用友云
yonyou cloud

迈向云端 创变未来

2017中国企业互联网大会

用友云
yonyou cloud

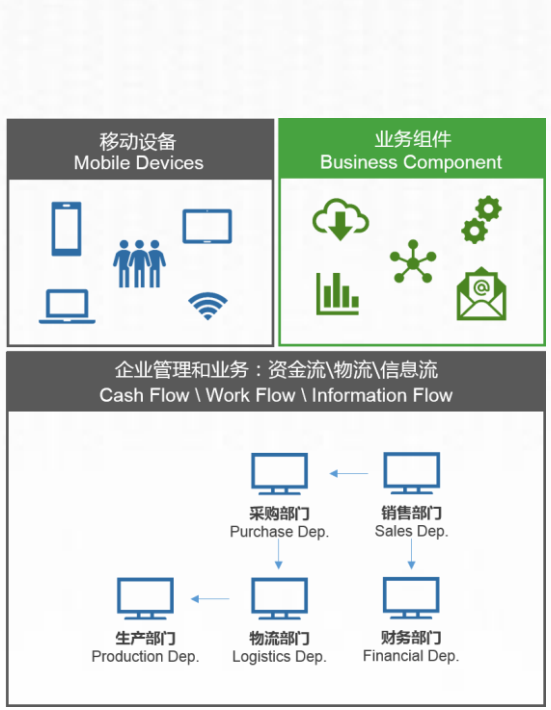
云安全大数据分析平台

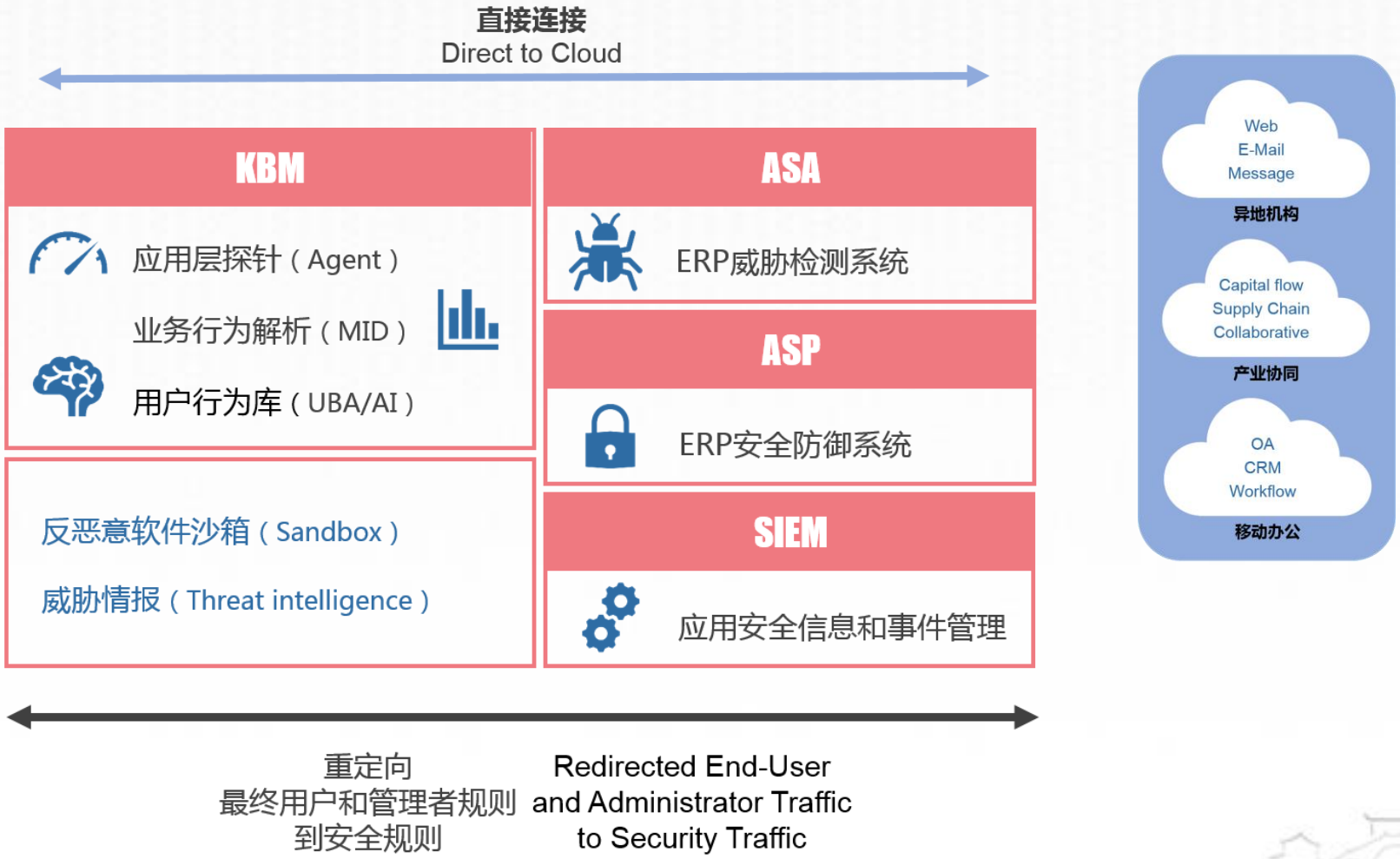
朱林　北京信御云安安全科技有限公司

Bowline® for ERP

