卡巴斯基嵌入式系统安全解决方案

kaspersky

嵌入式安全面临的挑战

1 **软件陈旧易遭攻击**
鉴于嵌入式设备生命周期相对冗长，其极有可能运行已脱离支持范畴的操作系统与应用程序，其中包含未加修补的漏洞，随时都可能为攻击者提供可乘之机。

2 **安全更新机制无章法**
即便软件仍处于支持与保障周期内，补丁的部署也可能出现滞后。设备地理分布松散、更新过程需要设备离线（可能引发阶段性的服务中断），以及在部署前必须进行充分测试等因素，都会导致补丁安装被延迟。

3 **流程连续性制约**
部分类型设备（如医疗设备）的短暂停用，也可能引发重大问题，进一步延长补丁未能及时安装的周期。

4 **公共场所加剧风险**
大量嵌入式设备都在开放的公共环境中运行，显著提升了设备遭受篡改的可能性。网络级防御手段在面对直接物理攻击时，往往难以发挥有效作用。

5 **设备性质蕴含高风险**
由于嵌入式设备通常与财务运营直接相关，且涉及敏感个人信息的处理，因此对网络犯罪分子来说极其具有吸引力。

一体化安全防护，专为嵌入式系统打造（同时适用其他系统）

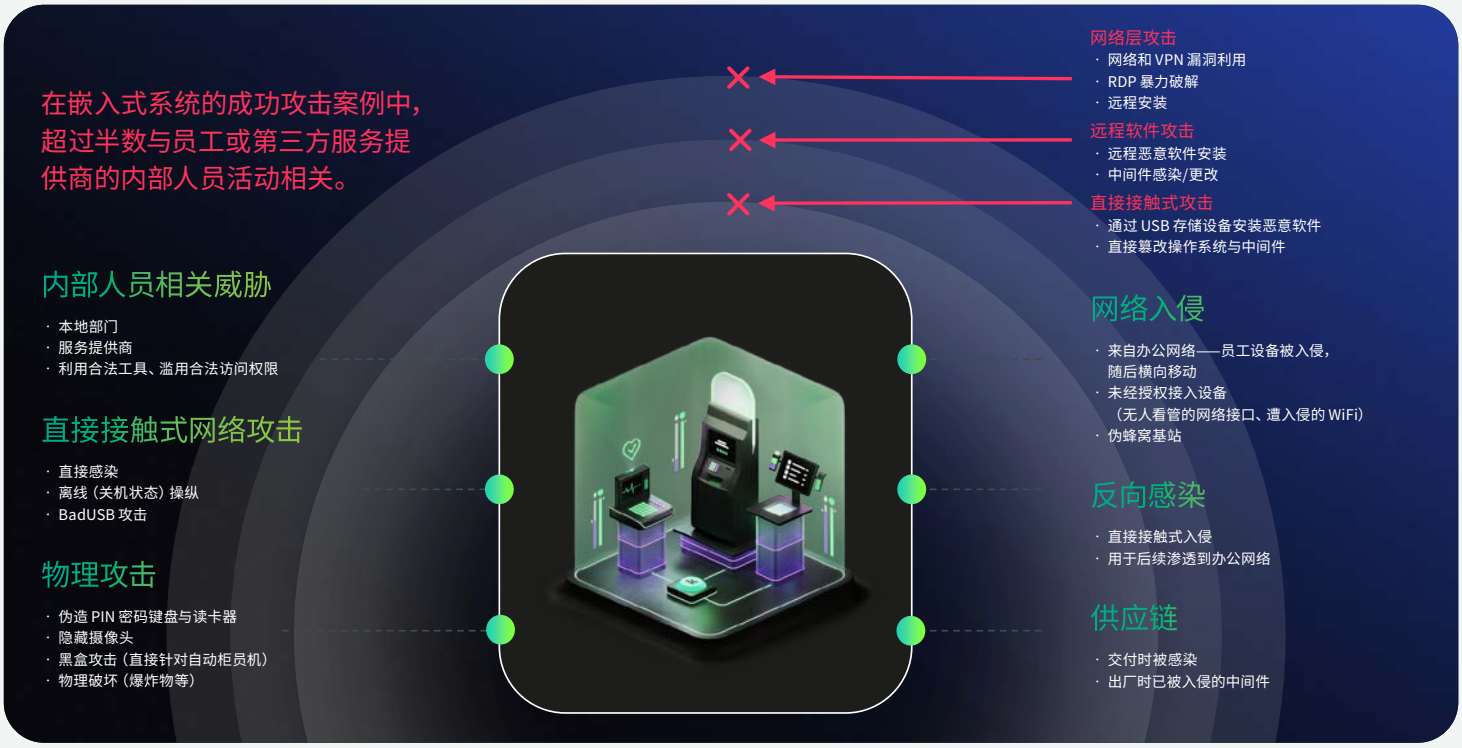
嵌入式系统已深度融入我们的生活场景，每天都与我们产生着密切交互。从 PoS 系统、ATM 机到医疗设备及自动加油站，嵌入式系统已成为其稳定运行的核心支撑，我们在诸多生活场景中皆对其产生深度依赖。随着嵌入式系统市场的持续拓展与深化，网络犯罪分子亦如影随形，他们不断精研策略、锤炼技术、优化程序，以精准适配这些广泛分布且细节繁杂的系统特性，伺机发动攻击。

