



快速恢复+溯源—— CDP技术在抵御勒索病毒中的应用

童亮

杭州信核数据科技股份有限公司产品副总裁



杭州信核数据科技股份有限公司成立于2006年，是国内**存储虚拟化**与**数据保护**领域的领导厂商。



总部位于杭州，在全国24地市设有分支机构。



专注于**数据中心灾备**及**云灾备**，保障客户业务7x24小时连续运行。



产品广泛应用于**政府、医疗、制造、金融、能源、教育**等行业。

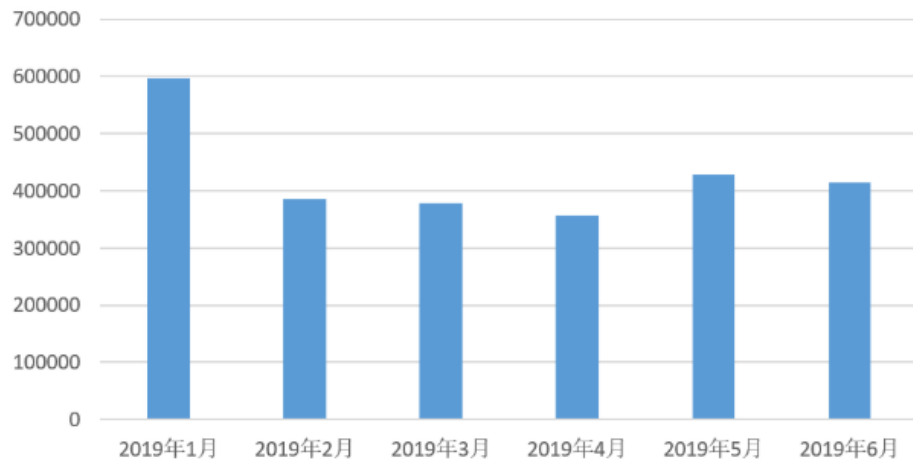
目录

抵御勒索病毒备份必不可少

传统备份恢复业务缓慢

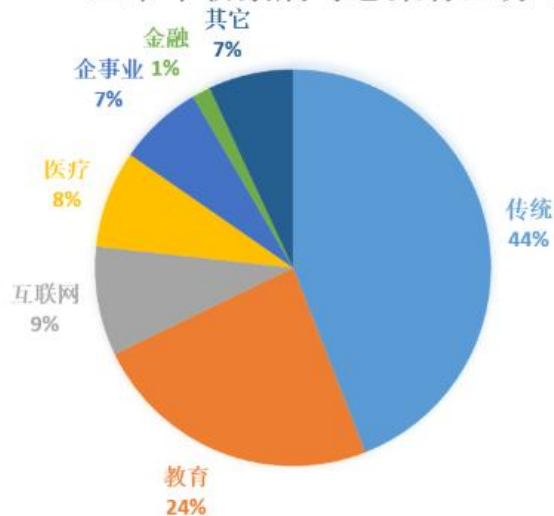
CDP快速恢复及溯源应用

2019上半年勒索病毒攻击趋势

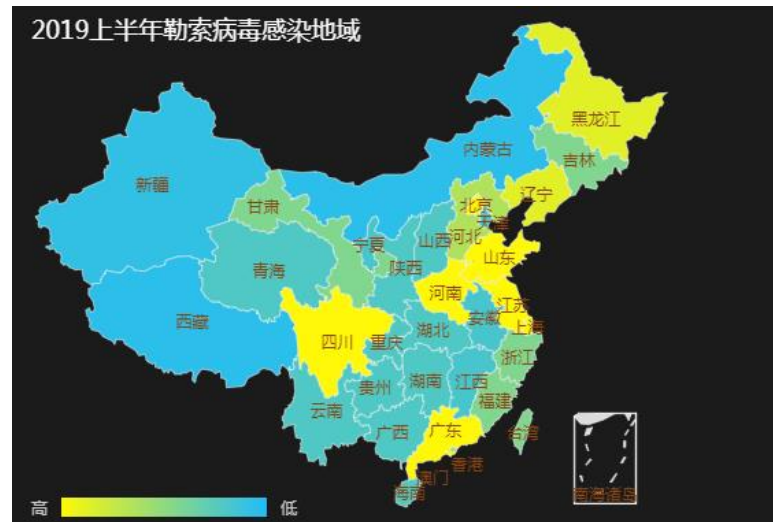


上半年250W台，平均每天1.37W台

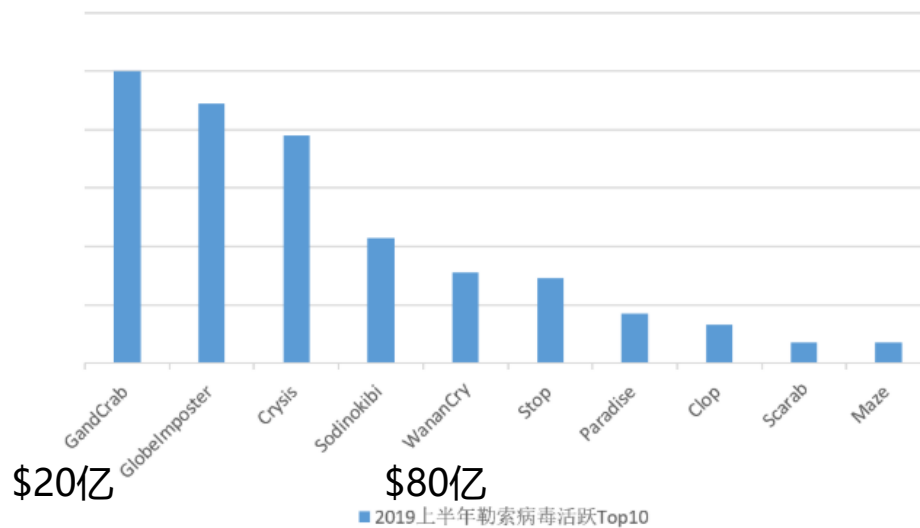
2019上半年勒索病毒感染行业分布



2019上半年勒索病毒感染地域



2019上半年勒索病毒活跃Top10





文件



数据库



磁盘

1. 加密数据的恢复
2. 业务的快速恢复
3. 溯源分析，防御下一次攻击



大部分勒索
病毒不可解

交了赎金不一定
能保证恢复数据

是否有做备份就可以了？

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE

Recovery Point Objectives
(RPO)

Recovery Time Objectives
(RTO)



