Akamai

API 运行时保护权威指南

目录

前言 3

为什么需要运行时保护? 5

不可或缺的运行时保护功能 8

Akamai API Security 运行时保护 11

获取有效 API 运行时保护的后续步骤 15

前言

为什么 API 安全防护极其重要

为了满足客户需求，企业之间激烈角逐，争先恐后地开发和制作出色的应用程序、服务和生成式 AI 工具，不断提升这些工具的性能。遗憾的是，一味地追求速度给企业带来了暗藏的风险：作为所有创新的幕后支持者，API 常常因仓促构建而出现配置错误、编码漏洞以及缺乏安全控制等问题。当这些 API 进入生产阶段后，不仅终端用户会与之交互，攻击者也会持续尝试各种手段来入侵 API 并窃取它们交换的数据。

错误配置和受到入侵的 API 正日益成为导致重大数据泄露的主要因素，然而，很少有企业能够密切监控其数字生态系统中成千上万的 API 调用。至于能够完全防范运行时 API 威胁的企业，更是寥寥无几。

例如，2021 年，一家健身零售公司的用户帐户数据 API 存在一个漏洞，使得任何人无需身份验证即可访问包括年龄、性别、城市、体重和出生日期等数据。尽管这一漏洞被安全研究人员及时发现并告知了该公司，但有些类似的漏洞可能被人利用数周乃至数月之久都未被觉察。

在保护 API 安全方面，企业惯常依赖的传统工具（例如，API 网关和 Web 应用程序防火墙）可以提供基本的保护。然而，随着 API 攻击的数量不断增加且日益复杂，当今的安全团队亟需增设更多的安全保护层。关键在于深化对漏洞、潜在攻击路径、恶意行为以及 API 行为的分析洞察，然后据此强化现有的控制措施。

企业可以通过采用涵盖以下四个方面的综合性 API 安全解决方案来获得这些能力：

1. API 发现
2. API 态势管理
3. API 运行时保护
4. API 安全测试

本指南涵盖的内容

API 运行时保护指的是，在 API 正常运行并管理请求的过程中对其进行保护。本指南阐述了 API 运行时保护的关键要求，包括 API 监控（用于防范错误配置与漏洞利用）以及 API 攻击防范。同时，也探讨了运行时保护的基本原理，并介绍了 Akamai API Security 所提供的运行时保护功能。

为什么需要运行时保护?

在 API 生命周期的整个使用阶段，API 运行时保护功能可持续保护 API，确保其处于正常运行状态，可以与预期的最终用户进行交互，同时防范攻击者的威胁。有效的运行时保护功能通过迅速识别并处理恶意 API 请求，为 API 筑起一道坚实的防线，抵御各类部署后可能遭遇的威胁，包括：

- 从 API 中提取大量敏感数据的攻击者
- 利用安全漏洞的特权提升攻击
- 在正常流程外部署未经授权的 API

为了阻止运行时 API 威胁，必须理解每个 API 的运行背景，这涵盖了 API 的访问模式、使用情况及行为。首先是明确您所拥有的 API 资产范围。《API 发现的权威指南》阐述了 API 清单的重要作用。拥有详尽的 API 清单能让您监控所有 API 流量，并对每个 API 的“典型”行为具有基本的了解，从而帮助您发现异常行为。API 运行时保护能够检测到：

- 数据泄漏
- 数据政策违规
- API 安全攻击
- 数据篡改
- 可疑行为

此外，运行时保护还会记录 API 流量、监控敏感数据访问、检测威胁以及屏蔽或修复攻击。

监控 API 流量，防范攻击

观察 API 流量行为对于识别风险至关重要。若不了解 API 资产的准确状况就部署监控解决方案，那么所能获得的监测能力将十分有限。完成 API 足迹清点后，API 运行时保护应持续监控流量和 API 使用情况，同时查找漏洞和错误配置。

