vinchin

# Veeam替代安全对比：智能无死角防护



vinchin

# 目 录

PART 01　云祺 VS Veeam 安全与运维多维对比

PART 02　云祺智能防护实践

vinchin

# PART 01

## 云祺 VS Veeam
## 安全与运维多维对比

# 2025–2026 勒索攻击密集爆发

### 事件一 • Weaxor 勒索

国内多起 Weaxor 攻击，文件被加密为 **".weax"** 后缀。
跨 Windows / Linux 双平台，目标覆盖企业服务器、数据库、OA 系统。
攻击特点：横向移动快、加密前先侦察备份

### 事件二 • Sorry / ths 变种

Sorry 勒索改名 **ths** 后卷土重来，席卷中小企业。
加密对象：数据库、**备份文件**、办公文档、源码仓库。
特点：专门先删本地 VSS 快照与备份副本

### 事件三 • IDCF Cloud 停摆

软银旗下 IDC Frontier 云被勒索攻击。
云服务器**全部停止运行且无法重启。**
影响 **495 家** 企业与市政机构，证明公有云自身也非安全港

结论：攻击者已将"删除 / 加密备份副本"作为标准动作。**支付赎金后数据恢复率不足 30%，可靠的安全备份才是唯一可控路径。**

# 备份 ≠ 安全备份

vinchin

## 被动恢复工具必须升级为安全备份中枢

### 传统备份：只解决"数据有没有"

- 定时把生产数据复制一份到存储
- 默认信任备份网络与备份管理员
- 不校验备份数据是否已被感染
- 备份盘与生产盘同网、同权限
- 恢复前不扫描，可能二次感染
- 校验靠人工抽查，链路易断

### 云祺安全备份：解决"备份本身可不可信"

- **零信任访问**：身份、授权、审计三层
- WORM + VDP：root 也删不掉备份
- **内置杀毒引擎**：隔离沙箱自动查杀
- **端到端加密**：传输 + 存储 + 恢复密钥
- **安全恢复**：恢复前扫描，杜绝二次感染
- **自动校验**：定期完整性比对与告警

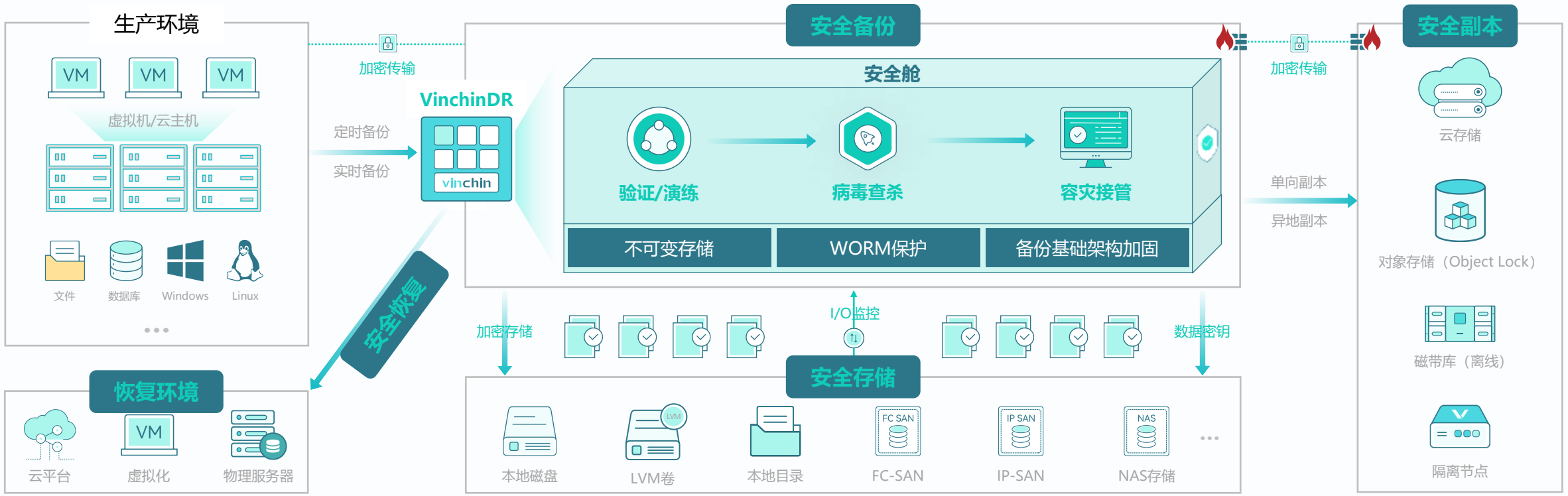
云祺观点：**备份不再是数据安全的最后一道防线，安全备份才是。**（来源：vinchin.cn/ransomware-protection）

