CASB保护零信任环境下的数据安全实践

白小勇　　炼石网络 CEO

2018 ISC 互联网安全大会 中国·北京
Internet Security Conference 2018　Beijing·China
（原“中国互联网安全大会”）

提要

1. 数字化催生业务级安全技术
2. CASB对内部威胁防护的实践
3. CASB对SAAS数据的安全防护实践

ZERO TRUST SECURITY

数字化同时带来了发展机遇和安全挑战

- 企业数字化推动了业务效率的快速提升，为企业带来了巨大利益
- 高价值使数据成为更加明确的攻击目标，重要数据关乎企业核心业务风险

- 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

内部威胁已经成为企业的主要安全威胁

70%

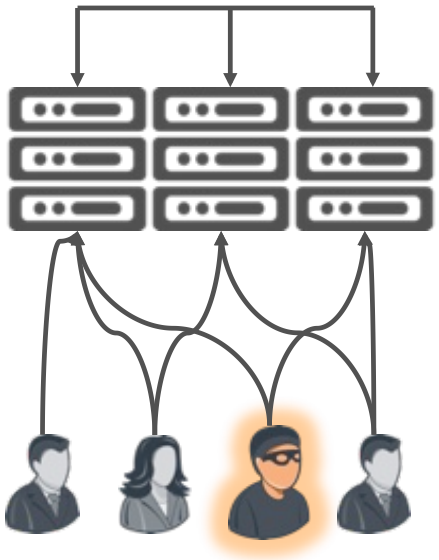
敏感信息泄露事件
来源于“内鬼”

65%

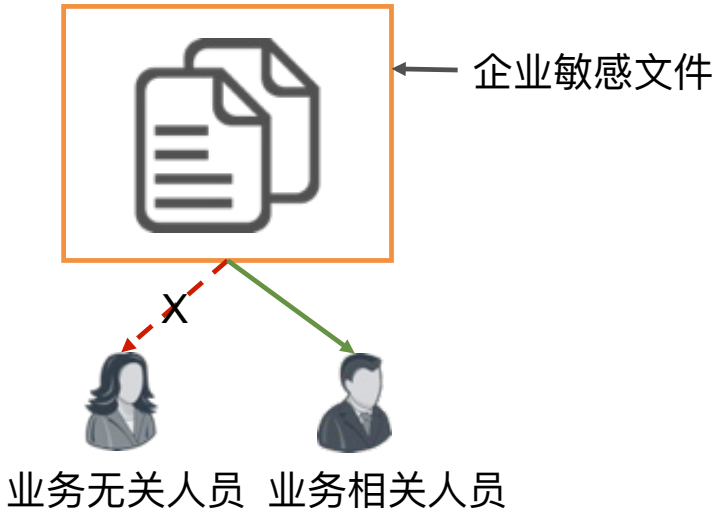
企业发生过严重的
商业秘密泄露事件

ZERO TRUST SECURITY

数据使用与保密面临“两难”，亟待新安全手段解决



VS



- 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

- 传统数据安全手段面向文档文件或数据库，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

安全策略需要综合考虑业务机会与安全风险

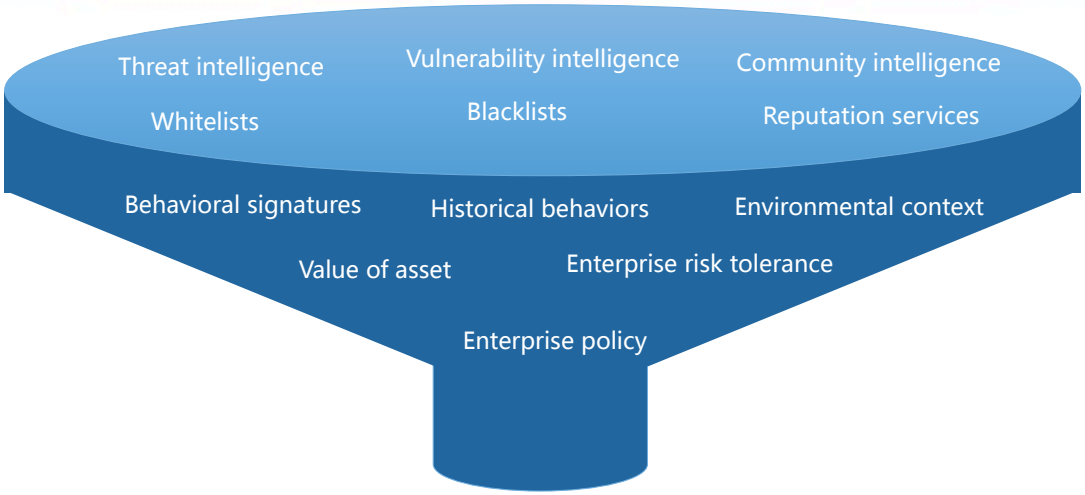
云和移动化等使得**企业不再拥有物理系统掌控、设备与业务交互**，同时数字化业务的规模和复杂度提升，导致传统手段难以分辨“好坏”

完美防御已然失效，**是否信任不再取决于单个向量，而是取决于场景的上下文**，同时信任与否是动态的，会随着业务场景持续变化

数字化业务的风险与机会共存，**新一代安全策略必须保持与业务发展快速同步，并且是自适应的**，能结合业务价值管理风险

ZERO TRUST SECURITY

CARTA主张结合业务上下文评估风险



Should this entity take this requested action on this entity **given the current context, my trust of the entity and my tolerance for risk?**

Continuous risk and trust engine

- Block/Prevent
- Ask for more context
- Allow
- Allow and log
- Allow and audit
- Allow and isolate
- Allow and throttle
- Deceive

Continuous adaptive risk and trust assessment

（持续自适应风险与信任评估）

* 源自Gartner

ZERO TRUST SECURITY

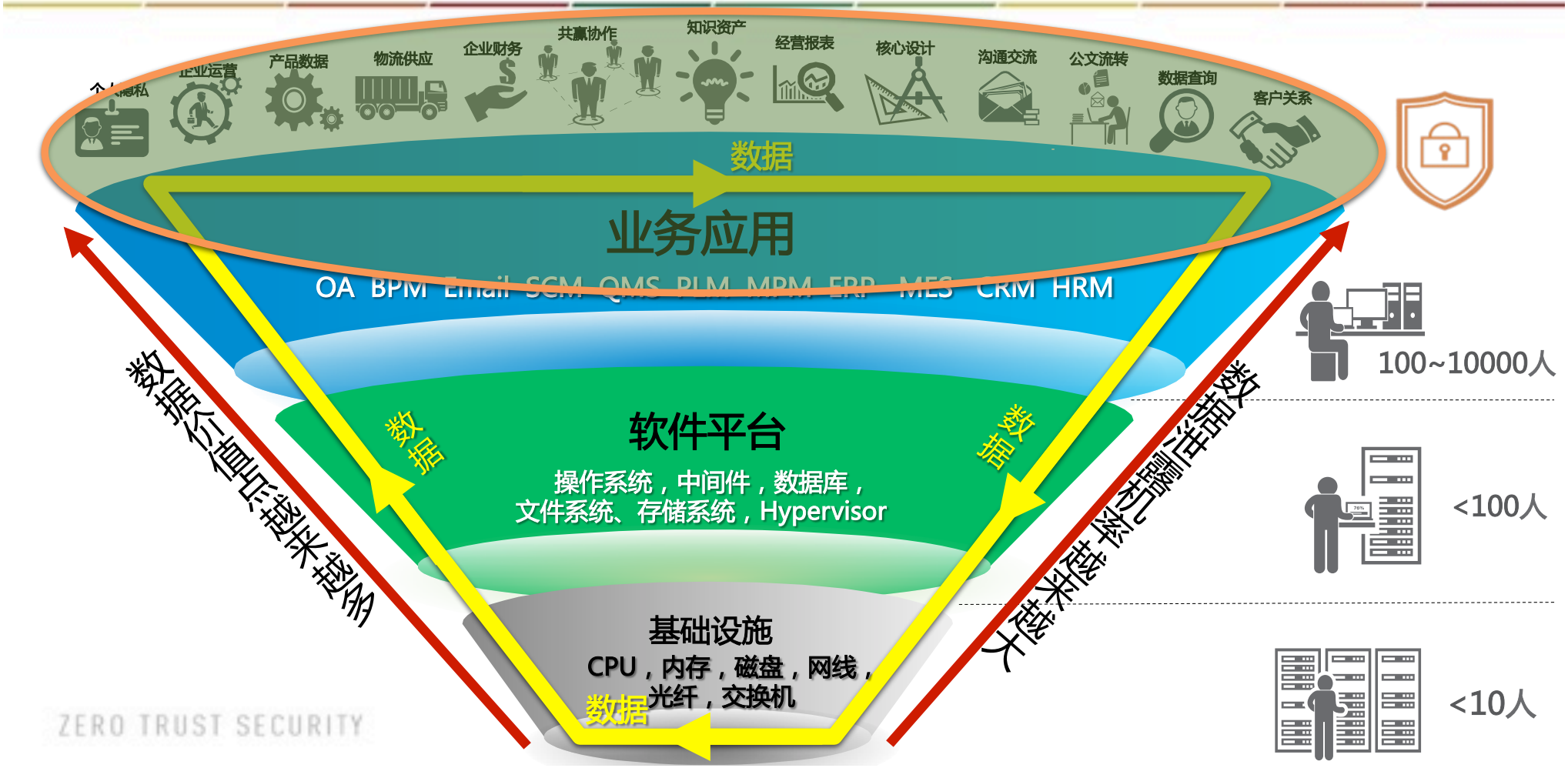
CARTA核心要素

- 持续动态评估
- 自适应
  - **业务场景丰富化，以提高评估准确度**
  - 响应和处置安全事件后，再将规则反馈到防护产品的安全策略集
- 风险与信任
  - **动态灰度名单取代了传统的静态黑白名单**
- 评估
  - 基于上下文，评估引擎计算Risk Score
  - **上下文不仅有IT基础设施上下文，更重要的是业务上下文**

