
互联网时代制造业的信息安全探索

齐亚卓

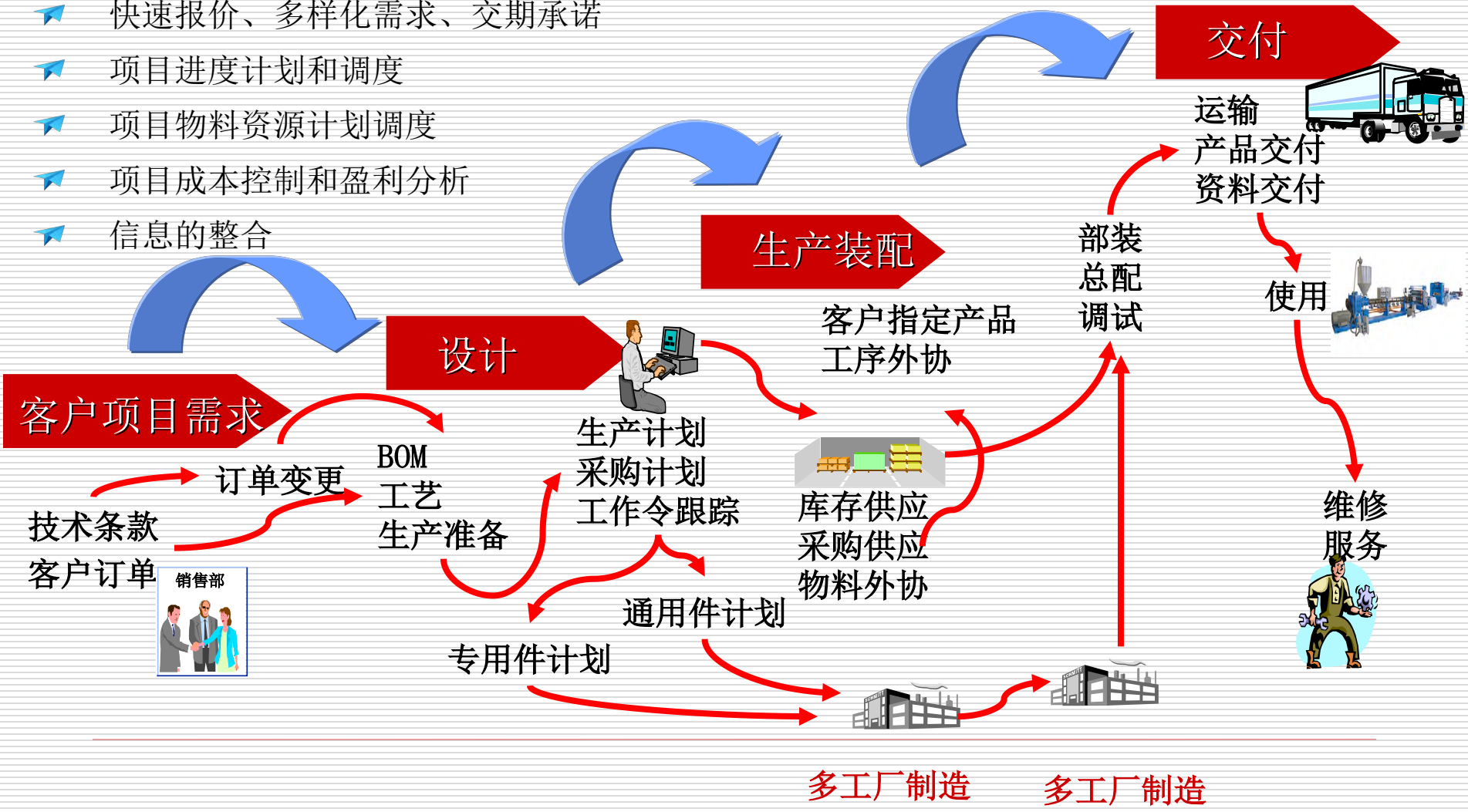
atlsico@hotmail.com

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

