



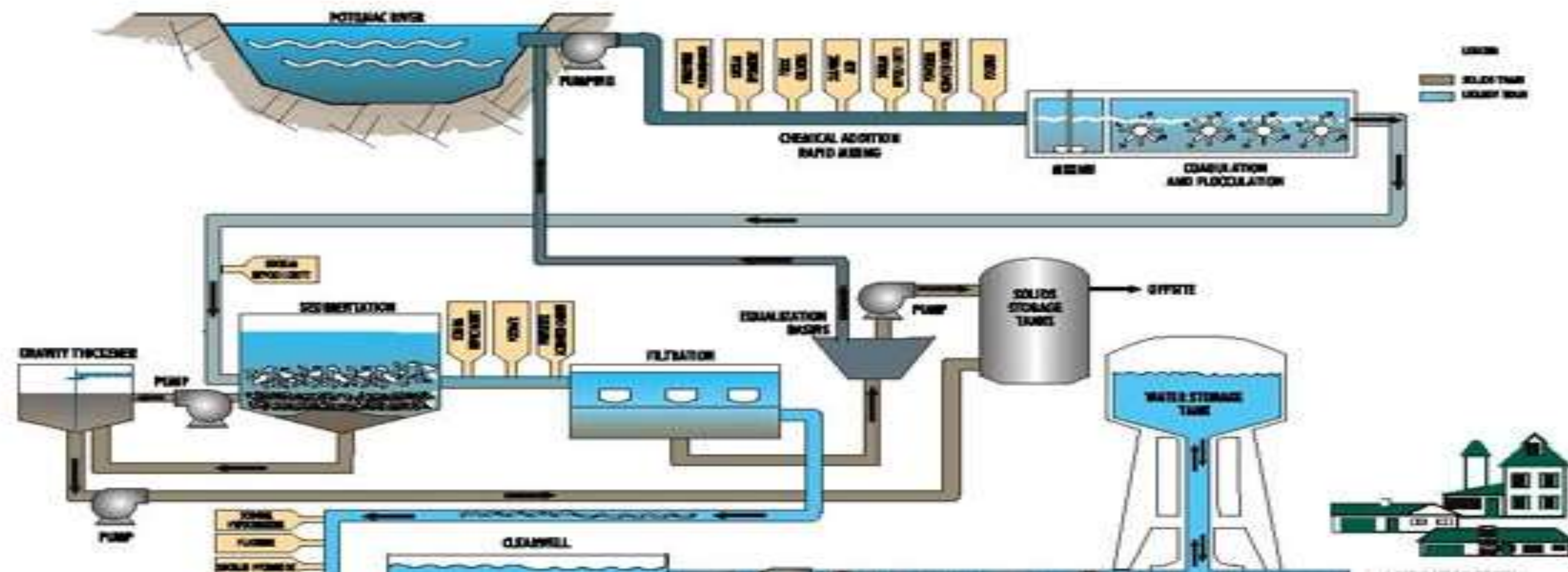
# CASB保护使用中的数据安全实践

演讲人：炼石网络CEO 白小勇





# 第二届中国数据安全治理 高峰论坛2018







# 数字化时代的安全趋势

第二届中国数据安全治理  
高峰论坛**2018**

## 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

第二届中国数据安全治理  
高峰论坛2018



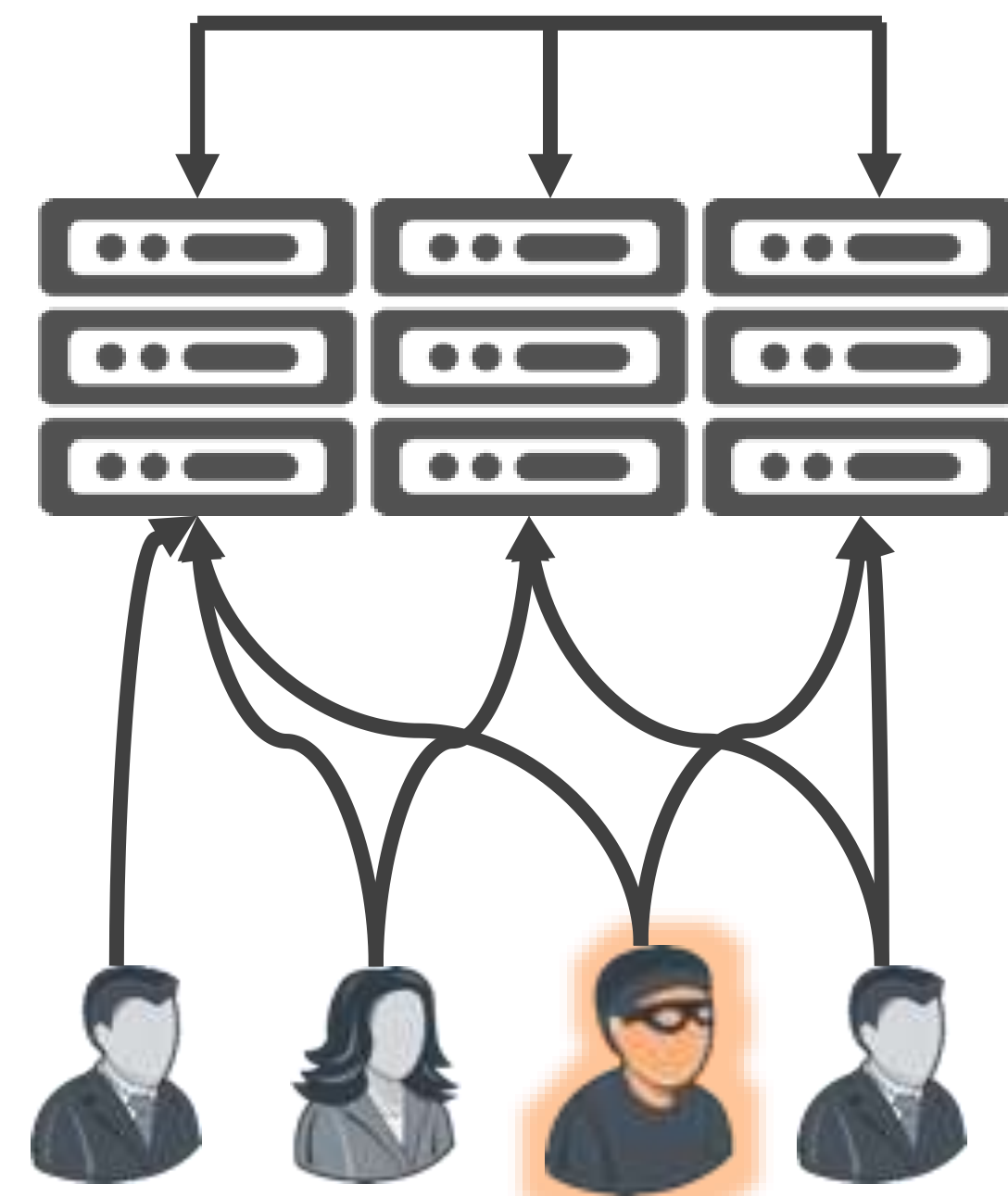




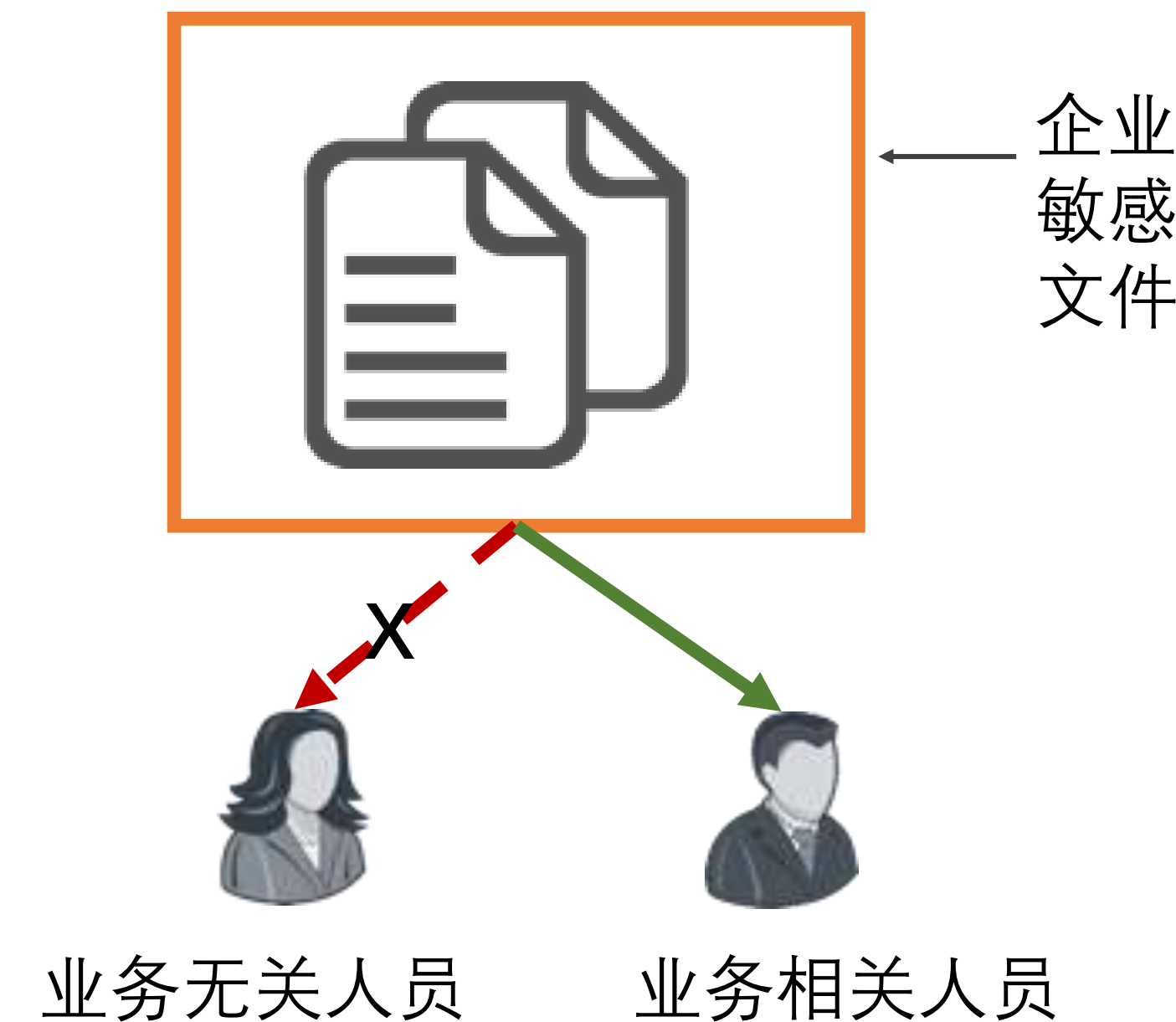
# 高价值数据共享与安全保密的“两难”

