vinchin

V6.0.5 灾备应用场景全解析

全域数据保护

vinchin

全面 | 安全 | 弹性 | 智能

vinchin

PART 01

异构数据迁移

兼容性强-满足不同环境迁移需求

vinchin

V2V无代理迁移

vinchin

无代理迁移

四大架构无代理对接，无需安装客户端，更少工作量、更少资源占用，更低兼容风险

异构智能转换

恢复时虚拟机数据、配置根据目标平台类型自动转换，任意平台都可恢复，并支持双向转换

自动替换修复

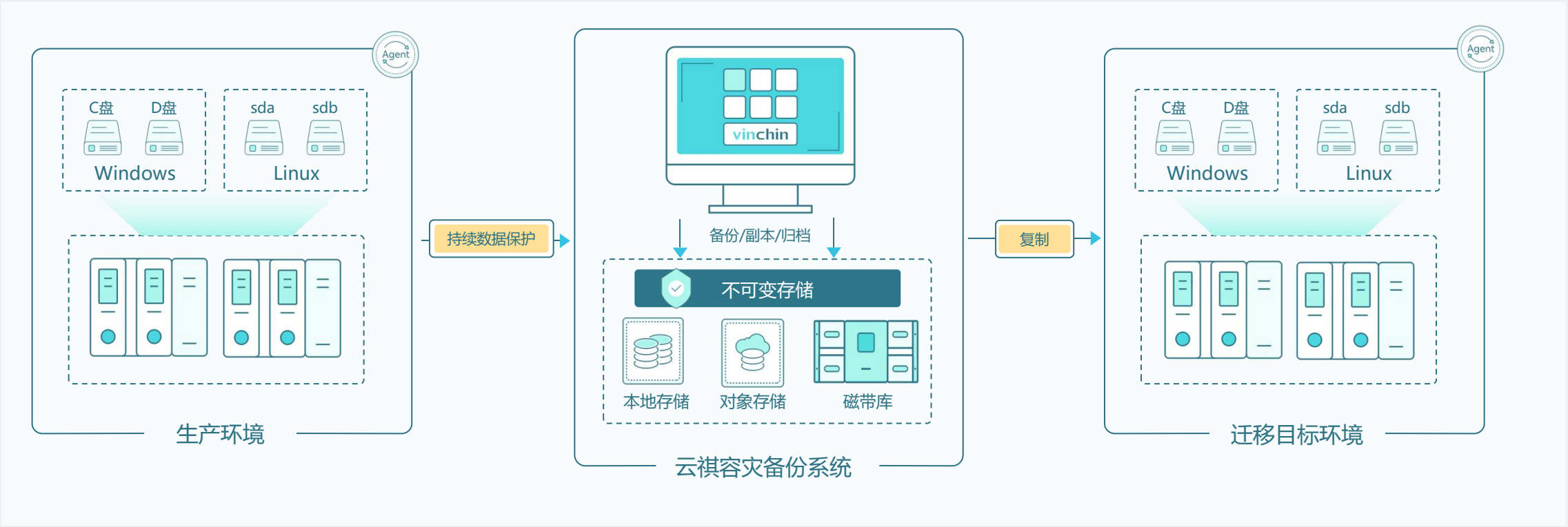
恢复过程中自动替换驱动、引导修复，整个过程无需手动干预，实现恢复即用

无缝跨云迁移

主流架构任意虚拟化/超融合/私有云/公有云无缝切换，满足国产化替代需求以及不被厂商绑定

整机在线实时迁移，减少业务中断时间

vinchin



一体化迁移

无需考虑应用兼容性，可直接对操作系统，应用及数据进行迁移，可迁移至物理机、虚拟机或云平台之上

数据实时迁移

减少迁移过程中生产主机的停机时间，减少对生产系统的影响。当同步完成后，所有变化均自动同步到新服务器

保障应用一致性

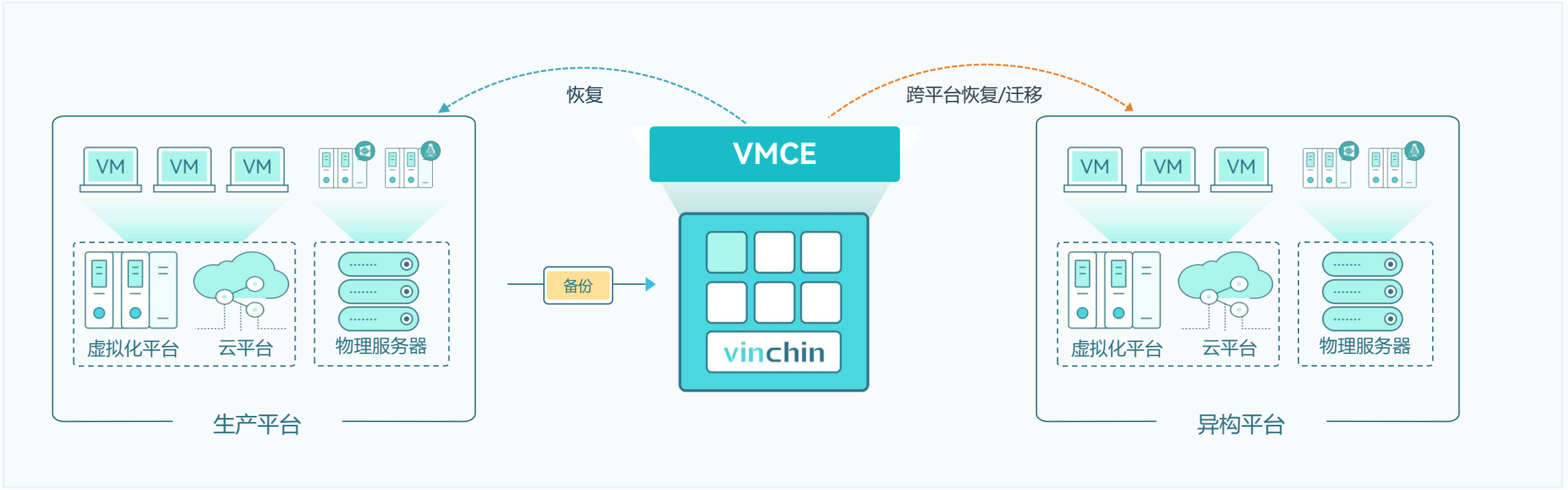
通过标签点策略，按一定时间间隔进行应用数据刷新操作，保证应用数据及时落盘，从而保障应用一致性

一键迁移

统一的WEB界面管理和监控整个的迁移过程，迁移的各个环节一目了然，界面简洁，方便用户快速掌握

整机异构迁移

vinchin



异构数据转换

恢复时主机数据、配置根据目标平台类型自动转换，任意平台都可恢复，并支持双向转换

自动引导修复

恢复过程中自动进行引导修复，如自动修复网络配置文件等，整个过程无需手动干预，实现恢复即用

驱动智能替换

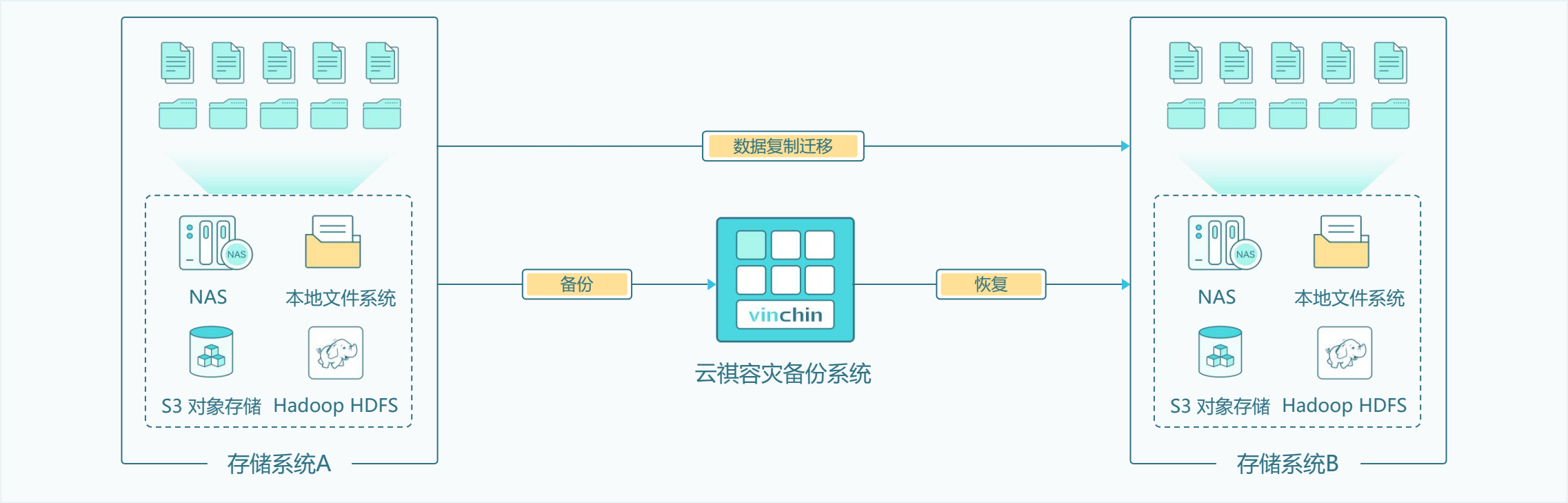
备份系统中包含专业的驱动库，涵盖大部分修复所需要的版本驱动，在恢复时会自动替换驱动，完成智能恢复

