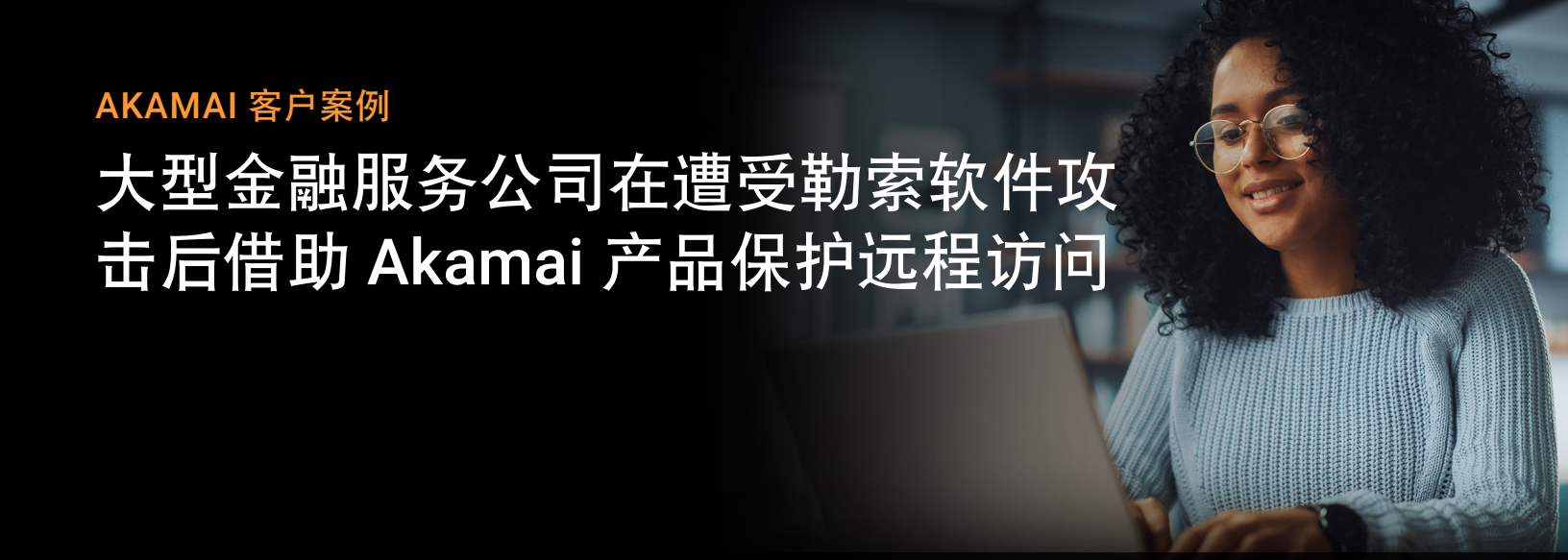
AKAMAI 客户案例

大型金融服务公司在遭受勒索软件攻击后借助 Akamai 产品保护远程访问



全面的网络监测能力

快速制定策略

保护远程员工

客户

总部位于巴西的一家大型金融服务公司。

挑战

远程访问增加

新冠疫情增加了许多企业的远程访问需求，这家金融服务提供商也不例外，该银行的许多 IT 员工改为在家办公，使用由公司管理的设备。为了完成工作，用户如今主要通过安全的公司网络访问必要的数据和应用程序，这造成这家公司的攻击面迅速扩大。

勒索软件攻击造成损失

在过渡到在家办公模式后不久，该银行的一个重要 Oracle Cloud 数据库遭到勒索软件攻击，后来他们发现，攻击的源头是 VDI 环境。安全和 IT 部门认识到，他们必须迅速采取行动，尽可能减少敏感财务数据丢失。此外，他们也知道，如果无法确定原始攻击媒介并采取针对性的防御措施，勒索软件就有可能横向扩展到备份服务器和企业生产环境。而这必定造成银行蒙受重大数据和财务损失。

选择解决方案

该银行已在其他领域广泛应用了 Akamai Guardicore Segmentation。在这次勒索软件攻击之前，该平台负责管理和执行 23,000 多台服务器的分段策略，其工作负载涵盖企业本地环境、虚拟环境、裸机和 VDI 基础架构，以及 Azure 和 OpenShift 容器环境。

该银行过去使用这一基于软件的分段解决方案实现了多项安全和合规性计划，包括对管理员跳转主机访问权限进行管理，以及执行 Swift 应用程序分段。在了解到该平台在提供卓越监测能力和快速策略制定时间方面的优秀往绩之后，响应团队快速采取行动，利用 Akamai Guardicore Segmentation 的功能应对入侵难题。

Large Financial Services Company

行业
金融服务

解决方案
Akamai Guardicore Segmentation

重要影响

- 减少勒索软件通过横向移动实现的传播
- 提供网络流量的精细监测能力
- 通过 VDI 环境分段来保护远程访问
- 实现快速事件响应

Akamai

Akamai Guardicore Segmentation 的优势

进程级监测能力

利用该平台，银行的响应团队对历史通信流开展了调查。通过追踪溯源，他们发现这一勒索软件最初来自一名数据库管理员的远程 VDI 连接与 Oracle Cloud 数据库的通信。

快速制定策略

在确定攻击媒介后，该团队快速跟踪了 VDI 分段，并将此列为头等要务。他们从星期六开始规划策略，利用 Akamai Guardicore Segmentation 的监测能力来界定潜在策略需求。到随后的星期二，该银行已为 3,000 多个连接到 Oracle Cloud 的 VDI 制定了可执行的策略。

勒索软件攻击后的恢复工作

该团队在备份应用程序上部署了 Akamai 代理，并配置了应用程序隔离，定义了什么应该可以与资产通信，并细化至进程级别。随后，他们将其部署到遭受入侵的区域，利用全局拒绝规则阻止勒索软件的进一步传播。

为了降低远程员工访问造成的额外风险，他们还为呼叫中心员工使用的两种 VDI 解决方案设置了策略，进一步阻止银行端点之间未经授权的横向移动。

分段策略在短短三天内就落地执行，帮助这家金融服务机构大幅降低了勒索软件事件的影响，并显著加强了未来的远程访问安全性。

> [Akamai Guardicore Segmentation] 提供的监测能力犹如一道光，驱散了黑暗！
>
> 大型金融服务公司基础架构安全主管

请访问 akamai.com/guardicore 以了解更多信息。

扫码关注 · 获取最新CDN前沿资讯