

A large red banner with a white outline on the left side. It contains a large, semi-transparent 'TOPSEC' logo in the background. Overlaid on the banner is the text '天融信终端威胁防御系统用户手册' in white, bold, sans-serif characters.

天融信终端
威胁防御系统
用户手册



北京市海淀区上地东路1号华控大厦 100085

电话：+8610-82776666

传真：+8610-82776677

服务热线：+8610-8008105119

<http://www.topsec.com.cn>

版权声明

本手册中的所有内容及格式的版权属于北京天融信公司（以下简称天融信）所有，未经天融信许可，任何人不得仿制、拷贝、翻译或任意引用。

版权所有 不得翻印 ©2017 天融信公司

商标声明

本手册中所谈及的产品名称仅做识别之用。手册中涉及的其他公司的注册商标或是版权属各商标注册人所有，恕不逐一列明。

TOPSEC®天融信公司

信息反馈

<http://www.topsec.com.cn>

目录

| | | |
|----------|-------------------|----------|
| 1 | 前言 | 1 |
| 1.1 | 文档目的 | 1 |
| 1.2 | 文档基本内容 | 1 |
| 1.3 | 约定 | 1 |
| 1.4 | 技术服务体系 | 1 |
| 2 | 系统简介 | 3 |
| 2.1 | 首页 | 4 |
| 2.2 | 系统设置 | 4 |
| 2.2.1 | 软件设置 | 4 |
| 2.2.2 | 安全日志 | 5 |
| 2.2.3 | 信任/隔离区 | 6 |
| 2.2.4 | 检查更新 | 6 |
| 2.3 | 病毒查杀 | 7 |
| 2.4 | 防护中心 | 16 |
| 2.4.1 | 病毒防御 | 16 |
| 2.4.2 | 系统防御 | 23 |
| 2.4.3 | 网络防御 | 27 |
| 2.5 | 扩展工具 | 30 |
| 2.6 | 托盘程序 | 47 |

1 前言

本用户手册主要介绍了天融信终端威胁防御系统的使用和管理。通过阅读本文档，用户可以了解系统的基本组成，并根据实际应用环境配置使用系统。

本章内容主要包括：

- 文档目的
- 读者对象
- 文档基本内容
- 约定
- 相关文档
- 技术服务体系

1.1 文档目的

通过阅读本文档，用户能够正确地配置使用系统。

1.2 文档基本内容

本用户手册包含以下章节：

- “前言”，介绍了本手册目的、读者对象、各章节的基本内容、文档约定和技术支持信息。
- “系统简介”，介绍了系统的功能、组成等，以及客户端程序的具体功能和操作。

1.3 约定

本文档遵循以下约定：

图形界面操作的描述采用以下约定：




“”表示按钮。

点击（选择）一个菜单项采用如下约定：

点击（选择）**高级管理 > 特殊对象 > 用户**；

文档中出现的注意、说明、示例等，是关于用户在使用本产品过程中需要特别注意的部分，请用户在明确可能的操作结果后，再进行相关配置。

这些标志的意义如下：

| 格式 | 说明 |
|---|---|
|  | “说明”图标，对操作内容的描述进行必要的补充和说明。 |
|  | “注意”图标，提醒操作中应注意的事项，不当的操作可能会导致数据丢失或设备损坏。 |
|  | “示例”图标，对相关描述进行举例说明。 |

1.4 技术服务体系

天融信公司对于自身所有安全产品提供远程产品咨询服务，广大用户和合作伙伴可以通过多种方式获取在线文档、疑难解答等全方位的技术支持。

公司主页

<http://www.topsec.com.cn/>

天融信全国安全服务热线

800-810-5119

400-610-5119

2 系统简介

天融信终端威胁防御系统是一款专为用户量身定制的内网终端安全管理软件，能够提供漏洞管理、系统加固、病毒查杀、软件管理、流量监控、资产管理等功能，并有多种扩展功能可选，极大地提升网络安全，适用于操作系统为 XP、WIN7、WIN8、WIN8.1、WIN10 等的消费者。

客户端程序主要针对杀、防、管控这几方面进行功能设计，主要有病毒查杀、防护中心、扩展工具三部分功能。

天融信终端威胁防御系统基于目前 PC 用户的真实应用环境和安全威胁而设计，除了拥有强大的自主知识产权的反病毒引擎等核心底层技术之外，更考虑到目前互联网环境下，用户所面临的各种威胁和困境，有效地帮助用户解决病毒、木马、流氓软件、恶意网站、黑客侵害等安全问题。

天融信终端威胁防御系统的客户端程序具有以下特点：

- 天融信智能防御引擎，是用户终端的强大保障。

天融信终端威胁防御系统反病毒引擎是天融信多年经验累积的结晶，是国内少有自主研发的新一代反病毒引擎。

- 天融信动态防御体系，提供全面的防护。

深度整合反病毒+主动防御+智能拦截三大防御模块，为用户提供一个纯净、无绑定的软件环境，有效抵御流行病毒以及流氓软件对电脑的伤害。

- 自律的软件系统，只关注用户的安全。

软件免费不简单，不会向用户推送任何干扰信息，不做桌面推广，不窃取隐私数据，一心做好用户正义的安全管家。

2.1 首页

安装完成后，天融信终端威胁防御系统的客户端会自动启用，如下图所示。



- 界面左侧显示客户端的三个主要功能，点击具体的功能名称会进入该功能的下级菜单；
- 界面的右上角显示客户端的标题按钮，“≡”表示客户端的主菜单，“-”表示最小化窗口，“×”表示关闭窗口并最小化到托盘。

