vinchin

数据有“轻重”，分级灾备有的放矢

主讲人：吴瑶

vinchin

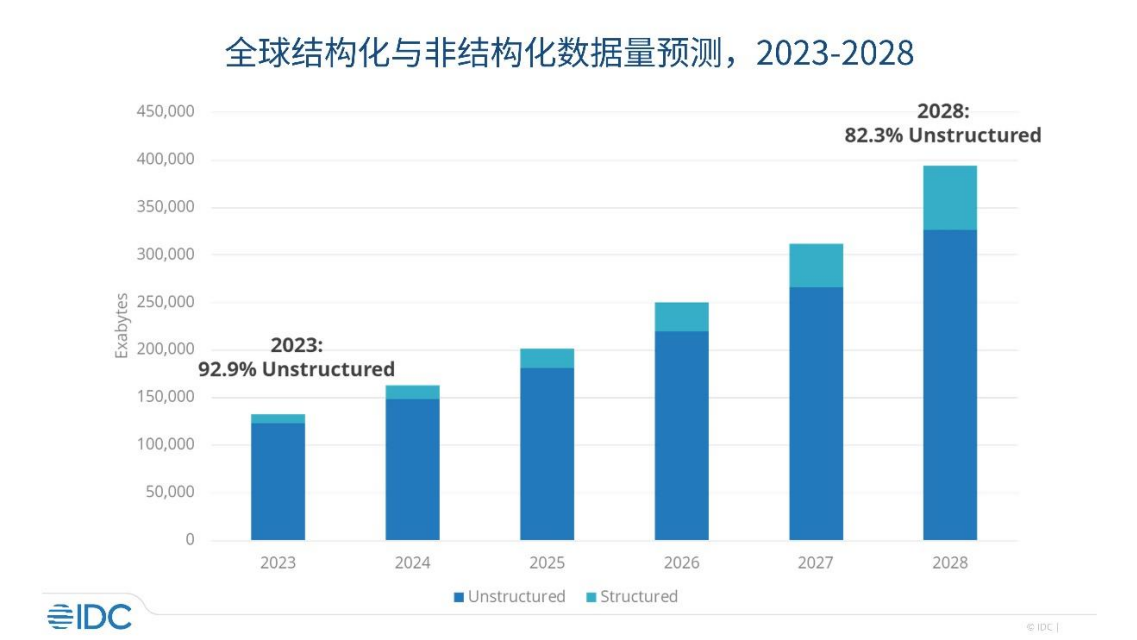
目 录

vinchin

PART 01

数据分级保护建设挑战

数据量激增带来数据安全挑战



IDC 预测，到2028年全球数据量将增长至**393.8ZB**，相比于2018年的39.9ZB，增长9.8倍。中国区数据量将达到接近100ZB。

- **数据量高速增长：**海量数据备份耗费大量时间，而海量非结构化数据备份由于由于各种原因导致的性能瓶颈，跟不上业务数据产生的速度，无法满足RPO要求
- **数据复杂度提升：**不同业务数据之间的关联性变得更加紧密和复杂，缺乏统一管理能力，无法满足数据生命周期管理要求
- **实时性要求高：**大量高并发业务对数据实时性提出更高要求，因此要求对业务数据进行实时保护，几乎不允许数据丢失

数据安全威胁频发，企业面临数据中断风险

vinchin

2024年7月微软蓝屏故障造成史上最大规模宕机，全球各地均受影响。

2023年办公产品语雀因存储升级工具BUG，导致服务器宕机8小时。

2024年6月，香港中文大学遭黑客攻击，约2万名师生信息被盗取。

2023年8月河南特大暴雨。西部数码、河南产权交易中心等中断服务。

业务中断使企业面临多重损失

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。

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。

复杂业务环境带来的数据保护难题

vinchin

方案实施难点

- 保护方案复杂
- 运维压力大
- 数据传输窗口长
- 数据管理难

数据安全合规性要求日益严苛

vinchin

《中华人民共和国网络安全法》

《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》

《信息系统灾难恢复规范 》

《金融数据中心容灾建设指引》-金融

《电子档案管理办法》-档案

《电子病历系统应用水平分级评价标准（试行）》-医疗

.....

信息安全技术 网络安全等级保护基本要求 (等保2.0)

等保二级：应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地；

等保三级：

- 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；
- 应提供重要数据处理系统的热冗余，保障系统的高可靠性。

