Akamai

白皮书

实现卓越安全态势的路线图

以 Zero Trust 为核心制定一份自定义转型计划

为了在不断演进的安全环境中保持领先，并防止出现任何懈怠，我们最近利用 Zero Trust 成熟度模型 (ZTMM) 对自身的安全状况进行了可视化评估。本文将阐述如何在您的企业中应用这些方法，从而明确需要改进的关键环节，并打造实现卓越安全态势的清晰路线图。

简化 Zero Trust 之旅

企业访问和安全体系错综复杂并且不断变化。鉴于此，企业可能很难确定应从哪发力才能打造卓越的 Zero Trust 安全态势。

因此，我们建议您使用 ZTMM 来评估和可视化您当前的安全态势。我们使用该模型评估了自身的企业安全态势以及多个客户的安全态势。当整个过程结束时，您将获得一个切实可行的行动路线图，帮助您逐步建立起 Zero Trust 架构。（请参阅附录 A，了解有关 Zero Trust 概念的更多信息。）

为何 Zero Trust 成熟度模型能够提供帮助

我们认为，在实现更强大的安全态势之路上，最关键的一步就是：付诸行动。但是，在纷繁复杂且不断变化的网络安全环境下，知易行难。我们看到很多企业都面临决策困难，不知道做什么、做多少以及应当按照什么顺序做出改变来实现 Zero Trust。

而这正是 ZTMM 的用武之地。它可以创建一个以 Zero Trust 为中心的框架，将复杂的问题线性化，使实施变得更容易。它可以帮助企业制定变革计划和更新预算。它还可以向非 IT 专家的决策者解释 Zero Trust 概念，这有助于 IT 团队获得所需的支持。

ZTMM 久经考验。它由美国网络安全和基础架构安全局 (CISA) 开发，已在美国联邦机构中得到了广泛采用。

Zero Trust 成熟度模型的五大支柱和三项功能

ZTMM 代表了五个不同支柱的实施梯度，因此可以随着时间的推移逐步进行微小的改进。这些支柱会要求您考虑身份、设备、网络、应用程序和工作负载以及数据（图 1）。ZTMM 还会要求您思考横跨五大支柱的三项功能：

- 监测与分析
- 自动化与编排
- 治理

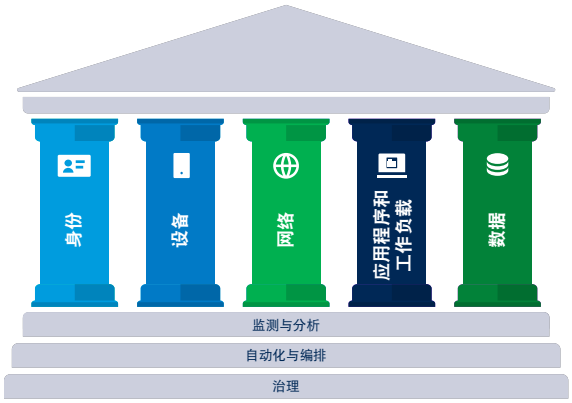


图 1：CISA 的 ZTMM 是支持向 Zero Trust 过渡的众多途径之一（来源：CISA）

其中的每个领域都分配有一个成熟度状态，该状态说明了企业在实现 Zero Trust 方法上的进展情况。四个成熟度阶段（传统、初始、高级和最佳）说明了从手动配置和 VPN 到理想的“无边界安全”设置的历程（图 2）。在成熟度的“最佳”阶段，企业可以向应用程序授予最低权限、拒绝对易受攻击设备的身份验证和访问、防止内部威胁扩散以及即时检测和应对安全事件。（请参阅附录 B，了解有关 ZTMM 框架的详细说明。）

