C3安全峰会
CYBER | CLOUD | COMMUNICATION

CSA国际云安全标准暨云安全全球最佳实践集

叶思海
CSA大中华区研究院院长

C3

目录

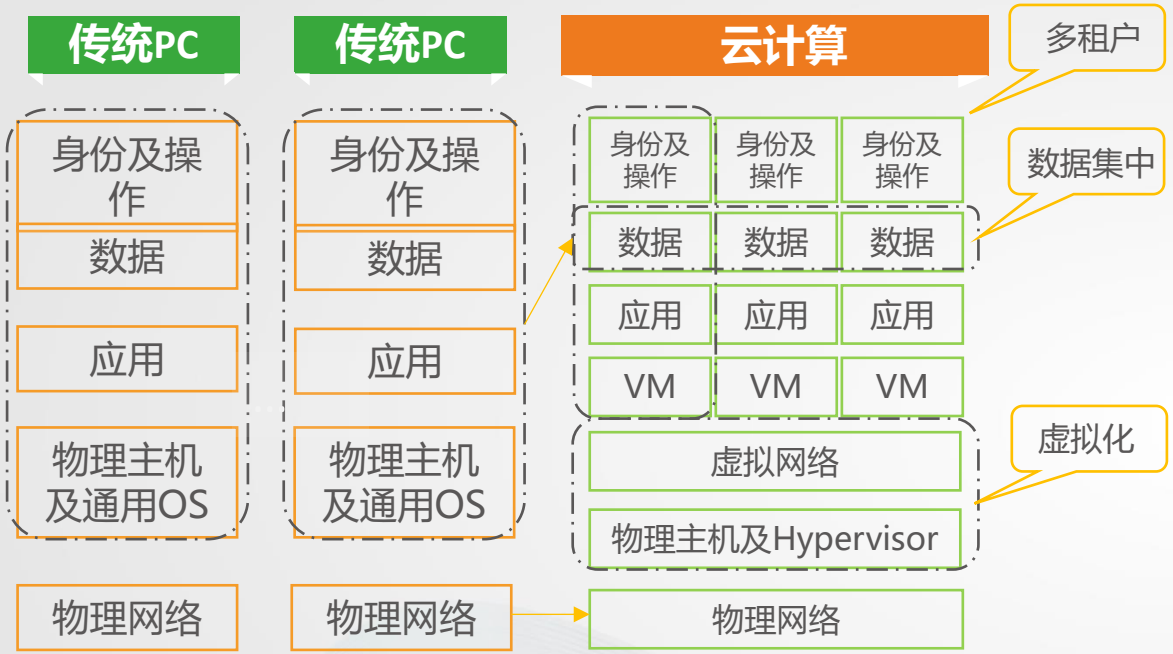
C3安全峰会
CYBER | CLOUD | COMMUNICATION

云安全威胁分析

传统安全威胁在云计算下同样存在

- **应用威胁** SQL注入、跨站等针对应用层的攻击已经成为安全最大的威胁。
- **主机威胁** 病毒蠕虫等将占用系统资源、破坏文件和数据。恶意用户也会利用本地漏洞和配置错误来获取额外权限。
- **数据安全** 破坏数据的机密性、完整性和可用性。
- **网络威胁** 针对网络层的攻击主要有拒绝服务、远程溢出、信息探测、网络监听等。

云计算面临新的威胁



- **虚拟化平台引入新的威胁：** 虚拟化平台运行在操作系统与物理设备之间，其设计和实现中出现的漏洞，将成为新的威胁。
- **多租户安全威胁：** 不同安全需求的租户可能运行在同一台物理机上，传统安全措施难以处理这种情况。
- **特权用户问题：** 应用系统和资源所有权的分离，导致云平台管理员可能访问用户数据，从而对数据机密性、完整性、可用性造成破坏。

除传统威胁外，虚拟化、多租户和特权用户问题使得云计算面临更大风险！

云计算面临的新威胁：虚拟化安全威胁

- **虚拟化平台引入新的威胁**

  在CVE的数据库中，虚拟化软件的漏洞累计超过超过700条，涉及各主要的虚拟机软件。

- **Hypervisor层的漏洞将影响所有的虚拟机**

  作为虚拟机的底层系统，一旦存在漏洞，将危及运行其上的所有虚拟机。

- **网络虚拟化安全威胁**

  同一物理机机上不同虚拟机之间的流量对传统网络安全设备不可见。

- **虚拟机镜像被修改的风险**

  虚拟机镜像在休眠时是数据文件形式存储的，有被修改的风险。

云计算面临的新威胁：多租户安全威胁

C3安全峰会
CYBER | CLOUD | COMMUNICATION

- **网络边界模糊**　不同的租户应用运行在同一物理机上，使网络的物理边界消失，只存在逻辑的边界。
- **恶意租户威胁**　恶意用户可以付费获得对虚拟机访问的权限，从而可以利用漏洞对 Hypervisor 或其它虚拟机进行攻击。
- **数据重用风险**　磁盘释放给其他租户使用，原有数据未被彻底清除的话，可能被新用租户获取

