互联网时代制造业的信息安全探索

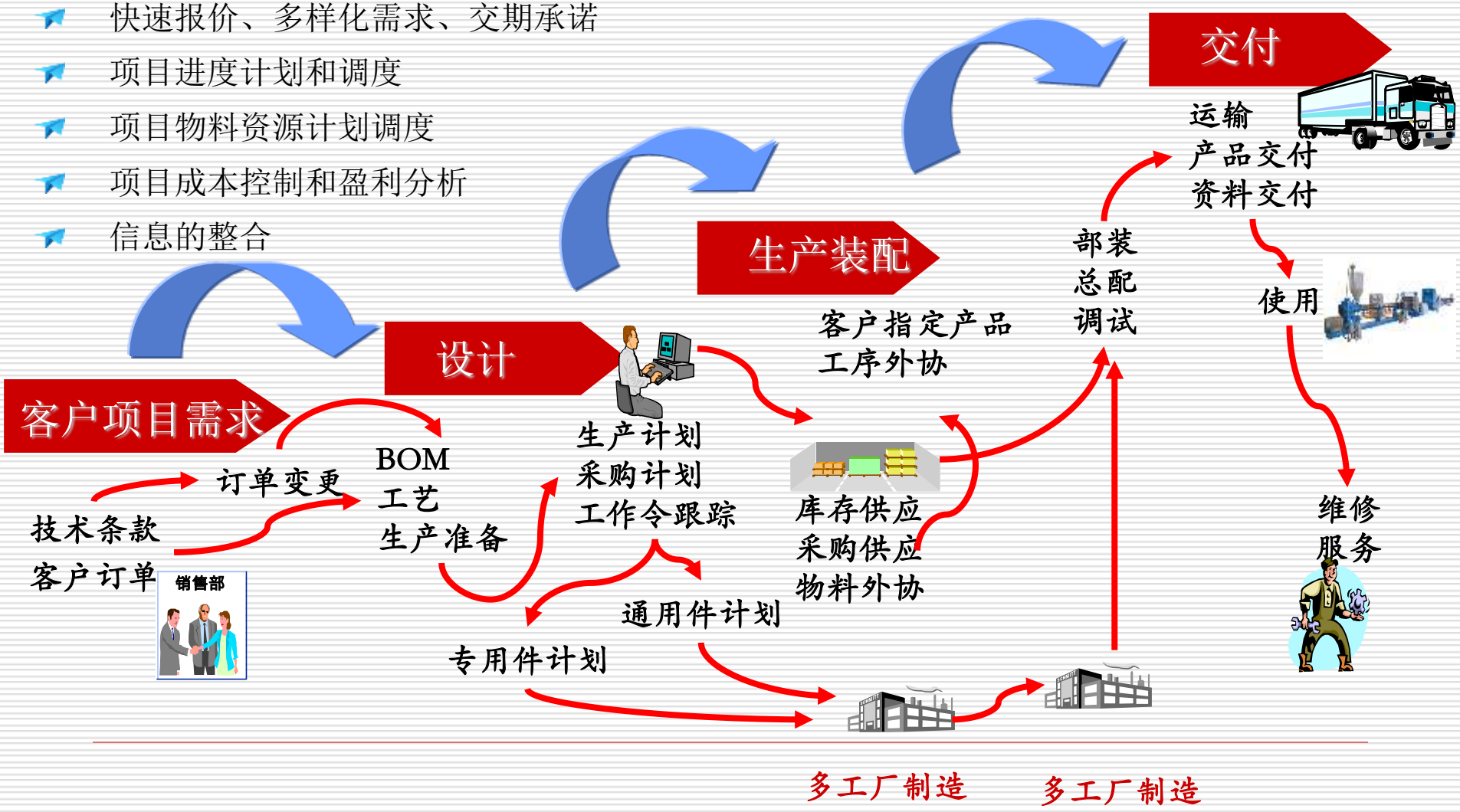
齐亚卓
atlsico@hotmail.com

目录

- 制造型企业信息安全见解
- 新宏昌重工信息安全分享

装备制造行业的管理重点和难点

- 快速报价、多样化需求、交期承诺
- 项目进度计划和调度
- 项目物料资源计划调度
- 项目成本控制和盈利分析
- 信息的整合



企业全面走向信息化

- **ERP**：企业资源管理
- **CAX**系统：产品设计与开发
- **SCM**系统：物资供应链管理，管理企业的供货资源
- **CRM**系统：客户关系管理，管理企业的客户资源
- **PLM**系统：产品生命周期管理，与生产、销售密切相关
- **PDM**系统：产品数据管理，与生产、销售密切相关
- **WEB/**代理服务：信息发布和信息获取
