FORTINET

FortiAI 2.0:
AI-Driven Security Redefined

Unmatched Innovation, Smarter Security

e-government 20:10 Mikulov 2.9.2025

Q3 2025

One of the largest and most trusted cybersecurity companies in the world.

2000:
Redefining Network Security
Proprietary ASIC and OS to accelerate network security functions

2016:
Leading the Convergence of Networking and Security
Introducing the Fortinet Security Fabric. Broad. Integrated. Automated.

2023:
Revolutionizing Security Fabric with Investment in Global Cloud Network
Long-term investments into key technologies to extend the power of the security fabric

- ***Headquarters**:* Sunnyvale, CA
- ***Listed in both**:* NASDAQ 100 and S&P 500 Indices
- ***Member of*** 2023 Dow Jones Sustainability World and North America Indices

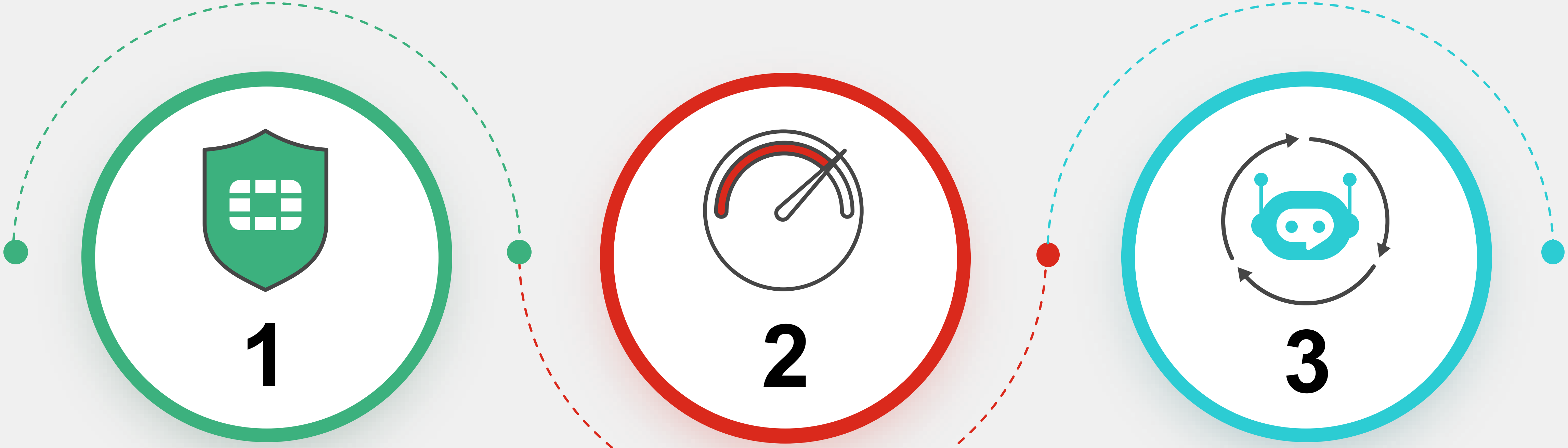
Global Customer Base
890K+
Lifetime Customers

2024 Billings
$6.53B+
(as of Dec. 31, 2024)

Market Capitalization
$80.9B
(as of June 30, 2025)

Employees Worldwide
14,800+
(as of June 30, 2025)

25 Year Mission – Cybersecurity Without Compromise



Best of Breed
Cyber Research & Protection

Best of Breed
Performance

Best of Breed
Automation
(including AI)

AI Opportunities & Challenges

The Rise of AI and GenAI: Unlocking Opportunities and Navigating Cybersecurity Risks

80%

of enterprises will adopt AI-augmented SOC tools by 2025 to combat AI-driven threats.

IDC, RSAC 2025 AI in Cybersecurity panels

30%

of cyberattacks will involve AI-generated deepfakes or adversarial AI, up from less than 2% in 2022.

Gartner, RSAC 2025 sessions on AI threats

45%

of organizations using third-party AI models have experienced a security incident due to unvetted AI dependencies.

RSAC 2025 Supply Chain Risk Sessions

How to Securely Use AI

AI & Security: Better Together

Visibility & control of **AI Usage**
Protect against **AI Threats**

Real-time, autonomous defense with **AI Intelligence**

Secure **AI Infrastructure** and **Supply Chain**

FortiAI: AI-Powered Security and Transformation

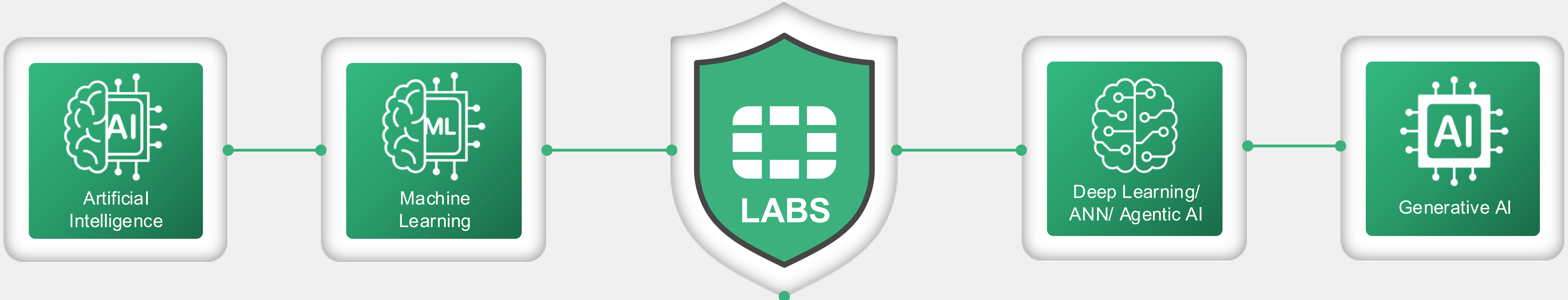
-- Portfolio --
Embedded
Interconnected
Automated