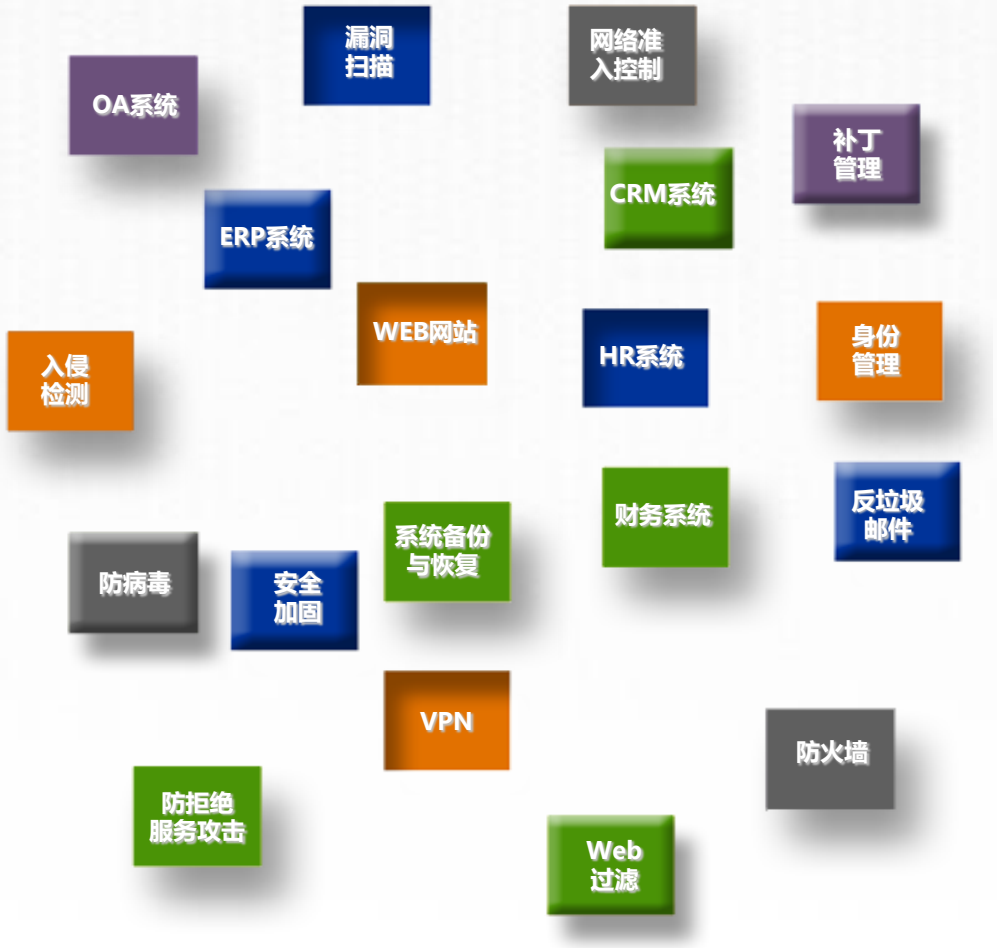
Security Technology

Bowline可以理解为一个整体设计、按需配置的“应用系统安全运作和分析平台”。有两个特点：**All in one**、**Security+ERP**





现状-单点安全方案的堆砌



- 企业中有大量的业务系统和安全系统
- 仅从各自视角看待问题
