HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY

华为区域智慧隔离安全解决方案

简易、智慧、安全、和谐

enterprise.huawei.com
HUAWEI TECHNOLOGIES CO., LTD.

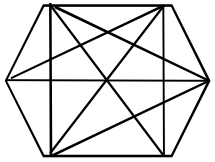
HUAWEI

Content

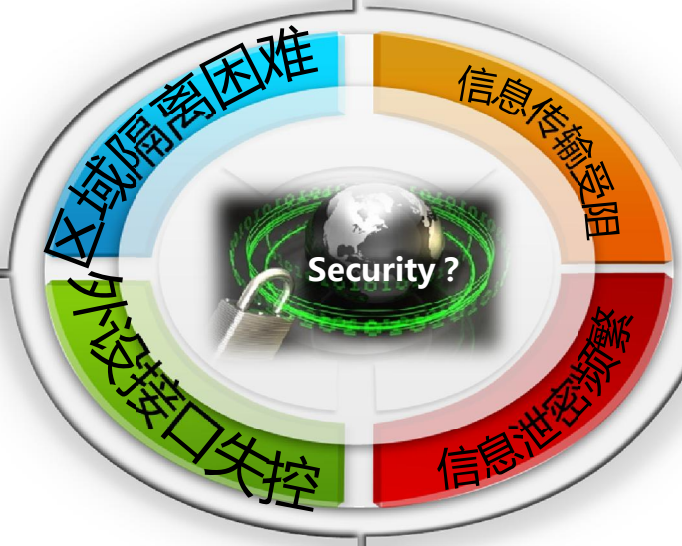
访问互联网的安全风险


内部泄密
防不胜防
无关应用
影响带宽
网络威胁
无孔不入
上网行为
难以管控
迅雷网络
XunLei Networking Technologies, Ltd
YOUKU 优酷
msn
腾讯QQ
飞信
Fetion
WWW

