SANGFOR
深信服科技

证监会152号令
《证券基金经营机构信息技术管理办法》
解读及方案

深信服 金融事业部

证券+基金行业应用汇报

证券+基金客户

- **私有云：超融合HCI/私有云aCloud**

  国泰君安、光大证券、申万宏源、西南证券、信达证券等**16**家

  招商基金、东海基金、英大基金、福安达基金、盈创投资等**7**家

- **内外部监控：云眼SAAS+安全感知SIP**

  西南证券(SAAS)、国都证券(SAAS)、东北证券(SIP)、远达证券(SIP)等**4**家

  国海富兰克林基金(SAAS)、海富通基金(SAAS)等**2**家

- **桌面虚拟化：桌面云aDesk**

  申银万国证券研究所、国泰君安证券、深圳证券、西部证券、中投证券等**18**家

  景顺长城、国开泰富、红土创新、中融基金等**4**家

- **企业移动管理：移动设备EMM**

  国金证券、中山证券、东兴证券等**3**家

  民生加银基金、景顺长城基金、国投瑞银基金等3家

- **业务负载均衡：应用交付AD**

  信达证券、中原证券、安信证券、上海证券、西南证券、国元证券等**21**家

  天弘基金、南方基金、新华基金、大成基金、东方基金、兴银基金等**17**家

- **防火墙：下一代防火墙AF**

  信达证券、深圳证券、华金证券、国都证券、深交所、浙商证券等**41**家

  中邮基金、新华基金、中信建设基金、国创基金、南方基金、华融基金、太平洋基金等**43**家

一

背景

《证券基金经营机构信息技术管理办法》（证监会152号令）“征求意见稿—正式稿—正式生效实施（2019年6月1日）”

SANGFOR 深信服科技

发布征求意见稿

2017年5月


关于就《证券基金经营机构信息技术管理办法（征求意见稿）》公开征求意见的通知

为加强证券基金经营机构、专项业务服务机构及信息技术服务机构的信息技术管理，保障证券基金行业信息系统安全、合规运行，保护投资者合法权益，我会起草了《证券基金经营机构信息技术管理办法（征求意见稿）》，现向社会公开征求意见。请将有关意见和建议以纸质或者电子邮件形式于2017年6月4日前反馈至中国证监会证券基金机构监管部。

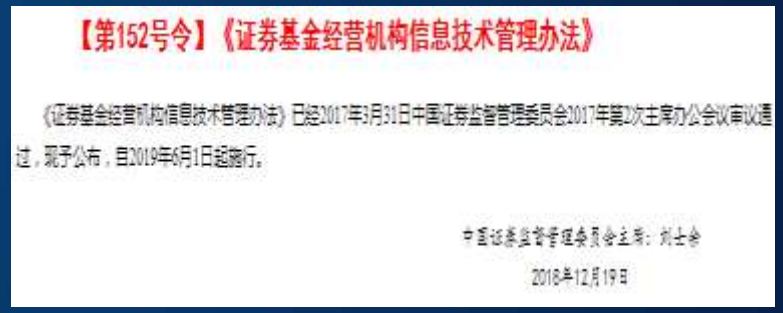
联系方式：

传真：010-88061446　　电子邮箱：jjgoubu@csrc.gov.cn

通讯地址：北京市西城区金融大街19号富凯大厦中国证监会证券基金机构监管部　邮编：100033

中国证监会

2017年5月5日


【第152号令】《证券基金经营机构信息技术管理办法》

《证券基金经营机构信息技术管理办法》已经2017年3月31日中国证券监督管理委员会2017年第3次主席办公会议审议通过，现予公布，自2019年6月1日起施行。

中国证券监督管理委员会主席：刘士余

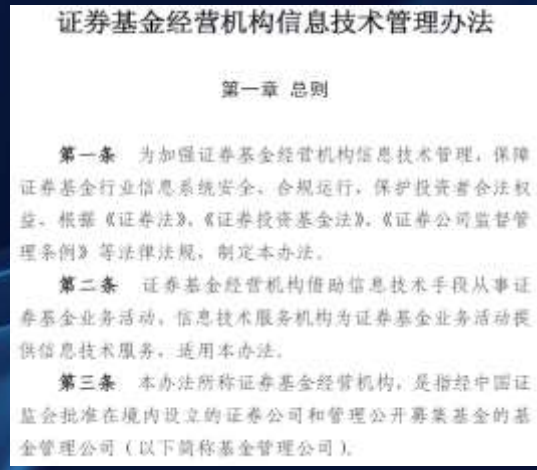
2018年12月19日

2018年12月

发布正式稿

正式生效实施

2019年6月


证券基金经营机构信息技术管理办法

第一章 总则

第一条 为加强证券基金经营机构信息技术管理，保障证券基金行业信息系统安全、合规运行，保护投资者合法权益，根据《证券法》、《证券投资基金法》、《证券公司监督管理条例》等法律法规，制定本办法。

第二条 证券基金经营机构借助信息技术手段从事证券基金业务活动，信息技术服务机构为证券基金业务活动提供信息技术服务，适用本办法。

第三条 本办法所称证券基金经营机构，是指经中国证监会批准在境内设立的证券公司和管理公开募集基金的基金管理公司（以下简称基金管理公司）。

《管理办法》7章64条管理规定：在信息技术方面明确治理、安全、合规三条主线，针对信息技术治理、数据治理、业务合规提出监管要求

SANGFOR 深信服科技

一是全面覆盖各类主体
明确信息技术监管安排，推动行业加大信息技术投入，提升竞争力

二是明确治理、安全、合规三条主线
在传统信息安全监管基础上，针对信息技术治理、数据治理、业务合规提出监管要求，明确经营机构应设立信息技术治理委员会及首席信息官，促进信息技术与业务、风控及合规管理深度融合

三是强化信息技术管理的主体责任
按照“**谁运行、谁负责，谁使用、谁负责**”**的理念**，督促经营机构与服务机构守住信息安全底线，回归本位，共同维护证券市场稳定运行

四是支持经营机构应用信息技术提升服务效能
允许经营机构设立信息技术专业子公司，允许经营机构母子公司共享信息技术基础设施，针对信息技术应用领域新情况、新问题，明确监管要求

五是强化监督管理
为督促各类市场主体切实履行自身信息技术管理职责，《管理办法》明确了相应处罚措施

《管理办法》2类被监督机构：证券基金经营机构+信息技术服务机构

SANGFOR 深信服科技

证券基金经营机构

经中国证监会批准在境内设立的证券公司和管理公开募集基金的基金管理公司

类型	数量
证券公司	131
基金管理公司	119
取得公募资格的资产管理机构	15
总计	265

地区	数量
上海	83
北京	60
深圳	48
浙江	6
广东	6
江苏	6
四川	4
广州	4
其他	48

信息技术服务机构

为证券基金业务活动提供信息技术服务的机构

信息技术服务的范围
重要信息系统的开发、测试、集成及测评
重要信息系统的运维及日常安全管理
中国证监会规定的其他情形

机构名录名单：http://www.csrc.gov.cn/pub/newsite/zjjg/hfjgml/xqhfjgml/

《管理办法》4个主管机构：证监会监督管理，证券协会/基金协会自律管理，中证信息备案、监测、检测和检查

《管理办法》处罚方式：证券基金经营机构与信息技术服务机构信息技术管理的监管要求和罚则

SANGFOR 深信服科技

第五十七条

- **证券基金经营机构**违反本办法规定的，中国证监会及其派出机构可以依法对其采取**责令改正、暂停业务、出具警示函、责令定期报告、责令增加合规检查次数、公开谴责**等行政监管措施；对直接负责的主管人员和其他责任人员采取**责令改正、监管谈话、出具警示函、公开谴责**等行政监管措施。

第五十八条

- **证券基金经营机构**违反本办法规定，反映公司治理混乱、内控失效的，中国证监会及其派出机构可以按照《证券投资基金法》第二十四条、《证券公司监督管理条例》第七十条的规定，采取**责令暂停部分或全部业务、责令更换董事、监事、高级管理人员或者限制其权利**等行政监管措施。

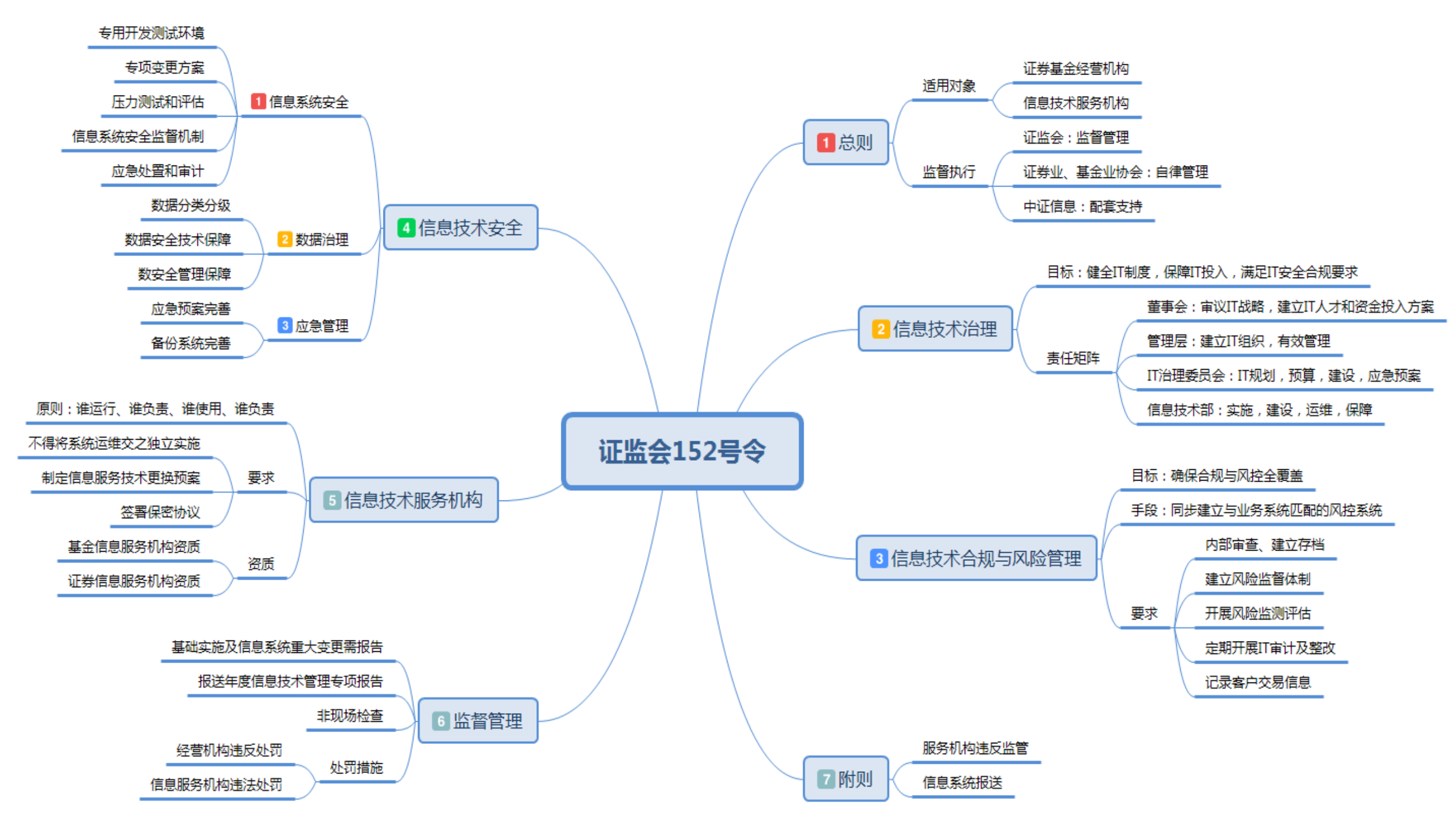
第五十九条

- **信息技术服务机构**违反本办法规定的，中国证监会及其派出机构可以要求其提交说明材料，并采取**责令改正、监管谈话、出具警示函**等行政监管措施，情节严重的，中国证监会及其派出机构可以对信息技术服务机构及其直接负责的主管人员和其他直接责任人员单处或者并处**警告、三万元以下罚款**。
- 信息技术服务机构在经营活动中无法持续符合本办法第四十七条所列条件或者违反第五十一条规定的，中国证监会及其派出机构可以**责令其改正**；拒不改正或者情节严重的，**注销备案**。

二

152号令解读

《证券基金经营机构信息技术管理办法》


证监会152号令
1 总则
适用对象
证券基金经营机构
信息技术服务机构
监督执行
证监会：监督管理
证券业、基金业协会：自律管理
中证信息：配套支持
2 信息技术治理
目标：健全IT制度，保障IT投入，满足IT安全合规要求
责任矩阵
董事会：审议IT战略，建立IT人才和资金投入方案
管理层：建立IT组织，有效管理
IT治理委员会：IT规划，预算，建设，应急预案
信息技术部：实施，建设，运维，保障
3 信息技术合规与风险管理
目标：确保合规与风险全覆盖
手段：同步建立与业务系统匹配的风控系统
要求
内部审查、建立存档
建立风险监督体制
开展风险监测评估
定期开展IT审计及整改
记录客户交易信息
4 信息技术安全
1 信息系统安全
专用开发测试环境
专项变更方案
压力测试和评估
信息系统安全监督机制
应急处置和审计
2 数据治理
数据分类分级
数据安全技术保障
数安全管理保障
3 应急管理
应急预案完善
备份系统完善
5 信息技术服务机构
要求
原则：谁运行、谁负责、谁使用、谁负责
不得将系统运维交之独立实施
制定信息服务技术更换预案
签署保密协议
资质
基金信息服务机构资质
证券信息服务机构资质
6 监督管理
基础实施及信息系统重大变更需报告
报送年度信息技术管理专项报告
非现场检查
处罚措施
经营机构违反处罚
信息服务机构违法处罚
7 附则
服务机构违反监管
信息系统报送

证券基金经营机构信息技术体系架构

SANGFOR 深信服科技

一、总则

- 法律法规
- 适用范围
- 责任主体
- 监管方式

二、信息技术治理

- 管理制度和操作流程
- 信息技术管理层
- 信息技术部门

三、信息技术合规与风险管理

- 信息技术合规管理机制
- 系统设计合规
- 风险监测系统

四、信息技术安全

4.1信息系统安全

- 专用开发测试环境
- 上线或变更流程
- 重要信息系统压力测试
- 信息系统安全监测机制
- 信息系统日志留痕可审计

4.2数据治理

- 组织架构和生命周期管理
- 数据安全管理制度
- 数据分类分级
- 数据安全保障措施
- 合规审查及风险控制
- 数据挖掘、梳理和分析

4.3应急管理

- 业务连续性管理
- 业务连续性计划
- 系统及数据备份机制
- 灾难灾害应对能力
- 安全事件的分级响应

五、信息技术服务机构

- 风险隔离要求
- 备案、自律、禁止性

六、监督管理

- 监管报送
- 监督管理、罚则

七、附则

- 实施时间
- 过渡期安排

第一到三章：总则+信息技术治理+信息技术合规与风险管理

SANGFOR 深信服科技

（一）总则

《办法》明确了立法宗旨、适用范围、适用主体、监督职责以及经营机构、专项业务服务机构借助信息技术手段从事证券基金相关业务活动的主体责任

（二）信息技术治理

《办法》督促经营机构建立健全信息技术管理决策、分工、授权、制衡、持续评估等工作机制，从源头上加强信息技术应用过程中的风险管控。

- 一是要求经营机构完善信息技术治理，保障与业务活动规模、水平相适应的信息技术投入，定期评估更新信息技术规划，并持续完善信息技术管理制度和操作流程。
- 二是明确经营机构经营管理层信息技术管理责任，要求经营机构指定或任命高管人员负责信息技术管理工作。
- 三是要求经营机构设立专门部门，统一归口管理信息技术相关工作，对合规、风控、审计等部门提出了履职要求。

