真实场景模拟
备份防勒索技术应用

V6.0

1 勒索病毒背景及现状
Chengdu Vinchin Technology Co.,Ltd.

2 云祺防勒索解决方案
Chengdu Vinchin Technology Co.,Ltd.

3 功能演示
Chengdu Vinchin Technology Co.,Ltd.

01

勒索病毒背景及现状

Chengdu Vinchin Technology Co.,Ltd.

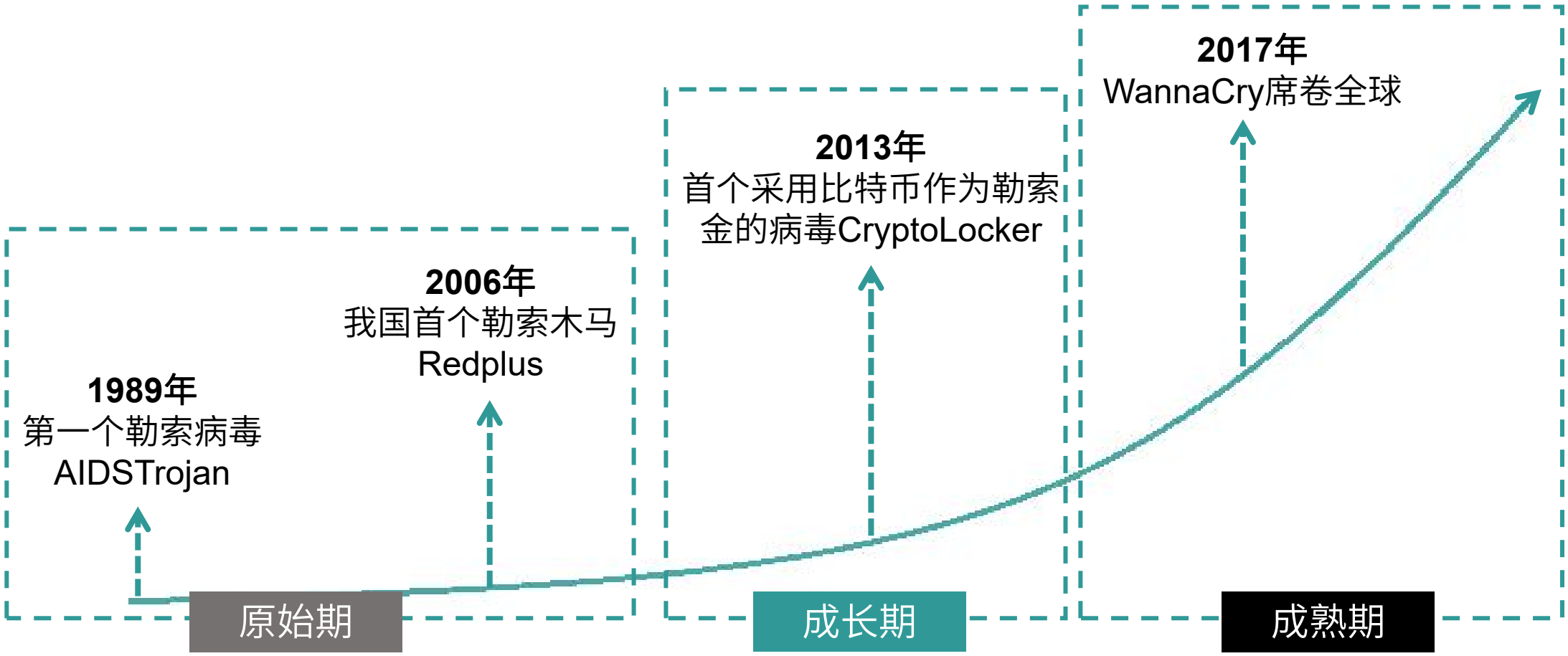
什么是勒索病毒

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。

勒索病毒发展史

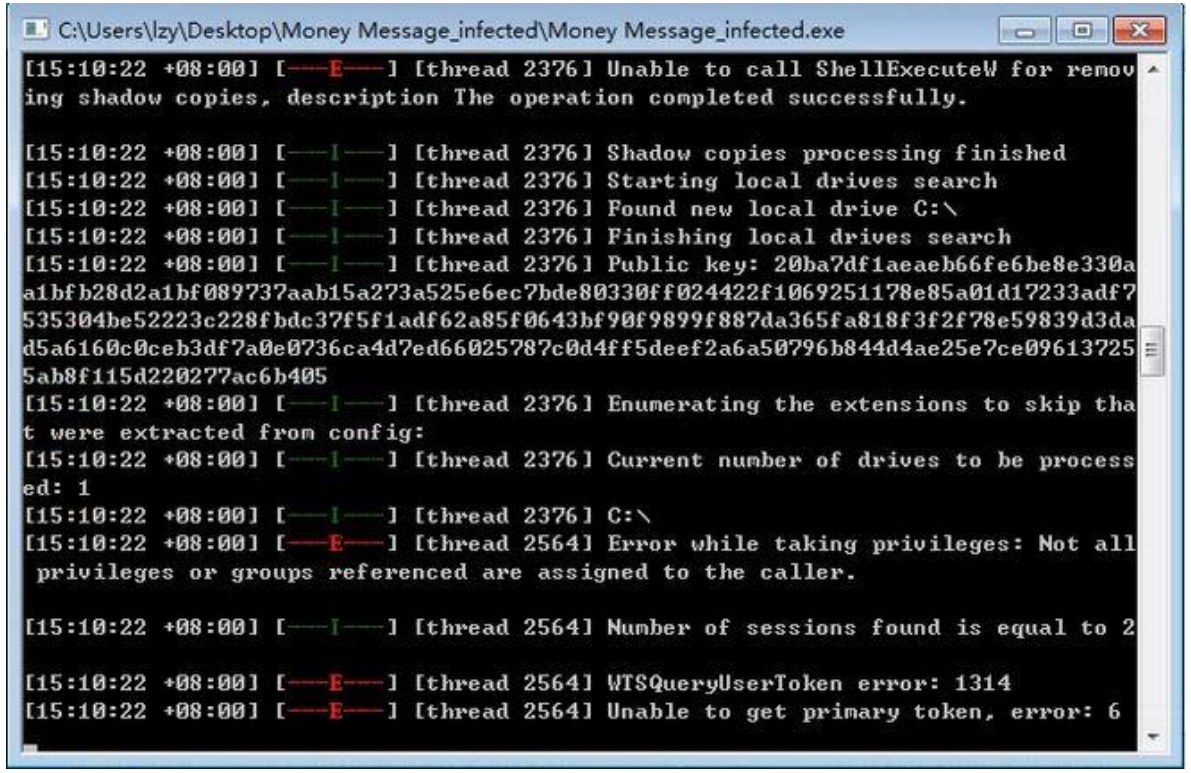

1989年
第一个勒索病毒
AIDSTrojan
2006年
我国首个勒索木马
Redplus
2013年
首个采用比特币作为勒索金的病毒CryptoLocker
2017年
WannaCry席卷全球
原始期
成长期
成熟期

勒索病毒感染态势

数据来源：深信服云端监测

数据来源：深信服云端监测

勒索攻击大事件



数据来源：安全圈

击穿24款杀毒软件

Money Message勒索病毒肆虐全网

近期，一个名为“Money Message”的新勒索软件团伙，大肆攻击全球知名企业，加密、窃取用户数据并索要巨额赎金，该团伙已攻击多家大型企业，包括年收入近十亿美元的孟加拉国家航空公司(Biman airlines)，以及世界知名计算机硬件提供商微星国际（MSI）等。

