瑞星安全云终端 3.0
使用手册

北京瑞星网安技术股份有限公司

2017 年 02 月

用户许可协议

重要提示：

在您使用北京瑞星网安技术股份有限公司（以下称“瑞星公司”或“瑞星”）产品（包括但不限于瑞星网络版杀毒软件、瑞星企业终端安全管理系统软件、瑞星虚拟化系统安全软件、瑞星企业移动管理系统软件及其他企业用产品，以下称“本产品”，具体参见本协议“4 定义 4.1”）之前，请务必仔细阅读本用户许可协议（以下称“本协议”或“EULA”），任何与本协议有关的产品软件、电子文档等都应依照本协议的条款而授权您使用，同时本协议亦适用于任何有关本产品软件的后期发行和升级。您在安装本产品前应仔细阅读本协议的各项条款，尤其需注意免除或者限制瑞星公司责任的免责条款及对用户的权利限制。您保证，在使用本产品之前，已理解并接受本协议。

1. 范围

本协议是您（自然人、法人或其他组织）与本产品的权利人瑞星公司之间就本产品及相关服务事项达成的最终的、完整的且排他的协议。您的雇员或其他代理商、经销商或承建商安装或使用本产品和（或）服务时，亦必须接受本协议后方可使用本产品和（或）服务。试用用户（见本协议“您定义 4.4 自）安装使用本产品，供评估本产品使用，亦须遵守本协议。

2. 协议生效

2.1 您在瑞星官网（www.rising.com.cn）下载安装使用本产品或者注册本产品信息，即表示您同意接受本协议各项条款的约束，本协议生效。

2.2 您通过安装光盘（CD/ DVD）、复制备份软件或者访问等其它方式使用本产品，即表示您同意接受本协议各项条款的约束，本协议生效。

2.3 您在使用试用版或其他版本的产品和（或）服务，即表示您同意接受本协议各项条款的约束，本协议生效。

3. 协议拒绝

如果您不能完全遵守本 EULA 的条件和条款，瑞星公司可以随时终止本 EULA。在此情况下，您必须销毁本产品的所有拷贝及其所有组成部分。

4. 使用的术语和定义

4.1 “本产品”是指：

以瑞星公司软件为主要内容的磁盘、光盘、或者是其它介质的所有信息、软件、材料、资料等，包括但不限于瑞星公司或者第三方电脑信息或者软件；

瑞星公司许可您使用的瑞星公司软件的升级程序、修改版本、更新和添加的产品功能以及瑞星公司发布的使用本软件所需相关工具（如果有）；

附带瑞星公司软件的硬件设备，包括但不限于主机、闪存卡、连接器等；

相关的说明性书面材料、产品包装和电子文档；

4.2 “组件服务”：是指购买本产品后会获得相应的产品软件注册服务、软件升级服务、电话支持服务，邮件服务、专家门诊服务、以及硬件上门调试、更换维修等。

4.3 “产品升级”：是指本产品软件开发维护的后续版本，包含 bug 修复或功能上的新增与改进，通常指小数点右侧的版本号的变化。

4.4 “试用用户”：是指没有购买本产品和（或）服务使用许可证的用户，其使用本产品和（或）服务的目的仅作为对产品的试用或评估，一般情况下试用期（评估期）为三十（30）个自然日。

4.5 “付费用户”：是指购买本产品和（或）服务使用许可证的用户。

4.6 “计算机”：是指个人计算机、工作站、手持个人电脑、手机或移动电话或其他数字电子设备。

4.7 “虚拟机”：指通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。

4.8 “使用”：指依据文档存取、安装、下载、复制或以其它方式对本产品做功能性使用。

4.9 “用途”指您使用本产品的限制和范围。本产品系瑞星企业级产品，您使用产品的用途限于您及您的员工在企业办公场所内从事日常经营使用，除非经瑞星公司另有书面授权，您不应将该产品授权企业或员工个人在购买企业办公场所以外使用，亦或不得授权非购买企业或其员工使用。

5. 试用用户使用许可

如果您为试用用户，在试用本产品和（或）服务（“一般是评估期起始之日起三十（30）自然日在非生产环境中使用的软件或服务进行评估或测试的目的”）评估期间，您有权获得电话支持服务、邮件服务、远程专家门诊服务，以及通过访问瑞星官网的形式获得产品更新、内容安全更新和服务更新，当试用期（评估期）结束后，瑞星公司有权终止该产品和（或）服务的使用，同时您必须删除或销毁所有瑞星公司的软

件和文档的副本、并归还相关软件载体或硬件设备。

6. 有偿使用许可

作为付费用户，在使用本产品和（或）服务期间，您有如下的权利和义务：

6.1 产品：在您遵守本协议条款和支付相应的许可费的条件下，您可以在授权许可范围内安装和使用该产品。

6.2 组件服务：在您遵守本协议条款和支付相应的许可费的条件下，可以获得相应的服务支持，如产品软件注册服务、软件升级服务、电话支持服务、邮件服务、专家门诊服务、硬件上门调试、更换维修以及根据与瑞星公司签订的其他协议依法享有的其他服务。

6.3 文档：您可以复制合理数量的副本以供内部培训和使用。但是，所有此类副本必须包含原始文档里瑞星公司的标识信息。

6.4 费用支付：您可以通过现金、支票或者银行转账方式向瑞星公司支付费用。具体的费用支付将由您与瑞星公司另行书面约定。

7. 知识产权

7.1 本产品及瑞星公司授权您制作的任何相关副本均为瑞星公司的产品，其知识产权归瑞星公司所有。本产品的结构、组织和代码均为瑞星公司的有价值的商业秘密和保密信息。本产品受到《中华人民共和国著作权法》、《中华人民共和国著作权法实施条例》及其他相关中国法律法规、规章制度的保护，同时受到国际著作权条约和其他国际知识产权条约的保护。您不得在本协议许可的范围之外复制瑞星公司的软件，否则将构成对瑞星公司知识产权的侵犯。同时，根据本协议您不得对瑞星公司软件进行逆向工程、反编译、反汇编或以其它方式尝试发现瑞星公司软件的源代码，瑞星公司书面授权许可您进行合法反编译的除外。瑞星公司提供的或您获得的有关瑞星公司的任何信息只能由您为本协议许可的目的而使用，不得透露给任何第三方或用于创建任何与瑞星公司软件风格相似的软件，在未经瑞星公司书面授权的情况下不得用作其他商业用途。

7.2 本协议对您使用本产品软件的授权并不意味着瑞星公司对其享有的知识产权做出任何部分或全部的转让。

8. 产品软件使用许可

在遵守本协议的条款的前提下，瑞星公司即授予您非独占性的软件使用许可，允许您依据本协议规定的用途使用本产品软件（包括硬件产品附带的瑞星公司软件）。

8.1 授权使用范围

对单个产品软件，瑞星公司只授权您在一台计算机上使用，但在下列情况下您可以将本产品软件用于多用户环境或网络系统上：

(a) 瑞星公司书面授权许可您用于多用户环境或网络系统上；

(b) 您使用软件的每一节点及终端都已向瑞星公司购买了使用许可。

8.2 复制、分发和传播

您应当按本协议的规定使用或复制瑞星公司产品软件。您必须保证根据本协议授权的每一份复制、分发和传播都必须是完整和真实的，包括所有有关本产品软件的相关软件、电子文档、版权和商标等方面的信息，亦包括本协议。出于备份或档案管理的目的您可以制作一个软件副本，但不可在任何未购买本产品软件使用许可的计算机和/或未经瑞星公司书面授权许可的其他计算机上安装或使用该副本。除经瑞星公司书面授权外，您不得以任何方式将该副本转让或许可给他人使用。

8.3 转让

除非本协议明示许可，您不得以任何方式，包括但不限于租用、出租、再许可或复制等方式，在其它用户的电脑上使用本产品软件的所有或任何部分。但是您可以在同时满足以下全部条件的前提下将本产品软件的使用权转让给其他人：

(a) 您同时将本协议、本产品软件和与本产品软件捆绑或预安装在一起的所有其它软件或硬件（包括所有副本、更新版和先前版本）一并转让给他人；

(b) 您不对任何副本及与本产品软件有关的任何材料、资料、软件等进行留存，包括但不限于您在电脑上存储的备份和副本；

(c) 受让方接受本协议的条款和条件以及您合法购买本产品时接受的任何其他条款和条件。

8.4 本软件引用、利用、使用的相关第三方成果，技术等关联许可，请查看软件许可目录内容并接受。

9. 产品软件注册

为了获得相应服务、产品更新和技术支持，您必须通过网络或者是纸质注册卡的方式向瑞星公司注册并激活软件和服务。注册使我们能够与您联系，以便确保只有有效授权实体接受相应的服务。注册需要一个实体的名称和地址，联系人姓名和联系方式，一个有效的产品序列号，一个有效的电子邮件地址和其他法律通知。注册失败并不会减少您使用本产品的权利，但瑞星公司无法提供接入服务、产品更新或技术支

持。

10. 维护/更新的有偿使用许可证

作为有偿使用本产品和（或）服务的用户，您有权要求产品更新和基于网络、电话或者电子邮件技术支持。从瑞星公司或授权经销商购买的软件许可和（或）服务（统称为“维护”）在您购买之日起的一个月内，您必须通过网络（即通过在瑞星官网在线注册）或者纸质注册卡的方式向瑞星公司注册激活软件和（或）服务以便获取您的用户 ID（即使用许可证），从您获取到用户 ID 之日将开始计算首次服务期限（即“定期保养”，具体期限以购买合同为准）。当定期保养维护期限届满后，若要保留该维护权利，您必须从您的供应商（或瑞星公司）购买续保维护服务。否则，您没有维护权利，即不能再享有后续更新软件版本的使用权和相应的服务，瑞星公司有权拒绝提供软件修改后的版本与服务，包括后续版本包含新特性或功能等。若在定期保养维护期限届满后，您中断一段时间之后要求恢复维护的，瑞星公司有权收取除了维修期限届满后逾期维护费外的其它复费；但是若维护中断时间超过一（1）年，您无权要求恢复维护。

11. 同意电子通信

瑞星将通过产品注册中指定联系人的电子邮件地址通知，或将在其网站上张贴通信，包括更新，升级，特殊优惠和定价或其他类似的信息，客户调查反馈（“通讯”）或其他请求。

12. 数据收集

为了给您提供服务和相关的技术支持已经提高软件和（或）服务的功能，除了产品注册信息外，瑞星公司必须处理和存储关于您网络及设备的相关信息（包括但不限于互联网协议(IP)地址、媒体访问控制(MAC)地址和操作系统版本）。为了改善产品的功能，瑞星公司会定期上传关于产品使用的安装软件，检测到的恶意软件或潜在的不必要的文件的电子信息，您同意瑞星公司进行如下的行为：

（1）为了提高产品的功能和服务的质量，使用已经上传的数据；

（2）与安全合作伙伴共享已经被确认为恶意或者是有害的数据。

13. 备份

在使用任何产品和服务期间，您应当在不同的介质上定期对您的数据和计算机系统进行备份。您理解并知晓在软件、服务或者更新发生错误时，任何一次备份的失败都可能会导致您数据和计算机系统的丢失。由于只有您能执行备份计划以确保在软件、服务或者更新发生错误时，能最大限度的恢复数据和计算机系统，故对您备份的失败，瑞星公司不承担任何责任。

14. 审计

在您正常的工作时间和合理的通知的条件下，瑞星公司有权审核您使用产品和服务的情况。如果审核发现了未经授权的计算机、虚拟机或用户，在接到瑞星公司通知的三十（30）个自然日以内，您应当就未经授权的计算机、虚拟机或用户支付产品许可费。若为未经授权的计算机、虚拟机或用户支付的费用超过审计之前已付费用的 5%，瑞星公司有权要求您赔偿审计所花费的成本和费用。

15. 承诺与责任免除

15.1 瑞星公司向愿遵照本许可协议的条款使用本产品而购买的用户保证，在您购买本产品之日起三十（30）个自然日内，如果本产品自身异常而导致的产品不能正常使用，瑞星公司在经过检测核实后负责更换，但若该异常是因用户错误使用、人为损坏、非法使用、突发事故导致或介质丢失的除外。如依据上述规定要求瑞星公司负责进行更换的，必须在购得本产品后三十（30）个产品日内自费将本产品连同购买凭据退回购买地点，否则视本产品为合格产品。

15.2 瑞星公司保证本产品在正常使用条件下实质上符合其产品说明书中规定的性能要求。

15.3 瑞星公司不对本产品特殊应用目的的商业性和适用性承担保证责任。

15.4 瑞星公司不保证本产品没有错误，或者能够不间断的操作。瑞星公司不保证本产品在任何情况下在任何计算机上均有效。

15.5 您知悉并理解由于防病毒产品软件的特殊性，该软件不可能对于现在或将来的任何病毒均有效。您同意瑞星公司不就因该软件未能防御病毒而发生的损失（包括已通知瑞星公司有可能发生该等损失的情形），包括但不限于营业利润损失、业务中断、业务信息、文档、数据丢失或其他后果性、附带性、间接性经济损失承担赔偿责任，除非该等损失是瑞星公司的故意或欺诈行为造成的。您同意，无论本协议中是否有其他规定，无论在任何情况或根据任何规定，在本协议或与本协议相关的协议履行期间，因瑞星公司造成您或您的相关方发生任何实际损失、或有损失的，瑞星公司对您或您的相关方的最大损失赔偿责任（无论是由于任何违约、侵权或瑞星公司的任何作为或不作为或其他）不应超过 1000 元人民币。

15.6 瑞星公司不对本产品中包含的第三方软件产品的适用性及功能性负责，您在使用本软件产品中遇到的因第三方软件产品引起的故障、损失由该软件产品相关权利人负责，瑞星公司将提供必要的、合理范围内的协助。

16. 用户的声明与保证

16.1 您承诺您具有签署并履行本协议的全部资格、权利、权力、许可及授权；

16.2 您承诺不以任何不合法的方式、为任何不合法的目的、或以任何与本协议不一致的方式使用本产

品和相关服务；

16.3 您承诺您通过本软件实施的所有行为均遵守中国（为本协议之目的，不包含香港特别行政区、澳门特别行政区和台湾地区）法律、法规和相关规定以及各种社会公共利益或公共道德。如有违反导致任何争议、纠纷等不利后果的发生，您将以自己的名义独立承担所有相应的法律责任。

16.4 您同意，因您违反本协议或经在此提及而纳入本协议的其他文件，或因您违反了相关法律法规、国家政策等或侵害了第三方的合法权利，而使第三方对瑞星公司或瑞星公司的职员、代理人提出索赔要求（包括但不限于司法费用和其他专业人士的费用），您必须对瑞星公司及瑞星公司的职员、代理人由此遭受的全部损失承担赔偿责任。

16.5 您承诺，未经瑞星公司书面许可，因签署、履行本协议而获知的有关瑞星公司任何形式的非公开信息（包括但不限于技术秘密、商业计划、商业秘密等）均不得向任何第三方（但为履行本协议而必须知晓的员工除外）公开，否则瑞星公司有权选择以下任意一种方式要求您承担责任；本协议终止的，不影响本款的效力。

（1）要求您支付许可费的 30%作为违约金；

（2）要求您赔偿瑞星公司全部的损失。

17. 协议终止

如果您未能遵守本协议的任何规定，瑞星公司有权随时终止授予您的对本产品的使用许可。终止许可后，您应在瑞星公司通知后，按照瑞星公司的要求处理本产品。

18. 其他

18.1 本协议所定的任何的部分或全部无效者，不影响其他条款的效力。

18.2 本协议的解释、效力及纠纷的解决均适用于中国（为本协议之目的，不包含香港特别行政区、澳门特别行政区和台湾地区），并不考虑法律冲突。

18.3 有关本协议的任何争议应由您与瑞星公司秉承善意友好协商解决。若协商不成，您与瑞星公司均同意将纠纷或争议提交北京仲裁委员会依据当时有效的仲裁规则在北京仲裁解决。仲裁裁决是终局的，对双方均有法律约束力。除非仲裁裁决另有规定，仲裁费用应由仲裁败诉方承担。

18.4 如果您对本协议有任何疑问或者希望从瑞星公司获得任何信息，请按下列地址和方式与瑞星公司联系。

地址：北京市海淀区中关村大街 22 号中科大厦 1403 室

邮编： 100190

网站： http://www.rising.com.cn

电话： 400-660-8866(免长途话费)或(86010)82616666

目录

1 软件产品说明

1.1 产品组成

当您通过合法途径获得瑞星安全云终端软件的使用权后，在安装使用前，请仔细检查核对包装内的《产品组件清单》。

1. 光盘：包含用户所购买的瑞星安全云终端软件所有程序。
2. 《使用手册》：即本手册，通过阅读它，掌握本软件的详细使用方法和技巧。
3. 产品序列号：为本套产品分配的唯一身份证明，缺少它，本软件将无法安装。

（注意：序列号请详见产品授权卡）。

1.2 应用环境

a. 软件环境

Windows XP 系统

Windows Vista 系统

Windows 7 系统

Windows 8 系统

Windows 8.1 系统

Windows 10 系统

Windows Server 2003 系列系统

Windows Server 2008 系列系统（包含 Windows Server 2008 R2 系统）

Windows Server 2012 系列系统

b. 硬件环境

Windows XP 系统：

CPU：500 MHz 及以上

剩余磁盘空间：1GB 及以上

内存：512 MB 系统内存及以上，最大支持内存 4GB

显卡：标准 VGA，24 位真彩色

其它：光驱、鼠标

Windows Vista 及以上Widnows 系统：

CPU：1.0 GHz 及以上 32 位 (x86) 或 64 位 (x64)

剩余磁盘空间：1GB 及以上

内存：1.0 GB 系统内存及以上，最大支持内存 4GB

显卡：标准 VGA，24 位真彩色

其它：光驱、鼠标

2 软件概述

瑞星安全云终端软件是瑞星信息技术股份有限公司推出的企业级杀毒软件产品，它为加强内网安全统一解决方案提供客户端支持，具有白名单、防病毒、漏洞扫描、文件监控、U 盘监控、系统加固、应用加固等功能。

传统的安全解决方案，比如防病毒、入侵检测等在网络安全中起到非常重要的作用，但很多企业在部署了这些安全产品后，还是得不到全面的安全防护，如：ARP 欺骗攻击、内部资料泄密等。这是由于传统的安全技术和解决方案主要保证网络边界的安全，而忽视内部网络的安全威胁。这些威胁主要表现在：移动电脑设备随意接入、非法外联难以控制、软硬件资产滥用、网络故障频发等。瑞星安全云终端软件产品，不仅包含传统的防病毒、入侵检测等安全功能，还具备增强内网信息安全性的强大功能，提供给企业用户一个完整的企业 IT 安全解决方案。可以更好的帮助企业用户解决内部信息安全问题、软硬件的运维管理问题。从而为企业用户提高 IT 维护效率，有效降低 IT 运营成本。

瑞星安全云终端软件产品实质上是内网管理平台的客户端组件，企业用户可以根据自身的需求在其上布置具有不同管理功能的子产品。本软件可以满足不同企业的不同需求，有针对性的解决企业遇到的各种安全风险，彻底改变了以往安全类软件功能过于笼统、不够灵活的缺点。瑞星安全云终端软件提供全盘查杀、快速查杀、自定义查杀等杀毒模式，并且在原有基础引擎的基础上引入了智能安全引擎查杀，包括：基础引擎、决策引擎（RDM）、云查杀引擎、基因引擎。防护中心专门为客户的特殊需求提供了诸如：飞客虫蠕虫、雨云病毒、威客虫蠕虫免疫、DLL 劫持免疫的特种专杀功能。设置简单方便，一键设置，一键查杀，多引擎混合，大大增强了病毒的查杀能力和覆盖范围。

打开瑞星安全云终端软件，进入到主界面，如图所示。

图 2-1

在主界面中心，病毒查杀页签内，主要是查杀病毒按钮，从左至右依次为：全盘查杀、快速查杀、自定义查杀。在查杀病毒按钮下方，显示智能安全引擎，从左至右依次为：基础引擎、决策引擎（RDM）、云查杀引擎、基因引擎。左下部为加入中心按钮。右下部是防护中心按钮。最下一栏分布着版本信息、上次更新时间以及检测更新按钮。当有更新时，检测更新按钮上方显示，如图所示。最下栏右侧为病毒扫描处理方式（发现病毒自动处理）和扫描完成自动关机。

点击上网防护页签，进入上网防护功能主界面。如图所示。

图 2-2

上网防护主界面主要是防护项的开关和拦截统计、右侧为上网管理和流量统计。最下一栏为恶意网址库版本信息和恶意网址库上次更新时间。

2.1 病毒查杀

瑞星通过总结近几年来恶意程序的发展状况，重新设计开发了使用恶意程序结构特征进行检测的反病毒技术。使用这种新的检测技术，瑞星安全云终端软件扫描时对系统资源的占用量非常小，并且速度有了大幅提升。

除此之外，瑞星安全云终端软件还采用了智能启发式检测技术、深度启发式检测技术、“云查杀”技术等。

2.2 防护中心

瑞星安全云终端软件为用户提供了全面的防护机制。电脑防护技术包括实时监控技术与智能主动防御技术。

主要技术包括文件监控技术、U 盘防护技术、系统加固技术、应用加固技术、病毒专杀技术、智能升

级技术。

2.3 上网防护

瑞星安全云终端软件为用户提供了全面的上网安全防护。上网防护技术包括拦截恶意木马网址、拦截钓鱼网址、拦截恶意下载、拦截跨站脚本攻击、搜索引擎结果检查、广告过滤以及防黑客攻击。

在上网管理窗口可以查看受限网址、受限程序和安全共享的相关信息；在流量统计窗口也可以查看流量的统计详情。

2.4 在线客服

瑞星安全云终端软件在线客服为客户提供了直接和客服沟通的渠道，包括机器人、远程服务和申请上门服务。

机器人功能和 Web 版的智能客服功能相同，详情请参考本文档章节 12 智能客服。

远程服务为客户提供远程的技术支持，节省解决问题的时间。

申请上门服务，当远程服务依然不能解决问题时，可以为客户现场解决问题。

2.5 设置中心

瑞星安全云终端软件设置中心提供了常用的软件设置项，可以对病毒查杀、上网防护、软件更新以及托盘功能进行设置。

2.6 日志中心

瑞星安全云终端日志中心记录了软件的查杀病毒操作日志，软件升级日志，云中心消息日志和云中心下发的命令日志等。

2.7 托盘功能

瑞星安全云终端软件提供的托盘功能可以快速的打开主程序、快速杀毒、快速查看日志、快速设置软件和退出程序。

2.8 检测更新

当需要更新软件时，点击主界面右上角的“  ”图标，选择“检测更新”选项，获取最新的软件。

2.9 在线修复

当瑞星安全云终端软件出现故障或者损坏时，可以通过在线修复为用户提供软件修复（版本提升）。

2.10 智能客服

智能客服为用户提供常见的问题咨询和解答，如果没有解决您的问题，在工作日工作时间内还可以转至人工服务。

3 安装与卸载

本章主要介绍瑞星安全云终端软件的安装和卸载方法步骤以及注意事项。

3.1 软件安装

第一步：将瑞星安全云终端软件光盘放入光驱内，启动产品安装主界面后，开始安装。

图 3-1

第二步：进入安装程序欢迎界面，勾选“我已阅读并同意瑞星用户许可协议”，勾选“同意安装过程中，重启系统网络”，点击【一键快速安装】，界面将显示安装进度。

图 3-2

也可以点击【自定义安装】，自定义安装路径和快捷方式。

图 3-3

第三步：安装大概需要 30 秒钟，安装结束后将进入如图界面，点击“开启安全之旅”按钮，进入瑞星安全云终端软件主界面。

图 3-4

第四步：进入主界面如图所示。

图 3-5

第五步：安装结束。

3.2 软件卸载

当需要卸载瑞星安全云终端软件时，可以通过 Windows 的开始菜单，找到瑞星安全云终端的【卸载】选项，如图所示：

图 3-6

勾选“删除隔离区下的隔离文件”复选框，卸载时将删除隔离区文件，不勾选将保留隔离区文件。

软件将快速的进行自动卸载，卸载完成后弹出完成界面如图所示。

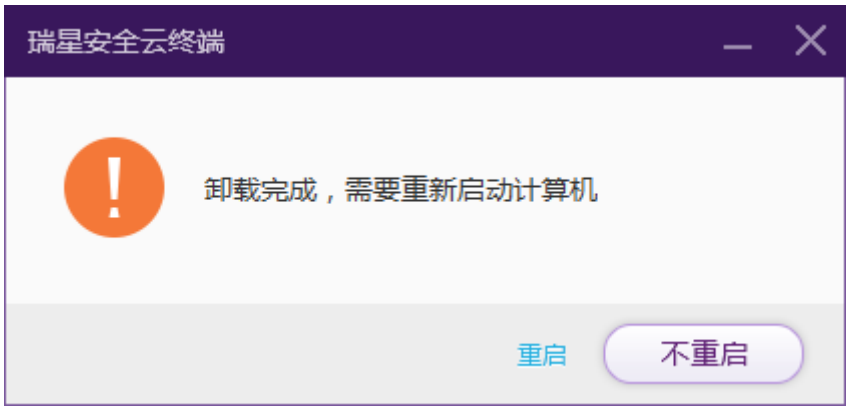


图 3-7

点击【重启】按钮，重启计算机后，卸载完成。

4 病毒查杀

瑞星安全云终端软件提供了多种方便快捷的查杀方式，包括：【快速查杀】、【全盘查杀】和【自定义查杀】。如图所示。请根据不同使用场景选择使用。

图 4-1

4.1 快速查杀

快速查杀可以对系统文件和关键文件进行扫描查杀，特点是快速有效的保护系统，防止病毒感染系统文件。

打开瑞星安全云终端软件主程序界面，单击主界面的【快速查杀】图标按钮，开始进行快速病毒查杀，界面将显示查杀进度、线程、速度、查杀模式、本地引擎发现威胁个数、云发现威胁个数、扫描个数、扫描速度、威胁个数、处理个数、扫描时间如图所示：

