近年典型勒索事件

vinchin

黑客勒索 4800 万：无力支付、破产、700 人失业。。。只因密码太简单。。。

大单网 云头条 2025年07月23日 23:30 河南

一家拥有 158 年悠久历史的英国运输公司在遭到勒索软件攻击后不幸倒闭。

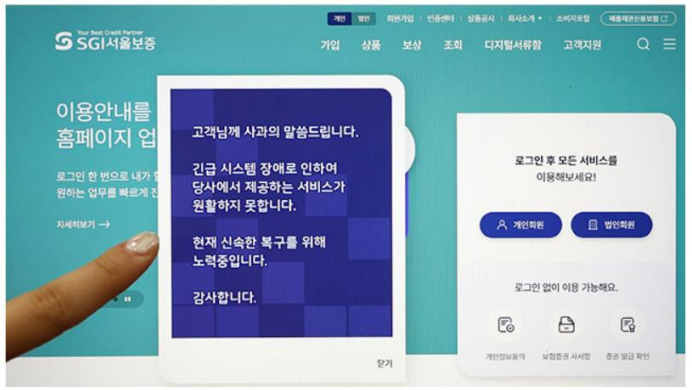
Knights of Old（KNP）位于北安普敦郡的约 500 辆卡车目前无法上路，700 人丢掉了饭碗，这一切都归咎于"Akira"的嗜钱如命的网络攻击者。

据称，这伙网络犯罪分子通过 KNP 的一名员工使用的弱密码入侵了该公司的互联网系统。

实际上，这个密码太弱了，很容易被猜到。

7月14日，据多家俄媒报道，俄罗斯酒业巨头 Novabev 遭遇勒索软件攻击，**导致旗下超 2000 家连锁门店被迫暂停营业**，销售系统和线上服务全面中断，物流发货等均受到影响。

7月14日，韩国最大的信用担保机构首尔保证保险株式会社（SGI）遭遇勒索软件攻击，导致其核心系统持续瘫痪三天，住房抵押贷款、传贳贷款、消费贷款等担保服务中断，仅**当天就有近 600 亿韩元（约合 4300 万美元） 的租赁贷款因无法担保被迫延期发放。**



SGI 是韩国最大的信用担保服务提供商，**专为个人和企业提供各类金融担保，包括住房租赁押金保险、月租贷款、分期付款信用保证等。**

加拿大新斯科舍电力公司披露称，自4月下旬遭受勒索软件攻击以来，客户侧的电表通信一直不畅；

公司最初暂停计费，近期准备开启计费账单，将派出抄表员入户抄表以提供准确账单，未能抄表的客户将提供预估账单。

跨国IT分销巨头英迈遭勒索攻击，业务服务已瘫痪近一周，官方最新公告称目前攻击已被遏制，受影响系统已得到修复，正在努力恢复上线；

由于服务瘫痪，大量客户无法在线提交订单，官方后续称中国等部分国家的订单已可通过电话或邮件处理；

关键供应商Synnovis遭勒索软件攻击，导致英国伦敦多家医院血检受影响，一名患者因等待时间过长不幸死亡。

vinchin

勒索病毒如何一招毙命?

用云祺构建数据安全的“钢铁壁垒”

云祺科技-产品中心

vinchin

目 录

vinchin

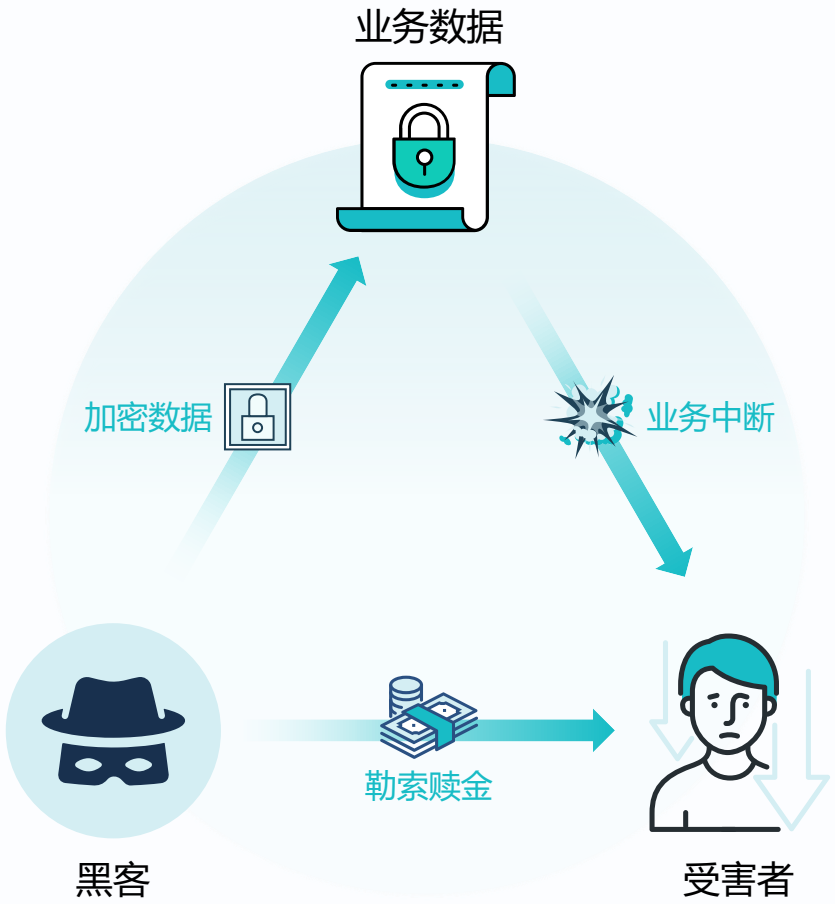
PART 01

什么是勒索病毒

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。

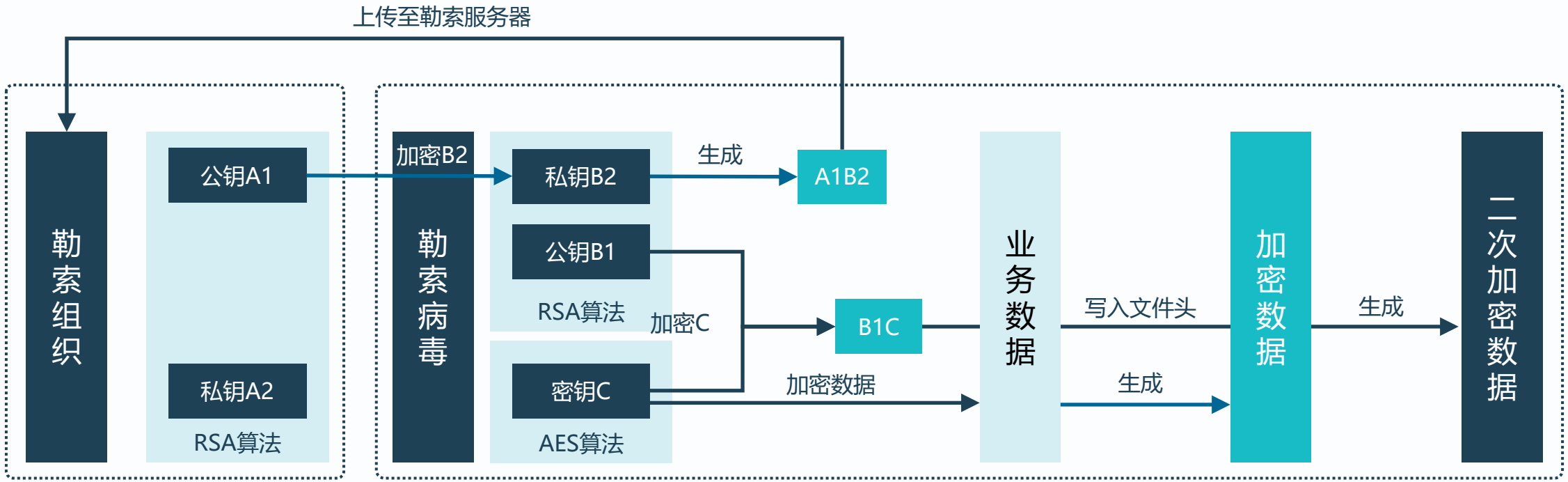
> 勒索攻击给受害者带来的影响是多方面的，除了需要支付高额赎金外，业务中断、声誉受损等问题也会接踵而至，更严重的是，违反数据安全法规可能导致严重的法律后果。

