

安克 诺斯机器学习保护您的数据

Acronis Active Protection是2017年年初推出的一项先进的技术，它使用了复杂的分析来监控系统任何可疑的行为，并快速停止它。在独立测试中成绩卓越，并从媒体获得了多项荣誉。安克诺斯一直在努力使其更好。所以，此次改进的版本结合机器学习和人工智能技术。

机器学习如何帮助？

让我们首先了解下机器学习到底是什么。这个术语通常与大数据相关联——大量数据的分析产生一些可行的结果。数据越多，产生的结果越好。因为机器学习是基于数据的数量和选择的算法。

而安克诺斯机器学习是如何工作的呢？第一步是堆栈跟踪分析。堆栈跟踪是一个报告，提供关于程序的子程序的信息。它通常被用在某些类型的调试中，期间堆栈跟踪可以帮助软件工程师找出问题所在，或者确认在执

行过程中各个子程序如何协同工作。

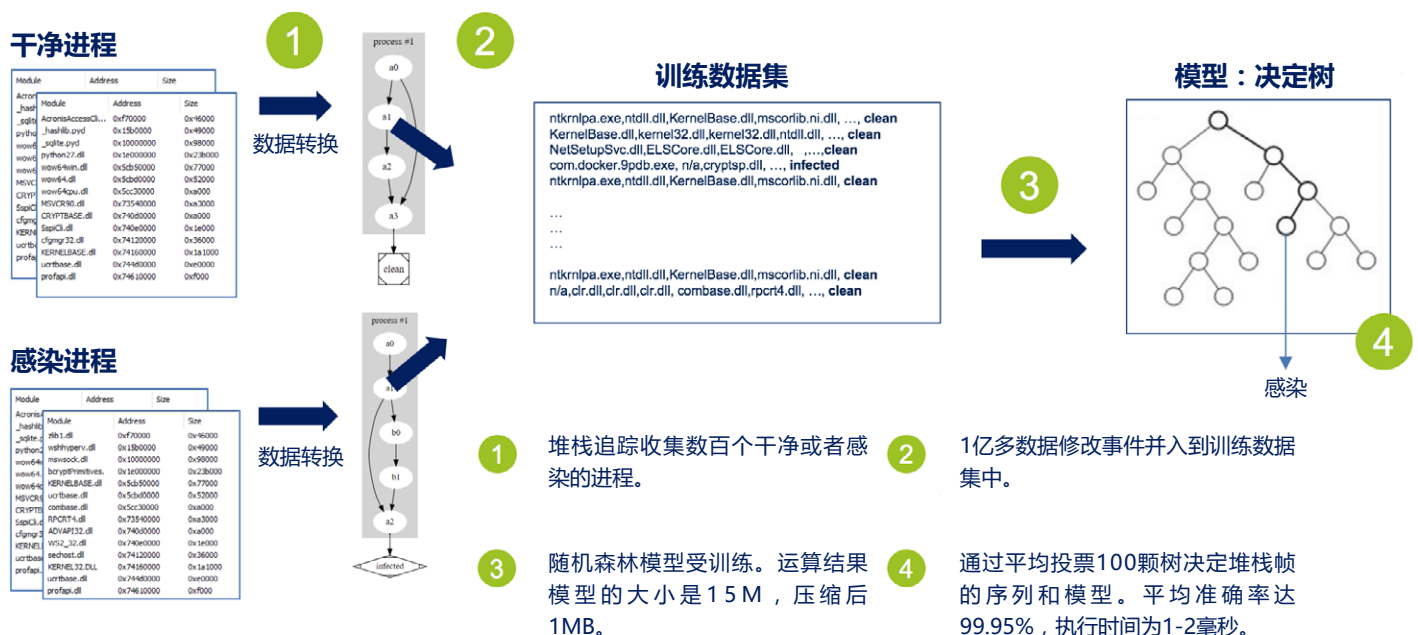
简单来说，使用基于机器学习方法的过程堆栈跟踪分析可以来检测来自勒索软件的代码注入。

