

vinchin

十五五安全导向， 灾备从建设到验证



目录

PART 01 解码十五五规划纲要各行业灾备要点

PART 02 公安部176号令审查重点

PART 03 云祺合规容灾备份实践

PART 01

解码十五五规划纲要各行业灾备要点





中华人民共和国中央人民政府

www.gov.cn



首页 | 简 | 繁 | EN | 登录 | 邮箱 | 无障碍

中华人民共和国国民经济和社会发展第十五个五年规划纲要

2026-03-13 21:44 来源： 新华社

字号：默认 大 超大

| 打印



新华社北京3月13日电

中华人民共和国国民经济和社会发展第十五个五年规划纲要

发布时间：2026年3月13日（第十四届全国人民代表大会第四次会议批准）

法律定位：国民经济和社会发展第十五个五年规划纲要（2026-2030年）

第四节 提升网络安全保障能力

- 深化网络空间安全综合治理，加快国家网络安全防御体系建设
- 健全关键信息基础设施安全防护、网络安全审查、云计算服务安全评估等基础制度
- 严厉打击网络违法犯罪行为，加强个人信息保护
- 支持网络安全技术创新和产业发展，鼓励发展安全可靠的信息产品和服务
- **推进容灾备份体系建设**，加强工业控制系统和新技术新应用的网络安全防护

数据安全与数据要素化

- 建立健全数据产权、流通利用、收益分配、安全治理等数据要素基础制度
- 实施数据分类分级管理，提升数据安全保护能力
- 强化国家关键数据资源保护能力，增强数据安全预警和溯源能力
- 一体推进网络、标识、平台、数据、安全体系建设和规模化应用
- 促进数据安全有序流动和高效开发利用

政策原文："推进容灾备份体系建设，加强工业控制系统和新技术新应用的网络安全防护"

维度	政策要求	技术导向
体系建设	构建完整的容灾备份体系，覆盖数据备份、业务容灾、应急恢复全链条	从单点备份向体系化建设演进，实现多层次、多地点的灾备布局
关键基础设施	加强关键信息基础设施安全防护，保障重要系统和数据的可用性	等保三级以上系统、关基运营者需建立完备灾备能力
新技术防护	加强工业控制系统、云计算、大数据、人工智能等新技术新应用安全防护	云灾备、容器备份、AI驱动的智能灾备调度成为新方向
安全可靠	鼓励发展安全可靠的信息产品和服务，推进国产化替代	国产备份软件、信创生态适配、自主可控成为建设硬要求

核心要求：强化生物安全和卫生健康信息安全

1. 卫生健康行业商用密码应用体系

完善卫生健康行业商用密码应用体系，建设医疗卫生机构、医务人员和患者可信数字身份管理系统

2. 国家生物安全风险监测预警体系

完善国家生物安全风险监测预警体系，强化实验室生物安全监管，加强人类遗传资源有效保护和合理利用

3. 全民健康数智化建设

推进全民健康数智化建设，医疗数据互联互通，电子病历、健康档案等核心数据需保障安全可靠存储

4. 灾备建设硬性要求

医院核心业务系统（HIS/LIS/PACS）需满足等保三级要求，建立数据备份与业务容灾能力，保障医疗业务连续性。

建设安全高效金融基础设施；完善多地灾备体系、强化关键系统容灾能力；系统重要性基础设施建立灾难备份机制。

要求维度	具体要求	灾备建设要点
数据分类分级	实施数据分类分级管理，加强技防措施建设，完善监测预警、事件报告、风险处置工作机制	按数据级别差异化备份策略，重要数据异地容灾
个人信息保护	建立健全个人信息保护制度，对金融消费者个人信息实施全流程管理	备份数据加密存储，访问权限严格管控，留痕审计
数据全生命周期	建立覆盖数据全生命周期的管理流程，确保数据源头可追溯	数据备份+归档+销毁全链路覆盖，满足监管审计要求
自主可控	稳妥选择使用技术自主、性能可靠、安全防护能力强的数据库产品	国产备份软件+国产数据库适配，信创生态认证
AI安全防护	加强模型安全护栏建设，严格管理外包过程中的数据安全	AI训练数据备份与隔离，防止数据泄露和模型窃取

