AI SECURITY & SOFTWARE SECURITY

AGENTIC DEFENSE FOR THE MODERN ENTERPRISE

Vijilan's 24/7 Expert SOC | CrowdStrike Falcon® AI-Native Platform

THE THREAT LANDSCAPE

Modern attacks start with stolen credentials. 80% of breaches involve identity compromise, yet most tools only detect policy violations—not active exploitation. Vijilan's ThreatRemediate Identity Protection, powered by CrowdStrike Falcon Identity, shuts down credential abuse in real time and stops lateral movement before damage is done.

THE VIJILAN + CROWDSTRIKE ADVANTAGE

Vijilan delivers fully managed, AI-powered cybersecurity through the CrowdStrike Falcon® platform—combining world-class technology with a 24/7 US-based expert SOC that doesn't just detect threats, but actively contains and remediates them.

98%+	<30ms	100%
AI Triage Accuracy	AI Prompt Blocking Latency	MITRE ATT&CK Detection

PLATFORM ARCHITECTURE

The Falcon platform is a single-agent, cloud-native architecture designed for rapid deployment and minimal system impact, managed end-to-end by Vijilan's expert team.

SPECIFICATION	DETAIL	SIGNIFICANCE
Delivery Model	Cloud-Native SaaS	Zero on-prem infrastructure required
Agent Footprint	40–50 MB disk / ~40 MB RAM	Deploys on legacy and constrained systems
CPU Usage	Typically < 1%	No performance degradation
Update Architecture	Cloud-native, zero-reboot	Continuous protection, no downtime
Supported OS	Windows, macOS, Linux, iOS, Android	Full cross-platform coverage
SOC Operations	Vijilan 24/7/365 US-Based SOC	Expert human oversight + AI automation

AI SECURITY CAPABILITIES

As generative AI expands the attack surface, Vijilan and CrowdStrike secure the full AI lifecycle—from prompts to infrastructure.

CHARLOTTE AI — Generative AI for SOC Operations

Charlotte AI is a telemetry-driven AI assistant managed by Vijilan analysts that accelerates SOC operations with 98%+ alert accuracy, natural language-to-query translation, unified incident summarization, instant script decryption, and no-code security agent automation.

FALCON AIDR — AI Detection & Response

Real-time security for AI interactions: prompts, agentic workflows, and model outputs—the "EDR moment for AI."

COLLECTOR	DEPLOYMENT	COVERAGE
Browser	Managed Extension	Employee use of ChatGPT, Claude, and public GenAI tools
Application	SDKs (C#, Python, Go)	Custom-built AI applications and internal LLM integrations
Agentic	MCP Proxy	Interactions between autonomous AI agents and servers
Gateway	API Boundary	Centralized monitoring of AI/API traffic (e.g., Kong)
Cloud	Native Cloud Service	AWS Bedrock, Vertex AI, Azure OpenAI telemetry

It blocks direct and indirect prompt injection attacks with sub-30ms latency, prevents data leakage by identifying and stopping credentials, PII, and source code before they reach external AI systems, and sanitizes outputs by removing toxic language and malicious URLs from AI-generated responses.

AI-SPM— AI Security Posture Management

Agentless visibility and protection for the infrastructure that powers AI—eliminating Shadow AI and securing the development pipeline.

- **Shadow AI Discovery:** Exposes the complete organizational AI footprint—every unsanctioned model and service in use.
- **Model Security Scanning:** Proactively scans AI models in containers for hidden malware, trojans, and backdoors.
- **Shift-Left CI/CD Integration:** Registry scanning, runtime image assessment, and dependency mapping across the SDLC.

vijilan
IT Security: Enabled

SOFTWARE SECURITY CAPABILITIES

Beyond AI-specific security, Vijilan manages the full CrowdStrike Falcon software platform to deliver unified protection across endpoints, identities, vulnerabilities, and cloud workloads.

ENTERPRISE GRAPH — The Foundation for AI Reasoning

A living, connected model of your organization unifying telemetry across all security domains.

GRAPH LAYER	FUNCTION
Threat Graph	Tracks process lineage and behavioral patterns—the "how" of an attack—correlating events into coherent adversary narratives.
Asset Graph	Real-time inventory of all systems, devices, and cloud workloads—the "where"—with criticality and ownership context.
Intel Graph	Maps behaviors against TTPs of 200+ tracked threat actors—the "who"—providing immediate adversary attribution.
Risk Graph	Dynamic risk scoring for every entity based on configurations, privileges, and environmental factors for prioritized remediation.

IDENTITY PROTECTION — AI-Driven UEBA & ITDR

Transforms identity from the #1 attack vector into a defensive asset through behavioral analytics and autonomous response.

- **Behavioral Baselines:** AI establishes baselines for every human, machine, and AI identity across authentication, protocol, and resource access patterns.
- **Autonomous Response:** Dynamically enforces MFA or blocks access when baselines are violated—stopping adversaries mid-attack without human intervention.
- **Algorithmic Account Linking:** NLP-powered identification of orphan, shadow, and duplicate accounts across domains for unified risk scoring per individual.

ExPRT.AI — Predictive Vulnerability Management

Replaces static CVSS scoring with real-time exploit prediction powered by adversary intelligence and global telemetry.

- **Dynamic Risk Ratings:** Continuously updated based on adversary TTPs, dark web activity, and platform-wide exploitation data.
- **Predictive Prioritization:** Identifies vulnerabilities likely to be exploited before exploitation occurs—surgical patching replaces brute-force remediation.
- **Operational Efficiency:** Focus on dozens of truly exploitable CVEs instead of struggling with thousands of "High" CVSS scores.

CERTIFICATIONS & COMPLIANCE

VIJILAN	CROWDSTRIKE
• ISO 27001 Certified • SOC 2 Type 2 Certified • HIPAA, PCI DSS, GDPR, CMMC Support	• 100% MITRE ATT&CK Detection (Round 5) • 100% Ransomware Prevention (SE Labs) • ISO 42001 Responsible AI Certification

Ready to Experience Security Without Compromise?

Contact your Vijilan partner representative or visit vijilan.com to schedule a strategic consultation.

vijilan.com | partners@vijilan.com

vijilan
IT Security: Enabled