当下面临的威胁形势

当下，新型犯罪商业模式如恶意软件即服务等不断涌现，显著降低了潜在攻击者的技术准入门槛。尽管 Microsoft 早已停止对部分老旧 Windows 版本（如 Windows XP，至今仍是嵌入式设备中应用最为广泛的操作系统）的支持，然而，仍有数以百万计的嵌入式设备与个人计算机持续运行着这些存在安全隐患的旧版操作系统。受多种因素制约，这些系统未能及时升级，这无疑为黑客大开方便之门，使其得以轻易入侵。

与此同时，基于 Linux 的嵌入式系统正在迅速普及，已然引起网络犯罪分子的高度关注，他们迅速调整自身技术策略并创建全新的工具以适配基于 Linux 的嵌入式系统的独特细节与运行机制。然而过度高估 Linux 系统本身的安全性其实暗藏风险。尽管攻击者近期才将注意力转向基于 Linux 的嵌入式设备，但他们正以惊人的速度追赶。与 Windows 可用的安全产品相比，当前基于 Linux 的嵌入式设备可用的网络安全产品数量有限、功能局限，在应对复杂多变的网络攻击时，也难以提供切实有效的防护。

如今的企业需要采取比以往更加精明、高效的行动策略，从而确保系统与数据安全。卡巴斯基嵌入式系统安全解决方案，集强大威胁情报能力、“选择加入”式恶意软件精准检测与漏洞利用防护、全面且精细的系统强化控制功能，以及灵活便捷的管理特性于一体，是专为嵌入式系统量身定制的一体化安全解决方案。它可为众多网络安全供应商已停止支持的旧版嵌入式系统提供专属且前沿的安全防护，同时，针对当下广泛应用的运行 Linux 操作系统的现代嵌入式设备，也能提供同等高水准的安全防护。



嵌入式系统：威胁模型

嵌入式安全面临的挑战

6 **严格的法规制约**
许多嵌入式设备经常会涉及财务及个人身份信息处理，受相关监管法规严格约束，必须采取高度谨慎的安全防护措施。

7 **内部人为风险**
根据卡巴斯基数据显示，在嵌入式系统所遭受的全部攻击中，成功得手的攻击事件里，有超过 50% 与员工或第三方服务提供商的“内部人员行为”紧密相关。

8 **Linux 相关隐忧**
嵌入式平台发展势头迅猛，具备更高的灵活性与更广泛的配置选择。然而，这一趋势已引起网络犯罪分子的关注，相较于 Windows 环境，现代专业安全解决方案的选择面临诸多限制，安全形势更为复杂。

产品亮点

可为任何嵌入式场景提供安全防护
卡巴斯基嵌入式系统安全解决方案可为各类嵌入式场景提供多层保护，适配不同能力水平设备与多样实施场景。这包括支持基于 Windows 和 Linux 等不同操作系统的平台。

兼容新旧版本的系统防护
卡巴斯基嵌入式系统安全解决方案经过优化迭代，可在Windows XP、7、8、10和11中全功能运行。未来，卡巴斯基将继续支持 Windows XP，给客户留出充足的升级准备时间。卡巴斯基嵌入式系统安全解决方案还支持运行Windows或Linux操作系统的最新架构。

低资源消耗，高级别防护
即使是在低端硬件上，卡巴斯基嵌入式系统安全解决方案也能有效运行，实现低资源消耗与高保护级别的平衡。

统一生态系统
卡巴斯基嵌入式系统安全解决方案是卡巴斯基解决方案系列的有机组成部分，可通过同一控制台与其他卡巴斯基产品协同管理，同时具备统一管理界面的可视化能力，采用统一工作流程。

核心功能

安全控制系统强化
系统安全强化技术涵盖应用程序、设备与更新控制，仅允许使用受信任的应用程序、外围设备及更新来源来用。可有效阻止未经授权的程序启动运行，包括恶意软件以及可能被恶意利用的应用程序。