RPO: 灾难发生后丢失多少数据

RTO: 灾难发生后多长时间才能恢复业务



物理机



虚拟机



云服务器

RPO

1天

分钟级-小时级

小时级-天级

RTO

数小时-数天

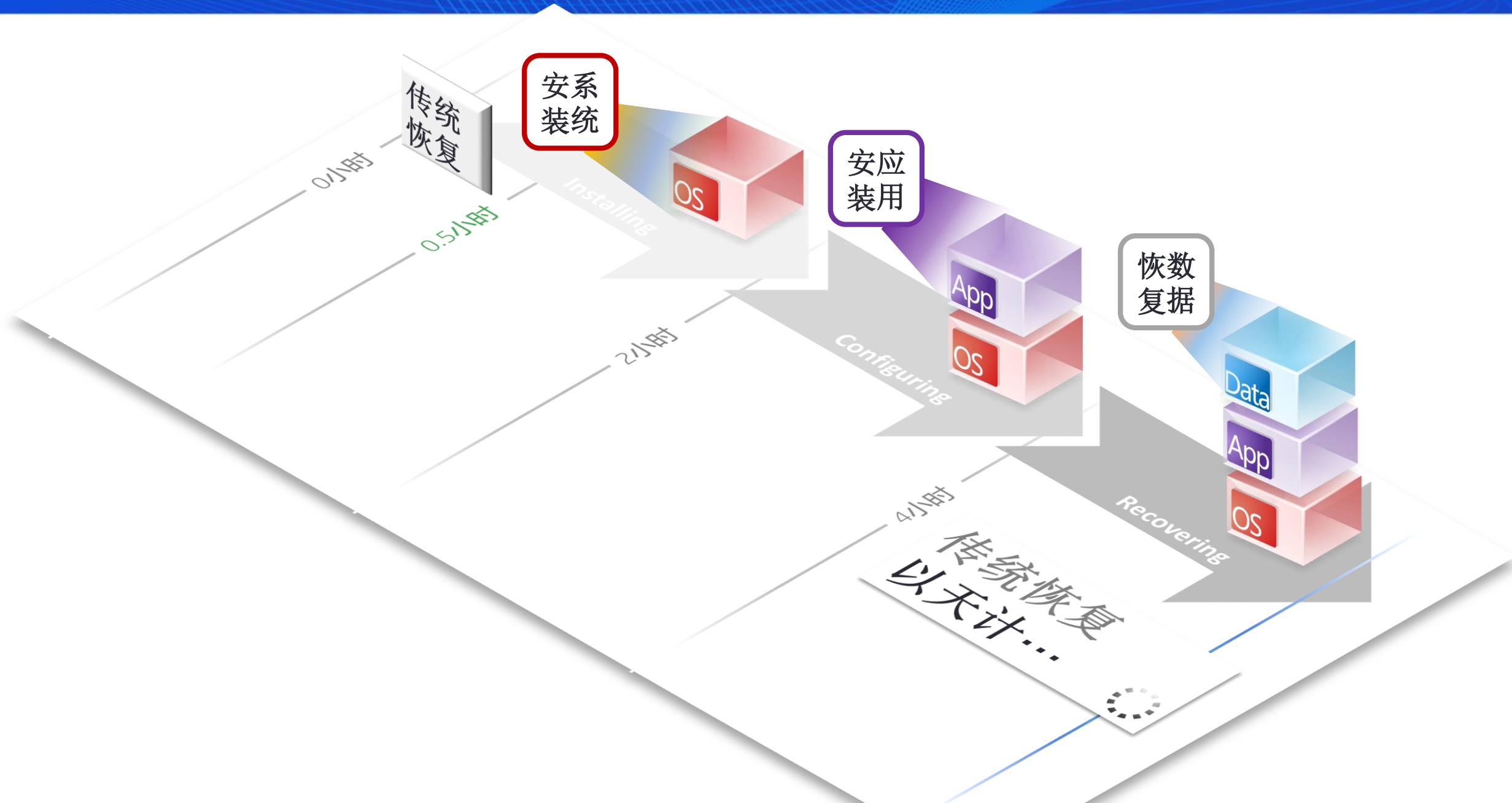
分钟级-小时级

分钟级-小时级

传统备份可恢复数据，但业务恢复漫长

2019 北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE



块级CDP

实时保护磁盘，分钟级恢复业务



物理机

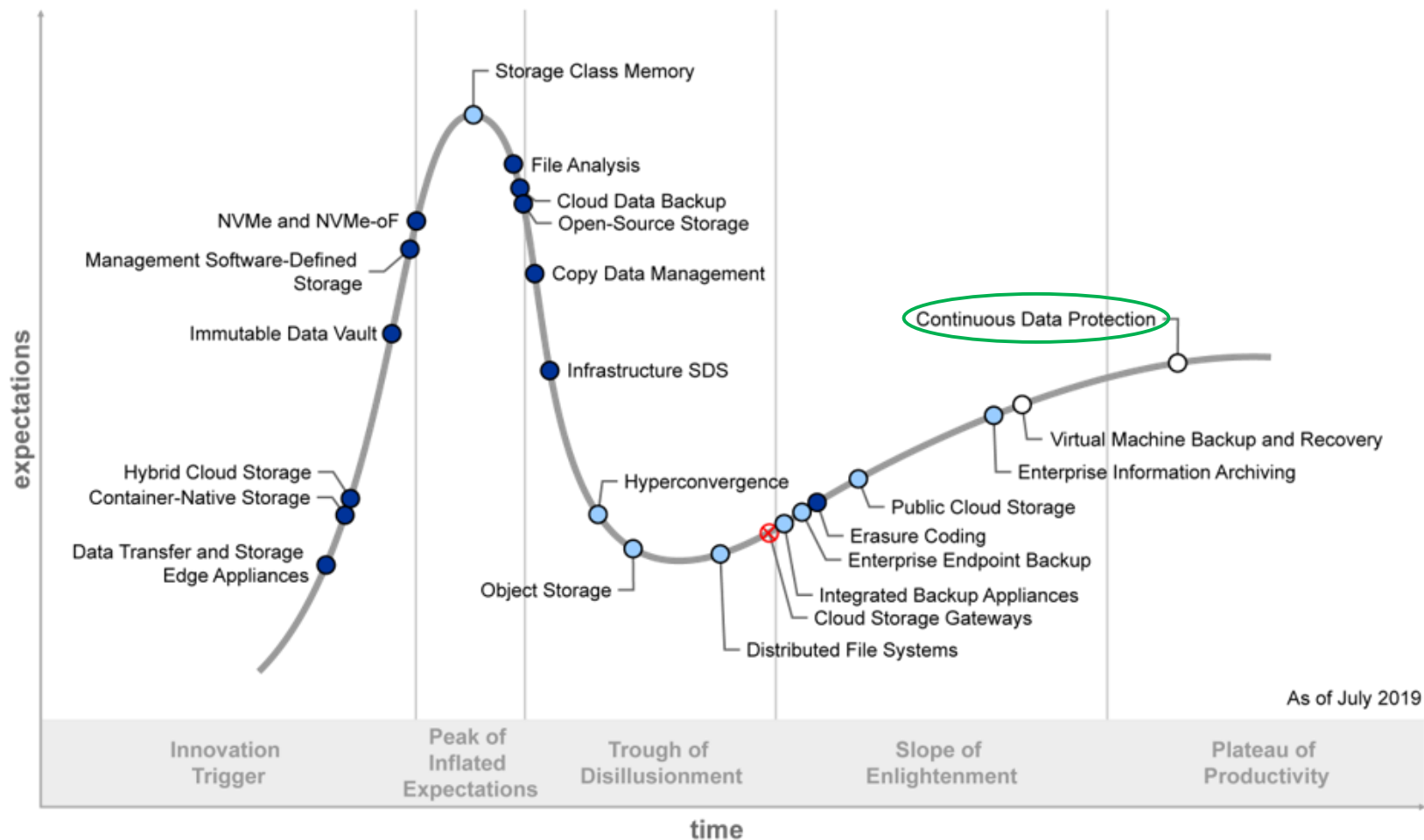


虚拟机



云服务器

Hype Cycle for Storage and Data Protection Technologies, 2019



Plateau will be reached:

○ less than 2 years ● 2 to 5 years ● 5 to 10 years ▲ more than 10 years ⊗ obsolete before plateau

块级CDP

复制原理:

当数据块写入生产数据的存储设备时，持续数据保护系统可以捕获数据的拷贝并将其存放在另外一个存储设备中。

复制粒度:

