Complete visibility into every AI conversation.

AI Monitoring & Governance in Your Azure Tenant

AI Sentry monitors every prompt and completion across all major AI providers — catching prompt injection, sensitive data exposure, credential leakage, and insider misuse. Deployed inside your Azure tenant.

CAPTURES FROM	DETECTION	DEPLOYED IN	FEEDS
Claude, ChatGPT, Gemini & more	3-tier · patterns → LLM judge → human	Your Azure tenant	Microsoft Sentinel & Purview

THE BLIND SPOT

Generative AI is everyday reality. But while you have telemetry for endpoints, identities, and cloud workloads, **AI usage remains a blind spot.** Shadow AI, prompt injection, data exfiltration, and insider misuse bypass traditional controls — and the EU AI Act, NIS2, DORA, and ISO 27001 are still catching up.

80%

of business leaders worry sensitive data could slip through the cracks due to unchecked AI use.

— Microsoft Digital Defense Report 2025

HOW IT WORKS

Three tiers, from line rate to human judgement

Every prompt and response flows through escalating layers of inspection. Your team only looks when a finding says so.

TIER 1 Pattern Detection

Real-time inspection of every prompt and response — catching prompt injection, PII, credentials, and sensitive patterns at line rate.

TIER 2 Deep Contextual Analysis

An LLM-as-judge running inside your Azure tenant reviews flagged conversations end-to-end, classifying manipulation attempts and data exfiltration in full context.

TIER 3 Human in the Loop

SOC analyst and Compliance officer review portal for classified incidents. Alerts and full conversation context flow into Microsoft Sentinel and Defender XDR.

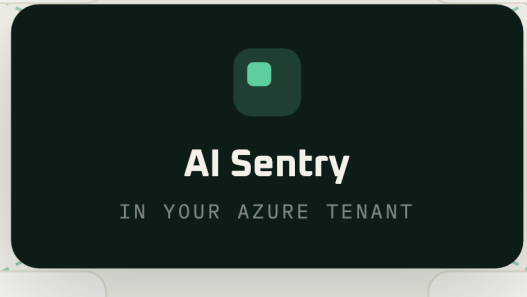
THE MICROSOFT SECURITY STACK

Extends your stack — doesn't replace it

AI Sentry plugs directly into the Microsoft security tools you already run.

Microsoft Sentinel
SIEM — incidents & transcripts correlate with your telemetry.

Microsoft Defender XDR
Unified incident triage across endpoint, identity & email.



Microsoft Purview
DLP sensitivity labels enforced on prompts & completions.

Azure AI Foundry
Governance of models & agents deployed on Foundry.

TWO DEPLOYMENT MODES

Passive Monitoring

Zero-impact observation. For visibility-first programmes.

Active Gateway

In-line blocking and policy enforcement. For teams ready to act in real time.

COVERAGE ACROSS THE AI ESTATE

`Anthropic Claude` `ChatGPT` `Google Gemini` `+ any other major provider`

One policy framework. Consistent detection regardless of vendor.

WHY CHOOSE NOIBIT

Red and Blue, under one roof

01 **Red + Blue under one roof**
Managed SOC and Red Team experience in a single partner — we know the attack, so we build the defence.

02 **Microsoft-native by design**
Direct integration with Microsoft Sentinel, Defender XDR, Purview, and Azure AI Foundry — it extends your stack, not replaces it.

03 **Self-sustained engagement**
We deploy, tune, and hand over. Your team keeps control — production-ready in days, not quarters.

04 **Proven across enterprise and public sector**
Trusted by regulated industries and critical infrastructure, where your data must stay in your control.

CREDENTIALS & CERTIFICATIONS

- ✓ **ISO 27001 · NIS2 · DORA**
  Certified information security, aligned to EU regulation.
- ✓ **ISO/IEC 27701**
  Privacy information management.
- ✓ **ISO 9001**
  Quality management system.

AI is in your organisation. The telemetry should be too.

Book a walkthrough of AI Sentry.

noibit.com