FortiAI-Protect
Protect against AI Threats

FortiAI-Assist
AI assisted operations

FortiAI-SecureAI
Secure LLM, AI systems

Our AI Journey Started with FortiGuard Labs



15+

Years Experience in AI/ML

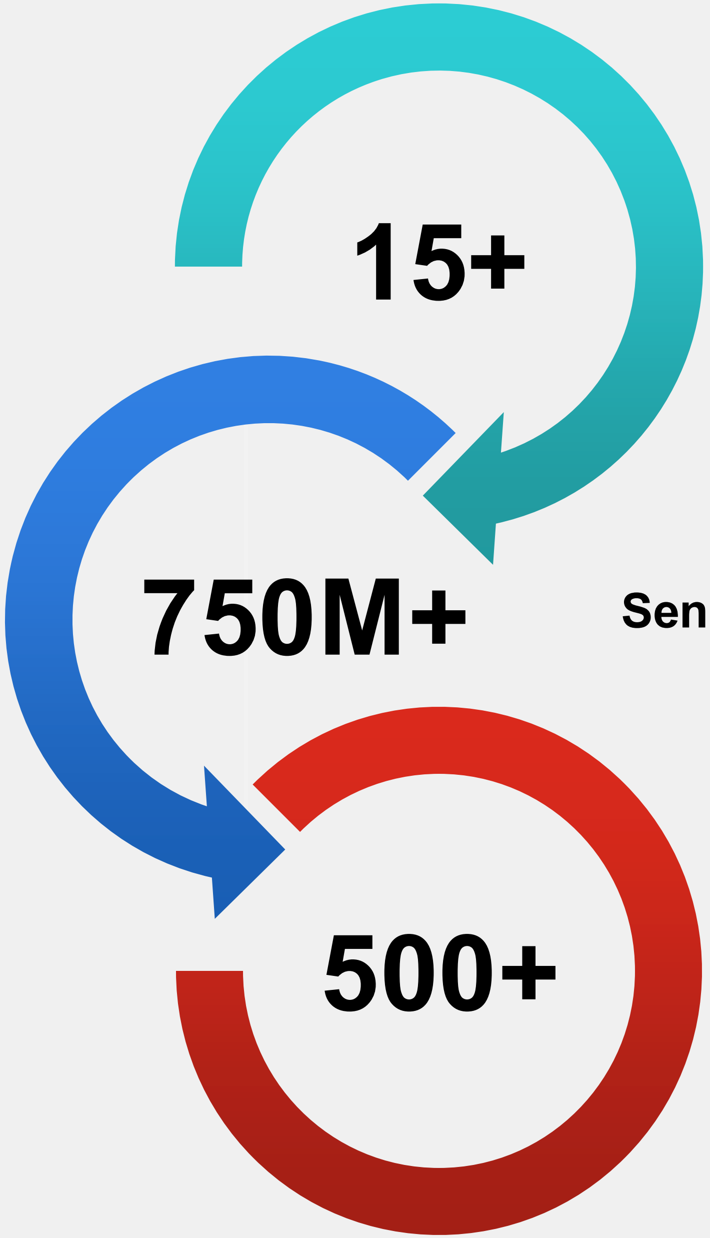
6th

Generation of Machine Learning

500+

AI Patents (awarded & pending)

Embedded and Empowering Fortinet Security Fabric



15+ **Years Experience in AI/ML**

750M+ **Sensors**

500+ **AI Patents** (awarded & pending)

FortiAI-Protect: Protecting the Attack Surface in Real-Time

AI Threat Protection

Utilizing Advanced AI analysis and threat intelligence to protect against broad spectrum of new and evasive threats and intrusions.

DLP IPS LABS

AI App Detection & Protection

Control unauthorized AI (shadow AI) use including GenAI use to reduce security and compliance risks