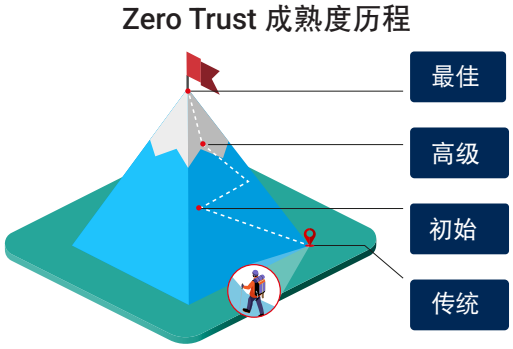


图 2：Zero Trust 成熟度历程（来源：CISA）

通过突出成熟度最低的领域，ZTMM 可帮助企业建立一个更加平衡的安全环境。Akamai 业界卓越的安全解决方案套件与我们的专业知识相结合，使得实现成熟的安全态势变得更加容易。

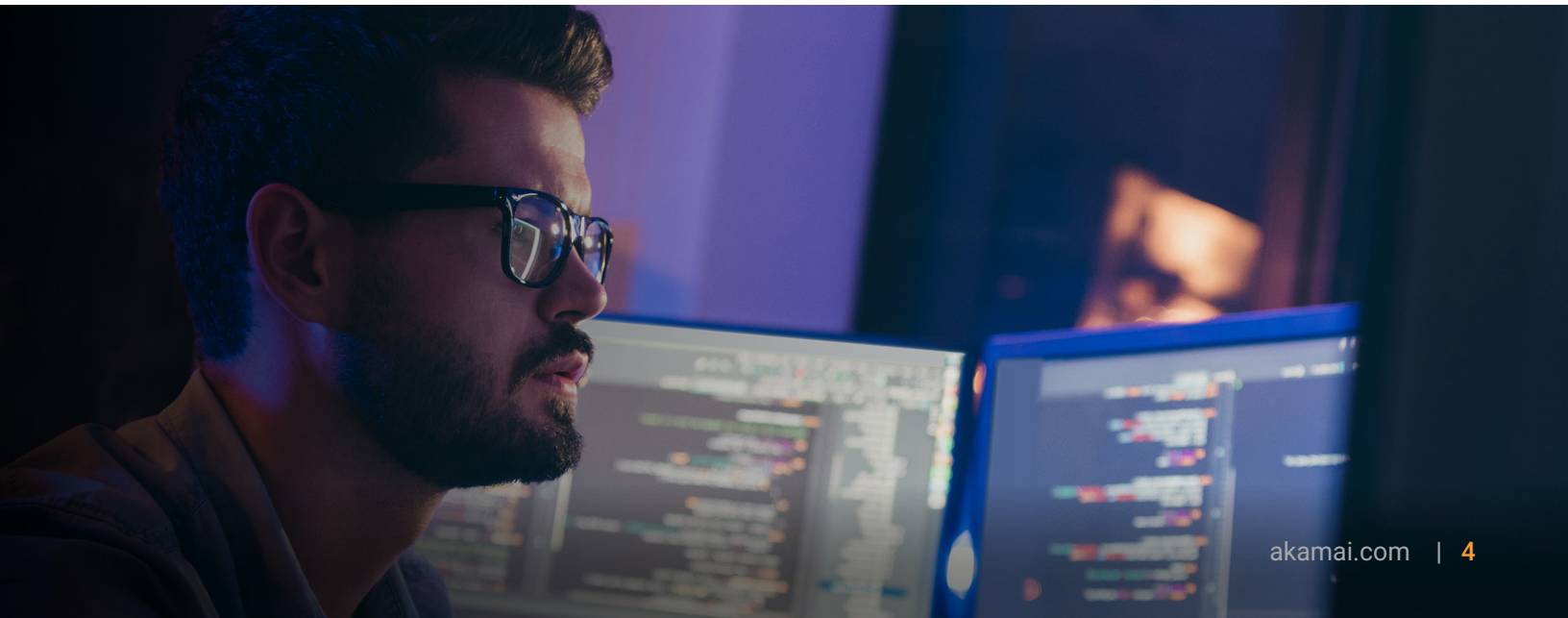
您的团队是否在实施 Zero Trust 方面遇到了困难？很多企业也有相同的问题。

