vinchin

安全备份体系·从容应对勒索

云祺容灾备份系统V6.0

产品中心-王斌

vinchin

目 录

vinchin

PART 01

勒索威胁形势严峻

什么是勒索病毒?

vinchin

全球数字化革命正在以迅猛的速度重塑经济发展与生产生活方式，随着数字化转型成本持续降低，数字化不再是一种奢侈品，而是企业保持竞争力和提升行业创新的必要条件，随着越来越多的数字化业务系统上线，数据安全威胁形式也越发严峻。

> 勒索病毒是一种特殊的恶意软件，它会攻击受害者的系统和数据，使其保持锁定或加密状态，并要求受害者向攻击者支付赎金，以此获取高利润。

> 勒索攻击给受害者带来的影响是多方面的，除了需要支付高额赎金外，业务中断、声誉受损等问题也会接踵而至，更严重的是，违反数据安全法规可能导致严重的法律后果。

勒索病毒全球肆虐

46%

2024年，勒索攻击受害者数量再度陡增，约较上一年增长46%

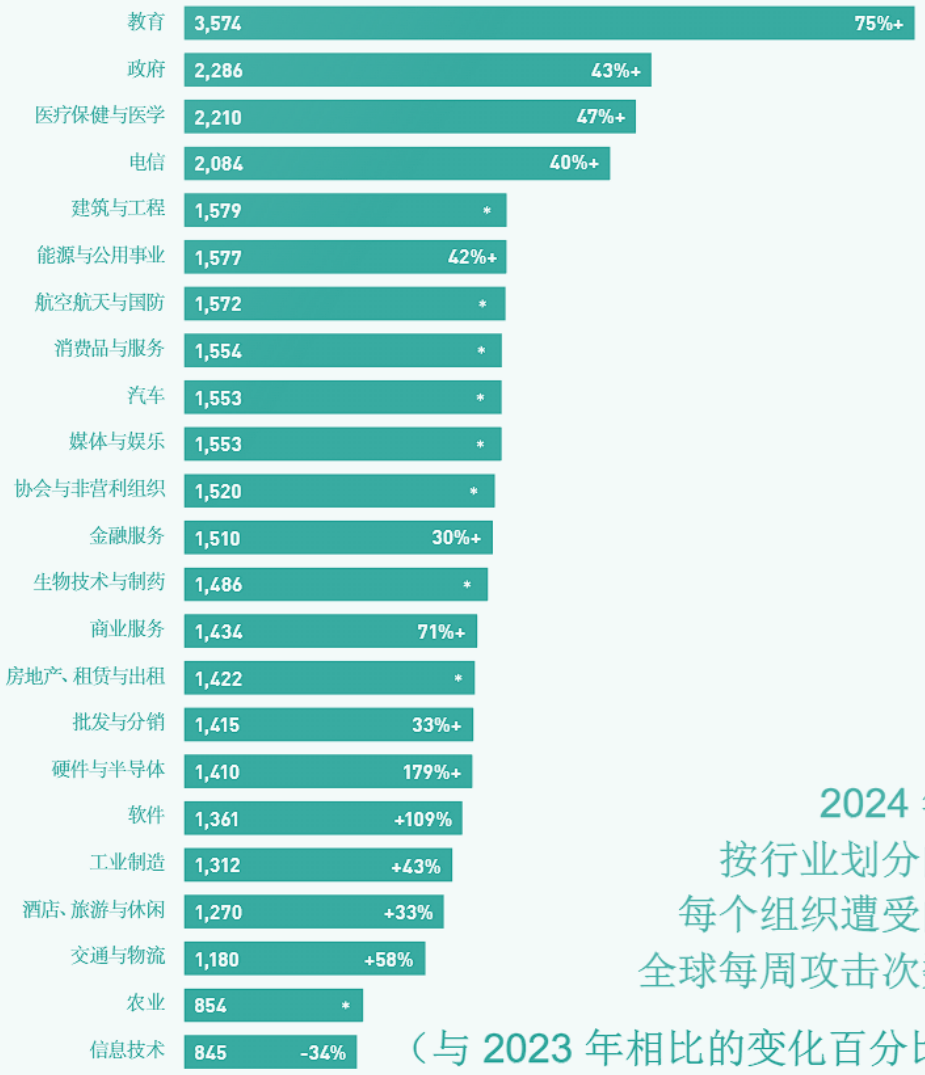
2024勒索攻击目标行业TOP 10

商业服务	零售	制造	建筑	金融
1302	820	573	287	257

医疗健康	教育	政府	科技	交通
248	204	191	174	163

来源：Check Point-2025网络安全报告

各行业勒索态势严峻



教育行业

高校的网络环境规模庞大且复杂，传统的网络安全建设难以有效抵御勒索。此外高校还面临的学生、教师等群体安全意识和信息安全技能水平参差不齐，流程与制度不够完善等问题。勒索病毒对高校保有的大量高价值科研数据带来威胁，并且高校也是黑客窃取个人信息的重点对象，勒索将导致大量个人信息泄露。

医疗行业

医疗行业的业务系统众多且相对独立，因此各类系统的安全防护非常依赖供应商，而供应商的安全能力通常较弱，无法及时修复漏洞。由于医疗业务系统与患者生命安全高度关联，对中断几乎是零容忍，并且医疗业务系统包含患者就诊记录、病例、个人隐私等敏感数据，业务中断、数据泄露带来的后果十分严重。

制造业

制造业通常因预算有限、缺乏安全人员与技能等原因导致安全防护薄弱，而汽车、半导体等高端制造业的生产已经高度自动化，并且由于制造业上下游呈链条式关联，即使只是其中一个供应商、一条生产线遭受勒索攻击，生产中断导致的交货能力断档将在整个行业引发广泛的连锁反应，造成重大经济损失。

零售业

零售业日常处理超大规模的交易，处理大量资金，并掌握着数百万甚至上亿顾客的银行卡、身份隐私信息。黑客往往选择在节日、大型促销期前对其老旧系统的发起攻击，使商家不仅面临数据安全风险与赎金支付成本，更会因为业务中断导致巨额的销售收入损失，这对高度依赖现金流的零售商可能造成毁灭性灾难。

金融行业

金融业有严格的法规和监管要求，因此其安全防护水平通常高于其他行业。但由于数字化程度高、资产价值高、数据高度敏感等特性，导致其成为勒索主要攻击目标。遭遇勒索攻击后，为保护敏感数据并维护声誉，其更有可能被迫支付巨额赎金。并且金融机构间关联密切，勒索可能导致整个金融体系出现连锁反应。

关键公共事业

随着地缘政治局势逐步升级，近年来能源、电信、水务等关键领域公用事业成为勒索团伙竞相瞄准的主要攻击对象。不法分子企图通过采取更为激进、更具破坏性的攻击手段制造大规模破坏来索取高额赎金。勒索攻击不仅会导致公共服务中断，更会引发公众对能源安全甚至国家安全的信任，造成严重的社会影响。

数据源：Check Point-2025网络安全报告

勒索病毒为何猖獗

vinchin

高额利润

2024年勒索组织累计勒索60亿人民币，利润使其不断发起攻击

匿名支付

匿名支付掩盖了交易者信息，使得执法部门难以进行打击

RaaS

暗网上一个勒索工具包只需要50美元，任何人都可以发起攻击

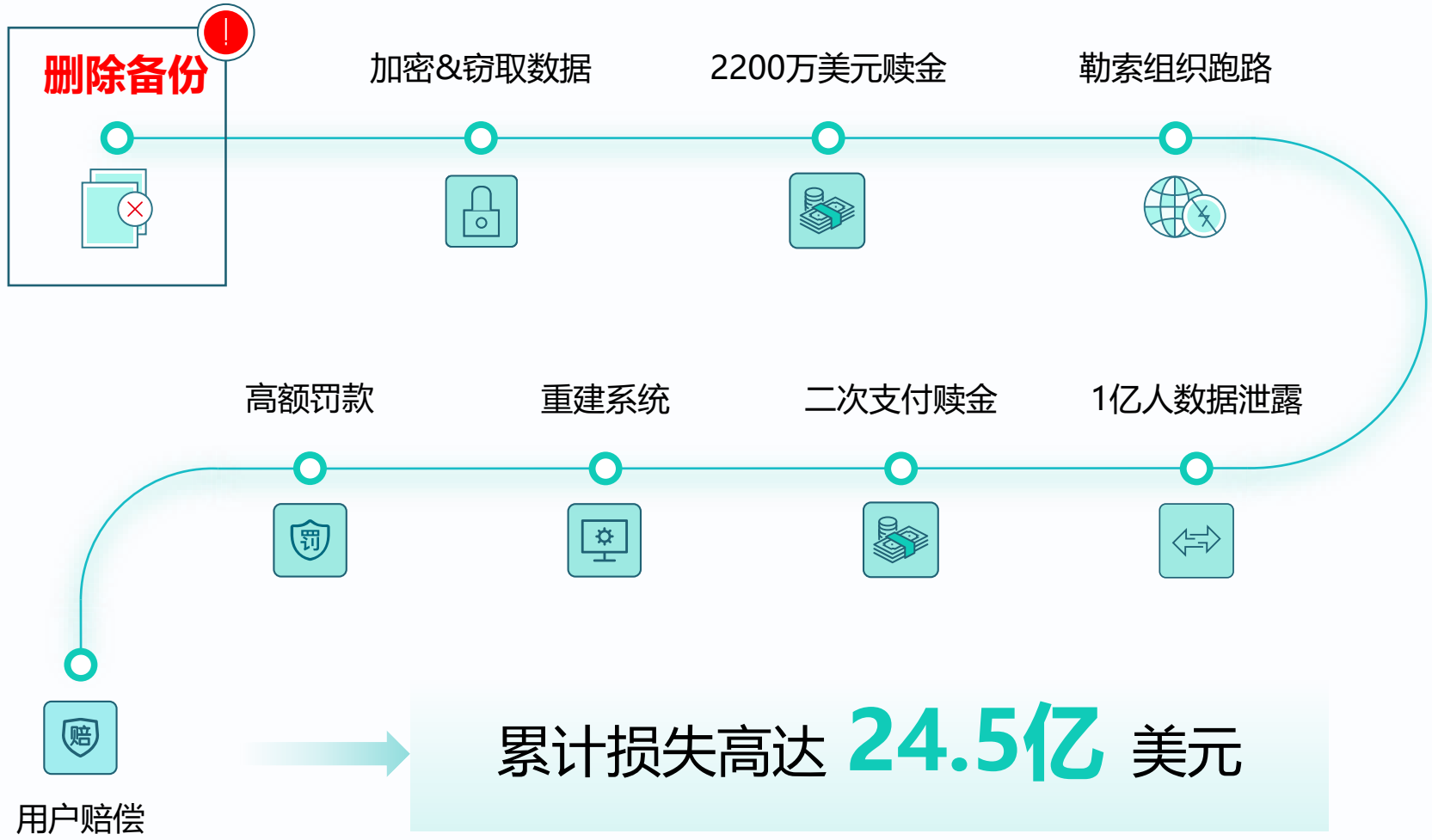
AI驱动

AI技术显著增强了勒索的攻击力，深度伪造使攻击防不胜防

数据安全的最后一道防线“备份”被攻破了

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

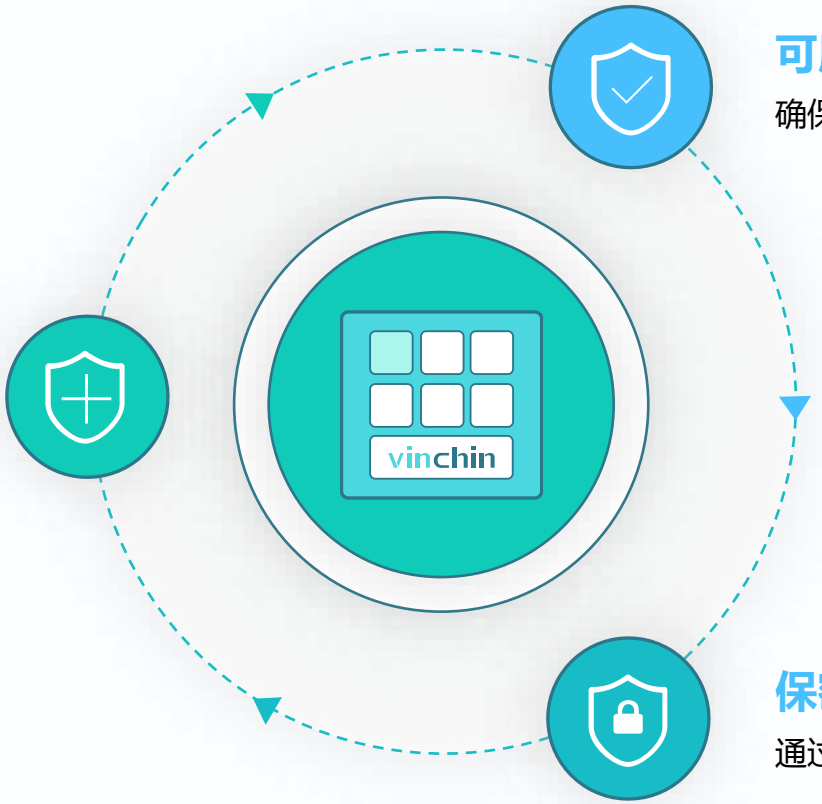
vinchin

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

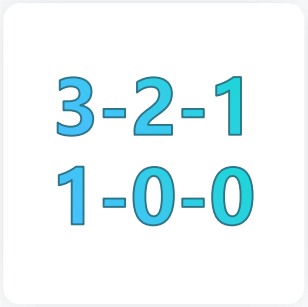
体系化安全防护，防止数据被破坏

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



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

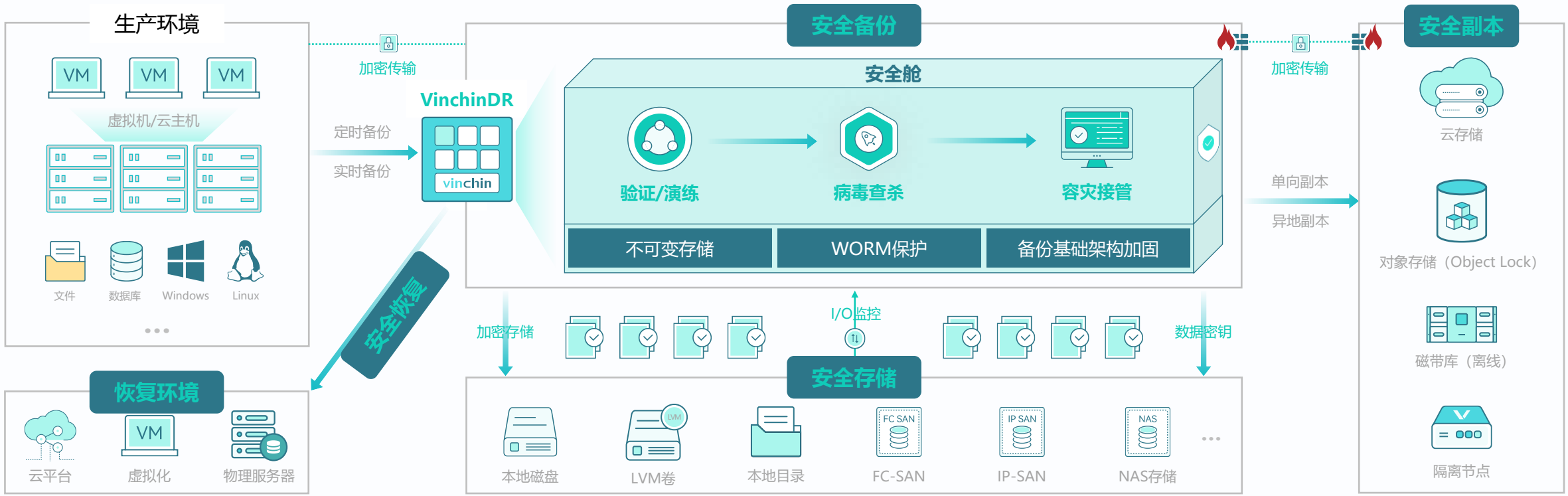
建立完善的灾难恢复管理制度并实施员工培训

云祺防勒索体系

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



不可变备份

主动病毒查杀

安全弹性恢复

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

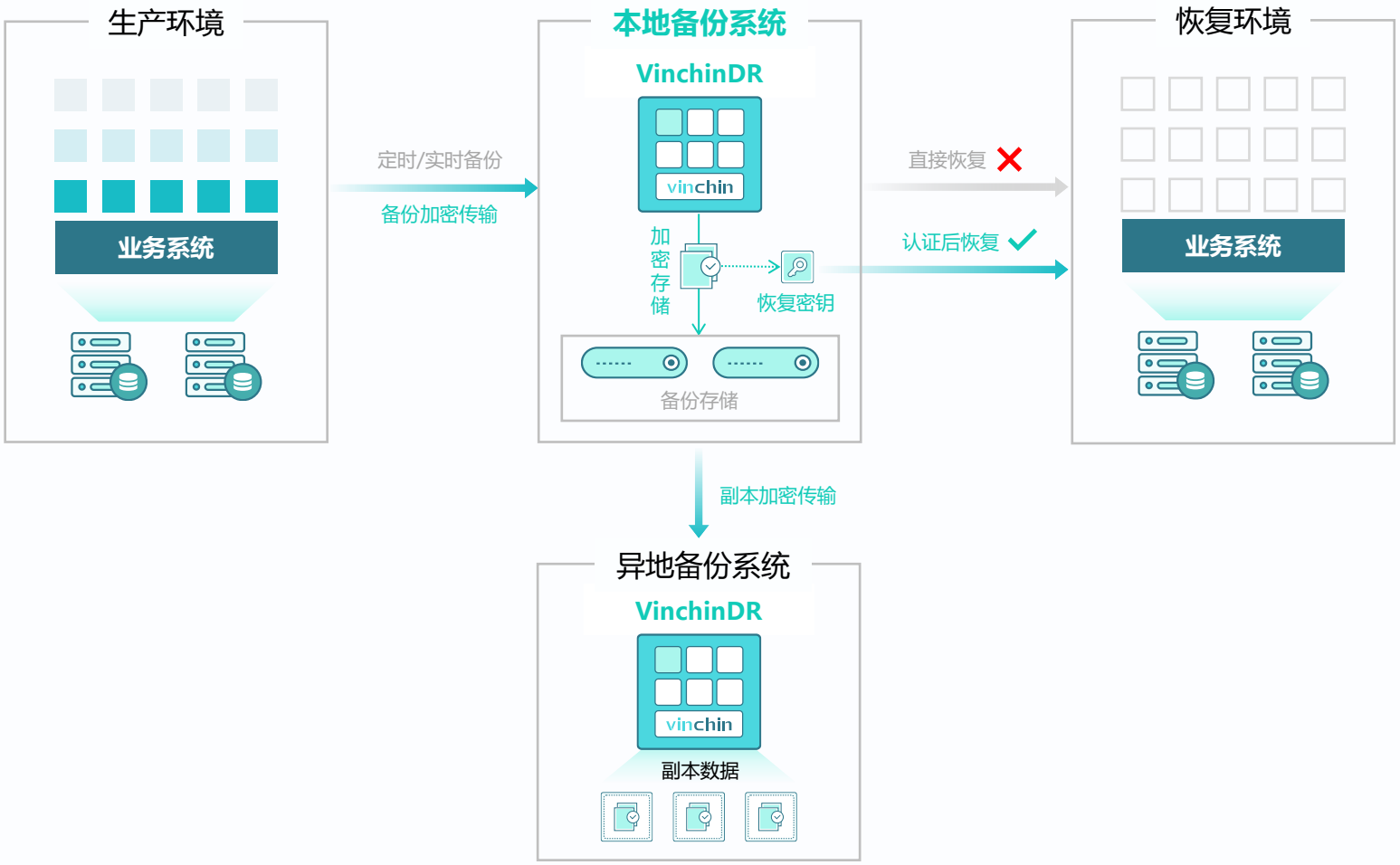
0

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

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

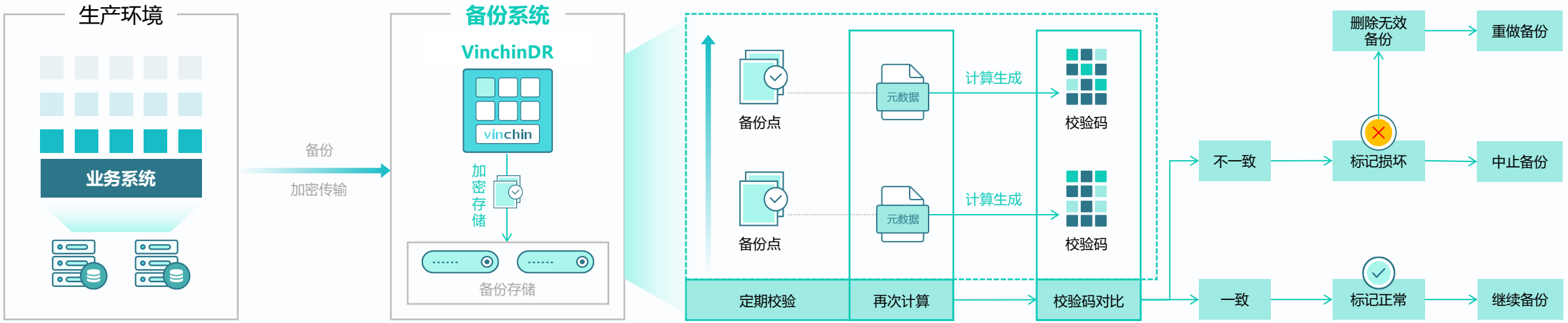
将数据加密后再写入到存储介质，防止恶意软件通过泄露的root账号密码从后台窃取明文数据

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

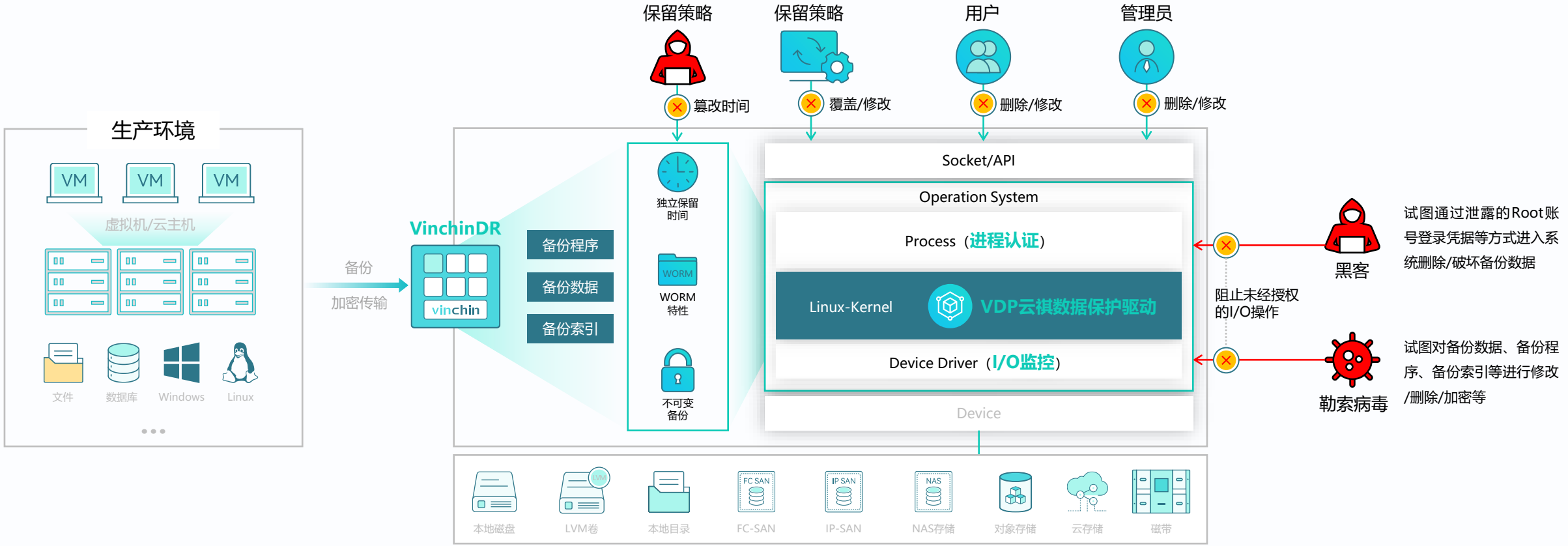
高效校验

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

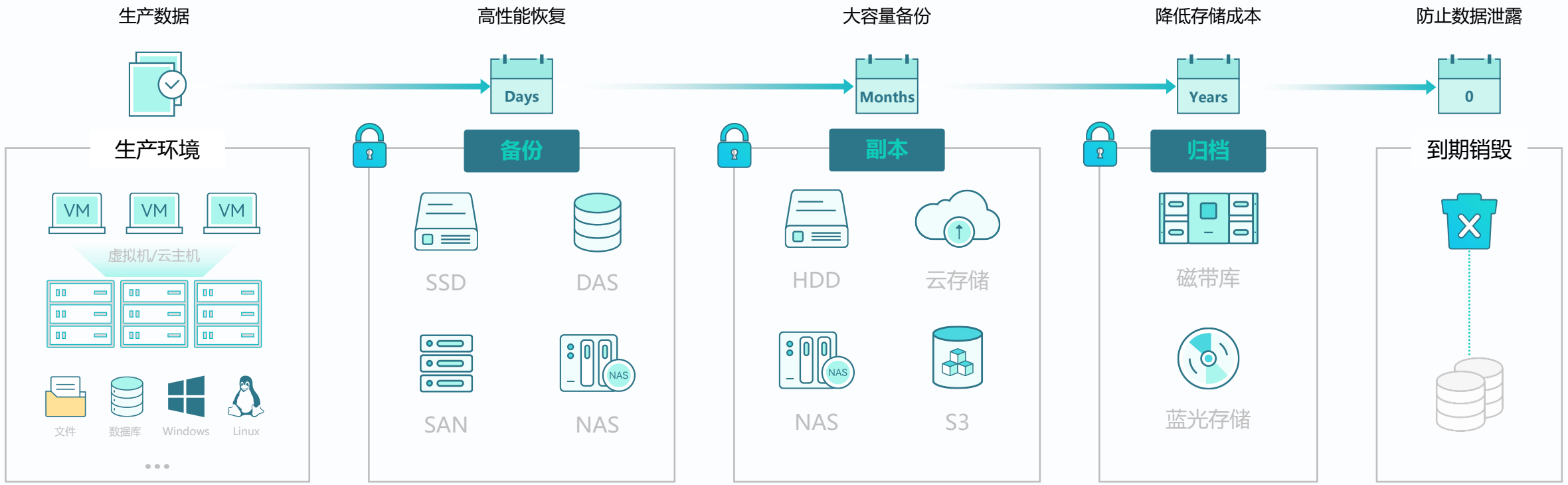
不可变存储：使用原生不可变存储或对象存储Object Lock、物理磁带离线存储等实现备份数据不可变特性

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

覆盖数据生命周期的不可变

vinchin

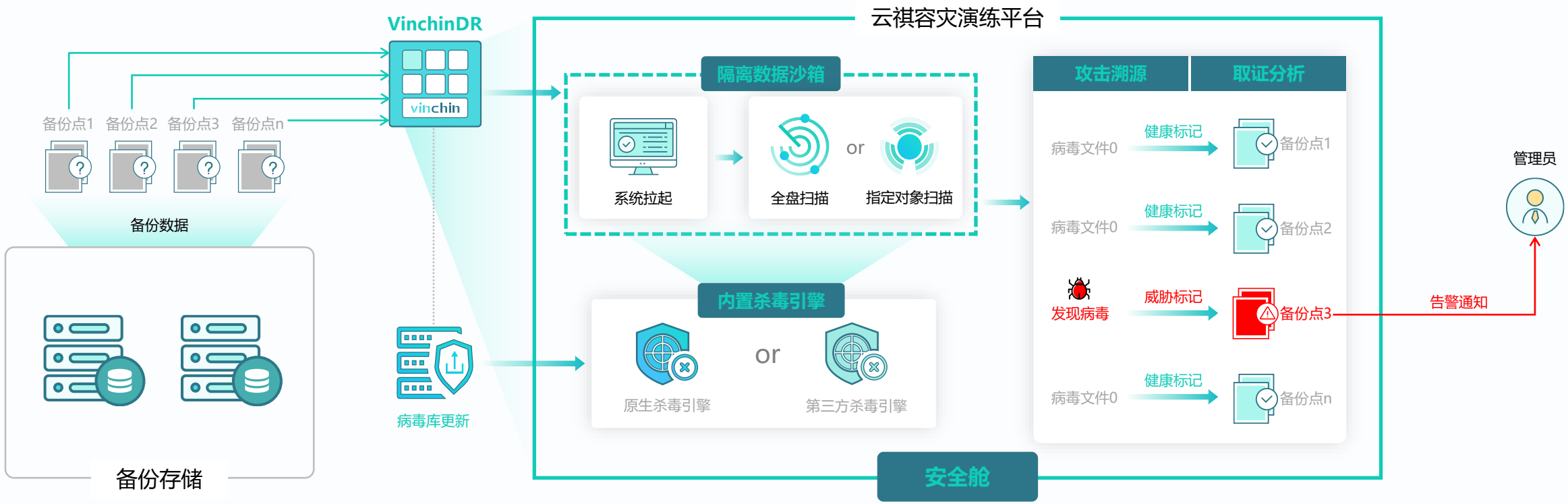
不可变备份 | 全程可持续 | 自动分层 | 横向可扩展 | 降低存储成本 | 满足合规要求



覆盖全程的不可变特性

主动查杀病毒

vinchin



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

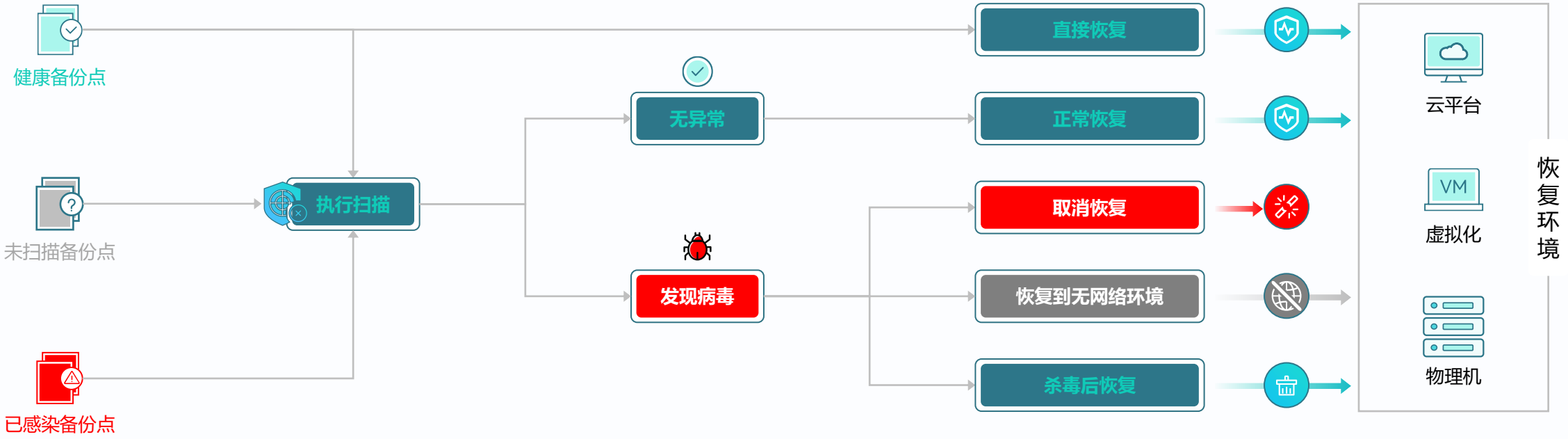
在备份数据中查找干净可用的备份点，为将来的安全恢复做好准备

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。



自动验证与恢复演练，始终确保成功恢复

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。

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

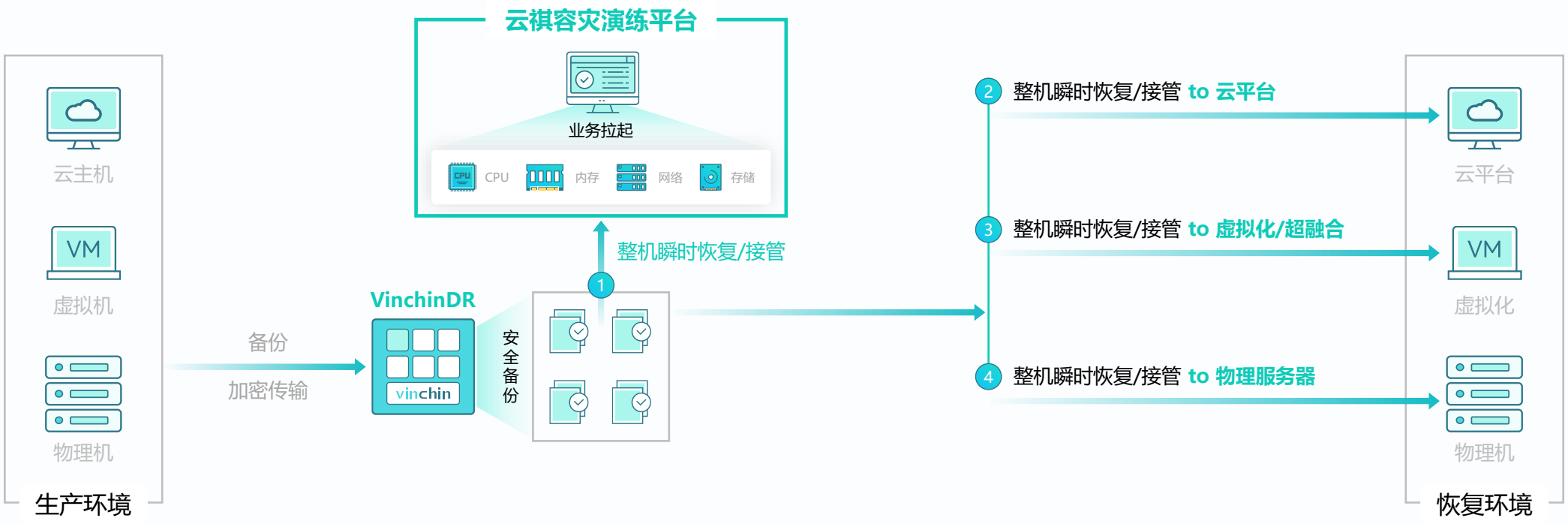
无需人工整理汇总可视化验证报告输出，结果清晰可见

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

快速恢复，业务AlwaysOnline

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

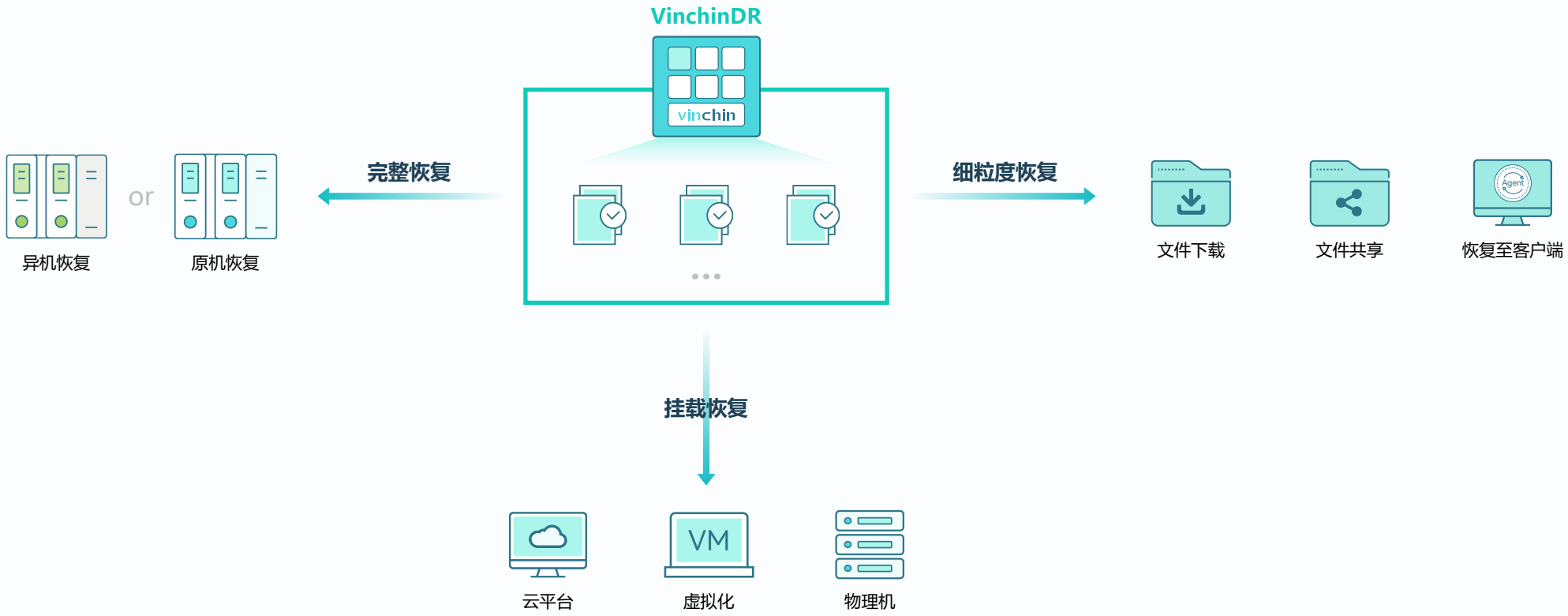
分钟级RTO

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

遭遇勒索攻击时，业务系统可能需要根据重要性、RTO/RPO要求、恢复资源位置等实际情况选择不同的恢复方式，因此，提供丰富的恢复手段或选项将使用户可以从容应对复杂的恢复场景，并提升恢复效率和成功率。



跨平台弹性灾难恢复

vinchin

当遭遇勒索攻击，尤其是出现平台级勒索灾难时，恢复可能受到异构数据格式差异、驱动缺失、系统引导损坏等诸多环境因素的限制，最终导致无法成功恢复业务。因此，提供完善的跨平台灾难恢复能力有助于进一步提升勒索恢复的效率和成功率，增强业务韧性。

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

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

第三方
集中管理平台

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

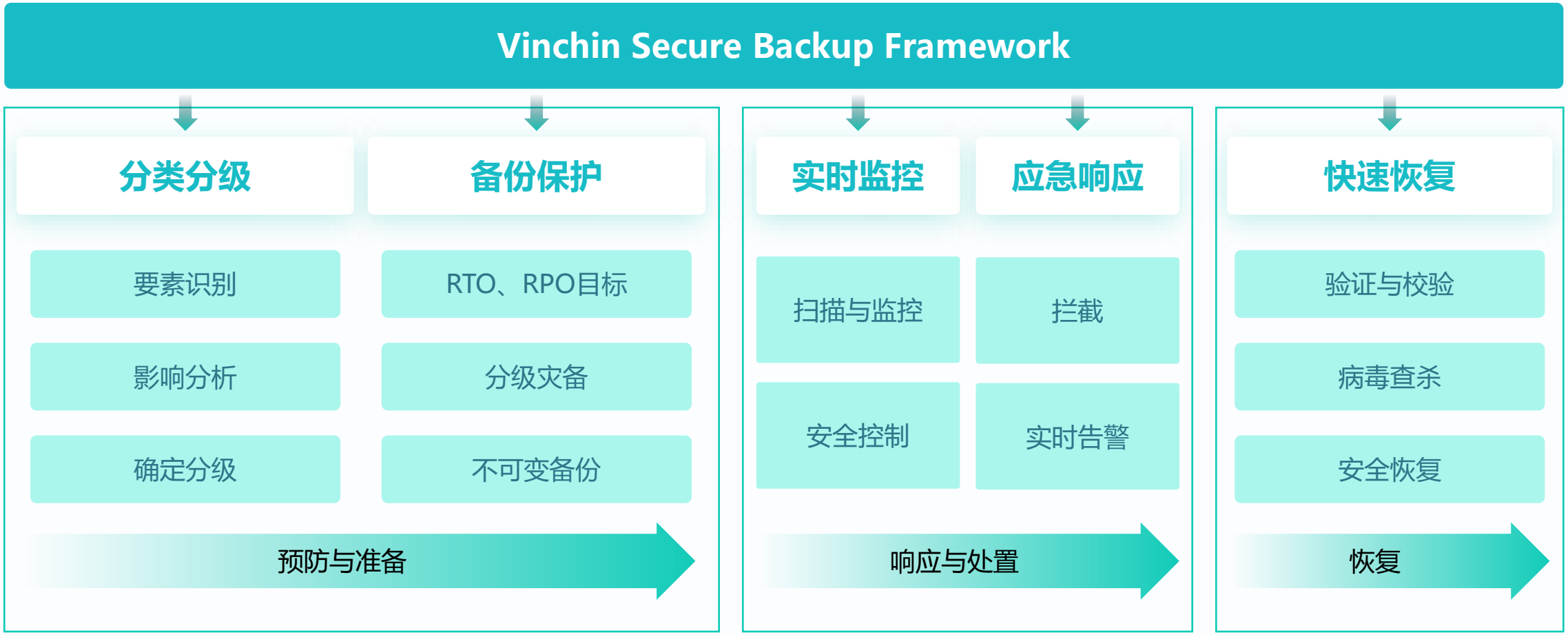
上报
安全事件

发送
告警通知

邮箱

企业微信

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

THANKS

云祺公众号

云祺视频号