

AKAMAI 产品简介

Akamai Hunt 使最隐匿的威胁无处藏身

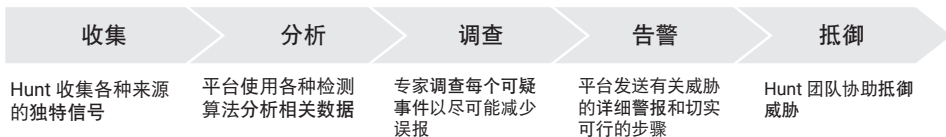
一种用于检测威胁和风险并进行补救的安全服务

借助 Akamai Guardicore Segmentation 的基础架构以及 Akamai 的全球大规模威胁情报，使您网络中最隐匿的威胁无处藏身

现代攻击经常能够绕过安全控制措施

诚然，在任何环境中随时都可能发生入侵，但 Hunt 团队一直致力于搜寻那些一贯能够绕过出色安全解决方案的异常攻击行为和高级威胁。在杀伤链的早期检测横向移动、恶意软件执行以及命令和控制通信等技术可能意味着能够避免灾难，即使安全控制措施失败也是如此。借助 Hunt，您会立即收到有关在您网络中检测到的任何严重事件的通知，我们的专家会与您的团队密切合作，以修复任何遭到入侵的资产，从而实现快速响应。

Hunt 处理流程



主要功能

全天候专家人工分析

我们的网络安全专业人员来自广泛的领域，包括安全研究、攻击安全、军事情报、红蓝对抗、事件响应和数据科学。

真实威胁告警

为了避免出现告警疲劳，Hunt 团队只会就真正的威胁向客户发出告警，从而完全避免误报。借助从全球客户群收集的数据，我们的专家维护着一项基准，以确保实现“健康的”数据中心和云应用程序通信，这有助于我们检测出影响力较大的威胁。

专有的搜寻工具

Hunt 专家经常会开发高级威胁搜寻算法（比如用户和网络活动异常、可执行文件分析、日志分析等），从而构建一个强大的工具集，可以实现快速检测和响应。Akamai Guardicore Insight 是一种基于 osquery 的强大工具，用于实时查询端点和服务器，并且包含在这项服务中，不需要额外付费。

对企业的好处



发现正在进行的攻击

Hunt 团队主动搜寻正在进行的攻击和新出现的攻击，从而尽可能减少攻击停留时间并缩短抵御时间。



为团队赋能

Hunt 专家代您的团队监测您的环境是否存在攻击者，从而帮您节省时间、精力和成本。



实现快速响应

您可以迅速获得每个检测到的关键事件的即时通知，这能赋予您信心，让您可以将工作重心放到业务方面。



获得量身定制的威胁搜寻服务

通过不断监测您环境中的攻击活动，该团队为您的安全配置制定了一个基准，并且可以根据您的具体拓扑结构定制搜寻方法。



具备丰富背景信息的威胁情报

我们的搜寻人员团队利用 Akamai Guardicore Segmentation 和 Akamai 的全球大规模威胁情报来收集各种入侵指标，包括 IP、域名、进程、用户和服务。

网络、云端和端点监测能力

通过整合来自 Akamai Guardicore Segmentation 部署点和 Akamai 全球传感器的数据（包括每天发送到 Akamai DNS 云的 7 万亿项 DNS 请求），可为我们的团队提供对您环境的全面监测能力。

即时通知和主动洞察

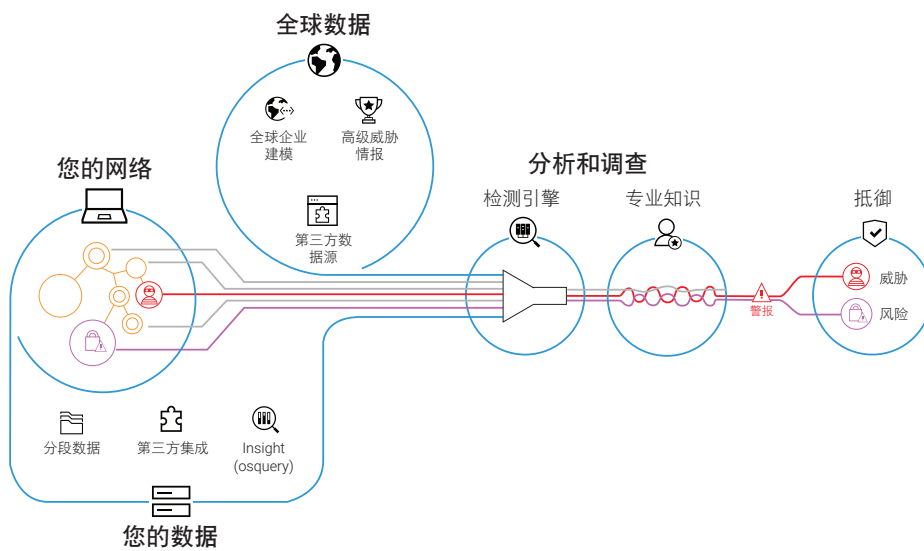
- 检测到威胁后，我们会立即向您发送威胁电子邮件通知。
- 定期发送的高级威胁报告，其中包括分析、统计数据和指标，使您的高管或董事会能够了解高调的攻击活动。
- 通过与 Akamai Guardicore Segmentation 控制台集成，可以轻松管理事件。



感谢 Akamai Hunt 团队协助我们处理数据泄露和执行快速补救。这帮助我们防止了关键任务系统出现数据泄露。

首席信息官

一家卓越的医疗中心



如需详细了解 Akamai Hunt 及其他安全解决方案，请[联系专家](#)。



扫码关注：获取最新CDN前沿资讯