vijilan
IT Security: Enabled

MANAGED AI DETECTION & RESPONSE (AIDR)

DATASHEET

The industry's first fully managed AIDR service — powered by enterprise-grade AI security technology trusted by 60% of the Fortune 500. Vijilan deploys, configures, and operates it 24/7 through our global SOC.

99%	<30ms	50+	180+
Prompt injection detection efficacy	Inline inspection latency	PII & PHI types detected & redacted	Prompt injection techniques tracked

The Problem

AI Has Created a New Attack Surface. Most Organizations Are Blind to It.

80% of employees use AI tools at work — most without IT approval. Adversaries are exploiting this: prompt injection attacks now rank #1 on OWASP's LLM Top 10, and AI-enabled attacks increased 89% year-over-year (CrowdStrike 2026 Global Threat Report).

Traditional security tools — EDR, SIEM, identity — cannot see inside a prompt. They protect infrastructure. They were never designed to monitor the AI interaction layer.

THE STAKES

Shadow AI Is Now a Leading Breach Vector

IBM's 2025 Cost of a Data Breach Report found organizations breached via Shadow AI paid an average of $670,000 more per incident than standard breaches. 63% of organizations have no AI governance policy.

80%	73%	89%	29min
Employees using unapproved AI	AI systems vulnerable to injection	YoY increase in AI-enabled attacks	Avg eCrime breakout time

The Solution

Managed AIDR: Full-Lifecycle AI Security. Fully Operated.

Vijilan's Managed AIDR service extends your security stack to the AI interaction layer. We deploy, configure, and continuously operate AI Detection and Response — monitoring every prompt, response, agent action, and data flow — through our 24/7 global SOC.

AIDR telemetry integrates directly into Falcon Next-Gen SIEM alongside endpoint, identity, and cloud signals. Your SOC analysts see AI threats with full cross-domain context. One platform. One workflow. Complete visibility.

- Shadow AI discovery & continuous inventory
- Real-time prompt injection detection & blocking
- PII/PHI/IP redaction before AI model exposure
- Agentic AI monitoring via MCP Proxy
- Immutable audit logging with cryptographic signing
- AI governance policy enforcement & reporting
- Compliance evidence generation (HIPAA, PCI, SOC 2, GDPR)

Six Collector Types

Collector	Coverage
Browser	ChatGPT, Copilot, Claude, Gemini in managed browsers (Chrome, Edge, Firefox)
Application	Enterprise AI apps via SDK (Python, Node.js, Go, Java, C#) + OpenTelemetry
Agentic	AI agent-to-agent communications via MCP Proxy (all tool calls & instructions)
Gateway	Kong, LiteLLM, Portkey, Apigee, Azure API Management
Cloud	AWS Bedrock, cloud AI infrastructure via S3 log ingestion
Endpoint	Desktop AI apps: ChatGPT, Copilot, GitHub Copilot, Cursor

© 2026 Vijilan Security, LLC. All rights reserved. vijilan.com

Core Capabilities

Prompt Injection Defense

Detects 180+ injection techniques using heuristics, neural classifiers, and dedicated GPU/CPU analyzers. Blocks direct and indirect injection in real time at sub-30ms latency.

AI Data Leakage Prevention

Detects 50+ PII/PHI/IP types. Redaction via masking, hashing, or format-preserving encryption. Inspects both inputs to AI models and outputs returned to users.

Agentic AI Control

MCP Proxy captures all agent tool calls, agent-to-agent communications, and autonomous decisions. Detects rogue behavior and manipulated agent workflows.

Shadow AI Discovery

Continuously inventories AI applications, LLM runtimes, MCP servers, IDE extensions, and cloud AI services across all managed endpoints and networks.

Immutable Audit Logging

Cryptographically signed, tamper-proof logs of all AI interactions. Supports HIPAA, SOC 2, PCI-DSS, and GDPR audit requirements. Fail-safe redaction prevents sensitive data in logs.

SOC Integration

AIDR telemetry streams into Falcon Next-Gen SIEM. 24/7 human analysts triage AI alerts with full endpoint, identity, and cloud correlation. One team. One platform.

Detection Engine

Nine Analyzer Types. Layered Defense-in-Depth.

AI Guard uses configurable policy recipes across the full AI data flow — from RAG ingestion through model input, model output, agent planning, and tool execution. Each recipe applies relevant analyzers for that stage of the pipeline.

- **Malicious Prompt** — Injection, jailbreak, role-play bypass detection
- **Confidential & PII** — 50+ entity types with redaction/FPE
- **Malicious Entity** — URLs, IPs, domains via threat intel feeds
- **Topic Control** — Toxicity, weapons, financial/health advice blocking
- **Custom Entity** — Organization-defined sensitive terms and patterns
- **Code Detection** — IP protection across 26 programming languages
- **Language Detection** — Allowlist/denylist enforcement
- **Prompt Hardening** — In-context cautionary instruction injection
- **Image Analysis** — Sensitive/inappropriate image content detection

Three Deployment Models

- **SaaS** — Fully hosted, zero infrastructure overhead
- **Edge** — Hosted control plane, customer-cloud data processing (AWS/Azure/GCP)
- **Private Cloud** — Fully self-managed for maximum data sovereignty

Performance Benchmarks

Enterprise-Grade. Zero Compromise.

99% Injection detection efficacy	**<30ms** Inline latency	**180+** Injection techniques tracked
50+ PII types detected	**26** Languages for code detection	**8/10** OWASP LLM risks covered

© 2026 Vijilan Security, LLC. All rights reserved. vijilan.com

Regulatory Compliance

Built for the Frameworks Your Clients Must Meet.

HIPAA

PHI detection & redaction. Tamper-proof audit logs. BAA-ready.

PCI-DSS v4

Cardholder data protection. Format-preserving encryption. Validated flows.

SOC 2 Type II

All five trust service criteria. Cryptographic audit trail.

GDPR / NIS2

Data residency options. Shadow AI discovery for data subject rights.

EU AI Act

Risk classification, technical docs, human oversight enforcement.

NIST AI RMF

All four functions: Govern, Map, Measure, Manage.

CMMC 2.0

CUI protection in AI workflows. AI control mapping.

ISO 27001

AI-specific Annex A controls. Continuous risk management.

Why Vijilan

CrowdStrike Powered

Authorized CPSP delivering AIDR natively on the Falcon platform. The same technology trusted by 60% of the Fortune 500, fully managed by Vijilan's global SOC.

24/7 Global SOC

Human analysts across global SOC locations. AI alerts correlated with endpoint, identity, and cloud telemetry — one team, one platform, complete cross-domain context.

Dual-Certified

SOC 2 Type II and ISO 27001 certified. Vijilan holds the same standards we help clients enforce — independently verified, continuously maintained.

Vijilan Security — Premium Managed Cybersecurity
vijilan.com • SOC 2 Type II • ISO 27001 • CrowdStrike CPSP

To learn more or schedule a consultation:
vijilan.com/msp-partner-program

© 2026 Vijilan Security, LLC. All rights reserved. vijilan.com