访问内网的安全风险



网络区域划分不合理，
内网的不同安全等级
区域无有效隔离



非受控传输，信息泄漏
受控传输，效率低下
信息传输，缺乏审计

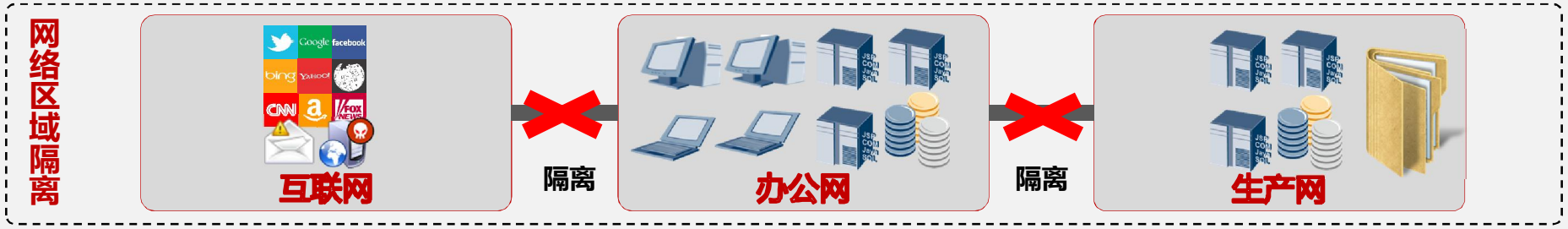
USB口、串口、并口、光
驱等外部接口无有效管理，
信息泄漏途径无法管控

机密信息存留在终端用户
机器，无意泄密、有意
泄密事件层出不穷

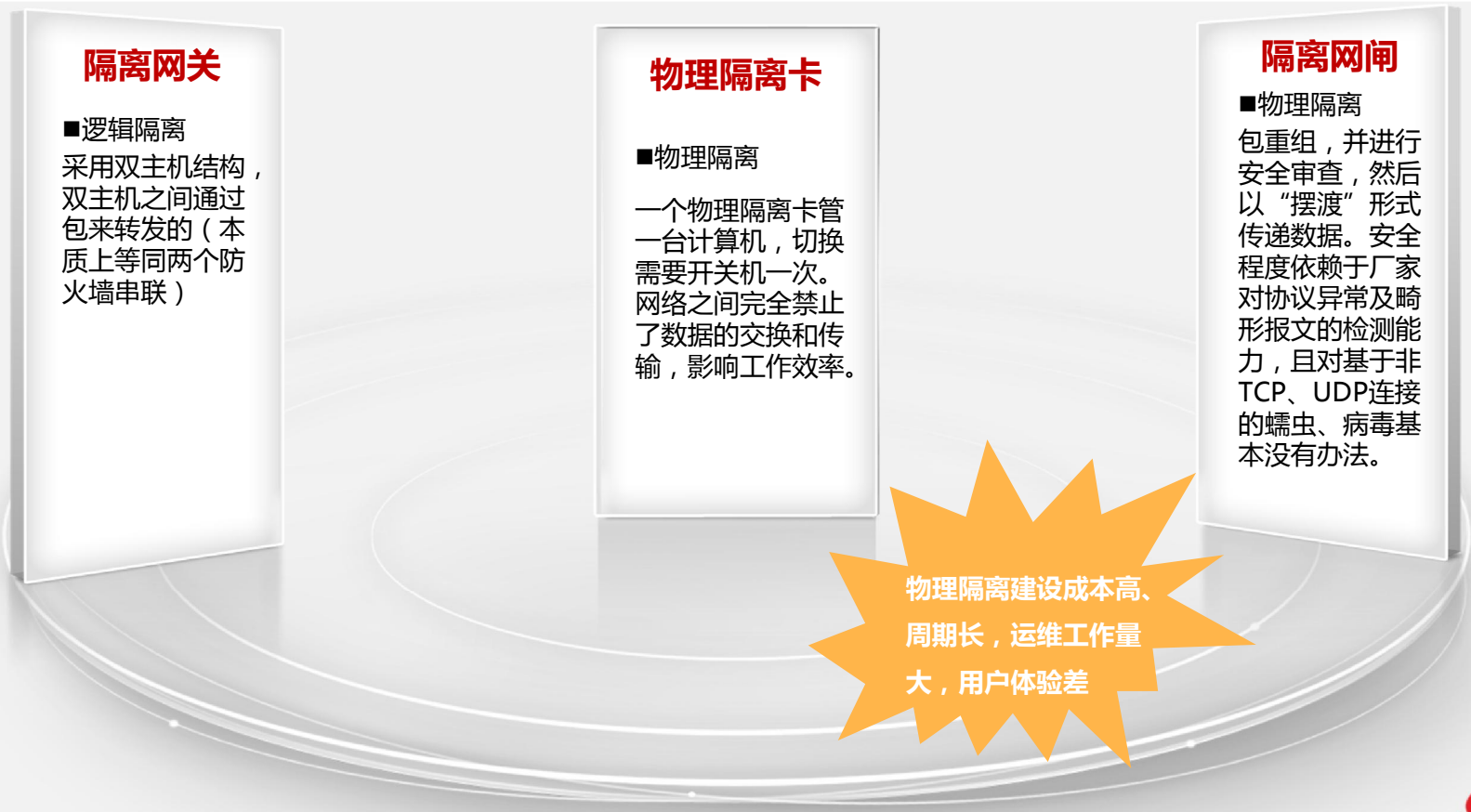
HUAWEI

政策驱动

- 《银行业金融机构信息系统风险管理指引》通知（银监发［2006］63号）
- 《商业银行信息科技风险管理指引》（银监发[2009]19号）
