Akamai | TechnologyAdvice

微分段对于商业行业的 Zero Trust 安全模式至关重要

零售、旅游和酒店行业的商企成为企图利用敏感公司数据或财务数据进行牟利的网络犯罪分子、勒索软件团伙及欺诈者垂涎的目标。根据《RH-ISAC 行业洞察报告》(RH-ISAC Industry Insights Report)，被窃取的最常见信息类型包括信用卡和付款信息、奖励或会员计划中的个人身份信息 (PII) 以及知识产权。

这些企业已经进入攻击者的视线，其安全团队必须解决网络中的大量潜在入侵点，以阻止攻击者部署勒索软件以及其他类型的恶意软件。虽然所有企业都要面对网络钓鱼电子邮件、VPN 凭据被盗以及零日漏洞利用等威胁所造成的影响，但是很多商企还必须管理售货亭、物联网设备、店内平板电脑、POS 终端、访客 Wi-Fi 等带来的额外风险！此外，每个零售点必须对公众开门营业，这使公司还要面临物理攻击面和各种其他威胁，进一步增加了复杂性。

有利可图的数据和不计其数的攻击媒介迫使企业的防御者增加投入，以预防人为错误——这是导致事故发生的主要原因，高达 82% 的安全事故都是人为错误所致。支付卡行业 (PCI) 或政府法规（GDPR、SEC 等）的监管审查愈加严格，这让本已捉襟见肘的 IT 安全预算和资源雪上加霜。

虽然不可能避开所有的风险，但现在的商企必须采取“假设发生入侵”的思维模式，以迅速发现无法避免的感染或者绕过边界防御措施的行为，防止进一步扩散。利用 Akamai 的 Zero Trust 分段解决方案，商业企业可以更轻松、快速地保护其应用程序、服务器和网络环境，并防止攻击者对敏感数据进行破坏性加密和泄露。

微分段是一种最适合由软件定义方法提供支持的功能，它是为商企实现三项关键功能的 Zero Trust 安全框架的重要基石。首先，微分段天生就能通过阻止横向移动，限制感染勒索软件带来的潜在影响。其次，它会帮助减少实现和维持 PCI 合规性所需的费用。最后，微分段能够提供所需要的精细监测能力和覆盖范围，以保护分布在混合、多云和微服务环境以及传统基础架构之中，技术先进但也更复杂的现代化生态系统。

限制勒索软件造成的潜在影响

点击电子邮件网络钓鱼链接、安全配置错误、开放的 RDP 端口或被盗的凭据经通常会给攻击者打开方便之门，让他们能够在准备好实施勒索软件攻击时开始探索网络，搜寻贵企业最重要的资产。那些沦为大规模加密事件受害者的企业，可能会因数据外泄而遭受双重勒索：即遭受多层面的经济损失以及业务损害。

这可能会立即造成**直接业务损失**，因为在线订单和店铺运营会变得速度缓慢或陷入停滞，导致客户无法购买商品或者预订酒店或机票。电商运营可能无法对现有订单进行处理、履单或发货，因为关键系统和服务器无法访问或被迫下线以试图限制攻击的蔓延。

如果敏感的公司或客户数据遭到泄露，**间接业务损失**首先会让公司在大众面前颜面尽失，品牌声誉受损。勒索软件团伙最喜欢使用的一种策略是在“点名羞辱”网站上公布攻击并泄漏数据作为证据，进一步勒索受害者并向其施加压力以成功获得赎金。此外，根据美国证券交易委员近期发布的要求，企业还必须在四天内向其上报事件对业务造成的的实质性影响（这可能会成为头条新闻）和声誉受损情况。

法律费用、事件响应、数据取证以及直接与勒索软件攻击后恢复工作相关的安全漏洞修复的**恢复成本**将会非常高昂，因为顾问和 IT 团队需要努力恢复数据、恢复备份并让系统重新上线。然而，因敏感信息泄露而造成的诉讼费用或监管罚款可能比上述恢复成本还要更高。网络保险保费可能会大幅增加，勒索软件索赔请求可能遭拒，保单可能被完全取消。

