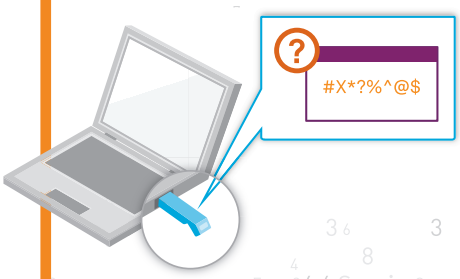
SafeNet

SENTINEL
SOFTWARE
MONETIZATION
SOLUTIONS



软件保护最佳实践——

通过 AppOnChip 加强硬件锁与应用程序之间的安全结合

功能简介

特性与优势

- 更高的安全性
- 自动化执行，易于实施
- 不占用硬件锁内存储空间
- 无需远程升级硬件锁

圣天诺外壳技术 概述

在当今计算环境下，软件发行商们所面临的一个最大问题就是如何防止其软件被非授权使用，同时又不会给那些合法购买软件的用户带来麻烦。软件盗版会阻碍公司的收益潜力，同时对付费客户造成不利影响，这些客户最终将承担非法使用软件所带来的成本。这就是为什么SafeNet会推出圣天诺外壳技术的原因——它可以让软件商快速地对软件IP实施强大的保护，从而保护市场收益和品牌声誉。

圣天诺外壳技术可以对您的应用程序实施加壳保护，通过文件加密、代码模糊处理和系统级别的反调试技术对IP进行保护，有效防止逆向工程。之后，它将为各个文件创建多个随机保护层，黑客若试图脱壳将极其复杂且费时费力，从而确保软件代码免于暴露，并保证对最终用户的服务不受影响。

AppOnChip – 最安全的软件保护途径

我们新发布的圣天诺外壳技术的一项功能“AppOnChip”，可促进圣天诺硬件锁与应用程序之间更安全的结合，从而为软件发行商提供最安全的软件保护解决方案。

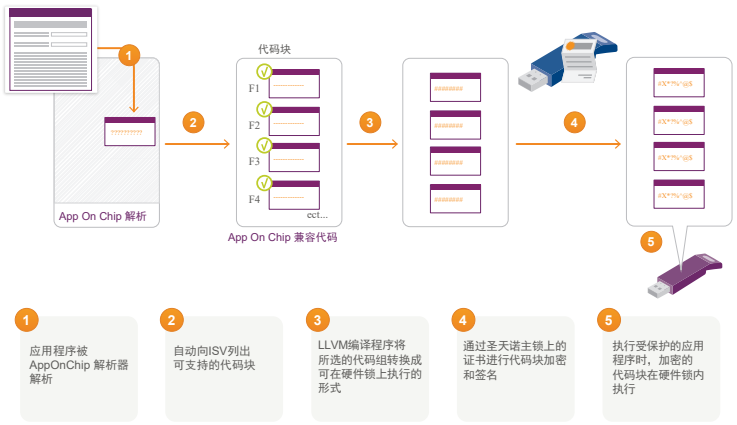
这一全自动的过程会检查应用程序，并向软件供应商列出其中含有与AppOnChip兼容代码块的功能清单。受保护的代码块经加密和签名，就可以动态加载并且在硬件锁上执行。这一附加的安全措施使其成为了市场最安全的软件许可实施方案。

特性与优势

- **更高的安全性：**
  AppOnChip要求用户插入硬件锁后才使用应用程序，有效防止非授权使用。
- **易于实施：**
  由外壳自动完成代码植入工作，无需开发商再做任何代码编制、转换。
- **不占用硬件锁内存储空间：**
  受保护的代码块不占用硬件锁的存储空间，从而确保独立软件供应商（ISV）能为许可存储提供最大的内存。
- **无需远程升级硬件锁 ：**
  有新软件版本发布时，无需进行硬件锁的远程升级。

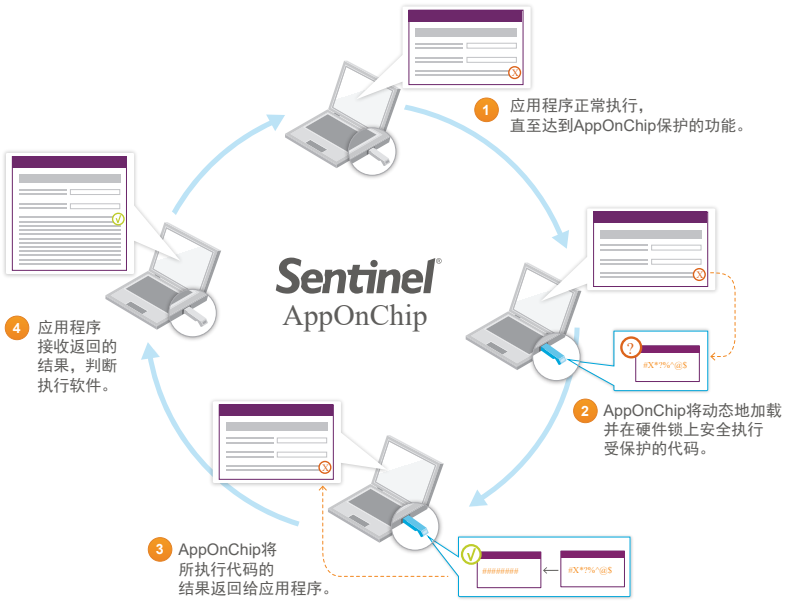
工作原理 – 保护与执行

保护： 一旦在圣天诺LDK中启用了AppOnChip功能，未受保护的应用将由AppOnChip解析，以分析所有受支持的功能。全部或若干功能中的代码块（取决于ISV的选择）将被转换成可在锁内执行的形式。这些经转换的代码块将加密和签名，以保证安全。



执行： 最终用户准备使用软件时，执行阶段就会启动。受保护的软件会正常执行，直至达到圣天诺LDK中的AppOnChip所保护的功能。应用程序中部分代码将传输给硬件锁。

AppOnChip将动态地加载并在硬件锁上安全执行受保护的代码。执行代码的结果将返回给应用程序并正常运行。



实现 AppOnChip 功能 – 只需5次点击

对于圣天诺LDK的软件商来说，启用AppOnChip软件保护功能的过程非常简单，5次点击即可。在LDK管理控制台，用户只需简单地：

1. 选择要使用此项功能的应用程序。
2. 选择 AppOnChip 标签。
3. 勾选 Enable AppOnChip 选项。
4. 选择软件命名以应用此项功能。
   启用功能后，LDK 将自动生成一组兼容命令，从中您可以进行选择。
5. 单机 Protect 可完成操作。

申请试用，请访问：
http://china.safenet-inc.com
试用申请栏目
选择圣天诺LDK产品。

成都市长今信息有限责任公司（圣天诺西南地区总代）
联系我们：13808212206（宁先生），028-85435028
网站：https://www.changinfo.com/