kaspersky BRING ON THE FUTURE

Kaspersky Sandbox

Fully automated advanced detection and remediation against evasive threats

Key benefits

- Advanced protection from the growing number of new, unknown and evasive threats
- Easy to manage – fully automated
- No additional investments in internal IT security expertise necessary
- No impact on systems performance and user experience/productivity
- Part of the Kaspersky security ecosystem, providing seamless multi-layered protection

Evasive threats

Some threats try to avoid detection by not performing any actions which are likely to be picked up by behavior detection, effectively staying dormant until the defenses of the endpoint are weakened – usually following a human mistake.
Another way of avoiding detection is to perform actions over a very long period of time, hours or days, which can extend beyond the correlation period for endpoint protection software's behavior analysis.

The challenge

Today's threats use a wide range of techniques to avoid detection by endpoint protection platforms. These evasive threats include:

- Previously unknown malware
- New viruses and ransomware
- Zero-day exploits, and others

This leads to threats being able to burrow into targeted systems and stay undetected for prolonged periods of time, radically increasing the damage, be it data exfiltration, ransomware, financial or other types of spyware.

The solution

Kaspersky Sandbox automatically detects evasive threats, even dormant ones, by using sophisticated patented detection technology[1].

The algorithm uses dynamic emulation of threats, allowing them to run in a seemingly unprotected isolated environment, and analyzes the file's behavior and generated traffic by a variety of factors.

Today's malware usually tries to detect if it's in a sandbox and evade detection, which is why Kaspersky Sandbox uses a variety of advanced anti-evasion and non-intrusive monitoring techniques.

Use cases

Kaspersky Sandbox's enhanced detection is especially effective at uncovering those techniques that evasive malware uses to avoid being discovered by even the most sophisticated endpoint behavior analysis engine. These techniques include, but are not limited to:

- Keylogging
- Taking screenshots
- Hidden recording of audio and video streams
- Use of multiple interpreters (e.g. malware runs .bat, which runs PowerShell, which runs VBS script)
- Passwords grabbing (e.g. from browsers)
- Crypto wallet addresses replacement in clipboard

Usability

Kaspersky Sandbox is designed for smaller cybersecurity teams and for organizations whose cybersecurity is handled by IT Operations. It's built for maximum automation, ease of deployment and endpoint productivity – and managed from a centralized console as a part of the Kaspersky security ecosystem.

[1] Patent no. US 10339301B2

Part of the Kaspersky security ecosystem

Kaspersky Sandbox is a part of the Kaspersky Optimum Security solution, designed to allow smaller IT security teams to take on evasive threats without overextending their resources. Learn more here: https://go.kaspersky.com/optimum

Delivery and scalability

Kaspersky Sandbox is provided as a preconfigured ISO image and can be deployed on physical or virtual servers. With configurations supporting from 250 up to 5000 protected endpoints, the solution scales easily, providing continuous protection for infrastructures of any size. Several servers can be clustered for more capacity and high availability.

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.

How it works

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 actions:

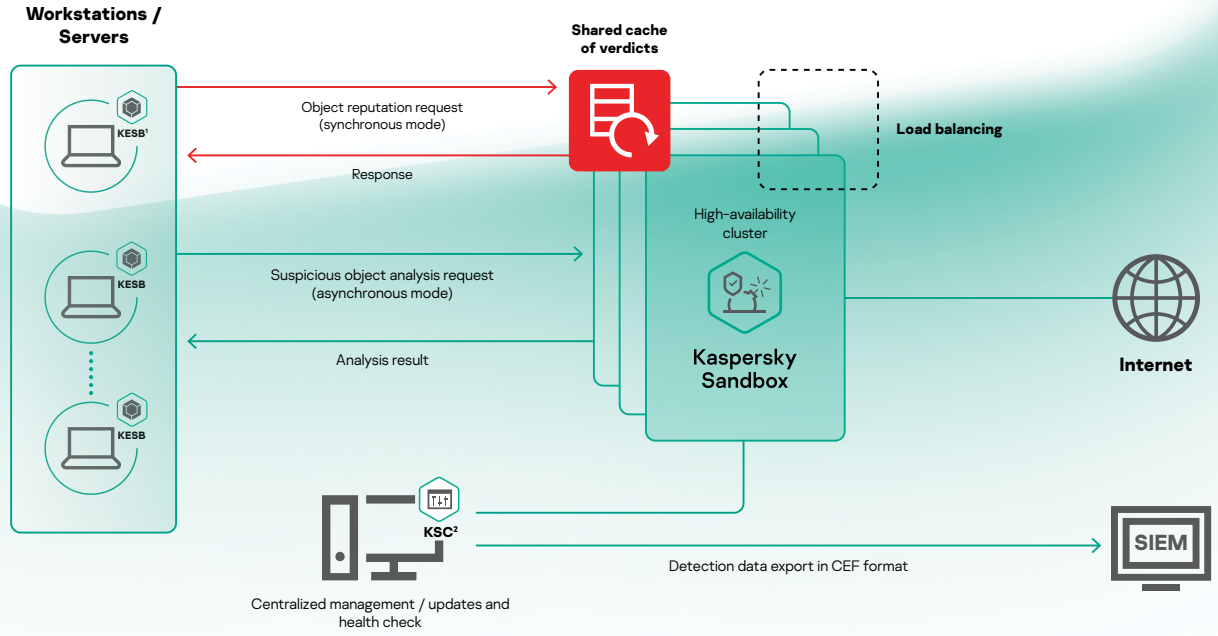
- Remove and quarantine
- Notify user
- Start a critical areas scan
- Search detected object on other machines within the managed network

If the verdict on an object's reputation can't be obtained from cache, the 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 and traffic analysis are 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 or Kaspersky Endpoint Detection and Response Optimum 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 Optimum Security. It automatically blocks new, unknown and evasive threats without the need for additional resources, and frees up IT security analysts to focus on other tasks



[1] Kaspersky Endpoint Security for Business
[2] Kaspersky Security Center

To find out more about how Kaspersky Sandbox enhances your protection against evasive threats, visit http://www.kaspersky.com/enterprise-security/malware-sandbox.

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.