Acronis 防勒索病毒的原理解析

1、 原理图：

2、 解释：

- Actively Protection 是一种新型的保护机制，不是杀毒也不是使用备份的文件恢复被感染的数据，而是主动判断病毒特征进行自动防护。
- 开启 Active Protection 保护后，安克诺斯保护进程在后台运行
- Active Protection driver 运行在系统底层，监控所有的文件类型变化（安克诺斯是可以完全检测磁盘文件变化的）
- 在文件类型发生改变前后分析文件的内容
    - 如果文件类型内容发生变化->当检测到本地有嫌疑的加密行为发生，Acronis 会记录加密过程，生成加密的日志和事件
    - 当 5 个连续的变化 -> 触发 active protection service 报警，停止病毒进程，根据记录的日志和事件恢复被加密的文件，不会有任何数据被加密，不需用之前的备份进行数据恢复。

3、 已经测试过的病毒样本

List of popular Ransomwares

Ransomware family	Behavior type
Tesla	In-place overwrite
Locky	Via rename
7ev3n	In-place overwrite
CryptoWall	In-place overwrite
Zepto	Via rename
Powerware	In-place overwrite
LeChiffre	In-place overwrite
Cryakl	In-place overwrite
Virlock	Via new file
Petya	Master Boot Record overwriting
CTB-Locker	In-place overwrite/or rename/or new file
Jigsaw	Via new file
Crypaura	Via new file