vinchin

# 交通新规落地,灾备合规怎么做

《交通运输数据安全管理办法》

vinchin

# 目 录

vinchin

# PART 01

# 交通数据安全规范解码

# 办法概述

vinchin

交通运输部行政规范性文件

下载文字版 下载

## 交通运输部关于印发《交通运输数据安全管理办法》的通知

交科技规〔2026〕3号

各省、自治区、直辖市、新疆生产建设兵团及计划单列市交通运输厅（局、委），国家铁路局、中国民用航空局、国家邮政局，中国远洋海运集团有限公司、招商局集团有限公司、中国交通建设集团有限公司，公路水路关键信息基础设施运营者、重要数据处理者，部属各单位、部内各司局：

现将《交通运输数据安全管理办法》印发给你们，请认真贯彻执行。

交通运输部

2026年6月18日

（此件公开发布）

### 交通运输数据安全管理办法

# 办法概述

vinchin

## 《交通运输数据安全管理办法》发布实施与核心背景

**发布&实施：**
2026年6月18日由交通运输部以“交科技规〔2026〕3号”正式印发，2026年7月1日起正式施行。这是交通运输行业首部数据安全专项管理规章，为行业数据治理提供了制度遵循。

**落实国家法律法规要求**
严格贯彻《网络安全法》《数据安全法》《个人信息保护法》等上位法要求，细化行业监管规则，确保合规经营与法治落地。

**破解流通共享现实难题**
解决跨主体、跨区域数据流通中“不敢共享、不能共享”的痛点，规范处理流程，促进数据要素在安全前提下高效开发利用。

**制度建设核心目标：** 构建“责任明晰、监管到位、分级精准、闭环管理、防控严密、监督规范”的全流程数据安全管理体系，为行业数字化转型筑牢安全底座，实现数据安全保障与要素价值释放的双向赋能。

# 数据分级框架

vinchin

## 交通运输数据分级


## 级别变更

一般数据及时变更数据级别

- 数据内容、规模、时效性、应用场景、加工处理方式等发生变化
- 因国家有关要求，导致原定级别不再适用

重要数据和核心数据

| | |
|---|---|
| 级别变更 | 按规定重新开展数据分类分级工作 |
| 信息变更 | 在30日内报告 |

# 数据全生命周期安全管理

vinchin

### 01 境内存储合规

关键信息基础设施运营者收集产生的个人信息和重要数据，原则上**必须在境内存储**，严控违规跨境流动风险。

### 02 等级保护定级

重要数据存储系统需满足**等保三级**要求；核心数据系统至少达到**等保四级**或关键信息基础设施保护标准。

### 03 容灾备份演练

必须实施多副本异地容灾备份，并**定期开展数据恢复测试与灾难恢复演练**，确保极端情况下数据可恢复。

### 04 安全可信底座

优先采用安全可信的软硬件产品与服务，构建自主可控的存储环境，从供应链源头防范数据安全风险。

## 数据全生命周期八大闭环管控环节

**01 收集**
规范采集边界

**02 存储**
安全加密存储

**03 使用加工**
脱敏与去标识化

**04 传输**
通道加密防护

**05 提供**
严格授权管控

**06 公开**
合规审核机制

**07 删除**
彻底销毁清理

**08 转移**
跨境安全评估

# 规范整体框架

vinchin

## 5类特殊场景安全要求

### 转移

- 明确数据转移方案
- 约定接收方保护义务

### 委托、共同处理

- 明确双方安全责任和义务
- 未经同意不得擅自使用

### 跨境

- 遵循国家跨境要求
- 个人信息满足单独要求

### 人工智能

- 全面评估风险
- 加强训练数据和处理活动管理

### 日志记录管理

- 按要求留存日志
- 满足风险溯源和事件处置需要

# 日志留存与合规审计

vinchin

## 普通日志 · 6个月

针对数据全生命周期的基础网络日志，满足日常运营的风险溯源与一般安全事件处置需求，法定留存时间不少于6个月。

## 重要日志 · 1年

涵盖政务应用系统访问记录、核心数据库操作日志及重要数据安全事件记录，支撑关键行为回溯，留存时间不少于1年。

## 核心日志 · 3年

针对核心数据泄露等重大安全事件、个人信息提供与委托处理记录，为事后定责与司法取证提供铁证，留存时间不少于3年。

## 合规审计常态化机制

**定期开展，闭环管理（第二十八条）**

交通运输领域个人信息处理者应建立定期合规审计制度，可委托具备资质的第三方机构实施。审计范围覆盖个人信息收集、存储、使用、共享、删除等全流程，重点审查是否符合最小必要原则、用户授权机制是否完善、技术防护措施是否有效。审计结果需形成报告并归档，针对发现的隐患限期整改，确保个人信息保护合规要求落地见效，防范法律与经营风险。

# 风险评估与应急处置

vinchin

## 常态化评估筑牢防线，标准化应急应对突发

《数据安全法》明确建立“事前评估、事中响应、事后复盘”闭环管理机制，针对重要数据与核心数据实施动态监测，以制度化手段将安全风险控制在萌芽阶段，保障数据全生命周期安全。

### 01 风险评估：定期体检 + 触发扫描

**定期评估**：处理重要/核心数据，或涉及超1000万人信息的主体，**必须每年开展一次全面风险评估**，形成报告留存备查。

**触发评估**：发生重大安全事件、委托处理重要数据、系统重大变更或数据出境时，需**立即启动专项评估**，未通过评估不得实施。

### 02 应急处置：预案先行 + 分级响应

**预案制定**：数据处理者需制定专项应急预案，明确报告流程、应急指挥、技术处置、舆情应对等关键环节的责任与操作规范。

**分级响应**：按危害程度将事件分为**特别重大、重大、较大、一般**四级，不同等级对应不同的响应启动条件与处置流程。

### ⚠ 合规硬性要求：应急演练不可缺席

重要数据和核心数据处理者**应当每年至少开展一次应急演练**，检验预案的可执行性与团队协同能力。发生安全事件后，必须按规定时限向网信等监管部门报告，严禁迟报、漏报、谎报，最大程度降低事件影响。

