



# 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”)



IT大咖说  
知识共享平台

# 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

ZERO TRUST SECURITY

# 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”

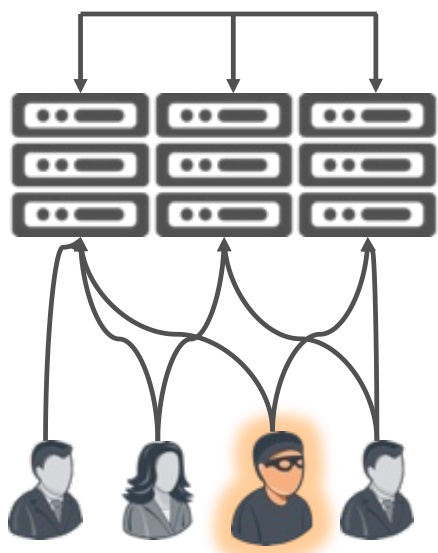
65%

企业发生过严重的  
商业秘密泄露事件

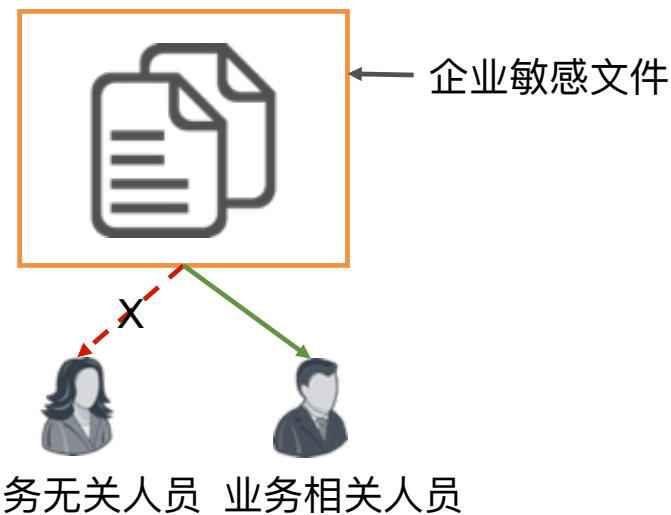
ZERO TRUST SECURITY



# 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

ZERO TRUST SECURITY



# 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”

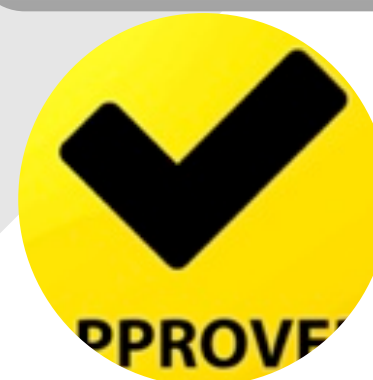


ZERO TRUST SECURITY

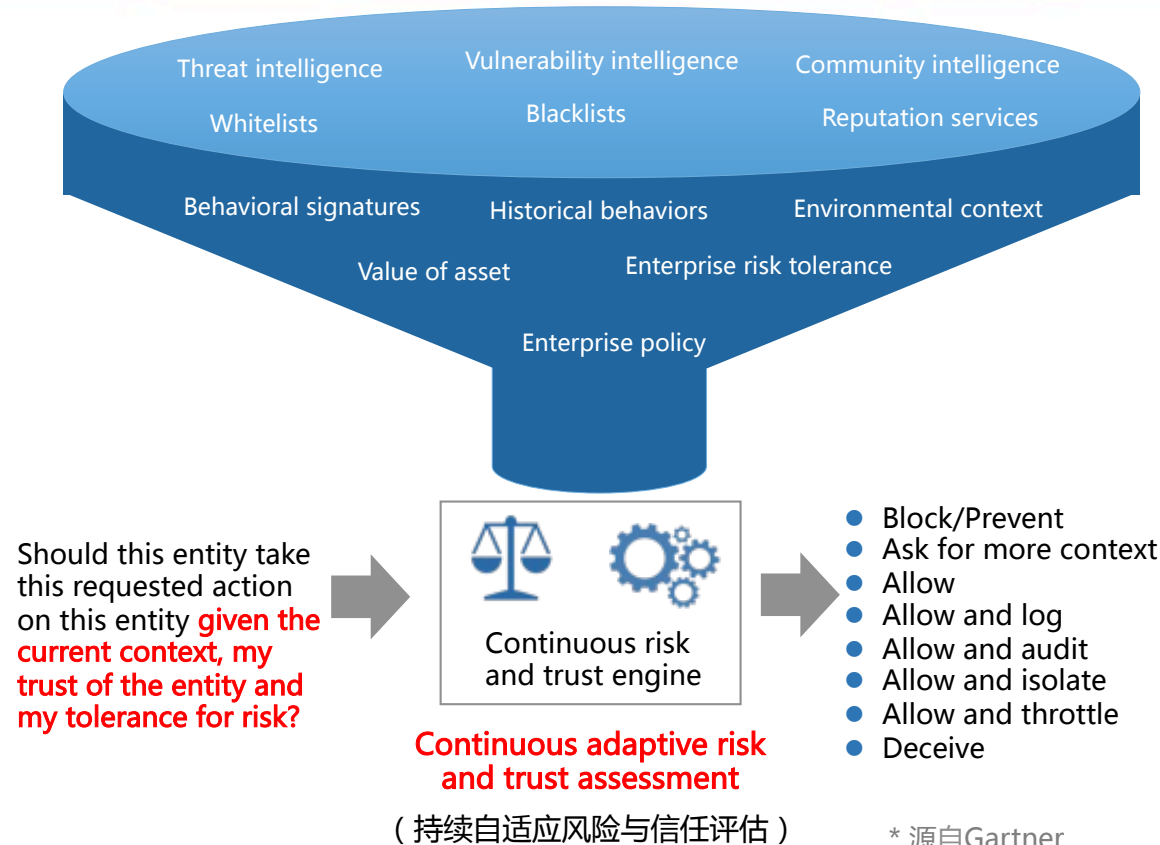
完美防御已然失效，**是否信任不再取决于单个向量，而是取决于场景的上下文**，同时信任与否是动态的，会随着业务场景持续变化



