悬镜管家 V3.0.1

操作手册

北京安普诺信息技术有限公司

（http://www.x-mirror.cn/）

二〇一六年

目 录

1. 前期准备

1.1 简介

随着互联网技术的不断发展，传统的服务器防护已经不能满足用户的需求。尤其是在移动互联网技术快速发展的当下。

经过对相关领域以及同行业发展态势的研究发现：许多具有竞争能力的安全服务器卫士都转向了以数据为驱动的云平台研究。同时对市场用户的需求调研发现：用户更加渴望快速、便捷的服务。

本着行业领先以及为了更好的适应用户需求的宗旨，安普诺一直在不断地探索，历时数月，在产品和研发团队持续不断的努力下，以悬镜管家为核心的安普诺云诺安全管控云平台 V3 版本诞生了。

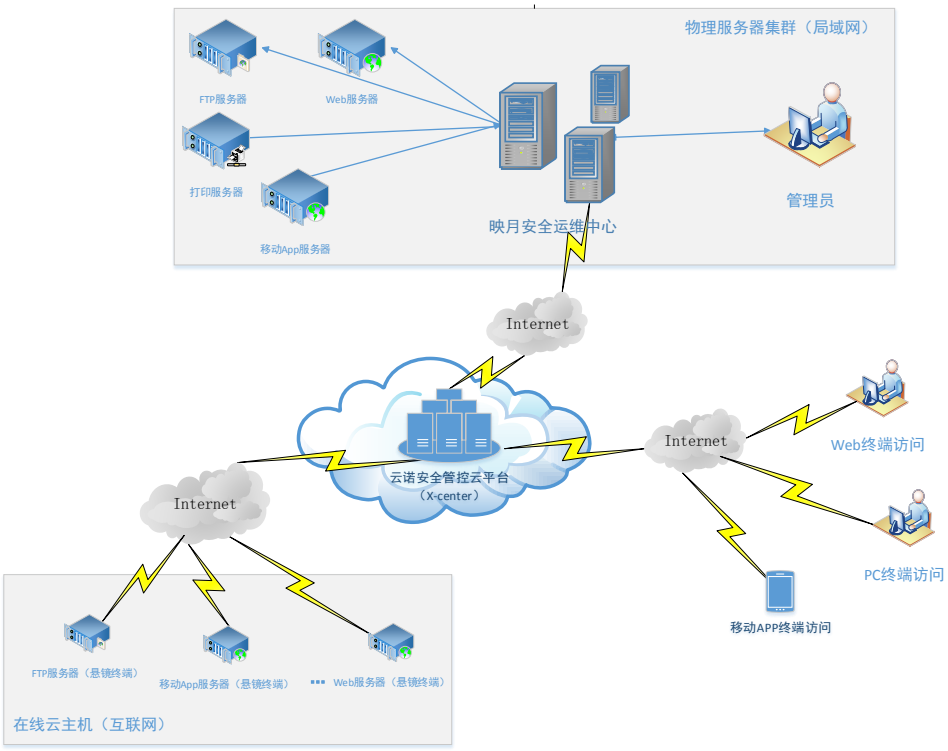

图 1-1-1 云诺安全管控云平台网络拓扑图

上图为云诺安全管控云平台的网络拓扑图，从图中可以看到，以云诺安全管控平台为中心，利用 Web 终端、PC 终端以及移动 APP 终端实现对平台的访问实现

对安装了悬镜服务器卫士服务器的管控，通过与映月安全运维平台的交互实现局域网内部服务器策略的更新以及下发，同时服务器也可以以在线云主机的方式实现与云诺安全管控云平台的交互。云诺安全管控云平台具有新一代服务器威胁感知与安全加固云系统的特点。

悬镜力求帮助用户以多终端的方式实时、批量管理服务器，云诺安全管控云平台以云诺云中心账号登录，每个云中心账号都提供万台服务器同时在线安全管理、批量监控的能力。

悬镜管家 Windows 端又分为：批量管理和一对一管理两种模式，批量管理是为多台网络服务器用户量身打造的一键式批量管理服务器安全软件。一个悬镜管家 Windows 端的批量管理模式下能够管理多台服务器。

通过悬镜管家 Windows 端的批量管理模式添加服务器到云诺安全管控云平台账户中，利用云中心账号登录到云诺安全管控云平台即可实现对多台服务器系统跨平台批量安全管理与监控，让服务器的管理变得更加快捷、简单。

图 1-1-2 云诺账户

一个云诺账号可以分别供 Web 端、Android 手机端、Windows PC 端使用，任何一种方式都能实现对服务器的管理。

1.2 部署环境及软件安装

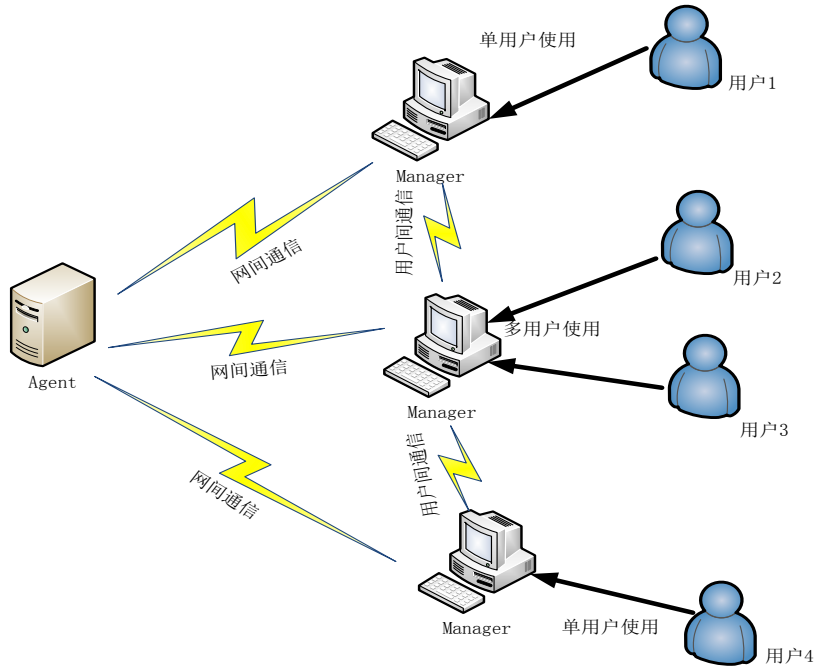

图 1-2-1 部署环境

表 1-1 软件部署环境（1）

悬镜管家（软件）	操作系统版本(部署环境)
管理端（Manager--Windows 平台） 1、 为用户提供管理操作界面； 2、 为用户提供可视化分析结果；	Windows 7 x86/x64、 Windows 8 x86/x64、Windows 8.1 x86/x64、 Windows 10 x86/x64
代理端（Agent--Linux server 平台） 1、 根据默认安全策略实时保护目标系统； 2、 实时解析管理端发过来的管控命令；	RHEL 5.x / 6.x / 7.x x86/x64 CentOS 5.x / 6.x / 7.x x86/x64 Ubuntu server 12.04/14.04/15.04/15.10/16.04 LTS x86/x64 SUSE10/11/12

表 1-2 软件部署环境（2）

悬镜管家	环境要求
管理端（Manager）	.NET 4.0 及以上
代理端（Agent）	如果您想使用网站漏洞防护功能请在安装本软件前确认 Apache 或者 Nginx 服务已运行！

表 1-3 软件支持的 Web 服务器版本

WEB 服务器	服务器版本
Apache	2.2.x 2.4.x
Nginx	0.x.x 1.x.x

1.3 软件安装

本软件是基于 C/S 架构，分别为管理端与代理端，管理端适用于 Windows 7 x86/x64 、Windows 8 x86/x64、Windows 8.1 x86/x64、Windows 10 x86/x64 平台，代理端适用于 CentOS

（RHEL）5.x /6.x　x86/x64 平台、7.x x64 平台、Ubuntu server 12.04/14.04/15.10 LTS x86/x64 平台以及 SUSE10/11/12。

软件针对 Web 服务器设计了一套全面的防护方案，支持的服务器为目前国内外主流的 Apache 和 Nginx 两大 Web 服务器，其中 Apache 支持版本为 2.2.x 与 2.4.x；Nginx 支持的版本为 0.x.x 与 1.x.x，同时，也支持类如 lampp 集成包安装配置的网站服务器。这里建议您在安装本软件前在服务器系统中安装并启动 Apache 或者 Nginx 服务，如果您的服务器系统中未安装并启动 Apache 或 Nginx 服务，本软件针对 Web 服务器防护的功能，例：SQL 注入防护、XSS 注入防护、CC 攻击防护功能将不会开启。在安装本软件前，请您确保服务器上的 Web 服务正在运行。

