AKAMAI 解决方案简介

借助 Akamai Guardicore Segmentation，Deloitte 的事件响应和勒索软件抵御能力如虎添翼

客户面临的挑战

传统成熟的安全产品类别常会承诺针对企业网络所面临的新型威胁提供更高级别的防范能力。但是，很少有解决方案能够提供全面、单一的解决方法，通过防止恶意横向移动来减少攻击面——无论此类横向移动涉及的是本地硬件、云端工作负载、最终用户设备还是容器，皆可有效防御。此外，由于存在技术限制且分析师专业知识有限，企业客户历来需要数月甚至数年的时间才能完成初始的 Zero Trust 分段计划，以便一旦攻击绕过传统防火墙、EDR 等成熟的安全产品防护，企业客户能够有效地阻断攻击。

在实施分段项目的过程中，企业客户通常会面临以下挑战：

- 缺乏在所有环境中监测所有资产、网络流量、用户和连接的能力
- 对不同技术和基础架构（例如混合云基础架构、传统操作系统和 OT/物联网）的安全控制措施有限
- 需要通过避免常与传统分段技术相伴的停机问题，确保业务连续性
- 缺乏能够构建、部署和管理 Zero Trust 支持计划的安全资源和人才

解决方案要点

Akamai Guardicore Segmentation 是一种基于主机的微分段解决方案，为在网络中实施 Zero Trust 原则提供了简单、快速和直观的方式。Akamai Guardicore Segmentation 使用了一系列基于代理的传感器、基于网络的数据收集器和虚拟私有云流量日志来绘制您的网络图，旨在通过单一直观界面来监控您的所有资产和基础架构，包括传统和现代操作系统、运营技术和物联网设备。然后，您便可轻松创建和实施相关策略以限制不必要的通信，同时减少攻击面并确保业务连续性。

主要的应用场景

- **东西向流量控制**
  隔离不需要进行通信的环境、应用程序、用户和基础架构
- **勒索软件抵御**
  利用 AI/ML 部署策略模板，阻止已知被各类勒索软件攻击所利用的攻击路径
- **应用程序安全围栏**
  重点保护关键业务应用程序的特定依赖关系，以实施严密的安全控制措施

- **基于用户的分段**
  阻止用户访问非工作必需的应用程序、环境和设备
- **受感染设备隔离**
  在一台或多台设备被感染后，控制攻击的传播范围
- **合规性**
  凭借对您的网络、设备和潜在攻击路径全面深入的了解，在收到通知后迅速证明合规性

为客户带来的好处

- 通过单一管理平台监测您的整个网络和所有连接（其中涉及服务器、端点、云、容器、用户等），化解监测能力方面的挑战
- 实施 Zero Trust 策略，降低勒索软件攻击得逞的可能性
- 利用威胁情报以及全面的入侵检测和欺骗功能，缩短事件响应时间
- 利用实时数据和历史记录功能，简化网络取证和合规项目

Deloitte 专业知识

1. **咨询**
   Deloitte 在颇具影响力的网络安全决策支持、安全漏洞分析和实施路线图创建方面拥有丰富的经验，无论是在入侵事件发生期间还是制定面向未来的规划时，都可以确保企业客户做出明智的决策
2. **专业服务**
   您可以享受到全托管实施服务，以及与现有安全、ITSM 和云解决方案的定制集成
3. **事件响应托管服务**
   即时享受 Deloitte 事件响应策略专家提供的周到服务，以控制入侵态势并帮助预防未来发生类似事件
4. **许可证订阅**
   Deloitte 提供了多种可供选购的许可证订阅服务

客户案例研究——Akamai 和 Deloitte 如何化解客户面临的勒索软件挑战

重大勒索软件攻击事件层出不穷，客户迫切需要能够在关键时刻迅速提供帮助的咨询服务和解决方案。Deloitte 事件响应和安全团队的实力配上 Akamai Guardicore Segmentation 提供的网络监测能力、入侵取证以及显著减少攻击面的后续措施，为客户带来了一种制胜的组合方案。

背景

以一家大型企业为例，他们曾经遭遇过一次重大勒索软件攻击，攻击者攻陷了他们的核心业务运营中心，而他们甚至都不知道从何处着手去解决这个问题。他们的整个数据中心被攻陷，数以千计的服务器被接管，因此他们需要立即采用安全的方法来控制入侵态势。这家客户选择了信任 Deloitte 的指导，来电询问下一步应该怎么做。在使用了 Deloitte 团队精心提供和部署的 Akamai Guardicore Segmentation 后，该客户能够快速监测攻击范围，了解哪些资产和应用程序已受到影响，并且了解了所有相关应用程序的依赖关系。

解决方案

通过深入分析该客户的整个环境并细化到单个进程级别，Akamai Guardicore Segmentation 能够发现恶意软件为了从所入侵的基础架构开展攻击而可能会利用的所有潜在路线，使 Deloitte 团队可以重点关注特定的网络部分，进而获得额外的取证分析能力。这有助于确保在客户恢复业务运营及其数据中心访问之后，不会存在漏网的受感染设备。

成果

在勒索软件攻击得到解决、数据中心重新上线并且业务运营恢复正常之后，该客户还采取了措施以降低此类攻击再次发生的可能性。与其他许多大型企业客户一样，该客户使用了分层安全方法，并且部署了多种优秀的解决方案，希望能够保护其设备、应用程序和用户等等。但是，类似网络钓鱼电子邮件这样极其简单的手段就能为攻击者打开突破口，仅仅依靠这些解决方案还不足以阻止攻击。在全面了解自己的网络、应用程序依赖关系以及有权访问数据中心的用户之后，该客户能够实施精准的微分段控制措施，从而大大减少了未来勒索软件入侵有可能会利用的路线。

在该客户体验到这种解决方案的价值并且增加了对 Deloitte 专业知识的信任之后，他们便决定部署该解决方案以继续实施 Zero Trust 分段，并请求 Deloitte 为他们提供该技术的日常管理。

总结

Deloitte 拥有深厚的技术专业知识，并在 Zero Trust 项目的执行当中为客户带来了出色的体验，使其在为客户部署和管理 Akamai Guardicore Segmentation 方面成为了一家理想的合作伙伴。在任何包含减少攻击面、控制横向移动、应用程序安全围栏或抵御勒索软件的安全计划中，客户都可以依靠 Deloitte 来充分利用分段技术。

关于 Deloitte

Deloitte 面向全球知名品牌提供卓越的审计、税务和咨询服务，其客户既包括财富 500® 强中将近 90% 的企业，也包括 7,000 多家私营公司。我们的员工秉持精益求精的精神，助力各行各业推动当今市场蓬勃发展。我们在资本市场创造的可衡量且可持续的成果深受公众信赖，激励客户在挑战当中把握转型和发展的机遇，并与我们一同打造更强大的经济和更健康的社区。Deloitte 很荣幸能成为大型全球专业服务网络的一员，为专注于在市场中谋求发展的客户提供优质服务。我们以超过 175 年的服务经验为基础打造了成员单位网络，覆盖 150 多个国家和地区。敬请访问 deloitte.com，了解 Deloitte 遍布全球的约 415,000 名员工如何共创影响力。

联系方式

Ola Sergatchov
Akamai 全球战略联盟负责人
osergatc@akamai.com