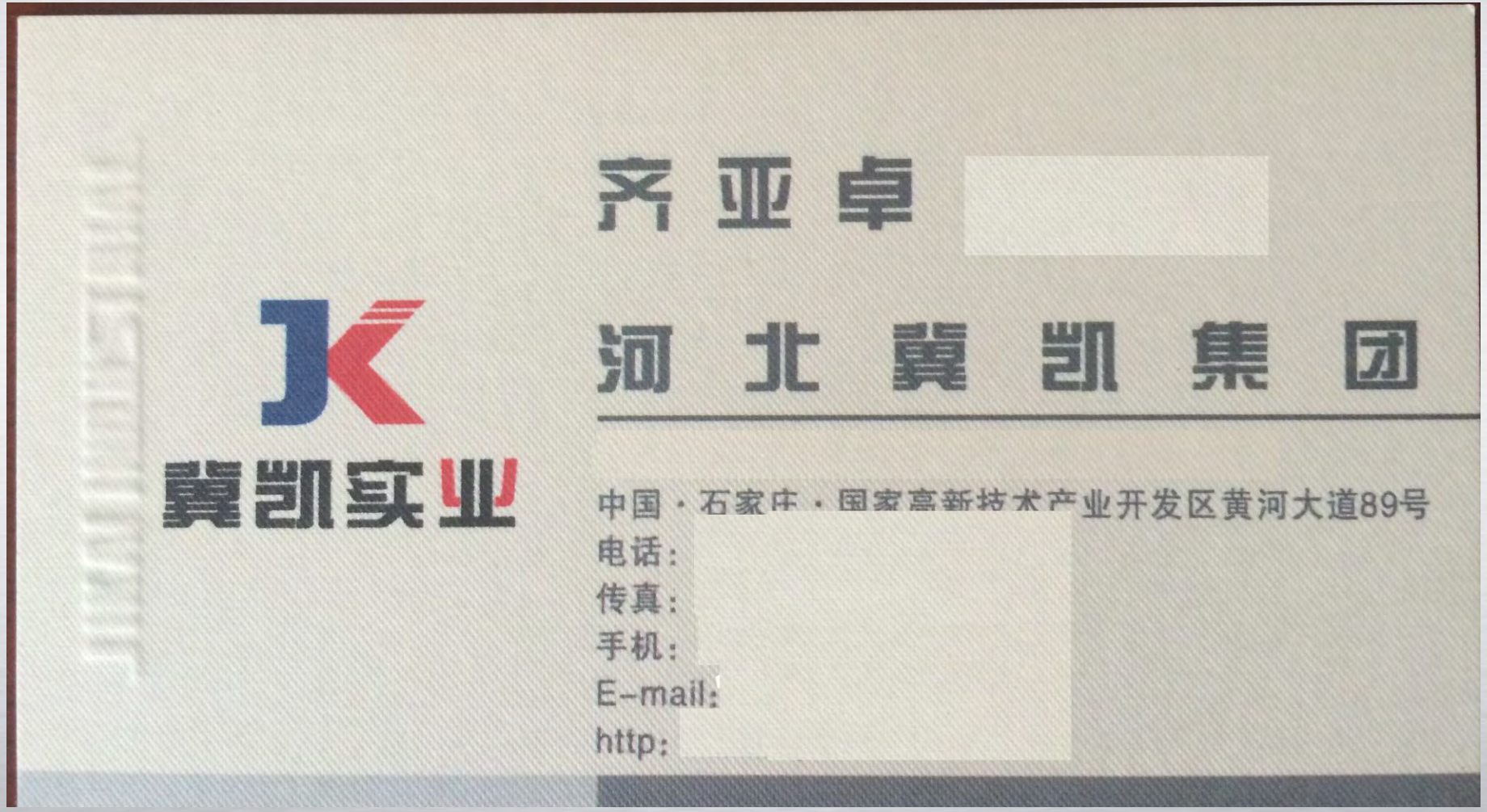
制造企业精益安全管理

—冀凯的WIMS之道

冀凯集团

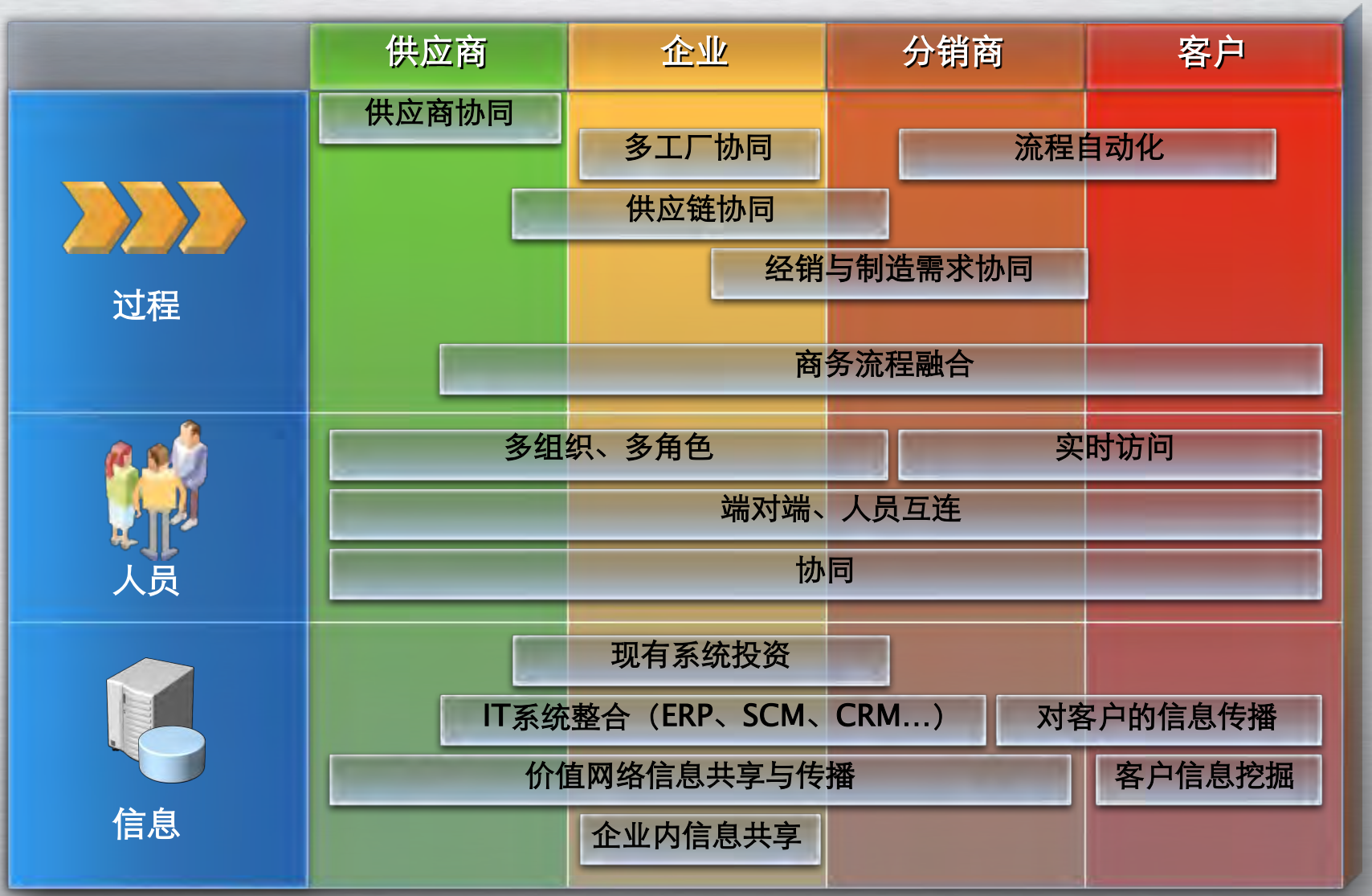

齐亚卓
河北冀凯集团
冀凯实业
中国·石家庄·国家高新技术产业开发区黄河大道89号
电话:
传真:
手机:
E-mail:
http:

目　录

1

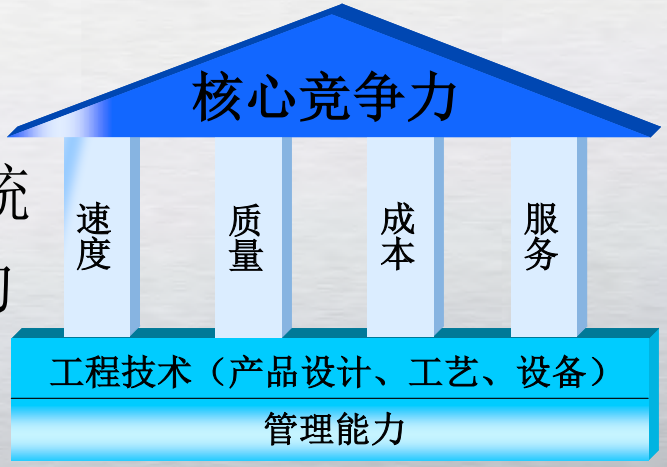
制造业信息化诉求

通过信息技术实现过程-人-信息的整合



信息化软件情况

- 数字化设计CAD/CAM/CAE/CAPP，实现产品生命周期管理PLM
- 数字化制造技术：数字化样机、数控加工、虚拟制造等
- 数字化管理ERP系统
  - 柔性的生产组织模式和生产管理
  - 项目驱动的先进计划排程
  - 支持多组织集中业务管控
  - 一体化的物资、采购、销售、
  - 生产、财务、质量、HR管理系统
- 制造执行系统MES，实现“可看见的现场制造”
- 供应链协同管理SCM



集团简介

- 煤矿设备、金刚石制品、金融租赁、劳务派遣、信息化软件
- 国家级制造业信息化科技工程应用示范企业
- 国家级国际科技合作基地
- 国家创新型试点企业
- 全国企事业知识产权试点单位
- 国家级守合同重信用企业
- 国家两化融合管理体系贯标试点企业
- 国家第二十一届企业管理现代化创新成果一等奖
- 省级第二十一届企业管理现代化创新成果一等奖
- 国家两化融合创新推进联盟成员
- 国家两化融合咨询服务联盟成员
- 省市两化融合示范企业

