intel

现代 AI PC 需配备先进安全功能

借助英特尔® 酷睿™ Ultra 处理器和英特尔® vPro® 平台，获得强大且智能的多层安全防护。

您的终端设备是否为 AI 新时代做好了充分的安全准备？

AI 为各行各业的企业开启了一个充满机遇与挑战的新时代。2024 年初，65% 的调查受访者表示，他们的企业已频繁使用生成式 AI（GenAI），这一比例较 10 个月前几乎翻了一番[1]。如今，企业和机构都在积极探索“AI 无处不在”的新时代中 AI PC 的应用场景，包括能够释放员工生产力的 GenAI 助手、能够解锁新体验的基于 AI 的企业应用，以及能够助力将 AI 融入企业应用的 AI 开发工具。在企业和机构全面采用并扩展 AI 之前，所有这些应用场景都必须先落实企业级安全保护。

许多企业和机构正在探索在核心领域之外，于整个企业范围内采用 AI 所带来的诸多益处。借助支持 AI 的台式机、笔记本电脑、工作站以及其他终端设备，可以安全地执行从客户端到云端的模型训练和推理任务。虽然 AI PC 在提升终端用户工作效率方面具有巨大潜力，但同时也大幅增加了黑客可利用的攻击面。在 PC 本地运行 AI 会使用到敏感数据集，这些数据集会成为具吸引力的庞大攻击目标。远程办公人员使用基于 AI 的客户端应用会产生新的攻击面，而这些攻击面不像在传统的企业防火墙内那样受到严密保护。

一旦企业和机构遭遇数据泄露，其后果可能不堪设想。除了可能需要支付数百万美元的罚款和承受运营中断的损失外，数据泄露还可能导致客户信任的永久丧失以及品牌声誉的长期损害。

45%
的企业和机构认为数据隐私问题是采用 AI 技术的主要阻碍[2]，而 34% 的企业和机构则在安全问题上犹豫不决[3]。

您的终端设备是否为 AI 新时代做好了充分的安全准备？（续）

488 万美元 一项 IBM 研究显示，2024 年数据泄露的平均成本达到 488 万美元，较 2023 年增长了 10%[4]。

如果上述统计数据让您感到担忧，这是十分正常的。威胁手段已经愈发复杂，并且仍在持续进化。这些威胁手段涵盖从内核漏洞利用到电子邮件网络钓鱼的各种形式，并且它们针对的是操作系统 (OS) 之上的和之下的不同 PC 攻击面。AI 正在被用来对抗自身，不法分子可以利用它来让自己的攻击更具隐蔽性和破坏性。

在防范主动威胁的同时，您可能还肩负着满足内部知识产权指导管理规范或监管合规性的任务。《健康保险携带和责任法案》(HIPAA)、《电信法》、《家庭教育权和隐私权法案》(FERPA) 以及《格雷姆-里奇-布里利法案》(GLBA) 只是众多法律中的一部分，这些法律规定了机密信息的存储、访问及使用方式。那么，AI PC 是否有助于解决这些数据问题，还是会因其在客户端独立存储 AI 所用数据而带来新的合规要求？

幸运的是，有一种全面的安全解决方案，通过硬件与软件的协同来保护您的 AI PC（让您高枕无忧）。本电子书将介绍基于英特尔® 酷睿™ Ultra 处理器和英特尔® vPro® 平台的 AI PC 如何助力您增强对现代网络威胁的防御能力。

在 PC 上安全运行 AI

正如之前所述，如今的 AI PC 需要先进的数据保护功能，以应对复杂的威胁、系统漏洞和安全要求，同时这种保护功能还需易于集成到您当前安装的安全软件中。而基于英特尔® 酷睿™ Ultra 处理器和英特尔® vPro® 平台的 AI PC，能够在硬件、操作系统和软件等多个层面提供主动防御、快速响应和恢复能力。

