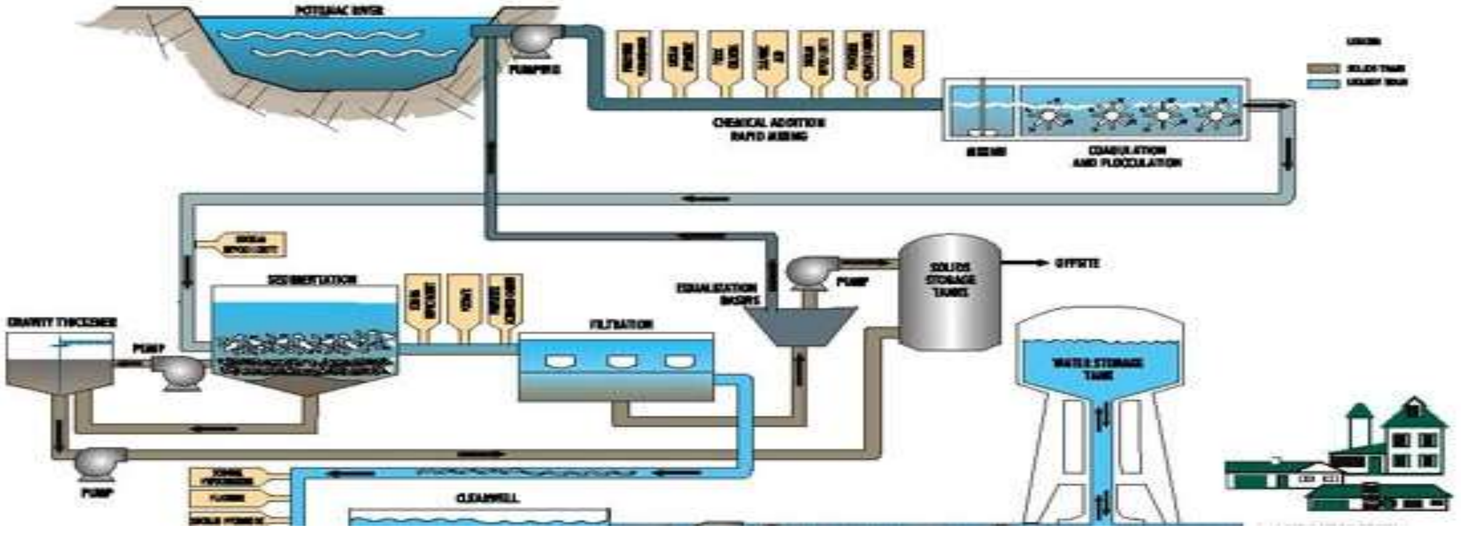
CASB保护使用中的数据安全实践

演讲人：炼石网络CEO 白小勇


POTOMAC RIVER
PUMPHOUSE
CHEMICAL ADDITION
RAPID MIXING
COAGULATION
AND FLOCCULATION
SEDIMENTATION
FILTRATION
EQUALIZATION
BASINS
PUMP
SOLIDS
STORAGE
TANKS
OFFSITE
GRAVITY THICKENER
PUMP
PUMP
WATER STORAGE
TANK
CLEARWELL

数字化时代的安全趋势

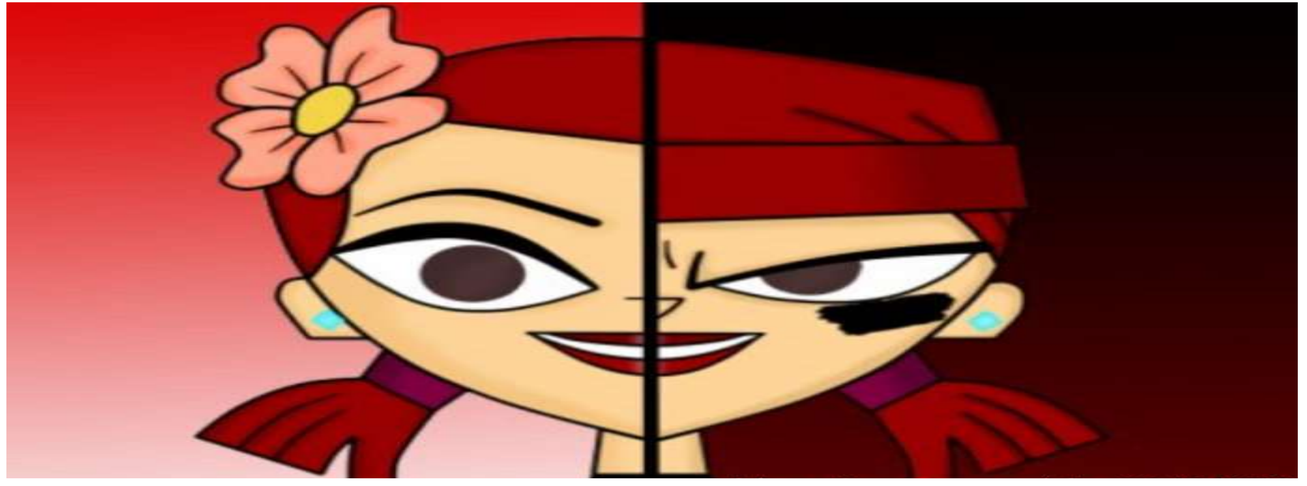
数据安全被提升到新的高度

- 数据成为企业的生产资料，是数字化时代的黄金、石油
- 高价值使数据成为更加明确的攻击目标
- 重要数据关乎企业的核心业务风险

传统安全手段失效

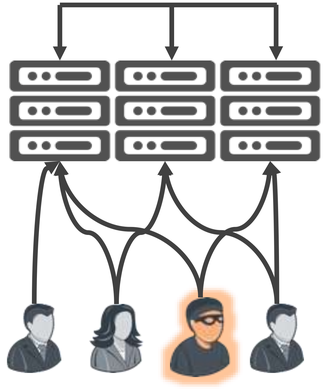
- 一切都可能被入侵/控制
- 无法简单区分是“好的”还是“坏的”
- 单纯的一次性阻断/允许策略已经没有意义

