everchanging security field
- **Shared security model**: Enables enterprises to shift some security functions to the GPU service provider to heighten enterprise security
- **Managed security service**: GPU service providers can deliver security value-added services that can help and drive GPU service adoption and revenue

NIST AI RMF Core

NIST

Functions organize AI risk management activities at their highest level to govern, map, measure, and manage AI risks. Governance is designed to be a cross-cutting function to inform and be infused throughout the other three functions.



Map
Context is recognized and risks related to context are identified

Measure
Identified risks are assessed, analyzed, or tracked

Govern
A culture of risk management is cultivated and present

Manage
Risks are prioritized and acted upon based on a projected impact

Elements of the NIST AI RMF

GOVERN

GOVERN 1
Policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks are in place, transparent, and implemented effectively.

GOVERN 2
Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks.

GOVERN 3
Workforce diversity, equity, inclusion, and accessibility processes are prioritized in the mapping, measuring, and managing of AI risks throughout the lifecycle.

GOVERN 4
Organizational teams are committed to a culture that considers and communicates AI risk.

GOVERN 5
Processes are in place for robust engagement with relevant AI actors.

GOVERN 6
Policies and procedures are in place to address AI risks and benefits arising from third-party software and data and other supply chain issues.

MAP

MAP 1
Context is established and understood.

MAP 2
Categorization of the AI system is performed.

MAP 3
AI capabilities, targeted usage, goals, and expected benefits and costs compared with appropriate benchmarks are understood.

MAP 4
Risks and benefits are mapped for all components of the AI system including third-party software and data.

MAP 5
Impacts to individuals, groups, communities, organizations, and society are characterized.

MEASURE

MEASURE 1
Appropriate methods and metrics are identified and applied..

MEASURE 2
AI systems are evaluated for Trustworthy characteristics.

MEASURE 3
Mechanisms for tracking identified AI risks over time are in place.

MEASURE 4
Feedback about efficacy of measurement is gathered and assessed.

MANAGE

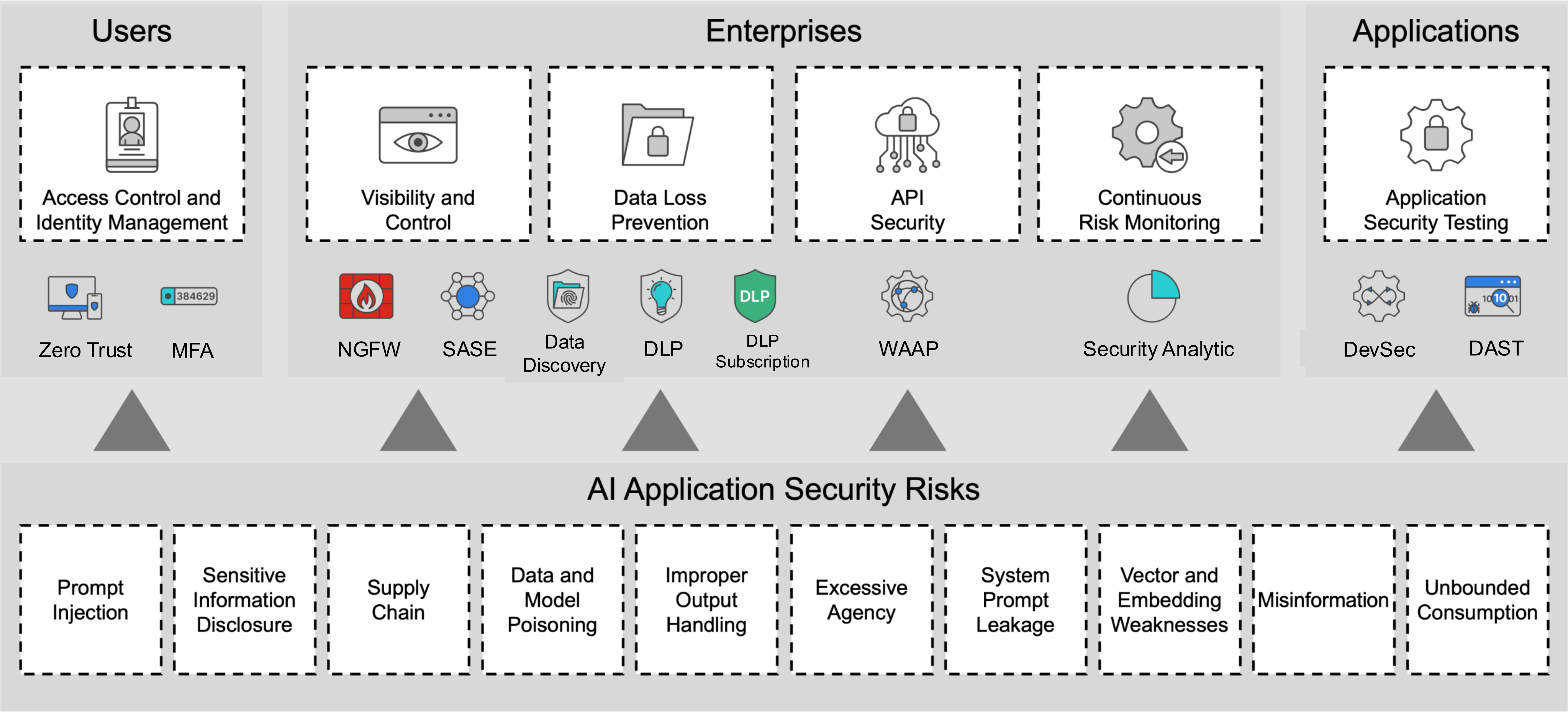
MANAGE 1
AI risks based on assessments and other analytical output from the MAP and MEASURE functions are prioritized, responded to, and managed.