# 云祺安全备份体系

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** | **自动验证/演练** | **安全恢复**

# 三段式安全闭环对比

vinchin

## 事前主动加固 → 事中检测告警 → 事后验证恢复

**事前预防**

### 把备份库建成"金库"

· 零信任访问 + RBAC + MFA
· 端到端加密（传输 / 存储 / 密钥）
· WORM 不可变存储
· VDP 内核级防篡改驱动
· 3-2-1-1-0-0 副本策略

**事中预警**

### 让风险被自动看见

· 内置杀毒引擎 + 隔离沙箱
· 数据完整性自动校验
· 异常备份点标记与告警
· 资源 / 容量 / 性能阈值告警
· Syslog / SIEM 审计集成

**事后验证**

### 确保"真的能恢复"

· 瞬时恢复 / 整机接管
· 文件 / 数据库细粒度恢复
· 恢复前安全扫描防二次感染
· 自动化演练 + 可视化报告
· 业务回切生产

**Veeam 同类能力分布：**

事前（RBAC / MFA / 不可变仓库）偏配置门槛高；事中（Threat Hunter / Recon Scanner / IoC）属高级版模块；事后（Secure Restore / Clean Rooms）需额外沙箱环境。云祺把三段能力全部内置在同一套系统中。

# 三段式安全闭环对比

vinchin

## 防勒索全流程对照：事前防御 → 事中告警 → 事后恢复

| | 云祺 | Veeam |
|---|---|---|
| **事前防御**<br>备份点打不动 | · WORM 不可变存储 + VDP 防篡改驱动<br>· 传输/存储双重加密，AES-256 + SM2 国密<br>· 3-2-1-1-0-0：3副本·2介质·1异地·1不可变·0恢复失败·0未授权访问 | · Hardened Repo / S3 Object Lock 不可变<br>· MFA、4-eyes 双人授权、RBAC<br>· Security & Compliance Analyzer 安全基线评估 |
| **事中告警**<br>异常早发现 | · 备份/验证/恢复全阶段自动病毒查杀（内置引擎）<br>· 完整性校验：异常告警+标记+自动重备修正备份链<br>· DataV 大屏实时监控 + 邮件/短信多渠道告警 | · Inline 熵值扫描 + Recon Scanner 主动评估<br>· Threat Hunter / YARA / IOC 多层检测<br>· Veeam ONE 告警 + SIEM/SOAR/XDR 联动（400+ ATT&CK） |
| **事后恢复**<br>干净、快、可证明 | · 隔离沙箱确认干净副本后恢复，杜绝二次感染<br>· 瞬时恢复：异地副本 快速拉起 / 整机分钟级拉起<br>· 恢复口令二次验证 + 验证报告自动生成 | · Secure Restore / Clean Room 洁净室验证<br>· Instant Recovery 瞬时恢复<br>· Coveware 勒索响应服务 + 恢复编排与自动文档 |

