等保2.0下的云等保创新解决方案

青藤云安全

QINGTENG

2018年12月

CONTENTS

1 等保2.0变化

2 安全计算环境解决方案

3 云等保创新解决方案

4 青藤等保产品与服务

等保2.0 1+N标准体系

为了适应移动互联、云计算、物联网和工业控制等新技术、新应用情况下信息安全等级保护工作的开展，需对GB/T 22239—2008进行修订，修订的思路和方法是针对移动互联、云计算、物联网和工业控制等新技术、新应用领域提出扩展的安全要求。


GB

中华人民共和国国家标准

信息安全技术
信息系统安全等级保护基本要求

GB/T 22239—2019

GB/T22239-XXXX《信息安全技术 网络安全等级保护基本要求》

信息安全技术 网络安全等级保护基本要求 第 1 部分 安全通用要求；
信息安全技术 网络安全等级保护基本要求 第 2 部分 云计算安全扩展要求；
信息安全技术 网络安全等级保护基本要求 第 3 部分 移动互联安全扩展要求；
信息安全技术 网络安全等级保护基本要求 第 4 部分 物联网安全扩展要求；
信息安全技术 网络安全等级保护基本要求 第 5 部分 工业控制系统安全扩展要求；

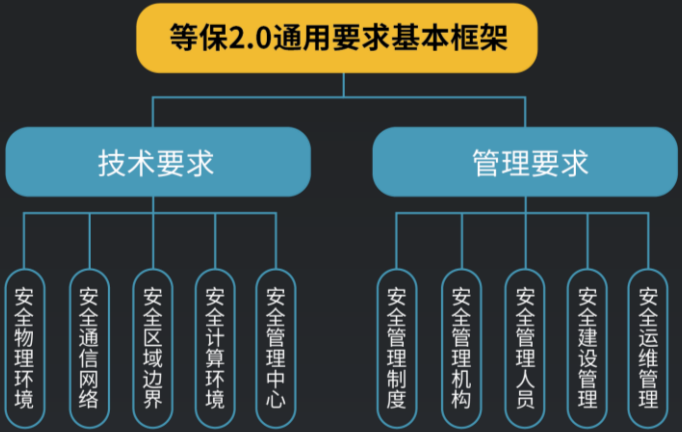
等保2.0核心：

全方位安全措施：将风险评估、安全监测、通报预警、案件调查、数据防护、灾难备份、应急处置、自主可控、供应链安全、效果评估等重点措施全部纳入等级保护制度并实施。

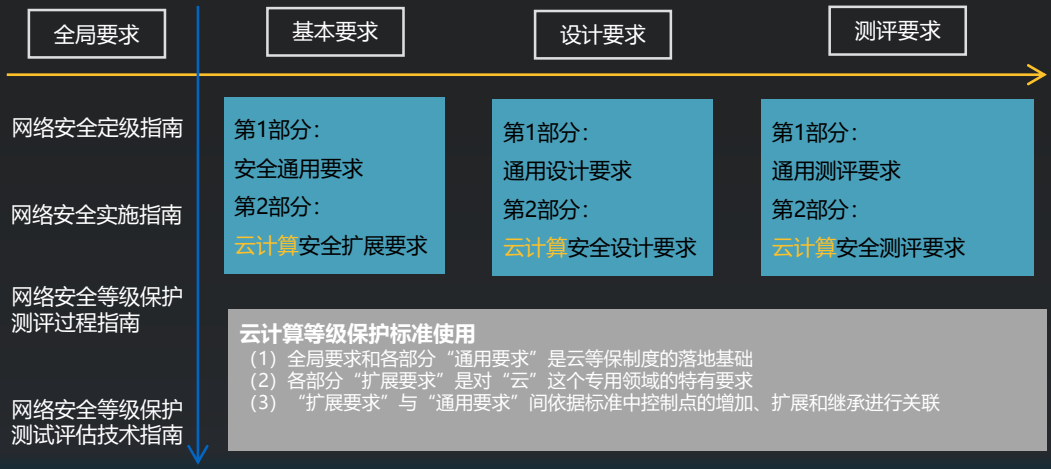
更广泛监管对象：将网络基础设施、重要信息系统、网站、大数据中心、云计算平台、物联网系统、工业控制系统、公众服务平台等全部纳入等级保护监管对象。