真坏人不可怕，可怕的是假好人

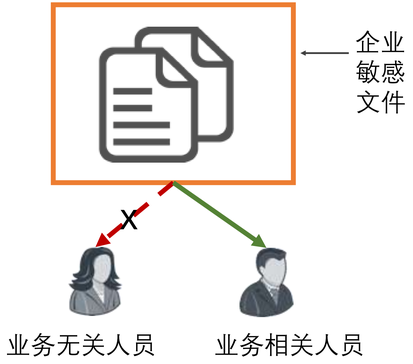


高价值数据共享与安全保密的“两难”

- 高价值数据在信息系统中流转和共享，是刚需
- 好人坏人难辨的情况下仍需要依靠信息系统进行业务发展



VS



- 传统数据安全手段面向文档文件，或数据库，或磁盘卷，要么脱离业务含义，要么粒度较粗
- 面对如今复杂的多人协同场景，单纯的阻断会影响业务效率，而允许会造成安全疏漏

企业要具备对风险和信任持续评估及改进的能力

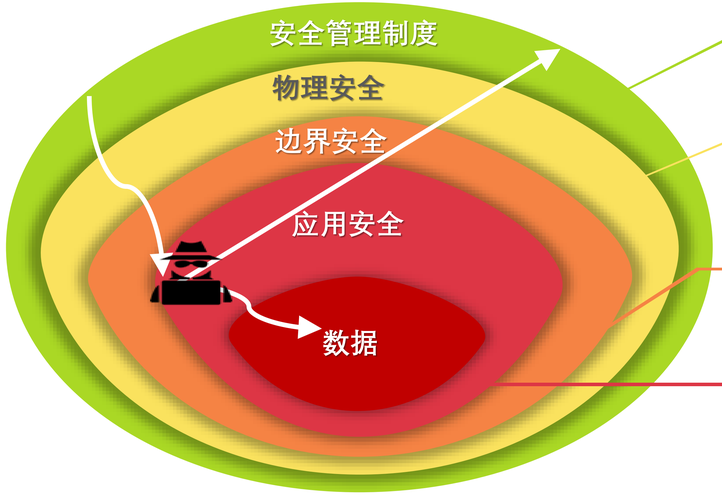
数字化企业不再直接掌控系统、设备与用户之间的交互和信息处理，传统手段难以分辨“好坏”。

对于数字化企业，风险和是否信任不再是yes or no，而是动态的，随着业务场景持续变化的。

所有系统和设备都必须认为存在被入侵/控制的可能，因此需要被持续进行风险和信任度评估。

评估信任所需的数据来源于用户与系统的交互上下文。只有获得足够的信任，用户才能完成请求的操作/数据。

经典的围墙式防护模型中，缺失数据上下文



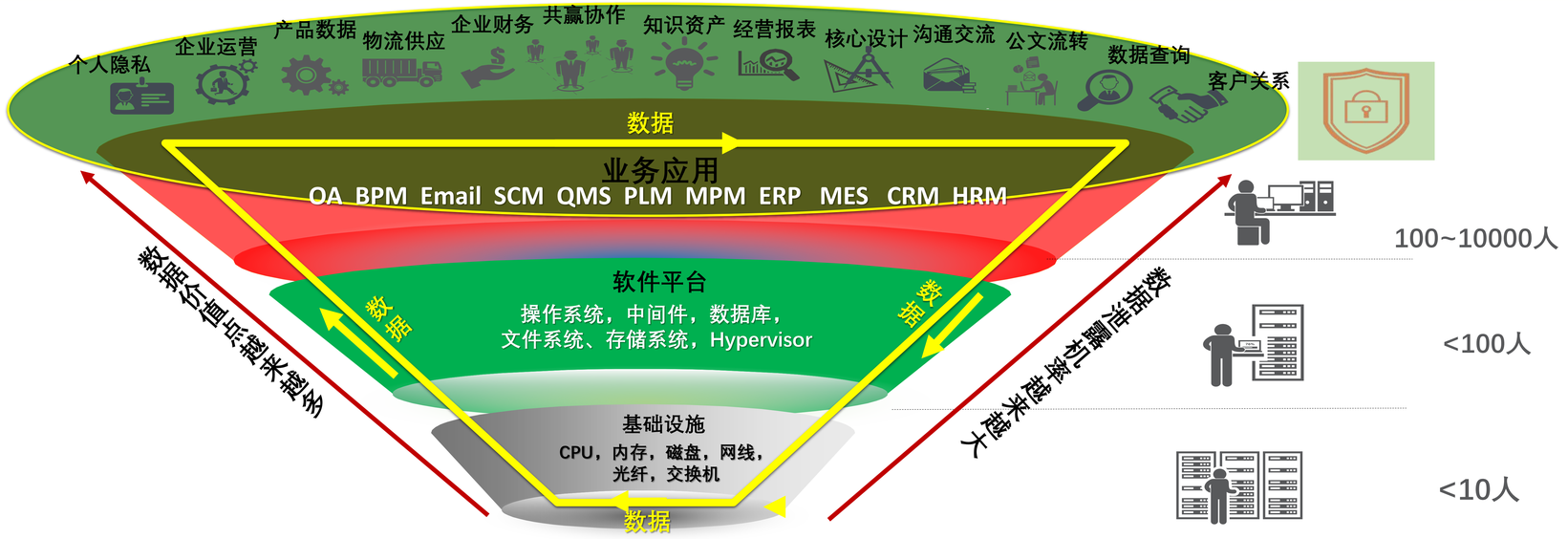
企业制定专门的信息安全保密管理制度，定级定密，定期对员工开展培训和检查，提高信息安全意识