# 端到端加密与访问控制对比

vinchin

**云祺 Encrypted Backups 全周期加密：**
生产出口加密 → 传输链路加密 → 存储静态加密 → 恢复前密钥校验。备份数据在被使用前始终处于密文状态，即使备份介质泄露也不会泄密。

| 防护环节 | 云祺容灾备份系统 | Veeam Data Platform |
| --- | --- | --- |
| **传输加密** | 数据离开生产系统即全程加密：传输加密+存储加密双重机制，使用前始终处于加密状态；支持 SM2 国密与 RSA 链路加密，副本公网传输不泄密 | 备份传输与静态加密（AES-256），云端仓储传输加密，防止传输链路截获 |
| **存储加密** | 网络传输到数据存储全流程加密，即使存储介质被盗取也无法读出明文；与不可变存储叠加形成「防篡改+强加密」 | 备份文件静态加密，配合 Hardened Repository 不可变存储 |
| **恢复防滥用** | 每次恢复操作需独立口令二次身份验证，防止凭证失窃后被直接拉取备份数据 | 4-eyes 双人授权拦截破坏性操作；MFA / OTP 二次验证登录 |
| **访问与审计** | 最小权限原则、登录密码严格管控；全流程审计追踪，操作行为可溯源、可追责 | RBAC 最小权限、SSO 单点登录；90+ 事件审计与变更跟踪报告 |
| **合规适配** | SM2 国密满足国内商用密码要求；不可变存储+审计日志+验证报告直接支撑等保 2.0 与数据安全法灾备义务 | 面向 GDPR、网络保险等国际合规框架；国内信创目录与国密资质缺失 |

# 零信任访问对比

vinchin

| 能力维度 | Veeam | 云祺容灾备份系统 |
| --- | --- | --- |
| **身份认证** | MFA / SAML SSO 需在企业版单独配置 | 开箱即用账号 + 口令策略，支持 LDAP / AD / 国密证书对接 |
| **权限模型** | 增强 RBAC + Four Eyes 两人审批，规则较粗 | RBAC 细粒度到备份作业、恢复点、存储库三级授权 |
| **操作审计** | 日志保留在本地，SIEM 对接需额外插件 | 全域行为审计，Syslog / SIEM 实时外发，等保可直接取证 |
| **特权账号** | Backup Admin 默认可删任意备份 | WORM 保留期内 root / admin 也无法删除备份点 |
| **访问入口** | Console / Web / PowerShell 多入口需分别加固 | 统一 Web 控制台，所有入口走同一套零信任策略 |

