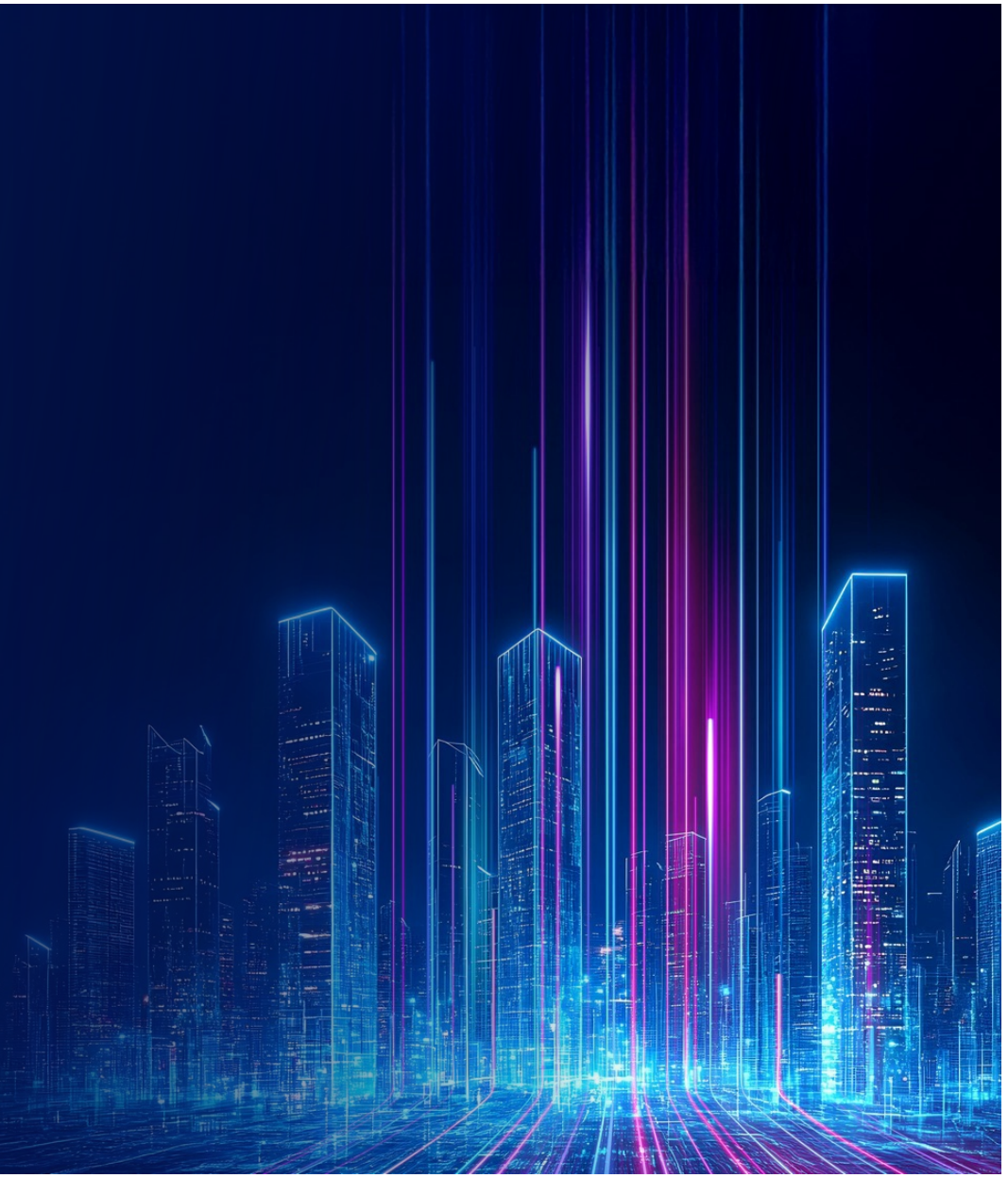
A10

Always Secure. Always Available.

A10 AI Firewall



Alvyern Lee

Sr. Systems Engineer | ASEAN, APAC

A10

Always Secure. Always Available.

Defend AI Applications, Wherever They Run with A10 AI Firewall.

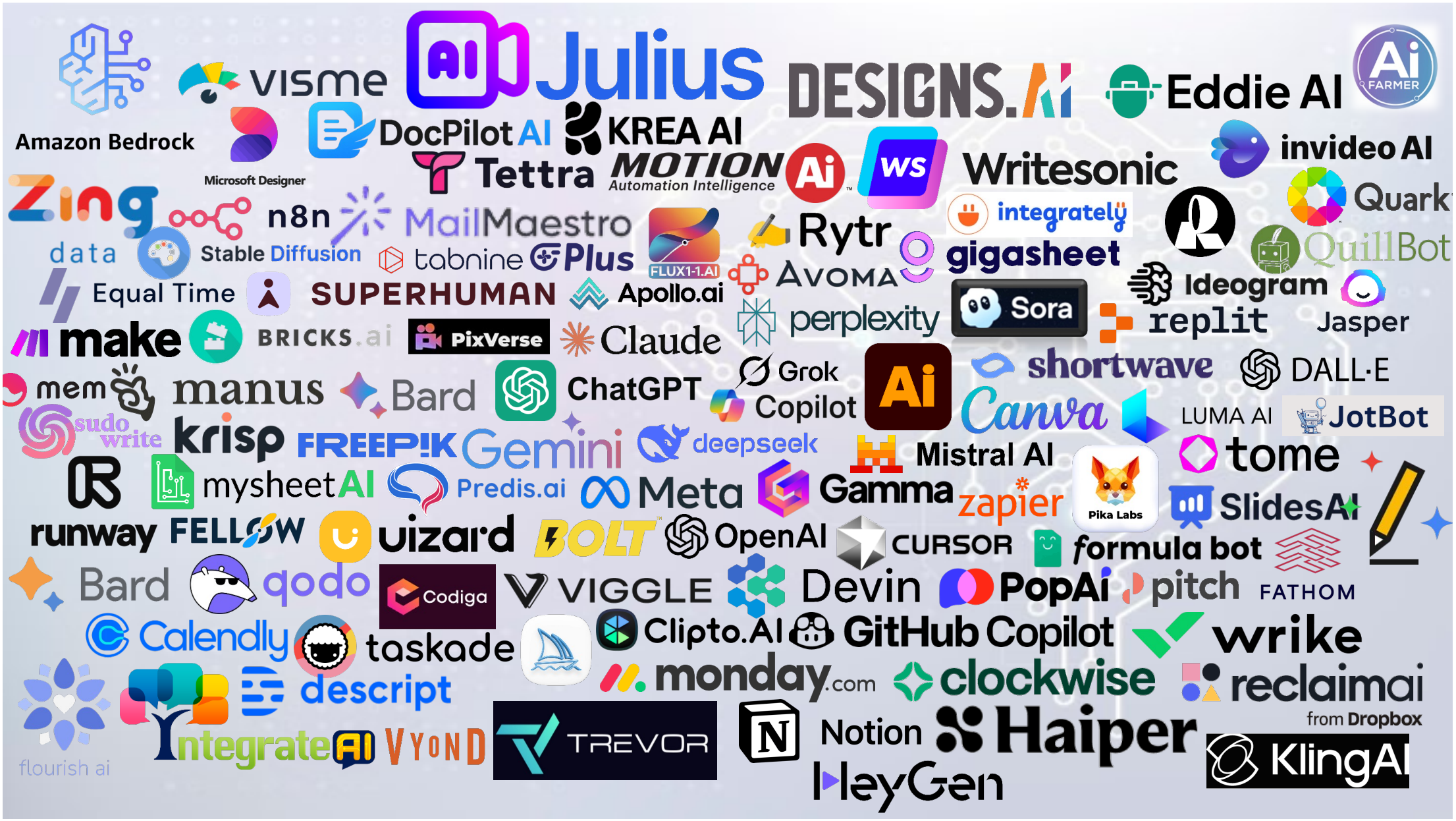
Overview

- What is AI?
- Why AI transformation happening fast?
- Evolution of AI
- Shift in security focus with AI
- Why Traditional Security Cannot See AI-Native Threats
- Transitional Security vs AI
- A10 AI Firewall

What is AI?

Artificial Intelligence (AI)
Systems that can simulate human intelligence by understanding, generating, and reasoning with data.

In the modern enterprise context, this is primarily driven by **Large Language Models (LLMs)** such as ChatGPT-style systems.