MANAGE 2
Strategies to maximize AI benefits and minimize negative impacts are planned, prepared, implemented, documented, and informed by input from relevant AI actors.

MANAGE 3
AI risks and benefits from third-party entities are managed.

MANAGE 4
Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks are documented and monitored regularly.

Security for AI Applications and AI Cloud Infrastructure



Users

- Access Control and Identity Management
- Zero Trust
- MFA

Enterprises

- Visibility and Control
- Data Loss Prevention
- API Security
- Continuous Risk Monitoring
- NGFW
- SASE
- Data Discovery
- DLP
- DLP Subscription
- WAAP
- Security Analytic

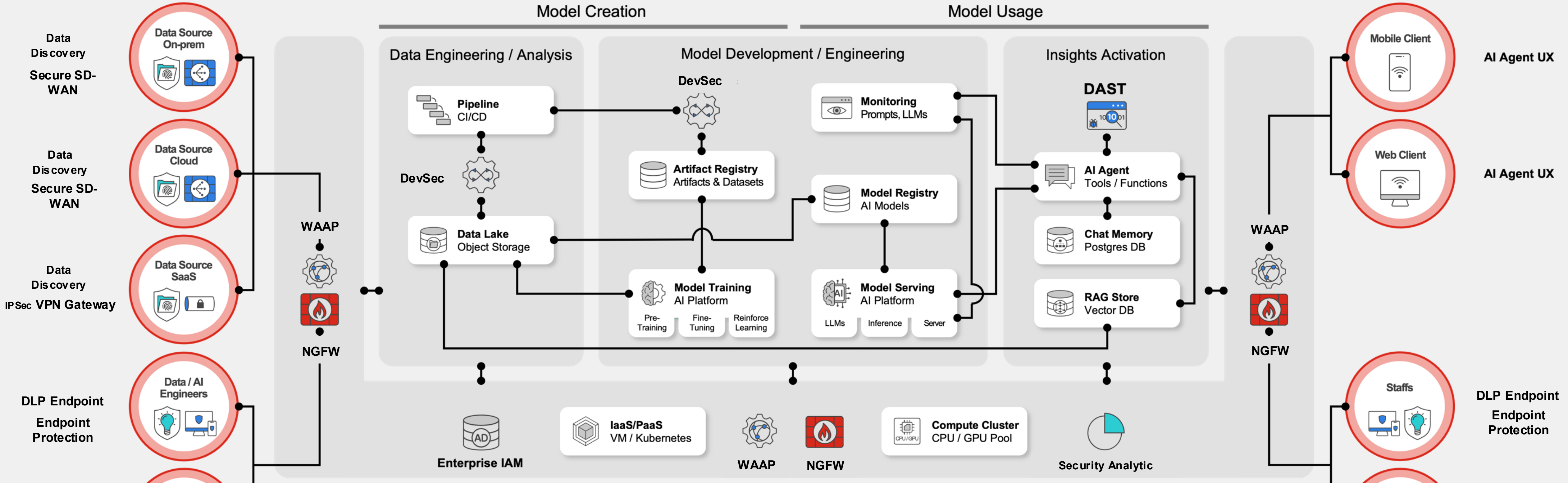
Applications

- Application Security Testing
- DevSec
- DAST

AI Application Security Risks

- Prompt Injection
- Sensitive Information Disclosure
- Supply Chain
- Data and Model Poisoning
- Improper Output Handling
- Excessive Agency
- System Prompt Leakage
- Vector and Embedding Weaknesses
- Misinformation
- Unbounded Consumption

Securing Critical Workloads and AI Data Center



Model Creation

Model Usage

Data Discovery

Secure SD-WAN

Data Source On-prem

Data Discovery

Secure SD-WAN

Data Source Cloud

Data Discovery

IPSec VPN Gateway

Data Source SaaS

DLP Endpoint

Endpoint Protection

Data / AI Engineers

DLP Endpoint

Endpoint Protection

DevOps / AppDevs

WAAP

NGFW

Data Engineering / Analysis

Pipeline CI/CD

DevSec

Data Lake Object Storage

Model Development / Engineering

DevSec

Artifact Registry Artifacts & Datasets

Model Training AI Platform

Pre-Training

Fine-Tuning

Reinforce Learning

Monitoring Prompts, LLMs

Model Registry AI Models

Model Serving AI Platform

LLMs

Inference

Server

Insights Activation

DAST

AI Agent Tools / Functions

Chat Memory Postgres DB

RAG Store Vector DB

