利用英特尔® vPro® 为远程办公人员提供硬件辅助端点安全保护

全新英特尔® vPro® 平台在经强化的安全环境下提升员工远程办公体验。

intel®

远程办公带来的几大安全挑战

如今，员工逐渐重返办公室，但很多人仍然倾向于远程办公。由于远程工作模糊了人们处理个人事务和办公之间的界限，如果没有明确的管理方针和技术保障措施，安全风险可能会成倍增加：

- **Wi-Fi 网络不安全。**在家中、酒店大堂或咖啡馆办公的员工可能会下载文件或访问不安全的网站，这会使企业网络面临各种攻击和恶意破坏。此外，家庭 Wi-Fi 网络往往会连接多个设备，如路由器、物联网设备（IoT）和智能家居设备，而这些设备可能很容易被攻破。

- **没有防火墙。**远程办公时，员工的设备并非总能得到传统网络安全措施（如 VPN 和防火墙）的保护，因此许多企业和机构都采取了零信任的安全原则。

- **网络钓鱼攻击。**不法分子能够通过电子邮件或短信轻易模仿凭据，远程员工可能因无法验证此类信息的来源而遭到欺骗，从而受到勒索软件攻击。

- **设备不安全。**员工在公共场所办公时，路人可能会看到他们的笔记本电脑屏幕，当员工将笔记本电脑放在无人看管的地方或汽车里时，可能会遭到偷窥或失窃，这些情况都可能导致数据和隐私泄露。

为了降低这些安全风险，企业和机构必须实施一系列最佳实践，部署相关技术，包括采用安全软件。但是，安全软件会降低笔记本电脑的性能。面对层出不穷的威胁，企业如何既能确保其 PC 设备群使用全新安全功能，并可持续更新，同时又不影响员工的远程办公体验和 PC 性能？

目录：

英特尔® vPro®：赋能 IT 实现计算安全与管理，满足当下办公环境的需求

各地的企业和机构都需要能够抵御网络威胁、提高员工工作效率，甚至可为 IT 部门节省时间和成本的专用 PC。英特尔® vPro® 这一商用计算平台整合了软硬件技术，可让 IT 部门更好地控制 PC，让用户保持应有的工作效率。英特尔® vPro® 平台以开箱即用的硬件增强型安全防护功能，帮助保护 PC 和数据安全。

借助内置的远程管理功能，无论员工在何处办公，IT 部门都不必接触他们的 PC 即可提供支持 [1]。英特尔® vPro® 有助于保持远程办公所需的性能，同时还提供独特的基于硬件的多层安全措施。

英特尔® vPro® 有助于增强堆栈各层的安全性，支持联合身份验证解决方案，如 Windows Hello 增强型登录和 Windows Server 的 Microsoft Active Directory。此外，英特尔® vPro® 还支持更高一层的保护——端点检测和响应 (EDR) 解决方案，如 Microsoft Defender 商业版和 OEM 操作系统 (OS) 之下的安全软件集成。

在数百名受访者中，91% 的人表示与以往相比，采用英特尔® vPro® 的笔记本电脑和台式机运行速度更快、性能更好 [2]。

加强 PC 设备群的安全性

英特尔® vPro® 具备更全面的安全功能，这些功能专为分散在各处的远程办公人员设计，帮助保护各个地方的 PC。借助英特尔® vPro®，企业能够为远程设备及时安装补丁并更新，确保安全措施常新、到位。英特尔与出色的 EDR 解决方案提供商合作，使方案中的安全功能更有效、性能更出色，确保良好的用户体验 (UX)。

最重要的是，许多功能开箱即用，无需配置，因而简化了 IT 部门的实施工作。

表 1. 英特尔® vPro® 平台的大部分安全功能已实现，无需配置

英特尔® vPro® 安全技术	开箱即用
英特尔® 硬件盾	✓
英特尔® 控制流强制技术（英特尔® CET）	✓
英特尔® 威胁检测技术（英特尔® TDT）	✓

英特尔® 硬件盾

英特尔® 硬件盾是一套有助于保护整个计算堆栈的技术。与安全软件不同，英特尔® 硬件盾提供操作系统之下的安全功能，可抵御固件和硬件层面的攻击。英特尔® 硬件盾还通过硬件加速的虚拟化加密技术提供应用和数据保护功能，通过高级威胁检测和保护技术保持出色性能。

