AKAMAI 产品简介

Secure Internet Access ThreatAvert

保护至关重要的网络资产，辨别影响订阅者的恶意软件

服务提供商认识到，网络安全会直接影响订阅者的满意度，进而影响品牌价值。大多数威胁依赖 DNS 发挥作用，已有专门针对关键 DNS 基础设施而开发的新威胁出现。提供商需要重新考虑如何保护网络资源和订阅者，尤其是考虑到，在这个万事万物互连的世界中，威胁的动态性和多变性与日俱增。

Akamai Secure Internet Access ThreatAvert 实时评估 DNS 查找，以检测和中断恶意活动。Secure Internet Access ThreatAvert 的目标是导致网络中断或拖慢网速、对订阅者体验有其他负面影响或破坏其他网络保护的威胁，包括：

- 基于 DNS 的 DDoS，它们能通过海量查询造成解析程序不堪重负
- 爬虫程序恶意软件，它们将窃取宝贵的个人数据或入侵消费者设备
- DNS 隧道，它们在 DNS 内承载其他协议，进而窃用服务

Secure Internet Access ThreatAvert 由 Akamai 卓越的 CacheServe DNS 解析程序提供支持，配备 Akamai 动态威胁数据源。CacheServe 是可靠性的黄金标准——在多年投资的支持下，其性能和各种软件增强功能得以优化，即使面对 DNS 流量高峰，也能保证弹性和可用性。Akamai 威胁情报由 Akamai 数据科学团队创建，该团队每天处理来自世界各地超过 1,000 亿条实时流式传输的 DNS 查询。

DNS 服务器理应具备 DNS 安全机制

DNS 查询是恶意活动的主要指标，因为实现大多数恶意活动的第一步都是解析恶意资源（命令和控制服务器、恶意软件下载、泄漏网站等）的地址。DNS 解析程序是嵌入情报以瞄准威胁的理想场所，因为这些解析程序可以看到提供者网络上的所有查询。通过将传入的查询与动态威胁列表中的条目进行匹配，即可检测恶意活动。

相比随着数据平面流量扩容的专用分组处理解决方案，在 DNS 控制平面中扩容的 Secure Internet Access ThreatAvert 的成本、运营工作量和网络影响都要低得多。

它轻量、高效，并且不会因网络流量产生额外的延迟。它基于网络、覆盖每个设备，因此客户端和主机无需进行安全软件安装或更新。

业务收益

- 轻量化解决方案，可扩展至数百万订阅者，覆盖每台设备
- 领先的数据科学，提供卓越的威胁覆盖深度和广度
- 由于威胁数据源持续更新，即便漏洞利用攻击不断变化，仍可实现持续保护
- 易于理解的实时报告可显示威胁状态一览，并挺详细信息链接
- 威胁和遥测数据的高效收集和可扩展管理

出色的准确度以及威胁覆盖深度和广度

恶意软件开发人员不断创新，以实现其漏洞利用攻击的投资回报率最大化。这意味着大多数威胁经过精心设计以规避检测，并且会快速变化，以持续保持有效性。攻击面也已扩大，覆盖的物联网种类之多令人咋舌，为实现自己的目标，攻击者采用了高度多样化的方法。

在认识到威胁环境有着微妙、多样的特征之后，Akamai 数据科学团队开发、实施并集成了关键系统，以分析实时流式传输的 DNS 查询。该流程中还整合了信誉列表、蜜罐系统及其他第三方来源的威胁数据。出色的威胁覆盖范围广度和深度以及准确性和敏捷性要归功于以下方面的投资：

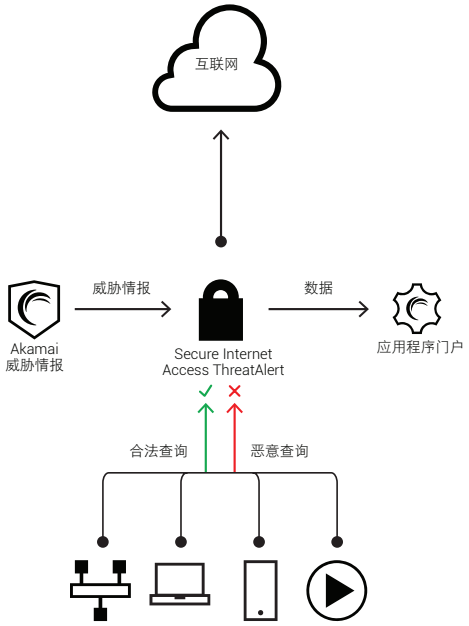
- 多种正在申请专利的算法，可即时检测异常行为（如 DNS-DDoS）、关联不同威胁，并确定新的爬虫程序域生成算法
- 多项高级技术，可自动将名称列入允许名单，以确保始终保护“合法”的 DNS 查询
- 具有多年安全经验，深入了解恶意软件和 DNS 数据的研究人员
- 支持实时处理实时数据流的全球网络和数据中心

精确策略可拦截非法流量、保护合法流量

Akamai 威胁情报源中整合了精确策略，以管理不需要的 DNS 流量。广泛而深入的功能集允许进行精确筛选，以瞄准恶意查询并保护（应答）合法查询：

- 精确策略可应用于传入的查询或传出的应答
- 筛选条件或速率限制可根据 IP、QTYPE、FQDN 或其他查询参数设置
- 筛选条件或速率限制可使用多种查询参数和逻辑运算符：QTYPE 和 FQDN、IP 和 FQDN 等
- 筛选条件或速率限制可与 Akamai 威胁情报动态威胁列表或运营商提供的列表进行匹配
- 策略和威胁列表可结合使用：与阻止列表匹配并且未在允许列表中
- 多个策略行为确定如何处理查询：放弃、合成应答、截断应答、NXD、NOERROR 等等
- 可将策略合并或嵌套起来使用，从而发挥更强大的功能

也可手动配置精确策略，以解决提供商网络中的局部问题。



Akamai 专家处理的大量数据流提供整个互联网中的恶意活动以及局部攻击的全面图景。

可扩展的数据管理、丰富的遥测和报告功能

Secure Internet Access ThreatAvert 整合了基于开放式解决方案的数据管理架构，该解决方案已在多个全球规模庞大的网络中得到验证，能够在万维网的体量和速度级别上实现卓越运营。来自 Secure Internet Access ThreatAvert 系统网络范围内的实时流式数据将聚合在一起，可用于报告（如下所述），还可供其他系统使用。弹性架构提供不间断的可用性，为不间断客户体验提供动力。提供适用于开放大数据系统（Splunk、Hadoop）的可选连接器或专门构建的应用程序，可用于获取额外的运营、安全和业务见解。

Secure Internet Access ThreatAvert 报告提供执行仪表板，显示拦截的 DNS 查询、节省的峰值 DNS 带宽、网络中排名靠前的恶意软件、受感染的订阅者以及威胁情报更新，进而实时评估安全态势。另一个安全仪表板提供 DDoS 和恶意软件明细图表。此外，只要点击一下，就能层层递进地连续查看有关恶意软件和受感染客户端的详情。自定义仪表板和报告可在几分钟内创建完毕，使用由用户定义的格式显示安全数据，从而满足独特的运营需求。基于标记的报告可让操作人员配置其 Secure Internet Access ThreatAvert 拓扑的视图，以满足其独特的要求。