白皮书

利用基于软件的分段消除网络安全障碍

Akamai Guardicore Segmentation 帮助欧洲金融业优化安全措施，并降低网络风险造成的代价

概述

金融业是欧盟经济的重要组成部分，一些欧洲政府和监管机构将金融体系视作关键基础设施。金融服务企业提供的产品和服务高度依赖于高可用性的 IT 系统，以及及时访问通过多种渠道、多个相关方交付的信息的能力。

但勒索软件和加密挖矿攻击表明，攻击者可以迅速造成这一关键基础设施瘫痪数天乃至数周，甚至可能会波及关联的第三方和同行。

为了追求竞争优势、争取客户和留住客户，欧洲金融机构必须采用先进的数字化技术。然而，监管机构对于安全控制措施和报告的要求不断提高，严重拖慢了云技术的采用速度。例如，根据欧盟《通用数据保护条例》(GDPR) 的规定，未能妥善保护客户的公司可能需要缴纳罚款，最高可达到其全球营业额的 4%。[1]

此外，环球银行金融电信协会客户安全计划 (SWIFT CSP) 和欧洲中央银行网络韧性监管预期 (ECB CROE) 等近期出台的规定都明确要求进行更精细的网络分段。

传统分段方法及其相关的人工程序已然不合时宜，无法跟上技术创新的步伐，也难以应对安全风险增加和法规不断收紧的局面。

企业不仅需要采用新工具，还需要从根本上改变其安全和分段流程，从而实现简单化、透明化和自动化。

本文内容包括：

- 欧洲金融业目前面临的主要网络安全挑战
- 银行和金融机构如何通过经济高效、简单直观的分段方法应对这些风险
- Akamai Guardicore Segmentation 的方法如何帮助企业简化安全流程、显著降低成本并加速实现合规

当今的网络安全格局错综复杂、管理成本高昂

在保证企业安全、保护客户数据方面，欧洲的银行和金融机构不遗余力。但在当今世界中，风险、第三方访问需求和合规要求不断发展变化，增强安全态势绝非易事。

更高的网络风险造成更重大的金钱损失

网络犯罪给金融机构造成的相关风险尤为严重。在所有行业中，金融业用于抵御攻击的支出目前位居第二，每次数据泄露的平均损失为 572 万美元。[2]

然而，实现强大的安全态势也需要付出高昂的成本。在实施安全控制措施时，企业不仅要保护多个平台，还要保护对商业服务的履行至关重要的第三方访问能力，然而，这是一项相当复杂的任务，更伴随着基础架构与人力成本的大幅增加。

合规成本上升

欧洲金融服务企业在为合规性做准备和执行验证方面所需的成本、时间和总体资源用量急剧增加。虽然法规有助于确保金融业的稳定性，但不断实行的新网络安全要求会拖慢数字化转型的速度，并且需要大量投资，而这会影响到盈利能力与增长。

收紧政策的压力不断增加，在首先颁布 GDPR 之后，欧洲相继又出台了《网络与信息系统安全指令》(NIS)、《欧洲中央银行 CROE 指南》以及最近的《欧盟网络安全法案》。再加上 SWIFT CSP 等供应商要求，要在当今环境中实现合规性，就要满足大量的报告和技术要求。

因此，在进行技术升级的同时，银行和金融机构还需要设法简化管理，降低与网络安全和合规性相关的运营成本。

第三方和金融市场互动的安全漏洞

欧盟的修订版《支付服务指令》(PSD2) 旨在给用户提供更高的便利度和透明度，但也增加了第三方访问和个人数据泄露的风险。金融服务同行和监管机构也在不断向金融机构施压，要求其提高业务和技术流程的效率与透明度。

客户对于安全性、移动性和新服务提出了更多要求，导致金融机构对第三方信息和通信技术基础架构、外包提供商及其供应链的依赖程度不断提高。

由于环境的互连互通程度远胜以往，保护所有类型的通信（包括自动化的银行间和银行内交易）已成为一项资源密集型工作。

现在，只要有一方数据中心遭遇一次入侵，就可能引发多米诺骨牌效应，因为攻击者只要成功利用一项资产就能在彼此关联的各方（包括同业金融机构和金融市场）之间横向移动，从而给整个欧洲金融服务生态系统的安全性和业务连续性造成风险。

