瑞星杀毒软件网络版企业防病毒解决方案
技术白皮书

2002 年 9 月 北京 • 中国

目 录

方案简介

瑞星杀毒软件网络版是国内著名反病毒软件公司——瑞星科技股份有限公司推出的企业级网络防病毒软件产品，它解决了以往网络防病毒软件在安装、设置、管理以及升级时遇到的不方便与不及时等问题，全新的查杀毒技术、直观友好的操作界面、强大的 Internet 与 Intranet 防病毒能力、及时周到的技术服务，使之成为各行业推行企业防病毒解决方案的首选。

简单地讲，瑞星杀毒软件网络版企业防病毒解决方案是通过瑞星管理员控制台对网络内的计算机进行安装、设置、管理、维护及升级，从而实现企业网络防病毒的目的。

产品简介

瑞星杀毒软件网络版可有效地保障企业内部网络不受病毒侵扰。

瑞星杀毒软件网络版产品由以下几部分组成：

- 瑞星系统中心
- 瑞星管理员控制台
- 瑞星杀毒软件服务器端
- 瑞星杀毒软件客户端

瑞星系统中心可以很容易地在整个网络内实现远程管理、智能升级、自动分发、远程报警等多种功能，有效的管理，严密的保护，杜绝病毒的入侵。

通过瑞星管理员控制台，管理员可以在网络中的任意一台计算机上对整个网络进行集中控制管理，清楚地掌握整个网络环境中各个节点的病毒监测状态，既方便了管理员，又最大程度的减少了整个网络中的安全漏洞，有效保障了整个网络的系统安全。

瑞星杀毒软件网络版适用于所有建立了企业内部网络的大中小型企业。根据客户网络规模的大小，瑞星公司推出的网络版系列产品包括：大型企业版、企业版、专用版、中小企业版和网吧版，可安装在下列各种平台：

- Windows 95/98/Me/2000/XP
- Windows NT/2000 Server
- Windows NT Workstation
- Novell NetWare
- FreeBSD
- UNIX（SUN Solaris 系列，IBM AIX 系列）
- Linux（RedHat Linux，Turbo Linux，红旗 Linux 等基于 Intel x86 芯片的系统）

瑞星公司还推出邮件服务器系统防病毒产品，支持的平台有：

- Microsoft Exchange Server
- Lotus Domino Server

注意：各版本的安装平台有所分别，请参阅“第六章 瑞星杀毒软件网络版产品系列”。

第一章 瑞星杀毒软件网络版的系统结构

1.1 分布式体系结构

瑞星杀毒软件网络版采用分布式的体系结构，整个防病毒体系是由四个相互关联的子系统组成：系统中心、服务器端、客户端、“移动式”管理员控制台。各个子系统协同工作，共同完成对整个网络的病毒防护工作，为企业级用户的网络系统提供全方位防病毒解决方案。