2.2 系统设置

点击客户端主界面右上角的“≡”，弹出菜单，可对天融信终端威胁防御系统的客户端程序进行基本设置。

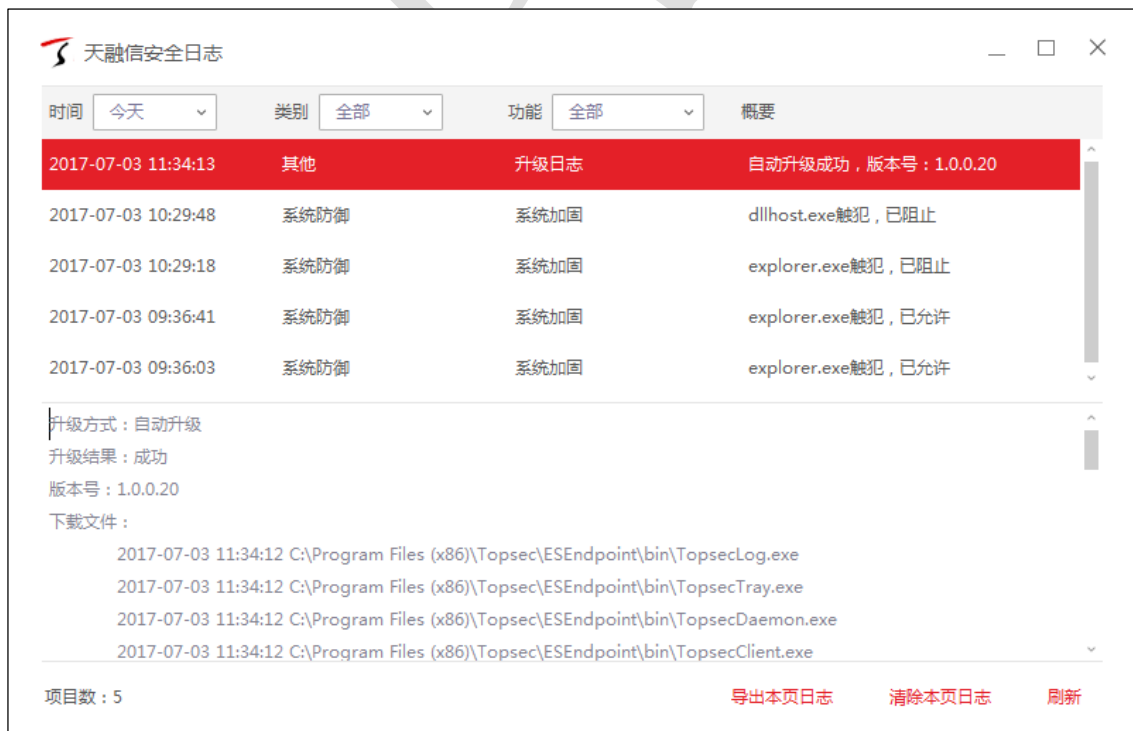
2.2.1 软件设置

选择 **软件设置 > 常规 > 基础配置**，弹出“设置”窗口，如下图所示。可对快捷操作、更新是否提示进行配置。



2.2.2 安全日志

选择 安全日志，弹出“天融信安全日志”窗口，如下图所示。



界面上方显示客户端日志信息，可通过选择时间、类别、功能对日志进行筛选；界面下方显示日志的详细信息。

用户可点击“导出本页日志”按钮将当前页的日志信息以 txt 文件的形式保存到本地；点击“清除本页日志”按钮将当前页的日志信息全部清除。

2.2.3 信任/隔离区

选择 **信任/隔离区**，弹出“天融信安全”窗口，如下图所示。关于信任/隔离区的操作具体请参见 [管理隔离区](#)和[管理信任区](#)。



2.2.4 检查更新

选择 **检查更新**，弹出“天融信安全-在线升级”窗口，如下图所示。



2.3 病毒查杀

病毒查杀是自安全杀毒软件诞生之初就一直存在的基础功能，用户可以利用病毒查杀主动扫描在电脑中是否存在病毒、木马威胁等。进行查杀前需要先选择查杀模式，客户端将通过自主研发的反病毒引擎高效扫描目标文件，及时发现病毒、木马，并帮助用户有效处理清除相关威胁。

具体操作步骤如下：

- 1) 选择 **病毒查杀**，如下图所示。



2) 选择扫描方式。

用户在进行病毒查杀之前，需要选择具体的检查方式。天融信终端威胁防御系统的客户端提供三种查杀方式。

- 快速查杀：病毒文件通常会感染电脑系统敏感位置，“快速查杀”针对这些敏感位置进行快速的查杀，用时较少。推荐日常使用。
- 全盘查杀：对计算机所有磁盘位置进行查杀，用时较长。推荐定期使用。
- 自定义查杀：用户可以指定磁盘中的任意位置进行病毒扫描，完全自主操作，有针对性地进行扫描查杀。遇到部分文件不确定安全时使用。

3) 发现病毒。

用户选择查杀方式后，会开始对具体的文件进行扫描。在扫描的过程中，发现威胁，界面会提示，通过点击“查看详情”可查看威胁的位置以及建议处理方式，如下图所示。



3) 选择查杀速度。

天融信终端威胁防御系统的客户端可选择以下两种查杀速度：

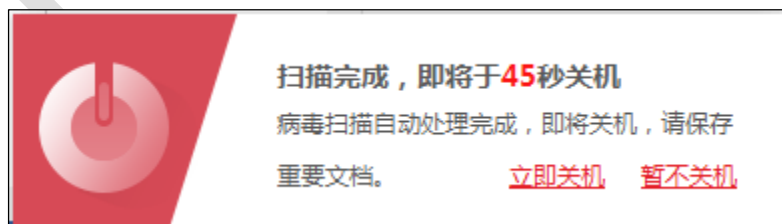
- 常规：占用较少的系统资源。
- 高速：占用较多的系统资源，提高扫描速度。

用户可在扫描过程中，点击“常规”或“高速”，对扫描速度进行切换。其中，若用户选择的查杀模式为“快速查杀”或“自定义查杀”时，默认的查杀速度为“高速”；若用户选择的查杀模式为“全盘查杀”，默认的查杀速度为“常规”。



4) 设置查杀完成后自动关机。

当用户利用休息或者离开电脑的时候，对电脑进行查毒操作，查杀完成后自动关机功能就可以很好帮助用户进行查毒和自动关机的操作。勾选此功能，在查杀完成后，客户端将自动处理扫描到的威胁，并将会提示用户 45 秒后自动关机，如下图所示。



用户可选择立即关机，也可选择撤销关机命令，暂不关机。

5) 处理威胁。

当扫描到威胁后，天融信终端威胁防御系统提供病毒处理方式的选择，如下图所示。

- 立即处理：对所选择的危险项，进行隔离处理。建议用户操作此项。

- 忽略：对扫描出的风险项目不做处理。

将威胁文件处理完毕后，系统提示扫描完成，如下图所示。显示扫描概况，并将上一步处理的威胁添加至隔离区。



6) 管理隔离区。

隔离区相当于操作系统的回收站，客户端会将扫描处理过的病毒威胁文件，经过加密后备份至隔离区。用户有特殊需要时，可以主动从隔离区中重新找回被处理过的威胁文件。

用户可以通过以下方式可以对隔离区的文件进行管理：

- (a) 点击客户端主界面右上角的“≡”，选择“信任/隔离区”，如下图所示。



(b) 在弹出的对话框中选择文件，在弹出的对话框中选中文件，可进行以下操作：

- 删除：将选中的文件从电脑上彻底删除，文件不可恢复；
- 恢复：将选中的文件恢复到其原始位置，同时从隔离区删除文件。相当于剪切。

- 提取：保留隔离区的文件，同时将文件提取至指定目录。相当于复制。

7) 管理信任区。

信任区相当于用户电脑文件的暂存库，用户确认安全的文件，或者不希望杀毒软件查杀的文件，可以添加至信任区，此列表中的文件或文件夹不会被病毒查杀、文件实时监控、恶意行为监控、U 盘保护、下载保护功能扫描。信任区支持增加文件夹或者文件，同时支持取消信任。