自动重建分区

恢复前可自动重建分区，减少用户手动分区操作，无需用户拥有较高专业能力

异构平台文件数据迁移

vinchin



异构平台广泛兼容

支持本地文件系统、NAS设备、对象存储、Hadoop HDFS、分布式存储互相跨平台恢复，满足不同存储平台之间的文件数据迁移需求

文件验证对比

对比源端和目标端的文件校验值，并提供对比差异结果，有效防止传输过程中的可能出现的数据丢失或损坏，确保迁移的高可靠性

细粒度迁移

可根据需求自主对文件进行排除或选定并提供基于时间点的筛选，同时可迁移基本读写权限至异构平台

方案价值

vinchin

减少业务中断时间

01

实时在线迁移方案，迁移过程中生产主机无需停机，对生产系统无任何影响。当同步完成后，所有变化均自动同步到新服务器

数据自由流动

03

X2X任意平台迁移，实现任意平台之前的数据自由流动，灵活应对各种业务场景，满足不同规模和复杂度的数据迁移需求，保障迁移过程的安全与高效。

降低迁移成本

02

利用现有备份资源，避免额外硬件投资，通过自动化工具减少人工干预，显著降低迁移成本，同时提高效率，缩短停机时间，快速实现业务上线。

简单高效

04

内置自动化脚本和图形化界面，简化配置与操作流程，降低技术门槛，使IT人员能够轻松完成复杂的迁移任务，减少错误发生，提升整体管理效率。

vinchin

PART 02

复制与容灾

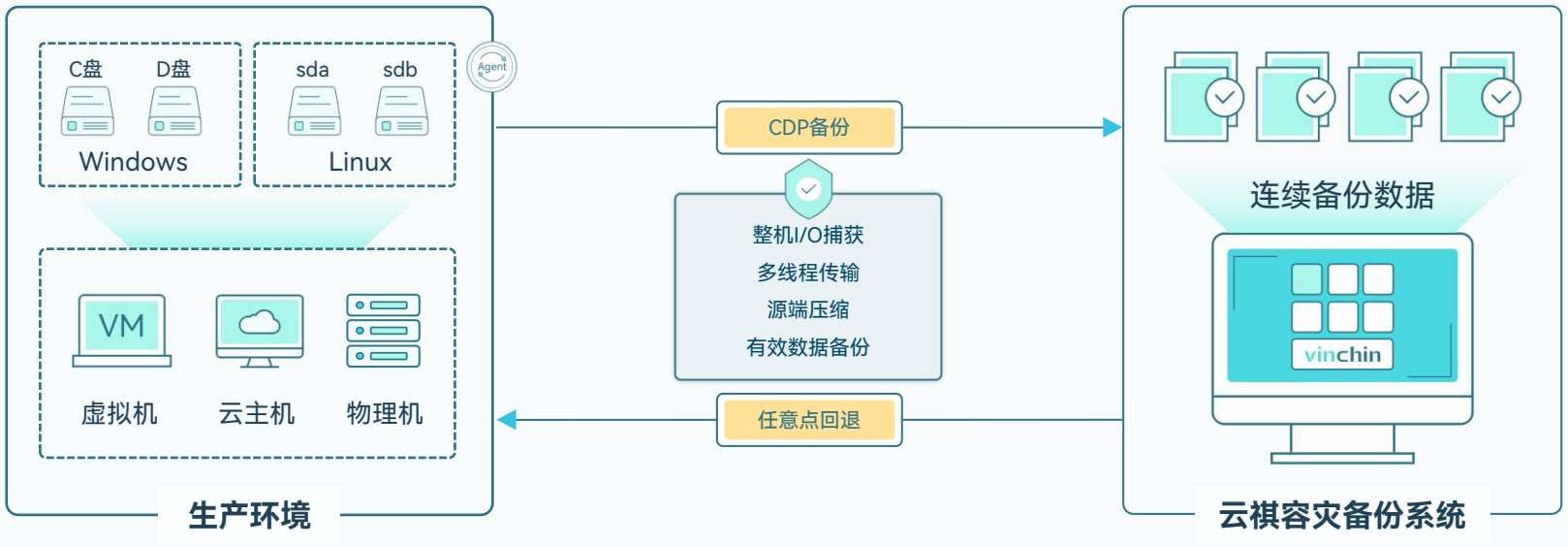
数据库主备实时复制

vinchin

在线日志解析 | 事务级实时复制 | 高效数据同步 | 主备读写分离 | 应急容灾接管

整机实时备份（CDP）

vinchin



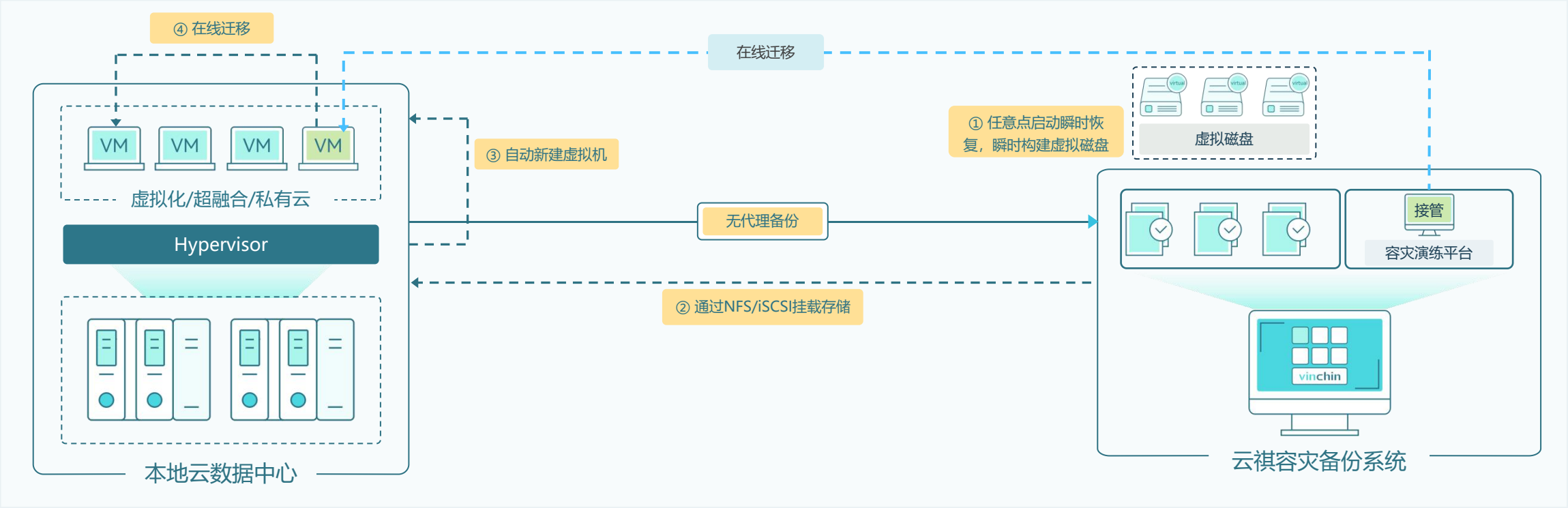
国产系统兼容

I/O实时捕获，RPO≈0

断点续传

动态负载均衡

应急接管，保障业务连续性



快速恢复业务

无关数据大小，秒级恢复虚拟机至原平台，分钟级快速恢复业务运行，恢复后自动开机，立即可用

跨平台容灾

任意云平台、备份系统内嵌平台无缝瞬时恢复，可实现分钟级跨平台业务拉起，有效减少平台级故障带来的损失

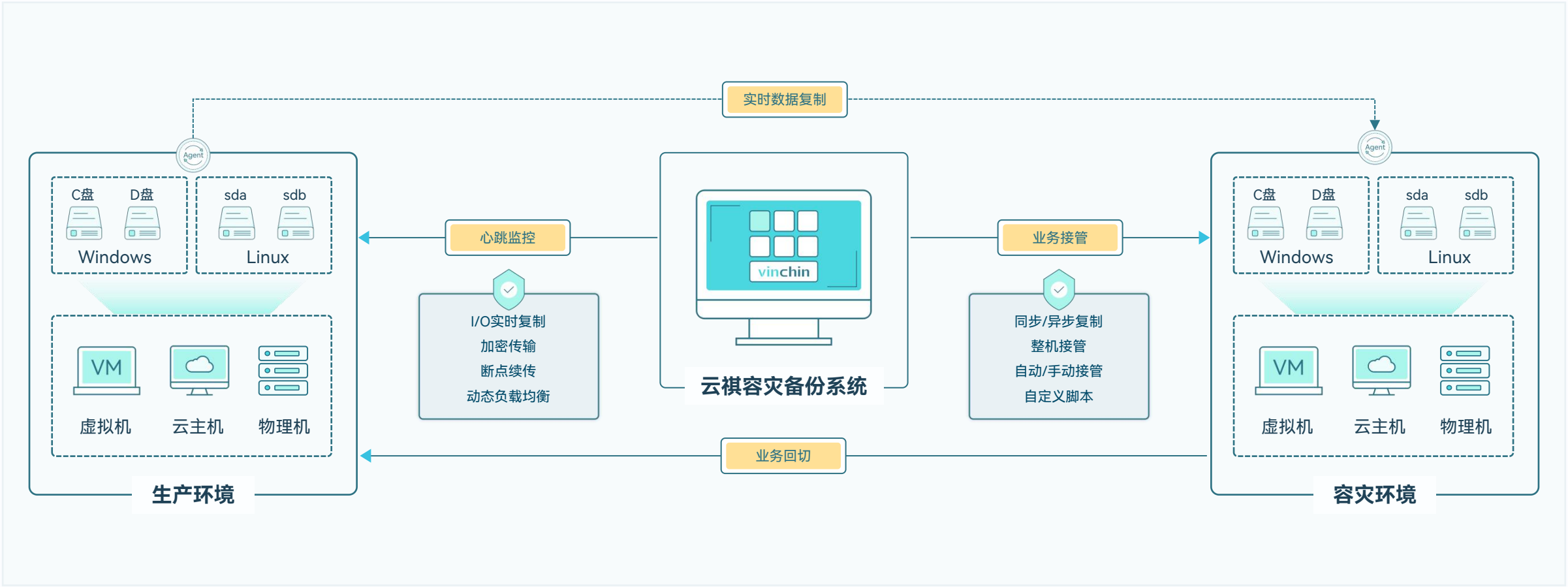
无缝数据回迁

支持无缝回迁瞬时恢复的虚拟机，同时回迁缓存数据，确保业务连续性、数据完整性

快速验证

借助瞬时恢复批量完成虚拟机恢复验证，确保备份数据安全可靠，增强应急恢复保障

整机复制与容灾



实时同步，RPO≈0

应用一致性保障

整机容灾接管，RTO≈0

业务一键回切

海量非结构化数据复制

vinchin

高效数据复制

异构跨平台复制

一致性保障

vinchin

PART 03

防勒索场景

什么是勒索病毒?

vinchin

全球数字化革命正在以迅猛的速度重塑经济发展与生产生活方式，随着数字化转型成本持续降低，数字化不再是一种奢侈品，而是企业保持竞争力和提升行业创新的必要条件，随着越来越多的数字化业务系统上线，数据安全威胁形式也越发严峻。

> 勒索病毒是一种特殊的恶意软件，它会攻击受害者的系统和数据，使其保持锁定或加密状态，并要求受害者向攻击者支付赎金，以此获取高利润。

> 勒索攻击给受害者带来的影响是多方面的，除了需要支付高额赎金外，业务中断、声誉受损等问题也会接踵而至，更严重的是，违反数据安全法规可能导致严重的法律后果。

勒索病毒全球肆虐

46%

2024年，勒索攻击受害者数量再度陡增，约较上一年增长46%

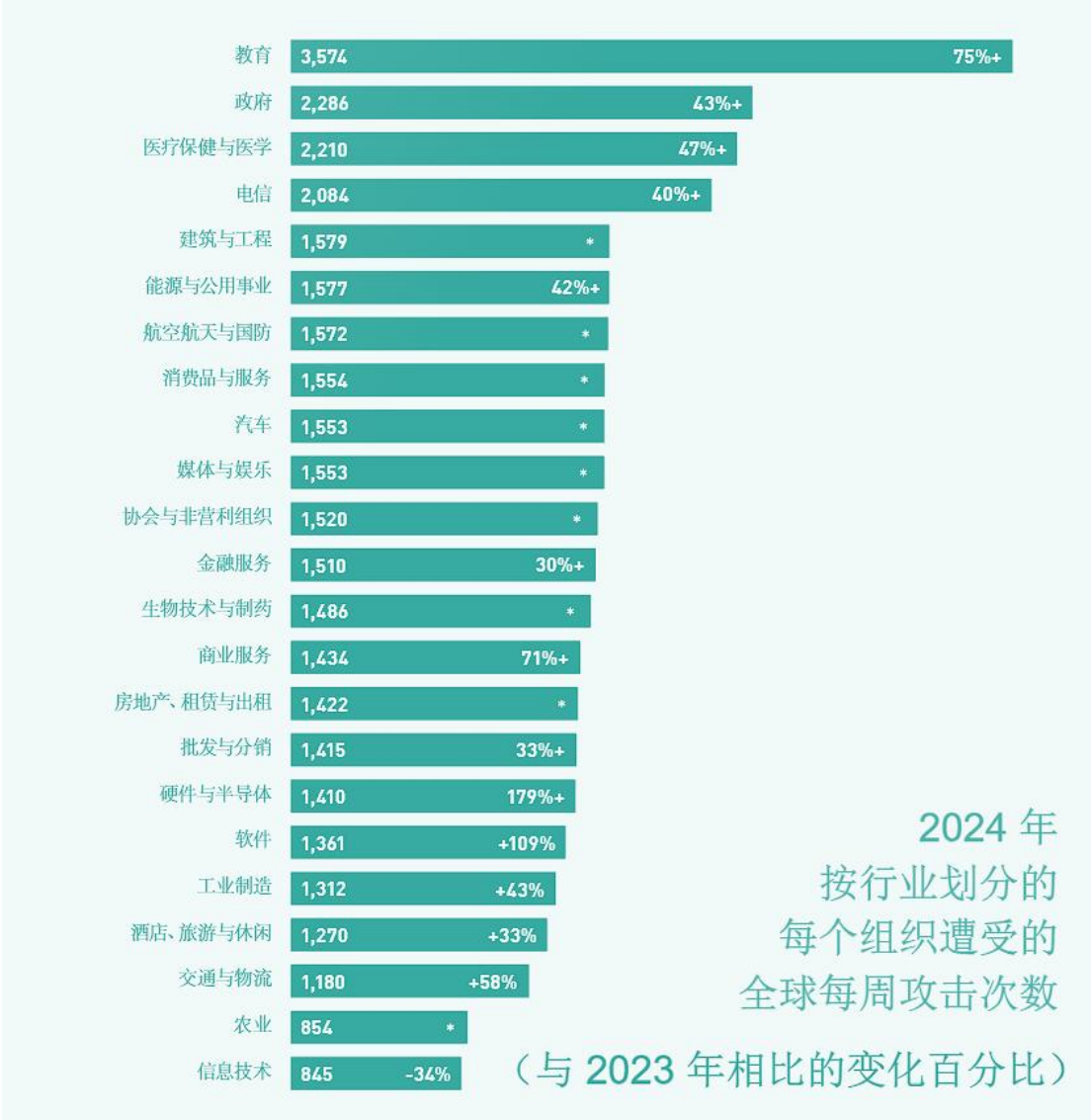
2024勒索攻击目标行业TOP 10

商业服务	零售	制造	建筑	金融
1302	820	573	287	257

医疗健康	教育	政府	科技	交通
248	204	191	174	163

来源：Check Point-2025网络安全报告

各行业勒索态势严峻



数据源：Check Point-2025网络安全报告

教育行业

高校的网络环境规模庞大且复杂，传统的网络安全建设难以有效抵御勒索。此外高校还面临的学生、教师等群体安全意识和信息安全技能水平参差不齐，流程与制度不够完善等问题。勒索病毒对高校保有的大量高价值科研数据带来威胁，并且高校也是黑客窃取个人信息的重点对象，勒索将导致大量个人信息泄露。

医疗行业

医疗行业的业务系统众多且相对独立，因此各类系统的安全防护非常依赖供应商，而供应商的安全能力通常较弱，无法及时修复漏洞。由于医疗业务系统与患者生命安全高度关联，对中断几乎是零容忍，并且医疗业务系统包含患者就诊记录、病例、个人隐私等敏感数据，业务中断、数据泄露带来的后果十分严重。

制造业

制造业通常因预算有限、缺乏安全人员与技能等原因导致安全防护薄弱，而汽车、半导体等高端制造业的生产已经高度自动化，并且由于制造业上下游呈链条式关联，即使只是其中一个供应商、一条生产线遭受勒索攻击，生产中断导致的交货能力断档将在整个行业引发广泛的连锁反应，造成重大经济损失。

零售业

零售业日常处理超大规模的交易，处理大量资金，并掌握着数百万甚至上亿顾客的银行卡、身份隐私信息。黑客往往选择在节日、大型促销期前对其老旧系统的发起攻击，使商家不仅面临数据安全风险与赎金支付成本，更会因为业务中断导致巨额的销售收入损失，这对高度依赖现金流的零售商可能造成毁灭性灾难。

金融行业

金融业有严格的法规和监管要求，因此其安全防护水平通常高于其他行业。但由于数字化程度高、资产价值高、数据高度敏感等特性，导致其成为勒索主要攻击目标。遭遇勒索攻击后，为保护敏感数据并维护声誉，其更有可能被迫支付巨额赎金。并且金融机构间关联密切，勒索可能导致整个金融体系出现连锁反应。