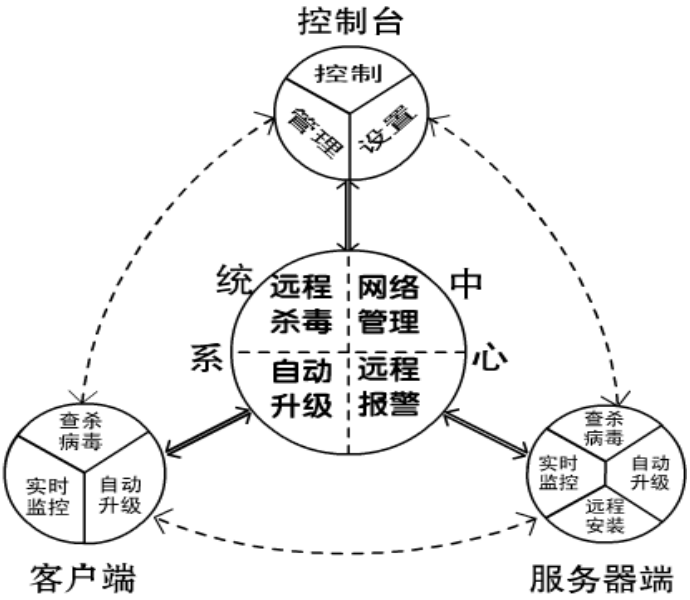

图 1 分布式体系结构

其中：

- 系统中心是整个瑞星杀毒软件网络版网络防病毒体系的信息管理和病毒防护的自动控制核心，它实时地记录防护体系内每台计算机上的病毒监控、检测和清除信息，同时根据管理员控制台的设置，实现对整个防护系统的自动控制。
- 服务器端/客户端是分别针对网络服务器/网络工作站（客户机）设计的，承担着对当前服务器/工作站上病毒的实时监控、检测和清除，自动向系统中心报告病毒监测情况，以及自动进行升级的任务。
- 瑞星管理员控制台是为网络管理员专门设计的，是整个瑞星杀毒软件网络版网络防病毒系统设置、管理和控制的操作平台，它集中管理网络上所有已安装了瑞星杀毒软件网络版的计算机，同时实现对系统中心的管理，它可以安装到任何一台安装了瑞星杀毒软件网络版的计算机上，实现移动式管理。

瑞星杀毒软件网络版采用分布式体系，结构清晰明了，管理维护方便。管理员只要拥有管理员账号和口令，就能在网络上任何一台安装了瑞星管理员控制台的计算机上，实现对整

个网络上所有计算机的集中管理。

第二章 瑞星杀毒软件网络版的安装特点

瑞星杀毒软件网络版具有多种安装方式，包括：智能安装、远程安装以及脚本登录安装等，通过这些多样化的安装方式，网络管理员可以十分轻松地在最短的时间内完成整个系统的安装。

2.1 智能安装

瑞星杀毒软件网络版可根据用户当前的操作系统和网络状态智能安装合适的模块，安装程序首先通过智能广播，确定整个网络内是否安装了系统中心。若没有找到系统中心，则判断当前计算机的操作系统是否为 Windows NT/2000 Server，若是，将自动安装系统中心，否则提示用户首先应在 Windows NT/2000 Server 计算机上安装系统中心。若找到了系统中心，则自动根据用户计算机的操作系统是 Windows NT/2000 工作站还是 Windows 95/98/Me/XP，自动安装客户端或服务器端。

瑞星杀毒软件网络版的整个安装过程完全是智能化设计，可以完全不需要用户指定系统中心位置，也不需要用户指定安装的模块，简单、方便、实用。

2.2 远程安装

远程安装包括两个部分，它们都可同时对多台机器进行远程安装：

第一，可远程安装瑞星杀毒软件网络版。也就是说，可通过瑞星管理员控制台，向所有网络邻居中的 Windows NT/2000 服务器/工作站远程安装瑞星杀毒软件网络版的服务器端或客户端。

第二，可远程安装瑞星管理员控制台。也就是说，可从瑞星管理员控制台向任何已经安装了瑞星杀毒软件网络版服务器端/客户端的计算机远程安装管理员控制台，实现移动式管理。

2.3 脚本登录安装

瑞星杀毒软件网络版能够自动识别域服务器，并为域服务器配置登录脚本。这种方式主要针对 Windows 95/98/Me/2000/XP、Windows NT 工作站等登录到域控制器的用户，当用户登录到本域时，实现自动为其安装瑞星杀毒软件网络版，避免系统管理员为每台计算机都进行手动或远程安装。

对于瑞星杀毒软件网络版，只需在域控制器上运行瑞星登录脚本安装程序，安装程序自动列出所有的用户供管理员选择，管理员可以根据需要选定部分或所有的用户即可，完全不需要管理员额外的操作。

第三章 瑞星杀毒软件网络版的安全管理

3.1 全面集中管理

瑞星杀毒软件网络版具有全面集中管理和全网设置的功能，网络管理员可以十分轻松地实现全网的统一设置，以及对客户端进行分组管理。

管理员可通过瑞星管理员控制台直接管理各种平台的服务器端/客户端：Windows NT/2000 服务器、Windows NT/2000 工作站、Windows 95/98/Me/XP 客户端、Novell Netware 客户端、UNIX/Linux 客户端。

在管理员控制台上，管理员能够对上述任何一种服务器端/客户端进行直接操作：设置、查毒、杀毒、通知升级、启动/关闭实时监控等。

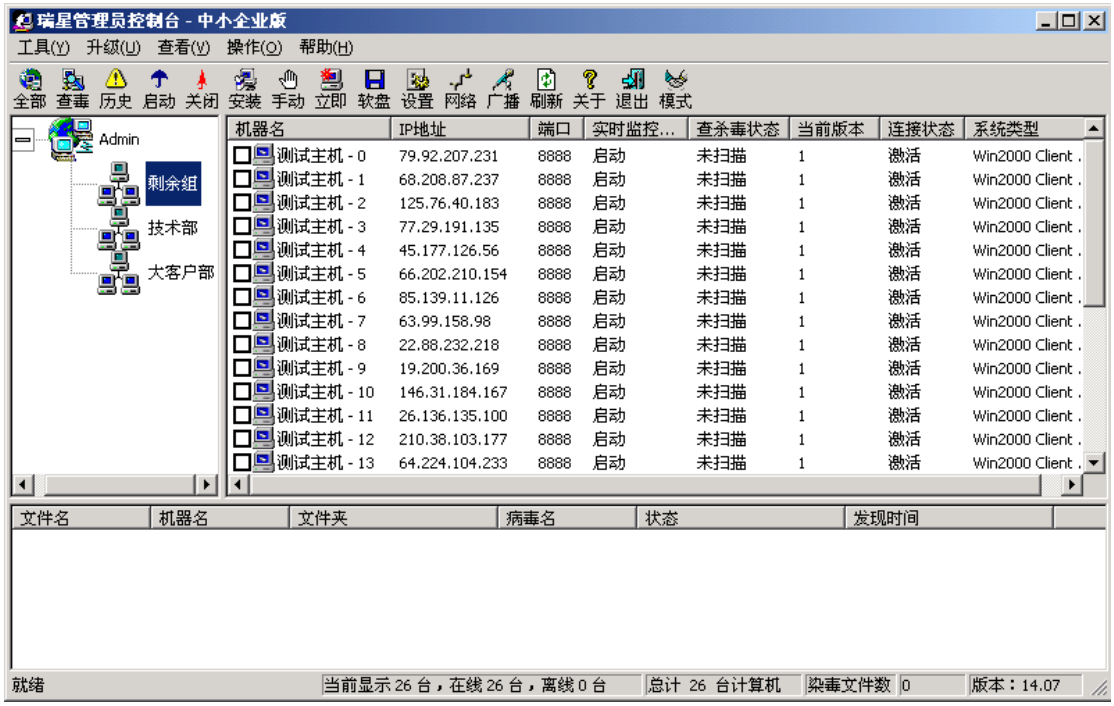

图 2 通过瑞星管理员控制台，实现全面集中管理

3.2 全网查杀毒

瑞星杀毒软件网络版能够随时启动对全网的统一查杀毒（即使本次没有开机的计算机，在下次启动后也会自动进行查杀毒），这样就能全网统一行动，最大程度的减小了病毒传播的可能。

当然，管理员也可以对很方便的使用瑞星管理员控制台对单个或多个客户端进行查杀毒。

3.3 全网设置

瑞星杀毒软件网络版能够随时对单个、多个或者全网的客户端进行设置，而且所有的设

置都是立即生效的，统一界面，操作简便。

3.4 直接监视和操纵服务器端/客户端

瑞星管理员控制台能够直接显示每一个服务器端/客户端的实时监控状态、安装的版本、查杀毒状态，这样管理员对于任何安装了瑞星杀毒软件网络版的计算机的状态都一目了然，随时监测有无异常情况出现。

此外，管理员能够随时启动/关闭单个、多个或者全网服务器端/客户端上的实时监控，确保整个网络上的每台计算机都处于最佳的防护状态。

3.5 远程报警

瑞星杀毒软件网络版系统中心记录了整个网络中任意服务器端/客户端计算机上查杀毒时发现的病毒信息，并且能够在控制台病毒列表栏上显示。管理员由此能及时发现染毒的计算机，做出及时的反应。

整个网络的病毒报警信息是由系统中心来统一维护的，因此管理员通过控制台能够查询和管理之前的病毒历史记录。对病毒的传播途径进行有效的跟踪，做到了层层防护。

3.6 移动式管理

瑞星杀毒软件网络版独有“移动式”管理员控制台，能够在任何一台安装了瑞星杀毒软件网络版的计算机上使用，因此管理员能够从任意具有管理员控制台的计算机上对全网进行管理，十分的方便。

3.7 集中式授权管理

瑞星杀毒软件网络版的授权管理由系统中心集中统一管理，系统中心自动维护整个网络的授权计数，客户端完全不用关心授权问题，只有在超出授权计数时才会提醒用户。

此外，瑞星授权计数是可以累加的，客户端增加时，只需在系统中心增加授权计数即可。

集中管理的好处在于只有在安装系统中心时才需要输入序列号，而且可以根据需要随时购买新的授权计数加入系统中心，而对客户端没有任何影响。

3.8 全面监控主流邮件服务器

瑞星杀毒软件网络版中集成了针对流行的邮件服务器 Exchange Server（包括 Exchange 5.5/2000），Lotus Domino（包括 Domino 4.6/5.0）的病毒防护产品，不仅有实时邮件病毒监控，而且有手动的邮件数据库扫描，功能强大，性能稳定，从根本上杜绝了病毒通过邮件方式的传入和传出。