集团简介-产品展示

支护机具

锚杆钻机

锚杆钻车

张拉机具

钻杆钻头

集团简介-产品展示

安全钻机

煤矿用深孔液压钻机

架柱支撑气动手持式钻机

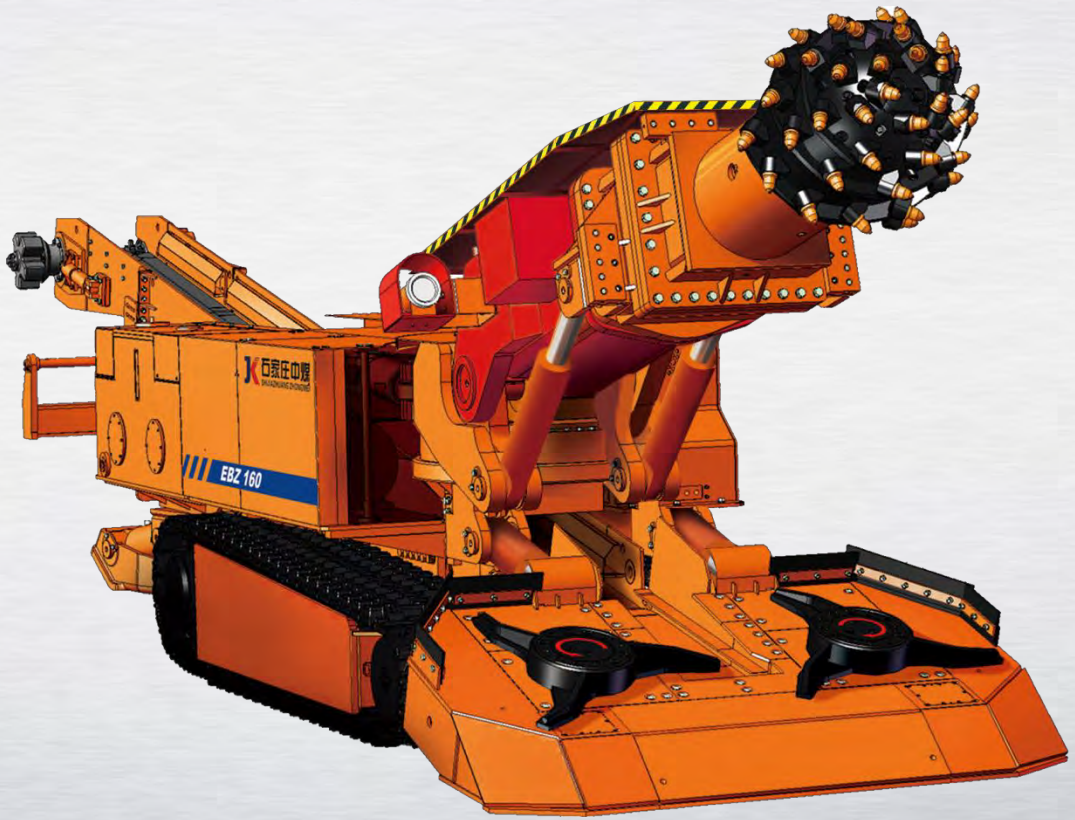
金刚石钻头

煤矿用全液压坑道钻机

煤矿用气动深孔钻车

集团简介-产品展示

掘进设备

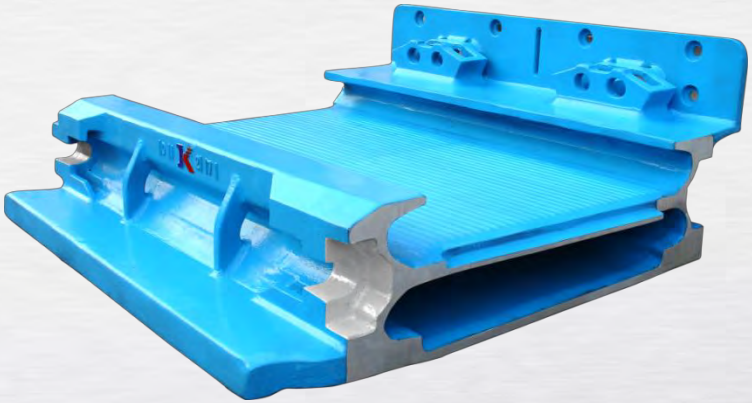


煤矿掘进机

集团简介-产品展示

运输设备

刮板输送机

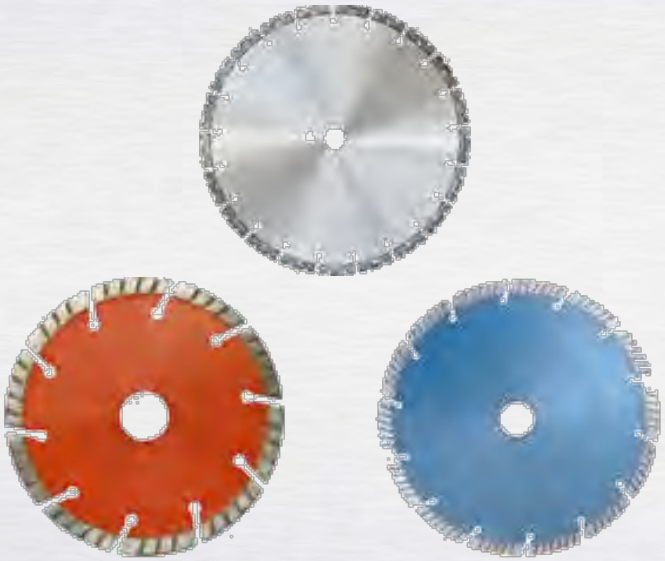


整体无焊接中部槽

集团简介-产品展示

金刚石制品

薄壁钻



金刚石锯片

金刚石磨片

装备制造行业特点

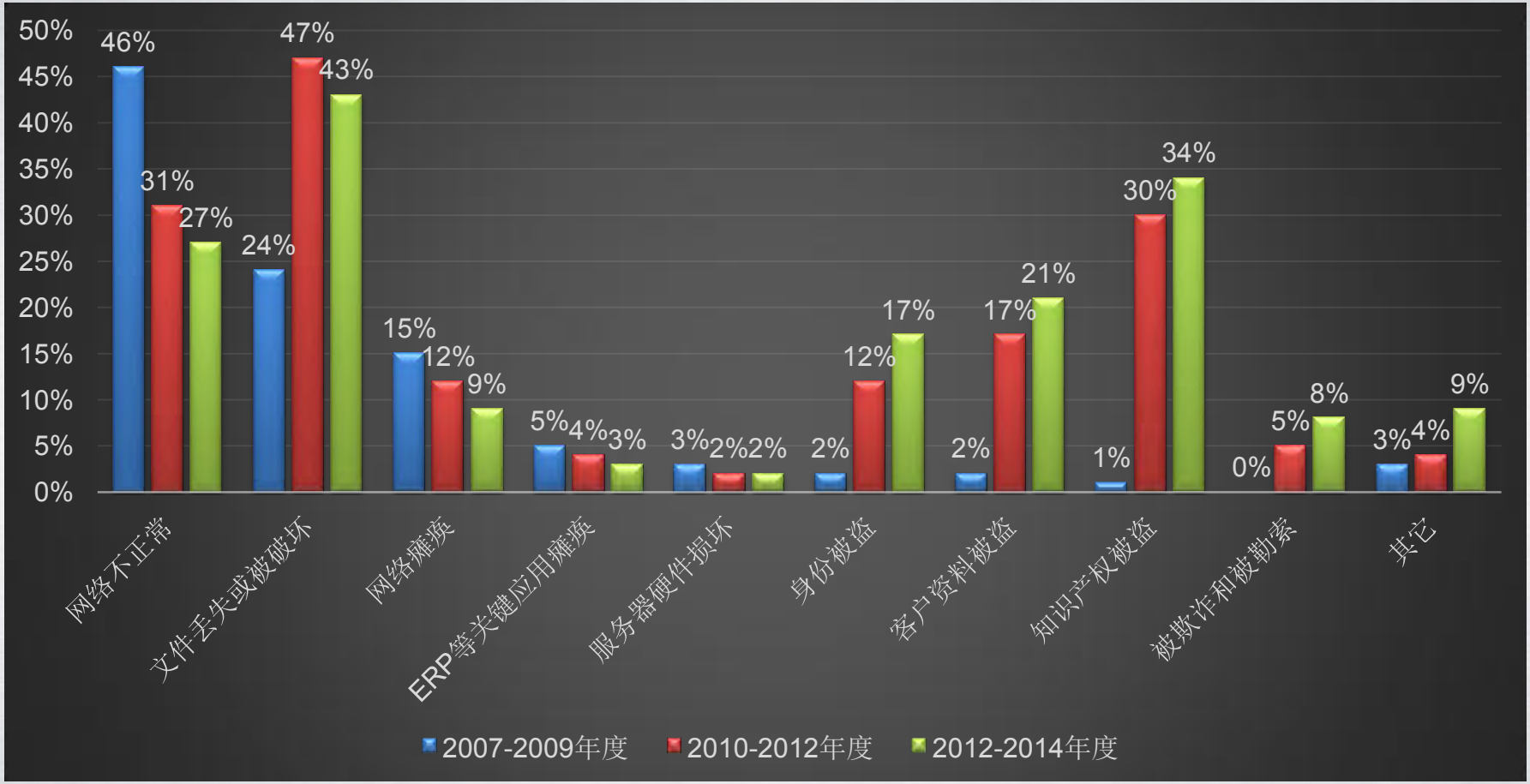
- 装备制造是典型的单件、多品种小批制造，涵盖面向库存生产MTS、面向订单装配ATO、面向订单生产MTO、面向订单设计制造ETO多种生产模式。
- 装备类产品大而结构复杂，生产工艺和制造过程复杂，生产技术准备和生产周期长，生产计划复杂多变，产品交货时间难保证。
- 装备制造产业链长、供应商多、产品配套要求高，难以按时配套，准时化物资供应难度大
- 企业在产品销售、采购、库存、物料配送、质量管理、绩效管理等方面、都需要设计部门、工艺部门提交大量设计管理信息，才能准确执行生产计划、采购计划，保证产品安装和顺利交付。




2

冀凯人的信息化安全需求

企业信息安全分析报告



从上图中我们可以看出自2010年开始企业信息安全事故的趋势产生了变化；从以前网络、ERP、服务器等硬见问题逐步转为文件丢失、知识产权被盗、客户资料被盗等软资产,我司也出现过同样的图纸外泄事件。