# 风险评估与应急处置

vinchin

## 特定情形的风险评估

存在下列情形之一：

- 发生重大数据安全事件或被通报存在重大数据安全风险
- 提供、委托处理、共同处理重要数据
- 重要数据的处理者出现重大变化、承载系统发生重大变更
- 向境外提供数据等高风险数据处理活动
- 其他可能危害国家安全、公共利益或严重危害个人、组织合法权益的情形

## 评估方式

- 自行评估
- 委托第三方评估

★ 第三方应当为国家有关部门认定的专业检测评估机构，或符合国家有关规定的其他机构

## 评估报告

- 符合国家和行业有关规定
- 至少保存3年

## 问题整改

- 及时整改问题，消除风险隐患
- 及时报告重大数据安全风险、事件或特殊紧急情况

# 重点场景数据安全风险与事故原因

vinchin

| 业务场景 | 主要数据类型 | 突出风险 | 事故常见原因 |
| --- | --- | --- | --- |
| **轨道交通** | 信号控制、车辆调度、CCTV、自动售检票 | 信号干扰、非法控车、乘客数据泄露 | 隔离不足、补丁滞后、备份未能即时恢复 |
| **高速公路** | ETC流水、门架牌识、路况发布 | 扣费错误、诱导屏篡改、数据丢失 | 软硬件故障、恶意软件、时间同步异常 |
| **场站枢纽** | 旅客身份、航班/车次、安检信息 | 敏感信息泄露、系统瘫痪导致人流混乱 | API漏洞、DDoS攻击、单点硬件故障 |
| **货运物流** | 电子运单、车辆轨迹、货主信息 | 商业机密泄露、物流调度篡改 | 内部权限滥用、接口未授权访问、备份数据未加密 |
| **交通调度中心** | 交通流量、信号配时、应急指挥 | 大屏信息篡改、通信中断 | 网络攻击、电力故障、历史数据归档缺失 |

# 典型业务场景数据保护要求（参考）

vinchin

| 业务场景 | 关键数据 | 灾备核心要求 | 恢复验证要求 |
| --- | --- | --- | --- |
| 轨道交通 | 信号系统配置/参数、列车运行图、自动售检票交易、乘客票务信息等 | 热备冗余+离线备份，实时同步保护，高可用性、实时性、数据完整性、容灾备份 | 每月至少一次沙箱恢复启动信号系统镜像验证 |
| 高速公路 | ETC交易流水、车牌识别数据、费率表、路网监控视频、交通流量数据等 | 异地备份，防止区域性故障；核心数据库定期快照，数据一致性、防篡改、异地备份、快速恢复 | 每季度验证一次全库恢复与流水完整性 |
| 场站枢纽 | 旅客身份信息、安检图像、航班/车次数据、场站运营数据、安防监控等 | 加密备份，数据脱敏后用于测试，离线副本隔离，个人信息保护、视频数据安全管理、分类分级 | 每半年进行全流程应急接管演练 |
| 货运物流 | 货物追踪数据、车辆GPS数据、电子运单、仓储信息、 | 业务系统整机备份，支持即时恢复，数据真实性、全链路防篡改、多方数据共享安全、隐私计算 | 每次系统升级后执行恢复校验和业务测试 |
| 交通调度中心 | 全局交通态势数据、应急指挥指令、交通控制策略参数等 | 核心数据识别与重点保护、最高等级安全防护、传输加密 | 每次系统升级后执行恢复校验和业务测试 |

