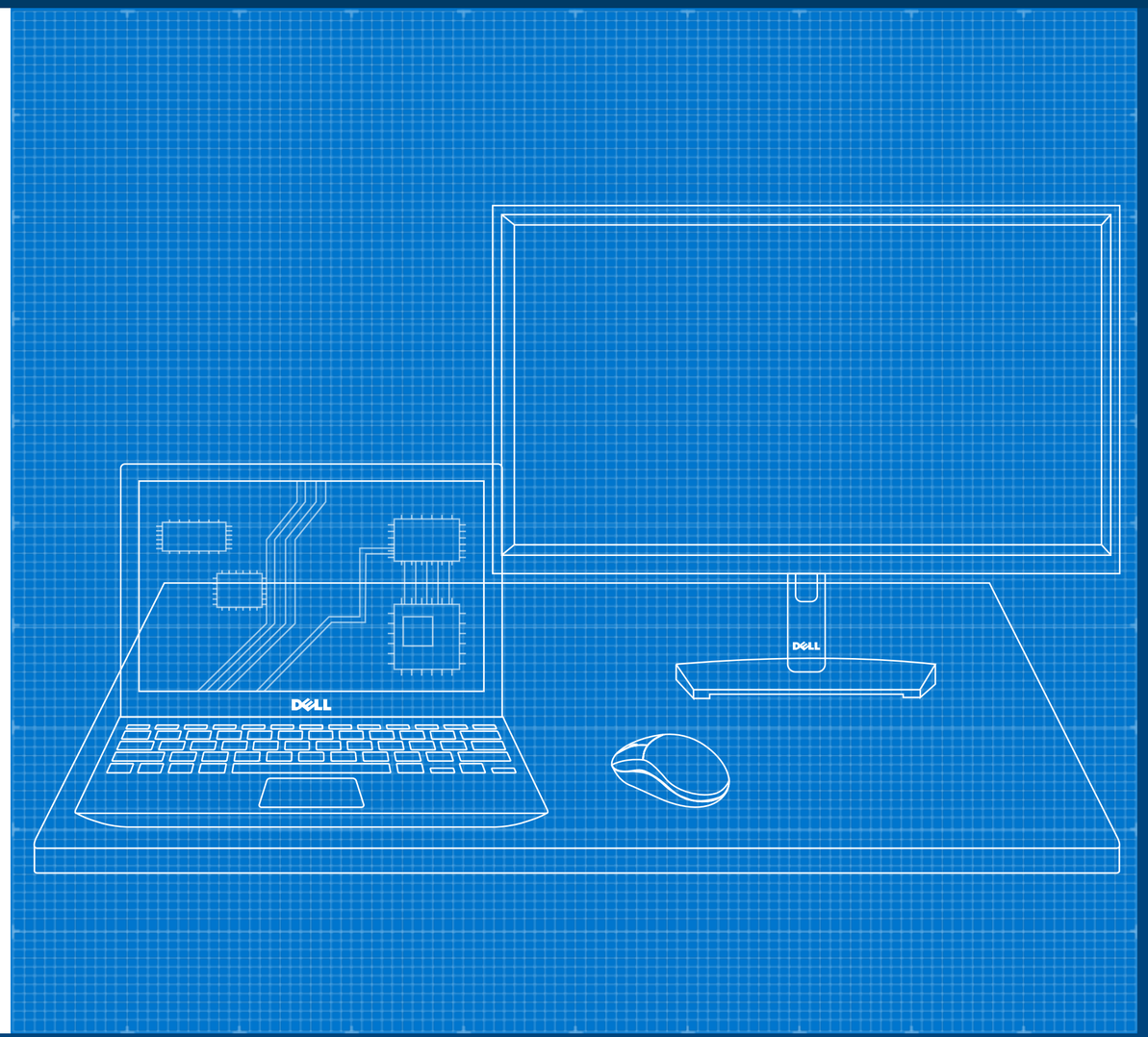
可信工作区深度剖析

通过多层防御手段提高机群的安全性



执行摘要

网络攻击在所难免，而且数量和复杂程度都在不断提升。端点设备、网络和云环境已成为主要攻击目标。

本电子书旨在为 IT 和安全决策者提供指引，说明要在如今不断变化的威胁环境中以最有效的方式防护端点，必须具备哪些条件。

目录

威胁环境

转向混合办公模式的过程带来了新的复杂性和新的攻击媒介，**端点、网络和云正在导致受攻击面不断扩大。**

更重要的是，攻击者现在会采用针对计算堆栈不同层的复杂技术，与有效的系统进程混在一起。有些方法甚至能让攻击者取得特权访问权限并*神不知鬼不觉*地禁用软件保护措施。

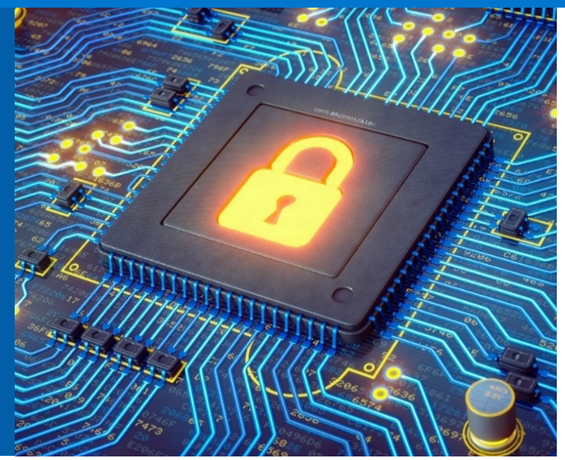
许多组织已踏上零信任之旅，以此应对这些威胁。但要启用零信任原则，您必须具备保持设备信任的能力。

随着攻击变得越来越频繁以及先进技术带来新的攻击媒介，**该如何维持设备信任呢**？

[1]《CrowdStrike Global Threat Report》，2024 年。
[2]《Dell Innovation Index》，2023 年。

您是否知道...

2023 年，75% 的攻击并非以恶意软件为媒介[1]



仅 41% 的受访组织能够满怀信心地表示，他们的技术和应用程序具有充分的安全性[2]

想探索零信任以提高您的网络安全成熟度？请参阅我们的电子书：*《端点安全性是零信任之旅的重要组成要素》*。

面临挑战

为了有效地确保端点安全性，了解您的对手及其工作方式非常重要。

一次得逞的入侵便可能会为攻击者带来大笔赎金，因此**攻击者通常会多次尝试入侵同一组织，利用不同的方法和侵入点来提高自己的胜算。**例如，在单个设备的生命周期中，攻击者可以尝试通过数十种媒介来利用漏洞。

传统的防御措施不足以确保端点的安全。当组织强化一个受攻击面时，攻击者便会转向其他更薄弱的目标。随着全球转向混合办公模式，攻击者发现了新的端点攻击媒介，并且造成了毁灭性的后果。

请参阅右侧的攻击示例

供应链攻击：瞄准供应商以取得权限来访问其系统、数据和/或网络，进而访问其客户的系统、数据和/或网络。**示例：通过篡改组件发起的硬件供应链攻击：**

攻击者拦截 PC 货物并更换硬盘。

IT 部门在整个公司部署遭篡改的设备。

攻击者安装恶意软件以在用户登录时提取凭据。

社会工程攻击：诱骗终端用户提供可用于获取设备和网络访问权限的敏感信息。**示例：通过网络钓鱼电子邮件发起的欺骗性攻击：**

终端用户落入网络钓鱼电子邮件的圈套，并在伪造的网页上提交凭据。

攻击者使用有效凭据远程访问网络。

攻击者通过 Web 服务窃取数据，对窃取的数据进行加密，并以此勒索赎金。

保护现代化工作区的安全

就端点保护而言，您需要在设备整个生命周期中的不同状态下，积极部署预防、检测与响应以及恢复与修正举措，从 PC 的采购和制造，到运输和部署，从使用到报废，无一例外。想象一下这种合并起来的受攻击面有多大！

能够为最坏情况做打算的网络安全策略，就是真正有效的策略。这种策略假设有发生入侵的可能性并嵌入了多层保护措施，以尽可能快速且频繁地中断攻击。它还包括修正功能，以尽量减少风险重复出现的可能性。