网络攻击非常猖獗，因此勒索软件攻击被视为 2024 年零售和酒店业首席信息安全官们面临的头号风险隐患，并且安全负责人已准备好在控制措施方面加大投资，以帮助降低攻击者入侵后四处扩散的风险，便不足为奇了。但是，要想让勒索软件进行传播，攻击者必须能够在获得初始访问权限后进行转向和横向移动才能实现影响最大化。2022 年微软数字防御报告指出，93% 的勒索软件事件都是由于横向移动控制措施不足造成的，这使得攻击者能够锁定关键应用程序和基础架构，并且该报告还指出攻击者从企业网络内的某个端点开始横向移动的平均时间仅为 1 小时 42 分钟。

Akamai 的最新分段现状数据指出，与其他行业相比，电商企业在过去 12 个月内报告的勒索软件攻击次数最高。正是出于此原因，首席信息安全官们和安全专家正在转为采用基于 Zero Trust 的安全工具（例如微分段），以降低勒索软件成功感染的风险、最大限度地减小攻击面并“打破”勒索软件杀伤链。

通过发现并阻止攻击者利用横向移动进行探索，他们将难以访问需要升级权限才能访问的 IT 资产，难以找到敏感信息以及进行大规模的勒索软件攻击。通过对整个商业基础架构中的关键工作负载应用最小访问权限原则，Akamai 备受分析机构认可的微分段解决方案可深入监测应用程序和工作负载的东西向数据流，并通过软件定义策略实现精细化保护，以立即限制横向移动和阻止攻击者的行动。

甚至优秀的网络保险公司也清楚微分段的价值。由于勒索软件促使投保量和索赔量的激增，很多保险公司不得不提高安全控制措施的要求和严加审查，提高保费（有时保费同比涨价高达 96%），以及降低赎金支付保额的上限以应对重大损失。有些企业甚至因保费过高无力投保，或被完全拒保。虽然仅依靠网络保险无法阻止破坏性的入侵和所产生的经济影响，但微分段之类的安全控制措施能够让企业更轻松地满足最新的承保要求。

“借助设备上部署的单个代理程序，我们已经彻底解决了通过横向移动发起端点攻击的问题。”