关键公共事业

随着地缘政治局势逐步升级，近年来能源、电信、水务等关键领域公用事业成为勒索团伙竞相瞄准的主要攻击对象。不法分子企图通过采取更为激进、更具破坏性的攻击手段制造大规模破坏来索取高额赎金。勒索攻击不仅会导致公共服务中断，更会引发公众对能源安全甚至国家安全的信任，造成严重的社会影响。

近年部分典型勒索事件

vinchin

时间	行业	受害单位	影响与损失
2023年2月	制造	美国应用材料公司（Applied Materials）	因供应商受攻击导致下季度出货受到影响，预计2.5亿美元损失
2023年11月	IT	印度Infosys 美国子公司	650万人数据泄露，引发多起诉讼，赔偿1750万美元
2024年2月	医疗	美国Change Healthcare公司	美国史上最大医疗数据泄露事件，累计损失约24.5亿美元，母公司被美国国会公开质询
2024年8月	制造	美国Keytronic公司（PCBA巨头）	美国和墨西哥站点运营暂停两周，预估当年Q4收入损失约1500万美元
2024年10月	制造	日本卡西欧计算机株式会社	系统瘫痪且恢复无进展，极大影响公司运营，交付严重延迟，财报推迟一周发布
2024年11月	制造	美国军工半导体厂商微芯科技（Microchip）	因勒索事件导致额外支出2140万美元
2024年11月	金融	美国LoanDepot 贷款公司	1600万人的个人信息泄露，累计损失约2690万美元
2024年12月	零售	宜家代理商Fourlis集团	黑五促销期间门店补货受影响，电商运营受影响近3个月，造成约2000万欧元的损失
2025年1月	制药	美国恩佐生化	约250万人次的诊断测试信息和个人数据遭到泄露，赔偿450万美元
2025年2月	关基	英国南方水务公司	勒索损失超4000万（450万英镑）
2025年3月	制造	印度塔塔科技（Tata Technologies）	高达 1.4TB 的数据泄露，涉及超过 73 万份文件
2025年4月	制造	美国森萨塔科技（Sensata Technologies）	部分设备遭到加密，致使业务运营中断
2025年4月	医疗	美国达维塔（DaVita）公司	部分网络系统被加密，有业务运营受影响中断服务

来源：网络公开勒索安全事件信息整理

勒索病毒为何猖獗

vinchin

高额利润

2024年勒索组织累计勒索60亿人民币，利润使其不断发起攻击

匿名支付

匿名支付掩盖了交易者信息，使得执法部门难以进行打击

RaaS

暗网上一个勒索工具包只需要50美元，任何人都可以发起攻击

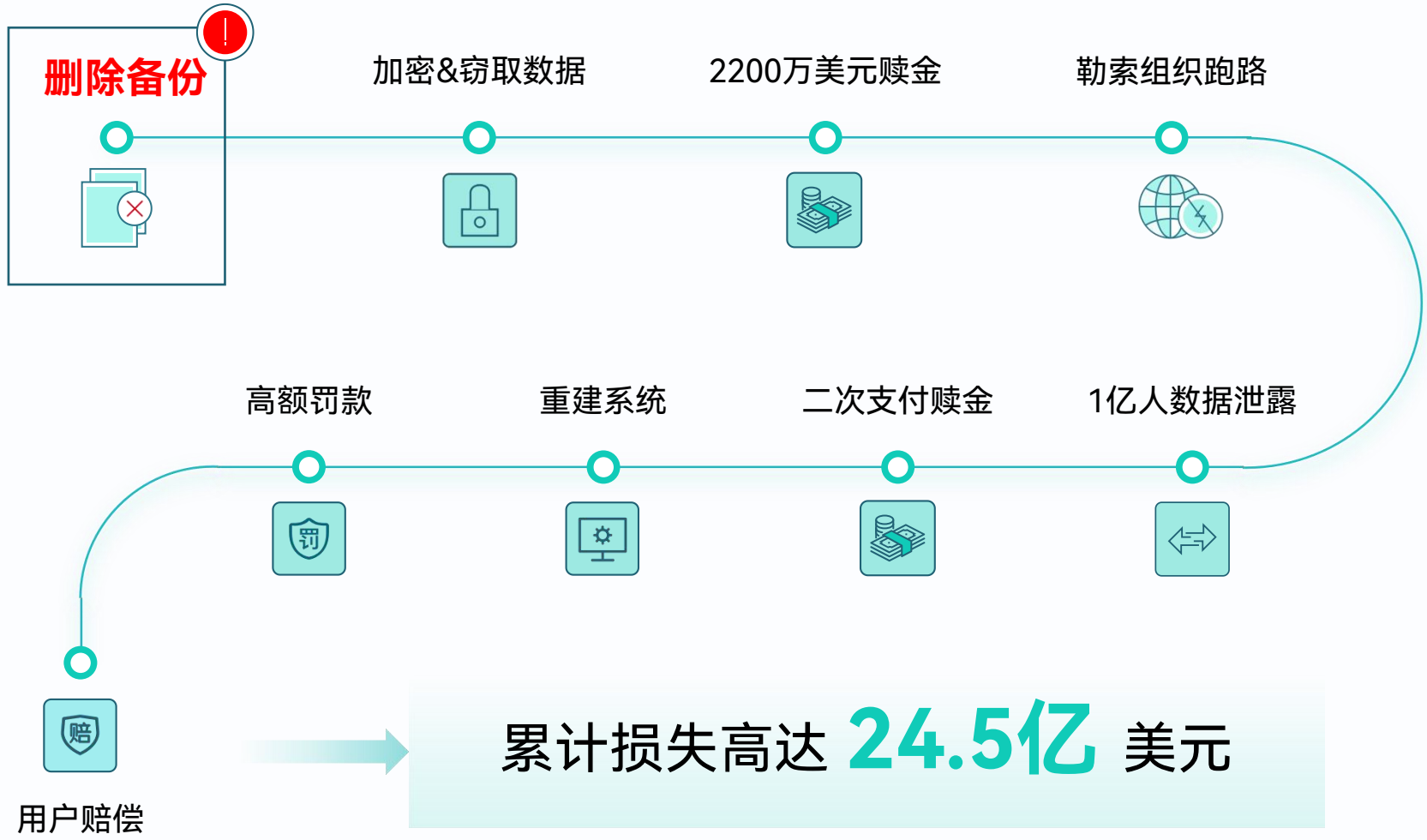
AI驱动

AI技术显著增强了勒索的攻击力，深度伪造使攻击防不胜防

“备份”被攻破案例

该公司是某国最大的医疗技术服务提供商，为全国各地的医院、药房、个人诊所等医疗机构提供医疗支付服务，处理众多医疗账单和保险，每年约处理150亿次交易，因此持有大量敏感的患者数据。2024年2月21日，其被Blackcat攻击，导致遍布全国的药店及医疗机构无法开具处方，更无法进行保险结算。