勒索病毒加密原理

vinchin

公钥：用于数据加密

私钥：用于数据解密



勒索软件采用高强度对称算法（对数据加密）和非对称加密算法（对密钥加密）对数据进行多重加密，除非勒索软件在实现上存在漏洞，否则在没有私钥的情况下几乎不可能破解。

勒索攻击无孔不入

vinchin

诱导受害者点击邮件链接或邮件附件，点击后，勒索病毒将自动下载和运行

网页投放广告并植入植入恶意链接，点击、访问触发下载勒索病毒

伪装成PE类文件，一旦受害者将其插入设备，即可自动感染设备

分析上网行为，在常访问的网站中植入恶意代码，一旦访问即会“中招”

利用系统和软件漏洞，通过漏洞攻击包（Exploit Kit）检测后传输病毒。

被不法分子通过僵尸程序操纵的机器组成的网络，勒索病毒传播主要途径

盗版软件中植入后门，受害者一旦下载安装，即可感染设备或系统

将勒索病毒伪装上传至网盘、QQ群、等分享给他人，诱导其下载

利用受害者对软件供应商的信任，劫持软件安装、升级更新等过程

扫描设备的高危端口，对弱口令进行暴力破解完成入侵，以便后续执行勒索

vinchin

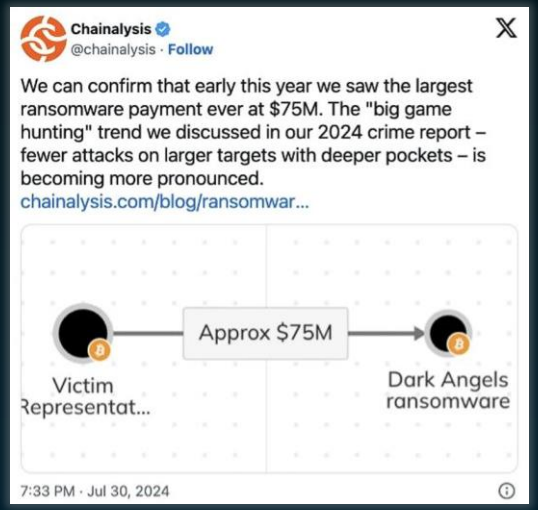
PART 02

勒索威胁形势严峻

勒索攻击攻击形式严峻

创记录的7500万美元赎金！

2024年，加密情报公司Chainalysis证实，一家财富50强公司向勒索软件组织Dark Angels支付了破纪录的7500万美元赎金，这成为目前已知的最高赎金支付金额。



大小通吃：37%的企业每天面临网络威胁，被勒索攻击的企业中，中小企业占比超80%，年均损失约145万美元

损失严重：如金融行业因网络攻击类导致近6年累计损失323亿美元，金融安全事件正以每年约 35% 的速度增长，涉及银行、保险、基金、证券等众多领域

威胁加剧：在2022年，勒索攻击平均约每11秒发生1次，而在2024年，平均约每7秒发生一次，平均停机时间达24天

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

任何人都可在暗网购买勒索服务发起攻击，而无需任何额外操作

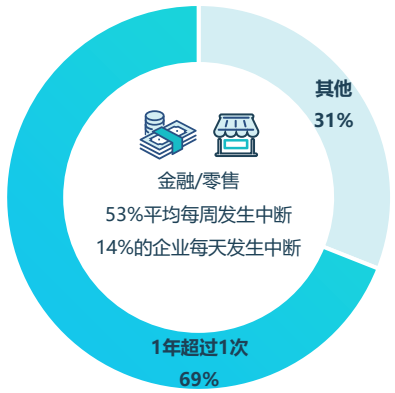
AI驱动

AI技术显著增强了勒索的攻击力，深度伪造等使攻击防不胜防

业务中断损失重大

vinchin

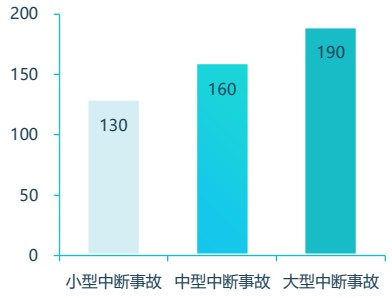
多数企业每年遭遇业务中断



业务中断频次统计

数据源：*New Relic-2024 Observability Forecast*

中断损失10万美元/hour



业务中断损失中位数统计（万美元）

数据源：*Cockroach Labs-The State of Resilience 2025*

业务中断使企业面临多重损失

44%

生产经营损失

生产停滞、工作流程中止或进度缓慢、产品或服务订单交付能力受限等导致的直接收入损失

17%

恢复/重建成本

硬性的恢复资源与环境成本、无法预估的人力投入以及无法保证完整恢复的技术支持服务支出

39%

其他隐形损失

品牌声誉损失以及客户信任流失将造成长期财务影响，违规罚款、甚至吊销营业执照以及面临法律风险

软硬件故障、网络攻击、人为误操作、自然灾害以及勒索病毒等安全威胁导致业务中断，再发生业务中断的企业中，绝大部分企业营收都会受到影响，其中34%的企业收入大幅下滑，而12%的企业则因客户赔偿、订单锐减、高额罚款、吊销许可等导致停业或倒闭