**云祺差异点：**

权限模型默认按"最小可用"配置，WORM 保护连系统管理员都无法绕过；审计日志原生支持等保 2.0 三级要求的 6 个月在线留存与实时外发。

# 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

# 不可变存储对比

vinchin

## Veeam：可用场景有限

**可用介质：**

· Hardened Linux Repository（专用 Linux 设备）

· 特定支持 Object Lock 的公有云对象存储

· 原生 NFS / FC-SAN 不支持不可变

**局限：**

· 存储类型受限，存量环境需改造

· 不可变策略在 Veeam 服务内，被入侵后仍有绕过风险

· 磁带离线需人工取带，RPO 不可控

## 云祺：原生三层不可变

**第一层 • WORM 保护**：保留期内独立计算，root / admin 也删不掉

**第二层 • VDP 防篡改驱动**：所有 I/O 必须通过 VDP 认证，未认证进程一律拦截

**第三层 • 多介质不可变：**

· 本地磁盘 / LVM 卷

· 对象存储 Object Lock

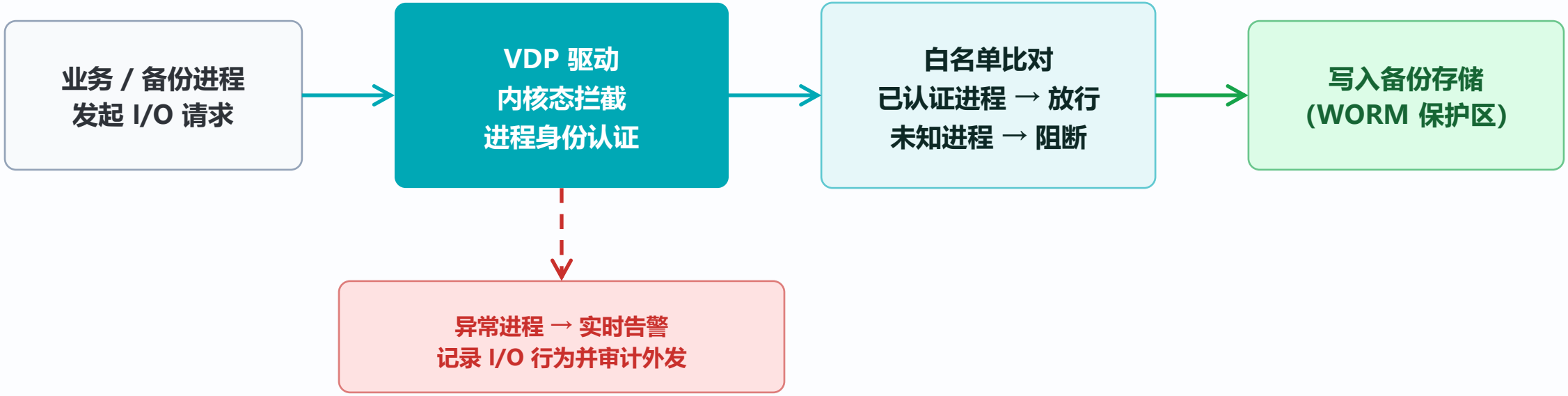
· 物理磁带离线副本

· IPSAN / FC-SAN / NAS 全兼容

# 防篡改对比

vinchin

## 所有 I/O 必须经过进程认证，异常即拦截




**与 Veeam 的本质差异：** Veeam 的不可变是"应用层规则"——一旦攻击者拿到 Veeam 服务账号或 root 权限，规则可被绕过；VDP 工作在内核态，即使备份管理员密码泄露，未通过认证的进程仍无法读写备份存储。

实时监控后台进程，第一时间识别勒索软件横向移动到备份节点的行为，从存储层切断攻击路径。

# 病毒查杀对比

vinchin

## 内置杀毒引擎 + 隔离沙箱：开箱即用，Veeam 需外挂工具

| 能力维度 | Veeam | 云祺 |
| --- | --- | --- |
| **杀毒引擎** | Threat Hunter / Recon Scanner 属高级模块，配置门槛高 | 内置杀毒引擎，备份完成自动查杀，零配置开箱即用 |
| **隔离环境** | Clean Rooms 需独立沙箱环境，额外资源投入 | 容灾演练平台内置完全隔离数据沙箱，不连生产网络 |
| **扫描时点** | 备份前 / 备份中 / 备份后三段式，需分别开关 | 备份完成即扫，恢复前再扫一次，双重确认干净 |
| **溯源取证** | IoC 工具集，需安全团队手动分析 | 任意备份点一键在隔离环境拉起，业务人员即可溯源 |
| **处置操作** | 标记可疑恢复点，人工判断是否恢复 | 支持取消恢复 / 断网恢复 / 杀毒后再恢复三档自动处置 |

**实际价值：**

常规备份软件无法感知备份数据已被感染，往往等生产再次拉起时才发现。云祺在备份落盘瞬间就完成查杀，避免"把病毒也一起备份下来"。

# 安全恢复杜绝二次感染

vinchin

## 恢复前再扫一次：杜绝把病毒恢复回生产；零成本自动演练

### 安全恢复三档处置（恢复前查杀）

**档一：取消恢复**
发现高风险病毒，直接中止恢复作业，避免污染生产。

**档二：断网恢复**
恢复到隔离网络，先观察再决定是否接入生产。

**档三：杀毒后恢复**
在沙箱内自动清除病毒，再把干净数据恢复生产。

### 常态化演练：零资源成本，自动出报告

· **Veeam 对比：**验证功能在部分平台受限，初始配置复杂，需要额外准备外部验证环境与资源。
· **云祺做法：**内置容灾演练平台，不准备外部环境，自动完成备份数据完整性、可用性核验。
· **输出物：**演练完成自动生成可视化验证报告，直接用于等保测评、内审汇报与监管检查。

