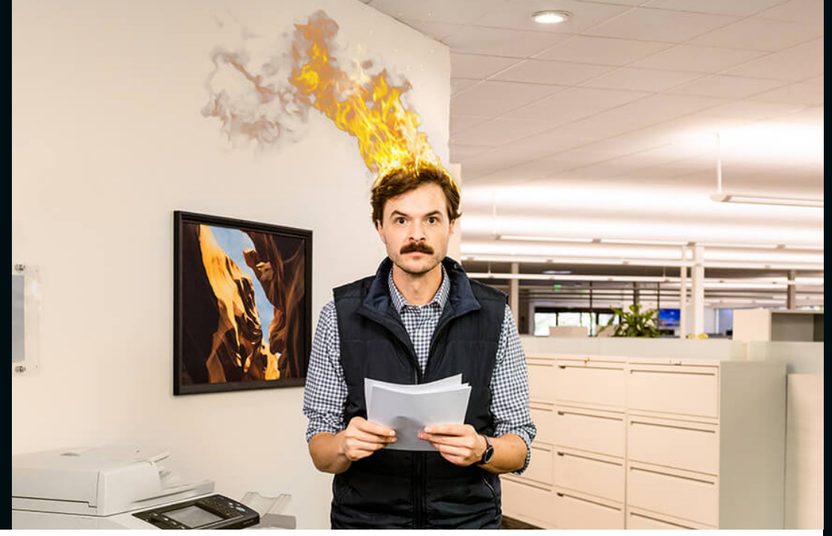
Gigamon®

如果没有深度可观测性，
您最后可能会焦头烂额。

网络衍生的情报可检测现有安全工具无法发现的威胁。

CISO 的难题



据《福布斯》，随着组织寻求在云转型中平衡业务灵活性与网络安全，预计到 2024 年，采用多云战略的大型组织数量将增至 85%[1]。

与此同时，网络攻击的成本和规模创历史新高，预计到 2025 年，全球网络犯罪成本将达到 10.5 万亿美元。[2]因此，各 CISO 面临着在愈加复杂的威胁环境中保护和监控其复杂基础设施的挑战，同时还要控制成本和复杂性。尽管在 SASE、EDR、网络细分领域和 SIEM 等最新安全策略和工具上的支出创下历史新高，但 CISO 仍难以应对日益增长的新兴威胁，尤其是勒索软件和内部漏洞。

1. Marr, B.（2024 年 2 月 20 日）。《2024 年十大云计算趋势：现在每个人都必须做好准备》。《福布斯》杂志。
2. Gartner 预测，到 2024 年，全球安全和风险管理支出将增长 14%。

漏洞对利润的影响

安全漏洞不仅会带来经济损失，还会以多种方式冲击业务：

- 造成停机和收入的损失，扰乱业务运营。
- 通过 IP 和客户数据盗窃损害组织的声誉和客户忠诚度。
- 导致网络保险成本增加（甚至无法购买）。
- 使组织及其高管面临监管和合规罚款的风险，甚至可能面临牢狱之灾。

您的安全工具表现很好：但这只是您所知的冰山一角。

如果没有深度可观测性，您最后可能会焦头烂额。

网络最大的盲点：横向流量和加密流量

随着云采用率的提高，保护和管理混合云基础设施的成本和复杂性也随之增加。不同的基础设施组件都有自己的监控工具和流程，这导致工具堆栈孤立且分散，无法让您全面了解混合云基础设施中的真实情况。

您的安全工具对纵向威胁表现良好，但意外的是对横向威胁却视而不见。

大多数安全工具会检查南北流量，但经常会忽略横向移动，这可能会给您的组织带来毁灭性后果。如果威胁行为者入侵您的网络，他们可以在混合云基础设施中自由移动而不被发现，最终获取组织敏感数据。

Gigamon Deep Observability Pipeline 是唯一专注于消除这一盲点的解决方案，它提供了横向可见性，能够检测以前难以发现的威胁，包括可能已经存在于网络中的威胁。

潜伏在加密流量中的危险

鉴于 95% 的网络流量是加密的，[4]在加密流量方面缺乏可见性的组织会面临其现有安全工具无法发现的隐藏威胁。随着加密技术的发展，威胁行为者利用加密渠道的机会也在增加。

每个网络都有隐藏的东西。直到现在。

解密所有流量既昂贵又复杂，需要很高的计算能力，同时会增加延迟并降低性能。但现在，您有了新的解决方法。Gigamon 提供强大的专利解决方案组合，包括我们屡获殊荣的 Precryption™ 技术和 GigaSMART© TLS/SSL 解密，这使获取加密流量的可见性变得经济实惠且可扩展。