第二届中国数据安全治理  
高峰论坛2018

- 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

第二届中国数据安全治理  
高峰论坛2018



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。



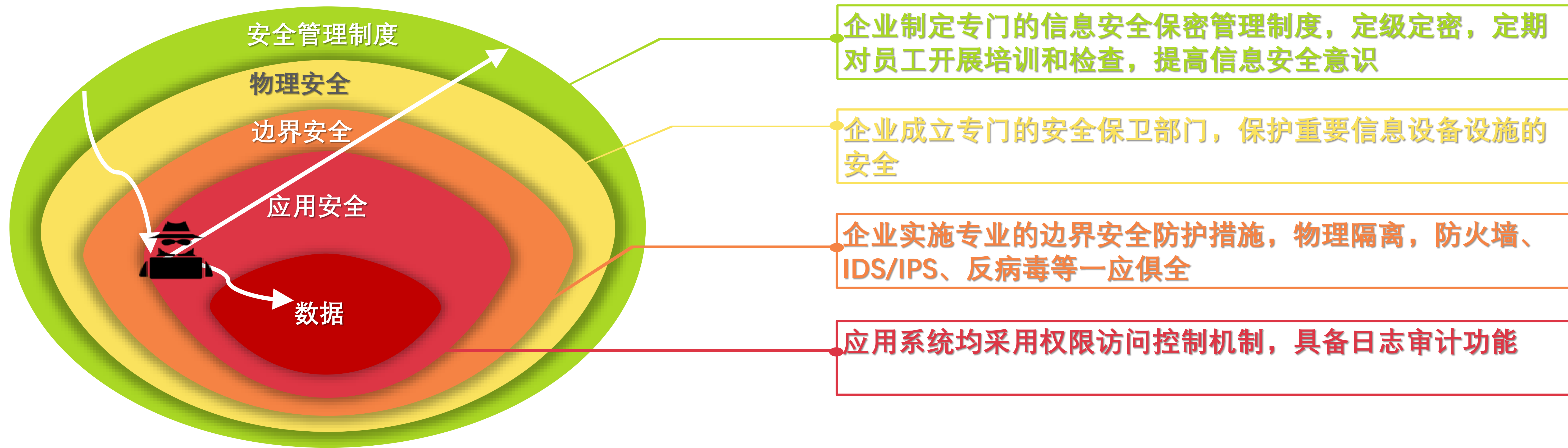
评估信任所需的数据来源于用户与系统的交互上下文。只有获得足够的信任，用户才能完成请求的操作/数据。





# 经典的围墙式防护模型中，缺失数据上下文

第二届中国数据安全治理  
高峰论坛2018

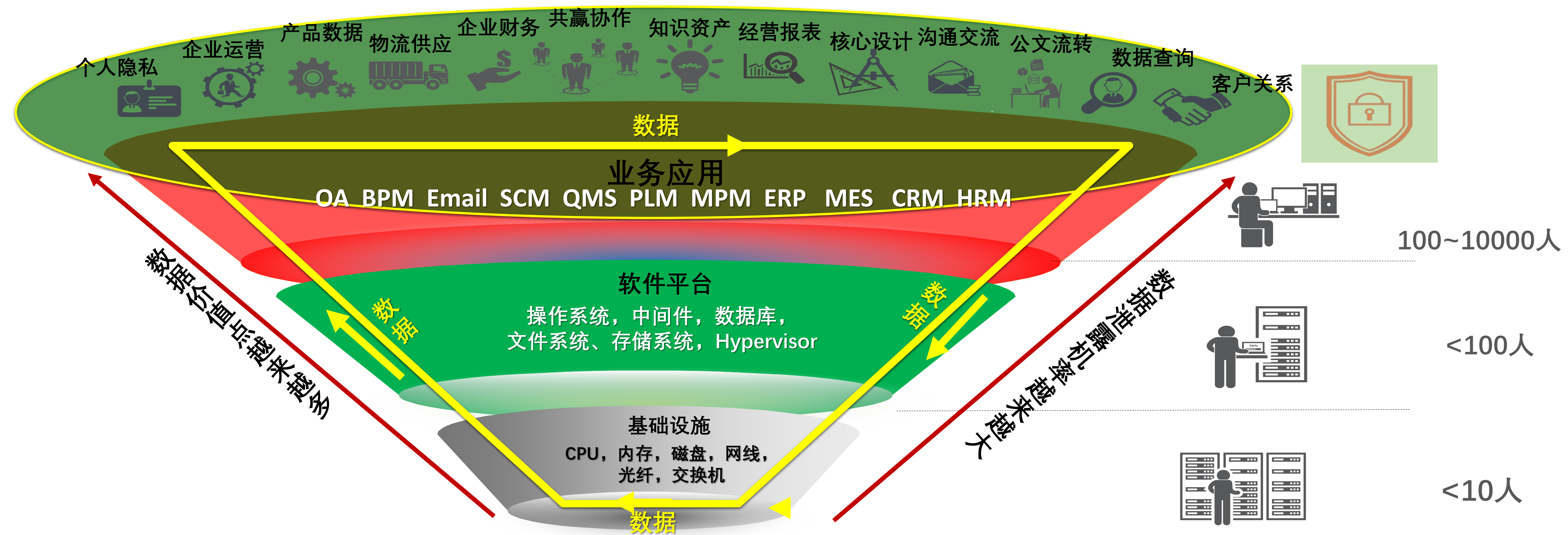






# 数据在信息化系统中的不同层次持续流转

# 第二届中国数据安全治理 高峰论坛2018







# 用CASB保护使用中的数据安全

第二届中国数据安全治理  
高峰论坛2018

CASB（云访问安全代理  
Cloud Access Security Broker）& CASB（关键应用安全代理  
Critical Application Security Broker）  
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