新增互联网企业：将互联网企业的网络、系统、大数据等纳入等级保护管理，保护互联网企业健康发展。

等保2.0通用要求基本框架



云等保的标准体系

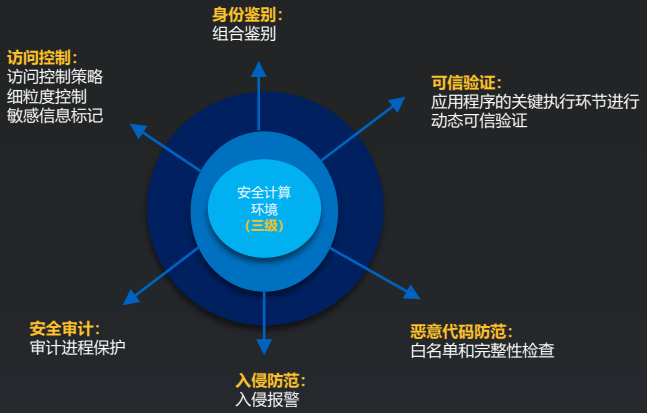

全局要求
基本要求
设计要求
测评要求
网络安全定级指南
网络安全实施指南
网络安全等级保护测评过程指南
网络安全等级保护测试评估技术指南
第1部分：
安全通用要求
第2部分：
云计算安全扩展要求
第1部分：
通用设计要求
第2部分：
云计算安全设计要求
第1部分：
通用测评要求
第2部分：
云计算安全测评要求
云计算等级保护标准使用
（1）全局要求和各部分“通用要求”是云等保制度的落地基础
（2）各部分“扩展要求”是对“云”这个专用领域的特有要求
（3）“扩展要求”与“通用要求”间依据标准中控制点的增加、扩展和继承进行关联

CONTENTS

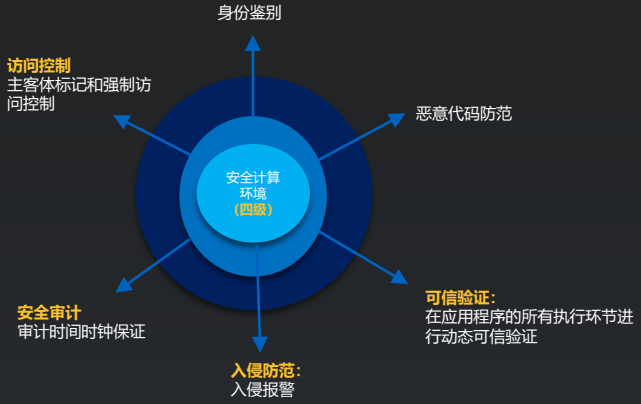
“安全计算环境”相关解读


身份鉴别：
防窃听
访问控制：
管理用户权限分离
最小权限
可信验证：
进行可信验证
安全计算
环境
（二级）
安全审计：
审计记录
审计报表
审计记录的保护
恶意代码防范：
记录、报警、阻断
与网络恶意代码库分离
入侵防范：
终端访问控制
发现漏洞修复漏洞

“安全计算环境”相关解读


身份鉴别：
组合鉴别
访问控制：
访问控制策略
细粒度控制
敏感信息标记
可信验证：
应用程序的关键执行环节进行
动态可信验证
安全计算
环境
（三级）
安全审计：
审计进程保护
恶意代码防范：
白名单和完整性检查
入侵防范：
入侵报警

安全计算环境相关解读


身份鉴别
访问控制
主客体标记和强制访问控制
恶意代码防范
安全计算环境
(四级)
可信验证:
在应用程序的所有执行环节进行动态可信验证
安全审计
审计时间时钟保证
入侵防范:
入侵报警

