

# IP-guard 产品白皮书

广州溢信科技有限公司

## 目录

一 前言 .....	1
1、 内网安全面临的威胁 .....	1
2、 内网管理面临的挑战 .....	1
3、 IP-guard的简介 .....	1
二 IP-guard系统的架构 .....	2
1、 IP-guard的逻辑组成 .....	2
2、 IP-guard的架构 .....	3
三 IP-guard的功能模块 .....	4
1、 基本框架 .....	4
2、 文档操作管控 .....	5
3、 文档打印管控 .....	6
4、 设备管控 .....	7
5、 移动存储控制 .....	7
6、 邮件管控 .....	8
7、 即时通讯工具管控 .....	8
8、 应用程序管控 .....	9
9、 网页浏览管控 .....	10
10、 网络管控 .....	11
11、 流量管控 .....	11
12、 屏幕监控 .....	12
13、 远程维护 .....	13
14、 资产管理 .....	14
四 IP-guard的运行环境与性能指标 .....	16
五 IP-guard的安装和部署 .....	18
六 关于广州溢信科技有限公司 .....	19

---

# 一 前言

自从上个世纪 60 年代末，互联网诞生，网络技术和通信技术都进入了飞速发展的时代。互联网的发展改变了世界，企业的运作模式也发生了巨大的变化，从过去的单一经营变化为多元化的发展，从传统的独立产销变化为合作联通。随着世界信息化大潮流的发展，已经没有一个企业能从生产到销售完全脱离信息化，企业的所有业务和运作都已经离不开计算机和网络。然而，信息化是一把双刃剑，它为企业带来了便利，也为企业带来了威胁。

## 1、 内网安全面临的威胁

信息联通的便利必然会带来信息泄露的便利。对于企业来说，核心产品的设计、关键的客户资料和敏感的财务信息无疑是企业的核心竞争力，而这些数据都是以电子形式存在的，但是根据FBI 和CSI 调查显示，超过 85% 的安全威胁来自企业内部，也就是说，信息的泄露大部分是来自于内部员工有意或无意的过失。另外，竞争对手利用间谍软件对信息的窃取，恶意程序、计算机病毒对企业的冲击，造成关键信息被窃取或被篡改删除，这都时时刻刻都威胁着企业的安全。

## 2、 内网管理面临的挑战

信息化除了为企业带来有用的资讯以外，还充斥着大量的休闲信息、娱乐信息，乃至不良信息。企业的计算机数目，尤其是员工个人使用的计算机众多，管理难度非常大。病毒、木马通过员工的不良行为被非法下载或通过移动存储设备被带到企业内部；由于缺乏有效的技术管理手段，很多管理规定得不到实施，例如：有些员工会在上班时间浏览与工作无关的网站、看电影、玩游戏、私自改变计算机的设置、非法外联等，员工的工作时间、工作效率完全得不到保障。

信息化还会对企业的IT资产管理带来困难。企业里的计算机数目较多，分布较散，IT 管理人员对计算机的日常维护非常困难，这些困难包括：

- 不能统计查询所有计算机的软硬件信息
- 不能对每个计算机的系统漏洞及时打上补丁，让系统存在风险
- 计算机的小故障小问题都需要维护人员现场解决
- 无法对计算机进行软件的批量安装部署

## 3、 IP-guard 的简介

IP-guard被定义为一款内网安全管理软件，IP-guard的诞生就是为了帮助企业解决上述问题。IP-guard划分为14个功能模块，覆盖了内网安全管理的方方面面，它运用系统管理思想，充分利用行为审计，分级授权，访问控制和集中管理等技术手段，全面解决信息安全、应用效率、系统管理三项内网安全难题。

---

## 二 IP-guard 系统的架构

### 1、 IP-guard 的逻辑组成

IP-guard 是基于 C/S 架构设计的，系统由三个模块组成，客户端模块、服务器模块和控制台模块，用户可以根据管理的需要将它们安装在网络中的计算机上。通常客户端模块部署在受管控的计算机上，服务器模块部署在一个稳定安全的计算机上，控制台模块部署于管理人员的计算机上。

