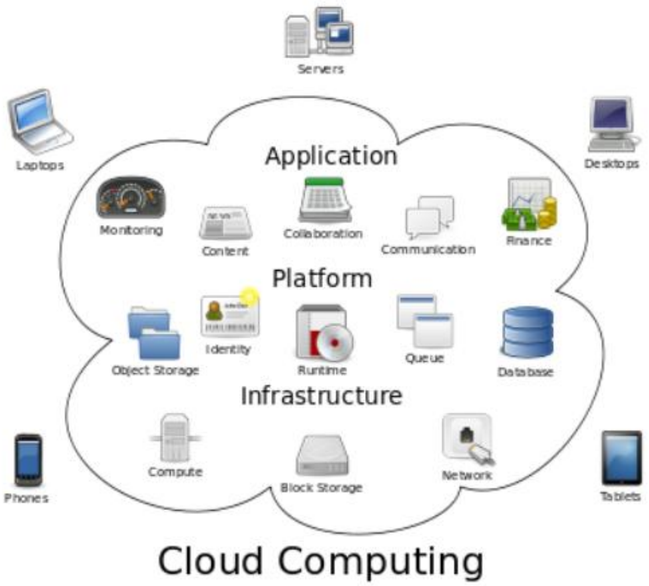
CSA研讨会–SaaS安全护航企业合规经营

云应用安全标准和测评

主讲人：陈妍 博士 副研究员

公安部第三研究所检测中心

云计算的三种服务模式



- 软件即服务（SaaS）——Software as a Service
- 平台即服务（PaaS）—— Platform as a Service
- 基础设施既服务（IaaS）—— Infrastructure as a Service

- **软件即服务（SaaS）——云应用**

通过网络为最终用户提供应用服务。绝大多数SaaS应用是直接在浏览器中运行的，不需要用户下载和安装任何程序。SaaS是由服务商管理和托管的完整应用软件，用户可以通过Web浏览器、移动应用或轻量级客户端应用访问它。

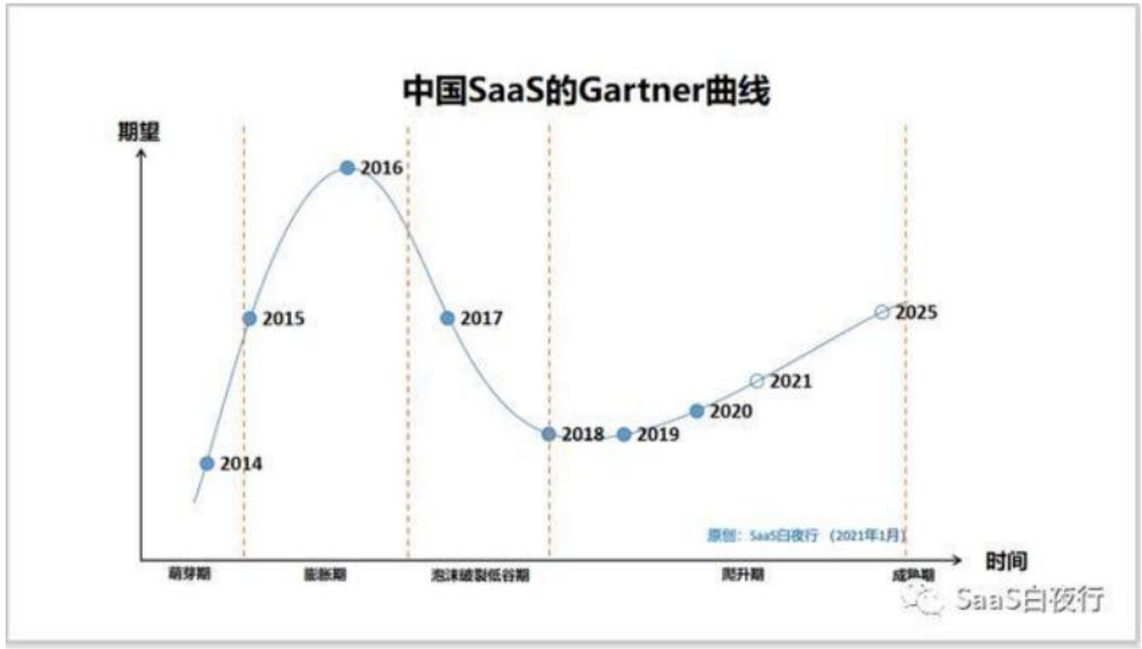
- **传统应用云化、安全云化**
- **Salesforce、Palo Alto Networks、金蝶、用友等**

云应用的市场规模

SaaS到达爆发式增长的拐点，云安全的下半场看云应用安全

SaaS风口

本翼资本预测，2025年中国企业软件市场规模有望达到1.1万亿元，企业级SaaS服务规模有望达到370亿美元。



云应用的安全问题

数据泄露

删库跑路

非法访问

- 被利用的漏洞
- 错误的配置管理
- 特权用户的不恰当使用
- 不安全的传输
- 应用的不可访问
- 安全责任的不明确
- 租户数据隔离
- 云上资产管理混乱
- 自身安全防护手段不足

