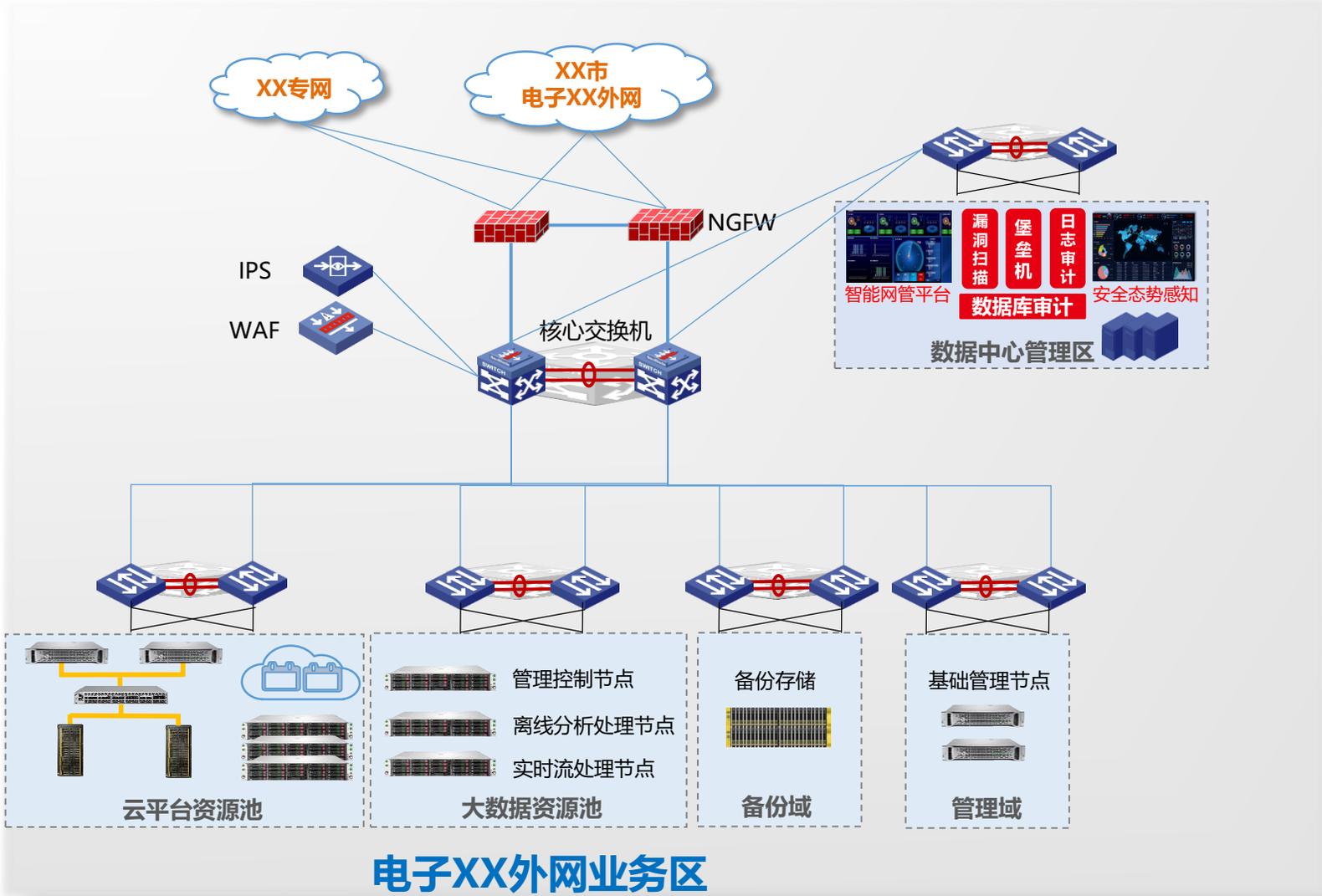


方案名称：**云计算安全解决方案**

个人信息：张元-伟仕佳杰

云计算安全建设现状



无虚拟机级别的东西、南北向网络安全监控

无租户级、业务系统间的隔离与南北向网络安全防控



导致云计算内部网络安全事件频发

业务上云后带来的安全挑战



提升安全使用体验

系统上云时，安全仍采用传统人工交付方式，存在手工配置易出错、交付时间长等问题，已经无法跟上云计算的节奏。软件定义安全将会成为未来安全体系应具备的一项能力。



新增安全运营需求

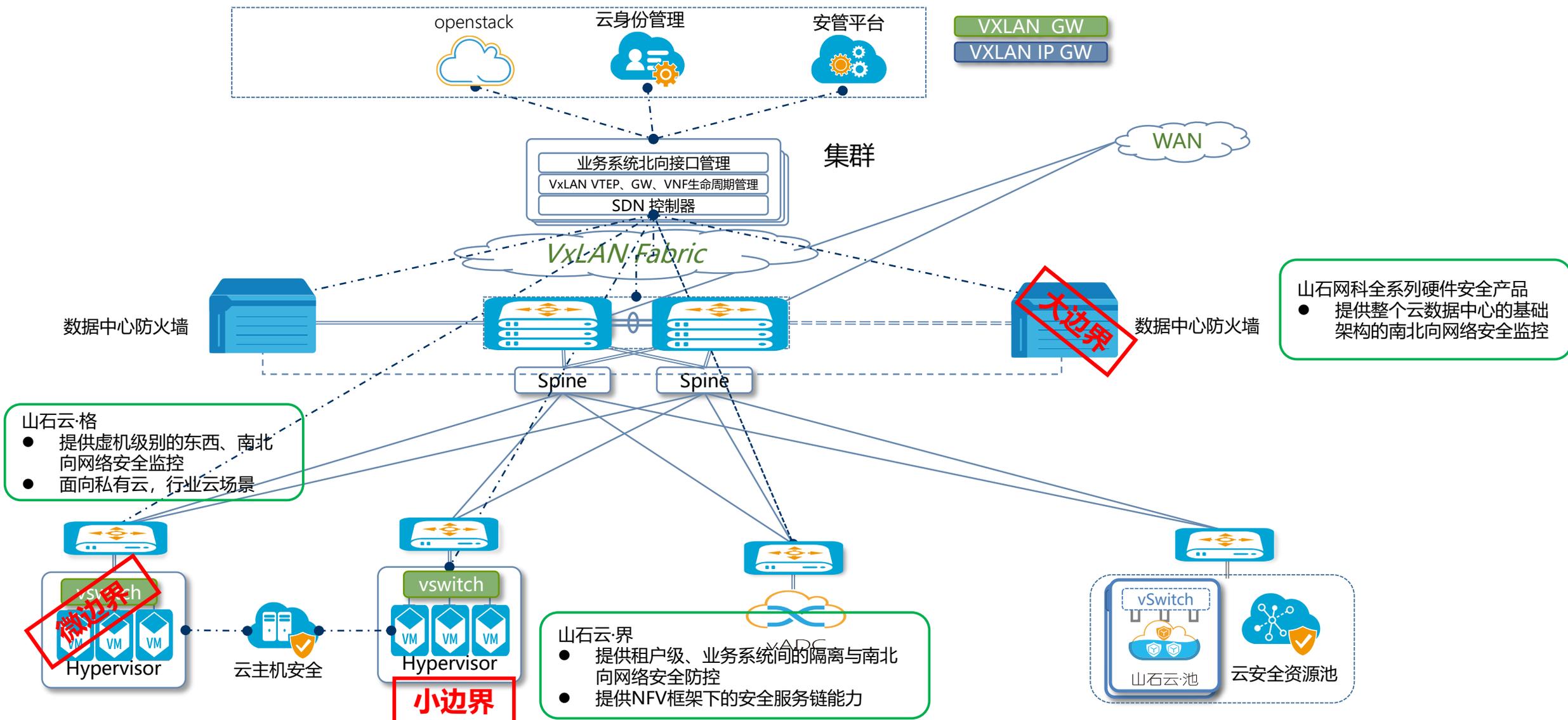
调查显示，尽管客户已经进行一定的安全建设和投入，但大部分用户的安全威胁监控与管理现状并不乐观，有效阻断扫描和探测行为的客户占比仅约4.3%，安全管理流程和机制不完善、安全人员缺少是主要原因。



合规性要求增强

《网络安全法》、网络安全等级保护系列标准和网络安全审查等，提出包括三同步原则、云服务使用不改变安全职责、新增安全工作等新安全要求，合规性要求越来越严格。

山石网科云安全解决方案



优势价值—山石网科助力云计算安全

协同事件处置，提高响应速度 基于安全管理平台，降低安全告警数量，降低安全运维工作量；

端到端安全防护，保护私有云平台

安全资源能力涵盖网络、主机、应用和数据等多个层面，流量防护覆盖南北向流量和东西向流量，帮助私有云建立纵深安全防护，确保云平台安全。



覆盖多项工作，助力安全合规

整体方案包括安全防护和安全运营，并提供了相应安全能力和服务，帮助各方建立安全防护体系，履行各自安全职责，改变原来安全职责不清的局面，减少安全风险，帮助履行安全职责，助力安全合规。

统一安全平台，全局安全可视

基于统一安全管理平台，实现全局安全可视化，一方面帮助安全运维人员了解各安全资源的运行状态和利用率，方便其及时做防护能力规划和调整；另一方面帮助安全运维人员掌握私有云的安全状态和安全态势，方便对安全事件和威胁做分析、处置和防护体系优化。