CROWDSTRIKE

CROWDSTRIKE FALCON SANDBOX MALWARE ANALYSIS

The world's most powerful malware sandbox

COMPLETE VISIBILITY INTO ADVANCED AND UNKNOWN THREATS

When an organization is hit by a cyberattack, visibility into the intent of the attack must be prioritized at the highest level. You need to quickly understand what the malware was attempting to do and how it works, so you can contain any damage and learn how to prevent attacks in the future. Today, malware analysis takes too long and often provides incomplete details about the threat — making it difficult for security teams to have confidence in the findings, leading to a never-ending need for further analysis. To make matters worse, adversaries are getting smarter, constantly evolving their malware to evade and find blind spots in common malware analysis tools and techniques.

CrowdStrike® Falcon® Sandbox™ defeats even the most evasive malware by running in the kernel and using sophisticated sandbox techniques that make it nearly undetectable. It exposes the most advanced targeted attacks, going beyond common static and dynamic file analysis to monitor all malicious behavior and system interaction. This allows Falcon Sandbox to deliver the most extensive set of indicators of compromise (IOCs) in the industry.

Falcon Sandbox also saves you time and makes all security teams more effective with easy-to-understand reports, actionable IOCs and seamless integration. CrowdStrike malware analysis reports provide practical guidance for threat prioritization and response, while still enabling forensic teams to delve deeply into memory captures and stack traces. The Falcon Sandbox API and pre-built integrations enable easy orchestration between existing security solutions.

KEY BENEFITS

- Provides in-depth insight into all file, network and memory activity
- Offers leading anti-VM detection technology
- Generates intuitive reports with forensic data available on demand
- Supports the MITRE ATT&CK™ framework
- Orchestrates workflows with an extensive API and pre-built integrations

KEY PRODUCT CAPABILITIES

DETECT UNKNOWN THREATS

- **Hybrid Analysis:** This combines runtime data, static analysis and memory dump analysis to extract all possible execution pathways even for the most evasive malware. In combination with extensive pre- and post-execution analysis, Falcon Sandbox extracts more IOCs than any other competing sandbox solution. All data extracted from the Hybrid Analysis engine is processed automatically and integrated into the Falcon Sandbox reports.
- **Anti-Evasion Technology:** Falcon Sandbox includes state-of-the-art anti-sandbox detection technology. The file monitoring runs in the kernel and cannot be observed by user-mode applications. CrowdStrike doesn't use an agent that can be easily identified by malware and continuously tests each release to ensure Falcon Sandbox is nearly undetectable by malware using even the most sophisticated sandbox detection techniques.
- **Environmental Customization:** Take control of how malware is detonated by configuring common settings that malware uses to attempt to hide from sandbox analysis, such as date/time, environmental variables, user behaviors and more.

ACHIEVE COMPLETE VISIBILITY

- **Analysis Reports:** Easy to understand reports make every analyst at every level more effective in their roles. The analysis is layered, providing security teams with practical guidance for threat prioritization and response, enabling incident response teams to threat hunt and forensic teams to drill-down for deep analysis into memory captures and stack traces.
- **Broad File Support:** Falcon Sandbox supports Windows, Linux and Android (static analysis only) operating systems. In addition, Falcon Sandbox analyzes over 40 different file types that include a wide variety of executables, document and image formats, and script and archive files.
- **Malware Search:** Falcon Sandbox will automatically search the industry's largest malware search engine to find related samples and within seconds expand the analysis to include all files. This unique capability provides analysts with a deeper understanding of the attack and a larger set of IOCs that can be used to better protect the organization.

RESPOND FASTER

- **Immediate Triage:** Falcon Sandbox provides threat scoring and incident response summaries to immediately triage and eradicate malware. In addition, analysis reports are enriched with information and IOCs from CrowdStrike Falcon MalQuery™ and CrowdStrike Falcon Intelligence™, providing the necessary context to make faster, better decisions.
- **Easy Integration:** It includes an easy-to-use REST API, pre-built integrations and support for indicator sharing formats including STIX, OpenIOC, MAEC, MISP, and XML/JSON. This enables users to delivers Falcon Sandbox results with SIEMs, TIPs and orchestration systems.
- **Flexible Deployment:** You can choose between a cloud or on-premises version of Falcon Sandbox. The cloud option provides immediate time-to-value and reduced infrastructure costs, while the on-premises version enables users to lock down and process samples solely within their environment. Both options provide a secure and scalable sandbox environment.

TAKE FALCON SANDBOX FOR A TEST DRIVE

The largest online malware analysis community is powered by Falcon Sandbox — which means it's field-tested by tens of thousands of users every day. Try it for free at www.hybrid-analysis.com, if you are pleased with the results, you can easily upgrade to a full Falcon Sandbox license.

The Falcon Sandbox on-premises version allows organizations to tailor the sandbox to their specific requirements. To enable targeted attack detections, Falcon Sandbox imports "golden" virtual machine images mirroring the operating system, applications and settings that reflect the real-world customer-specific environment. In addition, user behavior can be emulated and custom behavior indicators defined. The on-premises edition can be run "air gapped", without network connectivity to comply with the most stringent privacy policies.

ABOUT CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered next-generation endpoint protection. CrowdStrike has revolutionized endpoint protection by being the first and only company to unify next-generation antivirus, endpoint detection and response (EDR), IT hygiene and a 24/7 managed hunting service — all delivered via a single lightweight agent.