Kaspersky Vulnerability Management

Stop vulnerabilities and misconfigurations from becoming incidents

kaspersky

Not every vulnerability is critical. But any vulnerability can become an entry point.

The number of vulnerabilities is growing faster than security teams can process them. New CVEs appear every day, critical fixes are delayed for weeks, and manual prioritization leaves security teams with too little time to focus on the vulnerabilities that truly matter.

Kaspersky Vulnerability Management

Kaspersky Vulnerability Management helps organizations move from fragmented scanning to a managed process, with asset visibility, regular vulnerability detection, configuration assessment, patch management and remediation control.

The solution helps teams see real risks, remediate critical weaknesses faster and reduce operational workload without adding unnecessary infrastructure complexity.

Up to 44% of cyberattacks

begin with the exploitation of known vulnerabilities.[1]

Nearly 50,000 new CVEs

were registered in 2025.[2]

~40–55 days

The average time to remediate critical vulnerabilities, leaving infrastructure exposed to potential attacks.[3]

Finding vulnerabilities is only the first step. The real challenge is understanding which vulnerabilities create actual risk, where they are located, and whether they have been remediated before attackers can exploit them.

See assets. Prioritize risks. Remediate vulnerabilities.

1

Eliminate blind spots across your infrastructure

You can't protect what you can't see. Kaspersky Vulnerability Management helps discover devices, operating systems and installed software across the infrastructure, enabling security and IT teams to work with an up-to-date asset view instead of outdated spreadsheets and incomplete inventories.

The solution supports agent-based and network-based inventory, helping identify managed assets as well as devices without an installed agent.

2

Extend coverage without adding complexity

Regular scanning helps detect vulnerabilities across workstations, servers and network devices. The agent-based approach uses existing Kaspersky Endpoint Security components, while agentless network scanning checks ports and services on assets without an installed agent.

This expands infrastructure coverage and reduces the risk of critical vulnerabilities remaining beyond the organization's visibility.

[1] Anatomy of a Cyber World: Global Report by Kaspersky Security Services 2026
[2] https://www.cve.org/About/Metrics
[3] Edgescan Vulnerability Statistics Report 2026

3

Stop misconfigurations from becoming entry points

Misconfigurations can create risks as serious as unpatched CVEs. Kaspersky Vulnerability Management helps assess configuration settings against security requirements, regulatory practices and internal policies.

Support for predefined profiles based on security best practices and regulatory requirements simplifies compliance control and audit preparation.

4

Remediate vulnerabilities, not just report them

A scanner shows the problem. The business needs the result: reduced risk. Kaspersky Vulnerability Management helps integrate patch management into a unified vulnerability management process and use integration with Kaspersky Security Center Linux to manage Windows updates.

This helps close the gap between vulnerability detection and actual remediation.

