

vinchin

打不穿的备份 删不掉的数据

云祺容灾备份 × 数麟磁带库

云祺科技 售前工程师 李帅兵

目 录

- PART 01 勒索威胁新态势
- PART 02 云祺安全备份体系
- PART 03 磁带：最后的防线
- PART 04 云祺×数麟联合方案
- PART 05 案例分享

PART 01

勒索威胁新态势

勒索软件攻击的新链路

传统勒索只加密生产数据；现代勒索团伙先横向渗透备份系统，摧毁备份后再加密生产，让企业无据可恢。

STEP 1

横向渗透

利用漏洞/钓鱼进入内网

STEP 2

摧毁备份

删除/加密备份数据

STEP 3

加密生产

对业务数据加密勒索

STEP 4

索要赎金

无备份可恢复，被迫支付

核心挑战

- 备份系统在线连接，可被横向渗透
- 管理员账号泄露 = 备份可被删除
- 在线不可变存储仍有被绕过的风险
- 勒索病毒针对性攻击备份软件
- 生产+备份同时被加密 = 只能交赎金

需要一份物理隔离、网络不可达的离线副本作为最后防线

PART 02

云祺安全备份体系

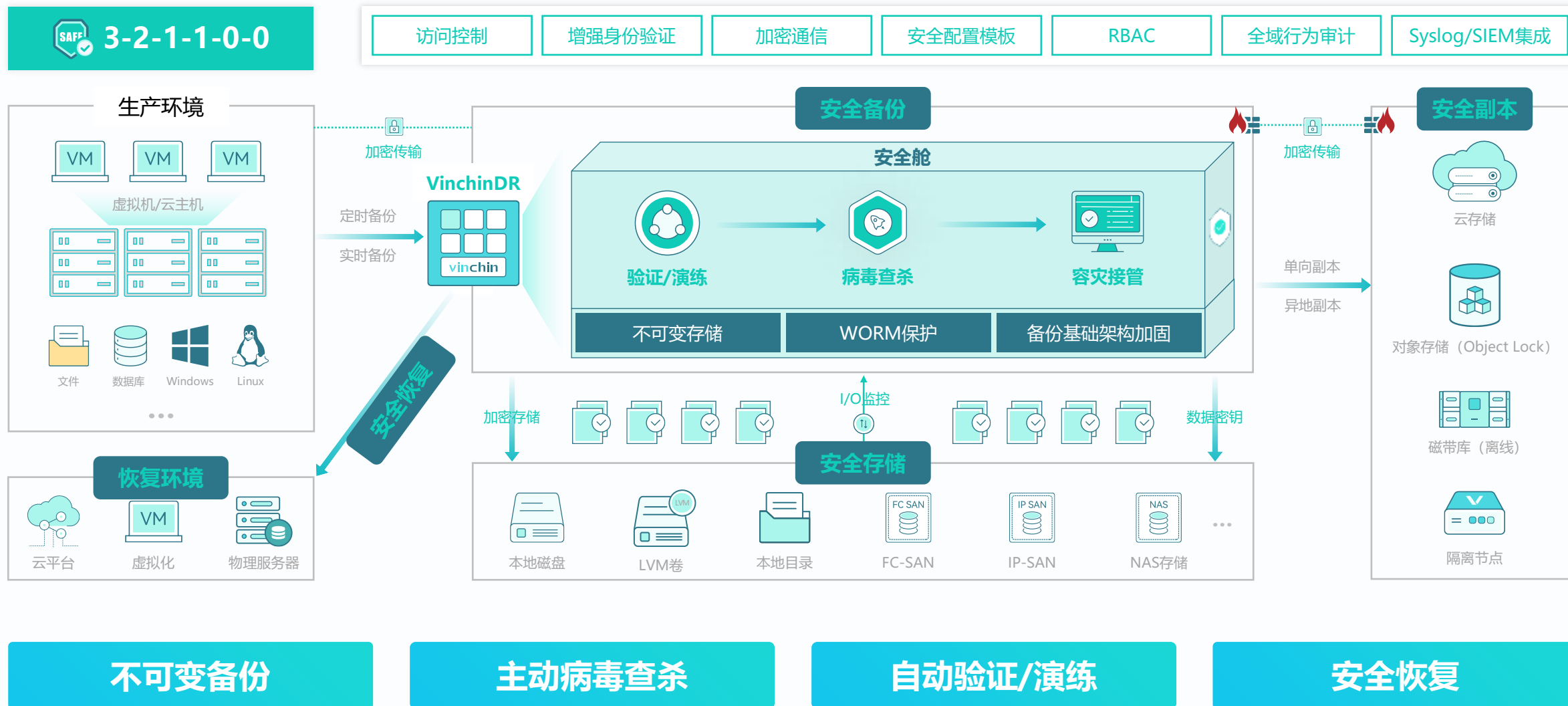
全域数据保护平台

vinchin



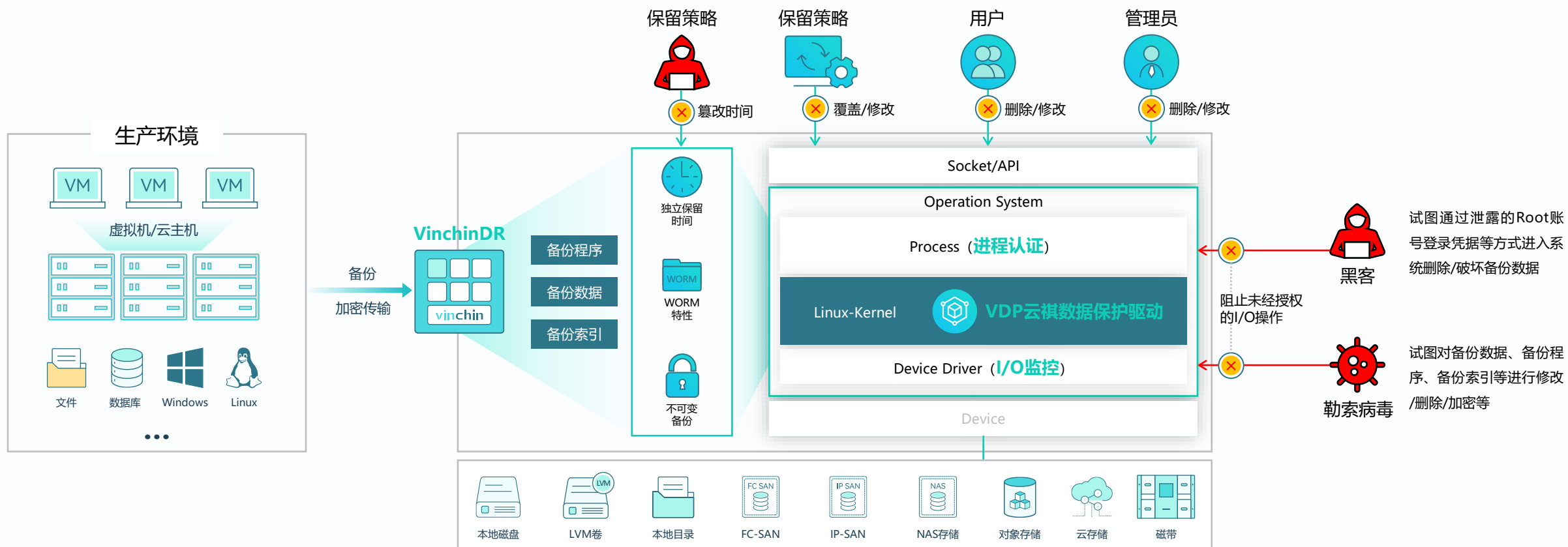
云祺安全备份体系

vinchin



防勒索：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

云祺容灾备份 × 数麟磁带库，构建从生产到离线的全链路数据保护体系

01 全面兼容混合环境

- 全域适配混合IT架构
- 统一纳管业务系统及存储
- 虚拟化/物理/云/容器全覆盖
- 简化整体运维，降低管理复杂度

02 业务数据分层存储

- 按业务需求和数据价值分级
- 热数据在线、温数据近线、冷数据离线
- 平衡灾备安全、数据合规与成本
- 磁带归档TCO仅为磁盘几分之一

03 强化防勒索能力

- 不可变备份 + WORM保护
- 离线磁带Air Gap气隙隔离
- 内核级防勒索加固 + 进程认证
- 构筑纵深防勒索安全体系

防勒索备份架构体系

本地 D2T

数据直接备份到磁带 简单高效，
成本最低

本地 D2D2T

磁盘备份 + 磁带归档 兼顾恢复
速度与离线安全

本地+异地 D2D2T

本地磁盘+异地磁带 双重容灾，
最高等级防护

PART 03

磁带：最后的防线

在线不可变 vs 离线气隙

在线不可变 vs 离线气隙：互补而非替代

在线不可变存储

防护层面	软件逻辑层
隔离方式	逻辑隔离 (WORM策略)
网络可达	是, 在线连接
被绕过风险	存在 (0day/管理面沦陷)
恢复速度	快 (瞬时恢复)
适用场景	日常备份、快速恢复
代表技术	云祺WORM、Object Lock

离线气隙 (Air Gap)

防护层面	物理介质层
隔离方式	物理断开 (不接电/不连网)
网络可达	否, 物理不可达
被绕过风险	极低 (需物理接触)
恢复速度	较慢 (顺序读取)
适用场景	最后防线、长期归档
代表技术	数麟磁带库、离线磁带