对应用操作和敏感数据的  
精细化识别能力

- 近百种应用操作；数十种文件类型，多种内容检测方法



对上下文环境的持续  
采集和分析能力

- 用户状态，账户状态，设备状态，访问目标



基于上下文环境的精细  
化访问控制能力

- 关联数十种主体、客体、环境参数



高速数据加解密和脱敏  
能力

- 数千兆商密加解密处理性能



多种策略响应动作

- 支持加密、阻断、隔离、水印、DRM、阻断用用户、带密码压缩、告警等等

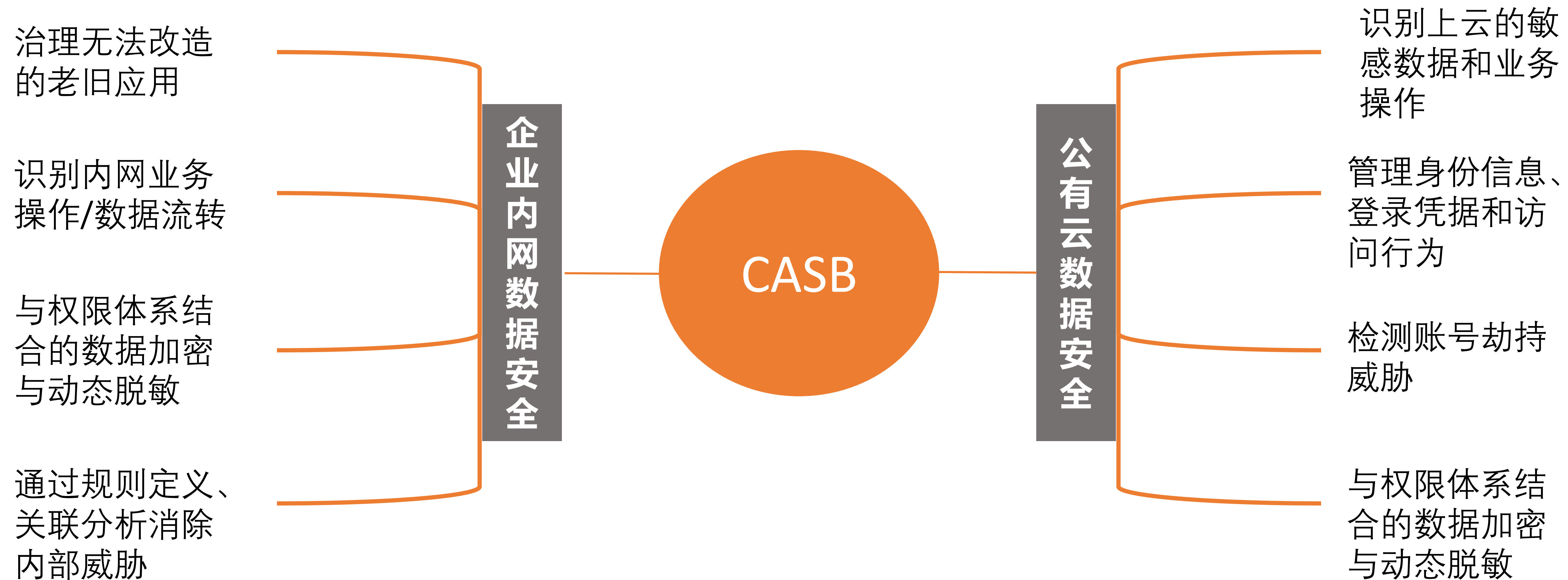
关键能力





# CASB的主要应用场景

第二届中国数据安全治理  
高峰论坛**2018**



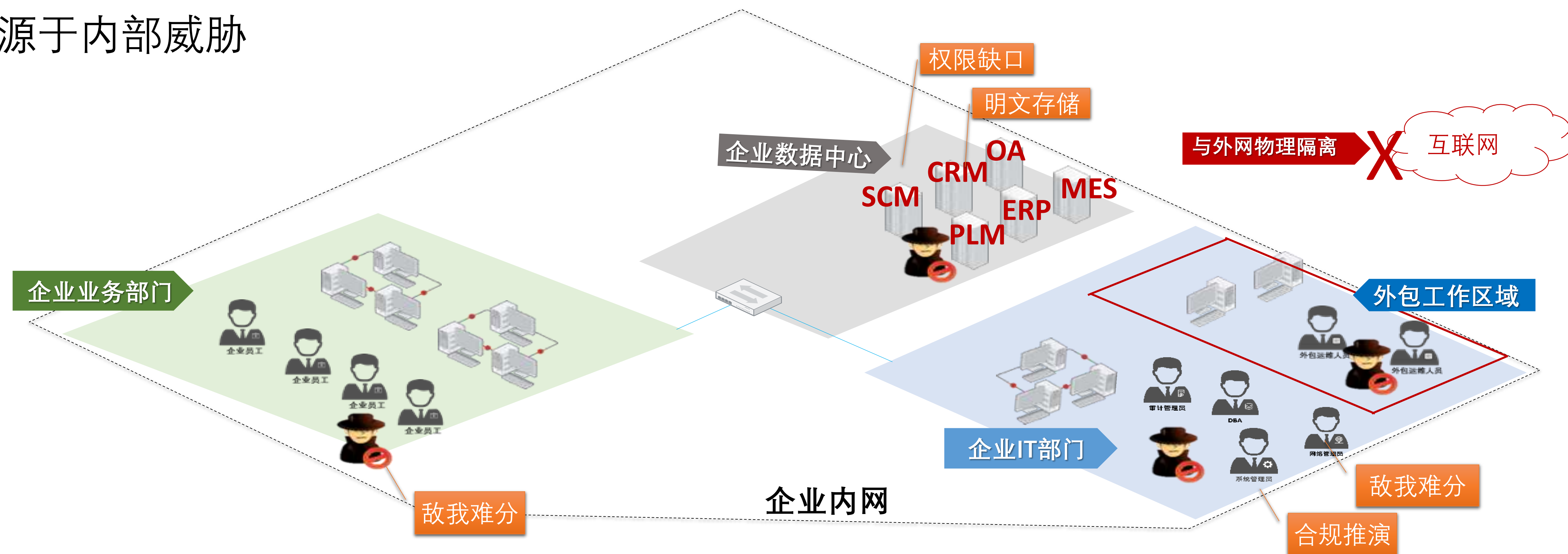




# 内部威胁客观存在

第二届中国数据安全治理  
高峰论坛2018

\* 70%以上的安全事件源于内部威胁

