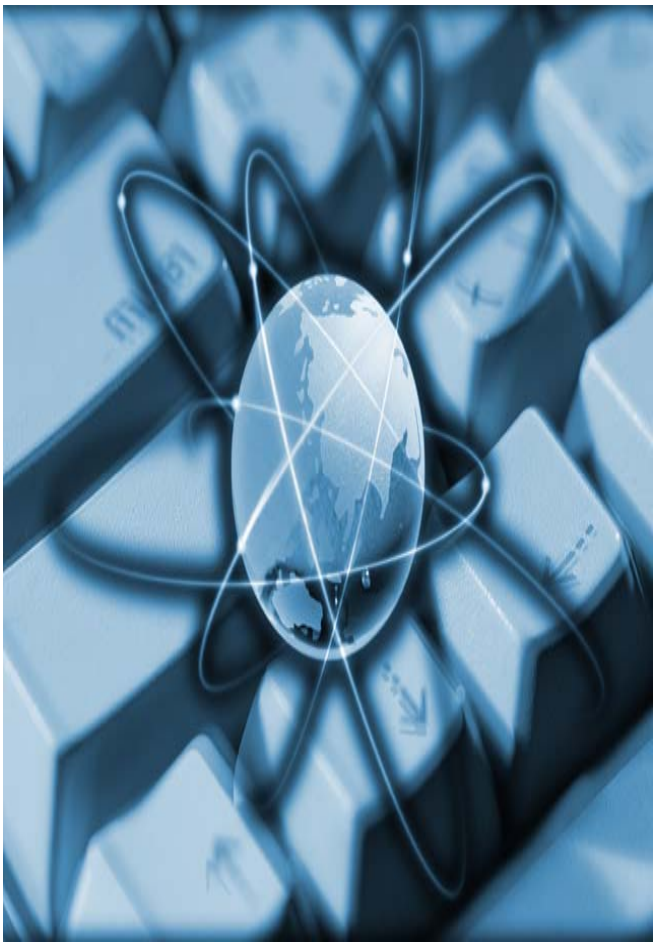
KINGSOFT
金山软件股份公司

量身打造中小型企业级网络安全之道

金山毒霸 2005 中小企业版

技术白皮书



毒霸信息安全网：**db.kingsoft.com**

毒霸企业安全网：**dbnet.kingsoft.com**

版权声明

目录

第一章 主要功能特点

全网智能漏洞修复

针对病毒利用系统漏洞传播的新趋势，金山毒霸 2005 中小企业版率先采用了分布式的漏洞扫描及修复技术。管理员可通过管理节点执行全网漏洞扫描，并精确部署漏洞修复程序；其通过 Proxy（代理）下载修复程序的方式，极大地降低了网络对外带宽的占用。全网漏洞扫描及修复过程无需人工参与，且能够在客户机用户未登录或以受限用户登录情况下进行。

全网杀毒，多维防护

- **率先实现每日病毒库实时更新、防毒体系主动实时升级并自动分发、防毒系统抢先在所有病毒之前启动，赢得时间。**

  金山毒霸 2005 中小企业版的主动升级机制可保证在第一时间获取最新病毒库，并自动分发给网内所有客户机。而这一切都不需要管理员作任何操作。即使面对病毒一日出现多个变种，网络体系依然可以有效防御。

  防毒胜于杀毒，抢先启动的防毒系统可保障在 Windows 未完全启动时就开始保护用户的计算机系统，早于一切开机自运行的病毒程序，使用户避免“带毒杀毒”的危险。抢先式防毒使您赢得时间，让安全领先一步。

- **分布式防毒体系，防毒从桌面到服务器覆盖到全网每个节点，在空间上不留盲点.**

  管理员可通过管理节点对全网或指定的客户机发出查杀病毒指令，以有效遏止病毒疫情爆发，避免网络内病毒交叉、重复感染；自动检测多途径的病毒源，实时监测各类病毒入侵，全方位体现病毒实时防护。

- **自动检测多途径的病毒源，实时监测各类病毒入侵，防毒从源头堵起。**

  自动检测多途径的病毒源，实时监测各类病毒入侵，全方位体现病毒实时防护。

- **国际领先的“蓝芯”杀毒引擎，全面查杀数万种病毒，支持数十种压缩格式、多重压缩包直接查毒杀。**

  核心技术采用国际领先水平的“蓝芯”杀毒引擎，对各类已知、未知病毒、可疑文件、木马以及其它有害程序可全面查杀；全面支持 DOS、

Windows、UNIX 等系统下的十数种压缩格式、多重压缩包的查毒；支持 ZIP、RAR 等压缩格式、UPX 加壳文件的包内直接查杀；嵌入协议层的邮件监控，可双向过滤邮件病毒；