安全计算环境解决方案

技术要求	二级解决方案	三级解决方案	四级解决方案
身份鉴别	弱密码、防暴力破解及异常登陆。	弱密码、防暴力破解及异常登陆+OTP	弱密码、防暴力破解及异常登陆+OTP
访问控制	账户管理、权限管理	账户管理、权限管理、强制访问、策略管理、敏感信息标记	账户管理、权限管理、强制访问、策略管理、敏感信息标记
安全审计	主机审计	主机审计、审计进程保护	主机审计、审计进程保护、时钟保证
入侵防范	补丁管理、基线核查、访问控制	补丁管理、基线核查、访问控制、报警	补丁管理、基线核查、访问控制、报警
恶意代码防范	恶意文件防护（包括病毒、木马）	恶意文件防护、文件完整性	恶意文件防护、文件完整性和进程白名单
可信验证	文件完整性	文件完整性+实时监控	文件完整性+实时监控
青藤提供产品	青藤等保合规基础版本	青藤等保合规标准版本	青藤等保合规高级版本

CONTENTS

等保2.0变化

安全计算环境解决方案

云等保创新解决方案

青藤等保产品与服务

云等保责任共担模型


安全责任
本地
IaaS
PaaS
SaaS
审计和监控
认证安全
数据安全
工作负载安全
虚拟层安全
网络安全
物理安全
客户责任
云服务商责任

云等保的保护对象及备案

层面	云计算系统保护对象	传统信息系统保护对象
安全物理环境	机房及基础设施	机房及基础设施
安全通信网络 安全区域边界	网络结构、网络设备、安全设备、综合网管系统、**虚拟化网络结构、虚拟网络设备、虚拟安全设备、虚拟机监视器、云管理平台**	网络设备、安全设备、网络结构、综合网管系统
安全计算环境 （设备和计算节点）	主机、数据库管理系统、终端、网络设备、安全设备、**虚拟网络设备、虚拟安全设备、物理机、宿主机、虚拟机、虚拟机监视器、云管理平台、网络策略控制器**	主机、数据库管理系统、终端、中间件、网络设备、安全设备
安全计算环境 （应用和数据）	应用系统、中间件、配置文件、业务数据、用户隐私、鉴别信息、**云应用开发平台、云计算服务对外接口、云管理平台、镜像文件、快照、数据存储设备、数据库服务器**	应用系统、中间件、配置文件、业务数据、用户隐私、鉴别信息等

