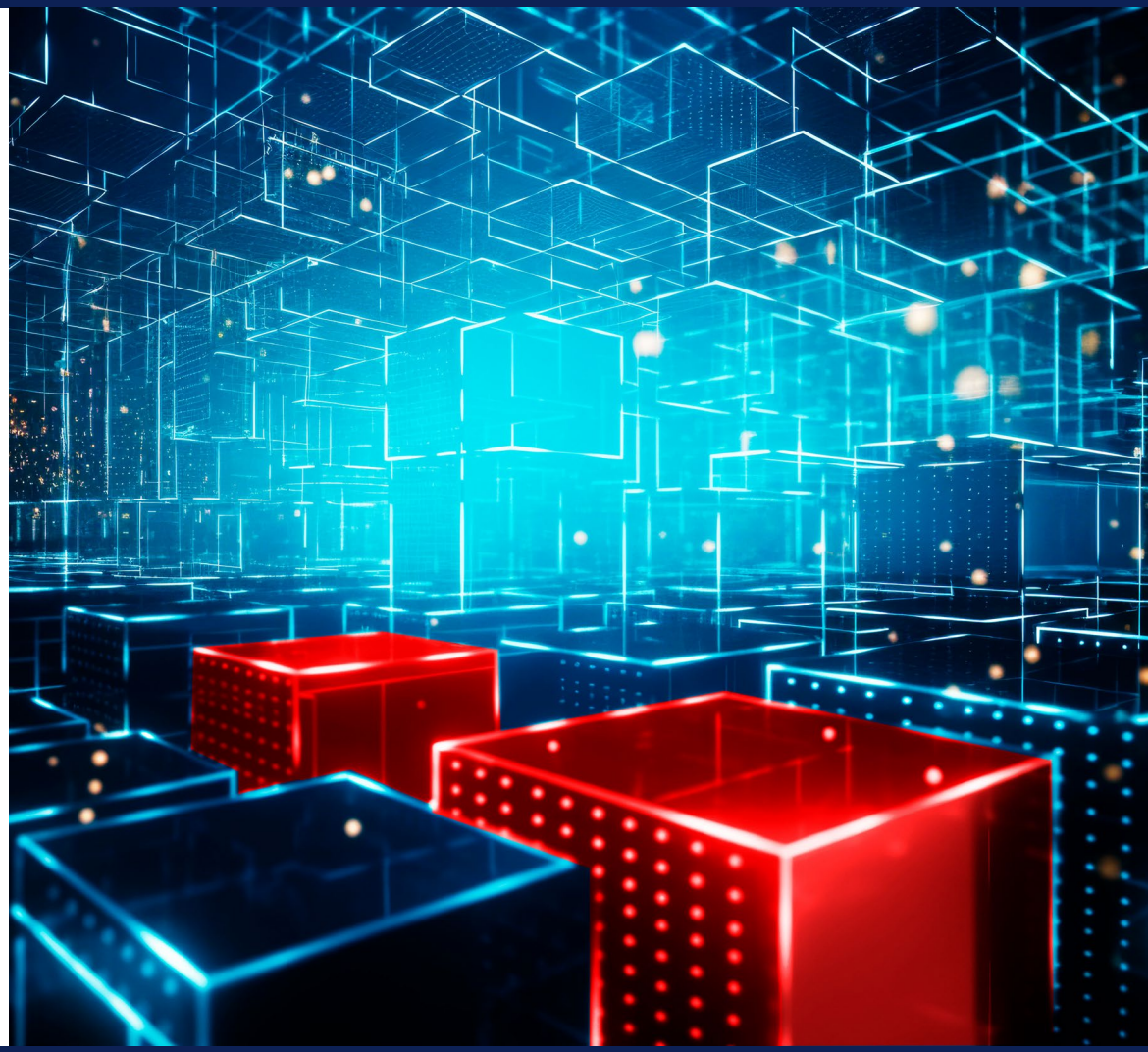
如何在端点保护 AI 的使用

通过安全的现代化设备和对抗性思维，防御设备端 AI 工作负载。



执行摘要

设备端 AI 虽优势显著，但也伴随着网络风险。在本电子书中，我们将逐步指导您如何让组织安全地在端点部署 AI 创新技术。

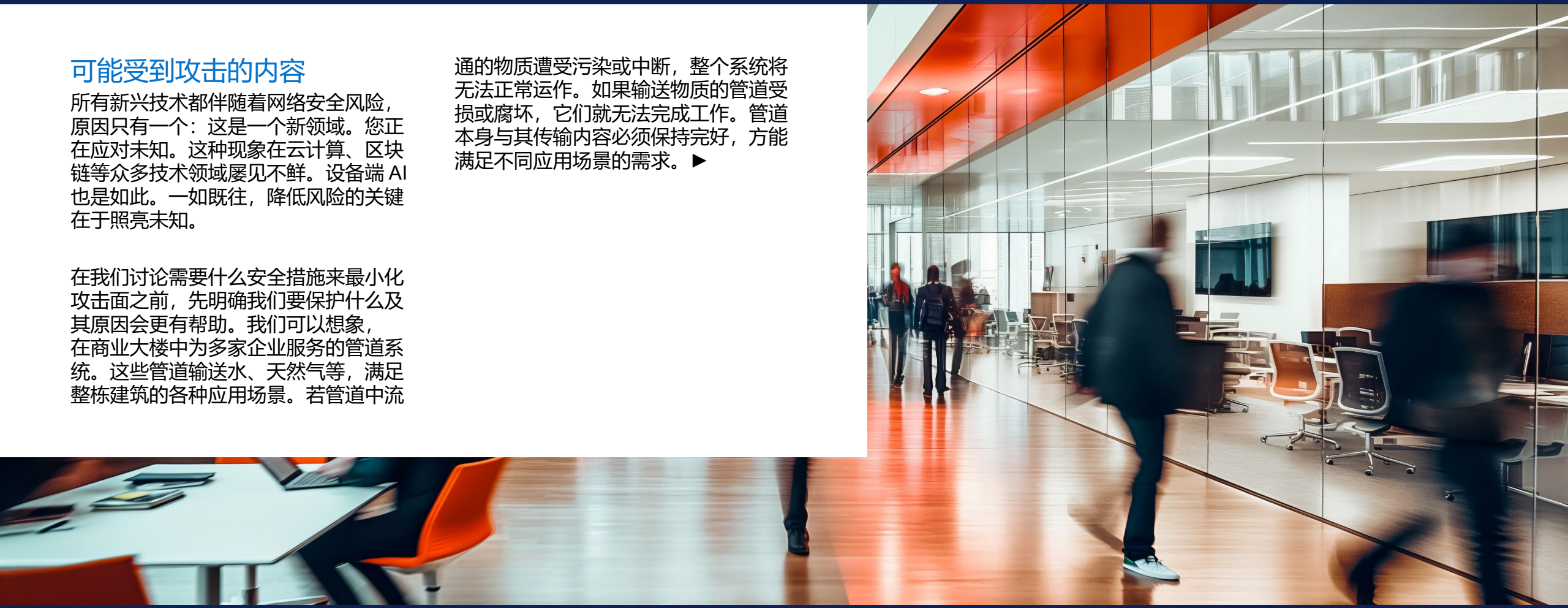
目录

设备端 AI 的攻击面

可能受到攻击的内容

所有新兴技术都伴随着网络安全风险，原因只有一个：这是一个新领域。您正在应对未知。这种现象在云计算、区块链等众多技术领域屡见不鲜。设备端 AI 也是如此。一如既往，降低风险的关键在于照亮未知。

在我们讨论需要什么安全措施来最小化攻击面之前，先明确我们要保护什么及其原因会更有帮助。我们可以想象，在商业大楼中为多家企业服务的管道系统。这些管道输送水、天然气等，满足整栋建筑的各种应用场景。若管道中流通的物质遭受污染或中断，整个系统将无法正常运作。如果输送物质的管道受损或腐坏，它们就无法完成工作。管道本身与其传输内容必须保持完好，方能满足不同应用场景的需求。►