等保四级：应建立异地灾难备份中心，提供业务应用的实时切换。

网络数据安全管理条例

定期组织开展网络数据安全风险监测、风险评估、应急演练、宣传教育培训等活动，及时处置网络数据安全风险和事件。

信息安全技术关键信息基础设施安全保护要求

7.10 数据安全防护：

e）应建立业务连续性管理及容灾备份机制，重要系统和数据库实现异地备份；

f）数据可用性要求高的，应采取数据库异地实时备份措施。业务连续性要求高的，应采取系统异地实时备份措施。

vinchin

PART 02

数据分级保护规划思路

数据分级基础模型

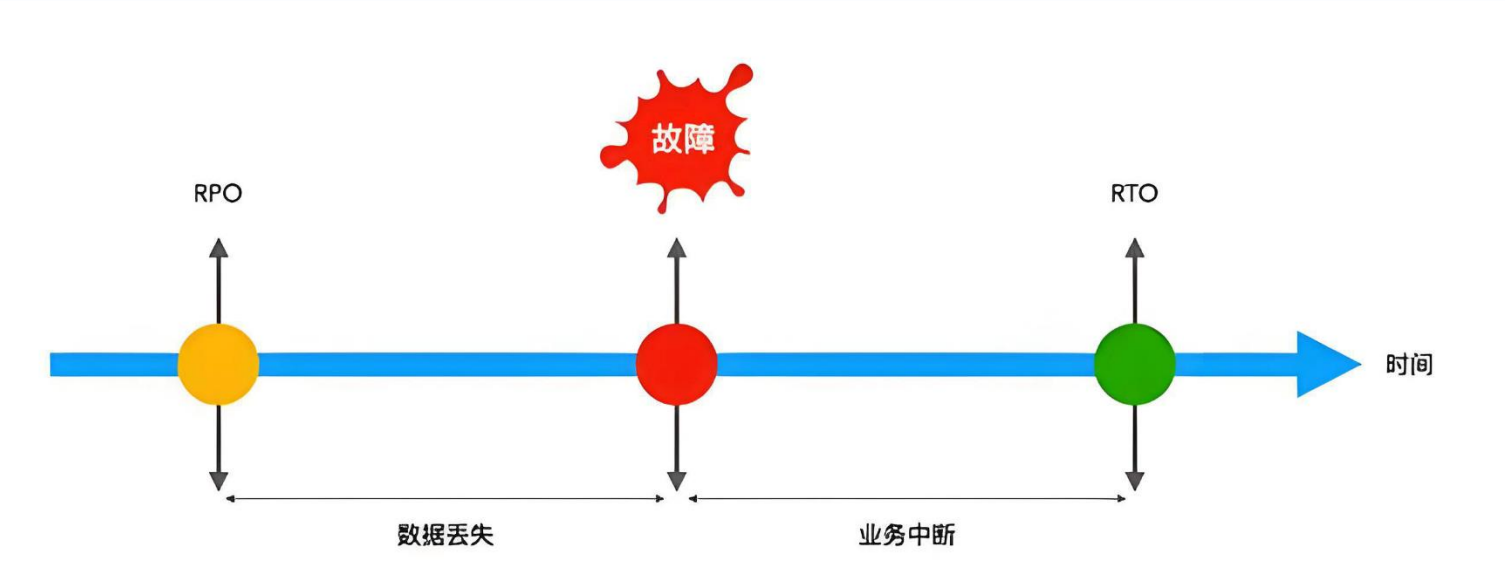
vinchin

RTO(RecoveryTimeObjective，恢复时间目标)

指灾难发生后，信息系统或业务功能从停顿到必须恢复的时间要求。也就是业务恢复运行的最长可接受时间，即**系统停机的容忍上限。**本质上是反映业务恢复的速度，例如：RTO=4小时，需在4小时内恢复服务；RTO≈0，需实现故障自动切换（如热备站点）。

RPO(RecoveryPointObjective，恢复点目标)

指灾难发生后，系统和数据必须恢复到的时间点要求。通俗点讲就是系统**可容忍的最大数据丢失量**，如最多丢失1小时数据。本质上是反映数据备份的频率，例如：要求RPO≤24小时，即最多丢失24小时数据，则需要系统每日备份一次；要求RPO≈0，即近乎零数据丢失，则需要系统实时备份。



相关要求对应的RTO、RPO

vinchin

- GB/T 20988-2025《网络安全技术 信息系统灾难恢复规范》提到不同灾难恢复能力等级的RTO和RPO。
- GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》规定了不同网络安全等级保护的安全通用要求和安全扩展要求。

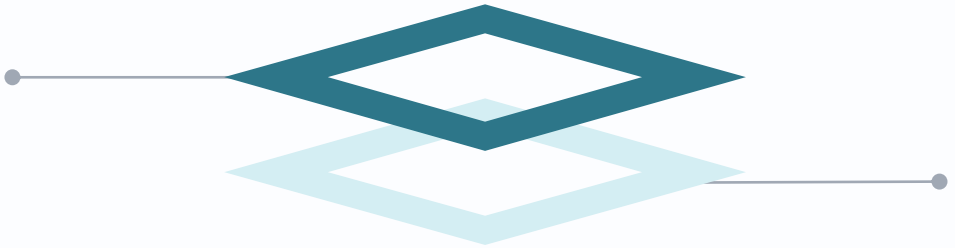
灾难恢复能力等级	相关要求	RTO（恢复时间目标）	RPO（恢复点目标）	等保2.0要求
1	备份	2天以上	1天至7天	一级： 本地备份
2	本地+异地备份	24小时以上	1天至7天	二级： 本地备份+异地备份
3	电子传输和部分设备支持	12小时以上	数小时至1天	二级： 本地备份+异地备份
4	电子传输和完整设备支持	数小时至2天	数小时至1天	三级：本地备份+异地实时备份+本地高可用
5	实时数据传输及完整设备支持	数小时至2天	0至30分钟	四级：本地备份+异地实时备份+本地高可用+异地高可用
6	数据零丢失和远程集群支持	数分钟	0	四级：本地备份+异地实时备份+本地高可用+异地高可用

