AKAMAI 产品简介

Secure Internet Access Enterprisee 基于云的 DNS 防火墙

随着企业采用直接互联网访问、软件即服务 (SaaS) 应用程序、云服务、随时随地办公策略以及物联网 (IoT)，他们的攻击面大大增加，并面临着大量新的安全挑战。保护企业和用户免受恶意软件、勒索软件、网络钓鱼、数据外泄等高级定向威胁的攻击变得越发困难。需要通过有限的资源管理传统本地解决方案中的安全控制点的复杂性和安全漏洞。

Akamai Secure Internet Access Enterprise 是一款基于云的域名系统 (DNS) 防火墙，它能帮助安全团队确保用户和设备在任何位置都能安全地连接到互联网，而且不存在其他传统安全解决方案固有的复杂性和管理开销。Secure Internet Access Enterprise 由实时威胁情报提供支持，此类情报基于 Akamai 对互联网和 DNS 流量出色的全球洞察力。

Secure Internet Access Enterprise

Secure Internet Access Enterprise 依托于全球 Akamai Connected Cloud 及 Akamai 运营商级递归 DNS 服务，是快速配置且易于部署的基于云的 DNS 防火墙，无需安装或维护硬件。

Secure Internet Access Enterprise 利用实时 Akamai Cloud Security Intelligence 来主动识别和拦截定向威胁，例如恶意软件、勒索软件、网络钓鱼和低吞吐量基于 DNS 的数据泄露。

无论员工从何处接入互联网，Akamai 门户支持安全团队都可以在数分钟内为所有用户集中创建、部署和实施统一安全策略和可接受使用策略 (AUP)。

对企业的益处

- 使用基于云的 DNS 防火墙将 Web 安全功能转移到云端；该防火墙只需在数分钟内即可在全球范围内完成配置和部署，而且可以快速扩展（不会对用户造成干扰）
- 通过主动拦截对恶意软件和勒索软件投放站点、网络钓鱼站点、恶意软件命令和控制 (C2) 服务器的请求，提高安全防御能力，并根据独有的最新威胁情报，识别低吞吐量 DNS 数据泄露
- 根据类别或风险评分来识别和阻止应用程序，从而控制对影子 IT 和未经批准的应用程序的使用
- 通过减少误报安全警报、减少来自其他安全产品的警报、随时随地在数秒内管理安全策略和更新以保护所有位置，最大限度地缩短安全管理时间和降低复杂性

工作原理

Secure Internet Access Enterprise 是一项基于云的安全服务，可以在不影响性能的情况下提高安全性并降低复杂性。这种保护可通过以下方法实现：使用一系列不同的方法（包括 IPsec 隧道、轻量级客户端）将递归 DNS 流量直接引导至 Secure Internet Access Enterprise，通过 Akamai 的托管 DNS 转发器转发递归 DNS 流量，或修改您现有的 DNS 解析器。

将根据 Akamai 的实时威胁情报检查每个请求的域，并自动拦截对已识别的恶意域的请求。将 DNS 用作初始安全层，可在查杀链的早期以及建立任何 Web 连接之前主动拦截威胁。此外，DNS 的设计对所有端口和协议有效，因此能抵御不使用标准 Web 端口和协议的恶意软件。该产品还能检查域名，以确定用户试图访问的内容类型。如果内容违反企业的 AUP，则予以拦截。

为了获得额外的防护能力，高风险域名会被转发给云代理以进行 URL 检查——根据 Akamai 的实时威胁情报检查请求的 HTTP/S URL，并自动拦截恶意 URL。

Secure Internet Access Enterprise 可轻松与其他安全产品和报告工具（包括防火墙、安全信息与事件管理 (SIEM) 解决方案以及外部威胁情报源）集成，让您实现对安全堆栈所有层的投资效益最大化。

此外，通过在设备上部署轻量级 Secure Internet Access Enterprise 客户端，企业还可以快速轻松地保护离线使用的笔记本电脑或移动设备。

