中国航天

聚焦数据与智能　持续为客户创造价值

航天大道安全桌面云解决方案

目录

目录

01 Part One 国防军工办公安全现状及趋势

国防军工办公安全现状及趋势

信息安全面临持续挑战

2009年
潜艇资料被窃事件

- 网络间谍工具钻入某科研人员违规上网的工作电脑
- 多份重要保密资料甚至一些绝密技术资料落入境外情报机关之手

2010年
维基解密

- 美军方下令全军禁止使用USB存储器等移动存储介质

2011年
震网病毒

- 被病毒感染的U盘插入USB接口后即感染电脑
- 令德黑兰的核计划拖后了两年

2012年
三星打印机后门

- 被发现包含硬编码帐号后门，可被远程控制设备，泄露敏感数据

2013年
棱镜门

- 奥巴马政府陷入丑闻，形象受损

信息安全上升到了国家战略高度

中华人民共和国中央人民政府
www.GOV.cn
The Central People's Government of the People's Republic of China

网站首页 | 今日中国 | 中国概况 | 法律法规 | 公文公报 | 政务互动 | 政府建设 | 工作动态 | 人事任免 | 新闻发布

当前位置： 首页>> 领导活动

中央网络安全和信息化领导小组第一次会议召开

中央政府门户网站 www.gov.cn 2014年02月27日 20时46分 来源：新华社

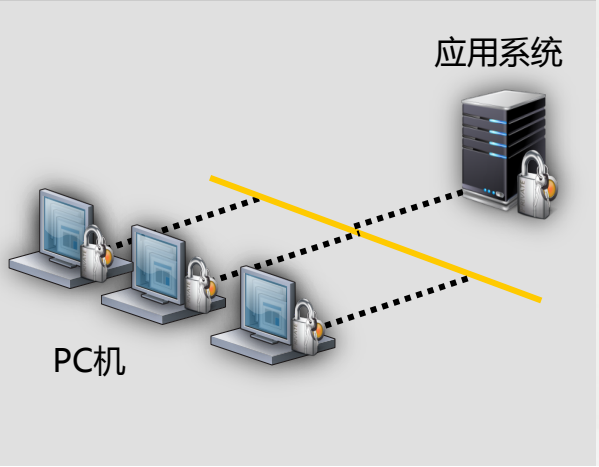
【字体：大 中 小】 打印本页 关闭窗口

习近平主持召开中央网络安全和信息化领导小组第一次会议强调
总体布局统筹各方创新发展 努力把我国建设成为网络强国
李克强 刘云山出席

新华社北京2月27日电 中共中央总书记、国家主席、中央军委主席、中央网络安全和信息化领导小组组长习近平2月27日下午主持召开中央网络安全和信息化领导小组第一次会议并发表重要讲话。他强调，网络安全和信息化是事关国家安全和国家发展、事关广大人

2016年4月19日，习总主持召开网络安全和信息化工作座谈会，探讨**网络信息安全技术能力建设顶层设计**

传统PC系统存在的问题

传统PC数据本地化 信息容易泄露	故障率高 故障维修时间长	固化不灵活 资源利用率低，人员流动成本高	维护管理困难，能耗大 后期运营维护开支大
			
安全性	可靠性	效率	运维管理

国防军工办公安全现状及趋势

国防军工终端存在安全隐患

多“鼠”多“机”

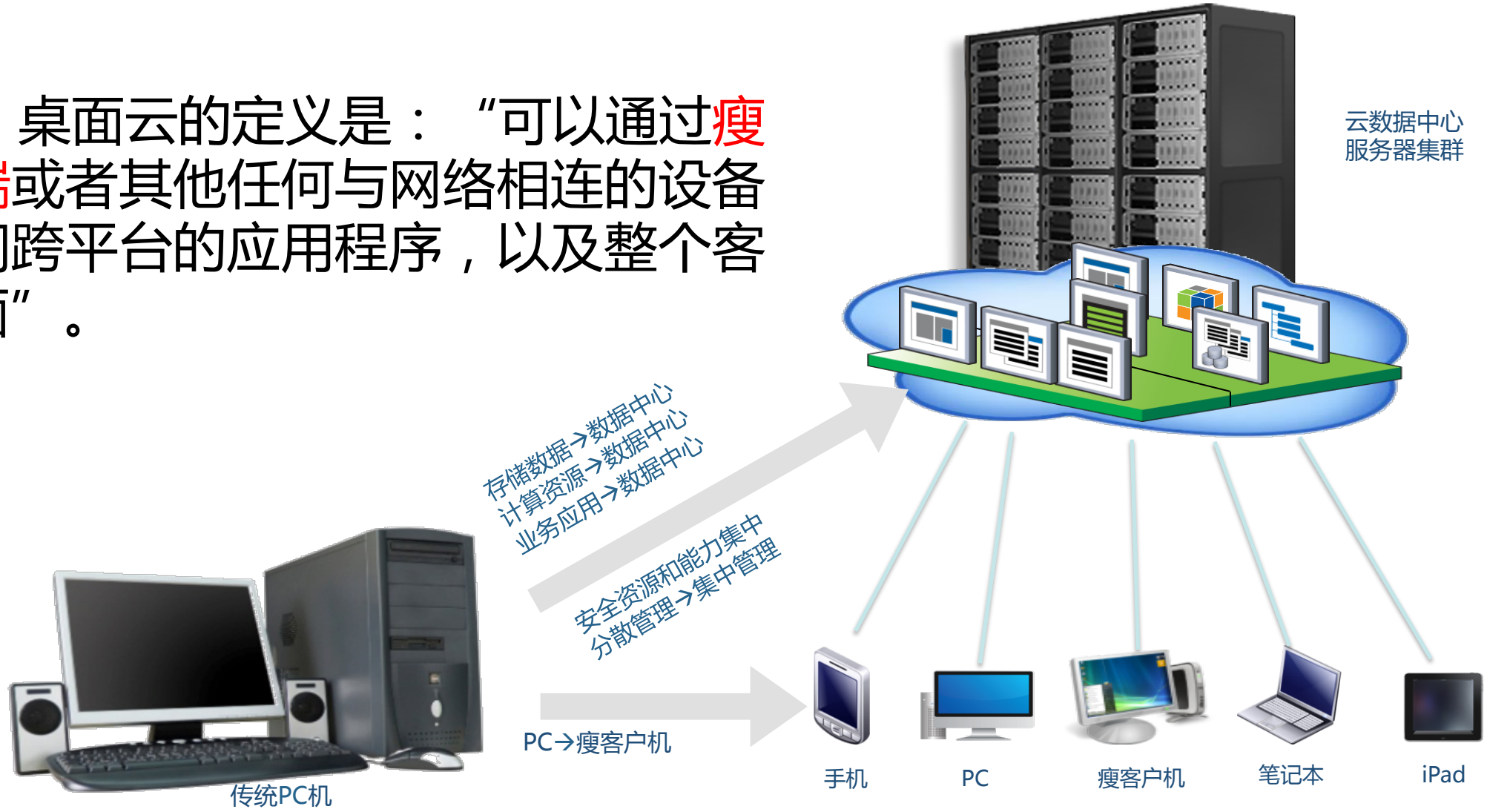
- 多重布线，基础设施建设和维护复杂
- 专网专维，维护成本高，效率低
- 不同业务数据共享在效率和安全上难两全

安全终端肥胖症

- 外设多，网络管控难，泄密途径多，防不胜防
- 防病毒、安全审计、终端加密，防非法外联，不堪重负
- 软件兼容性问题多，远程维护难实施，维护人员满天飞

国防军工办公安全现状及趋势

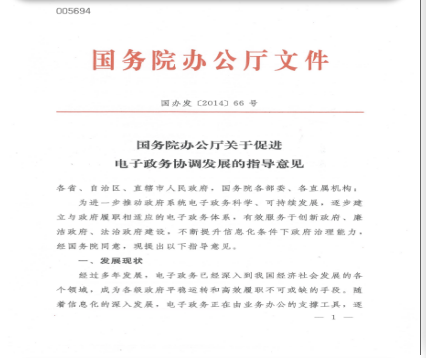
桌面云的定义是：“可以通过瘦客户端或者其他任何与网络相连的设备来访问跨平台的应用程序，以及整个客户桌面”。



国防军工办公安全现状及趋势

国家鼓励云计算应用创新

国办发〔2014〕66号



005694

国务院办公厅文件

国办发〔2014〕66号

国务院办公厅关于促进
电子政务协调发展的指导意见

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：

为进一步推动政府系统电子政务科学、可持续发展，逐步建立与政府履职相适应的电子政务体系，有效服务于创新政府、廉洁政府、法治政府建设，不断提升信息化条件下政府治理能力，经国务院同意，现提出以下指导意见。

一、发展现状

经过多年发展，电子政务已经深入到我国经济社会发展的各个领域，成为各级政府平稳运转和高效履职不可或缺的手段。随着信息化的深入发展，电子政务正在由业务办公的支撑工具，逐

— 1 —

国务院办公厅关于促进电子政务协调发展的指导意见

主要目标：信息共享、业务协同水平大幅提升

基本原则：

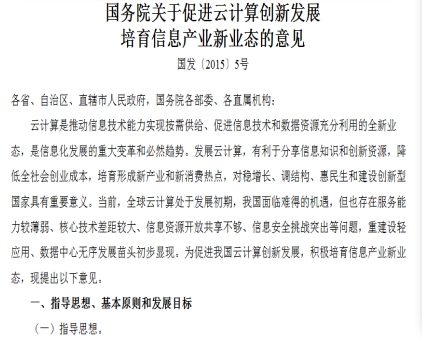
1、需求导向，不断提高电子政务的支撑作用和应用效能；

2、安全可控，确保网络、数据、应用安全

顶层设计：现有业务应用进行分类，分别向内网和外网迁移

保障措施：促进云计算、大数据在电子政务应用服务中的发展规划；政务网络和业务系统优先采用国产软硬件产品

国发〔2015〕5号



国务院关于促进云计算创新发展
培育信息产业新业态的意见

国发〔2015〕5号

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：

云计算是推动信息技术能力实现按需供给、促进信息技术和数据资源充分利用的全新业态，是信息化发展的重大变革和必然趋势，发展云计算，有利于分享信息知识和创新资源，降低全社会创业成本，培育形成新产业和新消费热点，对稳增长、调结构、惠民生和建设创新型国家具有重要意义。当前，全球云计算处于发展初期，我国面临难得的机遇，但也存在服务能力较薄弱、核心技术差距较大、信息资源开放共享不够、信息安全挑战突出等问题，重建设轻应用、数据中心无序发展苗头初步显现。为促进我国云计算创新发展，积极培育信息产业新业态，现提出以下意见。

一、指导思想、基本原则和发展目标

（一）指导思想。

国务院关于促进云计算创新发展培育信息产业新业态的意见

指导思想：以全面深化改革为动力，以提升能力、深化应用为主线

发展目标：云计算在重点领域的应用得到深化

主要任务：

1、大力发展公共云计算服务，实施云计算工程；

2、充分发挥云计算对数据资源的集聚作用，实现数据资源的融合共享，推动大数据挖掘、分析、应用和服务；

3、鼓励应用云计算技术整合改造现有信息系统，积极开展试点示范，探索基于云计算的信息化建设运行新机制。

02 Part Two 国防军工信息化需求分析

国防军工涉密网多种业务环境需求分析

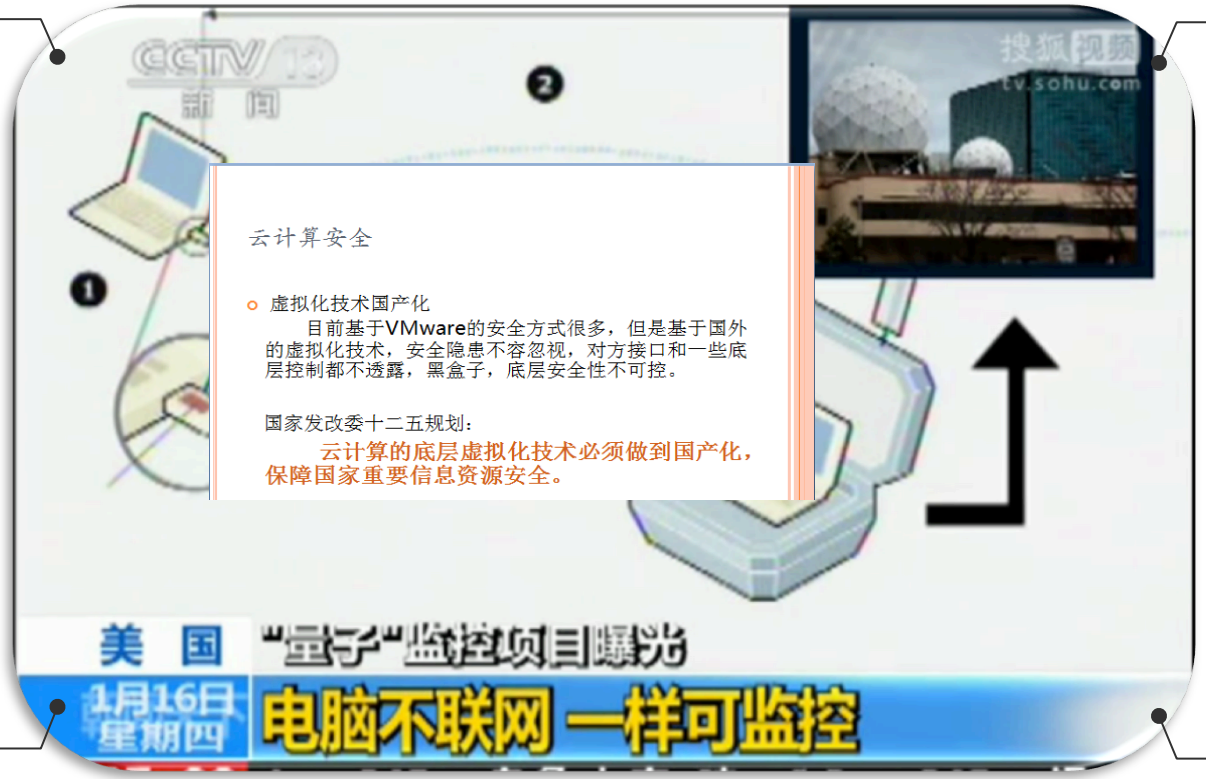
普通OA办公	软件研发	工业网	3D制图	会议评审
• 卓越体验 • 敏捷高效 • 高安全	• 跳转系统 • 代码持续集成 • 代码仿真 • 数据安全传输	• 软硬件调测 • 系统测试	• 高清制图 • 120MB高清编辑	• 涉密资料无纸化 • 快速启动 • 不保存个性化数据

