



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

华为数据安全安全管理实践

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

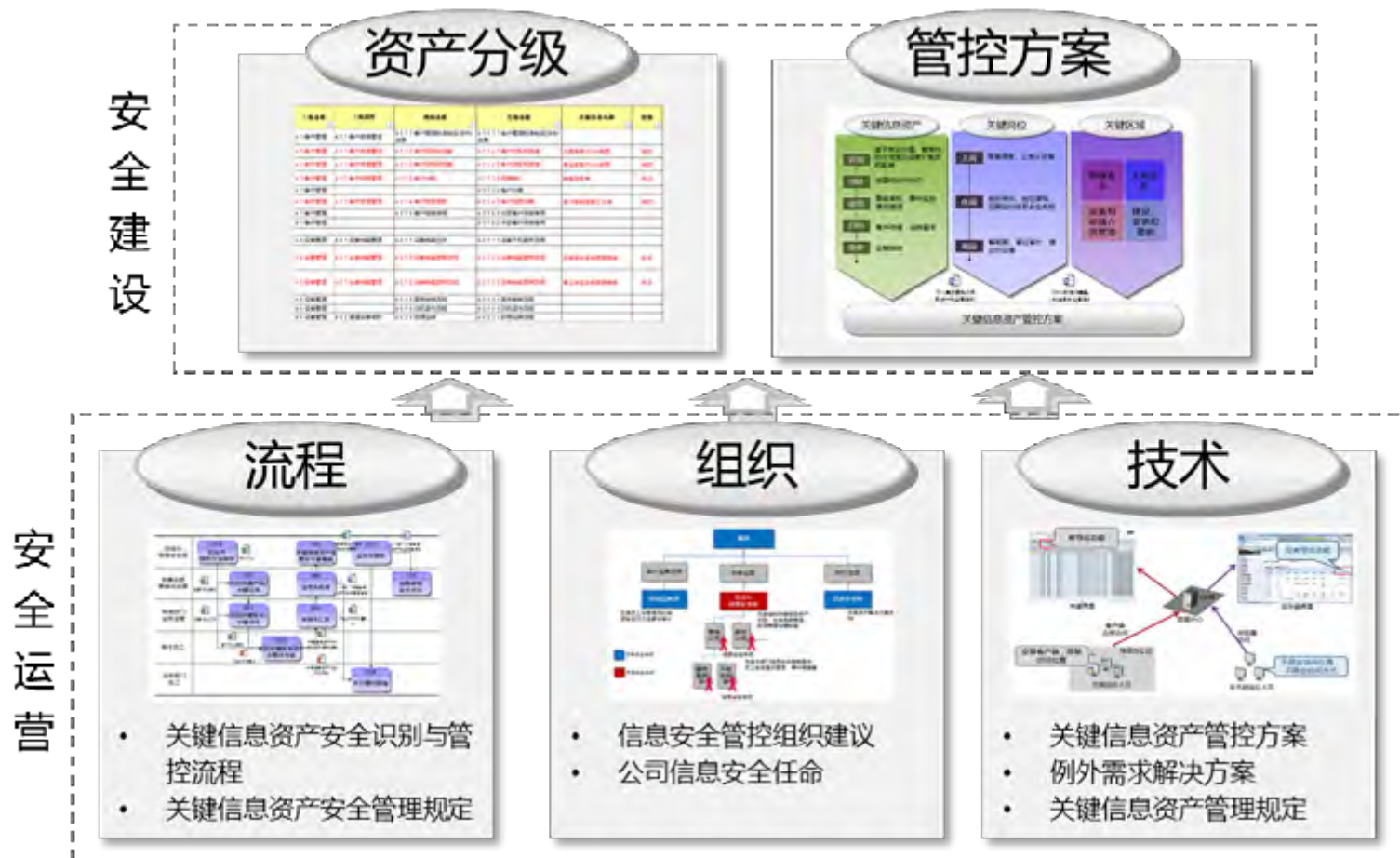
威胁

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

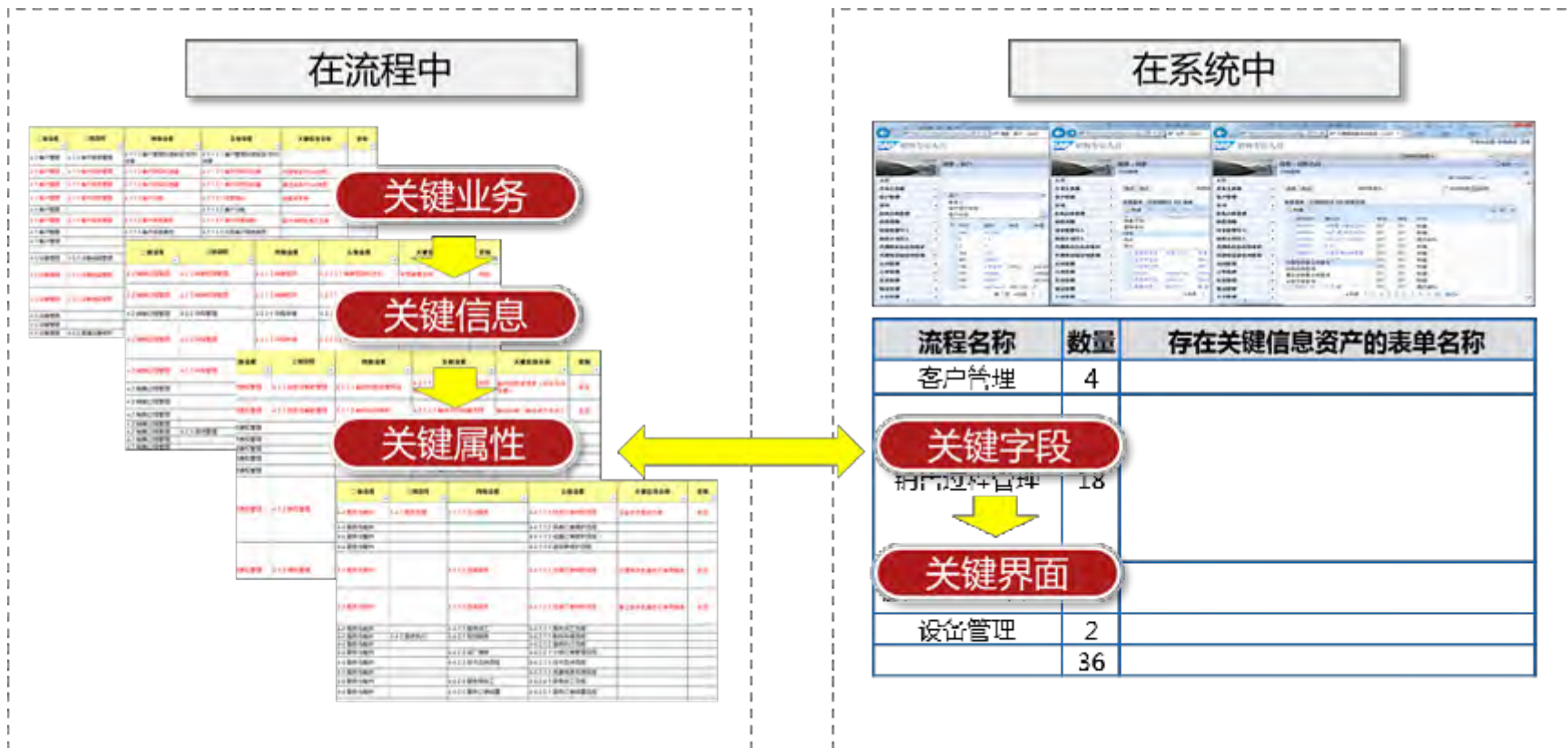




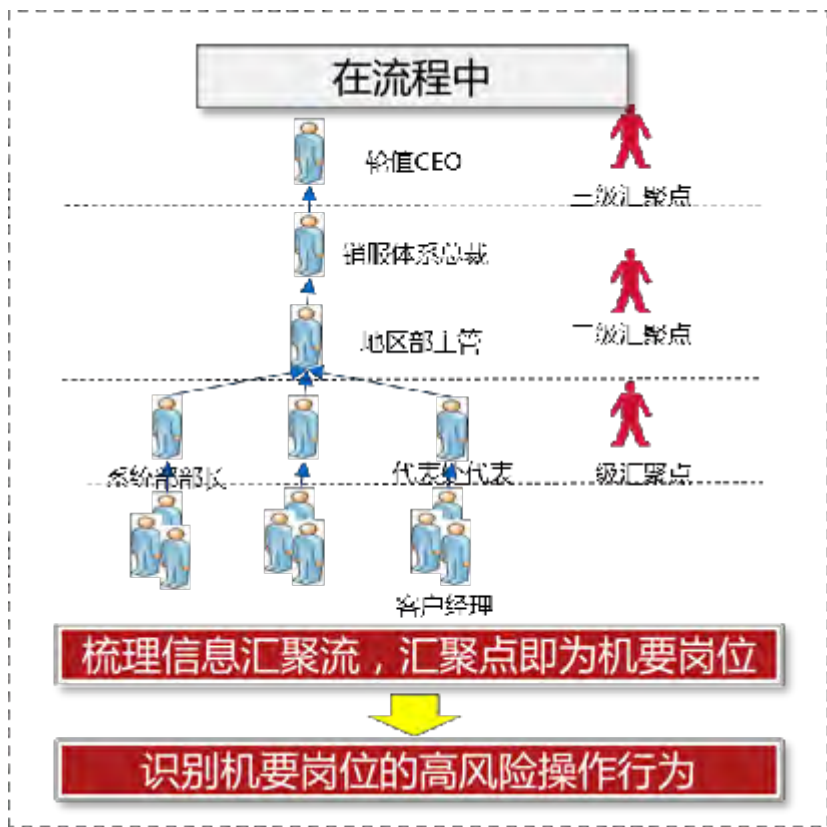
目录

- 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