云服务提供商：负责将云计算平台的定级结果向所辖公安机关进行备案， 备案地应为运维管理端所在地。

云租户：负责对云平台上承载的租户信息系统进行定级备案，备案地为 工商注册或实际经营所在地。

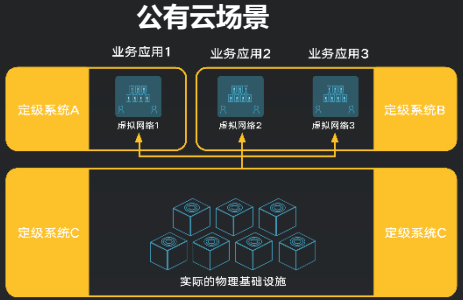
信息系统：信息系统设备设施所在地公安机关。

云等保保护要求项及责任划分

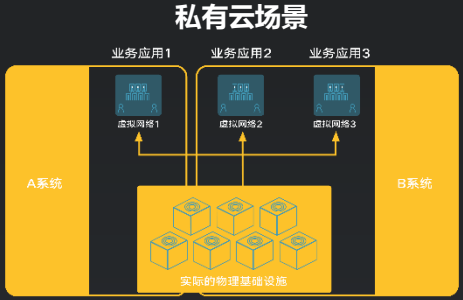
层面	云计算系统测评单元	传统信息系统测评单元	IaaS模式下云服务方与云租户的责任划分	
			安全组件	**责任主体**
安全物理环境	基础设施的位置	物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护	物理中心及物理设备	云服务方
安全通信网络 安全区域边界	网络架构、访问控制、入侵防范、安全审计、集中管控	网络架构、通信传输、可信验证、边界防护、访问控制、入侵防范、恶意代码防范、安全审计、可信验证	物理网络及附属设备、虚拟网络管理平台	云服务方
			云租户虚拟网络安全域	云租户
安全计算环境 （设备和计算节点）	身份鉴别、访问控制、入侵防范、镜像和快照保护	身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、	物理网络及附属设备、虚拟网络管理平台、物理宿主机及附属设备、虚拟机管理平台、镜像等	云服务方
			云租户虚拟网络设备、虚拟安全设备、虚拟机等	云租户
安全计算环境 （应用和数据）	数据安全性、数据备份恢复、剩余信息保护、云服务商选择、供应链管理、云计算环境管理	数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护	云管理平台（含运维和运营）、镜像、快照等	云服务方
			云租户应用系统及相关软件组件、云租户应用系统配置、云租户业务相关数据等	云租户

