vinchin

等保再升级，解码合规新标准

GA/T 2380-2026 《信息安全技术 网络安全等级保护数据安全基本要求》

vinchin

目 录

PART 01 新规细则解析

PART 02 与等保2.0的差异对比

PART 03 云祺合规解决方案

PART 04 案例分享

vinchin

PART 01

新规细则解析

vinchin

关于批准发布《中华人民共和国机动车行驶证》等28项公共安全行业标准的公告

时间：2026年01月29日　　字体：大 中 小　　分享到：

中华人民共和国公安部
公共安全行业标准公告

2026 年第 1 号

关于批准发布《中华人民共和国机动车行驶证》等 28 项公共安全行业标准的公告

公安部批准《中华人民共和国机动车行驶证》等28项公共安全行业标准，并报国家市场监督管理总局备案，予以公告。

公 安 部

2026年1月9日

序号	标准编号	标准名称	代替标准号	实施日期
18	GA/T 2380—2026	信息安全技术 网络安全等级保护数据安全基本要求	无	2026.06.01
19	GA/T 2381—2026	信息安全技术 网络安全等级保护数据安全测评机构能力要求	无	2026.06.01
12	GA/T 2394—2026	信息安全技术 网络安全等级保护数据安全测评要求	无	2026.07.01
13	GA/T 2395—2026	信息安全技术 网络安全等级保护数据安全测评过程指南	无	2026.07.01

标准概述与定位

vinchin

序号	标准编号	标准名称	发布日期	实施日期
1	GA/T 2380—2026	信息安全技术 网络安全等级保护数据安全基本要求	2026-01-09	2026-06-01
2	GA/T 2381—2026	信息安全技术 网络安全等级保护数据安全测评机构能力要求	2026-01-09	2026-06-01
3	GA/T 2394—2026	信息安全技术 网络安全等级保护数据安全测评要求	2026-02-28	2026-07-01
4	GA/T 2395—2026	信息安全技术 网络安全等级保护数据安全测评过程指南	2026-02-28	2026-07-01

（图片来自:公安部等级保护评估中心)

标准概述与定位

vinchin

《信息安全技术 网络安全等级保护数据安全基本要求》（GA/T 2380-2026）

发布机构：中华人民共和国公安部 | 发布日期：2026年1月9日 | 实施日期：2026年6月1日

标准定位：等保2.0的专项升级与补充

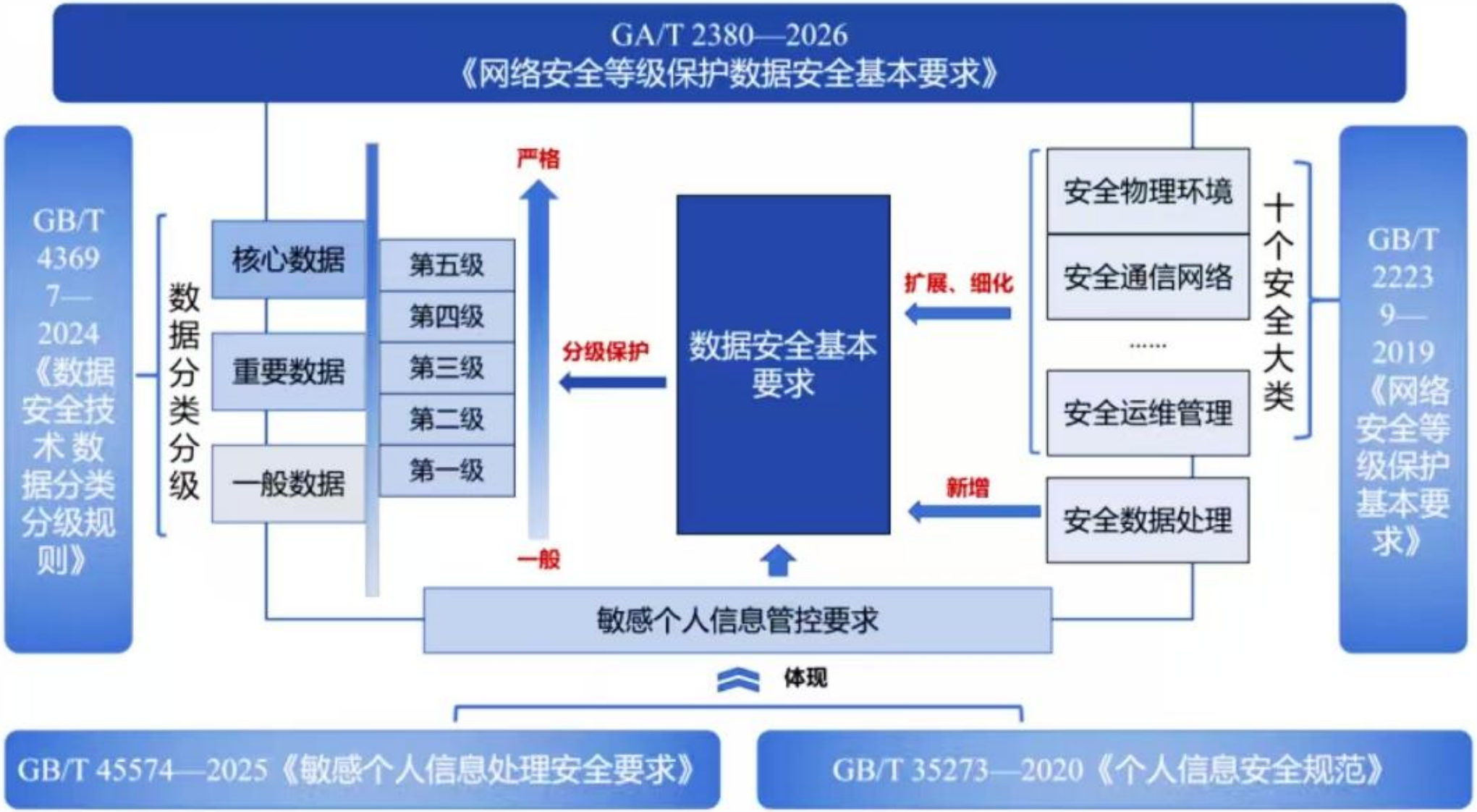
该标准并非替代GB/T 22239-2019（等保2.0），而是在其基础上针对数据安全领域进行的全面、细致扩充。它延续了等级保护的分级分类理念，将数据安全治理的要求深度融入等级保护体系，形成“系统+数据”的双重防护格局。

核心突破：确立数据安全独立考核维度

首次将“数据安全”提升为与“系统安全”并行的独立考核维度，意味着数据安全不再是系统安全的附属品，拥有了独立的评估体系、技术要求和管理规范。这一变革要求组织在建设和运营中，必须将数据安全作为核心目标之一进行规划与落地。

标准导向：从被动防御转向主动治理，将数据安全能力建设贯穿于系统设计、开发、运维的全生命周期，实现从“合规达标”到“实质安全”的根本性转变。

标准内容与框架



（图片来自:公安部等级保护评估中心)

标准内容与框架

（图片来自:公安部等级保护评估中心)

标准内容与框架

vinchin

以全生命周期为主线，构建“技术+管理+审计”三维支撑体系

核心主线：数据全生命周期闭环防护

以数据全生命周期为核心脉络，全面覆盖数据产生、收集、存储、使用、共享、传输、销毁等八个关键环节，针对每个环节制定明确且具体的安全管控要求，形成“事前预防、事中管控、事后审计”的完整闭环，确保数据在流转全过程中的安全性、完整性与可用性，实现数据安全的全流程、无死角管理。

01 技术防护支撑体系

集成核心技术筑牢数据安全防线，采用数据分级标记实现精细化管控，运用国密算法加密保障数据传输与存储安全；通过动态脱敏保护敏感信息、数据库审计监控访问行为，结合容灾备份机制，构建多层级、立体化的技术防护网。

02 管理体系保障机制

明确组织架构与岗位权责，建立健全数据安全管理制度体系；规范数据管理流程，落实数据安全责任制，明确各岗位安全职责与操作规范；完善人员管理、培训考核等机制，从制度层面为数据安全提供系统性、常态化的管理保障支撑。

03 审计监督闭环体系

强化审计监督的全流程覆盖，确保操作日志不可篡改且超长周期留存；开展风险研判，及时识别异常行为与潜在风险；实现数据操作全链路责任追溯，对违规行为精准定位、闭环整改，形成“留痕-研判-追溯-整改”的审计监督闭环。

协同效应：技术、管理、审计三大体系相互渗透、互为支撑，技术为管理落地提供工具，管理为技术应用明确规范，审计为技术与管理的有效性提供验证，共同构建稳固的数据安全防护闭环。

数据全生命周期闭环管控

新规首次将数据的**八大核心环节**全部纳入强制性管控范围，要求在数据流转的每一步都建立明确的安全措施与技术保障机制，形成“源头可溯、过程可控、结果可查、责任可究”的完整安全闭环，实现端到端的全流程治理。

基于数据分类分级的差异化防护

vinchin

分级施策：从基础防护到核心严控的全维度体系

01 一般数据（等保一、二级）

侧重基础安全防护能力的建设，重点落实身份鉴别、基础访问控制及安全审计机制，确保数据处理的合规性与可追溯性，构建数据安全的第一道防线。

02 重要数据（等保三级）

大幅提升防护强度，强制实施**加密存储、逻辑隔离与全链路数据溯源**；同时严格管控数据跨境传输行为，防止重要数据泄露与滥用。

03 核心数据（等保四级）

实施最高等级的安全管控，采用**动态组合身份鉴别与细粒度访问控制**技术，建立实时数据安全态势监测预警体系，确保核心数据绝对安全。

从“系统防护”到“数据治理”

vinchin

01. 评估体系重构：从单系统到“系统+数据”并行

等保2.0以系统安全为核心，数据安全仅为附加项；新规GA/T 2380实施“系统+数据”双独立评估。测评结论从弹性较大的百分制，升级为“符合/基本符合/不符合”的三级刚性判定，监管约束更明确。

02. 红线约束强化：重大隐患触发“一票否决”机制

新规明确33项重大风险隐患触发项，触碰即导致评估失败。数据覆盖范围从系统层面的安全控制，延伸至数据采集、存储、使用等全生命周期8个环节，实现了数据安全的全域闭环治理。

03. 技术标准硬约束：强制国密算法与日志留存升级

加密要求从“建议性”转为“强制性”，数据必须采用SM2/SM3/SM4国密算法。日志留存期限大幅提升：三级事件日志需留存≥1年，对外提供日志≥3年，确保安全审计的可追溯性。

04. 灾备机制升级：异地加密备份与独立密钥管理

灾备要求从基础的本地/本地+异地备份，升级为“异地加密备份+定期演练”，并要求密钥独立管理，从物理和逻辑层面双重保障数据的可用性与保密性，杜绝核心数据丢失或泄露风险。

三级等保系统核心技术要求

vinchin

政企单位合规建设的核心技术抓手与关键差距

01. 数据分类分级：

必须建立完善的数据分类分级制度，对系统内全量数据资产进行梳理、标记与台账化管理，精准划定重要数据和核心数据的边界范围，为后续差异化安全防护提供依据，解决数据资产“底数不清”的核心问题。

02. 审计加密与特权管控：核心数据的双重保险

重要数据存储需采用国密SM4等算法加密，对所有数据库访问行为（尤其是高危操作）全量审计留存；实现DBA等特权账号的行为可控、操作可追溯，杜绝越权访问与违规操作导致的数据泄露风险，保障核心数据全生命周期安全。

03. 敏感数据脱敏：非生产环境防护

在开发、测试、数据分析等场景中，对身份证、手机号等敏感信息实施变形或遮蔽处理，切断非生产环境下敏感数据泄露的渠道，平衡数据使用与安全保护的需求。

04. 国密算法强制化：信创合规关键

数据传输通道必须全面应用SM2/SM3/SM4等国密算法或合规安全协议，替代传统国际通用算法，构建自主可控的加密传输体系，满足信创与等保合规的双重技术要求。

三级等保系统核心技术要求

vinchin

05. 异地加密备份：物理隔离与双重加密保障

备份数据必须与生产系统实现物理隔离，满足“同城双活”（距离>30公里）或“异地灾备”（距离>100公里）的地域要求；同时备份数据本体需采用高强度加密算法存储，杜绝数据在非生产环境下的泄露风险，构建完整的容灾防护体系。

06. 审计日志管理：超长留存与防篡改技术

安全事件日志留存周期延长至**至少1年**，重要数据对外交互日志需留存**至少3年**。强制采用防篡改技术存储日志，确保日志生成后无法被篡改、删除或覆盖，为安全审计和司法取证提供可靠依据。

07. 数据销毁管控：全流程可追溯的安全销毁机制

数据达到法定或业务保存期限后，必须执行彻底的安全销毁操作，可选用多次覆写、消磁、物理粉碎等合规方式。销毁过程需建立完整的操作记录与凭证档案，确保数据销毁后不可恢复，从生命周期末端杜绝数据泄露的可能性。

vinchin

PART 02

与等保2.0的差异对比

GA/T 2380-2026 与 等保2.0 核心差异对比

01 评估逻辑重构

以系统安全为核心，数据安全仅作为附加要求；新规确立**“系统+数据”双独立评估体系**，合规重心转向数据资产本身

核心影响：从“保系统稳定”进阶到“保数据安全”，企业需重构安全建设的优先级。

02 全生命周期管控

等保2.0侧重系统边界防护，对数据流转覆盖不足；新规明确覆盖数据采集、传输、存储等全生命周期8个关键环节，无死角监管。

核心影响：倒逼企业建立端到端的数据流转监控机制，技术上需实现数据的全链路追踪。

03 结论定性刚性化

等保2.0采用百分制打分，有缓冲空间；新规实施“符合/基本符合/不符合”三级制，直接定性合规与否，无分数讨巧空间。

核心影响：测评结果更具威慑力，企业必须确保核心控制点完全达标，无法通过“凑分”通过验收。

04 33项一票否决红线

等保2.0无明确数据安全一票否决项；新规列明33项重大风险隐患触发条件，涵盖数据泄露、越权等关键场景，触碰即直接不合格。

核心影响：合规风险显著提升，任何关键安全短板都可能导致全盘合规失败，容错率极低。

05 强制国密算法应用

等保2.0仅建议性提及加密，无算法强制要求；新规明确要求核心数据必须采用国密算法进行保护，从“可选”变为“必选”。

核心影响：推动信创产业落地，企业需全面升级密码基础设施，实现国产化算法的全面适配。

06 日志留存期限升级

等保2.0要求留存6个月；新规细化分级：三级系统事件日志≥1年，对外提供服务的日志≥3年，且强调日志防篡改、防泄露能力。

核心影响：对企业的存储资源和日志管理技术提出更高要求，需建立完善的日志归档与审计体系。

vinchin

PART 03

云祺合规解决方案

创新生态，合作共赢

vinchin

数据备份

vinchin

虚拟机

整机

数据库

文件

定时备份

实时备份

普通恢复

细粒度恢复

瞬时恢复

应急接管

跨平台恢复

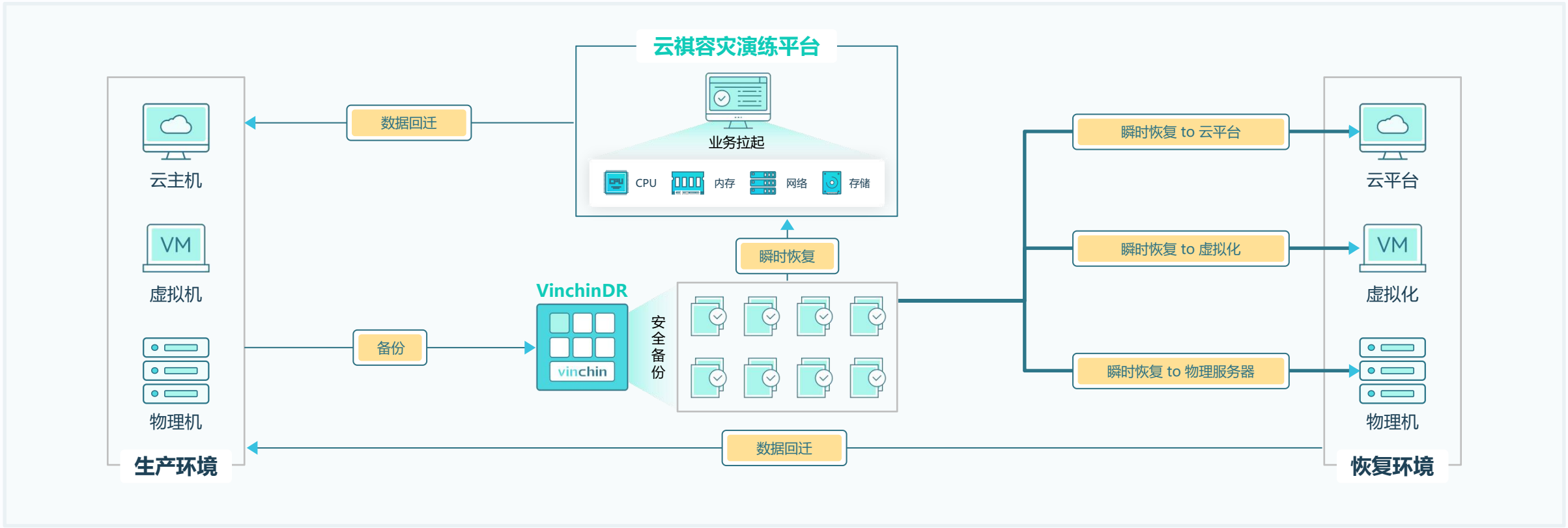
虚拟机保护	整机保护	数据库保护	文件保护	整机实时CDP保护
➢ 无代理	➢ 源端/永久增量	➢ 接口级在线热备	➢ 永久增量	➢ 断点续传
➢ 永久增量	➢ 自研一致性快照	➢ 源端压缩/重删	➢ 一致性保证	➢ 应用感知
➢ 瞬时/跨平台恢复	➢ 瞬时/跨平台恢复	➢ 支持单机/集群/分布式	➢ 权限备份	➢ 任意时间点恢复
➢ 深度有效数据提取	➢ 策略灵活	➢ 支持数据库原生能力	➢ 小文件备份加速	➢ 跨平台恢复
➢ 高性能备份	➢ 支持一体化验证容灾		➢ 海量文件备份性能优异	➢ 支持一体化验证容灾
➢ 策略完善				
➢ 支持一体化验证容灾				

• 兼容性广泛，具体以云祺产品兼容性为准

数据恢复

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

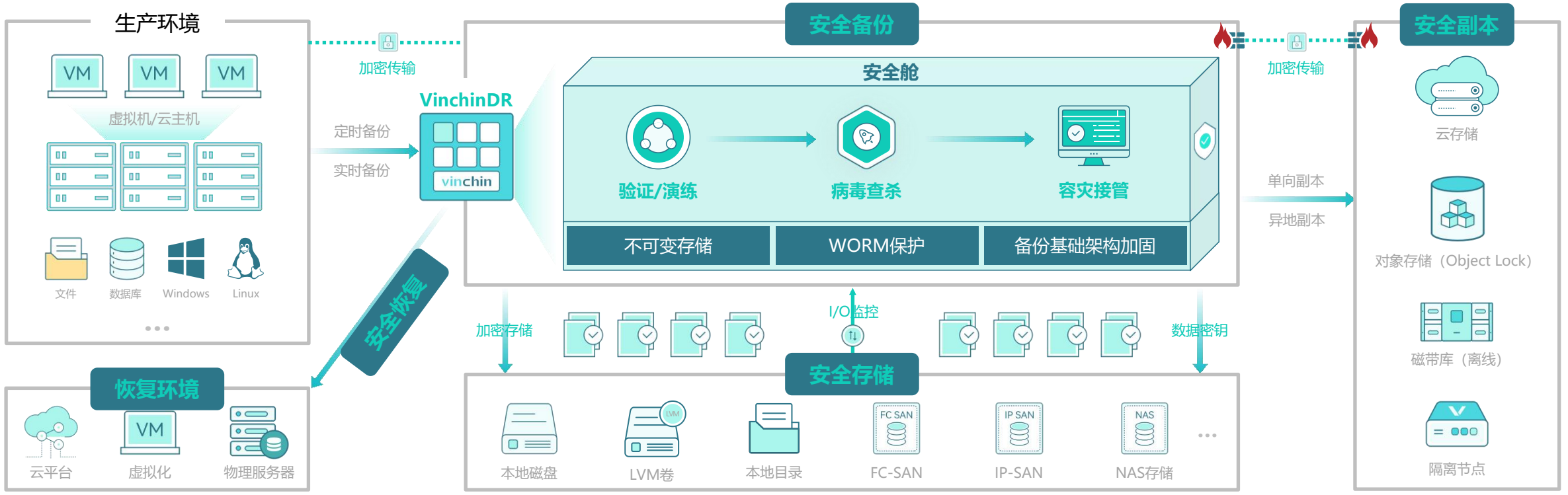
一键数据回迁

存储安全与全生命周期管理

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

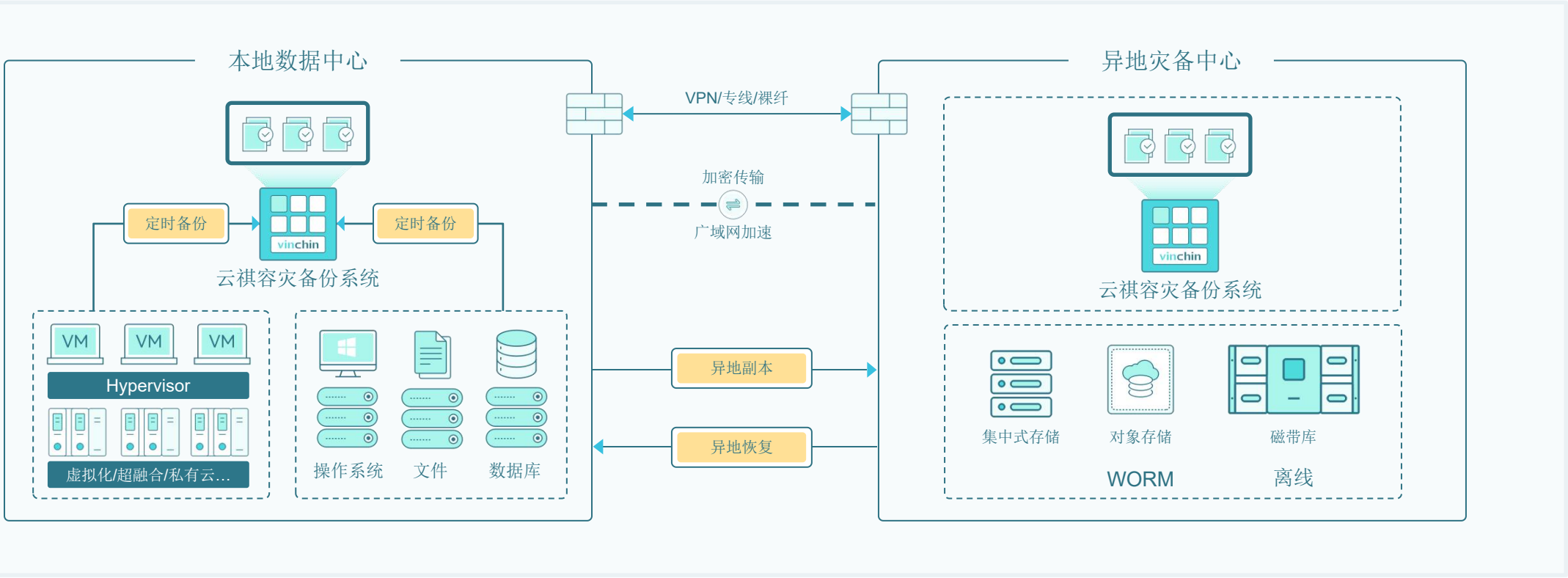
WORM 防篡改

异地副本容灾

全生命周期归档

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

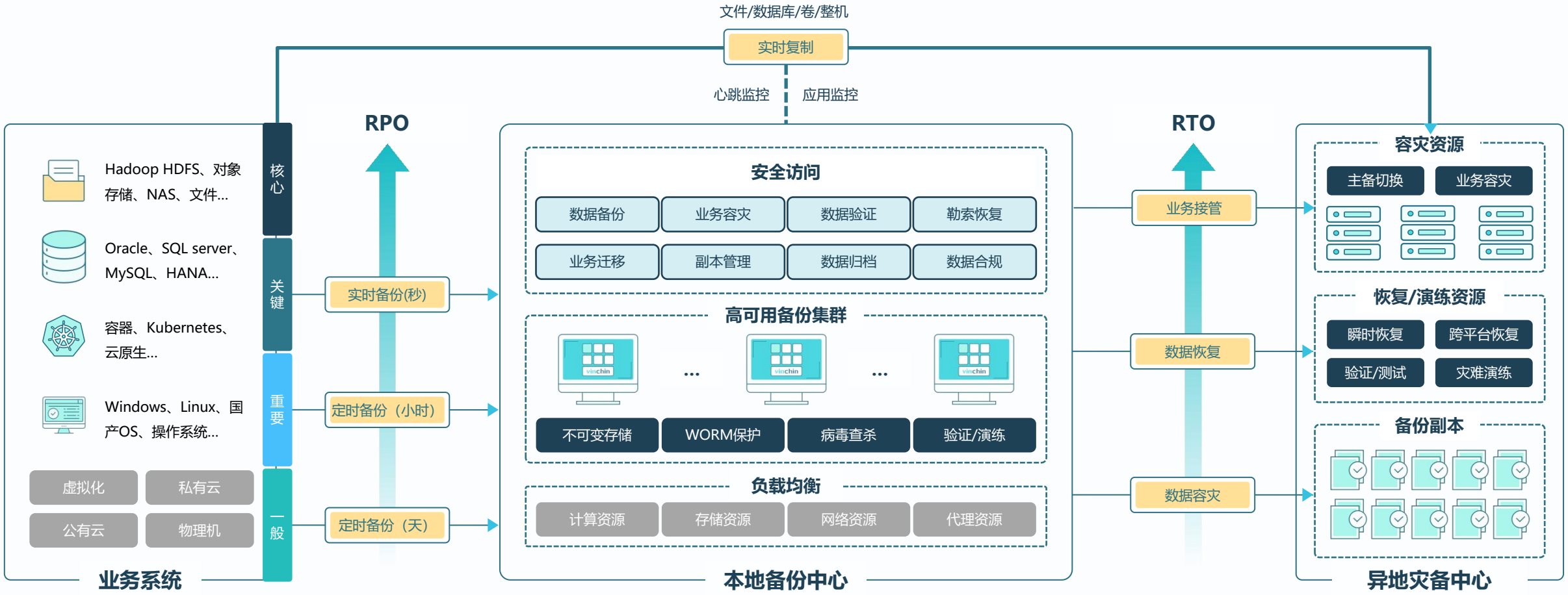
通过源端压缩、断网续传以及永久增量副本等技术适合窄带宽场景，提升传输效率。

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。

业务分级保护

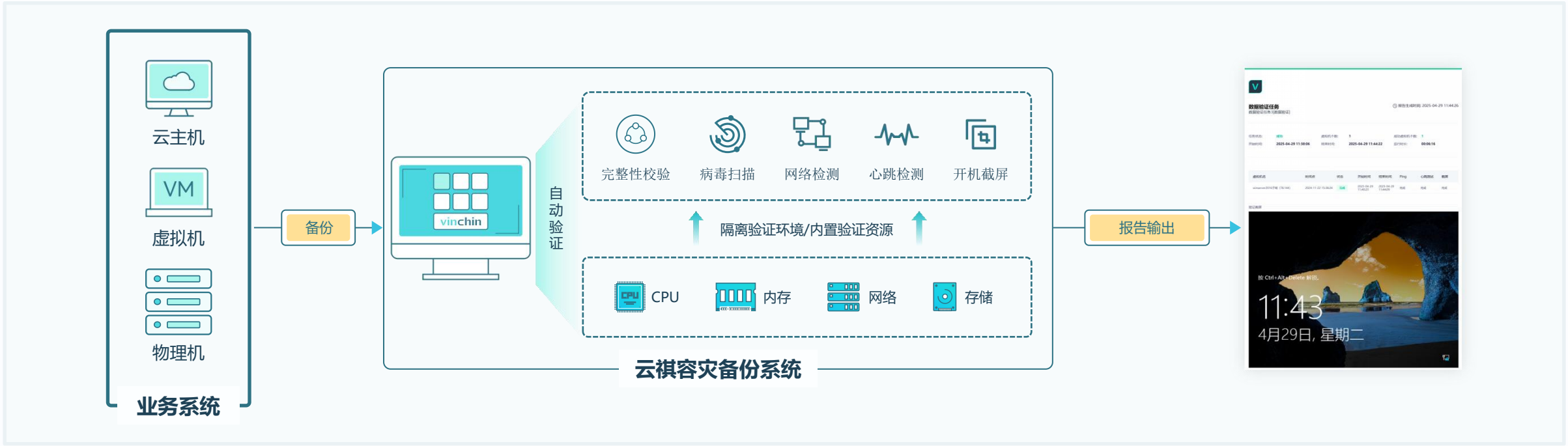
业务系统和数据的重要性各不相同，灾备建设的预算也不可能无限增长，因此不能盲目选择一揽子方案，适合的才是最好的，应当根据根据业务特点与数据重要程度选择合理的灾备方案，进行分级灾备建设，实现最佳成本控制。



验证与灾难演练

vinchin

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

vinchin

PART 04

案例分享

某市人民法院

vinchin

业务挑战：

该人民法院下属多个中级人民法院，每个中级人民法院都有数据中心，业务系统以虚拟化平台为基础设施，集中度高，功能强大，数据量大。

- 数据分散：高院及全部辖区法院数据分散，不方便统一管理；
- 业务系统庞大：150+台宿主机及500+虚拟机承载法院全部核心业务系统，数据量巨大；
- 基本的数据安全措施：采用RAID机制，确保在单个盘损坏的情况下，数据仍然有效，可用。

解决方案

某市中心医院

vinchin

业务挑战：

业务平台多

众多信息化系统都由虚拟化平台承载，平台压力大，容错能力低。

数据增量大

业务系统每日产生大量数据，对数据访问频度高。

面临风险多

医疗行业近年来频发勒索病毒入侵事件，建立安全保障机制刻不容缓。

解决方案

虚拟机整机备份

使用云祺备份整个虚拟机，备份过程中无需关机，不影响业务运行。

重复数据删除

通过重复数据删除技术，只备份虚拟机有效数据，减少备份数据量。

LAN-Free 备份

通过 LAN-Free 方式备份数据，不占用业务系统带宽，降低医院生产网络负载。

瞬时恢复

秒级时间内瞬时恢复任意备份点数据，恢复医院业务系统运行，减小业务中断风险。

多种时间策略配合

备支持多种备份模式，配合时间策略，解决业务系统数据增量大的问题。

某市中国人民银行支行

vinchin

业务挑战：

严苛金融监管合规要求

多种虚拟化平台

全区域分支行使用了多种虚拟化平台，需要一套解决方案解决多种虚拟化平台的备份。

大量数据

全区有众多分支行，业务系统24小时不间断运行，数据中心已积累了大量数据。

解决方案

永久增量与灵活策略

基于CBT技术实现永久增量备份，减少存储空间占用；支持灵活的策略配置，实现自动化、无人值守的备份任务管理。

高效无代理备份

采用无代理技术架构，无需在虚拟机内部安装代理软件，即可实现高效备份，极大简化了运维管理工作，降低了系统开销。

数据加密保护

采用高强度银行级加密算法，对备份数据进行全链路加密保护，从传输到存储层层设防，确保核心金融数据万无一失。

欢迎试用

vinchin

开放性测试

云祺容灾备份系统 V6.0

云祺 致力于持续打磨产品，不断完善现有产品能力。我们诚挚邀请您参与我们的产品试用，也欢迎您将使用后的意见或建议反馈给我们，期待云祺的产品在不远的将来能够帮助您的组织实现对数据安全的绝佳保护。

申请试用五步骤

登录官网：https://www.vinchin.cn

下载软件：云祺容灾备份系统

申请授权：在线填写信息申请试用授权

快速安装：嵌入系统，5分钟完成部署

软件试用：操作简单，10分钟熟悉软件