vinchin

# PART 02

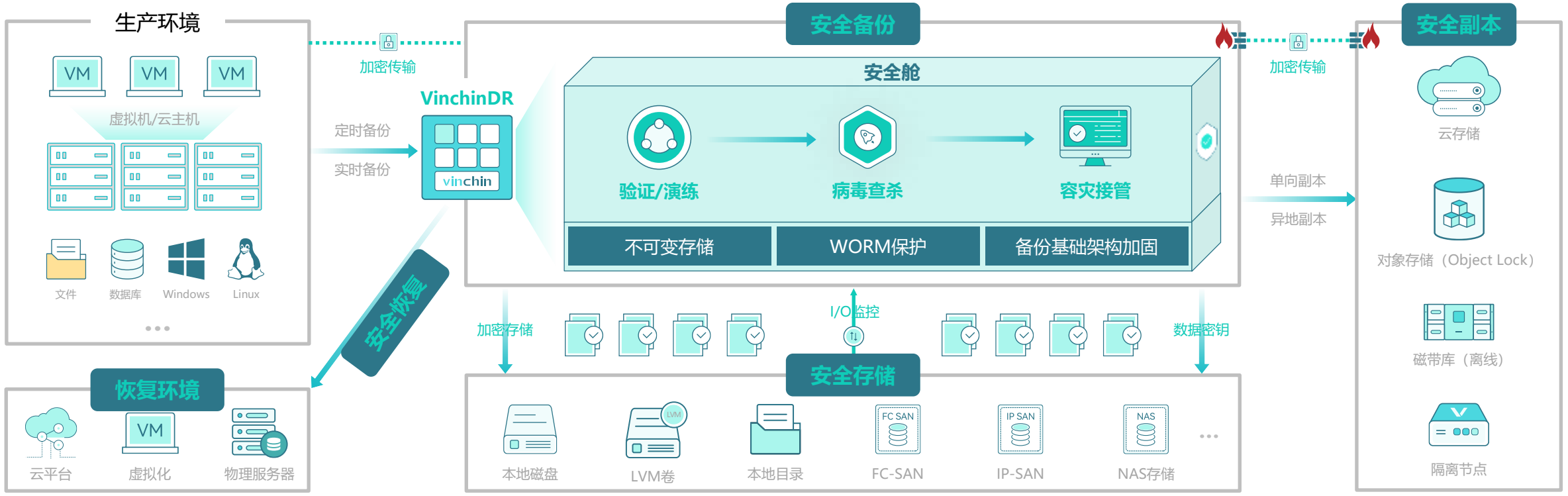
# 云祺合规解决方案

# 数据全生命周期管理

vinchin

3-2-1-1-0-0

访问控制 | 增强身份验证 | 加密通信 | 安全配置模板 | RBAC | 全域行为审计 | Syslog/SIEM集成




**全程加密防护**

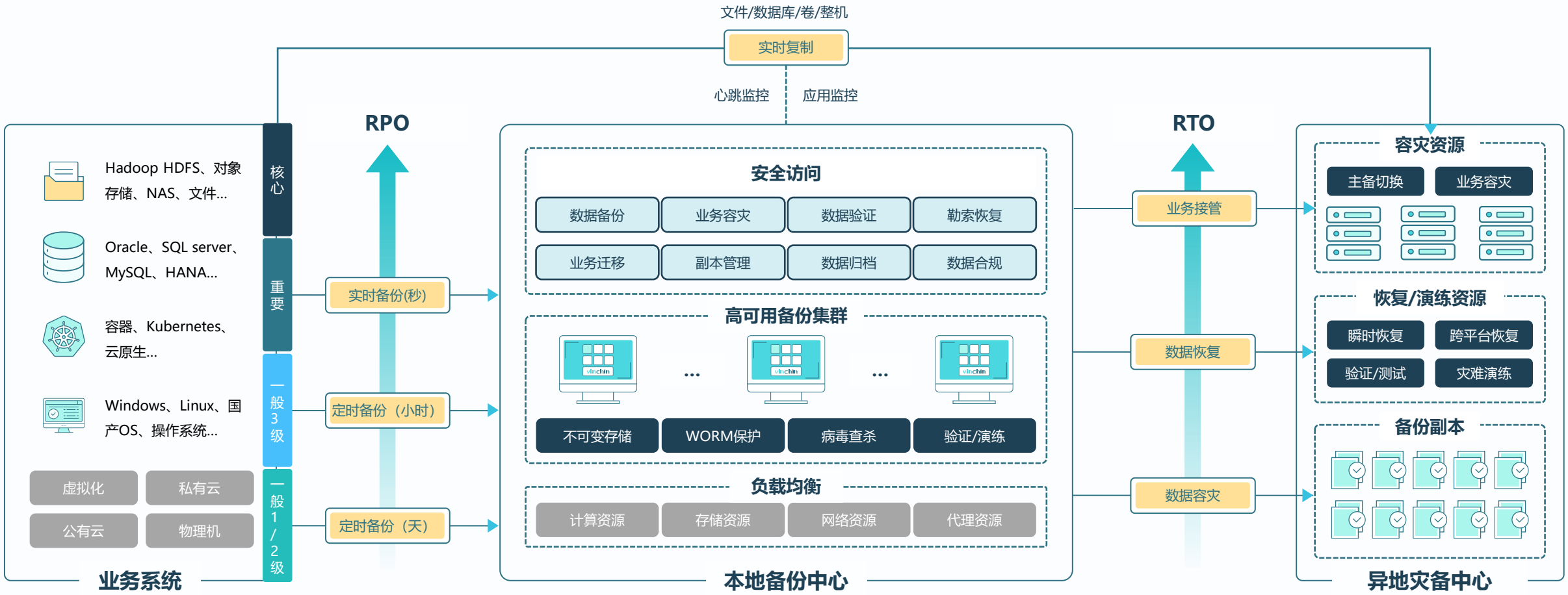
**WORM 防篡改**

**异地副本容灾**

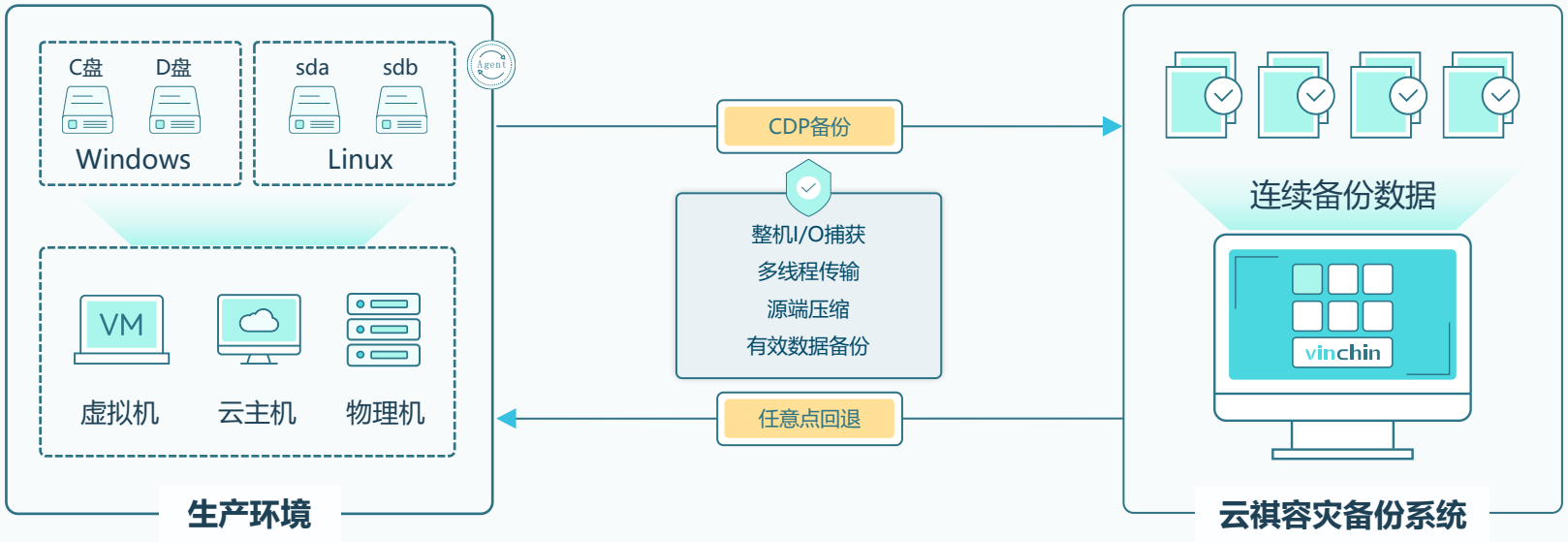