- 《关于银行业金融机构重要系统高可用性及信息安全管控风险提示的通知》（银监办发[2011]158号）
- 《关于加强银行网站及网银系统安全防范工作的通知》（银监办发[2011]175号）



传统区域隔离方法面临的挑战

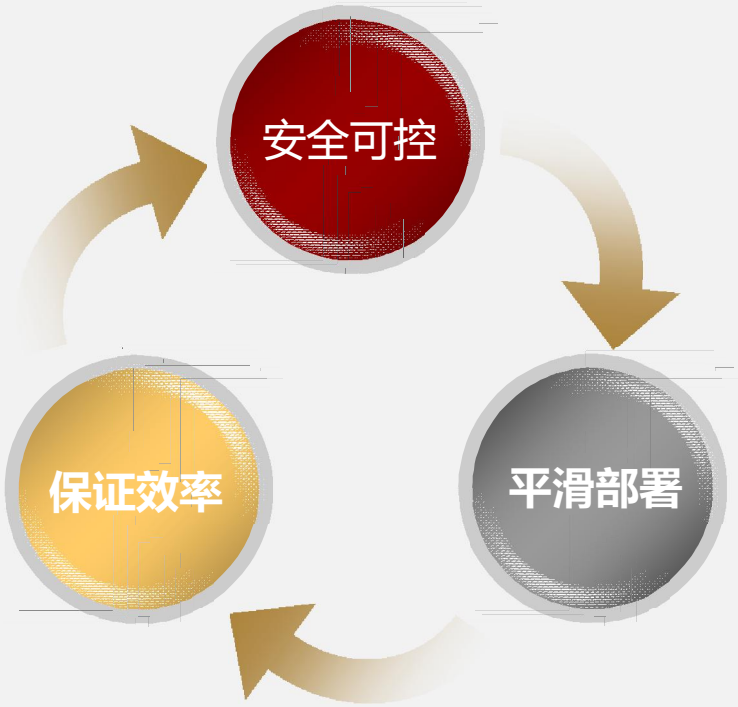


HUAWEI

区域隔离需求分析

安全和效率之间的最佳平衡

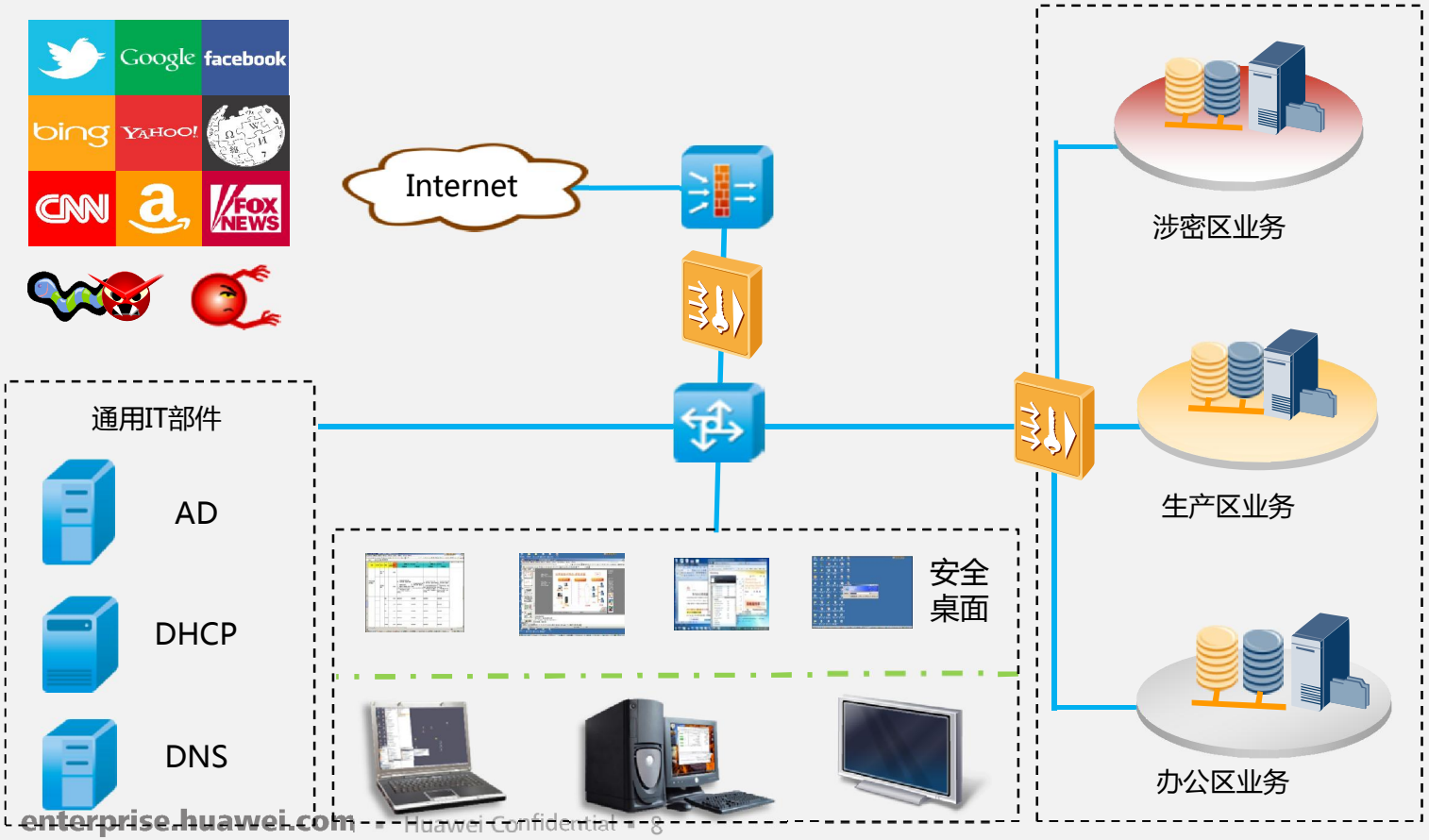
安全可控	数据保护，授权访问，审计追踪
保证效率	数据访问及时性，数据传输性能
平滑部署	兼容现有网络部署和IT应用