企业成立专门的安全保卫部门，保护重要信息设备设施的安全

企业实施专业的边界安全防护措施，物理隔离，防火墙、IDS/IPS、反病毒等一应俱全

应用系统均采用权限访问控制机制，具备日志审计功能

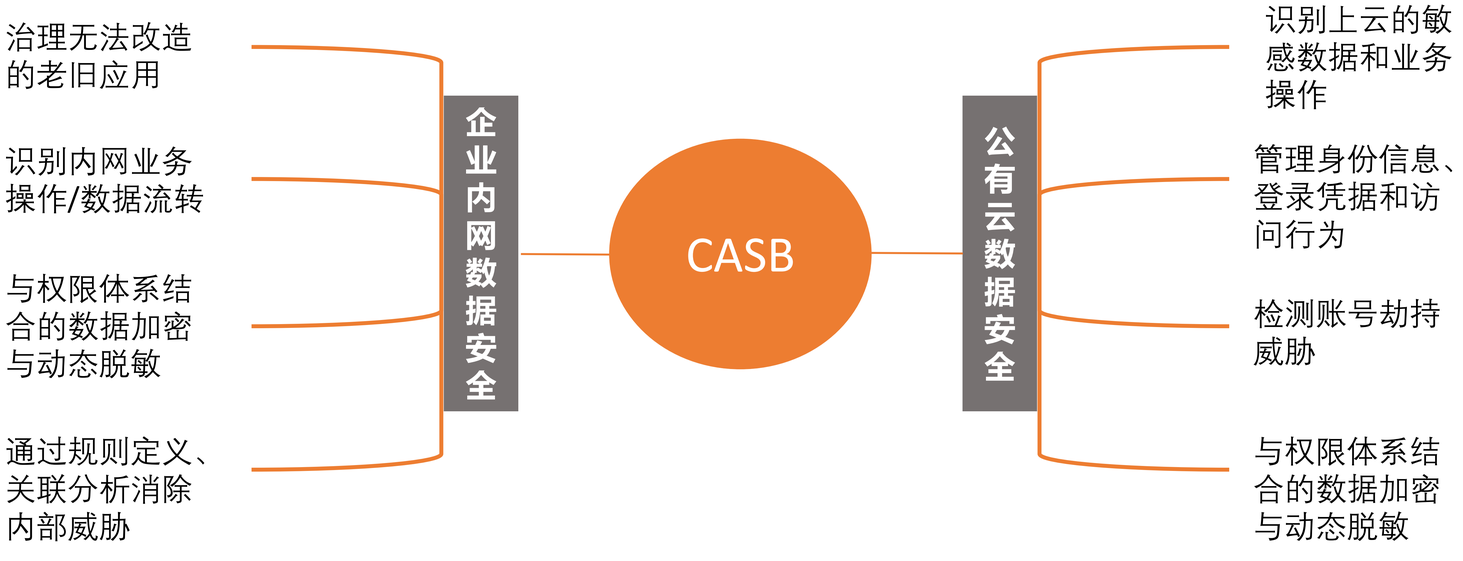
数据在信息化系统中的不同层次持续流转



用CASB保护使用中的数据安全

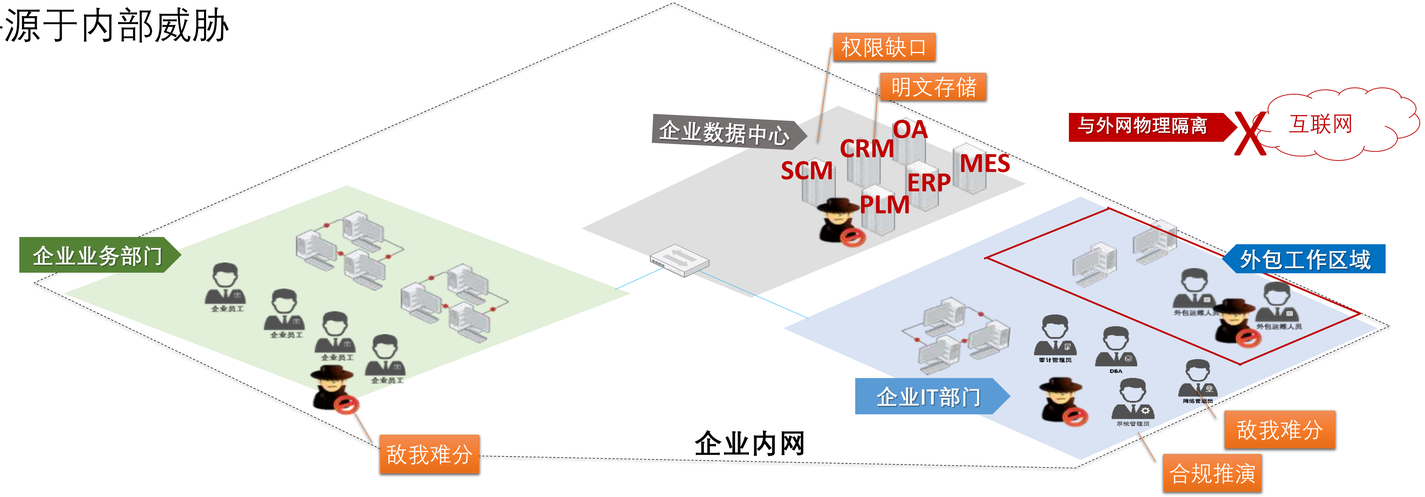
云访问安全代理
CASB（Cloud Access Security Broker）& CASB（Critical Application Security Broker）关键应用安全代理
将数据安全能力作用到持续变化的数据使用场景和业务流程中

