Confidence in a connected world.

无处不在的安全---Symantec 2009教育行业安全会议

Yang Hao

Solution Architect, China

IT系统安全在哪里？

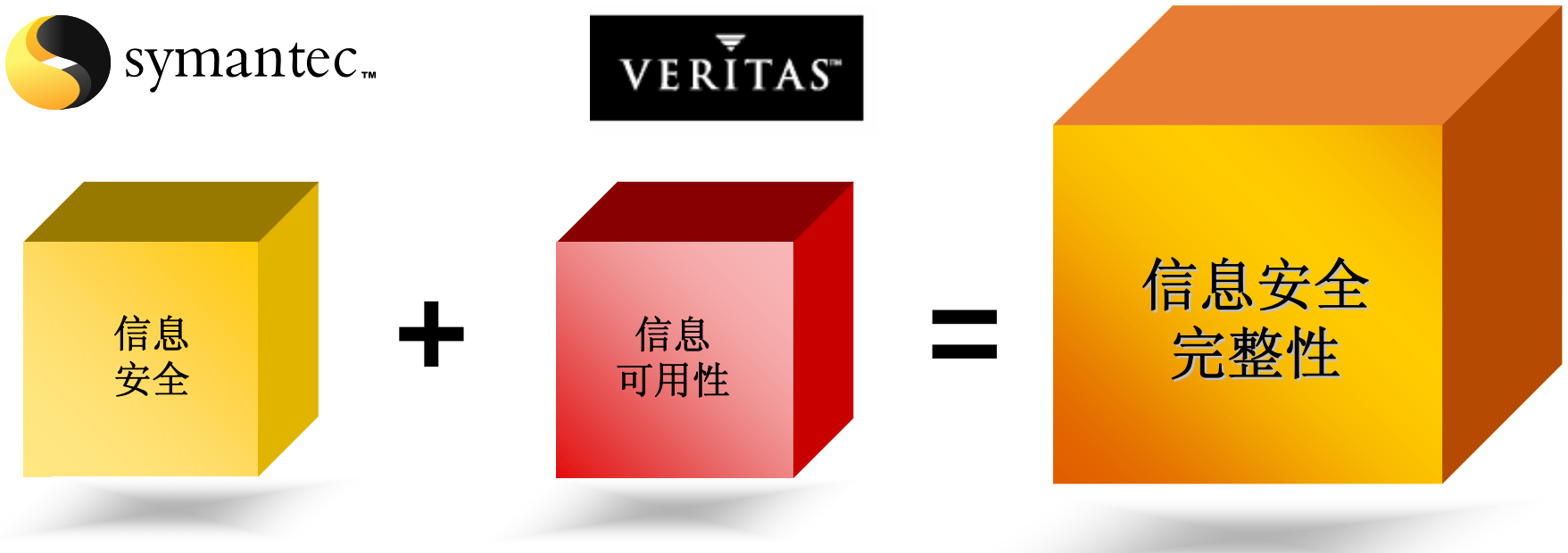
- 物理安全包括物理监控与检测、生物识别、认证令牌和卡、报警装置、物理锁以及相关的咨询实施等服务；

- 业务连续性安全则包括高可获得性与容错计算、性能监视、**RAID/SAN/NAS**、负载均衡、备份与灾难恢复以及相关的咨询实施等服务；

- 信息安全包括防火墙**/VPN**、入侵检测与漏洞评估、安全内容管理、安全**3A(**授权**/**认证 **/**管理**)**、加密机及加密软件以及相关的咨询实施等服务。

--------IDC 2004年安全大会

强强联手，进入一个全新的安全领域！



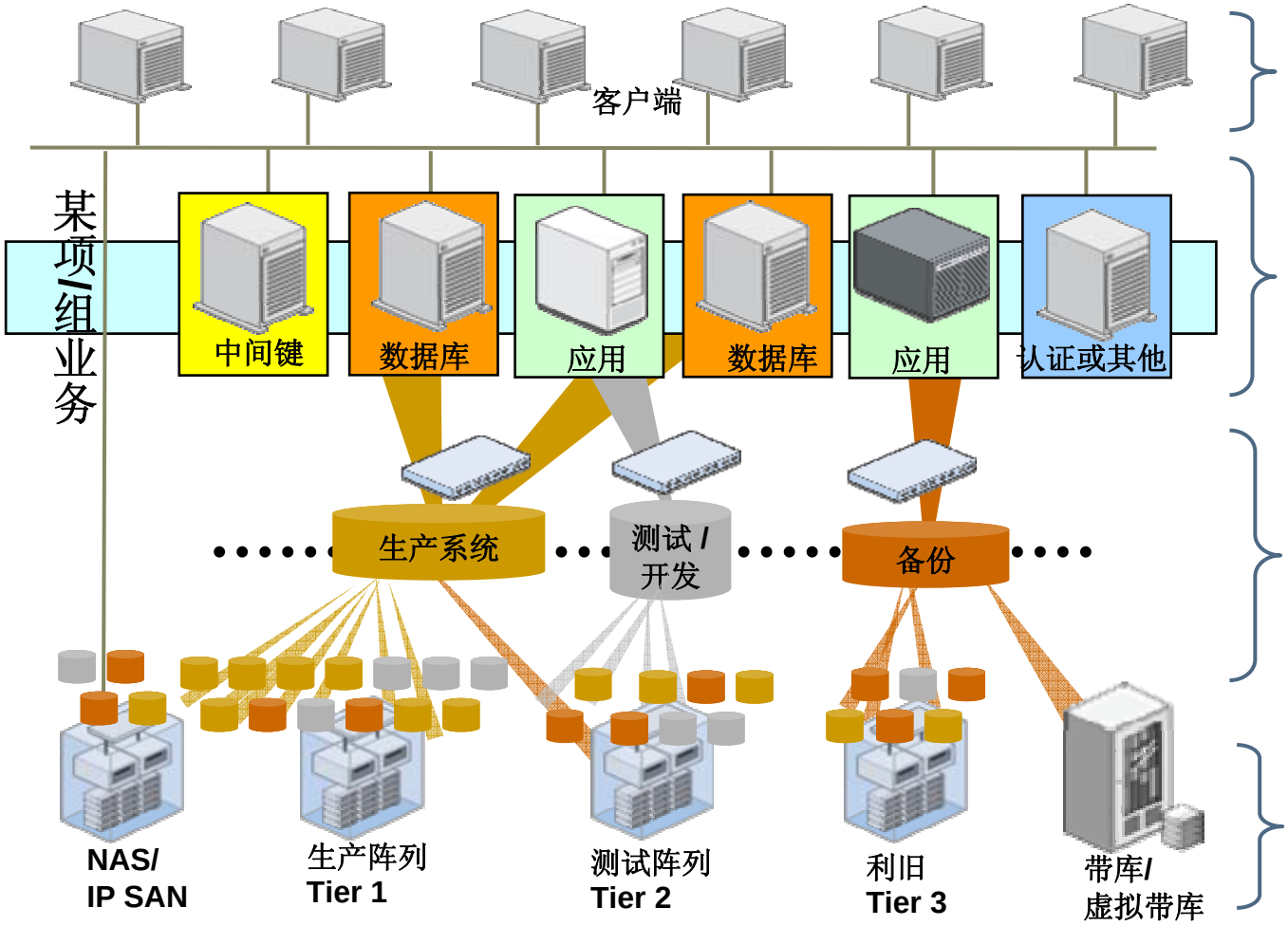
- Proactively protect all layers of the infrastructure against security threats
- Early warning of emerging threats
- Monitor systems for compliance

- Provision, optimize, monitor and remediate systems and storage to ensure uptime and performance levels are maintained
- Recover systems and data in the event of an outage

Information is secure and available
- **Greater Efficiency**
- **Less Complexity**
- **Greater Compliance**
- **Reduced Risk**