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

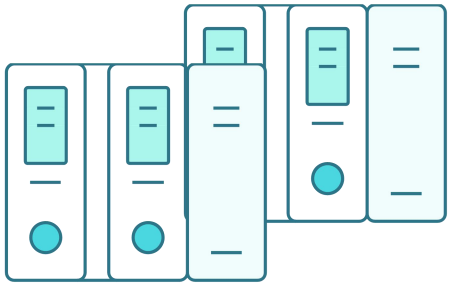
攻击目标多元化

电脑端 个人用户　　移动端 企业服务器

病毒变异不可控

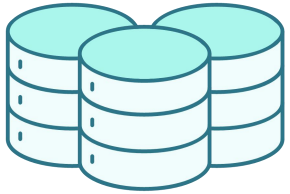
- Reveton
- CryptoLocker
- CryptoLocker.F
- TorrentLocker
- CryptoWall
- RSA4096
- WannaCrypt
- Petya
- …

关键信息被破坏



生产服务器集群

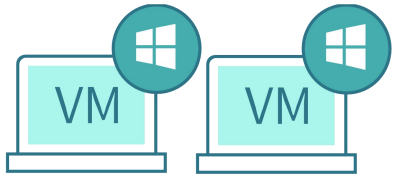
勒索攻击



核心数据库

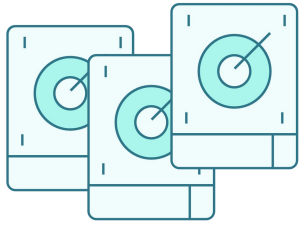
业务中断

系统加密



办公电脑

勒索攻击



文件

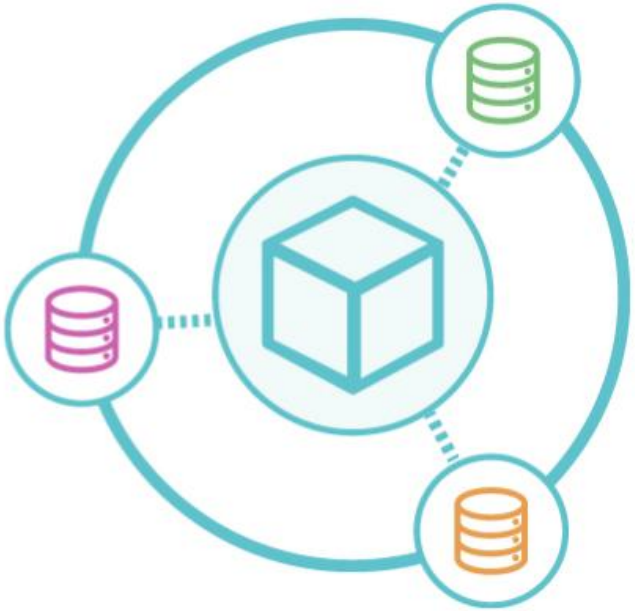
文件加密

信息盗取

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。

如何有效预防勒索病毒



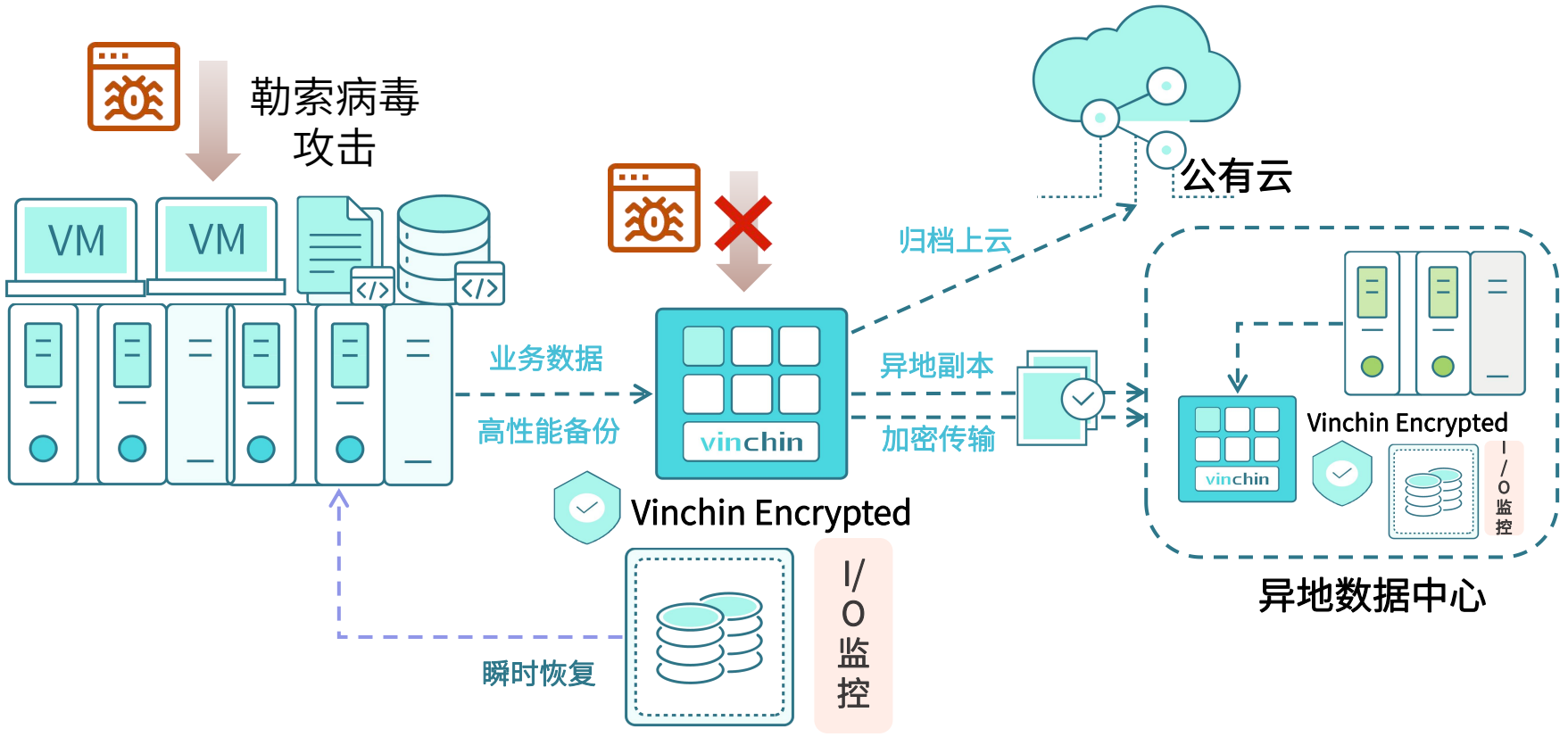
备　份

02

云祺防勒索解决方案

Chengdu Vinchin Technology Co.,Ltd.

