Akamai 合作伙伴案例

从代码到运行时，Apiiro 提供了全面的 API 安全保障

利用 API Security，确保客户尽可能无缝地响应 API 告警

采用策略降低风险

加快修复速度

节省开发人员时间

结合具体情境提升应用程序安全性

作为应用程序安全态势管理 (ASPM) 平台，Apiiro 增强了应用程序安全性和开发团队的能力，向开发团队提供他们所需的洞察，以便将应用程序安全地交付到云端。为完善 API 防护生态系统，Apiiro 与 Akamai 开展了广泛合作，包括使用行为分析的威胁发现和告警以及 API 管理和威胁补救等。API Security 将 Apiiro 平台的强大功能与 Akamai 的运行时相结合，使得企业能够在从代码到生产的整个过程中无缝地保护 API。

扩展 API 防护

应用程序安全和开发团队在将应用程序部署到云端之前，需要验证 API 安全控制措施。Apiiro 使用深度代码分析和运行时上下文来扫描企业的代码库，使用上下文数据对代码库进行扩充，并检测代码中的所有 API。由此，开发人员可在将代码部署到云端之前，确定风险优先级并予以修复。

apiiro

马萨诸塞州波士顿

apiiro.com

行业

高科技

解决方案

Akamai API Security

Akamai

Apiiro 的联合创始人兼首席执行官 Idan Plotnik 表示：“随着 API 的开发和发布速度呈指数级增长，攻击面也在持续扩大。对于企业而言，仅保护其代码中的 API 已经不够。在遇到漏洞时，企业希望减少进行修复所需的平均时间。”

改进分类

Apiiro 使用与 Akamai API Security 关联的开放 API，向企业提供代码和运行时中的 API 实时清单，同时帮助防止威胁升级。

通过将 API Security 与 Apiiro 的平台结合使用，企业能够将 Akamai 检测到的运行时 API 风险与 API 代码关联起来。Apiiro 向安全团队提供了对代码上下文的全面监测能力，包括根本原因、代码存储库、代码的特定行以及代码负责人。由此，安全团队可以识别触发安全告警的确切问题，节省他们评估风险告警的时间。 另外，他们也不需要确定或联系负责的开发人员。

Plotnik 表示：“Apiiro 和 Akamai 将运行时风险检测与详细的代码级监测能力结合起来，使得企业能够快速识别 API 安全威胁，确定安全威胁的优先顺序并予以解决。”

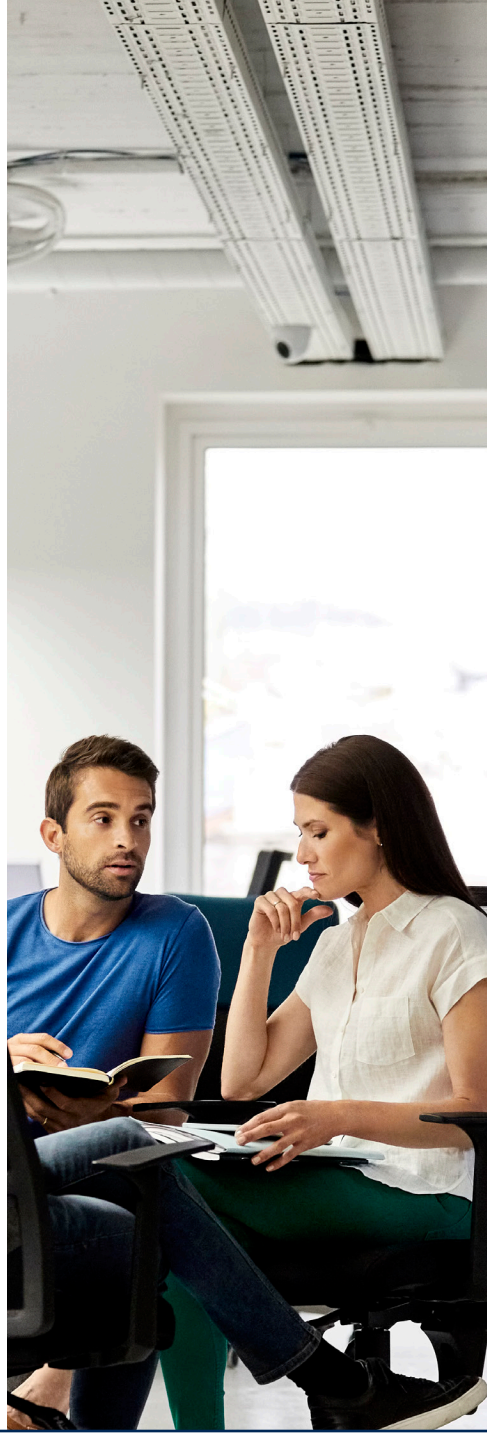
> 无论是开发软件还是使用第三方软件，每家公司都需要确保代码和运行时中具有 API 安全性，而我们与 Akamai 的合作做到了这一点。
>
> – Idan Plotnik
> Apiiro 联合创始人兼首席执行官

加快修复速度

Apiiro 将告警以及与风险相关的上下文传递给相关的代码负责人，辅之以 API Security 提供的切实可行的修复建议。Apiiro 拥有深厚的代码背景知识，而 API Security 则可以提供对运行时中 API 行为和威胁的洞察，两者的结合可以帮助开发人员更准确地确定风险的可能性和影响。这样一来，他们可以确定业务关键型 API 风险的优先级。

Plotnik 表示：“Akamai 和 Apiiro 强强联手，使得企业可以战略性地减少风险，同时节省宝贵的时间并满足其 SLA。”安全团队可以减少花费在追溯负责的开发人员和请求紧急修复上的时间。此外，借助对 API 威胁的清晰洞察，开发人员可以更快地修复问题。

Plotnik 总结道：“我们将 Apiiro 的深度代码分析所获得的洞察，与 Akamai API Security 提供的对运行时 API 安全性洞察相结合，为客户提供了所需的背景信息，让他们能够确定重要 API 风险的优先顺序、进行修复和预防风险。”



apiiro

Apiiro 为许多公司（如 Morgan Stanley、Rakuten、SoFi 和 Colgate）提供服务，帮助他们增强了应用程序安全性和开发团队的能力，使他们能够将应用程序风险监测、优先级排序、评估和修复措施统一起来，节省对安全调查结果进行分类和修复实际风险的时间，从而将安全的应用程序交付到云端。公司已得到风投公司 Greylock、Kleiner Perkins 和 General Catalyst 的投资。

Akamai