vinchin

勒索病毒现状与防范

RANSOMWARE STATUS AND PREVENTION

云数据中心备份存储保护

主讲人:陈洪帆　职位:产品经理

关注云祺公众号，获取更多解决方案

www.vinchin.com | 400-9955-698 | support@vinchin.com

CONTENTS

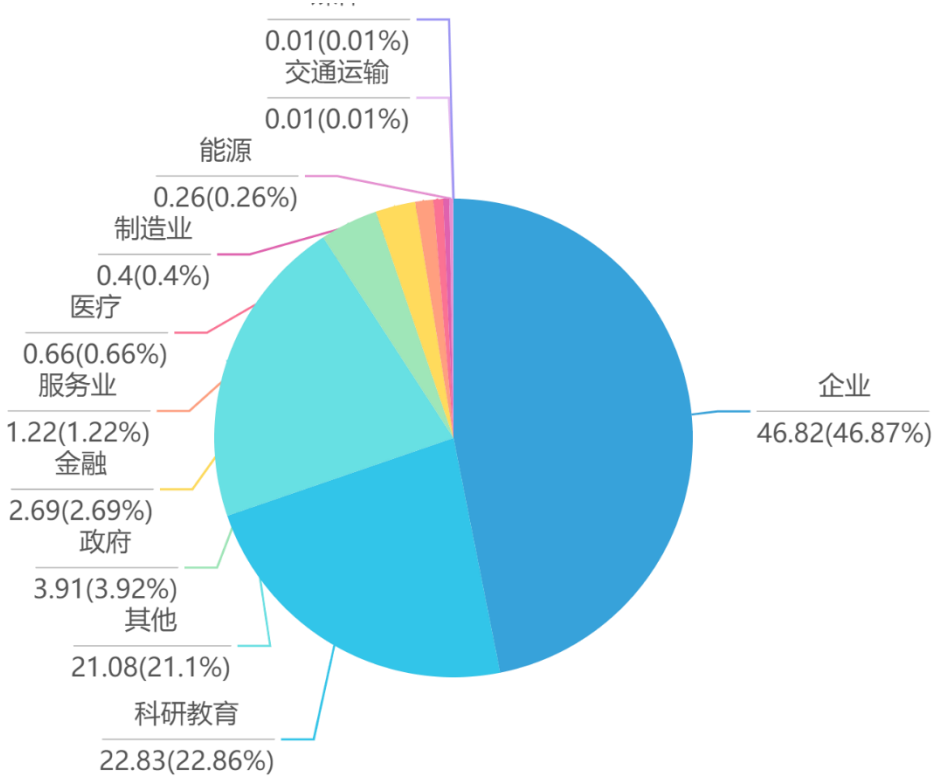
01

勒索病毒背景介绍

Chengdu Vinchin Technology Co.,Ltd.

