白皮书

Zero Trust 架构构建蓝图

目录

前言

Zero Trust 的概念大约始于 2009 年，当时 Forrester Research 率先力推这一概念，并向企业发出了预警，指出应彻底改变传统模式，应避免向通过网络边界的任何用户或应用程序授予无限制的访问权限。他们指出，企业应先验证所有设备、用户和网络流，然后才能授予完全访问权限。在那之后的数年中，受多方面因素影响，采用 Zero Trust 概念的紧迫性日渐提升。

在当今混合工作模式下，员工可能在不同地点工作，而且自带设备 (BYOD) 计划也允许员工使用公司管理和非公司管理的设备访问公司应用程序和资源。应用程序可以托管在任何地方，即云端、本地或混合环境。这些变化的最终结果是，原有的网络边界已不复存在。勒索软件攻击的频率和复杂程度都在增长，攻击者突破防御机制的几率更高，一旦他们成功入侵，给企业造成的代价也更高。《2024 年 IBM 数据泄漏成本报告》中指出，美国的数据泄露平均代价全球最高，达到 936 万美元。此外，诸如物联网 (IoT) 设备等联网设备不断增长，合作伙伴和客户也对网络访问提出额外要求，在这些因素的共同作用之下，企业的攻击面显著扩大。

在这种不断发展演变的网络安全环境中，网络与安全软件供应商争先恐后地用 Zero Trust 宣传自己的现有产品，或推出相应新产品，顾问与分析师则纷纷推出新的缩略词和市场定义。这导致安全团队难以解读这些有时较为复杂的概念，难以做出购买决策，来为过渡到 Zero Trust 策略的举措铺设基础。

本白皮书旨在确定投资 Zero Trust 的切入点，并概述重要差异化因素，从而帮助安全团队规划投资这项技术的蓝图。

混合办公与云应用程序打破了既往的网络安全模式

人们工作的时间、方式和地点均已经突破了办公室的限制。

网络边界不复存在——至少不再是可辨识的形式。您的用户有可能位于众所周知的防御层之外，也有可能位于防御层之内，两种情况的可能性相当。他们所使用的软件即服务 (SaaS) 类应用程序和多云实施也在激增。面对技术尖端和持久不断的威胁，一旦攻击者侵入网络，您就极有可能在不经意之间将重要资产的完全访问权限授予这些入侵者。在攻击者进入您的网络之后，如果您不具备全面的 Zero Trust 计划，他们可能就会为所欲为。

这不仅仅是理论。近年来发生的影响广泛且代价高昂的数据泄露事件证明了这一点，其中大部分事件的原因就是网络边界内的信任滥用。

与此同时，有些应用程序设计部署在网络边界之内，它们的安全状态通常堪忧。毕竟，如果您是开发人员，并且认定只有经过授权的、善意的员工才会访问您的系统，那您的防御意识还会像如今的编码人员（知道大量黑客会尝试攻击基于互联网的应用程序）一样强吗?