国防军工信息化需求分析

信息通信技术基础设施国产自主可控的需求

网络设备国产化
- 路由器
- 交换机

IT设备国产化
- 服务器
- 存储

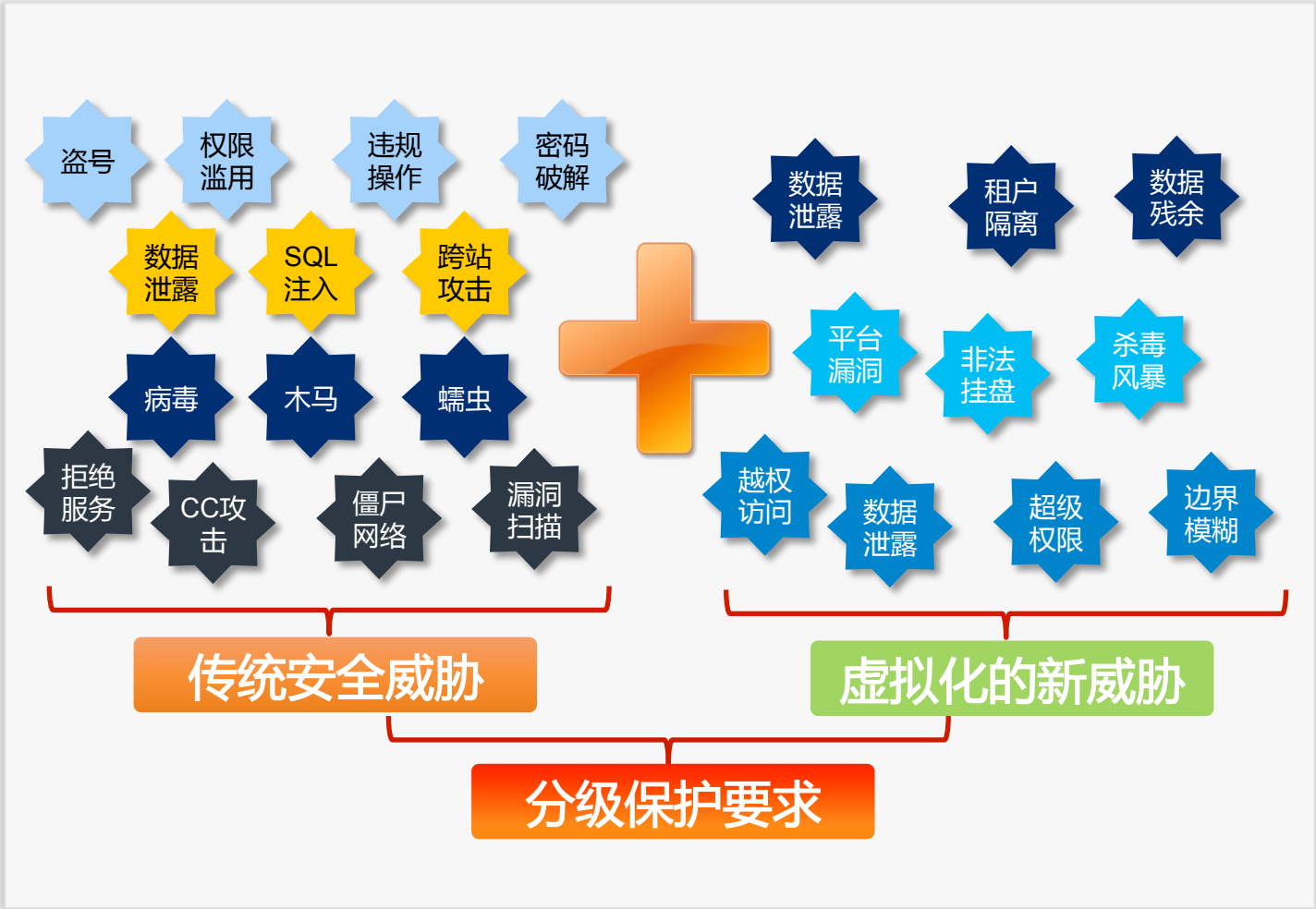


应用/平台国产化
- 操作系统
- 数据库
- 应用软件
- 虚拟化平台

安全产品国产化
- 防火墙
- 防病毒
- 入侵检测

国防军工信息化需求分析

安全防护需求分析



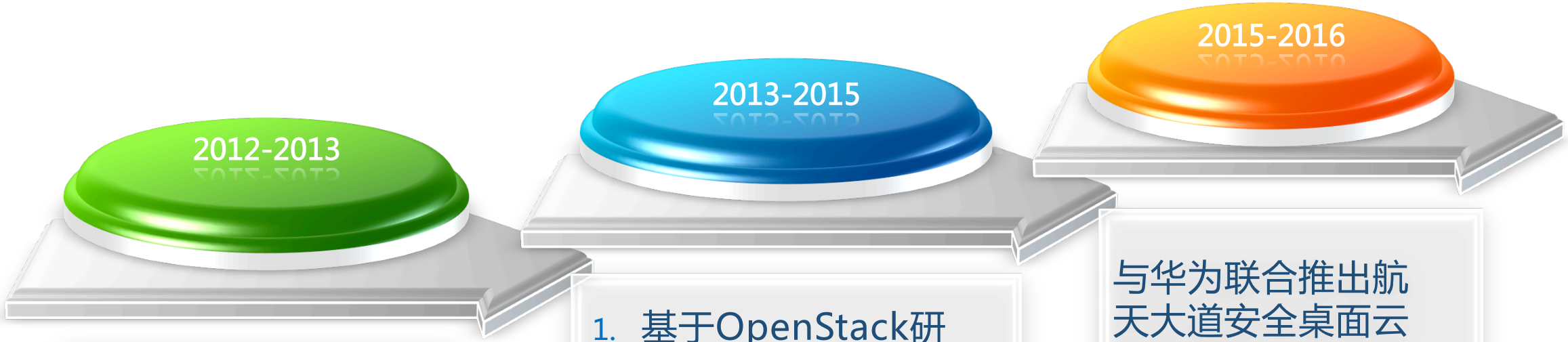
设计需求

- **满足保密局分级保护标准要求**
  - 《XXXXXX的虚拟化产品技术要求》
  - 《XXXXXX的虚拟化系统安全保密要求》（实施指南改名）
- **满足国密局加密算法要求**
  - 身份认证、传输加密、存储加密
- **传统安全威胁依然面临**
  - 病毒、木马、蠕虫等传播快速
  - 跨站攻击、SQL注入等攻击方式层出不穷
- **虚拟化架构变化带来的风险**
  - 租户之间的安全隔离问题，造成数据泄露风险增大
  - 虚机删除后，残余数据造成数据泄密
  - 规模杀毒带来的杀毒风暴问题

03 Part Three 航天大道安全桌面云

航天大道安全桌面云解决方案

研制历程：历时4年，与合作者共同努力，推出航天大道安全桌面云解决方案



基于CloudStack开发私有云平台应用于型号大数据处理。

1. 基于OpenStack研制研发云办公桌面；
2. 致力于云办公环境下的数据安全；

与华为联合推出航天大道安全桌面云解决方案

航天大道安全桌面云解决方案

航天大道安全桌面云（DaoCloud）为用户提供全面的信息基础设施安全解决方案，满足国防安全领域、军工行业以及对技术、商业秘密管控要求较高的民用企业桌面云与数据中心建设需求。

航天大道安全桌面云解决方案

支持多品牌软硬件，支持PC利旧

支持多种品牌TC（瘦客户机）


华为

联想


惠普

华硕

兼容多种品牌服务器


华为


浪潮


曙光


联想

软终端支持PC利旧

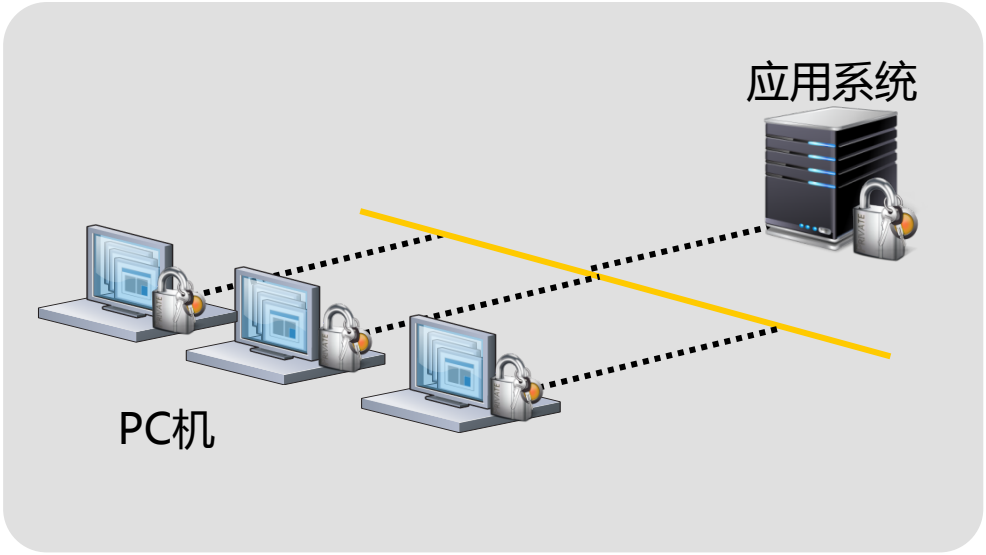
广泛的移动终端支持

多操作系统支持

DaoCloud产品价值

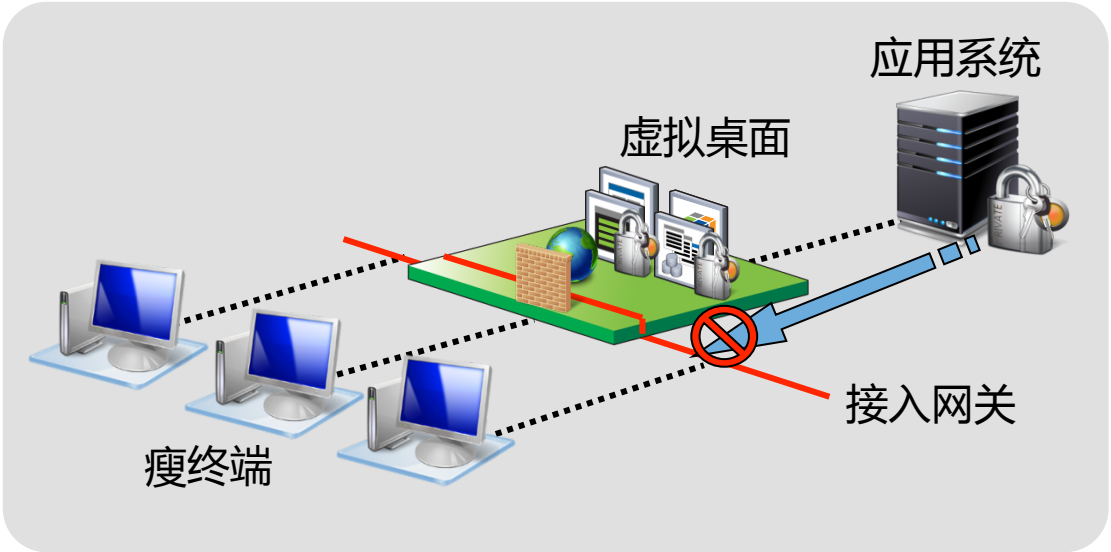
1.数据上移，信息安全

传统桌面：数据分散在每个终端



操作系统和应用部署在终端，信息在本地保存和运行，容易被病毒攻击、恶意窃取。

DaoCloud：应用与数据被集中管理



终端与信息分离，桌面和数据在后台集中存储和处理，访问可控，传输到终端的仅是屏幕的刷新。

DaoCloud产品价值

2.高效维护，自动管控

- 维护效率提升

桌面云不需要前端维护，强大的一键式维护工具让自助维护更加方便，提高了企业运营效率。使用桌面云后，每位IT人员可管理超过2000台虚拟桌面，维护效率提高4倍以上。

- 资源自动管控

白天可自动监控资源负载情况，保证物理服务器负载均衡；夜间可根据虚拟机资源占用情况，关闭不使用的物理服务器，节能降耗。

	传统办公	DaoCloud
维护流程	故障申报→安排人员维护→故障定位→进行维护	免维护 故障(死机)→员工自助重启→完成
维护时间	2-4 小时	3 分钟
维护人员占比	100 : 2 员工　IT管理员	2000 : 1 员工　IT管理员

