委托式安全代理
在业务应用安全中的实践

岑义涛 | 炼石网络联合创始人

FIT · FREEBUF

业务应用安全是长久以来忽视的问题

FIT · FREEBUF

用户

- 时常抱有侥幸心理
- 业务信息化后内控手段没有跟上
- 过度重视边界防护
- 基础安全水平仍需提升

供应商

- 在安全方面的投入几乎没有
- 缺乏足够的内建安全功能
- 缺乏安全生态与组件供应
- 安全意识水平较低

监管/合规

- 过度重视边界防护
- 对应用的安全功能无约束
- 细则较少，罚则较轻

企业面临巨大压力

- 《中华人民共和国网络安全法》
- 《关键信息基础设施安全保护条例（征求意见稿）》
- 《中华人民共和国密码法（草案征求意见稿）》

“中国安全市场的两大驱动力”

“合规从被动变主动”

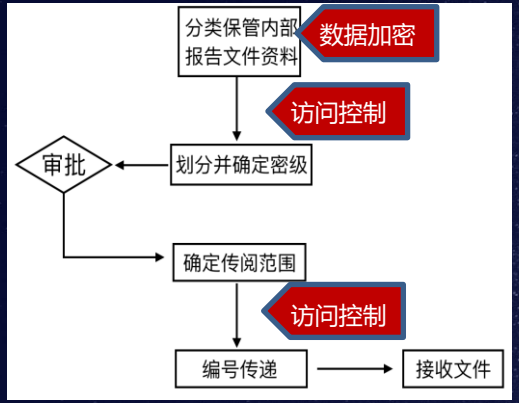
“商业秘密保护是必须”

应用系统的复杂性让企业面临更严峻的挑战

FIT · FREEBUF

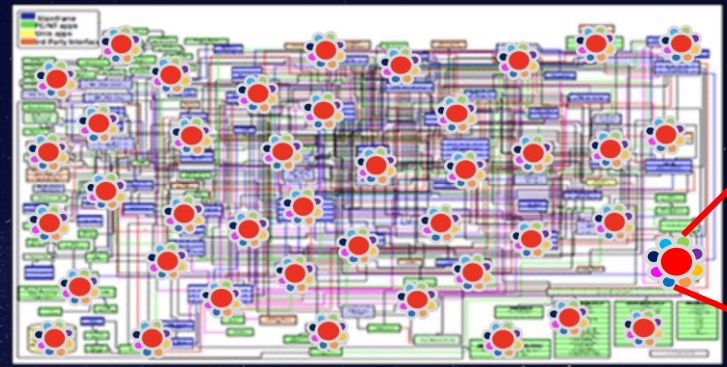
《企业内部控制应用指引》

- 内部报告形成及控制流程



商业秘密保护的大部分要求对应于应用的功能型安全需求：

- 功能型安全需求需要在系统中融合实现，但是升级系统成本高、风险大、难以实施。
- 商业秘密保护长期得不到落实，不仅会导致合规风险越来越大，而且企业业务因商业秘密泄露而导致的业务风险也会快速累积。



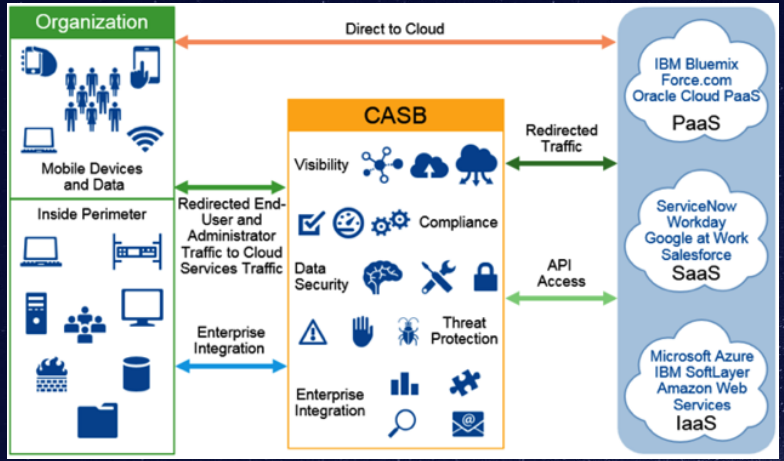
产业创新俱乐部

进行系统改造的方案没有可实施性

- 已有应用系统升级涉及面广
- 开发周期长
- 承担较大风险
- 失去维护的系统甚至缺失源代码

- 已上线的系统升级成本更高
- 重新部署上线，有业务中断风险
- 间接造成业务损失的风险

应对这种挑战的可借鉴技术模式



Source：Gartner (May 2015)

Cloud access security brokers (CASBs) are on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed.