某企业勒索实录



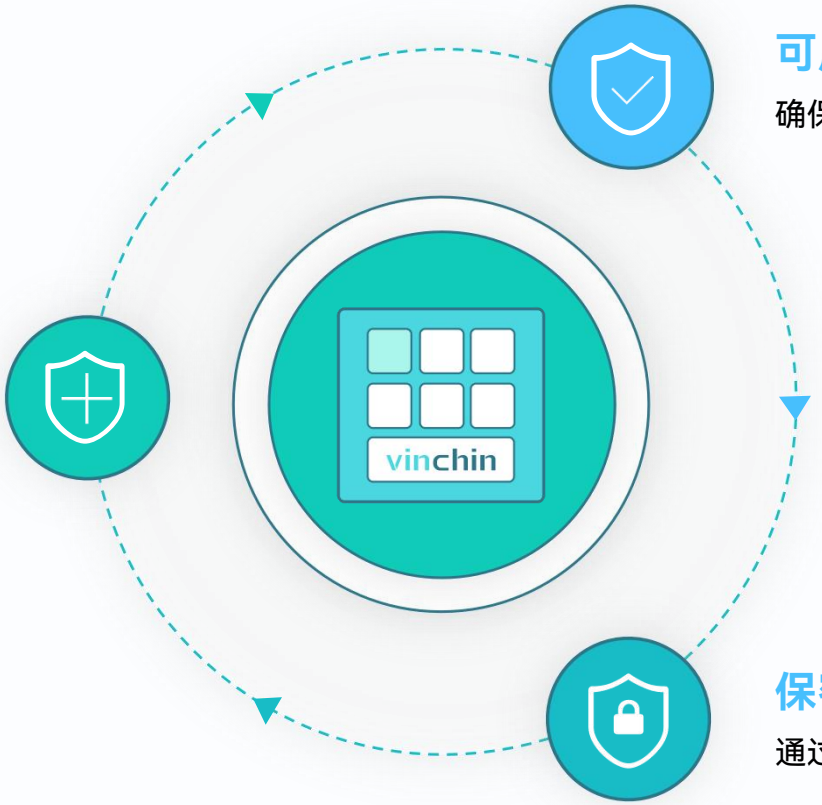
来源：网络公开勒索安全事件信息整理

vinchin

安全备份才是数据安全的最后一道防线

安全备份要做什么？

vinchin



可用性

确保数据正常恢复可用

安全性

体系化安全防护，防止数据被破坏

保密性

通过加密等措施防止敏感信息泄露

云祺防勒索最佳实践

vinchin

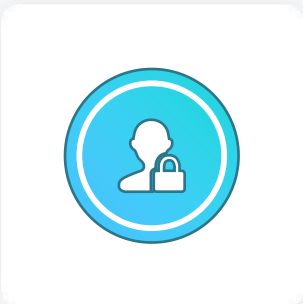
践行3-2-1-1-0-0安全备份策略

多层加固的备份系统以增强备份体系韧性

全流程端到端加密，防止敏感数据泄露

利用WORM等特性保持备份数据的不可变性

主动查杀恶意软件以确保备份的安全性

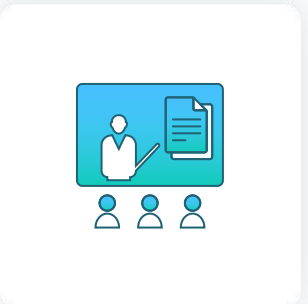


构建零信任体系，确保访问安全

定期验证和演练，以持续改进恢复流程

实时监控任务和数据状态，以便及时响应

针对不同业务/数据灾难场景构建弹性恢复措施



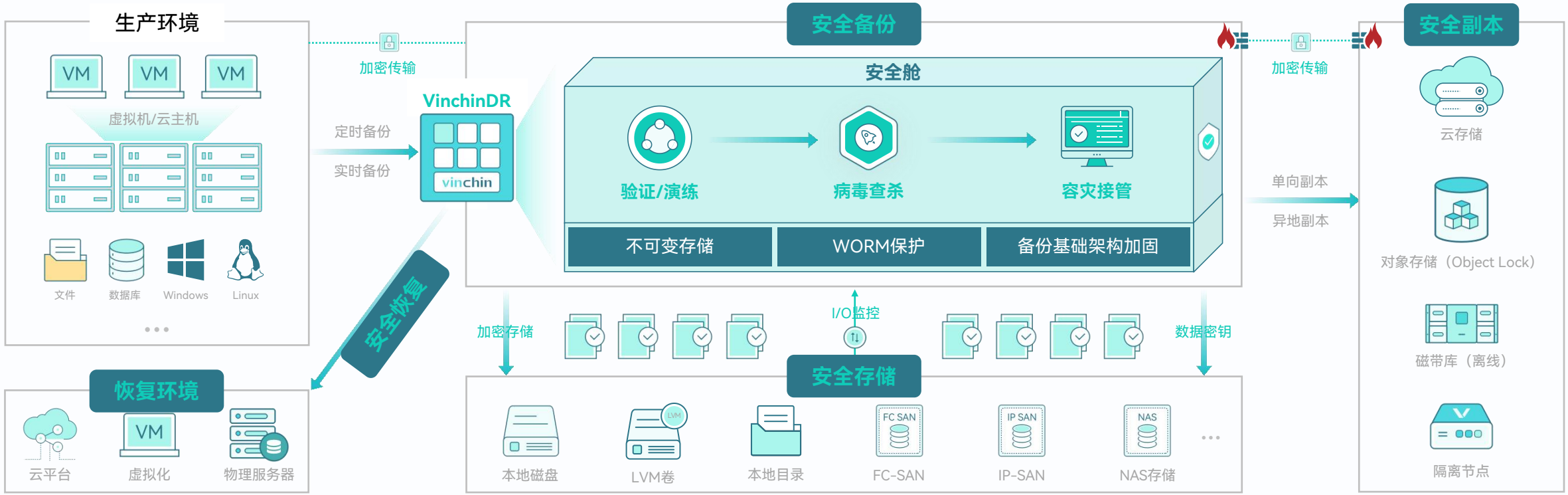
建立完善的灾难恢复管理制度并实施员工培训

云祺防勒索体系

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

安全弹性恢复

3-2-1-1-0-0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

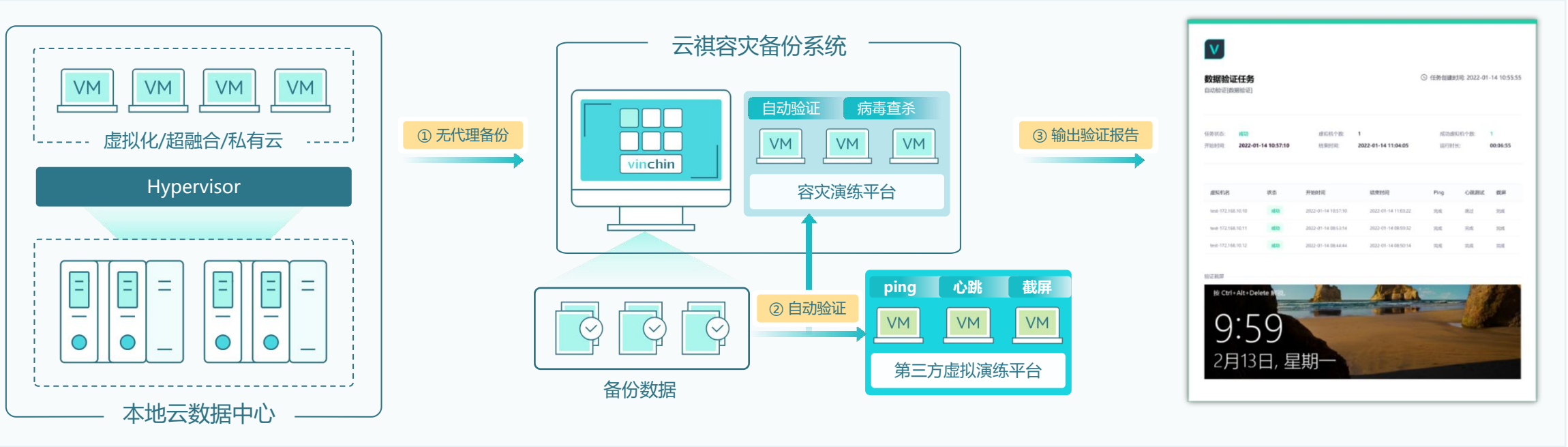
vinchin

PART 04

验证与演练

自动验证备份数据，确保数据完整可靠

vinchin



内置容灾演练平台

可基于云祺内置的容灾演练平台进行数据验证，无需准备验证环境，减少用户验证成本

隔离环境病毒查杀

验证环境与生产环境完全隔离，验证过程中不会与生产业务系统产生冲突，影响生产业务的正常运行

批量自动验证

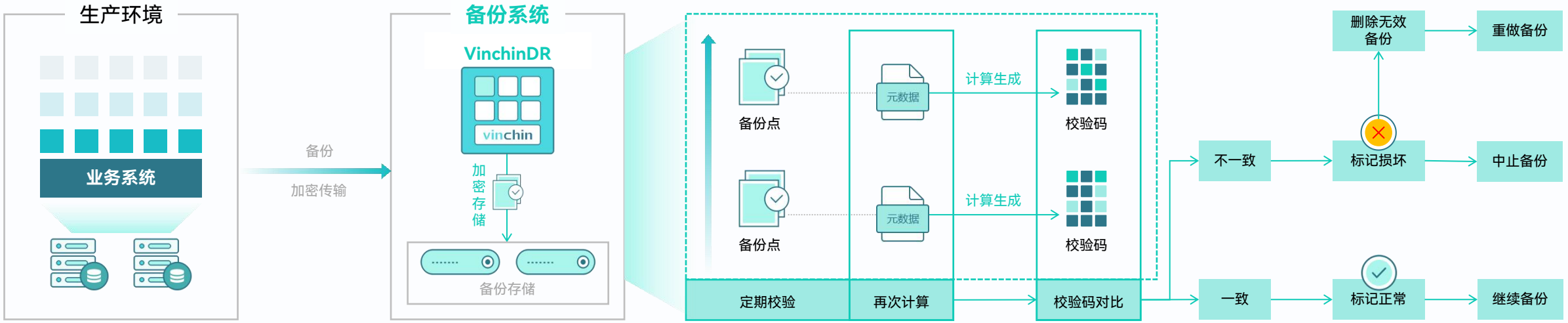
验证流程简单，除手动验证外，更支持定期、批量、自动验证最新备份点的可恢复性

可视化验证报告

自动生成验证报告，验证结果可视可见，便于决策分析，报告可发送到指定邮箱，支持自定义报告模板

数据完整性校验，尽早发现数据问题

为减少存储损坏、异常操作等不可控因素给数据恢复带来的影响，以及避免某个备份点损坏造成后续备份都成为无效数据的风险，可通过定期进行完整性校验来检查备份数据是否受到非预期的改动，以便尽早发现可能出现的数据问题并采取补救措施。



自动校验

可按每周/每天/每次等频率定期自动进行数据完整性校验，及时掌握备份数据状态

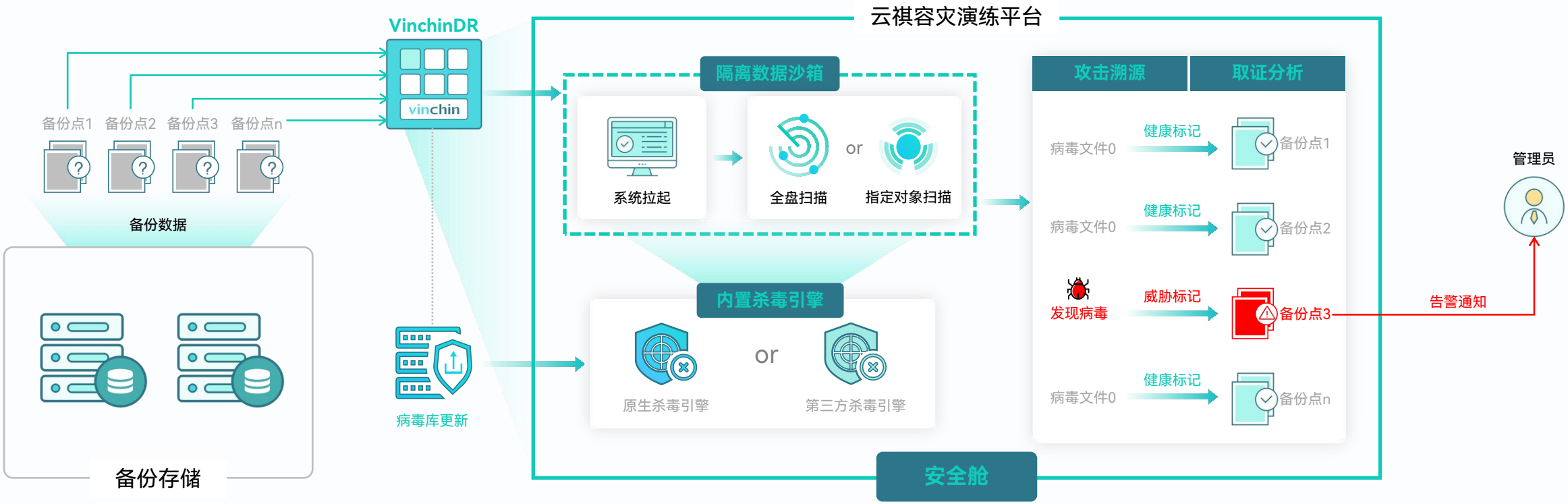
高效校验

无需校验整个备份链的所有数据，仅校验对比元数据，几乎无性能消耗，海量备份数据场景校验更高效

修正备份

校验发现异常时将发出告警，并标记异常备份点。支持清除无效备份点，以及自动重新备份来修正备份链

主动查杀病毒



自动查杀病毒

自动对备份数据进行病毒查杀，识别并标记安全的备份点，无需人工干预

内置杀毒引擎

系统集成杀毒引擎，开箱即用，无需准备杀毒环境以及向外部挂载数据，安全可靠

隔离数据沙箱

在云祺容灾演练平台中使用完全隔离的环境进行病毒查杀，不必担心病毒外泄

查找安全备份

在备份数据中查找干净可用的备份点，为将来的安全恢复做好准备

溯源与取证

用户可以随时将任何备份点在隔离环境中拉起，进行溯源与取证分析

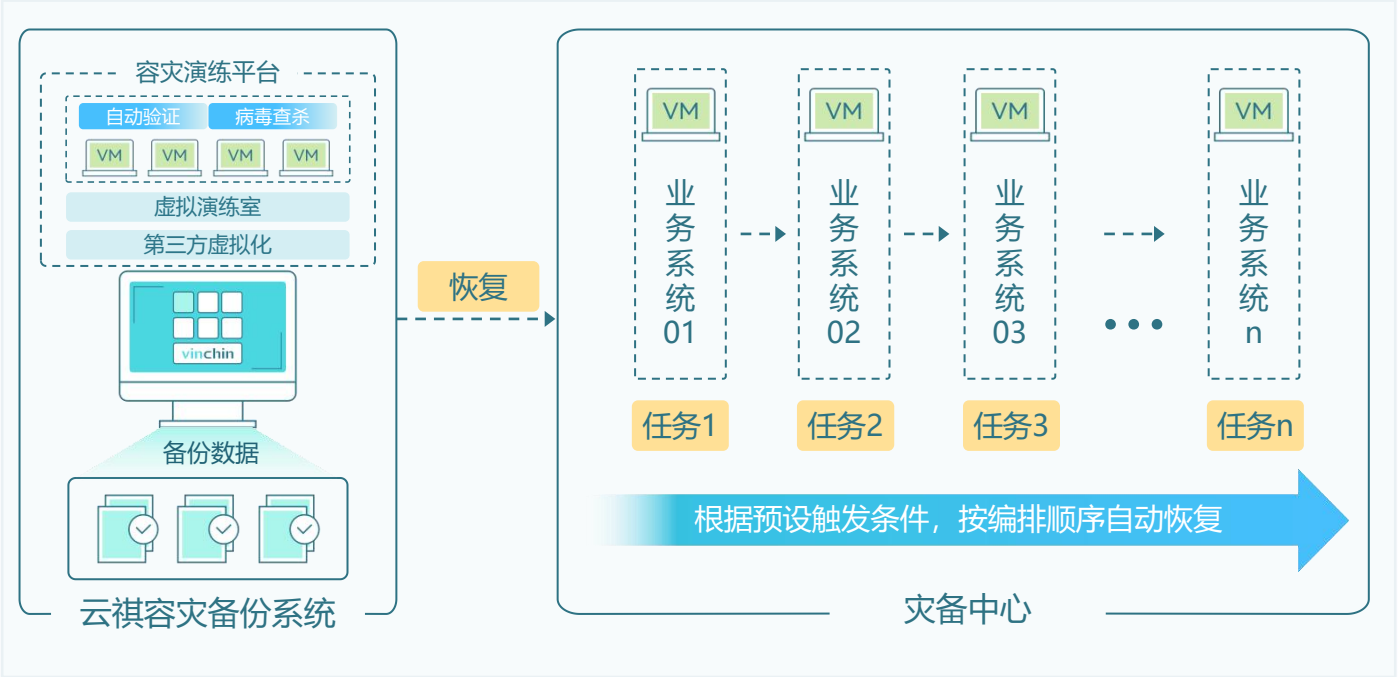
灾难演练

vinchin

场景描述

验证容灾计划的有效性，提高应急容灾能力：通过演练验证容灾策略和应急响应方案的有效性，验证数据正确性，确保在真实灾难发生时能够迅速恢复业务运行，提高应对突发事件的能力和效率。

优化容灾计划：容灾演练过程中，可能会暴露一些潜在问题和不足，如备份数据不完整、恢复时间过长等，这些问题可以帮助企业或组织优化容灾计划，提高灾难恢复的成功率和效率。



核心优势

任务编排自动化运行：通过提前自定义编排任务顺序及对应任务的触发条件，使得所有备份、恢复、验证任务根据触发条件自动化运行，确保在出现问题时能够及时响应，自动启动灾难恢复流程，有序恢复相关业务系统，保障业务连续性。

隔离环境数据验证：验证过程全程与生产环境隔离，不影响生产业务的正常运行，隔离环境不仅能够提高数据安全性，减少攻击面，同时能够简化运维和管理工作量。

病毒查杀：自动查杀备份数据的病毒，确保备份数据的安全性及可用性，保障恢复数据的安全。

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。

vinchin

PART 05

多云&混合云保护场景

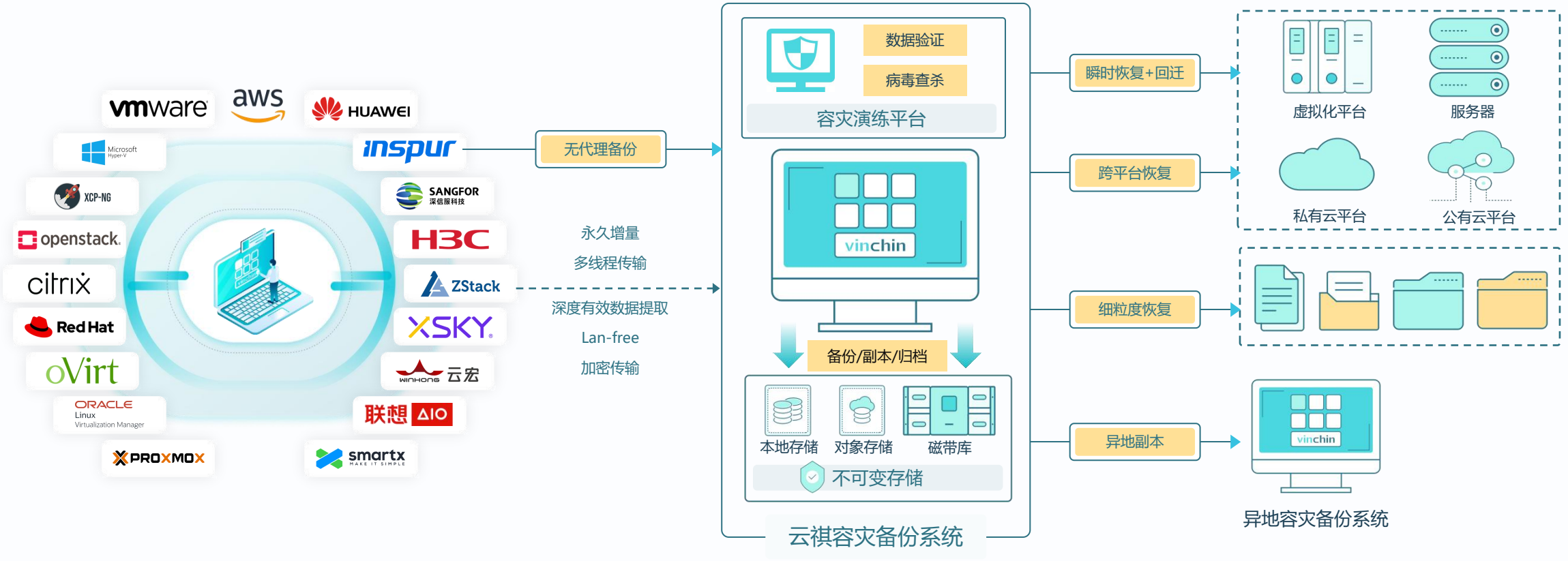
云环境保护整体方案

vinchin

无代理备份恢复

瞬时恢复数据回迁

跨平台恢复V2V



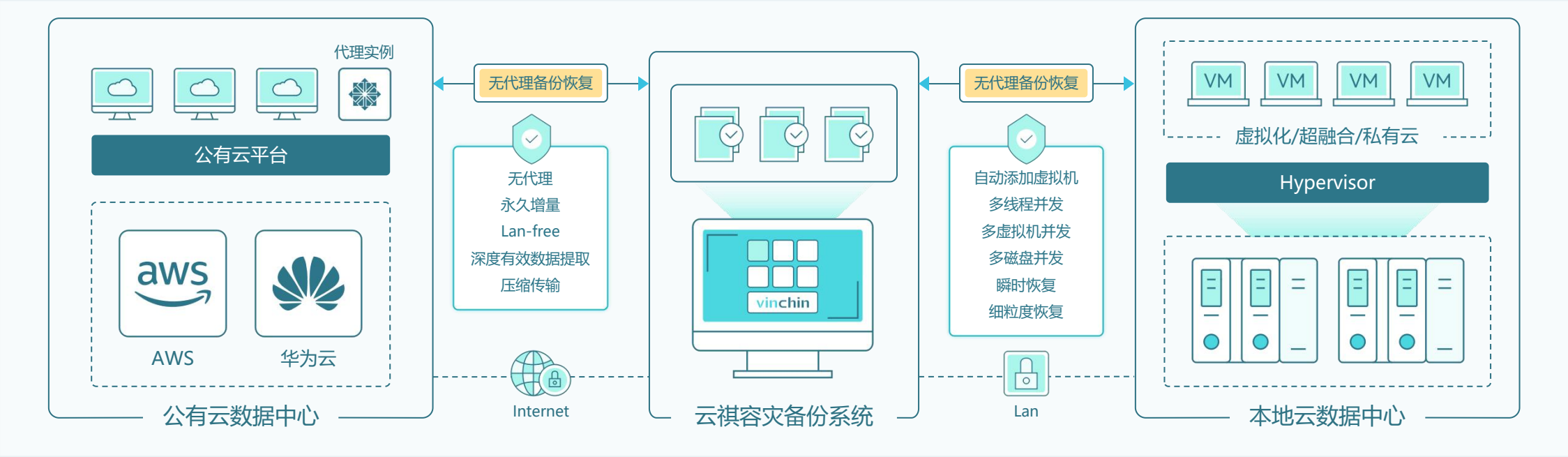
异地副本容灾

数据自动验证

病毒查杀

海量虚拟机高性能备份恢复

vinchin



智能无代理

四大架构无代理对接，无需安装客户端，更少工作量、更少资源占用，更低兼容风险

永久增量

除首次备份外，后续每次备份过程中只对新增的数据进行备份，大幅减少备份时间和占用的存储空间

Lan-free

通过存储网络进行数据传输，备份恢复时不经过局域网，不影响生产系统的正常运行，提升传输效率

深度有效数据提取

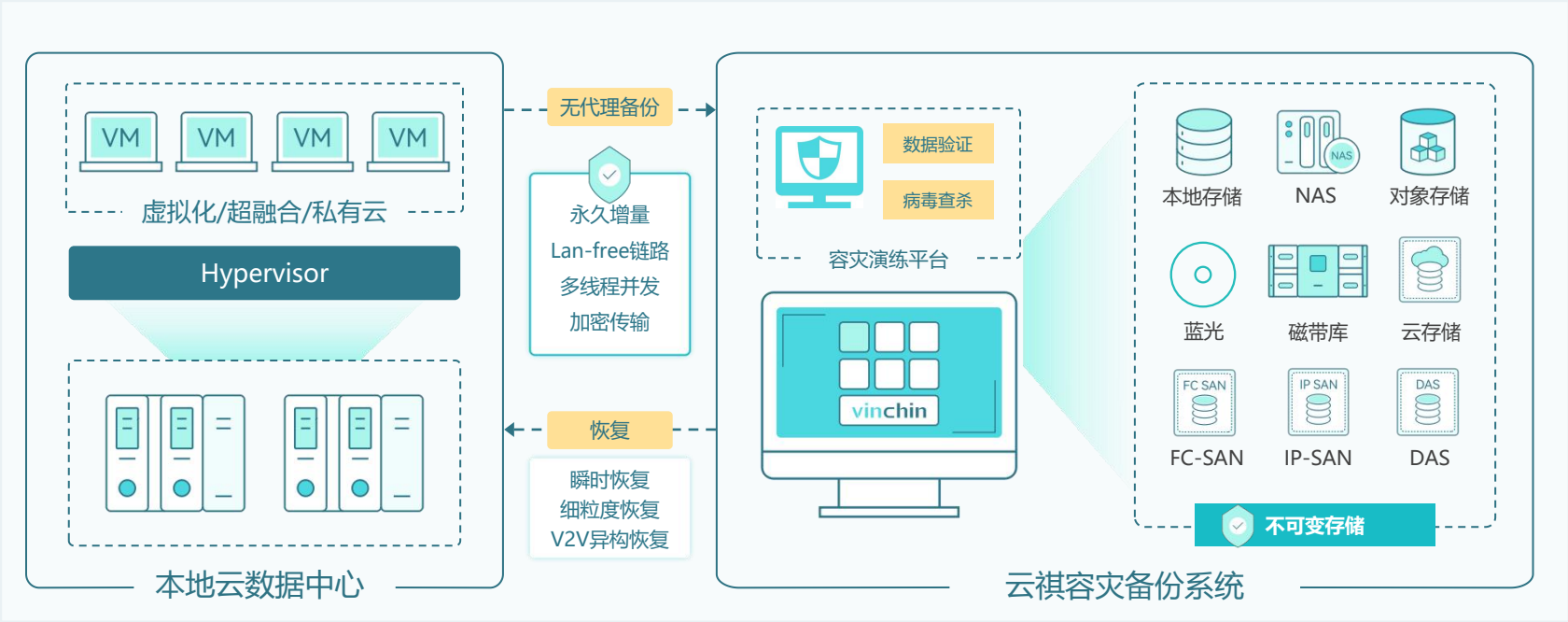
国内独家深层解析技术，深入虚拟机文件结构，快速排除非必要数据，进一步减少备份数据量

并发传输

支持多线程并发读取虚拟机磁盘数据、支持多虚拟机、多磁盘并行备份，保障数据一致性，提升备份恢复效率

海量虚拟机本地保护

vinchin



场景描述

- 数据中心的虚拟机数量庞大，需要对其进行数据保护，确保发生硬件故障、软件错误或大型自然灾害等突发事件时，本地灾备系统可提供快速恢复手段，恢复数据至原/新/云环境进行业务接管，确保业务稳定性。
- 需满足符合相关法规和规定（如等保2.0等），确保虚拟机中数据得到保护，符合标准，提升数据安全性。

核心优势

- 高效率备份恢复：无代理备份恢复降低日常运维成本，简化备份流程；通过多线程、多虚拟机、多磁盘并发备份功能提高数据传输速度；支持秒级恢复任意时间点备份数据，减少停机时间。
- 无代理跨平台迁移V2V：支持兼容范围内任意虚拟化平台之间的异构迁移，无需人工干预，自动转换配置、替换驱动，降低迁移成本，提升容灾能力。
- 低存储成本：通过永久增量备份策略，结合智能合并备份技术，缩减数据量，显著降低存储空间的需求，有效避免了资源浪费。
- 广泛兼容性：兼容国内外主流虚拟化平台；兼容主流公有云平台存储、对象存储以及传统磁带存储，提供多样化的存储选择。

vinchin

PART 06

国产化保护场景

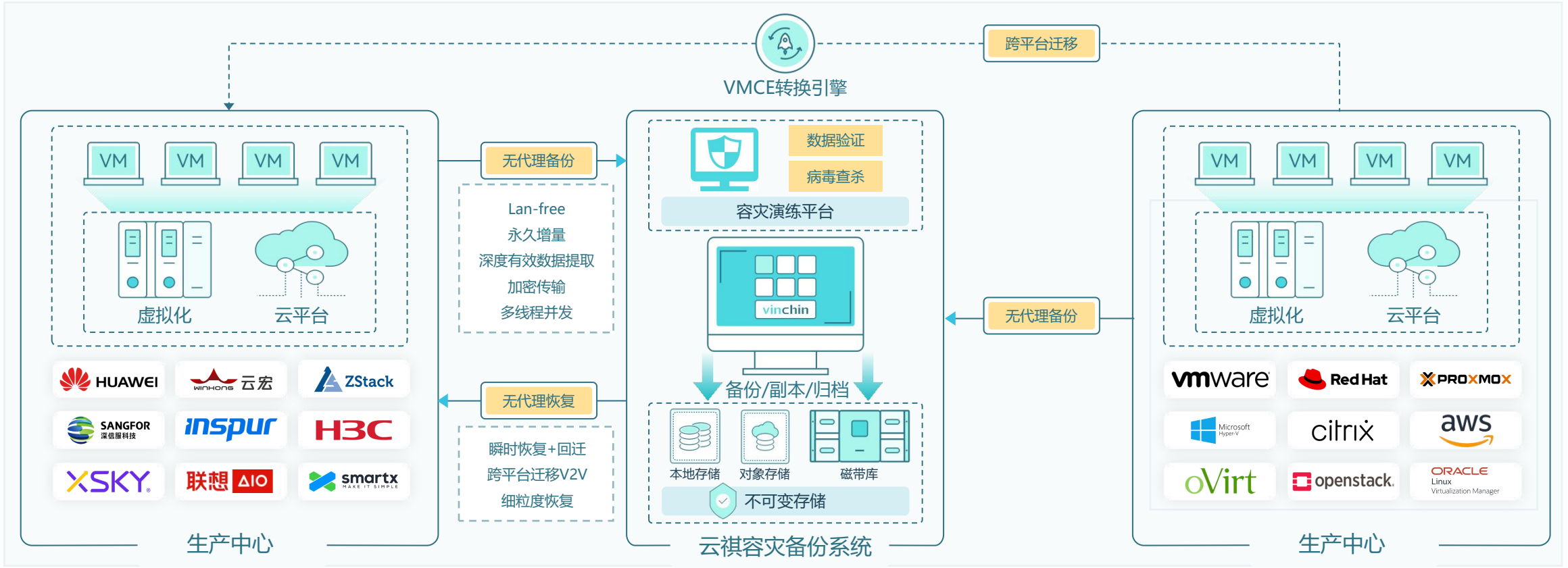
国产化场景灾备保护


东方通 TongTech
Landray 蓝凌
纷享销客
应用
海量数据 VASTDATA
openGauss
达梦数据库
KINGBASE
瀚高数据库
AsiaInfo 亚信科技
Antdb
数据库
麒麟软件
统信软件 UNIONTECH
OpenEuler
中科方德
操作系统
SANGFOR 深信服科技
云宏
ZStack Enterprise
华为云
H3C
inspur
HUAWEI
易捷行云 EasyStack
云平台
HYGON 中科海光
Kunpeng Processor
Phytium飞腾
兆芯
芯片架构
国产业务平台


国产平台数据体系化灾备
分级灾备
灾备管理
灾备运营
勒索防护
容灾演练
灾难响应
等保保护
安全合规
数据备份
定时备份
实时备份
业务容灾
容灾接管
异地容灾
数据验证
多维验证
自动验证
业务迁移
整机迁移
异构迁移
副本管理
数据副本
CDM
数据归档
离线归档
归档上云
麒麟软件
云祺容灾备份系统
OpenEuler
全栈信创灾备平台：
HYGON 中科海光
Kunpeng Processor
Phytium飞腾
兆芯

国产化混合云环境保护

vinchin



高效无代理备份恢复

四大架构无代理对接，无需安装客户端，更少工作量、更少资源占用，更低兼容风险

应急容灾接管

支持原平台/异构平台/容灾演练平台无缝瞬时恢复，分钟级跨平台业务拉起，减少平台级故障带来的损失，保障业务连续性

文件精准恢复

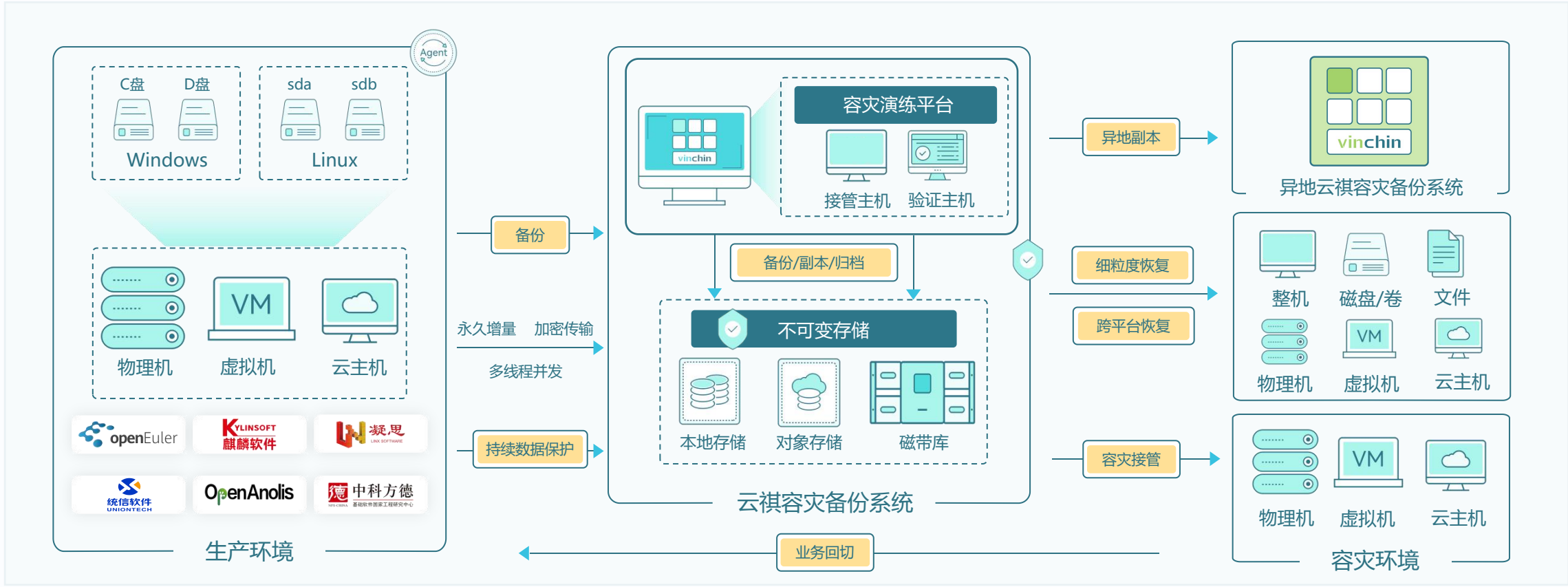
多种细粒度恢复方式，支持将单个文件/文件夹通过网络协议挂载到客户端/直接传输到指定客户端/web直接下载恢复，节省恢复时间

跨平台迁移V2V

通过云祺自研VMCE跨平台转换引擎，实现云平台间的无缝迁移，迁移全程自动进行，无需人工干预，减轻运维工作量

国产化操作系统保护

vinchin



多版本操作系统广泛兼容

支持国内外多种操作系统类型及多版本的定时与实时保护，保障数据安全与业务连续性

数据一致性保障

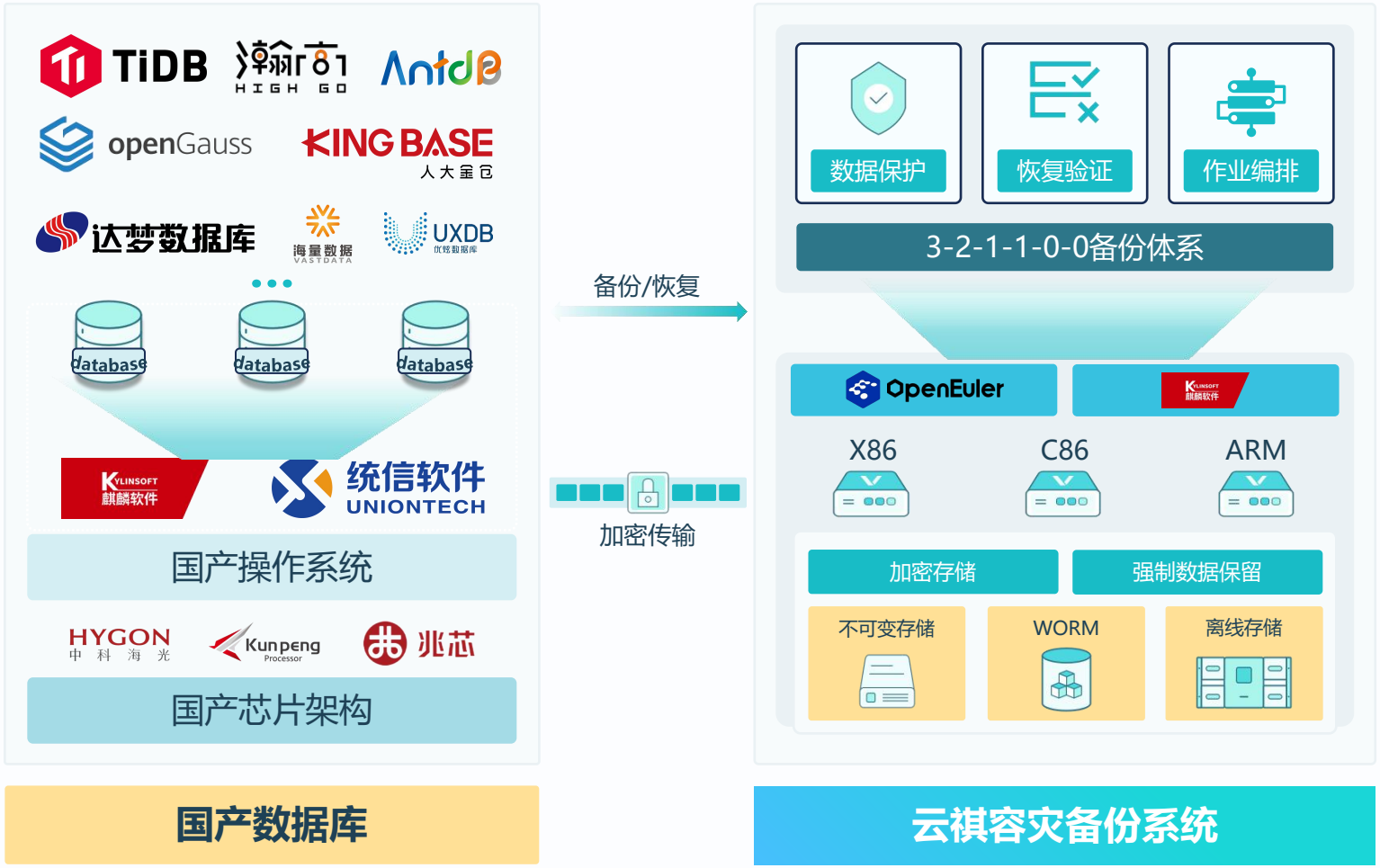
通过云祺自研的快照技术，实现Windows/Linux系统整机备份，保障数据一致性

跨平台异构恢复

支持任意平台间进行恢复，恢复时主机数据、配置根据目标平台类型自动转换，无需人工干预即可实现数据在各平台间的自由转换流动

国产化数据库保护

vinchin



国产生态融合

支持各类环境国产数据库备份，实现业务+备份全面国产化替代，助力信创战略推进

应用级一致性保障

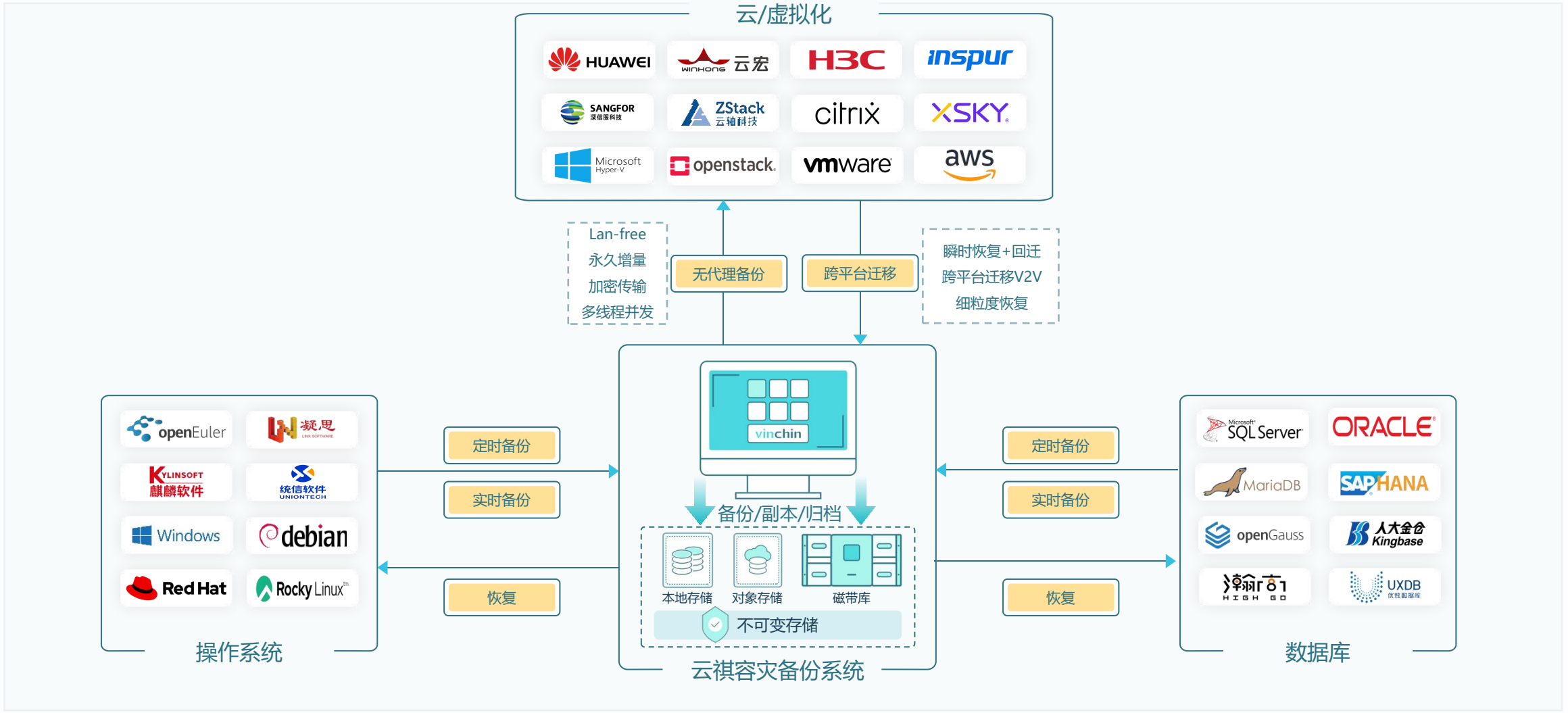
对接国产数据库标准接口备份，构建完善的生态方案，确保备份数据完整、可靠

增强数据安全

全流程加密，支持强制数据保留、不可变存储等多重安全机制保障备份数据安全

国产与非国产混合环境保护

vinchin



国内外云/操作系统/数据库广泛兼容

定时/实时备份，数据验证病毒查杀

高效备份、恢复与管理

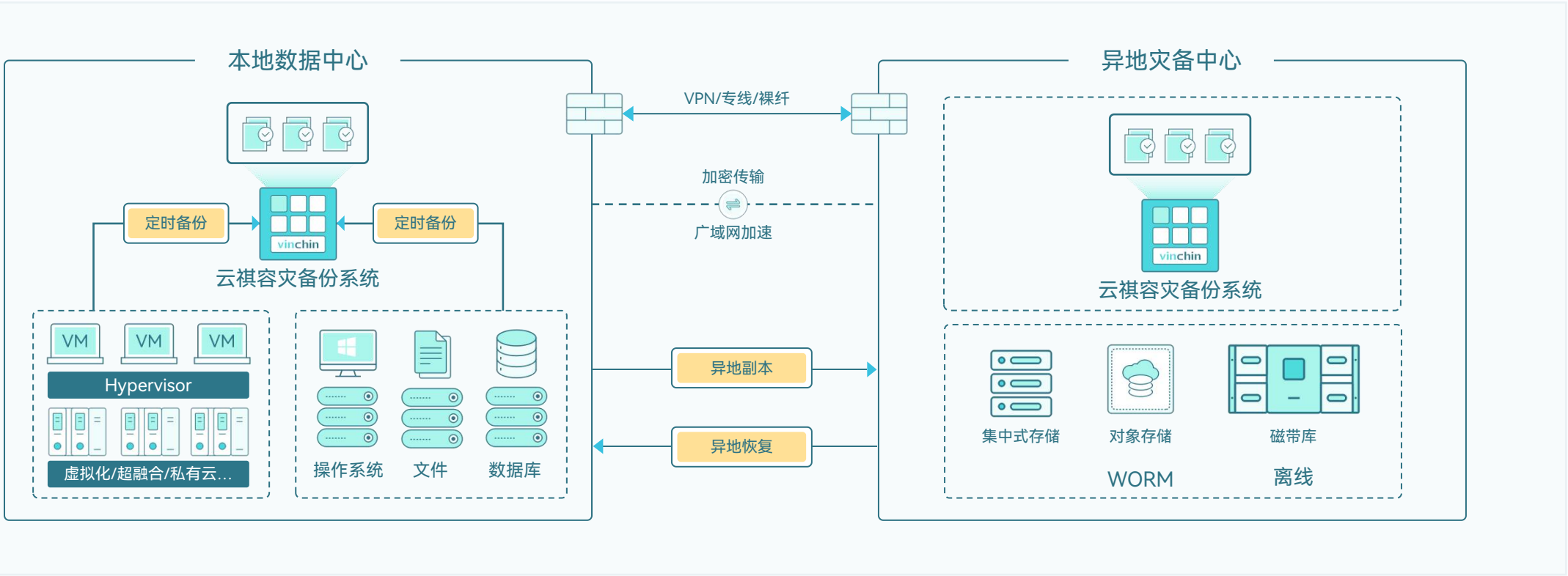
vinchin

PART 07

异地容灾

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。

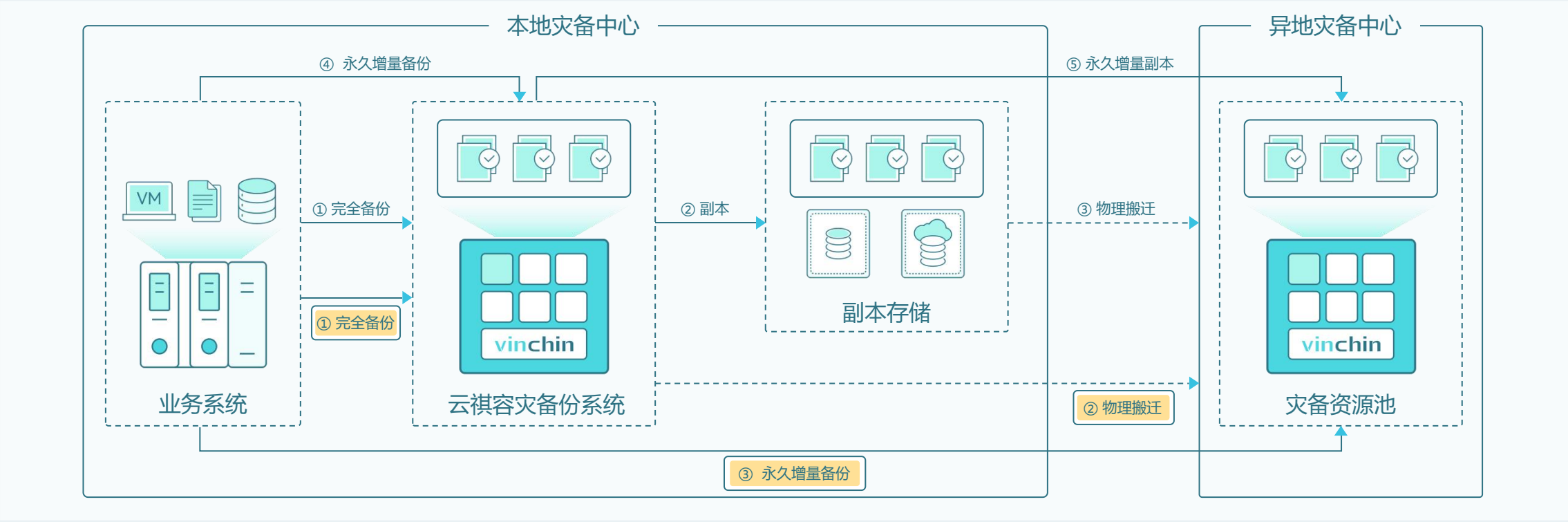
窄带宽异地传输

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。

异地窄带宽下提升传输效率



异地传输效率高

针对异地带宽有限环境，通过源端压缩、源端增量，并结合永久增量技术，减少数据传输，提高传输效率。

传输安全保障

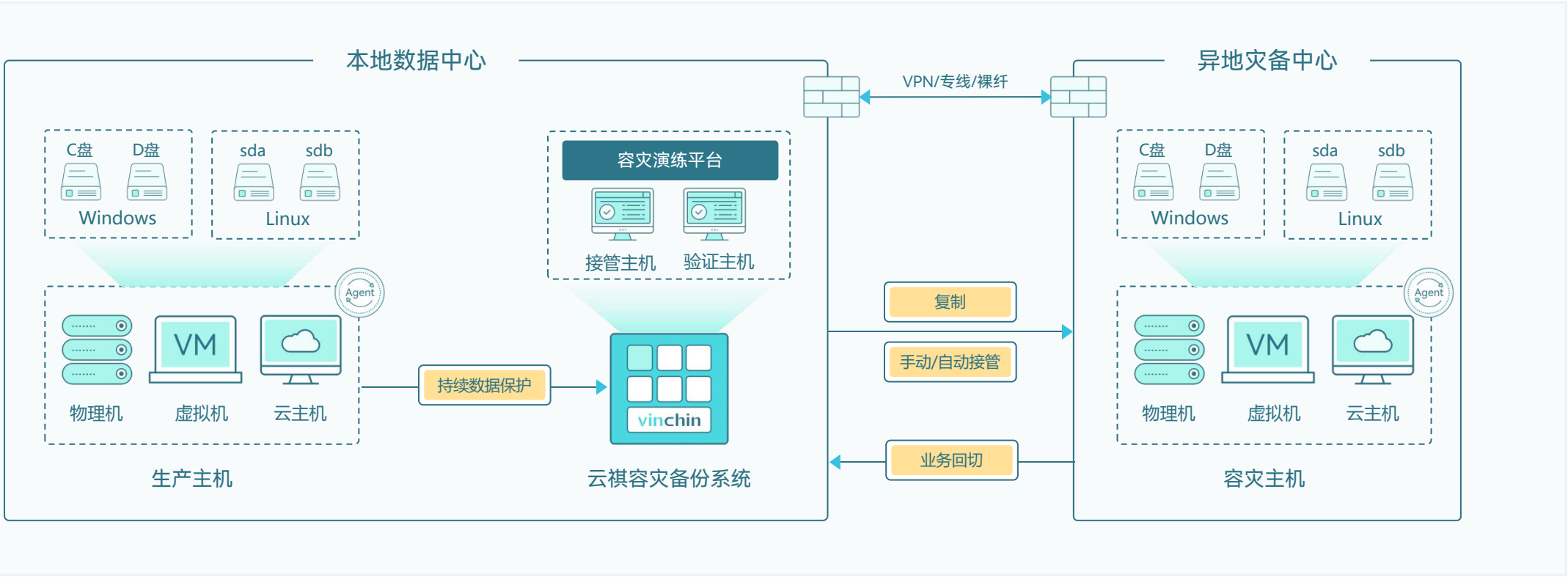
支持国密SM2和RSA的链路对副本数据加密，确保公网数据传输安全。

提升传输可靠性

支持在备份数据传输过程中，网络中断后从已处理的备份点继续进行传输。

异地复制容灾方案

vinchin



IO实时监控捕获

磁盘级实时备份，秒级IO捕获，实时同步数据，可确保数据接近于0丢失，实现RPO≈0。

保障应用一致性

通过标签点策略进行应用数据刷新操作，保证应用数据及时落盘，从而保障应用一致性。

异地容灾接管

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。

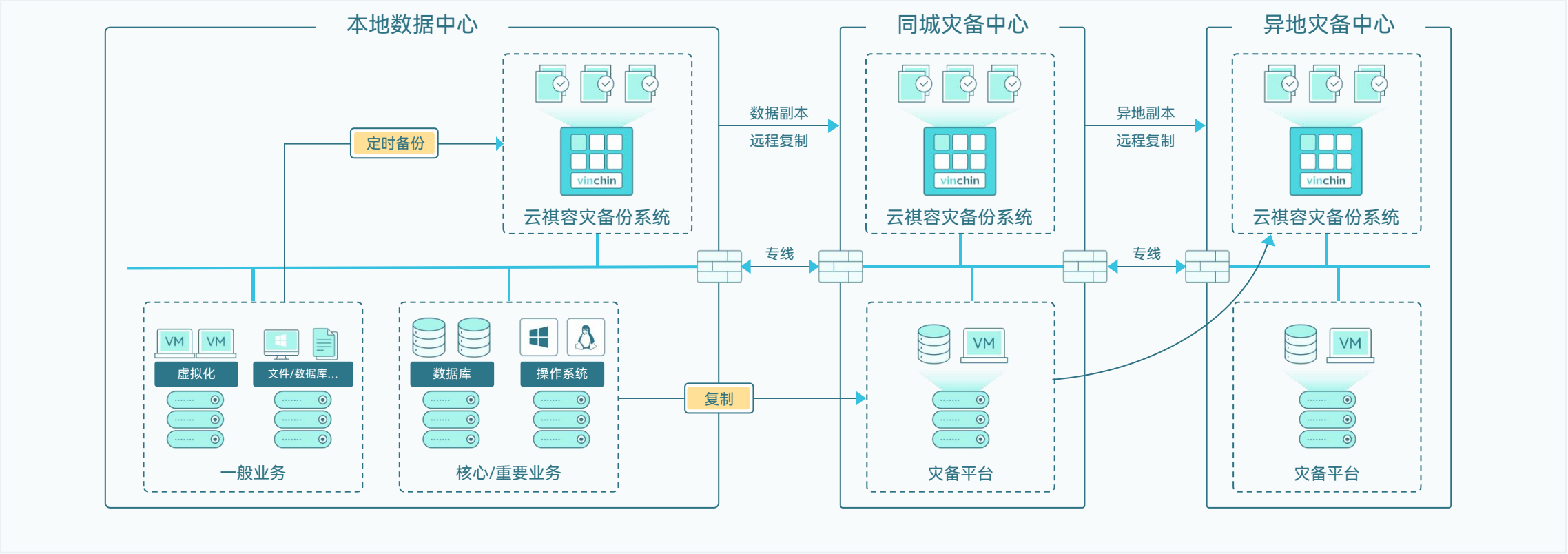
一键回切

备机接管业务后，将保存临时数据直至发起回切操作，确保数据完成回切至源环境。

两地三中心安全灾备方案

vinchin

基于3-2-1-1-0-0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。

方案价值

vinchin

01

提升业务连续性

- 提供分级分类数据保护方案，以满足不同RTO、RPO要求
- 本地数据异地保存，若本地业务故障能快速恢复或接管，保障业务连续性
- 异地传输效率高，满足窄带宽场景的高效数据传输

02

降低灾备管理复杂度

- 数据异地留存便于企业快速恢复业务系统，节省恢复成本，并有效避免数据丢失
- 可统一管理多套系统并提供可视化运维，并管理备份、副本、演练验证、容灾等多种任务

03

满足法规要求

- 满足行业法规和标准对数据备份、异地副本、异地容灾等要求
- 提供定期的数据验证并输出验证报告，保障数据的安全性和合规性

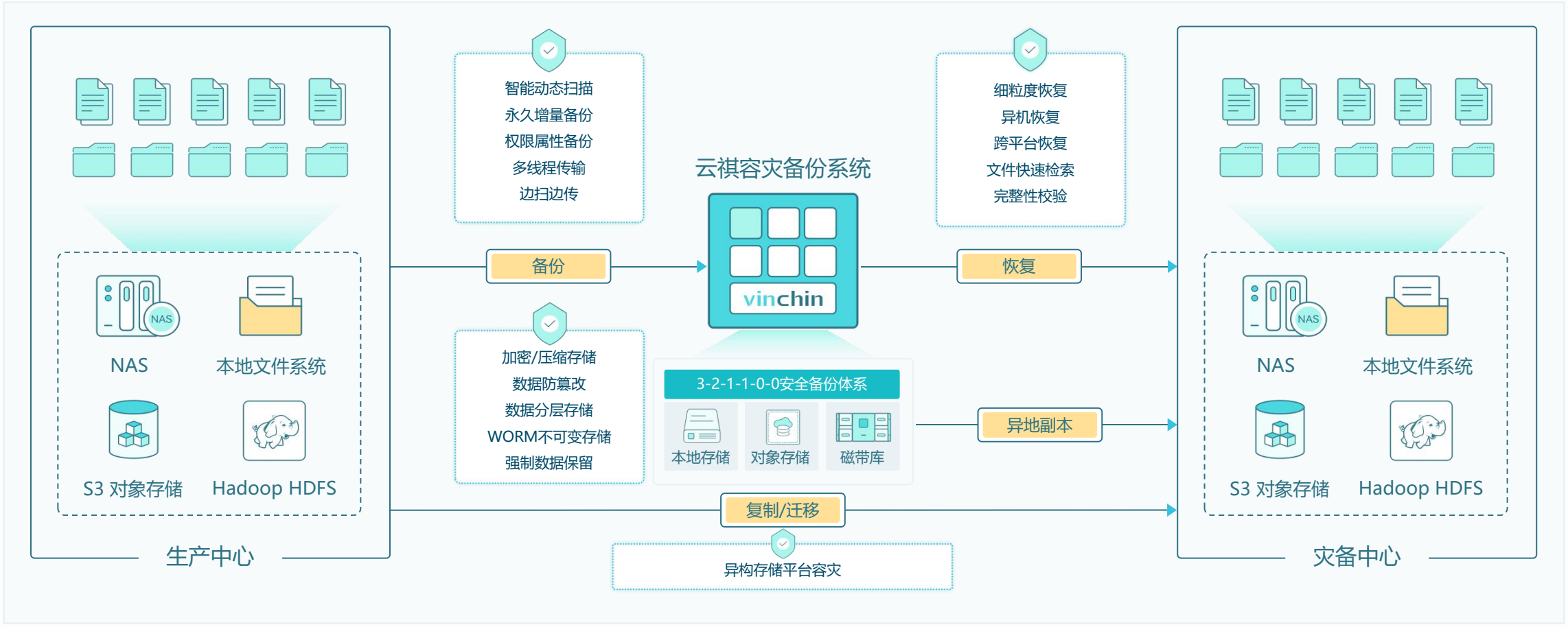
vinchin

PART 08

海量非结构化数据场景

非结构化数据保护整体解决方案

vinchin



高性能备份恢复

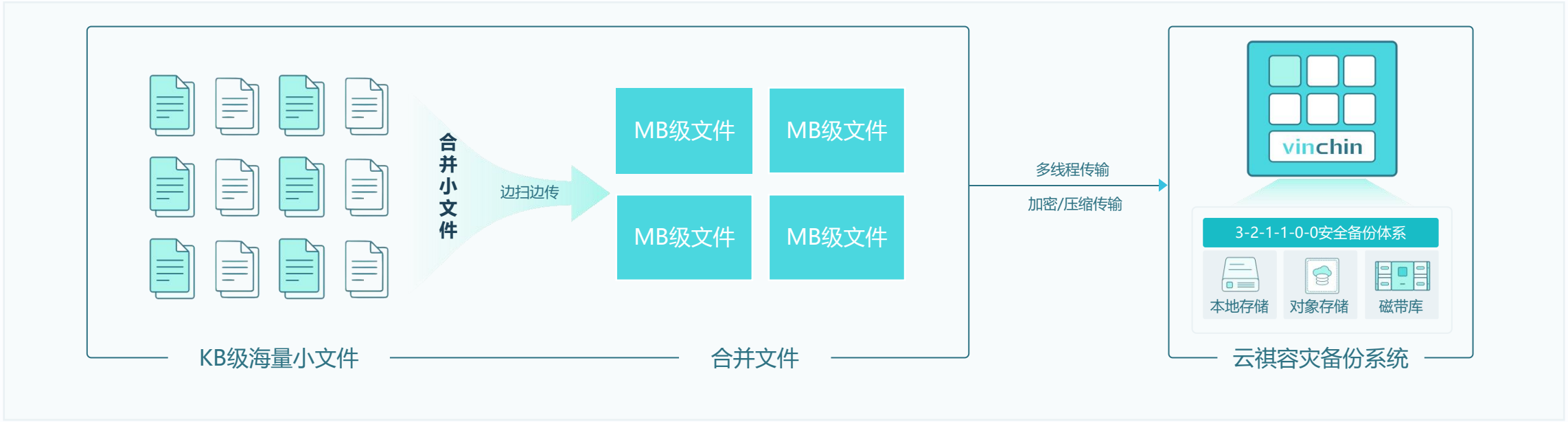
异构平台迁移

降低存储成本

保障业务连续性

高效处理小文件提升任务效率

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，结合多线程扫描和边扫边传实现海量文件的高速扫描。

多线程并发处理

支持单任务配置多线程，可同时结合多任务并发、多节点并发、边扫边传等大幅提升备份效率。

快速增量检测

通过云祺独创专利技术，构建元数据索引系统，通过将文件指纹与备份集对比实现增量数据快速识别，提升增量备份效率。

小文件备份高效性能

vinchin

实验环境

1亿小文件，文件大小随机小于20K，目录个数800万个，目录层级最深可达18层

本地文件

完备用时 **1小时40分**

扫描用时 **30分钟**

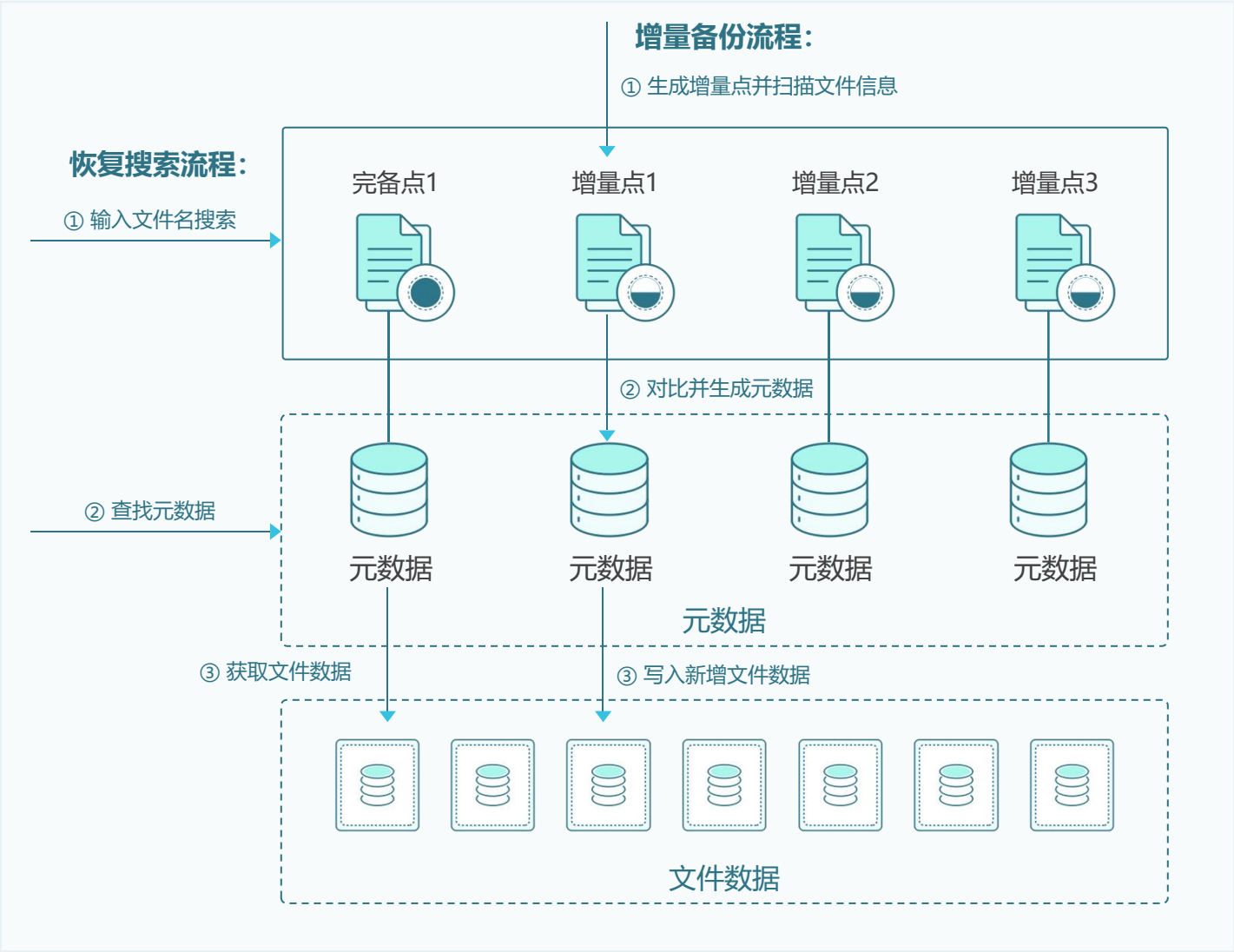
NAS

完备用时 **6小时**

扫描用时 **1小时**

元数据索引系统提升响应速度

vinchin



快速增量检测

通过云祺专利技术，构建独创的元数据索引系统，扫描对比上一时间点的元数据来快速识别增量数据。

恢复快速检索

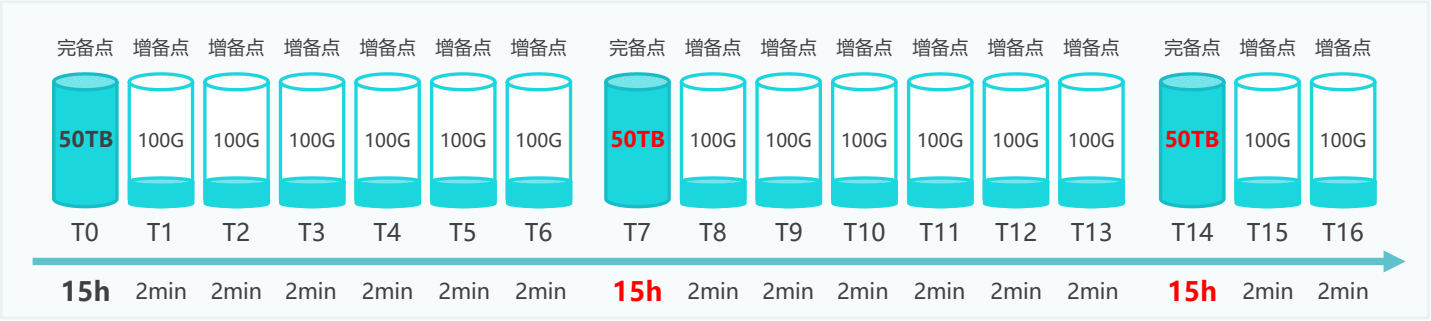
支持在恢复时，结合元数据索引系统，在已勾选恢复目录下进行关键词搜索，亿级别文件最快可在秒级内检索出目标文件。

文件永久增量减少时间窗口

vinchin

传统备份

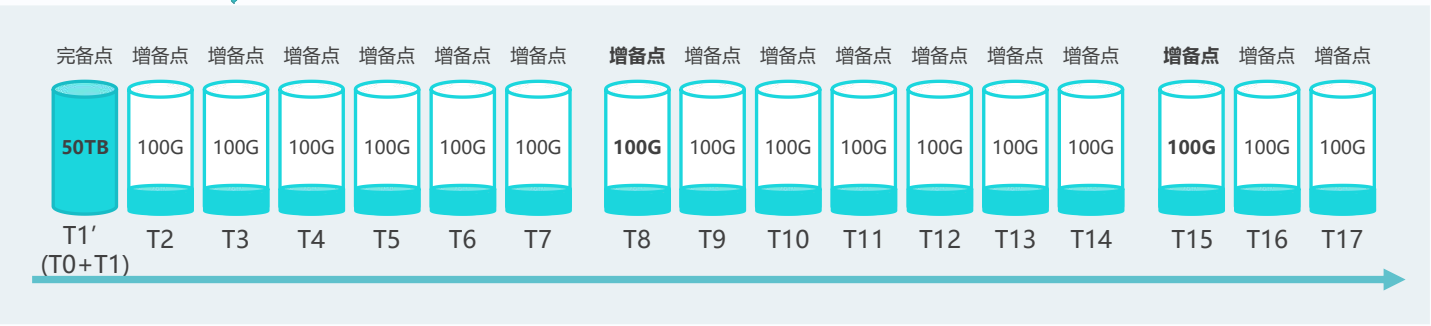
总数据量：151.37TB　　总时间：45.47H



永久增量

总数据量：51.56TB　　总时间：15.53H

保留17个备份点，第18次备份时触发保留策略，T0和T1数据合并



总数据大小：传统备份≈2.94永久增备

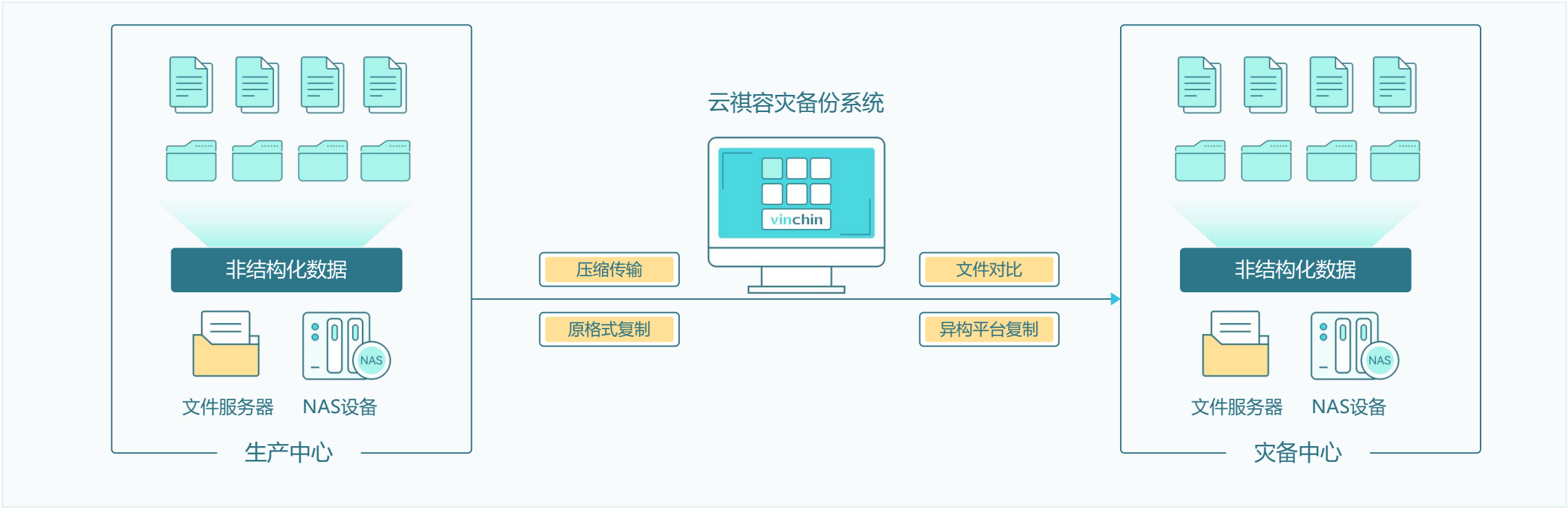
总时间花费：传统备份≈2.93永久增备

永久增量备份：只执行一次完备，后续每次备份过程中只对新增的数据进行备份，减轻数据传输负荷，减少备份时间和备份存储介质的空间占用。

例：若采用万兆网完备数据量大小50TB，备份时间窗口为15H，采用**永久增量**备份方式除第一次备份后，增量备份仅需要2min，T7时间点备份总窗口较传统方式快450倍；17个备份点的备份总窗口较传统方式**快3倍**，数据传输总量**减少66%**，**备份更高效、成本更节省**

文件复制保障业务连续性

vinchin



高效数据传输

结合压缩传输提升传输效率，智能增量对比获取变化数据并同步，减少数据传输量。

异构平台复制

支持不同设备之间进行文件数据同步，并迁移基本权限。

数据一致性保障

对比文件校验值来检测源端和目标端的差异性，并提供对比差异结果。

vinchin

实操展示

云祺容灾备份系统V6.0.5

vinchin

THANKS

云祺公众号

云祺视频号