CyAI – AI-Powered Advanced Threat Detection Engine for Cynet's All-in-One Cybersecurity Platform

Stop threats before they start with real-time, machine learning-based detection.

CyAI brings machine-learning accuracy and 24x7 SOC expertise together, giving MSPs and SMB IT teams enterprise-grade protection with zero extra overhead.

Cyber threats are growing faster than ever, and small security teams are overwhelmed by endless false alerts. CyAI cuts through this noise with continuously trained machine-learning models that inspect every executable on every endpoint. It reduces false positives by 90% and detects real and zero-day threats before they can cause harm. This level of precision makes Cynet's All-in-One "security on autopilot" vision possible. Teams benefit from full protection and complete detection visibility plus round-the-clock CyOps security experts who respond immediately, giving MSPs and SMEs enterprise-grade defense without enterprise-sized teams.

Why CyAI Matters

Challenge	Impact on MSPs & SMBs	CyAI Advantage
Exploding malware variants with tens of thousands of new executables each day	Signature-based AV lags behind; threats bypass defenses	Real-time ML scoring of every executable stops both known and zero-day attacks
Alert fatigue & false positives	Burned-out analysts, wasted time on tickets, missed SLAs	90% reduction in false positives keeps teams focused on what matters
Resource constraints	Limited staff & budget hinder advanced security	AI detection + built-in 24x7 Cynet CyOps security experts = instant expertise with no new headcount

What Is CyAI?

A proprietary machine learning antivirus engine embedded within the Cynet All-in-One Platform.

Trained on millions of benign and malicious samples

Treats anything ≥ 99% probability as malicious, triggering Cynet's automated response workflows and playbooks

Operates completely signature-less with no dependency on resource-intensive, daily pattern updates

Delivers a probability score (0–100%) for every .PE .EXE and .DLL encountered

How CyAI Works

Threat Verdict & Alerts

Unified "Malicious Binary" alert in Cynet console; auto-remediation handled by other AV layers to prevent duplicates.

Deep Analysis Cloud Loop

Each verdict feeds anonymized telemetry into Cynet cloud; models are retrained and hot-swapped without customer effort.

Smart Scoping

Scans defined directories with per-tenant granularity.

Feature Extraction on-device

Static & behavioral attributes fed into a lightweight ML model.

Local ML Model Inference

Sub-50ms scoring, even offline.

Use-Case Snapshots



100% Detection Visibility

Catch threats that other systems miss with CyAI and proven 100% MITRE ATT&CK® Protection & Visibility.



Boost Incident Response

Catch lingering "leftover" binaries that other engines miss; accelerate forensics with rich alert context.



Replace Legacy AV Systems

Replace antiquated AV systems that rely on complex, daily signature updates; keep endpoints safe, secure, and compliant.

Key Benefits & Outcomes

90% Fewer False Positives

Less noise = faster triage, happier, more secure customers

Immediate Zero-Day Coverage

Blocks unknown malware the first time it appears

No-Latency On-Device Detection

Stops threats before execution, even when offline

Seamless SOC Handoff

Cynet's 24x7 CyOps security experts validate & guide next steps

Single-Click Enablement

Quickly enable CyAI using the standard AV feature flag inside the Cynet Console

100% Mitre Att&Ck® Protection & Visibility

Independently validated confidence across detection, protection, and technique coverage with zero false positives

Benefits

Why Cynet

Cynet's All-in-One Cybersecurity Platform unifies a full suite of security capabilities on a single, simple solution, backed by 24x7 SOC support. Cynet is purpose-built to enhance protection for small-to-medium enterprises and to maximize margins for MSPs.

For more information, visit www.cynet.com