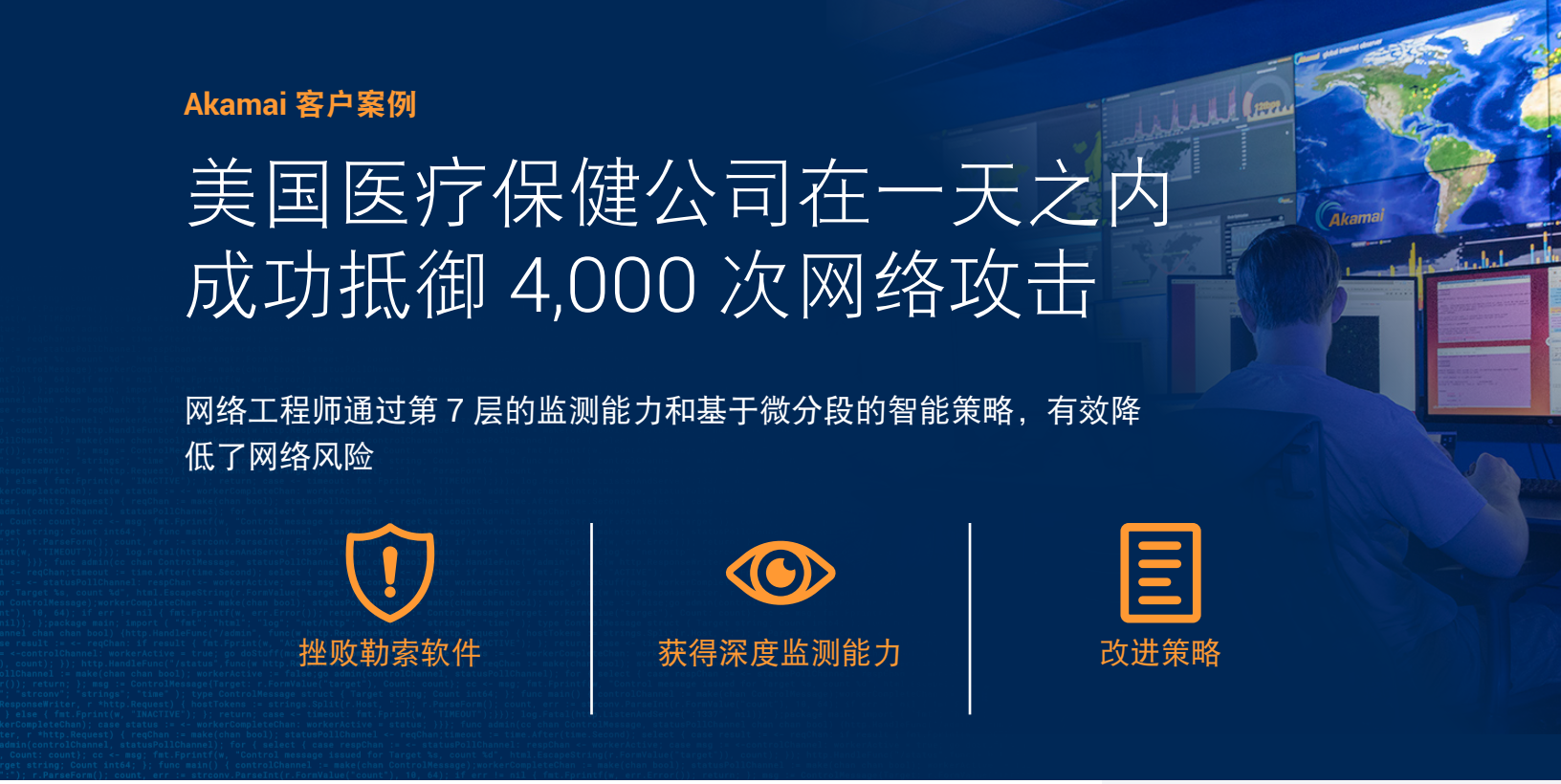
Akamai 客户案例

美国医疗保健公司在一天之内成功抵御 4,000 次网络攻击

网络工程师通过第 7 层的监测能力和基于微分段的智能策略，有效降低了网络风险



挫败勒索软件

获得深度监测能力

改进策略

让患者随时随地获享基础医疗保健服务

既要设法保护一个直接影响患者生命安危的网络，还要抢先防范日益复杂的网络攻击，这正是一家中等规模医疗保健公司所面临的现实情况。该公司的网络工程团队面临的勒索软件威胁日益严重。为了获得更强大的监测能力，该团队选择了 Akamai Guardicore Segmentation 来增强公司的安全态势。

扩展 Zero Trust 架构

该企业有一个宏伟愿景：利用 Zero Trust 原则增强其 IT 环境，同时符合 HIPAA 和 SOC 2 合规性的要求。由于风险很高，因此网络工程团队的目标包括：

- 即使在发生安全事件时，也能确保关键应用程序在线
- 通过遏制勒索软件攻击的速度来降低攻击影响
- 获得远超传统防火墙的精细网络监测能力

该企业需要一个既经济高效又可扩展，还无需对现有 IT 基础架构进行更替的微分段解决方案。此外，该解决方案还必须足够简单，方便精益团队进行管理，并且可以随着公司的发展而同步扩展。

正如一位网络工程师所解释的那样，“勒索软件以医疗保健行业为攻击目标。我们越快隔离并消除这些威胁，效果就越好。”

Healthcare Company

地点

美国

行业

医疗保健与生命科学

解决方案

Akamai Guardicore Segmentation

Akamai

找到正确的微分段解决方案

在迅速放弃采用容器化方法的方案之后，该公司对微分段解决方案进行了评估。该网络工程师解释道："我们希望获得下一代防火墙所具备的功能，也就是应用层的监测能力。"

