CSA GCR 6th Congress 第六届云安全联盟大中华区大会

CSA GCR cloud security alliance GREATER CHINA REGION

基于零信任安全模型的数据安全风险治理实践

演讲人：薛恺 杭州美创科技股份有限公司

CSA GCR 6th Congress 第六届云安全联盟大中华区大会

目　录

CONTENTS

数字经济发展

《“十四五”数字经济发展规划》：数字经济是继农业经济、工业经济之后的主要经济形态，是以数据资源为关键要素，以现代信息网络为主要载体，以信息通信技术融合应用、全要素数字化转型为重要推动力，促进公平与效率更加统一的新经济形态。

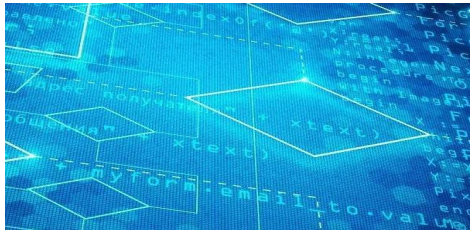
八大重点任务

优化升级数字基础设施	充分发挥数据要素作用	大力推进产业数字化转型	加快推动数字产业化
持续提升公共服务数字化水平	持续提升公共服务数字化水平	着力**强化数字经济安全体系**	有效拓展数字经济国际合作

面对风险的思考

开放的网络环境、复杂的业务数据类型、信息融合和共享等挑战给数据安全防护带来了挑战。如何实现多跨场景下数据安全管控，开展面向数据安全风险的感知、理解、计算、预测和防范的全过程研究变得更为迫切。

高价值的数据资产



复杂的数据生态系统

不止入侵防御/攻防

数据会流动且好流动

风险治理-突破

需要基于业务场景，对人、流程、访问、环境等多维因素进行相应的信任评估，
通过信任级别动态地调整权限，构建动态自适应的安全防护闭环。

静态的被动式风险防护无法应对复杂的业务场景风险

- 认知有限
- 无法穷举
- 动态变化
- ……

以资产和身份为核心的动态风险治理

资产

1. 定义资产
2. 定义敏感资产

身份

1. 确认你是你
2. 确认你的访问基于真实意图

CSA GCR 6th Congress 第六届云安全联盟大中华区大会

目　录

CONTENTS

数据安全新战法

知

合规认知，根据法律法规对数据安全的要求，整理输出适合本组织的数据安全制度流程和操作指南

理

对数据进行梳理，对敏感数据进行发现定位、分类分级

对风险进行梳理，采集日志，输入风险分析模型，全面了解组织面临的风险，有的放矢

控

全面管控，结合数据分级分类的结果、针对已有风险，采取有针对性的保护措施，对于违规操作做到**发现、预警、拦截**

监

持续监管，汇集安全日志，建设风险预警大屏；

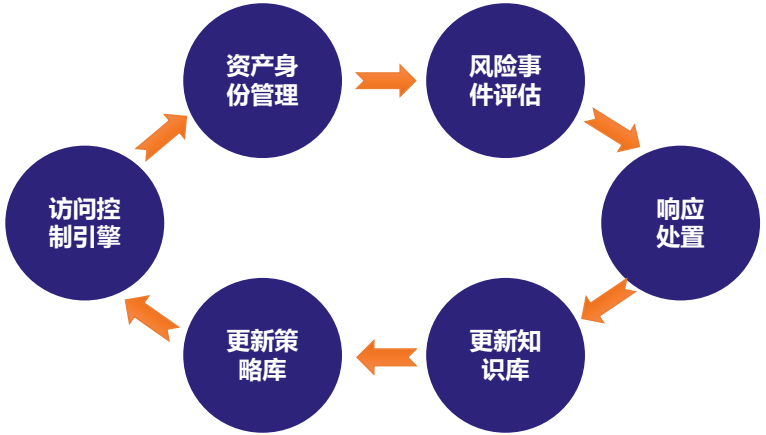
持续改进，结合安全控制点，定期自评，优化安全策略，对安全治理的成果进行持续改进

动态风险治理路径

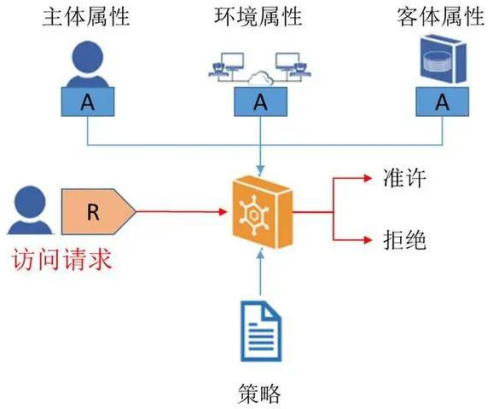
采用动态变化的度量方法，将访问主体的访问行为随着身份信息、访问上下文及环境等因素进行动态评估，对每次访问行为采用最小权限原则执行动态访问控制