#### **客户端模块基本功能：**

- 执行系统设定的各种管理策略
- 采集客户端运行的各项数据
- 定时将采集的数据传送到服务器
- 根据控制台发出的指令进行监控操作

#### **服务器模块基本功能：**

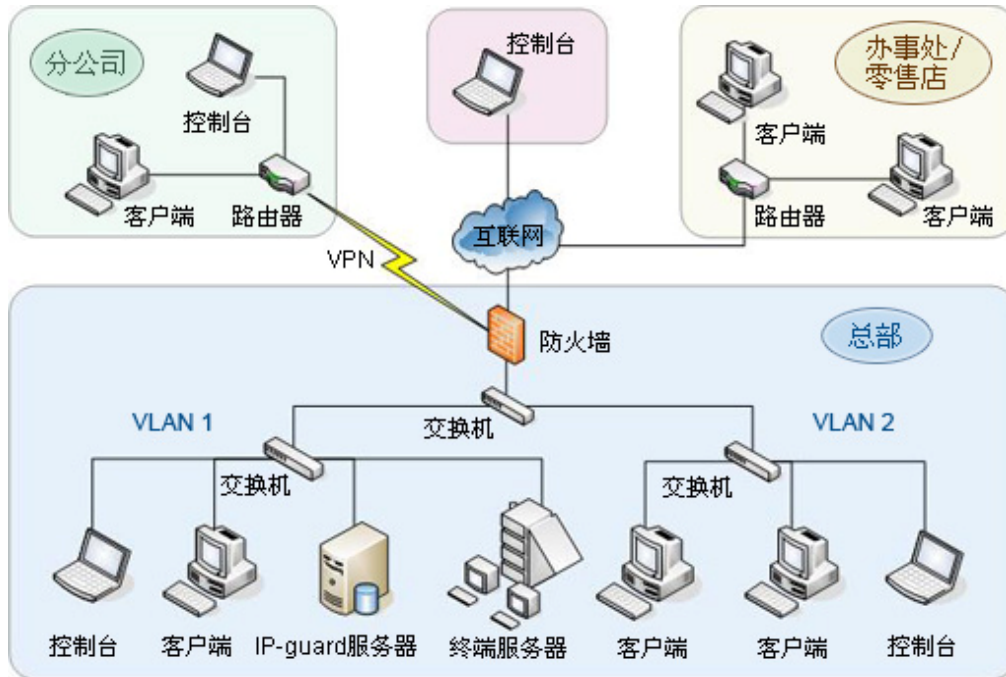
- 管理所有客户端计算机，并向其传递相关的规则和指令
- 收集客户端采集的数据并保存
- 提供方便灵活的记录管理、查看、归档、搜索等功能

#### **控制台模块基本功能：**

- 执行系统设定的各种管理策略
- 采集客户端运行的各项数据
- 定时将采集的数据传送到服务器
- 根据控制台发出的指令进行监控操作

## 2、 IP-guard 的架构

IP 的架构如下图所示：



架构图的简单说明：

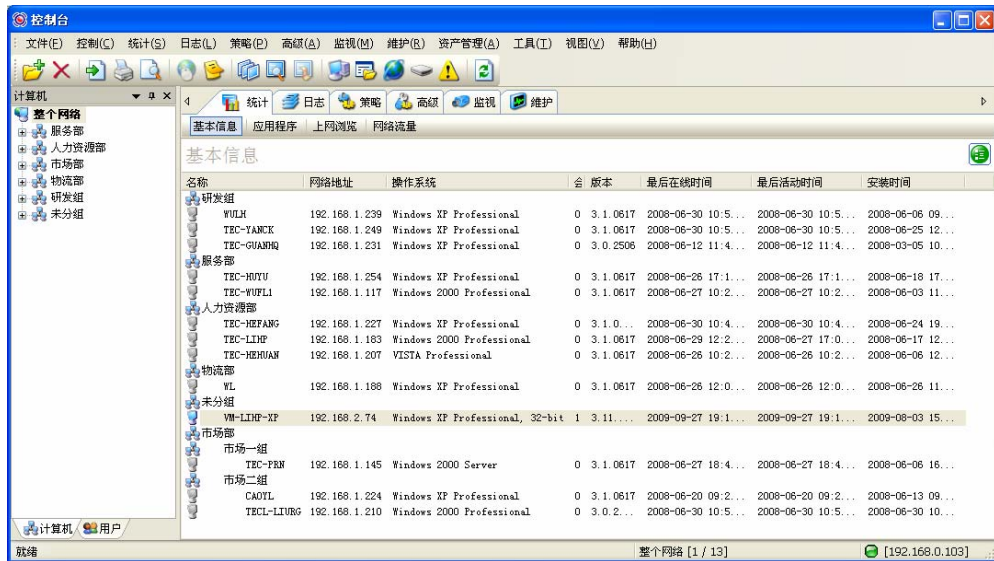
- IP-guard 是基于 TCP/IP 协议的网络架构。
- IP-guard 是通过服务器主动轮询与客户端主动连接服务器的双向连接方式。
- IP-guard 支持 Vlan 网络，支持多网段。
- IP-guard 支持通过虚拟专用网（VPN）接入的远程网络。
- IP-guard 支持通过互联网连接的异地网络。
- 控制台也可以通过互联网连接异地的服务器，实现在出差时也能对企业内部进行远程监控。