——更加强韧的IT基础架构，全面保障您的业务运行！

数据中心—业务连续性解决方案



Symantec 终端标准化解决方案

Symantec Veritas Cluster Server
本地集群
远程集群接口

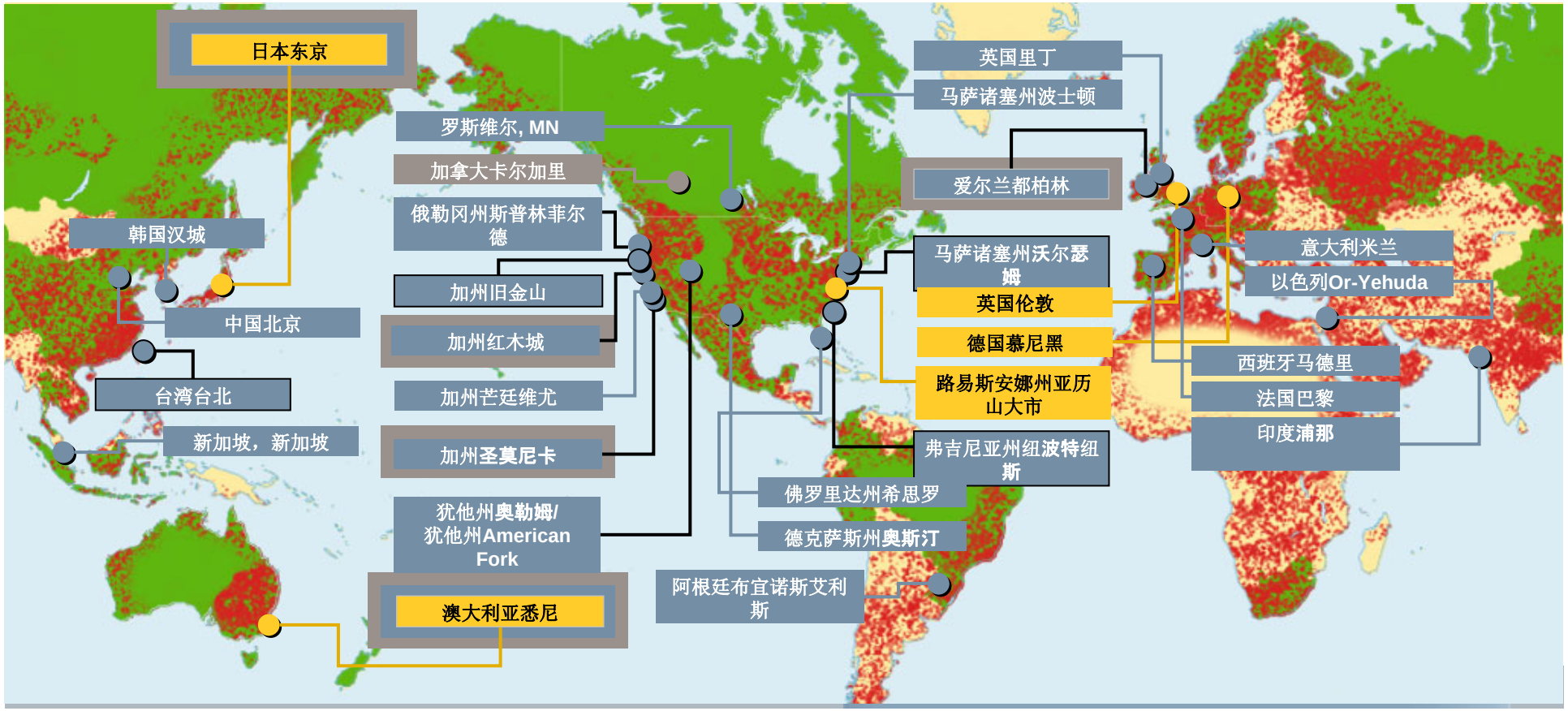
Symantec Storage Foundation Solution
虚拟化、自动化管理
物理、逻辑冗余
分级存储
I/O性能调优
远程数据容灾接口

Symantec Netbackup Solution
离线线保护的方案，利用磁盘来进行恢复

信息安全--全球威胁监控网络
无可比拟全局预警能力

5个赛门铁克安全操作中心（SOC） + 61 个赛门铁克监控的国家互联网范围 + 29 个遍布全球的赛门铁克支持中心 + 180 个国家的24，000个注册传感器 + 6 个赛门铁克安全响应实验室

4,300多台托管安全设备 ＋ 全球2亿赛门铁克用户

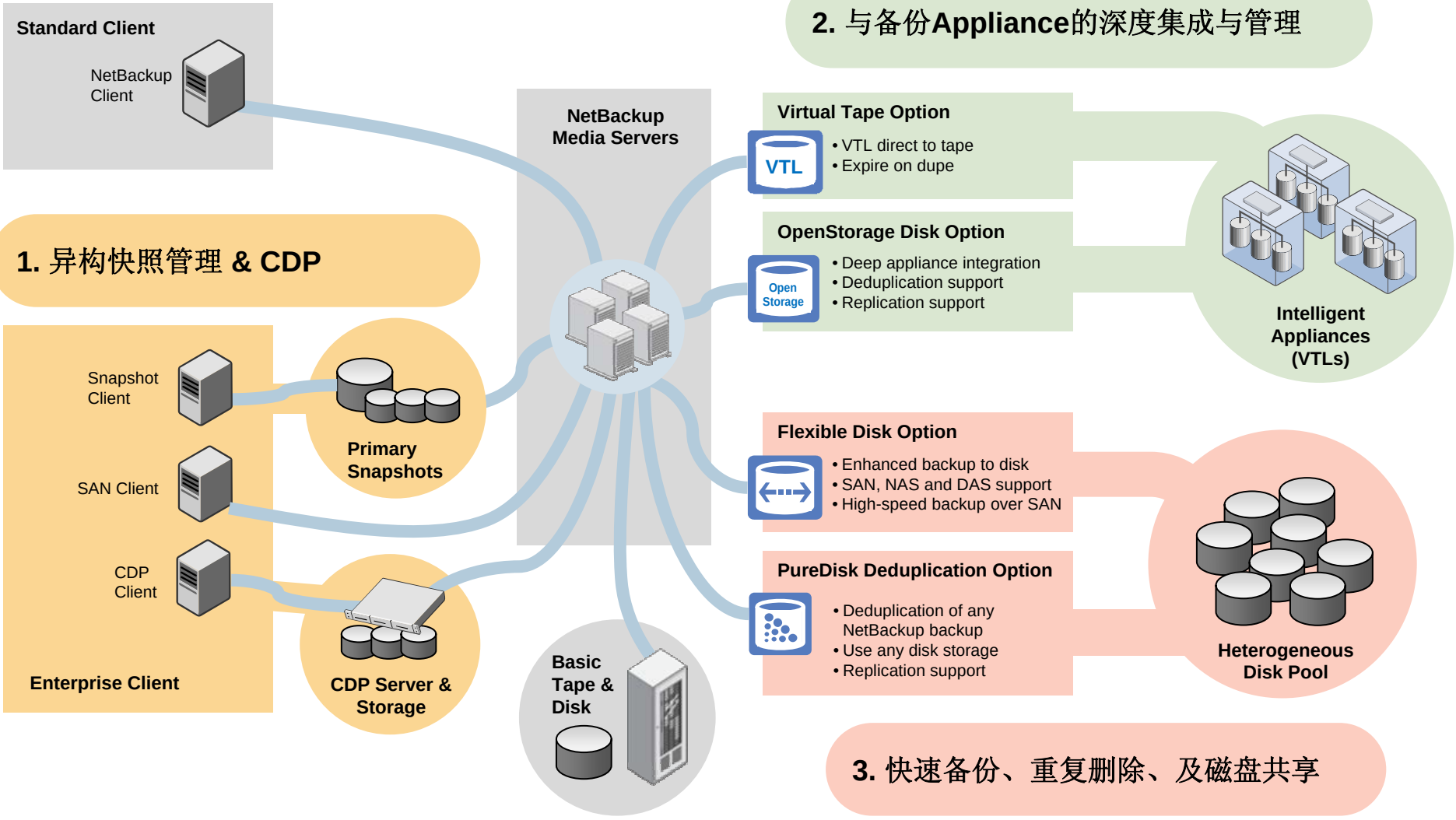


今天的Symantec 在中国

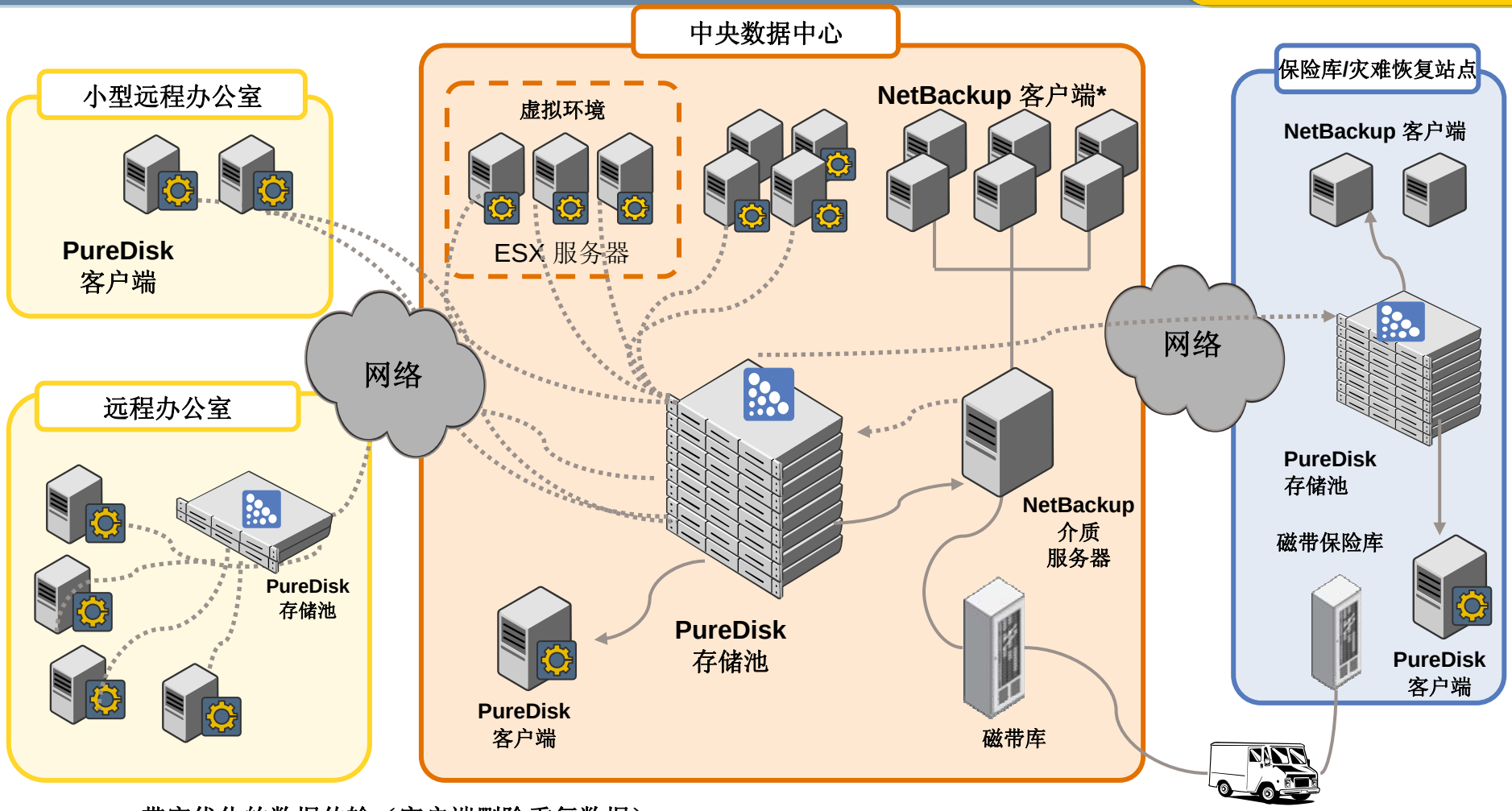
- 全球第四大独立软件公司
- 全球最大的信息安全厂商和服务商
- 赛门铁克中国有近2000名员工
- 中国研发中心有近500员工
- 2007年在中国成立安全响应中心，迅速响应来自本地的威。
- 2008年2月，赛门铁克公司和华为技术有限公司宣布，双方合资公司已正式成立。