用户可以通过以下方式可以对信任区的文件进行管理：

- (a) 点击客户端主界面右上角的“☰”，选择“信任/隔离区”，如下图所示。





(b) 管理信任文件。

在弹出的对话框中选中文件，可进行以下操作：

- 清除无效规则：清除无效的规则。
- 删除：不再信任该文件/目录。
- 添加文件：将需要信任的文件添加至信任区。
- 添加目录：将需要信任的目录添加至信任区。

8) 设置病毒查杀功能的其他配置。

点击客户端主界面右上角的“☰”，弹出菜单，选择 **软件设置 > 病毒查杀 > 常规查杀**，弹出“设置”窗口，如下图所示。可对全盘查杀设置、系统修复设置、发现病毒时的操作、清除病毒时的操作进行配置。



选择 **软件设置 > 病毒查杀 > 修复白名单**，弹出“设置”窗口，如下图所示。查看修复项目扫描结果中的白名单项目。



2.4 防护中心

防护中心显示当前客户端下发的安全策略的状态。防护中心设置了多达 11 类安全防护内容，当发现威胁动作触发策略开启的防护项目时，客户端将精准拦截威胁，帮助用户计算机避免受到侵害。

选择 **防护中心**，如下图所示。



2.4.1 病毒防御

病毒防御功能是针对电脑病毒设计的病毒实时防护系统。



- 文件实时监控

1) 当天融信终端威胁防御系统的文件实时监控功能开启时，默认情况下会在程序运行时，先实时扫描即将运行的程序是否安全，并拦截病毒程序执行，从而实时保护用户电脑不受病毒侵害，同时不影响电脑日常使用。

当有威胁触发了文件实时监控时，客户端程序将根据策略配置提示用户或自动处理威胁，如下图所示。



2) 设置文件实时监控功能的其他配置。

点击“文件实时监控”或点击客户端主界面右上角的“☰”，弹出菜单，选择 **软件设置 > 病毒防御 > 文件实时监控**，弹出“设置”窗口，如下图所示。可对扫描时机、排除设置、发现病毒时的操作、清除病毒时的操作进行配置。



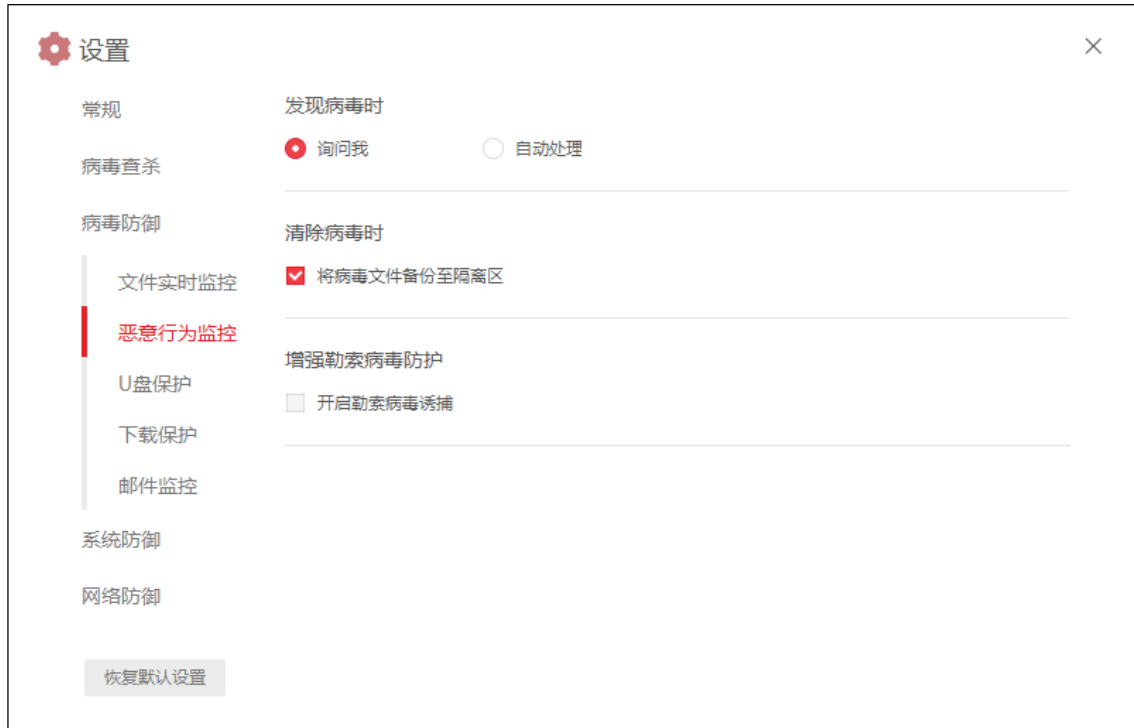
- 恶意行为监控

1) 恶意行为监控功能不单纯依赖病毒库校验程序是否安全, 而是通过监控程序运行过程中是否存在恶意操作来判断程序是否安全, 从而可以作为传统特征查杀的补充, 极大提升电脑反病毒能力。

当有威胁触发了恶意行为监控功能时, 客户端程序将根据策略配置提示用户或自动处理威胁。

2) 设置恶意行为监控功能的其他配置。

点击“恶意行为监控”或点击客户端主界面右上角的“☰”, 弹出菜单, 选择 **软件设置 > 病毒防御 > 恶意行为监控**, 弹出“设置”窗口, 如下图所示。可对发现病毒时的操作、清除病毒时的操作、勒索病毒防护进行配置。



- U 盘保护

为了避免病毒通过 U 盘进入用户的电脑，天融信终端威胁防御系统的客户端程序开发了 U 盘保护功能，在 U 盘接入电脑第一时间，对 U 盘进行快速扫描，及时发现风险。同时移动存储设备也会自动纳入文件实时监控等其他监控功能保护范围，全方位保护用户电脑的安全。