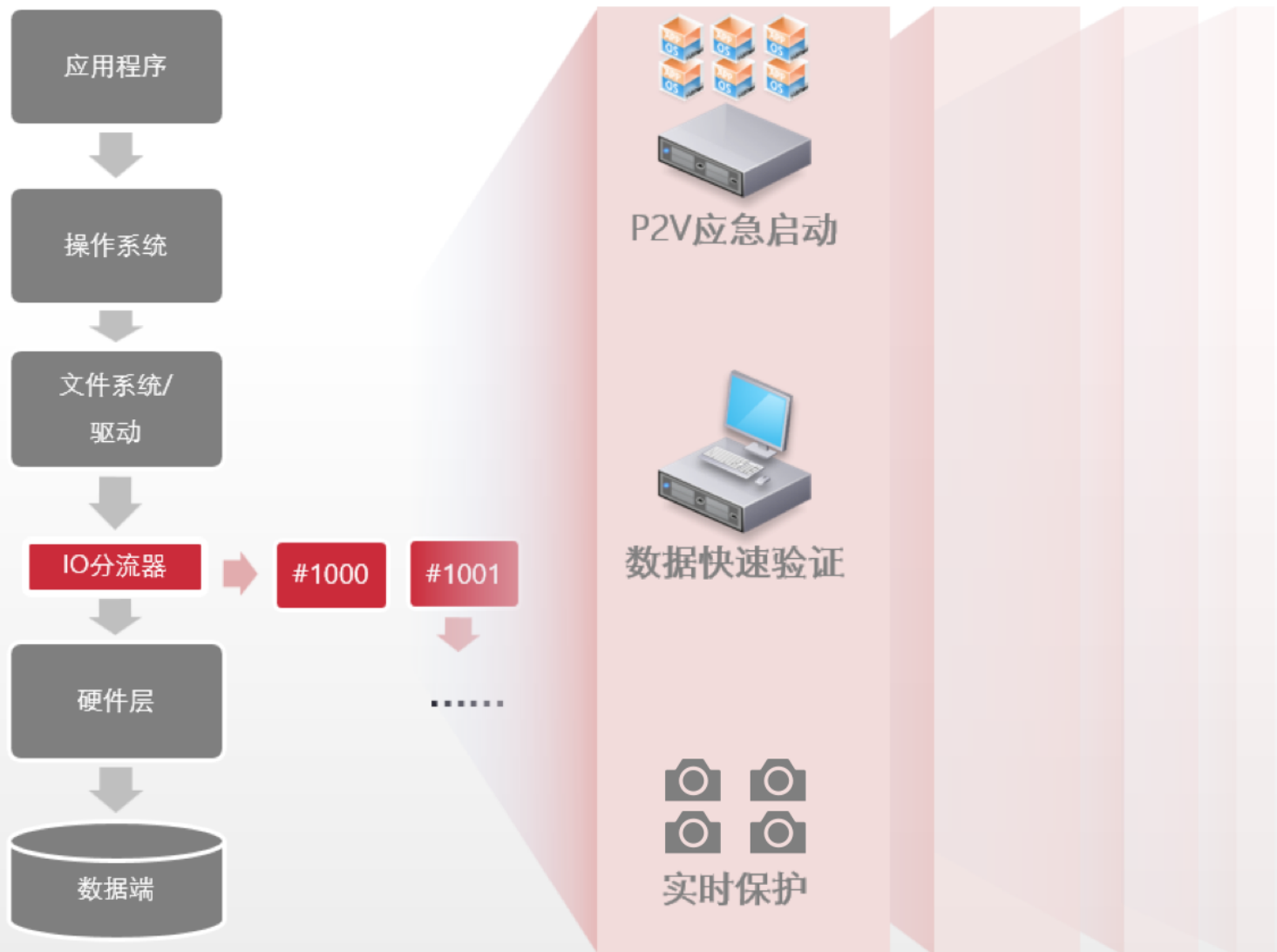
数据块级

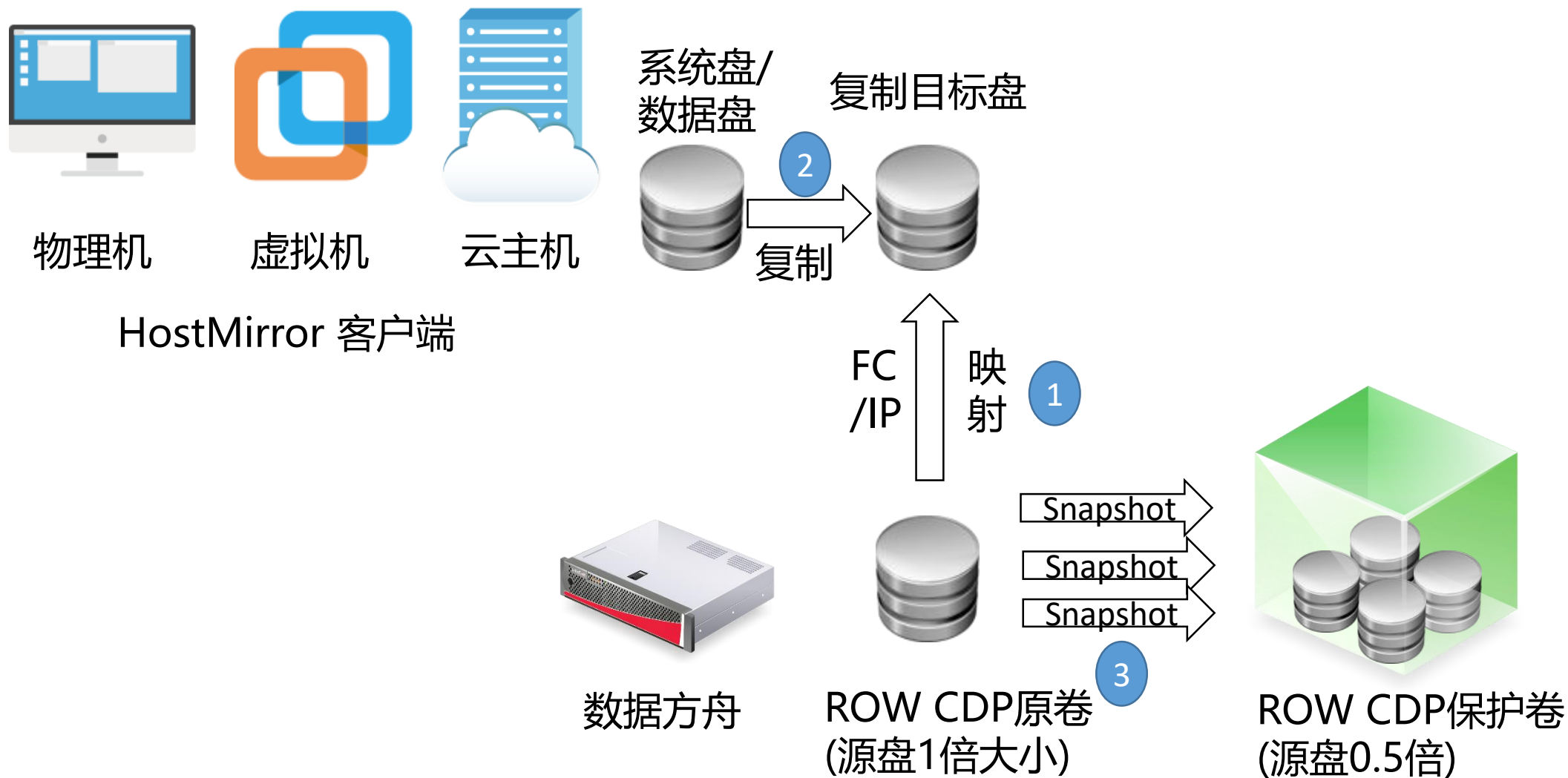
优点:

支持系统、应用、数据一体保护，
支持业务5分钟内应急恢复

缺点:

配置较多存储资源





修改任务计划

任务计划

选择开始日期: 2019/8/23 15

从 08 时 00 分开始 每 15 分钟 执行一次。

☐ 配置快照合并策略

秒
分钟
小时
天

确定

取消

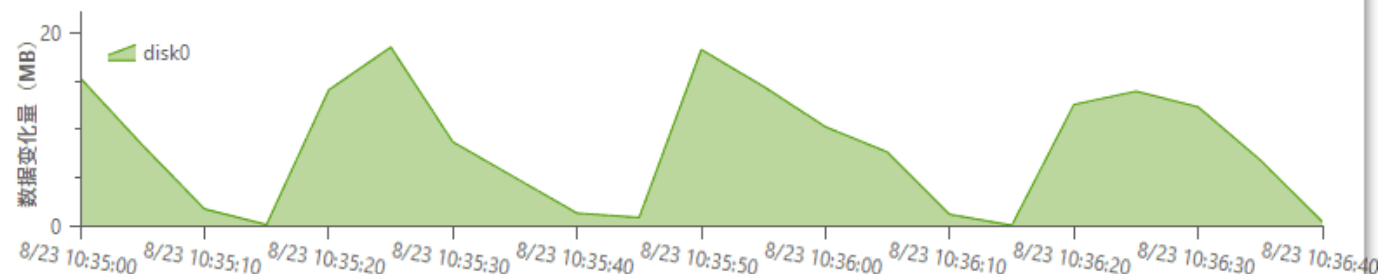
快照管理 - disk0

基本信息

碎片整理: 已启用 自动扩容: 已启用

名称	源卷大小	保存卷大小	保存卷剩余大小	备份状态
disk0	24.00 GB	48.00 GB	14.35 GB	已保护

连续保护视图



最大时间范围: 2019/08/23 09:52:25 至 2019/08/23 10:36:40

刷新

显示时间范围: 2019/08/23 10:35:00 至 2019/08/23 10:36:40

查看

选择恢复时间: 2019/08/23 10:36:40.000

恢复

快速挂载

快照列表

选择恢复状态: 全部

CDP快照总数: 501个

选择开始日期: 2019/7/23 15

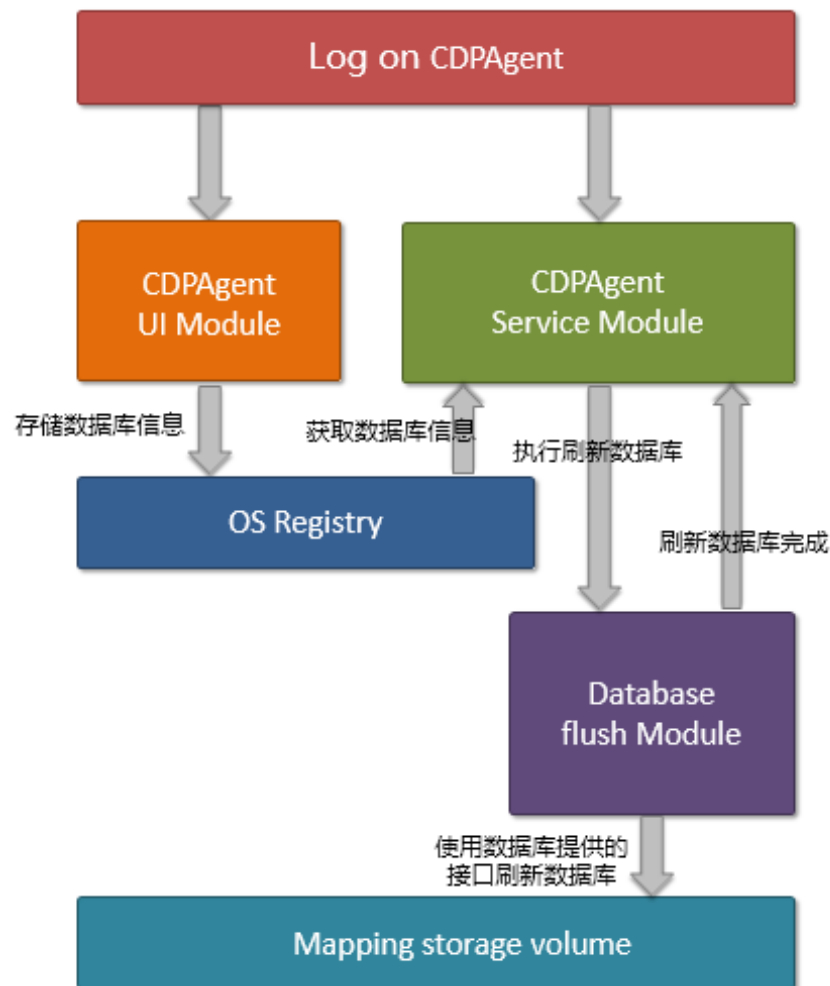
删除所有快照

创建时间	快照大小	恢复状态	使用状态	标签
2019/08/23 09:37:39	24.00 GB	未恢复	未使用	AgtMark
2019/08/23 09:38:40	7.50 MB	未恢复	未使用	AgtMark
2019/08/23 09:39:40	8.37 MB	未恢复	未使用	AgtMark
2019/08/23 09:40:40	8.68 MB	未恢复	未使用	AgtMark

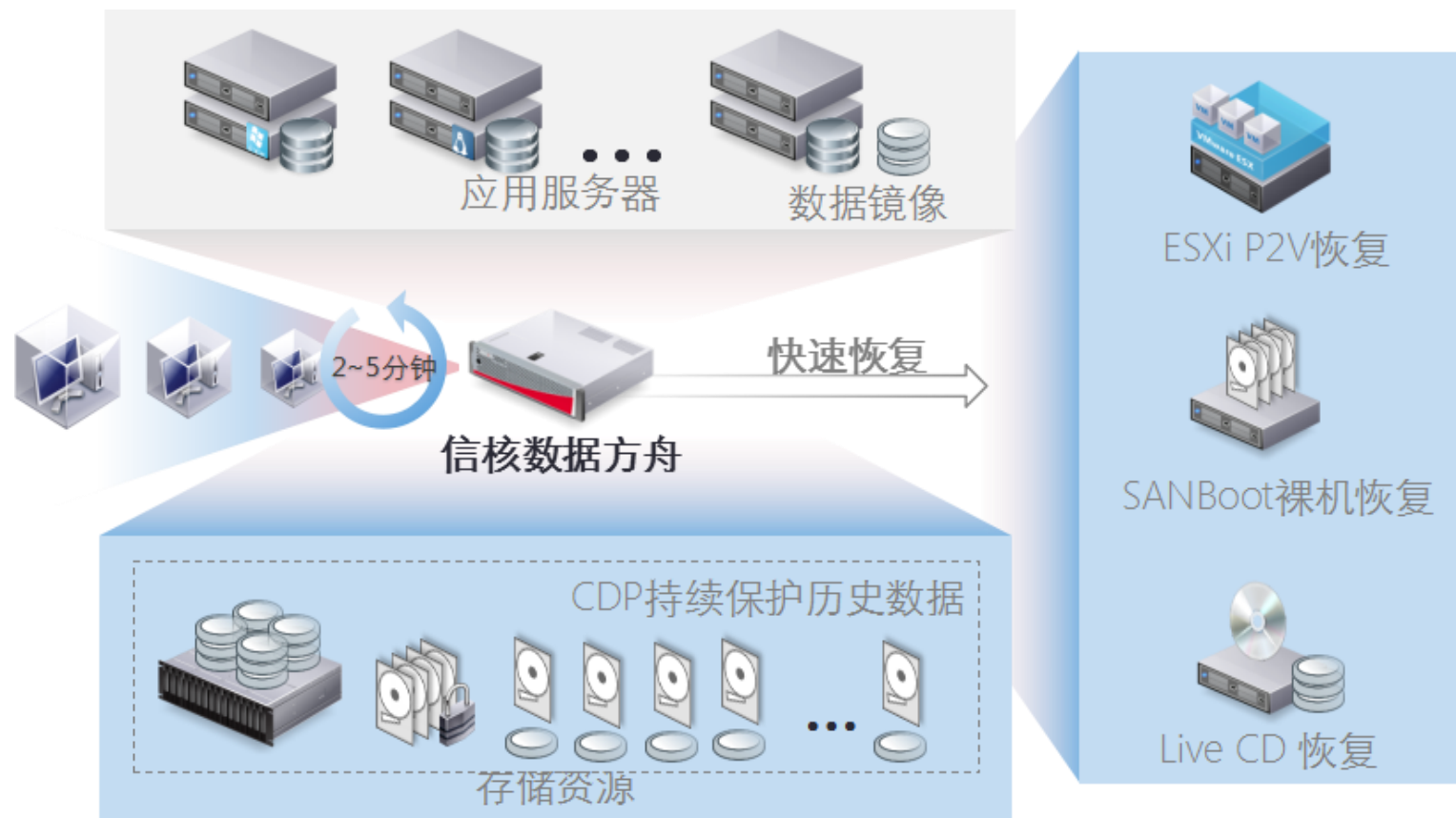
通过一致性代理按计划创建 CDP快照，创建快照之前需刷新文件系统及应用缓存数据。

