产品简介

Akamai Guardicore Segmentation 的 Exposure Analysis and Response (ExAR)

企业环境不断演变，一旦发生变动，您的静态安全边界便会自然脱节。攻击者利用这些结构性漏洞。他们现在采用人工智能来缩短传统漏洞利用时间，从数周缩短到大约 20 小时。人工速度补丁和静态安全边界已无法跟上机器速度侦察、AI 辅助漏洞利用和自动化横向移动的步伐。

Akamai Guardicore Segmentation 的 **Exposure Analysis and Response (ExAR)** 功能将微分段从静态网络控制转变为动态的、持续运行的安全层。

该平台将威胁检测和暴露感知整合到我们的方法论中，从而实现持续可达性映射、自动化行为检测和机器速度响应。

这种闭环方法助力您的安全团队持续验证策略有效性，立即准确定位活跃威胁链，以机器速度隔离易受攻击的资产，并在攻击损害您的业务之前先行自主阻断攻击。

核心挑战：连接路径的不对称性

大多数安全团队忙于管理孤立的离散信号，攻击者却在专注于寻找并利用通往数据的路径。传统防御层无法隔离真实风险，原因如下：

- **孤立的监测能力缺乏上下文信息：**风险暴露管理解决方案、检测和响应工具以及传统的分段解决方案通常存在于不同的孤岛中，这些孤岛彼此互不通信。而要全面了解攻击者的真实覆盖范围，需要网络、主机和身份检测之间相互关联，并结合基于分段现实的真实可达性。
- **严重性并不等同于可达性：**利用 AI，攻击者甚至可以将低严重性漏洞转化为重大影响。基于严重性或理论可利用性的漏洞管理，无法凸显因分段问题而暴露的漏洞。传统的分段解决方案缺乏原生漏洞检测功能，这为攻击者利用策略中的弱点带来了可乘之机。

给企业带来的好处

优先处理真实风险

根据真实可达性和业务背景，使用多维风险计算方式来评估风险暴露。即时隔离对您的重要资产构成最高爆炸半径的那部分网络访问路径。

以机器速度实施阻断

利用原生主动防御功能，瓦解高级后利用攻击手法、恶意横向移动和未经授权的 AI 工具。直接在应用程序层采取应对措施（如立即隔离易受攻击的资产），而不会造成运营延迟。

检测恶意活动

使用高保真、完全关联的事件取代被动告警分类，将主机进程、身份与网络遥测关联成一条无可辩驳的攻击链。

持续的态势保障

从时间点配置测试转变为自动化的持续性反馈循环。验证实施的 Zero Trust 规则是否在结构上遏制威胁并成功阻止横向移动。

Akamai Security

- **静态策略停滞不前：**规则例外、云蔓延、身份泄露和非托管资产不断侵蚀 Zero Trust 架构的实际成效。分段若无持续的自动化验证，只能提供理论层面的防护基线。

在 AI 加速型威胁时代，依赖于手动审核和静态策略墙，企业面临着高度暴露的风险。通过 ExAR 功能，Akamai Guardicore Segmentation 为您的遏制策略注入实战价值。这种新方法旨在将您的团队从持续救火式运维转为对真实内部攻击面的可预测、确定性控制。

暴露感知分段环路

通过持续性三步式闭环生命周期，ExAR 提供端到端安全性：

1. 了解并分析

ExAR 对攻击者在企业内部交互的确切攻击路径进行建模。通过将持续的资产发现和观测到的网络流量与详细的主机遥测、身份上下文和已知的软件缺陷相集成，该平台可以计算如果攻击路径未得到解决，您的企业将面临的真正风险。

2. 检测活动

内置的 **AI 威胁调查器**已超越理论风险和静态策略。
它可以自主检测活动并关联跨域遥测数据，以识别真正的攻击者行为。

- **威胁情报和入侵指标：**利用 Akamai 广泛的全球情报和入侵指标 (IOC) 来识别威胁。
- **高级威胁检测：**映射到 MITRE 框架的原生行为检测，用于检测隐蔽活动。
- **跨域攻击分析：**跨网络边界、身份池和端点关联安全事件。
- **横向移动检测：**经过微调，可在数据暂存前识别可疑的内部移动。