安装本软件时将管理端、代理端分别安装到适用环境下，代理端针对操作系统分为 32 位与 64 位。本操作手册中以代理端操作系统 CentOS 6.5 x86，管理端操作系统 Windows 7 x64 为例，其他系统环境类似，具体的安装步骤如下：

代理端安装步骤如下：

- 把悬镜代理端的安装包放在 linux 系统的用户自定义目录下。
- 打开终端输入 su　root，然后根据提示输入密码进入 root 权限；

```
[gs@localhost Desktop]$ su root
Password:
[root@localhost Desktop]#
```

图 1-3-1 su root 命令界面

- 进入到安装包所在目录，输入命令./Xmirror3.0.1.2927_rhel_x86.bin(输入的安装命令根据具体的安装版本有相应的调整)进行安装，如下图：

```
[root@localhost ~]# ./Xmirror3.0.1.2927_rhel_x86.bin
Preparing & Unpaking:

++++++++++++++++++++++++++++++++++++++++++++++++++=>100%

Do you want to save the previous configuration(Y/n): y
Init Environment:                                          [ OK ]
Check System:                                              [ OK ]
Init Dirs:                                                 [ OK ]
Copy Files:                                                [ OK ]
```

图 1-3-2 安装命令界面

免费公开版本中不需要下面的认证步骤，在非公开版本中代理端安装到最后步骤，需要根据安装的注册码申请 key，输入相应的 key，代理端才能安装成功。如果您是免费版本请跳过以下注册码的步骤（蓝色部分）。

专业版需要认证，同时支持两种认证方式，一种是在线认证方式，另一种是非在线认证方式。在线方式不需要相应的注册码，只需要输入 key 就会自动联网完成 key 的验证；非在线方式需要软件安装时产生的注册码，通过联系我们获得相应的 key，输入 key 后软件才能验证成功。

- 安装后获得软件启动验证码，拿这个验证码去申请 Key

图 1-3-3 xmirrord 的安装提示（3）

- 输入 key 后完成安装，如果像下图一样没有再次显示需要验证，证明 key 为正确，现在就可以使用了；如果继续提示请输入，说明输入的 key 不正确：

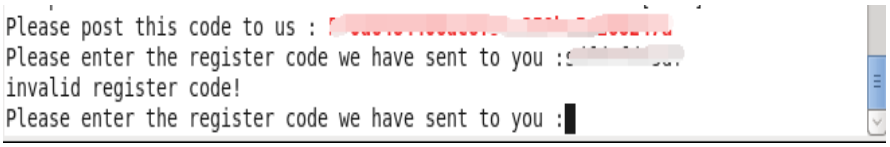

图 1-3-4 xmirrord 的安装提示（4）key 输入错误

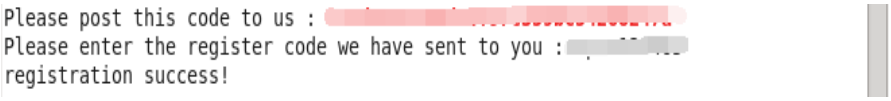

图 1-3-5 xmirrord 的安装提示（5）成功安装

- 看到“Welcome to Xmirror Protection,Enjoy!”提示后，代理端的安装就成功了，现在安全卫士已经启动了，可以输入 service xmirrord status 查看服务器卫士的服务状态；

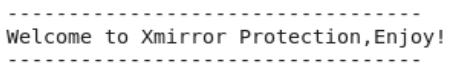

图 1-3-6 xmirrord 的安装提示（6）

如果您是在 CentOS（redhat）5.x x86/x64、CentOS（redhat） 6.x x86/x64 环境中可以输入以下命令对服务进行启动、停止以及卸载操作：

- 输入 service xmirrord start 启动服务
- 输入 service xmirrord restart 再次启动服务；
- 输入 service xmirrord stop 可以停止服务；
- 输入/usr/share/xmirror/scripts/uninstall.sh 可以卸载软件。

如果您是在 CentOS（redhat）7.x x64 环境中可以利用以下命令对服务进行启动、停止以及卸载操作：

- 输入 systemctl start xmirrord 启动服务
- 输入 systemctl restart xmirrord 再次启动服务；
- 输入 systenctl stop xmirrord 可以停止服务；

- 输入/usr/share/xmirror/scripts/uninstall.sh 可以卸载软件。

悬镜服务器卫士管理端（Windows 端）的安装，将 XmirrorManager3.0.0.2753.exe 放到操作系统的自定义目录下，点击安装。根据相应提示进行安装，具体操作参见以下步骤。

1.点击安装文件后，软件安装首界面

图 1-3-7 管理端安装首界面

2.点击“自定义”会出现自定义界面，如下图：

图 1-3-8 管理端安装详细界面

3.用户可以根据需求选择，完成选择后，点击安装，会进入到安装进度界面，界面中会显示安装的进度：

图 1-3-9 管理端安装进度界面

4.安装结束之后，显示立即体验界面，点击立即体验，界面会转到登录界面，证明安装成功，可以开始使用，立即体验界面如下图：

图 1-3-10 管理端立即体验界面

2. Windows 端操作模式

2.1 简介

悬镜服务器卫士的代理端，它的作用相当于是一个后台程序，来供管理端请求连接、请求通信并与管理端通信。主要的功能性操作集中在管理端，下面对这些特定功能项进行逐一介绍。

2.2 管理端登录

在软件安装完成后，会出现立即体验界面，点击立即体验界面中的“立即体验”按钮，管理端连接代理端的请求界面被唤出。

在管理端中有两种连接代理端（服务器）的管控方式，方式一：批量服务器管理，简单的理解是“一管多”，即是一台管理端可以管理多个服务器（代理）端；方式二：单台服务器管理，即是一对一的管理，本管理端管理一个服务器端。