在评估了很多解决方案之后，该企业注意到了 Akamai Guardicore Segmentation。一次成功的演示加上 Akamai 工程师的现场支持，最终促成了合作。该解决方案符合客户的所有需求，包括：

- **深度监测能力：**第 7 层检查和全面的网络见解
- **易于部署：**基于软件的代理，无需额外硬件
- **恢复能力：**核心网络中不会发生单点故障
- **灵活性：**支持各种操作系统

IT 基础架构和信息安全副总裁表示，Akamai Guardicore Segmentation 能够为精益团队带来巨大的优势。"在开始部署后，我们立即体会到了监测能力和控制方面的优势。"

IT 基础架构经理补充道："我们无需购买和管理多个东西向防火墙，从而节省了大量成本，而且还获得了无法通过防火墙实现的监测能力。"

阻断勒索软件的攻击

效果立竿见影，令人印象深刻。通过更好地隔离其应用程序以及使用 Akamai Guardicore Segmentation 开箱即用的勒索软件防范策略，该团队在一天之内成功化解了 4,000 次网络攻击。该解决方案甚至根据企业的特定需求定制了策略。

该网络工程师分享道："对于中等强度的策略，我们使用告警模式来标记事件，而不会导致停机。这是一种无需中断即可完善策略的好方法。"

> Akamai Guardicore Segmentation 不仅帮助我们解决了所面临的勒索软件问题，还改进了我们实现网络安全的方法。
>
> – 网络工程师

> “Zero Trust 就像是一座大山，翻越这座大山极具挑战性。Akamai Guardicore Segmentation 让我们快速翻过了这座大山，同时减少了费用和复杂性方面的挑战。”
>
> — IT 基础架构和信息安全副总裁

获得出色的第 7 层监测能力

这位 IT 基础架构经理表示，Akamai Guardicore Segmentation 提供了宝贵的见解，让我们可以深入了解不同应用程序之间的流量。这为该团队打开了一个数据宝库。现在，该团队可以检查第 4 层日志以外的详细信息：用户 ID、命令行输入，甚至服务相关性。