冀凯的信息化安全需求

国内外权威机构进几年来构成企业信息安全的威胁主要来与企业内部

经过数年的信息化建设2010已完成部分：

服务器、数据库、存储、最终用户分别划分到不同的网段，按需访问;
任何服务器或网络出现问题不会产生任何数据丢失;
基于授权MAC地址的可控制网络访问;
有效的保障了服务器、应用、数据库等日常安全
统一安装金山企业版杀毒软件及360安全卫士（这两套为免费软件）

目前存在的问题：

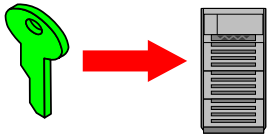
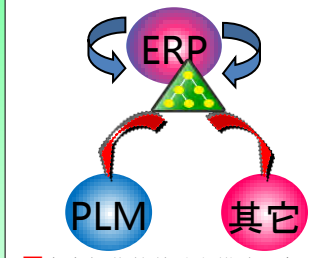
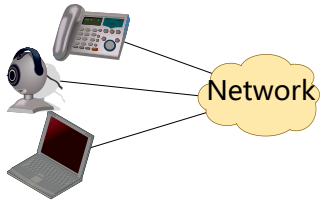
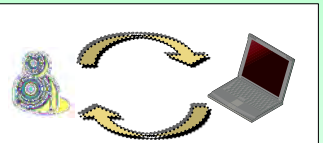
1、虽有杀毒、安全软件部分人员人为阻止其病毒库、木马库未及时更新，这种情况下不但影响自己，也会影响到自己所在的网段所有人的安全;
2、目前燕郊存在30个以上USB无线网络热点，用于个人手机、pad、笔记本随意接入公司网络;
3、通过现有能力已能屏蔽U盘、移动硬盘等存储设备接入公司电脑，但由于业务部门需求导致端口无法全量封堵;
4、对某一分公司361部电脑进行统计共发现1938款软件;
5、工作期间利用公司电脑玩游戏、聊天、干私活等;
6、利用公司网络访问色情网站;
7、员工存在众多的对外联络方式；如邮件、QQ、MSN等一旦发生泄密事件无法追述;
8、通过非法代理工具为其不具备上网条件的同事提供上网服务;
9、以共享方式进行文件交互;
10、公司出现数据遗失时没有相应的追述和防遗失手段;