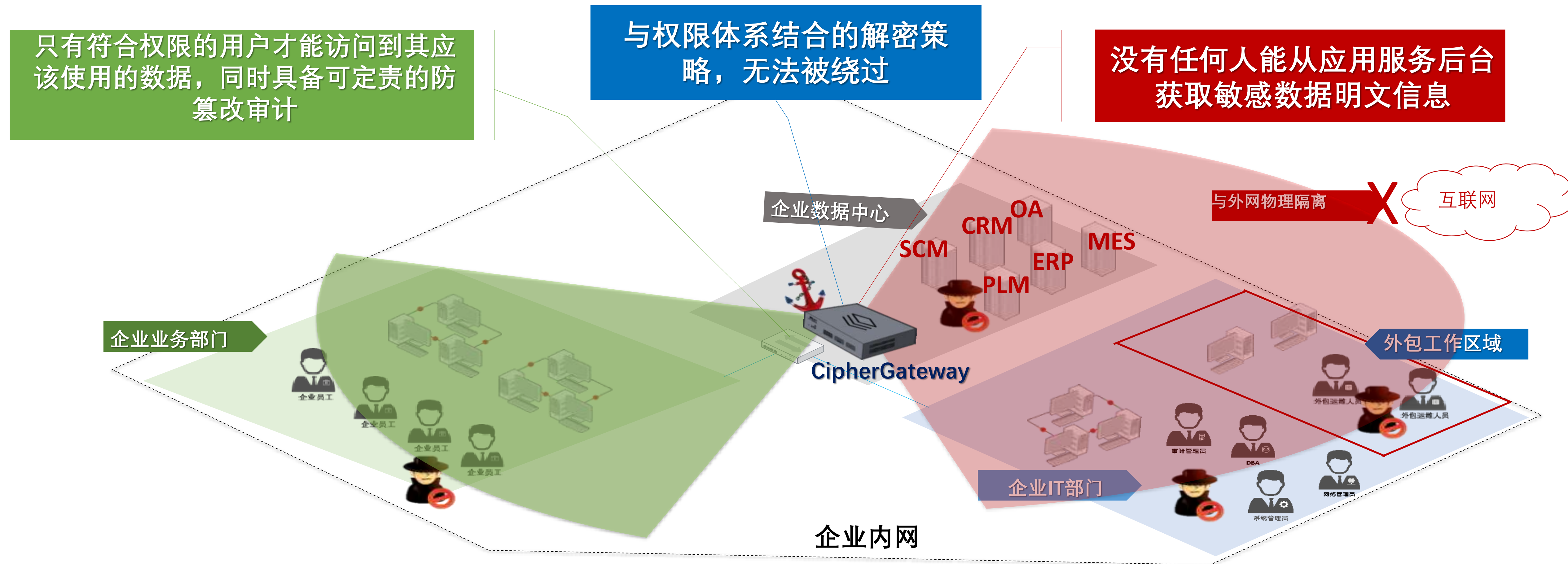






# 提供以数据为抓手的零信任安全架构

第二届中国数据安全治理  
高峰论坛2018

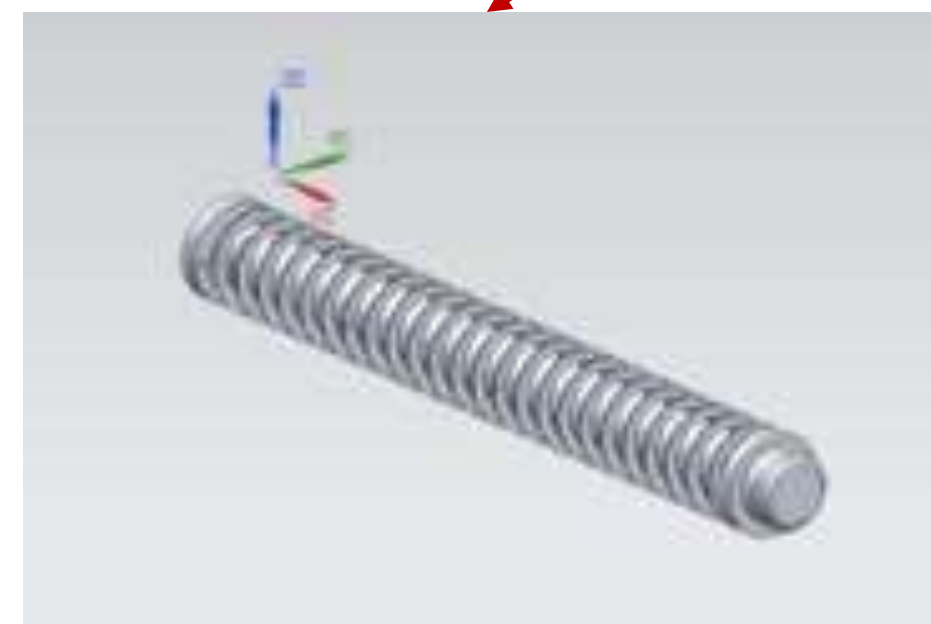






# 实践1—CASB保护装备研发流程中的数据安全

第二届中国数据安全治理  
高峰论坛**2018**



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。

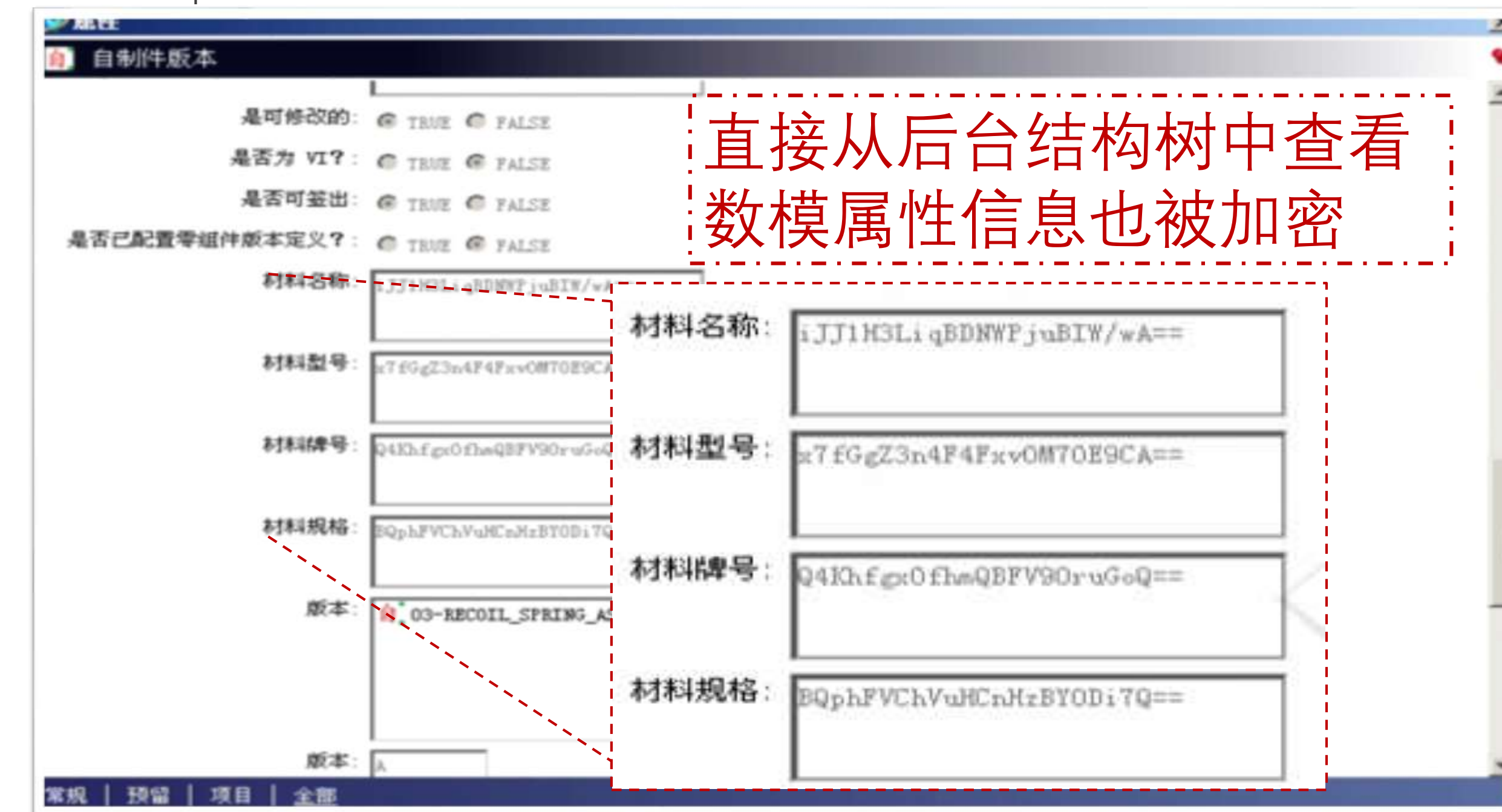
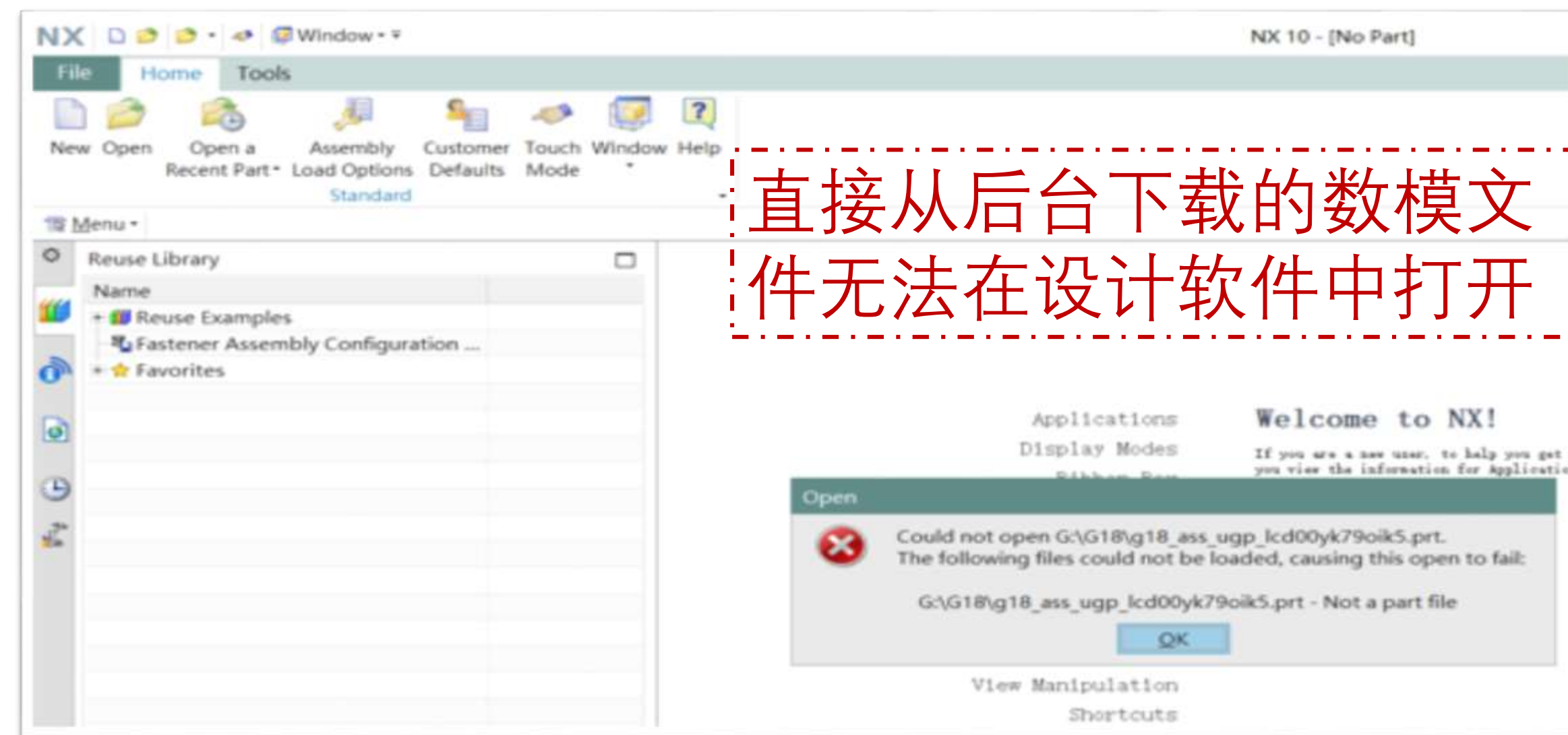
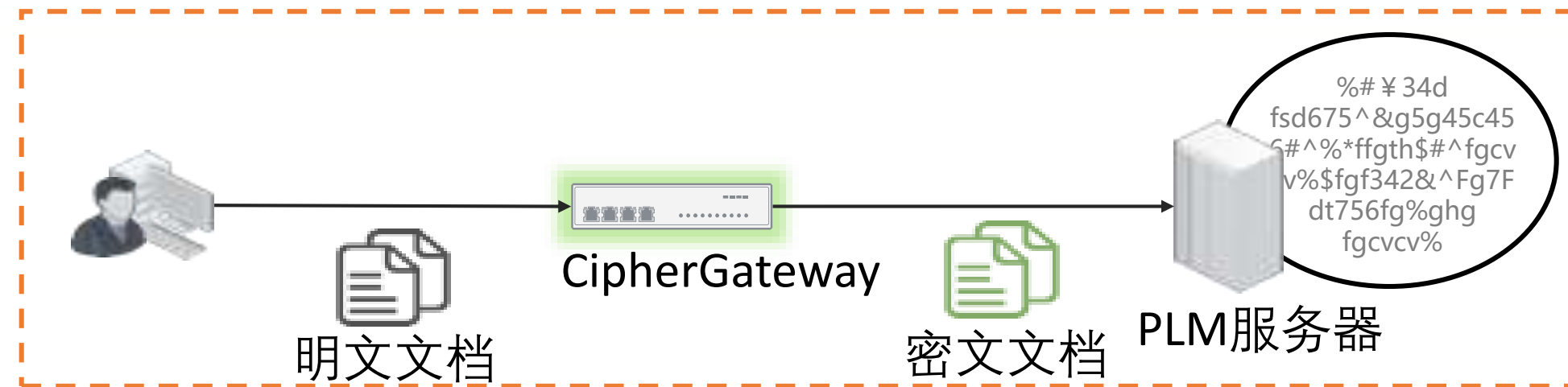
项目组使用 **SIEMENS TEAMCENTER** 作为协同工作平台





