vinchin

备份系统 VS 勒索病毒
孰强孰弱？

vinchin

目录

vinchin

PART 01

上期直播回顾

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。

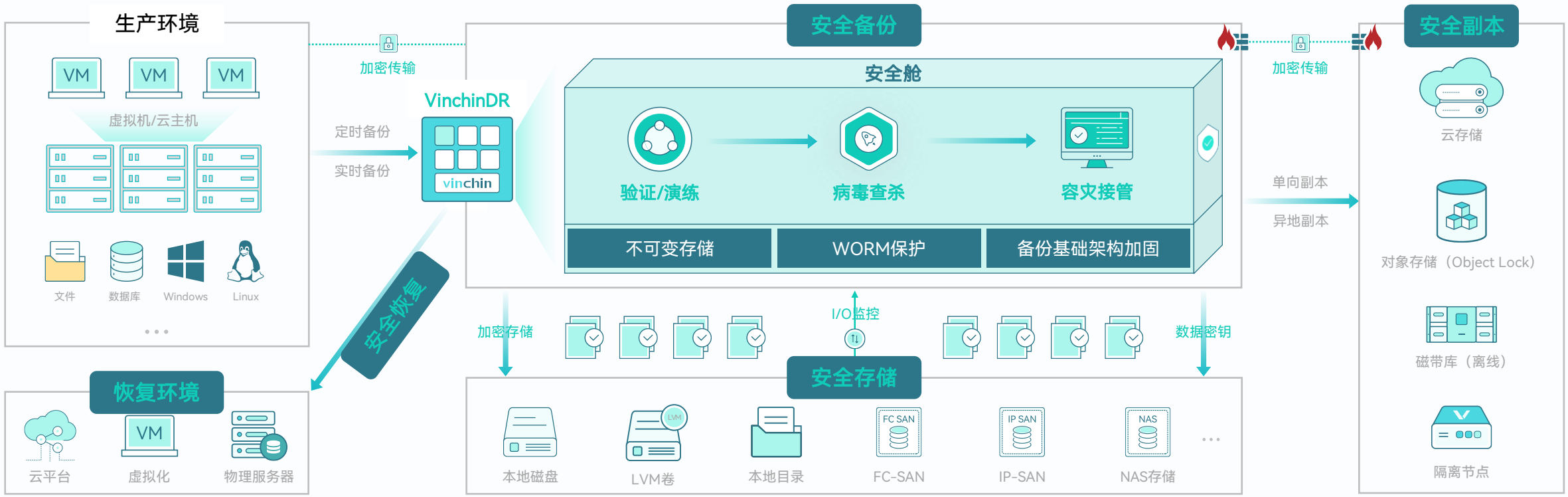
> 勒索攻击给受害者带来的影响是多方面的，除了需要支付高额赎金外，业务中断、声誉受损等问题也会接踵而至，更严重的是，违反数据安全法规可能导致严重的法律后果。

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

为何企业总在勒索面前陷入被动

关于勒索病毒的误区

vinchin

误区1：小企业不会被勒索病毒盯上

事实：黑客专攻防护薄弱目标——小企业因安全投入不足、漏洞未修补，反成高回报“理想猎物”

误区2：被勒索纯属“运气差”

事实：安全事件非偶然——防护缺失必中招，出事是必然，不出事是侥幸。

关于勒索病毒的相关问题解答

vinchin

黑客为何不直接联系?

黑客全程匿名操作：电话暴露身份易被追踪，且受害者信息不透明、黑客多位于境外，故仅通过加密提示勒索

能否找人解密文件?

无密钥则数据永久锁定——国际加密标准不可逆

为何有“解密”案例?

无密钥则无法解密——恢复案例实为中介代付赎金或特定病毒密钥泄露

是否支付赎金或恢复费用?

避免支付赎金；合法数据恢复按价值付费

中毒后应急指南

保留现场，专业溯源，预防再犯

关于勒索病毒的相关问题解答

vinchin

中勒索后是否上报?

