探索

Dell Trusted Workspace

随时随地安全工作

得益于专为当今基于云的环境而构建的硬件和软件防御措施。

混合办公模式让组织暴露于新型攻击媒介。恶意分子采用的技术愈发复杂，因此如今要想实现有效的端点安全性，需要多层防御手段来保护设备、网络和云。

通过全面的硬件和软件保护解决方案，减少受攻击面，防范现代威胁。

详细了解产品组合 →

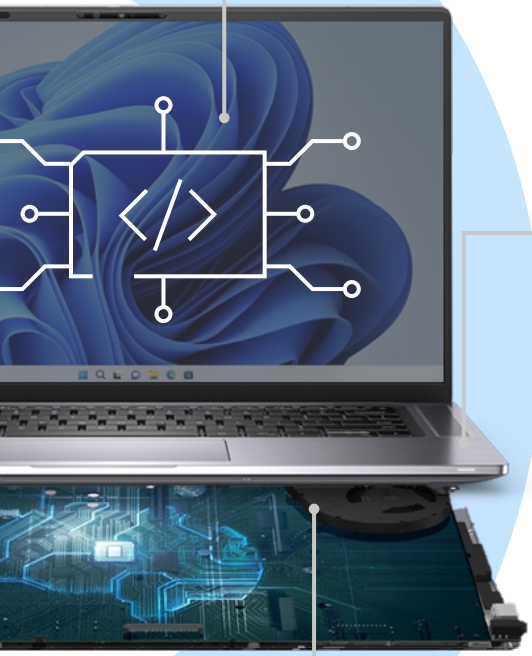
安全性出众的商用 AI PC[1] →

可提高各机群安全性的软件 →

DELL Technologies

Dell Trusted Workspace

多层防御



增置的
软件安全措施

借助经过专业挑选的合作伙伴生态系统中的软件，增强针对高级威胁的防范措施。充分利用整合式安全产品采购带来的优势和效益。

内置的
硬件和固件安全措施

戴尔商用 AI PC 安全性出众，可防范和检测基础攻击。[1] 通过在 BIOS/固件和硬件级别部署深度防御措施，可有效保护正在使用的设备。

戴尔率先将 PC 遥测与业界卓越的软件集成，用以提升整个机群的安全性。[1]

内建的
供应链安全性

确保您的设备从首次启动开始便安全无虞，让您放心工作。安全的 PC 设计、开发和测试，有助于降低产品漏洞风险。严格的供应链控制措施可降低产品遭篡改的风险。

防范、检测和应对来自不同位置的威胁

Dell SafeGuard and Response

Dell SafeData

持续防范不断进化的威胁

Dell SafeBIOS

Dell SafeID

确保交付时硬件未被篡改，让您安心无忧

Dell SafeSupply Chain

DELL Technologies

Dell Trusted Workspace 内建的安全性以及内置的安全措施

安全性出众的商用 AI PC[1]

安全性始终如一

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 完整性。
了解详情 →

保持 BIOS 完整性

通过戴尔特有的 BIOS 验证 **SafeBIOS** 发现和排除威胁。评估损坏的 BIOS，将其修复并从中得出见解，从而降低暴露于未来威胁之下的可能性。
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。了解详情 →

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，以免它们造成损害。
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。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。了解详情 →

Principled Technologies

*经 Principled Technologies 认可的行业优势地位**

通过 PC 遥测弥合 IT 安全缺口

利用操作系统之下的安全状况洞察，完善软件解决方案。戴尔开创业界先河，通过将 PC 遥测技术与业界卓越的软件服务进行整合，有效提升整个机群的安全性。[1]了解详情 →

探索戴尔可信设备

笔记本电脑 →

台式机 →

工作站 →

*研究结果仅适用于搭载英特尔处理器的设备。

DELL Technologies

Dell Trusted Workspace 增置的安全措施

可提高各机群安全性的软件

通过 Dell SafeGuard and Response 抵御高级网络攻击

防范、检测和应对来自不同位置的威胁。人工智能和机器学习可主动检测并阻断端点攻击，而安全专家可跨端点、网络和云帮助搜寻威胁并针对发现的威胁实施补救。

合作伙伴

CrowdStrike Falcon® →

Sophos | Secureworks® Taegis™ XDR →

利用 Dell SafeData 保护设备上和云中的数据

助力用户随时随地安全协作。Netskope 针对云安全性和访问权限采取以数据为本的应对方法，可随时随地保护数据和用户，而 Absolute 则在企业级防火墙外部提供 IT 可见性、安全性和持久性。

合作伙伴

通过 Absolute 实现端点、应用程序和网络的自我修复 →

通过 Netskope 探索安全服务边缘解决方案 →

探索戴尔安全服务

在戴尔的支持下，客户可以自行管理安全措施或让专家代为管理。通过我们完全托管的全方位 SecOps 解决方案，在 IT 环境中预防和应对安全威胁，并顺利从威胁事件中恢复。

详细了解 Managed Detection and Response Pro Plus →

DELL Technologies

Dell Trusted Workspace 硬件辅助式安全措施

集成的安全性

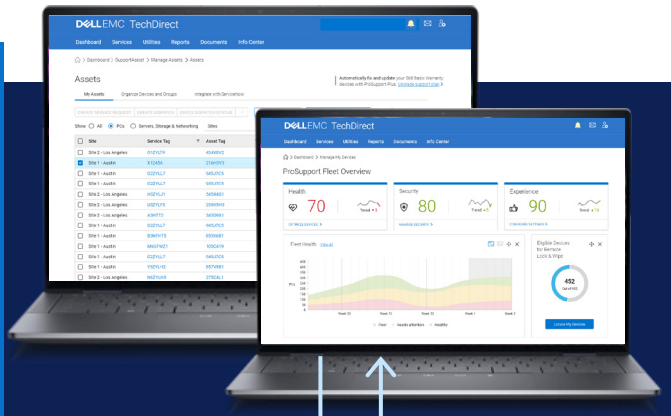
不断变化的网络威胁会设法绕开仅以软件为基础的防护措施。使用硬件辅助式防护措施协助缩小端点受攻击面。

要防范现代威胁，硬件和软件防护措施必须协同配合。戴尔可以在这方面助您一臂之力。我们携手业内知名的安全合作伙伴，将丰富的设备级遥测与尖端威胁检测技术相结合，提升您的机群的安全性。

- ✓ **减小受攻击面**
- ✓ **改进威胁检测**
- ✓ **保持设备信任**
- ✓ **整合提供商**

增置的软件安全措施

目前只有戴尔将 PC 遥测与业界卓越的软件集成，用以提升整个机群的安全性[1]、[2]



操作系统

内置的硬件和固件安全措施

Dell SafeBIOS

戴尔可信设备应用程序

BIOS Verification | CVE 检测 | 攻击指标

合作伙伴的“操作系统之下”芯片功能

内建的供应链安全性

Dell SafeSupply Chain[3]

在设备端•和云端
使用安全组件验证功能

DELL Technologies

Dell Trusted Workspace
助您随时随地安全工作。

内建和内置的硬件安全措施

增置的软件安全措施

通过多重防御措施，减少受攻击面，提升长期网络弹性。

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
LinkedIn /delltechnologies

X @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。搭载英特尔处理器的 PC 由 Principled Technologies 进行验证。《A comparison of security features》，2024 年 4 月。[2] 可与 CrowdStrike Falcon Insight XDR 和 Absolute 集成。[3] 供应情况因地区而异。

DELL Technologies