vinchin

备份存储减负指南
一套全周期管理方法

vinchin

目 录

vinchin

PART 01

备份数据的缩减

备份数据的缩减

vinchin

时间策略

不同业务级别
按照业务数据增长快慢
存储资源特别紧缺，永久增量

存储策略

重复数据删除
存储压缩及压缩等级

保留策略

不同业务级别
不同等保要求
GFS长期保留

不同备份模块

对于数据库只备份专门的业务实例，备份可以采用完备+日志备份
虚拟化备份和整机备份可以仅备份操作系统和业务数据所在磁盘，其他磁盘如存放自备份数据或不太重要的数据，可以排除备份
实时备份对于RPO要求不高的，可以将调整存储块大小

vinchin

PART 02

备份数据安全防护

勒索病毒攻击流程

vinchin

探测侦察

搜集基础信息

网络信息
主机信息
身份信息

寻找攻击入口

系统漏洞
弱口令
高危端口

攻击入侵

部署攻击工具

MetaSploit
CobaltStrike
RDPOverTor

获取访问权限

远程桌面入侵
明文凭据
密钥保管库
身份认证信息

病毒植入与扩散

植入勒索病毒

执行恶意脚本
修改注册表
混淆文件信息

获取管理权限

滥用特权账户
修改域策略
关闭安全软件

病毒横向扩展

渗透工具
WMI与PsExec
蠕虫复制

甄别重要数据

文件命名
文件格式
关键词检索
知识产权/财务

实施勒索

破坏备份数据

删除VSS
清理可还原点
破坏备份工具
破坏备份存储

加密/窃取数据

遍历文件
加密文件
回传重要数据
删除原始文件

完成勒索

清理攻击痕迹

删除日志
清理访问记录
覆写系统文件
销毁密钥

加载勒索信息

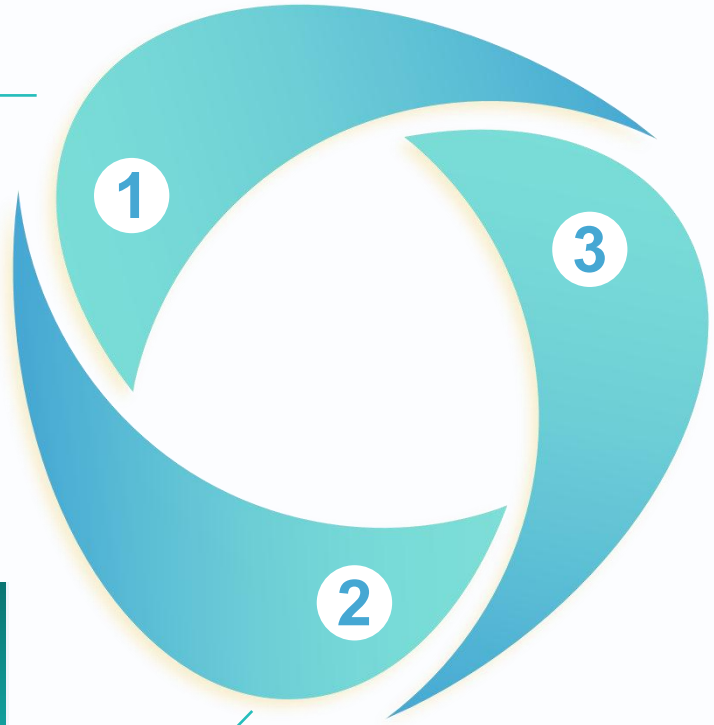
勒索弹屏
勒索信息文件
联系方式
付款地址

安全——全流程业务防勒索体系

vinchin

事前预防

- 自动化数据验证：系统内备份数据完整性与可用性验证并报告
- 安全体系构建与能力培训：基于3-2-1-1-0-0原则为用户提供安全建议，构建合理的数据保护框架



事后溯源与提升

- 操作与行为日志：系统内对相应操作进行记录，便于进行风险操作溯源
- 风险分析与取证：基于攻击路径帮助用户进行风险分析，同时协助用户进行攻击行为取证

事中恢复

- 瞬时恢复：领先的瞬时恢复技术，在遭受勒索后可以在分钟级进行快速数据恢复，保障连续性
- 病毒查杀：结合第三方杀毒引擎执行恢复前病毒查杀，确保恢复后数据安全性

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

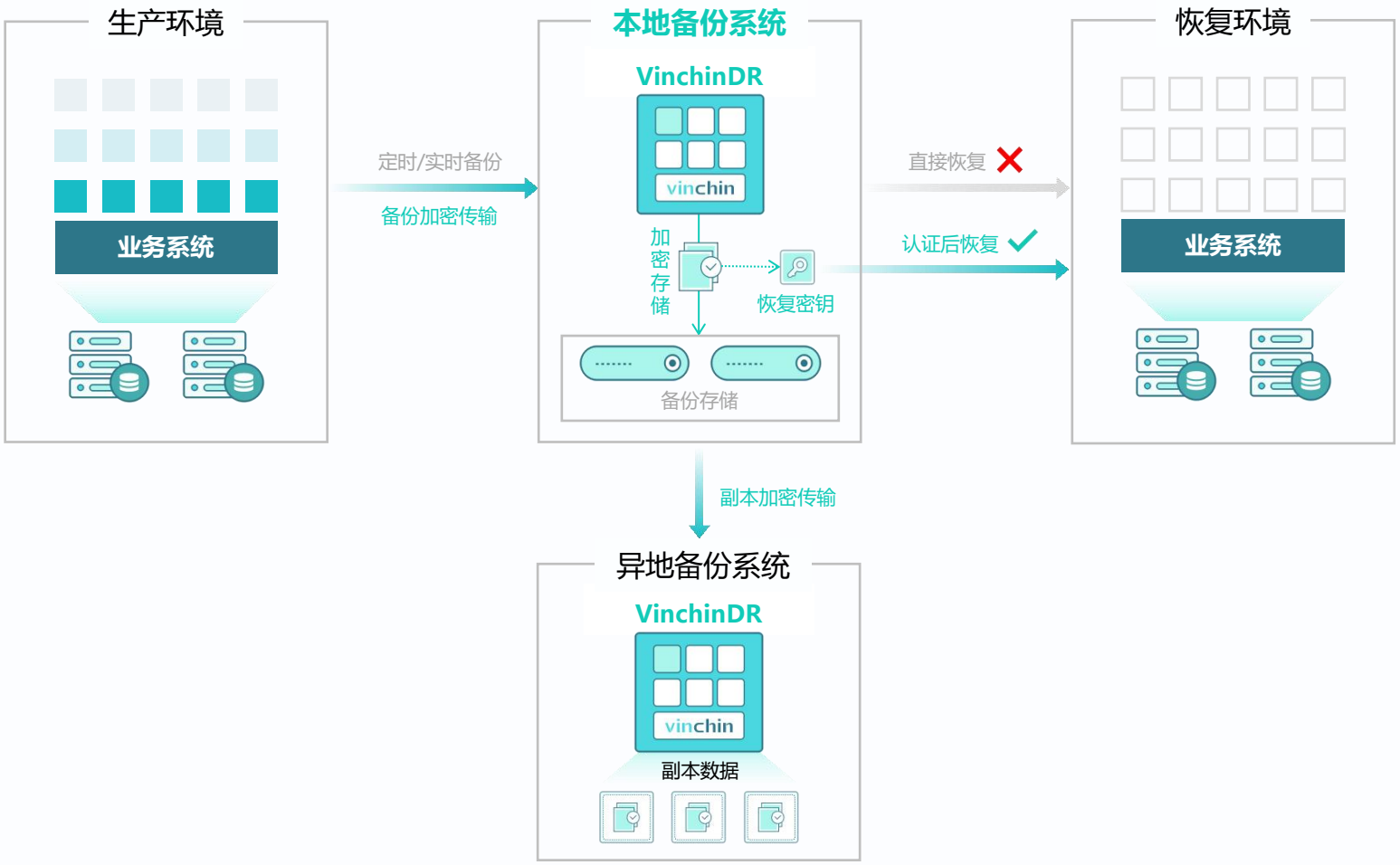
0

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

端到端加密，防止数据泄露

vinchin

黑客可能从备份传输链路抓取数据或通过泄露的root登录凭据进入备份系统底层实施数据窃取，因此对备份（包括数据传输和备份数据本身）进行加密有助于增强勒索病毒防护能力。



加密传输

对传输链路进行加密，防止恶意软件通过抓包截获明文数据，支持RSA/SM2等加密算法

加密存储

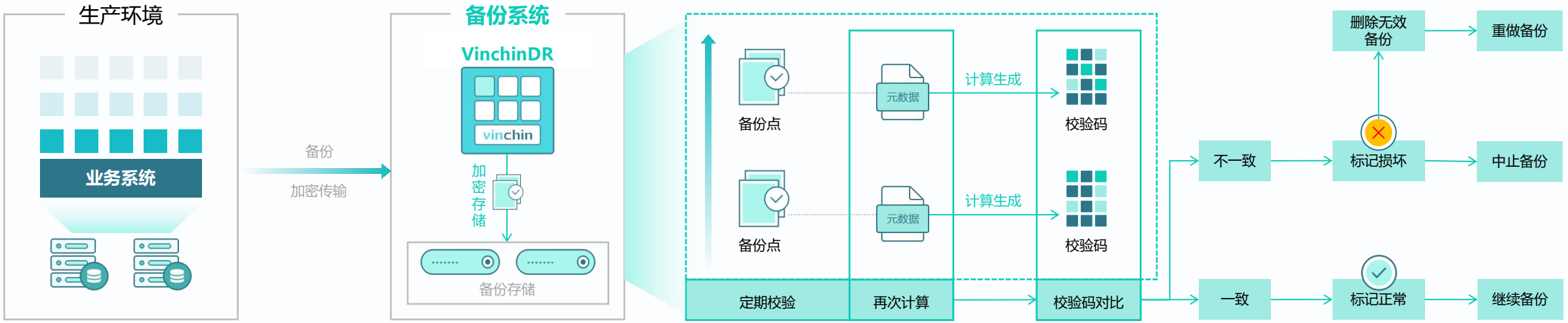
将数据加密后再写入到存储介质，防止恶意软件通过泄露的root账号密码从后台窃取明文数据

恢复密钥

支持对备份数据设置恢复密钥，恢复时将验证密码。防止恶意软件通过非法恢复窃取明文数据

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

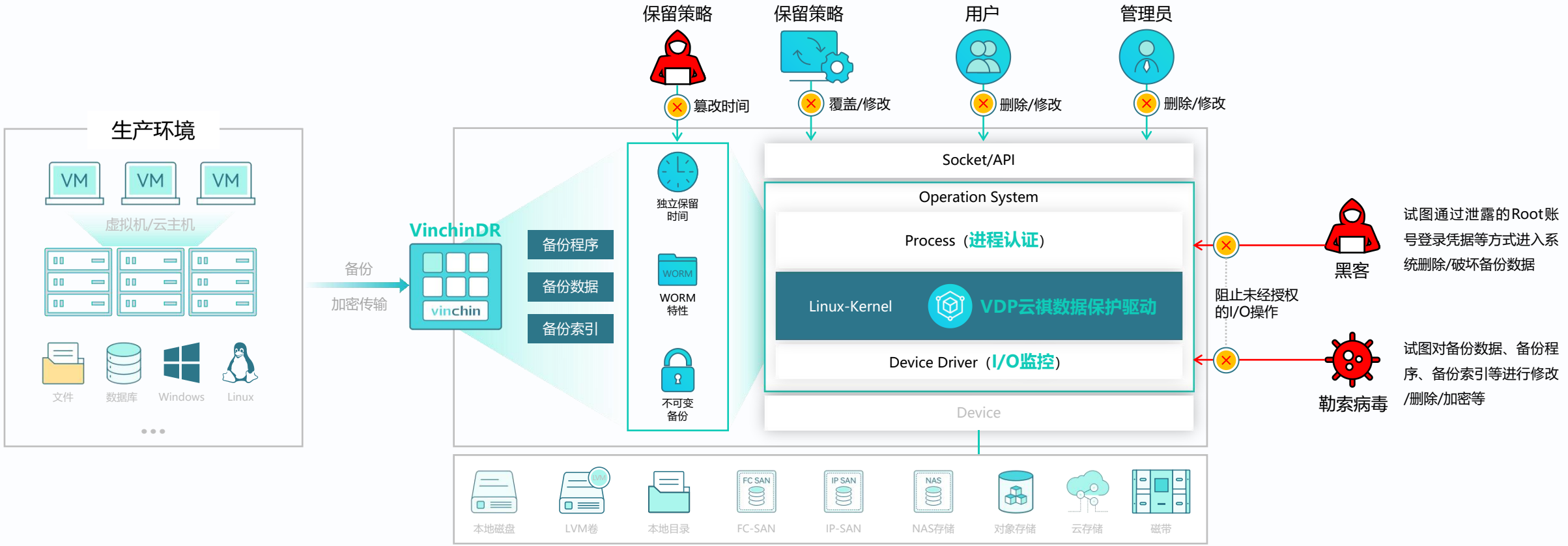
高效校验

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

不可变存储，以不变应万变



勒索防护：内核级防勒索加固，阻止恶意软件从后台破坏备份程序、备份数据、备份索引等关键数据和组件

进程认证：进程必须经过认证才可进行存储I/O操作，实时监控后台进程，第一时间阻断异常行为

不可变存储：使用原生不可变存储或对象存储Object Lock、物理磁带离线存储等实现备份数据不可变特性

WORM保护：保留时间独立计算，防止root账户、备份管理员非法删除、篡改备份数据以及NTP时钟攻击

多层安全加固、零信任访问

vinchin

管理员
用户

访问/验证/鉴权/审计

业务系统

第三方
集中管理平台

AAA安全访问架构

身份验证（Authentication）

- 增强账户安全
- 唯一访问密码
- 访问控制（IP）

访问授权（Authorization）

- RBAC
- 最小化权限
- 用户资源隔离

活动审计（Accounting）

- 三员管理
- 完整日志记录
- 永久保留日志

APikey

加密通信（TLS）

API校验

灾备服务

- 备份
- 恢复
- 容灾
- 验证
- 副本
- 归档
- 迁移

灾备资源

- 备份数据
- 元数据
- 备份程序
- 备份节点
- 存储资源
- 网络资源
- 灾备对象

灾备系统加固

- 服务精简
- IO监控
- 异常操作拦截
- 防火墙配置
- SSH配置
- 端口控制
- 更新升级

SIEM系统

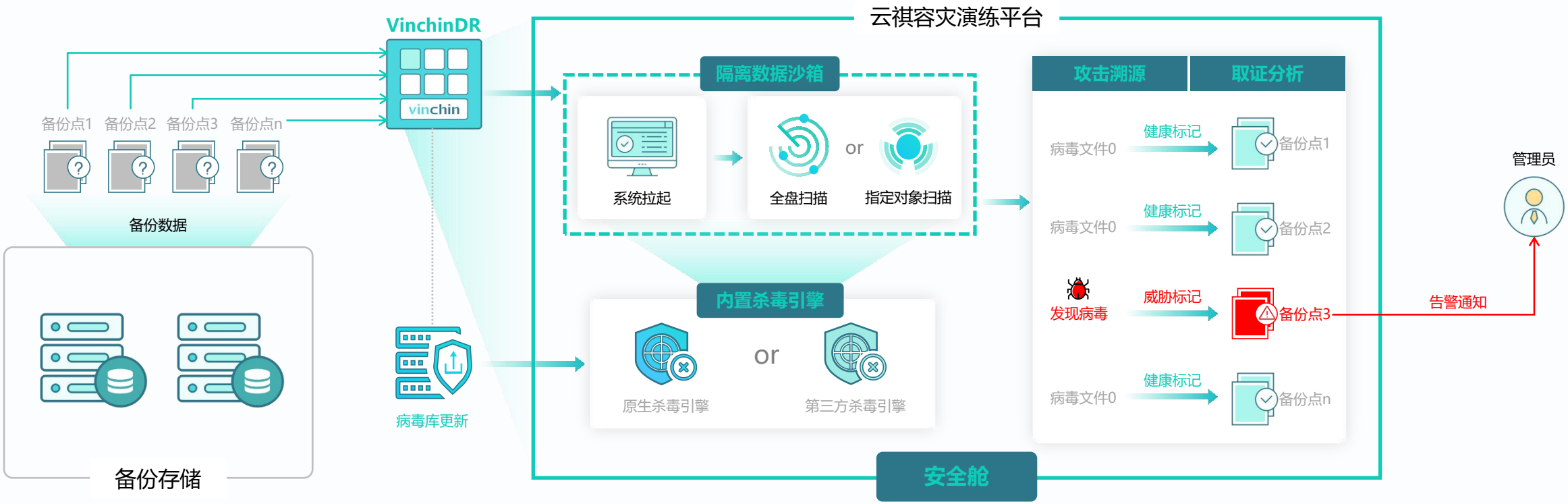
上报
安全事件

发送
告警通知

邮箱

企业微信

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

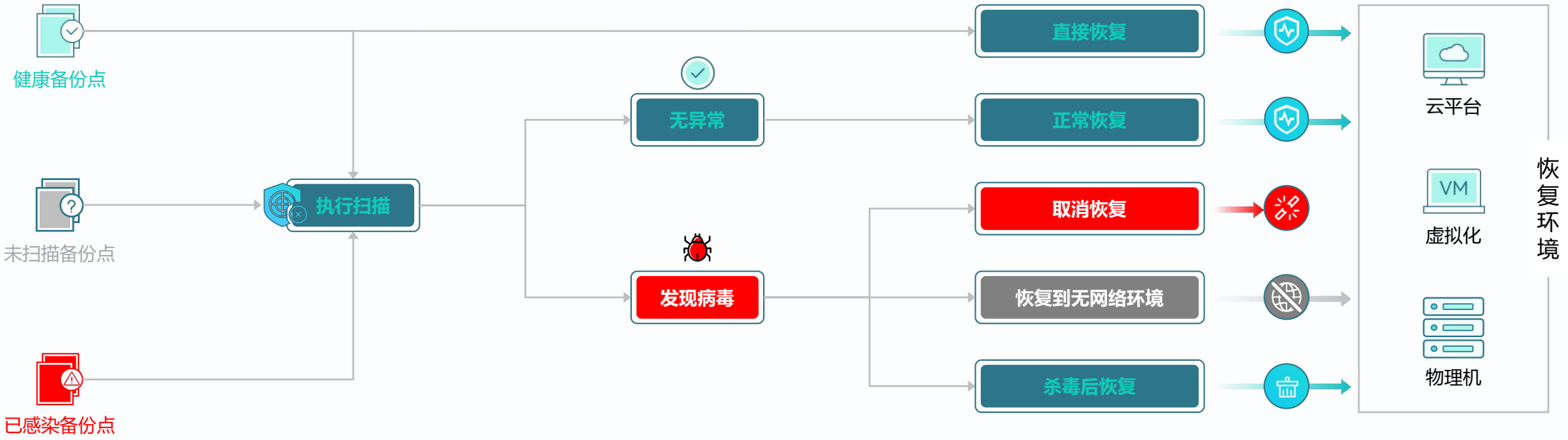
在备份数据中查找干净可用的备份点，为将来的安全恢复做好准备

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

安全恢复、杜绝二次感染

使用安全的备份恢复或在恢复前进行恶意软件扫描与查杀，以确保正确、干净、有效的恢复，防止恢复后造成二次感染。发现病毒时支持根据不同需要采取取消恢复、恢复到无网络环境或杀毒后再恢复。



vinchin

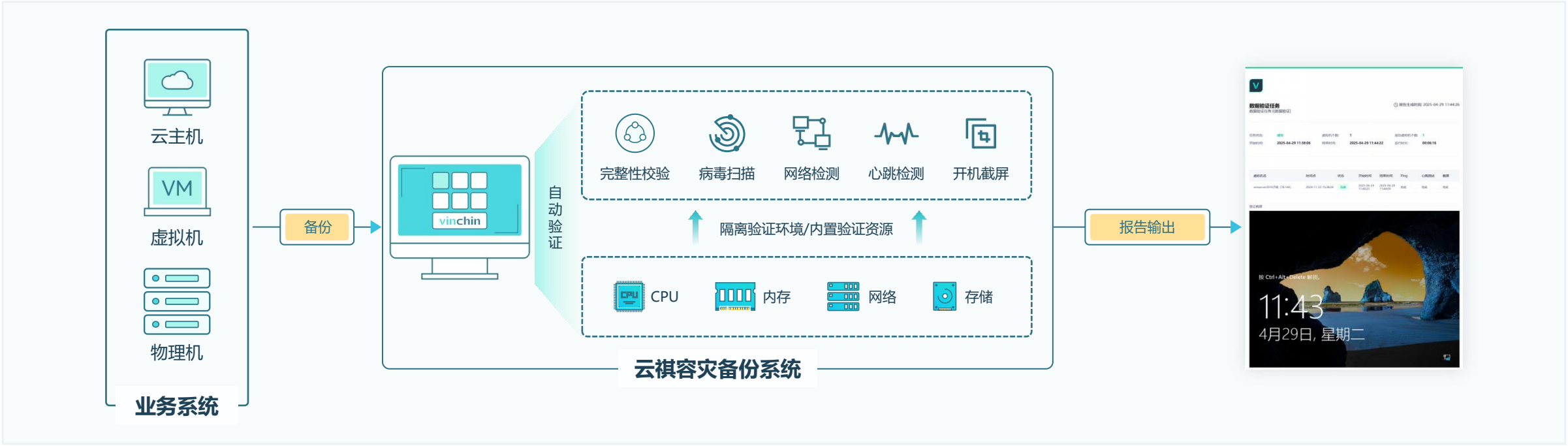
PART 03

备份数据容灾验证

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

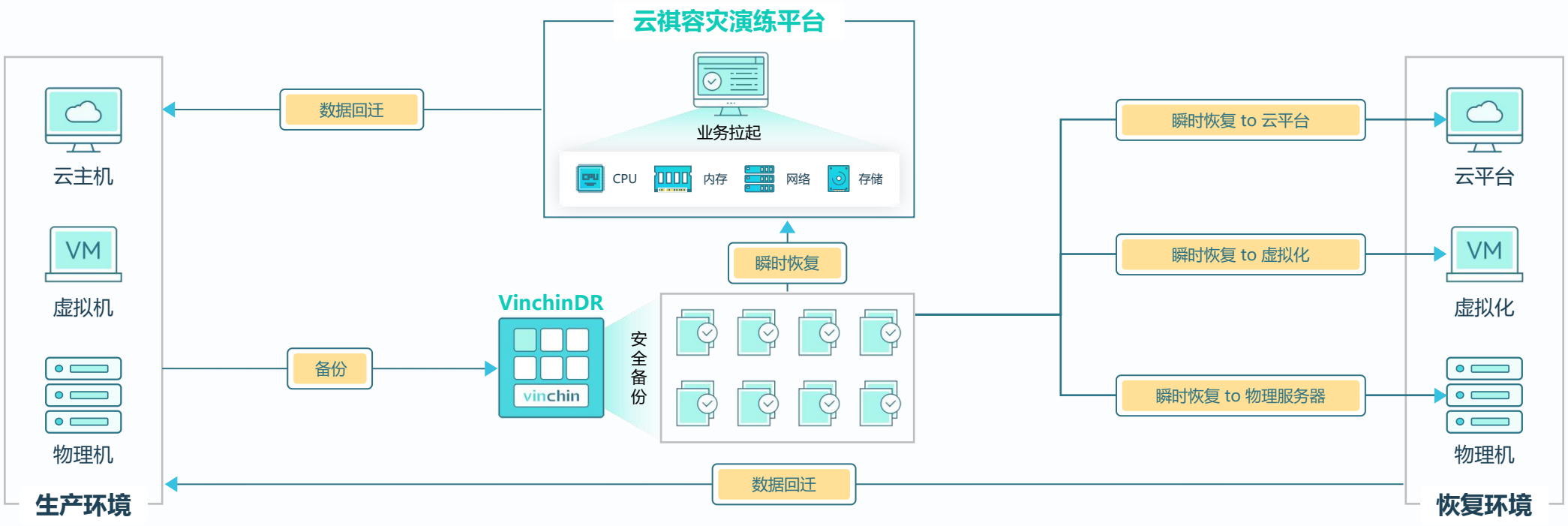
通过定期进行自动验证，确认备份数据状态，在异常时可及早接入采取对应措施

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

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

vinchin

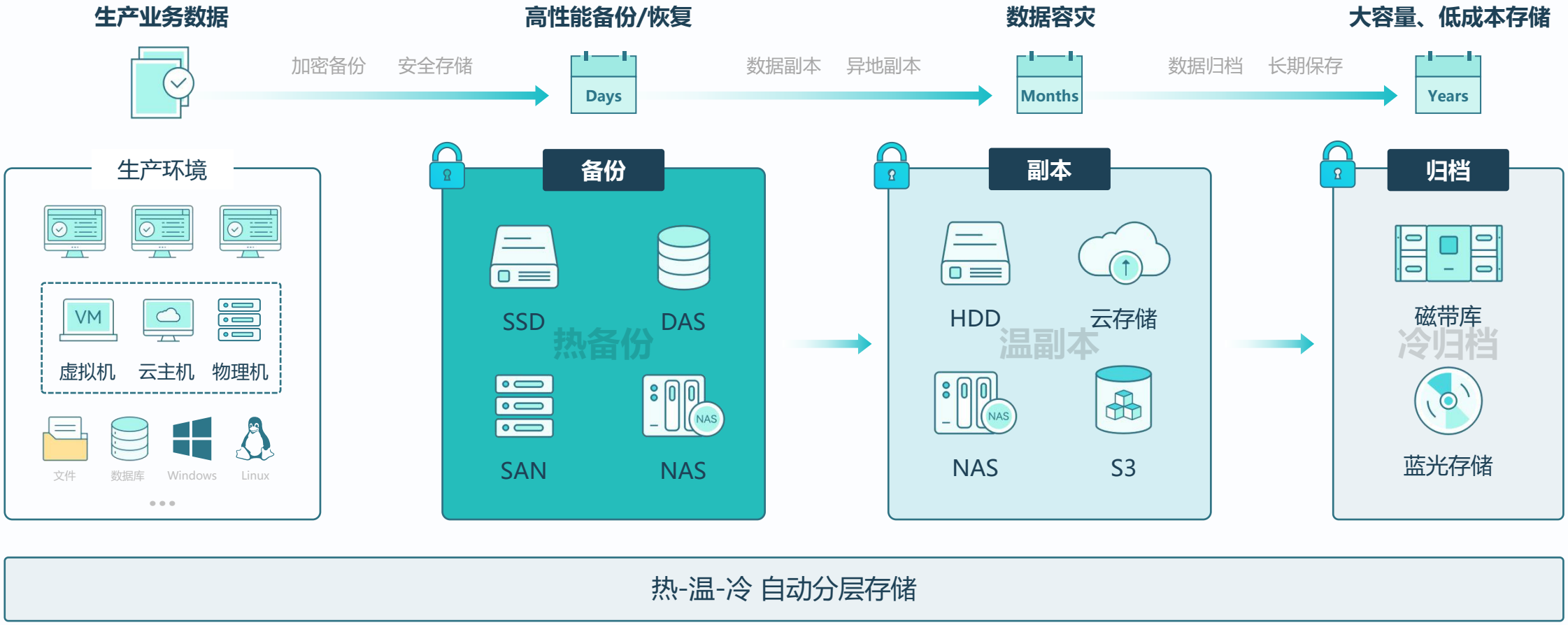
PART 04

备份数据副本与归档

分级数据管理

vinchin

不同业务系统对数据的可用性要求有所不同，不同类型数据的生命周期也存在显著差异，因此有必要根据其特点选择合适的数据存储策略与保留策略，并通过自动化的分层存储来简化用户的数据管理工作，并使其满足相应的数据合规要求。



副本

vinchin

副本回传

当主备份数据丢失时，副本回传功能支持异地备份数据回传至本地，并在本地恢复业务运行

快速业务接管

当生产环境发生灾难，主数据与备份数据同时丢失时，可在异地恢复/瞬时恢复副本数据，分钟级恢复业务运行

压缩传输

云祺异地副本对副本数据进行压缩处理，对备份数据进行源端重复数据删除与压缩，最大限度减少副本数据传输量，节约副本数据存储空间，降低存储成本，提高副本速度

完整备份系统

异地备份系统是一个完整的备份系统，具备备份系统所有功能，且备份系统中的副本存储，可作为另一个备份系统的副本异地存储使用

归档

vinchin

多源归档

多种数据源筛选方式，方便用户快速选择需要归档的数据。

双模式归档

对备份数据归档提供按策略归档与一次性归档两种归档方式。

自动精简存储

自动检测并删除或合并超出保留个数的归档数据，为用户节省存储空间，提高备份效率。

智能合并归档

云祺备份软件在数据归档时都将其智能合并为一个完全备份点进行数据归档。

灵活数据回传

用户可按虚拟机或时间点选择回传的归档数据，将归档数据回传至归档存储或者备份存储。

合规长期留存

满足合规性要求，将数据长期保存，实现数据的保留和长期的访问与检索。

vinchin

THANKS

云祺公众号

云祺视频号