

# Hybrid Analyzer

FAST, SCALABLE FILE ANALYSIS

Security teams struggle to detect new malware threats and quickly gather insights to triage alerts. Traditional anti-malware engines are fast and scalable, but only identify known bad files. Sandboxes provide exhaustive analysis of suspicious files, but they are notoriously expensive and slow. Cyren Hybrid Analyzer produces detailed analysis of file structure and behaviors at high speed and massive scale so service providers, cybersecurity vendors, and enterprises can cost-effectively lower the risk of undetected malware. **Detect more threats. Make better decisions. Reduce costs.**

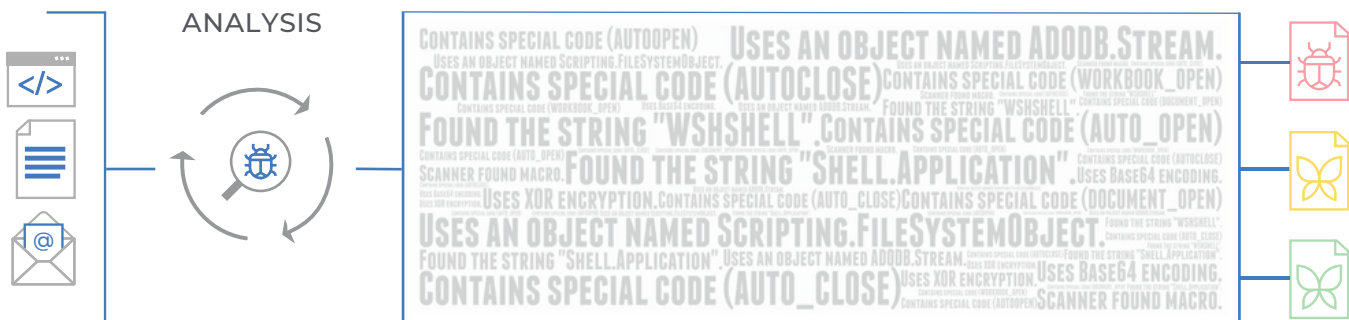
## DEEP AND COMPLETE ANALYSIS WITH HYBRID ANALYZER

Hybrid Analyzer bridges the gap between anti-malware detection and sandbox detonation by pushing the limits of emulation – delivering the ability to emulate many functions across many platforms. An innovation resulting from Cyren’s decades of experience building hyper-fast and scalable malware detection engines, Hybrid Analyzer combines our high-speed emulation technology with proven static analysis methods to provide actionable intelligence for each file.

Hybrid Analyzer produces valuable behavioral and structural details, indicators of compromise (IOCs), and impact ratings to enable real-time security decisions and granular policies. It automatically defeats evasion and obfuscation techniques to accurately and deeply analyze the entire file – in fractions of a second, not minutes.

**ADVANTAGES OF Hybrid Analyzer**

- Rapid extraction of file structure and behaviors
- Advanced emulation
- 100 times faster than a sandbox
- Easy, flexible integration



Equally suited for connected and air-gapped environments, Cyren Hybrid Analyzer does not rely on data sharing or cloud connectivity to operate. It comes with multi-platform support and flexible integration options, and is extremely light and portable.

## ADVANTAGES OF HYBRID ANALYZER

- **Analyzes a File in Milliseconds**

Not a sandbox, Hybrid Analyzer uses proprietary emulation technology developed over decades to inspect full file contents at speeds and throughput required by service providers.

- **Actionable Intelligence**

Hybrid Analyzer is capable of recognizing over 1,100 relevant file indicators and attributes.

- **Severity Ratings**

Each file behavior or attribute is rated for risk and severity factors. Ratings algorithms were developed

using analysis of 3 billion verified malicious and known clean files.

- **Light and Portable**

Optimized for embedded environments, Cyren Hybrid Analyzer operates in real-time using a minimal

memory and CPU footprint. It includes multiple integration options and platform support.

- **Preserves Privacy**

Never compromise performance or privacy; Cyren Hybrid Analyzer offers full performance without uploading files to Cyren clouds.

## INTEGRATION AND PLATFORM SUPPORT

- **Supported Platforms**

Runs on Windows, Linux, and FreeBSD

- **Supported File Types**

Analyzes files for Windows, Mac, Android like Office, PDF, HTML, JavaScript, archive, and more

- **SDK Library**

For full control and flexibility of integration

- **Service / Daemon**

Turnkey application for easy integration and automatic updates