WAAP

NGFW

Mobile Client

AI Agent UX

Web Client

AI Agent UX

Staffs

DLP Endpoint

Endpoint Protection

Contractors

DLP Point

Endpoint Protection

Enterprise IAM

IaaS/PaaS VM / Kubernetes

WAAP

NGFW

Compute Cluster CPU / GPU Pool

Security Analytic

Perimeter Firewall
- Protect against break-ins
- North-south visibility

Segmentation Firewall
- Prevent lateral movement
- East-west visibility

ZTNA Firewall
- Zero trust access
- Multi-factor authentication

IPsec VPN Gateway
- Data integrity and encryption
- Data source validation

Application Firewall
- Prompt security
- Secure API access

AMP **Anti-Malware Protection**
- Model integrity validation
- Detect & block malicious files or scripts

IPS **Intrusion Prevention**
- Adversarial attack protection
- Identify and block threats

DLP **Data In Motion Protection**
- User & data privacy protections
- Network data protection

Data In Use Protection
- User & data privacy protections
- Endpoint data protection

Data At Rest Protection
- User & data privacy protections
- Discovery, classify and label data

Security Monitoring
- Security alerting
- User activity monitoring

Incident Response
- Incident detection and response
- Security posture management

SAST
- Scans application source code
- Static or source code testing

DAST
- Scans OWASP Top10 & other vuln.
- Dynamic testing

SCA/OSS
- Scans third-party libraries
- Software supply chain security

Vuln Management
- Vulnerability assessment
- Penetration testing

About Fortinet

Leader in the Use of AI Technologies in Cybersecurity

FORTINET

Securing people, devices, and data everywhere.

Broad, Integrated Portfolio of

~60

Enterprise Cybersecurity Products

Global Customer Base

830,000+

10+

Years experience in AI/ML

6th

Generation of Machine Learning

528

AI Patents (approved and pending)

