1.软件介绍

我们安秉网盾软件采用 C/S 架构，即客户端/服务器架构，所有软件均私有化部署。软件包括客户端----服务器---管理端，

服务器端：负责后台连接数据库，对所有的策略及日志都存入后台数据库进行保存，所有管理端及客户端都连接服务器端。

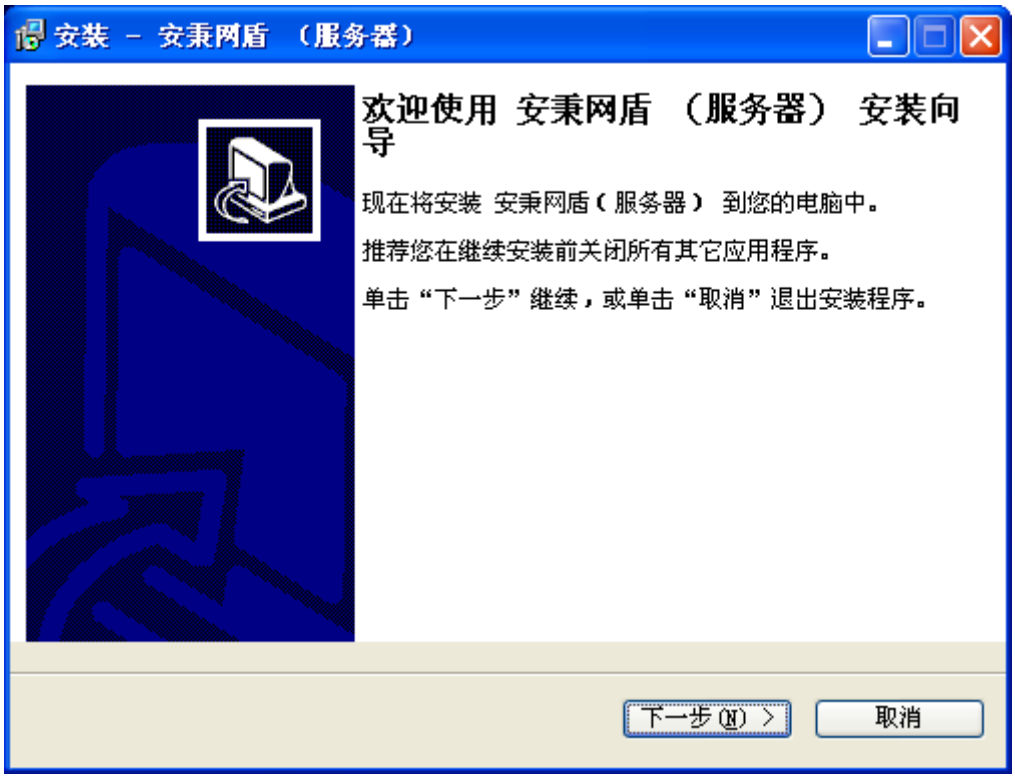
管理端:安装在管理员端负责对客户端电脑进行策略下发,及调取服务器日志进行查询。

客户端：主要是安装员工电脑，对员工电脑记录控制加密。

2.试用版安装教程

2.1 服务端的安装

管理员身份运行 SeverSetup.exe,显示安秉信息安全管理软件服务端安装欢迎界面。



选择服务端安装的目录，客户端日志默认是保存在服务端目录下，所以推荐安装在剩余空间比较大的分区上，点下一步，安装完成。

2.2 管理机安装

双击 ManageSetup.exe，显示安秉信息安全管理软件管理机安装欢迎界面。

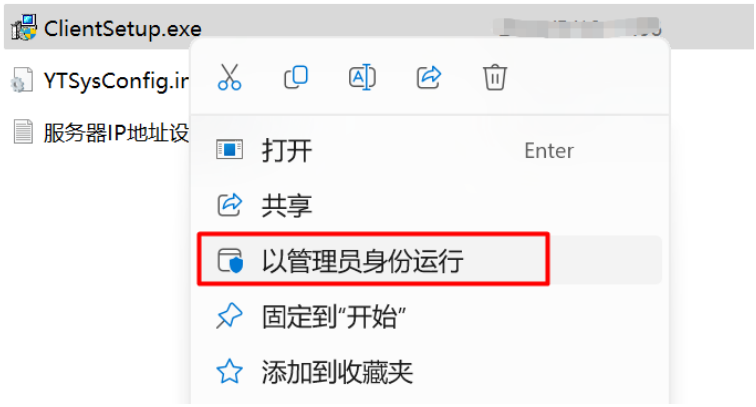
选择管理机安装的路径。

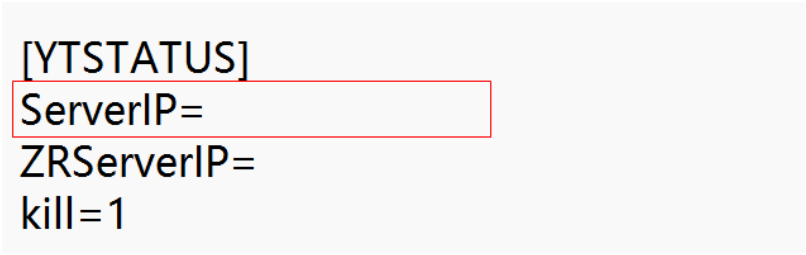
完成管理机的安装。

备注：以管理员身份打开，安装完成后打开管理端后直接点击确定，默认密码为空。

2.3 客户端软件的安装

打开客户端安装包，找到文件 YTSysConfig.ini，并打开，在“ServerIP=”后面填上服务端所在计算机的 IP 地址，然后保存。双击 ClientSetup.exe 执行安装，客户端计算机每次启动后自动连接到填写在 YTSysconfig.ini 中的服务端 IP 地址。