当有威胁触发了 U 盘保护时，客户端程序将根据策略配置提示用户或自动处理威胁。

2) 设置 U 盘保护功能的其他配置。

点击“U 盘保护”或点击客户端主界面右上角的“☰”，弹出菜单，选择 **软件设置 > 病毒防御 > U 盘保护**，弹出“设置”窗口，如下图所示。可对通用设置、U 盘接入电脑时的操作、发现病毒时的操作、清除病毒时的操作、U 盘中的压缩包扫描设置进行配置。



- 下载保护

1) 天融信终端威胁防御系统的客户端程序将在用户使用浏览器、下载工具、IM 进行文件下载时对文件进行病毒扫描，在病毒文件进入电脑的时候就将其查杀。

当有威胁触发了下载保护时，客户端程序将根据策略配置提示用户或自动处理威胁。

2) 设置下载保护功能的其他配置。

点击“下载保护”或点击客户端主界面右上角的“☰”，弹出菜单，选择 **软件设置 > 病毒防御 > 下载保护**，弹出“设置”窗口，如下图所示。可对排除设置、发现病毒时的操作、清除病毒时的操作、下载的压缩包扫描设置进行配置。

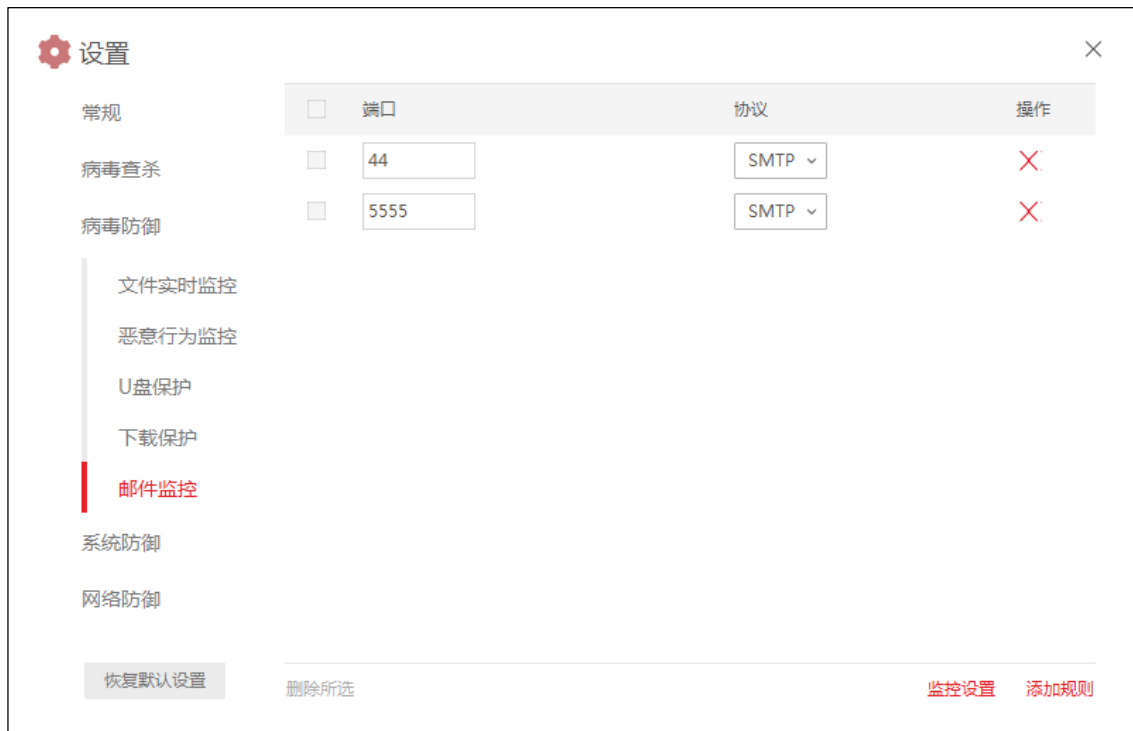


- 邮件监控

1) 用户在接收/发送邮件的时候，天融信终端威胁防御系统的客户端程序抢先截获用户接收/发送的邮件进行查杀毒。

2) 设置邮件监控功能的其他配置。

点击“邮件监控”或点击客户端主界面右上角的“☰”，弹出菜单，选择 **软件设置 > 病毒防御 > 邮件监控**，弹出“设置”窗口，如下图所示。点击界面下方的“监控设置”可对清除病毒时的操作、附件的压缩包扫描设置进行配置；点击“添加规则”可添加扫描邮件的端口规则。



2.4.2 系统防御

此模块功能主要防护计算机系统不被恶意程序侵害。



- 系统加固

1) 在当前安全形式下，除了单纯的病毒木马威胁以外，用户的电脑还面临着各类流氓程序的威胁，甚至连常规软件也可能为了利益，存在部分侵犯用户的权益的侵权行为。为了帮助用户处理这类不适合直接查杀的程序，又阻止这些程序对用户的电脑系统的恶意篡改等行为，天融信安全专家依据多年的积累，为用户提供了一套全方位的加固方案，保护用户的电脑系统各个安全关键点。

当有威胁动作触犯系统加固功能时，客户端程序会弹窗提示，用户可以根据需要选择对这个动作的处理方式。



2) 设置系统加固功能的其他配置。

点击“系统加固”或点击客户端主界面右上角的“☰”，弹出菜单，选择 **软件设置 > 系统防御 > 系统加固**，弹出“设置”窗口，如下图所示。激活“系统项目”项目页签，可对系统的具体项目选择执行方式；激活“自动处理”页签，可手动对系统中的其他程序创建处理方式。点击界面下方的“添加规则”可添加防护规则。



- 软件安装拦截

1) 天融信终端威胁防御系统的客户端程序在用户安装软件的时候帮助用户判断软件是否是推广软件，并将选择权交给用户，用户可以自由选择是否需要继续安装，从而减少用户在不知情的情况下安装不需要的软件。

当发现有推广软件正在安装时，客户端程序会弹窗提示，用户可以根据需要选择是否安装此软件。

阻止：阻止本次安装行为。

允许安装：允许本次安装行为。

勾选“记住本次操作，下次自动处理”后将记住这次的操作行为，下次再遇到此软件的安装，将会自动执行本次的选择，不再弹窗提示。

2) 设置软件安装拦截功能的其他配置。

点击“软件安装拦截”或点击客户端主界面右上角的“☰”，弹出菜单，选择 **软件设置 > 系统防御 > 软件安装拦截**，弹出“设置”窗口，如下图所示。显示选择自动处理的软件列表。