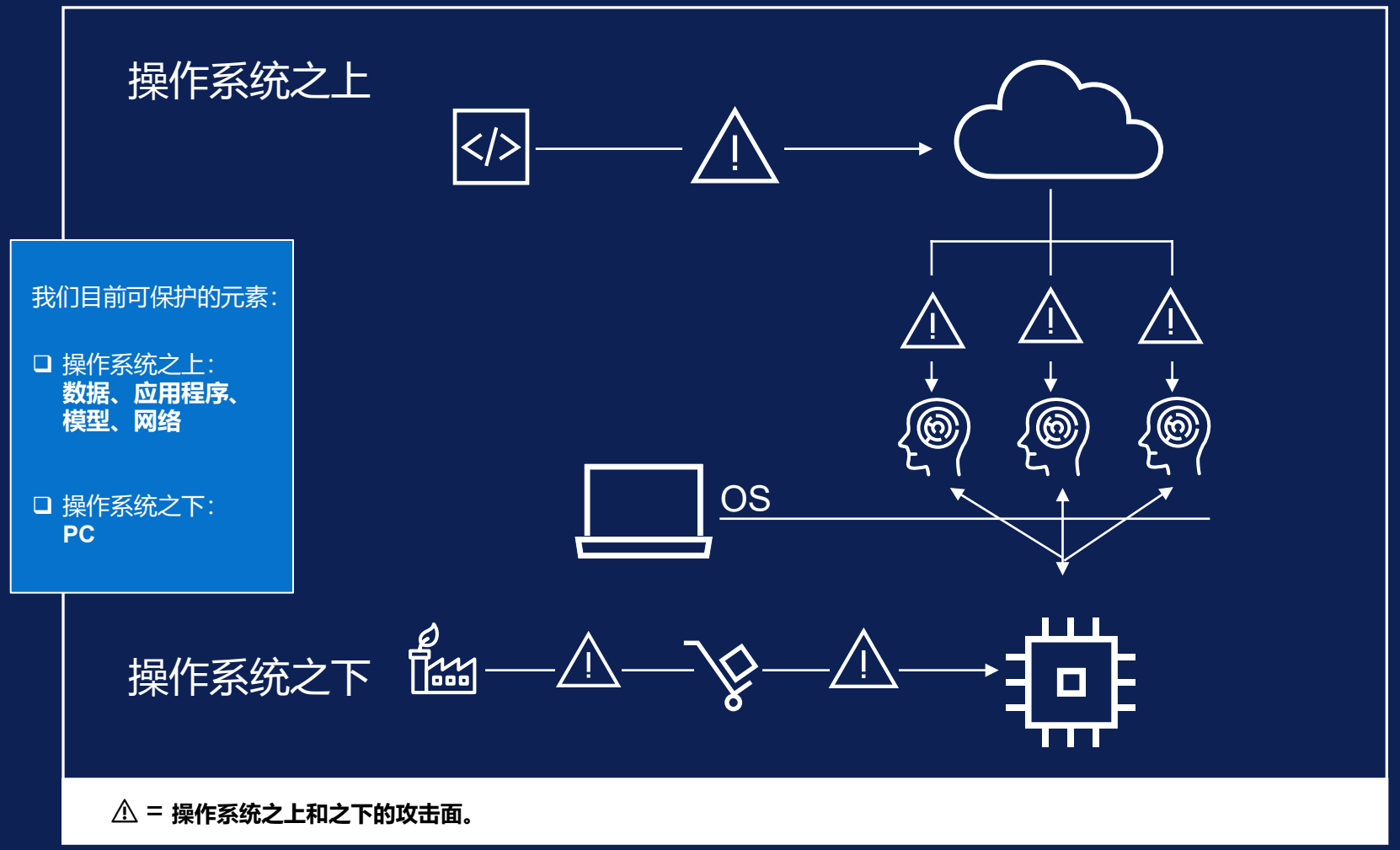
设备端 AI 的攻击面（续）

可能受到攻击的内容（续）

回归到端点的 AI 安全性这个核心议题：

- 管道就是您的基础架构 — 包括您的 PC、您的公司网络、工作方式与场所。
- 流经管道的内容是数据、应用程序和模型，它们驱动各种 AI 应用场景。完成工作所需的资产和资源。