混合云要求采用新的安全方法

合规性要求以及欧洲银行管理局[3]颁布的各项指导方针正在改变金融业对云技术的采用趋势。在欧洲，云技术的采用呈上升趋势，但相关法规增加了本地系统上云之旅的复杂性。

正因如此，欧洲企业更倾向于将核心职能保留在本地环境中，并采用混合云环境，而非纯云环境。许多银行也开始与多家云服务提供商合作，从而形成了多云基础架构。

然而，企业寻求的通常不只是提高安全性。他们还希望改变流程，从而节约成本、提高运营效率。自动化和流程现代化已成为成功的关键。

通过网络监测能力和分段应对关键网络安全挑战

在这些挑战中，贯穿着一个共同的主题：需要安全地隔离关键应用程序与工作负载，这就是我们常说的“分段”。这让金融机构能够根据业务需求大规模实现安全性，并展示符合监管要求的基于风险的方法。

传统防火墙并非应对之法

有几个原因造成欧洲银行和金融机构未能更广泛地采用和部署分段。

维护工作量和资源耗用量：许多安全和 IT 专业人员对分段计划的实施犹豫不决，认为这些计划耗时过长，而且需要占用多支团队和大量资源。这种犹豫完全可以理解，因为传统方法大多复杂且耗时。例如，在多个地点和环境配置 VLAN、ACL 和防火墙往往费力、缓慢且容易出错。此外，传统方法在很大程度上依赖于不可靠的身份数据（如 IP 地址），这些数据往往意义不大并且变动频率很高。

缺乏监测能力：由于缺乏对东西向流量的监测能力，企业进一步受到阻碍，难以确定分段间的依赖关系，也难以制定不会破坏关键组件的分段规则。即使使用流量监听或类似技术，所生成的视图也往往缺乏 IP 与端口之间所需的上下文和复杂转换。在平台即服务 (PaaS) 等动态环境中，这几乎不可能。

基础架构依赖关系：工作负载扩展到云端的情况越来越普遍，这一流程也变得愈加复杂。在每个数据出口点都安装硬件防火墙的成本过于高昂。复杂的网络配置带来了更多管理挑战。除了云计算和容器之外，还需要这些配置来满足具有虚拟化或传统资产的多元化环境的需求。

> “在某些领域，监管制度难以跟上技术创新的步伐，企业的风险管理和控制框架也同样较为落后”。
>
> ——《2023 年金融市场监管展望》(Financial Markets Regulatory Outlook 2023)，德勤 EMEA 地区监管战略中心

从根本上改变流程

即使是拥有数百台服务器的中型金融服务企业，也可能会产生数千个分段策略明细项。手动管理的效率低下，特别是在使用 Jenkins 和 CI/CD 循环等工具进行自动化应用程序交付的环境中。在此类环境中，上下文至关重要。

正因如此，Akamai Guardicore Segmentation 能够更进一步，帮助企业将策略创建和更新周期从基本手动流程转变为自动化流程。

利用 Akamai Guardicore Segmentation，只要应用程序的剖析实现自动化，并且理清了所有依赖关系，规则的创建和更新就能变成一种可重复的流程，而利益相关者和应用程序所有者仅需批准自动生成的策略。这几乎消除了人工干预的需要（人工干预可能会大大拖慢项目进度），并降低了配置不当和人为失误的风险。

自动化规则创建可以保持规则结构的一致性和策略本身的可扩展性，从而带来优化程度更高的防火墙。

加速 IT 转型，打造真正的 Zero Trust 环境

金融机构不该任由人工流程和有限的资源阻碍其实现大规模分段。真正的 Zero Trust 不仅需要正确的技术，还需要安全策略创建、更改和维护流程的现代化。

基于主机或软件的防火墙已成为应用程序级安全的一种直接且经济的方法。这种方法显著加快了实施速度、简化了持续维护，最终能够更有效地抵御威胁。从最初构建起，Akamai Guardicore Segmentation 的目标就是帮助各种规模的企业实现简单、经济、快速的分段。

它提供了数据中心所有应用程序及其依赖关系的可视化映射图。然后，安全操作员可以创建并实施网络和单个进程级的安全策略，从而对关键应用程序和资产实现隔离和分段。这种软件定义式叠加方法独立于底层基础架构，可保护覆盖本地传统系统、虚拟机、容器、云等环境的工作负载。您可围绕单个应用程序或按照应用程序逻辑分组创建策略，无论其位于何处。这些策略规定了哪些组件可以相互通信，哪些组件不能相互通信，为 Zero Trust 安全方法奠定了基础。

有效降低网络风险和成本

金融机构在使用 Akamai Guardicore Segmentation 后发现，他们可以在很短的时间内解决一些迫在眉睫的安全问题，同时降低成本：

在日益复杂、相互关联的环境中，实施网络安全机制和最佳实践，**降低网络风险造成的代价**。

通过精细的上下文监测和分段策略**简化合规性管理**，从而快速映射和隔离与合规性相关的资产和关键业务应用程序。通过使用单一管理平台方法，金融机构可以合理地证明其正在采取措施保护关键资产、降低欺诈风险，并保护客户隐私。

