防御攻击策略之保持领先黑客一步思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E9_98_B2_E5_BE_A1_E6_94_BB_E5_c101_644131.htm 围绕你的系统建一个高墙是不够的。黑客最终会找到一种突破这个围墙的方法，然后内部的一切东西都会受到攻击。随着当前基于Web环境的迅速变化，摆脱被动的技术并且在重要的系统中建立安全功能是非常重要的。 美国总统奥巴马在5月末发表的60天网络安全评估报告结果中把网络恐怖主义解释为“ 大规模杀伤性武器 ”。这个统计数据讲述了一个丑陋的故事：2008年网络犯罪分子从全球各地的企业中窃取了价值1万亿美元的知识产权。在过去的两年里，网络犯罪让美国人遭受了80多亿美元的损失。 黑客继续开发高级的手段，利用网络篡改、感染和窃取私营企业和公共部门的重要任务应用程序。云计算等新兴的基于Web的技术促使机构更加了解需要安全措施保护自己有价值的数据资产和知识产权。 IT行业需要软件保护技术增强防御软件功能，阻止那些窃取知识产权或者注入恶意软件等逆向工程攻击。这种逆向工程攻击能够降低重要任务应用程序要求的100%的完整性。 新的安全环境 过去，软件或者没有得到保护，或者仅仅通过模糊处理和加密等被动的技术得到保护。问题是这些被动的技术不能提供当前的威胁世界中所需要的安全。这些技术提供的静态的一次性的障碍很快就会被黑客攻破。这个受到保护的应用程序在那个单个的防御层被攻破之后没有进一步的救助措施。 目前的基于Web的环境打开了新的市场和机会，但是，它也使恶意软件和被攻破的软件更容易传播。攻击工具的开放和传播的速度很快，

从而是零日攻击非常普遍。企业越来越多地进行全球销售，越来越多地进行电子销售，使销售交易和软件面临着风险。虽然传统的安全思维导致许多人把重点放在保护网络、应用程序或者系统等周边环境的安全方面，但是，这种方法在当前的分布式计算环境中是不充分的。这个重点把资源和注意力从身边的真正任务转移到了其它方面(在应用程序中建立防御能力)，从而使这个环境中的一切东西都容易受到攻击。 简言之，企业广泛地应用过去的数据保护方法“ 保护周边环境 ”在当前的分布式计算环境中保护知识产权是不充分的。企业必须学习适应新的策略。这个策略就是把安全集成到软件和数据资产中。 软件保护的7个关键要求 成功的知识产权保护需要一些规则保护软件防御多种危险。这些规则包括多种多样的和分层次的防御措施。这些防御措施对于受保护的软件一旦在市场上应用不会受到攻击是非常重要的。另一个重要的事情是智能报警组件，能够对任何攻击一个系统的企图提供实时报警。这个保护解决方案应该包括这些要素，没有开发的开销或者严重的运行时间的不利后果。 1.耐久性。安全解决方案是由识别用户身份、确定用户权限或者验证交易等方法提供保护的。经验丰富的黑客善于识别和绕过构成单一故障点的“ 是- 否 ”决策点。这使黑客能够创建自动化的“ BORE ”(Break Once Run Everywhere，一旦突破即可到处使用)攻击工具。这种工具能够通过互联网迅速传播。 2.动态的。模糊处理和加密等代码转变是静态的过程。在这个过程中，源代码或者二进制码是以注定的方式隐藏起来的。这种保护措施还不够强大，不能满足防御黑客的大多数需求。而且，这种软件是被动的，不能防御黑客主动的攻击。 3.有弹性

。保护措施无论多么强大最终都会被攻破。因此，当应用程序更新的时候，保护方案必须也随之更新，以防御差值分析。此外，补丁必须同以前使用的补丁有很大区别，一个保证黑客不能利用以前突破的经验。任何人工的或者基于源代码的努力都是资源密集型的，因此，必须迅速发布补丁阻止收入泄露，从而导致恶性的“ 突破-补丁 ”循环周期。 4.使用方便。传统的软件保护产品没有为用户实施安全措施提供精确的控制。因此，传统的软件保护产品不允许用户建立针对自己独特的业务环境的解决方案。应用程序和环境有具体的安全要求。 5.得到证明。任何安全技术在刚刚进入市场的时候都会享受到短暂的不能被黑客攻破的安全期。然而，要充满信心地保护有价值的应用程序在其整个使用寿命周期内的安全，一种安全技术必须在现实世界中得到专家的测试和真正黑客的考验。此外，黑客的技术是在不断地发展的。如果你的解决方案提供商不能保持它的技术领先一步，你的软件很快就会成为盗版的牺牲品。 6.性能友好。一些保护解决方案在被保护的应用程序运行的时候会对这个应用程序的性能产生很大的负面影响。这些解决方案迫使开发人员在性能影响的程度和应用程序获得的安全的百分比之间进行选择。这是一种不可接受的交换条件。 7.开发友好。人工保护代码的安全是代价昂贵的和耗费时间的过程，需要使用一种反篡改应用程序编程接口的具有高超技能的资源，或者需要在源代码级工作。而且，任何源代码级的实施都是不能重复利用的，因此，实施的成本的是很高的。 在提供对网络攻击、盗版、篡改或者任何类型的危威胁的最大限度的防御措施的时候，上述关键的因素都应该考虑，以便使企业领先于黑客一步。

当下一次一个外国的间谍蠕虫进入你的敏感的应用程序的时候，你的应用程序将会发生这样的事情：你的应用程序立即通知这个异常情况，并且把丰富的证据发送到你的应用程序防火墙。你的安全信息和事件管理系统将实时得到通知，你的IT管理员将能够有效地做出反应。在强大的网络层和应用程序安全层后面，你的代码的完整性和知识产权是安全的。