云等保场景

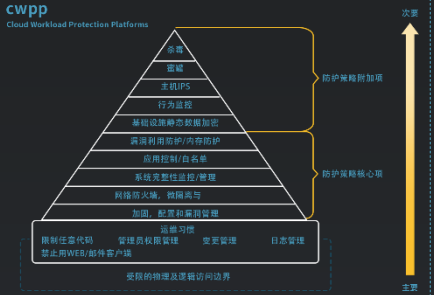
场景1

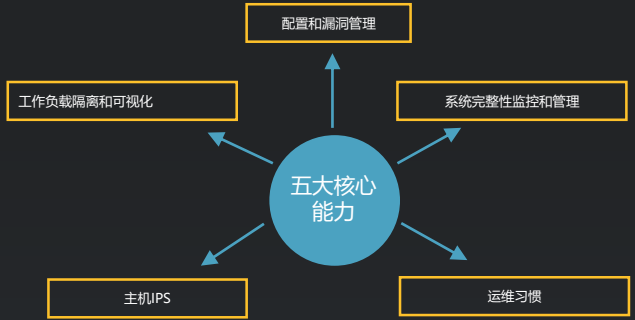


场景2



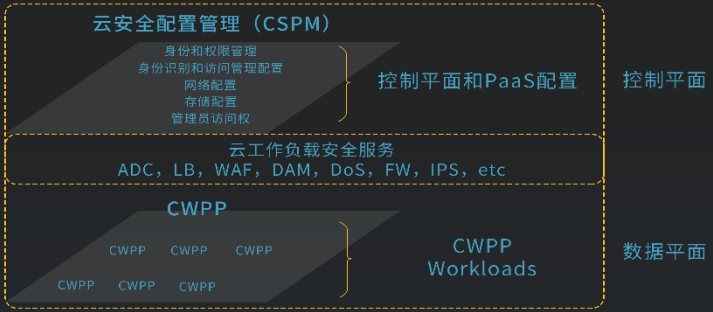
云等保解决方案-云工作负载保护平台





云工作负载保护平台（CWPP）是基于Agent底层技术的主机解决方案，主要满足现代混合数据中心架构中，服务器工作负载的保护要求

云等保解决方案-云工作负载保护平台



工作负载的安全防护：三个部分，两个平面

1.数据平面，主要包括针对云工作负载本身进行防护的CWPP，以及云工作负载之上的CWSS（云工作负载安全服务）。

2.控制平面，则都是在负载之上对负载进行防护的措施，就包括了CSPM，以及前面的CWSS（此处有重叠）。

云工作负载保护平台-测评机构

测评机构或应用安全评估单位，需要对大量等保系统进行测评。在云时代，在等级测评过程中也面临前所未有挑战。

云主机的数量巨大

虚拟机、容器不可见，造成无法评测

同平台的云租户，造成测评资源重复浪费

青藤的云工作负载保护平台，帮助测评机构全面了解云上资产，协助核查配置、漏洞管理，同时让流量清晰可见。

资产可见：通过对接云端系统，自动对租户和应用所涉及的主机资产可见。

配置检查：通过对海量云主机操作系统进行自动核查，加快速度节约成本。

漏洞管理：对主机上部署的系统和应用进行自动漏洞升级和打补丁，提高通过率。

流量可视化：将该主机的流量显示出来，提高可见性。

云工作负载保护平台-监管机构

云计算的快速发展给信息安全监管机构带来了巨大监管压力，要了解云租户整体情况，以及云等保测试过程，但目前无法主导持续监测和跟踪过程中，以及对于云端流量无法可视，成为了监管盲区

一次性检测
无法实时持续监控

流量不可见，成为监管盲区

海量云平台带来监管压力

青藤的云工作负载保护平台，让监管单位对云资产、测评过程、云运营商等清晰可见。

云租户资产可视：对于云租户以及拥有云资产可视。

云运营商可视：对云运营商运行情况整体可视，包括运行可靠性、稳定性、实时性等。

云等保检测过程可视：对于云等保项目、检测机构及人员、检测进度和出现问题可视。

云工作负载保护平台-云租户&云平台

云、虚拟机等技术给企业带来便利，与此同时也隐藏巨大风险。除此之外，如何应对来自监管单位合规要求成为了很多用户急需解决的问题。

无法实时了解合规状况

无法了解云平台流量

缺乏整改技术手段

青藤的云工作负载保护平台，让用户对所有云端资产、合规状况一目了然，同时可以协助用户对云主机进行实时监控，了解其安全状态。

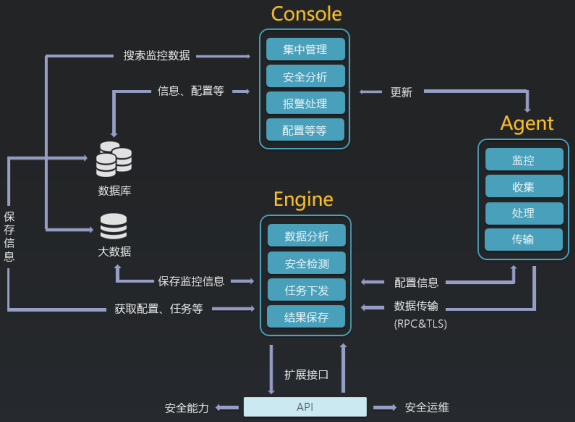
资产可见：通过对接云端系统，对所有主机资产及运行状况可视。

合规状态可视：对自身云主机的合规状态可视，对云主机上运行的应用程序可监控。

脆弱性管理：通过配置核查和漏洞管理来提升云主机安全。

可用性监测：实时检测云主机的心跳，获得云主机的可用性信息

集中管控解决方案



①如何对分散在网络各处服务器进行集中监测?

②如何应对安全策略、恶意代码、补丁升级?