正如您所料，网络对手都以两者为目标。他们可能窃取知识产权，以勒索或污染数据/模型，进而影响运营。一旦失守，后果都可能非常严重，导致财务损失、声誉损害和/或触发监管审查。 ►



端点的安全风险

攻击者用来寻得入口的战术

今天我们将讨论攻击者可能采用哪些方法来访问这两个目标。

设备入侵。从 Forrester Research, Inc. 在 2025 年 3 月发布的“端点安全市场洞察”中可以看出，PC 是现代网络威胁的主要目标之一。这种类型的攻击可能会在设备端 AI 启动前发生，即**硬件或软件供应链攻击。**供应链中存在数十个（甚至数百个）节点，在这些节点上恶意攻击者可能会篡改组件（例如，电路、固件），以植入可被日后利用的弱点。想象一下，一家投资公司收到一批带有伪造组件的新 PC 时将发生的灾难性后果。

身份入侵。凭据被盗或泄露的违规事件是增长最快的攻击媒介之一。这并不奇怪。（攻击者）使用有效凭据登录 PC 后，不仅能在企业网络内自由活动，还可长期隐匿行踪。依据 IBM 最新发布的数据泄露成本报告，这些泄露事件平均需要 292 天来识别和遏制，这在所有攻击途径中耗时最长。威胁行为者绝不会忽视如此高价值的访问权限。事实上，来自 Zscaler 的研究显示，恶意攻击者正在升级凭据窃取手段，利用生成式 AI 来改进和扩大网络钓鱼攻击规模。这种被应用于敏感训练数据、推理数据或直接应用于模型的未授权访问，被归类为**模型供应链攻击。**

内部威胁。最新研究表明，与其他攻击媒介相比，**恶意内部攻击**造成的成本最高，平均为 499 万美元。需要注意的是，内部攻击可能发生在硬件供应链、软件供应链和模型供应链中。►

终端用户遭遇**网络钓鱼**电子邮件的平均反应时间：不到 60 秒*

发现和遏制**凭据入侵事件**的平均时间为 292 天**

恶意内部攻击平均造成 499 万美元损失**

** 来源：Verizon DBIR，2024 年*
***来源：IBM 发布的《Cost of a Data Breach, 2024》*

制定应对措施

降低风险的方法

这些攻击目标本质上都不是新出现的。攻击者的终极目标并非单一层面。一如既往，我们希望专注于确保您的机群保持安全且具备弹性。**分层部署应对措施**有助于减少攻击面，并立即揭示任何可疑行为。

零信任思维可有效降低机群的整体风险。从不信任、始终验证和持续监控 — 这些原则可以帮助您保持领先于攻击者。须知：100% 阻断所有攻击并不可行。要获得强大的安全态势，您需要在整个 IT 生态系统中获得全面**可见性和控制力**。

基于此框架，建议重新评估基础架构，尤其是与 AI 交互的系统和流程。哪些应对措施可更大限度地降低设备入侵、身份入侵和内部威胁的风险？►

以下这些零信任原则有助于抵御风险并缩小网络活动的波及范围

- 假设最坏的情况
- 不授予任何隐式信任
- 持续进行身份验证

制定应对措施（续）

降低风险的方法（续）

总体而言，存在两大应对措施类别。

“操作系统之下”的安全性可保护您使用的 AI 设备。我们可以从两个层面构建防护体系：

- 通过**安全构建**的设备保护您的机群。这意味着使用设计安全的 AI PC，也就是说，它们采用安全的设计原则并在安全的供应链中进行开发。
- **内置安全性**的设备可保护您的机群。安全的 AI PC 包括嵌入式保护层，提供从 BIOS 到芯片层的可见性，且开箱即用。

