ZStack

ZStack与等保2.0

大道至简 极速部署

可信赖的、产品化的云平台

目录

Content

01 等级保护的基本概念

概念：

对国家安全、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。

由来：

简单而言，就是将全国的信息系统（包括网络）按照重要性和受破坏后的危害性分成五个安全保护等级（从第一级到第五级逐级增高），定级后第二级以上信息系统到公安机关备案，公安机关对备案材料审核合格后颁发备案证明。各单位根据系统等级按照国家标准进行安全建设整改，备案单位聘请符合国家规定的等级测评机构进行等级测评（第二级系统备案前要进行一次测评、第三级系统每年要进行一次测评）；公安机关对第二级信息系统进行指导，对第三级、第四级信息系统定期开展监督、检查。


ICS 35.040
L 80

中华人民共和国国家标准

GB/T 22239—2019
代替 GB/T 22239—2008

信息安全技术
网络安全等级保护基本要求

Information security technology—
Baseline for classified protection of cybersecurity

2019-05-10 发布　　2019-12-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

01 等级保护的发展与演进

1994-2003年 政策环境营造

- **1994年-国务院147号令第一次提出计算机信息系统实行安全等级保护。**
- 2003年-《国家信息化领导小组关于加强信息安全保障工作的意见》明确指出“实行信息安全等级保护”

2004-2006年 工作开展准备

- 2004-2006年，公安部开展涉及65117家单位，共115319个信息系统的等级保护基础调查和等级保护试点工作，为全面开展等级保护工作奠定基础。

2007-2010年 工作正式启动

- 2007年，颁布《关于开展全国重要信息系统安全等级保护定级工作的通知》。
- 2007年，召开全国重要信息系统安全等级保护定级工作部署专题电视电话会议，标志着信息安全等级保护制度正式开始实施。
- **2008年：GB/T 22239-2008基本要求；**

2010-2016年 工作规模推进

- 2010年，公安部出台《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》，提出等级保护工作的的阶段性目标。
- 2010年，公安部和国务院国有资产监督管理委员会联合出台《关于进一步推进中央企业信息安全等级保护工作的通知》，要求中央企业贯彻执行等级保护工作。

2017-2019 等保2.0

- **2016年11月7日，《中华人民共和国网络安全法》正式颁布，第二十一条明确“国家实行网络安全等级保护制”。**
- **2019年5月13日，，正式发布网络安全等级保护制度2.0版本GB/T 22239-2019 。**

01 安全保护等级划分

	一般程度的损害	严重程度的损害	特别严重的损害
公民、法人和其他组织的合法利益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家利益	第三级	第四级	第五级

第一级，等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，等级保护对象受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，等级保护对象受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，等级保护对象受到破坏后，会对国家安全造成特别严重损害。