Symantec 容灾技术介绍

NetBackup 磁盘备份解决方案



重复数据删除与窄带宽备份



带宽优化的数据传输（客户端删除重复数据）

常规数据传输

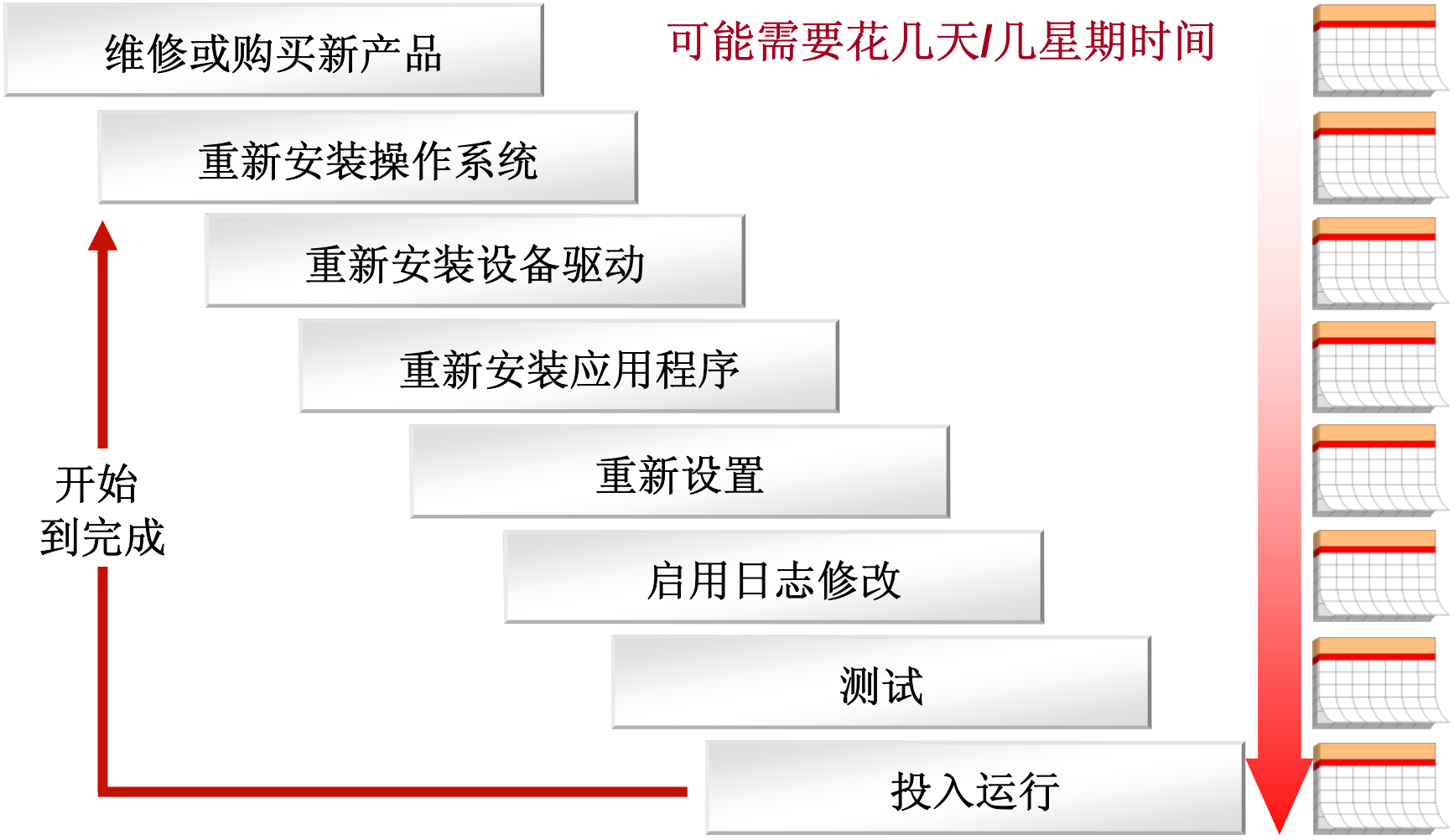
* 删除重复 NetBackup 映像是未来的一项功能，需要 PureDisk 6.5

UNIX 服务器操作系统灾难恢复（ Bare Metal Restore）

传恢复方法	BMR
Repair Hardware	Repair Hardware
Collect all necessary media together	Click “Prepare to Restore”
REBOOT	REBOOT
Reload OS from CD-ROM or floppies	
REBOOT	
Reload Backup Software from CD-ROM	
REBOOT	
Load recovery tape and restore system	
REBOOT	

- 全自动系统恢复
- 安全简单的步骤
- 快速简便
- 无需重装 OS
- 自动重建硬件配置
- 支持多平台
  - Windows
  - Solaris
  - AIX
  - HP-UX

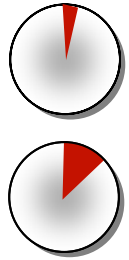
传统的手动方式系统恢复



系统恢复 – 新的自动化方式

选择恢复点

恢复整个系统



更快

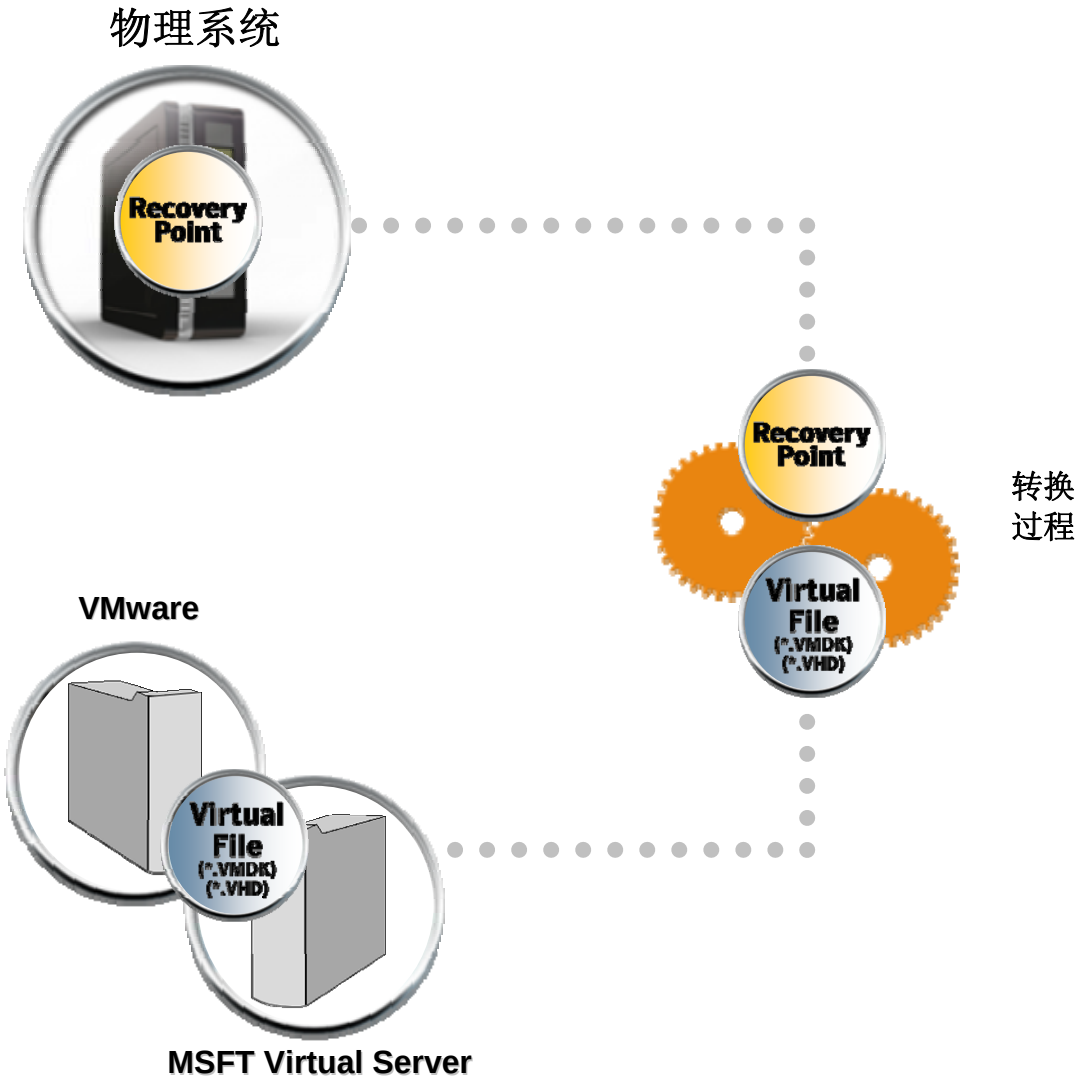
现在仅需几分钟!