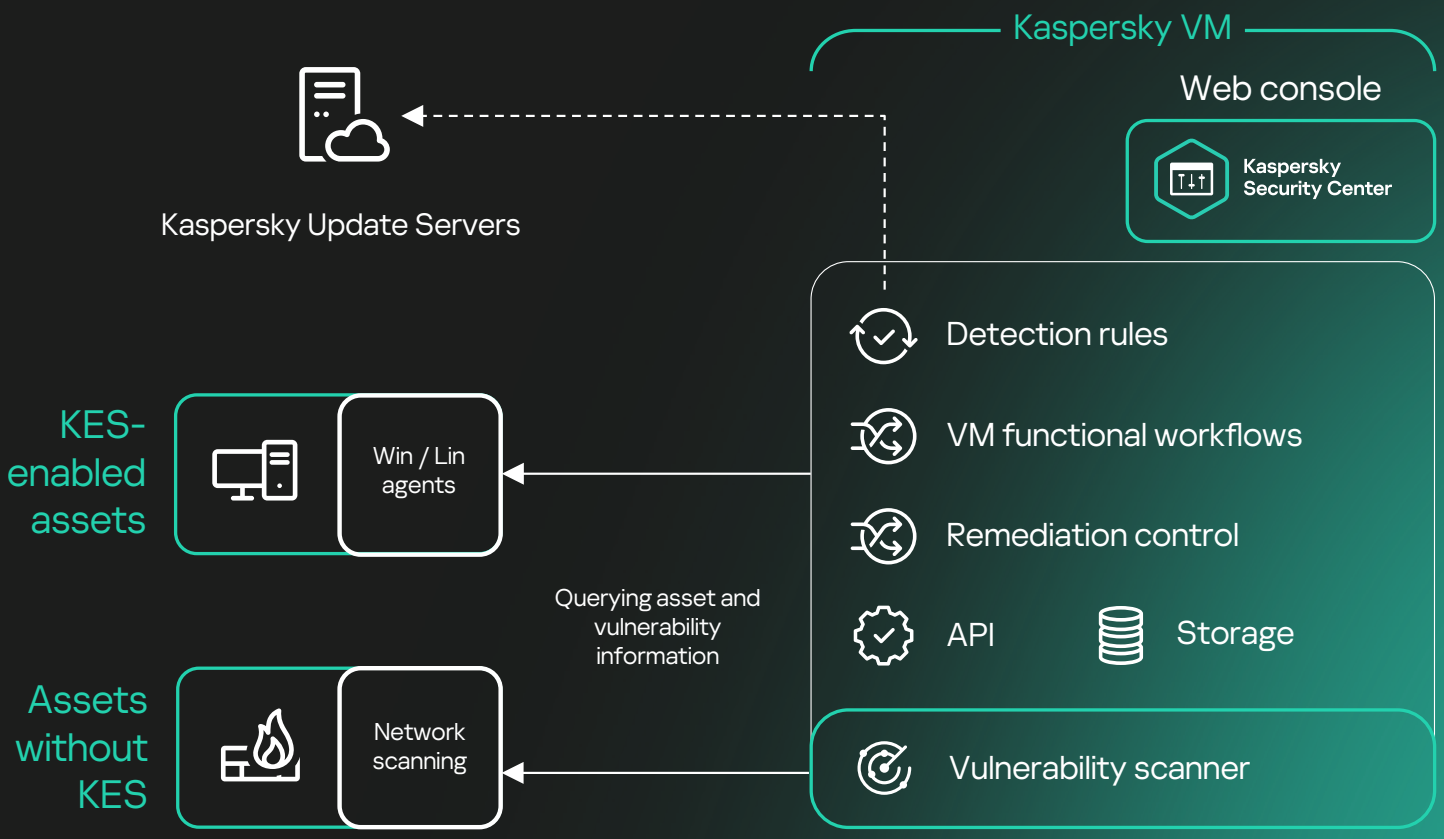
5

Confirm that risk has been closed

After remediation, teams must verify the outcome. The solution helps track the status of vulnerability remediation: which risks have already been addressed, which remain open, and where security or IT teams need to take further action.

This turns vulnerability management from a one-time check into a managed cycle: discover, prioritize, remediate, verify.

Built for connected vulnerability management operations



Business benefits

Visibility and control over assets and vulnerabilities

The solution helps maintain an up-to-date view of the infrastructure, installed software, and related vulnerabilities.

Faster response cycles and reduced mean time to remediate vulnerabilities

The combination of scanning, patch management and remediation control helps teams move faster from vulnerability detection to closure.

Lower risk of regulatory and industry compliance gaps

Configuration assessment, reporting and remediation monitoring demonstrate measurable risk reduction and support internal and external audits.

Improved security team efficiency

Centralized management and reporting reduce manual work and help security and IT teams focus on other important risks.

Native integration with Kaspersky products

Kaspersky Vulnerability Management is being developed as part of Kaspersky's unified security ecosystem, enabling vulnerability data to be used in the broader cyber risk management context.

Take control of vulnerabilities

Discover how Kaspersky Vulnerability Management helps reduce cyber risk across your infrastructure.

Kaspersky Vulnerability Management

Learn more

www.kaspersky.com

#kaspersky
#truetobusiness