在过去一年中经历过加密渠道攻击的组织中，85% 的组织目睹了针对“受信任”渠道的攻击（比如受信任组织或第三方供应商的合法网站），这清楚地提醒人们，没有 TLS/SSL 加密流量是绝对安全的。[5]

4. Google 透明度报告
5. Zscaler ThreatLabz 2023 加密攻击状态报告
6. 2024 年 Gigamon 混合云调查

准备不足

对加密流量安全性的过度自信会催生容易被利用的巨大盲点。

76%
的 CISO
相信加密流量是安全的

63%
的 CISO
认为加密流量不太可能被检测到

86%
的网络威胁
隐藏在加密流量中

62%
的公司
发现过去一年针对加密渠道的攻击有所增加[6]

即便是最强大的安全和可观测性工具也会存在盲点。

深度可观测性助力观测冰山全貌。

传统和原生云工具仅通过指标、事件、日志和跟踪 (MELT) 数据获得可见性，在识别范围以及监控当今复杂基础设施的深度或广度方面都会受到限制。

Gigamon Deep Observability Pipeline 超越了传统的可观测性方法，直接从网络流量中提取情报，并将其高效、实时地传递给您的工具。借助这种网络衍生的情报，您的工具可以检测出以前隐藏的威胁，从而帮助您降低应对攻击的成本和问题严重性。

深度可观测性有助于消除盲点，为您的工具提供所需的网络衍生情报和见解，从而检测以前可能被忽视的威胁。

实时威胁检测的重要性日益凸显

随着攻击者缩短了从最开始进入入口、横向移动和成功入侵之间的时间，网络攻击变得越来越快，攻击性也越来越强。

62 分钟

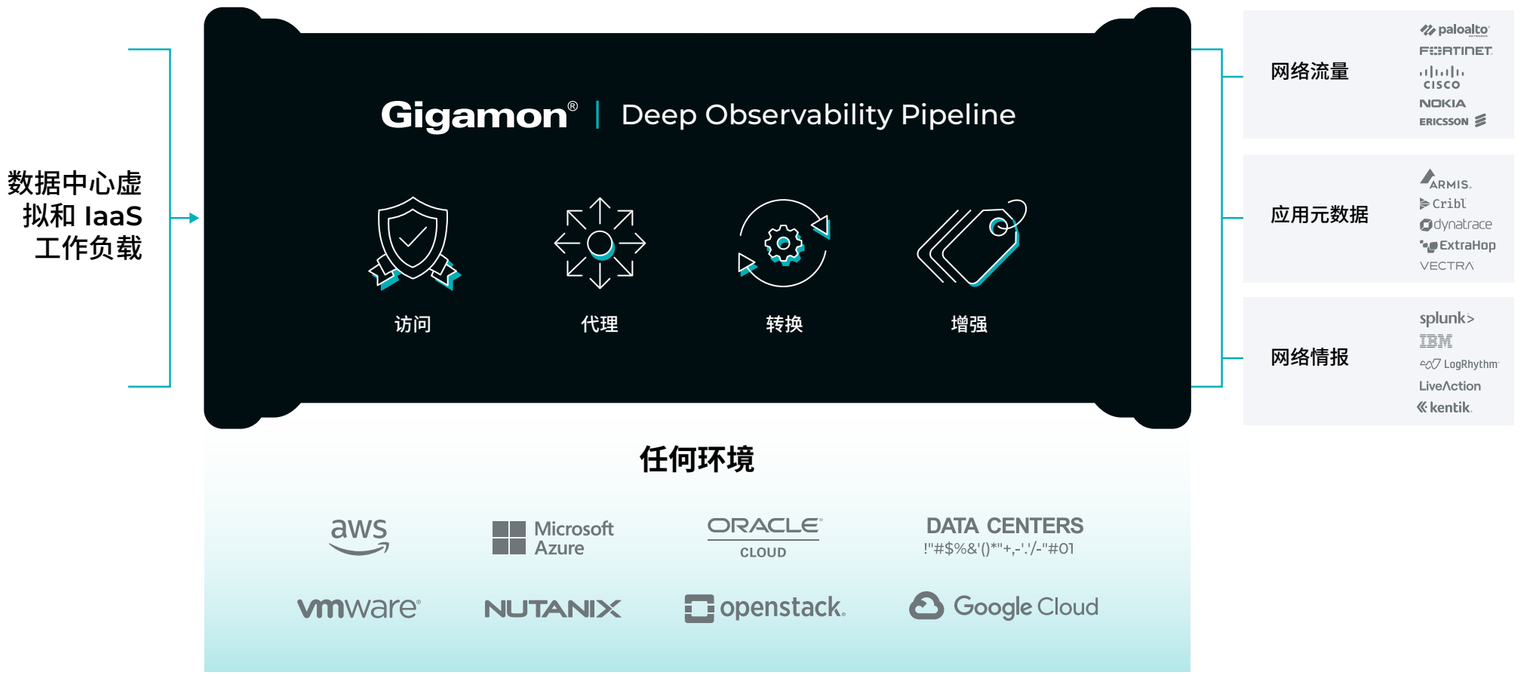
自去年以来，威胁行为者从组织内部最初受感染的主机转移到另一台主机所需的平均时间加快了 23%，有些只需要几分钟就能成功。