- 功能上相对独立
- 管理上相互割裂
- 无法集中监控管理
- 独立系统的简单叠加

问题-安全运营面临的挑战

企业安全状况

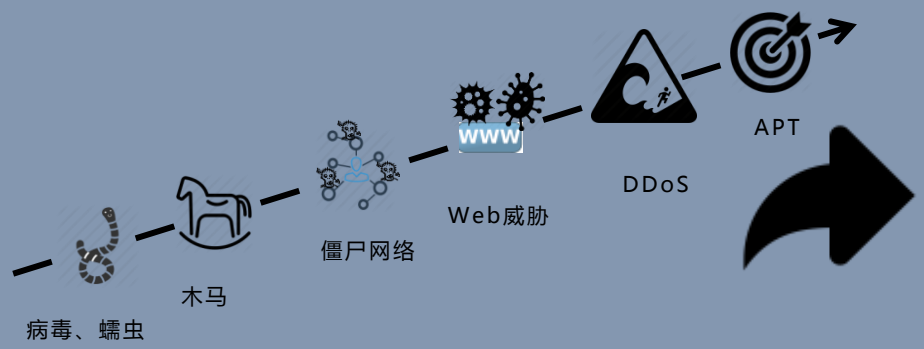
网元各自为战

运维困难

签名机制捉襟见肘

业务复杂度高

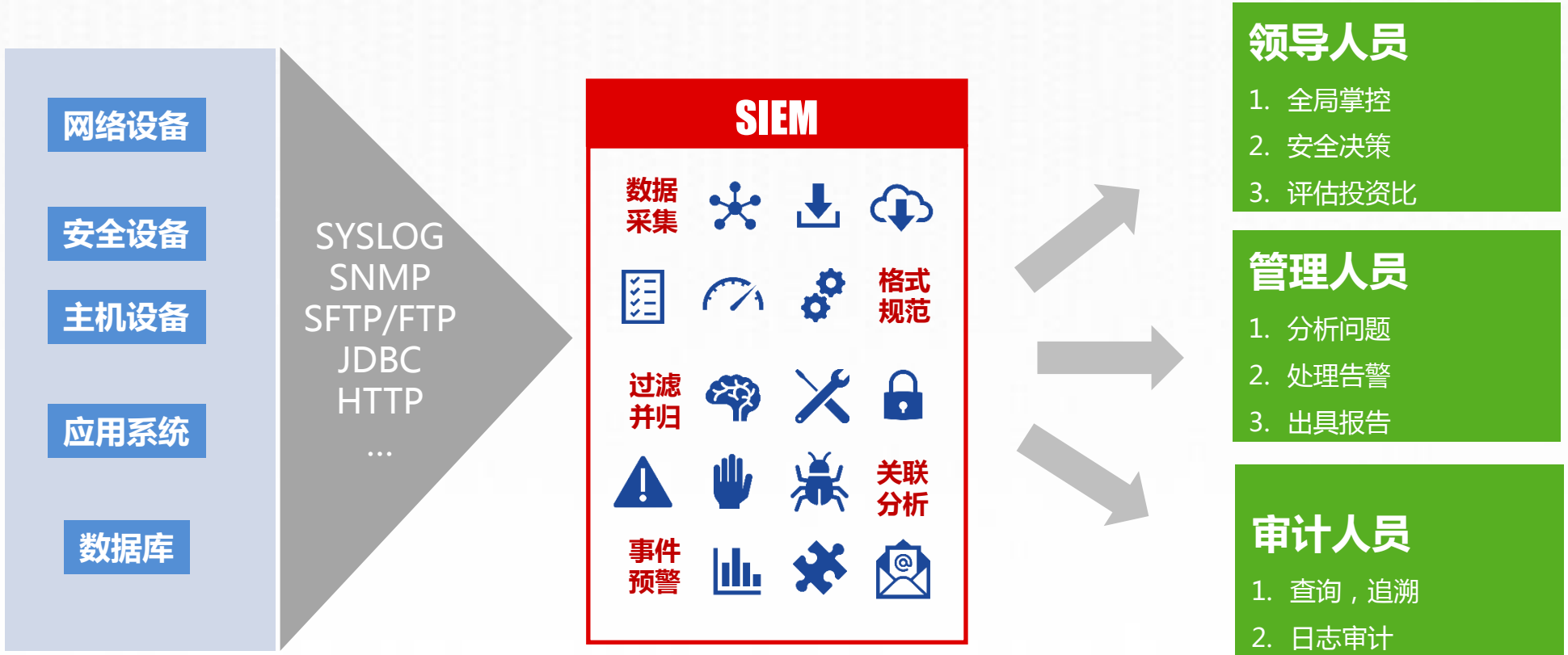
网络威胁



