混合云安全

认知 vs. 现实

一项针对全球1000名IT和安全领导者所做的调研显示，不少人对混合云安全性和可见性的认知与现实情况不符。另外，不断发展的立法工作也成为广大CISO主要担心的事项，这也表明实现深度可视化比以往任何一个时候都要重要。

认知 vs. 现实

94% 的全球受访者表示，安全工具和流程可以帮助他们实现对IT基础设施的全面可视化并获得洞察力。

50% 的受访者相信或者完全确信，其整个IT基础设施（从本地到云端）都受到了妥善保护。

96% 的受访者认为，实现云安全，依赖于对全部动态数据实现可视化。

97% 的受访者认为，在漏洞检测和响应方面，IT部门内部可实现良好协作。

只有 **30%** 的受访者可实现对加密数据的可视化，而三分之一的CISO则对如何确保其敏感数据安全缺乏信心。

只有 **10%** 的受访者表示，在过去18个月中未遭遇数据泄露事件。

超过 **30%** 的数据泄露事件未被安全或可视化工具发现。

超过 **16%** 的公司尚未实施集体负责制， SecOps作为负责安全的团队一直在孤立运行。

对可视化带来的风险，受访者的看法有些天真

除了对实现全面可视化抱有信心之外，IT和安全团队承认其IT基础设施中存在一定数量的已知可视化缺失。

他们会把可视化缺失看作一种威胁呢？

26%
超过1/4 (26%) 的受访者担心他们缺少实现组织安全所必需的工具和可视性。

52%
的组织无法实现对横向移动数据（也被称作东/西向流量）的可视化。

35%
的组织对容器流量只能实现非常有限的可视化。

意料之外的盲点
对意料之外的盲点的利用，成为56%受访者最担心的问题。

立法
立法（34%）已经成为主要的压力因素，如欧盟《网络弹性法案》便给全球出了难题。

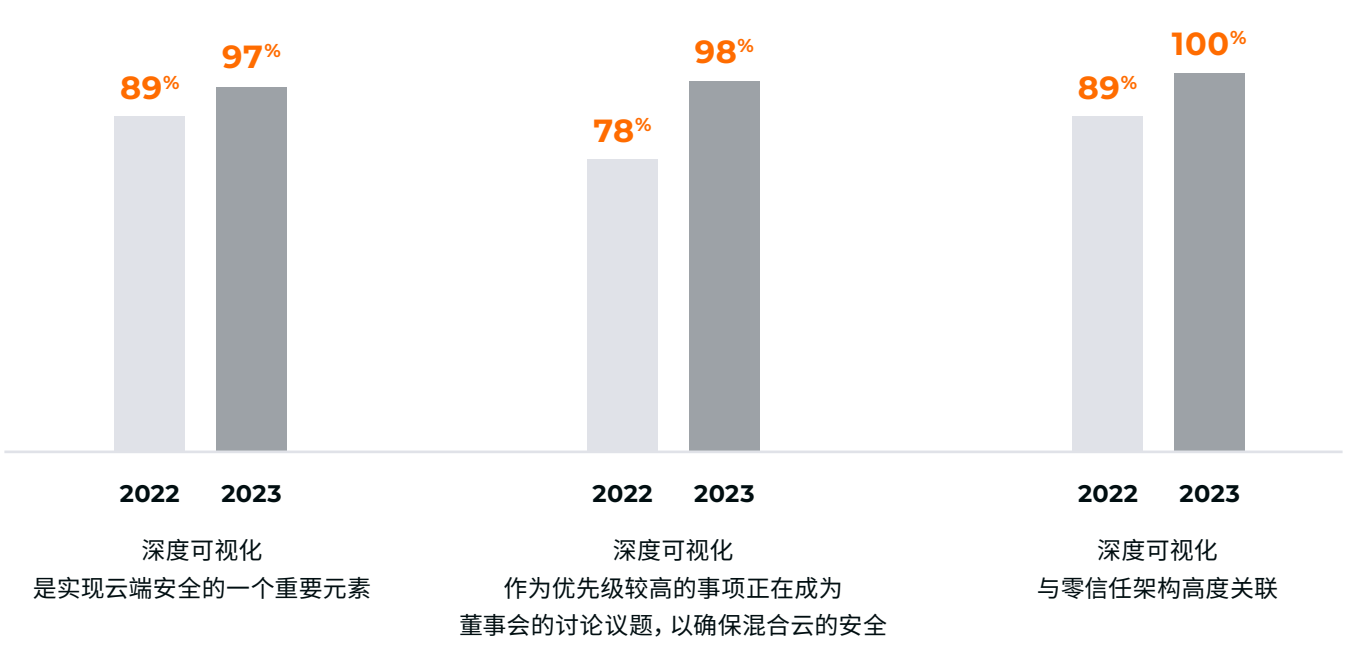
攻击复杂性
攻击复杂性成为CISO们更为害怕的因素 (32%)，高于缺少安全投资这一因素 (14%)。

盲点和立法让CISO们神经紧绷

2023年，IT和安全领导对于技能和投资方面的担心相对较低，只有19%的受访者认为，有效的员工安全教育是对IT基础设施安全抱有信心的关键因素。

深度可视化
日益成为云安全和零信任架构不可或缺的元素

深度可视化的重要性，将在2022至2023年间日益受到IT和安全领导的重视。



下载全文报告，查看报告中针对您所在地区的安全情况所形成的洞察
gigamon.com/cloud-security-survey

采集数据时间：2023年4月19日-5月2日
受访者：1020人，包括CIO/CISO/CTO以及其他网络和云相关负责人
地区：美国、英国、法国、德国、新加坡、澳大利亚

Gigamon®