DELL Technologies

如何通过集成端点安全与可管理性

来应对现代网络威胁

CROWDSTRIKE intel ABSOLUTE®

执行摘要

新兴攻击途径正带来新的风险。结合使用多层防御手段，预先防范现代端点威胁。了解如何将硬件遥测与软件集成，以提高整个机群的安全性和可管理性。借助易于管理的设备和解决方案，更快地中断攻击、推行零信任原则并安全地进行创新。

目录

威胁环境

挑战

解决方案

应用场景和应对措施

要点及行动呼吁

威胁环境

案例分析

2023 年，Eclypsium 发现中国台湾地区的一家制造商销售的主板固件存在缺陷。该代码原本只是用于保持固件更新，然而研究人员发现其实现存在安全隐患，可能被劫持并用于安装恶意软件。

这一发现尤其令人警醒，原因有以下几点

- 客户会因固件漏洞而面临风险。
- 该漏洞存在于设备中一个通常难以检测到威胁的区域。
- 此漏洞可用于发起可绕过凭证验证的远程攻击。

摘自头条新闻...

威胁环境

启示

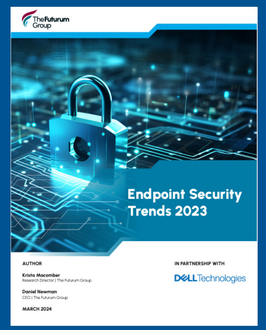
这正是导致 IT 和安全团队夜不能寐的关键因素之一：

基于设备的攻击。

这些复杂的恶意攻击可能使攻击者获得高级访问权限。很多攻击甚至可以在用户毫无察觉的情况下绕过传统的纯软件防护措施，比如防病毒软件。

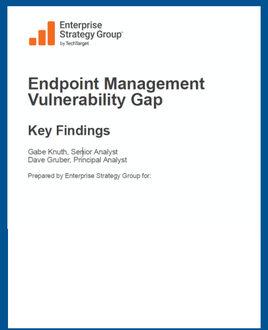
根据最近对 IT 和安全专业人员开展的一项全球调查[1]，组织在采购新硬件时，主要的评估标准包括：

自动检测 BIOS 固件事件



69% 的组织表示，在过去 12 个月内至少遭受了一次对其设备的攻击。这一比例相比 2020 年的调查增长了 1.5 倍！[2]

高风险配置



超过 75% 的组织表示，他们至少经历过一次因未知、非托管或管理不善的端点设备引发的网络攻击。[3]

挑战

那么，设备容易成为目标的原因是什么？

可见性

攻击者在通常难以监控的设备区域发起这些攻击，用户很难察觉。

可操作性

许多组织往往都会部署几十种各自独立运行的工具。因此，一旦检测到攻击，快速响应和修复将成为一大挑战，并且需要大量的手动操作。

解决方案

可见性

可操作性

作为全球主要的技术提供商之一，戴尔非常重视安全性。因此，**我们打造了出色的商用 PC，从一开始就很注重实现可见性和可操作性。**这就让 IT 和安全运营部门掌握了话语权。

我们的商用 PC 具有**独特的内置安全功能**，例如 BIOS 验证[4] 和攻击指标[4]，可助您预先检测威胁，以免造成损害。我们利用**戴尔独有的设备遥测技术**[4]，将这些检测结果清晰呈现。戴尔商用 PC 搭载英特尔 vPro® 技术，在设备层面检测到潜在威胁时，可将该信息发送给操作系统，以便更快速、更有效地进行调查和响应

业内领袖

戴尔提供了安全性出众的商用 PC[4]

了解如何维护设备信任以抵御现代威胁。

阅读 Principled Technologies 关于设备安全的研究报告 →


Principled Technologies®

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 equipment manufacturers (OEMs): Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device application.

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.

解决方案

安全性和可管理性相辅相成，助力应对各种威胁

戴尔拥有互联的合作伙伴生态系统，携手合作伙伴强强联手，致力于实现工作区的可见性和可操作性。其中包括：

- 戴尔助力实现供应链安全性并提供内置的硬件和固件防御功能
- 英特尔提供核心芯片和“操作系统之下”的保护
- 通过戴尔，使用统一端点管理控制台实现可管理性
- 由合作伙伴（包括 CrowdStrike 和 Absolute）提供的涵盖端点、网络和云的高级威胁防护

该生态系统使用 PC 遥测技术作为连接纽带，帮助缩小 IT 与安全解决方案之间的差距，以免威胁逃过检测。这种方法不仅有助于防范攻击，还可帮助您进行检测、响应、恢复和修正。