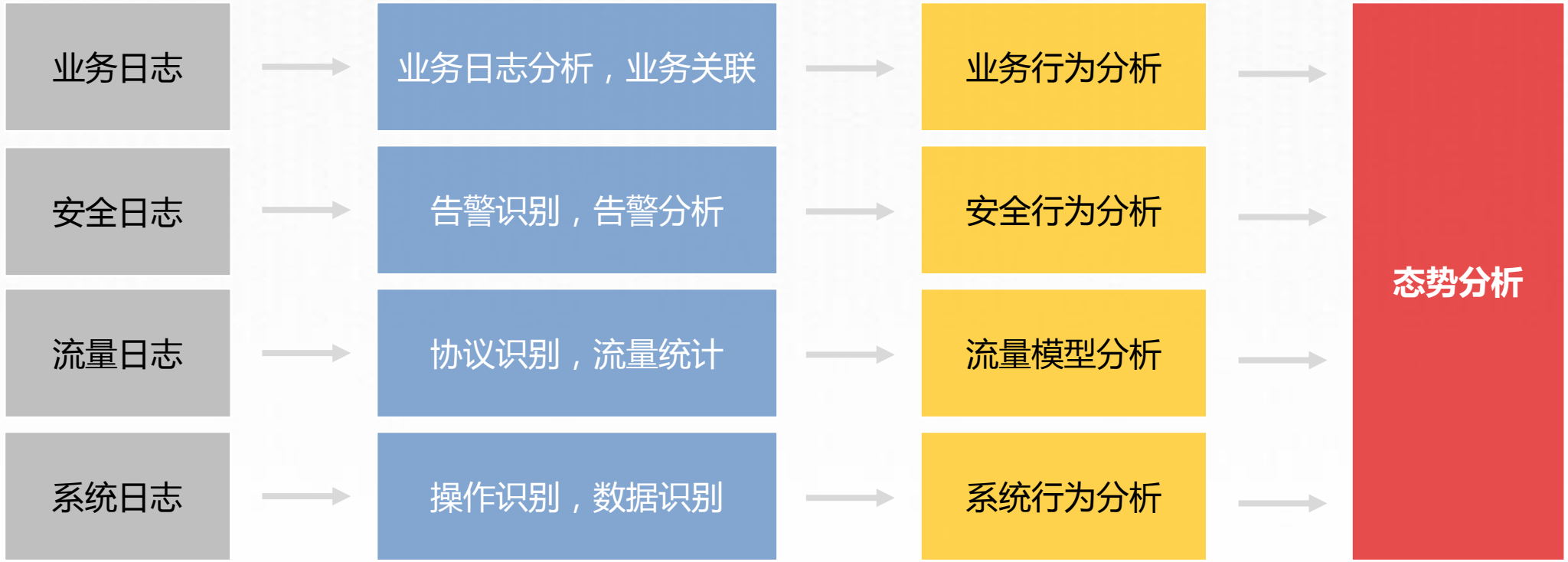
威胁类型激增 + 躲避&组合攻击 + 难以管控

什么是SIEM（安全信息和事件管理）？

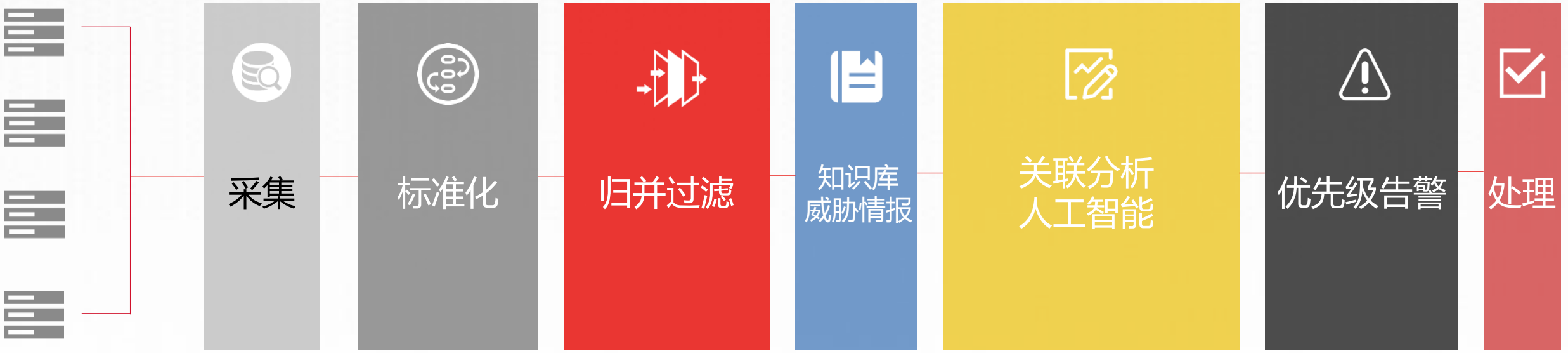
SIEM（Security Information and Event Management，安全信息与事件管理）