勒索病毒感染态势

2021年勒索病毒全行业感染情况



勒索病毒感染主要行业

全年勒索攻击总次数

22,349,579

数据来源：深信服2021年度勒索病毒态势报告

勒索攻击大事件

2021.03

acer

被索要3.3亿

2021.03

CNA

支付2.6亿

2021.05

JBS

支付7500万

2021.05

关闭东海岸运输管道

勒索病毒介绍

勒索病毒，是一种特殊的恶意软件，又被人归类为“阻断访问式攻击”（denial-of-access attack）

据“火绒威胁情报系统”监测和评估，从2018年初到9月中旬，勒索病毒总计对超过200万台终端发起过攻击，攻击次数高达1700万余次，且整体呈上升趋势。

该病毒在全球范围内造成了巨大的影响，其攻击用户的方式也是多种多样，让用户防不胜防。

勒索病毒特征

攻击路径
多样化

- 广告链接
- 恶意邮件
- 木马病毒
- 安全漏洞
- 移动介质
- RDP攻击

攻击目标
多元化

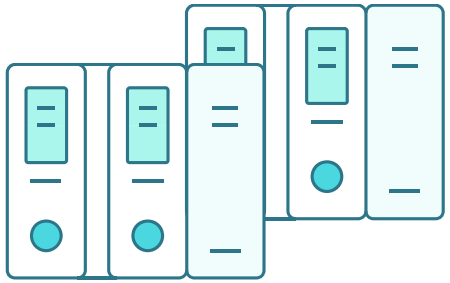
电脑端
个人用户

移动端
企业服务器

病毒变异
不可控

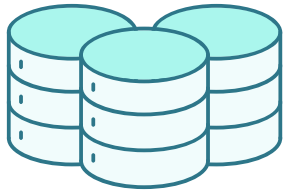
- Reveton
- CryptoLocker
- CryptoLocker.F
- TorrentLocker
- CryptoWall
- RSA4096
- WannaCrypt
- Petya
- …

