

Kaspersky continues to protect outdated versions of Windows

How to protect workstations with outdated operating systems

kaspersky cybersecurity true to business

kaspersky.com

Kaspersky continues to protect outdated versions of Windows

Microsoft stopped supporting the Windows XP operating system several years ago, meaning users of this OS no longer receive updates or security patches from the manufacturer. Furthermore, the entire system code for Windows XP was leaked, allowing anyone to find new ways to hack your devices. This makes the popular operating system extremely vulnerable. The problem is compounded by the fact that most enterprise-grade security solutions no longer support Windows XP, nor Windows 7.

After October 14, 2025, Windows 10 will also no longer be supported by Microsoft.

Microsoft ended support for Windows XP on April 8, 2014, after 12 years. Support for Windows 7 ended in January 2023, including paid extended security updates. Windows 10 support ended in October 2025. Security updates and technical support are no longer available for these legacy operating systems, so users must upgrade to a more modern version.

According to Microsoft, the recommended way to upgrade is by purchasing a new device with the latest version installed.

As of November 2023, more than 1.6 billion computers worldwide run Windows OS.

According to StatCounter, Windows holds around 77% of the global desktop market, and Windows XP still accounts for approximately 0.05% of that share. This puts the number of observable Windows XP computers worldwide at roughly 800,000. The actual figure could well exceed one million, as these unsupported systems are likely to be less connected and less visible to usage tracking than they once were.

Why Kaspersky Security for Business no longer supports Windows XP

Until 2020, our comprehensive endpoint security solution, Kaspersky Security for Business, supported the Windows XP operating system – even after most security vendors had stopped doing so. But over time, this became impossible.

The reality is that, unlike older versions of Windows, the threat landscape continues to evolve. We strive to offer our customers cutting-edge protection technologies against increasingly diverse and complex threats (for example, Adaptive Anomaly Control), but regardless of how advanced and effective these technologies are, they simply won't function properly on Windows XP.

Is there a choice?

The days of systems still running unsupported Windows versions are numbered. The quality and capabilities of alternative security solutions that continue to work with them are extremely limited. Most are aimed at home devices, and none offer the level of security required for an OS that the vendor no longer supports. Furthermore, these solutions themselves may soon cease to be supported as the market for security products supporting legacy Windows operating systems is rapidly shrinking.

Update your operating system

The signs are clear: it's time for your company to invest in modern hardware and software instead of continuing to struggle with the ever-increasing risks and inefficiencies of outdated and unsupported systems. Now is the time to develop a long-term upgrade plan.

As long as you continue to use an outdated operating system, you're at risk: on the one hand, Microsoft no longer provides support and updates, and on the other, you can't use the latest versions of security products like Kaspersky Security for Business or Kaspersky Symphony.

How to stay protected

Migrating to a new operating system takes time, and no business can afford to be unprotected during this transition.

Fortunately, we have another endpoint security solution that supports legacy versions of Windows and will continue to support them for the foreseeable future.

Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security provides complete protection and support until you're ready to migrate to more recent Windows operating systems that don't conflict with the latest security technologies in Kaspersky Security for Business.

Kaspersky Embedded Systems Security is a robust, multi-layered security system based on a proven anti-malware engine, and offers all the benefits of centralized management via the familiar Kaspersky Security Center console. The lightweight solution is specifically designed for Windows operating systems starting from Windows XP SP2.

It offers stable, straightforward protection for companies that need time to transition from legacy Windows versions or are unable to migrate to another operating system. The product is suitable for downtime-sensitive manufacturing, automated systems, low-power but critical machine operations, and any environment requiring reliable, multi-layered protection regardless of operating system limitations.

Functional comparison

The table below lists the features included in Kaspersky Embedded Systems Security and Kaspersky Endpoint Security for Windows. This information will help you understand what you'll gain by upgrading to Kaspersky Embedded Systems Security, and what will change. Kaspersky Embedded Systems Security includes the core security features you're accustomed to in Kaspersky Security for Business, all managed from a single console.

Function	Kaspersky Embedded Systems Security for Windows 4.1	Kaspersky Endpoint Security for Windows 14.x (for workstations)	What you gain
Compatibility and support			
Support for older operating systems, starting from Windows XP	+	-	Secure use of workstations with outdated systems that are difficult or impossible to upgrade.
Support for legacy hardware/ weak system characteristics	+	-	Security even for low-power systems.
Protection from threats			
File threat protection	+	+	Protection from file-based threats such as malware or misused legit dual-purpose tools.
Email threat protection	-	+	Protection from email attacks.
Web threat protection	-	+	Protection from web threats.
Network threat protection	+	+	Protection from network attacks.
Precise detection of threats using signature-based methods (execution prevention)	+	+	Accurate detection of malware without false positives (the core function of any endpoint security platform).
Heuristic analysis and AI models running locally and in the cloud	+	+	Detection of new and unknown threats through comprehensive analysis of indirect and static indicators.
Local sandboxing via emulation	+	+	Detection of sophisticated stealth/ encrypted malware by pseudo-executing in a safe simulated environment.