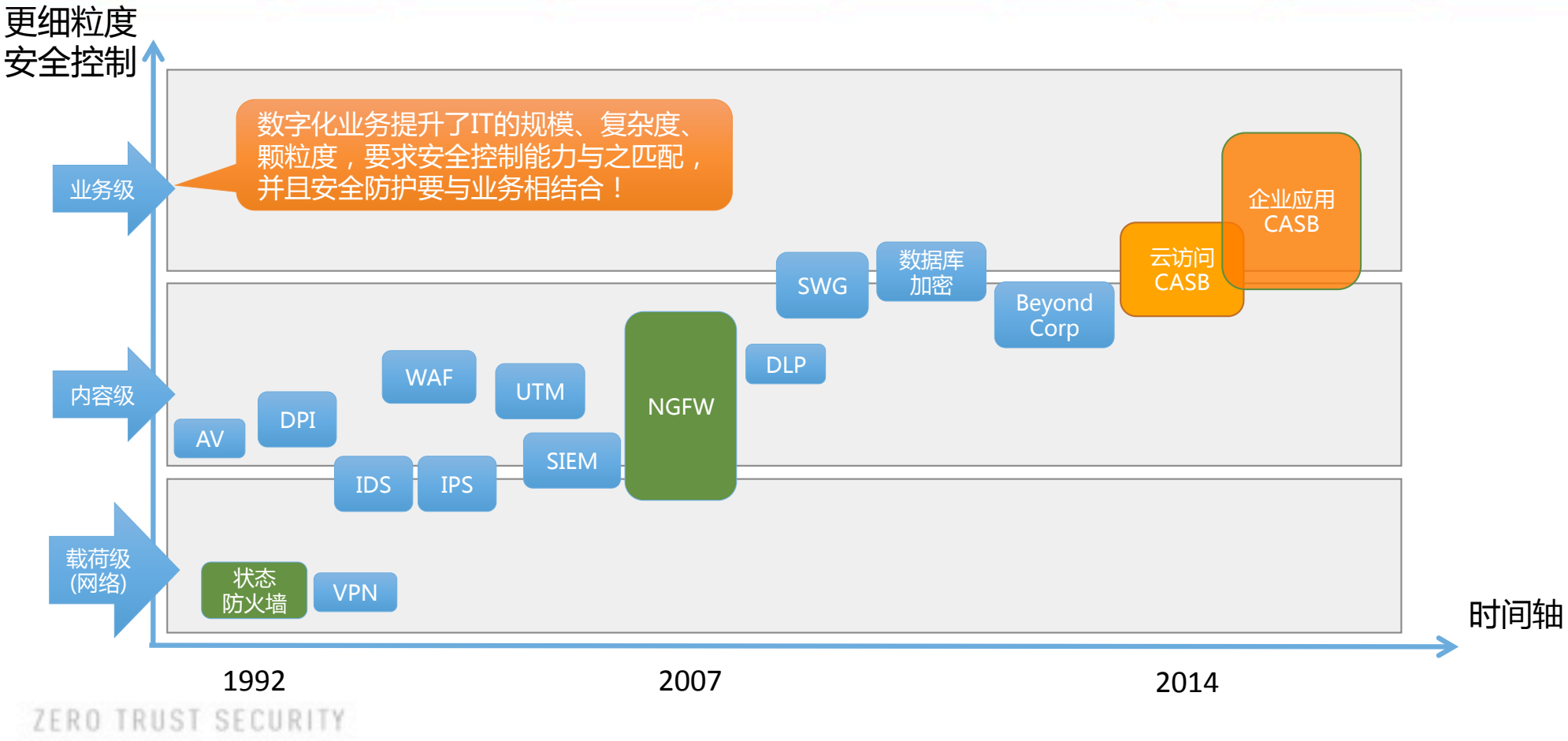
CARTA的启发

- **CARTA响应策略也取决于业务机会，与其失去业务机会，可承受一定风险**
- 对云服务的安全，云访问CASB是实施CARTA的主要手段

数据在信息化系统中的不同层次持续流转

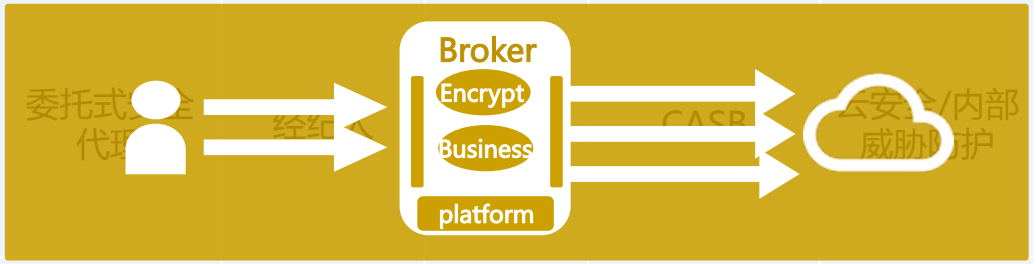


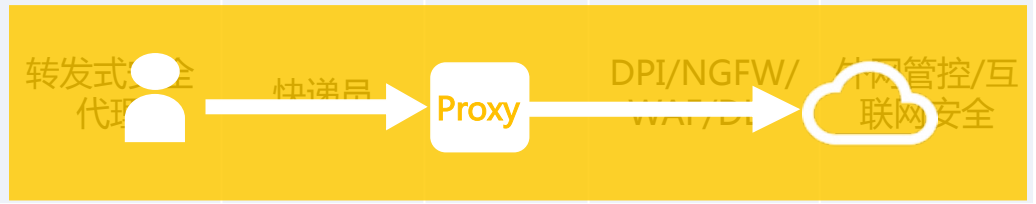
IT技术发展带来新威胁，推动安全产品向细粒度演进

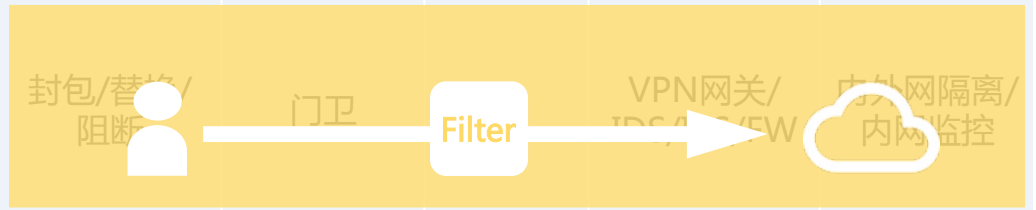


“业务感知”的CASB

类型	感知范围	请求关联	技术能力	功能特点	生活举例	业务结合	安全产品	适用场景
业务级	Business-awareness	Inter-request	Broker					
内容级	Content-awareness	Intra-request	Proxy					
载荷级(网络)	Payload-awareness	Intra-part-request	Filter					







CASB将丰富安全能力施加到业务级

企业应用安全代理 (Corp Application Security Broker) & 云访问安全代理 (Cloud Access Security Broker)