URL

Prioritize & Reduce Risks

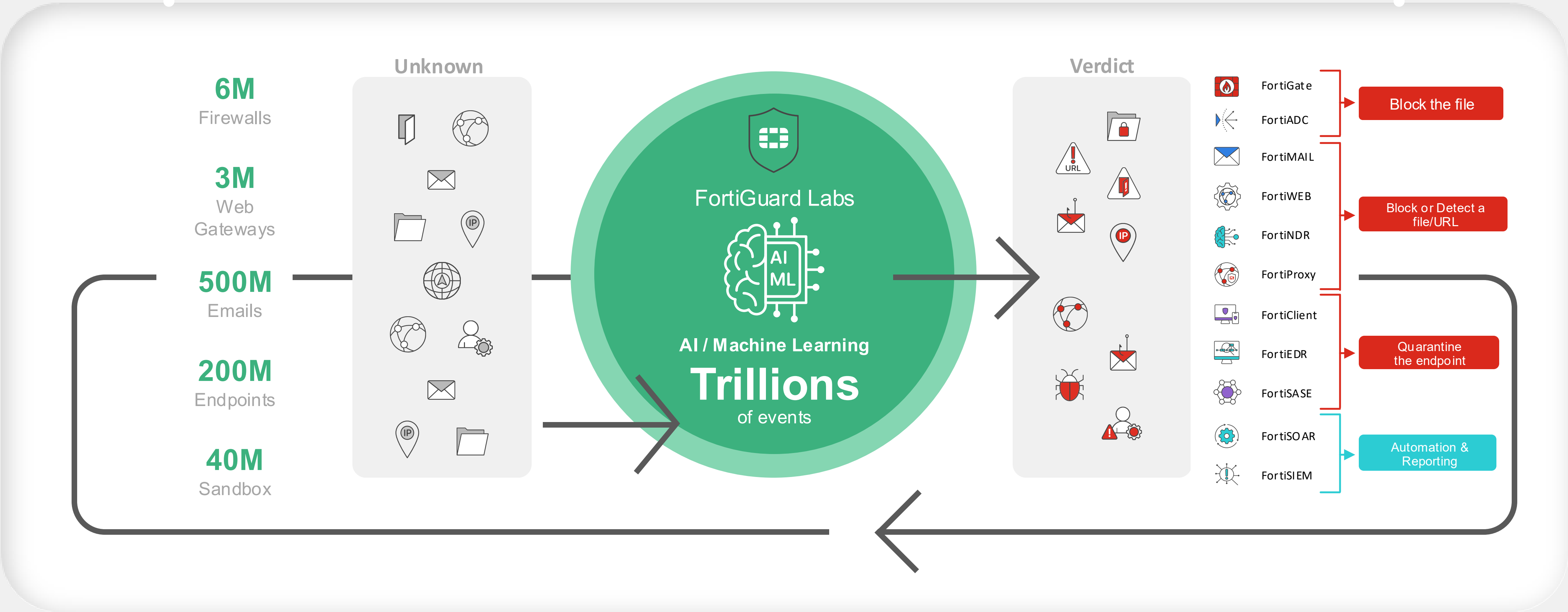
Prioritize critical threat responses with contextual risk assessment, enhanced accuracy reducing false positives to near-zero.

The Breadth & Scale of FortiGuard AI-Powered Security Services

Broad coverage
Telemetry from millions of Fortinet endpoints, networks, and applications

Early detection & response

Broad protection
across Fortinet Security Fabric



6M Firewalls

3M Web Gateways

500M Emails

200M Endpoints

40M Sandbox

Unknown

FortiGuard Labs

AI / Machine Learning

Trillions of events

Verdict

FortiGate
FortiADC

Block the file

FortiMAIL
FortiWEB
FortiNDR
FortiProxy

Block or Detect a file/URL

FortiClient
FortiEDR
FortiSASE

Quarantine the endpoint

FortiSOAR
FortiSIEM

Automation & Reporting

FortiAI-Assist

Proactive, automated
NOC and SOC

Incident Response Optimization

LAN, SD-WAN Optimization

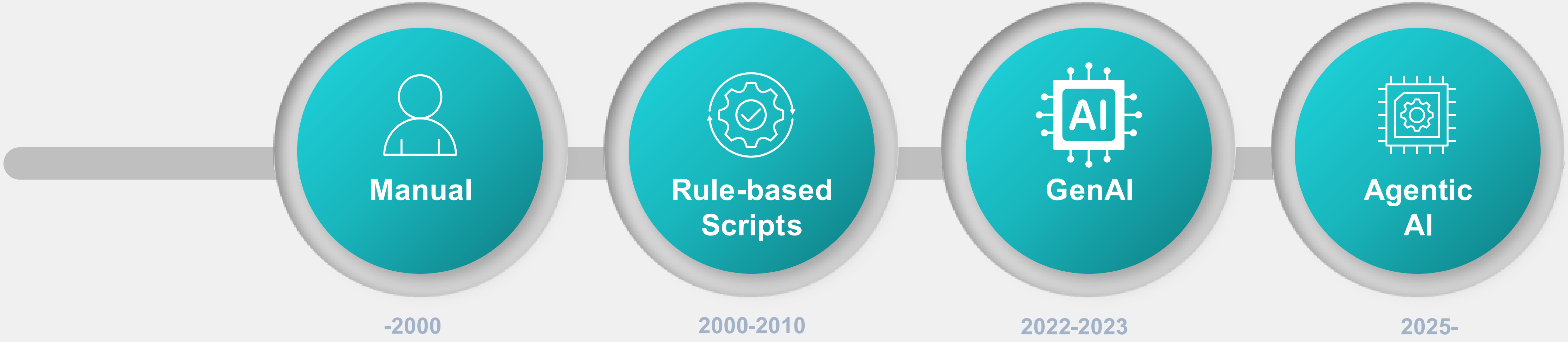
Automated Alert Triage

Policy Creation

Auto Configuration

Threat Hunting

Know Where Your Customers Are in Their AI Journeys



Speed (MTTR)	Slow (hours)	Medium (mins)	Fast (secs)	Instant (ms)
Scalability	Low	Medium	High	Very High
Adaptability	High	Low	Medium	High
Autonomy	None	Partial	Advisory	Full