100

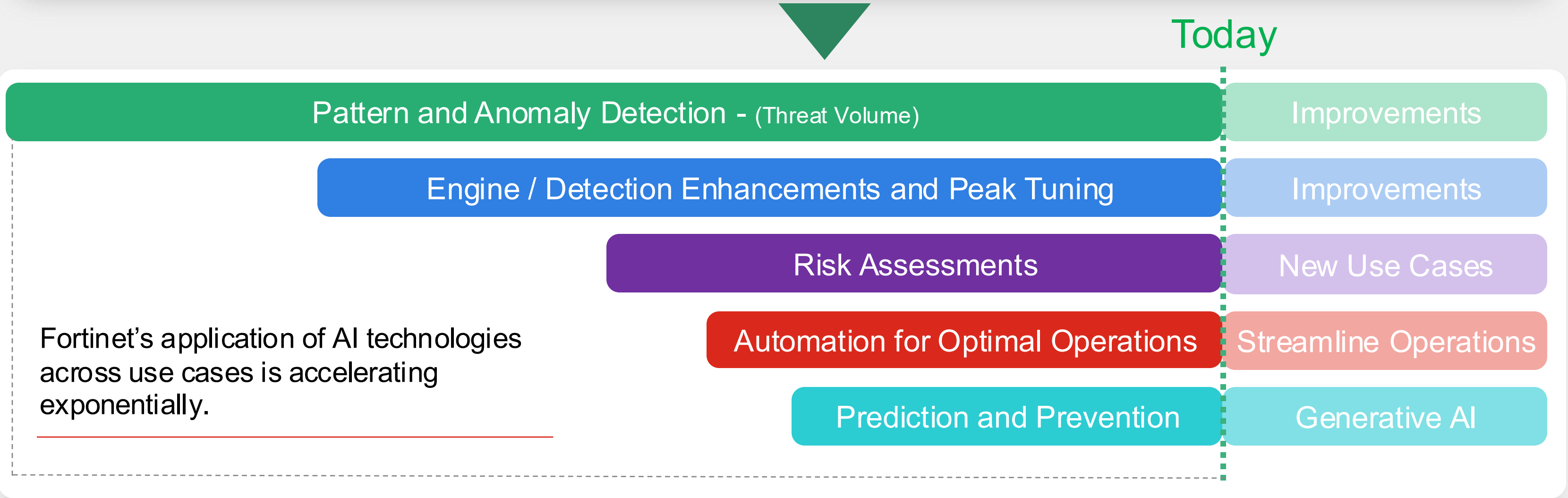
Documented applications of AI to-Date

8

Number of Security Domains Utilizing AI

42

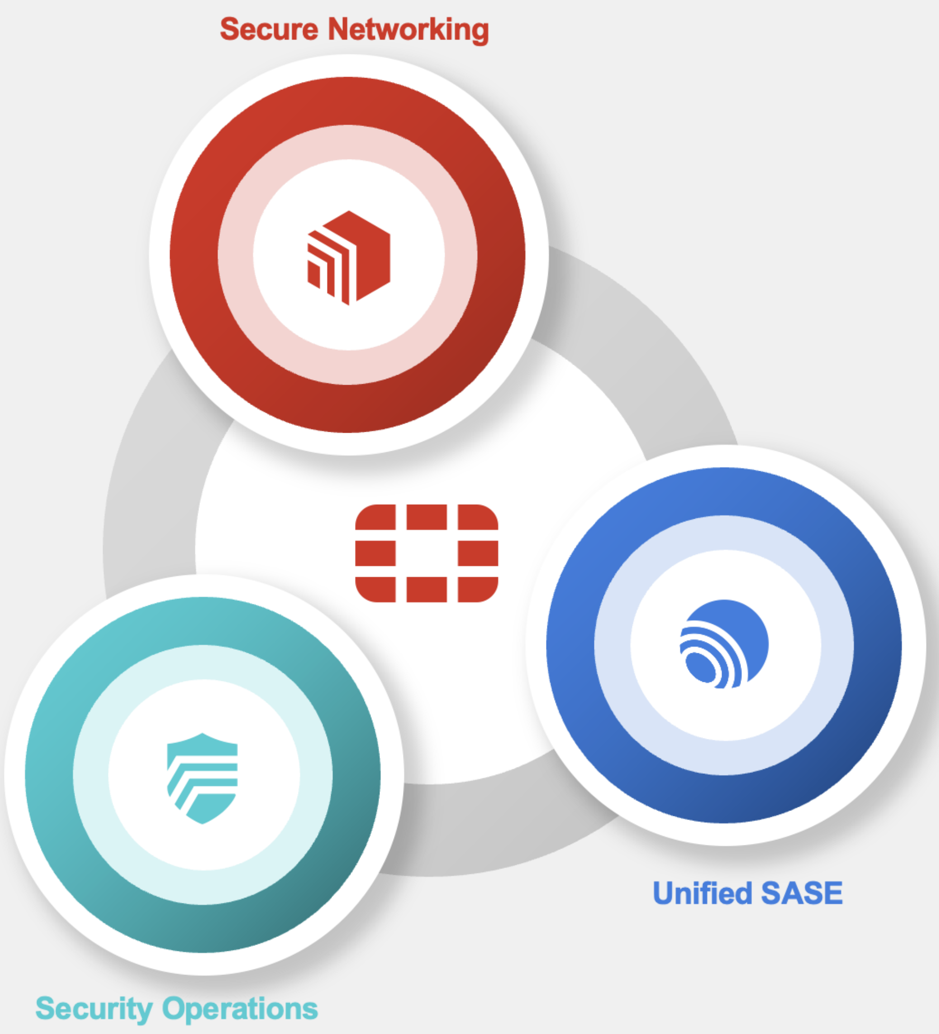
Number of solutions driven by AI today



Today
Pattern and Anomaly Detection - (Threat Volume)
Improvements
Engine / Detection Enhancements and Peak Tuning
Improvements
Risk Assessments
New Use Cases
Automation for Optimal Operations
Streamline Operations
Prediction and Prevention
Generative AI

Fortinet's application of AI technologies across use cases is accelerating exponentially.

#1 in Cybersecurity Solutions (~60 solutions)



#1 Most Trusted Security Company in the World

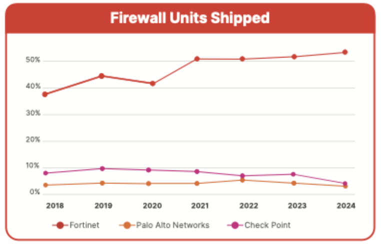
#1 in Enterprise

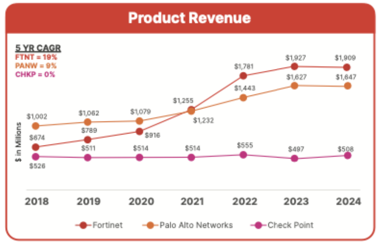
80% of Fortune 100 and 72% of Global 2000 depend on Fortinet to stay secure.

TOP 10/10 Business Services	TOP 10/10 Financial Services	TOP 8/10 Healthcare & Life Sciences	TOP 10/10 Manufacturing	TOP 10/10 Retail & Wholesale	TOP 10/10 Technology	TOP 10/10 Telcos & Carriers

#1 in Network Security

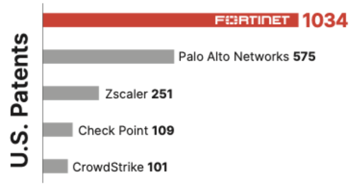