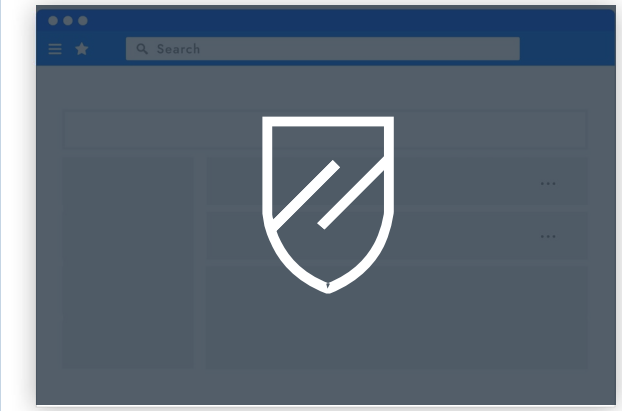
“操作系统之上”的安全性可保护对 AI 模型的访问。通过**软件安全性**保护您*使用的*数据和模型以及您*使用的*公司网络。保护机器学习安全运行并监视已部署 AI 工作负载的网络流量至关重要。►

操作系统之下的安全性

安全的 AI PC

硬件和固件安全性、供应链安全性、核心芯片

操作系统之上的安全性



软件安全性

端点、网络和云环境的额外安全层

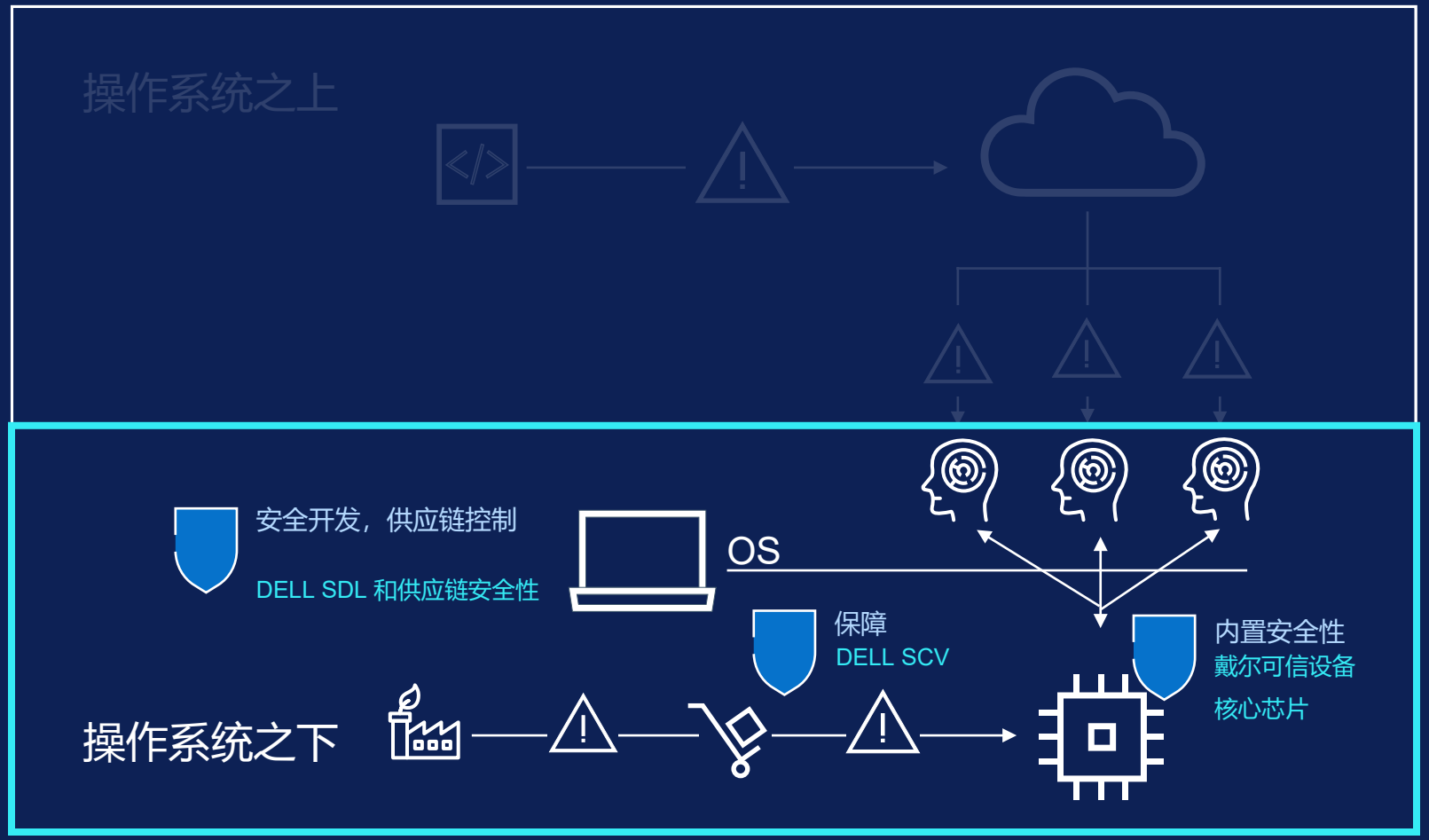
可整合所有要素的安全服务与专业知识。

将最佳实践应用于您的机群

戴尔 AI PC 如何为您的机群带来基础安全性

这正是 Dell Trusted Workspace 的用武之地。为了确保商用 AI PC 的安全性，我们的技术人员深刻理解了对抗性思维，并设计了相应的安全措施。

在操作系统之下，安全设计、强大的供应链控制和可选的供应链保障有助于确保 PC 从首次启动开始就安全无虞。