更可靠

基于磁盘的方案

通向虚拟世界的网关

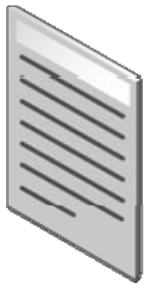
1. 创建系统恢复点
2. 转换 (P2V)
   恢复点到虚拟 Virtual环境
3. 在虚拟环境中加载系统
4. 用做生产或测试用途
5. 如果愿意，再转换回物理系统 (V2P)



备份报告管理方案：

Veritas Backup Reporter（备份报告管理器）

先进的备份报告管理，提供了对备份/恢复操作的可视性
整体框架为备份报告提供基本数据
将备份操作转化为商业服务
跨越不同的备份应用提供集中的报告



监 控

- 监控备份任务的成功，确保服务水平承诺
- 将备份基础架构成本与业务主管联系在一起，以便部门间的拆账

分 析

- 收集历史数据并分析出增长趋势
- 监视资源使用情况并发现不足
- 分析风险并且量化风险

定 制

- 定制数据视图—按照业务分类、备份域或应用类型
- 分级报告视图，提供进一步的数据钻取

NBU的可管理性
------多维度信息满足管理需求

Alerts

Total alerts	0
Critical	0
Major	0
Warning	0
Information	0

Jobs

Job history for the last: 24 Hours

Total jobs	450
Historical Jobs	
Failed jobs	0
Partially successful jobs	1
Successful jobs	446
Total data Backed up	1.36 TB
Current job activity:	
Active jobs	0
Queued jobs	0
Suspended jobs	0
Waiting for Retry jobs	0
Incomplete jobs	0
Undefined jobs	3

Drives

Total drives	18
Down drives	0
Mixed drives	3
Up drives	15
Total paths	162
Down paths	9
Up paths	153

Services

Total services	108
Stopped services	42
Running services	66
Other services	0

Master Servers

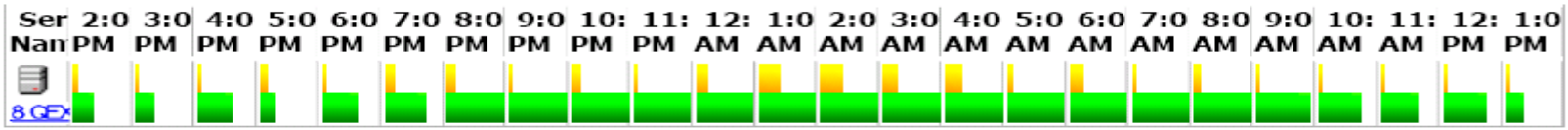
Total servers	1
Offline servers	0
Online servers	1
Partially Online servers	0

持续提高备份服务水平

Running Vs Queued Jobs

Report Parameters	
ReportingDay :	January 10, 2009 2:33 PM
IntervalFormat :	24 Hours at 1 hour intervals
TapeDriveUse :	off
Context:	UnbuMSTp01

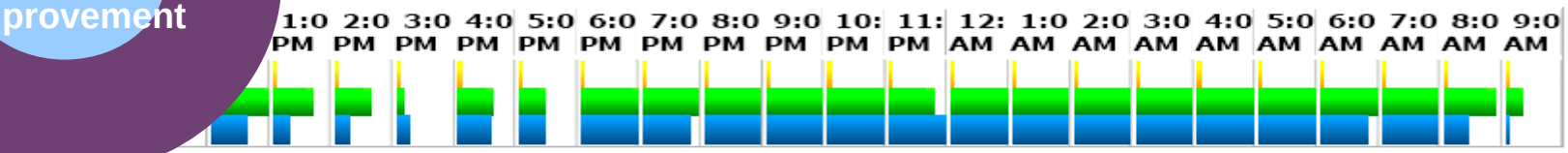
This report shows comparision between running and queued jobs



Running Vs Queued Jobs

Report Parameters	
ReportingDay :	January 12, 2009 10:04 AM
Format :	24 Hours at 1 hour intervals
e :	on
	/PDCCSnbuNOM01

comparision between running and queued jobs

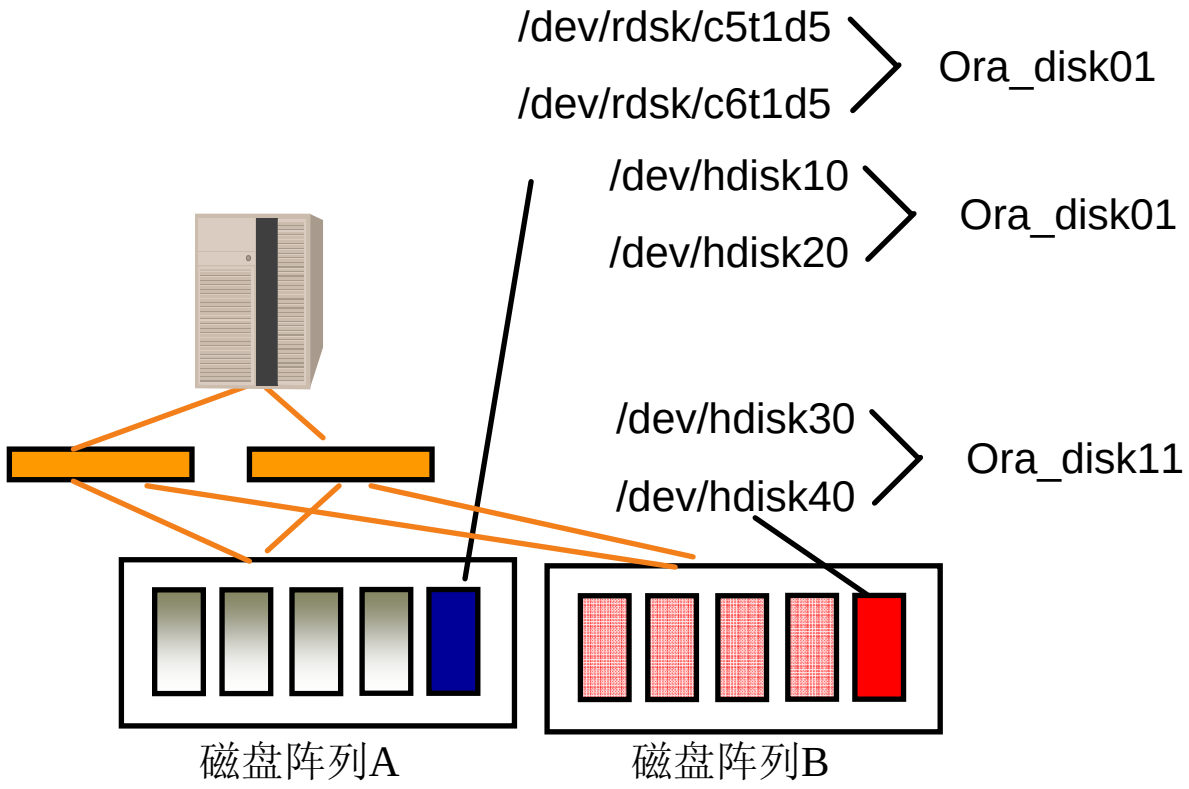


Continual Service Improvement

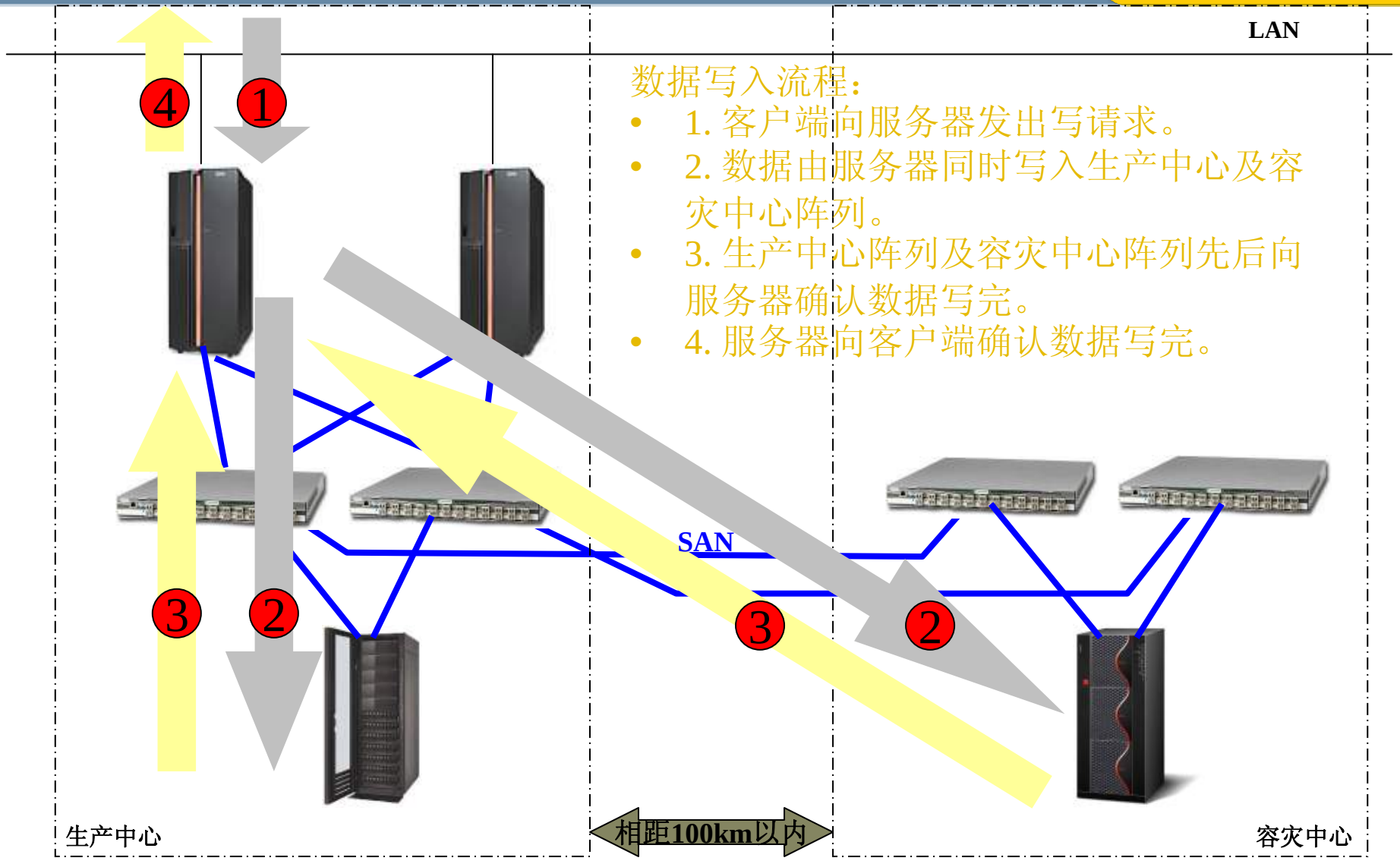
Symantec 容灾技术介绍

建立存储管理弹性架构-异构存储管理及存储虚拟化使用

- Storage Foundation DMP功能
  - Dynamic Multi-Pathing
  - 支持众多磁盘阵列
    - EMC
    - HP
    - IBM
    - HDS
    - Sun
    - Fujitsu
    - ……



数据安全-数据容灾



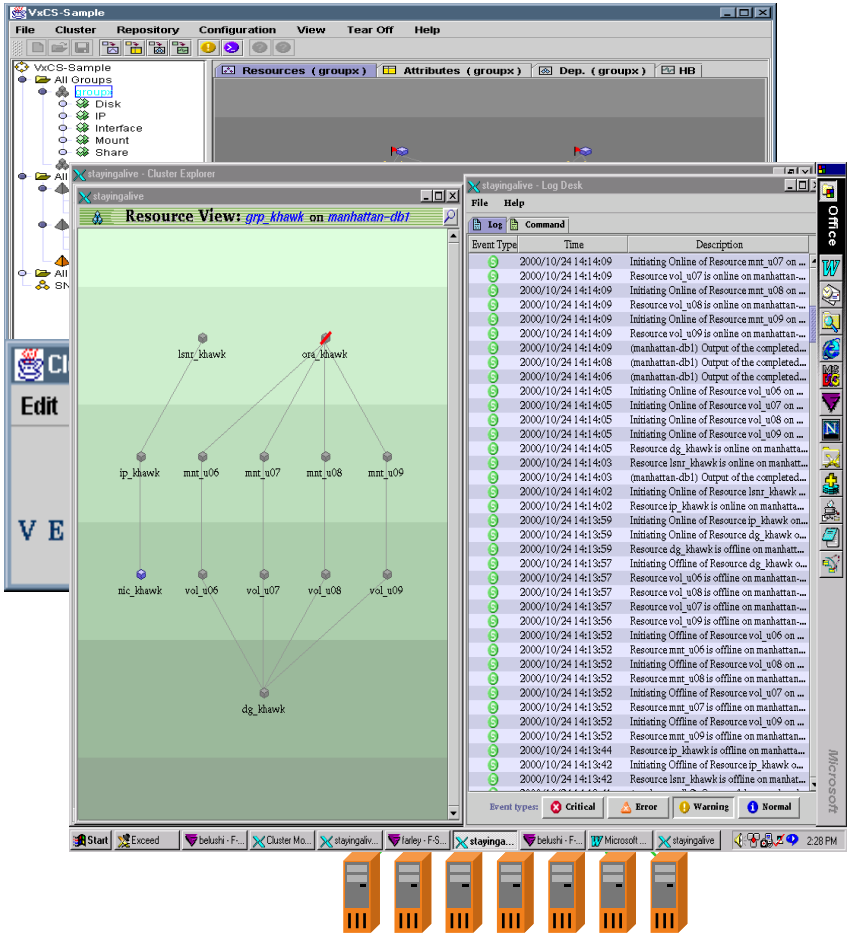
数据写入流程：

- 1. 客户端向服务器发出写请求。
- 2. 数据由服务器同时写入生产中心及容灾中心阵列。
- 3. 生产中心阵列及容灾中心阵列先后向服务器确认数据写完。
- 4. 服务器向客户端确认数据写完。

数据安全-Storage Foundation 物理冗余方案的优势

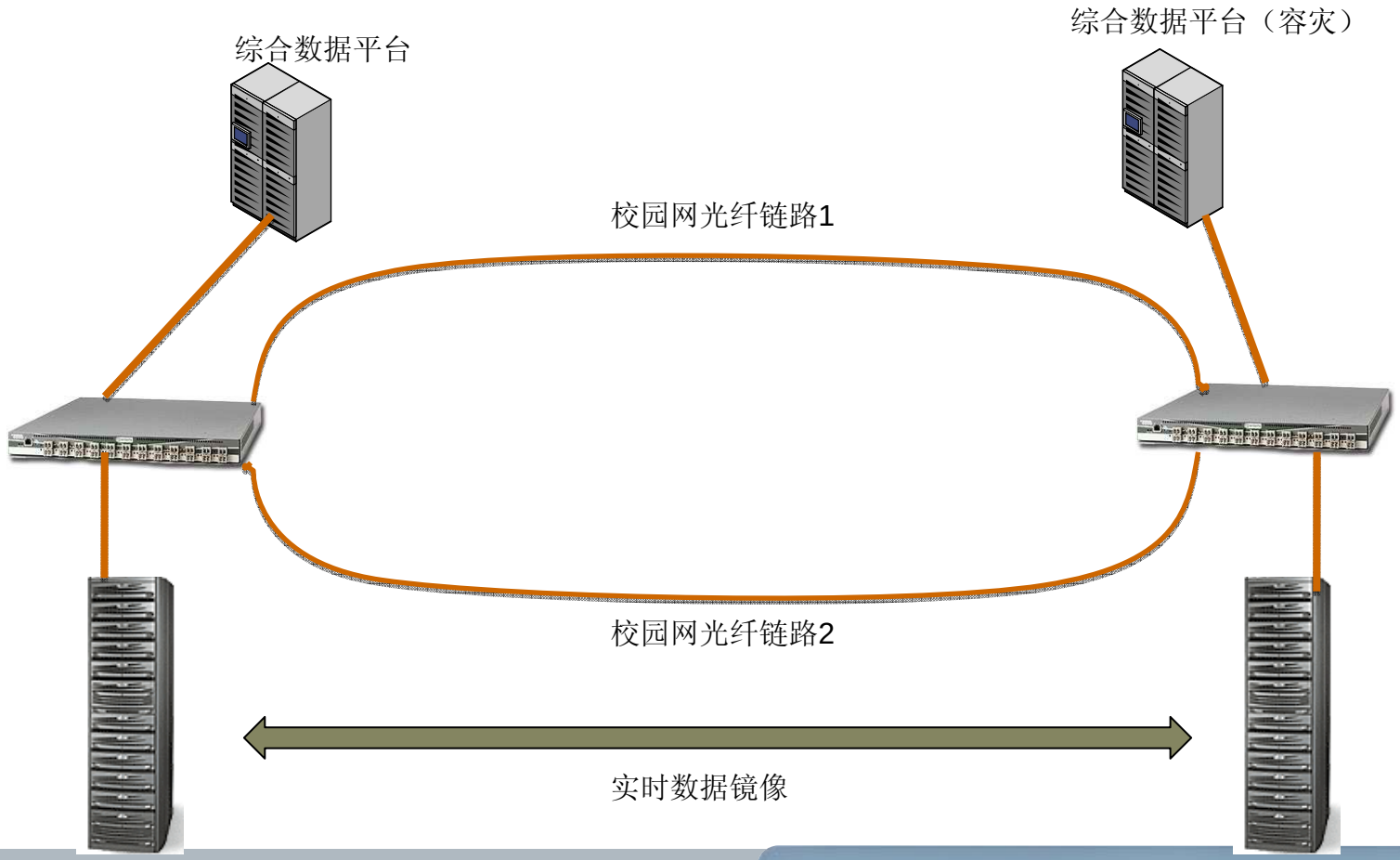
- 1．零停机时间，业务不中断。无论是生产中心还是容灾中心的磁盘阵列发生问题，都不会导致应用停顿，从而导致业务中断。
- 2．发生灾难时，无需手工活自动切换来恢复应用，应用会无缝的继续进行。从而也不会造成人为的错误发生。
- 3．由于应用不会中断，数据的一致性也没有任何风险，不会像其他的容灾方案，在容灾切换后，数据库仍然有启动不成功的可能性。
- 4．跨磁盘阵列镜像一旦发生灾难，修复后，跨阵列的可以实现增量的数据同步，而不需要重新同步所有数据，对系统的影响极小。
- 5．数据容灾进程高度可控，可以随时暂停、继续、终止，并能指定控制在一定的性能范围内实施数据同步。
- 6．跨磁盘阵列镜像还可以通过调整读写机制，提高系统的读写性能。
- 7．跨整列的镜像，支持在不同品牌，不同型号的磁盘阵列之间进行。可以最大限度的保护用户以前的投资。
- 8．基于SAN的容灾技术，其容灾距离可以在60到80公里的范围内，得到很好的想能保障。
- 9．同时提供多项逻辑容错技术， 帮助用户快速恢复逻辑错误，如误删除，误操作等。
- 10．提供强大的存储管理平台。

应用容灾技术：Veritas Cluster Server

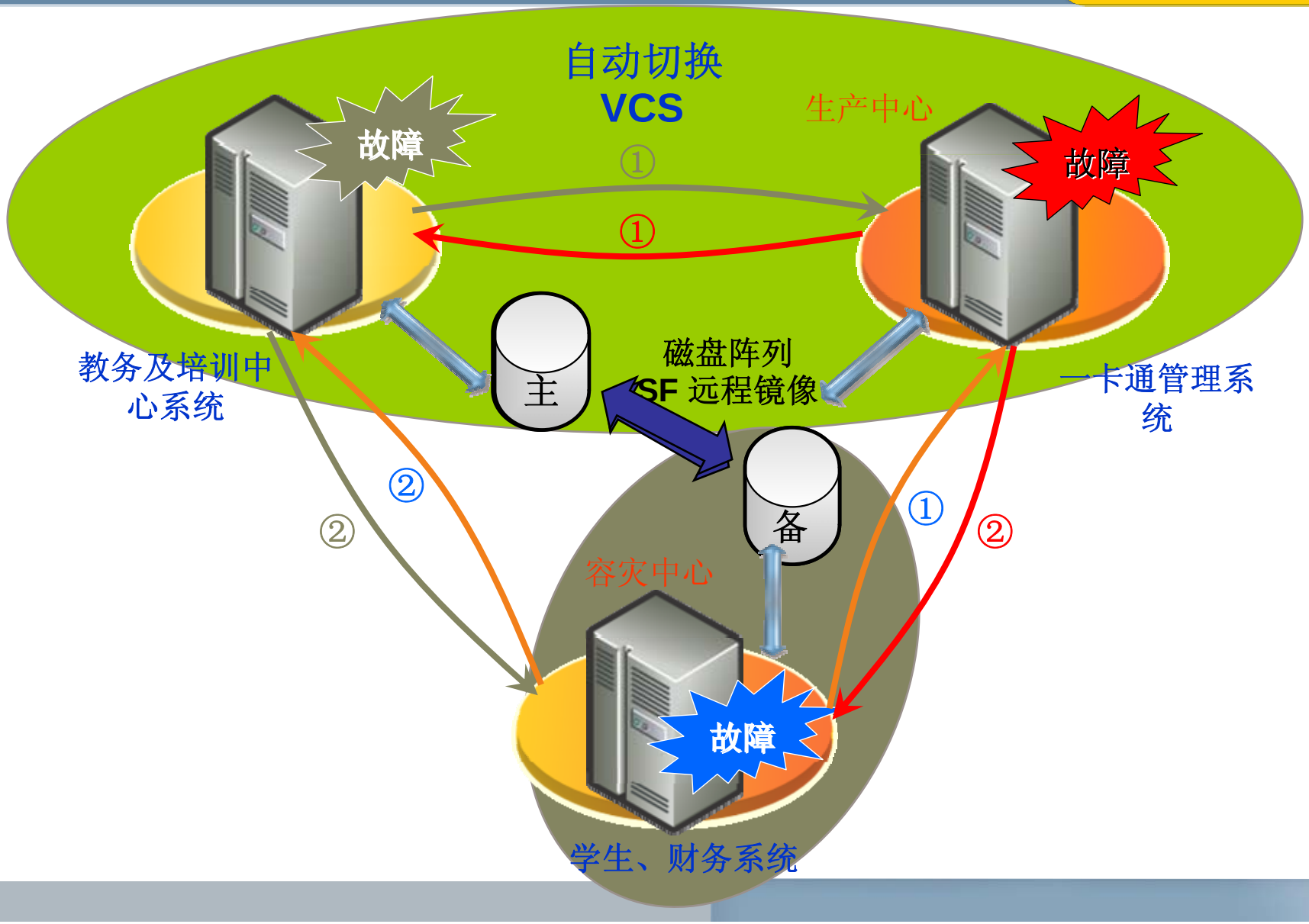


- 安装、配置、管理简单易用
- 应用服务级的群集技术
- 支持广泛的第三方平台
  - AIX
  - HPUX
  - Solaris
  - Linux
  - Windows
- Agent支持广泛的第三方软件
- 灵活定义依赖关系
- 方便定制用户应用的监控

核心业务系统的园区容灾解决方案
------Storage Foundation Enterprise HA



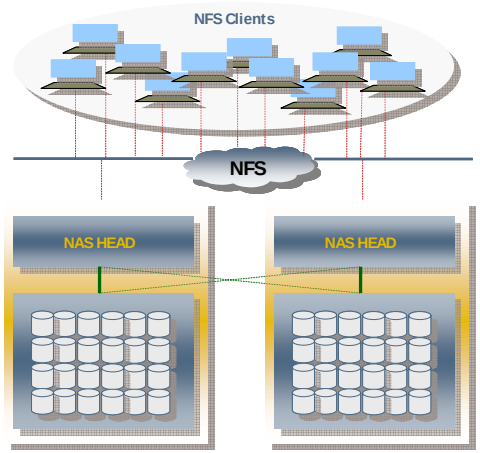
N to M 的集群类型


自动切换
VCS
生产中心
故障
①
①
故障
教务及培训中
心系统
主
磁盘阵列
SF 远程镜像
一卡通管理系
统
②
②
①
②
备
容灾中心
故障
学生、财务系统

Symantec 集群NAS技术介绍

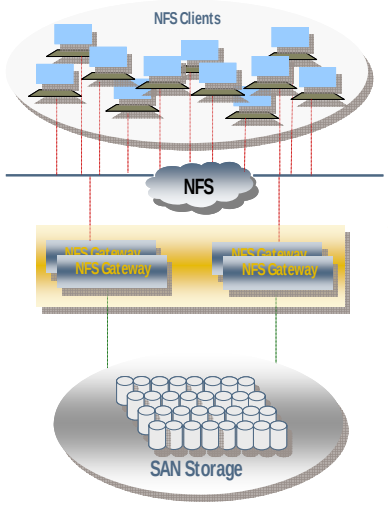
SFS 可攀升的集群 NAS 系统

Traditional Architecture



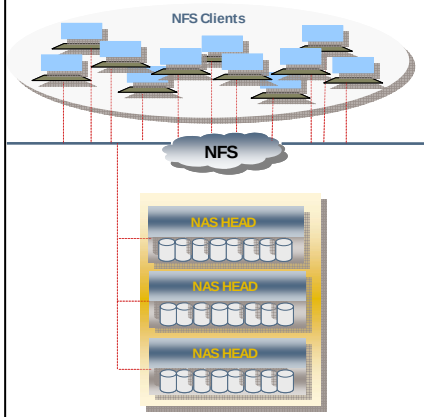
NetApp *FASxxxx*
EMC *NS / Celerra*
Sun *StorageTek NAS*
IBM *System Storage Nxxxx*
SGI *Infinite Storage NAS*
Pillar Data *Axiom*
Compellent *Storage Center*
Agami Systems *AISxxxx*
3PAR *Utility File Services*

Hardware Gateway



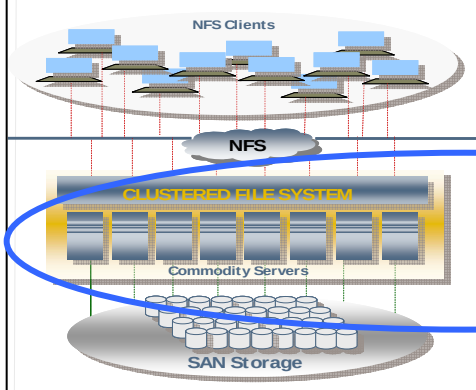
NetApp *V-Series*
IBM *System Storage Nxxxx Gateway*
BlueArc *Titan*
Hitachi *High-Perf. NAS Platform* (re-branded BlueArc)
EMC *NS Series Gateway*
ONStor *Bobcat*

Clustered Hardware



Isilon Systems *Isilon IQ xxxx*
Panasas *ActiveStor xxxx*
NetApp *Data OnTAP GX Systems*
NEC *HYDRAstor*
Rackable *Rapidscale Clustered Storage*
ONStor *Pantera Clustered NAS*