检测异常行为

对正常的 API 行为建立基线后，任何偏离这一基线的异常行为都会被识别出来。通过重新运行历史数据，我们不仅能发现异常行为，还能揭示出攻击者的意图。

对于任何潜在的异常行为，我们都应将其放在应用程序或网络中其他操作的背景下，进行更为深入的分析。例如，若某个数据请求的大小超出了常规范围，或者 API 调用所请求的数据量超出了正常请求的范围，这样的请求就应当被标记出来。这个请求可能是恶意的，也可能不是，但无论如何都需要进一步检查。

检测数据泄露

您资产中的某些 API 可能会传输和接收敏感数据。而安全漏洞可能导致这些敏感信息泄露，进而使攻击者有机会提升权限或进行不当的访问控制配置。AI 与机器学习技术在实时流量分析与异常检测中扮演着至关重要的角色，它们能够提供对数据泄露、数据篡改、数据政策违规、可疑行为和 API 安全攻击的情景洞察。

其中，网络犯罪分子窃取有效的 API 密钥已成为一种日益普遍的攻击手段。一旦攻击者窃取了有效的密钥，唯一能够防止不当 API 使用及潜在数据泄露的方法，就是检测并阻止异常行为及数据泄露。

API 安全审核

API 安全审核工具应能实时追踪流量，并提醒您注意攻击及其他恶意企图。作为最低要求，API 安全审核应能够：

- 执行持续监控以识别攻击者和恶意请求
- 被动地扫描（内部和外部）API，以发现可能导致或加剧漏洞或削弱防御措施的错误配置和疏忽。
- 采取策略来指定 API 应该（和不应该）发送或接收哪些数据

API 运行时保护应当结合 API 态势管理，以识别错误配置和已知漏洞。如需了解更多信息，请阅读**《API 态势管理权威指南》**。

不可或缺的运行时保护功能

如果贵企业正在积极开发和部署 API，就必须将强大的运行时保护纳入 API 安全计划。以下是您的运行时保护工具必须提供的关键功能。

实时带外监控

API 安全监控不得影响 API 流量、减慢其速度或增加延迟。它应完全在带外运行，无需对网络进行更改，也无需安装复杂和难以安装的代理。运行时保护工具应该对来自于已识别数据源的流量进行镜像，在后台对流量数据进行分析，并在发现任何问题后发出实时告警。

Akamai 默认在带外运行且无需代理，但如果您有需求，我们也能提供基于代理的检测以及内联拦截选项。

API 异常和漏洞利用检测

被动数据收集不足以满足要求，尤其是在 API 数量及 API 流量总量不断增加的情况下。解决方案必须持续分析 API 活动，以检测异常事件并向安全和运营团队发出告警。先进的平台工具融合了 AI 与机器学习功能，能够实时分析流量，并利用情景洞察来识别数据泄露、数据篡改、数据政策违规、可疑行为以及 API 安全攻击。

API 攻击防范和风险修复

在识别异常或其他问题并生成告警后，时间便至关重要。解决方案必须检测通过 API 未经授权地移动敏感数据或者其他可疑的 API 滥用行为，并予以修复。运行时保护应当不仅限于通过集成现有防火墙和 API 网关来防范 API 的滥用行为，还应提供修复选项，并尽可能实现自动化操作。寻找具备攻击者信心评分功能的保护工具，助力您的团队判断滥用、攻击或漏洞的迹象是否真实存在，从而决定是否需要升级响应措施。

事件响应的集成

一般来说，运行时保护工具应该能够与企业使用的其他安全、监控和管理工具轻松集成。例如，当事件发生时，运行时保护工具必须包含必要的集成功能，以确保将修复任务分配给相应的团队。如果检测到配置错误、数据策略违反情况或可疑行为，那么应该将它们报告给 API 网关、SIEM 系统和其他信息安全引擎，以确保引起充分的注意。攻击者信心评分功能可以助力团队排除干扰，将精力聚焦于真正优先的 API 安全事务上。

Rapyd

Rapyd 是一家全球性付款处理及金融科技公司，在全球 100 多个国家/地区运营支付系统。然而，由于缺乏对 API 使用情况和行为的精细监测能力，该公司需要一种更高效的解决方案来保护其面向公众的 API 以及数百个内部 API，这些 API 位于一个高度复杂且基于 AWS 云的全球系统中。Rapyd 迫切需要对其所有 API 进行全面清点，监测错误配置和漏洞，以及一种智能分配优先级的告警系统，以便采取更加合理的修复措施。

