云安全技术与应用

- 日照职业技术学院
- 电子信息工程系
- 赵娜

项目一

云安全概述

目录

CONTENTS

01.

O N E

理解云安全内涵

理解云安全的内涵

“云安全(cloud security)”是继“云计算”“云存储”之后出现的“云”技术的重要应用，是传统IT领域安全概念在云计算时代的延伸。

云安全通常包括两个方面的内涵：

一是云计算安全，即通过相关安全技术，形成安全解决方案，以保护云计算系统本身的安全；

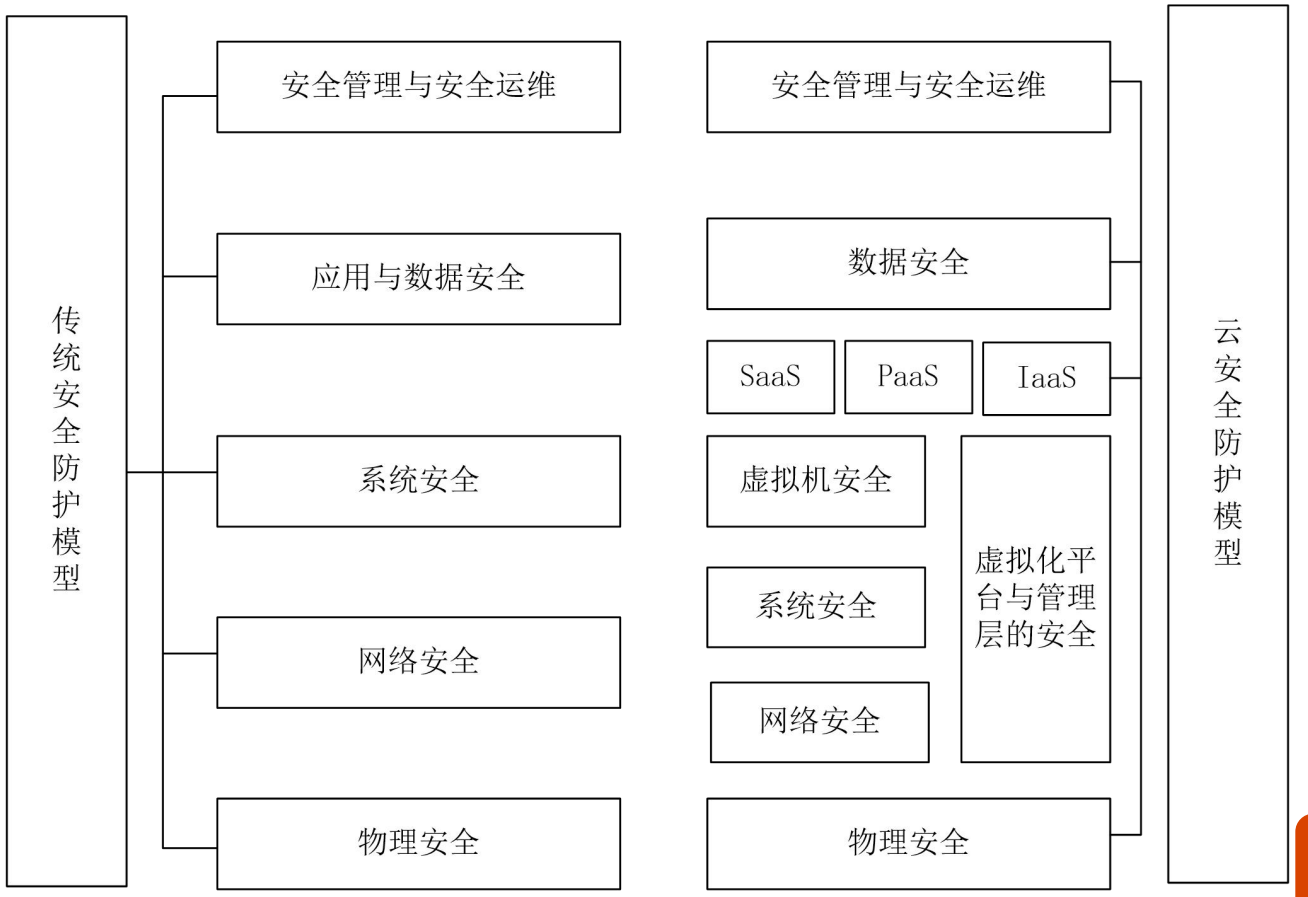
二是安全云，特指网络安全厂商构建的提供安全服务的云，让安全成为云计算的一种服务形式。