业务中断使安全团队面临个人风险

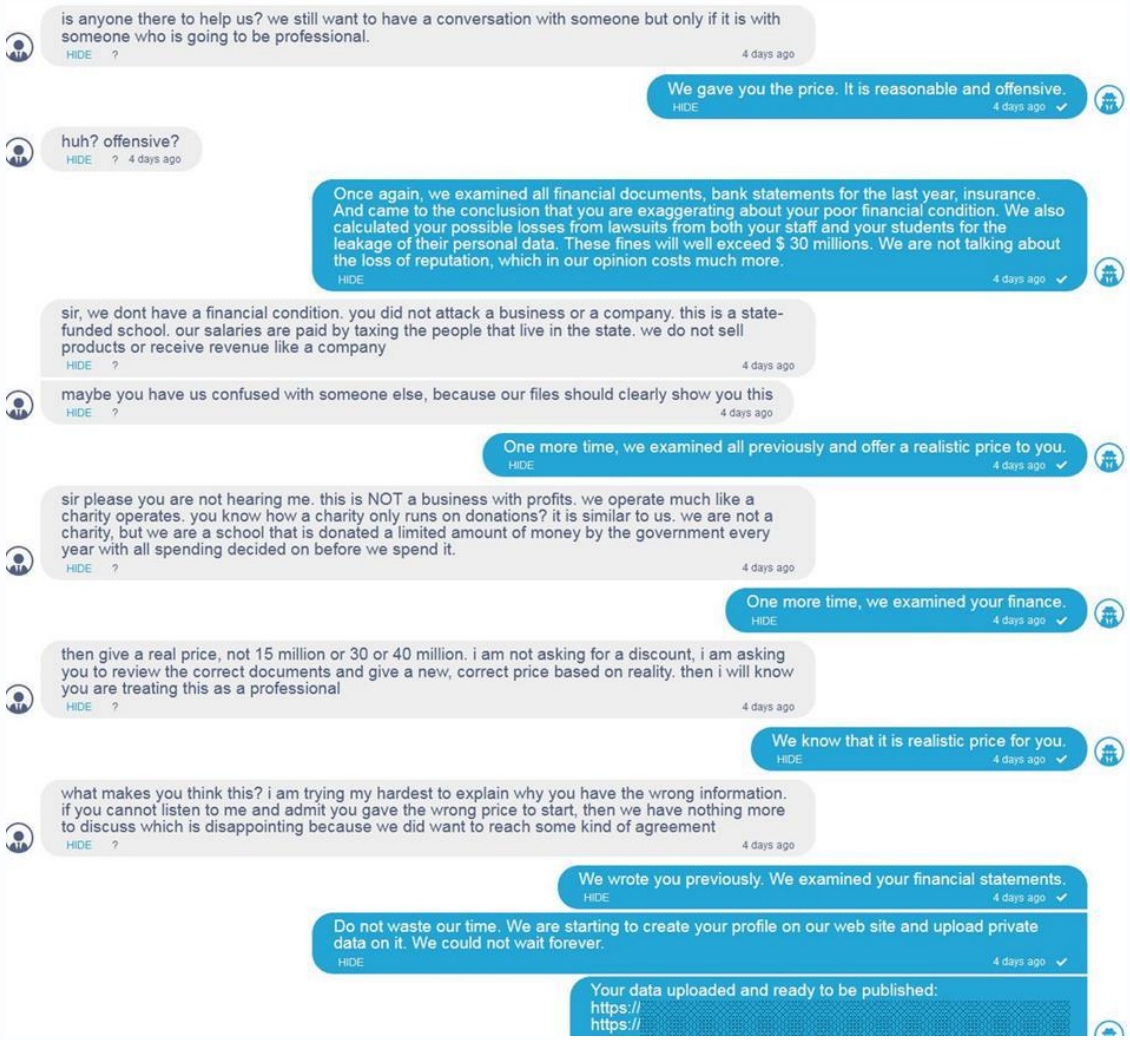
失职问责

精神压力

降职/解雇

法律责任

勒索气焰愈发嚣张



难以拒绝的勒索金额

勒索病毒成功潜入系统后，会分析企业和组织财务数据、交易信息，以此衡量赎金的价码，给出一个受害者容易接受的金额，实施精准勒索

使用法律勒索恐吓

勒索组织在发起攻击前，会研究高价值用户所在国家和地区的合规、监管相关的法律法规，以此加大勒索的恐吓力度，迫使受害者出于规避处罚的心理缴纳赎金

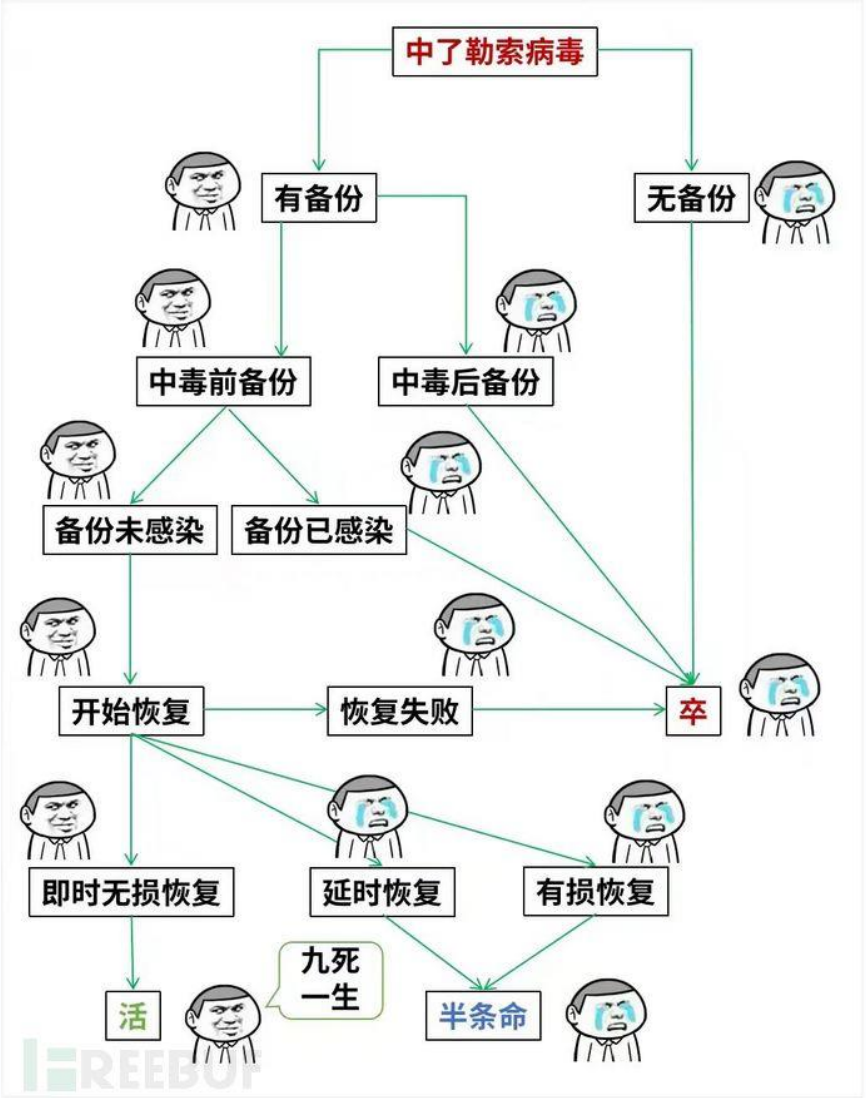
vinchin

PART 03

传统备份的勒索困局

传统备份“九死一生”的恢复

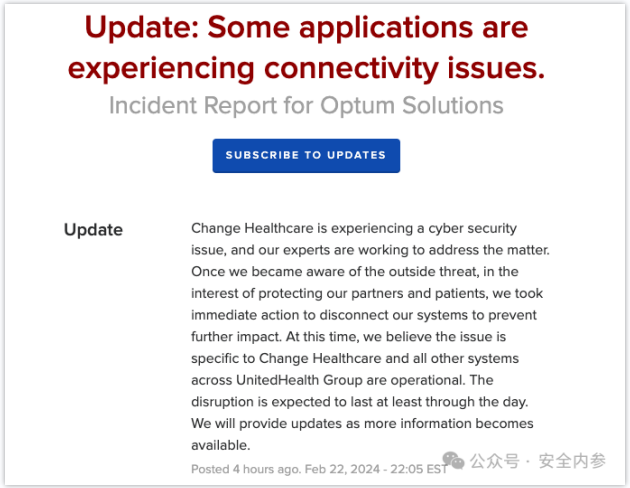
vinchin



如何应对勒索

vinchin

第一步：不要为不确定的结果支付赎金



Change Healthcare被攻击

犯罪分子收到赎金后跑路

受害者再次发生数据泄露

根据全球安全公司卡巴斯基进行的一项涉及15,000名消费者的全球调查，超过一半的勒索软件受害者支付了赎金，但只有四分之一完整找回了数据，有13%会丢失所有数据。即使网络犯罪分子良心发现提供解密程序，解密并恢复所有系统也将花费大量时间，并且解密程序是否能够解密也没有保证。支付赎金不仅对找回数据没有帮助，反而会鼓励、助长勒索气焰。