Akamai API Security 凭借其全面的监测能力和运行时保护能力，恰好满足了 Rapyd 的这一需求。该解决方案运用机器学习技术为每个 API 建立流量基线，并能自动检测异常行为及进行修复。

阅读完整的客户案例

> 现在，我们能够以科学方式切实评估我们的风险，掌控自己的命运。
>
> ——Nir Rothenberg
> Rapyd CISO

Akamai API Security 运行时保护

对企业而言，将第一时间识别和阻止 API 攻击的能力纳入合规性和风险评估计划中至关重要。当其他安全控制措施未能充分发挥作用时，它会成为您的最后一道防线。

Akamai API Security 的运行时保护模块涵盖了之前章节所述的全部功能。其主要作用是实时检测并阻止 API 攻击。基于自动机器学习的监控功能用于执行流量分析，并提供对数据泄露、数据篡改、数据政策违规、可疑行为和 API 安全攻击的情境洞察。运行时保护可检测出您的 API 流量中存在的异常和潜在威胁，并根据预先选择的事件响应策略来帮助进行修复。

运行时保护能够与 WAF、API 网关、ITSMS、SIEM 以及其他工作流工具集成，从而构建一个全面的防御体系来抵御攻击。您可选择以全自动的方式完成威胁修复，也可以要求进行不同程度的人工干预来实现更强的监测能力和控制。此外，Akamai API Security 解决方案还与 Akamai 平台原生集成，使我们能够在边缘直接拦截攻击者的 IP。

问题生成

Akamai 运用机器学习技术，为每个 API 构建专属模型。然后，利用正常行为基线来检测 API 业务逻辑攻击，如失效的对象级授权 (BOLA)，防止个人访问他们不应获取的数据。当 API 流量偏离正常行为时，Akamai 会实时生成一个问题。这个问题就像是告警一样，在检测到任何异常的 API 行为或发现错误配置时自动

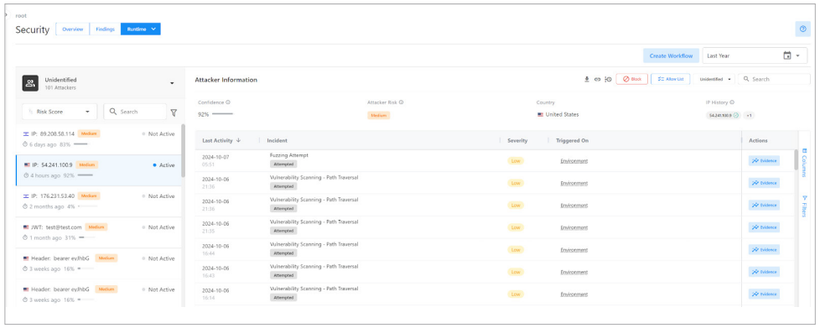
生成。生成问题后，告警会自动发送到诸如 Splunk 或 QRadar 等 SIEM。此外，告警也可以自动发送到如 ServiceNow 或 Jira 等服务工单系统。

问题详情

Akamai API Security 的运行时保护模块生成的每个问题都包含严重性、状态、与 OWASP 十大 API 风险的对应关系以及攻击者详细信息（如果适用）。