云计算面临的新威胁：特权用户问题

- **云计算特权用户也可以访问数据**

云计算环境下，除了租户访问自己的数据外，云管理员由于需要对资源进行管理，因此也可以接触数据，从而可能造成数据泄露、损坏或被修改。

- **可能存在多个特权用户**

IaaS root权限管理员是特权用户, PaaS RDS 数据库root权限管理员,也是特权用户。

CSA定义的12大安全威胁（1/2）

数据泄露

脆弱的身份、凭证和访问（IdEA）管理

不安全的API

系统和应用程序漏洞

账户劫持

恶意的内部人员

CSA定义的12大安全威胁（2/2）

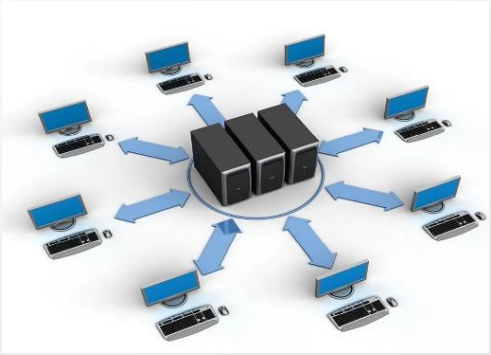
高级持续攻击(APT)

数据丢失

审慎尽职不足

滥用或违法使用云服务

拒绝服务攻击



共享技术的问题

C3安全峰会
CYBER | CLOUD | COMMUNICATION

CSA国际云安全联盟介绍

关于国际云安全联盟

C3安全峰会
CYBER | CLOUD | COMMUNICATION

CSA（Cloud Security Alliance）

2008年12月在美国发起，是中立的非盈利世界性行业组织，致力于国际云计算安全的全面发展，2011年美国白宫在CSA峰会上宣布了美国联邦政府云计算战略。全球300多个单位会员，7万多个个人会员。全球500强中的科技类企业都是会员单位，包括：亚马逊、微软、Google、FaceBook、IBM、Intel、Oracle、Vmware、HP、EMC、趋势科技、华为、阿里、腾讯、中兴通讯、Ucloud等主要的云服务提供商、云计算解决方案提供商。

CSA的宗旨：

- 提供用户和供应商必要的云计算安全需求和保证证书，并达到同样的认识水平
- 促进对云计算安全最佳实践的独立研究
- 推广正确使用云计算和云安全解决方案的宣传和教育计划
- 创建有关云安全保证的问题和方针的明细表

CSA持续从事新兴领域前瞻性安全研究

- CSA 研究院全球有**1000多**个安全专家，分布在美国、欧洲、中国主要的科技公司和研究机构，对新兴领域的安全进行前瞻性的研究，除了云计算，范围还涉及：**大数据、物联网、SDN/NFV、量子通讯等**
- CSA大中华区有**100多**个专家参与全球的安全研究，并在研究成果产业化方面作出独特的贡献。

CSA已经筹建的工作组有30多个，一些特色专题工作组如下：

- 结构及框架工作组
- 安全即服务工作组
- 一致性评估工作组
- 法律及电子发现工作组
- 虚拟化及技术分类工作组
- 数据中心运行及事故响应工作组
- 信息生命周期管理及存储工作组
- 可移植性、互操作性及应用安全工作组
- 身份与接入管理、加密与密钥管理工作组
- GRC，Audit，Physical BCM，DR工作组
- ……