01 等级保护定级工作流程

定级 1. 确定定级对象，以及相应安全防护等级，形成定级报告。

备案 2. 持定级报告和备案表到当地公安机关网监部门进行备案。

整改 3. 参照信息系统当前等级要求和标准，对信息系统进行整改加固。

测评 4. 委托具备测评资质的测评机构对信息系统进行等级测评，形成正式的测评报告。

监督检查 5. 向当地公安机关网监部门提交测评报告，配合完成对信息安全等级保护实施情况的检查。

01

等保2.0的几个变化

1. 防护理念的变化

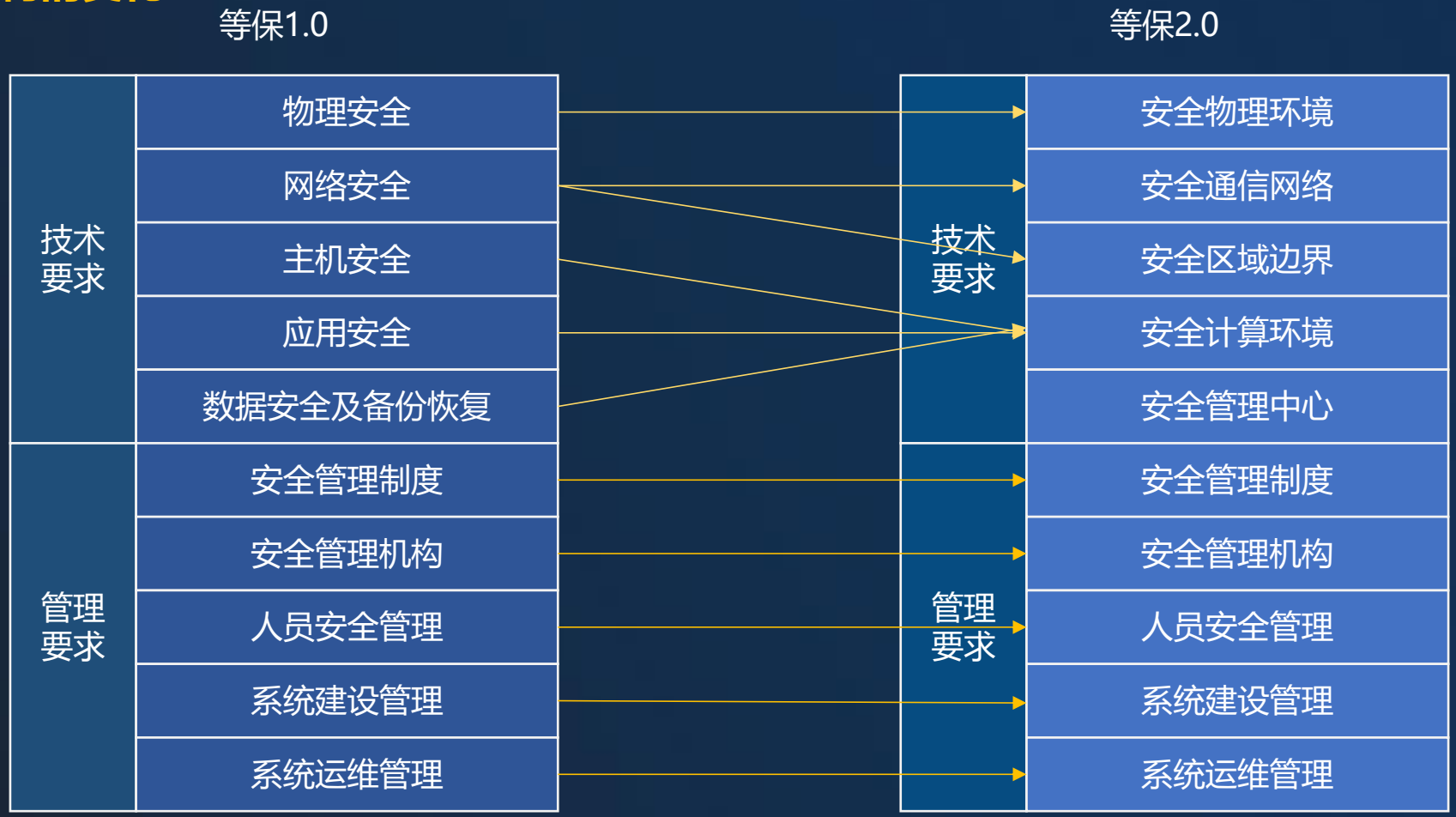
通用要求方面，等保2.0标准的核心是“优化”。删除了过时的测评项，新增对新型网络攻击行为防护和个人信息保护等新要求。等保2.0标准依然采用“一个中心、三重防护” 的理念，从等保1.0标准被动防御的安全体系向事前预防、事中响应、事后审计的动态保障体系转变，注重全方位主动防御、安全可信、动态感知和全面审计。

2. 保护对象的变化

01

等保2.0的几个变化

3. 控制结构的变化



等保2.0的几个变化

4. 控制项要求变化

安全通用要求针对共性化保护需求提出，等级保护对象无论以何种形式出现，必须根据安全保护等级实现相应级别的安全通用要求。安全扩展要求针对个性化保护需求提出，需要根据安全保护等级和使用的特定技术或特定的应用场景实现安全扩展要求。等级保护对象的保护需要同时满足安全通用要求和安全扩展要求。

层面	云计算平台测评对象	传统测评对象
物理和环境安全	机房及基础设施	机房及基础设施
网络和通信安全	网络结构、网络设备、安全设备、虚拟化网络结构、虚拟网络设备、虚拟安全设备	传统的网络设备、传统的安全设备、传统的网络结构
设备和计算安全	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、数据库管理系统、终端	传统主机、数据库管理系统、终端
应用和数据安全	应用系统、云应用开发平台、中间件、云业务管理系统、配置文件、镜像文件、快照、业务数据、用户隐私、鉴别信息等	应用系统、中间件、配置文件、业务数据、用户隐私、鉴别信息等