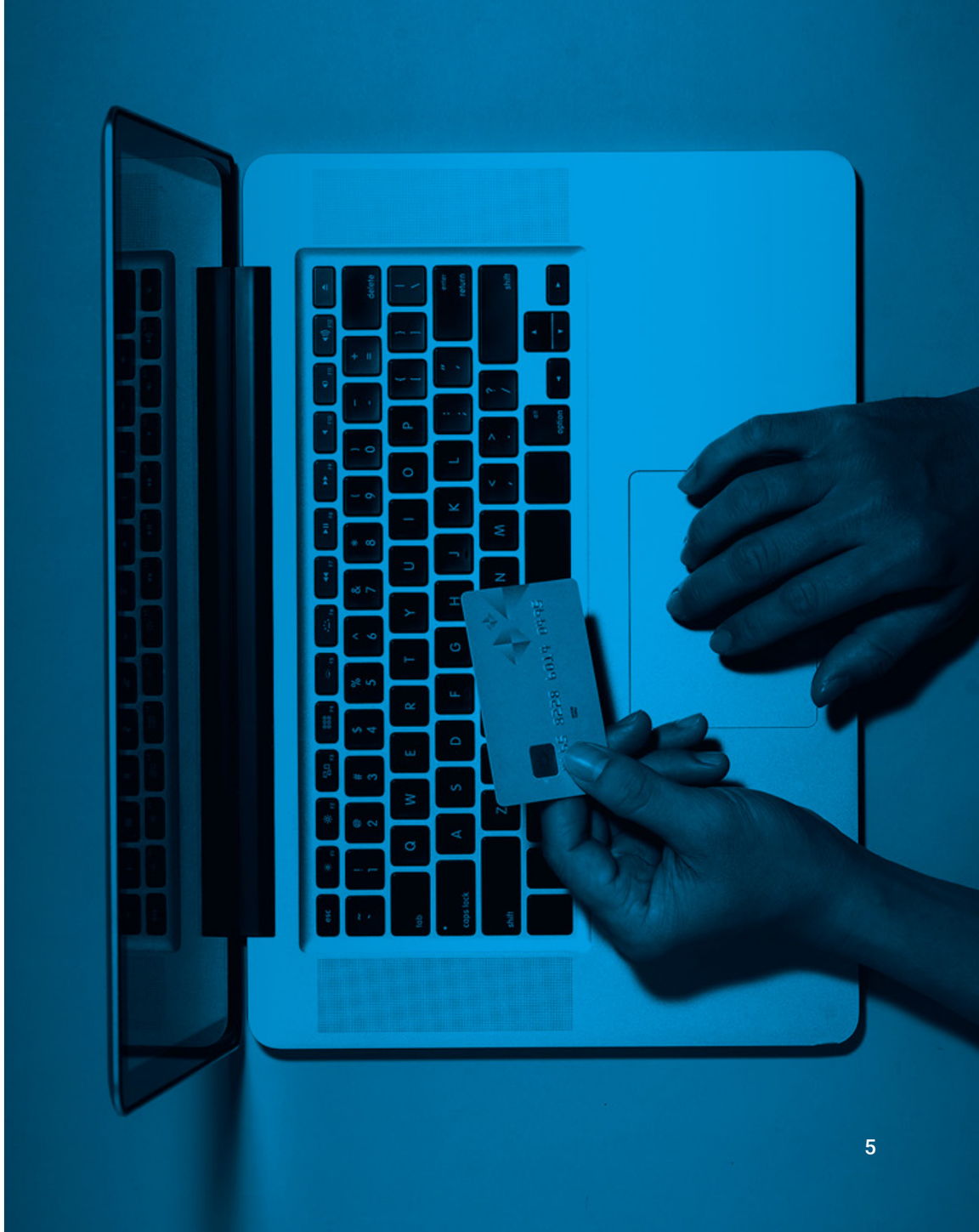
某全球零售与消费品制造商
基础架构架构师

缩少 PCI 合规审核范围

电商企业都很清楚，实现和保持 PCI 合规性所需成本占年度治理、风险和合规性预算的大头，会给安全全职员工和资源带来沉重负担。PCI 数据安全标准 (PCI DSS) 要求对安全策略和控制措施开展持续审计，以保护持卡人数据环境 (CDE)。PCI 范围界定是指确定与持卡人数据 (CHD) 进行交互或可能会影响这些数据的安全性的人员、流程和技术，此要求也会显著增加 PCI 审计相关的成本。

虽然 PCI DSS 没有正式要求必须进行网络分段，但商企多年以来一直在使用传统的网络分段方法（例如，vLAN、ACL 和内部防火墙）来帮助减少保持合规性的范围、成本、风险和难度。但是，随着现代零售企业的 IT 环境在混合、多云和微服务架构中变得更加动态，传统分段技术和方法无法跟上步伐，导致运营开销、复杂性和应用程序停机时间以及安全漏洞增加。