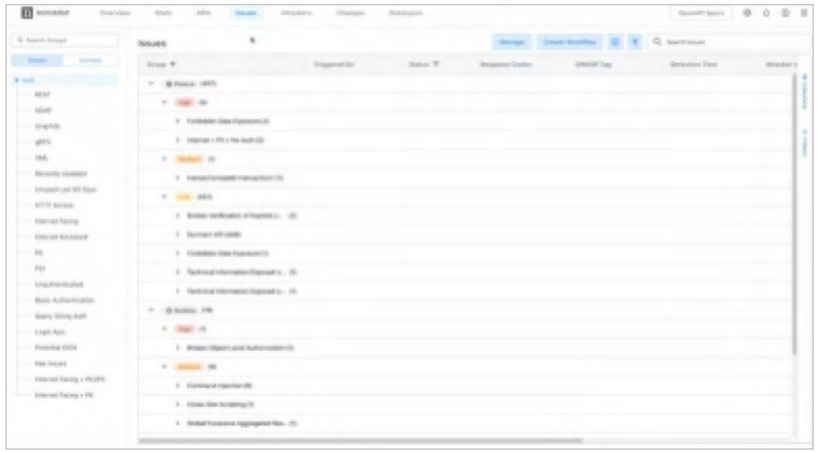
问题详情页面包含问题本身的描述、它对企业可能造成的影响，并提供相应的修复建议。此外，Akamai API Security 还使企业能够查看攻击者在特定时间段内所执行的操作类型、每次攻击的历史记录，并且对恶意攻击者采取行动。

示例：监测攻击者的行动

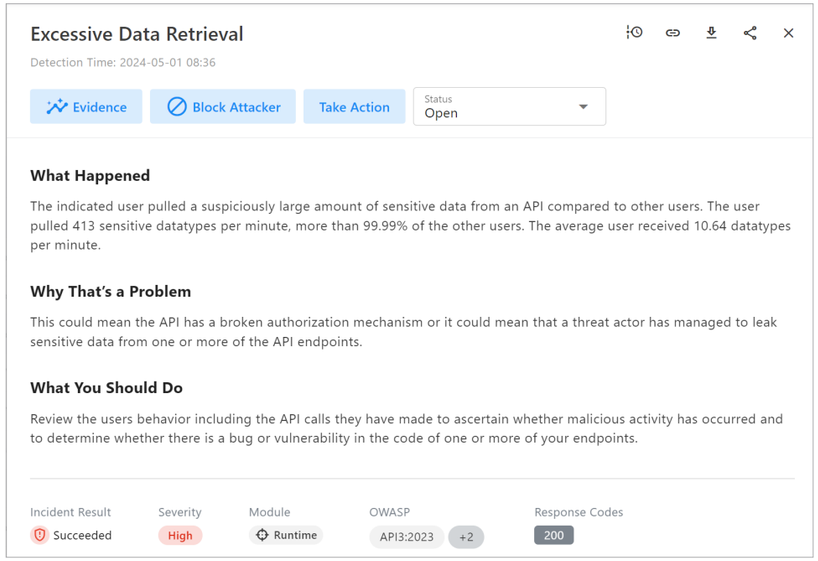


每个问题都包含证据。证据就是引发问题生成的攻击者会话的详细信息，以及 API 请求和响应的副本（涵盖标头和主体），有助于迅速分类并修复问题。Akamai API Security 解决方案的运行时保护模块，借助直观的仪表板、过滤功能、告警以及报告功能，能够协助企业了解事件、分析事件发生的原因，和明确后续应采取的措施。

示例：报告 API 问题和证据



示例：有关过度数据检索的洞察



策略操作

通过 Akamai API Security，企业能够对每个生成的问题执行半自动化的策略操作。这些操作可能涵盖开立工单、发送信息到 SIEM，或者发送 Webhook 到第三方系统。可能还包括阻止攻击者。而具体可以采取的操作类型，则取决于配置到 Akamai 平台上的集成类型。

该解决方案包含了众多开箱即用的预定义策略，旨在检测 API 攻击和 API 错误配置。此外，Akamai API Security 还包含超过 20 种预配置的数据类型，便于您根据需要创建数据策略，以便当您的 API 传输敏感数据时，您能够及时发现并采取措施。