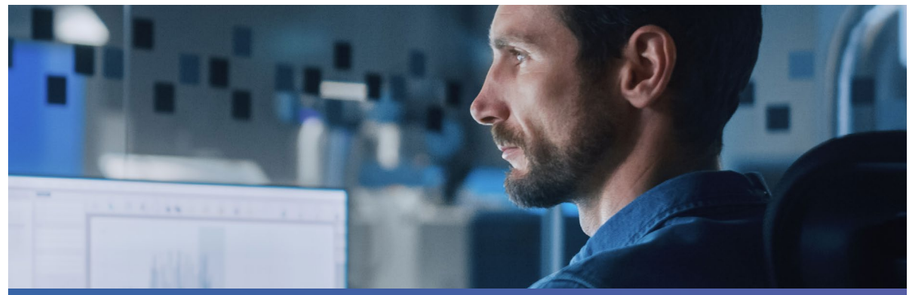
提高 AI 安全性的关键在于增强对异常行为和恶意软件活动的可见性。英特尔® vPro® 的基础保护现已映射至 MITRE 对抗性战术、技术和通用知识 (ATT&CK) 网络威胁框架以及针对 AI 系统的对抗性威胁景观 (ATLAS) AI 威胁框架，这使您能够深入了解有哪些硬件功能可以有效减轻真实场景下攻击技术的威胁。这些全球可访问的知识库能够帮助企业和机构了解不法分子针对 AI 系统所使用的策略与手段，使其能够更好地做好准备并应对潜在威胁。

通过与 ATT&CK 和 ATLAS 框架的整合，英特尔® vPro® 可为 AI PC 提供基于硬件的主动安全机制，能够更有效地识别攻击行为并减少潜在危害。如果您的 AI PC 运行的是Windows11系统，那么您将更为幸运，因为该操作系统同样与ATT&CK和ATLAS框架相兼容。这种操作系统层面的兼容为硬件安全再添一层至关重要的保障。

提升推理性能与安全性

在 AI 新时代，商用 PC 实现了巨大的飞跃，进化为如今的 AI PC。这些现代化的 PC 已成为推动数字化转型和提升终端用户工作效率的核心工具。它们能够在设备端运行推理及其他 AI 应用，同时确保数据在私有、封闭的环境中进行处理。这能够更有效地减少传输中或存储在云端的机密信息和知识产权 (IP) 暴露的风险。

基于英特尔® 酷睿™ Ultra 处理器和英特尔® vPro® 平台的 AI PC 通过基于硬件和 AI 的安全机制来保护其敏感数据。



英特尔® vPro® 平台具备基于硬件的安全功能，可将检测和解决安全漏洞所需的管理时间减少高达 35%[5]。

本地推理的优势

合规：对于监管要求严格的行业而言，本地推理通过将数据保存在设备范围内，帮助确保遵守数据保护法规。

控制：企业和机构可以更好地控制其数据和模型，使他们能够根据自身特定需求实施定制化的安全措施。

韧性：即便云服务中断，本地推理依然能够继续运行，从而确保了关键功能的持续可用性和访问性。

在操作系统之下增强保护

得益于基于硬件的身份验证和安全功能，用户和系统关键软件在启动时就受到保护。

借助英特尔® vPro® 提供的基于硬件的安全功能，可以将重大安全漏洞事件的数量降低多达 23%[5]。

操作系统之下的安全机制包括：

安全启动
英特尔® Boot Guard 是操作系统之下的安全功能，专用于防范通过 BIOS 发起的固件和软件攻击。

BIOS 保护
英特尔® Runtime BIOS Resilience 有助于降低向统一可扩展固件接口 (UEFI) 内存中注入恶意代码的风险，增强安全防护。

基于硬件的安全功能
英特尔® Partner Security Engine 为片上系统 (SoC) 提供了可与其他安全引擎隔离运行的安全机制。它使用一个专用的加密系统来卸载诸如安全启动、认证、密钥存储及其他加密操作等任务。

防范内核漏洞利用及其他内存攻击

在接受调查的 IT 负责人中，有 95% 的人表示网络攻击变得比以往任何时候都要复杂，并有许多 IT 负责人觉得对这些新的威胁载体准备不足[6]。内核漏洞利用就是一种会破坏操作系统内核的复杂攻击实例。

为了有效减轻运行时威胁，必须在操作系统运行时保护 AI 应用和数据。基于英特尔® 酷睿™ Ultra 处理器和英特尔® vPro® 平台的 AI PC 可以通过 Windows BitLocker 和基于 CPU 的英特尔® 高级加密标准新指令（Intel® Advanced Encryption Standard New Instructions，英特尔® AES-NI）来帮助保护用户数据和文件。英特尔® 全内存加密（Intel® Total Memory Encryption，英特尔® TME）有助于保护含有重要 AI 模型和数据资产的内存免受冷启动攻击的危害。基于英特尔® 全内存加密-多密钥（Intel® Total Memory Encryption–Multi-Key，英特尔® TME-MK）的 Windows 11 加密虚拟机有助于在执行期间保护 AI 模型及内存中的数据。