GenAI and Agentic AI are Reshaping NOC and SOC

Gartner 2025 AI Projections

Chatbots

70%

SOC teams will deploy AI-powered ‘co-pilots’ to combat analyst burnout

AIOps

30%

Through autonomously resolving tickets, AI-driven NOCs will cut operational costs by 30%

GenAI

40%

of SOC/NOC tasks will be automated by GenAI—reducing manual work by 50%

Agentic AI

60%

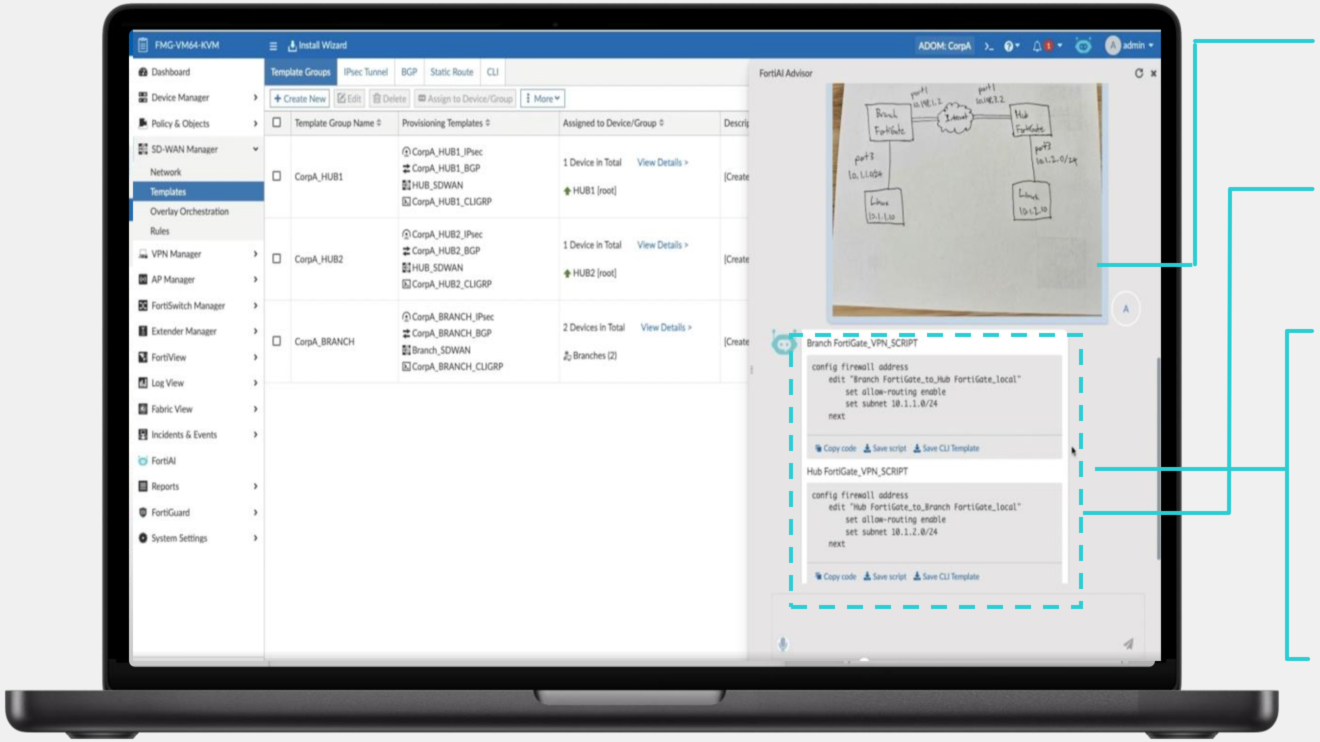
Mean-time-to-repair (MTTR) for outages will be faster by 60%

Source: *Gartner’s Top Trends in AI for IT Operations, 2025*

FortiAI-Assist on FortiManager

Why work harder when you can work smarter

FortiManager



☐	Template Group Name	Provisioning Templates	Assigned to Device/Group	Descrip
☐	CorpA_HUB1	CorpA_HUB1_IPsec CorpA_HUB1_BGP HUB_SDWAN CorpA_HUB1_CLIGRP	1 Device in Total View Details > HUB1 [root]	[Create
☐	CorpA_HUB2	CorpA_HUB2_IPsec CorpA_HUB2_BGP HUB_SDWAN CorpA_HUB2_CLIGRP	1 Device in Total View Details > HUB2 [root]	[Create
☐	CorpA_BRANCH	CorpA_BRANCH_IPsec CorpA_BRANCH_BGP Branch_SDWAN CorpA_BRANCH_CLIGRP	2 Devices in Total View Details > Branches (2)	[Create

Branch FortiGate_VPN_SCRIPT

```
config firewall address
    edit "Branch FortiGate_to_Hub FortiGate_local"
        set allow-routing enable
        set subnet 10.1.1.0/24
    next
```

Hub FortiGate_VPN_SCRIPT

```
config firewall address
    edit "Hub FortiGate_to_Branch FortiGate_local"
        set allow-routing enable
        set subnet 10.1.2.0/24
    next
```