HUAWEI

Content

华为智慧隔离方案



兼容桌面办公应用

- 可兼容各类Windows系列操作系统
- 可运行各类办公应用
- 虚拟系统文件系统/注册表...

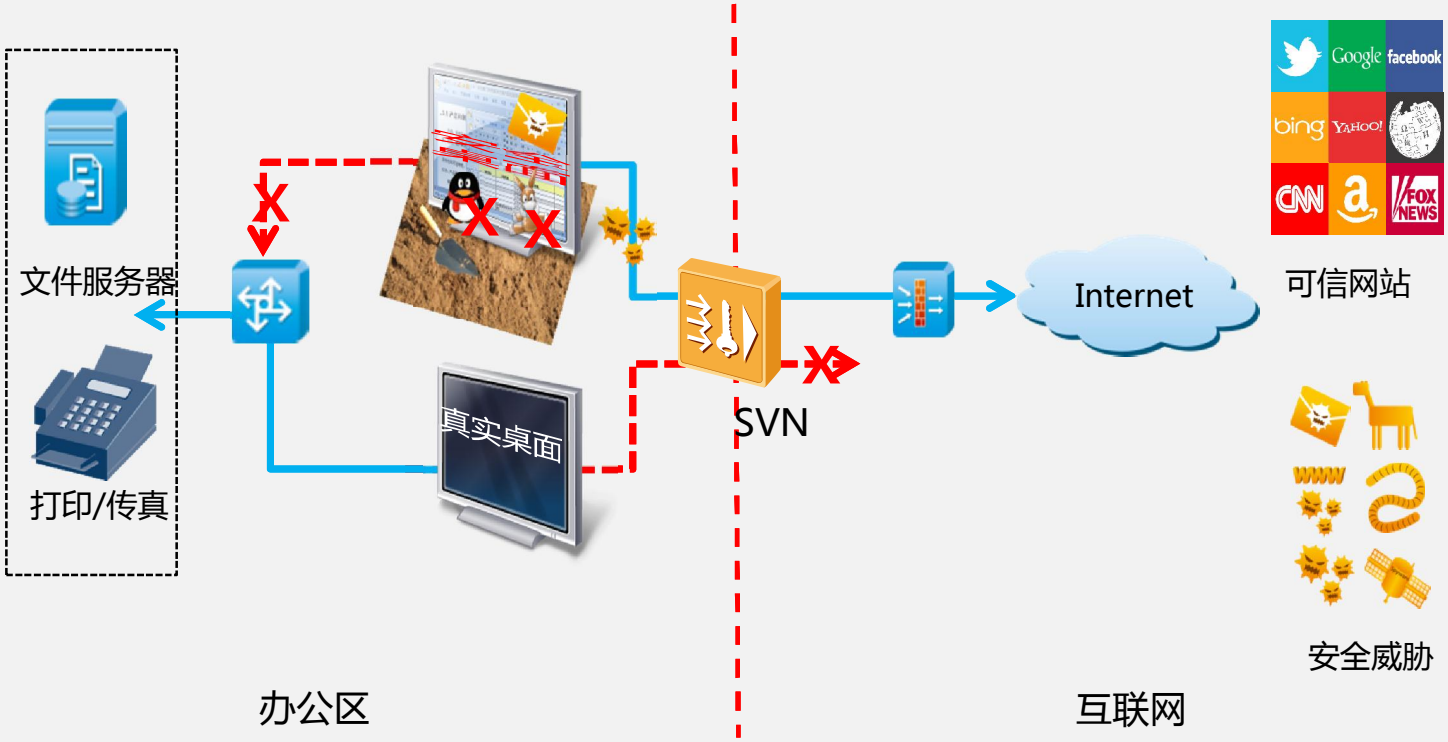
部署方便

- 接入网关旁路部署
- 支持集群部署
- 客户端自动推送安装

HUAWEI

华为智慧隔离方案典型应用

互联网安全访问 | 内网隔离安全访问



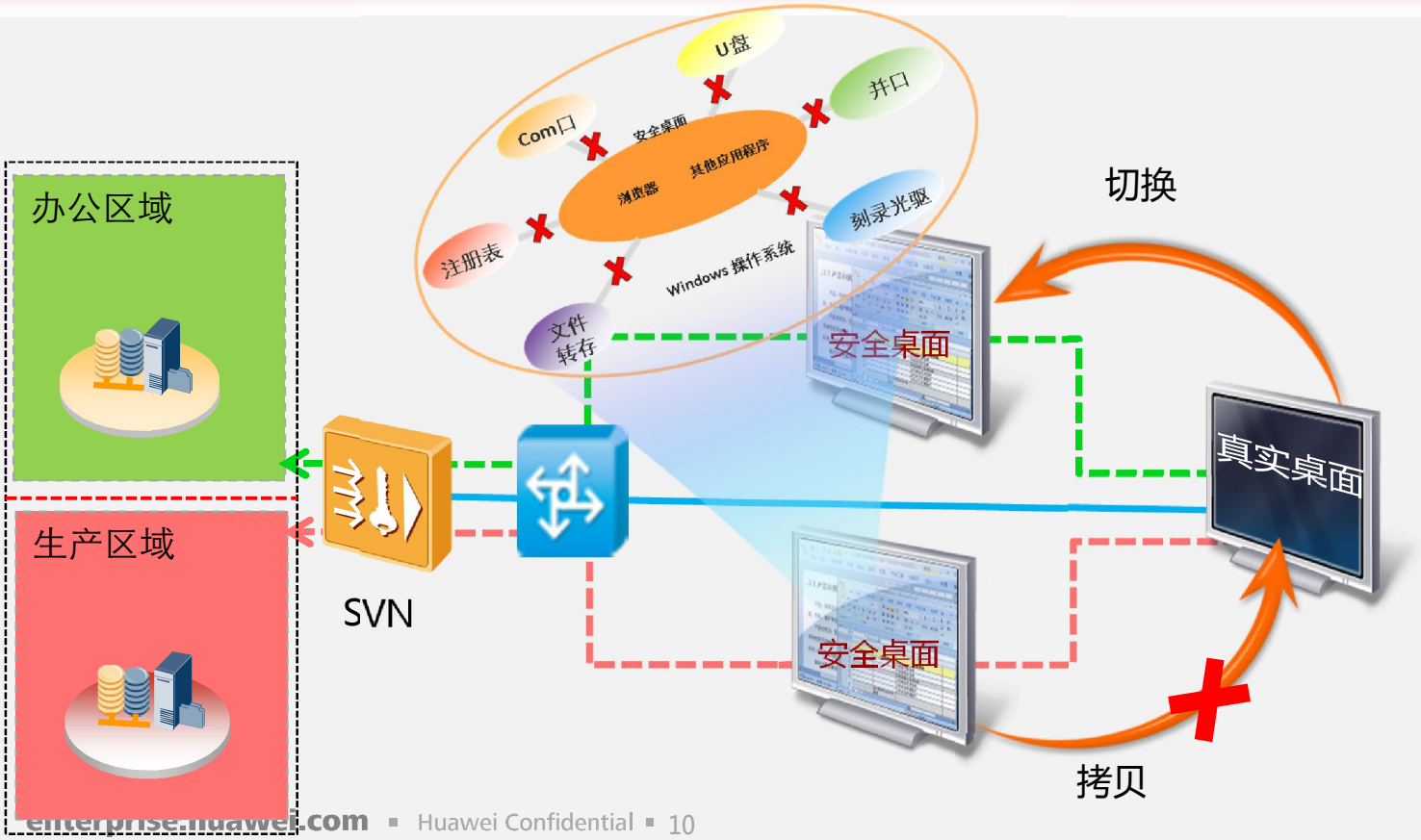
四大控制手段

- 禁止本地桌面访问Internet，但授权安全桌面访问，机密信息无法外传
- 高强度SSL加密隧道防止恶意监听
- 桌面环境完全隔离，防止本地桌面病毒/木马/恶意感染企业IT网络
- 控制安全桌面运行的网络应用和web访问，优化网络带宽，提供工作效率