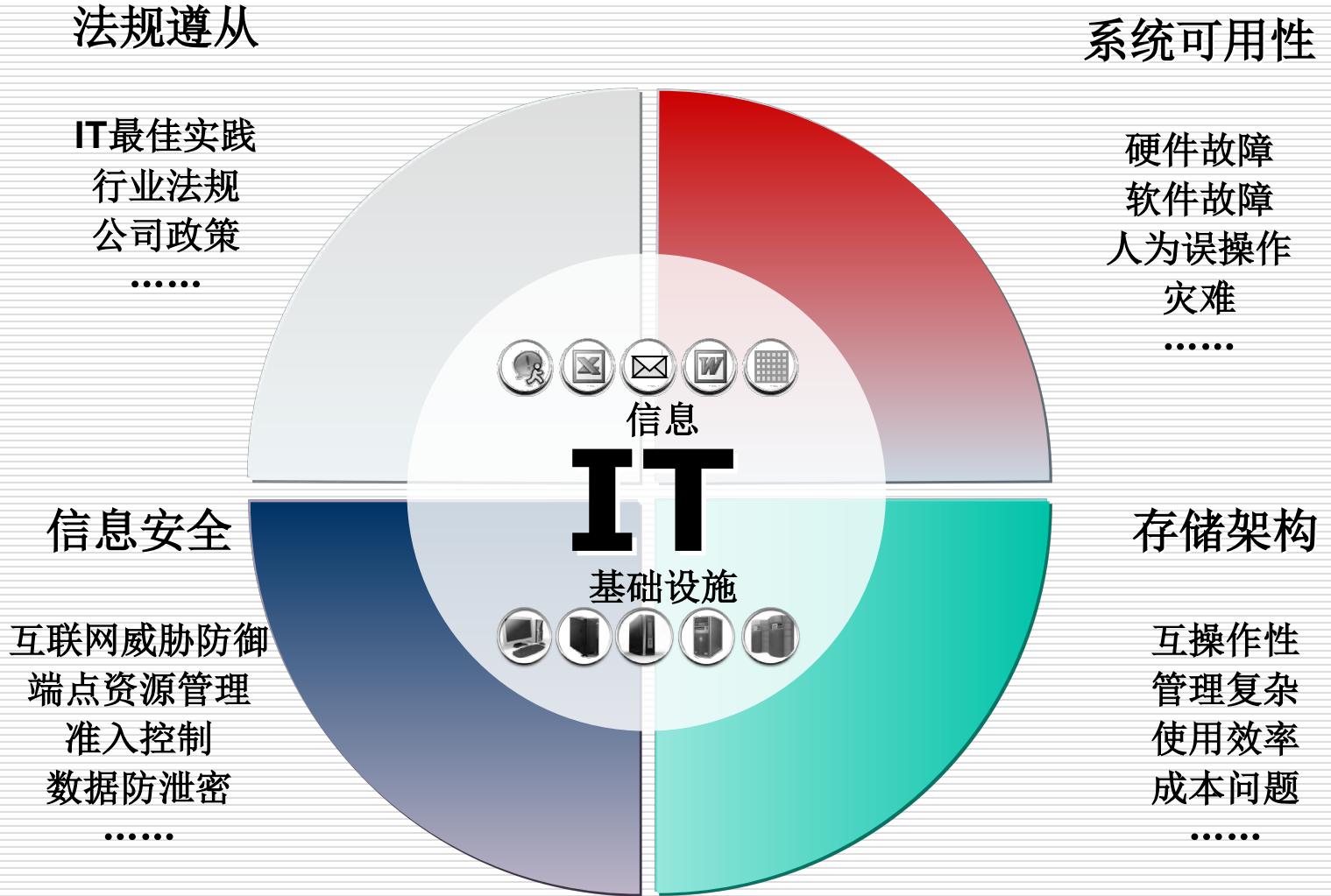
PDM系统: 产品数据管理, 与生产、销售密切相关

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



企业信息系统的挑战



目录

- 制造型企业信息安全见解
- 新宏昌重工信息安全分享

