CYWARE™ | Datasheet

Cyware Sandbox Service

Private, Multi-Engine Malware Detonation and Analysis Built Into Cyware Intel Exchange

Cyware Sandbox Service offers multi-engine malware detonation, powered by CAPE and Triage, directly inside Cyware Intel Exchange Private Communities. Analysts can execute suspicious files and URLs in Windows, Linux, and Android VMs, retrieve rich artifacts, and automatically enrich threat objects with MITRE ATT&CK-mapped behaviors without exposing their samples to external services.

Malware Detonation from Cyware Intel Exchange

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

Cyware Sandbox Service leverages Private Communities within Cyware Intel Exchange, that enable access to specific user groups to execute their sandbox detonations in as isolated environment. Cyware Intel Exchange contextualizes the sandbox analysis results with other intelligence sources and automates dissemination and actioning for downstream response.

Security Analyst Benefits

Deeper Context, Faster Analysis

Single-click detonation pushes behavior, IOCs, and TTPs back to investigations in seconds.

Tool Consolidation

Eliminate reliance on third-party sandbox portals and data exports.

Risk-Aware Decisions

Rich artifacts drive better detection engineering and response playbooks.

Key Capabilities

Privacy-First Sandboxing

All detonation activity is confined to Cyware Intel Exchange Private Communities, ensuring strict data segmentation and zero exposure to external sources.

Multi-Engine Malware Analysis

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

Flexible VM Environments

Supports multiple OS and file types including Android VMs, with the ability to toggle Internet connectivity during analysis.

IOC Extraction & Mapping

Automatically extracts hashes (MD5, SHA1, SHA256), network IOCs (IPv4, domains, URLs), and attack patterns mapped to MITRE ATT&CK TTPs.

Customizable Detonation Parameters

Analysts can select preferred VM image and network settings for tailored investigations.

Rich Output & Artifact Downloads

Each sandbox session yields downloadable artifacts, including PCAP files, dropped files, memory dumps, JARM signatures, video recordings of detonation, and full HTML reports.

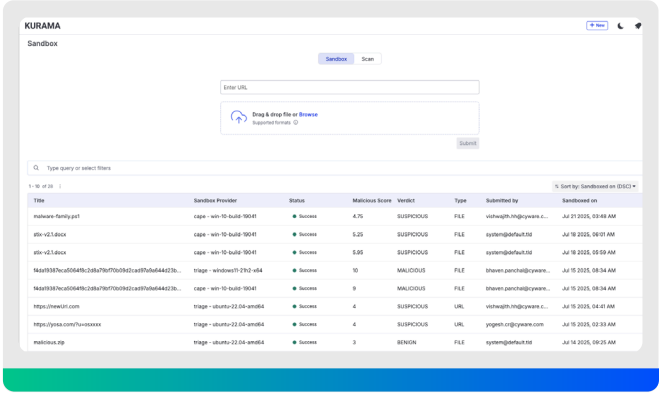

Fig 1. Cyware Sandbox Interface

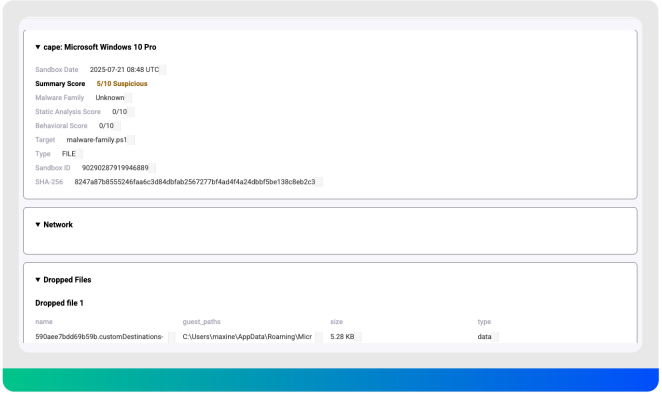

Fig 2. Malware Analysis Result

Use Cases

Malware Detonation & Analysis
Safely explode suspicious files and URLs in isolated VMs to observe behavior without risking production assets.

IOC & Artifact Extraction
Generate PCAPs, JARM signatures, dropped files, memory dumps, and extracted configs for deeper forensic analysis and rapid blocking.

Threat Investigation & Enrichment
Feed sandbox verdicts back into Cyware Intel Exchange to enrich related hashes, domains, URLs, and malware families for full-context investigations.

MITRE TTP Mapping
Automatically align observed behaviors with MITRE ATT&CK techniques to enhance detection rules and analytics.

Automated Response
Trigger Cyware Intel Exchange rules or Cyware Orchestrate playbooks to block malicious IPs, quarantine hosts, or open tickets the moment a sandbox verdict is produced.

Scale Your Threat Intel Program with the Cyware Intelligence Suite

Cyware Sandbox Service is one of several pre-configured capabilites in the Cyware Intelligence Suite. Together with Compromised Credential Management, Domain Sightings, Cyware Sectoral Malware Feeds, Team Cymru Threat Feeds, and AI-driven enhancements, establish a mature threat intel program in days, all within the Cyware Intel Exchange platform.

About Cyware

Cyware helps enterprise cybersecurity teams build platform-agnostic cyber fusion centers by delivering cyber threat intelligence and next-generation security orchestration and automation solutions. As a result, organizations can increase speed and accuracy while reducing costs and analyst burnout. Cyware's Cyber Fusion solutions enable secure collaboration, information sharing, and enhanced threat visibility for MSSPs, enterprises, government agencies, and sharing communities (ISAC/ISAO/CERTs and others) of all sizes and needs.

cyware.com

sales@cyware.com

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