[3]《Dell Innovation Index》，2023 年。

预防

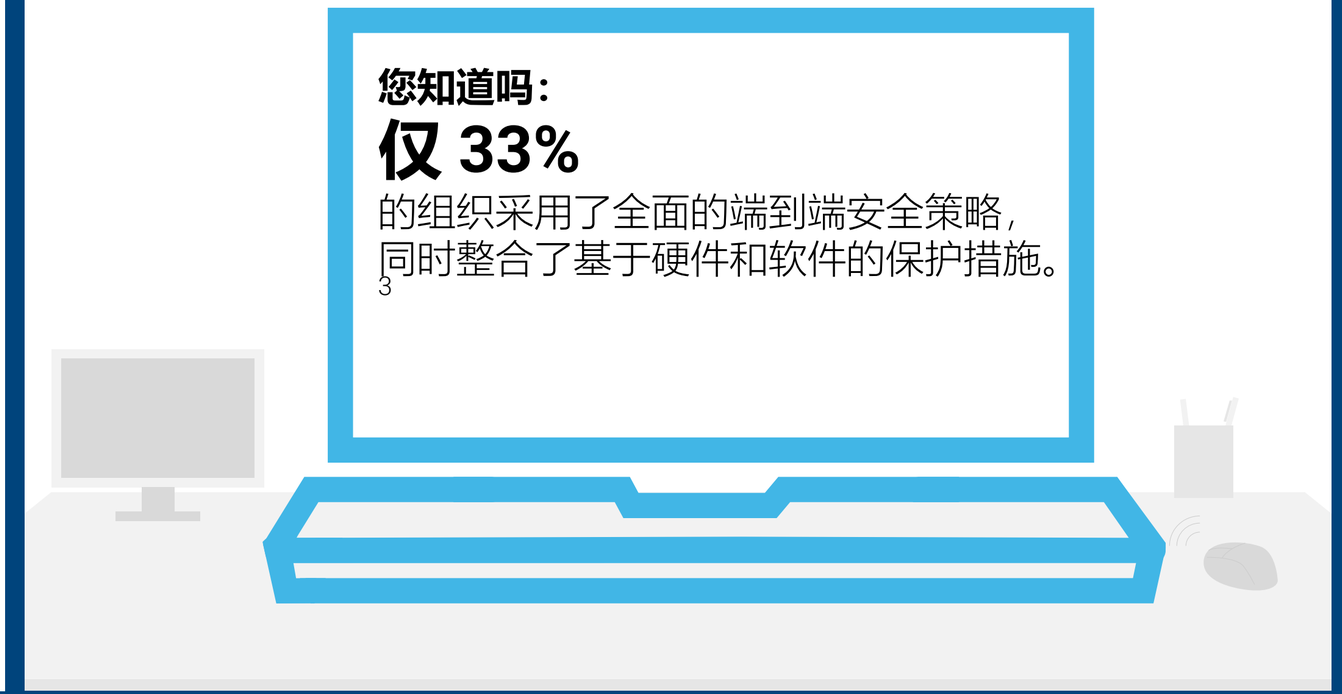
采用有助阻止攻击的防御措施，减少受攻击面。

检测与响应

始终假设有发生入侵的可能并保持警惕。

恢复与修正

减轻攻击的影响，让业务尽快恢复如常。



可信工作区深度剖析

必须确保以下三方面的安全，才能实现端点安全保护现代化：

1. **软件安全性：**现如今，企业网络之外的用户、设备和数据量比以往任何时候都更多。确保软件安全不仅能保护设备，还可将保护扩展到恶意活动经常发生的网络和云环境。

2. **硬件安全性：**设备必须包含内置安全功能。这涉及保护使用中设备的硬件和固件的安全。为了防护工作区，您必须拥有内置功能来监视和控制设备。

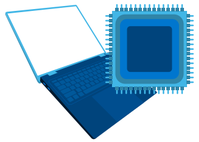
3. **供应链安全性：**必须确保设备制造安全。这意味着您合作的供应商要了解当前的威胁环境，具备相关的知识，并且能够随着环境的演变而将其付诸实践。安全的 PC 设计、开发和测试可以尽量降低产品出现漏洞的风险，而供应链控制措施则可以降低产品遭篡改的风险。

