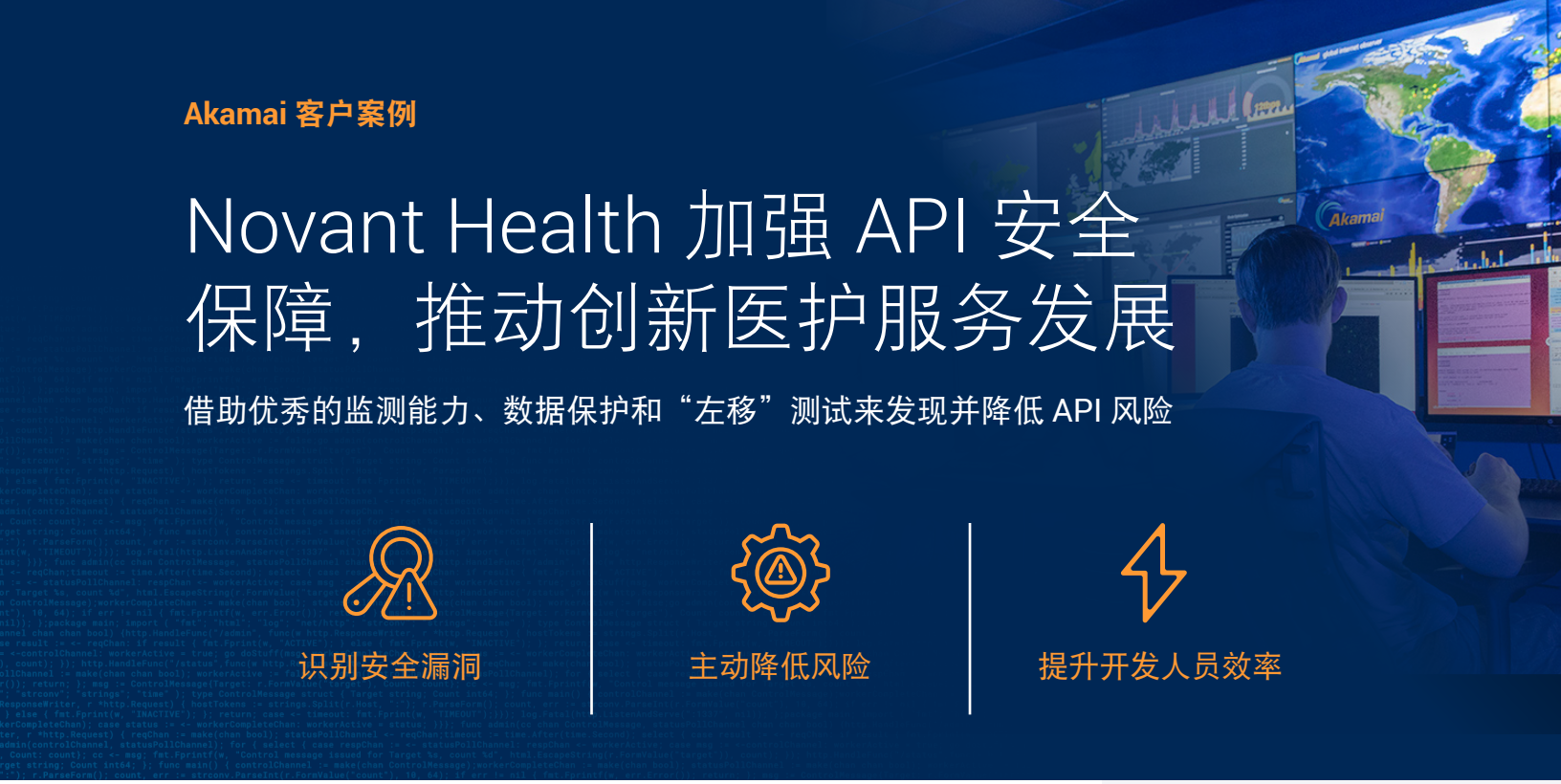
Akamai 客户案例

Novant Health 加强 API 安全保障，推动创新医护服务发展

借助优秀的监测能力、数据保护和“左移”测试来发现并降低 API 风险



识别安全漏洞

主动降低风险

提升开发人员效率

通过以社区为中心的全面医护服务，医疗系统能够惠及多少人的生活？对于 Novant Health 而言，答案无疑是令人震惊的，具体数据如下：

- 医生门诊就诊量达 680 万次
- 护理住院患者 155,964 名
- 急诊就诊量达 602,590 次
- 出生人数达 22,082 人

这些数字也清晰地表明了医疗机构需要保护哪些人和哪些信息，以防范攻击者通过 API 漏洞窃取敏感数据。

了解风险所在

Novant Health 是一家非营利性综合医疗系统，拥有 16 家医疗中心和超过 1,900 名医生，遍布 900 多个地点。这家总部位于温斯顿-塞勒姆的医疗企业规模宏大，拥有超过 36,000 名团队成员和医生合作伙伴，为北卡罗来纳州和南卡罗来纳州提供医疗服务。

