Akamai

白皮书

保护现代律师事务所

为关键应用程序和客户数据保驾护航

简介

法律专业人士每天都会处理敏感数据。考虑到这一点，很多公司会在更先进的安全控制措施上进行投资，并集中精力围绕 Zero Trust 概念设计其 IT 系统和流程，以保护其关键应用程序并控制最终用户访问权限。

Zero Trust 方法实现了一个具有最低特权的模型，可确保授权用户、系统和应用程序只拥有与其各自职责相对应的访问权限，同时还可以防范横向移动、勒索软件和未经授权的访问。在实施 Zero Trust 方法时，最灵活且最安全的方法之一是使用微分段。

为了理解这一点的重要性，我们将先来回顾一些历史事件。

备受瞩目的数据泄露事件：为法律行业敲响警钟

多年以来，美国联邦当局一直警告称，大型律师事务所极易成为网络犯罪分子的攻击目标，因为它们拥有信息丰富的公司数据存储库。FBI 开始警告一些著名的律师事务所，称早在 2009 年他们便成为有组织网络犯罪分子的目标。2011 年，他们甚至邀请了 200 家规模很大的律师事务所参与讨论针对该领域的复杂网络攻击不断增加的问题。

> **在实施 Zero Trust 方法时，最灵活且最安全的方法之一是使用微分段。**

据 Law.com 报道，从 2014 年开始，14 个州超过 100 家律师事务所发生了数据泄露。美国律师协会的《法律技术调查报告》是一份探讨法律行业内技术应用现状的年度调查报告，其 2022 年度报告发现，超过四分之一的律师事务所（各种规模）都遇到过安全漏洞问题。安全漏洞的影响包括勒索软件导致的停机以及客户数据在互联网上曝光后旷日持久的法律纠纷。

2015 年，法律领域首次出现在 Cisco 发布的黑客攻击目标行业年度排名中。因此，很多金融机构在与律师事务所开展业务合作时开始要求后者对其网络安全实践进行定期审核。

尤其是国际律师事务所 Mossack Fonseca & Co 和 DLA Piper 的两次大规模数据泄露事件，更是为整个法律和金融行业敲响了警钟。在名为“巴拿马文件”的泄露事件中，超过 1100 万份、时间跨度长达四十余年的文档从离岸律师事务所 Mossack Fonseca & Co 被泄露。这次数据泄露事件导致避税天堂曝光，多家全球化公司和有影响力的各国首脑的离岸账户遭到泄露，造成了严重的后果。2018 年，该律师事务所宣布停业，主要原因便是此次泄露事件产生的后果。律师事务所承担着道德和受托责任，必须尽一切合理努力保护所持有的信息。“巴拿马文件”数据泄露事件是迄今为止律师事务所与客户之间最大的机密信息泄露事件，促进了整个行业网络安全方法的变革。但是，尽管新成立的公司专注于增强安全态势，但攻击者并未展露出放缓攻击的迹象。

> **超过四分之一的律师事务所都遇到过安全漏洞问题。**
>
> — 美国律师协会《2022 年度法律技术调查报告》

几乎在 Mossack Fonseca & Co 泄露事件发生的同时，DLA Piper 成为 NotPetya 恶意软件攻击的受害者，这是全球著名的一家律师事务所，在超过 40 个国家或地区设有办事处的。这次攻击导致该律师事务所在数周内处于业务中断状态，业务损失、恢复成本高达数百万，而且公司声誉严重受损。

最近，Grubman Shire Meiselas & Sacks 遭受勒索软件击并丢失 756 GB 的高端客户群数据，其中包括 Lady Gaga、LeBron James 和 Madonna 等知名人士的数据。该律师事务所不愿意支付赎金，导致攻击者泄露 Lady Gaga 的相关信息，并对据称是包含其他客户详细信息的数据进行拍卖。

现代律师事务所：
实施现代网络安全解决方案刻不容缓

所述的大多数数据泄露事件都与高级持续威胁 (APT) 攻击相关，这些攻击包括网络钓鱼、恶意软件和勒索软件，它们会窃取敏感的客户数据、合并材料、知识产权和金融信息。在巨额金钱的诱惑下，有组织的犯罪团伙不惜砸下重金对攻击工具和专业团队进行投资，不断增强对攻击者的支持。

