微点主动防御软件
使用手册

北京东方微点信息技术有限责任公司

福建东方微点信息安全有限责任公司

目录

第 1 章 微点主动防御软件介绍 1

1.1 研发背景 1
1.2 微点主动防御技术及其原理 3
1.3 主动防御未知病毒的实例 4
1.4 微点主动防御软件的主要功能及其描述 5
1.5 微点主动防御软件设计者刘旭简介 7

第 2 章 安装和卸载微点主动防御软件 8

2.1 微点主动防御软件的适用环境 8
2.2 安装微点主动防御软件 8
2.3 注册软件 13
2.4 卸载微点主动防御软件 15

第 3 章 微点主动防御软件的主程序 17

3.1 启动／退出微点 17
3.1.1 启动微点 17
3.1.2 退出微点 17
3.2 软件的主界面 18
3.2.1 主界面结构及其说明 18
3.2.2 系统托盘图标 21

第 4 章 软件设置 24

4.1 程序行为实时监控策略 24
4.2 可信程序设置 26
4.3 程序访问网络策略设置 28
4.3.1 设置程序访问网络策略 28
4.3.2 智能识别功能 30
4.4 传统防火墙 30
4.4.1 传统防火墙设置 30

4.4.2 绑定MAC地址 34
4.5 有害程序隔离区 35
4.5.1 隔离区文件管理 35
4.5.2 隔离区设置 36
4.6 自启动项回收站 38
4.7 升级设置 39
4.7.1 在线升级设置 39
4.7.2 离线升级 42

第 5 章 报警处理 43

5.1 有害程序的报警 44
5.1.1 已知有害程序报警及处理 44
5.1.2 未知有害程序报警及处理 44
5.1.3 漏洞攻击的报警及处理 45
5.1.4 可疑程序的报警及处理 47
5.1.5 发现远程安装程序的报警及处理 47
5.1.6 修改注册表的报警及处理 48
5.2 异常网络访问行为的报警及处理 49
5.3 未知病毒命名更新 50

第 6 章 微点工具 51

6.1 可疑程序诊断 51
6.1.1 执行可疑程序诊断 51
6.1.2 分析诊断结果 52
6.1.3 处理可疑程序 54
6.2 漏洞扫描 55
6.2.1 启动漏洞扫描 56
6.2.2 修补漏洞 56
6.2.3 导出漏洞信息列表 56
6.3 注册表修复 57
6.4 注册表保护 58

第 7 章 进程分析 59

7.1 系统分析 59
7.1.1 进程综合信息 59
7.1.1.1 进程分类 60
7.1.1.2 进程综合信息的描述 61
7.1.1.3 进程综合信息的操作 61
7.1.2 系统自启动信息 64
7.1.3 模块/进程 66
7.1.4 系统信息 68
7.2 网络分析 68
7.2.1 进程网络信息 68
7.2.2 流量图 69
7.2.3 传统防火墙信息 70

第 8 章 日志分析 71

8.1 日志管理 71
8.2 安全日志 72
8.3 系统日志 73

第 9 章 辅助功能 75

9.1 修改注册信息 75
9.2 续费 76
9.3 查询剩余时间 77
9.4 密码设置 77
9.5 导入/导出设置 77
9.6 生成技术信息 78

附录 80

附录一 常见问题 80
附录二 联系技术支持 83
附录三 用户信息反馈卡 ..... 错误！未定义书签。

第1章 微点主动防御软件介绍

微点主动防御软件，是北京东方微点信息技术有限责任公司（以下简称微点公司）自主研发的具有完全自主知识产权的新一代反病毒产品，在国际上首次实现了主动防御技术体系，并依此确立了反病毒技术新标准。微点主动防御软件最显著的特点是，除具有特征码扫描技术查杀已知病毒的功能外，更实现了用软件技术模拟反病毒专家智能分析判定病毒的机制，自主发现并自动清除未知病毒。

1.1 研发背景

虽然绝大多数用户的计算机中都安装了各种品牌的反病毒软件，但令人遗憾的是，用户所面临的病毒危害并没有因此显著降低，反而呈现了上升趋势。根据国家计算机病毒应急处理中心《2007 年中国计算机病毒疫情调查技术分析报告》，截止 2007 年 6 月，我国计算机病毒感染率高达 91.47%，与前两年相比又出现了较大的反弹。传统反病毒技术已不再适应当前反病毒的需求是造成这种局面的主要原因之一。

传统反病毒技术——特征码扫描技术，其核心思想是反病毒公司从病毒体代码中，人工提取出病毒的特征码，然后由反病毒产品将被查对象与病毒特征码进行比对，如果被查对象中含有某个病毒的特征码就将其报为病毒。

反病毒公司已经提取特征码的病毒称为已知病毒，未提取特征码的病毒就称为未知病毒。特征码扫描技术依赖于从病毒体中提取的特征码，未获得病毒体就无法取得特征码。其技术原理决定了，特征码扫描技术只能识别已知病毒，不能防范未知病毒。

传统反病毒技术的流程为：当用户发现计算机出现异常现象，怀疑可能被病毒感染 → 具有一定反病毒知识的用户将可疑文件通过邮件等途径发送至反病毒公司 → 反病毒公司收到可疑文件后，由病毒分析工程师进行人工分析 → 如果认定是病毒，则从病毒代码中提取该病毒的特征码，然后制作升级程序并将其放在互联网上 → 最后，待用户升级反病毒软件后，才能对这个病毒进行查杀。但在用户升级之前，用户

计算机上的反病毒产品无法阻止该病毒的感染和破坏。

目前，传统的反病毒技术面临着非常严峻的病毒挑战，黑客大规模批量制造各种以窃取商业秘密、虚拟财产、银行帐号等为目的的木马病毒，这类以营利为目的的新型病毒已成为当前病毒发展的主导趋势。黑客为了避免木马被杀毒软件发现，开发出多种简单易行的病毒免杀技术，无须重新编写病毒程序，只需经过简单地加壳、加花指令、定位并修改病毒特征码等技术方式的处理，很短时间内就可大规模批量制造出可逃避传统反病毒产品查杀的木马变种。

更为严峻的是，已经出现了自动加壳、自动免杀机，甚至还实现了商业化，病毒作者每天对其进行更新，升级速度甚至超过了杀毒软件。黑客利用这类工具自动生成的木马变种，往往能够躲过最新版杀毒软件的查杀。木马生产的“工业化、自动化”导致木马越来越难以被反病毒公司收集，或者在收集到这些木马前，这些木马已经有着较长的生存时间，已经给用户造成难以挽回的损失。

据德国 AV 测试实验室介绍，2007 年出现约 550 万个通过互联网传播的恶意程序，反病毒公司每天需分析 1.5 万至 2 万个新病毒。这使反病毒公司的日均工作量增加至 2006 年的 4 倍，更是 2005 年的 15 倍。

传统反病毒技术“出现病毒—收集病毒—分析病毒—升级病毒库”的处理模式，

尽管能够较好防范已知病毒，用户仍面临大量反病毒公司还未收集到的病毒以及每天数以万计新病毒的威胁，用户的信息安全得不到有效保障。

传统反病毒技术落后于病毒技术的步伐已是不争的事实，它已经不适应当前反病毒的需求，因此，广大计算机用户迫切需要一种可以自动查杀未知病毒的反病毒软件。

1.2 微点主动防御技术及其原理

既然反病毒工程师可以通过分析程序行为而准确判定一个程序是否是病毒，那么能否将这种分析判断过程自动化、程序化呢？

我国著名反病毒专家刘旭认为，这种想法是可行的。微点主动防御技术正是根据这种思路设计而来：通过对病毒行为规律分析、归纳、总结，并结合反病毒专家判定病毒的经验，提炼成病毒识别规则知识库，模拟专家发现新病毒的机理，通过分布在操作系统的众多探针，动态监视所运行程序调用各种应用程序编程接口（API）的动作，将程序的一系列动作通过逻辑关系分析组成有意义的行为，再综合应用病毒识别规则知识，实现自动判定病毒。

反病毒专家刘旭在总结自己二十年来反病毒技术实践的基础上，在国际上率先创立了“监控并举、动态防护”的主动防御技术体系，开创性确立了主动防御产品的核心标准，即必须以具备动态仿真反病毒专家系统为先决条件，以自动准确判定未知病毒为基本诉求，以程序行为监控并举为机制保障。在刘旭的带领下，微点研发团队成功研制出世界首款可主动防御计算机病毒和网络攻击的新一代反病毒软件——微点主动防御软件，采用了动态仿真反病毒专家系统，自动准确判定新病毒、程序行为监控并举、自动提取特征码实现多重防护、可视化显示监控信息五项核心技术，实现了对未知病毒的自主识别、明确报出和自动清除，有效克服了传统杀毒软件滞后于病毒的致命缺陷。

面对当前形形色色的主动防御概念，刘旭指出，与所有的反病毒技术一样，主动防御技术也必须要实现对程序的性质做出明确判定，是病毒，就应明确报警并提示用户发现病毒。如果只是对程序的单一动作报警，由用户自己判断这个动作是否具有威胁，就不是主动防御。这里所说的程序动作，是指反病毒软件监控到程序调用了 Windows 提供的某个 API。API 是 Windows 为程序开发提供的功能，正常程序可以使用，病毒也可以使用，也就是说 API 本身并没有善恶之分。如果仅仅依据程序的一个动作就报警，那么普通的用户实在难以判断这个动作究竟是否有害，更会感到无所适从，这显然不是广大计算机用户所需要的反病毒技术。

2005 年，微点主动防御软件研制成功，开创了国际反病毒技术发展的一个崭新时代，主动防御技术成为下一代反病毒核心技术已成为国际反病毒公司的广泛共识。

经历了近三年不同寻常的超长时间公开测试，经历了数百万用户的大规模测试和使用，今天，微点主动防御软件产品以其更稳定、更成熟的优异品质迎接全球用户的考验。微点主动防御软件获得了用户广泛青睐，用户对其技术的先进性特别是防范未知病毒的能力普遍给予高度评价。

目前，作为国家 863 科技攻关项目，微点主动防御技术依然处于国际领先地位。

1.3 主动防御未知病毒的实例

“熊猫烧香”病毒是国内编写的一种蠕虫病毒，在 2006 年 10 月至 2007 年 2 月期间，造成全国数百万台计算机被感染和破坏，影响恶劣、损失巨大。

为了躲避杀毒软件查杀，病毒编写者每天多次更新修改“熊猫烧香”病毒程序，先后共编写并传播了数百种“熊猫烧香”病毒。病毒编写者甚至还在病毒中留言，公开挑战反病毒公司，展开了一场病毒编写者与反病毒公司之间的激烈较量。

在这场较量中，只有当某种“熊猫烧香”病毒出现并造成部分用户受损后，反病毒公司才能收集到该种病毒，然后更新病毒库为染毒用户提供处理方案。但是，“熊猫烧香”的变种速度甚至比杀毒软件更新速度更快，旧的“熊猫烧香”还未被完全剿灭时，新的“熊猫烧香”已开始在网络上兴风作浪。

“熊猫烧香”病毒不断更新，使得杀毒软件也要被迫不断升级，可“熊猫烧香”病毒的感染和破坏并没有因此而得到有效遏制。在这场长达数月的较量中，传统杀毒软件无力为用户提供有效保护，直到病毒编写者被捕后才告结束。“熊猫烧香”病毒凸显传统反病毒技术的致命缺陷，促使了反病毒技术从特征码扫描向主动防御转变。

这场残酷的较量中，微点主动防御软件经受住了“熊猫烧香”病毒的严峻考验。当时，微点主动防御软件是国际上仅有的一款无需升级即可防范“熊猫烧香”病毒的反病毒产品。使用微点主动防御软件的百万用户无一被病毒感染，即使没有升过级的微点主动防御软件 2005 年版本，同样可以实现对“熊猫烧香”所有变种病毒的准确报毒和自动清除，充分体现了微点主动防御技术的先进性。

1.4 微点主动防御软件的主要功能及其描述

1） 无需扫描，不依赖升级，简单易用，安全省心。

反病毒技术的更新换代，使得反病毒软件的使用习惯也发生了翻天覆地的变化。微点主动防御软件令用户感受到前所未有的安全体验，摒弃传统使用观念，无需扫描，不依赖升级，简单易用，更安全、更省心。

2） 主动防杀未知病毒

动态仿真反病毒专家系统，有效解决传统技术先中毒后杀毒的弊端，对未知病毒

实现自主识别、明确报出、自动清除。

3） 全面保护信息资产

严密防范黑客、病毒、木马、间谍软件和蠕虫等攻击。全面保护您的信息资产，如帐号密码、网络财产、重要文件等。

4） 智能病毒分析技术

动态仿真反病毒专家系统分析识别出未知病毒后，能够自动提取该病毒的特征码，自动升级本地病毒特征码库，实现对未知病毒“捕获、分析、升级”的智能化。

5） 强大的病毒清除能力

驱动级清除病毒机制，具有强大的清除病毒能力，可有效解决抗清除性病毒，克服传统杀毒软件能够发现但无法彻底清除此类病毒的问题。

6） 强大的自我保护机制

驱动级安全保护机制，避免自身被病毒破坏而丧失对计算机系统的保护作用。

7） 智能防火墙

集成的智能防火墙有效抵御外界的攻击。智能防火墙不同于其它的传统防火墙，并不是每个进程访问网络都要询问用户是否放行。对于正常程序和准确判定病毒的程序，智能防火墙不会询问用户，只有不可确定的进程有网络访问行为时，才请求用户协助。有效克服了传统防火墙技术频繁报警询问，给用户带来困惑以及用户因难以自行判断，导致误判、造成危害产生或正常程序无法运行的缺陷。