# 1) 为PLM赋予数据加密能力

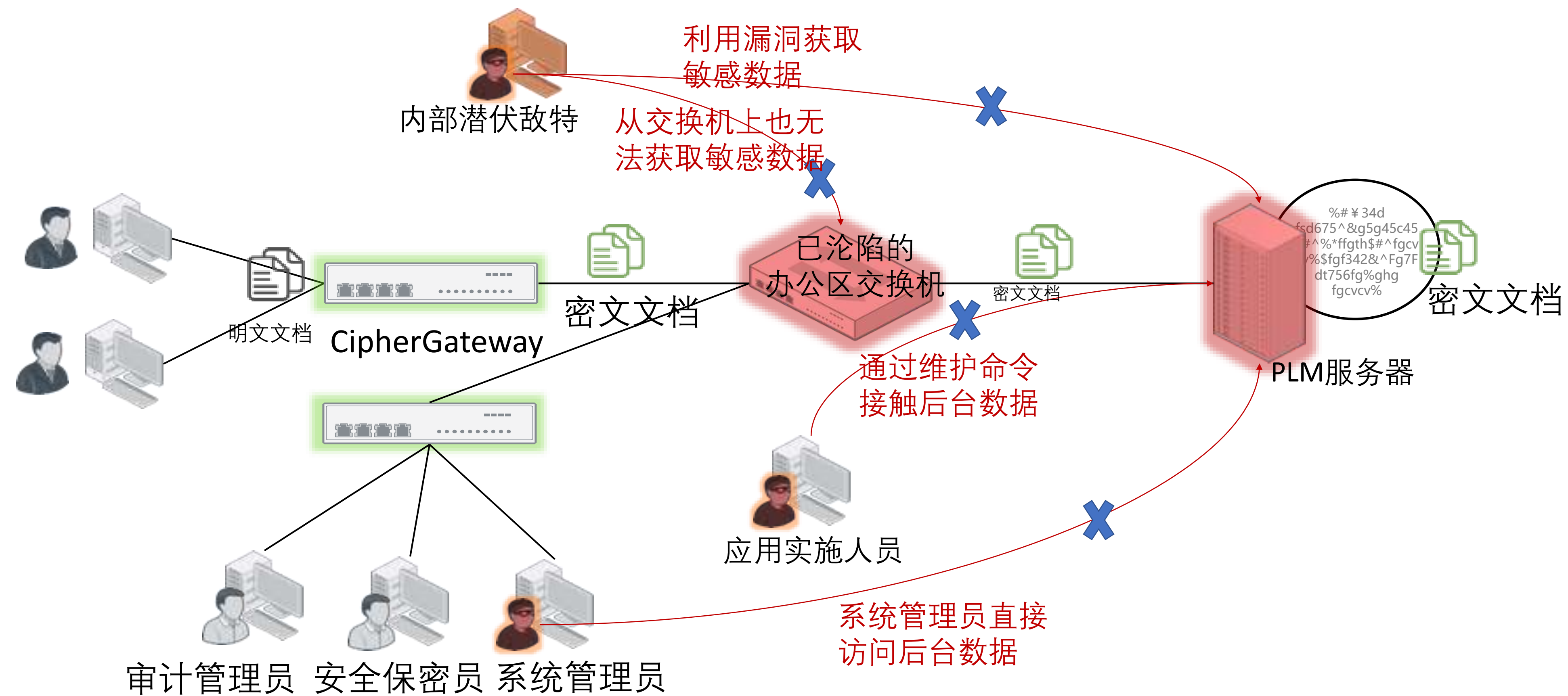
第二届中国数据安全治理  
高峰论坛2018







# 第二届中国数据安全治理 高峰论坛2018



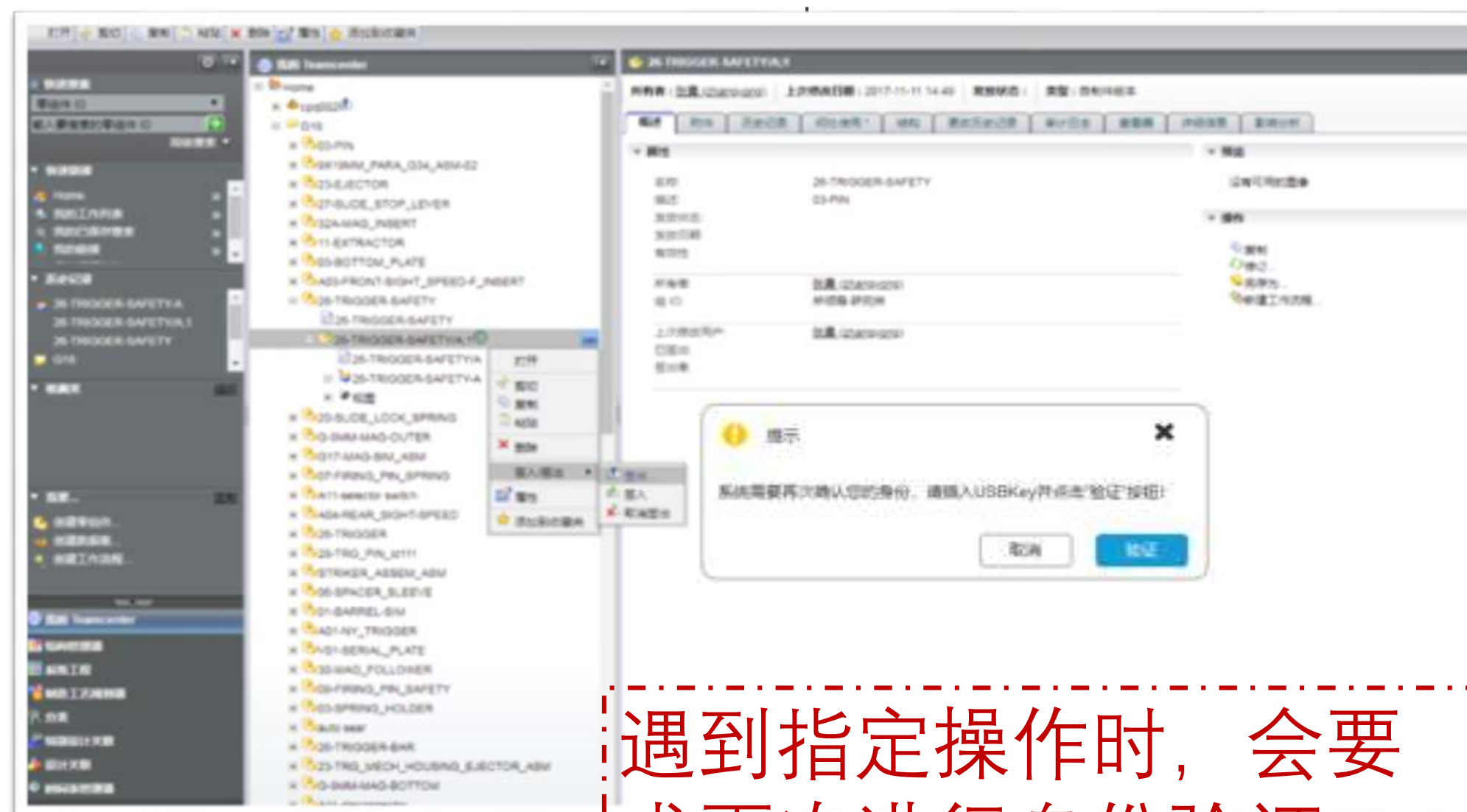
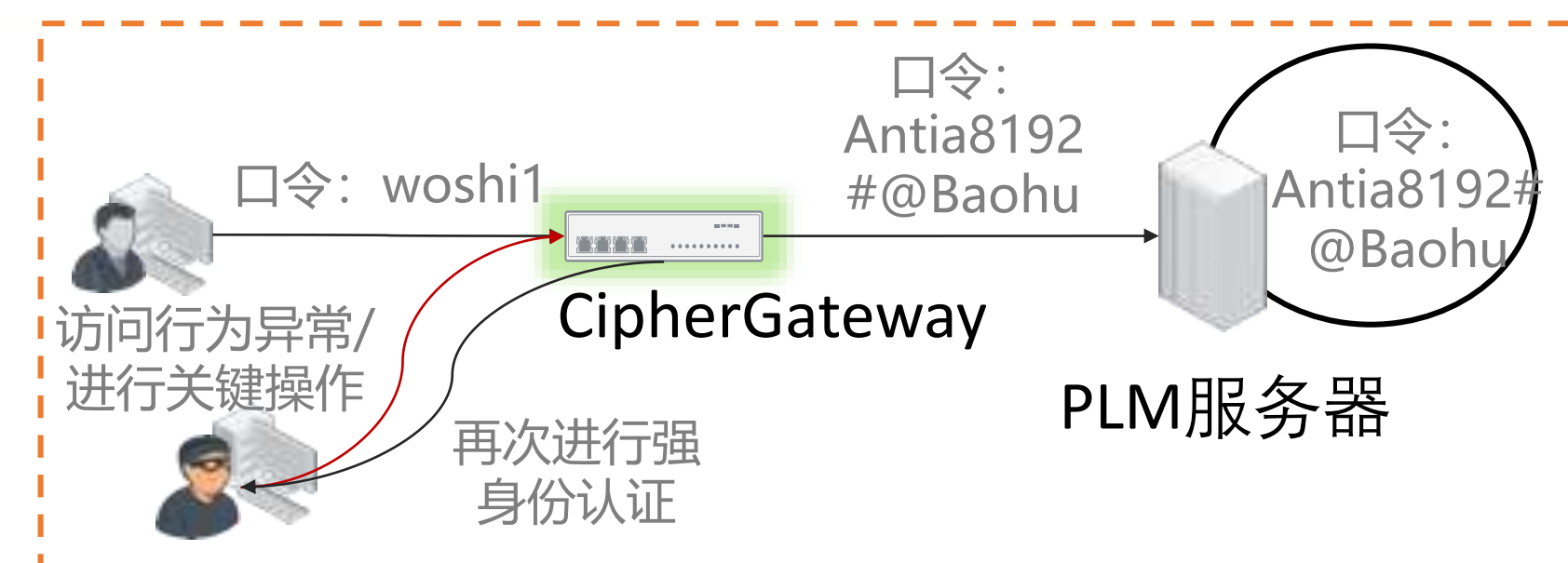
IT运维、外包实施、管理员、  
内部恶意人员、被控制主机、  
特木等人员和手段  
均无法直接从后台获取敏感数据