Novant 通过一系列数字化创新举措，让患者享受到更有效、更个性化、更高效的医疗服务。作为创新的核心，API 让应用程序、设备和系统之间能够流畅地交换患者数据。API 的重要性不言而喻。为此，Novant 专门成立了一个卓越中心 (COE)，集中人力、知识和资源以打造卓越的 API 产品开发能力。

NOVANT HEALTH

地点

北卡罗来纳州温斯顿-塞勒姆
novanthealth.org

行业

医疗保健与生命科学

解决方案

API Security

Akamai

该团队深知 API 安全的重要性，从一开始就将其置于首要地位，并对以 API 为中心的攻击如何影响医疗服务提供商进行了深入研究。他们一路搜集到的行业数据令人大吃一惊，也揭示了整个行业面临的严峻现实。例如，医疗数据泄露造成的平均损失高达 970 万美元。而且，79% 的医疗企业在过去 12 个月内曾经历过 API 安全事件。

明确问题症结

API 卓越中心 (COE) 将提升整个 Novant 企业内部的 API 安全水平作为首要行动。当时，他们仅部署了 Web 应用程序防火墙 (WAF) 解决方案。这些工具只能防御已知的攻击，而当今的医疗保健企业需要更全面的 API 安全保障措施，包括：

- 了解企业 IT 环境中有多少个 API
- 洞悉每个 API 的风险属性，比如所处理的数据类型
- 深入分析企业的 API 安全态势，包括发现攻击者利用的错误配置
- 防范利用 API 业务逻辑漏洞发起的攻击

此外，Novant 卓越中心团队还发现其企业内部在“左移”方面，也就是在开发早期阶段就考虑安全方面存在重大的不足。他们已经有了测试 Docker 容器的工具，但还需要一个 API 开发解决方案。考虑到诸如患者记录等敏感数据面临的风险，Novant 卓越中心团队一致认为需要找到一家人员和产品都 100% 专注于 API 安全保护的供应商。

找到解决方案

在了解到 Noname Security（现为 Akamai 旗下公司）拥有全面的 API 安全保护解决方案后，Novant 卓越中心团队便与该公司进行了会谈。双方共同对 Novant IT 环境中的每个 API 进行了深入的态势管理分析。借助 Noname 的 API 安全平台（现为Akamai API Security 的一部分），该团队发现了一个具有重大安全隐患的 Azure 漏洞。

> Akamai 帮助 Novant Health 弥补了一个重大的安全短板，让我们能够更清楚地了解哪些资产最容易受到恶意攻击。到目前为止，我们已经在 API 生态系统中发现了一些可以立即采取行动的安全漏洞，这些发现已经充分证明了其价值所在。在 Novant Health，保护数据资产是我们的第一要务。Akamai 与我们秉持相同的价值观，并且已经成为我们整体数据安全体系中不可或缺的重要组成部分。
>
> —— Justin P. Byrd
> Novant Health 数据平台与集成副总裁

Akamai

该平台的 API 态势管理解决方案揭示，Novant 云环境中的部分 API 请求没有经过 WAF 工具的*保护*，而是直接绕过了它。攻击者利用 WAF 无法防御的“后门”成功绕过 WAF，反复攻击 Novant 的 API，导致该公司在不知情的情况下遭受攻击。

Akamai 提供的分析结果既让人感到震惊，又带来了立竿见影的效果。对 Novant Health 而言，安全地开发和维护 API 离不开一个完全受保护的云工作空间。令 Novant 副总裁 Justin P. Byrd 及其团队印象深刻的是，Akamai 团队始终保持高度敬业精神，他们积极利用自己的 API 态势管理解决方案努力发现并解决存在的安全漏洞。

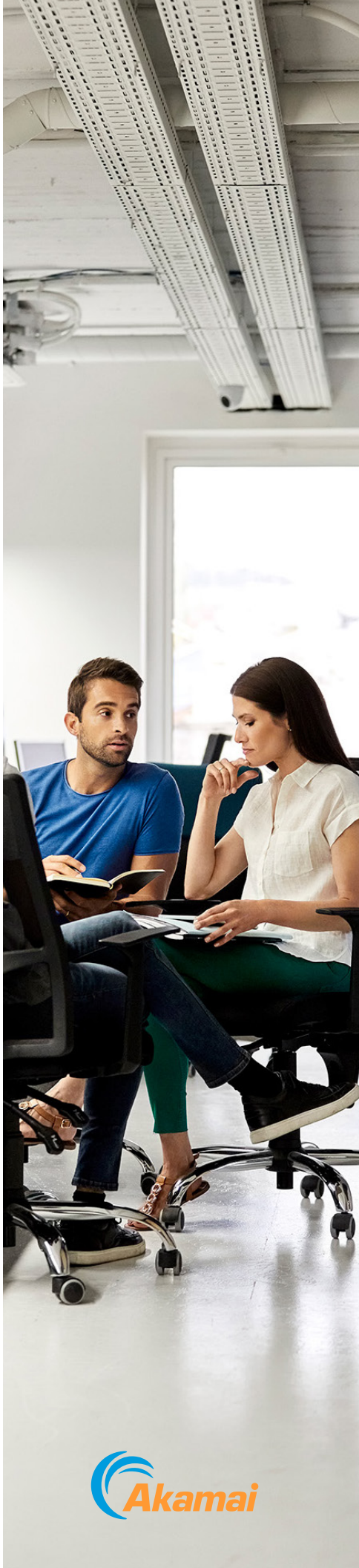
得益于 Akamai API 态势管理解决方案的自动化功能，卓越中心团队可以在初步发现的基础上持续监测 API 的错误配置和潜在风险，从而主动采取措施降低风险。这其中包括能够识别哪些 API 和内部用户有权访问敏感数据。