Akamai Cloud Security Intelligence

Secure Internet Access Enterprise 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威胁提供保护，并最大限度地减少安全团队必须调查的误报警报的数量。

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 11 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、机器学习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 Secure Internet Access Enterprise，从而实现实时保护。

Akamai Connected Cloud

Secure Internet Access Enterprise 服务依托于 Akamai Connected Cloud（该平台是全球分布广泛的云计算、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 (SLA)，并确保为企业 Web 安全提供出色的可靠性。

对企业的益处

- 借助轻量级 Secure Internet Access Enterprise 客户端，实施您的安全策略和 AUP，无需使用 VPN 即可轻松降低风险，提高离线设备的安全性
- 通过阻止对令人反感或不当的域名和内容类别的访问，快速一致地确保合规及实施 AUP
- 借助 Akamai Connected Cloud 和 Akamai 运营商级 DNS 平台提升恢复能力和可靠性

基于云的管理门户

Secure Internet Access Enterprise 的配置和持续管理通过基于云的 Akamai Control Center 门户完成，确保随时随地均能实施管理。

策略管理方便快捷，更改能在数分钟内推送到全球，即时确保您的所有位置和员工均受到保护。您可以通过配置实时电子邮件通知和定期报告，向安全团队发出关键策略事件警报，以便立即采取补救措施来识别和化解潜在威胁。实时仪表板提供流量、威胁和 AUP 事件的概要信息。可通过仪表板上的单个元素明细查看有关任何活动的详细信息。详细信息为安全事件分析和补救提供宝贵资源。

所有门户功能可通过 API 访问，而且数据日志可导出至 SIEM，从而支持 Secure Internet Access Enterprise 轻松有效地集成其他安全解决方案和报告工具。

功能

安全性
拦截恶意软件、勒索软件以及网络钓鱼交付域和 URL
拦截恶意软件 C2 请求
识别基于 DNS 的数据泄露
代理风险域，对请求的 HTTP 和 HTTPS URL 进行检查
为要进行 HTTP 和 HTTPS URL 检查的域创建自定义列表
对客户流量日志进行回溯分析，以识别新发现的威胁并发出告警
创建自定义允许/拒绝列表
结合其他威胁情报源
自定义错误页面
查询 Akamai 的威胁数据库，获取有关恶意域和 URL 的情报
增强离线设备（Windows、macOS、iOS、Android、Chrome）的安全性
可接受使用策略 (AUP)
创建基于组的 AUP 策略
监控或阻止在线和离线用户违反 AUP 的行为
强制启用 Google、Bing 和 YouTube 的安全搜索功能

云访问安全代理（内联）
识别并阻止影子 IT 应用程序
根据风险评分或应用程序组阻止应用程序
SaaS 租户实施
报告、监控和管理
IDP 和 Active Directory 集成
通过可自定义的仪表板查看企业范围内的所有活动
详细分析所有威胁和 AUP 事件
全面记录和了解所有登入的流量请求以及威胁和 AUP 事件
传送所有日志；日志将保留 30 天，可通过 API 进行导出
可通过 API 提供配置、自定义安全列表和事件
通过 API 与其他安全系统（例如 SIEM）集成
基于电子邮件的实时安全警报
计划每日或每周电子邮件报告
委托管理
Akamai Connected Cloud 平台
用于递归 DNS 的每位客户专用 IPv4 和 IPv6 VIP
100% 可用性 SLA
Anycast DNS 路由，可实现最佳性能
实施 DNSSEC、DoH 和 DoT 以增强安全性
企业设备实际归属分析
使用 DNS 转发器进行内联实际归属分析
使用 Security Connector 进行脱机实际归属分析
适用于笔记本电脑和移动设备（Windows、macOS、iOS、Android、Chrome）的、基于客户端的实际归属分析

要了解有关 Secure Internet Access Enterprise 的更多信息，并注册使用免费的试用版，请访问 akamai.com/zh。

扫码关注，获取最新CDN前沿资讯