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



# CARTA主张结合业务上下文评估风险



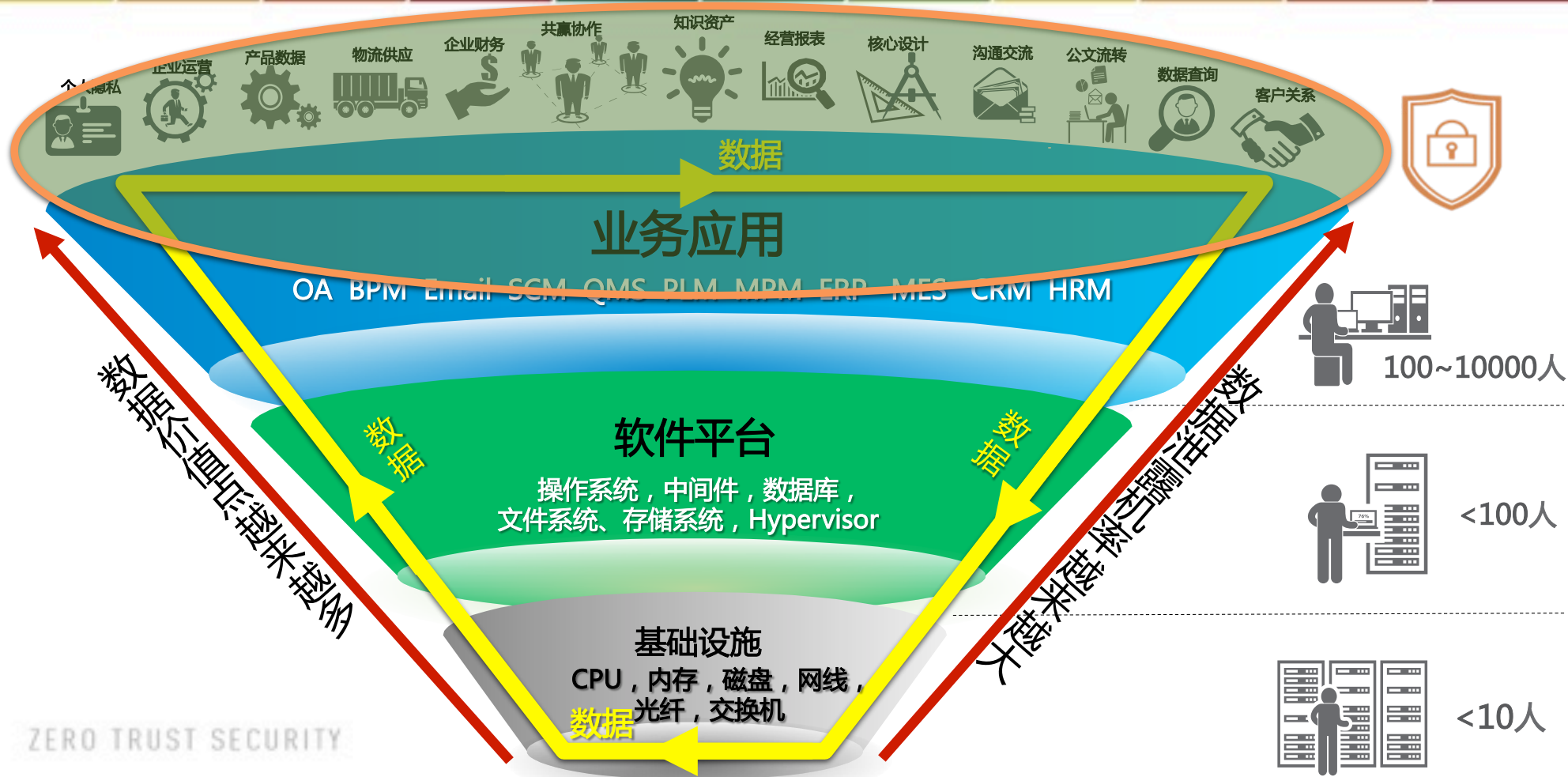
## CARTA核心要素

- 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

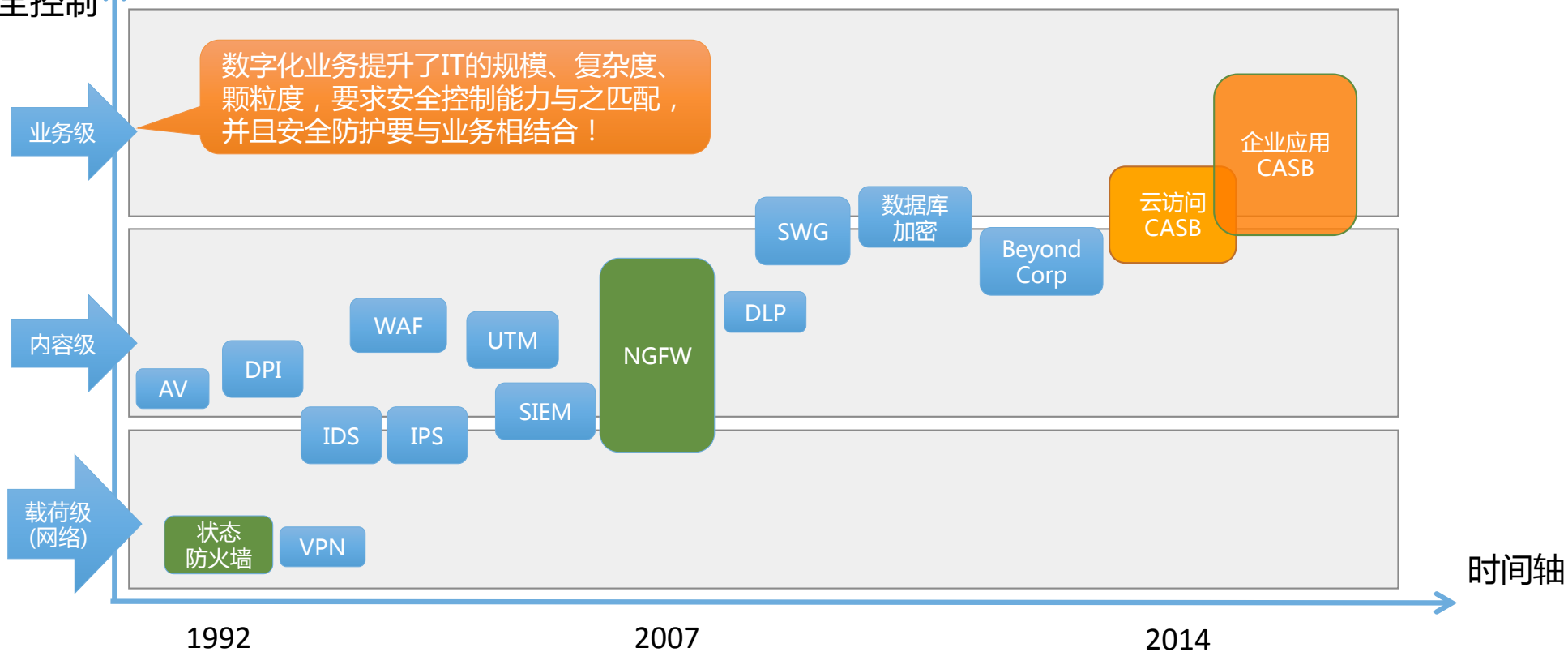




# IT技术发展带来新威胁，推动安全产品向细粒度演进



更细粒度  
安全控制



ZERO TRUST SECURITY

# “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	委托式代理	经纪人	Broker Encrypt Business platform	CASB	云安全/内部威胁防护
内容级	Content-awareness	Intra-request	Proxy	转发式代理	快递员	Proxy	DPI/NGFW/WAF/IPS	外网管控/互联网安全
载荷级(网络)	Payload-awareness	Intra-part-request	Filter	封包/替换/阻断	门卫	Filter	VPN网关/IPS/NGFW	内外网隔离/内网监控

ZERO TRUST SECURITY

# CASB将丰富安全能力施加到业务级



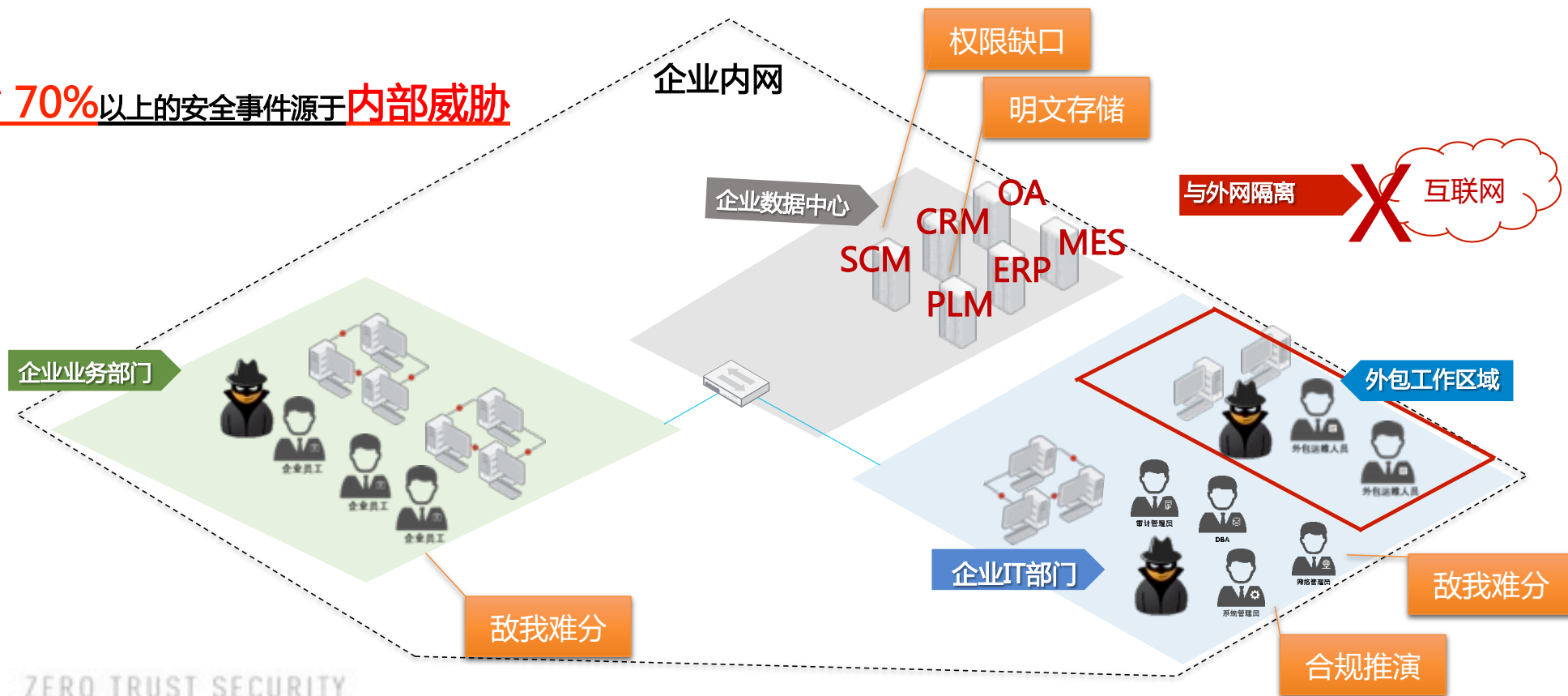
## 企业应用安全代理 (Corp Application Security Broker) & 云访问安全代理 (Cloud Access Security Broker)