等级保护2.0定级的变化

5. 定级要求的变化

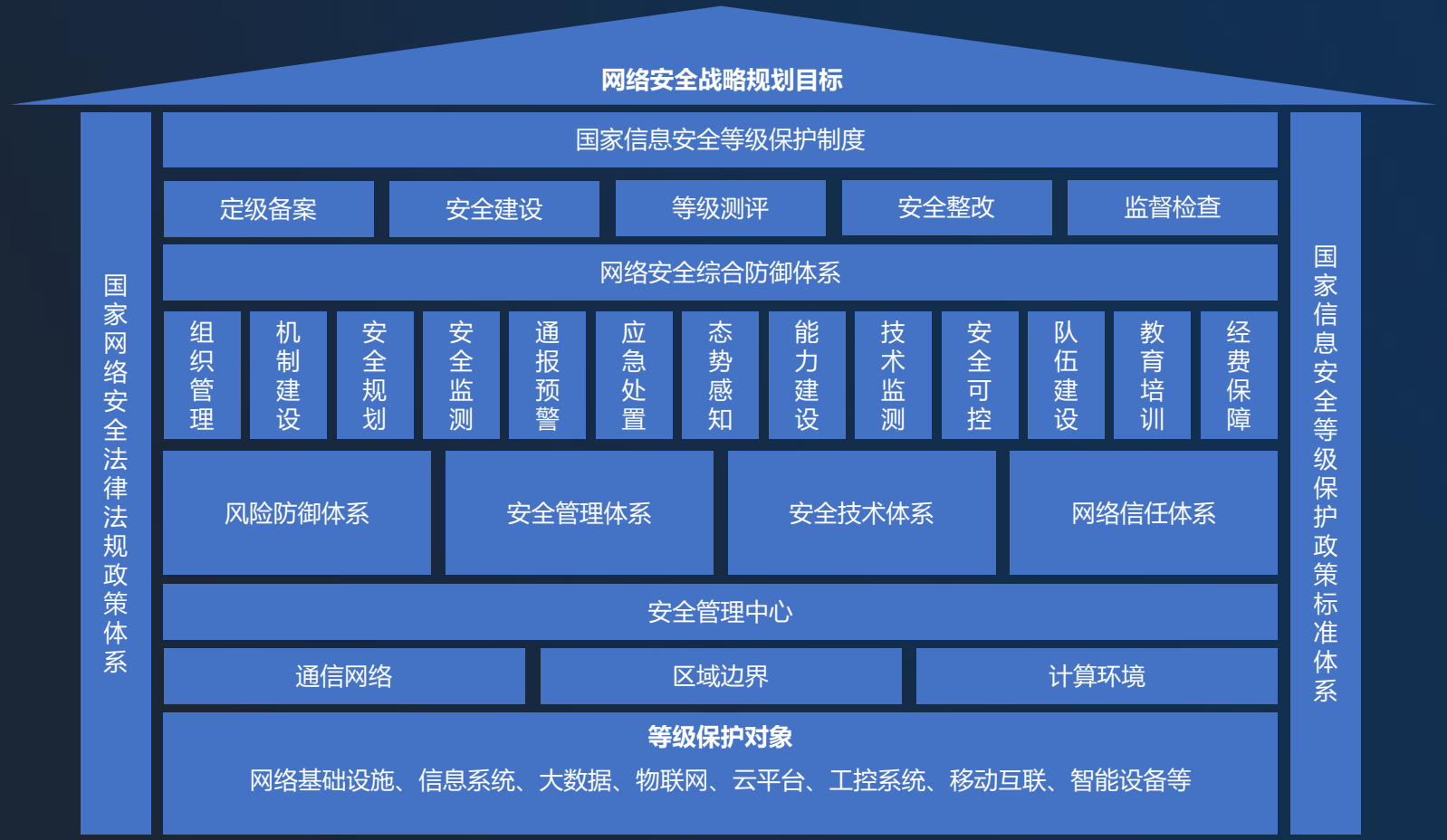
	受侵害的客体	对客体的侵害程度		
		一般程度的损害	严重程度的损害	特别严重的损害
等级的变化	公民、法人和其他组织的合法利益	第一级	第二级	第三级 -> 第三级
	社会秩序、公共利益	第二级	第三级	第四级
	国家利益	第三级	第四级	第五级

等保2.0标准不再自主定级，而是通过“确定定级对象—>初步确定等级—>专家评审—>主管部门审核—>公安机关备案审查—>最终确定等级”这种线性的定级流程，系统定级必须经过专家评审和主管部门审核，才能到公安机关备案，整体定级更加严格，将促进定级过程更加规范，系统定级更加合理。

6. 测评相关的变化

	等保1.0	等保2.0
测评周期	第三级系统每年一次，第四级系统每半年一次	第三级以上系统每年一次
测评结果	60分以上基本符合	75分以上基本符合

01 等保2.0安全防护框架



等保2.0安全框架核心内容

1. 依据国家网络安全法律法规和等级保护政策标准开展等级保护工作；
2. 确定等级保护对象；
3. 依然采用“一个中心、三重防护”的理念；
4. 建立安全技术体系和安全管理体系，构建具备相应等级安全保护能力的网络安全综合防御体系；
5. 开展组织管理、机制建设、安全规划、通报预警、应急处置、态势感知、能力建设、监督检查、技术监测、队伍建设、教育培训和经费保障等工作。

01 等保1.0 与 等保2.0 – 等保2.0的变化

从条例法规提升到法律层面

等保2.0标准要求的新增和优化

等级保护的实施环节有了优化改变

事前预防、事中响应、事后审计的动态保障体系转变

01 开展等级保护的必要性

国家要求

《中华人民共和国网络安全法》
《信息安全等级保护管理办法》

行业监管

《金融行业信息安全等级保护》
《电力行业信息安全等级保护》
《广电行业信息安全等级保护》
交通、教育、卫生 ... ...