Topology map to SD-WAN Config Scripts

With Explanations

Jinja and CLI

Syntax Validation and edits

Save and Execute

Auto Policy Creation

Day 0-1

Simplified Provisioning

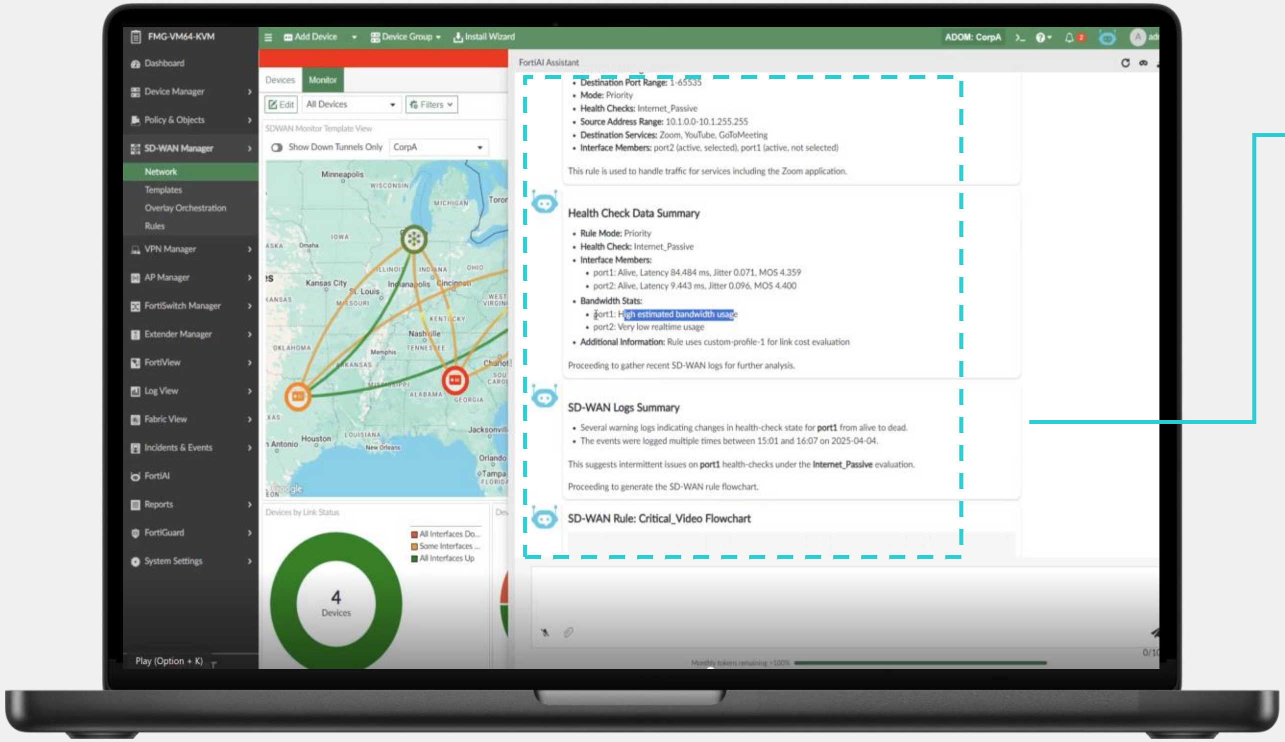
How to Acquire:

- Add-on FortiAI license for FortiManager (7.6~)
- Monthly Top-up Tokens when tokens used up.

FortiAI-Assist on FortiManager

Why work harder when you can work smarter

FortiAIOps FortiManager



- **Destination Port Range:** 1-65535
- **Mode:** Priority
- **Health Checks:** Internet_Passive
- **Source Address Range:** 10.1.0.0-10.1.255.255
- **Destination Services:** Zoom, YouTube, GoToMeeting
- **Interface Members:** port2 (active, selected), port1 (active, not selected)

This rule is used to handle traffic for services including the Zoom application.

Health Check Data Summary

- **Rule Mode:** Priority
- **Health Check:** Internet_Passive
- **Interface Members:**
  - port1: Alive, Latency 84.484 ms, Jitter 0.071, MOS 4.359
  - port2: Alive, Latency 9.443 ms, Jitter 0.096, MOS 4.400
- **Bandwidth Stats:**
  - port1: High estimated bandwidth usage
  - port2: Very low realtime usage
- **Additional Information:** Rule uses custom-profile-1 for link cost evaluation

Proceeding to gather recent SD-WAN logs for further analysis.

SD-WAN Logs Summary

- Several warning logs indicating changes in health-check state for **port1** from alive to dead.
- The events were logged multiple times between 15:01 and 16:07 on 2025-04-04.

This suggests intermittent issues on **port1** health-checks under the **Internet_Passive** evaluation.

Proceeding to generate the SD-WAN rule flowchart.