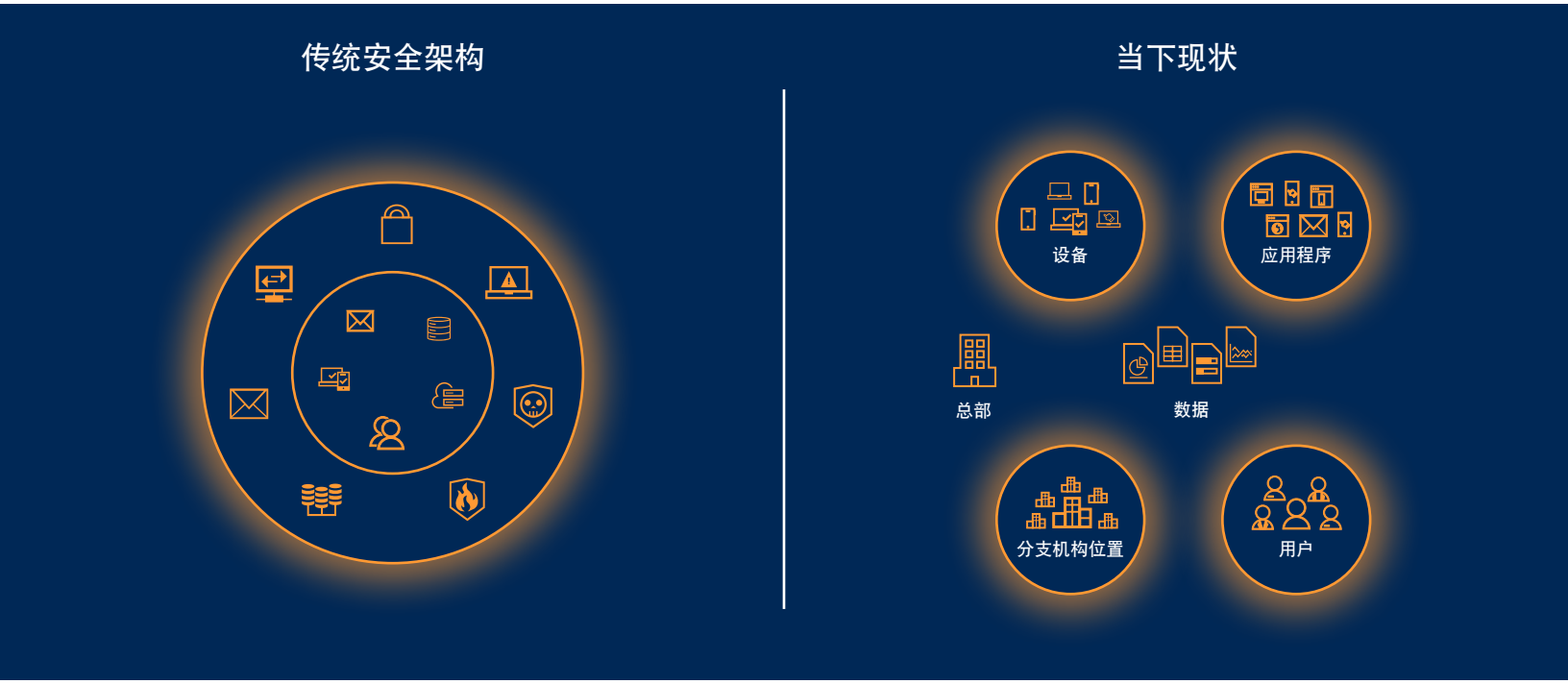
纵观整个市场，能应对这些挑战的解决方案就是 Zero Trust。

Zero Trust 安全架构

Zero Trust 背后的原理十分简单，但又无比强大：信任与位置无关。您不能仅仅因为某个东西位于您的防火墙之内便信任它。反之，无论是发生在何处的任何操作，只有获得明确许可的操作才能得到信任。最终，只有应该发生的操作才能够发生。企业需要消除对不必要操作的所有默示信任。例如，在只有少数用户需要财务系统访问权限时，为财务会计组中的所有用户授予访问权限会造成风险，而且毫无价值。

证明这一点的方法是强大的身份验证和授权，在建立信任之前，系统不应传输任何数据。此外，还应采用分析和日志记录来验证行为，并且持续监控入侵信号。

这种基本的转变在过去十年中抵御了大量入侵。攻击者无法再像以前一样，利用边界中的漏洞进入防御层以内，然后滥用您的敏感数据和应用程序。至此，防御层已经不复存在。只有应用程序和用户，每个应用程序或每位用户在访问发生前均必须相互验证身份并验证授权。



企业如何创建 Zero Trust 架构?