结论：在线不可变解决「软件层面删不掉」，离线气隙解决「物理层面碰不到」——两者结合才是完整防护

PART 04

云祺×数麟联合方案

云祺 × 数麟 联合防勒索方案：三层防护



典型应用场景

01 金融行业

交易记录、客户信息需长期留存；勒索高价值目标；磁带满足合规+气隙双重需求

02 医疗PACS

CT/MRI影像PB级增长，冷数据占比高；磁带归档成本仅磁盘几分之一；数据安全关乎生命

03 政务国产化

等保/关基要求独立备份存储；云祺+数麟全链路自主可控；物理离线符合合规要求

04 制造/设计院

产线数据、设计图纸是核心知识产权；磁带30年寿命完整守护知识资产

备份是数据的安全底线

云祺容灾备份

- 全域数据保护，全场景覆盖
- 内核级防勒索 + WORM不可变
- 瞬时恢复，秒级RTO
- 主动病毒查杀 + 自动验证
- 原生支持磁带库存储目标

数麟磁带库

- LT Zero Orion S3云磁带库
- Air Gap气隙物理隔离
- 单机架50PB高密度存储
- 30年超长数据保存寿命
- 国产化制造，自主可控

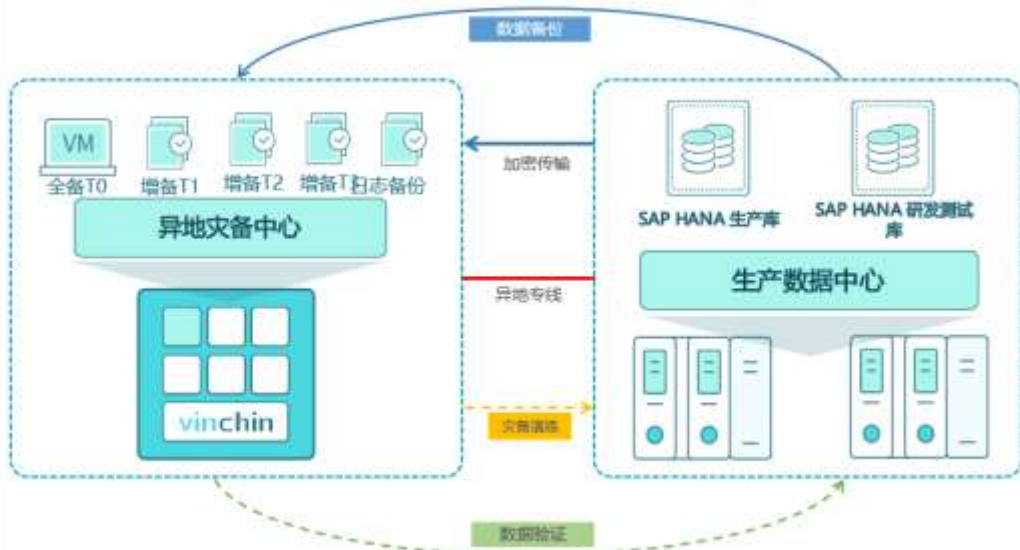
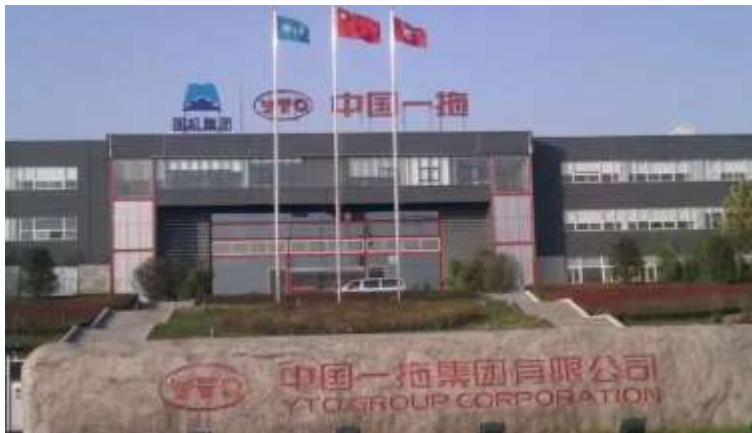
两者结合 = 完整的、有纵深的、经得起实战考验的数据防勒索方案

PART 05

案例分享

河南案例-XX有限公司

XX坐落河南洛阳，隶属国机集团，前身为 1955 年开建的第一拖拉机制造厂，是“一五”重点项目，被誉为农机工业长子中国一拖集...。旗下一拖股份为 A+H 股上市企业，“东方红”是首批中国驰名商标。企业构建完整农机产业链，主营拖拉机、收获机械及配套柴油机、传动部件，大中型拖拉机市占率行业第一，累计产销数百万台农机。作为农机产业链链主、制造业单项冠军，深耕智能农机研发，持续助力我国农业机械化与粮食安全保障



