聚·变

第二届顺丰信息安全峰会分论坛

网络空间安全

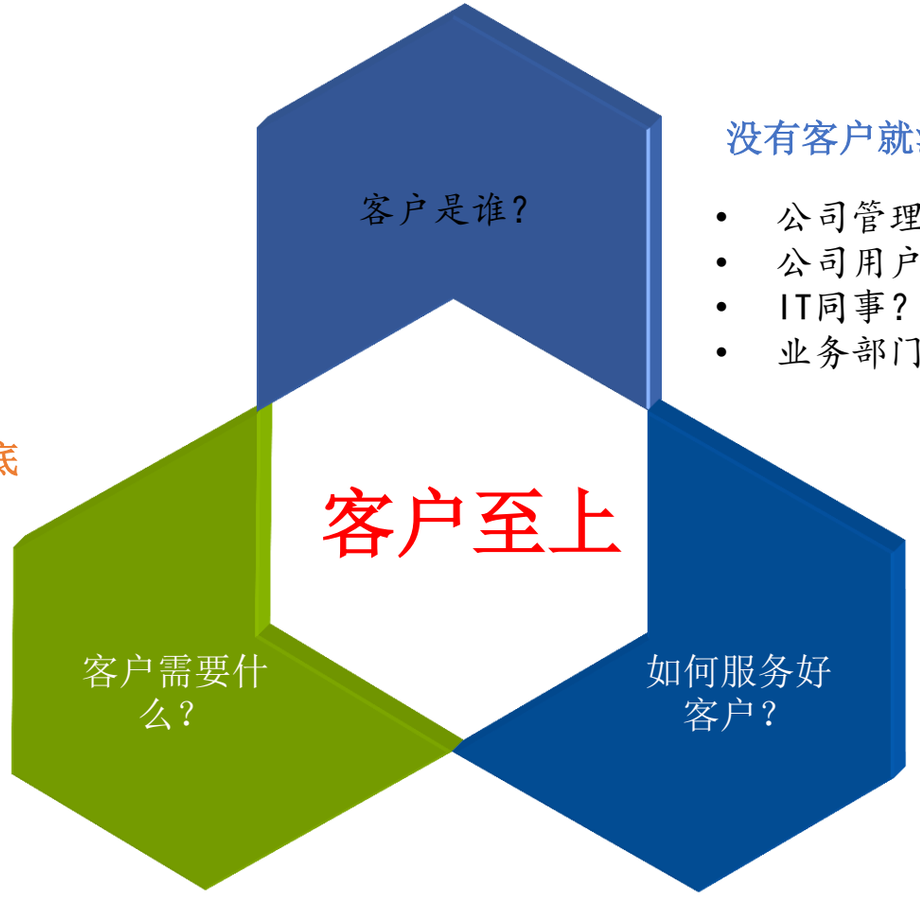
企业信息安全，如何从恨到爱？

-一个安全老兵16年的大型民企、国企的信息安全心路历程

企业信息安全建设过程中的“10万个为什么”，为什么受伤的总是我

- 用户会抱怨，为什么给我安装那么多的监控软件，电脑慢，没隐私！
- 公司IT同行对抗，为什么上线个系统要求那么多，严重影响效率！
- 老板不理解，花了那么多钱，为什么还经常出安全问题！
- 出了信息安全事故，大家都抱怨，信息安全人员都在干什么，一定要惩罚！
- 现在有关单位还可能给你寄个函，贵公司的网站XXX，请于XX日前往我单位接收处理！