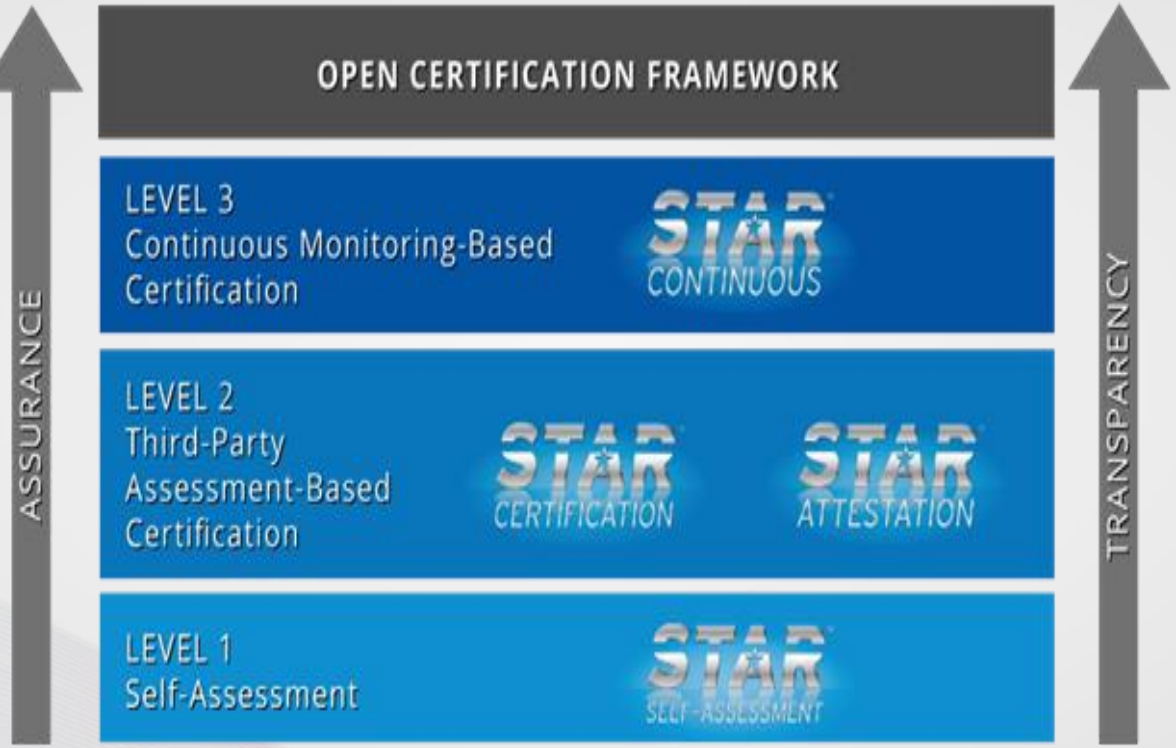
CSA 大中华区是世界标准的“连接器”！

CSA优秀实践概述

C3安全峰会
CYBER | CLOUD | COMMUNICATION

- 云安全指南
- 云安全威胁研究
- 可信云计算架构
- 云安全标准框架
- 量子安全框架
- 大数据安全威胁
- 物联网安全框架
- STAR云安全评估认证
- CCSK云安全培训认证
- 云审计协议
- 云管控、风险、合规工具
- 十大安全云设计实施指导
- SDP软件定义边界高度安全网络

Future: Mobile Application Security Test, Virtualization, Cloud Vulnerability, Cloud Security Eco-System，SDN/NFV，……



The CSA Open Certification Framework is an industry initiative to allow global, accredited, trusted certification of cloud providers.