为什么是CASB?

云（SaaS）的普及打破了传统的安全防护方法

- 用户无法控制SaaS中的数据
- 当时没有安全方案能够满足需求

通过Broker技术把传统安全技术“塞进”了SaaS中

- 没有新创安全技术
- 不影响用户体验，不改造服务端
- 让安全控制手段进入到了业务流程中

炼石利用CASB做了什么?

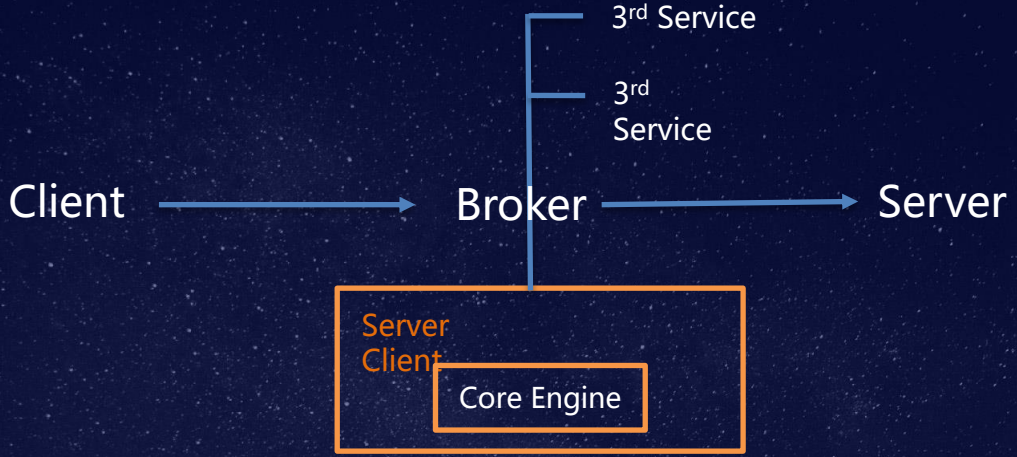
从云到本地

- Cloud Access Security Broker
  - CRM/Box/Collaboration/Office
- Critical Application Security Broker
  - ERP/PLM/OA/MES/NFS/CIFS