Amazon Bedrock
visme
Julius
DESIGNS.AI
Eddie AI
AI FARMER
Microsoft Designer
DocPilot AI
KREA AI
Tettra
MOTION
Automation Intelligence
Writesonic
invideo AI
Zing
n8n
MailMaestro
integrately
Quark
data
Stable Diffusion
tabnine
Plus
FLUX1-1.AI
Rytr
gigasheet
QuillBot
Equal Time
SUPERHUMAN
Apollo.ai
AVOMA
Ideogram
make
BRICKS.ai
PixVerse
Claude
perplexity
Sora
replit
Jasper
mem
manus
Bard
ChatGPT
Grok
Copilot
shortwave
DALL·E
sudo write
krisp
FREEPIK
Gemini
deepseek
Canva
LUMA AI
JotBot
mysheetAI
Predis.ai
Meta
Mistral AI
tome
runway
FELLOW
uizard
BOLT
OpenAI
Gamma
zapier
Pika Labs
SlidesAI
Bard
qodo
Codiga
VIGGLE
CURSOR
formula bot
Devin
PopAI
pitch
FATHOM
Calendly
taskade
Clipto.AI
GitHub Copilot
wrike
descript
monday.com
clockwise
reclaimai
from Dropbox
flourish ai
IntegrateAI
VYOND
TREVOR
Notion
Haiper
KlingAI
HeyGen

Why this transformation is happening so fast!

- LLMs are now embedded in enterprise apps (Microsoft, SaaS, APIs)
- Open ecosystems (RAG, plugins, agents) make integration easy
- Businesses demand automation and productivity gains
- AI is becoming a core interface between users and systems

AI is now a **production workload**, **not an experiment**

THE EVOLUTION OF AI

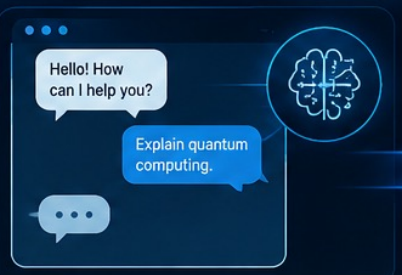
From Chatbots to Agents: A New Era of Intelligence

TIMEFRAME

CAPABILITIES

OUTCOME FOCUS

1 TRADITIONAL LLMs (2023)

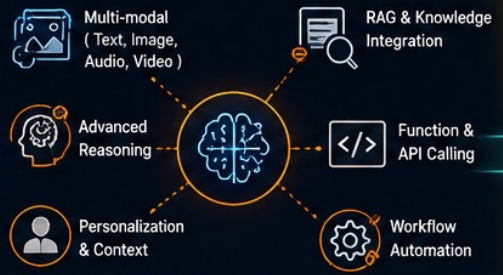


What it can do

- Text generation & conversation
- Answer questions
- Summarize information
- Single-turn interaction

FOCUS: INFORMATION

2 SMART LLMs / GenAI Applications (2024-2025)

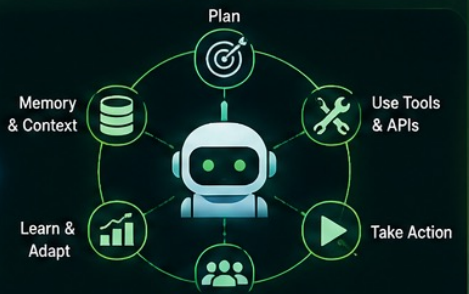


What it can do

- Understand context and intent
- Use enterprise data & tools
- Multi-step task assistance
- More accurate and relevant responses

FOCUS: ASSISTANCE

3 AGENTIC AI (2026 and beyond)



What it can do

- Autonomous decision-making
- Execute complex tasks end-to-end
- Interact with systems and people
- Continuously learn and improve

FOCUS: OUTCOMES

WHY THE RAPID TRANSFORMATION?

- Breakthroughs in foundation models
- Massive computing power & cloud scale
- Abundance of data & knowledge
- Business demand for automation & productivity
- Easy access via APIs & platforms

THE NEW THREAT LANDSCAPE

- **Prompt Injection** — Manipulating AI behavior
- **Data Leakage** — Exposing sensitive information
- **Model Manipulation** — Altering model outputs
- **Insecure Output** — Harmful or biased responses
- **Agent Abuse** — Unauthorized actions & tool misuse

VS

SHIFT IN SECURITY FOCUS

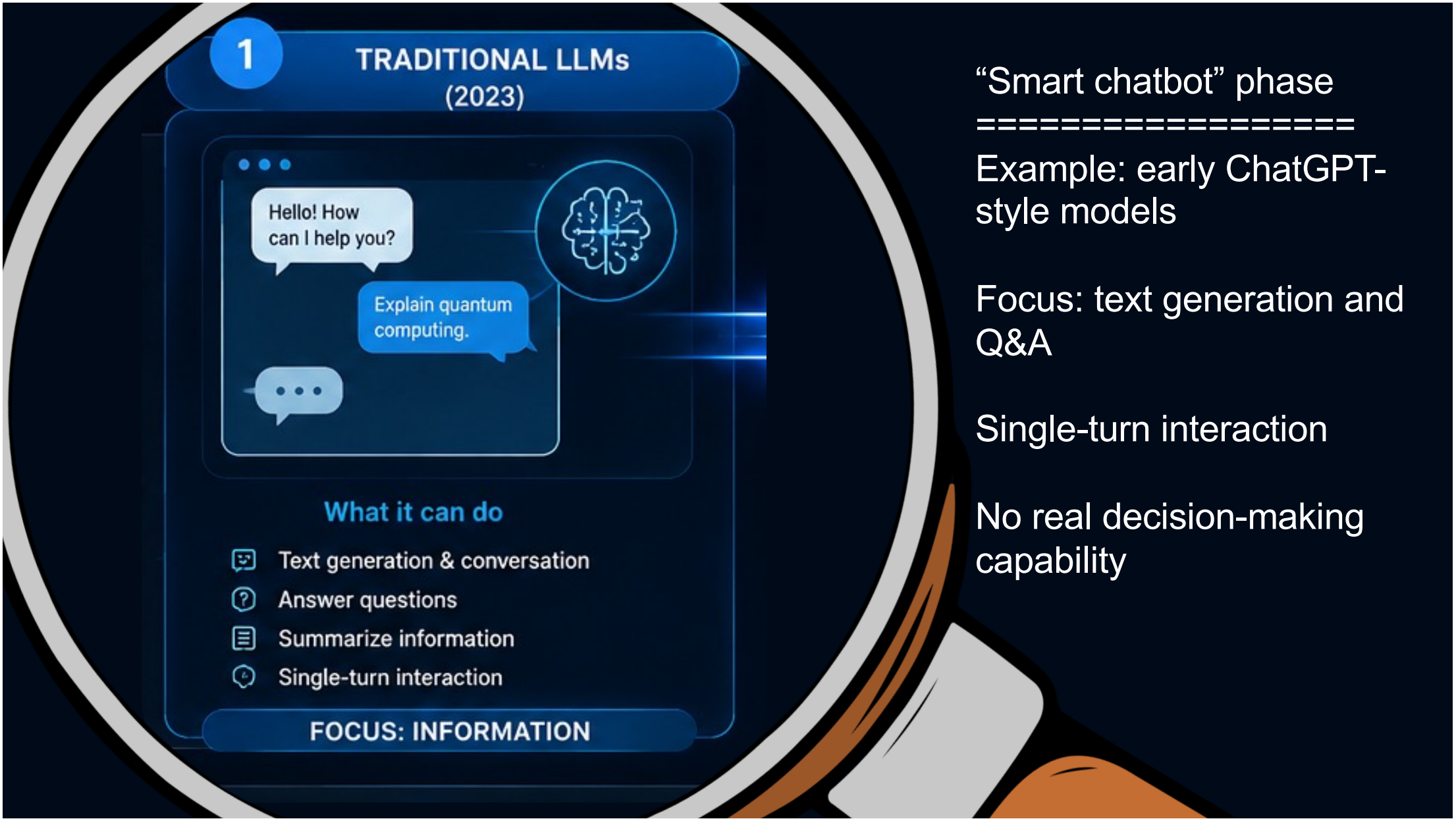
FROM **OWASP TOP 10** (Web Applications)

SQLi · XSS · CSRF · Auth Flaws · ...

TO **OWASP TOP 10** for LLM Applications

Prompt Injection · Data Leakage · Model Abuse · Insecure Output · ...

AI IS EVOLVING. SECURITY MUST EVOLVE TOO.
Protect AI, Your Data, Your Users, and Your Business.



