vinchin

备份筑盾·全方位抵御勒索攻击

vinchin

目 录

vinchin

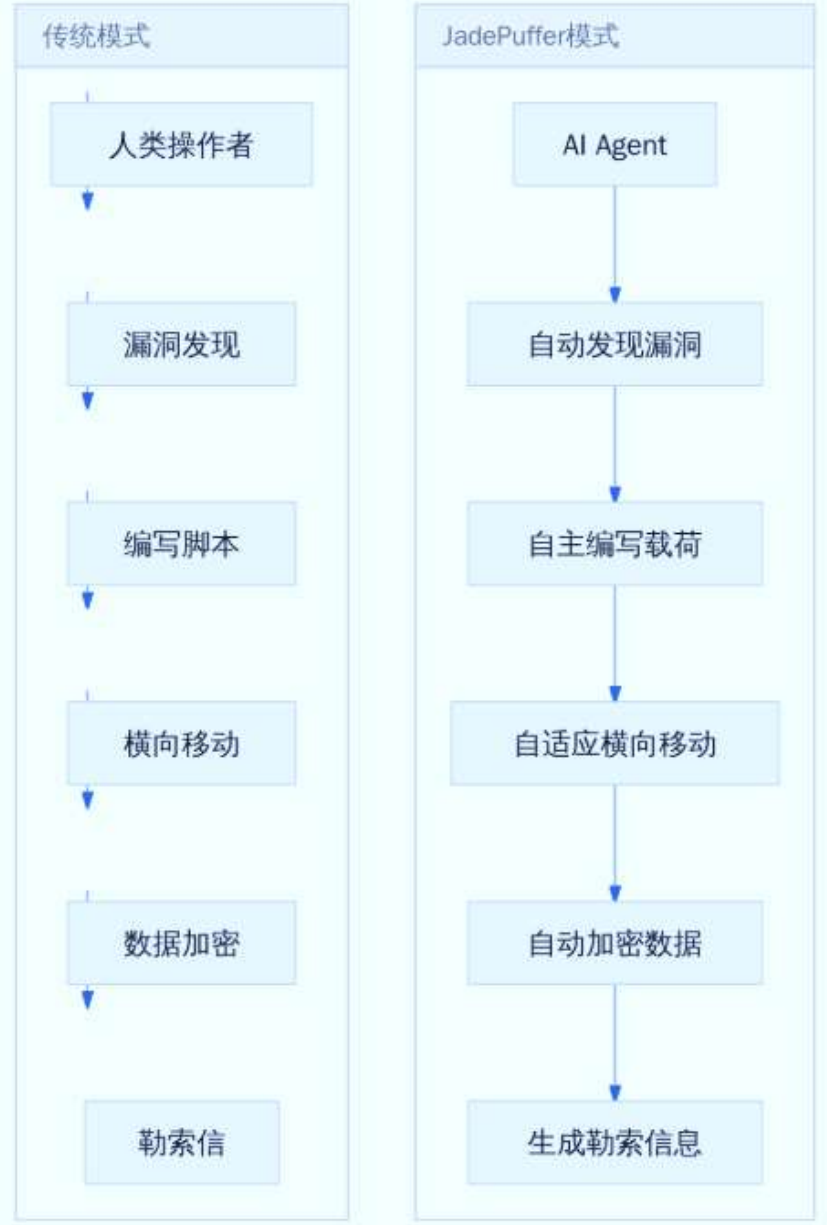
PART 01

数据安全事件回顾

事件1

AI驱动的自动化攻击：JADEPUFFER

2026年7月披露的全球首例AI代理型勒索软件，完全由大语言模型（LLM）自主驱动。它能利用软件漏洞独立完成入侵、凭证窃取、横向移动，直至加密销毁数据库的完整攻击链路，真正实现“无人值守”的自动化攻击闭环。



事件2

vinchin

印度核电站数据泄露

新华社北京7月18日电　印度媒体17日报道，**印度最大核电站库丹库拉姆核电站近日发生大规模数据泄露，包括工程设计图、供应商信息和员工资料等近1.9万份文件外泄。**这起数据泄露事件与该核电站承包商之一印度信实基建有限公司有关。据印度媒体报道，由于遭勒索软件攻击，信实基建有限公司共有逾85万份文件泄露，其中约1.9万份与库丹库拉姆核电站有关，这批外泄文件中最敏感内容，包括工程各阶段的设计图纸、人员资料、采购记录和保险单等。

事件2.1

印度塔塔电子（Tata Electronics）证实遭遇网络安全事件。
苹果印度代工厂遭病毒攻击，630GB绝密数据被挂暗网，iPhone 18 Pro Max所有细节遭曝光，连供应链底牌、自研芯片技术手册等核心数据彻底泄露。

事件3

公安部网安局公布5起打击“银狐”木马病毒典型案例

时间：2026年06月17日　来源：人民公安报　作者：张志颖　字体：大 中 小　分享到：

案例一、吉林公安网安部门侦破陈某等人制作“银狐”木马病毒案。吉林公安网安部门查明，以陈某为首的犯罪团伙开发“银狐”木马病毒变种，通过技术手段对抗安全检测，批量发送钓鱼邮件，窃取企业数据、搭建诈骗场景实施犯罪，涉案金额700余万元。目前，属地公安机关已对陈某等27名犯罪嫌疑人依法采取刑事强制措施。

案例二、浙江杭州公安网安部门侦破纪某等人制作并贩卖“银狐”木马病毒案。杭州公安网安部门查明，以纪某为首的犯罪团伙制作并贩卖“银狐”木马病毒，非法控制他人计算机信息系统，盗取网络资产，涉案金额300余万元。目前，属地公安机关已对纪某等5名犯罪嫌疑人依法采取刑事强制措施。

案例三、山东公安网安部门侦破杨某等人非法控制他人计算机信息系统案。山东公安网安部门查明，以杨某为首的犯罪团伙搭建多个钓鱼网站，诱导用户下载捆绑“银狐”木马病毒的软件安装包，非法控制他人计算机信息系统，盗取网络资产，涉案金额300余万元。目前，属地公安机关已对杨某等15名犯罪嫌疑人依法采取刑事强制措施。