**全生命周期归档**

# 数据分级保护

vinchin



# 核心/重要数据 整机实时保护




## I/O实时捕获，RPO≈0

将每一个生产系统的磁盘I/O实时同步到云祺容灾备份系统中，支持任意时间点回退或恢复

## 实时备份，瞬时恢复

支持对业务系统进行整机级秒级恢复，极大压缩恢复时间目标(RTO)，有效保障业务连续性不中断。

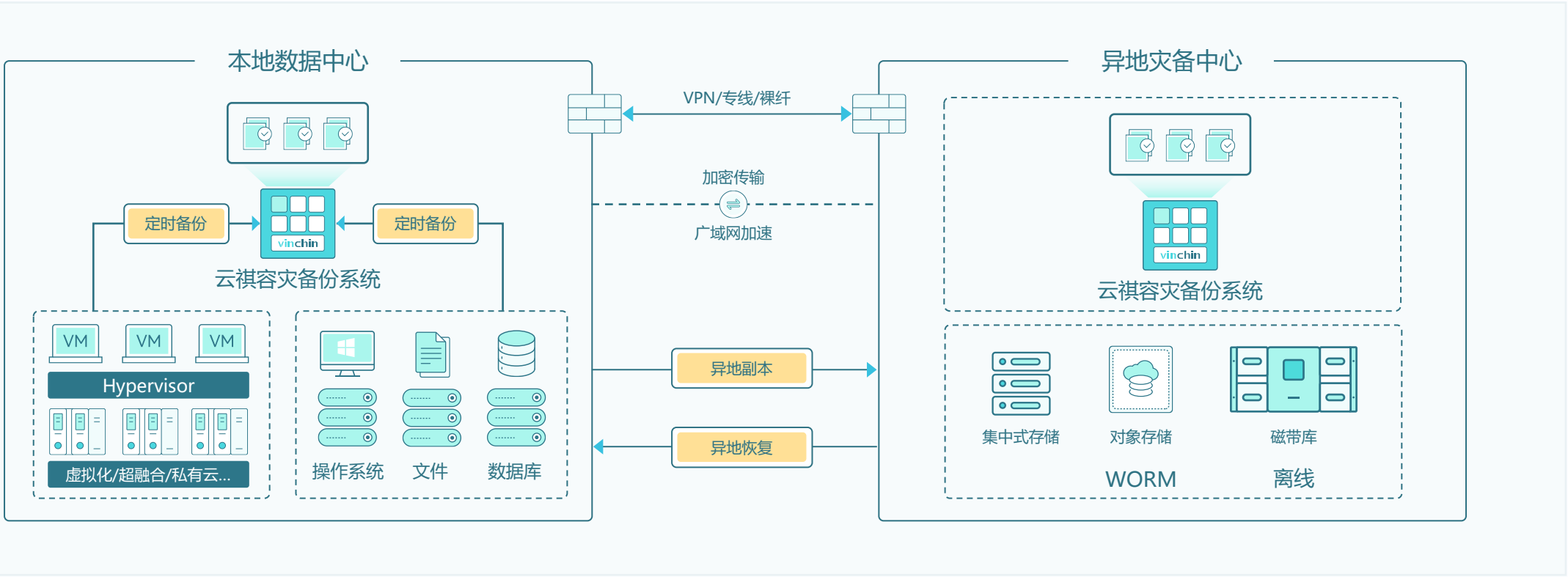
