



2016阿里安全峰会

2016 ALIBABA SECURITY SUMMIT

聚力·赋能

2016阿里安全峰会

2016 ALIBABA SECURITY SUMMIT



2016阿里安全峰会  
2016 ALIBABA SECURITY SUMMIT

# 华为数据安全管理的实践

孙颖

华为信息安全运营总监



# 目录

1

需求及解决方案

2

机要信息资产识别与管控

3

安全运营保障方案

4

成果展示



## 内外部环境变化驱动华为加大力度保护核心信息资产

信息资产

随着华为竞争力的提升，居于业界领先地位的自主研发的智力资产越来越多，信息资产价值越来越大

漏洞

云计算、移动化等IT技术在提升业务效率同时，引入了更多的安全风险

威胁

觊觎华为核心竞争力的竞争对手越来越多

安全建设  
势在必行

构建与华为业务发展和竞争态势相匹配的信息安全体系



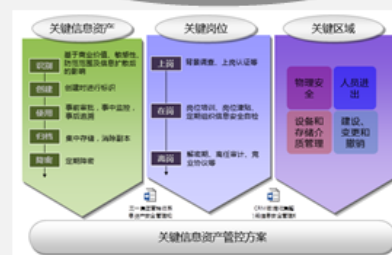
# 找到华为核心信息资产，从流程、组织、技术三个方面构建数据安全整体解决方案

安全建设

## 资产分级

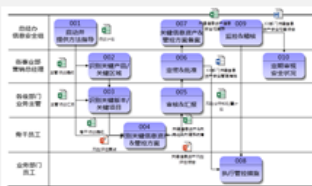
二级分类	三级分类	资产名称	资产来源	关键程度	策略
A1 客户管理	A1.1 客户信息管理	A1.1.1 客户管理后台数据访问权限	A1.1.1.1 客户管理后台数据访问权限	高	限制访问IP地址
A1 客户管理	A1.1 客户信息管理	A1.1.2 客户管理后台数据	A1.1.2.1 客户管理后台数据	高	限制访问IP地址
A1 客户管理	A1.1 客户信息管理	A1.1.3 客户管理后台数据	A1.1.3.1 客户管理后台数据	高	限制访问IP地址
A1 客户管理	A1.1 客户信息管理	A1.1.4 客户管理后台数据	A1.1.4.1 客户管理后台数据	高	限制访问IP地址
A1 客户管理	A1.1 客户信息管理	A1.1.5 客户管理后台数据	A1.1.5.1 客户管理后台数据	高	限制访问IP地址
A1 客户管理	A1.1 客户信息管理	A1.1.6 客户管理后台数据	A1.1.6.1 客户管理后台数据	高	限制访问IP地址
A1 客户管理	A1.1 客户信息管理	A1.1.7 客户管理后台数据	A1.1.7.1 客户管理后台数据	高	限制访问IP地址
A1 客户管理	A1.1 客户信息管理	A1.1.8 客户管理后台数据	A1.1.8.1 客户管理后台数据	高	限制访问IP地址
A1 客户管理	A1.1 客户信息管理	A1.1.9 客户管理后台数据	A1.1.9.1 客户管理后台数据	高	限制访问IP地址
A1 客户管理	A1.1 客户信息管理	A1.1.10 客户管理后台数据	A1.1.10.1 客户管理后台数据	高	限制访问IP地址
A1 客户管理	A1.1 客户信息管理	A1.1.11 客户管理后台数据	A1.1.11.1 客户管理后台数据	高	限制访问IP地址
A1 客户管理	A1.1 客户信息管理	A1.1.12 客户管理后台数据	A1.1.12.1 客户管理后台数据	高	限制访问IP地址
A1 客户管理	A1.1 客户信息管理	A1.1.13 客户管理后台数据	A1.1.13.1 客户管理后台数据	高	限制访问IP地址
A1 客户管理	A1.1 客户信息管理	A1.1.14 客户管理后台数据	A1.1.14.1 客户管理后台数据	高	限制访问IP地址
A1 客户管理	A1.1 客户信息管理	A1.1.15 客户管理后台数据	A1.1.15.1 客户管理后台数据	高	限制访问IP地址
A1 客户管理	A1.1 客户信息管理	A1.1.16 客户管理后台数据	A1.1.16.1 客户管理后台数据	高	限制访问IP地址
A1 客户管理	A1.1 客户信息管理	A1.1.17 客户管理后台数据	A1.1.17.1 客户管理后台数据	高	限制访问IP地址
A1 客户管理	A1.1 客户信息管理	A1.1.18 客户管理后台数据	A1.1.18.1 客户管理后台数据	高	限制访问IP地址
A1 客户管理	A1.1 客户信息管理	A1.1.19 客户管理后台数据	A1.1.19.1 客户管理后台数据	高	限制访问IP地址
A1 客户管理	A1.1 客户信息管理	A1.1.20 客户管理后台数据	A1.1.20.1 客户管理后台数据	高	限制访问IP地址

## 管控方案



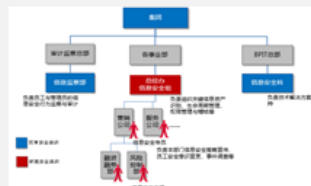
安全运营

## 流程



- 关键信息资产安全识别与管控流程
- 关键信息资产安全管理规定

## 组织



- 信息安全管控组织建议
- 公司信息安全任命

## 技术



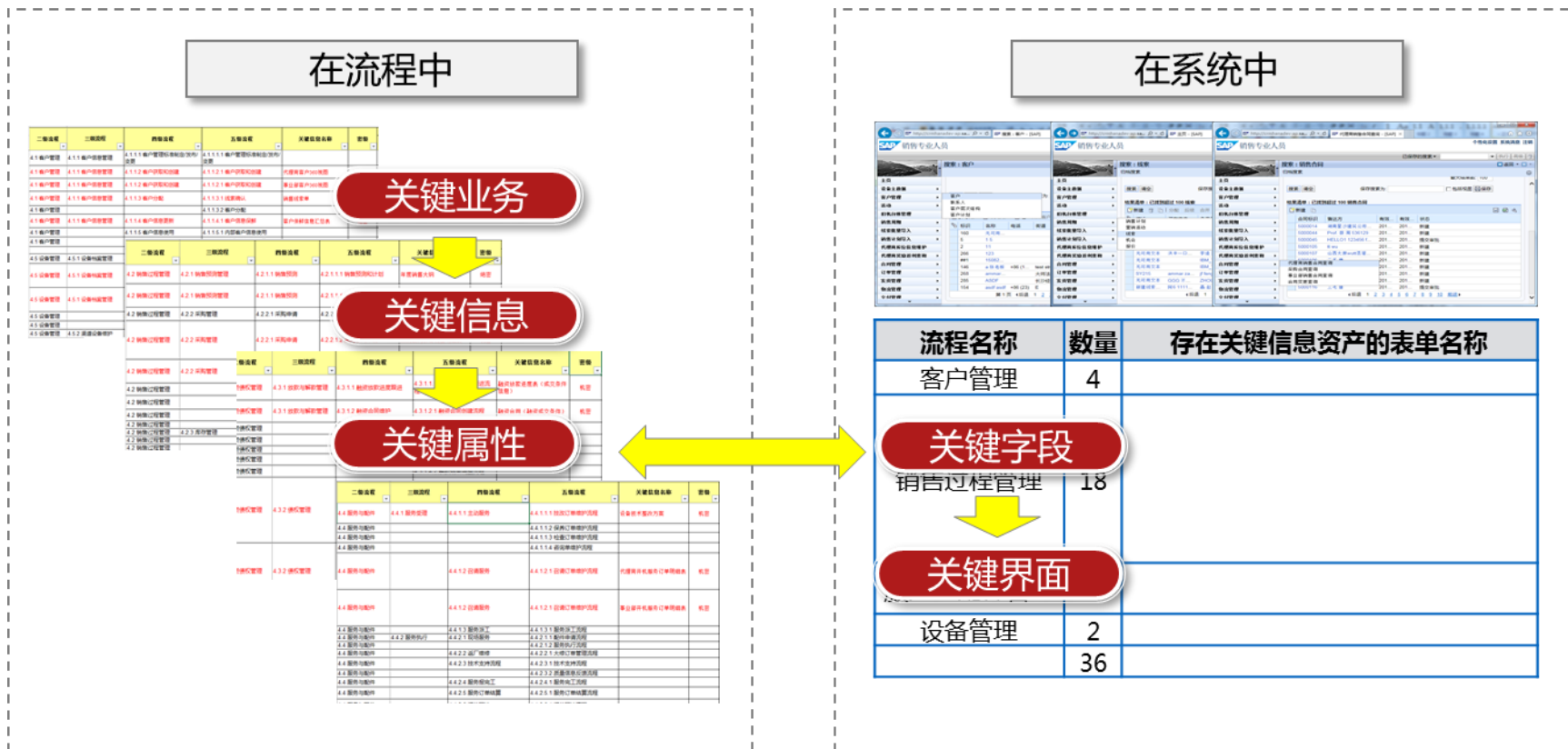
- 关键信息资产管控方案
- 例外需求解决方案
- 关键信息资产管理规定



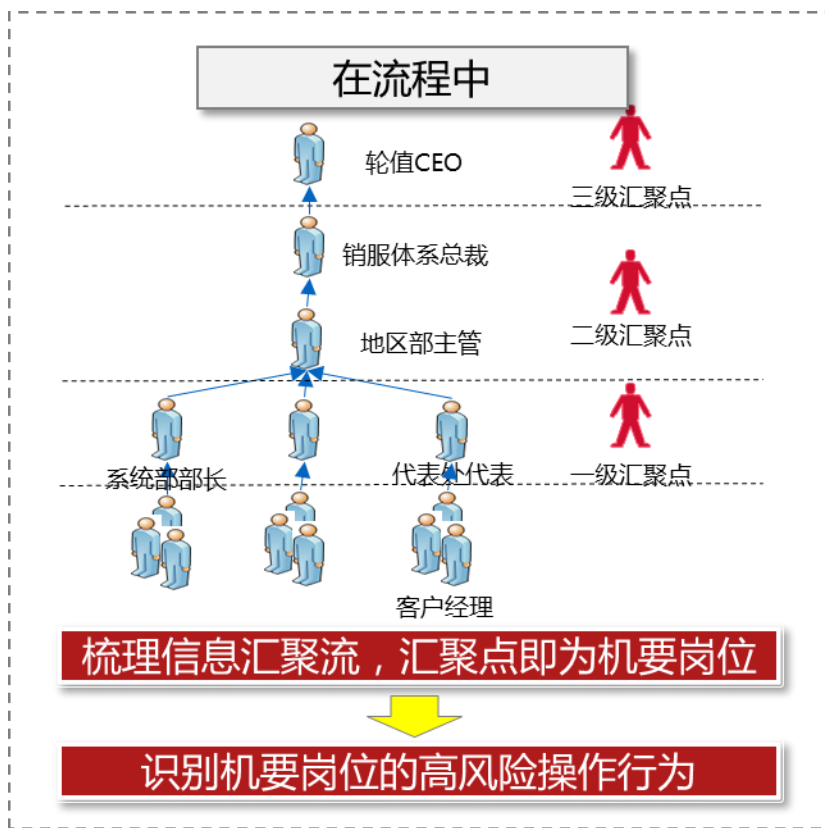
# 目录

- 1 需求及解决方案
- 2 机要信息资产识别与管控
- 3 安全运营保障方案
- 4 成果展示

# 信息：识别核心信息资产在流程中在系统中的位置



# 人：识别使用待保护资产的人在流程中在系统中的位置



**在系统中**

Role Name	客户				RecordType
	Read	create	Edit	Delete	
(Huawei China)CEO	Y				
(Huawei China)MKT管理员	Y	Y	Y		CUSTOMER
(Huawei China)MKT营销经理	Y	Y	Y		CUSTOMER
(Huawei China)MKT主管	Y	Y	Y		
(Huawei China)Region A					
(Huawei China)代表处产品					CUSTOMER
(Huawei China)代表处客户经理	Y	Y	Y		CUSTOMER
(Huawei China)代表处渠道经理	Y	Y	Y		CUSTOMER
(Huawei China)代表处销管	Y	Y	Y		CUSTOMER
(Huawei China)代表处主管	Y	Y	Y		
(Huawei China)分销业务部					CUSTOMER
(Huawei China)解决方案					
(Huawei China)解决方案					CUSTOMER
(Huawei China)解决方案产品	Y	Y	Y		
(Huawei China)解决方案产品线	Y	Y	Y		
(Huawei China)解决方案产品主管	Y	Y	Y		CUSTOMER
(Huawei China)渠道管理部渠道专员	Y	Y	Y		CUSTOMER
(Huawei China)渠道管理部主管	Y	Y	Y		
(Huawei China)商业销售					CUSTOMER
(Huawei China)商业销售					CUSTOMER
(Huawei China)系统部产品					CUSTOMER
(Huawei China)系统部产品主管	Y	Y	Y		CUSTOMER
(Huawei China)系统部客户经理	Y	Y	Y		CUSTOMER
(Huawei China)系统部渠道经理	Y	Y	Y		CUSTOMER
(Huawei China)系统部销管	Y	Y	Y		CUSTOMER

**机要权限**

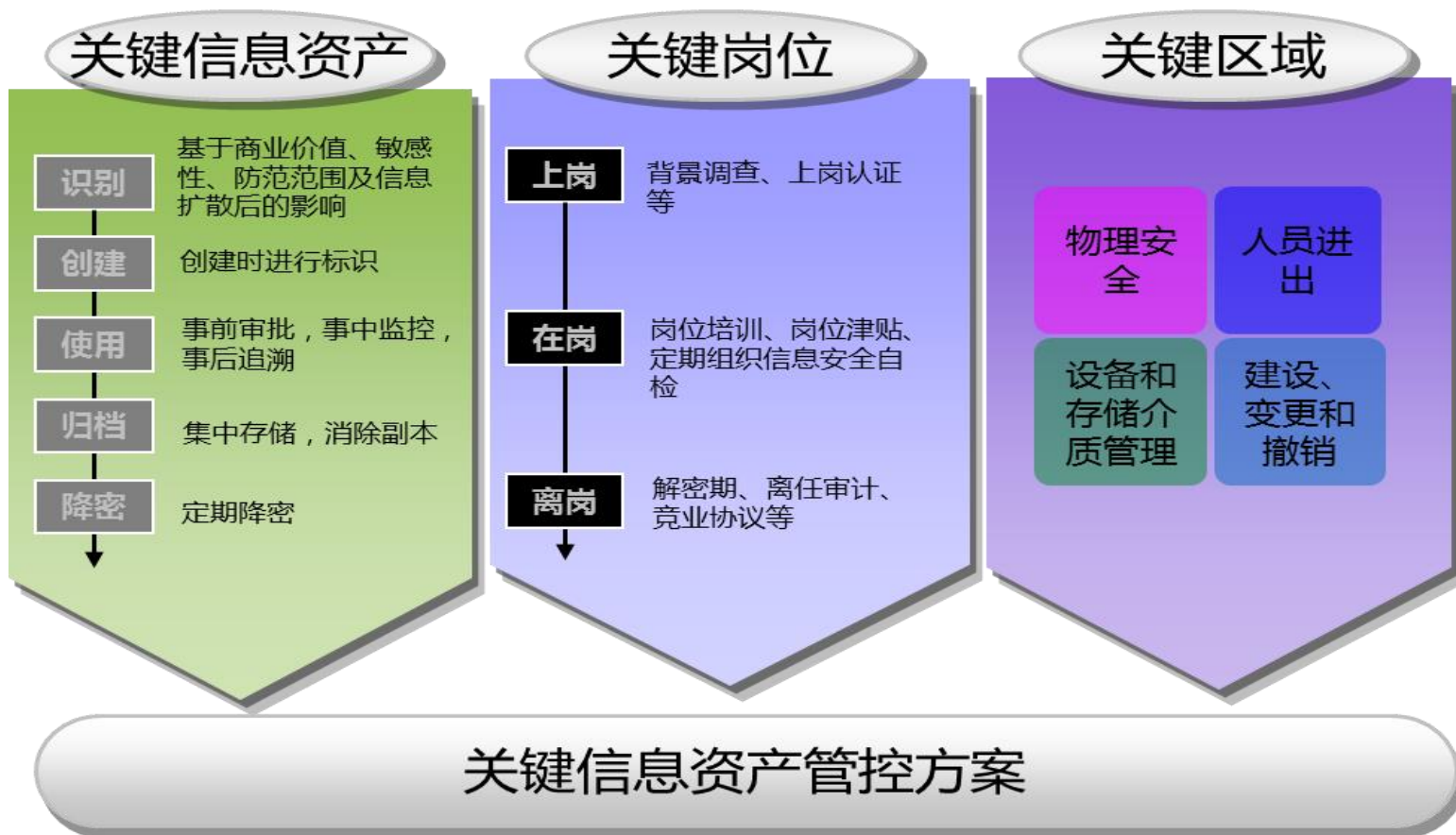
**机要角色**

**机要人员**





# 管控模式：什么人在什么时间什么地点如何使用哪些资产 (4W1H)





# 目录

1 需求及解决方案

2 机要信息资产识别与管控

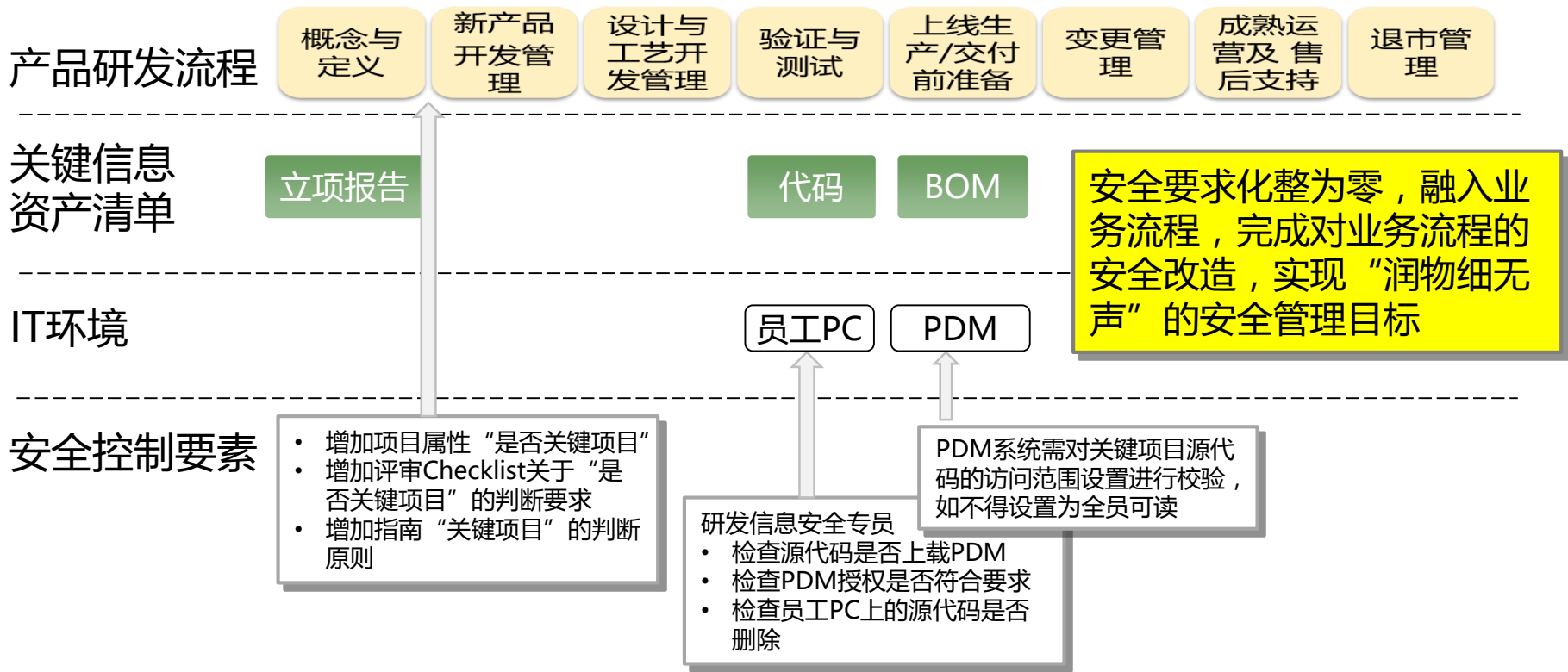
3 安全运营保障方案

4 成果展示



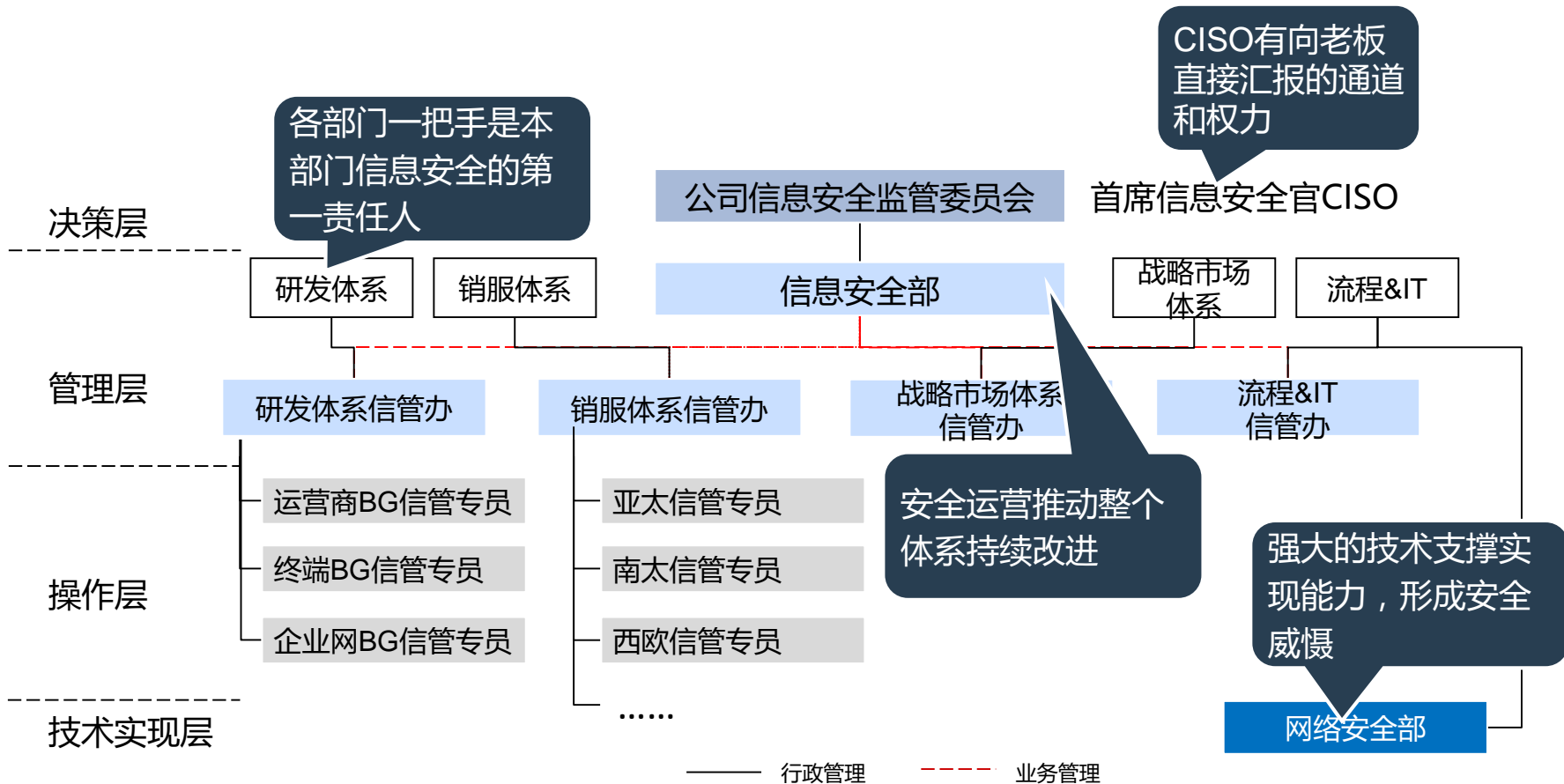
# 安全控制要素融入业务流程

安全要求：关键项目的源代码集成测试通过后要上载到PDM系统只允许最小授权范围可读，并删除本地源码。





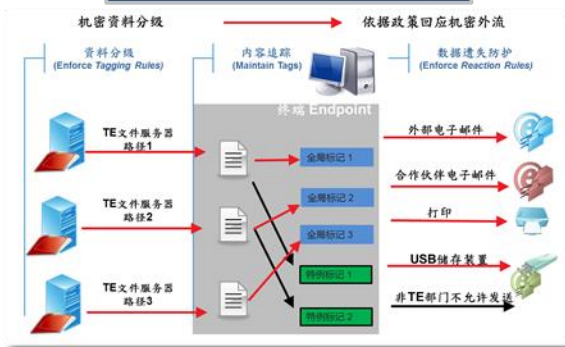
# 安全组织要上有支持下有支撑，持续运营推动改进



# 安全管控、安全服务、安全监控三位一体打造管理落地的技术基石

提升运作效率

## 安全管控解决方案

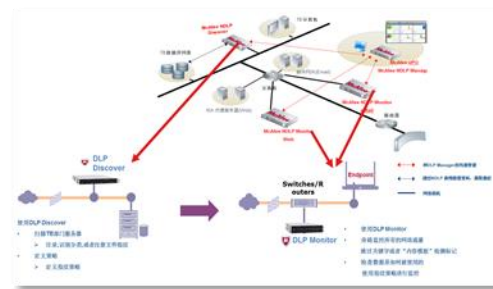
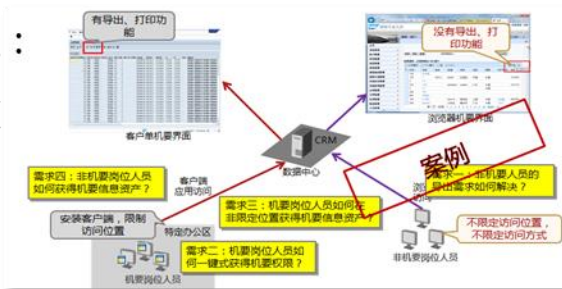


保障持续有效

## 安全服务解决方案

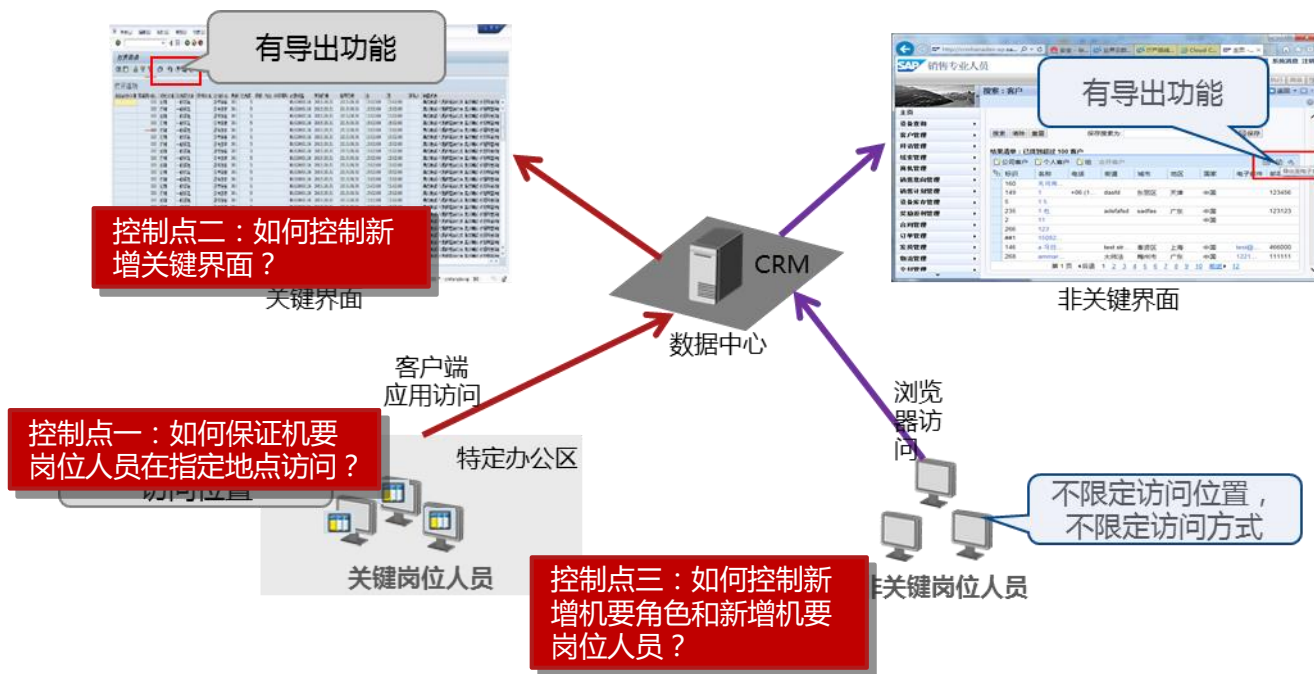
## 安全监控解决方案

在服务中管控：  
通过良好的服务来降低安全对业务效率的影响。



## 包含运营解决方案的安全管控方案

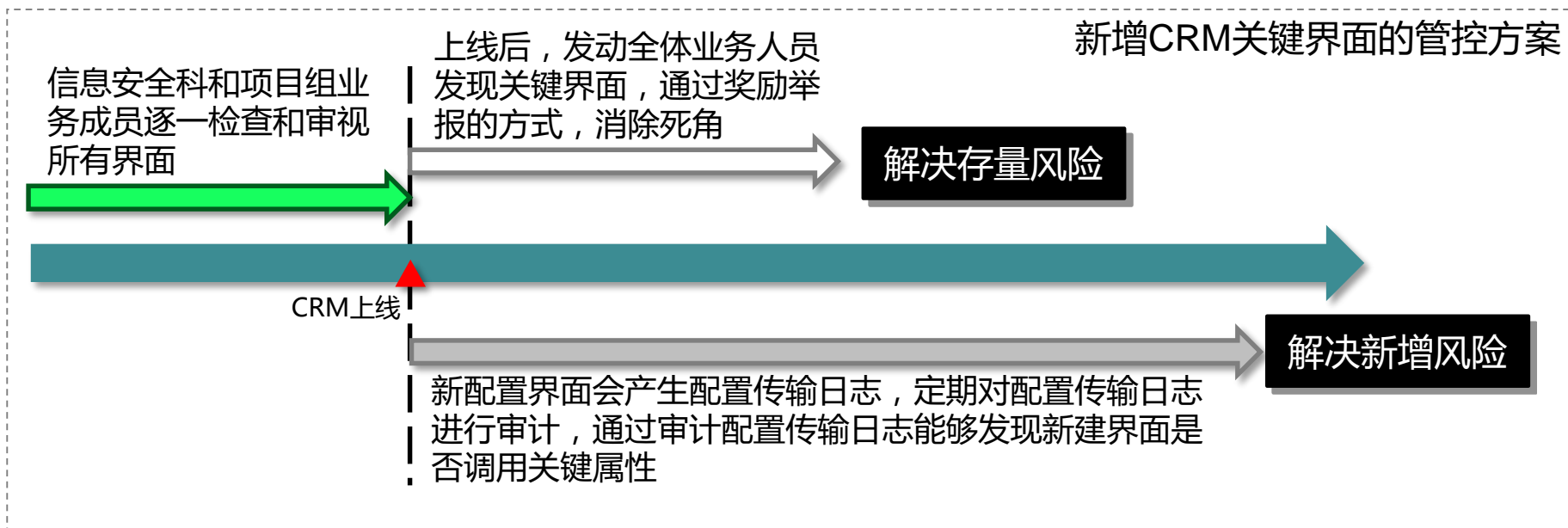
- 导出：只有关键角色才能拥有包含关键信息资产关键属性界面的导出权限，且只能在公司内网指定地点使用客户端进行导出操作。



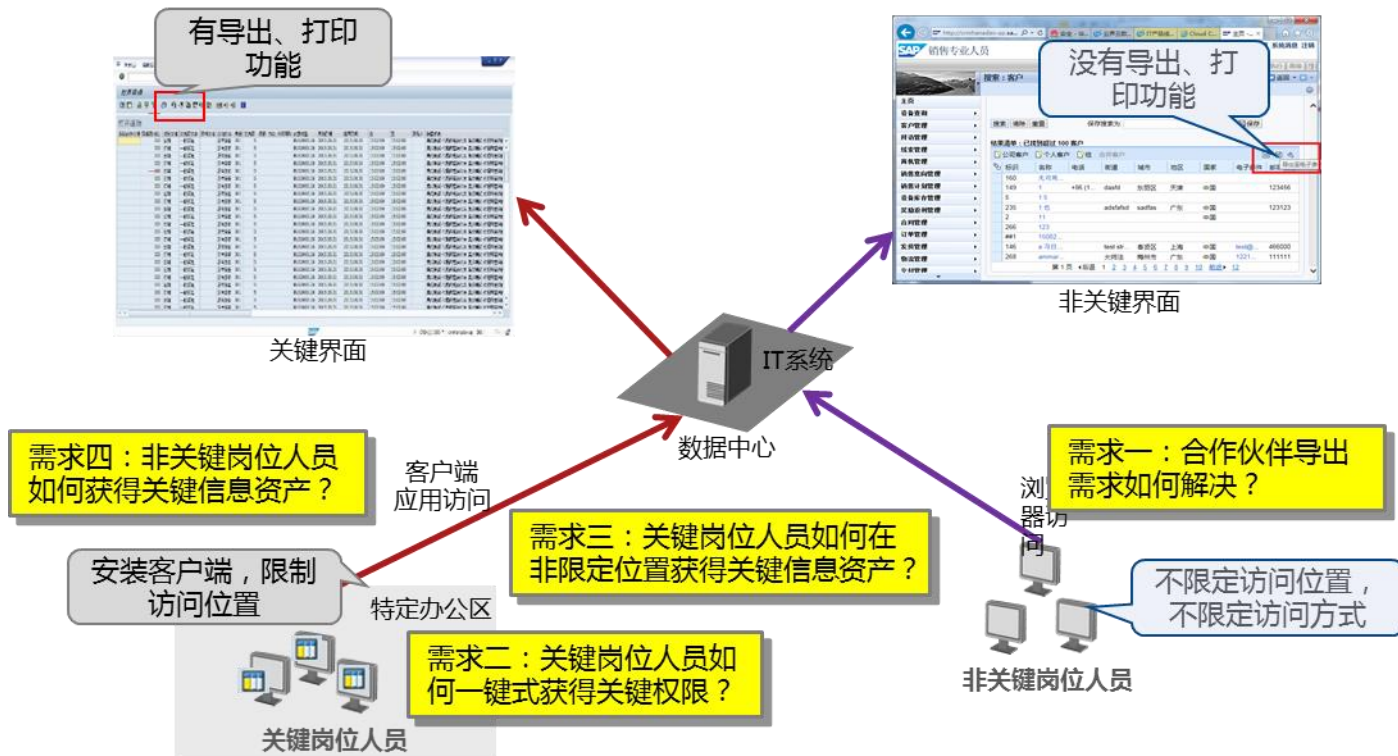
- 打印：只提供对单张报表进行打印的功能，无法对批量数据进行打印



## 安全运营管控举例：新增关键界面的管控方案



# 安全服务提升运营体验从而促成管控目标的达成



在服务中管控：需要通过良好的服务来降低安全对业务效率的影响。



# 安全服务举例：关键岗位人员一键式获得关键权限

- **一键式**：业务人员只要提交一次申请即可获得所有相关的资源
- **安全职责告知**：在申请流程中备注具体的安全管理要求和应尽职责义务，无须业务人员自行查找相关规定
- **直接主管负责制**：直接主管对授权负责，无须多层审批



工号 (必填)	用户名 (必填)	岗位 (必填)	邮箱	手机号码 (必填)	IP地址 (必填)	工厂 (必填)
emplno	account	jobno	email	mobile		
(自动带出)	(自动带出)	(自动带出)	(自动带出)	(自动带出)		

调用CRM复合角色清单

提供IP, 自动绑定

申请角色名称: (必填) (增加角色) 接, 含关键和非关键, 与清单一致性校验, 清单直接从CRM中取出

申请原因说明:

申请角色类别:  非关键角色  关键角色

自动识别是否关键角色

申请使用时间: (日历表选择, 必填)

特殊需求说明:

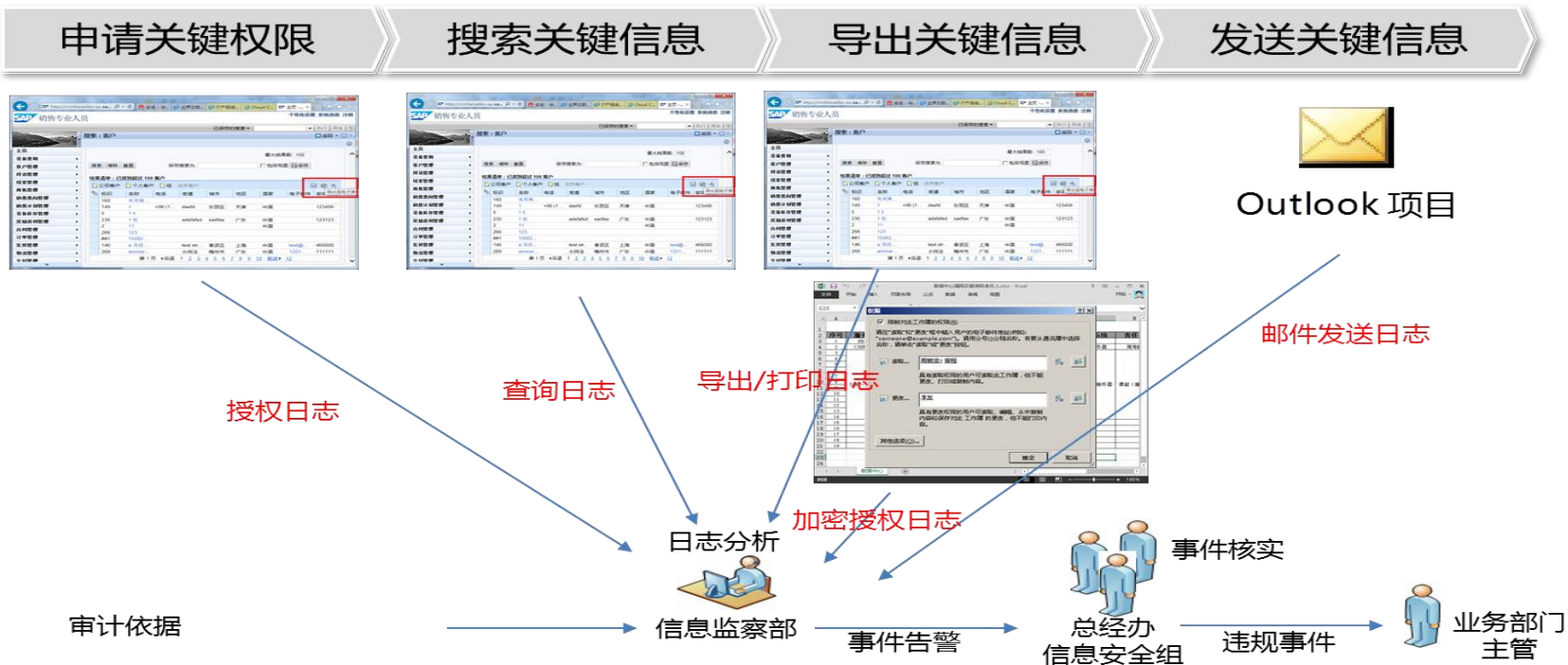
批量申请附件上传:

关键角色审批时, 系统提示管理风险

本部门直接领导确认  
(审批为选择关键角色时, 增加该行, 风险提示和保密承诺)

内部顾问确认  
(审批为选择关键角色时, 增加该行, 风险提示和保密承诺)

# 安全监控是建立安全威慑的重要保障



关键岗位张三用账号zhangsan登陆CRM，进入客户管理界面，搜索“客户360信息”，之后批量导出到excel文档，然后发送给主管李四。



# 目录

1 需求及解决方案

2 机要信息资产识别与管控

3 安全运营保障方案

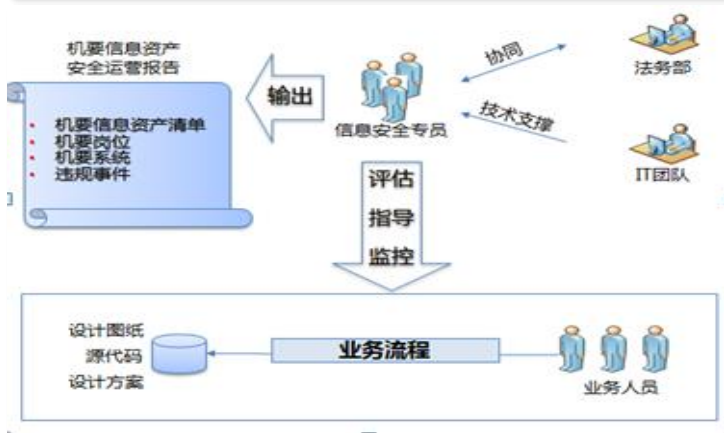
4 成果展示



# 安全运营蓝图：一个团队、一份报告

## 安全运营机制

安全运营团队评估、指导、监控业务人员在业务流程中对关键信息资产的使用，每月向公司管理层汇报关键信息资产安全状况。



## 安全运营报告

运营报告内容：包括关键信息资产清单、关键岗位人员清单以及分布情况、安全合规状况等。



保障安全管控持续有效

# 企业安全整体态势

业界安全态势

安全态势感知

## 业界安全态势

### 黑客组织

组织名称	所在国家	成员数量	攻击目标
蜻蜓组织	俄罗斯	30	能源企业
匿名者	美国	150	政府组织
飞猫	伊朗	100	网络间谍
推杆熊猫	中国	50	国防、航空产业

### 安全漏洞



### 对公司有影响的严重漏洞

漏洞名称	受影响服务器数量	受影响重要业务系统数量
Heartbleed	70	2
Linux Bash	30	1
Sandstorm	20	1

### 攻击事件



整体安全态势

## 入侵事件

### 事件类型

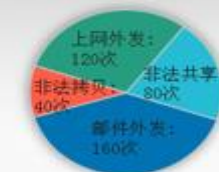


### 事件等级



## 内部泄密

### 泄密途径



### 泄密动机

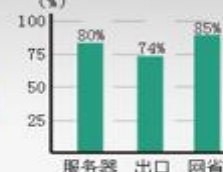


## 风险预测

### 风险预测

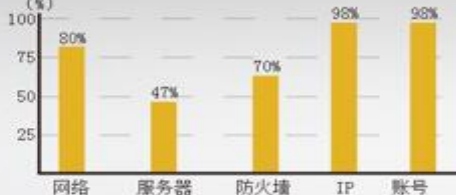


### 监控覆盖率

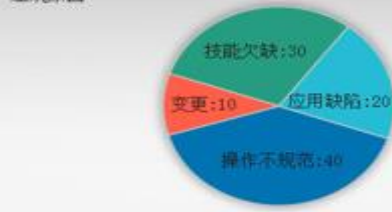


## 配置违规

### 配置合规率



### 违规原因





2016阿里安全峰会  
2016 ALIBABA SECURITY SUMMIT

孙颖

华为信息安全运营总监