瑞星虚拟化系统安全软件

技术白皮书

北京瑞星网安技术有限公司

2019 年 **2** 月 北京 • 中国

目 录

公司简介

瑞星品牌诞生于 1991 年刚刚在经济改革中蹒跚起步的中关村，是中国最早的计算机反病毒标志。瑞星公司历史上几经重组，已形成一支中国最大的反病毒队伍。瑞星以研究、开发、生产及销售计算机反病毒产品、网络安全产品和反“黑客”防治产品为主，拥有全部自主知识产权和多项专利技术。

目前，瑞星公司已推出基于多种操作系统的瑞星全功能安全软件单机版、网络版软件产品；以及企业防毒墙、防火墙、网络安全预警系统等硬件产品，是全球第三家、也是国内唯一一家可以提供全系列信息安全产品和服务的专业厂商。

在公安部组织的计算机病毒防治产品评测中，“瑞星全功能安全软件”单机版、网络版曾双双荣获总分第一的殊荣，并连续 5 年蝉联至今。公司拥有国内最大、最具实力的反病毒和网络安全研发队伍，并且拥有国内安全行业唯一的“电信级”呼叫服务中心和“在线专家门诊”Online 服务系统。

瑞星和政府机构、商业伙伴以及媒体有着广泛而深入的合作关系，借助内外部各种资源，目前已建成五大安全网络体系——全球计算机病毒监测网、全球计算机病毒应急处理网、全国计算机病毒预报网、全国反病毒服务网以及全球病毒疫情监测网。

瑞星公司总部设立在北京，在全国各地设有分支机构。目前公司拥有国内最大的信息安全研发团队、国内最大的客户服务团队，以及销售、市场、网站等部门，并已经建成覆盖全国的庞大的销售和市场体系。

目前瑞星拥有 6000 万正版个人用户，7 万多家企业用户，主要软件产品以中（简、繁体）、英、俄、德、日五种语言版本推向全球市场，销售网络覆盖北美、欧洲、亚太等地区。作为在中关村成长起来的高科技企业，瑞星正逐步走向世界，实现公司的美好愿景——成为全球最具价值的信息安全产品和服务提供商。

方案简介

瑞星虚拟化系统安全软件是北京瑞星信息技术有限公司推出的企业级虚拟化平台的安全防护软件产品解决方案。

瑞星虚拟化系统安全软件是瑞星公司推出的国内首家企业级虚拟化安全防护解决方案，支持对虚拟化环境与非虚拟化环境的统一管控，包括 VMware vSphere、HUAWEI Fusion Sphere、 Windows 系统与 Linux 系统等，可以有效保障企业内部虚拟系统和实体网络环境不受病毒侵扰，是各行业虚拟化产品安全防护解决方案的首选。

产品简介

瑞星虚拟化系统安全软件可有效地保障企业虚拟网络和物理网络不受病毒侵扰。

瑞星虚拟化系统安全软件产品由以下子系统组成：

- 瑞星管理中心
- 瑞星安全虚拟设备
- 瑞星日志中心
- 瑞星升级中心
- 瑞星查杀协作

瑞星虚拟化系统安全软件适用于所有大中小型企业。可安装在下列各种平台：

- Windows 2000（32-bit and 64-bit）
- Windows XP SP2（32-bit and 64-bit）
- Windows 2003 SP2（32-bit and 64-bit）
- Windows Vista（32-bit and 64-bit）
- Windows 2008（32-bit and 64-bit）
- Windows 2008 R2（64-bit）
- Windows 7（32-bit and 64-bit）
- Windows 8（32-bit and 64-bit）
- Windows 8.1（32-bit and 64-bit）
- Windows 10（32-bit and 64-bit）
- VMware vCenter 4.0.0 及以上
- ESXi 5.0.0 及以上版本
- FusionSphere R5、R6、6.3.1KVM 等版本

安全终端Linux杀毒支持目前主流的国内外Linux操作系统、国内外芯片

- Linux系列： Red hat Linux、CentOS、SUSE Linux、红旗Linux、Ubuntu Linux、深度、凝思、中标麒麟、银河麒麟、湖南麒麟等
- 芯片系列：Intel x86、龙芯、飞腾、申威

产品优势：

100%自主知识产权：整套系统全部由瑞星公司自主研发，安全可控。

国内首家：国内首家完美支持华为和 VMware 等主流虚拟化平台的安全解决方案。

全球领先的无代理模式：从最底层深度保护数据安全、网络安全及数据完整性。

统一智能管控：对所有虚拟机进行统一查杀病毒以及升级管理，并实时监控所有虚拟机的网络安全状况。

零安全风暴：避免安全风暴，最大化发挥虚拟平台的资源优势。

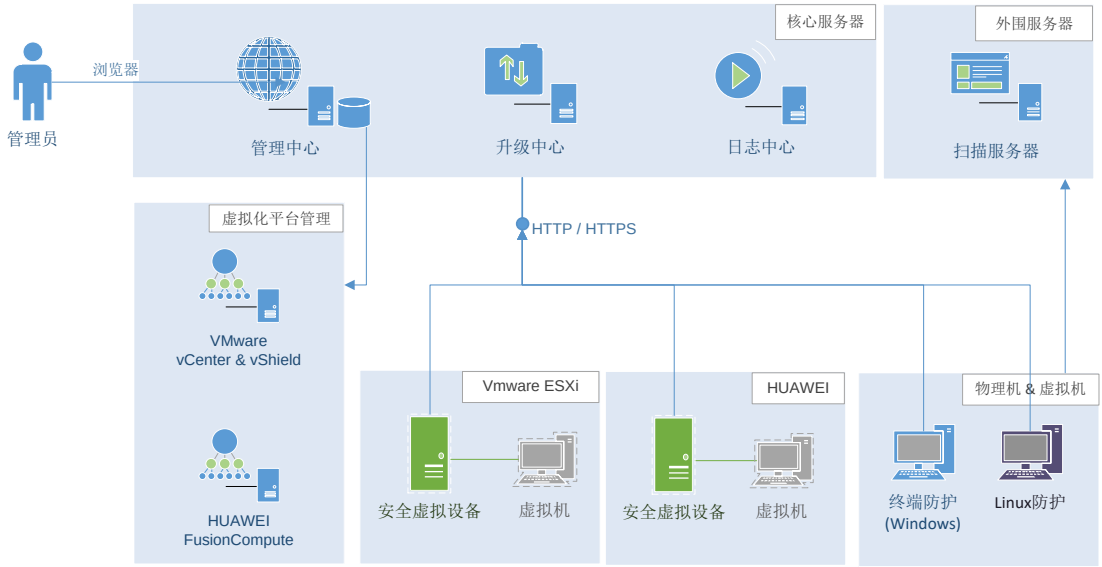
四维立体防护：基于瑞星基因决策引擎、下一代虚拟化 DPI 技术、虚拟攻防系统及大数据采集分析，全面保护虚拟化平台的系统与网络安全。