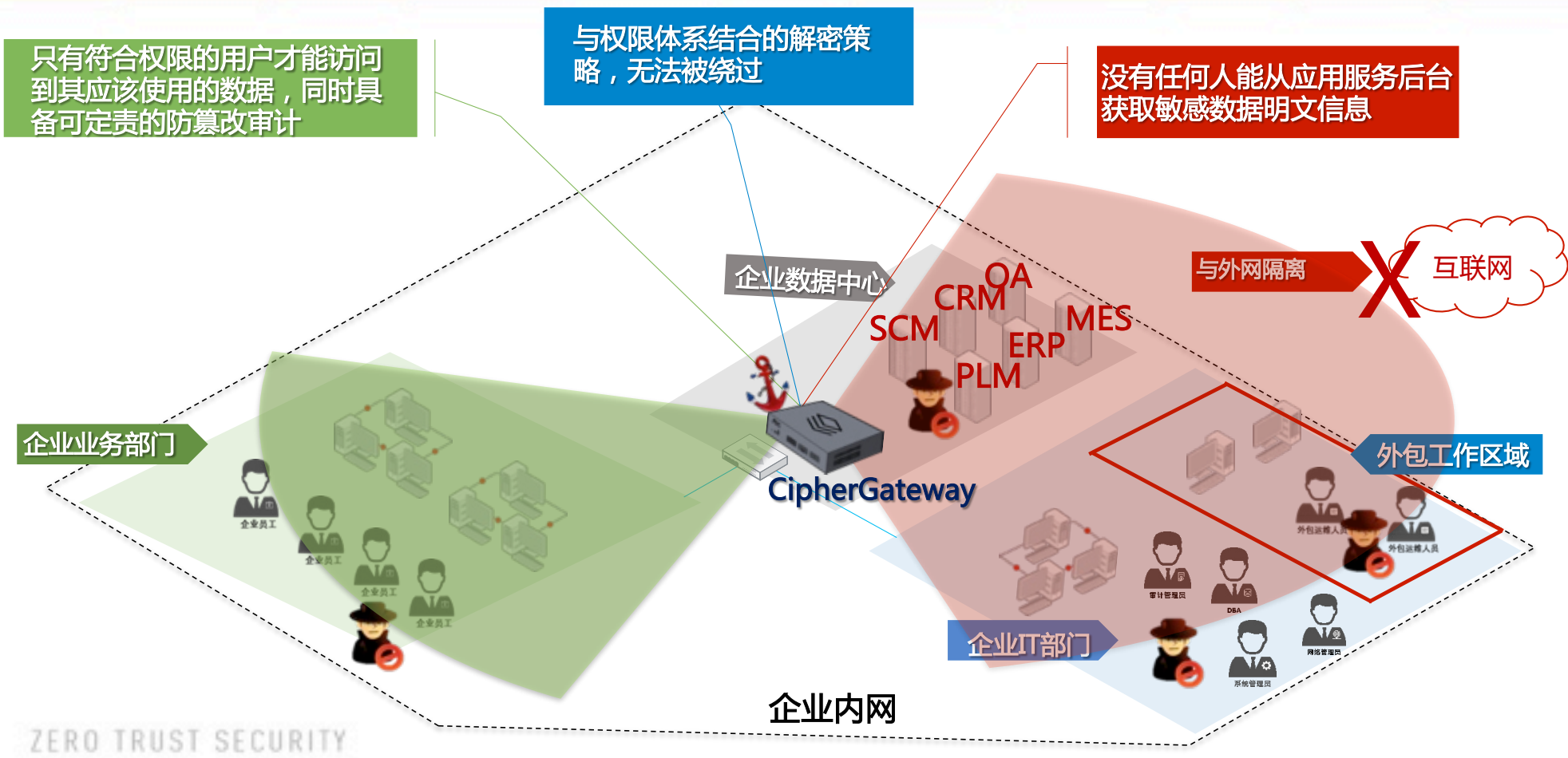
# 场景一：企业内部威胁防护场景



\* 70%以上的安全事件源于**内部威胁**



# 企业应用CASB提供以数据为抓手的零信任安全架构



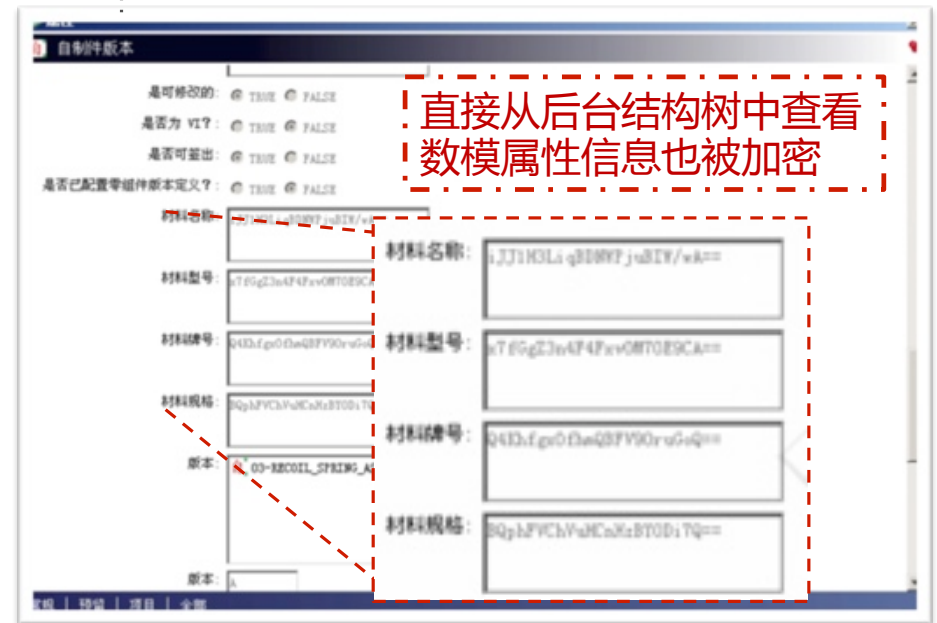
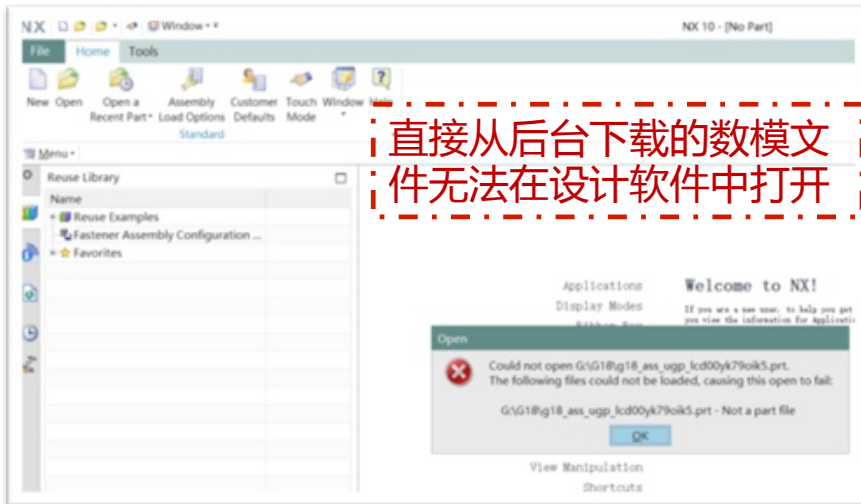
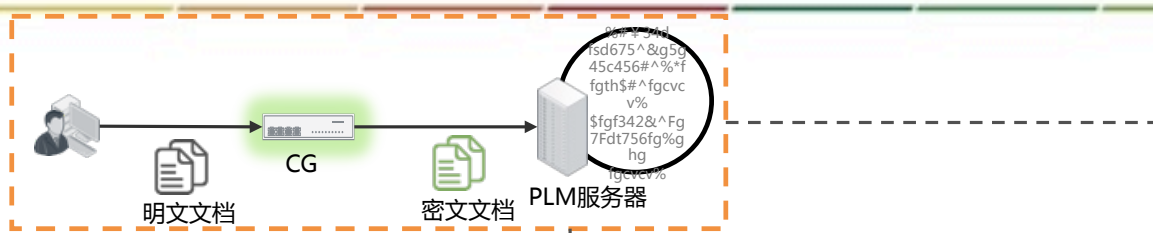