在瑞星杀毒软件网络版中，管理员可以通过管理员控制台直接对邮件防护产品进行监控设置和对邮件数据库进行病毒扫描，染毒邮件信息直接在控制台中显示。

3.9 全面监控邮件客户端

瑞星杀毒软件网络版提供了几乎针对所有流行邮件客户端产品的实时病毒监控和手动病毒扫描功能，瑞星杀毒软件网络版支持的邮件客户端产品包括：Outlook，Outlook Express，Lotus Notes，FoxMail，Netscape 等，最大程度的防止了病毒通过邮件方式的扩散。

3.10 统一的管理界面

针对其它网络版杀毒软件设置复杂，操作繁琐的弊病，瑞星采用智能化的底层优化技术，在保持功能强大的前提下，实现了界面简洁统一（无论是从管理员控制台调用设置或查杀毒界面，还是直接调用客户端的主程序，都采用与瑞星单机版一致的界面）、操作便利的目标，最大限度地减少了用户操作难度和工作量。

特别地，为了最大程度的发挥软件的功能和方便用户，瑞星杀毒软件网络版的客户端包括了单机版的所有功能，这样在客户端即使没有连接到网络时，也能够使用瑞星杀毒软件网络版客户端来完成病毒查杀和实时监控，达到最大程度的保证计算机的安全。

3.11 支持大型网络统一管理的多级中心系统

面对新的经济形势，大、中型企业纷纷踊跃地加入信息化建设，大力建设多级中心网络系统，其网络呈现出多层级、分隶属的复杂结构。如何在这些不同层级的网络中实现统一的、全面的、及时有效的计算机反病毒管理呢？

"瑞星杀毒软件网络版多级中心系统"及时地满足了大、中型企业在这方面的需求。通过该系统，可实现反病毒的统一管理和分布管理，统一管理表现为由上级中心统一发送查杀病毒命令、下达版本升级提示，并及时掌握全部系统中心（包含下级中心）的病毒分布情况等；分布管理表现为下级中心既可以在收到上级中心的命令后做出响应，也可以管理本级，并主动向上级中心发送请求和汇报信息。可见，网络版多级中心系统支持大型的、多层级的、复杂的网络。

网络版多级中心系统是基于网络版单级中心系统进行开发的，因而既能在单网段中使用，又能在多网段中使用，能够对多网段的大型网络进行很好的统一管理。

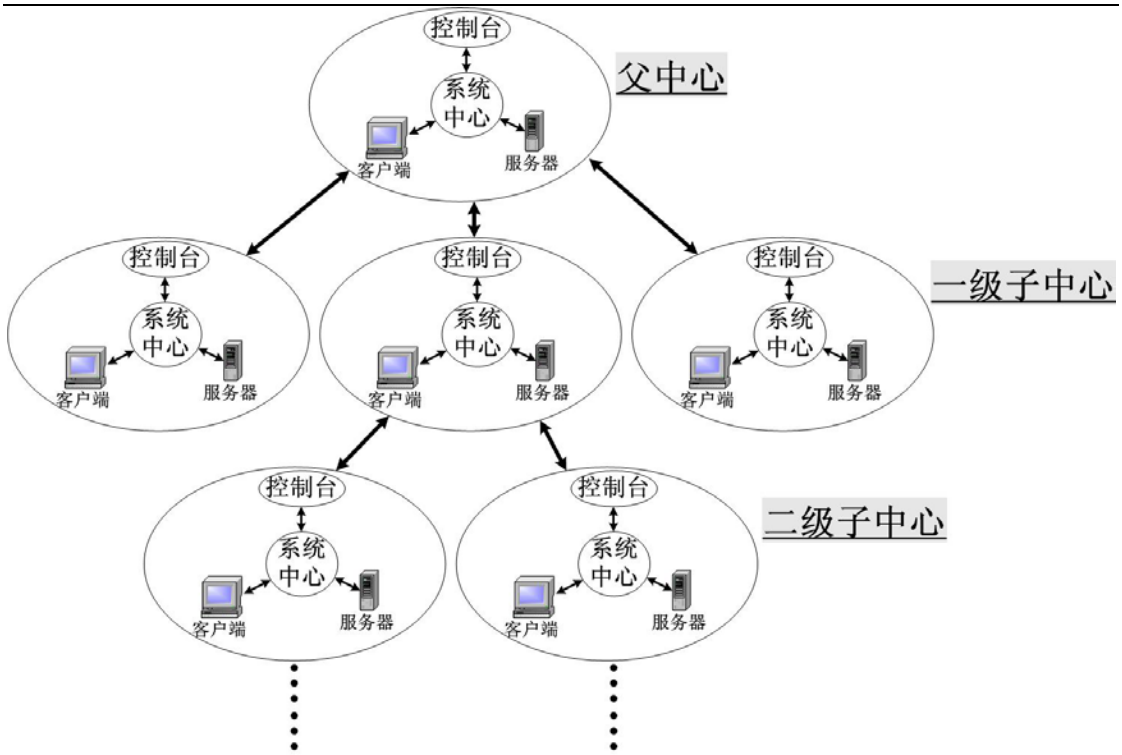

图 3 瑞星杀毒软件网络版可管理大型网络

第四章 瑞星杀毒软件网络版的升级管理

4.1 多种升级方式

瑞星杀毒软件网络版提供了多种升级方式以及自动分发的功能，而且支持多种网络连接方式，具有升级方便、更新及时的特点，网络管理员可以十分轻松地按照预先设定的升级方式实现全网内的统一升级。

具体地讲，瑞星杀毒软件网络版的升级模块有如下特点：

- **全网统一升级**：瑞星杀毒软件网络版的升级过程为系统中心先进行升级，然后系统中心通知每一个客户端或服务器端进行升级，对于当前没有开机的计算机，将在下一次开机时进行升级，这样就保证了全网内的计算机上的瑞星杀毒软件网络版时刻都是最新的，而且时刻版本都是一致的，并且完全杜绝了由于版本不一致而可能造成的安全漏洞和安全隐患。
- **立即升级功能**：管理员在控制台使用立即升级功能，将根据管理员的升级和网络配置，立即启动系统中心的升级进程。
- **管理员只需关心系统中心的升级问题**，而对于客户端和服务器端的升级完全是自动的，一旦系统中心升级完毕，所有的服务器端和客户端将立即自动进行升级，这就最大程度的减少了管理员的参与。
- **对于系统中心的升级，提供三种升级方式供管理员选择：自动下载、自动升级；自动下载、手动升级；手动下载、手动升级**，管理员可以根据自己的网络状况自由选择合适的方式。其中，自动下载、自动升级是根据管理员设定的时间定时从瑞星网站下载更

新文件，自动对全网进行升级；自动下载、手动升级则是自动定时下载手动升级包，然后通知管理员从控制台进行手动升级；手动下载、手动升级则是将控制权交给管理员，由管理员自己去瑞星网站下载手动升级包，然后使用控制台的“手动升级”功能对全网进行升级。

- **支持多种网络连接方式**：局域网或专线上网，代理方式上网（支持 HTTP 代理、SOCKS 代理），拨号上网（支持自动重拨、自动挂断）。
- **下载过程采用了断点续传技术**，使得下载更迅速及时和安全可靠。

4.2 独特的降级功能

出于对用户负责的考虑，确保某些特殊情况（比如升级文件被破坏造成升级之后的功能不正常）下的整个网络的安全不受影响，瑞星杀毒软件网络版提供了回退功能，任何安装了瑞星杀毒软件网络版的计算机都可以安全的回退到上一版本，这样就确保了整个网络在任何情况下都能置于瑞星杀毒软件网络版的最佳防护下。

4.3 增量升级

瑞星杀毒软件采用了全新的增量升级方式，它不象以往那样把升级文件整个下载回来，而是只下载网站上的文件与本地的文件的差异，因而下载量小，减少了网络流量，减轻了网络传输的负担，满足低带宽用户的升级需求。

第五章 瑞星杀毒软件网络版客户端的技术特点

5.1 未知病毒和未知宏病毒查杀技术

瑞星杀毒软件采用了先进的虚拟机技术，能根据程序的行为模式，发现并清除未知病毒和未知宏病毒，这样就在不需要病毒特征码的情况下，有效的防止了新型病毒的破坏和扩散。与其它杀毒软件查杀未知病毒的方法相比，瑞星杀毒软件对未知病毒的查杀具有如下优点：

