DATASHEET

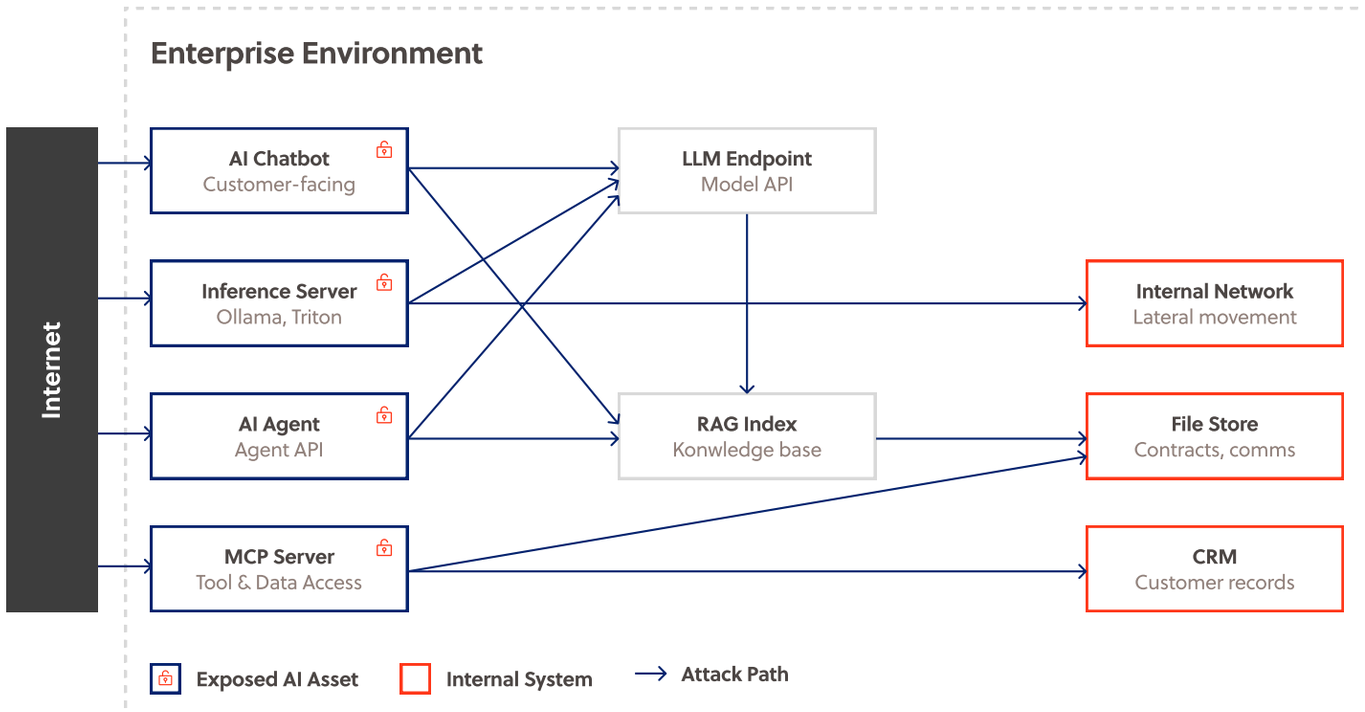
AI Exposure Management

Continuously manage your AI infrastructure.

AI is now part of your attack surface and is scaling fast. Teams stand up model endpoints, MCP servers, agents, and RAG pipelines on their own, and few ever reach your inventory. One in five organizations has already been breached through shadow AI, at an average of $670,000 in added cost.[1]

[1] IBM, Cost of a Data Breach Report 2025 IBM Newsroom (Jul 30, 2025)

How Compromised AI Assets Impact The Enterprise



Continuous AI Exposure Management

CyCognito closes that gap. It finds your AI assets and infrastructure the way an attacker would: from the outside in. It reveals what makes each one exposed, whether it can be compromised, and who owns it, then brings it into the inventory and workflows your security team already runs.

COVERAGE	PERSISTENCE	SCALE
Dozens of dedicated detection modules across the AI stack: AI chatbots, MCP servers, LLM endpoints, inference servers, and more, with new modules added as the AI ecosystem evolves.	CyCognito rescans your external surface daily, catching new and changed AI services as they appear, so your security team keeps pace with AI adoption as it scales.	Proven at Fortune 500 organizations with millions of assets. As AI deployments multiply across the business, CyCognito is ready to support any scale.

How It Works

CyCognito runs a continuous, five-stage pipeline across your external AI attack surface, where each stage feeds the next.

1 DISCOVER

CyCognito starts from public sources and builds a graph data model of all your assets, including your AI services, and the relationships between them. Each one is fingerprinted for unique identification, with supporting evidence (headers, banners, certificates, TLS configuration) and a probability score.

2 CONTEXTUALIZE

Discovery establishes that an asset exists; context establishes what it is and why it matters. CyCognito enriches each AI asset with:

- **Tech stack:** The framework, service, and version behind it.
- **Interconnections:** What the asset relates to and can reach.
- **Business criticality:** What data it holds, where, and who owns it.

Attribution and context carry evidence and certainty scores, so ownership and impact are provable.

3 VALIDATE

CyCognito runs the same active, safety-curated security testing across AI services that it runs across the rest of your external surface, confirming which externally reachable assets are actually exploitable: missing or unenforced authentication, misconfigurations, data exposure, and known CVEs. Every finding ships with the evidence behind it, keeping false positives low.

4 PRIORITIZE

CyCognito combines that business context, the validated exposures, and external threat intelligence (known vulnerabilities, exploit availability, attractiveness and discoverability) into a single risk score and grade. The output is a ranked, defensible short list of the AI exposures that can actually be compromised.

5 REMEDIATE

Owner-linked workflows route each finding to the team that owns the asset, with guided, per-issue remediation steps and an estimate of effort. After a fix is applied, CyCognito re-tests and re-discovers to confirm the exposure is closed.

IN PRACTICE

An externally reachable MCP server is left with inconsistent authentication enforcement. CyCognito discovers the reachable MCP service and attributes it to the subsidiary running it, enumerates the tools and schemas it exposes (the same introspection an attacker would use as an action map), validates that requests are accepted without enforced authentication, and routes a guided fix to the owner before a single exposed server becomes a gateway into downstream systems.

Surface Shadow AI

CyCognito closes that gap. It finds your AI assets and infrastructure the way an attacker would: from the outside in. It reveals what makes each one exposed, whether it can be compromised, and who owns it, then brings it into the inventory and workflows your security team already runs.

Support Safe AI Adoption

CyCognito gives security a defined, evidence-backed view of every reachable AI asset across the organization, so the business can move fast on AI while security keeps a clear picture of the exposure that comes with it.

One Inventory, AI included

CyCognito treats AI assets like any other exposed asset. They enter the same inventory, run through the same attribution and validation, and route to the remediation workflows your team already uses.

Comply with AI Standards

The rise of AI is creating new compliance standards and growing complexity. CyCognito keeps you in lockstep with the evolving requirements, covering the exposure and inventory provisions of NIST AI RMF, ISO 42001, and the EU AI Act today, and moving with new ones as they arrive.

CyCognito is an external exposure management platform that reduces risk by discovering, testing and prioritizing security issues. The platform scans billions of websites, cloud applications and APIs and uses advanced AI to identify the most critical risks and guide remediation. Emerging companies, government agencies and Fortune 500 organizations rely on CyCognito to secure and protect from growing threats.

To see how CyCognito surfaces and secures your
AI attack surface, contact your CyCognito account representative or email info@cycognito.com.