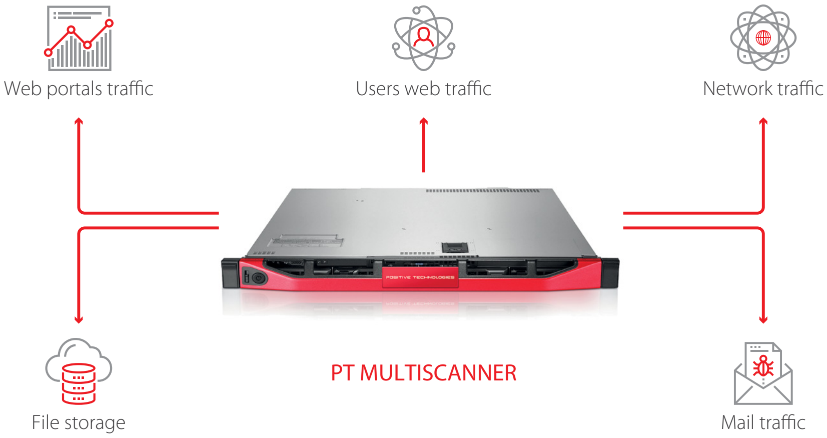
POSITIVE TECHNOLOGIES

PT MULTISCANNER:
MULTILAYERED PROTECTION AGAINST MALWARE ATTACKS

Malware is hitting companies hard. According to Positive Technologies research, 39% of digital attacks in 2017 involved use of viruses or other malicious software.[1] Around 350,000 new copies of malware appear every day, while malware as a service is putting advanced threats in the hands of anyone willing to pay. Malware detection technology continues to improve—but not quickly enough to respond to the threat. Problems with the conventional approach include:

- Difficulty of localizing distributed attacks as well as their past and current consequences
- Single-vendor monocultures for malware protection
- No single point for monitoring all objects in infrastructure traffic

As a multistream malware detection system, PT MultiScanner makes these drawbacks a thing of the past. With a more modern approach, it is easier to detect, track, and block the spread of malware on corporate infrastructure both in real time and retrospectively.



PT MultiScanner is a server-based solution that deploys on existing infrastructure to monitor and block threats wherever they are: email, the web, file storage, or web portals traffic. The system detects infected objects in all kinds of data streams, aggregating similar attacks into threat chains. These chains are the best way to spot mass infections and investigate, especially for events that occur gradually over time and would be easy for humans to overlook.

BENEFITS

- **Threat localization**
  Pinpoint who is sending and spreading malware in order to investigate and react to threats.
- **Detection of advanced persistent threats (APTs)**
  With PT MultiScanner, gain an additional layer of protection for reacting to complex multistage attacks. Use retrospective analysis to spot incidents caused by zero-day vulnerabilities, and uncover malware hidden on network infrastructure.
- **Single point of insight**
  Centrally store and analyze objects across all traffic flows for ease of investigation.

[1] Cybersecurity threatscape 2017: trends and forecasts, Positive Technologies

KEY FEATURES

+ **Multivendor approach**
Suspicious objects are scanned with a multiple anti-malware engines, static analysis, and Positive Technologies reputation lists. The solution supports scaning for both files and archives, including recursively compressed.

+ **Full coverage of all data flows**
PT MultiScanner detects and blocks malicious activity all across corporate infrastructure: web portals, file storage, network traffic, web traffic, and email.

+ **Retrospective analysis**
Thanks to retrospective analysis, the solution detects stealthy malware buried deep in infrastructure as well as the newest threats.

+ **Ease and convenience**
Centralized monitoring of malicious activity across all data flows makes it easy to track and localize threats. Intuitive interface makes all information readily available to security staff in at-a-glance dashboard form.

+ **Speed of deployment**
PT MultiScanner supports all the important standard interfaces (SPAN, MTA, BCC, ICAP, REST API) and deploys in less than one hour.

+ **Scalability and high availability**
The architecture is perfect for scaling both vertically and horizontally. It is fully fit for cluster deployment in active–active configuration with one central management console.

ALL-AROUND PROTECTION WITH PT MULTISCANNER

Corporate traffic (monitoring)

Scanning of files via SPAN mirroring of network traffic in real time. Enriched event context in protection systems (IPS/IDS, SIEM). Rapid incident reaction and investigation.

Mail traffic (monitoring and blocking)

Online verification of email messages. Detection of malicious attachments and senders (with an attachment sanitizing for most common file extensions, such as .docx, .xlsx, .rtf, .pptx, .pdf, .html, .jpg, .zip, etc.). Scanning of mail archives (including multipart and password-protected ones). Protection against malware infection attempts involving social engineering.