CASB的主要应用场景

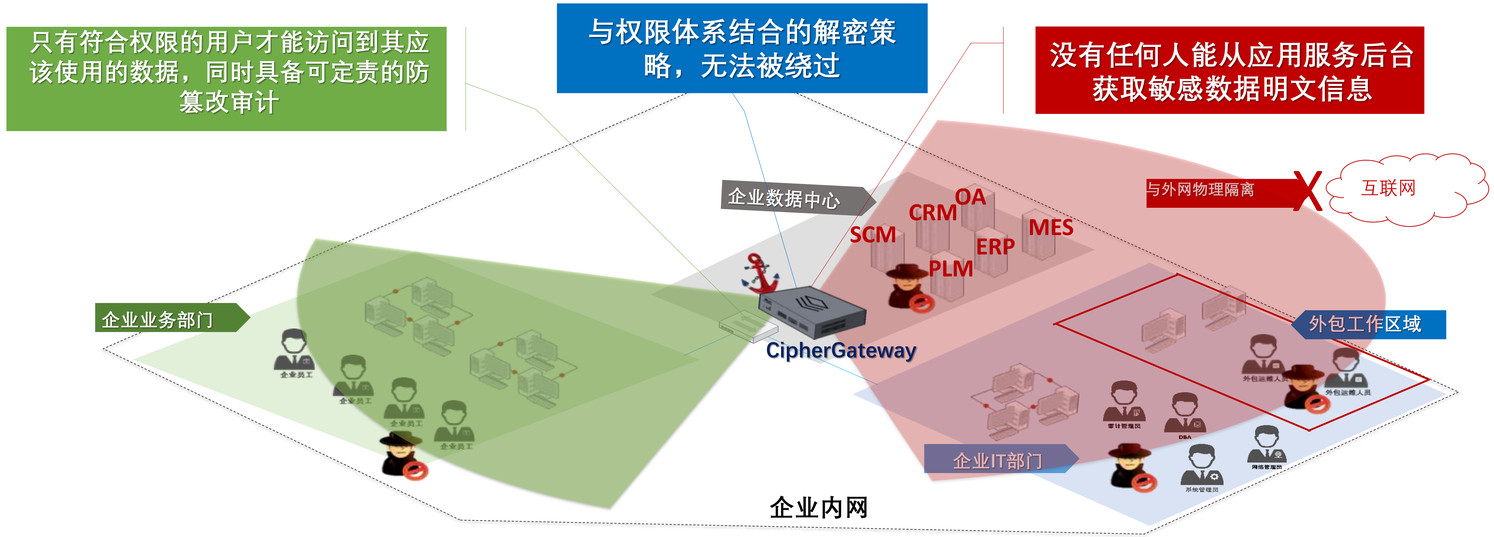


内部威胁客观存在

* 70%以上的安全事件源于内部威胁



提供以数据为抓手的零信任安全架构



实践1—CASB保护装备研发流程中的数据安全

某研究所承担一款制式手枪的性能升级项目，由于要求指标高于所有外军已知同类型武器，并且首次采用了**新工艺、新材料**，因此对保密要求十分严格较高。

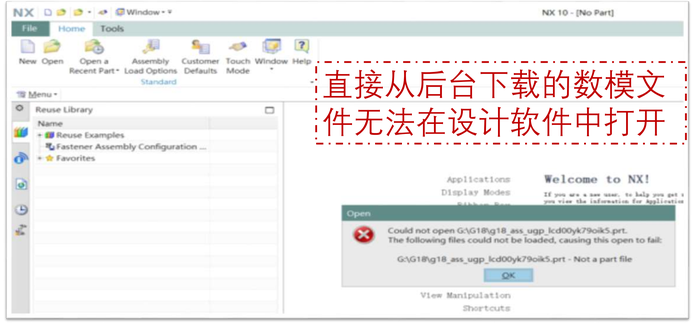
此次型号改型升级的重点在于**核心组件设计**（枪管组件与复进簧组件）及其使用的**新型材料**，相关重要敏感数据包括：

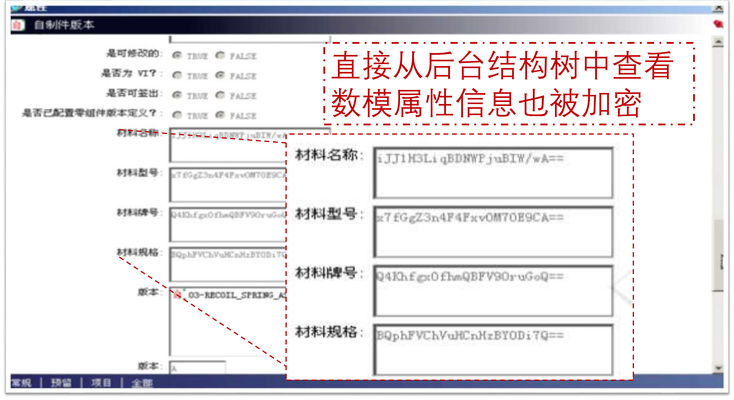
✓敏感组件的**设计图纸数据（三维数模）**，涉及到的组件为枪管组件和复进簧组件。