痛点及需求

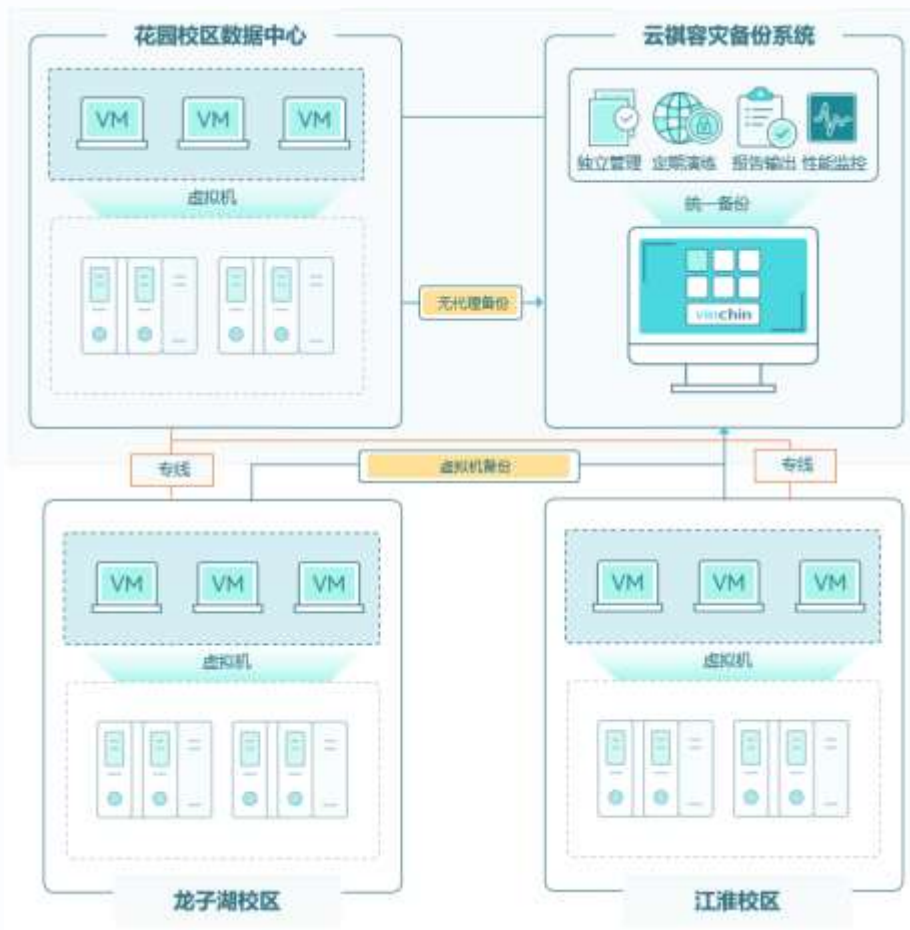
- 核心业务系统没有异地备份，一旦出问题，恢复时间难以预估；
- IT系统种类多、结构复杂，涉及操作系统、文件、数据库等不同层级，保护难度大；
- 运维依赖人工，备份工作易被忽略、难以统一管理；
- SAP HANA数据库无异地备份方案，出错风险大；
- 合规要求提升，《等保2.0》等政策对数据备份与容灾提出硬性标准。

云祺方案及价值

- 云祺为企业设计并部署了一套“分层保护 + 异地备份 + 自动运行”的完整数据保护体系，确保无论是服务器故障、误操作还是网络灾难，都能第一时间实现系统恢复、业务接续。
- 关键数据库 SAP HANA 定时自动整库备份和增量备份，无需脚本操作，实现异地备份需求，简化运维工作，轻松完成配置和恢复；
- 整机系统镜像备份，一旦出现设备损坏或系统崩溃，可将整个系统环境恢复至原机或异构设备，省去重装部署环节，大大缩短恢复时间。
- Windows/Linux等环境下的文件/目录灵活选择备份，所有备份任务可设定自动周期执行，并传输到异地数据中心一份，保障多场景下的数据可靠性，数据传输过程支持加密、防篡改，有效防范勒索病毒入侵。
- 满足《等保2.0》等政策要求

河南案例-XX水电大学

XX电大学 1951 年创建于北京，前身为中央水利部水利学校，历经多地搬迁，1990 年迁至郑州，2013 年定现名，由水利部与河南省共建、以豫为主管理。学校是河南省特色骨干大学、“双一流” 创建高校，首批硕士学位授予权单位、中西部高校基础能力建设工程高校。现有花园、龙子湖、江淮三个校区，设 26 个教学单位，69 个本科专业，以水利为特色、工科为主干，多学科协调发展。



