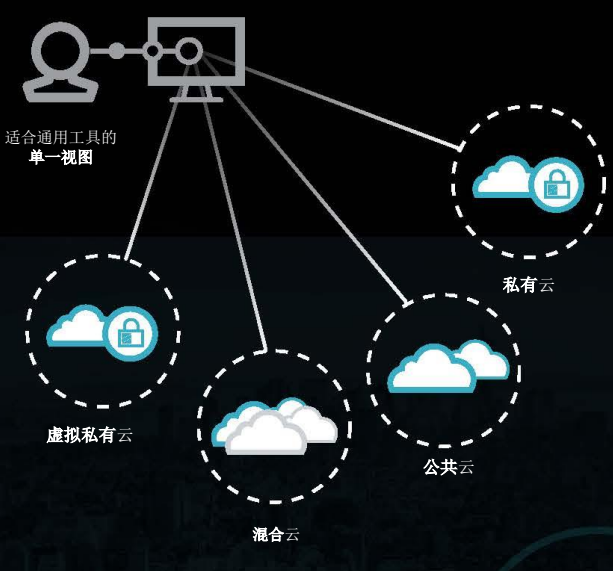
可视性架构
最佳实践

统一视图...

可视性架构充当各个网段的数据分发中心，接收传入的数据流并加以整合，再智能地将其分发到安全、分析和合规系统。

...支持所有环境



让您实时洞察自己的数据

Ixia 可视性架构实现可扩展的性能，以满足您应对数据量不断增长的需求。

部署最佳实践
安全行动

安全重在行动
请牢记，安全是一种持续的过程，绝不能松懈怠慢。企业生命周期安全管理包括观察、评估、缓解、审计和不断重复这些动作。

您的安全测试足够聪明吗？
您还可以依据微软首创的 STRIDE 模型评估测试效果，为威胁建模提供初步框架。STRIDE 代表欺骗、篡改、否认、信息泄露、拒绝服务和特权升级。测试系统的能力决定了您在实际情况下的安全准备度。

了解骗子的思维方式
实施新一代漏洞、合规、社交、行为分析、用户训练、云应用使用方式、移动安全和 IP 工具。跨越各种设备、用户、应用和数据的可视性正变得至关重要，而口号也从“通过隐匿性实现安全”变为“通过可视性实现安全”。例如，禁止使用未经 IT 部门认可的云应用程序、强制使用强密码并采用多因素身份验证。

成为教官
通过重新分配任务和强调训练来消除例行程序，避免安全警报疲劳。这也是军队坚持进行演练的原因之一。《安全故障是件好事吗？》一文对此进行了充分说明。

监控您的弱点
针对最终用户的要求和培训学习至关重要。您以为人人都知道该如何处理？但事实可能让您大跌眼镜。请务必认真考虑如何优化产品、人员和流程三大要素。

了解您的供应商
确保所有供应链合作伙伴和厂商都实施了恰当的安全措施——尤其是提供重要软件或需要访问您内部系统的合作伙伴和厂商。

修补漏洞
最后，您应及时处理已知的漏洞。它们可能不在您的优先事项中，但事先修补总比事后更加容易和廉价。Gartner 指出：“到 2020 年，仍有 99%被黑客利用的漏洞是安全和 IT 专家在一年前就已发现的。”[1]

欲了解可视性架构如何助您一臂之力，敬请访问：
www.ixiacom.com/solutions/network-visibility

[1] 《Gartner，如何应对 2017 年威胁形势》（Gartner, How to Respond to the 2017 Threat Landscape”，2016 年 12 月 8 日）