Broker Engine

- 一次适配，打开无限可能
- 再造业务应用的安全功能
- 支撑面向集成商的适配平台，大幅降低门槛和工作量

委托式安全代理（Broker）的技术模型



与Proxy的区别：

- Inter-Request
- 充分还原上下文
- 可以根据需求（策略），调用外部服务（认证服务、反病毒、外部系统）

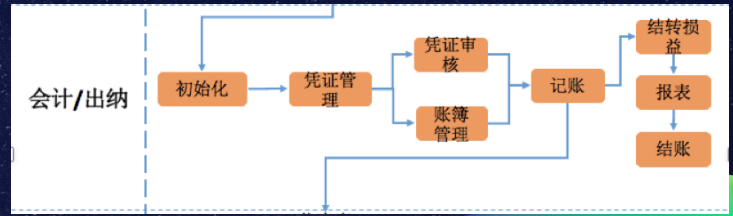
独家可以适配进业务流程的安全方案

强制认证：

- 免改造继承与接管原有认证机制

访问控制：

- 基于属性和角色的访问控制；



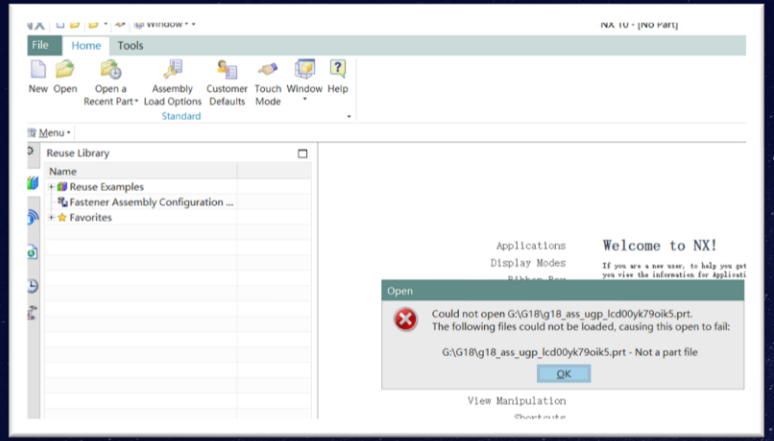
数据加密：