8） 强大的溢出攻击防护能力

即使在 windows 系统漏洞未进行修复的情况下，依然能够有效检测到黑客利用系统漏洞进行的溢出攻击和入侵，实时保护计算机的安全。避免因为用户因不便安装系统补丁而带来的安全隐患。

9） 准确定位攻击源

拦截远程攻击时，同步准确记录远程计算机的 IP 地址，协助用户迅速准确锁定攻击源，并能够提供攻击计算机准确的地理位置，实现攻击源的全球定位。

10）专业系统诊断工具

除提供便于普通用户使用的可疑程序诊断等一键式智能分析功能外，同时提供了专业的系统分析平台，记录程序生成、进程启动和退出，并动态显示网络连接、远端地址、所用协议、端口等实时信息，轻轻松松全面掌控系统的运行状态。

11）详尽的系统运行日志记录，提供了强大的系统分析工具

实时监控并记录进程的动作行为，提供完整的、丰富的系统信息，用户可通过分析程序生成关系、模块调用、注册表修改、进程启动情况等信息，能够直观掌握当前系统中进程的运行状况，能够自行分析判断系统的安全性。

1.5 微点主动防御软件设计者刘旭简介

刘旭，北京东方微点信息技术有限责任公司总经理兼总工程师，我国著名反病毒专家，原国家 863 反病毒专家，中科院高级工程师，曾多次获得中科院、北京市和福建省科技进步奖。

刘旭从事反病毒技术研究二十年，曾任北京瑞星电脑科技开发公司总工程师、北京瑞星科技股份有限公司总裁，是瑞星杀毒软件、瑞星防病毒卡的原设计者。在 2000 年之前，独自一人编写了瑞星杀毒软件、瑞星防病毒卡的所有程序代码。2003 年 2 月，刘旭辞去北京瑞星科技股份有限公司总裁职务。

2005 年 1 月，刘旭创办了北京东方微点信息技术有限责任公司，主持设计和开发了具有国际领先水平的自主创新产品——微点主动防御软件。

第2章 安装和卸载微点主动防御软件

2.1 微点主动防御软件的适用环境

运行微点主动防御软件需要的计算机环境：

硬件要求：

处理器：Intel Pentium Ⅱ 450MHz 或以上

内　存：128M 以上

硬　盘：300M 以上剩余空间

适用的操作系统：Windows 2000/XP/2003/VISTA/2008/7

支持语言：简体中文和英文

2.2 安装微点主动防御软件

【第一步】将微点主动防御软件的安装光盘插入光盘驱动器，会自动进入安装界面，单击“安装微点主动防御软件”；或者运行光盘根目录下的安装程序 MPSetup.exe，打开如图 1 所示的语言选择窗口，选择一种语言后，单击“下一步”，开始安装；

图 1

【第二步】进入微点主动防御软件的安装向导如图 2：

图 2

【第三步】单击“下一步”按钮，出现【许可证协议】对话框，如图 3。请用户仔细阅读“许可证协议”，接受“许可证协议”选择“同意”。否则选择“不同意”，将退出安装程序；

图 3

【第四步】选择“同意”后，单击“下一步”，继续安装。在打开的【客户信息】窗口（如图 4）中正确输入以下信息：用户名、公司名、产品序列号（**随产品提供，序列号见说明书首页**）；

图 4

【第五步】单击“下一步”按钮，指定微点主动防御软件的安装路径（如图 5），若想更改安装路径，请直接单击“浏览”，在系统中选择所要的路径即可；

图 5

【第六步】选择安装路径后，单击“下一步”，进入【选择程序文件夹】（如图 6），用户既可以使用默认的程序文件夹名称 Micropoint，也可以自定义程序文件夹名称。建议用户使用默认的程序文件夹名称；

图 6

【第七步】单击“下一步”按钮，进入【开始复制文件】（如图 7），【开始复制文件】窗口中显示了刚才设置的信息、安装路径以及程序组名称，提示用户对设置信息进行确认，若需要修改这些信息可以单击【上一步】进行更改；

图 7

【第八步】确认信息无误后，单击“下一步”，开始复制文件并进行程序的初始化，如图 8 所示，这个过程需要持续几分钟时间；

图 8

【第九步】程序初始化结束后，弹出如图 9 所示的【初始设置】窗口。推荐使用软件的默认设置值，你也可以单击“点击修改”更改设置。软件安装完成后，可以随时调整这些设置；

图 9

【第十步】单击“下一步”进入【产品注册】窗口，根据提示信息进行注册（注册参看 2.3【注册软件】），若暂时不想对软件进行注册，可单击“跳过”，继续进行软件的安装；建议您立即注册本软件，以便能实时升级。

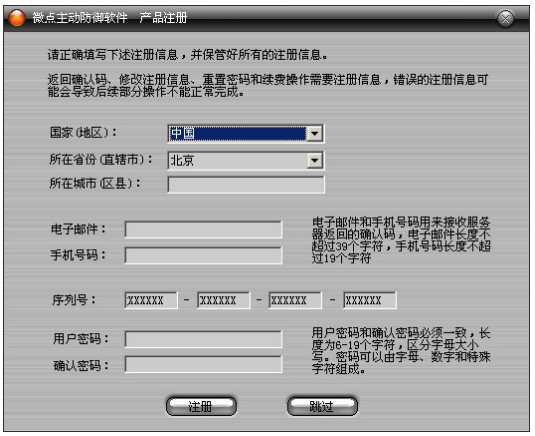


图 10

【第十一步】软件安装完成，提示如图 11：

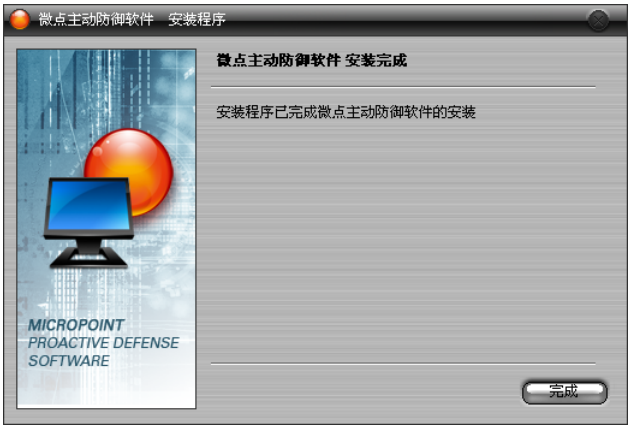


图 11

【第十二步】单击“完成”，软件提示要求重新启动计算机（如图 12），重新启动单击“是”重新启动计算机，完成微点主动防御软件的安装。若暂时有重要事情不能重启计算机，请点击“否”，稍后重启计算机，待事情处理完成后，尽快重启计算机，以完成微点主动防御软件的安装。

图 12

微点提示：微点主动防御软件安装完成后，需要重新启动计算机才能正常运行。在重启前，不会对系统提供安全防护，建议用户安装完成后，立即重启计算机。安装后未重新启动计算机前，请不要启动微点软件，以免出现意外现象。

2.3 注册软件

请在线注册微点主动防御软件，注册后可以享受软件全面的升级服务。

【第一步】注册前请检查网络，确保您的计算机已经连接到互联网上；

【第二步】详细阅读【产品注册】详细信息区中提示信息，依据提示信息，正确输入各项内容（如图 13）；

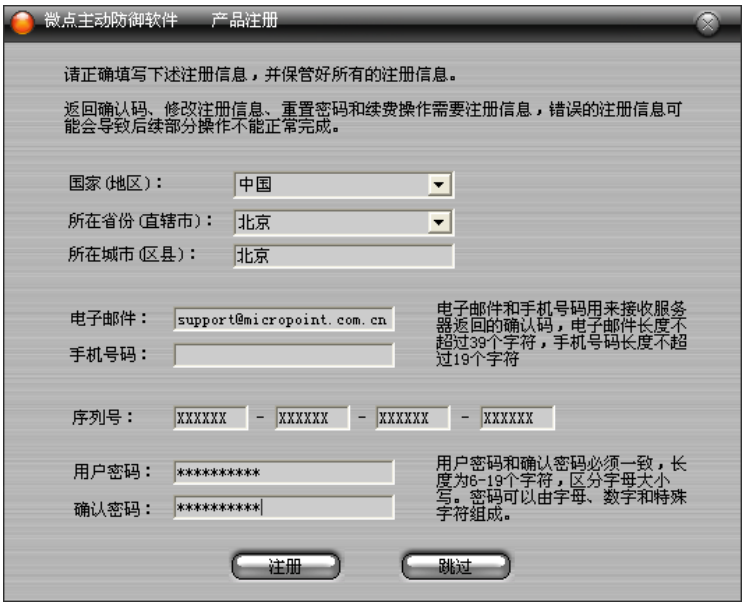


图 13

微点提示：

①. 家庭版包含三个授权，可以在三台计算机上安装注册。在不同计算机上注册请使用不同的用户信息，比如使用不同的邮箱或者相同邮箱不同密码。

②. 国家、所在省份、所在城市、邮件帐号、用户密码是必填项目。建议填写您经常使用的邮件帐号，以便您在注册时能够迅速及时收到“确认码”，完成注册。

③. 手机号码为选填项目。填写后，能够以短信的方式接收注册“确认码”和重置的“新密码”，接收这些信息完全免费。

【第三步】信息输入完成后，单击“注册”，请等待微点软件注册服务器返回信息：确认码；

【第四步】请到您注册使用的邮箱或手机短信中获取微点软件注册服务器发出的确认码；

【第五步】在如图 14 中输入“确认码”；

图 14

【第六步】单击“确认”按钮，若确认码输入无误，微点主动防御软件提示如图 15，表示软件已经成功注册。

图 15

微点提示：

① 家庭版在三台计算机上分别注册成功后，微点软件将自动给用户分配三个新

的序列号，此序列号具有唯一性，请牢记此序列号及注册信息，重装微点软件时请输入分配后的序列号进行安装注册。

② 注册成功后，您可以到微点网站注册通行证，然后使用通行证提供的序列号绑定功能，将序列号进行绑定，以便以后查找您的序列号、注册邮箱，同时在忘记注册密码时，可以进行密码重置。

如果安装过程中没有注册，安装完成后打开微点主动防御软件主界面，在【辅助功能】中单击【注册】标签页或单击系统托盘区  的右键菜单中的“注册”，根据提示进行注册。

2.4 卸载微点主动防御软件

微点主动防御软件提供了自动卸载的功能，操作步骤如下：

【第一步】单击【开始】→【程序】→【Micropoint】→【卸载微点主动防御软件】，打开【欢迎使用微点主动防御软件卸载向导】（如图 16）；

图 16

【第二步】单击“下一步”，自动卸载微点主动防御软件，如图 17；

图 17

【第三步】卸载完成，微点主动防御软件提示（如图 18）“卸载本程序需重启，是否现在重启？”，单击“是”，重新启动计算机，即可完全卸载微点主动防御软件。

图 18

另外，也可以从【控制面板】中的【添加 / 删除程序】中快速删除微点主动防御软件。

第3章 微点主动防御软件的主程序

3.1 启动／退出微点

3.1.1 启动微点

启动微点主动防御软件的两种方式：系统自启动和手动启动。

1) 系统自启动：

微点主动防御软件安装完毕，重新启动计算机后，微点主动防御软件以服务的形式加载启动，系统托盘区会出现一个图标，表示微点主动防御软件的主程序已经启动成功。

2) 手动启动：

退出微点主动防御软件主程序后，重新启动需手动启动，启动方式有两种：

- 程序菜单启动

  单击【开始】→【程序】→【Micropoint】→【微点主动防御软件】后，在系统托盘区出现一个图标，表明微点主动防御软件主程序已经启动成功。

- 桌面快捷方式启动

  双击桌面上的微点主动防御软件的快捷图标，即可启动微点主动防御软件主程序。

3.1.2 退出微点

鼠标右键单击系统托盘区中的图标，在弹出的菜单中单击“退出”，托盘区的图标消失，表示微点主动防御软件已退出。微点主动防御软件退出后，将不再对系统提

供安全保护。

3.2 软件的主界面

微点主动防御软件为用户提供一个友好的、可操作性强的管理主界面，便于用户管理系统的安全。

启动微点主动防御软件主界面有三种方式：

1) 桌面快捷方式启动：

双击桌面快捷图标  ，打开微点主动防御软件的主界面。

2) 程序菜单启动：

单击【开始】→【程序】→【Micropoint】→【微点主动防御软件】，启动微点主动防御软件主界面。

3) 托盘启动：

双击桌面右下角系统托盘区微点的托盘图标或者选择托盘图标  右键菜单中的“主界面”，可迅速打开微点主动防御软件的主界面。

3.2.1 主界面结构及其说明

微点主动防御软件主界面结构及名称如图 19 所示：

图 19

【①菜单栏】 — 通过菜单您可以迅速定位到各功能窗口。

【②工具栏】 — 为方便用户使用提供了重要功能的快捷按钮：

— 查看：查看进程综合信息，详细请参阅第 7.1.1 的【进程综合信息】。

— 诊断：诊断当前系统中的可疑程序。详细请参阅 6.1【可疑程序诊断】。

— 扫描：扫描并报告系统当前存在的已知漏洞。详细请参阅 6.2 的【漏洞扫描】。

— 设置：迅速打开程序行为实时监控策略设置窗口。详细请参阅 4.1【程序行为实时监控策略】。

— 升级：更新微点主动防御软件程序和已知病毒特征库。

【③界面模式切换按钮】 — 用于进行微点主界面模式切换的按钮，微点主界面有两种模式：简约模式（如图 20）、标准模式（默认）。

图 20

【④智能窗口】—微点主动防御软件的智能窗口实时显示计算机系统进程数量以及计算机与外界网络通讯状态，并通过 IP 地址地理信息库，可以定位到本计算机与互联网络中通讯计算机的地理位置。