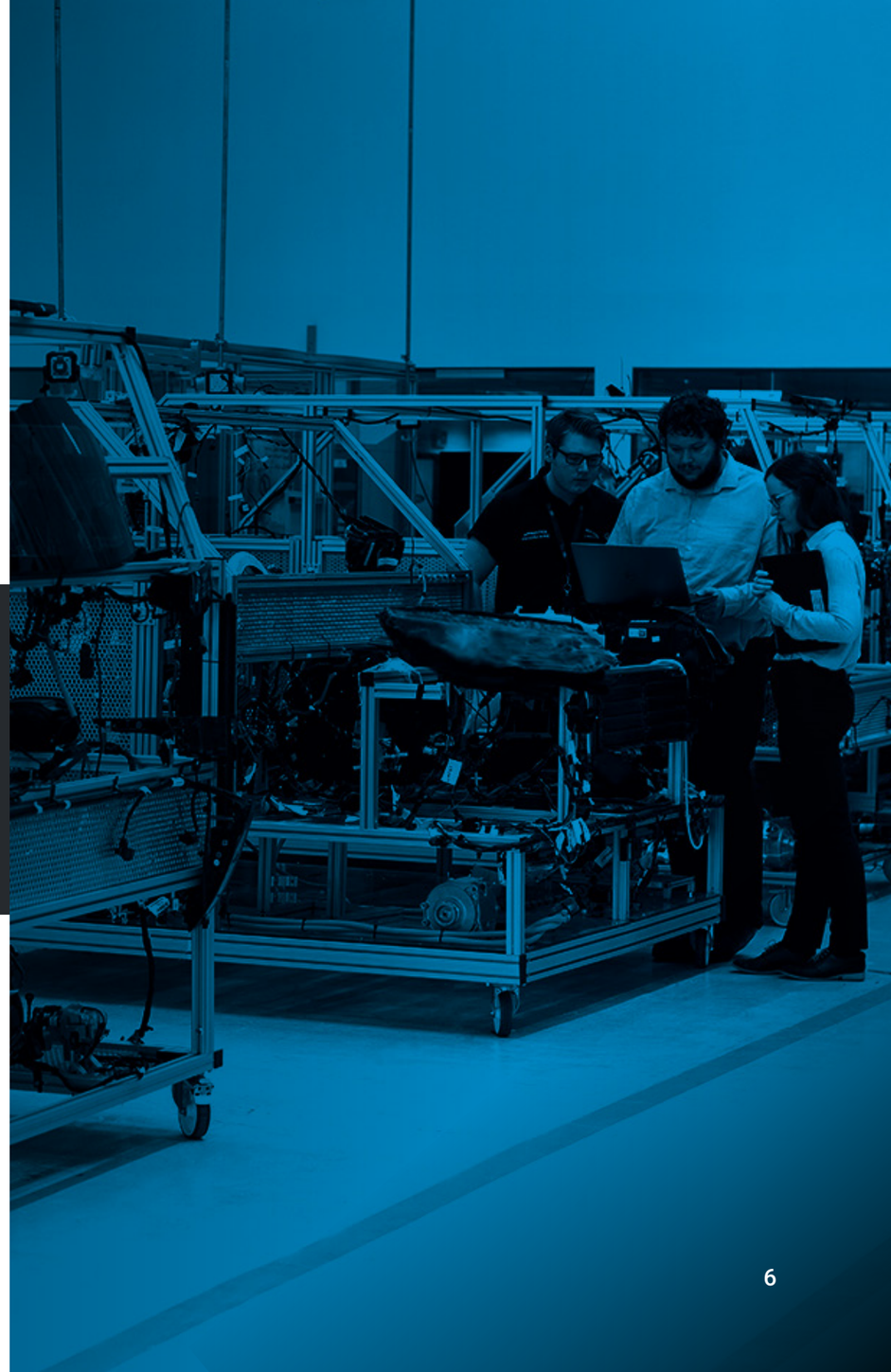
这是因为传统分段方法难以管理和维护，需要消耗资源来确保 CDE 边界内的系统、网络和应用程序都得到了妥善保护和控制。随着企业运营从数据中心和云转向基于容器的资产，很多企业都缺少对应用程序和系统通信流的全面监测能力，并且难以保持 PCI 要求的防火墙配置标准。



这会导致出现糟糕的分段做法，从而产生安全漏洞并造成 PCI 审计失败。正是出于此原因，商企正在转为使用软件定义的分段，以便更轻松地在基础架构中强制隔离 CDE 与范围外的系统，缩小 PCI 审计的范围，并通过在最高达到进程第 7 层（这远超出了传统功能可以支持的范围）的层级启用分段和实施来加快实现合规。Akamai 的轻量级代理不需要防火墙或更改网络，也不需要重新启动服务器，并独立于底层基础架构运行，这意味着不需要任何应用程序中断运行，也无需更改控制或维护窗口。

由于软件定义的分段会将安全措施与底层基础架构和操作系统分离，因此可以独立执行分段，而不影响网络或应用程序。通过此方法，商企可以利用充当分布式状态检测防火墙的解决方案，在各种环境中进行精细的网络和资产监测以实现全面覆盖。由于部署和管理所需的工作及资源更少，并且 SecOps 生产率大约提高 95%，因此企业能够增强安全态势，同时避免 PCI 合规性带来的很多难题。不仅如此，我们的解决方案能够让商企在审计过程中利用网络的实时视图和历史视图来验证合规性。

> “软件定义的分段使我们能够在进程级别创建和实施分段策略，从而显著改善安全态势并提高满足 PCI-DSS 技术要求的能力。”
>
> The Honey Baked Ham 公司高级基础架构工程师



实现监测能力以及从物联网到传统基础架构的全面覆盖

从阻止勒索软件的传播到管理 PCI 合规性安全控制措施，商企还需要面对保护实体场所（例如实体店、生产设施和配送仓库）安全的额外复杂性。对于航空公司来说，物联网传感器和设备可以对飞机系统进行实时监控和预测性维护，从而提升性能和安全性。酒店企业可部署依托物联网的设备来打造专为提升客户体验和运营效率而设计的智能酒店客房。