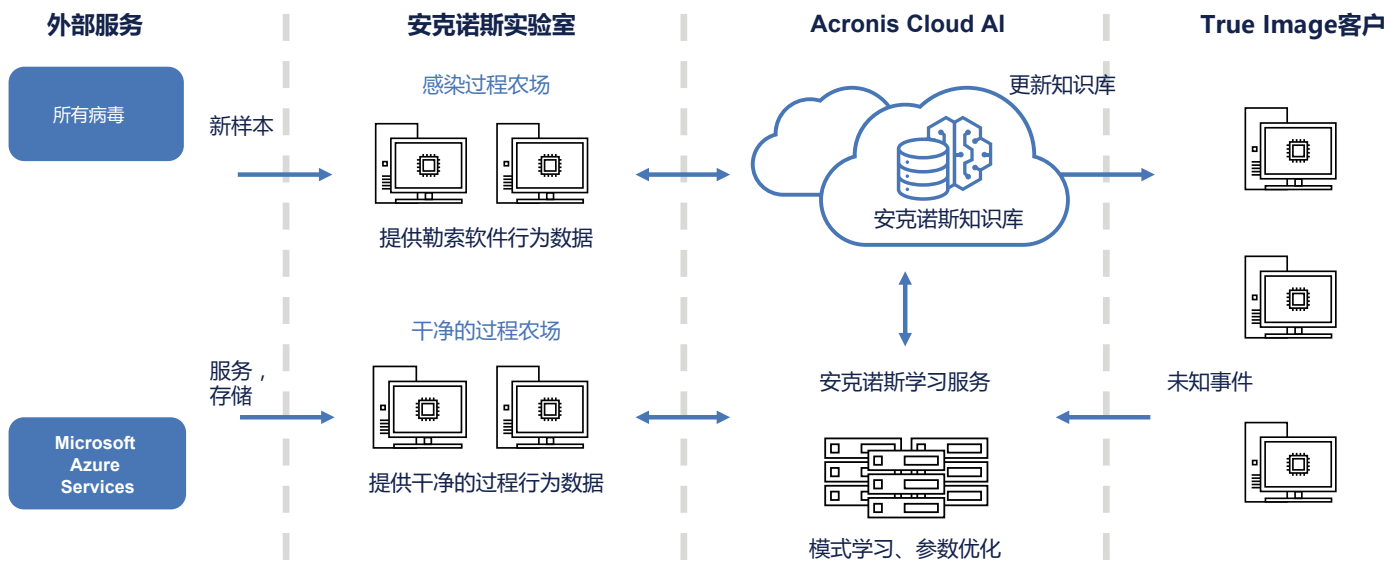
在真实场景中如何工作？

首先，安克诺斯通过采用运行着多个合法进程的干净的Windows系统来编译大量的数据。接下来，我们获得了数百万个这些过程的合法堆栈跟踪，并使用决策树学习构建了不同的“良好”行为模型。我们还从各种来源采取恶意堆栈跟踪提供了不好的样本。

基于这些数百万个学习样本，开发了模式。使用决策树学习，我们从项观察转移为项目标值总结。目的是创建一个可以基于多个输入变量预测目标变量的模型。阿克诺斯专家使用决策树，因为我们不应该在收集和发送数据时影响客户端机器的性能，并且该算法使我们能够实现这一目标。

所以，什么时候机器学习在实际的产品中被激活？正如我们已经说过的，Acronis Active Protection是基于行为启发式。在2.0版本中，我们增加了多个可以寻找合法进程的新启发式算法。如果Active Protection发现合法





进程中有异常，它就会采取一个堆栈跟踪并将其发送到我们的机器学习模块，该模块将行为与现有的干净和受感染的堆栈跟踪模型进行比较，以确定它是否是一个威胁。如果行为被确认是恶意的，用户就会得到一个警告，建议他应该阻止该类似勒索软件的进程。所以，机器学习可以主动地减少任意潜在的威胁行为。因为，它就像行为启发的第二次授权，可以让你做出最终的决定。

防御勒索软件的新高度

随着机器学习的发展，所有这些技术都将Acronis Active Protection提升到一个全新的水平，特别是在涉及零日威胁时。它创建一个合法进程的模

型，所以即使恶意分子发现新的漏洞或另外可以渗透系统的方法，机器学习将检测恶意软件的进程并停止。

搭建安克诺斯机器学习基础架构以便定期上传新的匿名用户数据进行分析。这个基础架构可以同时管理上百万个请求。由于这些持续的信息流，产品启发式的更新也会随之更快，安全性也会进一步的提高。用户是不会注意到幕后这些分争必秒的工作的，他们只要启动Acronis Active Protection既可。

安克诺斯还正在通过机器学习进行静态代码分析来进一步扩展这项技术。这将在预执行阶段完成。所以，当你下载一个文件或者副本到硬盘驱动

时，它们的代码将会立即被检测异常。如果有任何可疑，该进程可以在用户启动或某些自动脚本启动之前被阻止。

机器学习模型可用于分析脚本，并且我们已经在这个方向上取得了一定的进展。NioGuard Security Lab最近执行的测试进一步的表明哪怕是最强大的防病毒解决方案也不可能检测到基于脚本的攻击。虽然与这些防恶意解决方案对比后，安克诺斯Active Protection效果更好，但是我们的目标是让我们的防勒索技术更好。