Users web traffic (monitoring and blocking)

Strengthened perimeter security thanks to detection of malicious content in files downloaded from external subnets (including via HTTPS).

Web portals (monitoring and blocking)

Active protection of sites against malicious content. Detection of data leaks and bots. Verification of user-originated content.

File storage (monitoring and blocking)

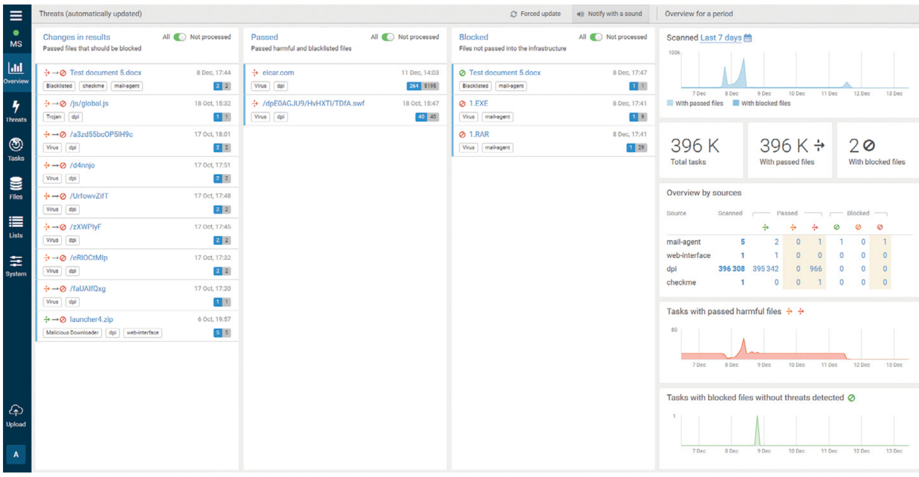
Detection of malicious content, infected executables and documents. Rapid blocking to prevent spread of malicious files. Retrospective scanning and re-scanning of potential threats when knowledge bases are updated.

Internal service

Manual scanning of files. Knowledge base. Statistics about verdicts and downloaded objects. User alerts if malware is detected in previously downloaded files.

Incident investigation

Tools and information needed to support the investigation process. Retrospective identification of attacked hosts and analysis of vectors used for attack spread.



Threats (automatically updated)

Changes in results — All / Not processed
Passed files that should be blocked

- Test document 5.docx — 8 Dec, 17:44 — Blacklisted, checkme, mail-agent — 2 2
- /js/global.js — 18 Oct, 15:32 — Trojan, dpi — 1 1
- /a3zd55bcOP5lH9c — 17 Oct, 18:01 — Virus, dpi — 2 2
- /d4nnjo — 17 Oct, 17:51 — Virus, dpi — 2 2
- /UrfowvZifT — 17 Oct, 17:48 — Virus, dpi — 2 2
- /zXWPlyF — 17 Oct, 17:45 — Virus, dpi — 2 2
- /eRlOCtMlp — 17 Oct, 17:32 — Virus, dpi — 2 2
- /faUAlfQxg — 17 Oct, 17:20 — Virus, dpi — 1 1
- launcher4.zip — 6 Oct, 19:57 — Malicious Downloader, dpi, web-interface — 5 5

Passed — All / Not processed
Passed harmful and blacklisted files

- elcar.com — 11 Dec, 14:03 — Virus, dpi — 264 5195
- /dpE0AGJU9/HvHXTI/TDfA.swf — 18 Oct, 15:47 — Virus, dpi — 40 40

Blocked — All / Not processed
Files not passed into the infrastructure

- Test document 5.docx — 8 Dec, 17:47 — Blacklisted, mail-agent — 1 1
- 1.EXE — 8 Dec, 17:41 — Virus, mail-agent — 1 9
- 1.RAR — 8 Dec, 17:41 — Virus, mail-agent — 1 29

Overview for a period

Scanned Last 7 days

396 K Total tasks

396 K ÷ With passed files

2 ⊘ With blocked files

Overview by sources

Source	Scanned	Passed			Blocked		
		÷	÷	÷	⊘	⊘	⊘
mail-agent	5	2	0	1	1	0	1
web-interface	1	1	0	0	0	0	0
dpi	396 308	395 342	0	966	0	0	0
checkme	1	0	0	1	0	0	0

Tasks with passed harmful files ÷ ÷

Tasks with blocked files without threats detected ⊘

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com