



通过全面的分段保护 AWS 中的工作负载—更轻松、更快捷的安全保护

不要让安全顾虑成为云采用的障碍。一种解决方案即可在 AWS 中提供监测能力，并实现横向移动防范以及入侵检测和响应。

全球超过 60% 的企业认为，[安全性是企业不采用云技术的主要原因](#)。将关键工作负载迁移到 AWS 的好处显而易见，您不必再承担基础架构成本和维护工作，可以利用几乎没有止境的资源和算力提高可扩展性和弹性，并利用机器学习和人工智能等创新大幅提升性能和分析能力。但安全方面的顾虑让许多企业望而却步。

AWS 环境中的安全挑战

在考虑全新的环境时，您需要从头开始重新评估安全性，这是情理之中的做法。您或许是刚刚接触云技术，也或许是迁移自不同的供应商，正在选择新的混合式解决方案，或是要将 AWS 添加到现有生态系统中。无论如何，云都需要自己的特定工具集，以应对这种基础架构带来的独特挑战。在所有挑战中，有些是所有云计算供应商所共有的，而其他一些挑战则是 Azure、Google Cloud Platform (GCP) 或 AWS 所独有的。在使用云或混合云（包括 AWS 技术）时，企业的部分主要顾虑包括：



了解共同责任：将工作负载迁移到 AWS 时，您需要认识到，您仍然承担着重大责任。您需要保护客户数据、应用程序和平台。Gartner 预测，由于客户对于责任共担模式的了解不足，到 2025 年，[99% 的云安全故障都将来自客户方过错](#)。



缺乏监测能力：您无法管控看不到的事物。在云环境中，监测能力要复杂得多，尤其是在保护和直观显示东西向和南北向网络流量时。仅关注流量还不够。您的关键资产可能分布在多个 AWS 账户、容器或网络安全组中，如果不对所有这些方面执行情境分析，就不可能准确了解流量和相互依赖关系。



对策略创建的控制有限：如果您的企业习惯于获得本地环境中第 7 层的洞察，那么必定不想在工作负载迁移到云之后降级为仅有第 4 层监测能力，失去精细的洞察力和控制力。亚马逊安全群组支持至多在第 4 层上控制流量。但无论底层基础架构如何，相较于仅依靠端口和 IP，第 7 层监测能力和控制能力都能赋予您更强大的能力，因为在很大程度上来说，仅依靠端口和 IP 不足以执行入侵检测或故障排查。



容器安全：AWS 使用亚马逊安全群组来应用容器安全策略，但这仅限于群集，而非个别 pod。为了全面了解通信情况，您需要找到一种解决方案，它应该能识别在顶层运行的叠加网络的情境，并且能精细地深入到 pod 层。如果要创建兼具虚拟机和容器的网络策略，情况会进一步复杂化，往往需要企业处理两套安全控制措施。

利用一体化安全平台应对这些难题

亚马逊提供了一些内置工具，如亚马逊安全群组，可应对将基础架构迁移到云端所造成的一些挑战。我们鼓励企业充分利用 AWS IAM（身份和访问管理），使用群组来分配权限、定期轮换凭证，并利用 IAM 组来简化工作。但在当今动态多变的公有云环境中，这些工具本身仅仅是起点，尤其考虑到混合环境覆盖较广，不但涉及到传统基础架构，还涉及到多云和容器技术等。先进的安全解决方案让您借助一项技术消除盲点，并与安全堆栈的其余部分无缝配合，即便在混合环境中也不例外，从而与 AWS 优势互补。以下是 Akamai Guardicore Segmentation 提供的优势：

全面监测 AWS 实例

IT 基础架构越复杂，就越需要深入、自动的监测能力。手动移动、添加、更改和删除不仅不可靠，容易造成漏洞和错误，而且会拖慢速度，成为云技术采用的障碍。相比之下，增强的自动监测能力可发现所有应用程序和进程，大幅提升实例监测能力，可细化至单个进程级别。

