kaspersky BRING ON THE FUTURE

Kaspersky Sandbox

Advanced detection capabilities to protect against unknown and evasive threats – without having to hire IT security professionals

Today's advanced cyberattacks have the power to paralyze companies and wreak financial and reputational havoc. Theft of financial assets and trade secrets, loss of customer confidence due to downed services and numerous other negative effects of complex threats have a serious impact on business stability and prosperity. To prevent rapidly evolving cyberattacks, traditional tools designed to protect the network perimeter (firewalls, email/web gateways, proxy servers), as well as workstations and servers (antivirus protection and Endpoint Protection Platform class solutions with basic functionality), are insufficient on their own. This is why forward-thinking companies need to seriously consider specialized tools for detecting, investigating and responding to complex incidents.

The Kaspersky Sandbox solution is suitable for:

- Companies with no dedicated security team, where the IT security role is assigned to the IT department.
- Small businesses that don't want to incur additional IT security resources.
- Large organizations with a geographically distributed infrastructure and without on-site IT security specialists.
- Companies who need to ensure that their full-time IT security analysts are fully focused on critical tasks.

For over twenty years, Kaspersky has been building protection tools for companies of every size, industry and level of IT security maturity. Due to continuous research and development, and the advances we've made in threat hunting, investigation and response, Kaspersky remains at the forefront of combating cybercrime.

Kaspersky's product and service portfolio for countering complex threats includes:

- Kaspersky Anti Targeted Attack, a cutting-edge solution for detecting and investigating complex threats and targeted attacks at the network level.
- Kaspersky Endpoint Detection and Response, a solution for detecting, investigating, and responding to complex cyberthreats aimed at workstations and servers
- Kaspersky Threat Intelligence Portal, providing access to the Cloud Sandbox, with analytical reports on APT threats, and other services

However, to effectively utilize these solutions and services, companies need to have a fully-fledged IT security department with the appropriate experience and expertise. The global shortage of specialists trained to deal with complex threats, and the cost of hiring them, is often the main factor that stops companies from acquiring these types of solutions and services.

Based on patented technology (patent no. US 10339301B2) Kaspersky Sandbox helps organizations fight the growing number and complexity of modern threats that can bypass existing endpoint protection. Complementing the functionality of Kaspersky Endpoint Security for Business, Kaspersky Sandbox allows organizations to significantly increase the level of protection of their workstations and servers against previously unknown malware, new viruses and ransomware, zero-day exploits, and others – without the need for highly specialized information security analysts.

This spares small businesses the expense of having to recruit and hire these highly valued professionals. It also helps large enterprises with distributed networks to optimize costs for effective protection of their remote offices while alleviating the manual workload on their security analysts.

Delivery and deployment options:
Kaspersky Sandbox is provided as an ISO image, with preconfigured CentOS 7 and all necessary solution components. It can be deployed on a physical server or on virtual servers based on VMware ESXi.

Integration:
- SIEM systems can receive information about detections made by Kaspersky Sandbox. This information is sent via Kaspersky Security Center in the general events flow.
- An API is implemented in Kaspersky Sandbox for integration with other solutions, allowing files to be sent to Kaspersky Sandbox for scanning and file reputations to be requested from it.

Scalability
With the basic configuration supporting up to 1,000 protected endpoints, the solution scales easily, providing continuous protection for large infrastructures

Clustering
Several servers can be clustered for more capacity and high availability.

Licensing
Kaspersky Sandbox is licensed as a software appliance. One license includes support for up to 1,000 users of Kaspersky Endpoint Security for Business.

How it works

Kaspersky Sandbox harnesses our expert best practices in combating complex threats and APT-level attacks, and is tightly integrated with Kaspersky Endpoint Security for Business. It's managed from Kaspersky Security Center, our unified policy-based management console.