2.2.1 批量服务器管理

图 2-2-1 批量服务器管理登录请求界面

新用户可以在悬镜官网进行账户注册，通过审核后，利用新注册的账户在上图界面中进行登录，登录后的界面如下图：

图 2-2-2 批量服务器管理登录后首界面

界面中显示当前管理的服务器的安全状况，除了今日安全指数、今日服务器状态外还包括：今日拦截攻击、今日告警信息，可以下拉界面查看这些信息。

点击界面中的管理服务器，进入服务器管理界面：

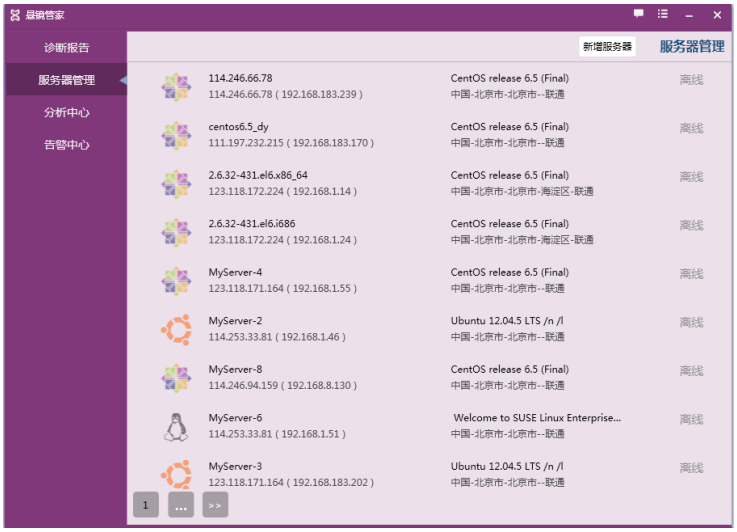

图 2-2-3 管理服务器界面

在管理服务器界面中以列表的方式显示连接过的服务器，点击某具体服务器，会出现远程管理按钮，点击远程管理按钮就会连接到服务器进入到管理服务器的相应界面：

图 2-2-4 连接代理端界面

图 2-2-5 连接代理端后界面

点击导航中的“服务器管理”按钮回到服务器管理界面。

点击服务器管理界面的新增服务器按钮，可以添加服务器进行连接：

图 2-2-6 添加服务器界面

在服务器管理界面中还存在分析中心界面与告警中心界面。界面如下：

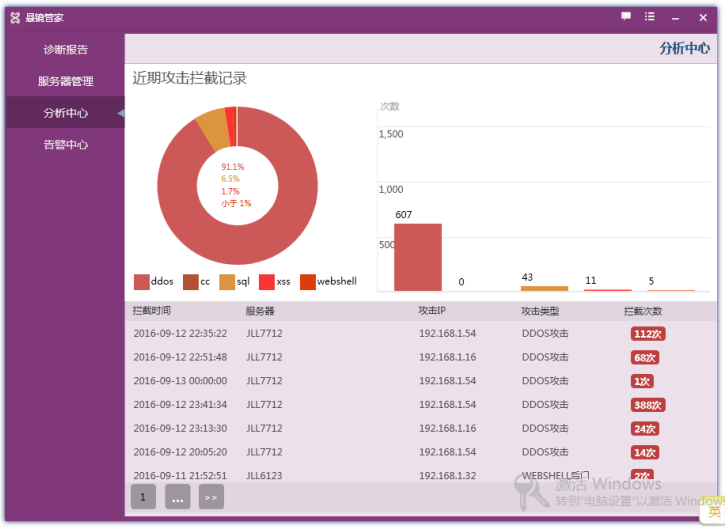

图 2-2-7 分析中心界面

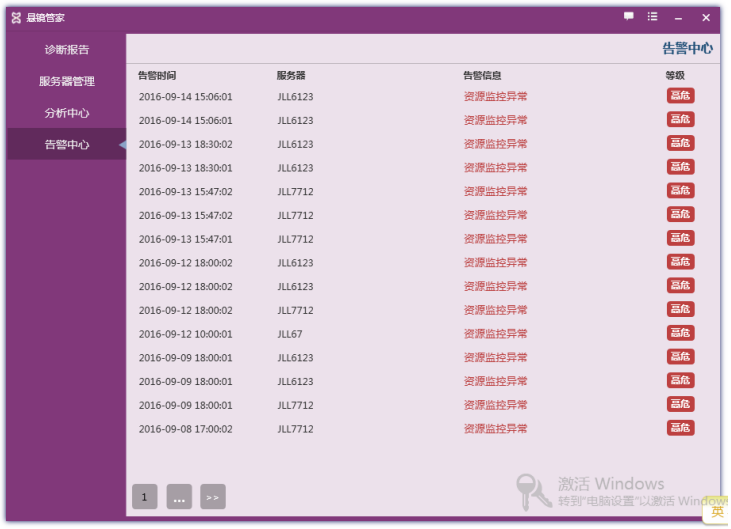

图 2-2-8 告警中心界面

2.2.2 单台服务器管理

输入需要包括代理端主机 IP、代理端系统用户名、代理端系统登录密码，在代理端启动的情况下用这三项就可以远程连接到代理端服务器，界面如下图：

图 2-2-9 单台服务器管理登录请求界面

图 2-2-10 管理端连接代理端登录界面

在确定了代理端服务器 IP、用户名、登录密码后，可以勾选记住密码，方便以后的登录管理。点击登录按钮后连接远程代理端服务器，之后进入系统。

下面介绍的内容中是批量服务器管理与单台服务器管理共有的功能：

2.3 安全巡检

1.初始登录后，界面中显示的是服务器体检界面，在未做任何操作时，界面显示如下图：

图 2-3-1 安全巡检界面

点击“立即检查”完成检查功能，检查结束后出现检查结果界面，在结果界面中将不安全项列出来，您可根据提示做出相应的处理，也会列出检查过的项，同时软件还会对总体的体检结果给出一个评分，可以帮助您更好的管理系统的安全性。

2.巡检的结果界面中，如果存在危项会建议您进行处理，体检结果界面如下图：

图 2-3-2 巡检结果界面

2.4 主机防护

典型服务防护采用虚拟化技术，在现有 Linux 操作系统空间中根据不同的用户应用分别创建出多个虚拟空间，实现用户与用户之间的隔离，服务与服务之间的隔离，该虚拟空间被称作“安全域”，每个安全域均具备增强型 RBAC、TE、BLP 安全机制。这些被保护的系统典型服务具有各自对应的安全域，实现用户与系统之间的隔离。对于原有应用或服务来说都是完全透明的，这也意味着对于原有应用的业务不会有丝毫改变。

具体来说，设置服务防护后本系统可对受保护的相关服务的端口监听、端口外联、文件读写、用户目录访问等操作进行主动安全域隔离，全面提升系统服务的完整性和安全性。

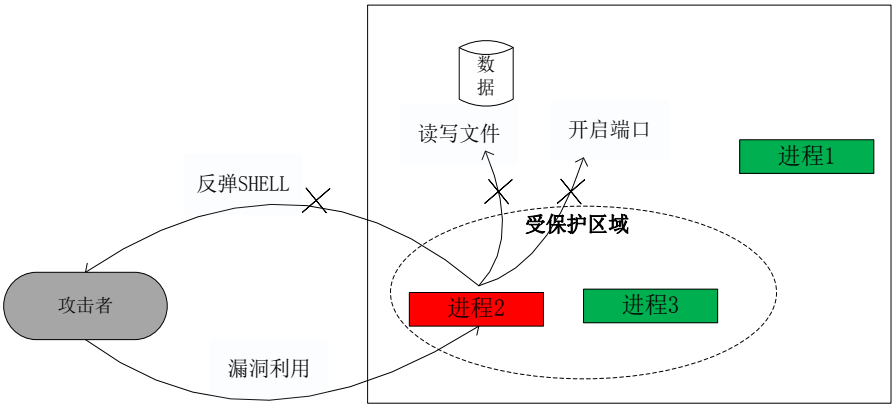

图 2-4-1 典型服务防护原理图

如上图所示，当前系统内运行着三个常用进程，分别是进程 1、进程 2 和进程 3。若进

程 2 具备读写系统任意文件，开启任意端口和外联任意端口等特权（具备针对系统进行危险操作的权限），当进程 2 存在的安全漏洞被利用时，则入侵者可将进程 2 作为跳板通过端口反弹进一步控制系统（例如借助 webshell 等），拿到系统控制权或者该进程 2 的特权后，非法读取或篡改系统上的重要文件或系统配置数据，在非授权情况下对系统监听端口进行变更等。典型服务防护模块正是基于此类场景的攻击的防护，可有效缓解此类安全威胁带来的风险。

下图界面中显示了 Apache、Samba、MySQL、SSHD、FTPD、SNMP 服务包括在服务防护功能中，对于在代理端开启了的服务默认状态下为“防护中”，未开启的服务则处于“服务未启动”状态，对于开启的服务可以点击图标关闭防护，再次点击图标可以开启保护，同时，您也可以点击“全部防护”便捷式的一键开启保护，对于关闭状态的服务即使一键开启所有防护，状态显示还是“服务未启动”，服务防护功能只是对开启了的服务起到作用，所以如果您想使用该部分功能，请确保服务器端这些服务处于开启状态：

图 2-4-2 主机防护界面

2.5 应用防护

应用防护中主要包括 SQL 注入防护、XSS 注入防护、CC 攻击防护、网马主动拦截四个功能模块，SQL 注入防护以及 XSS 注入防护中添加了详细的规则防护，您可以根据自己网站的需求对这些规则进行开启或者关闭设置，同时为了方便您的使用，软件也设计了一套默认的

规则，只需要点击“使用默认”按钮即可设置成功。下面将会针对这四个功能分别进行介绍。

2.5.1 SQL 注入防护

SQL 注入防护界面如下图所示：

图 2-5-1 SQL 注入防护界面

SQL 注入防护中进行了细致的分类，每条规则中包括五个开关项，分别是：Get、Post、Cookie、Headers、Xml,您可以根据自身 Web 服务器的实际需求对这些操作进行设置。

对于 SQL 注入防护以及 XSS 注入防护中的规则项,其中 Get 防护项的含义是对 Get 类型请求中的所有的键值对的键和值以及去除域名的 URI 进行检测，检测到不合法的项进行拦截；Post 防护项的含义是对 Post 类型请求的所有键值对的键与值（除文件外）以及文件上传时的文件名进行检测，检测到不合法项进行拦截；Cookie 防护项是对所有 Cookie 键值对的键和值（除_utm、_pk_ref 外）的 URI 进行检测，检测到不合格项进行拦截；Header 防护项是对请求 Header 里的 X-Forwarder-For、User-Agent 和 Referer 字段的值进行检测，检测到不合法项进行拦截。

对于 SQL 注入防护中具体的规则设置,您可以根据自身网站的实际需求进行开启与关闭操作，这一功能操作相对简单快捷，为了方便您的操作系统中有一套默认的规则设置，只需要点击界面中“使用默认”即可设置成功。