对业务操作和敏感数据的精细化识别

- 近百种应用操作；数十种文件类型，多种内容检测方法

上下文环境的持续采集和还原

- 用户，账户，设备，操作目标，业务含义，业务关联

丰富的安全策略及响应动作

- 支持加密、阻断、隔离、水印、DRM、阻断用户、带密码压缩、告警、日志等

基于业务上下文的细粒度访问控制

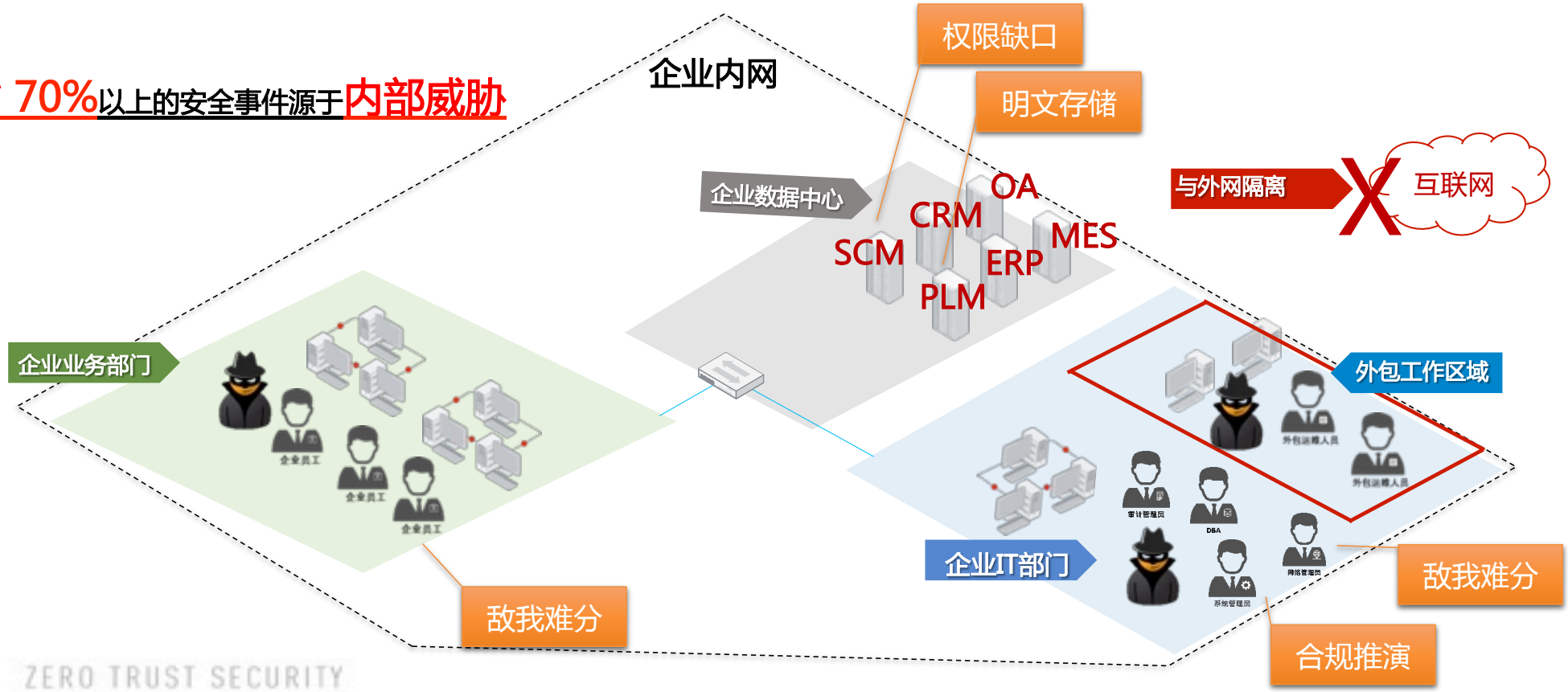
- 关联数十种主体、客体、环境参数
- 基于属性和角色的访问控制

数据加密和脱敏

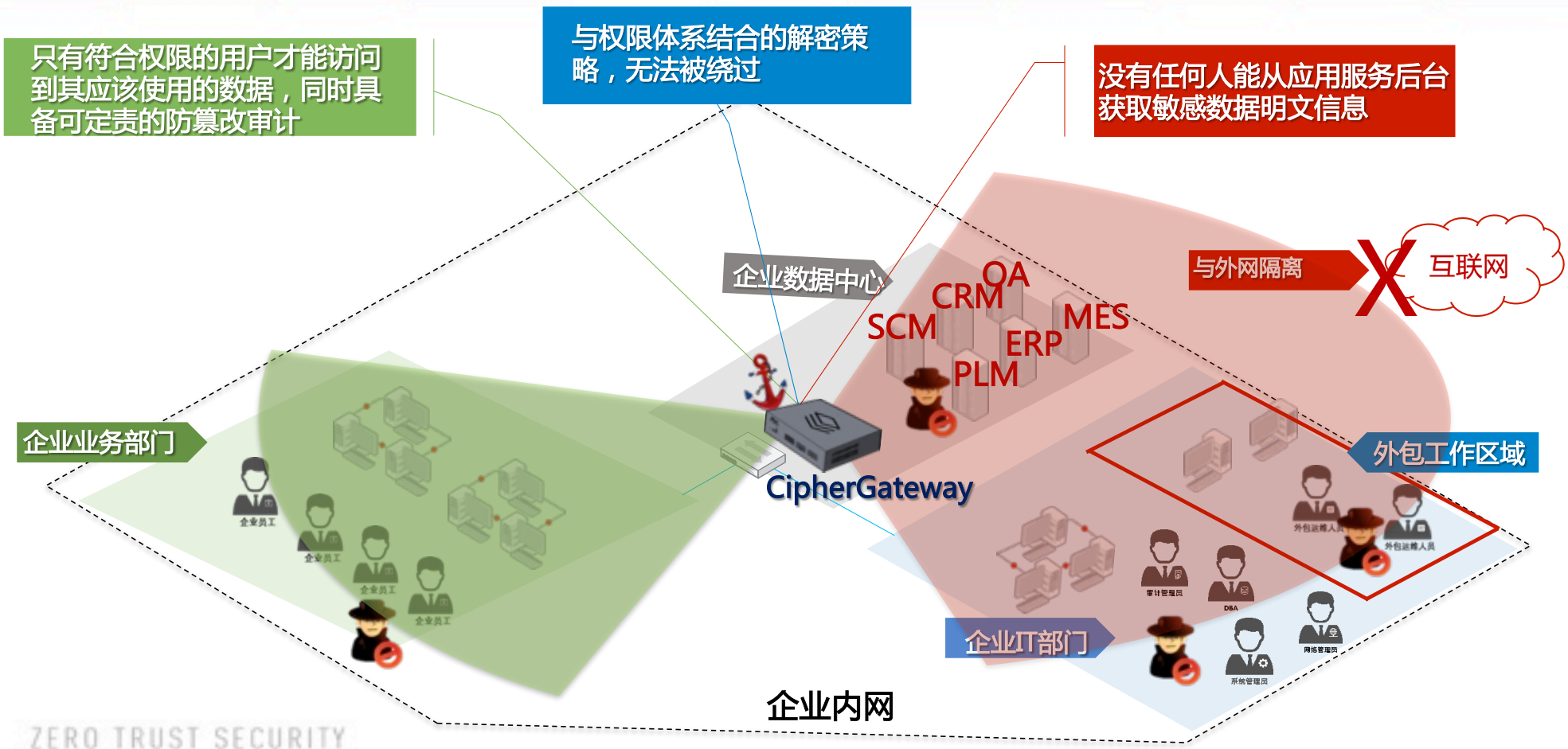
- 万兆级商用密码加解密处理性能
- 对字段或文件提供格式保留加密

将数据安全和威胁防护能力作用到持续变化的业务场景中

场景一：企业内部威胁防护场景

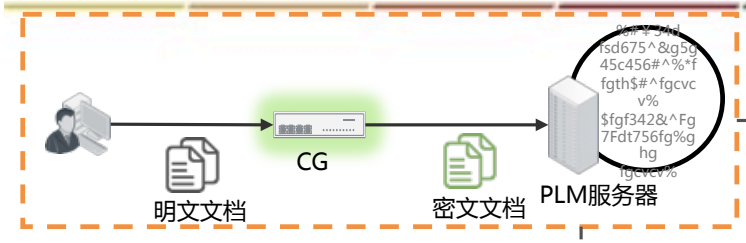