安全能力提升

我国唯一体系化信息安全政策标准
提升信息安全保障能力
保障信息系统安全稳定运行

规避法律风险

等级保护工作上升到法律层面
不开展等级保护可能追究法律责任

目录

Content

02 云平台及云上业务的安全挑战

1. **云平台基础架构安全**
   云平台网络架构、访问控制、入侵防范、系统加固 ...
2. **云中网络安全**
   租户之间网络隔离、自主定义安全策略、入侵防范 ...
3. **云主机安全**
   恶意代码、访问控制、身份鉴别 ...
4. **云中数据安全**
   数据完整性、保密性、备份恢复、剩余信息保护
5. **云中安全管理**
   统一调度、集中审计、流量分离 ... ...
6. **安全责任划分**
   云服务商和云租户方责任边界定义

ZStack

02

等保2.0提出云计算安全建设要求

云计算平台系统等级保护建设，不仅要满足安全通用要求，同时要满足云计算安全扩展要求

02

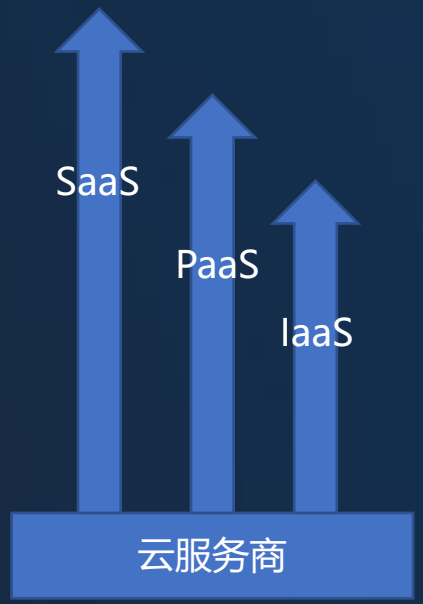
等保2.0明确云计算安全责任主体

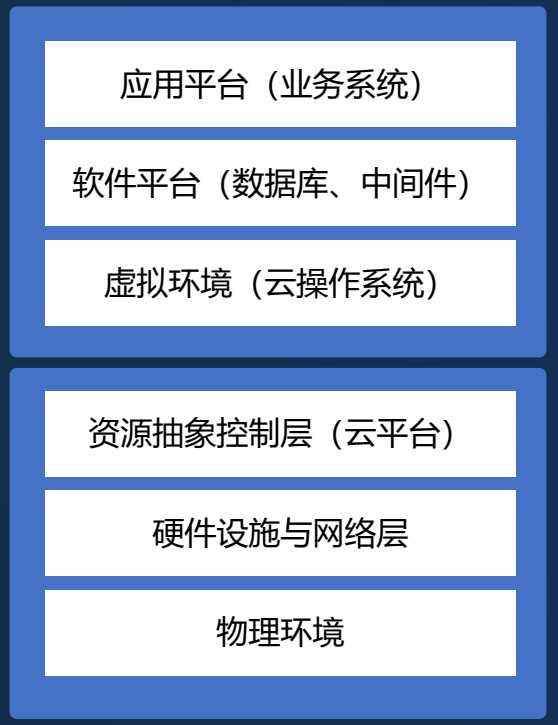
责任主体一分为二

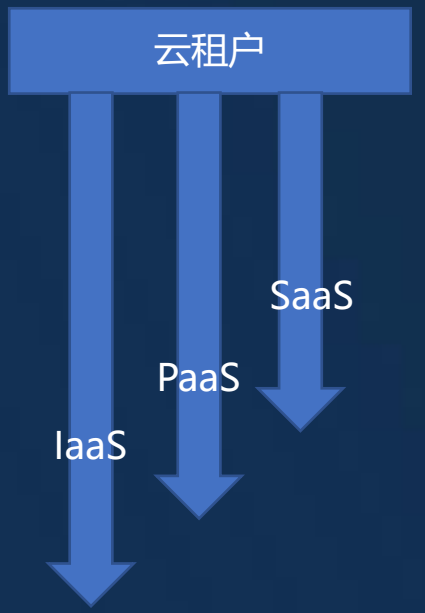
- **云服务商**
- **云租户**

共担安全责任

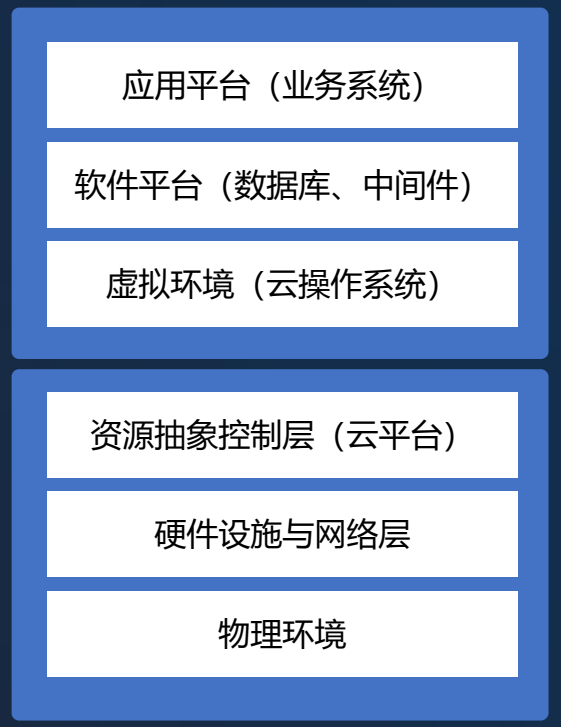
不同云服务模式，云服务商和云租户承担安全的责任边界也不同，如：IaaS服务中，云服务商与云租户的责任边界位于虚拟环境与资源抽象控制层之间，之下由云服务商建设并担责，之上有云租户建设并担责！







