

AKamai 客户案例

东海大学

东海大学通过 Akamai Secure Internet Access Enterprise
改善安全性并缩短事件管理时间

Akamai 帮助这所大学腾出安全团队资源并减少外部安全通知

现代公司面临复杂的网络威胁，因为攻击者使用越来越复杂的方法来绕过安全防御。您如何平衡针对此类攻击的主动防护需求与大学内的大规模国际化人群的灵活性和自由度需求？

这是东海大学计算机中心团队面临的挑战。该大学采用数字化学习技术，并建立了智能校园，为学生和教职员工提供校园内外的免费高速无线互联网接入。每个学年开始时，学生都会到来并将他们的笔记本电脑连接到大学网络。

但是，由于 IT 策略并未强制要求在学生的设备上安装防病毒软件，许多笔记本电脑都感染了恶意软件。这些被感染的设备导致校园内外的网络崩溃、消耗过多带宽并产生恶意僵尸网络流量。此外，恶意软件横向移动到该大学管理的计算机中，导致该大学收到了来自台中网络区域中心的通知，告知东海大学网络受到攻击，其网络正在发起异常连接。

网络技术总监欧建晖表示：“计算机中心安排了信息安全培训，敦促学生和教职员工不要点击电子邮件或网页中的任何奇怪链接。但攻击者花样百出，不断推出更狡猾的策略，这使得用户很难马上分辨某样东西是否合法，最终造成用户成为攻击受害者。”

东海大学网络部的张广钦说道，“依靠分析和识别恶意代码的传统防病毒软件和信息安全解决方案不够及时。如果环境中出现新的恶意软件变体，而防病毒软件供应商尚未识别它的代码和更新的签名，则无法检测到该恶意软件。由于加密 Web 流量的趋势，攻击者现在也在使用这些加密通道发起攻击，使零日攻击变得越来越难以阻止。”



东海大学
台湾台中
eng.thu.edu.tw

行业
公共部门

解决方案
[Secure Internet Access Enterprise](#)

重要影响

- 改善了安全态势，缩短了安全管理和事件解决时间
- 主动阻止来自感染设备的命令和控制服务器流量并减少横向移动
- 减少了外部安全通知的数量
- 通过将投资从资本支出转移到运营支出来优化安全预算



Akamai 有效阻止可疑连接

在意识到大学现有安全态势有待改进之后，计算机中心团队开始关注利用 DNS 作为安全控制点的产品。他们认为这种方法将使该大学能够提升整体安全性，而不会影响学术自由。

通过竞争评估流程，该大学选择了 Akamai Secure Internet Access Enterprise 作为其首选解决方案。Akamai Secure Internet Access Enterprise 采用云端服务的形式，可通过分析每个 DNS 请求主动保护网络及其用户。它通过 Akamai 优秀的互联网流量监测能力收集实时威胁情报，并对照其检查每一条查询，随后相应地阻止或交付请求的 Web 内容。

张广钦表示：“Secure Internet Access Enterprise 可检测并阻止对某些域发出的 DNS 请求，这些域可能提供恶意内容，比如勒索软件或挖矿恶意软件，或者会窃取用户信息。即使学生的计算机在校园里使用期间受到恶意软件感染，在计算机返回校园网络后，该恶意软件也无法从外部连接到攻击者的命令和控制服务器。”

在使用 Secure Internet Access Enterprise 之前，解决信息安全事件是一项艰巨的任务。收到异常连接的报告后，网络管理人员通常必须使用 IP 地址来跟踪受到感染的计算机，从日志文件中查找连接记录，以说服受影响的一方相信发生了事件，然后要求该方配合执行病毒清除流程。

张广钦说：“正因如此，解决事件大约需要一周时间，而且要占用我们大量的安全资源。但在部署 Secure Internet Access Enterprise 后，报告的安全事件数量大大减少，这使我们能够腾出资源来关注其他安全项目。”

张广钦又补充道：“Secure Internet Access Enterprise 的部署和配置特别快速且简单，这与传统物理设备完全不同，传统物理设备需要先断开网络连接，然后进行测试，接着才能将系统投入使用。使用 Secure Internet Access Enterprise 时，只需将 DNS 流量直接导向 Akamai 平台，这个过程会在几分钟内完成。”

欧总监表示：“Secure Internet Access Enterprise 可自动提供详细的事件报告，以便安全团队可以快速了解客户端计算机感染了哪些恶意软件，或者在计算机感染了加密货币挖矿恶意软件之前，用户点击了哪些 Web 链接。这些数据与我们的 SIEM 集成，因此这些报告还可帮助团队了解最近的任何异常网络活动，以便我们能够主动做出响应。”



部署 Secure Internet Access Enterprise 后，我们收到的安全事件报告数量大大减少，这使我们能够腾出资源来关注其他安全项目。

Kuang-Chin Chang

东海大学网络部

节省大量人力和成本

东海大学电子计算机中心主管杨朝栋强调了战略优势。“信息安全现在非常重要，随着数字化应用的发展，信息安全在未来将变得越来越重要。东海大学始终会优先保护 IT 应用程序和实施信息安全，并且大学主席支持投资信息安全。”

杨朝栋继续道：“回头审视 IT 当前的发展方向时，显然，基于云的服务始终都是趋势所在。以前的防御系统是使用软件和硬件组合进行部署的，并且维护、更新修补程序等工作需要投入人力和时间。”

Akamai 基于云的服务带来了改变，从而使维护工作得以减少。杨朝栋对基于云的信息安全服务的未来充满乐观，他说道：“它们不仅会减少人力，还会减少对物理计算机机房空间的需求，并节省空调和电力资源。这与计算机中心的目标一致，即减少设备机房所使用的能源量。”

杨先生指出：“在成本方面，与直接购买物理设备不同，在使用基于云的服务时，不需要一次性投入大笔资金。Secure Internet Access Enterprise 以年为租赁周期，这让东海大学能够更轻松负担这笔费用。”

随后，杨先生总结道：“信息安全工作永无尽头。但是，借助 Secure Internet Access Enterprise，事件管理工作量大大减少，从而 IT 团队有更多的余力来加强针对僵尸网络攻击的防御和开展更全面的活动分析。”



Secure Internet Access Enterprise 的部署和配置特别快速且简单，这与传统物理设备完全不同，传统物理设备需要先断开网络连接，然后进行测试，接着才能将系统投入使用。

张广钦

东海大学网络部



东海大学成立于 1955 年，是台湾第一所私立大学。该大学是首个、也是唯一一个拥有从幼儿园到博士的全面教育计划的教育机构。东海大学目前有九所学院：艺术学院、科学院、工程学院、管理学院、社会科学院、农业学院、美术和创意设计学院、法学院和国际学院。东海大学拥有大约 17,000 名学生和近 500 名教师：<http://eng.thu.edu.tw/>。