## 互联网时代制造业的信息安全探索

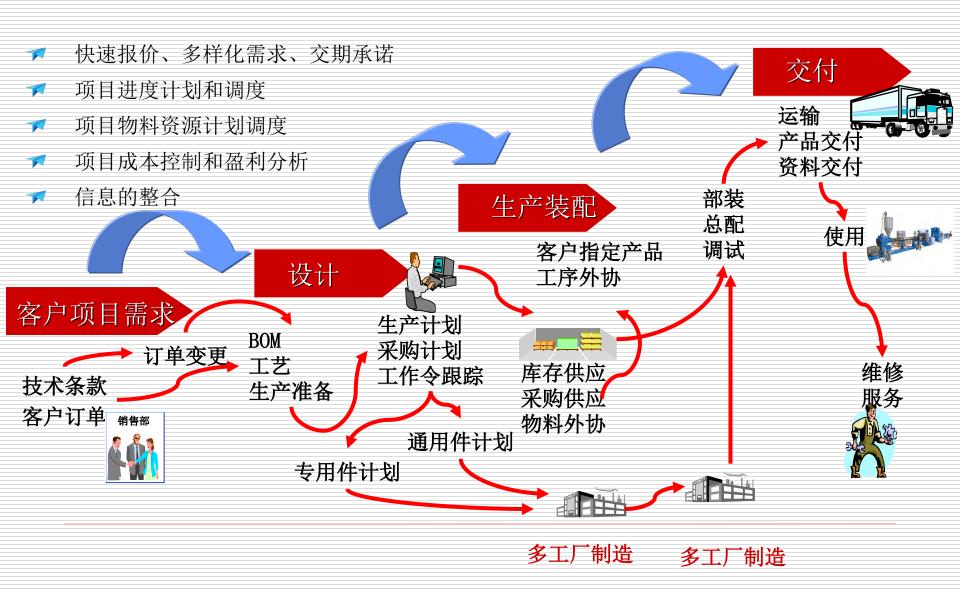
齐亚卓

atlsico@hotmail.com

## 目录

- 口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



#### 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

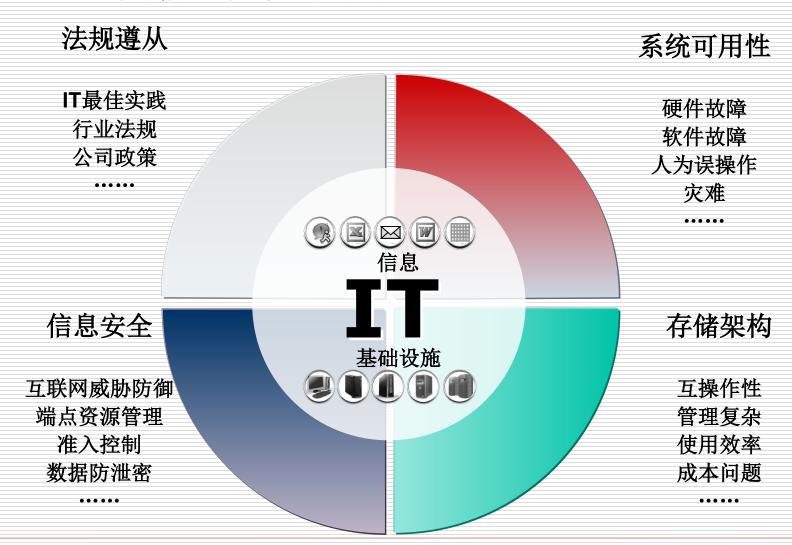
WEB/代理服务:信息发布和信息获取

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



## 录目

- □制造型企业信息安全见解
- □新宏昌重工信息安全分享

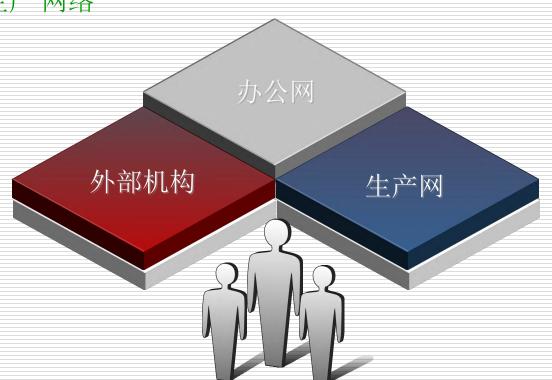


## 一中心

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

#### 合规

- ✓ 监控
- ✓ 审计
- ✔ 行为分析

#### 重保

- ✓ 重要服务器
- ✓ 重要业务系统
- ✓ 重要数据

## 四风险

- ✔ 如何发现漏洞利用行为
- ✔ 如何检测攻击行为

系统一定 有未发现的漏洞

系统已经被渗透

- ✔ 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

- ✔ 及时发现漏洞
- ✔ 强制修补漏洞

系统一定 有已发现但仍未修补的漏洞

员工并不可靠

- ✔ 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 制度 24小时必须重启一次 终端有漏洞必须修复 密码最少15位 员工是第一道防线 也是最脆弱的防线 隔离 问责 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

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

囝

.....