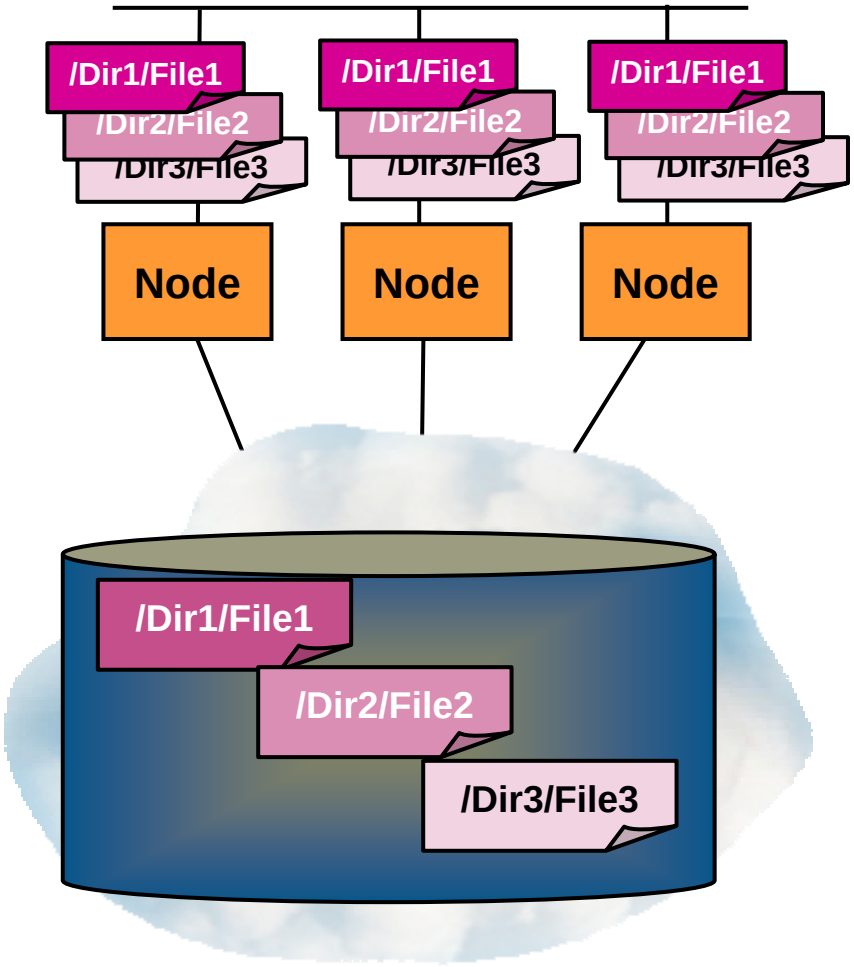
Software Gateway



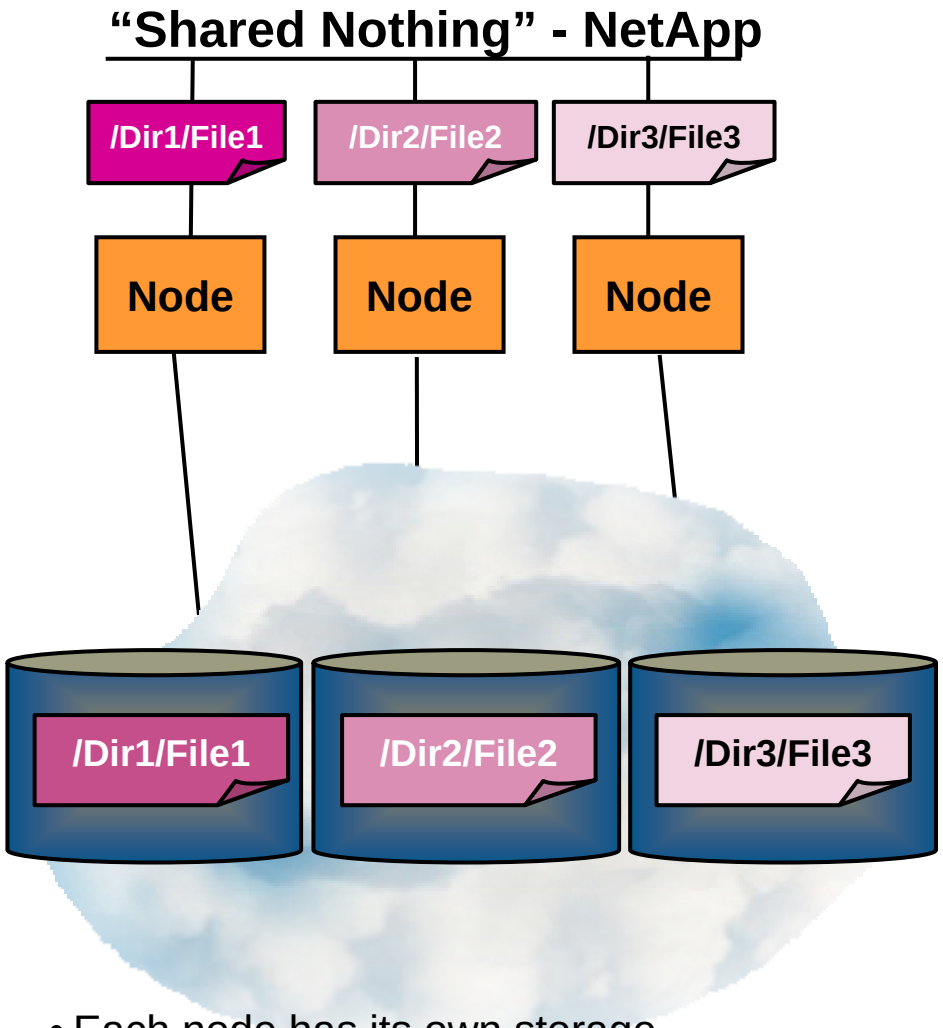
SFS

HP *Polyserve Matrix Serving Cluster*
Quantum *StorNext*
Ibrix *Fusion*
Exanet *ExaStore*
Cluster File Systems, Inc. *Lustre*

SFS和NAS的架构区别



- All Nodes see the same storage



- Each node has its own storage
- On failover, storage is moved to another node

Symantec 终端安全介绍

SEP—4个厂商、5种产品的技术

威胁	保护技术
移动终端、非法接入、外设管理、外联管理、行为监控	策略符合性检查和自动修复
零日攻击、恶意软件、特洛伊木马、应用程序注入	异常行为检测
Slurping、IP 窃取、恶意软件	外设控制
缓冲溢出攻击、程序注入、按键记录	防反堆栈溢出
恶意软件、Rootkits、零日漏洞	O/S 保护
蠕虫、探寻和攻击	网络IPS
	客户防火墙
病毒、特洛伊木马、恶意软件和间谍软件	反间谍软件
	防病毒

Symantec

Symantec Endpoint Protection

Symantec 主机安全及网页防篡改技术介绍

SCSP 主机服务器关键系统多重防护功能

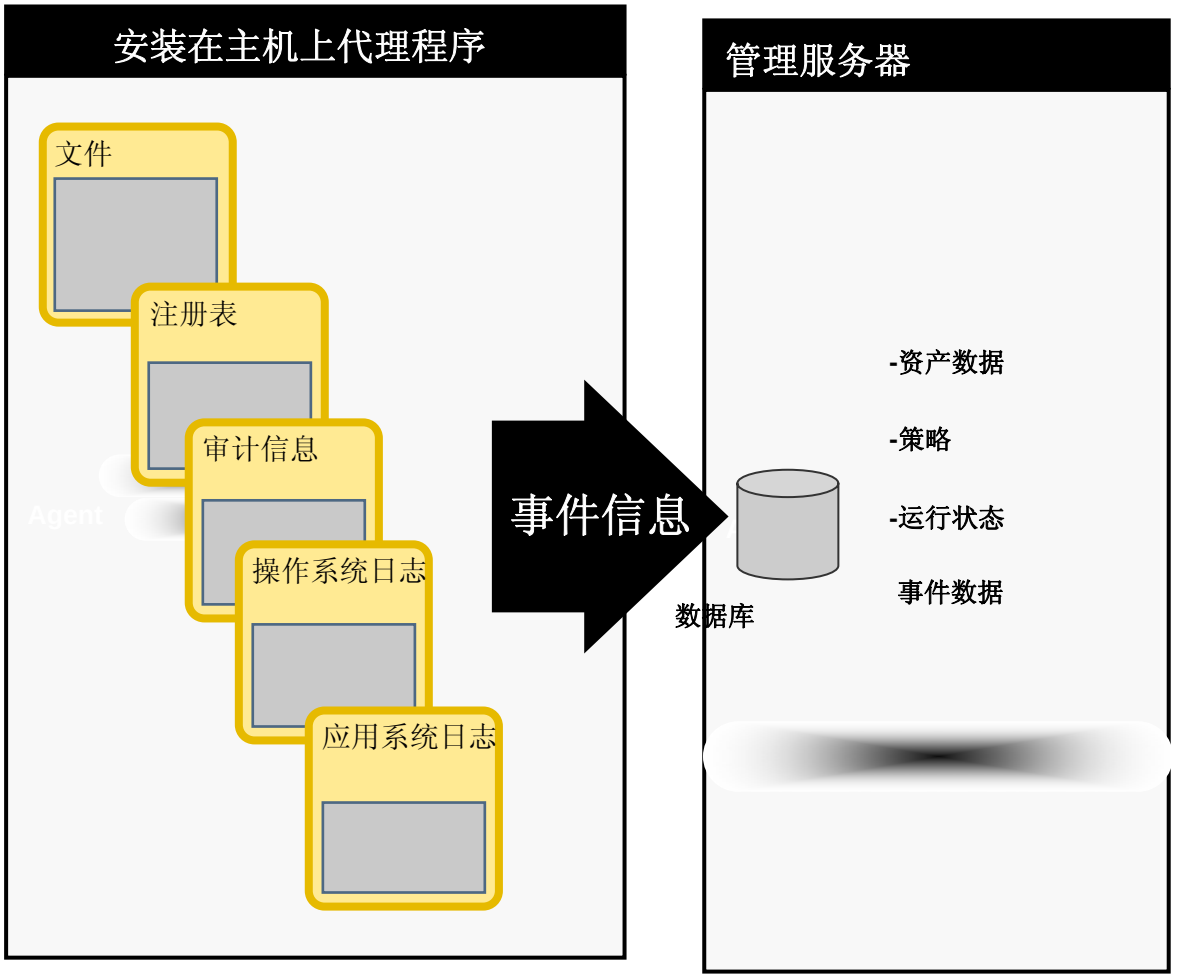
- 阻止后门
- 限制应用程序的网络连接
- 限制进出流量
- 主机防火墙功能
- 默认策略即可有效保护系统