图 1.借助英特尔® VT-x 和英特尔® VT-rp，帮助保护虚拟化环境免遭内存攻击和未经授权的访问

英特尔® 虚拟化技术（Intel® Virtualization Technology，英特尔® VT-x）和英特尔® Virtualization Technology with Redirect Protection（英特尔® VT-rp）能够在操作系统运行时于内存中运行，从而帮助保护虚拟化环境。英特尔® VT-x为虚拟机管理程序分配了更高的权限级别，从而更有效地将其与客户机操作系统隔离开。英特尔® VT-x 还可防止未经授权的访问并实施安全策略。而英特尔® 产品专有的英特尔® VT-rp 则仅允许经授权的代码对关键结构进行修改，以防止内核内存遭到破坏。此外，它还可以帮助减轻页表攻击，并隔离重要数据。

由用户与网页浏览器进行交互所触发的跳转导向编程（JOP）和返回导向编程（ROP）内存攻击，长久以来一直难以仅凭软件层面的解决方案来有效防御。英特尔® 控制流强制技术（Intel® Control-flow Enforcement Technology，英特尔® CET）通过基于硬件的机制（如影子堆栈和间接分支跟踪）来帮助防范 JOP 和 ROP 攻击，阻止未经授权的软件更改和恶意代码执行。

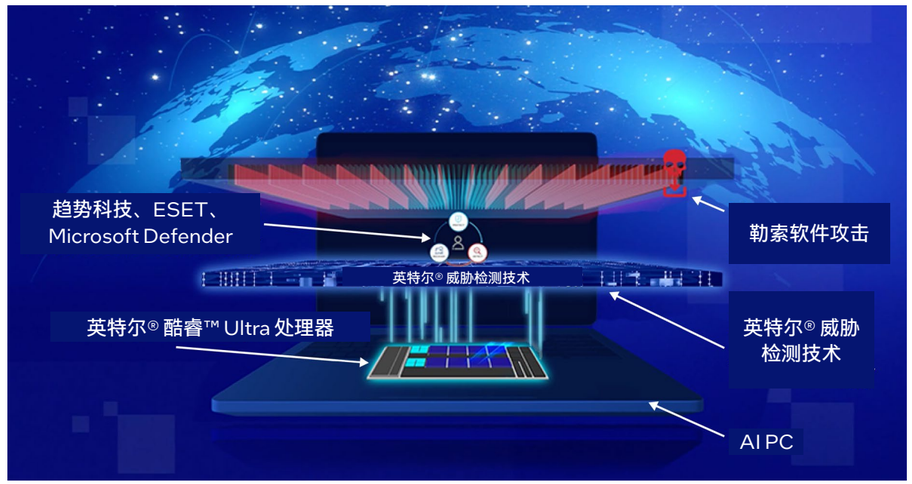
利用客户端 AI 帮助阻止勒索软件攻击

勒索软件攻击日益猖獗。据 2023 年调查结果显示，受访企业中有 100% 在过去 24 个月内遭受过勒索软件攻击[7]。这些攻击极具破坏性，每起事件可能给受害企业带来高达 1000 万美元的经济损失，甚至更多[7]。

勒索软件攻击是严峻的威胁，需要同样强大的安全策略来应对。仅仅依赖以软件和数据备份为核心的传统策略，如今已远远不够。您的安全计划应当包含培训用户识别网络钓鱼及可疑行为。您的终端安全也必须超越传统的启发式算法不断发展，它必须足够智能以识别新出现的威胁。

传统的端点检测和响应软件在应对勒索软件等复杂威胁时往往效果不佳，因为其主要依赖于已知的签名。内置英特尔® 威胁检测技术（Intel® Threat Detection Technology，英特尔® TDT）的英特尔® vPro® 则能够实时洞察新型攻击行为，并与您的安全软件紧密配合，从而有助于阻止勒索软件的侵袭，大大提升您的安全防护等级。这种基于 AI 并通过硬件实施的防护方法，对于快速演变的威胁变种或使用混淆技术的攻击同样有效。