HUAWEI

华为智慧隔离方案典型应用

互联网安全访问 | 内网隔离安全访问



四大控制手段

- 禁止本地桌面访问高密区信息，授权安全桌面访问，防止高机密数据本地存留；
- 支持多安全桌面，不同安全桌面访问不同网络区域，逻辑隔离不同机密级别的信息；
- 安全桌面内禁用USB口、光驱、串口等接口，并禁用网络文件共享，防止物理途径泄漏信息；
- 安全数据传输控制，保证不同区域的数据传输可管可控

HUAWEI

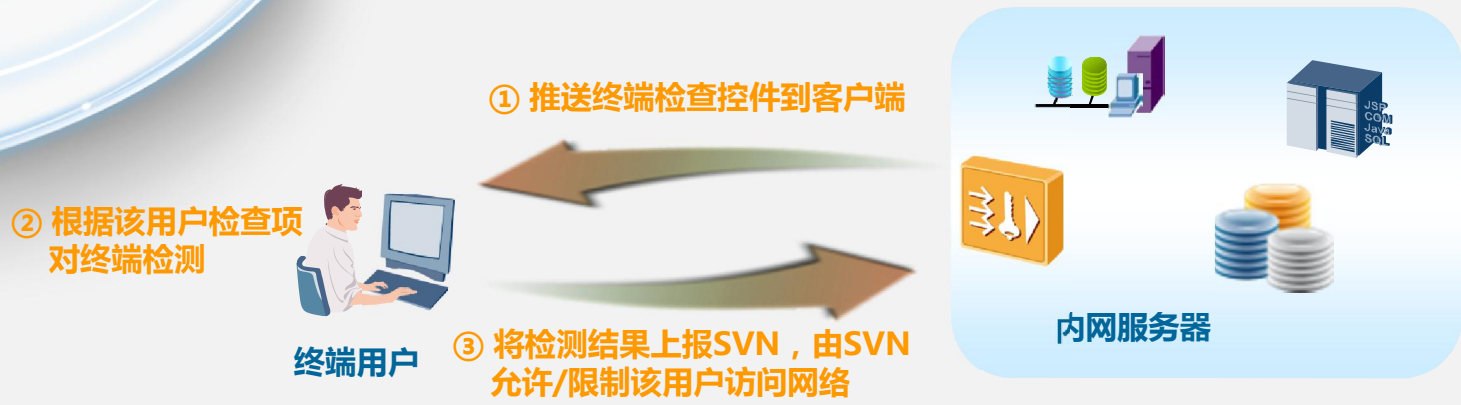
丰富的身份认证方式

- 远端认证支持与RADIUS、LDAP、AD、SecurID等标准协议的认证服务器对接
- 支持内置CA，并支持产生设备证书CSR（Certificate Signing Request），减少用户成本
- 支持多种认证方式的组合认证，进一步提高对用户的认证强度

