



FORTINET

COLOMBIA
& ECUADOR

XPERTS26

FORTINET | COLOMBIA
& ECUADOR
XPERTS26

Applied IA for Cybersecurity



Fortinet Team



David



Ismael



Jose



Benoit



Fabián González

Principal Systems Engineer Colombia

<https://www.linkedin.com/in/fab-gonzalez>

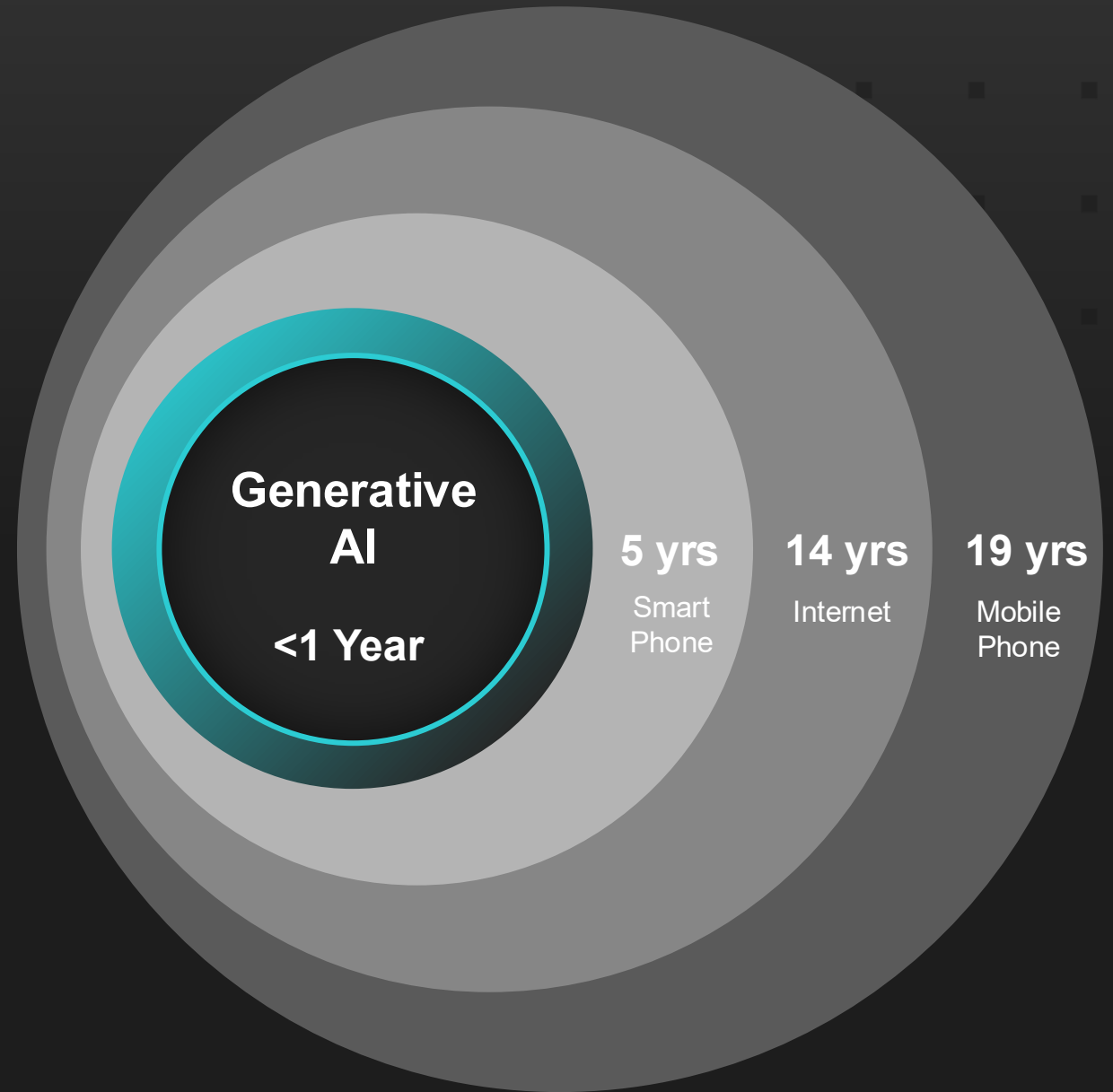


Empower Innovation with AI, Secured by Fabric



Accelerated Gen AI Adoption

Time to reach **1 billion**
users & enabling
technologies



Global AI Adoption for Efficiency

Broad Usage

94%

of organizations are either already using or exploring Gen AI

Capgemini 

Customer Service

80%

of customer service by 2026

Gartner