关键信息被破坏



生产服务器集群

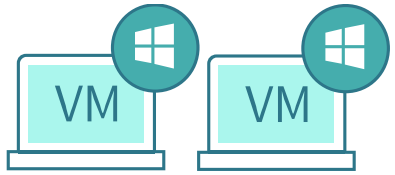
勒索攻击



核心数据库

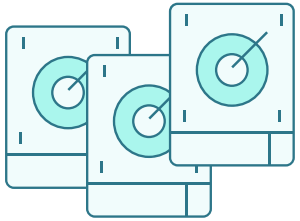
业务中断

系统加密



办公电脑

勒索攻击



文件

文件加密

信息盗取

政府 教育 医疗 制造 零售 金融 能源

02

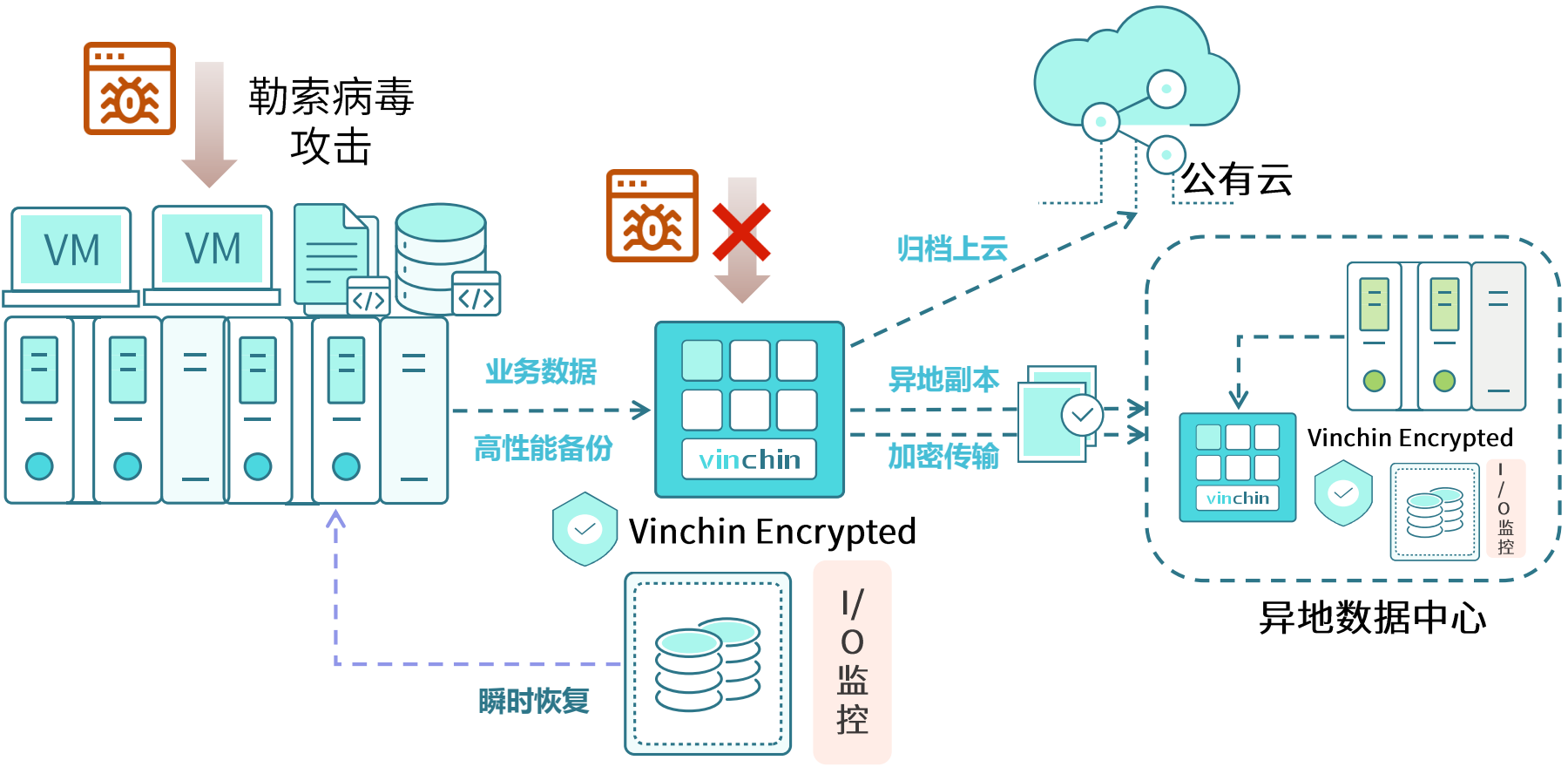
云祺防勒索解决方案

Chengdu Vinchin Technology Co.,Ltd.

防勒索方案分析

	解决方案	分析方案
网络安全方向	在网络出入口做一系列拦截策略，利用防火墙、网络边界设备、探针等，构建终端检测、安全感知平台，拦截勒索病毒。	网络设备的拦截策略依然是依赖与病毒库和特征码的，病毒的变异速度是我们无法估量的，无法做到精准的查杀和拦截。
公有云厂商	利用云端病毒库进行主动查杀和防御，以及对象存储的WORM功能，实现数据仅可读，难修改的效果，避免被误删除。	主动查杀和防御功能高度依赖病毒库的更新，时效性较差，防御容易失效。方案复杂，仅限定对象存储才可以实现以上效果。