#### 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) **Gateway Enforcer LAN Enforcer Self Enforcer** 策略决策点 **DHCP Enforcer On-Demand Enforcer** IP地址服务 AC AP 策略强制点 - DHCP 局域网交换机 & 无 认证服务 -端点 - PFW 透明网关 远程接入 **RADIUS** Gig-E SSL & IPsec 接入设备 已管理的移 未管理的 已管理的 无法管理的 **PDA** 动用户 台式机

#### 实现法规遵从

IT策略与 外部法规的遵从审核

内部与外部恶意威胁的消除 数据泄漏的防护

强化数据安全

保证数据和系统的可靠性

信息

ΙT

基础设施

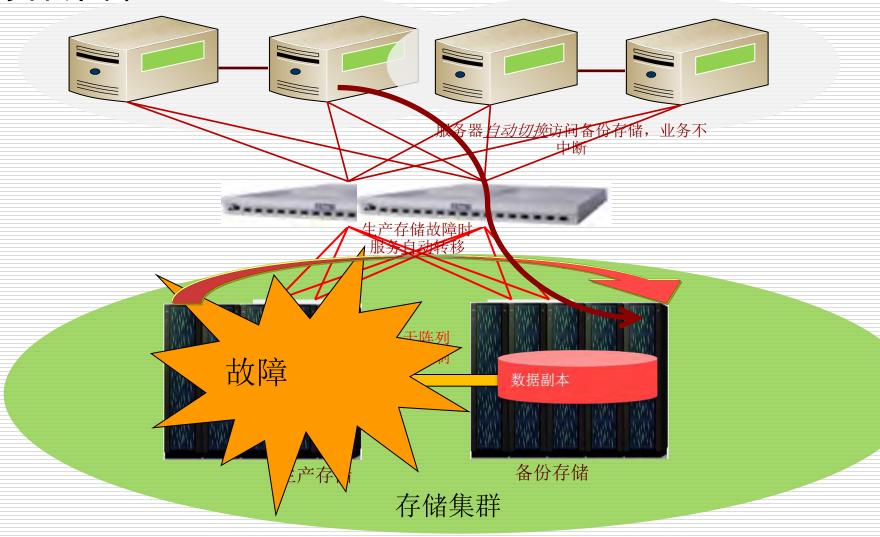


应用系统及数据的可用性保障

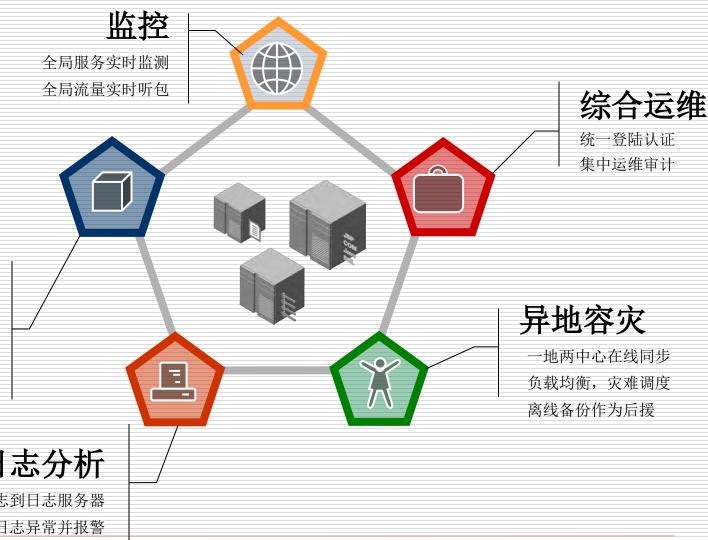
存储服务标准化

简化数据存储基础架构

## 存储集群



#### 服务器与业务系统



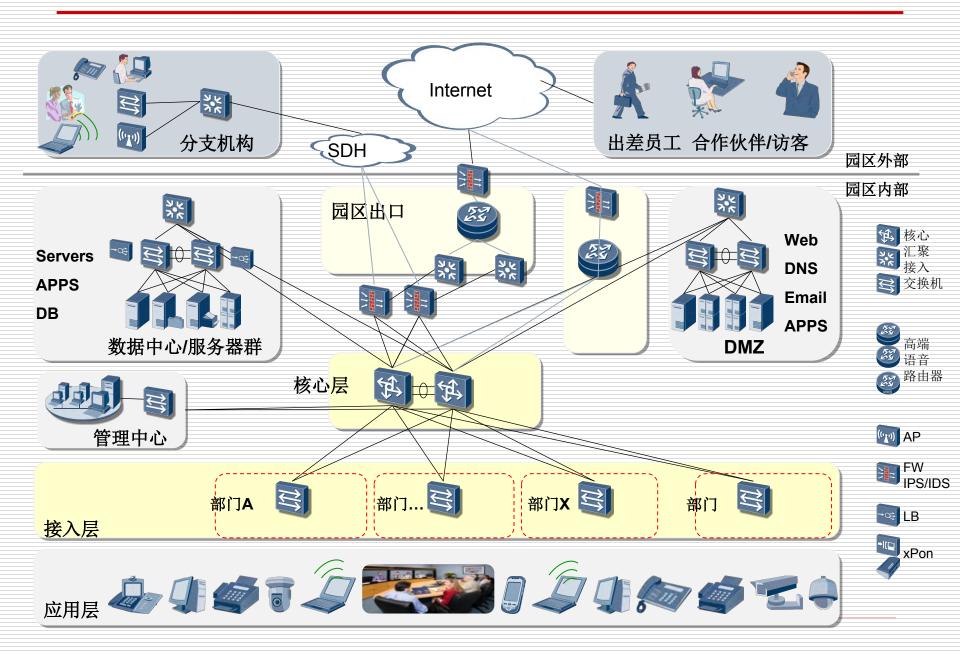
#### 补洞

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

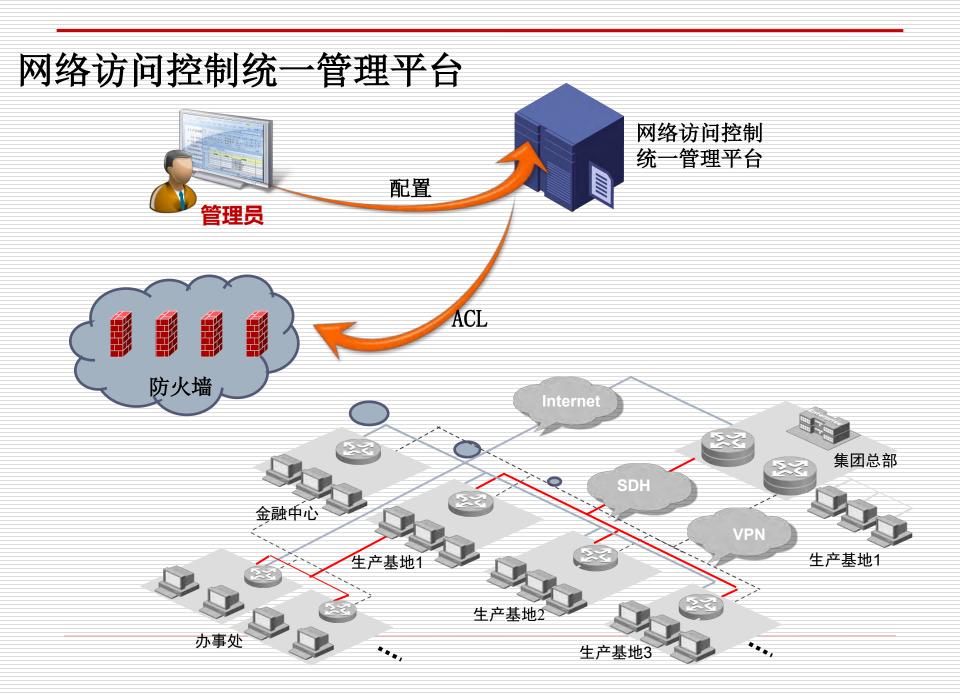
#### 日志分析

实时抓取系统日志到日志服务器 识别日志异常并报警

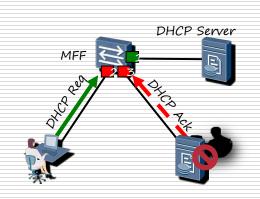
