



A Kaspersky continua protegendo versões desatualizadas do Windows

Como proteger estações de trabalho com sistemas operacionais desatualizados

kaspersky bring on
the future

kaspersky.com.br

A Kaspersky continua protegendo versões desatualizadas do Windows

A Microsoft deixou de oferecer suporte ao sistema operacional Windows XP há vários anos, o que significa que os usuários desse sistema operacional não recebem mais atualizações ou patches de segurança do fabricante. Além disso, todo o código-fonte do Windows XP foi vazado, permitindo que qualquer pessoa encontre novas maneiras de invadir seus dispositivos. Isso torna o popular sistema operacional extremamente vulnerável. O problema é agravado pelo fato de que a maioria das soluções de segurança de nível empresarial não oferece mais suporte ao Windows XP nem ao Windows 7.

Após 14 de outubro de 2025, o Windows 10 também deixará de ter suporte da Microsoft.

A Microsoft encerrou o suporte para o Windows XP em 8 de abril de 2014, após 12 anos. O suporte para o Windows 7 terminou em janeiro de 2023, incluindo as atualizações de segurança estendidas pagas. O suporte para o Windows 10 terminou em outubro de 2025. As atualizações de segurança e o suporte técnico não estão mais disponíveis para esses sistemas operacionais antigos, portanto, os usuários devem atualizar para uma versão mais moderna.

Segundo a Microsoft, a forma recomendada de fazer a atualização é adquirindo um novo dispositivo com a versão mais recente instalada.

Em novembro de 2023, mais de **1,6 bilhão** de computadores em todo o mundo executavam o sistema operacional Windows. Segundo a **StatCounter**, o Windows detém cerca de 70% do mercado global de computadores desktop, e o Windows XP ainda representa cerca de 0,38% desse número. Isso significa que aproximadamente 6 milhões de computadores em todo o mundo ainda estão executando o Windows XP.

Por que o Kaspersky Security for Business não é mais compatível com o Windows XP?

Até 2020, nossa solução abrangente de segurança de endpoints, Kaspersky Security for Business, era compatível com o sistema operacional Windows XP, mesmo depois que a maioria dos fornecedores de segurança deixou de oferecê-la. Mas, com o tempo, isso se tornou impossível.

A realidade é que, ao contrário das versões mais antigas do Windows, o cenário de ameaças continua evoluindo. Nos esforçamos para oferecer aos nossos clientes tecnologias de proteção de ponta contra ameaças cada vez mais diversas e complexas (por exemplo, Controle Adaptativo de Anomalias), mas, independentemente do quão avançadas e eficazes essas tecnologias sejam, elas simplesmente não funcionarão corretamente no Windows XP.

Existe alguma opção?

Os dias em que os sistemas ainda executam versões do Windows sem suporte estão contados. A qualidade e as capacidades das soluções de segurança alternativas que continuam funcionando com eles são extremamente limitadas. A maioria é voltada para dispositivos domésticos, e nenhuma oferece o nível de segurança necessário para um sistema operacional que o fornecedor não oferece mais suporte. Além disso, essas soluções podem em breve deixar de ser suportadas, visto que o mercado de produtos de segurança compatíveis com sistemas operacionais Windows antigos está encolhendo rapidamente.

Atualize seu sistema operacional

Os sinais são claros: chegou a hora de sua empresa investir em hardware e software modernos, em vez de continuar lutando contra os riscos e ineficiências cada vez maiores de sistemas desatualizados e sem suporte. Agora é o momento de desenvolver um plano de upgrade a longo prazo.

Enquanto você continuar usando um sistema operacional desatualizado, estará em risco: por um lado, a Microsoft não oferece mais suporte e atualizações e, por outro, você não poderá usar as versões mais recentes de produtos de segurança como o Kaspersky Security for Business ou o Kaspersky Symphony.

Como manter sua segurança?

A migração para um novo sistema operacional leva tempo, e nenhuma empresa pode se dar ao luxo de ficar desprotegida durante essa transição.

Felizmente, temos outra solução de segurança de endpoints que oferece suporte a versões antigas do Windows e continuará oferecendo suporte a elas num futuro próximo.

