立即开始通过 3 种简单方法实施 Zero Trust 安全模式

新的业务计划和流程不断扩大了攻击面。应用程序、用户和设备正在向传统的企业控制区之外迁移，曾经受信的边界分崩离析，所以企业安全和网络必须相应做出调整才能保护业务。对于大多数组织而言，进行全面的 Zero Trust 的安全转型并非一日之功。许多公司都需要时间来全面实施主要的网络和安全更改，但一开始您可以立即采取几个简单的步骤。以下三项措施将为您实现“永不信任，始终验证”这一安全模式铺平道路：

1. 执行威胁检查。了解您的环境并确定设备当前是否受到恶意软件/网络钓鱼的威胁。许多网络已遭到攻击并且存在已逃脱现有安全措施检测的恶意软件。**执行免费的 30 天威胁检查**，您可获得一份有关当前您环境中的活跃威胁的定制报告，以及针对这些高级威胁如何补救的专享建议。此操作实施起来快速简便，而且可最大程度减少网络更改。对于 IT 团队而言，这通常是实现运营优势的捷径。

2. 停止向用户授予网络访问权限。完全网络访问权限会增加您受到威胁的风险。用户访问权限应限制用户仅可访问个人需要的应用程序，而非整个网络。为了确保运营效率，从最容易迁移的应用程序（如 Web 应用程序和任何新应用程序）开始即可，并基于 Zero Trust 安全原则发布这些应用程序。然后，**执行 Zero Trust 架构评估**，以制定从当前状态迁移到 Zero Trust 框架的全面计划。这包括分析用户和应用程序，以及为所有应用程序（包括原有的本地应用程序）制定定制的阶段性计划。

3. 淘汰特定用户组的传统 VPN。Zero Trust 安全框架建议您停止隐式信任您的端点并停用原有的访问权限（包括 VPN 和特权企业 Wi-Fi/以太网段），以删除内部层的相关信任。首先，根据 Zero Trust 安全原则为承包商等高风险用户组配置访问权限。然后，为所有用户确定原有访问权限的逐步淘汰计划。

为了应对不断发展的业务和威胁形势，必须不断调整企业的安全方法。通过迁移到 Zero Trust 安全架构，您将能够简单有效地保护应用程序、用户和设备。这种迁移可通过一个逐步的过程来实现，但首先需要从这三个可行的基本任务开始。要了解有关立即开始 Zero Trust 转型的更多信息，**请安排与 Akamai 安全专家开展一场研讨会**。让我们一起共同确定其他机会和措施，以迁移到 Zero Trust 安全模式。