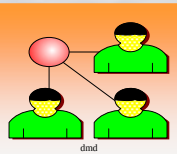
3

冀凯人的信息安全应对

解决方案

安全管理架构

	核心数据	系统及应用	网络及支撑	桌面终端
目标	建立简单、易用、可审计的安全架构体系，实现安全策略的标准化和流程化，强化安全事件的集中监控和处理			
对策	✓核心数据零丢失 ✓服务器故障5分钟恢复  □应用服务器每7天执行一次快照 □所有系统产生的数据均备份至存储 □数据库按照保障每天一次备份 □存储采用主备模式数据间隔5分钟	✓保障主备系统双活 ✓通过端口策略和日志全量保障服务器  □在虚拟化的基础上搭建服务器环境，单一应用服务出现问题后15分钟切换到其它应用 □全量记录服务器日志， □数据库及应用服务器开启自身防火墙，只放行允许端口；	✓基于防火墙构建域安全 ✓网络隔离及访问控制 ✓基于MAC地址的身份限制 ✓  □通过内网、外网、专网防火墙对所有用户进行域划分  □应用、数据库、特殊业务部门网段进行隔离保护 □全局用户白名单准入	✓时时掌控客户端安全运行状况 ✓统一管控外接设备  ✓客户统一杀毒及安全软件  ●全面实现终端加入域，强制WINDOW登录12位



