REVERSINGLABS

# ReversingLabs Cloud Sandbox

## Cloud-Based Dynamic Analysis: Detonate files and URLs, observe real behavior, act on results

Organizations face a growing volume of unknown and evasive threats that bypass traditional detection tools. The ReversingLabs Cloud Sandbox provides a fully managed, highly-available and highly-scalable cloud-based environment where suspicious files and URLs are safely executed and observed, revealing their true behavior without any risk to your infrastructure. With no hardware to deploy or maintain, security teams gain immediate access to deep behavioral analysis across Windows, macOS, Linux, and Android environments, all through a simple API integration or as part of the Spectra Analyze malware analysis workbench. Results are delivered as rich, structured reports ready to feed SOC workflows and security tools.

# What You Can Submit for Analysis

## Dynamic Analysis Submission

Submit any suspicious file or URL for execution in an isolated cloud environment. The sandbox safely runs the sample, captures everything it does, and makes results available for retrieval, without exposure to your organization's systems.

| Windows 11 | Windows 10 | Windows 7 |
|---|---|---|
| Modern enterprise desktop with current Office, browser, and reader versions | Widely deployed enterprise configuration with legacy and current application support | Legacy environment for analyzing threats targeting older infrastructure |

| macOS 11 (Big Sur) | Linux (Ubuntu 20.04) | Android 12 |
|---|---|---|
| macOS environment for threats targeting Apple desktop users | Server and workstation environment covering scripts, documents, and Linux binaries | Mobile threat analysis including runtime permissions, network activity, and app behavior |

## Submission Capabilities

- **Files & URLs** — submit any file (up to 400 MB) or web address directly for analysis. The same sample can be simultaneously submitted to multiple environments for comprehensive coverage.
- **Archives** — submit a compressed package and automatically analyze up to 10 contained files as individual, independent detonations, ideal for multi-stage droppers and installer bundles.
- **Email files** — submit a suspicious email and the sandbox automatically detonates each attachment and analyzes URLs extracted from the email body. The most severe result is surfaced to the top-level report.
- **Wide file type coverage** — Windows executables, Office documents, PDFs, scripts, mobile apps, macOS disk images, Linux binaries, web pages, and more.
- **Geographic simulation** — route sandbox network traffic through 11 regions (US, UK, Germany, Japan, Brazil, India, Singapore, France, Italy, Spain, or anonymized via TOR) to uncover malware that only activates in specific target countries.
- **Language & locale simulation** — configure the sandbox to present a specific language and regional setting, exposing threats designed to check for a target environment before executing.
- **Network isolation mode** — run analysis with a simulated network instead of live internet connectivity to protect infrastructure while still capturing command-and-control behavior.
- **Flexible analysis duration** — configure sandbox execution time from 30 to 500 seconds to ensure slow-activating or time-delayed threats are fully observed.

**Results are typically available within approximately 15 minutes of submission. Each submission receives a unique identifier, enabling precise retrieval of per-environment reports.**

# Data Privacy & Sharing Controls

Organizations retain full control over whether submitted files and analysis artifacts are visible to other ReversingLabs customers.

**SHARED MODE: Analysis results and artifacts (network captures, screenshots, memory data, dropped files) are accessible to the broader ReversingLabs customer community, thus contributing to collective threat intelligence.**

**PRIVATE MODE: Only your organization can access submitted files and their artifacts. Other customers may see analysis verdicts but cannot download any file contents or associated artifacts.**

# What the Sandbox Reports: Full Behavioral Visibility

## Dynamic Analysis Report

After detonation, the Dynamic Analysis Report delivers a complete picture of what the threat actually did from the moment it launched to every system change, network connection, and file it touched. Reports are available as a full history across all past analyses, as a focused result for a specific run, or as per-file breakdowns for submitted archives.

