CODEHUNTER

# Go Beyond the Sandbox with CodeHunter

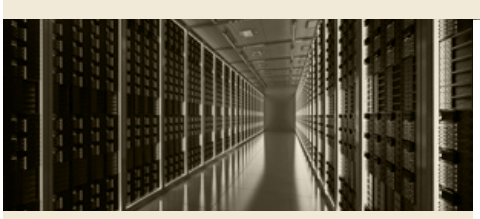
The **CodeHunter malware analysis platform** is a patented, advanced cybersecurity solution designed to provide deep insights into malware threats targeting your business. By combining dynamic, static, and AI-driven analysis, CodeHunter automates the malware reverse engineering process in minutes and delivers threat verdicts and actionable insights on each file analyzed. With CodeHunter, security teams get comprehensive data on malicious activity, so they can **identify**, **mitigate**, and **respond** to threats **faster**.

## The CodeHunter Difference

CodeHunter starts where other security solutions stop. We go beyond what sandbox technologies can do, with a holistic analysis approach that tracks key actions such as file system changes, network activity, and attempts to exploit vulnerabilities to:

- **Provide** deep insights into a threat's full attack lifecycle—from initial compromise to persistence mechanisms and lateral movements.
- **Uncover** even the most evasive malware including zero-day, multi-part, and custom attack campaigns.
- **Unlock** proactive threat intelligence to enable a proactive approach to threat hunting.


## How It Works



### PRE-PROCESSING

Examines large volumes of files, directories, repositories, and cloud storage to identify dangerous files and classifies them as data or executable.

### DEEP ANALYSIS

Automates behavior computation and binary analysis. Removes obfuscation, creates simplified object code, and uses proprietary rules to detect suspicious or malicious behaviors.

### OUTPUT

Generates clear verdicts and actionable insights and maps findings to industry standards like MITRE ATT&CK Matrix®, Malware Behavior Catalog, YARA™, and CAPA.

## Key Features of the CodeHunter Platform

### COMPREHENSIVE MALWARE ANALYSIS:

CodeHunter combines patented Dynamic, Static and AI analysis, automating time-consuming, reverse-engineering to deliver faster and more comprehensive results than today's existing solutions.

### WIDE FILE FORMAT SUPPORT:

CodeHunter supports a variety of file types, including:

- Executable Files
- Documents
- Macros
- Script Files
- .NET

This broad support ensures the platform can handle common and advanced threats across diverse file formats.

### CLEAR VERDICTS & ACTIONABLE INSIGHTS:

The platform provides clear verdicts and actionable insights on each file instantly including whether the sample is benign or malicious, the type of threat, and the associated risks so security teams can quickly prioritize their threat response.

### AUTOMATED MALWARE REVERSE ENGINEERING:

Security professionals get deep insights into malware functionality without requiring specialized skills.

### SCALABILITY FOR LARGE FILES:

Supports files up to **five times larger** than other malware analysis platforms – critical for handling complex malware samples so that even the most sophisticated and large-scale threats can be effectively analyzed.

### SEAMLESS INTEGRATION WITH SECURITY ECOSYSTEMS:

Easily integrates with EDRs, SIEMs, SOARs, etc. to supercharge an organization's security stack, powering threat triage, faster response times, and enhanced collaboration between different security tools and teams.

### PLATFORM ACCESS TO INTEL FEED:

CodeHunter allows security analysts to retrieve real-time threat intelligence directly from the platform. Crowdsourced intelligence updates are provided in a downloadable format so an organization can take a proactive approach to its threat-hunting practices.

### COST AND RESOURCE EFFICIENCY:

CodeHunter reduces the workload for security teams and minimizes the need for manual intervention, saving valuable time, money, and resources.

**CodeHunter empowers organizations to rapidly identify, understand, and respond to threats, accelerating incident response while saving valuable time, money, and resources.**

**LEARN MORE**
**codehunter.com**

CODEHUNTER