AKAMAI 解决方案简介

# 机密计算：保护使用中的数据

当下，各种安全威胁的范围和规模不断扩大，其复杂程度亦持续提升。对于这些挑战，尤其是在数据移动过程中对其进行加密和限制对存储数据的访问方面，企业安全团队大多能够从容应对。但有一点日渐清晰，安全团队也需要在数据被编辑、读取或处理时（通常称为*使用中的数据*）对数据进行保护。

随着计算技术的发展和 AI 的崛起，保护使用中的数据这一缺口正日益凸显其重要性。混合和多云计算的普及扩展了企业收集和存储数据的方式。与此同时，随着企业寻求利用 AI，他们正在使用大量未加密和不受保护的数据集，这些通常是最有价值且敏感的数据。

这些风险导致人们对机密计算愈加关注，这种安全方法可以确保应用程序、进程或服务所使用的所有敏感数据保持处于加密和受保护状态。

## API 增加了复杂性

API 正在普及，它们在企业着力发展的云环境和服务以及 AI 模型两大领域发挥着关键作用。在云端，API 对于实现技术通信和共享数据至关重要。借助 AI，大语言模型 (LLM) 使用 API 访问和组合数据以执行语言理解及文本生成等复杂任务。

遗憾的是，API 并没有像应用程序和基础架构那样受到安全团队的重视。而攻击者正在利用这一安全漏洞。过去 12 个月里，有 84% 的企业遇到了 API 安全事件。[1] 为了保护云端 API 以及与 AI 相关的 API 所接触的敏感数据，企业需要在其机密计算环境中运行全面的 API 安全保护功能。

## 锁上所有三道门

即使对传输中和存储中的数据进行加密保护，仍然可能有一道门（即，使用中的数据）四敞大开，从而导致公司面临风险。

在机密计算中，此类数据会在硬件级别上被认为可信的环境中进行处理。通过利用 API，企业可以部署其专为保护 API 流量而构建的私有机器学习实例，而无需利用公有云 API 服务，从而显著减小企业的攻击面。在机密计算环境中运行 API 安全解决方案可以提供一层额外的安全保护。即使部分系统遭到入侵，受保护环境中的数据仍然安全无虞。在受信任的环境中对此数据运行 API 分析更加安全，并且可以消除传统环境中存在的风险。

将 AI、API 安全和机密计算相结合，有助于防止未经授权的实体（例如，虚拟机监控程序、主机操作员、系统基础架构所有者，或者可以进行物理访问的任何人）在执行期间查看或更改代码或数据，从而防范内部威胁（例如，有恶意的系统管理员或在不受信任的基础架构上运行的工作负载）和外部威胁（例如，利用漏洞的攻击者）。

### 对企业的好处

**增强数据安全**
通过强有力的控制措施限制对使用中的数据的访问，减小攻击面并保护 API 驱动的敏感流程免受未经授权的访问

**保护 API**
执行深度 API 流量分析，同时保持敏感数据在使用过程中处于加密状态，从而降低监控期间的暴露风险

**提升合规性**
满足不断变化且严格的全球数据保护法规的要求，确保符合行业和政府标准

1. Akamai 的 2024 年 API 安全影响研究

## 优势

随着 API 威胁的激增，以及使用中的数据日渐成为极具吸引力的目标，攻击者将很快蜂拥而至。出于多种原因，高瞻远瞩的企业开始采用机密计算：

- 首先是通过强有力的控制措施可以限制对使用中的数据的访问
- 对数量不断增加的 API 进行安全分析
- 利用机密计算提供的控制措施满足全球各地新的、严格的数据保护合规要求

无论是寻求保护在线交易的金融服务公司，还是保护患者数据的生命科学公司，机密计算都可以为这些受到严格监管的企业带来巨大的优势。此方法也可以帮助独立软件供应商保护它在从边缘到云端的多个位置分发给客户的 AI 模型。实际上，任何对其重要数据进行实时分析处理的企业 IT 组织都需要考虑采用机密计算。

### Akamai 与合作伙伴如何提供帮助

有效的机密计算需要一整套紧密协作的解决方案，以提供全面的控制和保护。Akamai 与我们的合作伙伴英特尔及 IBM 携手，为使用中的数据提供从硬件层到云端再到 API 的安全保障。

首先，英特尔® 信任域扩展 (TDX) 提供受信任的执行环境，这些环境可以：

- 抵御来自攻击者和/或不应该进行访问的非恶意实体的外部入侵
- 对于控制在云端创建虚拟资源（例如，网络、服务器和存储）时所用技术的软件，提高其安全性
- 为负责管理这些分布式系统的人员增加一层急需的安全保障，从而降低出现无心之过的风险并减少潜在的内部恶意活动

此外，英特尔 Tiber™ Trust Authority 验证和令牌让企业能够限制并控制对使用中的未加密数据的访问。

Akamai API Security 解决方案提供了企业中所用 API 的清单，然后可以监控并检测这些 API 的使用方式。它会通过分析流量模式和行为来自动检测并阻止恶意的 API 请求，无需人工干预即可在网络边缘有效阻止威胁。这可以实时抵御数据泄露、未经授权的访问和逻辑滥用等 API 攻击。

三方的强强联合汇集 Akamai 优秀的远程机器学习引擎，以及搭载英特尔至强® 处理器的 IBM Cloud Virtual Server（这些服务器由英特尔 TDX 提供安全保障并经英特尔 Tiber Trust Authority 认证），共同打造了一个私密且具备超大规模可扩展性的环境。无论外部威胁来自 AI 驱动的爬虫程序攻击还是人为攻击，都可以通过该环境来防止这些威胁在数据使用的最后阶段访问未加密的数据。

## 保护使用中数据的时刻已然到来

企业需要一个高度可信的环境为其最有价值的公司数据提供安全保障，不仅需要在数据的存储或访问过程中提供保护，也需要在数据的实际使用过程中提供保护。他们正在向 Akamai 和我们的合作伙伴寻求全面的安全保障。这些计算领域的知名企业将携手合作，确保数据在生命周期的每个环节都受到安全保障。

详细了解我们的机密计算合作伙伴关系如何帮助保护您的敏感数据。

详细了解 Akamai API Security 解决方案。

扫码关注 - 获取最新云计算、云安全与CDN前沿资讯