借助基于身份的分段，隔离并限制用户经过网络，对第三方流量实施路由，从而**确保安全的第三方访问**。这加强了第三方与金融市场交互的安全性，防止攻击者从另一个遭遇入侵的系统“登陆并扩展”。

将转账和支付系统与常规 IT 系统隔离开来，以满足电子转账和支付系统（特别是 SWIFT）的要求，进而将 SWIFT 服务与机构的一般 IT 环境严格隔离开来。通过精细分段，银行 IT 团队可围绕服务提供商的“分区”，设置基于上下文（用户、网域）的边界，从而进一步限制未经授权的访问。

在迁移之前，映射工作负载并清点所有关键应用程序及其依赖关系，从而**安全、快速地迁移到云**。隔离策略可将这些映射作为基础，在整个迁移过程中保持工作负载的一致安全性。这种方法可以实现更快、更安全的云迁移，且无论应用程序或基础架构如何变化，都能让安全控制机制保持不变。

通过东西向流量和入侵指标的精细监测能力，在发生异常移动时发出警报，在攻击者外泄敏感的财务和客户数据之前阻止他们，从而**有效抵御入侵，确保业务连续性**。

通过限制横向移动来降低风险。当今数据中心的大部分流量均为应用程序之间的横向移动流量（东西向流量），而非从外部传入数据中心的流量（南北向流量）。通过关键业务应用程序和系统的围栏设置内部边界，从而有效缩小攻击面、防止攻击横向扩散，并在发生入侵时限制损失。

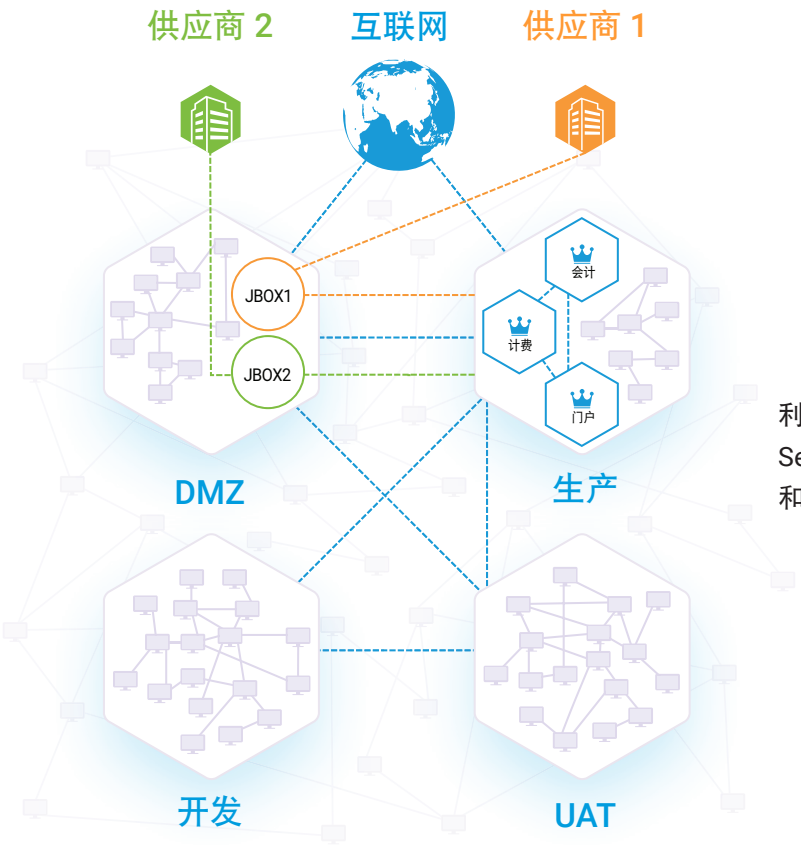
案例研究：
某大型欧洲跨国银行降低合规成本

某大型欧洲银行正在寻找一种高效的新网络分段方法，以满足多个监管机构的技术要求，包括纽约联邦储备银行 (FRBNY)、新加坡金融管理局 (MAS)、欧洲中央银行 (ECB) 等。

该银行使用过传统的分段方法、防火墙规则和 VLAN，但事实证明这套方案的效果并不理想，导致每年的违规成本居高不下。此外，创建和更新策略所需的大量生产停机时间和资源也给 IT 运营造成了影响。

为了实现银行的分段目标，需要找到一种更经济高效、易于实施的方法。对于新解决方案，关键要求是确保对银行基础架构和资源的影响最小，同时还要完全符合相关法规。

在对多家供应商进行全面评估后，该银行的基础架构和 IT 安全团队中的决策者达成了共识：Akamai Guardicore Segmentation 为实现微分段提供了迅速、直接的途径。