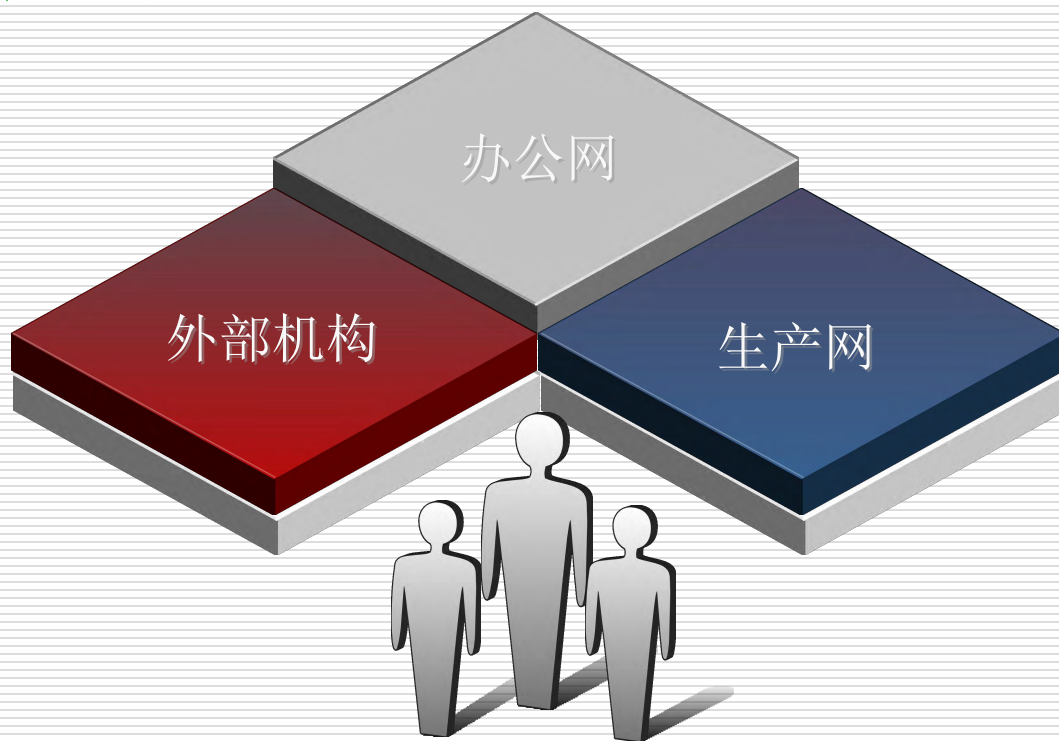


一中心

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

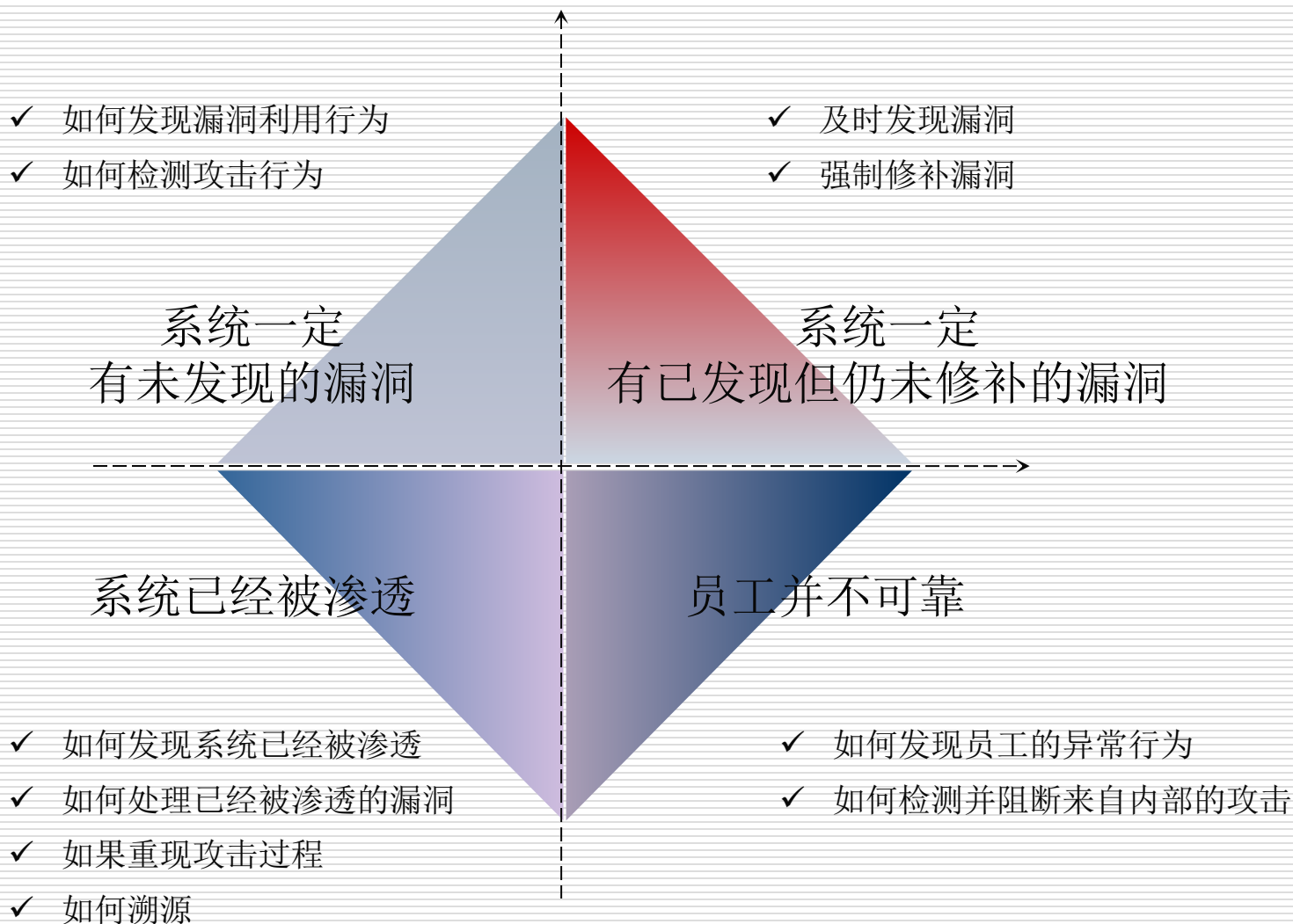
重保

