vinchin

云祺容灾备份系统
整机数据保护解决方案

vinchin

目 录

vinchin

PART 01

中小企业数据灾备现状

vinchin

CASE 01 ·四川某连锁超市遭勒索攻击（2025年）

- •超市管理系统突然死机，无法正常交易
- •货物库存、供货、会员储值等数据全被加密锁定
- •旗下多家超市一周内未能恢复营业，损失逾20万元
- •黑客共攻击30多家企业，迫使多家支付赎金
- •嫌疑人通过虚拟货币交易收取赎金

CASE 02 ·杭州某科技公司遭境外窃取（2026年）

- •服务器端口存在弱口令漏洞，被黑客攻击利用
- •数据库相关数据被境外窃取
- •未履行网络安全、数据安全保护义务
- •违反《网络安全法》《数据安全法》，被罚款5万元

警示反思：数据安全是企业生存的生命线

这两起案例暴露出中小企业普遍存在的短板：基础防护缺失、漏洞修复不及时、缺乏灾备意识。勒索病毒攻击往往不分规模大小，任何一次对安全的忽视，都可能导致企业面临生存危机。筑牢数据安全防线，从修补每一个漏洞、部署每一道防护开始。

中小企业勒索病毒威胁

国家计算机病毒应急处理中心、计算机病毒防治技术国家工程实验室联合发布安全预警：我国境内已出现多起**“Sorry”勒索病毒**攻击案例。**入侵后会加密用户设备内全部重要文件，统一追加“Sorry”后缀，同时留存勒索信。**

关于“Sorry”勒索病毒的预警报告

发布时间：2026-08-10

一、相关病毒案例

近日，国家计算机病毒应急处理中心和计算机病毒防治技术国家工程实验室依托国家计算机病毒协同分析平台（https://virus.cverc.org.cn）在我国境内发现多起我国用户遭“Sorry”勒索病毒攻击事件。用户重要文件被加密后文件名被更改为原文件名+“.sorry”后缀字符串，同时，攻击者会在用户主机上留下勒索信，要求用户下载加密通信工具与其联系。如图1，图2所示。

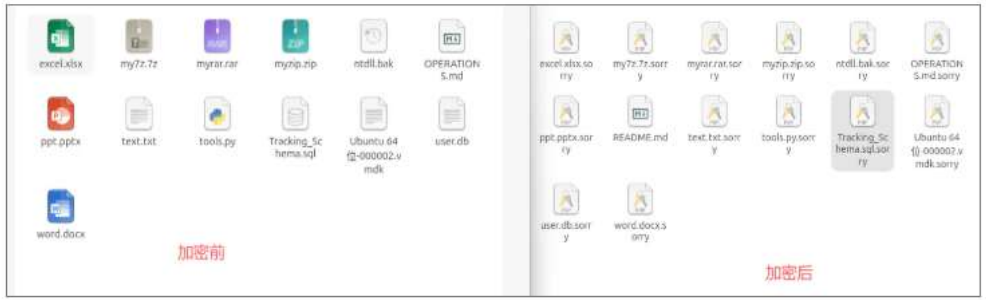


图2 勒索信内容

中小企业勒索病毒威胁

vinchin

关键统计数据

全球网络勒索受害者中，**中小企业占比超过三分之二**
中小企业遭受网络勒索的案例年增53%
勒索软件涉及88%的中小企业数据泄露事件，而大型企业仅为39%
2025年第一季度勒索软件事件同比增长近两倍（1537起 vs 572起）

恢复困境

40% 支付赎金的企业仍未能恢复数据

93% 支付赎金的受害者数据仍被盗

遭遇数据泄露的企业中，仅不到一半（41%） 能实现100%数据恢复

生存率

仅6% 的公司可在数据丢失后生存下来

43% 的公司会彻底关门

51% 的公司会在两年之内消失

业务停摆 ⟶ 客户信任削弱 ⟶ 营收断崖 ⟶ 企业永久倒闭

中小企业灾备现状

vinchin

灾备1.0（2010年前）： 磁带备份为主，成本高昂，仅大企业有能力部署
灾备2.0（2010-2020）： 虚拟化备份兴起，但中小企业因成本压力建设率不足30%
灾备3.0（2020-2024）： 云灾备兴起，成本降低50%，中小企业灾备需求快速增长
灾备4.0（2025至今）： 2025年中小企业灾备市场规模预计达100亿元，数据韧性服务市场复合快速增长率，远超传统灾备

云备份渗透率

29.7%

中小企业上云备份普及度偏低，数字化防护的基础环节存在明显短板。

数据来源：豆丁网(2026)

无灾备方案占比

21%

超过五分之一的企业处于数据“裸奔”状态，无任何灾难恢复计划与防护手段。

数据来源：Daily Research

灾备投入占比

< 3%

在企业整体IT总支出中，用于灾备建设的预算占比极低，资源配置严重失衡。

数据来源：行业调研报告

平均恢复周期

> 72h

一旦发生数据灾难，业务平均恢复时间超过3天，期间将造成巨额营收损失。

数据来源：IBM Security

恢复失败风险

70%

绝大多数受影响的机构无法在期望时间内完成业务恢复，面临生存挑战。

数据来源：Commvault

合规驱动

vinchin

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

首页 > 政策 > 国务院政策文件库 > 国务院部门文件

字号：默认 大 超大 | 打印 收藏

标　　题：	工业和信息化部等15部门办公厅（秘书局、办公室、综合司）关于促进中小企业提升合规意识加强合规管理的指导意见	发文机关：	工业和信息化部办公厅等
发文字号：	工信厅联企业〔2025〕14号	来　　源：	工业和信息化部网站
主题分类：	工业、交通\其他	公文种类：	意见
成文日期：	2025年03月07日		