云应用安全技术规范

- **29**家单位参与
- **31**位专家起草
- 业界第一个云应用安全类的标准
- 分为基础级和增强级

标准价值：

☐ 建设指导：指导厂商研发安全的云应用

☐ 评估指导：指导租户评估云应用的安全性

☐ 合规证明：通过标准认证可以快速向租户证明云应用的安全性

两个视角：

☐ 云应用厂商：保障云应用整体安全并提供租户级安全功能

☐ 云应用租户：用好租户级安全功能，符合云安全责任共担模型

更关注租户安全：

☐关注租户自助能力

☐关注租户差异化能力

☐关注租户定制化能力

最后一公里安全：

☐云应用实施安全

☐云应用交付安全

☐云应用服务安全

关注数据安全与隐私合规

☐ 数据安全合规：数据存储位置与跨境

☐ 隐私保护合规：隐私保护功能设计

云应用安全框架

8个控制域

控制域	控制项数量
云应用架构设计要求	22
应用运行环境要求	29
云应用程序安全要求	67
访问控制安全要求	27
租户级安全自助能力要求	9
云应用实施/交付/服务安全要求	23
数据安全要求	27
安全管理能力要求	15

219个控制项

紧跟新技术、新业务场景步伐

控制域介绍

云应用架构设计要求

- □ 高可用：弹性、容错、故障隔离、灾备
- □ 高性能：缓存、索引、性能监测与预警
- □ 高安全：数据/资源隔离、默认安全、纵深防御

控制域介绍

运行环境安全要求

- ☐ 操作系统：加固、访问控制、补丁、变更、镜像完整性
- ☐ 容器与编排平台：配置、镜像完整性、补丁、访问控制
- ☐ 数据库：漏洞、访问控制、审计
- ☐ 中间件：加固、访问控制、补丁
- ☐ 熔断与环境隔离：数据/资源隔离、故障隔离、故障熔断

控制域介绍

云应用程序安全要求

- ☐ Web安全：**Owasp Top 10...**
- ☐ 移动APP安全：加固、完整性、权限
- ☐ API接口安全：资产、文档、验证、权限、传输
- ☐ 小程序安全：加固、访问控制、补丁
- ☐ 后台应用程序安全：身份鉴别、租户路由、业务上下文
- ☐ 第三方SDK安全：管控、完整、官方来源
- ☐ 云应用代码防泄露：监测、发现、预警

控制域介绍

访问控制安全要求

- 通信安全：认证、授权、加密、防攻击、弹性
- 安全区域：网络区域、资源/数据区域、访问控制、IP白名单
- 会话安全：并发、会话时效、异常提醒、锁定与解锁
- IAM：RBAC、ABAC、最小权限原则、动态权限
- 访问终端：终端识别、终端行为识别

控制域介绍

租户级安全自助能力要求

- □ 租户级IAM自助服务：账号、凭证、认证、授权、SSO
- □ 租户级自助审计：登录、操作审计

控制域介绍

应用实施/交付/服务安全要求

- □ 应用实施/交付/服务安全控制：实施人员权限控制、数据初始化安全、灰度交付、SLA保障
- □ 互操作性和可移植性：集成能力、迁移能力
- □ 安全即服务SecaaS：安全服务自身安全保障
- □ 功能扩展与定制化交付：零代码、低代码、APaaS、ISV

控制域介绍

数据安全要求

- □ 租户数据隔离：实施人员权限控制、数据初始化安全、灰度交付、**SLA**保障
- □ 机密性
- □ 可用性
- □ 完整性
- □ 隐私保护:产品隐私政策“同意”“单独同意”“撤销”“注销”等功能
- □ 数据位置与跨境

控制域介绍

安全管理能力要求

- 厂商：保障云应用及相关资源及数据的安全相关安全管理动作
- 租户 ：合理使用云厂商提供的安全能力，其他应由租户承担的安全义务

运营与安全可信认证

- 云应用安全可信认证：CSA Cloud Application Security Trust （简称“CAST认证”）。
- 包括但不限于SaaS产品、所有在线订阅类服务、IaaS/PaaS云的应用部分，可以是软件产品，也可以是在线服务。
- 依据《CSA GCR C001-2022 云应用安全技术规范》
- “公安部第三研究所安全防范与信息安全产品及系统检验实验室”与“国际云安全联盟CSA大中华区”联合认证。
- CAST认证作为独立的第三方认证，相关的评估体系和标准由国际云安全联盟、公安部第三研究所安全防范与信息安全产品及系统检验实验室组织数十家云应用、网络安全或相关领域的头部厂商共同参与制定，旨在客观公正的对云应用进行安全和可信能力测评，并将逐步替代CSTR（云计算产品信息安全认证） SaaS类产品认证。
- CAST证书的有效期 3 年，证书失效后需重新申请。

认证流程

① 受理申请：委托单位提出申请，填写《云应用安全可信认证申请书》。

② 合同签订：《云应用安全可信认证委托检验检测合同》。

③ 提交相应材料：云应用安全可信认证产品送检技术资料。

④ 开展测评：测评机构根据测评计划开展测评活动。

⑤ 整改：委托单位视测评情况进行整改。

⑥ 开展复测：由测评机构对整改后的产品开展复测。

⑦ 出具测评报告：满足一定条件（包括分数达到一定要求、没有中高风险），出具测评报告。

⑧ 获得认证：认证机构向测评结果达标的委托单位发放认证证书。

整个流程完成在合同受理后的45个工作日。

THANKS

CSA GCR cloud security alliance GREATER CHINA REGION ® × 上上签 —电子签约云平台—