- 已知进程 — 当前系统中的已知进程总数。“已知进程”指的是微点已识别的正常进程，包括：进程综合信息中显示的 Windows 系统软件类、应用软件类的进程以及用户自己添加到“可信程序”列表中的进程。
- 其他进程 — 当前系统中其他进程总数。“其他进程”指的是微点主动防御软件未识别的进程，即进程综合信息中显示为“其他软件”的进程。
- 当前连接 — 当前系统中正在进行网络连接的进程的总数。
- 当前流量 — 当前系统中正在进行网络连接进程的总流量，包括上传总流量和下载总流量。
- 远端地址 — 滚动显示当前系统中正在与本地计算机进行网络通讯的远端计算机的 IP 地址和地理位置。用鼠标单击滚动的某 IP 地址，可以直接打开【进程网络信息】，定位到正在访问远端地址的进程。

【⑤标签栏】— 显示已打开的标签页的名称列表。

【⑥标签页操作按钮】:

 —【⑥标签页列表显示按钮】：单击该按钮，在下拉菜单中显示当前标签栏中所有已打开的标签页列表。

 —【⑥标签页分离按钮】：单击该按钮，可将当前标签页从主界面中分离出来，便于用户在不同标签页中查看、对比、分析标签页详细信息区内的信息。鼠标右键单击标签栏中的当前标签页的名称也可以将当前标签页从主界面分离出来，您可以根据习惯选择适宜的操作方式。

 —【⑥标签页关闭按钮】：关闭标签栏中的当前标签页。双击标签栏中

的当前标签页的名称也可关闭当前标签页，你可以根据习惯选择适宜的操作方式。

【⑦主功能区】 — 进行功能设置及操作的区域，与主菜单栏完成同样的管理任务。

【⑧功能区隐藏按钮】 — 单击该按钮可以将功能区隐藏。

【⑨详细信息区】 — 显示标签页包含的详细信息。

【⑩状态栏】 — 显示微点主动防御软件当前版本号及更新时间。

3.2.2 系统托盘图标

微点主动防御软件启动后，会在系统托盘处显示微点主动防御软件的图标，托盘图标的不同状态表示微点主动防御软件不同的监控状态。

系统托盘图标

 — 防护状态：微点主动防御软件正在对系统提供实时安全防护。

 — 暂停状态：暂时停止微点主动防御软件的实时监控，在此状态下微点主动防御软件不对系统提供防护功能。

 — 报警状态（红色图标）：提示微点主动防御软件监测到系统中存在有害程序或可疑程序。

 — 过期状态（灰色图标）：提示微点主动防御软件已经过期，此时必须重新购买新的微点主动防御软件重新安装或购买续费号进行续费才能继续使用。

 — 正在升级（红色闪动箭头）：提示微点主动防御软件正在进行升级。

 — 升级完成（绿色闪动箭头）：表示微点主动防御软件已经升级完成，正在退出升级程序。

右键菜单

为了方便用户的操作，微点主动防御软件在系统托盘处提供了丰富的右键操作功能。

鼠标右键单击系统托盘处的  图标，打开右键菜单，如图 21：

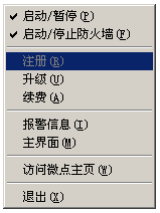


图 21

【启动/暂停】— 启动或暂时停止微点主动防御软件的实时监控。

【启动/停止防火墙】— 启动或停止微点主动防御软件的防火墙功能，默认情况下，不开启防火墙功能。

【注册】— 单击“注册”，进入产品注册向导，进行软件注册。详细参阅 2.3【注册软件】。

【升级】— 用于已知特征库、程序版本的立即升级，在注册成功并设置好升级方式以后，选择并执行此选项，若网络连接正常，程序会立即执行升级。

【续费】— 用户在这里通过简单的操作就可以实现续费，以获得继续使用微点主动防御软件的权利。详细参阅第 9 章【辅助功能】中的【续费】。

【报警信息】— 显示微点主动防御软件启动后记录的报警信息，报警信息窗口内的记录将在关机时自动清除。如图 22：

图 22

【主界面】— 打开微点主动防御软件的主界面。

【访问微点主页】— 单击进入微点公司网站。

【退出】— 关闭微点主动防御软件，退出后微点主动防御软件不再对系统提供安全保护。

第4章 软件设置

4.1 程序行为实时监控策略

微点主动防御软件是在对病毒行为规律分析、归纳、总结，并结合反病毒专家判定病毒经验的基础上，提炼成病毒识别规则知识库，创立了动态仿真反病毒专家系统。微点主动防御软件模拟专家发现新病毒的机理，通过分布在操作系统中的众多探针，动态监视所运行程序调用各种应用编程接口（API）的动作，自动分析程序动作之间的逻辑关系，然后自动判定程序行为的合法性，实现自动诊断新病毒，明确报告诊断结论，实时发现并拦截新有害程序（木马、蠕虫、后门、间谍、病毒），同时自动提取新有害程序的特征码，自动更新本地特征库。

在【安全防护与策略】中选择【程序行为实时监控策略】如图 23：

图 23

1) 发现有害程序处理方式

微点主动防御软件在发现有害程序时有三种处理方式：自动处理、采用静默方式、询问后处理，默认选项是“询问后处理”。

- 自动处理

“自动处理”是指微点主动防御软件在监控系统过程中，如果发现有害程序，自动拦截有害程序行为并将有害程序删除到【有害程序隔离区】

中，同时弹出警示框告知用户。

- 采用静默方式

“静默方式”是指微点主动防御软件在监控系统过程中，如果发现有害程序，自动拦截有害程序行为并将有害程序删除到【有害程序隔离区】中，不弹出警示框提示用户。

- 询问后处理

“询问后处理”是指微点主动防御软件在监控系统过程中，如果发现有害程序，弹出警示信息窗口，提示用户发现有害程序，并由用户选择处理方式。弹出的报警窗口按照预先设定的“询问等待时间”保留一定的显示时间，以便用户查看报警窗口的信息。该询问等待时间值的设置见“设置报警窗口的询问等待时间”。

2) 设置报警窗口的询问等待时间

询问等待时间是指有害程序报警窗口的显示时间。微点主动防御软件默认的“询问等待”时间是 48 秒，用户可根据情况自己定制 10-300 秒内的任意时间值，然后单击“保存”按钮，即可完成设置。

3) 报警时播放声音

“报警时播放声音”，即以声音的方式提示微点主动防御软件的报警事件。如果想使用声音提示，勾选此项后，并在后面的下拉菜单中选择相应的报警声音即可。

4) 上报截获的未知有害程序样本

对于确认删除的未知有害程序样本，微点主动防御软件提供三种处理方式：自动传送、智能询问处理、不传送，默认的处理方式是“自动传送”。

- 自动传送 — 即自动将捕获到的未知有害程序样本提交给微点公司。
- 智能询问处理 — 捕获到未知有害程序时，弹出信息提示框，询问用户是否将未知有害程序样本提交给微点公司。

- 不传送 — 不发送未知有害程序样本到微点公司。

5) 锁定系统时间

“锁定系统时间”即保护系统时间不被修改。启动“锁定系统时间”后，则禁止对系统时间进行修改设置。默认状态下，不启用此功能，用户可根据需要选择是否锁定系统时间。

6) 显示启动界面

微点主动防御软件在每次启动时，会弹出一个动态启动界面，提示用户已经启动微点主动防御软件，用户可根据情况自行选择启动时是否显示该启动界面。

7) 显示动态托盘图标

“显示动态托盘图标”即在系统托盘区，以动态方式（黄球循环滚动）显示微点主动防御软件的托盘图标。若取消此勾选，则以静态方式显示微点主动防御软件的托盘图标，用户可自行选择是否显示动态托盘图标。

8) 保存设置

修改设置后，请注意单击“保存设置”按钮，以保存您改变的设置。

4.2 可信程序设置

可信程序是由用户自己认可的一切可信任的程序文件，可信程序由用户自己添加。对于添加到“可信程序”列表中的程序文件，微点主动防御软件对其以可信模式监控。

在主功能区【安全防护与策略】中单击【程序行为实时监控策略】，在打开的标签页中单击“可信程序设置”按钮，打开【可信程序】窗口，如图 24：

图 24

【可信程序】的操作包含：添加、修改、删除。

1) 添加策略

【第一步】在【可信程序】窗口中，单击“添加”按钮，或单击鼠标右键选择“添加策略”，选择要添加为可信程序的程序文件。

【第二步】选择可信程序类型：选中程序后，单击“打开”按钮，微点主动防御软件提示如图 25，要求对选中的程序选择可信程序类型。

图 25

- 可信任程序 — 即由用户自己认可的一切可信任程序（不包含具有修改其他程序行为的程序）。
- 允许修改程序 — 即由用户自己认可的允许修改其他程序的可信程序。

【第三步】 选择完可信程序类型后，单击“确定”，完成可信程序的添加。

2) 修改策略

在【可信程序】窗口中，选中要修改的可信程序后，单击“修改”按钮，或单击右键菜单中的“修改策略”，修改可信程序的类型。

3) 删除策略

在【可信程序】窗口中，选中要删除的可信程序，单击“删除”按钮或单击右键菜单中的“删除策略”，则删除选中的可信程序。

单击右键菜单中“全部删除”，删除列表中所有的可信程序。

4.3 程序访问网络策略设置

【程序访问网络策略】是对系统中试图访问网络的进程设置访问网络规则。

4.3.1 设置程序访问网络策略

在【安全防护与策略】中单击【程序访问网络策略】，打开【程序访问网络策略】标签页，如图 26：

图 26

【程序访问网络策略】信息区的操作包含：添加、删除、修改、刷新。

1) 添加策略

【第一步】进程选择：单击“添加”按钮，在系统中选择要添加的应用程序。

【第二步】设置规则：添加应用程序后，单击“打开”，设置程序的网络访问规则，如图 27：

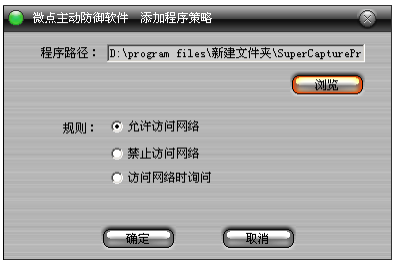


图 27

- 允许访问网络 — 允许所选程序访问网络。
- 禁止访问网络 — 禁止所选程序访问网络。
- 访问网络时询问 — 设置为此规则的程序访问网络时微点主动防御软件会弹出警示框如图 28 询问用户是否允许该程序访问网络。

图 28

【第三步】单击“确定”，完成程序规则的添加。

2) 修改策略

在程序规则信息区中，选择要修改的规则，直接单击“修改”按钮或单击鼠标右键选择“修改策略”，则弹出 【修改程序规则】对话框修改新的规则，然后单击“确定”，完成修改。

3) 删除策略

在程序规则信息区中，选择要删除的规则，直接单击“删除”按钮或单击右键菜单中的“删除策略”，删除所选程序访问网络策略。

单击右键菜单中的“全部删除”，删除列表中的所有程序访问网络策略。

4.3.2 智能识别功能

“智能识别”就是通过微点主动防御软件的动态仿真反病毒专家系统能够自动处理系统中可识别程序的访问网络行为，不需要用户参与。可识别程序包括：可信程序、已知程序（包括微点识别的系统程序和正常应用软件程序）。

勾选“智能识别”后，微点软件只对非可识别程序的访问网络行为弹出报警窗口询问用户，可识别程序访问网络行为将直接放行，减少了用户自行判断的烦恼。

【程序访问网络策略】默认设置开启了“智能识别”功能。若取消“智能识别”功能，则系统中任意进程访问网络时，微点主动防御软件都会弹出报警窗口询问用户。

4.4 传统防火墙

4.4.1 传统防火墙设置

微点主动防御软件提供的传统防火墙实时监控任何网络连接，过滤不安全的服务，减少计算机被攻击的风险，为计算机系统提供更全面的保护。

在【安全与防护策略】中单击【传统防火墙设置】，打开传统防火墙设置窗口，如图 29 所示：

图 29

1) 传统防火墙默认规则包

微点主动防御软件提供了五个规则包供用户选择，用户可以根据实际使用

环境选择不同的规则包，传统防火墙默认使用的规则包为：规则包（一）。为了确保用户安全，微点主动防御软件提供的五个默认规则包不允许进行任何更改。用户可以根据自己的需要，自行编辑定义新规则包，也可以采用另存方式，在微点主动防御软件提供的默认规则包的基础上编辑自己的防火墙规则策略。

规则包一：开放网络，不对进出数据包做任何限制。

规则包二：禁止网络，禁止任何数据包进出。

规则包三：允许本机连接共享，适用于局域网内部用户。

规则包四：适用于普通用户。

规则包五：关闭本机连接共享，适用于使用互联网的用户。

2) 使用防火墙规则包

- 新建规则包

  在“规则包列表”中，单击右键，选择“新建”，在打开的窗口中输入规则包名称及其对该规则包的描述信息后，单击“确定”，则新建一个空的规则包。

- 应用规则包

  在“规则包列表”中，选择要应用的规则包，单击右键，选择“应用”，或者直接单击快捷按钮应用列表中的规则包，提示“设置成功”的对话框，表示应用新规则包成功。

- 导入规则包

  在“规则包列表”中，单击右键，选择“导入”，打开【从文件导入规则包】窗口，选择需导入的规则包文件。

- 导出规则包

  在“规则包列表”中，选择要导出的规则包，双击该规则包，打开【编辑规则包】窗口，在编辑窗口中单击图标  ，将当前规则包导出到指定的磁盘目录，规则包的文件类型为.rpk。

- 另存规则包

在“规则包列表”中，选定一规则包后，单击右键菜单中的“另存”则可将已存在的规则包重命名后作为一个新的规则包加到“规则包列表”中，当需要对默认规则包进行重新编辑修改时，可使用此设置。

- 修改规则包

在“规则包列表”中选中要更改的规则包后，双击或选择右键菜单中“修改”，打开规则包的编辑窗口，可对规则包的各项规则进行修改。

微点提示： 传统防火墙的默认规则包不允许进行编辑修改，如需要编辑默认规则包，可将要更改的默认规则包“另存”后，进行编辑。

- 删除规则包

在“规则包列表”中选中自定义的规则包后，选择右键菜单中的“删除”，将选定的规则包从规则包列表中删除。

3) 编辑防火墙规则策略

双击“规则包列表”中的规则包名称，打开【编辑规则包】窗口进行编辑。

- 更改描述信息

单击“编辑规则包”窗口中的“描述”按钮，在打开的【规则包描述】对话框中修改规则包的描述信息。

- 新建规则

单击快捷图标  或单击右键菜单中的“新建策略”在弹出的【微点主动防御软件 地址规则】窗口中设定。

【第一步】填写规则名称及其描述信息。

【第二步】设置规则的条件：选择规则的数据包协议类型：TCP、UDP、IGMP、ICMP、IP。

【第三步】选择规则对哪个方向的数据包有效：发送、接收、双向。

【第四步】设置端口和地址。

【第五步】设置对规则的处理：拦截和放行。

- 【拦截】 — 阻止该数据包进入您的计算机。
- 【放行】 — 允许该数据包进入您的计算机。
- 【报警】 — 若勾选该项则实时在【传统防火墙信息】中显示防火墙拦截或放行的数据包信息。
- 【记日志】 — 若勾选该项，则将拦截或放行的数据包信息记录到【传统防火墙日志】中。

- 设置 IP 地址段

单击快捷图标  按钮，在弹出的【IP 地址段设置】窗口中，设置传统防火墙组策略的 IP 地址段。

- 设置端口段

单击快捷图标  ，在弹出的【端口段设置】窗口，设置传统防火墙组策略的端口段。

- 导入规则策略

单击右键菜单中的“导入策略”或者单击快捷图标  ，从微点主动防御软件提供的默认规则库中移入要导入的规则，单击“确定”按钮，将规则导入到自定义规则列表中。

微点主动防御软件对应用程序访问不同地址和端口设置了两条特殊规则即：允许可识别程序通过（TCP）、允许可识别程序通过（UDP）。

在这里提及到的可识别程序是指：可信程序、已知程序、以及“程序访问网络策略”中允许访问网络的应用程序。为了减少用户对网络访问报警处理的参与，可识别程序的网络访问将被全部允许，不受后面其他规则对端口、协议及访问地址的限制。

微点建议：在您创建自己的规则包时，建议您导入“允许可识别程序通过（TCP）”和“允许可识别程序通过（UDP）”两条规则。

- 修改规则策略

单击右键菜单中的“修改策略”或者单击快捷图标  ，对所选策略进行修改。

- 调整规则优先级

单击右键菜单中的“上移”将提高选中规则的优先级，单击“下移”将降级选中规则的优先级；也可以单击快捷图标（  ：上移选定的规则  ：下移选定的规则）完成同样的功能。

- 删除规则策略

选择要删除的规则策略后，单击右键菜单中“删除策略”，或者单击快捷按钮  ，将所选策略删除。

- 保存规则包策略

编辑完成规则包策略后，单击“保存”按钮或者单击快捷图标  ，保存对当前规则包的修改。

- 取消对规则包策略的更改

点击“取消”按钮或者单击快捷图标  ，则放弃对当前规则包所做的修改。

4) 恢复传统防火墙的默认设置

单击【传统防火墙设置】标签页上的“恢复默认设置”，则恢复到传统防火墙的初始设置。

4.4.2 绑定MAC地址

微点主动防御软件的传统防火墙提供了绑定 MAC 地址的功能，通过将 IP 地址与 MAC 地址绑定，防御局域网内的 arp 欺骗。

在【传统防火墙设置】窗口中，单击“绑定 MAC 地址”按钮，打开如图

30：

图 30

启用 IP 与 MAC 地址的绑定

单击“刷新网关”或“查找所有主机”搜寻局域网内的其他计算机的 IP 地址以及其对应的 MAC 地址的列表，单击中间的方向按钮，将其移动到左边的列表，勾选“启用绑定”，单击“应用”按纽，实现对左边列表中的 IP 与 MAC 地址的绑定。

您也可以在两边的列表中，单击右键菜单中的“添加”，手工添加要绑定的 IP 地址和 MAC 地址，进行绑定。或者单击右键菜单中的“修改”或“删除”，对列表中的信息进行更改和删除操作。

4.5 有害程序隔离区

微点主动防御软件对于确认删除的有害程序直接将其删除到微点主动防御软件的【有害程序隔离区】，放置在【有害程序隔离区】中的文件都经过特殊格式保存，不会对系统造成任何影响。

4.5.1 隔离区文件管理

单击【安全防护与策略】中的【有害程序隔离区】，打开【有害程序隔离区】标签页，如图 31，对隔离区的文件进行备份、恢复、删除以及样本上报等管理。

图 31

隔离区文件管理

- 另存为 — 将有害程序隔离区信息列表中选定的文件另存到指定目录。
- 恢复所选 — 将有害程序隔离区列表中选定的文件恢复到原目录。
- 全部恢复 — 将有害程序隔离区列表中的所有隔离文件全部恢复到原目录。
- 删除所选 — 将选定的隔离文件从有害程序隔离区列表中彻底删除。
- 全部删除 — 彻底删除当前有害程序隔离区列表中的所有隔离文件。
- 上报样本 — 将有害程序隔离区列表中的病毒文件上报给微点公司。

4.5.2 隔离区设置

单击【有害程序隔离区】中的“设置”按钮，弹出【隔离区大小设置】窗口，如图 32，用户可根据情况自行设置隔离区空间的大小以及隔离区的存储路径。

图 32

设置隔离区

1) 设置隔离区存储路径

单击“浏览”按钮，在磁盘中选择隔离文件的存储位置。

2) 隔离区尺寸的设置

- 自动调整隔离区大小

  默认的设置方式，即隔离文件可存储在磁盘自由使用区内，隔离区空间的大小只跟磁盘的自由使用区的大小有关。

- 限定隔离区大小

  即对隔离区的大小作限制，隔离文件只能存储在限定的空间中，拖动隔离区尺寸设置图中的分割线来设置隔离区、自由使用区、分区保留区的大小。

  - 隔离区 — 用来存储被隔离的有害程序的空间。
  - 自由使用区 — 用于扩充隔离区的使用空间。
  - 分区保留区 — 磁盘保留的空间。
  - 当前分区空闲空间 — 隔离区所在的磁盘分区的剩余空间。

3) 保存设置

单击“应用”按钮，保存对隔离区更改设置。

微点提示：当隔离区内各文件字节之和超过隔离区空间后，微点软件会自动删除

最早的隔离文件，放入新的隔离文件。

4.6 自启动项回收站

【自启动项回收站】是用于存储用户从【系统自启动信息】中自行右键删除的自启动信息的空间，放置在【自启动项回收站】的文件都经过特殊格式保存，不会对系统造成任何影响。

单击【安全防护与策略】中的【自启动项回收站】，打开【自启动项回收站】标签页，如图 33 所示，对【自启动项回收站】的文件进行删除、备份、恢复，刷新等管理。

图 33

自启动项回收站文件管理

- 另存为 — 将回收站列表中选定的隔离文件另存到指定目录。
- 恢复所选 — 如果用户误操作右键删除了自启动信息，点击“恢复所选”将误删除的自启动信息恢复。
- 全部恢复 — 如果回收站的文件都是用户误操作删除的自启动信息，请单击“全部恢复”将所有自启动文件恢复。
- 删除所选 — 彻底删除当前回收站列表中选定的隔离的自启动信息。
- 全部删除 — 彻底删除当前回收站列表中所有隔离的自启动信息。
- 上报样本 — 将回收站列表中选定的隔离文件上报给微点公司。

4.7 升级设置

微点主动防御软件提供在线升级和离线升级两种形式，升级包含病毒特征库的升级和程序文件的升级。请您及时升级，以便微点主动防御软件能够给您更安全的防护。

4.7.1 在线升级设置

“在线升级”是指在计算机连接互联网的前提下，启动在线升级程序，通过互联网直接连接到微点网站下载升级数据，自动升级微点主动防御软件。

单击【辅助功能】中的【升级设置】，打开升级设置标签页，如图 34 所示：

图 34

图 34 显示的是默认的升级设置方式，大多数用户可直接采用默认的设置方式进行升级，无须更改。

1） 选择升级方式

微点主动防御软件提供了如下三种升级方式供用户选择：

- 自动实时升级

  默认的升级方式，启用“自动实时升级”，在网络连接正常的情况下，微点主动防御软件直接连接到微点网站自动下载升级数据，并自动升级。微点公司建议用户采用“自动实时升级”方式实时对微点主动防御软件进

行更新，更好地对您的系统安全提供防护。

- 定时升级

“定时升级”是指在设定的时间间隔内，定时对微点主动防御软件进行升级，微点主动防御软件默认定时升级时间间隔是 14 天，用户可自行修改定时升级时间间隔，微点主动防御软件将在您设定的时间间隔里自动下载升级文件，并自动升级。

- 手动升级

“手动升级”即关闭微点主动防御软件的自动升级功能。设置手动升级后，需要升级微点主动防御软件的时候可单击主界面上的“升级”按钮或托盘区  右键菜单中的“升级”进行升级。

- 启用重要更新

在“升级方式”设置为“定时升级”或“手动升级”的状态下，将提供一个可选项“启用重要更新”。勾选此项后，微点主动防御软件将对重要更新进行自动升级。此选项默认为勾选状态。

2） 设置代理服务器

用户若采用代理服务器的方式进行升级，就需要设置代理服务器，详情可咨询您的上网服务提供商或网络管理员。

- 使用系统代理设置

系统代理是指当前系统正在使用的代理（一般是 Internet Explorer 正在使用的代理地址），单击右边的“使用系统代理设置”，软件会自动提取系统代理相关设置信息，无需用户手工输入，单击“保存按钮”完成系统代理设置。

- 手动设置代理服务器

当用户使用特定的代理服务器时，在代理服务器选项中，选择代理类型（ Sock4、Sock5、HTTP ），然后对代理服务器的相关参数进

行设置：

【代理服务器地址】 — 代理服务器的 IP 地址。

【端口】 — 代理服务器提供的代理服务的端口号（0－65535）。

【用户名】 — 访问代理服务器的用户名。

【口令】 — 访问代理服务器的密码。

【域】 — 代理服务器的域名。

- 测试代理服务器

代理服务器设置完毕，请单击“测试代理连接”测试您设置的代理服务器是否能够正常使用。

3） 高级设置

在【升级设置】信息区中单击“高级按钮”打开如下图 35：

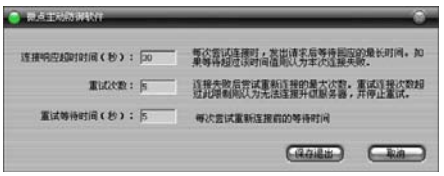


图 35

在“高级”设置窗口中包含的信息：连接响应超时时间、重试次数、重复等待时间，用户可根据实际情况进行修改。

【响应超时时间】 — 微点主动防御软件升级时，在对微点软件升级服务器发出连接请求后，等待回应的最长时间。达到此时间依然没有回应则认为此次连接失败。微点主动防御软件连接东方微点升级服务器默认响应的超时时间为 30 秒。

【重试次数】 — 微点主动防御软件如果第一次连接失败，允许重试连接的次数。微点主动防御软件连接微点软件升级服务器的默认重试连接次数为 5 次。

【重试等待时间】 — 第一次连接失败到第二次重新尝试连接微点软件升

级服务器所需要的等待时间。默认的重试等待时间是 5 秒。

4） 保存设置

设置完成后，请单击“保存设置”，保存当前的升级设置。

4.7.2 离线升级

如果您的计算机不能连接互联网，您可以使用“离线升级”的方式对软件进行升级。请找一台可以连接互联网的计算机，进入微点网站下载升级包，拷贝到本地计算机，然后单击主界面菜单栏【辅助功能】下拉菜单中的【离线升级】，依据提示选择已下载的升级包文件，进行软件升级。

第5章 报警处理

微点主动防御软件采用以动态仿真反病毒专家系统判断为主、结合特征码判断技术为辅的方式，实时监控系统所有进程的动作，实时发现并拦截已知有害程序、未知有害程序。微点主动防御软件主要采用以下方式判断有害程序：