## 应用一致性保障

支持识别应用并定期刷新数据，确保及时落盘的同时记录一致性恢复点，在恢复时可通过标签快速定位

## 动态负载调度

可根据生产主机内存负载动态调度任务状态，实现实时备份的同时避免对生产业务的影响

# 核心数据异地容灾




## 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。

## 业务异地容灾

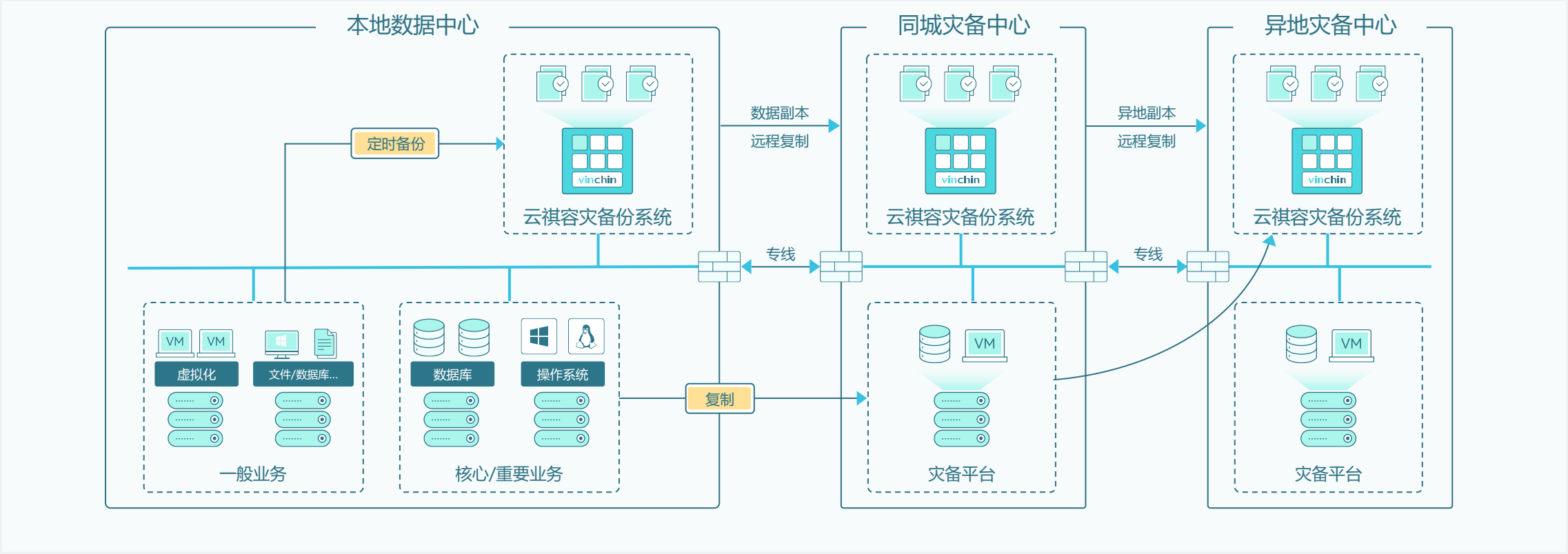
本地实时备份的同时，向异地容灾环境实时复制，即使本地系统全部故障，也可在异地拉起核心业务