“Smart chatbot” phase

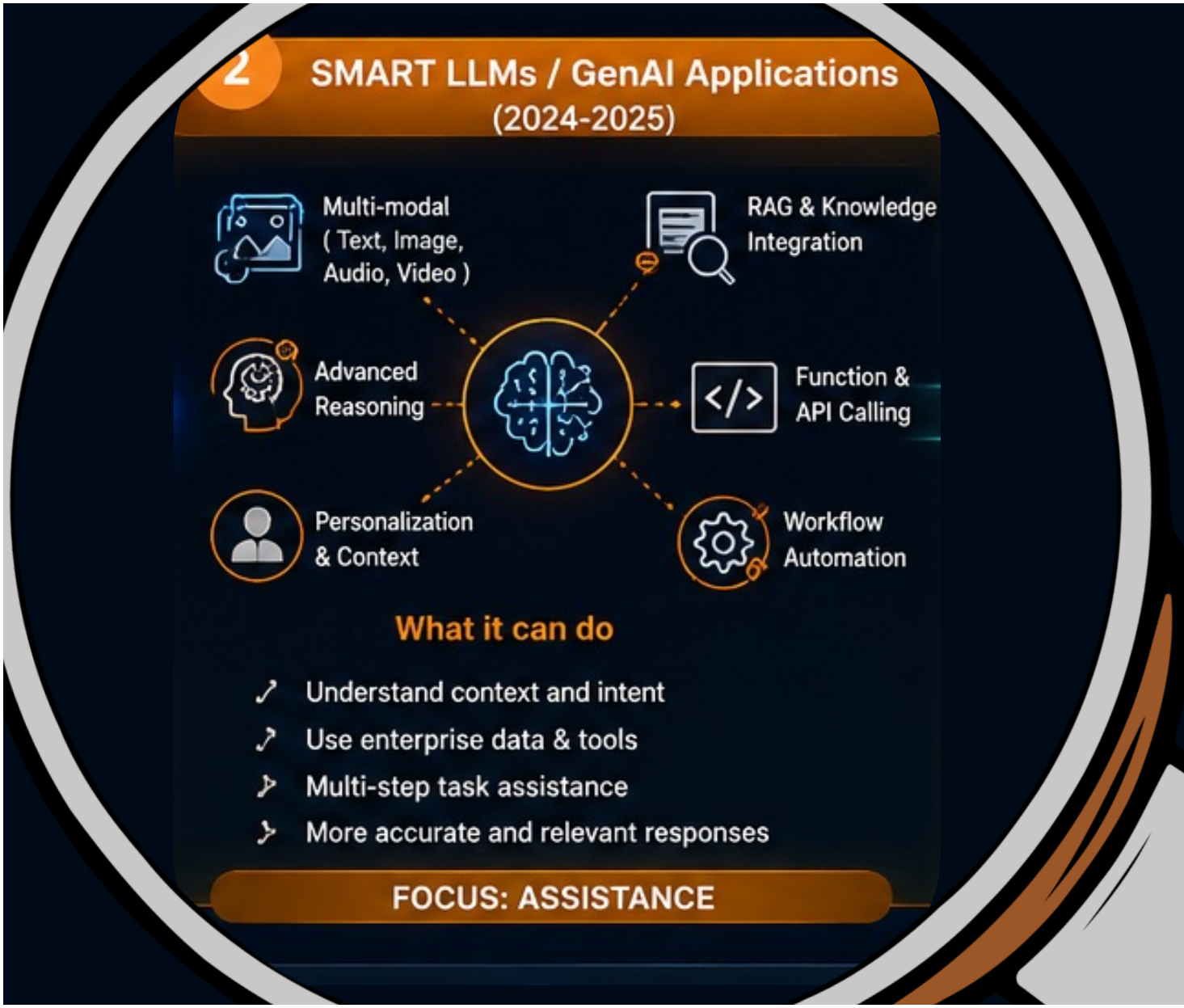
==========

Example: early ChatGPT-style models

Focus: text generation and Q&A

Single-turn interaction

No real decision-making capability



“Enterprise Assistant” phase

==========

Context-aware conversations

Summarize, Analyze, and assist workflows

Integrated into enterprise applications via APIs

Supports multi-step reasoning

“Autonomous Digital Worker” phase

==========

LLMs that can act, not just respond

Execute tasks, call APIs, make decisions

Multi-step autonomous workflows

Connected to tools, data, and systems

THE EVOLUTION OF AI

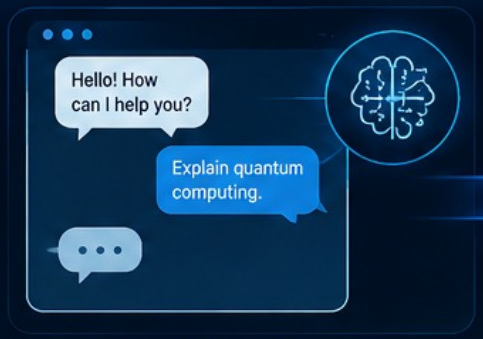
From Chatbots to Agents: A New Era of Intelligence

TIMEFRAME

CAPABILITIES

OUTCOME FOCUS

1 TRADITIONAL LLMs (2023)

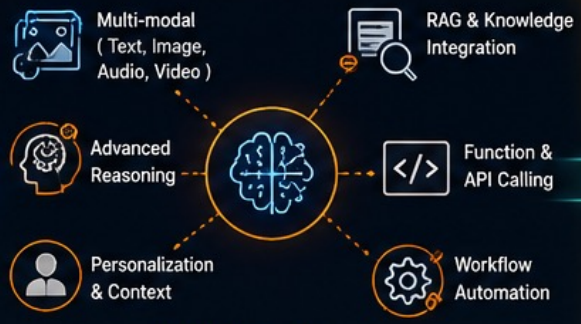


What it can do

- Text generation & conversation
- Answer questions
- Summarize information
- Single-turn interaction

FOCUS: INFORMATION

2 SMART LLMs / GenAI Applications (2024-2025)

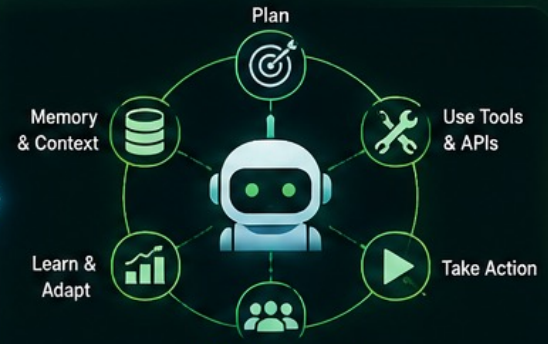


What it can do

- Understand context and intent
- Use enterprise data & tools
- Multi-step task assistance
- More accurate and relevant responses

FOCUS: ASSISTANCE

3 AGENTIC AI (2026 and beyond)



What it can do

- Autonomous decision-making
- Execute complex tasks end-to-end
- Interact with systems and people
- Continuously learn and improve

FOCUS: OUTCOMES

WHY THE RAPID TRANSFORMATION?

- Breakthroughs in foundation models
- Massive computing power & cloud scale
- Abundance of data & knowledge
- Business demand for automation & productivity
- Easy access via APIs & platforms

THE NEW
THREAT LANDSCAPE

AI introduces new risks that traditional controls were not designed to stop.

Prompt Injection
Manipulating prompts to bypass guardrails and control the model.

Data Leakage
Exposing sensitive information through model responses.

Model Manipulation
Altering model behavior or exploiting weaknesses to generate harmful outputs.

Insecure Output
Generating harmful, biased, or misleading content.

Agent Abuse
Exploiting agent autonomy to perform unauthorized actions or misuse tools.

API Abuse
Automating attacks and abusing APIs at scale.

Excessive Agency
Granting excessive permissions leading to uncontrolled actions.

Data Poisoning
Injecting or poisoning data in training or retrieval sources to corrupt model behavior.

AI systems can be manipulated, misused, and compromised in ways traditional security cannot detect.

