vinchin

全栈容灾，筑牢企业业务韧性

主讲人：钟广宁

vinchin

目 录

vinchin

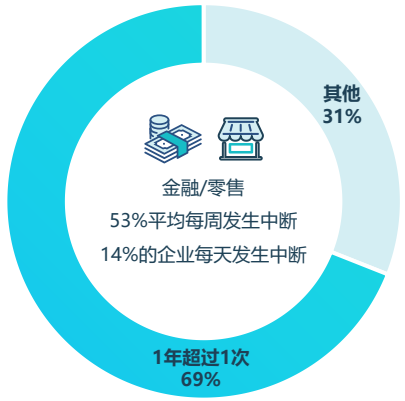
PART 01

业务连续性背景与挑战

灾难威胁升级，数据丢失/业务中断损失重大

vinchin

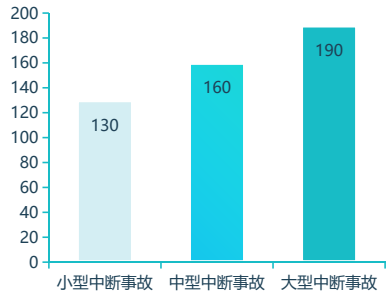
多数企业每年遭遇业务中断



业务中断频次统计

数据源：*New Relic-2024 Observability Forecast*

中断损失10万美元/hour



业务中断损失中位数统计（万美元）

数据源：*Cockroach Labs-The State of Resilience 2025*

业务中断使企业面临多重损失

44%

生产经营损失

生产停滞、工作流程中止或进度缓慢、产品或服务订单交付能力受限等导致的直接收入损失

17%

恢复/重建成本

硬性的恢复资源与环境成本、无法预估的人力投入以及无法保证完整恢复的技术支持服务支出

39%

其他隐形损失

品牌声誉损失以及客户信任流失将造成长期财务影响，违规罚款、甚至吊销营业执照以及面临法律风险

发生业务中断的企业中，绝大部分企业营收都会受到影响，其中34%的企业收入大幅下滑，而12%的企业则因客户赔偿、订单锐减、高额罚款、吊销许可等导致停业或倒闭

业务中断使安全团队面临个人风险

失职问责

精神压力

降职/解雇

法律责任

故障风险类型

vinchin

硬件与基础设施故障	硬盘物理损坏	阵列故障	存储控制器故障	存储控制器故障	服务器故障	网络硬件故障
	网络拥塞	负载均衡故障	电力故障	空调故障	物理安全	…
软件与系统故障	系统崩溃/蓝屏	系统文件损坏	内核panic	数据库崩溃	数据库损坏	数据库配置错误
	代码Bug	中间件故障	虚拟化故障	虚拟机文件损坏	网络存储下线	…
网络与通信故障	服务不可达	DNS故障	网络协议问题	网络分区	IP冲突	路由错误
	ACL规则错误	VLAN错误	主干网络中断	CDN失效	网络时延	…
人为错误	文件/数据误删	配置文件误改	误覆盖	执行错误命令	错误的系统操作	版本部署错误
	系统升级中断	变更管理不当	权限管理不当	恶意删除数据	恶意操作	…
安全事件	勒索软件	病毒/蠕虫	木马	DDoS攻击	SQL注入	暴力破解
	撞库	内部威胁	APT攻击	间谍软件	数据泄露	…
灾难性事件	地震	洪水	强风暴	火灾	大规模电力中断	大规模网络攻击
	纷争/恶意活动	极端高温	工业事故	…		

衡量灾备能力的黄金指标：RTO & RPO

vinchin

RTO (Recovery Time Objective)· 恢复时间目标

定义：从灾难发生到业务系统恢复正常运行所经历的时间长度。
目标：数值越小越好，代表业务中断的时间越短。如 RTO=5分钟。

RPO (Recovery Point Objective)· 恢复点目标

定义：灾难发生后，系统恢复的数据状态对应的时间点，即允许丢失的最大数据量。
目标：数值越小越好，代表数据丢失越少。如 RPO=0 代表零数据丢失。

灾难发生点
业务中断 / 数据写入停止

RPO 数据恢复
基于备份恢复到可用状态

RTO 业务恢复
系统上线，对外提供服务

传统恢复方式的四大痛点

vinchin

01. 恢复时间长 (RTO高)