- **OA/**邮件系统：管理内部邮件和日常办公的公文流转

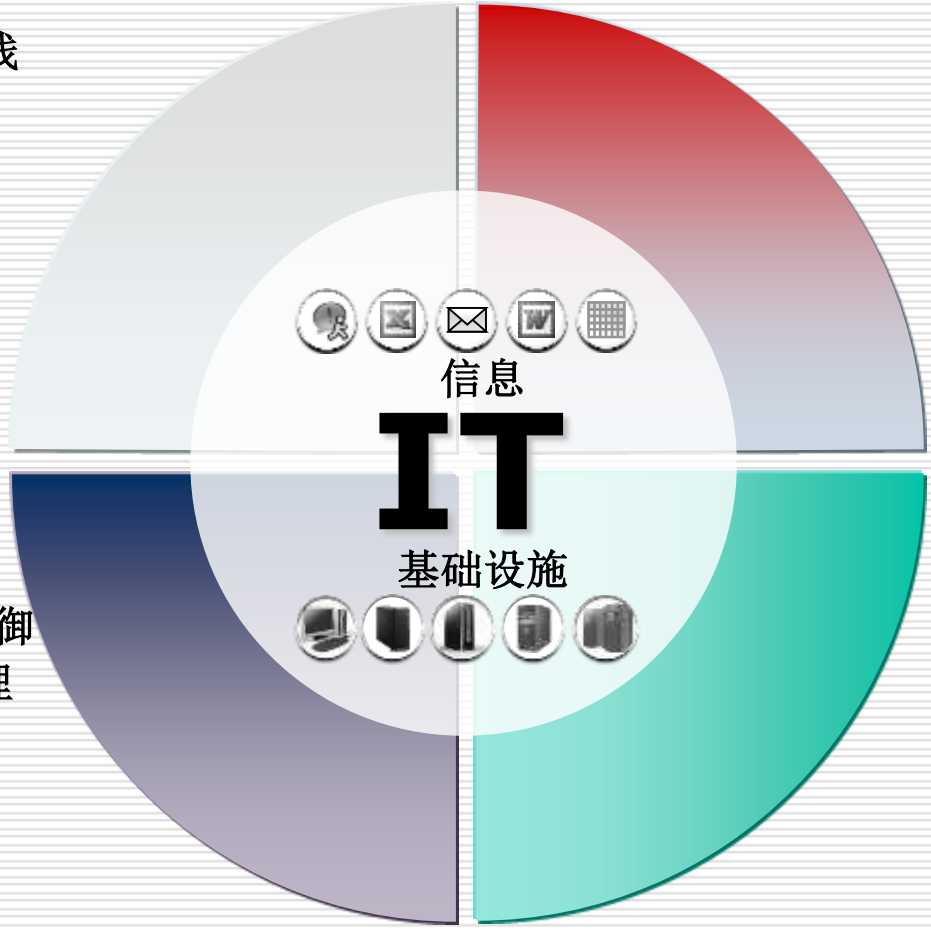
归纳企业IT面临的风险和问题

法规遵从

IT最佳实践
行业法规
公司政策
……

系统可用性

硬件故障
软件故障
人为误操作
灾难
……



信息安全

互联网威胁防御
端点资源管理
准入控制
数据防泄密
……

存储架构

互操作性
管理复杂
使用效率
成本问题
……

企业信息系统的挑战


访问
风险
信息安全
服务质量
安全威胁
意外或人为事故
法规遵从
成本
HACKERS
复杂性
Microsoft
Apache Software
Lucent Technologies
PeopleSoft
SAP
bea
SIEBEL
IBM
ORACLE
Microsoft
Sun
IBM
HITACHI
EMC²
客户端
网络
应用
数据库
服务器
存储