应用场景和应对措施

为了展示集成式安全性和可管理性如何助力提升网络弹性，我们将介绍两个应用场景，其中包括攻击场景和应对措施。

首先是对 BIOS 固件发起的攻击。在这里，我们将了解 BIOS 降级攻击的网络杀伤链[5] 是如何形成的。

BIOS 降级攻击

初始访问：通过可移动介质进行复制 + 网络钓鱼

步骤 1a

恶意内部人员利用现有 BIOS 漏洞远程窃取操作系统凭据。设备遭到黑客攻击，BIOS 降级。

步骤 1b

攻击者会发起鱼叉式网络钓鱼攻击，当管理员错误地在恶意站点上进行身份验证时，攻击者将窃取会话令牌。

步骤 2

凭据访问

攻击者创建额外的管理员账户以实现持久访问，并继续在网络上移动。

步骤 3

横向移动

攻击者映射网络，并找到系统管理服务器。

步骤 4

泄露

攻击者通过 Web 服务将数据外泄。

应用场景和应对措施

BIOS 降级应对措施

攻击者能够比以往更快地入侵网络。事实上，根据 CrowdStrike’ s Global Threat Report，在 2023 年，电子犯罪的平均突破时间（成功入侵系统并横向移动所需的时间）从 2022 年的 84 分钟缩短到了 62 分钟。观察到的最快突破时间仅为 2 分 7 秒！[6]

如需了解戴尔与其合作伙伴英特尔® 和 CrowdStrike 如何通过硬件辅助的安全防护，全程识别并抵御 BIOS 降级攻击，请参阅：

应用场景和应对措施

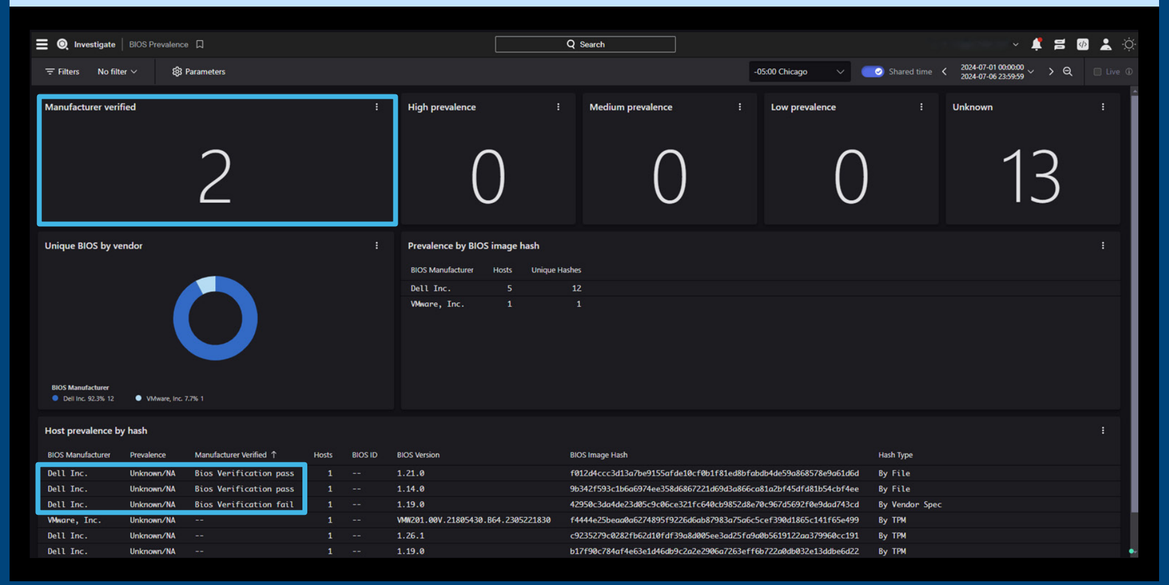
BIOS 降级应对措施

攻击者能够比以往更快地入侵网络。事实上，根据 CrowdStrike’ s Global Threat Report，在 2023 年，电子犯罪的平均突破时间（成功入侵系统并横向移动所需的时间）从 2022 年的 84 分钟缩短到了 62 分钟。观察到的最快突破时间仅为 2 分 7 秒！[6]

如需了解戴尔与其合作伙伴英特尔® 和 CrowdStrike 如何通过硬件辅助的安全防护，全程识别并抵御 BIOS 降级攻击，请参阅：

防范 | **检测和响应** | 恢复和修正

在 CrowdStrike Falcon 平台上检测 BIOS 认证：启用戴尔设备遥测后，管理员可以在 CrowdStrike Falcon 上远程查看 BIOS 验证等内置安全功能推送的通知，助您快速检测可疑活动，以免造成任何持久性损害。