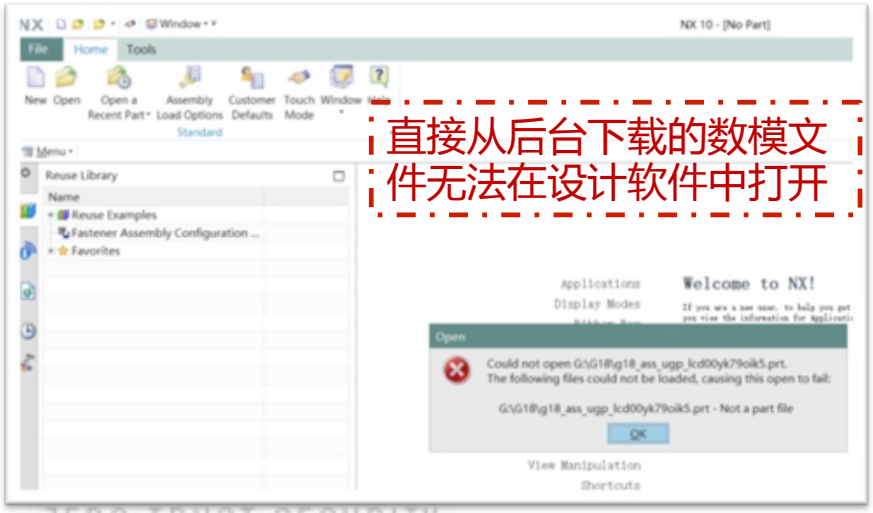
企业应用CASB提供以数据为抓手的零信任安全架构

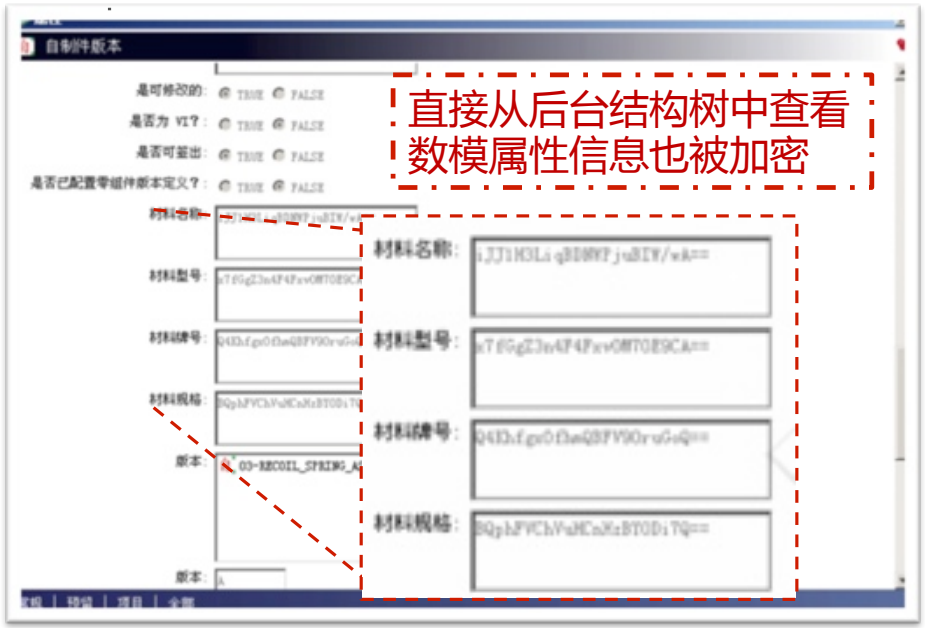


实践：CASB防护PLM数据安全

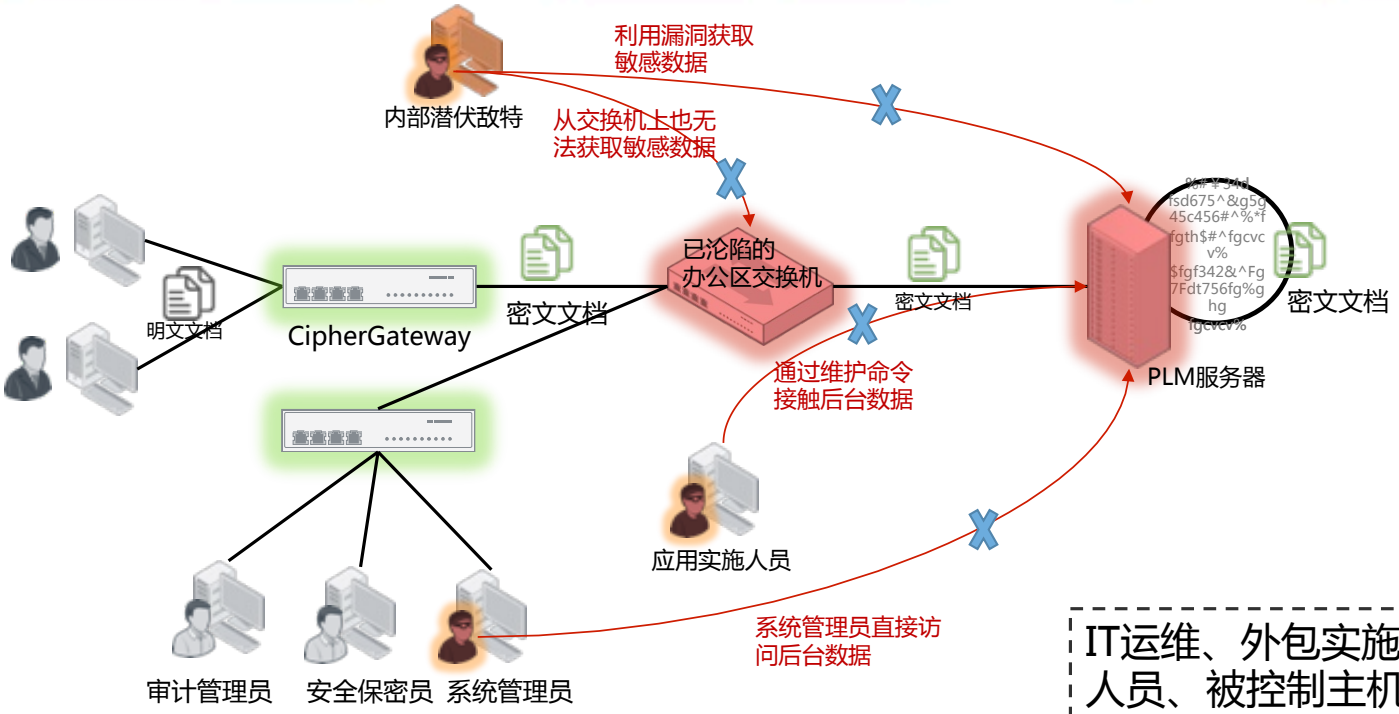
1) 为PLM赋予数据加密能力







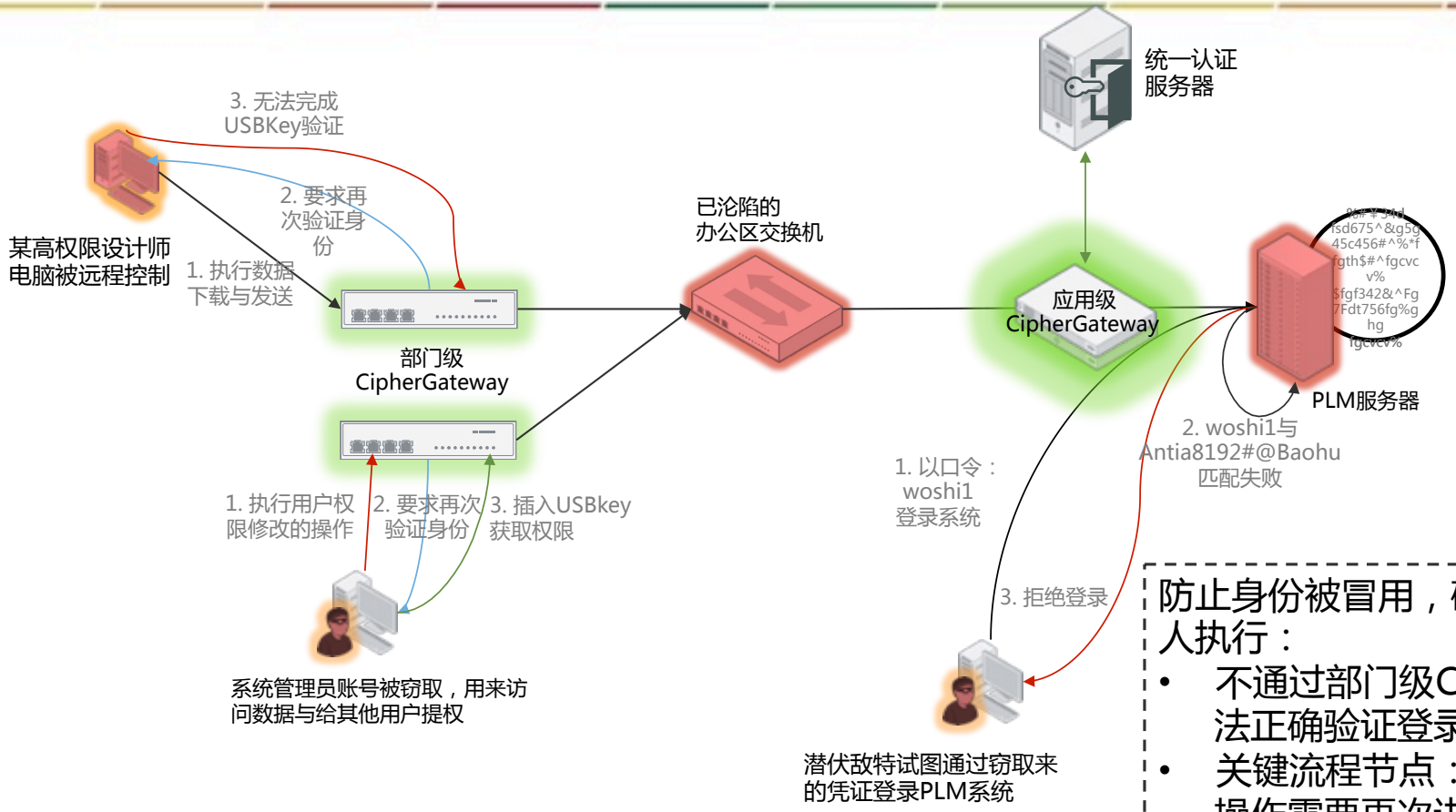
1) 从后台非法获取的敏感数据只有密文



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

2) 增强关键业务操作和数据使用的身份验证

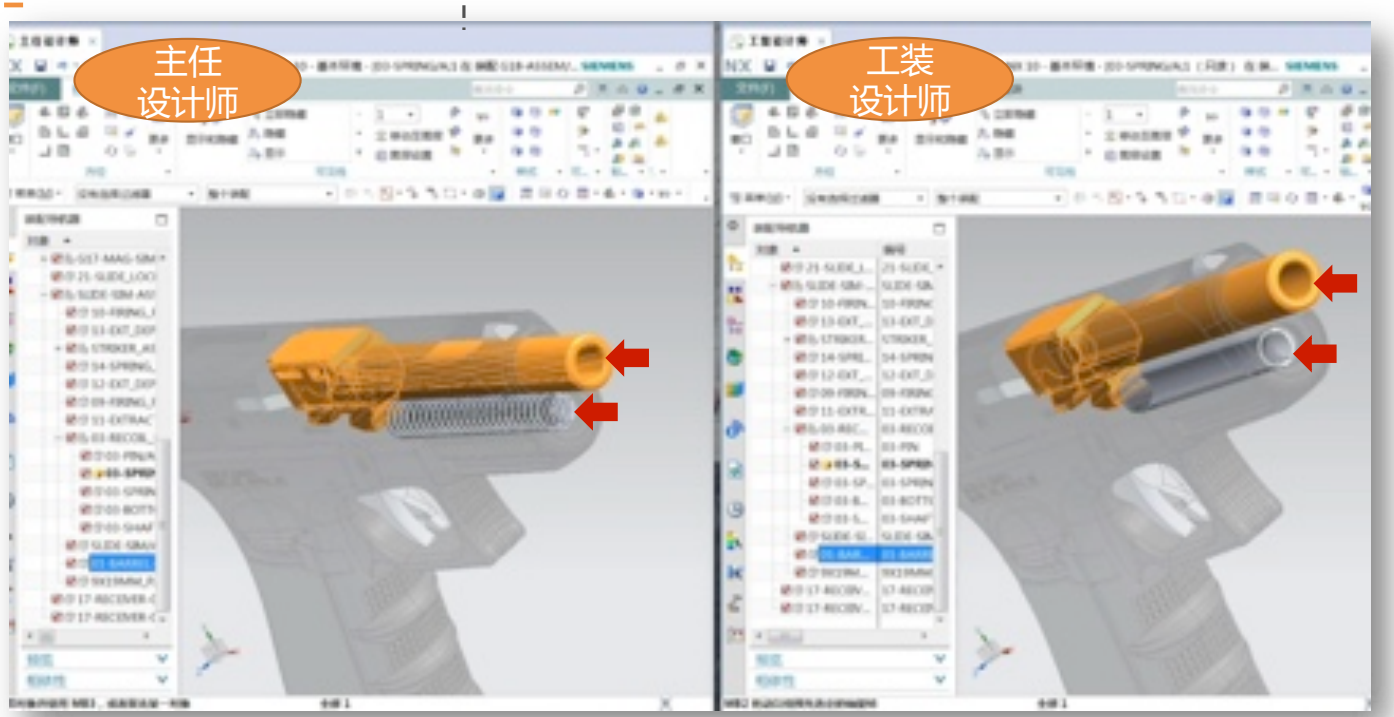


防止身份被冒用，确保操作为用户本人执行：