SIEM数据来源


业务日志
安全日志
流量日志
系统日志
业务日志分析，业务关联
告警识别，告警分析
协议识别，流量统计
操作识别，数据识别
业务行为分析
安全行为分析
流量模型分析
系统行为分析
态势分析

数据处理流程



企业应用效果

有效地降低企业安全威胁	■ 从海量汇总信息中屏蔽大量无用信息，及时告警重要的安全事件 ■ 内置丰富的告警分析策略和威胁情报来源，及时准确地发现海量日志信息中的已知威胁 ■ 消除各安全系统孤立情况，报警信息相互关联，分析挖掘潜在的安全威胁
显著地提高安全运维效率	■ 支持安全设备、网络设备、操作系统、数据库、业务系统等各类软硬件产品，全面地监测企业安全态势状况，有效降低安全事件威胁影响 ■ 简单直观友好的图形化界面展示，便于快速发现、分析、响应、处置安全问题,节省时间成本 ■ 实现安全技术和安全管理有机结合实现统一指挥调度
更好地满足合规审计要求	■ 支持海量日志的快速查询和存储，满足企业自身日志审计需求和国家对企业日志存储的合规要求 ■ 内置的丰富的报表模板，快速生产国家合规报表和企业自身要求报表，充分满足上级检查和企业自查的需求

产品展示

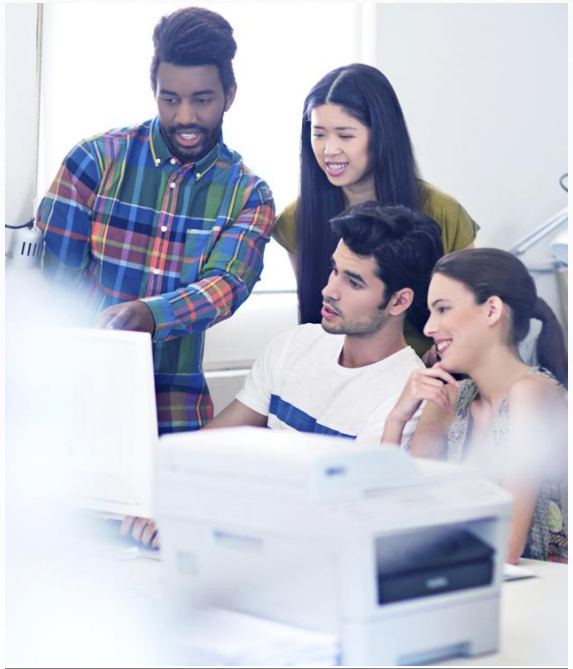

179
22530


41838
77336
51832
36


1296310
2208061
1038330
81436
1844
214959

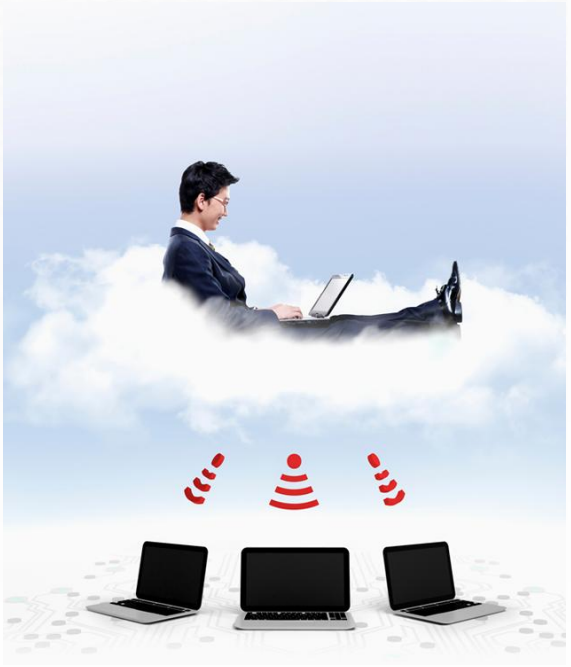
信御云安携手用友云

用友云
yonyou cloud



通过与用友云合作
带来大量优质的商机

独特的“业务安全”产品
与用友产品无缝衔接，为更
多用友用户提供优质的服务



依托用友云全新业务模式，
推动企业持续变革

未来将继续与用友云在企业
信息安全领域展开更深入的
合作

用友云 | 企业服务都在这

yonyou cloud