DELL Technologies

可信设备剖析

了解戴尔商用 AI PC 为何具备卓越的安全性[1]

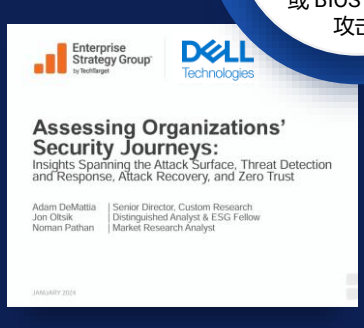
威胁形势与挑战

操作系统以下层面的新兴攻击载体正在带来新的风险

端点设备是安全漏洞的主要入口。近年来，随着混合办公模式的推行，受攻击面扩大，人们对设备安全性的担忧激增。攻击者越来越多地将供应链、rootkit 和其他固件漏洞作为攻击目标，而仅靠过时的 EDR 软件基本上无法检测到这些漏洞。

自 2020 年以来，基于设备的威胁增长了 1.5 倍。[2]

69%
的组织报告称，至少遭遇过一次设备或 BIOS 层面的攻击[2]



采购新 PC 时的主要评估标准：

- 自动检测 BIOS 事件[3]
- 解决高风险配置问题[3]

为应对现代威胁，设备须从设计之初就具备安全性，并配备内置安全功能，以便有效发现和排除各种攻击。

解决方案

利用安全性出众的商用 PC[1] 预防、检测、响应基础性攻击，并从中恢复。

机群的安全性取决于其每台 PC。但是确保设备安全可信的因素是什么呢？那就是可见性和可操作性。获取更多数据有助于做出明智的决策，从而检测到极为隐蔽的新兴威胁。自动化技术能够助您更快地解决潜在问题。

基于英特尔和 AMD 处理器的戴尔商用 PC 具有强大的硬件和固件防御功能，可为机群带来出色的可见性和可操作性。

戴尔可信设备剖析

权益

- 严格控制供应链，从首次启动起就确保安全
- 通过全面深入的固件级别可见性维护 BIOS 完整性
- 保护终端用户身份，防止恶意软件窃取凭证
- 收集“操作系统层面之下”的遥测数据，并与操作系统级别的数据相结合，以更快地发现问题，做出响应，并进行修正

通过 PC 遥测改善安全性

利用操作系统之下的安全状况洞察，弥合 IT 安全缺口并完善软件解决方案。戴尔通过将 PC 遥测技术与业界卓越的软件提供商进行集成，以提升整个机群的安全性。[1]
了解详情 →

保持 BIOS 完整性

通过戴尔特有的 BIOS 验证功能发现和排除威胁。利用 BIOS Image Capture 评估损坏的 BIOS、进行修复，并获取相应见解以降低未来面临威胁的风险。[1]
了解详情 →

验证固件完整性

戴尔特有的固件验证通过英特尔处理器提供基于硬件的安全功能，可防范针对高权限固件的未经授权访问和篡改。[1]

发现隐患

攻击指标是戴尔提供的一项早期警报功能，可以扫描基于行为的威胁，以免其造成损害。[1]
了解详情 →

检测已知漏洞

戴尔特有的常见漏洞和风险 (CVE) 检测功能可监测公开报告的 BIOS 安全缺陷，并提供更新建议以降低风险。[1]
了解详情 →

保护终端用户凭据

戴尔特有的 SafeID 是一种专用的安全芯片，可验证用户的访问权限，保护用户凭据，确保凭据不被恶意软件窃取。[1]
了解详情 →

在整个 PC 生命周期内确保安全使用

严格且先进的供应链控制措施以及可选附加功能，如戴尔特有的安全组件验证，可确保 PC 在交付期间及其整个生命周期内的完整性。[1]
了解详情 →

行业优势地位

戴尔能提供 BIOS 级可见性，堪称 PC 制造商中的佼佼者。[1]

了解如何维护设备信任以抵御现代威胁。[4]
了解详情 →


A Principled Technologies report: In-depth research. Real-world value.

A comparison of security features in Dell, HP, and Lenovo PC systems

Approach

Dell™ commissioned Principled Technologies to investigate 10 security features in the PC security and system management space:

- Support for monitoring solutions
- BIOS security and protection features
  - Platform integrity validation
  - Device integrity validation via off-site measurements
  - Component integrity validation for Intel® Management Engine (ME) via off-site measurements
  - BIOS image capture for analysis
  - Built-in hardware cache for monitoring BIOS changes with security information and event management (SIEM) integration
- Microsoft Intune management
  - BIOS setting management integrations for Intune
  - BIOS access management security enhancements for Intune
- Remote management
  - Intel vPro® remote management
  - PC management using cellular data

These features rely on manufacturer-enabled communication between the hardware and the operating system (OS). We reviewed publicly available marketing claims and feature documentation for three Windows original

探索戴尔可信设备


笔记本电脑 →


台式机 →


工作站 →

Dell Trusted Workspace 助您随时随地安全办公

内建和内置的硬件安全措施

增置的软件安全措施

访问我们
dell.com/endpoint-security

联系我们
global.security.sales@dell.com

了解详情
端点安全性博客 →

加入对话
delltechnologies @delltech

来源和免责声明

[1] 基于戴尔内部分析，包括 2024 年 10 月进行的分析（针对英特尔处理器）和 2025 年 3 月进行的分析（针对 AMD 处理器）。适用于搭载英特尔和 AMD 处理器的 PC。并非所有 PC 都提供所有功能。某些功能需要额外购买。经 Principled Technologies 验证。《A comparison of security features》，2024 年 4 月。

[2] 来源：Futurum Group，《Endpoint Security Trends》，2023 年。

[3] 来源：Dell Technologies 委托 TechTarget 旗下部门 Enterprise Strategy Group 撰写的定制研究调查报告，《*Assessing Organizations' Security Journeys*》，2023 年 11 月。

[4] Principled Technology 研究结果仅适用于搭载英特尔处理器的设备。