操作系统之下的安全性为何重要？

操作系统之下的安全功能有助于识别未经授权篡改硬件和固件的行为，通过统一可扩展固件接口 (UEFI) 保护和可视性防止恶意代码注入。OEM 在其配备在操作系统之下的安全包中采用了英特尔® vPro® 的多项功能。

英特尔® 硬件盾

操作系统之下的安全
由 BIOS 和启动流保护技术提供

- 英特尔® BIOS Guard
- 英特尔® Boot Guard
- 英特尔® Firmware Guard
- 英特尔® Firmware 更新/恢复
- 英特尔® 平台可信技术（Intel® Platform Trust Technology 英特尔® PTT）
- 英特尔® Runtime BIOS Resilience
- 英特尔® System Resources Defense
- 英特尔® 可信执行技术（Intel® Trusted Execution Technology，英特尔® TXT）
- 英特尔® System Security Report
- 英特尔® Tunable Replica Circuit—Fault Injection Detection

图 1. 英特尔® 硬件盾内置于英特尔® vPro® 平台中，有助于全面保护 PC，包括保护操作系统之下的层面

英特尔® 威胁检测技术（英特尔® TDT）

英特尔® TDT 通过基于硬件的监控功能来检测和预防恶意操作行为，从而帮助防止勒索软件攻击、挖矿劫持攻击甚至是内存扫描攻击。

英特尔® TDT 是一套利用硬件遥测和加速功能的技术。这项技术可以收集和分析原始数据，以帮助实时识别多态恶意软件、挖矿劫持攻击、无文件脚本和其他有针对性的攻击，并尽可能降低对终端用户的影响。

英特尔® TDT 采用机器学习（ML）启发式方法来减少误报警报，同时也有助于提高 Microsoft Defender for Endpoint、CrowdStrike 和 Fidelis 等能够持续监控端点设备的端点检测和响应（EDR）解决方案的性能。为实现这一点，英特尔® TDT 将内存扫描功能从 CPU 卸载到辅助图形处理单元（GPU），从而减少安全软件解决方案的资源占用率，并提供更好的员工整体用户体验。

与 CPU 相比，使用 EDR 解决方案时内存扫描性能可提升 4 到 7 倍，能够在需要时支持更广泛的内存扫描 [3]。CrowdStrike 近期在面向 Windows 系统的 CrowdStrike Falcon 传感器中引入了英特尔® TDT 加速的内存扫描，以提高可见性并检测内存威胁 [4]，从而针对无文件威胁再增一层保护。2022 年，在所有检测到的攻击中，无文件威胁占 71%[5]。

英特尔® TDT 与 EDR 解决方案结合，能够检测出高达 97% 的已知和未知攻击 [6]。

英特尔® 控制流强制技术（英特尔® CET）

英特尔® CET 是一种先进的缓解技术，有助于防范返回导向编程、跳转导向编程和调用导向编程 (ROP/JOP/COP) 攻击。这些攻击利用内存安全漏洞，常见于浏览器和会议工具等联网应用中。

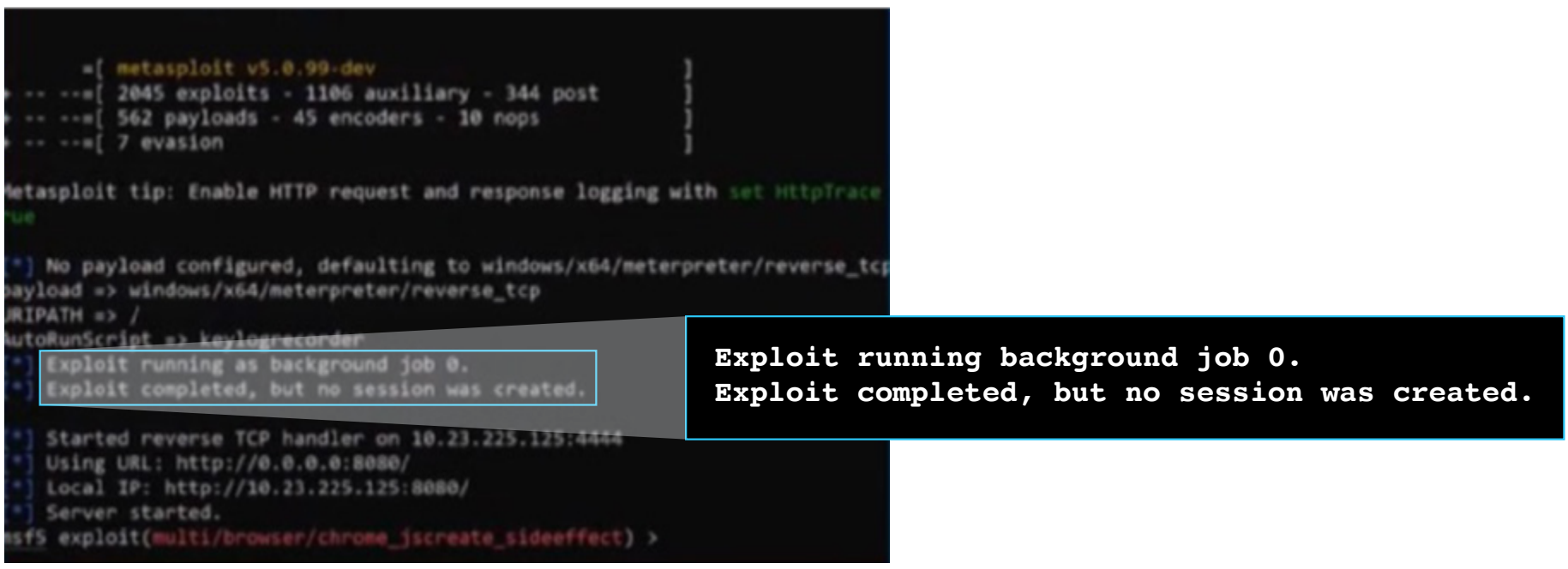

图 2. 英特尔® CET 可缓解难以检测但易于执行的攻击，如通过点击浏览器链接执行的攻击

攻击者可以利用运行在可执行内存上的现有代码片段来修改系统组件。这些攻击尤其令人担忧，因为它们难以检测，长期以来一直无法被纯软件安全解决方案发现。

英特尔® CET 是对软件安全功能的补充，可应对 ROP/JOP/COP 攻击，并提供更高级别的安全防护[7]。据一份报告称，英特尔® CET 的实现被认为是“朝着消除运用 ROP 及其他控制流劫持技术迈出的重要一步”[7]。目前，微软已在 Windows 操作系统中采用了英特尔® CET，Windows 10 的 20H1 及更高版本中皆有配备。这项技术当前还在进一步开发中，将支持 Linux 内核。同时，它也支持 Google Chrome 及相关浏览器的安全关键型浏览器进程[7]。

英特尔® 虚拟化技术（英特尔® VT）

远程办公推动了基于虚拟化的安全技术（VBS）的兴起。IT 团队可以使用 Windows 10 和 11 的可用策略启用英特尔® vPro® 安全功能。英特尔® VT 现已用于配备英特尔® vPro® 平台的 PC，使其能够支持活动分区、工作负载隔离、嵌入式管理、传统软件迁移和灾难恢复等用途。通过虚拟化，企业可在一台服务器各独立分区中运行多个操作系统和应用，从而隔离工作负载，减少恶意软件轻易传播的机会。隔离功能对于混合办公尤为重要，因为员工可能会将 PC 用于满足办公和个人需求。

图 3. 英特尔® vPro® 平台上的英特尔® VT 支持工作负载隔离，通过支持创建隔离的虚拟机（VM）减少受攻击面，降低恶意软件在资源间持续传播的能力

英特尔® 全内存加密-多密钥（英特尔® TME-MK）

英特尔® TME-MK 对 DRAM 中系统内存各部分（包括操作系统和应用数据）进行加密，帮助防御物理冷启动攻击。英特尔® TME-MK 允许虚拟容器/虚拟机使用多个密钥对不同的内存区域进行加密，藉此通过隔离数据来增强安全性。