图 4-2

如需暂停查杀，请点击查杀界面【暂停】按钮，点击【继续】恢复查杀；如需停止查杀，请点击查杀界面【停止】按钮，弹出确认提示窗口。如图所示：

图 4-3

点击【停止查杀】停止查杀病毒。继续查杀病毒请点击【继续查杀】。

快速查杀模式默认选择“自动模式”，可根据实际需要选择“办公模式”或者“高速模式”。“办公模式”可以降低 CPU 的占用率，查杀时电脑卡顿推荐使用该模式；“高速模式”可以提高查杀速度，需要节省查杀时间并且 CPU 频率较高可使用该模式。

进行快速查杀时，任务栏的瑞星软件图标显示状态为“ ”。

在快速查杀界面左侧，可以显示线程 ID、文件路径和线程状态，如图所示。

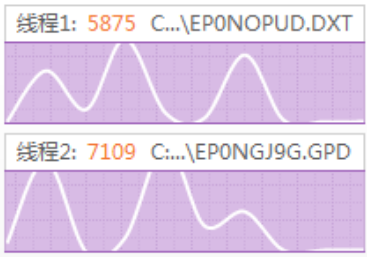


图 4-4

查杀到病毒时，软件会显示病毒信息，若查杀病毒设置为【自动清除病毒并提醒】，则状态为“处理成功”，如图所示：

图 4-5

通过查杀结果，可以查看一共有多少威胁，扫描对象数量，扫描共计用时。通过统计图，还可以看到近期的病毒情况。

点击【查看日志】，可以查看日志详情。点击【智能客服】，咨询常见问题。点击结果统计界面右上角的  ，返回主界面。

4.2 全盘查杀

全盘查杀将对计算机的所有硬盘进行扫描，能全面有效的保护计算机安全。

打开瑞星安全云终端软件主程序界面，单击【全盘查杀】图标按钮即可开始进行全盘病毒查杀，如图所示；

图 4-6

如需暂停查杀，请点击查杀界面【暂停】按钮；如需停止查杀，请点击查杀界面【停止】按钮。

全盘查杀模式默认选择“自动模式”，可根据实际需要选择“办公模式”或者“高速模式”。“办公模式”可以降低 CPU 的占用率，查杀时计算机卡顿推荐使用该模式；“高速模式”可以提高查杀速度，需要节省查杀时间并且 CPU 频率较高可使用该模式。

查杀结束后，可以看到查杀结果，病毒数量，处理方式，以及历史查杀病毒折线图。

图 4-7

点击【查看日志】，可以查看日志详情。点击【智能客服】，咨询常见问题。点击结果统计界面右上角的 ，返回主界面。

4.3 自定义查杀

自定义查杀，用户可以根据需求选择查杀病毒区域，可选区域包括：硬盘分区、U 盘、系统引导区、系统目录、系统内存和系统桌面。

打开瑞星安全云终端软件主程序界面，单击【自定义查杀】开始进行快速病毒查杀。如图所示。

图 4-8

弹出界面如图所示。

图 4-9

选择需要查杀的区域，如 C 盘、桌面、系统引导区等，点击【开始查杀】，显示界面如图所示。

图 4-10

可以查看到扫描的文件数量、扫描速度、威胁数目、已经处理的数目以及扫描时间。

如需暂停查杀，请点击查杀界面【暂停】按钮；如需停止查杀，请点击查杀界面【停止】按钮。

自定义查杀模式默认选择“自动模式”，可根据实际需要选择“办公模式”或者“高速模式”。“办公模式”可以降低 CPU 的占用率，查杀时计算机卡顿推荐使用该模式；“高速模式”可以提高查杀速度，需要节省查杀时间并且 CPU 频率较高可使用该模式。

在详细的栏中可以看到病毒对应的病毒类型和病毒文件的路径以及病毒所处的状态。

在扫描的时候，勾选【发现病毒自动处理】，则详细记录栏会先是病毒的详细情况及其处理状态。勾选右下角的【扫描完成自动关机】，则完成扫描任务后自动关机。

扫描完成后，显示如图所示界面。

图 4-11

点击【查看日志】，可以查看日志详情。点击【智能客服】，咨询常见问题。点击结果统计界面右上角的 ，返回主界面。

4.4 智能安全引擎

智能安全查杀引擎有四个，分别是：基础引擎、决策引擎、云查杀引擎、基因引擎。可执行程序引擎经过重写，引擎的可扩展性和兼容性得到了提升。同时，查杀方法、病毒库、病毒记录方式进行了优化。理论上，查杀速度变得更快，病毒库变得更小。

下面将具体介绍每个引擎的功能。

4.4.1 基础引擎

基础引擎用于查杀各种恶意软件和插件，能够精准的识别出恶意软件和插件。

4.4.2 决策引擎

决策引擎基于高级人工智能算法，能够智能识别未知的病毒和木马，即使病毒库中没有，也可以通

过算法将未知病毒查杀。

4.4.3 云查杀引擎

通过瑞星云端引擎，能够瞬间匹配亿万病毒库数据，根据病毒特质，进行秒杀，新型病毒也可以瞬间杀死。

4.4.4 基因引擎

通过流行的病毒数据，提取出“软件基因”，对流行性病毒和木马群进行针对性查杀。

5 防护中心

在主界面右下角，点击【防护中心】按钮，进入防护中心。如图所示。

图 5-1

防护中心分为两类，分别为：监控类防护和专杀类防护。

各防护功能通过滑动开关进行控制，点击相应功能开关即可打开或关闭功能。当功能下的开关处于 已开启 时，表示该功能开启，功能图标呈蓝色；当处于 已关闭 时，表示该功能关闭，功能图标呈灰色。

在防护中心的右上角，显示安全防护功能开启的数量和防护功能总数。

点击右下角的【安全设置】，进入所有防护功能的设置界面，可以对文件监控、邮件监控等进行详细设置。

点击右下角的【防护日志】，进入安全防护功能的日志记录界面，查看防护中心产生的日志。

点击右上角的 ，关闭防护中心界面。

5.1 监控类防护

监控类防护包括：文件监控、邮件监控、共享监控、U 盘监控、系统加固、应用加固。如图所示。

图 5-2

文件监控：主要针对计算机本地存储的文件，对文件的活动和状态进行有效的监控，对病毒严防死守。设置详情请参考章节 7.1.5 文件监控。

当文件监控发现病毒时，会以弹窗的形式提醒。若文件监控设置【发现病毒处理】设置为自动清除，则提示“发现病毒并清除成功”，如图所示：

图 5-3

弹窗将显示病毒所在位置、病毒名称和相关进程。还可以通过点击【查看日志】，跳转到病毒处理的详情日志界面，详情请查看日志中心的章节 8.1 病毒详情。点击【我知道了】关闭窗口。

若【发现病毒处理】设置为【手动清除】，则弹出病毒警告，提示“发现病毒需要处理”，如图所示：

图 5-4

弹窗将显示病毒所在位置、病毒名称、相关进程以及出现问题的原因和处理建议。

在弹窗中选择【删除】，删除病毒文件；否则，选择【不处理】，不对病毒文件做任何处理。对不做处理的病毒，可以点击文件定位图标 ，定位病毒文件位置。

如果不需要再弹窗提示，请勾选“重启前不提示”复选框，那么在重启计算机之前，都不再弹窗提示。

查杀结束后，显示查杀结果，如图所示。

U 盘监控：主要针对插入计算机的 U 盘进行扫描和监控，对有害文件进行及时的拦截和处理。设置详情请参考章节 7.2.6 U 盘监控。

系统加固：对系统的重要文件进行加固防护，保护系统安全，对破坏系统文件类型病毒有很好的防护效果。设置详情请参考章节 7.2.7 系统加固。

启用系统加固后，使用文件、注册表、进程、系统文件遭到删除或篡改时，瑞星安全云终端软件将进行拦截，并弹出提示，如图所示。

图 5-5

应用加固：对系统安装的应用进行加固，防止病毒或木马对系统上的应用进行破坏，或者是阻止木马盗取系统应用数据。设置详情请参考章节 7.2.8 应用加固。

开启应用加固后，瑞星安全云终端软件将对浏览器/办公软件实时进行保护。有对浏览器/办公软件进行攻击和修改的行为，都将进行拦截并弹出提示，如图所示。

图 5-6

5.2 专杀类防护

专杀类防护主要包括：飞客虫蠕虫、雨云病毒、威客虫蠕虫免疫、DLL 劫持免疫。专杀类防护功能开启后，对上述病毒进行针对性防护。如图所示。

图 5-7

飞客虫蠕虫：飞客虫蠕虫(Hack Exploit Win32 MS08-067)是一个利用微软 MS08-067 漏洞发起攻击的蠕虫病毒。该病毒会对随机生成的 IP 地址发起攻击，攻击成功后会下载一个木马病毒，通过修改注册表键值来使安全软件功能失效。病毒会修改 hosts 文件，使用户无法正常访问安全厂商网站及其服务。

雨云病毒：雨云病毒为蠕虫病毒，中毒后的表现为任务管理器中有 wscript.exe 运行，在桌面上有名为 yuyun_ca 的图标，并且无法删除。通过共享方式进行传播，在局域网中很容易传播。

威客虫蠕虫免疫：威客虫蠕虫病毒中毒表现为无法启动系统，若启动系统后进行全盘扫描，则直接死机，该蠕虫病毒主要针对硬盘，中毒后只能格式化整块硬盘。

DLL 劫持免疫：DLL 劫持表现为，当一个可执行文件运行时，Windows 加载器将可执行模块映射到进程的地址空间中，加载器分析可执行模块的输入表，并设法找出任何需要的 DLL，并将它们映射到进程的地址空间中。

6 上网防护

在主界面点击【上网防护】页签，进入上网防护功能界面。包括防护项、上网管理和流量统计。如图所示。

图 6-1

6.1 防护项

在上网防护界面，总共有 7 个防护功能项。分别为：拦截恶意木马网址、拦截钓鱼网址、拦截恶意下载、拦截跨站脚本攻击、防黑客攻击、搜索引擎结果检查和广告过滤。其中已经开启的功能图标呈蓝色，未开启的图标呈灰色。默认防黑客攻击和流量统计等功能未开启，所以呈灰色。

点击右上部的 

，所有防护项将被开启，图标均变为蓝色，并且图标下方显示 已开启 。上网防护界面变为如图所示。

图 6-2

若想关闭某个防护项，直接点击该防护项图标即可关闭，再次点击图标又打开该功能。也可以通过点击图标下的 ，选择“重启前关闭”或者“永久关闭”。如图所示。

图 6-3

“重启前关闭”是暂时关闭该功能，在下一次重新启动计算机时，该功能又自动生效，而“永久关闭”是重启时不自动开启，需要手动开启。

在各防护功能图标的正下方，可以显示相应的拦截次数，方便了解上网防护拦截情况。

6.1.1 拦截恶意木马网址

本防护项可以拦截带有木马病毒的网址的访问，并统计拦截次数。避免用户计算机被挂马网站的病毒感染，保护上网安全。

6.1.2 拦截钓鱼网址

本防护项拦截钓鱼网站的访问，并统计拦截次数。

6.1.3 拦截恶意下载

本防护项拦截网站的下载，并统计拦截次数。

6.1.4 防黑客攻击

本防护项拦截网站的黑客攻击，并统计拦截次数。

6.1.5 拦截跨站脚本攻击

本防护项拦截跨站脚本攻击，并统计拦截次数。

6.1.6 搜索引擎结果检查

本防护项检查搜索引擎结果，拦截有害的结果，并统计拦截次数。

6.1.7 广告过滤

本防护项对广告进行过滤和拦截，并统计拦截次数。

6.2 上网管理

上网管理主要对拦截网站、拦截程序和安全共享功能进行展示和统计。上述功能的统计信息都将展示在上网管理面板上。如图所示。

图 6-4

点击受限网址、受限程序将进入相应的设置界面，设置的具体详情请参考章节 7.2.5 受限网址 和 7.2.6 受限程序。

点击安全共享，进入安全共享统计界面，界面展示共享数量、近一周访问人数和近一周访问次数，还可以增加新的共享。如图所示。

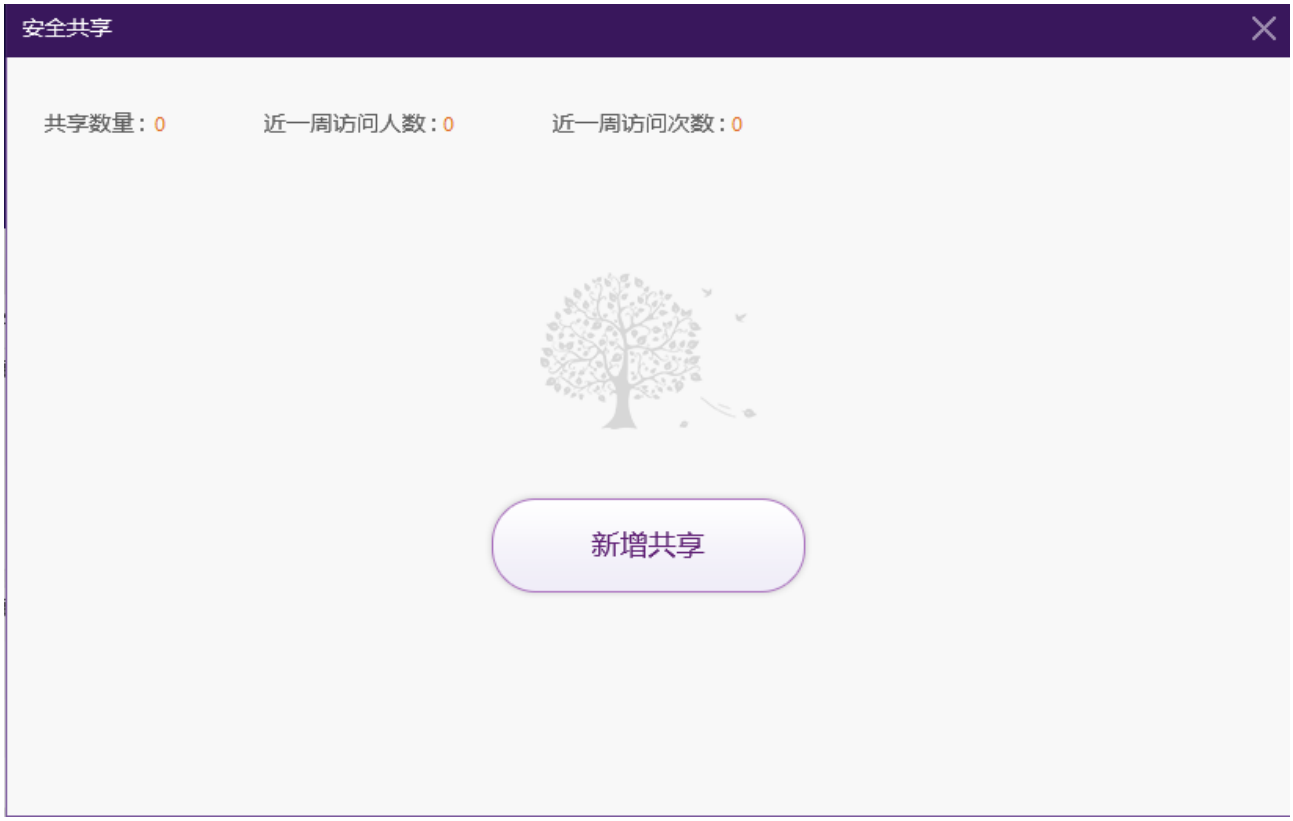


图 6-5

点击【新增共享】，弹出添加窗口，填写资源共享名称、选择文件共享路径和设置访问权限（只读、读写），如图所示。

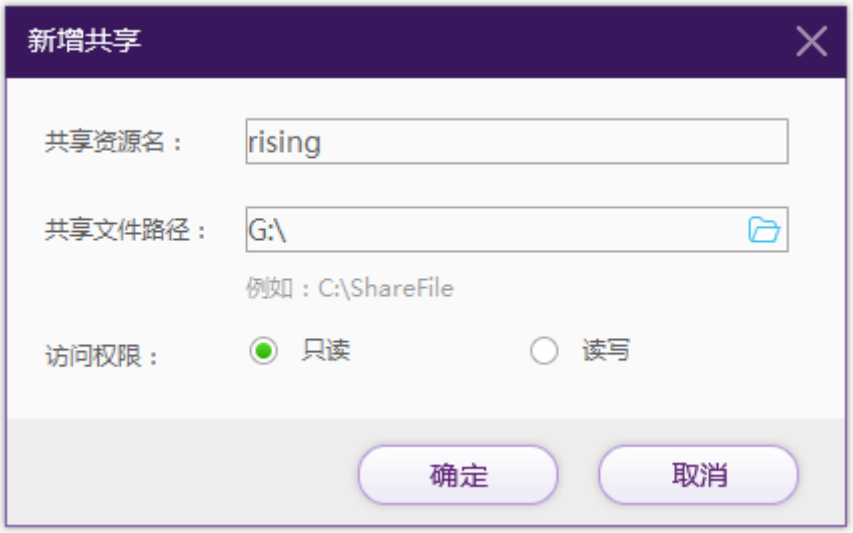


图 6-6

设置完成后，共享资源信息将展示在共享资源面板上，如图所示。

图 6-7

点击设置好的资源图标，进入到对应的共享目录文件夹。资源图标上还展示设置的共享资源名称、权限、访问次数和共享位置。

点击资源图标右上角的删除图标，停止资源共享，确认即可删除，如图所示。

图 6-8

6.3 流量统计

统计图通过折线展示了近一段时间（时间段设置请参考章节 7.2.7 流量管理）流量流入流出，方便用户实时掌握流量使用情况。可以及时发现流量异常。

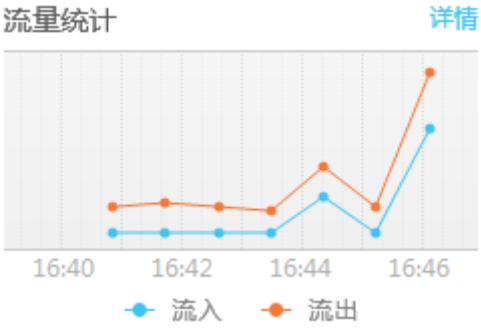


图 6-9

点击【详情】，将进入到上网流量日志信息界面。详情请参考章节 8.2.7 上网流量。

7 在线客服

在主界面上点击【在线客服】页签，进入在线客服功能界面。如图所示。

图 7-1

界面功能包括机器人、远程服务和申请上门。界面设置包括设置、导出日志和更换皮肤。如图所示。

图 7-2

7.1 机器人

在机器人的对话框中输入您的问题，点击【发送】，机器人将自动返回问题的解决办法。在您输入问题的同时，输入框上方将自行匹配近似的问题，选择问题，机器人直接放回答案。如图所示。

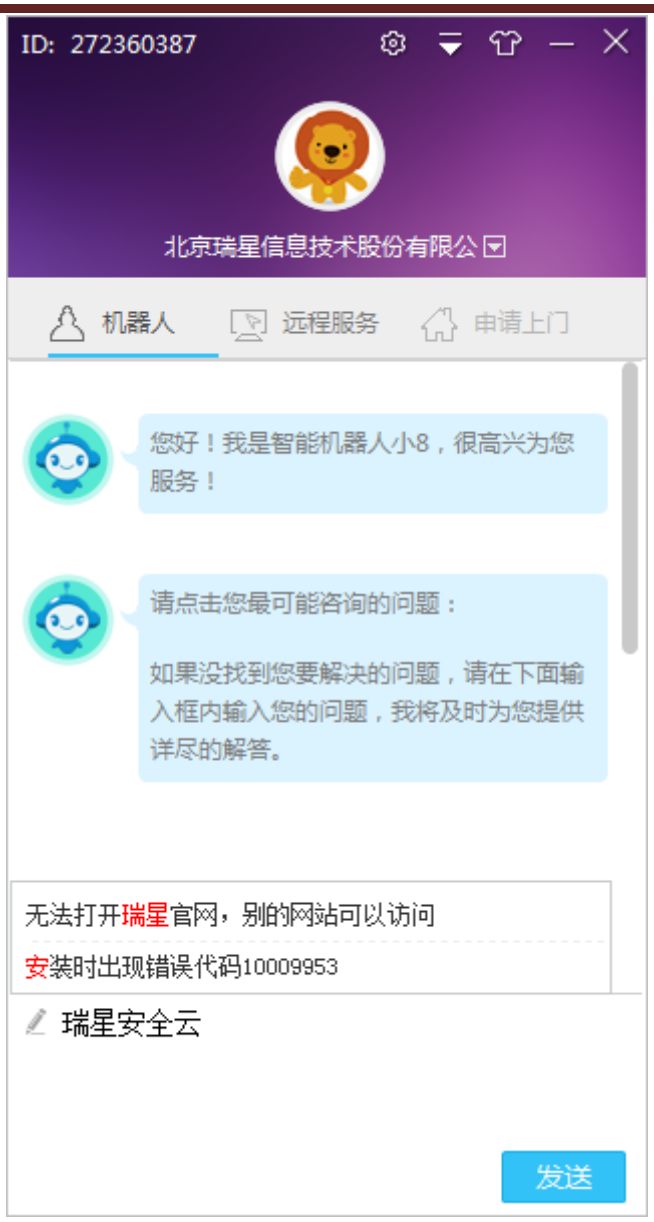


图 7-3

7.2 远程服务

在线客服的主界面选择【远程服务】页签，进入远程服务。如图所示。

图 7-4

可以点击【直接去排队】，系统将自动匹配客服工程师。匹配后就可以和客服工程师直接交流问题和解决办法。

您也可以拨打服务商电话 400-600-8866，同时将您的 ID 号告知客服工程师。ID 号显示于在线客服界面的左上角。如图所示。

图 7-5

7.3 申请上门

7.4 设置

在线客服主界面的顶端点击图标，进入设置界面。如图所示。

图 7-6

设置分基本设置和主从设置。主要针对的是远程服务所进行的设置。

7.4.1 基本设置

基本设置包括远程服务时本机信息、连接密码、消息热键、声音提醒、高级选项和文件默认存储目录。

本机信息：点击【设置信息】，弹出如下图所示界面。填入主机备注、联系人姓名和联系方式，保存。

图 7-7

连接密码：用于远程连接时，保证信息安全。点击【设置密码】，在密码设置界面输入密码。如图所示。

图 7-8

如需更改密码，请点击【修改密码】，在界面中分别输入原密码和新密码。点击【确定】保存。如图所示。

图 7-9

消息热键：用于设置会话聊天时发送信息的按键。热键方式二选一。

声音提醒：勾选【开启聊天消息声音提醒】，聊天中将以声音提醒收到消息。

高级选项：可以设置解决远程问题、自动接收文件和密码连接自动接收文件。

当远程连接过程中遇到问题时，可以尝试勾选【作为系统服务运行，能够有效解决无人值守时，屏保、电脑重启、远程无法登陆系统等问题】解决。

【自动接收文件】，勾选后，聊天中将会自动接收客服工程师的文件。

【密码连接自动接收文件】，勾选后，远程连接若通过密码方式进行的，将自动接收来自客服工程是的文件。

文件默认存储目录：用于指定接收文件的存储目录，点击【更改目录】进行修改。

所有设置项都设置完毕后，请点击【保存】，保存设置。

7.4.2 主从设置

主从设置用于设置局域网内主机的主从关系。解决局域网内部分客户端无法联网进行远程服务的问题。如果在同一局域网内，有电脑无法联网，可以将这台电脑设置为“从客户端”，能联网的电脑设置为“住客户端”，使“从客户端”能够通过“主客户端”获取远程服务。

