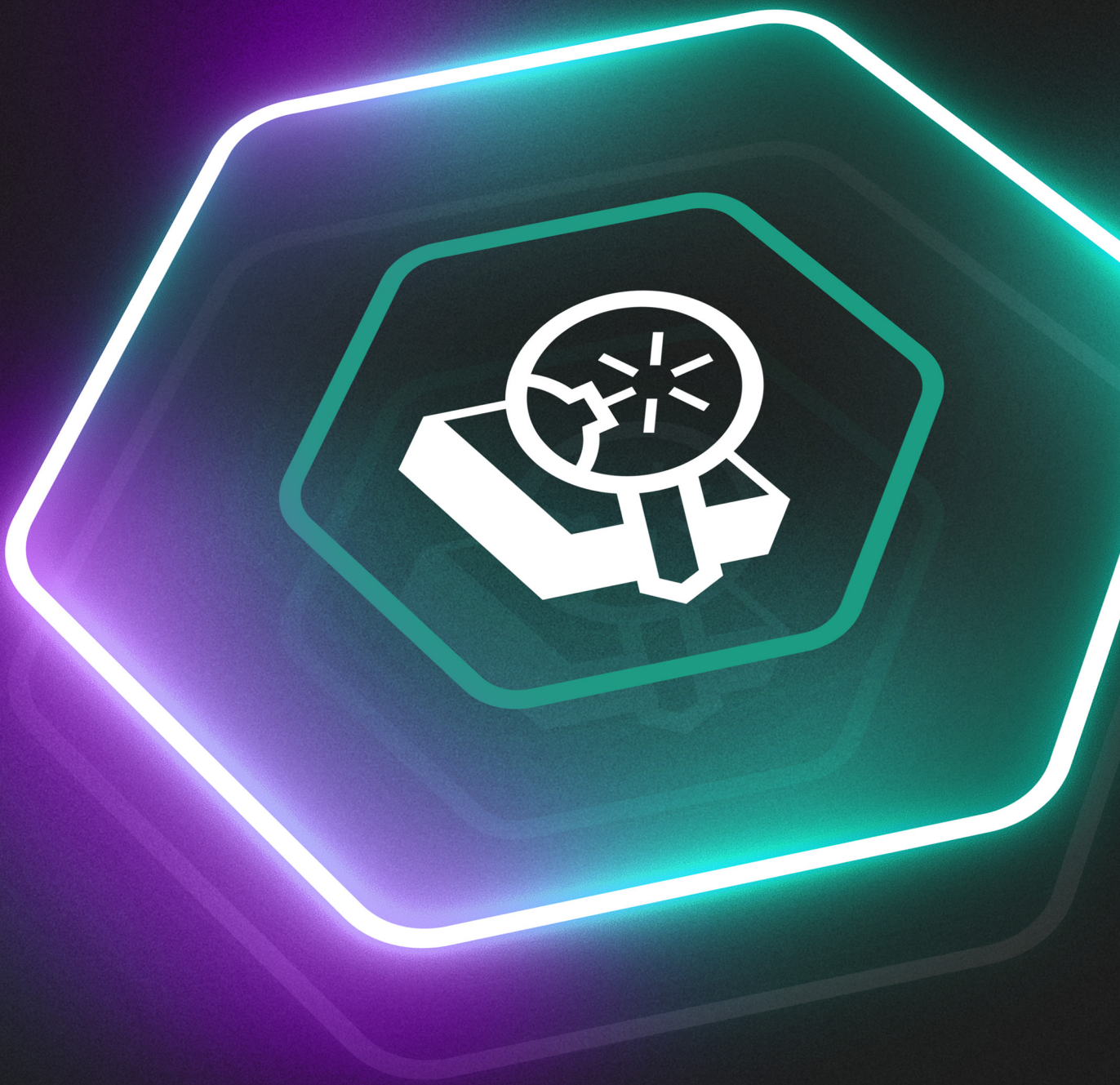


Kaspersky Research Sandbox

kaspersky BRING ON THE FUTURE

Sandboxing technologies

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.

Kaspersky Research Sandbox

Making an intelligent decision based on file or URL behavior while simultaneously analyzing the process memory, network activity, etc., is the optimal approach to understanding current sophisticated targeted and tailored threats.

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 trace. For the malicious code to execute, the sandboxing environment must therefore be capable of accurately mimicking normal end-user behavior.