对于像 Novant 这样的企业，他们管理着包含数百万患者互动的健康数据，为了建立和维系与患者、提供商和监管机构之间的信任关系，了解哪些 API 会处理敏感信息至关重要。

兼顾安全与商业价值

Novant 的卓越中心由一群经验丰富的工程领导者组成，他们认为另一项重要任务是将安全保障整合到企业的 API 测试环节中。API 的开发速度至关重要，尤其对像 Novant 这样的企业，API 直接关系到患者护理水平。然而，为了让产品尽快上线而一味地追求开发速度，很容易让开发人员忽略漏洞或设计缺陷的存在。

为了评估每个 API 的安全防护效果，卓越中心团队需要具备可靠的 API 测试能力。这意味着要进行全面的测试，以发现身份验证机制、权限控制、数据完整性和加密协议等方面存在的不足之处。



当然，要想成功实施任何新的安全工具，不仅要依赖于工具本身的功能，还需要关键利益相关者积极参与。开发人员深知安全的重要性，但考虑到他们需要加快开发速度，所以对不熟悉的工具可能造成的效率降低往往会心存顾虑。

最初在 Novant Health 就是这种情况。

随着与 Akamai 加深合作，Novant 团队发现了一系列功能可以帮助他们的开发人员在保证安全的前提下高效完成工作。例如，Akamai API Security 的主动测试功能可主动发现潜在错误。这些错误若不及时发现，可能会在后续流程中演变成耗时耗力的重大问题。

此外，该解决方案还能帮助卓越中心团队快速指导开发人员提高效率。这对于该团队的成员来说是一个意外之喜，因为他们之前并不知道该解决方案还能进行非安全性的质量保证检查。例如，他们现在可以确定 API 的参数是否与构建的 API 实际提供的内容相匹配。不久之后，起初对 Akamai API Security 不甚热情的开发人员开始意识到它在安全性和效率方面的优势，转而与卓越中心团队一同积极使用该解决方案。

Byrd 表示：“从一开始，Akamai 就成了我们信赖的顾问，在从编码到上线的整个过程中，全程为我们提供 API 发现、保护和测试等方面的专业指导。这让我们的卓越中心能够向整个公司展示如何兼顾安全与效率，实现双赢。这种伙伴关系不仅仅是产品层面的合作，Noname（现为 Akamai 旗下公司）团队对我们的业务以及推动 API 开发的各种因素都了如指掌，并给予我们充分的支持。”

Novant 的领导层也对此表示认可，他们认为 Akamai API Security 能够“防患于未然”，这有力地推动了该公司将 API 安全保护融入到“安全左移”的策略之中。

巩固 API 安全防护成果

如今，Novant 利用 Akamai API Security 为其所有 API 以及支持的各项数字化举措提供“自动保护”，实现全面安全保障。鉴于 Novant 在 API 发现、清点、评估和测试方面取得的进展，卓越中心团队目前正在应用该平台的全面保护功能来保护其开发的所有新 API。该团队认为，只要 Novant 开发人员能够根据一致的最佳实践构建 API，就能让每个 API 都自动获得安全保障。

展望未来，卓越中心团队希望将 Akamai API Security 推广到公司内部的其他团队，让更多人受益。为了构建跨企业协同的 API 保护模式，卓越中心团队期望与 Novant Health 的安全团队以及基础架构团队携手合作，共同利用Akamai API Security。

NOVANT HEALTH

扫码关注 - 获取最新云计算、云安全与 CDN 前沿资讯

Novant Health 是一家规模庞大的非营利性综合医疗系统，拥有 19 家医疗中心、2,000 多名医生，服务范围覆盖 900 多个地点，同时还提供众多门诊手术、医疗广场、康复计划、影像诊断中心和社区健康服务。Novant Health 在北卡罗来纳州和南卡罗来纳州拥有近 40,000 名团队成员和医生合作伙伴，致力于为当地的患者和社区提供优质的医疗服务。

Akamai