传统备份多为全量或增量备份，数据恢复过程耗时漫长，动辄数小时甚至数天，严重影响业务连续性。

⚠ **痛点：业务中断时间长，企业损失巨大。**

02. 数据丢失多 (RPO高)

恢复过程可能因数据损坏或不完整导致部分数据丢失，无法确保恢复后数据的完整性和一致性。

⚠ **痛点：关键业务数据丢失，严重影响业务运行。**

03. 恢复过程复杂

恢复流程繁琐，依赖人工操作，步骤多、易出错，对运维人员的技术水平和经验要求极高，增加了试错成本。

⚠ **痛点：恢复效率低下，且易引入新的操作风险。**

04. 场景适应性差

难以有效应对虚拟化、云环境、数据库、应用等复杂IT架构，无法提供针对性、细粒度的保护和恢复方案。

⚠ **痛点：数据保护不全面，企业IT环境存在安全盲区。**

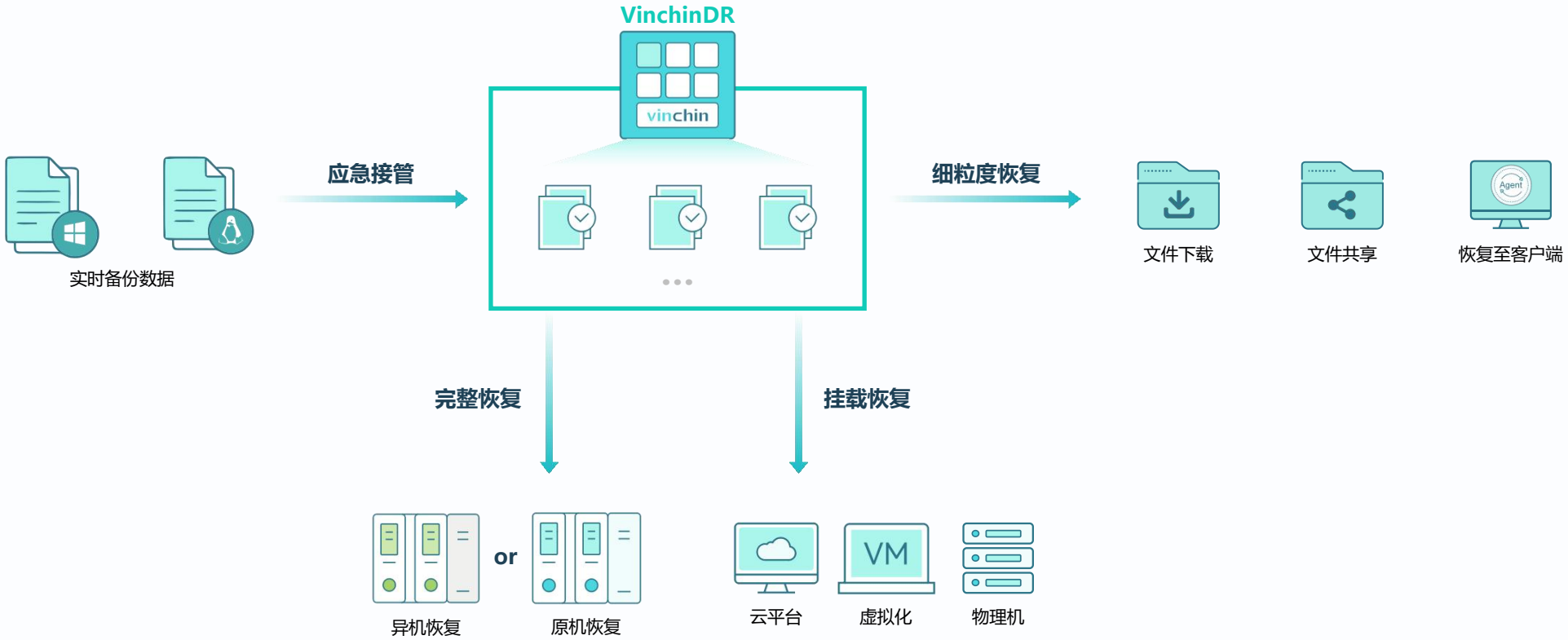
vinchin

PART 02

弹性恢复能力解析

灵活恢复选项，满足不同恢复需要

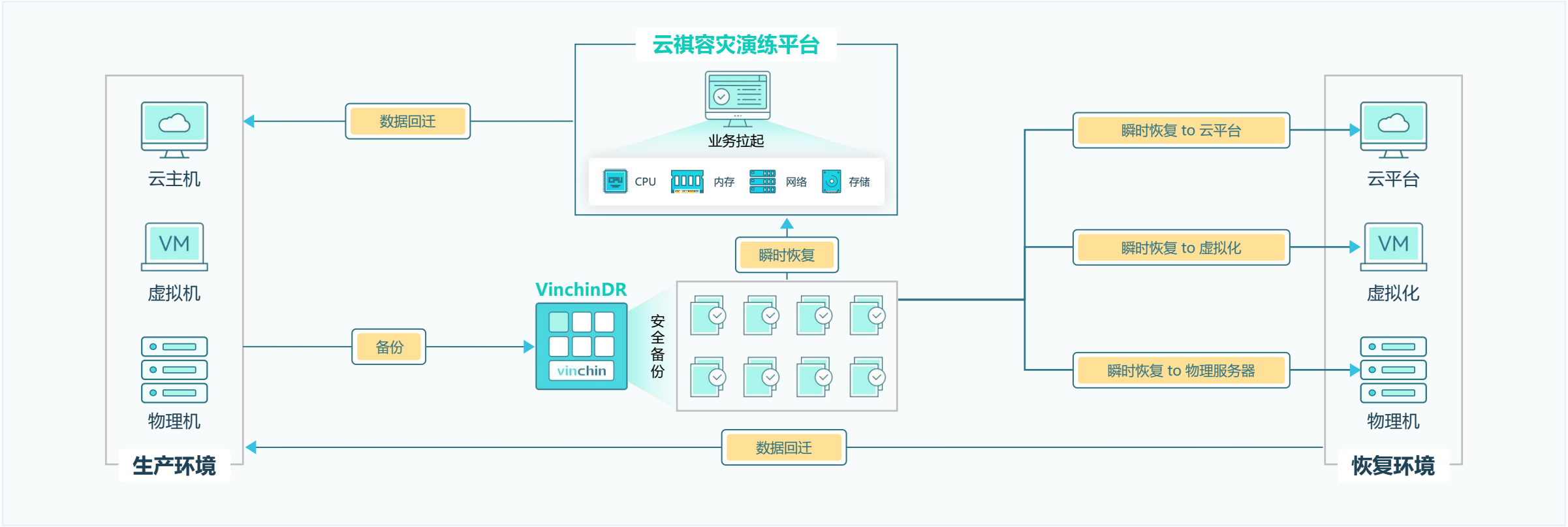
业务系统可能需要根据重要性、RTO/RPO要求、恢复资源位置等实际情况选择不同的恢复方式，因此，提供丰富的恢复手段或选项将使用户可以从容应对复杂的恢复场景，并提升恢复效率和成功率。



瞬时恢复

vinchin

当业务系统发生故障时，需要尽快恢复数据或业务系统来保障业务的连续性，减少业务中断带来的影响和损失，而实际恢复时，准备环境、等待数据传输等过程耗时耗力，将极大的影响恢复效率。