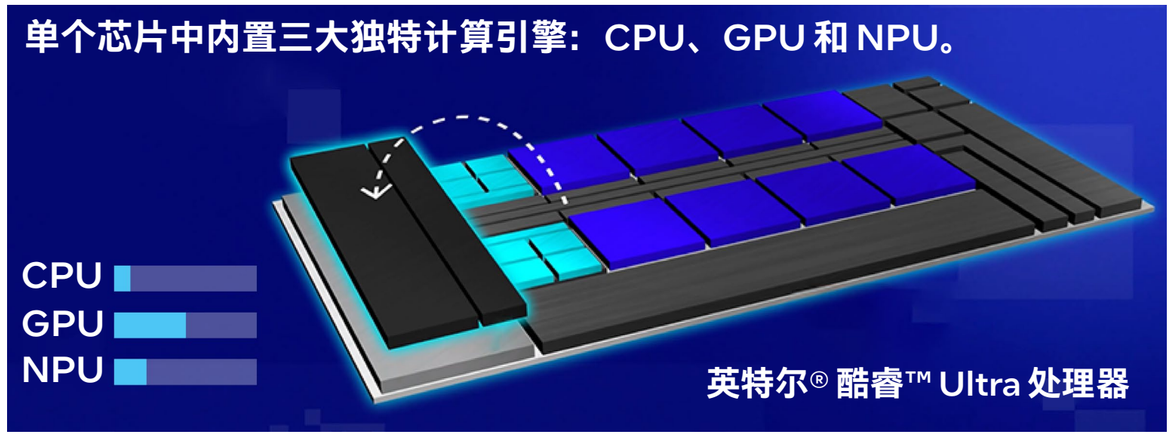
趋势科技（Trend Micro）、ESET、Microsoft Defender 以及其他主流独立软件供应商（ISV）解决方案均支持可开箱即用的英特尔® TDT。此外，英特尔® TDT 的活动被卸载到 GPU 上，这有助于确保用户的计算体验不会因为额外的安全处理而受到干扰。



与仅依赖软件的机制相比，英特尔® TDT 利用 AI 和硬件，将威胁检测效率提升了至少 24%[8]。

借助三大独特计算引擎，增强现有安全软件

搭载英特尔® 酷睿™ Ultra 处理器的 AI PC 在单个芯片中内置三大计算引擎：中央处理单元（CPU）、图形处理单元（GPU）以及神经处理单元（NPU，一种 AI 和机器学习 [ML] 引擎）。英特尔与生态系统合作伙伴紧密合作，提供全面的安全解决方案，从操作系统之下到整个堆栈，帮助全方位保护终端用户和设备的安全。此外，英特尔还与 ISV 携手合作，确保您的第三方解决方案能够无缝集成且运行稳定可靠。



以下软件解决方案面向英特尔® 酷睿™ Ultra 处理器进行了优化：

LiveDrop
利用 NPU 和 GPU 实现硬件加速文件传输，非常适合需要安全离线数据传输的场景。

Proofpoint
利用 NPU 在终端设备上运行复杂的数据丢失防护（DLP）工具，同时不影响用户的工作效率。Proofpoint 还增加了对敏感数据的自主保护，有助于阻止未经授权的数据外泄，并提供实时安全通知。

BUFFERZONE SafeBridge AI
利用 NPU 或 GPU 创建隔离的虚拟环境，并运用内容解除与重建（CDR）技术对恶意软件进行文档分析。

BUFFERZONE Safe Data
利用 NPU 或 GPU 直接在设备上智能扫描并分类包含敏感数据的文件，并将这些文件安全存储于仅经过身份验证的用户可访问的虚拟保险库中。此威胁检测与分析过程快速高效，不会影响用户的工作效率。

采取全方位的安全策略

面对不断涌现的新威胁，需要采取更加智能的安全防护方式。英特尔® 酷睿™ Ultra 处理器和英特尔® vPro® 平台提供了 AI 增强型端点保护，这种保护从硬件层开始，贯穿软件堆栈，并扩展至整个生态系统。要抵御当前普遍存在的勒索软件和网络钓鱼攻击等经 AI 增强的威胁，需要借助基于 AI 的工具。如果您部署了基于英特尔® 酷睿™ Ultra 处理器和英特尔® vPro® 平台的 AI PC，这些具智能适应性和主动性的安全保障措施将提供一层“隐形防护”，您无需进行任何配置即可发挥作用。

