positive technologies

# MaxPatrol VM

A vulnerability management system

## MaxPatrol VM CAPABILITIES

**Keeps IT infrastructure data up to date.** MaxPatrol VM uses active and passive data collection mechanisms to obtain comprehensive asset information.

**Automates asset management.** MaxPatrol VM automatically identifies assets, allowing you to assess their importance, assign them to groups, and control asset scanning and data aging.

**Identifies and prioritizes vulnerabilities.** MaxPatrol VM leverages its continuously updated knowledge base to assess the asset security level.

**Helps establish a vulnerability management process.** MaxPatrol VM allows you to define scanning and remediation policies and control compliance with them.

**Monitors trending vulnerabilities.** Positive Technologies provides expert information on the most relevant critical vulnerabilities within 12 hours.

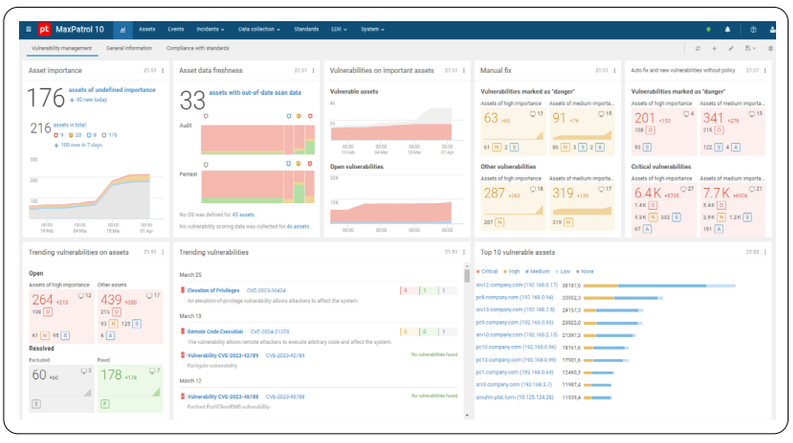
**MaxPatrol VM** is a system that helps build a full-fledged vulnerability management process, making it difficult and costly for attackers to penetrate your network.
**It is an advanced solution with guaranteed delivery of intelligence on trending vulnerabilities within 12 hours.**

MaxPatrol VM is based on a unique security asset management (SAM) technology. This allows MaxPatrol VM to collect data in active and passive mode, identify assets by multiple parameters, and use them to build an up-to-date model of your IT infrastructure. It gives the cybersecurity team a full overview of the IT environment to be protected. Based on this information, the team can build and automate a vulnerability management process, taking into account the importance of network components for business processes and keeping track of all infrastructure changes.

MaxPatrol VM separates asset intelligence and vulnerability detection. It remembers the results of previous asset scans and uses them to automatically calculate the relevance of a new vulnerability to your network hosts.

This helps detect new vulnerabilities without additional scanning, enabling a much faster response by initiating immediate remediation or applying compensating controls.

The **MaxPatrol HCC module in MaxPatrol VM** allows you to check if your infrastructure is compliant with practical cybersecurity standards. It has dynamic dashboards that help you track the fulfillment of the most crucial requirements relevant to your assets. You can customize the checks to accommodate your company's specific demands and set remediation deadlines.




**MaxPatrol VM interactive dashboard**

## ADVANTAGES OF MaxPatrol VM

**Deep integration** with SIEM and NTA systems and mutual enrichment of asset intelligence

Full **depiction** of your IT environment thanks to unique asset discovery technology

**Rapid vulnerability detection** without rescanning, enabled by stored asset intelligence

**Expert support** and notification of novel high-severity vulnerabilities within 12 hours

**Comprehensive automation** of asset security analysis and asset management

**TRY A PILOT DEPLOYMENT**

**Test MaxPatrol VM on your infrastructure.** Fill out a form on our website and start building your vulnerability management process.

## With MaxPatrol VM, you can:

- Get complete and continuously updated information about your IT infrastructure.
- Take into account the significance of assets to be protected.
- Identify and prioritize vulnerabilities and configure vulnerability processing rules.
- Rapidly detect novel high-severity vulnerabilities.
- Control vulnerability remediation and monitor the company's overall security posture.

## How MaxPatrol VM works

**Maintains an up-to-date asset databas**

MaxPatrol VM collects the most complete asset intelligence. The database is populated with data obtained by black- and white-box scanning and data imports from various sources: external directories (Active Directory, SCCM, hypervisors) and other cybersecurity solutions that analyze events and traffic (SIEM and NTA systems). A proprietary asset discovery algorithm consolidates information about a particular host even if the data comes from multiple sources.

**Evaluates and classifies assets**

Classification of assets by their importance level keeps the focus on high-priority hosts while monitoring the appearance of new assets. The system also reports unassessed assets and alerts you to those which are potentially important.

**Vulnerability detection and prioritization**

MaxPatrol VM performs an in-depth inspection of your IT infrastructure: it detects vulnerabilities and configuration errors in information system components and helps you set up remediation activities, taking into account the vulnerability severity level and parameters of the vulnerable asset (vendor, OS version, and settings).

**Defines policies**

Scanning and remediation policies in MaxPatrol VM automate various operations on assets and detected vulnerabilities. For example, you can define a scan schedule or a date for routine processing of vulnerabilities on multiple assets.

**Monitors trending vulnerabilities**

Positive Technologies provides intelligence on novel high-severity vulnerabilities within 12 hours. This allows you to promptly detect them in your infrastructure and schedule high-priority scanning of potentially vulnerable systems.

**Coordinates vulnerability management**

MaxPatrol VM tracks the statistics of regular scans. This information helps cybersecurity experts to control the scanning quality. In addition, retrospective analysis enables you to assess the progress of vulnerability remediation and also monitor infrastructure security level and compliance with policies.

global.ptsecurity.com
info@ptsecurity.com

Positive Technologies is an industry leader in result-driven cybersecurity and a major global providerof 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.

MP-VM_A4.ENG.0001.09.APR.2024