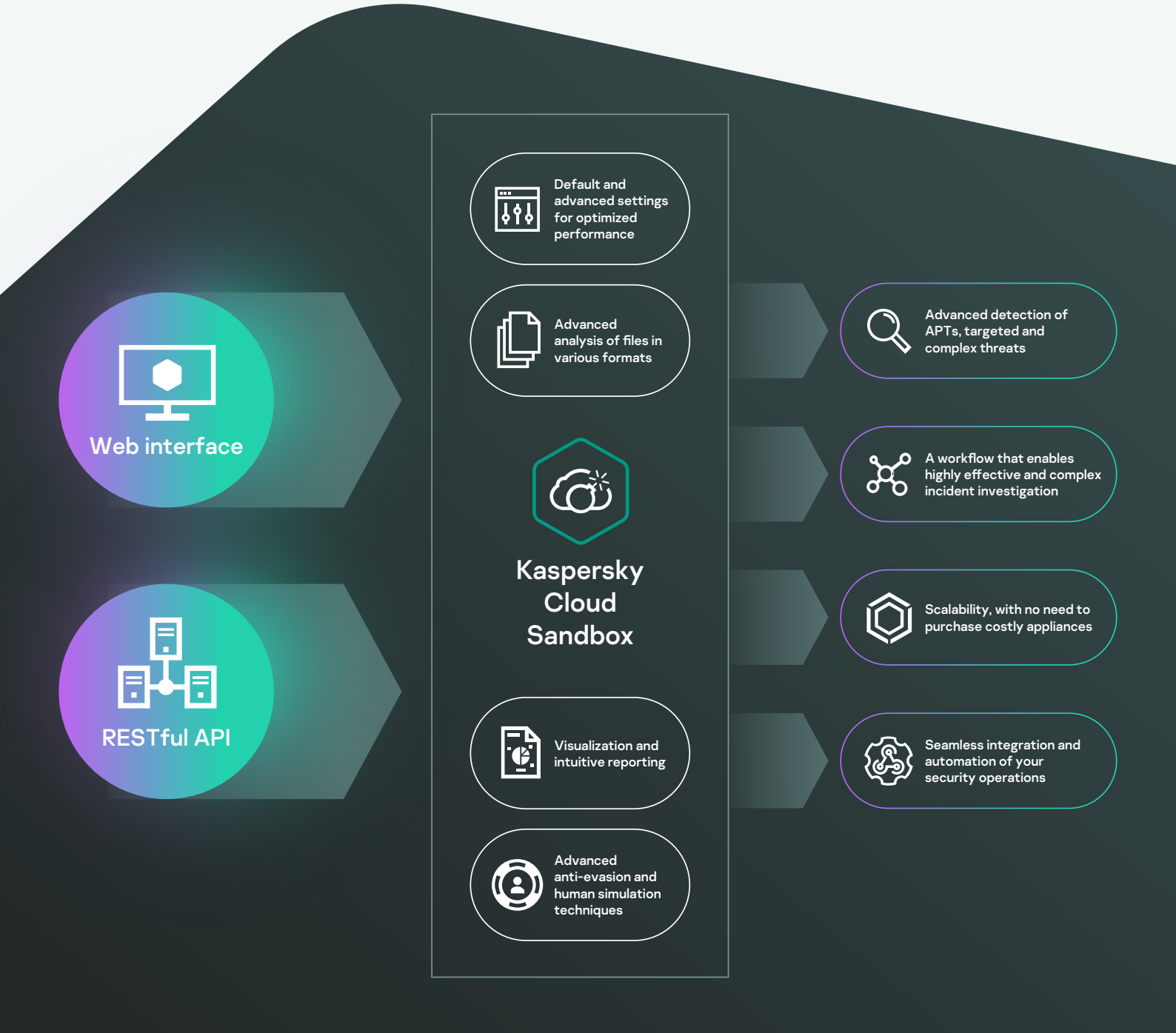
Kaspersky Cloud Sandbox

kaspersky BRING ON THE FUTURE

Kaspersky Cloud Sandbox

It's impossible to prevent today's targeted attacks just with traditional AV tools. Antivirus engines are capable of stopping only known threats and their variations, while sophisticated threat actors use all the means at their disposal to evade automatic detection. Losses from information security incidents continue to grow exponentially, highlighting the increasing importance of immediate threat detection capabilities to ensure rapid response and counter threats before any significant damage is done.