> **在发生数据泄露事件时，IT 环境中缺少合理分段的律师事务所会面临保险公司拒绝赔付的风险。**

现在，在决定与哪家律师事务所进行业务合作时，更多的客户将网络安全视为一项重要因素。与已采取措施增强其安全态势并展示对保护客户数据的承诺的律师事务所相比，缺少现代安全控制措施的律师事务所更可能丢掉业务。此外，很多网络保险公司现在要求对敏感数据和应用程序进行某种形式的分段。在发生数据泄露事件时，IT 环境中缺少合理分段的律师事务所会面临保险公司拒绝赔付的风险。

缺少了什么：
保护律师事务所的关键应用程序

正如您所看到的，律师事务所已不再是秘密资料的安全存储场所。现在，网络犯罪分子将律师事务所视为存放网络安全攻击所觊觎的专有和敏感公司数据的宝库。

实际上，与其大多数客户相比，律师事务所常常被视为更容易攻击的目标。正因为如此，想要从某个公司获取特定数据的攻击者通常会先尝试通过该公司的律师事务所获取这些数据。律师事务所存储的都是涉密信息且种类繁多，再加上它们的安全控制措施通常比较薄弱，因而成为攻击者眼中利润丰厚的目标。

攻击者对律师事务所的业务关键应用程序中存储的信息有着令人难以置信的兴趣，尤其是文档管理系统 (DMS) 和电子邮件应用程序中的信息。从 IT 安全角度来看，律师事务所最关键的业务应用程序是其 DMS 和电子邮件应用程序。这些应用程序中存放着最有价值的高度机密和敏感的私密客户信息，并且在很多情况下，它们都并非仅驻留在本地数据中心。

DMS 应用程序提供了广泛的功能，包括文件和文件夹的集中式组织管理、版本管理、电子邮件管理、文档编辑、索引编制和搜索、权限管理等。它们通常部署在混合有虚拟服务器和裸机服务器的多种类 IT 环境中，并且需要与内部安全级别不同的多个其他系统进行集成。尽管这样的集成可以加大 DMS 对律师事务所的作用，但也会降低安全性并显著扩大其攻击面。

此外，端点的移动性和动态性日益增强，而传统安全解决方案常常无法保护端点，因为和很多企业一样，律师事务所将其安全工具投资主要集中在边界上。这些解决方案提供的保护级别无法再满足律师事务所对保护关键应用程序的需求。另外，现实情况是，在攻击者通过被入侵的端点访问网络后，很多律师事务所仍然缺少检测或阻止攻击者进行横向移动以及访问敏感数据系统所必需的控制措施。

考虑到所有这些挑战，很多现代律师事务所现在开始着手投资，部署能够满足其不断变化的独特需求的新一代网络安全解决方案。基于软件的分段，特别是微分段，可通过提供更精细的方法来控制网络内的通信，以仅允许授权用户和系统与关键应用程序进行通信的方式，支持以 Zero Trust 方法保护关键应用程序和数据。这使得攻击者更加难以在您的网络中进行横向移动，进而限制了潜在入侵的作用范围。

新冠疫情让事情变得更加困难：

- 很多律师事务所转为远程办公
- 出于此原因，员工们不再从其公司办公室连接到网络，而是从不安全的家庭网络进行连接
- VPN 和 VDI 解决方案的使用日益增加，让实施安全策略以及将网络流量限制为授权用户变得更加困难

Akamai 帮助律师事务所保护客户数据的四种方式

全面监测能力

全面监测工作负载，以了解与存放敏感数据的应用程序的所有开放连接。

用户访问控制

实施对应用程序和数据的访问权限进行控制的策略，而不必考虑它驻留在本地还是云端。

基于软件的分段

对 DMS 和电子邮件等关键应用程序进行快速、灵活的微分段，以降低发生入侵事件时的暴露风险。

威胁检测和预防

将动态分段和拦截功能相结合，以检测和限制主动入侵并保护客户数据。

借助 Akamai Guardicore Segmentation 实现统一保护

Akamai Guardicore Segmentation 提供用于保护业务关键应用程序的全面微分段解决方案。它极大地加快了分段策略的实施速度，简化了持续维护，并且能够更加有效地抵御依赖横向移动才能取得成功的威胁。

