kaspersky BRING ON THE FUTURE

Kaspersky Research Sandbox

Making an intelligent decision based on a file's or URLs behavior while simultaneously analyzing the process memory, network activity, etc., is the optimal approach to understanding current sophisticated targeted and tailored threats. Sandboxing technologies are powerful tools that allow investigation of file sample origins, collection of IOCs based on behavioral analysis and detection of malicious objects not previously seen.

Product highlights:

- On-premises deployment makes sure no data is exposed outside the organization
- Supports the analysis of more than a hundred file types
- Advanced anti-evasion techniques
- Custom images allowing to analyze threats across a range of operating systems and applications and only those that apply to real environments
- Separate analysis of each process to detect suspicious activities with associated network connections
- Detailed analysis reports, including all system activities, extracted files, network activities (PCAP) and visual graphs
- Manual file/URL submission and RESTful API for seamless integration and automation of your security operations

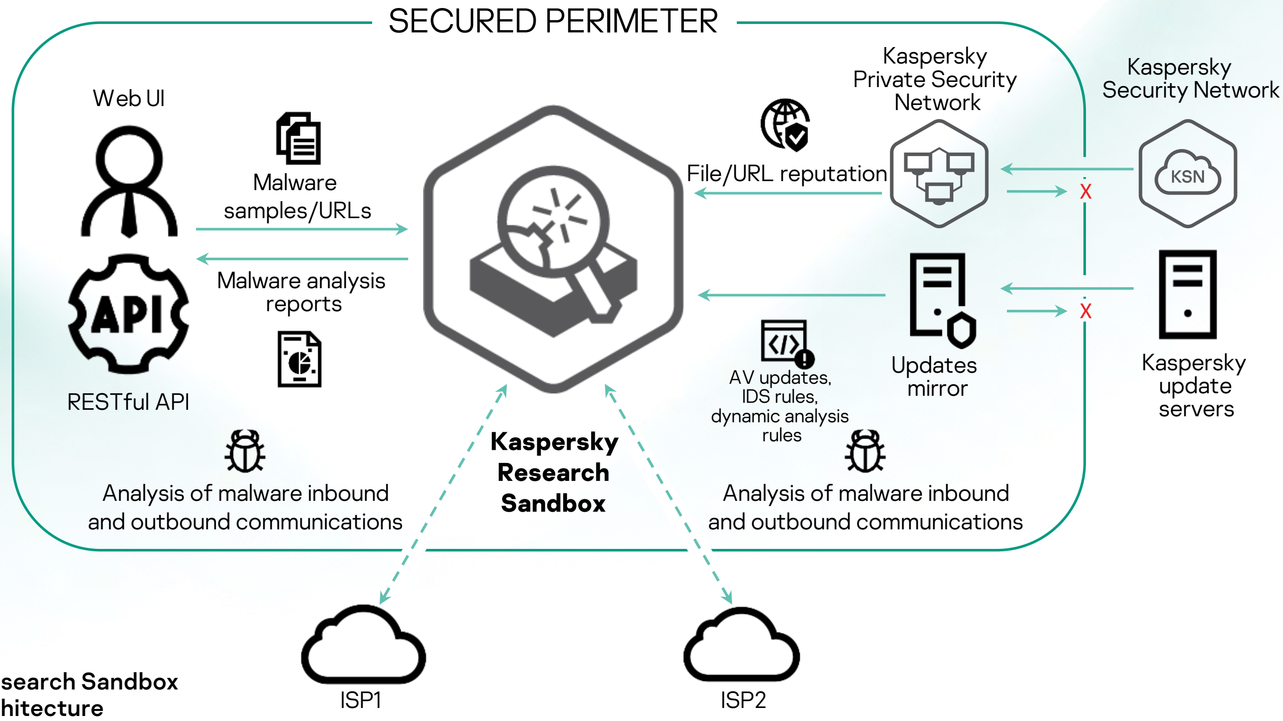
IMPORTANT: Integration with Kaspersky Private Security Network is required

Today's malware uses a whole variety of methods to avoid executing its code if this could lead to exposing its malicious activity. If the system does not meet the required parameters, the malicious program will almost certainly destroy itself, leaving no traces. For the malicious code to execute, the sandboxing environment must therefore be capable of accurately mimicking normal end-user behavior.

