云计算安全问题思考

中国科技网 龙春

2015.11.18

提纲

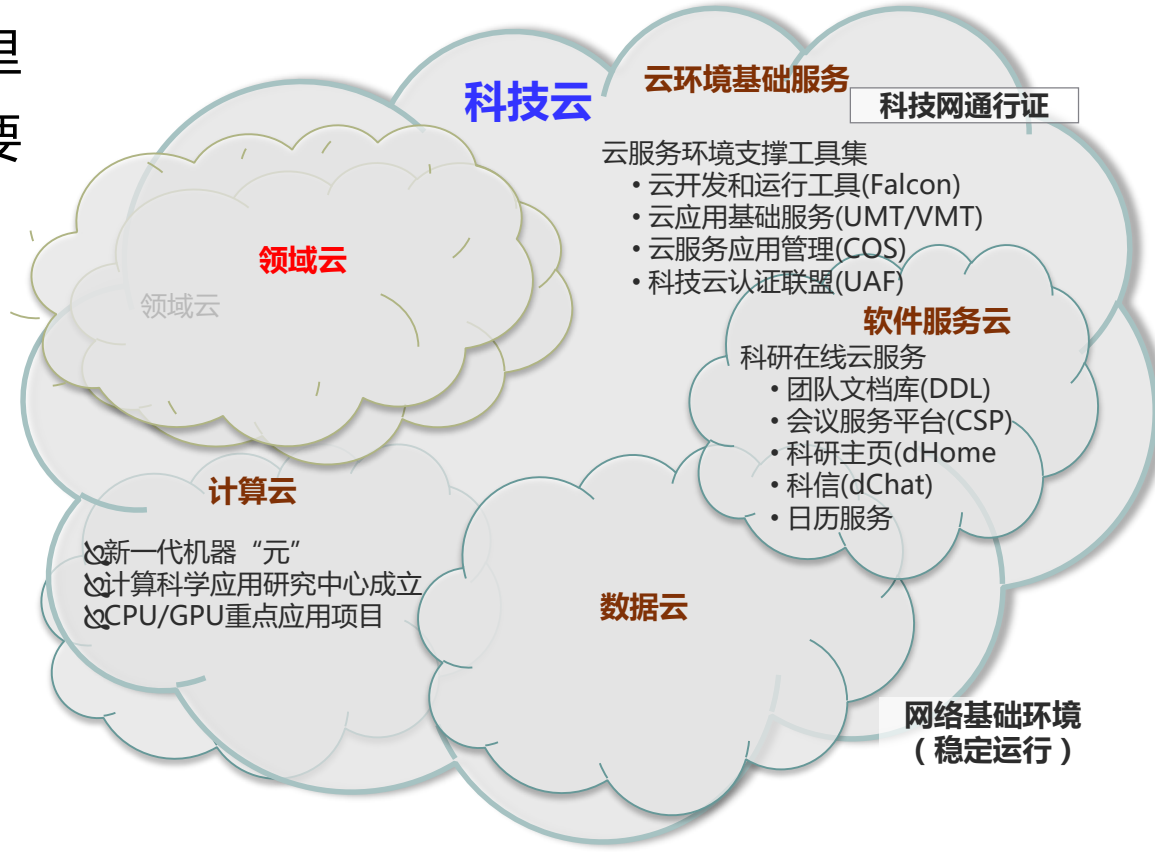
- 云计算环境安全风险
- 云计算安全保障框架
- 安全态势感知和威胁分析系统

安全工作目标

- 信息系统及服务稳定运行
  - 网络
  - 云计算平台
  - 应用服务
- 确保信息仅被授权方获取
  - 防止工作、知识产权等信息泄露
  - 防止隐私泄露
- 防止信息被非法修改
  - 防止篡改
  - 防止删除

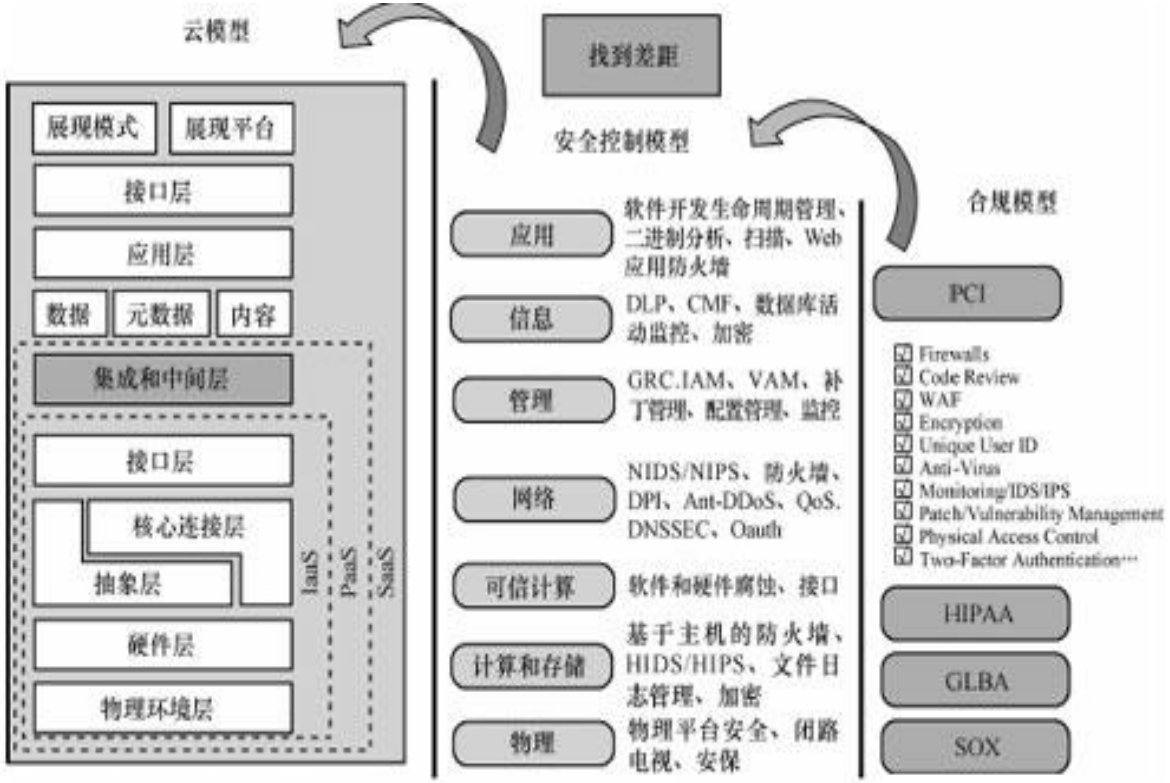
云计算环境的安全风险

- 资源集中带来的风险
  - 所有的鸡蛋都在一个篮子里
  - 网络传输的可用性更加重要
- 特权用户风险
- 虚拟化和共享的安全风险
  - 数据存储位置的不确定性
  - 数据访问控制措施复杂
  - 数据恢复的不可控制
- 终端的安全风险
  - 终端本身安全风险
  - 无线传输链路风险