> 为了更好地保护客户数据，很多律师事务所开始转为使用微分段之类的解决方案来实施更精细的方法，以控制网络内的通信，从而仅允许授权用户和系统与关键应用程序进行通信。

我们的解决方案提供了数据中心内所有应用程序和其他资产的可视化示意图，同时还列明了它们的依赖关系。安全运营商可以快速、直观地创建和实施网络及进程级安全策略，以便对其关键应用程序和资产进行隔离与分段。此软件定义的分段方法与底层基础架构无关，使得它能够跨本地系统（传统和现代）、虚拟机、容器、云和设备对工作负载提供一致的保护。

可以围绕单个或逻辑分组的应用程序创建策略，而不必考虑它们驻留在数据中心中的什么位置。这些策略规定哪些应用程序可以相互通信，哪些应用程序不能，从而为 Zero Trust 方法提供支持。Akamai Guardicore Segmentation 的另一项重要专属功能是我们的集成化入侵检测和响应，它可以降低管理多个专用工具的复杂性。必须具备入侵检测和响应能力，才符合纽约州金融服务部门 (DFS) 的法规和 PCI DSS 等其他行业强制规范的要求，并且这也是高端客户在审核其律师事务所时的硬性指标。

Akamai Guardicore Segmentation：对关键应用程序的全面保护

保护客户数据：在日益复杂并且联系日益紧密的环境中，为 Zero Trust 框架奠定基础并实施网络安全机制和最佳实践。

将关键应用程序与更广泛的 IT 基础架构分隔开来：利用安全围栏策略对高价值资产（例如，DMS 或电子邮件应用程序）进行分隔，降低暴露在来自律师事务所内部和外部的威胁中的风险。

安全、快速地采用云技术：绘制工作负载图，并在迁移前列出所有关键应用程序及其依赖关系的清单。安全围栏策略使用这些图作为在整个迁移流程中与工作负载关联的一致安全性的基础。利用此方法，可以更快、更安全地将工作负载迁移到云端，从而确保实施相同的安全控制措施。

借助高效的入侵抵御措施确保业务连续性：使用高精度监测能力监测东西向流量，并且将入侵指示器设置为在发现异常移动时发出报警，从而在勒索软件或其他威胁导致业务中断前阻止攻击者。

通过限制横向移动来降低风险：设置内部边界并为业务关键应用程序和系统建立安全围栏，以减小攻击面。这样可以有效地防止攻击横向传播，降低发生入侵事件时造成的损害。

结论

Akamai Guardicore Segmentation 为律师事务所提供了一个解决方案，让他们能够监测并了解可能会被攻击所利用的开放连接。此外，借助该解决方案，律师事务所还能够使用微分段保护这些连接。

我们的解决方案可以跨混合 IT 环境地为驻留在虚拟机和裸机上的以及本地、IaaS 或 PaaS 中的律师事务所关键应用程序提供全面安全保障。它提供对应用程序依赖关系和流量的监测能力、精细的分段策略实施以及集成化入侵检测和响应。这些功能对于避免可能导致业务中断的数据丢失和业务中断情境至关重要。

使用 Akamai Guardicore Segmentation 的律师事务所能够更好地了解其环境并保护其关键应用程序，还能够显著减少发生入侵事件时的影响并缩短响应时间。此外，与很多其他分段解决方案（例如，传统防火墙）中的分段功能相比，我们所提供的基于软件的分段功能更加经济高效、耗时更少、更加灵活并且更加有效。总之，Akamai Guardicore Segmentation 是业界领先的安全解决方案，功能完善，可以应对现代律师事务所的安全挑战。

了解如何能够保护客户的宝贵数据。如需了解更多详情，请访问 akamai.com/guardicore。

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 的安全、计算及交付解决方案，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：2023 年 7 月。

扫码关注，获取最新CDN前沿资讯