DaoCloud产品价值

3.应用上移，业务可靠

应用集中部署
集中管控，数据信息安全

应用远程发布
随时随地接入，便捷使用体验

应用集中运维
业务快速上线，远程0维护

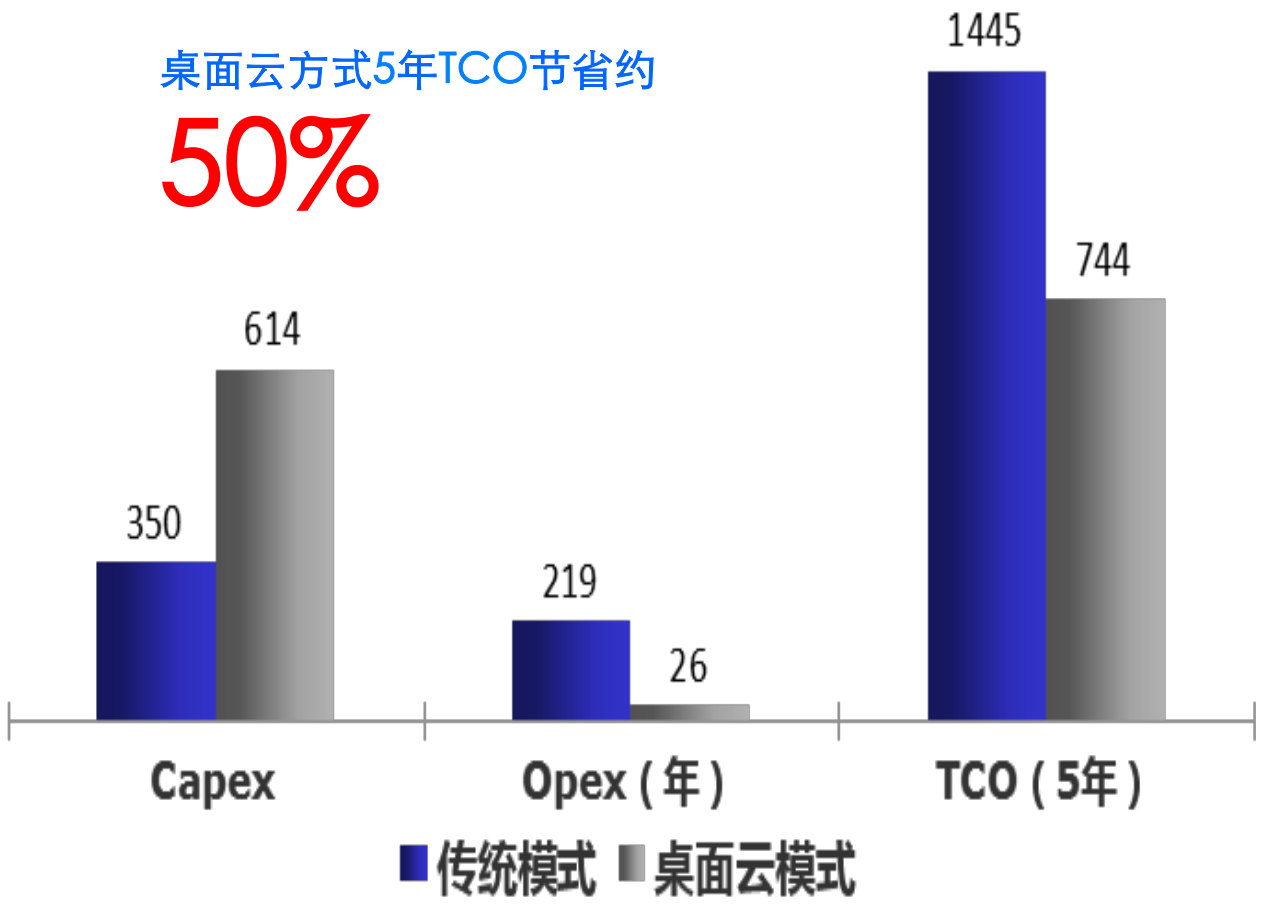
高性价比
减少部署成本，绿色节能

DaoCloud产品价值

4.节省成本，绿色办公

桌面云方式5年TCO节省约

50%



1. 传统PC建设模式

Capex：350万

PC：3500*1000=350万

Opex：219万/年

PC电费：0.25*24*365*1*1000=219万

5年TCO：1445万　　350+219*5=1445万

2. 桌面云建设模式

Capex：614万

TC：2400*1000=240万

服务器+存储：40000*15+1*1000000=160万

桌面云软件：2138*1000=214万

Opex：26万/年

TC电费：0.025*24*365*1*1000=21.9万

服务器电费：0.3*24*365*1*15=4万

5年TCO：744万　　614+26*5=744万

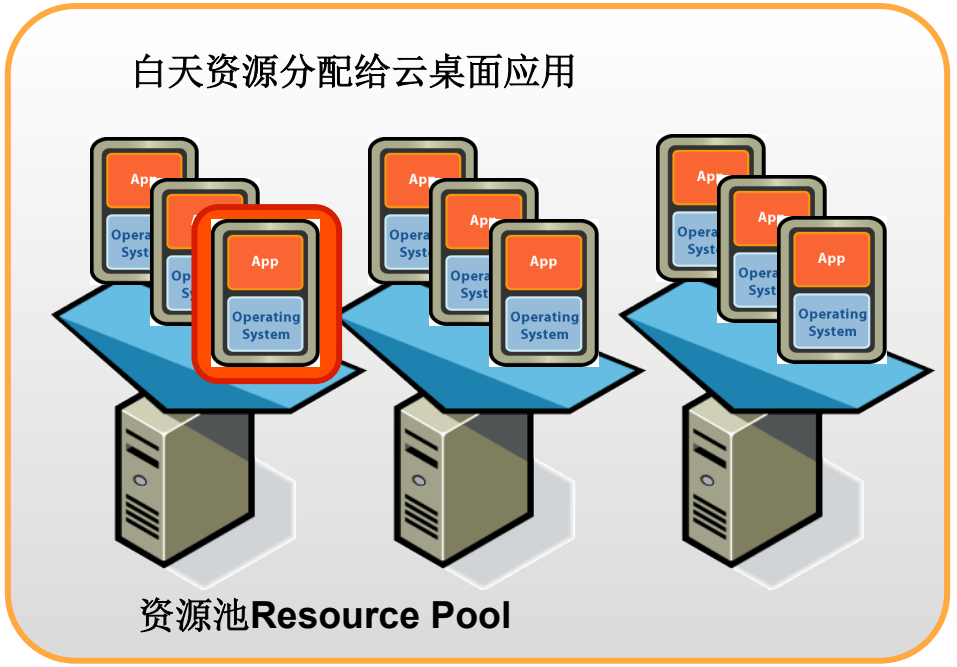
说明　1、以上计算数据取业界常规参考值

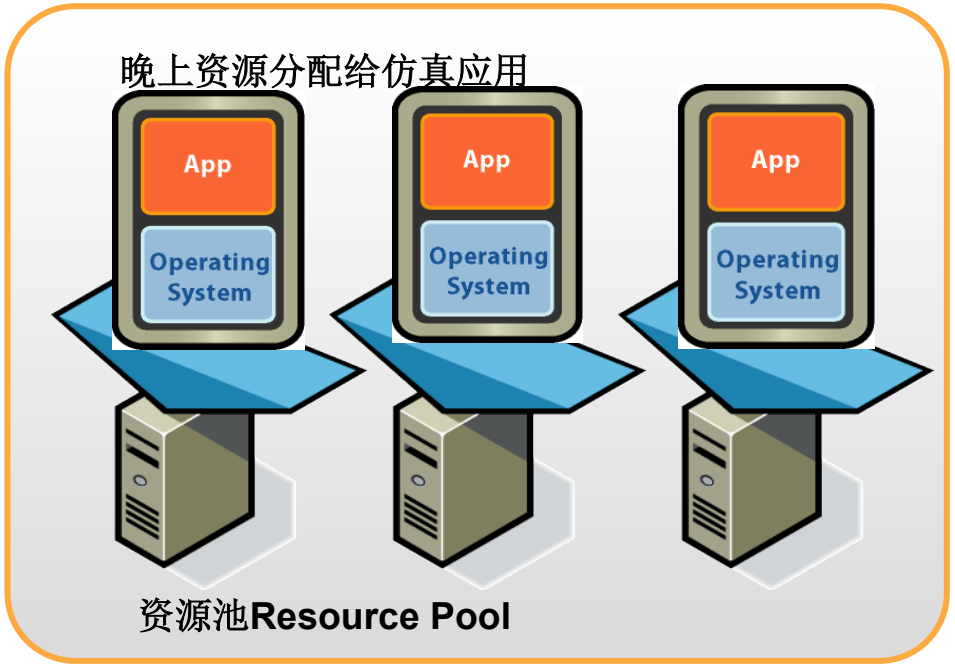
2、未计算部分共有成本，如客服软件等

3、未计算维护人力、管理等节省成本

DaoCloud产品价值

5.资源弹性，复用共享



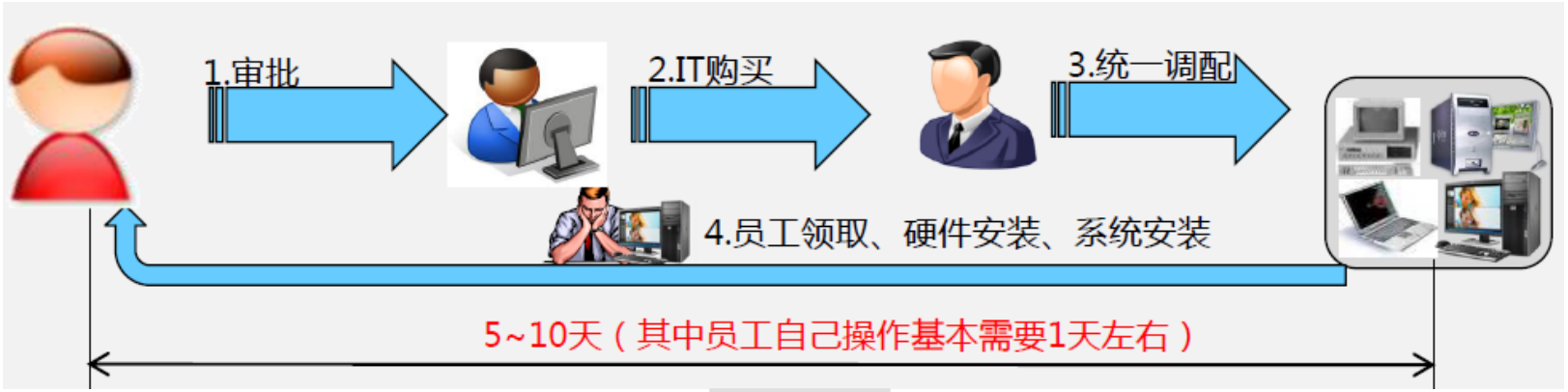


动态资源分配，保证所有应用需要的的资源

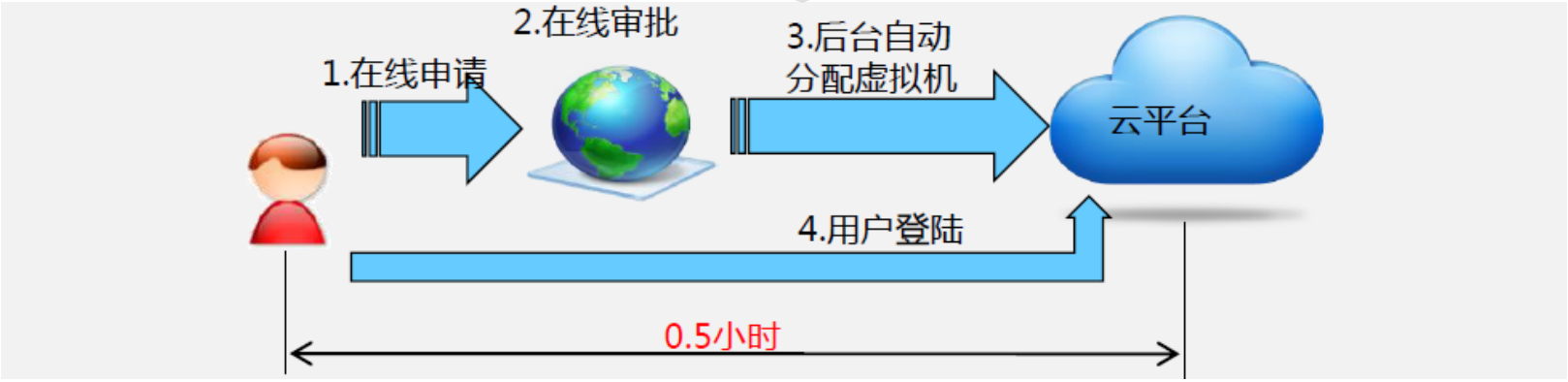
DaoCloud产品价值