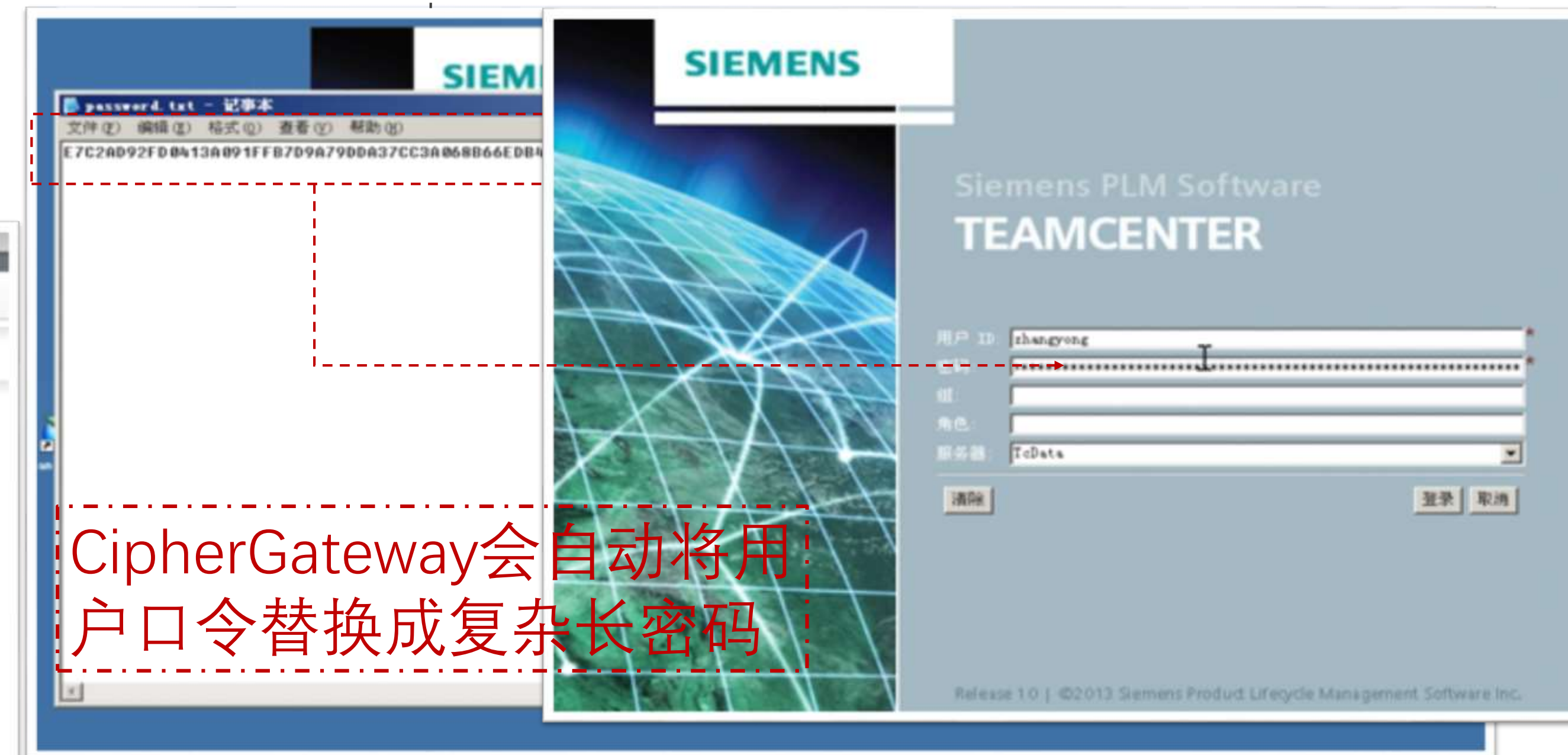


## 2) 杜绝关键操作时身份被冒用

第二届中国数据安全治理  
高峰论坛**2018**



遇到指定操作时, 会要求再次进行身份验证



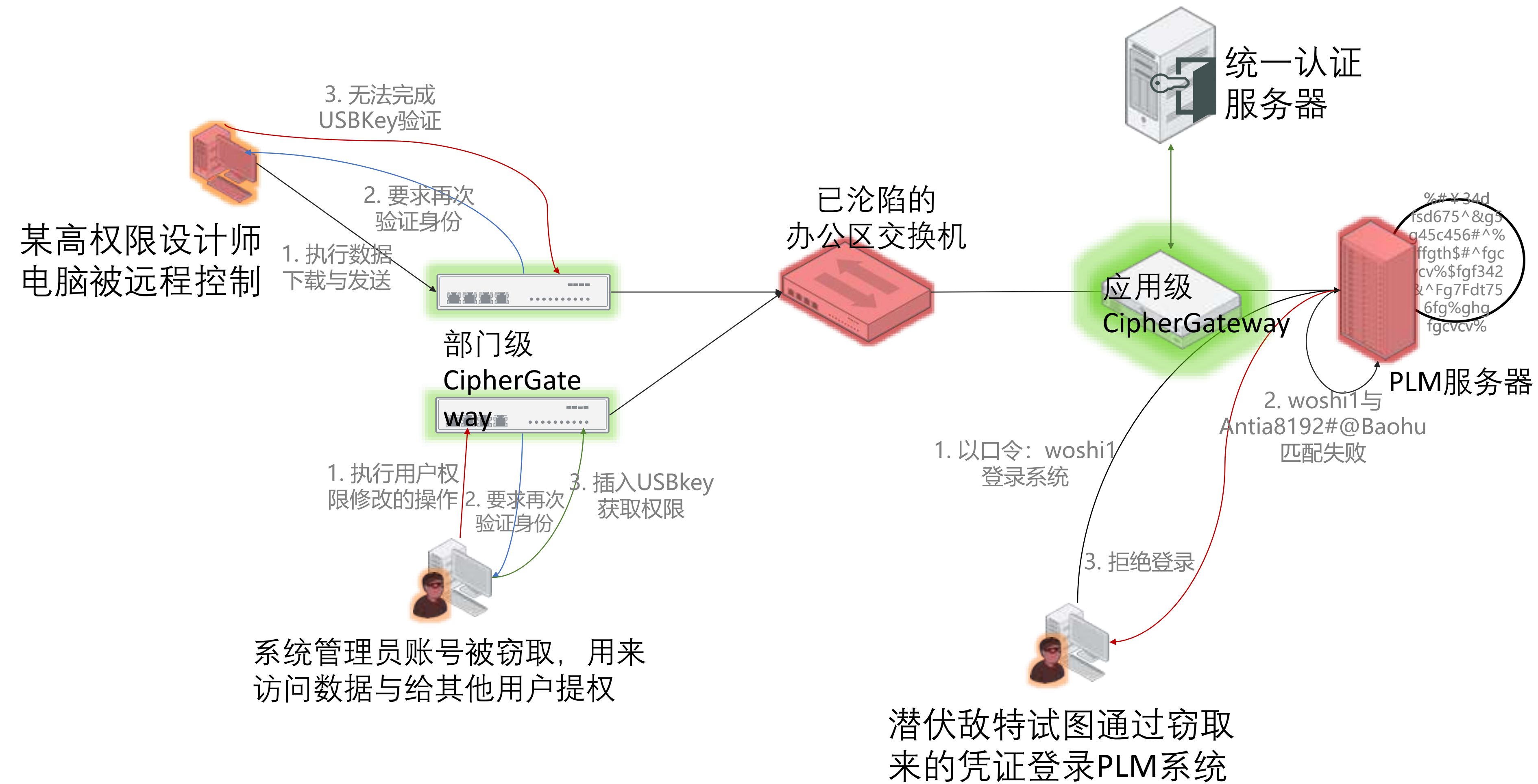
CipherGateway会自动将用户口令替换成复杂长密码





# 增强关键业务操作和数据使用的身份确定

第二届中国数据安全治理  
高峰论坛2018



防止身份被冒用，确保操作为用户本人执行：

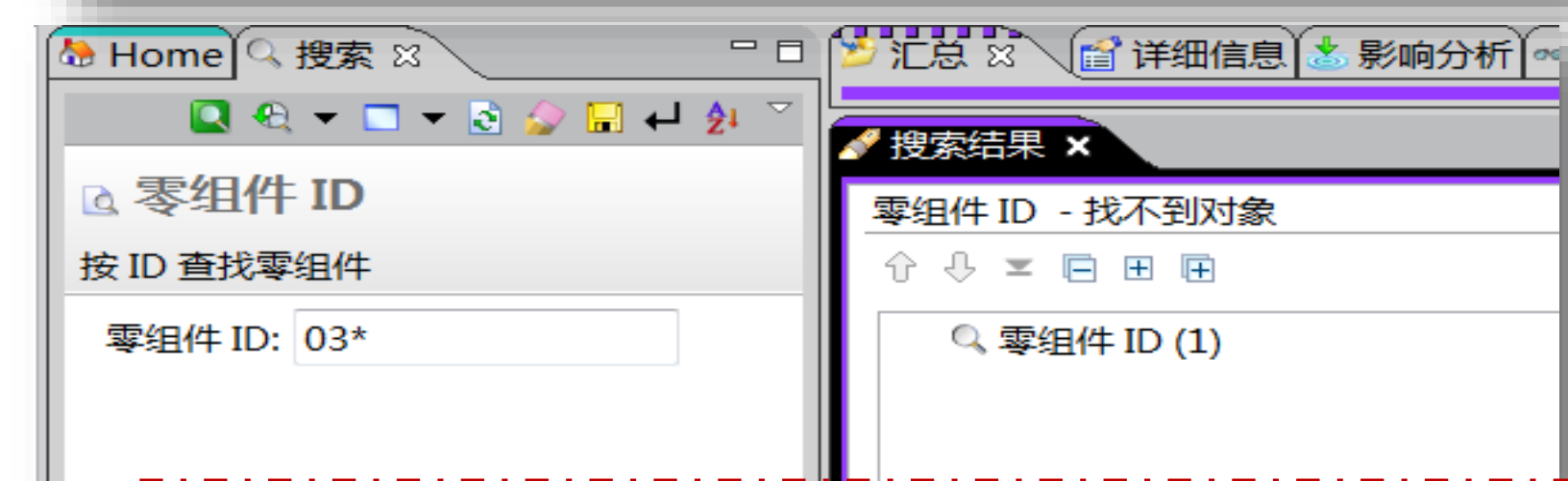
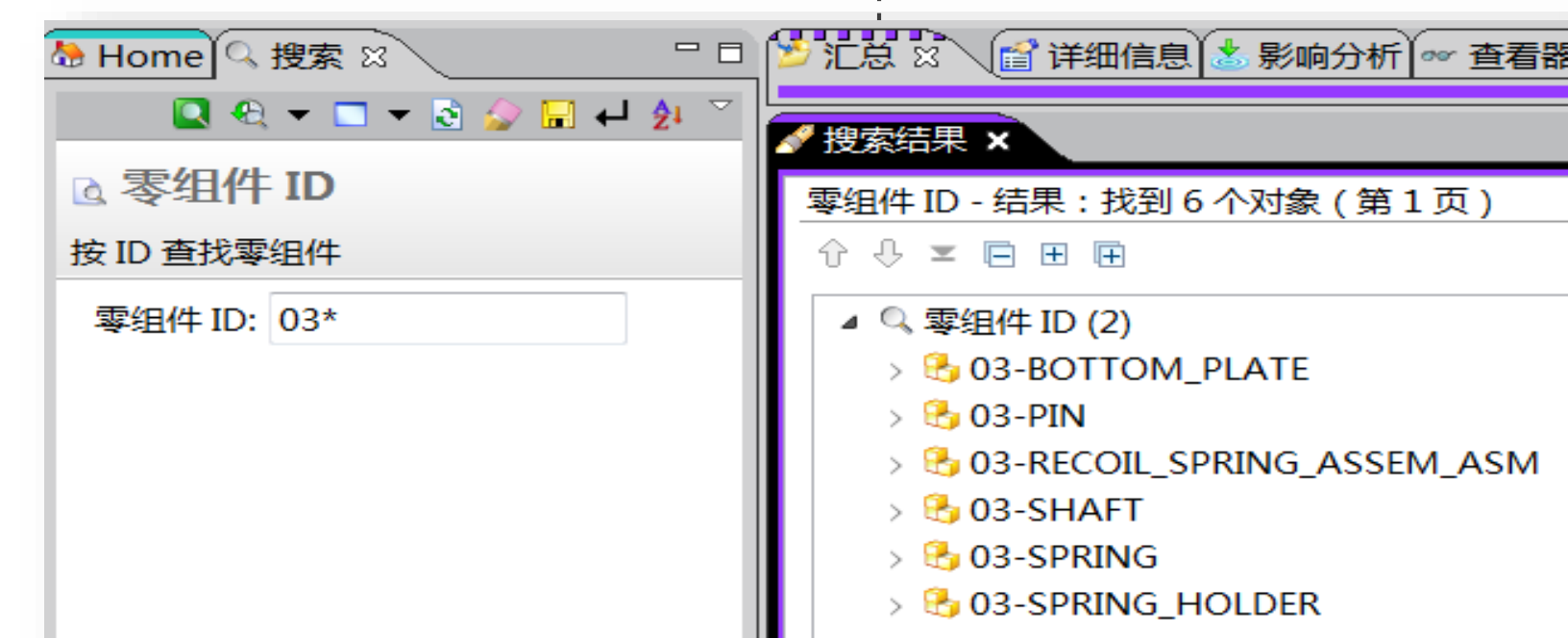
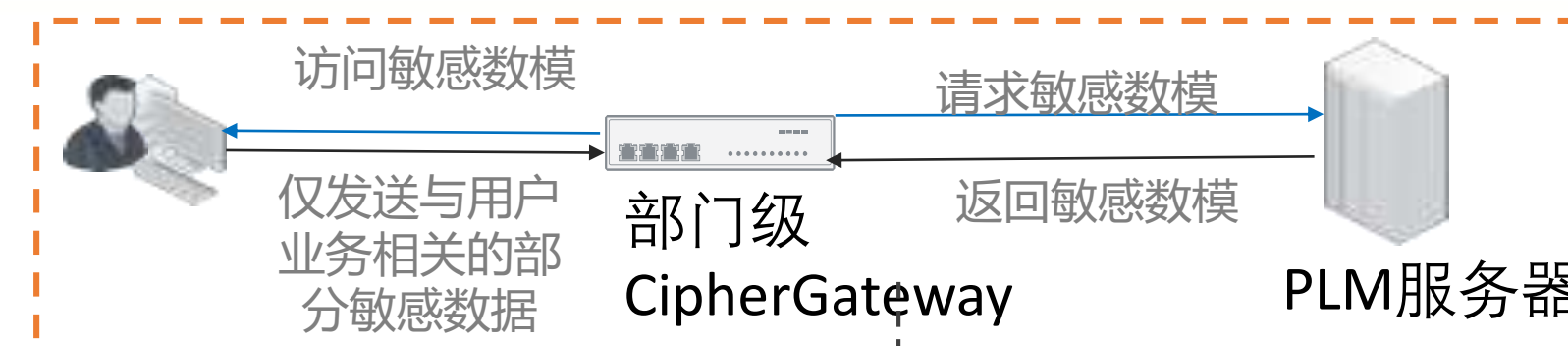
- 不通过部门级CipherGateway无法正确验证登录凭证
- 关键流程节点：敏感操作/异常操作需要再次进行强身份认证