# 运维 / 部署架构对比

vinchin

## 云祺：单一系统「多合一」灾备管理

统一 WEB 控制台 · 向导化操作

| | | | |
|---|---|---|---|
| 数据备份 | 业务容灾 | 勒索恢复 | 数据验证 |
| 业务迁移 | 副本管理 | 数据归档 | 日志审计 |

**智能运维三件套（同一控制台内）**

**任务编排：**自定义编排任务顺序与触发条件，备份、恢复、验证等任务自动化串联运行

**备份集群：**多备份节点统一管理，按资源负载动态调度，多节点并行提升备份效率

**DataV 大屏 + 报表：**可视化大屏实时监控 + 按模块自定义报表，运维状态一目了然

## Veeam：平台 + 组件 + 版次组合

多产品组合 · 按版次解锁

**Veeam Data Platform**

备份恢复核心；安全与编排高级能力集中在 Proactive / Premium 版次

**Veeam ONE**

监控、报表、分析；Security & Compliance Analyzer 合规评估

**Recovery Orchestrator**

恢复编排、DR 测试、自动化文档

**Cyber Secure + Coveware**

勒索响应服务、勒索保修（付费增值项目）

**65+ 安全生态集成**

SIEM / SOAR / XDR / 防火墙联动，需逐一集成配置

技术路线差异：云祺把验证、编排、大屏做成同一系统的原生模块，「一套系统 = 一个控制台 = 一份授权」；Veeam 通过组件组合实现同等能力，功能上限更高，但组件间集成、版次与授权管理本身成为运维工作的一部分。

# 运维 / 管理控制台对比

vinchin

## 单 Web 控制台管到底 vs 三个客户端来回切

| 运维维度 | 云祺 vinchin | Veeam |
| --- | --- | --- |
| **访问入口** | 单一 Web UI，浏览器登录即用 | B&R Console（Win 客户端）+ Enterprise Manager Web + Veeam ONE Client，三端切换 |
| **多租户/多站点** | 原生多组织、多备份服务器统一纳管 | Enterprise Manager 集中管理，需额外授权 |
| **自动化编排** | 智能作业编排，策略批量下发，容量在线扩 | PowerShell 脚本 / REST API，需二次开发 |
| **操作审计** | 任务日志 + 系统操作日志全程留痕可追溯 | 历史记录需查 SQL 数据库或导出 CSV |
| **移动端/远程** | Web 响应式，手机/平板可看大盘与告警 | 仅 Web 仪表盘有限视图，操作须回 Console |

