POSITIVE TECHNOLOGIES

MaxPatrol VM

Next-Generation Vulnerability Management System

MAXPATROL VM CAPABILITIES

Continuously updates data related to IT infrastructure. MaxPatrol VM uses active and passive data collection to obtain full information.

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

Detects and prioritizes vulnerabilities. MaxPatrol VM leverages the continuously updated knowledge base in assessing the level of asset protection.

Establishes the vulnerability management process. Allows you to set scanning and vulnerability elimination policies and ensure compliance.

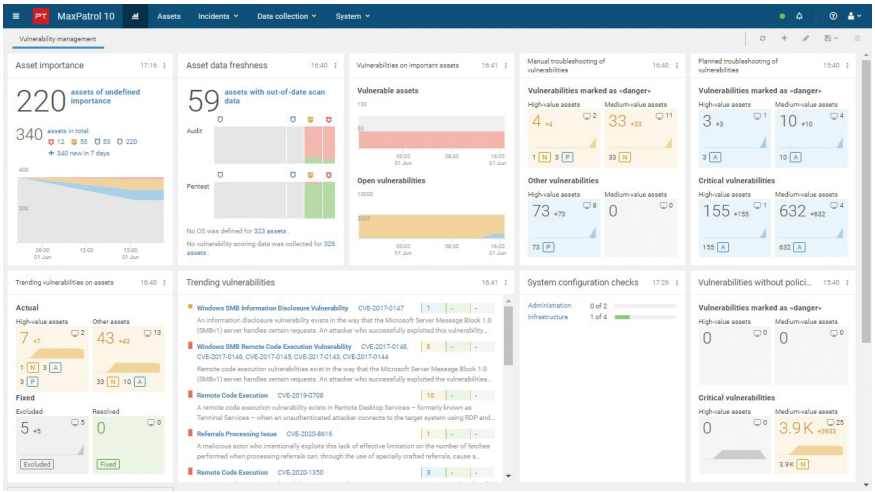
Monitors trending vulnerabilities. The PT expert team delivers up-to-the-second intelligence on critical vulnerabilities.

MaxPatrol VM lets you build a full-fledged vulnerability management process and monitor the security of the IT infrastructure at all times.

MaxPatrol VM is based on the 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 the IT infrastructure. In this way, the solution shows what the protected IT environment looks like. Infosec experts can then adopt and automate the vulnerability management process, assessing the importance of network components for business processes and covering all company systems with due regard to infrastructure changes.

MaxPatrol VM separates asset intelligence and vulnerability identification. The solution remembers the results of previous asset scans, on which basis it automatically calculates the applicability of a new vulnerability to network nodes. This detects new vulnerabilities without additional scanning, enabling a much faster response by initiating immediate elimination or compensatory measures.

To make it easier to monitor the level of infrastructure security, MaxPatrol VM provides interactive dashboards. These help to track the status and validity of critical asset scans, the appearance of new unassessed network assets, the number of high-severity vulnerabilities, and vulnerability elimination metrics.



MaxPatrol VM interactive dashboard

MAXPATROL VM ADVANTAGES

Part of the all-in-one security platform MaxPatrol 10 for deep integration with SIEM- and NTA-class products and cross-fertilization of asset intelligence

In-depth understanding of the IT environment due to the unique asset detection technology

Real-time vulnerability identification without rescanning on account of storing asset intelligence

Expert support with notification of high-severity vulnerabilities

Maximum automation of asset protection management and analysis

GET FREE PILOT

Assess the capabilities of MaxPatrol VM on your infrastructure — fill out an application form online and harness Positive Technologies expertise to build your own vulnerability management process.

With MaxPatrol VM you can:

- Get complete and continuously updated data on the IT infrastructure.
- Factor in the significance of protected assets.
- Identify, prioritize, and set vulnerability processing rules.
- Identify new dangerous vulnerabilities in real time.
- Control vulnerability elimination and monitor the company's overall security level.

How it works

COLLECTS AND MAINTAINS AN UP-TO-DATE ASSET DATABASE

MaxPatrol VM collects the most complete asset intelligence. The database is refreshed and populated by scanning in black- and white-box mode and importing data from various sources: external directories (Active Directory, SCCM, hypervisors) and other infosec solutions (SIEM and NTA systems based on event and traffic analysis). The proprietary asset discovery algorithm consolidates intelligence on the same network node, even if obtained from different sources.

EVALUATES AND CLASSIFIES ASSETS

Classification of assets by level of importance keeps the focus on priority nodes while tracking new assets as they appear. The system additionally reports unassessed assets as well as potentially significant ones.

IDENTIFIES AND PRIORITIZES VULNERABILITIES

MaxPatrol VM performs deep scanning of the IT infrastructure: it detects vulnerabilities and configuration errors in information system components, and allows vulnerability elimination methods to be set in line with severity levels and other parameters (vendor, OS version, asset on which vulnerabilities were found).

DEFINES POLICIES

MaxPatrol VM scanning and elimination policies automate the execution of various operations on assets and detected vulnerabilities. For example, you can set a recommended scan schedule or a date for routine processing of vulnerabilities on multiple assets.

MONITORS TRENDING VULNERABILITIES

Current vulnerability intelligence provided by Positive Technologies allows real-time discovery of high-severity vulnerabilities on the infrastructure, plus scheduled priority scanning of systems where they might be present.

CONTROLS VULNERABILITY MANAGEMENT

MaxPatrol VM tracks the dynamics of regular scans, which helps infosec experts to control scan quality. Retrospective analysis makes it possible to assess the vulnerability elimination process and monitor compliance with policies and the level of infrastructure protection.

About Positive Technologies

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

For 19 years, Positive Technologies has been creating innovative solutions for information security. We develop products and services to detect, verify, and neutralize the real-world business risks associated with corporate IT infrastructure. Our technologies are backed by years of research experience and the expertise of world-class cybersecurity experts.

Over 2,000 companies in 30 countries trust us to keep them safe.

Follow us on social media (LinkedIn, Twitter) and the News section at ptsecurity.com.