等保 2.0 的概念

以《中华人民共和国网络安全法》为法律依据，以 2019 年 5 月发布的《GB/T22239-2019 信息安全技术 信息系统安全等级保护基本要求》为指导标准的网络安全等级保护办法，业内简称等保 2.0。等保 2.0 依旧采用“一个中心，三重防护”的技术理念，并在原标准基础上提出新的技术要求和管理要求，如可信技术、云计算、物联网等新兴领域的安全扩展要求等。因此，用户在安全防护体系建设、风险评估和安全管理上需要更加全面，并关注所在行业的安全要求和定级标准，满足等保二级、等保三级认证要求。

为什么要做等保

满足法律法规的要求

《网络安全法》第 21 条明确要求，网络运营者要履行的等级保护制度义务

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

满足行业准入门槛或甲方要求的行业

大部分行业如医疗、教育、交通、能源、电信等等关键信息基础设施行业都要满足等保要求

企业提升自身安全要求

我国等级保护拥有完整的安全标准体系。是目前最佳时间也是企业最佳可参考选择，保障企业信息安全。

服务优势

覆盖全国的服务能力

青莲网络在全国多地拥有分部和资深等保服务经验的技术团队，能够帮助客户解决全国不同地区的等保需求。

高效快速

提供安全、可靠、专业的安全合规产品和服务，为您降低等保合规风险，快速、高效提升您的合规能力，可节省 60%的时间。

防护架构严固

青莲网络帮助您减少基础环境和安全产品投入，建立完整的安全技术架构，形成安全纵深防御，从而帮助您完成安全整改，以满足等保的基础合规技术要求。

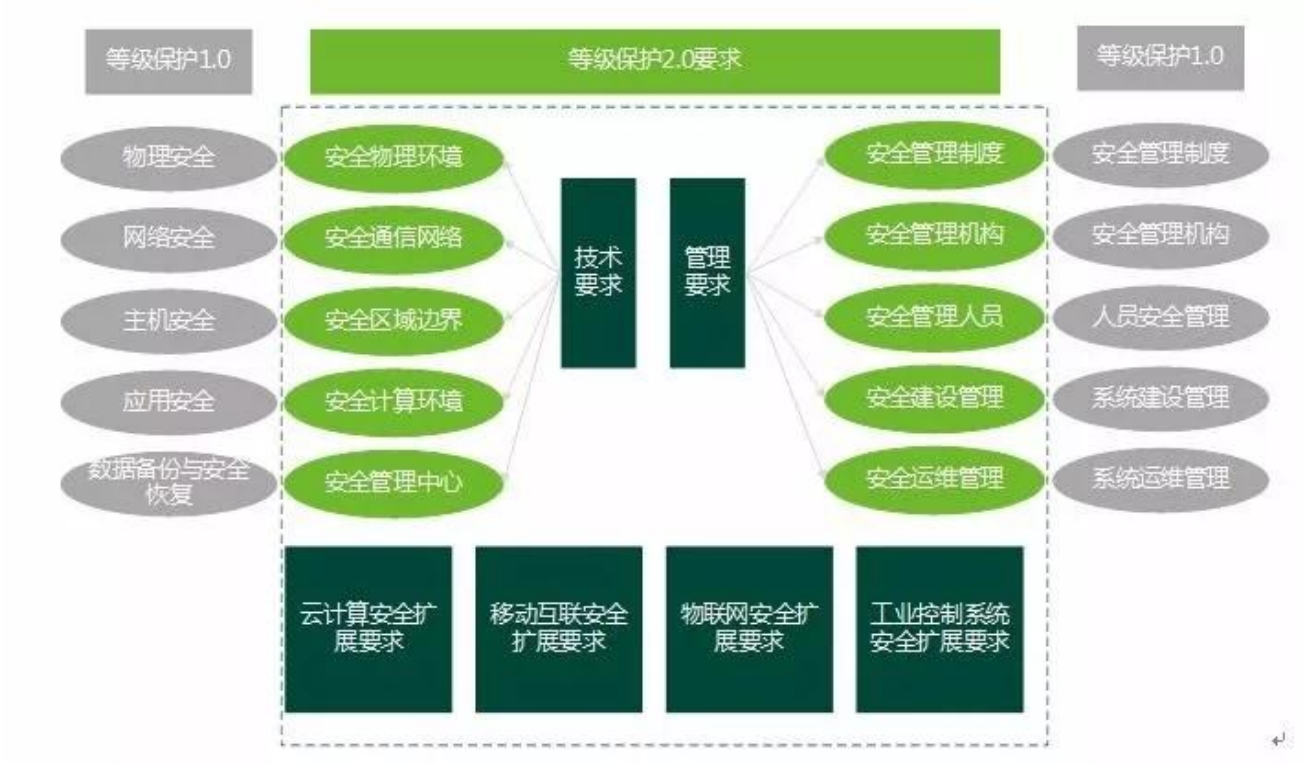
有效降低成本

根据测评过程中发现的安全问题，青莲网络为您提供全周期的安全解决方案。结合灵活便捷、按需的选用青莲网络合规产品和服务，极大节省您的合规成本。

等保流程的五个阶段

流程	运营、使用单位	公安机关	科泰博	测评机构
定级	确定安全保护等级，填写定级备案表、编写定级报告		协助运营、使用单位确认定级对象，为其提供咨询服务，辅导运营、使用单位准备定级报告，并组织专家评审（二级以上）	可承接运营、使用单位的定级咨询服务
备案	准备备案材料，到当地公安机关备案	当地公安机关审核受理备案材料	辅导运营、使用单位准备备案材料和提交备案申请	可承接运营，使用单位的备案服务
建设整改	建设符合等级要求的安全技术和管理体系		依据相应等级要求对当前实际情况进行差距分析，针对不符合项以及行业特性要求进行个性化的整改方案设计，协助运营、使用单位完成建设整改工作	对等级保护对象符合性状况进行测评
等级测评	准备和接受测评机构测评	公安机关监督检查运营、使用单位是否按要求开展等级保护工作	在测评阶段会指导运营、使用单位配合测评中心开展等级测评工作，并保障顺利通过等保测评获得测评报告	
监督检查	接受公安机关的定期检查		根据运营、使用单位需要配合完成自查工作，协助运营、使用单位接受检查和进行整改	

等保 2.0 的基本要求



等保 2.0 政策将等保 1.0 基本要求中各级技术要求的“物理安全”、“网络安全”、“主机安全”、“应用安全”和“数据安全和备份与恢复”修订为“安全物理环境”、“安全通信网络”、“安全区域边界”、“安全计算环境”和“安全管理中心”；各级管理要求的“安全管理制度”、“安全管理机构”、“人员安全管理”、“系统建设管理”和“系统运维管理”修订为“安全管理制度”、“安全管理机构”、“安全管理人员”、“安全建设管理”和“安全运维管理”。

方案设计参考模板

“一个中心三重防御“，针对安全管理中心和计算环境安全、区域边界安全、通信网络安全的安全合规进行方案的定制化设计,建立以计算环境安全为基础,以区域边界安全、通信网络安全为保障,以安全管理中心为核心的信息安全整体保障体系。