kaspersky BRING ON THE FUTURE

Kaspersky Cloud Sandbox

It's impossible to prevent today's targeted attacks purely 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 the threat 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 understand current 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.

Key Features:

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

Key Benefits:

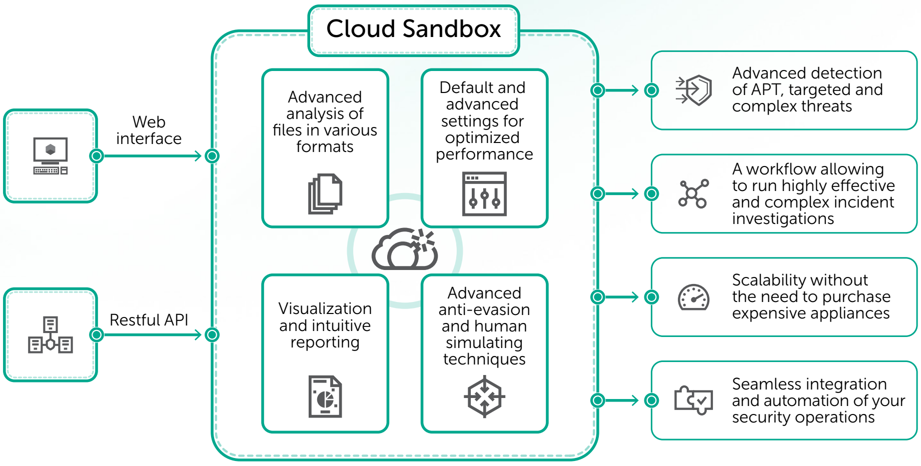
- Advanced detection of APTs, targeted and complex threats
- A workflow allowing the running of highly effective and complex incident investigations
- Scalability without the need to purchase costly appliances or worry about system resources
- Seamless integration and automationof your security operations

Proactive mitigation for threats circumventing your security barriers

Today's malware uses a whole variety of methods to avoid executing its code if this could lead to the exposure of 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 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. The result is an instrument of choice for the detection of unknown threats.

This product has been developed directly out of our in-lab sandboxing complex, a technology that's been evolving for over a decade. This technology incorporates all the knowledge about malware behaviors acquired by Kaspersky Lab during 20 years of continuous threat research, allowing us to detect 350 000+ new malicious objects each day and to provide our clients with industry-leading security solutions.


Cloud Sandbox
Web interface
Restful API
Advanced analysis of files in various formats
Default and advanced settings for optimized performance
Visualization and intuitive reporting
Advanced anti-evasion and human simulating techniques
Advanced detection of APT, targeted and complex threats
A workflow allowing to run highly effective and complex incident investigations
Scalability without the need to purchase expensive appliances
Seamless integration and automation of your security operations

As part of our Threat intelligence Portal, Kaspersky Cloud Sandbox is the final component that completes your threat intelligence workflow. While the portal retrieves the latest detailed threat intelligence about URLs, domains, IP addresses, file hashes, threat names, statistical/behavior data, WHOIS/DNS data, etc., Cloud Sandbox allows that knowledge to be linked to the IOCs generated by the analyzed sample.

Inspection can be very resource intensive, especially when it comes to multi-stage attacks. Kaspersky Cloud Sandbox is an ideal tool to boost incident response and forensic activities, providing you with the scalability for processing files automatically without purchasing expensive appliances or worrying about system resources.

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

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

www.kaspersky.com