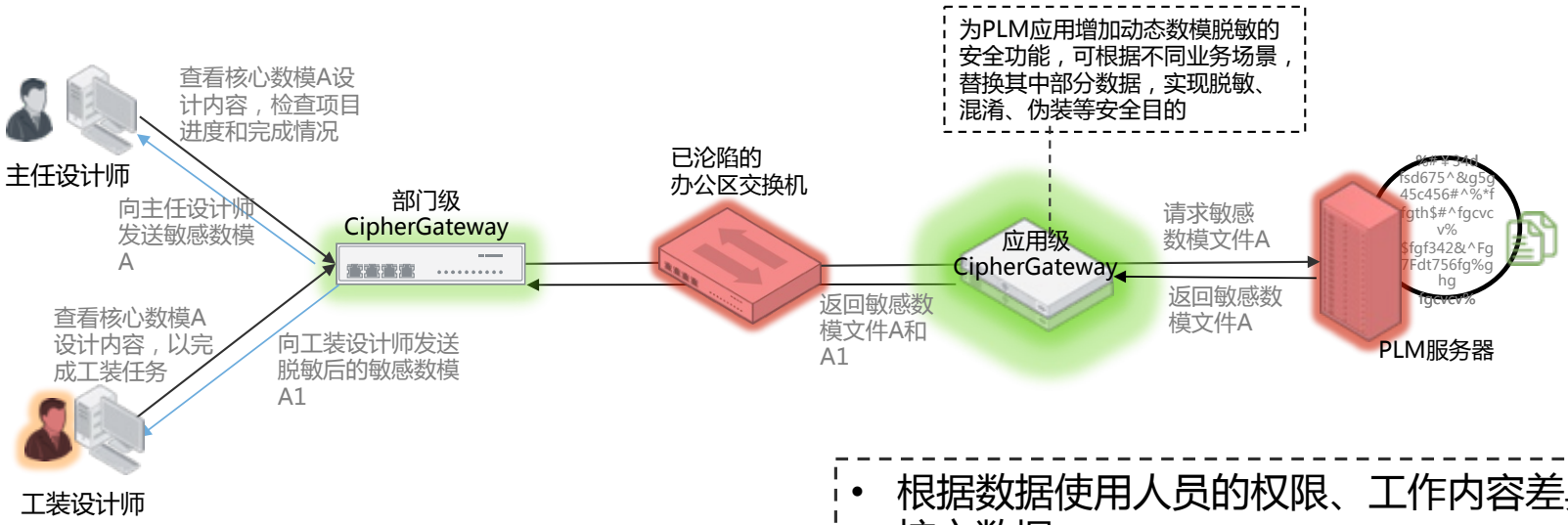
- 不通过部门级CipherGateway无法正确验证登录凭证
- 关键流程节点：敏感操作/异常操作需要再次进行强身份认证

3) 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

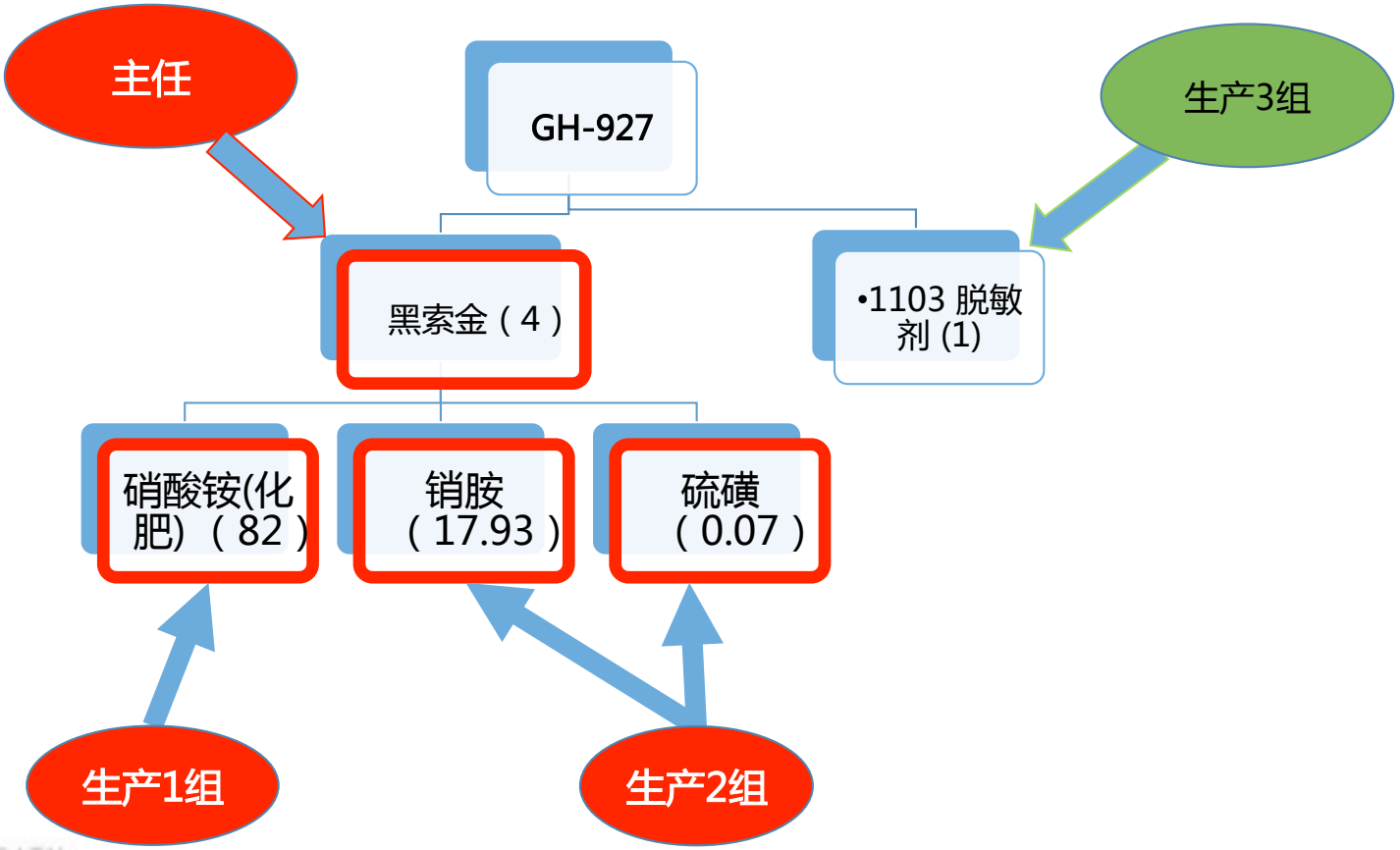


3) 最小化敏感数据阅读范围，迷惑恶意人员

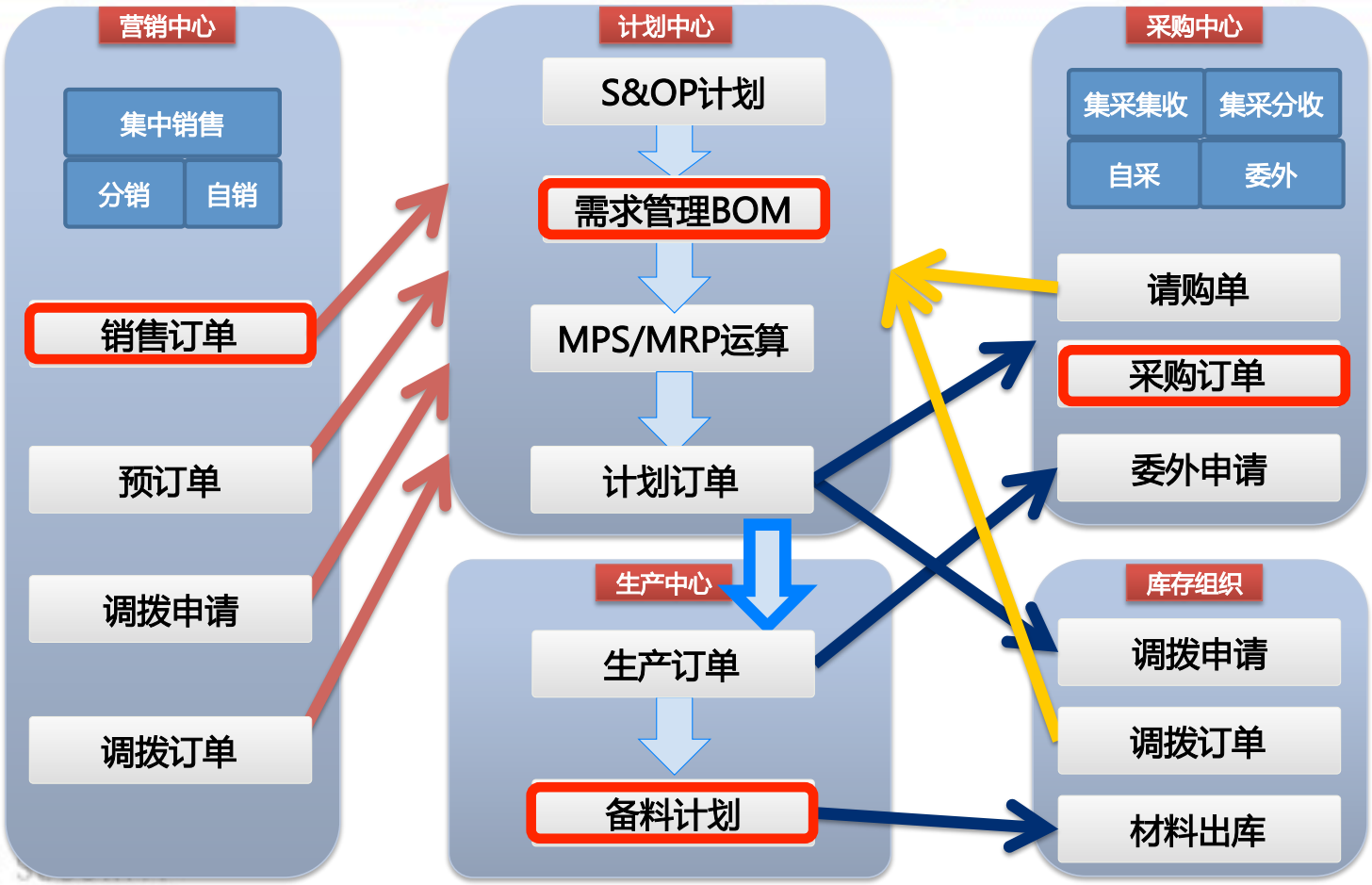


- 根据数据使用人员的权限、工作内容差异，定向脱敏核心数据；
- 对于不应该看到数据却需要数据来工作的员工，仅开放其权限内的数据，或给部分假数据；
- 降低大型项目数据泄露的风险；
- 同时可以针对性投放高仿真欺骗数据，迷惑潜伏敌特；