首先，所有企业都需要为其现有环境制定战略，并确定是否需要为其员工队伍招募新人才，以及何时需要这样做。该流程中的这一关键步骤可以用一整篇论文来专门论述，但有助于履行 Zero Trust 战略的实际产品应由三个目标推动。

1

不相信任何实体，始终需要验证。

这句话还可总结为更简单的说法：“从不相信，始终验证”。如果只是简单地隔绝对所有系统、所有数据的访问，您就相当于锁定了系统。真正的难点在于始终验证，但又不会造成重大业务中断，特别是考虑到大多数系统在设计时均以默示信任为前提。您需要广泛地监测并控制所有类型的访问，还需要简单且实用的方法来实施和维护策略。

2

完成验证后，确保提供尽可能少的访问权限。

在 Zero Trust 环境中，一旦用户通过验证，必须确保仅授予其角色所需要的访问权限。

3

持续监控威胁。

大多数业内专家都会告诉您，Zero Trust 是一种持续不间断的做法。在企图入侵企业防御时，攻击者采用的手法日渐复杂，企业必须持续监控、验证并限制访问权限。Zero Trust 模式有一种优势，它不关注攻击者在干什么，而是关注企业自身在做些什么。一旦实施了真正的 Zero Trust 策略，攻击者就很难一次性破坏您的业务运营所需的全部资源。理想情况下，您可以在攻击链上的某个点阻止每一次攻击。这也包括阻止未曾设想过的攻击的能力。您也不必考虑它是不是零日攻击，因为 Zero Trust 都能帮您抵御。

Zero Trust 不利的一面

但在企业开始实施 Zero Trust 时，还必须考虑到这种永不信任、限制访问权限的模式也有不利的一面。从根本上来说，Zero Trust 主要是使用拒绝列表来限制访问。这种做法明确指定了允许执行的操作；并且默认拒绝其他一切操作。这确实可以削弱攻击者从事恶意活动的能力，但往往也会增加意外地造成其他人无法正常工作的可能性。或者，反复核查工作负载和设备的做法可能会导致延迟积少成多，最终造成不满。如果 Zero Trust 策略造成用户无法有效完成工作，那就不具备可行性。

因此，强大的 Zero Trust 策略应该在安全性与顺畅访问之间取得平衡。它还需要在可以有效实现的目标与安全团队的资源（预算和人员）之间达成平衡。

Zero Trust 组成要素

从 Forrester 最初提出 Zero Trust 概念至今，已经过了 15 年。许多企业的 Zero Trust 之旅才刚刚起步，面临着错综复杂的软件产品市场。在这个市场中，有些产品已经发布多年，并着重满足 Zero Trust 架构特定部分的需求，还有许多新近涌现的新产品，更有许多软件提供商迅速采取行动，将其产品改头换面为 Zero Trust 产品。此外，许多分析师和行业观察家都会告诉您“Zero Trust 不是某一种产品，而是一种全方位的策略”以及“Zero Trust 并非终点，而是一段旅程”。但对于需要制定 Zero Trust 技术解决方案决策的买家而言，这些一再重复的声明并无帮助，甚至有可能让人更加迷茫。

由于没有单独一种产品能让企业实现 Zero Trust，而且每一家企业的优先事项和薄弱环节都有所不同，所以每家企业的起点都不尽相同。但由于技术的进步和行业的整合，企业如今可以从单一来源获得实施 Zero Trust 策略所需的多种工具。分析机构也开始认识到这一点。

Gartner 跟踪了所谓的安全服务边缘 (SSE)，也就是安全 Web 网关、云访问安全代理和 Zero Trust 网络访问 (ZTNA) 的组合。在《实施 Zero Trust 时需要启动的有效项目》报告中，Gartner 还纳入了微分段（他们称之为“工作负载之间的分段”），并给出了这样的建议：“如果企业希望有效实施 Zero Trust，则应关注两个主要项目：用户与应用程序之间的分段 (ZTNA) 以及工作负载之间的分段（基于身份的分段）。”

与其类似，IDC 则将 Zero Trust 归结为安全访问和分段，并将其定义为运用逻辑分段、访问控制和威胁检测来保护计算系统、资源和数据的各种新兴技术与传统技术所构成的综合视图。

但其核心挑战在于将这些彼此独立的系统整合起来，形成一种协调一致的策略。在构建适用的 Zero Trust 架构时，CIO、CISO 和其他安全专业人员应该关注哪些关键要素?