以客户为中心：因为有你，所以安全



没有客户就没有这项业务

- 公司管理层？
- 公司用户？
- IT同事？
- 业务部门？

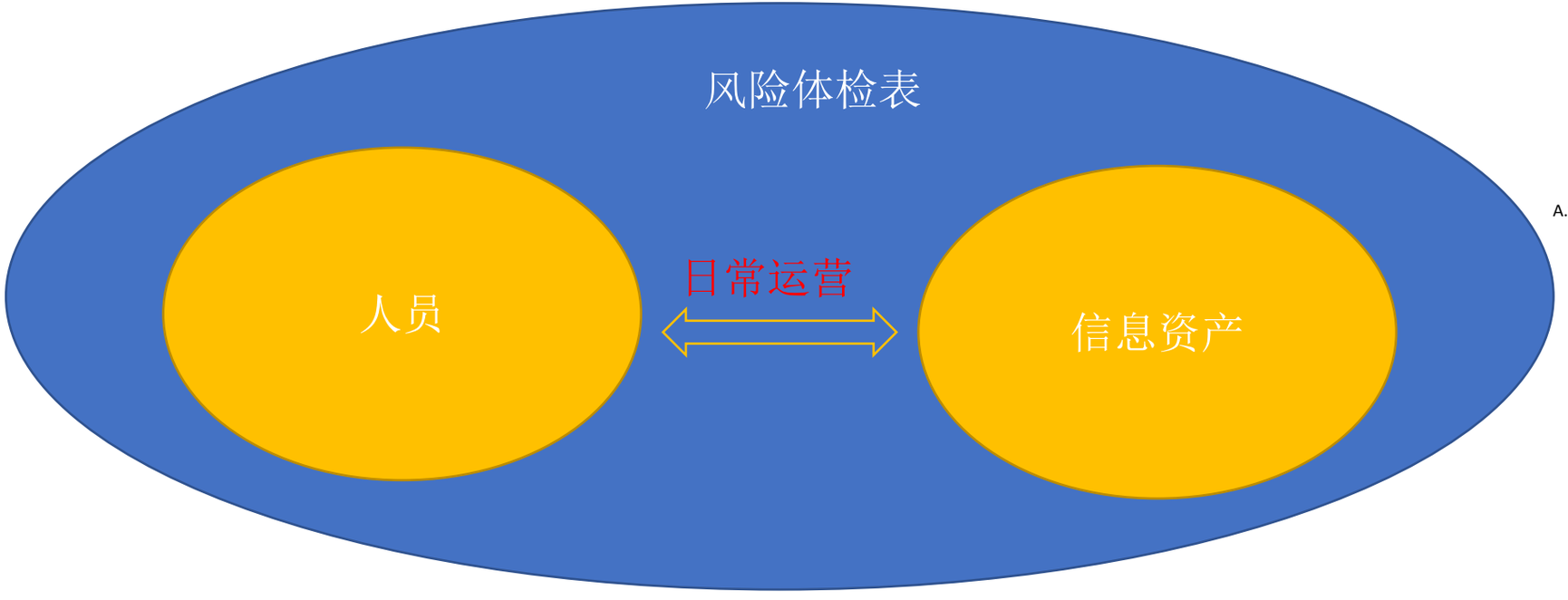
支持我们生存的客户到底需要什么

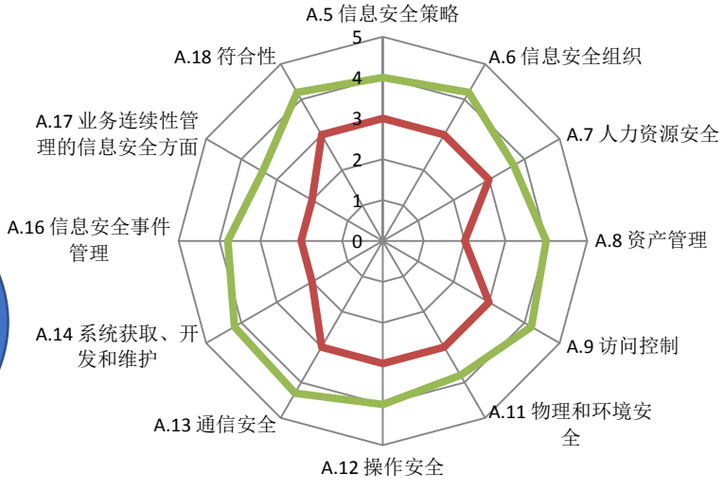
- 系统不要被攻破？
- 少踩红线，别被通报？
- 自己单位安全成熟度高点？

问题及时反馈，用户全程的参与

- 好的产品？
- 好的服务？
- 好的运营？

安全运营的是什么：人员+信息资产+风险体检表的一体化运营，提升企业安全成熟度





如何运营：成人达己，合伙共赢，团结一切可以团结的力量

信息安全是管理工作，要以业务和管理思路来推动，以技术为牵头很难达到效果

集团：IT有管理能力可以牵头，或以集办牵头，团结人力、法务等部门成立集团工作小组/委员会，定考核，落策

IT团队：以网络、主机、应用和数据风险为切入、以终为始，提高应用及数据安全质量

应用安全现状描述

应用安全从应用防火墙（waf）、应用开发安全（SDLC）、渗透、扫描4个维度整体评估。整体应用系统较为安全，可抵挡一般黑客攻击和扫描。简述如下：
1、应用防火墙（waf）：waf目前覆盖了梅林机房主要对外应用系统，阿里云的对外应用也使用阿里云的waf进行保护，较为安全可以阻挡一般的黑客入侵及扫描；少河备用机房（有物业的少量应用存在）的waf暂未启用，内部waf启用监听模式，可追溯攻击来源。
2、应用开发安全（SDLC）：未开始，存在架构、业务逻辑、部分代码层面的风险，waf无法解决，如遇高水准的黑客攻击，无法有效抵挡，风险较高。