- ✓ 重要服务器
- ✓ 重要业务系统
- ✓ 重要数据

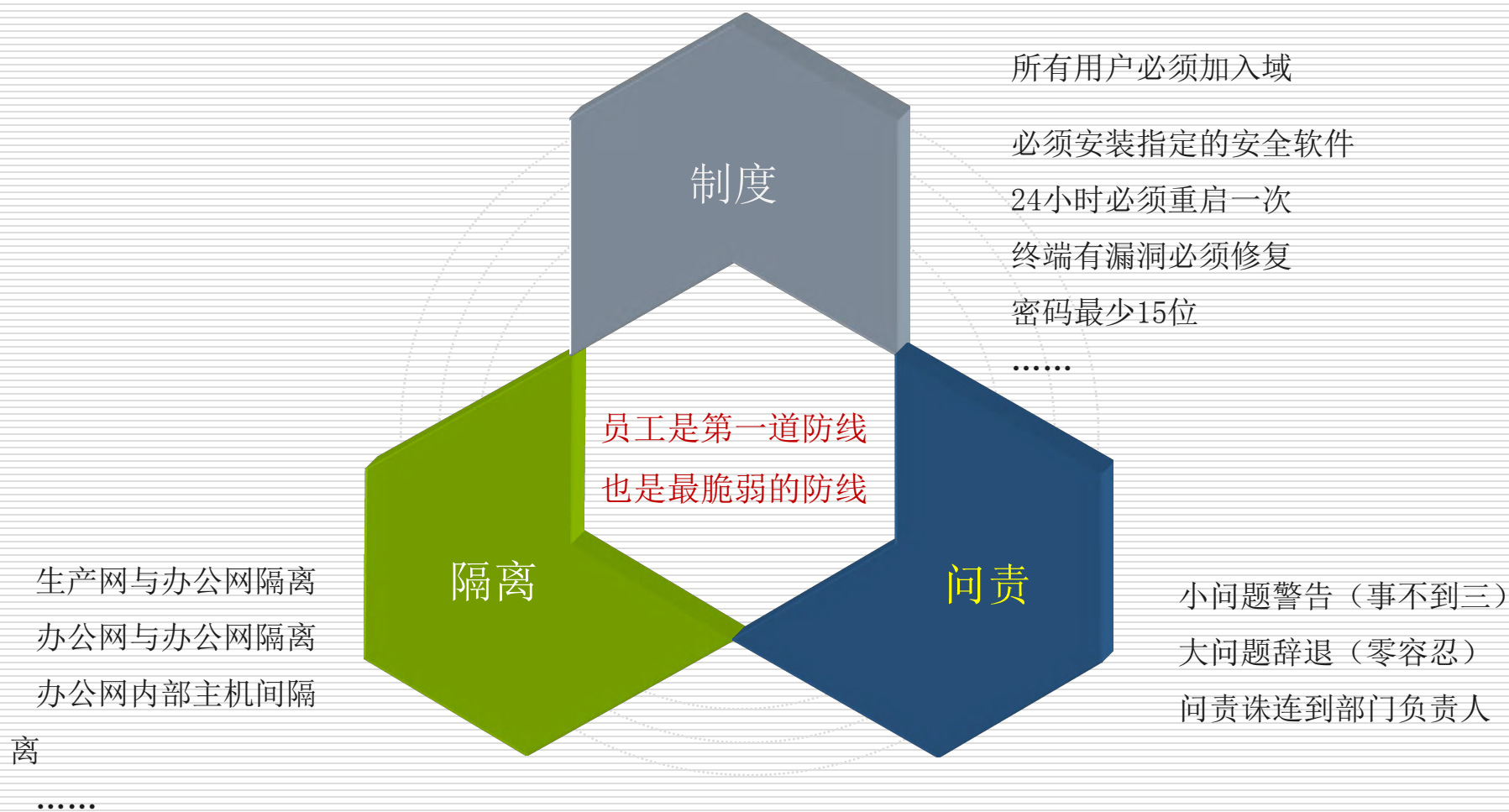
合规

- ✓ 监控
 - ✓ 审计
 - ✓ 行为分析
- 

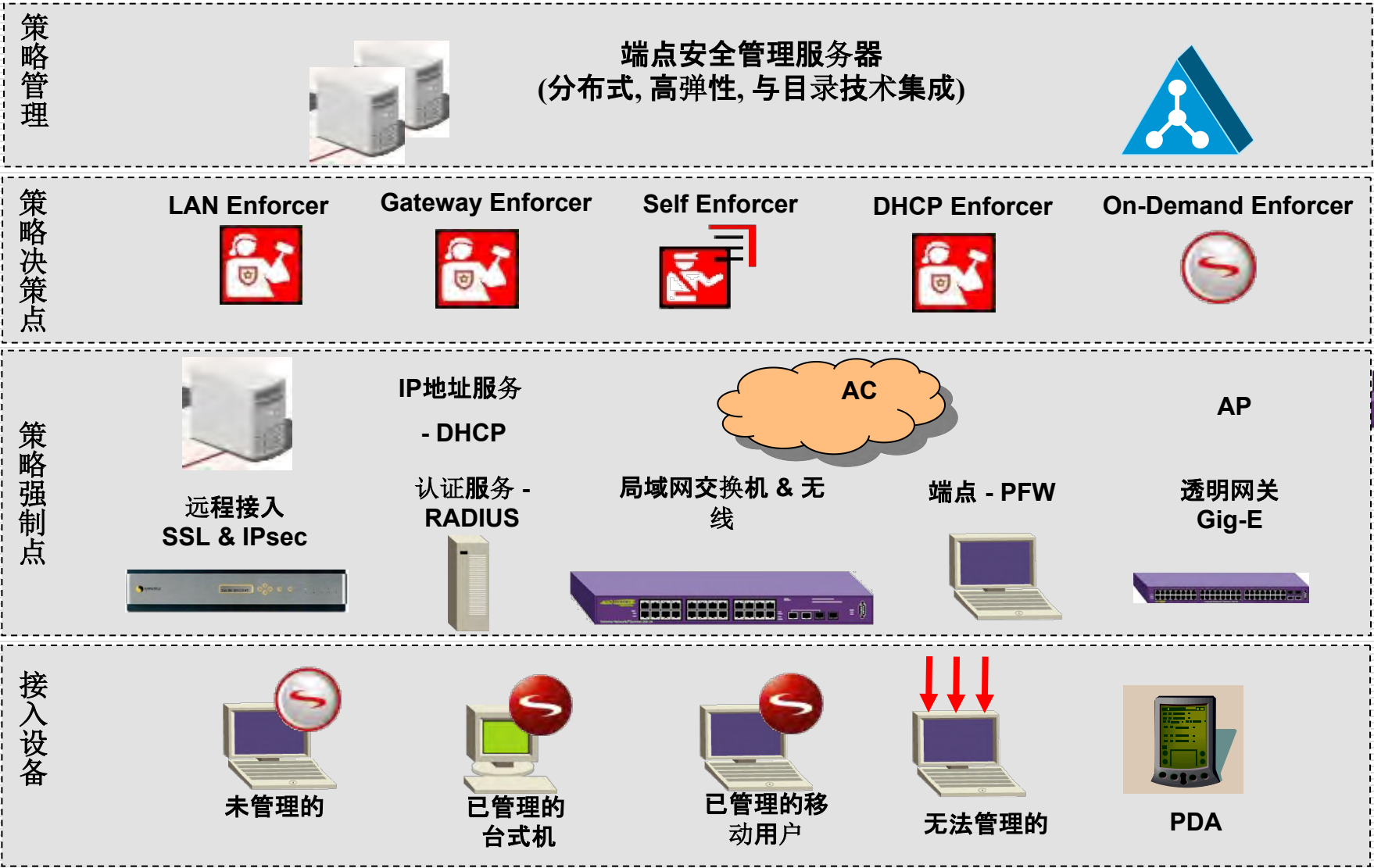
四风险



安全是责任