HUAWEI

终端安全检查

对用户物理终端的安全性、可信性进行检测，避免用户所用终端对企业内网安全造成的威胁



HUAWEI

封闭的安全隔离环境

基于沙箱技术的安全桌面

文件访问隔离
- 在安全桌面中只允许用户操作真实桌面指定的文件夹和目录
- 跨区域获取的数据文件重定向加密存储在虚拟空间中，退出安全桌面后无痕化清除

注册表安全
- 采用重定向技术防止木马、病毒危害

网络传输控制
- 禁止网络共享等网络传输方式

外设端口控制
- 禁止USB存储接口，打印机，COM口

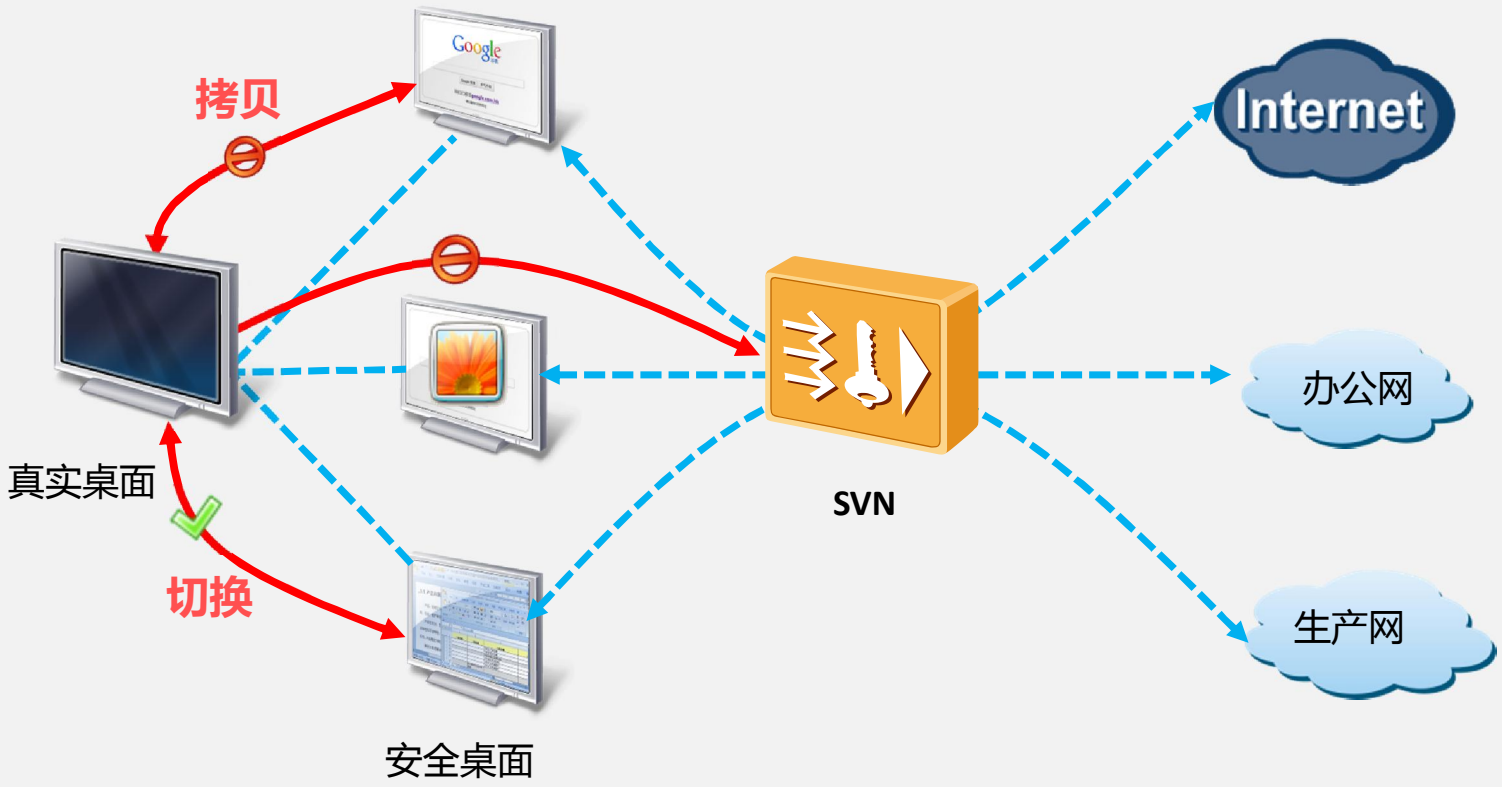
防截屏、防粘贴板拷贝

进程控制
- 可配置应用程序白名单，只允许在安全桌面内执行白名单内的软件

高强度透明加解密
- 安全桌面采用强度最高的AES256加密算法加密保存，加密密钥动态生成，周期更新

HUAWEI

专业的多实例技术

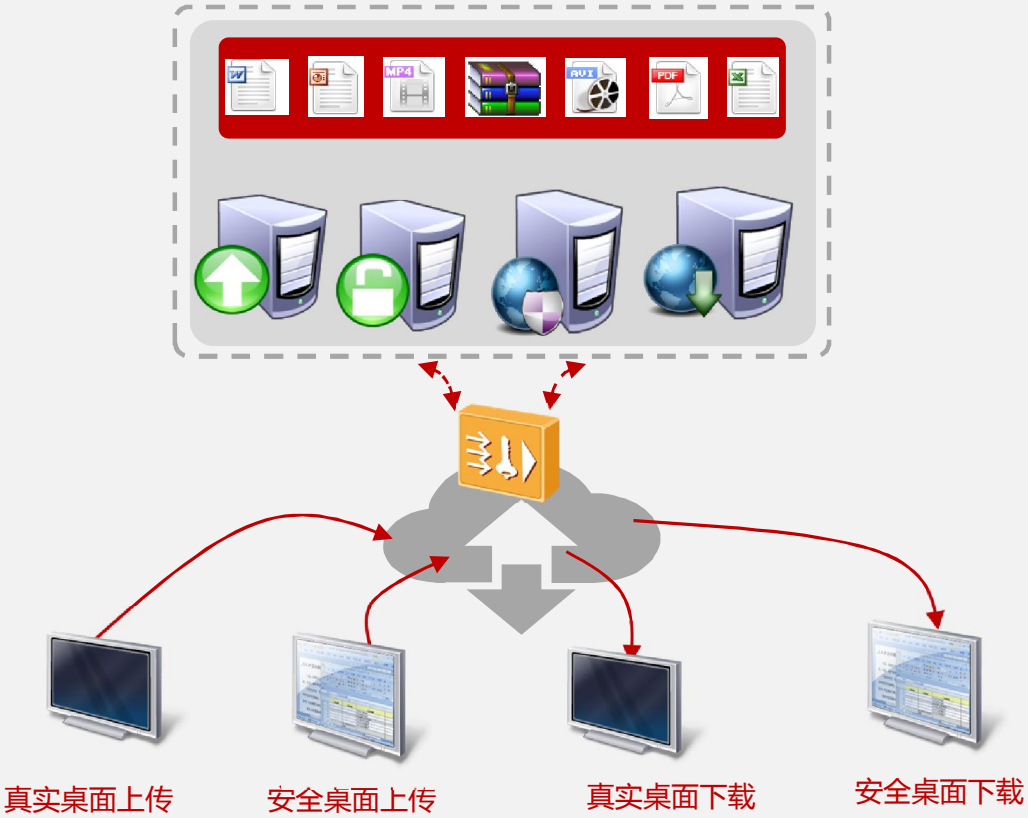


- **多个实例：**一个台物理机器可以同时生成多个安全桌面，用户通过不同的安全桌面访问不同的网络，达到所有区域的安全隔离
- **防止剪切板拷贝：**安全桌面虚拟化了一个粘贴板，和系统粘贴板进行了隔离。在安全桌面内拷贝的数据保存在虚拟化粘贴板内，只能复制到安全桌面内的进程中，无法复制到真实桌面内的进程中
- **桌面切换：**用户可在终端屏幕上方浮动的导航条上进行多屏幕切换、操作方便
- **桌面自动启动：**安全桌面可以设置开机自启动、退出安全桌面注销或者关闭计算机