工业和信息化部等15部门办公厅（秘书局、办公室、综合司）关于促进中小企业提升合规意识加强合规管理的指导意见

工信厅联企业〔2025〕14号

各省、自治区、直辖市及计划单列市、新疆生产建设兵团中小企业主管部门、党委宣传部、网信办、财政厅（局）、人力资源社会保

（七）网络和数据安全合规。引导中小企业遵守网络安全、数据安全等方面法律法规，加强信息系统、网络、数据的安全防护和安全意识教育；制定实施数据安全合规管理制度，加强对数据的分类分级和权限管理，加强人员管理和技术控制，履行重要数据识别备案、分级防护、风险评估等责任义务，防范并及时应对和处理数据泄露、篡改、丢失事件；重点梳理向第三方输出、共享、委托、提供数据，从第三方接受数据，处理个人信息及跨境传输数据等活动中的合规要求和风险，落实特定类型信息收集与使用合规义务，保护企业数据及个人信息安全。

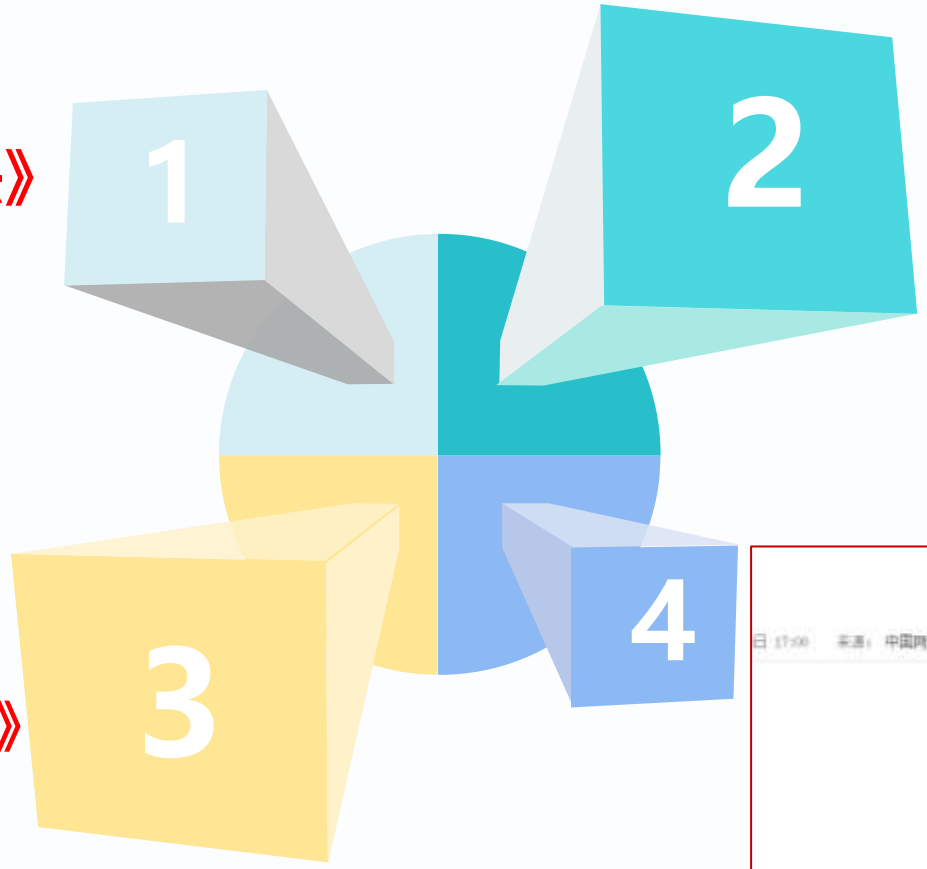
“合规红线”要求

vinchin

《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》



小型个人信息处理者个人信息保护简化措施规定

【打印】【纠错】

国家互联网信息办公室

中华人民共和国公安部

令

第25号

《小型个人信息处理者个人信息保护简化措施规定》已经2026年6月26日国家互联网信息办公室2026年第14次室务会会议审议通过，并经公安部同意，现予公布，自2026年9月1日起施行。

国家互联网信息办公室主任 庄荣文

公安部部长 王小洪

2026年7月22日

合规要求

vinchin

中华人民共和国公安部
Ministry of Public Security of the People's Republic of China

首 页　机构设置　警务信息　办事服务　警民互动　请输入关键字

当前位置：首页 > 政策文件 > 正文

《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

中小企业灾备建设重难点

vinchin

建设重点：

1.核心业务数据保护 —— 客户数据、财务数据、生产数据等
2.快速业务恢复能力 —— 最小化停机时间
3.勒索软件防护 —— 不可变备份、隔离恢复
4.合规性保障 —— 满足《数据安全法》等法规要求

实施难点	具体表现
成本压力	传统灾备方案费用高昂，无法针对多重灾难分别规划
人才短缺	缺乏专业IT人员，无力运维复杂灾备系统
业务中断顾虑	47%担扰灾备测试影响正常业务
技术复杂	异构环境（物理机、虚拟机、多云）备份恢复困难
验证困难	缺乏演练环境，备份有效性无法验证
策略缺失	仅备份数据不等于灾难恢复计划

场景业务场景实施难点

vinchin

业务场景	典型需求	实施难点
ERP系统	财务+进销存数据一体化保护	数据库复杂，恢复关联性强
OA办公系统	文档、流程数据实时备份	用户基数大，恢复时间要求高
电商平台	订单、用户数据7×24保护	业务不能停，RPO要求极高
生产制造MES	工艺参数、生产记录保护	系统老旧，异构环境兼容难
医疗信息系统	患者数据合规存储与备份	数据量大，合规要求严格
零售POS系统	交易数据实时保护	门店分散，网络条件不一