6.安装便捷，部署快速

传统PC



DaoCloud桌面云



04 Part Four DaoCloud产品特点

DaoCloud产品特点

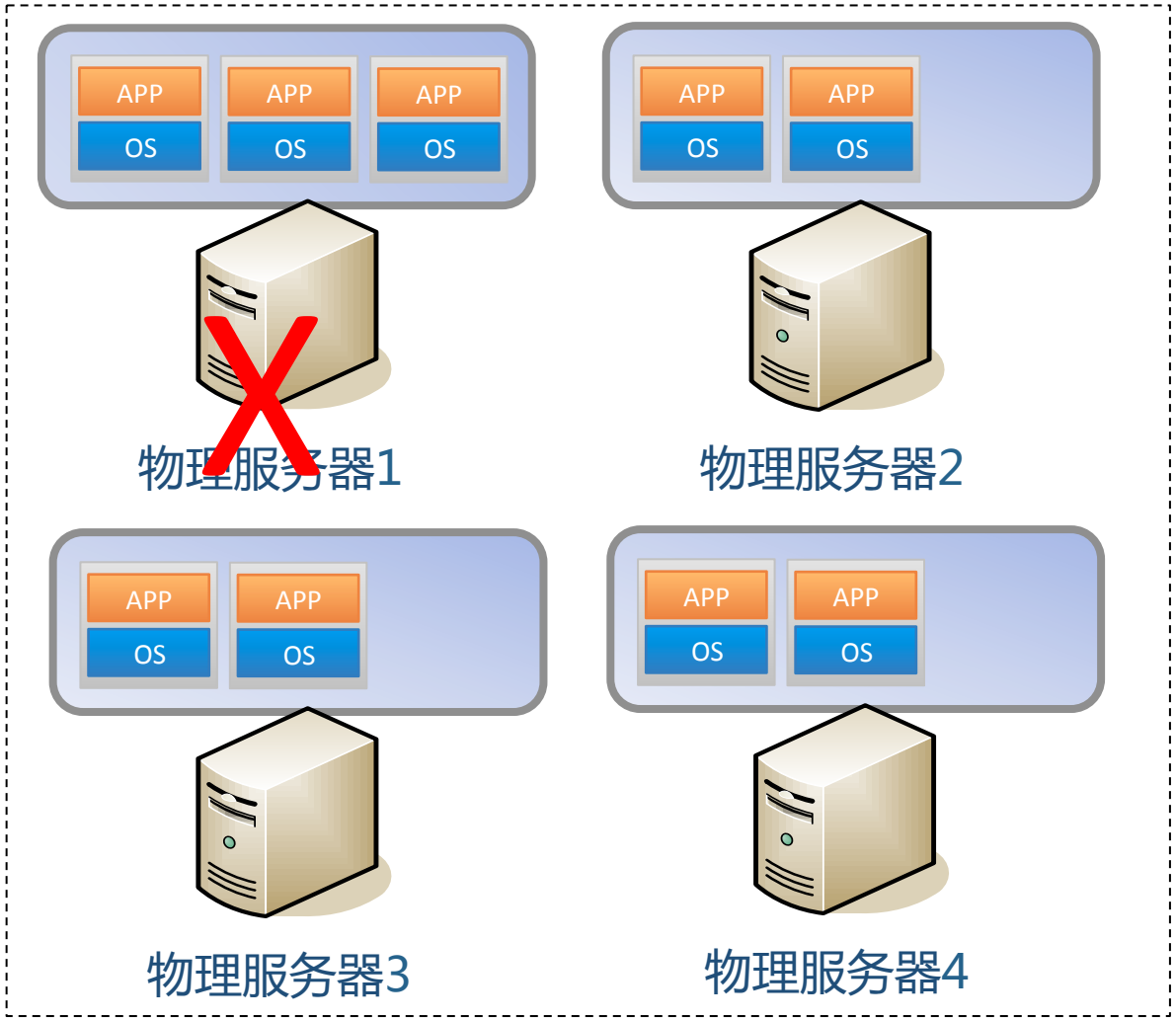
安全可靠

卓越体验

敏捷高效

DaoCloud产品特点：安全可靠

DaoCloud可靠：故障快速恢复，减少业务中断时间

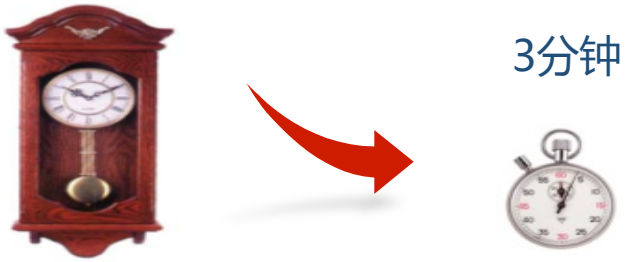


主机、虚拟平台、虚拟机多方故障检测

物理服务器故障时自动重启虚拟桌面

虚拟桌面操作系统故障时自动重启

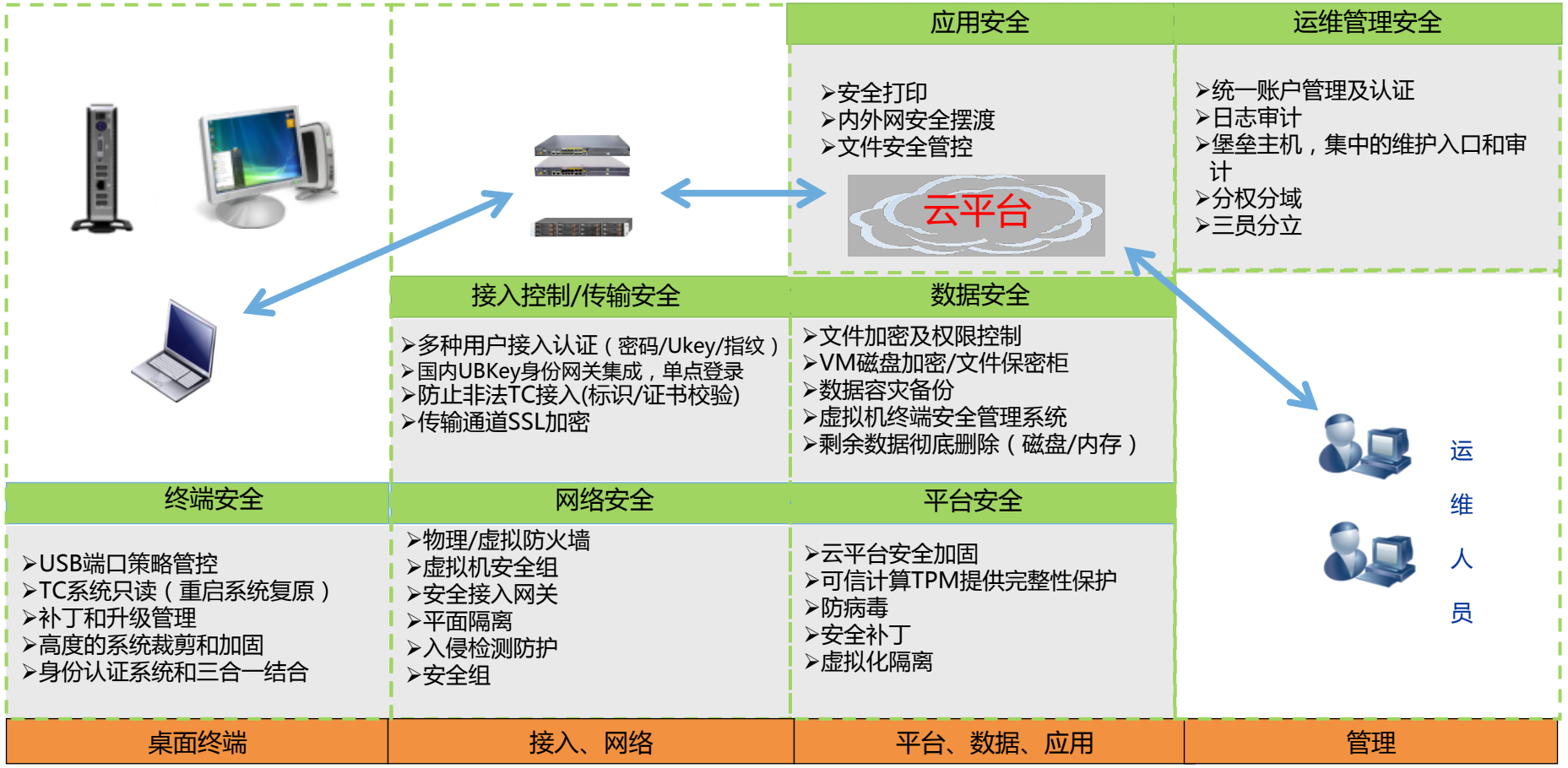
故障恢复时间



提高桌面故障恢复速度，降低业务中断时间，保障业务连续性，提高办公效率。

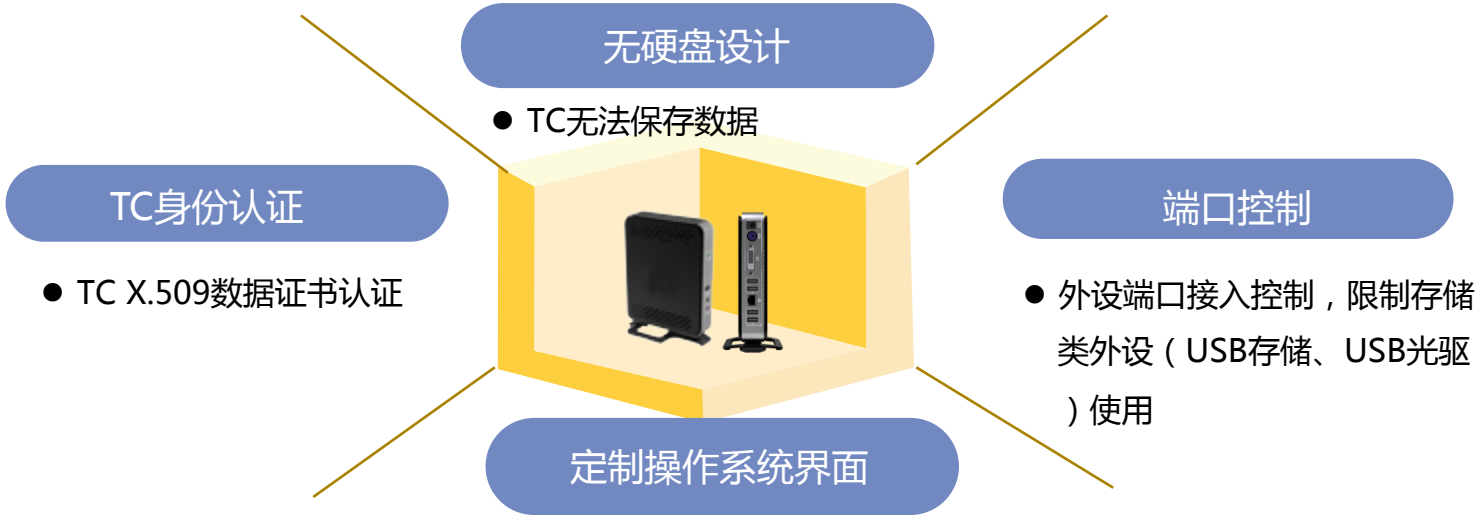
DaoCloud产品特点：安全可靠

DaoCloud安全：八大安全体系实现立体防护



八大安全体系

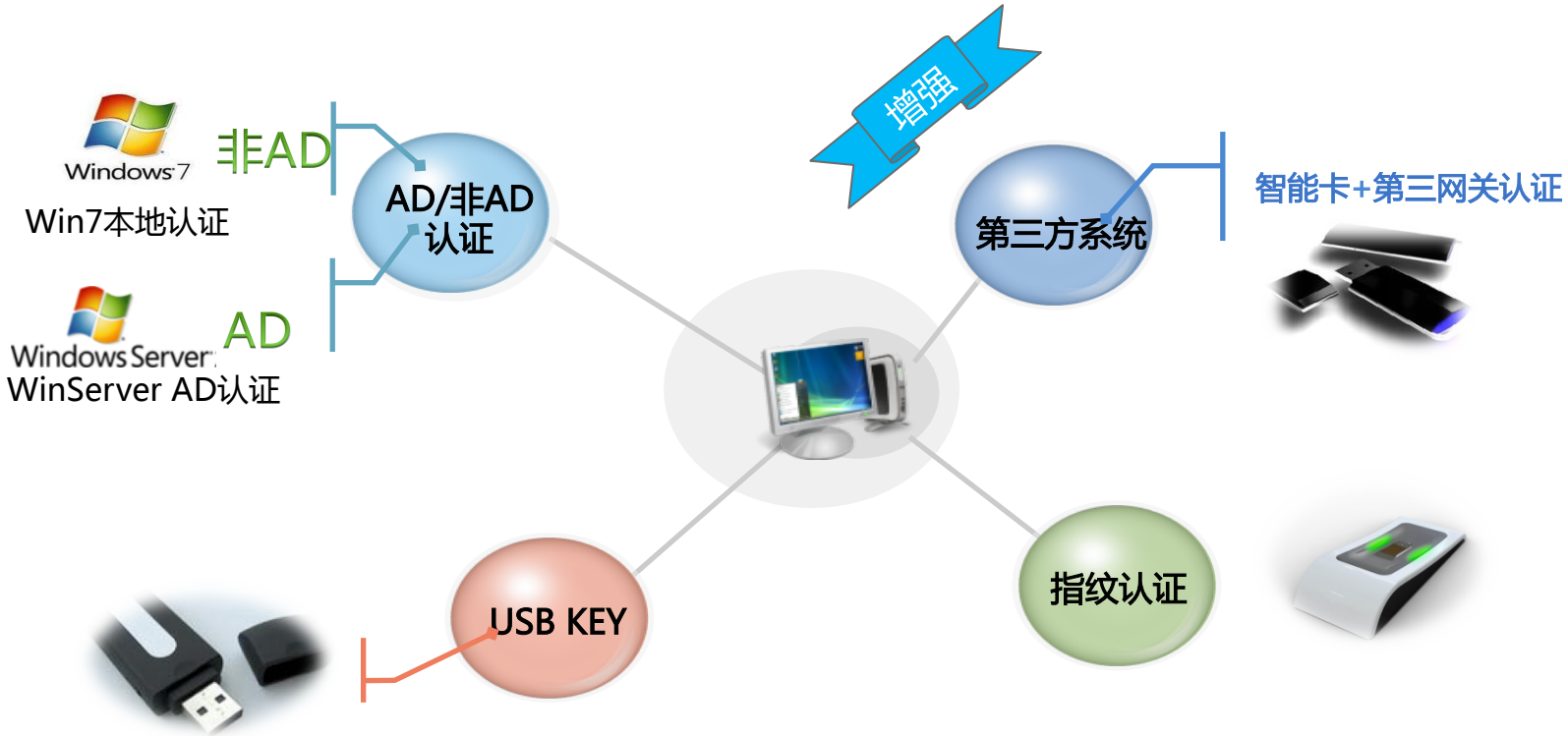
1. 终端安全--TC加固



瘦终端采用精简的OS固件，系统更为安全可靠

八大安全体系

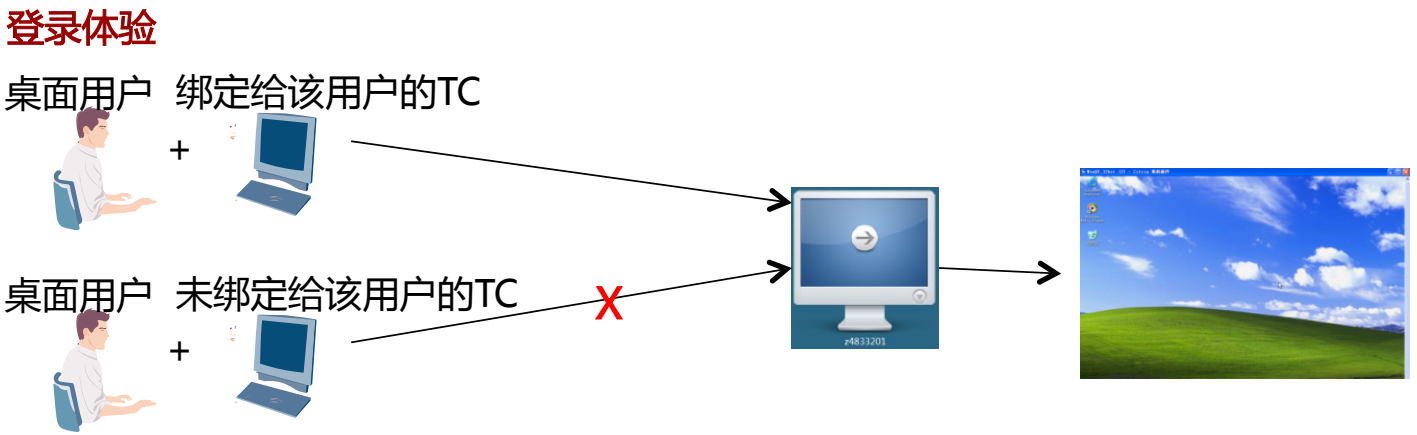
2. 接入安全--完善的用户接入身份认证



丰富的认证方式，支持多级认证、双因子认证

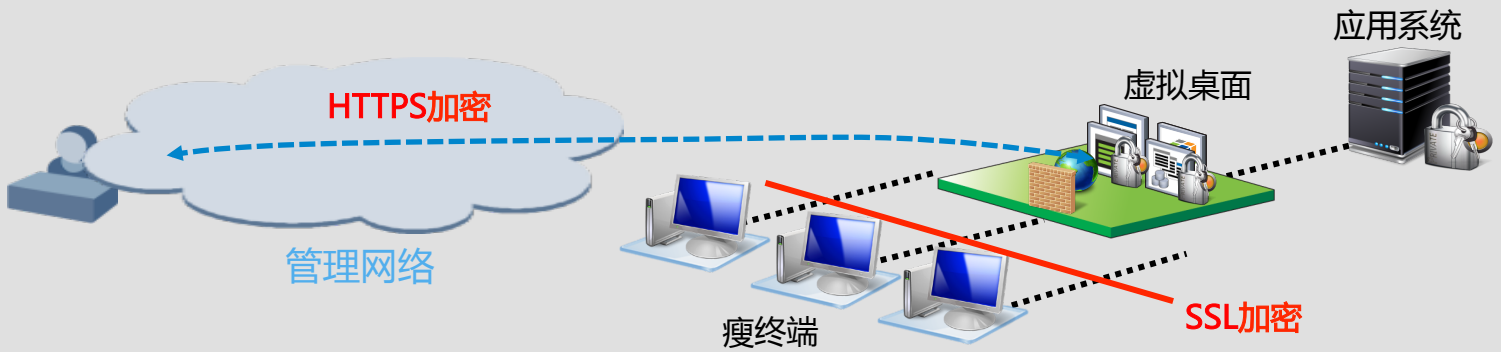
2. 接入安全--固定TC登录

- 通过在TC MAC地址/MAC地址组与域用户/域用户组之间建立绑定关系，实现指定域用户/域用户组成员从固定TC/TC组接入桌面。固定TC接入可以和WI任何一种认证方式同时使用。