创建 Zero Trust 架构并非某一个部门的职责。它需要企业各个层面的利益相关者提供支持、赋予灵活性和给予批准。

Akamai 是一家致力于支持并保护在线商业活动的网络安全和云计算公司。我们将卓越的安全解决方案、出色的威胁情报与全球运营团队相结合，在世界各地的每个接触点保障关键数据和应用程序的安全。凭借这种全球化的视野，我们能够了解实现 Zero Trust 安全态势过程中所面临的常见挑战，并且帮助您找到解决方案。

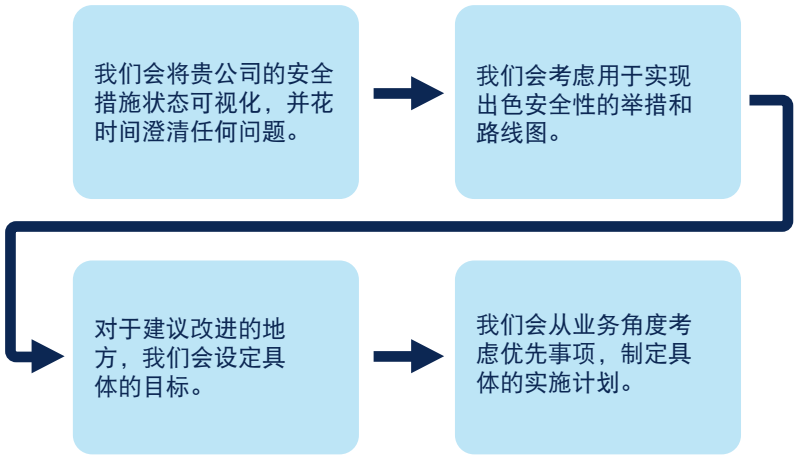
三种常见的 Zero Trust 挑战

1. **确定从何处着手。**我们通常建议从工作负载监测开始并缩小攻击面以增强网络恢复能力——诚然，这取决于企业当前的安全态势。
2. **快速取得成功。**实现 Zero Trust 似乎是一项艰巨的任务，团队很难专注于任何一件事，也很难庆祝为实现目标所迈出的一小步。
3. **展示投资回报率。**Zero Trust 项目的成本并不低，并且它们通常需要在企业内部进行文化变革和技术变革。展示投资回报的能力（无论是缩小攻击面、减少数据泄露、修复漏洞还是实现财务收益）至关重要，对于决策者和安全负责人来说尤其如此。



准备好开启您的 Zero Trust 之旅并实现安全态势可视化了吗?

正如我们在 Akamai 所做的那样，您可以使用 ZTMM 来实现贵企业当前安全态势成熟度状态的可视化。通过这种方式，您可以更清楚地了解如何让您的流程更加平衡，以及需要做出哪些改变才能实现 Zero Trust 架构。



Akamai 如何引导您实现 Zero Trust 安全态势

成功的 Zero Trust 架构会利用各种控制措施和原则来解决安全挑战。

我们将考虑各种举措和路线图来帮助您制定一个实施计划，该计划会将您的整个业务及其目标考虑在内以实现出色的安全性。通过此方法，我们可以与您合作构建长期有效且可持续的安全系统和流程。

除了 Akamai 云外，我们的安全产品套件（包括先进的分布式 ZTNA 解决方案、业界卓越的微分段、防网络钓鱼多重身份验证 (MFA) 和主动 DNS 防火墙）将使您的安全态势朝向 Zero Trust 成熟度规模的“最佳”阶段发展。此外，单个代理使用单个控制台即可运行整个系统（图 3）。

