白皮书

操作指南：

Zero Trust 安全转型

Akamai

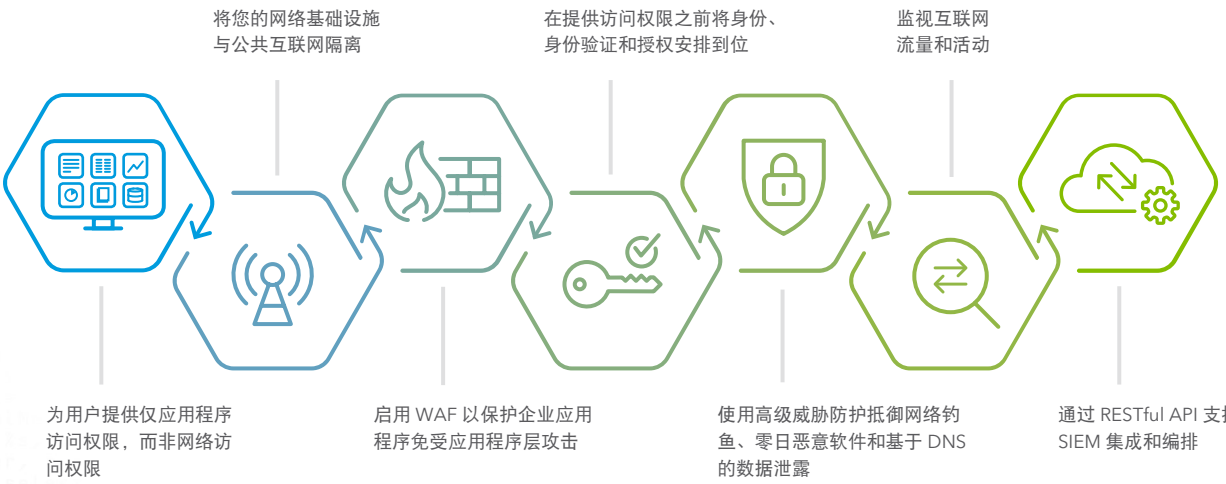
执行摘要

企业控制区域之外的每个人都是恶意的，而该区域之内的每个人都是诚实且善意的，这一网络边界的概念在当今的业务环境中不再可靠。广泛采用 SaaS 应用程序、迁移到基于云的架构、越来越多的远程用户以及大量 BYOD 设备使得基于边界的安全变得不合时宜。此外，以边界为中心的防御需要设备和安全策略管理，以及频繁的软件升级，这无疑加重了原本已让 IT 团队不堪重负的操作复杂性和压力。随着攻击面的扩张，紧缺的 IT 资源难以管理日益复杂的网络架构，同时网络罪犯也越发精通、老练并且受利益驱使，他们竭力避开各种安全措施。亟需一款可应对这些不同挑战的战略性安全框架。

什么是 Zero Trust 安全，为什么它如此重要?

Zero Trust 模式取代了以边界为中心的安全架构。它可确保根据身份、设备和用户环境动态实施安全和访问决策。Zero Trust 安全框架还规定，只有经过身份验证和授权的用户和设备才能访问应用程序和数据。同时，它还可以保护这些应用程序和用户免遭互联网上的高级威胁。

为了推进 Zero Trust 之旅并保护用户、应用程序和您企业的未来，我们建议您：



为用户提供仅应用程序访问权限，而非网络访问权限

虚拟专用网络 (VPN) 等传统远程访问技术无法满足当今无边界数字化企业日益增长的需求。传统 VPN 对企业安全构成威胁，因为它本身就会在防火墙上形成漏洞，从而提供不受限制的网络访问。一旦攻击者位于内部，其就可以自由地横向移动以访问和利用网络中的任何系统或应用程序。传统 VPN 不仅会使企业面临安全风险，而且它们还是复杂的解决方案，需要大量 IT 资源来进行硬件和软件管理，同时维护和扩展的成本高昂。

网络分段有时被视为全面访问的对策，事实证明其成本高昂、难以实施，而且管理起来很麻烦。而且，其最终不会降低风险；“完全允许”访问仍允许在网络中横向移动。虽然它划分了子网中的东西流量，但它不能阻止同一子网中的水平传播。

要保护您的业务并启用 Zero Trust，仅允许用户访问其角色所需的应用程序。将此访问基于授权、用户身份、设备状态、身份验证和授权。这些最佳做法将减少横向攻击，进而减少网络风险敞口。淘汰传统 VPN 将改善用户体验、提高员工工作效率并减少帮助台故障单。摆脱对防火墙、硬件和软件的依赖意味着可降低 IT 维护成本。此外，仅应用程序权限还可改善管理，提供对访问应用程序的人员、数据传输位置以及访问方式的可见性和洞察力。

仅向用户授予其所需应用程序的访问权限，并将此访问基于授权、用户身份、设备状态、身份验证和授权。

将您的网络基础设施与公共互联网隔离

将内部应用程序和访问基础设施暴露于互联网会使它们容易遭受 DDoS、SQL 注入和其他应用程序层攻击。网络罪犯变得越来越狡猾。他们利用不断发展的技术来扫描企业网络配置，以发现易受攻击的应用程序和重要数据。因此，企业必须将应用程序和访问架构与公共互联网隔离开来，这样恶意攻击者就无法利用开放的侦听端口将其作为攻击目标。如果网络罪犯无法找到网络或确定目标设备正在运行的应用程序和服务，其将无法实施攻击。