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

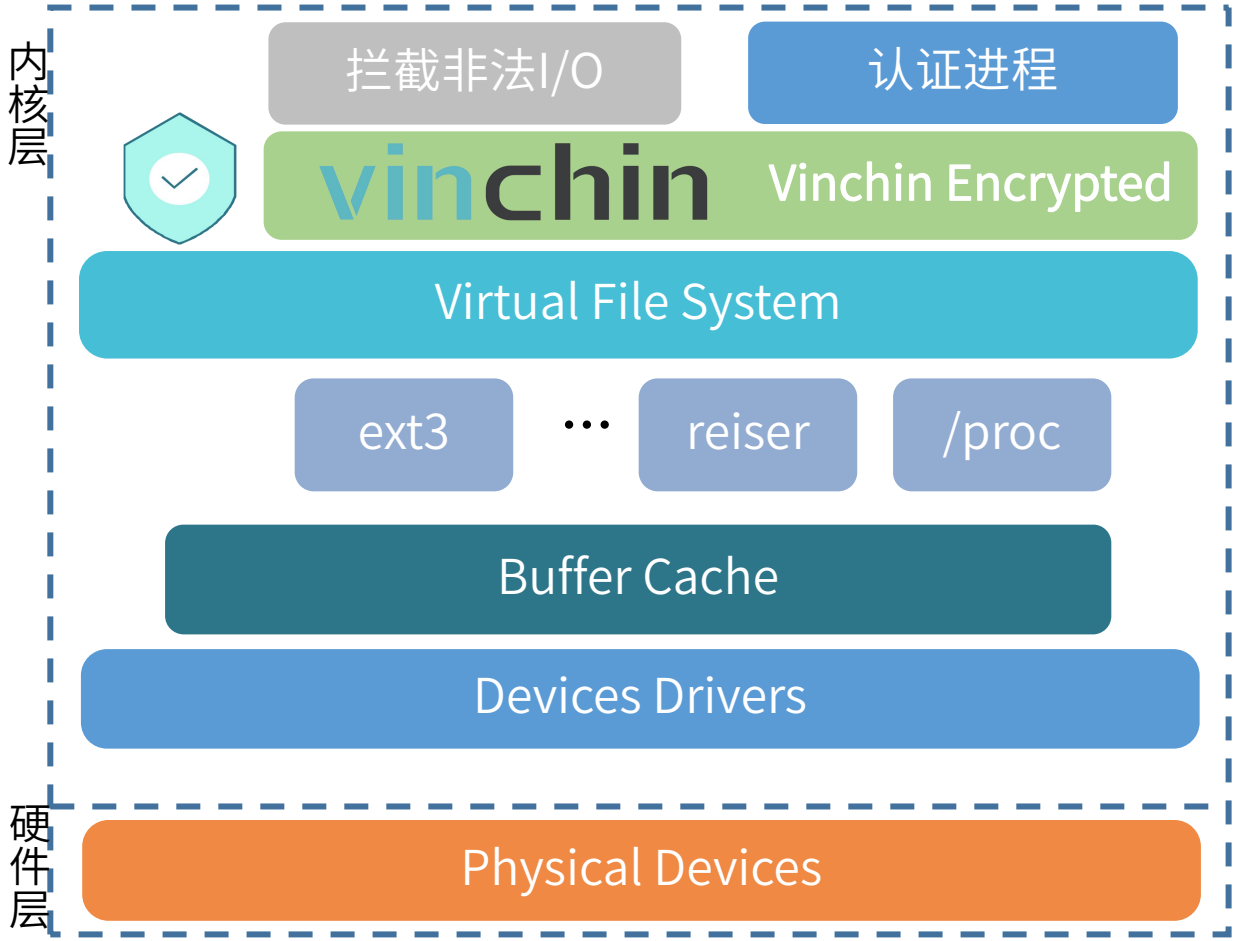
内核级存储保护

✓ 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