Software Development

97%

of developers have used Gen AI at some point

GitHub

Security Operations

93%

of organizations are considering for Security Operations

Gartner





Security Challenges of AI Adoption

Visibility

Governance

Data Privacy

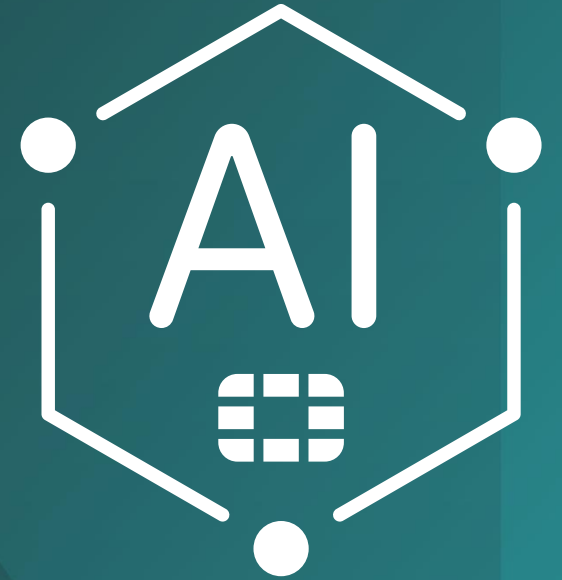
Usage Control

Trust & Transparency

Compliance

Integration

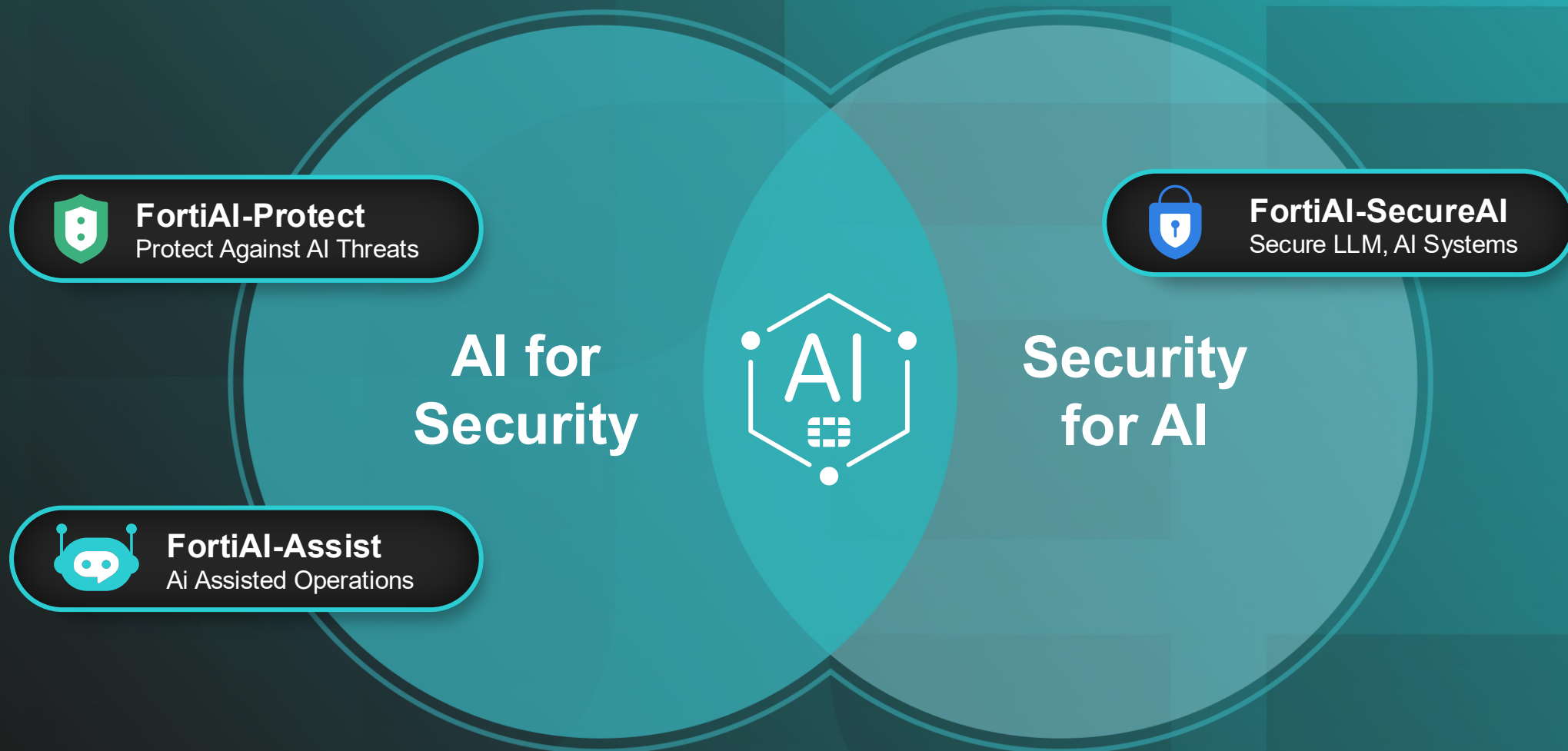




FortiAI Framework & Security Fabric



FortiAI: Protecting the AI Enterprise





FortiAI-Protect
Protect Against AI Threats

One Fabric, Amplified by AI

One Coordinated Defense

FortiGuard Labs

Real time threat intelligence
for real time protection.

>500M

Sensors

>1000

Researchers

Security Fabric

Embedded AI across entire
Fortinet Solution

>30

products with
AI/ML features

Best in Class AI

Mature and Full Stack
of AI

>15

Yrs of Experience

>500

Patented/Pending

>300

AI/ML Engineers

Broad Coverage

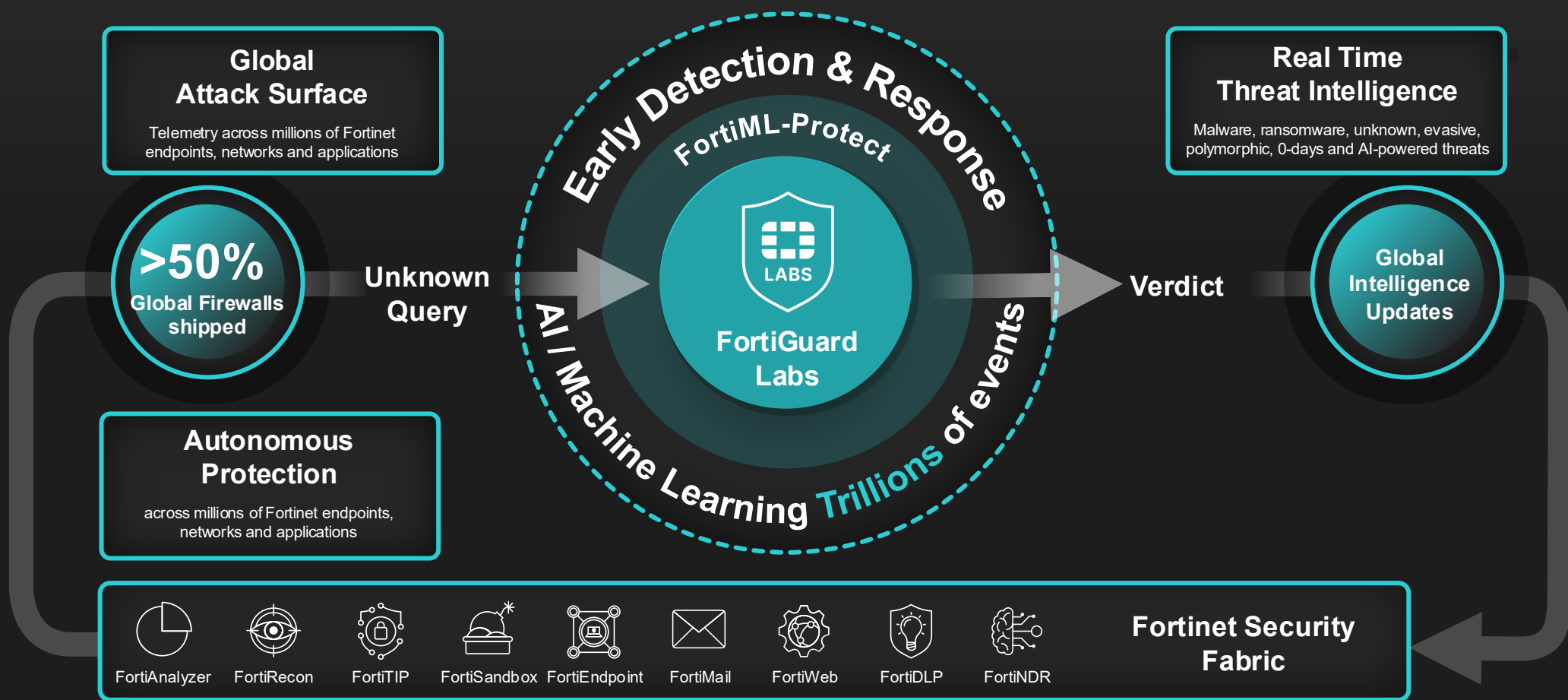
Comprehensive AI to Protect
Data, Apps & AI Infrastructure

>100

AI/ML
features



FortiGuard Labs AI-Powered Security





FortiAI-Protect
Protect Against AI Threats

Fabric, Amplified by AI



FortiGuard Labs



FortiMail
Workspace



FortiMonitor



FortiSASE



FortiAI Ops



FortiWeb



FortiNDR



FortiAI Gate



FortiSOC



FortiDLP



FortiCNAPP



FortiSIEM



FortiGate



FortiSandbox



FortiEDR



FortiCASB



FortiAnalyzer



Classify malicious files and
network-based threats



Behavior anomaly
detection



Identifies unusual user
behaviors



simplify and automate
the management



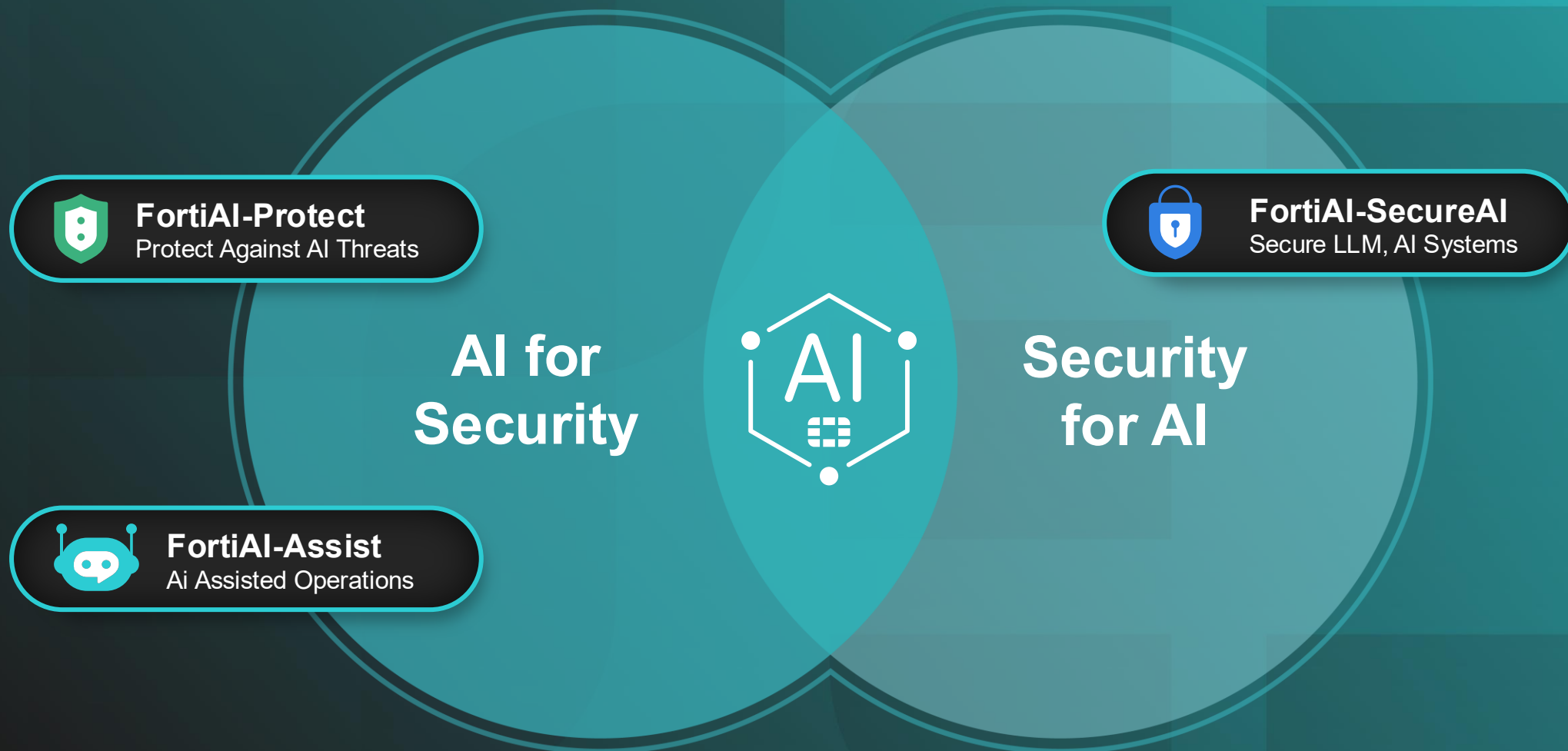
Malicious mail
detection and BEC



Forecast metrics and
dynamic baselines

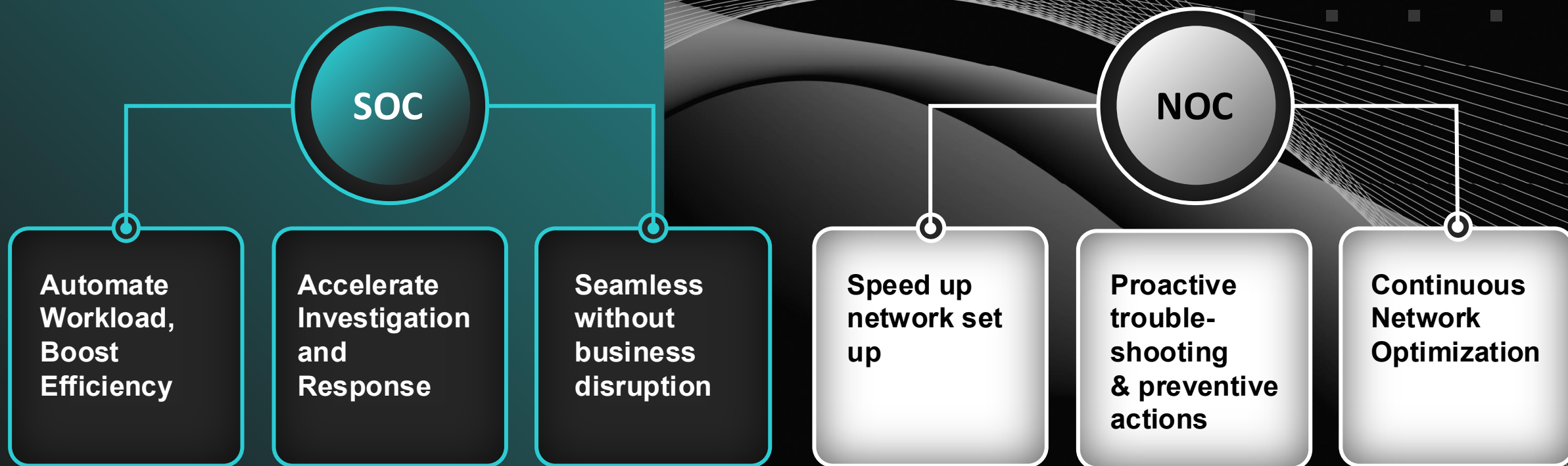


FortiAI: Protecting the AI Enterprise



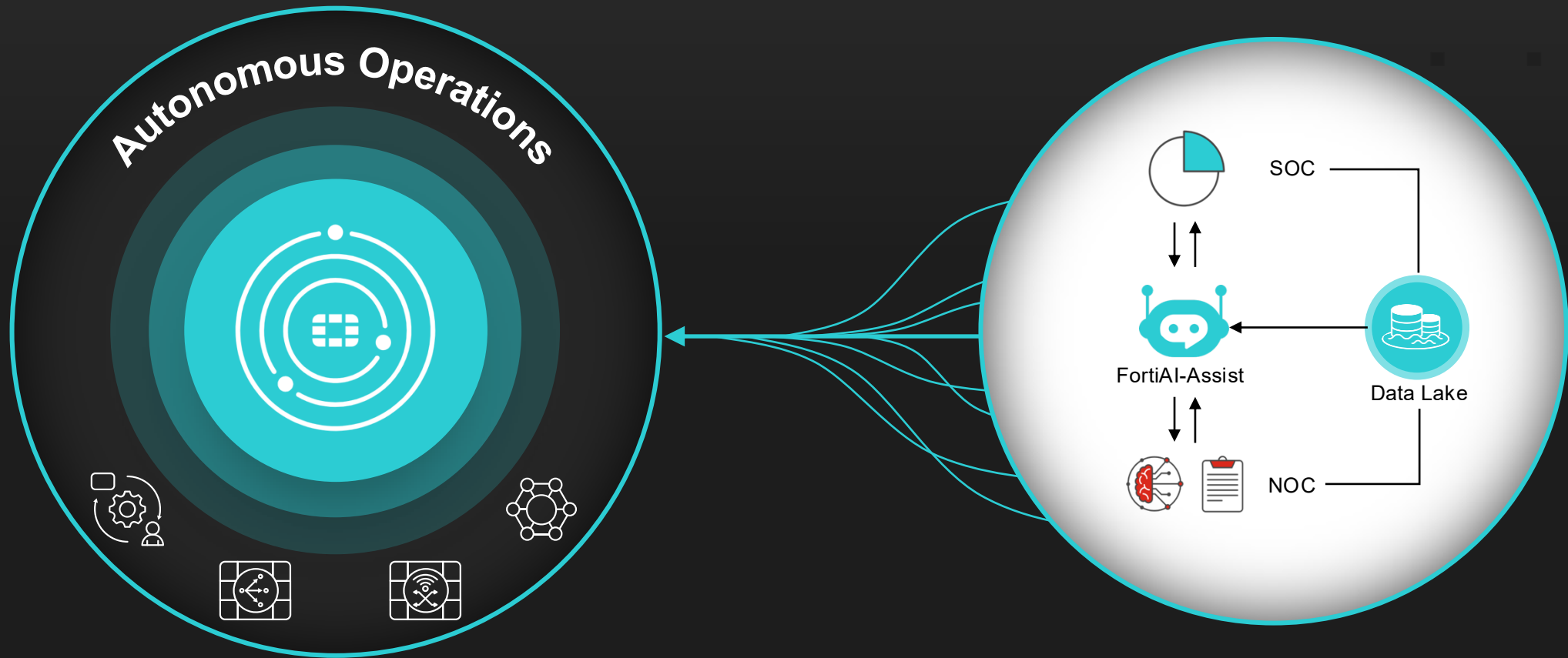
FortiAI-Assist

What Customers Care About



FortiAI-Assist

GenAI and Agentic AI Powered Operations



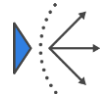
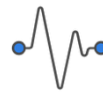
Predictive, proactive and adaptive towards autonomous operations



Fabric, Amplified by FortiAI

20+ Solutions, with 500+ Patents

 FortiAI-Assist

 FortiAnalyzer	 FortiManager	 FortiSASE	 FortiAIOps	 FortiADC	 FortiWeb	 FortiNDR	 FortiMonitor
 FortiGate	 FortiDLP	 FortiCNAPP	 FortiSIEM	 FortiSOAR	 FortiSandbox	 FortiCASB	 FortiMail Workspace
 LAN, SD-WAN Optimization	 Threat Hunting	 Automated Alert Triage	 Policy Creation	 Auto Configuration	 Incident Response Optimization		

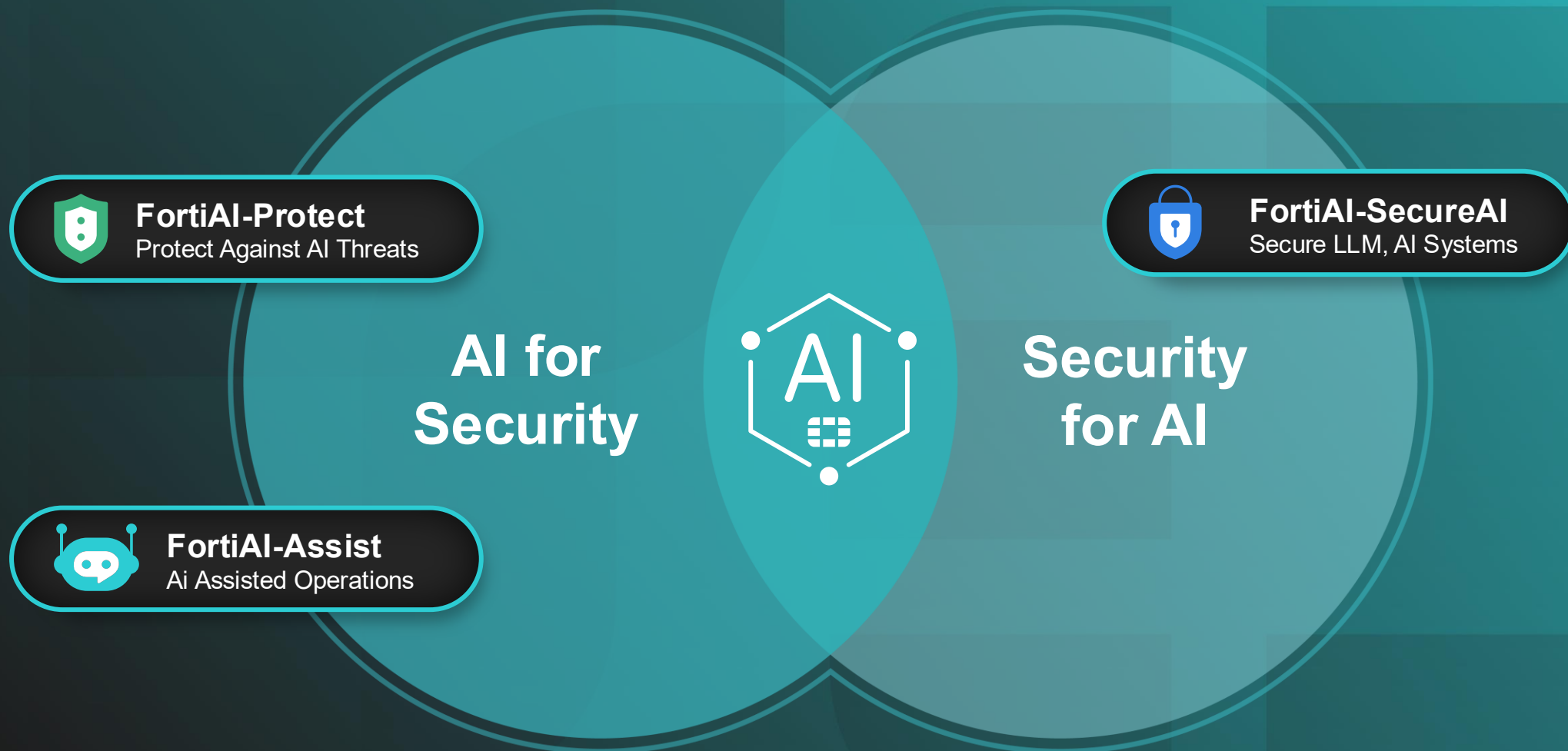
FortiAI Is Embedded Across



the Security Fabric Platform



FortiAI: Protecting the AI Enterprise





FortiAI-SecureAI
Secure LLM, AI Systems

Enterprise AI Maturity

Generative AI

Prompt-driven,
Reactive

Gemini  Claude

Private LLM

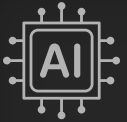
AI Model hosted
privately for
compliance, cost
and controlled use

 DeepMind  Meta



Generative AI

What Should Worry Customers



**GenAI
Visibility
and Risk**



**Enable Safe
AI Use and
prevent data
loss**



**Control
application
access by
risk**



**Accurate
analysis**



**Boost threat
detection
accuracy**





FortiAI-SecureAI
Secure LLM, AI Systems

Controlling the GenAI Use



Users



**Perimeter
Security**



**Browser
Security**



**Application
Identification**



**Data Leakage
Prevention**



**SaaS
Monitoring**

Gemini



✱ Claude



FortiGate



FortiDLP



FortiCASB





FortiAI-SecureAI
Secure LLM, AI Systems

Enterprise AI Maturity

Generative AI

Prompt-driven,
Reactive

Gemini  Claude

Private LLM

AI Model hosted
privately for
compliance, cost
and controlled use

 DeepMind  Meta





Gaining Control,

The Shift to Private LLMs



3X ratio

By 2027, for every single use of a general-purpose LLM, organizations will have three separate, more specialized models in use - Gartner

- Protect Data
- Ensure Privacy and confidentiality
- Protects Organizational IP
- Compliance and Data Sovereignty
- Flexibility
- Reduced Attack Surface
- Manage Shadow AI



Risks & Concerns

The shift in AI Application architecture creates additional security gaps

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

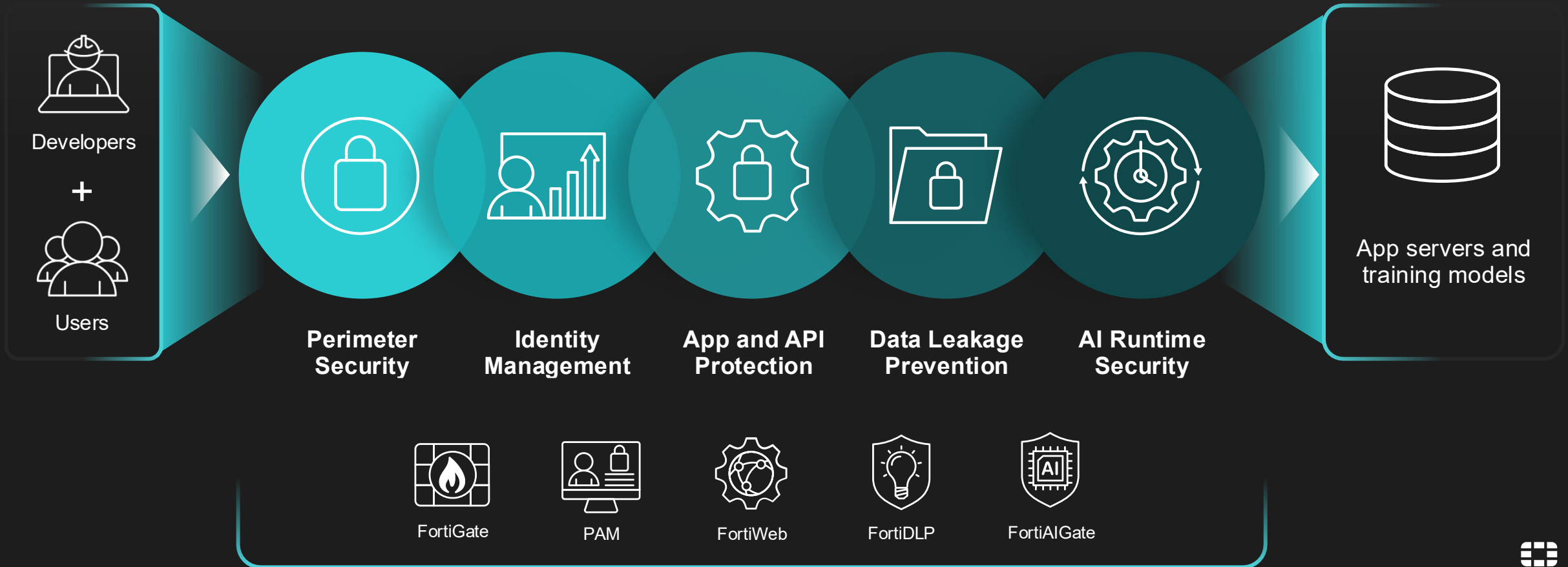
Models that reveal sensitive data when interacting with a threat actor



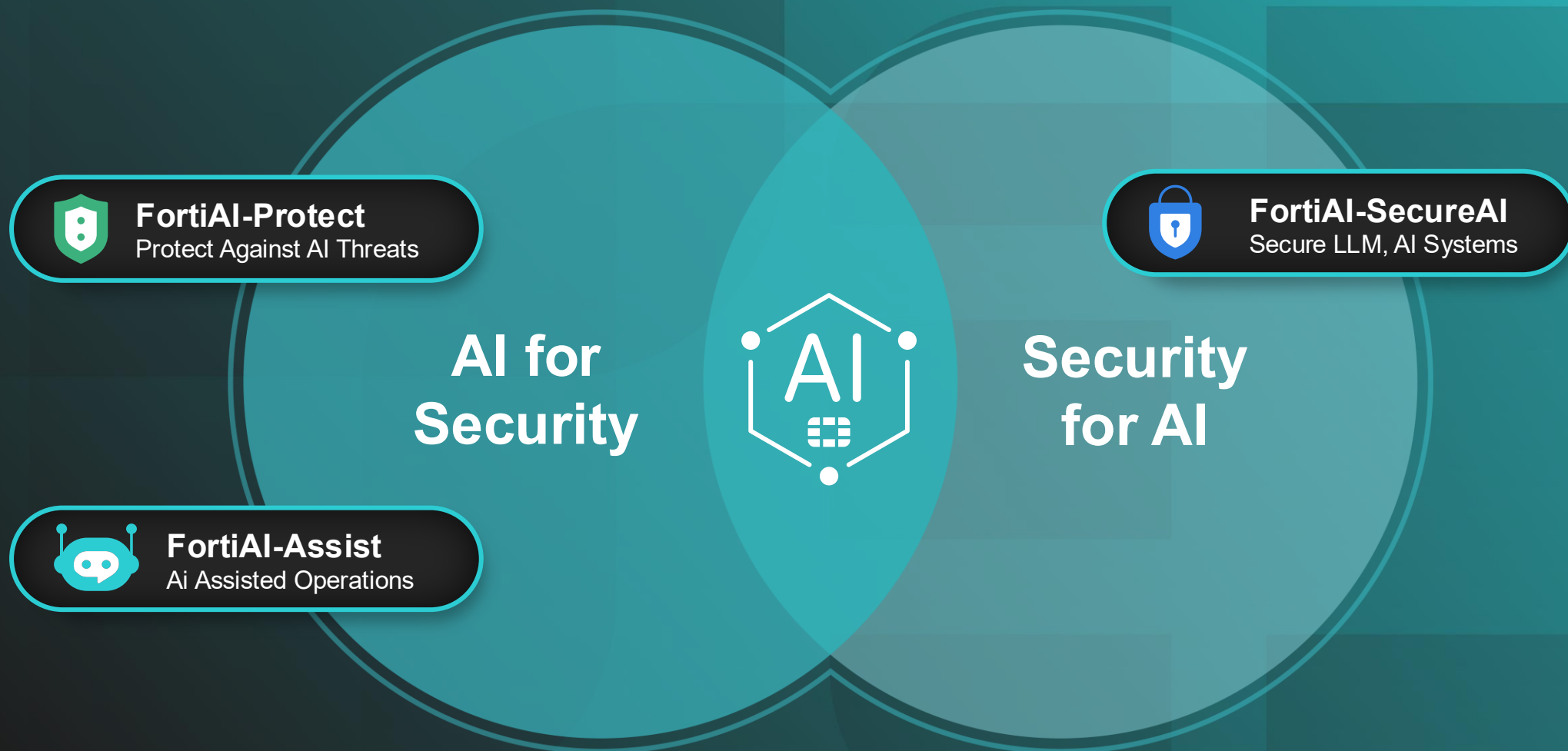


FortiAI-SecureAI
Secure LLM, AI Systems

Securing the AI Application Architecture End to End



FortiAI: Protecting the AI Enterprise



Agenda



FortiAI-Assist

Ai Assisted Operations

FortiAI-Assist in action Theory

Demo:

- SD-WAN
- FortiManager
- FortiAnalyzer
- FortiAI



FortiAI-SecureAI

Secure LLM, AI Systems

Shadow AI Theory

Laboratory:

- FortiGate
- FortiDLP
- FortiMail WorkSpace
- FortiCASB SSPM

FortiWeb AI Security Theory

Laboratory:

- FortiWeb
- FortiAI

LLM Security Theory

Laboratory:

- FortiPAM
- FortiAIGate



Applied AI - Challenge





Applied AI - Challenge

Capture the Flag

<https://colecuxperts-ai-dev.lwctf.com/>

Registration:

- Corporate email
- Access code **Xperts2026**

Start CTF:

- Click on “Página de Retos”



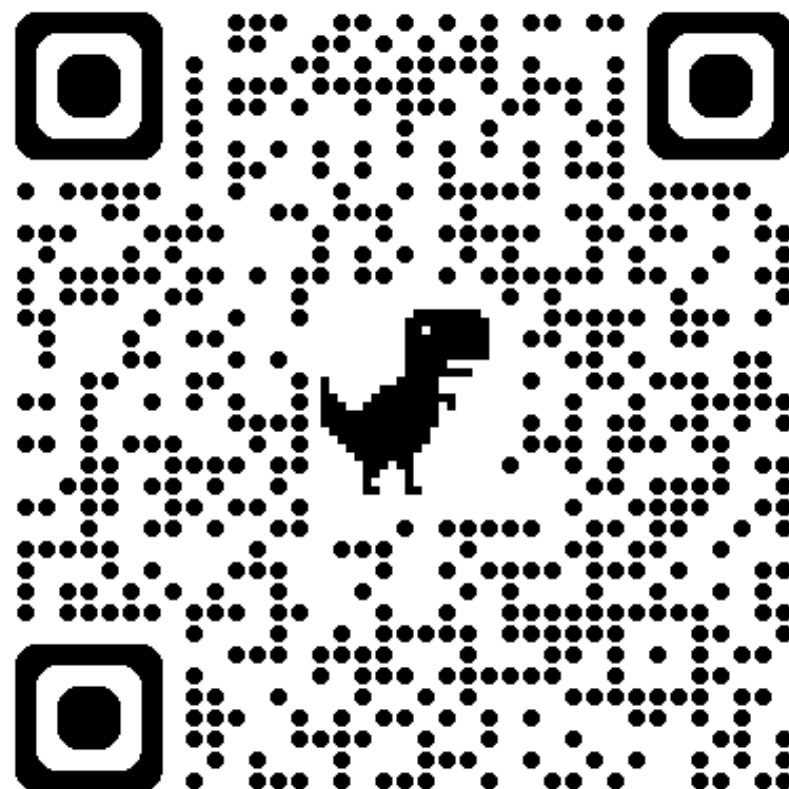
Material de Referencia



Página de Retos



Guía Rápida





FORTINET

COLOMBIA
& ECUADOR

XPERTS26