HUAWEI

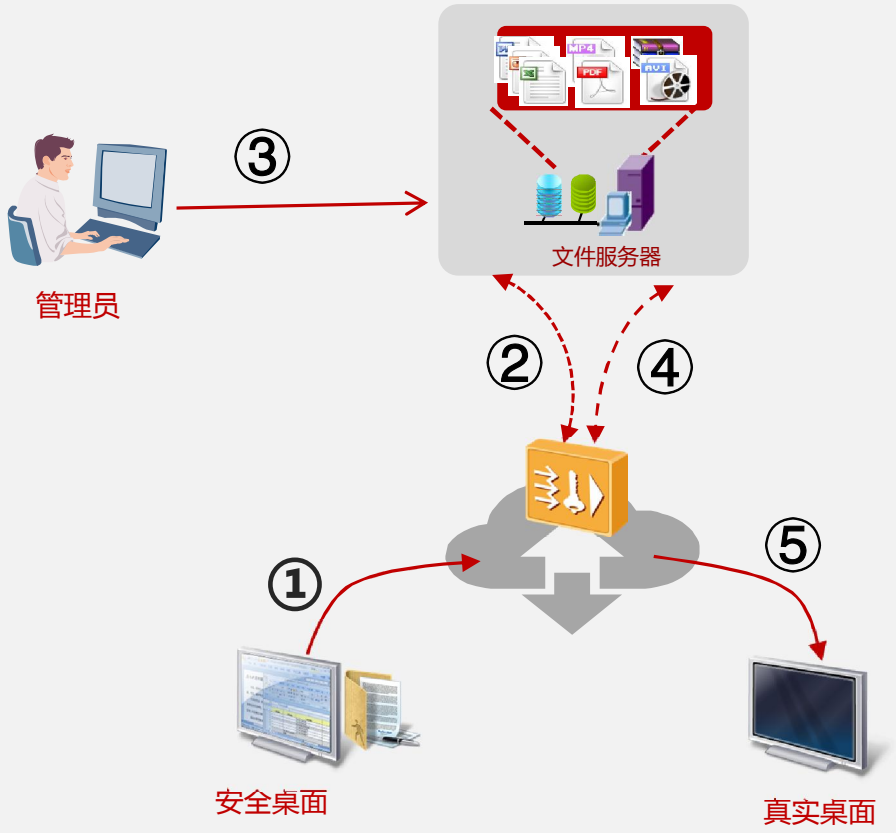
安全数据传输控制

- 上传下载目录统一指定，操作被审计
- 非受权服务器不允许文件传输
- 传输内容通过关键字过滤
- 传输链路高强度加密
- 跨区域传输被禁止



HUAWEI

安全桌面数据导出



①在安全桌面将要导出的内容上传到文件服务器

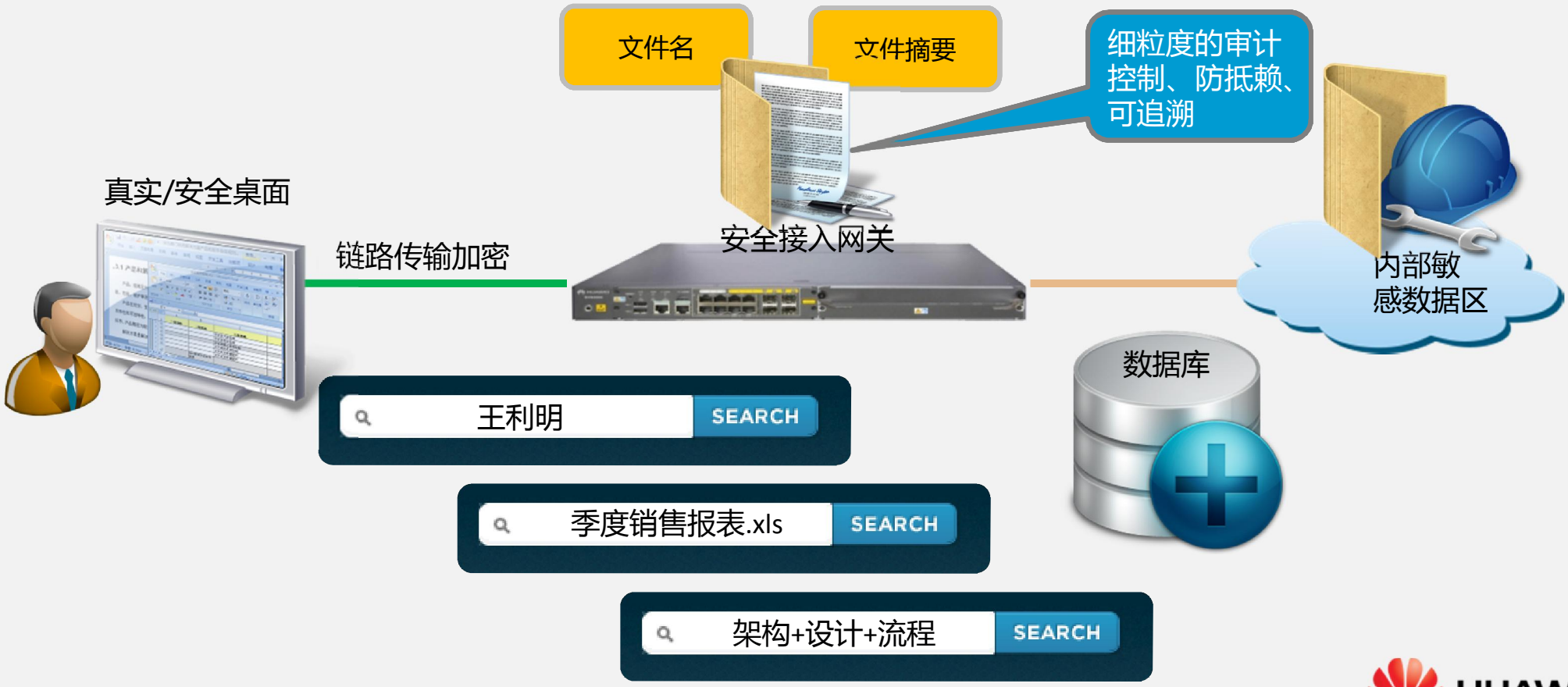
②SVN审计上传的内容将内容发送到文件服务器

③管理员审计文件内容的合规性

④在真实桌向文件服务器下载文件，SVN做文件审计

⑤文件传送到真实桌面

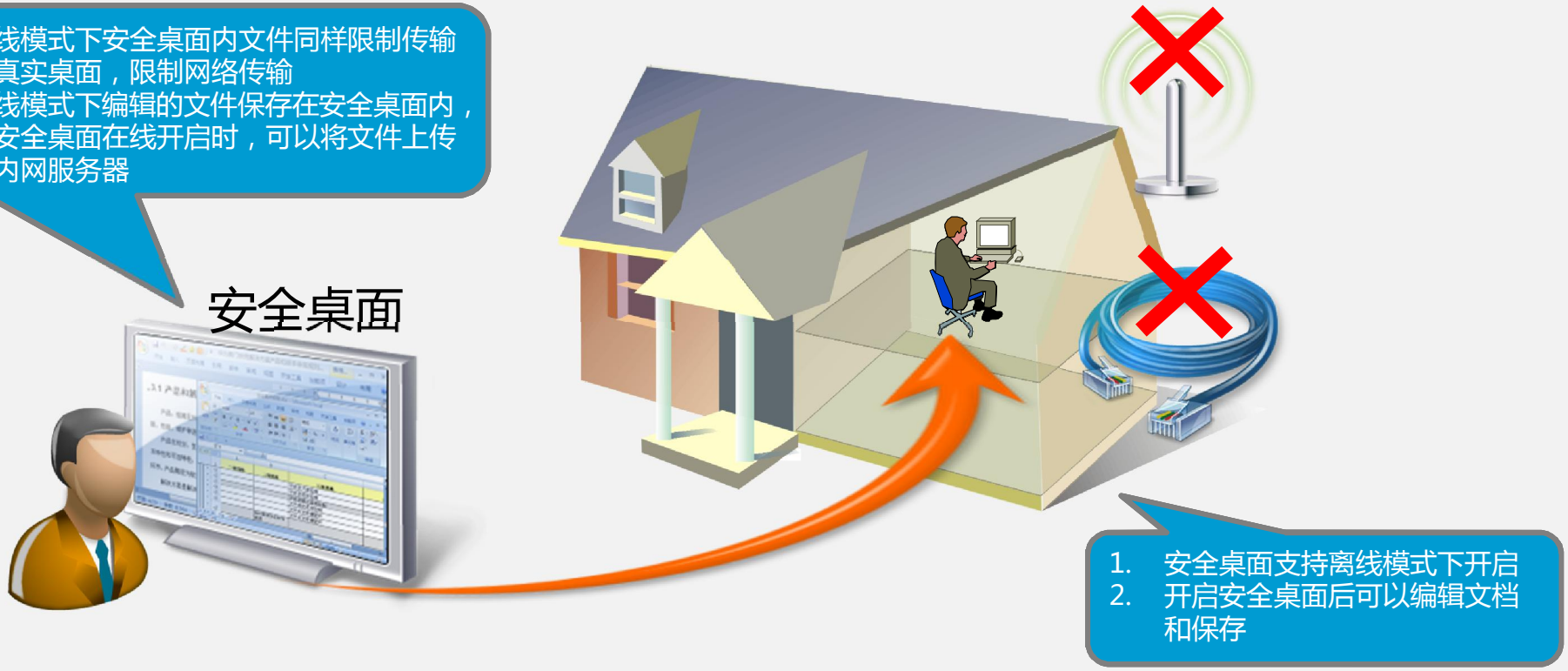
数据细粒度审计



HUAWEI

安全的离线办公

1. 离线模式下安全桌面内文件同样限制传输到真实桌面，限制网络传输
2. 离线模式下编辑的文件保存在安全桌面内，当安全桌面在线开启时，可以将文件上传到内网服务器



1. 安全桌面支持离线模式下开启
2. 开启安全桌面后可以编辑文档和保存

HUAWEI

华为区域智慧隔离方案亮点

业安全厂商全力打造

领先的安全沙箱
区域安全隔离，有效防止病毒、木马攻击；白名单配置，防止运行工作无关应用，提高工作效率；
专业的多实例技术
一个物理桌面内可创建多个安全桌面，不同安全桌面访问不同的区域，一机多用，大幅度降低投资成本；