实践：CASB防护ERP数据安全



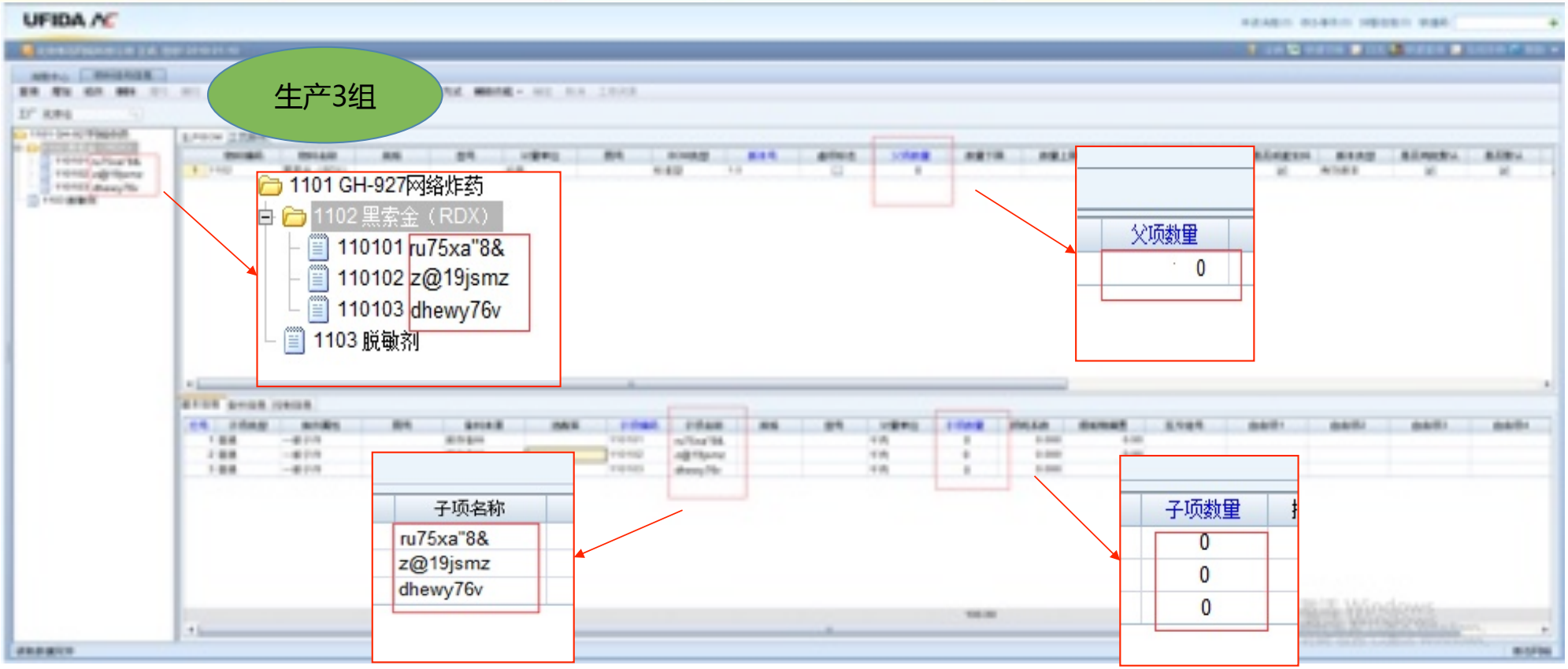
ERP业务流程与核心关键点



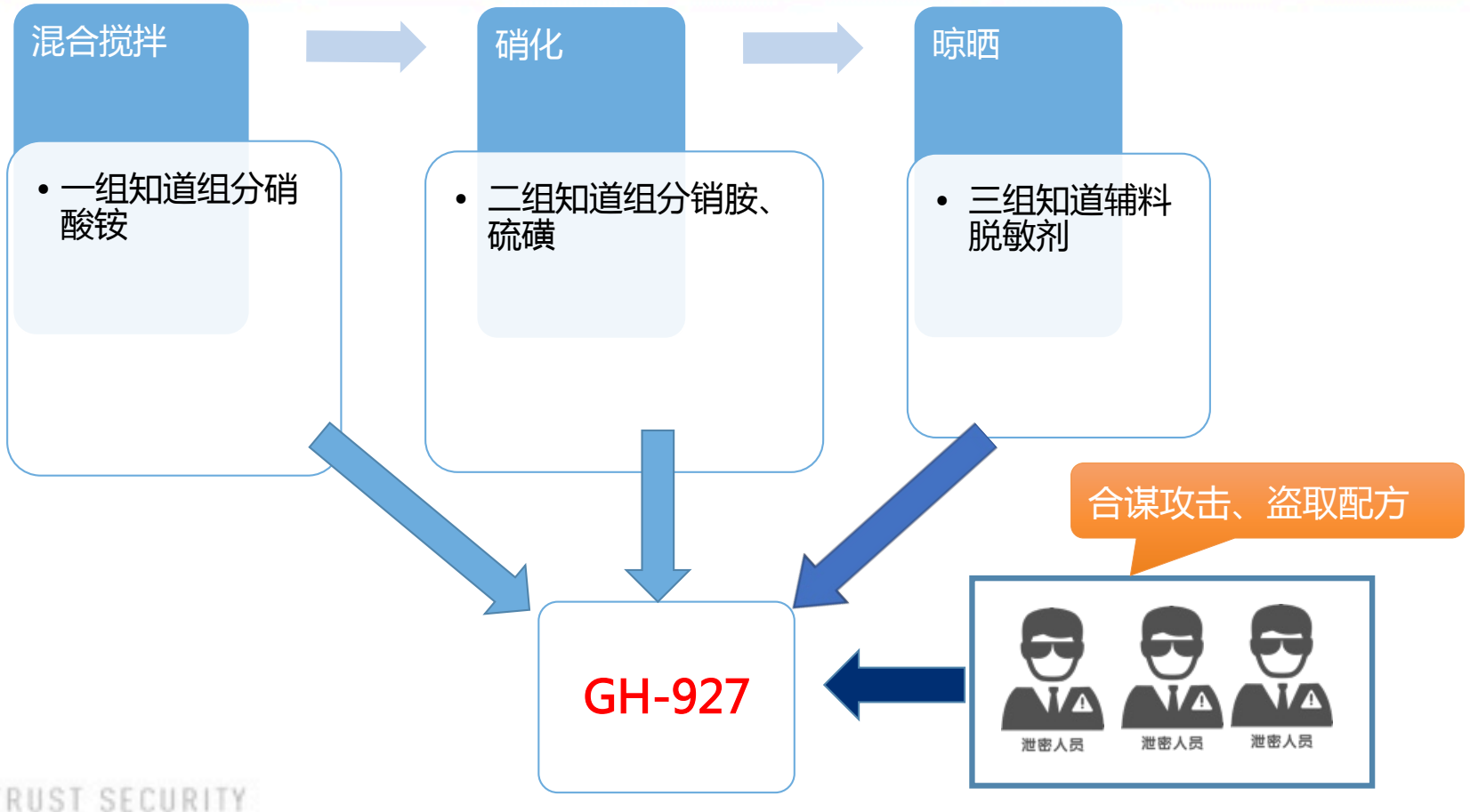
相同单据互斥角色看到不同材料内容

- 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。

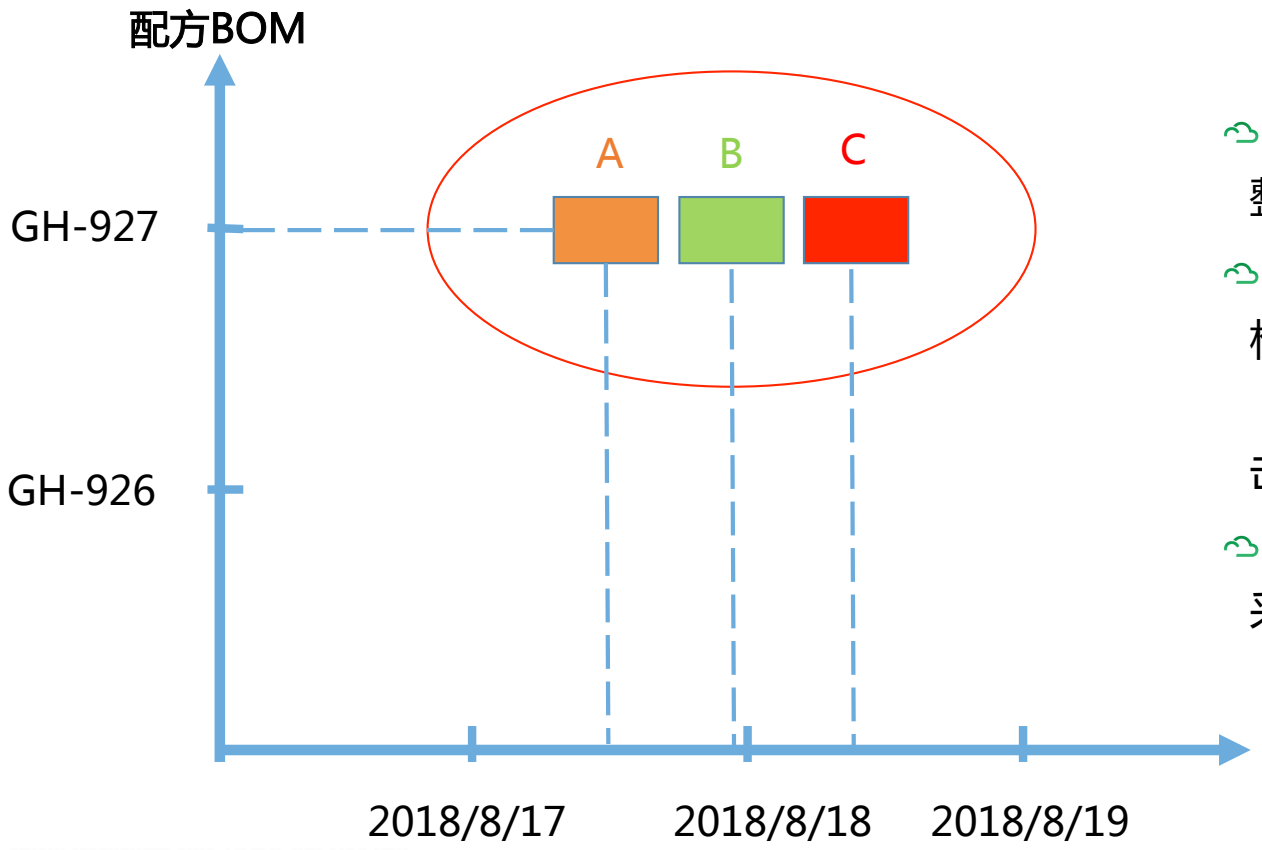
数据权限细控，非相关人员查看数据加密



同一工艺流程中同一配方BOM的不同组分，有不同的知情人