The Kaspersky Endpoint Security for Business agent requests data about a suspicious object from the shared operational cache of verdicts, located on the Kaspersky Sandbox server. If the object has already been scanned, Kaspersky Endpoint Security for Business receives the verdict and applies one or more remediation options:

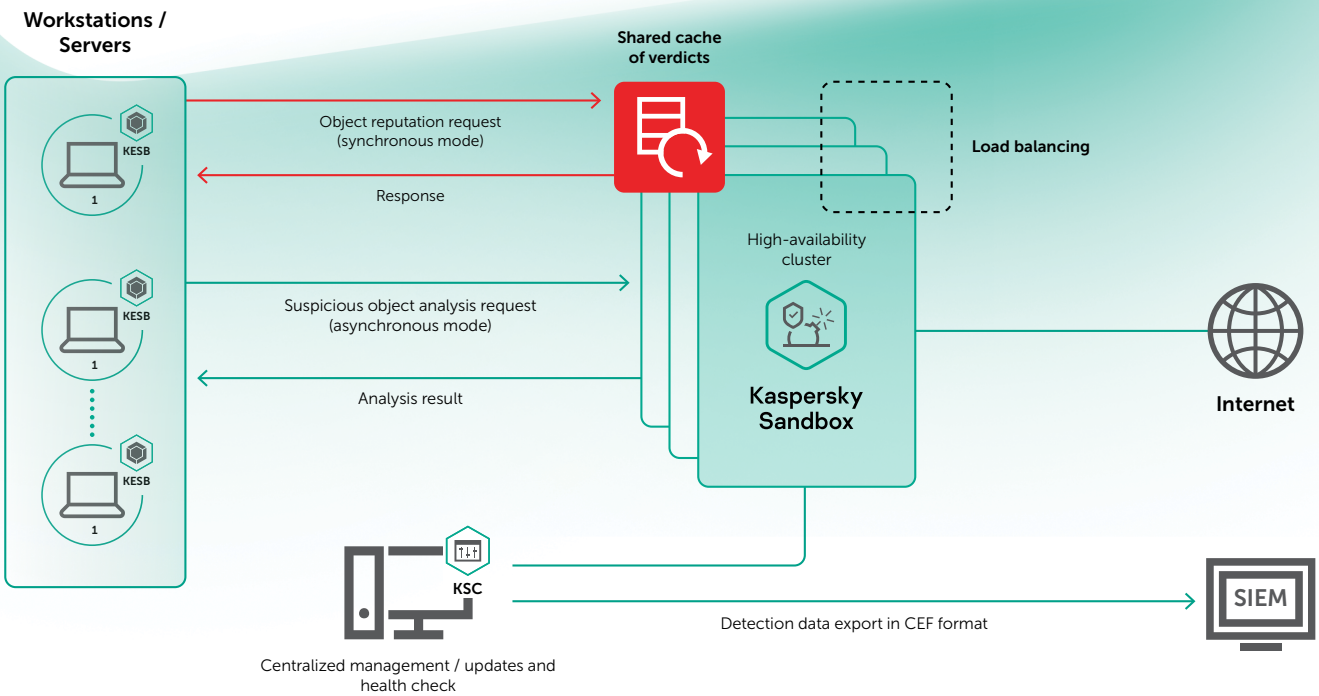
- Remove and quarantine
- Notify user
- Start a critical areas scan
- Search detected object on other machines within the managed network.

If the verdict on an object's reputation can't be obtained from cache, the Kaspersky Endpoint Security for Business agent sends the suspicious file to the Sandbox and waits for a response. The Sandbox receives a request to scan the object, at which point the test object is run in an environment isolated from the real infrastructure.

File scanning is performed in virtual machines equipped with tools that emulate a typical working environment (operating systems/installed applications).To detect the malicious intent of an object, behavioral analysis is carried out, artifacts are collected and analyzed, and if the object performs malicious actions, the Sandbox recognizes it as malware. During sandbox analysis, a verdict is assigned to the object.

Once the object emulation process is complete, the resulting verdict is sent in real-time to the shared operational cache of verdicts, allowing other hosts with Kaspersky Endpoint Security for Business installed to quickly obtain data on the reputation of the scanned object without having to analyze the same file again. This approach ensures rapid processing of suspicious objects, reduces the load on Kaspersky Sandbox servers, and improves the speed and efficiency of the response to threats.

Kaspersky Sandbox is an essential addition to Kaspersky Endpoint Security for Business. It automatically blocks advanced, unknown and complex threats without the need for additional resources, and frees up IT security analysts to focus on other tasks.



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

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 tommorow.

Know more at kaspersky.com/transparency

Proven.
Transparent.
Independent.