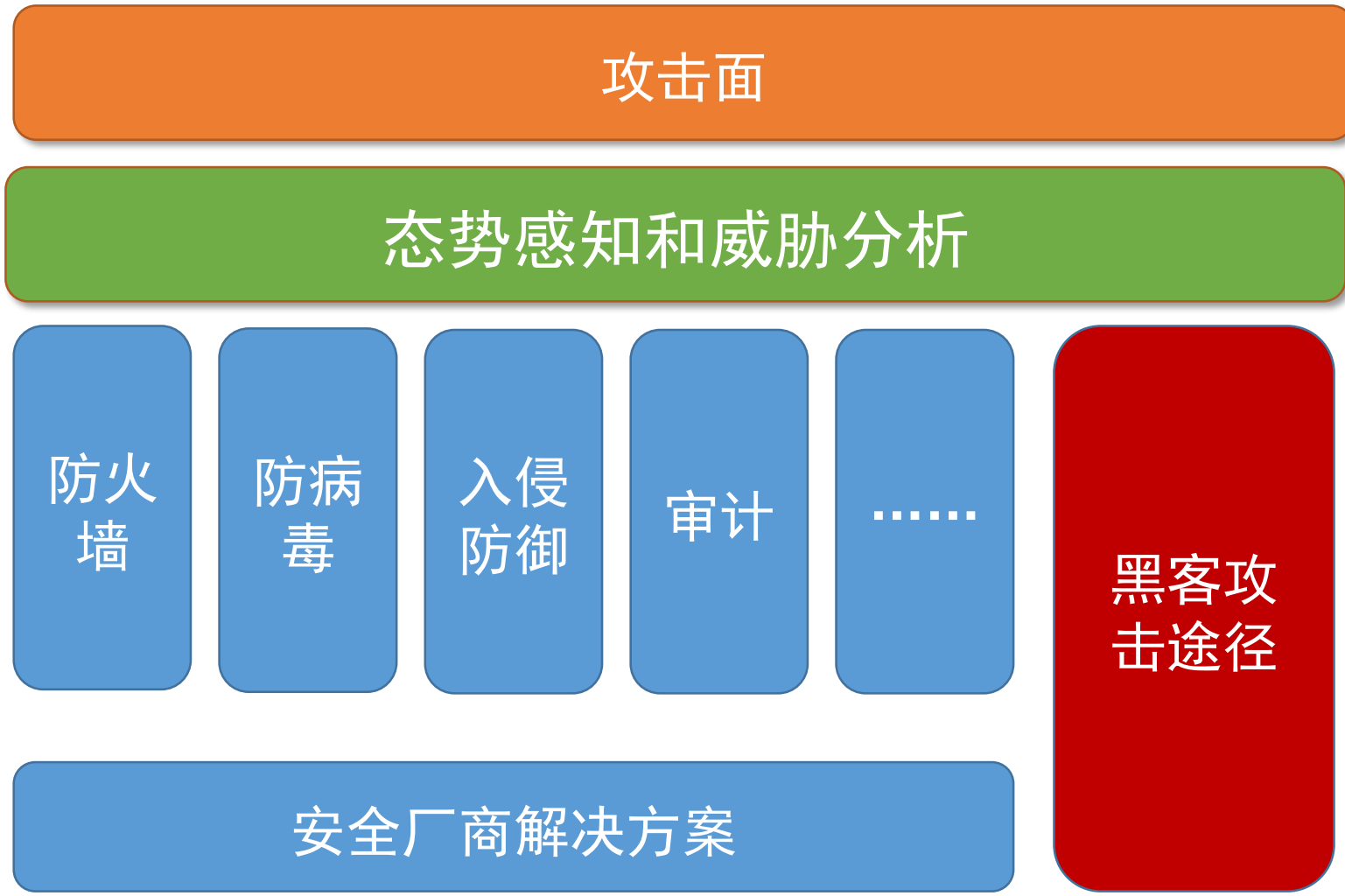


云计算及数据安全

- 业务连续性保障
- 网络和数据隔离
- 重要数据加密
- 用户认证和权限管理
- 特权账户操作审计
- 建设、开发和运维规范

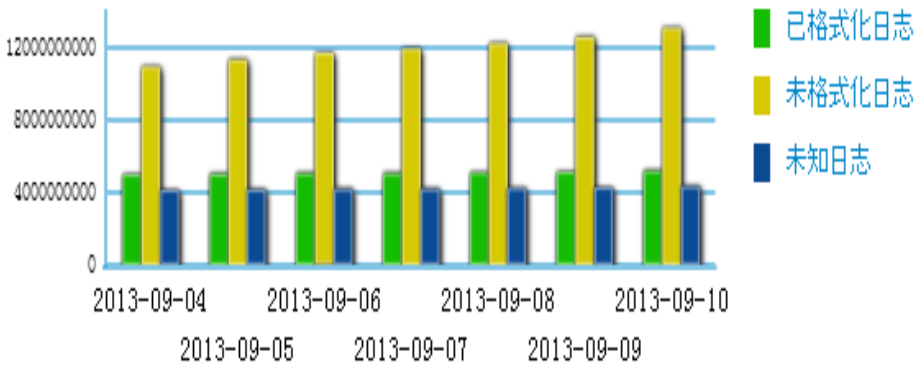


为什么需要态势感知和威胁分析



中国科技网安全大数据采集

- 每天采集原始数据日志量约2亿条，处理数据包括：
  - 入侵检测数据
  - 漏洞扫描数据
  - 网站访问日志
  - Netflow
  - 审计系统
  - ……



进展情况

- IDS、IPS24小时实时数据预处理、格式化
- 6个季度网站、主机扫描报告数据爬取过滤
- 业务划分、分布式存储

数据收集

- 安全态势评估方法重定义
- 安全域定义
- 数据聚类
- 数据关联分析
- 建立安全特征匹配库

数据分析

- 全球实时攻击
- 全国实时攻击
- 全网安全态势
- 全院漏洞分布
- 通知与公告

数据可视化

谢谢！ Q&A