AKAMAI 客户案例

州立大学选择 Akamai 来保护 24 个校区的运营技术

全面的网络监测能力

分段策略

威胁检测与响应

客户

大型州立大学

这所大型州立大学满足超过 10 万名学生的高等教育需求，其 24 个校区共有超过 1.7 万名教职员工。

挑战

集中管理包含 600 多座建筑物的网络基础架构

某著名州立大学希望将建筑物自动化系统安全地整合到全州智能校园计划之中。负责大学实体设施和 OT 系统的团队担心，这些设备和应用程序缺乏分段保护机制。他们担心的另外一个问题是，如果大学的 IT 网络脱离了现有的物理隔离状态，会造成怎样的后果。因此，负责这项工作的团队决定做一件大事情，将建筑物的自动化系统集中起来，并提高安全性。

该大学的项目负责人解释说：“过去，所有校区几乎是各自为营，这种情况在大概两年前才有所改观。我们托管了主应用程序服务器，但是各个校区的控制器驻留在 IT 网络上，这些控制器也没有完全在不同的 VLAN 上与校区的其他流量分段。

这意味着，针对单栋建筑物控制系统的攻击一旦得逞，很容易就能在校园的 IT 网络中蔓延，反之亦然。

该项目还有另外一个经济方面的原因。项目负责人解释说：“我校想要管理能耗情况，看看可以从哪些削减成本，然而，由于各校区的系统彼此独立，我们无法获取这些校区的任何数据。

所以我们需要将它们连接起来，但也要保证连接建立过程的安全性。通过利用远程校园与我们的数据中心之间的连接，攻击者有可能创建后门，入侵我们的网络，还有可能发起攻击。”

Large State University

行业
教育

解决方案
Akamai Guardicore Segmentation

重要影响
- 防止横向移动
- 应用程序隔离

Akamai

这个雄心勃勃的项目旨在将所有设备都纳入共享网络基础架构，其范围涵盖 24 个校区的 600 多座建筑物。大学选择了该部门的设施自动化团队来执行这个项目。

然而，大学自动化系统的复杂性和所涉及的供应商数量又带来了一项艰巨的挑战。

“我们需要管理电梯系统、暖通空调系统、振动分析、照明、配电和电气计量。另外还有各种公用设施，包括锅炉、配电和废水处理。我们要与大约 260 多家承包商打交道，他们分别来自不同的公司，负责这些不同的系统。”所有这些供应商都需要访问网络，但又不能造成风险，也不能干扰彼此的控制系统。

> 防火墙管理系统无法与 [Akamai] 解决方案相提并论。
>
> 大学项目负责人

选择解决方案

迫切需求：东西向流量监测和集中化的策略

Tempered Networks 是一家专注于智能控制系统和物联网的安全服务提供商，这所大学与该提供商合作，解决偏远校区与大学主数据中心之间的南北向连接问题。在克服这一挑战之后，这所大学仍然面临着一大难题，他们需要保护数据中心内运行的 300 多台服务器免遭入侵。

这所大学的项目负责人回忆说：“我们当时想寻找有可能处理东西向流量的解决方案，但没有一款能达到我们理想的简洁程度。”

该团队最初了解到 Akamai，是接触到了他们免费的 Infection Monkey 入侵和攻击模拟工具。Infection Monkey 可帮助数据中心运营商评估其环境抵御入侵后攻击和横向移动的能力。

该团队下载并开始使用这款工具后，他们意识到，Akamai Guardicore Segmentation 可以解决 Infection Monkey 发现的问题。

当今市面上专注于微分段的解决方案并不多，Akamai Guardicore Segmentation 就是其中之一。它能帮助操作人员轻松定义、创建和部署安全策略，以管理单个应用程序或逻辑分组应用程序之间的通信。

在为大学进行的首次演示中，Akamai 团队展示了该平台独特的监测功能。凭借 Akamai Guardicore Segmentation，数据中心运营商可以查看在其环境中运行的所有应用程序，并以图形方式映射它们之间的依赖关系。

“这款解决方案很快就解决我们的问题，我们当时就认识到，这就是我们需要的产品。”

Akamai Guardicore Segmentation

Akamai 解决方案与内部防火墙的对比

“使用中央防火墙管理时，您还是需要为每个防火墙单独设置规则。有了 [Akamai]，我们可以创建一个应用程序群组，然后指定这些系统只能彼此通信。”

防火墙还存在成本、资源和可管理性等问题。“管理所有那些防火墙简直就是一场噩梦。我们可能需要六七个人来部署系统，确保不存在问题，然后还需要安排至少两个人专门负责管理。

此外，防火墙缺乏在应用程序级别上设置和修改策略的灵活性。“使用 [Akamai]，我们可以侦听一段时间，了解系统之间的通信情况，以及系统之间可能需要通信的原因。而防火墙是采取“全有或全无”模式。防火墙只会阻止端口到端口的通信，仅此而已。”

集中化、易于管理的微分段

他们认为，另外一项重要优势就是团队成员创建和部署规则的速度和便捷性。

这位项目负责人指出：“我们在启动它的第一天，就在几台设备上安装了这款解决方案，然后尝试创建了一项策略，阻止一家供应商看到另一家供应商。于是它就锁定了第一家供应商，就是这么简单。这充分证明了这就是我们一直在寻找的产品。”

Akamai 的微分段工具和方法并不需要专家。“这款产品足够简单易用，我们团队中的任何人都可以轻松驾驭它，对我来说，这是一个很有吸引力的卖点。”

不仅限于微分段：检测和响应

通过 Akamai 产品提供的监测能力，还能发现数据中心内的运营异常。这位项目负责人回忆说：“我们发现，一项打印排队服务连接到了一个并不属于我们的网络。我们追踪到根本原因后，发现是某位用户的远程桌面会话已经断开，但从未彻底终止，它还在不断尝试与其 PC 上的打印服务器通信。一旦这台 PC 遭到感染，就有可能成为攻击者入侵应用程序服务器的通道。”

现在，该团队在积极使用 Akamai 解决方案，这所大学也已经开始构想进一步提高安全性和效率的做法。

“在将来的项目中，我们要实现大量网络功能的自动化，以在发生事件时能够自动响应。例如，如果我们检测到某个建筑物内有一个恶意 MAC 地址或接入点，就可以使用 [Akamai Guardicore Segmentation] 向 Tempered Networks 解决方案发送命令，锁定该建筑物，然后向操作人员发送警报，提醒采取补救措施并查明发生了什么情况。就目前而言，我们还不具备这种检测能力。”

Akamai 平台让这所大学的设施自动化团队能够比以往更快捷、轻松地达到预期的安全状态。这位项目负责人解释说：“我们从来没用过这样的主动式工具，它能够持续监控一切。”

Akamai 可以监控数据中心的东西向流量，从而帮助其团队分担了这方面的工作。“我希望我们的团队能够专注于自身的职责，也就是帮助我校节省能源和资金。如果我们仍要为数据中心而担心，就无法专注于这项职责。

该大学的团队开始寻找一种简单易用的微分段解决方案。Akamai 解决方案满足了他们的心愿，甚至超越了他们的期望。

“产品的功能完全与宣传相符。”

> 在我们完成安装之后，支持团队就能够到达现场帮助我们完成部署，并设置一些保护规则，然后就地完成销售过程。
>
> 大学项目负责人

请访问 akamai.com/guardicore 以了解更多信息。