### 三 IP-guard 的功能模块

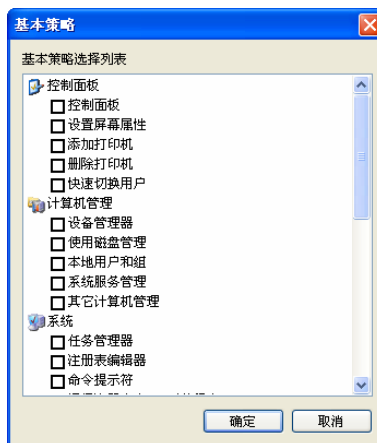
IP-guard 依据功能划分为基本框架和另外十三个功能模块。

#### 1、基本框架

IP-guard 的基本框架提供方便灵活的管理模式，让使用者使用简单、管理细致。



- IP-guard 除了支持对计算机模式的管理以外，还支持以用户模式的管理，因此 IP-guard 能支持终端服务器和瘦客户机的管理。
- 提供多管理员帐号的管理。可以设定管理范围和管理权限各不相同的管理员，帮助企业达到一个细致的管理。同时也能对每个管理员的操作做详细的审计。
- 获取每个计算机和用户的基本信息，记录计算机的启动、登录、注销、关闭等操作，还能通过远程对计算机进行注销、重启、关闭、锁定键盘鼠标等操作。
- 对计算机的基本设置（包括控制面板、系统设置、网络设置等）进行保护，让系统不会因为被随意修改而降低安全性。

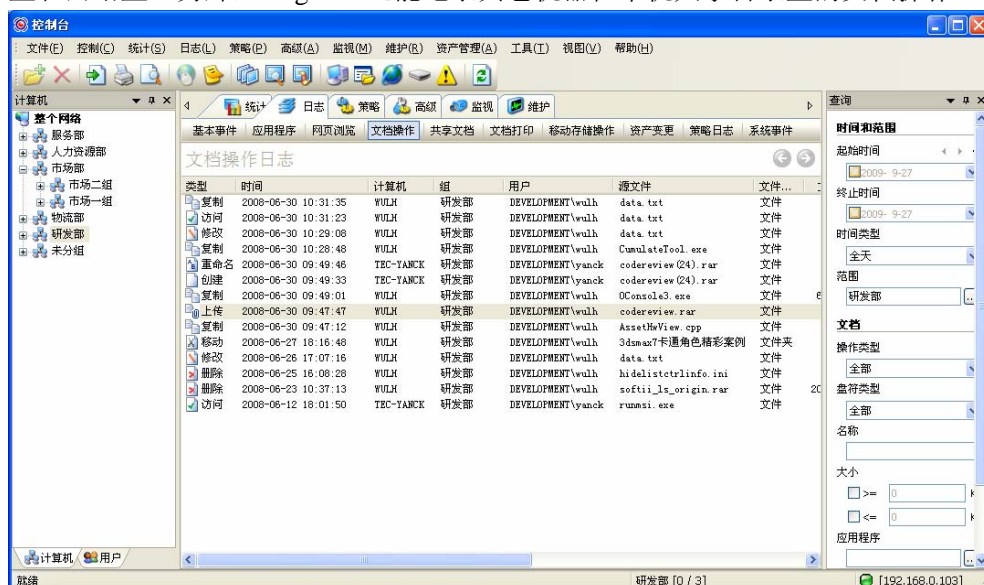


- 对于计算机系统的软硬件变化或计算机的属性变化如系统时间发生改变、服务发生改变、启动项发生变化等向控制台发出报警。
- 支持简体中文、繁体中文、英语、日文等多种语言操作界面。