反恶意软件功能
开启该安全层后，借助本地或云端运行的威胁情报、启发式模型与机器学习模型，通过精确的检测逻辑识别已知、未知及高级威胁，专用反加密勒索技术也可保护您的设备免受勒索软件侵害。

漏洞利用防御
防止正在运行的 Windows 系统组件和第三方应用程序中的漏洞被利用，助力抵御更高级的攻击，包括绕过默认拒绝模式应用程序控制机制的攻击以及采用无文件技术的攻击。

网络威胁防护
可防止对操作系统的入侵，抵御端口扫描、暴力破解攻击，以及利用网络相关漏洞针对目标设备的网络攻击，从而阻断针对嵌入式系统的主要攻击途径。

完整性监控与合规性支持
完整性监控与合规性支持1具备文件完整性和注册表访问监控功能，可追踪对指定注册表项、文件及文件夹的操作，并阻止任何非预期的更改。既能检测恶意软件发起的入侵，也能察觉对关键资源的直接访问或离线修改，符合数据保护法规推荐对策，助力合规进程。

支持功能较少与旧版的系统
可支持使用陈旧硬件、不受支持操作系统（最低支持 Windows XP SP2）的低功率嵌入式系统，让用户能继续安全运行旧款设备或旧版桌面，直至做好升级准备。

日志检查[1]
通过监测和检查 Windows 事件日志检测潜在安全破坏行为。当应用程序检测到显示网络攻击企图的异常行为时，会及时通知管理员。

本地&云端的灵活管理
可按需通过本地管理服务器或卡巴斯基安全中心 SaaS 云控制台，管理企业嵌入式系统及其他卡巴斯基解决方案的安全安全性能。本地管理适用于严格保障隐私的场景，但由供应商运行的云端 SaaS 控制台能降低资本和运营支出，快速启动安全工作流程，减少维护烦恼。

[1] 仅限 Windows 操作系统

防火墙管理

可从卡巴斯基安全中心中直接配置操作系统防火墙，借助统一控制台轻松管理本地防火墙。在嵌入式系统未入域、无法集中配置 Windows/Linux 防火墙设置时，这项功能尤为重要。面向 Windows 系统设有专有应用级防火墙，可通过更精细化地管理应用程序网络连接，进一步缩小攻击面。

解决连接性差难题

由于许多类型的嵌入式设备通常处于远程位置，蜂窝覆盖不佳、近距离无线电干扰等因素容易导致连接性差。卡巴斯基嵌入式系统安全解决方案即使在非常低的带宽下也能稳定运行，即使长时间没有连接仍可提供可靠防护。

集成托管检测和响应

该解决方案与卡巴斯基安全运营中心集成，实现全天候监控与快速响应。可及早检测并遏制针对嵌入式设备的复杂攻击，避免企业遭受重大财务损失。

专家服务和高级支持

正确维护安全解决方案的生命周期需要投入大量精力，而嵌入式设备因自身特殊性，与常规端点存在差别，这导致维护嵌入式系统安全性往往格外耗费心力。卡巴斯基专家服务能够为嵌入式系统安全解决方案的全生命周期保驾护航，涵盖从部署与更新、配置与性能优化，到迁移至更新型硬件的每一个关键阶段。不仅如此，我们提供的高级支持服务，可确保各类事件得到优先且专业的处理，更有专职技术客户经理凭借其专业累积的行业知识，为您提供多方位支持。

更多解决方案

卡巴斯基威胁情报

提供多元服务选择，融合多方情报源、威胁数据源及内部研究成果，由专业安全团队深入剖析，助您全面洞悉针对贵组织的网络威胁态势。

支付系统安全评估

针对 ATM 与 POS 设备展开全方位分析，清晰呈现当前安全防护级别，助力您提升安全性、优化设备配置，消除各类安全漏洞。

卡巴斯基新一代安全系列解决方案

全管控于一体，兼具 EDR 的透明度集前沿的端点防护与高效的安与快速响应能力，以及 XDR 的全局可视化与高性能工具优势，构建灵活的分层产品体系。

行业

- 金融服务
- 交通和旅游（票务）
- 零售业
- 酒店
- 医疗
- 政府和非商业
- 娱乐

设备

- 自动取款机
- 售票机
- 加油机
- 结帐
- 销售点
- 医疗设备
- 传统端点
- 投币式自动售货机和游戏机

使用嵌入式设备的行业

www.kaspersky.com.cn

我们致力于构建更为安全的世界，让技术赋能美好生活。这正是我们守护网络安全的初心，让全球各界人士都能共享技术发展带来的无限机遇。确保网络安全，创造更安全的明天。

了解有关更多信息，可访问：
kaspersky.com/about/transparency

Proven.
Transparent.
Independent.