整机瞬时恢复

内置恢复资源

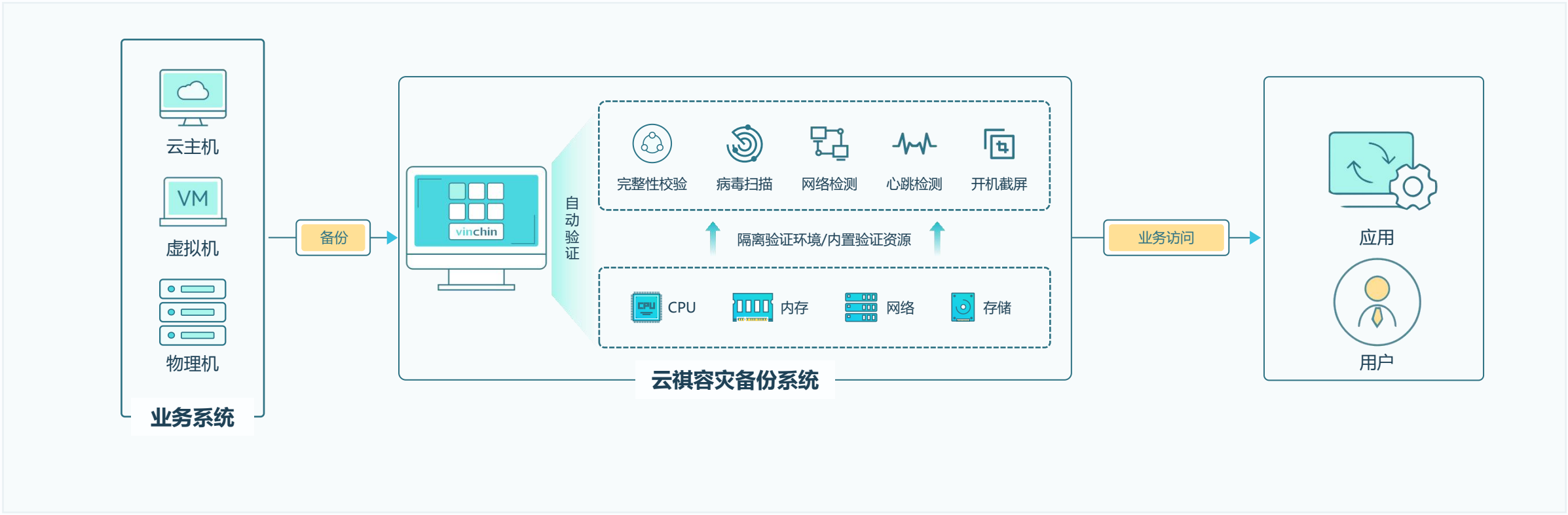
分钟级RTO

一键数据回迁

业务应急接管

vinchin

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

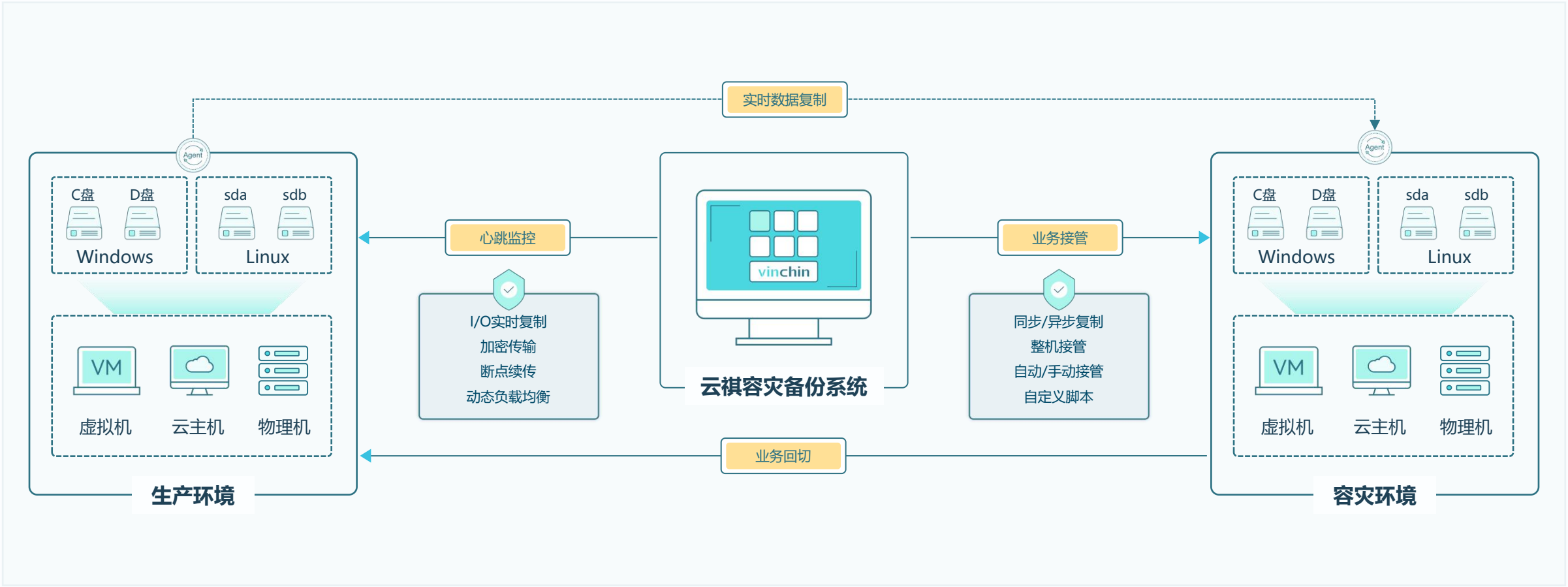
内置恢复资源

分钟级RTO

一键数据回迁

整机复制与容灾

vinchin



实时复制，RPO≈0

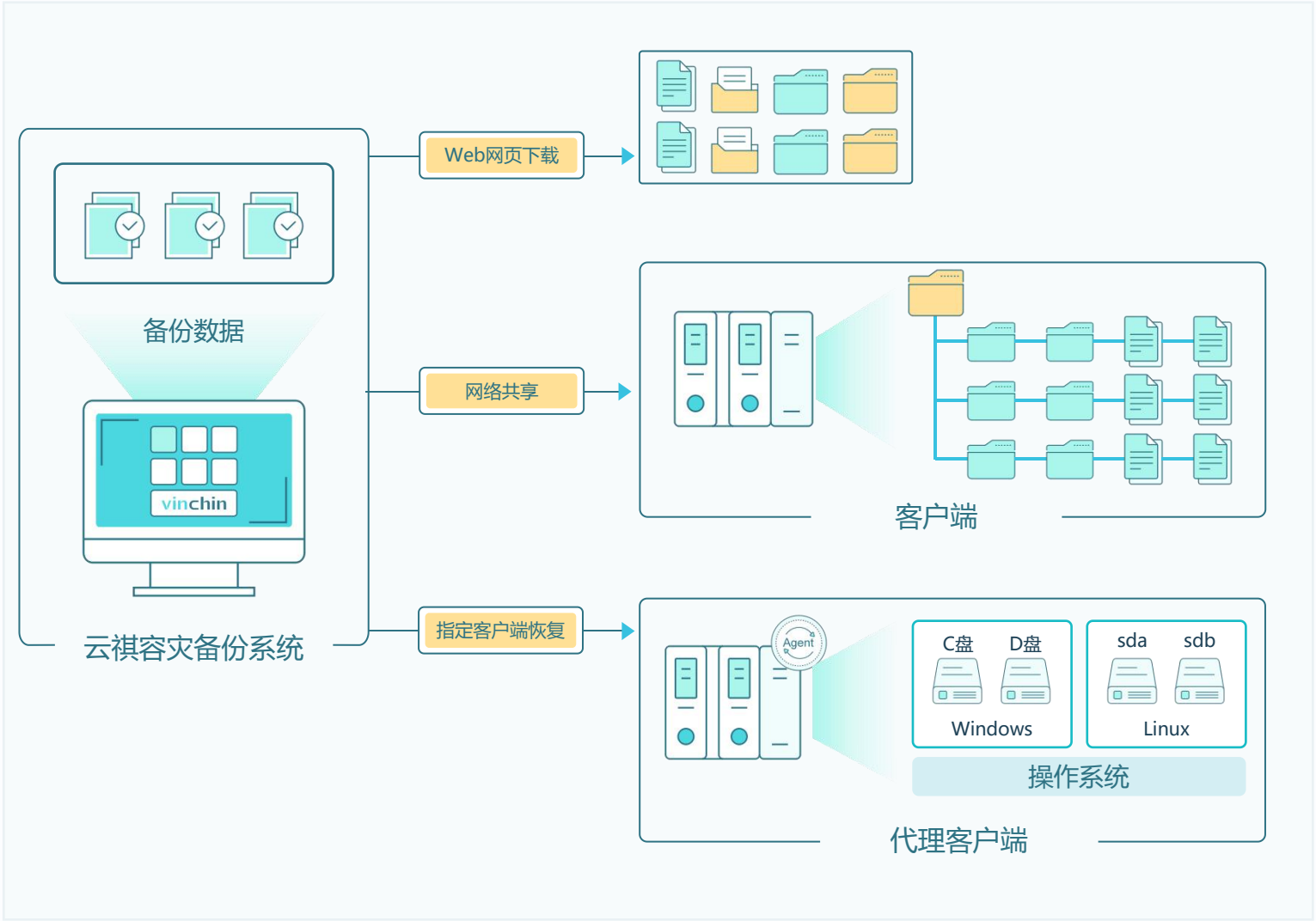
应用一致性保障

整机容灾接管，RTO≈0

业务一键回切

文件细粒度恢复

vinchin



WEB网页下载

通过浏览器Web页面，可直接查看任意备份时间点数据的文件/文件夹，支持立即下载所需文件/文件夹。

网络共享

通过smb网络协议将文件系统挂载到客户端进行生产、测试、演练。

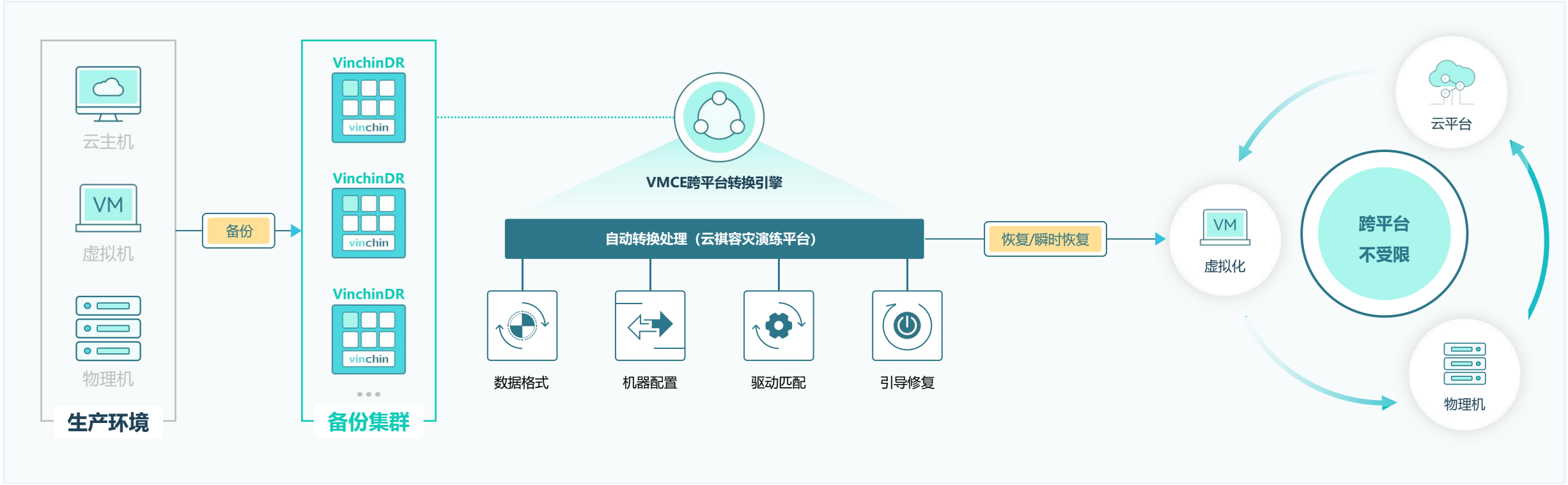
指定客户端恢复

支持选择需要恢复的某一个/多个文件/文件夹，指定恢复路径至安装代理的原客户端/其他任意客户端，恢复的文件/文件夹具备读写权限。

跨平台数据自由转换

vinchin

当遇到平台级故障时，恢复可能受到异构数据格式差异、驱动缺失、系统引导损坏等诸多环境因素的限制，最终导致无法成功恢复业务。因此，提供完善的跨平台灾难恢复能力有助于进一步提升勒索恢复的效率和成功率，增强业务韧性。



异构智能转换

根据目标平台类型自动转换数据格式与系机器配置

驱动智能替换

根据系统配置需要自动从内置驱动库匹配驱动进行替换

引导自动修复

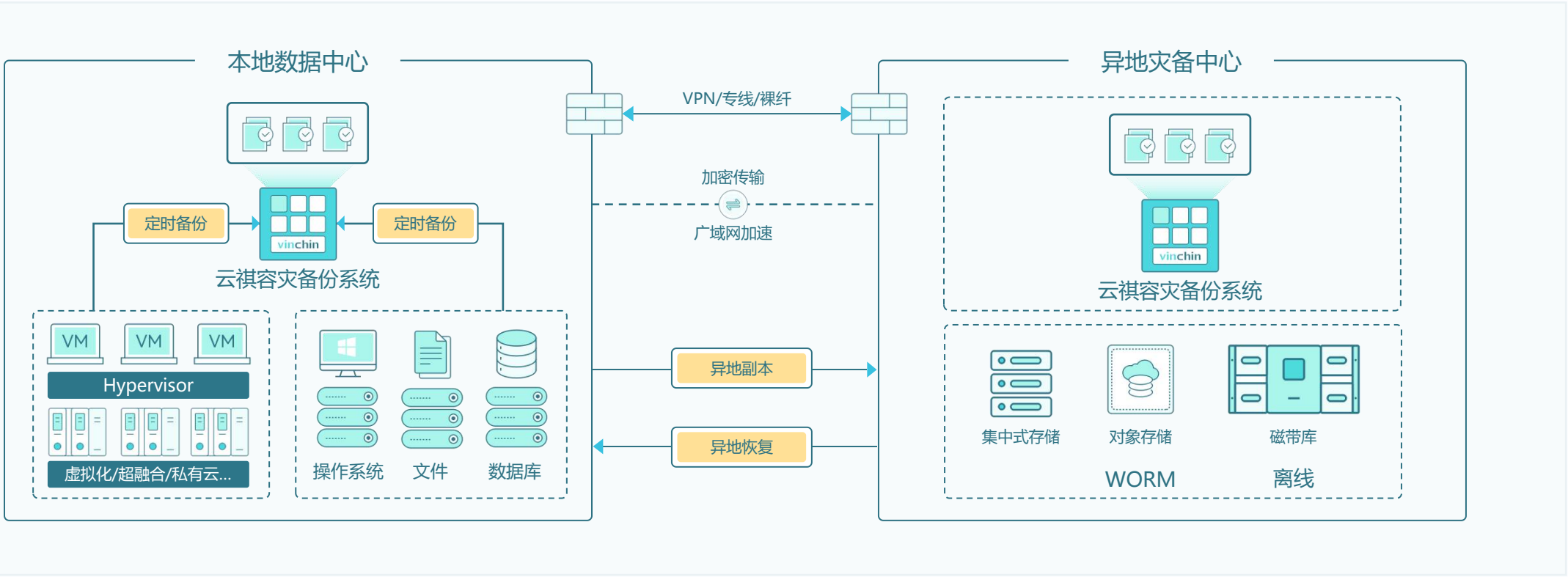
无需手动干预，恢复后自动修复系统引导，确保成功恢复

平台级容灾

不受位置、备份方式限制，任意支持平台双向弹性恢复

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，可在异地进行数据恢复。

窄带宽异地传输

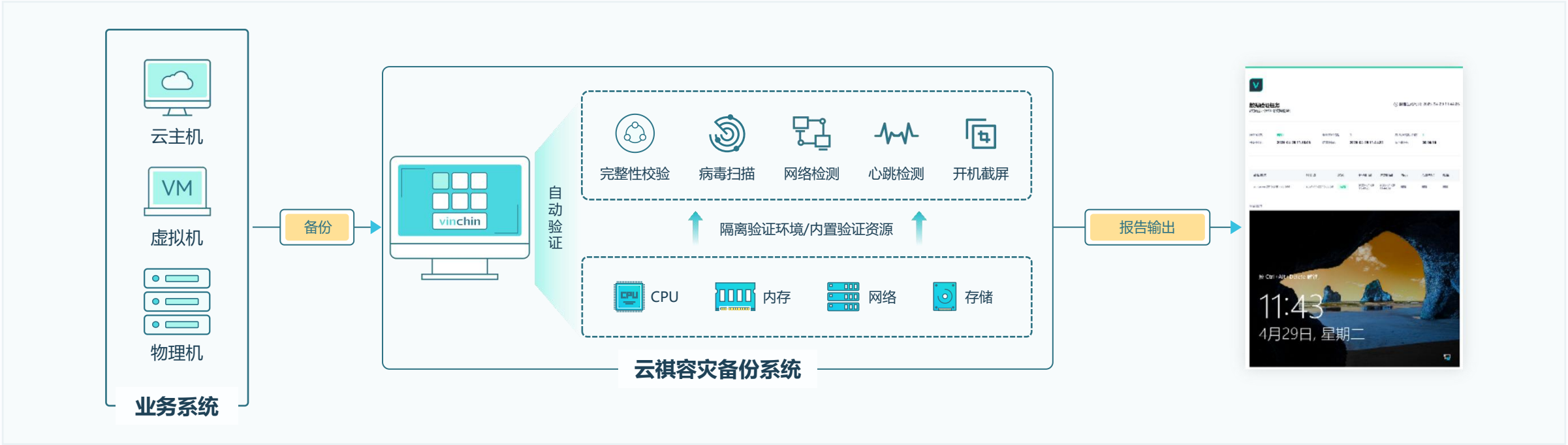
通过源端压缩、断网续传以及永久增量副本等技术适合窄带宽场景，提升传输效率。

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。

数据验证与灾难演练

备份像是一个“黑盒子”，在没有恢复前，我们无法知道备份是否真正可用。实际恢复时，也有可能数据出现非预期的问题导致恢复失败。因此不仅要做好备份，还应通过验证来不断测试、检验备份，以确保在需要恢复时，备份处于可用状态。



无需准备资源

无需额外准备服务器、存储、网络等资源，可直接备份系统内置资源进行验证

无需搭建环境

无需手动搭建操作系统、应用、网络等环境，备份系统将自动生成隔离环境进行验证

自动验证、安全合规

支持批量自动验证，自动回收清理验证资源，验证结束后将生成可视化验证报告

灵活利用，提升数据价值

支持用户使用容灾演练平台的内置资源拉起主机进行数据查询分析、验证测试等

vinchin

PART 03

案例实践

应急接管与容灾应用案例

vinchin

案例一：大型游乐园售票系统故障5分钟恢复

在一个周末的上午10点，某著名大型游乐园迎来入园高峰，售票窗口和线上渠道排起长队。突然，核心售票系统因底层存储硬件故障完全宕机——所有售票窗口无法出票，线上App显示错误，园区入口陷入停滞。每分钟，都意味着巨大的收入损失和不可估量的客户满意度暴跌。

应急过程：

- **告警与决策　（故障发生后1分钟）：**运维工程师确认售票系统不可用
- **一键瞬时恢复（故障发生后2分钟）：**运维工程师通过云祺容灾备份系统控制台，启动瞬时恢复流程
- **业务恢复正常（故障发生后5分钟）：**窗口恢复出票，App可正常下单，入园流程恢复正常。游客仅感受到短暂“卡顿”

案例二：大型汽运物流企业业务调度系统故障，30 分钟内完成应急接管

某大型汽运物流企业的 IT 管理员在周一午间发现，核心业务调度中心的虚拟机突然运行缓慢、关键业务数据无法正常访问，整个调度集群出现严重故障 —— 这意味着车辆无法派单、货物无法跟踪、司机与调度员失去联系，全国物流网络面临 “瘫痪” 的风险。

应急过程：

- **隔离与诊断（0-5分钟）：**确认核心调度系统出现异常故障，第一时间隔离故障环境，防止影响扩大。
- **选中与预案启动（5-10分钟）：**运维人员通过云祺容灾备份系统，选中最新的干净备份数据，一键启动应急接管流程。
- **业务验证与恢复（故障发生后10-30分钟）：**经快速验证，调度、派单、跟踪等核心业务功能全部恢复正常。从发现故障到业务全面恢复可用，仅用时约 30 分钟，未对全国物流调度造成重大影响。

vinchin

THANKS

云祺公众号

云祺视频号