02 等保2.0明确云计算安全责任主体



定级系统对象：业务系统

担责方：云租户方

定级系统对象：云平台

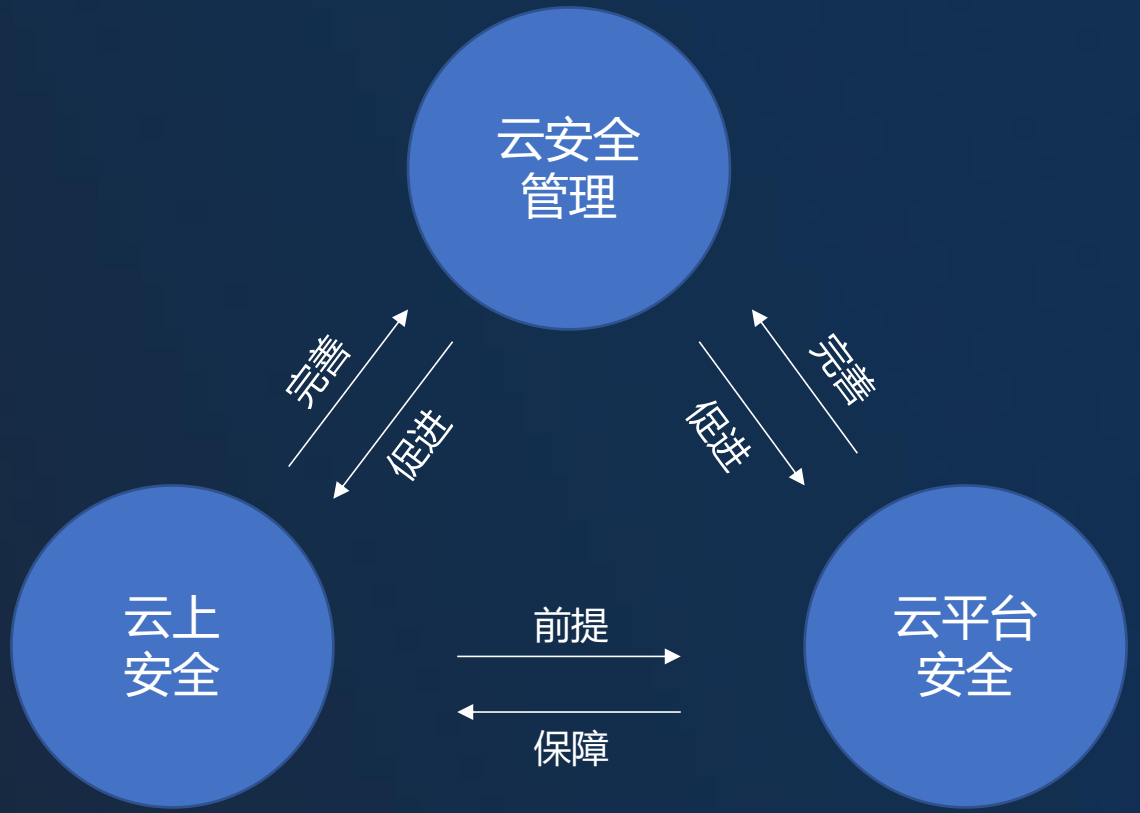
担责方：云服务商

云计算平台不得承载高于平台等级的信息系统；

如云平台系统定级三级，那么之上只能承载三级及三级以下的业务系统

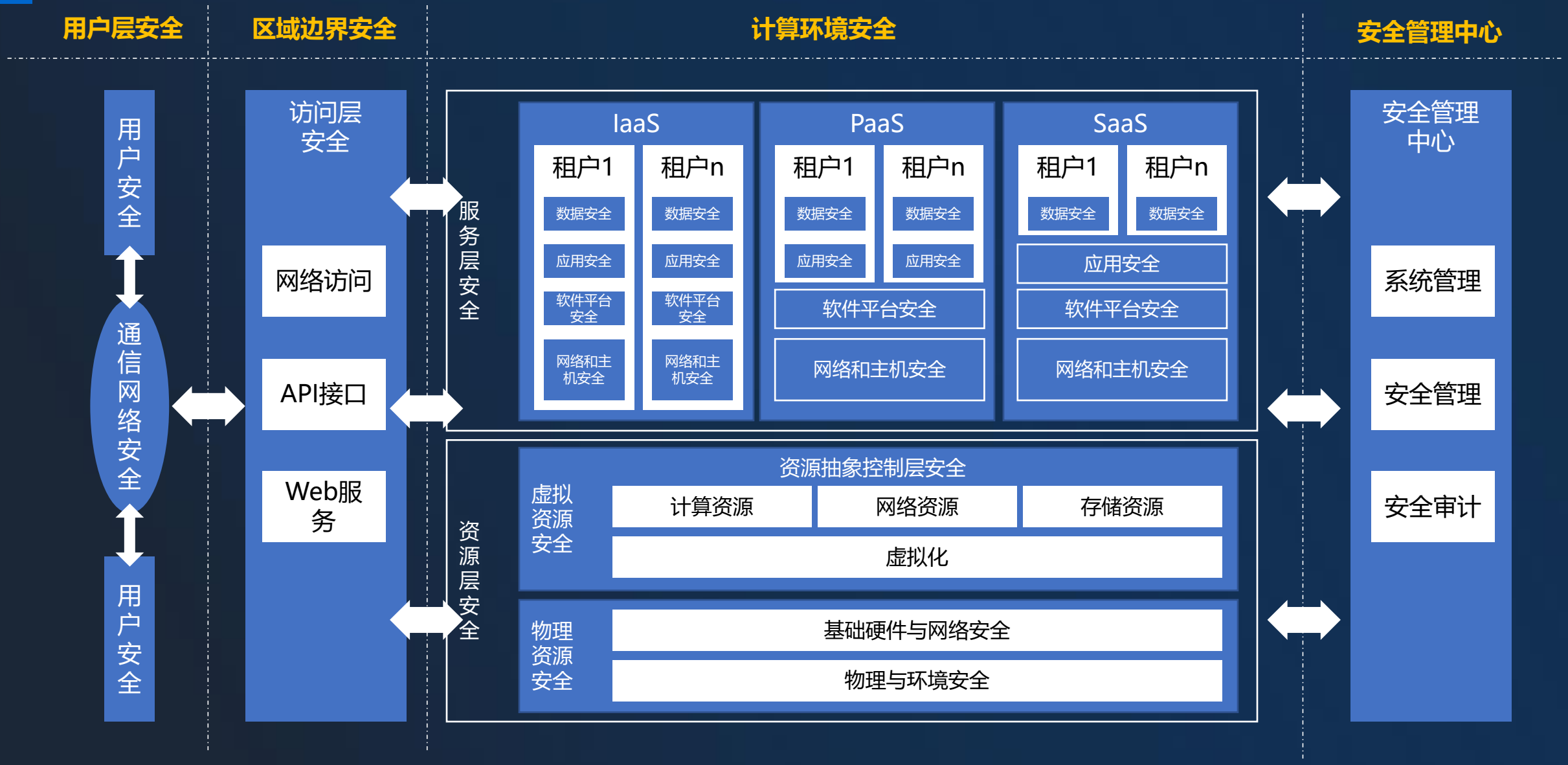
02

云计算安全整体建设思路



02

等保2.0云计算安全建设技术框架



目录

Content

03 云计算安全扩展要求

章节	项目	子章节	细则	具体要求	符合程度
8.2.1	**安全物理环境**	**8.2.1.1**	**基础设施位置**	应保证云计算基础设施位于中国境内。 测评对象：云计算平台和业务应用系统定级备案材料；	符合
8.2.2	**安全通信网络**	**8.2.2.1**	**网络架构**	a) 应保证云计算平台不承载高于其安全保护等级的业务应用系统； 测评对象：网络资源隔离措施、综合网管系统和云管理平台；	符合
				b) 应实现不同云服务客户虚拟网络之间的隔离； 测评对象：网络资源隔离措施、综合网管系统和云管理平台；	符合 VPC/VLAN
				c) 应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力； 测评对象：防火墙、入侵检测系统、入侵保护系统和抗APT系统等安全设备；	部分符合 无入侵检测系统、入侵保护系统和抗 APT 系统
				d) 应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略； 测评对象：云管理平台、网络管理平台、网络设备和安全访问路径；	部分符合 同上
				e) 应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。 测评对象：相关开放性接口和安全服务及相关文档；	符合