Kaspersky Embedded Systems Security

O Kaspersky Embedded Systems Security oferece proteção e suporte completos até que você esteja pronto para migrar para sistemas operacionais Windows mais recentes que não entrem em conflito com as tecnologias de segurança mais recentes do Kaspersky Security for Business.

O Kaspersky Embedded Systems Security é um sistema de segurança robusto e multicamadas baseado em um mecanismo antimalware comprovado, que oferece todos os benefícios do gerenciamento centralizado por meio do console familiar do Kaspersky Security Center. A solução leve foi projetada especificamente para sistemas operacionais Windows a partir do Windows XP SP2.

Ela oferece proteção estável e descomplicada para empresas que precisam de tempo para fazer a transição de versões antigas do Windows ou que não conseguem migrar para outro sistema operacional. O produto é adequado para processos de fabricação sensíveis ao tempo de inatividade, sistemas automatizados, operações de máquinas críticas de baixa potência e qualquer ambiente que exija proteção confiável e multicamadas, independentemente das limitações do sistema operacional.

Comparação funcional

A tabela abaixo lista os recursos incluídos no Kaspersky Embedded Systems Security e no Kaspersky Endpoint Security for Windows. Essas informações ajudarão você a entender o que você ganha ao atualizar para o Kaspersky Embedded Systems Security e o que muda. O Kaspersky Embedded Systems Security inclui os principais recursos de segurança que você já conhece do Kaspersky Security for Business, todos gerenciados a partir de um único console.

Função	Kaspersky Embedded Systems Security for Windows 4.0	Kaspersky Endpoint Security for Windows 12.x (para estações de trabalho)	O que você recebe
Compatibilidade e suporte			
Suporte para sistemas operacionais mais antigos, a partir do Windows XP	+	-	Uso seguro de estações de trabalho com sistemas obsoletos e de difícil ou impossível atualização.
Suporte para hardware legado e características de sistema fracas	+	-	Segurança mesmo para sistemas de baixa potência.
Proteção contra ameaças			
Proteção contra ameaças de arquivos	+	+	Proteção contra ameaças baseadas em arquivos, como malware ou uso indevido de ferramentas legítimas de dupla finalidade.
Proteção contra ameaças de e-mail	-	+	Proteção contra ataques de e-mail.
Proteção contra ameaças da Web	-	+	Proteção contra ameaças da web.
Proteção contra ameaças de rede	+	+	Proteção contra ataques de rede.
Detecção precisa de ameaças usando métodos baseados em assinaturas (prevenção de execução)	+	+	Detecção precisa de malware sem falsos positivos (a função principal de qualquer plataforma de segurança de endpoints).
Análise heurística e modelos de aprendizado de máquina do lado do cliente (antes e durante a execução do malware)	+	+	Detecção de ameaças novas e desconhecidas por meio de análise abrangente de indicadores estatísticos indiretos.