- 与访问控制体系结合，形成无法绕过的安全锚点；

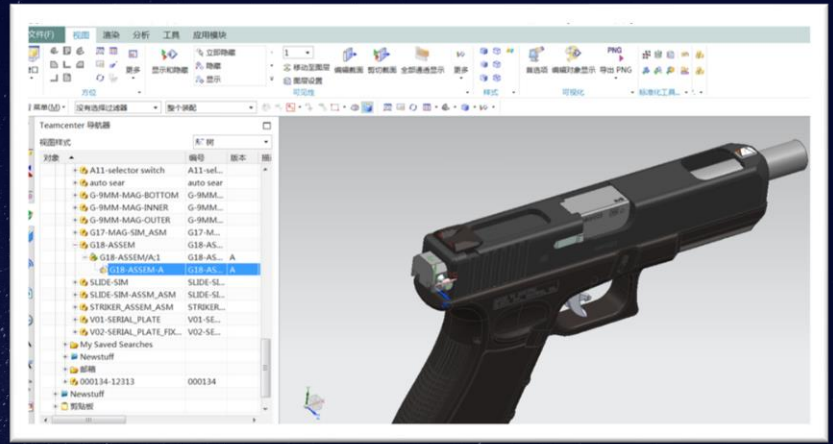
行为监控：

- 可定责的日志防篡改审计

CipherGateway的实现效果

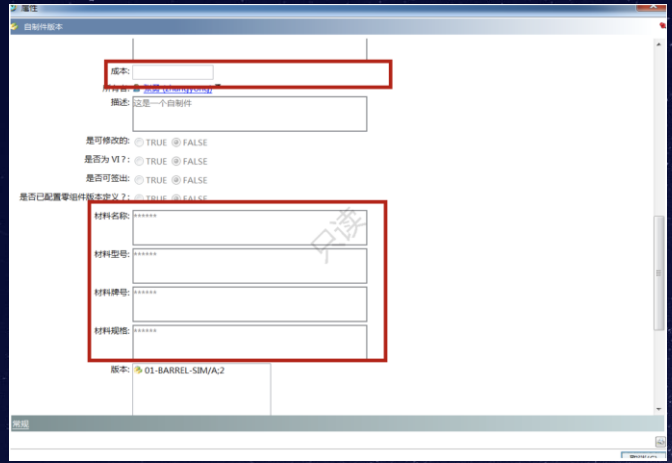


加密后数模文件无法直接打开

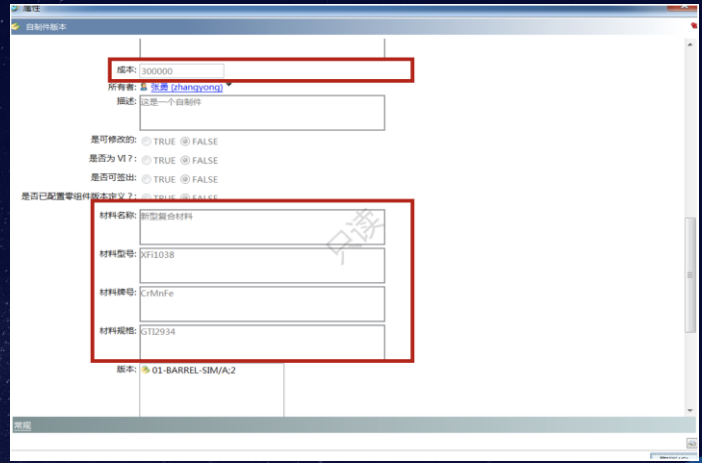


有权限的用户可以打开数模

CipherGateway的实现效果

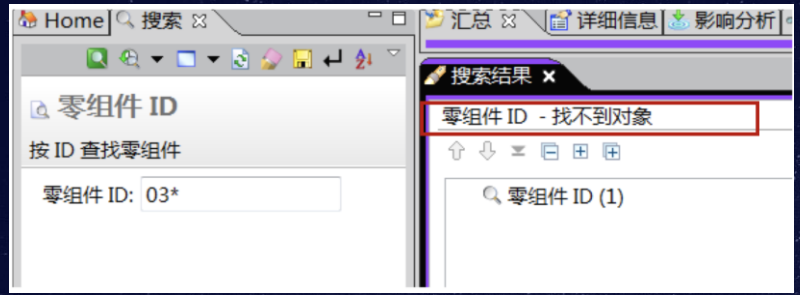


低权限用户不能查看敏感属性信息

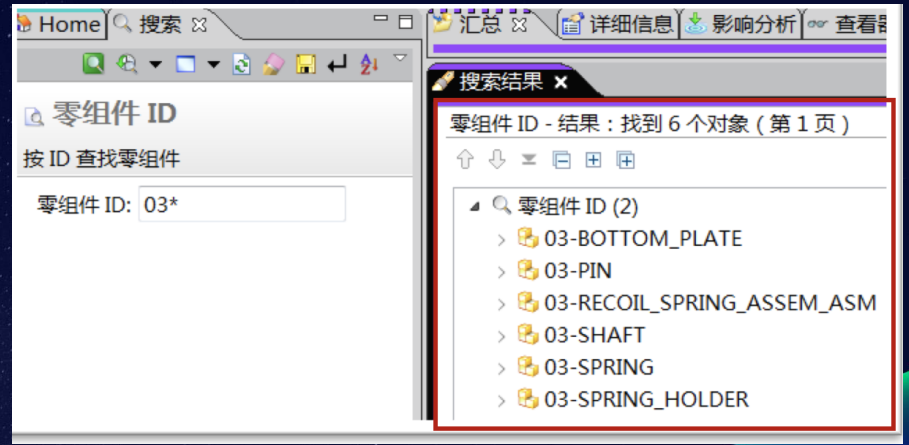


