AKAMAI 产品简介

Account Protector

借助帐户滥用防范功能，将欺诈者拒之门外，避免信任受损

如何判断用户是真实用户还是冒充者？客户要靠您来明辨真伪。

随着数字交易和新数字资产的普及，帐户滥用的风险和后果比以往任何时候都更为严重。您扩展数字业务和保护客户的能力取决于您能否在欺诈手段不断演变的环境中维系信任关系。

欺诈性开户（新帐户欺诈）和帐户接管 (ATO) 等与帐户相关的滥用行为给各行各业的企业带来了重大挑战和成本问题。被盗和虚假帐户可能会给企业带来严重的财务和声誉受损后果。一旦帐户被侵入，攻击者便可随意利用该帐户从事各种恶意活动，例如将余额洗劫一空，进行欺诈交易，禁用多重身份验证等安全功能或窃取敏感的个人信息。 另一方面，虚假帐户可用于利用免费试用和积分等促销活动，进行短信轰炸，并向平台发送大量垃圾邮件或不当内容。这些攻击所造成的影响非常严重，企业面临客户信任度下降、因欺诈损失数百万、以及应对监管罚款和声誉损害的风险。

Akamai Account Protector

Account Protector 是一款旨在防止整个帐户生命周期内出现帐户滥用情况的安全解决方案。它利用机器学习和大量风险与信任指标数据集来判断用户请求的合法性。该解决方案能够实时分析行为，从帐户创建、登录及后续操作中，识别欺诈活动的蛛丝马迹。如果检测到可疑或异常行为，Account Protector 会提供即时抵御选项，以保持用户体验的流畅性，例如在边缘进行阻止并采取措施、提供加密和行为挑战、提供替代内容等。

对企业的好处

提升您和用户的可信度：
知道哪些互动是合法的，减少用户遇到的阻碍，同时保护用户免遭欺诈活动。

开发专为您的企业量身定制的保护方案：
利用自动调整的爬虫程序检测功能，并且支持根据用户与您网站的互动方式了解用户群体特征。

获取深度见解和可见性：
根据明确的信号和指标，从容采取行动。

降低补救措施带来的负面影响：
减少调查被盗帐户、更换被盗资产等方面的财务损失和资源消耗。

制定更好的数据驱动式安全和身份决策：
与欺诈工具、SIEM 和其他安全工具集成，从而允许使用 Account Protector 的风险和信任信号，提高准确性并提升已经为这些工具付出的投资的价值。

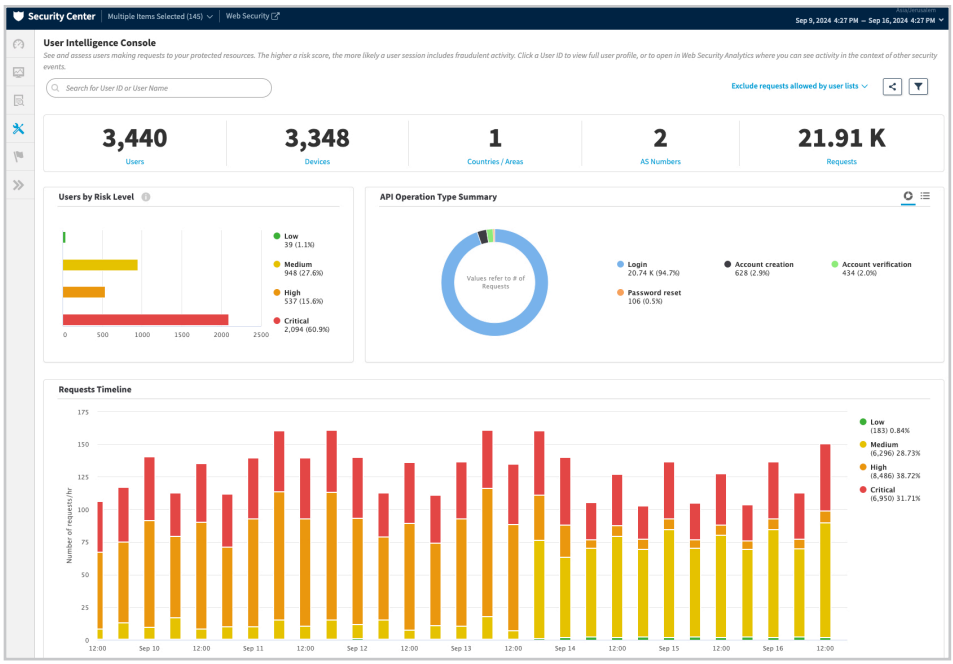
全面防御帐户滥用

保护用户帐户在整个生命周期内免受滥用——提供高级保护，防止开户滥用、帐户接管攻击以及由此形成的攻击方案。

开户滥用——抵御创建虚假帐户问题，避免这些帐户被用于在促销活动中谋利、进行短信轰炸、测试被盗信用卡信息以及囤积居奇等行为。

帐户接管——防止冒名顶替者获得合法客户帐户的访问权，将其价值抢劫一空、窃取敏感数据并进行欺诈交易。

复杂恶意爬虫程序攻击——保护用户帐户免受撞库攻击、库存操控和其他自动攻击，这些攻击通常与开户滥用或 ATO 同时发起，目的是窃取有价值产品、金钱或其他有价值资产。



