Continuing to secure your old versions of Windows with Kaspersky

How to protect your legacy endpoints

kaspersky bring on the future

kaspersky.com

Continuing to secure your old versions of Windows with Kaspersky

Windows XP is no longer supported by Microsoft, so users will no longer receive the manufacturer's security updates and patches. Add to this the fact that the full XP source code has recently been leaked to the general public, making it available to any hacker looking for a new way into your system, and this respected OS has become a serious security liability. The problem has become even more acute as the vast majority of cybersecurity vendors have discontinued their support for Windows XP in their corporate products. Windows 7 is also no longer supported.

After 12 years, all support for Windows XP ended on April 8, 2014. Windows 7 was left without ANY support (including paid Extended Security Updates) in January 2023. Microsoft will no longer provide security updates or technical support for the Windows XP and 7 operating systems. It's critical to migrate now to a modern OS.

According to Microsoft, the best way to migrate from Windows XP to the newest Windows version is buy a new device.

How many PCs are still running XP?

As of November 2023:

According to recent calculations there are more than 1,6 billion PCs running Windows worldwide.

According to StatCounter - Windows claims around 70% of the Windows market, while Windows XP still holds 0.33%. This means the number of XP-based PCs still out there is ~4,8 million.

Kaspersky Endpoint Security for Business and old versions of Windows – time to call it a day

Until 2020 we continued to support XP in our flagship Kaspersky Endpoint Security for Business products, long after many security vendors ceased doing so. But that's no longer possible.

Unlike XP itself, the threat landscape keeps on evolving, and we're committed to delivering ever more advanced and powerful technologies to protect all our customers against increasingly diverse and sophisticated attack scenarios. No matter how lean and mean we make the new technologies (like our firmware scanner and Adaptive Anomaly Control, for example) that we incorporate into Kaspersky Endpoint Security for Business, XP simply can't accommodate them.

What's the alternative?

XP's days are numbered – we all know that. Alternative security options that still support XP now extremely are limited in terms of quality and capabilities – most are consumer orientated, and none can deliver the levels of protection that an unsupported operating system, in particular, desperately needs. Plus, these products are themselves unlikely to remain supported for long – the security market for systems running old Windows OS is fading fast.

Upgrade your systems

This could be the wake-up call your organization needs to start investing in up-to-date hardware and software, rather than continuing to cope with the ever-increasing risks and inefficiencies endemic to running an unsupported system. Now's the time to make serious plans about where you go next, and how and when to upgrade.

While you continue to run an obsolete OS, your protection is compromised. You no longer have the lifeline of support and updates from Microsoft, and your current OS is preventing you from benefiting from all the latest developments in products like Version 12 of Kaspersky Endpoint Security for Business.

But what about right now?

Moving to a new operating system takes time, and we don't want to leave you unprotected in the interim.

Fortunately, we have another endpoint security product which supports old Windows OSs, and will continue to do so for the foreseeable future.

Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security will fully protect and support you until you're ready to upgrade to a Windows OS capable of accommodating the latest anti-threat technologies offered in Kaspersky Endpoint Security for Business Version 12.

Kaspersky Embedded Systems Security offers all the reliable protection of a multi-layered security solution based on our award-winning anti-malware engine – plus the benefits of centralized management via the familiar Kaspersky Security Center. And, being specifically designed to support a broad range of Windows operating systems, starting from Windows XP SP2, it makes low demands on hardware resources.

The solution delivers rugged, straightforward security for those organizations where moving away from XP may take time, or just isn't an option. It's used in downtime-sensitive environments, in automated systems, in cases where machine operations are low-powered but vitally important, and wherever rugged multi-layered security is essential, regardless of OS limitations.

Features comparison

The table below shows what's included in Kaspersky Embedded Systems Security, in your current version of Kaspersky Endpoint Security for Business (Version 10), and in the latest Version 12. So you can see exactly what moving to Kaspersky Embedded Systems Security would mean for you, and how little would actually change. Kaspersky Embedded Systems Security provides the crucial security layers you're already used to in Kaspersky Endpoint Security for Business, managed from our familiar central console.

Feature	KESS for Windows 3.3	KES for Windows 12.x (workstation)	Benefits
Compatibility & Support			
Support for old OSs, starting from Windows XP	+	-	Allows the secure use of older endpoints where upgrade is problematic or impossible.
Legacy hardware/low system specs support	+	-	Allows the provision of security even for underpowered systems.
Threat Protection			
File threat protection	+	+	Protects the system against file-based malware.
Mail threat protection	-	+	Protects the system against email-borne malware.
Web threat protection	+/- (malware & exploits only)	+	Protects the system against web-based threats.
Network threat protection	+	+	Protects the system against network-based attacks.
Precise, signature-based threat detection (pre-execution)	+	+	A core capability of any EPP solution, allowing the precise detection of malware specimens - without false positives.
Heuristics and on-premises machine-learning models (pre- and peri-execution)	+	+	Allows the detection of as-yet-unknown threats via the complex analysis of indirect static indicators.
Emulative sandboxing	+	+	Enables the detection of complex, heavily obfuscated/encrypted malware via pseudo-execution in a safe simulated environment.