# 运维 / 监控告警对比

vinchin

## 云祺：开箱即用的告警矩阵

**告警覆盖：**

· 备份作业成功/失败/超时通知

· 存储池容量阈值告警

· 节点在线状态、资源利用率告警

· 备份数据完整性校验异常告警

**通知通道：**

· 邮件 / 短信（开箱配置）

· 钉钉 / 企业微信 / 飞书 Webhook

· 与国产运维平台通过 REST API 对接

**自动验证：**定期自动校验最新备份点可恢复性，自动出报告。

## Veeam：Veeam ONE 是另一个产品

**监控能力：**

· 200+ 项预设告警、智能诊断、自动补救策略

· 能力强，但属于 Veeam ONE 高级模块

**部署代价：**

· Veeam ONE Server + Web + Client 三件套

· 必须依赖独立 Microsoft SQL Server

· 大环境需拆分部署、单独 License

**国产 IM：**邮件/Slack/Teams 原生，钉钉/企微需通过 Orchestrator 脚本或第三方插件打通。

# 运维 / 服务与 TCO 对比

vinchin

| 服务维度 | 云祺 vinchin | Veeam（海外总部） |
| --- | --- | --- |
| **响应方式** | 原厂 7×24 电话/远程/上门，中文母语工程师 | 国内靠代理商一线，二线走海外工单，时差明显 |
| **交付形态** | 软件/超备一体机开箱即用，含实施+培训+演练协助 | 纯软件 License，硬件/实施另算，专业服务按人天 |
| **License 授权** | 按物理 CPU/虚拟机授权，安全+运维功能同包，不拆高级模块 | 标准版/企业版/增强版分级，Threat Hunter、Clean Rooms、Veeam ONE 均加购 |
| **合规与源码** | 国产自研源码，可做安全评估、密评、等保配合 | 境外闭源，关键行业采购受供应链审查与出境数据约束 |
| **POC 与替换** | 免费功能试用，POC 期间原厂工程师协助，平滑切换 | NFR 试用版，替换期需代理商和咨询方共同实施 |
| **升级方式** | Web 内一键升级，节点灰度滚动，业务不中断 | 需下载补丁包逐台安装，大版本升级要重启 B&R Server |
| **迁移替换** | 提供 POC 评估、Veeam 备份数据迁移工具、原厂陪跑切换 | 迁移工具偏 VMware 生态，国产环境需第三方实施 |

vinchin

# PART 02

# 云祺智能防护实践

# 安全 × 运维全维度能力12 项对照

vinchin

| 能力项 | 云祺 | Veeam |
| --- | --- | --- |
| 无代理备份 | 虚拟化/物理机/云 全平台统一无代理，零客户端 | 核心平台无代理，国产平台需代理或不支持 |
| 不可变备份 | 系统内建 VDP+WORM，无硬件依赖，root 不可删改 | Hardened Repo / Object Lock(对象存储），依赖特定存储形态 |
| 病毒查杀 | 内置 病毒查杀引擎，备份/验证/恢复全阶段自动查杀 | Inline 扫描 + Secure Restore（需对接第三方杀软） |
| 威胁检测 | 内置查杀 + 完整性校验告警 + 自动重备 | Recon / Threat Hunter / YARA / IOC，检测体系更庞大（高版次） |
| 加密与合规 | AES-256 + SM2 国密，恢复口令二次验证 | AES-256 + MFA + 4-eyes，面向国际合规，国密缺位 |
| 验证演练 | 内置演练平台零额外资源，自动验证报告在线审批 | DataLabs / SureBackup，洁净室与编排按版次授权 |
| 实时容灾 | CDP 秒级 RPO≈0，备机自动接管 + 一键回切 | 复制 + Failover，Orchestrator 编排切换 |
| 瞬时恢复 | 异地副本 15 秒拉起，不触碰原始备份 | Instant Recovery，官方口径最高 5x |
| 部署运维 | 0 客户端，备份端升级一次全网生效 | 长尾负载逐机装代理、逐机升级 |
| 监控告警 | DataV 大屏 + 邮件/短信告警 + 统一日志平台 | Veeam ONE：AI 诊断 / 容量预测 / SIEM 联动更深入 |
| 授权模式 | 一套系统一份授权，八项能力原生内置 | 平台版次 + 组件 + 订阅组合授权 |
| 信创适配 | 芯片/OS/数据库/虚拟化全栈适配 + 信创工委会单位 | 信创生态适配滞后，暂无国产化目录路径 |

# 信创合规适配

vinchin

| 合规要求 | 核心义务 | 云祺对应能力 |
| --- | --- | --- |
| **《数据安全法》《网络安全法》《个人信息保护法》** | 重要数据备份与灾备义务，防止数据篡改、泄露、丢失 | 本地 / 异地备份副本 + 远端增量复制；端到端加密防泄露；WORM 防篡改 |
| **等保 2.0 及 GA-T2380-2026（三级以上）** | 备份恢复能力 + 定期灾难恢复演练验证要求 | 内置容灾演练平台零资源演练；验证电子报告自动生成、在线审批、全程可溯 |
| **信创替代政策** | 重要信息系统自主可控、国产化替代 | 完全自研、自有知识产权；芯片 / OS / 数据库 / 虚拟化全栈国产适配；信创工委会技术活动单位 |
| **行业规范（医保影像云、交通运输数据安全等）** | 分级 RTO / RPO 合规可控，业务分级防护 | CDP 秒级 RPO + 热 / 温 / 冷分层存储，按业务重要性分级保护策略 |
| **商用密码应用要求** | 关键信息基础设施需采用商用密码保护 | SM2 国密链路加密（Veeam 不支持国密），网络安全专用产品安全检测证书 |

