

# Gigamon 深度可观测性路线

为您的混合云提供更高级别的安全性和合规性保证

随着 IT 组织向应用程序和基础设施现代化迈进，他们正在转向混合云部署。虽然越来越多的应用程序迁移到各种公有云，但在可预见的将来，很多应用程序仍将留在本地。不幸的是，分布式的多供应商的架构管理也带来了复杂性。IT 团队可能很难保持一致的安全性和合规性态势。故障排除和解决问题需要更长时间。

这就是 Gigamon 深度可观测性路线的用武之地。我们简化了复杂的网络环境，使您能够重新掌握控制权。现在，您可以扩展熟悉的云或本地工具、流程和规程的价值，以保护您的云工作负载；此外，无论工作负载位于何处，均可设置通用策略。

Gigamon 通过消除安全与性能盲点，以及使用切实可行的网络衍生情报和见解补充指标、事件、日志和追踪 (MELT)，帮助保护您的混合云基础架构。通过提供借助深度数据包检测提取的信息，Gigamon 深度可观测性路线可为您当前的 SIEM、APM 和可观测性工具集带来更多安全用例。这些安全用例包括 1) 发现网络上的资产和 API 通信，2) 使用弱密码或即将过期的 TLS 证书识别托管或非托管主机，以及 3) 检测未经授权的活动，如加密挖矿。



图 1: Gigamon 深度可观测性路线可从任何来源获取动态数据，并将切实可行的网络级情报发送到任何安全或可观测性工具。

	功能	优点
接入	从任何虚拟机 (VM)、容器或物理网络基础设施获取流量；Gigamon 自动目标选择可以动态适应虚拟机或容器实例和位置的变化	可以轻松获得混合云基础架构中的东西向、南北向和容器流量的全面可见性，并可确保在云部署扩大或缩小时获得持续可见性
代理	可将网络流量数据包或元数据发送到在任何平台上运行的任何安全、可观测性或监控工具	可以通过重复使用现有的监控和安全基础架构，实现本地级别的安全性和合规性治理，并可加快云迁移
转换	筛选过滤、数据包去重、高级流量切片、负载均衡和 NetFlow 生成	可以显著降低工具成本开销，同时提高工具效率和有效性
丰富	应用程序元数据情报，具有 7,000 多个流量协议和与应用程序相关的元数据属性，适用于您的 SIEM 和可观测性工具	可以更快检测异常，加快对安全事件和性能瓶颈的根本原因分析
管理	通过 GigaVUE-FM 结构管理器或原生开发运维 (DevOps) 方法，统一了可见性管理和编排	可以减少在管理混合云和多云基础架构相关的运营开销

## 加快云应用

在加大云迁移力度的同时，如何确保您的应用程序和服务仍旧保持安全？为了实现安全保证和有效的安全治理，您需要在所有环境中保持一致的可见性。

现代化基础设施和应用程序还会迎接需要 IT 组织适应的重大变革。但是，变更管理需要时间。我们可以为您节省时间，因为团队无需为新的云部署从头重构安全和监控基础架构。相反，他们可以依靠熟悉、经过验证的数据中心工具、流程和规程。使用现有工具不仅可以节省时间和资金，还能帮助您实现一致的安全性和合规性态势。

借助 Gigamon 深度可观测性路线，即可全方位实现云转型。可以解决安全和运营问题，这些问题会拖慢数字化举措的速度，使贵组织容易受到威胁和漏洞的影响。

借助 Gigamon，您可以：

- + 放心地将应用程序迁移到公有云，同时满足严格的合规性和安全性要求
- + 使用您选择的解决方案整合您的安全和可观测性工具堆栈
- + 采取超越基于 MELT 的传统方法的云端主动安全态势
- + 监控不生成日志的非托管主机/端点和物联网 (IoT) 设备
- + 通过更全面地了解所发生的情况，加快根本原因分析和故障排除
- + 统一所有混合云基础架构间的可见性管理，轻松将流量映射和过滤到工具

# 解决方案

Gigamon 深度可观测性路线可以利用源于数据包、流和应用程序元数据的实时网络情报,扩展您现有的云安全和可观测性工具的价值。这是您首次可以在深度防御中添加一个新层,该层具有全面的数据包可见性,并能为您当前的安全和可观测性工具提供网络衍生情报和见解。

该解决方案包括:

- + GigaVUE® Cloud Suite, 配有 GigaVUE V 系列可见性节点和虚拟 UCT, 用于虚拟和容器基础架构中的流量获取、处理及转发
- + GigaVUE HC/TA 物理设备和物理 UCT, 用于物理基础架构内的流量获取、处理及转发
- + GigaVUE-FM 集中管理平台, 用于混合和多云基础架构中 Gigamon 深度可观测性路线的统一管理
- + GigaSMART® 应用程序 (如 SSL/TLS 解密、重复数据删除和应用程序元数据情报) 可以提高工具效率和可见性



图 2: 适用于物理和云基础架构的 Gigamon 深度可观测性路线组件。

## 流量智能

主要优点:

- + 可以通过删除网络交换机镜像/SPAN 端口、多个 TAP 点或多个虚拟镜像源产生的重复数据包,使流量减少 50% 以上
- + 可以删除或截断数据包或流,使转发到工具的流量减少 75% 或以上
- + 可以获得对 SSL/TLS 加密流量 (包括 TLS 1.3 加密流) 的可见性
- + 可以通过数据脱敏遵守数据隐私规则
- + 可以去掉不需要的标记和封装,提高您的工具的有效性和效率
- + 对于虚拟流量源、多站点互连和转发到虚拟工具的隧道支持

## 应用智能

主要优点:

- + 可以识别您的云和物理基础架构中运行的所有应用程序——影子 IT 和其他未获授权的应用程序
- + 可以筛除或专注于用户流量中的特定应用程序,使您的监控和安全工具更加高效和有效
- + 可以生成丰富的应用元数据,为无法接收原始数据包的监控和安全工具提供信息
- + 无需单独的探测器即可为视频分析工具 (例如 Nokia AVA 的 PVA) 创建视频数据记录

## 用户智能

主要优点：

- + 可对 3G、4G 和 5G 控制及用户平面会话进行筛选、安全列表和/或采样，将注意力仅放在重要流量上
- + 可在同一工具的多个实例之间平衡 3G、4G 和 5G 负载
- + 可对 SIP 信号和 RTP 数据会话进行筛选、安全列表和/或采样，将注意力仅放在重要流量上
- + 可在同一工具的多个实例之间平衡 SIP 和 RTP 负载

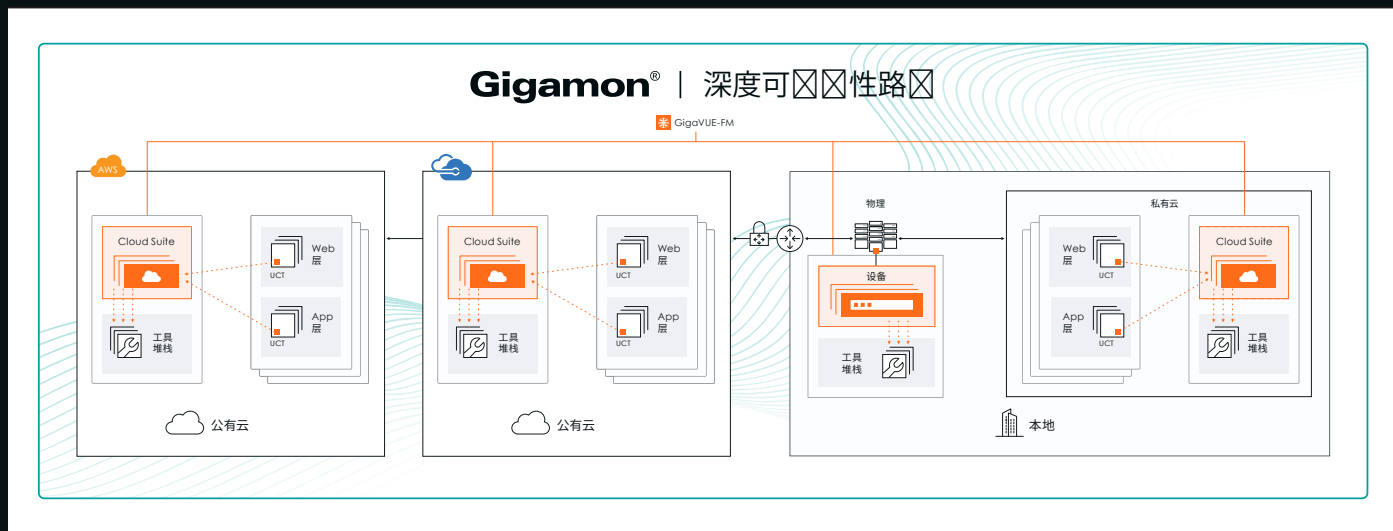


图 3: 使用 Gigamon 深度可观测性路线进行混合云部署。

## 结论

Gigamon 深度可观测性路线既可让您享受混合和多云基础设施的敏捷性及弹性优势,同时又能降低安全和违规风险。我们的深度可观测性路线利用网络衍生情报和见解来增强您的云、安全和可观测性工具的功能。网络情报与 MELT 数据的这种强大的组合,使 IT 组织能够确保安全性和合规性治理,加快根本原因分析,并降低与管理混合和多云 IT 基础设施相关的运营开销。结果: 贵组织可以实现云的全面转型承诺。

**Gigamon®**

全球总部  
3300 Olcott Street, Santa Clara, CA 95054 USA  
+1 (408) 831-4000 | [gigamon.com](http://gigamon.com)

© 2023 Gigamon。保留所有权利。Gigamon 和 Gigamon 徽标是 Gigamon 在美国和/或其他国家的商标。Gigamon 商标请参见 [gigamon.com/legal-trademarks](http://gigamon.com/legal-trademarks)。所有其他商标是其各自所有者的商标。Gigamon 保留更改、修改、转让或以其他方式修订此出版物的权利,恕不另行通知。