●构建人力、行政、信息三位一体的组织

●制定安全标准/流程

解决方案

通过2010年的硬件建设，及2014年信息部自建部分冀凯的企业安全以具备了一定的基础，建议从以下方面开始实施：

一、桌面安全：

1、通过网络挂接存储和计算机加装还原卡实现计算机内不保存任何数据，重启电脑后数据清零；

2、对所有计算的应用端口（USB、串口等）进行审计和管理，达到数据只入不出的管控模式；

3、对于技术体系建立外网资料查询摆渡机，通过安装隔离卡实现内外网物理分离

4、所用计数机全部进入域，每日务必关闭计算机；

二、网络隔离：

1、对全集团的计算机实现网络全隔离，不同网段之间不能访问和共享，如共享可通过RTX、OA、邮件、云存储（只针对科级以上）；

2、外发文件一邮件作为第一发送方式，对于大型文件的外发在信息部指定终端上完成；

3、以MAC地址为唯一放行标记，通过ACL白名单全量屏蔽非法用户；

4、基于ACL白名单技术屏蔽一切网络中不可用的端口；

三、行为审计

1、按照员工的岗位职能划分行为约束规则；

2、按时段限制员工的网络流量；

解决方案

3、监控员工的的网络行为（聊天内容、邮件内容、光看网页内容等）；

4、强化邮件发送规则，无对外业务的用户只拥有公司内部的邮件收发权限，全员邮件收发内容可查可记录

四、外部办公安全

1、当计算机脱离公司环境后必须通过VPN接入公司网络，否则任何系统无法访问（包括邮件、RTX、OA等）；

2、对所有外出电脑启用DLP，限制其文件打印和显示次数；