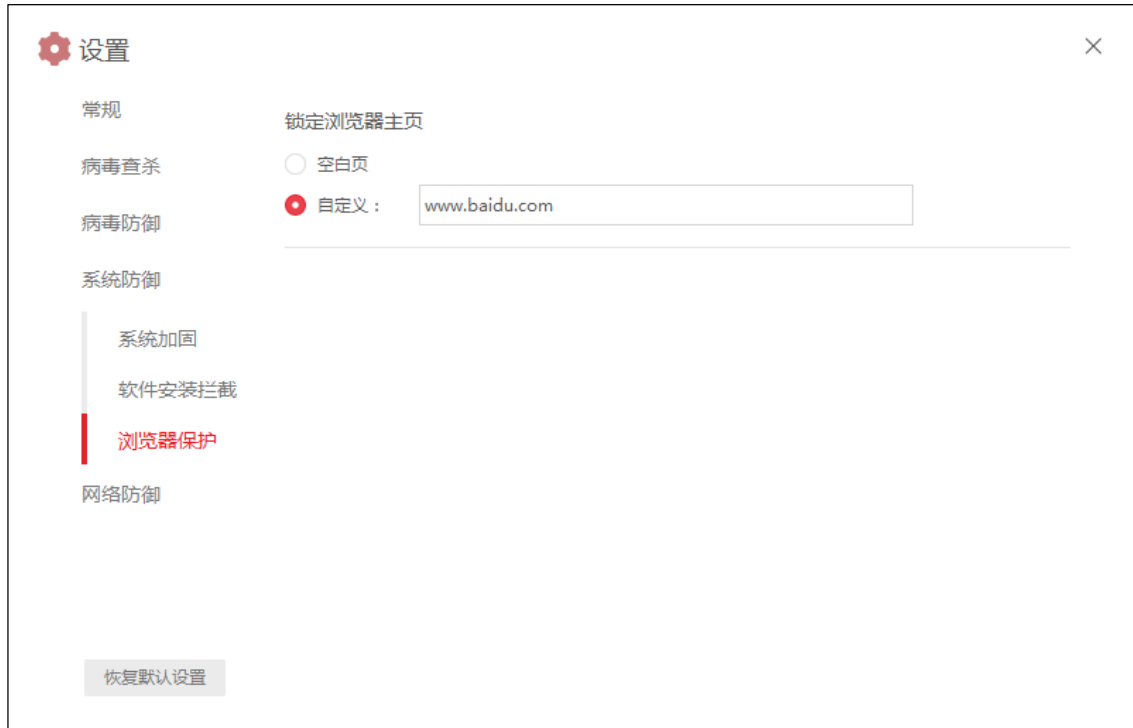
- 浏览器保护

1) 由于控制用户的浏览器访问某些商业网站，可以获取广告分成收入，导致目前无论是常规软件或恶意程序，都有可能通过篡改、锁定、劫持等各种侵犯用户的权益的方式控制用户的浏览器主页，从而获得收入。这些侵权行为导致用户的主页可能被不同软件反复篡改，影响用户的体验。

天融信终端威胁防御系统的客户端程序提供浏览器保护，可以锁定浏览器首页和默认搜索，防止用户的浏览器设置被恶意篡改。

2) 设置浏览器保护功能的其他配置。

点击“浏览器保护”或点击客户端主界面右上角的“☰”，弹出菜单，选择 **软件设置 > 系统防御 > 浏览器保护**，弹出“设置”窗口，如下图所示。可对浏览器的主页进行设置。



2.4.3 网络防御

此模块功能主要防护计算机在使用过程中，对网络危险行为的防御。



- 黑客入侵拦截

1) 现在用户的电脑除了受到病毒的危害,还可能会受到黑客的侵犯,黑客入侵拦截将检测用户通过网络传输的数据包中是否包含敏感入侵信息,从而一定程度上避免用户的电脑遭到黑客入侵。

当有发现有黑客入侵时,天融信终端威胁防御系统的客户端程序将阻止入侵,并通过托盘 tips 通知用户。

2) 设置黑客入侵拦截功能的其他配置。

点击“黑客入侵拦截”或点击客户端主界面右上角的“☰”,弹出菜单,选择 **软件设置 > 网络防御 > 黑客入侵拦截**,弹出“设置”窗口,如下图所示。可对黑客入侵后的操作进行设置。



● 对外攻击检测

1) 黑客通过各种方式入侵了用户的电脑后,可能利用用户的电脑向其他终端目标发起对外攻击,从而达到破坏其他终端或致使其他终端网络瘫痪的目的。天融信终端威胁防御检测系统客户端提供对外攻击检测,防止用户的电脑被黑客入侵后的对外对外攻击行为,避免用户的利益受到损害。

当有发现有对外攻击时,天融信终端威胁防御系统的客户端程序将记录攻击行为,并通过托盘 tips 通知用户。

2) 设置对外攻击检测功能的其他配置。

点击“对外攻击检测”或点击客户端主界面右上角的“☰”，弹出菜单，选择 **软件设置 > 网络防御 > 对外攻击检测**，弹出“设置”窗口，如下图所示。可对检测到对外攻击发生后的操作进行设置。



● 恶意网站拦截

1) 互联网高度发达的今天，不法分子通过在网站内恶意种植木马、病毒等恶意程序，发布虚假、欺骗信息，仿冒正规网站等手段，伪装诱导用户等方式，使用户的计算机感染病毒，造成用户的损失。恶意网站拦截功能，可以在用户访问网站时自动分辨即将访问的网站是否存在恶意风险，如果存在风险将拦截访问行为，并告知用户，避免侵害。

当用户在浏览网页的时候，访问到有恶意风险的网站，天融信终端威胁防御系统的客户端程序将拦截网站并提示用户。

2) 设置恶意网站拦截功能的其他配置。

点击“恶意网站拦截”或点击客户端主界面右上角的“☰”，弹出菜单，选择 **软件设置 > 网络防御 > 恶意网站拦截**，弹出“设置”窗口，如下图所示。可对恶意网站的检测类型进行设置。