## 统一管理

一个平台统一管理两地本地备份、异地副本、异地容灾，结合可视化大屏实现轻松监控运维

# 两地三中心安全灾备方案

vinchin




## 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。

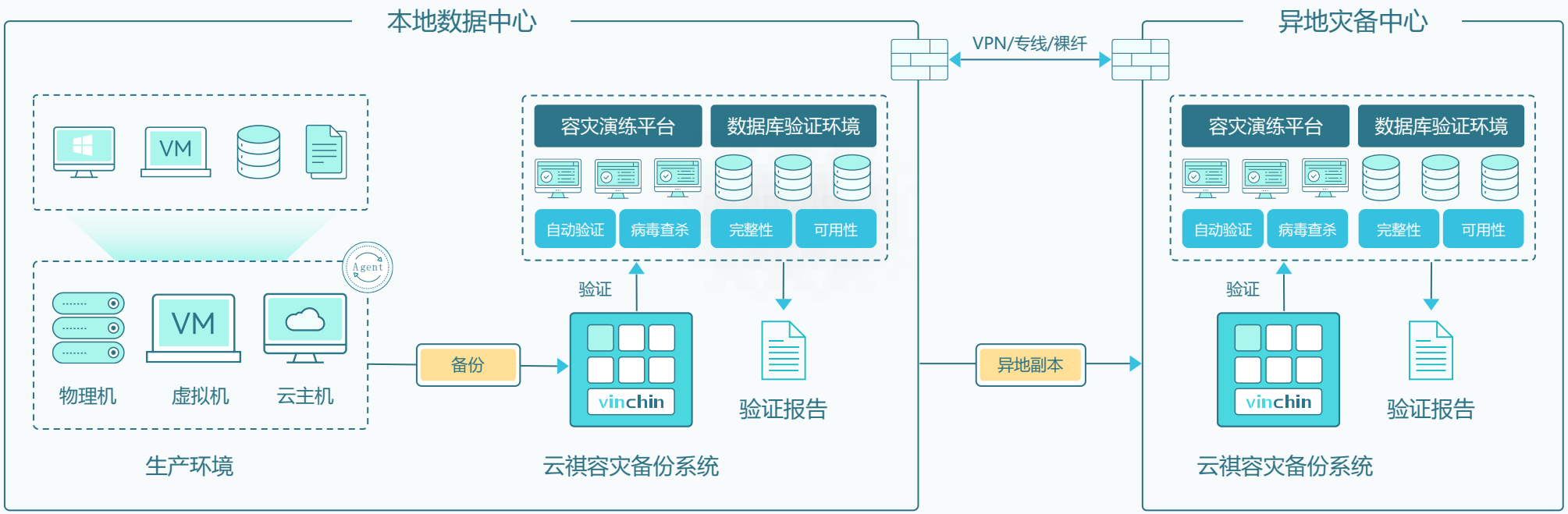
## 异地数据容灾

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。

# 数据演练验证




## 隔离环境病毒查杀

验证过程全程与生产环境隔离，结合第三方杀毒软件，在隔离环境对备份数据进行查杀。

## 降低验证成本

使用内置容灾演练平台可直接拉起系统环境进行数据验证，减少用户隔离环境搭建成本。

## 安全合规

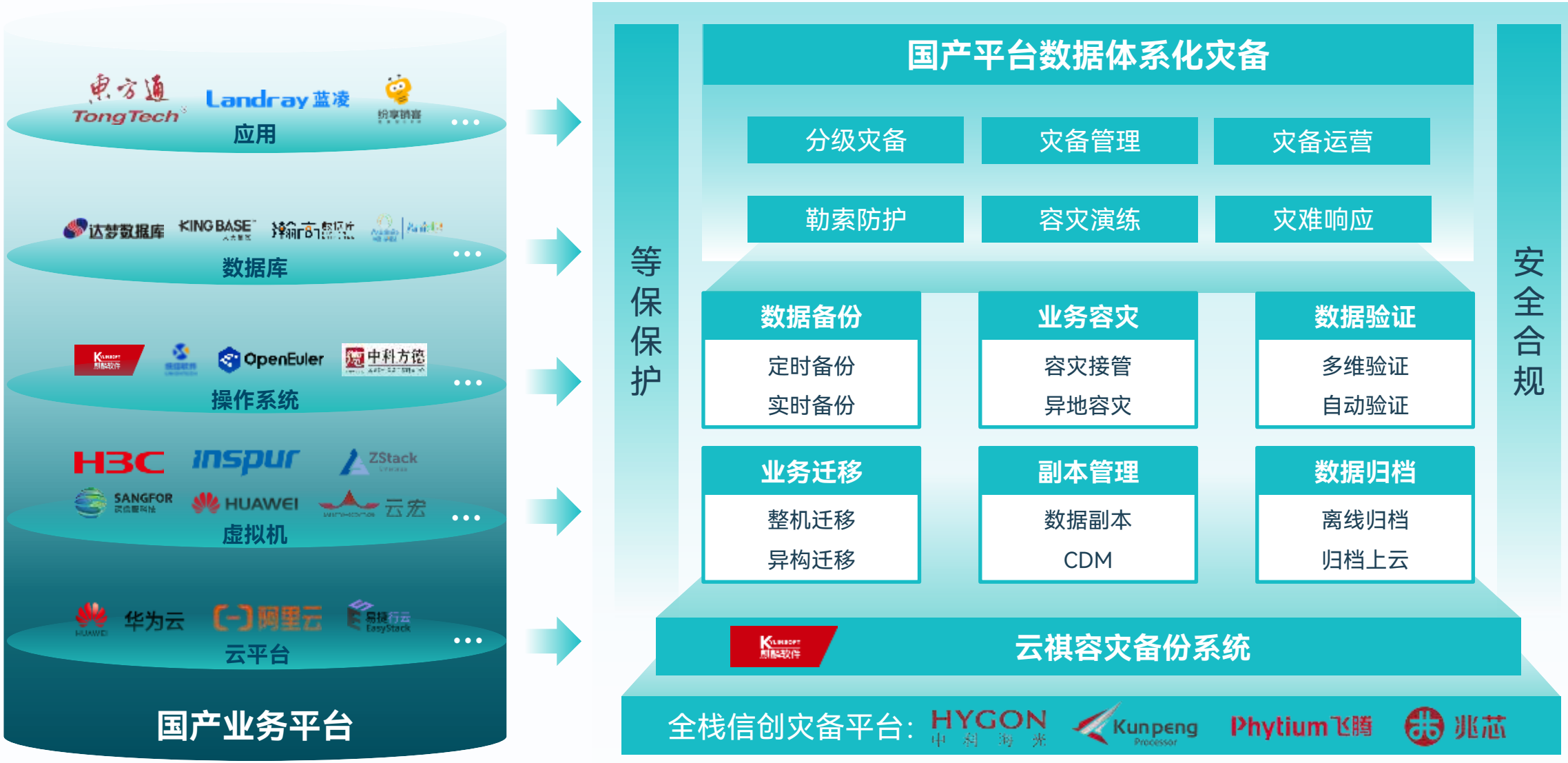
通过定期进行容灾演练，生成数据验证以及病毒查杀报告，企业可以大大增强其安全合规性。