- 被绑定到固定TC的桌面用户，只能从被绑定的TC登录WI，而无法使用其他TC登录桌面。

3. 传输安全--传输通道加密



- **管理Portal over HTTPS**

  用户通过portal界面的访问传输通道都是加密的

- **连接协议 over SSL**

  信任域与非信任域之间全部用SSL加密

4. 网络安全--全流量监控

- 虚拟环境威胁检测
  - 将vSwitch流量定向到物理安全设备上进行威胁检测，提供虚拟环境可视。

恶意软件检测

- 蠕虫
- 木马
- 间谍软件
- 广告软件
- 僵尸网络

DDOS检测

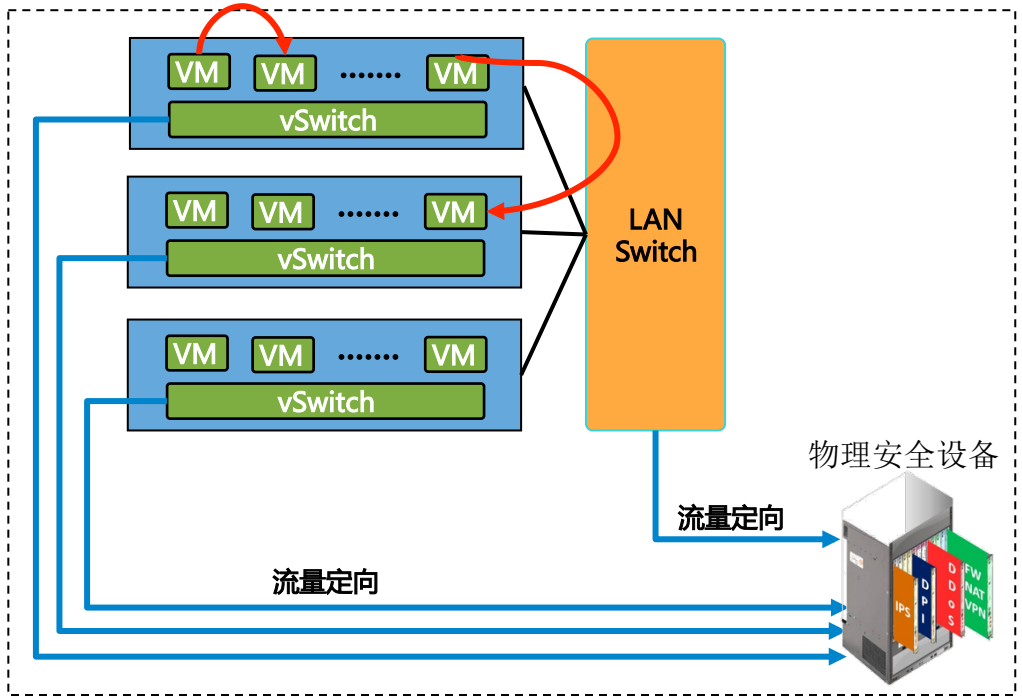
- 针对应用服务的DoS
- 针对操作系统的DoS
- 扫描探测

服务器攻击检测

防止对HTTP、FTP、DNS、Mail等服务器的各种攻击：缓冲区溢出、系统或服务漏洞攻击、暴力破解等。

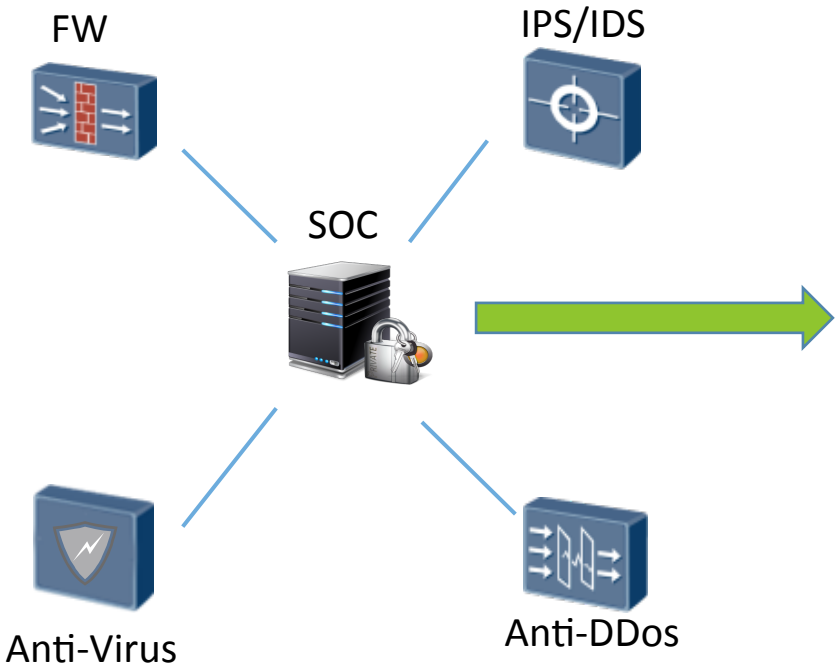
Web攻击检测

检测Web应用相关攻击，包括Web2.0及后台数据库； 对注入攻击、跨站脚本、目录穿越等提供重点防护。



4. 网络安全--安全管理平台

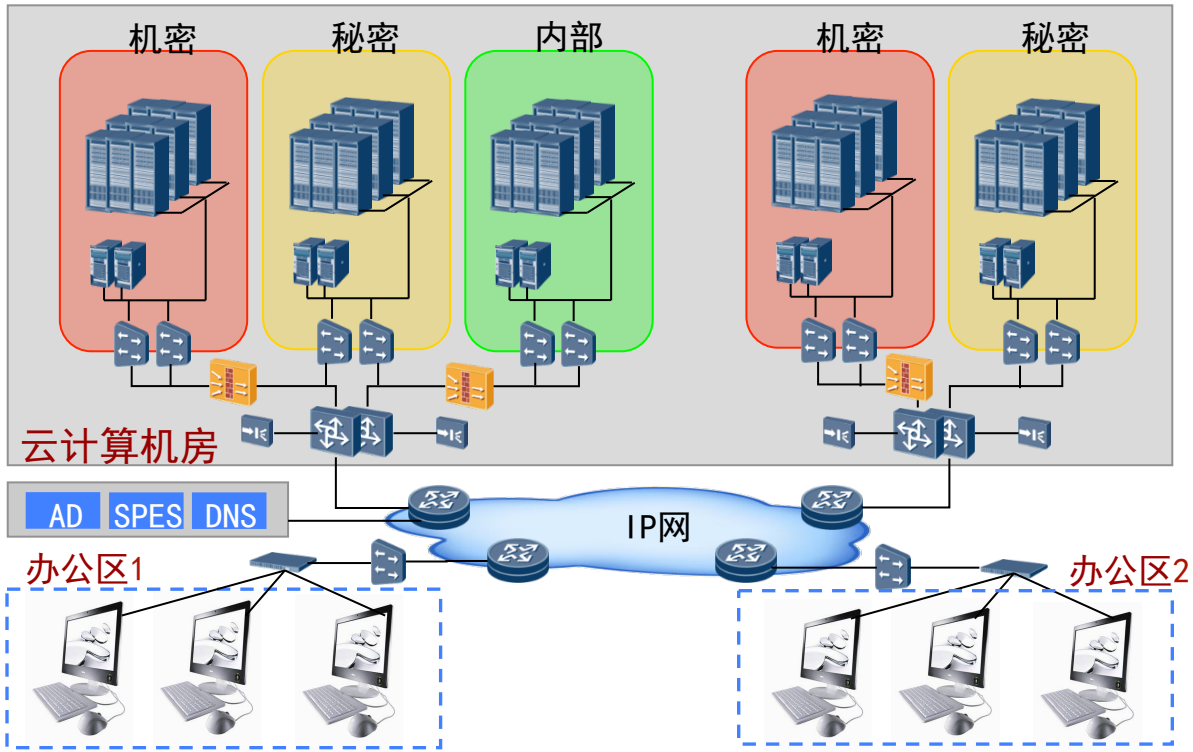
安全管理平台以资产为核心，以安全事件管理为关键流程，
采用安全域划分的思想，建立一套实时的资产风险模型



统一的监控界面

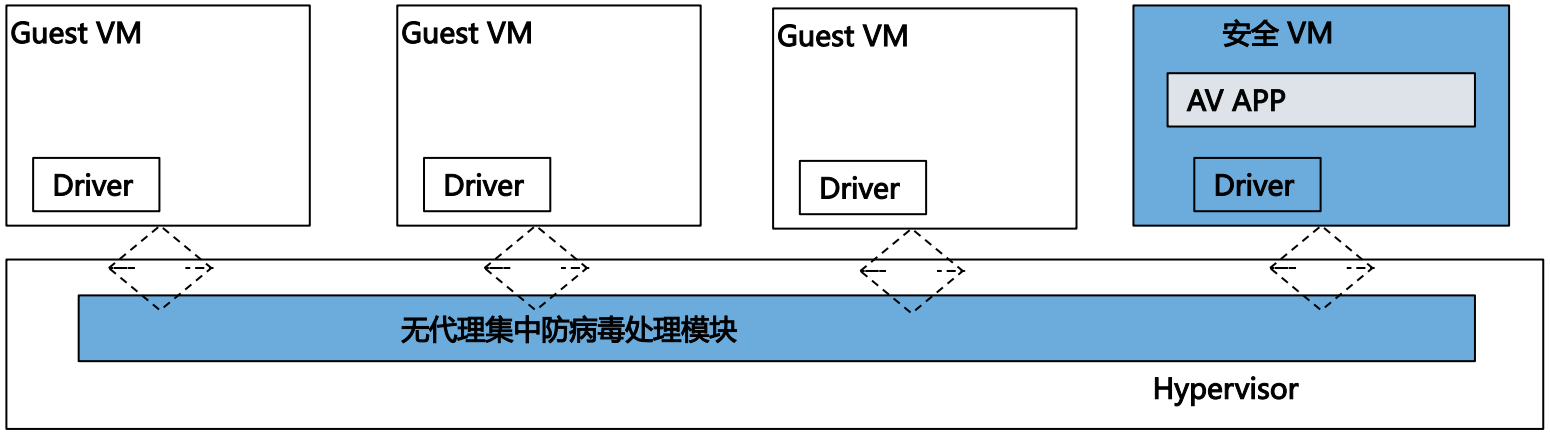
5. 数据安全--按密级分区隔离

- 机密\秘密：计算存储资源配置了专用的硬件设施，杜绝不同密级混用
- 不同密级或部门之间采用通过平面隔离，租户VLAN隔离，IP安全组以及虚拟机防止地址欺骗和嗅探等手段实现安全，避免威胁扩散

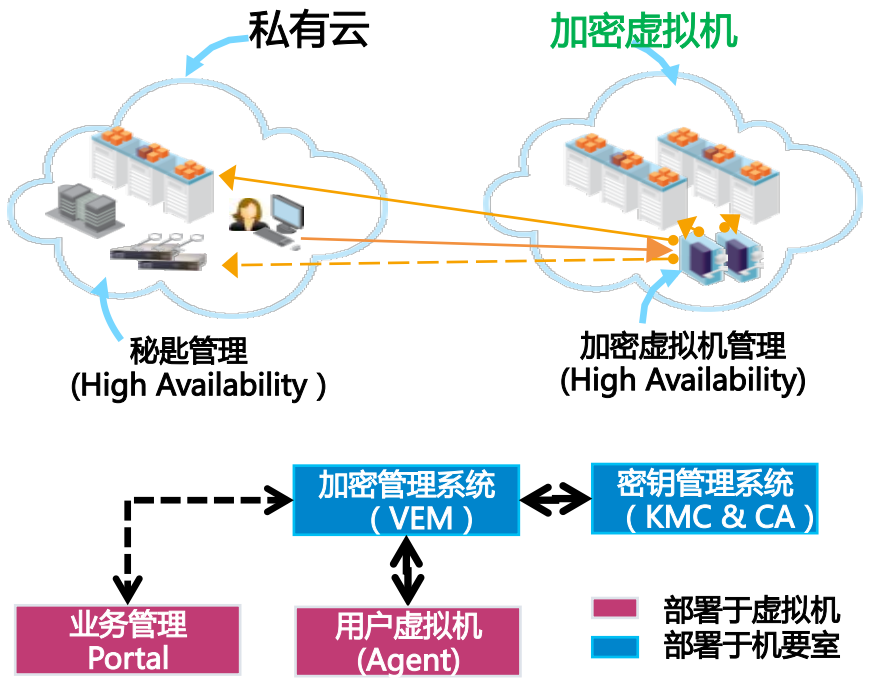


5. 数据安全--虚拟化防病毒

- 一个物理服务器上只在一个独立虚拟机上安装一个防病毒引擎，对所有的用户虚拟机进行防护，用户虚拟机无需安装防病毒引擎。
- 避免杀毒风暴，提升用户体验。
- 支持瑞星，趋势等。



5. 数据安全--虚拟机磁盘加密



技术特点

- **虚拟磁盘加密**

  对系统卷、数据卷进行全盘的加密，对上层应用程序透明

- **集中管理**

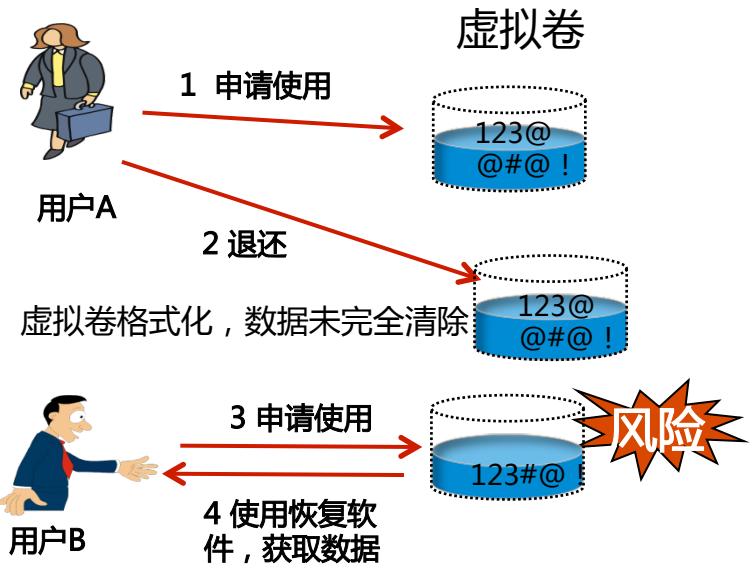
  部署集中管理服务器，对客户端进行统一的策略管理和维护

- **加密硬件加速**

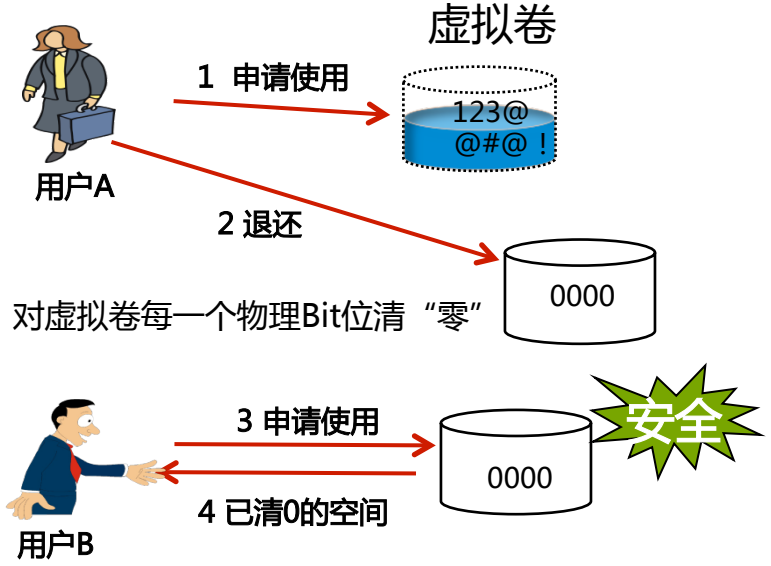
  基于CPU硬件加密指令，**性能损失<10%**

虚拟机磁盘加密，得到数据也很难破解

5. 数据安全--安全删除虚拟机

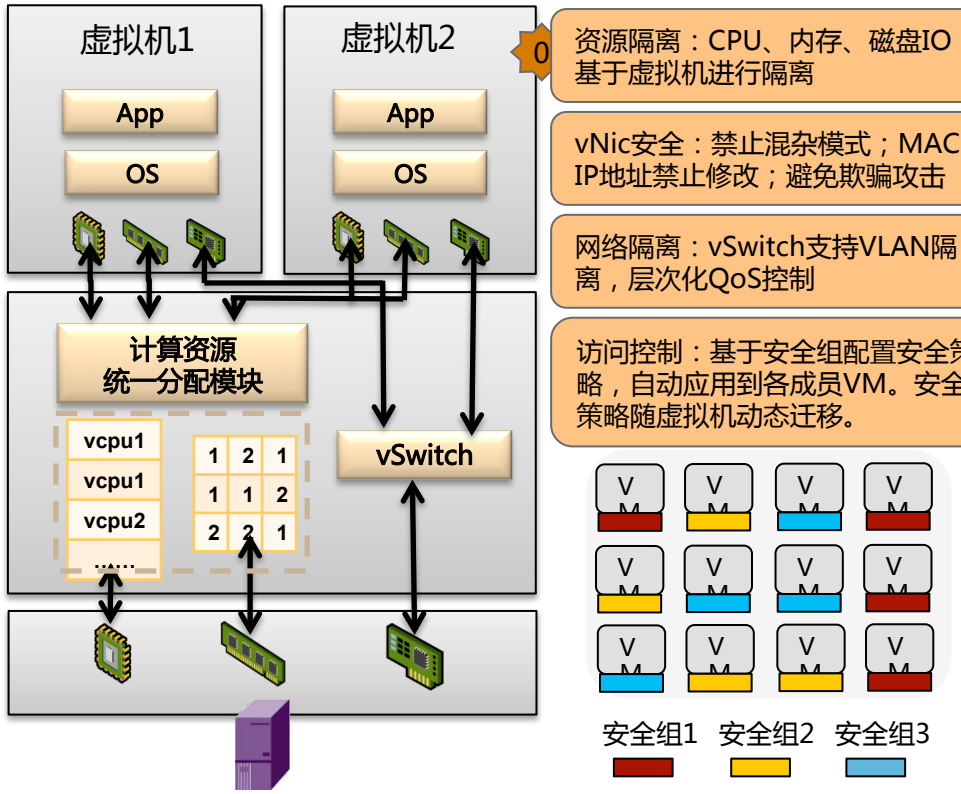


普通模式：
虚拟卷通过格式化方式清除数据，不彻底，可恢复，存在信息泄漏风险



安全模式：
对销户虚拟卷采用物理Bit清零措施，确保数据不可恢复，杜绝信息泄漏风险

6. 平台安全--层次化安全防护



0 资源隔离：CPU、内存、磁盘IO基于虚拟机进行隔离

vNic安全：禁止混杂模式；MAC、IP地址禁止修改；避免欺骗攻击

网络隔离：vSwitch支持VLAN隔离，层次化QoS控制

访问控制：基于安全组配置安全策略，自动应用到各成员VM。安全策略随虚拟机动态迁移。

特点：层次化的安全防护

基础设施隔离：管理平面、存储平面、业务平面物理网络隔离。

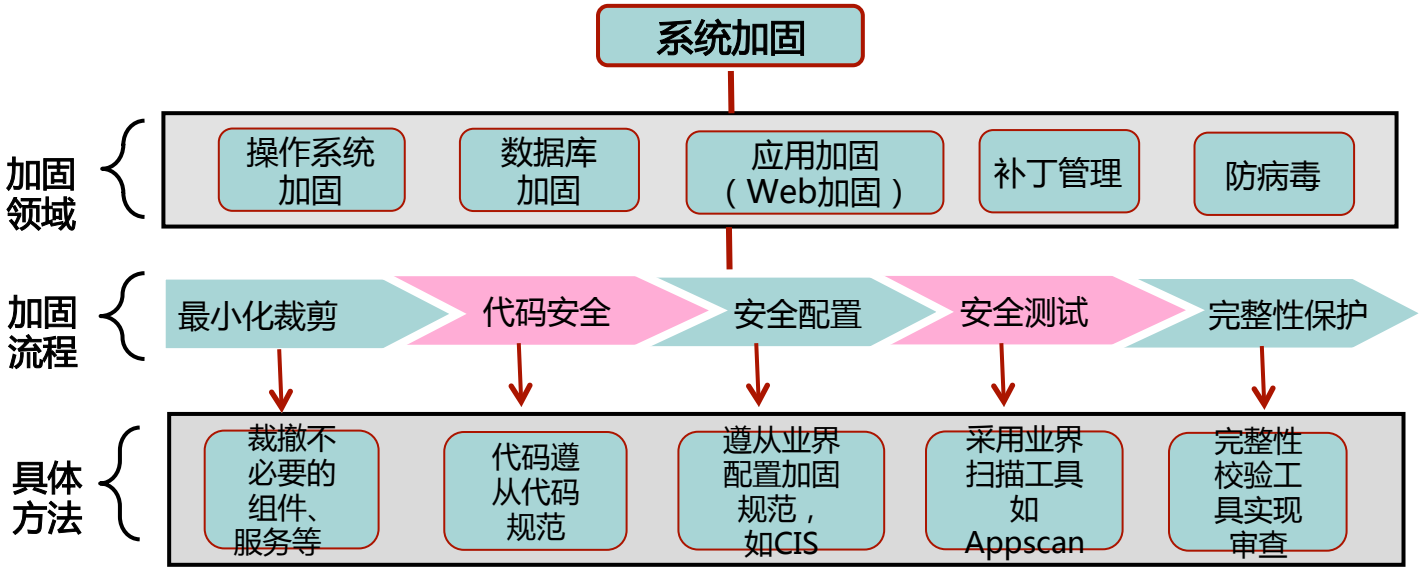
虚拟化边界隔离：通过虚拟化防火墙实现数据中心的边界隔离和访问控制。提供ACL、Anti-DoS、IPsec VPN等功能。

虚拟化资源隔离：虚拟机之间通过VLAN实现二层隔离，通过安全组实现三层隔离和访问控制。VM IP和MAC绑定，防止ARP欺骗攻击。

价值

- 提供虚拟机级别的访问控制手段，避免病毒、威胁在不同租户间扩散，防止威胁蔓延
- 智能、弹性安全防护，VM漂移、扩容无需人工配置安全策略

6. 平台安全--系统加固



- 由于软件存在bug，在安全上就可能引起相应的漏洞，通过对操作系统、数据库、应用的加固以及补丁管理，可以修补这些漏洞
- 通过严格的服务裁剪、网络端口扫描、操作权限及访问控制等措施，保证主机平台对外安全可靠

八大安全体系

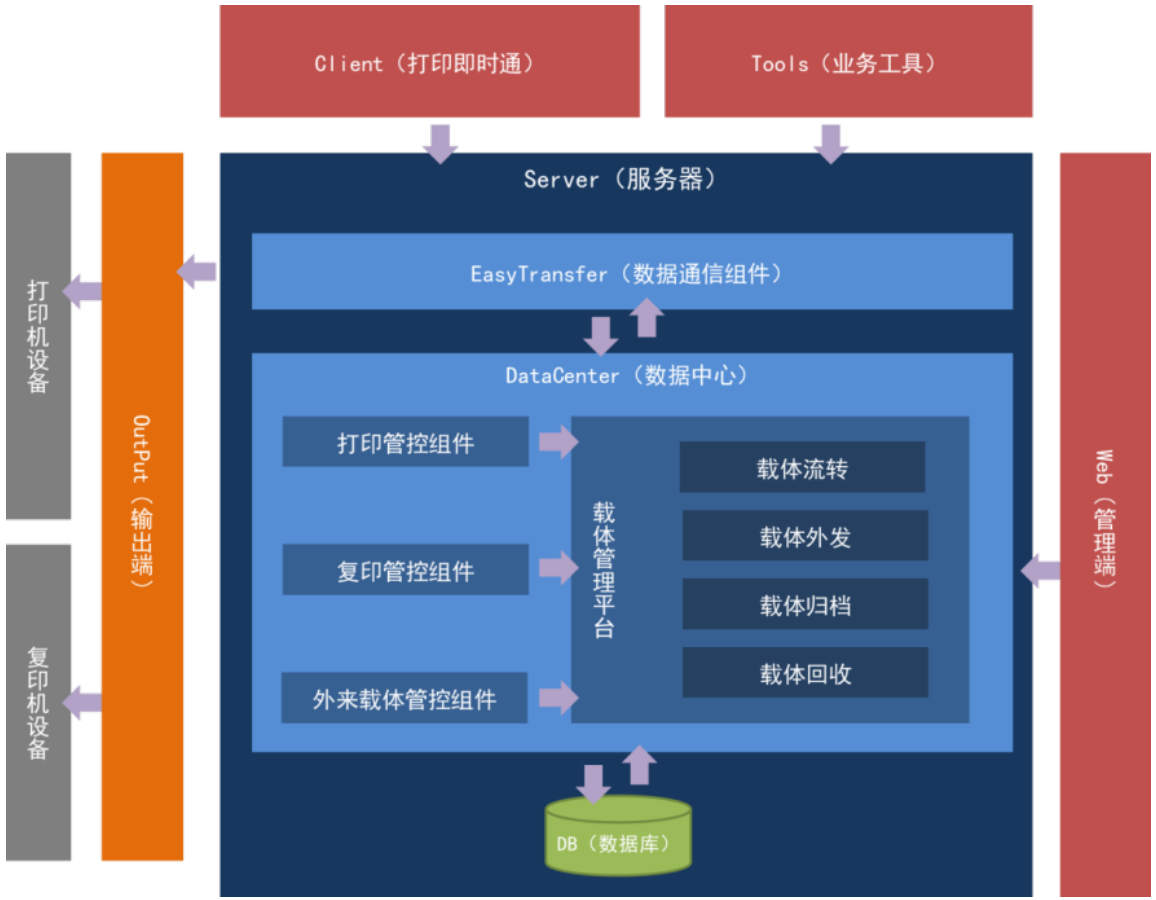
7. 应用安全

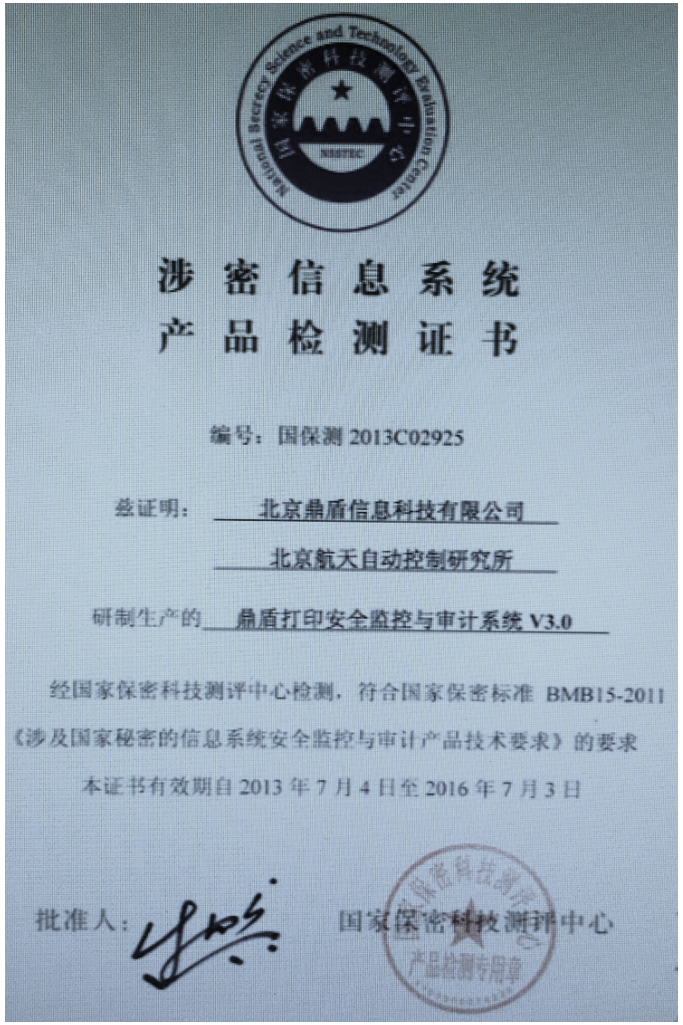
- **数据安全管控无死角：**
  - 载体管控，涉密实物，电子文档；
  - 过程管控：实物、电子资料全生命周期管控；
  - 域内域外：通过透明加密实现文档内部域以及外部域的管控。

八大安全体系

实物涉密载体管理及打印审计系统

- 系统以数据中心作为核心业务处理平台，以打印管控、复印管控及外来载体管控三个模块作为载体信息主要搜集渠道；
- 以二维条码作为主要的载体识别手段，由载体流转、载体归档、载体外发、载体回收四个载体管理业务构建载体管理平台。