下一代虚拟化 DPI 技术：通过“瑞星虚拟攻防系统”、瑞星云端大数据分析，智能生成海量拦截规则，有效解决 APT、NDay 及 0Day 等已知未知网络威胁。

第一章 瑞星虚拟化系统安全软件的系统结构

1.1 完整防护体系结构

瑞星虚拟化系统安全软件的完整防护体系由管理中心、升级中心、日志中心、扫描服务器、安全虚拟设备、安全终端 Linux 杀毒和安全防护终端等子系统组成，各个子系统均包括若干不同的模块，除承担各自的任务外，还与其它子系统通讯，协同工作，共同完成企业内部的安全防护。



1.2 子系统描述

1. 管理中心：作为管控服务器，一方面为管理员提供 B/S 方式的管理界面交互，另一方面负责为客户端提供策略、任务、授权等业务数据。

2. 升级中心：在企业内部为所有客户端提供 http 方式的升级服务，以减轻客户端对互联网的依赖；自身同时支持手动与自动方式升级。

3. 日志中心：接收各客户端产生的日志数据，统一进行入库操作，并负责之间的数据同步；。

4. 扫描服务器：独立子产品，提供云端查杀服务查杀协作是轻量化高性能软件组件，可选安装在被保护的虚拟机上，配合安全虚拟设备实现查毒后的隔离及后处理操作。

5. 安全虚拟设备：存在于每一台虚拟主机上（如 ESXi），为其上的每一台无代理虚拟机提供安全防护服务，不需要被保护的虚拟机再安装安全产品。

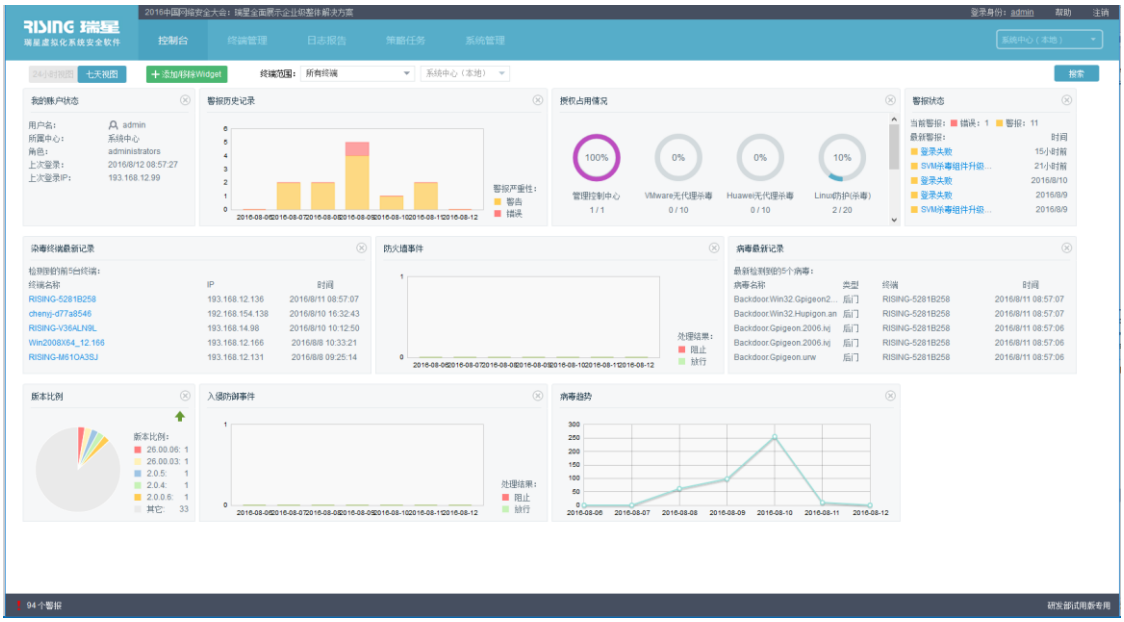
6. 终端防护与 Linux 防御：终端安全类子产品，支持 Windows 与 Linux 系统，主要安装在物理机上，也支持安装在虚拟机上，此时将接管无代理安全防护。

瑞星虚拟化系统安全软件支持对虚拟化环境与非虚拟化环境的统一管控，管理员可以对 VMware vSphere / HUAWEI Fusion Sphere 环境内的虚拟机和物理设备进行一致化管理。系统工作时，管理员按需为终端设定策略与任务，各终端连接管理中心后得到相关信息，按管理员的设置参数工作，并将产生的安全业务日志上报到日志中心。

第二章 瑞星虚拟化系统安全软件的系统功能

2.1 全面直观掌握系统安全状况

管理员能够实时查看到每个客户虚拟机的扫描状态、实时监控状态、版本信息、感染病毒情况等信息，并实时跟踪到每一个虚拟机的防毒状况，以便做出应对措施。

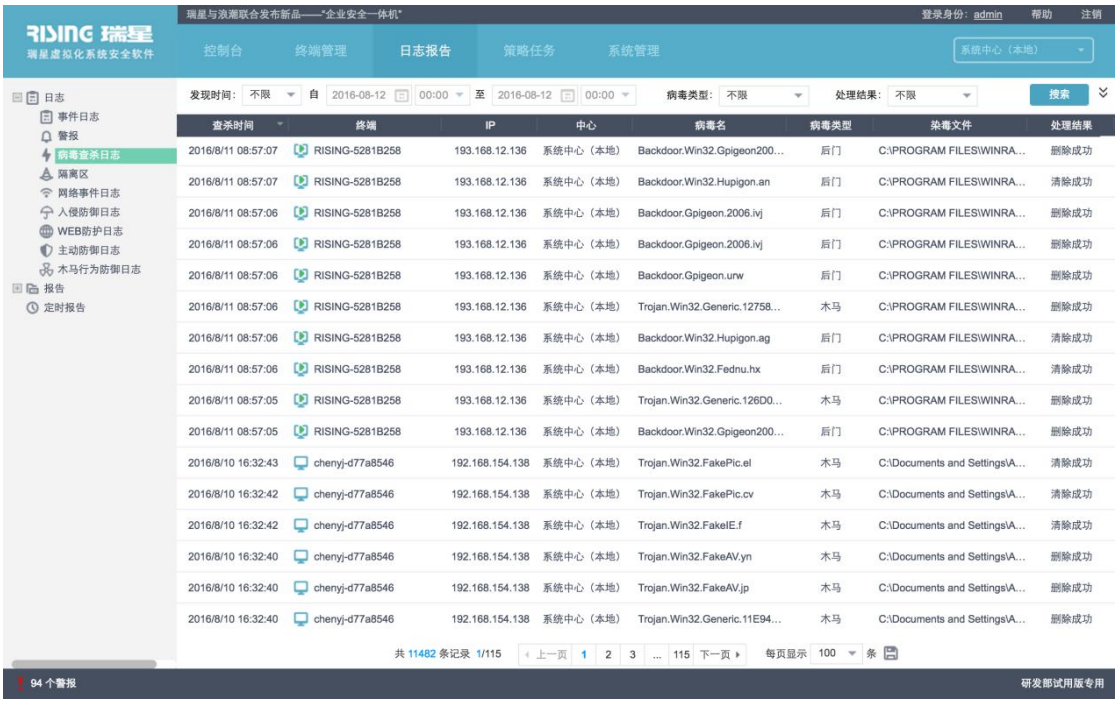


2.2 全网查杀病毒

能够随时对虚拟机网络执行统一查杀毒，最大程度的减小了病毒传播的可能。当然，管理员也可使用管理控制台对单个或多个客户虚拟机进行查杀病毒。

2.3 病毒与安全事件报警

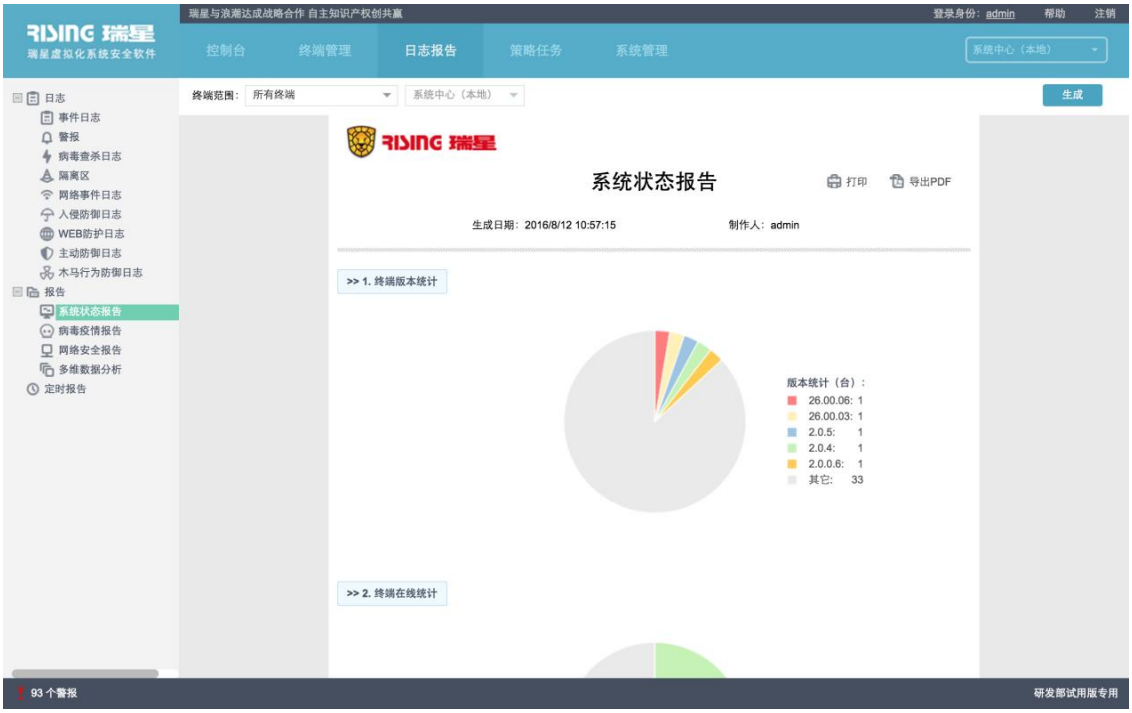
安全软件管理中心记录整个虚拟机网络中任意终端上发现的病毒信息和异常事件，方便管理员能及时发现染毒的客户虚拟机和系统运行的异常，并做出及时反应。



2.4 丰富的病毒日志统计与分析功能

能够统计染毒终端最新记录、病毒最新记录、病毒趋势等诸多日志分析数据和图表，便

于管理员直观地掌握虚拟机网络内病毒感染情况和发作趋势。



2.5 防毒策略的定制与分发

管理员可通过管理控制台对全网或某个分组设置统一的防毒策略，也可对特定的虚拟机设置防毒策略，保证防病毒策略的有效实施。

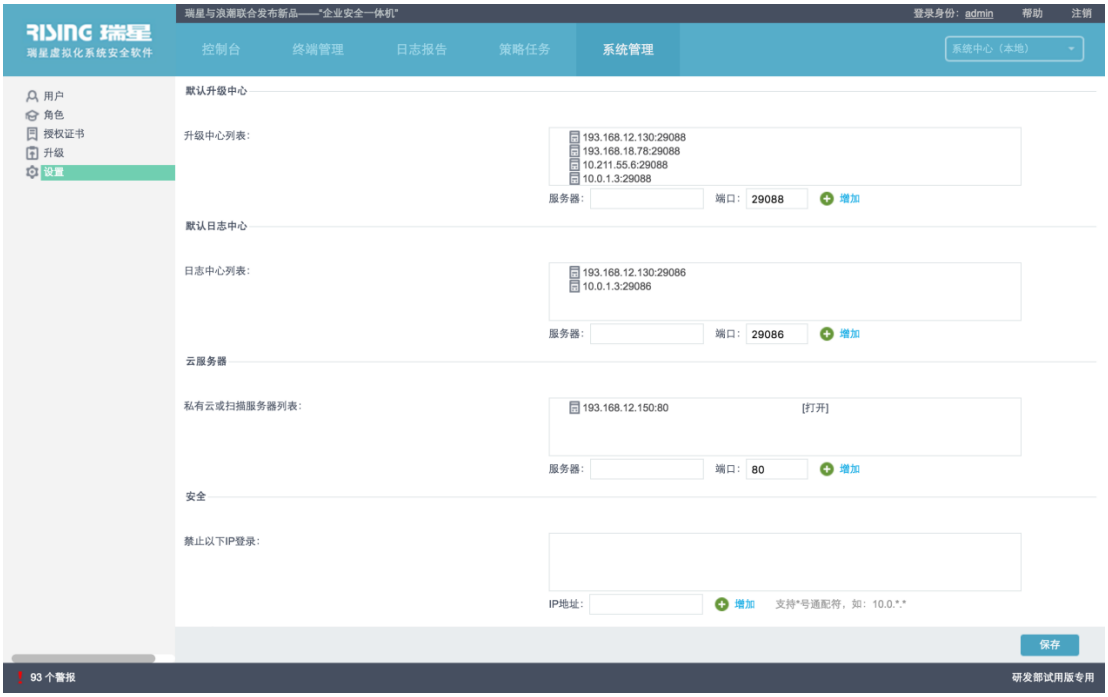
2.6 多升级中心负载均衡

支持升级中心多级分层结构，且对分层级数没有限制，可以实现升级任务的负载均衡，

提高产品升级效率。

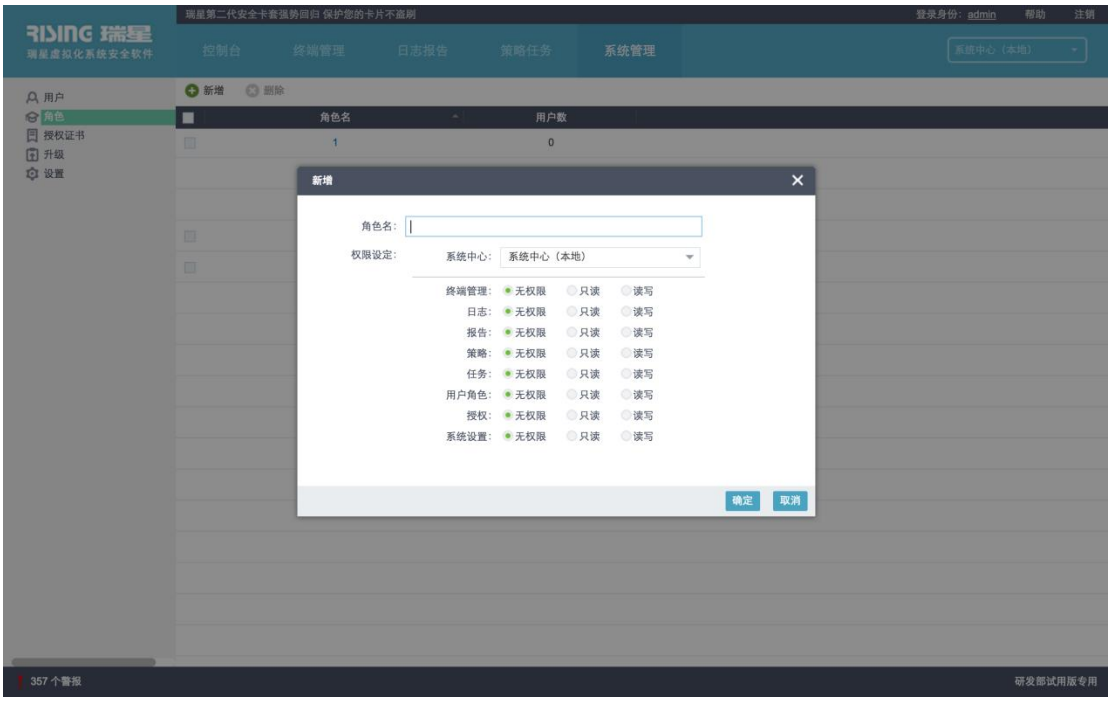
2.7 日志负载均衡

规避各类系统日志、安全日志给虚拟机网络带来的资源占用问题，提高日志上报效率。



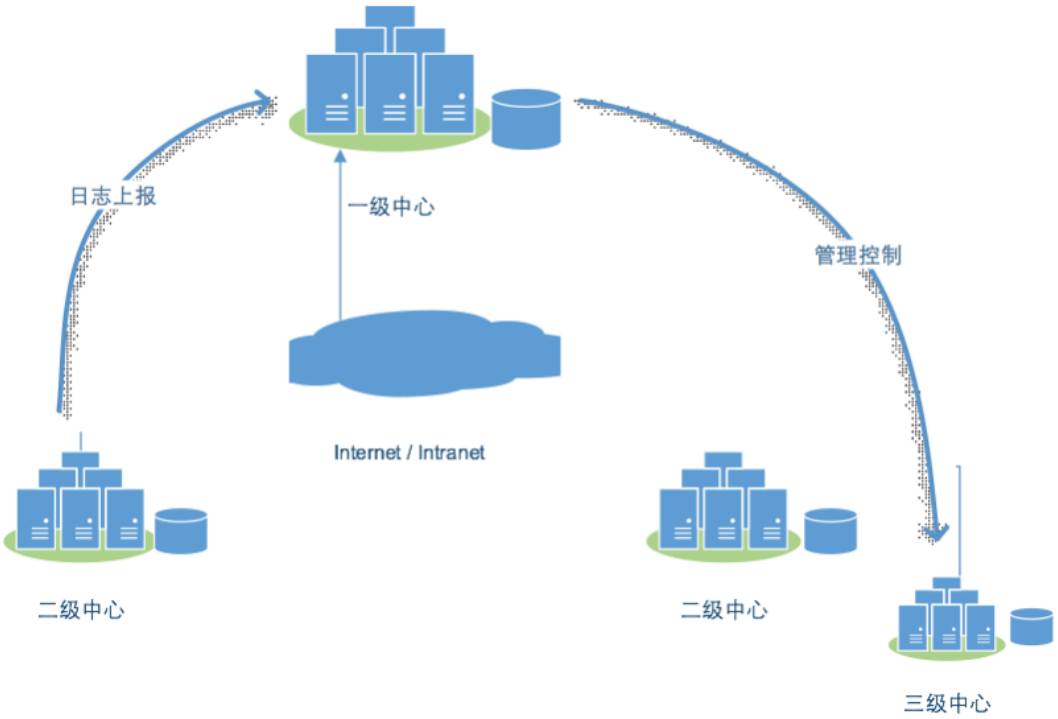
2.8 支持设置不同权限层级用户

基于角色的用户管理，支持设置不同权限层级用户的访问和编辑权限集合，控制用户可以操作和查看的功能信息，避免非授权人员使用引发的安全风险。



2.9 跨级管理

上下级之间可以级联为一个更大的整体，以适应组织过大、异地管理等问题。下级中心的部分日志会适时同步到上级中心，供上级中心统一生成报表或查看详情。上级中心可直接管控下级中心，就像管理本级中心一样。跨级可以适应较复杂的链路环境，只要求下级中心对直接所属的上级中心有单向连接能力即可。级联理论上可以支持无限个层级。



第三章 瑞星虚拟化系统安全软件的安全管理

3.1 管理中心

管理中心提供的管理控制台是瑞星虚拟化系统安全软件集中管理所有终端安全状态的管理工具。管理员通过管理控制台，可以了解整个用户网络的总体安全状况，直观的查看所有终端当前的实时监控状态、病毒查杀情况、组件版本信息等；能够对任意终端执行远程安全管理，进行定期、实时地查杀病毒和全网统一升级管理，真正做到在整个用户网络中建立起坚实的安全防护系统。