2.5 扩展工具

天融信终端威胁防御系统的客户端程序为用户提供了方便操作管理电脑的各类小工具。

选择 **扩展工具**，如下图所示。



- 右键管理

天融信终端威胁防御系统的客户端程序为用户提供了针对右键菜单管理的小工具，方便用户设置自己真正需要的右键菜单。

选择 **扩展工具 > 右键管理**，弹出“天融信安全-右键管理”窗口，如下图所示。可对在文件、桌面、IE 图标右键弹出菜单的具体选项进行配置。其中，文件右键菜单是指在文件图标上右键出现的菜单；桌面右键菜单是指在桌面空白处上右键出现的菜单；IE 右键菜单是指在 IE 浏览器上右键出现的菜单。



- 垃圾清理

天融信终端威胁防御系统的客户端程序为用户提供了垃圾清理工具，清理不必要的缓存文件，节省电脑使用空间。

1) 选择 **扩展工具 > 垃圾清理**，弹出“天融信安全-垃圾清理”窗口，如下图所示。



2) 勾选界面下方的垃圾类型图标，可选择是否对该类型的垃圾进行检测。

3) 设置完成后，点击“扫描垃圾”按钮，弹出“扫描中”窗口，如下图所示。



4) 扫描完成后, 如下图所示。点击“一键清理”按钮, 可对检查出的垃圾删除清理。用户也可点击具体的垃圾文件, 自行选择想要清理的文件后, 再进行清理。点击“重新扫描”, 重新进行垃圾扫描。



5) 清理完成后, 如下图所示, 点击“完成”按钮, 完成此次清理。



6) 点击界面右上角的“▽”，弹出菜单，选择 **清理设置**，弹出“清理设置”窗口，如下图所示。勾选“定时扫描垃圾”后，可对垃圾大小阈值、自动扫描周期进行设置。



7) 点击界面右上角的“▽”，弹出菜单，选择 **创建快捷方式**，垃圾清理功能将会在桌面创建快捷方式，如下图所示。




- 文件粉碎

在用户使用电脑过程中，有部分不需要的文件，但是通过常规删除，无法删掉；或者有部分文件需要彻底删除，防止被技术手段恢复，这时需要对文件进行彻底粉碎，天融信终端威胁防御系统的客户端程序的文件粉碎功能为用户提供稳定安全的粉碎方式。

1) 选择 **扩展工具 > 文件粉碎**，弹出“天融信安全-文件粉碎”窗口，如下图所示。



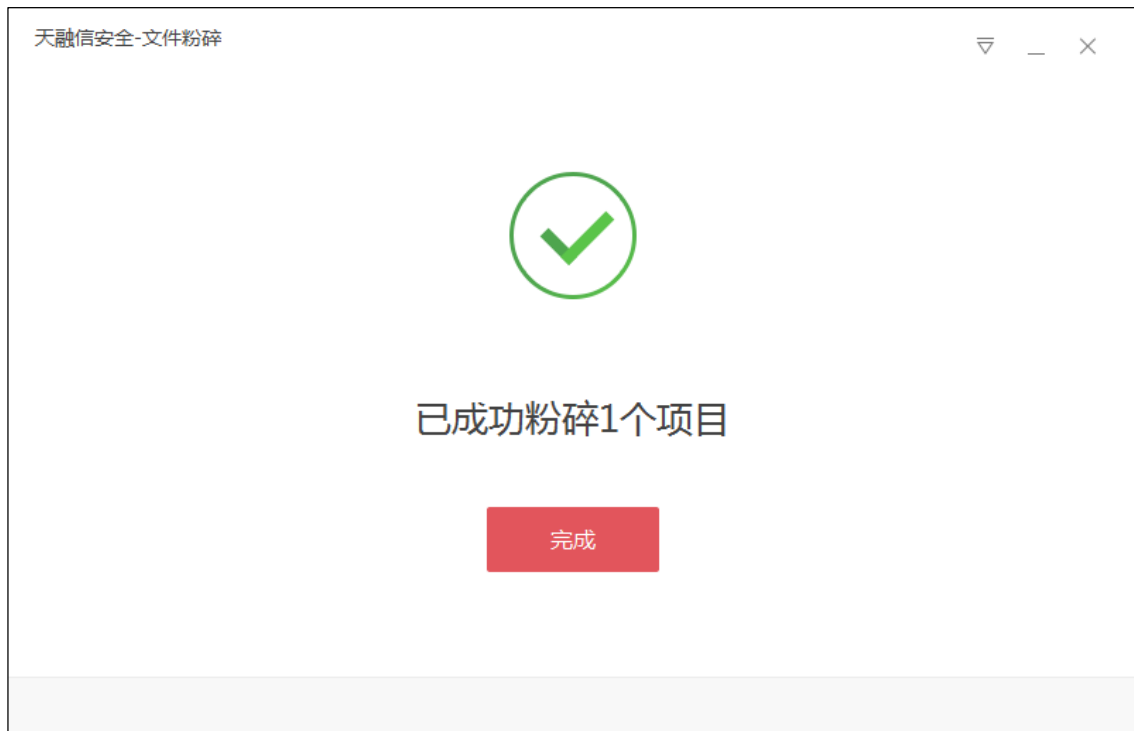
2) 点击“添加文件”按钮或点击“”按钮添加文件或文件夹，也可直接拖拽目标文件/文件夹到窗口。

3) 添加完成后，点击“开始粉碎”按钮。用户可勾选“彻底粉碎”，彻底粉碎文件，组织文件恢复，保护隐私安全，但粉碎时间较长。

4) 弹出“提示窗口”，如下图所示，点击“确定”按钮。



5) 粉碎完成后，如下图所示，点击“完成”按钮，完成此次粉碎。



6) 点击界面右上角的“▽”，弹出菜单，选择 **软件设置**，弹出“文件粉碎-设置”窗口，如下图所示。可将“文件粉碎”功能加入右键菜单。



6) 点击界面右上角的“▽”，弹出菜单，选择 **粉碎历史**，弹出“文件粉碎-粉碎历史”窗口，如下图所示。查看粉碎的历史文件，也可选择以后粉碎文件时不生成历史记录。



- 弹窗拦截

如今电脑软件商业化十分严重，很多软件在使用的过程中，会通过弹窗的形式，来推送咨询、广告甚至是一些其他软件，这些行为严重影响到用户对电脑的正常使用。天融信终端威胁防御系统的客户端程序的弹窗拦截功能，用户可以采用多种拦截形式，自主、有效的拦截弹窗。