CCSSP
Certified Cloud Security Systems Professional

CCSMP
Certified Cloud Security Management Professional

C-CCSK
China- Certificate of Cloud Security Knowledge

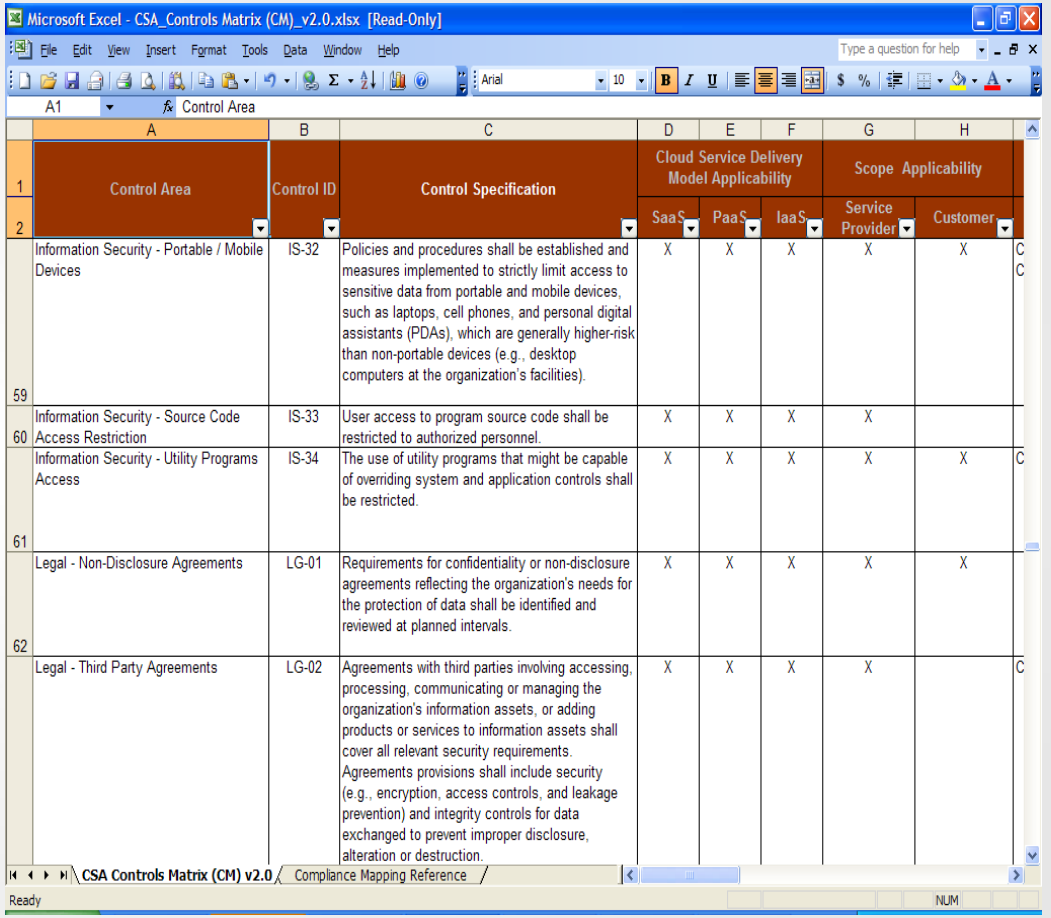
CSA优秀实践1：云安全指南

- CSA “Security Guidance for Critical Areas of Focus in Cloud Computing云计算关键领域安全指南”从2009年推出开始，已持续更新到V3.0.1版本
- **是云安全领域奠基性的理论基础**，得到全球普遍认可，具有广泛的影响力，被翻译成6国语言，成为业界云安全研究、各个国家和地区建立云安全标准和云安全战略最权威的理论和实践基础
- V4.0版本正在写作中 (2017.5.16推出)

CSA优秀实践2：云安全控制矩阵

CCM
Cloud Controls Matrix

- 在CSA云安全指南基础上推出“云安全控制矩阵CCM”，成为云计算信息安全行业国际公认标准
- CCM结合云计算业务特点，匹配了国际主要的信息安全标准和行业标准：ISO 27001, COBIT, PCI, HIPAA, FISMA, FedRAMP, Countries
- CCM核心内容被ISO 27017（信息安全治理架构）与ISO 27036（供应商关系的信息安全）采纳


Microsoft Excel - CSA_Controls Matrix (CM)_v2.0.xlsx [Read-Only]

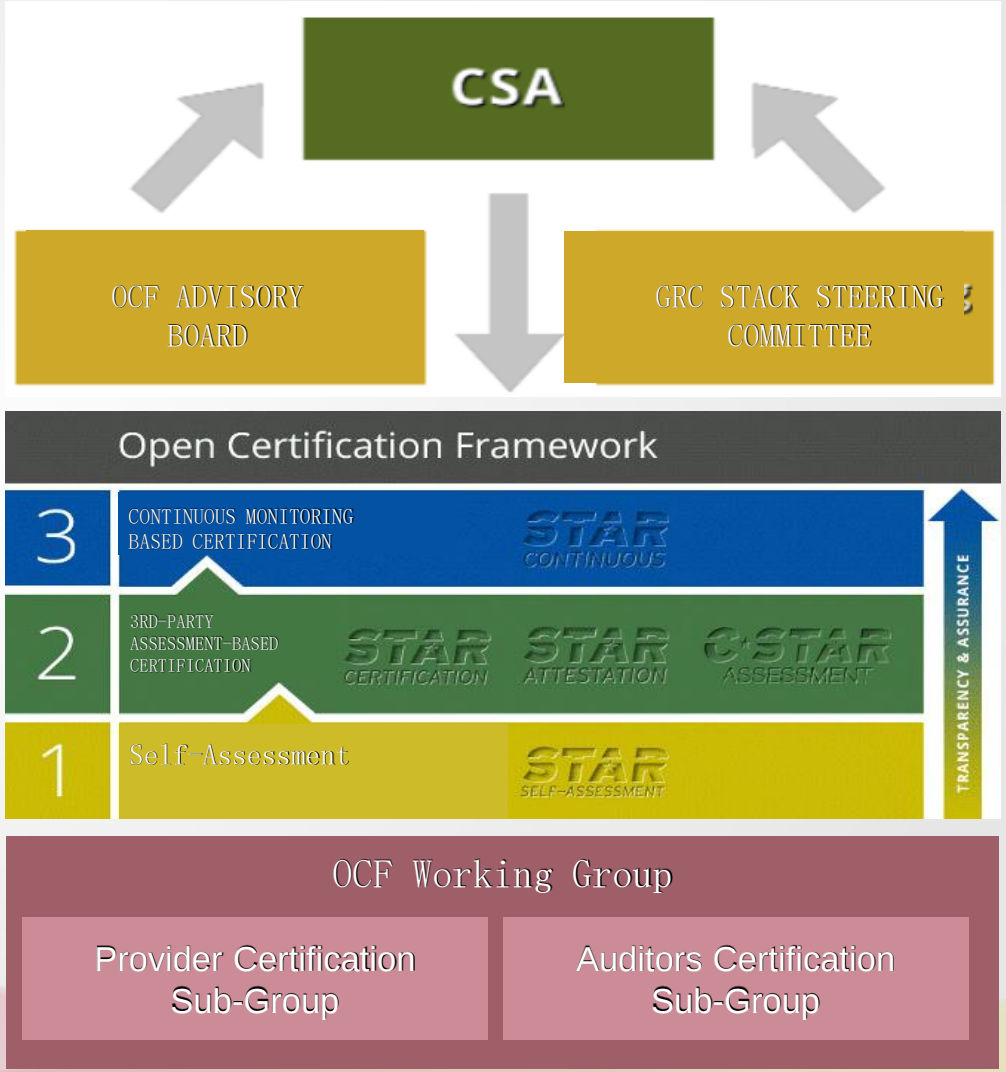
	Control Area	Control ID	Control Specification	Cloud Service Delivery Model Applicability			Scope Applicability		
				SaaS	PaaS	IaaS	Service Provider	Customer	
59	Information Security - Portable / Mobile Devices	IS-32	Policies and procedures shall be established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).	X	X	X	X	X	C C
60	Information Security - Source Code Access Restriction	IS-33	User access to program source code shall be restricted to authorized personnel.	X	X	X	X		
61	Information Security - Utility Programs Access	IS-34	The use of utility programs that might be capable of overriding system and application controls shall be restricted.	X	X	X	X	X	C
62	Legal - Non-Disclosure Agreements	LG-01	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of data shall be identified and reviewed at planned intervals.	X	X	X	X	X	
	Legal - Third Party Agreements	LG-02	Agreements with third parties involving accessing, processing, communicating or managing the organization's information assets, or adding products or services to information assets shall cover all relevant security requirements. Agreements provisions shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.	X	X	X	X		C