政策依据：《银行业保险业数字金融高质量发展实施方案》 《银行业保险业AI安全开发应用指导意见》 《金融信息服务数据分类分级指南》

核心要求：提升电网运行韧性 + 能源数据安全防护体系

电力安全应急体系建设

- 完成东北、西北国家级电力应急基地建设
- 优化完善"7+2+N"国家电力应急力量体系
- 制定极端状态下电网保底供电方案
- 完善大面积停电事件应急预案，定期开展应急演练
- 实施"人工智能+电力应急"创新工程
- 提升源网荷储各环节风险管控能力

能源数据安全与隐私保护

- 制定能源行业数据分类分级标准规范
- 加强能源关键信息基础设施与数据保护
- 构建覆盖数据全生命周期的安全防护体系
- 定期开展安全审核与风险评估
- 推动隐私计算、密态计算等前沿安全技术
- 加快可信流通技术研发和应用推广

政策依据：《电力安全生产"十五五"行动计划》&《新型电力系统建设"十五五"规划》。

核心制度：交通运输数据三级分类分级保护

核心数据 关系国家安全、国民经济命脉等关键数据 最高级别保护，需异地容灾、实时备份	重要数据 一旦遭到篡改、破坏等会危害公共利益的 需建立完备备份机制，定期恢复演练	一般数据 除核心数据和重要数据的其他数据 基础备份要求，保障数据可用性即可
---	--	---

全生命周期安全管理要求

可信采集	加密传输	可靠存储	受控交换	存证溯源	销毁确认
数据来源可追溯	传输加密保护	备份+容灾	交换审批流程	操作留痕审计	彻底销毁确认

《综合交通运输标准化发展“十五五”规划》

区块链的进出港业务电子平台、海运区块链架构与数据交互规范；交通运输信息系统商用密码应用、数据安全监测预警、网络威胁情报共享要求；船舶

两大专栏：网络和数据安全能力提升 + 新型工业化安全保障

专栏一：网络和数据安全能力提升

- 网络安全防护体系建设
- 数据安全治理能力提升
- 数实融合安全保障
- 安全产业发展壮大

专栏二：新型工业化安全保障

- 工业互联网安全保障
- 电信网络诈骗治理提效
- 关键信息基础设施安全保护
- 云网融合安全防护能力

信息通信行业灾备建设特殊要求

要求领域	具体内容
基础电信网络灾备	基础电信企业需建立异地容灾备份中心，保障通信网络不中断，满足《关基条例》要求
数据中心灾备	IDC/云服务商需提供数据备份和容灾能力，保障用户数据安全可靠

2026年灾备领域新规范政策(部分)

序号	政策/标准名称	发布机构	实施时间	灾备相关的核心要求
1	十五五规划纲要	全国人大	2026.3	推进容灾备份体系建设，关键信息基础设施安全防护
2	公安部176号令	公安部	2026.10	等保、关基、数据安全义务监督检查，每年现场检查
3	GB/T 20988-2025	国标委	2026.1	灾难恢复规范新国标，云灾备、量化评价、安全建设
4	GA/T 2380-2026	公安部	2026.6	明确数据安全独立考核维度、评估体系、技术要求和管理规范。
5	交通运输数据安全管理办法	交通运输部	2026.7	数据三级分类分级，全生命周期安全管理
6	电力安全生产十五五行动计划	国家能源局	2026.8	电力应急体系，大面积停电预案，数据安全防护
7	信息通信行业十五五规划	工信部	2026.9	网络和数据安全能力提升，关键信息基础设施保护
8	数据存储灾备服务能力成熟度模型	工信部	2026.1	行业标准报批，灾备服务能力分级评价

PART 02

公安部176号令审查重点



《公安机关网络空间安全监督检查办法》（公安部令第176号）

时间：2026年08月07日

字体：

大

中

小

分享到：



中华人民共和国公安部令

第176号

《公安机关网络空间安全监督检查办法》已经2026年7月1日第2次公安部部务会议审议通过，现予以公布，自2026年10月1日起施行。

部 长 王小洪

2026年8月6日

公安机关网络空间安全监督检查办法

第一条 为了维护国家安全和社会公共利益，保障公民、法人和其他组织合法权益，规范公安机关对网络空间安全的监督检查工作，防范、治理网络违法犯罪，根据《中华人民共和国人民警察法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《关键信息基础设施安全保护条例》《网络数据安全管理条例》《互联网信息服务管理办法》等有关法律、行政法规规定，制定本办法。

第二条 本办法适用于公安机关依法对网络运营者、数据处理者、个人信息处理者等履行法律法规规定的网络安

关键时间节点



核心定位与适用范围

维度	具体内容
监管对象	网络运营者、数据处理者、个人信息处理者、关键信息基础设施运营者等8类主体
监管内容	网络安全、数据安全、信息安全“三位一体”监督检查，结合网络服务合规
检查方式	线上巡查 + 远程检测 + 现场检查 三种方式结合，以及专项监督检查
执法依据	《网络安全法》《数据安全法》《个保法》《关基条例》《网络数据安全管理条例》等

资料来源：中华人民共和国公安部令第176号（公安部网站，2026年8月7日发布）

监督检查重点：11项法定检查内容

依据：《公安机关网络空间安全监督检查办法》第七条

序号	检查内容	序号	检查内容
1	依法办理联网单位备案，报送接入单位和用户基本信息	7	针对网络安全漏洞、隐患采取整改措施，消除风险隐患
2	制定并落实网络安全、数据安全、信息安全管理制度和操作规程	8	对禁止发布或传输信息采取防范措施
3	记录并留存用户注册信息和上网日志信息	9	落实算法安全主体责任，建立算法推荐管理制度和技术措施
4	网络安全等级保护定级备案、等级测评、建设整改、自查义务	10	履行数据安全、个人信息保护义务
5	关键信息基础设施安全保护义务	11	为公安机关维护国家安全、侦查犯罪等提供技术支持和协助
6	防范计算机病毒和网络攻击、网络侵入等技术措施		

四类检查方式

线上巡查 网络信息巡查、信息审核能力测试、漏洞扫描等不影响正常业务的方式 提前3个工作日告知	远程检测 设区市级以上公安机关开展漏洞探测、渗透性测试 提前3个工作日告知，通报网信部门和行业主管部门	现场检查（重点） 进入机房、查看技术措施运行情况、开展技术检测 人民警察不得少于2人，出示证件和检查通知书	专项监督检查 结合重大网络安全保障、专项治理行动、舆情风险、安全事件复盘等，开展针对性专项检查。
---	--	--	---

检查频次规则

对象类型	检查频次	备注
等保三级（含）以上网络运营者	每年一次现场检查	复用其他主管部门检查结果
关键信息基础设施运营者	每年一次现场检查	委托技术支持需告知行业主管部门
曾发生安全事件或被处罚未整改	重点监督检查	不受频次限制

来源：《公安机关网络安全监督检查办法》第四、五、九、十条

风险隐患处置四级响应（第十七条）



约谈机制（第十九条）

情形	约谈主体	约谈对象
网络安全、信息安全存在较大风险或发生安全事件	省级以上公安机关	法定代表人/主要负责人
数据安全、个人信息处理存在较大风险或发生事件	县级以上公安机关	有关组织、个人

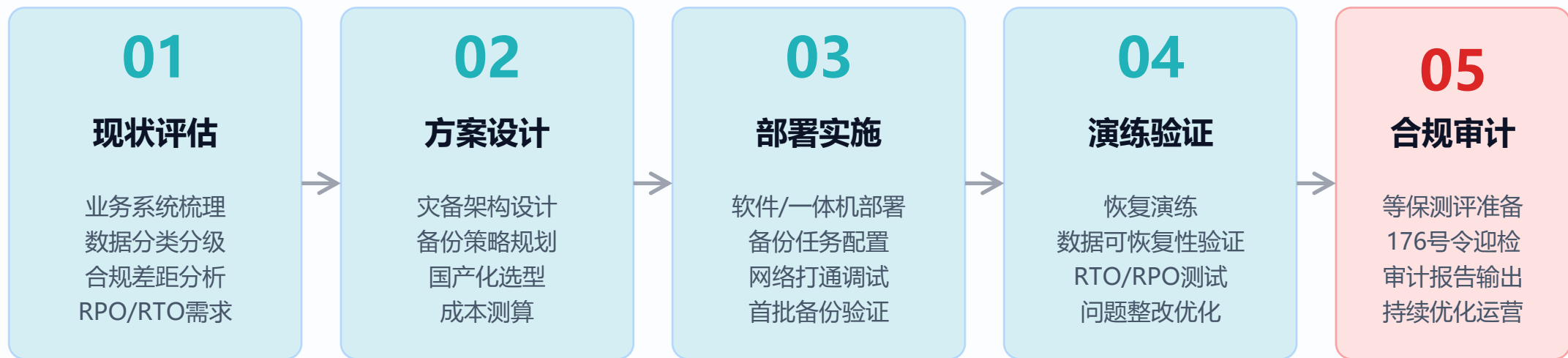
资料来源：《公安机关网络空间安全监督检查办法》第十六、十七、十八、十九条

PART 03

云祺合规解决方案



五步实施路径



合规审计关键输出

审计日志：

所有备份操作、恢复操作、配置变更全程留痕，支持审计追溯 **演练报告**：定期恢复演练记录，验证数据可恢复性

等保测评：

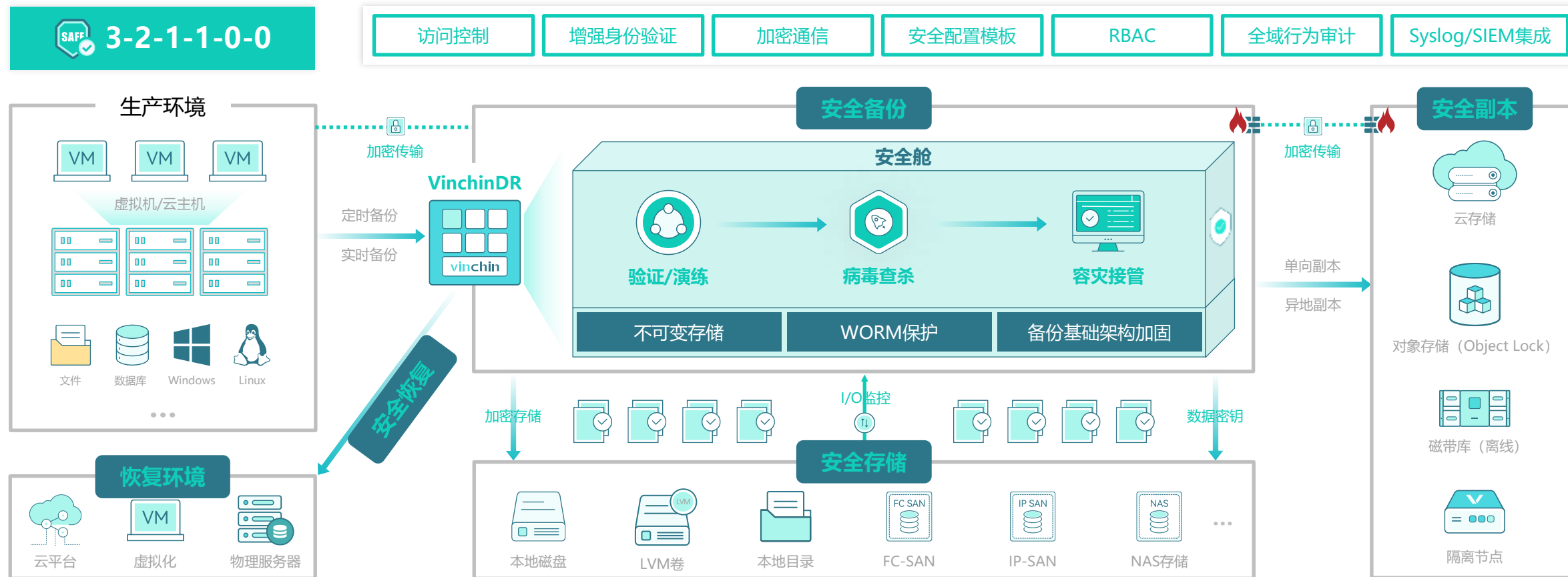
满足等保三级灾备相关测评项 **176号令迎检**：备份系统运行状态可查，管理制度完备，应急演练记录完整

国产化证明：

信创适配认证证书，国产化替代方案文档

备份存储与全生命周期防护

vinchin



全程加密防护

WORM 防篡改

异地副本容灾

全生命周期归档

虚拟化/私有云/公有云平台备份

vinchin



智能无代理

无需在虚拟机中安装客户端，无代理对接各虚拟化/云平台，更少工作量、更低兼容性风险、更高安全性

分钟级瞬时恢复

虚拟机故障时，可直接将数据挂载到目标平台拉起虚拟机继续使用，无需等待数据传输，分钟级RTO

V2V跨平台恢复/迁移

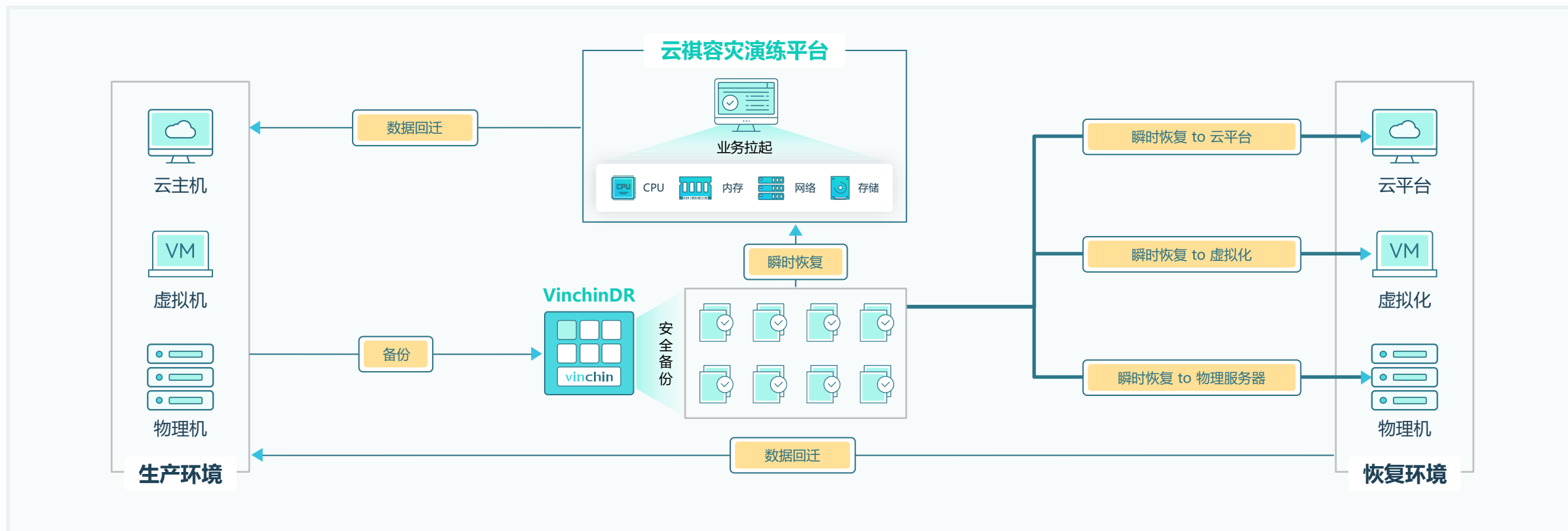
遭遇平台级灾难时，可将虚拟机恢复到异构平台，实现跨平台容灾，也可满足国产化替换等迁移需求

高性能备份恢复

采用多线程并发，多虚拟机并行备份、Lan-free传输、永久增量等方式提升备份恢复效率

数据恢复

任何时候出现故障，我们都希望尽可能快的恢复业务，避免业务长时间中断。因此如果可以采用某种方式快速恢复，使中断的业务迅速重新上线，这将会大幅减少业务中断带来的损失。



整机瞬时恢复

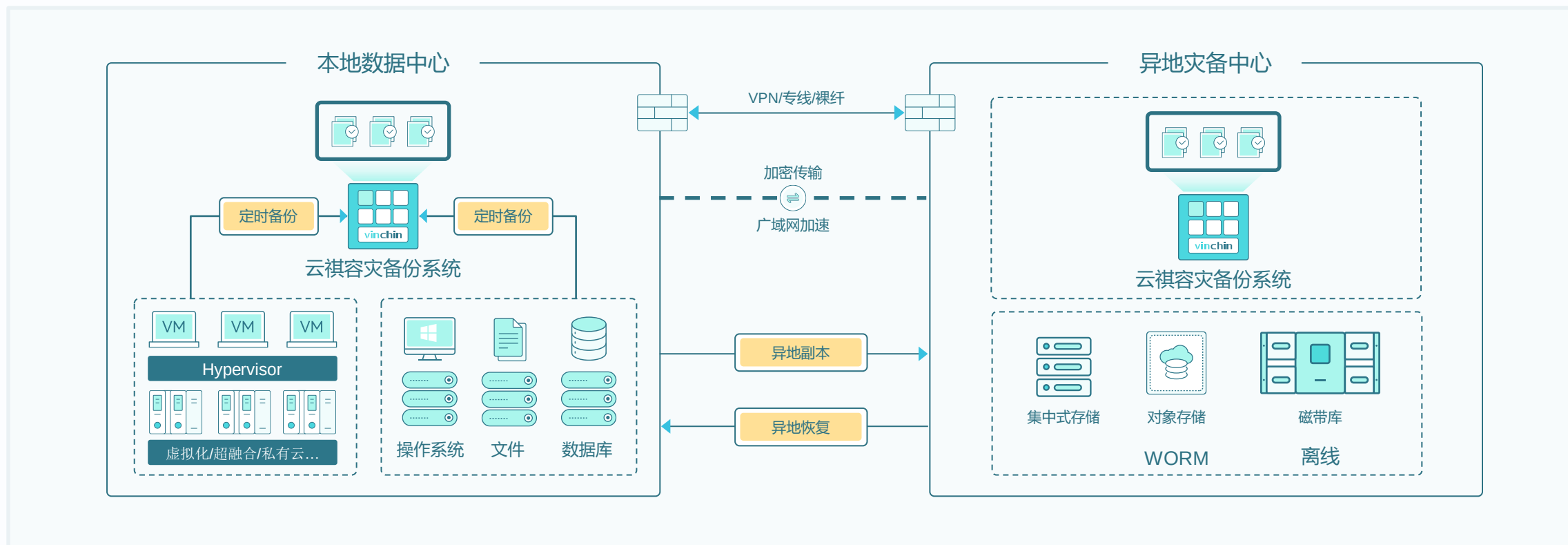
内置恢复资源

分钟级RTO

一键数据回迁

异地副本数据容灾方案

vinchin



数据异地副本

定期将最新备份数据自动传输到异地数据中心，避免机房级灾难，支持广域网加速与加密传输。

窄带宽异地传输

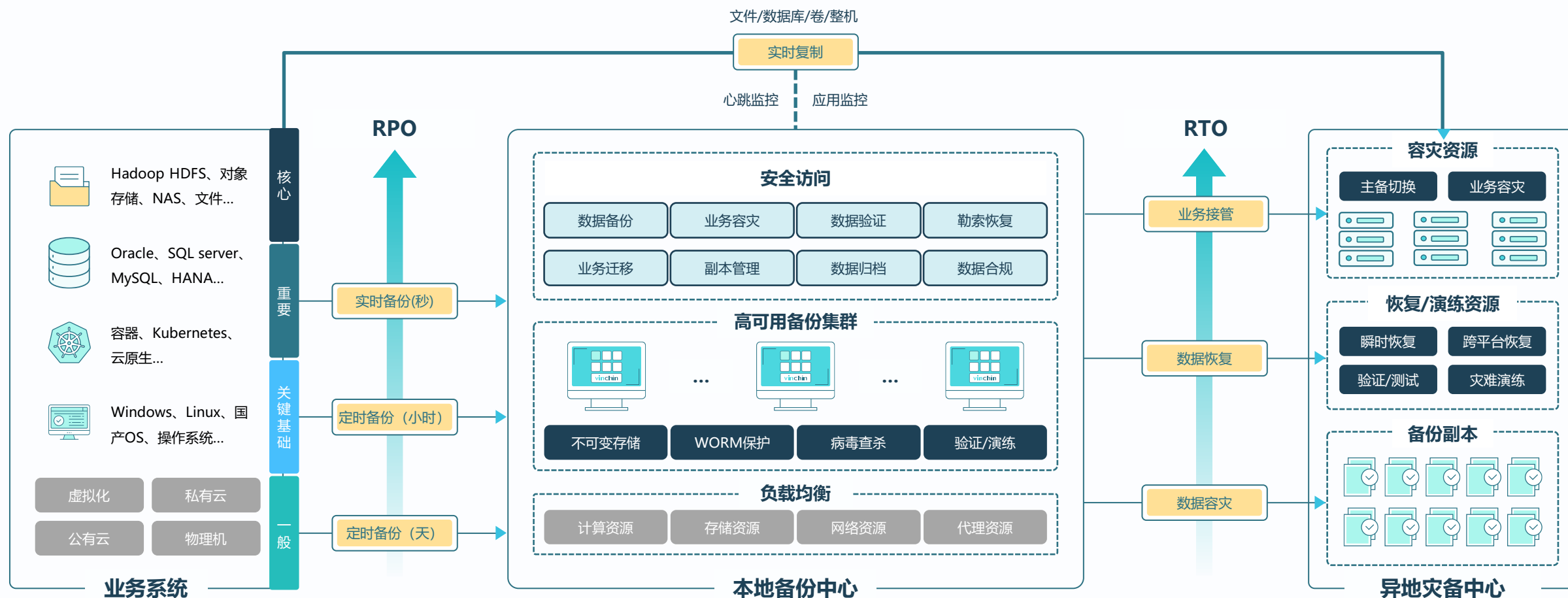
通过源端压缩、断网续传以及永久增量副本等技术适合窄带宽场景，提升传输效率。

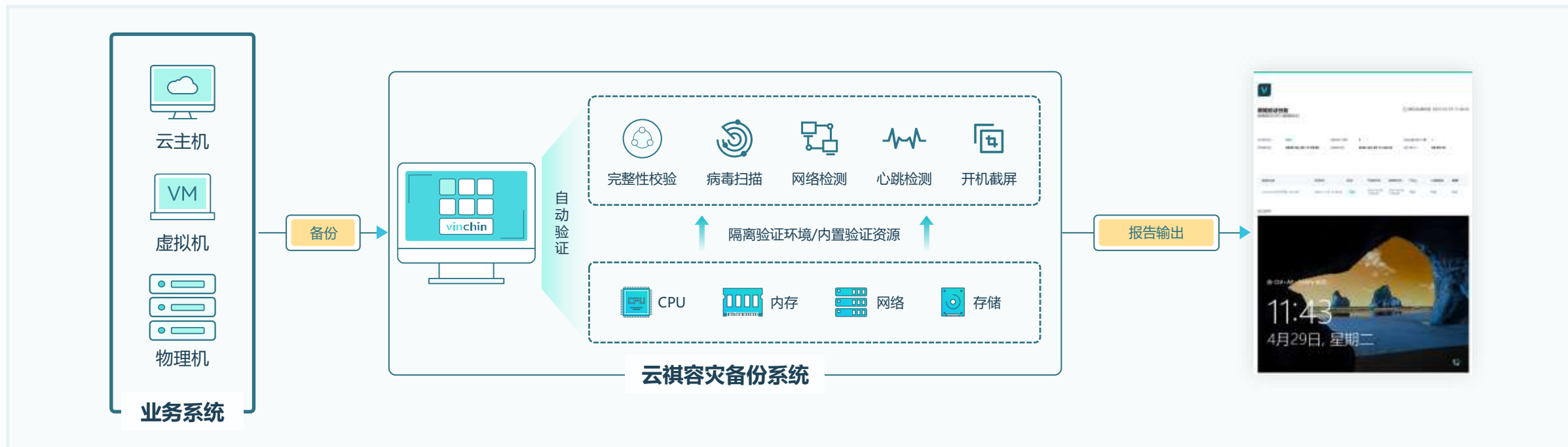
统一管理

一个平台统一管理两地本地备份、异地副本，结合可视化大屏实现轻松监控运维。

数据分类分级保护

业务系统和数据的重要性各不相同，灾备建设的预算也不可能无限增长，因此不能盲目选择一揽子方案，适合的才是最好的，应当根据根据业务特点与数据重要程度选择合理的灾备方案，进行分级灾备建设，实现最佳成本控制。





零验证资源成本

无需额外准备服务器、存储、网络等资源，可直接使用备份系统内置资源进行验证演练

零生产影响

备份系统可自动生成隔离验证环境，不与外界通信，验证时不影响生产业务正常运行

确认恢复就绪

通过定期进行自动验证，确认备份数据状态，在异常时可及早接入采取对应措施

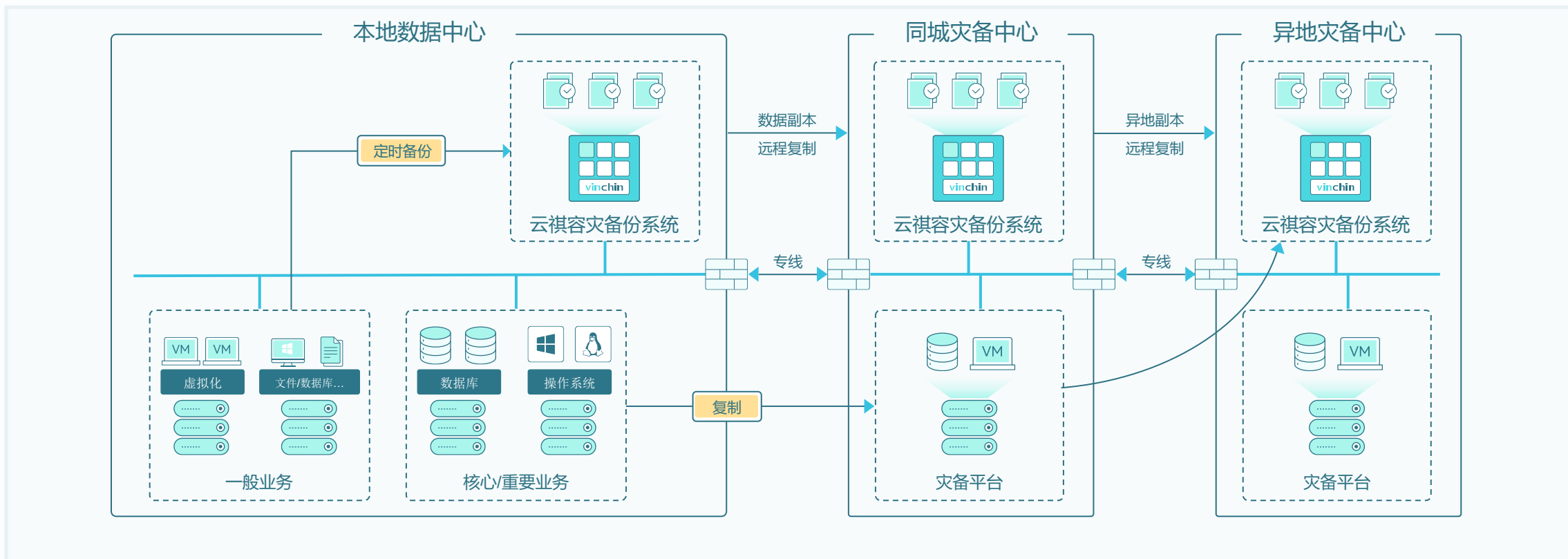
帮助持续改进

持续的定期演练可帮助用户发现恢复问题，不断优化策略配置，改进恢复流程等，提升应急响应效率

两地三中心安全灾备方案

vinchin

基于3-2-1-1-0备份体系构建数据中心安全灾备方案



数据分级保护

根据业务系统重要程度分级保护，满足不同业务等级的RTO、RPO需求。

提升业务连续性

通过主备复制，当生产出现故障时，同城灾备中心可快速接管业务。

异地数据容灾

即使生产站点与同城灾备站点遭遇区域性灾难，异地灾备站点也有数据可恢复。

跨域灾备管理

两地三中心接入统一管理平台，提供跨区、跨地的灾备可视化管理能力。