SD-WAN Rule: Critical_Video Flowchart

Auto-fix Wi-Fi performance Issues

Detect Access issue to Zoom Application and auto-adjust policies

Auto-optimize SD-WAN routes & bandwidth usage

Day N

Autonomous Optimization

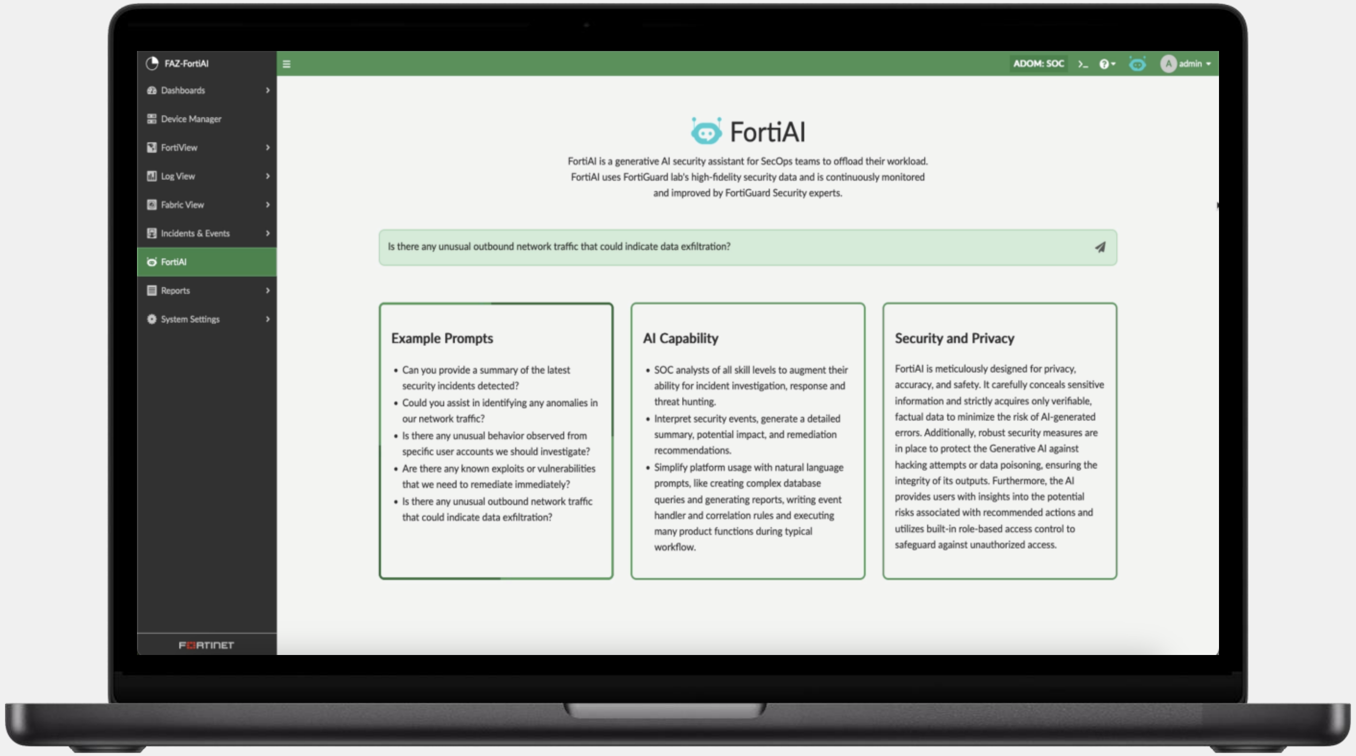
How to Acquire:

- Add-on FMG FortiAI Lic
- Add-on FortiAIOps license

FortiAI-Assist on Fortinet SOC Platform with FortiAnalyzer

Why work harder when you can work smarter

SOC Platform
FortiAnalyzer



FortiAI

FortiAI is a generative AI security assistant for SecOps teams to offload their workload. FortiAI uses FortiGuard lab's high-fidelity security data and is continuously monitored and improved by FortiGuard Security experts.

Is there any unusual outbound network traffic that could indicate data exfiltration?

Example Prompts

- Can you provide a summary of the latest security incidents detected?
- Could you assist in identifying any anomalies in our network traffic?
- Is there any unusual behavior observed from specific user accounts we should investigate?
- Are there any known exploits or vulnerabilities that we need to remediate immediately?
- Is there any unusual outbound network traffic that could indicate data exfiltration?

AI Capability

- SOC analysts of all skill levels to augment their ability for incident investigation, response and threat hunting.
- Interpret security events, generate a detailed summary, potential impact, and remediation recommendations.
- Simplify platform usage with natural language prompts, like creating complex database queries and generating reports, writing event handler and correlation rules and executing many product functions during typical workflow.

Security and Privacy

FortiAI is meticulously designed for privacy, accuracy, and safety. It carefully conceals sensitive information and strictly acquires only verifiable, factual data to minimize the risk of AI-generated errors. Additionally, robust security measures are in place to protect the Generative AI against hacking attempts or data poisoning, ensuring the integrity of its outputs. Furthermore, the AI provides users with insights into the potential risks associated with recommended actions and utilizes built-in role-based access control to safeguard against unauthorized access.

"How many attacks will I receive tomorrow based on past trends?"

AI Built for Analysts

- Voice-to-text & guided prompts
- Auto-generates reports & insights
- Optimizes workflows

AI for Continuous Threat Analysis

- Real-time log & behavior correlation
- Detects hidden threats
- High-fidelity alerts

AI for Autonomous Response

- Playbook execution
- Audit-ready logging
- Cross-platform coordination

Risks and Concerns with Securing GenAI and LLMs Models

Model Poisoning

Manipulating the learning model to degrade performance or introduce vulnerabilities