安全管理架构



实现法规遵从

保证数据和系统的可靠性

IT策略与
外部法规的遵从审核

应用系统及数据的可用性保障



信息

IT

基础设施



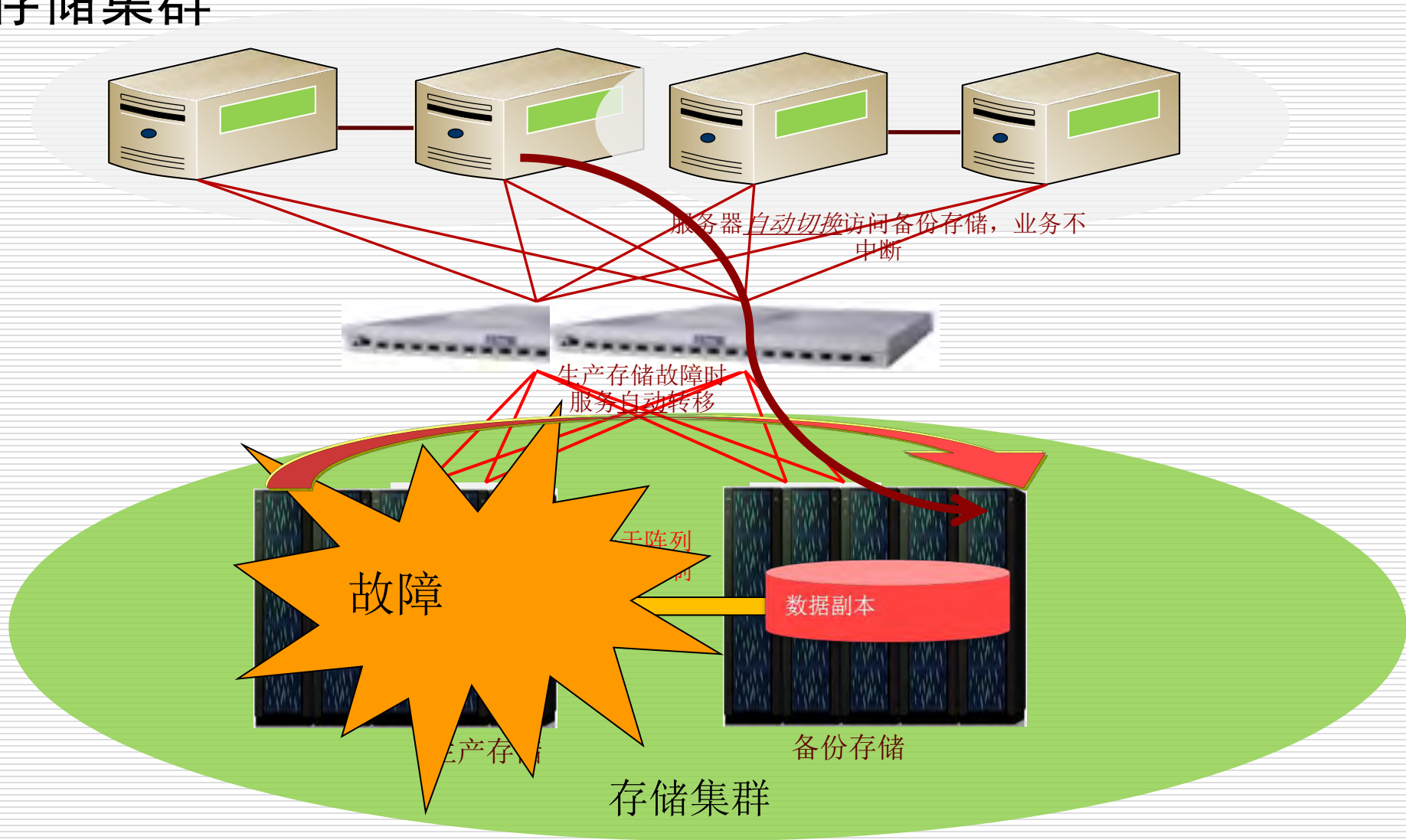
内部与外部恶意威胁的消除
数据泄漏的防护

存储服务标准化

