AKAMAI 客户案例

KKLab

这家创业工作室采用 Akamai 的 Zero Trust 解决方案，获得面向内部和外部网络的灵活性和保护机制

100

每天自动拦截 100 封存在恶意行为的电子邮件

在短短 30 分钟内设置概念验证

在加强安全的同时保持灵活性

2015 年前后，KKBOX 的研发部门（后于 2019 年成为创新研究公司 KKLab）开始认真审视信息安全问题。这支研发团队开展了多项不同的实验，并聘请了一支外部专业团队进行黑客入侵演习和渗透测试，以发现系统中的潜在漏洞，进而挖掘完善和改进机会。该部门决定实施多重身份验证，他们采用 Akamai Secure Internet Access Enterprise 来抵御定向攻击，并采用 Akamai Enterprise Application Access 来确保应用程序系统访问安全性。通过引入这两项云端信息安全服务，该公司实现了 Zero Trust 安全模式。

朝着 Zero Trust 架构发展的过程中，发现了传统 VPN 的不足

KKLab 的副总裁助理 Hung-Yi Chen 表示，KKBOX 集团一直以技术为导向。他于 2005 年毕业时加入该集团，15 年来始终专注于技术研发工作。随着集团的发展，他帮助引进了许多值得关注也富有挑战性的新技术。其中包括在 2010 年组建一支网站可靠性工程团队，引入 CI/CD 并部署了一个混合云架构。后来，他加入了云端技术服务提供商 KKLab，利用自身对于云技术和人工智能的研究底蕴，帮助企业推进技术转型。

KKLab 为集团旗下各企业（如 KKBOX、KKTV、KKStream、KKTIX 和 theFARM）的技术服务提供支持。他们还专注于人工智能和机器学习工具链、大数据高速计算平台、多种混合云环境搭建，以及咨询服务，并就这些主题与外部公司展开合作。该公司扩展了数字支持服务的范畴，为高科技制造、零售物流、媒体和娱乐以及金融和保险等领域的企业提供服务。

KKLab
中国台湾台北市
www.kklab.com

行业
媒体

挑战
借助多重身份验证、应用程序系统访问安全和进一步防范定向攻击的举措，朝着 Zero Trust 安全模式迈进

解决方案
- Secure Internet Access Enterprise
- Enterprise Application Access

在提供技术服务的同时，KKLab 也将信息安全视为一大重要目标。该公司特别引入了第三方信息安全测试能力，并利用黑客入侵演习来揭示系统中的潜在安全薄弱环节。当时该公司的许多员工都相信，他们公司的信息安全非常出色，应该能够轻松通过测试。但经过数据库攻击测试后，他们才发现，许多帐户和密码都可能被黑客攻破。这让 KKLab 团队意识到，通过 VPN 访问内部网资源的传统信息安全框架和概念实际上相当危险。一旦黑客获得内部帐户密码，他们就可能通过 VPN 进入内部网，随意窃取信息，给集团造成巨大的运营风险。

为了抵御风险，KKLab 采取了两阶段式安全强化措施。首先是强制实施多重身份验证机制。所有人都必须同时输入帐户密码和一次性验证码，这样才能连接到 VPN。此外，KKLab 积极规划实施 Zero Trust 架构，持续检查和验证每一位访问者是否确实属于合法用户。KKLab 的最终目标是围绕 Zero Trust 的理念，打造更灵活、更安全的工作环境。

借助 Secure Internet Access Enterprise 和 Enterprise Application Access 构建安全防护网，阻断所有可疑连接

Chen 指出，专注于娱乐媒体和流媒体技术服务的 KKBOX 集团希望能够利用这种灵活性，即时阻止恶意行为。该公司并不希望采取过度严格的控制措施，因为那会抑制员工创造力，也正因如此，KKLab 建议采用 Zero Trust 模型。该解决方案必须易于部署和维护，同时尽可能降低对于用户工作流程的影响。根据这些要求，该公司决定选择 Akamai 解决方案。