目录

- 制造型企业信息安全见解
- 新宏昌重工信息安全分享

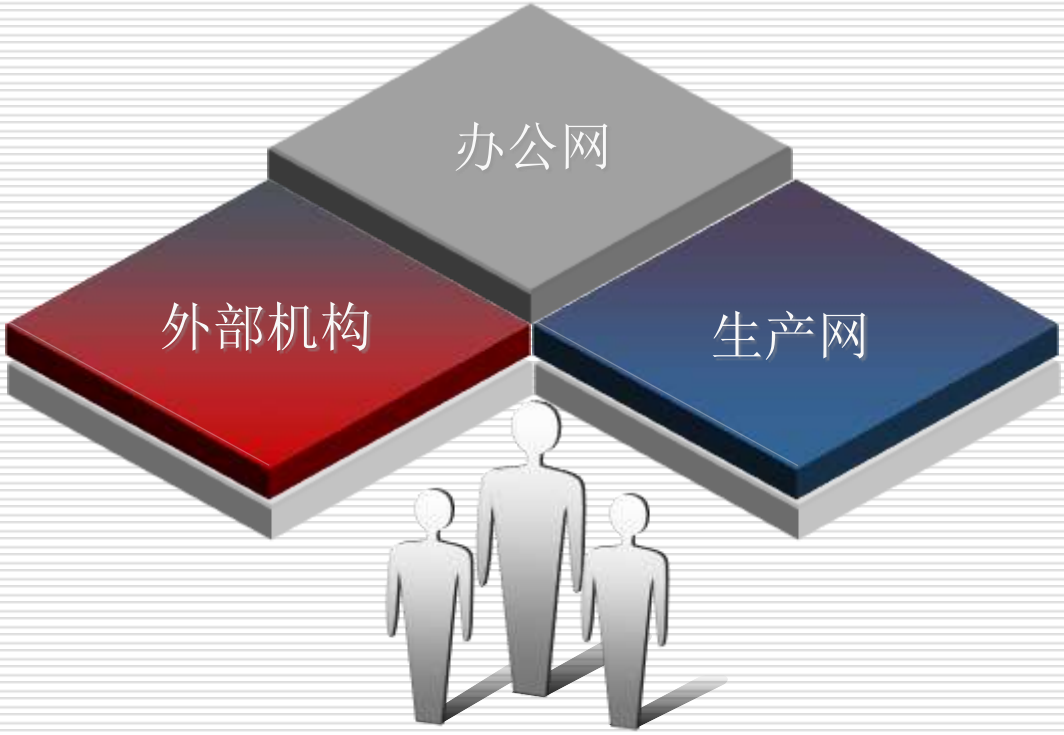

一中心
两平衡
新宏昌
三博弈
四风险

一中心

10 多个Lan办公网络

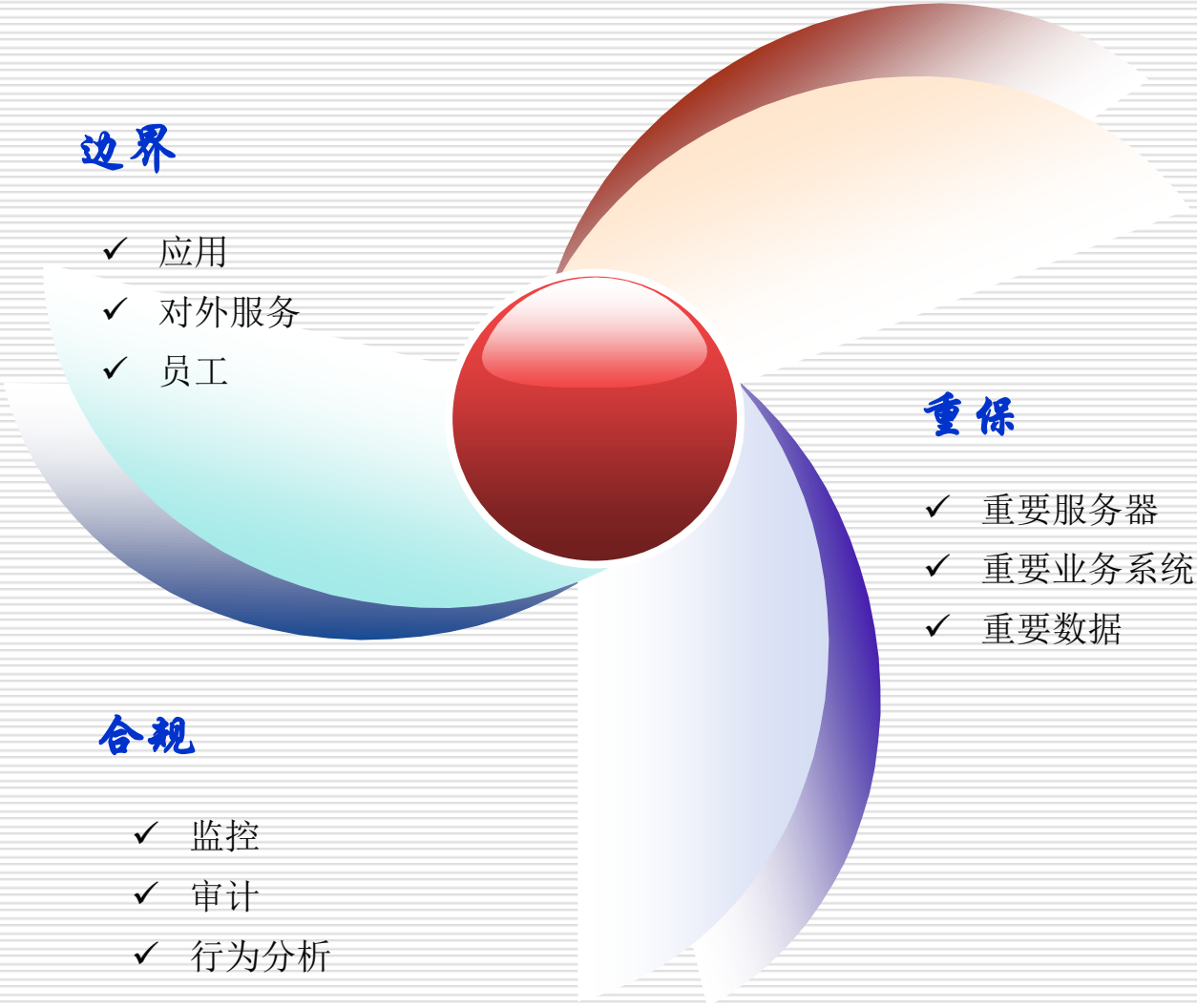
众多个外部机构

生产 网络



两平衡