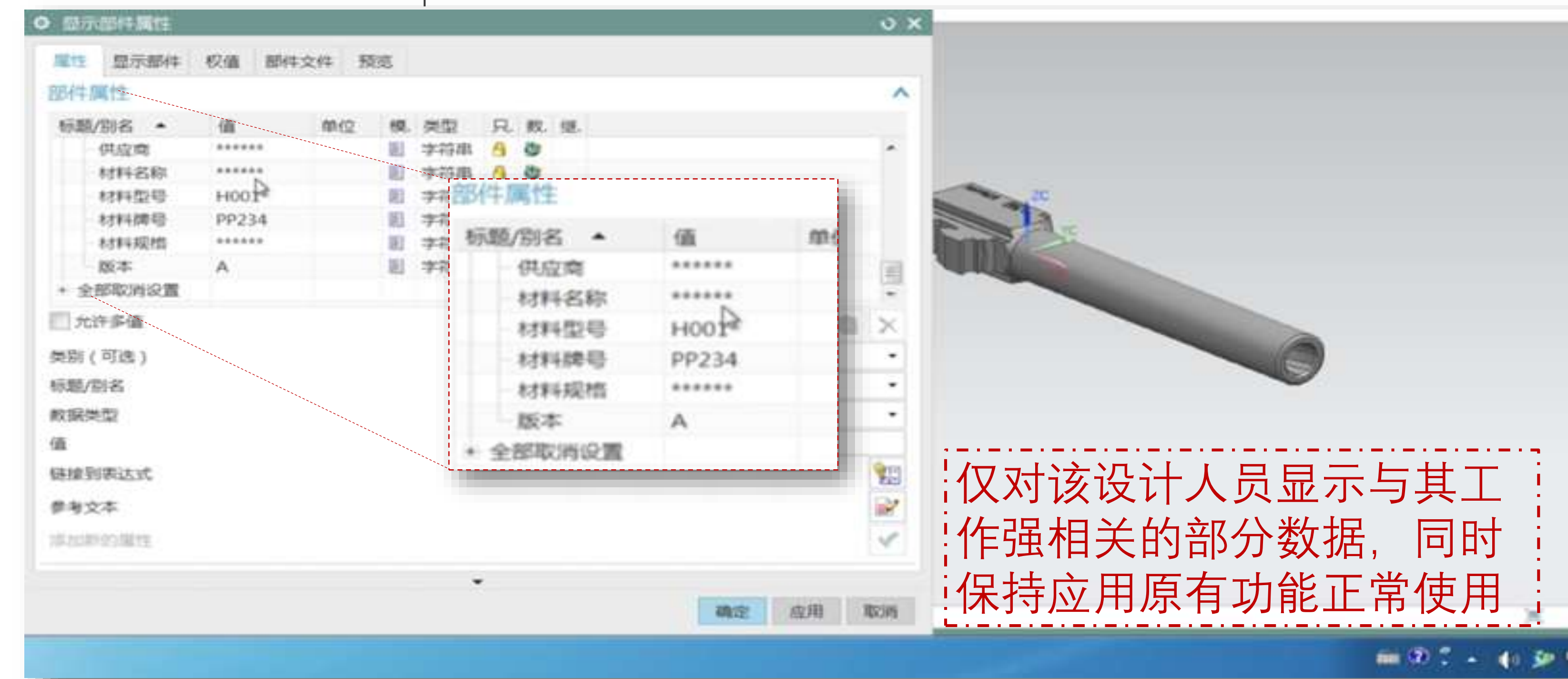


# 3) 参与人员只能访问其业务相关数据

第二届中国数据安全治理  
高峰论坛2018



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。

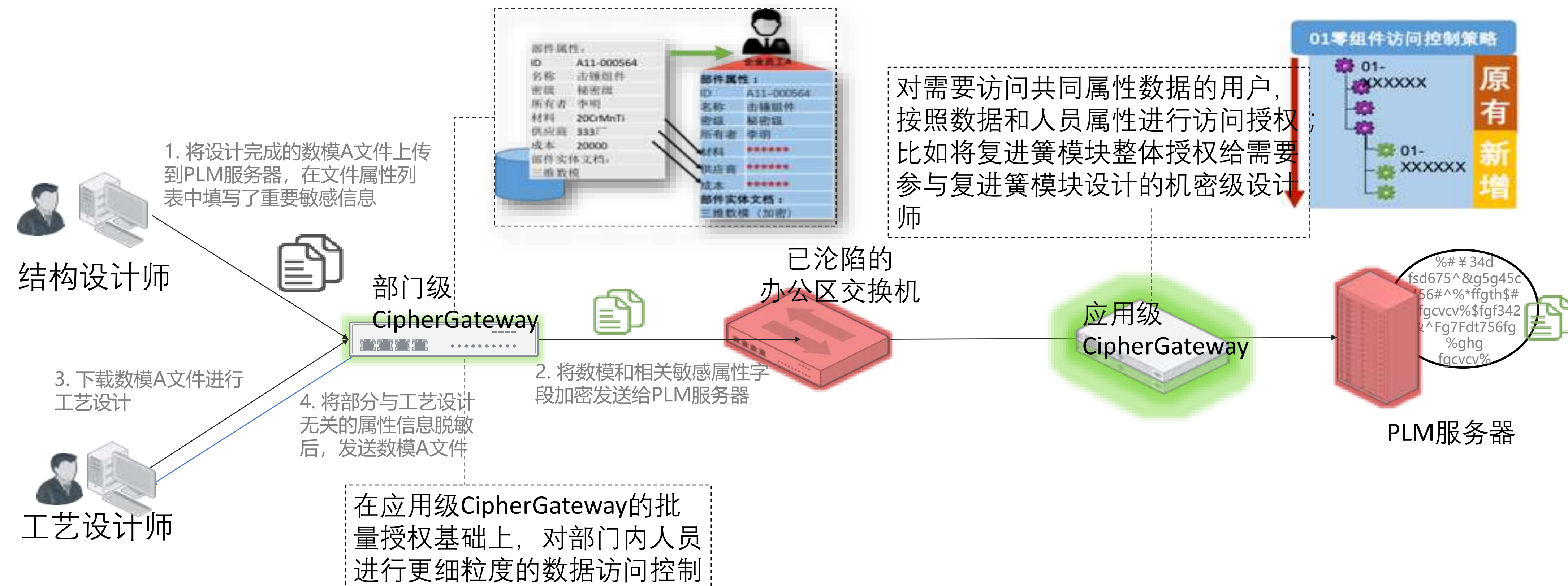






# 在复杂数据结构中最小化数据访问授权

第二届中国数据安全治理  
高峰论坛2018



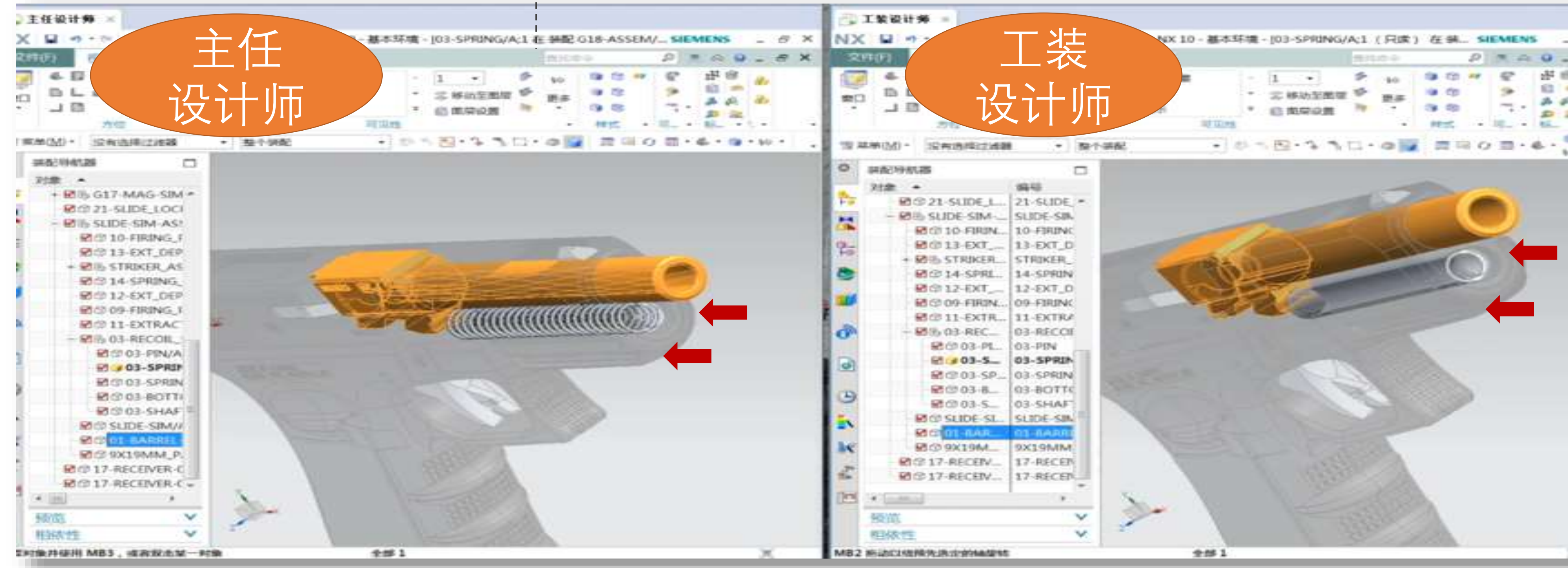
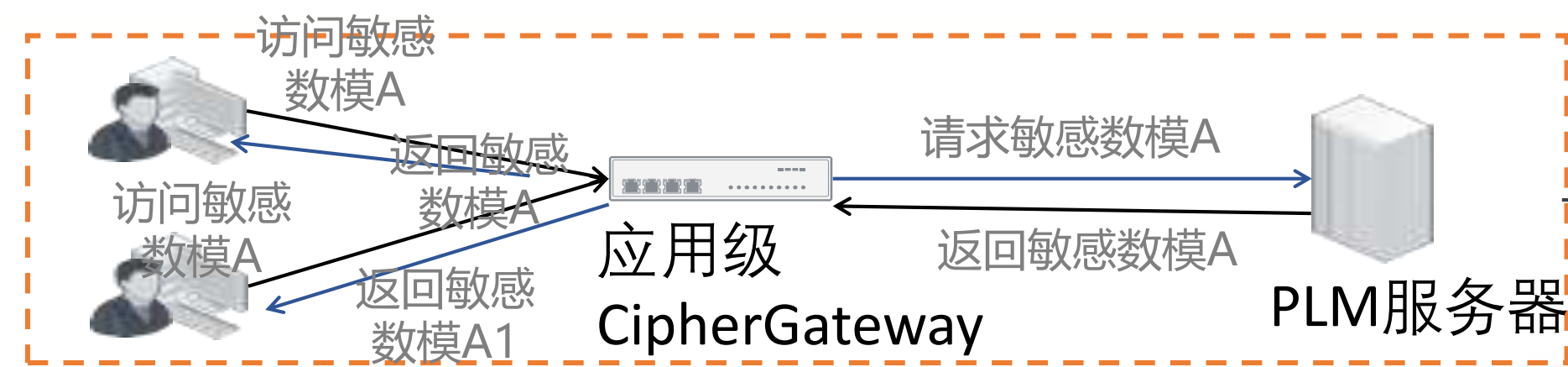
- 基于人员属性、环境属性和数据属性进行灵活精细的访问控制；
- 做到给确定有业务关系的人解密数据；
- 减小敏感数据暴露的风险；
- 降低了策略配置复杂度、使得权限可以动态继承；
- 对数据的访问控制配置快速，提升安全事件的响应能力





## 4) 深度结合数据使用的脱敏机制

第二届中国数据安全治理  
高峰论坛2018



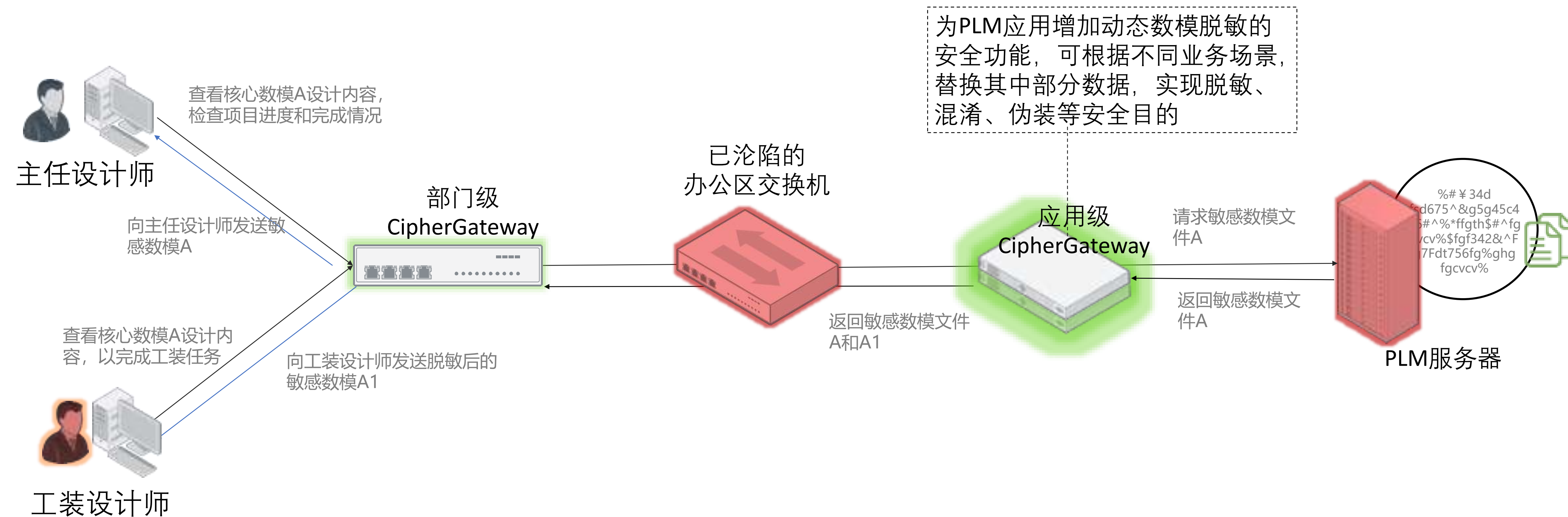
基于人员权限和策略，对没有权限的人进行定向脱敏，对“内鬼”或潜伏在内部的敌特人员，提供欺骗数据