02

比较云安全与传统安全

比较云安全与传统安全

随着传统环境向云计算环境的大规模迁移，云计算环境下的安全问题变得越来越重要。传统安全与云安全的对比如右图所示。



传统安全与云安全

比较云安全与传统安全

传统安全和云安全相同之处如下:

- 目标相同：都是为了保护信息、数据的安全和完整。
- 保护对象相同：保护的对象均为系统中的用户、计算、网络、存储资源等。
- 技术类似：包括加解密技术、安全检测技术等。

比较云安全与传统安全

云计算面临威胁和挑战:

2013年在美国旧金山举行的RSA大会上，CSA提出了“2013年云计算的九大威胁”：

- 数据泄露
- 数据丢失
- 账户劫持
- 不安全的API
- 拒绝服务攻击
- 内部人员的恶意操作
- 云计算服务的滥用
- 云服务规划不合理
- 共享技术漏洞

比较云安全与传统安全

云计算面临威胁和挑战:

2016年，CSA再次列出了2016年“十二大云安全威胁”：

- 数据泄露
- 凭证被盗和身份验证如同虚设
- 界面和API被黑
- 系统漏洞利用
- 账户劫持
- 恶意内部人士
- APT(高级持续性威胁)寄生虫
- 永久的数据丢失
- 调查不足
- 云服务滥用
- 拒绝服务(DoS)攻击
- 共享技术，共享危险

比较云安全与传统安全

综合网络安全行业的各类分析报告及云计算安全的现实情况，云计算安全面临的挑战主要来源于技术、管理和法律风险3个方面，具体如下：

- 数据集中。聚集的用户、应用和数据资源更方便黑客发动集中的攻击，事故一旦产生，影响范围广、后果严重。
- 防护机制。传统基于物理安全边界的防护机制在云计算的环境难以得到有效的应用。
- 业务模式。基于云的业务模式给数据安全的保护提出了更高的要求。
- 系统复杂。云计算的系统非常大，发生故障的时候要进行快速定位的挑战也很大。

比较云安全与传统安全

- 开放接口。云计算的开放性对接口安全提出了新的要求。
- 管理方面。在管理方面，云计算数据的管理权和所有权是分离的，需要不断完善使用企业和云服务提供商之间运营管理、安全管理等方面的措施。
- 法律方面。法律方面主要是地域性的问题，如云信息安全监管、隐私保护等方面可能存在法律风险。

03.