易用灵活的部署及管理，为中小企业量身定做

- **可移动的 Web 管理控制台**
  控制台基于 WEB 结构开发，管理员无需安装额外的控制软件，就可以在任意一台计算机上轻松管理整个防毒体系，真正实现了“管理无处不在”。

- **高效的安装部署方式**
  管理员可以根据企业网络环境采用 WEB 页面（ActiveX）安装、远程安装、域脚本安装等方式，在较短的时间内完成网络内大量客户端的安装，简单快速地实现整个网络反病毒体系的部署，最大限度贴合网络实际环境。

- **灵活定制企业级安全策略**
  通过金山毒霸 2005 中小企业版的管理节点，既可以配置全网统一的安全策略，又可以将具有不同需求的客户机分配到特定的组，配置具有针对性的组策略。通过这种灵活的配置方式，管理员可以轻松地定制企业级安全策略。

- **多途径报警机制**
  管理员可以通过 SNMP Trap、NT 事件日志、Email 及 Windows 信使服务等多种方式接收病毒事件报警，以保证及时应对病毒疫情。

- **图形化统计病毒信息**
  图形化的统计页面可以将网络内的病毒分布状况直观地呈现出来，以便于管理员分析网内病毒发展趋势，并采取针对性的措施。

跨平台

- **跨平台的病毒防护**
  支持 Windows、Linux 等多种平台操作系统，彻底扫除网络反病毒盲点。
- **跨平台的应急杀毒盘**
  金山毒霸创造性地采用 Linux 作为应急启动盘，通过跨操作系统杀毒确保系统环境的绝对干净，支持包括 NTFS 分区在内的多种分区格式。

随需切换的客户端操作界面

针对不同用户的需求，客户端采用两种操作界面，用户可通过安全状态界

面查看大部分信息并可执行“一键升级”、“一键杀毒”、“一键漏洞扫描”等常见任务,操作简单方便。切换到主界面后，高级用户可进行更为复杂的操作和设置。

第二章 体系结构

金山毒霸 2005 中小企业版是一套专为中小型企业级网络环境设计的反病毒安全解决方案，它能够为企事业单位网络范围内的工作站和网络服务器提供可伸缩的跨平台病毒防护。金山毒霸 2005 中小企业版实现了集中式配置、部署、策略管理和报告，并支持管理员对网络安全进行实时审核，以确定哪些节点易于受到病毒的攻击，以及在出现紧急病毒情况时采取何种应急处理措施。网络管理员可以通过逻辑分组的方式管理客户端和服务器的反病毒相关工作，并可以创建、部署和锁定安全策略和设置，从而使得网络系统保持最新状态和良好的配置。

金山毒霸2005中小企业版采用了业界主流的B/S开发模式,由系统中心(拥有基于 WEB 的系统中心控制台)、服务器端、客户端组成了反病毒安全保障体系。

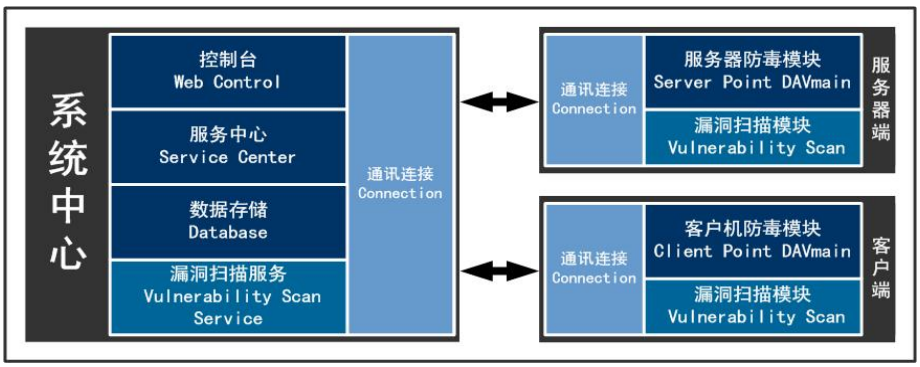


图 2-1 金山毒霸 2005 中小企业版系统结构图

2.1 系统中心

系统中心是金山毒霸 2005 中小企业版进行信息管理和病毒防护的控制核心。系统中心基于 CORBA 与其它子系统（服务器端和客户端）连接，其它子系统在系统中心控制下完成协同工作。通过数据库技术，系统中心可以实时记录网络防护体系内每台计算机上的病毒防护信息、防毒设置信息和终端资源信息。同时，系统中心集成了基于 WEB 方式的控制台，能够集中管理网络上所有已安装过金山毒霸 2005 中小企业版客户端的计算机，保障每个纳入金山毒霸反病毒体系的计算机时刻处于最佳的防病毒状态。