默认主从设置为【不设置】，请根据说明和实际需求进行设置。设置完后请记得点击【保存】。如图所示。

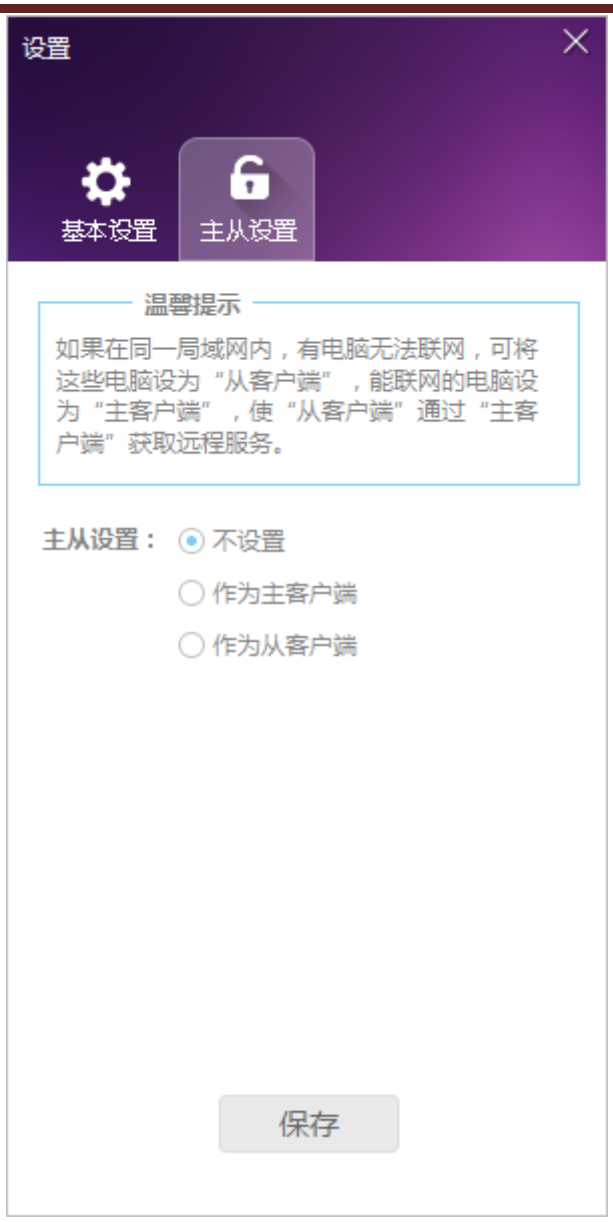


图 7-10

7.5 导出日志

导出日志，用于导出客户端的操作日志和客户端后台日志。

在设置右侧，点击，弹出 导出日志，点击【导出日志】，提示操作成功。如图所示。

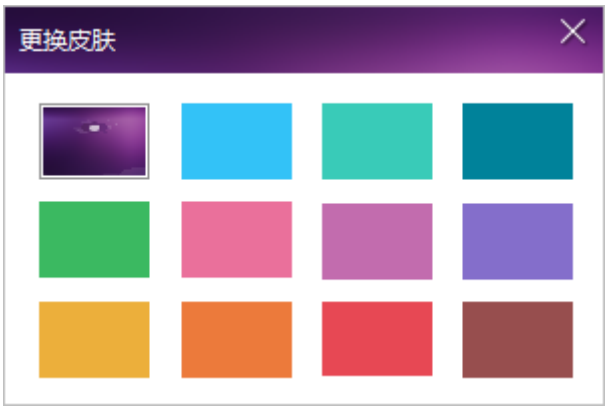
图 7-11

点击【打开日志】，进入目录，即可查看日志信息。如图所示。

图 7-12

7.6 皮肤设置

在线客服的右上角，点击图标，弹出更换皮肤界面，如图所示。



点击喜欢的皮肤即可。

8 设置中心

在瑞星安全云终端软件的主界面右上角点击“ ”，进入设置中心，如图所示。

图 8-1

设置中心分病毒查杀、上网防护和基础设置三大设置项。下面将详细说明各项目设置方法。

8.1 病毒查杀

病毒查杀设置可以对瑞星安全云终端软件的杀毒、扫描进行详细设置，主要有常规项、白名单、杀毒备份、查杀病毒、文件监控、邮件监控、共享监控、U 盘监控、系统加固和应用加固等，如图所示。

8.1.1 常规项

常规项设置可设置项为：运行环境、病毒跟踪、病毒日志、引擎设置、扫描缓存。

点击【病毒查杀】>【白名单】，进入常规项设置，如图所示。

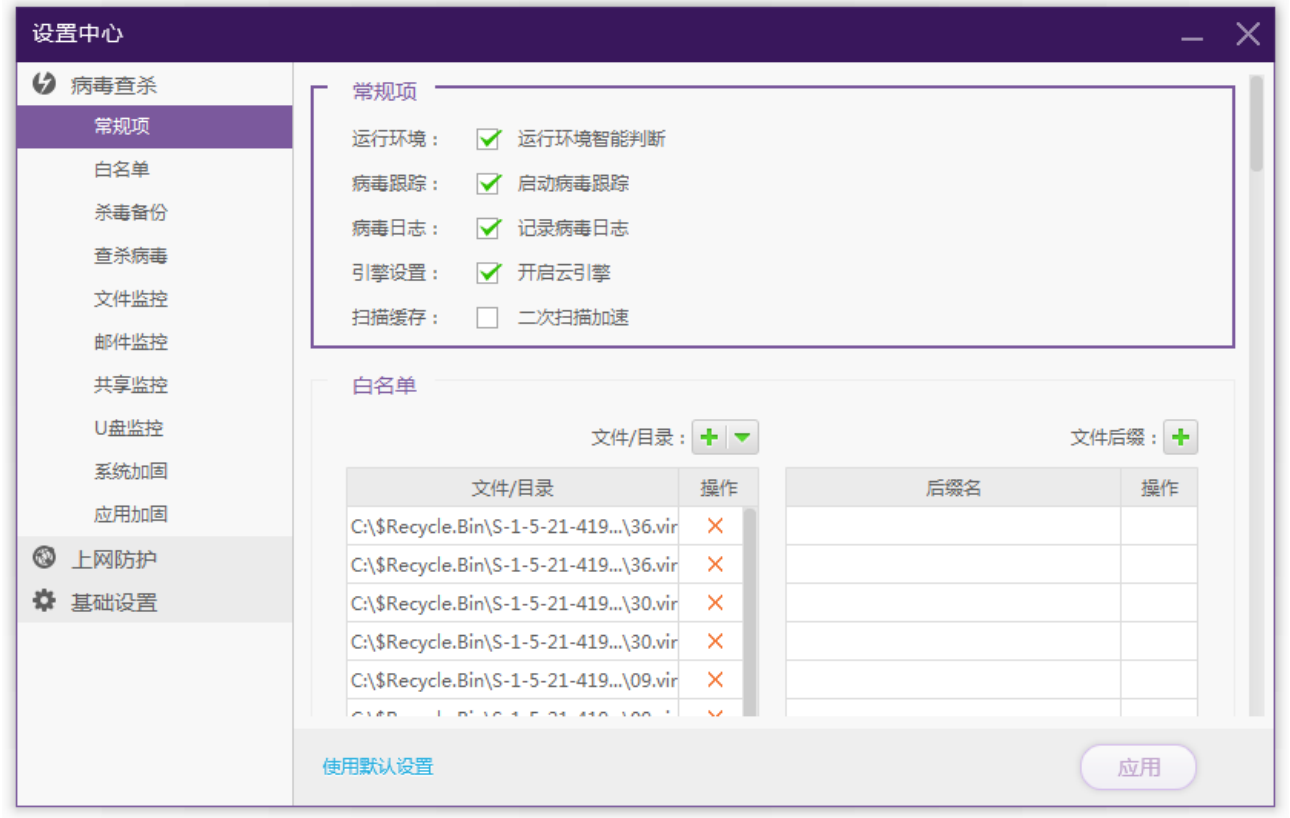


图 8-2

运行环境：勾选【运行环境智能判断】选项后，软件将自动设置好参数，适应系统，发挥最好的性能。

病毒跟踪：勾选【病毒跟踪】选项后，软件将启用病毒跟踪功能，对常见和流行性病毒进行实时跟踪。

病毒日志：勾选【病毒日志】选项后，软件将会对系统查杀和扫描的病毒信息进行记录，方便进行病毒分析和病毒防疫。

引擎设置：勾选【引擎设置】选项后，软件将开启云查杀模式，使用瑞星自主研发的云引擎，提高查杀效率和速度。

扫描缓存：勾选【扫描缓存】选项后，软件将开启二次扫描加速功能，对一段时间内扫描状态进行缓存和优化，使扫描更快、更流畅。

8.1.2 白名单

白名单用于添加那些不需要扫描和查杀的文件，添加白名单后，软件扫描和监控时将智能跳过这些文件。白名单添加方式分为两种：一种是以文件/目录方式，另一种是以文件后缀方式。如图所示。

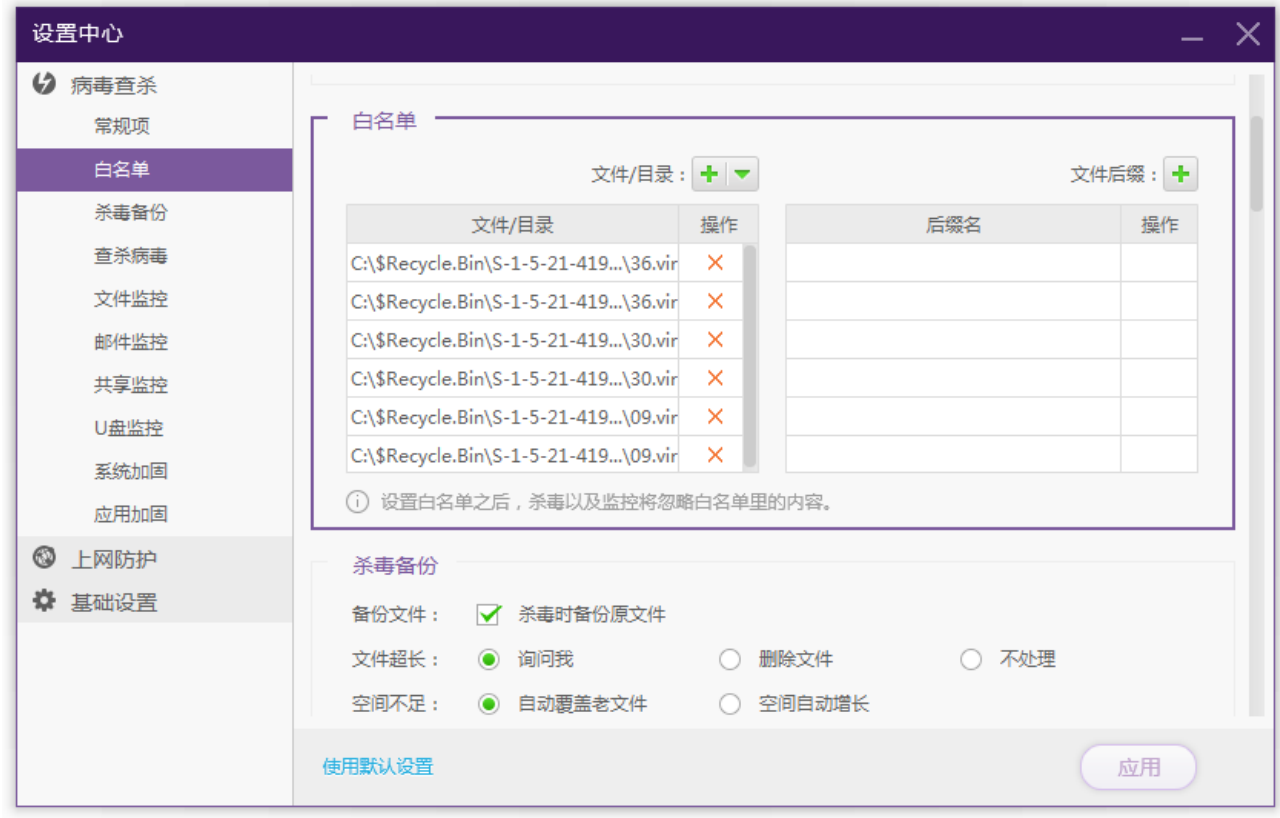


图 8-3

8.1.2.1 文件/目录

点击【病毒查杀】>【白名单】，然后在文件/目录栏点击图标“  ”，出现下拉菜单，如图所示。

图 8-4

在菜单中，可以通过四种方式设置文件和目录，分别是：

目录+子目录：扫描时，软件将所选的目录和它的子目录一起忽略。

目录：扫描时，软件将忽略掉所选目录中的文件，而其子目录中的文件依然会扫描到。

子目录：扫描时，软件只忽略所选目录的子目录。

文件：扫描时，软件忽略掉所选的文件。

如果需要将已经加入白名单的文件/目录删除，请点击表中“操作”一栏的删除✕。如图所示。

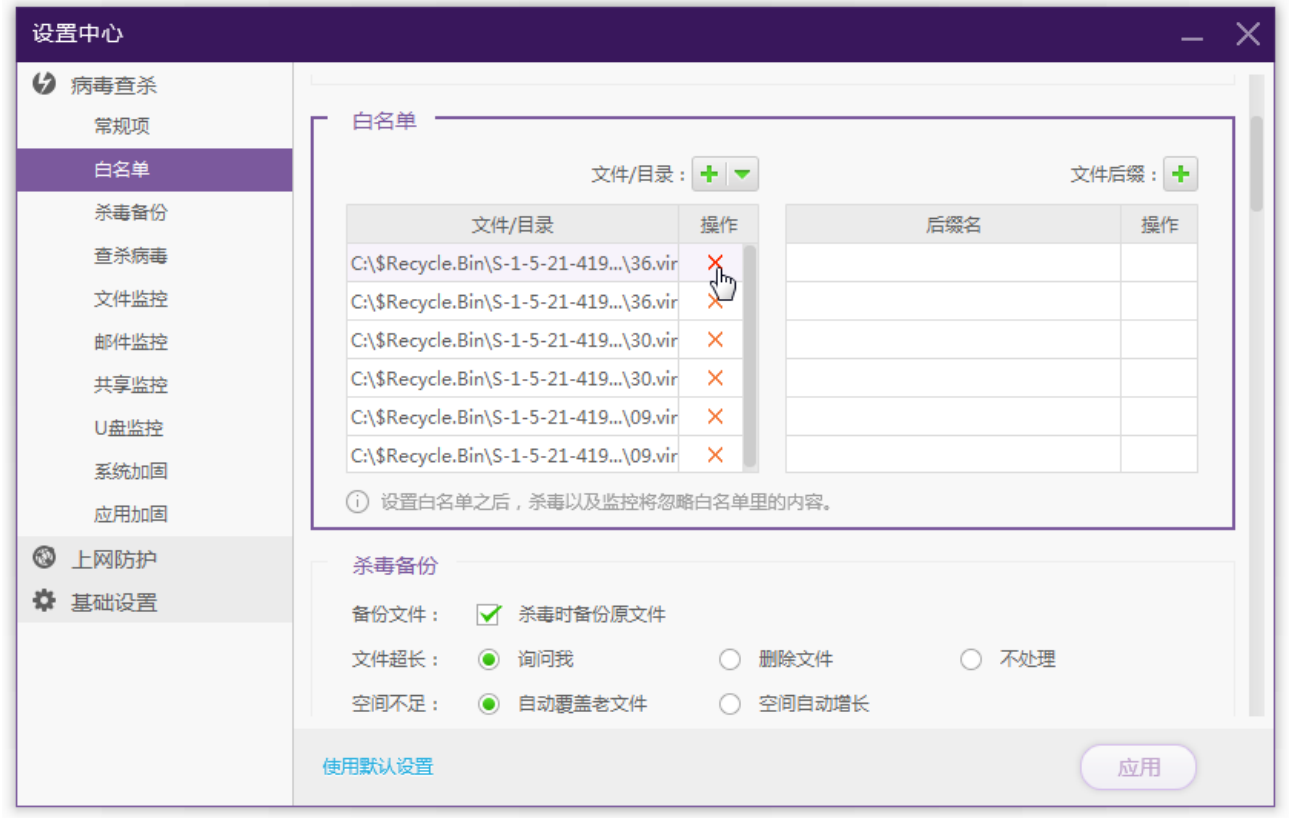


图 8-5

设置完成后，点击右下角 应用 ，保存设置。

8.1.2.2 文件后缀

点击【病毒查杀】>【白名单】，然后在文件后缀一栏点击图标“ ”，下方的表格中将添加一行，输入需要加入白名单文件的后缀名，如图所示。

图 8-6

如果要从白名单中删除，点击“操作”一栏中的删除 。如图所示。

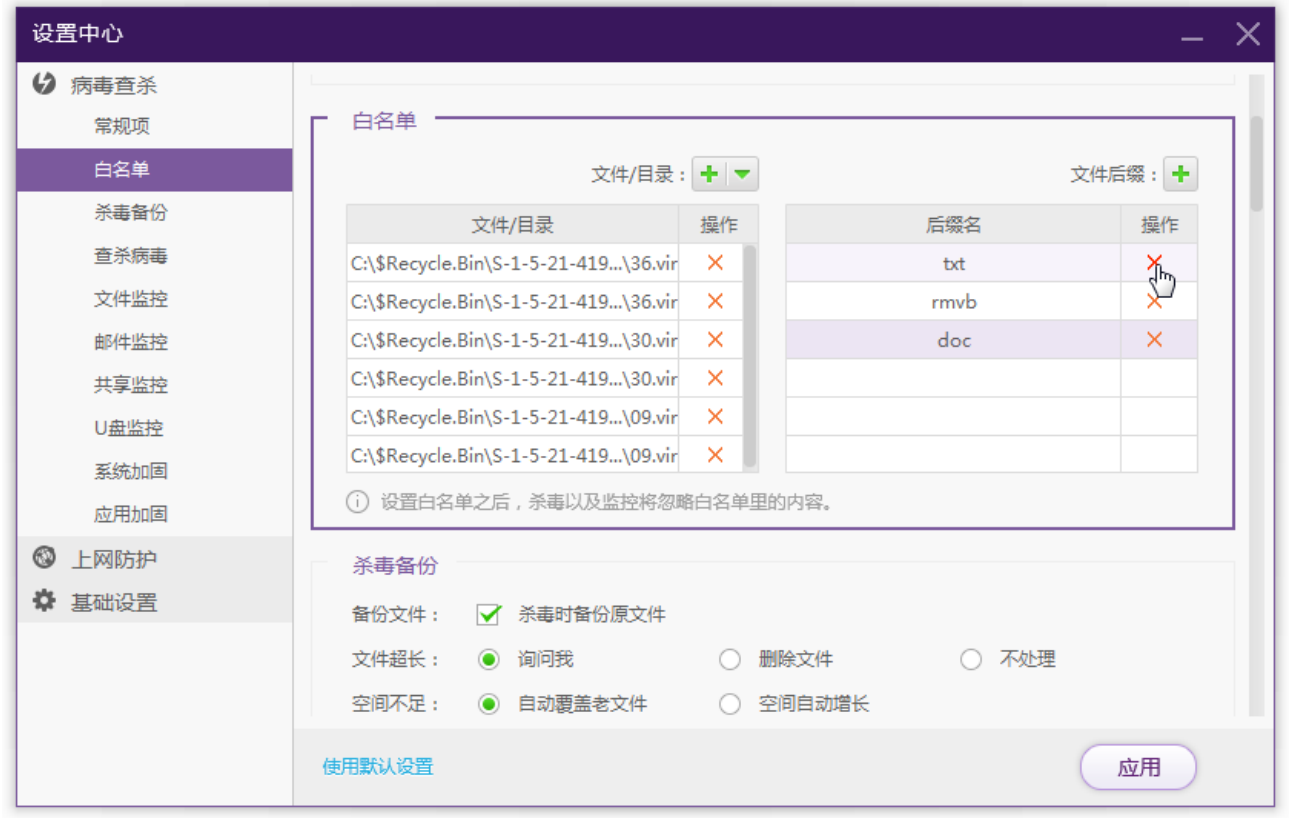


图 8-7

设置完成后，点击右下角 应用 ，保存设置。

8.1.3 杀毒备份

杀毒备份相当于病毒隔离区，将病毒文件隔离起来，既可以有效防止继续感染其他文件，又可以保留病毒源文件。

点击【病毒查杀】>【杀毒备份】，进入病毒备份设置，如图所示。

图 8-8

杀毒备份设置项如下：

备份文件：勾选【杀毒时备份原文件】，即可将病毒文件备份到隔离区，供以后使用。

文件超长：查杀时，文件很大，可以设置询问、直接删除、不处理。

空间不足：当隔离区备份的文件过多，导致隔离区空间不够时，空间的处理方式可以自动覆盖老文件，或者空间自动增长。用户根据具体环境进行选择。

备份失效：备份的病毒文件由于时间过长等原因导致失效，可以设置询问我、删除文件和不处理的方式。用户根据具体环境进行选择。

所有设置项设置完成后，点击右下角 

，保存设置。

8.1.4 查杀病毒

查杀病毒可以设置扫描文件类型、查杀引擎的选择等。

点击【病毒查杀】>【查杀病毒】，进入查杀病毒设置，如图所示。

图 8-9

文件类型：杀毒软件需要在查杀时扫描的文件类型，默认为所有文件，也可以选择程序和文档。

查杀引擎：杀毒软件带有 4 个查杀引擎，分别针对不同类型的病毒和安全威胁。勾选“仅查杀流行病毒”，会重点查杀最近比较活跃的病毒；勾选“启发式查杀”，可以有效的对可疑的文件查杀；勾选“压缩包检查”，并设置好压缩包的容量，查杀时可以嵌入到压缩包中查杀。

发现病毒：发现病毒的处理方式，可选自动或者手动。自动方式无需用户确认，自行清除病毒文件；手动处理方式，需要用户确认是保留还是删除病毒文件。

所有设置项设置完成后，点击右下角 

，保存设置。

8.1.5 文件监控

文件监控能对终端的读写、文件、程序进行实时保护，一旦发现可疑文件和可疑操作立即拦截。

点击【病毒查杀】>【文件监控】，进入文件监控设置，如图所示。

图 8-10

文件监控设置项如下：

文件监控：勾选【开机启用】，则文件监控功能随计算机启动，实时监控扫描病毒和木马。

智能黑名单：勾选【开启】，黑名单生效。

监控设置：勾选【开启内核监控】，监控功能生效。

监控模式：可选项包括【所有】和【智能】，所有会监控所有文件的改动，智能是根据程序智能规则自行判断需要监控的文件。

文件类型：可以选择【所有文件】或者【程序和文档】。

监控加速：勾选【信任程序分析】，功能生效。

嵌入查杀：勾选【启用嵌入式查杀】，嵌入式查杀功能生效。

查杀引擎：勾选【仅查杀流行病毒】，即对活跃病毒进行重点的查杀；勾选【启发式查杀】，即将所有的可疑文件都列入查杀范围；勾选【启动压缩包查杀】，即可以查杀压缩包内的文件，同时对压缩包的大小可以进行限定。

发现病毒：选择发现病毒时的处理方式，可选择【自动处理】，如需手动处理，则选择【手动处理】。

8.1.6 邮件监控

邮件监控功能可对来往邮件及其附件进行及时查杀，对可疑邮件进行拦截，并阻止其继续在网络中传播。

点击【病毒查杀】>【邮件监控】，进入邮件监控设置，如图所示。

图 8-11

邮件监控：勾选【开机启用】，邮件监控功能在开机时才生效。选择文件类型，【所有文件】或者【文档和程序】。

查杀引擎：勾选【仅查杀流行病毒】，即对活跃病毒进行重点的查杀；勾选【启发式查杀】，即将所有的可疑文件都列入查杀范围；勾选【启动压缩包查杀】，即可以查杀压缩包内的文件，同时对压缩包的大小可以进行限定。