# 实践：CASB防护PLM数据安全

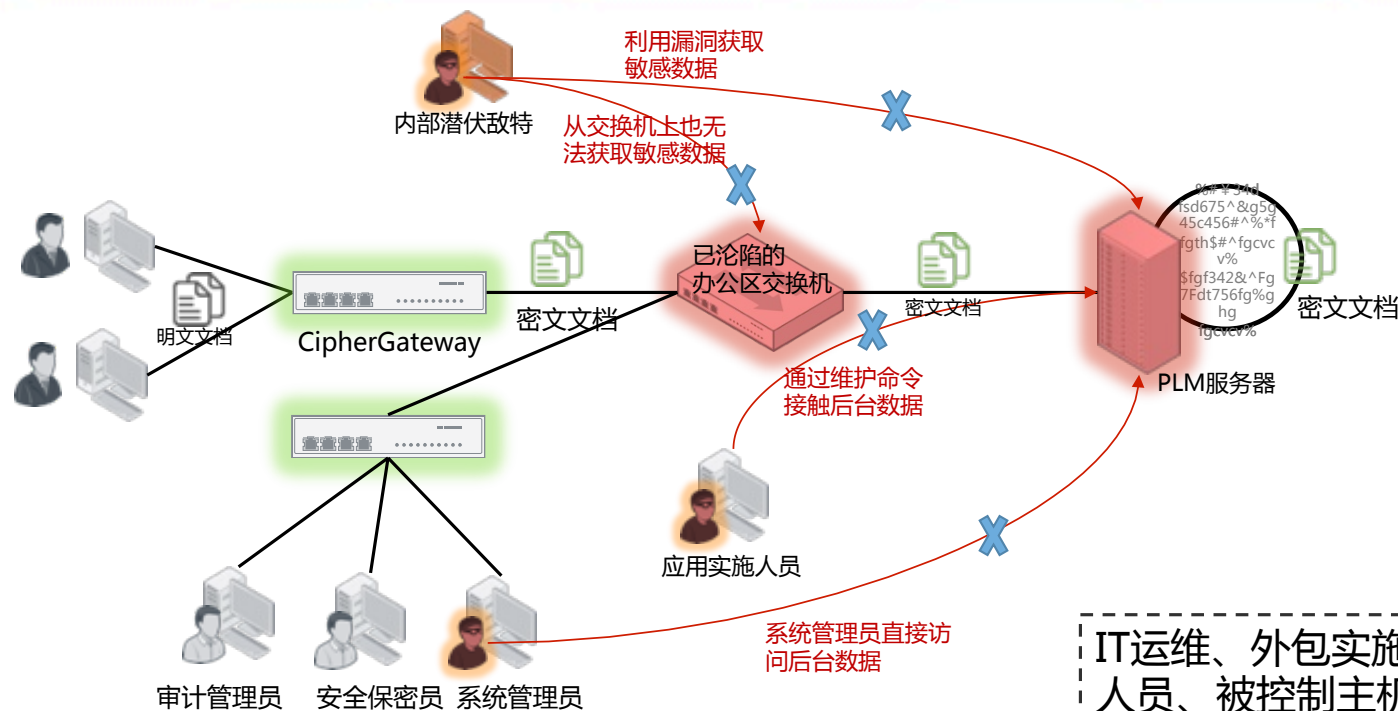


ZERO TRUST SECURITY

# 1) 为PLM赋予数据加密能力

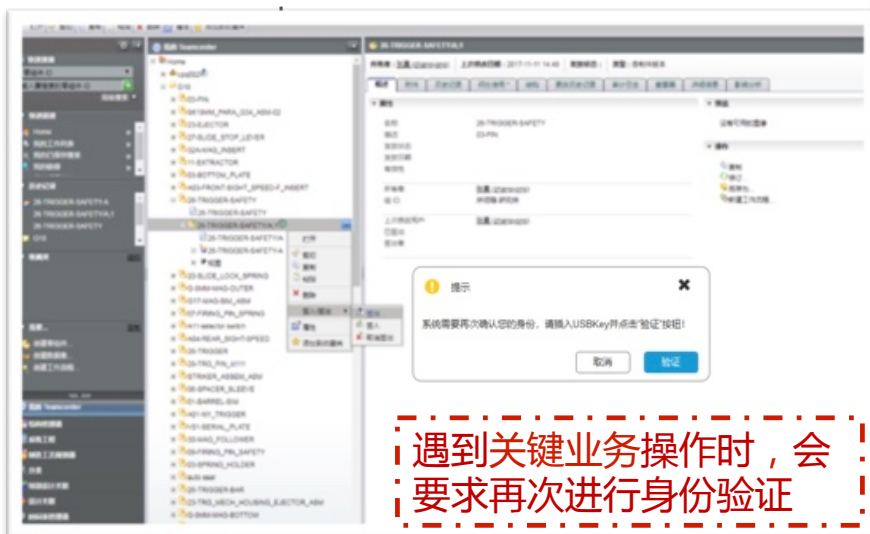
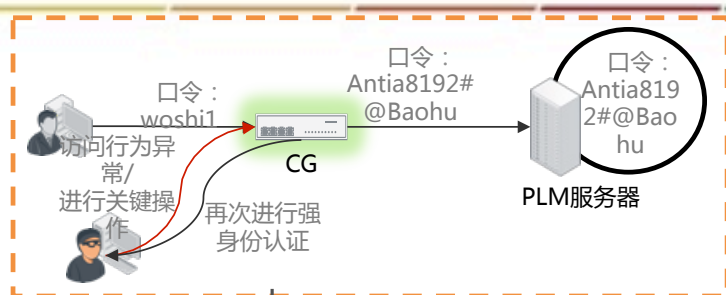