## 2、 文档操作管控

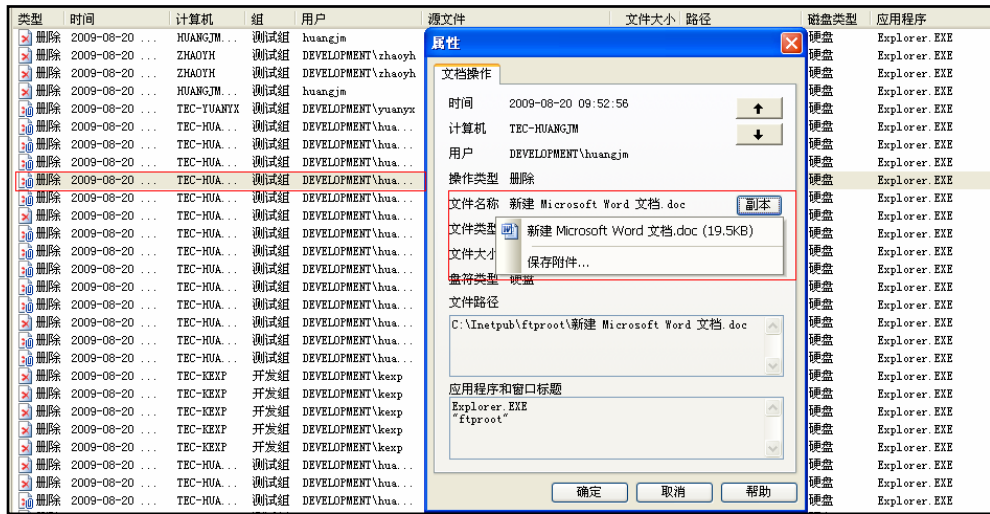
文档操作管控模块能管控计算机的文档使用，控制文档的访问权限，记录文档的使用日志。

- IP-guard 能记录每个员工在本机文档操作信息；文档日志记录的信息包括操作类型，操作时间，文档名称，文档路径，标题等。其中操作类型多种多样包括：创建、复制、移动、重命名、删除、恢复、访问、修改、上传、下载和刻录等。同时，IP-guard 记录的磁盘类型也是非常丰富的，包括：软盘、硬盘、光盘、可移动盘和网络盘。另外，IP-guard 还能记录其它机器在本机共享目录里的文档操作。



- IP-guard 能控制内网所有计算机对某些文档的读取/修改/删除权限；不同的计算机和不同的文档之间可以有不同的权限。

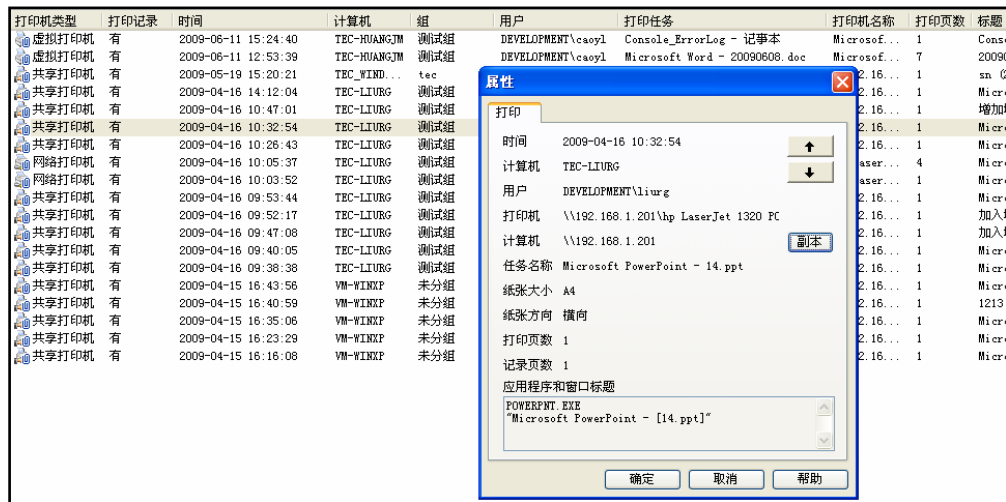
- 对于计算机里的一些比较敏感的文件，IP-guard 可以设定在其被移动、修改或被删除前把文件备份到服务器，保证重要的文件不会因为误操作或被恶意篡改、删除而丢失。



