戴尔的设备安全实践

建立设备信任的三个注意事项

戴尔网络专家阐述了设备安全防护实践对于保持 IT 生态系统长期弹性所具有的关键作用。

作者
Rick Martinez
戴尔研究员兼副总裁

Eric Baize
产品和应用程序安全部副总裁

简介

在当今拥挤的网络市场中，安全产品和解决方案的选择可能让您饱受困扰。如果我告诉您，安全策略中最重要的部分并不是您的安全产品，您会怎么想？

作为一家大型 PC 制造商，戴尔高度重视安全问题。近年来，随着我们目睹勒索软件攻击造成的毁灭性后果以及基于固件的恶意软件不断蔓延，端点设备正日益成为显著的攻击目标，这一趋势已变得愈发清晰。遗憾的是，对于单点解决方案而言，无论怎样创新，皆无法完全保障用户和数据的安全。

当您重新评估现有生态系统安全性并考量换新升级设备时，除了关注采购哪些产品外，更需考量 PC 制造商的安全理念与实践方式。为什么？您可能会认为这与产品评估有关，但实则同等重要的是对供应商的全面评估。一家值得信赖且经验丰富的安全 PC 供应商可深度洞察威胁形势，并且能够利用专业知识，在威胁环境演进中为您的组织提供持续防护。与这样的合作伙伴携手，您将构建能智能化解必然攻击、驱动长期网络弹性的安全生态系统。

安全始于早期阶段，可能比您预想的更早

IT 决策者和终端用户通常会与销售人员、设备和产品支持人员进行互动。在安全方面，这只是冰山一角。为什么？这类似于食品安全。您不能仅凭与餐厅服务员的互动来判断食品安全，因为食品安全始于厨房。同理，确保设备安全的措施也必须在产品生产前就已落实 — 而这些措施通常难以直观地看到。戴尔投入了无数的工程时间与智慧成果，从底层构建客户 IT 工作的安全体系，这套精细复杂的流程和协议贯穿每台设备的设计、开发和交付全生命周期。那些无人目睹的工作，正是构筑底层稳定基础的基石，最终成就了极致安全的设备。这些工作在为保障客户 IT 工作环境的安全贡献力量，无论是联邦客户、大型企业还是中小企业都能从中受益。戴尔坚信，所有企业无论规模大小，都应享有现代化安全保障，我们致力于提供守护贵企业安全、进而保障您客户安全的解决方案。

我们的设备安全实践

在规划商用设备的安全防护体系时，我们始终以安全成效为导向，即设备如何助力提升组织的整体安全态势。设备如何帮助防范攻击？遭受攻击时如何维持安全状态？它如何在整个生命周期中保持安全？

如您所料，我们拥已实施数十项符合行业标准的商用 PC 安全开发实践，全面支持零信任安全方法。下面我将重点介绍三个核心主题：安全供应链、安全代码与使用中的安全保护。

1.我们筑牢设备供应链安全防线。这意味着对硬件和软件供应链（即物理供应链和数字供应链）进行严格管控。这些控制措施有助于保障产品在制造、装配、交付和部署全流程中的完整性，确保客户获得的设备与采购需求完全一致，无任何冗余或缺失。此外，我们还将这些严格的要求传达给我们的所有供应商。尽管如此，本着真正的零信任"假设已被入侵"原则，我们在此流程的每个环节中都植入验证机制。

这些检查包括 Secured Component Verification* 等先进技术，用于识别组件更换，以及 SafeBIOS 脱机验证技术检测系统最高权限固件的篡改行为并实时发出警报。这些功能与众多其他特性已内置于戴尔可信设备中，它们正是 Dell Trusted Workspace 产品组合的核心组成部分。但我们也在整个供应链中充分利用这些功能特性，确保链条上所有环节的完整性与安全性。这使我们能够提前发现偏差，避免其进入供应链下一环节。（* 可作为选配功能另行购买。具体供应情况视国家/地区而异。）

这就是我所说的以结果为导向。这些功能特性的开发并非为了创新而创新，而是因为它们能切实解决客户在供应链安全和机组管理方面的现实痛点。从不信任，始终验证。

回归供应商评估的本质：请谨记，您选择的 OEM 供应链即延伸为您自身的供应链 — 因此务必核查其已实施的安全实践体系。（如需深入了解保障供应链安全的关键要素，请参阅供应链白皮书中的观点。）

2.我们致力于设计与开发安全设备。正是在此处，您将看到安全实践与功能特性的深度融合。这正是我们打造高效创新硬件与固件的核心方法。

如今，安全功能特性已成为我们面向市场的产品中不可或缺的一部分，但这还只是整个安全"拼图"的一部分。如果我们产品的设计、开发和测试不受我们规定的安全开发生命周期 (SDL) 的约束，那么产品安全就无从谈起。所有技术提供商的一个核心责任，是确保销售的产品不会因存在漏洞而无意间将风险转嫁给用户。为了防范攻击并增强安全软件堆栈的韧性，我们在软件开发过程中执行严格的威胁建模，针对高度复杂的对抗性假设识别风险，甚至将这种方法论应用于关键硬件。

在整个开发过程中，我们与一些顶尖的渗透测试顾问和第三方研究人员合作，测试并验证这些威胁建模假设，向他们提供戴尔系统，请他们尝试入侵。除此之外，我们还推出了漏洞披露赏金计划，旨在对商用 PC 的安全性进行压力测试。这些测试报告的结果会在整理后反馈给工程部门，以便工程部门制定缓解措施。然后持续迭代。我们为什么要这样做？戴尔客户的环境需要经过安全强化、受信任的设备才能高效运营。

3.我们致力于确保设备在使用过程中安全无虞。安全需要群策群力。如今，真正的安全性包括硬件、固件以及软件层面的防护。因此，戴尔倾力打造了一个由经过全面审查、业界卓越的合作伙伴组成的生态系统，以提供针对高级威胁的防护。其中许多防护功能已直接集成到我们的商用 PC 中。然而，黑客也在不断创新攻破软件的方法。为此，我们的 SDL 实践旨在将保护扩展到产品发布之后，包括快速轻松地识别和修复漏洞的能力。戴尔还会主动报告即将发布的安全更新和清晰的安全支持策略，以便客户更轻松地了解其产品在整个生命周期内如何持续受到保护。为了帮助客户快速找到有关漏洞和产品版本适用性的信息，我们将所有安全公告和通知整合到同一个位置。结合记录详实的漏洞响应策略文档，我们就能在有新漏洞报告时与研究人员紧密合作。这缩短了循环周期，并确保始终提供准确的信息，从而让客户能够评估并修复其环境中的风险。

一家安全合作伙伴，全面整合各类防护措施

戴尔致力于建立一个可靠安全的互联世界。我们不懈努力，时刻将您的数据、您客户的数据、网络、组织和安全置于首位，在我们所有的端到端解决方案中融入安全防护基因。有关我们的安全实践的更多信息，请访问戴尔安全和信任中心。如有疑问，请与戴尔代表联系，或通过 global.security.sales@dell.com 联系我们的安全专家

详细了解戴尔端点安全

联系 Dell Technologies 专家

查看更多资源

加入 #HashTag 对话

DELL Technologies