- 限制应用和操作系统的行为
- 阻止缓冲区溢出攻击
- 检测零日攻击
- 减少系统宕机时间
- 操作系统加固

- 锁定系统配置和设定
- 注册表保护
- 文件系统保护
- 强制遵从安全策略
- 限制用户的权限
- 限制移动存储设备

- 监控日志和安全事件
- 归并并转发日志到SSIM平台
- 智能事件响应

主机日志分析和行为审计—SCSP IDS模式



智能报警……

- •主控台报警
- •邮件通知
- •SNMP Trap
- •禁用恶意帐户
- •保存事件信息供进一步分析
- • 转发日志到管理服务器供报表和分析
- •基于策略的自定义响应动作

主机行为监控内容

- 未授权的系统配置更改
- 未授权的管理权限更改及滥用
- 用户登录、退出，和失败登录
- 操作命令和参数
- 重要文件未授权访问、更改
- 变更内容
- 注册表的更改（针对Windows平台）
- ……

Symantec 终端生命周期管理

重新定义 IT 生命周期管理

Altiris ITIL 的解决方案…

执行工具

- 部署解决方案
- 客户端管理
- 远程控制
- 网管 / Windows
- 客户端/服务器备份和修复
- 软件分发解决方案
- 备份和修复解决方案
- Wise 打包工具

程序管理工具

- 帮助台解决方案
  - 事件管理
  - 问题管理
  - 变动管理
  - 发布管理

分析工具和自动报警

- 服务器监控解决方案
- 网管 / Windows
- 应用测量管理
- 合同管理
- 网络报表
- TCO 解决方案
- 补丁管理解决方案

统一的配置管理和资产管理数据库

- 资产管理解决方案
- 固定资产管理解决方案
- 应用软件管理解决方案
- 条形码解决方案

计算中心桌面统一管理平台
------Altiris

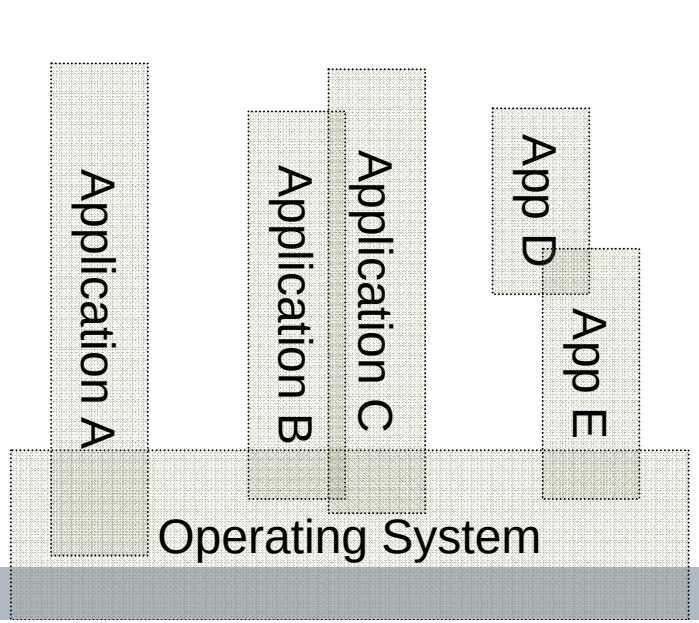
- 计算中心教学用桌面面临繁琐的管理压力
  - 需要经常更改软件环境
  - 各种教学用软件同时安装可能发生冲突
  - 时间要求高，一种软件经常只使用一节课
- Altiris解决方案完全解决教学桌面的难题
  - 桌面部署解决方案
  - 软件虚拟化解决方案

计算中心桌面统一管理平台
------Altiris 软件虚拟化SVS

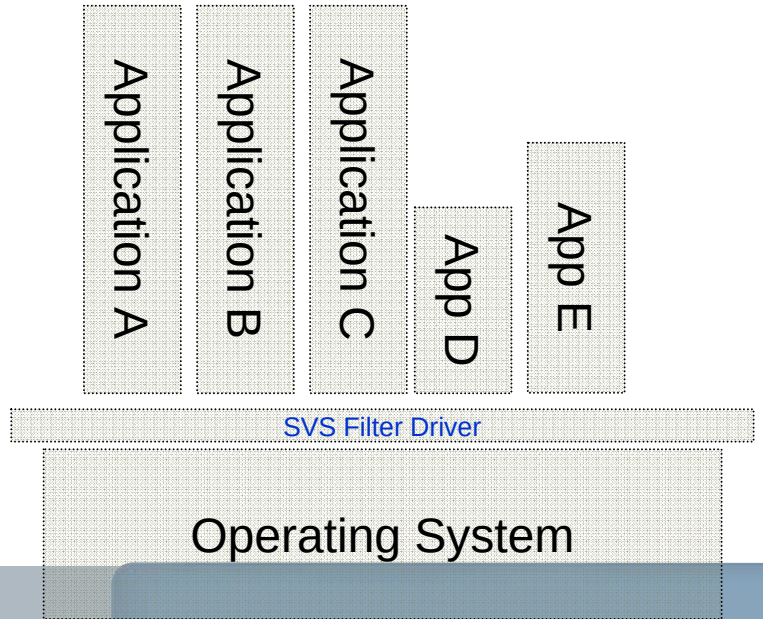
- 部署困难
- 各种软件冲突
- 注册表混乱
- 卸载不干净
- 难以修复

- 一次制作，简单部署
- 各种软件不冲突
- 注册表不修改
- 不卸载，只禁用
- 单击修复

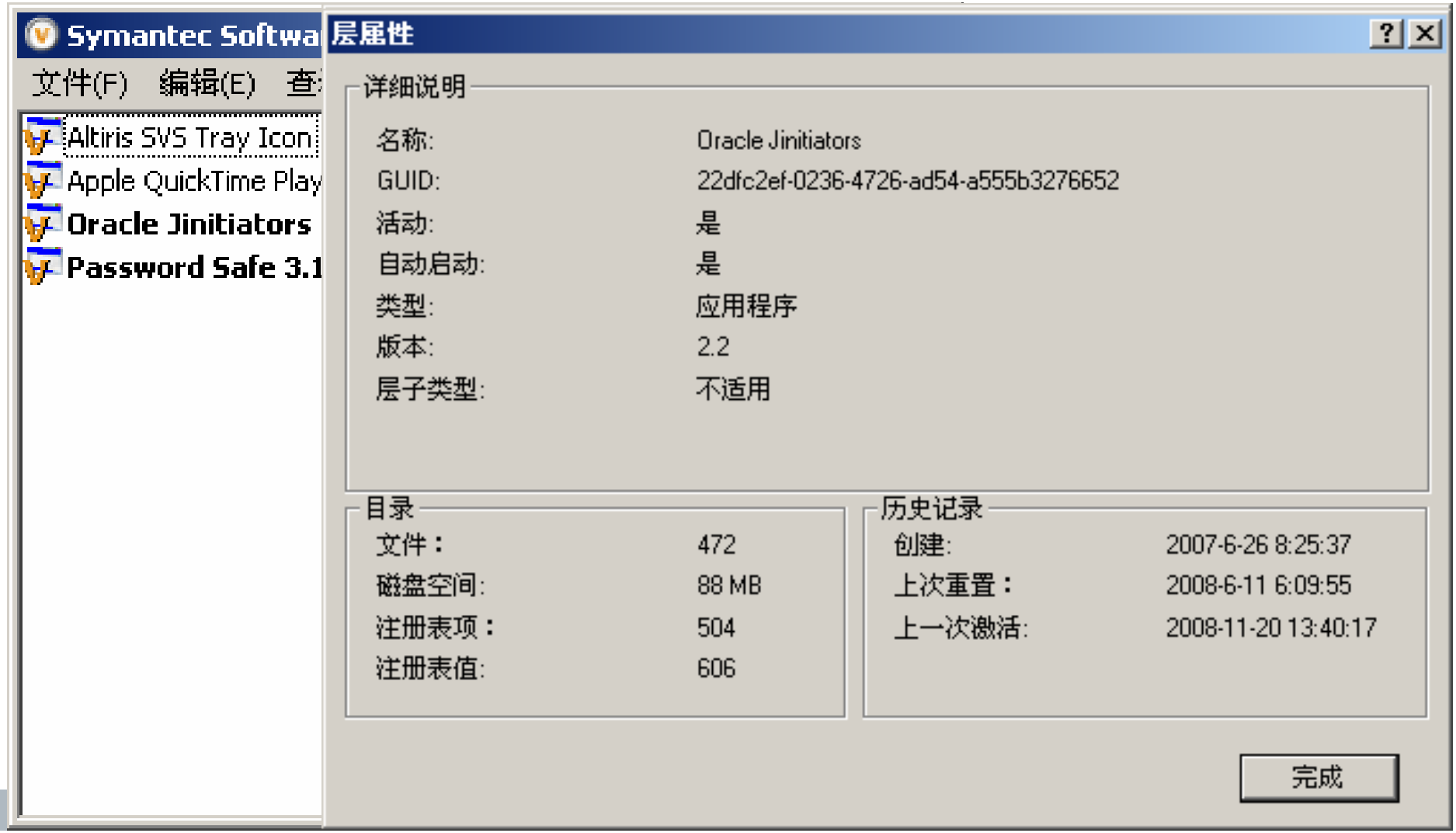
传统环境



SVS 环境



计算中心桌面统一管理平台
------Altiris 软件虚拟化SVS



计算中心桌面统一管理平台
------Altiris 软件虚拟化SVS

- 同软件安装说再见
- 同软件冲突说再见
- 同注册表修复说再见
- 一键修复/隐藏
- 同CMS结合，将日常桌面机的维护时间下降至10分钟

Thank You!

YangHao 杨豪
Sr. SE
Symantec Shanghai Office
0086-021-32174788-5517(Office)
0086-021-52925291 (Fax)

Hao_yang@symantec.com