如何应对勒索

研究表明，备份是比支付赎金更便宜的恢复加密数据的方法。在所有遭受勒索攻击的受害者中，通过备份来恢复数据的成本相比支付赎金来恢复数据成本**便宜50%以上**。

第二步：通过备份恢复数据

没有100%有效的防御体系，中了勒索说明所有的前置防御措施均已失效，此时最紧要是恢复数据，因此需要思考以下几个问题：

有没有备份数据

备份为勒索后的恢复提供保障，如果没有备份，恢复难上加难

备份数据是否安全

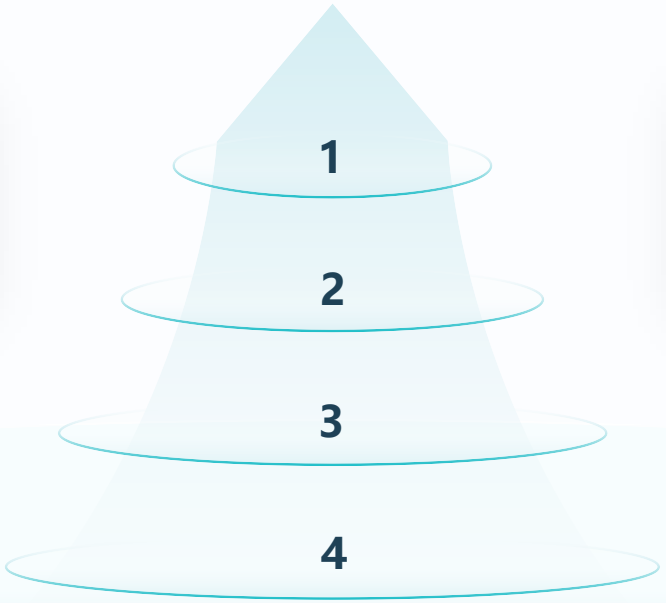
备份数据或备份存储如果遭到破坏，恢复预期将大大降低

如何快速恢复数据

如果不能尽快的恢复数据和业务，业务中断将带来更多损失

如何避免二次感染

备份数据可能潜伏勒索病毒，不加处理的恢复可能再次受害



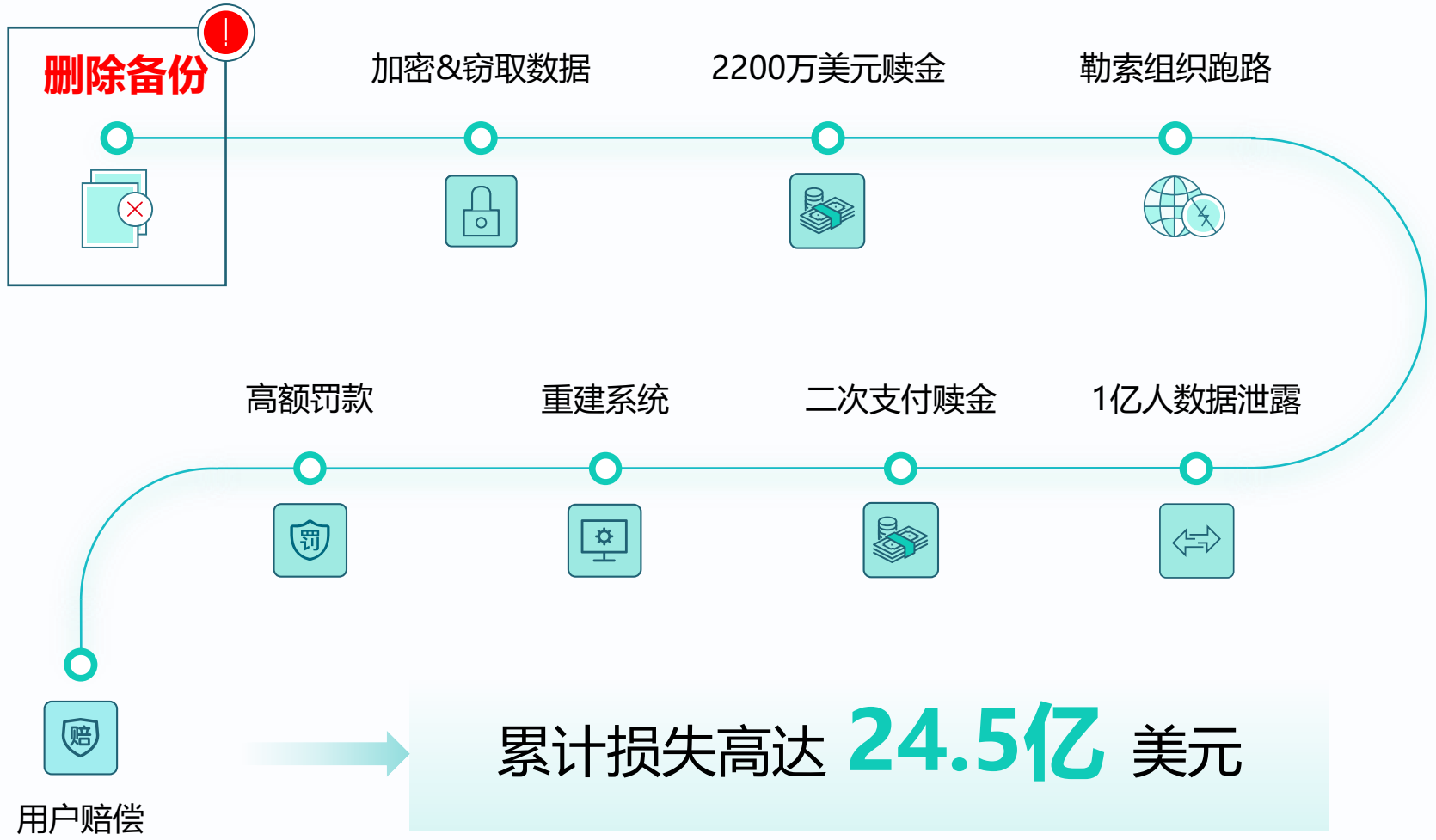
如何快速、安全的恢复所有数据

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

勒索病毒攻击流程

vinchin

探测侦察 → 攻击入侵 → 病毒植入与扩散 → 实施勒索 → 完成勒索

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

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

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

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

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

vinchin

安全备份才是数据安全的最后一道防线

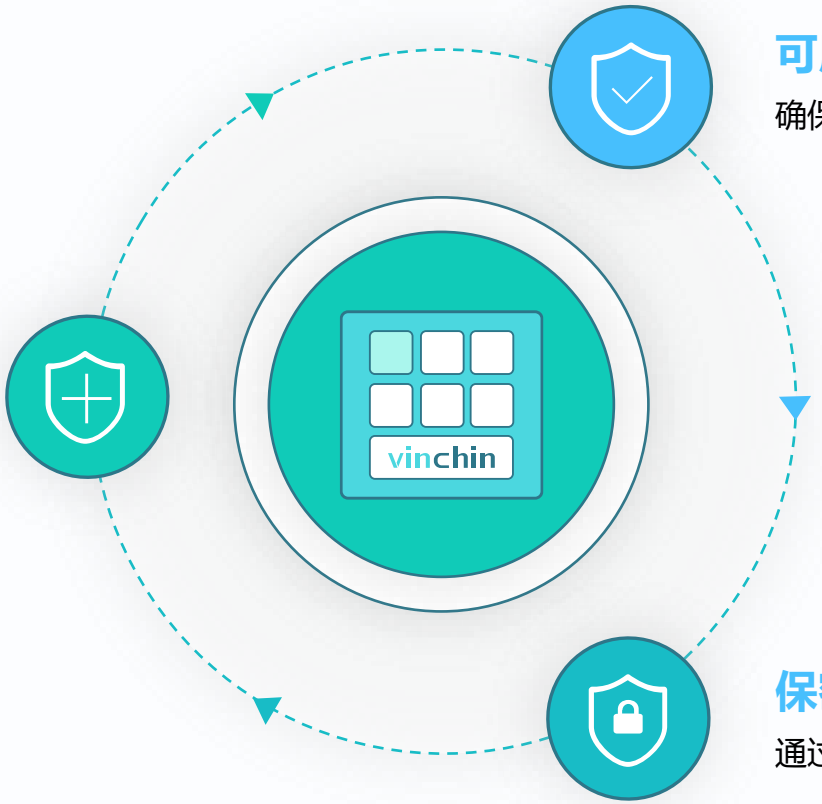
vinchin

PART 04

安全备份体系，从容应对勒索

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

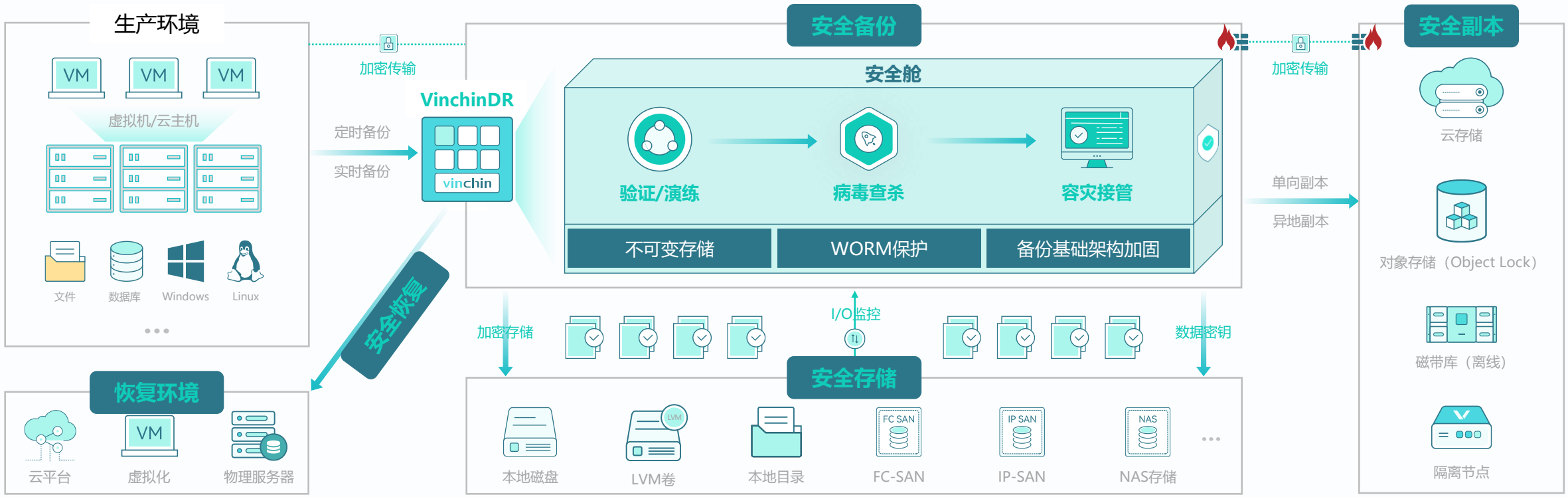
建立完善的灾难恢复管理制度并实施员工培训

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

vinchin

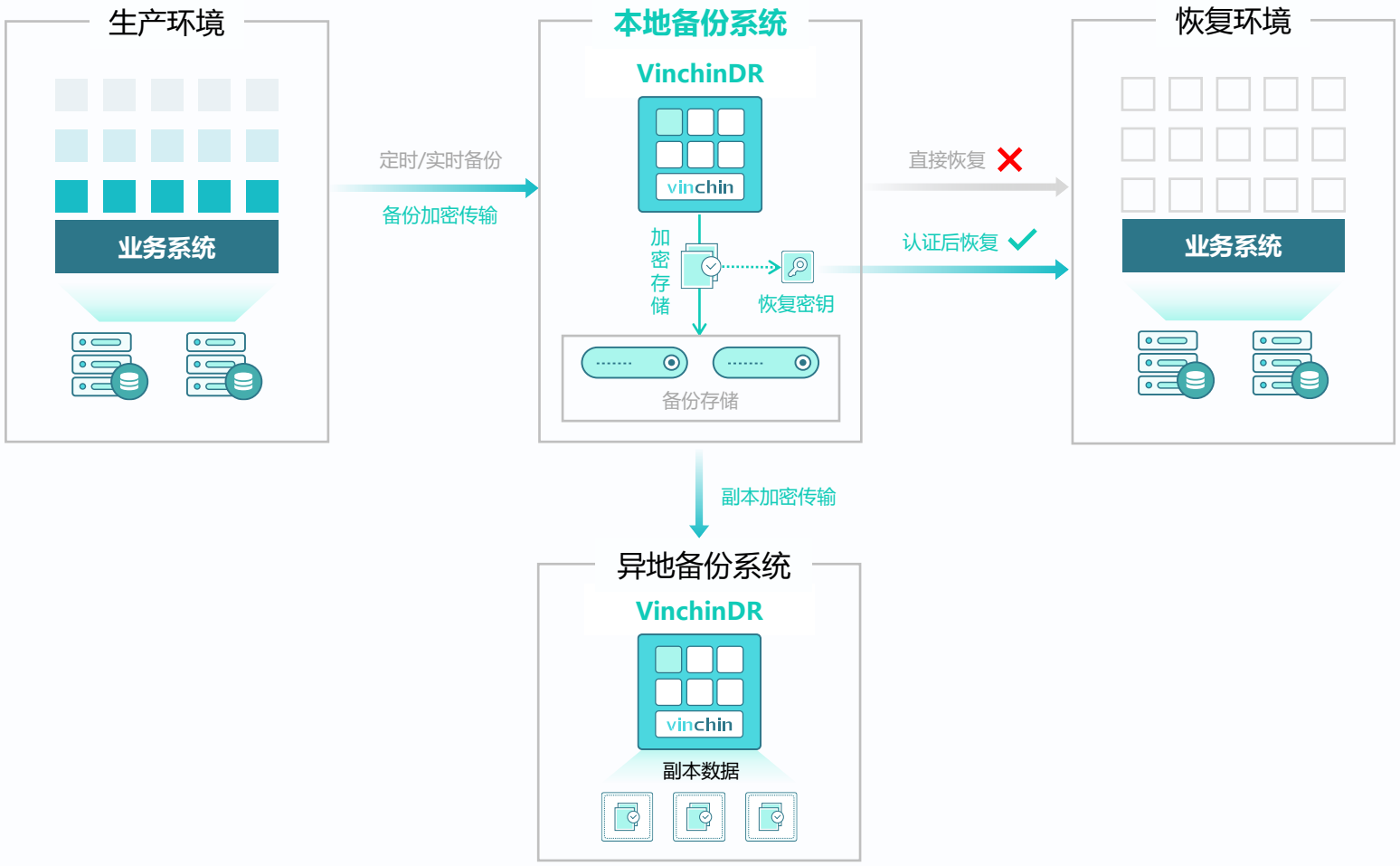
PART 04

云祺安全备份优势与价值

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

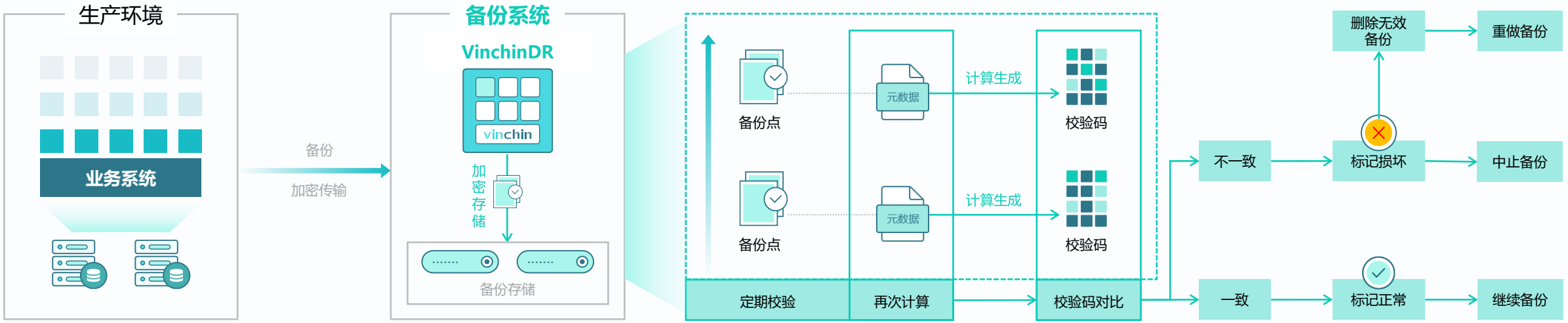
将数据加密后再写入到存储介质，防止恶意软件通过泄露的root账号密码从后台窃取明文数据