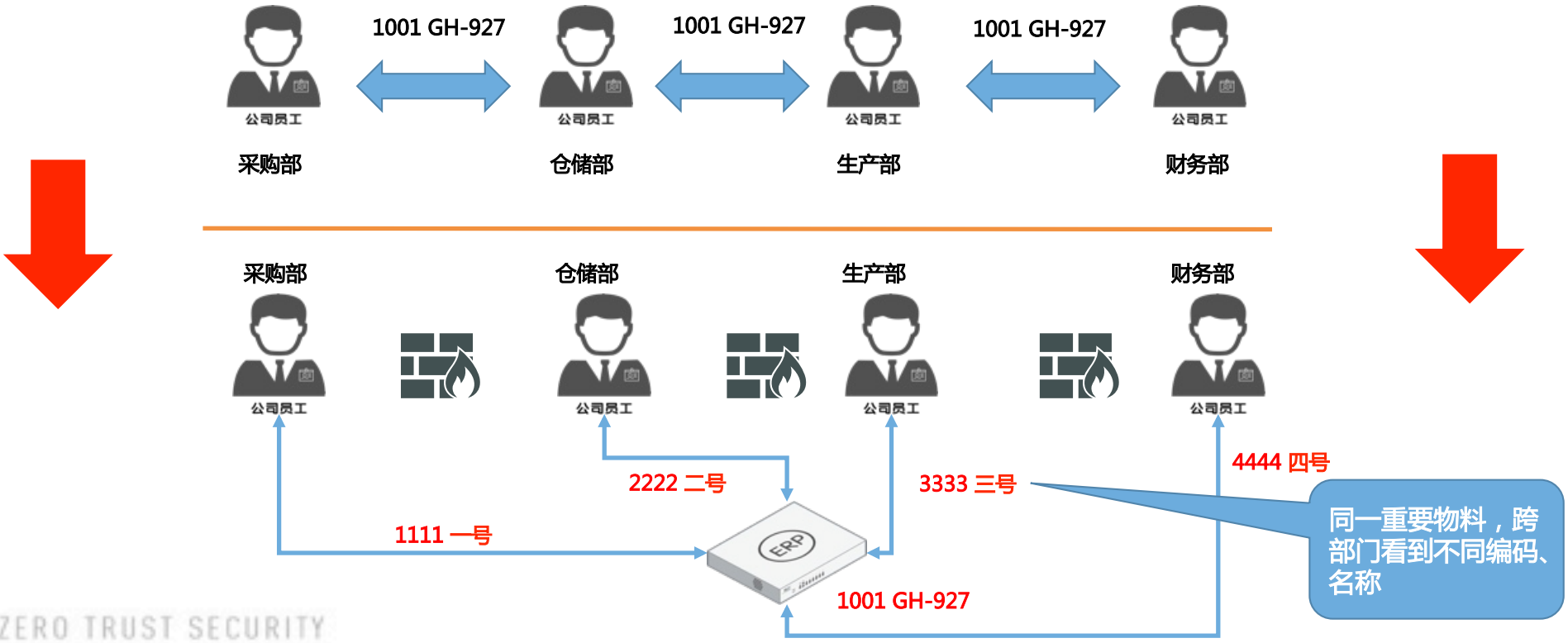
结合配方与人员上下文，感知合谋窃取数据行为



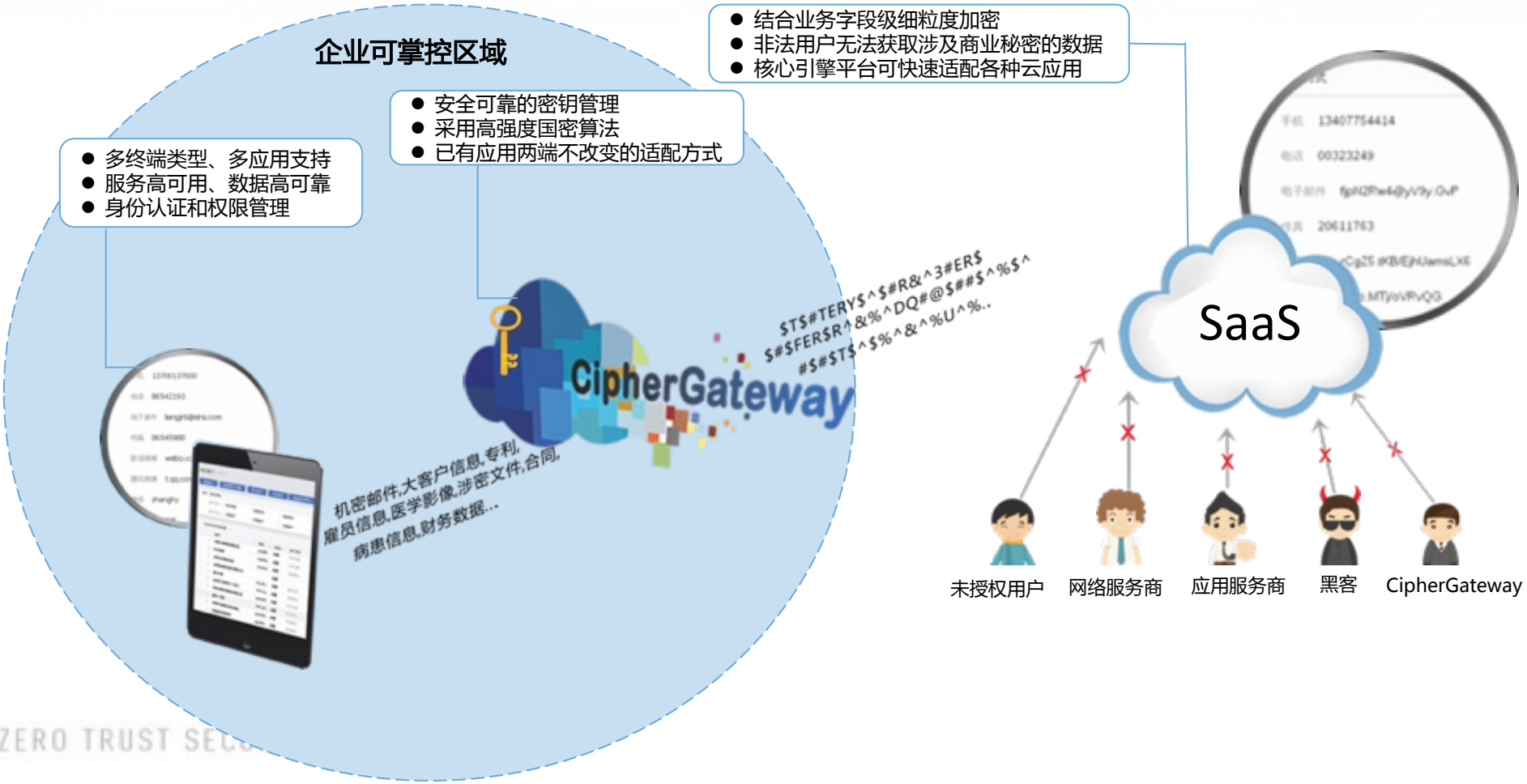
- 企业关键配方也是不断微小调整变化的。
- 当一组、二组、三组不同数据权限的人，在几乎同一时间段，访问同一BOM单时，合谋攻击的倾向非常明显。
- 系统自动对管理员预警，公司采取措施。

智能重造编码，防串通

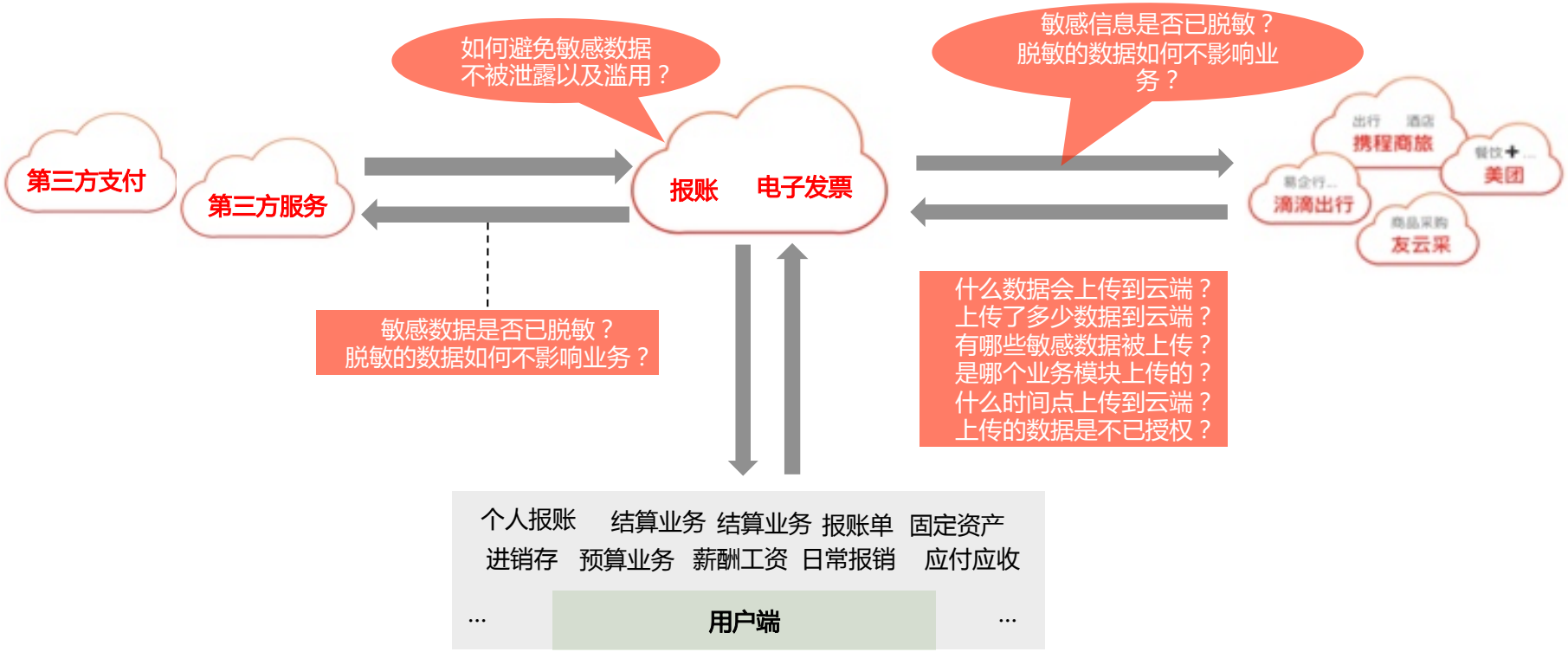
- ERP的业务流程很长，涉及重要敏感的物料的环节很多。
- 最小化各个部门用户数据权限并隔离，通过CG编码转换，避免合谋攻击。