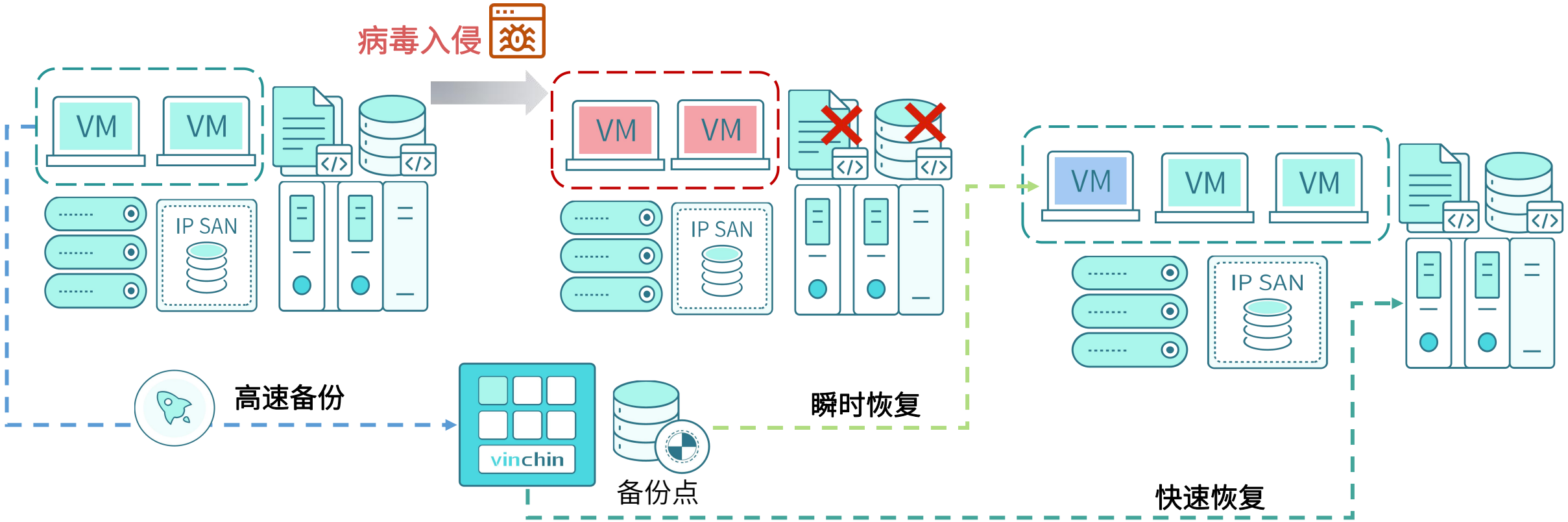
Vinchin Encrypted原理介绍



云祺防勒索方案核心原理

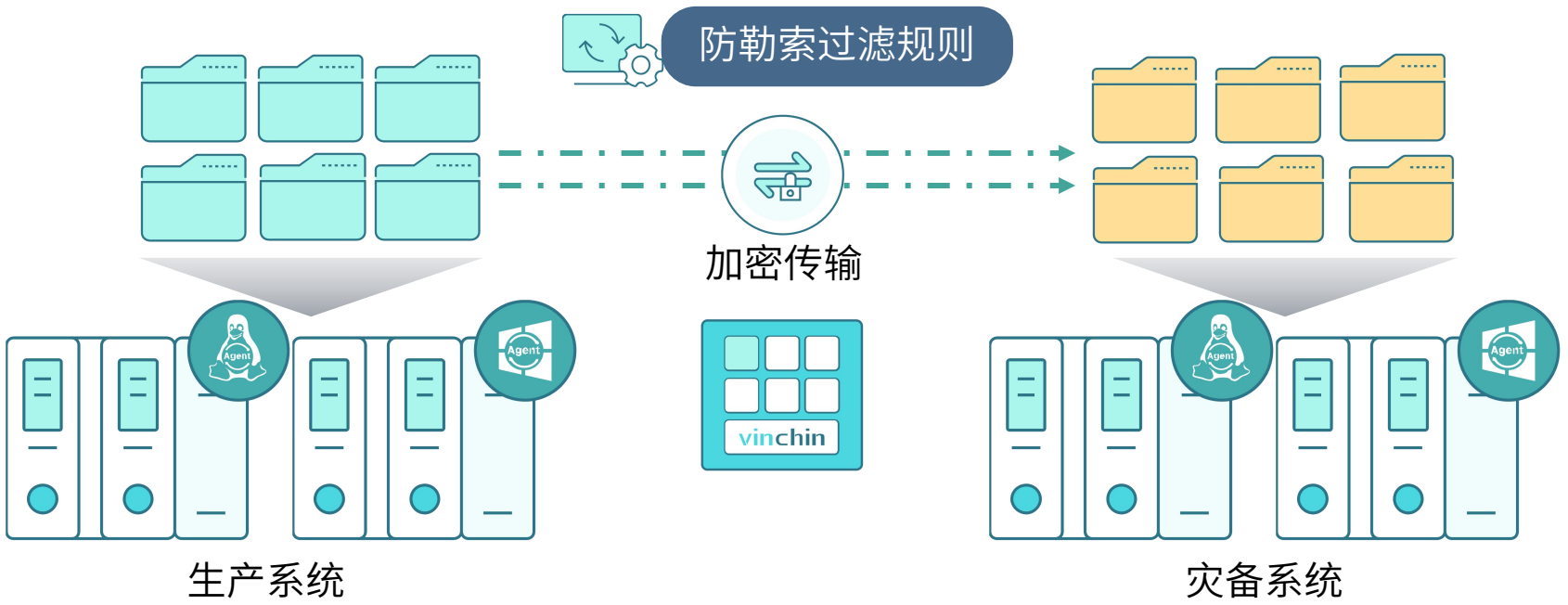
云祺在系统内核层注入Vinchin Encrypted核心进程，实时监控系统I/O情况，拦截非法进程对存储数据的恶意修改和删除，确保备份数据的安全

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。

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

云祺容灾备份系统：免费下载、测试试用

申请测试

登录**官网**：https://www.vinchin.com

下载软件：云祺容灾备份系统

快速**安装**：嵌入系统，10分钟完成部署

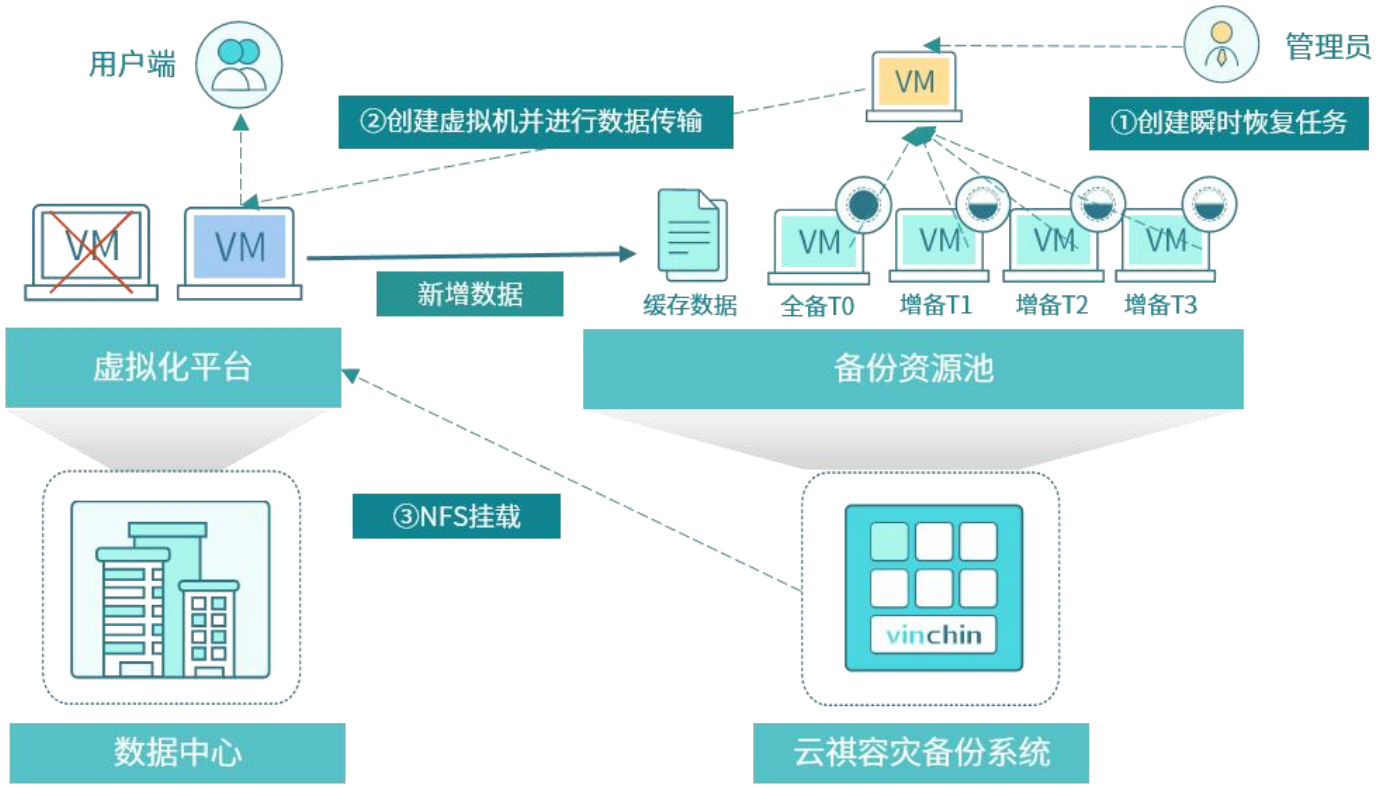
申请授权：在线填写信息申请试用授权

软件**试用**：操作简单，10分钟熟悉软件

03 功能演示

Chengdu Vinchin Technology Co.,Ltd.

演示一



环境介绍