中小企业灾备如何快速落地

vinchin

“四步走”落地路径：

第一步：现状评估（数据分类分级梳理）

↓

第二步：方案选型（轻量化+整机保护）

↓

第三步：部署实施（无代理+自动化）

↓

第四步：持续运营（自动演练+合规审计）

维度	关键措施
技术选型	整机一体化保护方案，避免数据与应用分离
成本控制	采用云灾备/按需付费模式，降低初始投入
运维简化	自动化备份+自动演练，减少人力依赖
合规先行	满足等保、数安法等法规要求，规避处罚风险
演练常态化	定期验证备份有效性，确保灾难时“可用”

vinchin

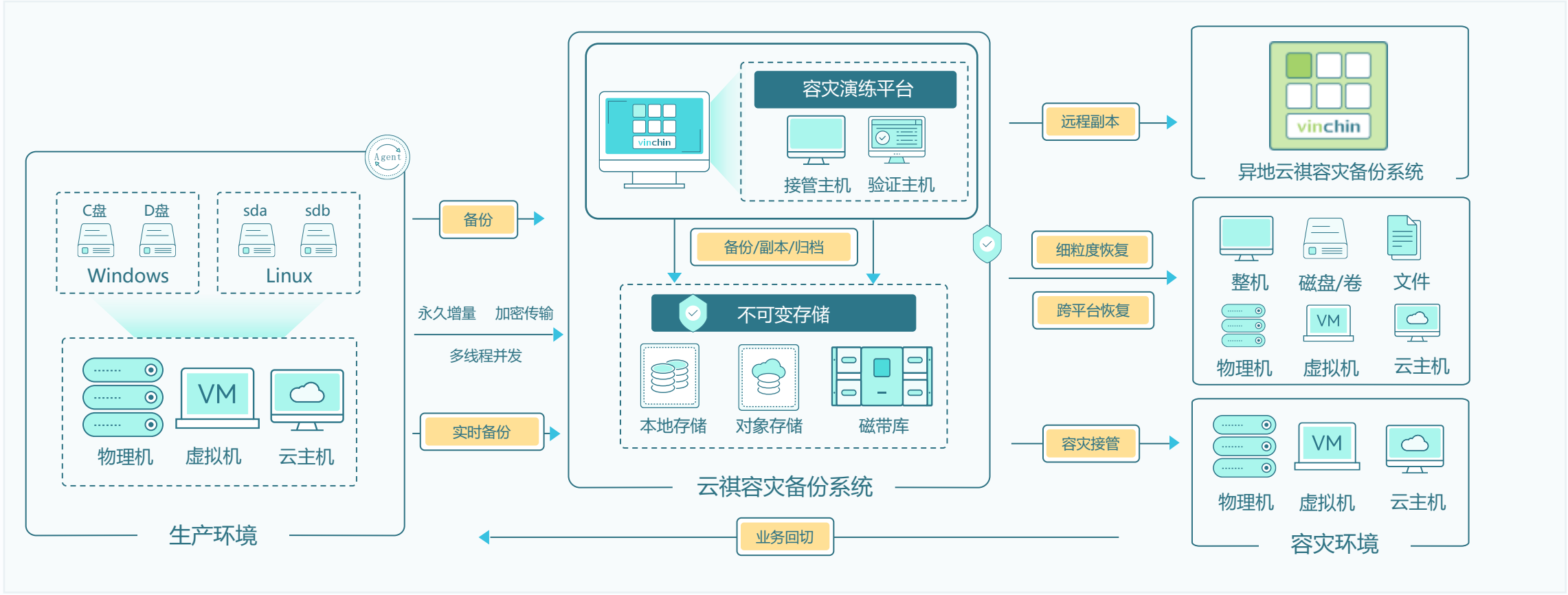
PART 02

整机一体化落地防护

整机一体化保护方案

vinchin

定时/实时备份 | **数据快速恢复** | **数据自动验证**



应急容灾 | **自动化运维** | **保障业务连续性**

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

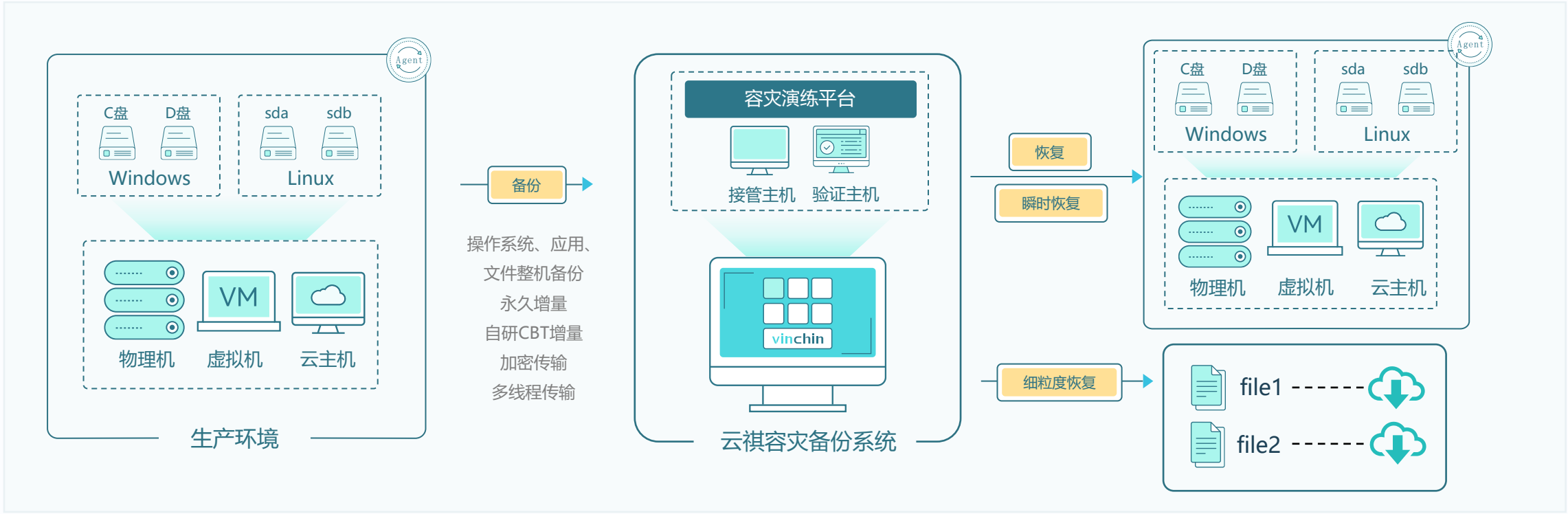
定期对备份数据进行自动验证，确认备份数据的可用性，保证在需要时可以正确恢复

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

整机定时备份，轻量化部署

vinchin



异构环境覆盖

物理机 / 虚拟机 / 云主机

无需客户端，即装即用

智能数据处理

CBT增量捕获 / 压缩去重

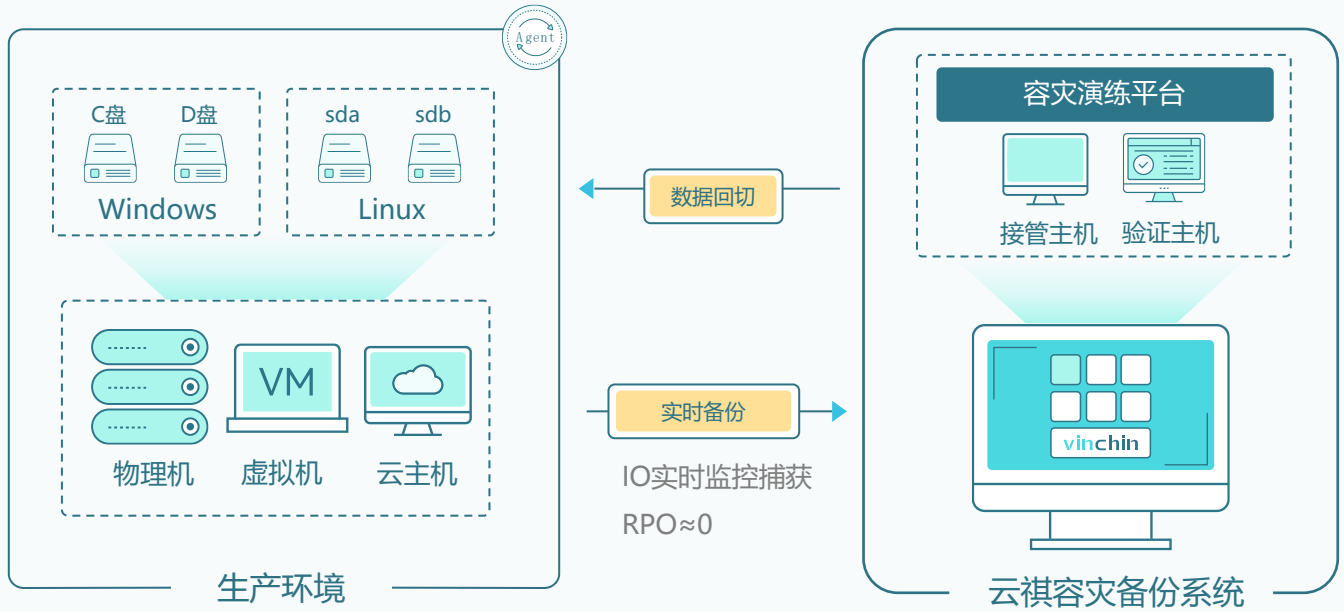
带宽占用降低60%+

成本最优

分级存储

投入减半

整机实时备份



内置容灾演练平台

一套系统即可同时满足数据验证、容灾接管，在保障数据安全的同时，帮助用户降低验证、容灾成本

应急容灾

云祺容灾备份系统实时监控生产主机心跳，生产故障时可通过容灾演练平台自动完成接管，继续提供业务支撑

任意时间点回退

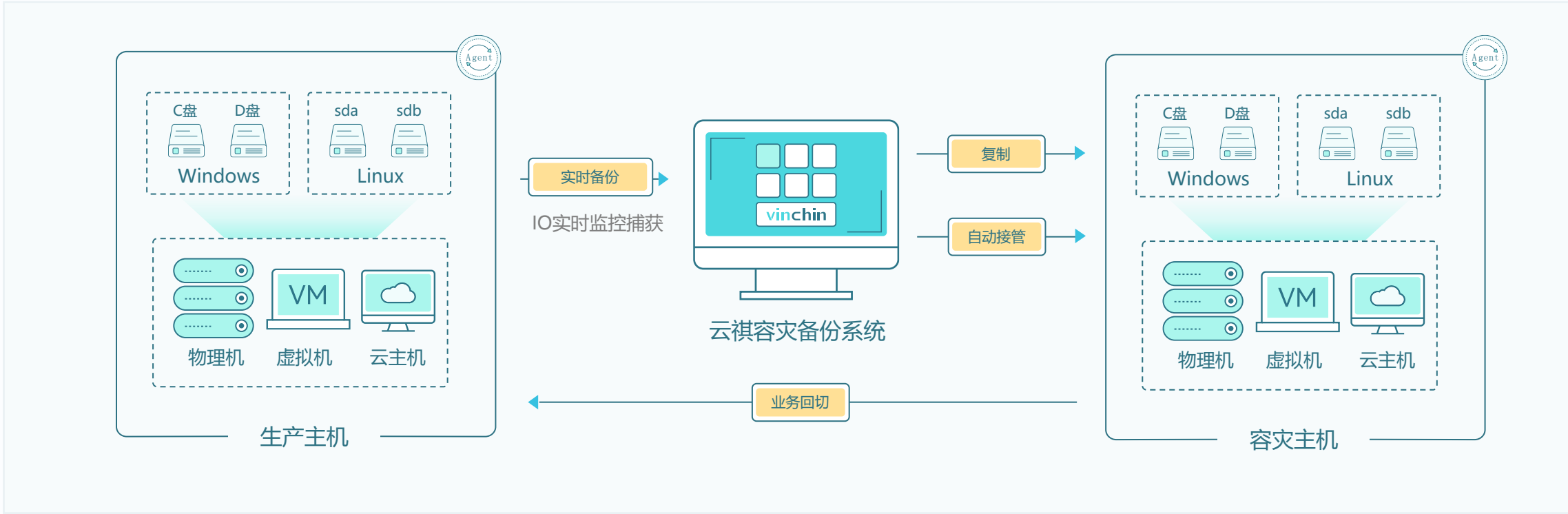
连续捕获生产IO并同步至备份系统，出现逻辑错误或误操作时，可回退至任意时间点

隔离验证环境

隔离验证环境，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

整机复制容灾

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，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

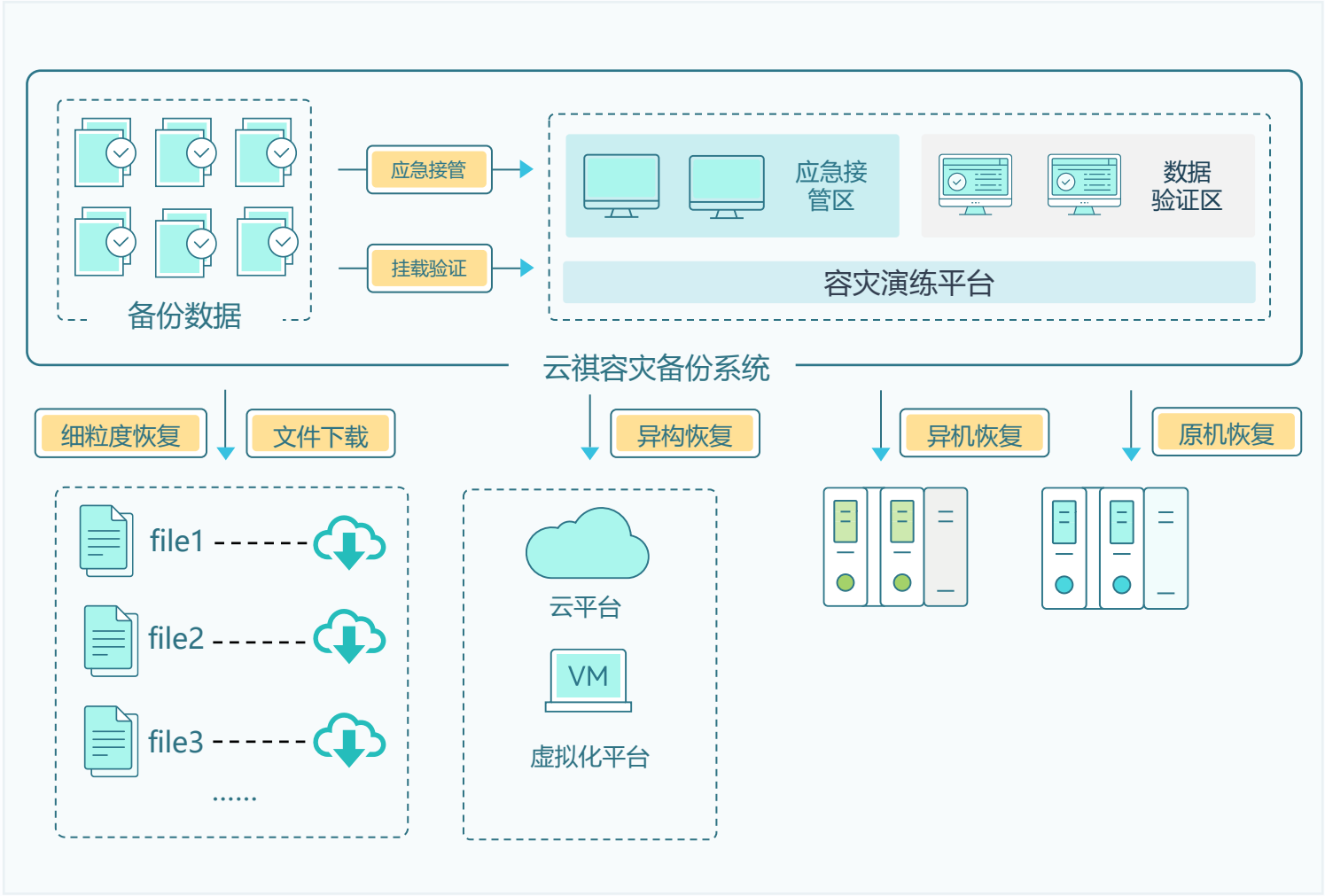
整机容灾接管

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

弹性恢复，让业务持续在线



应急接管

云祺容灾备份系统实时监控生产主机心跳，生产故障时可通过容灾演练平台自动完成接管，继续提供业务支撑，保障业务连续性

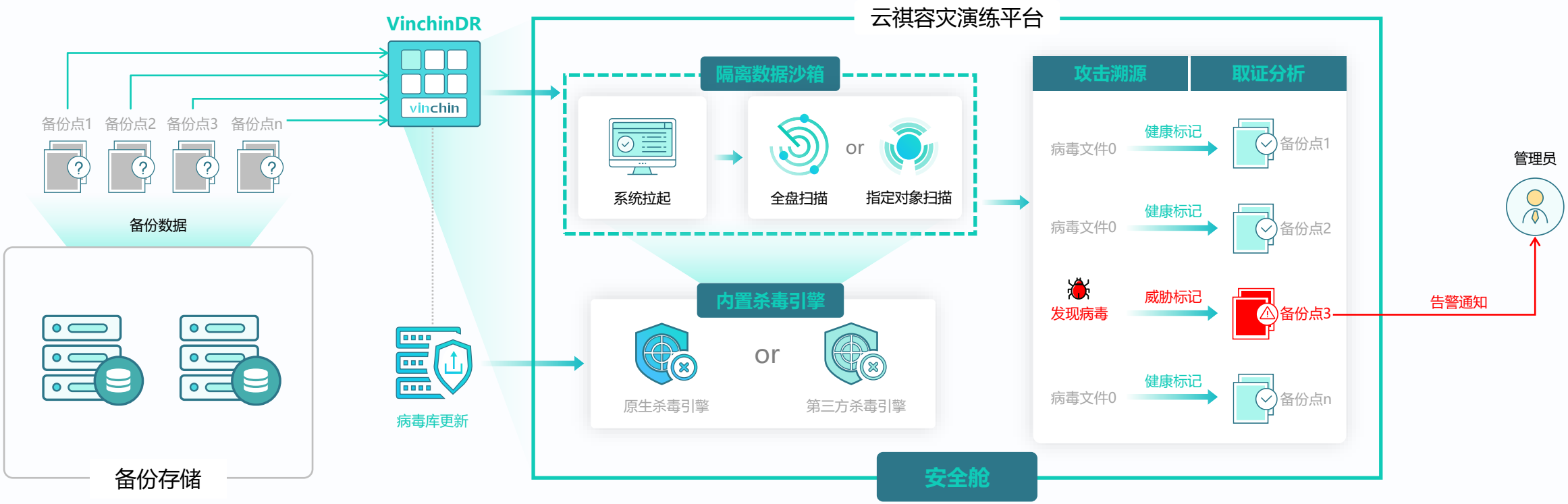
细粒度恢复

用户可在浏览器直接下载文件、也可将文件恢复到其他客户端，或通过网络协议将文件系统挂载到其他客户端进行生产、测试、演练

异构平台快速恢复

vinchin

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

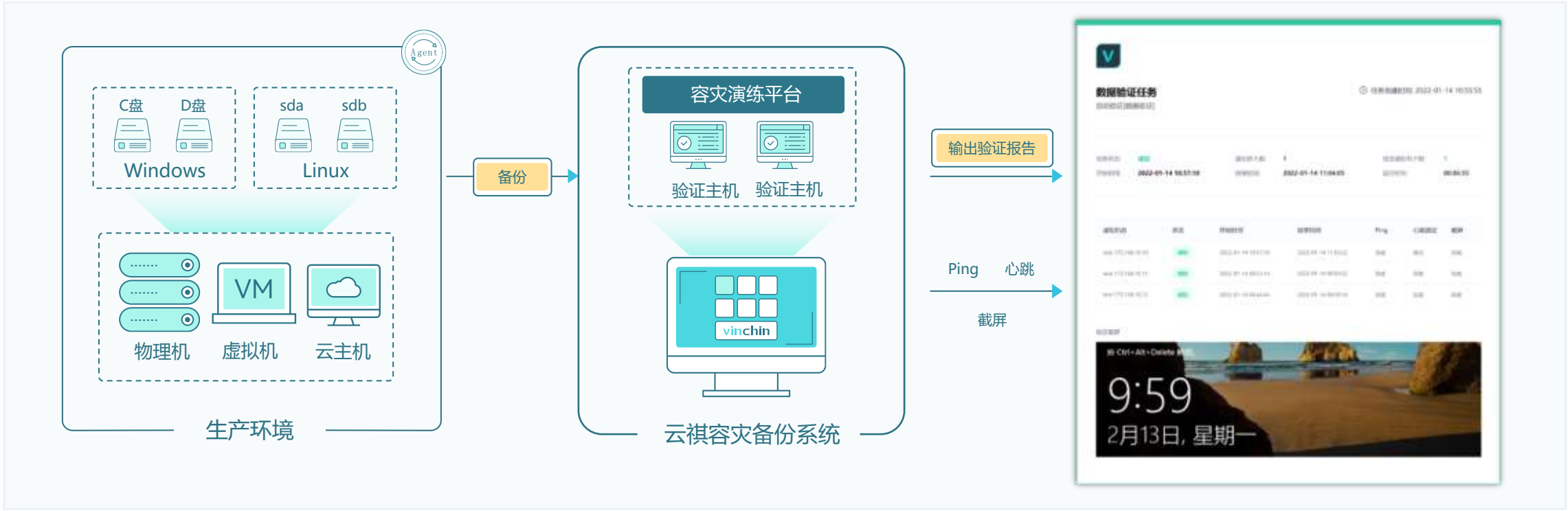
在备份数据中查找干净可用的备份点，为将来的安全恢复做好准备

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

自动验证&病毒查杀，确保数据完整可靠

vinchin



内置验证平台

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

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，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

自动化运维管理

vinchin

策略定义

灵活配置备份规则，按需定制策略模板

自动执行

智能识别环境，全自动调度任务运行

容灾接管

故障毫秒级检测，自动切换保障连续

全局监控

实时状态可视，异常即刻告警

01 智能策略管理

支持全量、增量、差异备份策略的灵活定义，支持按时间窗口、业务负载自动调度执行。提供策略模板化管理，可一键下发至集群主机，减少人工配置成本，确保备份策略精准落地。

02 应用一致性保障

自动发现并适配Oracle、SQL Server、MySQL等主流数据库及业务系统。利用应用级快照技术，确保备份数据的事务一致性与完整性，恢复后业务系统可直接接管使用，无需额外修复。

03 故障自动接管

生产端发生故障时，系统毫秒级检测异常，容灾备机可自动或手动快速接管业务流量。接管过程无需人工复杂干预，实现业务的秒级恢复，有效降低业务中断带来的经济损失。

04 可视化监控告警

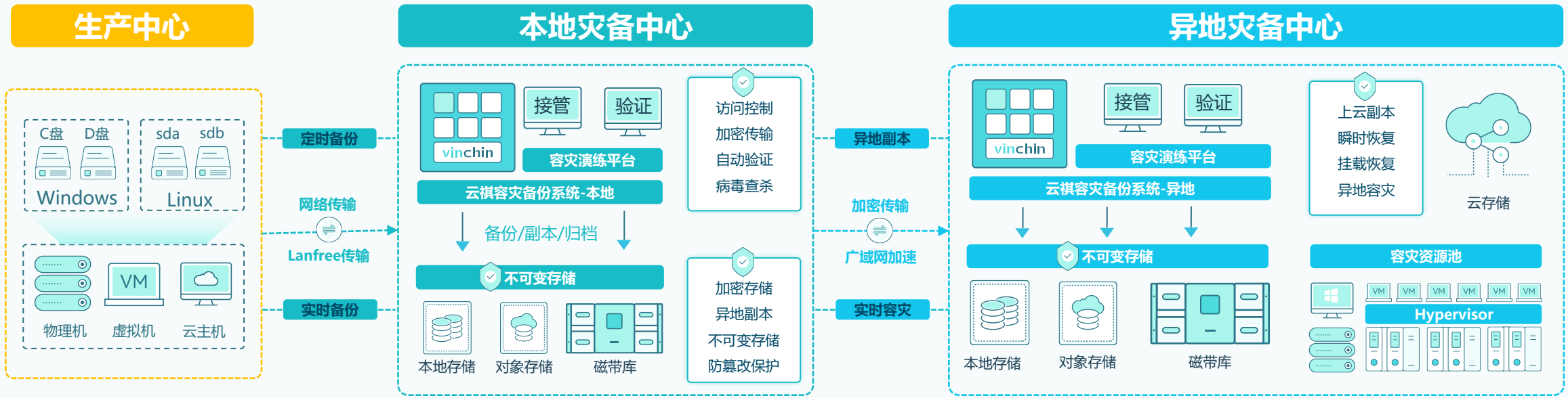
提供可视化的全局运维监控看板，实时展示备份进度、设备健康状态及容灾链路连通性。异常情况即时通过邮件、短信等多渠道触发告警，支持历史日志审计与追溯。

vinchin

PART 03

应用场景

整机防勒索



场景描述

勒索病毒攻击事件频繁发生，如何保障整机备份数据的安全性和完整性成了重中之重。若备份数据中存在病毒，恢复时就可能导致病毒传播或其他生产数据受到感染，进而影响业务正常运行。此时需要对备份数据进行病毒查杀，确保数据恢复时不会被病毒感染，提高备份数据的安全性。

防勒索架构：3-2-1-1-0-0

3：三份副本

2：两种不同存储介质

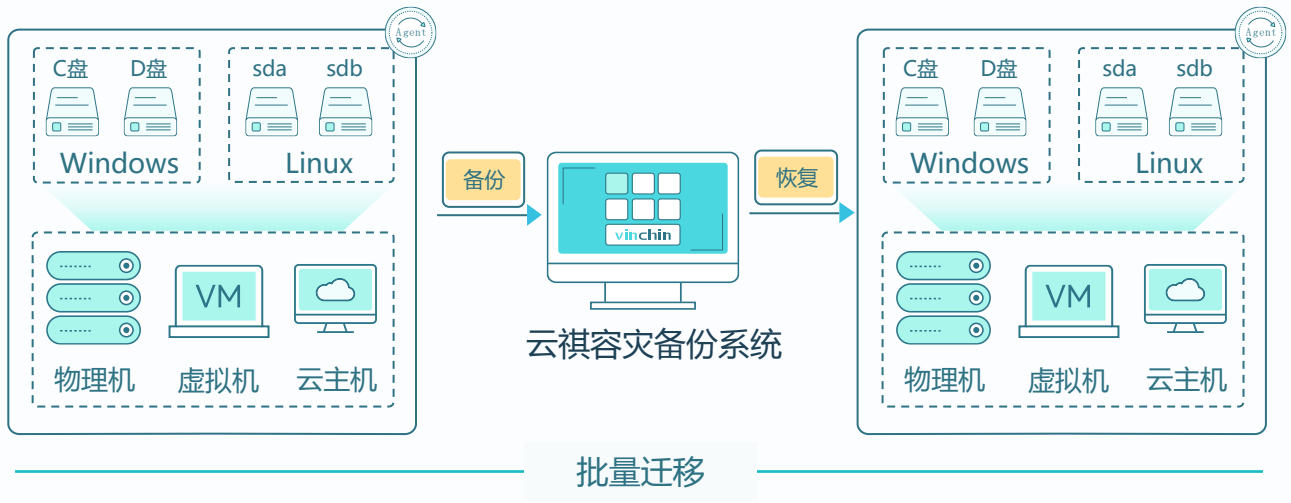
1：一份异地副本

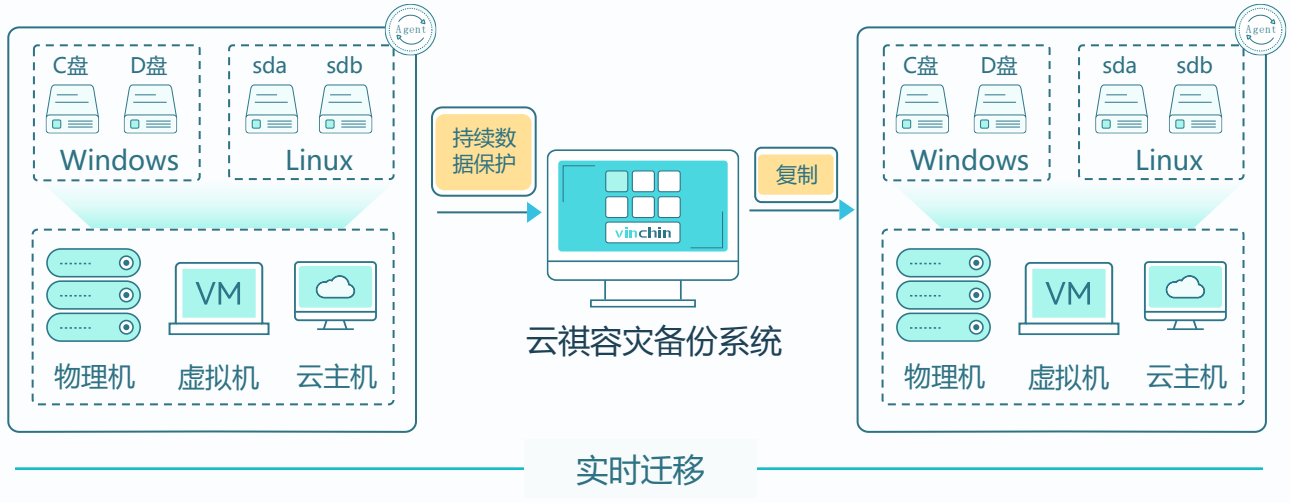
1：一个离线或不可变存储

0：零个验证错误

0：零个未经授权访问

业务迁移





场景特点

- **兼容性限制：**迁移往往涉及不同品牌硬件之间、不同虚拟化厂商之间乃至物理设备到虚拟化的迁移，兼容性可能会受到限制。
- **停机时间长：**传统迁移过程中，每次启、停业务都需要耗费至少数小时，同时数据转移还需耗费时间，导致整个业务系统中断时间按天计算，时间过长。
- **操作复杂：**传统迁移时需手工搭建与原业务系统相同的运行环境，包含操作系统、数据库、应用程序等，再导入数据，配置业务，步骤繁多，费时费力，增加运维难度。

优势价值

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

数据实时迁移：在迁移过程中生产主机无需停机，将数据从生产主机实时同步到新环境中，对生产系统的正常运行无任何影响。

图形化管理：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，方便用户快速掌握操作和使用方式。

国产化场景灾备

场景特点

国家鼓励和支持信息技术应用创新产业发展，推动核心领域如芯片、操作系统、数据库等的国产化替代。同样，备份作为数据安全的重要组成部分，也面临着国产化的需求。此外，政策和法规的发布也在各行各业中彰显出国产化数据保护的重要性。

优势价值

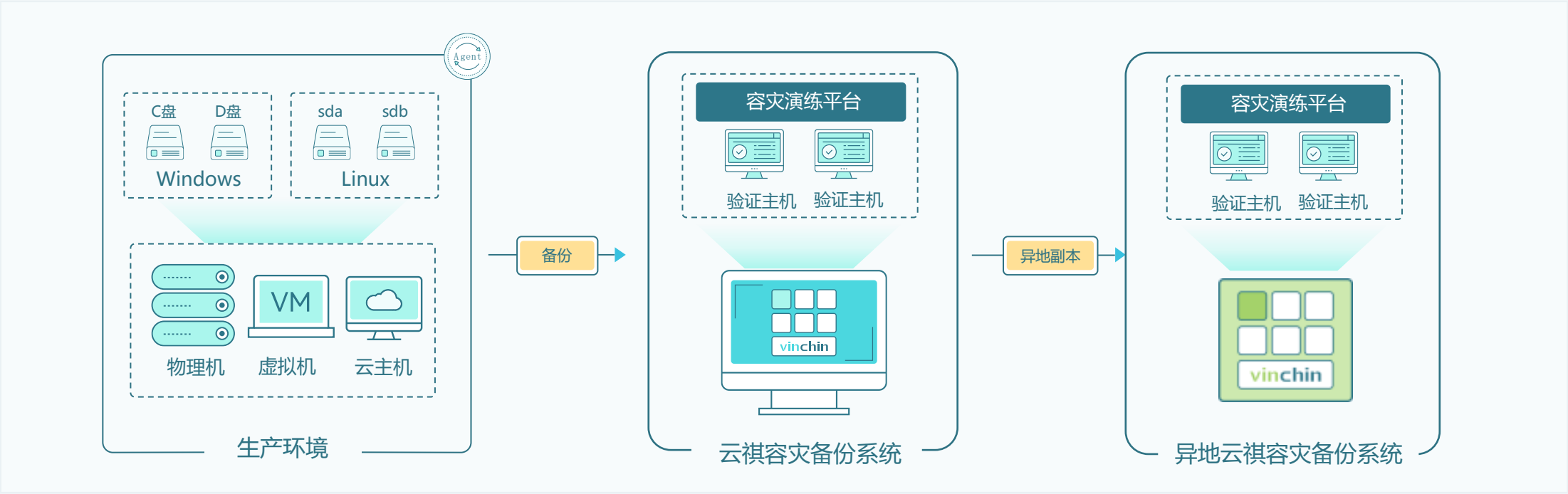
多版本操作系统兼容：针对国产操作系统，云祺容灾备份系统广泛兼容，实现整机数据高效备份与恢复。

确保数据一致性：云祺科技自研快照，实现Windows/Linux系统整机备份，并保障数据一致性。

多种恢复方式：支持整机、磁盘、卷、文件各种恢复粒度；支持原机恢复、异机恢复、异构恢复，可恢复到物理机、公有云或虚拟化平台；

灾难恢复演练

vinchin



场景特点

- 资源消耗：备份数据验证需要消耗大量的计算资源和存储资源，包括CPU计算资源、内存资源等。
- 影响生产环境：若测试环境与生产环境共享相同的物理资源（如存储设备或网络资源），在恢复备份数据时，可能会占用这些资源，从而影响生产环境的性能。
- 成本投入较高：为了减少对生产环境的影响，有时会使用独立的计算资源，如虚拟机或云服务器，而这些将产生额外的成本，增大用户负担。

优势价值

隔离演练环境：由于采用内置容灾演练平台方式进行演练恢复，整个环境中只有备份系统可以与隔离网络内的虚拟机进行通信验证，不会对用户生产环境造成网络冲突、业务冲突的影响；

自动验证：验证全程自动化，web界面清晰明了，用户只需简单操作即可获得验证报告

降低演练成本：一套备份系统即可完成隔离演练环境的搭建，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