1) 选择 **扩展工具 > 弹窗拦截**，弹出“天融信安全-弹窗拦截”窗口，如下图所示。



点击“取消拦截”，可以关闭弹窗拦截功能。

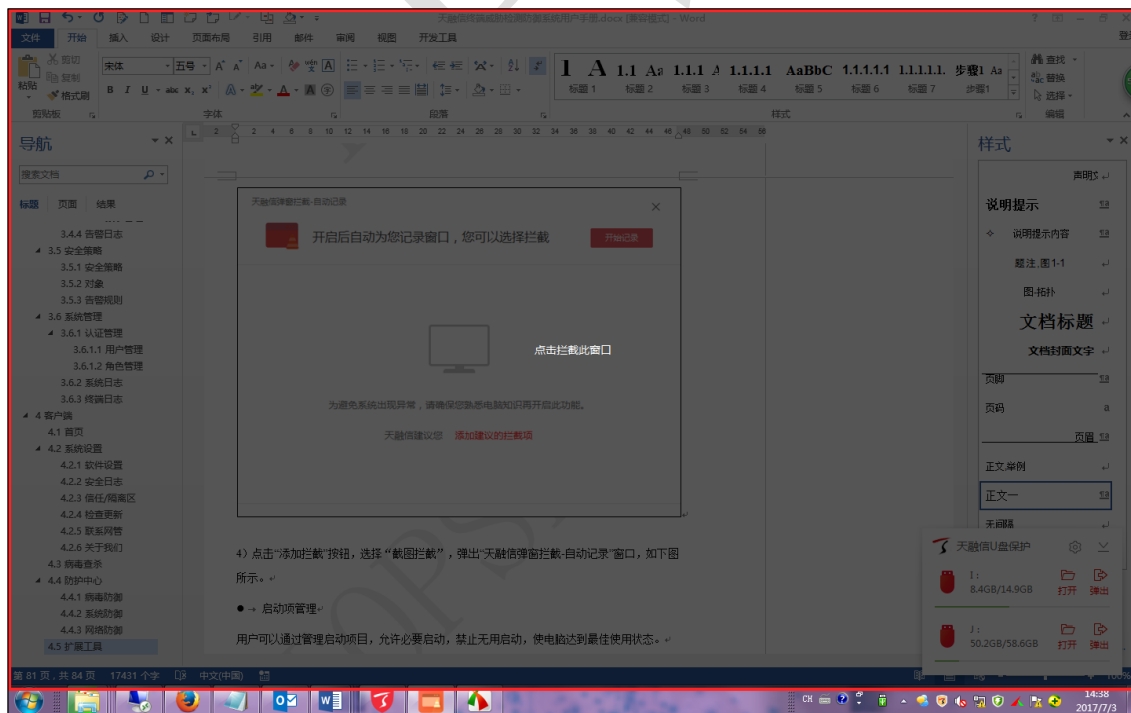
2) 点击“添加拦截”按钮，选择“建议拦截”，弹出“天融信弹窗拦截-建议拦截”窗口，如下图所示。界面显示当前由客户端程序检测出的当前主机中建议拦截的程序，用户可自行选择想要拦截的弹窗程序，点击右侧“开启拦截”；也可点击“一键拦截”按钮，对所有建议拦截的弹窗进行拦截。



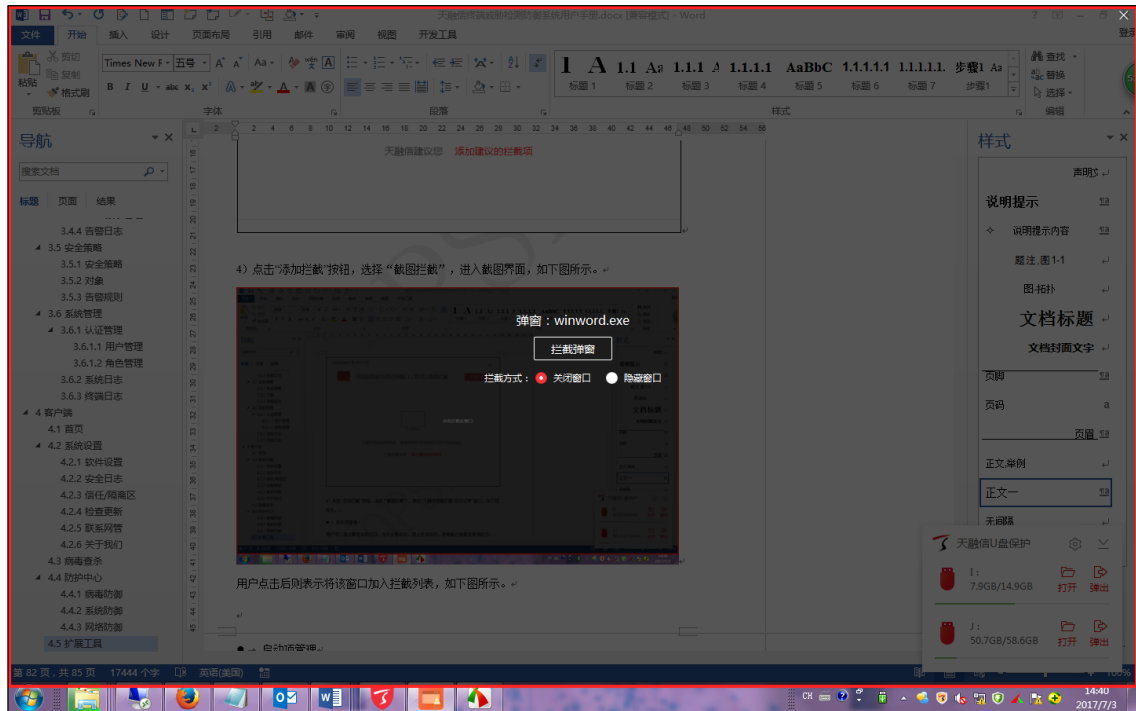
3) 点击“添加拦截”按钮，选择“窗口记录”，弹出“天融信弹窗拦截-自动记录”窗口，如下图所示。点击“开始记录”按钮，客户端程序会自动记录窗口，用户可选择后，进行拦截。



4) 点击“添加拦截”按钮，选择“截图拦截”，进入截图界面，如下图所示。



用户点击后则表示将该窗口加入拦截列表，如下图所示。选择拦截方式后，点击“拦截弹窗”按钮，拦截该窗口。



5) 点击界面右上角的“▽”，弹出菜单，选择**软件设置**，弹出“拦截设置”窗口，如下图所示。可对通用设置、快捷键设置进行设置。



- 启动项管理

用户可以通过管理启动项目，允许必要启动，禁止无用启动，使电脑达到最佳使用状态。

1) 选择 **扩展工具 > 启动项管理**，弹出“天融信安全-启动优化”窗口，如下图所示。显示当前主机中的开机启动项目。



2) 激活“启动项”页签，显示开机启动的应用程序，客户端程序给出了对各个启动项目的建议，用户可点击右侧的下拉列表选择“禁止启动”该项目；用户也可将鼠标移动到某条启动项目，点击右侧出现的“⚙️”，选择对该启动项忽略、从启动项列表中删除或者打开程序所在目录。