该网络工程师表示：“我们的网络团队可以查看流量来排查问题，并且可以为安全团队提供全面调查事件所需的信息。”

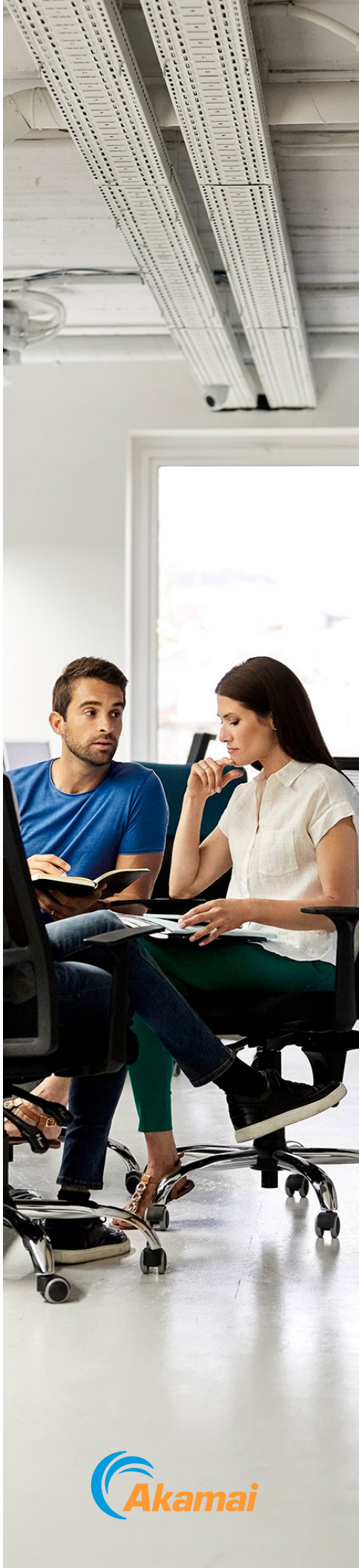
在出现意外的策略违反情况时，这种监测能力非常有用。新员工将 PC 直接连接到其运营商的客户本地设备 (CPE)，而不是连接到受家用级路由器保护的 LAN 端口。这是绝对不行的，因为 CPE 为 PC 分配了一个公共 IP，使其容易受到互联网公共扫描的影响。

正如该企业的网络工程师所解释的那样：“Akamai Guardicore Segmentation 立即检测到了该问题，让我们能够隔离该 PC 并在问题恶化之前加以解决。此外，也促使我们制定了一项旨在防止今后再次发生此类事件的策略。”

更智能的标签，更完善的策略

借助直观的标签和策略创建功能，网络工程团队可以轻松映射流量并实施安全规则。该网络工程师表示：“我们可以决定什么最适合公司的环境。该功能给我们留下了深刻的印象，远超我们的预期，并且帮助我们高效地制定了策略。”

例如，该团队限制了对打印服务器的访问，仅允许受信任区域进行访问，该举措立竿见影，增强了企业的整体安全态势。该工程师继续说道：“这让我们能够立即解决那些容易解决的问题。”



增强信心的监测能力

一个意料之外的好处？对内部流量和应用程序行为一目了然。借助这种新发现的监测能力，可以更好地与应用程序所有者进行协作，并优化了维护窗口。例如，该团队能够向应用程序所有者显示其流量是否被拦截。

该网络工程师表示：“过去，故障排除和面向未来一直是个难题。现在，在切换期间，我们能够自信地确认流量何时从旧服务器转移到新服务器。这让我们能够毫无顾虑地淘汰旧系统。”

该企业的 IT 基础架构和信息安全副总裁总结道：“Akamai Guardicore Segmentation 已发挥了重要作用，成为我们安全实践中不可或缺的产品。我期待在整个企业内扩大其部署。”

扫码关注，获取最新云计算、云安全与CDN前沿资讯