03 云计算安全扩展要求

章节	项目	子章节	细则	具体要求	符合程度
8.2.3	安全区域边界	8.2.3.1	访问控制	a) 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则； 测评对象：访问控制机制、网络边界设备和虚拟化网络边界设备；	符合 防火墙
				b) 应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；	符合 防火墙
		8.2.3.2	入侵防范	a) 应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； 测评对象：抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS 攻击系统和入侵保护系统或相关组件；	不符合 借助第三方安全服务
				b) 应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； 测评对象：抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS 攻击系统和入侵保护系统或相关组件；	不符合 借助第三方安全服务
				c) 应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量； 测评对象：虚拟机、宿主机、抗APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件；	不符合 借助第三方安全服务
				d) 应在检测到网络攻击行为、异常流量情况时进行告警。 测评对象：虚拟机、宿主机、抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件；	不符合 借助第三方安全服务
		8.2.3.3	安全审计	a) 应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启； 测评对象：堡垒机或相关组件；	不符合 借助第三方安全服务
				b) 应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。 测评对象：综合审计系统或相关组件；	部分符合 日志审计

03 云计算安全扩展要求

章节	项目	子章节	细则	具体要求	符合程度
8.2.4	安全计算环境	8.2.4.1	身份鉴别	当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。 测评对象：管理终端和云计算平台；	符合 证书+https
		8.2.4.2	访问控制	a） 应保证当虚拟机迁移时，访问控制策略随其迁移； 测评对象：虚拟机、虚拟机迁移记录和相关配置；	符合
				b) 应允许云服务客户设置不同虚拟机之间的访问控制策略。 测评对象：虚拟机和安全组或相关组件；	符合 安全组
		8.2.4.3	入侵防范	a） 应能检测虚拟机之间的资源隔离失效，并进行告警； 测评对象：云管理平台或相关组件；	符合
				b) 应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警； 测评对象：云管理平台或相关组件；	部分符合（无告警）
				c) 应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。 测评对象：云管理平台或相关组件；	不符合 安骑士、安恒EDR
		8.2.4.4	镜像和快照保护	a） 应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务； 测评对象：虚拟机镜像文件；	符合 系统镜像加固
				b) 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改； 测评对象：云管理平台和虚拟机镜像、快照或相关组件；	符合 镜像切片加密存储
				c) 应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 测评对象：云管理平台和虚拟机镜像、快照或相关组件；	符合 操作系统加密

03 云计算安全扩展要求

章节	项目	子章节	细则	具体要求	符合程度
8.2.4	安全计算环境	8.2.4.5	数据完整性和保密性	a) 应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定； 测评对象：数据库服务器、数据存储设备和管理文档记录；	符合
				b) 应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限； 测评对象：云管理平台、数据库、相关授权文档和管理文档；	符合 合同协议明确责任
				c) 应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施； 测评对象：虚拟机；	基本符合 使用MD5
				d) 应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。 测评对象：密钥管理解决方案；	符合 支持第三方安全服务
		8.2.4.6	数据备份恢复	a) 云服务客户应在本地保存其业务数据的备份； 测评对象：云管理平台或相关组件；	符合 灾备模块
				b) 应提供查询云服务客户数据及备份存储位置的能力； 测评对象：云管理平台或相关组件；	符合 灾备模块
				c) 云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致； 测评对象：云管理平台、云存储系统或相关组件；	符合 灾备模块或分布式存储
				d) 应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。 测评对象：相关技术措施和手段；	符合 v2v
		8.2.4.7	剩余信息保护	a) 应保证虚拟机所使用的内存和存储空间回收时得到完全清除； 测评对象：云计算平台；	符合
				b) 云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。 测评对象：云存储系统和云计算平台；	符合