Zero Trust 网络访问

有时，人们会将 ZTNA 与 Zero Trust 的整体实现方法混为一谈，但 ZTNA 实际上是该技术堆栈的基础部分。在任何 Zero Trust 框架中，安全访问都是至关重要的初始步骤。遗憾的是，与该过程中的许多要素相似，这个步骤的复杂性很快就会超出预想。安全访问并不是二选一的决策。用户与应用程序的分布日渐广泛，在适当的时机，为适当的用户授予对适当应用程序的适当级别的访问权限，这变得愈加复杂。实际上，在对用户的确切定义中，现在还可以包括客户、供应商、合作伙伴和员工。与此同时，应用程序可能包括传统应用程序、SaaS 或移动应用程序，访问来源和访问目标涉及到数据中心、互联网或云环境。

有效的 ZTNA 解决方案将验证用户的身份及其设备的运行状况，并验证他们能否访问所需应用程序（无论用户位于何处），从而减少可能的受攻击区域，同时提高灵活性并改善监控。数十年来，企业一直依靠由身份提供商支持的虚拟专用网络 (VPN) 来提供访问权限。世易时移，面对当今分布式员工队伍的规模和范围，这些 VPN 已经力不从心。ZTNA 已取得长足发展，不仅能取代 VPN，还能根据用户及其设备的身份验证结果及多种属性（时间和日期、地理位置、设备安全状况等）来给予其适当的信任级别，进而授予访问权限。

选购 Zero Trust 网络访问解决方案时的考虑要点

随着企业开始使用更复杂的身份管理解决方案取代较为陈旧的 VPN，他们需要考虑多方面的因素。当今更为先进的解决方案应融合身份和访问管理、应用程序安全、多重身份验证 (MFA) 与单点登录，并通过单一界面提供管理监测能力与控制能力。对于致力于实施 Zero Trust 计划的企业，应选择既能满足当前需求，又能随业务而扩展的解决方案，从而帮助通过并购公司而获得的员工快速融入新环境、支持不同市场或地理位置的制造或生产、轻松增加和移除承包商以适应不断变化的业务需求，以及以颇具成本效益的方式将应用程序迁移到云端，同时保证不牺牲安全性。

理想的解决方案应能直接集成企业现有的身份基础架构，即使其中涉及到多家目录和身份服务提供商。这样，企业即可在不必更改现有身份基础架构或架构的前提下，快速部署 ZTNA 服务。

关注边缘

市面上的产品之间还存在一个至关重要的差异化因素，而 Zero Trust 采购团队可能会忽视这个重要考虑要点。整合边缘云平台的解决方案可充当身份感知代理，从而消除与边缘平台的连接，确保在远离数据中心的边缘完成所有身份验证，给企业带来额外的优势。有些企业采用的是在 DMZ 内运行的访问代理架构，但这种方案无法利用云的能力来更好地吸收攻击、提供缓存带宽，以及按需自动扩缩。

在云端构建的身份感知代理可以按需扩缩，运行 CPU 密集型资源，并有效吸收攻击。此外，这种方案基于私有 IP 地址，无法直接通过互联网访问。对性能和安全最为敏感的活动发生在最靠近最终用户的边缘。此外，进入应用程序的敏感进入路径使用了反向应用程序隧道，这有效去除了边界的 IP 可见性，并降低了流量攻击的风险。

> **整合边缘云平台的解决方案可以充当身份感知代理，从而为企业提供额外的优势。**

构建 Zero Trust 蓝图时关于多重身份验证的考虑要点

随着混合办公方式的兴起，人们需要更好的访问能力，这已经促使大多数企业采纳了 MFA，并实施了某种解决方案。但有必要认识到，企业级访问与 MFA 有着一加一大于二的协同效应。MFA 要求您拥有密码以外的验证因素，并因此成为信任概念的核心。密码保护是最常被滥用的信用区域之一，所以您要设第二道验证，以免身受其害。此外也要谨记，并非所有的 MFA 解决方案都一般无二。