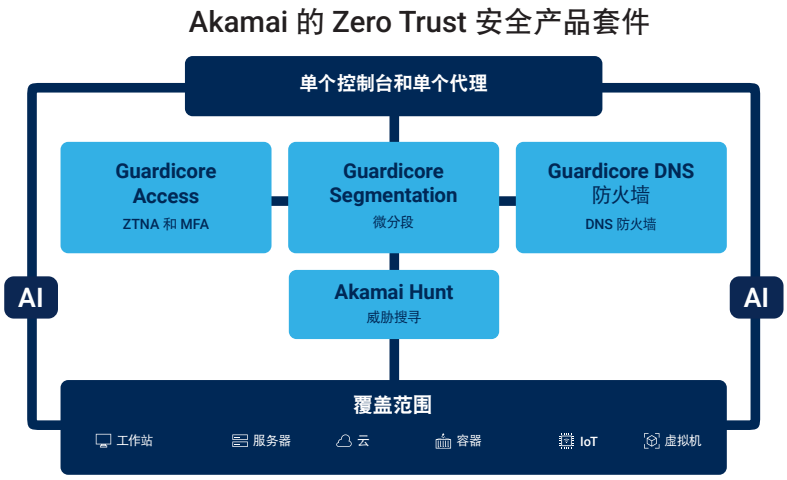


图 3：单个代理使用单个控制台即可运行 Akamai 的安全产品套件

案例研究

使用 Zero Trust 成熟度模型实现跨国零售商电子商务安全态势的可视化

我们最近分析了一家跨国零售商的电子商务安全态势，实现了其安全状态的可视化并提供了相应的路线图，帮助其逐步实现出色的安全态势。我们的专家团队确定了 ZTMM 中需要改进的领域，并按重要性从高到低的顺序进行了排序。接下来，我们将分享相关结果。

系统不平衡，实施存在差异

在每个支柱中，我们都发现一些功能以最高成熟度水平（“最佳”）实施，例如移动设备管理和应用程序部署自动化。但是，每个支柱中的一些功能仍然处于“传统”水平，这带来了严重的风险。

尤其是，身份和网络支柱中的重要功能未得到增强；这些支柱是 Zero Trust 架构的基础。这些功能包括了 MFA、身份基础架构的集成管理、基于上下文的访问控制以及微分段。

高风险 ID 基础架构

我们的分析人员发现，ID 和密码身份验证是该零售商内部的标准验证方法；只有少数几个系统使用 MFA。这导致身份验证信息被滥用的风险很高。此外，存在多个 ID 基础架构，例如 Microsoft Entra ID、本地 Active Directory (AD) 以及轻型目录访问协议 (LDAP)。由于该零售商的管理未进行集成，因此存在从采用较弱安全措施（例如，LDAP）的 ID 基础架构开始发生数据泄露的风险。

未集成的授权控制

授权控制未进行集成，因此每个应用程序都是单独处理的。无法阻止来自易受攻击设备的访问或可疑访问：如果有权访问公司网络的某个员工或合作伙伴的 PC 感染了恶意软件，则通过横向移动对系统和资源进行未经授权访问的风险很高。

分段不充分

我们发现，该零售商的安全措施只重视外部威胁，而忽视了已入侵网络的攻击者带来的风险。如果没有进行稳健的内部分段，则通过仓库的 Wi-Fi 网络或 VPN 漏洞进行的入侵可能会导致不受控制的横向移动。这种缺乏内部屏障的情况会显著增加系统遭到大规模入侵、数据泄露和运营中断的风险，因为攻击可以在没有遏制措施的情况下在网络中自由移动。

漏洞管理和响应措施不充分

该零售商没有将软件物料清单 (SBOM) 与漏洞信息相关联的管理系统。这意味着，它无法快速识别和应对应用程序漏洞，这带来了很高的风险。

我们的建议

我们建议该零售商采取以下五个步骤来增强其安全态势：

1. 采取主动措施，以降低当前设置中存在的未经授权入侵和横向移动的风险
2. 继续将身份基础架构集成到其现有技术堆栈中
3. 制定用于增强身份验证和授权功能的计划，并与 Zero Trust Network Access 相结合
4. 确定实施精细工作负载和应用程序保护的最有效方法
5. 针对未知的未来威胁构建应对系统及流程，建立加强漏洞管理和响应的系统及流程，并制定相应的计划