……

Agent - 主机探针

Engine - 安全引擎

Console - 控制中心

CONTENTS

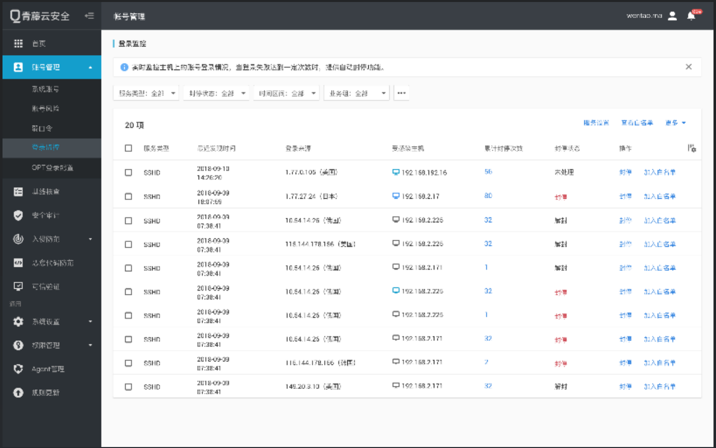
等保2.0变化

安全计算环境解决方案

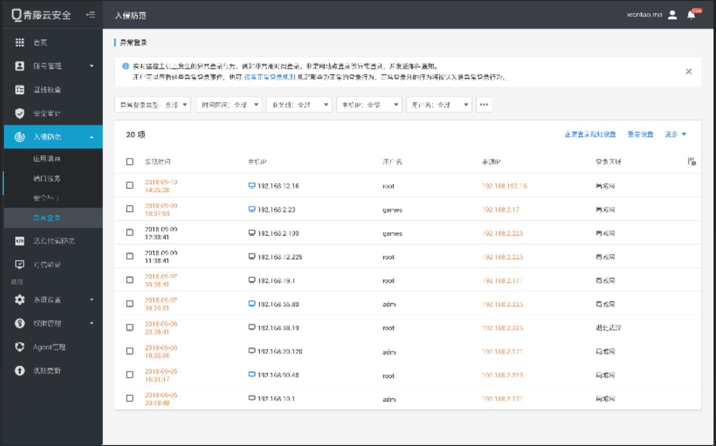
云等保创新解决方案

青藤等保产品与服务

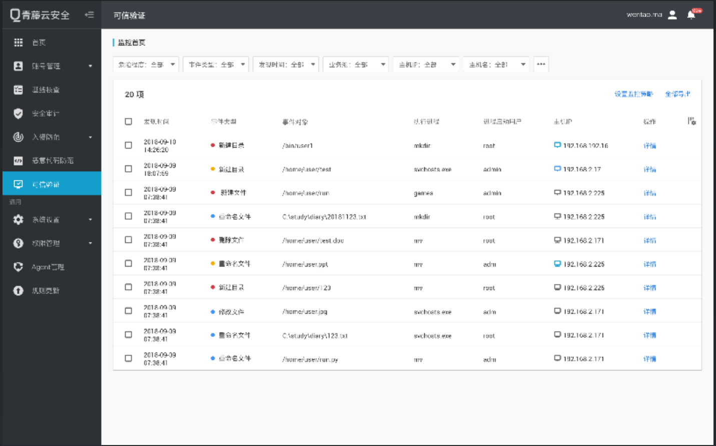
青藤等保安全产品



青藤等保安全产品



青藤等保安全产品


青藤云安全
可信验证
监控首页
20 项
2018-09-10 14:26:20
/bin/user1
mkdir
root
192.168.192.16
2018-09-09 18:07:59
/home/user/test
svchosts.exe
admin
192.168.2.17
2018-09-09 07:38:41
/home/user/run
games
admin
192.168.2.225
2018-09-09 07:38:41
C:\study\diary\20181123.txt
mkdir
root
192.168.2.225
2018-09-09 07:38:41
/home/user/test.doc
mv
root
192.168.2.171
/home/user.ppt
/home/user/123
/home/user.jpg
C:\study\diary\123.txt
/home/user/run.py
详情

青藤等保安全服务

服务类型	服务名称	服务内容
等级保护安全服务	定级咨询	根据等级保护定级国家标准和定级对象，给定级对象进行合理定级
	备案	协助到公安机关进行等级保护备案工作
	差距评估	使用相关产品自动化进行技术差距评估并生成报告
	技术整改方案	根据等级保护级别和现状，提出整体技术整改方案
	管理整改方案	根据等级保护相关级别的管理要求，协助完成管理体系
	安全复查	在测评机构测评过程中，配合进行复查
高级安全服务	应急演练	根据不同的安全事件，进行相关情况的应急演练
	应急响应	针对突发的安全事件，协助进行回溯、回复和取证相关工作
	安全意识培训	对人员进行安全意识教育，提高安全意识水平，并进行考试打分
	渗透测试	针对特定对象和采用特定方式，进行渗透式测试，并产出报告

服务价值

Thank you