完备的文件访问隔离
只允许用户访问指定的真实桌面文件与目录，跨区域数据文件加密（AES256高强度加密）存储在虚拟空间中，退出后无痕化清除；
外设及网络访问控制
禁止安全桌面内访问终端外设及网络传输
防截屏、防粘贴板拷贝
通过屏蔽截屏、虚拟化粘贴板等措施，防止机密数据泄漏

文件内容扫描
跨区域数据传输和安全桌面与真实桌面数据导入导出都支持按关键字监控；
指纹级操作审计
用户文件的操作都会被详细的记录，管理员可根据记录定期审计用户行为，回溯用户的非授权操作；

便捷的部署
网络区域边界部署SVN网关、客户端可自动安装
桌面自启动
安全桌面可设置开机自启动、退出安全桌面注销或关闭计算机
多桌面切换
终端屏幕上方浮动导航条上进行多屏幕切换、操作方便

Content

HUAWEI

华为信息安全管理-建设阶段

01年成立信息安全部，直接向CIO汇报，制定公司信息安全政策，流程，制度
03年设立信息安全审计部，与财务审计并列为2大关键点审计
05年全面审视信息安全管理体系，建立以风险驱动的安全监管体系

技术型企业
（事件驱动）

基础保证

- 信息安全评估和差距分析
- 建立信息安全组织体系
- 初步推行安全管理体系
- 启动安全基础设施建设

1999~2003

制度型企业
（流程驱动）

集中建设

- 实现制度化、流程化和经常化
- 建设整体的信息安全防护体系
- 建立集中监控平台

2003~2005

成熟型企业
（风险导向）

策略固化

- 建设应急响应机制。
- 建立安全配置管理，实现安全风险的量化管理机制
- 建立风险驱动安全管理持续优化机制

2005~现在

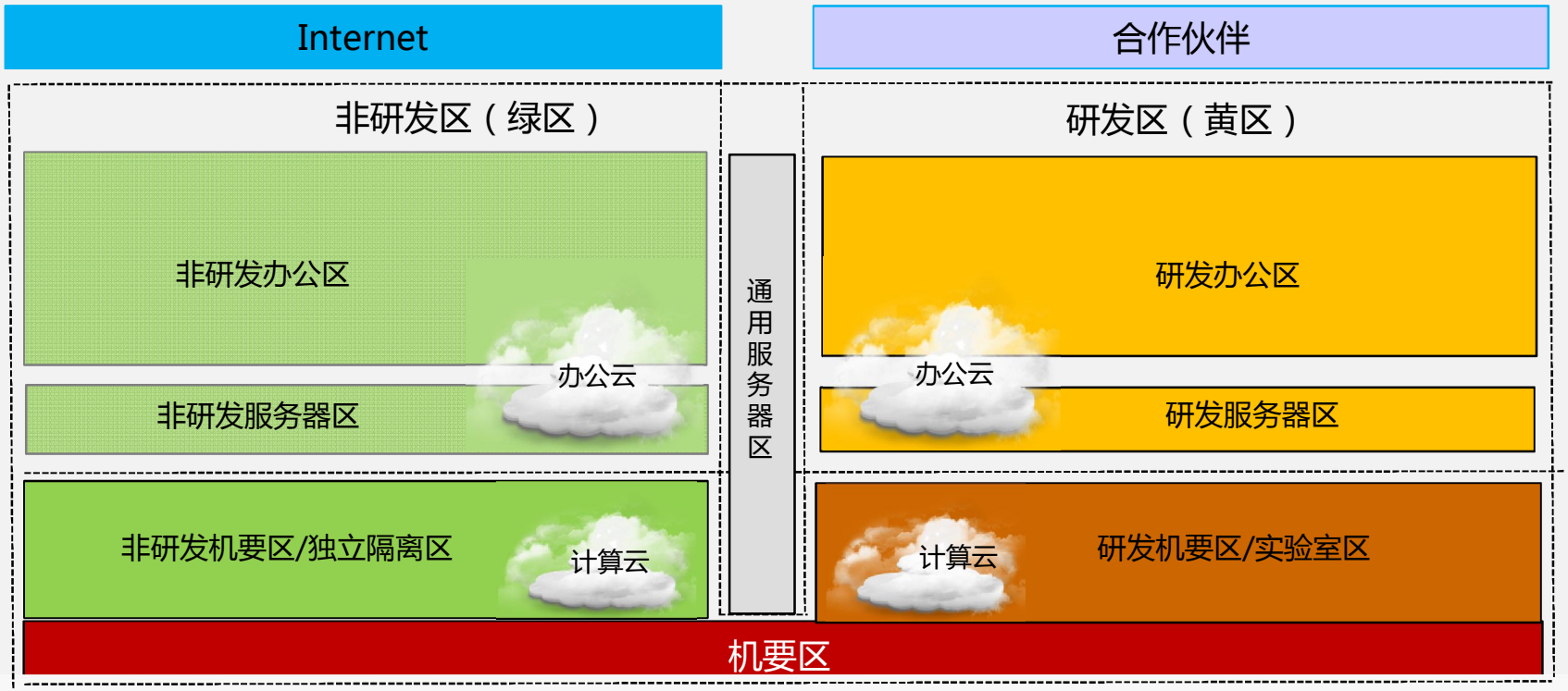
3要素

企业高层支持

分步实施策略

技术产品支撑

华为公司安全区域简介



华为公司在全球有300多个分支机构，公司产品和解决方案已经应用于全球150多个国家。

拥有14万多名员工，研发占比44%；拥有超过20万台PC/便携机，移动办公用户超过7万，桌面云用户超过8万。

HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY