

**RSA[®]CONFERENCE
C H I N A 2012
RSA信息安全大会2012**

**THE GREAT CIPHER
MIGHTIER THAN THE SWORD
伟大的密码胜于利剑**



终端虚拟化重塑企业网络安全壁垒

----终端数据安全保护的实践分享

殷浩

深信服科技 市场技术总监

yin-hao@sangfor.com



RSA CONFERENCE
C H I N A 2012
RSA信息安全大会2012

不平凡的2012、2011。

■ 各种企业数据安全泄密事件层出不穷

[CSDN泄密门 互动百科](#)

www.hudong.com

[CSDN泄密门-20](#)

及邮箱遭到泄漏

简介 - 干扰实名

[破解CSDN泄](#)

www.enet.com.cn

2012年1月31日 -

门"事件逐渐接近

[多家网站卷入](#)



关于"CSDN泄密"

[多家网站卷入 CSDN泄密事件](#)

www.chinanews.com/fi/2011/12-23/3

[银行数据外泄的新闻搜索结果](#)



[【深度·悦读】个人隐私贩卖渐成产业谁来保护个人信息？ -浙江在线 ...](#)

zjnews.zjol.com.cn/05zjnews/.../018649482.shtml - 网页快照

2012年7月13日 - 【深度·悦读】个人隐私贩卖渐成产业谁来保护个人信息？ ... IT男网

络贩卖个人信息二手转卖每个个人信息赚25块钱. 舒、吴交代，知道阿俊的游戏账户 ...

[跟人隐私贩卖的新闻搜索结果](#)

finance.qq.com

[个人信息变成人名大全网站牟利的工具](#)

[和讯网 - 6 小时前](#)

个人信息被“卖”令人不胜其烦，涉及到个人隐私的信息被人像萝卜、白菜一样“论斤”卖掉，无疑是信息化时代的“贩卖人口”。个人信息被叫卖，原因是 ...

[“个人信息”缘何能成网站牟利的“肉鸡”](#)

[南方网 - 1 天前](#)

[醉江南：“个人信息”缘何能成网站牟利的“肉鸡”](#)

[荆楚网 - 1 天前](#)

[“个人信息”缘何能成网站牟利的“肉鸡”](#)

hlj.rednet.cn , 红辣椒频道 - 网页快照 分享

2 days ago - 个人信息被“卖”令人不胜其烦，涉及到个人隐私的信息被人像萝卜、白菜一

>>

分享：企业终端风险防范的实践经验



SANGFOR
深信服科技

目录

- 企业安全风险的变化
 - 业务环境更加恶劣
 - 传统应对手段的问题
- 虚拟化技术----业务安全的新选择？
- 沙盒技术的实践及演进



企业应用、终端更加多样

RSACONFERENCE
C H I N A 2012



SANGFOR
深信服科技

终端数据更高价值

RSACONFERENCE
C H I N A 2012

行业

制造业

政府和军队

金融、电信机构

咨询型企业

设计类机构

各行业主要保护的对象

- 设计图纸、价格体系、商业计划、客户资料、合同订单.....
- 公文、统计数据、机要文件、军事情报、军事地图、作战方案.....
- 交易数据、融资投资信息、大客户信息、上市公司年报.....
- 咨询报告、招投标文件、专利、客户资料、价格.....
- 设计图、设计方案、专利、策划方案、客户信息、软件程序.....

无法想象这些数据被泄密的后果



SANGFOR
深信服科技

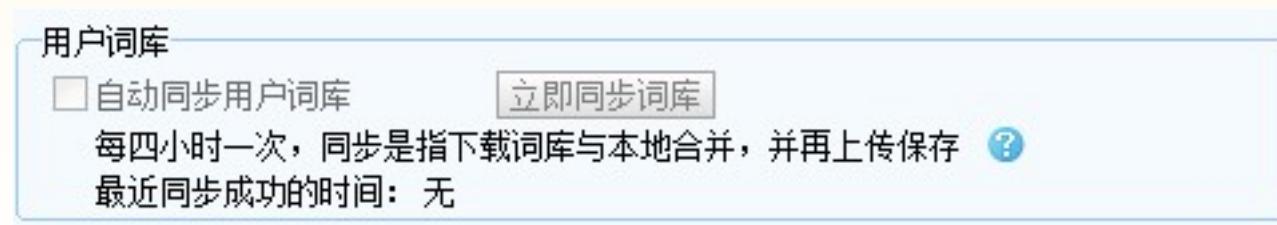
黑客手段更加高明

- 从大张旗鼓 到偃旗息鼓
- 定向的APT攻击
- 数据泄密实例：

序号	时间	URL/目录	源IP	目的IP	描述	严重等级	详细
1	2011-12-18 23:56:33	http://inf.../single/detail.aspx?c...207	246.166	246.166	DLP_Policy/PhoneNumber_50_Times content:00 <	高	查看
2	2011-12-18 23:41:08	http://inf.../single/detail.aspx?c...53.158	246.166	246.166	DLP_Policy/PhoneNumber_50_Times content:	高	查看
3	2011-12-18 22:35:19	http://inf.../single/detail.aspx?c...182	224.197	224.197	DLP_Policy/PhoneNumber_50_Times content:综合:	高	查看
4	2011-12-18 22:16:20	http://inf.../detail.aspx?channel=...140	246.166	246.166	DLP_Policy/ID_Card_50_times content:74 蒋...	高	查看
5	2011-12-18 21:59:20	http://inf.../stepshop/steps...211	224.210	224.210	DLP_Policy/PhoneNumber_50_Times content:ascr	高	查看
6	2011-12-18 21:59:17	http://inf.../single/detail.aspx?t...161	224.197	224.197	DLP_Policy/Secret_KeyWord_50Times content:贵...	高	查看
7	2011-12-18 21:36:36	http://inf.../detail.aspx?topic=frx&i...70.68	224.210	224.210	DLP_Policy/Email_50Times content:	高	查看
8	2011-12-18 20:10:44	http://inf...					
9	2011-12-18 19:24:55	http://inf..._DLP_Policy/ID_Card_50_times content:74 蒋...					
10	2011-12-18 18:22:49	http://inf...					
11	2011-12-18 17:23:34	http://inf.../detail.aspx?id=265558	249.213	224.210	DLP_Policy/Email_50Times content:	高	查看
12	2011-12-18 14:29:18	http://inf.../single/detail.aspx?c...108.169	246.197	246.197	DLP_Policy/PhoneNumber_50_Times content:92-2:	高	查看
13	2011-12-18 14:01:58	http://inf.../single/detail.aspx?c...61.120	246.166	246.166	DLP_Policy/PhoneNumber_50_Times content: 21	高	查看
14	2011-12-18 13:41:40	http://inf.../detail.aspx?id=ne02	70.68	224.197	DLP_Policy/Email_50Times content:讯资讯中心:	高	查看
15	2011-12-18 13:40:02	http://inf.../single/detail.aspx?c...108.90	224.197	224.197	DLP_Policy/PhoneNumber_50_Times content:00 <	高	查看
16	2011-12-18 13:34:17	http://inf.../detail.aspx?topic=frx&i...70.68	224.210	224.210	DLP_Policy/Email_50Times content:	高	查看
17	2011-12-18 13:28:12	http://inf.../single/detail.aspx?id=ne02	134.67	224.197	DLP_Policy/Email_50Times content:讯资讯中心:	高	查看
18	2011-12-18 13:22:23	http://m.../stepshop/steps...113.76	246.181	246.181	DLP_Policy/PhoneNumber_50_Times content:ss="	高	查看
19	2011-12-18 13:22:12	http://m.../stepshop/steps...213.76	246.181	246.181	DLP_Policy/PhoneNumber_50_Times content:ascr	高	查看
20	2011-12-18 13:14:15	http://inf.../detail.aspx?id=206232&t...249.213	224.210	224.210	DLP_Policy/Email_50Times content:	高	查看

“云”让泄密渠道更多

- 某些输入法---自动上传本地个性化字库



- 各种网盘---文件数据随意共享

The screenshot shows a cloud storage interface. On the left, there are icons for "圈子" (Circle) and "网盘" (Cloud Disk). The "网盘" section is highlighted with a blue bar containing the text "数据放在了云端就更安全了吗？" (Is it safer to store data in the cloud?). Below this, a list of files is shown:

文件名	类型	日期	大小	操作
FY12Q2销售业绩分析.docx	DOC	2012-08-28	6.06MB	分享 下载
VIP客户名单整理20120722.xlsx	XLS	2012-08-28	21.02KB	分享 下载
2012商业政府主要市场机会点及典型案例-改.pptx	PPT	2012-08-28	1.77MB	分享 下载



SANGFOR
深信服科技

传统防止数据外泄的基本思路

阻断数据外泄通道

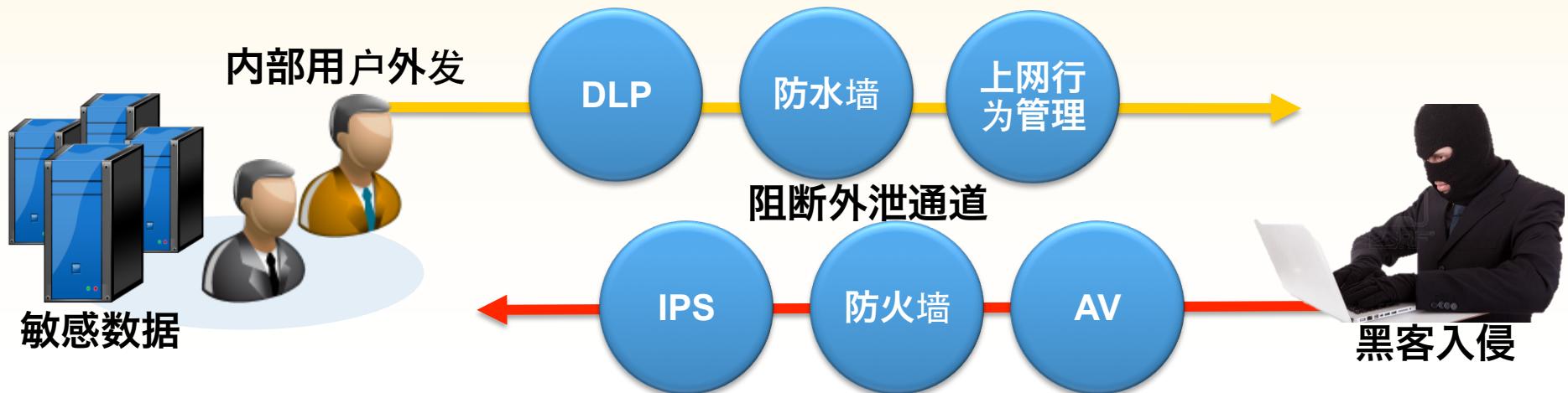


控制数据内容权限



SANGFOR
深信服科技

传统方案—阻断外泄通道



核心技术：

- 基于特征的比对，识别入侵行为/敏感信息

缺点：

- 在数据内容匹配上有一定的误判率
- 部署实施过程较为复杂，用户接受程度弱



SANGFOR
深信服科技

传统方案--控制数据内容权限

RSACONFERENCE
C H I N A 2012



SANGFOR
深信服科技

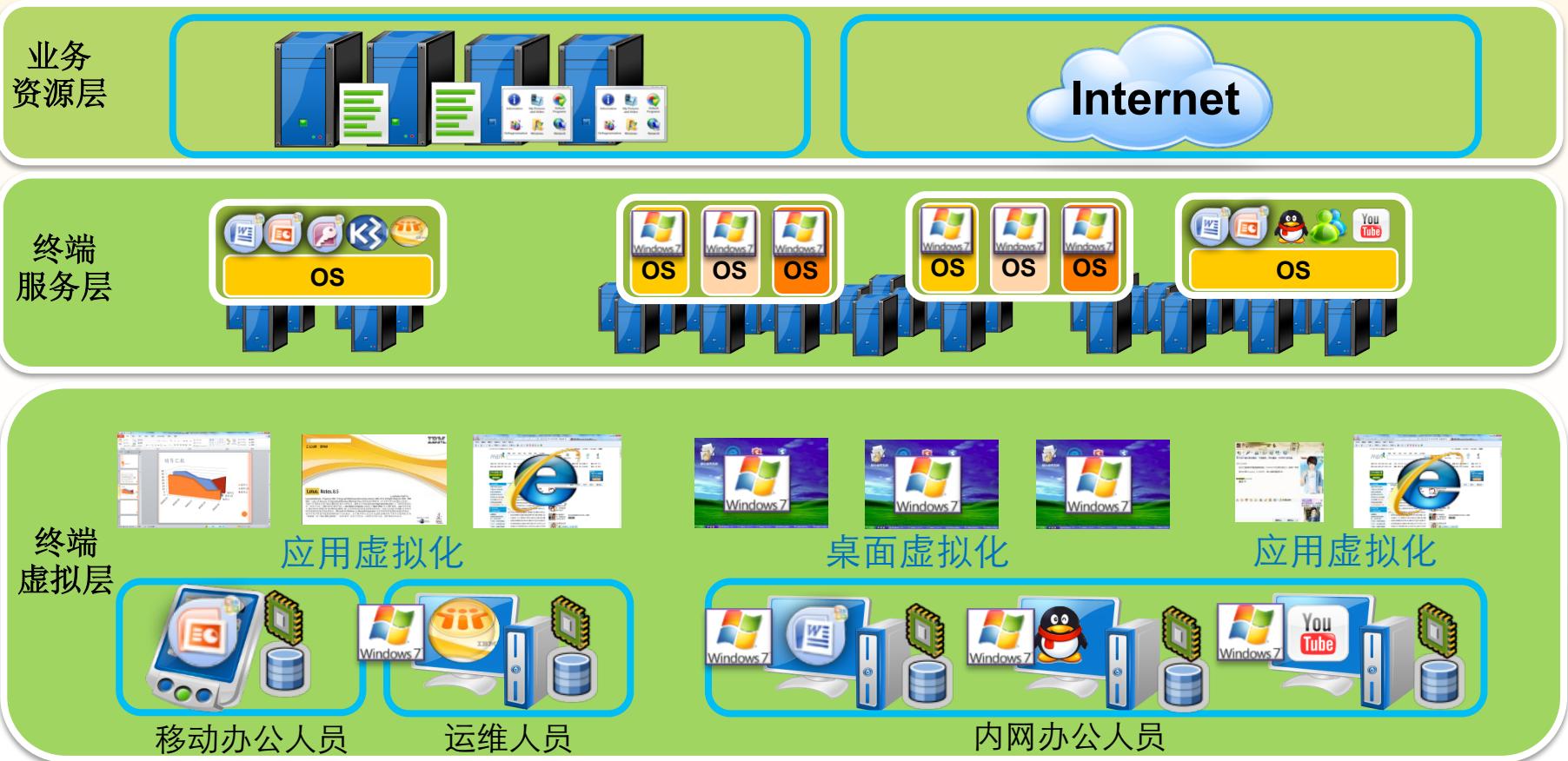
目录

- 业务安全风险的变化
- 虚拟化技术----业务安全的新选择？
 - 桌面/应用虚拟化技术的安全价值
 - 新的终端虚拟化技术---安全沙盒
- 沙盒技术的实践及演进



应用/桌面虚拟化：安全的“新的选择”？

RSACONFERENCE
C H I N A 2012



- 集中化：计算、存储、应用、系统等资源集中化部署
- 虚拟发布：对终端发布虚拟的应用/桌面图像
- 优势：集中管理，简化运维

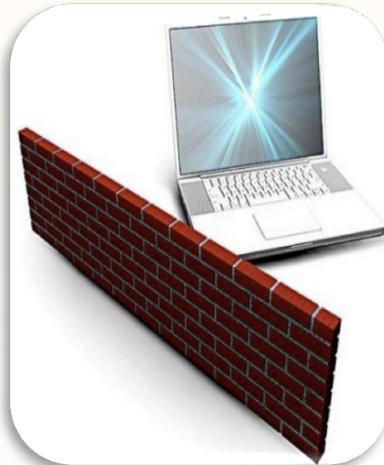


SANGFOR
深信服科技

RSA信息安全大会2012

桌面/应用虚拟化技术的安全价值

RSACONFERENCE
C H I N A 2012



多业务安全隔离

数据集中管理
数据防泄密

- 应用虚拟化更加适合：小规模、网络质量较低、应用单一的业务、跨平台部署的场景，如移动终端接入等



SANGFOR
深信服科技

RSA信息安全大会2012

桌面/应用虚拟化现阶段的问题

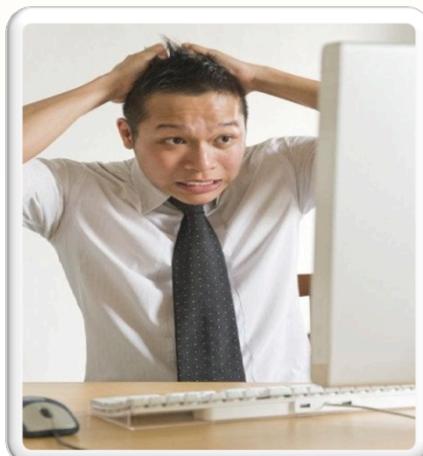
RSACONFERENCE
C H I N A 2012

成本高



1-1.2万/每用户

体验有
待改善



数据迁移
离线环境

组织架构
能否支撑



分散到集中
无法一步到位

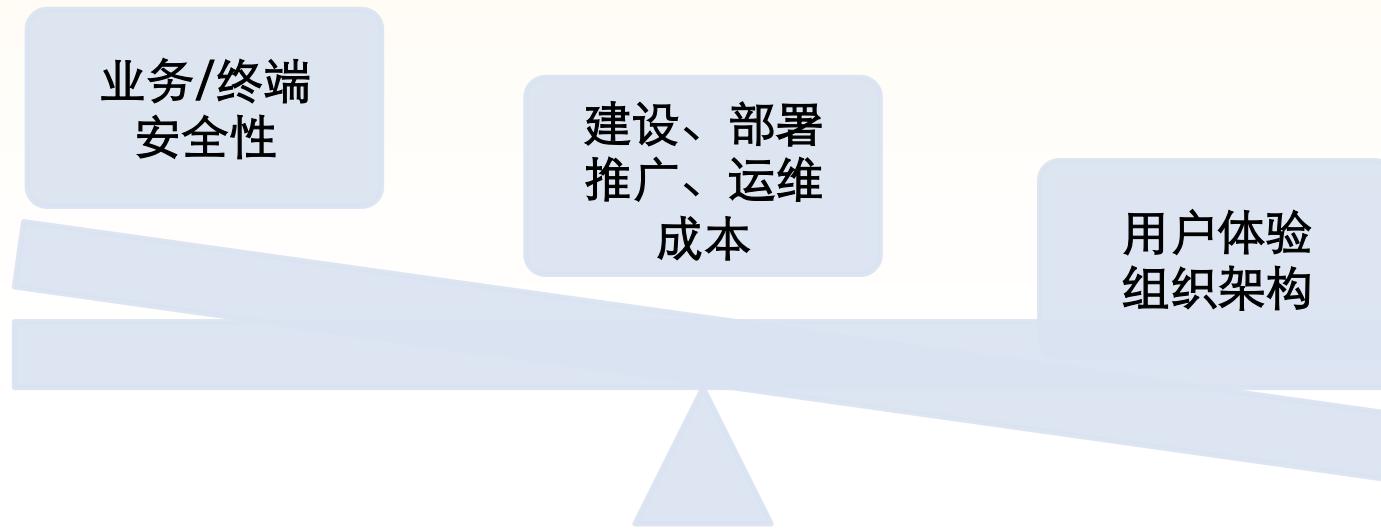


SANGFOR
深信服科技

RSA信息安全大会2012

用户的选择：多维度的平衡

RSACONFERENCE
C H I N A 2012



真正切实可行的方案才是用户所需要的！！！

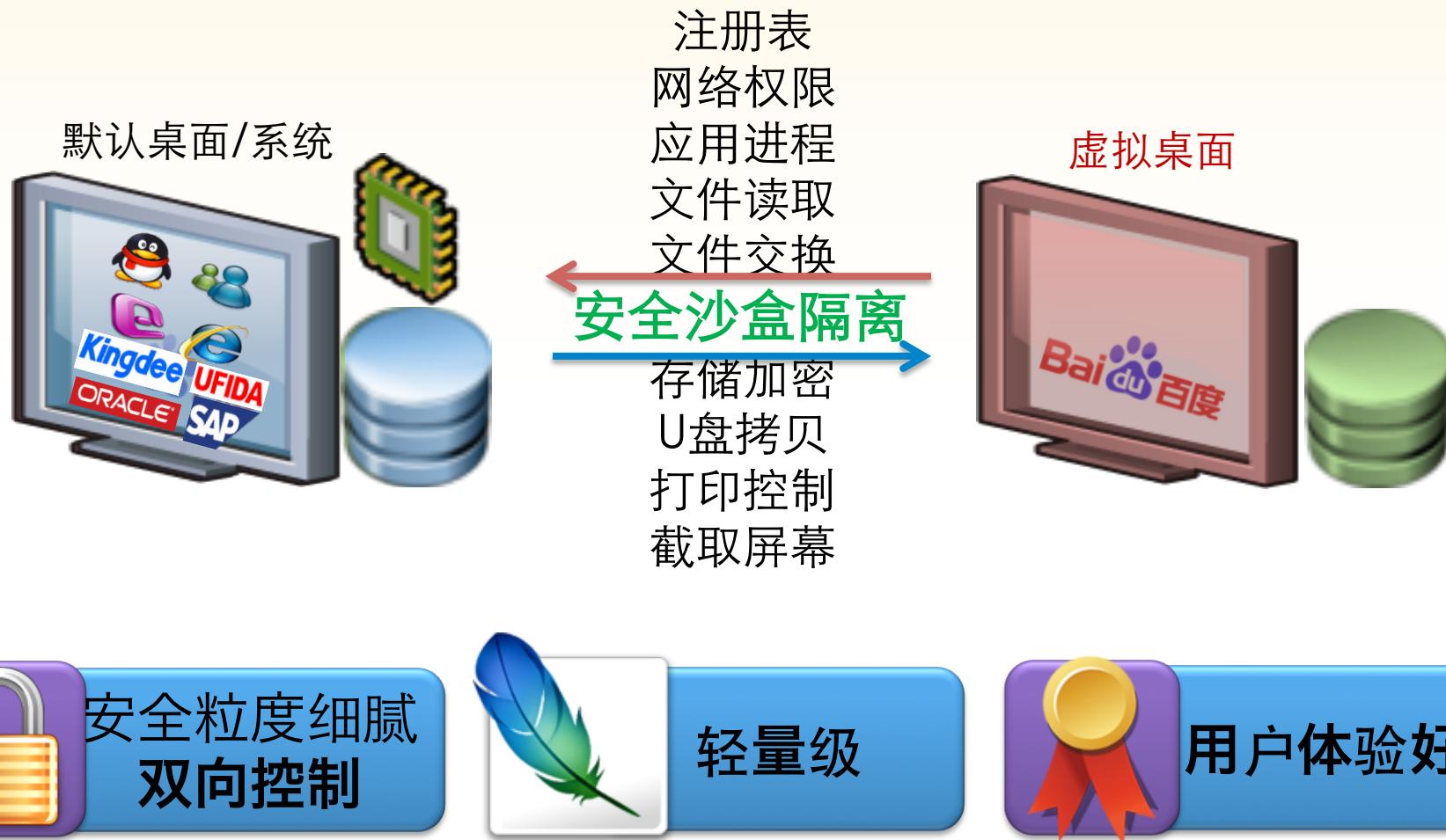


SANGFOR
深信服科技

RSA信息安全大会2012

新的虚拟化探索：安全沙盒技术

RSACONFERENCE
C H I N A 2012

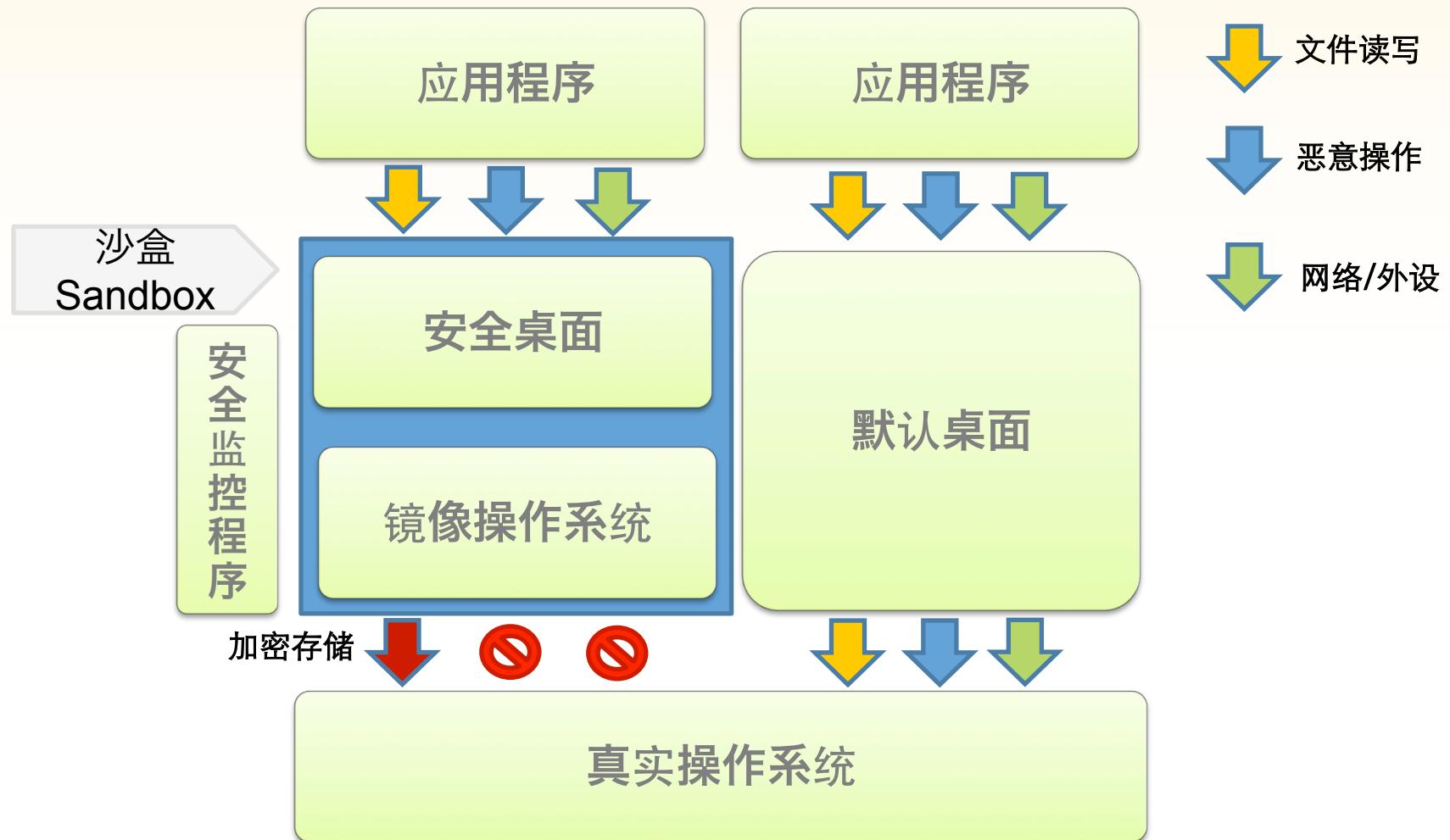


SANGFOR
深信服科技

RSA信息安全大会2012

安全沙盒价值：数据、网络等有效隔离

RSACONFERENCE
C H I N A 2012



SANGFOR
深信服科技

更有效的安全控制：病毒、木马等拦截

RSACONFERENCE
C H I N A 2012



修改注册表：被重定向处理拦截



篡改文件：被重定向处理拦截



感染、攻击虚拟环境外进程或服务：行为被禁止



感染、攻击内网其它终端：行为被禁止



SANGFOR
深信服科技

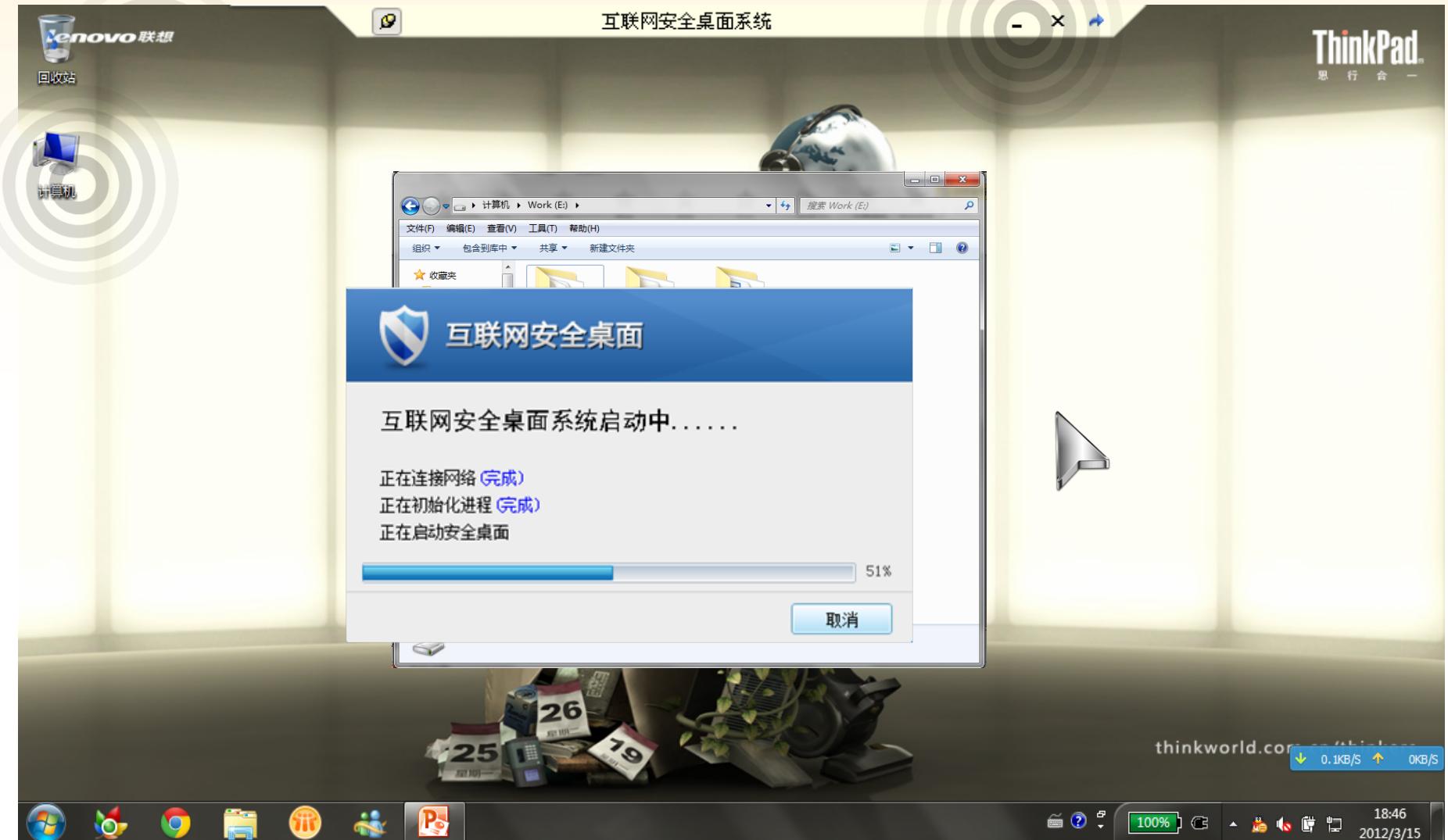
视频介绍

- 让我们一起看一段视频，
看看安全沙盒在企业IT环境中的一种典型应用
——上网安全桌面隔离互联网风险



安全沙盒：轻量级、用户体验一致

RSACONFERENCE
C H I N A 2012



SANGFOR
深信服科技

RSA信息安全大会2012

桌面/应用虚拟化 VS 安全沙盒虚拟化

RSACONFERENCE
C H I N A 2012

Same



网络虚拟隔离



数据安全存储



传输安全控制

Different



离线访问



可扩展性



高并发



高性价比



SANGFOR
深信服科技

目录

- 业务数据风险的变化
- 虚拟化技术----业务安全的新选择？
- 沙盒技术的实践及演进
 - 安全沙盒的实践应用
 - 统一终端虚拟化=安全沙盒+桌面虚拟化
 - 方案价值与未来演进



安全沙盒：多安全桌面方案

RSACONFERENCE
C H I N A 2012



SANGFOR
深信服科技

通过默认桌面实现日常办公系统的直接访问



- 用户体验无差异
- 无需迁移数据
- 满意度高

通过上网安全桌面实现Internet的安全访问



- 隔离互联网风险
- 用户体验更好
- 一键重启恢复
- 减少PC运维工作量

防泄密安全桌面访问

RSACONFERENCE
C H I N A 2012

通过防泄密安全桌面实现核心数据的安全访问



- 拦截各种数据防泄密途径 (U盘拷贝、截屏、网络外发、打印控制、加密保存等)
- 用户体验更好
- 易部署、易运维

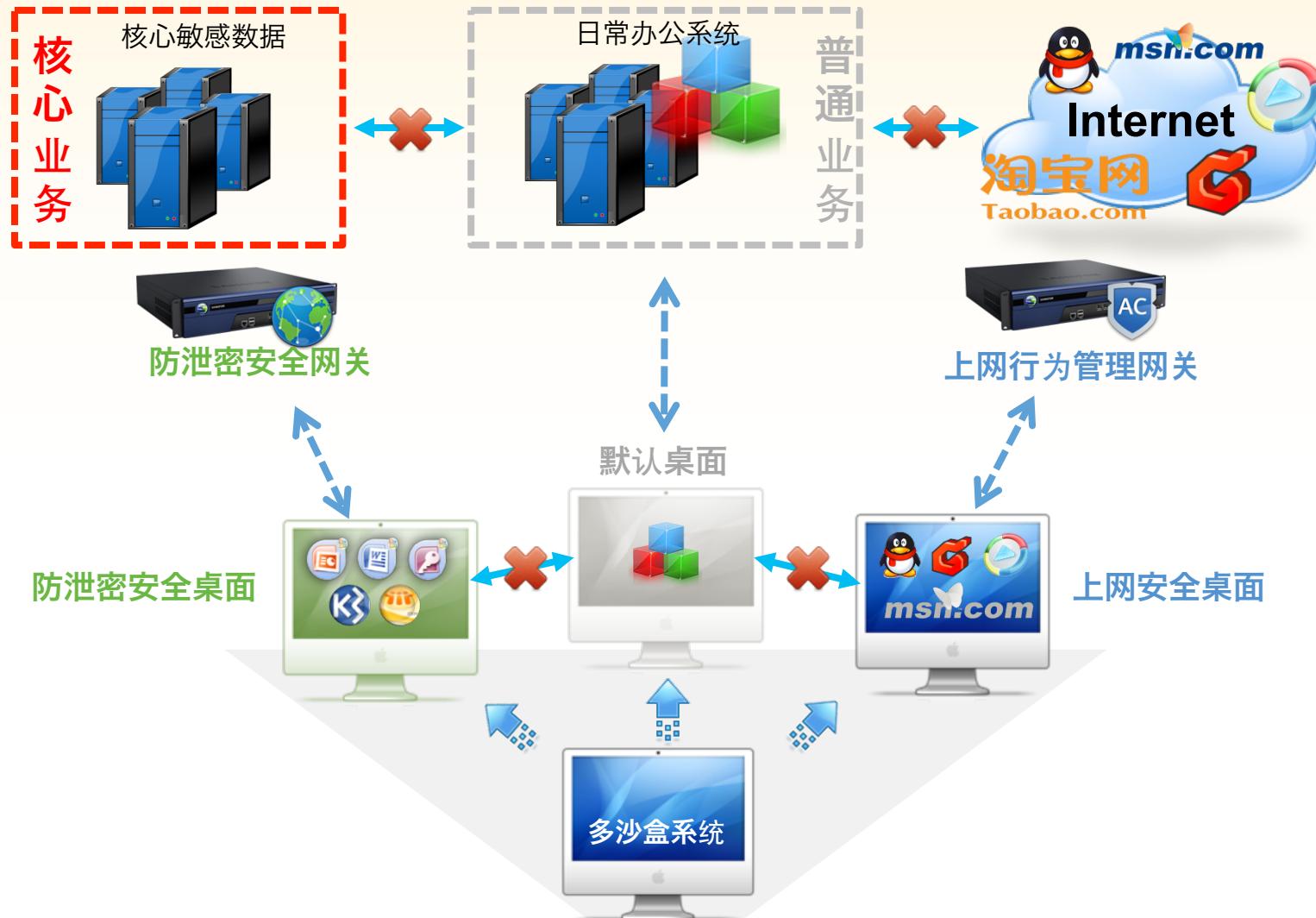
易用性增强：多桌面切换等

RSACONFERENCE
C H I N A 2012



多安全桌面架构的终端虚拟化

RSACONFERENCE
C H I N A 2012



SANGFOR
深信服科技

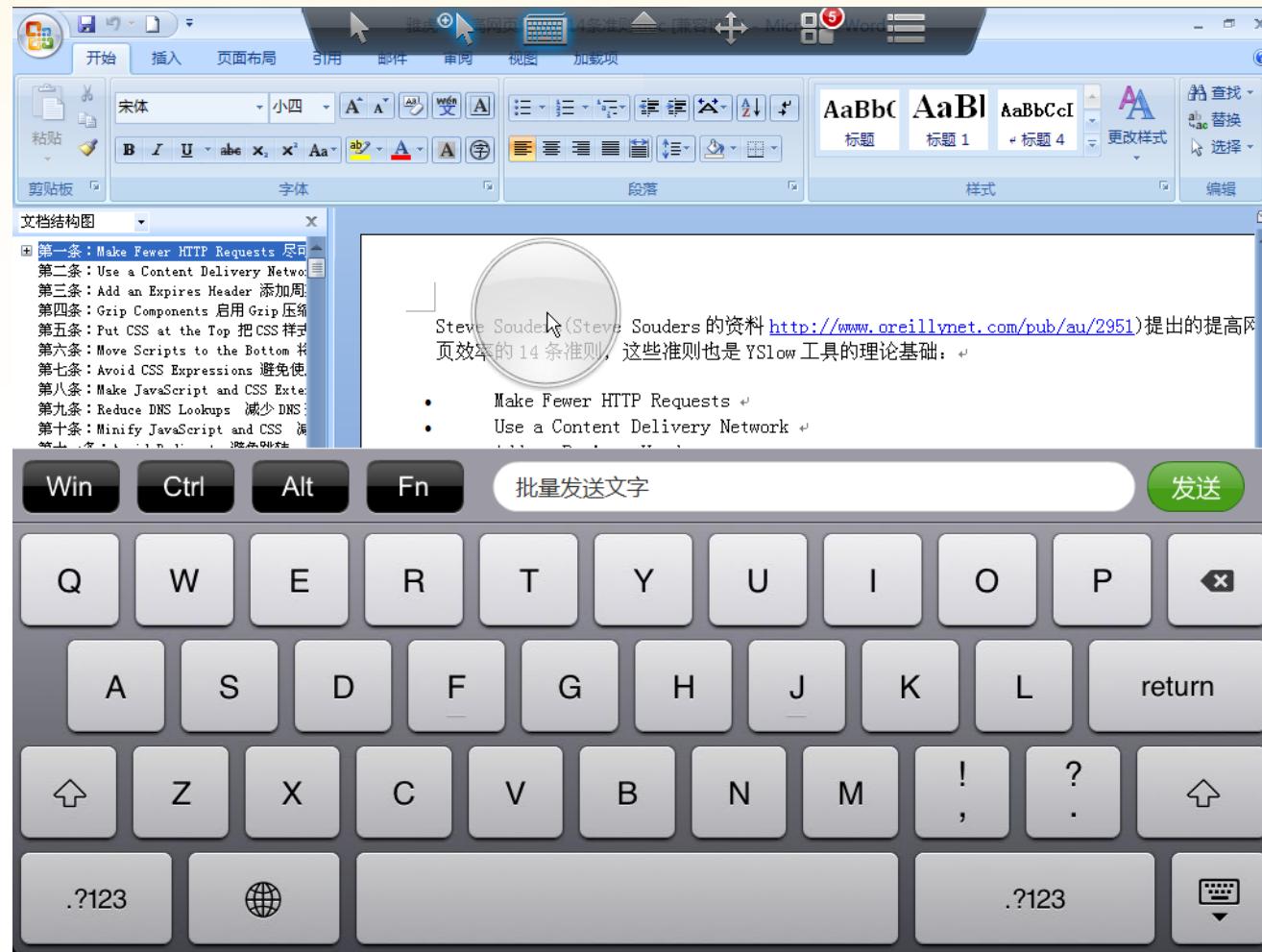
安全桌面暂时的弊端：

- Only PC
- Only One Device

- 移动终端如何解决？
- 数据共享如何解决？



移动终端的选择：应用/桌面虚拟化

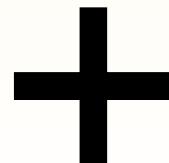


SANGFOR
深信服科技

RSA信息安全大会2012

更好的选择：统一终端虚拟化！！

远端虚拟化：应用虚拟化



本地虚拟化：安全桌面



统一终端虚拟化



SANGFOR
深信服科技

RSA信息安全大会2012

统一终端虚拟化：

整合计算资源，按需隔离防护，提升用户体验，降低TCO

RSACONFERENCE
C H I N A 2012

业务
资源层



Internet

终端
服务层

虚拟应用服务



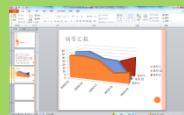
云存储服务



网络
服务层



终端
虚拟层



应用虚拟化

桌面虚拟化

安全桌面

应用虚拟化



SANGFOR 移动办公/运维人员
深信服科技

内网办公人员

RSA信息安全大会2012

解决方案的价值及优势

RSACONFERENCE
C H I N A 2012

整合计算资源，按需隔离防护，提升用户体验，降低TCO

统一终端虚拟化



SANGFOR
深信服科技

RSA信息安全大会2012

实际部署效果对比

病毒事件降低90%以上



同等的安全效果，更低的TCO1 : 4



SANGFOR
深信服科技

终端虚拟化未来的演进

基于用户身份的桌面灵活迁移



更加灵活、更加安全、更加易用

谢谢

填写调查问卷，可以到五楼展台领取精美礼
品一份

殷浩 深信服科技 市场技术总监

+86-186-7561-8111

yin-hao@sangfor.com

www.Sangfor.com



RSA CONFERENCE
C H I N A 2012
RSA信息安全大会2012