涉密信息系统
产品检测证书

编号：国保测 2013C02925

兹证明：北京鼎盾信息科技有限公司
北京航天自动控制研究所

研制生产的 鼎盾打印安全监控与审计系统 V3.0

经国家保密科技测评中心检测，符合国家保密标准 BMB15-2011
《涉及国家秘密的信息系统安全监控与审计产品技术要求》的要求

本证书有效期自 2013 年 7 月 4 日至 2016 年 7 月 3 日

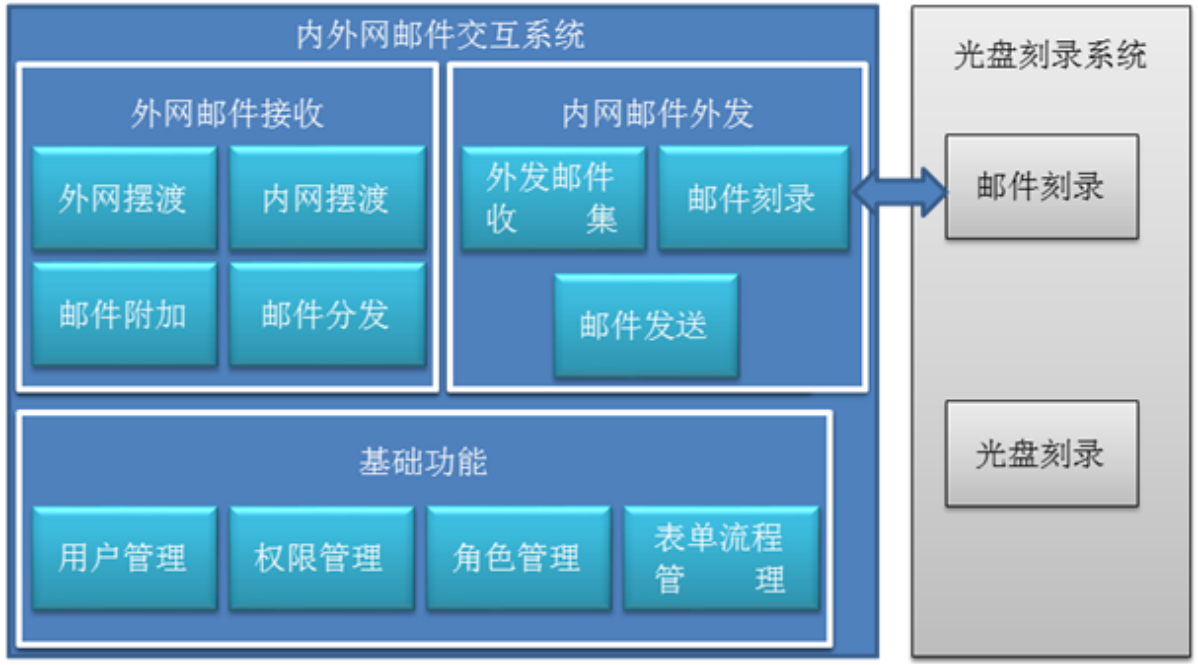
批准人：

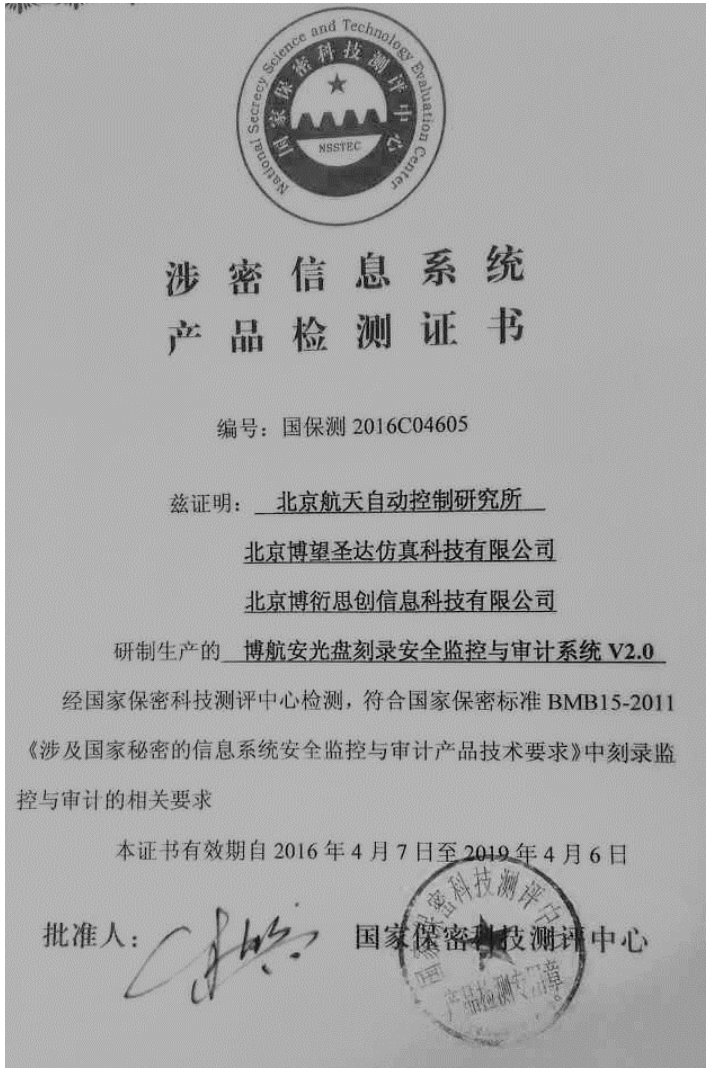
国家保密科技测评中心

八大安全体系

内外网邮件交换系统

- 自助刻录光盘规避人为因素干扰；
- 强化非密导出信息的把关，由保密处或专家审批；
- 自动匹配导入信息审批，匹配成功则自动发送邮件，减少人工操作。





涉密信息系统
产品检测证书

编号：国保测 2016C04605

兹证明：北京航天自动控制研究所
北京博望圣达仿真科技有限公司
北京博衍思创信息科技有限公司

研制生产的博航安光盘刻录安全监控与审计系统 V2.0

经国家保密科技测评中心检测，符合国家保密标准 BMB15-2011《涉及国家秘密的信息系统安全监控与审计产品技术要求》中刻录监控与审计的相关要求

本证书有效期自 2016 年 4 月 7 日至 2019 年 4 月 6 日

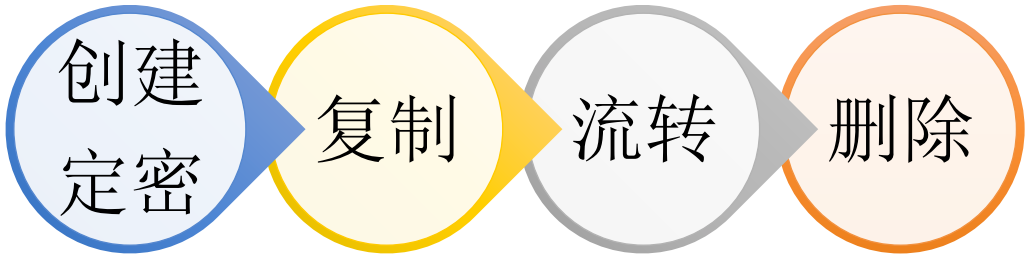
批准人：

国家保密科技测评中心

八大安全体系

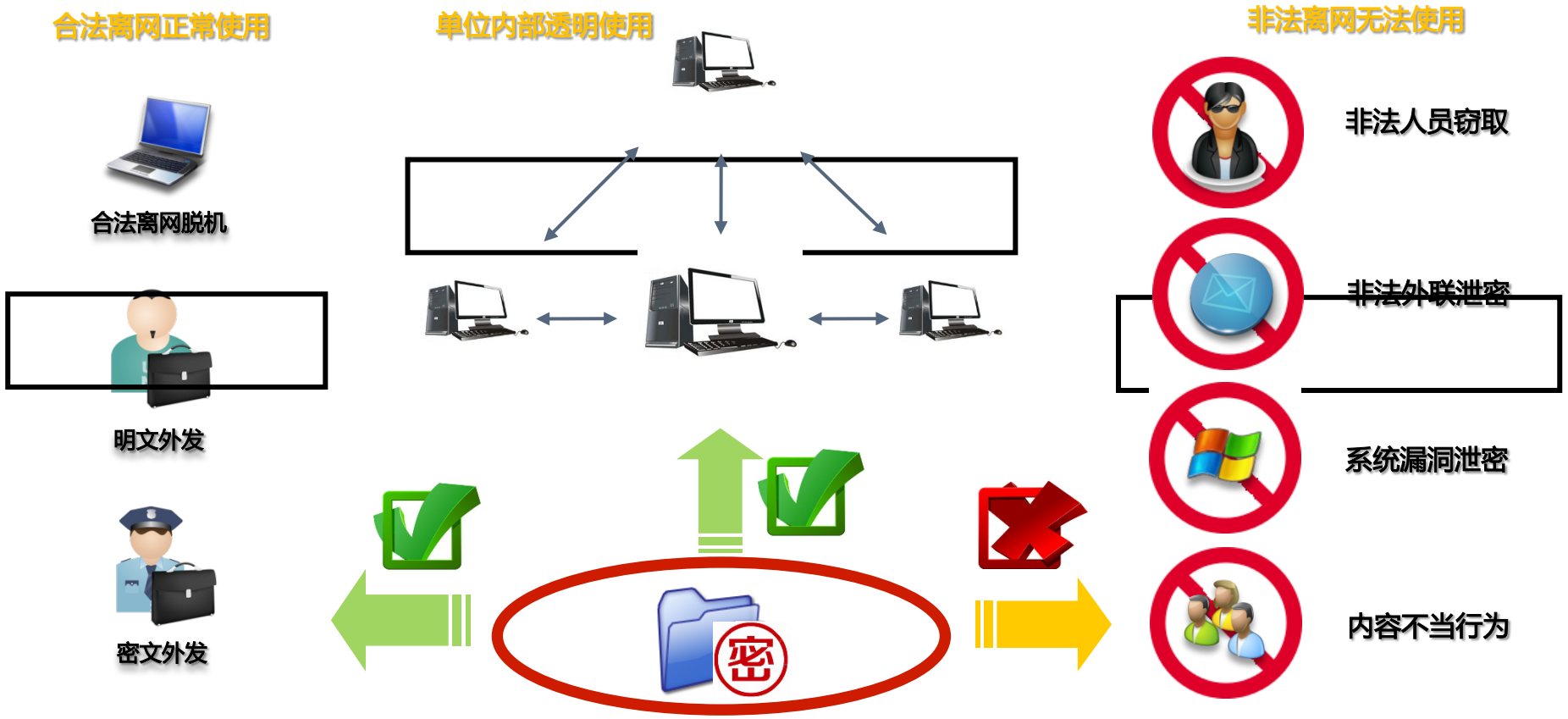
电子文档管控与行为审计系统

实现员工终端指定电子文档类型的全生命周期的监控，操作时间，应用名称，文档名称（全路径），文档的操作类型、秘级信息，文档大小，用户信息，终端地址，时间戳，并且将操作日志发送到指定的服务器进行保存。



八大安全体系

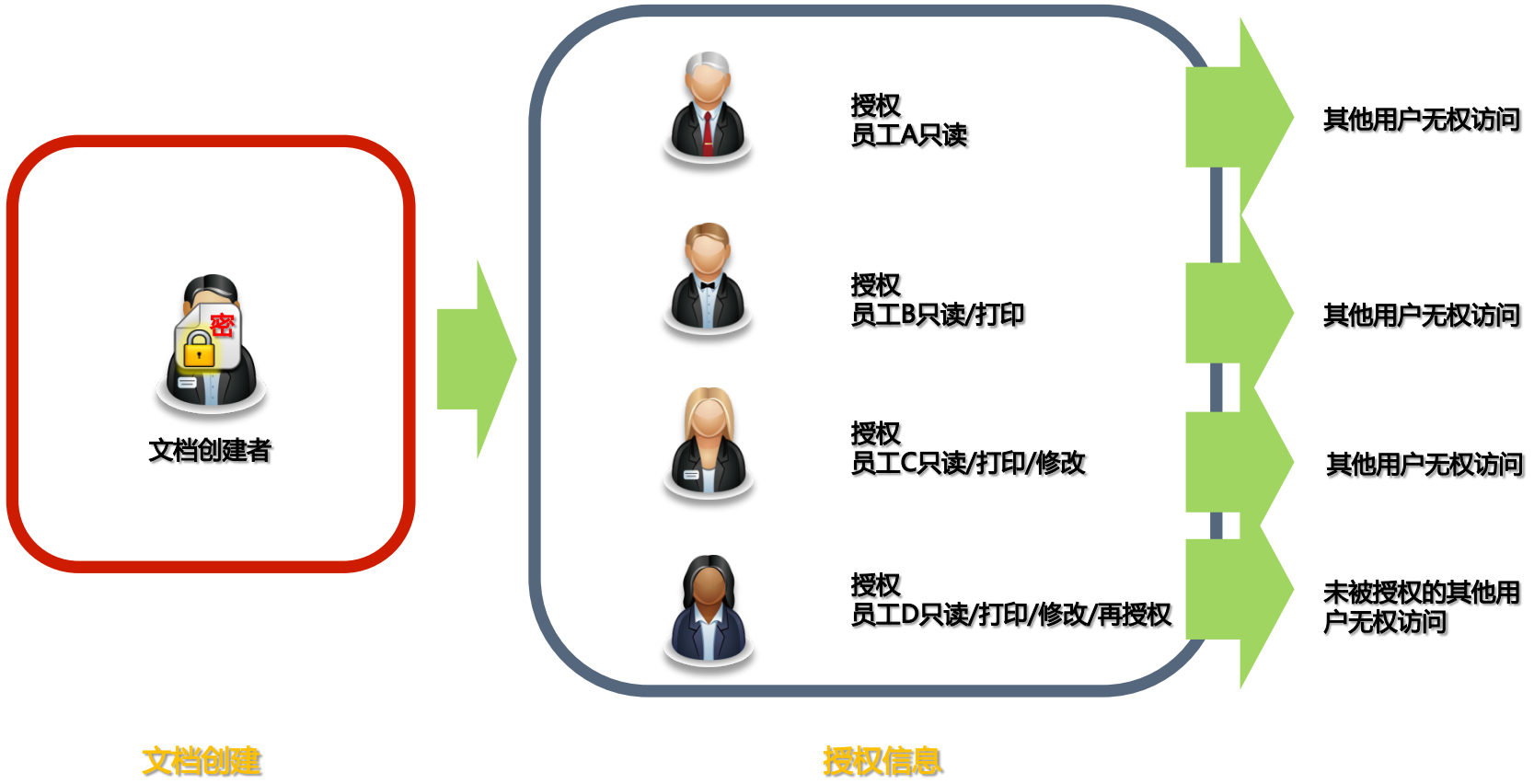
电子文档透明加密



在涉密文档开始创建时即被动态透明加密保护，内部协同办公可任意使用，脱离保护环境将密文呈现！

八大安全体系

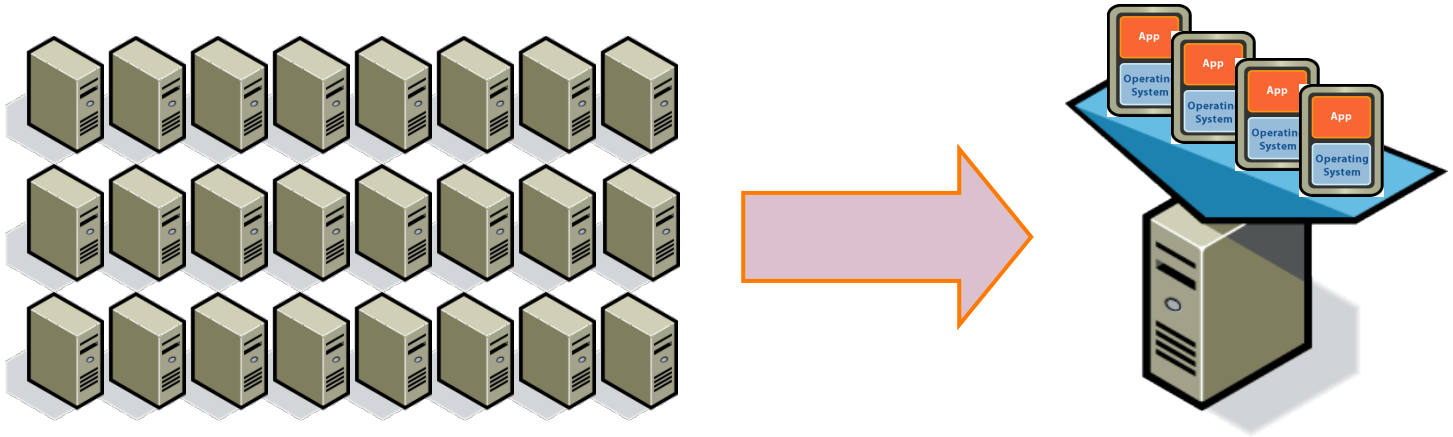
电子文档分级授权 对内部文档进行细粒化授权管理！



与透明加密混合使用，可达到文档创建到流转的全过程加密及分权限处理！

八大安全体系

实物载体管理及打印审计
内外网邮件交换
电子文档管控与行为审计
电子文档透明加密
OA、邮件等其他服务器应用



借助华为虚拟化技术，可以统筹考虑虚拟办公桌面以及各种服务器应用的计算和存储资源需求，借助终端安全管控以及航天大道云安全解决方案，在云计算环境中提供信息安全一站式服务。

八大安全体系

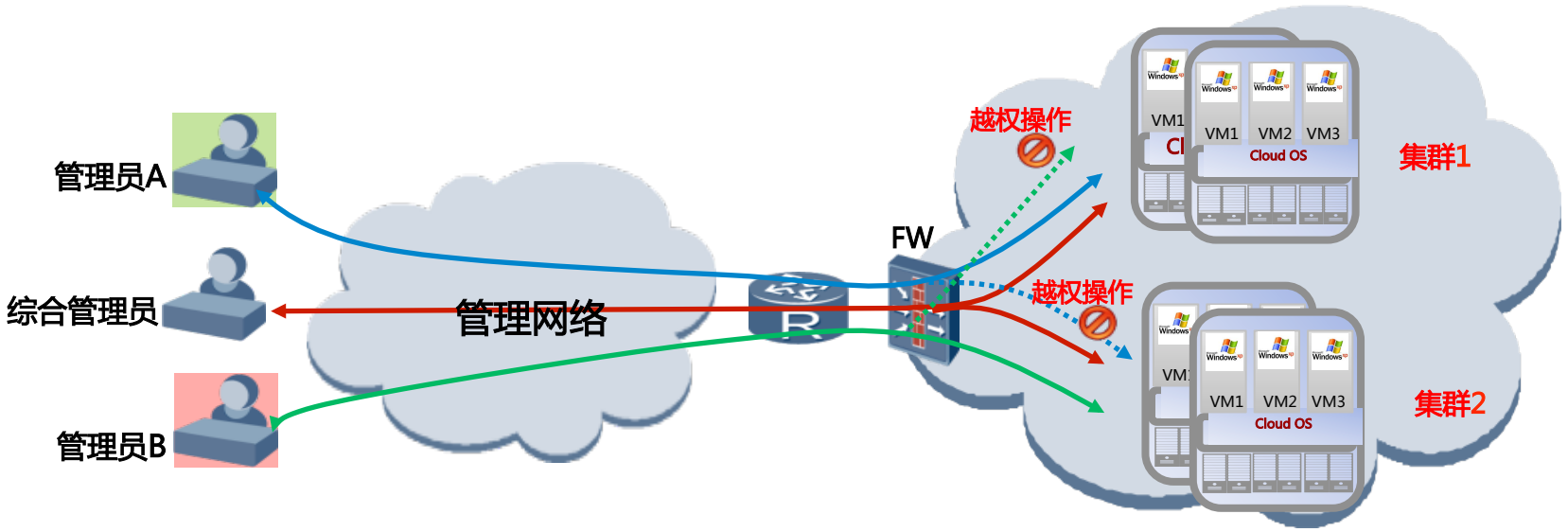
8. 管理安全--支持“三员分立”