英特尔® Wi-Fi 近距离感应技术

英特尔® Wi-Fi 近距离感应技术有助于简化远程办公人员在公共场所或共享办公空间工作时的安全防护工作。这项技术利用无线信号检测附近区域的环境变化。当用户离开笔记本电脑时，这项技术会感应到他们的移动并自动锁定设备。当用户回来开始办公时，它又会“唤醒”PC，准备投入使用。

英特尔® Wi-Fi 近距离感应技术可智能感知何时锁定或唤醒用户的笔记本电脑

离开即锁定[8]

Wi-Fi 能感应到用户离开
并在数秒内锁定 PC

安全防护

用户忘记锁定 PC → 人体存在检测 → 自动锁定 PC

靠近即唤醒[8]

Wi-Fi 感应到用户返回
并在数秒内唤醒 PC

便捷轻松

检测到人体存在 → 自动唤醒 PC → 显示登录界面

英特尔® 远程安全擦除（英特尔® RSE）

当 PC 退出使用、重复利用、返回维修或丢失时，信息安全策略通常会要求从硬盘上“擦除”数据。现场操作时，擦除可能就很困难并且耗时，远程操作时更是几乎无法实现。英特尔® RSE 提供了一种远程安全擦除硬盘的方法，可通过英特尔® 主动管理技术（Intel® Active Management Technology，英特尔® AMT）实现[9]。

采取零信任措施，支持员工随时随地办公

英特尔® vPro® 平台的综合安全措施可以通过多种硬件攻击应对措施帮助减少 PC 的受攻击面。英特尔® vPro® 通过采取零信任的安全原则支持远程工作，确保用户均经过身份验证，并评估每台设备的健康状况和对应用的访问。

研究证实了英特尔® vPro® 强化安全功能的有效性。员工人数超过 5,000 人且主要采用基于英特尔® vPro® 平台的设备的企业和机构，与未采用英特尔® vPro® 的企业和机构相比，平均每年报告的安全漏洞事件更少[10]。

- 未采用英特尔® 技术的企业和机构平均每年报告的重大安全漏洞事件为 3.9 起，而采用英特尔® 技术的企业和机构每年报告的重大安全漏洞事件为 2.8 起[11]。
- 使用英特尔® 技术的企业和机构因外部攻击、内部事件、涉及第三方供应商的攻击或事故以及资产丢失或被盗而遭受破坏的可能性更小[12]。
- 92% 的受访 IT 专业人士表示，基于英特尔® vPro® 实施标准化管理后，自身笔记本电脑和台式机的安全性明显增强[2]。
- 全面使用英特尔® vPro® 的所有硬件安全功能，可将受攻击面减少多达 70%[7]。

增强安全防护，提升性能表现

基于英特尔® vPro® 平台的设备专为远程办公和安全工作负载而设计。英特尔® vPro® 代代升级，始终专注于安全创新，致力于帮助企业防范于未然，免受不法分子侵害。英特尔® vPro® 技术自推出起便提供了出色的操作系统之下的安全性，如今已演进到基于第 13 代英特尔® 酷睿™ 处理器的英特尔® vPro® 平台，它有助于提高操作系统之上的安全性，帮助企业避免出现安全漏洞，并为 IT 节省宝贵时间。

英特尔® vPro® 通过优化通常位于企业防火墙后的技术和安全功能，为企业提供更全面的安全防护 [13]。

在真实商用计算场景下提升员工的用户体验和安全性

进一步了解基于英特尔® vPro® 的全新 PC 及其为您的员工和企业带来的显著安全优势。

[1] 英特尔® 标准可管理性 (Intel® Standard Manageability) 和英特尔® 主动管理技术（Intel® Active Management Technology，英特尔® AMT）均支持在预配 Windows 的 PC 上执行远程带外管理功能，但只有面向 Windows 的英特尔® vPro® Enterprise 才能借助英特尔® AMT 支持远程 KVM（键盘、显示器、鼠标）控制。