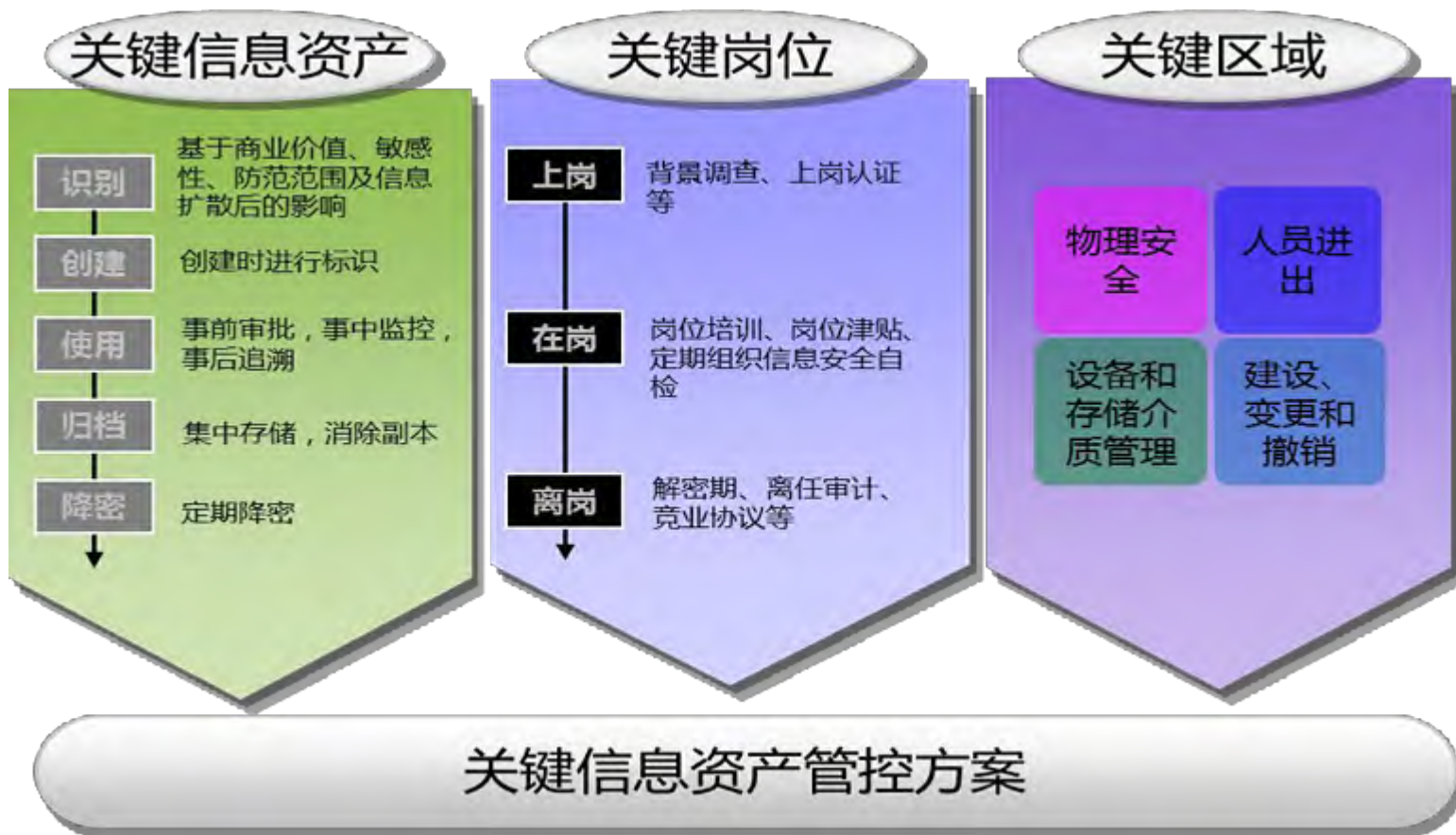
Role Name	客户				RecordType
	Read	create	Edit	Delete	
(Huawei_China)CEO	Y				
(Huawei_China)系统管理员	Y	Y	Y		CUSTOMER
(Huawei_China)系统营销经理	Y	Y	Y		CUSTOMER
(Huawei_China)系统主管	Y				
(Huawei_China)Region A					
(Huawei_China)代表处产品					CUSTOMER
(Huawei_China)代表处客户经理	Y	Y	Y		CUSTOMER
(Huawei_China)代表处渠道经理	Y		Y		CUSTOMER
(Huawei_China)代表处主管	Y		Y		CUSTOMER
(Huawei_China)代表处主管	Y		Y		CUSTOMER
(Huawei_China)分销售务部					CUSTOMER
(Huawei_China)解决方案					
(Huawei_China)解决方案产品					CUSTOMER
(Huawei_China)解决方案产品线					
(Huawei_China)解决方案产品线					CUSTOMER
(Huawei_China)解决方案产品线					
(Huawei_China)渠道管理部渠道专员				Y	CUSTOMER
(Huawei_China)渠道管理部					
(Huawei_China)华北销售					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)系统部销售	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