当您的企业和机构需要升级 PC 时，请选择基于多代 IT 开发测试的解决方案。这些方案在每个环节都集成安全功能，并且由评估安全韧性的专业团队提供支持。

凭借其先进的 AI 和安全功能，基于英特尔® 酷睿™ Ultra 处理器和英特尔® vPro® 平台的 AI PC 提供了一种智能的安全解决方案，能够帮助保护您的数据安全、满足监管要求，并保持业务连续性。那么，何不充分利用这些先进设备，将您的精力更多地投入到推动业务创新和增长中去呢？

更多信息请见 intel.com/AIPC 和 intel.cn/vpro。

英特尔在产品安全保障领域位居榜首

ABI Research 的一项独立研究评估了主流芯片供应商在其安全保障实践方面的创新与实施表现，英特尔被评为第一[9]。

[1] McKinsey，“The state of AI in early 2024: Gen AI adoption spikes and starts to generate value（2024 年初 AI 现状：生成式 AI 采用率激增，并开始创造价值）”，2024 年 5 月。
[2] Searce，“STUDY: AI Adoption Spends Jump Among Enterprises as Eliminating Data Privacy Concerns Remains a Foremost Opportunity for Driving Long-Term Growth and ROI（研究：随着减少数据隐私问题成为推动长期增长和提高 ROI 的首要契机，企业在 AI 采用方面的支出激增）”，*BusinessWire 网站*，2024 年 8 月。
[3] DigitalOcean，“AI and Privacy: Safeguarding Data in the Age of Artificial Intelligence（AI 与隐私：在人工智能时代保护数据安全）”，访问时间：2024 年 10 月。
[4] IBM，“Cost of a Data Breach Report 2024（2024 年数据泄露成本报告）”，2024 年 7 月。
[5] 基于英特尔委托 Forrester Consulting 进行的一项研究，该研究调查了全球使用英特尔® vPro® 的 500 名企业 IT 决策者（ITDM），包括来自美国、加拿大、法国、 德国、英国、澳大利亚、中国、印度及日本等国的 ITDM。为便于展现研究结果，Forrester Consulting 将受访者的数据和经验汇总到了一个假定年收入 10 亿美元、拥有 10,000 名员工的综合性企业或机构中。来源：Forrester Consulting，“The Total Economic Impact™ of the Intel vPro® Platform（英特尔® vPro® 平台的总体经济影响™）”，受英特尔委托，2024 年 1 月。
[6] 思科，“Cisco Cyber Threat Trends Report: From Trojan Takeovers to Ransomware Roulette（思科网络威胁趋势报告：从木马接管到勒索软件）”，2024 年 6 月。
[7] Cybereason，“Ransomware: The True Cost to Business 2024（勒索软件：2024 年给企业带来的真实成本）”，2024 年。
[8] 英特尔，“Intel® Threat Detection Technology: Protect Your PC Fleet from Advanced Cyberattacks（英特尔® 威胁检测技术：帮助保护您的 PC 免受高级网络攻击）”，访问时间：2025 年 2 月。
[9] ABI Research，“Embracing Security as a Core Component of the Tech You Buy（将安全作为技术采购的核心要素）”，访问时间：2025 年 2 月。

实际性能受使用情况、配置和其他因素的差异影响。更多信息请见 www.Intel.cn/PerformanceIndex。
性能测试结果基于配置信息中显示的日期进行的测试，且可能并未反映所有公开可用的安全更新。详情请参阅配置信息披露。
没有任何产品或组件是绝对安全的。
具体成本和结果可能不同。
英特尔技术可能需要启用硬件、软件或激活服务。
AI 功能可能需要额外购买软件、订阅或由软件或平台提供商启用，或可能有特定的配置或兼容性要求。数据时延、成本和隐私优势是指非基于云的 AI 应用。更多信息请见 intel.com/AIPC。
所有版本的英特尔 vPro 平台均需配备符合条件的英特尔处理器、受支持的操作系统、英特尔 LAN 和/或 WLAN 芯片、固件增强功能以及其他必要的软硬件，以实现平台特有的可管理性用例、安全功能、系统性能和稳定性。
如欲了解更多信息，请访问 https://edc.intel.com/content/www/cn/zh/products/performance/benchmarks/intel-vpro/。
© 英特尔公司版权所有。英特尔、英特尔标识以及其他英特尔商标是英特尔公司或其子公司的商标。其他的名称和品牌可能是其他所有者的资产。