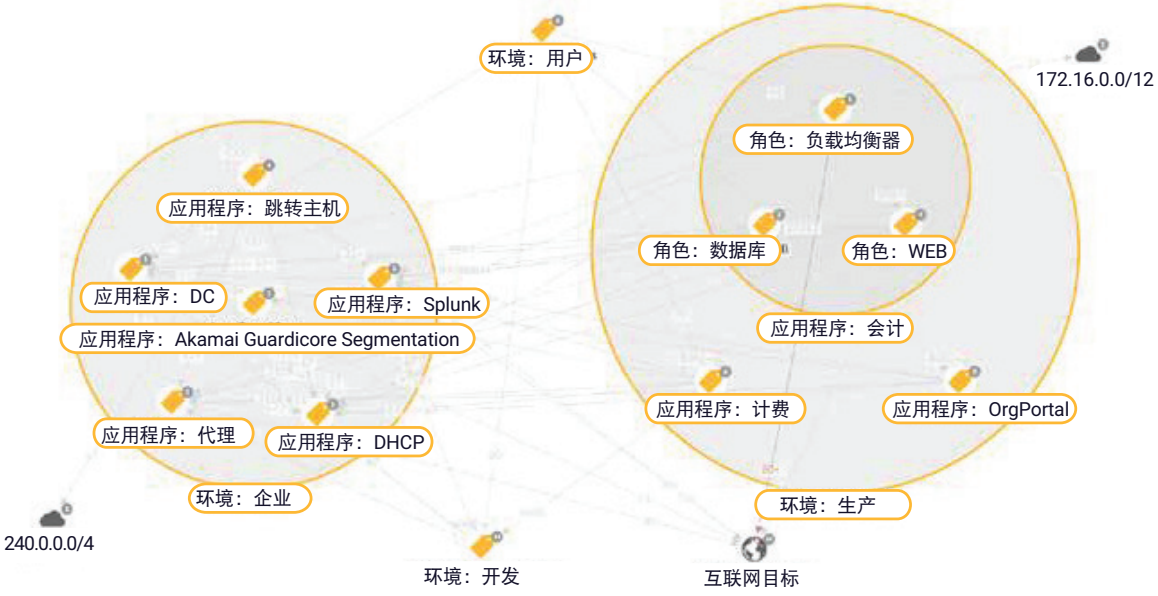
利用 Akamai Guardicore Segmentation 实现环境分段和第三方访问控制

简化和加速分段

该银行在多个地区和多种 IT 基础架构中部署了 Akamai Guardicore Segmentation 解决方案（包括容器）。由于不需要更改应用程序，因此在生产环境中未造成停机。它还使该银行能够迅速实现针对数据中心工作负载的集中监测，并隔离生产、测试和开发环境。通过使用 Akamai Guardicore Segmentation，客户还能限制打印机、其他物联网设备和未经授权的用户对服务器的访问。

在不到三个月的时间里，该项目便顺利完成。相比最初使用传统分段方法时的预估速度，该项目的完成速度是前者的 10 倍。通过快速规划环境并根据收集的信息创建策略，该银行改善了安全态势，并使超过 10000 个不合规的资产满足了合规要求。快速完成的部署降低了风险，还显著节省了成本和资源。

Akamai 的专业服务团队帮助该银行全面改造了其分段流程。如今，资产标签和分段策略能够以全自动的方式执行，并嵌入到应用程序开发和部署流程中。标签创建、变更管理、安全事件和服务请求已完全集成到了 ServiceNow 工作流程中。该平台带来的结果、所提供的价值以及 Akamai 技能娴熟且专注的技术服务团队令客户感到非常满意。



如需了解有关 Akamai Guardicore Segmentation 的更多信息，请访问 akamai.com/guardicore

1 《有哪些 GDPR 罚款？》(What are the GDPR Fines?)，GDPR.eu，2019 年 2 月 13 日。

2 《2022 年数据泄露造成的代价》(Cost of a data breach 2022)，IBM。

3 《欧洲银行业云技术采用综合指南》(A comprehensive guide to cloud adoption in Europe's banking sector)，Techerati，2019 年 10 月 31 日。

Akamai 可在您创建的一切内容和体验中融入安全性——无论您在何处进行构建，将其分发到何处，从而保护您的客户体验、员工、系统和数据。我们的平台具备监测全球威胁的能力，这让我们得以帮您调整并增强安全状况，从而实现 Zero Trust、阻止勒索软件、保护应用程序和 API 或抵御 DDoS 攻击，让您信心十足地不断创新、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 06 月。

扫码关注，获取最新CDN前沿资讯