必须报警，但合规先行

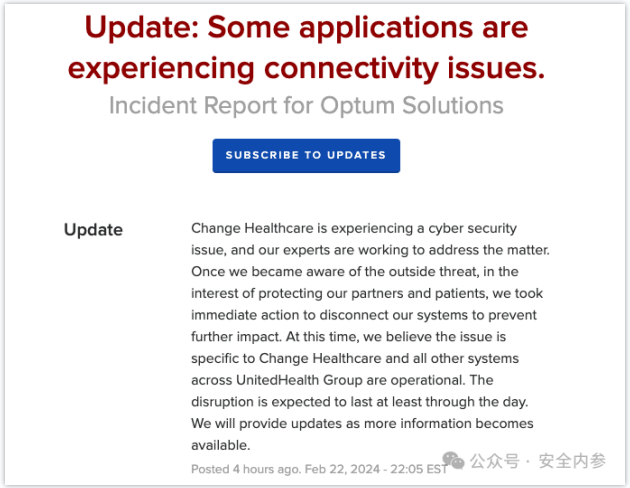
如何预防勒索攻击?

双重防线：专业防护 + 离线备份

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

vinchin

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

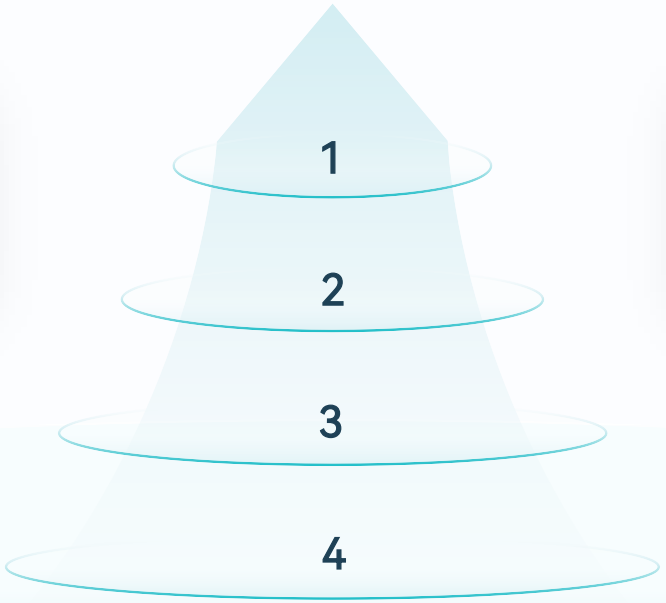
没有100%有效的防御体系，中了勒索说明所有的前置防御措施均已失效，此时最紧要是恢复数据，因此需要思考以下几个问题：