Making an intelligent decision based on a file's behavior while simultaneously analyzing the process memory, network activity, etc., is the optimal approach to understanding the latest sophisticated targeted and tailored threats. While statistical data may lack information on recently modified malware, sandboxing technologies are powerful tools that allow the investigation of file sample origins, the collection IOCs based on behavioral analysis and the detection of malicious objects not previously seen.



Comprehensive reporting

- Loaded and run DLLs
- External connections with domain names and IP addresses
- Created, modified and deleted files
- Detailed threat intelligence with actionable context for every revealed indicator of compromise (IOC)
- Process memory dumps and network traffic dumps (PCAP)
- HTTP and DNS requests and responses
- Created mutual extensions (mutexes)
- RESTful API
- Modified and created registry keys
- Processes created by the executed file
- Screenshots
- **and much more**

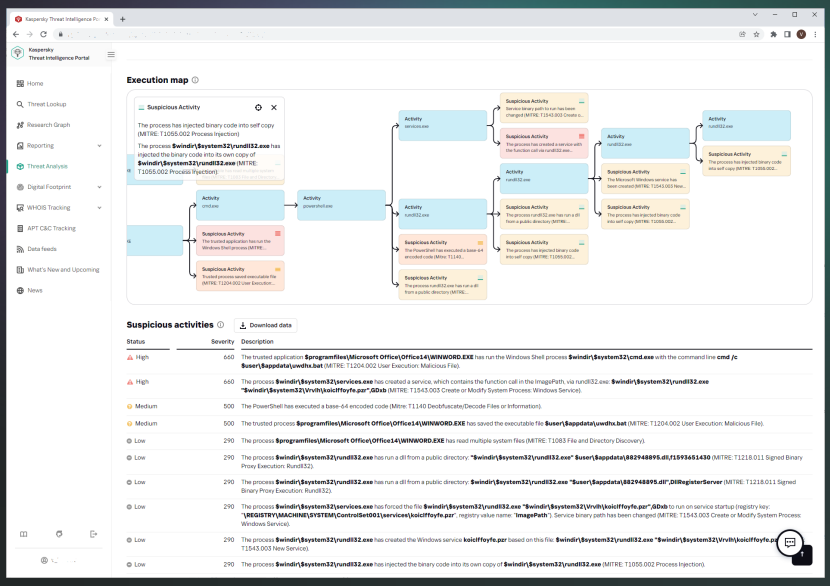
Proactive threat detection and mitigation

Malware uses a variety of methods to disguise its execution from being detected. 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 be capable of accurately mimicking normal end-user behavior.

Kaspersky Cloud Sandbox offers a hybrid approach combining threat intelligence gleaned from petabytes of statistical data (thanks to Kaspersky Security Network and other proprietary systems), behavioral analysis, and rock-solid anti-evasion, with human-simulating technologies such as auto clicker, document scrolling, and dummy processes.

This product has been developed in our in-house sandboxing lab, evolving for over a decade. The technology incorporates all our knowledge of malware behavior gained over 20 years of continuous threat research. This allows us to detect over 360 000 new malicious objects every day to provide our customers with industry-leading security solutions.

As part of our Threat Intelligence Portal, Cloud Sandbox is the important component in your threat intelligence workflow. While Threat Lookup retrieves the latest detailed threat intelligence about URLs, domains, IP addresses, file hashes, threat names, statistical/behavior data, WHOIS/DNS data, etc., Cloud Sandbox links that knowledge with the IOCs generated by the analyzed sample.



Now you can run highly effective and complex incident investigations, gaining an immediate understanding of the nature of the threat and connecting the dots as you drill down to reveal interrelated threat indicators.

Inspection can be very resource-intensive, especially when it comes to multi-stage attacks. Kaspersky Cloud Research Sandbox boosts your incident response and forensic activities, providing you with the scalability for processing files automatically without having to buy expensive appliances or worrying about system resources.

www.kaspersky.com