- **Verdict & risk score** — every analyzed sample receives a clear classification (Malicious, Suspicious, Clean, or No Threats Found) and a risk score from 0–10, giving security teams an immediate signal for prioritization and escalation.
- **Threat names & behavioral signatures** — identified malware families, threat designations, and a curated set of observed capabilities. Each with a plain-language description and risk rating, designed to communicate clearly across technical and non-technical audiences.
- **MITRE ATT&CK mapping** — all observed tactics and techniques aligned to the industry-standard ATT&CK framework, enabling direct integration into detection and response workflows.
- **Process & system activity** — a full record of every process spawned during execution, including files accessed or created, registry changes, processes launched, and system components loaded; plus a complete, ordered process tree.
- **Network communications** — all outbound connections made by the sample, including web requests, DNS lookups, and direct IP connections, with classification and category labels for each destination.
- **Attacker infrastructure (C2)** — command-and-control server addresses and URLs extracted directly from the malware's embedded configuration data, capturing what static analysis alone cannot reveal.
- **Network threat detection** — network traffic analyzed against Snort and Suricata detection rule sets to flag known attack patterns and C2 communication signatures.
- **Dropped files** — all files written to disk during execution, each with its own classification and threat verdict. Ultimately surfacing payloads deployed by loaders, installers, or multi-stage malware.
- **YARA rule matching** — automated detection against YARA rules across the sample, dropped files, memory captures, and network traffic, enabling fast identification of known malware families and custom threat signatures.
- **Screenshots** — visual captures of the desktop during execution, providing immediate context for phishing pages, ransom notes, or deceptive application behavior. Retained for one year.
- **Full network traffic capture (PCAP)** — the complete PCAP recording from the sandbox session, available for download by security teams for deep-dive investigation. Retained for one year.
- **Memory analysis** — strings extracted from process memory during execution, useful for uncovering indicators that are decrypted or assembled only at runtime. Retained for one year.
- **Sigma detections** — sandbox system events matched against open-standard Sigma detection rules, producing output directly compatible with major SIEM platforms.
- **Android app behavior** — for mobile threats, reveals what permissions the app actually exercised at runtime versus what it declared, along with background services and communication handlers registered dynamically.
- **Email threat chain** — for email submissions, surfaces sender and recipient details, attachment verdicts, and URL analysis results that are all linked in a single, navigable report chain across the full email threat lifecycle.

**Reports are available in three modes: a merged view across all historical analyses for a sample, a specific report for a single run, and archive reports with per-file breakdowns for submitted archives. Artifact download links are generated on demand and valid for one hour.**

# Common Use Cases

### Unknown & Evasive Threat Analysis

Submit suspicious files that evade static detection. Use geographic and language simulation to expose regionally targeted malware that only activates in specific countries or language environments (a technique increasingly common in advanced, targeted attacks).

### Phishing & Email Threat Investigation

Submit a suspicious email and automatically receive verdicts for every attachment and embedded URL in a single workflow, thus eliminating manual extraction. Results are linked across the full email threat chain in one unified report.

### Attacker Infrastructure Discovery

Extract command-and-control (C2) addresses directly from malware configurations captured at runtime and going beyond static analysis. Cross-reference against network detection alerts to map the full extent of attacker infrastructure.

### Multi-Stage & Dropper Analysis

Submit a malicious archive and receive individual analysis reports for every file it contains; covering the complete infection chain from initial dropper through final payload, without any manual unpacking.

### Mobile Threat Validation

Detonate Android applications to see what they actually do at runtime and not just what they declare. Identify unauthorized data access, hidden network communications, or covert background activity invisible through static review alone.

### SOC & Platform Integration

Integrate submission and report retrieval directly into SIEM, SOAR, and threat intelligence platforms via REST API. Automate analysis pipelines for suspicious files surfaced during incident response, endpoint alerts, or email security triage.

## Get started!

Improve your detection efficacy with high-fidelity, validated threat intelligence and threat classifications you can trust.

REQUEST A DEMO

reversinglabs.com

## About ReversingLabs

ReversingLabs is the trusted name in file and software security. We provide the modern cybersecurity platform to verify and deliver safe binaries. Trusted by the Fortune 500 and leading cybersecurity vendors, RL Spectra Core powers the software supply chain and file security insights, tracking over 450 billion searchable files with the ability to deconstruct full software binaries in seconds to minutes. Only ReversingLabs provides that final exam to determine whether a single file or full software binary presents a risk to your organization and your customers.



Rev-DS-07.29.26

REVERSINGLABS

Worldwide Sales +1.617.250.7518
sales@reversinglabs.com