通过内置的硬件与固件安全性，确保设备在使用过程中持续受保护，例如：戴尔独有的* BIOS 级篡改检测 (Dell SafeBIOS) 和无密码凭据安全性 (Dell SafeID)，有效防御未授权访问。此外，英特尔® 芯片技术为 AI PC 客户端提供了保护 AI 各应用环节的基础支撑。例如，通过支持磁盘模型加密加速，英特尔可帮助客户端实现静态 AI 数据的安全防护。►



将最佳实践应用于您的机群（续）

戴尔 AI PC 如何为您的机群带来基础安全性（续）

为强化操作系统之下的安全性，我们的合作伙伴 Absolute 的持久化技术可嵌入出厂系统中，从而在整个 PC 生命周期内提供更强大的可视性与控制力。例如：对运输中的设备实现地理位置追踪，以及在极端情况下实现关键应用程序的自修复功能。

实际上，戴尔已构建了一个软件合作伙伴解决方案生态系统（包括 CrowdStrike Falcon XDR 和 Absolute Secure Access），这些方案通过实施零信任原则，保护您的模型供应链免受**操作系统之上**未授权访问的威胁。应用这些解决方案时，您可通过以下方式创建并执行安全策略：实施精细访问控制（如基于角色的访问控制/RBAC），以有效降低恶意内部人员访问或篡改 AI 模型的风险。►