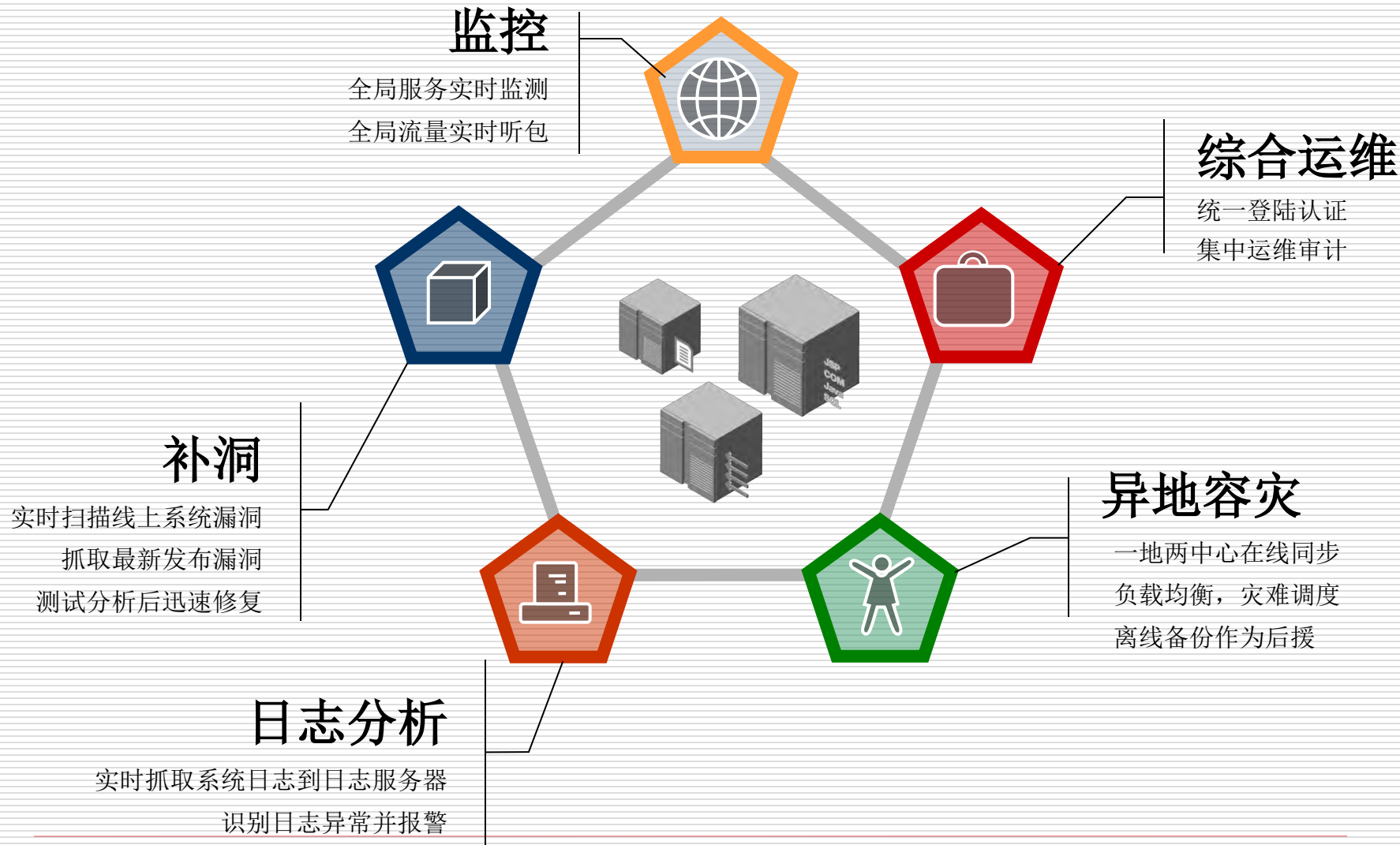
强化数据安全

简化数据存储基础架构

存储集群

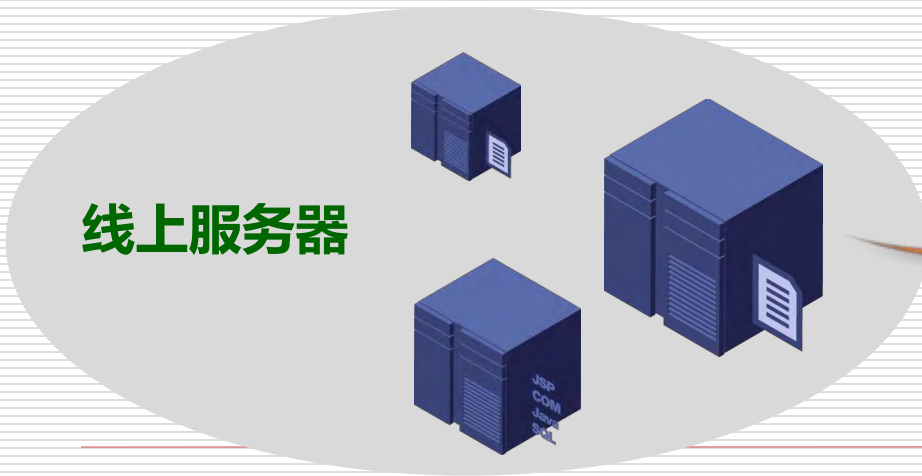
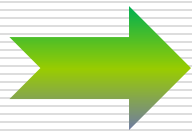


