卡巴斯基为已过时的 Windows 版本继续提供防护

如何保护搭载过时操作系统的工作站

kaspersky 引领未来

kaspersky.com.cn

卡巴斯基为已过时的 Windows 版本继续提供防护

微软已于数年前停止对 Windows XP 操作系统的支持服务，自此，该系统用户无法再获得厂商推送的更新及安全补丁。不仅如此，Windows XP 的完整系统代码已遭泄露，这导致任何人都有可能探寻到入侵您设备的新方式，令这款曾广泛普及的操作系统极易遭受攻击。更为严峻的是，多数企业级安全解决方案已不再兼容 Windows XP，同样情况的还有 Windows 7。

而 2025 年 10 月 14 日后，微软也停止对 Windows 10 的支持。

微软于 2014 年 4 月 8 日停止了对已沿用 12 年的 Windows XP 的支持服务；2023 年 1 月，又终止了对 Windows 7 的支持，付费扩展安全更新服务也一并停止；对 Windows 10 的支持于 2025 年 10 月结束。这些过时操作系统将无法获取安全更新及技术支持，用户必须升级至更新版本。

微软建议，购买预装最新操作系统版本的新设备是升级的最佳途径。

截至 2023 年 11 月，全球范围内，运行 Windows 操作系统的计算机数量超 16 亿台据 StatCounter 数据显示，Windows 在全球台式机操作系统市场中占比约 70%，其中 Windows XP 仍占约 0.38%。这意味着全球约有 600 万台计算机仍在使用 Windows XP。

为何卡巴斯基安全解决方案 for Business 不再支持 Windows XP

直至 2020 年，我们的综合端点安全解决方案卡巴斯基安全解决方案 for Business 仍继续为 Windows XP 提供支持，彼时多数安全厂商已停止对该系统的支持服务。但随着时间的推移，这一支持已难以为继。

现实表明，过时的 Windows 版本已无法跟上威胁态势的持续演变。我们始终致力于为客户提供前沿的保护技术，以应对日益复杂多元的威胁（如自适应异常控制技术），但无论技术多么先进高效，在 Windows XP 系统上都无法有效运行。

还有其他选择吗？

使用已不再受支持的 Windows 系统的时间已经所剩无几。目前仍能适配这类系统的替代安全解决方案，其质量和功能都极为有限。多数方案仅适用于家用设备，且没有任何一款能为其所适配的、厂商已停止支持的操作系统提供足够的安全防护水准。此外，这些解决方案自身也极有可能很快停止服务，毕竟，支持过时 Windows 操作系统的安全产品市场正急剧萎缩。

更新您的操作系统

信号已然明确：贵公司亟需投资现代化硬件与软件，避免持续承受不受支持过时系统带来的风险递增与效率损耗。当下正是制定长期升级规划的关键时刻。

如果您继续使用过时操作系统，将始终面临着风险：一方面，微软不再提供支持与更新；另一方面，您无法使用最新版本的安全产品，如卡巴斯基安全解决方案 for Business 或卡巴斯基 Symphony。

如何持续获得防护？

迁移至新操作系统需要耗费一定时间，任何企业都无法承受过渡阶段出现的安全防护断层。

幸运的是，我们还有另一款端点安全解决方案，能够为过时的 Windows 版本提供支持，并将在可预见的未来持续保障其安全。

卡巴斯基嵌入式系统安全解决方案

卡巴斯基嵌入式系统安全解决方案可提供多方面防护与支持，直至您完成向更新版 Windows 操作系统的迁移（此系统可无缝兼容卡巴斯基安全解决方案 for Business 的最新安全技术）。

卡巴斯基嵌入式系统安全解决方案是一款高效能多层级安全系统，基于成熟的反恶意软件引擎构建，支持通过您熟悉的卡巴斯基安全中心控制台实现集中管理。这款轻量级解决方案专为 Windows XP SP2 及更高版本的 Windows 操作系统设计，

能够为需要时间从过时 Windows 版本过渡，或因特殊原因无法迁移至其他操作系统的企业提供稳定有效的防护。该产品尤其适用于对停机高度敏感的生产制造、自动化系统、低功耗但非常关键的机器操作场景，以及任何不受操作系统限制，却仍需可靠的多层级防护环境。

功能比较

下表列出了卡巴斯基嵌入式系统安全解决方案与卡巴斯基端点安全 for Windows 的功能差异。 这些信息将有助于您了解升级至卡巴斯基嵌入式系统安全解决方案后可获得的能力，以及相应的变化。卡巴斯基嵌入式系统安全解决方案涵盖了用户在卡巴斯基安全解决方案 for Business 中所熟悉的核心安全功能，并可通过统一的管理控制台进行集中管理。