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

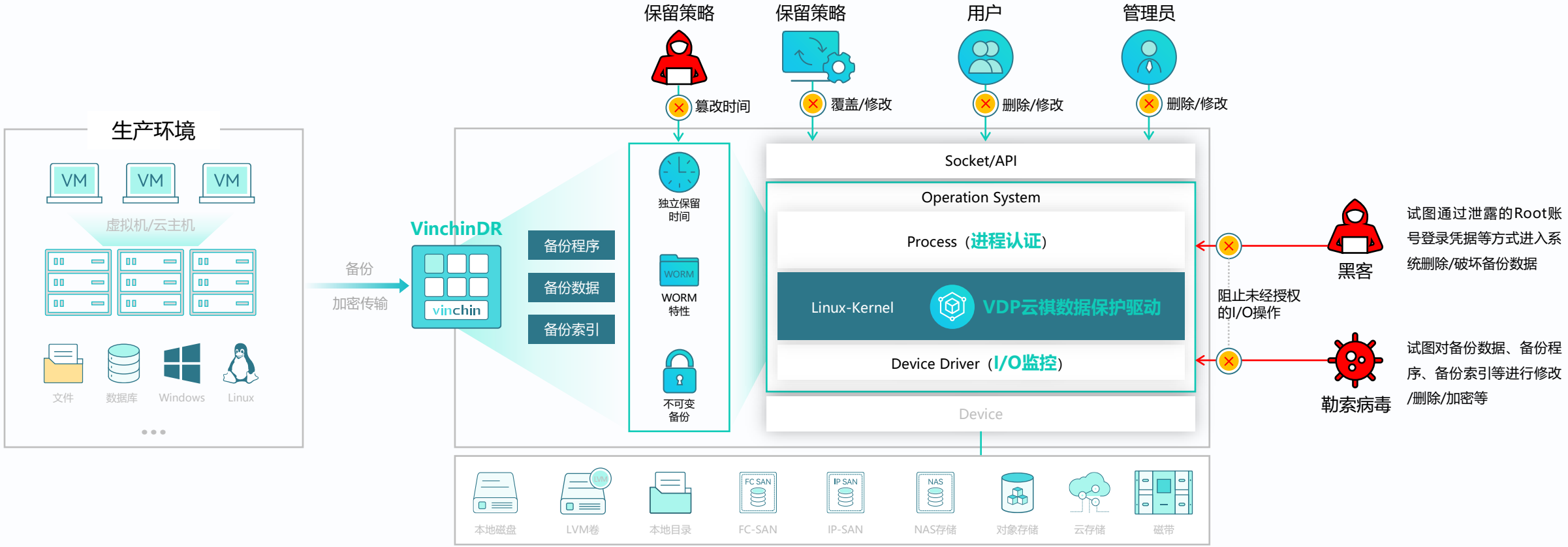
无需校验整个备份链的所有数据，仅校验对比元数据，几乎无性能消耗，海量备份数据场景校验更高效

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

vinchin



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

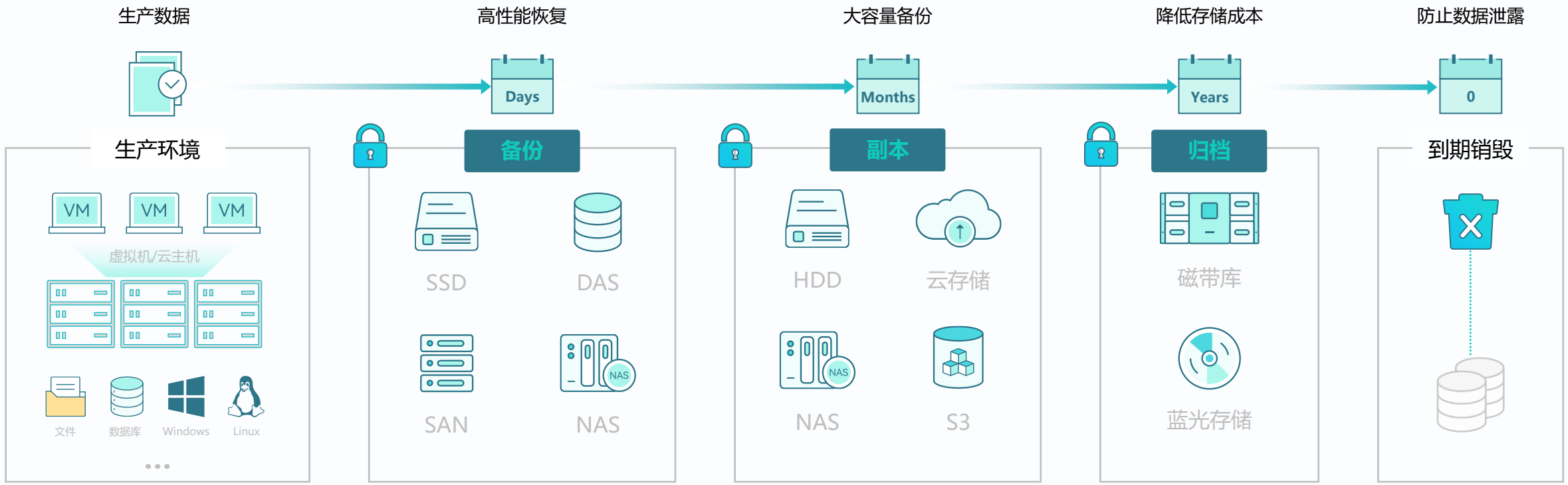
不可变存储：使用原生不可变存储或对象存储Object Lock、物理磁带离线存储等实现备份数据不可变特性