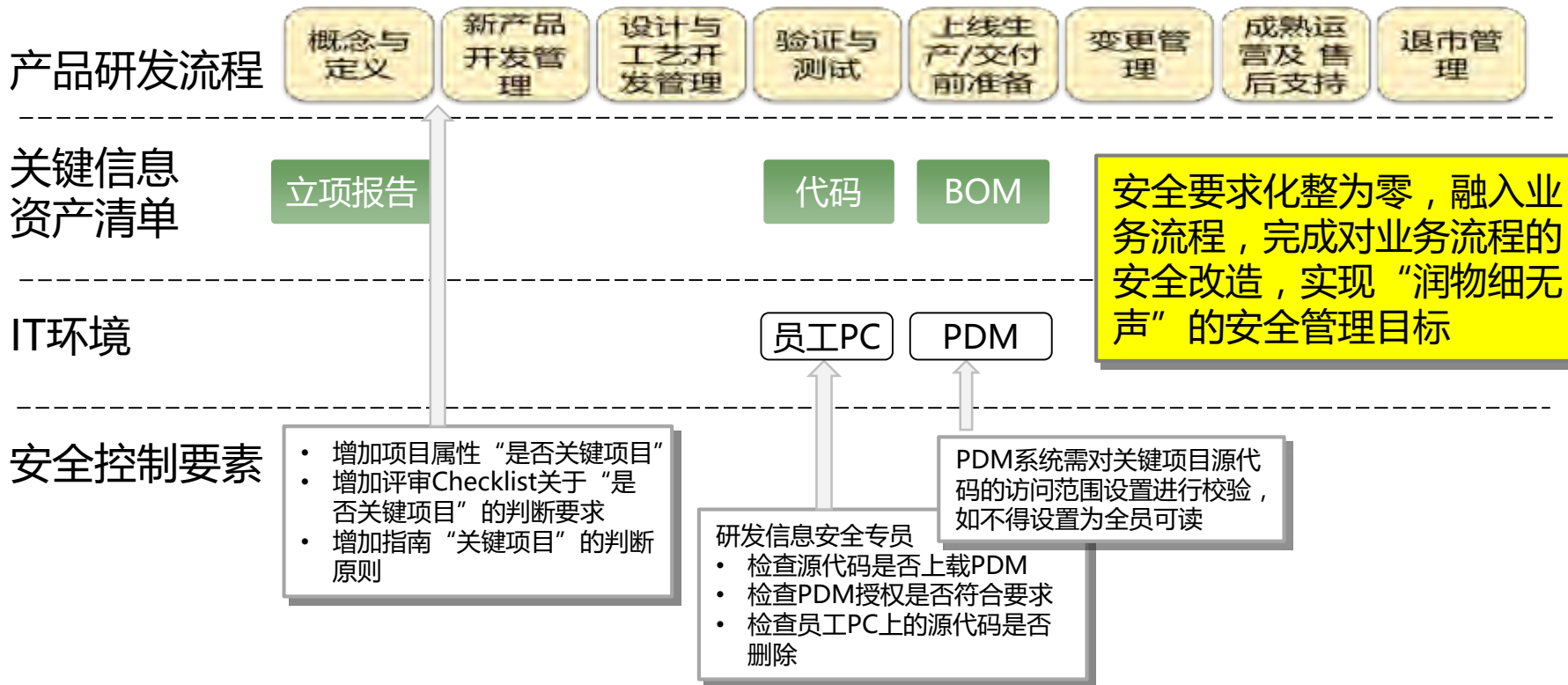
安全运营保障方案

4

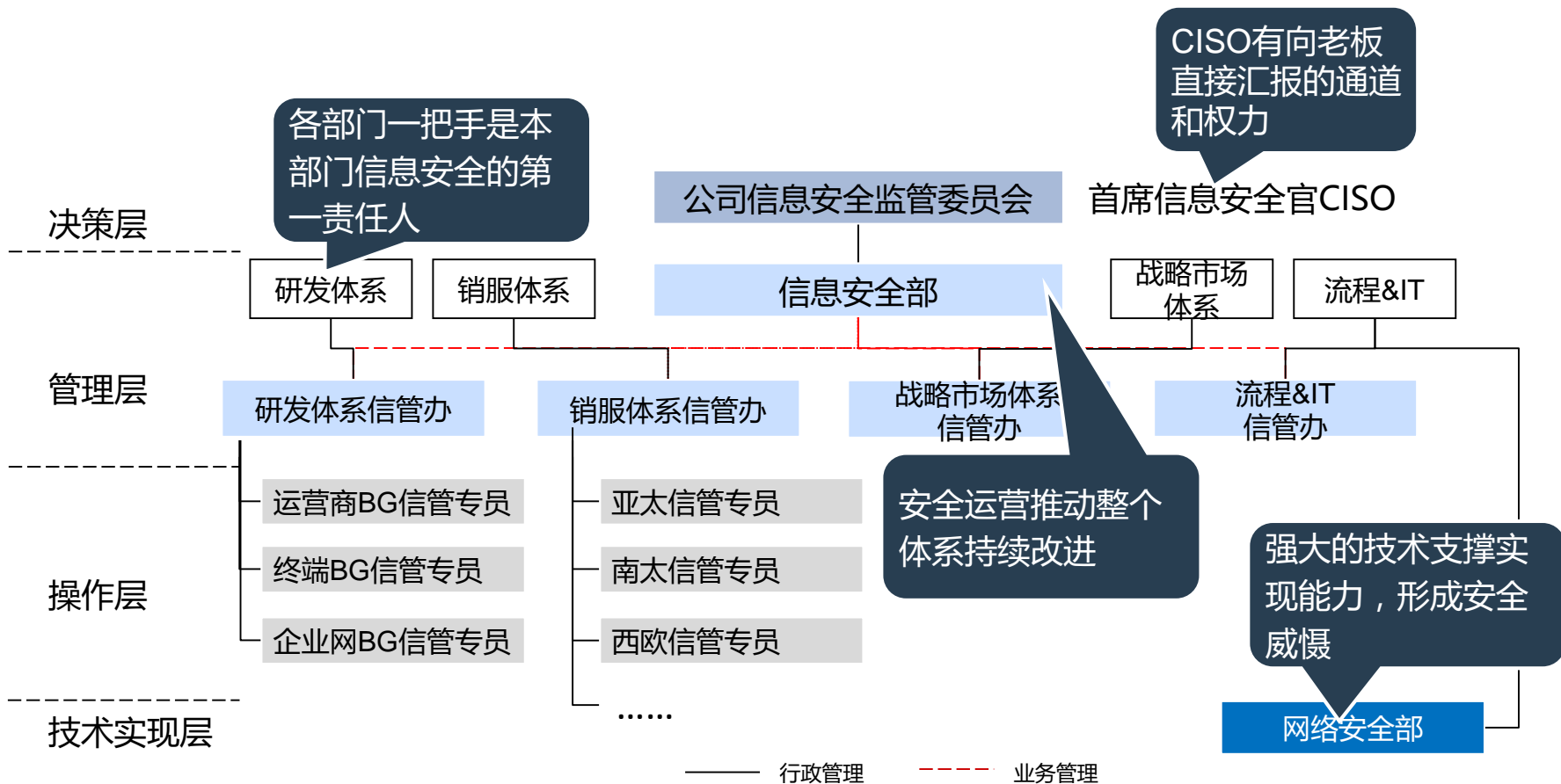
成果展示