保证所做的CDP快照的数据一致性。

支持主流WIN、LINUX系统及主流数据库、应用。



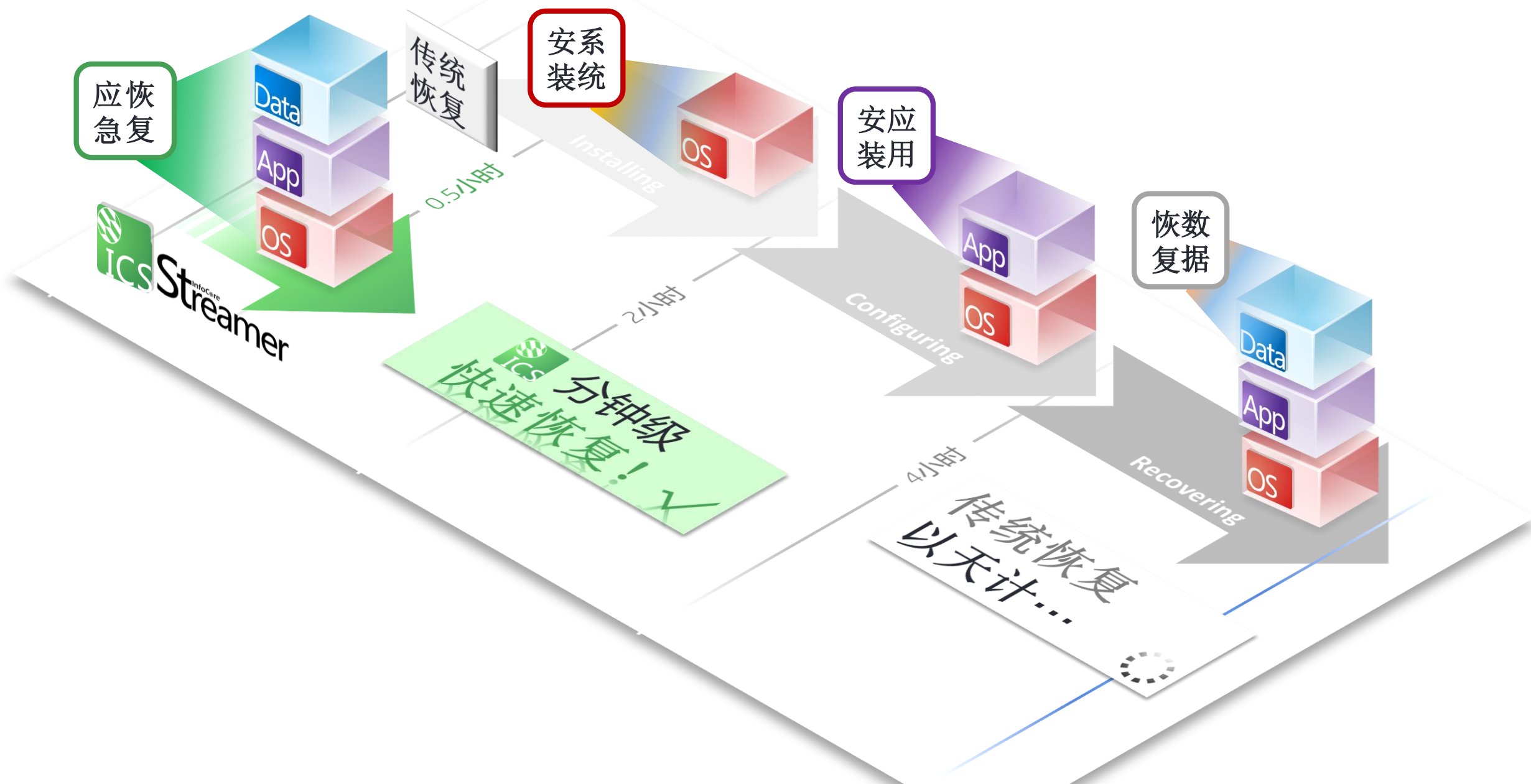
- 本地应急：5分钟一键恢复业务至内置虚机
- P2V：5分钟快速恢复业务至VMware虚机
- P2P：10分钟内SANboot恢复业务至物理机
- LiveCD：支持在线复制应急虚机数据回源主机