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

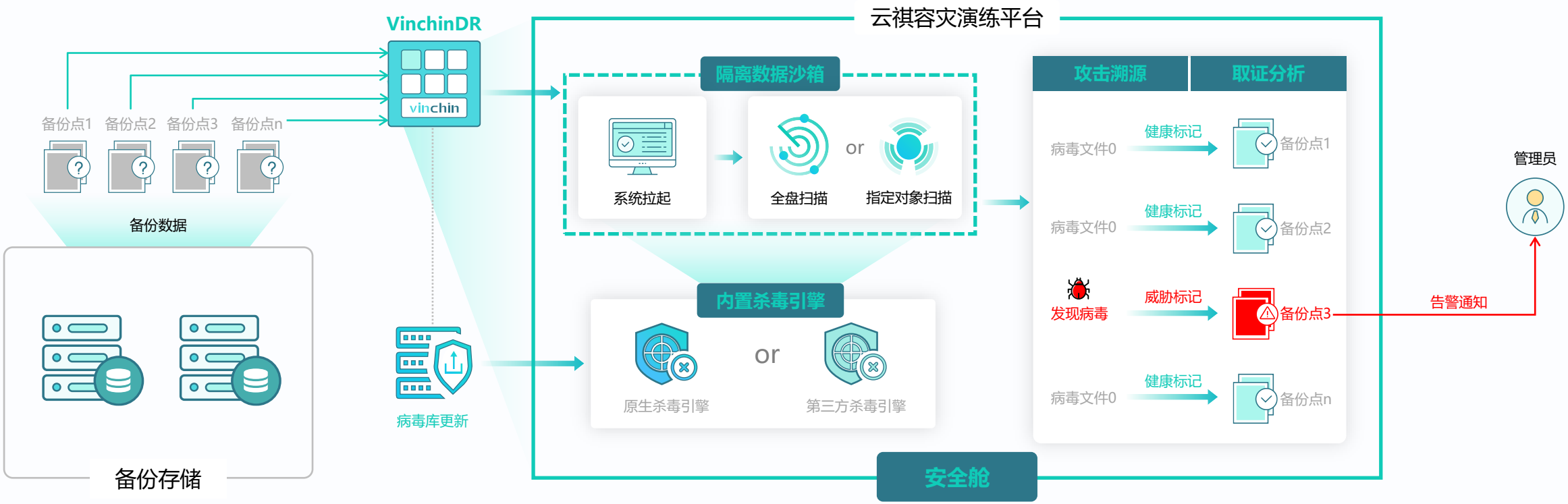
vinchin

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

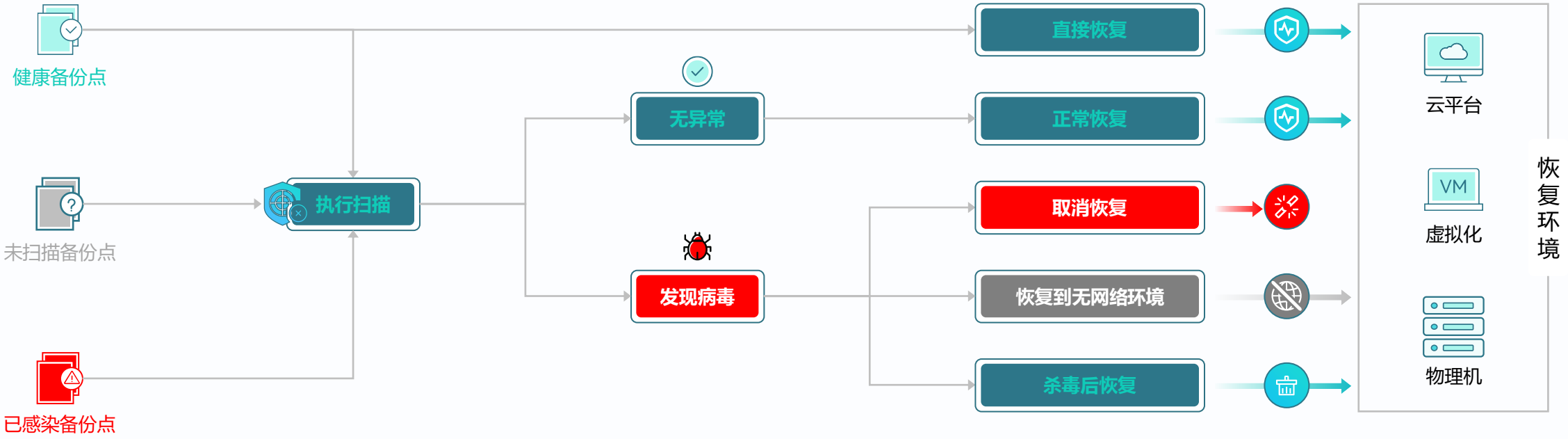
在备份数据中查找干净可用的备份点，为将来的安全恢复做好准备

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。



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

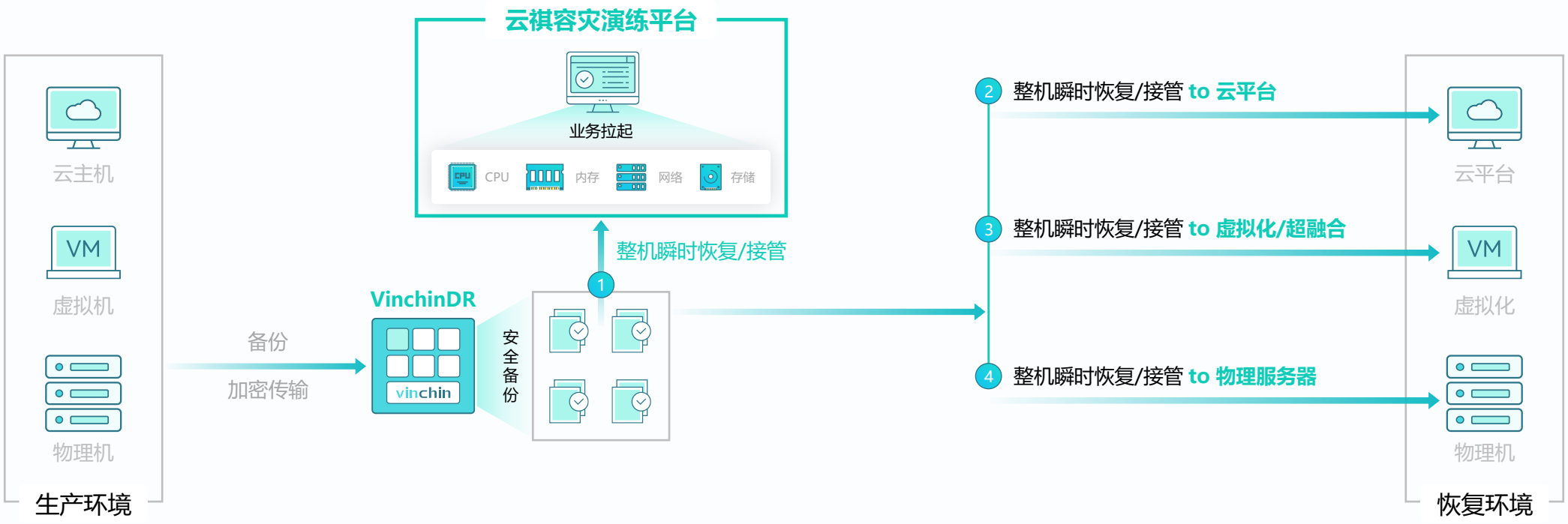
帮助持续改进

根据验证结果持续优化策略，提高数据安全管理水平

恢复快人一步，业务AlwaysOnline

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

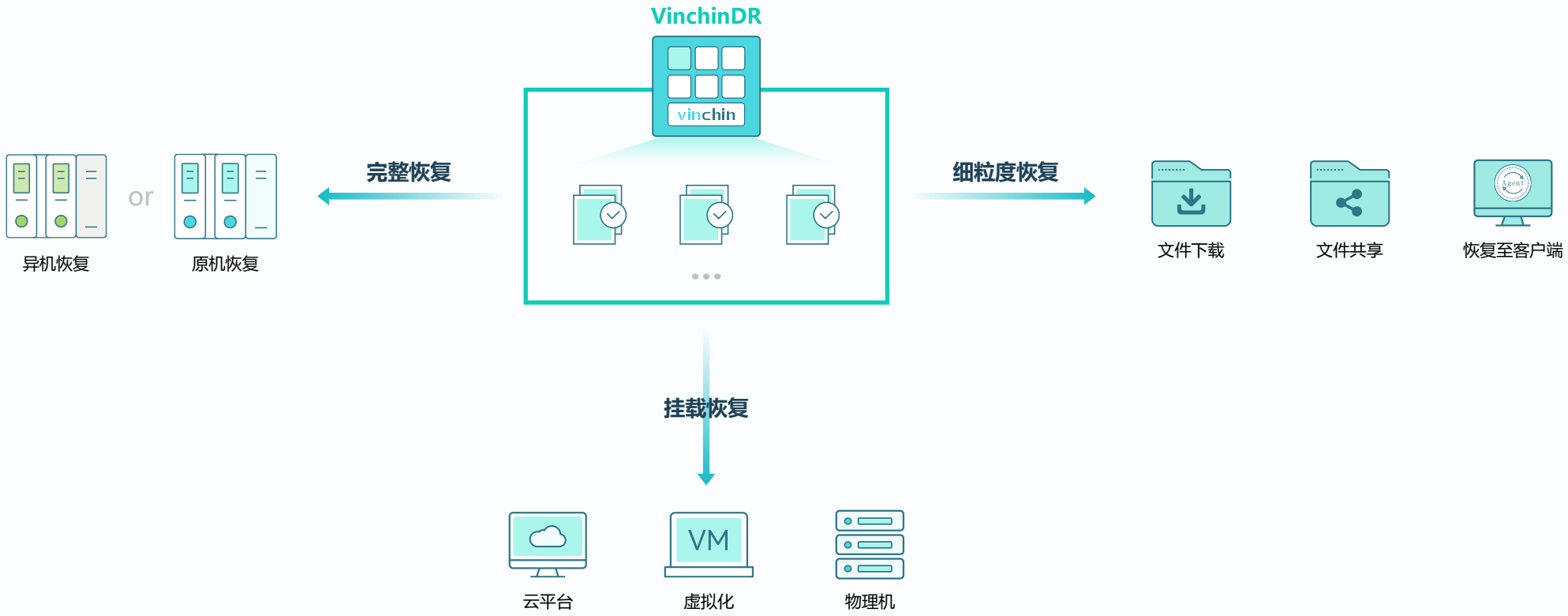
分钟级RTO

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