CSA Controls Matrix (CM) v2.0 | Compliance Mapping Reference
Ready

CSA优秀实践3：OCF和STAR认证体系

STAR™ SELF-ASSESSMENT

- 基于CCM，CSA建立了“开放认证框架”OCF（ Open Certification Framework ）和STAR认证体系（ Security, Trust and Assurance Registry ）
- CSA与英国标准协会BSI强强联合，在全球开展CSA STAR认证；CSA在中国，结合等保，推出针对中国市场的CSA C-STAR认证。
- CSA STAR认证是全球最权威的云安全管理体系认证，主流的云服务商都遵守CCM，并通过了STAR和C-STAR认证：亚马逊、微软、HP、阿里、华为等



CSA优秀实践4：云安全技术标准（CSTR）

- CSA CSTR（Cloud Computing Security Technology Requirements）是全球第一个针对云计算产品与解决方案的技术标准，系统呈现了全球主要云服务商和云计算解决方案提供的优秀实践
- CSTR由CSA大中华区主导，全球主流云计算厂家和研究机构共同制定，发源于中国，贡献到全球的原创性标准：亚马逊、微软、Intel、Oracle、华为、阿里、腾讯、百度、中国移动、中国电信、中兴、金蝶、京东云、Ucloud、浪潮、中科院、公安三所、武汉大学、深圳标准技术研究院等。
- CSTR标准2016年10月25日CSA大中华区峰会上发布，基于CSTR标准（草案），CSA全球将推出CSA STAR Tech国际认证。

CSA优秀实践4：云安全技术标准（CSTR）

CSA优秀实践5：STAR Tech云计算产品安全认证

C3安全峰会
CYBER | CLOUD | COMMUNICATION

STAR Tech
Security, Trust and Assurance Registry Tech

- 基于CSTR,CSA在“开放认证框架”OCF（ Open Certification Framework ）基础上，开展STAR Tech认证体系
- CSA在中国联合赛宝实验室开展CSA STAR Tech认证。
- CSA STAR Tech认证是全球最权威的云计算产品安全认证。


CEPREI

CSA STAR Tech
云计算产品信息安全认证证书

（正本）
兹证明

XXXXX 有限公司
统一社会信用代码：XXXXX
注册地址：XXXXX
运营地址：XXXX XXXXXX
产品名称、版本：
XXXXXX
XXXXXXXXXXXXXX

依据技术标准要求：
CSA 《CSA 云计算安全技术要求》中的增强级要求

该产品已经 CSA 认可的赛宝认证中心按照以下认证模式和认证规则实施认证，符合以上认证要求，特发此证。

认证制度：产品检测 ☑
现场检查 ☑
获证后监督 ☑

注 册 号：XXXXXX
颁证日期：YYYY.MM.DD
有效期至：YYYY.MM.DD
换证日期：YYYY.MM.DD

总经理：

CEPREI
CSA cloud security alliance

证书样例

CSA优秀实践6：国际注册云计算安全专家认证体系

C3安全峰会 CYBER | CLOUD | COMMUNICATION

初级

C-CCSK (Foundation)