五、安全教育及管理

1、通过微信、OA、内刊、手册、贴画、鼠标垫等提高员工安全意识；

2、以自然月为间隔进行员工安全教育，每年分两次对新员工进行教育；

3、组建信息安全管理专项部门，由人力、行政、信息3个部门抽调人员；

六、硬件安全（可选）

1、为机房添加柴油发电机，保障机房的动力不间断；

2、通过新购及利旧的方式在运营商的IDC中构建新的一套环境，实现一地两中心的双活数据中心，保障各系统的实时有效运行；

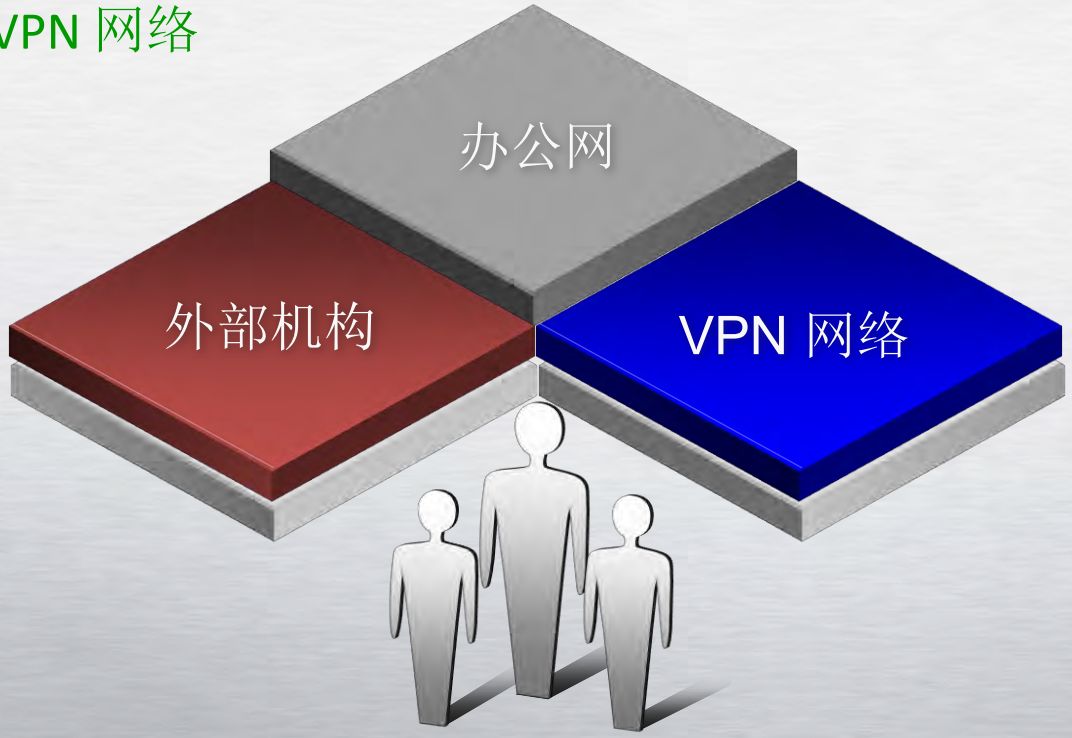
一、二、三、四

统一数据中心

整体部署

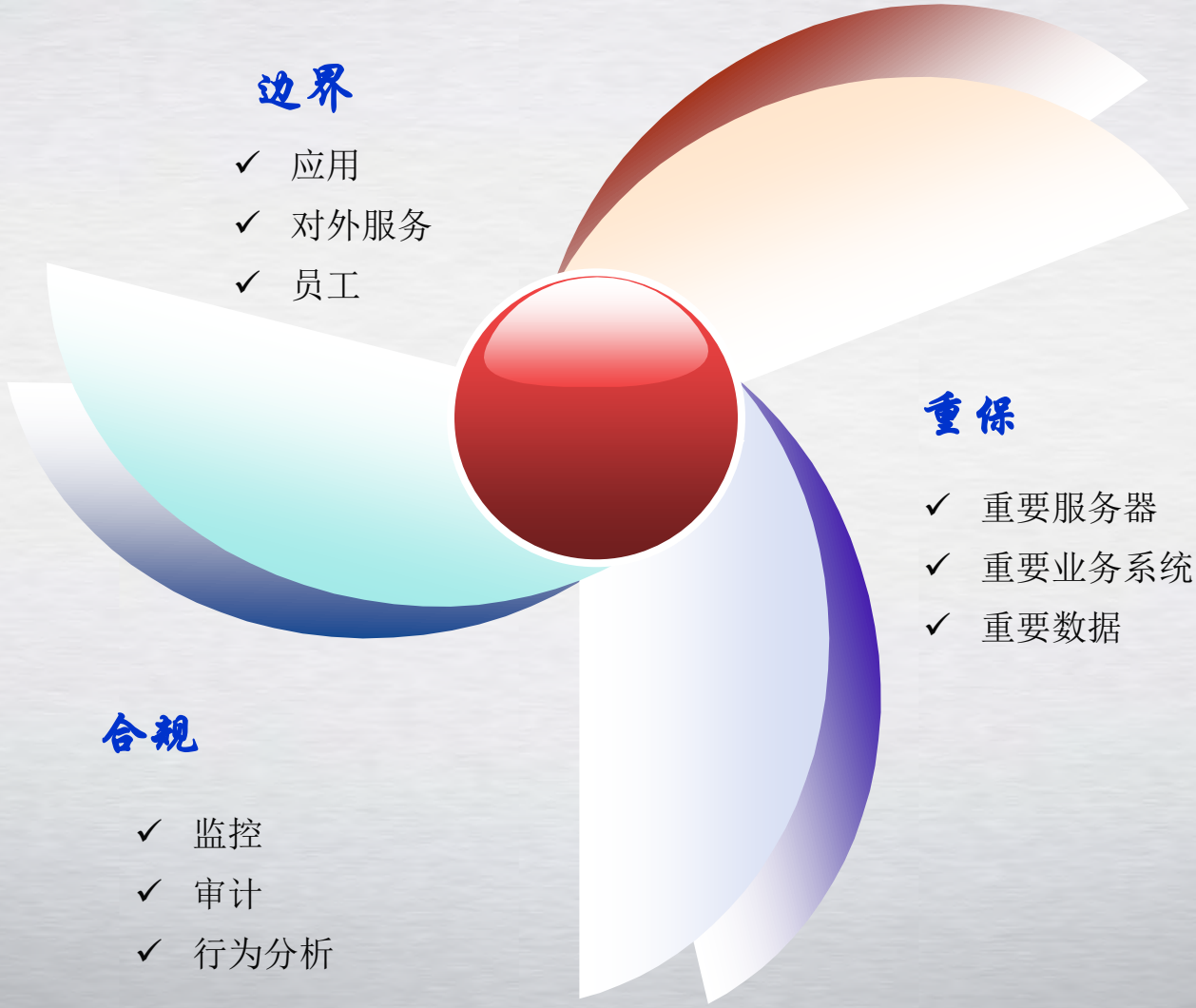
数十个Lan办公网络

- 众多的成员单位
- VPN 网络



两个平衡

三个博弈



边界

- ✓ 应用
- ✓ 对外服务
- ✓ 员工

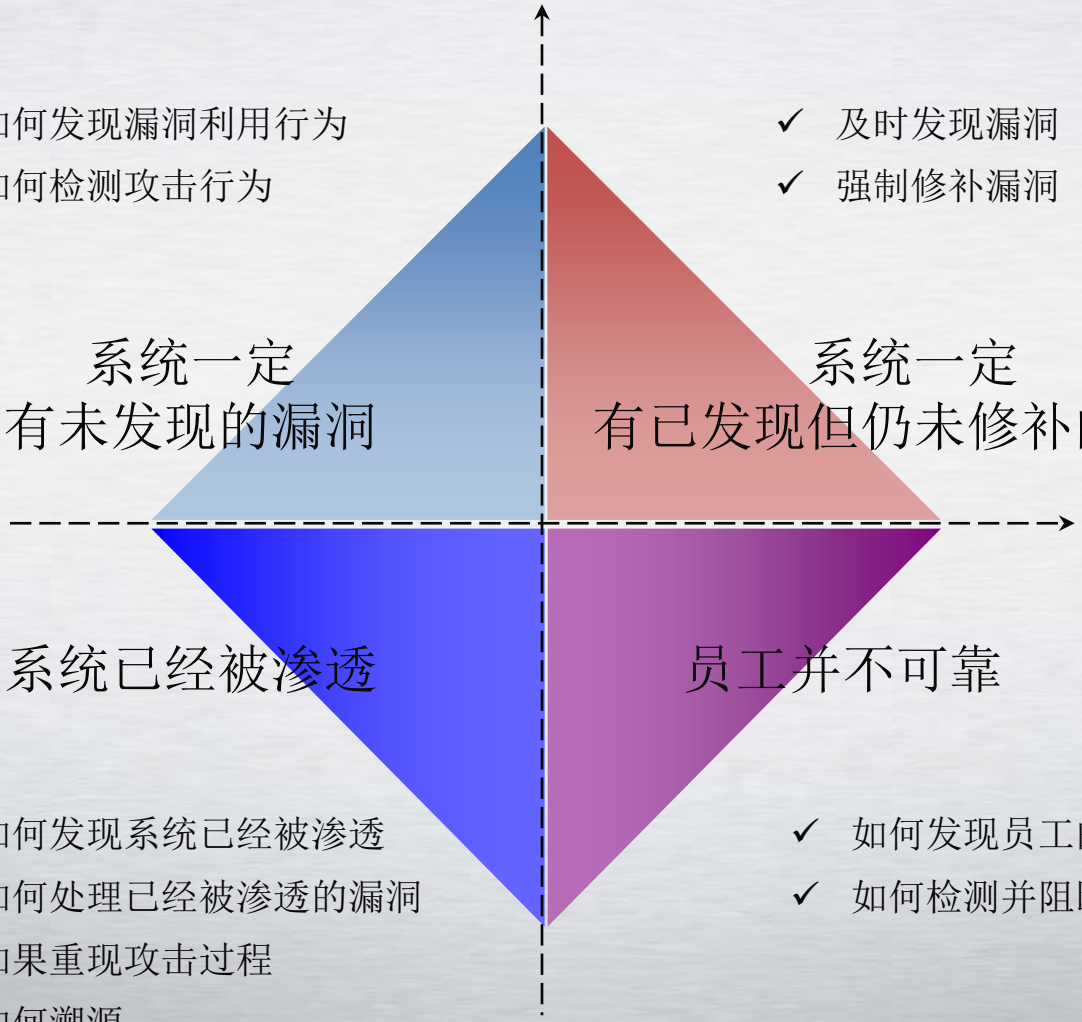
重保

- ✓ 重要服务器
- ✓ 重要业务系统
- ✓ 重要数据

合规

- ✓ 监控
- ✓ 审计
- ✓ 行为分析

四个风险



- ✓ 如何发现漏洞利用行为
- ✓ 如何检测攻击行为

- ✓ 及时发现漏洞
- ✓ 强制修补漏洞

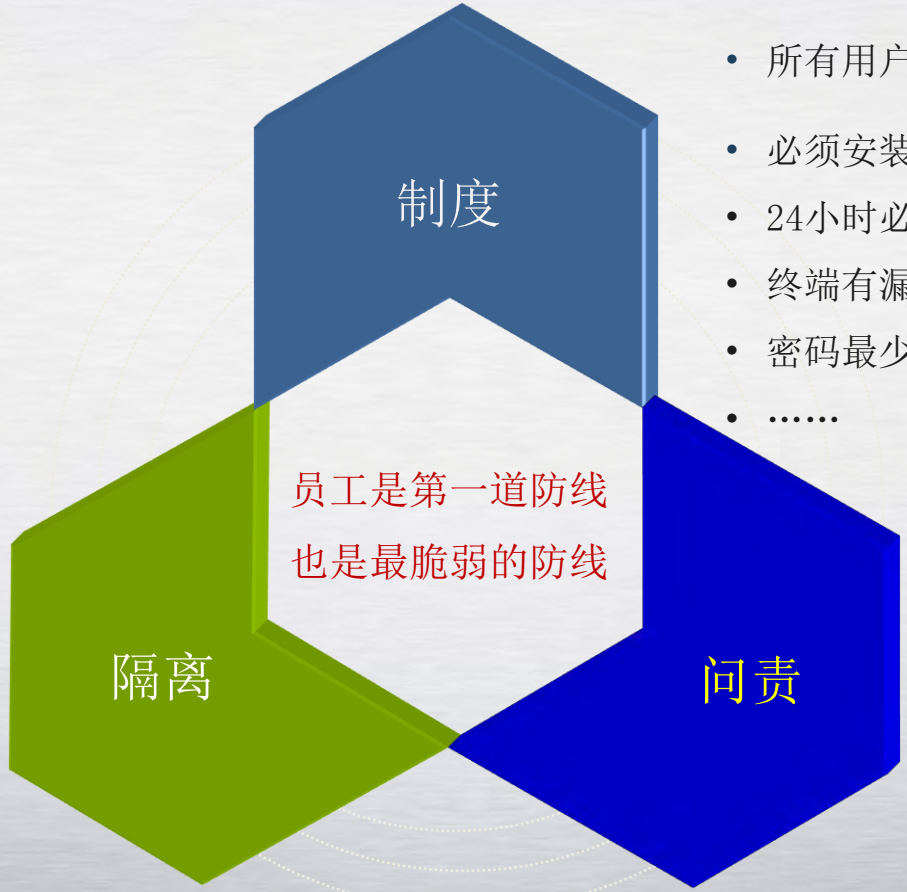
- ✓ 如何发现系统已经被渗透
- ✓ 如何处理已经被渗透的漏洞
- ✓ 如果重现攻击过程
- ✓ 如何溯源