在评估要纳入 Zero Trust 策略的 MFA 解决方案时，企业应寻找具有如下特点的解决方案：

- 集成身份管理和企业访问
- 符合 FIDO2 标准，可确保用户凭据在用户个人设备上得到分散、隔离和加密，这对于抵御网络钓鱼攻击尤为重要
- 支持通过智能手机验证用户身份，而无需依赖物理密钥

微分段

Zero Trust 没有完美状态可言。最顽固的攻击者可能会发现其中的漏洞，并利用其发起攻击，这不可避免。因此，任何综合性的 Zero Trust 方法都需要微分段。当今的大多数网络都没有分段，或者仅有极少的分段。企业传统上使用防火墙来保护其关键应用程序，但出于多方面的原因，这种方案的实施难度实际并不小。从根本上来说，防火墙要求实施网络策略，而这会形成瓶颈点。您的网络连接需要穿过防火墙，这不仅会快速增加防火墙的成本，而且防火墙还存在两个问题，其一，现代网络流量中的很多风险它都难以察觉；其二，它更改起来难度极高。许多企业都在纷纷改用基于软件的微分段，这种方案能简化许多劳动密集型流程。

微分段领域的差异化因素

微分段是任何 Zero Trust 计划的核心要求，但通常会与核心 ZTNA 解决方案分别考量。微分段解决方案的销售形式不一，有些提供商将其纳入安全平台进行销售，还有些则将其作为独立解决方案销售，买家需要清楚其中的一些核心差异。

我能将它部署到哪里？如果微分段解决方案的构建初衷是用作网络工具，而没有采用安全至上的方法，并且微分段解决方案是专为本地环境而构建的，潜在买家就要提起警惕了。当今的工具应该能部署到云端、本地环境、设备上（包括无法安装代理的设备）以及混合环境中的容器内。这通常就需要基于云的软件。如果微分段解决方案只能为您环境中 80% 的部分提供支持，那么就不足以发挥实效。

它提供了多强的监测能力？微分段解决方案会限制访问，但过多的限制可能会妨碍业务流程，引发 COO 的关切。微分段要求深入了解您的环境。哪些服务器可以访问哪些服务器？您能否定义某个 Kubernetes 集群与某台 Windows 2008 服务器之间的策略？许多攻击都不具备向下兼容至 2008 版本的代理，也不具备在 Kubernetes 上实施策略这种前瞻性理念。为了有效地部署 Zero Trust，微分段软件必须能够应对这些复杂性。

此外，微分段软件买家需要考虑产品要支持的策略的精细程度。大多数系统都会在应用层实施覆盖不同端口和进程的策略。更精密的产品可能会在微服务层实施策略。例如，攻击者可能会利用某些 svchost 服务（例如任务调度器）在整个网络中横向移动。但 svchost 本身有着太多重要作用，企业不能彻底将其阻止。此时，能够在微服务层实施策略的微分段解决方案就有了用武之地。

实施难度如何？表示当下需要的策略的难度如何？同样重要的是，满足未来需求的难度如何？对于任何微分段解决方案而言，这都应该是核心考虑要点。无论您正处于规划阶段，还是您的环境出现了需要防守的威胁，都要确保您投资购买的引擎能轻松支持这两类策略。

在实施微分段项目时，从允许列表入手可能会让安全团队感到紧张不安，因为这种方法存在错误地拒绝必要的应用程序或服务的风险。复杂的微分段解决方案应该附带拒绝列表模板，并且可供团队快速轻松地部署拒绝列表，从而为项目实现某些速效方案。在实现这些方案之后，企业即可继续推进这一旅程，迈向采用允许列表的全面防护方案，在其中纳入准确的依赖关系和有上下文的清单映射功能。

> 如果微分段解决方案的构建初衷是用作网络工具，而没有采用安全至上的方法，并且微分段解决方案是专为本地环境而构建的，潜在买家就要提起警惕了。

DNS 防火墙

在 Zero Trust 环境中，不被信任的不只有用户，还有互联网本身。员工需要访问互联网，随着 SaaS 和移动应用程序、云服务、混合办公和 IoT 设备的普及，企业的攻击面也在扩大。保护企业和用户免受恶意软件、勒索软件、网络钓鱼、数据外泄等等威胁的侵扰变得越发困难。企业资源有限，不足以管理安全控制点的复杂性以及传统本地解决方案的安全漏洞。