[2] 基于对全球使用英特尔® vPro® 平台的美国、英国、德国、日本和中国企业的 416 名 IT 决策者进行的调查。92% 的受访者表示“同意”或“非常同意”。结果可能不同。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，2021 年 1 月。https://www.intel.cn/content/www/cn/zh/business/enterprise-computers/resources/vpro-platform-tei-case-study-2021.html。

[3] 基于 CrowdStrike 博客中所述的与 CPU 内存扫描方法在速度上的比较，通过英特尔® TDT API 将内存扫描卸载到集成 GPU，速度提高了 4–7 倍。详情请见 https://edc.intel.com/content/www/cn/zh/products/performance/benchmarks/intel-vpro/。

[4] CrowdStrike，“CrowdStrike Falcon® Enhances Fileless Attack Detection with Intel Accelerated Memory Scanning Feature（CrowdStrike Falcon® 利用英特尔® 加速内存扫描功能增强无文件攻击检测能力）”，2022 年 3 月。crowdstrike.com/blog/falcon-enhances-fileless-attack-detection-with-accelerated-memory-scanning/。

[5] CrowdStrike，“2023 Global Threat Report（2023 年全球威胁报告）”，2023。https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf。

[6] SE Labs，“Enterprise Advanced Security (Ransomware): Intel [企业高级安全防护（勒索软件）：英特尔]”，2023 年 2 月。https://selabs.uk/reports/enterprise-advanced-security-ransomware-intel-threat-detection-technology-2023-02/。

[7] IOActive，“13th Generation Intel Core Attack Surface Study（第 13 代英特尔® 酷睿™ 受攻击面研究）”，受英特尔委托，2023 年 3 月。https://www.intel.cn/content/dam/www/central-libraries/us/en/documents/2023-03/ioactive-intel-13th-generation-attack-surface-study-summary-report.pdf。

[8] Windows 11 支持“离开即锁定”和“靠近即唤醒”。英特尔® Wi-Fi 近距离感应技术目前仅适用于 Windows PC 上符合条件的英特尔 Evo 和英特尔® vPro® 设计。

[9] 请咨询您的 OEM，确保您的设备支持英特尔® RSE。

[10] Forrester Consulting，“The Total Economic Impact™ Of Intel vPro® Hardware-Enabled Security Features（英特尔® vPro® 基于硬件的安全功能的总体经济影响™）”，受英特尔委托，2022 年 9 月。https://www.intel.cn/content/www/cn/zh/business/enterprise-computers/resources/impact-of-vpro-hardware-enabled-security-paper.html。

[11] 基于全球 719 位负责端点管理的 IT 决策者 (ITDM) 对“过去一年中，您的企业或机构使用基于 [处理器] 的 [设备] 发生了多少起安全漏洞事件？”这个问题的回答。来源：Forrester Consulting 受英特尔委托进行的研究，2021 年。

[12] 基于全球 239 名负责端点管理的 IT 决策者对“您之前表示您所在的企业或机构在过去 12 个月内曾发生过安全漏洞事件。请问安全漏洞事件是如何发生的？”这个问题的回答。来源：Forrester Consulting 受英特尔委托进行的研究，2022 年 9 月。

[13] 截至 2023 年 3 月，根据英特尔® vPro® 为各种规模的企业提供的操作系统之上和之下的安全功能、应用和数据保护、先进的威胁防护组合，以及英特尔安全为先的产品设计、制造和技术支持来衡量。所有基于英特尔® vPro® 平台构建的商用 PC 均已根据严格的规范进行验证，包括那些独特的基于硬件的安全功能。详情请见 https://edc.intel.com/content/www/cn/zh/products/performance/benchmarks/intel-vpro/。结果可能不同。

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。

英特尔技术可能需要启用硬件、软件或激活服务。

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。

英特尔并不控制或审计第三方数据。请您审查该内容，咨询其他来源，并确认提及数据是否准确。

0823/RR/PRW/PDF 请回收利用