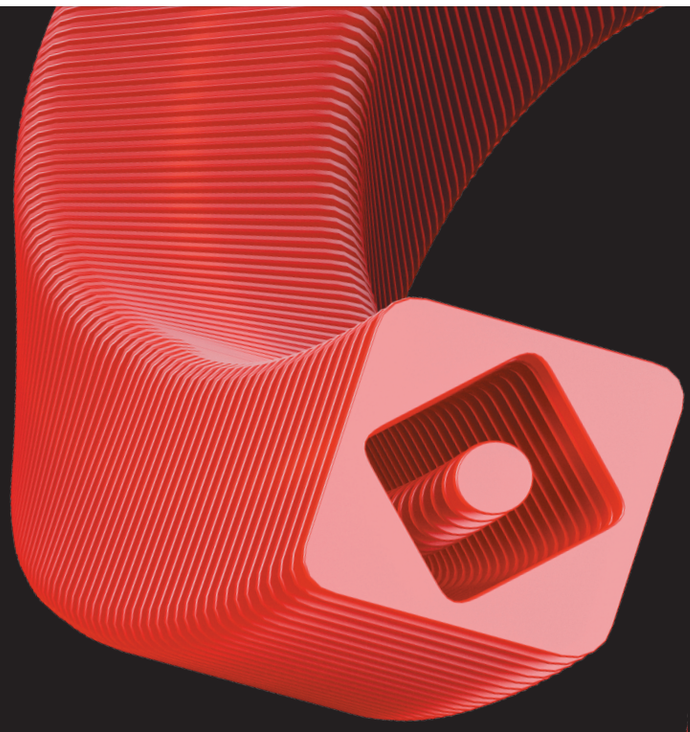
positive technologies



PT Sandbox

A network sandbox for detecting complex targeted malware attacks

PT SANDBOX DETECTS THREATS IN:

- **Email**
- **File storage**
- **User web traffic**
- **Corporate network traffic**
- **Web portals where files are scanned manually**
- **Corporate systems, including document management systems**

PT EXPERT SECURITY CENTER EXPERTISE

PT ESC is Positive Technologies expert security center. PT ESC specialists investigate incidents in large companies and constantly monitor activity of hacker groups. Threat intelligence generated during these investigations is promptly delivered to PT Sandbox.

In half of all cyberattacks, criminals use malware disguised as regular files and links in order to bypass antivirus software, firewalls, IDSs, IPSs, email and web gateways. According to Positive Technologies, 70% of companies experience malware activity missed by basic protection tools.

Solution

PT Sandbox is a risk-driven network sandbox that detects sophisticated cyberthreats even if an attacker is hiding in a network. PT Sandbox protects against targeted and mass malware attacks and zero-day threats, and detects both common malware (encryption malware, ransomware, spyware, remote control utilities, and loaders) and sophisticated hacker tools, such as rootkits and bootkits.

Each object is analyzed in PT Sandbox using machine learning technologies, as well as static and dynamic methods with the help of the unique rules of PT Expert Security Center (PT ESC), and scanned by several antivirus engines.

PT ESC expert knowledge on the latest threats are added to PT Sandbox within 2.5 hours. This allows you to protect your company against a cyberattack when a criminal tries to exploit a zero-day vulnerability for which a patch has not yet been released.

Advantages

Adjusts to the specifics of your business
A key feature of PT Sandbox is that it can adjust protection to compan-specific IT infrastructure and business processes. For this, the following mechanisms are in place:

- **Support of virtual environments for analysis** (Windows of various versions and Russian operating systems such as Astra Linux and RED OS). PT Sandbox fully covers MITRE ATT&CK tactics and techniques that criminals may use to attack these operating systems.
- **Flexible customization of virtual environments.** You can enhance your virtual environments by adding specific software or software versions used at your company that could potentially serve as an entry point for attackers.
- **Detection of threats both in corporate and industrial sectors.** The industrial version of PT Sandbox analyzes objects in an industrial virtual environment and detects specific malware targeting ICS components.
- **Honeypots that provoke malware to act, making an attacker visible.** Files created as honeypots contain fake credentials, configuration files, or other seemingly valuable data. Processes used as honeypots mimic operational banking systems, development software, and user activity. PT Sandbox detects attempts to steal from or infiltrate honeypots. Most honeypots for Windows and Linux are ready to be used out of the box; PT ESC can also create tailored honeypots to imitate your business-critical systems.

OTHER CAPABILITIES

High performance

Flexible management of file and link processing and unlimited horizontal scalability of PT Sandbox ensure high performance under any load.

Monitoring and blocking modes

PT Sandbox monitors threats and blocks malware in automatic mode.

Easy integration

PT Sandbox supports multiple out-of-the-box integration options and has a flexible API, which allows you to use the product in any configuration of information systems.

Positive Technologies ecosystem support

PT Sandbox can be smoothly integrated with MaxPatrol SIEM, PT Application Firewall, PT ISIM, PT Network Attack Discovery, and PT XDR.

On-premise option

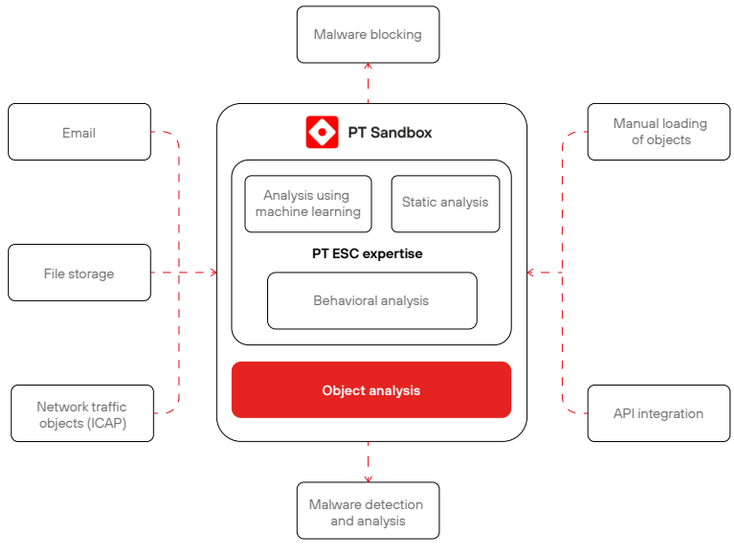
Confidential files do not leave the company perimeter when being checked.

Detection of previously missed threats.

PT Sandbox performs regular retrospective analysis of previously checked files after the knowledge base has been updated. This allows you to detect threats hidden in the infrastructure as quickly as possible and respond to attacks before criminals have reached their target.

Threat detection in files and traffic.

PT Sandbox checks files, analyzes traffic generated during file analysis, and detects malicious activity hidden by TLS encryption. This approach significantly improves the efficiency of attack detection, even in encrypted traffic.



How PT Sandbox works

TEST PT SANDBOX AT YOUR COMPANY

To assess the efficiency of PT Sandbox in your infrastructure, sign up for a pilot project.

global.ptsecurity.com
info@ptsecurity.com

Positive Technologies is an industry leader in result-driven cybersecurity and a major global provider of information security solutions. Our mission is to safeguard businesses and entire industries against cyberattacks and non-tolerable damage. Over 4,000 organizations worldwide use technologies and services developed by our company.

PT-SANDBOX_A4.0010.005.SEPT.22.2023