系统中心控制台

系统中心控制台是整个金山毒霸 2005 中小企业版系统设置、使用和控制的

操作平台。它的界面结构友好、直观，符合用户的使用与操作习惯。系统中心控制台基于 WEB 结构开发，管理员无需安装额外的控制软件，网络内任何一台装有 IE5.0 及其以上浏览器的终端都能用来实现对整个网络的管理，真正实现了“管理无处不在”。

2.2 客户端

客户端面向网络中的客户机群提供反病毒安全防护，是金山毒霸 2005 中小企业版反病毒体系的执行终端之一。它能够实时监控系统的运行与操作，先进的反病毒“蓝芯”引擎确保了能够全面查杀硬盘及驻留系统内存中的病毒、蠕虫以及特洛伊木马，基于病毒行为检测的启发式查杀技术确保您能及时发现出潜在的未知威胁并采取相应安全措施。病毒隔离系统可以将所有不可修复的受病毒感染文件置于受金山毒霸控制的安全区域内，以便您采取数据过滤等进一步处理措施。邮件防护能够自动监测收发邮件过程，及时发现隐藏其中的病毒。漏洞扫描技术能够使您的系统彻底杜绝利用漏洞传播攻击的病毒危害，这其中就包括冲击波、振荡波、红色代码等极其严重的威胁。

结合金山毒霸多项屡获殊荣的反病毒技术，金山毒霸 2005 中小企业版客户端能有效防范来自软盘、光盘、网络共享及邮件、网络下载等各种途径的病毒入侵，实现全方位的病毒防护。并且，客户端的相关安全信息会及时反馈给系统中心，管理员能在最短时间内了解网络内安全状况，并通过系统中心向客户端发出指令，远程控制其操作及安全策略设置。客户端的升级过程无需人工参与，系统中心在获得最新更新后将向客户端自动分发。

2.3 服务器端

服务器端面向网络中服务器群提供反病毒安全保护，是金山毒霸 2005 中小企业版的另一执行终端。它具备了客户端的所有功能（由于服务器不存在个人的邮件收发行为，服务器端不包括邮件监控），同时为了贴合服务器操作系统的性能特点，服务器端还进行了针对性优化处理，适合于服务器的海量高速运转。服务器端作为服务随系统启动，在管理员不登录系统的情况下，仍可接受管理。

第三章 工作方式

3.1 管理控制通信方式

金山毒霸 2005 中小企业版的整体控制通信方式是采用以系统中心为消息处理、转发中心及具体功能节点，客户端和服务器端为具体防毒节点的整体反病毒解决方案。

管理员通过控制台向系统中心发出具体的操作命令，系统中心解析具体的命令目的地，按需转发或者处理。

客户端或者服务器端每次启动都会登录到指定的系统中心并且定时汇报自己的状态，并且将发现的病毒信息反馈到系统中心。

3.2 升级工作方式

在金山毒霸 2005 中小企业版中，系统中心的升级服务模块负责升级文件的获取、更新及分发。同时，系统中心亦负责发布升级消息，客户端及服务器端将在接到升级通知后连接系统中心执行升级。其具体升级流程如下

- 系统中心按管理员的预定义设置或手动升级命令连接到 Internet 更新升级文件；
- 系统中心下载升级程序完成后通知客户端及服务器端升级；
- 客户端及服务器端收到消息后连接到系统中心执行升级。

3.3 漏洞扫描工作方式

金山毒霸 2005 中小企业版漏洞扫描分为集中扫描和客户端独立扫描两种方式。普通用户可以通过本机的客户端手动进行漏洞扫描和安装修补程序。管理员可以通过系统中心来通知局域网内所有的在线的客户端进行漏洞扫描，客户端在扫描之后将结果反馈到位于系统中心的漏洞扫描服务端，管理员根据结果选择需要安装的客户机和需要安装的修补程序，并通知其下载和安装修补程序。