## 可视化验证报告

自动生成验证报告，确保验证结果可视可见，可发送到邮箱，支持自定义报告模板。

# 灾备国产化实施

vinchin



# 总结：合规功能矩阵

vinchin

### 01 数据底层安全保护

采用**不可变存储技术**构建勒索防御屏障，确保备份数据不被篡改或删除，从源头阻断勒索病毒对备份资产的威胁。

### 02 全域数据备份

覆盖虚拟机、数据库、文件系统、NAS及云环境的**全场景备份能力**，实现业务数据的统一采集，消除传统备份的覆盖盲区。

### 03 容灾备份与恢复演练

基于CDP**持续数据保护**实现秒级RPO，支持一键接管与异地容灾，提供自动化恢复演练功能，验证数据可用性。

### 04 全生命周期数据管理

建立“采集-备份-归档-销毁”的**全流程闭环体系**，支持多副本策略与分级存储，兼顾数据合规留存与存储成本优化。

### 05 日志留存与合规审计

全链路操作日志**加密留存且不可篡改**，自动生成符合网安法要求的合规审计报告，满足监管追溯需求。

### 06 国产化合规替换

全面适配鲲鹏、飞腾、麒麟、统信等主流信创生态，支持国产化数据库与中间件的无缝备份，**助力行业信创改造落地**。

vinchin

# PART 03

## 案例分享

# 某铁路公司

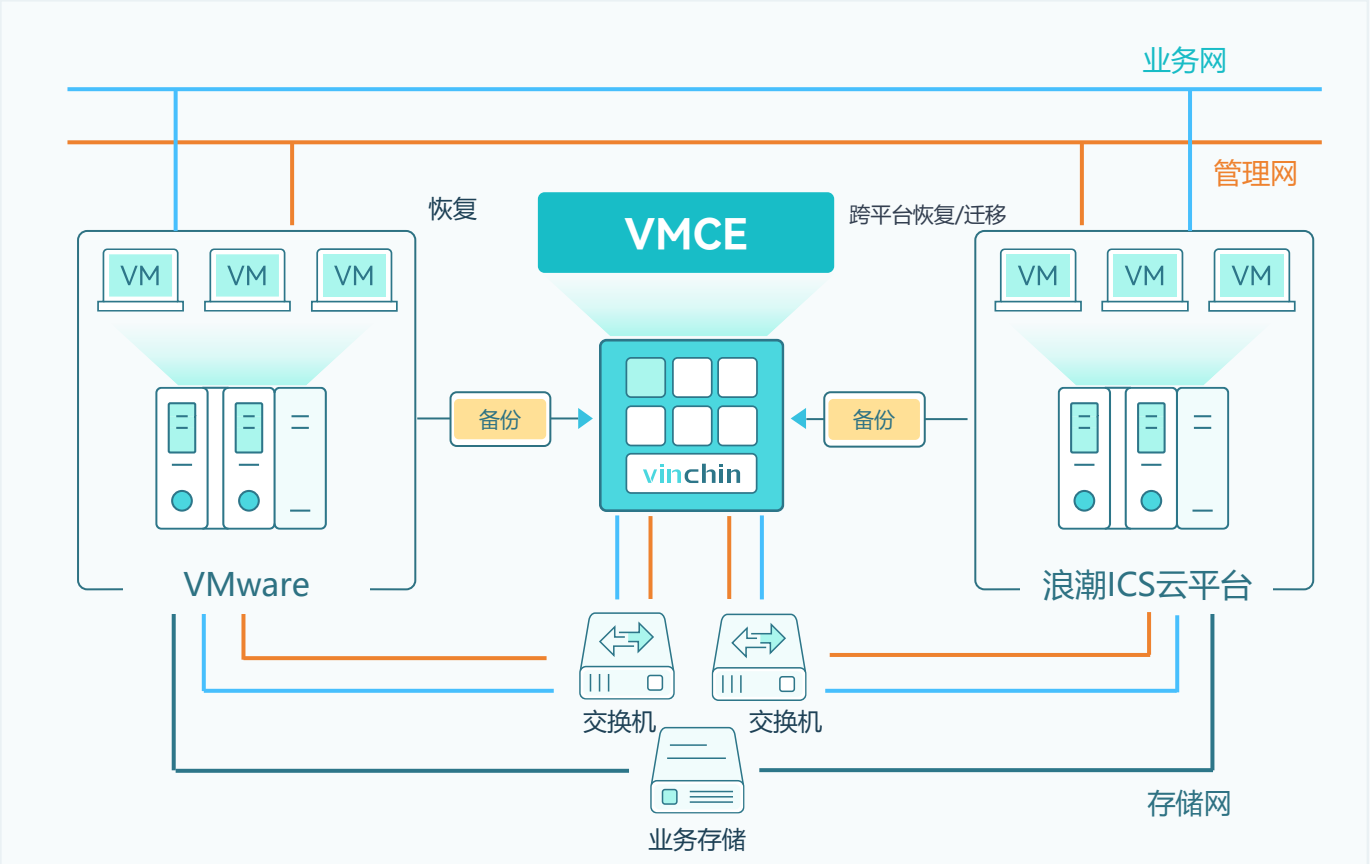
vinchin

## 现状及需求

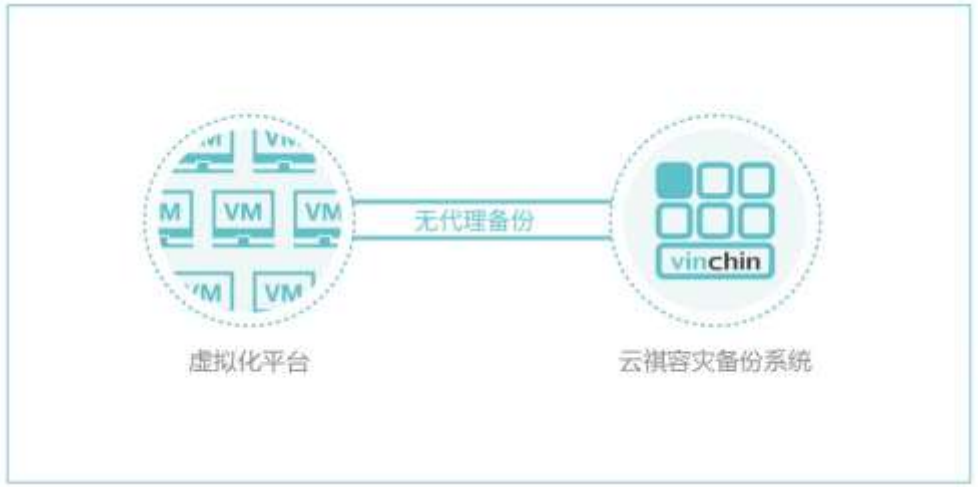
- 该铁路公司大量业务数据运行在VMware vSphere虚拟化平台；
- VMware计算和存储资源紧张，新建国产浪潮ICS私有云平台；
- VMware vSphere虚拟化平台业务数据通过NBU备份产品进行数据保护；
- NBU备份系统老旧，无原厂技术支持，维护成本高，且存储空间不足，无法备份新建国产浪潮ICS私有平台数据；

## 云祺方案及价值

- 采用无代理方案实现VMware和浪潮ICS私有云平台数据保护；
- 通过异构无代理跨平台恢复技术实现VMware到浪潮ICS私有云平台的数据迁移及数据快速恢复演练；
- 虚拟演练室功能定期自动验证备份数据完整性，减少运维工作量；
- 国产化软硬件灾备系统满足合规性要求。