安全控制要素融入业务流程

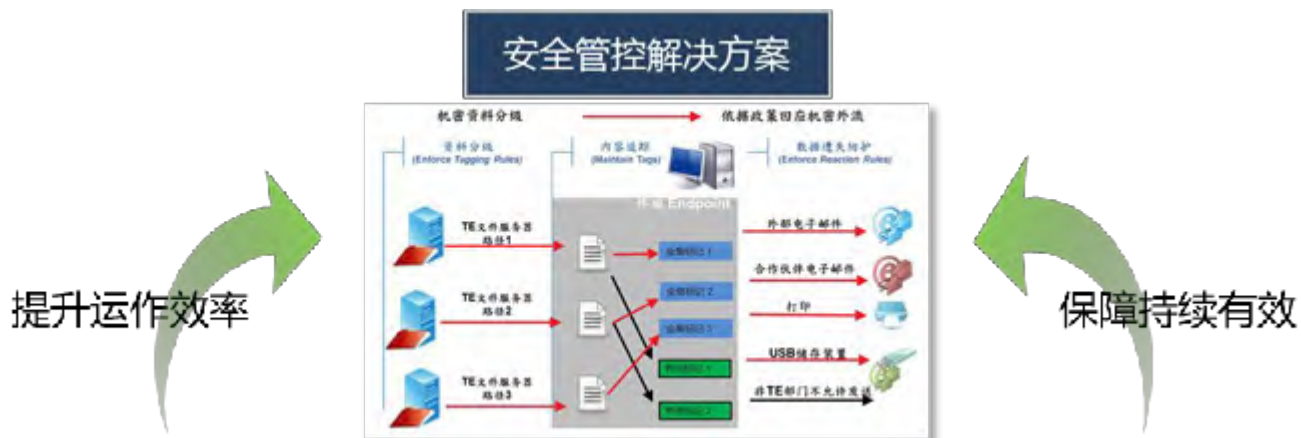
安全要求：关键项目的源代码集成测试通过后要上载到PDM系统只允许最小授权范围可读，并删除本地源码。



