AKAMAI 客户案例

一家上市制造公司借助 Akamai Guardicore Segmentation 实现安全控制措施标准化并节省时间

这家制造公司需要一种全球安全解决方案

全面的网络监测能力

跨 IT 基础架构的分段

对勒索软件威胁的响应

客户

这是一家在纽约证券交易所上市的优秀制造公司，为世界各地的市场提供服务。

挑战

保护跨国企业

该公司的 IT 安全团队负责保护全球多个经营地点，其中大部分是具备混合用途的办公和制造设施。为了确保实现强大的安全态势，该团队需要在全企业范围内为安全控制措施实现标准化，并在位于不同地理区域的经营地点提供一致的保护。

负责开展分段项目的基础架构师解释说：“我们希望从开放的扁平网络迁移到采用最佳做法的分段架构。”

与许多公司一样，这家制造公司最初打算在该项目中选用防火墙。

但是，他们需要在整个网络中管理众多基于基础架构的规则和工作站级别的变更及升级，这项工作很快就变得非常耗时，即使仅在一个经营地点完成这些任务也是如此。此外，尽管改善了监测能力，但这种能力仍然局限于特定区域，导致团队难以全面、集中地了解网络活动以及资产之间的依赖关系。

阻止未经授权的横向移动

虽然防火墙提供了一些粗糙的分段控制措施，但它们无法解决安全团队面临的另一个关键问题：非托管式点对点通信。因此，必须将保护和监测范围扩大到该特定区域。如果不解决这个问题，就会使企业容易遭受“哈希传递”攻击、勒索软件以及其他依靠端点间横向移动进行传播的威胁的侵扰。

Manufacturing Company

位置
美国

行业
制造业

解决方案
Akamai Guardicore Segmentation

重要影响

- 减少恶意软件通过横向移动实现的传播
- 提供精细监测能力
- 通过分段保护端点
- 助力提升事件响应速度

Akamai

选择解决方案

在经历了几次不成功的防火墙控制措施部署后，该团队了解到了 Akamai Guardicore Segmentation，并开始在内部讨论新一代分段解决方案的好处和可能具备的前景。

该公司必须对自身实施的所有全新解决方案开展研究，因此这支团队还评估了几个备选方案。在经过全面细致的审查后，该团队最终选择了 Akamai Guardicore Segmentation。这位基础架构师表示：“只有 [Akamai] 能为我们提供整套解决方案，我们只需要使用客户端上部署的一个代理程序，就能进行流量监测，还能使用灵活的标签功能以及丰富的应用程序级监测功能。”

> “借助设备上部署的单个代理程序，我们已经彻底解决了通过横向移动发起端点攻击的问题。
>
> 一家制造公司的基础架构师

Akamai Guardicore Segmentation

在项目的第一阶段，该公司在大约 2,000 个工作站上部署了 Akamai Guardicore Segmentation。在部署该解决方案后，IT 安全团队立即发现，他们对于网络及其通信流的监测能力得到了极大提升。

实时获得新的见解并实施分段

这位基础架构师表示：“借助 [Akamai] 流量图，我们的监测能力现在提高了 1,000%，并且还能监测 PC 间的通信。”

该企业既能了解整体应用程序级活动，又能深入分析单个计算机的活动，并借此制定了更明智的安全决策。例如，一些用户在他们的公司笔记本电脑上安装了家庭打印机的应用程序。曾经发现，许多此类应用程序会不断扫描公司网络以查找支持的设备。根据 Akamai 监测功能提供的这一新见解，该团队能够阻止这些扫描。

Akamai Hunt：利用 Akamai Guardicore Segmentation 进行威胁检测

这种对网络活动的全新理解也帮助该公司阻止了外部的攻击者。例如，在该平台部署后不久，Akamai Hunt 服务检测到某个资产在与一个文件进行通信，该文件具有已知恶意软件（名为 GoldenSpy）的特征。Hunt 团队将检测到的威胁告知了该公司的 IT 安全团队。Hunt 团队还向客户提供了分析，其中涵盖了感染范围、潜在风险（将调查结果与 MITRE 的 GoldenSpy 信息进行匹配）、取证（利用 Insight）以及与内部调查和抵御措施有关的建议。该公司随后使用 Akamai 策略控制措施来隔离受感染的系统，并阻止恶意软件横向移动到新设备上。

标准化和节省时间

该公司现在还可以集中创建和管理策略，包括一项集中统筹的全球工作站策略，并且可以根据应用场景的需求灵活创建一次性的例外处理方式。这确保了在有 Akamai 代理的任何地方都能一致地执行策略，并减少了出现配置错误和延迟的风险。

此外，该企业的策略实施时间也得到了极大改善。例如，在部署新平台之前，要对防火墙控制措施进行修改，可能需要耗费几天时间。通过使用 Akamai 的新策略模板作为初始指南，IT 安全团队可以在一小时内为复杂应用场景创建安全控制措施，并在几秒内将其应用到部署的所有系统上。

与 Akamai 合作，共创未来

虽然该项目最初的重点是实现端点分段和访问安全控制措施的标准化，但该公司也在计划利用 Akamai 解决方案来应对其他应用场景。各方利益相关者正在讨论扩大保护范围，以涵盖服务器和关键应用程序，比如企业的 ERP 系统。

无论未来计划有哪些，在这家制造商看来，这一初始项目已经取得了成功，极大地缩小了公司工作站的攻击面并降低了所面临的风险。该团队现在对企业的安全态势更有信心，相信它能抵御在端点间横向移动的攻击。正如项目负责人解释的那样：“现在，借助设备上部署的单个代理程序，我们已经彻底解决了这个问题，我们现在可以在 30 秒内，在一台没有任何策略的工作站上全面实施安全控制措施。”

请访问 akamai.com/guardicore 以了解更多信息。

> 借助 [Akamai] 流量图，我们现在的监测能力提高了 1,000%，并且还能监测 PC 间的通信。
>
> 一家制造公司的基础架构师