

Cyware Intelligence Suite

Unify your intelligence. Focus on what's relevant. Act at scale.

Where Traditional CTI Programs Break Down



Intelligence Without Decisions

Teams receive more intelligence than they can review, and still have to work out what applies to them, how urgent it is, and what to do next.



Fragmented Intel Ecosystem

Feeds, enrichment, and monitoring scattered across tools, with no central hub to correlate them.



Reactive Digital Risk Posture

Dark web, credential leaks, and brand abuse tracked in silos, with no attacker-eye view of your footprint.



Months to Stand Up a CTI Program

Configuring feeds, sandboxes, and response tools drags on for months, delaying outcomes that should be immediate.

The Solution

Security teams don't need more intelligence. They need answers from the intelligence they already have: what matters in our environment, how urgent it is, why, and what to do next. Cyware Intelligence Suite delivers those answers. A pre-configured, Cyware AI-powered CTI program built on Cyware Intel Exchange, it starts with relevance: the Priority Intelligence Requirement Agent continuously matches incoming intelligence against what your organization cares about. Around that engine, the suite combines curated sectoral and vulnerability feeds, optional digital risk protection, integrated exposure management, native malware sandboxing, and Intel Operations across 400+ tools. Cyware AI runs across the suite, so your team spends its time deciding and acting, not sorting.



Key Benefits

One Hub for the Full Intel Lifecycle

Feeds, enrichment, sandboxing, exposure management, and optional digital risk protection work together in one hub, tying your footprint to active campaigns.

Live in Days, Ready to Act

Pre-configured intel programs go live within days, and every prioritized finding comes with a clear next step your team can carry out through playbooks across 400+ tools.

Relevance You Can Prove

Cyware AI weighs every signal against your priority intelligence requirements and shows where coverage is strong, quiet, or missing, so your team acts on what matters.

AI That Shows Its Work

Cyware AI handles research, normalization, reporting, and prioritization. Every output points to its source, and your team stays in control of every action.

Cyware AI: The Agentic Layer Powering Cyware Intelligence Suite

At the core of Cyware Intelligence Suite, Cyware AI agents prioritize, research, and summarize incoming intelligence, so analysts can focus on decisions.

RELEVANCE ENGINE

Priority Intelligence Requirement Agent

Matches incoming intelligence against your plain-language priorities, tracks coverage, and signals meaningful changes.

Intel Research Agent

Researches across your intelligence, digital risk alerts, and vetted sources to deliver analyst-grade findings.

Alias Detection and Normalization Agent

Unifies the many names sources give one actor or malware family into a single profile.

Threat Bulletin Agent

Turns investigated intelligence into analyst-ready bulletins, with IOCs defanged and ATT&CK techniques mapped.

What's Available in Cyware Intelligence Suite

Built on Cyware Intel Exchange, Cyware Intelligence Suite unifies threat feeds, optional digital risk protection, exposure management, malware sandboxing, and intel operations in one hub, connected to the tools your team already runs.

Cyware Threat Intelligence Platform

- Ingests, de-duplicates, and normalizes multi-source threat data
- Intel Research and Alias Detection agents speed research and keep threat profiles consistent

Cyware Threat Intelligence Feeds

- Malware, ransomware, and sector-specific feeds for healthcare, energy, finance, and more
- Exploitation-aware vulnerability scoring with Cyware Vulnerability Feeds, powered by Securin

Cyware Digital Risk Protection (optional)

- Monitors brand and domain impersonation, credential leaks, and threats to executives
- Digital risk alerts flow into the suite alongside the rest of your threat intelligence

Cyware Exposure Management

- Compromised Credential Management with full source, timestamp, and risk context
- Agentic AI ties exposures to active campaigns and drives response through playbooks

Cyware Sandbox Service

- Detonates malware to extract IOCs and artifacts, mapped to MITRE ATT&CK
- Runs in private, isolated environments for full data privacy

Cyware Intel Operations

- Pre-built connectors extend action across 400+ tools, including SIEM, EDR, and firewalls
- Playbook Builder and Custom Code Generator put your team's response workflows into motion

See How Cyware Intelligence Suite Turns Threat Intelligence Into Action

[Book a Demo](#)

About Cyware

Cyware is the agentic AI-native platform that turns threat intelligence into clear, confident action. Cyware AI brings relevance, context, and machine-speed analysis to every stage of the intelligence lifecycle. Through trusted, bidirectional sharing, Cyware delivers that intelligence across enterprises, MSSPs, government agencies, and sharing communities such as ISACs, ISAOs, and CERTs, down to the last member organization.

cyware.com
sales@cyware.com

111 Town Square Place Suite 1203,
#4 Jersey City, NJ 07310