解决了传统静态风险治理机制下，安全策略动态适应不足的问题，提升了应对风险有效响应的能力

以资产为中心、以身份为边界、以风险为界面



风险治理-访问控制



访问控制

1. 管理员定义好策略，策略下发到策略引擎
2. 每个资源请求都会经过策略引擎
3. 策略引擎给出一个放行、阻断、脱敏等的响应

定义谁在什么情况下可以访问什么东西，以及不能访问什么东西。必须界定每种可能的语境条件组合，以适应现实世界中不断变化的条件。

风险治理-动态评估

资产、身份动态验证

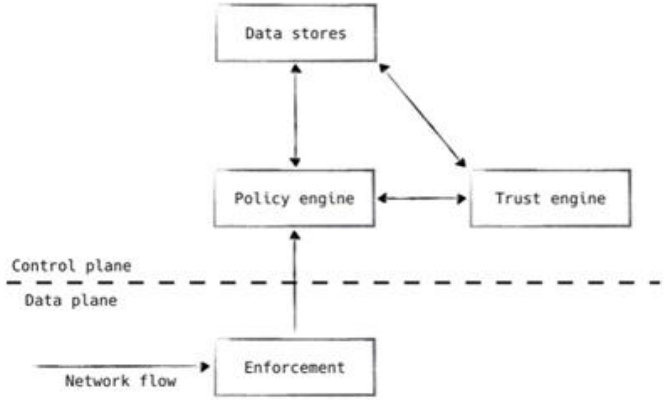
静态属性

- IP地址
- MAX地址
- 设备型号
- 操作系统
- 数字证书
- 应用hash等

动态属性

- 设备上下文
- 网络上下文
- 行为上下文
- 时空上下文
- 操作上下文

风险治理-静态转向动态



信任引擎

1. 信任引擎对请求和活动的风险进行评估，将这些风险评分传递给策略引擎
2. 策略引擎根据具体的策略决定使用哪些评分参与授权决策
3. 信任引擎可以为策略引擎做出正确的访问判断提供有力的支撑。

静态的访问控制（策略引擎）转向动态的控制

风险治理-智能决策

智能分析

资产、身份的行为分析，如时间上下文，空间上下文等，监视上下文信息和活动，预测并建立风险库/策略库。

风险治理-动态体系

动态防护

数据收集、分析完成后，反馈到策略引擎。策略引擎根据风险评分因子，进行动态策略调整，解决弥补策略引擎（访问控制）策略部署难的问题。

风险治理体系化建设

通过统一的数据安全中心构建三大跨域能力

- 适应性动态风险能力，通过策略的适应性进化，让策略能够随着身份和资产的变化而不断进化
- “看见”能力，需要能够看见身份、资产、风险，实现复杂系统的可见性
- 多层级响应能力，包括封闭边界，简单响应，复杂响应，流程干预，应急响应，恢复响应等多个层级的响应能力