2.5.2 XSS 注入防护

XSS 防护具体界面如下图：

图 2-5-2 XSS 注入防护界面

XSS 注入防护中也进行了细致的分类，每一条规则中包括五个开关分别为 Get、Post、Cookie、Headers、Xml。

XSS 注入防护操作类似于 SQL 注入防护，这里不再赘述！

2.5.3 CC 攻击防护

CC 攻击的目的是消耗服务器资源，使服务器不能正常对外提供服务，需要单个或者多个 IP，攻击的方式主要分为快 CC 攻击与慢 CC 攻击两种。

悬镜 CC 攻击防护分为基础防护、中级防护、高级防护。基本原理是限制在一段时间内每个 IP 的 HTTP 请求数量，全服务器端实现，基本无法绕过。基础防护测试时不要使用浏览器，因浏览器需要手动，时间会比工具测试长，会有服务器缓存影响，导致测试结果不准确（CC 防护不会对服务器缓存进行防护和干涉），而应使用工具测试，比如 webbench，分析工具生成的报告，同时在测试阶段，为了保证准确性，工具测试时，尽量减少浏览器的访问，以减少干扰 。对于并行连接的测试，最好也使用工具测试，webbench 可行，但如果需测试的并行数较大时，可能无法控制并行发包的数量，需注意的是，此处的并行数是指一个 ip、同一时间点正在服务器被处理的请求数 中级防护是在基础防护的基础之上加入真实用户识别算法，即以每个 IP 首次（服务器无此 IP 记录）访问时，返回浏览器可解析的 JS 加密脚本，浏览器解析 JS 并解密后将使用相关解密信息再次请求服务器完成验证。高级防护在基

础防护的基础上，加入真实用户识别算法，即以每个 IP 首次（服务器无此 IP 记录）访问时，返回图形验证码，用户肉眼识别图形验证码，并将识别出来的验证码发送到服务器完成验证。

下图为 CC 攻击防护界面：

图 2-5-3 CC 攻击防护界面

上下拖动设置条以调节防护的等级。

2.5.4 网马主动拦截

网马主动拦截功能是对 WebShell 的主动检测与拦截，界面如下图所示：

图 2-5-4 网马主动拦截界面

2.6 网络防护

防火墙中分为网络防火墙、端口管控、黑白名单。在网络防火墙中包括了网络层攻击防护：DDos 攻击防护；局域网连接防护：Ping 命令防护、外网连接防护、SSH 防护。这里您可以使用的权限是开关这些防护以及定义这些防护规则。以下详细介绍防火墙的使用方式。

2.6.1 网络防火墙

网络防火墙界面如下图所示：

图 2-6-1 网络防火墙界面

✧ 网络层的攻击防护：DDos 攻击防护，点击开关，弹出规则设置框，它的项主要是单 IP 最大同时访问数限制、SYN 包每秒最大限制访问数、超限检测前 SYN 包允许个数、SYN 超过限制时最大容忍次数、ICMP 包超限次数、ICMP 每秒最大限制访问数。通过对这些项的设定完成 DDos 防御规则的设定，这些项的值都是用户根据系统的特性来设定的，软件本身也会有默认值，设定结束后，点击开启防御就完成了 DDos 防御的设定与启动了。

图 2-6-2 DDos 攻击防护规则界面

对于局域网连接防护，例如 Ping 命令保护、外网连接防护、SSH 防护，操作比较简单，只要点击开启或是关闭即可。

关闭/开启是软件一键开启这些功能的按钮，这时候 DDos 就是默认的值。您可以根据系统的需求进行这些操作。

2.6.2 端口管控

端口管控，开启该功能时会将正在使用的端口添加到白名单中，全局则是黑名单，在黑名单中的端口将会被拦截、屏蔽。

1.端口管控界面中，显示正在使用的端口、协议、占用进程、进程 ID、运行用户、状态及操作。

图 2-6-3 端口管控界面

2.在端口管控功能开启的状态下，点击“添加到白名单”后，状态变化如下：

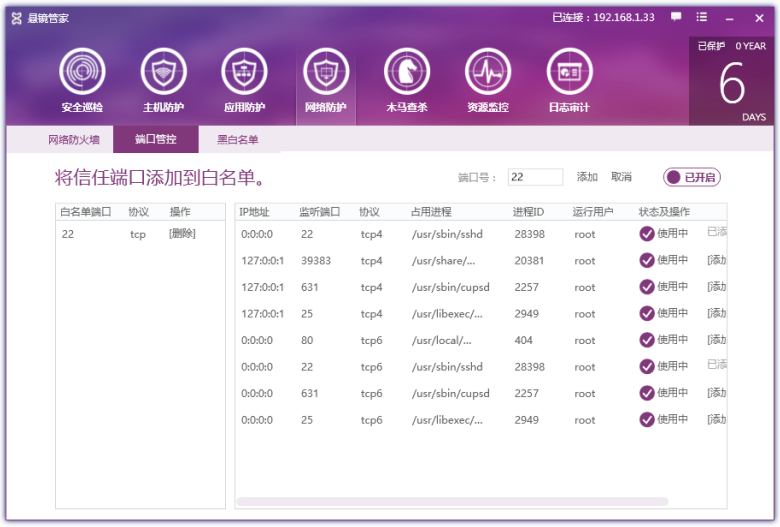

图 2-6-4 端口“22”添加到白名单后状态

3.点击“手动添加”按钮，弹出输入框，添加端口后，点击“添加”，操作成功；点击“取消”，操作会取消：

图 2-6-5 点击“手动添加”后界面

对于以上的操作，添加到白名单中的端口会在左侧的白名单列表中显示，点击“删除”可以将列表中已有的规则删除。

2.6.3 黑白名单

黑白名单，可以添加新的规则操作如下：

图 2-6-6 黑白名单界面

添加一条规则进入白名单界面，显示如下：

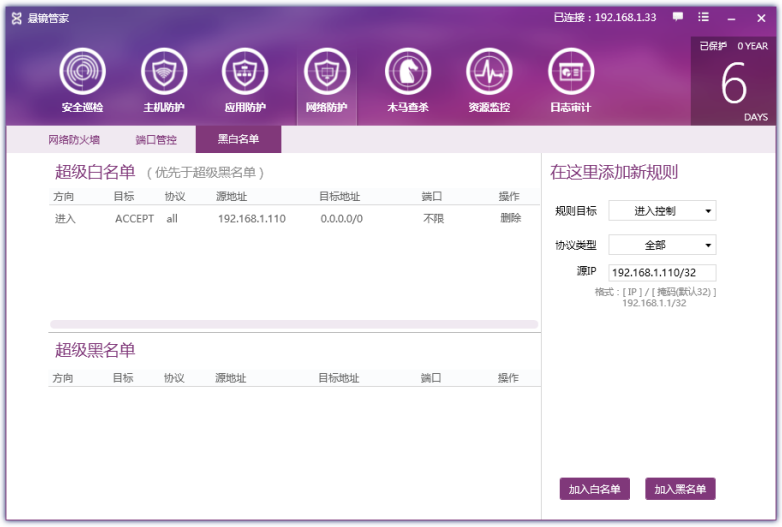

图 2-6-7 添加一条规则进入白名单

2.7 木马查杀

木马查杀功能主要是对网站 WebShell 的检测，WebShell 检测主要分为快速扫描和自定义扫描，同时还有恢复区与信任区。快速扫描是对系统中的 Web 文件进行检测扫描，快速扫描的路径是由 Linux 系统中 Web 服务器配置的网站路径决定的；自定义扫描的含义是用户可以自主选择哪些文件及目录要被检测。

恢复区主要是为了防止您的误操作，例如：您可能会将一些重要文件当做是威胁文件而

误清理掉，从而影响到系统的正常使用，所以在您点击了清理操作后，系统并未将威胁文件直接删除，而是将其放入恢复区中，您可以将因为误操作而清理掉的文件从恢复区中“找回”，并且被清理到恢复区的文件已经不能对系统产生威胁；

信任区是用户添加的可以信任的文件区域，当系统进行 WebShell 扫描之后，会存在一部分可疑文件，这些文件中可能存在一些敏感威胁信息，所以会被认定为威胁文件，但是您可以肯定这一类文件对系统并没有任何威胁，对于这类文件您可以将其添加到信任区，并且信任区内的文件再次扫描时不会被扫描到。用户可以根据不同的选择进行有针对的操作。扫描结束后界面中会显示扫描的结果：WebShell 的个数、可疑文件个数以及威胁文件等，可以查看威胁文件的详细信息以及建议的处理方式，也可以点击一键修复。下面将通过图文结合的方式来详细演示 Webshell 的具体操作。