ExAR 在生产服务器上提供这些高级情报，不产生任何代理资源开销，也不会出现 CPU 使用率激增情况。

3. 主动防御

边界违规或后利用技术一经验证，ExAR 即可为安全团队提供快速响应行动手册和自动化抵御工具。可通过以下方式立即调整防御措施：通过原生 DNS 防火墙引入动态边缘拦截、部署真实的欺骗蜜罐以重定向并耗尽自动化攻击者工具、提供分段策略调整以封堵易受攻击路径，以及通过网络控制隔离易受攻击的资产。

最佳适用领域

带 ExAR 功能的 Akamai Guardicore Segmentation 专为以下应用场合打造：

面临 AI 驱动型攻击者的企业
意识到人工速度补丁周期和传统端口拦截防火墙无法阻止自动化、24 小时内的武器化窗口的企业。

遭受告警疲劳之苦的 SecOps 团队
必须适应当今现实环境的安全团队——根据企业重要资产的真实可达性，对风险与威胁进行优先级排序。

实现分段策略现代化的安全负责人
积极寻求分段解决方案的企业——该方案通过从第一天起就将 AI 驱动的威胁能力纳入考虑范围，使其防御面向未来。

敏感型混合基础架构受严格监管的行业（例如金融、医疗保健或核心制造业），这些行业需要确定性证据来证明安全控制变更不会中断生产正常运行时间。

Zero Trust 计划日趋成熟希望增加一层无可撼动的持续验证的企业，以确保应用和容器配置随时间变化时，网络边界始终保持有效。

基于资产的优化套件

在 AI 加速型攻击时代，威胁可以实时修改自身的攻击策略，在没有持续暴露映射的情况下部署分段会造成无法接受的监测能力盲区。

为了在防范失败时确保边界不失守，每次 Akamai Guardicore Segmentation 部署都可以从第一天起在整个企业全域集成 ExAR 套件。

功能矩阵

功能	增强版	高级版
高保真的关联事件（MITRE TTP, 取证数据）	✓	✓
跨域遥测检测（主机、网络、身份）	✓	✓
交互式暴露仪表板（全面态势分析）	✓	✓
智能体 AI 威胁调查器（自主检测和推理）	✓	✓
建议的操作（量身定制的响应操作）	✓	✓
深度主机级监测能力（原生嵌入式 osquery 遥测）	✓	✓
Akamai 威胁情报集成（全球情报馈送）	✓	✓
人工主导的全天候威胁搜寻（资深分析师调查）	⊘	✓
实时支持协调（事件实时指导）	⊘	✓
DNS 防火墙边缘保护（深度防御）	附加组件可用	✓
动态欺骗蜜罐（以机器速度实现攻击中断）	附加组件可用	✓

经证实的实际成果

案例研究 1：阻止权限滥用和隐蔽扫描

- **环境：**跨国电子产品制造商
- **事件：**攻击者攻陷了一个内部特权帐户，再经异常端口隧道化 SSH 流量以规避检测，并下载了一个自定义网络枚举二进制文件。
- **ExAR 的与众不同之处：**ExAR 的深度遥测能够看穿正常的网络活动，识别可疑可执行文件的隐蔽下载，其跨域引擎将网络扫描活动归因于同一个二进制文件和特权用户。由此，ExAR 生成了一个单一的高严重性事件，并明确推荐了关闭目标路径所需的分段规则。

案例研究 2：抵御 Active Directory 入侵

- **环境：**大型医疗保险提供商
- **事件：**攻击者利用 Cobalt Strike 框架快速部署了 10 个随机化 Windows 服务。这些服务抓取了凭据、枚举了目录配置并收集了 Azure AD 数据库文件。
- **ExAR 的与众不同之处：**传统的告警结构生成了一系列次要的、互不关联的事件。ExAR 即时将全部 10 个后利用动作关联为一条有序的攻击链，验证主动入侵，并建议具体的微分段边界，以阻止攻击者达成目标。

抢先一步，预防 AI 加速型威胁。立即申请演示。

© 2026 Akamai Technologies | 支持 | 发布时间：2026 年 8 月

扫码关注，获取最新云计算、云安全与CDN前沿资讯