客户机下载和安装修补程序是通过系统中心的下载代理功能来实现的，对于同一个修补程序，当第一个客户端请求之后，系统中心连接到微软升级网站下载相应的修补程序，完成之后，所有的客户端都可以直接在系统中心漏洞修复下载代理的缓存（Cache）中直接下载安装此修补程序，这种方式不但使得不能上网的客户端可以下载修补程序，而且还大幅加快了下载的进程，减少了对于网络资源的占用。

第四章 安装部署

金山毒霸 2005 中小企业版的安装分系统中心安装和客户机安装，金山毒霸 2005 中小企业版系统中心现行版本支持 Windows NT Server4.0、Windows 2000 Server 、Windows 2000 Advanced Server、Windows Server 2003 Standard Edition 、Windows Server 2003 Enterprise Edition 等操作平台。未

来通过移植后可以支持 FreeBSD、UNIX（SUN Solaris 系列，IBM AIX 系列）。

4.1 系统中心安装

金山毒霸 2005 中小企业版系统中心的安装是全网安装的基础,在安装金山毒霸 2005 中小企业版服务器端程序前，首先要安装 JAVA 2 SDK，其后的安装过程与安装普通软件基本没有差异。为了保证金山毒霸反病毒安全保障体系正常运作，需要为系统中心确定一个合理的网络节点位置。对于若干常见的企业级网络构建型式，我们给出如下安装建议：

网络环境	系统中心安装位置建议
单网段局域网	■ 至少保证安装于局域网内联网的计算机上，并且该计算机拥有局域网内长期固定不变的 IP 地址； ■ 建议选择专用服务器系统 ■ 建议选择非经常性大负荷运转的服务器
多网段局域网	■ 建议安装于能够直接访问 Internet 的网段之中 ■ 其余参考“单网段局域网”系统中心安装位置建议
存在物理隔离的局域网	■ 建议安装于具有移动存储设备的服务器，以便于离线更新病毒库 ■ 其余参考“单网段局域网”系统中心安装位置建议

4.2 客户机安装

可以根据管理员的需求定制采用 WEB 页面（ActiveX）安装、远程安装、域脚本安装、光盘安装等方式，在较短的时间内完成网络内部众多客户端的安装作业，简单快速的实现整个网络反病毒体系的部署。在安装好金山毒霸 2005 中小企业版系统中心后，通过系统中心控制台进行 Web 页面（ActiveX）安装、远程控制安装或域脚本安装，光盘安装可通过本机进行。

WEB 页面安装

通过浏览器访问控制台网页，下载 ActiveX 控件即可实现安装，这种方式适用于各个客户端自行下载进行安装。

远程安装

可通过管理控制台，向所有网络邻居中的 Windows NT/2000/2003 服务器/工作站远程安装金山毒霸 2005 中小企业版客户端,安装时需要目标客户端管理员口令。

域脚本安装

能够自动识别域服务器，并为域服务器配置登录脚本。当用户登录到本域时，实现自动为其安装金山毒霸 2005 中小企业版客户端，系统管理员不需为每台计算机都进行手动或远程安装。

客户端支持的操作系统

Windows 98/98 SE/Me
Windows 2000 Professional
Windows XP　Professional

服务器端支持的操作系统

Windows NT Server4.0
Windows 2000 Server
Windows 2000 Advanced Server
Windows Server 2003 Standard Edition
Windows Server 2003 Enterprise Edition
主流 Linux 操作系统

第五章 安全管理

系统中心控制台是可移动的操作平台（基于 WEB 服务架构），它支持您在任何一台 32 位且安装有 IE5.0 及以上浏览器的 Windows 计算机上，通过可移动的方式对系统中心进行管理、操作和设置，进而能够实现对网络中系统中心所辖客户机群的管理、操作和设置。基于系统中心的后台架构服务，系统中心控制台为您提供了提供简洁、易用的交互界面，让您的管理控制更加高效有序。通过有效的密码保护，系统中心控制台只允许经过特别授权的管理人员执行与维护反病毒安全保障体系的各项任务，以确保您的网络体系安全。控制台可以针对网络系统的特点灵活配置，能设置不同的任务对不同的客户机进行管理，实现网络内的自动化防毒操作。