防勒索备份解决方案



全面数据保护

- ✓ 提供业务系统的高效备份、异地副本、数据上云及归档功能
- ✓ 提供RPO约等于0的实时备份保护以及应急接管

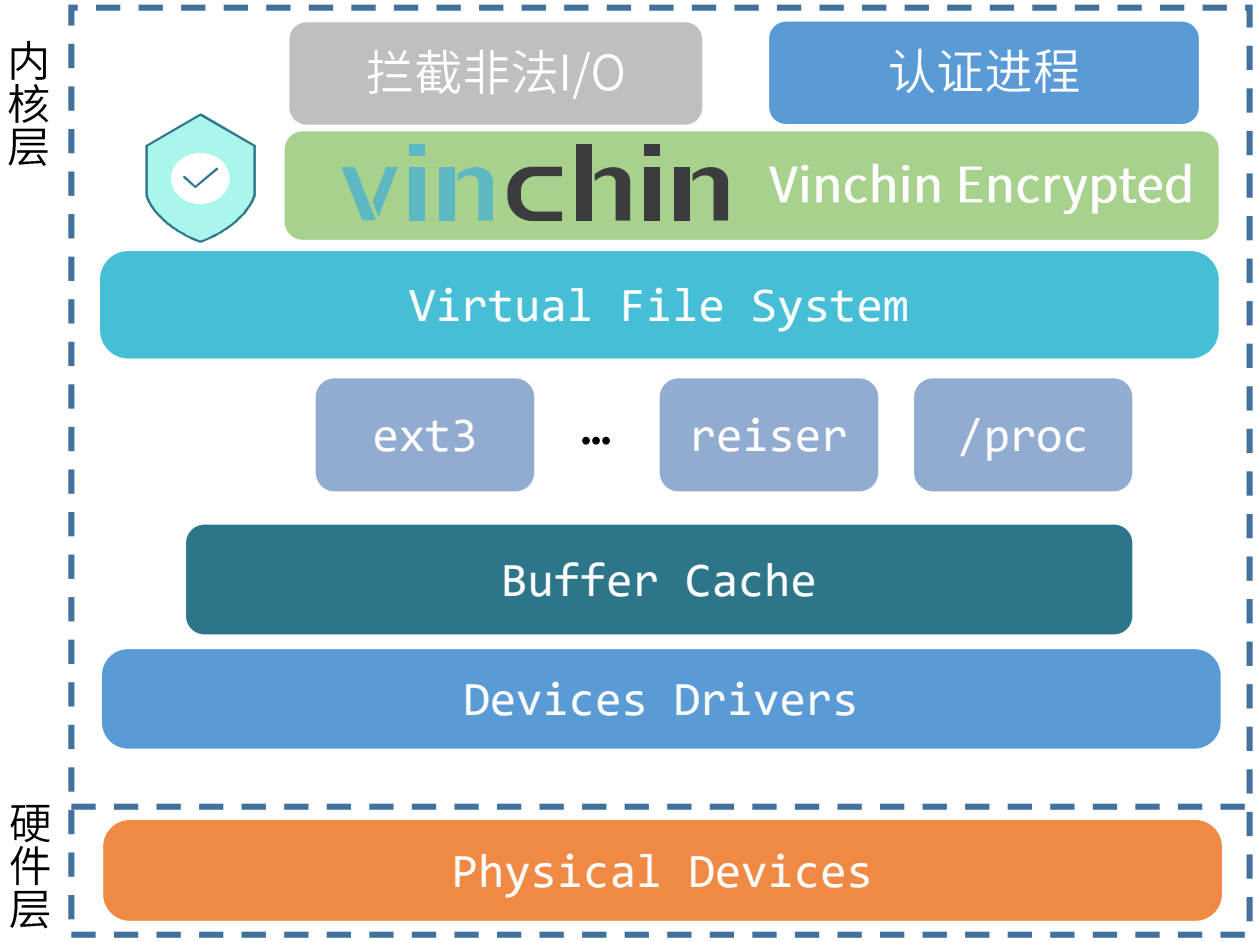
内核级存储保护

- ✓ 支持Vinchin Encrypted实时保护备份数据不被恶意破坏

高效恢复

- ✓ 支持瞬时恢复，秒级拉起，分钟级恢复业务系统