1. 点击导航条的“木马查杀”，界面如下

图 2-7-1 木马查杀界面

2. 点击“快速扫描”，进入到快速扫描界面，会出现下图扫描状态：

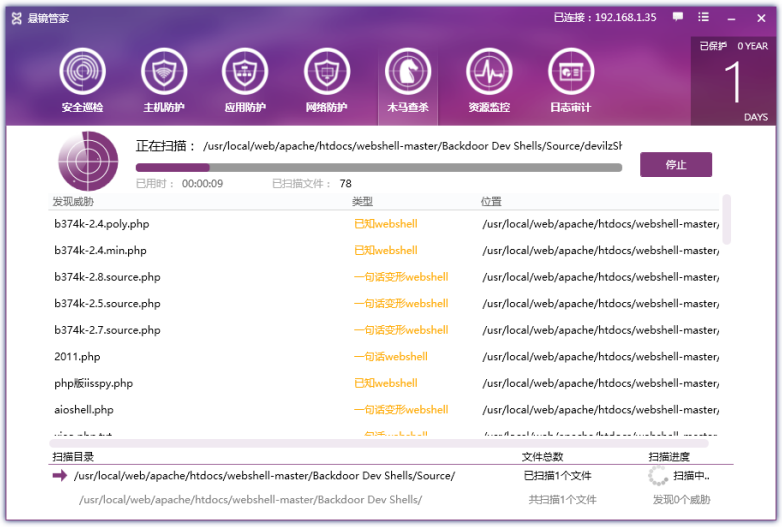

图 2-7-2 快速扫描过程界面

3. 扫描结束，如果扫描出可疑文件或者 WebShell 文件，会出现如下图界面：

图 2-7-3 快速扫描结果界面

4. 对扫描结果进行处理后，系统会将扫描的结果直观地反映出来，扫描的方式、扫描用时、扫描结果，处理后的安全文件分布用柱状图显示出安全文件分布。

图 2-7-4 快速扫描处理后结果界面

5. 点击自定义扫描之后，会出现选择目录，用户可根据需要选择扫描的文件

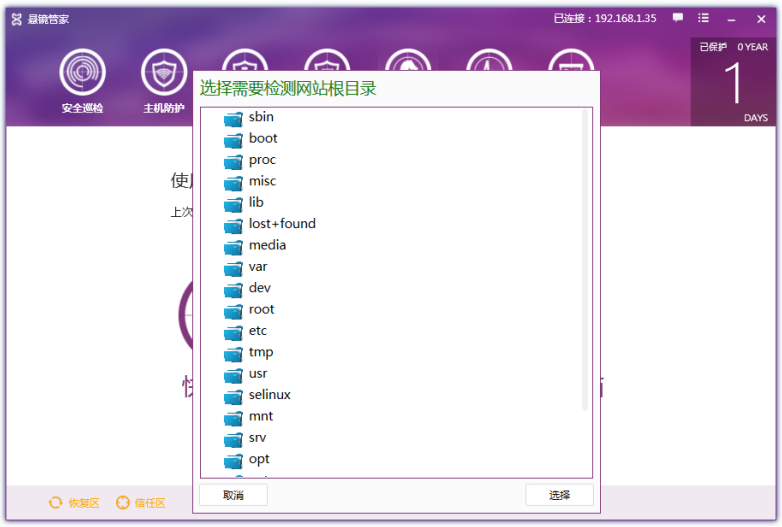

图 2-7-5 自定义扫描界面

6. 点击选择按钮，系统进入自定义扫描界面，对选择过的目录进行检测：

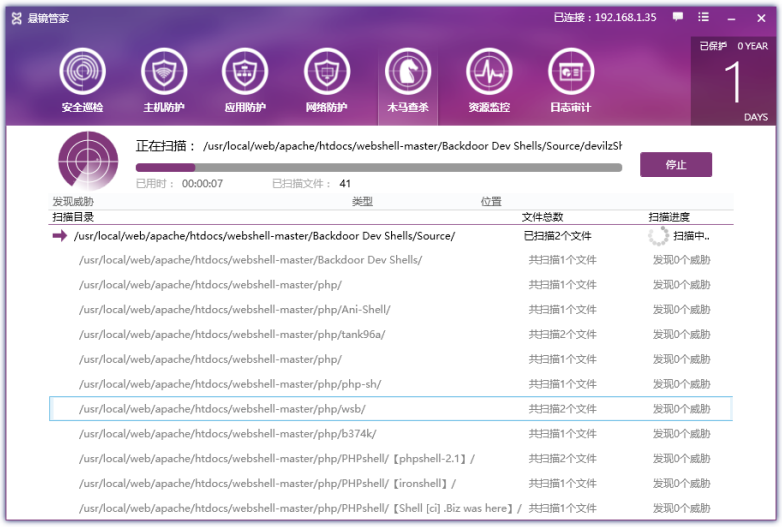

图 2-7-6 自定义扫描进行界面

7. 扫描结束后，显示扫描结果界面，会列出可疑文件，您也可以查看详细信息，系统会给您一定的操作建议，供您选择，具体信息如下图：

图 2-7-7 自定义扫描结果界面

8. 对于 WebShell 中的“恢复区”、“信任区”，“恢复区”中的文件是这样一类文件：上一步扫描出的威胁文件，可能是 WebShell 文件或者可疑文件，对扫描结果进行一键修复或者清理操作后，这些威胁文件会被放入恢复区中。恢复区设计的主要的目的是为了避免您之前的误操作，如果您不小心清理了重要的文件，可以在这里进行恢复，点击“恢复区”会出现以下界面：

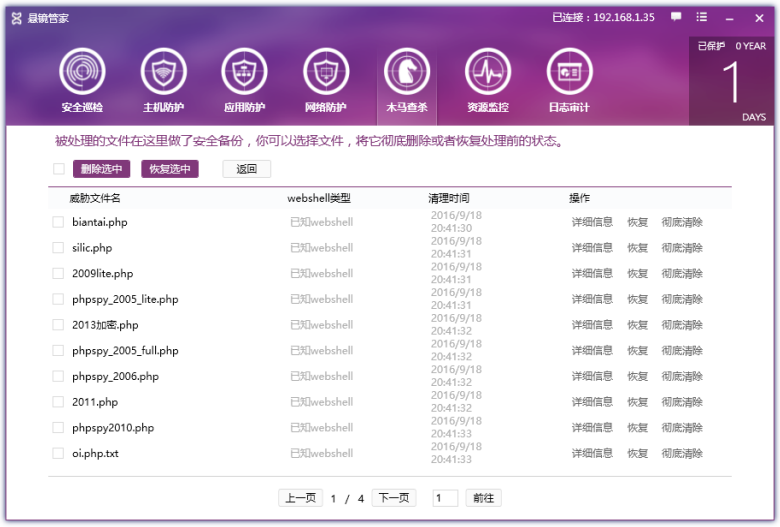

图 2-7-8 恢复区界面

在界面中会出现以往处理过的文件名、清理时间、操作，可以选择文件进行恢复。

9.“信任区”：信任区界面如下， 被添加到信任区中的文件不会再被当成威胁文件扫描，并且您也可以选择取消信任。

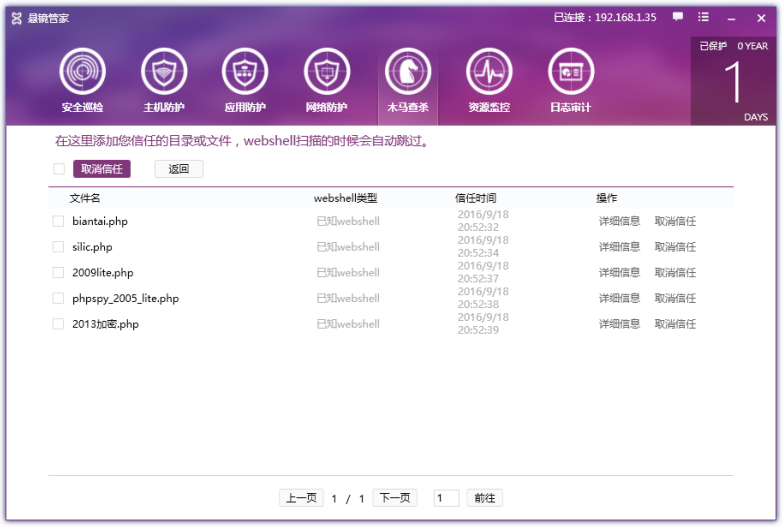

图 2-7-9 信任区界面

2.8 资源监控

资源监控功能实现了客户端远程对代理端的 CPU 使用率、内存使用率、磁盘使用率、流量等的监视，并且可以对监控参数进行设置，通过对 CPU 使用率、内存使用率、磁盘使用率、流量的上限和超过上限以及定时时间等参数的设置，实现对代理端的监控，会将监控

的结果记录到防护日志中的监控日志中。如果代理端在每个定时时间时超过了设置的参数限制，会记录并保存到日志。

图 2-8-1 资源监控界面

2.8.1 CPU 监控

CPU 监控：对 CPU 使用率定时监控，您可以设定时间、使用上限，在设定的时间段里不超过使用上限，为合法的。您可根据系统情况进行设定。也可以使用默认值，使用默认值时，点击开关就可以，自己设定点击应用，也能完成。