✓敏感组件及**其子件的描述**、材料、供应商的属性信息。

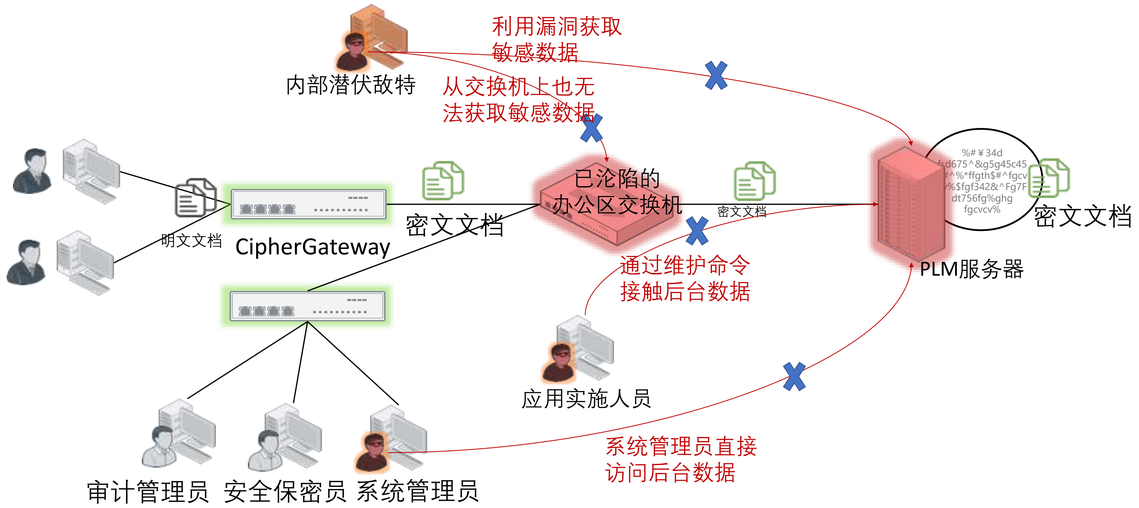
项目组使用 SIEMENS TEAMCENTER 作为协同工作平台

1) 为PLM赋予数据加密能力



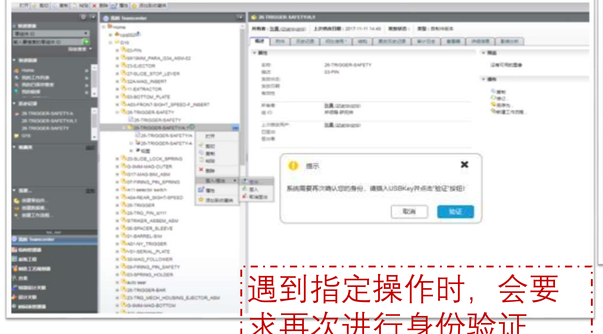


无法直接从后台获取敏感数据



IT运维、外包实施、管理员、
内部恶意人员、被控制主机、
特木等人员和手段
均无法直接从后台获取敏感数据

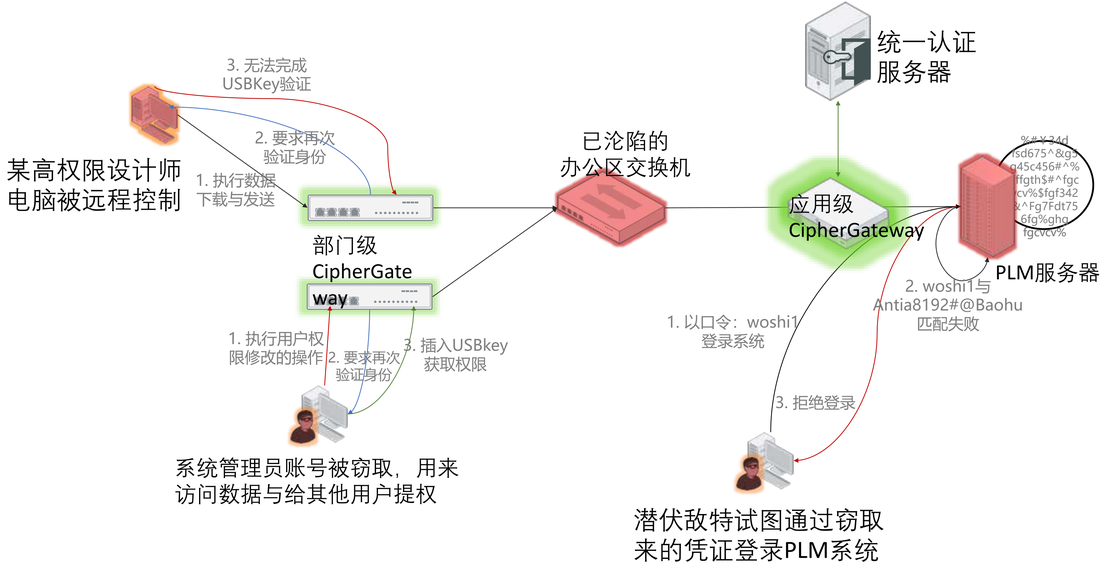
2) 杜绝关键操作时身份被冒用



遇到指定操作时，会要求再次进行身份验证

CipherGateway会自动将用户口令替换成复杂长密码

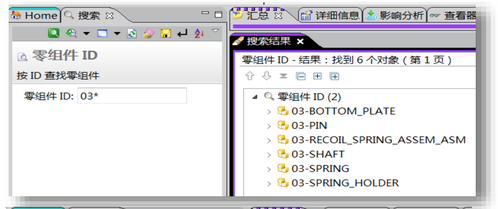
增强关键业务操作和数据使用的身份确定



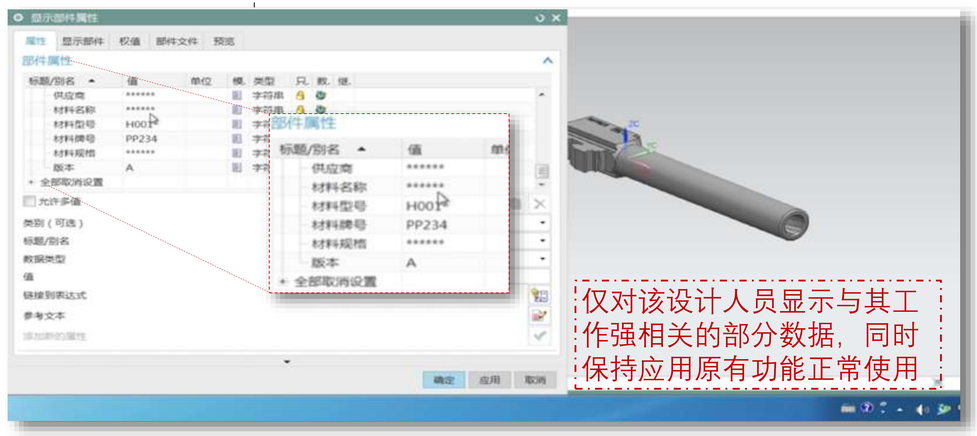