Shift in Security Focus

How is AI Changing Security

Nature of AI Traffic

- Asymmetrical, non-deterministic, semantic interactions
- Tokenized, conversational exchanges
- Pattern-based inspection can’t interpret AI interactions

Semantic Threats

- AI attacks exploit intent and context, not patterns or signatures
- Threats use natural language prompts and instructions
- AI models follow instructions, making them easy to manipulate
- Multi-modal in nature

Expanded Attack Surface

- AI agents connect to tools, APIs, databases, and knowledge sources
- New pathways for data access and manipulation
- Expanded attack surface across the AI application pipeline

AI FOR SECURITY

AI PROTECTS YOUR SYSTEMS

THREAT DETECTION & PREVENTION

BEHAVIOR ANALYSIS

REAL-TIME RESPONSE

AUTOMATED PROTECTION

AI WORKS FOR YOU TO PROTECT WHAT MATTERS

VS

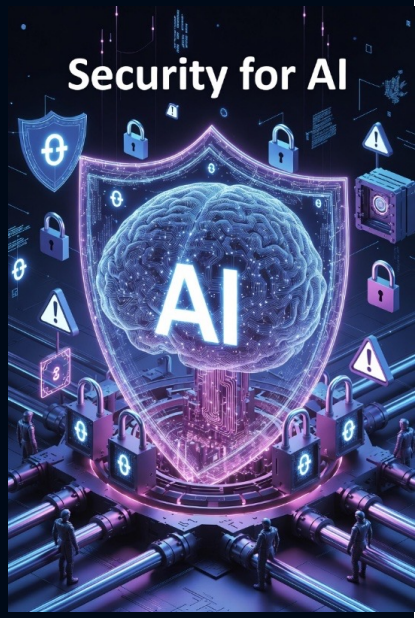
SECURITY FOR AI

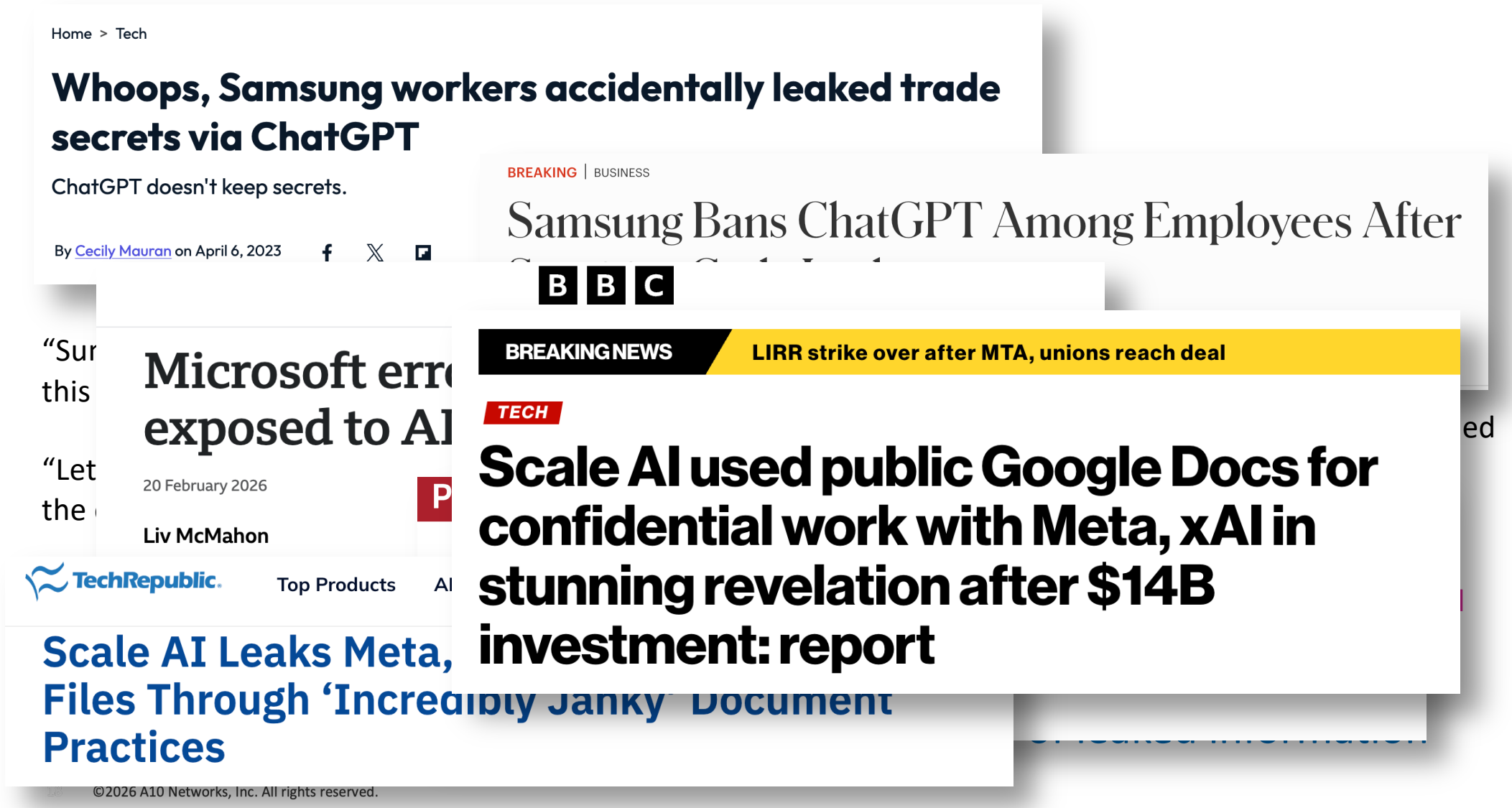
SECURITY PROTECTS AI AND YOUR DATA

SECURITY BUILT AROUND AI. SAFE, TRUSTED, RESPONSIBLE.

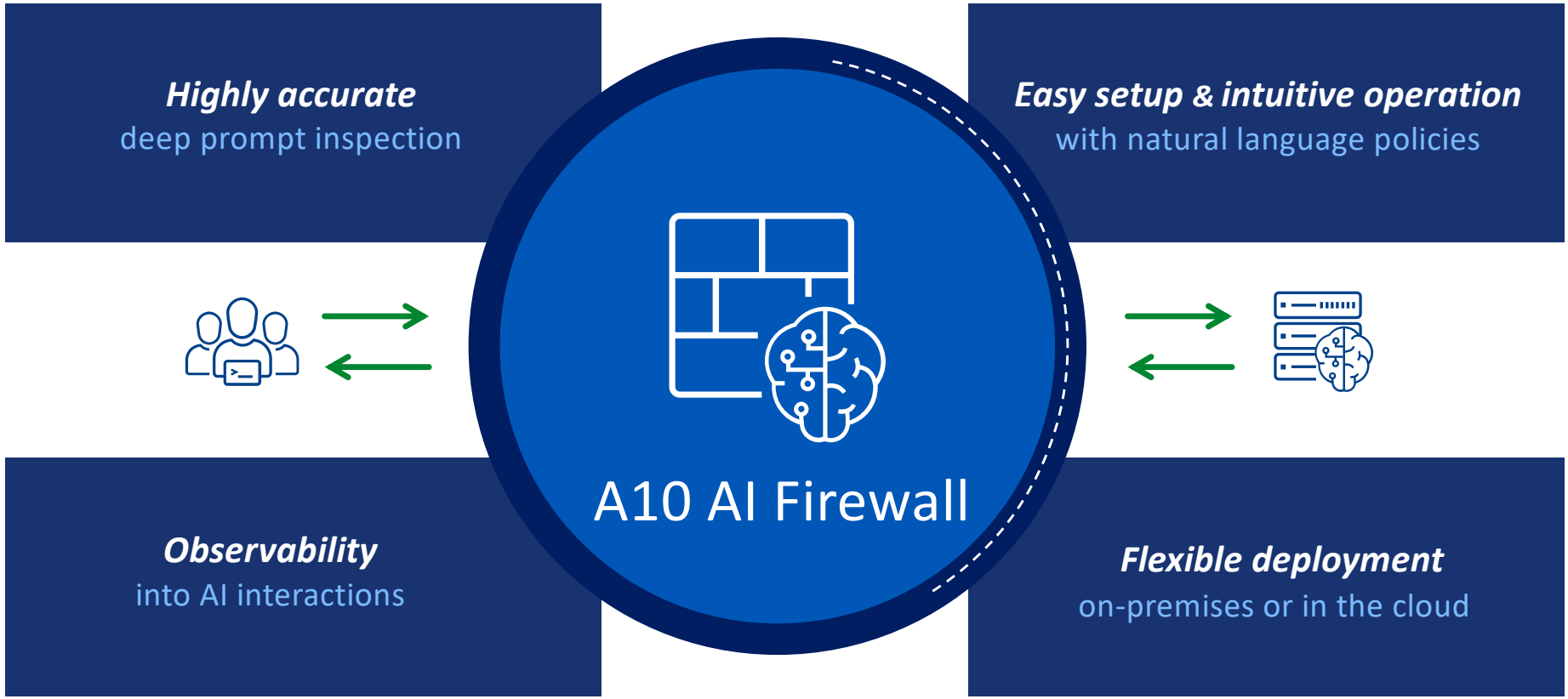
Traditional Security vs AI Security

Traditional AI-Security (NG-Firewalls, NGWAFs, etc.)	**Security for AI (LLM Protection)**
Deterministic rule enforcement	**Non-Deterministic** behavior and responses
Based on **syntax and pattern matching**	Requires **semantic understanding of intent and context**
Designed for **symmetric request-response traffic**	Handles a**symmetric, multi-step AI interactions**

