CYWARE™ | Solution Brief

Cyware Quarterback AI:
AI Fabric for Accelerating Threat Intel Actioning

The Threat Intelligence Operations Challenge

Modern security operations are drowning in data but starving for insights. Analysts spend countless hours on repetitive, error-prone tasks, parsing reports in multiple formats, correlating indicators, and custom workflows.

How Cyware Quarterback AI Accelerates Threat Intelligence Actioning

Cyware Quarterback AI applies an AI fabric that acts as a connected layer of threat intelligence management that powers every Cyware product by embedding AI into every stage of the threat-to-response workflow.

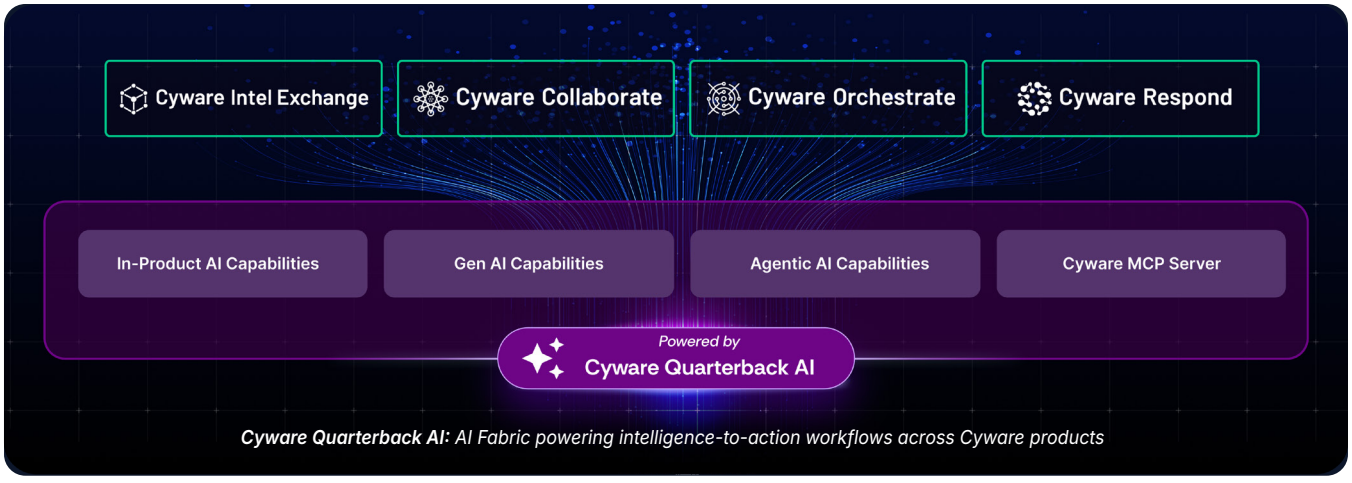
It converts unstructured threat data into actionable insights, automates decisions, and accelerates incident response with unmatched precision and speed.

From AI-powered threat intel parsing and summarization in Cyware Intel Exchange to intelligent playbook generation, troubleshooting, and automation in Cyware Orchestrate, AI is woven throughout the Cyware ecosystem, creating a high-velocity SOC where human expertise and machine intelligence work as one to outpace evolving threats. The Cyware MCP Server further extends the AI capability by enabling natural language interaction within threat intelligence workflows, allowing analysts to query, summarize, and act on data through conversational AI.

Cyware Quarterback AI

The AI Fabric is woven into your security workflows, combining the power of in-product AI, generative AI, and agentic AI, enabling you to:

- **Get Faster Access to Critical Threat Intelligence**
- **Accelerate Threat Investigations**
- **Orchestrate Security Workflows at Machine Speed**
- **Rapidly Operationalize Threat Intelligence**



Cyware Quarterback AI: *AI Fabric powering intelligence-to-action workflows across Cyware products*

CYWARE™

How Cyware Quarterback AI Enables Security Teams to Operationalize Threat Intelligence Management and Actioning

Cyware Quarterback AI consolidates all AI capabilities into an AI Fabric, including generative and agentic AI, into a single, connected layer of threat intelligence management.

With AI directly embedded into the platform, security teams can act faster, make smarter decisions, and orchestrate responses with precision.

Cyware Intel Exchange

Threat Intelligence Parser: Automatically extracts IOCs, TTPs, threat actors, malware, vulnerabilities, and recommended actions from text, documents, or websites, eliminating the manual effort of data collection and entry.

Threat Intel Summarization: Provides instant summaries of threat intelligence reports and related objects (e.g., IOCs, malware, threat actors), helping analysts quickly digest information and reduce alert fatigue. By accelerating knowledge discovery, it supports faster incident response.

Advanced Threat Intel Crawler (Browser Plugin): Instantly converts threat intelligence from websites into structured, enriched data. Eliminates manual scraping, reduces human error, and speeds up ingestion for fast, reliable threat data capture. Compatible with Google Chrome and Microsoft Edge.

Cyware Collaborate

Cyware Security Advisories: A generative AI-powered capability that transforms the daily deluge of open-source threat alerts, research data, bulletins, and cyber threat intelligence reports into a continuous stream of high-fidelity threat advisories.

Cyware Respond

Connect the Dots Context Recommendations: Provides AI-generated insights to surface contextual links that enhance analyst productivity. This feature automates the gathering and connection of contextual information, helping analysts quickly identify root causes, understand the full scope of complex threats, and uncover hidden patterns that are difficult to detect manually.

Cyware Orchestrate

Playbook Builder Agent: Simplifies playbook creation on Cyware cloud deployments with an intuitive, LLM-assisted interface that turns natural language descriptions into workflows. By leveraging Cyware's extensive library of actions and integrations, it accelerates security automation.

Custom Code Generator Agent: Automatically generates custom code blocks for playbooks from natural language prompts, eliminating the need for advanced coding expertise. This reduces development time while enabling broader teams to customize workflows.

Playbook Runlog Debugger Agent: Helps debug failed playbook runlogs by identifying root causes and providing step-by-step remediation guidance. Embedded directly in the playbook runlog interface, it streamlines troubleshooting and accelerates error resolution.

AI Action Node for Threat Actioning: A playbook node that leverages pre-built natural language interface for intelligent alert analysis, data normalization, and threat intelligence summarization. By automating complex tasks, it reduces manual effort and accelerates response. Supports multiple AI providers, including OpenAI, Mistral, Meta Llama, Gemini, and Anthropic.

Step Into the Future of Threat Intelligence Actioning with Cyware Quarterback AI

Book Your Demo Today!

For more information:

111 Town Square Palace Suite 1203 #4 Jersey City, NJ 07310 cyware.com | sales@cyware.com

CYWARE™