安全组织要上有支持下有支撑，持续运营推动改进



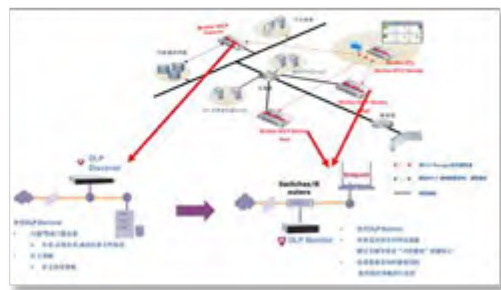
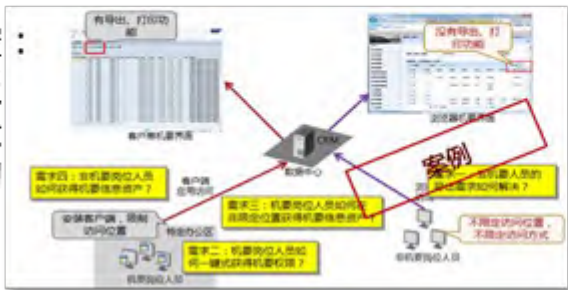
安全管控、安全服务、安全监控三位一体打造管理落地的技术基石



安全服务解决方案

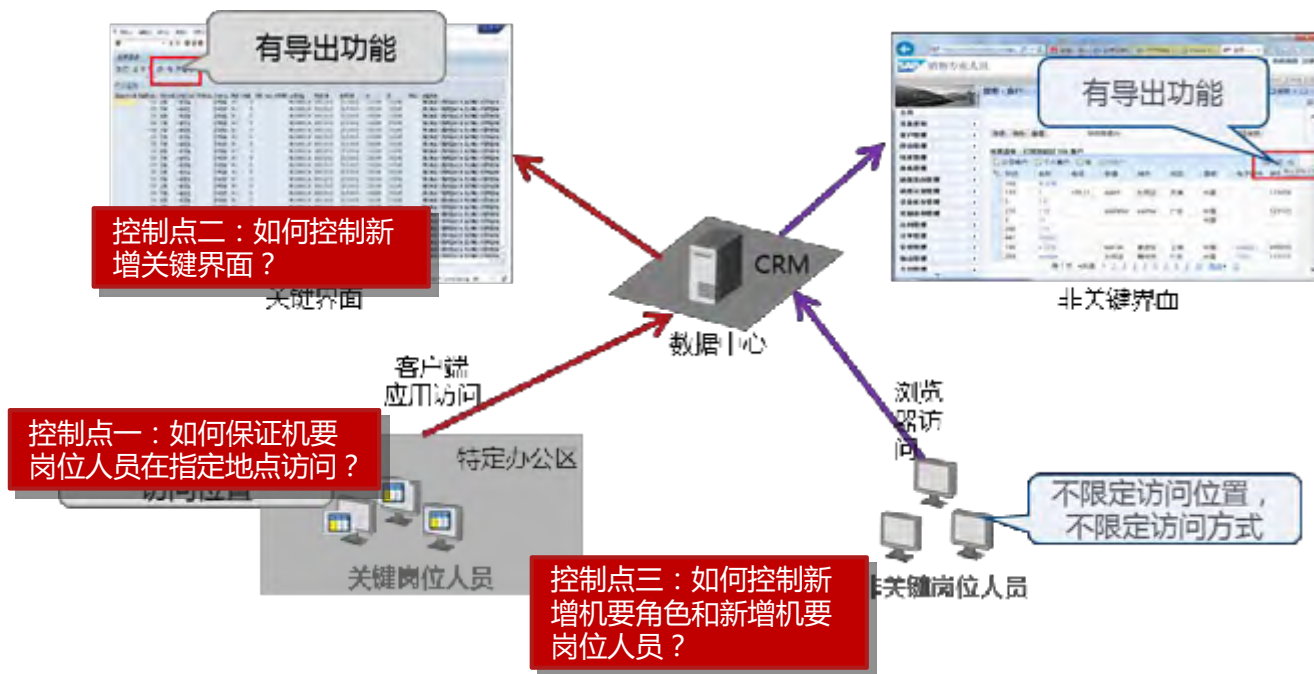
安全监控解决方案

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。



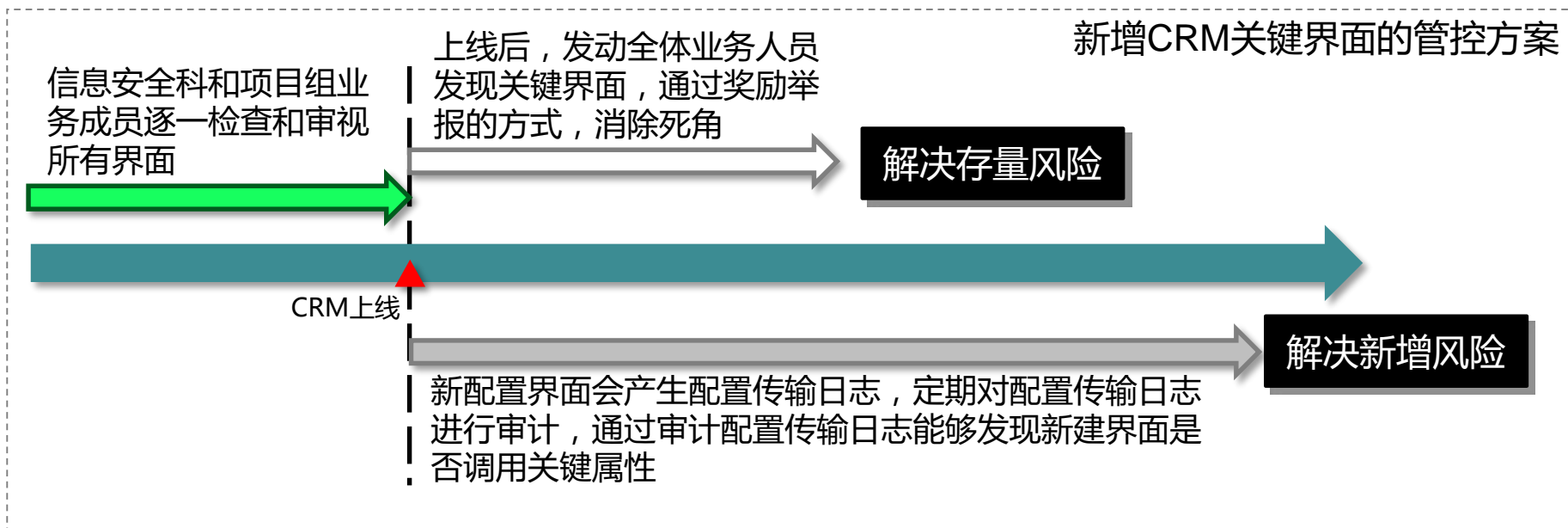
包含运营解决方案的安全管控方案

- 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。

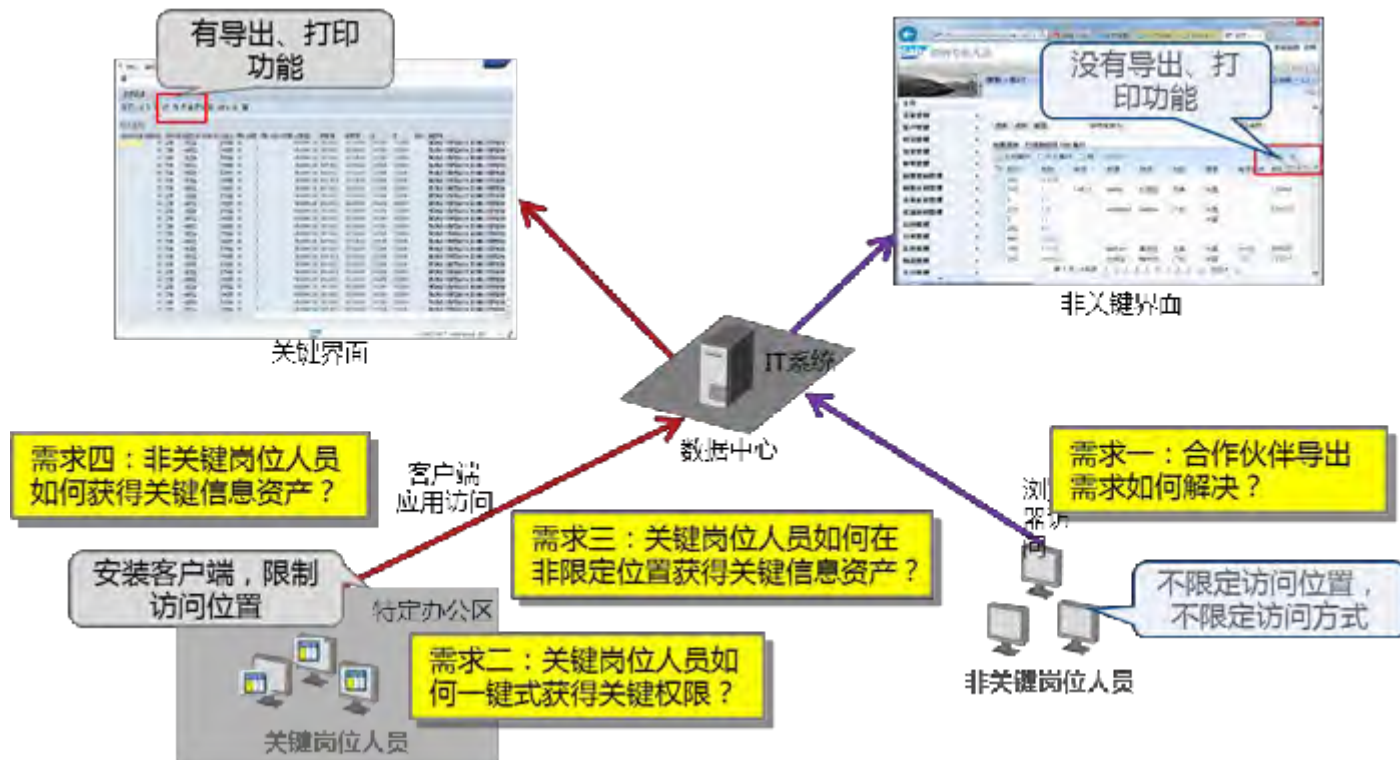


- 打印：只提供对单张报表进行打印的功能，无法对批量数据进行打印

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。

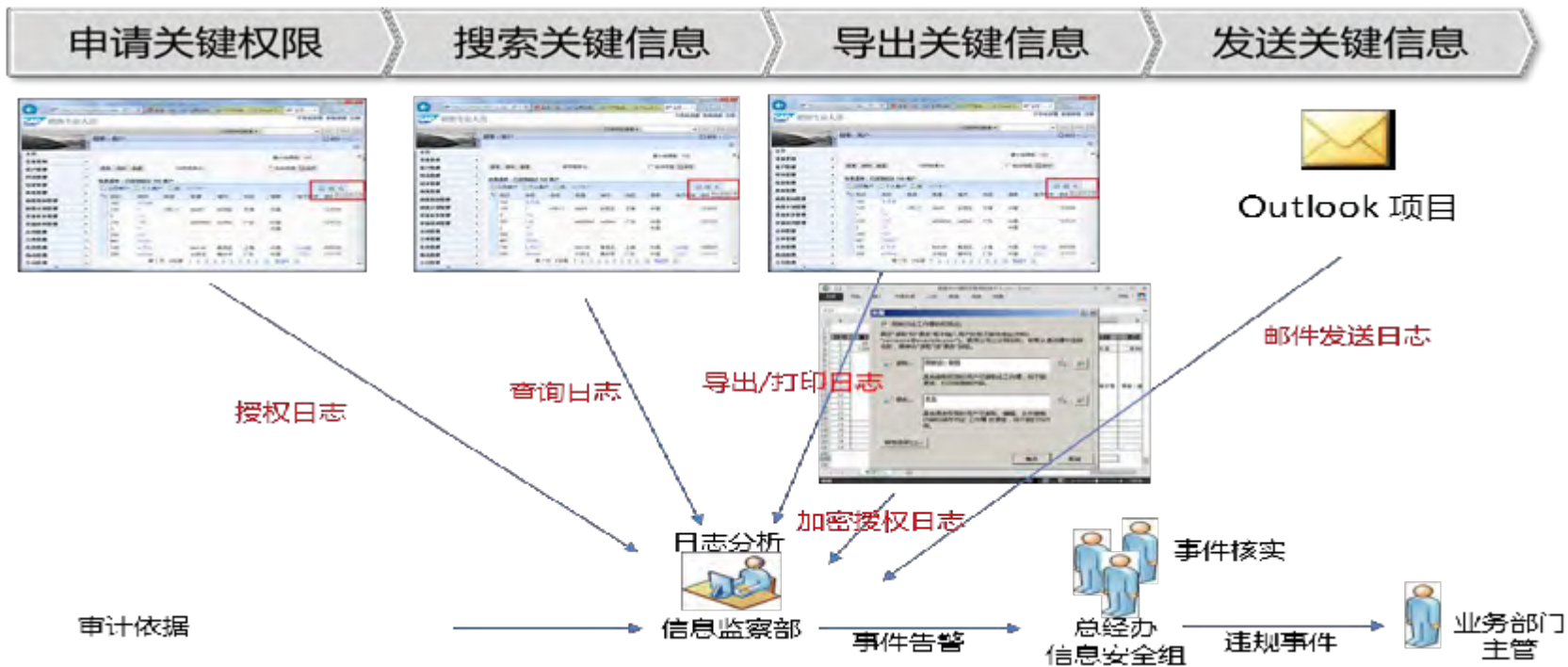