三博弈



边界

- ✓ 应用
- ✓ 对外服务
- ✓ 员工

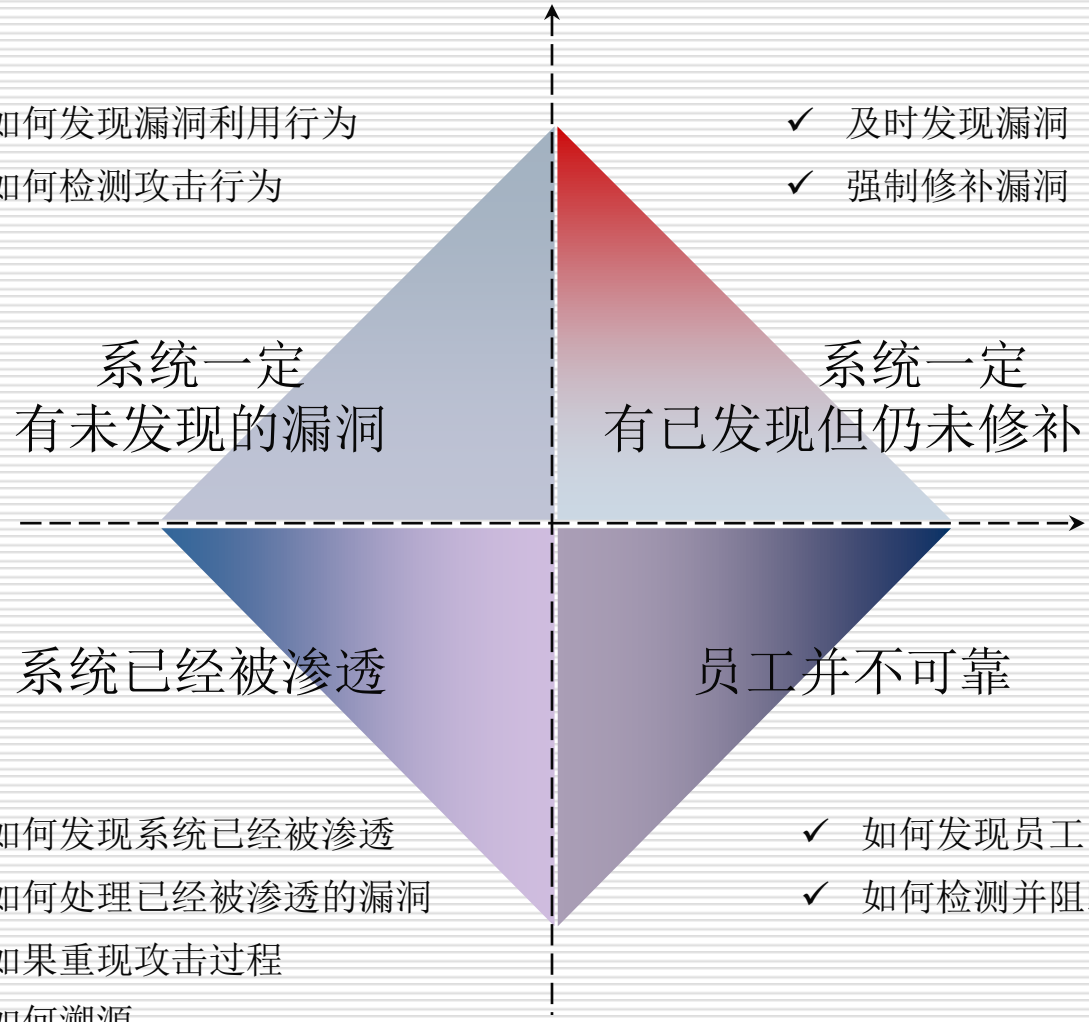
重保

- ✓ 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



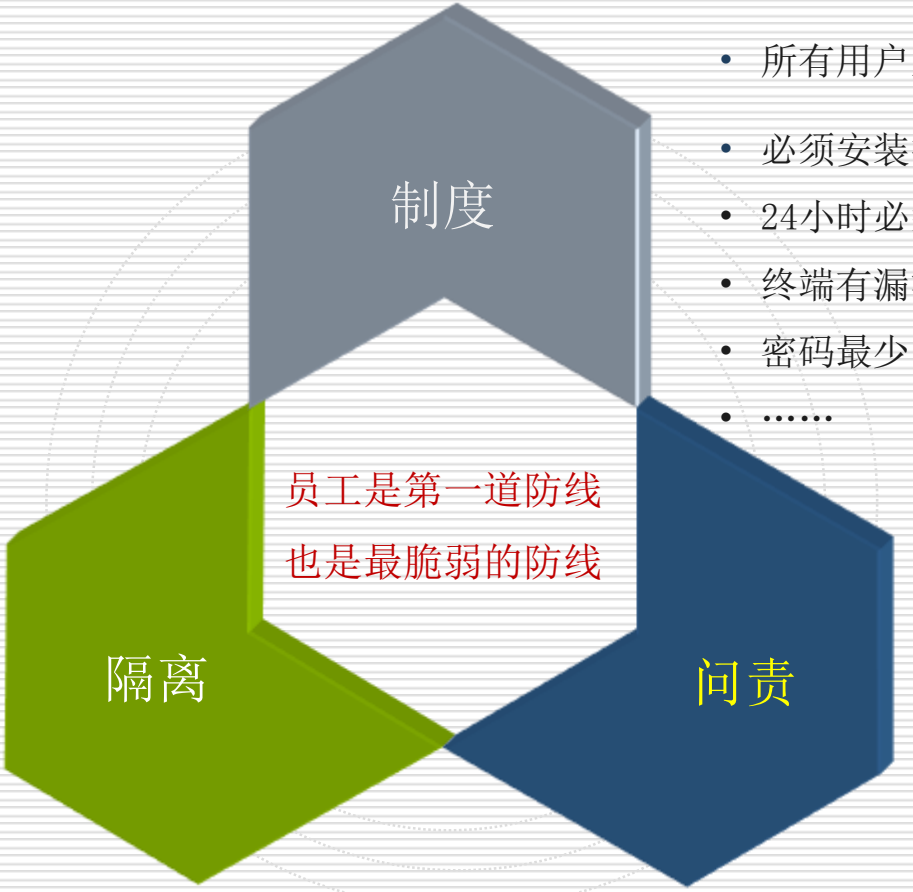
- ✓ 如何发现漏洞利用行为
- ✓ 如何检测攻击行为

- ✓ 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



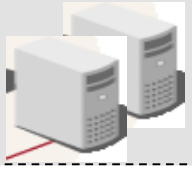
- 所有用户必须加入域
- 必须安装指定的安全软件
- 24小时必须重启一次
- 终端有漏洞必须修复
- 密码最少15位
- ……

- 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
- ……

- 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

安全管理架构

策略管理



端点安全管理服务器
(分布式, 高弹性, 与目录技术集成)