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

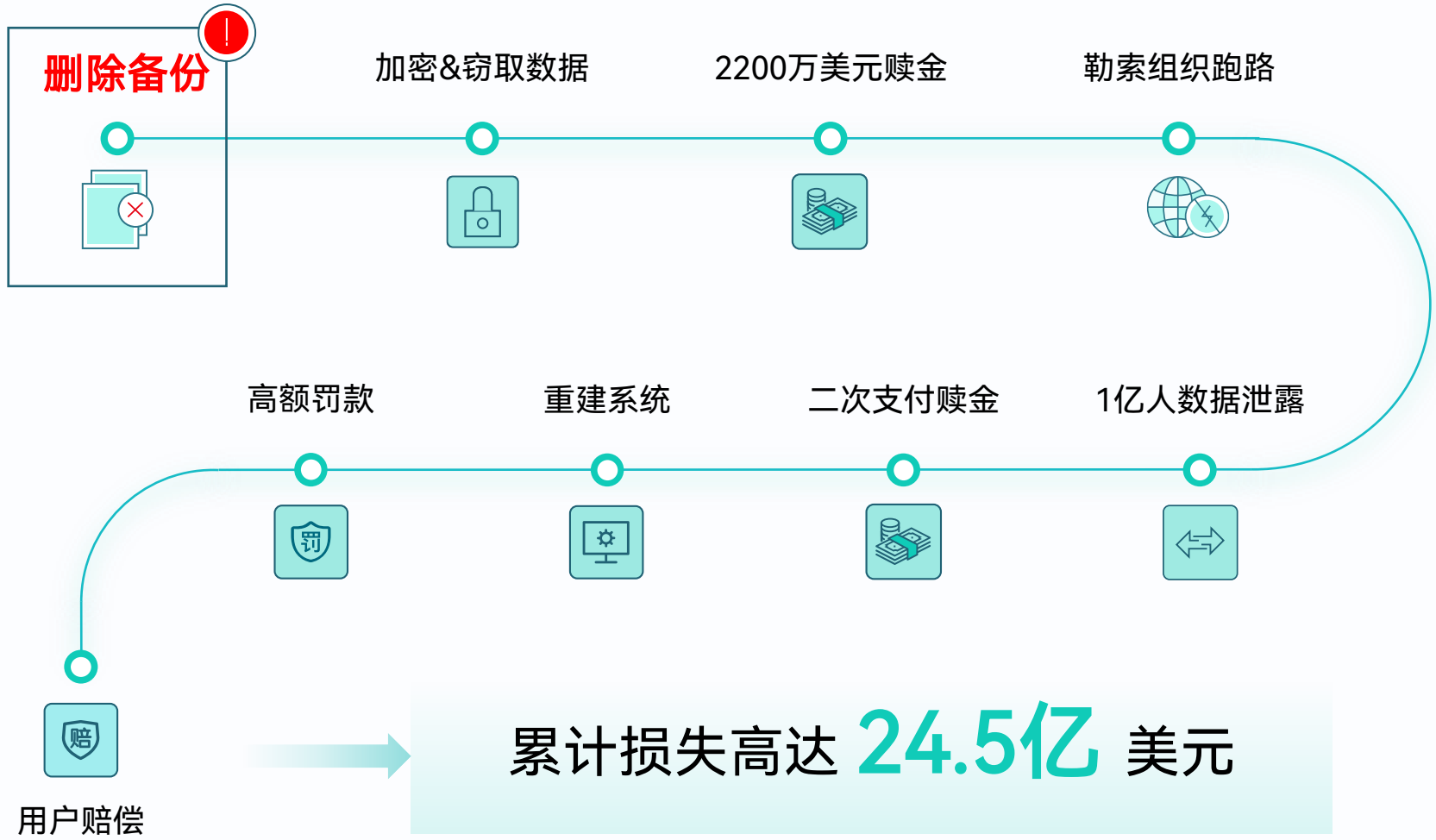
如何快速、安全的恢复所有数据

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

vinchin

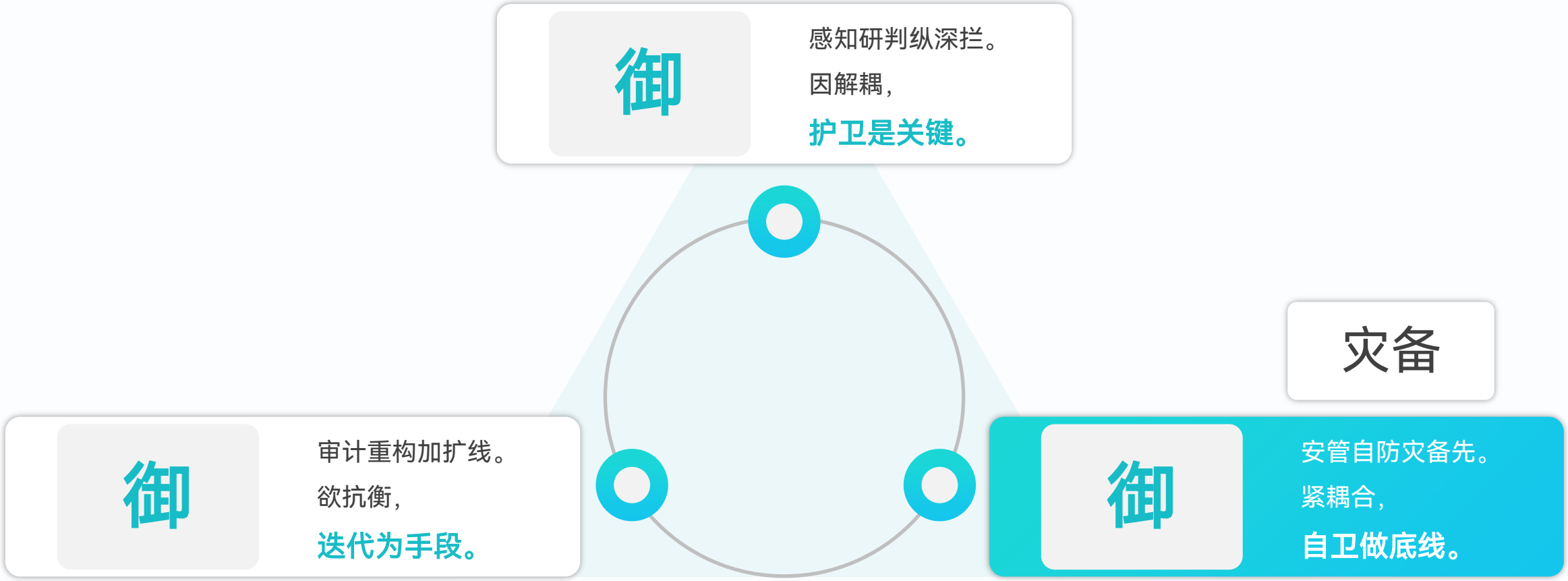
PART 02

备份系统 VS 勒索病毒
属强孰弱?

未感染勒索病毒时

vinchin

2023年中国网络和数据安全产业高峰论坛：十六字令·网御三部曲



概念来源于2023年中国网络和数据安全产业高峰论坛

勒索病毒攻击流程

vinchin

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

勒索病毒感染/发作时

vinchin

勒索病毒	VS	云祺容灾备份系统
感染生产数据		通过备份数据恢复
感染备份数据		异地多副本确保不同生产域中都有数据副本，不至于“一锅端”
		不可变存储、WORM等机制确保备份数据不被感染
潜伏型勒索病毒，潜藏在生产与备份数据中		周期性自动扫描备份数据，提前发现病毒
		清除攻击痕迹，利用备份数据朔源
		安全恢复：备份数据杀毒后进行恢复
黑客针对性攻击备份系统		内核级数据保护（不可变、WORM）
		通过备份系统将备份数据存入离线存储
		备份服务集群化运行，部分节点下线不影响整体备份业务
		体系化告警，第一时间发现异常
内部攻击		加密备份数据，拔盘拷贝也于事无补
		精细的日志记录并强制保留
		备份服务访问客户端黑/白名单，限制可访问范围
…		…

vinchin

备份系统 VS 勒索病毒
属强孰弱?

vinchin

“魔高一尺，道高一丈”

勒索病毒有手段

备份系统有对策

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

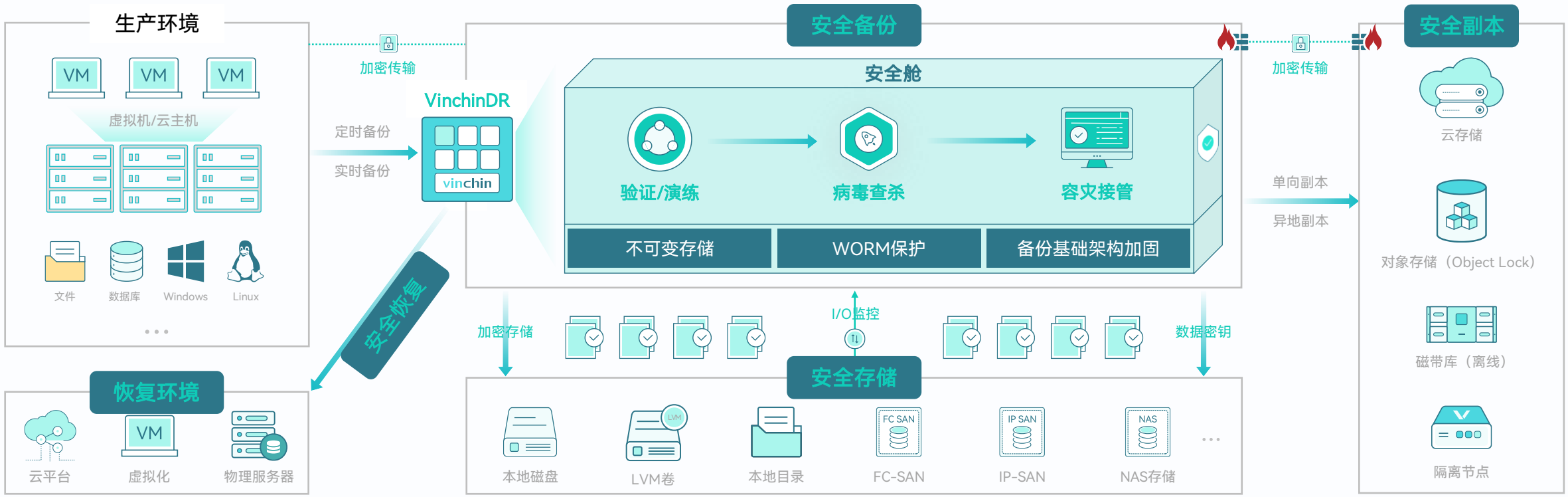
建立完善的灾难恢复管理制度并实施员工培训

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

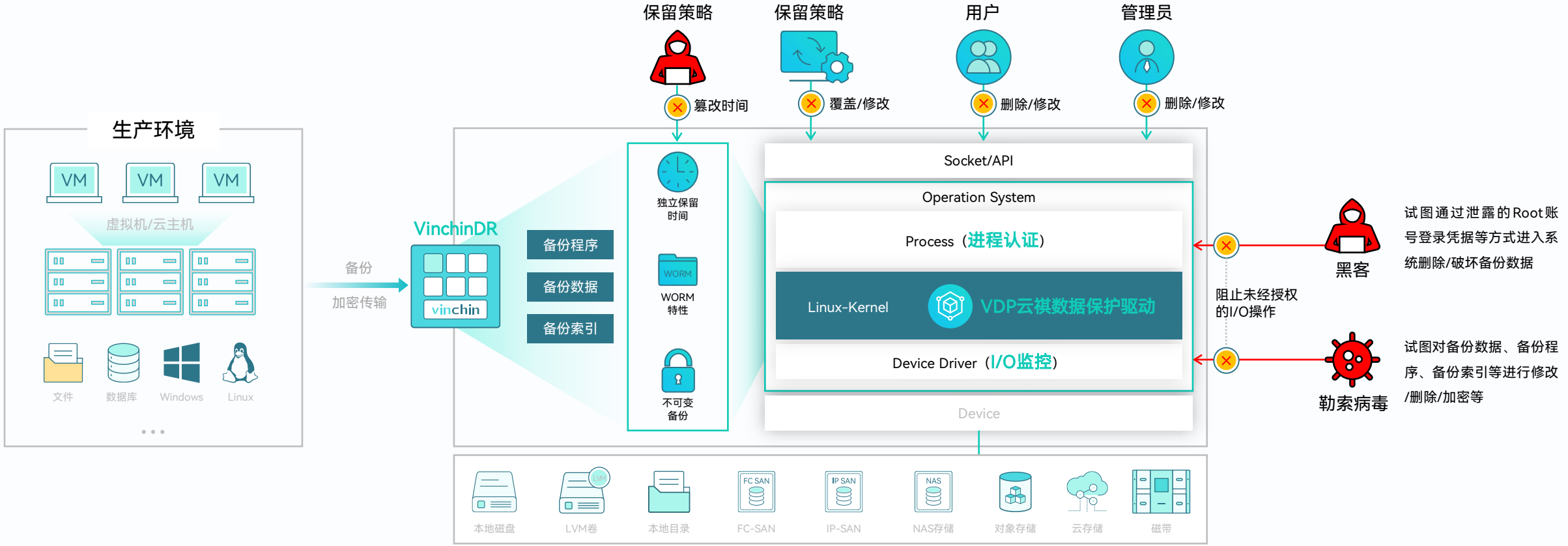
依据零信任原则对备份系统实施多层安全加固，防止任何未授权访问与操作

vinchin

PART 03

云祺容灾备份系统防勒索特性

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

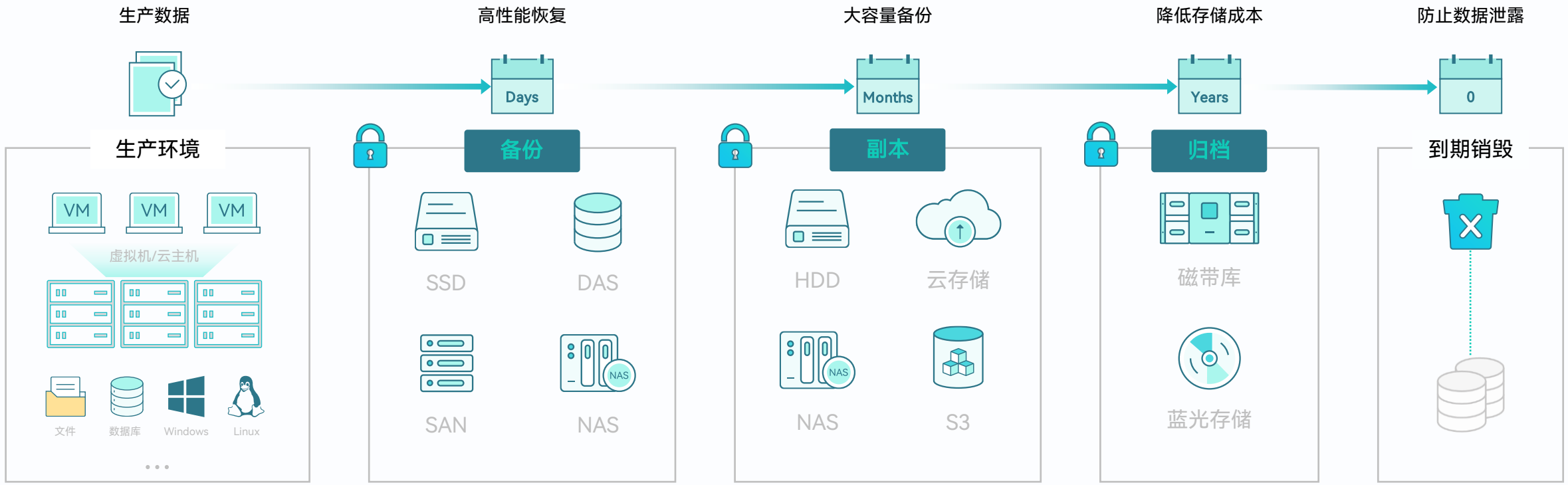
不可变存储：使用原生不可变存储或对象存储Object Lock、物理磁带离线存储等实现备份数据不可变特性

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

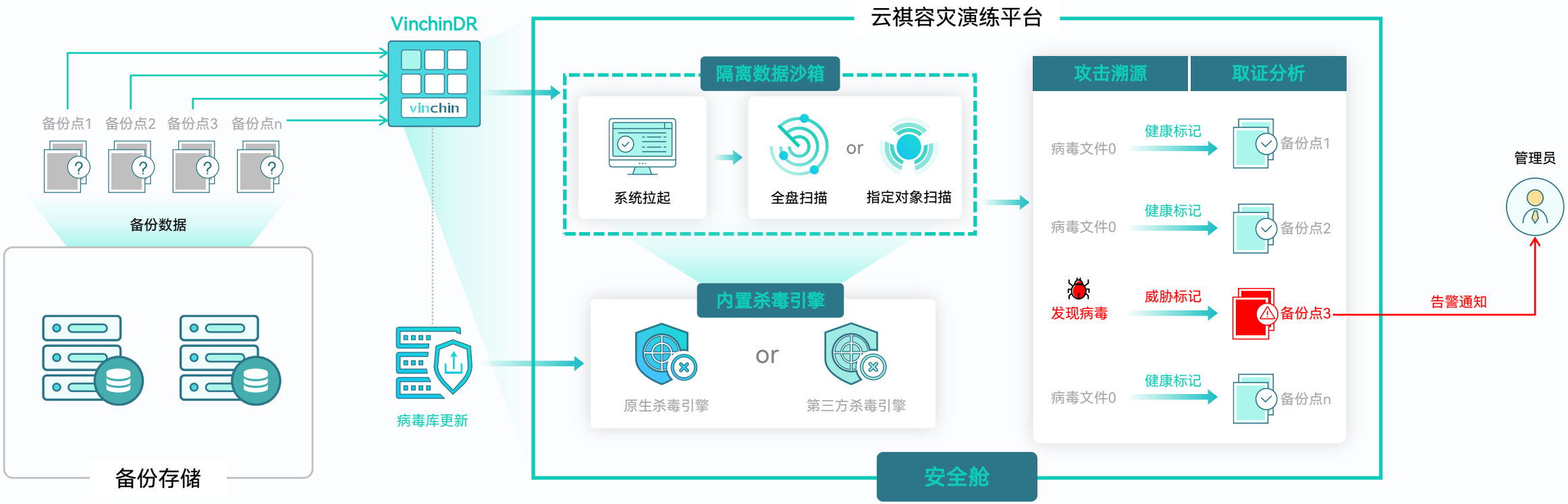
vinchin

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



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

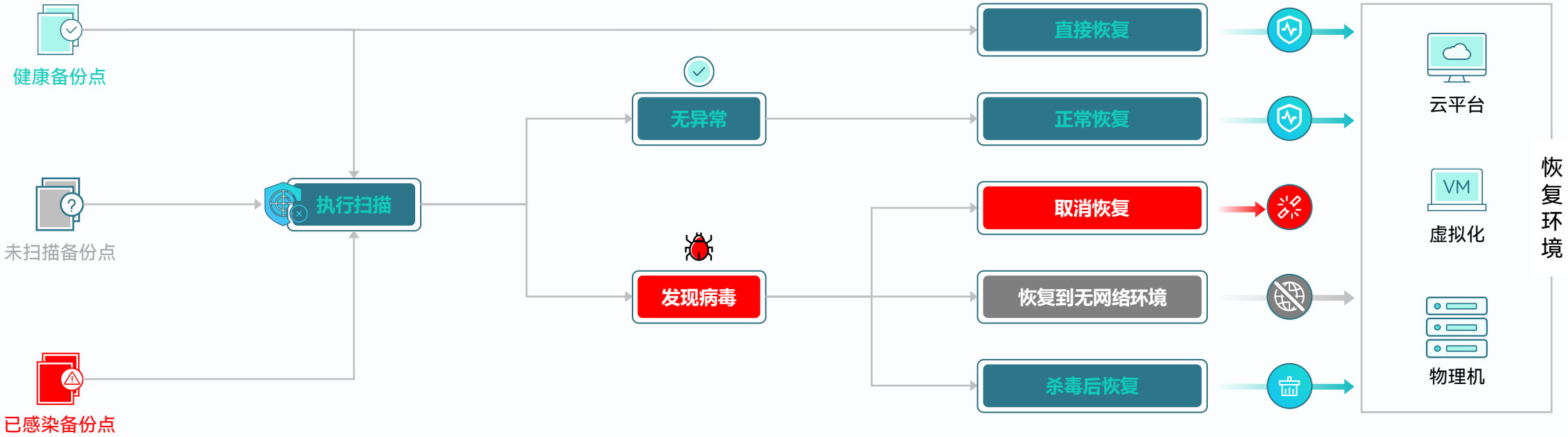
在备份数据中查找干净可用的备份点，为将来的安全恢复做好准备

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

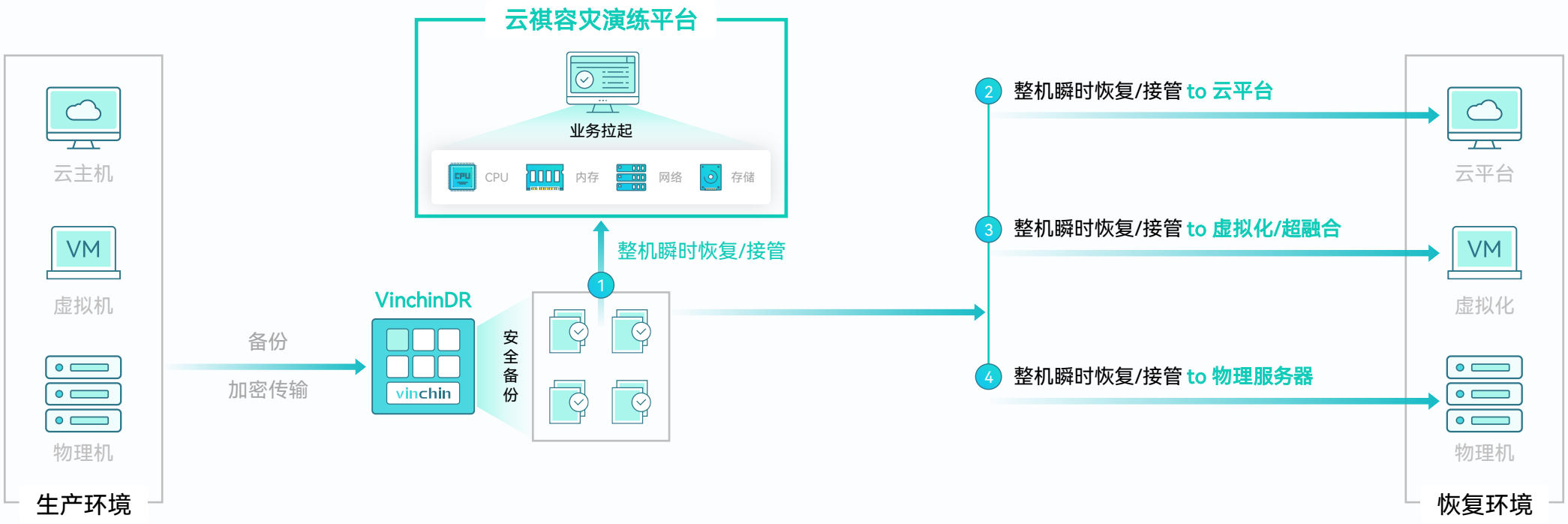
使用安全的备份恢复或在恢复前进行恶意软件扫描与查杀，以确保正确、干净、有效的恢复，防止恢复后造成二次感染。发现病毒时支持根据不同需要采取取消恢复、恢复到无网络环境或杀毒后再恢复。



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

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

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

业务系统

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

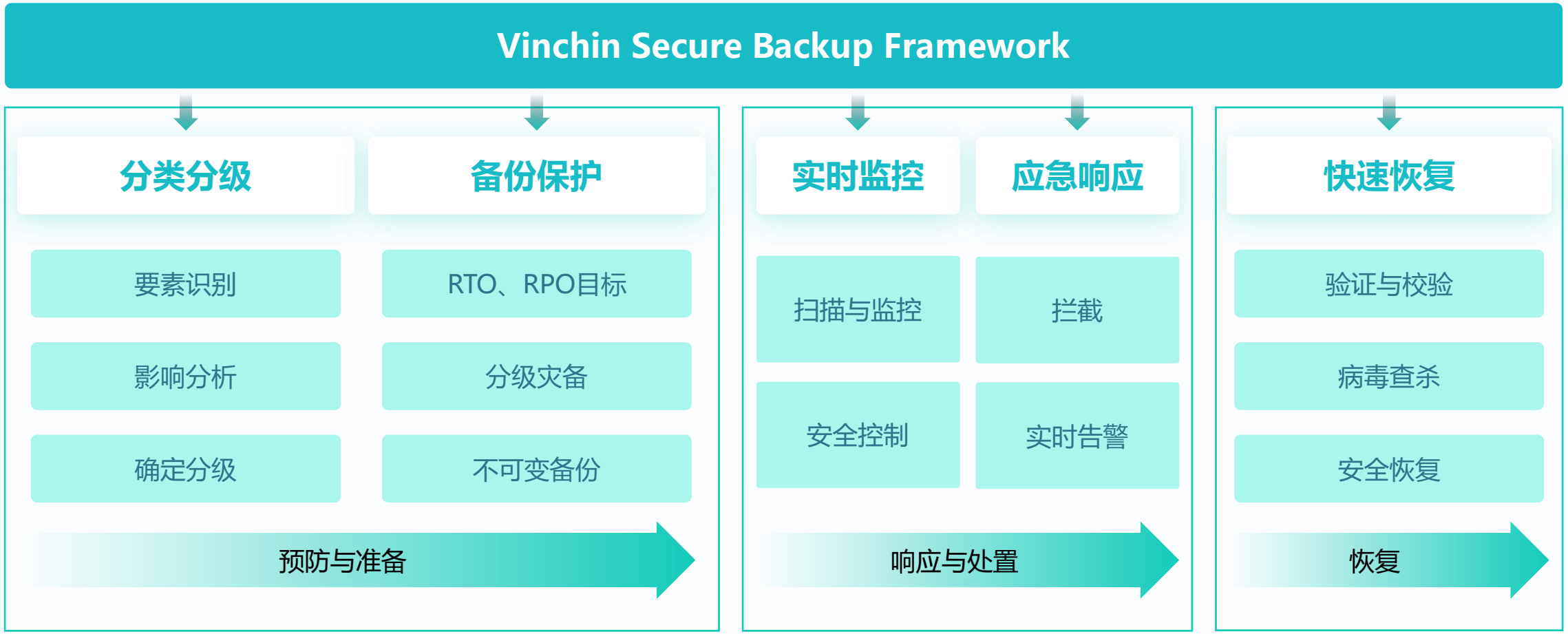
上报
安全事件

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。

云祺易用性与简单运维

vinchin

云祺容灾备份系统的部署与使用及日常运维

- 云祺容灾备份系统提供软件、超备一体机两种交付方式，部署安装简单；
- 在云祺容灾备份系统的使用上，用户及仅需通过个人办公PC浏览器即可访问管理界面，功能逻辑清晰简单易用；
- 在前期灾备规划并实施完成灾备策略后，后续不做调整的情况下，用户仅需关注邮件或其他告警触达方式。也可通过云祺可视化大屏时刻监测灾备情况。

产品无门槛免费试用-云祺容灾备份系统

www.vinchin.cn

vinchin

THANKS

云祺公众号

云祺视频号