3.1.1 控制台

控制台展示时间试图，提供 Widget、搜索等功能。

3. 1. 2 终端管理

终端窗口显示可以监控和管理的网络上的终端组织结构信息，包括名称、IP、端口、产品形态、版本、防病毒、网络安全、主动防御、状态、操作系统和主机。

终端窗口支持条件搜索，可选条件包括：终端名称/IP、类型（包括不限、虚拟主机、安全虚拟设备、虚拟机、物理机）。

3. 1. 3 日志报告

【日志】分为【事件日志】、【警报】、【病毒查杀日志】、【隔离区】、【入侵防御日志】、【WEB 防护日志】、【主动防御日志】和【木马行为防御日志】。

【报告】分为【系统状态报告】、【病毒疫情报告】、【网络安全报告】和【多维数据分析报告】。

3. 1. 4 策略任务

瑞星虚拟化系统安全软件支持创建各种杀毒策略和终端代理策略模板，用于下发设置至组和终端，简化管理操作。

任务窗口显示所有任务事件，任务事件信息包括创建时间、类型、创建人、状态、进度以及详情链接。

计划任务支持自动化和预设某些常见任务，已设定的计划任务将根据预设的时间表启动。

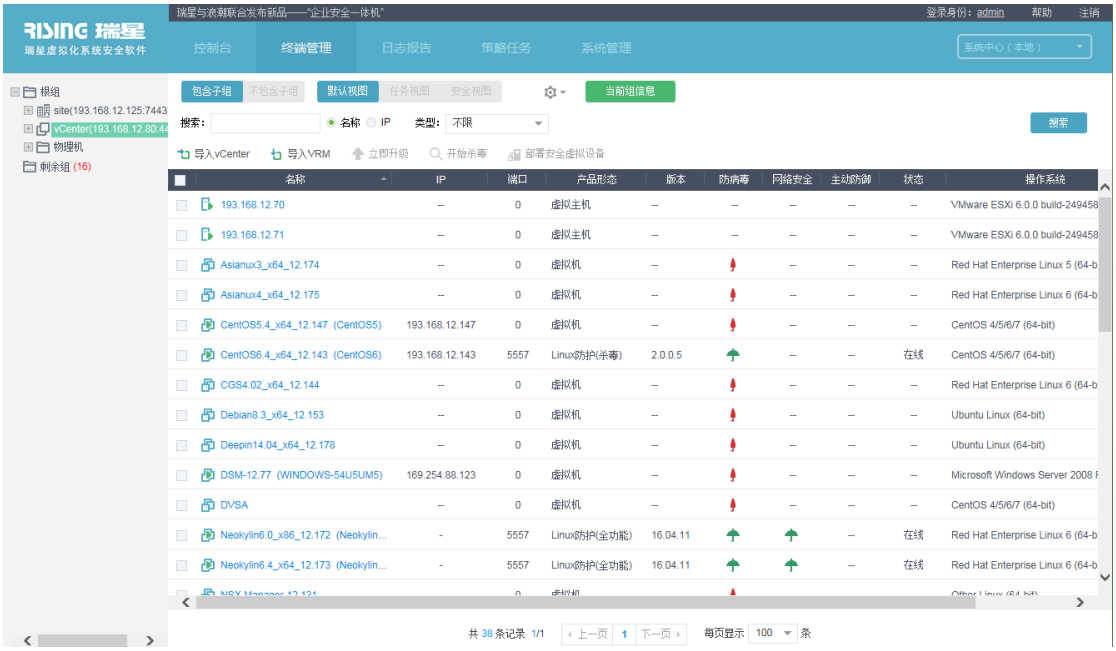
3.1.5 系统管理

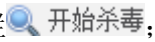
系统管理可以进行用户、角色、授权证书、升级及设置项管理。

3.2 VMware 无代理

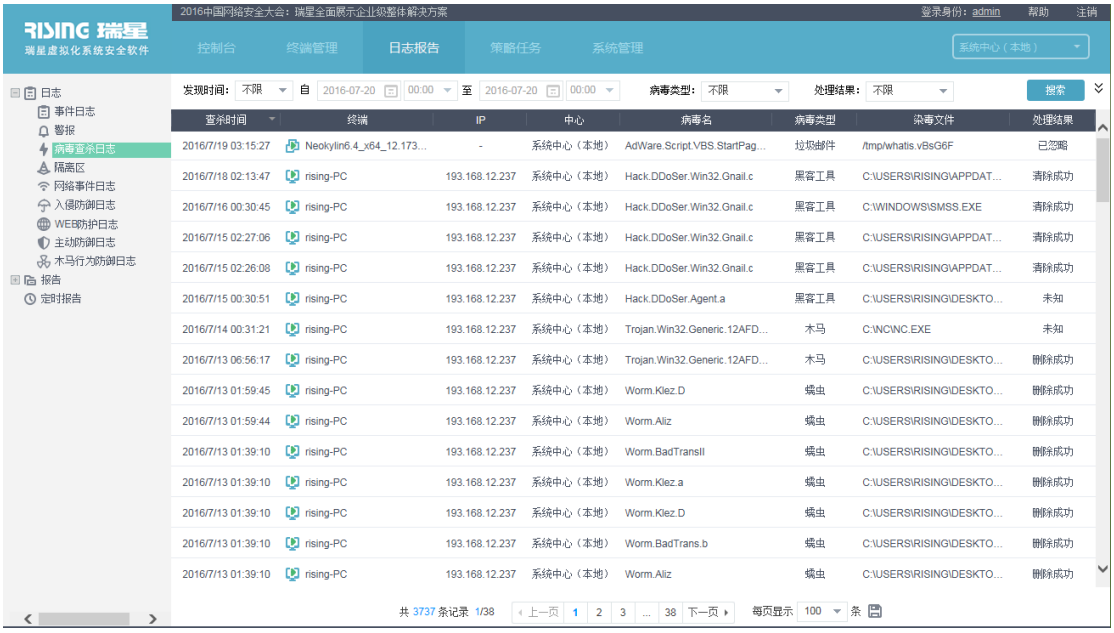
3.2.1 手动查杀

管理员可通过管理控制台或工具对客户虚拟机执行手动查杀操作，在【终端管理】标签页，点击【vCenter】组，显示所有被管理的 VMware 终端；



勾选需要查杀的虚拟机终端，点击工具栏  ；

当查杀病毒时，点击【病毒查杀日志】，实时查看查杀记录；



3.2.2 文件监控功能

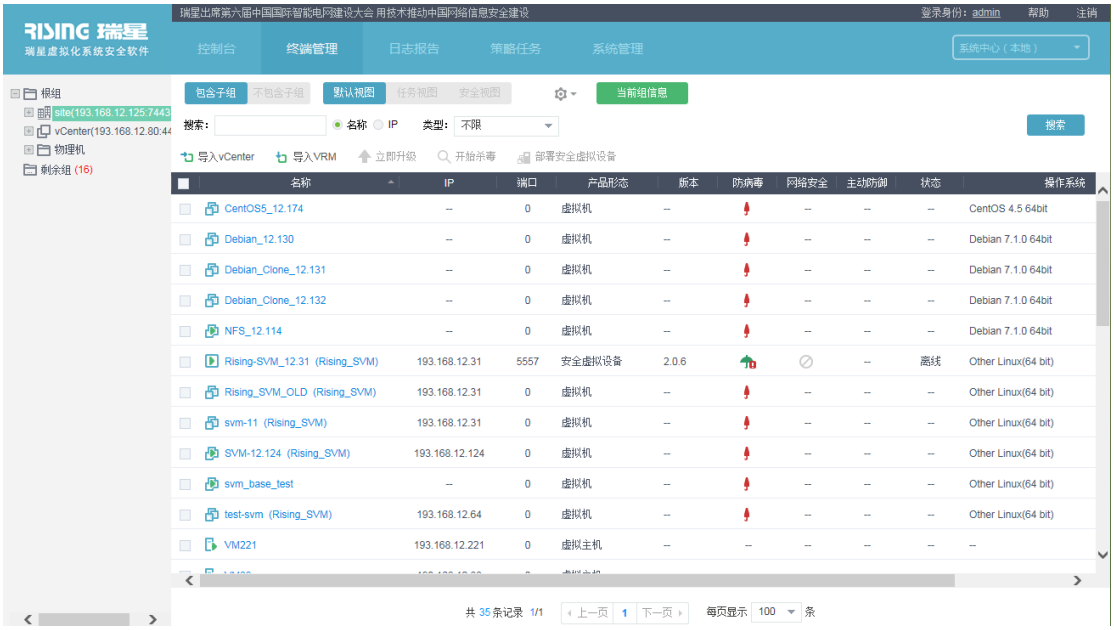
文件监控用于实时的监控虚拟化系统中的文件操作，在终端进行文件操作之前对文件查毒，从而阻止病毒运行，保护虚拟化系统安全。