显然，这些场所和环境很多都包含不计其数的物联网 (IoT) 或运营技术 (OT) 资产，这些资产无法运行基于主机的安全代理，使它们更容易出现硬件和软件漏洞。Forrester 的《2023 年物联网安全状况报告》(The State of IoT Security, 2023) 指出，33% 的全球安全高级负责人认为物联网设备是外部网络攻击的头号目标。因此，企业需要部署具有无代理功能的分段解决方案以保护物联网和运营技术环境，并最大限度地降低攻击者利用设备漏洞试图访问更广泛的 IT 基础架构的风险。

此类解决方案必须能够持续监控新连接的设备，并自动阻止未经批准的设备与网络进行通信。通过集成的设备指纹技术，Akamai 的解决方案可以自动发现已连接的设备并将其分类为多个逻辑组，从而为可扩展的抽象安全策略奠定基础。可以通过一个统一界面为物联网和运营技术设备创建分段策略，并且与其他策略一样，这些策略将跟踪带指纹的设备，而不管这些设备位于何处（即使设备漫游到新的网络位置），也不管环境中的设备有多少。

基于 Zero Trust 的策略会通过网络交换机 ACL 进行实施而无需使用代理，从而消除了可能会在物联网和运营技术部署中产生风险的实施漏洞。虽然建立了这些安全边界，但仍然允许和 IT 管理系统、专用更新服务器及日志记录服务器建立必要的连接，以减少安全阻碍。利用我们的解决方案，您可以发现、监测和映射所有物联网及运营技术系统以及您的 IT 基础架构，从而获得企业资产的单一视图。

除了保护物联网/运营技术资产及其他物理隔离的端点之外，很多零售企业都极其依赖于在旧版或停止提供支持的操作系统和基础架构上运行的系统、服务器和应用程序，这些操作系统和基础架构无法安装补丁，从而造成重大风险。其中的很多旧版服务器都无法移除，因为它们还在为企业带来收入或依然是企业的骨干系统，那些不是“诞生于云端”的电商企业尤其面临这一难题。Akamai 的代理有着行业领先的广泛覆盖范围和兼容性，可在现代操作系统和旧版操作系统上运行，能够对 Windows 和 Linux 操作系统的网络流进行全面的进程级和服务级监测，监测范围还可以覆盖 MacOS 端点。

其他解决方案仅对旧版操作系统提供部分监测能力，无法监测 Windows Server 2008 R2 之前的 Microsoft Windows 系统。这是因为传统微分段解决方案代理依赖于 Windows 防火墙实施策略，而该防火墙功能从 Windows 2002 版之后的系统才开始提供。Linux 系统的代理仅支持第 4 层监测能力，没有适用于 Linux 环境的第 7 层进程级规则，而且该系统依赖于 iptables 来实施策略。Akamai Guardicore Segmentation 功能几乎在所有 Windows 和 Linux 操作系统（无论新版系统还是旧版系统）上都受支持，因为我们的解决方案不依赖于底层基础架构就能正常工作。

简单、快速、直观——并且更安全

从总部到零售店，从数据中心到云端，以及其他方面，微分段对于采用 Zero Trust 来保障和保护关键 IT 资产来说至关重要。

与速度较慢的传统网络分段方法相比，Akamai Guardicore Segmentation 的简单性显著减少了部署和实施、监控及事件响应所需的时间和工作。对策略的任何更改都可以快速实施，而不需要进行复杂的网络更改，这在销售旺季、促销、产品发布或其他备受瞩目的活动期间至关重要。

结论：就像您不会让自己的客户、宾客或乘客在质量与安全性之间做出取舍一样，优秀的微分段解决方案也不会让您在安全性与敏捷性之间做选择题。现在，停止这种困难的分段方式的时机已成熟。

想要了解更多信息?

了解如何利用 Akamai Zero Trust 产品组合中的 Akamai Guardicore Segmentation 来减小您的攻击面、保护关键的应用程序以及简化合规性。

了解更多

TechnologyAdvice | Akamai

扫码关注，获取最新CDN前沿资讯

无论您在何处构建内容，以及将它们分发到何处，Akamai 都能在您创建的一切内容和体验中融入安全屏障，从而保护您的客户体验、员工、系统和数据。我们的平台能够监测全球威胁，这使得我们可以灵活调整和增强您的安全格局，让您可以实现 Zero Trust、阻止勒索软件、保护应用程序和 API 或抵御 DDoS 攻击，进而信心十足地持续创新、发展和转型。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。