### 3、 文档打印管控

文档打印管控模块控制打印机的使用权限，记录打印机资源的使用状况。

- IP-guard 能记录使用者对打印机的使用情况，包含打印的时间、文档名称，打印的页数、打印机名称、执行打印任务的 PC 机器名以及登录用户名。



- IP-guard 能控制工作人员打印文档的权限，根据需要控制使用者在指定的打印机上打印，也可根据应用程序或指定的文档名称控制打印的操作。打印的控制可以区分本地打印机、共享打印机、网络打印机和虚拟打印机。
- IP-guard 能获取打印机的映像文件而，并记录下来备份到服务器上，而不是根据文档路径直接把要打印的文档做复制备份，保证保存的内容即是打印的内容。

## 4、 设备管控

IP-guard 能控制计算机使用外部设备的权限。在每一类的设备里，IP-guard 都能把设备的控制细化，如 USB 设备，会被细分为 USB 鼠标、USB 键盘、USB 硬盘等。

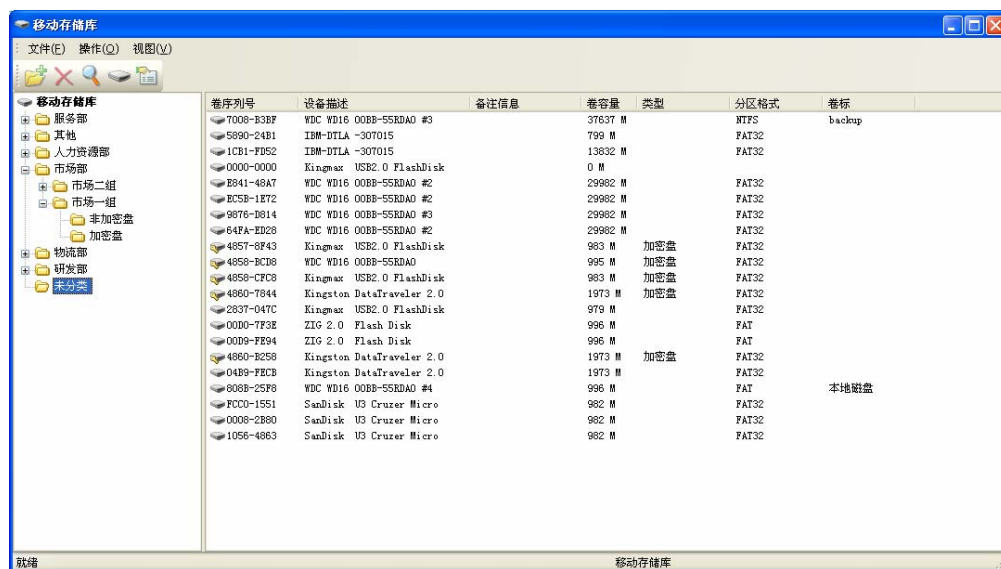
控制客户端各种类型的设备：

- 存储类设备：软/光盘、刻录机、磁带，可移动存储设备等；
- 通讯类设备：串/并口、SCSI、1394、蓝牙、红外线、MODEM、直接对联线等；
- USB 类设备：USB 键盘、鼠标、MODEM、映像设备、存储、光驱、硬盘和其他 USB 设备；
- 网络类设备：无线网卡、即插即用网卡、虚拟网卡等；
- 其他类设备：声音设备、虚拟光驱等。
- 禁止任何新增加的设备

## 5、 移动存储控制

移动存储控制模块能设置对移动存储设备的读写权限授权，并能加密移动存储设备。

- IP-guard 能自动将在网络中使用过的移动存储设备的信息加入到移动存储类别库中，管理人员可以把这些移动存储设备进行归类管理。



- IP-guard 能对移动存储库中的移动盘设置读写权限，可以控制指定的移动盘在指定的电脑上读/写的操作
- IP-guard 能对复制到移动存储上的文档进行自动加密，同时在有权限的计算机上，复制回硬盘时自动解密
- IP-guard 能对移动存储设备做整盘的加密格式化，加密格式化后，在有权限的机器上是透明使用的，但一旦把移动存储设备带离了授权区域，移动存储设备将不能被识别

## 6、 邮件管控

邮件管控模块能监控邮件收发情况，防止信息泄露。

- IP-guard 能详细记录普通标准协议邮件、 Exchange 邮件的收发以及网页邮件和 Lotus notes 邮件的发送，记录的内容包括收件人，发件人，邮件正文及附件等信息