文件监控发现病毒时，在管理中心控制台的病毒查杀日志窗口会列出相应的病毒查杀记录信息。

3.3 Huawei 无代理

3. 3. 1 手动查杀

管理员可通过管理控制台或工具对客户虚拟机执行手动查杀操作，切换到【终端管理】标签页，点击【site】组，显示所有被管理的 VRM 终端，；



勾选需要查杀的虚拟机终端，点击工具栏 开始杀毒 。手动查杀请参考本文档章节 3.2.1

3. 3. 2 文件监控

文件监控请参考本文档章节 3.2.2 文件监控。

3.4 安全终端 Linux 客户端

安全终端 Linux 杀毒提供有代理部署场景下的 Linux 系统安全防护功能，不但支持使用客户端设置执行本地查杀，而且能够接收管理中心下发策略进行远程扫描，处理结果以日志形式统一上报管理中心。

3.5 安全防护终端

安全防护终端提供有代理部署场景下的 Windows 系统安全防护功能，支持使用病毒查杀设置执行本地查杀和远程扫描指令，并能够实现本地实时监控、主动防御等高级防护，处理结果以日志形式统一上报管理中心。

3.6 全功能安全防护终端

全功能安全防护终端是一款多功能的软件，既能防止病毒入侵保护系统文件安全，又能阻止网络攻击防护网络安全，同时实现管理中心管理和客户端自我管理两种方式，满足企业和个人的不同需求。另外该软件适用于多种环境，既可以安装在虚拟机维护虚拟机的安全，又可以安装在实体 PC 上，可以根据客户的不同需求能够同时满足系统防护和网络防护功能，又能单独安装一个功能，用户可以根据自己的需求定制化安装。

3.6.1 配置管理

在虚拟化安全软件系统中，管理员可以通过管理中心对安全防护软件进行管理，既可以对所有安全防护软件的客户端进行统一管理，也可以针对不同客户端进行定制化管理。管理员可以管理的内容为：

策略设置：

1.杀毒策略设置：查杀策略 文件监控策略 内核监控策略 U 盘防护策略等， 从主动查杀到系统监控，做到全面的安全设置。

2.网络防护策略设置：防止入侵攻击策略 VPatch 策略 阻止对外攻击策略 web 信誉策略 敏感词管理策略 以及防火强的 IP 策略 端口策略 应用程序管理策略等，从网络防护的内部和外部全面防护。

3.通用设置：升级策略 升级中心 日志中心 云查杀中心等策略设置

任务管理：

1.扫描任务：管理员可以通过下发扫描任务对客户端系统进行多种扫描方式，包括全盘扫描，快速扫描和自定义扫描，管理员可以根据需求下发扫描任务。

2.备份恢复任务：当病毒文件被查杀，会保存在隔离区内，管理员可以根据需求针对隔离文件进行恢复。

3.升级任务：管理员可以设置定时任务，有管理中心在设定的时间下发升级任务，也可以在需要升级的时候，管理员直接下发升级任务，从而及时更新软件和软件内部的病毒库攻击库等，及时有效的保护系统安全。

监控状态显示：

客户端会实时上报监控状态，管理员可以根据客户端的权限，设置不同的监控开关，做到统一化和个性化管理。

日志管理：

客户端会实时上报日志信息，包括事件日志，病毒查杀日志，隔离日志，安全防护日志，网络事件日志，入侵防御日志，出站攻击日志，联网程序日志以及 web 信誉日志等等，及时提醒管理员注意客户端的状态，以便管理员尽早发现攻击，采取合适的对策。

3.6.2 病毒查杀

全功能安全防护终端为用户提供多种查杀方式：快速查杀、全盘查杀、自定义查杀，用户可以根据自己的需求进行选择。

瑞星安全防护软件提供三种查杀途径：公有云 私有云和本地库查杀

公有云：瑞星公有云拥有非常全面丰富的木马库，客户端可以非常快速的通过公有云查询到本机感染病毒的文件，同时降低本地的 CPU 占用，内存占用以及 IO 接口的读取时间，

大大节省系统资源。

私有云：由于企业的网络环境，部分企业可能无法连接瑞星公有云，在这种情况下，企业可以在内部部署瑞星私有云，能够代替公有云实现快速查杀，瑞星私有云可以在线升级，也可以通过手动包升级，以便及时丰富木马库，保证系统安全。

本地病毒库：当企业的网络环境，既不能连接瑞星公有云，也不能部署瑞星私有云，我们为杀毒提供了全面的本地病毒库，不放过任何一个病毒，保护系统的安全。

管理员可以根据自己的网络环境，为各个客户端配置查杀途径。

3.6.3 系统防护

全功能安全防护终端的系统安全既能够提供多种的快捷病毒查杀方式，又能对系统进行实时监控和主动防御，从而保障系统不受病毒侵害。系统防护功能包括：文件监控、内核监控、U 盘防护。

3.6.4 网络防护

网络安全功能主要为系统提供全面的网络防护功能，主要包括以下功能：IDS/IPS、SQL 防注入、VPatch、web 信誉、阻止对外攻击、敏感词审查、联网程序控制、ip 规则设置以及端口规则设置。

3.6.5 上网管理

管理员可以通过此功能对员工的上网行为进行控制，规定员工的上网时间、可访问的网址、禁止使用的上网程序。管理员可以设置工作日工作时间内，禁止使用聊天工具，禁止使用下载工具，禁止玩网络游戏，禁止播放器播放在线视频，还可以设置其他禁止使用的应用程序，保证企业员工的有效工作时间，营造良好的企业工作氛围。同时为了丰富员工的业余生活和休闲时间，管理员可以设置非工作时间开放这些限制，方便员工进行网络购物和网络娱乐，提升员工的幸福感，激发员工的工作积极性。