防止身份被冒用，确保操作为用户本人执行：

- 不通过部门级CipherGateway无法正确验证登录凭证
- 关键流程节点：敏感操作/异常操作需要再次进行强身份认证

3) 参与人员只能访问其业务相关数据

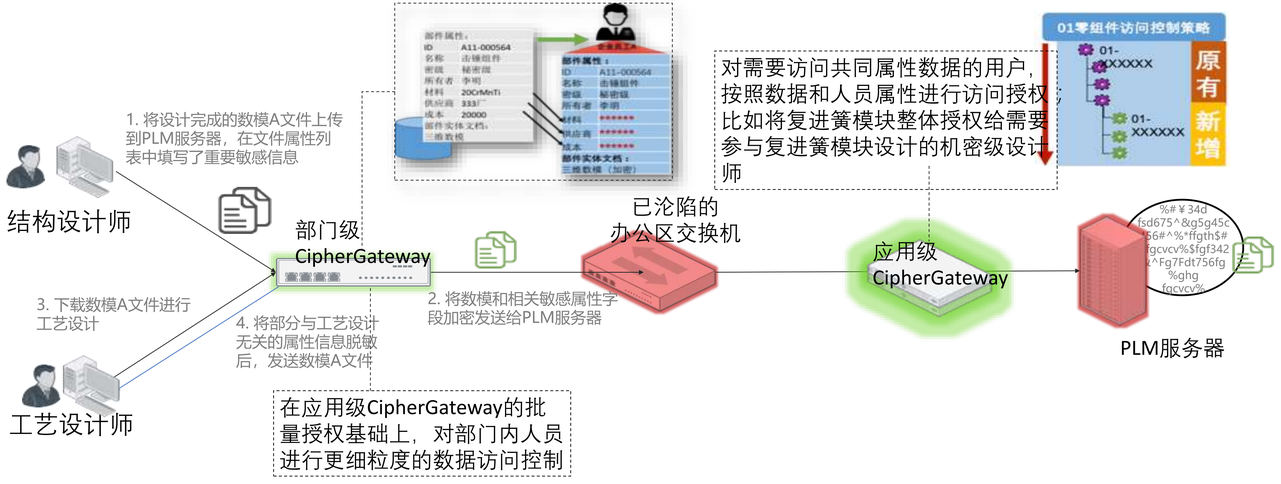


带有业务含义访问控制策略，让一条策略能作用众多零组件，且零组件关系变化时自动执行有效控制。



仅对该设计人员显示与其工作强相关的部分数据，同时保持应用原有功能正常使用

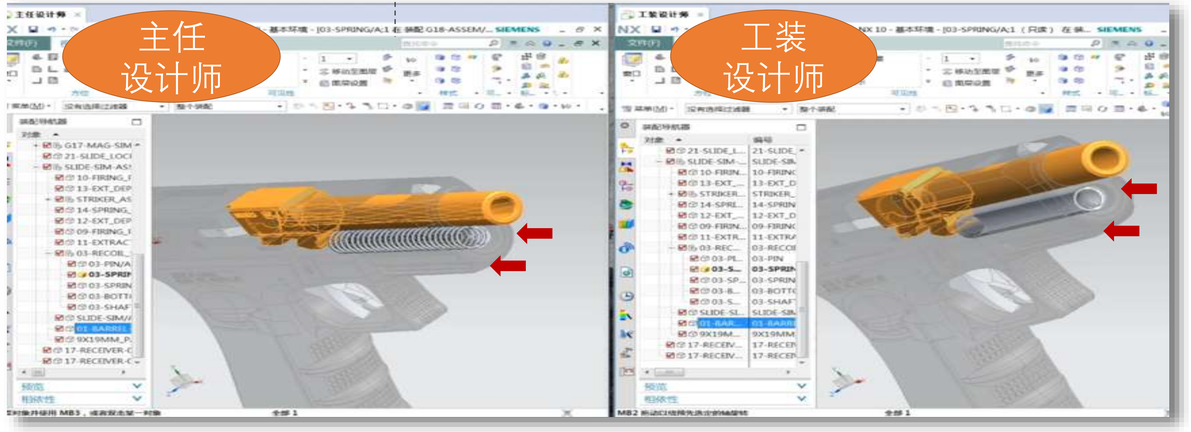
在复杂数据结构中最小化数据访问授权



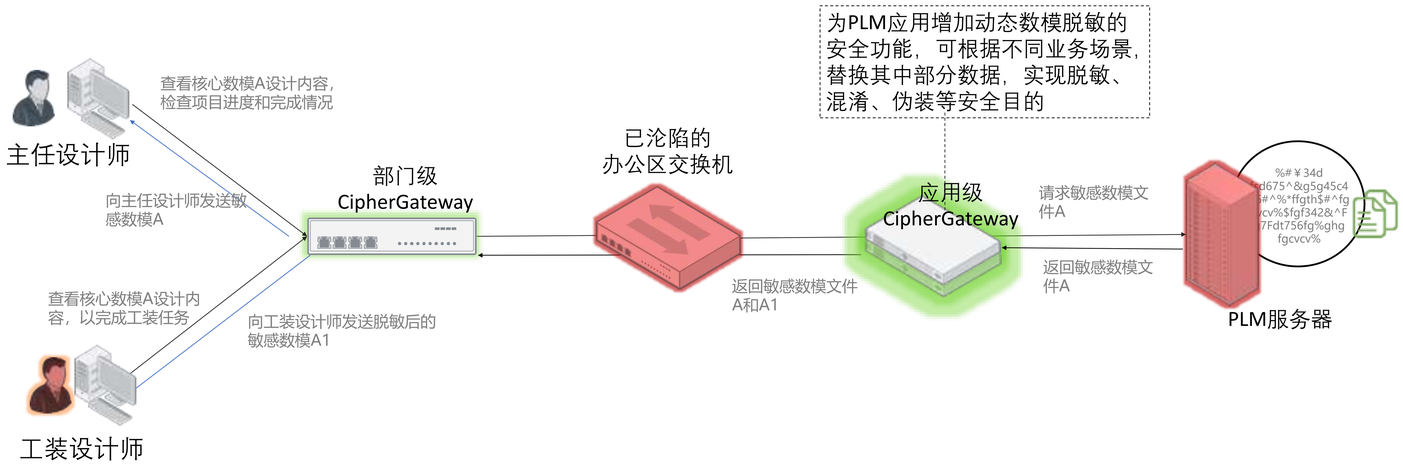
- 基于人员属性、环境属性和数据属性进行灵活精细的访问控制；
- 做到给确定有业务关系的人解密数据；
- 减小敏感数据暴露的风险；
- 降低了策略配置复杂度、使得权限可以动态继承；
- 对数据的访问控制配置快速，提升安全事件的响应能力

