vinchin

安全验证先行，实现数据干净恢复

主讲人：赵琴

vinchin

目 录

vinchin

PART 01

背景与挑战

—— 备份≠恢复，恢复前验证已成刚需

有了备份就一定能恢复吗?

vinchin

“备份数据被病毒篡改加密，无法进行恢复。”

“生产数据本身就有问题，无法恢复。”

“有备份，但恢复的时候才发现数据损坏。”

“备份数据里有病毒，恢复造成二次感染。”

勒索等灾难带来业务中断风险

vinchin

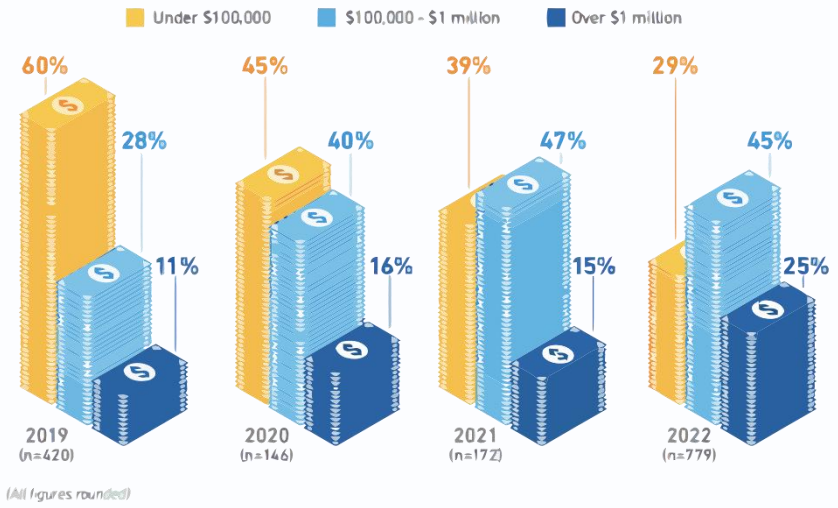
意外，正为您的业务系统带来极大的中断风险。

- **勒索攻击变得愈发猖獗：**

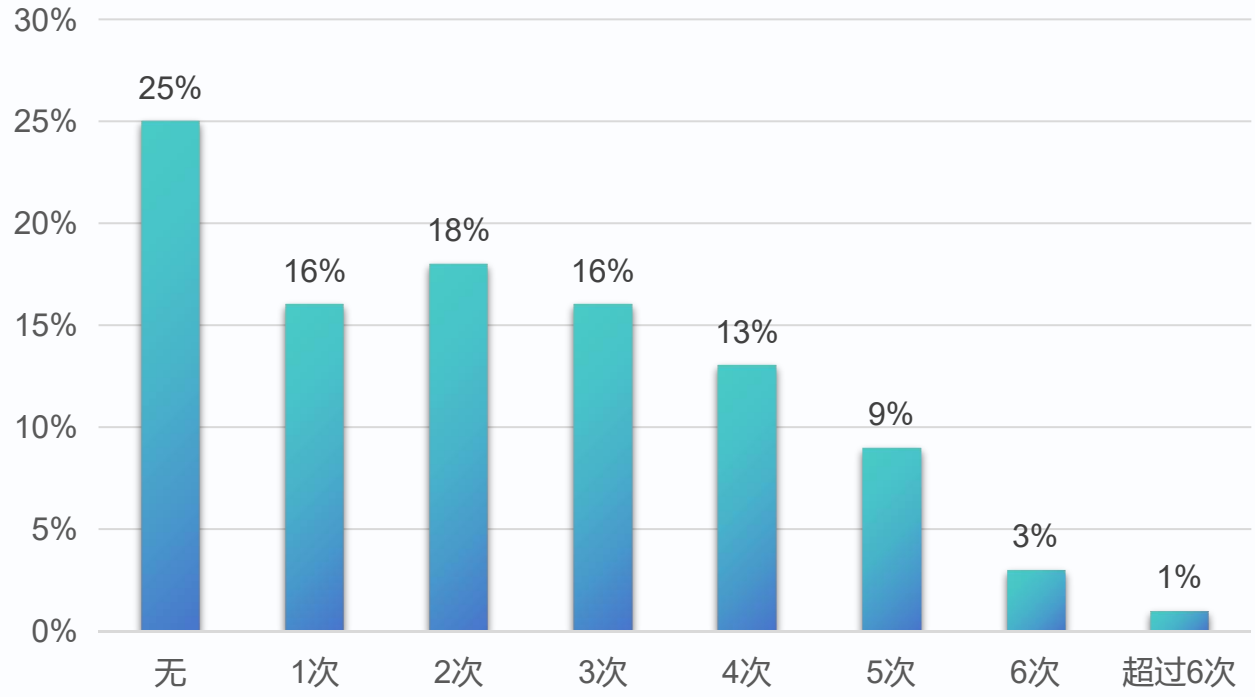
  据不完全统计，过去1年有超过50%以上的中大型企业遭受过勒索攻击。

- **其他意外所面临的数据风险不能忽视**

  除了勒索攻击以外，计算机的逻辑错误、意外灾害以及人为破坏等都是影响业务连续性所无法忽视的问题。



过去12个月所遭受的勒索攻击数量



数据源：2024 Ransomeware trends report

*25%的组织受中断造成的损失超过100万美元

数据保护与连续性要求正成为监管关注

vinchin

法律法规

- 《中华人民共和国网络安全法》
- 《中华人民共和国计算机信息系统安全保护条例》
- 《中华人民共和国数据安全法》
- 《中华人民共和国国家安全法》
- 《中华人民共和国个人信息保护法》
- 《突发事件应急预案管理办法》

行业标准

金融行业网络安全等级保护实施指引

第八条 保险机构应持续开展灾难恢复工作，以保障灾难恢复策略、灾难备份系统和灾难恢复预案的适用性。

ISPE GAMP5

验证过程中应对电子记录备份及恢复方法进行确认，确保备份数据的完整性、准确性和恢复数据的能力

工业和信息化领域数据安全管理办法

第十五条存储重要数据和核心数据的，应当采用校验技术、密码技术等措施进行安全存储，定期开展数据恢复测试。

电子病例系统应用水平分级评价标准

每季度至少进行一次数据恢复验证，保障备份数据的可用性；对于重点系统数据与系统的恢复时间不大于 2 小时，数据丢失时间不超过 1 天。

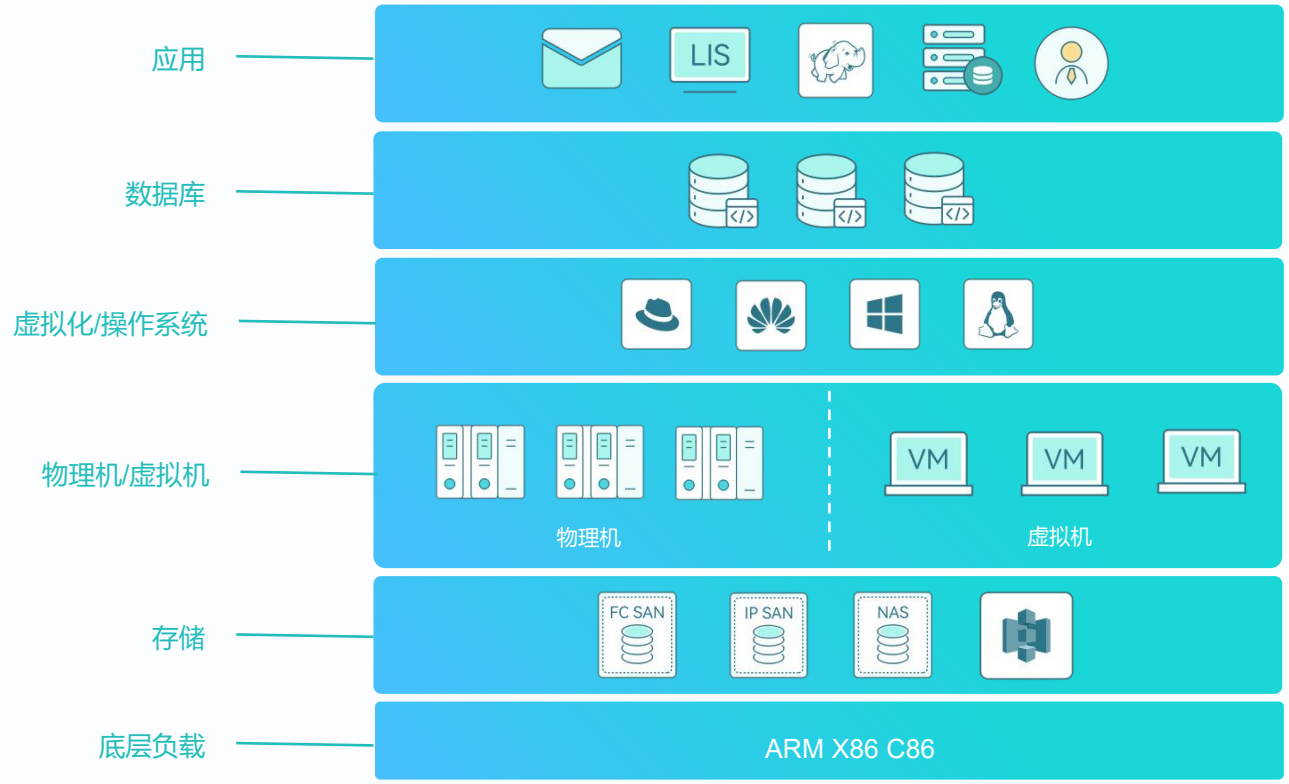
业务环境的复杂化正使传统恢复验证难度加大

伴随业务地持续复杂化与应用的升级，大规模、多类型、多层级的业务环境构成已成为常态，这在为应用与服务带来更多想象的同时，也给数据的恢复与完整性、可用性验证带来了更多挑战。

复杂性增加的重要原因：

- 终端设备、应用程序的数量和类型增多
- 多云或混合云战略的持续落地
- 业务应用的关联度快速增加
- 海量数据、多种应用负载场景的不断出现

数字化业务架构示意



传统地恢复与验证方式带来额外的负担

vinchin

无论是恢复还是验证总是伴随着诸多操作，手动执行也麻烦重重。

每次恢复或按照要求定期地执行数据验证总是伴随着操作流程与业务系统的联动，这可能需要耗费一些时间。此外，验证前对环境的配置与准备同样需要耗费大量的人力或硬件资源。

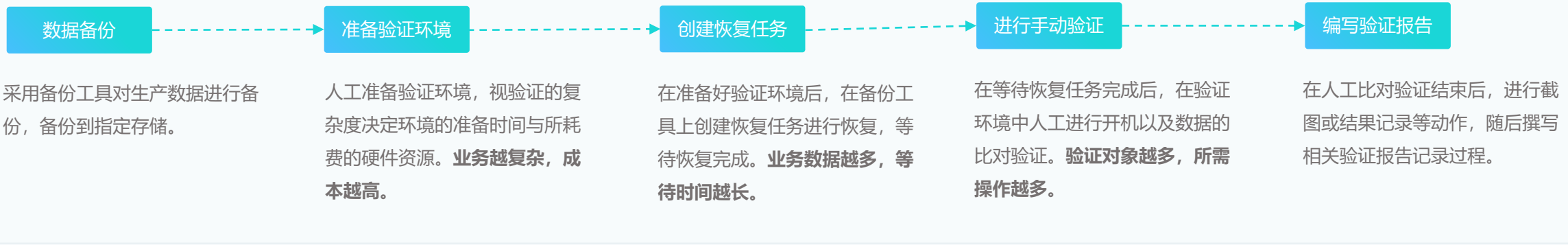
准备验证环境成本高

资源成本：基于对备份点的检查与恢复验证的需要，传统方式准备除生产以外的验证环境会带来较大的资源与成本投入。

人力成本：作为日常运维的必要操作，传统验证方式定期的备份、验证或副本等行为会为相关系统运维人员带来较为沉重的执行负担。

时间成本：传统的恢复验证方式，伴随着业务复杂度以及数据规模的持续提升，单次验证所需时间也随之大幅提升，为验证操作带来瓶颈。

传统验证方式所必需的5步：



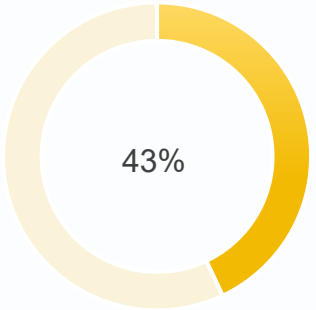
备份一定能确保干净正确地恢复吗?

vinchin

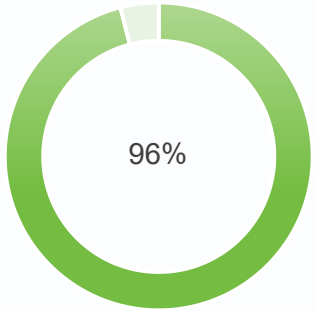
仅有备份是否可靠？在基础的备份之上，我们是否还可以做些什么?

伴随着人们对数据保护的重视程度加深，备份正成为一种共识。

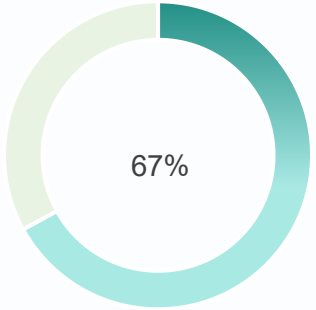
- 备份存储可能存在失效风险，导致在未来意外发生时无法得到正确的恢复。
- 备份数据可能遭受勒索病毒的攻击，备份数据存在被篡改或不安全的风险。



在遭受勒索软件攻击后，43%的数据受影响无法完全恢复

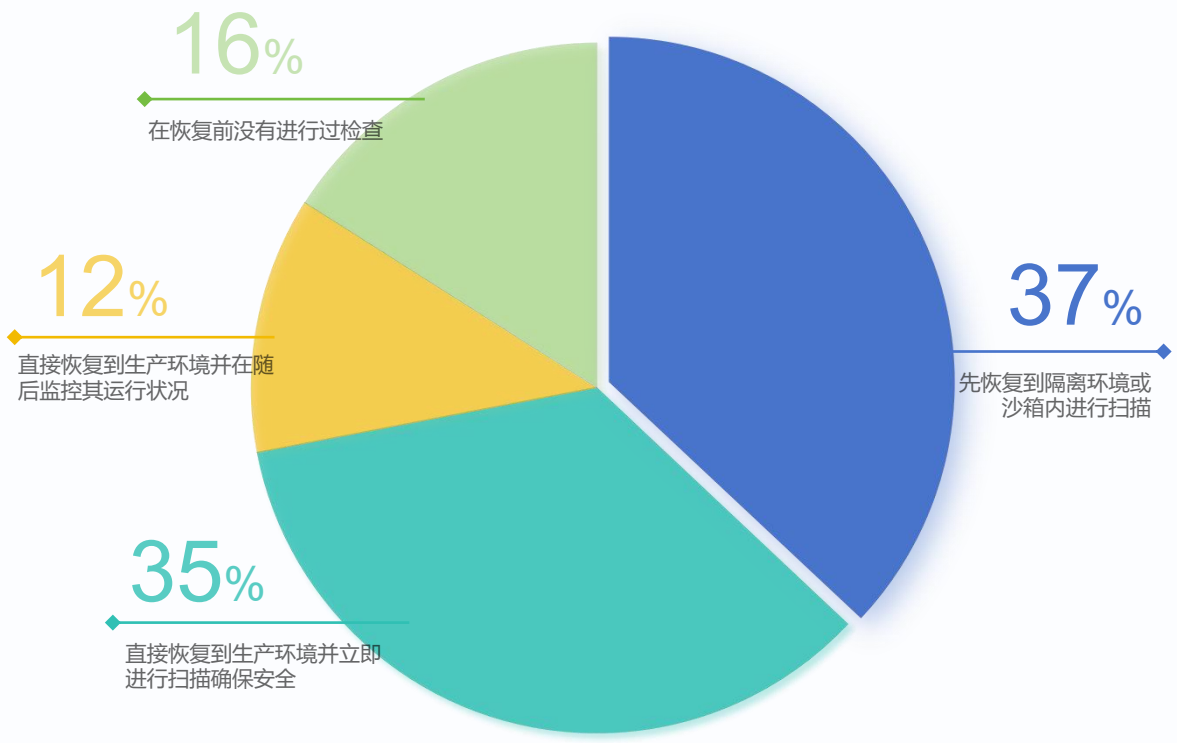


96%的勒索软件会攻击备份数据



在建有普通备份的情况下只约有67%的人获得了正确恢复

只有37%的企业在恢复前进行过验证或扫描



确保备份点的可用与安全性，恢复是目标，验证是手段。

数据验证面临的挑战

vinchin

合规监管压力大

- 监管对灾难恢复的能力与要求日益增多，执行压力日益加大
- 人工对恢复或验证过程进行记录和分析，流程繁琐且容易出错
- 灾难恢复或日常验证应遵循哪些逻辑，采取何种策略最为恰当无从知晓

人力或资源投入大

- 业务验证或恢复操作复杂，工作量大，全部依靠人力执行的难度大
- 验证资源有限，难以低成本实现针对日常备份的应急恢复演练，确保数据可用性
- 业务环境日益复杂，恢复资源多，类型多，缺乏切实可行的恢复计划，需要大量投入

验证与恢复操作执行难

- 缺乏制度性的演练要求，无法进行数据的验证
- 数据恢复后业务仍存在不可用风险，可能包含病毒入侵、恢复错误等多种意外情况
- 验证资源有限，难以低成本实现针对日常备份的应急恢复演练，确保数据可用性
- 恢复流程与业务逻辑复杂，临时恢复或验证管理混乱，难以完全按照理想状态恢复

vinchin

PART 02

核心能力

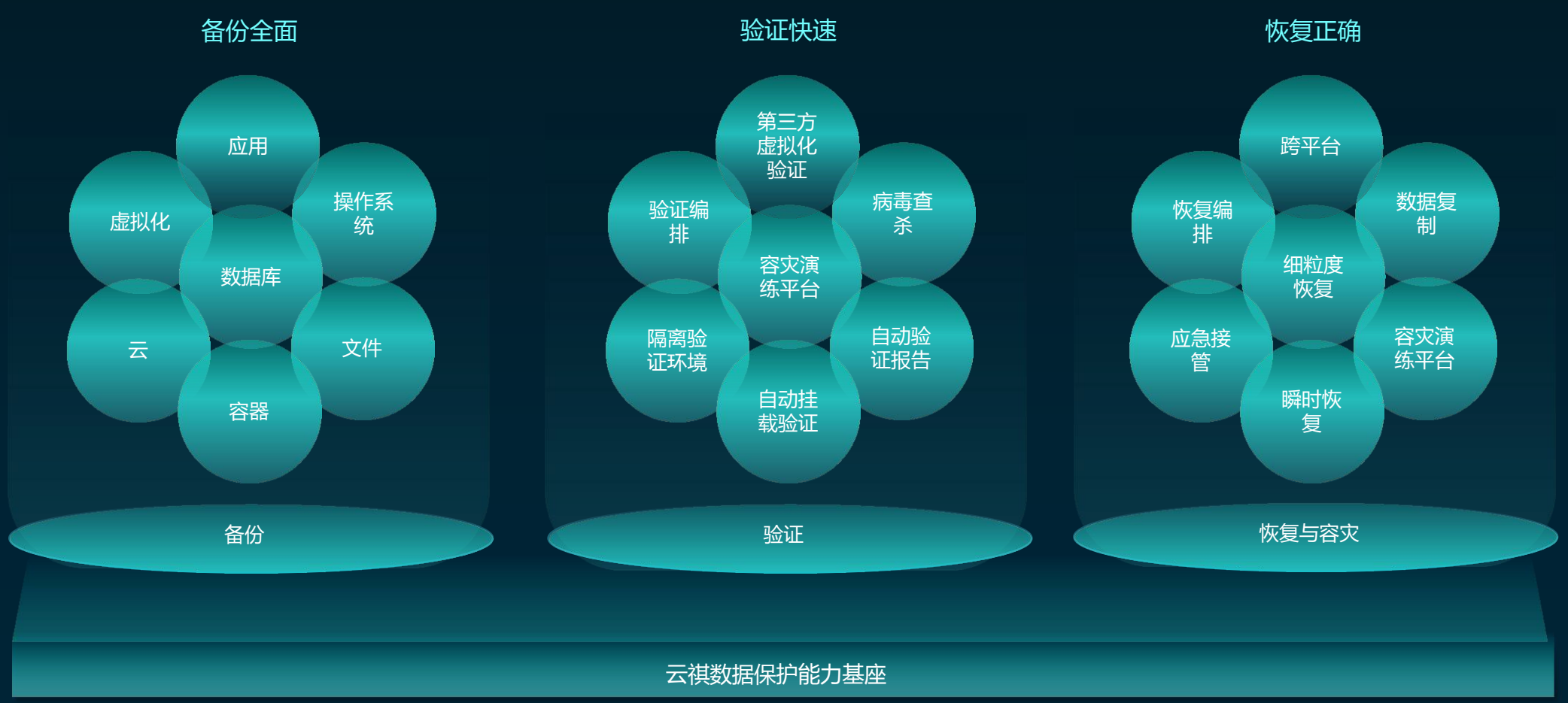
—— “内置验证+主动查杀”守护数据安全

灾难恢复与验证体系

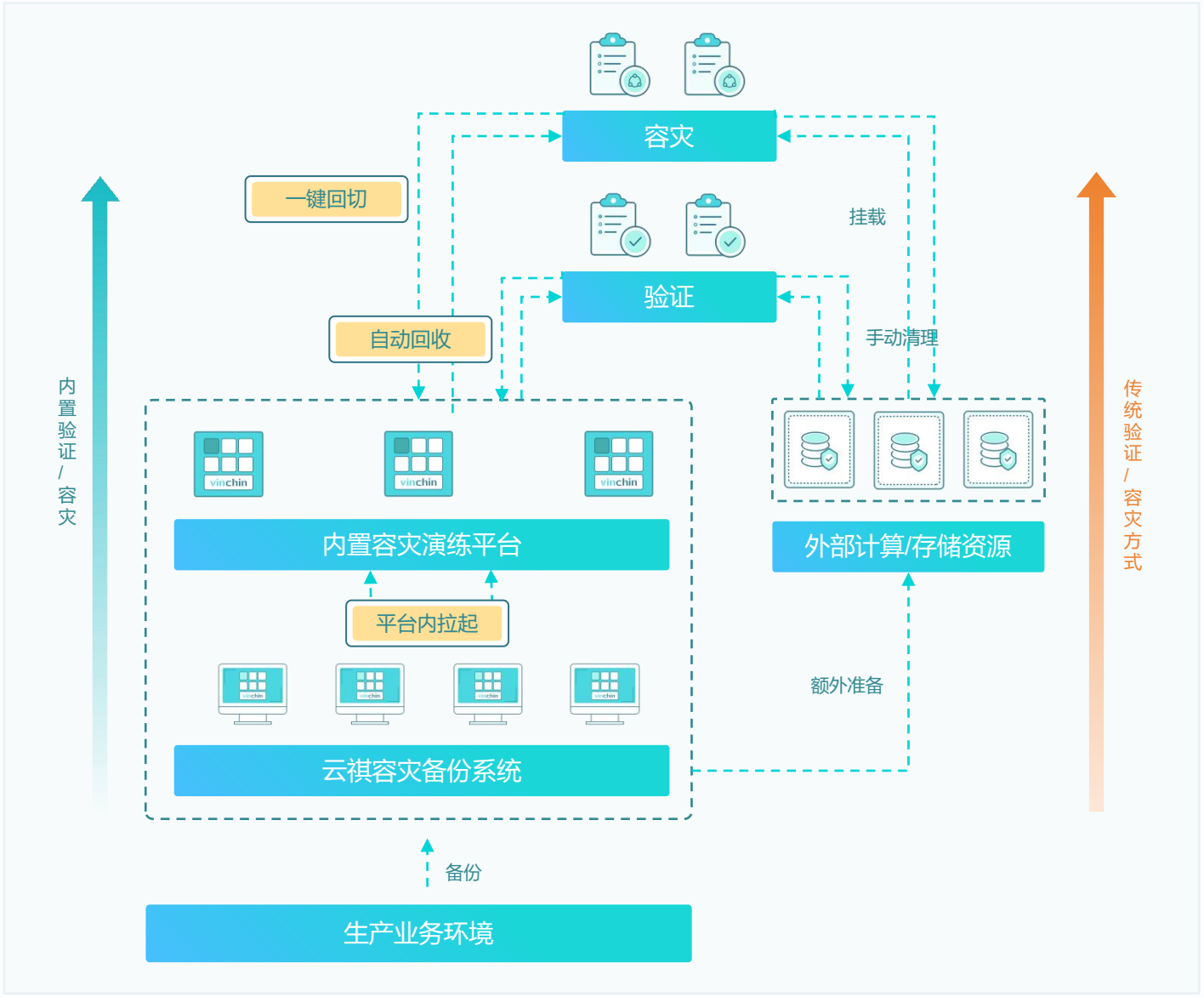
vinchin

基于保障业务快速恢复的核心原则，构建基于备份-验证-恢复与容灾于一体的灾难恢复与验证管理体系。

保证业务连续性 —— 提升灾难恢复能力 —— 减少运维与实施成本



内置验证与容灾资源



无需准备额外验证环境

内置容灾演练平台，无需准备外部验证环境，系统内即可实现备份数据验证与业务应急状态下的容灾。

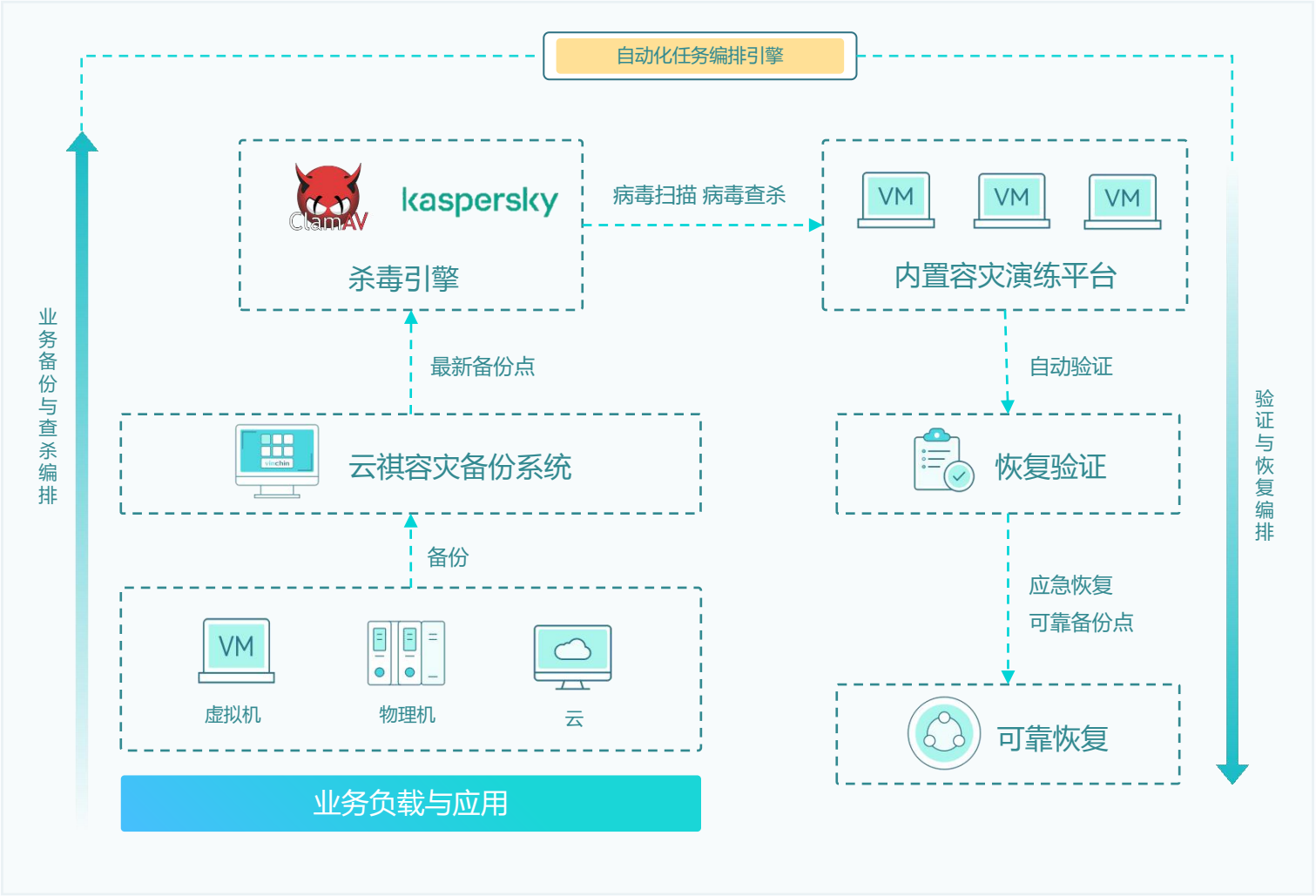
分钟级拉起验证环境

基于内置验证与容灾资源，需要时可以实现分钟级1:1拉起，快速获得验证环境进行数据验证。

多种可选的验证方式

除了内置验证与容灾平台资源，同时支持挂载或恢复到外部存储与计算资源进行演练验证等操作。

主动病毒查杀



主动式病毒查杀

在备份完成后或进行恢复前主动进行病毒查杀，相较于在遭受勒索后的被动行为，具有更加显著的预防意义。

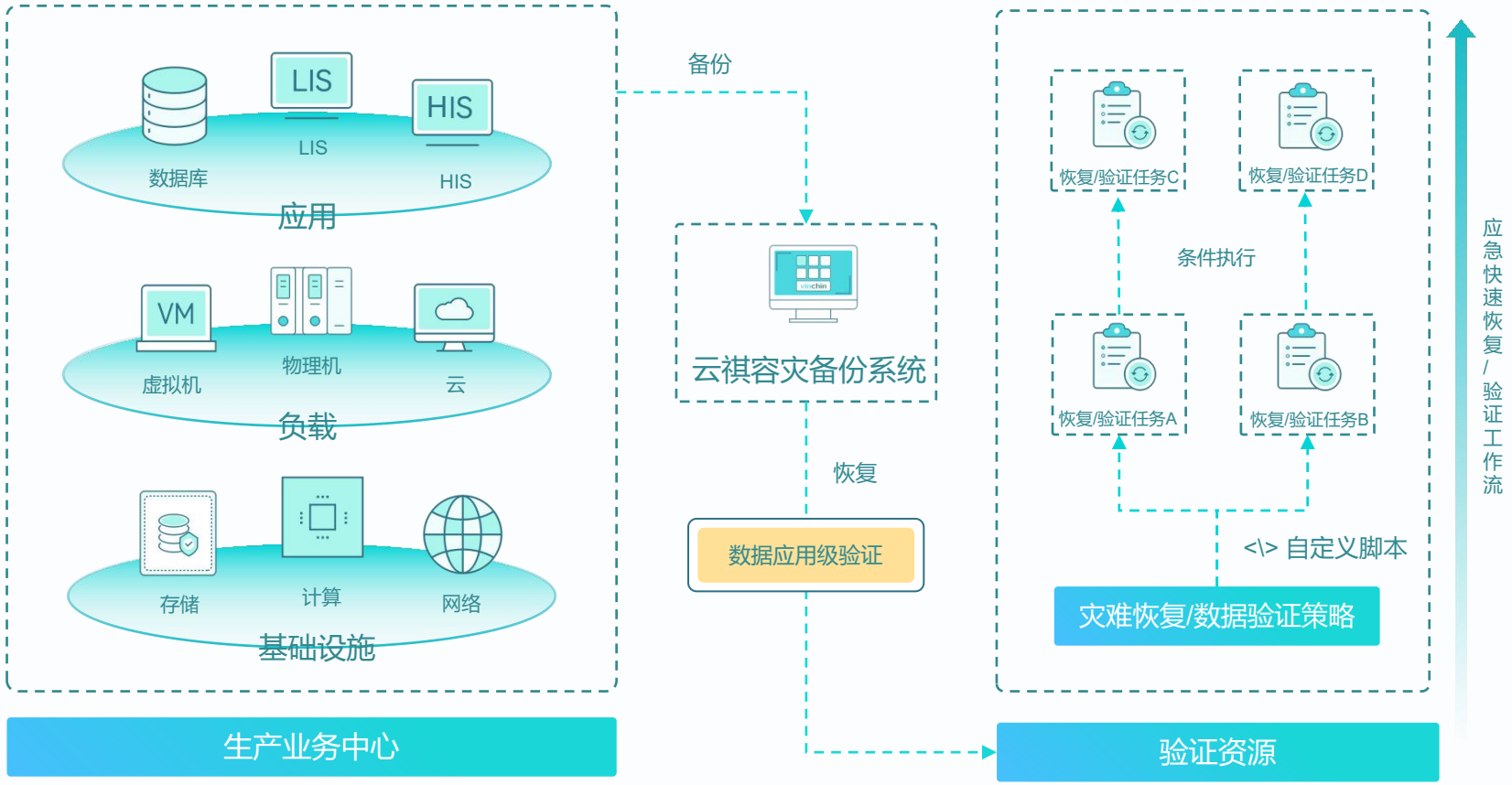
内置杀毒引擎

系统内置ClamAV与Kaspersky杀毒引擎，通过SDK方式集成，区别于传统挂载方式杀毒更加方便与快捷，同时更加安全。

获得干净的恢复

通过依赖可信的杀毒引擎进行主动式病毒查杀，在进行验证等操作后获得干净的恢复。

应用级验证与应急恢复



应用级数据验证

通过在恢复后执行自定义脚本，实现针对数据库等应用的数据验证。

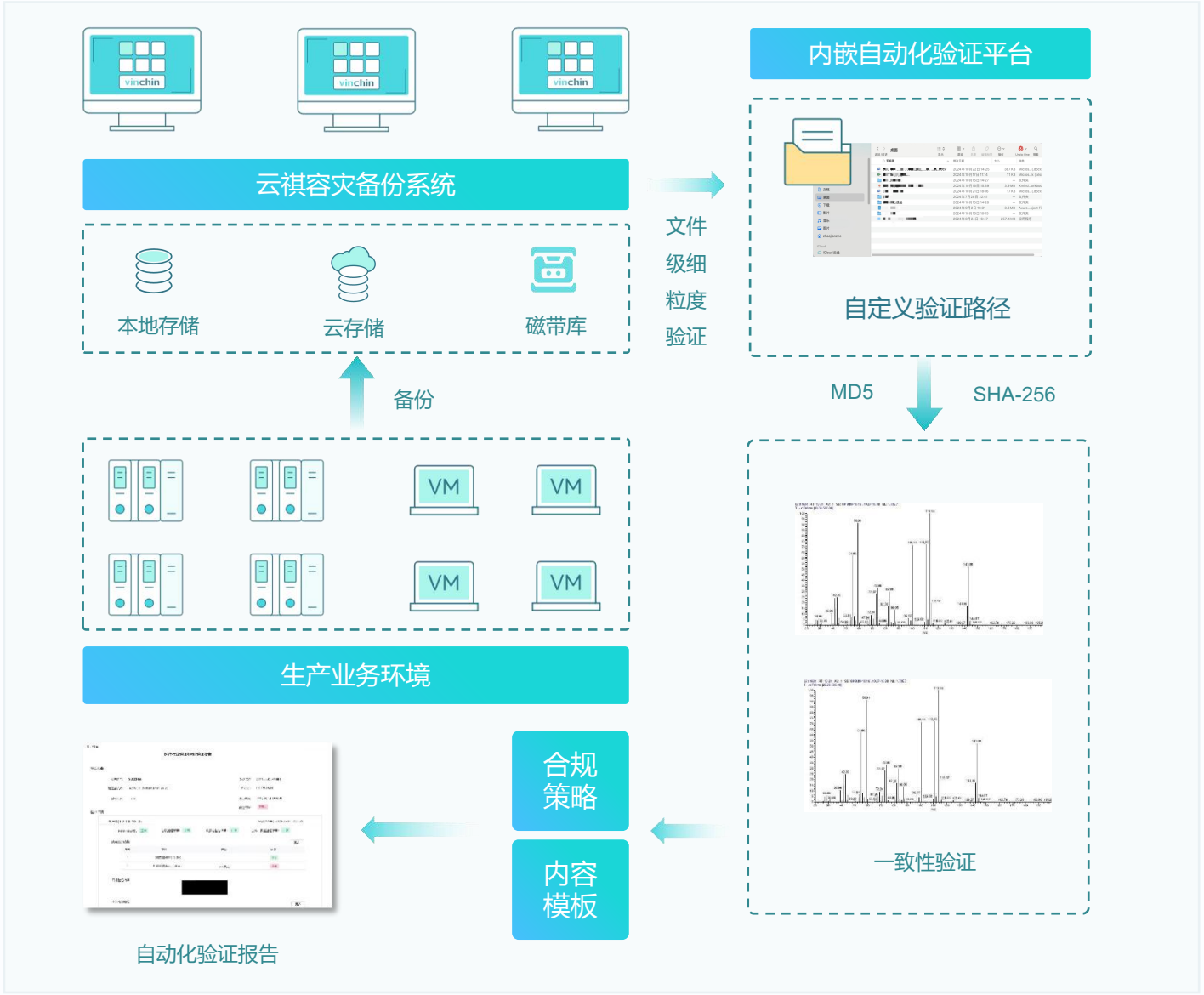
应用组验证

构建符合业务关联的应用为应用组，快速统一进行拉起，并在此基础上进行验证操作。

可供编排的应急恢复

结合任务编排，实现针对不同业务系统特点执行的多样化恢复方式，在意外情况下一键执行恢复。

文件级数据一致性验证



文件级细粒度验证

支持按实际需求进行文件级细粒度验证，避免传统方式因大面积恢复带来的存储或等待浪费。

可靠的验证算法

采用可靠的比对算法，快速实现文件级数据一致性比对，快速获取比对结果。

字段级自定义验证报告

用户可根据自身业务需要自定义数据一致性验证报告内容，通过拖拽字段方式最大化自由度支持多种应用场景需求。

vinchin

PART 03

典型应用场景

——多行业适配，合规落地干净恢复

医疗行业数据验证

vinchin

医疗行业的验证要求

《全国医院信息化建设标准与规范》

医院信息化系统应确保数据的安全性和可靠性。同时，要对备份的数据进行定期检查和验证，确保备份数据的完整性和可用性，避免因数据损坏或丢失导致的信息丢失风险。

《电子病例系统应用水平分级评价标准》

每季度至少进行一次数据恢复验证，保障备份数据的可用性；对于重点系统数据与系统的恢复时间不大于 2 小时，数据丢失时间不超过 1 天。

医疗行业的核心痛点

数据本身的验证无法保障

医院的HIS以及EMR这些系统，验证的一个核心是连续性问题，另外也要注意数据的完整性问题，传统的恢复验证方式在检验数据完整性上存在障碍，很麻烦。

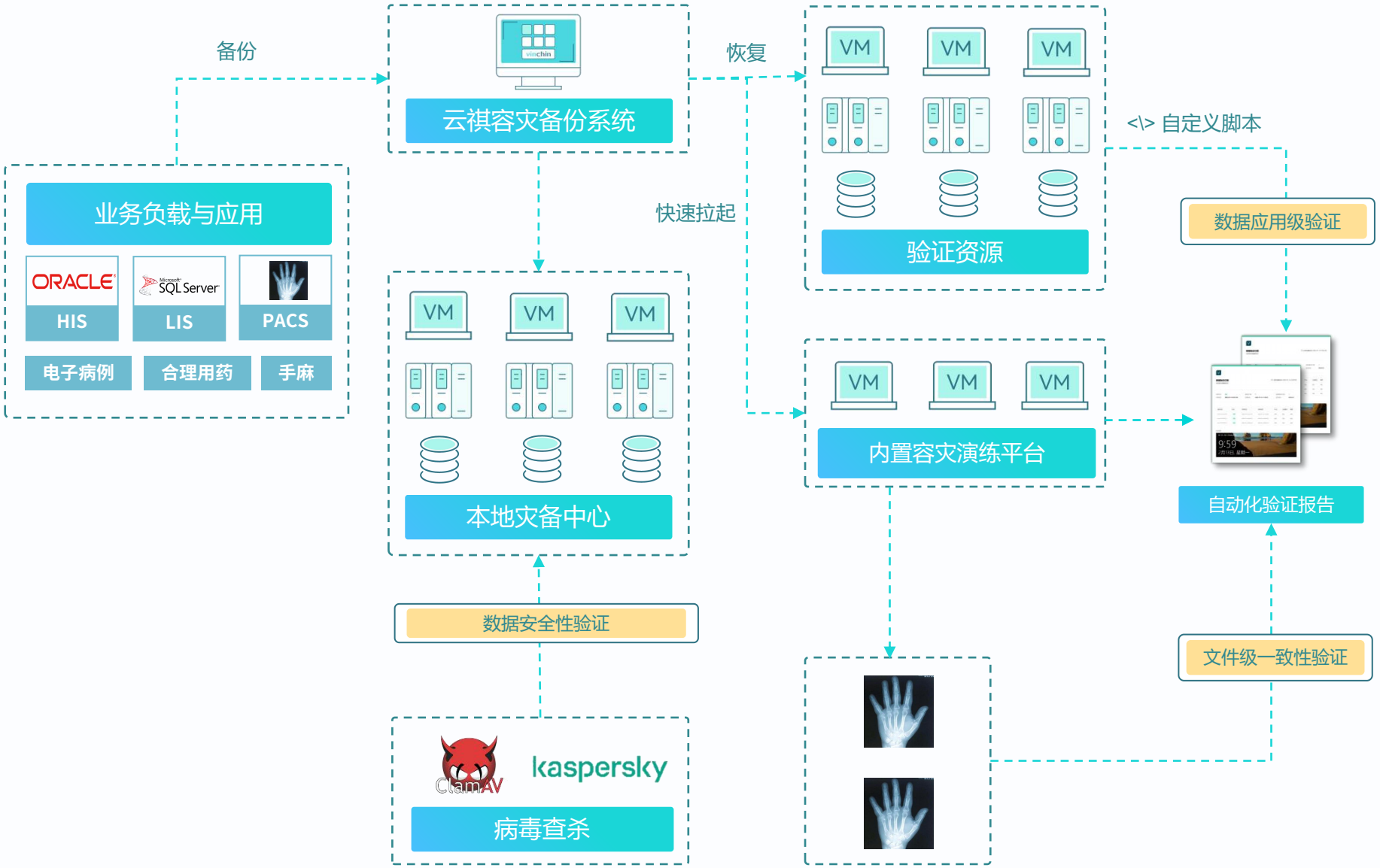
具有代表性的验证系统

- **针对HIS、EMR的验证**

医院的HIS与EMR（电子病历）系统，作为医院的核心业务系统，其通常是验证的重点。HIS底层通常由数据库支持，需对其数据库进行验证。同样，也需要针对性对其数据的完整性可用性进行验证。

医疗行业数据验证

vinchin



满足电子病例评级

不仅仅是备份，同时支持内嵌环境下进行数据验证等操作，满足电子病例的备份与定期验证要求。

实现针对数据的验证

针对结构或非结构化数据，可以针对不同的数据类型实施不同的验证，通过完整性验证、杀毒等保障完整性与安全性。

日志永久保留

医疗行业追求强合规驱动，备份系统内的所有关键操作都会被记录，同时支持永久保留，不可删除。

政务云数据验证

vinchin

政务云的验证要求

政务云的数据验证来源于实践

对于政务云而言，其并没有像医院那样有明确地数据验证要求，但从政务云所拥有的特殊性以及实践要求来讲，其需要定期进行数据验证，并且也有一定的特点。

具有代表性的验证对象

- **针对业务系统的验证**

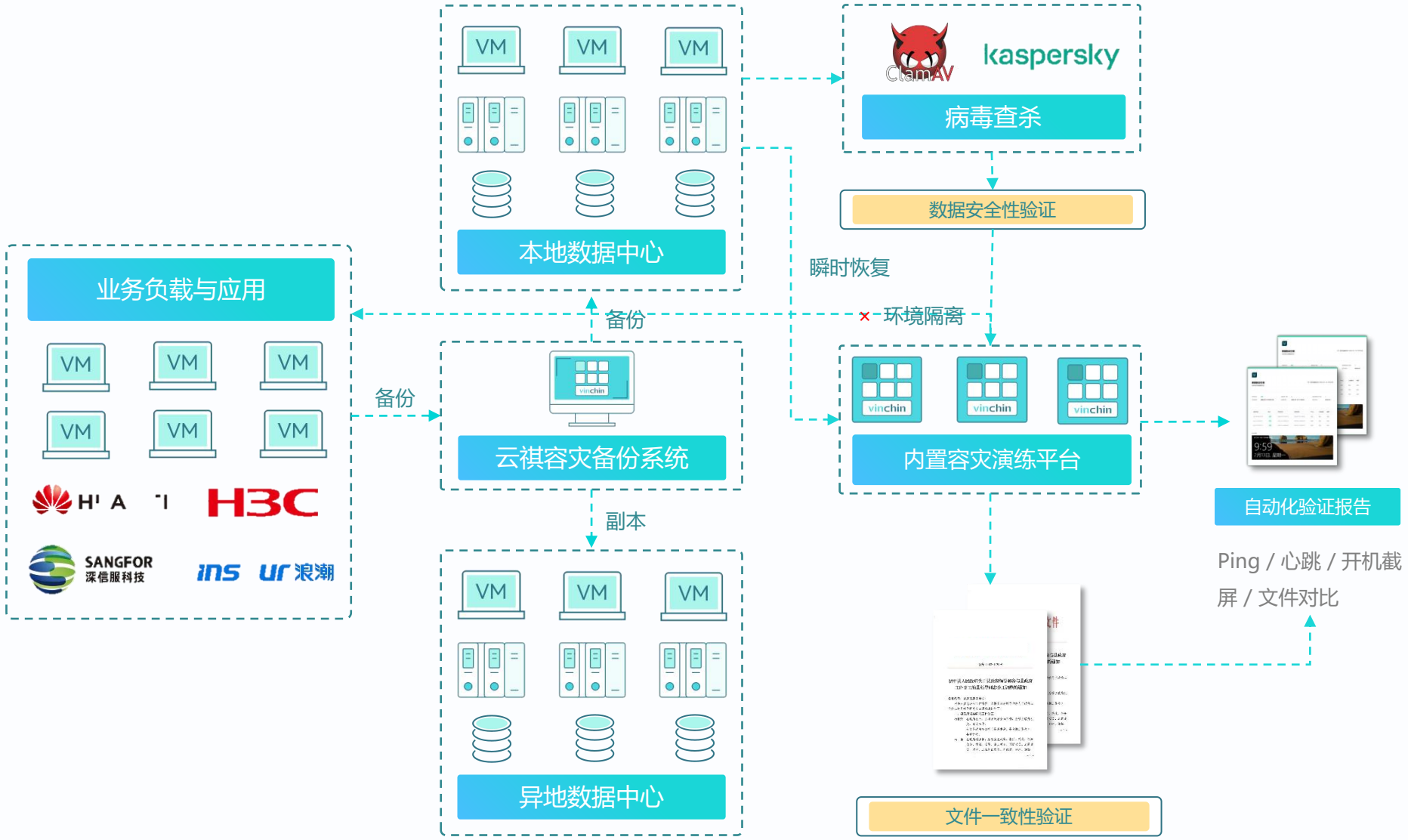
政务云的很多业务都由虚拟化向外提供服务，对虚拟机做验证是政务云场景下验证一个非常重要的动作。

政务云的核心痛点

验证规模大，耗费人力物力

政务云的特点就是其拥有较大的业务规模，上千台虚拟机都是十分普遍的，这意味着即使每次选择一部分机器进行验证，也会带来非常大的压力。

政务云数据验证



实现海量虚拟机场景下验证，节省成本并提升效率

政务云通常需定期进行部分机器的恢复验证，通过内嵌验证平台可进行快速的批量数据验证，提升效率的同时节省资源与时间成本。

快速应对数据本身的验证，防范勒索

通过数据的完整性验证以及内置杀毒引擎，快速了解数据的完整性与安全性情况，并进入报告。

自定义自动验证报告，覆盖更多留痕场景

支持自定义报告模板，在验证动作完成后自动进行输出，快速合规并留痕。

金融行业数据验证

vinchin

金融行业的验证要求

《金融行业网络安全等级保护实施指引》

保险机构应持续开展灾难恢复工作，以保障灾难恢复策略、灾难备份系统和灾难恢复预案的适用性。

《证券期货业网络和信息安全管理办法》

核心机构和经营机构应当每季度至少对数据备份进行一次有效性验证，并建立灾难备份设施确保业务连续运行。

金融行业的验证特点

业务系统多，验证成本高

银行、券商等金融机构里拥有各式各样的业务系统，按照强制要求进行验证，传统方式会花费大量的资源与人力成本，同时耗费时间。

对数据本身的验证要求高

金融行业的数据完整性、安全性关乎到资金往来等重要信息，所以也是验证本身的重点环节，应当予以保障。

具有代表性的验证对象

- **针对支付清算系统、资金管理系统的验证**

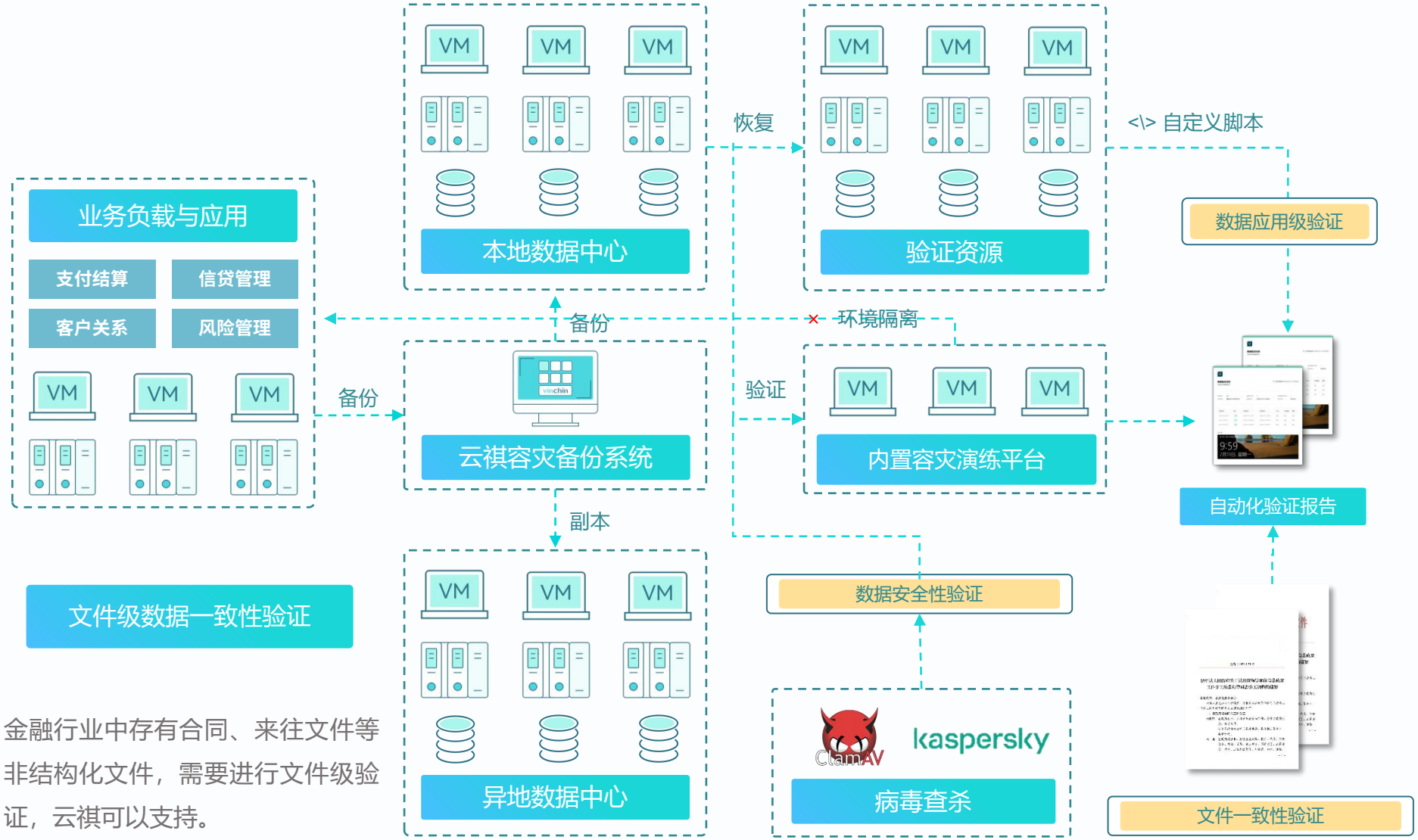
银行等金融机构的核心业务系统，包括支付清算、资金管理等对数据读写要求高，结构化特征显著的应用通常底层由数据库进行支持，验证时也需要进行针对性验证。

- **针对电子合同管理系统、客户服务与工单系统、影像管理系统的验证**

同样，金融机构拥有非常复杂的业务管理系统，大量数据也用于其合同管理、客户服务以及资料留存等业务环节，同样需要定期验证数据的有效性。

金融行业数据验证

vinchin



金融行业中存有合同、来往文件等非结构化文件，需要进行文件级验证，云祺可以支持。

支撑数据库的定期验证，提升验证效率

金融行业很多业务系统底层都由数据库做支撑，针对数据库做验证很重要，同时基于内嵌验证也可以提升整机方式的验证效率。

针对数据的完整、安全验证

金融行业的诸多业务其所包含的数据类型与支撑负载不一，通过整机、应用级到文件级的多种验证能力，构建更加完善的体系。

自定义验证报告，构建多样的合规表现

金融行业作为强合规驱动，支持自定义报告模板，在验证动作完成后自动进行输出，快速合规并留痕。

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

vinchin

vinchin

THANKS

云祺公众号

云祺视频号