Akamai Guardicore Segmentation 附带强大的 AWS API，它可以提取编排数据，为您提供有价值的情境信息，可支持您执行标签添加和应用程序映射，还能自动拉取 EC2 标记，以直观显示 EC2 实例。对基础架构执行基准评估时，您可以获得必要的详细信息，从而充分了解应用程序彼此之间如何通信，在何处存在相互依赖关系，以及应如何创建策略以实现流畅性和敏捷性。用户可以通过一个仪表板直观查看原生云信息和 AWS 特定数据，而不必为每个云供应商或环境单独配备一种安全解决方案。我们的解决方案可跨多种平台、基础架构和云运行，为您提供零盲点的监测能力。

分段与执行——一项与工作负载关联的策略。

在所有环境中实现这种“单一管理平台”视图之后，即可开始设计和部署安全策略。应用程序感知策略比 Amazon 安全群组更进一步，提供了第 7 层而非第 4 层的粒度。有些企业目前尝试在本地环境中使用下一代防火墙来限制横向移动，但这只能对东西向流量实现粗略分段。若要将其用作精细分段控制解决方案，难度极其之高，因为企业需要对基础架构和网络做出大规模更改，才能调整流量路由，使其通过防火墙。即便这在本地环境中曾经是一种可选方案，也会给企业留下在云端保留这种水平的控制能力的难题。第 7 层微分段可以解决这种难题，其策略专门针对动态工作负载而构建，完全不需要更改底层网络基础架构。由于策略与工作负载本身关联，我们消除了手动更改的需要，并加强了企业采用敏捷、灵动的 DevOps 的能力。简化混合环境，一项微分段策略就能跨区域、VPC、容器、虚拟机和本地环境执行规则，而且所有这些环境均采用一致的策略表达方式。依托我们提供的监测能力，您可以在短短几分钟内完成分段策略的定义和应用。自动策略建议还能在公有云上提供出类拔萃的安全协议，这也能增强策略创建过程。

AWS 云上的入侵检测和事件响应

选择 Akamai Guardicore Segmentation 这样的全方位解决方案，您可以在 AWS 安全性方面更进一步，超越仅使用分段或监测能力能取得的成果。检测策略违规是入侵检测的重要环节，可让您实时应对潜在网络威胁，并提供应用程序级别的详细信息。我们提供多种入侵检测方法，支持立即就混合云环境中的恶意意图发出警报：

- **信誉分析：**自动检测流量中的可疑信息，检测范围从域名、IP 地址，一直到文件哈希值和命令行。
- **动态欺骗：**在攻击者不知情的情况下与其交锋，将他们转移到高度交互式蜜罐环境中，而您可以在此类环境中安全地了解他们的行为方式。





- **加速事件响应的工具：**我们的解决方案可集成 AWS，因此任何策略违规或安全事件都能实时发送到 AWS Security Hub。
- **定制威胁搜寻：**借助 Akamai Guardicore Segmentation 的基础架构以及 Akamai 的全球大规模威胁情报，通过 [Akamai Hunt](#) 服务阻止混合云环境中最隐匿的威胁。

全面统合，增强 AWS 及其他系统的安全性

迁移到云端并不一定代表着做出妥协，接受低于企业本地环境的安全性、监测能力或控制能力。利用 Akamai Guardicore Segmentation，您可以全面监测 AWS 实例和整个基础架构。利用这一基本映射，您就能实现无缝的策略创建，并增强 AWS 安全群组，从而在不需要人工支持的情况下实现精细控制。入侵监测和事件响应则补全了整块拼图，赋予您一个全面保护 AWS 云环境的端到端平台。

请访问 akamai.com/guardicore 以了解更多信息。



无论您在何处构建内容，以及将它们分发到何处，Akamai 都能在您创建的一切内容和体验中融入安全屏障，从而保护您的客户体验、员工、系统和数据。我们的平台能够监测全球威胁，这使得我们可以灵活调整和增强您的安全格局，让您可以实现 Zero Trust、阻止勒索软件、保护应用程序和 API 或抵御 DDoS 攻击，进而信心十足地持续创新、发展和转型。如需详细了解 Akamai 的安全、计算及交付解决方案，请访问 akamai.com 和 akamai.com/blog，或者扫描下方二维码，关注我们的微信公众号。发布时间：2023 年 5 月。



扫码关注，获取最新 CDN 前沿资讯