China - Certification of Cloud Security Knowledge
云计算安全**基础知识**认证

中级

C-CCSK

China - Certification of Cloud Security Knowledge
云计算安全**知识**认证

高级

CCSMP

Certified Cloud Security Management Professional
国际注册云安全**管理**认证专家

高级

CCSSP

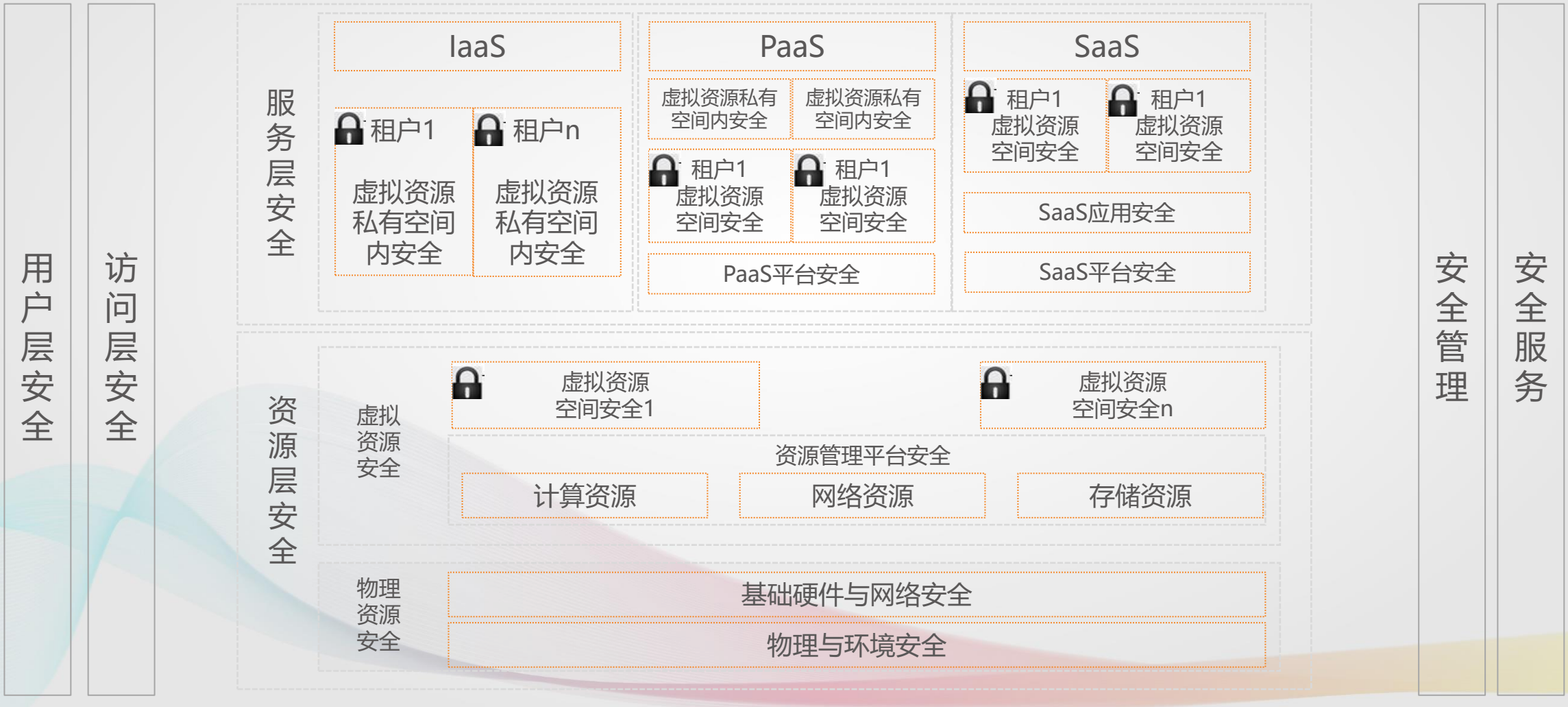
Certified Cloud Security Systems Professional
国际注册云安全**系统**认证专家