图 2-8-2 CPU 监控界面

2.8.2 内存监控

内存监控：对内存使用率定时监控，您也可以设定时间、使用上限，在设定的时间段里不超过使用上限，为合法的。您可根据系统情况进行设定。也可以使用默认值，使用默认值时，点击开关就可以，自己设定点击应用，也能完成。

图 2-8-3 内存监控界面

2.8.3 磁盘监控

磁盘监控与 CPU、内存设置类似。

图 2-8-4 磁盘监控界面

2.8.4 流量监控

流量监控：网络流量监控中除了对时间的设定外，还有上行下行流量的设定，操作也类似 CPU、内存设置。

图 2-8-5 流量监控界面

2.9 日志审计

日志审计功能中包括了操作日志、监控日志、网络防护日志、应用防护日志四类日志。

2.9.1 操作日志

操作日志中主要记录的是用户的操作行为，主要包括：近期日志、连接代理端、体检日志、网络防火墙日志、资源监控日志、应用防护日志。每一条日志由时间、IP、功能模块、描述、执行结果这些项组成。

图 2-9-1 操作日志详细日志界面

图形日志包括分布图与走势图，分布图中包括近期历史操作记录分布环状图与操作次数柱状图：

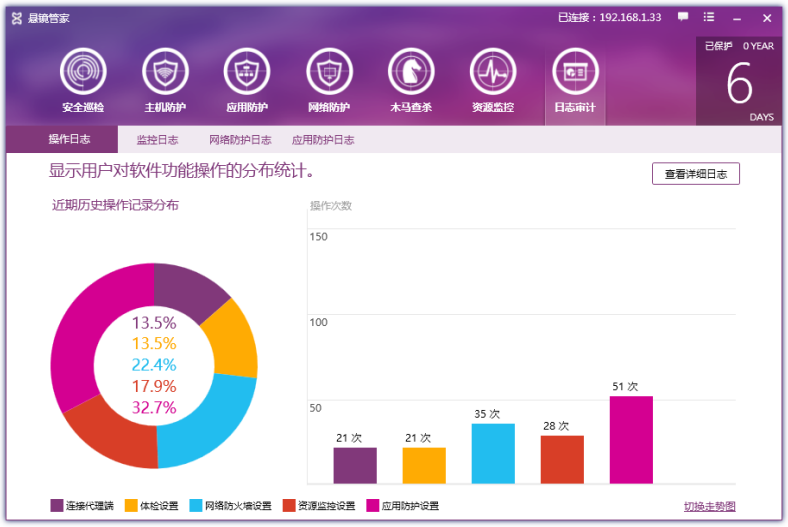

图 2-9-2 操作日志分布图图形界面

点击右下角的切换走势图切换到折线图界面。折线图中分别存在以天为单位和以小时为单位的记录，点击“今日功能操作记录”切换到今日功能操作记录，页面出现“今日”操作的记录；点击“近期历史操作记录”切换到近期历史操作记录，页面中出现的是一周内的数据的信息，您还可以设置图形日志中显示的项目，具体如下图：

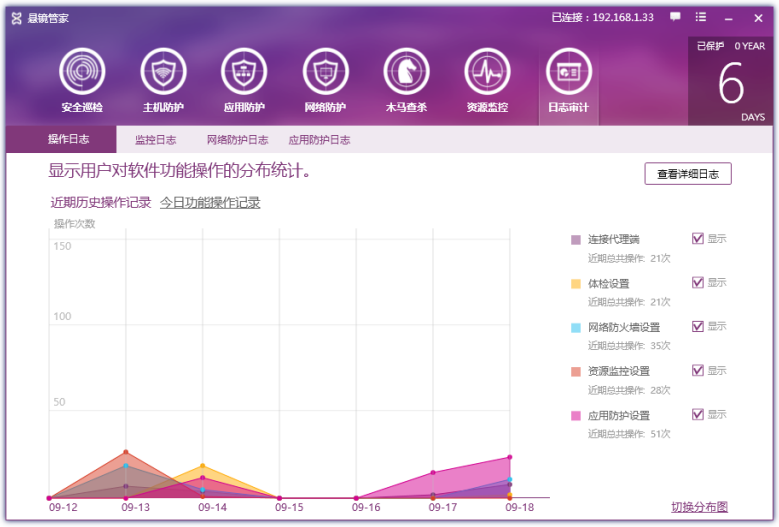

图 2-9-3 操作日志走势图图形界面

2.9.2 监控日志

监控日志中主要记录的是 CPU 监控、内存监控、硬盘监控、流量监控，每一条日志包含的项是时间、监控类型、警告信息。

图 2-9-4 监控日志图形界面

图形日志包括分布图与走势图，分布图中包括近期资源监控告警分布环状图与告警次数柱状图：

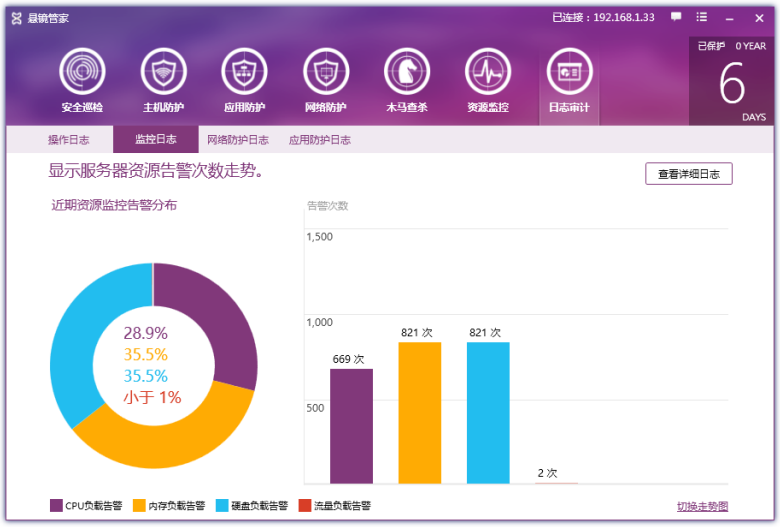

图 2-9-5 监控日志分布图图形界面

点击右下角的切换走势图切换到折线图界面。折线图中分别存在以天为单位和以小时为单位的记录，点击“今日资源监控告警”切换到今日资源监控告警，页面出现“今日”资源监控的告警记录；点击“近期资源监控告警”切换到近期资源监控告警记录，页面中出现的是一周内的数据的信息，您还可以设置图形日志中显示的项目，具体如下图：

图 2-9-6 监控日志走势图图形界面

2.9.3 网络防护日志

网络防护日志中记录软件的防护记录，主要的项是 DDos 防护日志、被动 PING 阻断日志、自身上网阻断日志、被动 SSH 连接阻断、端口管控日志，应用层防护日志，每一条日

志包含的项是时间、功能、主机名、ID、协议、源地址、目的地址、MAC 地址。

图 2-9-7 防护日志图形界面

图形日志包括分布图与走势图，分布图中包括近期历史攻击记录分布环状图与拦截次数柱状图：

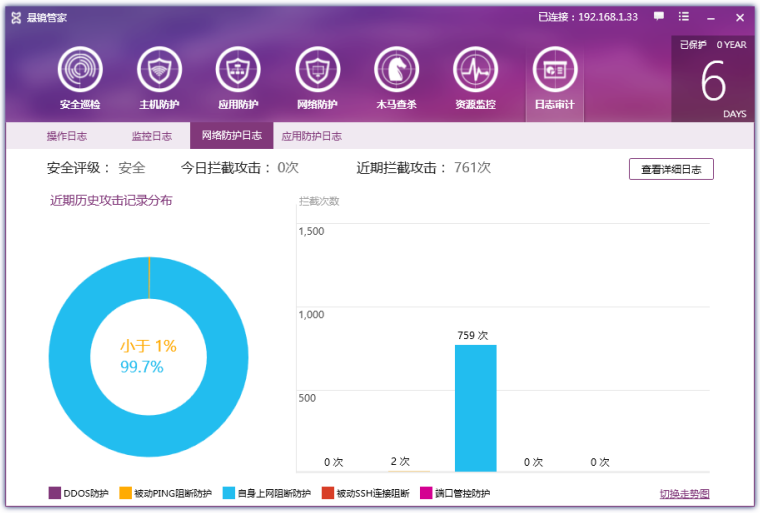

图 2-9-8 防护日志分布图图形界面

点击右下角的切换走势图切换到折线图界面。折线图中分别存在以天为单位和以小时为单位的记录，点击“近日拦截攻击记录”切换到今日拦截攻击记录，页面出现“今日”拦截的攻击记录；点击“近期历史攻击记录”切换到近期历史攻击记录，页面中出现的是一周内的数据的信息，您还可以设置图形日志中显示的项目，具体如下图：