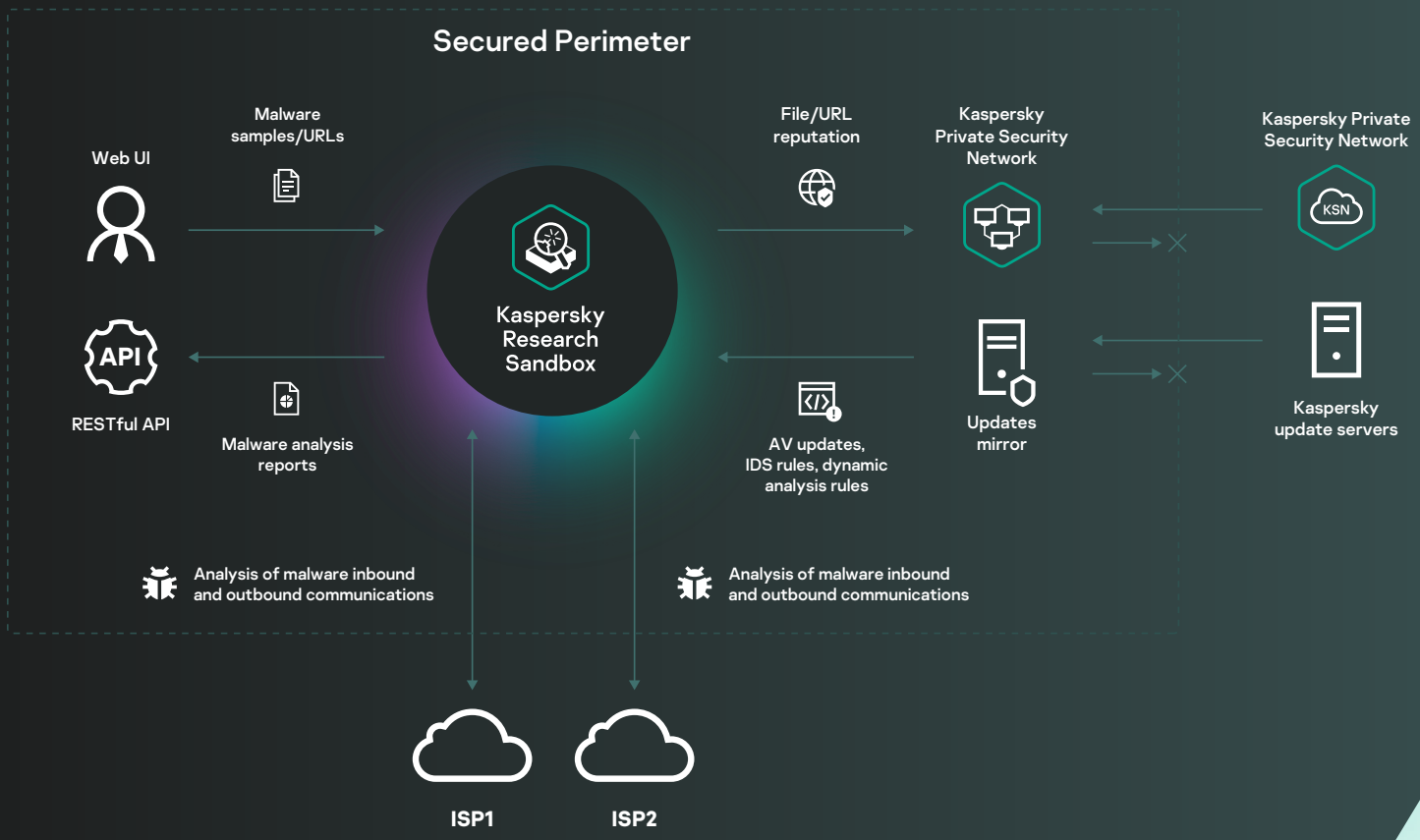
Kaspersky Research Sandbox has been developed directly out of our in-lab sandboxing complex, a technology that's been evolving for over a decade. It incorporates all the knowledge about malware behaviors we have acquired throughout our continuous threat research, allowing us to detect 380 000+ new malicious objects every day. Deployed on-premise, this powerful technology also prevents exposure of data outside the organization.

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

Product highlights:

- Automated object analysis in Windows, Linux and Android environments
- Custom images allow threat analysis across Windows operating systems and applications (only those that apply to real environments)
- The threat score based on metrics and data obtained during file execution shows the danger level of analyzed object
- On-premise deployment ensures that no data is exposed outside the organization
- Advanced anti-evasion techniques and human-simulating technologies
- Manual file/URL submission and RESTful API
- Support for analysis of over 100 file types with detailed analysis reports
- Custom Suricata rules to scan network traffic can be added and used together with the Suricata rules provided out-of-the-box
- The product supports bare metal deployment and can be easily scaled depending on the required performance

Kaspersky Research Sandbox high-level architecture



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.

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

To avoid exposure, a malicious file may first investigate if it's in a virtual machine or stay inactive 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. 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.

Detailed analysis reports

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.

Detection names

A list of detects (both AV and behavioral) that were registered during the file execution.

Triggered network rules

A list of network Suricata rules that were triggered during analysis of traffic from the executed object.

Execution map

A graphically represented sequence of object activities and the relationship between them.

Suspicious activities

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 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.

www.kaspersky.com