关于自由软件与信息安全的关系探讨 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/145/2021_2022__E5_85_B3_E4_BA_8E_E8_87_AA_E7_c103_145165.htm 信息安全自由软件的好处 许多企业不愿意使用免费信息安全软件，担心使用这种工具软件会遇到麻烦。但是，正如我们在这篇应用技巧中指出的那样，免费的软件工具确实能够帮助企业安全从业人员应付日益增长的攻击的冲击。 对自由软件共同担心的问题 一些企业担心自由软件(一般是开源软件)可能会存在能够被坏蛋利用的安全漏洞。然而，自由软件通常会受到研究人员更严格的审查，因为自由软件更容易评估、免费的工具软件更容易下载，而且不需要评估某些商业软件所需要的长时间的和令人厌烦的采购过程。这就意味着自由软件中的严重安全漏洞能够比商业软件更容易在产品生命周期的早期阶段被发现。而且由于只有少数人在开发阶段能够接触到商业软件，商业软件中的一些重要的可以被利用的安全漏洞在很长一段时间都不会被人发现。这就意味着当一个真正的攻击者发现利用这个安全漏洞的方式时，事态的发展就会非常快和非常严重，就像在过去的两年里某些入侵防御系统和备份产品所解释的那样。 另一个共同担心的问题是自由软件缺少厂商的支持。这是一个重要的问题，是人们必须认真对待的问题。虽然某些自由软件工具有积极的用户群和网站，开发人员可以在这种网站交流想法和解决方案，但是，一个开发人员可以欺骗其他人，这个开发人员会转向别的事情，对这种“放弃的”软件不再提供技术支持了。信息安全从业人员应该努力使用拥有社区支持的工具。替代的方法是某些安全服务

提供商和其它厂商将为免费的产品提供技术支持服务。不过，这种服务是收费的。 另一个经常提到的担心的问题是如果免费的工具引起问题，没有任何人承担法律责任。这个观点主要集中在这个前提之下，即企业可以起诉销售给他们有安全漏洞的产品的商业软件厂商。遗憾的是，商业软件的许可证协议几乎都要免除厂商为他们的工具软件造成的任何损失承担的责任，即使是商业软件厂商的错误也是如此。因此，商业软件市场的法律声明与自由软件市场是一样有限的。 不用争论免费工具软件是不是比商业工具软件更便宜，成本肯定是要考虑的一个问题。最后，软件的价格通常都低于与这个软件有关的运行和技术支持成本，无论这个软件是自由软件和商业软件都是如此。当把这两种成本结合在一起进行比较时，自由软件和商业软件的成本是很接近的。 自由软件的好处 还不相信吗?那么，重点考虑如下两个因素： 1.自由软件工具通常好于类似的商业软件。有些自由软件甚至提供了商业软件迄今为止还没有提供的功能。 2.机构不再需要依赖那些许诺神奇地解决最新的信息安全问题的厂商宣传册，因为许多自由软件提供了先试用后购买机会。这就意味着你可以测试自由软件中指定的功能，看这个功能是否适用于你的环境和运营，然后确定在没有软件成本的情况下这个功能对你是否很重要。如果这个自由软件能够提供理想的功能，你可以继续选择依靠自由软件工具，或者购买一个提供同样功能的商业软件产品。 因此，对于有用的功能的承诺和先试用后购买的能力，以及通常被抵消的经济、技术支持和法律责任问题，你将为你的企业选择哪一个自由软件呢?我看到一些好的自由工具软件，大型、中型和小型企业使用这些软件都取

得了很好的效果。这些自由软件包括： 调查工具：Helix可启动CD光盘是一个很好的Unix、Linux和Windows取证分析工具套装软件。这个软件在一个可启动的Linux ISO镜像CD盘上提供，非常方便。Sleuth是另一种分析工具，以Windows和Unix/Linux两个版本提供。 系统分析和故障诊断工具：有许多这种类型的自由软件，其中最好的是Sysinternals。这个软件是著名的Windows权威人士Mark Russinovich和David Solomon编写的。这个分析工具套装软件肯定能够帮助人们查出Windows机器内部正在运行什么。这个套装软件中有一些著名的程序，如进程浏览器(这个程序使Windows内置的任务管理器看起来像傻子一样)、TCPvie(显示正在使用的TCP和UDP端口)、进程监视器(详细说明计算机正在运行的每一个进程)以及其它许多程序。微软在2006年7月收购了Sysinternals套装软件，显示了这个软件的有用性。微软在其网站上免费提供这个软件(这个软件至少在写这篇文章时还是免费的)。 运行增强工具：我喜欢的一些能够直接用于运行支持的自由工具软件与入侵检测有关，也就是Snort和围绕它制作的套装软件。那些考虑使用新的入侵检测系统的人们经常问我他们应该购买什么工具。我经常建议他们一开始先使用自由软件工具Snort。使用Snort能够让他们发现入侵检测系统是如何在他们的环境中使用的。然后，根据他们的经验，他们能够为商业性采购准备一份现实世界需求的文件，既可以购买一个商业版本的Snort，也可以购买一个完全不同的商业性的入侵检测系统。Snort是先试用后购买概念的一个极好的例子。 虽然并非每一个企业都要运行上述每一个工具并且让进程适应这些工具软件，但是，企业至少应该考虑这些工具

软件，不要因为它们是自由软件就不加以考虑。我建议向内部信息安全专业人员提供在适当的地方使用自由工具软件的能力。