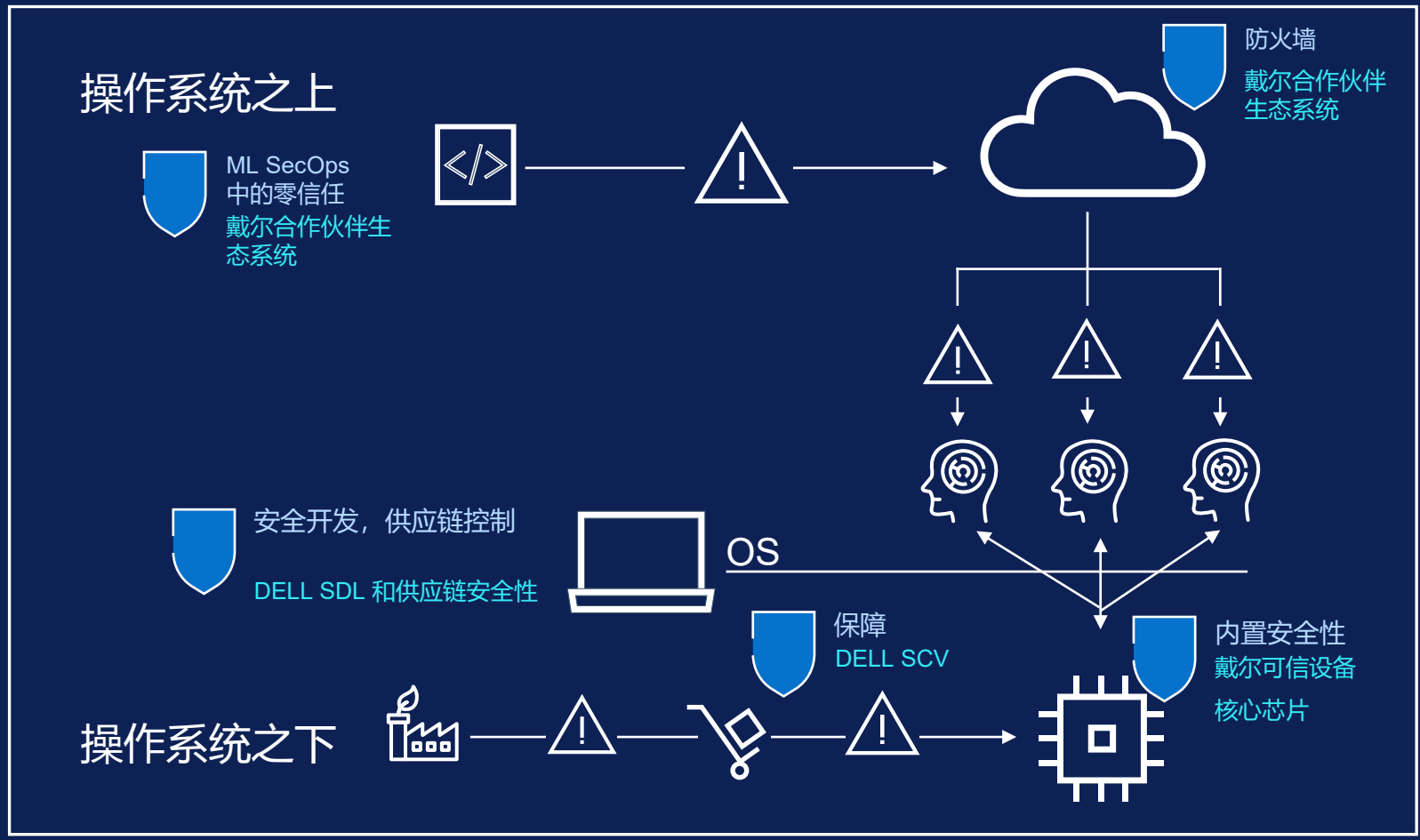
将最佳实践应用于您的机群（续）

戴尔 AI PC 如何为您的机群带来基础安全性（续）

这一切构筑了 ***AI 时代的安全保护***。这些功能可保护设备端 AI 工作负载免受网络攻击，让您能够专注于创新和赢得商机。 ►

以软硬件协同防御，阻击高级终端攻击

戴尔携手英特尔和 CrowdStrike，通过硬件辅助安全技术实现操作系统之下与之上的无缝集成防护。
了解详情 >



学习要点和后续步骤

携手戴尔，在端点保护 AI

根据 Absolute 公司最近对 CISO 的一项调查显示，企业对 AI 充满热情，但在 AI 技术准备度方面却进展滞后。对数百万台设备进行的分析表明，大量 PC 设备难以全面承载新型 AI 功能。**戴尔可以帮助整合这一切。**

依托安全的现代化基础，开发和部署 AI 模型。Windows 10 支持将于 2025 年 10 月终止。届时，PC 将不会再收到安全更新、功能更新和 Windows 10 支持。旧设备可能无法满足 Windows 11 的要求，并且可能缺乏最新的内置性能、安全性以及 AI 增强功能。升级到 **Dell Pro** 或 **Dell Pro Max — 搭载英特尔® 酷睿™ Ultra 处理器和英特尔® vPro®** — 凭借这些**安全可靠的商用 AI PC，解锁安全优势并防御 AI 工作负载。***►