Function	Kaspersky Embedded Systems Security for Windows 4.1	Kaspersky Endpoint Security for Windows 14.x (for workstations)	What you gain
Behavioral analysis	+	+	Detection of unknown advanced threats using behavioral analysis.
Exploit protection	+	+	Prevention of exploitation of vulnerabilities in critical applications.
Firewall	+	+	Limits unnecessary, unverified, and dangerous connections between the system and external nodes.
Integration with Advanced Detection and Response (Kaspersky EDR, Kaspersky MDR)	MDR	EDR, MDR	Additional capabilities for detecting complex threats and broad automated infrastructure response capabilities.
Integration with KSN/KPSN	+	+	Updated threat data directly from the Kaspersky cloud infrastructure.
Firmware scanner	+	+	Targeted firmware scans designed to detect specific malware hidden, for example, on a UEFI flash drive.
Encryption protection for network folders	+	+	Protection against ransomware.
BadUSB protection	+	+	Protects the host from malicious USB devices masquerading as HIDs (keyboards, mice, etc.)
Strengthening the system (reducing the attack surface)			
Compact security configuration based on "Default Deny"	+	-	Compact, low-system-intensive configuration: the default "Deny" policy is used as the basis, and more resource-intensive protection levels are disabled.
Self-defense	+	+	Protection against reduced security levels as a result of disruption of solution components.
Protection against unauthorized configuration changes	+	+	Protection against security degradation due to unauthorized changes to solution settings.
Program control	+	+	Protection against the use of untrusted external devices, reducing the risk of infection and data leakage.
Device control	+	+	The ability to control the use of individual web resources and their categories, reducing the likelihood of infection, missing phishing attacks and, consequently, the loss of information and credentials.
Web control	-	+	Analysis of program usage scenarios and detection of suspicious activity to detect advanced threats.
Adaptive anomaly control	-	+	Controls program launches and blocks unauthorized launches, including file-based malware.
Intrusion Prevention System	-	+	Protection against attacks based on a specific number of permitted actions for insufficiently trusted applications.
Vulnerability and Patch Management	+ (Compliance Edition)	+ (starting with Kaspersky Next EDR Optimum)	Monitoring of vulnerabilities in systems installed on workstations and fixing them through timely automatic updates.
Centralized encryption management	+	+	Manage full-disk encryption via Windows' built-in BitLocker utility through Kaspersky Security Center, alongside other Kaspersky security controls.'

Function	Kaspersky Embedded Systems Security for Windows 4.1	Kaspersky Endpoint Security for Windows 14.x (for workstations)	What you gain
System integrity monitoring			
File integrity monitoring	+ (Compliance Edition)	+ (Only in Kaspersky Hybrid Cloud Security Enterprise Server/CPU)	Detection of unauthorized system changes (including those made when the power is off), meaning detection of any interference.
Log analysis	+ (Compliance Edition)	+ (Only in Kaspersky Hybrid Cloud Security Enterprise Server/CPU)	Detection of prohibited activity in the system by monitoring changes in system logs.
Monitoring registry access	+ (Compliance Edition)	+ (Only in Kaspersky Hybrid Cloud Security Enterprise Server/CPU)	Monitoring and blocking of attempts to make unauthorized changes to the system registry.
Monitoring and management			
Centralized local management via Kaspersky Security Center	+	+	A unified security ecosystem that allows centralized management of Kaspersky products.
Managing application configuration via the local console on the device	+	+	The ability to configure the solution in the absence of communication with the control server.
Kaspersky Security Center Cloud Console	+	+	Easy deployment and resource savings: no need to install and maintain a separate management server.
Command line control	+	+	Ease of administration and simple workflows that don't require a graphical interface.
Integration with SIEM systems	+	+	The solution complements the security picture with event data at workstation level.

Industrial Use

If your industrial control system or SCADA system runs on Windows XP, we recommend Kaspersky Industrial CyberSecurity for Nodes, a specialized solution for protecting ICS. It provides continuous support for legacy operating systems over the long term while maintaining compatibility with your industrial systems.

Don't delay

Upgrade your operating system as soon as possible. If your company wants to continue operating efficiently and securely from an IT perspective, you need to start planning your transition now.. While you're making and implementing decisions, Kaspersky Embedded Systems Security will protect your legacy workstations.

Learn how to protect your existing infrastructure running legacy Windows operating systems with Kaspersky Embedded Systems Security by following this link.

www.kaspersky.com

© 2026 AO Kaspersky Lab.
Registered trademarks and service marks
are the property of their respective owners.