（三）信息技术合规与风险管理

《办法》要求经营机构将合规管理和风险控制的要求贯穿在信息技术管理各个环节。

- 一是建立事前合规审查、事中风险监测、事后评估审计的信息技术合规管理机制；
- 二是结合具体业务系统特点，确保关键“合规点”在系统设计中落在实处；
- 三是建立信息技术应用与风险控制措施的同步机制，业务信息系统必须与风险监测系统同时上线，并及时更新监测指标及预警阈值。

SANGFOR 深信服科技

（四）信息技术安全管理

第一节 信息系统安全

- 一是规范技术管理工作，明确了经营机构信息系统开发、测试、上线、部署、变更等环节的监管要求；

第二节数据治理

- 二是加强数据安全管理工作，有效保护客户信息；

第三节应急管理

- 三是加强业务连续性管理，制定业务连续性计划，优化系统及数据备份机制，提升灾难灾害应对能力。

第一节 信息系统安全-规范技术管理工作，明确了经营机构信息系统开发、测试、上线、部署、变更等环节的监管要求

SANGFOR 深信服科技

第一节信息系统安全	第21条	第二十一条 证券基金经营机构应当建立**独立于生产环境的专用开发测试环境**，避免风险传导；**开发测试环境使用未脱敏数据的，应当采取与生产环境同等的安全控制措施**。证券基金经营机构在生产环境开展重要信息系统技术或业务测试的，应对测试流程及结果进行审查。	**生产和测试分开、测试数据脱敏**
	第22条	第二十二条 证券基金经营机构重要信息系统上线或发生重大变更的，应当制定专项实施方案，并对信息系统上线或变更操作行为进行审查、确认和跟踪。 证券基金经营机构重要信息系统计划停止使用的，应当开展技术和业务影响评估，制定完整的系统停用和数据迁移保管方案，并组织必要的评审及停用后的安全检查。	**系统上线、变更、下线流程**
	第23条	第二十三条 证券基金经营机构应当结合公司发展战略、市场交易规模等因素定期对重要信息系统开展压力测试和评估分析，确保其容量满足业务开展需要。	**定期开展压力测试**
	第24条	第二十四条 证券基金经营机构应当**建立健全信息系统安全监测机制，设定监测指标并持续监测重要信息系统的运行状况**。证券基金经营机构应当指定专人跟踪监测发现的异常情形，及时处置并定期开展评估分析。	**信息系统安全监测机制**
	第25条	第二十五条 证券基金经营机构应当妥善保存信息系统开发、测试、上线、变更及运维过程中产生的文档，并根据业务开展情况以及信息系统的重要程度建立与监测工作相适应的日志留痕机制，确保满足应急处置和审计需要	**文档保存、日志留痕**
	第26条	第二十六条 证券基金经营机构重要信息系统部署以及所承载数据的管理，应当遵循法律法规等规定。	**文档保存、日志留痕**
	第27条	第二十七条 证券基金经营机构可以在安全、合规的前提下为子公司提供机房、通信网络及其他信息技术基础设施，并协助开展相关运维工作。证券基金经营机构为其子公司提供信息技术服务的，应当充分评估信息技术基础设施的支撑能力与冗余程度，并与子公司签订服务协议，明确合作双方的权利义务，以及建立日常协作、业务隔离和应急管理机制，防范基础设施共用产生的新增风险。 证券基金经营机构可以设立信息技术专业子公司，为母公司提供信息技术服务。信息技术专业子公司经中国证监会备案后可为其他金融机构提供信息技术服务。	**为子公司提供IT的要求** **合同、职责、业务隔离、应急预案** **信息技术专业子公司：服务母公司，备案后方可服务其他经营机构**
	第28条	第二十八条 证券基金经营机构应当确保重要信息系统具备可审计功能，并可以根据监管部门的要求转换、提供数据。	**日志审计**

第二节 数据治理-加强数据安全管理工作，有效保护客户信息

第二节数据治理	第29条	第二十九条 证券基金经营机构应当结合公司发展战略，建立全面、科学、有效的数据治理组织架构以及数据全生命周期管理机制，确保数据统一管理、持续可控和安全存储，切实履行数据安全及数据质量管理职责，不断提升数据使用价值。	**数据全生生命周期管理理机制**
	第30条	第三十条 证券基金经营机构应当将经营及客户数据按照重要性和敏感性进行分类分级，并根据**不同类别和级别作出差异化数据管理**制度安排。	**重要、敏敏感分类分级 差异化数据管理理制度**
	第31条	第三十一条 证券基金经营机构应当完善**网络隔离、用户认证、访问控制、数据加密、数据备份、数据销毁、日志记录、病毒防范和非法入侵检测**等安全保障措施，保护经营数据和客户信息安全，防范信息泄露与损毁。	**数据加密、数据备份、数据销毁 日志记录**
	第32条	第三十二条 证券基金经营机构应当遵循最少功能以及最小权限等原则分配信息系统管理、操作和访问权限，并履行审批流程。合规管理和风险管理部门应当对权限管理制度和操作流程进行合规审查及风险控制。证券基金经营机构应当建立对信息系统权限的定期检查与核对机制，确保用户权限与其工作职责相匹配，防止出现授权不当的情形。 证券基金经营机构应当**对重要信息系统的开发、测试、运维实施必要分离**，保证信息技术管理部门内部岗位的相互制衡。	**最少功能以及最小小权限 权限审批流程 定期权限检查与核对**
	第33条	第三十三条 证券基金经营机构应当记录经营数据和客户信息的使用情况，并持续监督信息技术服务机构等相关方落实保密协议的情况。证券基金经营机构发现其他机构、个人违规存储或使用自身经营数据和客户信息的，应当排查数据泄露途径、评估影响范围，采取合理可行的整改措施，及时处置风险隐患，并按照中国证监会规定履行报告和调查处理职责。 证券基金经营机构发现信息技术服务机构等相关方违规存储或者使用自身经营数据和客户信息的，应当责令其立即改正并销毁已获取的经营数据和客户信息；信息技术服务机构等相关方拒绝配合整改的，证券基金经营机构应当立即停止与其合作，并采取措施维护自身及客户的合法权益。	**记录数据使用用情况 违规数据使用用发现 泄漏漏溯源分析能力力力**
	第34条	第三十四条 证券基金经营机构应当建立健全数据安全管理制度，不得收集与服务无关的客户信息，不得购买或使用非法获取或来源不明的数据。在收集使用客户信息之前，证券基金经营机构应当公开收集、使用的规则和目的，并征得客户同意。 除法律法规和中国证监会另有规定外，证券基金经营机构不得允许或者配合其他机构、个人截取、留存客户信息，不得以任何方式向其他机构、个人提供客户信息。	**数据来源安全、用用户授权**
	第35条	第三十五条 证券基金经营机构应当充分挖掘、梳理和分析数据内容，提高管理精细化程度，在业务经营、风险管理与内部控制中加强数据应用，实现同一客户、同类业务统一管理，充分发挥数据价值。	**不不得提供客户信息**

第三节 应急管理-加强业务连续性管理，制定业务连续性计划，优化系统及数据备份机制，提升灾难灾害应对能力

SANGFOR 深信服科技

第三节应急管理	第36条	第三十六条 证券基金经营机构借助信息技术手段从事证券基金业务活动的，应当建立信息技术应急管理的组织架构，确定重要业务及其恢复目标，制定应急预案，配置充足资源，稳妥处置信息技术突发事件，并积极开展应急演练和信息技术应急管理的评估与改进。	**目标-建立应急组织、建立应急预案**
	第37条	第三十七条 证券基金经营机构应当落实下列应急管理职责： （一）信息技术管理部门为信息技术应急管理的牵头组织部门，组织开展信息技术应急预案的制定、演练、评估与改进工作，并负责信息系统的应急响应与恢复； （二）各业务部门负责评估本业务条线信息技术突发事 件相关风险，开展业务影响分析，确定并实施重要业务恢复目标和恢复策略； （三）风险管理部门负责评估信息系统与相关业务恢复目标和恢复策略制定的合理性，确保与公司整体风险管理策略保持一致。	**责任主体:** **1.IT部门：牵头** **2.业务部门：BIA、确定恢复目标和恢复策略** **3.风险管理部：评估**
	第38条	第三十八条 证券基金经营机构应当制定并持续完善应急预案，包括应急管理建设目标、备份信息系统建设和恢复机制、备份数据恢复机制、业务恢复或替代措施、应急联系方式、与客户沟通方式、向监管部门及有关单位的报告路径、应急预案披露与更新机制等内容。 证券基金经营机构应急预案应当充分考虑重要信息系统故障、相关信息技术服务机构无法继续提供服务、证券基金经营机构信息技术高管或重要技术团队发生重大变动以及自然灾害等可能影响重要信息系统平稳运行的事件。	**总体要求：** **1.制定、完善应急预案，持续更新** **2.每年开展应急演练**
	第39条	第三十九条 证券基金经营机构应当根据系统变更、业务变化等情况，持续更新应急预案。 证券基金经营机构应当根据应急预案定期组织关键岗位人员开展应急演练，演练频率不低于每年一次，并确保应急演练在两年内覆盖全部重要信息系统。应急演练应当形成报告，保存期限不得少于五年。	**每年开展应急演练**
	第40条	第四十条 证券基金经营机构应当在公司网站、客户交易终端等渠道公示信息技术突发事件发生时客户可采取的替代交易方式等信息，提示客户防范和应对可能出现的风险。	
	第41条	第四十一条 **证券基金经营机构应当确保备份系统与生产系统具备同等的处理能力，保持备份数据与原始数据的一致性。重要信息系统应当符合下列信息系统备份能力等级要求：** **（一）实时信息系统、非实时信息系统的数据备份能力应当达到第一级；** **（二）非实时信息系统的故障应对能力应当达到第二级；** **（三）证券公司实时信息系统的故障应对能力应当达到** **第四级，基金管理公司实时信息系统的故障应对能力应当达到第三级；** **（四）实时信息系统、非实时信息系统应当具备灾难及重大灾难应对能力，相关技术指标应当分别达到灾难应对能力第五级、重大灾难应对能力第六级；** **（五）灾难应对能力可以通过重大灾难应对能力体现，但重大灾难应对能力相关技术指标应当达到灾难应对能力第五级。**	**建立同城灾备/异地灾备，处理能力与生产等同**
	第42条	第四十二条 证券基金经营机构应当按照中国证监会有关规定，建立信息安全事件的分级响应机制，明确内部处置工作流程，确保相关信息系统及时恢复运行。	**系统灾备能力：灾备应对能力第五级、重大灾难应对能力第六级**

第五到七章：信息技术服务机构+监督管理+附则

（五）信息技术服务机构

《办法》主要围绕专项业务服务机构开展的专项业务服务提出监管要求，包括开展专项业务活动的信息系统与其兼营业务相关信息系统之间的风险隔离要求、开展专项业务活动的信息技术人员及信息安全保障要求、开展信息技术风险评估以及应急处置的相关要求等。

- 一是明确了经营机构委托信息技术服务机构提供信息技术服务的范围和选取要求；
- 二是明确了基金信息技术服务机构备案有关事项；
- 三是明确了证券信息技术服务机构可以自愿申请加入证券业协会并接受协会的自律管理；
- 四是规范了经营机构的信息技术服务协议、服务管理、应急处置有关事项；
- 五是明确了经营机构委托信息技术服务机构提供信息技术服务的禁止性要求。

（六）监督管理

《办法》明确了对证券基金经营与服务机构信息技术管理的监管要求和罚则。根据现行法律法规授权，对信息技术服务机构作了相应的监管安排。

- 一是规定经营机构、专项业务服务机构关键信息基础设施、与证券基金交易相关的信息系统及提供信息系统外部接入的备案要求；
- 二是明确证券基金经营与服务机构的报告职责和流程要求；
- 三是规定中国证监会及其派出机构可以采取现场检查、组织应急演练、监管评价等监管手段，对证券基金经营与服务机构借助信息技术手段从事证券基金相关业务活动或者提供信息技术服务实施监督管理；
- 四是根据证券基金经营与服务机构违规的具体情形，明确罚则。

