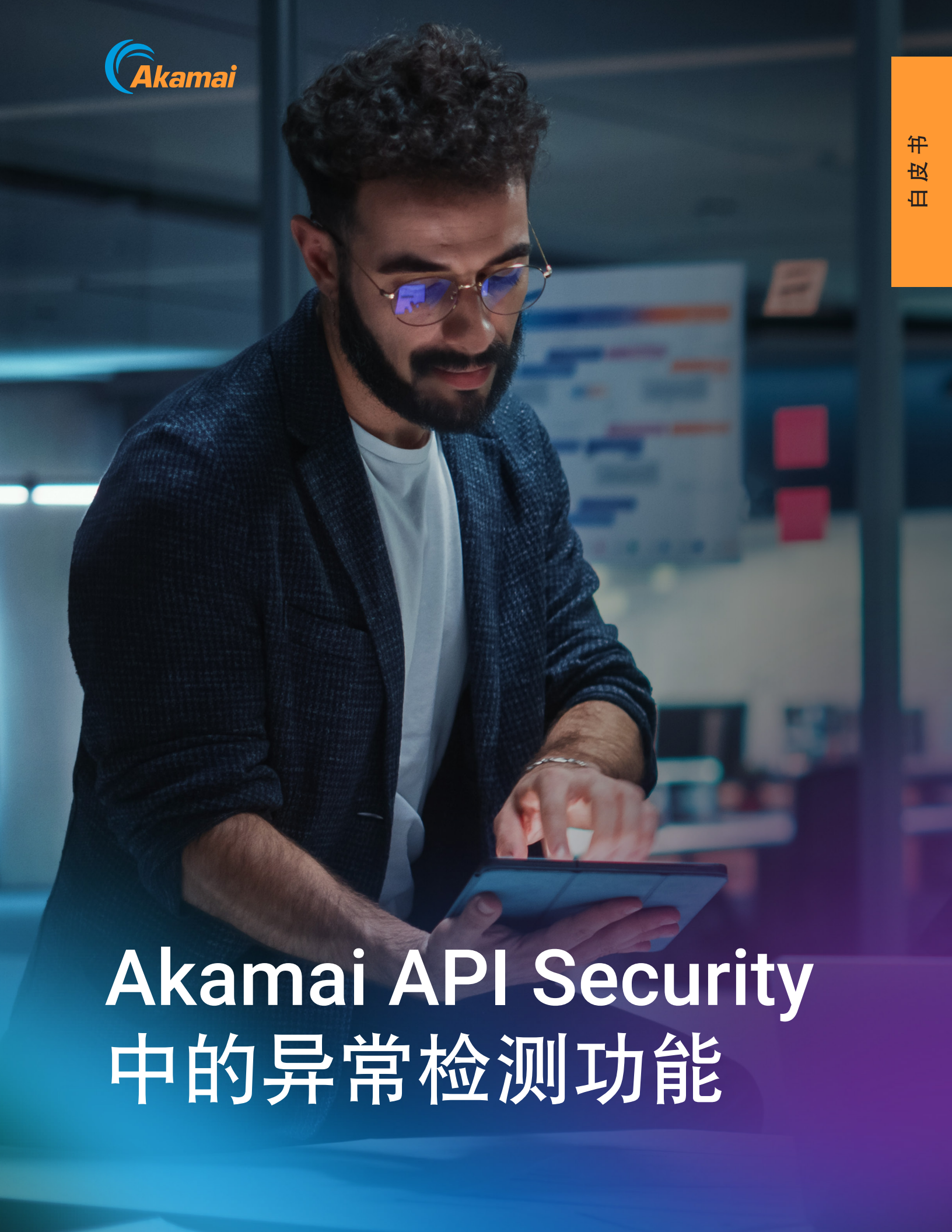


白皮书

Akamai API Security 中的异常检测功能

API 是企业服务客户、创造收入和高效运营的关键组成部分。但是，API 的持续增长、与敏感数据的紧密关联以及缺少安全控制措施等因素，使得 API 成为当今攻击者眼中诱人的目标。实时了解用户行为是主动识别潜在 API 滥用或攻击迹象的关键。

Akamai API Security 解决方案的异常检测功能旨在识别异常用户行为，这类行为预示着攻击者可能会尝试恶意利用企业的 API。Akamai 的异常检测功能将建立正常流量的基线，并将传入请求与基线进行比较，确定是否有可能是攻击者执行的操作。