高权限用户能够查看敏感属性信息

CipherGateway的实现效果

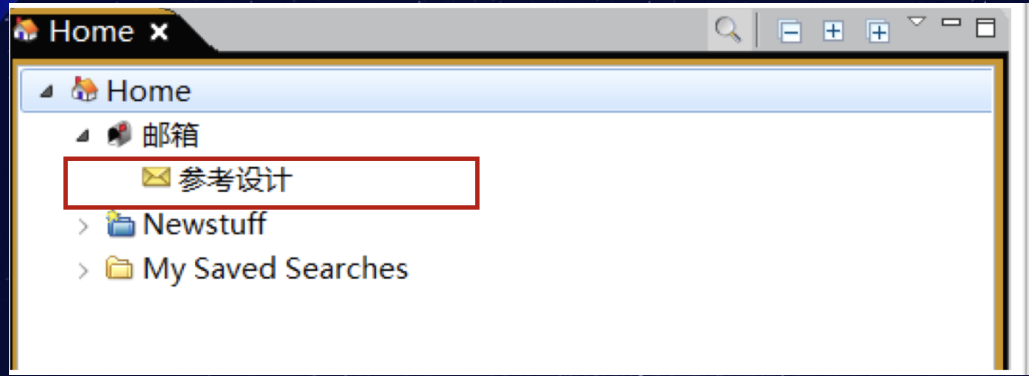


未授权用户无法搜索到限制数据

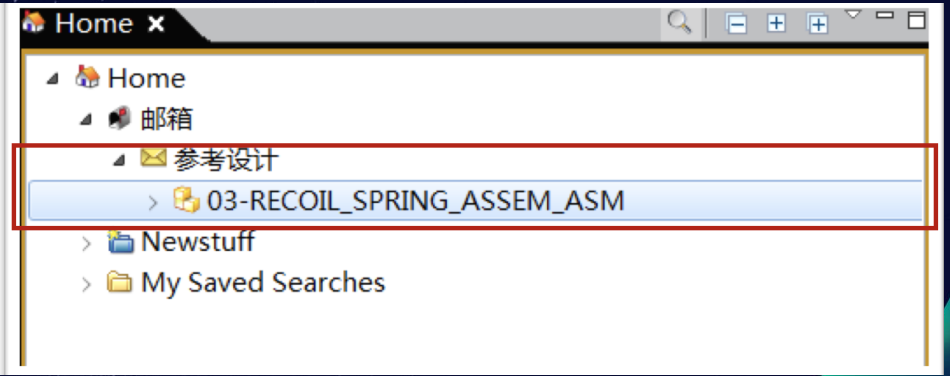


有权限用户可搜索到限制数据

CipherGateway的实现效果

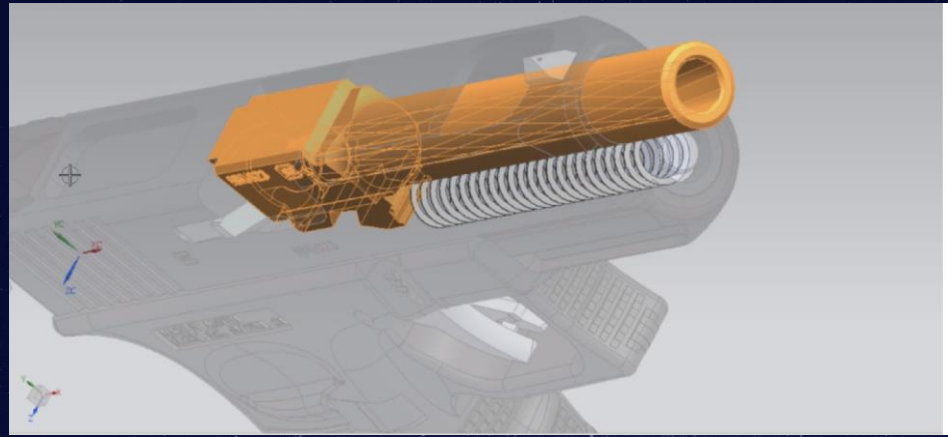


未授权用户无法收到限制数据

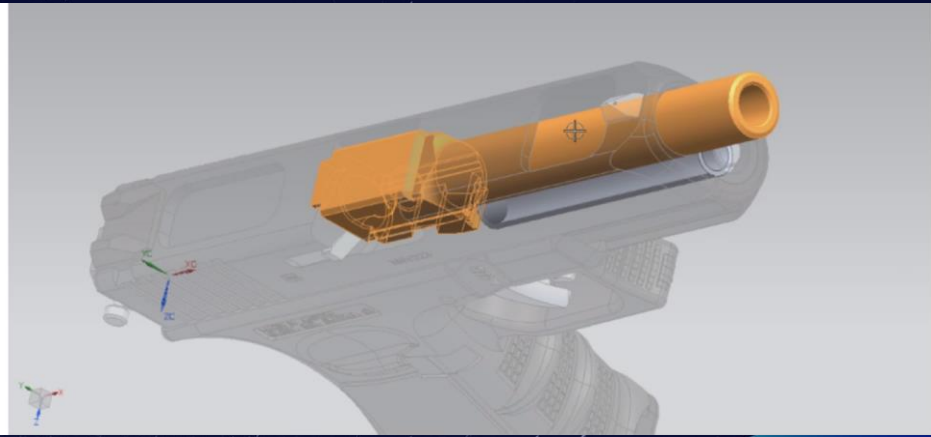


有权限用户可正常收到限制数据

CipherGateway的实现效果



脱敏前数模



脱敏后数模