3、渗透：外网应用已全部进行渗透检测，内网部分核心应用进行渗透检测，高危漏洞全部修复。
4、漏扫：基本全覆盖，部分一线未进行扫描，发现高危漏洞全修复。

附
1、总共有204个应用系统，其中对外发布63个，内部约141个，核心应用约51（核心平台+客户平台+协同办公+人事2个+资金+其余10个）个
2、核心应用评判标准：支撑面向客户交付的应用且停止服务会给公司造成重大损失或影响如：ICP，客户平台，K2，微V，官网），承载关键信息流或作为关键数据的数据源（如：资金系统）。

应用安全评估标准

安全分数（满分100）	waf覆盖-30%	SDLC-35%	渗透-25%	漏扫-10%	总分
得分	70-30%=21	0-35%=0	60-25%=15	90-10%=9	21+0+15+9=45
打分描述	1、内网2台监控，2、梅林主机房启动阻断，少河机房暂未启动	没做	1、外网应用系统全覆盖 2、内网核心应用系统部分覆盖	覆盖率高达90%以上	

IT基础-应用-数据安全标准

说明：

1、适应范围：
--适用于万科集团公司（含万翼科技、一线地产和新业务）自行建设、运维、管理的IT基础环境和开放的应用系统。
--部署于第三方数据中心（非万科管理）和海外地区的系统参照实施。

2、目的：针对万科科技团队在系统开发、系统部署、系统运维及数据使用过程中，建立安全技术及标准，减少主机上线、应用系统运营及数据使用面临的风险。

3、版本：本稿为V1.0版本，后续由公司协同办公与信息安全部进行更新。

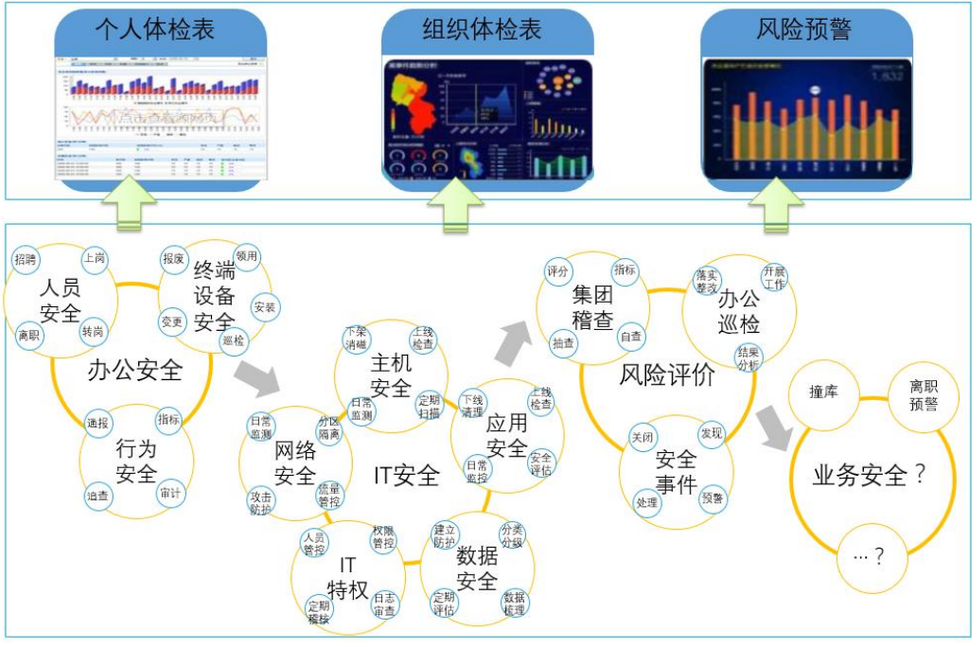
4、集团安全联系人：主机安全--XX，网络安全--XX，应用安全--XX，数据安全--XX

