CYWARE™ | Datasheet

Cyware Malware Sandboxing

Private, Multi-Engine Malware Detonation and Analysis Built Into the Agentic AI-Powered Cyware Intel Exchange

As a core component of the Cyware Intelligence Suite, Cyware Sandbox Service enables secure, multi-engine malware detonation within Intel Exchange Private Communities. Analysts can safely execute files and URLs to extract forensic artifacts and map behaviors to MITRE ATT&CK without external data exposure. This intelligence directly feeds Digital Risk Protection (DRP) and Exposure Management modules, bridging the gap between internal analysis and external threat exposure.

Malware Detonation from Cyware Intel Exchange

Cyware Intel Exchange is a fully automated, Agentic AI-powered Threat Intelligence Platform that ingests, deduplicates, normalizes, enriches, scores, and correlates threat data at scale. The platform offers 400+ out-of-the-box integrations, rule-based automation, customizable risk scoring, and bi-directional threat sharing capabilities.

The sandbox service leverages Private Communities within Cyware Intel Exchange to give designated security teams a strictly isolated environment for their detonations. Once analysis is complete, the platform automatically contextualizes the sandbox results alongside global feeds, active campaigns, and Digital Risk Protection (DRP) signals to orchestrate rapid downstream defense.

Security Analyst Benefits

Deeper Context, Faster Analysis

Single-click detonation pushes behavioral profiles, IOCs, and TTPs directly back into active investigations in seconds , fueling AI agents to reconstruct complex adversary behavior sequences.

Tool Consolidation

Replaces fragmented point tools by consolidating threat feeds, sandboxing, credential exposure, and external digital risk tracking into a single central operational hub.

Risk-Aware Decisions

Rich, multi-engine artifacts empower security teams to build higher-fidelity detection engineering rules and automated response playbooks.

Key Capabilities

Privacy-First Sandboxing

All detonation activity is strictly confined to Cyware Intel Exchange Private Communities, ensuring rigorous data segmentation and zero exposure to external public repositories.

Multi-Engine Malware Analysis

Leverages industry-leading sandbox technologies to provide robust behavioral and static analysis across a wide range of sophisticated malware samples.

Flexible VM Environments

Supports multiple operating systems and file types including Windows, Linux, and Android VMs with the capability to toggle live internet connectivity during execution.

IOC Extraction & Mapping

Automatically extracts critical indicators such as file hashes (MD5, SHA1, SHA256), network IOCs (IPv4, domains, URLs), and observed attack patterns.

Customizable Detonation Parameters

Allows analysts to dynamically select preferred VM images, network configurations, and execution settings for tailored forensic investigations.

Rich Output & Artifact Downloads

Every sandbox session generates downloadable forensic packages, including PCAP files, dropped files, memory dumps, JARM signatures, detonation video recordings, and comprehensive HTML reports

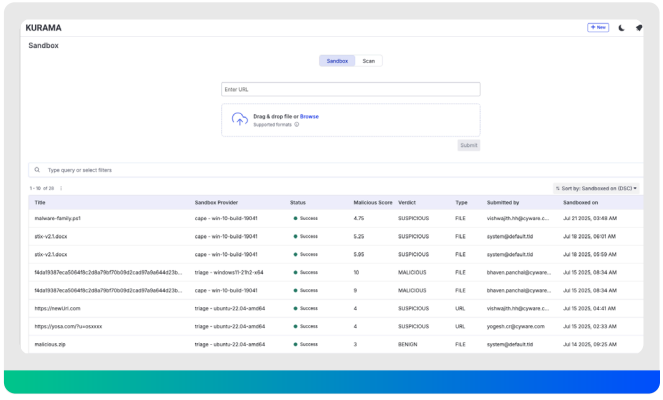

Fig 1. *Cyware Sandbox Interface*

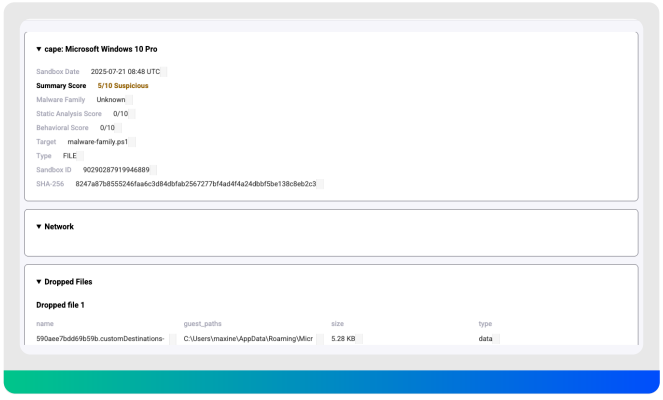

Fig 2. *Malware Analysis Result*

Use Cases

Advanced Malware Detonation & Analysis

Safely execute unknown files, URLs, QR codes, or hashes within isolated virtual machines to observe execution behavior without risking corporate production assets.

Forensic IOC & Artifact Extraction

Generate deep technical data (PCAPs, JARM signatures, dropped files, memory dumps, and extracted configurations) to accelerate forensic analysis and facilitate rapid blocking across security infrastructure.

Unified Investigation & Threat Enrichment

Feed sandbox verdicts directly back into Cyware Intel Exchange to enrich related hashes, domains, URLs, and malware families. This allows analysts to investigate dark web data and brand exposure alongside active malware campaigns.

MITRE ATT&CK TTP Mapping

Automatically align observed runtime behaviors to the MITRE ATT&CK framework, helping security teams uncover exact adversary techniques and deploy proactive detection rules.

DRP and Automated Incident Response

Link sandbox verdicts to automated response workflows. If a detonated sample reveals links to external brand abuse or phishing infrastructure, the platform can trigger Agentic AI playbooks to orchestrate automated SOCRadar takedown services or block malicious assets across SIEM, EDR, and firewalls

Scale Your Threat Intel Program with the Cyware Intelligence Suite

The Cyware Sandbox Service is a core, pre-configured capability delivered within the unified Cyware Intelligence Suite. By unifying sandboxing with Digital Risk Protection (DRP), Exposure Management (including Compromised Credential Management and Automated Domain Exposure Monitoring), Cyware Sectoral Feeds, and Agentic AI capabilities, organizations can bypass months of traditional tool integration and establish a mature, proactive threat intelligence program in just days.

About Cyware

Cyware is leading the industry in Agentic-powered Operational Threat Intelligence and Collective Defense, helping security teams transform threat intelligence from fragmented data points to actionable, real-time decisions. We unify threat intelligence management, intel sharing and collaboration, with orchestration and automation, eliminating silos and enabling organizations to outmaneuver adversaries faster and more effectively. From enterprises to government agencies and ISACs, Cyware empowers defenders to turn intelligence into impact.

cyware.com

sales@cyware.com

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