如果要在个人与互联网之间实施 Zero Trust，就需要一种 DNS 防火墙，并使其成为任何 Zero Trust 计划的核心要素。

DNS 防火墙投资的核心 Zero Trust 要求

投资购买 DNS 防火墙虽然看似简单，但技术买家仍需考虑一些要求。许多企业已经部署了本地 DNS 防火墙，但现在需要将它的保护范围扩大到可能身处任何位置的用户。与身份管理类似，具备强大边缘平台的提供商能通过扩展平台获得相应的威胁情报，因此往往具备更强大的 DNS 安全保护能力。决策者应仔细考量这些核心要求。

DNS 检查。提供商应能根据复杂的威胁情报实时检查所有网域，并自动阻止恶意网域。解决方案还需要对所有端口和协议有效，这样才能抵御不使用标准 Web 端口和协议的恶意软件。不同提供商的 DNS 检查质量千差万别，买家应寻找市场中具备丰富经验和客户成功往绩的提供商。

保护所有设备。提供商应该为网络内外使用的所有设备安装代理，例如笔记本电脑、智能手机和平板电脑。

灵活的 DNS 接入。提供商应该能采用多种方法将 DNS 请求转发到 DNS 防火墙，以实现超高的灵活性并涵盖所有用例。

DNS 数据泄露识别与阻止。DNS 数据泄露，尤其是低吞吐量的数据泄露，可以让攻击者通过 DNS 通道窃取敏感数据。在寻找提供商时，应关注他们是否具备根据专有检测算法来进行内联和脱机 DNS 渗透检测的能力。

威胁监控

Zero Trust 核心技术的最后一个要素是威胁监控。尽管 Zero Trust 会假设一切都不可信，但企业需要保持警惕，确保发现正在进行和初露苗头的攻击，以及潜在风险（如配置不当或过度授予的访问权限）。在安全团队评估市面上的软件时，应该审视有效威胁监控的如下三个要点。

关键考虑要点

有效的算法

任何威胁监控服务都应包含精密的算法，这种算法在根据用户和网络活动异常、可执行文件分析、日志分析等因素制定决策方面应具备成功往绩。

强大的信号检测

软件和人工智能是威胁监控的重要工具，但 Zero Trust 决策者仍应评估与其合作的供应商的内部专业实力。威胁监控服务需要能区分好的信号与坏的信号，从而帮助避免警报疲劳，并提供任何事件的即时通知。包含高调攻击活动分析的定期报告也是企业应该关注的一个方面。

经验丰富的员工

团队成员应该具有广泛的背景，包括攻击、事件响应和数据科学，并且应该可以全天候待命。在这个领域，内容交付提供商可以提供实质性的额外优势。因为此类供应商每秒监测数百 TB 的流量，并从中获得宝贵洞见，这能给任何信号检测提供独特的视角。

从何处入手?

Zero Trust 计划永远没有“完成”可言，因此对于考虑相关软件、硬件和招聘要求的人员而言，首要问题往往是：“应该从何种技术入手？”

与许多事情一样，答案取决于各公司的具体需求、风险评估结果以及相对优势和劣势。许多行业观察家给出的回答是首先实施 ZTNA。确实如此，保护企业免受恶意南北流量的侵袭不失为精明的起点。但也有人认为，东西向微分段方法（特别是软件定义的东西向微分段）要更为理想。

从微分段入手的理由

大多数专家都认为防御总有漏洞，恶意攻击不可能彻底避免，如果您也认同这种观点，那么您必定希望保护自己的重要资产。这就是微分段的意义所在。企业不愿开始实施微分段方案的原因之一在于，他们认为这种方案非常复杂。

首先，微分段并非“要么全面实施，要么完全不实施”的方法。与 Zero Trust 本身一样，它可以分阶段实施。企业可以首先确定自己的重要资产。关注点应放在真正关键的资产上。应该确保在系统遭到入侵时，您的业务不会因此而中断。资产的重要性可以根据资产内的数据判断，也可以根据现有保护级别判断。