公司用户：以安全红线、办公巡检和安全考试为切入，让员工主动参与学习和提升

一线及业务单位：建立金银铜排机制，搭台唱戏，内部赶帮超，落实谁运营谁负责、谁使用谁负责、谁管理谁负责

科技赋能安全：信息安全体系能力通过平台固化，安全风险可视化和数字化，安全能力服务化，并逐步向业务安全发展，安全行业的“ERP” 将会加速发展，这也是以科技能力服务好客户的需要

安全作业中心



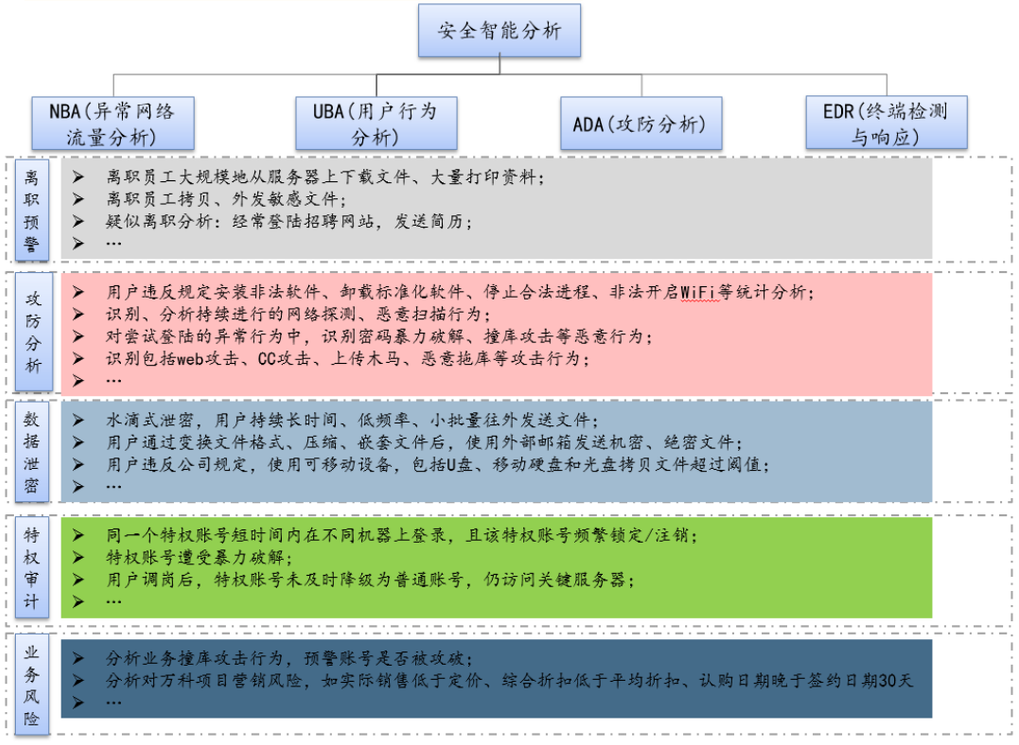