应用场景和应对措施

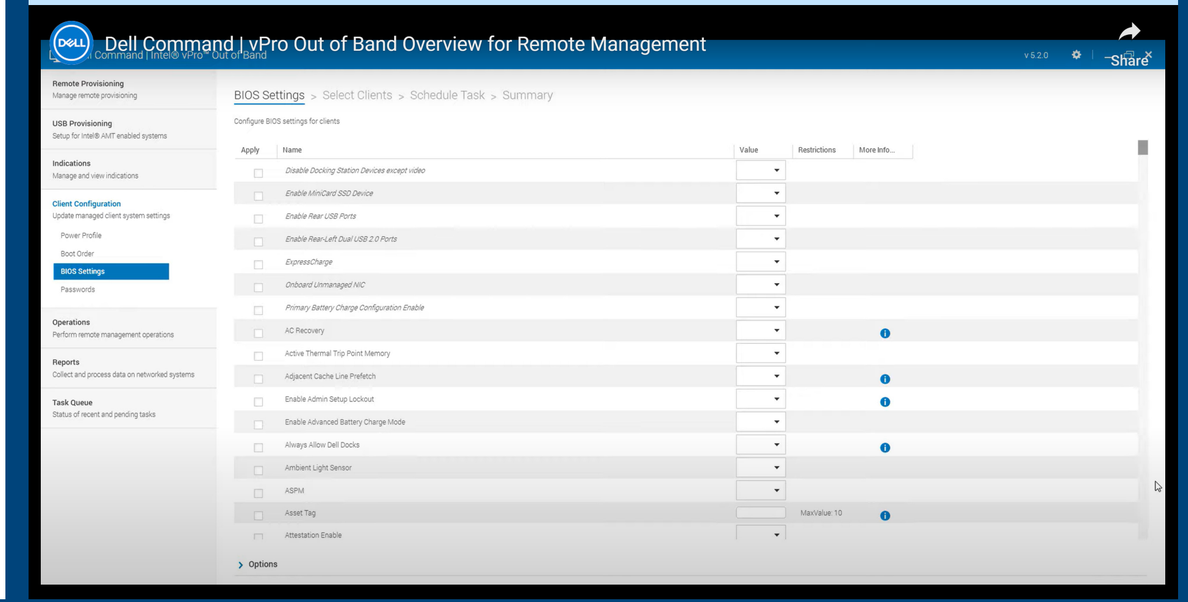
BIOS 降级应对措施

攻击者能够比以往更快地入侵网络。事实上，根据 CrowdStrike’ s Global Threat Report，在 2023 年，电子犯罪的平均突破时间（成功入侵系统并横向移动所需的时间）从 2022 年的 84 分钟缩短到了 62 分钟。观察到的最快突破时间仅为 2 分 7 秒！[6]