功能	卡巴斯基嵌入式系统安全解决方案 for Windows 4.0	卡巴斯基端点安全 for Windows 12.x（工作站）	优势
兼容性与支持			
支持旧版操作系统（Windows XP 起）	+	-	为难以升级的系统提供安全保障。
支持老旧硬件与低性能系统	+	-	即使在低算力环境中也可部署安全防护。
威胁防护能力			
文件威胁防护	+	+	防护基于文件的恶意代码及被滥用的合法工具。
邮件威胁防护	-	+	防御邮件攻击。
网页威胁防护	-	+	预防网页攻击。
网络威胁防护	+	+	防御网络攻击。
基于特征的精准检测（防止执行）	+	+	在降低误报的同时实现准确检测（所有端点安全平台的核心功能）。
启发式分析与客户端机器学习模型（恶意软件执行前后）	+	+	通过统计分析识别新型与未知威胁。
本地沙盒仿真	+	+	在安全环境中分析隐匿或加密恶意代码。
行为分析	+	+	通过行为分析检测未知的高级威胁。
漏洞利用防护	+	+	防止关键应用中的漏洞被利用。
防火墙	+	+	限制系统与外部节点之间不必要、未验证或存在风险的连接。
与高级检测和响应解决方案集成（卡巴斯基 EDR、卡巴斯基 MDR）	MDR	EDR、MDR	具备复杂威胁检测能力及自动化响应支持。
与 KSN/KPSN 集成	+	+	直接从卡巴斯基云基础设施获取威胁数据更新。
固件扫描程序	+	+	定向扫描固件，检测隐藏的特定恶意软件（如 UEFI 闪存中的恶意软件）。

功能	卡巴斯基嵌入式系统安全解决方案 for Windows 4.0	卡巴斯基端点安全 for Windows 12.x（工作站）	优势
系统加固（减少攻击面）			
网络文件夹加密保护	+	+	防御勒索软件。
基于“默认拒绝”原则的精简安全配置	+	-	配置精简、系统资源占用低：以默认“拒绝”策略为基础，禁用资源消耗较高的防护级别。
自我保护	+	+	防止因解决方案组件遭破坏而导致安全级别降低。
防止未经授权的配置更改	+	+	防止因未授权修改解决方案设置而导致防护能力下降。
程序控制	+	+	防止使用不受信任的外部设备，降低感染风险与数据泄露风险。
设备控制	+	+	控制单个网络资源及其类别的使用，降低感染、漏防网络钓鱼攻击的几率，进而减少信息与凭证丢失的风险。
网页控制	-	+	分析程序使用场景并检测可疑活动，以发现高级威胁。
自适应异常控制	-	+	控制程序的启动并阻止未经授权的启动操作，包括基于文件的恶意软件。
入侵防御系统	-	+	基于应用可信度限制其可执行操作。
漏洞和补丁管理	+（合规版）	+（自卡巴斯基新一代安全 EDR 优选版起）	监控安装在工作站上的系统的漏洞，并通过及时自动更新进行修复。
系统完整性监控			
文件完整性监控	+（合规版）	+（仅卡巴斯基混合云安全企业版服务器/CPU）	检测未经授权的系统更改（包括关机状态下的更改），即检测任何干扰行为。
日志分析	+（合规版）	+（仅卡巴斯基混合云安全企业版服务器/CPU）	通过监控系统日志变化，检测系统中的违规活动。
监控注册表访问	+（合规版）	+（仅卡巴斯基混合云安全企业版服务器/CPU）	监控并阻止未经授权尝试对系统注册表进行修改的操作。
监控和管理			
通过卡巴斯基全球中心实现本地集中管理	+	+	统一的安全生态系统，可集中管理卡巴斯基产品。
通过卡巴斯基全球中心实现本地集中管理	+	+	与控制服务器无通信连接时，仍可配置解决方案。
卡巴斯基安全中心云控制台	+	+	部署便捷、节省资源：无需安装和维护单独的管理服务器。
命令行控制	+	+	管理便捷、流程简单，无需使用图形界面。
与 SIEM 系统集成	+	+	该解决方案通过引入工作站层面的事件数据，补充和完善整体安全态势。

工业场景应用

如果您的工业控制系统或SCADA仍运行在WindowsXP上，我们建议您选择 **卡巴斯基工业网络节点安全**。该解决方案专为工业控制系统防护而设计，可在长期支持老旧操作系统的同时，保持与工业系统的兼容性与运行稳定性。

不要再拖延

请尽快升级您的操作系统。从 IT 安全角度来看，若企业希望持续保持高效、稳定且安全的运行状态，现在就需要开始规划系统升级与迁移方案。在规划和实施升级决策的过渡阶段，卡巴斯基嵌入式系统安全解决方案可为仍运行旧版 Windows 的工作站提供必要的安全防护。

如需了解如何使用卡巴斯基嵌入式系统安全解决方案保护基于旧版 Windows 操作系统的现有基础设施，请通过以下链接获取更多信息。

www.kaspersky.com.cn