Unauthorized Access

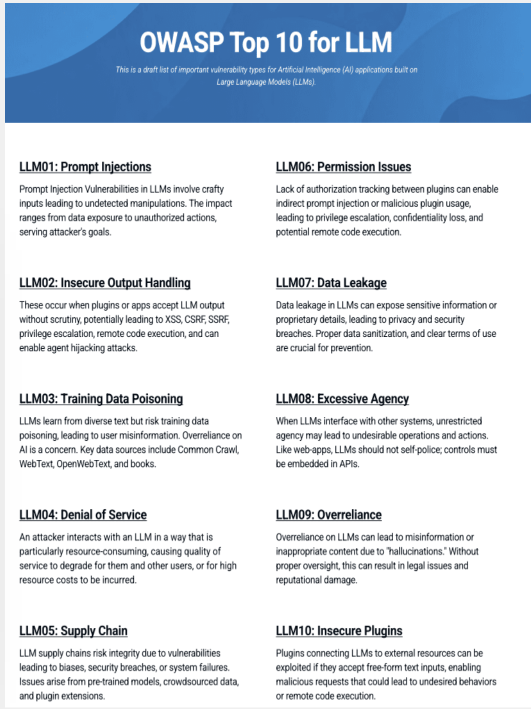
An adversary obtaining direct or indirect access or entitlements to AI models

Malicious Prompts

Logic manipulations, malicious scripts, or command injections

Data Leakage

Models that reveal sensitive data when interacting with a threat actor



OWASP Top 10 for LLM

This is a draft list of important vulnerability types for Artificial Intelligence (AI) applications built on Large Language Models (LLMs).

LLM01: Prompt Injections

Prompt Injection Vulnerabilities in LLMs involve crafty inputs leading to undetected manipulations. The impact ranges from data exposure to unauthorized actions, serving attacker's goals.

LLM02: Insecure Output Handling

These occur when plugins or apps accept LLM output without scrutiny, potentially leading to XSS, CSRF, SSRF, privilege escalation, remote code execution, and can enable agent hijacking attacks.

LLM03: Training Data Poisoning

LLMs learn from diverse text but risk training data poisoning, leading to user misinformation. Overreliance on AI is a concern. Key data sources include Common Crawl, WebText, OpenWebText, and books.

LLM04: Denial of Service

An attacker interacts with an LLM in a way that is particularly resource-consuming, causing quality of service to degrade for them and other users, or for high resource costs to be incurred.

LLM05: Supply Chain

LLM supply chains risk integrity due to vulnerabilities leading to biases, security breaches, or system failures. Issues arise from pre-trained models, crowdsourced data, and plugin extensions.

LLM06: Permission Issues

Lack of authorization tracking between plugins can enable indirect prompt injection or malicious plugin usage, leading to privilege escalation, confidentiality loss, and potential remote code execution.

LLM07: Data Leakage

Data leakage in LLMs can expose sensitive information or proprietary details, leading to privacy and security breaches. Proper data sanitization, and clear terms of use are crucial for prevention.

LLM08: Excessive Agency

When LLMs interface with other systems, unrestricted agency may lead to undesirable operations and actions. Like web-apps, LLMs should not self-police; controls must be embedded in APIs.

LLM09: Overreliance

Overreliance on LLMs can lead to misinformation or inappropriate content due to "hallucinations." Without proper oversight, this can result in legal issues and reputational damage.

LLM10: Insecure Plugins

Plugins connecting LLMs to external resources can be exploited if they accept free-form text inputs, enabling malicious requests that could lead to undesired behaviors or remote code execution.

FortiAI-SecureAI: Securing AI Infrastructure

On-prem and cloud

Secure access to AI workloads

Monitor identities and entitlements, Enforce ZTNA and protect AI workloads

FortiCNAPP **ZTNA FW**

Find vulnerabilities in AI apps

Test your AI applications to find vulnerabilities in advance

FortiDAST

Sanitize prompts and input

Inspect HTTP traffic for unethical prompts, command injections and data theft attempts

FortiWeb

Prevent data leakage

Apply sensitive data filtering on outputs

ForitDLP

FortiAI-SecureAI Business Benefits

Model Integrity

Protect intellectual property and investments in AI by fending off threats to your GenAI and LLMS

Minimized Threat Exposure

A comprehensive coverage of multiple risks to LLMs/Gen AI at both the network and application levels

Integrated Solutions

A single provider of proprietary technology that shares data and translates insights into actions in real time

Compliance

360-degree observability for compliance management across AI applications.