如需了解戴尔与其合作伙伴英特尔® 和 CrowdStrike 如何通过硬件辅助的安全防护，全程识别并抵御 BIOS 降级攻击，请参阅：

防范 | 检测和响应 | **恢复和修正**

修正 BIOS 降级：有助于防范带外系统未来面临的威胁。Dell Client Command Suite 搭载英特尔 vPro 技术，支持远程修正。



应用场景和应对措施

在第二个应用场景中，我们将了解软件供应链攻击杀伤链中的步骤是如何进行的。

软件供应链攻击

步骤 1

初始访问：供应链漏洞

攻击者将恶意代码注入软件实用程序（BIOS/固件）。

步骤 2

持久性

客户在更新设备时下载恶意代码。
攻击者安装恶意软件。

步骤 3

横向移动

攻击者欺骗他们刚刚攻击的用户，并向另一个用户发送恶意链接。该用户单击链接，攻击者窃取其凭据。

步骤 4

泄露

攻击者将数据外泄。

应用场景和应对措施

供应链已成为攻击者的主要目标。虽然这种攻击不太常见，但成功发起攻击可能会造成灾难性后果，因为组织仍在学习如何加强防御来抵御这些攻击。

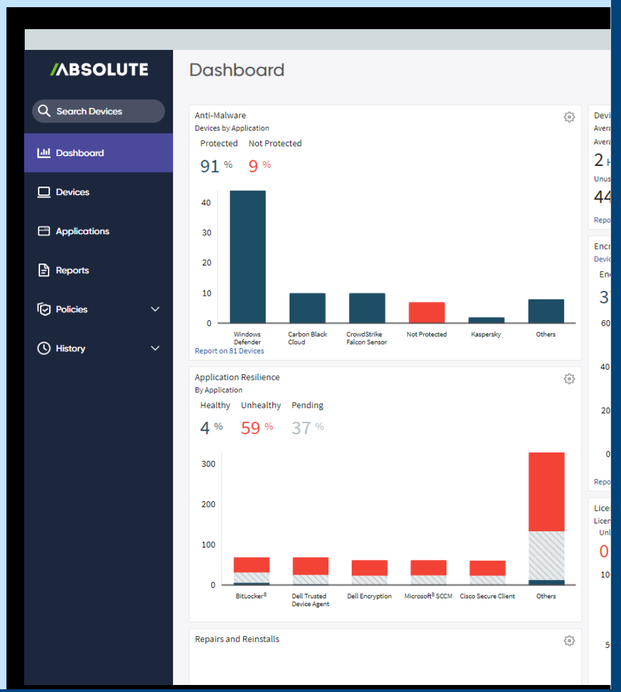
所有技术提供商都应确保销售的产品不会因存在漏洞而无意中给用户带来风险，这是他们的一项核心职责。

为了帮助企业防范攻击并使安全堆栈具有弹性，戴尔和英特尔® 恪守安全开发周期[7] 严格的流程和协议。我们提供额外的供应链保障（例如 Dell Secured Component Verification[8]），以及 Absolute 固件级安全性（如右图所示），让客户在 PC 的整个生命周期内安心无忧。

防范 | **检测和响应** | **恢复和修正**

出厂时的端点可见性：借助在戴尔管理的工厂中嵌入的 Absolute 技术，查看网络内外的所有设备。Absolute 自定义出厂安装 (CFI) 可省去部署过程中的步骤，并为可能运送到仓库和多个终端用户位置的设备提供保护。通过基于云的控制面板全面了解机群状况，从而降低风险。

- 轻松查找和维护完整的 IT 资产和应用程序清单
- 定位整个机群并绘制图表
- 优化资产使用并监视安全态势
- 跨平台支持（Windows、Mac 和 Chrome）
- 已嵌入 27 个卓越 PC OEM 的 BIOS 中



应用场景和应对措施

供应链已成为攻击者的主要目标。虽然这种攻击不太常见，但成功发起攻击可能会造成灾难性后果，因为组织仍在学习如何加强防御来抵御这些攻击。

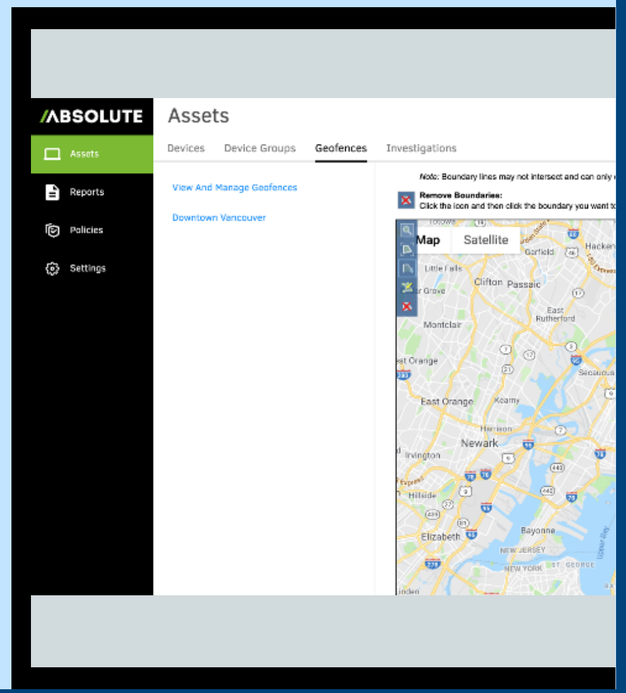
所有技术提供商都应确保销售的产品不会因存在漏洞而无意中给用户带来风险，这是他们的一项核心职责。

为了帮助企业防范攻击并使安全堆栈具有弹性，戴尔和英特尔® 恪守安全开发周期[7] 严格的流程和协议。我们提供额外的供应链保障（例如 Dell Secured Component Verification[8]），以及 Absolute 固件级安全性（如右图所示），让客户在 PC 的整个生命周期内安心无忧。

防范 | **检测和响应** | 恢复和修正

控制端点：利用 Absolute 技术，检测端点何时遭到入侵（例如，关键应用程序被恶意软件损坏或 PC 在运输途中丢失）。立即执行远程操作，使设备失效和/或删除设备包含的数据，对威胁进行修正。