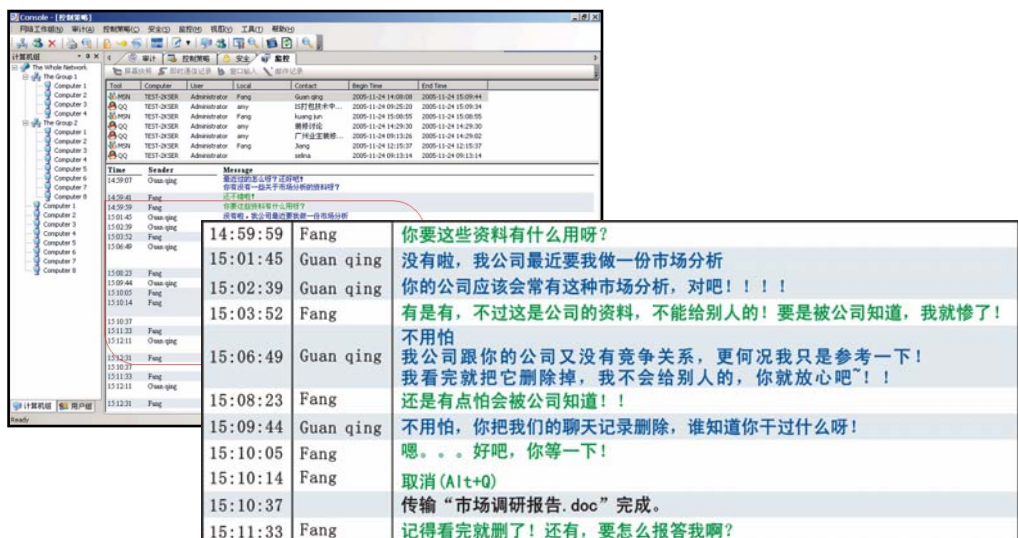


- IP-guard 能按指定的发件人、收件人、邮件主题、邮件大小对普通邮件和 Exchange 邮件的发送作控制。

## 7、 即时通讯工具管控

即时通讯工具管控能记录聊天记录，控制文件传输，防止信息泄露。

- IP-guard 能对 msn、QQ、TM、icq、yahoo、uc、popo、skype 等多种聊天工具的聊天内容进行监控，能完整的记录聊天的双方和聊天的内容



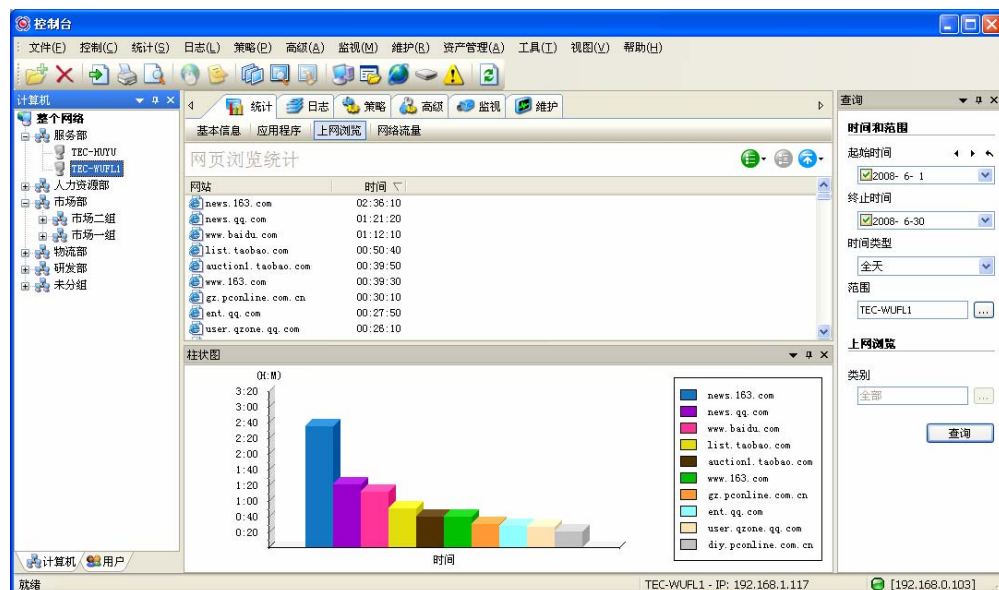


- IP-guard 能记录每个用户或计算机的所有应用程序的启动/关闭，以及窗口的切换标题动作，并且可以根据时间范围，计算机范围，应用程序名称，应用程序路径、窗口标题这几种查询条件查询
- IP-guard 能根据管理者的意愿定义控制策略，控制是否允许客户端计算机上各种应用程序的使用