# 服务器日志异地存储与分析系统 ✓ 日志<mark>远程</mark>存储 日志存储与 ✓ 日志全量异常分析 服务器日志自动上传 线上服务器



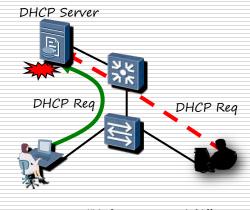
Page 19



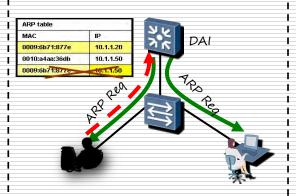
#### 多种监听技术及风暴抑制实现内网安全



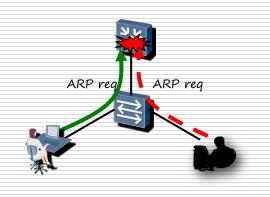
MFF—非法服务器



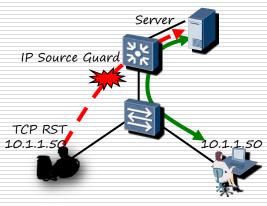
DHCP 限速—DHCP 泛洪



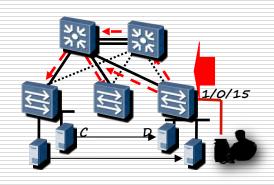
DAI—ARP欺骗



ARP 限速—ARP扫描



IP Source Guard—IP欺骗



MAC 限速—MAC 泛洪

## 架构-基弧用户的安全策略

#### 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



- 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



- ► 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

#### 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



- > 安全策略与网络结构解耦
- 安全策略灵活支持移动办公



- 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!