发现病毒：发现病毒处理方式，可以选择【自动处理】或者【不处理】。

扫描结果：扫描完邮件及其附件后的提示方式，可选项包括【不提示】、【发现病毒时提示】和【有病毒、无病毒都提示】。

端口策略：设置需要监控的邮件端口，默认已经设置了 25 和 110 端口，请用户根据自身具体邮件端口号进行设置，并选择相应的协议。点击 添加端口策略，点击 删除已经存在的端口策略。

8.1.7 共享监控

共享监控是对计算机共享监控的设置，可设置共享文件发现病毒时处理方式和提示方式。

点击【病毒查杀】>【共享监控】，进入共享监控设置，如图所示。

图 8-12

勾选【开机启用】后，共享监控才在计算机启动后生效，选择文件类型，选择查杀引擎，再设置发现病毒处理方式，最后设置扫描结果是否提示。

8.1.8 U 盘监控

U 盘监控，对 U 盘进行防护，能有效的防止病毒从 U 盘感染计算机。

点击【病毒查杀】>【U 盘监控】，进入 U 盘监控设置，如图所示。

图 8-13

插入 U 盘时：选择【询问是否查杀】或者【立即查杀】。

查杀深度：可以设置对 U 盘文件的查杀递归层次，数字设置越大，能查杀的目录层次越深，查杀的文件越多。

8.1.9 系统加固

对系统的重要文件进行加固防护，保护系统安全，对破坏系统文件类型病毒有很好的防护效果。

点击【病毒查杀】>【系统加固】，进入系统加固设置，如图所示。

图 8-14

可设置项如下：

发现威胁：【自动处理】或者【通知我】。

拦截日志：勾选【记录拦截日志】，则在日志中心产生日志记录，否则不生成日志。

监控灵敏度：分为【低】、【中】、【高】，灵敏度越高，需要消耗更多的系统资源，推荐选择【中】。

审计模式：勾选【开启】后，审计模式生效，对所有触犯规则的动作都做放行处理。

其他：勾选【放过带数字签名的程序】，对系统中已经获得微软等安全数字签名认证的程序一律放行。

8.1.10 应用加固

当对系统安装的应用进行加固，防止病毒或木马对系统上的应用进行破坏，或者是阻止木马盗取系统应用数据。

点击【病毒查杀】>【应用加固】，进入应用加固设置，如图所示。

图 8-15

可设置项包括：

发现威胁：选择【允许运行】，是继续让威胁应用运行，选择【禁止运行】，让威胁应用立即停止运行。

处理方式：发现威胁后通知用户的方式，要么选【自动处理】，即不通知；要么选【通知我】，即以弹窗的形式提醒用户威胁。

拦截日志：勾选【记录拦截日志】后，在日志中心将产生应用加固的日志信息。否则没有应用加固拦截日志。

启动弹框：勾选【启动时弹出软件保护框】，在计算机启动时弹出软件对计算机的保护信息。

8.2 上网防护

上网防护设置项主要有上网防护、白名单、广告过滤等功能的设置项。

8.2.1 上网防护

上网防护设置项对拦截恶意木马网址、拦截恶意下载、防黑客攻击、拦截跨站脚本攻击、搜索引擎结果检查和广告过滤等功能进行设置。

点击【上网防护】>【上网防护】，进入上网防护设置，如图所示。

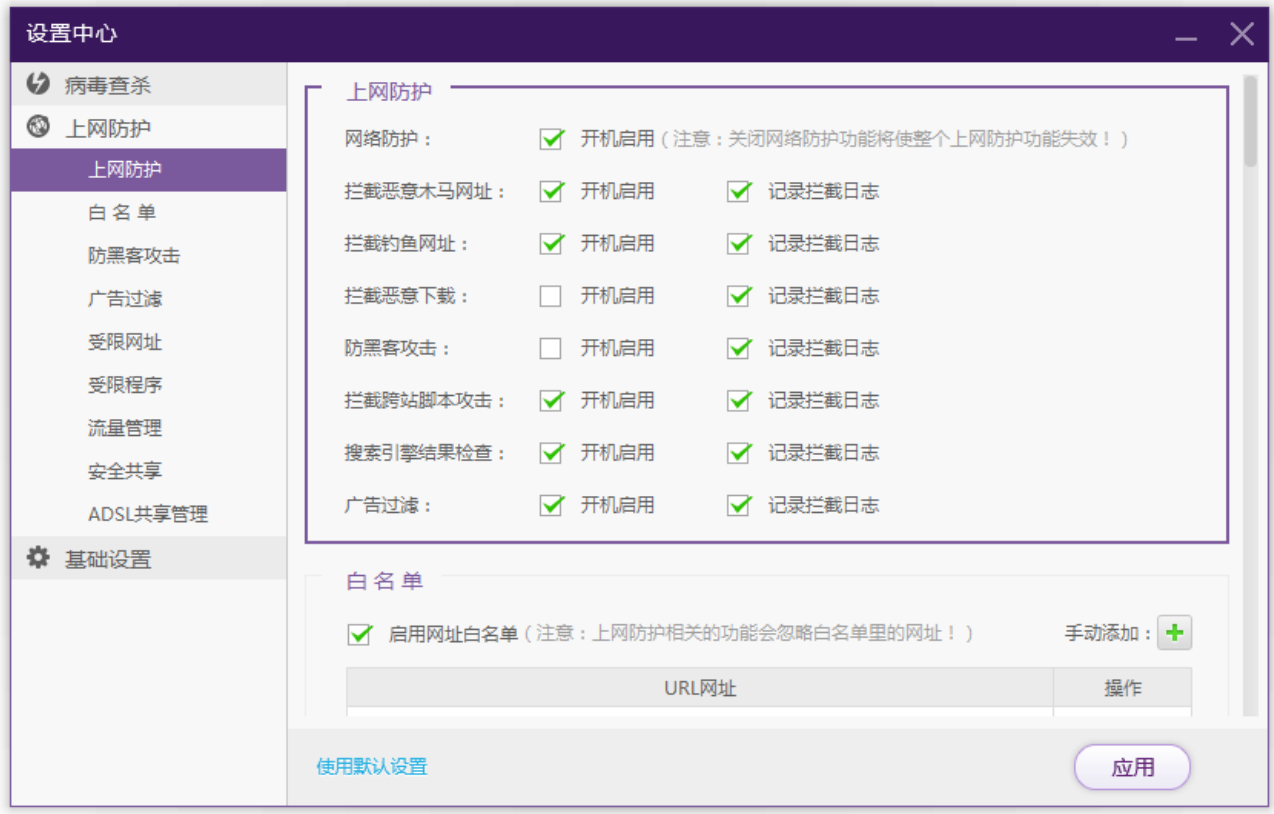


图 8-16

要使上网防护功能生效，必须勾选上网防护【开机启用】，然后请用户按照环境需要勾选相应的功能是否【开机启用】，还可以相应勾选【记录拦截日志】。

8.2.2 白名单

白名单功能作用于整个上网防护功能，只要在白名单里的网址，均被上网防护忽略，不会拦截。

点击【上网防护】>【白名单】，进入白名单设置，如图所示。

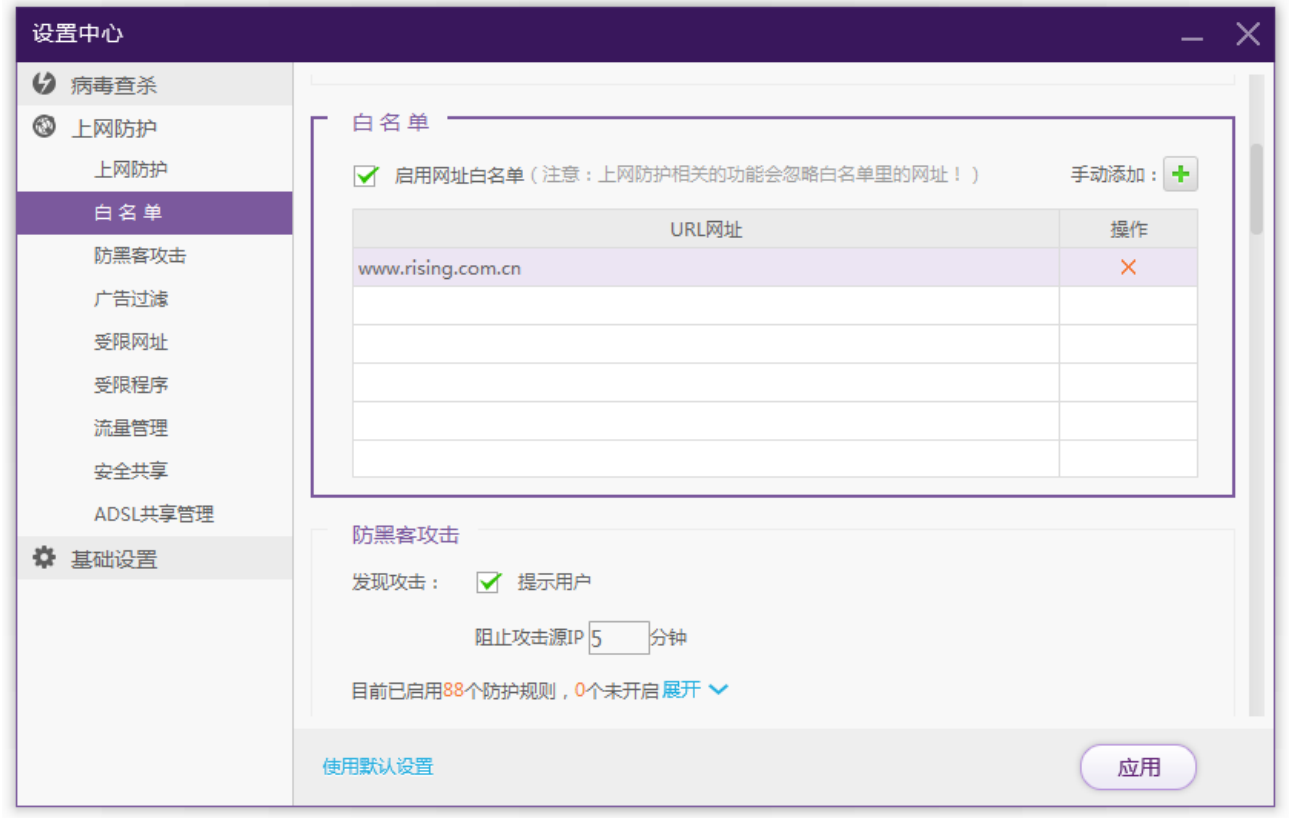


图 8-17

勾选【启用网址白名单】后，白名单功能才能在计算机启动时生效。点击手动添加后的，在下方新增的输入框中输入网址，如：www.rising.com.cn。点击操作栏的，可以删除白名单列表中的网址。

8.2.3 防黑客攻击

防黑客攻击设置对黑客攻击的提示，以及启用相关的防护规则。

点击【上网防护】>【防黑客攻击】，进入防黑客攻击设置，如图所示。

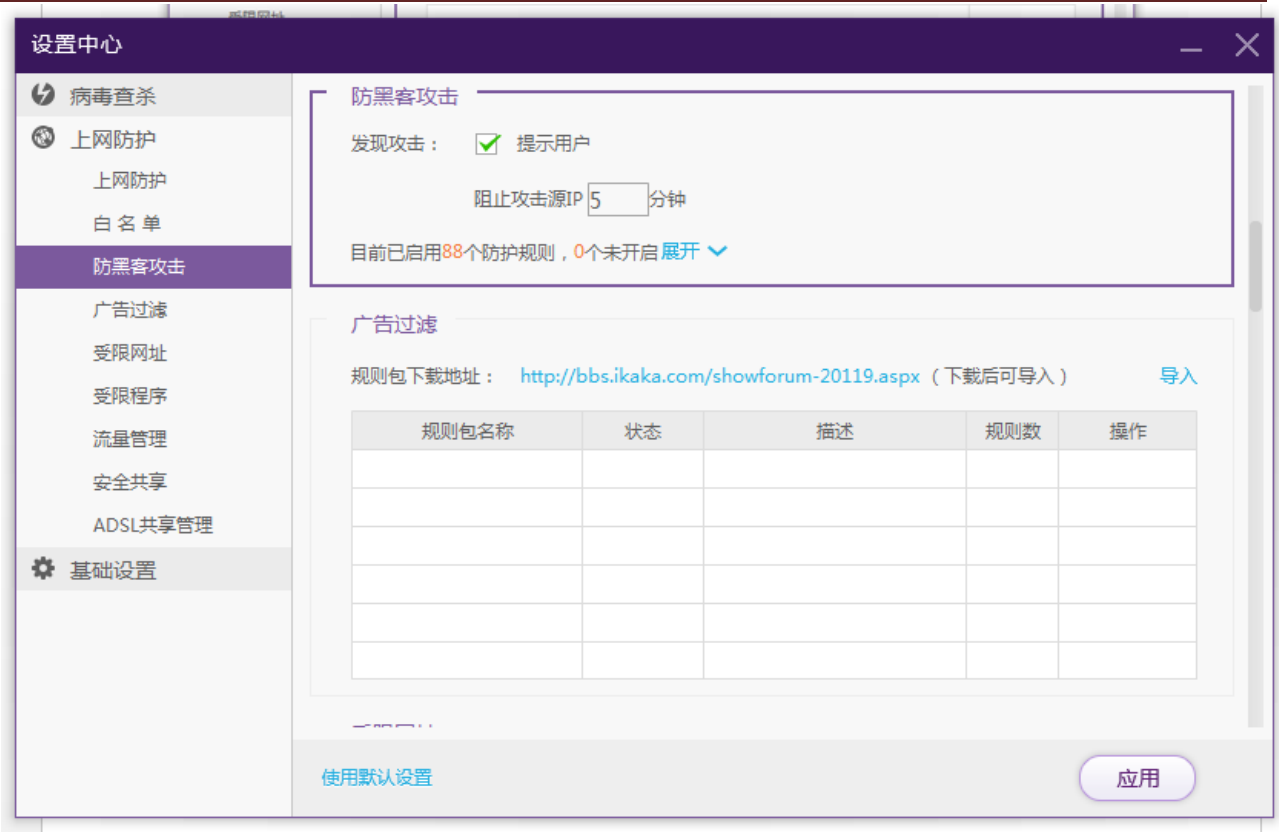


图 8-18

发现攻击：勾选【提示用户】，发现攻击时会提示用户，并按照用户设置的【阻止攻击源 IP】的时间，对攻击源 IP 地址进行阻止。

点击展开，出现如下图所示规则列表。

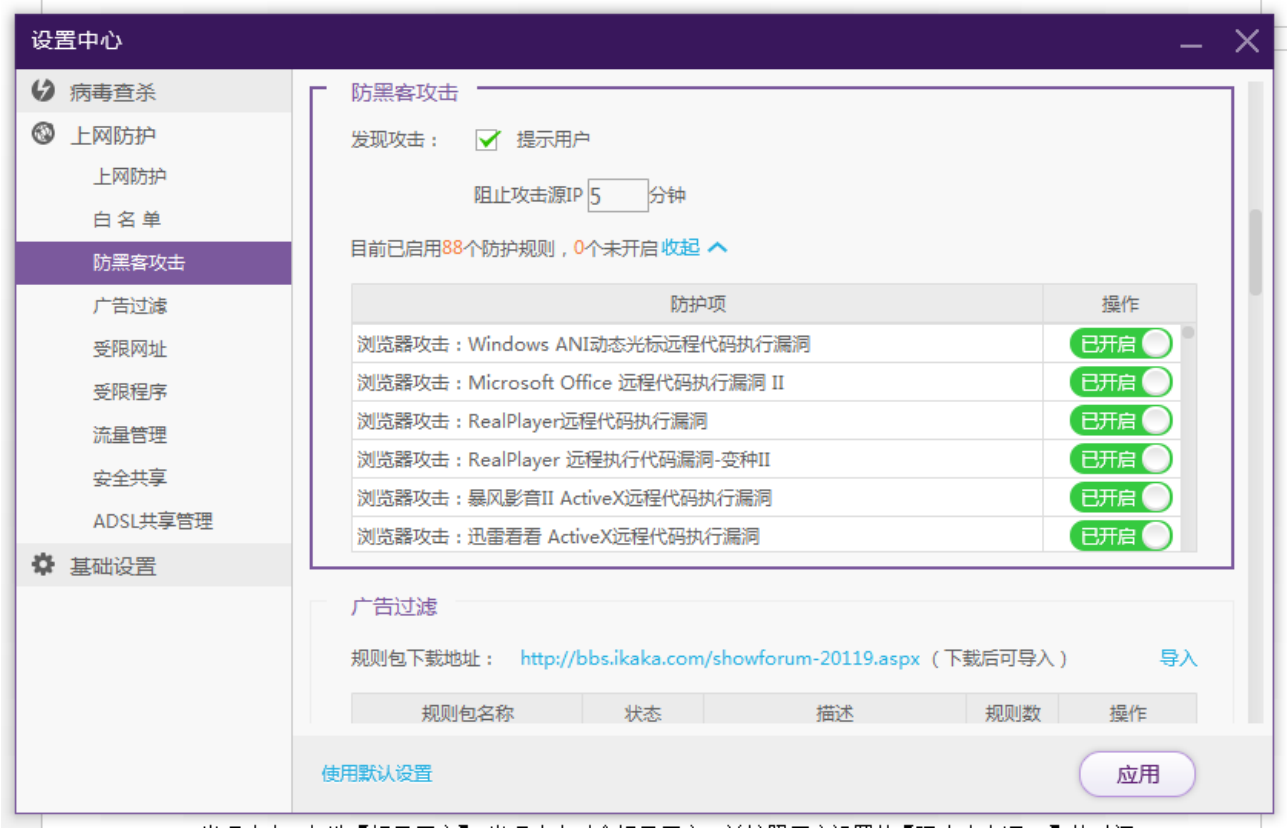


图 8-19

列表左侧是防护规则的名称，右侧是防护规则的启用开关，开关处于 

时，表示该防护规则启用；开关处于 

时，表示该防护规则停用。用鼠标向下拉滚动条，可以看到更多的防护规则，请用户根据实际需求进行开启和关闭，如不了解规则内容，请直接使用默认的设置。

8.2.4 广告过滤

广告过滤的设置可以从瑞星卡卡社区下载过滤规则包，然后导入过滤规则。

点击【上网防护】>【广告过滤】，进入广告过滤设置，如图所示。

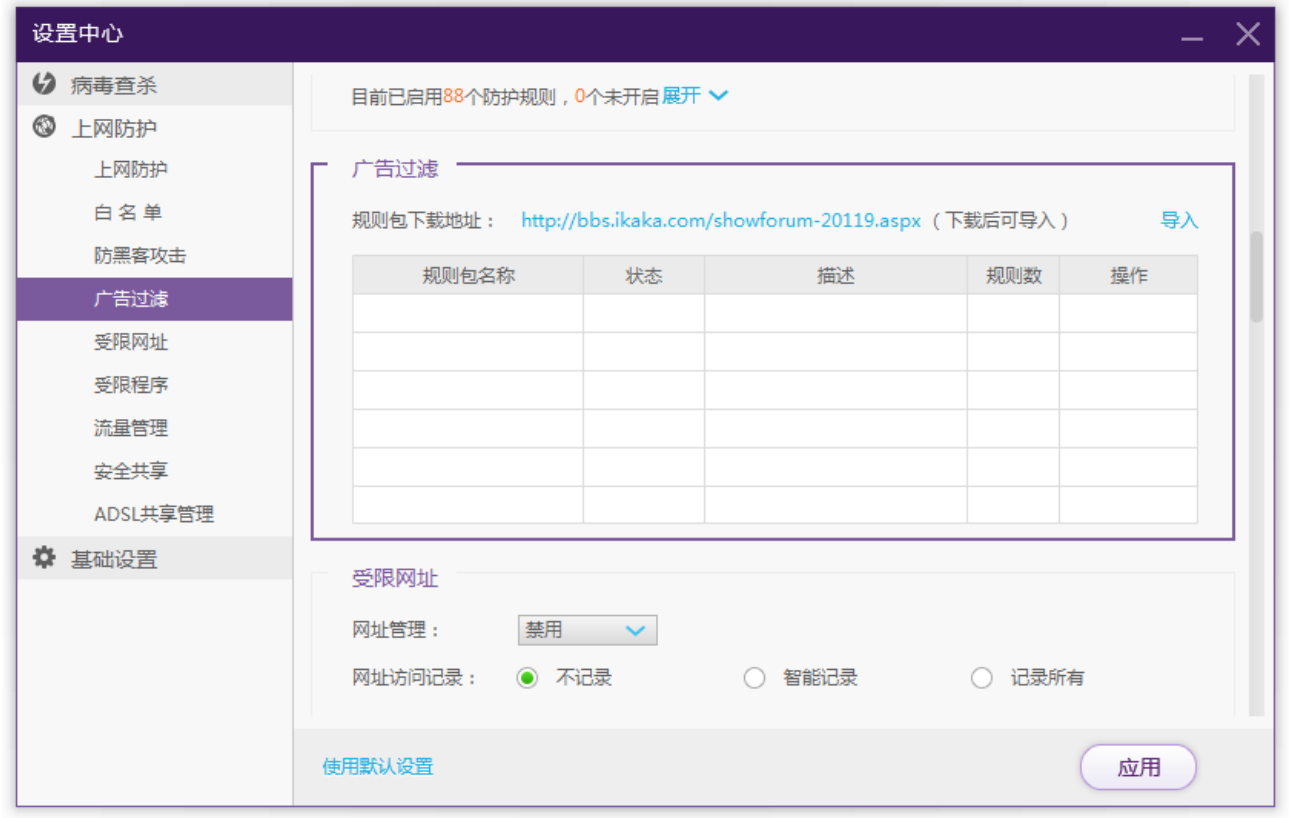


图 8-20

点击规则包下载地址后的链接，浏览器自动打开规则所在网页，请用户在浏览器下载相应的过滤包。下载后解压文件，然后点击 导入，选择解压后文件。在列表中就会显示导入的规则信息，如规则包名称、状态、描述、规则数和操作。如图所示。

图 8-21

在状态一栏，点击开关开启或者关闭规则，在操作一栏点击删除规则，点击导出已有规则。

8.2.5 受限网址

受限网址用于企业内部网络访问管理，对某些网站实施管制，提高员工工作效率。可以设置受限时段，可以设置拦截提示，还可以设置拦截后跳转到指定网址。

点击【上网防护】>【受限网址】，进入受限网址设置，如图所示。

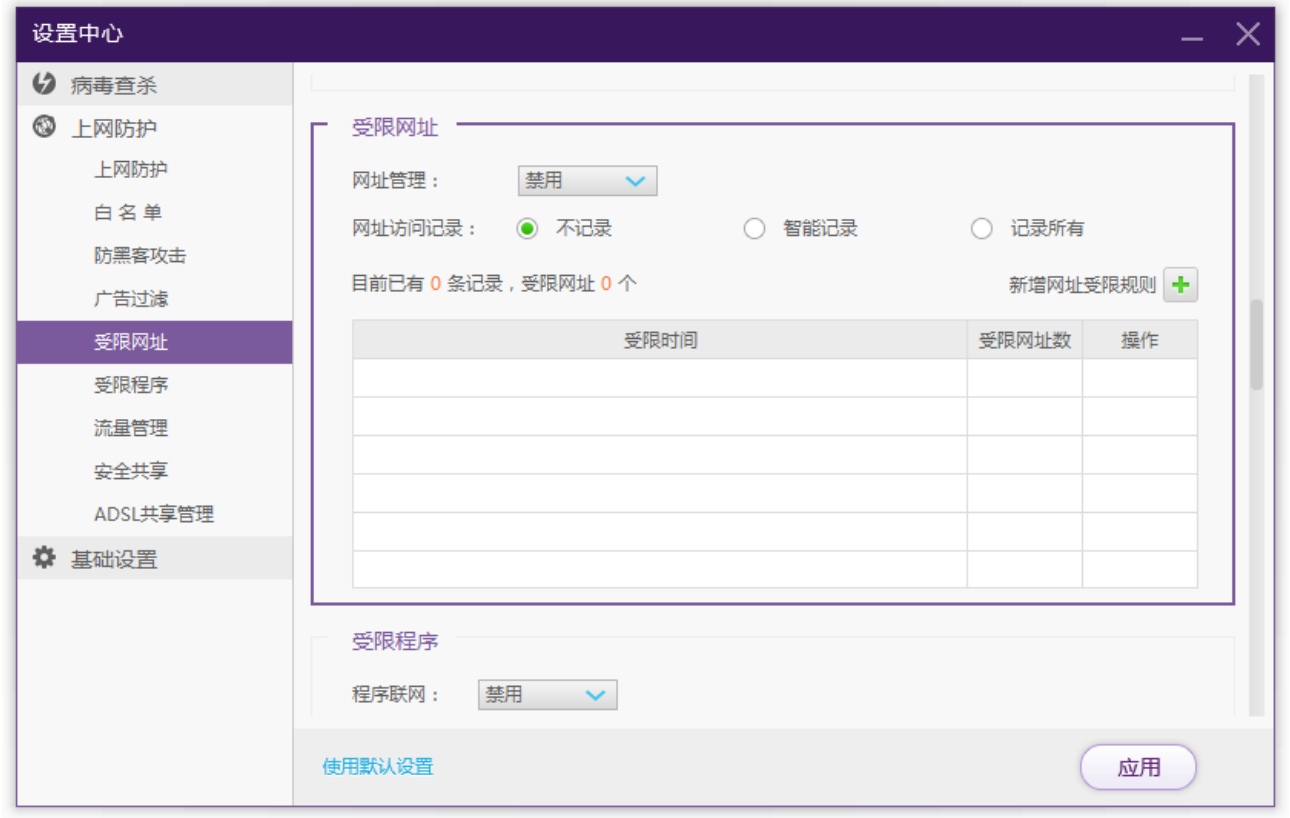


图 8-22

在网址管理选择【开启】，受限网址功能才能生效。然后选择网址访问记录方式：不记录、智能记录或者记录所有。

在新增网址受限规则处点击  ，添加受限规则。在弹出的界面进行设置。如图所示。

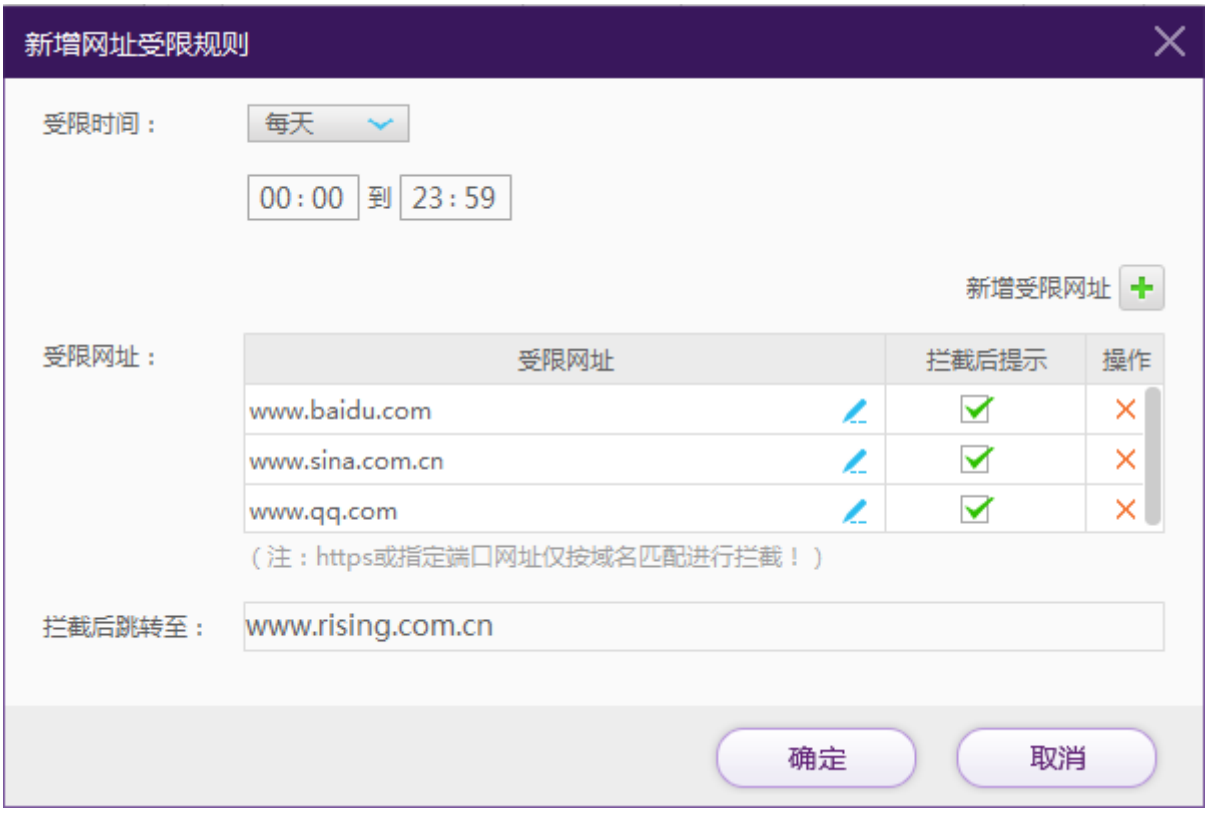


图 8-23

受限时间：可以选择每天、每周和日期。填写受限时间（00:00-23:59）。

新增受限网址：点击新增受限网址后的，在受限网址列表中填写受限网址，勾选拦截后提示。

拦截后跳转至：对于需要在拦截受限网址并跳转的，可以设置跳转目标网址，例如这里设置为 www.rising.com.cn。

对于已经添加的网址，可以通过点击操作中的进行删除。

如图所示，访问受限网站被拦截并跳转到指定网站，同时在右下角弹出网页浏览事件弹窗，显示被拦截的网址。

图 8-24

在浏览器将提示如图所示：

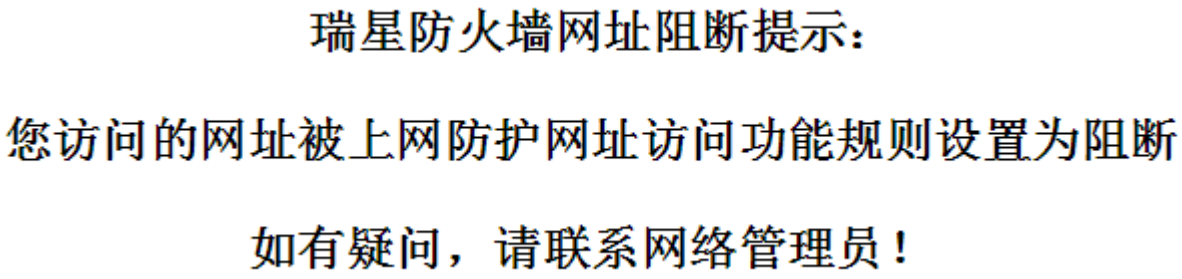


图 8-25

8.2.6 受限程序

受限程序用于阻止非法程序运行，有效杜绝病毒通过不明程序传播。

点击【上网防护】>【受限程序】，进入受限程序设置，如图所示。

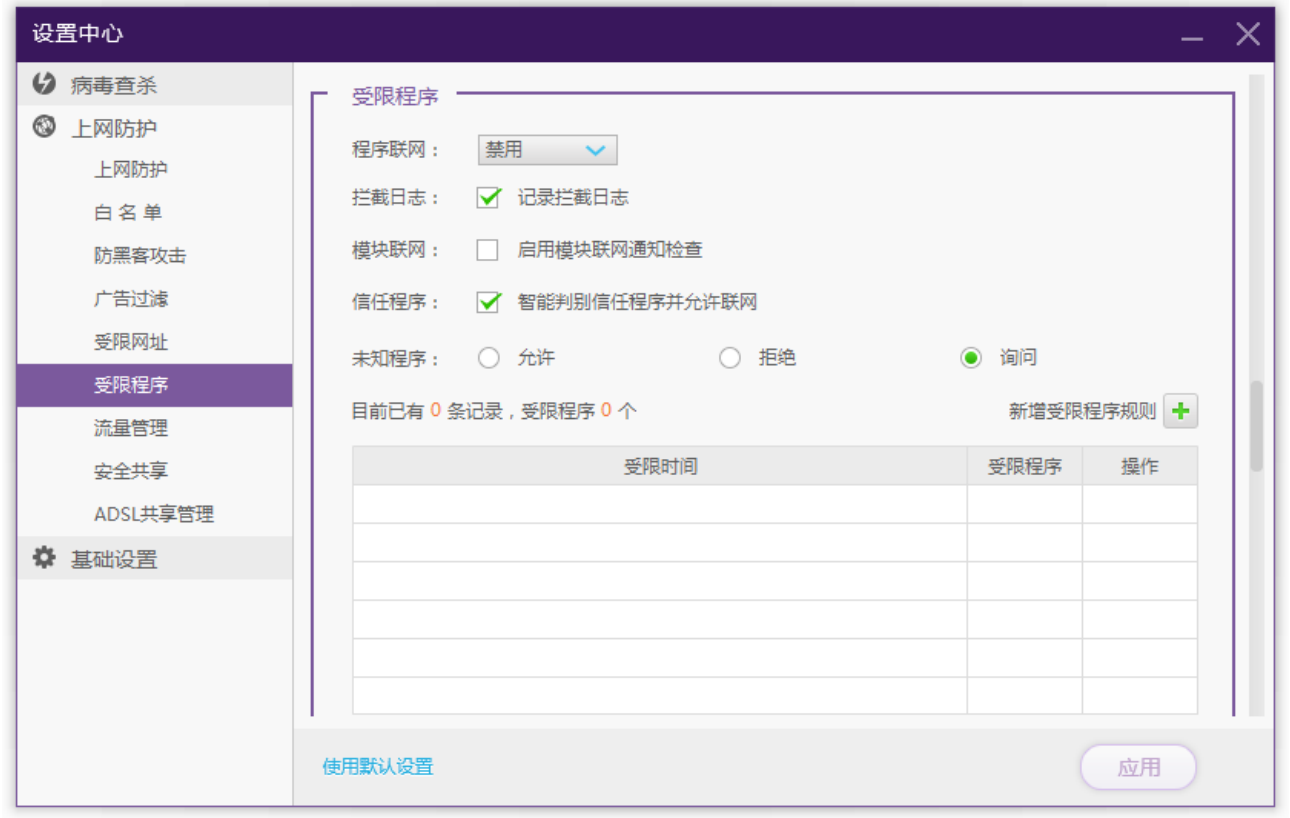


图 8-26

程序联网选择【启用】。勾选【记录拦截日志】。受限程序功能生效并记录拦截日志。

模块联网：勾选【启用模块联网通知检查】，功能生效。

信任程序：勾选【智能判别信任程序并允许联网】，软件将对可信程序一律放行，除非用户自行设置拦截。

未知程序：对于未知的程序，可以选择允许、拒绝或者询问。选择允许，每次有未知程序有联网请求时都一律放行；选择拒绝，每次有未知程序有联网请求都一律禁止访问网络；选择询问，每次有未知程序有联网请求都要询问，如图所示。

图 8-27

选择【本次放行】时，本次允许该程序联网，下次该程序再次发起联网请求，依然会询问。

选择【本次拒绝】时，本次拒绝该程序联网，下次该程序再次发起联网请求，依然会询问。

选择【总是放行】时，从此以后，该程序发起的联网请求一律放行。

选择【总是拒绝】时，从此以后，该程序发起的联网请求一律拒绝。

8.2.7 流量管理

流量管理是对流量统计功能的设置，可以设置流量监控的开启和关闭，可设置记录流量的时间间隔。

点击【上网防护】>【流量管理】，进入流量管理设置，如图所示。

图 8-28

选择【开启】流量监控，然后在记录流量一栏设置时间间隔，单位为分钟。

8.2.8 安全共享

安全共享功能的设置，是对监控共享资源、系统和访问权限的设置

点击【上网防护】>【安全共享】，进入安全共享设置，如图所示。

图 8-29

系统共享：勾选【关闭默认共享 C$/D$/E$】，软件将对计算机默认的共享区域（如 C 盘、D 盘、E 盘等）进行关闭。勾选【关闭远程管理 ADMIN$】，将关闭 ADMIN 从远程登录计算机的功能。

共享资源：勾选【记录本机共享文件夹】，将对本机已经共享的文件和文件夹进行记录。

共享访问：勾选【记录日志】后，共享访问的操作和访问信息记录日志。

访问控制：选择启用访问控制功能，开启对共享文件的访问控制，访问规则生效。

拒绝访问：勾选【提示用户】，当由访问共享资源遭到拒绝的事件发生时，弹窗提醒用户有非法用户试图访问共享资源。

不在规则列表 IP：可以选择【允许访问】或者【禁止访问】。

新增访问 IP 或 IP 段：点击新增访问 IP 或 IP 段后的  ，选择 IP 或者 IP 段，这里以 IP 端为例。在新建的列表中填入 IP 段。然后动作选择【允许】或者【禁止】，选择【允许】，则该段 IP 内的主机能访问共享资源；选择【禁止】，则该段 IP 内的主机不能访问共享资源。如图所示。

图 8-30

还可以对已经存在的 IP 段列表进行编辑和修改，如果要删除某段 IP 地址，请点击操作中的 。

8.2.9 ADSL 共享管理

ADSL 共享设置，可以控制带宽，前提是需要勾选【启用】ADSL 共享。

点击【上网防护】>【ADSL】，进入 ADSL 设置，如图所示。

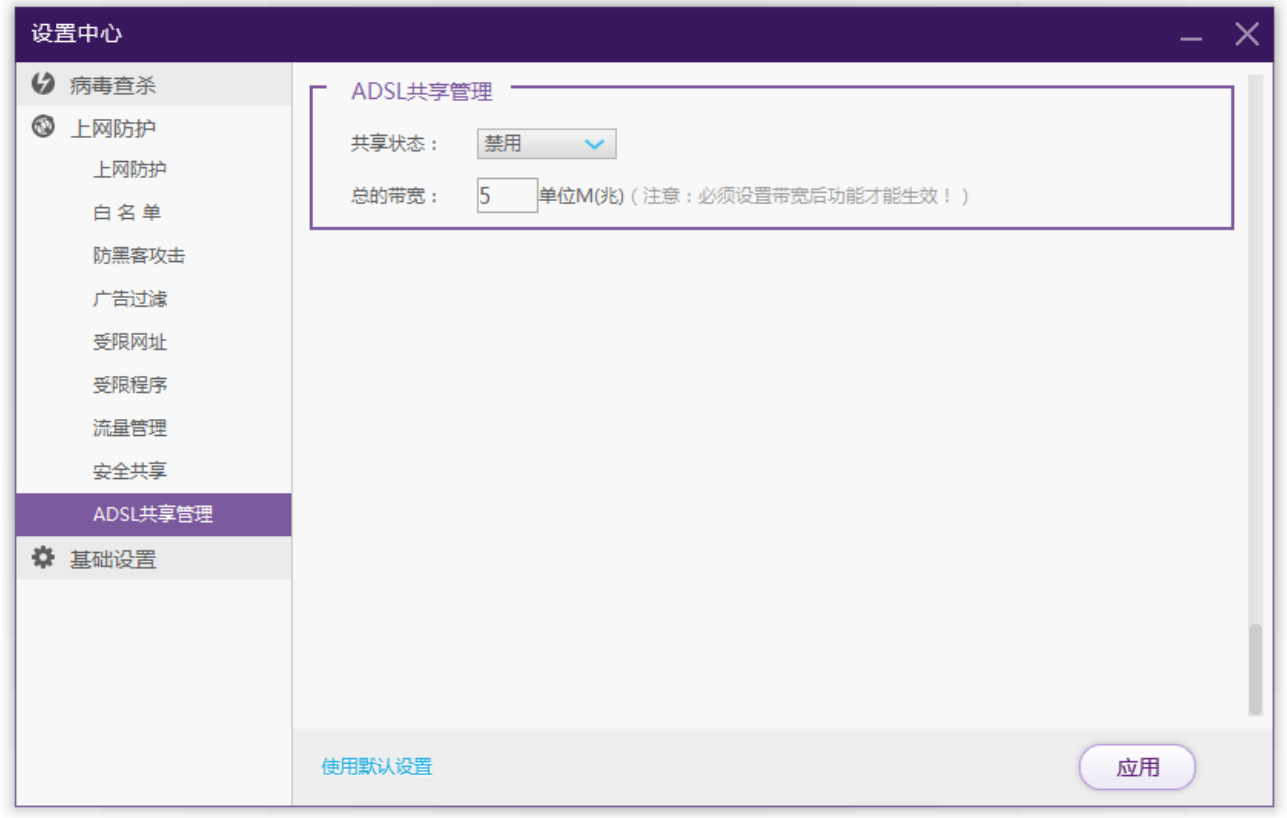


图 8-31

共享状态：选择【开启】。

总的带宽：设置实际需要的数字，单位是 M。

点击【应用】，使所有设置保存。

8.3 基础设置

基础设置包括管理员身份、托盘设置和软件更新设置。

8.3.1 管理员身份

管理员身份可以设置一个管理员密码，这是作为管理员的唯一身份标识，特殊操作时所用，密码锁定后不可修改。如图所示。

图 8-32

点击【设置一个】，在弹出的管理员密码设置窗口中填写密码和重复密码。

图 8-33

8.3.2 托盘设置

托盘设置中，勾选【隐藏任务栏托盘图标】后，在任务栏将不会再显示托盘图标。

图 8-34

去掉勾选后，任务栏将重新显示图标 

8.3.3 软件更新

软件更新设置包括升级模式、升级内容和代理设置。如图所示。

图 8-35

升级模式：可以设置瑞星安全云终端软件的升级模式，分【自动升级】和【手动升级】。

升级内容：可以选择【升级所有】或者【仅升级病毒库】。其中，升级所有组件，可以勾选【恶意网址库即时生效】，那么升级后，恶意网址库立即就生效了（需要重新连接网络）。

在代理设置中，可以设置直接连接、使用浏览器设置、使用代理设置三种方式，如图所示。

图 8-36

选择好相应的代理设置后，在下面的地址、端口、账号、密码栏分别设置好参数。

图 8-37

9 日志中心

日志中心包括病毒查杀日志、上网防护日志和基础日志。点击主界面右上角【菜单】，在选择【日志】，进入日志中心。

9.1 病毒查杀

病毒查杀日志包含病毒查杀详情日志、扫描事件日志、系统加固日志、应用加固日志和隔离区日志。

9.1.1 病毒详情

点击【病毒查杀】>【病毒详情】，进入病毒详情日志界面。如图所示。

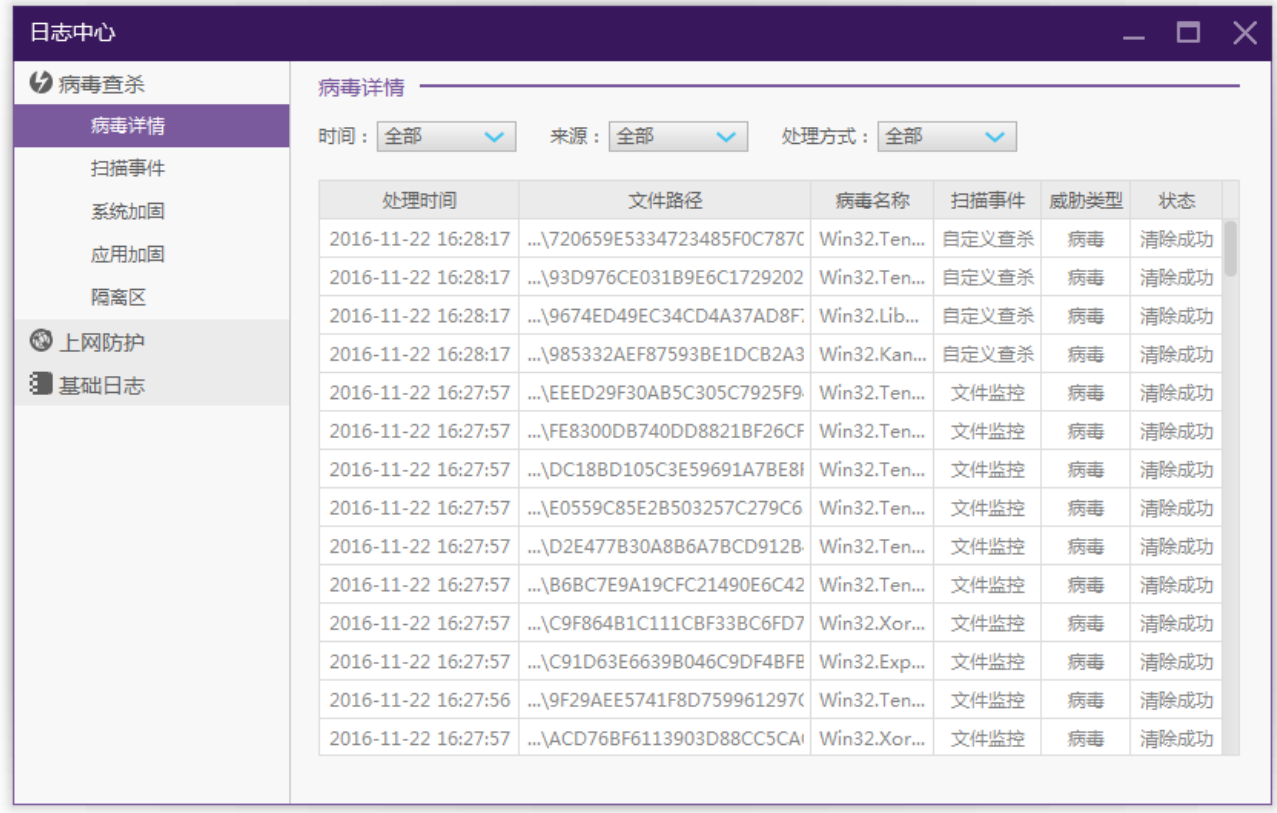


图 9-1

在详情日志界面内，可以进行过滤筛选，选择时间、来源和处理方式，显示不同的日志信息。

在日志信息列表中，从左往右依次是：处理时间、文件路径、病毒名称、扫描时间、威胁类型和状态。

9.1.2 扫描事件

扫描事件日志，记录了扫描发生的时间和详细情况。

点击【病毒查杀】>【扫描事件】，进入病毒详情日志界面。如图所示。

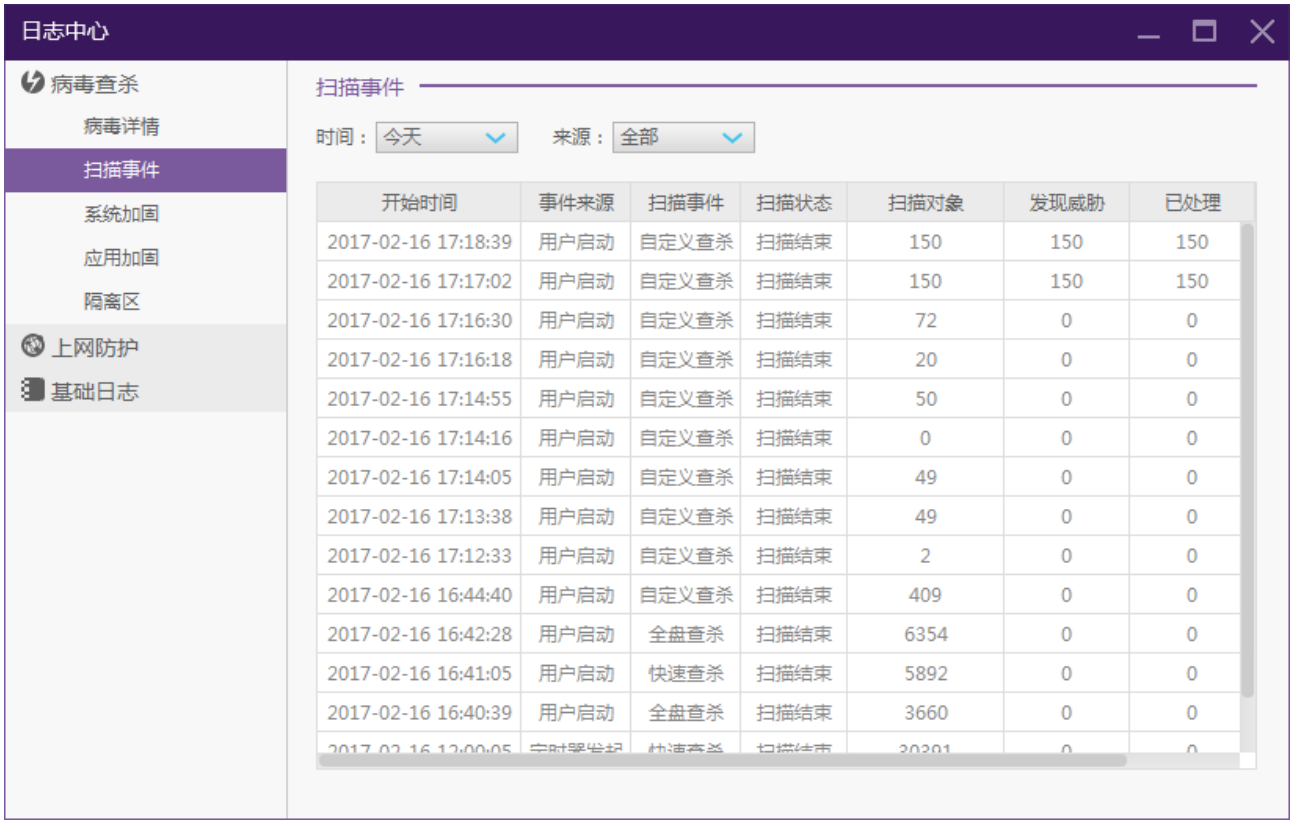


图 9-2

可以通过时间和来源筛选扫描事件。在扫描事件日志列表中，从左到右的项目分别是：开始时间、事件来源、扫描事件、扫描状态、扫描对象、发现威胁和已处理。

开始时间：指扫描开始的时间。

事件来源：指事件产生的方式，可能是用户启动，也可能是软件被规则触发等。

扫描事件：指扫描时选择的扫描模式，可能是快速查杀、全盘查杀或者自定义查杀中的一种。

扫描状态：指启动的扫描所处状态，处在运行中、已暂停或者扫描结束中的一种。

扫描对象：指该次总共扫描的文件数量。

发现威胁：指在该次扫描中，发现病毒木马等威胁的数量。

已处理：指在发现的威胁中已经被删除或隔离的数量。

9.1.3 系统加固

系统加固日志记录了拦截的威胁日志信息。

点击【病毒查杀】>【系统加固】，进入系统加固日志界面。

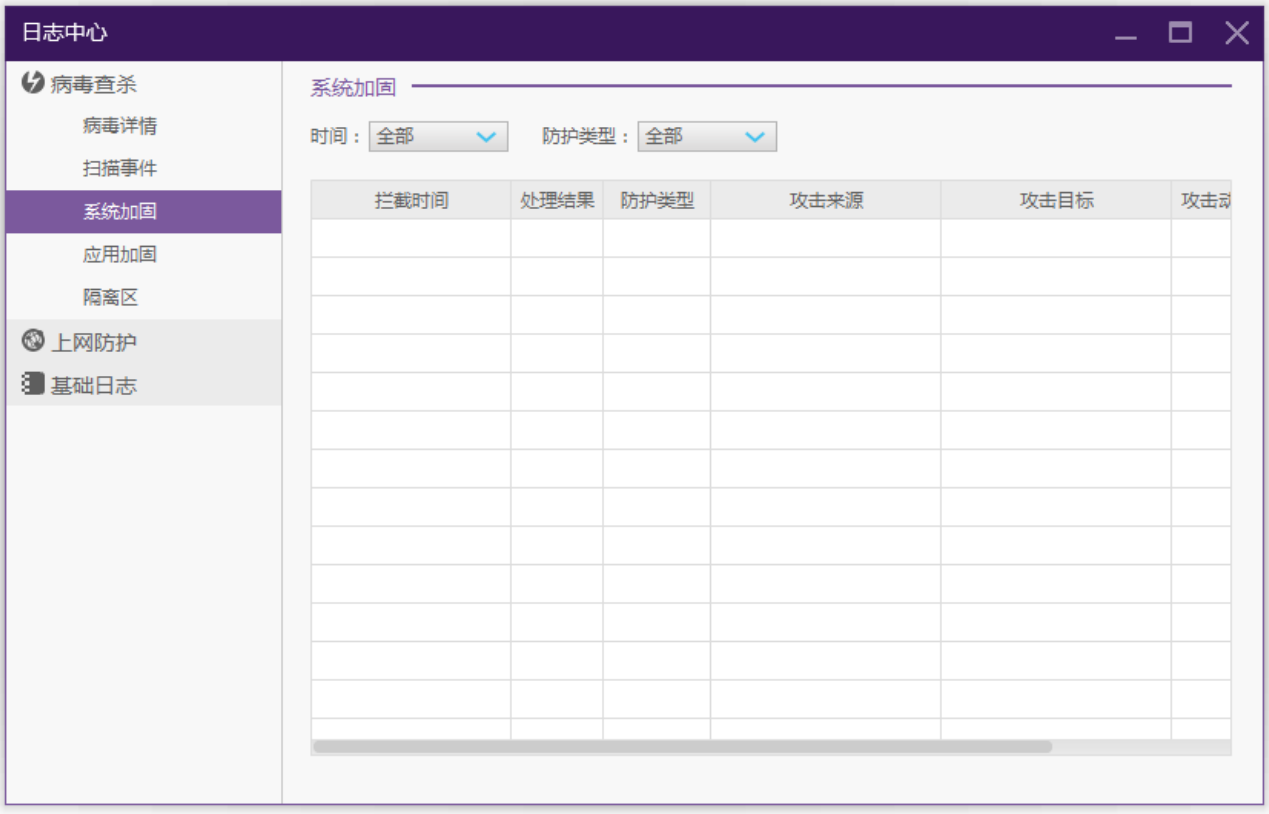


图 9-3

9.1.4 应用加固

应用加固日志记录触犯规则的应用及其记录。

点击【病毒查杀】>【应用加固】，进入应用加固日志界面。

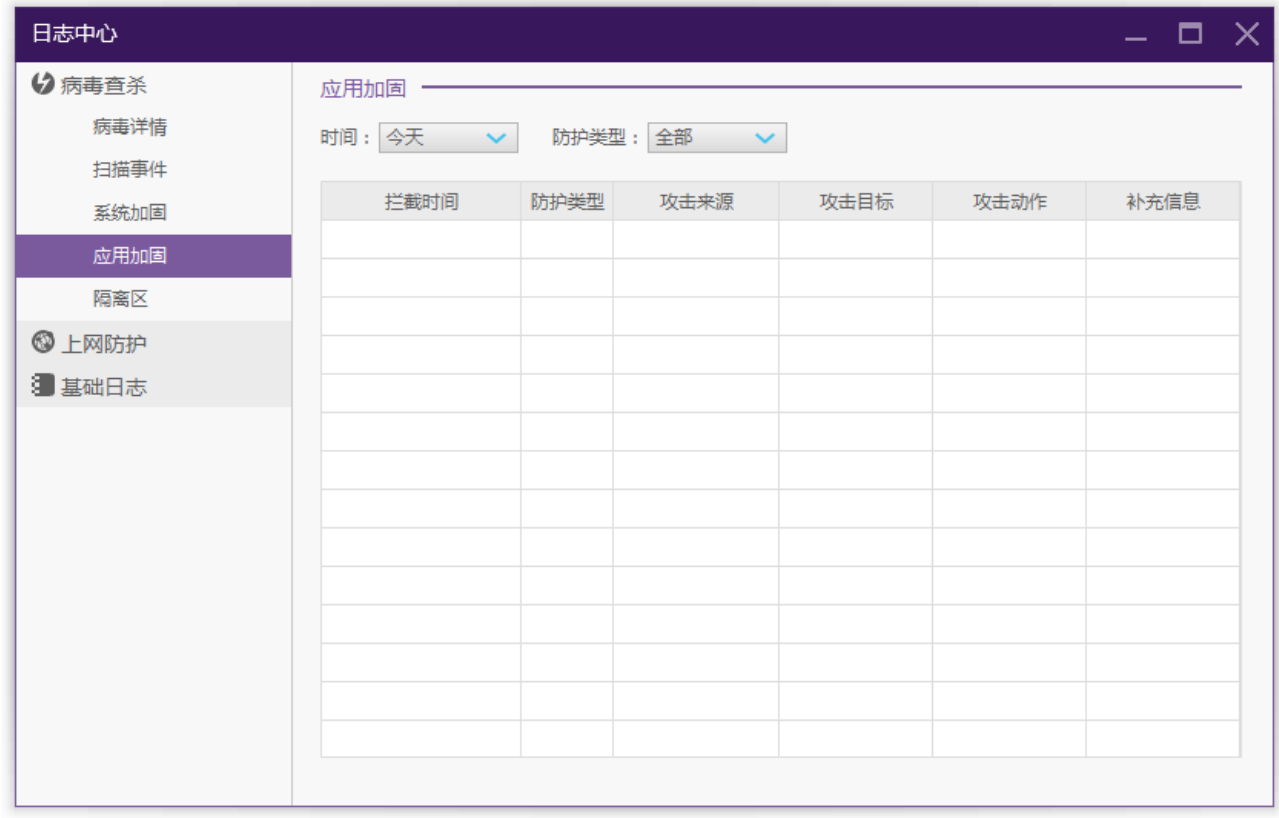


图 9-4

9.1.5 隔离区

瑞星安全云终端软件隔离区用来实现病毒文件的隔离和处理功能，软件将查杀的病毒放入隔离区，既可以保留病毒源文件，又可以随时进行恢复文件而不被病毒感染。

隔离区日志显示了被隔离的文件和病毒信息。如图所示。

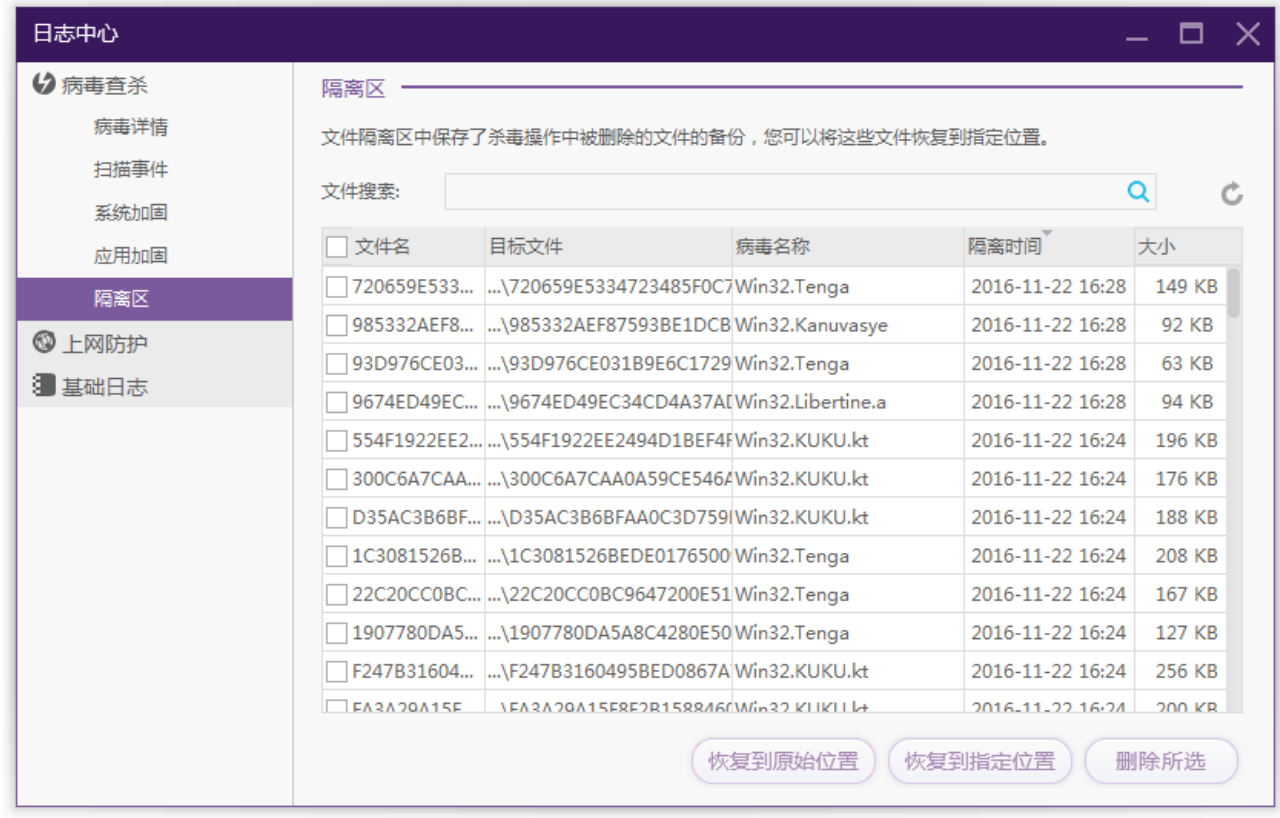


图 9-5

通过隔离区能够恢复备份文件，通过勾选需要恢复的文件，然后点击【恢复到原始位置】，则备份文件恢复到被删除前的位置；点击【恢复到指定位置】，并指定文件保存位置，文件被恢复到指定的位置；点击【删除所选】，则被勾选的备份文件会被永久性删除，请谨慎操作。

如果隔离区文件太多，可以通过上方的搜索栏进行文件搜索。

通过文件名进行排序，点击列表栏的表头【文件名】，文件名按照字母顺序排序；再次点击【文件名】，文件名按照字母的逆顺序排序。

同理点击【目标文件】，文件按照路径升序排列，再次点击【目标文件】，文件按照路径降序排列。

同理点击【病毒名称】、【隔离时间】和【大小】，都分别按照相应的升降顺序排列。

9.2 上网防护

上网防护记录了恶意网址、黑客攻击、广告过滤、网址访问、联网程序、共享访问和上网流量的日志信息。

9.2.1 恶意网址

恶意网址记录了被拦截的恶意网址信息。

点击【上网防护】>【恶意网址】，进入恶意网址日志界面。如图所示。

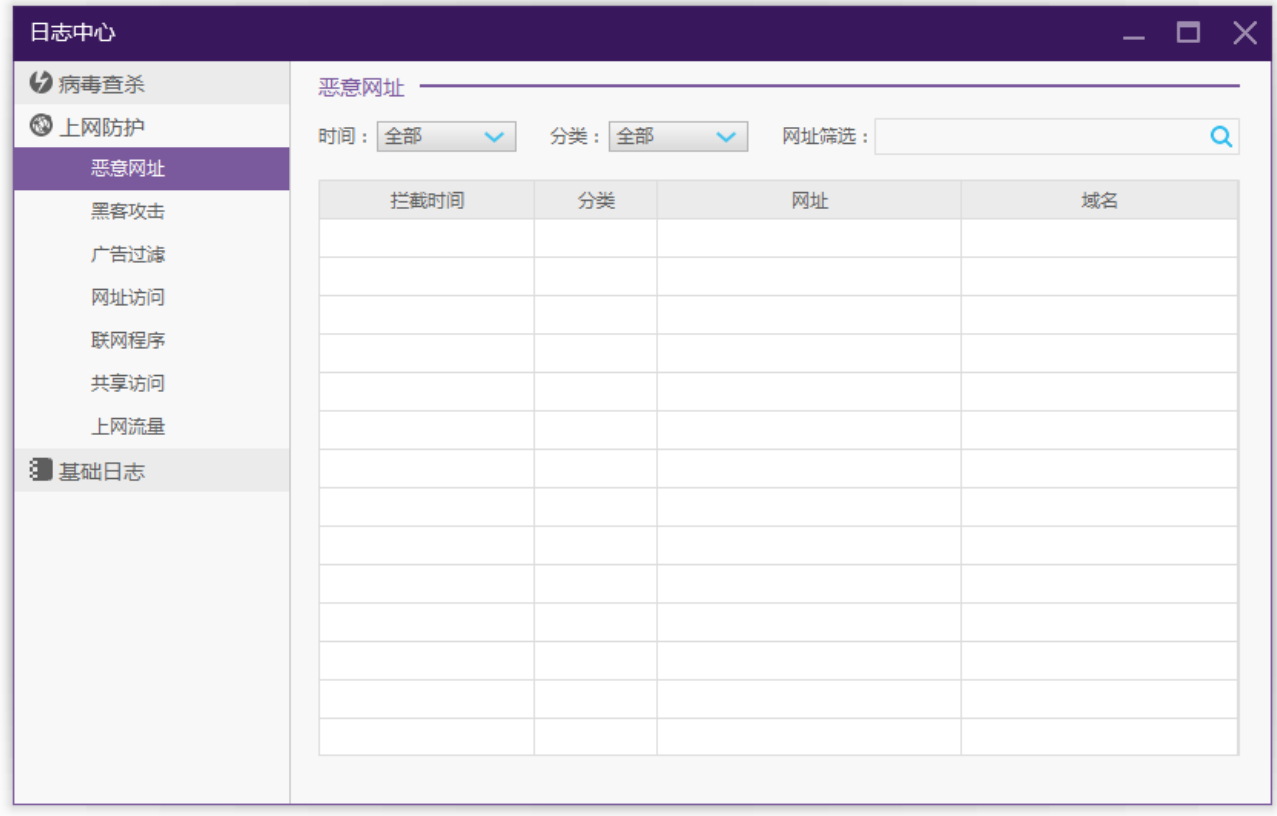


图 9-6

9.2.2 黑客攻击

黑客攻击日志记录了所有的黑客攻击行为，包括攻击的时间、攻击目标、黑客信息、攻击状态和拦截原因。

点击【上网防护】>【黑客攻击】，进入黑客攻击日志界面。如图所示。

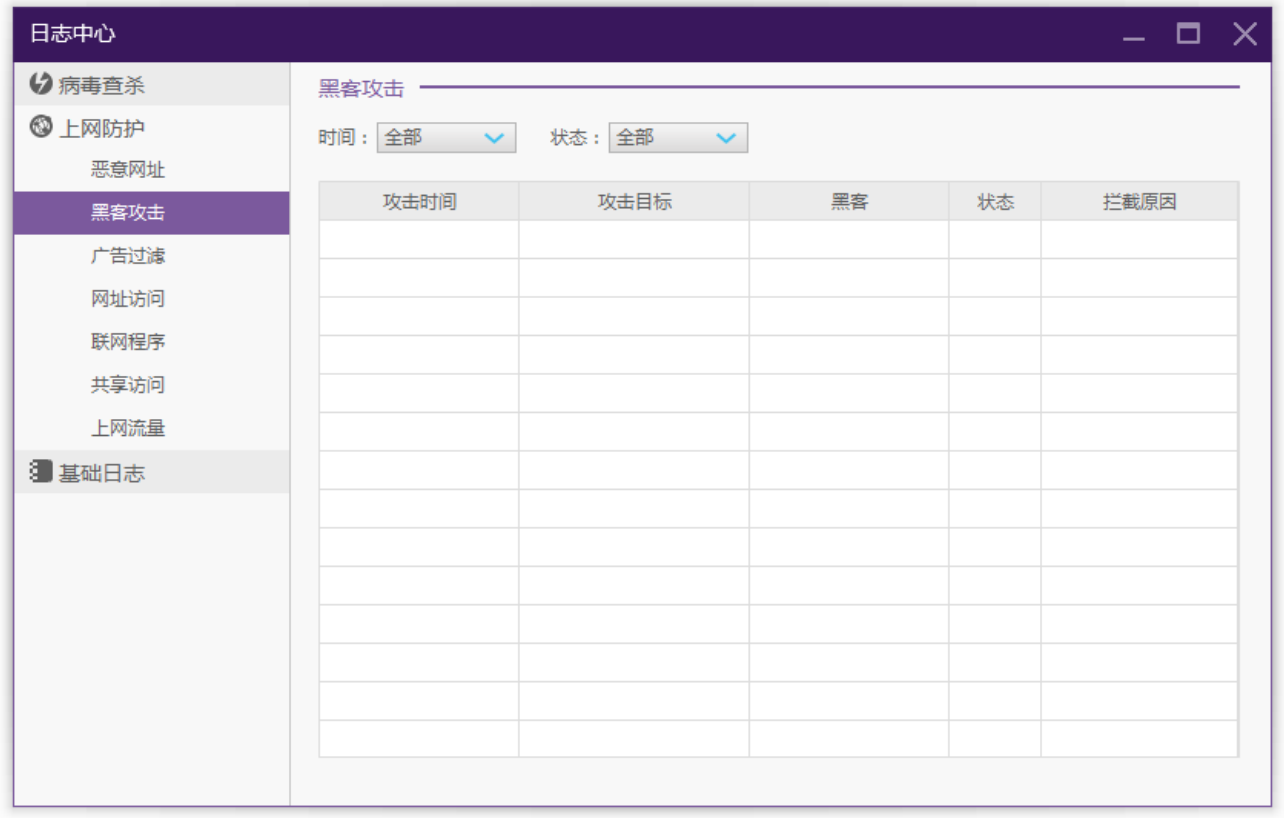


图 9-7

9.2.3 广告过滤

广告过滤日志记录了所有的广告拦截信息，包括拦截的时间、拦截的网址和拦截的域名，可为分析广告拦截规则提供样本。

点击【上网防护】>【广告过滤】，进入广告过滤日志界面。如图所示。

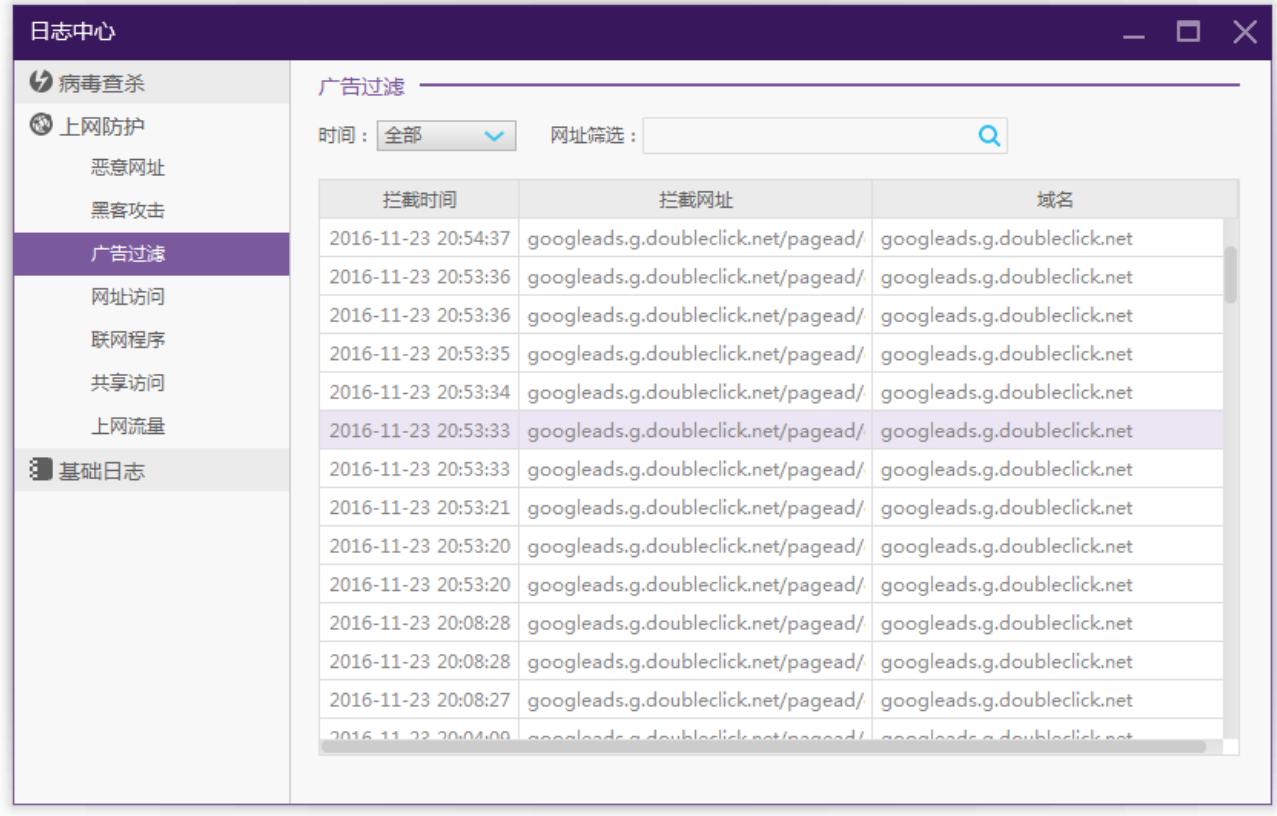


图 9-8

9.2.4 网址访问

网址访问日志记录的是关于所有网页访问记录，包括网址访问时间、网页标题、网站网址和访问时拦截状态。

点击【上网防护】>【网址访问】，进入网址访问日志界面。如图所示。

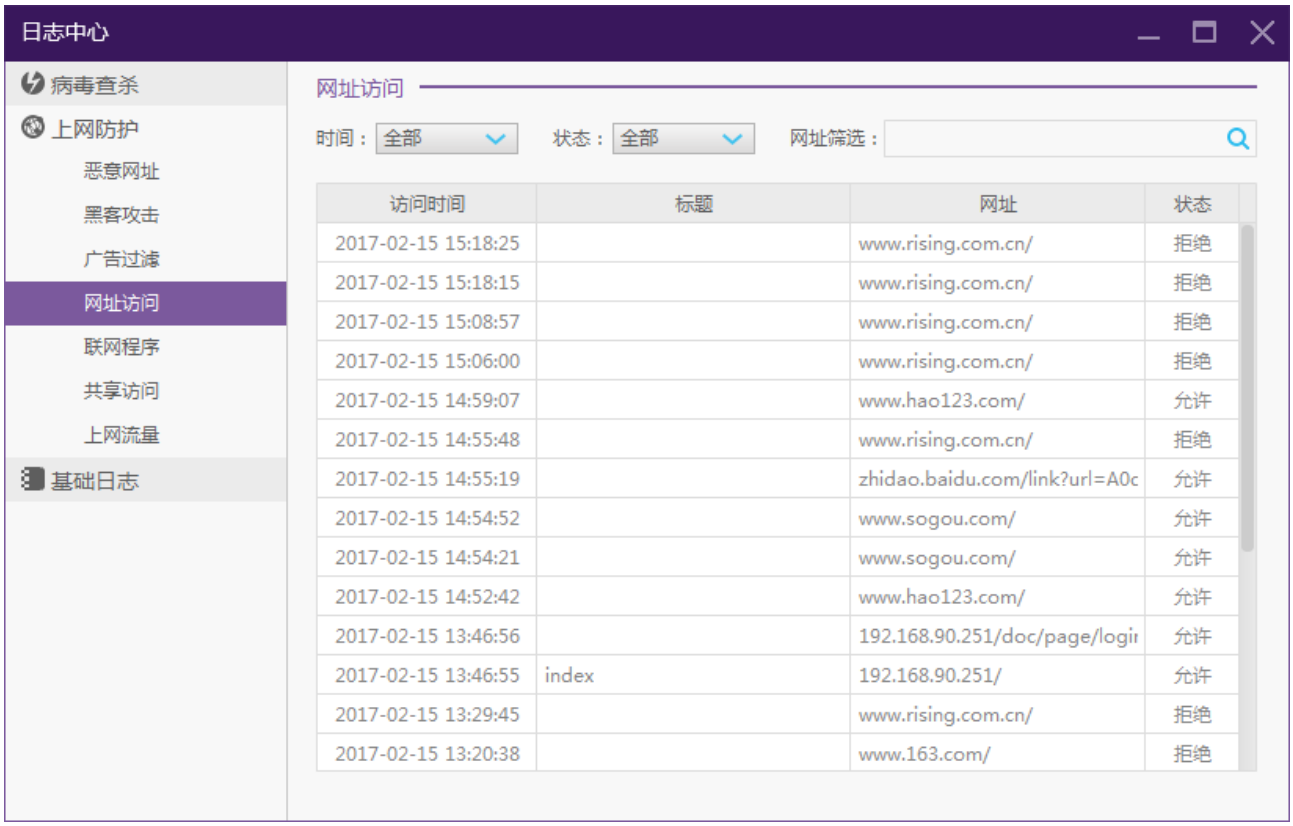


图 9-9

9.2.5 联网程序

联网程序日志记录了所有程序的联网信息，包括访问时间、程序名称、访问地址和本机对应的端口和地址。

点击【上网防护】>【联网程序】，进入联网程序日志界面。如图所示。

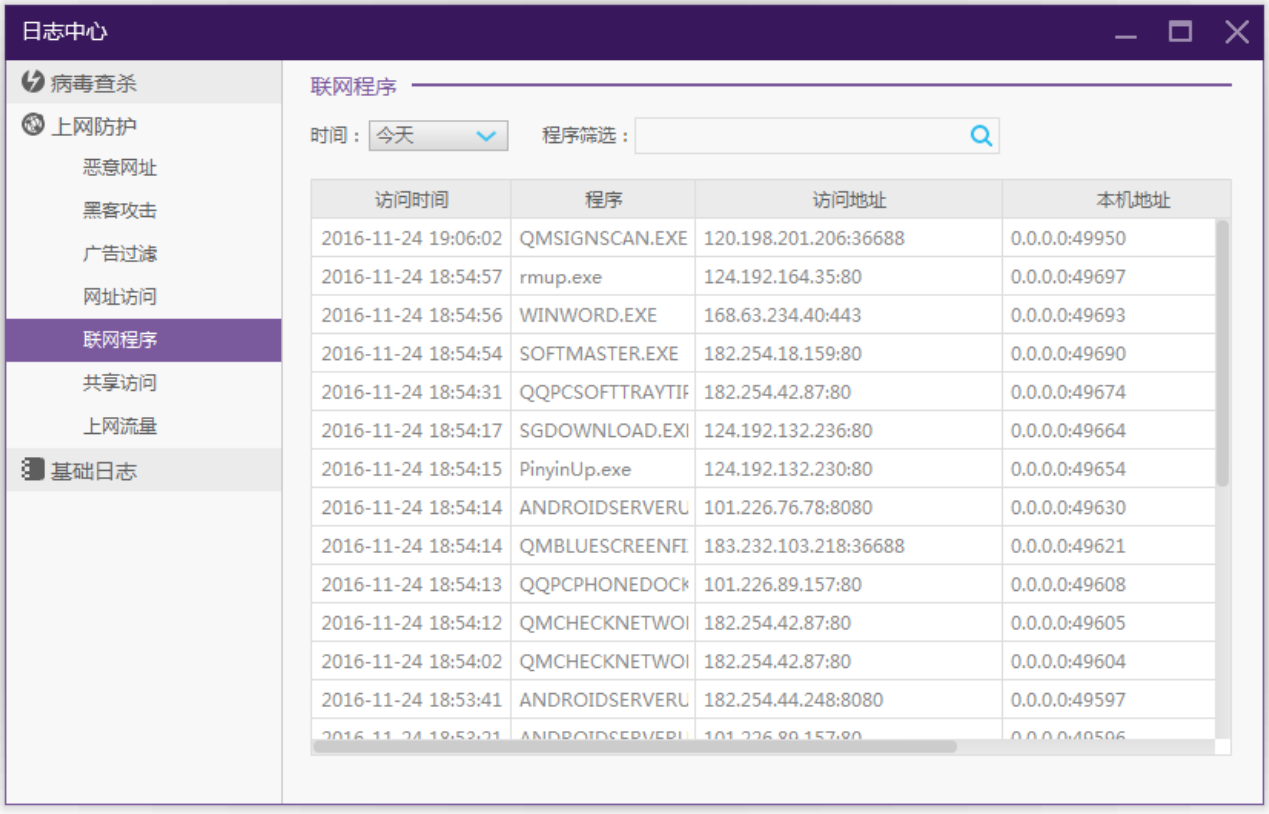


图 9-10

9.2.6 共享访问

共享访问日志记录了所有共享资源访问的记录，包括访问时间、访问者、操作和共享文件。

点击【上网防护】>【共享访问】，进入共享访问日志界面。如图所示。

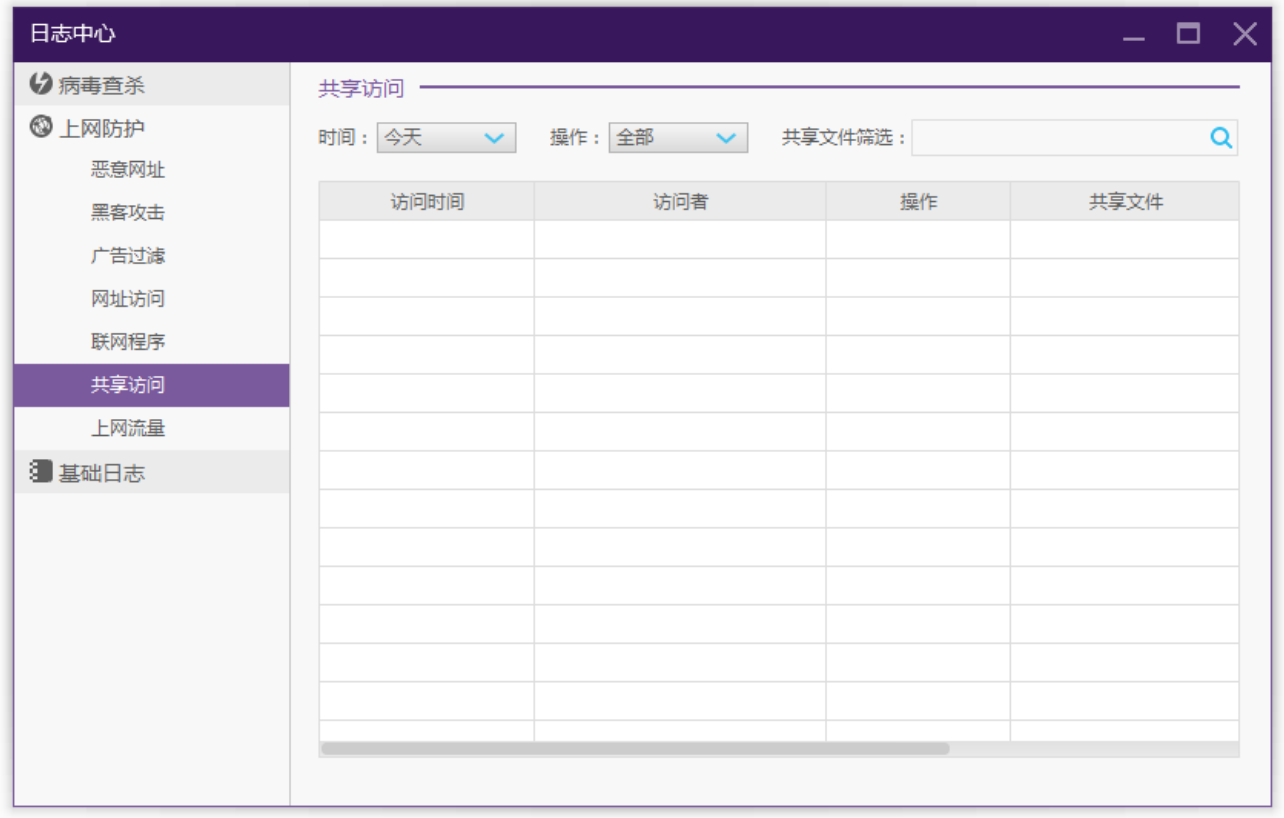
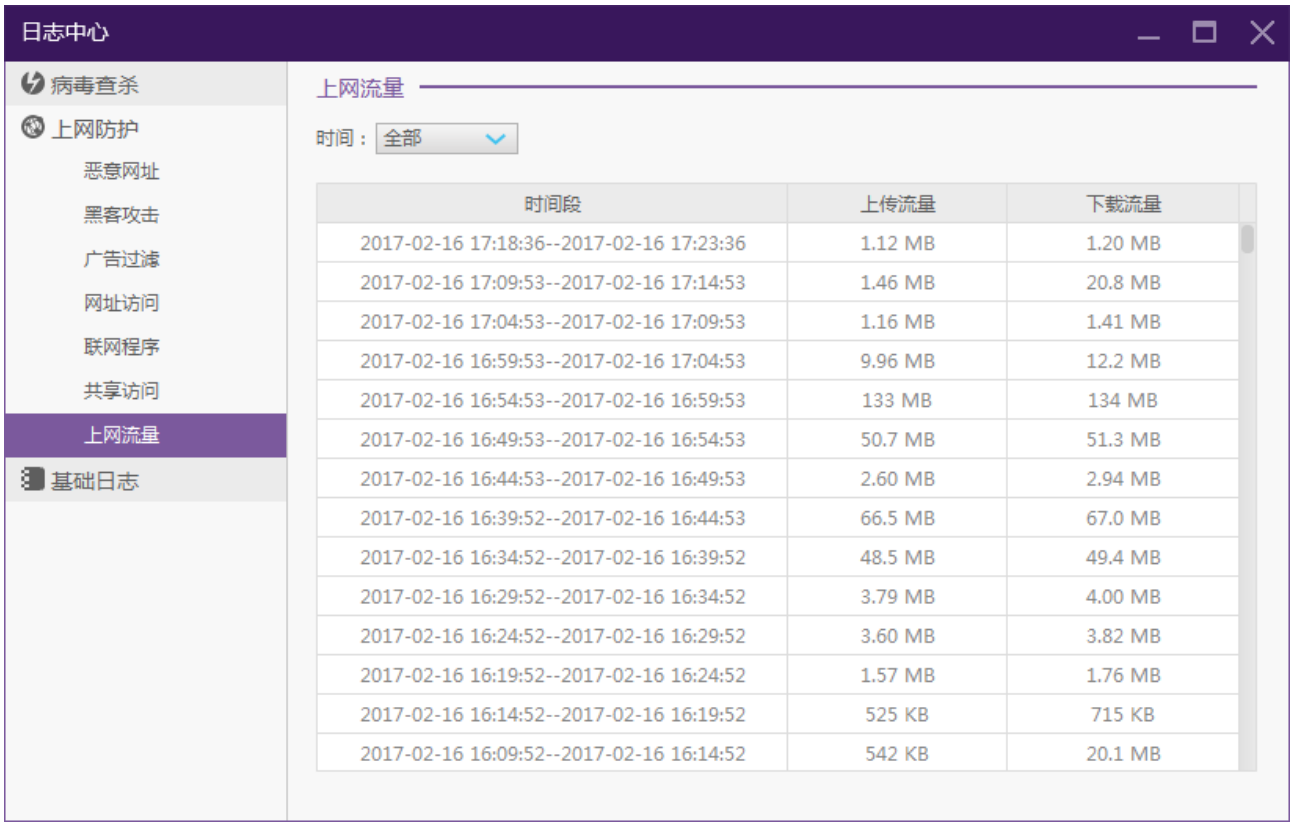


图 9-11

9.2.7 上网流量

上网流量日志记录了计算机上所有的联网信息和每次流量使用情况，包括上网时间、上传流量和下载流量。

点击【上网防护】>【上网流量】，进入上网流量日志界面。如图所示。



时间段	上传流量	下载流量
2017-02-16 17:18:36--2017-02-16 17:23:36	1.12 MB	1.20 MB
2017-02-16 17:09:53--2017-02-16 17:14:53	1.46 MB	20.8 MB
2017-02-16 17:04:53--2017-02-16 17:09:53	1.16 MB	1.41 MB
2017-02-16 16:59:53--2017-02-16 17:04:53	9.96 MB	12.2 MB
2017-02-16 16:54:53--2017-02-16 16:59:53	133 MB	134 MB
2017-02-16 16:49:53--2017-02-16 16:54:53	50.7 MB	51.3 MB
2017-02-16 16:44:53--2017-02-16 16:49:53	2.60 MB	2.94 MB
2017-02-16 16:39:52--2017-02-16 16:44:53	66.5 MB	67.0 MB
2017-02-16 16:34:52--2017-02-16 16:39:52	48.5 MB	49.4 MB
2017-02-16 16:29:52--2017-02-16 16:34:52	3.79 MB	4.00 MB
2017-02-16 16:24:52--2017-02-16 16:29:52	3.60 MB	3.82 MB
2017-02-16 16:19:52--2017-02-16 16:24:52	1.57 MB	1.76 MB
2017-02-16 16:14:52--2017-02-16 16:19:52	525 KB	715 KB
2017-02-16 16:09:52--2017-02-16 16:14:52	542 KB	20.1 MB

图 9-12

9.3 基础日志

基础日志记录的主要是关于安装部署、远程操作命令和远程消息日志。

9.3.1 安装部署

安装部署日志记录了瑞星安全云终端软件及其组件的安装时间、动作、条目、版本信息和重启标志。

点击【基础日志】>【安装部署】，进入安装部署日志界面。如图所示。

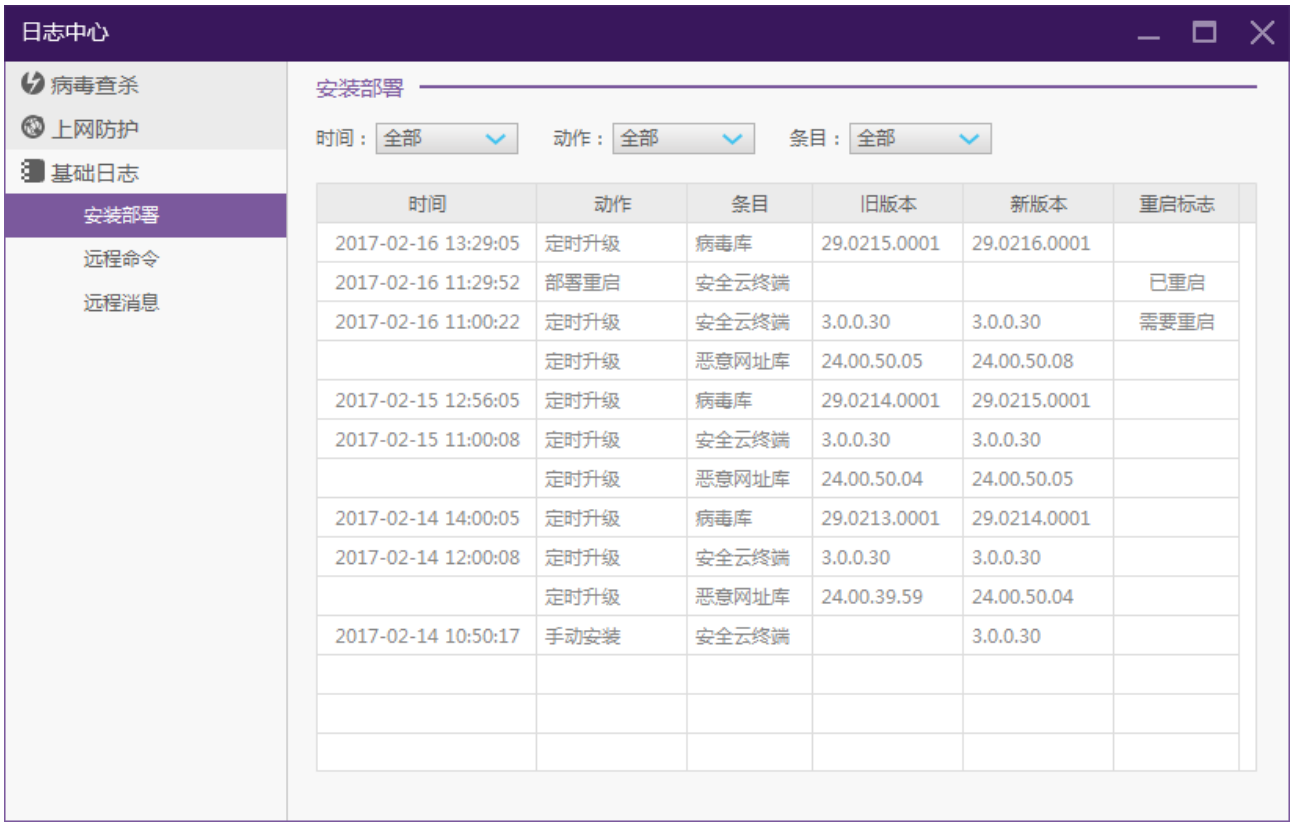


图 9-13

9.3.2 远程命令

远程命令日志记录命令的操作信息，包括发起命令的时间、命令内容、命令执行结果和附加消息。

点击【基础日志】>【远程命令】，进入远程命令日志界面。如图所示。

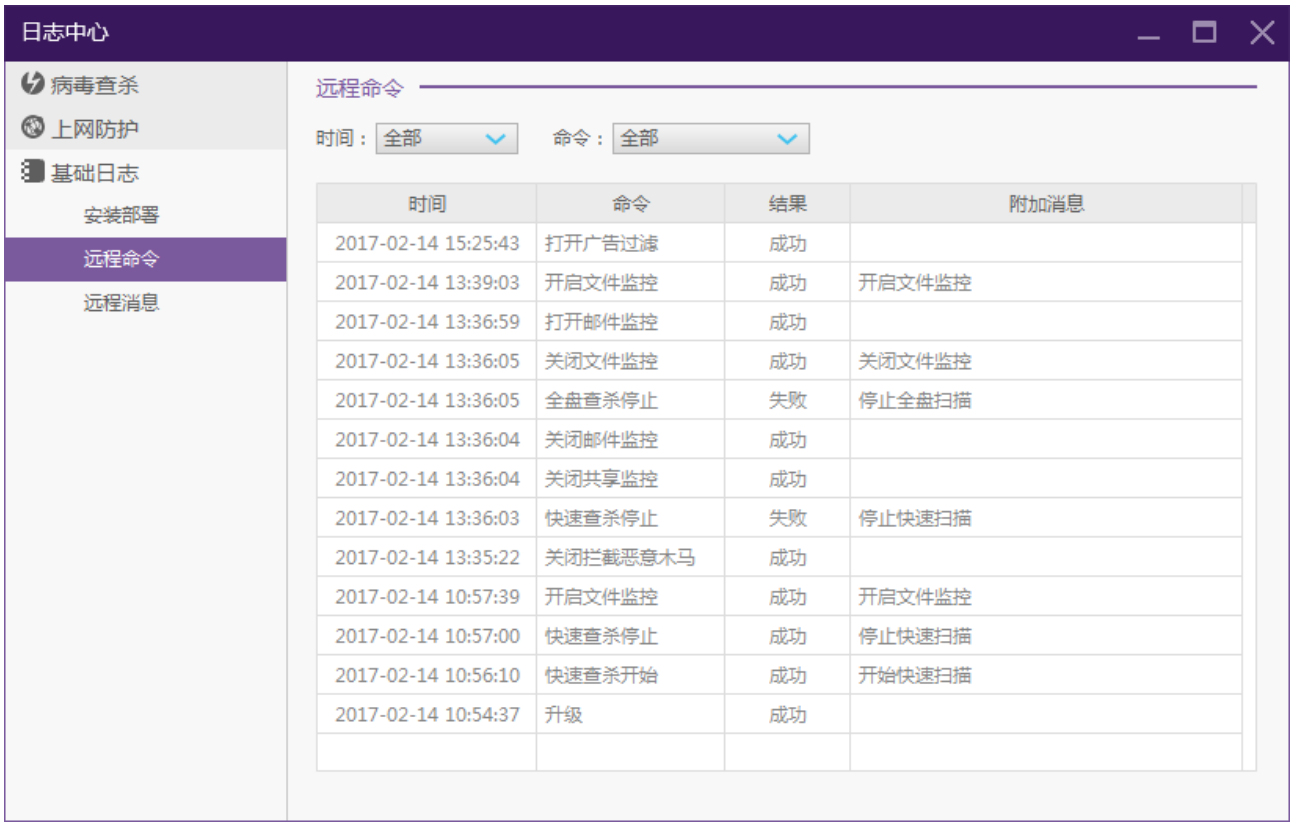


图 9-14

9.3.3 远程消息

远程消息日志记录远程管理端发送的消息，包括发起消息的时间和消息内容。

点击【基础日志】>【远程消息】，进入远程消息日志界面。如图所示。

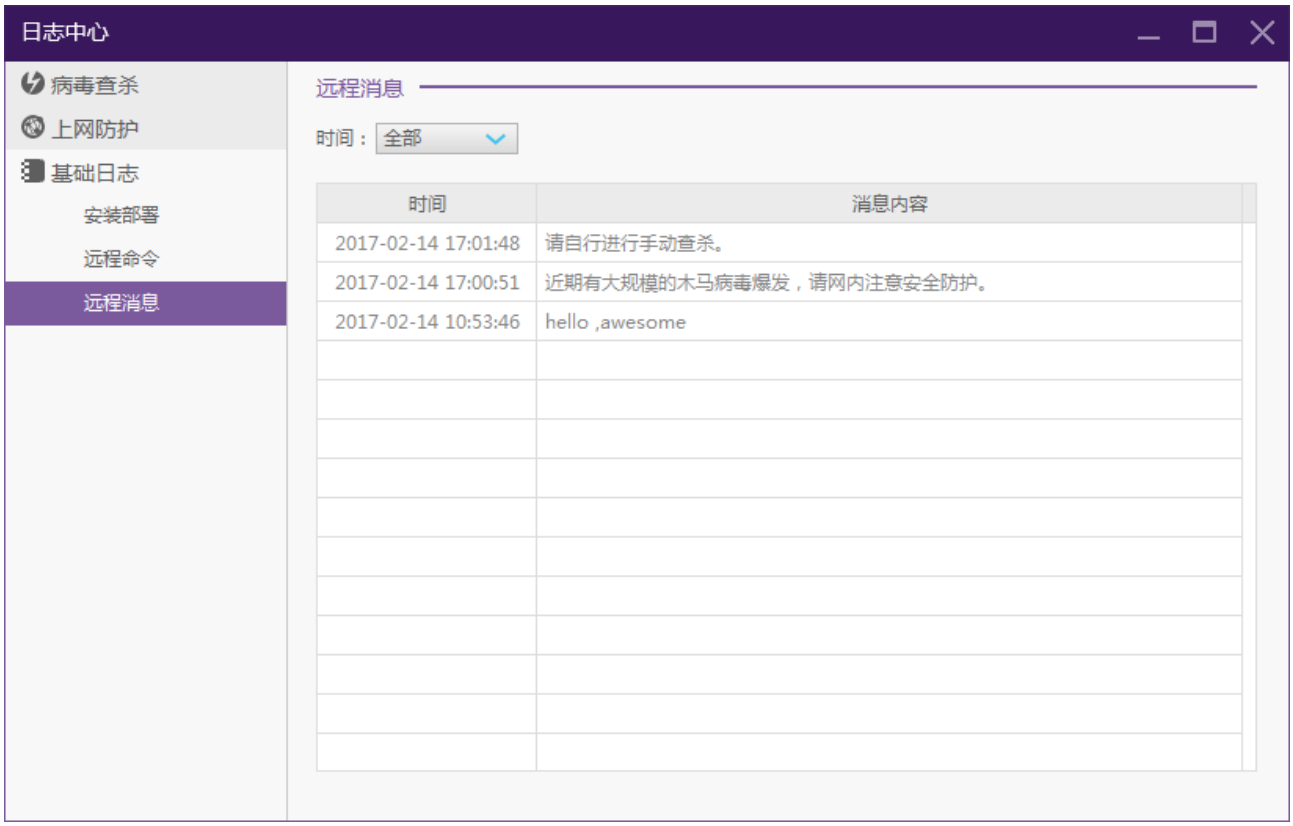


图 9-15

远程消息发送后，在终端接受到的提示框如图所示：

图 9-16

10 托盘功能

托盘是位于任务栏上的图标，用于提示用户正在运行的软件，同时也能通过托盘实现主要功能的快速操作。

瑞星安全云终端软件托盘功能提供了快速进入主界面的方式，除此之外，还有多项功能的快捷入口，包括：快速查杀、网络防护、自我防护、设置、日志、升级和退出。

如图所示。

图 10-1

11 检测更新

当需要更新软件时，点击主界面右上角的“ ”图标，选择“检测更新”选项，

图 11-1

将出如图所示界面：

图 11-2

软件将自动连接瑞星的更新服务器，获取最新的数据，并进行自动安装。

12 在线修复

图 12-1

13 智能客服

在主界面找到如图所示图标，点击【智能客服】。

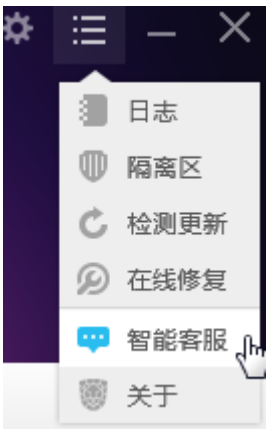


图 13-1

打开智能客服后，通过浏览器弹出一个窗口，如图所示。

图 13-2

然后输入您想咨询的问题，如图所示。

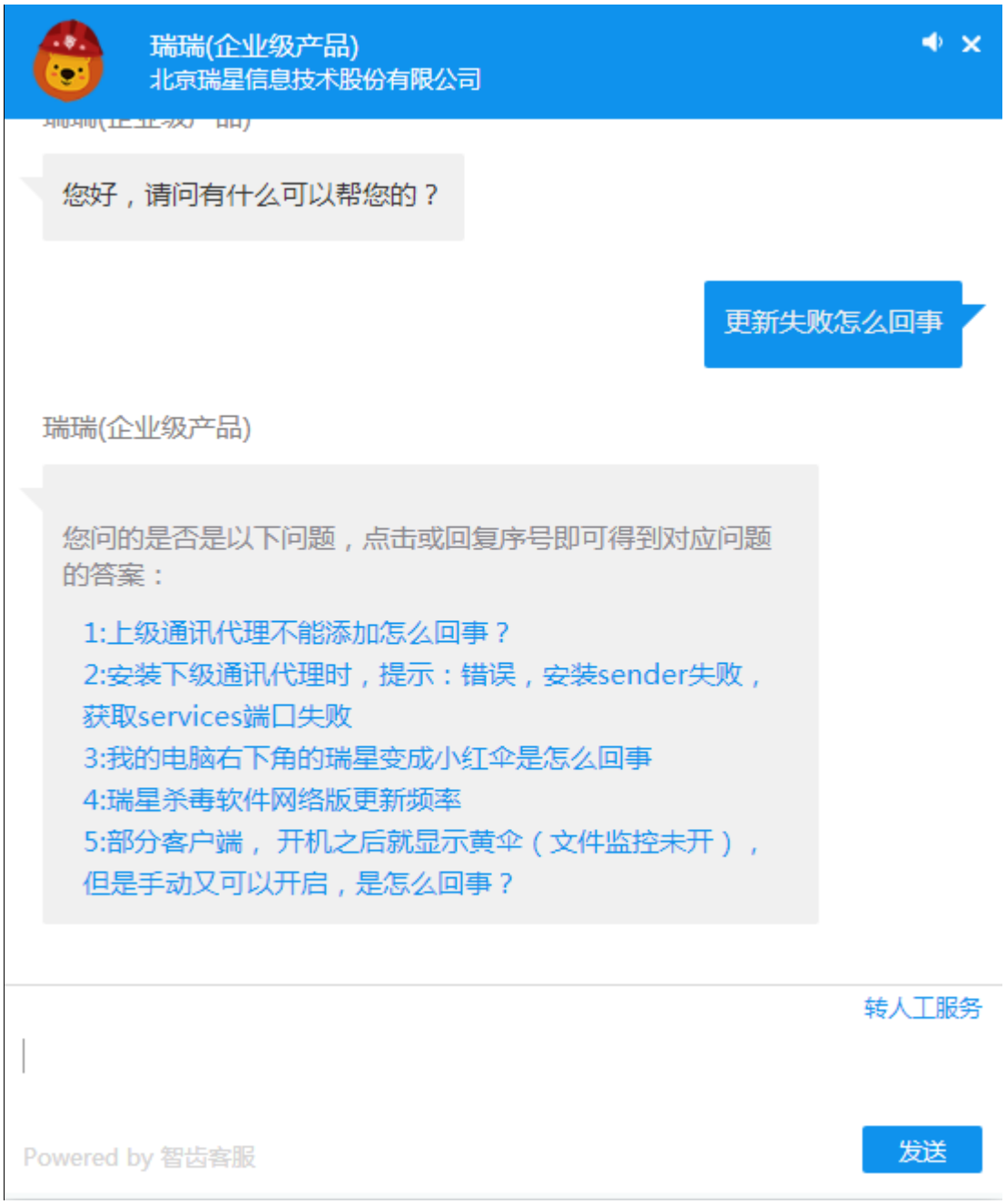


图 13-3

如果智能客服依然不能解决您的问题，请点击右下角的 转人工服务 。

人工服务时间段（工作日：9：00 - 17：30）。

14 加入中心

瑞星安全云产品主要分为两部分：瑞星安全云中心、瑞星安全云终端。其中瑞星安全云终端可适配的平台有 Windows、Linux 和 Android，实现了跨平台、跨终端病毒扫描查杀。瑞星安全云中心的管理和设置都是通过浏览器来实现。通过瑞星安全云中心可以管理各终端（包括 Windows 客户端、Linux 客户端和 Android 客户端）。

因此，通过加入中心功能，让瑞星安全云终端加入到瑞星安全云中心，既便于管理员对网络内的所有终端进行统一高效的管理；也能有效防止病毒隐匿在某个终端，从根本上防止病毒传播。

下面介绍加入瑞星安全云中心的步骤方法。在瑞星安全云终端软件主界面左下角，点击【加入中心】图标，进入安全云中心界面。然后输入中心号后，点击【搜索】，在搜索结果中选择中心，然后点击【立即加入中心】按钮，提示成功加入到瑞星安全云。如图所示。

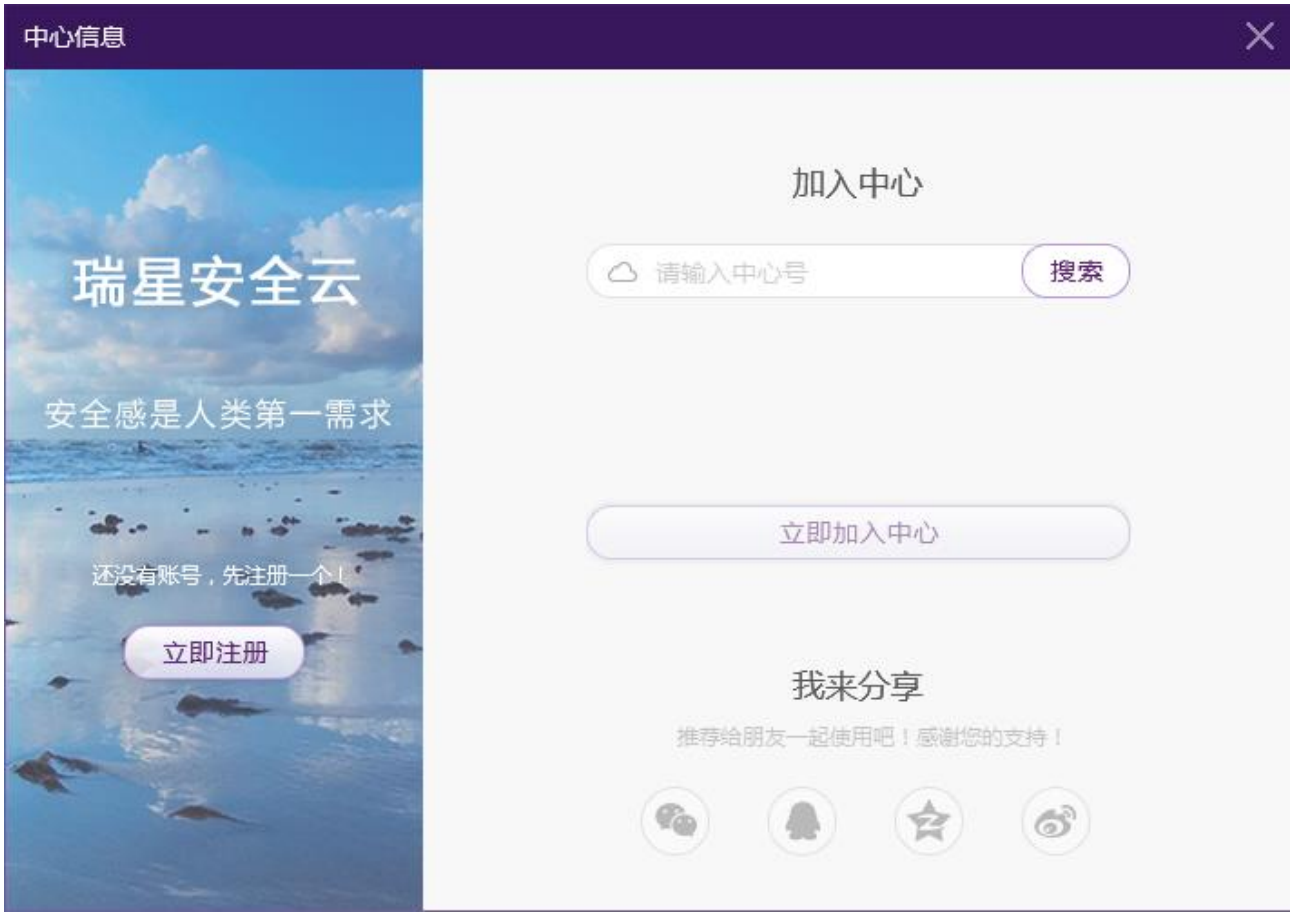


图 14-1

加入瑞星安全云中心后的界面显示如下图所示。

15 关于

点击主界面右上角的“  ”图标，选择【关于】，查看软件详细信息，包括软件当前版本、病毒库版本、最近一次升级时间、版权所有信息和软件使用许可协议。点击【确定】退出。


瑞星安全云终端软件 3.0
当前版本：3.0.0.30
病毒库版本：29.0216.0001
升级时间：2017-02-16 11:00:22
版权所有：北京瑞星信息技术股份有限公司 许可协议
确定

图 15-1

附录一 北京瑞星网安技术股份有限公司简介

瑞星公司主营业务为信息安全整体解决方案的研发、销售及相关增值服务。公司自成立以来一直专注于信息安全领域，以优质的产品和专业的“安全+”服务，向政府、企业及个人提供基于桌面安全、边界安全、管理安全、审计安全、移动安全、虚拟化安全等核心技术的整体解决方案，帮助所有用户有效应对各种类型的信息安全威胁。

公司的主要业务包括企业及个人两大部分。企业级业务涉及：企业终端安全防护、企业网络边界防护、企业网络安全预警、企业网络监测、企业信息审计、虚拟化信息安全、云存储安全、企业移动安全、企业信息安全检测、企业信息安全培训、企业数据恢复、应急响应服务等领域。个人级业务涉及：个人电脑终端安全、个人移动安全、个人网络边界防护、个人数据恢复等领域。

瑞星公司是具有认证资质的高新技术企业，承担了我国第一个虚拟化反病毒国家实验室的建设，并承接了我国第一例虚拟化云存储项目的信息安全建设工作，具有雄厚的技术实力。此外，依托二十余年坚持不懈的产品技术创新和项目经验积累，瑞星在国内信息安全市场中赢得了良好的声誉及口碑。

未来，受“互联网+”计划影响，国内所有传统企业都将大幅向互联网模式转变，信息安全将成为决定企业生存发展的重要因素。因此，瑞星根据多年的技术经验积累，以云计算安全、大数据安全、移动安全、桌面安全、边界安全为基础，为“互联网+”下的企业量身打造了一套“企业信息安全+”整体解决方案，力争为所有企业用户提供最安全最便捷的信息安全保障。

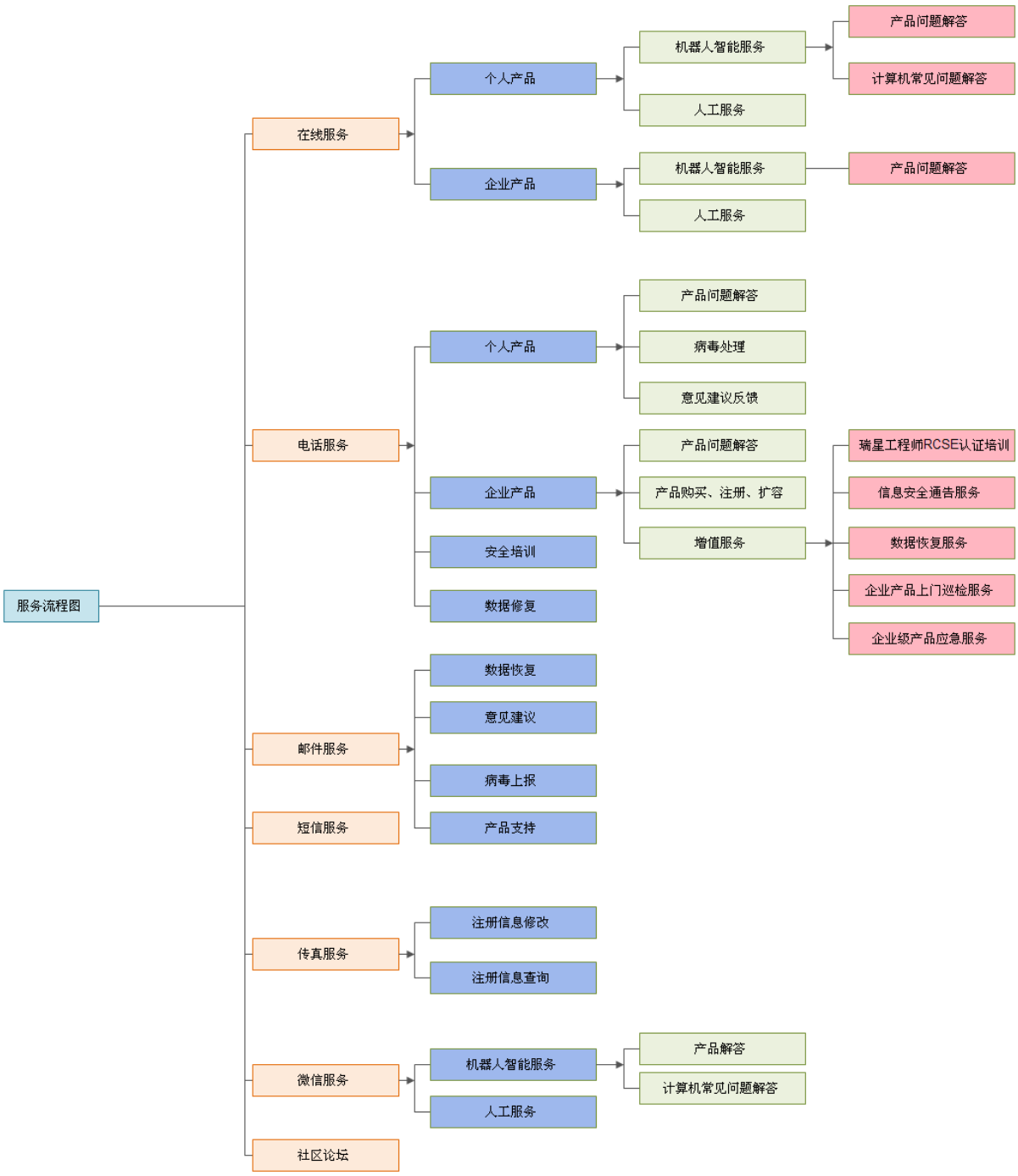
瑞星旗下所有产品均为瑞星公司自主研发，拥有 100%自主知识产权。作为国内唯一一家拥有完整自主知识产权的信息安全整体解决方案提供商，瑞星在国内设有监控中心、研发中心和病毒响应中心等，为所有用户提供最完整最领先的安全服务。

附录二 瑞星客户服务简介

一、 服务体系说明

瑞星公司拥有百余位专业信息安全工程师通过在线服务、电话服务、邮件服务、短信服务、传真服务、微信服务及社区论坛等多种服务方式为您提供全面、专业、及时的技术支持与安全解决方案。

您可参照以下服务体系及其服务流程进行问题咨询和求助。



二、 服务方式介绍

1. 在线服务

·智能服务（7 × 24）：

瑞星公司引入了目前最先进的智能机器人服务系统，通过“智能服务+人工服务”的全新服务模式，给用户提供最专业、最全面的问题解答。

现在点击瑞瑞的头像来尝试和瑞瑞聊天吧！当然您还可以访问瑞星客服中心网站(http://csc.rising.com.cn/index.html)，根据您使用的产品选择相应的在线服务，瑞星智能机器人“瑞瑞”会 7

x 24 小时全天解答您的任何问题。

·人工服务（5 × 8）：

当您遇到特殊问题需要与瑞星工程师咨询反馈时，您可以在机器人瑞瑞的聊天界面中选择“转人工服务”直接与工程师沟通。

2. 电话服务

2004 年瑞星公司斥资 500 万建设业内第一个“电信级”呼叫中心，2007 年再次投资 1500 万元扩建呼叫中心，2009 年开通 400 服务热线为客户提供更优质服务。

客户服务电话：400-660-8866 (免长途话费)

北京及未开通 400 电话地区：010-82678800（个人级）010-82616666（企业级）

3. 邮件服务

您可以访问邮件服务中心(http://mailcenter.rising.com.cn)，发送咨询邮件获得专业指导。

4. 短信服务

短信客服号码：106575020236

短信服务是针对瑞星用户提供的特色服务，您可通过短信获得技术支持，此服务目前仅针对中国移动用户提供。

手机里输入您要咨询的内容，发送短信至 106575020236，瑞星工程师会在工作日内即时回答您的问题。

5. 传真服务

个人级产品：010-82678800（请根据语音提示选择对应数字键进行传真）

企业级产品：010-82616666-8

6. 微信服务

瑞星客户服务中心微信号：Rising-Service

您可以使用手机微信搜索“瑞星客服”或“Rising-Service”，也可以直接扫描二维码添加瑞星客服公众号，在公众号右下角菜单的“更多”中选择“智能客服”，随时随地咨询瑞星相关问题。

7. 社区论坛

论坛服务：http://bbs.ikaka.com/

访问卡卡安全论坛，解决产品使用中遇到的问题，获取最新问题解决方案。

三、 增值服务

（一）信息安全预警服务

1、 短信通报和邮件通报

通过短信和邮件发送最新安全动态、病毒、漏洞等信息，使各企事业单位信息安全管理员获取最专业权威的资讯，并提前消除网络中的安全威胁，排除安全隐患。

2、 挂马网站预警

当用户的 WEB 网站被遭到挂马攻击，系统会自动通知用户网站管理员进行处理，避免产生严重后果。

（二）信息安全专家服务

1、 专属电话通道

用户加入 VIP 客户电话通道后，拨打客服热线，可优先接入，遇忙转接至指定高级工程师，享受问题咨询优先受理。

2、 信息安全顾问

为企业客户指定“一对一”安全顾问提供服务，针对该企业的网络结构、管理要求、网络安全要求等实际情况，提供有针对性的防毒产品部署、配置方案。

3、 光盘邮寄

针对特殊网络环境、上网不方便、管理要求严格的客户，提供加密光盘邮寄服务，光盘内容包括产品安装程序、升级程序、引导杀毒映像、使用手册、技术白皮书、产品解决方案等个性化内容。

（三）信息安全响应服务

1、 现场巡检

指定高级安全顾问与客户建立紧密的长期合作关系，定期为客户提供上门巡检服务，服务内容包括：产品使用培训、产品运行检测、病毒日志分析、现场技术支持等服务，并提供内容可定制的巡检报告。

2、 远程巡检

由指定的高级安全顾问与客户建立紧密的长期合作关系，定期为客户提供远程巡检服务，服务内容包括：产品运行检测、病毒日志分析、远程技术支持等服务，可提供内容定制的巡检报告。

3、 现场紧急救援

针对在发生突发性问题（如：病毒、网络和瑞星产品等问题）时提供及时现场技术支持，提供解决方案并协助解决问题，根据路线可在 1-3 小时内抵达现场。

4、 远程紧急救援

通过远程工具、远程桌面或瑞星企业版用户在线服务等方式针对发生突发性问题（如：病毒、网络和瑞星产品等问题）时提供技术支持，为用户提供解决方案并协助用户第一时间解决问题。

5、 数据灾难恢复

当存储介质出现损伤或由于误操作、病毒导致磁盘数据丢失或损坏的情况。数据灾难恢复服务将帮助客户挽救数据，挽回损失。

（四）信息安全培训服务

从日常网络安全维护、防火墙应用、流行病毒处理、网络攻击应对以及危机发生处理等等方面进行全方面的培训。包括电脑安全使用基础培训、计算机反病毒普及培训、网络安全工程师认证培训、网络管理员高级培训等等，也可以根据企业个性化需求定制培训。

服务须知

了解更多增值服务细节或购买请咨询 400-660-8800(010-82616666)或访问瑞星客户服务中心(http://csc.rising.com.cn/index.html)。

四、 联系方式

工作时间：国家法定工作日 9:00-17:30

联系地址：北京市海淀区中关村大街 22 号中科大厦 1403 室

邮政编码：100190