positive technologies

MaxPatrol Endpoint Detection and Response

Protecting company and employee devices from complex targeted attacks

78% of attacks in 2023 were targeted

Top 3 that attackers are using right now: ransomware, infostealers, remote access trojans

Trends

MaxPatrol EDR

MaxPatrol EDR helps promptly detect complex and targeted attacks, ensuring confident response and automation of routine operations while taking into account the characteristics of your company's infrastructure and security processes.

- Identifies attacks developing on devices at early stages that may be missed by other security tools.
- Collects important data for investigations.
- Stops the attacker in seconds.
- Helps SOC analysts and cybersecurity service managers to investigate and prevent attacks by blocking malicious actions on end devices.

- Autonomous agent operation capability
- Static and behavioral analysis on the agent
- Flexible configuration of detection and response rules
- Doesn't conflict with other security solutions
- Customizable file sandboxing
- Support for Windows, Linux, macOS

Instant response on hosts

Offers an extensive set of actions for automatic and timely response: process termination, file deletion, device isolation, sending files for analysis, and sinkholing.

Dynamic threat detection

Detects attacks that use legitimate tools (PowerShell, WMI, CMD, Bash) that traditional signature-based analysis may overlook.

Timely and continuous detection of malware

Comes with a set of expert PT ESC rules enabling the identification of threats and common attacker tactics and techniques from the MITRE ATT&CK matrix (top 50 for Windows and top 20 for Linux).

Easy integration into infrastructures

Acts as a single agent for detection, response, and collection of telemetry and information about vulnerabilities on hosts. Supports operation on all popular operating systems, including Russian ones, and in VDI structures.

Suitable for different organizations

Saves specialists' time and resources

Building layered protection based on comprehensive solutions or integrating multiple products is not always in the organization's budget. With MaxPatrol EDR, you can affordably begin to protect your employees' and organization's devices and gradually establish security processes.

Doesn't conflict with othe security solutions

Organizations can use multiple protective solutions, making the most of different vendors' expertise without affecting business processes.

Adapts to infrastructure features

Allows flexible configuration of detection and response policies as required by the architecture. Maintains an ideal balance between host load and meeting SOC requirements.

Automates response functions

Often, EDR solutions have no automatic response functions other than terminating processes and deleting files. MaxPatrol EDR lets you control the logic and use all available response options both manually and automatically.

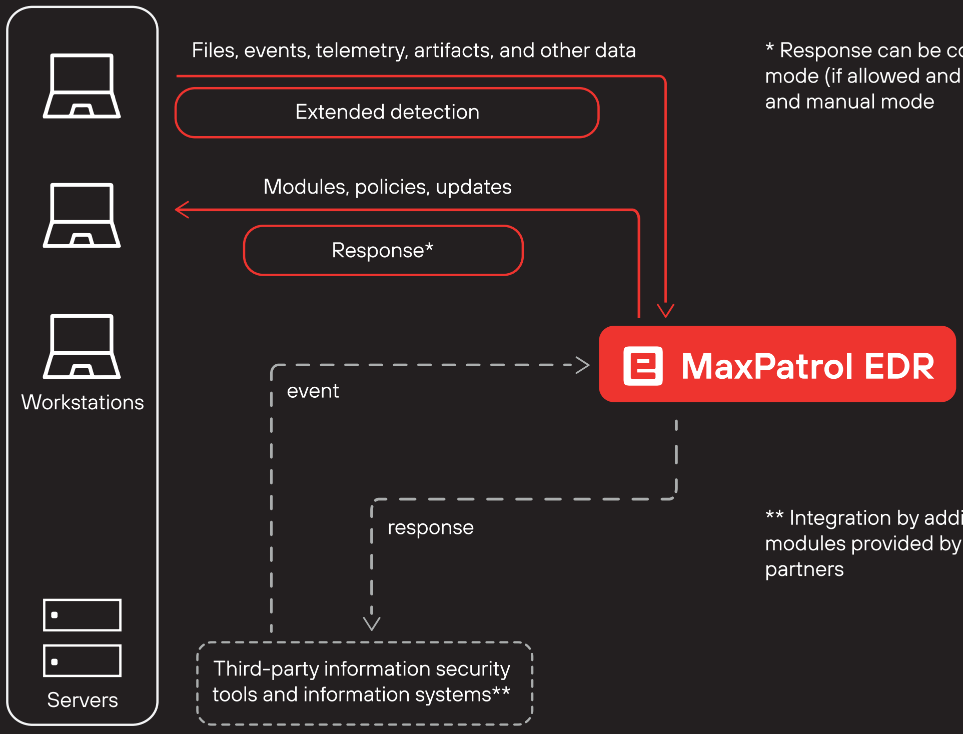
Works in closed segments

Doesn't require Internet access to function. Expertise updates can be delivered via an intermediary server if one-way transmission is required.

Has a familiar logic and interface

MaxPatrol EDR is created in the same style as other Positive Technologies products and provides familiar entities, authentication, services, and cross-product scenarios, ensuring an easy start for the user.

How MaxPatrol EDR works



Files, events, telemetry, artifacts, and other data
Extended detection
Modules, policies, updates
Response*
MaxPatrol EDR
event
response
Workstations
Servers
Third-party information security tools and information systems**

* Response can be configured both in automatic mode (if allowed and supported by the policy) and manual mode

** Integration by adding custom functional modules provided by Positive Technologies and partners

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.