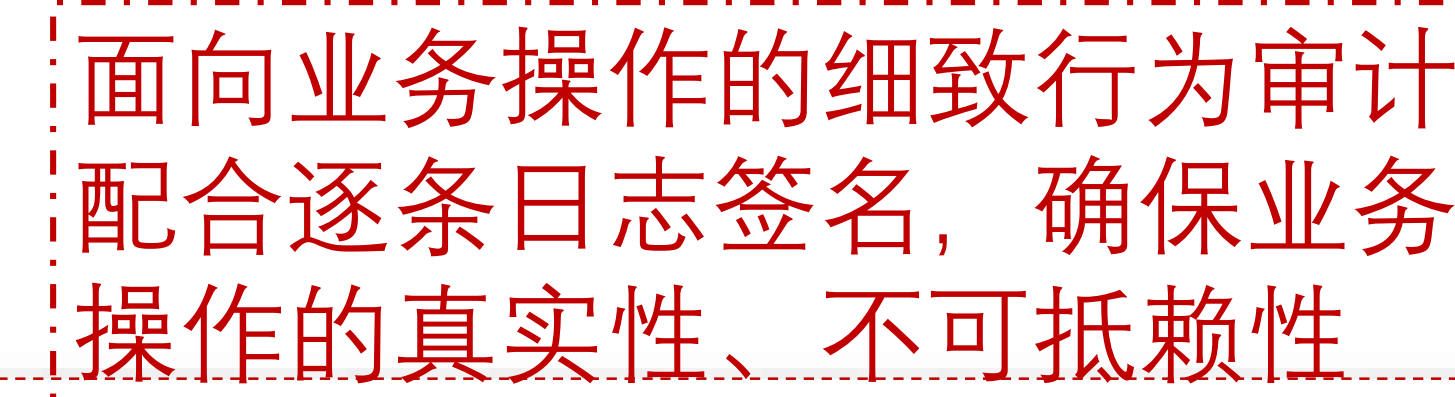
# 最小化敏感数据阅读范围，迷惑恶意人员

第二届中国数据安全治理  
高峰论坛2018



- 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;





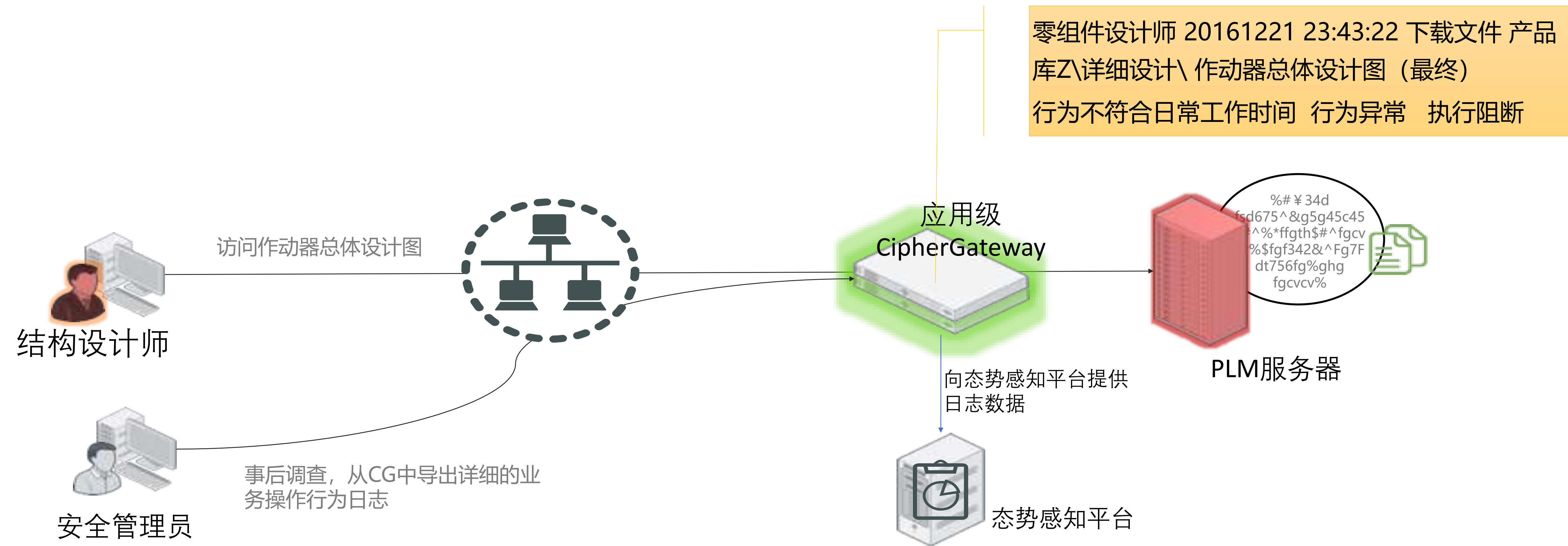
操作时间	操作者	行为	操作对象	操作对象ID	操作对象名称	操作对象所有者	状态	是否告警	告警类型	附件属性	客户端IP	日志签名
2018-02-01 16:13:25	Root	下载	邮件	09_9	09_9	Root	成功	否	否	279568	172.16.10.98	MEUCI QC/7L...
2018-02-01 16:13:25	Root	下载	邮件	01_1	01_1	Root	成功	否	否	213008	172.16.10.98	MEUCI ApAW...
2018-02-01 16:13:25	Root	下载	邮件	03_3	03_3	Root	成功	否	否	95760	172.16.10.98	MEQC GVgOL...
2018-02-01 16:13:24	Root	下载	邮件	01_13	01_13	Root	成功	否	否	96784	172.16.10.98	MEUCI MEUCQQYVwvTNGDYAxbKQp64u8IbMw5OnkXUyVWMT
2018-02-01 16:13:24	Root	下载	邮件	02_2	02_2	Root	成功	否	否	376336	172.16.10.98	MEUCI QDYw...
2018-02-01 16:13:24	Root	下载	邮件	04_4	04_4	Root	成功	否	否	163344	172.16.10.98	MEUCI BFG...
2018-02-02 16:17:59	ymh	上传	邮件	04_9	04_9	ymh	成功	否	否	175344	172.16.10.98	MEUCI BFG...





# 辅助业务人员进行事后取证与定责

第二届中国数据安全治理  
高峰论坛2018



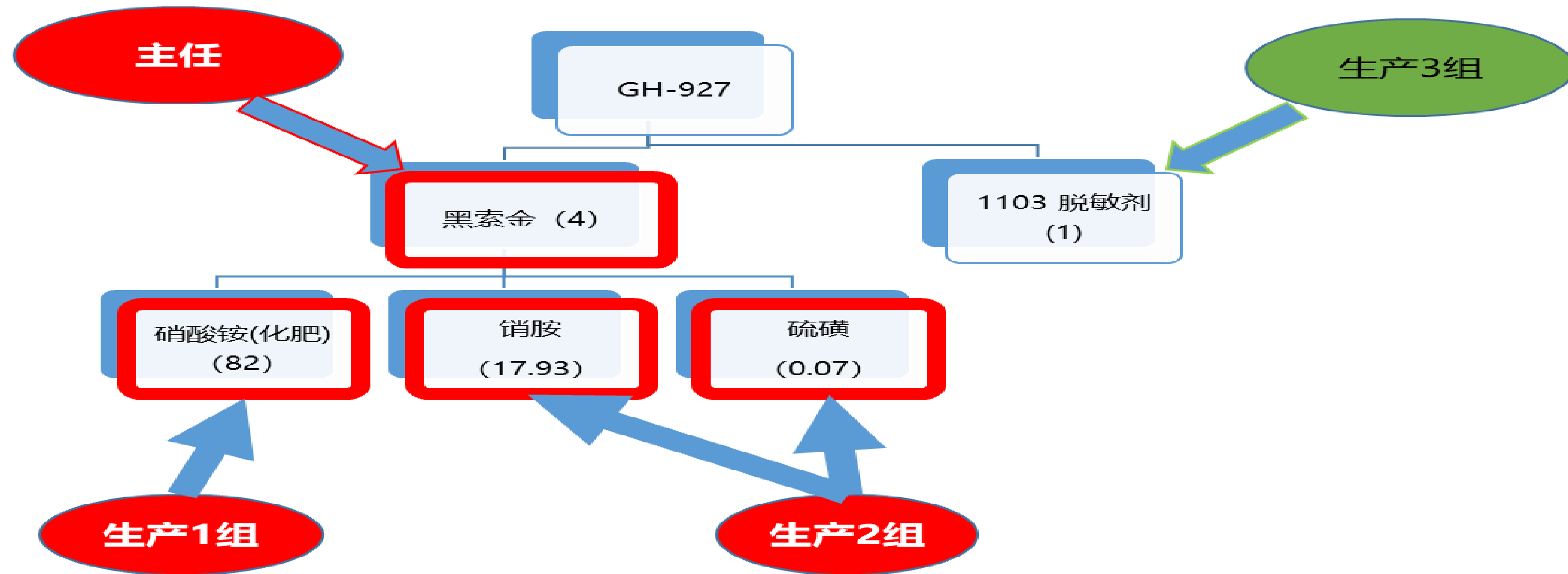
- 辅助事后调查、取证和追溯定责；
- 作为业务语言的安全日志内容输出给态势感知平台，提升整体分析、预警能力；





# 实践2—CASB保护ERP流程中的配方数据安全

第二届中国数据安全治理  
高峰论坛2018







# 业务流程与核心关键点

第二届中国数据安全治理  
高峰论坛2018







**生产1组**

材料编码	材料名称	出库仓库编码
1 110101	硝酸铵(化肥)	1
2 110102	z@19jsmz	1
3 110103	dhewy76v	1

材料名称: 硝酸铵(化肥)  
z@19jsmz  
dhewy76v

计划出库数量
82.00
0
0

库管员名称	计划出库数量	转计划出库数量	累计出库数量
	82.00		0.00
	0		0.00
	0		0.00

**生产2组**

材料编码	材料名称	出库仓库编码
1 110101	ru75xa"8&	1
2 110102	销胺	1
3 110103	硫磺	1

材料名称: ru75xa"8&  
销胺  
硫磺

计划出库数量
0
17.93
0.07

库管员名称	计划出库数量	转计划出库数量	累计出库数量
	0		0.00
	17.93		0.00
	0.07		0.00





# 不参与关键配方的用户只能看到密文

第二届中国数据安全治理  
高峰论坛2018

UFIDA AC

生产3组

1101 GH-927网络炸药

1102 黑索金 (RDX)

110101 ru75xa"8&

110102 z@19jsmz

110103 dhewy76v

1103 脱敏剂

父项数量

0

子项名称

ru75xa"8&

z@19jsmz

dhewy76v

子项数量

0

0

0

行号	子项类型	子项名称	图号	物料来源	子项数量	物料系数	提前期	互斥组	自由项1	自由项2	自由项3	自由项4
1	普通	子项	110101	ru75xa"8&	0	0.000	0.00					
2	普通	子项	110102	z@19jsmz	0	0.000						
3	普通	子项	110103	dhewy76v	0	0.000						

\* 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

第二届中国数据安全治理  
高峰论坛**2018**

**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

第二届中国数据安全治理  
高峰论坛2018



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