Chen 表示：“Akamai Secure Internet Access Enterprise 主要负责过滤和分析从内部网发起的连接，并准确判断目的地是否具有恶意 IP 地址或域名。这其中的关键就在于大数据数据库。”他还补充说，Akamai 拥有很高的市场份额。KKLab 选择 Akamai 的第一个理由在于，其基础围绕 CDN 和防范 DDoS 攻击的服务而建立，并且从这些服务中收集了大量的恶意行为数据。这些强大的资源是支持 Secure Internet Access Enterprise 有效运作的重要基石。

第二个理由是：他们也研究过市面上与 Secure Internet Access Enterprise 相似的解决方案，发现那些解决方案的部署要求有所不同。有些解决方案要求在每个终端设备上安装一个代理，有些则要求在企业主干网络上安装一个连接器。而 Akamai 支持同步连接。Akamai 连接器采用轻量级虚拟机映像的形式，只要求对一些网络设置进行调整。2018 年，KKLab 在短短 30 分钟内就完成了概念验证。通过这次概念验证，该公司确认，凭借丰富的情报数据库，采用 Akamai 连接器的 Secure Internet Access Enterprise 可以满足其需求，并因此敲定了与 Akamai 的合作。

> Akamai Secure Internet Access Enterprise 主要负责过滤和分析从内部网发起的连接，并准确判断目的地是否具有恶意 IP 地址或域名。这其中的关键就在于大数据数据库。
>
> **Hung-Yi Chen**
> KKLab 副总裁助理

在利用这款产品过滤内部和外部连接的基础上，2020 年，KKLab 采用了 Enterprise Application Access，以控制员工从任何地点访问内部网资源的行为。他们使用 Docker 映像部署了 Akamai 连接器。到目前为止，KKLab 已经通过 Enterprise Application Access 连接了 100 多个内部应用程序系统。KKLab 的许多合作伙伴都在使用更复杂的 VPN 通道连接到内部网系统，而 KKLab 则可以使用 Enterprise Application Access 模型，避免了更多 IT 维护的风险，并为同事免去了额外的维护负担。

自从部署 Akamai 解决方案之后，KKLab 不断学习成长，如今已经不再仅仅是 Akamai 客户的角色。KKLab 在企业客户服务方面有深厚的底蕴，为 Akamai 提供了许多对客户有益的建议和用例，例如在报告中增加更深入的信息。例如，除了了解某一时期木马或网络钓鱼等事件的统计数据外，KKLab 还希望知道哪些用户、哪些设备触发了这些事件。他们还建议，在报告中原有的文字与数字的基础之上，增加数据的可视化表现形式，例如饼状图、柱形图和折线图。Akamai 迅速回应了这些建议，调整了报告，让全球用户都从中受益。

如今，在 Akamai Zero Trust 解决方案的保护下，KKBOX 集团每天平均自动拦截约 100 封试图诱使用户访问带有恶意广告、恶意程序或网络钓鱼行为的网站的电子邮件。KKLab 还能轻松了解任何可疑的连接行为，并在问题产生危害之前加以防范。随后，他们可以审查架构或用户行为中的问题并做出改进，推动 KKBOX 集团信息安全不断提升。展望未来，KKLab 计划建立一个 Zero Trust 旅程体验模型，并将其以服务的形式提供给集团以外的公司，让各种公司都能从中受益。

原文发布于 iThome，2020 年 12 月 7 日。

KKLab 科科实验有限公司成立于 2019 年，致力于研发先进科技、加速产业发展、协助企业数字化转型，并且同步提供“AI 人工智能与机器学习、云平台建设和运营以及网站可靠性工程 (SRE)”等一站式服务。KKLab 同时拥有创新服务/IP 开发加速团队，协助开发新的业务机会。目前其服务范围跨越多个行业，如媒体、娱乐、电信、医疗、塑化等。 KKLab 持续改进技术、深耕产业，致力为客户和行业缔造更多价值。 www.kklab.com

扫码关注・获取最新CDN前沿资讯

 | 支持 | 发布时间：2023 年 1 月