图 2-9-9 防护日志走势图图形界面

2.9.4 应用防护日志

应用防护日志中记录软件的应用防护记录，主要的项是 CC 攻击防护日志、SQL 注入防护日志、XSS 注入防护日志、WebShell 防护日志，每一条日志包含的项是时间、攻击 IP、描述、操作。

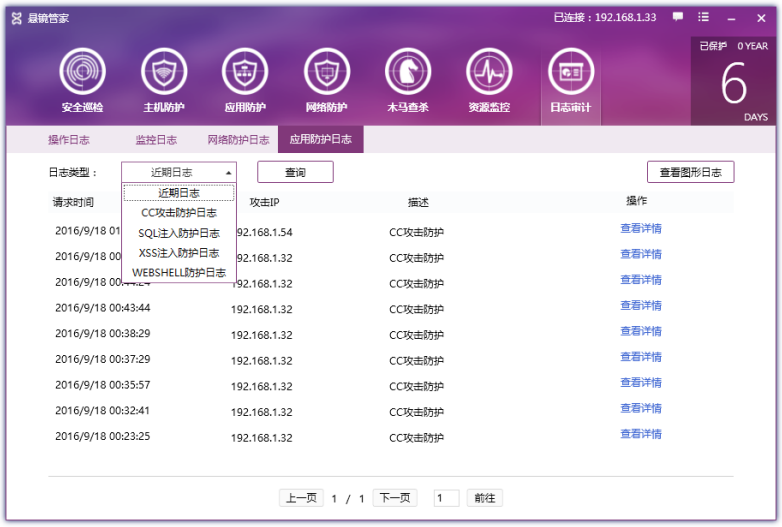

图 2-9-10 应用防护日志详细界面

图 2-9-11 应用防护日志分布图界面

图 2-9-12 应用防护日志走势图界面

2.10 安全设置

安全设置功能开启后通过添加相应的客户端的名片，只有符合安全名片规则的客户端才能连接代理端。需要设置的项主要包括：主机名、用户名、主机 IP、磁盘序列号。

图 2-10-1 安全设置界面

填好本地主机信息后点击“添加新名片”，如下图：

图 2-10-2 安全设置界面

界面中会显示该张名片的状态“使用中”，您也可以点击“禁用”，禁用该设置，也可以点击“删除”，删除名片，也可以设置多个。

2.11 产品更新

悬镜管家更新功能主要是用来实现软件版本更新控制，当管理端登录连接代理端时，如果代理端或者管理端存在高版本，在初始登录时软件会检测版本更新并且提示用户进行版本更新，具体代理端的更新提示如下：

图 2-11-1 代理端版本更新提示界面

更新按钮：界面中左上角菜单栏中的向上箭头图标主要是用于检测是否存在新的版本，在版本显示信息右侧会提示检测结果，如果不存在新版本，提示信息是：服务端已为最新版本。如果存在新的版本则会弹出提示框让用户选择是否进行更新。

更新界面：当登录时如果存在更新版本，界面会自主唤出，提示用户有新版本存在，可以选择是否进行更新操作；如果已经进行过登录，可以点击更新按钮进行检测更新，如果存在新版本，更新界面也会被唤出，如果不存在新版本会提示已经为最新版本。

更新检测：登陆之后系统进行检测版本更新，先检测代理端更新，再检测管理端更新，这里需要说明的是代理端与管理端在更新时会主动断开连接，用户可以根据具体需要选择更新。

图 2-11-2 管理端版本更新提示界面

3. Web 端操作模式

3.1 前期准备

本着以数据驱动为核心，软件防御为主体的安普诺云诺安全管控云平台，以下章节中将会详细介绍运用到的技术以及核心功能。

3.1.1 用户账号登录/注册

新用户可以登录网址 http://www.xmirror.cn/，进行注册：

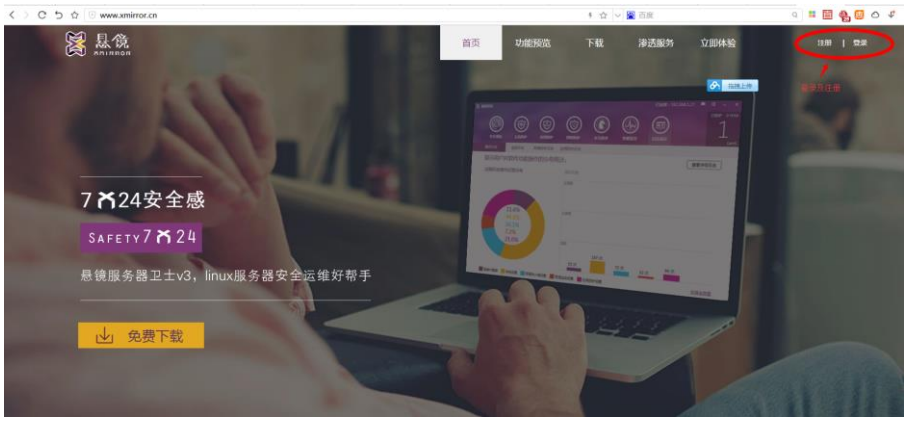

图 3-1-1 用户登录/注册界面

点击注册进入到注册界面，这里需要值得注意的是填写邮箱必须保证正确有效，因为在填写表单提交后，云诺安全管控云平台会向邮箱发送链接以激活用户账户：

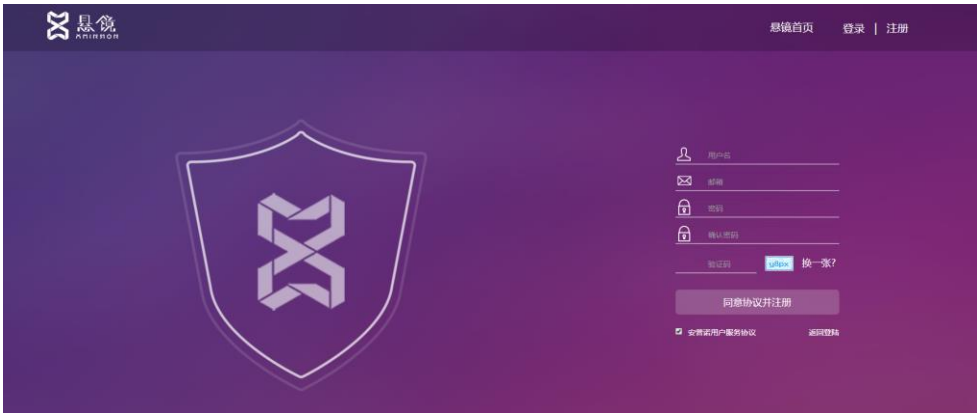

图 3-1-2 新用户注册界面

如果填写无误邮箱正确，后台会向该邮箱发送一个链接，点击链接激活链接后，账户既可以使用。

回到之前登陆/注册界面，用刚注册的账户登录即可。

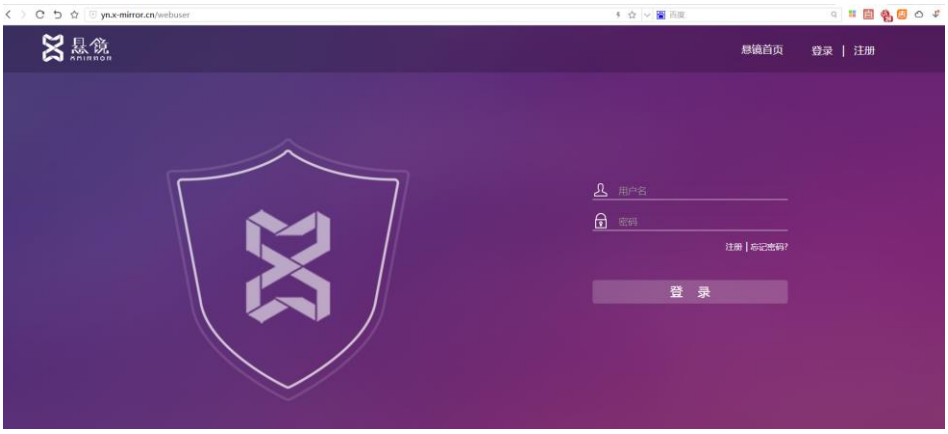

图 3-1-3 用户登录界面

3.1.2 新用户登录后界面

如果只是简单地注册账户后登录云诺：

图 3-1-4 新用户登录后界面

由于是初次登录系统，并且还未连接服务器，界面中会提示如下信息：

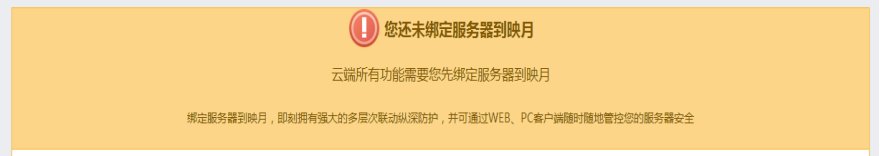

图 3-1-5 新用户登录后界面提示

第一步 下载安装悬镜代理端

根据服务器版本以及类型进行选择安装后端版本：

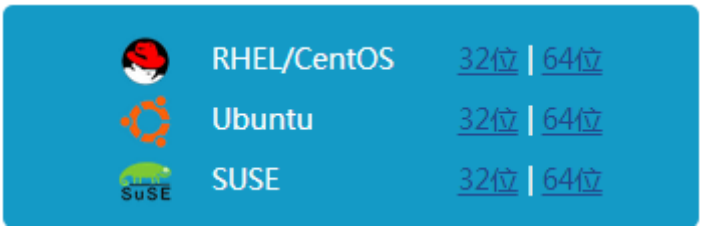

图 3-1-6 代理端版本下载

在 Root 账户下执行以下命令：（以 RedHat_x86 版本为例）

```
tar zxvf Xmirror3.0.1.2927_rhel_x86.tar.gz
chmod +x Xmirror3.0.1.2927_rhel_x86.bin
./Xmirror3.0.1.2927_rhel_x86.bin
```