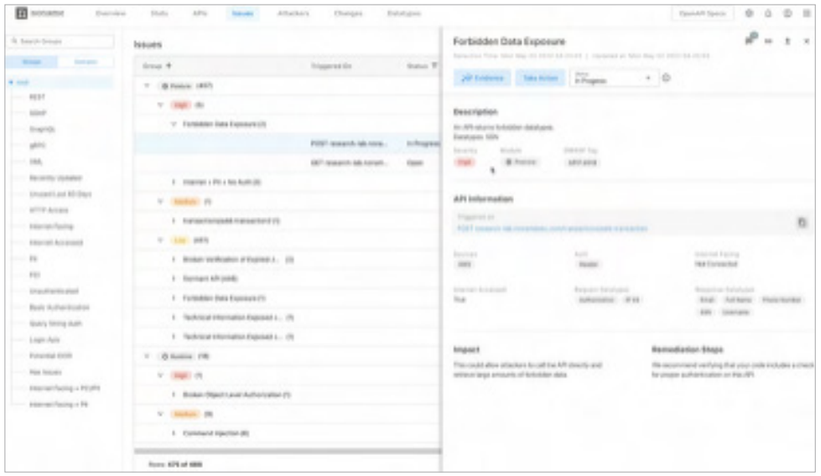
总之，Akamai API Security 解决方案的运行时保护模块可以实时检测和防范 API 攻击，并且持续检测是否存在 API 错误配置，同时包括很多用于简化操作和修复的常用工作流集成。

API 安全事件剖析

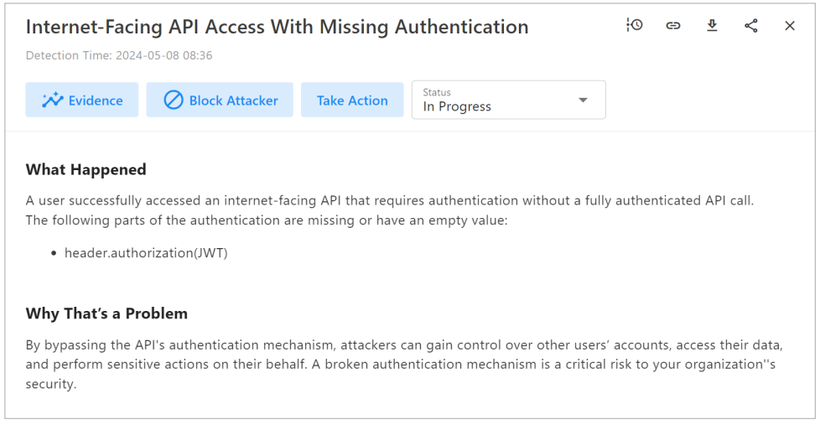
我们来深入探究一个禁止传输的数据被泄露的示例。这个示例揭示了 API 内部存在的一个安全态势问题。Akamai 平台能够感知每个 API 相关联的数据类型及其值在具体情境下的用途。

在下图中，禁止传输的数据正通过 API 被泄露。Akamai 平台能够检测正在传输的数据类型，本例中为社会保险号码 (SSN)，并知晓 SSN 数据之前已被标记为禁止传输的数据。此外，Akamai 还能检测到 API 外部的错误配置，比如那些可以通过互联网访问却未注册到 API 网关的 API。

示例：有关禁止传输的数据被泄漏的洞察



示例：识别缺少身份验证的 API



获取有效 API 运行时保护的后续步骤

每当有客户、合作伙伴或供应商与贵企业进行数字互动时，后台都会有相应的 API 来帮助实现数据（通常是敏感数据）的快速交换。通过实施关键的 API 运行时保护功能，比如监控 API 以防止错误配置和漏洞利用，以及防范 API 攻击，您可以更好地为企业筑起一道防线，抵御快速增长的攻击媒介。

了解如何评估 API 安全供应商，确保他们能够提供关键的运行时保护功能。

预约定制化 Akamai API Security 演示，了解我们如何为您提供帮助。

Akamai Security 可为推动业务发展的应用程序提供全方位安全防护，而且不影响性能或客户体验。诚邀您与我们合作，利用我们规模庞大的全球平台以及出色的威胁监测能力，防范、检测和抵御网络威胁，帮助您建立品牌信任度并实现您的愿景。如需详细了解 Akamai 的云计算、安全和内容交付解决方案，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：2024 年 12 月。

扫码关注，获取最新云计算、云安全与CDN前沿资讯

Akamai