AKAMAI 客户案例

通信基础架构提供商

使用 Akamai 的产品阻断勒索软件的攻击

预防了高达 100 万美元的潜在损失

阻止了潜在的影子 IT

监测东西向流量

客户

这家美国通信基础架构提供商致力于确保企业和居民在当今快节奏的世界中保持互联互通。该公司负责保障客户日常生活所依赖的基站网络和光纤网络的畅通运营。

挑战

端点监测能力和控制能力有限

整个企业中部署的笔记本电脑已超过 6,000 台，IT 安全团队越来越担心机群给日渐庞大的 IT 环境带来风险。此外，该公司一些高级用户的影子 IT 活动持续出现问题，亟待解决。

尽管最终用户计算团队已经采取了一些安全措施，但效果有限。这些措施都无法精细地控制用户对系统的访问，也无法限制对等连接通信进而有效阻止恶意软件传播，而后者是企业面临的重大隐患。

为化解这些挑战，利益相关者希望通过引入一款解决方案来改进企业的安全态势。借助该解决方案，他们能够对员工设备进行监测和精细分段控制。此外，他们还能发现并阻止未经授权的横向移动。

选择解决方案

一段时间以来，安全利益相关者一直在考虑使用 Akamai Guardicore Segmentation，有意将其用于多个网络安全用例。该企业决定采用分阶段的方法，以了解精细监测和简单直接的策略创建过程的巨大潜力。

通信基础架构提供商

位置
美国

行业
通信基础架构

解决方案
Akamai Guardicore Segmentation

重要影响
- 抵御勒索软件
- 阻止影子 IT
- 监测东西向流量

由于 Akamai 的软件定义的分段策略与底层基础架构并无关联，因此该提供商可以选择实施任意数量的安全举措。然而，由于员工笔记本电脑机群被确定为高风险，该团队优先将 Akamai 代理部署到其端点。

Akamai Guardicore Segmentation

该项目开始后，Akamai 精简的 Windows 代理很快部署到了企业的计算机上。这样便将用户访问和笔记本电脑活动纳入到了进程级监测范围内。

然后，IT 安全团队能够针对这些端点集中创建和管理安全管控措施，而所有这些都以准确的环境数据为基础。然后，他们立即制定了几条策略，包括针对特定的 Microsoft 远程桌面协议 (RDP) 活动（如登录尝试失败）发出警报。

精细监测的实际应用

部署后不久，所配置的用于报告 RDP 异常活动的策略就发出了一系列告警。很快真相大白，攻击者在发现一次又一次登录失败后，试图实施暴力破解攻击。

IT 安全团队密切监控这一情况，在发现攻击者持续深入展开攻击后，他们决定果断采取行动，利用 Akamai 代理阻止每个端点上的 RDP。只需点击几下，他们就制定并实施了一个新的分段策略。该策略禁用了 RDP，在任何端点遭受破坏之前，就及时阻止了攻击者。

阻断勒索软件

事后，安全团队很快意识到所有指征都指向一个臭名昭著且影响范围极大的勒索软件攻击者。

如果行动成功，攻击者可能会试图继续他们惯用的手段，在发出赎金通知之前加密一切可及的内容。鉴于提供商的组织规模和当前趋势，攻击者索要的金额肯定会超过 100 万美元。如果 ERP 系统等业务关键型资产受损，将带来严重的中断和停机。

然而，多亏安全团队和 Akamai 的快速应对，这次攻击尝试并未对企业产生任何影响。

阻止影子 IT

除了阻止外部威胁，该团队还能利用该平台应对内部挑战。在使用 Akamai 的产品之前，端点监测的范围有限，因此一些用户可以轻松避开官方流程，自行开展不符合企业政策的活动。采用新的见解和功能来对端点实施安全管控后，IT 安全团队能够遏制影子 IT。这包括阻止 DevOps 企业成员在未经官方渠道授权的情况下自行启动新资源。

使用 Akamai 的产品扩大保护范围

对于这家通信基础架构提供商来说，保护端点仅仅是开始。它计划探索更多新功能，在其数据中心部署 Akamai 的产品，保护其 Citrix 环境，并对外部供应商应用第三方访问控制。

凭借该平台的灵活性，IT 安全团队可以保证，无论未来如何推进其并购战略或数字化转型计划，他们都能够扩大保护范围，随时随地抵御环境中的高级威胁。

请访问 akamai.comguardicore 以了解更多信息。