Função	Kaspersky Embedded Systems Security for Windows 4.0	Kaspersky Endpoint Security for Windows 12.x (para estações de trabalho)	O que você recebe
Sandbox local via emulação	+	+	Deteção de malware sofisticado, oculto/criptografado, por meio de pseudo-execução em um ambiente simulado seguro.
Análise de comportamento	+	+	Deteção de ameaças avançadas desconhecidas por meio de análise comportamental.
Proteção contra exploits	+	+	Prevenção de exploits de vulnerabilidades em aplicativos críticos.
Firewall	+	+	Limita conexões desnecessárias, não verificadas e perigosas entre o sistema e nós externos.
Integração com sistemas Detection and Response avançados (Kaspersky EDR, Kaspersky MDR)	MDR	EDR, MDR	Capacidades adicionais para deteção de ameaças complexas e amplas funcionalidades de resposta automatizada da infraestrutura.
Integração com KSN/KPSN	+	+	Dados de ameaças atualizados diretamente da infraestrutura de nuvem da Kaspersky.
Verificador de firmware	+	+	Análises de firmware direcionadas, projetadas para detectar malware específico oculto, por exemplo, em uma unidade flash UEFI.
Proteção de criptografia para pastas de rede	+	+	Proteção contra ransomware.
Fortalecimento do sistema (redução da superfície de ataque)			
Configuração de segurança compacta baseada em "Negação padrão"	+	-	Configuração compacta e com baixo consumo de recursos do sistema: a política "Negar" padrão é usada como base, e os níveis de proteção que consomem mais recursos são desativados.
Autodefesa	+	+	Proteção contra a redução dos níveis de segurança resultante da interrupção de componentes da solução.
Proteção contra alterações de configuração não autorizadas	+	+	Proteção contra a degradação da segurança devido a alterações não autorizadas nas configurações da solução.
Controle do programa	+	+	Proteção contra o uso de dispositivos externos não confiáveis, reduzindo o risco de infecção e vazamento de dados.
Controle de Dispositivos	+	+	A capacidade de controlar o uso de recursos web individuais e suas categorias, reduzindo a probabilidade de infecção, evitando ataques de phishing e, consequentemente, a perda de informações e credenciais.
Controle da Web	-	+	Análise de cenários de uso do programa e deteção de atividades suspeitas para identificar ameaças avançadas.
Controle adaptativo de anomalias	-	+	Controla a execução de programas e bloqueia execuções não autorizadas, incluindo malware baseado em arquivos.
Sistema de prevenção de intrusões	-	+	Proteção contra ataques baseados em um número específico de ações permitidas para aplicativos com confiabilidade insuficiente.
Vulnerabilidade e gerenciamento de correções	<div>+</div> <div>(Edição de Conformidade)</div>	<div>+</div> <div>(a partir do Kaspersky Next EDR Optimum)</div>	Monitoramento de vulnerabilidades em sistemas instalados em estações de trabalho e correção delas por meio de atualizações automáticas oportunas.

Função	Kaspersky Embedded Systems Security for Windows 4.0	Kaspersky Endpoint Security for Windows 12.x (para estações de trabalho)	O que você recebe
Monitor de integridade do sistema			
Monitoramento de integridade de arquivos	+	+	Detecção de alterações não autorizadas no sistema (incluindo aquelas feitas com a energia desligada), ou seja, detecção de qualquer interferência.
	(Edição de Conformidade)	(Apenas no servidor/CPU Kaspersky Hybrid Cloud Security Enterprise)	
Análise de registros	+	+	Detecção de atividades proibidas no sistema por meio do monitoramento de alterações nos registros do sistema.
	(Edição de Conformidade)	(Apenas no servidor/CPU Kaspersky Hybrid Cloud Security Enterprise)	
Acesso ao registro de monitoramento	+	+	Monitoramento e bloqueio de tentativas de realizar alterações não autorizadas no registro do sistema.
	(Edição de Conformidade)	(Apenas no servidor/CPU Kaspersky Hybrid Cloud Security Enterprise)	
Monitoramento e gerenciamento			
Gerenciamento local centralizado por meio do Kaspersky Security Center	+	+	Um ecossistema de segurança unificado que permite o gerenciamento centralizado dos produtos Kaspersky.
Gerenciamento da configuração do aplicativo por meio do console local no dispositivo	+	+	A capacidade de configurar a solução na ausência de comunicação com o servidor de controle.
Console do Kaspersky Security Center Cloud	+	+	Implementação simplificada e economia de recursos: não há necessidade de instalar e manter um servidor de gerenciamento separado.
Controle de linha de comando	+	+	Facilidade de administração e fluxos de trabalho simples que não exigem uma interface gráfica.
Integração com sistemas de SIEM	+	+	A solução complementa o panorama de segurança com dados de eventos ao nível da estação de trabalho.

Uso industrial

Se seu sistema de controle industrial ou sistema SCADA roda no Windows XP, recomendamos o [Kaspersky Industrial CyberSecurity for Nodes](#), uma solução especializada para proteger ICS. Ele oferece suporte contínuo a sistemas operacionais legados a longo prazo, mantendo a compatibilidade com seus sistemas industriais.

Não demore

Atualize seu sistema operacional o mais rápido possível. Se sua empresa deseja continuar operando de forma eficiente e segura do ponto de vista de TI, você precisa começar a planejar sua transição agora mesmo. Enquanto você toma e implementa decisões, o Kaspersky Embedded Systems Security protege suas estações de trabalho legadas.

Saiba como proteger sua infraestrutura existente que executa sistemas operacionais Windows legados com o Kaspersky Embedded Systems Security clicando neste [link](#).