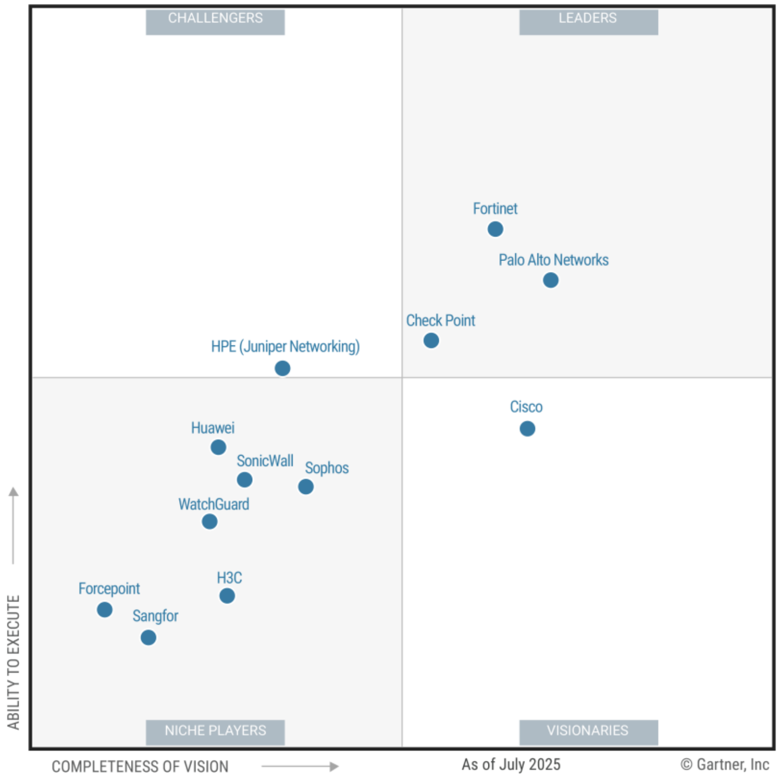
Summary

AI-enhanced attacks and AI usage is a key emerging risk that needs to be addressed

FortiAI protects from AI threats and GenAI usage, automates security and network operations, and secures AI deployments

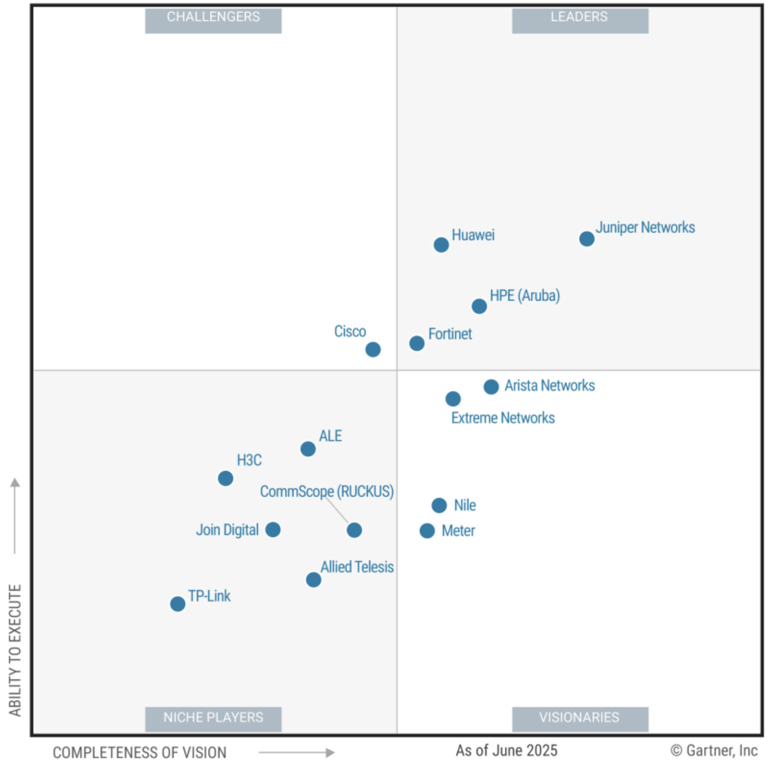
Leverage FortiAI solutions that are embedded as a part of Fortinet fabric to enable your AI transformation

Figure 1. Magic Quadrant for Hybrid Mesh Firewall



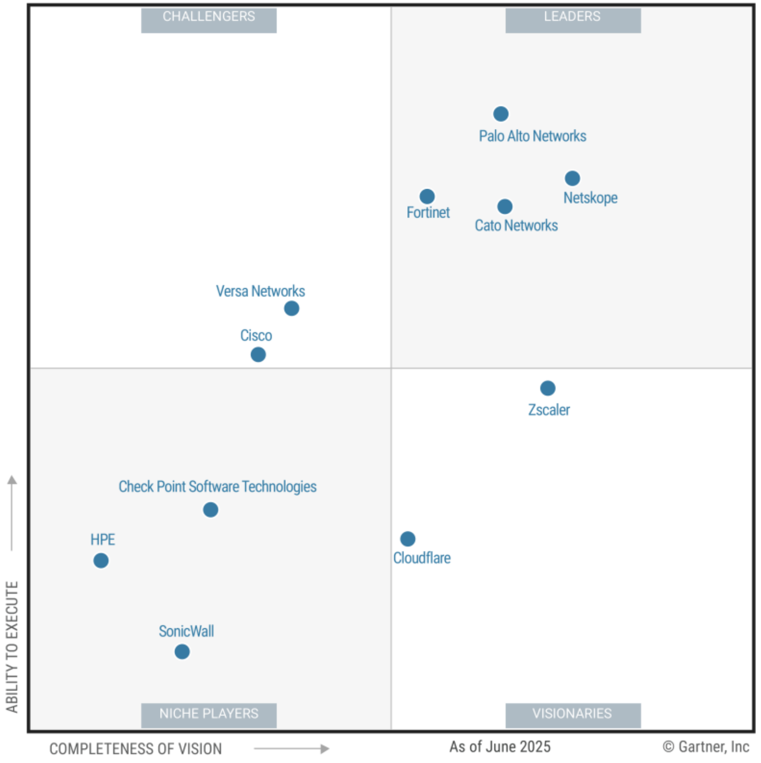
Gartner

Figure 1: Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure



Gartner

Figure 1: Magic Quadrant for SASE Platforms



Gartner

FORTINET

Security Day

6. října 2025 | Praha
Forum Karlín

Fortinet Security Day 2025 - Praha

pondělí, 6. října 2025, od 11:00 hod. | Forum Karlín, Praha

FORTINET