# 1) 从后台非法获取的敏感数据只有密文

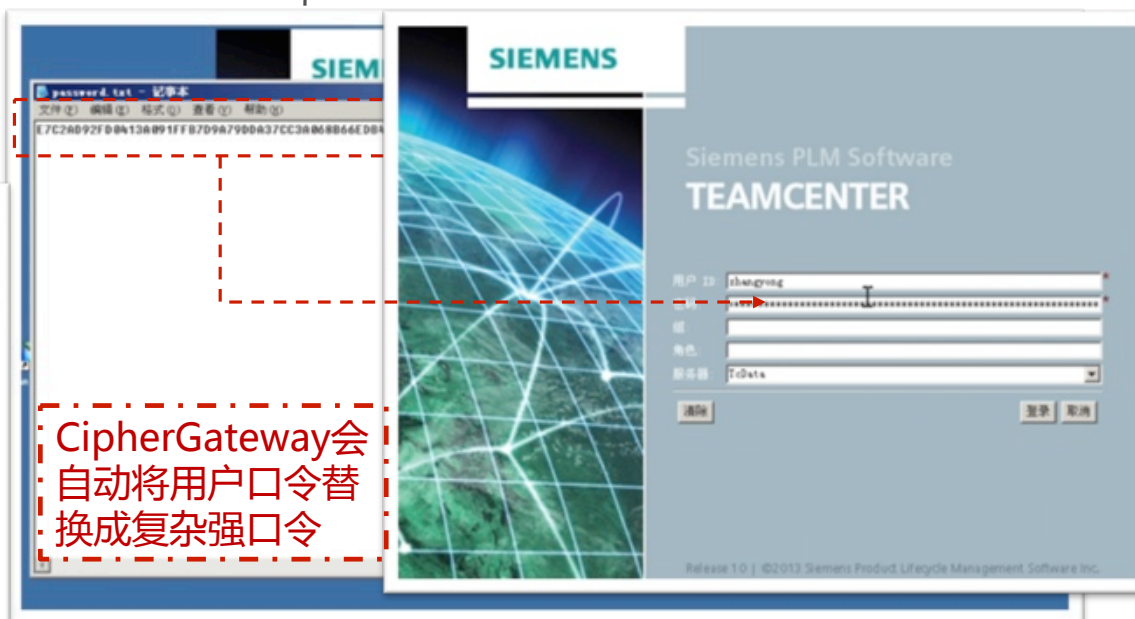


IT运维、外包实施、管理员、内部恶意人员、被控制主机、特木等人员和手段均无法直接从后台获取敏感数据

## 2) 杜绝关键操作时身份被冒用

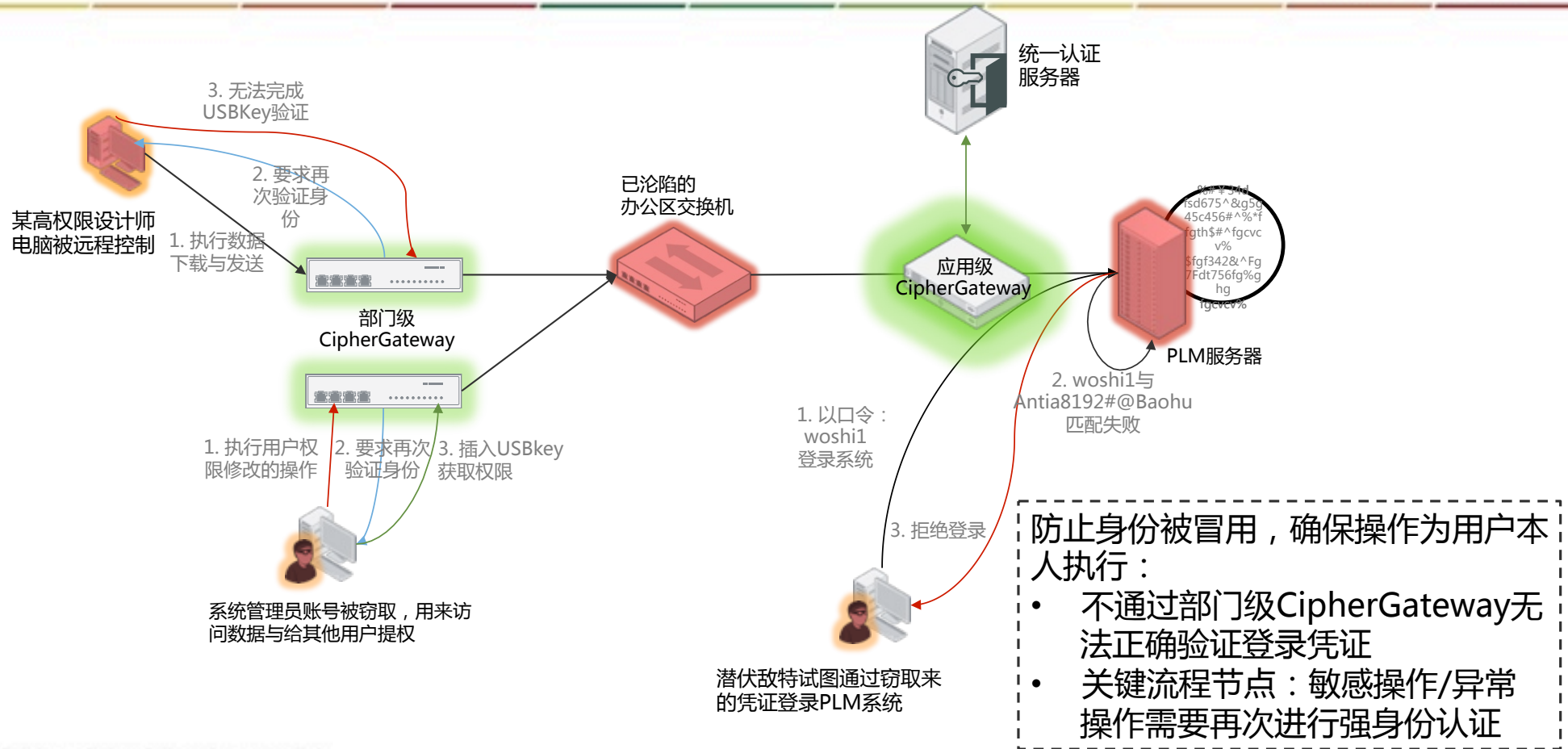


遇到关键业务操作时，会  
要求再次进行身份验证



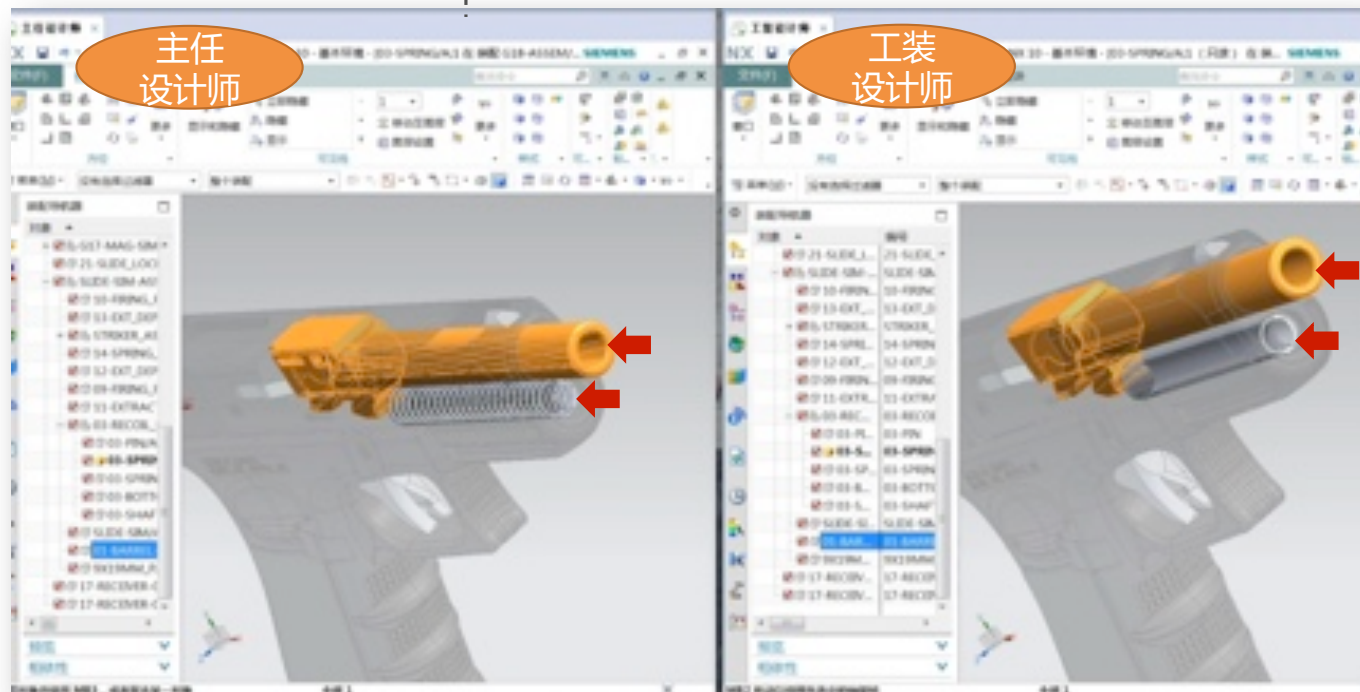
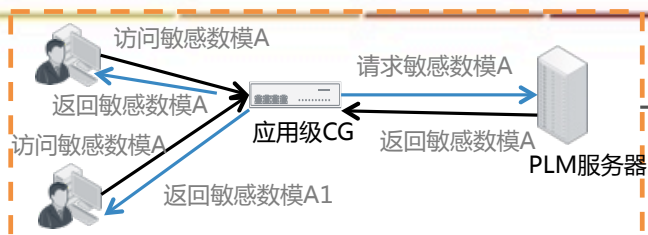
CipherGateway会自动将用户口令替换成复杂强口令

## 2) 增强关键业务操作和数据使用的身份验证



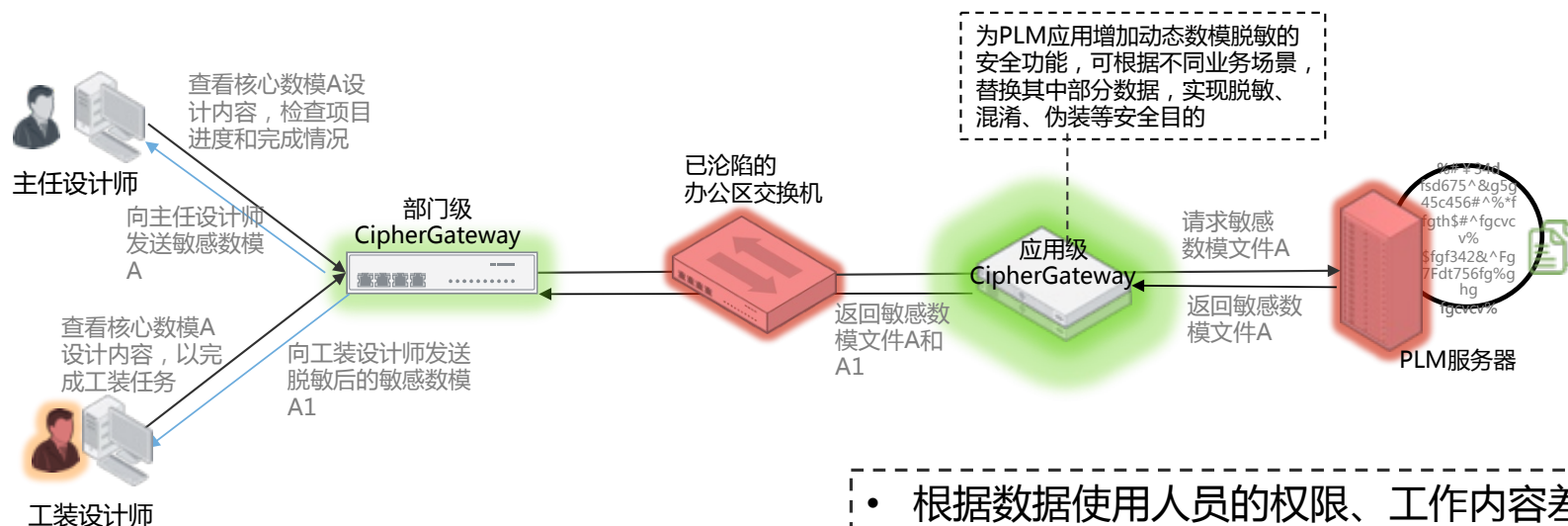


### 3) 深度结合数据使用的脱敏机制



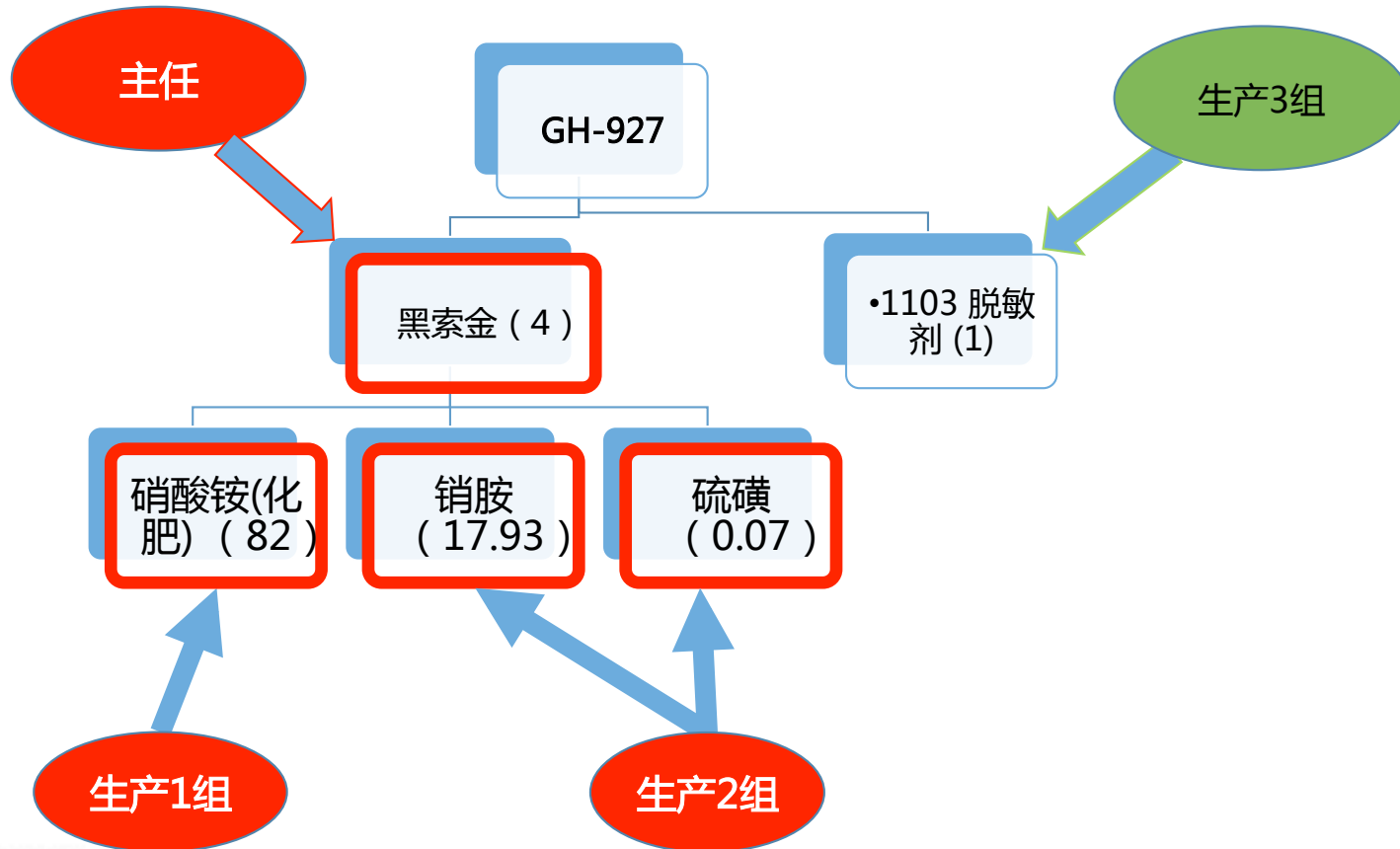
基于人员权限和策略，对没有权限的人进行定向脱敏，对“内鬼”或潜伏在内部的敌特人员，提供欺骗数据