Feature	KESS for Windows 3.3	KES for Windows 12.x (workstation)	Benefits
Behavior detection	-	+	Offers the behavior-based detection of sophisticated, as-yet-unknown malware.
Exploit prevention	+	+	Protects against the exploitation of vulnerabilities in important applications.
Firewall	+ (Windows firewall management)	+	Restricts unnecessary, untrusted and dangerous network connections between the system and external peers.
Integration with advanced detection and response (EDR, advanced sandbox, etc.)	-	+	Offers extra capabilities for the detection of sophisticated threats and the means for an infrastructure-wide automated response.
Integration with KSN/KPSN	+	+	Provides the most recent threat data instantly, directly from Kaspersky's cloud threat-processing infrastructure.
Firmware scanner	-	+	Conducts dedicated checks on the system's firmware, to detect specialized malware hidden in, for example, UEFI flash memory.
Anti-Cryptor for network shares	-	+	Prevents remotely initiated mal-intentioned encryption.
System Hardening (attack surface reduction)			
Lean protective configuration based on Default Deny	+	-	Enables a very lean configuration for low-spec systems – using only system hardening controls in a tight Default Deny mode and disabling more resource-hungry security layers.
Self defense	+	+	Guards against protection being compromised through interference with application components.
Unsanctioned configurations change protection	+	-	Guards against protection being compromised through interference with application configuration.
Application control	+	+	Regulates the launching of applications, and blocks unsolicited launches, including those of file-based malware.
Device control	+	+	Prevents the use of unsolicited external devices, reducing risk of infection and data leaks.
Web control	-	+	Regulates the use of web resources and their categories, helping to reduce the probability of infection, successful phishing attacks and the resultant loss of data and credentials.
Adaptive Anomaly Control	-	+	Analyzes apps' usage scenarios and detects abnormal behavior, helping to discover sophisticated infections.
HIPS (host-based intrusion prevention)	-	+	Prevents specific attack scenarios though reducing the scope of permitted activitiesin apps lacking a sufficient trust level.
Vulnerability and patch management	+ (additional license)	+ (Advanced and Total or additional license)	Allows keeping track of the presence of vulnerabilities in corporate endpoint systems and helps close them through timely, automated updates.

Feature	KESS for Windows 3.3	KES for Windows 12.x (workstation)	Benefits
System integrity control			
File Integrity Monitor	+ (compliance edition)	-	Detects unsolicited system changes, including those conducted during a power-off, thus helping to discover any intrusion.
Log inspection	+ (compliance edition)	-	Enables the detection of illicit activities in a system, by monitoring changes in system logs.
Registry Access Monitor	+ (compliance edition)	-	Monitors attempts of unauthorized meddling with System Registry and blocks them to prevent malicious effects
Monitoring & Management			
Centralized on-premises management (using Kaspersky Security Center)	+	+	Enables the centralized management of multiple Kaspersky products, offering a unified security ecosystem.
KSC web-based console	+	+	Offers simplified management and systems deployment and promotes resource economy, through no agent being installed to access the management system.
Kaspersky Security Center cloud console	+	+	Offers simplified deployment and resource economy, as no need to install and maintain a dedicated management server.
Command-line management	+	+	Offers additional convenience for administrators and enables lean, GUI-less scenarios.
SIEM integration	+	+	Enriches your unified security picture with endpoint-level events.

Industrial environments

If you're currently running XP in an industrial process control/SCADA environment, we strongly recommended considering Kaspersky Industrial CyberSecurity for Nodes for protection. This solution also offers ongoing long-term legacy OS support – and at the same time is designed to be SCADA-compatible, which brings significant benefits.

Upgrade now!

Upgrade your XP OS as soon as you can. Start planning right now, and explain to the Board that moving to an up-to-date system running a fully supported OS is an absolute fiscal priority if you're to ensure business continuity, efficiency and security from an IT perspective. And, while they're deciding, Kaspersky Embedded Systems Security will keep your old endpoints safe.

To find out how to secure your XP infrastructure with Kaspersky Embedded Systems Security, please get in touch.

Cyber Threats News: securelist.com
Threat Intelligence Portal: opentip.kaspersky.com
IT Security for Enterprise: www.kaspersky.com/enterprise
Kaspersky TechnoWiki: www.kaspersky.com/technowiki

www.kaspersky.com