（七）附则

- 明确了名词释义、实施时间、参照执行的主体及过渡期安排等事项。

三

信息系统安全解决方案

信息系统安全——关键需求及设计思路

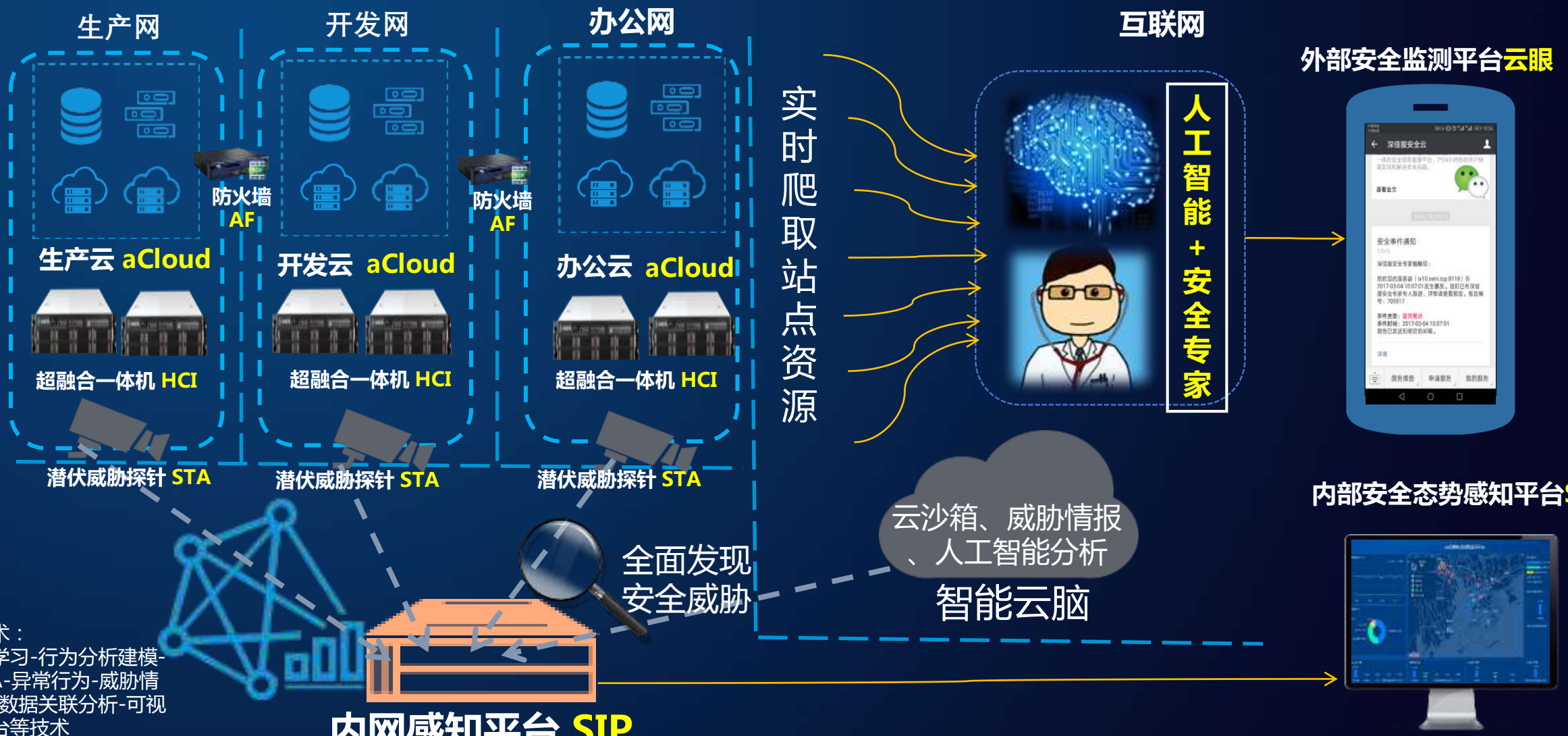
SANGFOR 深信服科技

要求	问题	解决方案
第二十一条 •证券基金经营机构应当建立独立于生产环境的专用开发测试环境，避免风险传导；开发测试环境使用未脱敏数据的，应当采取与生产环境同等的安全控制措施。证券基金经营机构在生产环境开展重要信息系统技术或业务测试的，应对测试流程及结果进行审查	**未建立独立于生产环境的专用开发测试环境** •未建立独立于生产环境的专用开发测试环境，存在风险传导威胁 •开发测试环境使用未脱敏数据的，未当采取与生产环境同等的安全控制措施 •在生产环境开展重要信息系统技术或业务测试的，未对测试流程及结果进行审	**优化、整合现有资源，构建合规安全的专用开发测试环境** 服务器整合、虚拟化 采用超融合技术HCI，建立独立开发测试环境 采用下一代防火墙AF，与生产网/办公网逻辑隔离
第二十四条 •证券基金经营机构应当建立健全信息系统安全监测机制，设定监测指标并持续监测重要信息系统的运行状况。证券基金经营机构应当指定专人跟踪监测发现的异常情形，及时处置并定期开展评估分析	**未建立健全信息系统安全监测机制** •未建立健全信息系统安全监测机制，设定监测指标并持续监测重要信息系统的运行状况。证券基金经营机构应当指定专人跟踪监测发现的异常情形，及时处置并定期开展评估分析	**部署内外部监控工具，完善信息系统安全监测机制** 采用云眼技术SAAS构建外部监测机制 采用安全态势感知技术SIP构建内部监测机制

信息系统安全整体框架：以专用开发测试环境+安全隔离为核心，以外部+内部安全监测机制为切入，保障金融信息系统安全

SANGFOR 深信服科技

采用超融合技术快速构建专用开发测试环境，采用云眼技术构建外部监测机制，态势感知技术构建内部监测机制



关键技术01：超融合技术

深信服超融合HCI架构，快速构建企业级私有云aCloud

开发测试云数据中心

核心系统 二代支付 开户 查询 视频会议 日程安排 在线培训 源代码仓库 数据仓储 人事

aCloud 云平台

资源编排管理 分级分权管理 运营服务化管理 异构资源管理

超融合基础架构

计算虚拟化 aSV

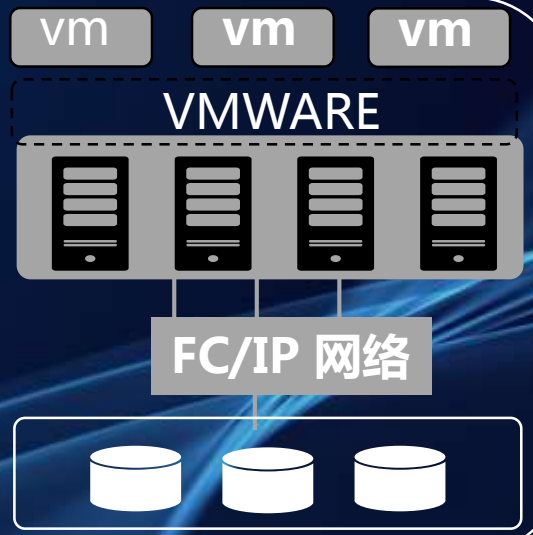
存储虚拟化 aSAN

网络虚拟化 aNET

安全虚拟化 NFV

超融合一体机 超融合一体机 超融合一体机

传统基础架构



传统数据中心 vs 超融合数据中心

传统数据中心

极简 随需应变 平滑演进

超融合数据中心

金融超融合数据中心建设步骤

SANGFOR 深信服科技

01 计算和存储的融合（极简的建设）

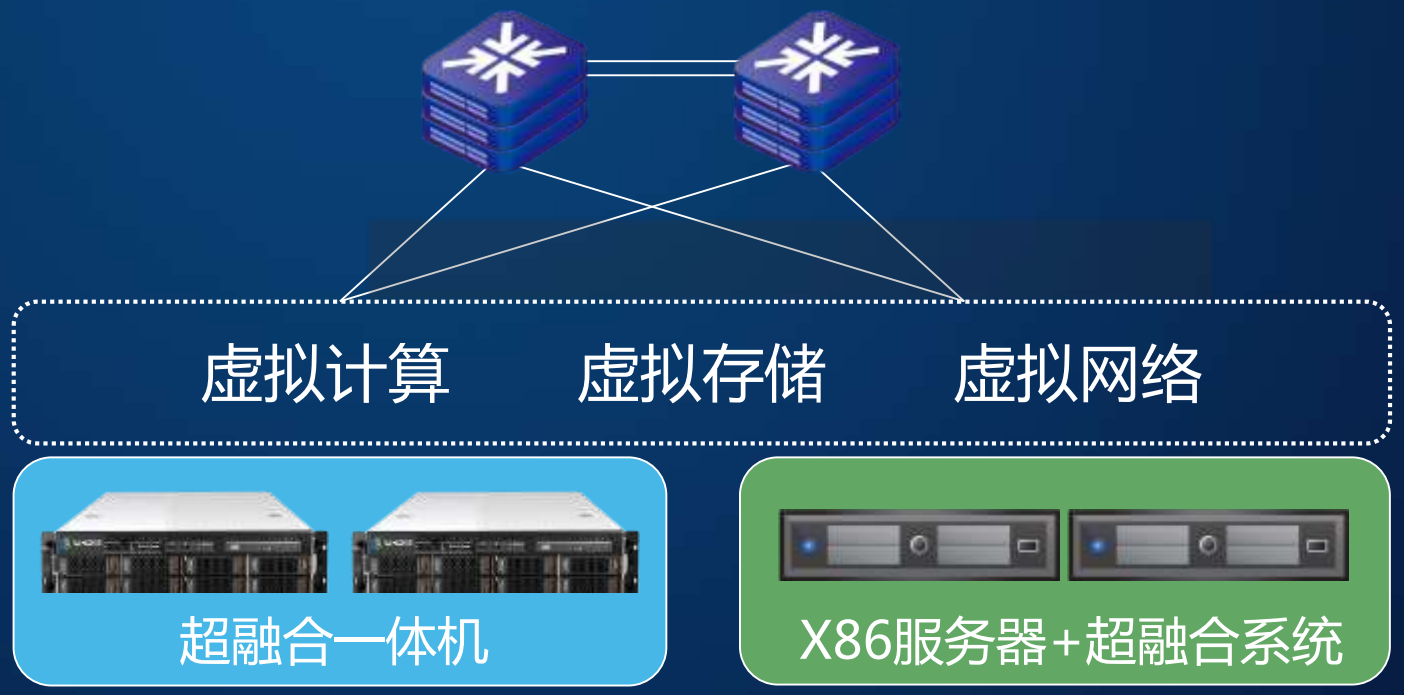
02 利用迁移工具将业务迁到超融合上

03 网络和NFV组件的融合

04 自动化运维管理/排障

05 模块化弹性扩展（纵向和横向）

第一步 计算和存储的融合（极简平台）



设计思路

- 部署几台超融合一体机，先把新建业务和利旧服务器上的业务系统迁上去；
- 利旧服务器做改造（支持VT-x），建议配备6个GE+2个10GE，1块480G SSD+2到3块4T HDD；
- 小型机保留原架构，基于x86的HIS、PACS等可放心迁移。

第二步 利用迁移工具将业务迁到超融合上

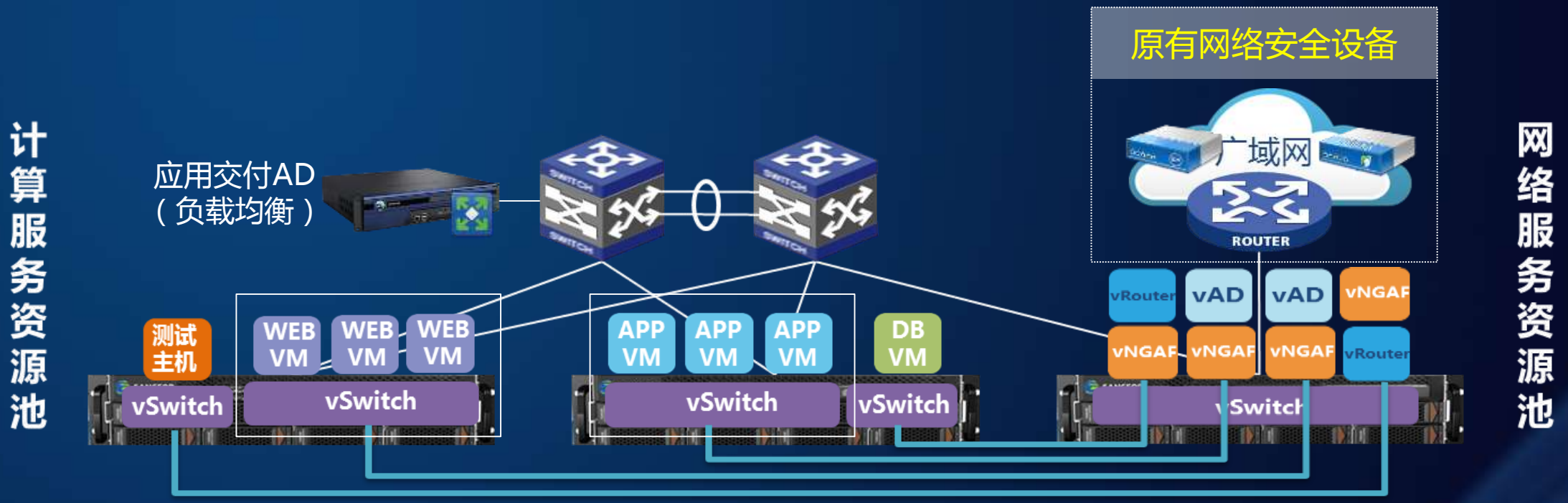
虚拟机转虚拟机V2V

支持VMware、Xen、Hyper-V、其他厂商的KVM

物理机转虚拟机P2V

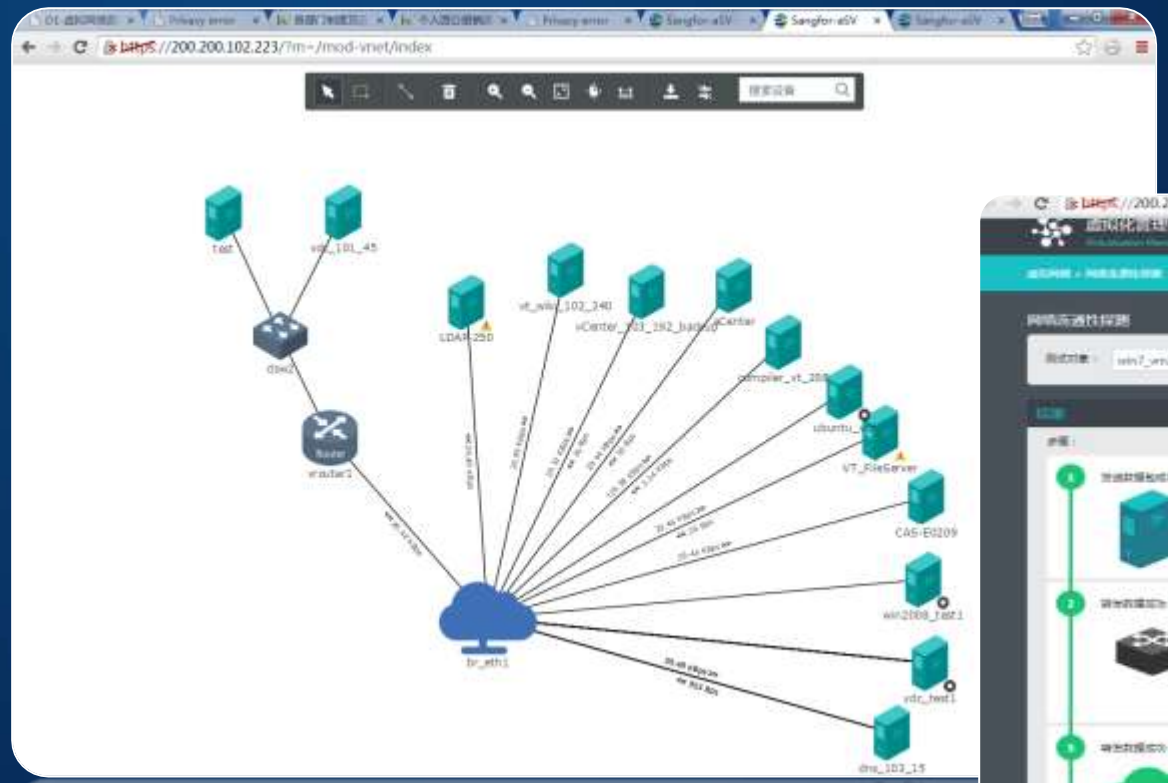
支持业界主流操作系统，一般转换时间70MB/S

第三步 网络和NFV的融合（深度集成）



- 原有安全设备无需丢弃，可部署于边界，提供南北向流量的安全防护。同时，新增下一代防火墙NGAF等NFV组件，提供东西向流量（虚机之间）的安全防护。
- HIS、PACS等核心系统建议部署多台虚机，前端通过硬件AD或虚拟AD实现更专业的负载均衡（稳定、安全、高效的交付核心应用）。