### 3) 最小化敏感数据阅读范围，迷惑恶意人员



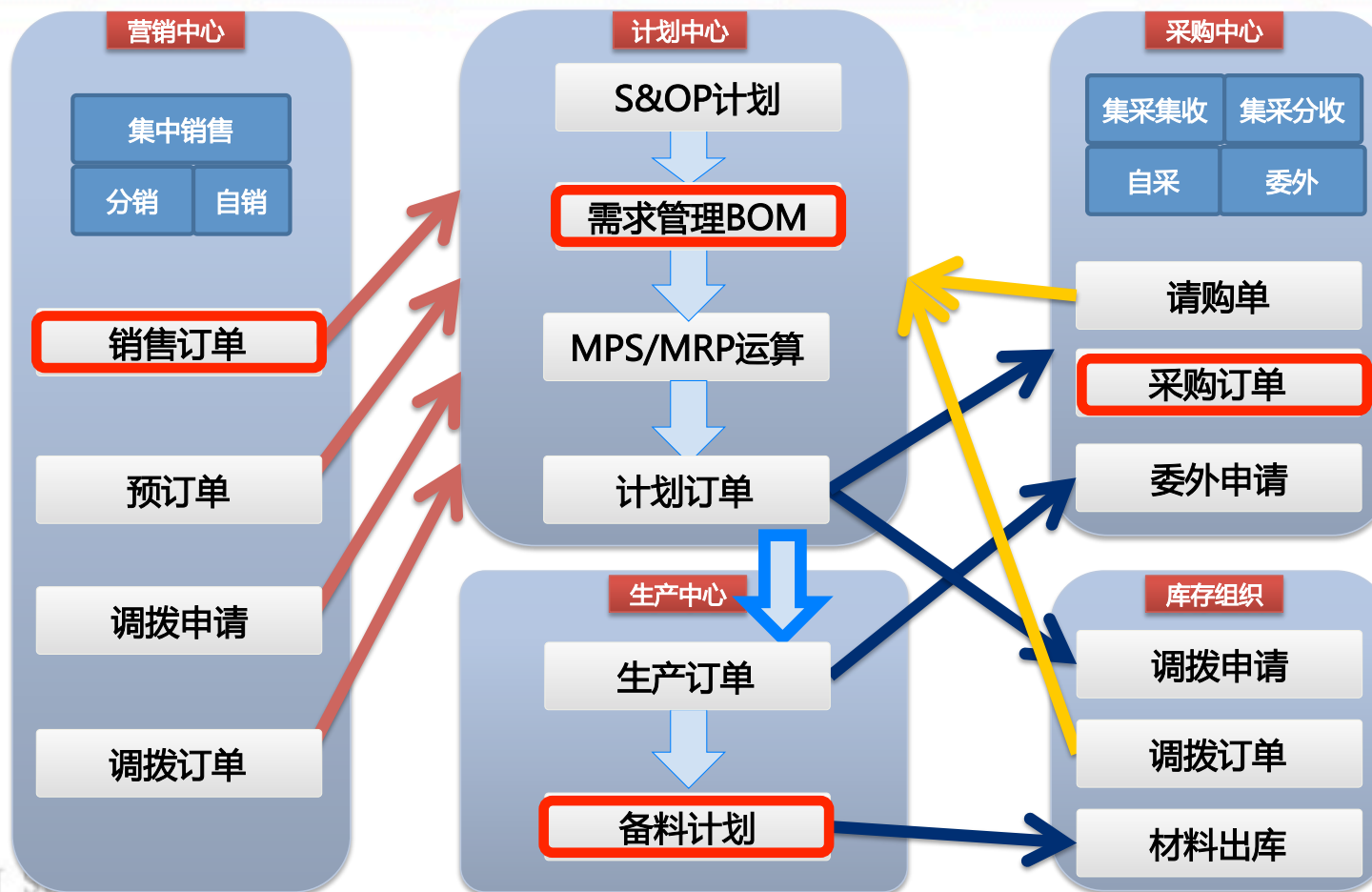
- 根据数据使用人员的权限、工作内容差异，定向脱敏核心数据；
- 对于不应该看到数据却需要数据来工作的员工，仅开放其权限内的数据，或给部分假数据；
- 降低大型项目数据泄露的风险；
- 同时可以针对性投放高仿真欺骗数据，迷惑潜伏敌特；

# 实践：CASB防护ERP数据安全



ZERO TRUST SECURITY

# ERP业务流程与核心关键点



ZERO TRUST S

# 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。

**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	辅计划出库数量	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	硝胺	1
3 110103	硫磺	1

材料名称
ru75xa"8&
硝胺
硫磺

计划出库数量
0
17.93
0.07

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



# 数据权限细控，非相关人员查看数据加密



生产3组

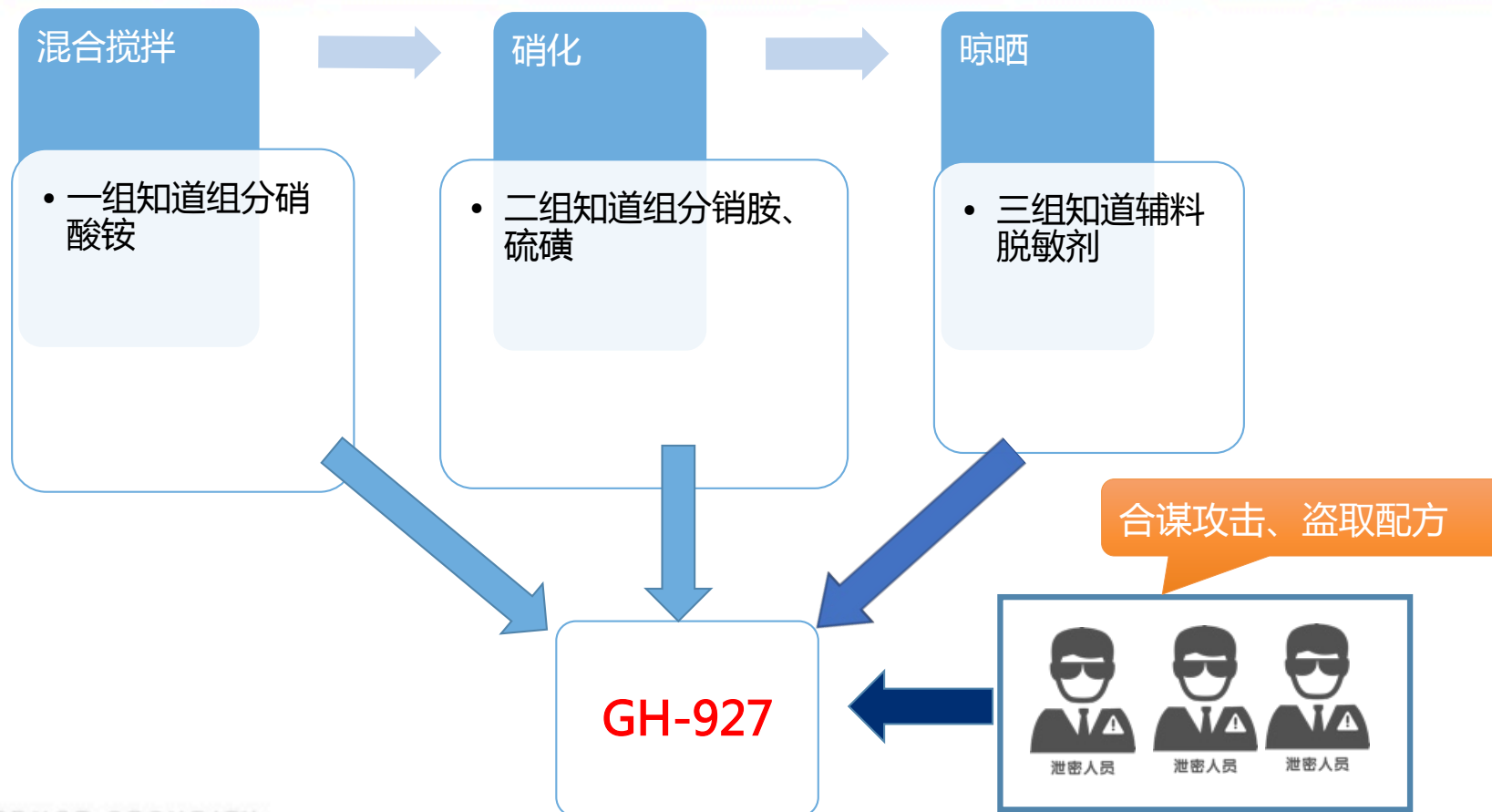
1101 GH-927网络炸药  
1102 黑索金 (RDX)  
110101 ru75xa"8&  
110102 z@19jsmz  
110103 dhewy76v  
1103 脱敏剂