- ✓ 如何发现员工的异常行为
- ✓ 如何检测并阻断来自内部的攻击

安全是责任

强制策略

- 所有用户必须加入域
- 必须安装指定的安全软件
- 24小时必须重启一次
- 终端有漏洞必须修复
- 密码最少15位
- ……



最小化访问权限

- 生产网与办公网隔离
- 办公网与办公网隔离
- 办公网内部主机间隔离
- ……

不妥协！

- 小问题警告（事不到三）
- 大问题辞退（零容忍）
- 问责诛连到部门负责人

服务器与业务系统

监控

全局服务实时监测

全局流量实时听包

综合运维

统一登陆认证

集中运维审计

补洞

实时扫描线上系统漏洞

抓取最新发布漏洞

测试分析后迅速修复

异地容灾

一地两中心在线同步

负载均衡，灾难调度

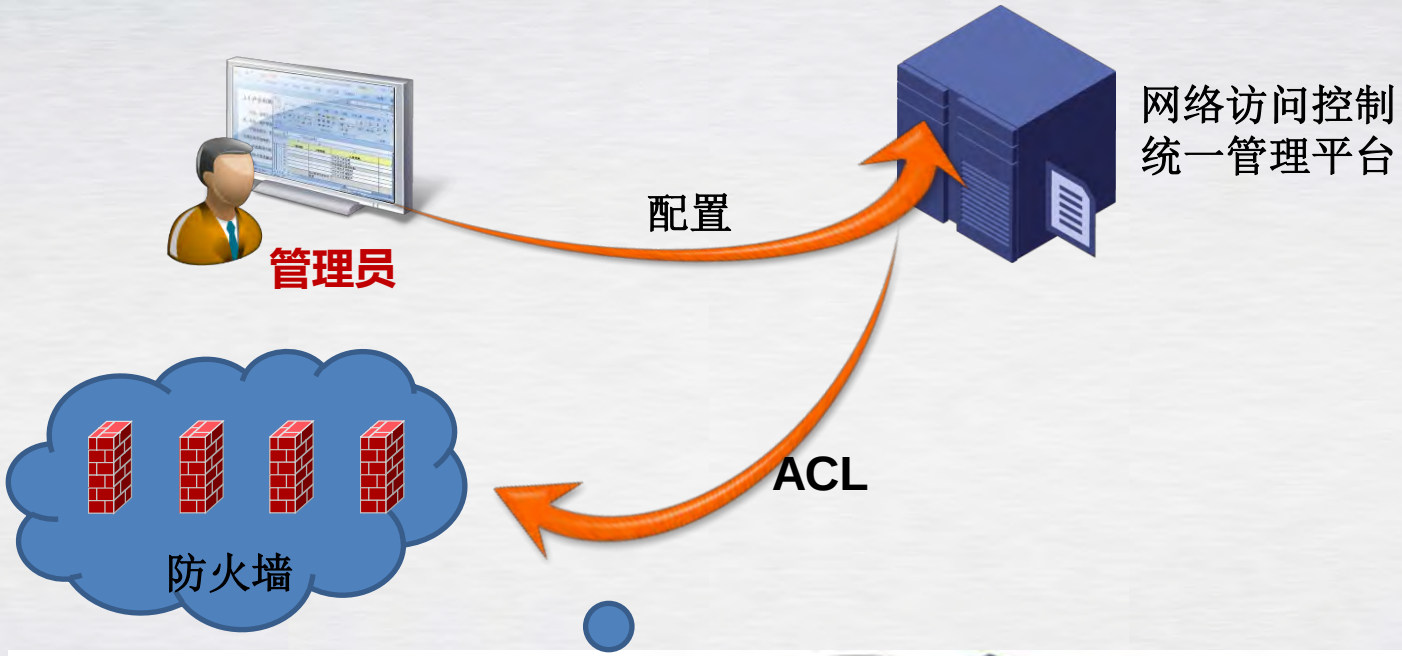
离线备份作为后援

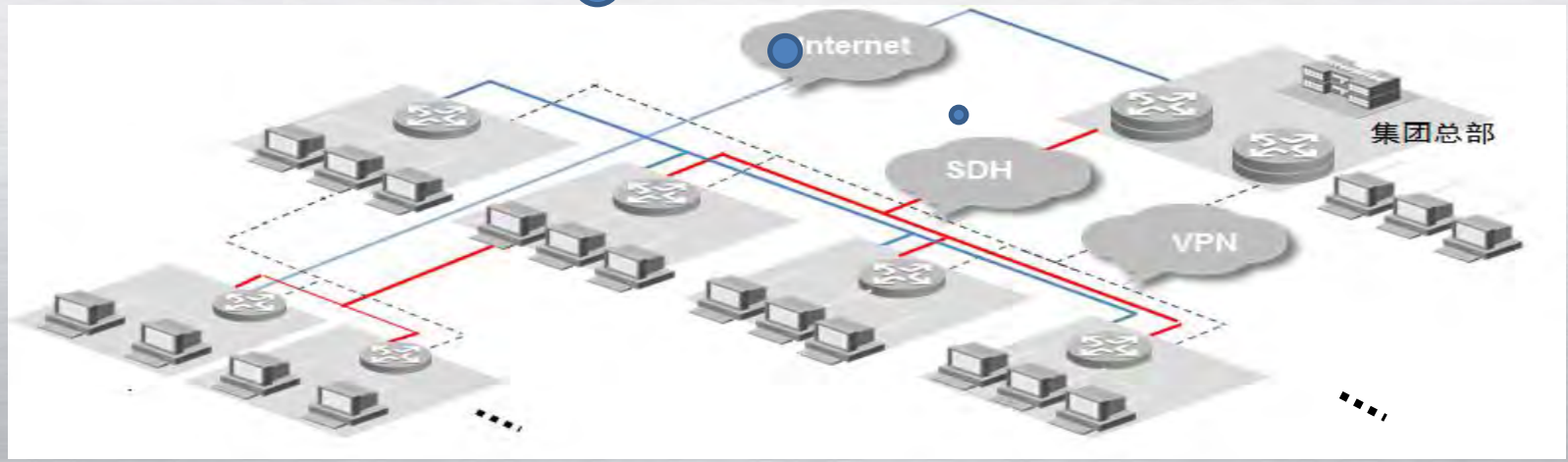
日志分析

实时抓取系统日志到日志服务器

识别日志异常并报警

网络访问控制统一管理平台





Wifi终端设备：受控使用

- 通过MAC认证的设备才能使用公司内部的Wifi上网
- 只有使用域账号才能连接上公司内部的Wifi
- 可以通过AC定位到Wifi终端的物理位置

BYOD远程办公：数据隔离与加密

- 动态口令识别
- 办公数据加密
- VPN通道加密
- 基于MAC地址的身份识别

请各位专家批评指正！