CDP分钟级快速应急恢复

2019 北京网络安全大会

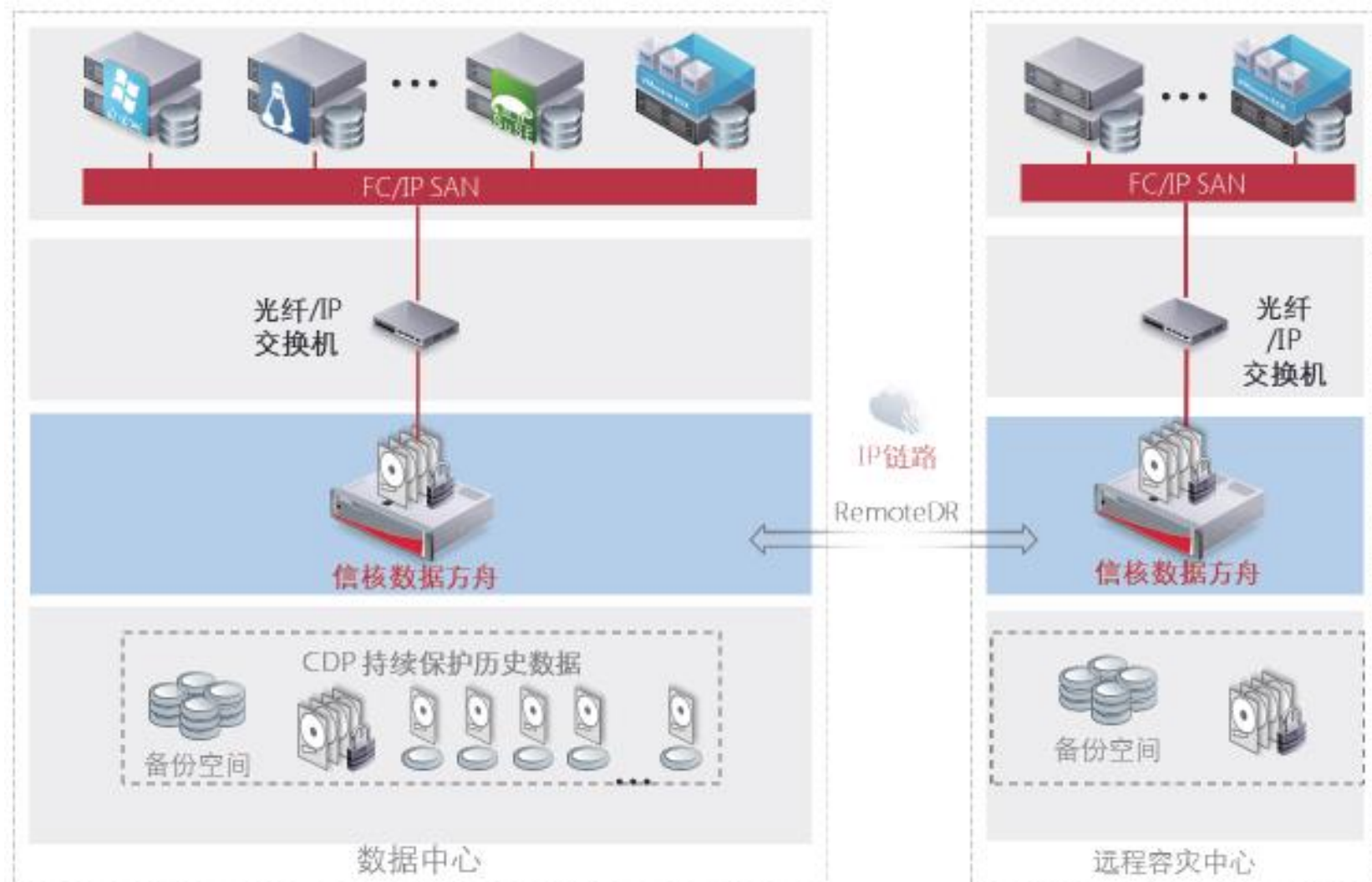
2019 BEIJING CYBER SECURITY CONFERENCE



基于Linux

支持远程容灾

支持云灾备

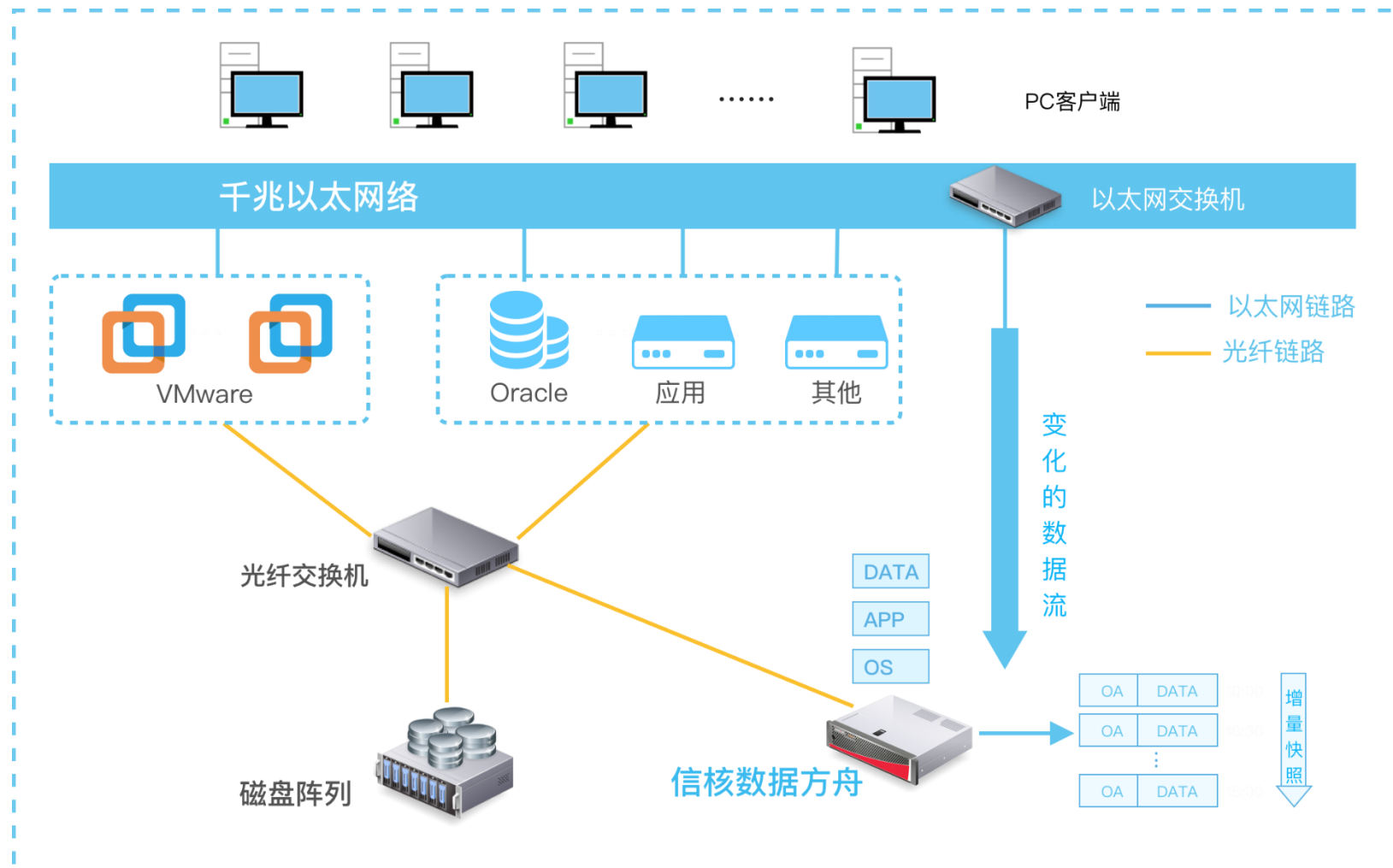


背景情况：

- 2018年1月某日，客户电商仓库出入库Oracle物理服务器被勒索病毒攻击锁死，导致无法发货。

应急处理：

- 集成商接到电话迅速赶到现场，排查问题并与客户决策用信核数据方舟上的历史快照进行恢复。发现最近第3个快照点未被感染，P2V恢复至VMware虚拟机，接管业务。2小时内客户业务恢复正常。