4) 深度结合数据使用的脱敏机制

基于人员权限和策略，对没有权限的人进行定向脱敏，对“内鬼”或潜伏在内部的敌特人员，提供欺骗数据

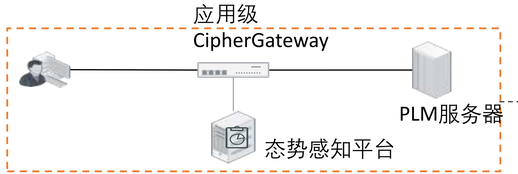


最小化敏感数据阅读范围，迷惑恶意人员



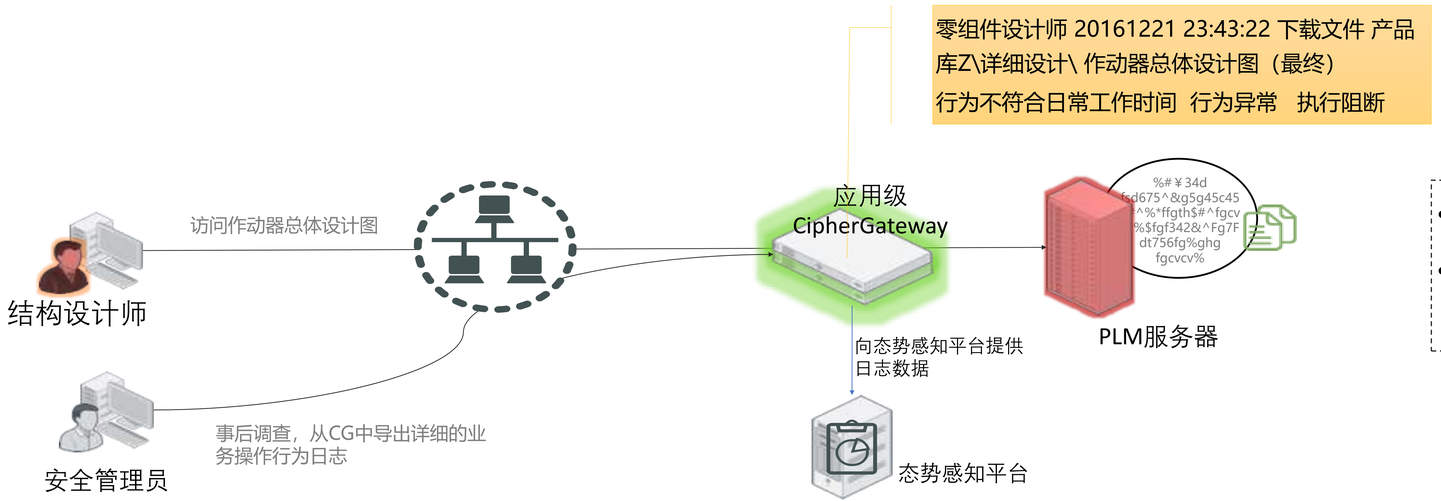
- 根据数据使用人员的权限、工作内容差异，定向脱敏核心数据；
- 对于不应该看到数据却需要数据来工作的员工，仅开放其权限内的数据，或给部分假数据；
- 降低大型项目数据泄露的风险；
- 同时可以针对性投放高仿真欺骗数据，迷惑潜伏敌特；