安全服务举例：关键岗位人员一键式获得关键权限

- **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



The screenshot shows a '账号权限申请表' (Account Permission Application Form). The form includes fields for '工号' (Employee ID), '用户名' (Username), '岗位' (Position), '邮箱' (Email), '手机号码' (Mobile Number), and 'IP地址' (IP Address). There are also fields for '申请角色名称' (Apply role name), '申请角色说明' (Apply role description), '申请角色类别' (Apply role category), '申请使用时间' (Apply use time), '特殊需求说明' (Special requirements), and '批量申请附件上传' (Batch application attachment upload). The form is annotated with several red callout boxes: '调用CRM复合角色清单' (Call CRM composite role list), '提供IP, 自动绑定' (Provide IP, automatic binding), '自动识别是否关键角色' (Automatic identification of key roles), and '关键角色审批时, 系统提示管理风险' (When approving key roles, the system prompts for risk management).

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

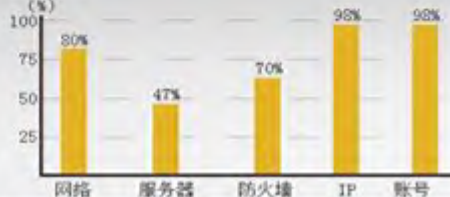


监控覆盖率

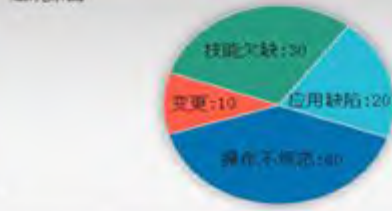


配置违规

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