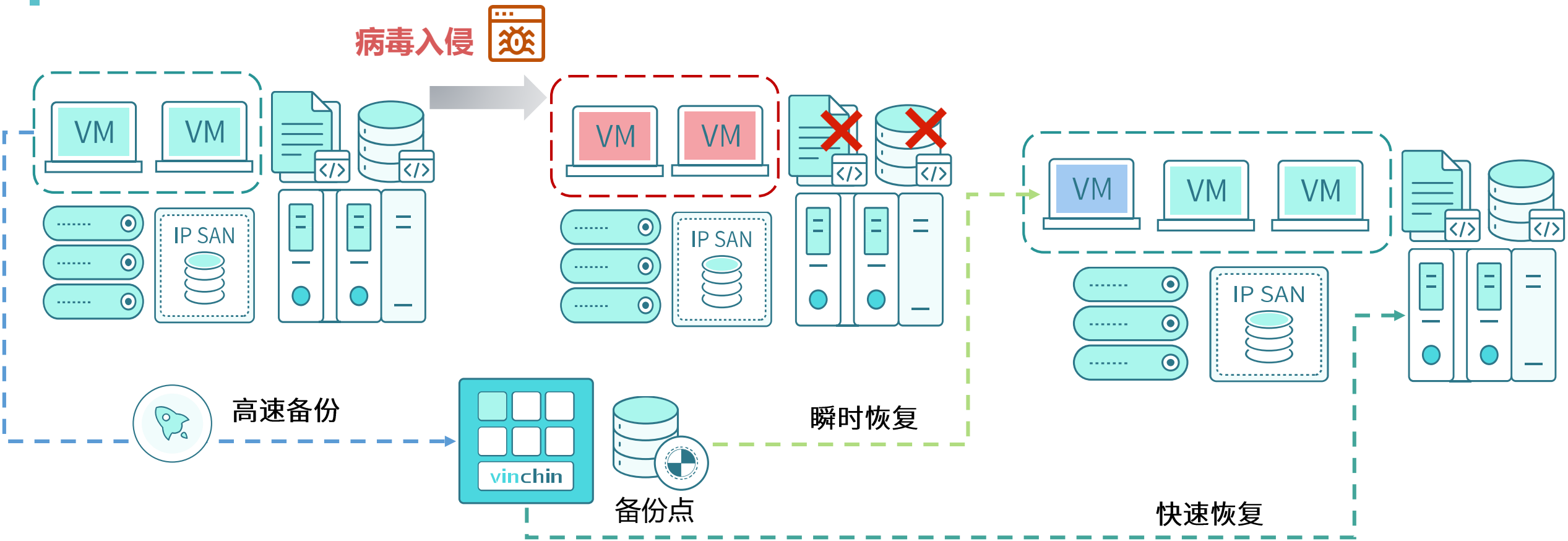
Vinchin Encrypted原理介绍



云祺防勒索方案核心原理

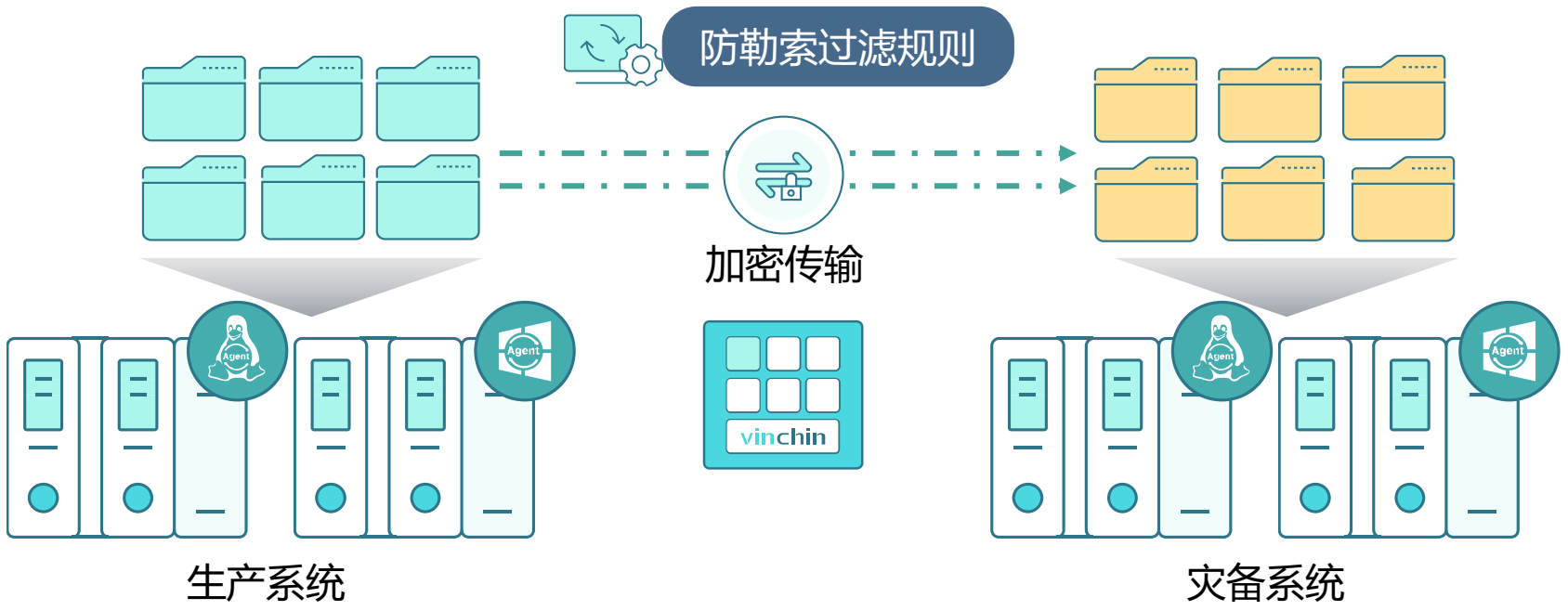
云祺在系统内核层注入Vinchin Encrypted核心进程，实时监控系统I/O情况，拦截非法进程对存储数据的恶意修改和删除，确保备份数据的安全