- 保护脱离所定义范围的设备
- 远程保护和清理关键数据
- 使用合规性证书执行设备生命周期结束时的数据擦除
- 锁定设备以按需保护关键资产
- 启用远程固件保护



应用场景和应对措施

供应链已成为攻击者的主要目标。虽然这种攻击不太常见，但成功发起攻击可能会造成灾难性后果，因为组织仍在学习如何加强防御来抵御这些攻击。

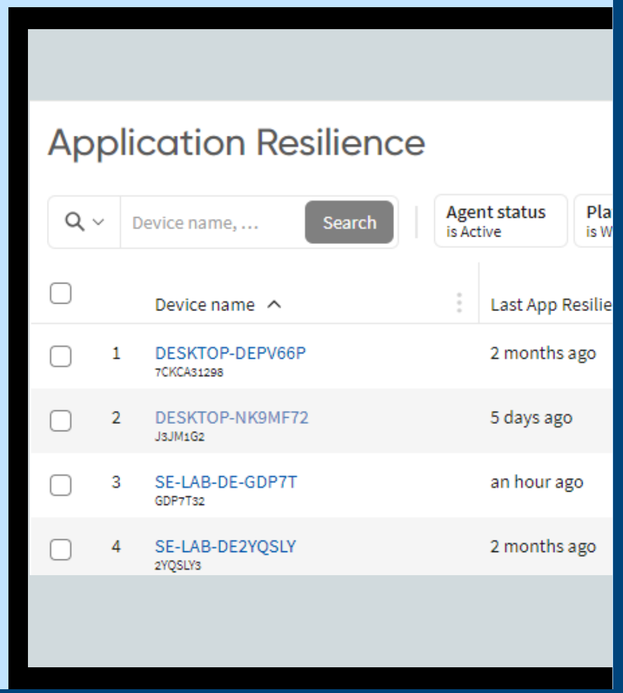
所有技术提供商都应确保销售的产品不会因存在漏洞而无意中给用户带来风险，这是他们的一项核心职责。

为了帮助企业防范攻击并使安全堆栈具有弹性，戴尔和英特尔® 恪守安全开发周期[7] 严格的流程和协议。我们提供额外的供应链保障（例如 Dell Secured Component Verification[8]），以及 Absolute 固件级安全性（如右图所示），让客户在 PC 的整个生命周期内安心无忧。

防范 | 检测和响应 | **恢复和修正**

自我修复：借助戴尔 BIOS 固件中嵌入的 Absolute Persistence 技术，在检测到篡改时恢复到原始状态。Absolute 可以对 Application Resilience 目录中任何遭到入侵的端点或受支持的应用程序（80 多个应用程序）进行自我修复或持久维护，包括建立了其他应对措施库，例如使用戴尔可信设备应用程序和 Zscaler 技术。

- 在端点上查找并轻松删除敏感数据
- 通过自定义脚本库，在设备之间采取补救措施
- 监视和自我修复应用程序
- 大型且不断增长的第三方端点控制的 Application Resilience 目录
- 通过 Absolute 调查团队调查和定位丢失或被盗的设备



要点

机群的安全性取决于其每台 PC。

为了应对现代威胁，必须安全地构建设备并实现内置安全性。

确保实现端点安全性和可管理性，
这两种特性相辅相成，可助您捕获和
抵御攻击并从攻击中恢复。

实现安全性需要整个团队相互配合。
结合使用硬件和软件，进行出色的防御。

访问以下网址了解更多信息：

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

采取下一步行动

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。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。

1. 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。
2. 来源：Futurum Group，《Endpoint Security Trends 2023》。
3. 来源：TechTarget 旗下部门 Enterprise Strategy Group 撰写的研究报告，《*Managing the Endpoint Vulnerability Gap: The Convergence of IT and Security to Reduce Exposure*》，2023 年 5 月。
4. 基于戴尔在 2024 年 10 月进行的内部分析。适用于搭载英特尔处理器的 PC。并非所有 PC 都提供全部功能。某些功能需要另行购买。经 Principled Technologies 验证。《A comparison of security features》，2024 年 4 月。
5. 来源：《What is the Cyber Kill Chain? Introduction Guide》— CrowdStrike。
6. 来源：《CrowdStrike 2024 Global Threat Report》。
7. 来源：《建立设备信任的三个注意事项》（英文版）| Dell USA。
8. 来源：《如何建立牢固的设备信任》（英文版）| Dell USA。