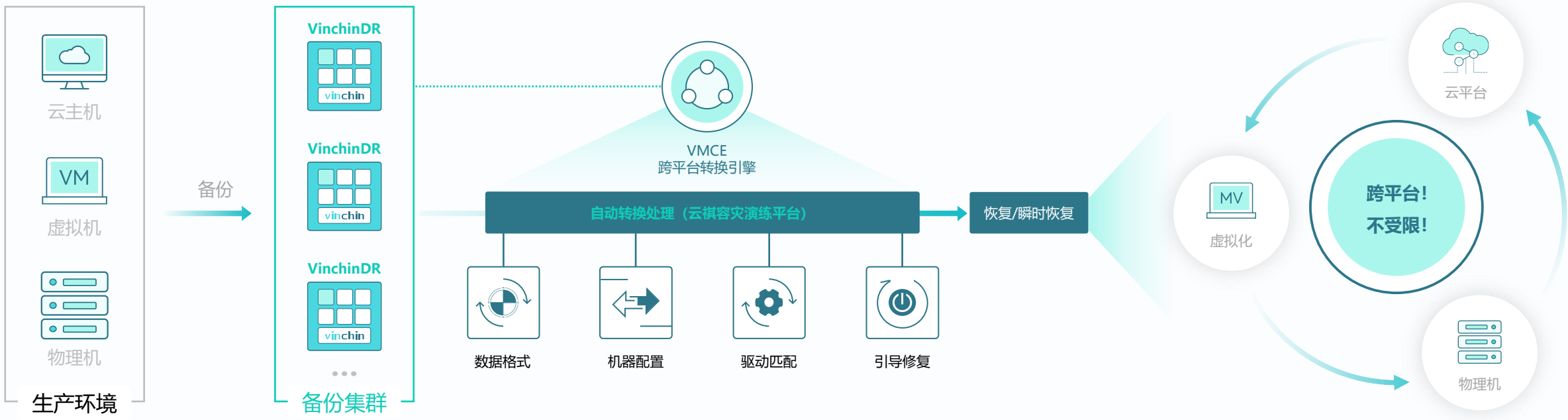
遭遇勒索攻击时，业务系统可能需要根据重要性、RTO/RPO要求、恢复资源位置等实际情况选择不同的恢复方式，因此，提供丰富的恢复手段或选项将使用户可以从容应对复杂的恢复场景，并提升恢复效率和成功率。



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

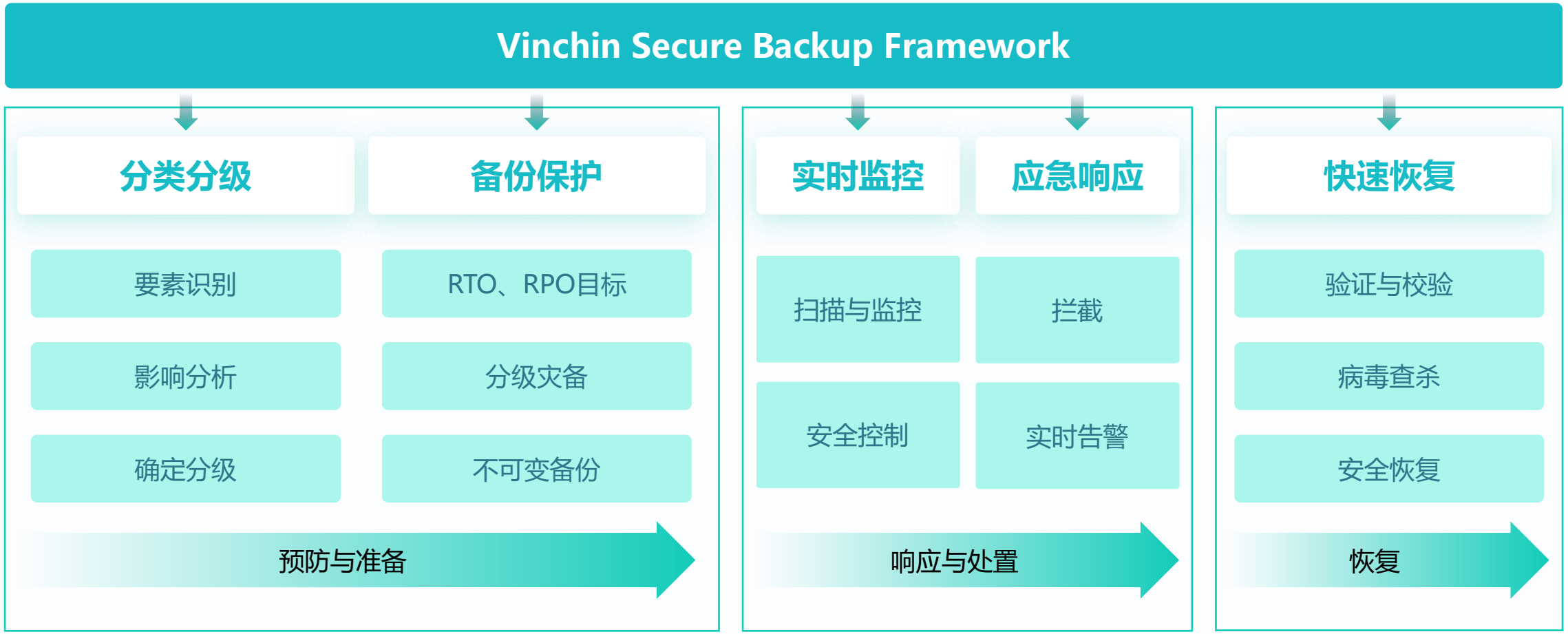
上报
安全事件

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。

云祺防勒索安全备份体系的价值

vinchin

您担心的	无防护的后果	云祺方案效果	其他方案效果
中勒索了怎么办?	我不知道	验证过了，可以用	我先看看
业务能恢复吗?	我不知道	杀过毒的，可以用	这个恢复出来有毒
业务啥时候上线?	我不知道	有WROM呢，没被改	明天晚上才能恢复完
妈呀，天大一笔赎金	我.....	等几分钟就好啦	我恢复不出来
...	...		...

安全恢复快人一步

减少业务中断损失

验证确保安全合规

vinchin

THANKS

云祺公众号

云祺视频号