8 个步骤实现

ZERO TRUST

全面、切实可行的路线图

随着应用程序、用户和设备的演变，曾经受信的企业边界分崩离析，
许多企业开始转向 Zero Trust 安全模式来抵御攻击。

使用 Akamai 首席技术官 Charlie Gero 编撰的这份分步实施指南，
构建一个包容一切的有形 Zero Trust 架构，帮助在云原生世界中实现安全应用程序访问。采用这一规范流程，轻松过渡到无边界环境，逐步分阶段部署应用程序，
从而减小您的迁移风险。

1

应用程序预检阶段

首先，检查并确保应用程序符合您已部署的访问代理的要求。在 Charlie Gero 所著的本白皮书中，阅读关于预部署假设和必要前提条件的详细内容。

2

访问代理准备阶段

接下来，配置您的访问代理，以便其知晓该应用程序及其特定的安全和访问权限。考虑配置访问代理时所处的环境（在云端还是在本地），以及如何将其推送到您的最终用户。

3

测试实验室登入阶段

现在您可以开始登入用户。我们建议事先建立一个指定的测试实验室群组；这些用户将是最先负责验证应用程序功能完整性的用户。此时，测试实验室成员应确认身份验证正确工作，多重身份验证配置得当，单点登录对于所有其他之前登入的应用程序均有效。关于用户分组方法的更多信息，请参阅白皮书。

4

安全性升级阶段

一旦测试实验室用户能够安全地访问应用程序，您就应该考虑启用原本在传统边界模式下不可能实施的安全功能。我们建议启用：

- Web 应用程序防火墙 (WAF)，用于防范 SQL 注入、跨站点脚本攻击和常见注入攻击
- 高级威胁防护
- 浏览器和操作系统治理
- 非托管设备相对于托管设备的限制
- 地理拦截和基于 IP 的限制

无论您启用什么功能，测试实验室成员都应确保安全选项不仅有效，而且不妨碍应用程序的正确功能。

5

性能升级阶段

现在，您应该检查性能有无下降。在传统的访问和安全模式中，企业应用程序性能经常受限于应用程序服务器的稳健性，以及企业各分支位置之间的相关链路。我们建议通过以下功能来缓解这些问题：

- 缓存
- 利用内容交付网络 (CDN)
- 路由优化
- 前向纠错 (FEC)
- 数据包复制

不论如何，为了准确地评估性能改善，我们建议在此阶段以及在应用程序登入之前监测性能。

6

外部用户登入阶段

现在该为外部用户部署应用程序了，因为采用非传统的访问方法，就意味着移除该群组的 VPN。外部用户还最容易受到性能问题影响，并处于最危险的环境中 — 他们所在的位置将您的应用程序和数据置于风险之下。虽然除了性能提升以外，这种过渡应近乎无形，但我们还是建议事先通知用户，以便他们能够密切注意功能的正确性。关于用户分组方法的更多信息，请参阅白皮书。

7

内部用户登入阶段

此时，您可以将应用程序作为 CNAME（规范名称）条目，添加到通用视图中。然后，所有用户应立即通过访问代理开始访问此应用程序。通过前面六个阶段，所有错误或配置不当都应当已被发现和纠正；所有用户现在都应享受到更轻松、更快、更安全的访问。关于用户分组方法的更多信息，请参阅白皮书。

8

VLAN 迁移阶段

在经过适当的时间以后，您可以将应用程序移动到防火墙后的 VLAN 中。在此之前，应用程序服务器本身仍可直接通过其 IP 地址访问，因而容易受到您的网络边界内恶意软件的攻击。最后的这个阶段消除了所有直接 IP 访问，使应用程序与除访问代理以外的一切有效隔断。有关后部署操作的指南，请阅读完整的白皮书《超越边界式安防》。

查看 Akamai 的 Zero Trust 参考架构，直观地了解此流程，
或者访问 akamai.com/zerotrust，进一步了解能协助您完成
以上实施的解决方案。

Akamai