- 能够查到的未知病毒，绝大多数都能正确的清除。目前其它杀毒软件都不能做到清除未知病毒，瑞星杀毒软件在查杀未知病毒方面的技术处于国际领先地位。
- 对于未知病毒的查杀，查杀率和准确率都很高。

5.2 内存监控

能够监视系统中所有进程和线程运行，在病毒感染或破坏前将病毒清除，并且不影响宿主的正常运行，从而可以安全运行网络或光盘等只读介质上的染毒文件，而目前其它反病毒产品都不能做到这一点。正是运用这一先进技术，瑞星杀毒软件能够彻底查杀内存中的 FunLove 病毒。

5.3 Windows 共享文件杀毒

瑞星杀毒软件成功地解决了正在运行的程序不能被修改的共享冲突难题，在染毒程序运行的情况下，也可以查杀程序文件中的病毒。

5.4 硬盘备份和恢复工具

瑞星杀毒软件提供了功能强大的硬盘数据备份和恢复工具，对用户的数据进行保护，与其它的硬盘备份和恢复工具相比较而言，瑞星杀毒软件的硬盘备份和恢复具有如下独有的优点：

- 备份数据保存在硬盘中，而不是像其它硬盘备份工具使用软盘来保存，因为软盘具有容量小、容易损坏、使用不便、备份和恢复时间长等诸多缺点。
- 实时备份，瑞星杀毒软件硬盘备份和恢复工具可以根据设置进行定期和定时的自动备份，完全不需要用户的参与。
- 备份的数据更多，瑞星杀毒软件硬盘备份和恢复工具能够对 FAT16/FAT32/NTFS 文件系统的引导扇区、文件分配表和目录结构等进行备份，而其它的产品由于软盘容量的限制，不会对目录结构进行备份，这样一旦目录结构遭到破坏就无法恢复，而瑞星杀毒软件硬盘备份和恢复工具则可以轻松恢复。
- 对 NTFS 分区数据进行备份，保存所有与硬盘结构相关的信息。而其它的产品都无法对 NTFS 分区的数据进行备份。

5.5 实现在 DOS 环境下查杀 NTFS 分区

瑞星公司以领先的技术，突破了 Windows NT/2000 NTFS 文件系统格式的读写难题，解决了在 DOS 环境下对 NTFS 格式分区文件进行识别、查杀的问题。瑞星杀毒软件可以彻底、安全地查杀 NTFS 格式分区下的病毒，免除了因 NTFS 文件系统感染病毒带来的困扰。

5.6 SMTP 与 POP3 邮件监控

瑞星杀毒软件的 SMTP 与 POP3 邮件监控，在客户端邮件病毒防护方面又迈出了重要一步，在采用了瑞星杀毒软件的 SMTP 与 POP3 邮件监控之后，用户再也不用担心会发送或接收到染毒的邮件，因为瑞星杀毒软件的 SMTP 与 POP3 邮件病毒监控在用户发送或接收到邮件之前，就已经先对邮件进行了彻底的扫描，让病毒无处藏身。

5.7 支持查杀多种压缩格式文件

瑞星杀毒软件对各种压缩工具进行了细致的分析，支持 DOS，Windows，UNIX 系统下的常用压缩格式，如 ZIP，GZIP，ARJ，CAB，RAR，ZOO，ARC，LZH，UPX……，使得病毒无处藏身。

只要系统资源许可，瑞星杀毒软件支持不限深度的多重解压缩，使得隐藏在压缩包深处的病毒也难以逃脱。

第六章 瑞星杀毒软件网络版产品系列

根据客户网络规模的大小，瑞星公司推出了网络版系列产品，包括：大型企业版、企业版、专用版、中小企业版和网吧版。这些产品间的区别是：

- **大型企业版**：拥有网络版系列产品的所有功能，可控制下级系统中心，可直接控制下级系统中心的任一个客户端；
- **企业版**：多个企业版可组建呈树状结构的多级系统中心，上级系统中心可控制下级系统中心，但不能直接控制下级系统中心的客户端，客户端数量无限制；
- **专用版**：与企业版属同级产品，但在功能设计上是根据用户需求来定制的；
- **中小企业版**：不支持多个中小企业版系统中心之间的通讯，客户端数量≤200；
- **网吧版**：与中小企业版属同级产品，支持在 Windows 9x 操作系统下安装系统中心，但不支持远程安装瑞星杀毒软件、远程查杀和远程设置。