痛点及需求

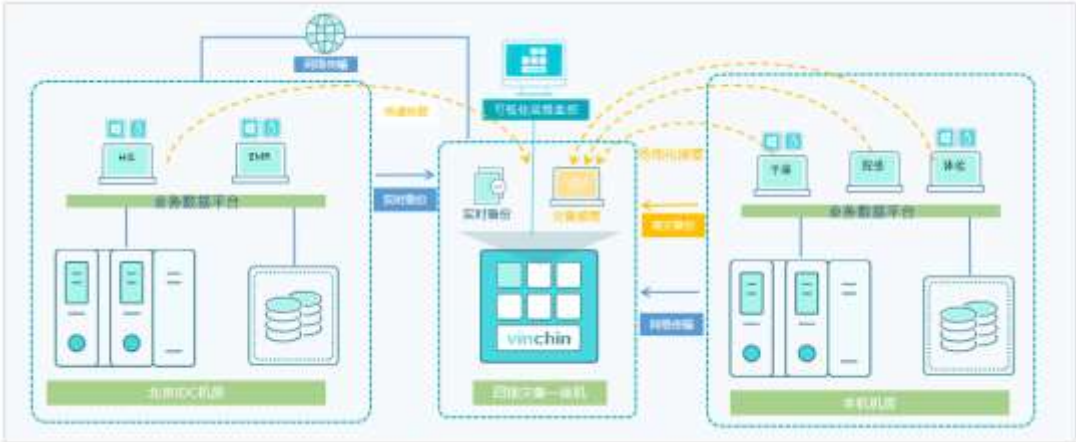
- 国产化架构适配难：校内部署深信服超融合平台，同时混用 x86、国产架构，需实现跨平台、跨架构统一数据保护，适配高校多元化教学科研 IT 环境。
- 多部门分权管控需求：数据中心涵盖教学、科研、行政等多类数据，需按院系 / 部门划分模块权限，实现各部门数据本地备份与独立管理，兼顾全校统一管控与部门自主性。
- 海量数据备份效率压力大：汇聚教学资源、科研数据、学生信息等海量数据，需缩短备份窗口（避开上课、办公高峰），同时提高现有存储利用率，降低高校 IT 运维成本。

方案及价值

- 灵活部署适配混合架构：无缝兼容 x86 & 国产化混合架构下的深信服虚拟化平台，快速融入高校现有 IT 体系，无需大规模改造。
- 高效备份匹配教学节奏：通过指定网络备份机制提速，大幅缩短备份窗口，避开教学办公高峰；优化存储利用，减少资源浪费，贴合高校成本控制需求。
- 集中保护 + 分权管理：实现全校数据本地集中备份，故障时快速恢复业务虚拟机，保障教学、科研、行政业务不中断；支持多用户模块权限划分，满足各院系 / 部门独立管理数据的需求，操作简便。
- 灵活恢复提升抗风险能力：支持虚拟机瞬时恢复，面对系统故障可快速恢复教学平台、科研数据库等核心业务，最大限度减少对教学科研的影响。

河南案例-XX脑科医院

XX脑科医院是集医疗、教学、科研、保健、康复一体化的三级神经专科医院，也是河南省、郑州市医保定点机构，郑州市残疾儿童康复救助定点服务机构等。三博脑科医院以“发展神经科学事业”为使命，践行博医、博教、博研的办院理念，秉承技术、服务、品质的服务信条，创新管理模式，各科室与首都医科大学三博脑科医院实行模块化对口运营、同质化管理。



痛点及需求

- 院内现有HIS、EMR、LIS、PACS、手麻、体检等业务系统无有效的数据备份方案，一旦出现设备故障或数据被加密，及有可能会造成数据丢失。从而会影响到院内的经济问题和院方的名誉。且此现状更不符合国家对医疗机构的数据保护的政策性要求。
- 由于是全国性质医院，所以现有核心HIS和EMR托管在北京IDC机房，除托管在北京IDC机房的HIS和EMR外，本地机房还有运行在Vmware 虚拟化平台的LIS、手麻、体检、院感等业务系统。
- 这给业务连续性带来一定的考验，一旦出现线路故障或机房故障，会出现业务不能访问等情况。因此为保证业务连续性，对院内的业务系统进行容灾备份和接管是非常迫切的。

云祺方案及价值

- 本地的LIS、手麻、PACS等系统及数据实时备份完成后并对业务系统及操作系统和操作系统上运行的数据库及应用进行容灾接管的配置，并做数据一致性验证，在发生物理故障、系统故障、机房故障等灾难的情况下可以进行业务的接管，从而保证业务的连续性，满足RPO≈0，RTO<5分钟的需求及政策要求。
- 针对Vmware虚拟化平台上次核心业务系统，采用虚拟无代理批量备份的方式，保证每天定时自动备份数据，一旦出现故障既有数据可恢复，也可实现业务系统虚拟机的瞬时恢复和快速的应急接管，保障了业务连续性。
- 有效的数据备份实现了备份数据防勒索病毒的需求。

河南案例-XX政务云

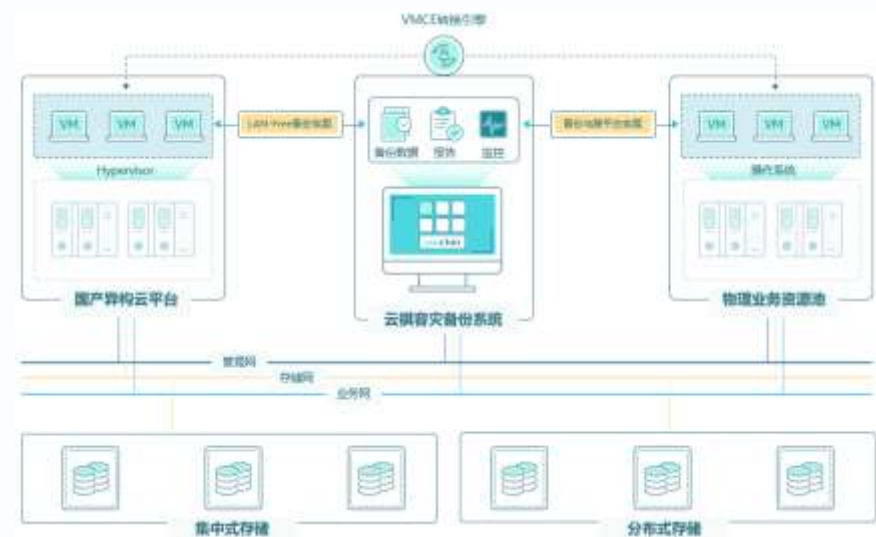
XX政务云是XX市数字政府建设的核心基础设施，由市行政审批和政务信息管理局主导推进，旨在通过统一的云计算平台支撑全市政务业务高效运行。遵循“统一规划、统一建设、统一管理、统一平台、统一数据、统一组织”的原则，构建全市一体化的政务云服务体系。该体系通过高效集约的建设模式，整合了市、县、乡三级政务资源，实现了政务系统的云端迁移与数据共享。

痛点及需求

- 同时拥有异构云平台 and 物理业务资源池，虚拟机数量1000+，需要对所有的虚拟机进行备份。
- 网络复杂，不改造网络的提前下，需实现从云平台 and 物理平台跨域的备份数据稳定、安全传输。
- 备份数据量大，备份虚拟机业务系统多，由各个局办自行管理。
- 重要业务的核心数据需要实时备份，保障数据不丢失。

云祺方案及价值

- 数据统一管理：多种异构云平台集中备份，备份数据统一管理；
- 简化备份网络：不改变网络结构，采用NAT方式轻松实现数据可靠备份传输。
- 混合架构数据保护：不仅支持传统Windows、Linux架构下数据的备份，并且支持对ARM CPU架构下的麒麟、统信操作系统下数据的保护，实现混合类型数据的多元化保护；
- 异地数据容灾：使用云祺远程复制功能，无需增加成本，实现多云数据异地备份
- 核心数据库保护：重要业务安装客户端，采用实时保护方式，保障核心数据不丢失。



THANKS



云祺公众号



云祺视频号