3.6.6 安全日志

用户可以通过安全日志查看病毒日志、隔离日志、防护日志、监控日志、扫描日志、内核加固日志、上网拦截日志、防黑客日志、规则触发日志、共享管理日志、自我保护日志以及软件升级日志等，使用户可以全面了解系统的安全信息。

3.7 Linux 全功能防护端

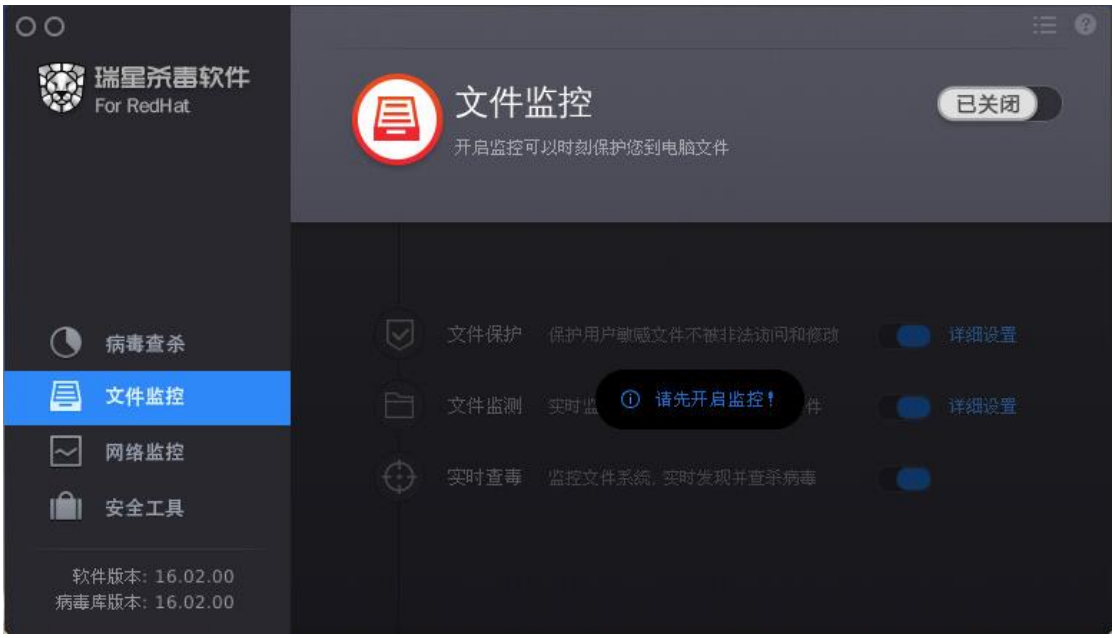
Linux 全功能防护端主要提供的功能模块有“病毒查杀”、“文件监控”、“网络监控”、“安全工具”四大项。

3.7.1 病毒查杀

“病毒查杀”是指用户发起的对计算机系统上的磁盘文件进行扫描，并对扫描出的木马病毒进行查杀，该项目包括“自定义查杀”、“快速查杀”、“全盘查杀”等功能模块。

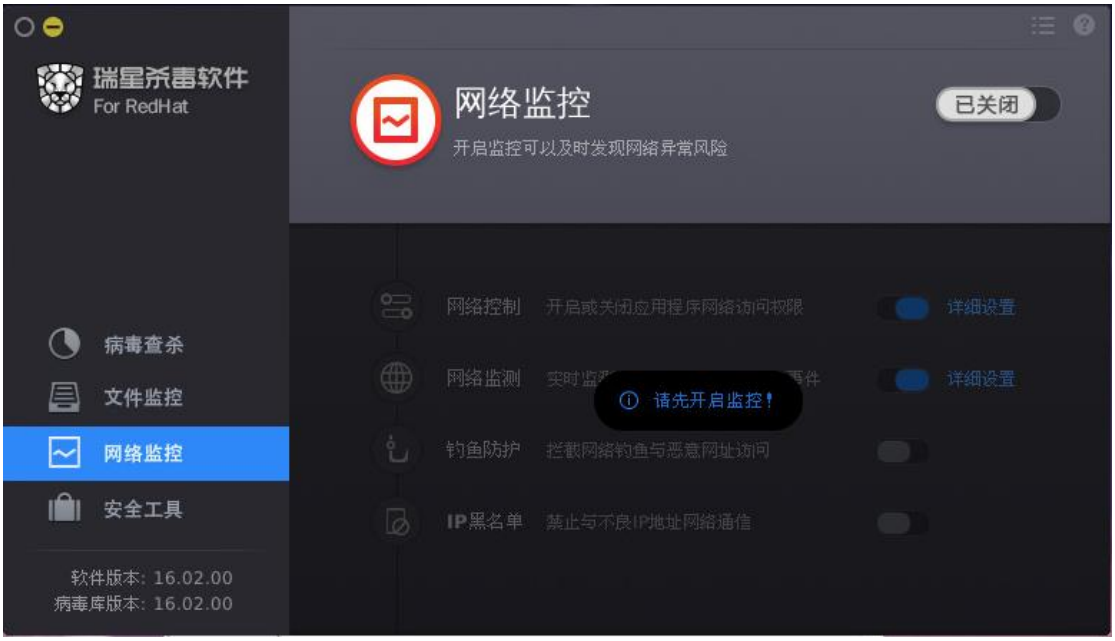
3.7.2 文件监控

文件监控模块实现对系统相关的文件操作进行监控，提供的功能包括：文件保护、文件监测和实时查毒。



3.7.3 网络监控

“网络监控”可以对本系统正在运行的进程或可执行程序对网络的访问进行监控，可根据设置控制程序或进程对网络数据访问并记录日志。其提供的功能有：网络控制、网络监测。



3.7.4 安全工具

安全工具可为用户提供方便、安全的软件或相关服务，包括“瑞星安全工具”和“系统使

用工具”。

用户可在瑞星杀毒软件 for Linux 的主界面点击左列“安全工具”来打开“安全工具”界面。