5) 细致的行为审计



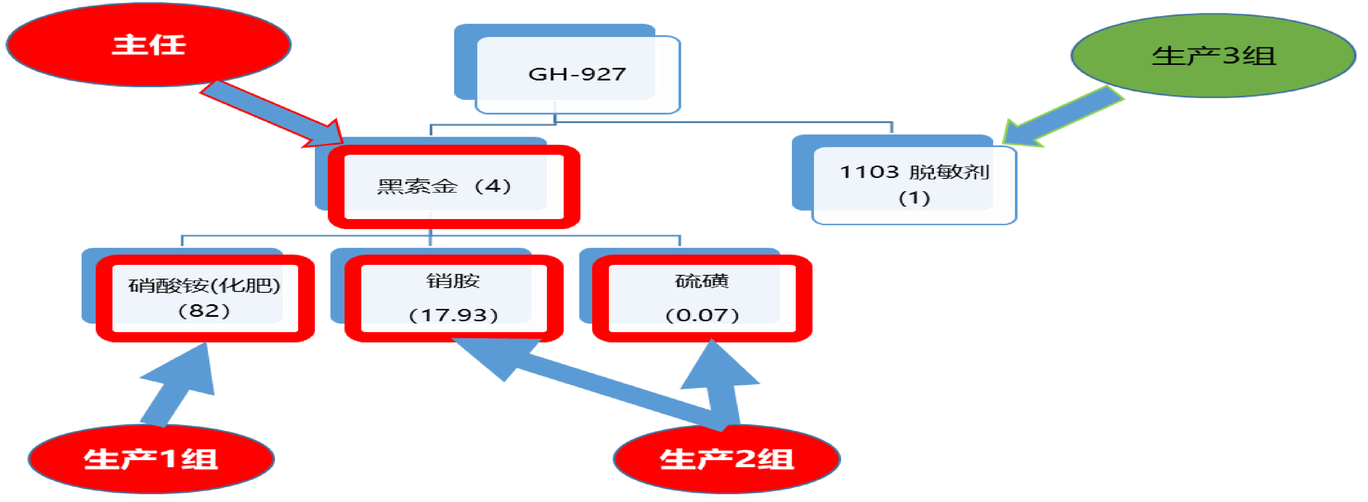
面向业务操作的细致行为审计
配合逐条日志签名，确保业务操作的真实性、不可抵赖性

辅助业务人员进行事后取证与定责

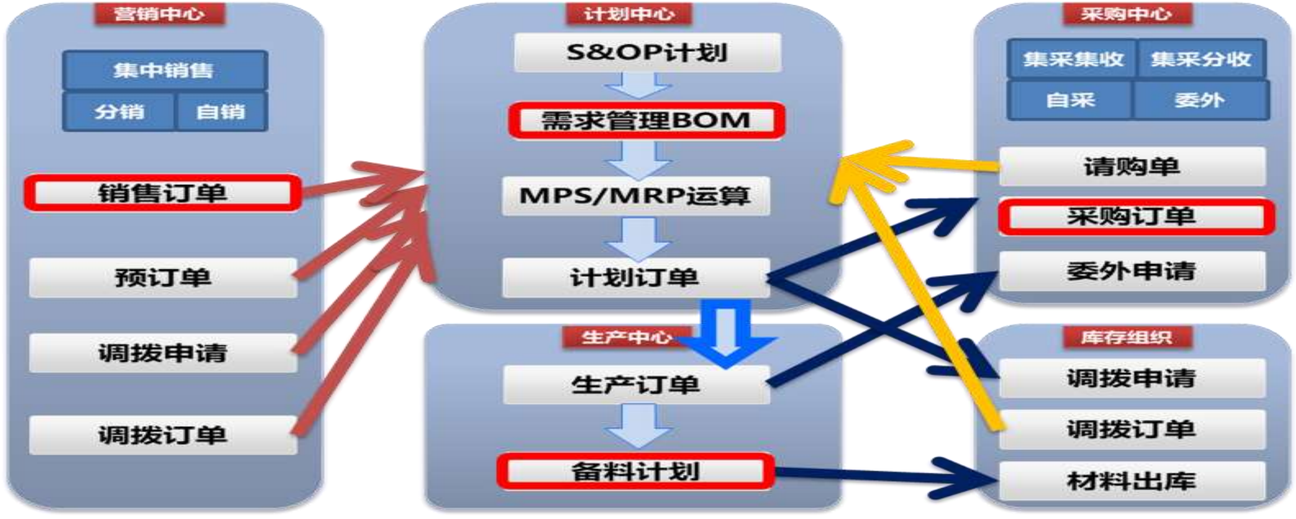


- 辅助事后调查、取证和追溯定责；
- 作为业务语言的安全日志内容输出给态势感知平台，提升整体分析、预警能力;

实践2—CASB保护ERP流程中的配方数据安全

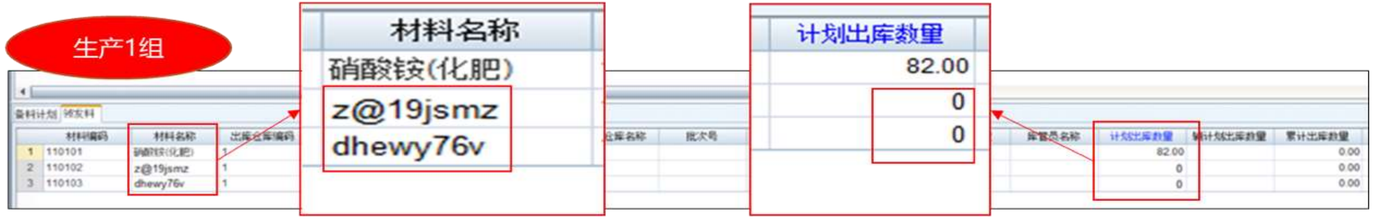


业务流程与核心关键点

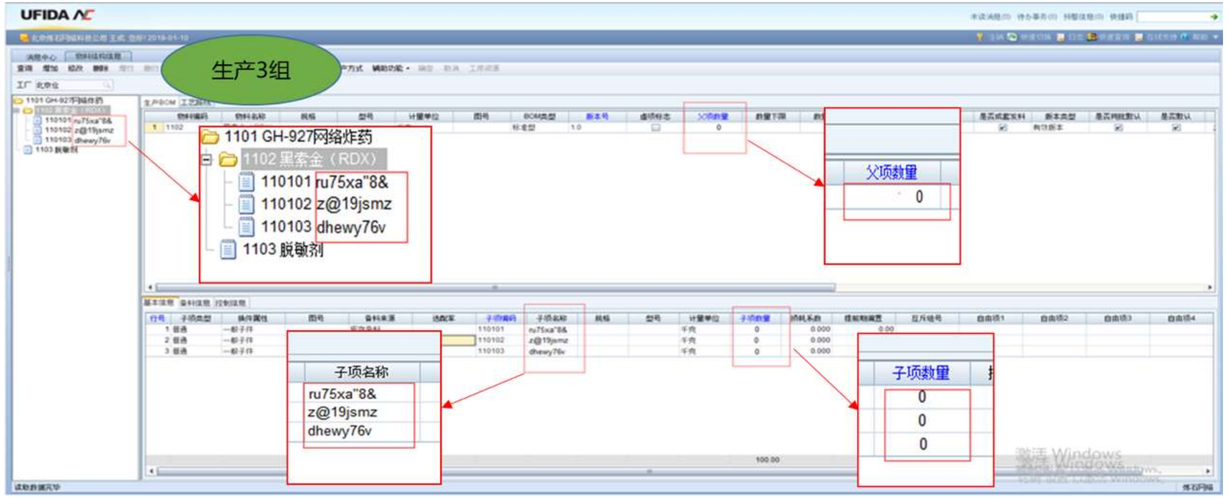

营销中心
集中销售
分销
自销
销售订单
预订单
调拨申请
调拨订单
计划中心
S&OP计划
需求管理BOM
MPS/MRP运算
计划订单
生产中心
生产订单
备料计划
采购中心
集采集收
集采分收
自采
委外
请购单
采购订单
委外申请
库存组织
调拨申请
调拨订单
材料出库

相同单据互斥角色看到不同材料内容

- “黑索金”秘方生产过程中分为生产1组和生产2组，1组负责硝酸铵(化肥)， 2组负责硝铵和硫磺。
- 避免同一组人根据物料出库情况推测出配方构成。



不参与关键配方的用户只能看到密文



* 不涉密情况说明：本文档的制式手枪数模、黑索金炸药配方等数据，均从互联网公开数据搜索。

使用中的数据安全

使用中的数据安全，就是在企业关键信息化应用中，

将加密和细控能力适配进业务流程，输出有效的数据安全防护价值。

关于炼石

炼石
CipherGateway

可以适配进业务流程的数据安全

- 创始团队具有丰富的应用开发、安全、和密码学背景与从业经验；
- 解决方案顾问团队在大型企业应用领域具有15年以上从业经验；
- 独立信息安全研究实验室CGLab；

- 把安全融入应用
- 构筑应用安全生态，保障企业业务发展

- CipherGateway业务应用安全网关
- CipherSuite密码套件

THANKS