父项数量
0

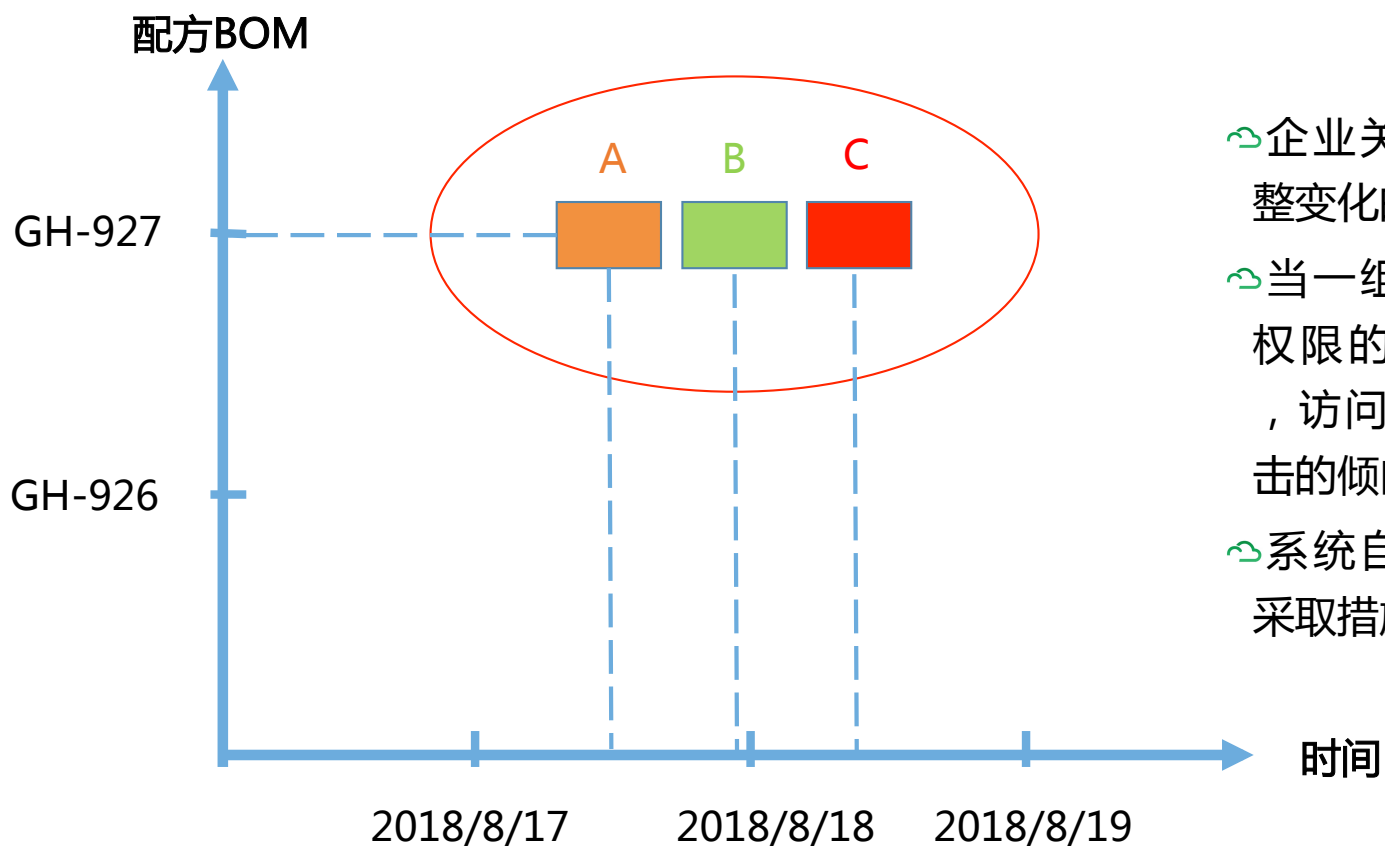
子项名称
ru75xa"8&
z@19jsmz
dhewy76v

子项数量
0
0
0

# 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

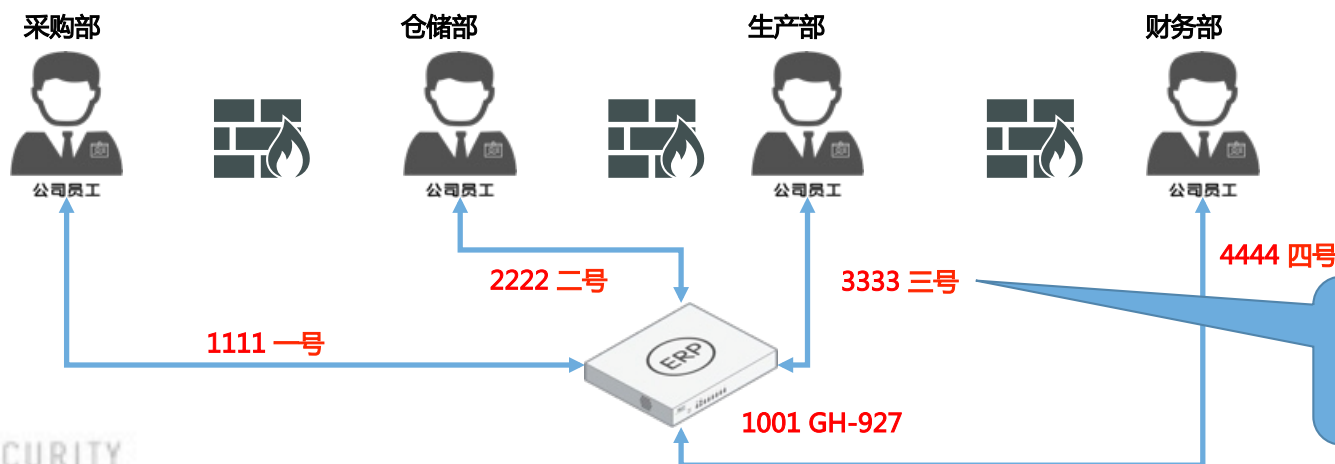
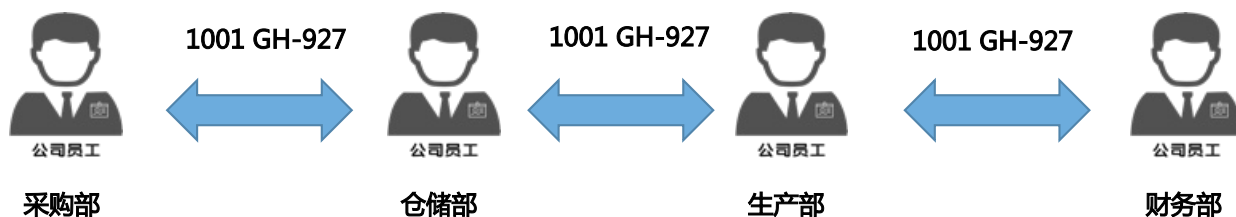


- 企业关键配方也是不断微小调整变化的。
- 当一组、二组、三组不同数据权限的人，在几乎同一时间段，访问同一BOM单时，合谋攻击的倾向非常明显。
- 系统自动对管理员预警，公司采取措施。