许多情况下，您都希望微分段解决方案能够涵盖您的传统系统，因为这些系统运行的常常是业务关键应用程序，并且特别容易遭受攻击。但是，有些微分段解决方案并不能保护这些传统系统。

其次，软件定义的微分段可消除企业认定的大部分复杂难题。您不需要处理硬件，也不需要一再地联系网络架构师和安全架构师。您要做的只是部署软件，这大大降低了入门的门槛。

微分段计划一旦启动，就能立竿见影地获得初步的好处，而这有助于推动后续项目。例如，您现在可以获得环境中动态的事实来源，而且是立即获得，甚至不需要实施策略。而在您实施策略之后，您就能很好地理解通信流的来龙去脉。此外，在企业启用应用程序围栏之后，您可以快速轻松地锁定关键应用程序，仅允许其通过特定端口和进程进行通信。

或者，针对特定威胁的策略可用作速效方案。精密的微分段平台应具备内置的拒绝列表。这样，您就可以快速创建策略，阻止远程桌面服务与互联网之间的不必要连接。例如，企业可以快速消除导致 Colonial Pipeline 攻击的漏洞。

无论起点如何，在任何持续进行的 Zero Trust 旅程中，平衡都是要义。无论身份管理有多出色，如果分段不善或者 Web 访问保护能力不尽人意，也无法实现良好的安全性。

平台与专用工具的对比

就像许多技术决策一样，在制定购买 Zero Trust 软件的决策时，最终要在独立专用工具与整合多个组件的平台之间做出选择。考虑到 Zero Trust 对安全团队、集成人员、架构师和分析师的影响，以及这些人员在多个控制台、多个不同的代理和多种集成之间维护策略的需要，平台是一种令人信服的方案。在人力市场紧张、娴熟的网络安全专业人员稀缺的现状下，平台方案尤具优势。管理多家供应商的解决方案可能会显著增加人力成本，因为彼此之间无法有效通信的解决方案会造成误报，而这会给最终用户加重负担，并且可能需要额外的支持与培训。

此外，在涉及到支持和合同谈判时，如果只需与单一人员联系，这绝对是与平台提供商合作实施 Zero Trust 的一个重大优势。

您应该寻找一家具有灵活方法的单一供应商——既能提供 Zero Trust 的综合平台，也能提供独立的单点产品。这种灵活性让您既能更轻松地实现 Zero Trust 架构，又能享受单一供应商带来的便捷性。

> **企业不愿开始实施微分段方案的原因之一在于，他们认为这种方案非常复杂。**

重新审视 Zero Trust 组成要素

知道您的用户是谁。
确保其经过验证。

保护您的资产。
对所有交易进行身份验证/授权。

保护您的用户。
防止恶意软件感染用户。

结论

大多数关注网络攻击防御的企业最终都会认识到，他们需要尽早采取行动来转向 Zero Trust 架构。面对远程办公的兴起，很多公司已经踏上 Zero Trust 之旅，有些采取渐进的做法，有些则更为激进。但随着攻击者愈发老练、威胁面愈加广泛、需要远程访问的员工日益增多，对于协同工作的全面解决方案组合的需求必然会只增不减。

如需具体了解 Akamai Zero Trust 方法的特定要素，欢迎访问 akamai.com/solutions/security/zero-trust-security 或咨询我们的专家。

Akamai 安全解决方案简介

Akamai 安全解决方案可为推动业务发展的应用程序提供全方位安全防护，而且不影响性能或客户体验。诚邀您与我们合作，利用我们规模庞大的全球平台以及出色的威胁监测能力，防范、检测和抵御网络威胁，帮助您建立品牌信任度并实现您的愿景。如需详细了解 Akamai 的云计算、安全和内容交付解决方案，请访问 akamai.com 和 akamai.com/blog，或者扫描下方二维码，关注我们的微信公众号。发布时间：2024 年 10 月。

扫码关注，获取最新云计算、云安全与CDN前沿资讯