1） 已知特征库判断：

使用已知有害程序特征库进行扫描，如果监测是已知有害程序，立即阻止该程序的运行并报告有害程序名称，对该程序及相关文件做相应的处理，然后将处理结果写入日志。

2） 未知特征库判断：

使用已知特征库扫描后，继续使用未知特征库扫描。未知特征库中特征码的来源见【5）自动更新本地特征库】。

3） 程序行为特征判断：

在使用已知和未知病毒库扫描后，微点主动防御软件通过动态仿真反病毒专家系统实时监控系统的所有进程，及时发现并拦截新的有害程序。

4） 自动提取特征码：

微点主动防御软件确定某进程为未知有害程序后，能够自动提取该有害程序的特征码。

5） 自动更新本地特征库：

微点主动防御软件自动提取新有害程序特征码后，自动更新本地未知特征库，当该有害程序再次攻击或感染时有利于快速检测。

5.1 有害程序的报警

5.1.1 已知有害程序报警及处理

微点主动防御软件使用已知特征库检测到已知有害程序，自动阻止该有害程序的运行，并弹出报警窗口（如图 36）报告有害程序类别、名称以及有害程序源文件及其路径，提示用户删除该有害程序文件，并将处理结果记录到相应类别的【安全日志】。

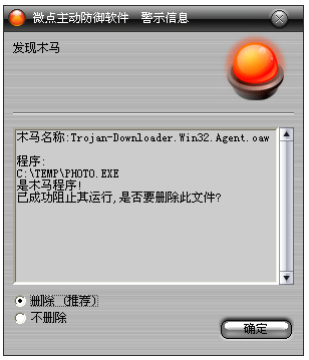


图 36

5.1.2 未知有害程序报警及处理

微点主动防御软件通过动态仿真反病毒专家系统发现未知有害程序时，立即结束该有害程序的运行，并弹出警示信息窗口（如图 37）提示用户对该未知有害程序及其生成文件做出处理，同时将处理结果记录到相应类别的【安全日志】。

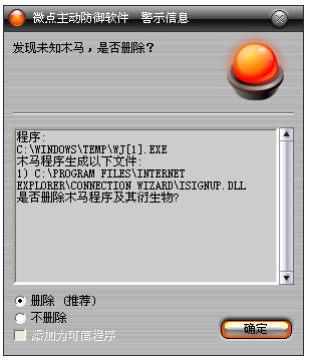


图 37

【删除】— 将未知有害程序及其生成文件删除到【有害程序隔离区】，同时提取该有害程序的特征码，添加到本地的未知有害程序特征库中，若该有害程序再次对系统进行攻击，微点主动防御软件直接利用本地特征库快速检测有害程序，弹出报警窗口（如图 38）提示用户删除该未知有害程序。

图 38

【不删除】 — 结束未知有害程序的运行，不删除未知有害程序。如果该有害程序再次运行，微点主动防御软件将会再次弹出报警信息，提示该程序为未知有害程序，要求用户对其进行处理。

【不删除＋添加为可信程序】 — 选择“不删除”并勾选“添加为可信程序”，微点主动防御软件结束该程序的运行，并将该程序加入到【可信程序】。以后若该程序再次运行时，微点主动防御软件将对该程序的动作行为采用可信任模式进行监控。

5.1.3 漏洞攻击的报警及处理

在监控到来自远程计算机利用本地计算机系统的漏洞对系统进行攻击时，微点主动防御软件会立即阻断攻击，并弹出如图 39 所示的报警窗口提示用户：发现并阻止了本地程序被远程溢出攻击，同时记录拦截日志到【溢出日志】中。

图 39

在阻止远程计算机的第一次远程攻击后，微点主动防御软件会自动提取远程网络攻击数据包的特征，如果黑客继续利用同一个漏洞进行攻击，微点主动防御软件在阻止黑客下一次攻击的同时会直接捕获到攻击本地计算机的远程 IP 及其端口，如图 40，同时记录拦截日志到【网络入侵日志中】中。

图 40

微点提示：勾选“下次不再询问”，再出现同样的攻击时，微点主动防御软件会自动在后台阻断攻击，而不再弹出报警信息窗口。

5.1.4 可疑程序的报警及处理

在监测到系统中危险程度高但又不足以准确判定为未知有害程序的进程时，微点主动防御软件会弹出可疑程序的报警窗口（如图 41），并将处理结果写入【可疑程序日志】。

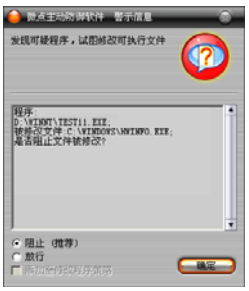


图 41

【阻止】— 阻止该程序的可疑动作，用户选择阻止后，微点弹出如图 42 所示警示框，要求对该进程进行处理（删除或不删除）。

图 42

【放行】 — 允许该程序的本次的可疑动作。

【放行+添加至修改程序策略】— 选择“放行”和“添加至修改程序策略”后，则允许该进程的动作继续，并产生该进程的允许策略自动添加到【可信程序】中。对添加到【可信程序】中的程序，微点主动防御软件将对其以可信模式进行监控。

5.1.5 发现远程安装程序的报警及处理

微点主动防御软件在监测到有来自其他计算机通过网络向本计算机系统安装程序

时，立刻会弹出报警窗口（如图 43），用户可对远程安装程序做出“放行”或“阻止”的处理。

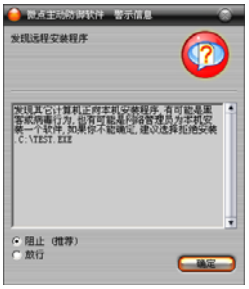


图 43

【阻止】 — 阻止远程安装程序的运行。

【放行】 — 允许远程安装程序的运行。

微点提示：黑客等攻击者常常采用远程安装的手段将木马等有害程序植入受害者计算机，当微点主动防御软件弹出“发现远程安装程序”报警时，如果不能确认是可信任的远程安装，建议立即阻止，防止有害程序对系统的破坏。

5.1.6 修改注册表的报警及处理

微点主动防御软件提供的【注册表保护】功能，实时监控注册表项的修改状态，当设置为“保护”状态的注册表项被其他程序或手工修改时，会弹出报警窗口（如图 44）提示用户：系统中有程序正在修改某一注册表项，用户可做出“阻止”或“放行”的处理。

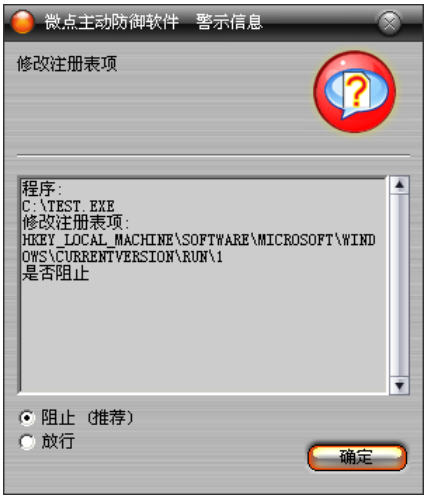


图 44

【阻止】 — 阻止当前进程对注册表项的修改。

【放行】 — 允许当前进程对注册表项的修改。

5.2 异常网络访问行为的报警及处理

微点主动防御软件防火墙监测到系统中有可疑程序试图访问网络时，会弹出报警窗口（如图 45），用户可对该程序的网络行为做出放行或阻止处理，并将处理结果记录到【异常网络访问日志】中。

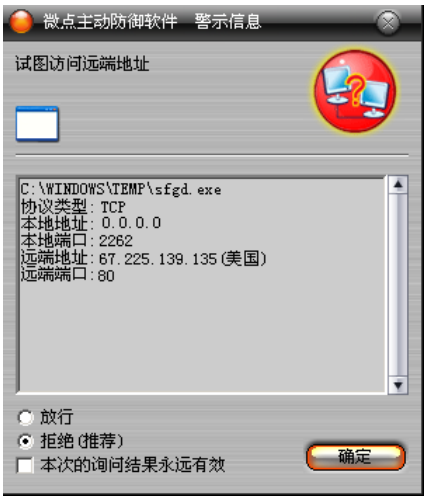


图 45

【放行】 — 允许该程序的本次网络访问行为，若该进程再次访问网络时，会再次弹出报警信息。

【拒绝】 — 禁止该进程的本次网络访问行为，若该进程再次访问网络时，会再次弹出报警信息。

【放行+本次的询问结果永远有效】 — 选择“放行”并勾选“本次的询问结果永远有效”，则永远允许该进程访问网络，并添加一条允许访问网络策略到【程序访问网络策略】中。

【拒绝+本次的询问结果永远有效】 — 选择“拒绝”并勾选“本次的询问结果永远有效”，则永远禁止该进程访问网络，并添加一条禁止网络访问策略到【程序访问网络策略】中。

5.3 未知病毒命名更新

对于微点主动防御软件自动捕获的未知有害程序，微点公司获取样本后将对该有害程序命名，并通过升级方式更新已知病毒特征库。

升级后将自动对【安全日志】的相关记录进行更新（如图 46）。

图 46

并弹出如图 47 所示窗口告知用户：您计算机上已成功删除的未知有害程序已经命名。

图 47

第6章 微点工具

6.1 可疑程序诊断

可疑程序指的是具有类似病毒、木马、蠕虫行为但还不足以准确判定为新病毒、木马、蠕虫的程序。

诊断系统进程，可及时发现当前运行程序中具有类似病毒、木马等危险动作的进程，发现系统存在的潜在威胁，协助用户有针对性地对可疑程序做进一步的分析和处理。

6.1.1 执行可疑程序诊断

可疑程序诊断操作步骤：

【第一步】执行可疑程序诊断：在【安全防护与策略】的子功能项中单击【可疑程序诊断】，开始对系统中的进程进行诊断；

【第二步】查看诊断结果：诊断结束，显示诊断结果并在信息区显示诊断出的可疑程序的 PID（进程号）、全路径以及该进程的可疑行为，如图 48。

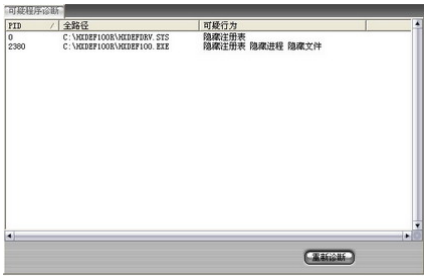


图 48

6.1.2 分析诊断结果

在您进行可疑程序诊断后，如果微点主动防御软件报告有可疑程序时，建议您将可疑程序发送到微点公司，或者依照下述步骤进行分析，对可疑程序作进一步判断和处理。

【第一步】分析可疑程序的当前信息：

在【可疑程序诊断】的详细信息区中鼠标指向“可疑程序”后单击右键，在弹出的菜单中选择“进程信息”，打开所选可疑程序的进程信息窗口，如图 49 所示。通过对进程信息中的内容进行初步分析，详细了解该进程运行后的动作结果，为进一步判断提供信息。

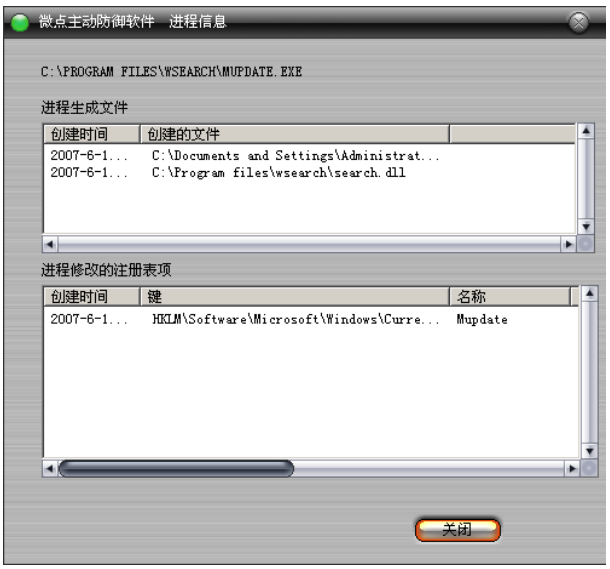


图 49

进程信息记录程序从程序最后一次启动到当前时间，该程序修改注册表项和生成可执行文件的历史信息。包含：进程生成文件、修改的注册表项：

【进程生成文件】——可疑进程生成的文件。

【进程修改的注册表项】——可疑进程修改的注册表项。

为了便于做出进一步的判断，用户可结合查看【进程综合信息】(可疑程序属

于其他软件）、【进程网络信息】、【端口流量图】、【进程流量图】等功能模块提供的信息进行综合分析。

【第二步】分析可疑程序的历史信息：

在【可疑程序诊断】的详细信息区中鼠标指向可疑程序后单击右键，在弹出的菜单中选择“程序信息”，打开所选可疑程序的程序信息窗口，如图 50 所示。通过对程序信息中的内容进行分析，详细了解该进程的历史动作，为进一步判断提供信息。

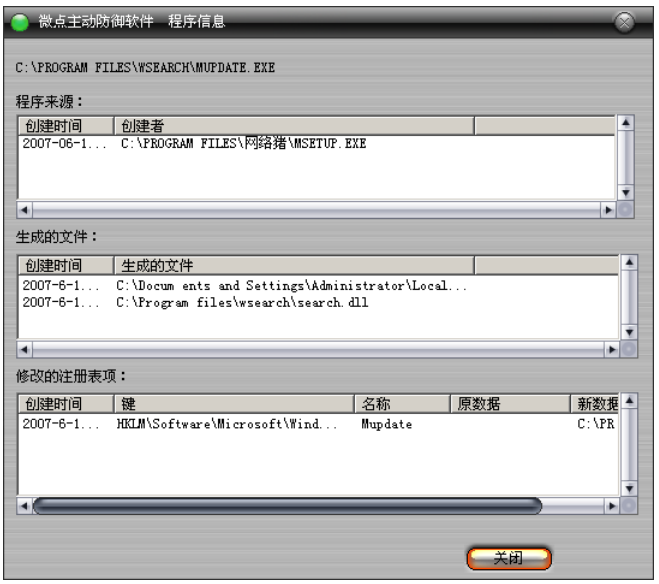


图 50

程序信息记录是从第一次程序运行开始到当前时间，该程序修改注册表项和生成可执行文件以及该程序来源的全部历史信息。

【程序来源】— 可疑程序的来源，即生成可疑程序的源程序。包含可疑程序创建时间以及创建可疑程序的源程序全路径。

【生成的文件】— 记录可疑程序生成的所有文件。包含生成文件的创建时间以及全路径。

【修改的注册表项】— 记录可疑程序修改的注册表项。

另外，也可通过查看【程序生成日志】、【进程启动日志】、【注册表变更日志】对可疑程序的来源、启动信息、行为动作做进一步分析，从而得出正确的判断。

6.1.3 处理可疑程序

在对诊断做出正确的分析判断后，即可对诊断出的可疑程序做相应的处理。在【可疑程序诊断】的详细信息区中鼠标指向可疑程序后单击右键，弹出如图 51 所示的右键菜单：

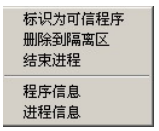


图 51

1) 标识为可信程序

如果确认所判断的可疑程序为正常进程，单击“标识为可信程序”，则自动将所选可疑程序添加到【可信程序】中，添加成功提示如图 52：

图 52

2) 删除到隔离区

【第一步】选择可疑进程，鼠标右键弹出的菜单中选择“删除到隔离区”后，弹出提示是否将可疑程序上报微点公司，如图 53：

图 53

【第二步】单击“是”，微点主动防御软件会自动将可疑程序的样本上报给微点公司，并提示用户对可疑程序进行处理，如图 54：

图 54

【第三步】删除可疑程序文件：在图 54 中单击“确定”，则删除可疑程序文件。

3) 结束进程

结束进程即停止当前可疑程序的运行。

操作步骤：

【第一步】选择可疑进程，在右键弹出的菜单中选择“结束进程”后，微点主动防御软件会弹出如图 55 提示框：

图 55

【第二步】单击“确定”按钮，结束进程，微点主动防御软件弹出是否将可疑程序上报微点公司的提示框，如图 56：

图 56

【第三步】要上报微点公司请单击“是”，不上报单击“否”。

6.2 漏洞扫描

【漏洞扫描】是对 Windows 系统中存在的已知系统漏洞进行检查，并提供相应的补丁下载链接。建议用户通过补丁列表信息下载并安装补丁，以提高操作系统的安全性。

6.2.1 启动漏洞扫描

在【安全防护与策略】的子功能项中选择【漏洞扫描】后，即可启动系统的漏洞扫描。扫描结束，在漏洞扫描标签页中显示详细的安全漏洞信息及其链接，如图 57 所示：

图 57

6.2.2 修补漏洞

【第一步】查看漏洞补丁的详细信息：单击“在浏览器中打开”，打开漏洞补丁的详细说明的网页，了解漏洞补丁的详细说明。

【第二步】下载漏洞补丁：在漏洞扫描详细信息区中选择要下载的补丁，单击“下载补丁”，微点主动防御软件会自动链接到微软的官方网站下载最新补丁；

【第三步】修补漏洞：将漏洞补丁下载到本地以后，双击该补丁，即可运行补丁程序，完成漏洞的修补。

6.2.3 导出漏洞信息列表

【第一步】在漏洞扫描详细信息区中，单击“导出”按钮，选择本地的保存路径并输入文件名：程序会自动命名导出文件，也可由用户自定义文件名，文件的格式为

html；

【第二步】单击“保存”，微点主动防御软件提示“导出文件成功”，则将漏洞列表导出到用户指定的存储路径。

6.3 注册表修复

微点主动防御软件提供的注册表修复工具主要用于解决系统中的注册表项被程序恶意修改，导致系统的一些重要功能不能正常使用的问题。

在【系统分析】中，单击【注册表修复】工具，打开如图 58 所示的标签页：

图 58

【注册表修复】功能包含：锁定、解锁以及修复。

1) 解锁

某些恶意网页或病毒会造成 IE 主页、注册表、任务管理器等重要功能项的锁定，在注册表修复列表中，勾选当前值为“锁定”的项目，然后单击“解锁”按钮，解除被锁定的注册表项。

2) 锁定

对系统中的某些重要功能进行屏蔽。如：“注册表锁定”启用后，则无法使用编辑器对注册表进行修改。用户可根据需要自行锁定某些功能，以防止他人或恶意软件对系统进行某些修改或破坏。

3) 修复

修复被恶意更改的重要注册表项，在发现 IE 设置项等被恶意的更改时，请勾选要修复的项目，单击“修复”，即可修复所选项目。

6.4 注册表保护

微点主动防御软件提供的【注册表保护】工具主要为系统的一些重要注册表项提供保护功能，防止系统中一些重要的注册表项被恶意程序修改。

在【系统分析】中，单击【注册表保护】，打开如图 59 所示的标签页：

图 59

1) 保护注册表项

勾选要保护注册表项后，单击“保护”按钮，完成注册表项的保护，此时注册表项的“保护状态”显示为“保护”，对于设置为保护的注册表项，在被其他程序修改时，微点主动防御软件会立即弹出报警信息阻止修改。

2) 取消注册表的保护

勾选列表中状态为“保护”的注册表项，单击“取消保护”按钮，此时注册表项的“保护状态”显示为“未保护”，则取消了当前注册表项的保护。

第7章 进程分析

微点主动防御软件为用户提供了详细了解与分析系统所有进程运行状态的工具，主要包括【系统分析】和【网络分析】两大分析工具，用户通过分析工具提供的信息，可以详细了解进程的运行状态、启动模式、程序生成时间，以及生成关系、进程与模块的关系、进程的网络访问等等信息，用户可通过分析这些信息直观掌握当前系统中进程的运行状态，能够自行分析判断系统的安全性。

7.1 系统分析

【系统分析】提供了【进程综合信息】、【系统自启动信息】、【模块/进程】、【系统信息】四种进程分析工具，系统分析工具是对系统中当前所有进程的运行状况、程序及进程信息、进程启动模式、进程与模块的关系、进程网络连接状态等信息全面分析的工具，是用户学习系统知识的工具。

7.1.1 进程综合信息

【进程综合信息】对系统当前进程进行分类管理，显示进程的网络连接情况、端口信息、网络流量、以及每个进程的本地路径等详细信息，并显示相应进程所调用的模块信息。

通过查看【进程综合信息】用户可以了解系统当前进程的运行状况，并可自行分析判断系统中的可疑进程。

进程综合信息主要包含三个区域：①进程列表区、②进程详细信息区、③模块信息区，如图 60：

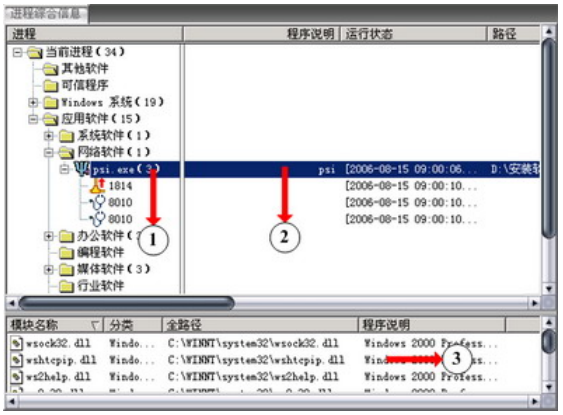


图 60

①进程列表区是以树状索引结构根据进程的不同特性分类显示系统中当前运行的所有进程。

②进程详细信息区显示系统中当前运行进程的详细信息。

③模块信息区显示进程列表区中的进程所调用模块的详细信息。

7.1.1.1 进程分类

微点主动防御软件将系统中的进程划分为四大类：其他软件、可信程序、Windows 系统软件、应用软件。

- 其他软件 — 微点主动防御软件不能识别的进程，这些进程包含用户安装的某些行业性软件、可疑进程。
- 可信程序 — 用户自己认可并添加到【可信程序】列表中的进程。
- Windows 系统软件 — 所有正在运行的 Windows 系统进程。
- 应用软件 — 微点主动防御软件能够识别的当前系统中正在运行的应用软件的进程。根据软件的特点微点主动防御软件将其规划为八类：系统软件、网络软件、办公软件、编程软件、媒体软件、行业软件、游戏软件、安全软件。

7.1.1.2 进程综合信息的描述

1) 进程文字颜色描述

- 蓝色文字 — “其他软件”的进程信息。
- 黑色文字 — 正常软件的进程信息。
- 蓝色高亮 — 被选中的进程信息。

2) 网络端口图标描述

-  — 端口正在连出。
-  — 端口正在连入。
-  — 端口处在监听状态。

7.1.1.3 进程综合信息的操作

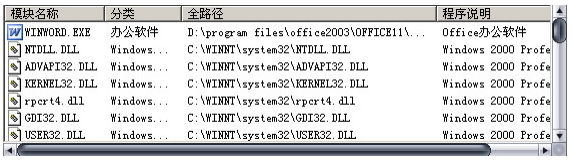
【进程综合信息】中提供了丰富的操作功能方便用户对系统中的进程进行查看、分析判断。

1) 查看文件属性

将鼠标轻移到进程综合信息中任意进程或模块的名称上，即可显示该进程或模块的文件自述、产品名称、描述、公司名称、文件版本，以及进程（或模块）启动/退出时间。

2) 查看进程调用的模块信息

在“进程列表区”选择要查看的进程，单击该进程名称，在模块信息区显示该进程所调用模块信息，如图 61 显示进程 WINWORD.EXE 所调用的模块信息。



模块名称	分类	全路径	程序说明
WINWORD.EXE	办公软件	D:\program files\office2003\OFFICE11\...	Office办公软件
NTDLL.DLL	Windows...	C:\WINNT\system32\NTDLL.DLL	Windows 2000 Profe
ADVAPI32.DLL	Windows...	C:\WINNT\system32\ADVAPI32.DLL	Windows 2000 Profe
KERNEL32.DLL	Windows...	C:\WINNT\system32\KERNEL32.DLL	Windows 2000 Profe
rpcrt4.dll	Windows...	C:\WINNT\system32\rpcrt4.dll	Windows 2000 Profe
GDI32.DLL	Windows...	C:\WINNT\system32\GDI32.DLL	Windows 2000 Profe
USER32.DLL	Windows...	C:\WINNT\system32\USER32.DLL	Windows 2000 Profe

图 61

3) 字段栏右键菜单

鼠标右键单击【进程综合信息】中的标签页字段栏，在弹出的列表中选择要显示的字段信息（如图 62）。用户可以自己定制进程详细信息区所要显示的字段内容。

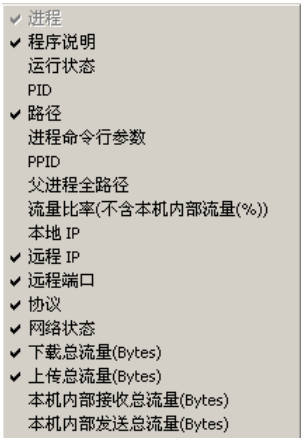


图 62

【程序说明】— 描述进程的类别名。

【流量比率】— 进程的总流量占本计算机总流量的百分比。

【PID】— 进程号。

【PPID】— 父进程号。

【本地IP】— 本计算机的IP地址。

【远程IP】— 远程计算机的IP地址。

【远程端口】— 连接的远程计算机的端口。

【协议】— 进程访问网络时所采用的协议，包含的协议：TCP、UDP、RAW。

【运行状态】 — 进程当前状态。包含两种状态：进程启动日期－时间－运行、进程启动日期－时间－停止。

【父进程全路径】— 父进程的绝对路径。

【路径】— 进程的绝对路径。

【进程命令行参数】— 显示执行当前进程的运行参数。

【网络状态】— 包含连入、连出、监听三个状态。

【上传总流量】— 显示进程的上传总流量。

【下载总流量】— 显示进程的下载总流量。

【本机内部接收总流量】 — 显示进程循环地址的接收总流量。

【本机内部发送总流量】 — 显示进程循环地址的发送总流量。

4) 查看进程状态信息

方式一：通过定制标签页字段栏中的显示字段，在详细信息区中查看进程的状态信息。

方式二：双击“②进程详细信息区”中要查看的进程记录，显示进程状态信息。

5) 进程列表区右键菜单

在①进程列表区，选择列表中的任意进程，单击右键，弹出如图 63 所示操作列表。

图 63

- 程序信息 — 显示从微点主动防御软件安装之后监控到的当前进程的所有信息，包括程序来源、创建时间、修改的注册表项。
- 进程信息 — 显示当前进程的状态，包含该进程本次运行时生成的文件和修改的注册表项。
- 流量图 — 动态显示所选进程的所有本地端口的网络流量情况。流量的操作方式请参看【网络分析】中的【流量图】。
- 结束进程 — 在右键菜单中选择“结束进程”或“结束进程树”，结束所选进程的运行。
- 查找目标 — 打开资源管理器，搜索并定位到所选进程的路径。
- 添加到可信程序 — 在“其他软件”类别中，选择右键菜单中的“添加到可信程序”将选中的“其他软件”的进程， 添加到可信程序中。

  您也可以直接在“可信程序”列表中删除可信程序，详细请参考【可信程序设置】。
- 从可信程序移除 — 在 “可信程序”类别中，选择右键菜单中的“从

可信程序中移除”，将选中的进程从可信程序策略列表中删除。

您也可以直接在“可信程序”列表中删除可信程序，详细请参考【可信程序设置】。

6) 模块信息区右键菜单

在①进程列表区选定一进程后，在③模块信息区单击右键可对该进程调用的模块进行如下操作。

- 隐藏已知的模块信息 — 只显示所选进程调用的“其他软件”的模块信息。
- 显示所有模块信息 — 显示所选进程调用的所有模块信息。
- 查找目标 — 打开资源管理器，搜索并定位到所选模块的路径。

7.1.2 系统自启动信息

自启动信息是指那些未经用户执行，随 Windows 操作系统启动而自动加载的文件，有些自启动程序则是在后台运行，用户根本感觉不到。正因为这个特点，绝大多数恶意程序都利用自启动方式实现其危害的目的。微点主动防御软件的【系统自启动信息】模块可以作为用户分析系统中某进程是否为类似于木马或蠕虫等有害程序的判断依据之一。

在【系统自启动信息】中用户可查看自启动程序的相关信息，如图 64。

图 64

1) 系统自启动信息颜色描述

- 蓝色文字 — “其他软件”的自启动信息。
- 黑色文字 — 已知程序的自启动信息。
- 红色文字 — 隐藏注册表或者隐藏文件的自启动信息。
- 灰色文字 — 文件已经不存在但注册表键值仍存在的自启动信息。

2) 查看系统自启动信息的文件属性

将鼠标轻移到【系统自启动信息】列表中的任意自启动程序的名称上，即可显示该自启动程序的文件自述、产品名称、描述、公司名称、文件版本。

3) 右键菜单

- 隐藏已知/显示所有启动信息
  - 隐藏已知的启动信息：隐藏【系统自启动信息】列表中已知的启动信息，仅显示归类为“其他软件”的启动信息。
  - 显示所有启动信息：显示当前【系统自启动信息】列表中所有的启动信息。
- 导出启动信息
  - 导出“其他软件”启动信息：将归类为“其他软件”的启动信息以 txt 文本方式导出到磁盘的指定目录。

- 导出所有启动信息：将当前【系统自启动信息】列表中所有的启动信息以 txt 文本方式导出到磁盘的指定目录。

- 删除自启动信息

对于归类为“其他软件”的自启动信息，微点主动防御软件提供了右键删除的功能，可对其注册表键值以及文件进行手工删除。

- 仅删除自启动项：将选定的自启动程序的注册表键值删除到【自启动项回收站】中。
- 删除文件与自启动项：将选定的自启动程序的文件以及其注册表键值全部删除到【自启动项回收站】中。

- 查找目标

打开资源管理器搜索并定位到所选自启动程序中涉及的程序文件的路径。

4) 修改注册表键值

鼠标左键双击【系统自启动信息】详细信息区中的任意一项记录，可以直接打开 Windows 的注册表编辑器，并准确定位到该项记录的注册表键值，用户可以对该项记录的注册表键值做修改和删除操作。

微点提示：对于不熟悉注册表修改的用户，我们强烈建议您不要对注册表做任何修改操作，以免因误操作造成系统瘫痪或软件不能正常使用。

7.1.3 模块/进程

【模块 / 进程】显示当前系统中已载入的所有模块以及调用这些模块的进程。

单击主功能区【系统分析】中的【模块 / 进程】，打开【模块 / 进程】标签页，显示如图 65：

图 65

1) 查找目标

打开资源管理器搜索并定位到所选模块的路径。

2) 查看调用模块的进程信息

在模块信息区，单击要查看的模块，在进程信息区可以看到当前正在调用该模块的所有进程的详细信息，如图 66 表中显示的是正在调用 ntdll.dll 模块的所有进程的信息。

图 66

3) 隐藏已知/显示所有模块信息

- 隐藏已知的模块信息 — 只显示当前系统中“其他软件”（微点主动防御软件不能识别）的模块信息。
- 显示所有模块信息 — 显示当前系统中所有模块信息。

4) 进程信息区的右键菜单

- 程序信息 — 查看所选进程的程序信息。
- 进程信息 — 查看所选进程的进程信息。

- 结束进程 — 结束所选进程的运行。
- 查找目标 — 打开资源管理器搜索并定位到所选进程的文件路径。

7.1.4 系统信息

在【系统分析】中，单击【系统信息】，在打开的【系统信息】可以查看和了解当前计算机的硬件信息以及操作系统的信息。

7.2 网络分析

微点主动防御软件提供的【网络分析】工具帮助用户监控和分析进程的网络访问信息和异常情况，提供【进程网络信息】、【IP 流量图】、【端口流量图】、【进程流量图】和【传统防火墙信息】五种网络分析工具。

7.2.1 进程网络信息

【进程网络信息】实时详细报告系统中所有正在运行进程的访问网络情况，提供 IP 地址、协议、本地端口、远端端口、状态以及网络流量信息，通过对这些信息的分析，用户可以判断当前运行的进程是否异常，是否存在有害程序（如木马等）在运行，以便进一步采取措施对系统进行防护。

在【网络分析】子功能中，单击【进程网络信息】，查看进程的网络信息。

1) 网络状态背景颜色描述

- 绿色背景 — 即将结束的网络连接。
- 黄色背景 — 正在通讯的网络连接。
- 红色背景 — 新建的网络连接。

2) 查看网络进程的文件属性

将鼠标轻移到【进程网络信息】列表中的任意进程的名称上，即可显示该进程文件的文件自述、产品名称、描述、公司名称、文件版本，以及文件启动/

退出时间和本地端口打开/关闭时间。

3) 进程网络信息区右键菜单

- 程序信息 — 查看所选进程的程序信息。
- 进程信息 — 查看所选进程的进程信息。
- 流量图 — 查看所选进程的总流量以及其开启的端口流量。
- 结束进程 — 结束正在进行网络连接进程的运行。
- 关闭该 tcp 连接 — 中断所选进程当前的 tcp 连接。
- 查找目标 — 打开资源管理器搜索并定位到所选进程的文件路径。

7.2.2 流量图

微点主动防御软件提供了【IP 流量图】、【端口流量图】、【进程流量图】，直观显示系统中正在访问网络进程的流量状况，通过流量图分析进程的流量情况，可判断是否有可疑进程在运行，再结合系统的其它分析工具（进程分析）来判断系统是否存在有害程序。

默认情况下显示当前系统中 IP/端口/进程的瞬时总流量（红色）及前四个瞬时流量最大的流量波形情况（从高到低分别为绿、蓝、 棕、墨绿）。

- 【IP 流量图】是以 IP 地址作为索引，以波形图的方式显示系统中所有（包括内部网、外部网）IP 地址的瞬时流量（流入和流出）情况。
- 【端口流量图】是以端口号作为索引，以波形图的方式显示系统中所有打开端口的流量情况。
- 【进程流量图】是以进程名称作为索引，以波形图的方式显示当前系统中正在运行的进程的流量情况。

举例：查看当前正在进行网络连接的 flashget.exe 进程的瞬时流量。

【第一步】选择进程：在进程流量图中的下拉列表中选择要查看流量的进程。

【第二步】查看进程流量波形图：通过调整“纵向每格代表的流量”，显示所选的

进程流量的完整波形图。

【第三步】查看进程的瞬时流量：用鼠标左键单击波形图中某一点（流量最高点或其他点），即可显示该点的瞬时流量信息，如图 67 显示进程 flashget.exe 在 17：26：31 的网络流量（流入）为 13.6KB。

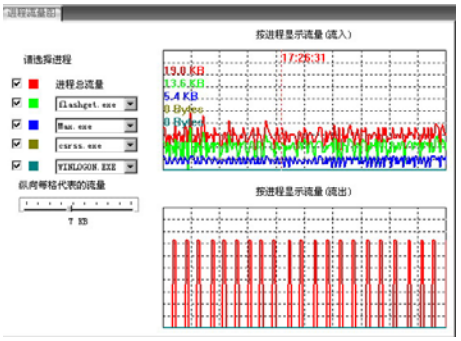


图 67

7.2.3 传统防火墙信息

【传统防火墙信息】记录微点主动防御软件传统防火墙的报警信息，当系统中检测到需要记录报警信息策略的数据包时，就会将该信息记录到防火墙信息中，提示用户进出数据包的协议类型、本地地址、远程地址、方向。如图 68：

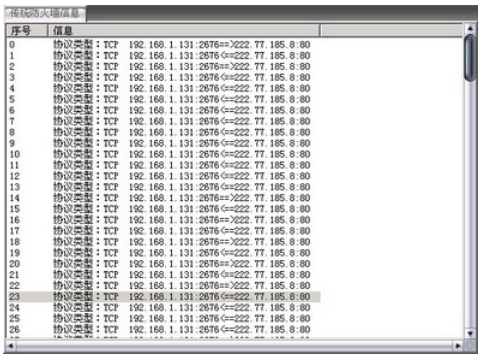


图 68

微点提示：传统防火墙的默认规则包不记录报警信息。

第8章 日志分析

日志系统是微点主动防御软件提供给用户的一款卓越的系统信息监控器。微点主动防御软件具有强大的日志记录功能，包括两个类别的日志：【安全日志】和【系统日志】（如图 69）。通过对两大日志的分析，结合【可疑程序诊断】和【进程分析】，用户可以发现一些异常现象或潜在的危害。

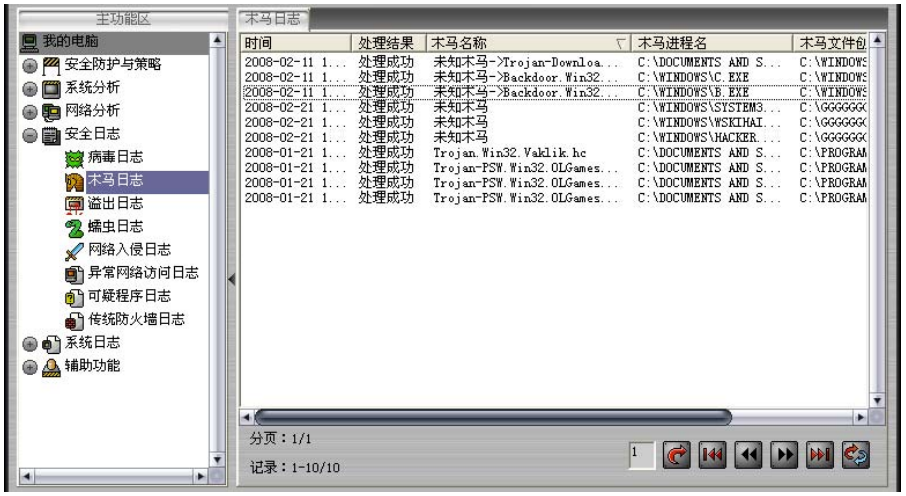


图 69

8.1 日志管理

微点主动防御软件对【安全日志】和【系统日志】提供了右键菜单对日志文件进行查询、删除、备份等操作。

1) 删除日志

为了有效地节约系统空间，用户可以把自己已经了解的日志记录信息，或您认为已经没有用的记录信息删除。

选择要进行日志操作的类别，打开标签页，在其详细信息区单击右键，在打开的右键菜单中选择：

- 【删除选择的日志】— 删除所选择的日志记录。
- 【删除显示的日志】— 删除当前显示的日志记录。
- 【清空日志】— 将所选类别中的所有日志删除。

2) 导出日志

选择要进行日志操作的类别，打开标签页，在其详细信息区单击右键，在打开的右键菜单中选择“导出日志”，则可将所选日志类别中的日志内容备份到指定的路径。

- 【导出全部日志】— 以 txt 文档的格式将当前所选类别的日志中的所有日志导出
- 【导出显示的日志】—以 txt 文档的格式将当前所选类别日志中所显示的日志导出。

3) 日志查询

在所选日志类别的标签页详细信息区右键菜单中单击“查找日志”，在弹出的【查询日志记录】对话框中，选择要查询的日志时间范围：选择“开始时间”和“结束时间”后单击“查询”按钮，即可查询指定时间段内的日志信息。

4) 查找目标

在【程序生成日志】右键菜单中增加了一个“查找目标”的功能，该功能可以打开资源管理器，搜索并定位到所选文件的路径。

8.2 安全日志

【安全日志】详细记录微点主动防御软件对监控到的病毒、木马、蠕虫等恶意程序的处理日志。根据有害程序的特点，【安全日志】主要划分为：

- 【病毒日志】— 记录系统中所有被微点主动防御软件监测出的已知和未知病毒的处理信息。
- 【木马日志】— 记录系统中所有被微点主动防御软件监测出的已知和未知

木马病毒的处理信息。

- 【溢出日志】— 记录系统中所有被微点主动防御软件监测出的来自本地或远程病毒第一次溢出攻击的攻击处理信息。
- 【蠕虫日志】— 记录系统中所有被微点主动防御软件监测出的已知和未知蠕虫病毒的处理信息。
- 【网络入侵日志】— 记录微点主动防御软件拦截处理本地或远程计算机利用系统漏洞通过溢出攻击手段对本机第一次溢出攻击后再次入侵的详细信息。
- 【异常网络访问日志】— 记录微点主动防御软件对系统中程序访问网络报警的处理信息。
- 【可疑程序日志】— 记录被微点主动防御软件监控到的具有高危险动作但还不足以判定为未知有害程序的可疑进程的处理信息。
- 【传统防火墙日志】— 是记录微点主动防御软件防火墙策略中数据包连入或者连出系统的信息，通过分析这些日志可以发现曾经以及正在发生的对系统的入侵行为。

微点提示：传统防火墙的默认规则包不记录日志。

8.3 系统日志

【系统日志】详细记录了系统中的进程启动、程序生成、注册表变更等日志信息。主要包含：

- 【管理员日志】— 记录管理员对微点主动防御软件进行管理时的动作。管理员日志记录的内容包括对可信程序、程序访问网络策略所作操作的描述。
- 【升级日志】— 记录微点主动防御软件升级的状态及历史情况。
- 【进程启动日志】—记录系统中进程的每次启动及退出信息。
- 【程序生成日志】—记录系统中程序的创建时间及生成关系的详细信息。

- 【注册表变更日志】— 记录系统中程序创建或修改注册表键值动作的详细信息。

鼠标左键双击【注册表变更日志】的任意一项记录，可以直接打开 Windows 的注册表编辑器，并准确定位到该项记录的注册表键值，用户可以对该项记录的注册表键值做修改和删除操作。

微点提示：对于不熟悉注册表修改的用户，我们强烈建议您不要对注册表做任何修改操作，以免因误操作造成系统瘫痪或软件不能正常使用。

第9章 辅助功能

9.1 修改注册信息

注册完成后，若需要修改注册信息，单击【辅助功能】中的【修改注册信息】如图 70：

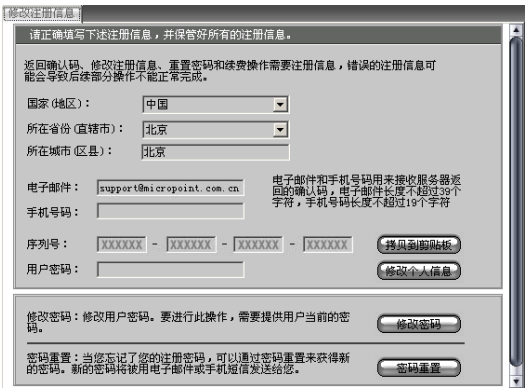


图 70

1) 修改个人信息

个人信息包含： 国家、所在省份、所在城市、电子邮箱、手机号码。

更改个人信息后，输入注册时的“用户密码”，单击“修改个人信息”，修改完成。

2) 修改密码

即更改微点主动防御软件的注册密码。单击“修改密码”，在弹出的输入框中输入“当前密码”和“新密码”后，在“密码确认”中重新输入新密码，单击“确定”，完成密码更改。

3) 拷贝到剪贴板

软件注册成功后，单击“拷贝到剪贴板”，当前序列号将会自动复制到 Windows 剪贴板，然后可以直接粘贴到文件中对当前的序列号进行备份。

4) 密码重置

用户在忘记注册密码时，单击“密码重置”，微点主动防御软件会请求微点注册服务器自动生成新的密码并发送到用户注册所用的邮箱或手机上。

微点提示：

1. 修改信息前，请确保您的计算机连接到互联网上。

2.修改完毕后，请用户牢记修改的各项内容，以后重新安装微点主动防御软件时，再次注册要确保邮件地址、密码一一对应，否则将无法完成注册。

9.2 续费

在微点主动防御软件的有效使用期到期后，用户若想继续使用微点主动防御软件可通过续费的方式实现。

1) 获取续费号

用户获取续费号有两种方式：

- 登录微点公司网站通过交易平台获得。
- 到距离最近的微点主动防御软件产品经销处直接购买。

2) 产品续费

在【辅助功能】中单击【续费】，打开续费标签页，如图 71：

图 71

【第一步】进行续费前，请确保您的计算机已经连接到互联网上；

【第二步】在续费详细信息区内输入续费号；

【第三步】确定正确无误后，单击“续费”按钮，弹出要求输入确认码的提示信息。

【第四步】输入通过邮箱或手机收到的确认码后，单击“确认”，将出现如图 72 所示的提示信息，表示续费成功。

图 72

9.3 查询剩余时间

在【辅助功能】中打开【续费】标签页，单击详细信息区中的“查询剩余时间”按钮，即可查询微点软件的剩余使用时间。

9.4 密码设置

【密码设置】功能是用来保护微点主动防御软件不被意外停止和恶意修改。用户通过设置密码，可以防止未授权用户开启软件的主界面、停止防火墙以及退出或暂停软件。默认情况下安装微点主动防御软件没有设置密码，在【辅助功能】中打开【密码设置】标签栏，输入要设置的密码，单击“保存设置”，则完成密码的设置。

微点提示：密码设置完成后，请牢记密码，在开启软件的主界面、停止防火墙以及退出或暂停软件的操作时都需要正确输入设置的密码。

9.5 导入/导出设置

为了避免用户因重新安装微点主动防御软件而需要重新对微点主动防御软件进行设置，微点主动防御软件提供了导入/导出设置的功能，对微点软件的一些设置项目进行导出、导入。这些设置项目包含：实时监控设置、可信程序名单、修改程序策略、程序网络访问策略、传统防火墙策略、升级设置。

1) 导出当前设置

【第一步】在 【导入 / 导出设置向导】中，选择“导出当前设置到文件”后，单击“下一步”后，打开如图 73 所示【导出设置到文件】的窗口：

图 73

【第二步】在“设置项目列表”中勾选要导出的设置项目，并单击“浏览”按钮选择设置文件的存储位置后，单击“下一步”完成导出设置。

2) 导入设置

【第一步】在【导入 / 导出设置向导】中，选择【从文件导入设置】后，单击“下一步”后，打开如图 74 所示【从文件导入设置】的窗口：

图 74

【第二步】单击“浏览”按钮导入备份的微点软件设置文件。

【第三步】在“设置项目列表”中，勾选要导入的设置项目，然后按“下一步”进行导入。

9.6 生成技术信息

为了方便微点公司技术人员分析您所遇到的问题，微点主动防御软件提供了【生成技术支持信息】功能，它能提取与问题有关系的系统信息，并自动压缩成一个报告文档。报告文档中信息内容包括：操作系统的版本号、微点主动防御软件的具体版本信息、系统自启动信息、微点主动防御软件的日志信息（包含系统日志和安全日志）、当前运行的进程和模块信息。该报告文档中的文件采用文本文件类型（.txt），用户也可以打开查看。

该报告文档可通过微点官方网站客户服务中心（邮件客户服务）页面或者微点技术支持邮箱（support@micropoint.com.cn）以附件的方式发送至微点公司，发送报告文档时请在邮件内容中详细描述您所遇到问题的现象，以便您能够尽快收到微点公司技术人员的回复。

导出【生成技术支持信息】:

【第一步】 在【辅助功能】中打开【生成技术支持信息】;

【第二步】导出【生成技术支持信息】：单击“选择路径”设置导出文件的存储路径和文件名，默认存储路径为系统的根目录下，单击“确定”，则会自动导出一个压缩格式的文档。

附录

附录一　常见问题

1)　微点主动防御软件支持哪些操作系统？

解 答：

微点主动防御软件支持 Windows 2000/XP/2003/vista/2008/7 的操作系统 。

2)　无法注册，提示“连接注册服务器失败....”

解 答：出现这种问题的原因可能有三个：

a. 是否正常连接网络？

如果不能上网，请检测网络连接。确认已正常连接网络后，再进行注册。

b.是否使用代理上网？

请尝试在微点软件的“升级设置”窗口设置好代理服务器，并测试代理通过后，再进行注册。

c.是否安装有其他安全软件或防火墙？

如果安装了其他安全软件，请尝试将微点软件的程序：MPSVC.exe、MPSVC1.exe、MPSVC2.exe、MPMon.exe、MPMain.exe、MPUpdate.exe、Download.exe 添加到其允许进程通讯的策略中或者监控排除列表中，再注册。若不清楚如何添加或添加后仍无法注册，请尝试暂时关闭或卸载其他安全软件后再注册，或请直接联系微点客服。

如上述操作后，仍无法注册，请及时与微点客服联系处理。

3)　一个序列号能否在多台计算机上注册使用

解 答：除非特别说明，微点主动防御软件同一个序列号只能在一台计算机上注册使用。如果同时在多台计算机上注册使用同一序列号，则只有最后注册的那台计算机上的微点软件可以正常升级。

4)　无法注册微点软件，提示“您输入的用户信息不正确或此序列号已被注册”

解 答：您当前使用的序列号已注册，重新注册时，需要使用上次注册成功的用户信息，请使用上次注册成功的用户信息（电子邮件、注册密码等）进行注册。

5） 无法升级，提示“服务器繁忙或网络不通”

解 答：出现此问题的原因：

原因一： 没有连接网络。

解决办法：请正确连接网络后，再进行升级。

原因二：使用代理上网。

解决办法：在“升级设置”窗口设置代理服务器，并测试代理通过后，再进行升级。

原因三：系统中安装了其他安全软件或防火墙阻止了微点软件的升级。

解决办法：请将微点软件安装目录下的程序：MPSVC.exe、MPSVC1.exe、MPSVC2.exe、MPMon.exe、MPMain.exe、MPUpdate.exe、Download.exe 加入到防火墙允许程序通讯的策略中或者监控排除列表中，然后再尝试升级，如仍有问题，请与微点客服联系。

原因四：微点软件的升级服务器繁忙。

解决办法：请选择其他时间升级，如仍有问题，请与微点客服联系。

6） 无法升级，提示“用户身份合法性验证失败”

解 答：出现此问题的可能原因：

原因一：使用同一个序列号在多台计算机上安装注册。

微点主动防御软件单机版序列号，除非特别说明，一个序列号只能在一台计算机上安装注册，否则，只有最后一台计算机上注册成功的微点软件能升级，在原其他计算机上注册的微点软件将无法升级和修改注册信息。

解决办法：如果在多台计算机安装微点软件，请购买多套微点软件使用。

原因二：在同一台计算机上注册微点软件，进行过系统还原或者 ghost 还原（注：还原系统中已安装注册了微点软件）。

解决办法：微点网站下载新的安装包，卸载原微点软件，重新安装注册即可。

7） 查看微点主动防御软件的当前版本号以及更新时间

解 答：可通过以下三种方法查看：

a.将鼠标移到系统托盘区微点主动防御软件的图标上，即可显示微点主动防御软件的程序版本、特征版本以及最后一次更新时间。

b.打开微点主动防御软件的主界面，主界面底部的状态栏显示微点主动防御软件的程序版本号以及最后一次更新时间。

c.打开微点主动防御软件主界面，单击【辅助功能】->【关于】，显示微点主动防御软件的程序版本、特征版本以及最后一次更新时间。

8） 如何安装和注册微点主动防御软件家庭版？

解 答：

微点主动防御软件家庭版包含三个授权，可以在三台计算机上安装注册。在不同计算机上安装注册时，请使用不同的用户信息注册，比如使用不同的邮箱，相同的密码，或者相同的邮箱不同的密码。

家庭版在三台计算机上分别注册成功后，微点软件将自动给用户分配三个新的序列号，此序列号具有唯一性，请牢记此序列号及注册信息，重装微点软件时请输入分配后的序列号进行安装注册。

家庭版注册成功后，用户可进入软件主界面【辅助功能】—>【修改注册信息】，更改注册信息。

9） 微点主动防御软件过期后，能否继续使用？

解 答：微点主动防御软件过期后不能继续使用， 请在即将过期时通过交易平台购买续费号或者购买新的正式版保护您的系统安全。

10） 忘记注册用的密码怎么办？

解答： 可以采用以下三种方式获得：

a.密码重置方式获得：这种情况只能是在微点主动防御软件没有卸载的情况下，且已经注册，单击【修改注册信息】中的“密码重置”，微点软件注册服务器自动生成新的密码并发送到用户注册所用的邮箱或手机上。

b. 登录微点通行证，对绑定的序列号进行密码重置。

登录微点通行证，打开绑定序列号列表，搜索当前序列号，单击序列号对应的“重置”按钮，微点软件注册服务器自动生成新的密码并发送到用户注册所用的邮箱或手机上。

c. 联系微点客服进行密码重置。

附录二　联系技术支持

用户手册和软件帮助（软件主界面—>【辅助功能】—> 【帮助】）提供了有关微点软件的详尽信息，请查阅这两个文档确定是否包含您所需要的信息，如果找不到您所需要的信息，请通过以下方式与微点技术支持联系，我们将尽快回复您的问题。

服务方式：

一、自助在线检索

登陆微点公司的客户服务中心http：//service.micropoint.com.cn可以在常见问题和使用技巧栏目根据问题的类型或关键字进行搜索查询，获取相关问题的解决方案。

二、在线提交问题

登陆微点公司的微点电子邮局http：//service.micropoint.com.cn/mail.php选择相应的问题类型，根据提示尽可能提供详细的相关问题信息，微点公司会尽快以邮件的方式将结果回复至您的邮箱。

或者登录微点社区http：//community.micropoint.com.cn提交您的问题。

三 、电话服务

技术服务热线：（010）59798298

四 、传真服务

传真：（010）88891696

五 、邮件服务

技术支持邮箱：support@micropoint.com.cn

六 、公司通信地址

地址：北京市海淀区蓝靛厂东路 2 号 B 区写字楼 1608 室

邮编：100097