Windows 10 支持将于 10 月终止。

升级到搭载英特尔的全新戴尔 AI PC，以释放安全优势和 AI 增强功能：

选购 Dell Pro ● Dell Pro Max

*安全可靠的商用 AI PC**

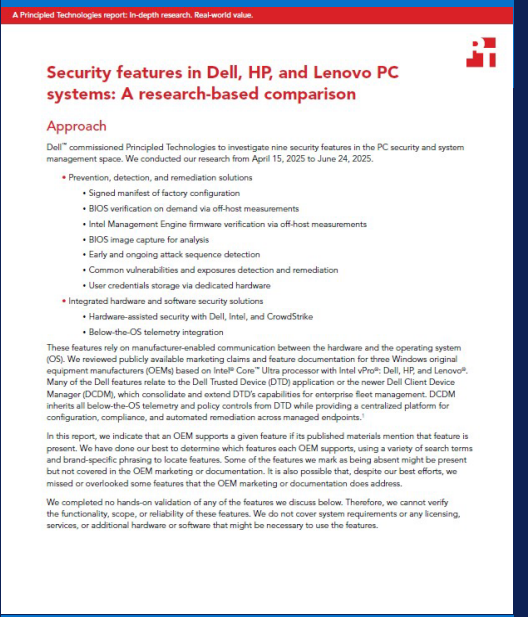
探索增值软件和服务，以改善您的安全态势：

软件和集成

服务

行业优势地位

Principled Technologies 发现，戴尔和英特尔商用 AI PC 级安全性优于同类产品


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

Security features in Dell, HP, and Lenovo PC systems: A research-based comparison

Approach

Dell™ commissioned Principled Technologies to investigate nine security features in the PC security and system management space. We conducted our research from April 15, 2025 to June 24, 2025.

- Prevention, detection, and remediation solutions
  - Signed manifest of factory configuration
  - BIOS verification on demand via off-host measurements
  - Intel Management Engine firmware verification via off-host measurements
  - BIOS image capture for analysis
  - Early and ongoing attack sequence detection
  - Common vulnerabilities and exposures detection and remediation
  - User credentials storage via dedicated hardware
- Integrated hardware and software security solutions
  - Hardware-assisted security with Dell, Intel, and CrowdStrike
  - Below-the-OS telemetry integration

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 equipment manufacturers (OEMs) based on Intel® Core™ Ultra processor with Intel vPro®: Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device (DTD) application or the newer Dell Client Device Manager (DCDM), which consolidate and extend DTD's capabilities for enterprise fleet management. DCDM inherits all below-the-OS telemetry and policy controls from DTD while providing a centralized platform for configuration, compliance, and automated remediation across managed endpoints.[1]

In this report, we indicate that an OEM supports a given feature if its published materials mention that feature is present. We have done our best to determine which features each OEM supports, using a variety of search terms and brand-specific phrasing to locate features. Some of the features we mark as being absent might be present but not covered in the OEM marketing or documentation. It is also possible that, despite our best efforts, we missed or overlooked some features that the OEM marketing or documentation does address.

We completed no hands-on validation of any of the features we discuss below. Therefore, we cannot verify the functionality, scope, or reliability of these features. We do not cover system requirements or any licensing, services, or additional hardware or software that might be necessary to use the features.

阅读调查报告

免责声明

* 基于 Principled Technologies 开展的第三方分析，该分析对比了搭载英特尔处理器的戴尔商用 AI PC 与其他同类产品的表现，2025 年 7 月。基于戴尔在 2024 年 10 月对全球 PC 市场进行的内部分析。适用于搭载英特尔处理器的 PC。并非所有 PC 都提供所有功能。某些功能需要额外购买。

要了解更多信息，请：

联系我们： Global.Security.Sales@Dell.com

访问我们的网站： Dell.com/Endpoint-Security

关注我们： LinkedIn @DellTechnologies | X @DellTech

关于 Dell Endpoint Security

对于各种规模的组织来说，安全都是一个令人生畏的话题。**与经验丰富的安全和技术合作伙伴合作，实现端点安全保护现代化。**

Dell Trusted Workspace 可帮助您保护端点，打造零信任就绪型现代 IT 环境。借助戴尔特有的全面硬件和软件保护产品组合，减小受攻击面并提升网络弹性。我们高度协调、以防御为基础的方法，通过将内置的保护与持续的警戒功能相结合来抵御威胁。专为当今基于云的环境而构建的安全解决方案可以让终端用户高效工作，让 IT 充满信心。