AKAMAI 产品简介

Akamai Guardicore DNS 防火墙

全面监测和管控工作负载 DNS 流量

域名系统 (DNS) 对于互联网服务至关重要，但它无法区分良性请求和恶意请求。因此，企业纷纷实施 DNS 防火墙来检查 DNS 查询、阻止有害域名并解析安全域名。但是，随着 DNS 的使用范围不断扩大，将工作负载、服务器和其他联网设备纳入其中，如果缺乏对此类 DNS 流量的监测与管控，将给企业带来进一步的安全风险。

统一分段和 DNS 防火墙

Akamai Guardicore Segmentation 与 Akamai Guardicore DNS 防火墙相结合，为您的网络提供强有力的防御。此集成解决方案通过阻止恶意 DNS 请求并隔离关键网络区段，可显著减少您的攻击面并防止威胁传播。这种双层方法可增强安全性、确保合规性并保持高效运营，是实现强有力的网络保护的必备解决方案。

Akamai Guardicore DNS 防火墙的工作原理

Akamai Guardicore DNS 防火墙在几分钟内即可激活，可以在不影响性能的情况下提高安全性并降低复杂性。对照 Akamai 的实时威胁情报检查所请求的每个域，并自动拦截对恶意域的请求。将 DNS 用作初始安全层，可在查杀链的早期，在建立任何 IP 连接之前主动拦截威胁。此外，DNS 的设计对大多数端口和协议有效，因此能抵御不使用标准 Web 端口和协议的恶意软件。

如果 DNS 请求被阻止，就会创建一个事件，可为安全和威胁搜寻团队提供有关威胁被阻止原因的详细信息，在地图中直观显示的请求源和目的地，以及提供有关入侵指标的详尽信息。

对企业的益处

全面的威胁防护
通过在网络边界过滤 DNS 流量并在内部网络级别实施微分段，企业可以有效地防御恶意软件、网络钓鱼、命令和控制以及数据外泄企图。

更高的威胁搜寻效率
事件可帮助安全团队更好地检测、分析和应对新兴威胁，极大限度地减少入侵活动带来的影响并加强整体网络安全防御。

更高的监测能力和相关的上下文
结合 DNS 防火墙和微分段，可以更好地监测 DNS 流量模式，从而识别潜在威胁和策略违反情况。

简化管理
将 DNS 防火墙与微分段集成，通过提供统一的策略创建、实施和监控，简化安全管理。这降低了复杂性和运营开销，使企业能够高效管理其安全基础架构。

Akamai Cloud Security Intelligence

Akamai Guardicore DNS 防火墙依托于 Akamai Cloud Security Intelligence 技术，后者能够针对威胁及其带来的风险提供实时情报。Akamai 威胁情报旨在针对可能影响业务的当前和相关危险进行防范，并极大限度地减少安全团队必须调查的误报告警的数量。此情报以 Akamai Connected Cloud 每日采集的数据为基础，该平台每日管理高达 30% 的全球 Web 流量，并交付多达 14 万亿次 DNS 查询。Akamai 结合数百个外部威胁源，提升情报水平，并采用先进的行为分析技术、人工智能和专有算法不断分析和管理联合数据集。一旦识别到新威胁，这些威胁会被立即添加至威胁情报数据集，从而实现实时保护。

Akamai Connected Cloud

Akamai Guardicore DNS 防火墙服务依托于 Akamai Connected Cloud，这是一个分布范围超越同类平台的云计算、安全和内容交付平台。Akamai Connected Cloud 可以提供 100% 可用性服务级别协议，并确保为企业 DNS 安全提供出色的可靠性。

如需了解详情，请访问 Akamai Zero Trust 安全。