服务器与业务系统

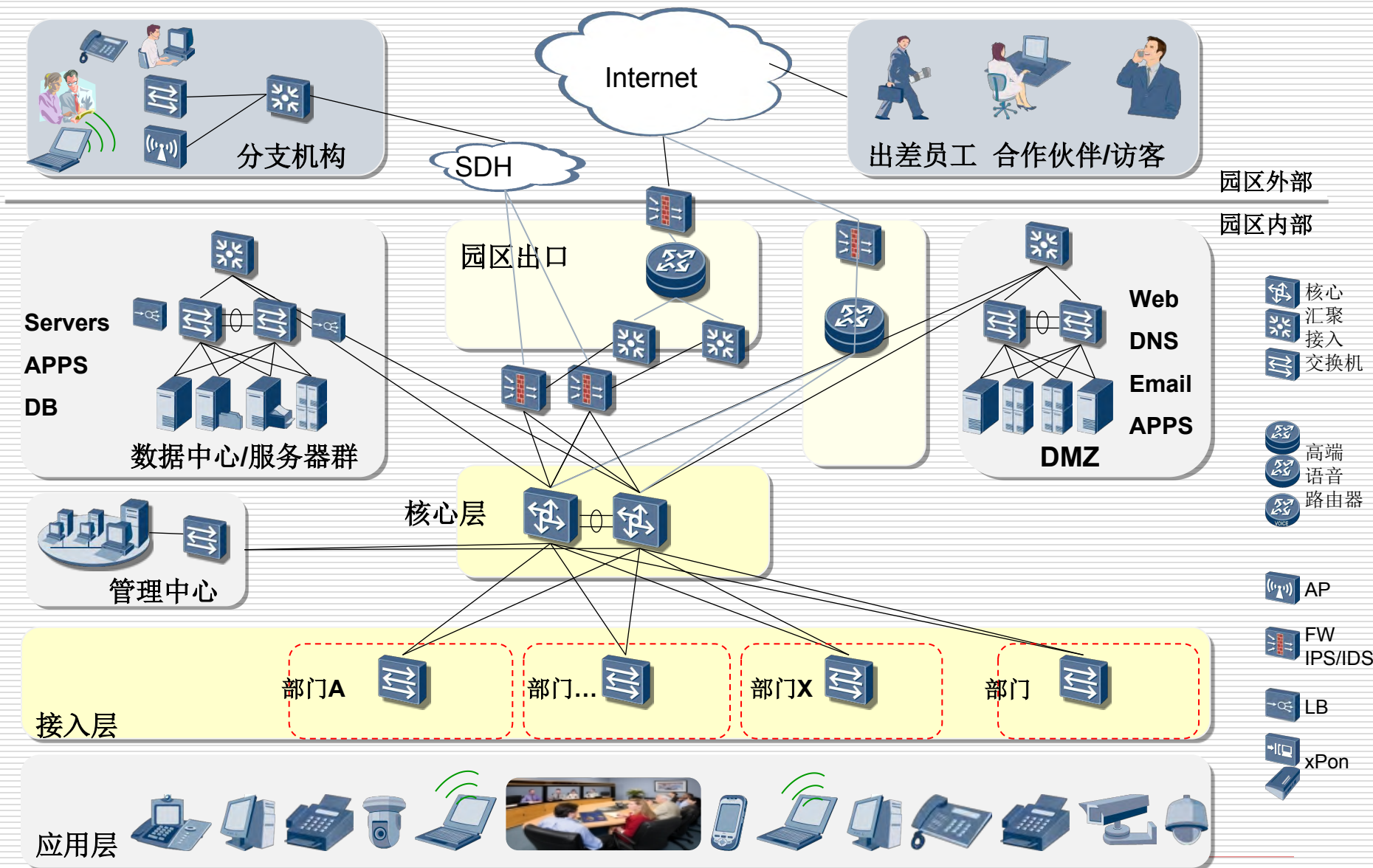


服务器日志异地存储与分析系统

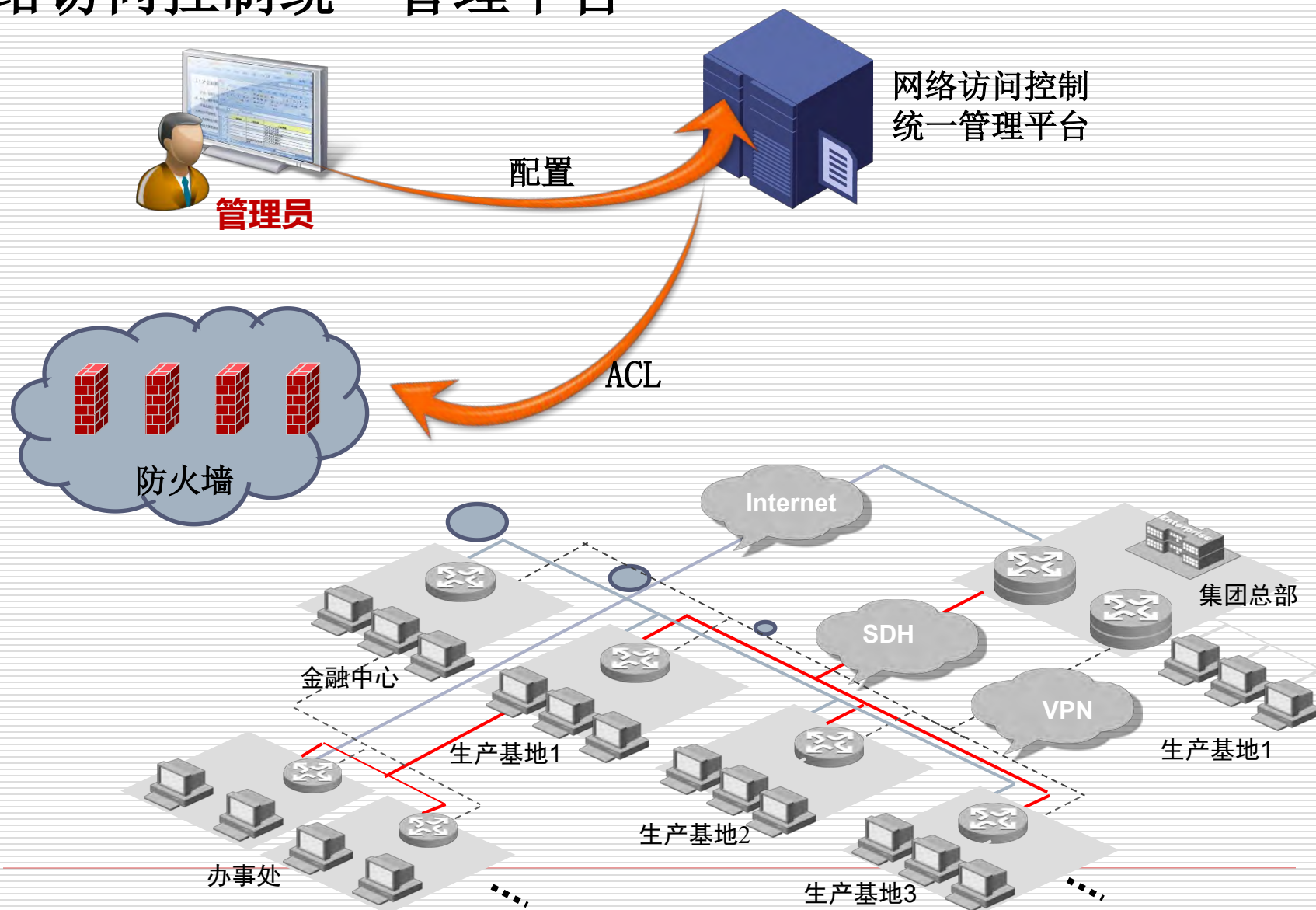
- ✓ 日志**远程**存储
- ✓ 日志**全量**异常分析



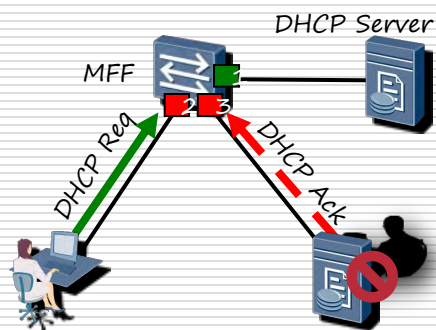
服务器日志自动上传



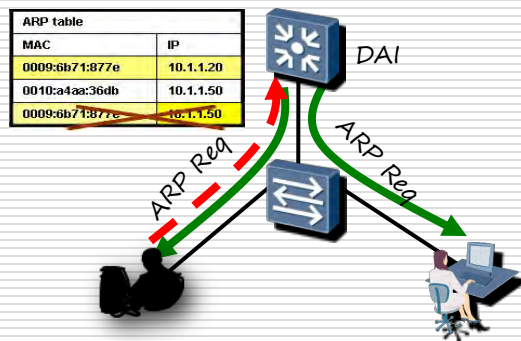
网络访问控制统一管理平台



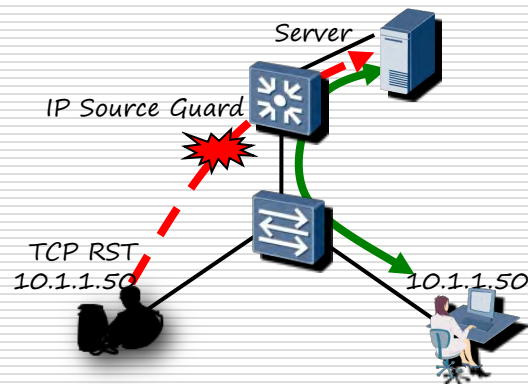
多种监听技术及风暴抑制实现内网安全



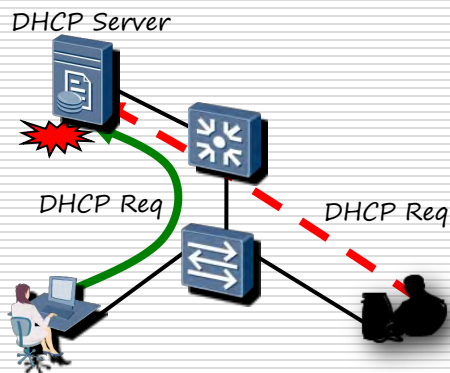
MFF—非法服务器



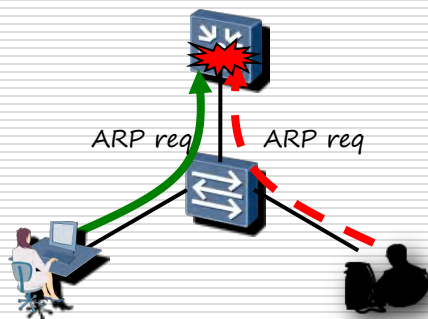
DAI—ARP欺骗



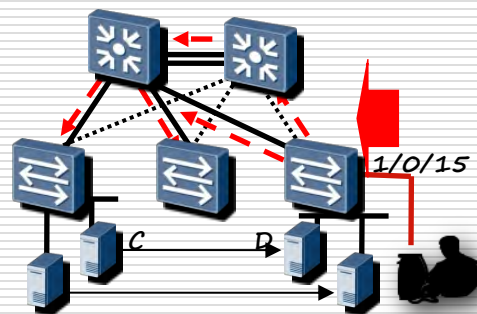
IP Source Guard—IP欺骗



DHCP 限速—DHCP 泛洪



ARP 限速—ARP扫描



MAC 限速—MAC 泛洪

架构-基于用户的安全策略

用户认证

- 本地/第三方认证
- 事前/会话认证
- Web/AD/Radius/LDAP多认证方式

安全策略

- 基于用户的策略
- 基于用户的审计

用户管理

- 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

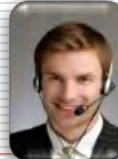
- 安全策略与网络结构解耦
- 安全策略灵活支持移动办公



- 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！