第二步 下载安装悬镜管家 Windows 端

双击安装包，按照安装提示选择相应路径进行安装。完成后点击“立即体验”。

第三步 登录悬镜客户端

使用 Web 平台用户名、密码直接登录

图 3-1-7 Windows 端登录界面

第四步 连接代理端

输入要添加的服务器的 IP、用户名、密码，点击“确认添加”：

图 3-1-8 客户端中添加服务器

第五步 等待连接成功

连接成功后，返回“服务器管理”，发现已添加成功：

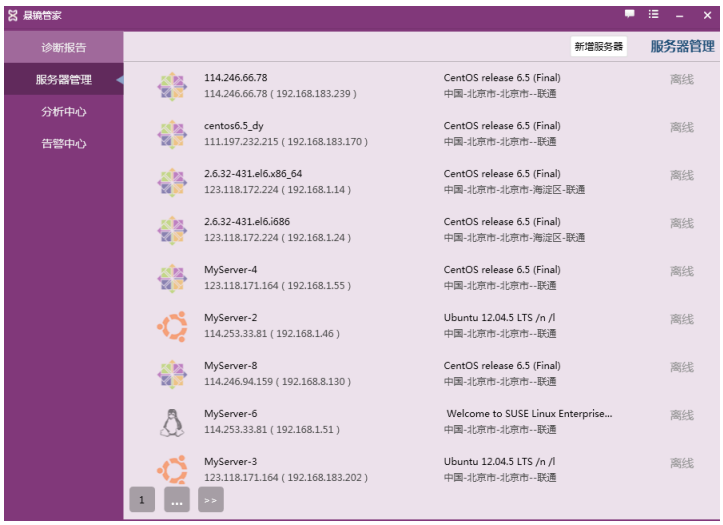

图 3-1-9 添加成功界面

第六步 查看 Web 平台服务器管理

客户端添加成功后，Web 平台自动同步添加

图 3-1-10 同步添加到 Web

3.2 操作说明

3.2.1 态势感知

如果已经将服务器添加到云诺安全管控云平台中，再登录时界面如下：

图 3-2-1 已有服务器加入平台的账号登陆后界面

在界面中首先显示的是态势感知，在态势感知中主要显示了在线服务器数以及离线服务器数，另外，会显示未受到安全威胁的服务器数、正在遭受攻击的服务器数、存在安全风险的服务器台数以及情况未知的台数。

除此之外还会显示今日服务器安全情况、今日攻击分布图、今日拦截攻击数以及今日告警信息。

3.2.2 服务器管理

在服务器管理中会以列表的形式显示该账户下的服务器数目：

图 3-2-2 服务器管理界面

点击任一服务器显示列的“查看主机”按钮进入到该服务器详情页：

图 3-2-3 服务器显示详情页

页面中会显示服务器的状态：是离线还是在线状态，基本系那是的信息包括：告警信息、拦截记录、安全检测、资源信息这些信息。

3.2.3 运维监控

在运维监控中显示可用性监控、CPU 监控、内存监控、硬盘监控、流量监控，界面如下：

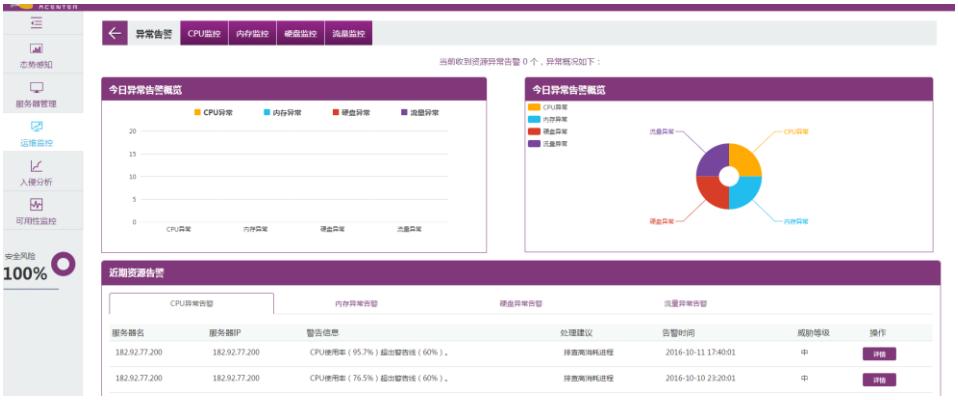

图 3-2-4 运维监控

3.2.4 入侵分析

在入侵分析中会将服务器所受到的攻击地域分布进行显示，同时也会将攻击事件以列表的方式呈现出来，包括：时间、服务器、服务器 IP、攻击 IP 信息、攻击类型、拦截次数、操作，界面如下：

图 3-2-5 入侵分析界面

点击攻击信息操作中的详情，会进入到攻击详情信息界面：

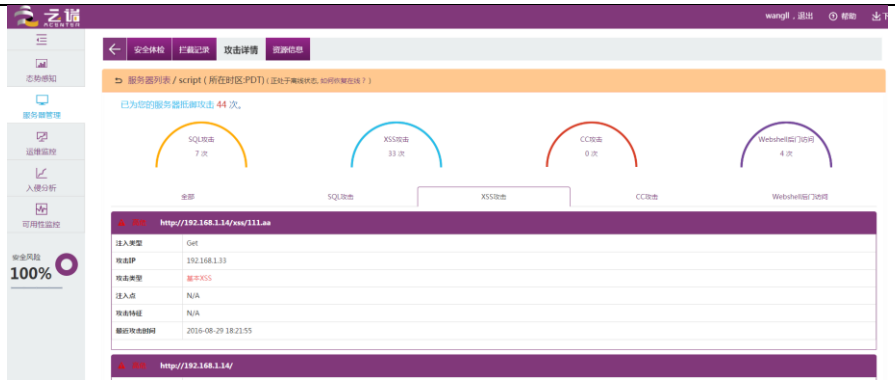

图 3-2-6 攻击详情信息界面

3.2.5 可用性监控

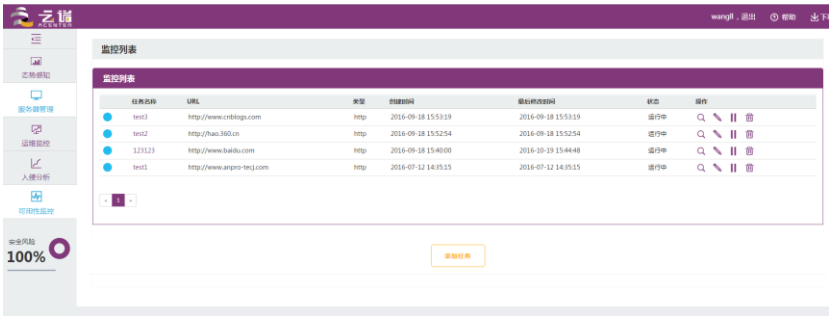

图 3-2-7 可用性监控界面

4. 专业版产品购买

当免费版无法满足您的要求时，您可以选择联系我们进行订购专业版或定制化开发。

4.1 商务流程

- 客户提出试用申请，通过审核后，双方签订保密协议，发出试用版本，并协助联调测试；
- 客户试用满意，双方达成合作意向，签订正式服务合同；
- 提供正式版本和客户 ID，并协助客户完成产品的集成和上线。

4.2 联系方式

张涛 [商务经理]
联系电话：18510237215
Mail: zhangtao@anpro-tech.com QQ：510691049
公司地址：北京市海淀区信息路科实大厦 B 座 06A2 室 邮编：100085