CSA GCR 6th Congress 第六届云安全联盟大中华区大会

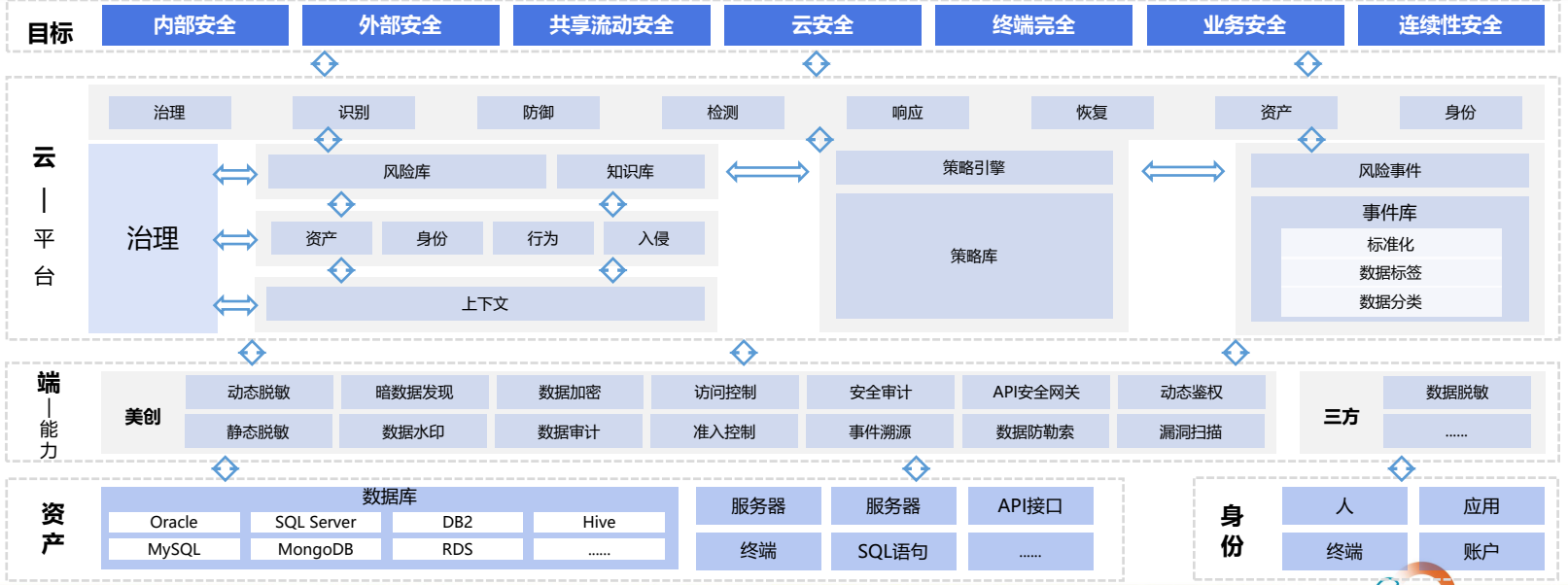
目　录

CONTENTS

新一代安全架构

统一的云中心收敛各种安全业务差异性，云中心展现复杂业务逻辑，轻量级的端点快速适配各种场景；

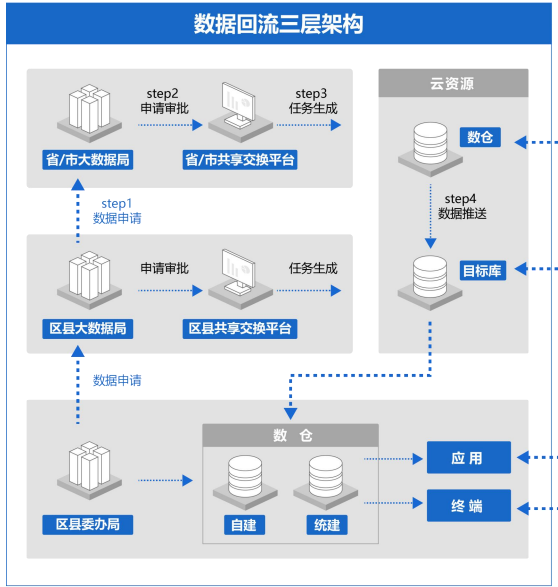
实现统一的资产治理、全域身份、风险模型、安全数据中心、自动化响应 + 轻量级快速扩展的端点

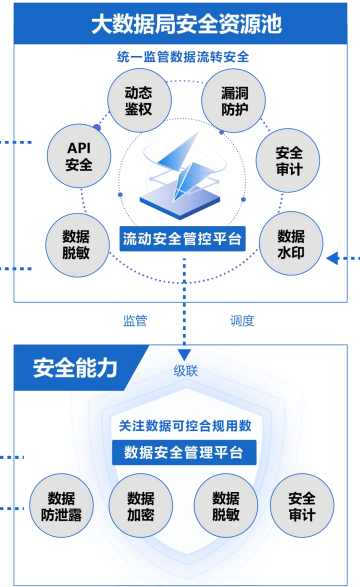


数据流动场景风险治理实践

从数据访问到数据流动的全过程对资产暴露面进行有效管控，并对数据流转链路进行全面的风险监测，精准识别风险并进行有效的响应处置

构建全时全域全面的数据流动风险监测与防护能力，让数据在流动过程中实现现状可知、安全可管、风险可视、事件可溯。





CSA GCR 6th Congress 第六届云安全联盟大中华区大会

CSA GCR cloud security alliance® GREATER CHINA REGION

THANK YOU.