"Fortinet is the #1 vendor for firewall shipments globally with more than 50% share." *–650 Group*





#1 in Innovation

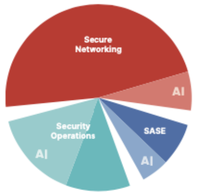
2x more patents than comparable cybersecurity companies.



Source: U.S. Patent Office, as of Dec 31, 2024

1,378
Global Patents

1,034 U.S. Patents
344 International Patents
451 Pending Patents



528 AI Patents
Issued and Pending

#1 Most Trusted U.S.-Based Cybersecurity Company

Forbes
MOST TRUSTED COMPANIES
IN AMERICA
2025

Fortinet is the only cybersecurity company in the Top 50, ranked #7 in the Forbes Most Trusted Companies 2025 list.

#1 in Product Energy-Efficiency

Product environmental impacts are central to our sustainability approach.

Third Consecutive Year

Member of the Dow Jones Best-in-Class World and North America indices

Pledge to Reach Net Zero

By 2030 across scopes 1 and 2 emissions from Fortinet's owned facilities worldwide.

Lead in Energy-Efficiency

88% less power consumption over industry-standard CPU

62% average reduction on product energy consumption[1]

[1] Based on new models of 2022 FortiGate F series (compared to equivalent models from previous generation).