生态身份：信创工委会技术活动单位 · 2024 信创 500 强 · 国家级专精特新——SM2 国密与信创目录资质为相较于 Veeam 的独有项。

# 云祺落地场景

vinchin

| 事故场景 | 典型表现 | Veeam 应对 | 云祺应对 |
| --- | --- | --- | --- |
| **防勒索攻击** | 生产与备份副本同时被加密；攻击者删除备份存储 | 不可变仓库限特定存储；Clean Rooms 需额外沙箱；Threat Hunter 高级版 | WORM + VDP 内核驱动三层兜底；内置杀毒沙箱，恢复前再扫；磁带离线 |
| **软硬件故障** | 磁盘坏道、RAID 降级、存储控制器异常、服务器宕机、虚拟化平台崩溃、数据损坏 | 靠硬件监控；Instant Recovery 限 VMware；复制容灾限虚拟化平台 | 硬件健康纳入平台监控；跨国产虚拟化瞬时接管、备机自动接管整机业务（自动识别数据库等应用）分钟级拉起；任意时间点回退；故障修复后一键回切且数据完整 |
| **误操作** | 误删数据库表、误格式化卷、误删虚拟机 / 文件、误改配置、恶意管理员删库 | 不支持数据库级恢复；需整机恢复后导出；CDP 另购 | Oracle / MySQL / 达梦单表单记录恢复；数据库 CDP 毫秒级时间点回退 |
| **资源 / 容量告警** | 备份作业失败、CPU/内存过载、存储容量告急、节点异常、任务堆积 | Veeam ONE 监控：热图、容量预测、假设建模；智能诊断 + 自动化补救；告警可触发动作（如自动加入 SureBackup 验证） | 可视化大屏实时呈现存储/节点/任务状态；邮件、短信告警第一时间触达；备份集群按资源负载动态调度 |
| **机房级灾难** | 机房断电、火灾、区域级灾害导致生产中心整体失效 | 异地副本 + 副本互备容灾；源端压缩、远端增量、断网续传适配弱网；容灾备机一键接管，业务异地快速切换 | 异地副本 / Cloud Restore 云端拉起；Data Cloud Vault 不可变异地副本；恢复编排保障切换有序 |

# 云祺智能防护总结

vinchin

### 安全 Secure

· WORM + VDP 内核驱动
· 端到端加密 + 国密
· 内置杀毒沙箱
· 零信任默认开启

### 全面 Comprehensive

· 整机 / 数据库 / 文件全覆盖
· VMware / 华为 / 深信服 / 新华三
· Oracle / MySQL / 达梦 / 人大金仓
· Windows / Linux / 麒麟 / 统信

### 弹性 Elastic

· 瞬时恢复秒级拉起
· 跨云 / 跨平台恢复
· 副本互备、异地容灾
· 一体机 / 软件 / 云交付

### 智能 Intelligent

· 自动完整性校验
· 演练自动出报告
· 容量趋势预测
· 异常行为告警

## 实施情况

· 已在**金融、医疗、制造、政务、教育、交通**等行业规模落地，覆盖等保 2.0 三级、医保影像云、金融两地三中心等场景。
· 提供 15 天免费试用版，支持从 POC 到规模替换的完整路径；本地原厂 7×24 支持，配合等保测评与密评整改。
· Veeam 平滑迁移：备份作业自动导入、保留策略对齐、恢复点验证，不中断现有业务。

# 云祺替换 Veeam：安全灾备建设

vinchin

## 选择云祺，不只是替换 Veeam，
## 更是把备份系统升级为安全备份中枢

### 事前

WORM + VDP + 国密加密

把备份库建成外部拿不到、内部改不动的金库

### 事中

内置杀毒 + 自动校验 + 异常告警

让被感染的备份和异常行为被自动看见

### 事后

瞬时恢复 + 细粒度 + 安全演练

确保真出事时业务能秒级拉起、恢复数据干净可用