剖析云安全体系架构

剖析云安全体系架构

云计算安全参考模型

云安全联盟提出的云计算安全参考模型如图所示。

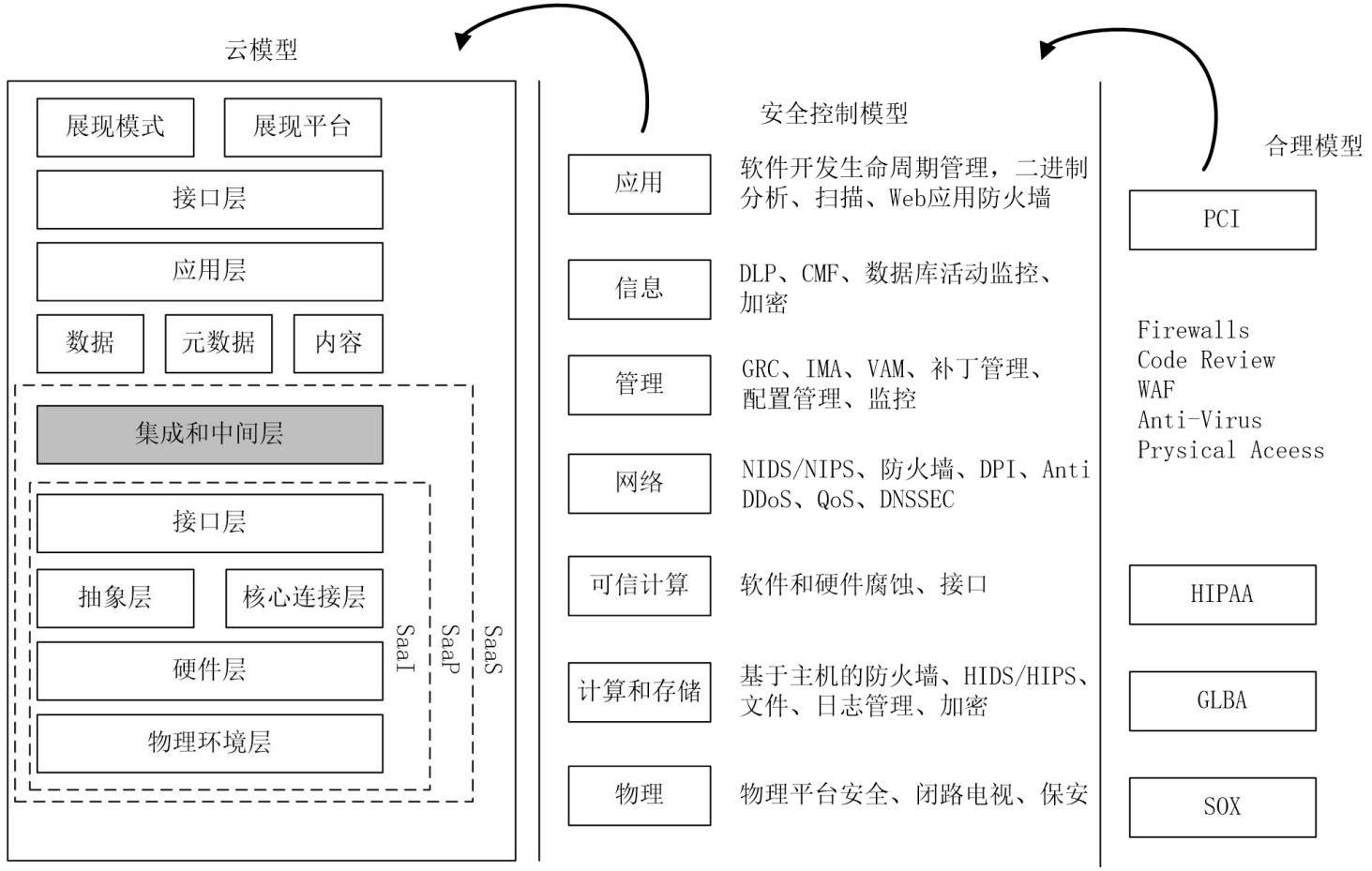
云计算安全参考模型描述了合规模型、安全控制模型和云模型之间的关系，也详细地描述了云模型中IaaS。PaaS和SaaS之间的关系。

IaaS涵盖了从机房设备到硬件平台等所有的基础设施资源层面。

PaaS位于IaaS之上，增加了一个层面用以与应用开发、中间件能力以及数据库、消息和队列等功能集成。

SaaS位于底层的IaaS和PaaS之上，能够提供独立的运行环境，用以交付完整的用户体验，包括内容、展现、应用和管理能力。

剖析云安全体系架构



云计算安全参考模型（云安全联盟）

剖析云安全体系架构

云计算安全模型分析

安全厂商可以基于CSA提出的云计算安全模型，提出独具特色的云安全解决方案。右图为国内厂商提出的一种典型的云安全架构。

某厂商提出的一种典型的云安全架构

04

了解云安全主要内容

了解云安全主要内容

云安全包含的内容与技术非常广泛，既包括传统的安全内容和技术，也包括云计算架构下的新型的安全内容和技术。云安全主要内容和技术如下：

（1）数据安全

数据传输、数据隔离、数据残留

（2）应用安全

终端用户安全、SaaS安全、PaaS安全、IaaS安全

（3）虚拟化安全

虚拟化软件、虚拟服务器

05.