我们的异常检测算法可以识别异常行为，例如：

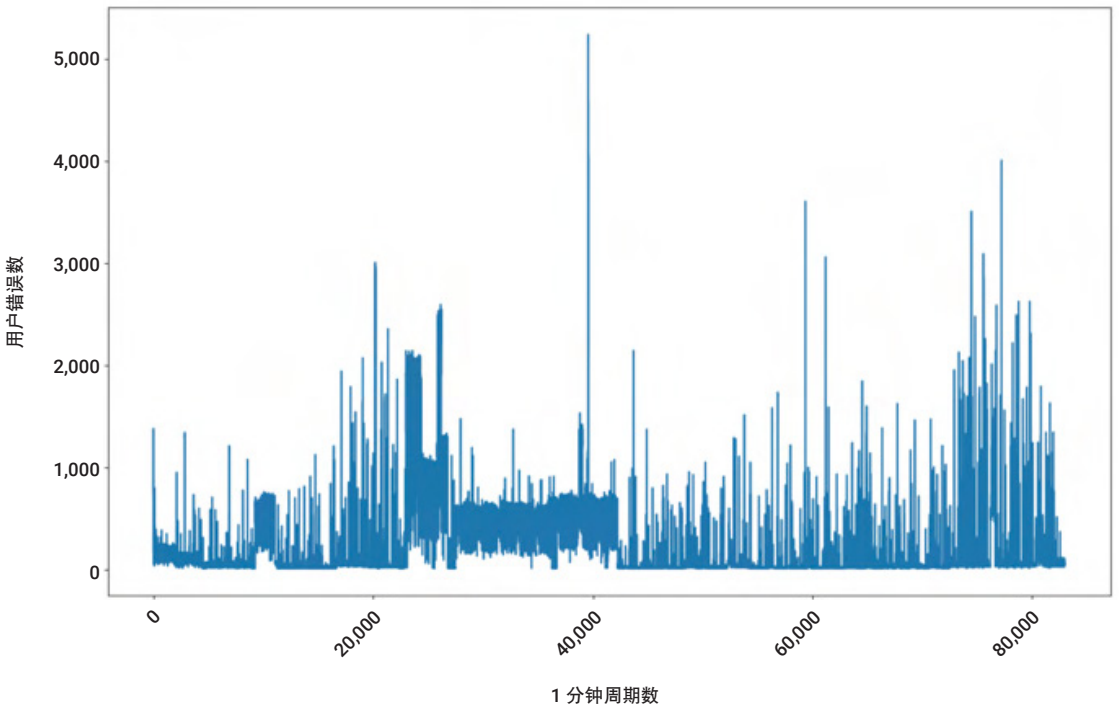
- 在 API 请求中使用意外字段
- 与普通用户相比，从服务器提取更多数据
- 尝试使用其他用户/管理员资源
- 调用 API 的顺序不合常理

该算法基于无监督式在线学习人工智能和机器学习 (AI/ML) 模型，此模型能够学习流量统计行为的多种特征，并在固定的学习周期后检测异常事件。我们的模型能够适应流量随时间的变化，并能够辨别用户标记为误报的异常。

在学习阶段，我们的系统会解析客户数据，并识别不同的 API、身份验证方法、用户、数据类型等。针对每个 API，该模型都制定了普通用户流量的一个特征列表，其中包括 API 点击次数、生成的错误数、经过身份验证的请求所占的百分比、从服务器检索的数据量等。我们的算法通过将用户和 API 的特征与我们算法所学习的统计模型的预期结果进行比较来检测用户异常。