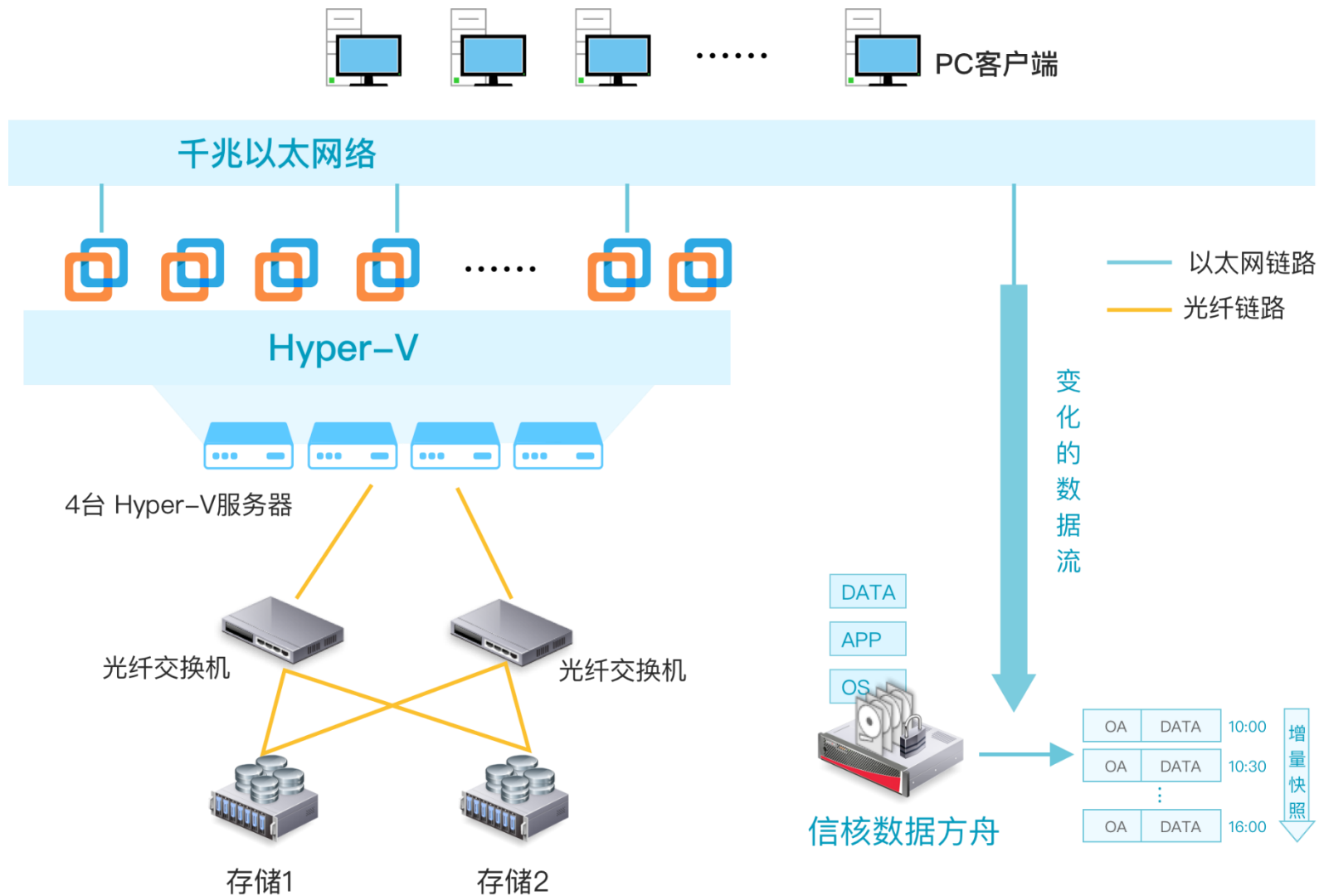


背景情况:

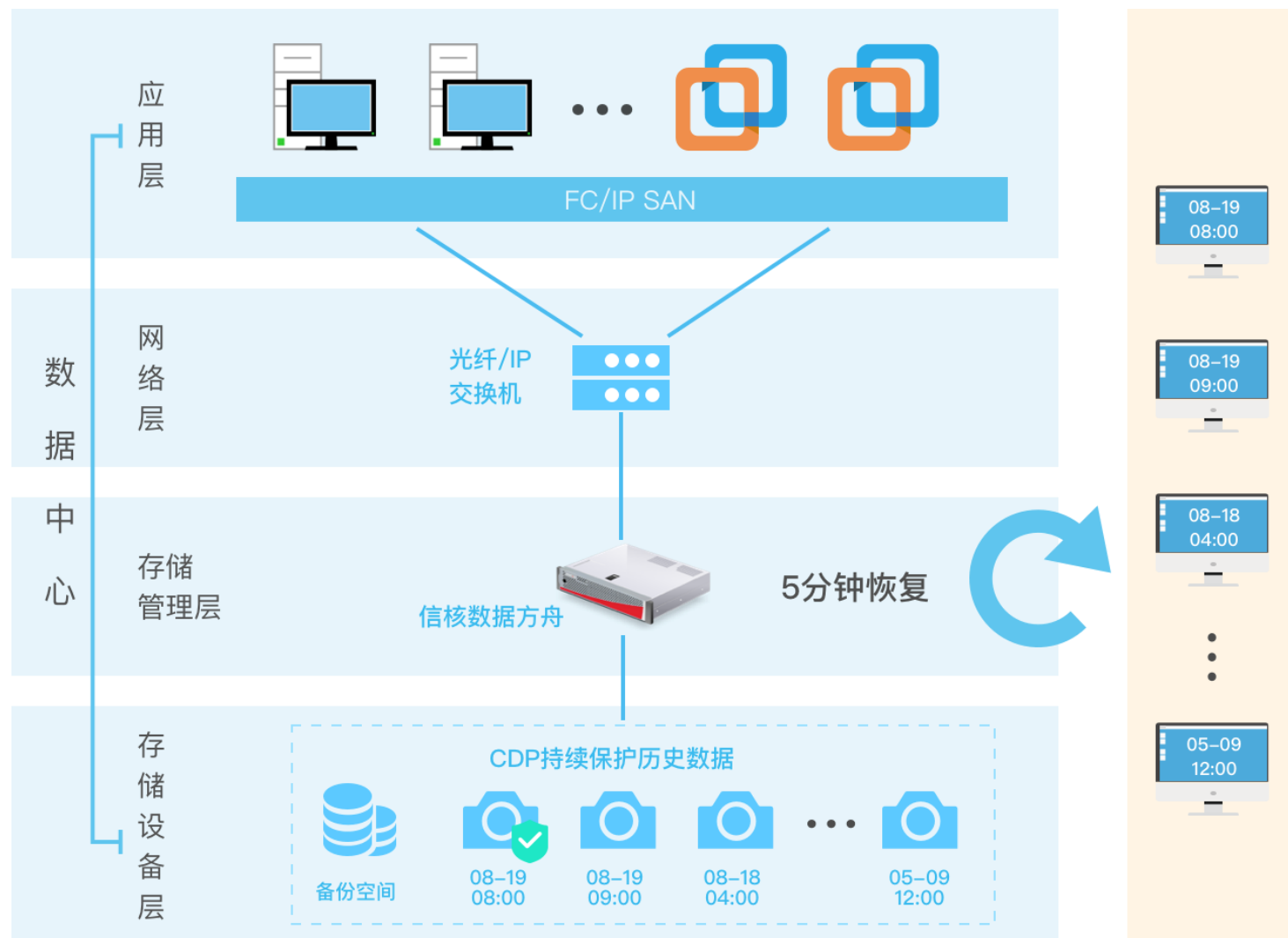
- 2019年5月某日18:00, 客户17台Win2008 R2 Hyper-V虚拟机遭到勒索病毒攻击, 无法远程登陆, 包括金蝶财务系统、设计系统TSL、SQL Server数据库及Web、OA等业务系统, 数据及系统被锁死

应急处理:

- 因该客户已部署信核数据方舟, 工程师接到求援电话后迅速赶到现场, 找到16:00时刻的快照未感染病毒, 1日内将所有17台虚拟机恢复至16:00时刻, 成功恢复客户关键数据及业务。