面向业务系统的防勒索病毒场景



✓ 通过已备份的虚拟机备份点数据，进行解压缩，利用瞬时恢复快速挂载给正常的业务平台，达到快速恢复业务系统的目的。

面向海量文件的防勒索方案



- ✓ 可自定义的文件同步过滤规则
- ✓ 屏蔽被勒索病毒修改后的文件
- ✓ 备份即用，灾备端可以直接使用备份数据，无需恢复

03

数据保护案例

Chengdu Vinchin Technology Co.,Ltd.

勒索病毒感染客户1


它真的来了...泰国某物流公司VMware虚拟机被勒索病毒感染!

Back IT Up 云祺 2021-03-19 12:10

收录于话题
#勒索软件攻击 17 #网络攻击 17

vinchin

它真的来了!

就在昨天云祺科技发布出现虚拟机勒索病毒的新闻后（具体内容请看 VMware用户请注意...），我们收到了来自泰国某物流公司用户的求助，他们的**VMware虚拟机也中了勒索病毒!**

根据反馈，用户数据中心约**30%VMware**虚拟机被勒索病毒攻击，其中重要的**物流业务数据均被加密**，导致他们**部分物流工作被迫中止**。按照"惯例"，他们需要支付一定的赎金才能拿回数据。

云祺的用户当然不用支付这笔额外费用，因为定期备份的良好习惯让用户遇"勒索"不慌。

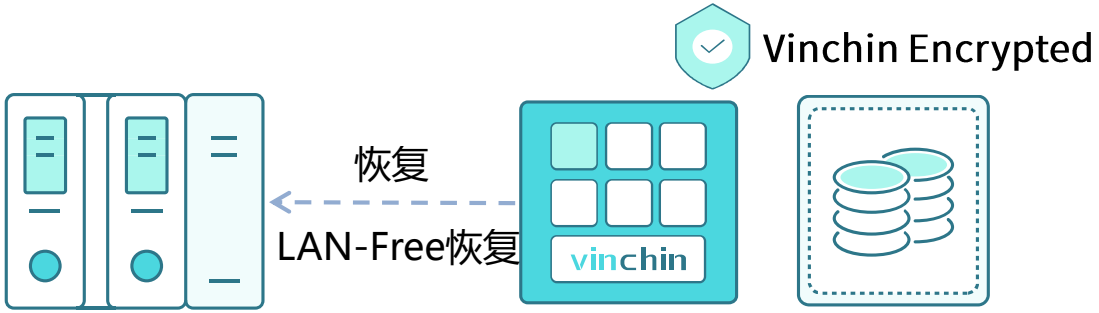
Vinchin &

昨天 12:44

luwen can i restore many vm at the same time?

