AKAMAI 产品简介

针对物联网设备和运营技术设备应用分段策略

将 Zero Trust 分段功能扩展应用到所有连接的设备

许多企业正在加大对物联网设备和运营技术的使用，以推动增长、提升效率以及更有效地服务客户。这些技术能够解锁巨大的业务价值，但也会成为安全团队必须重点防御的新型攻击媒介。物联网设备特别容易出现硬件和软件漏洞，而许多传统运营技术系统则在设计时并未考虑互联世界中的安全需求。有了 Akamai Guardicore Segmentation，企业便可将 Zero Trust 安全扩展应用到这些设备上，从而降低攻击者利用这些设备入侵企业内其他 IT 基础架构的风险。

对企业的好处

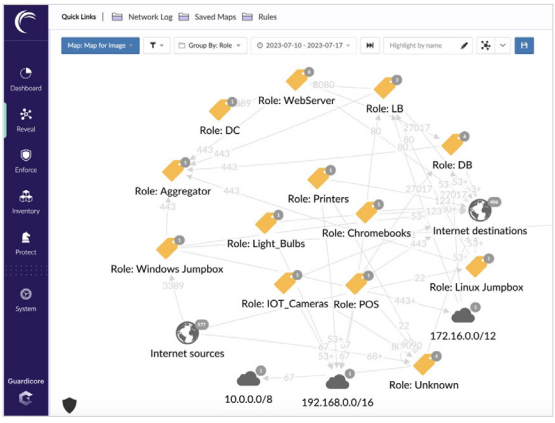
- 发现所有连入网络的设备，为其生成指纹并分类
- 通过单一界面，实施 Zero Trust 分段策略，包括针对特定的物联网和运营技术系统实施分段策略
- 结合基于代理和无代理的策略实施，确保全面覆盖

持续发现新连接设备

物联网设备和运营技术设备的部署与端点及其他传统企业设备大不相同。最显著的是，物联网设备和运营技术设备的部署数量要大得多，而且设备可能根据不断变化的业务需求，频繁地移动位置。Akamai Guardicore Segmentation 能够持续监控并发现所有连入网络的物联网设备和运营技术设备。这样便可确保未经批准的设备无法进行通信，同时对授权设备进行清点和保护。

识别所有连入网络的设备并分类

Akamai Guardicore Segmentation 具有集成式设备指纹识别技术。与使用易被伪造的设备标识符的方法相比，我们的方法更先进、更安全，因为它可通过分析网络行为和其他信号，为每个连入网络的设备生成可信的指纹。这些设备在被识别后会被分组到不同类别，进而方便创建可扩展的抽象安全策略。



全面监测您企业的所有资产

由 Akamai Guardicore Segmentation 发现并分类的物联网设备和运营技术设备会与更传统的企业端点和应用程序工作负载一起显示在 Akamai Guardicore Reveal 网络图上——这是一个高度交互式单一可视化界面。这使得安全团队能够轻松了解各种类型的连接设备如何相互作用，并制定有效的 Zero Trust 分段策略，结合基于主机和无代理的实施技术。

对所有设备应用精细分段策略

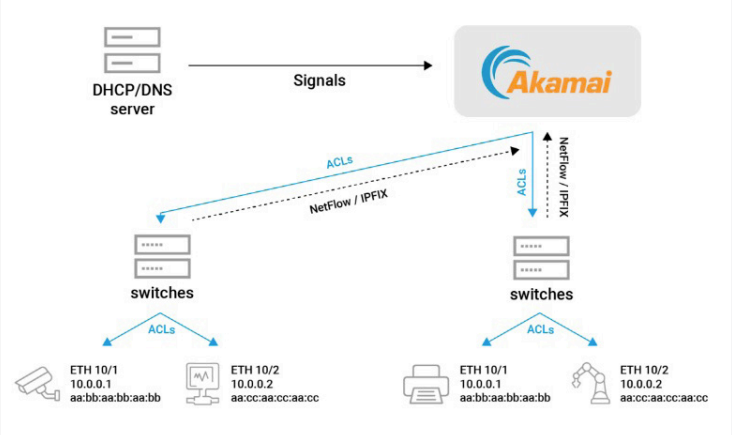
对于无法运行基于主机的安全软件的物联网设备和运营技术系统，Akamai Guardicore Segmentation 专门设计了基于网络的分段，无缝扩展了其 Zero Trust 策略的实施范围。这使您能够控制并限制运营技术设备和物联网设备之间的通信，以及与其他网络资源之间的通信。它还允许您建立安全边界，同时保持与 IT 管理系统、专用更新服务器和日志服务器等必要连接的畅通。

保持对漫游设备的可见性和控制能力

即使设备移动到新的网络位置，Akamai Guardicore Segmentation 架构仍能发现并监测这些设备。这些能力可确保始终实施适当的 Zero Trust 分段策略，包括任何所需的基于位置的调整。

工作原理

您的网络设备产生的流量会包含一些信号（例如，DHCP、DNS、Netflow、TCP 等），Akamai Guardicore Segmentation 可利用这些信号来识别所有设备并分类。然后，可通过统一的界面创建分段策略。对于物联网设备和运营技术设备以及其他无法运行基于主机的代理的设备，分段策略通过在网络层自动实施访问控制规则来执行。



敬请访问我们的网站，详细了解如何将 Zero Trust 扩展应用于物联网设备和运营技术设备