# 瑞士BVB（公共交通运营商）





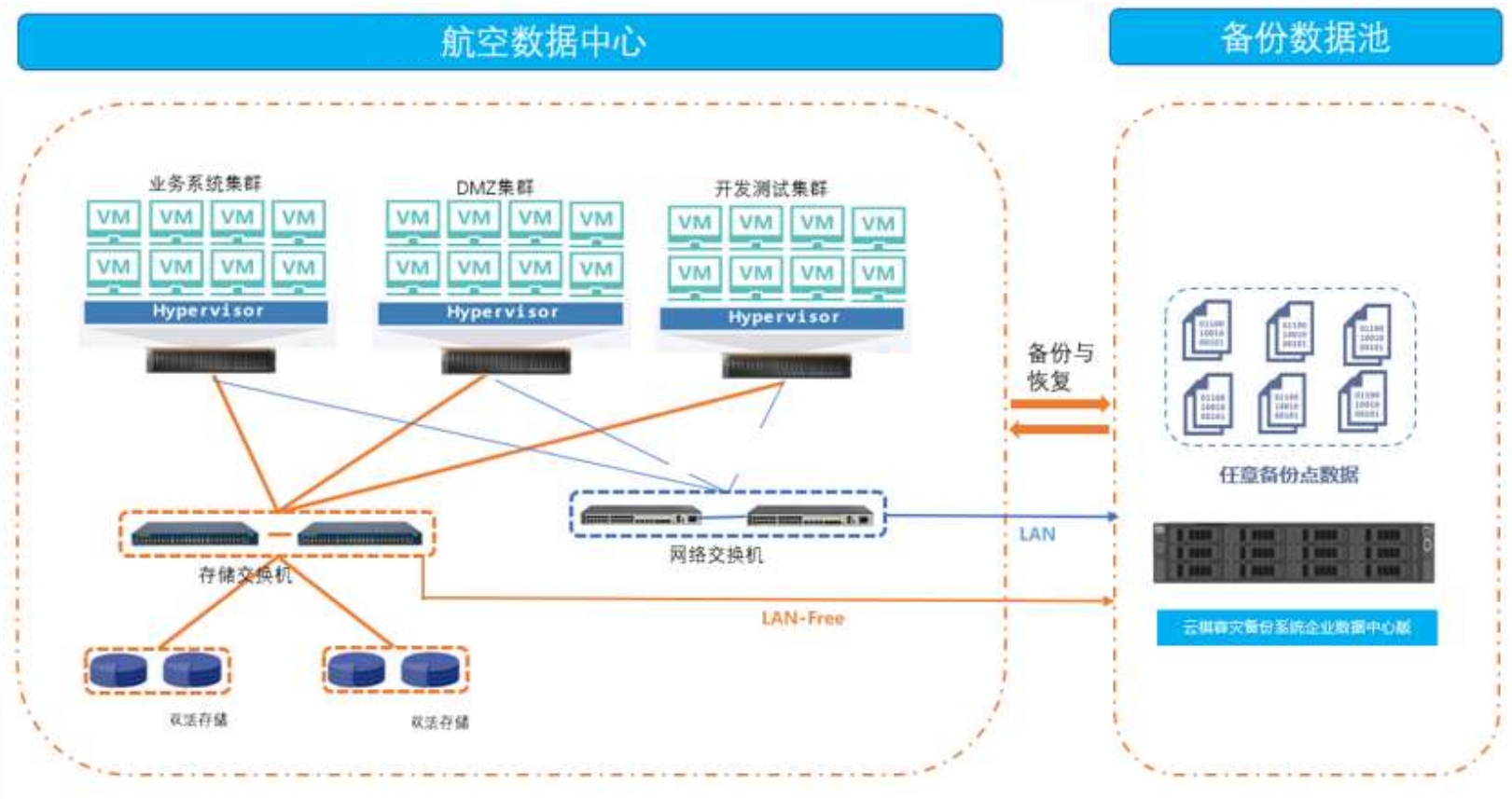
## 现状及需求

- BVB建立了以XenServer虚拟化平台为构架IT业务系统，并且配有简单的备份保护系统，但需要为每台新增的虚拟机安装代理程序，才能执行备份任务。
- 随着BVB的业务量增加，之前的备份系统无法承担当前业务保护压力。员工在运营备份和恢复工作上花费了双倍甚至更多的时间，这影响到了他们的日常服务工作。因此，需要一个更有效的备份解决方案，解决目前复杂的IT系统保护管理压力，提高业务运维的工作效率，同时，减轻新增虚拟机时的工作负载问题。

## 云祺方案价值

- 无代理备份：只需要花费几分钟就可以将云祺备份系统安装到对应的Xenserver环境，新增再多的虚拟机都不用担心以前繁琐的代理安装工作。
- 备份节点扩展：考虑到BVB不断增长的环境，提供了备份节点扩展功能，可以备份多个 XenServer群集，并同时将这些数据拆分到多个存储设备。并且所有这些节点都由一个WEB控制台管理。
- 多用户管理：对备份系统的权限进行设置，只有指定的员工才有权通过管理员帐户访问系统，其他人可以通过其他用户帐户进行访问。不同的帐户权限设置实现高效管理和监控工作。

# 某航空有限公司




## 现状及需求

- 现存3个某虚拟化平台集群，由三套双活存储承载，超过20台服务器的超大虚拟化平台，其中运行着重要的业务系统，一旦出现系统崩溃，将会为企业带来不可衡量的损失。
- 数据备份需考虑未来数据增长的趋势灵活扩展，且三个不同的业务集群需要统一的保护和管理，备份过程中不能影响业务系统的稳定运行，不能改变现有系统架构，需要一套高效的数据保护方案。

## 云祺方案价值

- 采用无代理模式进行三个集群平台虚拟机备份；
- 采用LAN-Free传输机制，提高备份任务的传输速度，降低备份时间窗口；
- 利用瞬时恢复功能，将测试环境快速恢复，验证数据有效性；