2025全球多领域安全事件一览

vinchin

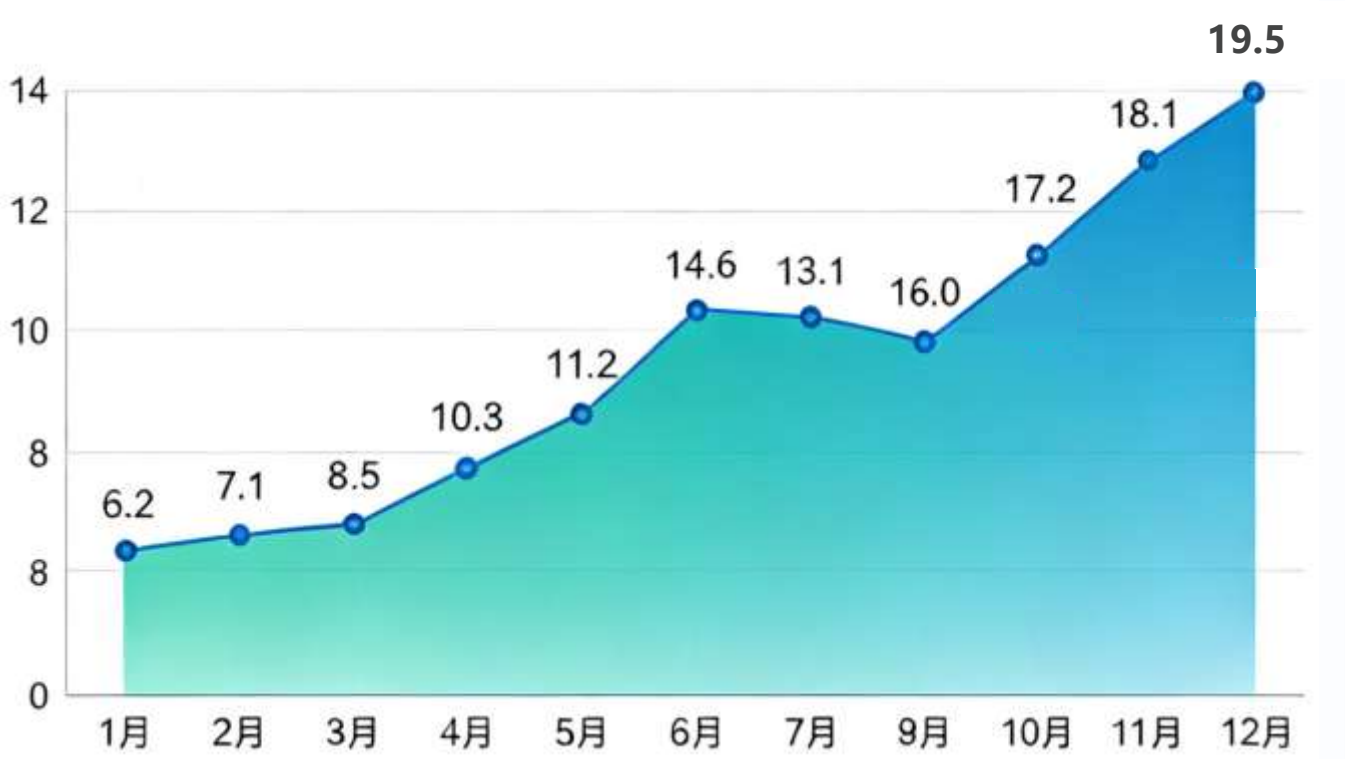
时间	所属行业	受害公司 / 机构	影响 & 损失
2025.01	**互联网**	社交平台 X（推特）	2.01 亿用户数据泄露，含邮箱、位置、账号资料等
2025.01	**AI**	DeepSeek	持续跨境应用层攻击，防御难度大幅提升
2025.02	**金融**	Bybit 交易所	Lazarus 团伙供应链攻击，被盗 49 万枚 ETH（约 14.6 亿美元），史上最大加密盗窃案
2025.02	**区块链**	WEMIX 平台	NFT 密钥被盗，865 万代币失窃，币价暴跌 30%，平台被标注风险资产
2025.03	**军工**	俄罗斯 NPOMars 国防企业	250GB 军工指挥系统、舰船控制技术图纸泄露
2025.04	**制造**	HELUKABEL（德电缆龙头）	RALord 双重勒索，30GB 图纸 / 客户数据被盗，全球供应链存连锁风险
2025.04	**医疗**	达维塔透析服务商	网络加密，全美 3000 家诊所业务受限，20 万患者诊疗受影响
2025.05	**政务**	秘鲁政府 Gob.pe 门户	Rhysida 双重勒索，3300 万公民护照、医疗、户籍数据泄露
2025.06	**军工无人机**	俄罗斯 Gaskar 无人机厂商	数 TB 无人机设计源码、员工数据被盗，厂区安保系统锁闭
2025.06	**通信**	AT&T 电信	8800 万用户社保、住址、身份信息暗网出售，欺诈风险激增
2025.07	**航空**	俄罗斯航空	网络瘫痪，54 + 航班取消，出行高峰大面积延误
2025.08	**汽车制造**	捷豹路虎	全球工厂停产，经销商新车注册系统瘫痪，员工停工
2025.08	**互联网托管**	俄罗斯 Filanco 集团	800TB 数据销毁、600 台虚拟机失效，2 万企业客户服务中断
2025.09	**信用金融**	越南 CIC 国家征信中心	1.6 亿国民信贷、身份数据泄露，越南史上最大数据泄露事件
2025.10	**电力能源**	瑞典国家电力 Svenska kraftnät	Everest 勒索，280GB 电力内部数据失窃，供电主干系统未受冲击
2025.11	**金融保险**	俄罗斯 VSK 保险巨头	备份系统遭破坏，7 天业务停摆，3300 万客户理赔全面中断
2025.11	**AI 安全**	Anthropic（Claude 厂商）	黑客利用 AI 自动完成渗透扫描、漏洞利用，30 余家机构遭间谍攻击
2025.12	**政务**	法国内政部	1640 万法国公民犯罪档案、身份信息泄露，刑事系统被入侵

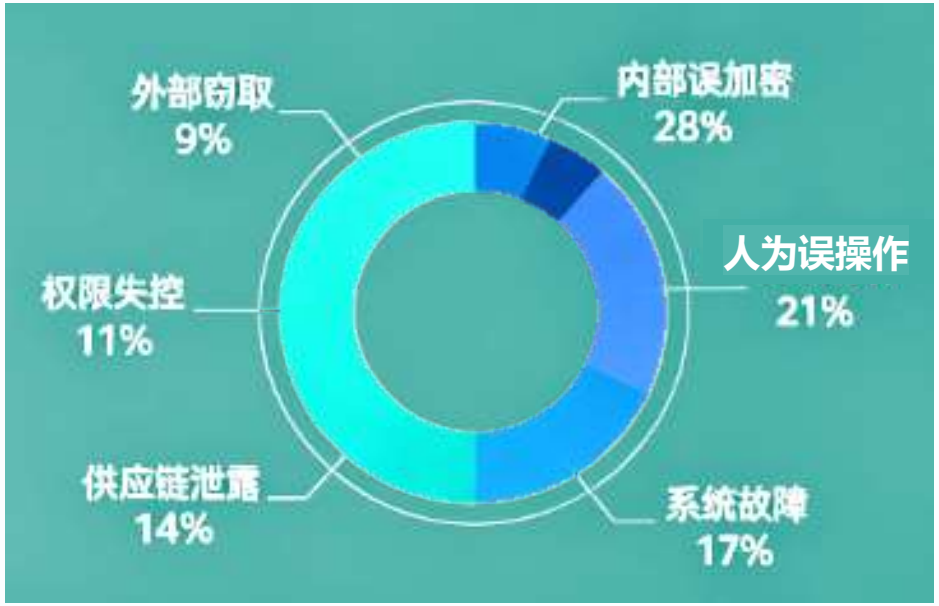
来源：网络公开勒索安全事件信息整理

24年~25年数据泄露情况

vinchin

2024-2025数据丢失与泄露频率变化（变化指数%）





勒索加密:攻击直接造成业务数据不可访问

内部误操作:删除、覆盖与配置错误占比稳定

系统故障:存储、数据库与云同步异常影响业务连续性

供应链泄露:第三方接口与服务商风险传导

权限失控:过度授权、弱口令与审计缺失放大泄露面

外部窃取:钓鱼、木马与定向攻击获取敏感数据

来源：网络公开勒索安全事件信息整理

24年~25年勒索攻击情况

增长情况：
2025年公开受害企业约7419家，同比增长32.2%

攻击变化：
双重勒索占比有明显提升，先窃取后加密成为标准流程

风险预测：
关键基础设施、制造和医疗仍为高价值目标

来源：网络公开勒索安全事件信息整理

各行业勒索态势严峻

vinchin

01. 教育行业

校园数据环境复杂且用户基数庞大，师生弱密码现象泛滥。据统计，人为操作失误造成的信息泄露占比高达72%，极易成为攻击者的突破口。

02. 医疗行业

承载生命安全业务，对零停机有着刚性需求。面对勒索攻击时支付赎金的意愿最强，同时业务停摆与数据泄露叠加，使得单起事件综合损失位居全行业最高。

03. 能源行业

关乎国计民生的关键基础设施，其网络攻击具备国家级的破坏潜力。除普通勒索外，还频繁遭受APT组织定向渗透，威胁国家安全。

04. 金融行业

虽整体安全防护体系最为成熟，但资产价值极高。勒索团伙索要的赎金金额通常最高，同时针对员工的新型AI钓鱼诈骗正呈快速激增态势。

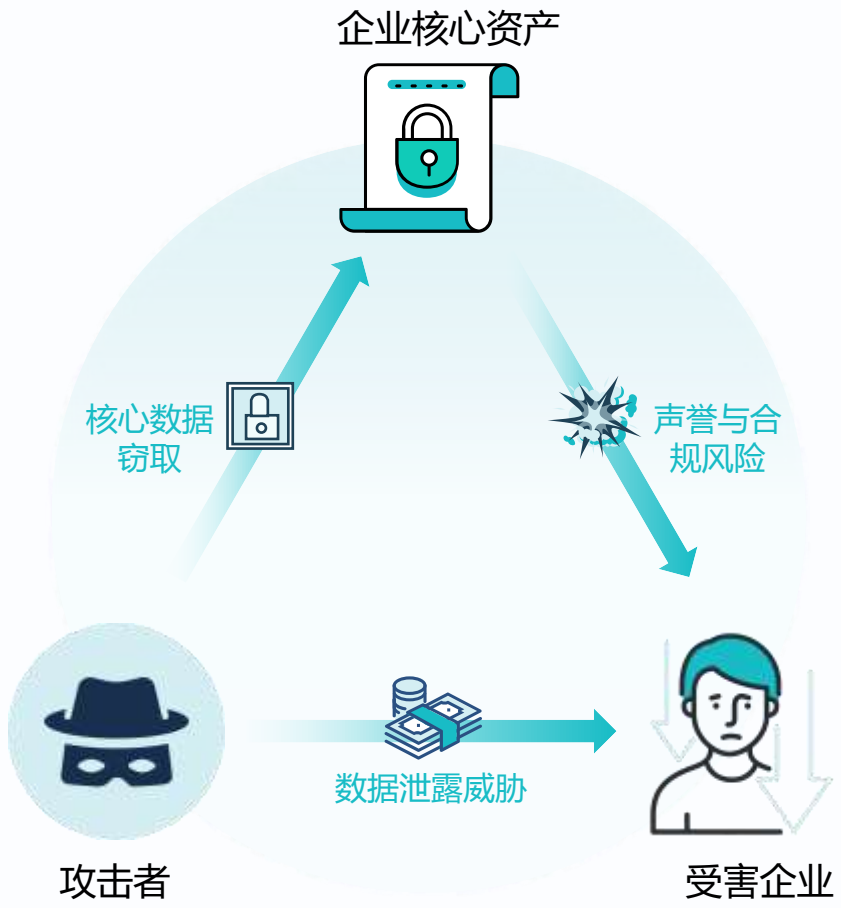
05. 制造行业

工控OT网络与办公IT网络加速打通，防护边界彻底模糊。一旦遭遇攻击导致产线停工，将造成巨额直接经济损失，已成勒索团伙的主攻方向。

06. 公共基建

涵盖政务、交通等系统，一旦数据泄露将波及海量公民隐私，触发巨额合规处罚。同时外包运维接口繁多，大量遗留漏洞成为攻击捷径。

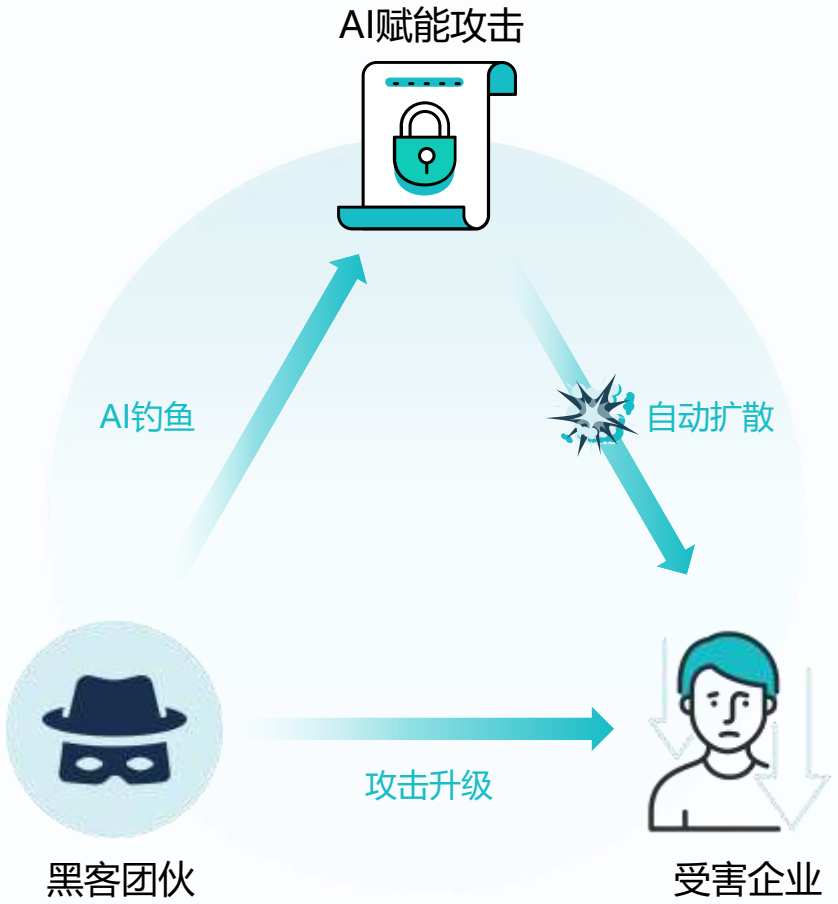
勒索攻击新趋势



双重勒索已成主流：
攻击者不仅加密数据，还窃取财务、客户等核心资料，以“泄密公开”威胁企业，形成“加密锁机+数据泄露”的双重施压。

无加密勒索悄然兴起：攻击者不再加密系统，仅窃取敏感数据后实施勒索。这种方式更隐蔽，避开传统加密检测机制，攻击窗口期更长，企业往往在数据泄露或收到勒索信时才察觉，隐私泄露与合规处罚的风险更为隐蔽且持久。

勒索攻击新趋势



AI辅助钓鱼精准度飙升：生成式AI可批量制作高度逼真、高度个性化的钓鱼邮件与文档，让攻击更具隐蔽性。数据显示，2025年用于构建攻击的高风险AI提示词数量激增97%，精准度与成功率同步大幅提升。

攻击工具自动化降低门槛：勒索软件即服务（RaaS）模式持续进化，自动化攻击套件让技术门槛降至新低，非专业人员也能发起攻击。攻击流程实现全链路自动化，新型勒索家族快速迭代，潜在攻击者基数呈几何级扩大。

勒索攻击新趋势

01 身份冒充，合法入侵

攻击者利用社交工程冒充IT支持或管理人员，通过钓鱼邮件、即时通讯欺骗员工执行恶意指令，借此窃取合法身份权限，轻松绕过传统边界防御，实现隐蔽的“合法”入侵与内网横向移动。

02 供应链攻击，祸及池鱼

攻击不再局限于单一企业，而是瞄准供应链薄弱环节实施渗透。2025年Shai-Hulud活动通过攻陷开源组件传播恶意代码，波及全球开发者生态，恶意npm包数量同比激增100%，引发上下游连锁式安全危机。

03 防御升级：从单点到生态协同

传统单点防御已失效，企业需构建“身份零信任+供应链全审计”的双重防线。一方面强化身份鉴权与行为审计，另一方面对第三方组件、开源代码进行全生命周期安全检测，实现从个体防护到生态协同的安全体系升级。

应对勒索”硬合规“要求

vinchin

ICS 35.030
CCS L 80

GB

中华人民共和国国家标准

GB/T 20274.2—2026

代替 GB/T 20274.2—2008,GB/T 20274.3—2008,GB/T 20274.4—2008

网络安全技术　信息系统安全保障评估框架　第2部分:安全保障要求

Cybersecurity technology—Evaluation framework for information systems security assurance—Part 2: Security assurance requirements

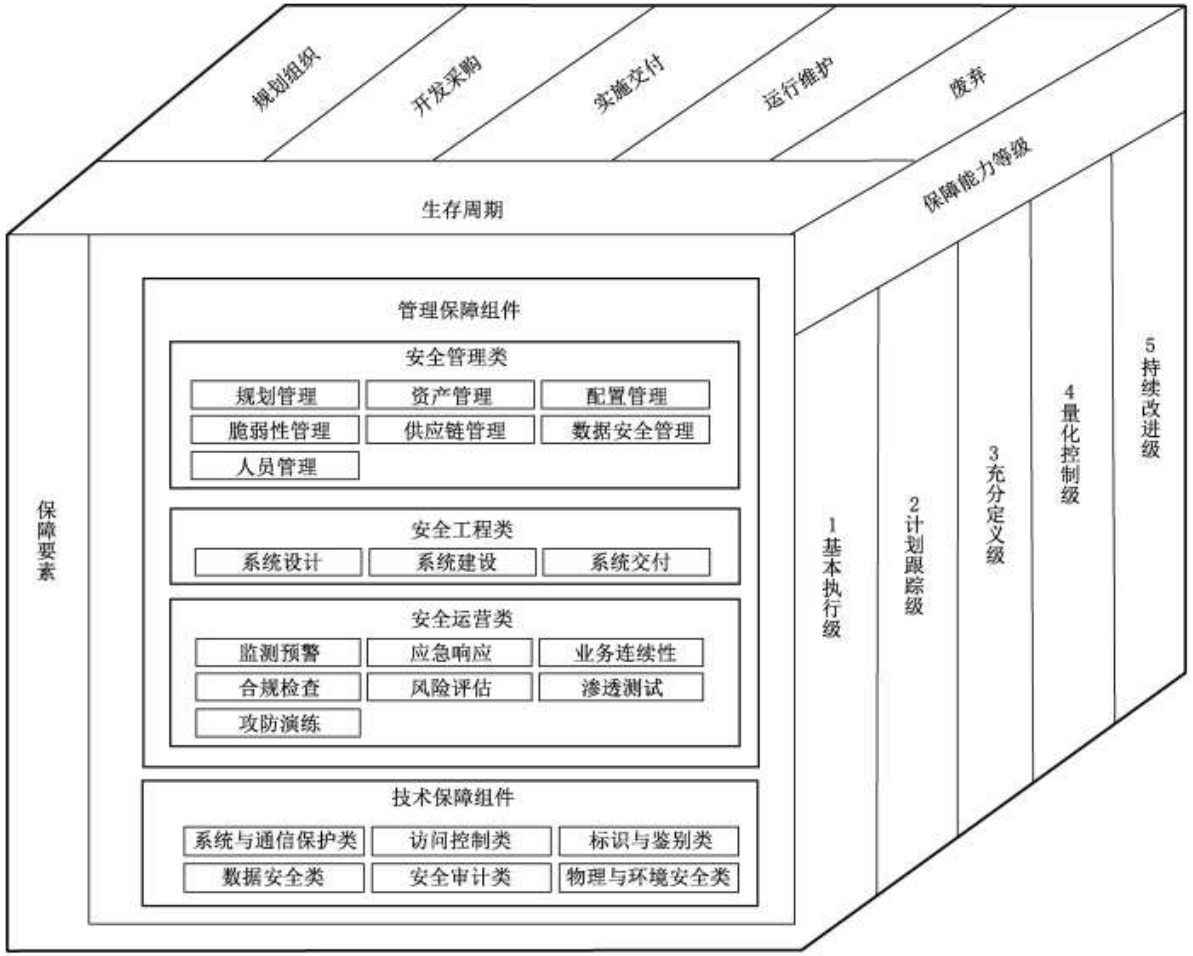
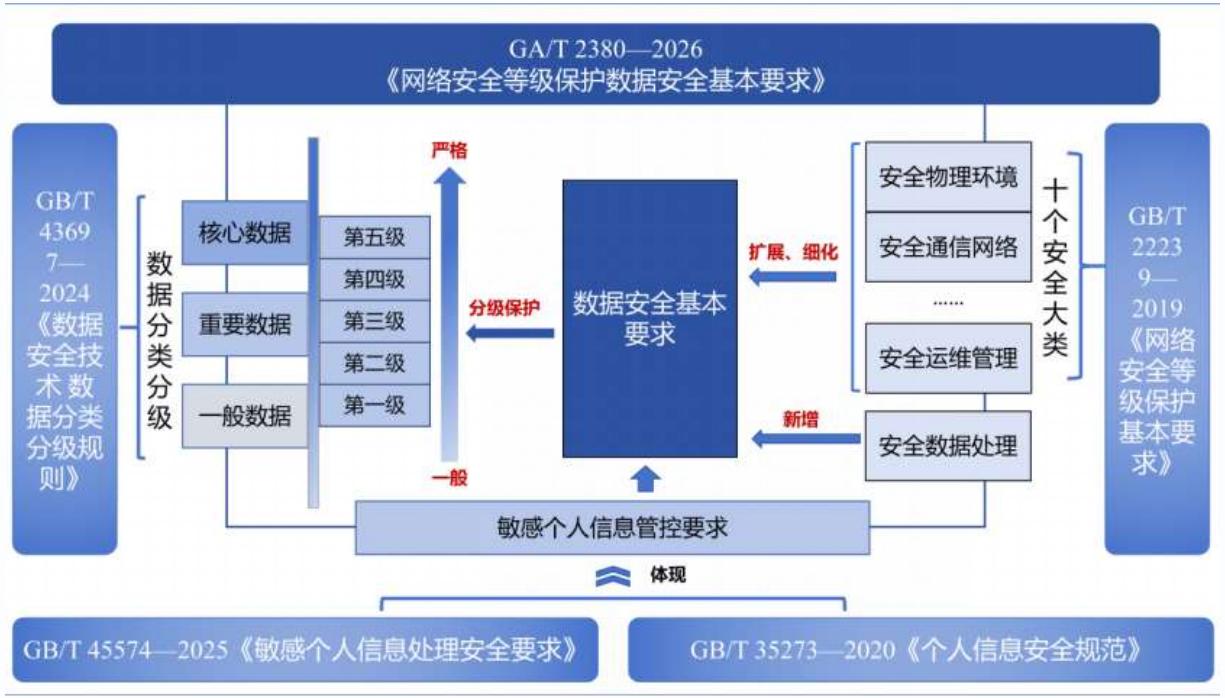


图 1　信息系统安全保障评估模型

应对勒索”硬合规“要求

vinchin

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》



01. 从“附加项”到“独立体系”

新增“安全数据处理”大类，不再依附于系统安全，全面覆盖数据采集、传输、存储、使用到销毁的全生命周期管控。

02. 双维度差异化精准保护

结合网络系统本身的安全等级，叠加数据分级（一般、重要、核心），针对不同组合配置差异化的防护要求，重点强化核心数据保护。

03. 测评聚焦“数据流动”过程

不再仅检查静态系统配置，而是沿数据全流程展开核查；明确33项“一票否决”重大风险项，触及底线直接判定不通过。

04. 确立硬性技术执行指标

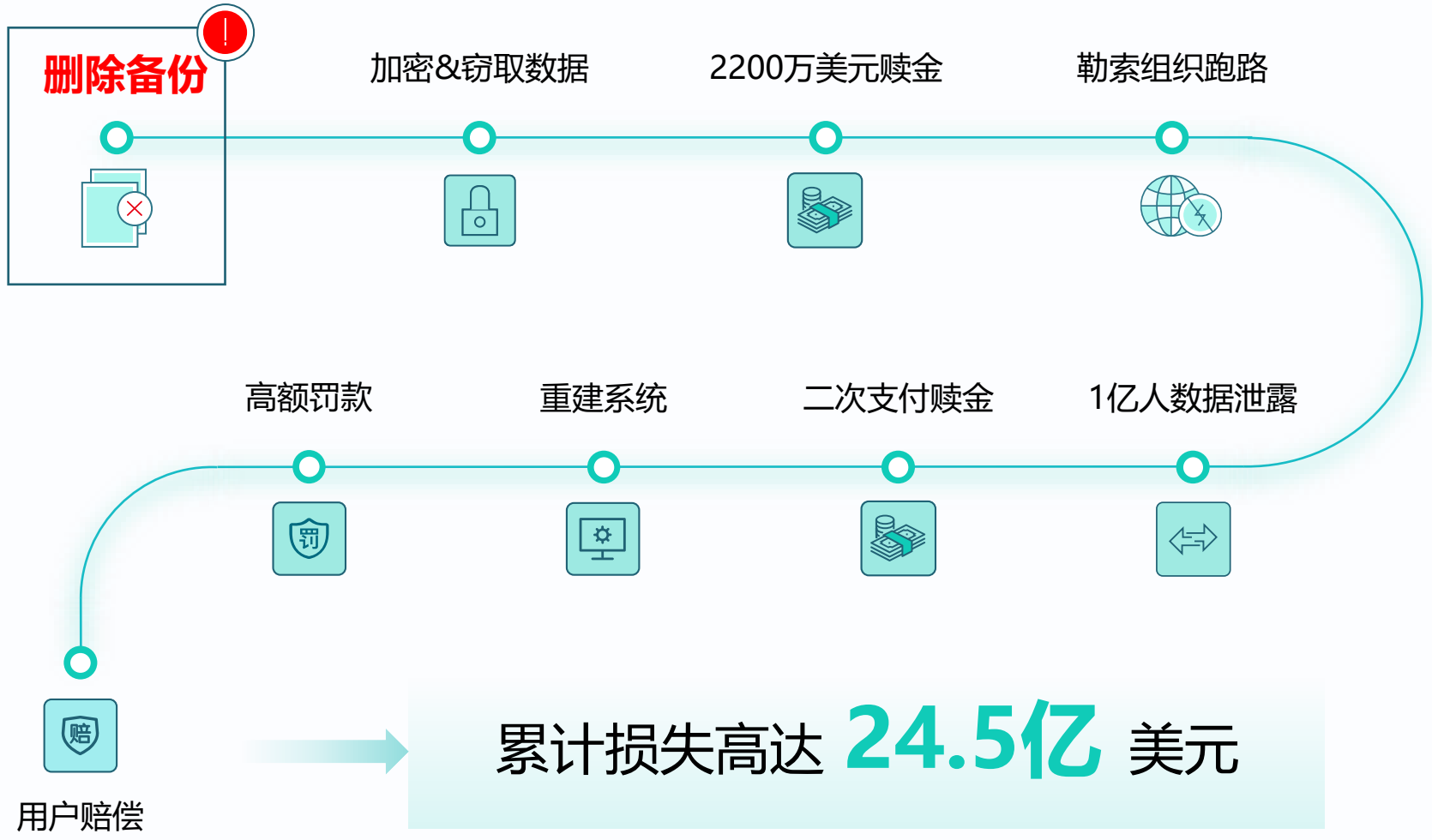
强制要求落地国密算法加密、敏感数据脱敏展示、安全日志完整留存1年以上等硬性措施，实现合规可验证。

数据安全的最后一道防线“备份”被攻破了

vinchin

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

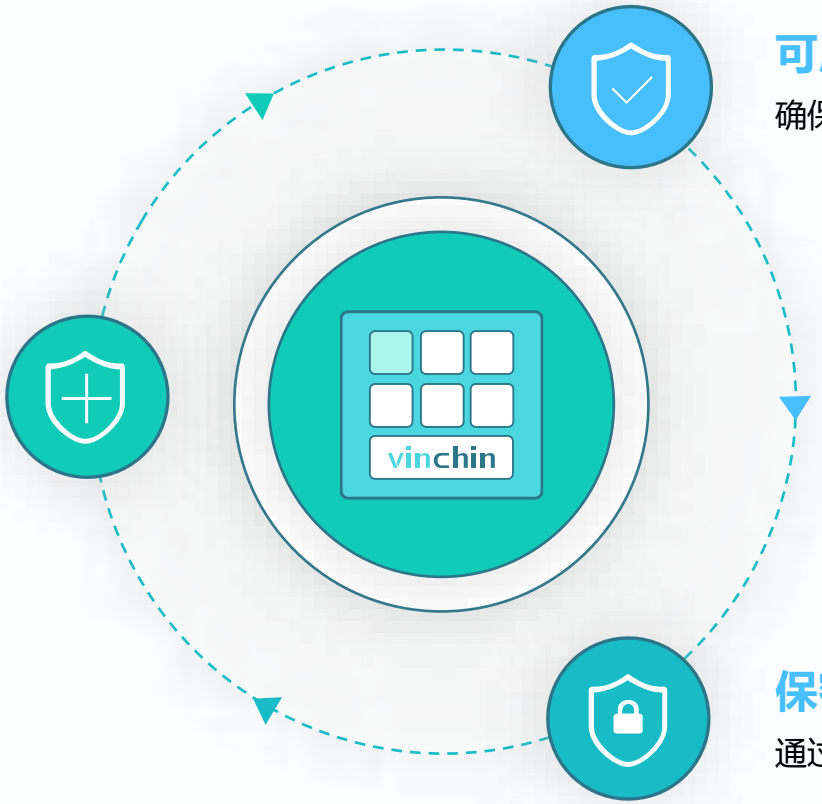
vinchin

PART 02

云祺安全备份体系

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

3-2-1
1-0-0

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

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

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

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

第三方
集中管理平台

SIEM系统

上报
安全事件

发送
告警通知

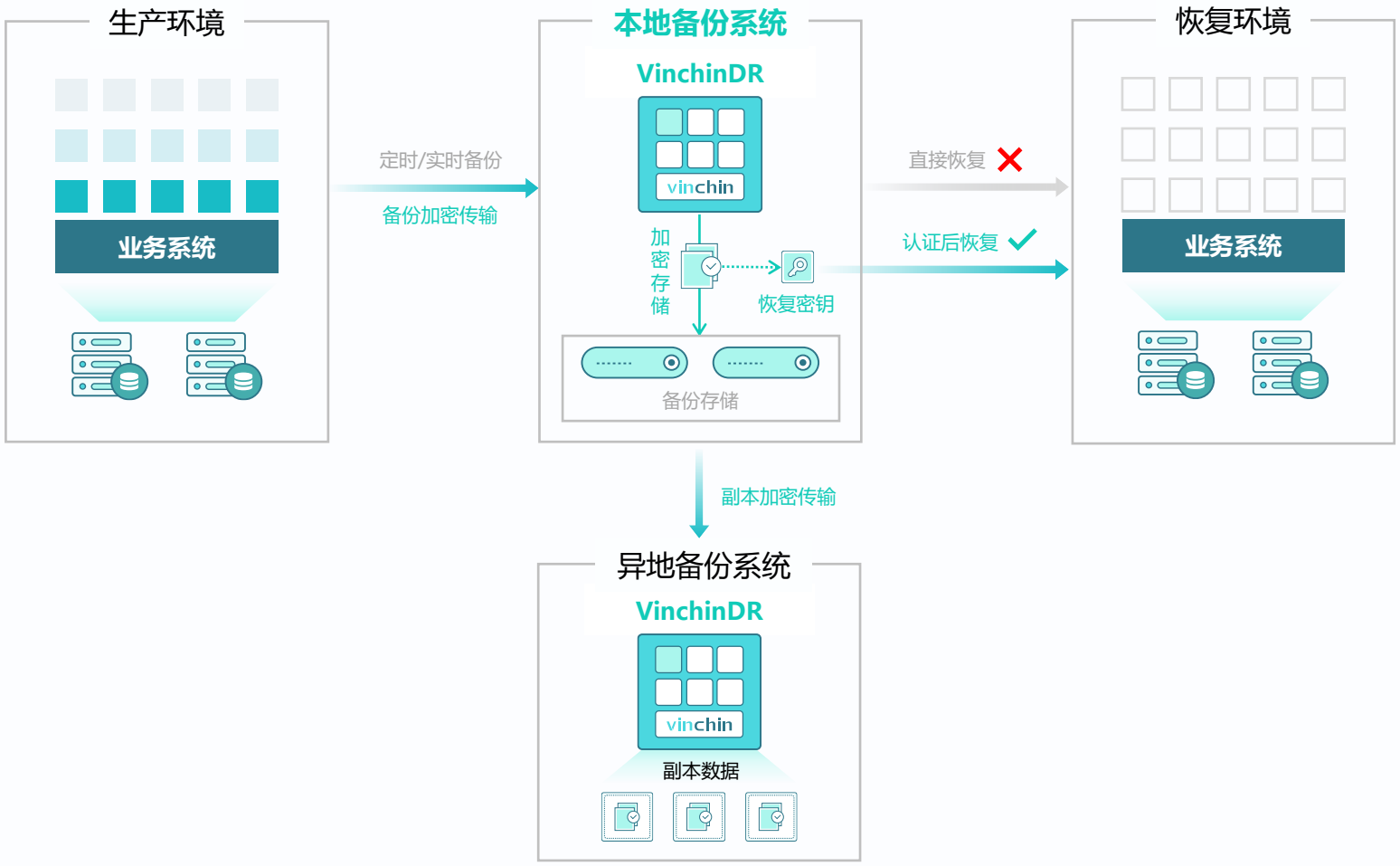
邮箱

企业微信

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

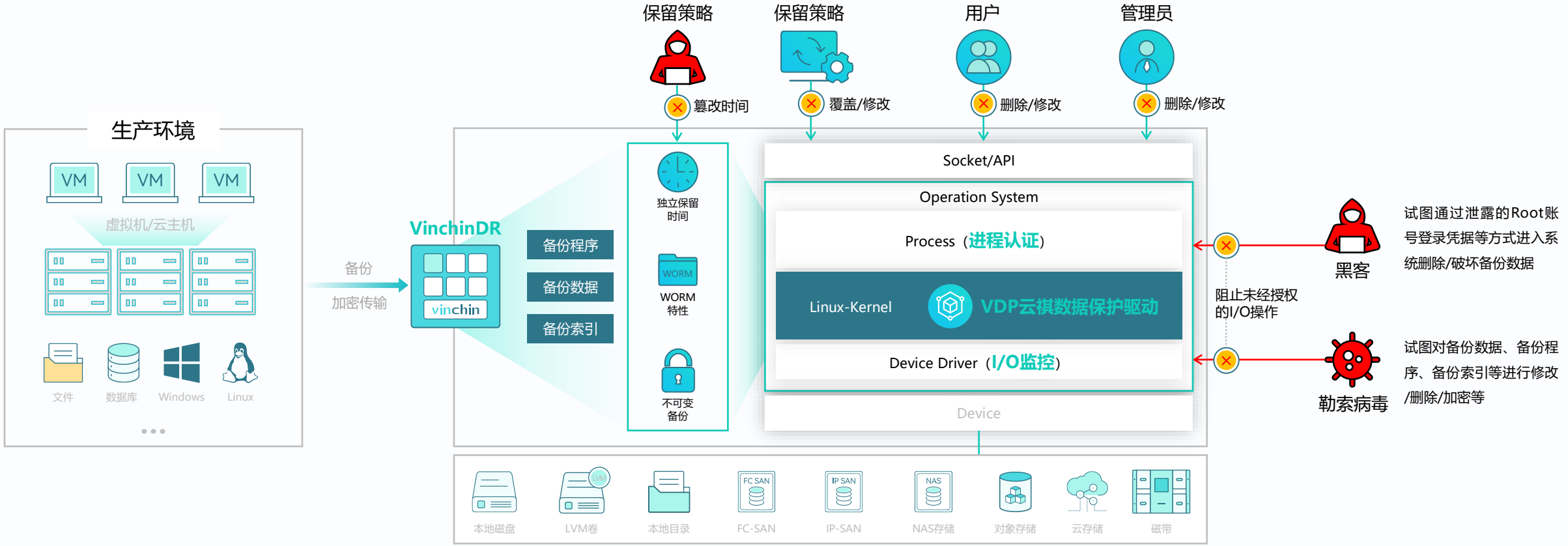
加密存储

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

不可变存储防篡改



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

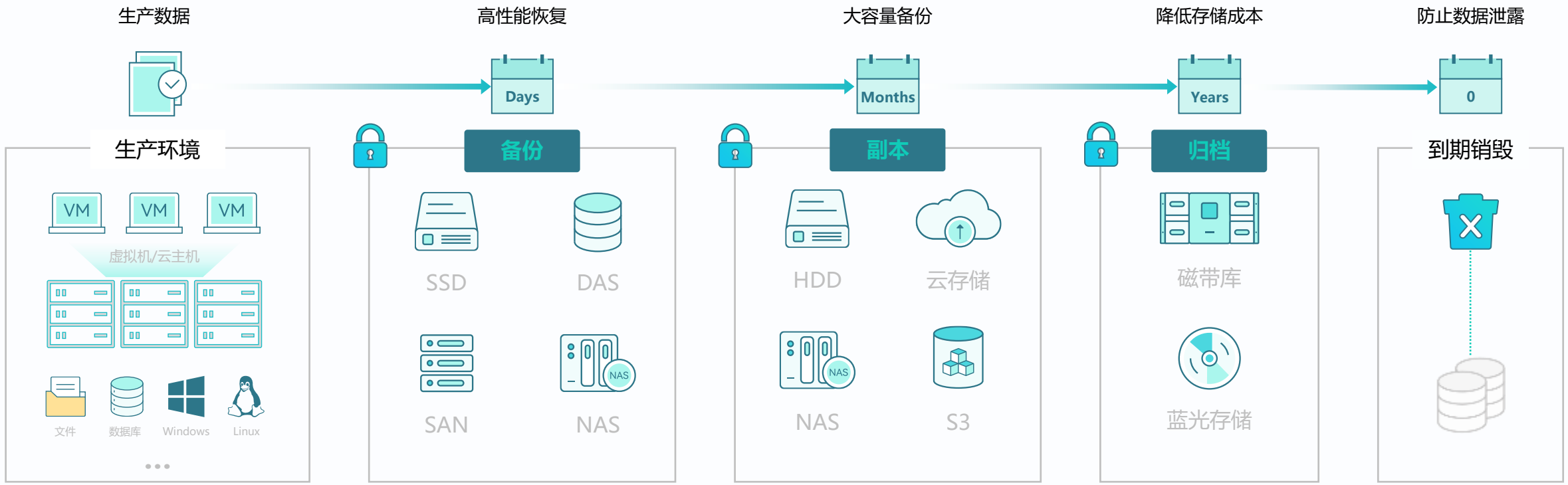
不可变存储：使用原生不可变存储或对象存储Object Lock、物理磁带离线存储等实现备份数据不可变特性

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

覆盖数据生命周期的不可变

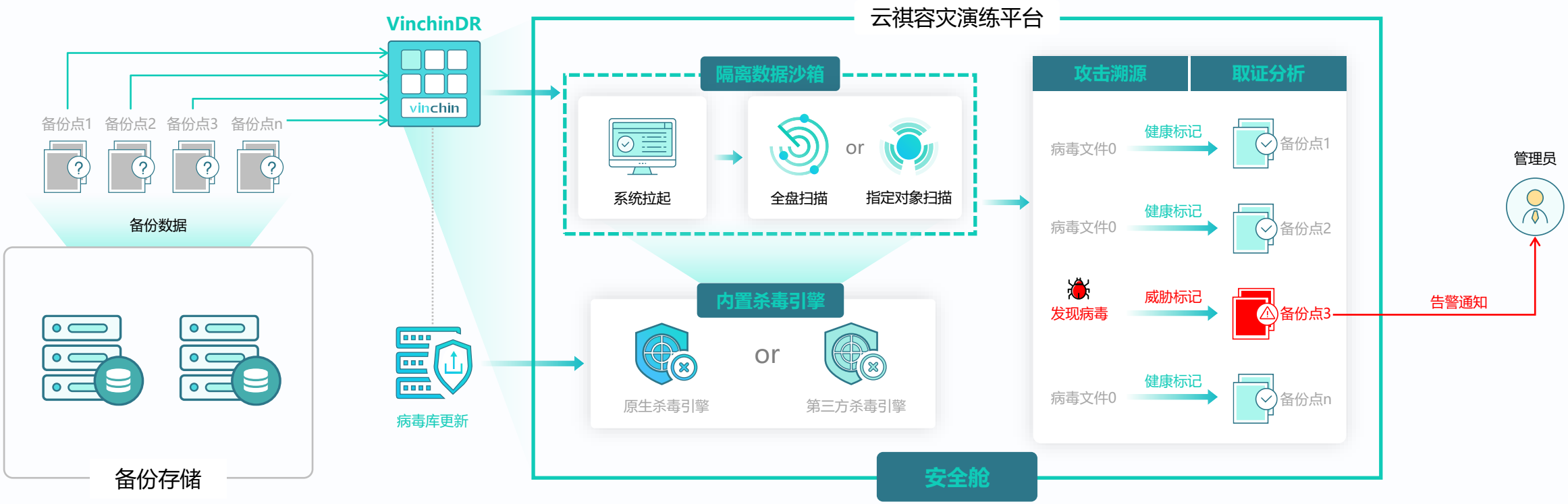
vinchin

不可变备份 | 全程可持续 | 自动分层 | 横向可扩展 | 降低存储成本 | 满足合规要求



覆盖全程的不可变特性

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

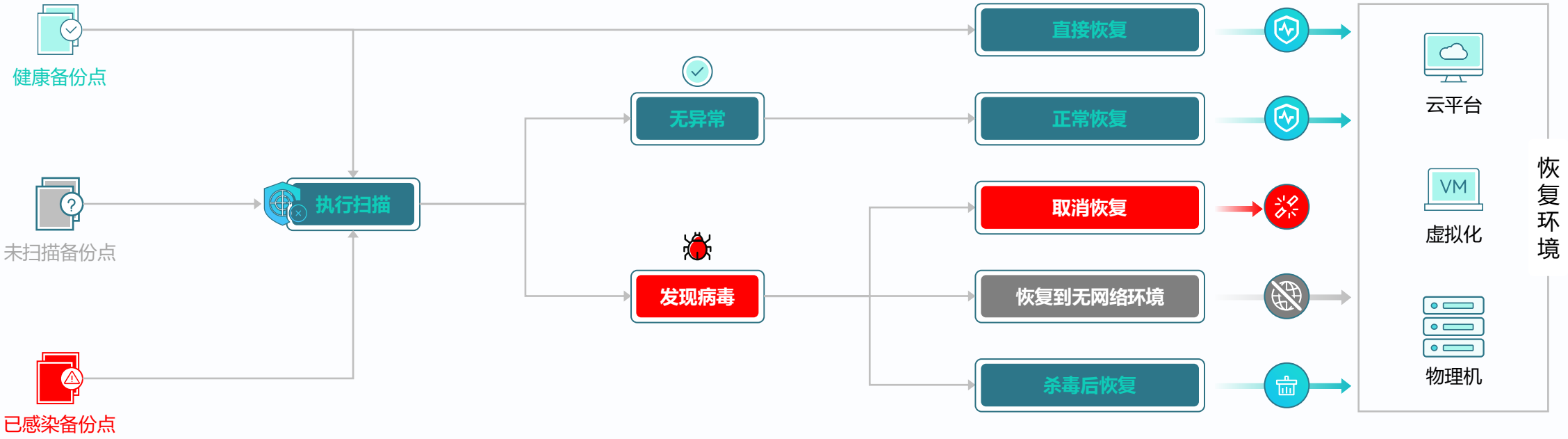
在备份数据中查找干净可用的备份点，为将来的安全恢复做好准备

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

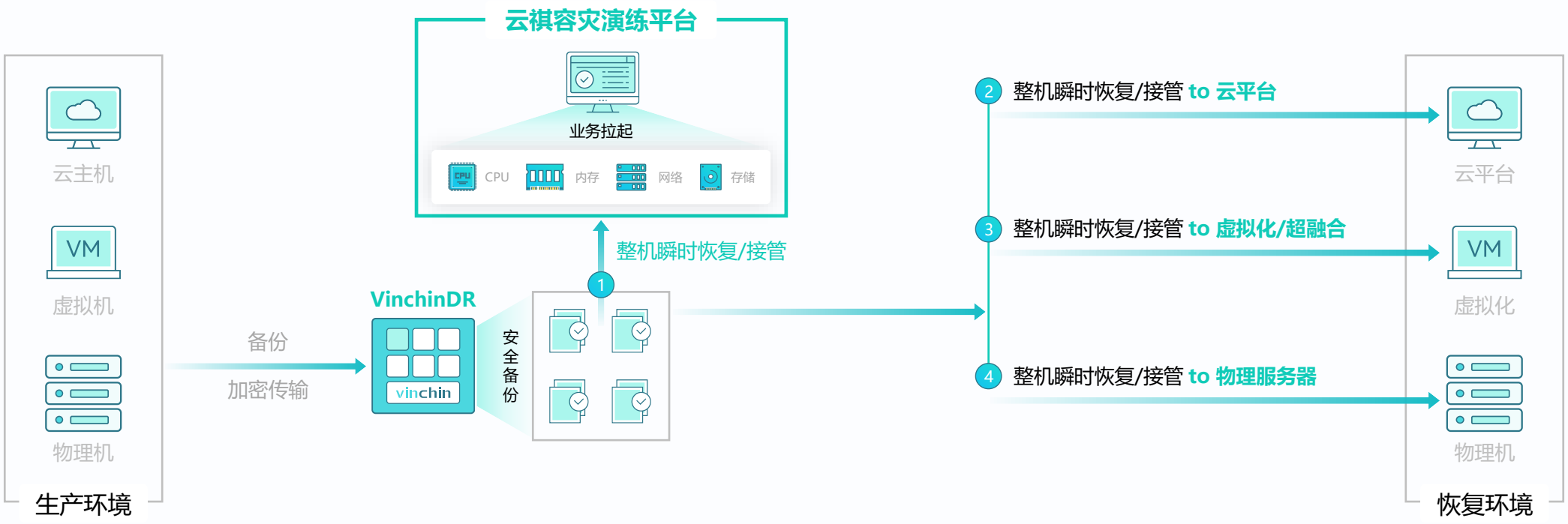
使用安全的备份恢复或在恢复前进行恶意软件扫描与查杀，以确保正确、干净、有效的恢复，防止恢复后造成二次感染。发现病毒时支持根据不同需要采取取消恢复、恢复到无网络环境或杀毒后再恢复。



快速恢复——实现业务“零中断”

vinchin

当生产遭遇勒索时，需要尽快恢复数据或业务系统来保障业务的连续性，减少业务中断带来的影响和损失，而实际恢复时，准备环境、等待数据传输等过程耗时耗力，将极大的影响恢复效率。



整机瞬时恢复

无需处理系统、应用、数据等复杂关联，直接整机拉起

内置恢复资源

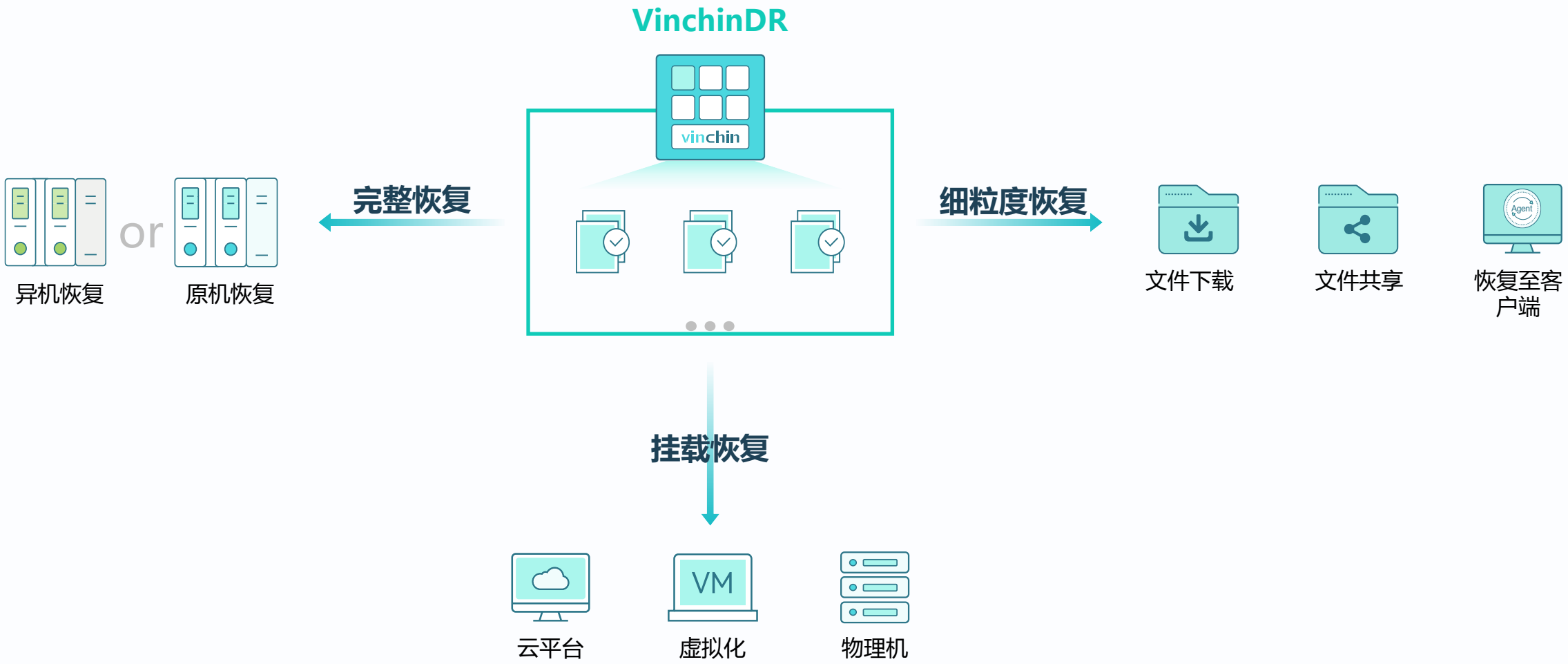
使用内置恢复资源快速支撑业务恢复，降低恢复成本

分钟级RTO

无需等待数据传输，分钟级完成恢复并开机使用

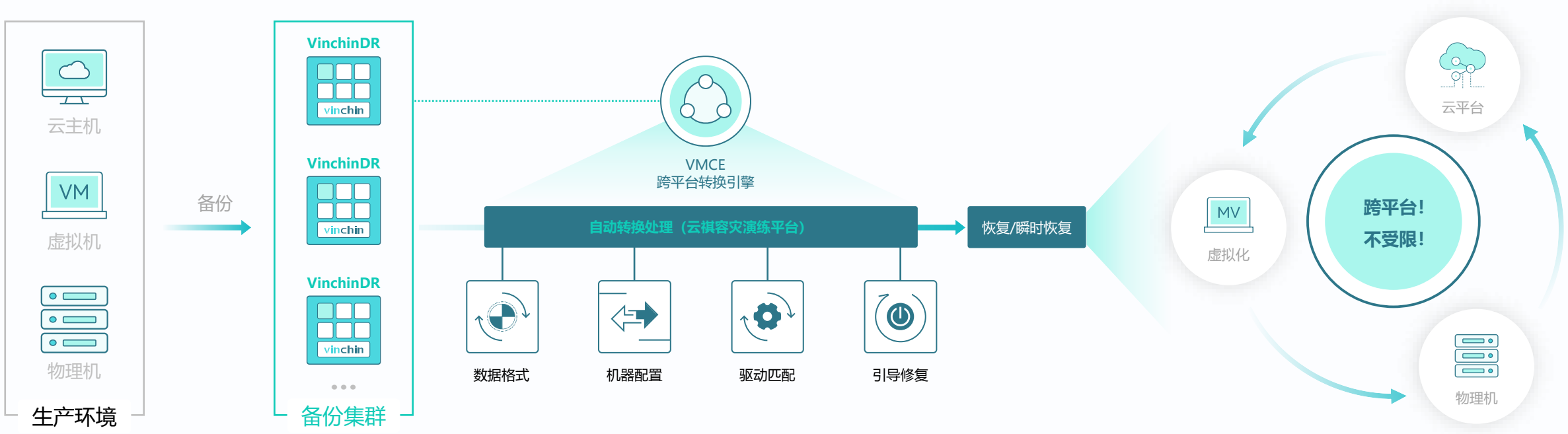
灵活恢复选项，满足不同恢复需要

vinchin



跨平台弹性灾难恢复

vinchin



异构智能转换

根据目标平台类型自动转换数据格式与系机器配置

驱动智能替换

根据系统配置需要自动从内置驱动库匹配驱动进行替换

引导自动修复

无需手动干预，恢复后自动修复系统引导，确保成功恢复

跨平台弹性恢复

不受位置、备份方式限制，任意支持平台双向弹性恢复

自动验证与恢复演练

vinchin

确认恢复就绪

定期验证业务恢复的可行性，测试恢复是否就绪

自动化验证

自动验证每一份备份数据，大幅简化人工操作

0资源成本

系统内置验证/演练所需资源，降低验证成本投入

0生产影响

隔离验证环境，验证不影响生产业务正常运行

降低管理难度

验证智能编排，批量验证业务，大幅减少管理工作

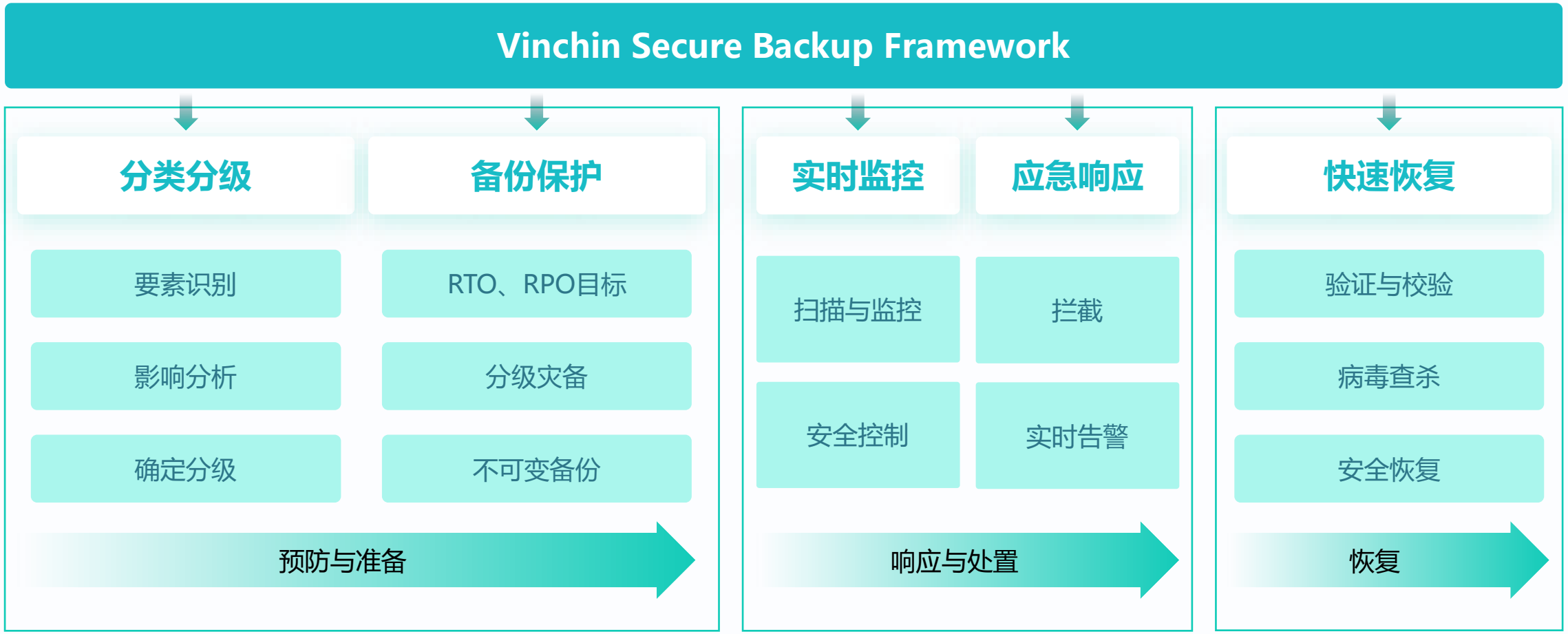
简化报告工作

无需人工整理汇总可视化验证报告输出，结果清晰可见

帮助持续改进

根据验证结果持续优化策略，提高数据安全管理水平

云祺安全备份框架(VSBF)



云祺安全备份框架（**Vinchin Secure Backup Framework**）包含分类分级、备份保护、实时监控、应急响应、快速恢复5个部分，针对勒索攻击不同阶段的特性构建安全体系，帮助用户实现精准、快速、安全的恢复，最大程度减少或避免因勒索导致的业务中断与经济损失。

vinchin

PART3

演示&答疑

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