启用 WAF 以保护企业应用程序

现代网络攻击具有高度针对性。恶意攻击者利用电子邮件、社交媒体、即时消息、短信等社交工程，通过高度相关和个性化诱饵来攻击个人。网络罪犯会寻找具有所需资历、技能集和访问级别的特定用户，然后发起针对这些用户权限的应用程序攻击。

如果用户的计算机遭受入侵，它通常被用作僵尸设备，在所有者不知情的情况下，对企业应用程序执行攻击，这些应用程序据称在防火墙后方是安全的。虽然大多数公司都使用 Web Application Firewall (WAF) 来保护面向外部的应用程序免受此类攻击，但许多公司尚未将此保护扩展到网络内部的企业应用程序。WAF 可以保护内部应用程序及其背后的数据免受应用程序层和注入攻击，例如 SQL 注入、恶意文件执行、跨站点请求伪造 (CSEF) 和跨站点脚本编写。

网络罪犯将以设备为目标，将其转变为僵尸机器，并利用它攻击防火墙后方被认为安全的应用程序。

在提供访问权限之前将身份、身份验证和授权安排到位

数字系统向输入正确密码的任何人授予访问权限，而不会验证此人员的身份。重复使用安全性较弱的凭据和密码显著增加了企业的攻击面和风险。在当今的威胁形势下，单单依赖用户名和密码等单因素身份验证显然不够。多重身份验证 (MFA) 提供了额外的验证和安全级别；它可确保仅经过验证的用户才能访问业务关键的应用程序。

多重身份验证是必不可少的。安全性较弱的凭据以及在应用程序中重复使用用户名和密码显著增加了企业的攻击面。

通过 MFA 对用户进行身份验证和授权后，单点登录 (SSO) 允许用户使用一组凭据登录所有应用程序。这提高了工作效率；无需重新确认每个应用程序的身份，也免除了跨应用程序的同步问题。根据诸多信号做出持续访问决策 — 包括跨 IaaS、本地和 SaaS 应用程序的 MFA 和 SSO — 在为最终用户提供便利的同时，也为企业带来了更出色的保护。

使用高级威胁防护抵御网络钓鱼、零日恶意软件和基于 DNS 的数据泄露

尽管公司广泛采用分层安全性，但恶意攻击者还是继续通过利用安全弱点来继续获得对企业数据的访问权限。即使部署了防火墙、安全的 Web 网关、沙盒、入侵防御系统和端点防病毒产品，相关企业也会遭受网络钓鱼、零日恶意软件和基于 DNS 的数据泄露，成为受害者。那么企业究竟缺少了什么呢？

DNS 是一个经常被忽略的向量。网络罪犯已经开发出专门用于利用这一安全漏洞的恶意软件，从而避开现有的安全层渗入网络并泄露数据。添加利用 DNS 协议的安全层至关重要；通过利用此初始查询阶段作为安全控制点，DNS 安全解决方案可以在击杀链中及早检测和阻止网络攻击，从而主动保护企业。

企业应利用 DNS 协议作为安全控制点，帮助在击杀链中及早检测和阻止网络攻击。

监视互联网流量和活动

企业必须假定环境是充满敌意的。这是 Zero Trust 的核心原则。因此，公司需致力于审核和确认所有活动，而不是盲目地允许。要做到这一点，企业需要了解其网络上发生的情况，需要有充足的流量和情报来进行相关比较。

企业必须监控和验证来自公司网络内外设备（无论是来自笔记本电脑、移动电话、台式机、平板电脑、访客 Wi-Fi 还是 IoT 设备）的所有 DNS 请求，确保查询不会指向恶意或不可接受的网站。公司还必须能够检查流量行为是否存在可疑活动的迹象，例如与命令和控制服务器通信或数据泄露，并即时向 IT 发出任何问题警报。对全局流量和威胁趋势的了解使 IT 更容易标记不规则或危险的模式。

支持通过 RESTful API 与安全信息与事件管理 (SIEM) 和编排集成

企业可能拥有数百甚至数千个应用程序。因此需要通过 API 进行配置，以便快速批量部署应用程序，同时设置访问策略控制。对于寻求从传统 VPN 访问快速迁移到特定于应用程序的访问的任何大规模应用程序环境而言，这是一项关键功能。随着企业采用 DevSecOps 并寻求可通过 RESTful API 执行的监视和配置任务，API 的采用率将继续提高。他们还需要插件将威胁和事件数据整合到 SIEM 中，以便开展进一步调查和关联。可扩展的系统还必须通过向第三方端点检测和响应解决方案发送信号，与工作流自动化平台和威胁纠正集成。

结论

数字转型是现实，企业必须采用 Zero Trust 安全模式，在不影响安全性的前提下成功发展业务，实现创新和灵活性。跨所有 SaaS、本地和 IaaS 应用程序的高级威胁防御、应用程序加速、MFA 和 SSO 是在 Zero Trust 环境中运行的一些重要优势。Zero Trust 安全模式通过 API 实现编排，并与 SIEM 和工作流自动化平台集成，从而提供有关用户和应用程序的可见性，同时又可在短时间内促进大规模部署。

Akamai 可帮助指导您的网络和安全发展。完成一个包含七个问题的 Zero Trust 评估，以了解您的企业为 Zero Trust 安全框架做好准备的程度。您将收到针对网络转型定制的后续步骤。或者，如需资源快速开始转型，请访问 akamai.com/3waystozerotrust。