策略决策点

LAN Enforcer

Gateway Enforcer

Self Enforcer

DHCP Enforcer

On-Demand Enforcer

策略强制点

远程接入
SSL & IPsec

IP地址服务
- DHCP

认证服务 - RADIUS

AC

局域网交换机 & 无线

端点 - PFW

AP

透明网关
Gig-E

接入设备

未管理的

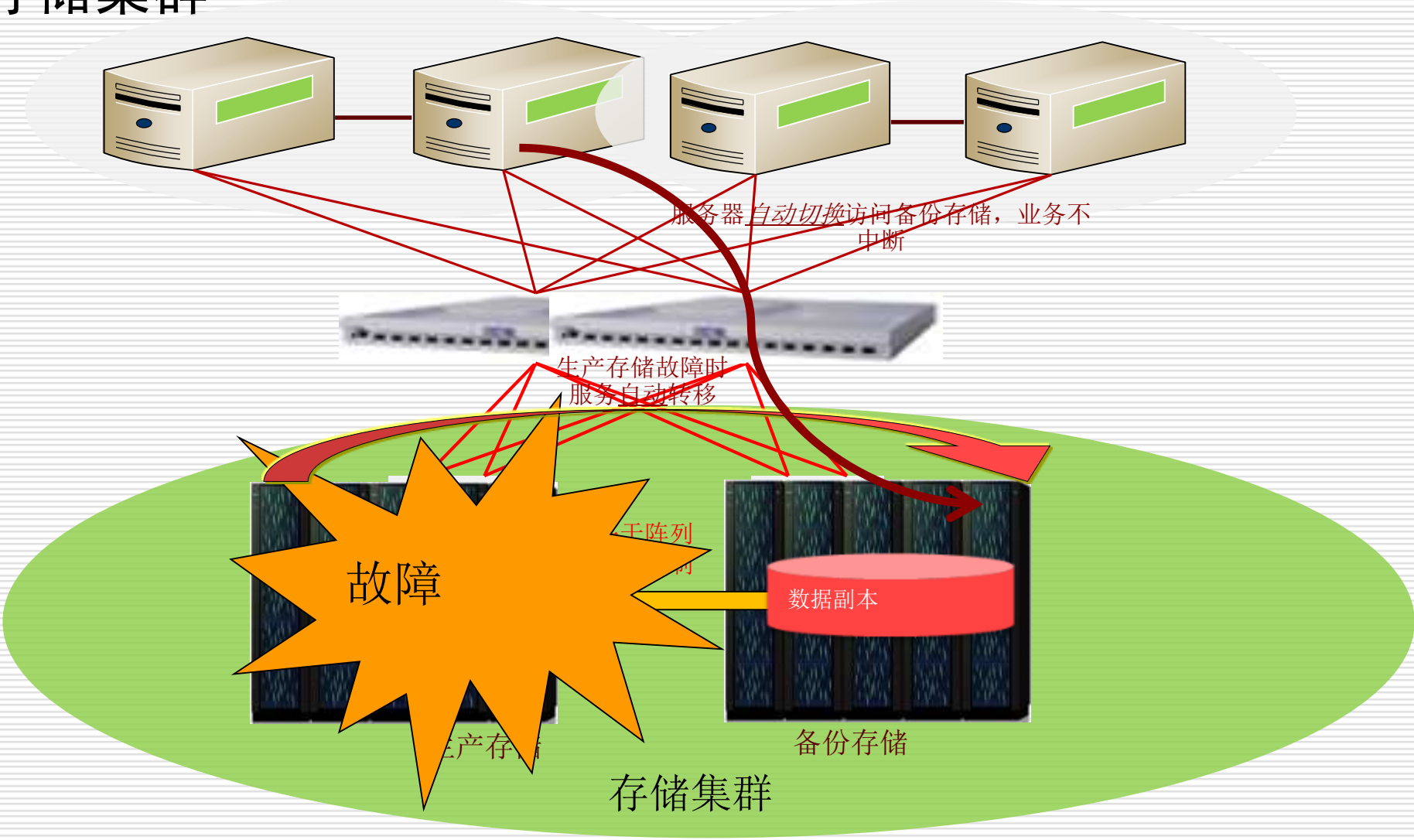
已管理的
台式机

已管理的移
动用户

无法管理的

PDA

存储集群



服务器与业务系统

监控

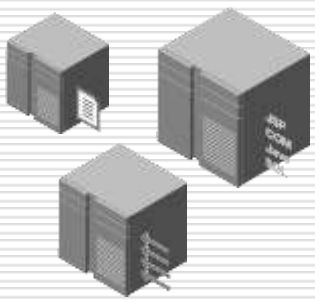
全局服务实时监测

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

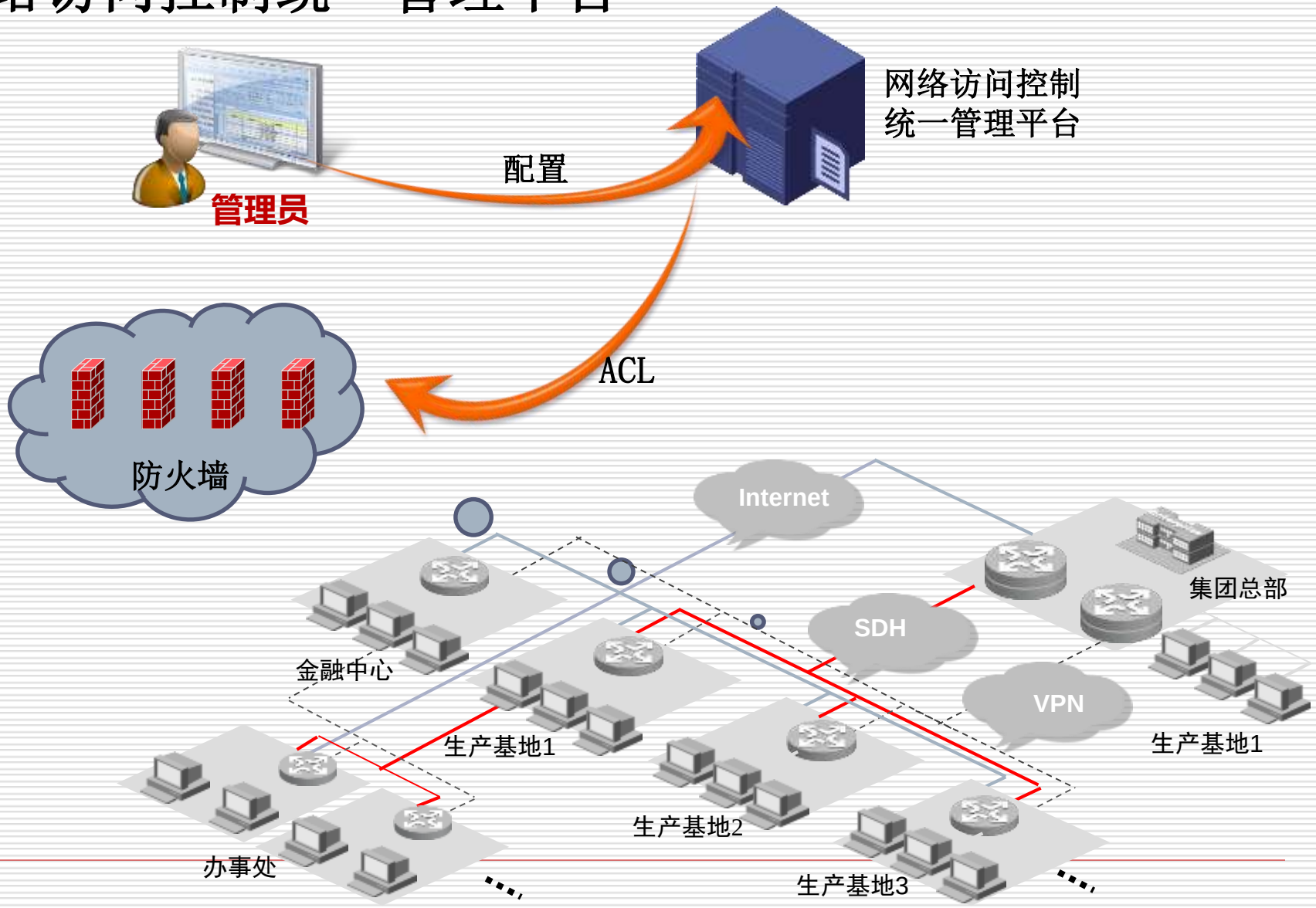
离线备份作为后援

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



架构-基于用户的安全策略

用户认证	安全策略	用户管理
➢ 本地/第三方认证 ➢ 事前/会话认证 ➢ Web/AD/Radius/LDAP多认证方式	➢ 基于用户的策略 ➢ 基于用户的审计	➢ 本地/第三方用户管理 ➢ 组织架构管理&同步 ➢ 用户状态管理

基于用户的架构

- IP缺乏组织架构含义，应对困难
- 复杂策略难以实施

易用性

- 管理层次自然对应企业组织架构
- 法规制度无缝融合管理策略

- 策略绑定IP，不能应对网络变化
- 策略固化，无法支撑人员流动办公

灵活性

- 安全策略与网络结构解耦
- 安全策略灵活支持移动办公

- IP等策略对象缺乏明确含义
- 多人共用一个终端无法区分策略

精确性

- 策略对象可以精确到具体的用户
- 可针对每一个终端用户制定策略

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

远程办公：数据隔离与加密

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

请各位专家批评指正！