场景二：CASB让用户重获SaaS数据掌控权

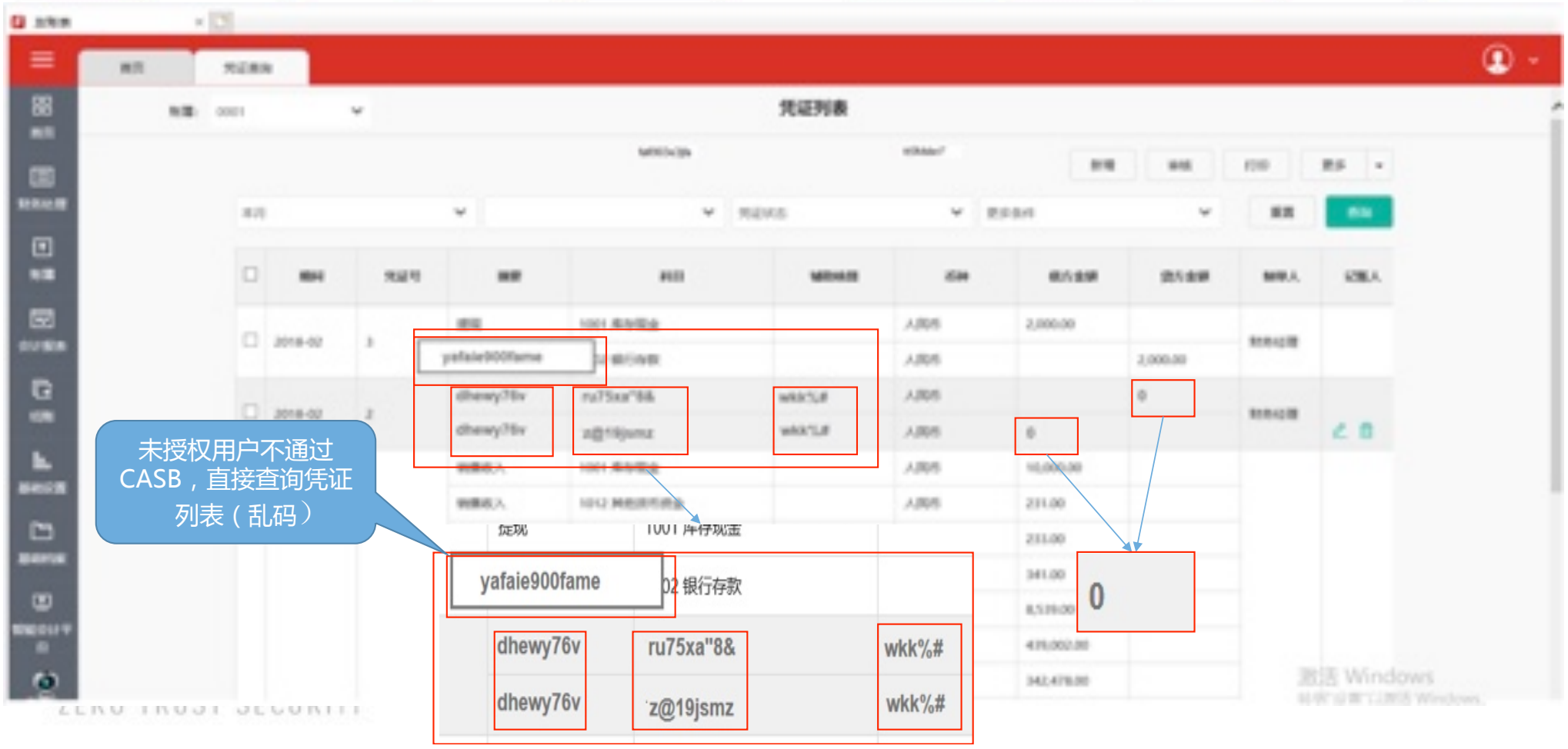


实践：SaaS云端数据安全

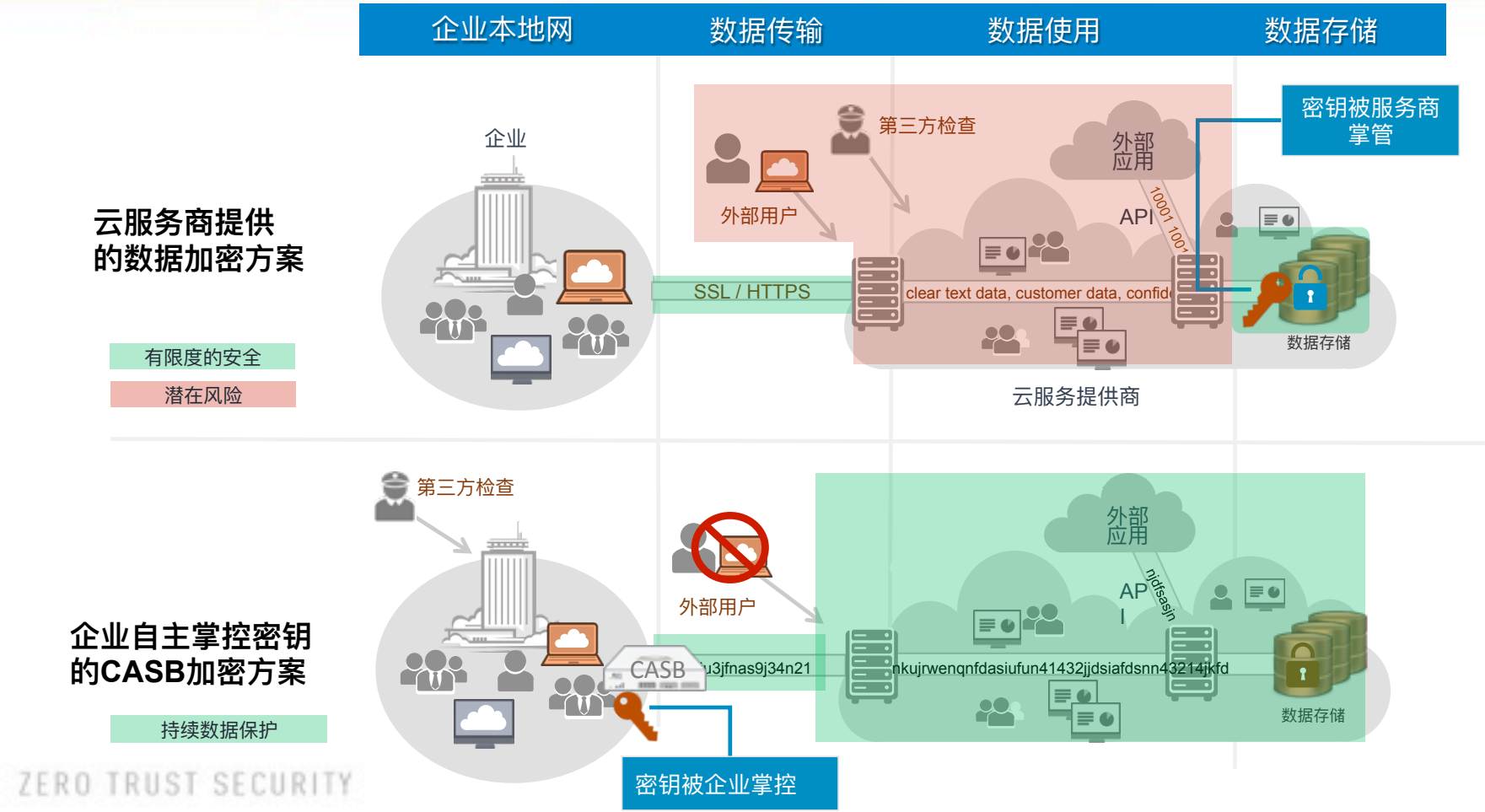


合法用户通过CASB，查询凭证列表

非授权用户数据安全加密



云访问CASB提供了不同的数据安全模型



构筑应用安全生态，保障企业业务发展

【Build Security In】

- 把密码、访问控制、检测分析等安全能力融入到广泛的企业应用系统中，保护国家秘密、商业秘密和公众隐私
- 软件应用与安全行业形成能力融合，共同构筑健康的安全生态

关于我们

炼石 CipherGateway

CG Lab

- 创始团队具有丰富的应用开发、安全、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；

- 愿景：让数字化业务更安全
- 使命：将数据安全适配进业务流程，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【CASB】
  - 可以适配进业务流程的数据安全与威胁防护产品
- CipherSuite密码套件
  - 高效、安全、易用、支持商用密码算法的密码套件


ISC
谢 谢！
2018 ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
（原“中国互联网安全大会”）