第四步 集中监控和自动化管理

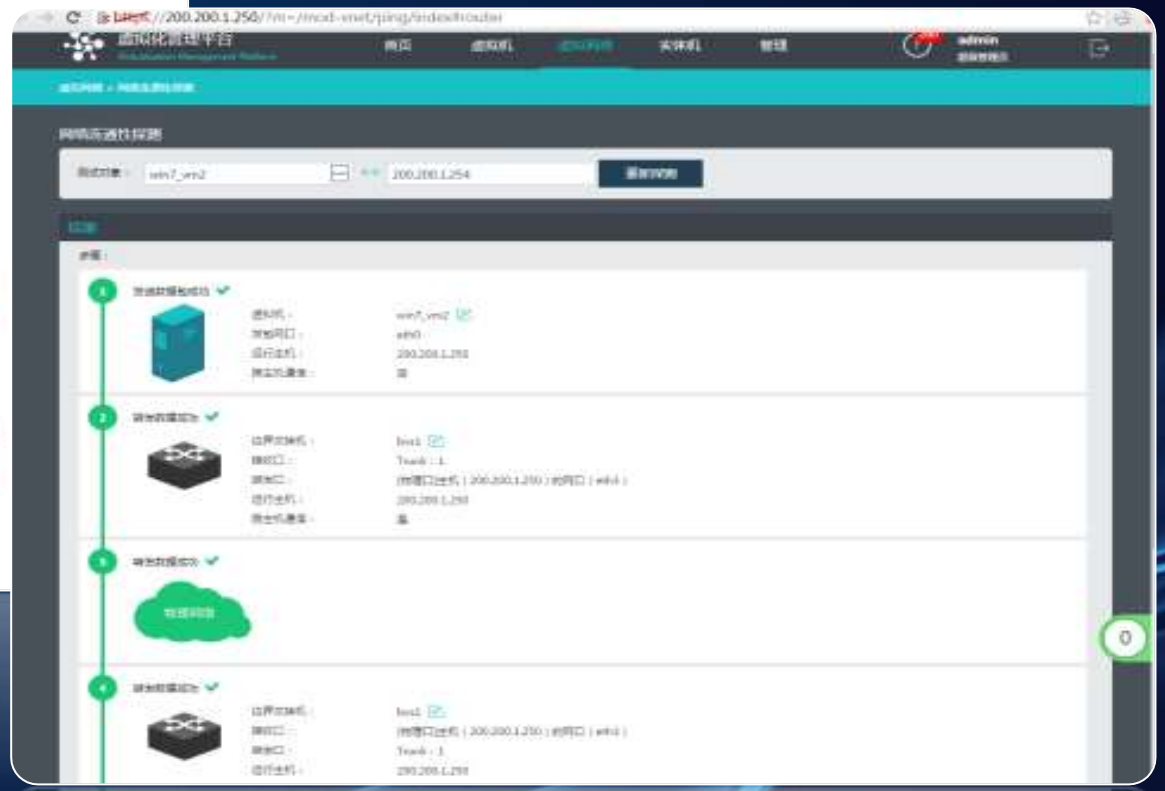


全网流量可视

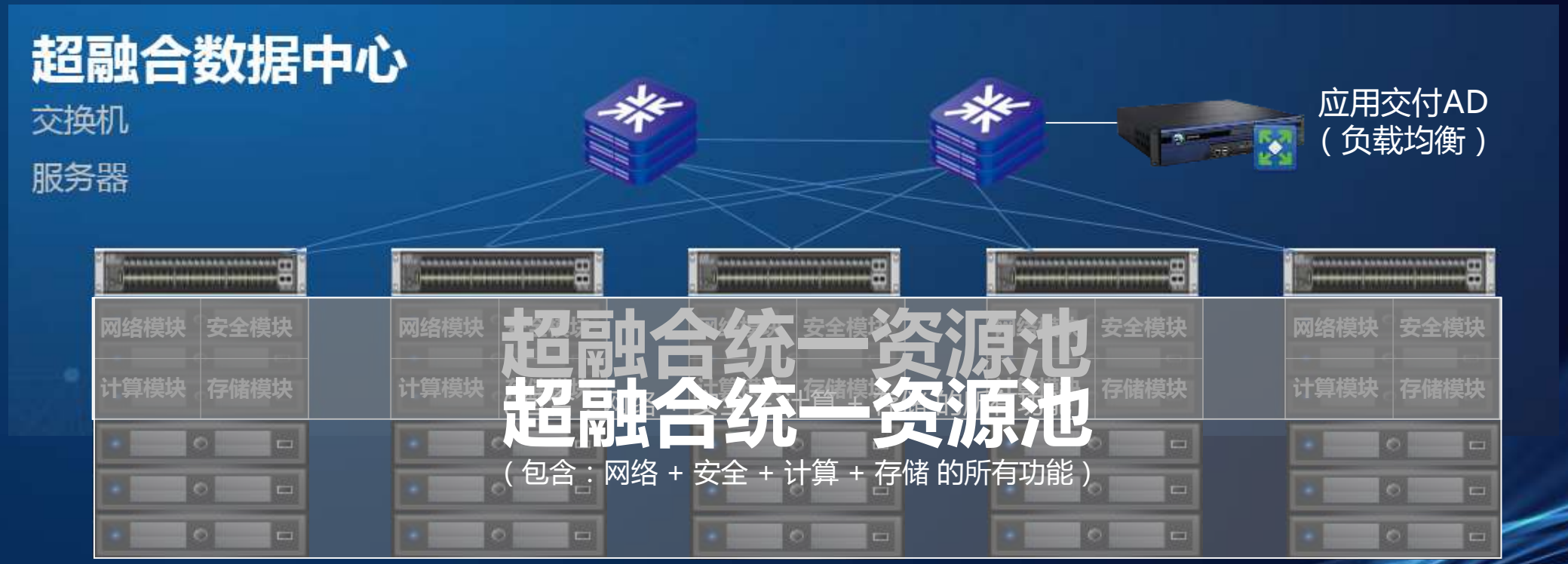
基于虚拟机端口、上下行链路实时显示流量

连通性探测工具

基于源、目的，实现连通性探测并定位故障



第五步 模块化弹性扩展（纵向和横向）



步骤：A、添加超融合节点；B、数据自动平衡；
C、DRX动态资源扩展（单虚机）或AD负载均衡灵活调度（多虚机）。

专业服务金融行业客户

SANGFOR 深信服科技

海通期货

开发测试系统
小规模试用

深度合作
100C+规模

光大期货有限公司 EVERBRIGHT FUTURES CO.,LTD.

兼容性对接
HP服务器承载

银期互联业务
更高的稳定性
USB KEY兼容

国泰君安证券股份有限公司 Guotai Junan Securities CO.,LTD.

固定收益业务
上海+香港

衍生品交易业务
仿真业务

富安达基金管理有限公司 FUANDA FUND MANAGEMENT CO.,LTD

开发测试系统
利旧服务器对接——开发测试、办公

关键技术02：外部主动监测技术

云眼集安全评估、监测、告警为一体，实时监测网站安全状态，提供可持续感知的资产变化、事前风险、事后入侵事件，提前发现风险

SANGFOR 深信服科技

持续评估　实时监测　篡改监测　应急响应　全局可视

核心技术1：持续评估，从定期评估，转为“持续评估”，减少风险暴露周期，减少被利用机会

SANGFOR 深信服科技

- 暴露面
- 脆弱性
- 内容安全

新业务上线，会进行首次全面评估，并做为基线，每天持续复查

每日持续评估

- 高危风险持续复查
- 资产变更持续检测

前期高危漏洞是否已修复；是否有新上线的资产、业务、页面模块。及时发现影子资产和新增漏洞。

新增资产增量评估

- 新增资产增量评估

发现资产变更后，自动对“变动资产”进行增量评估。减少新漏洞在网上暴露时间。

- 暴露面
- 脆弱性
- 内容安全

每月一次整体运营情况总结，让用户掌握业务系统风险总况。

上线评估

每月评估

核心技术2：持续加固，保持最优防护状态，精准拦截恶意攻击

核心技术3：主动响应，发生即发现，发现即处理，实时监测安全事件
3-5分钟内生成可视化报告，主动响应并告知用户

SANGFOR 深信服科技

实时爬取站点资源

人工智能 + 安全专家

网页篡改监测
- 首页5分钟一次
- 人工审核，确保零误报

0Day监测
- 24小时内，触发式检测

网马监测
- 5分钟一次

黑链监测
- 域名首页，5分钟一次

可用性监测
- 模拟访问，3分钟一次

微信预警

关键技术03：内部主动监测技术

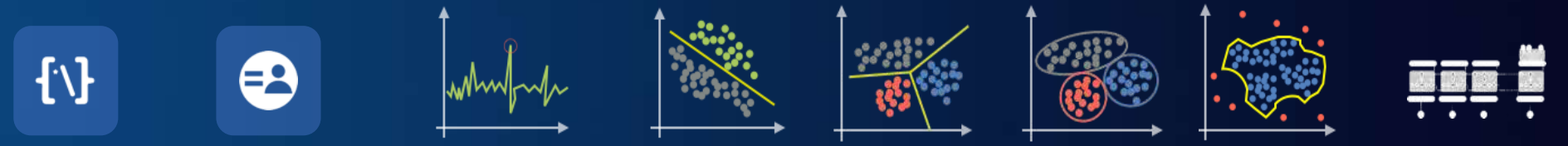
安全感知平台SIP：主动防御技术，集检测、可视、响应等多功能于一体的大数据安全分析平台和统一安全运营中心

SANGFOR 深信服科技

攻防专家

数据科学家

安全分析师



规则	特征	时间序列分析	二类分类	多类分类	聚类	离群点检测	深度学习
挖矿病毒检测	恶意URL检测	DNS放大攻击检测	扫描检测	Webshell检测	流量查毒	异常行为检测	僵尸网络检测

安全云脑

安全感知系统

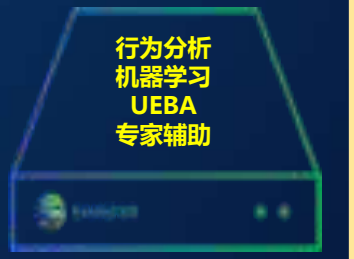
内部威胁情报 → 私有情报

数据中心 → 潜伏威胁探针

广域网 局域网 → 潜伏威胁探针

本地大脑

\+



管理平台

运维处置可视化

领导决策可视化

我现在安全吗？

哪里不安全？

造成了什么危害？

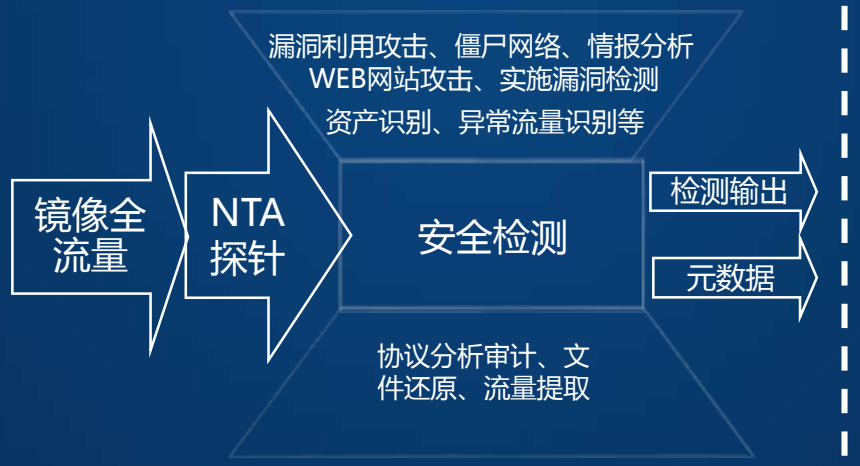
我该如何处置？

探测 → 工具 → 传送 → 漏洞利用 → 植入 → C&C → 操纵

数据采集与分析架构

SANGFOR 深信服科技

数据来源 | 数据采集 | 智能分析 | 可视与溯源



- 安全设备
- 终端安全
- 操作系统
- 中间件
- 云脑平台
- 威胁情报
- 网络设备

flow元数据

转换xFlow形式（netflow、**dnsflow、mailflow、httpflow等元数据**）

安全检测日志

安全检测日志、**审计数据、异常行为**、文件样本、**违规访问**

文件样本	审计数据
违规访问	异常行为
终端安全日志	安全设备日志
操作系统日志	中间件日志
IOC情报信息	网络设备日志

- 安全日志分析
- 文件威胁检测
- 域控行为分析
- 攻击行为分析
- 威胁情报关联
- UEBA
- Flow引擎分析
- 应用识别
- 异常流量分析

- 可视化展现
- 溯源分析展现
- 整体态势展现
- 异常与失陷主机

核心能力

SANGFOR 深信服科技

数据采集 → **持续检测** → **运维处置** → **溯源取证**

- 全流量采集
- 威胁情报
- 终端安全日志采集
- 操作系统日志采集
- 文件还原

- 漏洞攻击检测
- 文件威胁分析
- WEB攻击检测
- 异常行为分析
- 失陷主机检测
- UEBA基线学习
- 业务脆弱性分析
- 全攻击链关联

- 事件响应处置
- 安全知识库
- 事件详细举证
- 联动响应
- 安全专家
- 云沙箱联动

- ES快速搜索
- 大容量存储空间
- 流量元数据存储
- 攻击入口点溯源
- 影响面分析
- 终端日志
- 操作系统日志

三大维度的安全可视能力

SANGFOR 深信服科技

内部异常

通俗解释：内部设备（服务器+PC终端）攻击某个领域（企业内部或者企业外部）

安全事件和失陷主机	失陷主机的横向威胁	失陷主机的外连威胁
打击方式	内部攻击内部设备（内打内）	内部攻击外部互联网（内打外）
安全事件检测	横向威胁定义	外连威胁定义
失陷主机检测	攻击	攻击
服务器（业务主机）失陷	可疑行为	APT C&C 通信
终端（用户）失陷		服务器风险访问

外部攻击

通俗解释：外部互联网对企业内部进行攻击

外部攻击情况	风险访问情况
外部互联网进来破坏	外部连接进来窃取及控制
外部攻击的种类	风险应用访问
高危攻击	
暴力破解	

脆弱性

通俗解释：企业内部的漏洞

脆弱性分析
包括像弱密码-web明文-服务器漏洞
弱密码检测
web明文传输分析
服务器漏洞预警

找失陷主机、找内鬼

找绕过攻击、找攻击入口

找漏洞、找暴露面

案例1：某股份制银全行安全感知威胁检测项目，采购40+设备，部署40+分行办公网、生产网、开发网、外联网

SANGFOR 深信服科技

全攻击链监测需求

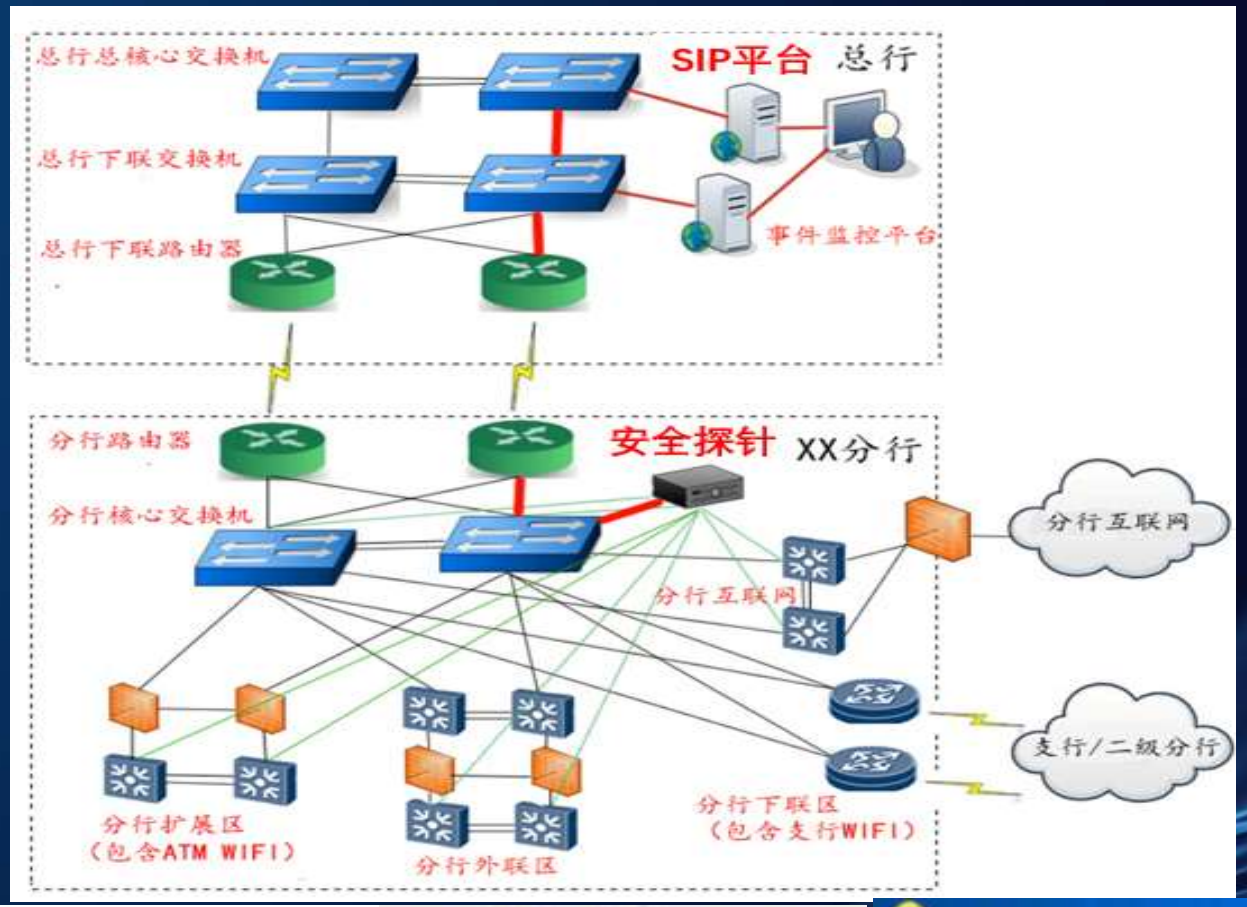
- 设备集中管理和运维
- 安全策略集中下发
- 外网攻击流量可视
- 内网攻击流量可视

解决方案

- 总行-分行办公/生产/开发/互联网
- 总行：BBC+SIP+4STA，8个流量口，5个区域生产、外联、办公、开发、外网
- 39家分行：39STA，8个流量口，5个区域分行外联、扩展、上联、下联、外网

方案效果

- 分支发现生产服务器/办公服务器失陷
- 高级webshell注入/敏感目录操作
- 内网扫描、内网SMB/RDP暴力破解
- 外网WEB漏洞攻击
- 病毒内部横向渗透



中信银行 CITIC

上海联合产权交易所 SHANGHAI UNITED ASSETS AND EQUITY EXCHANGE

中华人民共和国自然资源部

UnionPay 银联 中国银联 China UnionPay

东北证券 NORTHEAST SECURITIES

中华人民共和国审计署 National Audit Office of the People's Republic of China

专业服务金融行业客户

SANGFOR 深信服科技

中信银行全行

中国银联全国

宁波银行

新网银行

东北证券

中银消费

上海联交所

……

金融/政府/企业/医疗/教育……

四

数据治理安全解决方案

数据治理安全——关键需求及设计思路

SANGFOR 深信服科技

要求

第三十条

•证券基金经营机构应当将经营及客户数据按照重要性和敏感性进行分类分级，并根据不同类别和级别作出差异化数据管理制度安排。

第三十一条

•证券基金经营机构应当完善网络隔离、用户认证、访问控制、数据加密、数据备份、数据销毁、日志记录、病毒防范和非法入侵检测等安全保障措施，保护经营数据和客户信息安全，防范信息泄露与损毁。

第三十二条

•证券基金经营机构应当遵循最少功能以及最小权限等原则分配信息系统管理、操作和访问权限，并履行审批流程。合规管理和风险管理部门应当对权限管理制度和操作流程进行合规审查及风险控制。证券基金经营机构应当建立对信息系统权限的定期检查与核对机制，确保用户权限与其工作职责相匹配，防止出现授权不当的情形

第三十三条

•证券基金经营机构应当记录经营数据和客户信息的使用情况，并持续监督信息技术服务机构等相关方落实保密协议的情况。

•证券基金经营机构发现其他机构、个人违规存储或使用自身经营数据和客户信息的，应当排查数据泄露途径、评估影响范围，采取合理可行的整改措施，及时处置风险隐患，并按照中国证监会规定履行报告和调查处理职责。

第三十四条

•第三十四条 证券基金经营机构应当建立健全数据安全管理制度，不得收集与服务无关的客户信息，不得购买或使用非法获取或来源不明的数据。在收集使用客户信息之前，证券基金经营机构应当公开收集、使用的规则和目的，并征得客户同意。

问题

未建立敏感数据安全技术保障环境

•未对重要性和敏感性高的经营和客户数据建立高等级的安全数据保障环境

•未完善完善网络隔离、用户认证、访问控制、数据加密、数据备份、数据销毁、日志记录、病毒防范和非法入侵检测等安全保障措施

•未遵循最少功能以及最小权限等原则分配信息系统管理、操作和访问权限

未建立移动/互联网数据保障环境

•未遵循最少功能以及最小权限等原则分配信息系统管理、操作和访问权限

解决方案

构建合规安全的敏感数据安全技术保障环境

采用桌面云aDesk技术，构建开发测试敏感数据保护环境

采用桌面云aDesk技术，构建生产环境敏感数据保护环境

采用桌面云aDesk技术，构建办公环境敏感数据保护环境

构建合规安全的移动设备和互联网出口技术保障环境

采用企业移动管理EMM技术，构建移动设备数据保护环境

采用行为分析BA技术，构建互联网出口数据保护环境

深信服金融数据安全整体框架

SANGFOR 深信服科技

以重点数据重点保护为核心，以内部防泄密和外部防入侵为切入，保障金融数据流转和落地安全

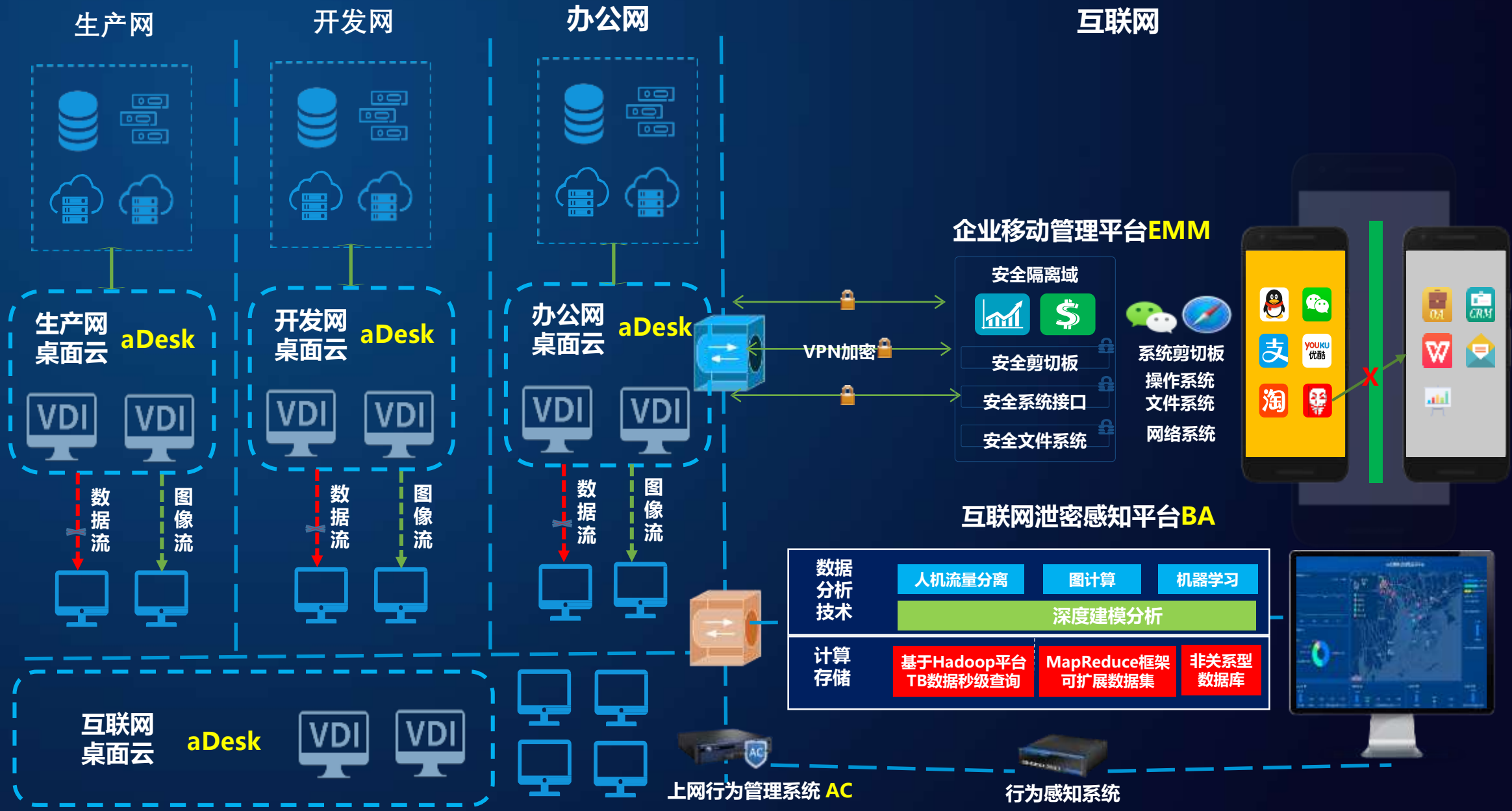
安全分级 重点数据 重点保护

用户	行内机构	外包机构	合作单位	监管机构	远程办公员工	……
用户使用安全	敏感数据不落地	数据流转可监管	拍照截屏带水印	文件外发可审计	移动终端强隔离	
终端环境	办公环境	生产环境	开发环境	测试环境	互联网环境	BYOD环境
终端操作安全	办公桌面云	生产桌面云	开发/测试桌面云	互联网桌面云	移动终端沙盒	
网络环境	办公网	生产网	开发网	测试网	互联网	移动互联网
网络传输安全	互联网敏感信息防泄密	移动互联网数据传输防泄密	邮件敏感数据外发防泄密	非法外联传输防泄密		
数据环境	客户数据	产品数据	交易数据	渠道数据	担保物数据	资本合规数据	关键统计数据	……
数据交换安全	数据安全等级划分	数据跨网络策略控制	数据流转共享控制			

内部防泄漏 外部防入侵

采用桌面云对内网重点数据进行保护，数据分析技术对外发文件分析和阻断，移动沙箱技术保护移动数据

SANGFOR 深信服科技



关键技术01：桌面虚拟化技术

深信服桌面云aDesk整体架构

SANGFOR 深信服科技

用户端


STD-100


STD-200H


STD-PRO-200H


STD-500

网络接入

传输端

SRAP

HEDC

VPN隧道


交换机

数据中心端

云桌面报表中心

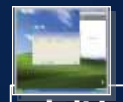
资产管理 | 策略审计 | 文档审计 | 日志管理

桌面控制器

硬件VDC | 软件VDC




VDI桌面



虚拟应用/共享桌面

虚拟化层

服务器虚拟化 | 网络虚拟化

存储虚拟化 | 安全虚拟化



硬件层


桌面云超融合服务器


英伟达


信锐智能交换机

aCenter

集中授权

统一升级

全局模板

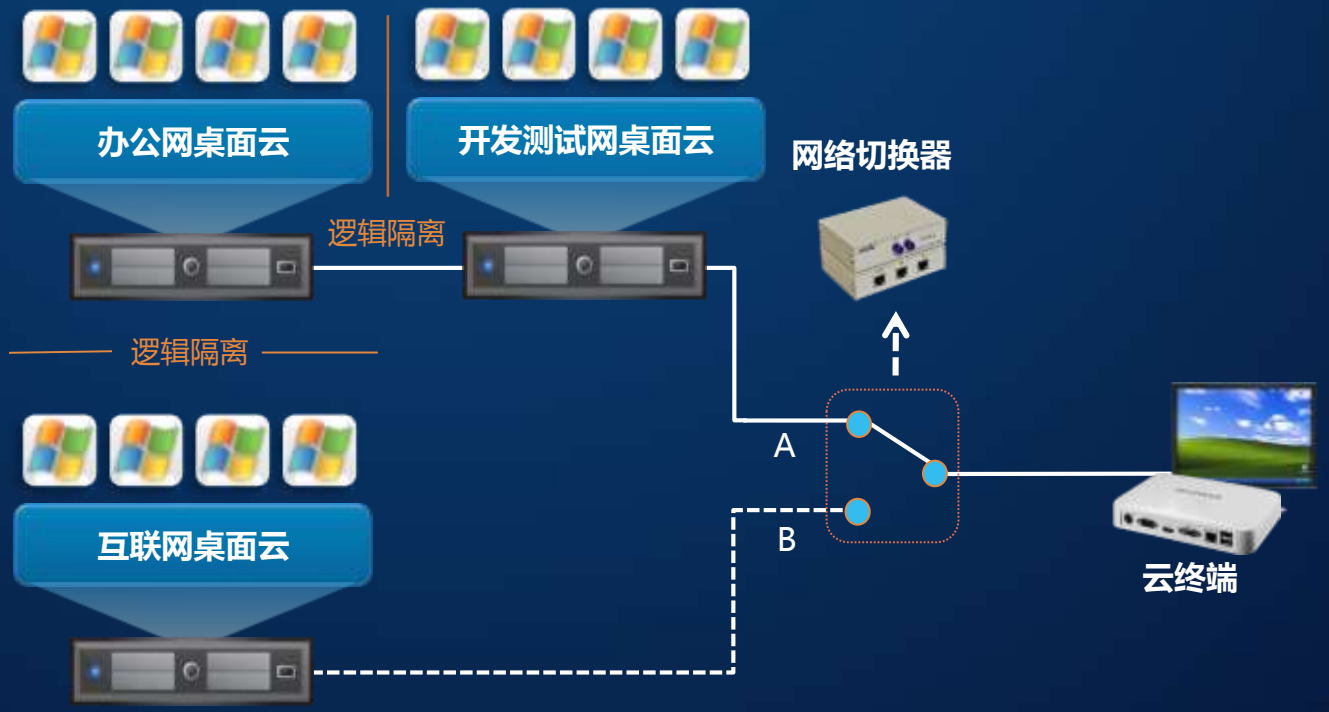
分支管理

监控运维

桌面云aDesk—保护开发测试/内网办公/敏感系统访问环境数据安全，服务人民银行、华夏银行、中国银行、交通银行、兴业银行等金融机构

SANGFOR 深信服科技

低带宽：广域网场景体验效果与Citrix持平



外设安全

2000+外设兼容验证

SRAP

专用协议和断网保持

软件分发

增量式更新和秒级分发

案例1：中国人民银行（77家分支行）打造安全内网办公/培训室桌面云

SANGFOR 深信服科技

项目背景

- PC时常发生软件系统崩溃、配件损坏（硬盘、内存）等故障，**运维难度逐年增加**
- 内网办公、TCBS、ACS、货币发行系统产生大量保密数据，**PC缺乏有效数据保护手段**
- 传统PC**软件升级无法统一进行，硬件扩展需要花费大量时间**进行系统和软件重新安装
- 数据安全、上网数据的隔离、风险区域的隔离有待完善

解决方案

- 2016年-2017年在**34家分支行**，2018年在**43家分支行**，共部署**7000+点**，**软硬件均使用深信服**（瘦终端STD-200H、一体机VDS-3550/6550）
- 在内网办公场景引入桌面云方案，实现人民银行科技管理水平和效率提高
- 兼容专业应用软件：国库会记TCBS、中央银行会计核算ACS、货币发行、办公OA等系统
- 兼容各类外设：网银KEY、扫描仪、针式打印机、高拍仪、摄像头等各类外设

客户价值

- 桌面和资源的集中化，显著**减少设备硬件故障率**，极大的提升IT运维效率
- 补丁更新/环境设置/故障恢复/软件下发等一键下，**减少80%运维工作量**
- 对U盘等外设的精准控制，保证业务交付中数据不落地，**保障内部数据安全**

中国人民银行 THE PEOPLE'S BANK OF CHINA

案例2：华夏银行（全行入围）打造安全办公/开发/生产全场景桌面云

SANGFOR 深信服科技

项目背景

- **ECC场景：**各类业务类、办公类软件、AD域及外设设备
- **Call Center场景：**各类业务类软件及外设设备
- **研发中心场景：**各类开发软件、办公软件均及外设
- **办公应用环境：**各类办公软件、开发软件、外设设备
- **柜面环境：**各类串口多功能键盘、19针打印机、扫描仪、身份证刷卡器等
- **上网网吧环境：**各类互联网软件、办公软件、U盘设备等
- **支行网银体验机环境：**串华夏银行USBKEY、USB白名单控制等

解决方案

- 2017年2月-8月天津分行/绍兴分行，**部署近500点，**软硬件均使用深信服
- 2018年3月总行软件开发中心，**部署近200点，**软硬件部分使用深信服
- 2018年9月，**桌面云系统入围华夏银行全行**

客户价值

- 行内ECC/Call Center/研发中心/办公应用/柜面场景，有效保证行内数据安全

深信服桌面云成功交付55万个虚拟桌面，IDC排名市场第二

SANGFOR 深信服科技

截止2017年底，已经成功交付**55万**个虚拟桌面。

上千规模案例**100+**个，拥有丰富的交付经验和完善的实施方法论

IDC

IDC 数据引用授权书

使用方： 深信服科技股份有限公司	部门：市场行销部 联系人：陈娟娟 电话：13612870126 传真：0755-26581959 电邮：chenjuanjuan@sangfor.com.cn 地址：深圳市南山区 邮编：518000
IDC 数据引用用途：投标	
数据来源（IDC 报告名称）： IDC 中国企业级终端 VDI 市场跟踪报告，2018Q1	
以下数据引用授权有效期至此授权书签发日起三个月内，或 IDC 发布相关报告的更新版为止。	
IDC 数据/引用详细内容： 深信服在中国市场/Sangfor In China Market	

时间 Calendar Year	市场 Market	市场份额（按厂商销售额） Market Share (by Vendor Revenue)	排名（按厂商销售额） Ranking (by Vendor Revenue)
2017	企业级终端 VDI	21.4%	2

2017年桌面云IDC排名，**21.4%**市场份额占有率位，个桌面云市场**第二**

快速创新每年保持**20%**人员增长

专业服务金融行业客户，构筑金融行业安全高效桌面云

SANGFOR 深信服科技

300+ 金融行业用户

84+ 监管机构用户

40% TOP18银行用户

典型案例

监管机构

中国人民银行（77个分支行）

中国银行督管理委员会（7个分局）

国有大行

农业银行（分行）

中国银行（分行）

交通银行（分行）

邮储银行（分行）

股份制银行

华夏银行（全行入围）

浦发银行（分行）

兴业银行（分行）

中国人民银行 THE PEOPLE'S BANK OF CHINA
中国银行业监督管理委员会
中国农业银行 AGRICULTURAL BANK OF CHINA
中国银行 BANK OF CHINA
交通银行
中国邮政储蓄银行
华夏银行
浦发银行
兴业银行
锦州银行
朝阳银行
阜新银行
葫芦岛银行
东营银行
营口银行
長安銀行
德州银行
齐商银行
秦皇岛银行
YICHUAN 伊川农商银行
蓝海银行
深圳农村商业银行
阳泉市商业银行
四川农信
邹城农村商业银行
湖南省农村信用社联合社
如东农村商业银行
……

关键技术02：数据分析技术

深信服行为感知系统BA架构

BA结合上网行为管理的网络日志数据进行分析，发现泄密的风险和进行泄密追溯

发邮件

即时聊天软件

搜索文件

文件外发

访问网盘

图计算
机器学习
MVCC

外发个人隐私信息

敏感文件外泄至竞争对手

高危行为

外发可疑通路

百度网盘
翻墙软件
外发邮件至竞争对手

内网暴露风险

TeamViewer
SSL VPN

外发
敏感文件
检测

外发加密文件

zip
rar
Docx

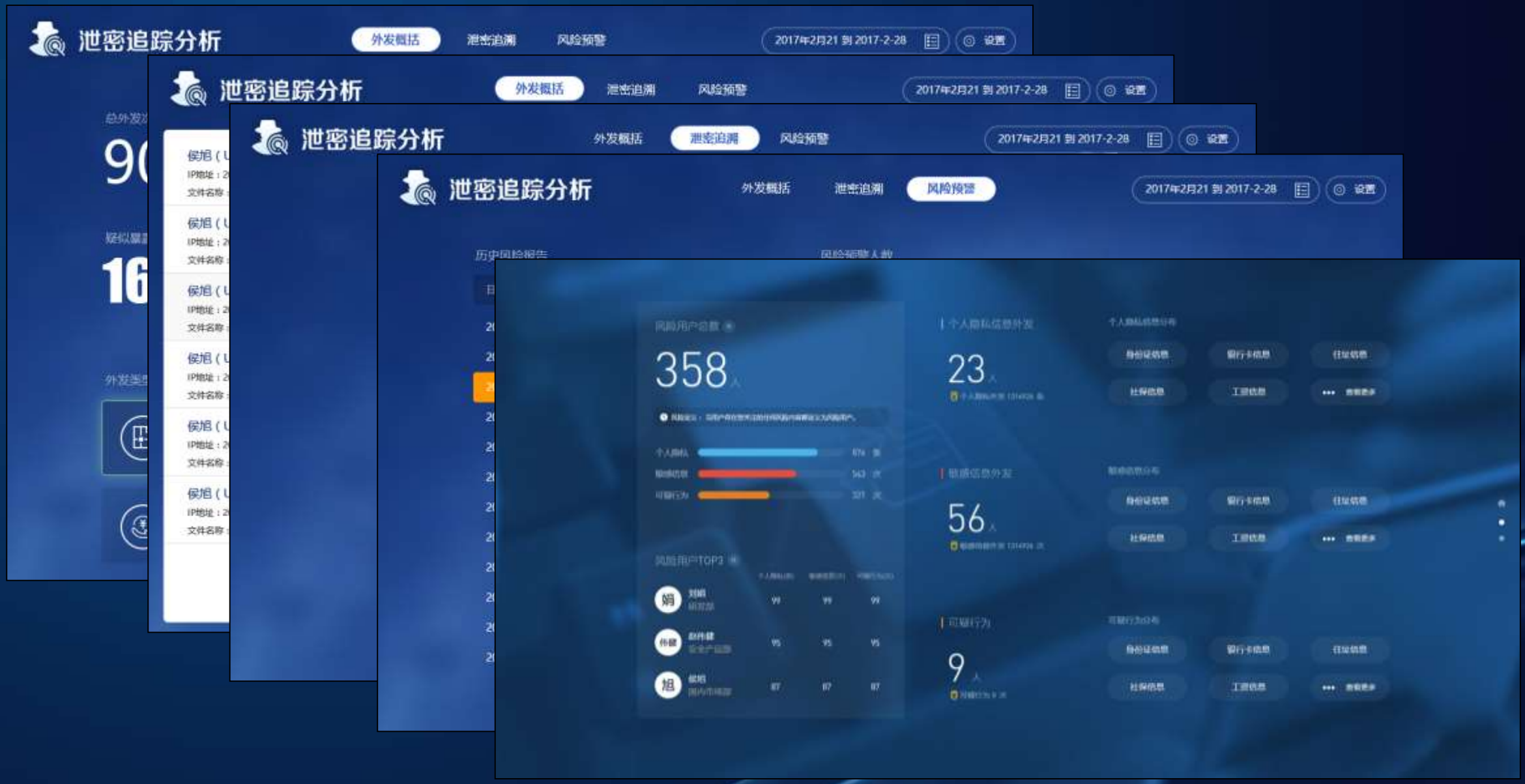
异常外发流量

上行流量突发
异常时段登录
异常时段外发

AC收集上网行为数据

BA建模分析

行为感知系统应用效果


泄密追踪分析
外发概括
泄密追踪
风险预警
2017年2月21 到 2017-2-28
设置
泄密追踪分析
外发概括
泄密追踪
风险预警
2017年2月21 到 2017-2-28
设置
泄密追踪分析
外发概括
泄密追踪
风险预警
2017年2月21 到 2017-2-28
设置
泄密追踪分析
外发概括
泄密追踪
风险预警
2017年2月21 到 2017-2-28
设置
历史风险报告
风险预警人数
风险用户总数
358
人
风险用户TOP3
个人隐私信息外发
23
人
敏感信息外发
56
人
可疑行为
9
人

关键技术03：EMM移动沙箱技术

EMM移动沙箱技术—保护移动数据高安全弱管控更易用的“数据工作空间”移动安全解决方案，为BYOD移动办公、业务移动展业场景，提供数据安全保障

SANGFOR 深信服科技

案例1：国投瑞银基金—EasyWork+保障金融客户终端强管控

项目情况

- 目前国投瑞银基金使用华为手机进行移动办公，通过深信服远程应用发布访问内部业务系统，考虑到终端遗失、窃取后数据外泄的风险

解决方案

- 国投瑞银基金使用easywork+方案对员工华为终端进行管控，一旦设备遗失，即可通过远程擦除数据、删除用户信息，从而保护核心业务系统的数据安全
- 终端类型：IOS及安卓系统
- 项目规模：2台VPN及500个终端授权

案例2：中国邮政集储蓄银行—EasyWork+保障金融客户终端强管控

SANGFOR 深信服科技

项目背景

随着新农村建设不断推进、农村地区移动网络通信等基础设施不断完善、智能终端的普及，农村金融市场，逐渐成为消费、理财、信贷等金融市场的新蓝海。于此同时互联网金融凭借其高效的支付优势，正逐步向县域和广大农村地区渗透。

- 先期邮储银行移动展业采用4G网络通过运营商VPDN接入SSL VPN访问内网应用，为实现WiFi网络安全接入移动展业，将移动展业运营商4G网络SSL VPN接入和WiFi网络SSL VPN安全接入分割为二。

中国邮政储蓄银行 POSTAL SAVINGS BANK OF CHINA

解决方案

- 对移动展业APP采用SDK封装安全加固代码，实现对VPN加密模块的调用。
- 对用户完全透明，用户无感知，正常点击APP即可实现VPN加密、接入。
- 支持为APP增加用户名/密码、匿名认证、证书认证、短信认证、动态令牌、LDAP、Radius等多种认证方式与或组合。
- APP采用HTTPS形式，后端服务器前端部署SSL安全网关实现SSL加解密卸载。

- SDK代码不超过50行；应用封装免开发
- 高强度SSL加密，支持国密算法；自动封装后支持手势认证，安全易用

五

应急管理
解决方案

应急管理——关键需求及方案

SANGFOR 深信服科技

要求	问题	解决方案
第四十一条 •证券基金经营机构应当确保备份系统与生产系统具备同等的处理能力，保持备份数据与原始数据的一致性。重要信息系统应当符合下列信息系统备份能力等级要求： •（一）实时信息系统、非实时信息系统的数据备份能力应当达到第一级； •（二）非实时信息系统的故障应对能力应当达到第二级； •（三）证券公司实时信息系统的故障应对能力应当达到第四级，基金管理公司实时信息系统的故障应对能力应当达到第三级； •（四）实时信息系统、非实时信息系统应当具备灾难及重大灾难应对能力，相关技术指标应当分别达到灾难应对能力第五级、重大灾难应对能力第六级； •（五）灾难应对能力可以通过重大灾难应对能力体现，但重大灾难应对能力相关技术指标应当达到灾难应对能力第五级。	**未建立完善灾难恢复基础设施** •未确保备份系统与生产系统具备同等的处理能力，保持备份数据与原始数据的一致性 •同城灾难备份中心的交易系统无足够的处理能力，无法确保届时能完全承担交易、清算及交收业务 •异地灾难备份中心的交易系统无足够的处理能力，无法确保届时能完全承担交易、清算及交收业务	**优化、整合现有资源，构建稳定、弹性的备份资源池** 服务器整合、虚拟化 采用超融合技术HCI，建立独立的备份（两地三中心）环境
	备份架构有待进一步优化 • 同城灾难备份中心与中心机房之间的通信连接除主用线路外、是否有备用线路 • 实时信息系统、非实时信息系统的数据备份能力未达到第一级 • 非实时信息系统的故障应对能力未达到第二级	**提升备份架构的可靠性，打造坚固的备份平台** 采用负载均衡技术AD构建高可靠性服务器/链路/备份架构

应急管理—云数据中心灾备建设关键能力

SANGFOR 深信服科技

流量分发

流量可以灵活、弹性的调度，保证用户接入最优的数据中心，提高用户访问体验，使各数据中心的压力相对均衡。

故障切换

当链路、服务器甚至是数据中心出现异常时，运维人员可第一时间获悉，访问流量可根据需要灵活的引流至正常节点，保证用户访问的连续性。

安全可靠

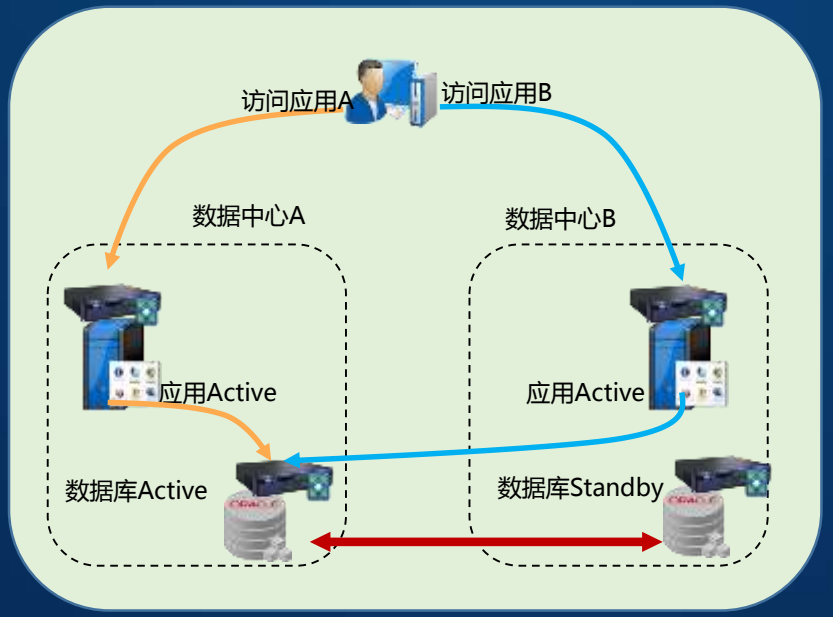
基础架构稳定可靠，数据中心内部各业务分区有严格的安全控制，应用系统无已知安全风险，数据中心能抵抗各类DDoS攻击。