数据分级常见误区

数据分级不是简单的“贴标签”，而是一项基于风险、驱动决策的持续管理过程 。

误区一：简单分级

简单将数据划分为“高、中、低”级别，忽视定量与定性分析结合，无法识别关键数据资产。

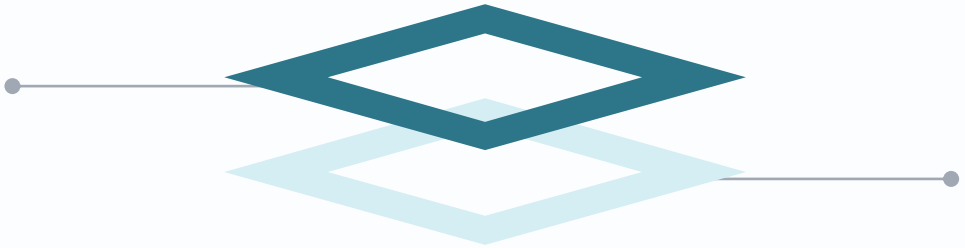


误区二：忽略依赖

只关注单一系统数据重要性，未通过业务影响分析（BIA）明确系统间依赖关系和数据优先级。

误区三：混淆分级与灾备

将数据分类直接对应灾备等级，未考虑成本与风险平衡原则，导致资源分配不合理。



误区四：静态管理

数据分级完成后长期不更新，未结合定期风险评估和业务变化动态调整分级结果。

数据分类分级建设思路

vinchin

数据资源梳理

1

- 结构化数据资产梳理
- 非结构数据资产梳理
- 资产相关信息和相关方识别
- 形成数据资产清单

数据分类分级

2

- 识别核心数据
- 识别重要数据
- 一般数据定级
- 个人信息定级

数据分级保护方案

3

- 明确架构和方案选型
- 数据分级安全策略制定
- 分级数据保护
- 满足合规要求

实施管理维护

4

- 灾难恢复演练
- 数据分级定期更新
- 优化灾备实施方案
- 灾备方案动态调整

不同级别系统灾备能力建议表

vinchin

根据企业业务系统的重要性、优先级、风险、性能需求等因素，将系统中的各类业务按层次或等级划分，以便进行更有效的管理和资源分配。通过这种分级管理，可以针对不同级别的数据提供差异化的保护措施，确保业务系统的高效运行和数据安全。

应用级别	判断标准	RTO	RPO
核心业务系统	这类业务是公司运营的核心，一旦停滞，会直接影响公司主要的收入来源或核心服务的正常运转。核心业务通常需要最高级别的可用性和灾备支持	≤30分钟	≈0
重要业务系统	这类业务对企业的运营至关重要，虽然可能不是直接影响收入，但它的停滞会严重影响公司运行效率和客户体验	≤24小时	≤12小时
一般业务系统	这类业务对公司运营的重要性较低，即使中断，影响也较小。对这些业务的可用性和性能要求相对较低。	≤48小时	≤24小时

vinchin

PART 03

数据分级保护方案

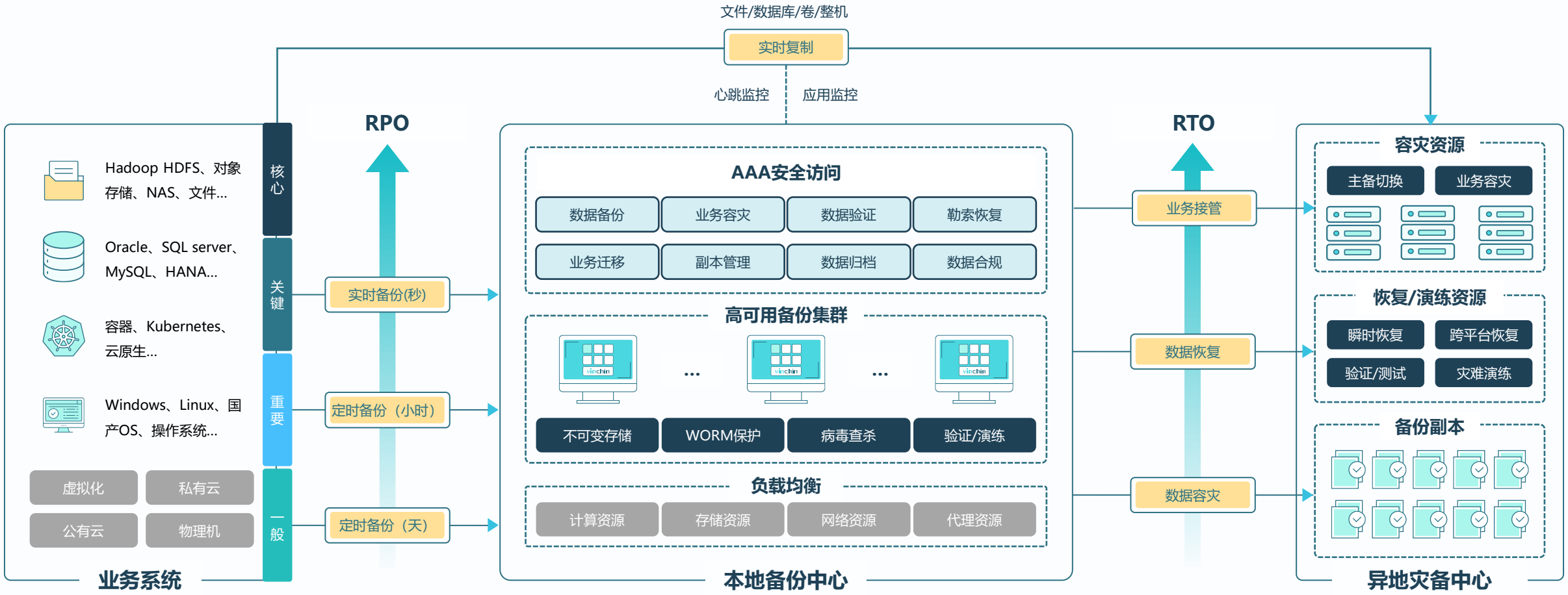
全域数据保护

vinchin

全面 | 安全 | 弹性 | 智能

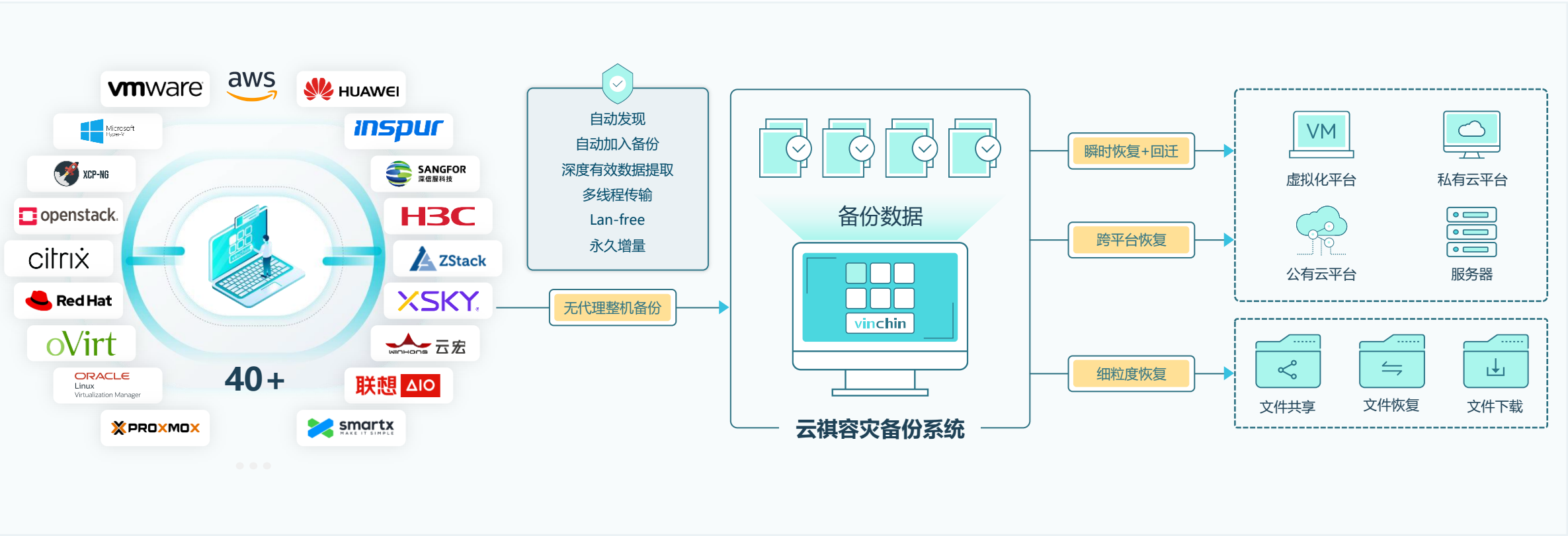
分级数据保护

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。



虚拟化/私有云/公有云平台备份

vinchin



智能无代理

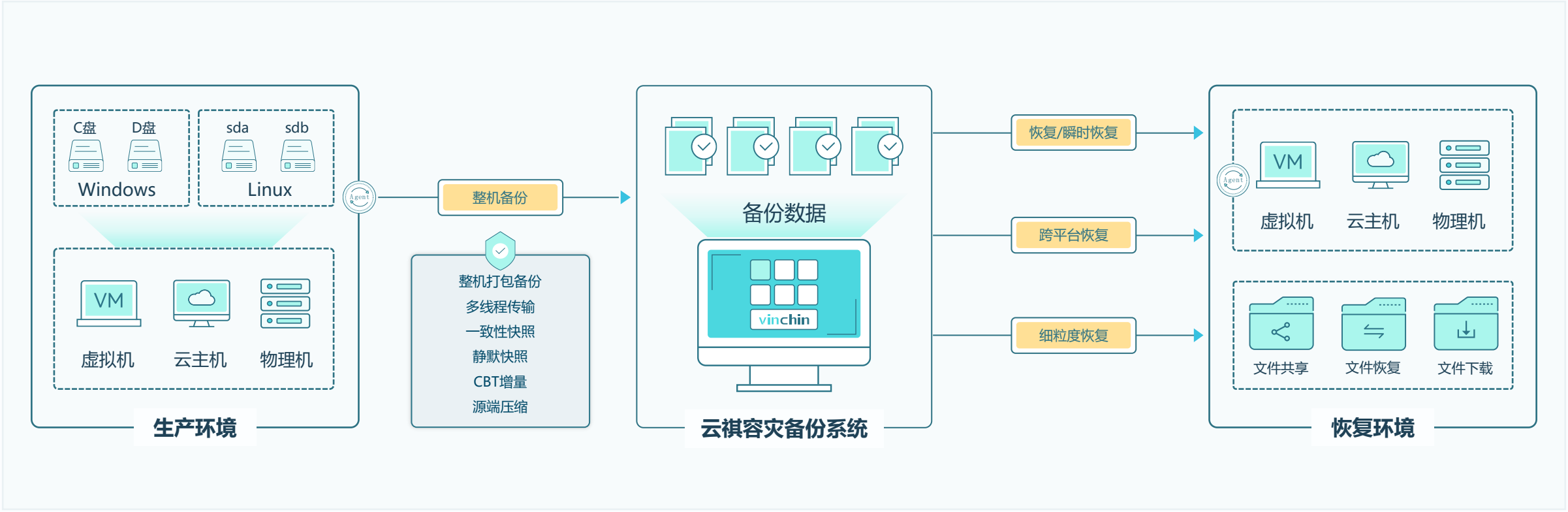
分钟级瞬时恢复

V2V跨平台恢复/迁移

高性能备份恢复

整机备份

vinchin



一致性快照

支持Windows/Linux国产系统整机备份，自研磁盘级一致性快照，保证系统与数据的一致性

源端CBT增量

自研源端CBT增量技术，可快速获取系统变化数据，减少需要传输的数据，显著提升增量备份效率

永久增量备份

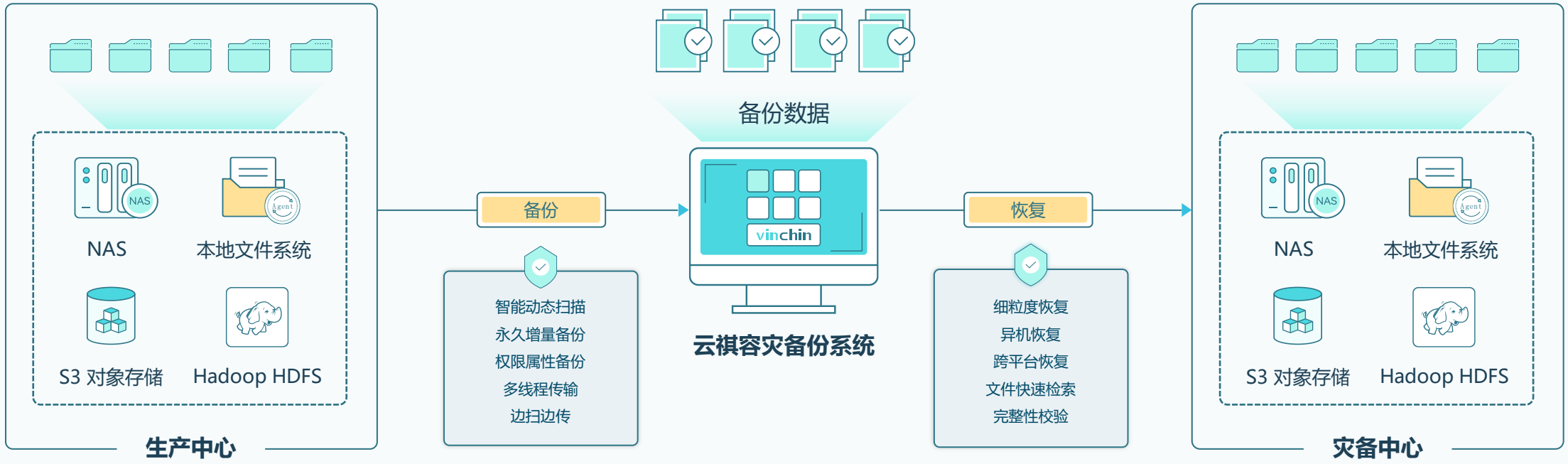
只需第一次完全备份，后续每次只做增量备份，提高备份效率，自动合并清理冗余数据，节省存储空间

跨平台异构迁移

支持跨平台迁移，可在迁移过程中自动转换数据格式、替换驱动、修复系统引导，保障迁移成功率

非结构化数据备份

vinchin



智能动态扫描

深广度自适应扫描引擎可根据生产环境目录结构智能调整扫描策略，实现海量文件的高速动态扫描

高速聚合，边扫边传

海量小文件自动合并传输，减少网络交互，大文件切片并发传输，无需等待全量扫描完成，边扫边传

智能文件过滤

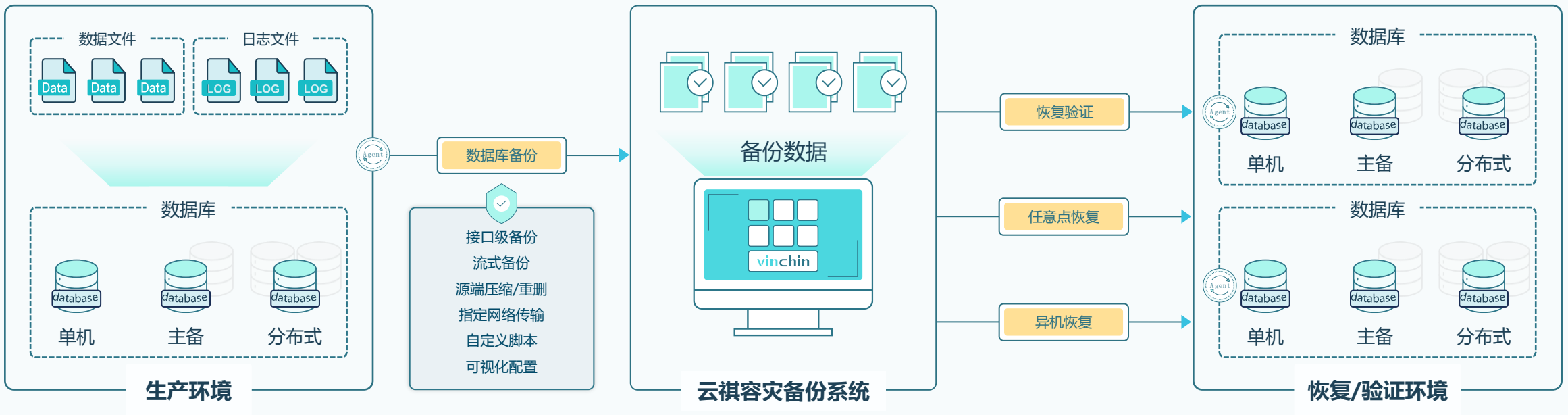
支持用户浏览文件目录选择文件/文件夹，也可使用通配符进行快速匹配或过滤，精准匹配备份内容

永久增量备份

只需第一次完全备份，后续每次只做增量备份，提高备份效率，自动合并清理冗余数据，节省存储空间

数据库流式备份

vinchin



接口级备份

对接Oracle/SQL Server/MySQL/达梦等国内外主流数据库原生备份接口/工具，确保数据库的一致性

流式备份

读取到数据后采用数据流直接传输到备份系统，无需在本地进行缓存，不占用生产环境存储空间

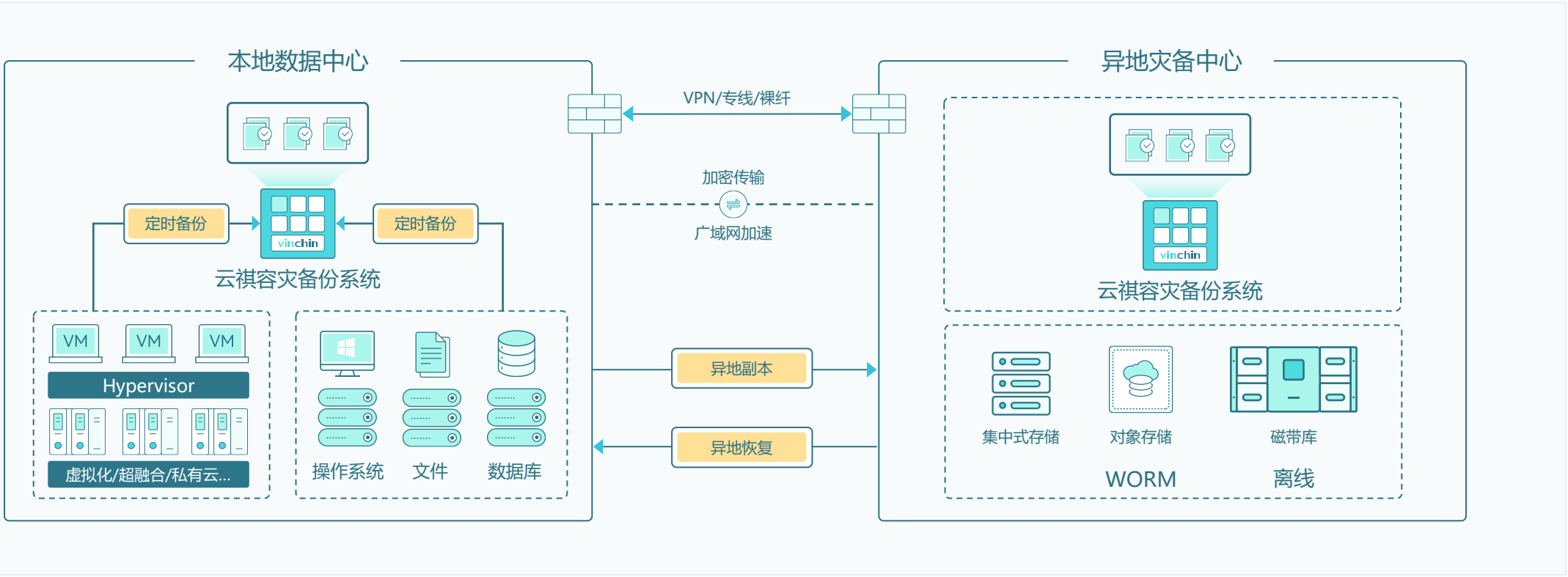
可视化配置

大部分数据库备份/恢复配置均支持在WEB界面点击鼠标进行引导式配置，降低用户使用门槛与运维压力

任意点恢复

支持对备份的数据库进行任意时间点的回退和恢复，灵活满足误操作、逻辑错误等场景的恢复需求

本地备份及异地副本容灾



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。

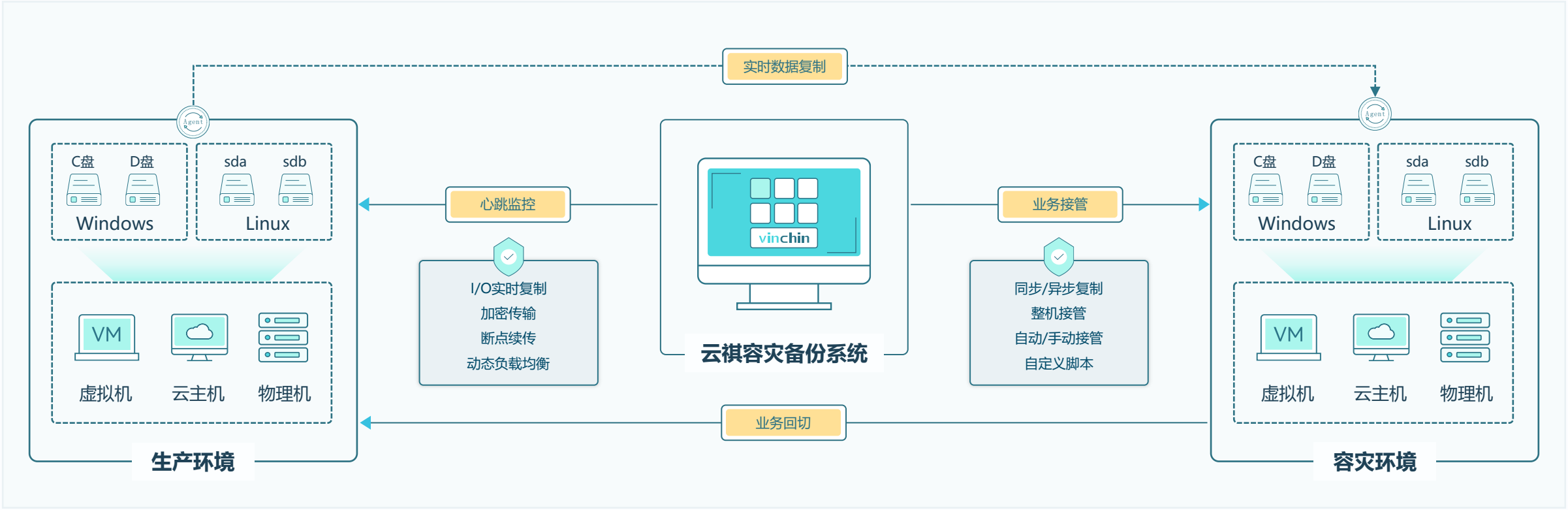
窄带宽异地传输

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。

整机复制与容灾



实时复制，RPO≈0

实时捕获生产系统的I/O，并将其1:1实时复制到容灾环境，可确保数据接近于0丢失，实现RPO≈0

断点续传

实时复制期间支持断点续传，防止网络波动、带宽高负载、主机重启等异常情况导致复制失败

整机容灾接管，RTO≈0

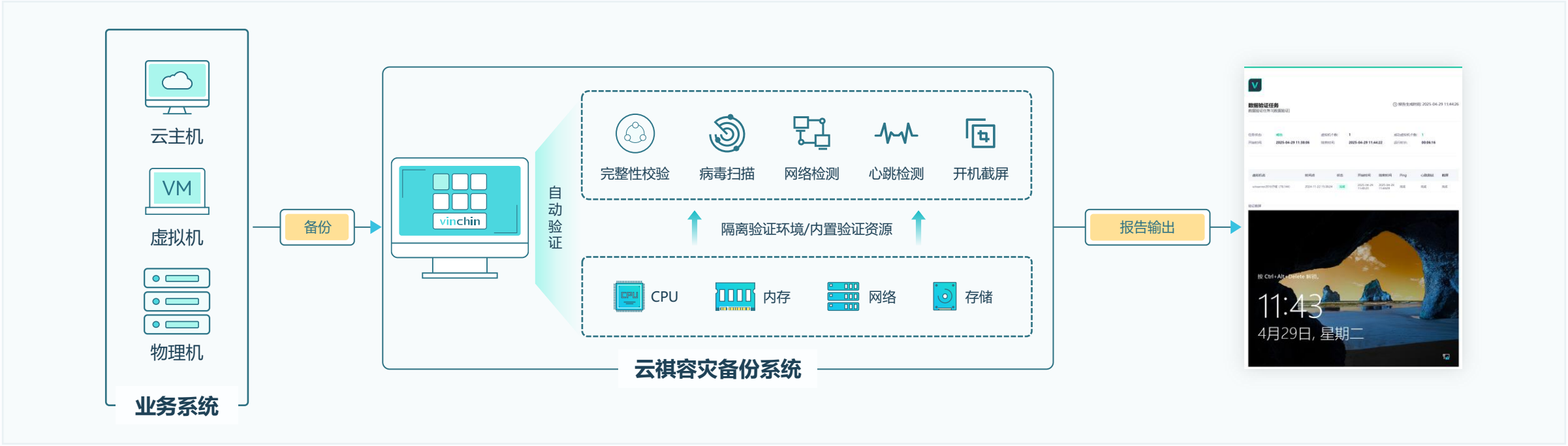
支持主备复制并自动识别数据库等应用，故障时可自动完成系统和应用等在内的整机接管

业务一键回切

容灾环境接管业务后，将持续保存临时数据直至发起回切操作，确保数据无缝回切至源环境

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。



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

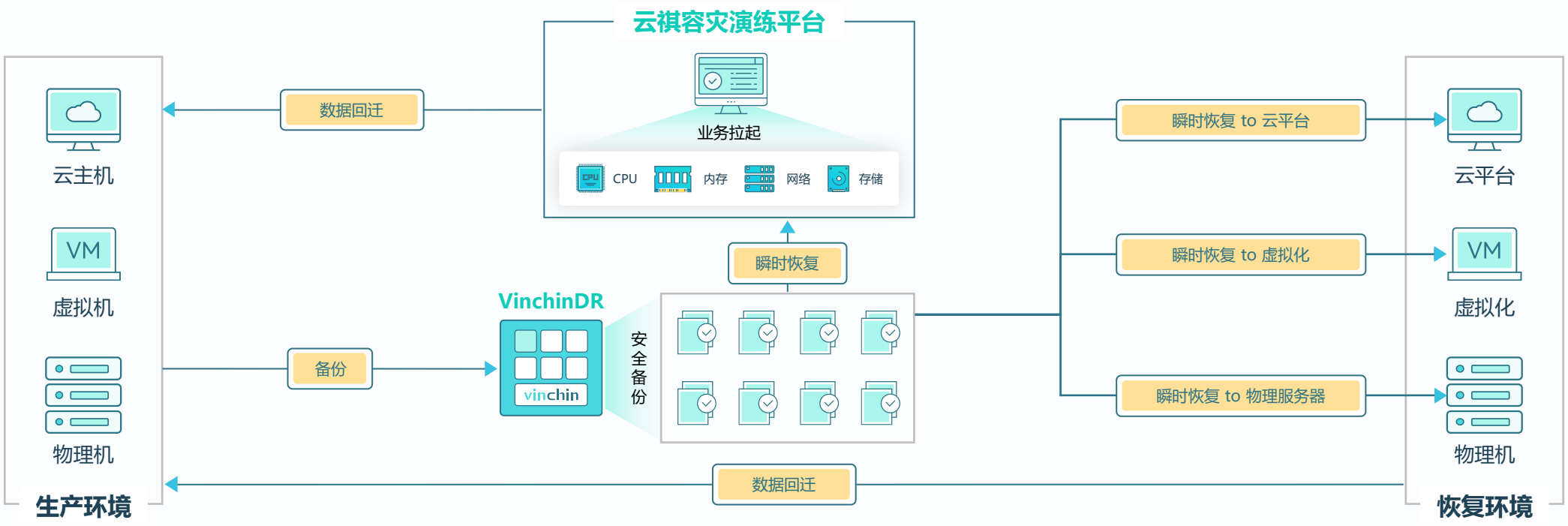
通过定期进行自动验证，确认备份数据状态，在异常时可及早接入采取对应措施

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

业务应急接管

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。



内置容灾资源

无需额外准备服务器/存储等资源，也无需临时搭建环境，可直接使用备份系统内置资源拉起容灾主机

业务应急容灾

生产主机故障时，支持从容灾演练平台将主机连带业务系统和数据一起拉起实现应急接管业务

分钟级RTO

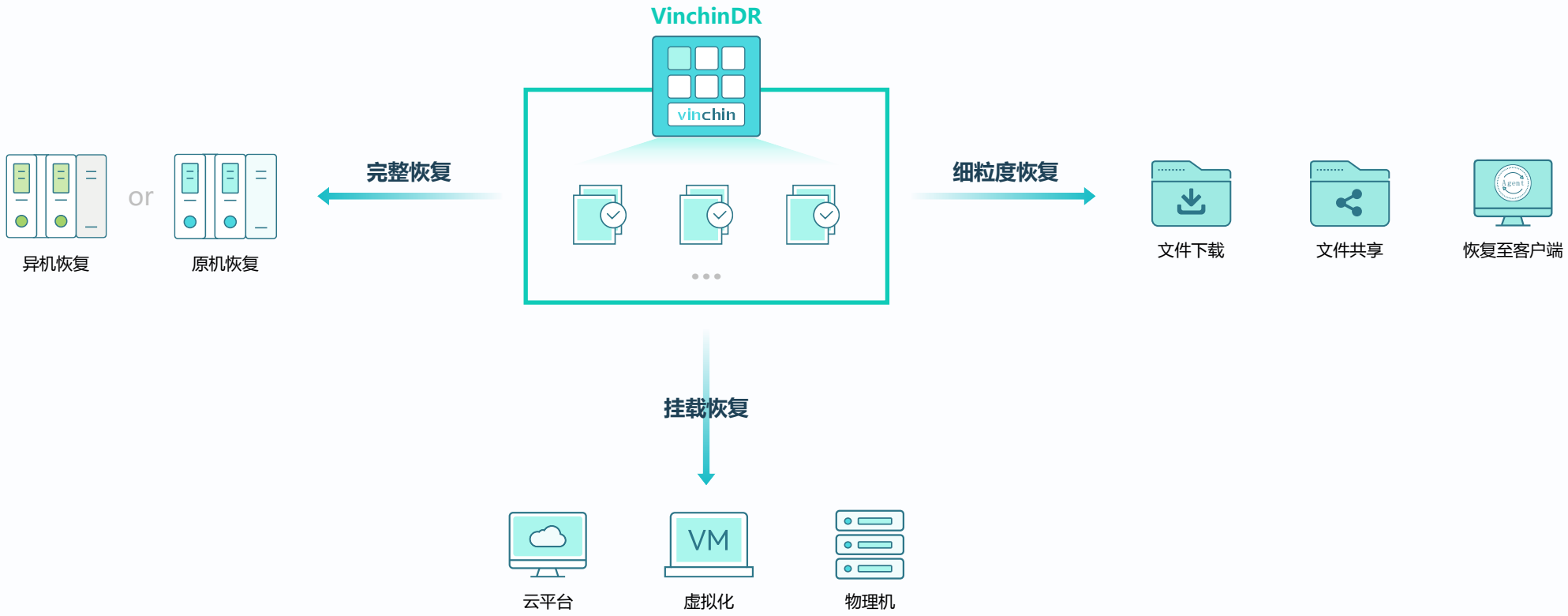
分钟级在容灾演练平台拉起一台主机应急接管业务，可继续对外提供服务，减少业务中断带来的损失

一键数据回迁

应急接管期间产生的数据将得到安全保存，当生产系统修复后，可将数据完整的无缝回切到源环境

灵活恢复选项，满足不同恢复需要

遭遇勒索攻击时，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。

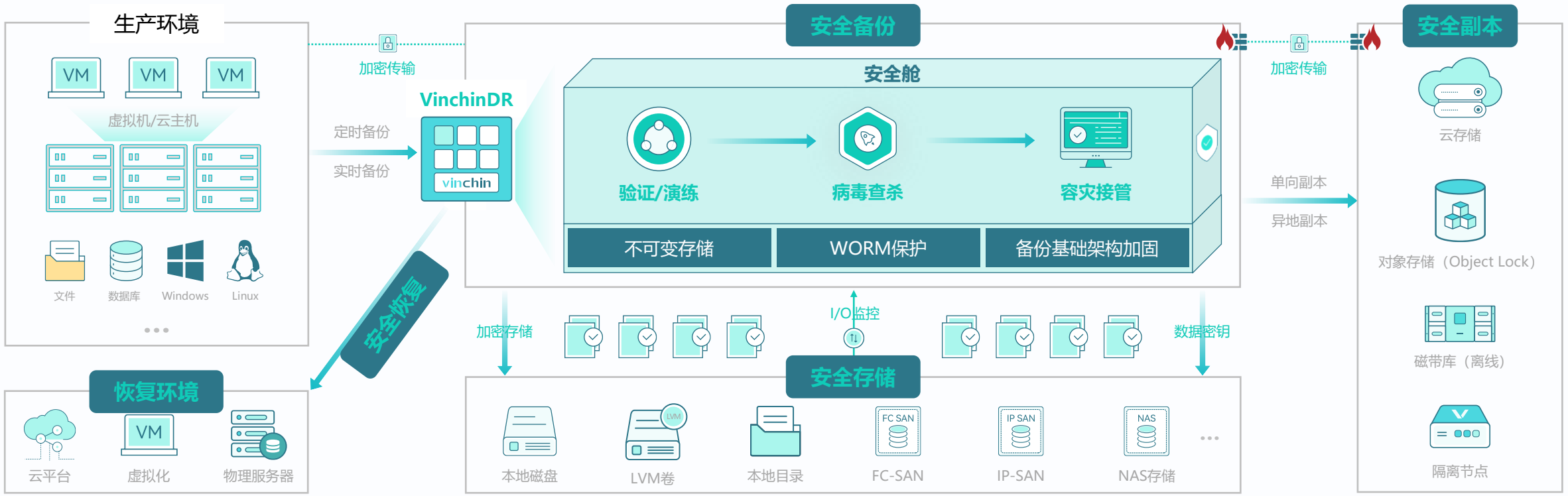


云祺安全备份体系

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



不可变备份 | **主动病毒查杀** | **自动验证/演练** | **安全弹性恢复**

3-2-1-1-0-0防勒索安全备份策略

vinchin

3

至少“生产+备份+副本”3个副本，降低单一副本损坏造成无法恢复的概率

2

数据至少存储在2种不同的存储介质上，避免单一存储损坏导致无法恢复

1

保证至少1个数据副本保存在异地，避免机房级数据灾难导致无法恢复数据

1

通过不可变存储、WORM、离线存储等技术加强安全性，防止备份数据被篡改

0

定期对备份数据进行自动验证，确认备份数据的可用性，保证在需要时可以正确恢复

0

依据零信任原则对备份系统实施多层安全加固，防止任何未授权访问与操作

vinchin

THANKS

云祺公众号

云祺视频号