2021年泰国某物流公司VMware虚拟机被勒索病毒感染

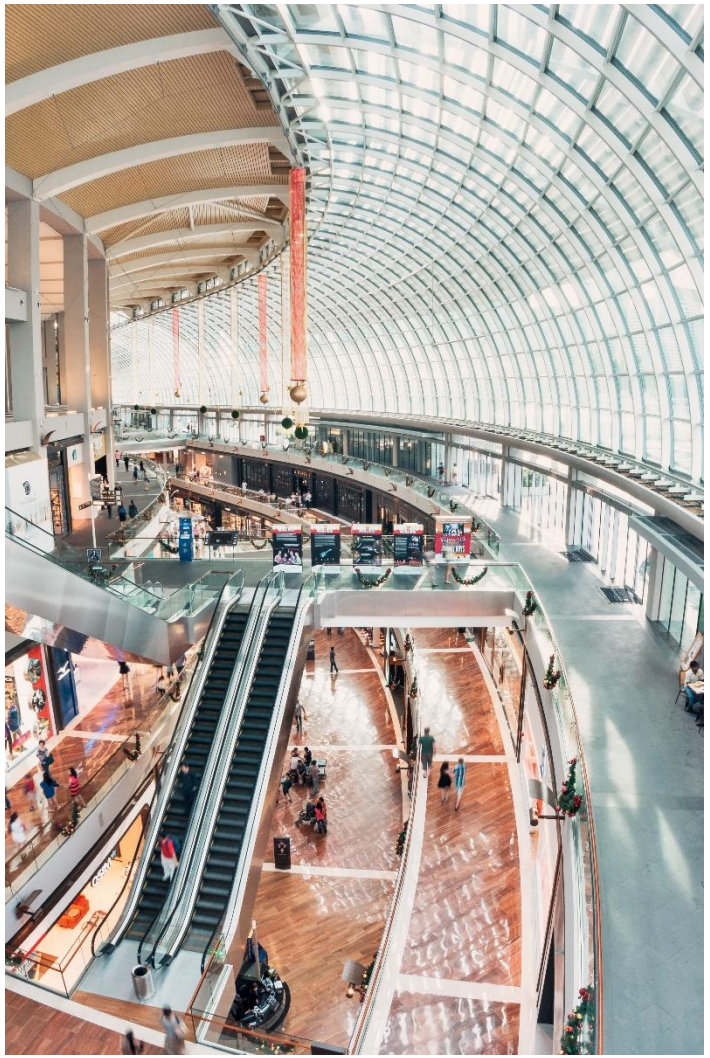
客户的数据中心有30%的VMware虚拟机被勒索病毒攻击，其中最为**重要的物流业务数据均被加密**，导致公司部分物流**工作被迫停止。**



得益于Vinchin Encrypted的保护下，勒索病毒并未感染备份存储中的备份数据。

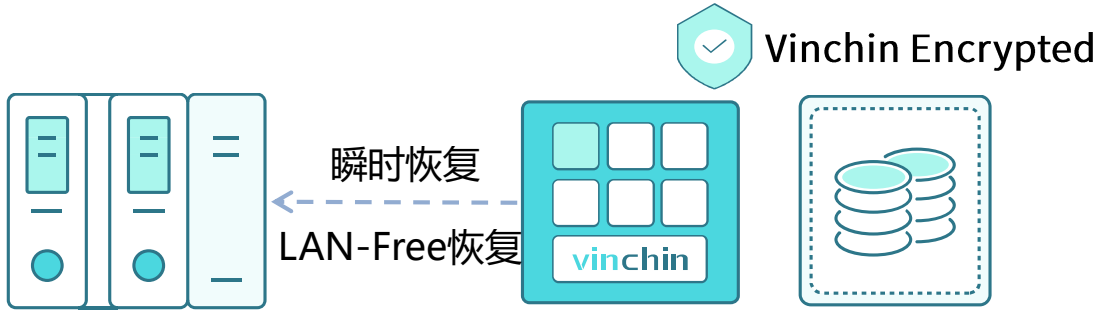
云祺工程师将虚拟机数据成功恢复回生产系统，业务也得以继续进行。

勒索病毒感染客户2



2022年成都某购物商城VMware虚拟机被勒索病毒感染

购物商城负责结算的核心虚拟机被勒索病毒攻击，**交易数据被加密**，导致购物中心部分结算节点**被迫停止交易**。



云祺售后工程师利用瞬时恢复功能将重要的虚拟机在**30秒内**拉起，**10分钟内**完成数据验证和业务系统恢复，大幅度降低了业务中断时间，不停机的状态下通过在线迁移将数据传输回生产系统。

THANKS

CHENGDU VINCHIN TECHNOLOGY CO.,LTD.

www.vinchin.com | 028-85530156 | support@vinchin.com