主要功能

帐户生命周期内给予全方位保护——从帐户创建到帐户更新、密码更改和支付等登录后活动的任何阶段识别和分析用户风险。

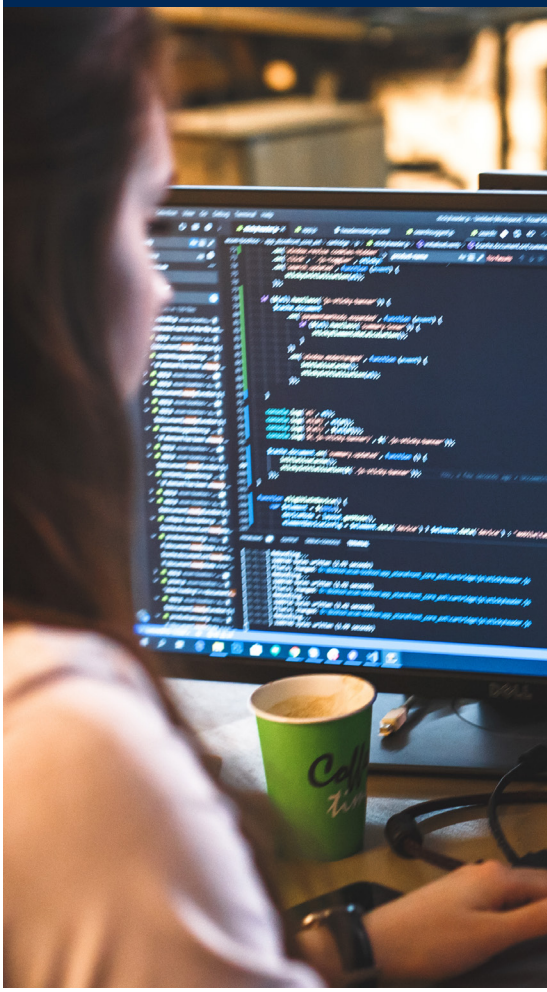
实时用户会话风险评分——评估整个用户会话中的风险和信任度，进而评估用户请求来自合法用户还是冒名顶替者。

电子邮件地址智能——分析电子邮件地址的语法和电子邮件的异常使用，以检测恶意模式。

电子邮件域智能——评估来自各个电子邮件域的活动模式，包括一次性域和电子邮件域的过度使用。

有力的保护，带来良好的信任和用户体验

实时分析风险并阻止滥用，持续监控帐户在整个生命周期中的可疑行为迹象。



全球受信用户识别——监测 Akamai 网络中的用户行为，就登录的可信度做出更明智的决策。

用户行为特征——根据之前观察到的位置、网络、设备、IP 地址和活动时间构建用户行为特征，以识别回访用户。

用户群体特征——将企业的用户特征聚合为一个超集，由此还能将行为差异与整个用户群体进行比较，以检测是否存在异常。

来源声誉——根据过去在所有 Akamai 客户（其中包括全球许多规模庞大、流量颇高且频繁受到攻击的网站）中观察到的恶意活动评估来源的声誉。

指标——为每个请求的评估提供风险、信任和常规指标，以评估帐户滥用的风险。这些指标与最终用户风险评分一并提供，并可用于分析。

高级爬虫程序检测——使用各种 AI 和机器学习模型和技术，在与未知爬虫程序首次交互时就能准确将其检测出来。这类模型和技术包括用户行为 / 遥测数据分析、浏览器指纹识别、自动浏览器检测、HTTP 异常检测、高请求率等。

分析和报告——提供实时报告和历史报告。分析各个端点上的活动、调查特定用户、按风险级别审查用户并获得深入见解。

高级响应操作——提供各种可用于阻止帐户滥用的操作，包括提醒、拦截、延迟、提供加密和行为挑战、提供替代内容等。此外，企业还可以根据 URL、具体时间、地理位置、网络或流量百分比分配不同的措施。

标头注入——发送用户风险信息以进行分析和实时防御。 在转发的请求中注入额外的请求标头，其中包含有关用户风险评分以及作为评分依据的风险、信任和一般指标的信息，以便进一步分析和实时抵御风险。

利用机器学习实现自动化——自动更新用于识别人为欺诈活动和爬虫程序的特征和行为，其中包括行为模式和整个 Akamai 平台上的最新声誉得分。

SIEM 集成（可选）——将用户风险信息集成到 SIEM 工具中，供需要更高的集成安全可见性的客户使用。您可以利用来自 Account Protector 的见解来充实现有工具，提升其价值。

请与您的 Akamai 代表联系或访问 Akamai.com，以了解更多信息。