C3安全峰会
CYBER | CLOUD | COMMUNICATION

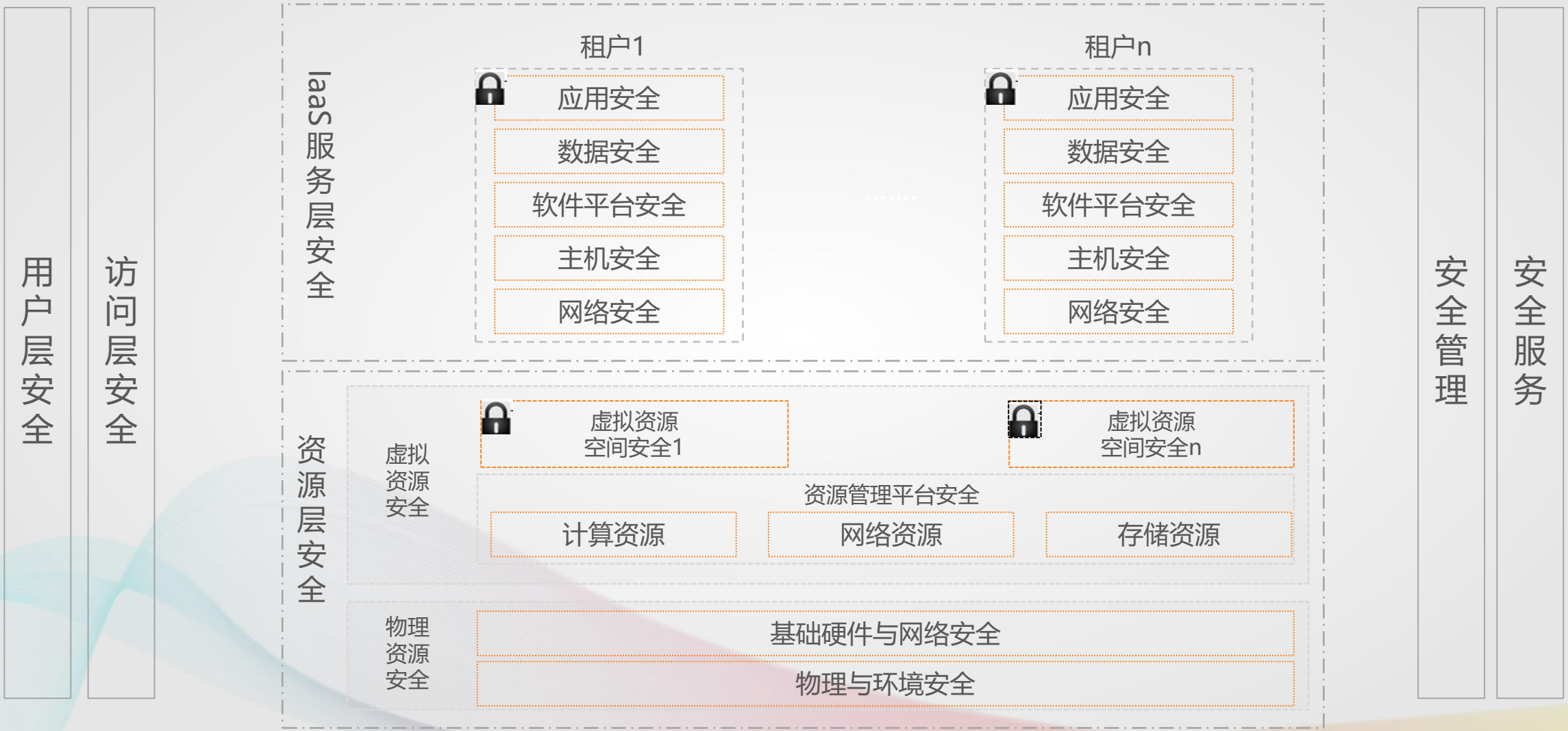
CSA云安全标准与实践集

ISO/IEC 17789定义的云计算层次框架

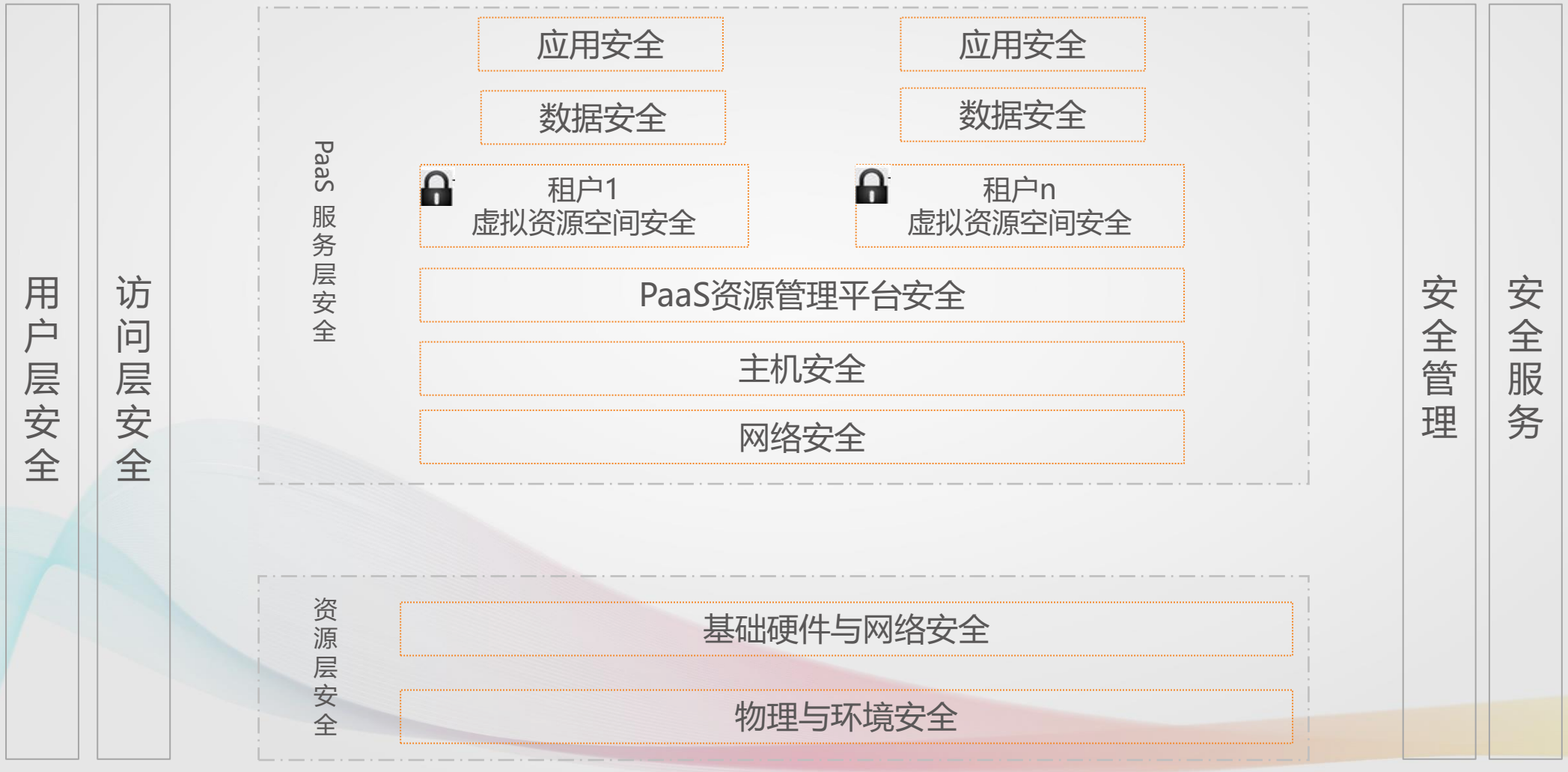