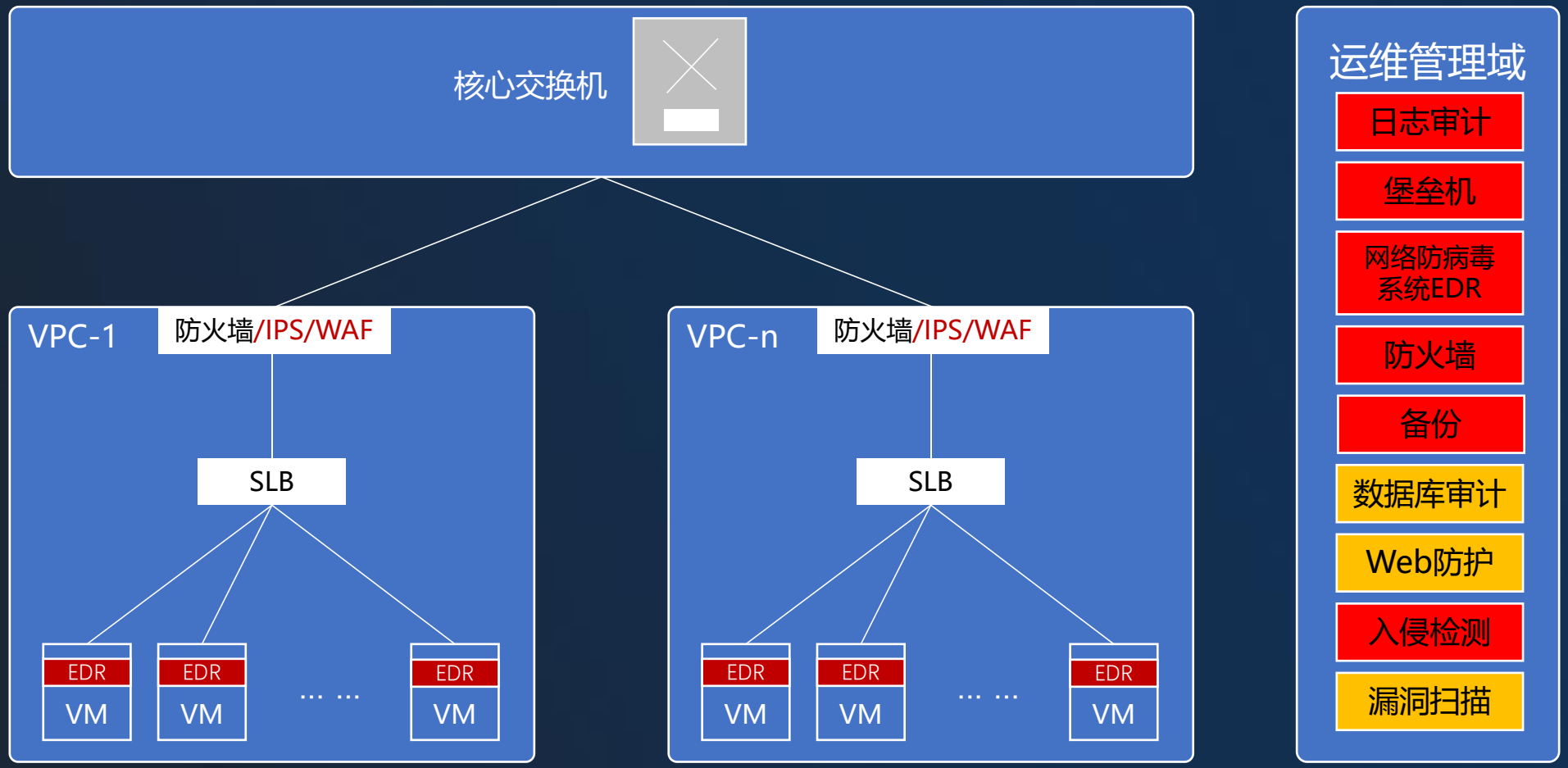
03 云计算安全扩展要求

章节	项目	子章节	细则	具体要求	符合程度
8.2.4	安全管理中心	8.2.5.1	集中管控	a) 应能对物理资源和虚拟资源按照策略做统 - 管理调度与分配； 测评对象：资源调度平台、云管理平台或相关组件；	符合
				b) 应保证云计算平台管理流量与云服务客户业务流量分离； 测评对象：网络架构和云管理平台；	符合
				c) 应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计； 测评对象：云管理平台、综合审计系统或相关组件；	基本符合 无集中审计
				d) 应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。 测评对象：云管理平台或相关组件；	符合

03 差距汇总（云计算安全扩展要求）

安全区域边界	入侵防范	a） 应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； 测评对象：抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS 攻击系统和入侵保护系统或相关组件；	不符合 借助第三方安全服务
		b) 应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； 测评对象：抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS 攻击系统和入侵保护系统或相关组件；	不符合 借助第三方安全服务
		c) 应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量； 测评对象：虚拟机、宿主机、抗APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件；	不符合 借助第三方安全服务
		d) 应在检测到网络攻击行为、异常流量情况时进行告警。 测评对象：虚拟机、宿主机、抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件；	不符合 借助第三方安全服务
	安全审计	a） 应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启； 测评对象：堡垒机或相关组件；	不符合 堡垒机
安全区域边界	入侵防范	b) 应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警； 测评对象：云管理平台或相关组件；	不符合 未知
		c) 应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。 测评对象：云管理平台或相关组件；	不符合 网络防病毒软件EDR

03 整体解决方案（云计算安全扩展要求）



感谢大家！
THANKS

ZStack 微信公众号
zstack_io

ZStack 中国社区QQ群
443027683

ZStack 官网
www.zstack.io

ZStack