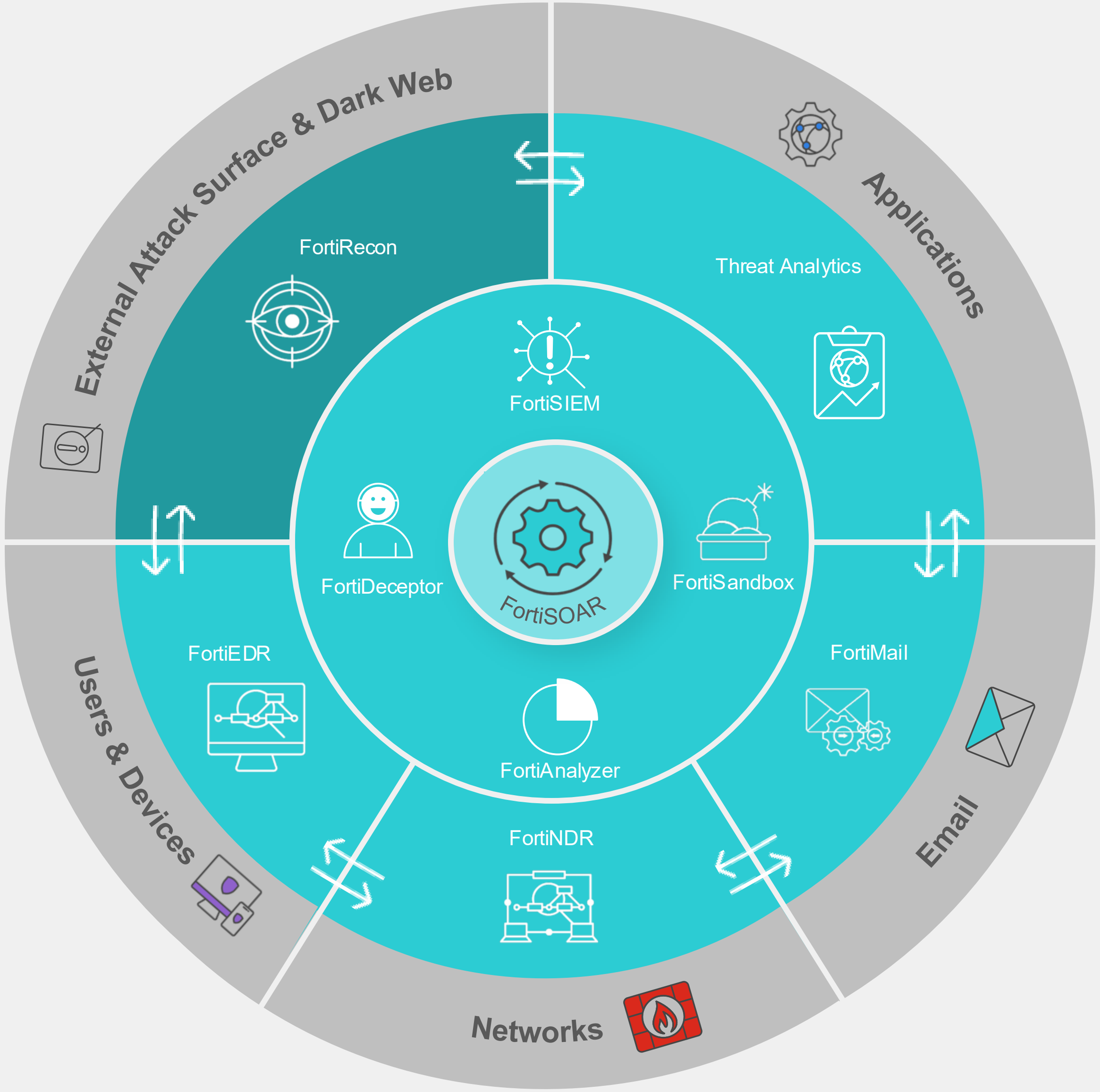
Fortinet AI Security Fabric Portfolio

A cybersecurity platform- built on AI and Automation- to accelerate time to detect and respond to cyber intrusion

AI Security Platform

CONSOLIDATE

Consolidated security operations platform to accelerate time to detect and respond.



AI Across the Attack Surface

Monitor a specific domain, or across domains, to detect intrusion

Fabric-native Integration

Interoperate beyond industry norm, to detect *and disrupt*

Centralized analytics and response

Orchestrate, automate and/or augment operations

Dr. Rattipong Putthacharoen
rputthacharoe@fortinet.com