云计算解决方案安全技术要求框架



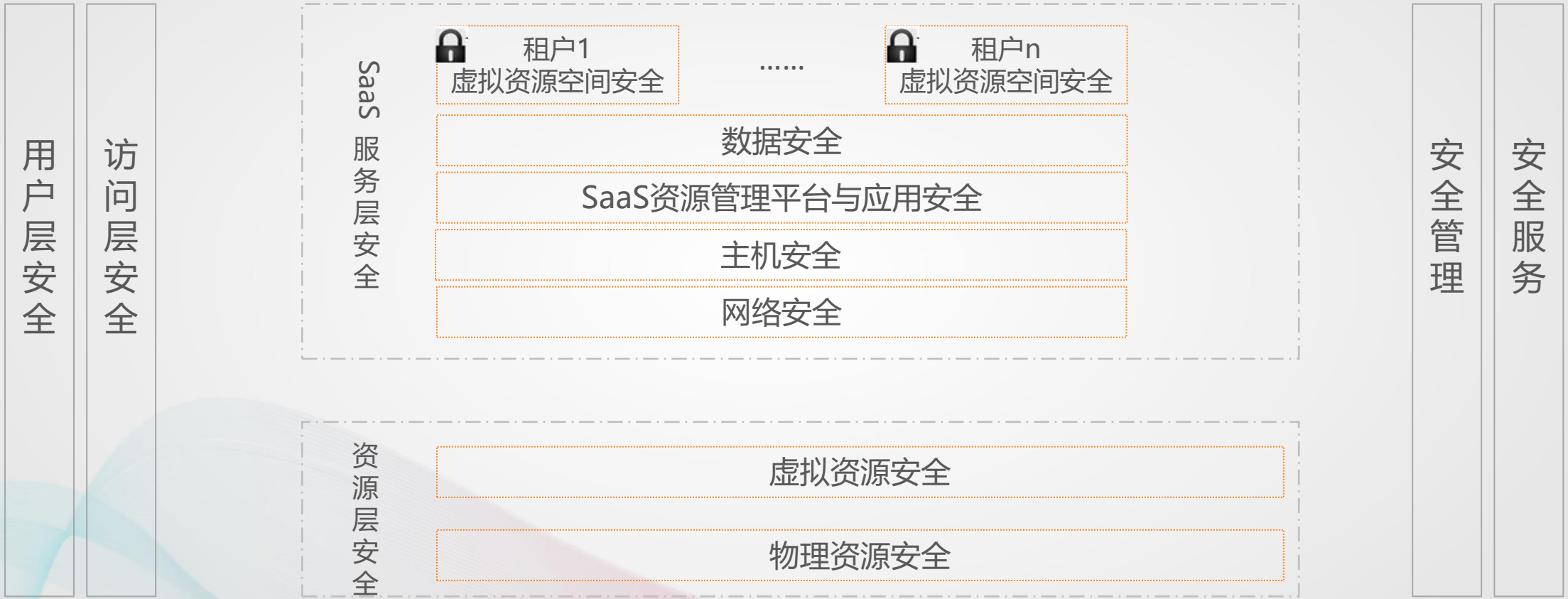
IaaS云服务安全技术要求框架



PaaS云服务安全技术要求框架



SaaS云服务安全技术要求框架



C3安全峰会
CYBER | CLOUD | COMMUNICATION

Thank You