安全即服务（SECaaS）

认知SECaaS

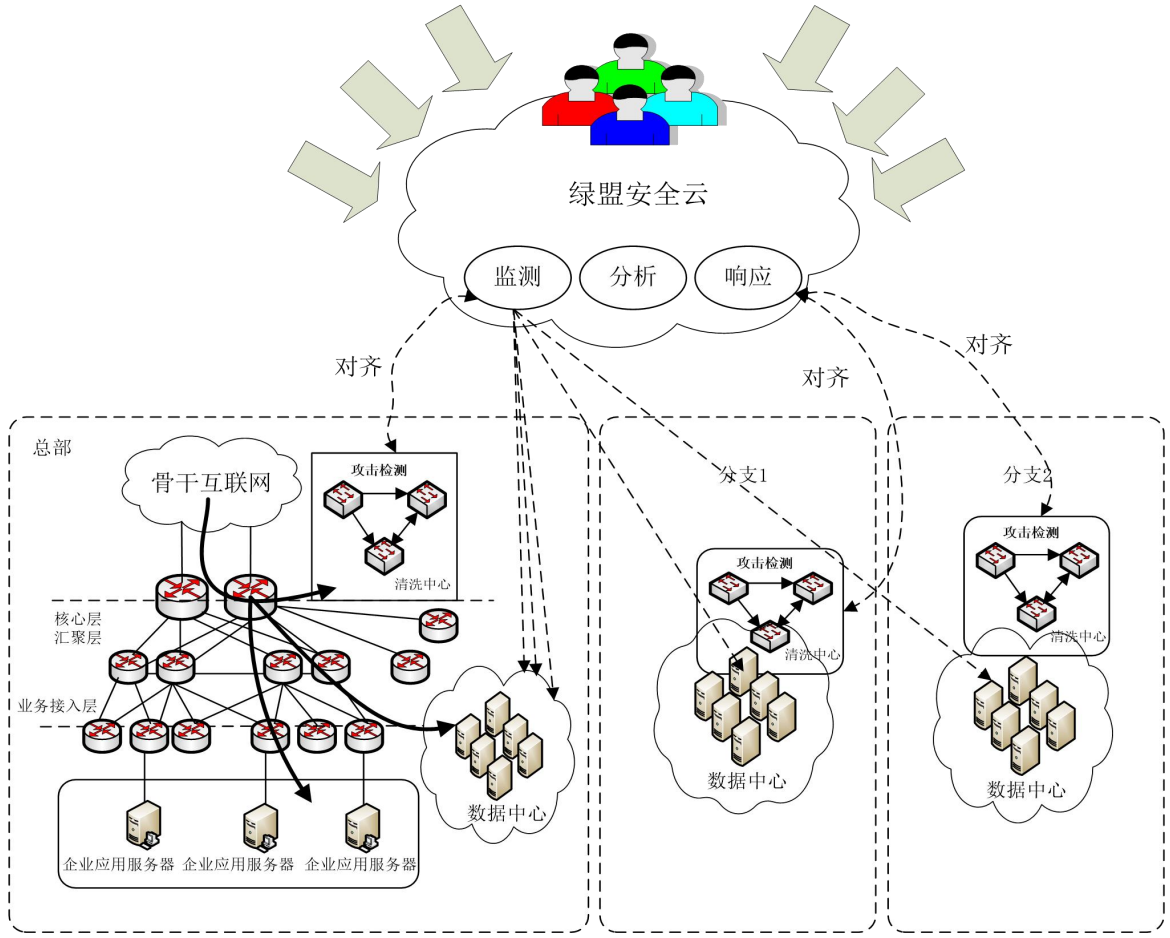
安全即服务(Security as a Service，SECaaS)是一个用于安全管理的外包模式。通常情况下，SECaaS包括通过互联网发布的应用软件(如反病毒软件)，基于互联网的云安全产品是SaaS的一部分。

SECaaS是从云的角度出发来考虑企业安全，通过基于云的服务来保护云中的、传统企业网络中的及两者混合环境中的系统和数据。

SECaaS产品的厂商有Cisco、McAfee、熊猫软件、Symantec、趋势科技和VeriSign。

认知SECaaS

2014年5月，绿盟科技云安全运营服务业务获得ISO27001管理体系的认证，这标志着绿盟科技成为国内首家通过ISO270011认证的可管理安全服务(简称MSS)和SECaaS提供商。绿盟ADS可管理的安全服务(NSFOCUS MSS for ADS，原名PAMADS)示意图如右图所示。



绿盟MSS for ADS示意图

认知SECaaS

从发展趋势来看，安全服务未来将不仅限于咨询和运维，SECaaS这种新的商业模式将成为网络安全产业的未来发展方向。相比于传统模式，具有以下几个优点：

- 无需本地部署安全系统，只需数据中心对接。
- 响应速度快，升级快。
- 企业的安全支出将会更加弹性，对于广大中小企业尤其是互联网创业公司，可以减少自己初期的开支，刺激他们的需求。

解读SECaaS优势

- 人员力量增强
- 提供先进的安全工具
- 提供专业技术知识
- 将信息安全定位为业务推动力
- 身份管理
- 虚拟机管理
- 网络层保护

概览SECaaS应用领域

- 身份、授权和访问管理服务
- 数据泄露防护(DLP)
- Web安全
- Email安全
- 安全评估
- 入侵检测 / 防护(IDS/IPS)
- 安全信息和事件管理(SIEM)
- 加密
- 业务连续性和灾难恢复
- 网络安全

06

O N E

课后扩展

课后查询资料

目前流行的云安全解决方案：

1. 长城网际云安全解决方案
2. 蓝盾云安全解决方案
3. 绿盟科技云安全解决方案