多层安全性剖析

（列出安全保护措施的代表性示例）

软件安全性

- 下一代防病毒软件 (NGAV)
- 端点检测和响应 (EDR)
- 扩展检测和响应 (XDR)
- 云数据保护
- 网络保护
- 自动自我修复



硬件和固件安全性

- 启动时验证
- 运行时验证
- 用户身份验证
- 安全通知和警报/遥测

供应链安全性

- 安全开发实践
- 安全的供应链实践
- 组件验证
- 防拆封包装

我们的方法：Dell Trusted Workspace

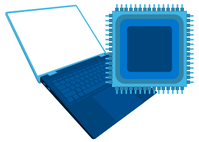
戴尔是可靠的安全和 IT 合作伙伴，致力于为世界各地的组织服务。与点式解决方案不同，戴尔专注于整体安全结果，构建了一套解决方案来中断杀伤链，帮助您提高抵御网络攻击的网络弹性。**Dell Trusted Workspace 包括：**

- 独具特色的**硬件和固件保护措施**，让戴尔成为全球安全性出众的商用 PC 提供商。[4] *（固有安全性和内置安全性）*
- 一个由**业界卓越的软件**合作伙伴组成的生态系统，为设备、网络和云提供高级威胁防护。 *（增置安全性）*

[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。某些功能需要额外购买才能使用。经 Principled Technologies 验证。《A comparison of security features》，2024 年 4 月。

来自合作伙伴生态系统的*增置*软件安全性

- **Dell SafeGuard and Response：** **CrowdStrike** 和 **Secureworks** 提供威胁检测、响应和修正功能。
- **Dell SafeData：** **Netskope** 为基于云的应用程序提供可见性、监视和数据丢失预防。**Absolute** 支持应用程序和网络的自我修复。



选择安全性出众的商用 PC，获得*内置*的硬件和固件安全性[4]

保护使用中的设备的功能示例：

- **Dell SafeBIOS** 主机外 BIOS 验证*、攻击指标* 和 CVE 检测* 有助于及早发现恶意活动，阻止其入侵 PC。
- **Dell SafeID** 使用专用安全芯片保护用户凭据。*
- **主机外固件验证**可保护高权限固件的完整性。*
- 通过**戴尔可信设备应用程序**，戴尔将设备遥测技术与业界卓越的软件集成在一起，以提高整个机群的安全性。*

***与生俱来*的供应链安全性有助于确保 PC 从首次启动时即安全无虞**

- Dell Secured Component Verification* (SCV) 等 **Dell SafeSupply Chain** 附加服务为产品的完整性提供了额外保障。

** 戴尔独有*

通过戴尔实现完全整合

硬件和软件对策落实到位后，就可以通过有助于防止常见攻击的防御措施，来减小受攻击面。

检测和响应功能瞄准的是那些可能蒙混过关的隐蔽攻击。

在第 4 页讨论的供应链攻击中，如果您与戴尔合作，**安全供应链实践**等预防措施可以在杀伤链的早期中断攻击。如果攻击成为漏网之鱼，其他对策（如 **SCV**）也可发挥作用。

在社会工程攻击中，即使攻击者成功诱骗用户交出有效凭据，**基于硬件的用户验证（例如 SafeID）**也可以阻止攻击者的行动并拒绝进一步的访问。**Next-Gen Secure Web Gateway** 等安全软件可以提供另一层监视保护。

反击通过篡改组件发起的硬件供应链攻击。

攻击者拦截 PC 货物并更换硬盘。

- **安全的供应链实践**
- 防拆封包装
- 门锁

IT 部门在整个公司部署遭篡改的设备。

- 安全组件验证 (SCV)
- 运行时验证

攻击者安装恶意软件以在用户登录时提取凭据。

- 云访问安全代理
- Next-Gen Secure Web Gateway

反击通过网络钓鱼电子邮件发起的社会工程攻击。

终端用户落入网络钓鱼电子邮件的圈套，并在伪造的网页上提交凭据。

- NGAV
- EDR
- XDR

攻击者使用有效凭据远程访问网络。

- 使用 SafeID 进行多因素身份验证
- 零信任网络访问

攻击者通过 Web 服务窃取数据，对窃取的数据进行加密，并以此勒索赎金。

- 新一代安全 Web 网关 + 用户实体行为分析

要点

入侵在所难免。有效的端点安全保护方案总是会假定最坏的情况，并专注于中断杀伤链，无论杀伤链在设备、网络还是云端，都能覆盖到。

没有哪种解决方案能够 100% 阻止所有攻击。将硬件和软件对策相结合，以提供尽可能完善的防护措施。

您的安全取决于您的供应商。请要求您的供应商概述他们采取的安全措施。

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

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。**请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 可帮助为现代的零信任就绪型 IT 环境保护端点。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。