01 安全管理和体系能力通过平台固化，降低对人的依赖

02 面临的挑战越来越复杂，需要科技能力解决安全问题

03 客户信息保护、业务系统安全由被动到主动

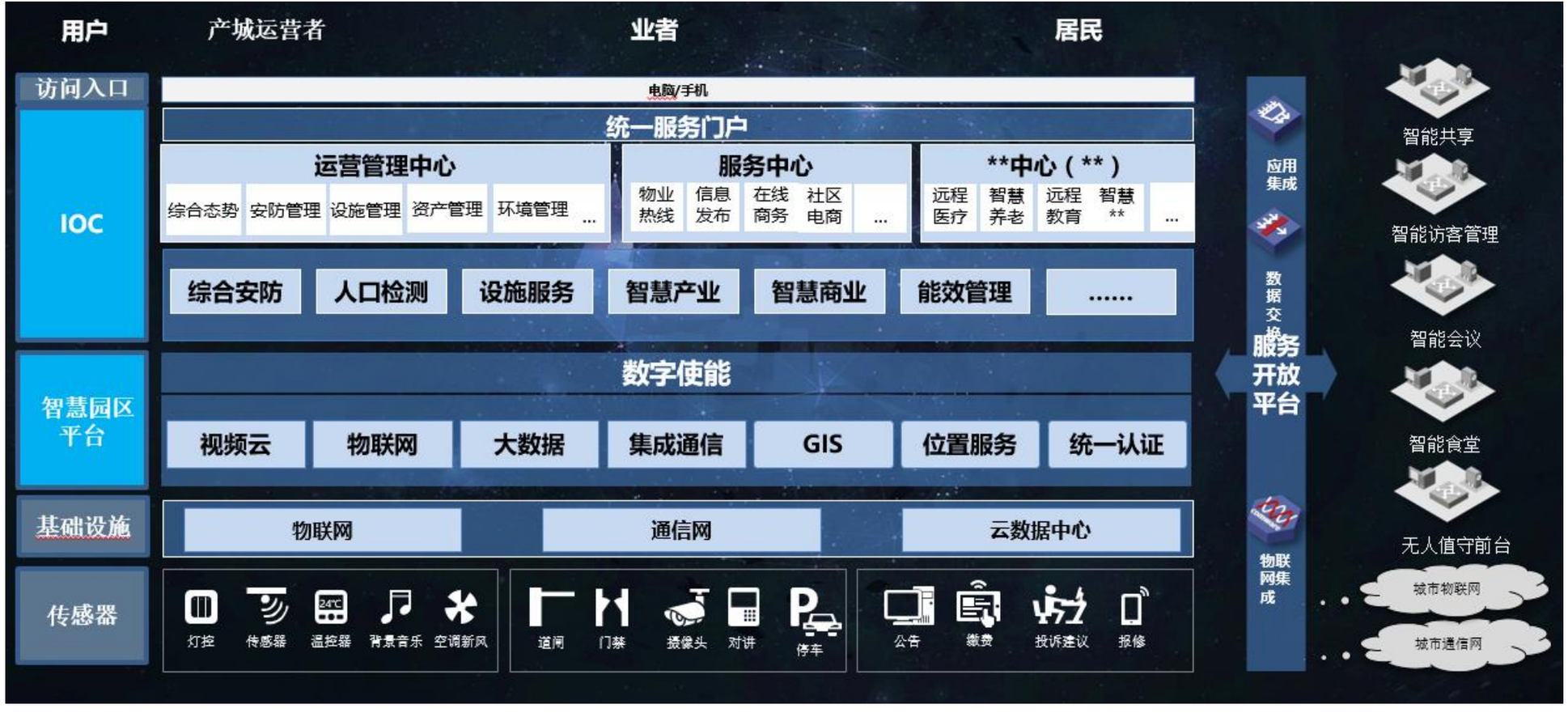
04 合规合法要求高，需信息平台支持体系运作和落地

数据分析和预警中心



业务视角的适度超前：在满足人们美好生活需求的驱动下，办公和生活的智能化，各类场景设备物联将是大势所趋，安全如何应对？

产城物联网 ＋ 智慧办公



THANK YOU