如果您有兴趣开启 Zero Trust 之旅，请联系我们进行免费的安全评估。

附录 A：Zero Trust 概念的概述

Zero Trust 是一种安全理念，它的核心原则是：不信任企业网络边界内外的所有用户、设备或系统，

而应通过验证过程和监控来最大限度地降低风险。这包括实施严格的身份和访问管理 (IAM) 策略、使用多重身份验证 (MFA) 以及优先考虑基于角色的访问控制 (RBAC) 等方法。

Zero Trust 概念问世已有 15 年的时间，但随着新冠疫情期间各企业对远程访问需求的增加，它也变得更加重要。很多公司都意识到，他们现有的安全措施无法应对用户和设备分散在各个地方而不是集中在一起的情况。

现在，Zero Trust 原则有很多实现方式，包括 Zero Trust 架构、Zero Trust Network Access (ZTNA)、Zero Trust 安全 Web 网关 (SWG) 和微分段。

详细了解 Zero Trust

附录 B：ZTMM 2.0 框架

五大支柱

在需要跨支柱协调之前，每个支柱都可以按自身进度独立发展，其进度也可能各不相同。

支柱	说明
身份	一个属性或一组属性，用于唯一地描述机构用户或实体（包括非人员实体）
设备	任何可以连接到网络的资产，包括服务器、台式机和笔记本电脑、打印机、手机、物联网 (IoT) 设备、网络设备等
网络	一种开放的通信媒介，包括典型渠道（例如机构内部网络、无线网络和互联网），以及用于传输消息的其他潜在渠道
应用程序和工作负载	在本地、移动设备上和云环境中执行的机构系统、计算机程序和服务
数据	驻留或曾驻留在系统、设备、网络、应用程序、数据库、基础架构和备份中的结构化和非结构化文件及片段，以及相关的元数据

跨支柱功能

这三项功能为整个 Zero Trust 框架提供支持，以确保安全措施的整合性、快速响应性和一致性。

功能	说明
监测与分析	企业应该清晰、实时地了解所有用户活动、设备状态和网络交互。快速检测并应对威胁，这可以降低风险。企业做出明智、主动的安全决策。
自动化与编排	人为错误是导致发生安全问题的常见原因。当自动化和编排得到优化时，发生这种情况的可能性会降到最低。自动化可以简化日常任务，而编排可以协调不同系统间的安全操作。这可以为更快、更协调地应对威胁创造良好条件。
治理	良好的安全治理能够明确责任归属，从而确保每个人都遵守相同的安全实践和规定。这可以为安全运营奠定坚实的基础。此外，它还可以设定明确的 Zero Trust 准则，并帮助企业满足合规性标准。

Zero Trust 成熟度模型的成熟度方面

ZTMM 2.0 为每项功能定义了四个成熟度级别。目的是确定五大支柱和三项功能的当前成熟度级别，然后制定计划，将每项功能提升到最高成熟度级别。

成熟度级别	说明
传统	手动配置、响应和抵御；静态和孤立的策略及解决方案
初始	开始采用自动化；初步的跨支柱解决方案；对最低权限进行一些响应性更改；内部系统的聚合可见性
高级	自动控制（如适用）；跨支柱策略实施；根据风险/态势对最小权限进行更改；对预定义抵御措施的响应
最佳	自动控制（如适用）；跨支柱策略实施；根据风险/态势对最小权限进行更改；对预定义抵御措施的响应

欢迎联系我们，与我们一起探讨 Akamai 安全套件以及我们能为贵企业的安全体系带来哪些长期改变。