Akamai API Security 异常检测的工作原理

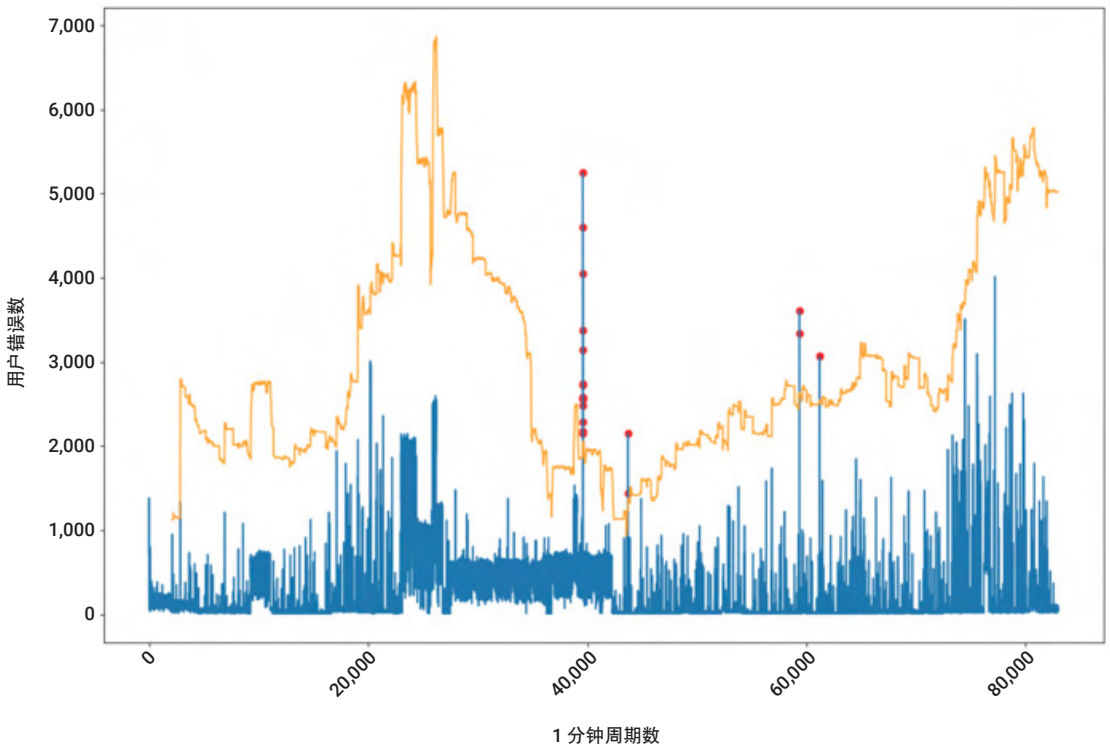
Akamai API Security 的异常检测功能可识别出与其他用户相比产生错误过多的用户。这让我们能够识别暴力破解、路径扫描和抓取等攻击。下图显示了环境中用户在每个 1 分钟周期内产生的最大用户错误量。



在这种情况下，识别异常面临多种挑战：

1. 在计算阈值时，模型需要考虑数据漂移。
2. 我们希望在模型的学习周期内避免学习异常行为。
3. 学习是流式进行的，这意味着模型永远看不到整体数据，并需要在每个时间步进行调整。
4. 告警必须是实时的，因此我们的算法不能依靠未来的数据来预测异常。
5. 为避免向用户发送垃圾邮件，我们的模型需要学习数据的统计保证阈值。

在下图中，您可以看到我们的模型是如何根据传入数据调整阈值，进而满足这些要求的。



橙色线条显示了模型计算出的阈值函数，红点显示了模型基于该函数检测到的异常。

常见问题

Akamai 的异常检测算法需要多长的学习周期?

我们的大多数算法需要两到七天的学习周期。此外，算法的学习周期也受到学习周期内观察到的不同用户行为数量的影响。

当检测到异常行为时，需要多长时间才能生成告警?

在大多数情况下，我们的算法会在收到异常流量后 30 到 60 秒内为客户端创建相关告警。

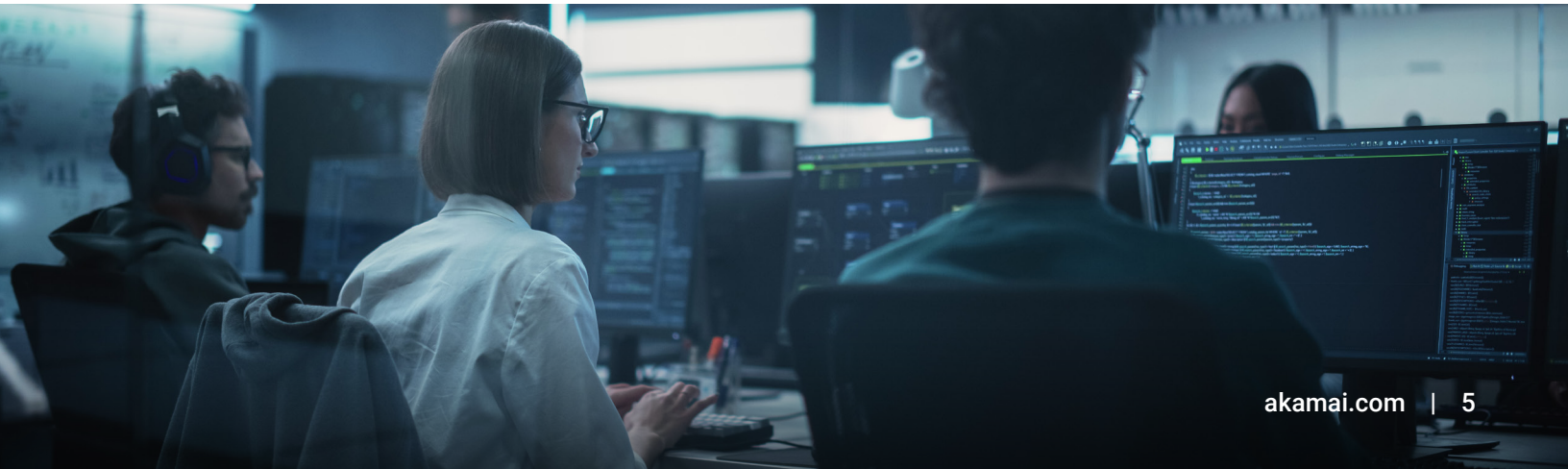
该算法采用监督模型还是无监督模型?

我们的算法基于无监督模型，因而无需事先了解客户环境的特征，便能适应每个客户的环境。此外，我们的算法会通过在线学习来适应环境随时间的变化。

Akamai API Security 可检测出哪些不同类型的异常?

Akamai API Security 可检测出两种类型的异常：

- 基于模式——通过识别流量中的恶意模式而检测出的异常，如 Web 入侵技术和已知的恶意用户代理，比如命令注入、路径遍历和可疑用户代理。
- 基于行为——基于用户的学习行为检测出的异常，同时识别出异常用户，如过度使用 API、范围违规和受损的对象级别授权。



在触发异常时，Akamai API Security 会考虑哪些参数?

我们的算法基于通过对流量进行统计分析而设计的多个特征，例如：

- 使用 API 的不同用户数
- API 的身份验证状态
- 服务器的响应代码
- 用户提取的数据量
- 用户的 IP 地理位置
- 用户的用户代理等

用户能否控制算法的灵敏度?

可以，用户可以通过修改相关策略的灵敏度来控制对每种异常的检测灵敏度。策略灵敏度是介于 1（低）和 5（高）之间的数字；当某种策略选用了最高值时，Akamai API Security 将以最高的灵敏度检测系统异常。我们的算法将此参数作为模型的一部分考虑在内。

用户能否将 Akamai 告警的问题标记为误报，这将对算法产生何种影响?

可以，为改进我们的异常检测，我们的用户可以将相关问题标记为“误报”。当一个问题被标记为误报时，我们的算法会考虑到这一点，并根据用户的输入调整模型。

如果某个用户持续发送相同的攻击场景，Akamai 如何避免向客户端发送垃圾邮件?

我们的算法将识别针对同一用户和 API 不断触发的类似问题。在这种情况下，我们的算法将在一个恒定周期内忽略类似的问题。

Akamai 如何处理数据中的漂移/季节性?

Akamai API Security 利用几种不同的算法来检测数据中的异常。根据底层数据预处理和算法复杂性，我们可能会放松阈值调整，或者在需要异常检测的保证统计阈值的每个周期强制进行调整。配合使用垃圾邮件控制，即使特定算法需要额外的周期来调整阈值，我们也可以提供一个简便的界面。

Akamai 如何处理数据投毒?

作为一种在线学习算法，Akamai API Security 需要应对各种挑战，例如：

- 新 API
- 现有 API 中的新字段
- 字段中值类型/范围的更改
- 服务器可用性问题
- API 中的漏洞，这些漏洞可能会产生错误（404、500 等）和其他挑战，要决定哪些需要学习，哪些不需要学习（Akamai 会采取预防措施，在达到要求的最小用户数、时间周期和持久性的组合条件时才触发学习，从而避免学习这些异常）