云祺容灾备份系统v6.0

Vmware ESXI 6.7

winserver2012

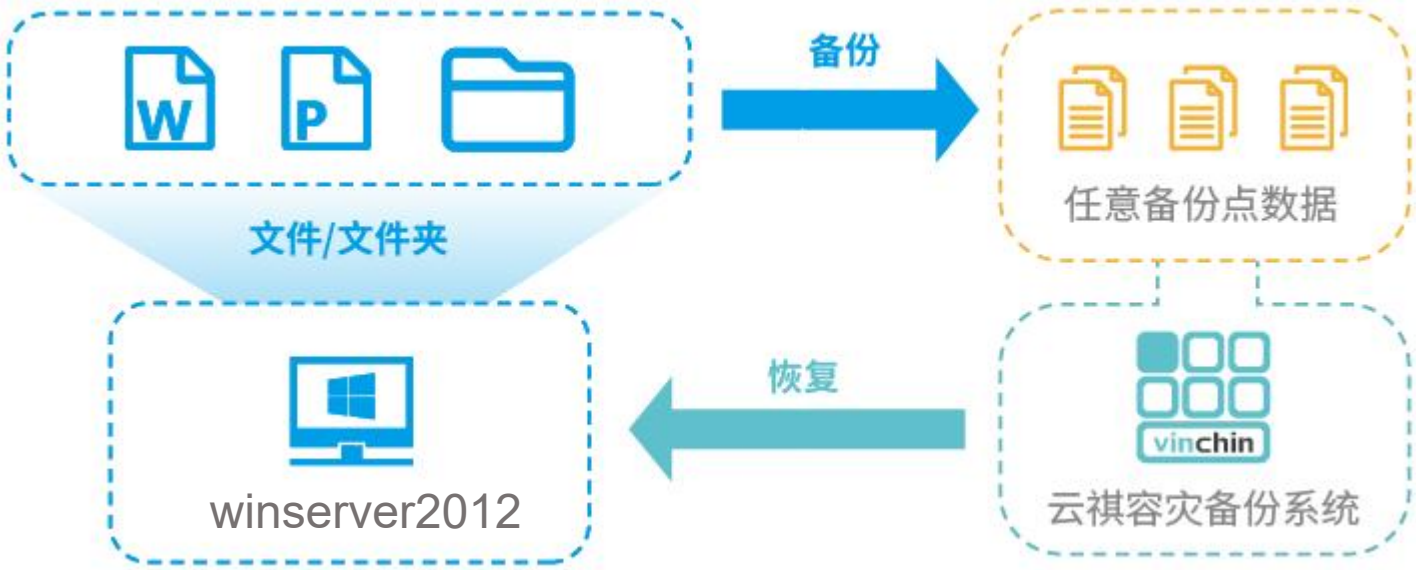
演示内容及步骤

备份winserver2012虚拟机

使用money message使虚拟机文件加密

通过瞬时恢复的方式恢复虚拟机

演示二



环境介绍

云祺容灾备份系统v6.0

winserver2012主机

演示内容及步骤

备份主机中的vinchin文件夹

使用money message使主机文件加密

通过备份系统恢复所需文件

THANKS

CHENGDU VINCHIN TECHNOLOGY CO.,LTD.
www.vinchin.com | 028-85530156 | support@vinchin.com