3.使用说明

安装完成之后所有操作均在管理端进行。

软件功能主要分两大块，终端管控和文件加密。

3.1 终端管控

它的设计理念是什么呢，它也可以防泄密，它主要是做这个事前过滤和这个事后审计的功能。

也就是说，我们可以把我们想到的泄密途径给封禁，比如说我们的 U 盘可能去随意地拷贝文件，包括邮件，网盘，这些通常是我们可以想到的，但是互联网应用太多了，我们是想不到的，用这种封禁的方法来说，它的安全系数不是那么高，但是，它有一个日志审计功能，这个泄密的事情已经发生了，我们就可以通过日志审计来定位是谁造成的泄密。

这里列举几个系统常用的功能：远程协助、文件分发，屏幕日志（每隔一段时间截取一下屏幕）、USB 管控、抓取聊天日志，远程卸载软件等等。

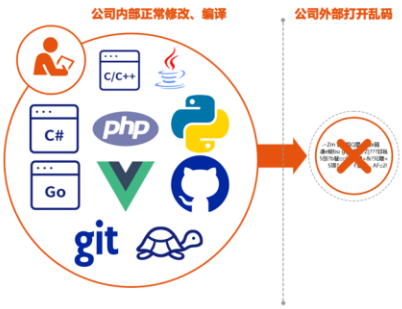
3.2 文件加密

驱动层透明加密，三种模式：透明模式、老板模式、半透明模式，主要包括加密策略、加密参数、解密审批、文件密级等等、具体可在安装试用版本后体现。

4.方案介绍

4.1 源代码防泄密

源代码防泄密-员工本地文件进行加密



对各种开发语言源代码文件进行加密：

源码文件透明加密

只对源代码文件进行透明加密，加密后的文件只能在公司电脑打开修改，正常编译，编译后文件自动不加密，并且无任何多余操作。

支持开发语言

支持所有软件开发语言C、C++、C#、Java、Vue、Php、Python等。

支持开发工具

支持Eclipse、MyEclipse、Visual C++、SourceInsight、Keil、delphi、Visual Studio、 Android Studio、MPLAB IDE、 IntelliJ IDEA 、VsCode等。

源代码防泄密--SVN\GIT服务器防泄密

与 SVN\GIT等版本库无缝兼容

版本服务器无需部署

安秉方案只用所有需要加密的机器部署加密客户端，而 svn 服务器不用部署客户端。

服务器密文保存

svn/git客户端当源代码文件更新上传至服务器保存为加密状态。

客户端不影响比对

将版本对比工具注册为合法进程，因为全程是密文状态，所有对比工具要可以读取密文源码文件,丝毫不影响客户端文件比对。

特殊场景：

场景一：源代码需本地调试设断点改BUG

需求描述	员工电脑源代码加密后，需本地调试设置断点找bug，会不会有影响。

安秉源代码防泄密方案只对源代码文件加密，编译后的文件不加密，
不影响任何代码调试以及代码的运行速率。

场景二：版本服务器密文保存如何备份明文?

需求描述	公司内部有对版本服务器拉取定时备份的电脑，可以不可以设置备份的代码为明文。

安秉源代码防泄密方案支持git，svn脚本自动拉取备份为明文。

场景三：版本服务器密文，Jenkins自动发布可以用吗?

需求描述	当版本服务器密文时，Jenkins服务器拉取的也是密文，可以支持Jenkins正常使用吗?

安秉源代码防泄密方案有linux版本，可以完美与Jenkins对接，支持jenkins的正常编译，发布。

场景四：版本服务器密文，影响客户端版本比对合并吗？

需求描述	当版本服务器密文时，客户端的版本比对合并有影响吗？

安秉源代码防泄密方案，可以支持版本管理服务器密文状态下，不影响员工电脑的版本比对合并。

场景五：需要带源代码去客户现场电脑调试怎么办？

需求描述	需要带源代码去客户电脑上调试，又不想解密源代码，调试完客户电脑上源代码自动失效？

安秉信息源码防泄密方案是当员工外出时，让用户使用外发key，
带Ukey以及加密的源代码去客户现场即可，把Ukey插上可以正常调试，Ukey拔掉加密源代码打不开。

场景六：版本服务器密文，外协人员怎么用？

需求描述	当版本服务器密文时，外协人员如何使用源代码进行开发？

外协人员的使用场景特点是：

使用个人电脑。公司加密的代码可以用，用后还是加密的，个人代码不加密。开发结束公司加密的代码自动失效

安秉方案：

安秉外协客户端，支持加密源代码可以正常的看，未加密文件不加密。

场景七：出差离线笔记本电脑防丢失?

需求描述	对于出差的笔记本电脑，与服务器断开连接，能否继续加密并且防止丢失?

装上加密默认笔记本上的源代码只能在笔记本本地使用，但为了防止离线笔记本丢失造成的损失，设置离线时间，超过时长上面源代码文件自动打不开，需要公司服务器重新认证授权后，方可使用。

具体功能可在使用过程中与我们安秉信息的商务人员交流：微信