全局可视

多数据中心以统一入口的方式对外提供服务，用户不需要关心多个数据中心的存在。运维管理人员需要直观、详细的了解各数据中心的流量分布和故障情况。

双活数据中心的建设模式

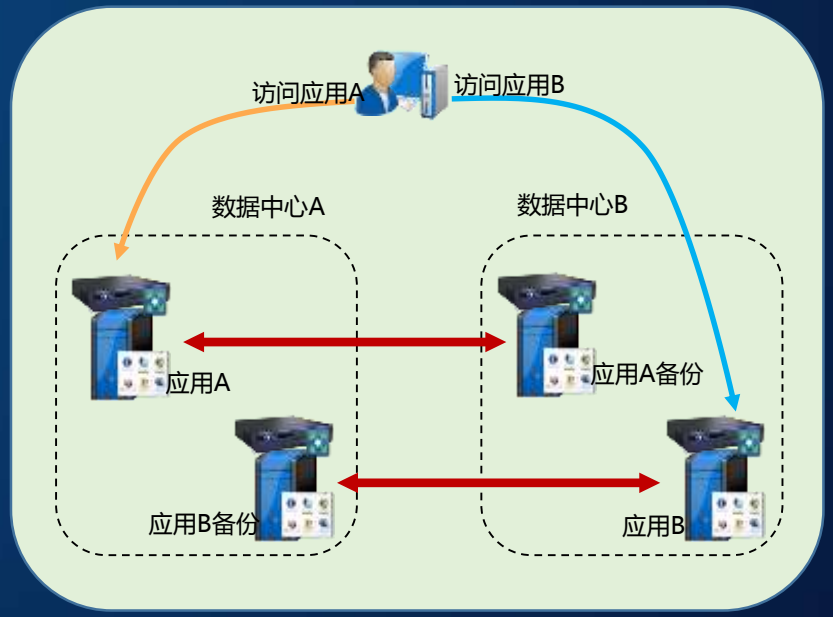
非对称应用双活



条件：GLB+SLB+数据库主备复制

代价：中

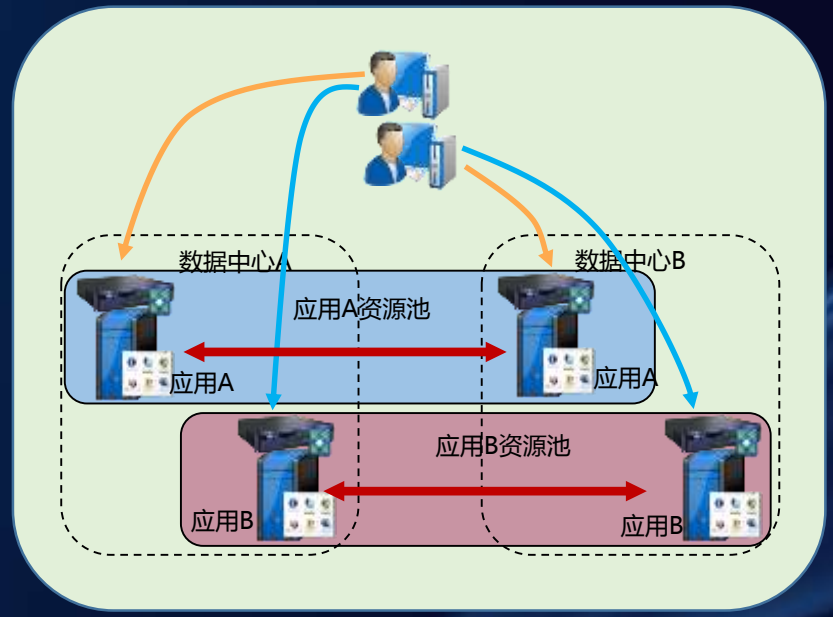
分应用双活



条件：GLB+主备站点数据复制

代价：低

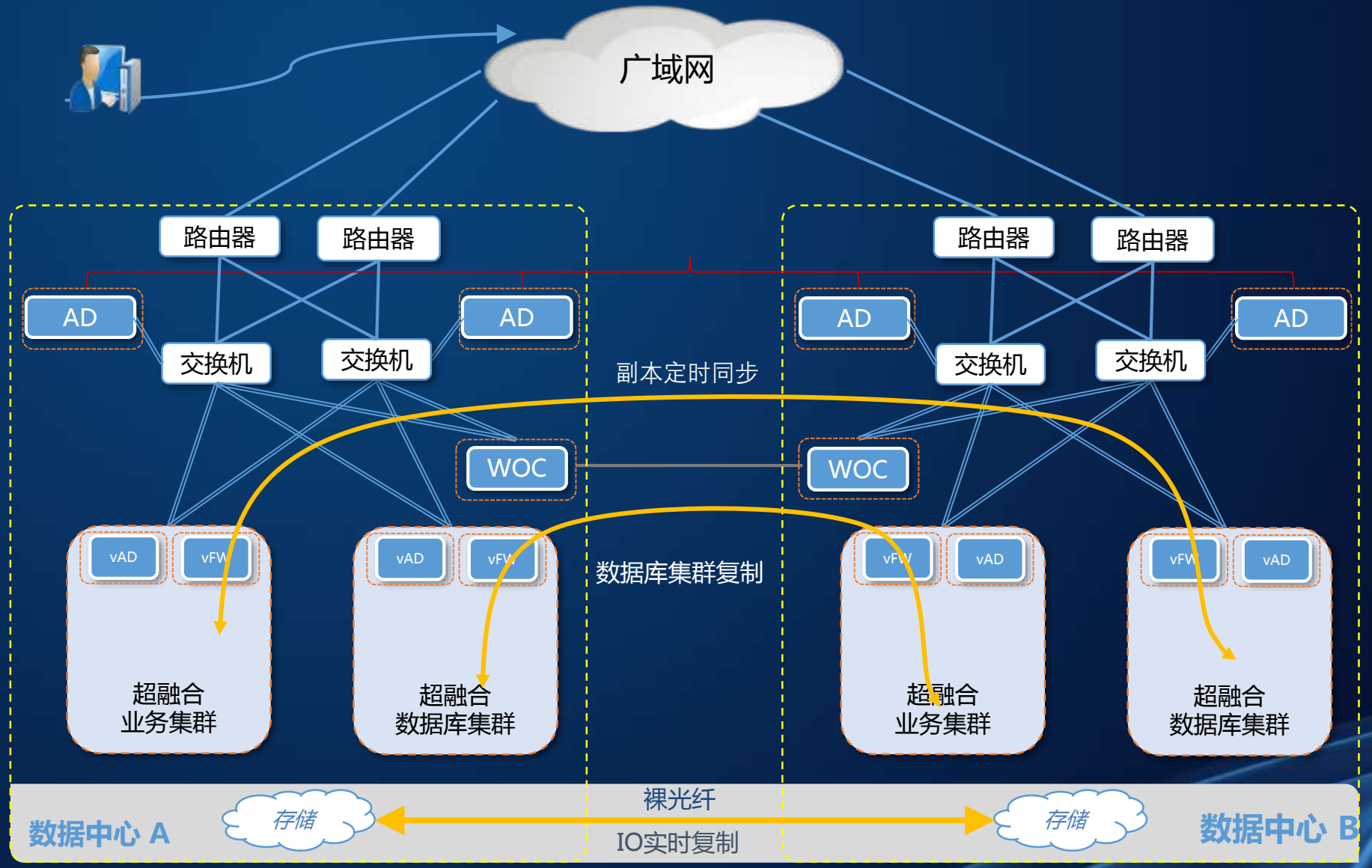
对称双活



条件：GLB+SLB+高速低时延存储链路 + 存储双活 + 数据库双活 +（大二层网络）

代价：高

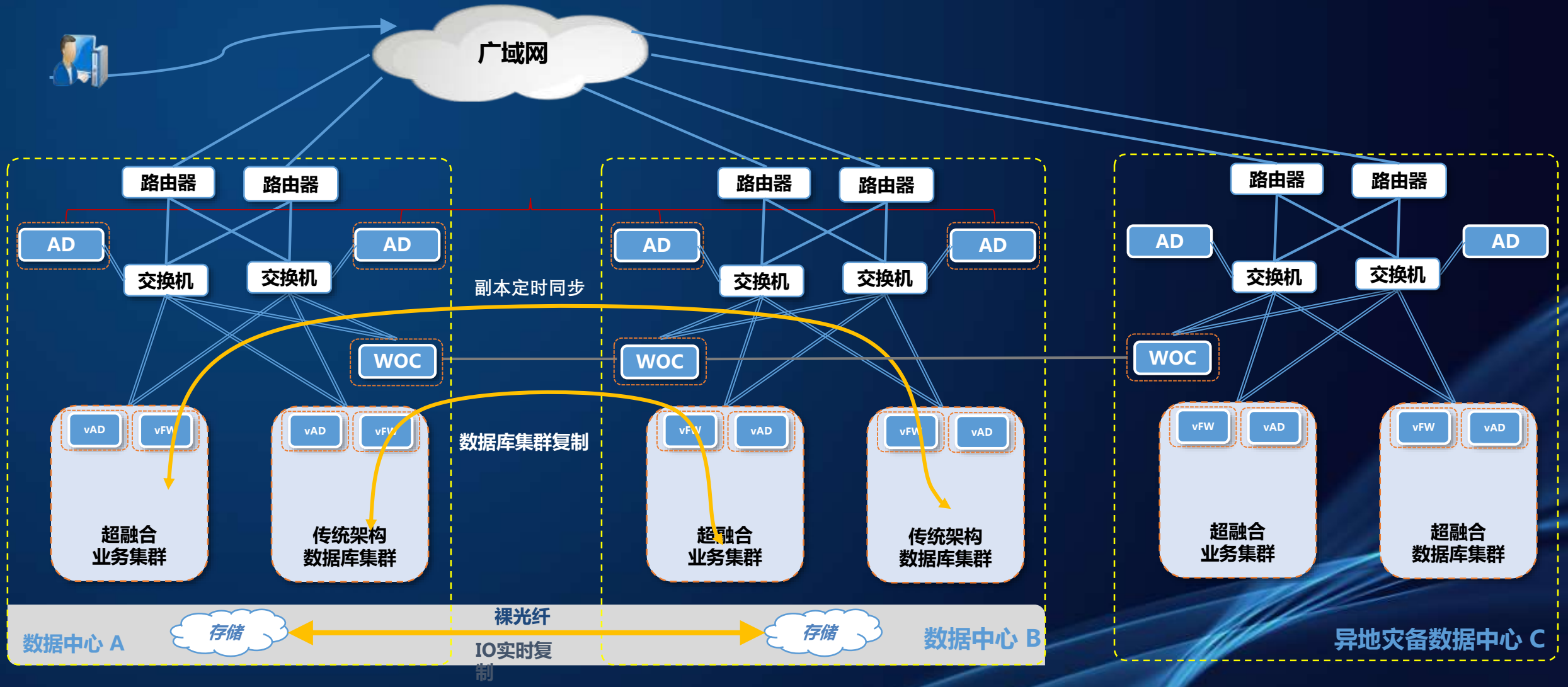
双活数据中心建设参考架构



关键技术

- 资源池化（计算、存储、网络）
- 存储分级，引入分布式存储技术，降低成本。
- 数据中心数据复制路径融合IP网络，增加冗余，降低成本。
- 数据中心流量切换智能化

双地三中心建设参考架构



深信服双活数据中心云灾备方案优势

SANGFOR 深信服科技

双活数据中心

A

高资源利用率

资源池化，双活数据中心无需同等配置，按需建设，降低成本。
多种数据复制技术避免技术绑定。

B

高业务连续性

数据中心故障时，业务不中断，提升业务连续性

D

灵活应对突发业务

当一个数据中心资源不足时，可通过调度使用另一个数据中心资源

C

提升用户体验

全局负载智能调度，用户访问最佳数据中心节点，提升用户体验

典型案例：建设银行（全行入围）服务器负载场景

SANGFOR 深信服科技

项目背景

➢建行负载国产化采用**“入围测试—准入观察试用—正式入围”**的渐进式路径

➢14年开始启动负载均衡国产化调研，并在14-15年进行技术论证、POC测试。分高端12G、中端6G、低端4G的三档

➢凭借过硬的产品设计、丰富的业务优化和虚拟化技术，最终以高出**友商16分**的优异成绩胜出。经过两阶段测试，**深信服作为唯一的国产化品牌入围建行负载均衡**

解决方案

➢ 2015-2016年，部署**13台**20Gbps、**11台**10G设备，应用**总行CA统一认证平台、青岛、广州、南京分行前置及特色业务系统**

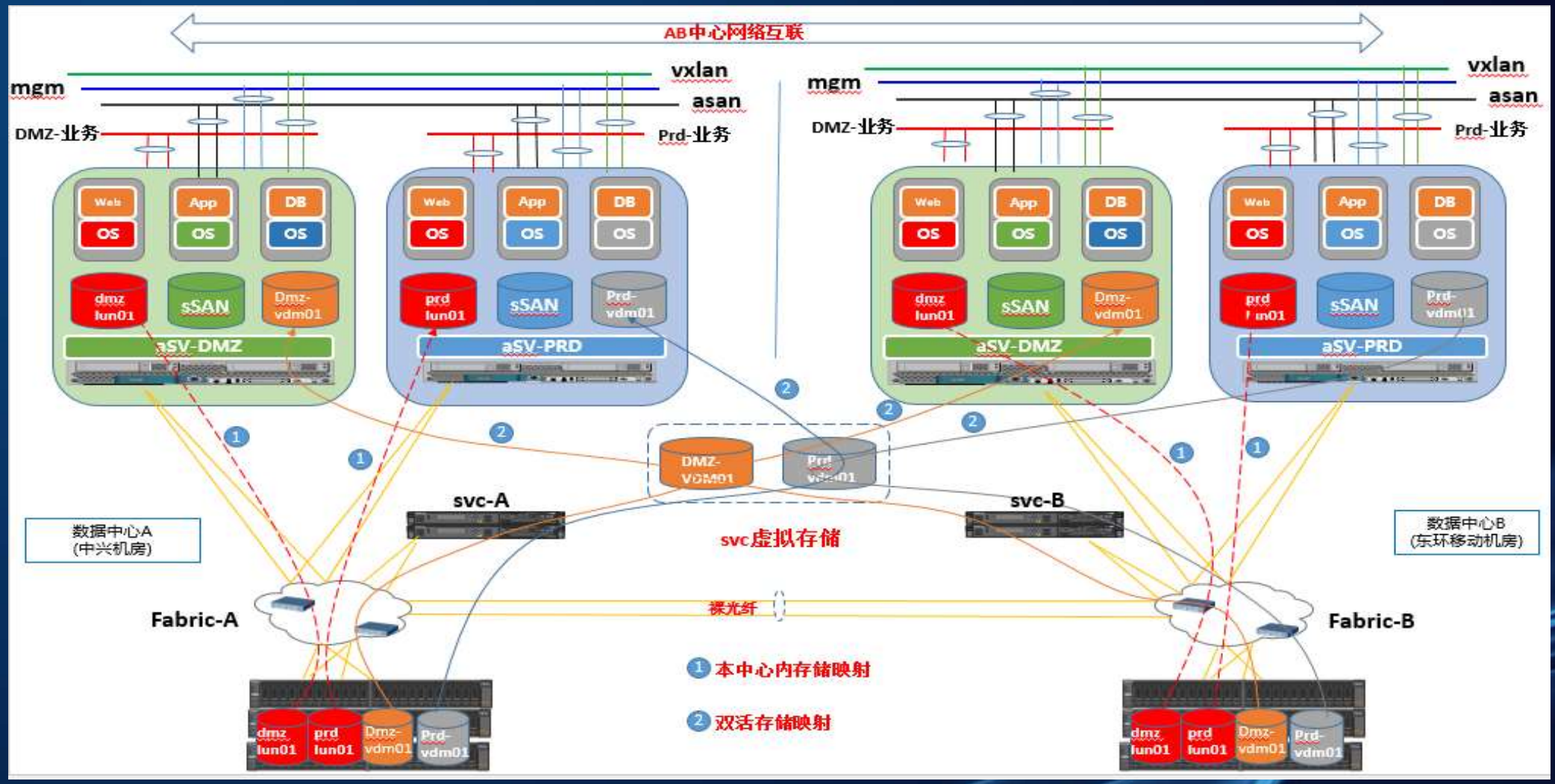
➢ 2017-2018年，总行数据中心，部署**7台**20Gbps设备，应用稻香湖新建数据中心**开放平台**生产环境

客户价值

➢充分利用服务器群的整体性能，解决了个别服务器压力过大导致的访问体验差的问题，提高了应用系统的生产效率

➢通过双机热备模式部署，避免了单点故障，保证了业务的高可靠性和连续性

典型案例：邢台银行-双活数据中心融合资源池



双活数据中心融合资源池

典型案例：南方基金-双活数据中心

项目背景

➢作为业内最早成立的基金公司之一，南方基金非常注重信息系统的建设，已建有两地三中心：深圳CS中心，深证NS本地灾备中心和合肥异地灾备中心，并于2017年完成双活数据中心所需的网络线路改造

➢南方基金内网应用中，部分系统使用域名访问、部分使用IP地址访问，计划通过负载均衡实现内网应用的高可用性

解决方案

➢2018年12月，部署**8**台，包括4台AD-1000-F680、4台AD-1000-G642，用于**双活数据中心全局负载**

➢在CS数据中心和NS数据中心的外网核心区、交易核心区各部署2台AD设备，同时启用IP-Anycast路由注入和智能DNS功能，实现全局负载均衡

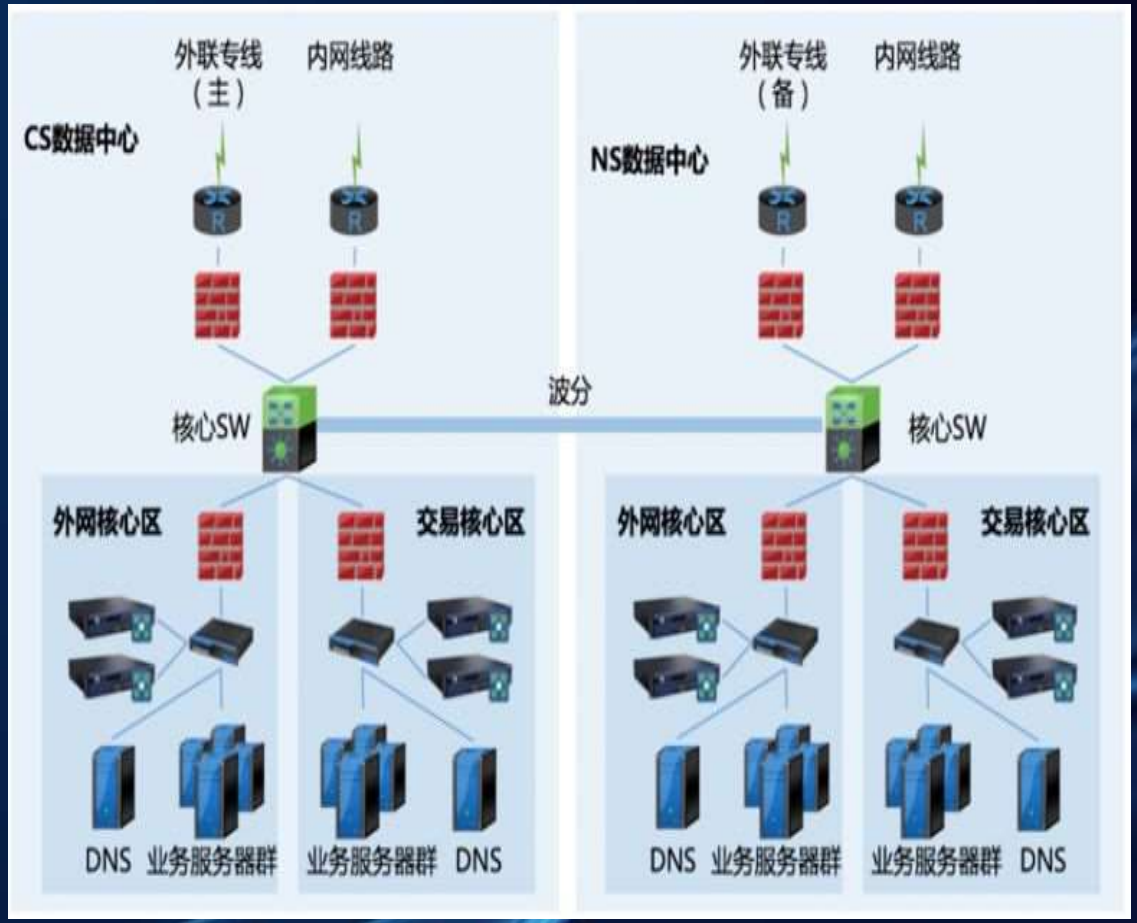
客户价值

➢增强业务连续性，降低RTO和RPO，提升用户体验

➢提高运维效率，运维人员可对双数据中心应用做到整体感知，统一运维

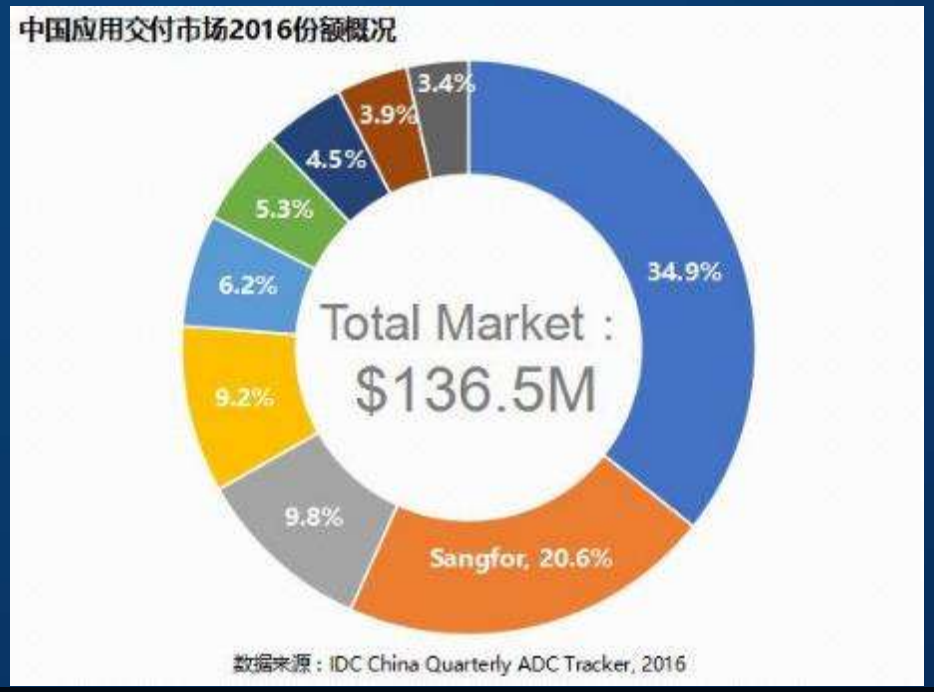
➢实现应用的灰度发布与不停机更新

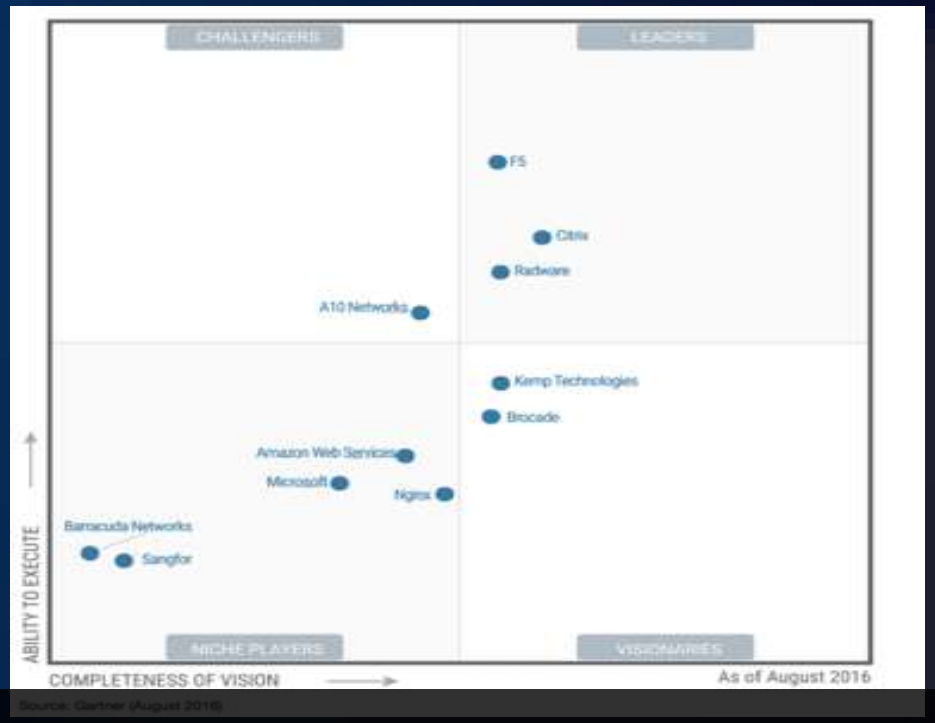
➢有效利用两个数据中心资源，提高投资回报率



深信服应用交付AD产品：连续5年入围Gartner，IDC排名市场第二

SANGFOR 深信服科技





- 2016年AD应用交付IDC排名，**20.6%**市场份额占有率位，市场**第二**
- 打破国外品牌垄断格局，全面突破金融生产网，成功应用**银行生产系统**

- 唯一连续**5**年入选**Gartner**魔力象限的中国厂商
- 快速创新每年保持**20%**研发人员增长

深信服应用交付AD产品：构筑金融行业稳定高效应用交付

SANGFOR 深信服科技

350+ 金融行业用户

100+ 银行用户

75% TOP22银行用户

典型案例

监管/政策银行—100%

- 中国人民银行（10个分支行）
- 国家开发银行（总行）
- 中国农业发展银行（全行）
- 邮政集团/银行（总行+7分行/170+）

国有大行—100%

- 工商银行（全行入围/150+）
- 农业银行（分行）
- 中国银行（全行入围/60+）
- 建设银行（全行入围）
- 交通银行（总行+分行）

股份制银行—58%

- 中信银行（分行）
- 招商银行（总行）
- 浦发银行（总行）
- 民生银行（总行）
- 华夏银行（分行）
- 平安银行（总行）
- 广发银行（总行）

中国人民银行 THE PEOPLE'S BANK OF CHINA
中国工商银行
中国农业银行 AGRICULTURAL BANK OF CHINA
中国银行 BANK OF CHINA
中国建设银行 China Construction Bank
交通银行 BANK OF COMMUNICATIONS
中国邮政储蓄银行
中信银行 CHINA CITIC BANK
招商银行 CHINA MERCHANTS BANK
浦发银行 SPD BANK
中国民生银行 CHINA MINSHENG BANK
华夏银行 HUAXIA BANK
中国平安 平安银行 PINGAN BANK
广发银行 CGB
国家开发银行 CHINA DEVELOPMENT BANK
中国农业发展银行 AGRICULTURAL DEVELOPMENT BANK OF CHINA
广州银行 BANK OF GUANGZHOU
内蒙古银行 Bank of Inner Mongolia
成都农商银行 CHENGDU RURAL COMMERCIAL BANK
兰州银行 BANK OF LANZHOU
XJBank 新疆银行
富滇银行 FUDIAN BANK
青岛银行
廊坊银行 BANK OF LANGFANG
西安银行 BANK OF XI'AN
云南红塔银行 YUNNAN HONGTA BANK
宁波银行 BANK OF NINGBO

证券+基金行业应用汇报

证券+基金客户

- **私有云：超融合HCI/私有云aCloud**

  国泰君安、光大证券、申万宏源、西南证券、信达证券等**16**家

  招商基金、东海基金、英大基金、福安达基金、盈创投资等**7**家

- **内外部监控：云眼SAAS+安全感知SIP**

  西南证券(SAAS)、国都证券(SAAS)、东北证券(SIP)、远达证券(SIP)等**4**家

  国海富兰克林基金(SAAS)、海富通基金(SAAS)等**2**家

- **桌面虚拟化：桌面云aDesk**

  申银万国证券研究所、国泰君安证券、深圳证券、西部证券、中投证券等**18**家

  景顺长城、国开泰富、红土创新、中融基金等**4**家

- **企业移动管理：移动设备EMM**

  国金证券、中山证券、东兴证券等**3**家

  民生加银基金、景顺长城基金、国投瑞银基金等3家

- **业务负载均衡：应用交付AD**

  信达证券、中原证券、安信证券、上海证券、西南证券、国元证券等**21**家

  天弘基金、南方基金、新华基金、大成基金、东方基金、兴银基金等**17**家

- **防火墙：下一代防火墙AF**

  信达证券、深圳证券、华金证券、国都证券、深交所、浙商证券等**41**家

  中邮基金、新华基金、中信建设基金、国创基金、南方基金、华融基金、太平洋基金等**43**家

SANGFOR
深信服科技

THANKYOU

Thanksforwatching

深圳市南山区学苑大道1001号南山智园A1栋
BlockA1,NanshaniPark,No.1001XueYuanRoad,NanshanDistrict,Shenzhen

0755-86627888
market@sangfor.com.cn

www.sangfor.com.cn