5.1 登陆管理限制

为了防止未经授权的非安全登陆，系统中心控制台的登陆需要提供登陆密码。并且管理员可以随时修改登录控制台的密码

图 5-1 系统中心控制台登陆密码修改界面

5.2 客户机集中管理

金山毒霸 2005 中小企业版支持管理员通过系统中心控制台对全网客户机实施病毒查杀、升级、文件实时监控、安全日志审查及邮件监控的操控、客户机管理等。

图 5-2 系统中心客户机集中管理范围

查杀病毒：

选定需要进行操作的客户机后，单击相应按钮即可开始对所选客户机进行病毒查杀，查杀过程完全由管理员通过系统中心控制台控制，可随意启动、停止，并可自定义所选客户机的查杀路径。

升级客户端：

通常情况下，已部署完毕并设置好的金山毒霸 2005 中小企业版反病毒体系无需手动升级客户端。但在某些特殊需求下，管理员仍可手动对所选客户机进行升级。

文件实时监控：

管理员可以根据需求所选客户机的文件实时监控实施开启及关闭操作。

邮件监控：

管理员可以根据需求所选客户机的邮件监控实施开启及关闭操作。

客户机管理：
支持管理员对所选客户机进行客户机信息查看、改变所在分组、卸载、删除客户端记录等操作。

组选项设置：
支持管理员对选定分组进行整体安全策略配置，包括查毒设置、文件实时监控设置、邮件监控设置、任务调度设、权限设置。

5.3 管理针对性细化（组策略）

金山毒霸 2005 中小企业版支持您对客户端（或服务器端）进行逻辑分组管理及配置，从而更符合客户机的具体防毒需求差异。归属到一个组中的客户机可以按照统一的方式进行管理，可以通过设置组选项来统一同一组内所有客户机的行为和权限等。您可以通过组策略实现：全网统一的病毒防护策略，执行统一的组策略配置；基于需求的自定义分组；针对不同的组实施不同病毒防护策略；准确定位，只对特定组发出指令，避免影响网络全局。通常的分组方式有：域（或工作组）、部门、操作系统、Internet 应用、安全需求级别等。

5.4 客户机安全性针对细化

金山毒霸 2005 中小企业版支持用户对逻辑分组内的客户机进行统一的安全策略设置，这些设置能够帮助用户更好的针对网络内的安全需求制定措施，用户可以进行：客户机的查毒设置、文件实时监控设置、邮件监控设置、任务调度设置、权限设置。

5.5 多途径远程报警

金山毒霸希望能为用户提供真正可靠的反病毒解决方案，除了能够有效预防病毒的侵害，使用户及时掌握您所管理网络的病毒疫情也是我们的设计目标之一。金山毒霸 2005 中小企业版可以让管理员设置多种报警方式，在网络出现病毒疫情时及时反馈。当网络上的计算机受到病毒感染时，管理员会收到可靠的报警通知，包括可自定义的邮件通知、SNMP Trap 通知（简单网络管理协议，一个管理网络设备和计算机的一个标准协议）、NT 事件日志通知、信使服务。

5.6 安全日志集中获取、统计及管理

金山毒霸 2005 中小企业版安全日志信息记录了全网反病毒体系的安全状态及历史。面对病毒威胁，网络管理员需要快速制定有针对性的安全措施，这需要大量详实准确的网络安全信息作为依据。金山毒霸 2005 中小企业版具有强大快捷的安全日志功能，能够对网络内的病毒信息、客户端升级信

息、客户端安全信息进行统一的收集、统计并有效管理，形成图形化的日志汇总。

病毒日志记录了感染病毒的计算机详细信息，同时也记录了金山毒霸发现病毒，采取措施，直到清除病毒的具体过程，您可以根据日志文件中保存的状态信息充分了解整个网络内感染病毒的范围和几率，获知病毒的类型和危害，掌握病毒的清除结果，从而可以正确并迅速的做出决策——若是利用漏洞攻击的病毒爆发，则立即为局域网内存在此漏洞的计算机打上补丁；若是蠕虫病毒在网络内肆虐，暂时切断病毒源的网络连接，重新启动计算机；若是文件形病毒作怪，则确定感染病毒的计算机，立即重启进入安全模式或 DOS 环境，然后采用全面查毒方式，彻底清除病毒。

一旦发生病毒疫情，管理员可通过系统中心控制台查看网络中任意一台纳入金山毒霸反病毒体系计算机的受感染文件、感染的病毒信息、感染时间、清除结果。并且，可以对网络内桌面系统遭受邮件病毒危害的信息进行查看，包括受邮件病毒危害的客户机名、受感染文件名、危害的病毒名称、危害发现时间、附带该病毒的邮件名称、发件人、收件人、清除结果等。

升级日志记录了金山毒霸 2005 中小企业版系统中心从外网升级的状态及历史。通过察看升级日志，可以获取升级类型、升级开始时间、升级结束时间、升级结果等信息。管理员可以及时发现出现的升级异常情况。

第六章 客户机防护

在金山毒霸 2005 中小企业版反病毒安全保障体系中，客户机是面向网络中的终端设备而设计的病毒防护执行终端。根据具体保护的对象不同，分为客户端和服务器端。它提供了实时监控、全面查杀、病毒隔离、邮件防护及漏洞扫描等多种功能，同时兼具备份和应急盘创建的功能，针对可能来自软盘、光盘、网络共享及邮件、网络下载等各种途径的病毒入侵，实现全方位的病毒防护。当发现病毒时，客户机会及时将病毒信息反馈给系统中心。客户机还能接收并执行系统中心发出的指令，按系统中心设定的策略配置选项。客户机通过系统中心指定的服务器升级，升级过程无需人工参与。

金山毒霸 2005 中小企业版客户机是安装在客户机上响应系统中心命令或自定义查杀病毒，开启、关闭文件实时监控、邮件监控等功能的操作平台，是金山毒霸 2005 中小企业版防毒功能的实际执行者。

金山毒霸 2005 中小企业版客户端：

金山毒霸 2005 中小企业版客户端是面向局域网络中的桌面操作系统设计的反病毒保障执行终端。根据用户的不同操作需求，它分为“安全状态界面”和“主界面”，充分体现了人性化的设计思想。

图 6-1 客户端安全状态界面

图 6-2 客户端主界面

金山毒霸 2005 中小企业版服务器端：

金山毒霸 2005 中小企业版服务器端是面向局域网络中的服务器操作系统设计的反病毒保障执行终端。

图 6-3 服务器端主界面

附录

金山毒霸简介

金山毒霸是中国信息安全及反病毒领域最具品牌影响力、拥有最高市场占有率及领先技术的产品及服务提供商。

作为金山软件最重要的业务组成部分之一，金山毒霸以公司完善、发达的销售渠道和市场营销平台为依托，业务范围横跨个人用户市场和企业级用户市场两大领域，是金山软件整体业绩及利润高速增长的强劲动力。

1997 年，携金山软件的整体品牌及技术优势，金山毒霸进入信息安全领域。

1999 年，金山毒霸测试版隆重发布，近 200 万用户参与的长达 18 个月的严格测试，奠定了金山毒霸获得成功的坚实基础。

2000 年，金山毒霸正式产品一经推出随即凭借其出众的性能，迅速跻身国内信息安全领域顶尖品牌之列。

2001 年，金山毒霸面对疯狂肆虐的红色代码、齿轮先生、尼姆达、求职信等恶性病毒，以最快的反应速度发布了有效解决方案，大大降低了病毒的危害。同时，轰动全国的“缉毒世纪行”、“缉毒万里行”两大市场活动，使金山毒霸－“互联网时代最好的杀毒软件”的品牌形象更加深入人心。

2002 年，金山毒霸信息安全事业部正式成立。同时，金山毒霸针对市场和用户的实际消费需求，发布了对反病毒市场影响深远的“蓝色安全革命”活动，不仅创下了国内反病毒软件市场单一品牌 50 天销售 55 万套的奇迹，更以近 60％的市场占有率成为国内信息安全及反病毒领域公认的领导性品牌。

2002 年底，金山毒霸针对企业级用户的网络版产品顺利通过了公安部的严格测试，成为金山毒霸正式进军企业级反病毒市场的重要标志，金山毒霸的发展掀开了崭新的一页。

2003 年 8 月，金山发动助力 10 万企业的安全体验风暴，正式进军企业反病毒市场。金山毒霸上海、南京、广州、成都企业反病毒服务中心相继成立。

2003 年 9 月，金山正式宣布成立企业护航阵线，为企业提供本地化的反病毒专业服务。

2004 年金山毒霸继续保持技术领先、不断创新和实现了自我突破，推出了多款新一代产品，同时在病毒播报、病毒应急处理以及升级服务上保持了始终领先的地位；

中国的信息安全领域有巨大的市场发展潜力和广阔的发展空间。作为今日国内反病毒及信息安全领域公认的领导性品牌，金山毒霸不仅拥有成功的过去，更将创造一个辉煌灿烂的未来！