Kaspersky Research Sandbox has been developed directly out of our in-lab sandboxing complex, a technology that's been evolving for over a decade. It incorporates all the knowledge about malware behaviors acquired by Kaspersky throughout our continuous threat research, allowing us to detect 350 000+ new malicious objects every day. Deployed on-premises, this powerful technology also prevents exposure of data outside the organization.

It offers a hybrid approach, combining behavioral analysis, and rock-solid anti-evasion, with human-simulating technologies. Kaspresky Research Sandbox also allows to customize images of the systems for analysis tailoring them to real environments, which increases the accuracy of threat detection and the speed of investigation.

The diagram below describes the high-level architecture of Kaspersky Research Sandbox.


SECURED PERIMETER
Web UI
Malware samples/URLs
Malware analysis reports
API
RESTful API
Analysis of malware inbound and outbound communications
Kaspersky Research Sandbox
File/URL reputation
Kaspersky Private Security Network
Kaspersky Security Network
KSN
X
X
Updates mirror
AV updates, IDS rules, dynamic analysis rules
Kaspersky update servers
Analysis of malware inbound and outbound communications
ISP1
ISP2

Kaspersky Research Sandbox high-level architecture

Kaspersky Research Sandbox is based on a patented proprietary technology (patent no. US10339301). By creating the exact conditions that triggers malware execution, it allows researchers to analyze a suspicious file/URL in a single attempt.

The product supports bare metal deployment. Hardware configuration depends on the required performance and can be scaled. It requires 100 Mbps network connection for each channel and at least one independent ISP connection (two or more are recommended for fault-tolerance). The ISP should be aware and ready for malicious traffic.

Once the analysis is complete, Research Sandbox provides a detailed report on the behavior and functionality of the analyzed sample, allowing you to define the appropriate response procedures:

- **Summary** — general information about a file's execution/URL browsing results.
- **Sandbox detection names** — a list of detects (both AV and behavioral) that were registered during the file execution.
- **Triggered network rules** — a list of network SNORT rules that were triggered during analysis of traffic from the executed object.
- **Execution map** — a graphically represented sequence of object activities (actions taken on files, processes and the registry, and network activity) and the relationship between them. The root node of the tree represents the executed object.
- **Suspicious activities** — a list of registered suspicious activities.
- **Screenshots** — a set of screenshots that were taken during the file execution/URL browsing .
- **Loaded PE images** — a list of loaded PE images that were detected during the file execution/URL browsing.
- **File operations** — a list of file operations that were registered during the file execution/URL browsing.
- **Registry operations** — a list of operations performed on the OS registry that were detected during the file execution/URL browsing.
- **Process operations** — a list of interactions of the file with various processes that were registered during the file execution.
- **Synchronize operations** — a list of operations of created synchronization objects (mutex, event, semaphore) that were registered during the file execution/URL browsing.
- **Downloaded files** — a list of files that were extracted from network traffic during the file execution/URL browsing.
- **Dropped files** — a list of files that were saved (created or modified) by the executed file.
- **HTTPS/HTTP/DNS/IP/TCP/UDP and etc.** — network sessions/requests details that were registered during the file execution/URL browsing
- **Network traffic dump (PCAP)** — network activity can be exported in PCAP format.
- **MITRE ATT&CK matrix** — all identified process activities recorded during emulation are presented in the form of a MITRE ATT&CK matrix.

Kaspersky Research Sandbox is the instrument of choice for detecting unknown threats. It's more mature and more focused on advanced threats than any other solution.

To avoid exposure, a malicious file may first investigate if it's in a virtual machine or stay inactive for a period of time until the sandbox is no longer operating. In such cases, the patented technology speeds up the time flow inside the virtual machine so the malicious code is forced to execute sooner.

Malware may not show its malicious behavior if it targets a specific application that is missing in the sandbox. To resolve this challenge, researchers must review logs, understand what is missing, add it to a virtual machine and run this process again. In doing so, when malware tries to access an application, the patented system intercepts this attempt. It doesn't wait until the file execution is finished, but rather pauses the process to create the required application as well as the content.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise
Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Know more at kaspersky.com/transparency

Proven.
Transparent.
Independent.