- **技术特点**
  - ✓ 三员分立，权限由系统管理员、安全管理员、安全审计员分摊(无超级管理员)。管理员间的权限应相互制约、互相监督，避免由于权限过于集中带来的安全风险。
  - ✓ “三员分立”机制需在系统安装时指定，否则依然采用传统的超级管理员模式。

- **应用场景**

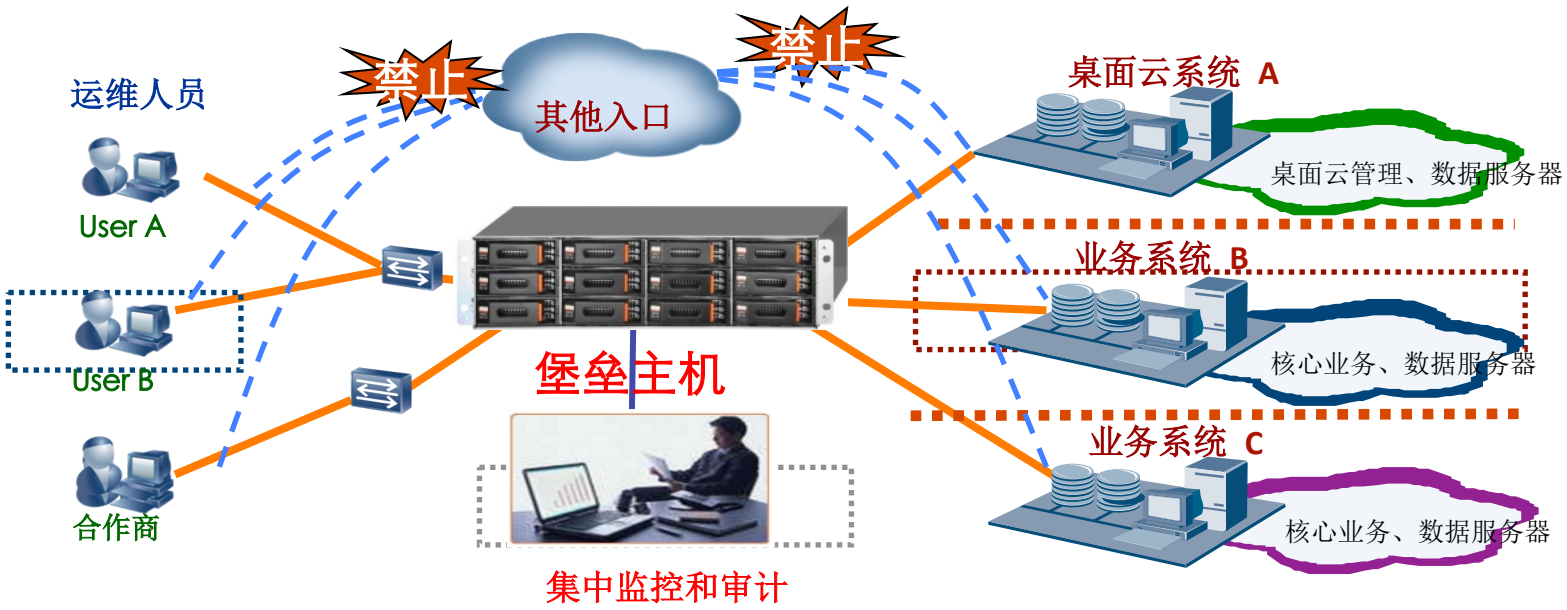
✓ 满足国内涉密安全应用场景。分级保护标准BMB17中明确规定，系统要支持三员分立的管理。即实现系统管理员、安全管理员、安全审计员的权限制衡。

8. 管理安全--分权分域管理



支持分权分域管理，防止越权管理

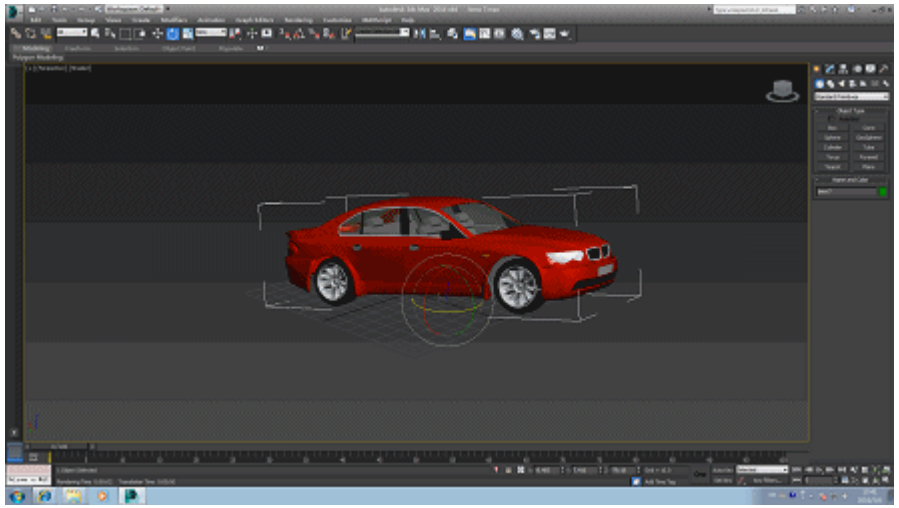
8. 管理安全--堡垒主机

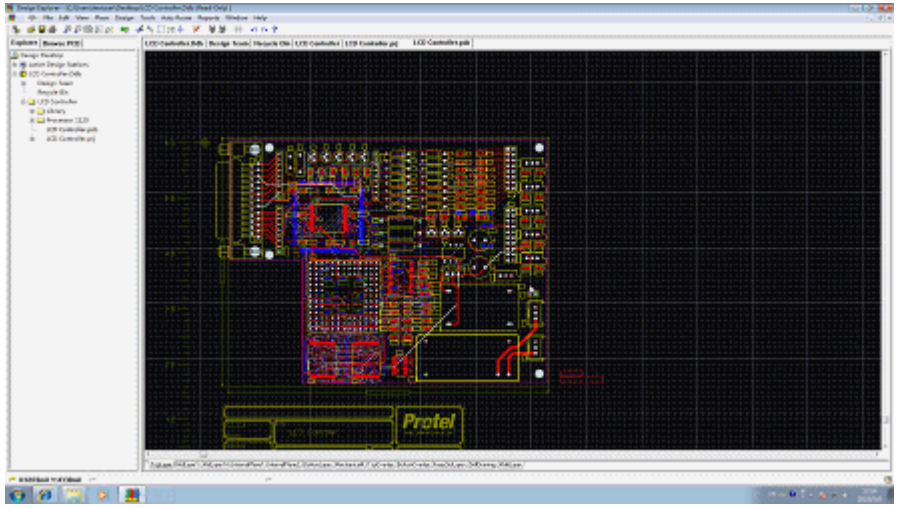


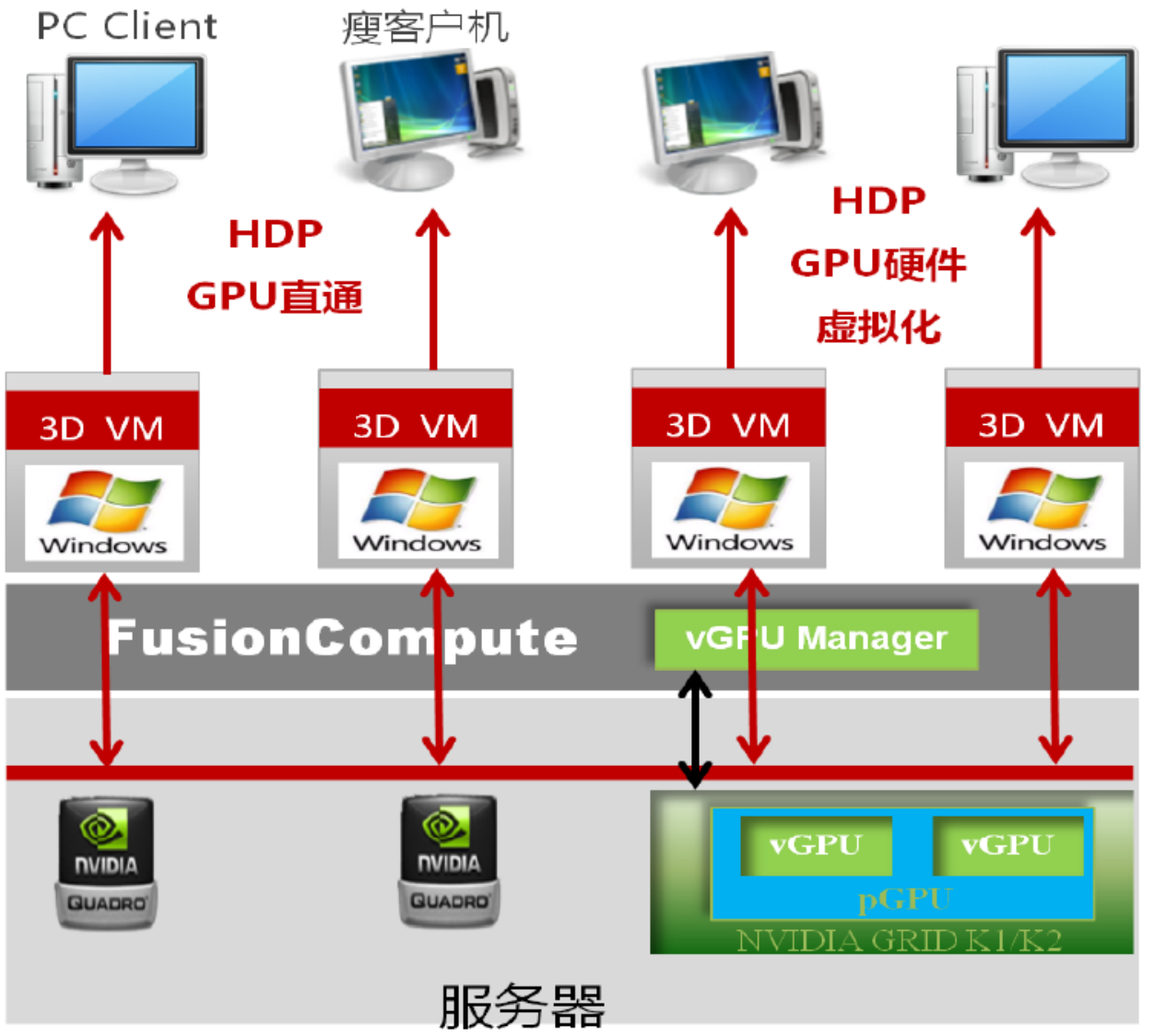
- 统一数据中心的管理入口；
- 完善的日志审计，支持对图形终端、字符终端、数据库应用、文件传输等。 提供实时视频监控录屏，对高危的操作（删除或重启等）可以实时的截断；
- 可进行集中的用户管理、单点登录、密码定时更新等。

DaoCloud产品特点：卓越体验

DaoCloud卓越体验



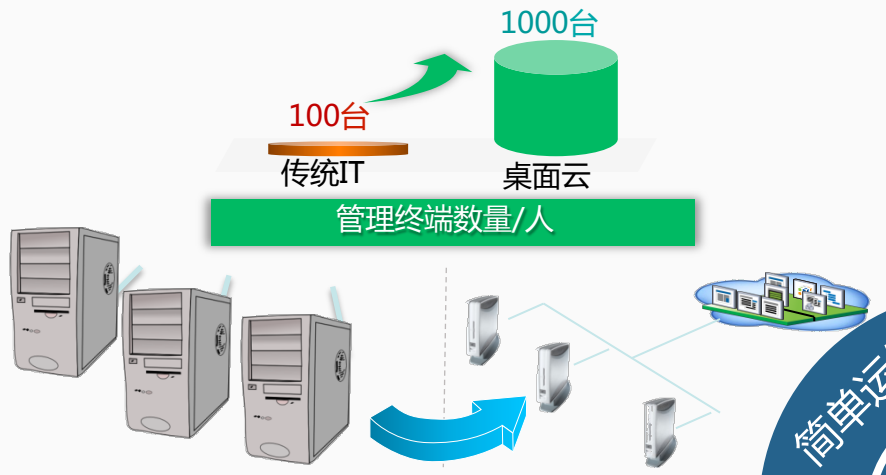


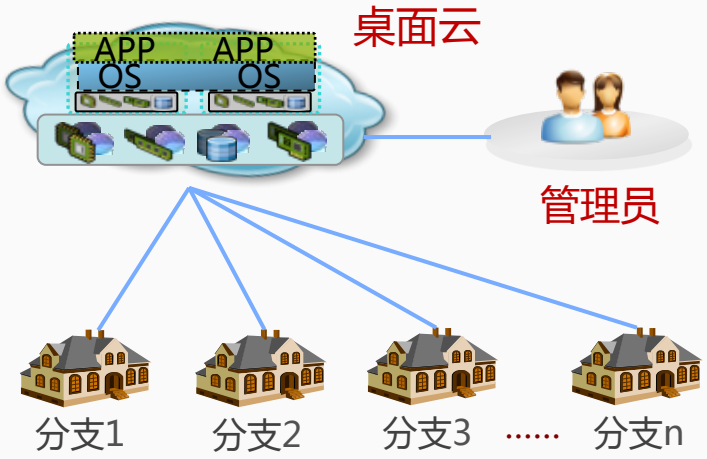


DaoCloud产品特点：敏捷高效

DaoCloud敏捷高效：运维高效，便捷管理

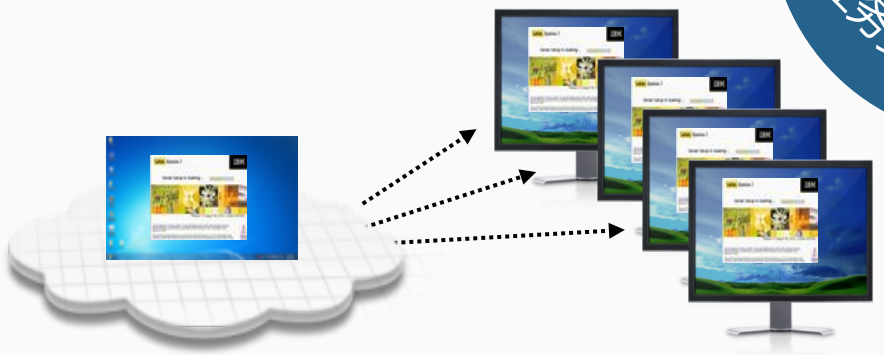
统一运维 高效管理

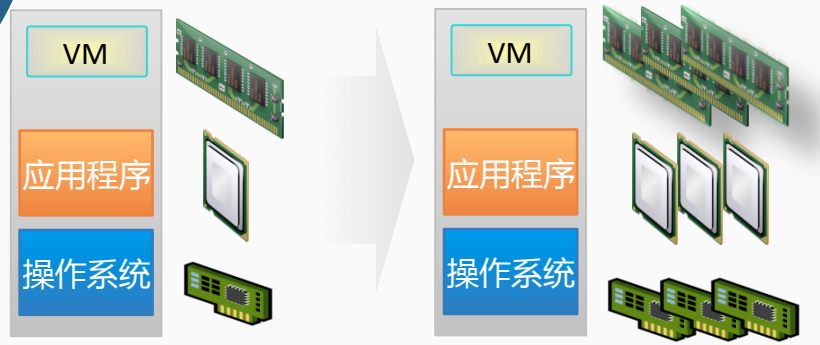




终端免维护 集中管理

快速批量发放





灵活升级 动态调整


聚焦数据与智能
持续为客户创造价值
智慧产业项目部感谢您的支持！