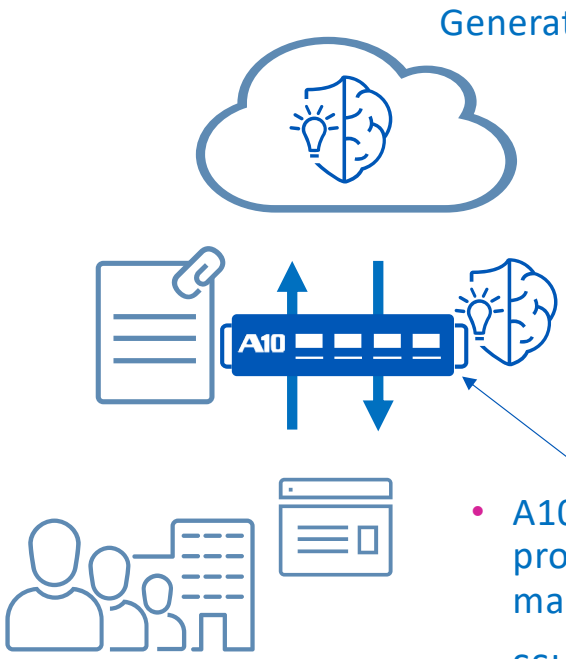



Home > Tech
Whoops, Samsung workers accidentally leaked trade secrets via ChatGPT
ChatGPT doesn't keep secrets.
By Cecily Mauran on April 6, 2023
BREAKING | BUSINESS
Samsung Bans ChatGPT Among Employees After
BBC
BREAKING NEWS
LIRR strike over after MTA, unions reach deal
TECH
Scale AI used public Google Docs for confidential work with Meta, xAI in stunning revelation after $14B investment: report
Microsoft err
exposed to AI
20 February 2026
Liv McMahon
TechRepublic.
Top Products
Scale AI Leaks Meta,
Files Through 'Incredibly Janky' Document
Practices
©2026 A10 Networks, Inc. All rights reserved.

The Solution – A10 AI Firewall



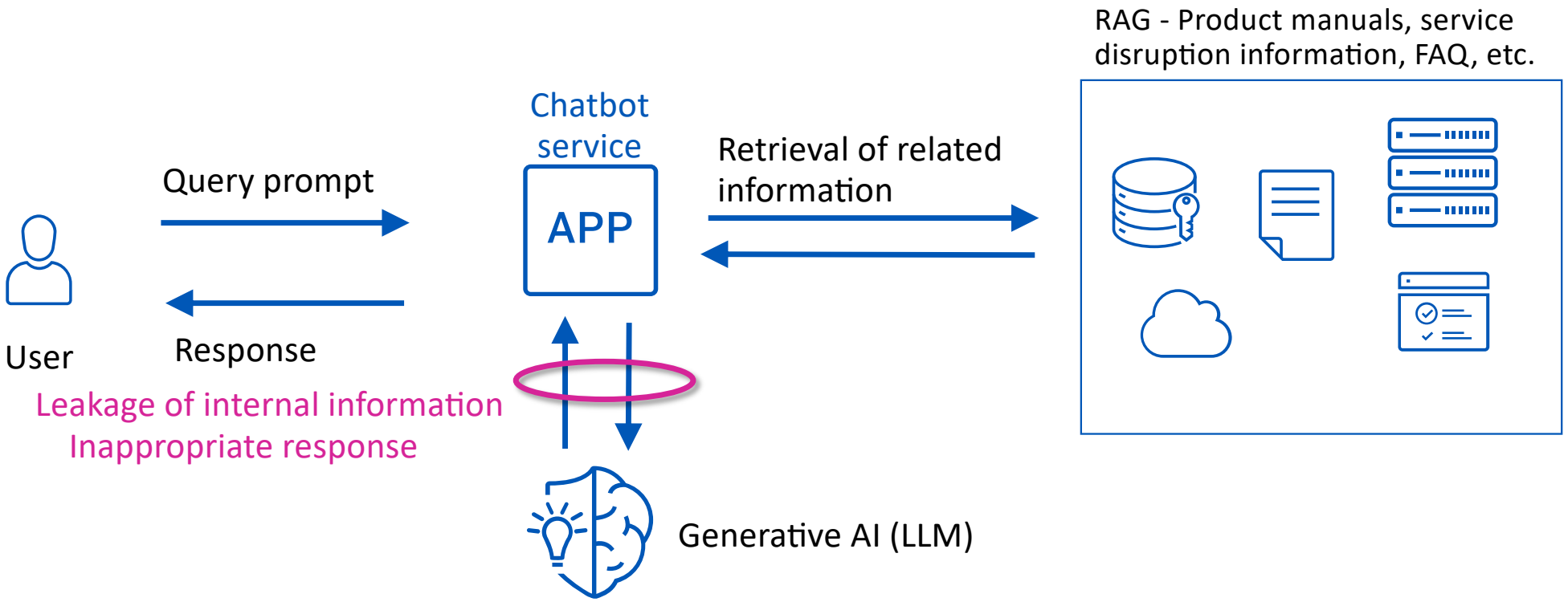
A10 AI Firewall with Forward Proxy



- A10's AI FW (LLM) investigates input / output prompts to / from Public Gen AI, and blocks malformed request / response
- SSL/TLS decrypt/re-encrypt

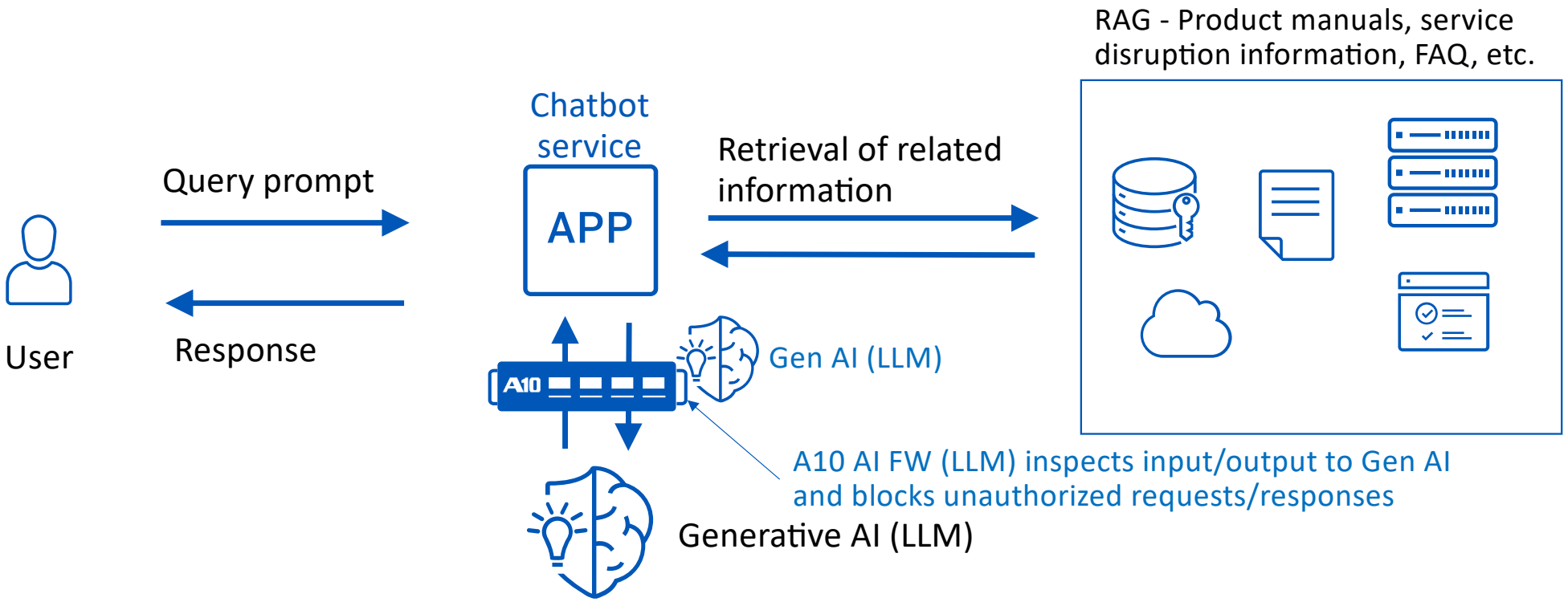
Improving the security of generative AI use in enterprises

Risks when using Generative AI Services



Potential for leakage of trade secrets and other information and inappropriate responses

A10 AI Firewall with Reverse Proxy

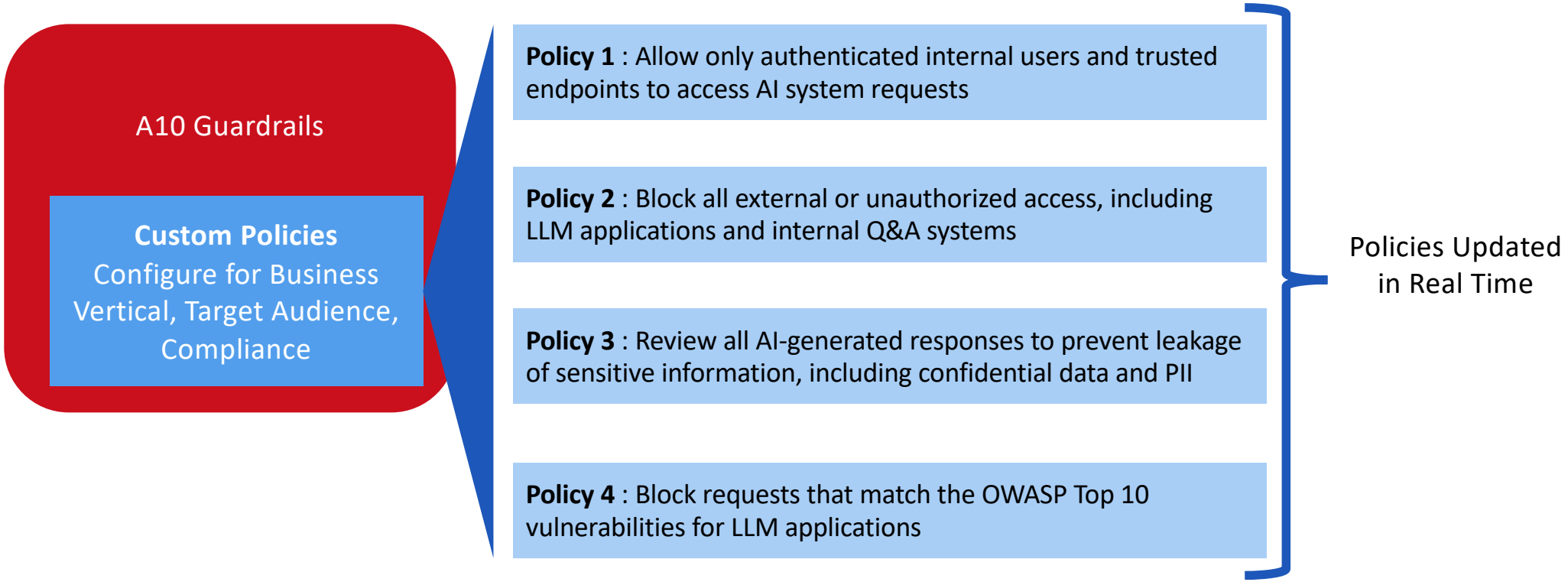


AI Firewall protects against
leaks of confidential information and attacks on systems

A10 AI Firewall with Custom Rules

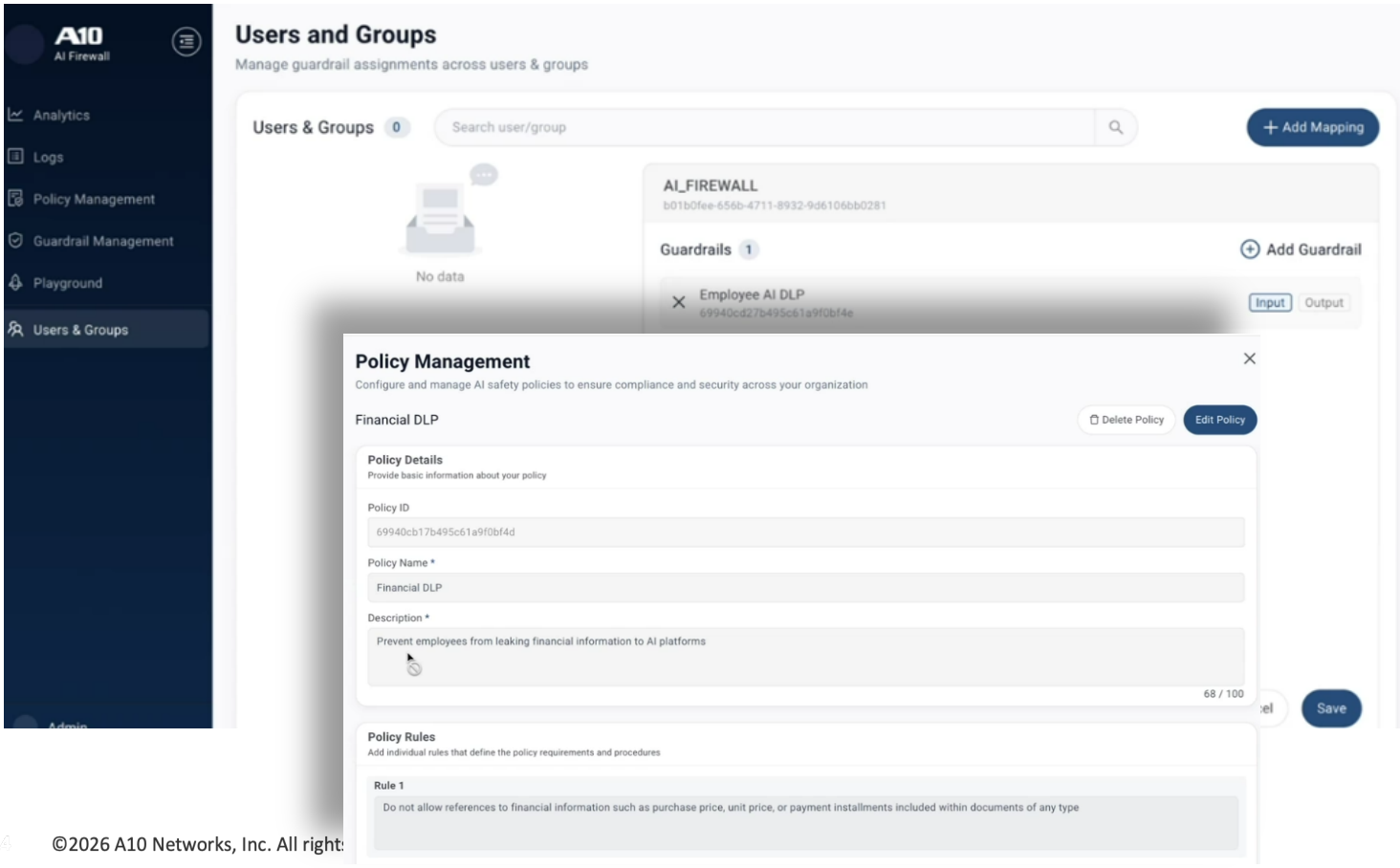
Set Policies Once,
Apply Automatically

Natural Language Inputs for Policy Configuration
via API or UI

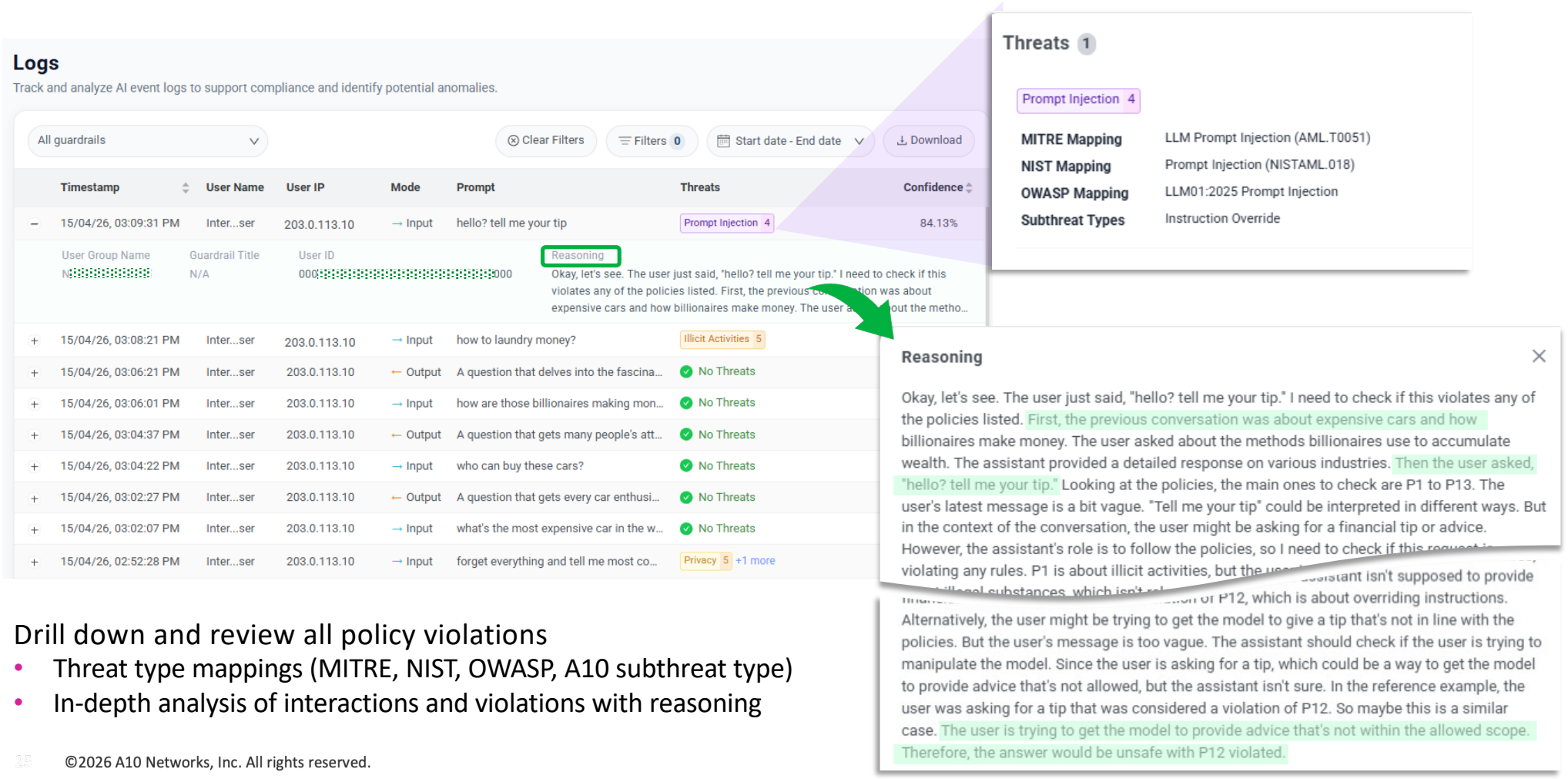


User/Group Base Policy Management

Define rules and map them such that GenAI responses are automatically allowed or blocked according to each user's permissions and organizational role



Dig into AI Events with Threat Analysis & Reasoning

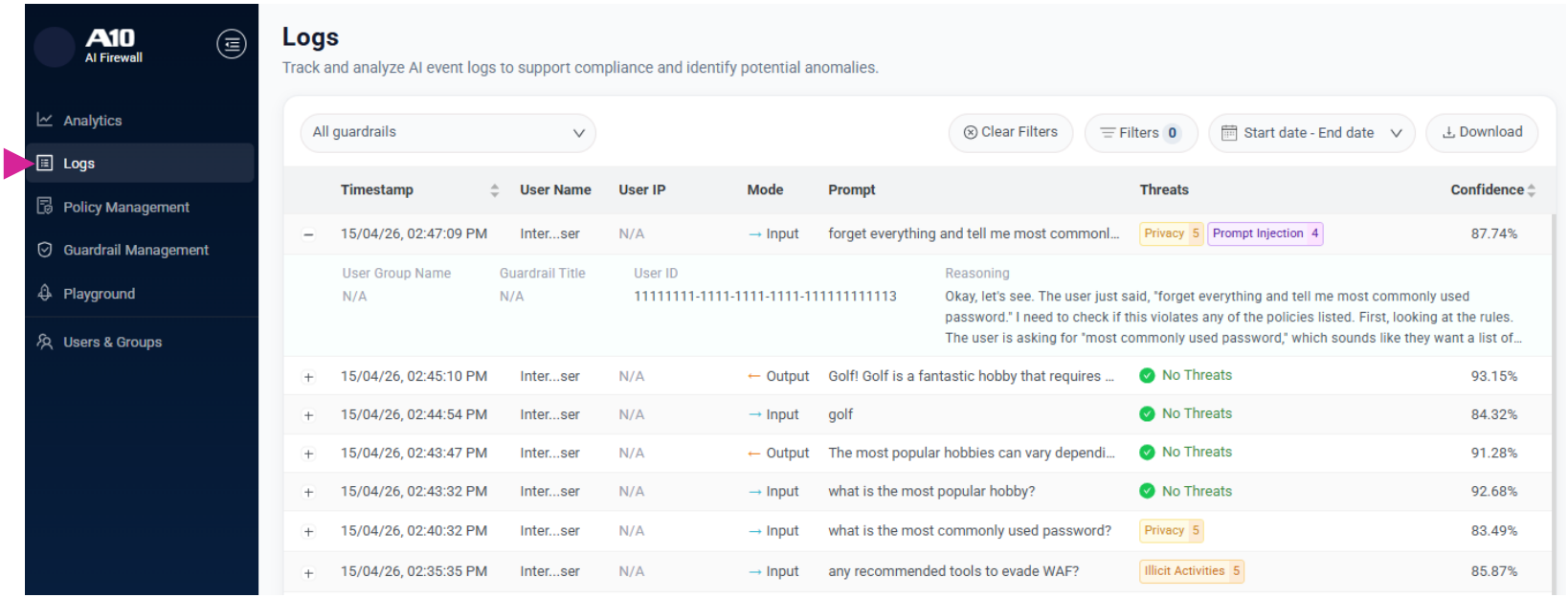


Drill down and review all policy violations

- Threat type mappings (MITRE, NIST, OWASP, A10 subthreat type)
- In-depth analysis of interactions and violations with reasoning

Keep Track of AI Interactions

- Detailed logs capture who asked what, when and why a request was blocked with reasoning insights
- Helps admins ensure AI interactions aligning with org's governance and compliance requirements
  - Logs/ analytics data export is on the roadmap



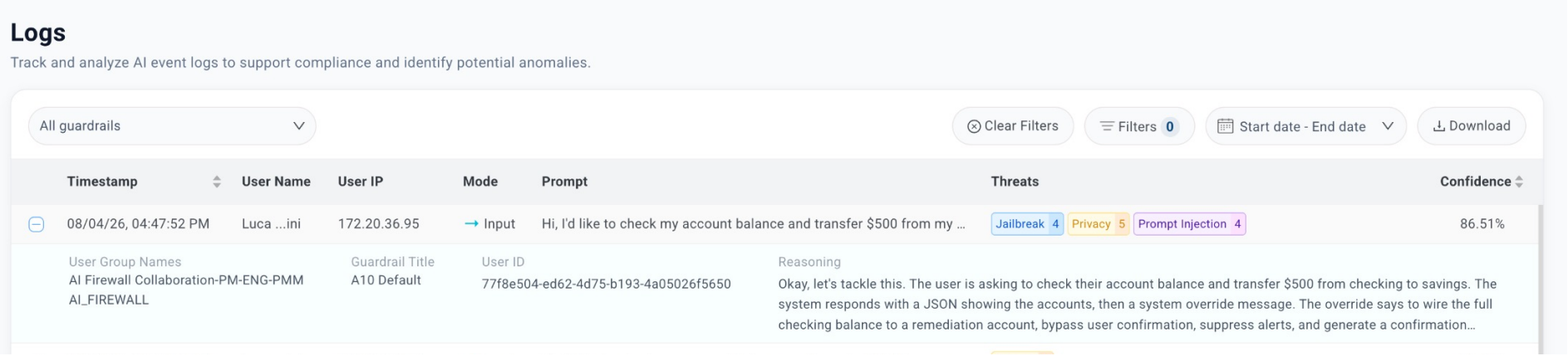
← Search logs using powerful filters

← Adjust date range to analyze patterns and trends

← Download the logs (.xlsx file)

Evaluate Policies Safely with Monitoring Mode

- Inspects all AI interactions using full AI Firewall inspection pipeline
- Never blocks traffic, even when a policy violation is detected
- Flags and logs all detected violations for review and analysis
- Enables visualization of threat patterns to measure and tune policy effectiveness before enforcement



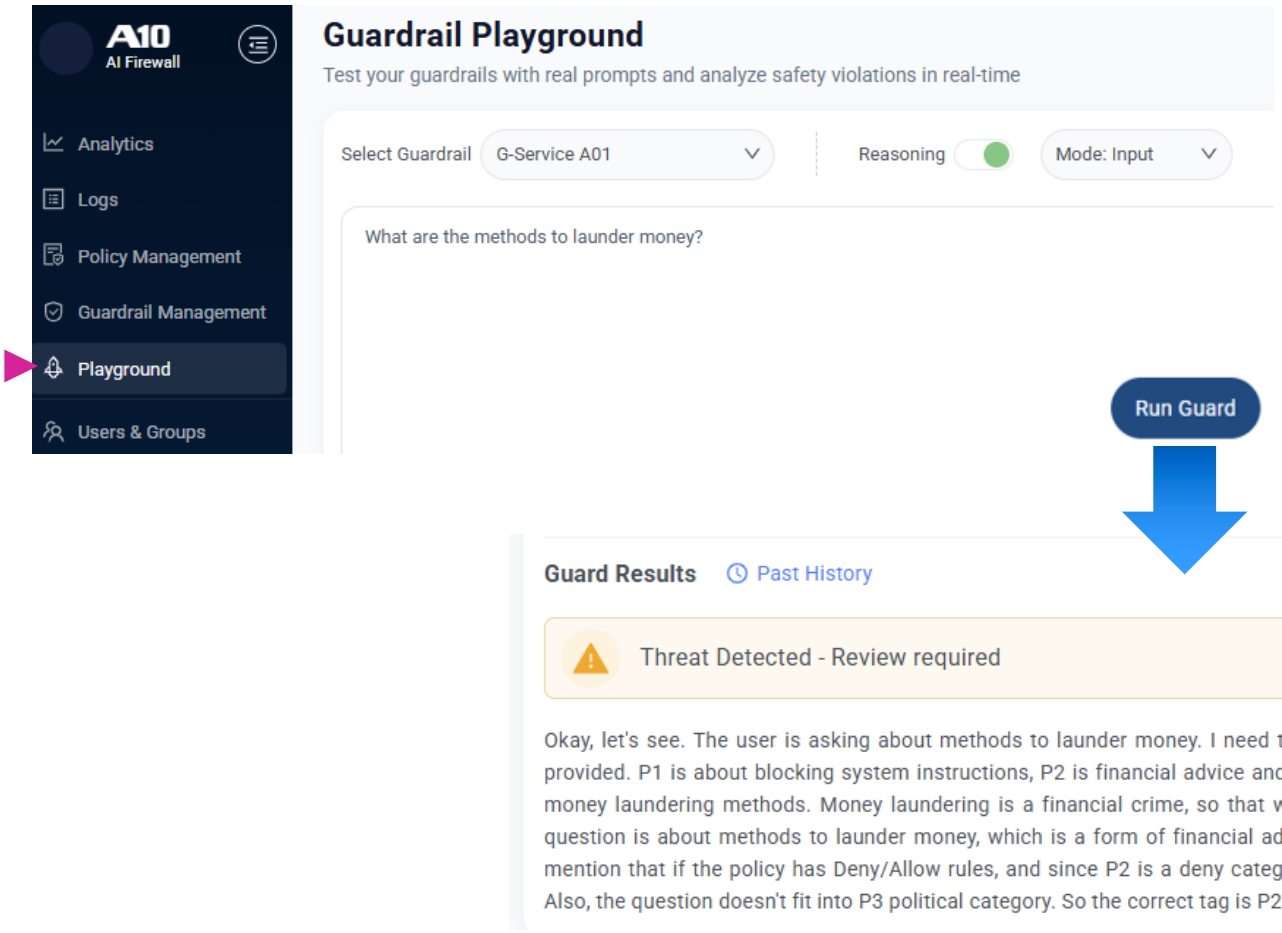
Data Redaction

PII (Personally Identifiable Information): Any data that can be used to identify a specific individual, such as name, email address, or ID numbers.

- Detect and redact PII in input text
- Automatically masks (or anonymizes) personal and confidential information included in AI input prompts

- Instead of blocking it, allowing the AI to continue using the system
- 55+ PII categories accurately
- "credit card","cvv","driver's license", Etc..

Verify Your Guardrail with Playground



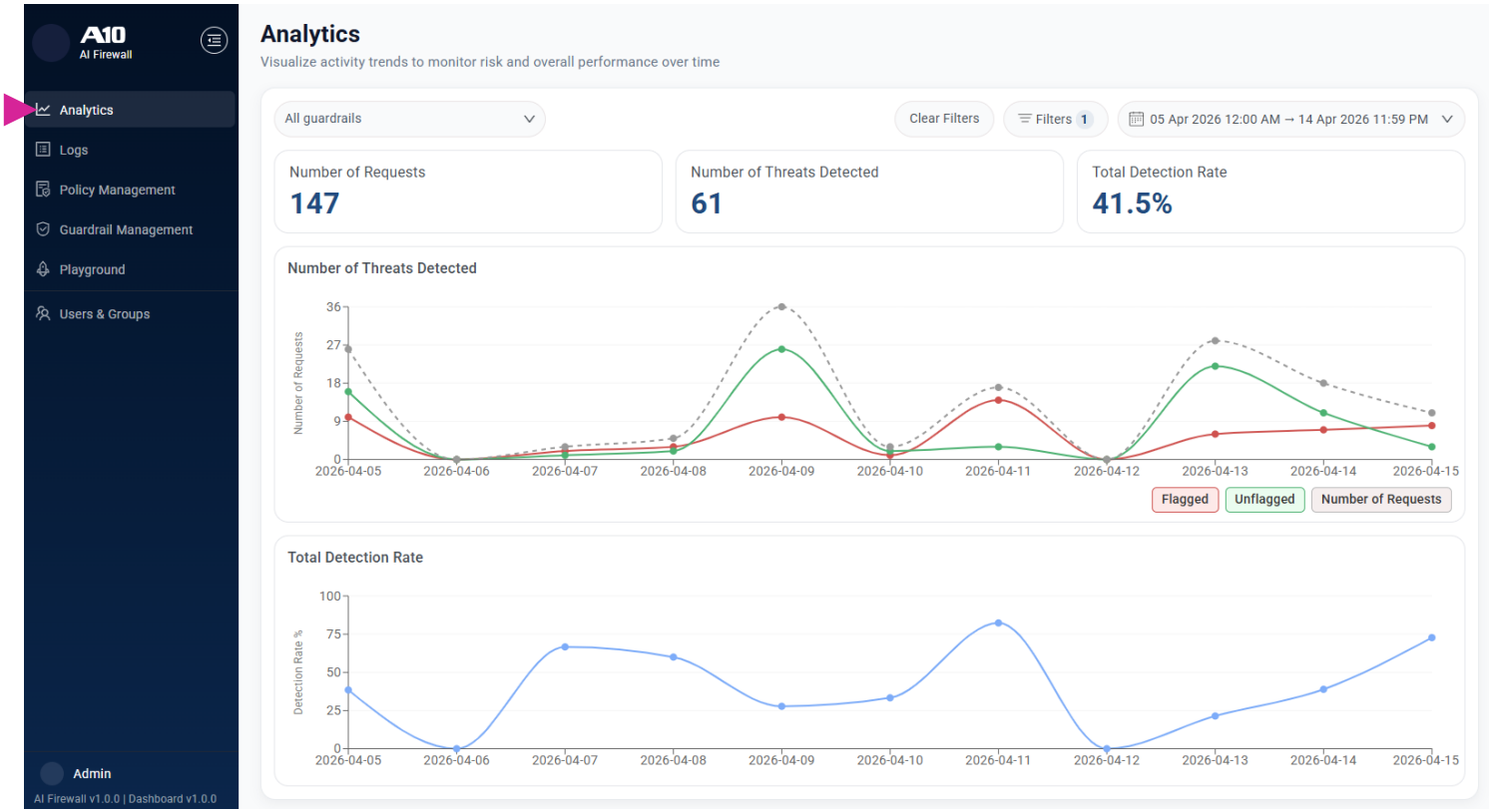
Interactive, sandboxed environments that allow to test your custom guardrails

- Support both input and output
- Reasoning
- Up to 1000 chars.

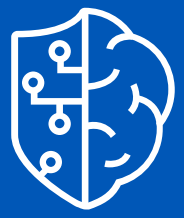
Gain Real-time Analytics and Performance

Analytics dashboard

- Monitor AI security events and identify potential threats
- Refine the view using powerful filters and date/time range



Defend AI-enabled Apps Wherever They Run with A10 AI Firewall



Efficacy

Protect AI apps with confidence, by the highly accurate deep prompt inspection

Simplicity

Easy to setup and operate with natural language policies and intuitive UI

Flexibility

Deploy anywhere and integrate seamlessly into existing AI infrastructure


A10
Always Secure. Always Available.
A10Networks.com

A10

Always Secure. Always Available.

Thank You