# 智能重造编码，防串通

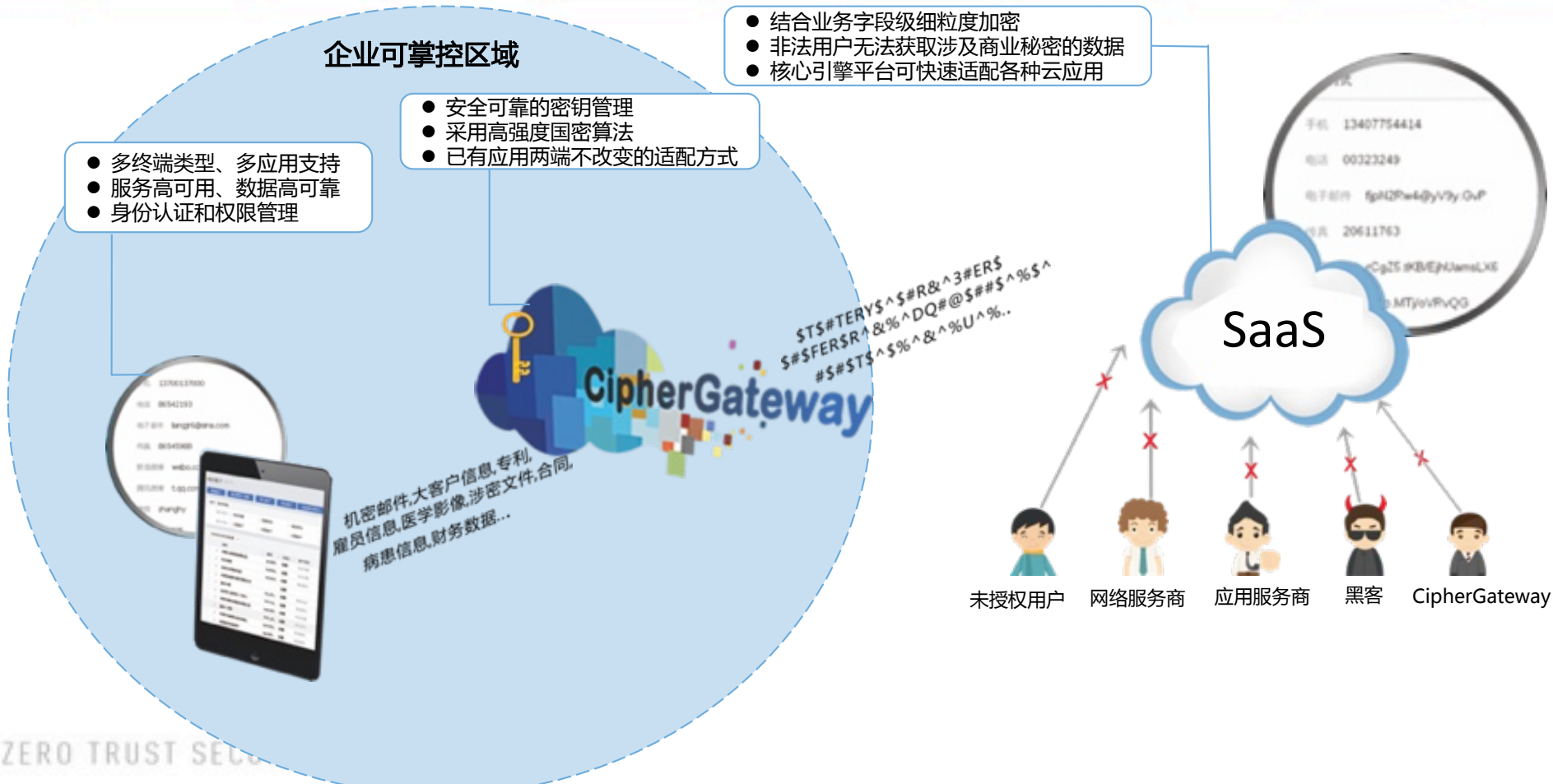


- ERP的业务流程很长，涉及重要敏感的物料环节很多。
- 最小化各个部门用户数据权限并隔离，通过CG编码转换，避免合谋攻击。



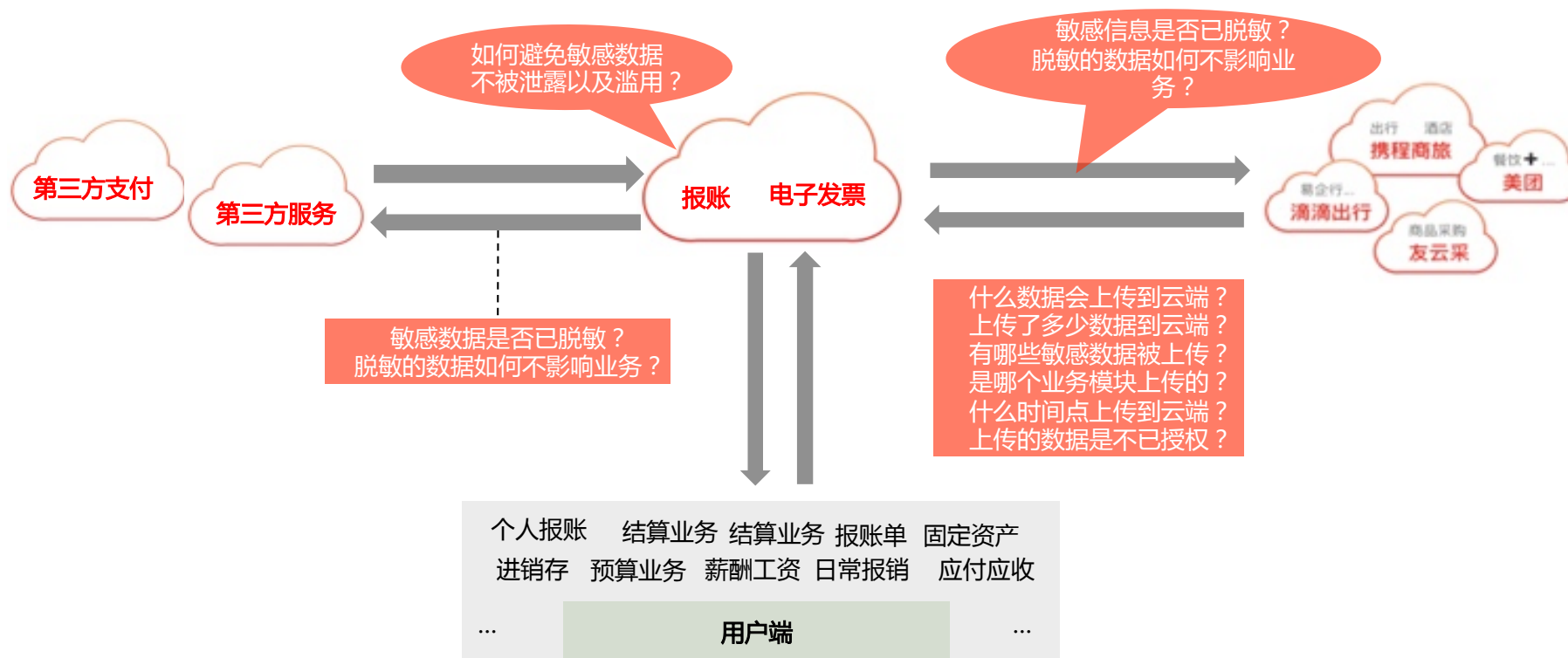
ZERO TRUST SECURITY

# 场景二：CASB让用户重获SaaS数据掌控权



ZERO TRUST SEC

# 实践：SaaS云端数据安全





# 合法用户通过CASB，查询凭证列表



凭证列表

数量: 0001

新增 审核 打印 更多

凭证号 凭证状态 凭证日期

日期	凭证号	摘要	科目	辅助核算	币种	借方金额	贷方金额	制单人	记账人
2018-02	1	提现	1001 库存现金		人民币	2,000.00		财务经理	
		应收账款—某客户	1122 应收账款	客户: 某客户	人民币		2,000.00		
2018-02	2	提现	1001 库存现金		人民币	10,000.00		财务经理	
		应收账款—某客户	1122 应收账款	客户: 某客户	人民币		10,000.00		
		主营业务收入	1012 其他销售收入		人民币	211.00			
		主营业务收入	1004000104 1321201	客户: 万达	人民币	230.00			
		主营业务收入	100200 其他收入		人民币	341.00			
		主营业务收入	110101 成本		人民币	6,199.00			
		主营业务收入	1012 其他销售收入		人民币	426,902.00			
		主营业务收入	1001 库存现金		人民币	342,476.00			

ZERO TRUST SECURITY

# 非授权用户数据安全加密



未授权用户不通过CASB, 直接查询凭证列表(乱码)

ID	日期	凭证ID	名称	科目	所属机构	币种	账户余额	凭证金额	制单人	记账人
1	2018-02	yafaie900fame	1001 现金存款	1001 现金存款	人民币	人民币	2,000.00	2,000.00	制单经理	
2	2018-02	dhewy76v	ru75xa"8&	1001 现金存款	人民币	人民币	0	0	制单经理	
		dhewy76v	z@19jsmz	1012 其他货币存款	人民币	人民币	0	0		
				1001 现金存款	人民币	人民币	10,000.00			
				1012 其他货币存款	人民币	人民币	211.00			
				1001 现金存款	人民币	人民币	211.00			
				02 银行存款	人民币	人民币	341.00			
					人民币	人民币	8,128.00			
					人民币	人民币	4,190,002.00			
					人民币	人民币	342,478.00			

# 云访问CASB提供了不同的数据安全模型



企业本地网

数据传输

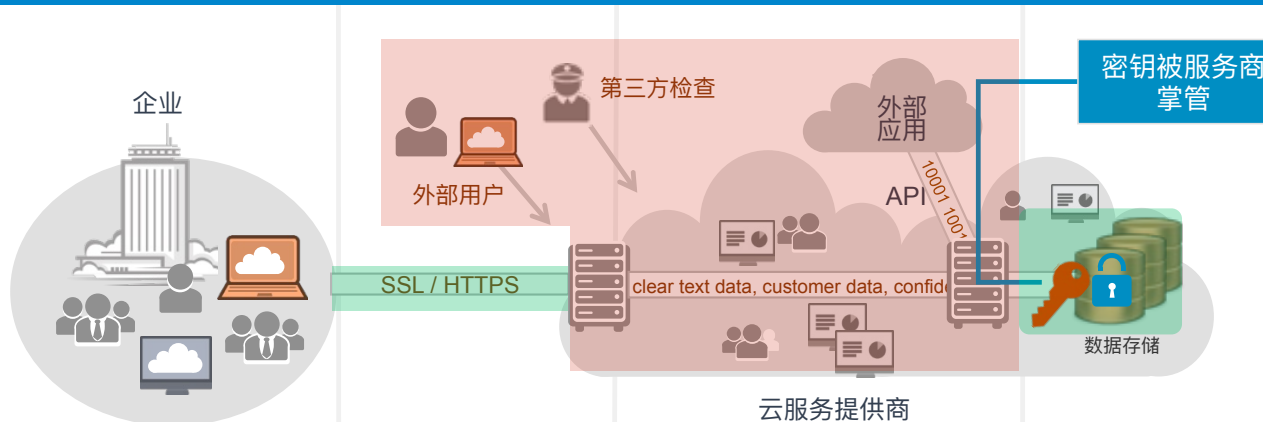
数据使用

数据存储

### 云服务商提供的 数据加密方案

有限度的安全

潜在风险



### 企业自主掌控密钥的 CASB加密方案

持续数据保护

ZERO TRUST SECURITY



## 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

ZERO TRUST SECURITY

# 关于我们



炼石  
CipherGateway



- 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

ZERO TRUST SECURITY



# 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”)