204 天

组织平均需要 204 天才能发现数据泄露事件，而发现数据泄露则需要 73 天。[7]

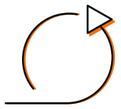
7. CrowdStrike 2024 全球威胁报告

专门构建的深度可观测性管道



基于 GigaVue Cloud Suite™ 的 Gigamon Deep Observability Pipeline 能够高效地向您的云端、安全和可观测性工具提供源自网络的情报。这有助于消除安全盲点并降低工具成本，使您能够更好地保护和管理混合云基础设施。

增强安全工具，取得切实成果



提高敏捷，降低成本

加强安全态势不一定要靠投资更多工具。实际上，事实证明，拥有太多的工具在检测和缓解威胁方面效果较差，因为它们会让安全团队不堪重负，并造成数据孤岛，产生可见性差距和盲点。[3]

Gigamon 可优化工具的性能和有效性，帮助组织管理工具无需扩张，降低成本，最重要的是，获得消除盲点所需的深度可观测性。

节省运营成本

通过优化和改善网络流量采集的信噪比，Gigamon 客户通常可以节省 50-60% 的工具支出，并且可以推迟年内的扩容购买计划。Gigamon 不再需要昂贵的云网关和负载均衡服务，这将云流量获取成本从每千兆字节 GB 0.75 美分降至 0.04 美分。

深度可观测性使您现有的安全和可观测性工具的效率提升最多 90%，并将工具和带宽成本降低最多 50%：普通中型客户在 4-6 个月即可实现投资回报。

3. 2020 年网络弹性组织报告

防患于未然。

如果没有深度可观测性，您很容易受到看不见的威胁侵害。

深度可观测性的市场领导者

根据市场情报研究公司 650 Group 的数据，Gigamon 是深度可观测性的市场领导者，在 2023 年拥有 63% 的市场份额。

全球最具安全意识的政府机构和企业依靠 Gigamon 来切实降低风险。

4,000+
全球客户

10 家位居前 10 的
美国联邦机构

8 家位居前 10 的
知名医疗保健提供商

100 家中的 83 家
《财富》100 强公司

7 家位居前 10 的
全球知名银行

9 家位居前 10 的
知名移动网络运营商

“在过去的六个月里，我们很快检测到几起事件，就在攻击者获得服务器所有权后大约一个小时内。我们得以在任何实际损害发生之前就及时抓住他们，这得益于我们采用的安全工具，Gigamon 也在向这些安全工具注入大量数据。”

Kajeevan Rajanayagam，
University Health Network 网络安全总监

“组织不断将越来越多的工作负载转移到云中，但由于缺乏可见性，这些混合和多云环境带来了重大的安全挑战。使用 Gigamon 和 Vectra AI 创建一站式解决方案是云安全的重大突破。现在，我们能够为全球客户提供适用于所有云网络的完整网络防御解决方案，通过将 Gigamon 与 Vectra AI 基于 AI 的一流威胁检测、调查和响应平台相结合，为他们提供所需的深度可观测性。”

Paul Eccleston，
Exclusive Networks 欧洲、中东和非洲高级副总裁

“去年，随着漏洞、勒索软件和数据泄露的报道，我们看到了新的网络安全威胁的影响。这些漏洞使深度可观测性，及其对加密流量提供的横向可见性，成为所有组织运营的关键基础，推动了当今对安全和 IT 预算的需求。Gigamon 凭借其深度可观测性管道保持领先地位，为保护和管理现代混合云基础设施提供了一种创新的方法。”

Alan Weckel，650 Group 创始人兼技术分析师

结语

在 Gigamon，我们的目标是保护全球结构复杂的大型组织，为其混合网络和数据保驾护航。我们致力于学习、协作和创新，力求提供保护组织免受网络威胁的解决方案。根据员工、合作伙伴和客户的意见，我们开发了深度可观测性管道，可提供当今最高水平的混合云安全性。

让 Gigamon 通过添加以下内容，增强您的云、安全和可观测性工具性能：**具实操性的网络衍生情报和见解**。

了解有关深度可观测性的更多信息

Gigamon®

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