3) 激活“服务项”页签，显示开机启动的服务，其他操作同“启动项”页签中的操作。

4) 激活“任务计划”页签，显示开机启动的任务计划，其他操作同“启动项”页签中的操作。

5) 点击“查看详情”按钮，弹出“天融信启动优化-一键优化”窗口，界面显示当前由客户端程序检测出的当前主机中建议优化的启动项目，用户可自行选择想要优化的启动项目，点击右侧“立即优化”；也可点击“一键优化”按钮，对所有建议优化的启动程序进行优化。



6) 点击界面右上角的“⚙️”，弹出“启动优化-设置”窗口，如下图所示。可设置是否自动扫描可优化项目。



- 网络流量

当一条网络中，很多程序都在利用网络下载上传数据，在真正需要网速的时候，会造成访问缓慢的情况，通过网络流量管理可以更好地控制上网的程序，查看使用网络情况，防止网络阻塞。

1) 选择 **扩展工具 > 网络流量**，弹出“天融信安全-网络安全”窗口，如下图所示。

| 程序名称 | 下载速度 | 限制下载 | 上传速度 | 限制上传 | 连接数 |
|---------------------|------|------|------|------|-----|
| 360rp.exe | 0B/s | 未限制 | 0B/s | 未限制 | 5 |
| 360tray.exe | 0B/s | 未限制 | 0B/s | 未限制 | 2 |
| emagent.exe | 0B/s | 未限制 | 0B/s | 未限制 | 3 |
| FeiQ.1060559168.exe | 0B/s | 未限制 | 0B/s | 未限制 | 3 |
| firefox.exe | 0B/s | 未限制 | 0B/s | 未限制 | 5 |
| java.exe | 0B/s | 未限制 | 0B/s | 未限制 | 5 |
| mysqld.exe | 0B/s | 未限制 | 0B/s | 未限制 | 2 |
| NewCenterSom.exe | 0B/s | 未限制 | 0B/s | 未限制 | 1 |
| oracle.exe | 0B/s | 未限制 | 0B/s | 未限制 | 3 |

2) 激活“实时流量”页签，界面显示应用程序、系统程序、限速程序和所有程序的流量信息，包括下载速度、上传速度，连接数等。

用户可点击某个程序的连接数，弹出“网络连接详情”窗口，如下图所示。界面显示该程序的连接信息。用户可点击“文件属性”，查看并修改该程序的属性；也可点击“定位文件”，打开程序所在目录。



用户可点击某个程序右侧的“⚙️”，选择对该程序的上传下载速度进行限制或者结束该进程。

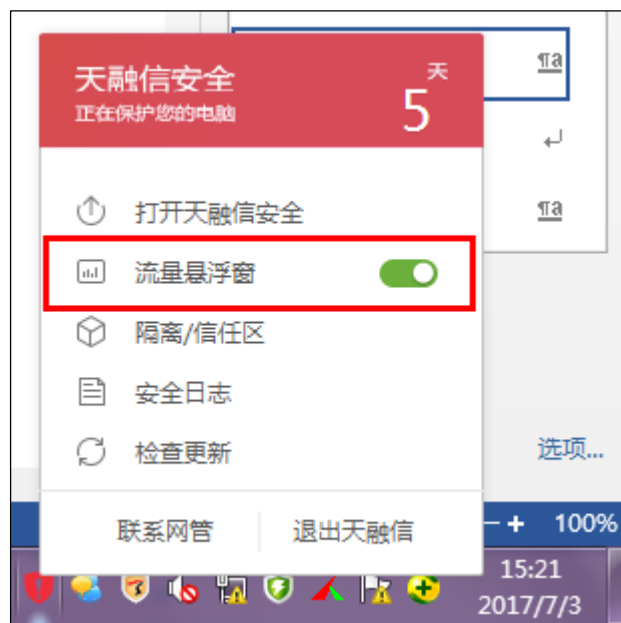
3) 激活“历史流量”页签，界面显示当天、7天、30天和使用至今的流量信息，包括首次联网时间、下载流量、上传流量等，如下图所示。



用户可点击某个程序右侧的“⚙️”，选择对该程序的上传下载速度进行限制。也可点击“流量清零”，将网络流量的历史记录清除。

4) 天融信终端威胁防御系统的客户端程序为用户提供了便捷查看流量的方式，通过流量悬浮窗可以查看当前流量使用状态，用户可以通过以下两种方式开启流量悬浮窗（该悬浮窗默认不显示）：

(a) 通过鼠标右键点击托盘图标，在弹出菜单中可以打开，如下图所示。



(b) 点击客户端主界面右上角的“☰”，弹出菜单，选择 **软件设置 > 常规 > 基础配置**，弹出“设置”窗口，如下图所示。



2.6 托盘程序

天融信终端威胁防御系统的客户端程序启动后需要在电脑后台实时保护用户的电脑，此过程客户端程序进程在托盘系统中运行，这样可以节省电脑资源，用户也可以通过系统托盘区域，在需要的时候方便快捷的找到天融信终端威胁防御系统的客户端程序。

右键单击系统托盘图标，显示右键快捷菜单。



- 打开天融信安全：启动天融信终端威胁防御系统的客户端程序的主界面。
- 流量悬浮窗：开启流量悬浮窗，悬浮窗支持贴边隐藏。
- 隔离/信任区：快速开启隔离/信任区。
- 安全日志：快速打开安全日志。
- 检查更新：启动升级程序，检查软件版本情况。
- 联系网管：联系天融信的工作人员。
- 退出天融信：停止天融信终端威胁防御系统的客户端程序对电脑的保护。

声明

1. 本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信不另行通知。
2. 本手册中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，此可能产生的差异为正常现象，产品功能和性能请以产品说明书为准。
3. 本手册中没有任何关于其他同类产品的对比或比较，天融信也不对其他同类产品表达意见，如引起相关纠纷应属于自行推测或误会，天融信对此没有任何立场。
4. 本手册中提到的信息为正常公开的信息，若因本手册或其所提到的任何信息引起了他人直接或间接的资料流失、利益损失，天融信及其员工不承担任何责任。