1. 支持保存数月甚至数年的历史快照
2. 支持系统、配置及数据的一体回滚
3. 支持一键应急恢复,方便分析攻击路径



分析攻击路径
防御二次攻击



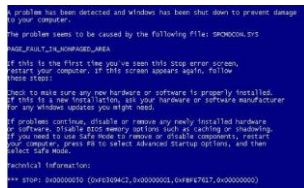
快速电子取证
主动出击



人为误操作



勒索病毒



系统崩溃



硬件故障

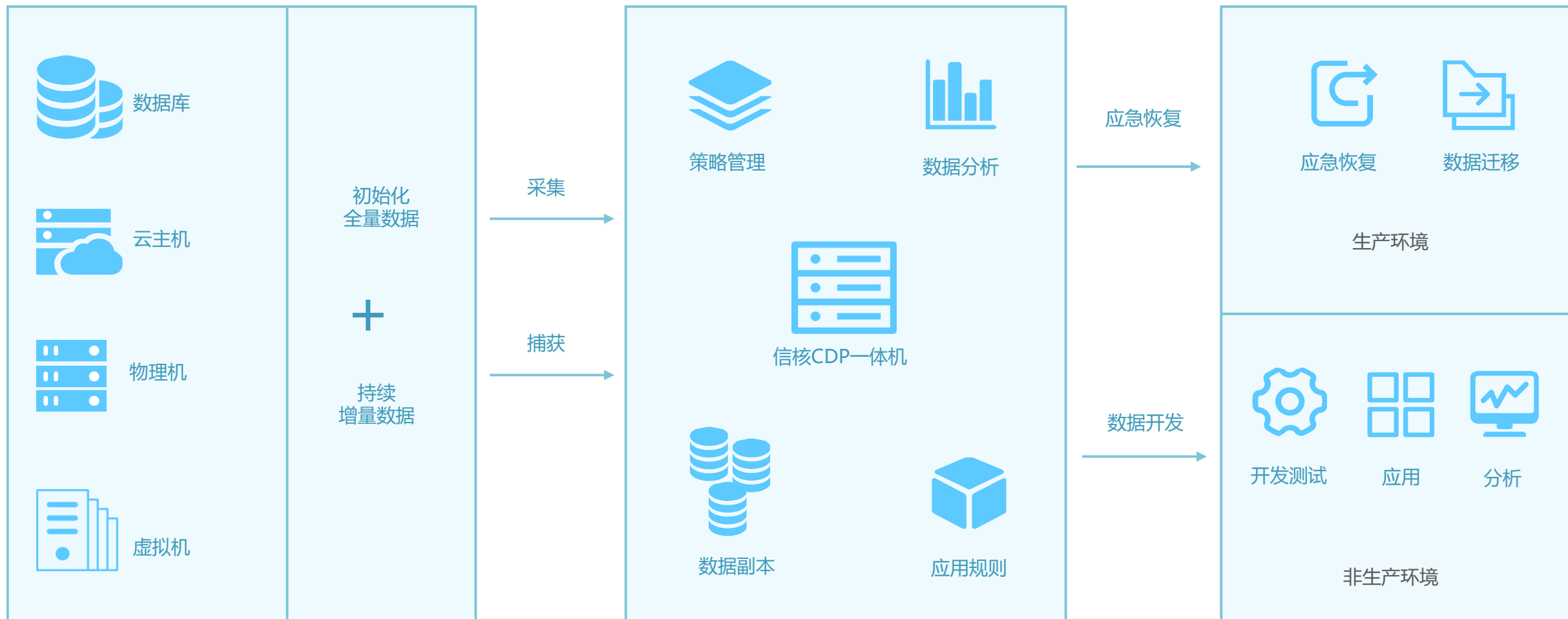


站点级灾难



信核数据方舟

持续数据保护，数十万个历史数据副本
快速校验数据，5分钟应急接管业务
支持远程容灾、云灾备



面临的问题：

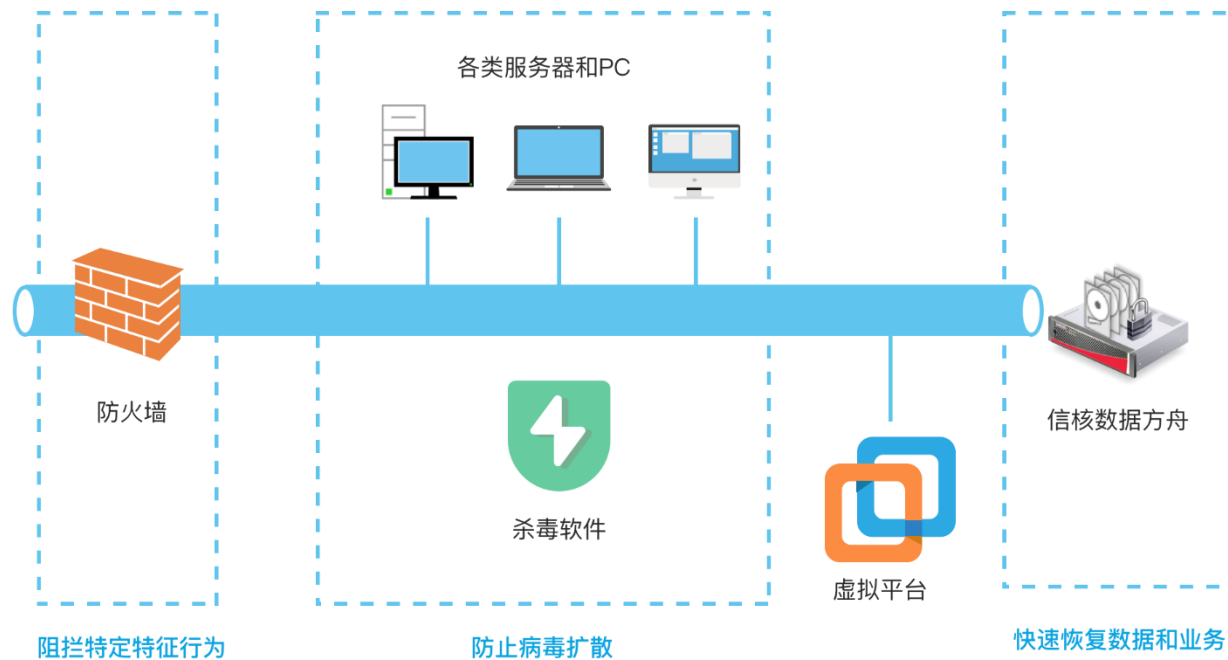
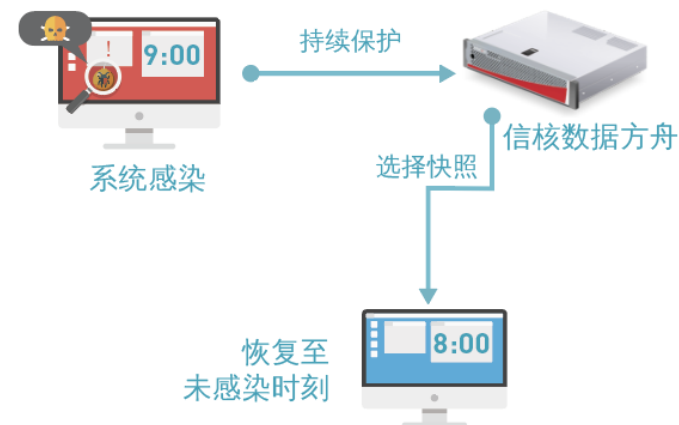
- 勒索病毒防不胜防
- 传统灾备产品往往只能恢复数据，恢复业务长达数天

解决方案：

- 部署CDP灾备产品，对关键业务主机系统和数据进行持续保护
- 如果业务系统被勒索病毒攻击锁死，选择未感染的历史副本进行快速恢复，一般1-2小时即可恢复业务
- 可调用长达数月的CDP历史快照对攻击路径进行分析

勒索病毒克星

信核数据方舟可以对业务主机提供系统级防护，已保护的主机若感染了勒索病毒，数据方舟可在分钟级内将业务恢复至感染前。




了解更多信息



关注信核数据



联系我们

The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that create a sense of depth and movement, resembling a grid or a series of overlapping planes.

THANKS

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE