INFOSHEET

With AI Segmentation, Zero Networks gives you actual control.

AI is already in your environment. The question isn't whether to use it – it's whether you can scale it safely. Zero Networks is how organizations do both: use AI where and when they want, with the confidence that every agent, tool, and model operates within boundaries they actually control.

The tech world has responded to the AI wave by slapping "AI-powered" on products that haven't fundamentally changed, and optimizing for visibility when the problem demands control. Attacks now spread in as little as 27 seconds and a single compromised host can reach 85% of an environment in one hop. No detection chain was built to keep pace.

AI isn't a visibility problem. It's a control problem, on two fronts. Attackers are using AI to move faster than any response cycle can handle. And AI agents are already running inside your environment – accessing data, connecting externally, operating with privileges nobody explicitly signed off on.

Most vendors address one or neither. Zero controls both.

Zero Networks on AI: No Hype, Just What Works

Most security vendors treat AI as something to bolt on. Zero Networks treats it as a tool with specific strengths – and intentional limits. And its already embedded in our platform.

AI DOES THIS

Visibility, investigation, and risk scoring

AI surfaces what matters – letting teams query live network activity in plain language, identify anomalous behavior across billions of connections, score risk against frameworks like NIS2 and CIS, and see which AI tools are running in the environment.

ZERO'S DETERMINISTIC ENGINE DOES THIS

Enforcement, containment, and policy

Security controls must be exact. Even a 1% error rate in segmentation can break applications and disrupt operations. Zero's policy engine is deterministic: it's based on real network behaviors. No probabilistic guesswork where the stakes are too high for "probably right."

AI helps humans understand the network. *A deterministic approach protects it.*

AI Segmentation: Three Capabilities. One Platform.

AI Visibility + Control

Saas AI Control

Not every AI tool your employees can reach is one you've approved. Zero governs which cloud AI services – ChatGPT, Gemini, Copilot, and others – users and devices can access at the network layer. If you're paying for Copilot, nothing on your network should be reaching ChatGPT. Zero enforces that automatically.

AI Agent Control

Every AI agent running in your environment is a process – and like any process, it has an identity. Zero applies the same controls governing every user and device to every AI agent in your environment. Identify which agents are running, what they're accessing, and how they communicate – while enforcing strict least-privilege boundaries on every interaction.

LLM Protection

Your LLMs – like code – can be tampered. Bad data, invisible backdoors installed, behavior quietly poisoned. Think SolarWinds, but for your AI models. Zero segments your model infrastructure at the network layer so only authorized systems can reach it. You can't tamper with what you can't reach. And a compromised model can't act on what it can't access.

AI Lateral Movement Control (AILM)

Stop the spread of both AI-driven attacks and autonomous agent activity by eliminating lateral movement at its source. By enforcing identity- and network-based least privilege, Zero Networks removes unnecessary connectivity across the environment – ensuring unauthorized users, systems, or AI agents cannot access critical resources, regardless of how the attack was initiated.

AI-Powered Compliance & Risk Engine

Embed AI into security operations to simplify investigation and continuously prove compliance. Query live network activity in natural language and analyze behavior across billions of connections, while the platform evaluates activity against frameworks like NIS2 and CIS Benchmarks – assigning dynamic risk scores and identifying the most critical gaps in real time.

The Bottom Line

AI gives attackers speed. Zero takes away the open network they'd move through.

Every AI agent in your environment gets the same identity-based controls you already apply to users and devices. Every path an attacker would move through gets closed before it can be used. And the same platform that does both continuously scores your risk posture and maps it to the frameworks your board and auditors care about.

Not dashboards. Not alerts – just control and enforcement.

Contain AI, don't chase it.

Govern AI agents. Stop lateral movement. Prove compliance – continuously.

Request a Demo →

ZERO Networks