## 9、 网页浏览管控

网页浏览管控模块能记录并控制网页浏览行为。

- IP-guard 支持多种内核类型的浏览器，其中包括 IE 以及 IE 内核的浏览器如：Maxthon、The world (世界之窗)等；非 IE 内核的浏览器如：火狐浏览器（Mozilla firefox）、Opera 和 chrome(google)等。
- IP-guard 支持网页的分类管理，管理员可以自定义类别，并将添加的网站归类到所属类别中，同时 IP-guard 也支持网址库的导入
- IP-guard 能统计访问的网页及其使用时间并以列表和图表两种方式显示。通过自定义的时间范围，对单个工作人员，部门，或整个网络的计算机的上网浏览使用情况进行统计



- IP-guard 能记录使用者访问过的所有网页信息：包括访问的计算机和用户，访问的时间，网页标题，网址等信息
- IP-guard 能根据网页的类库或网址的通配符对使用者访问网页的行为进行控制。

## 10、 网络管控

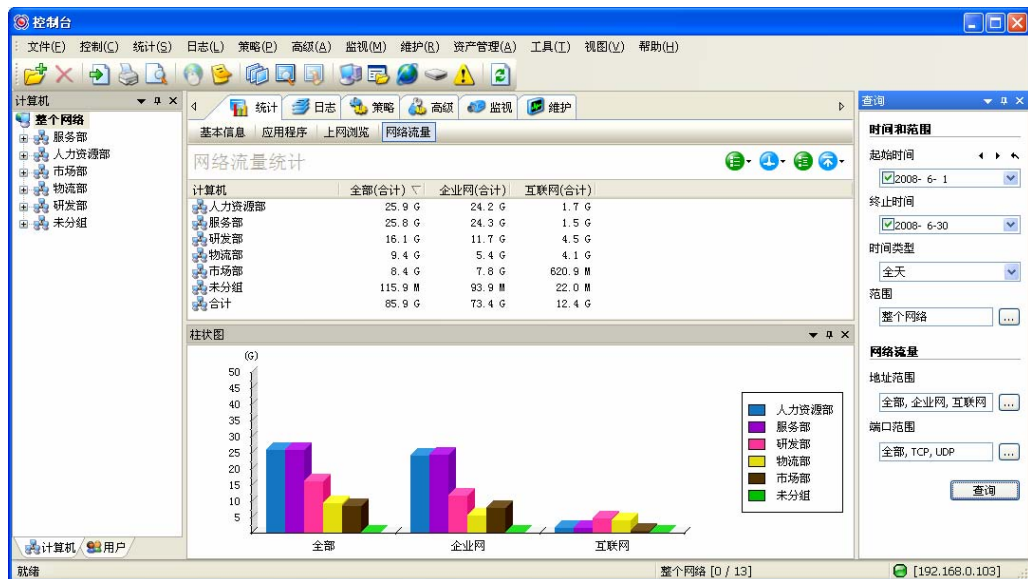
网络管控模块监管网络内计算机通信情况，增强企业网络的抵御能力

- IP-guard 提供网络地址和网络端口的分类，其中默认的网络地址类别有企业网、互联网，局域网、外网；默认的网络端口类别有 ICMP, TCP,UDP,邮件，网页，网络共享等，管理者还可以根据需要定义网络地址类别和网络端口类别
- IP-guard 能通过对网络通讯方向、IP 地址范围、网络端口范围的设置管理内网计算机使用网络的权限
- IP-guard 提供网络接入检查，能检测网络内是否有非法计算机接入，如有发生马上向管理者给出报警，并根据设定的策略阻止非法计算机接入网络

## 11、 流量管控

流量管控模块帮助统计分析计算机的流量情况，并对计算机的流量进行控制。

- IP-guard 能从多角度统计网络流量资源，分析各个计算机使用网络带宽的情况，统计方式包括按地址明细，端口明细，地址类别，端口类别

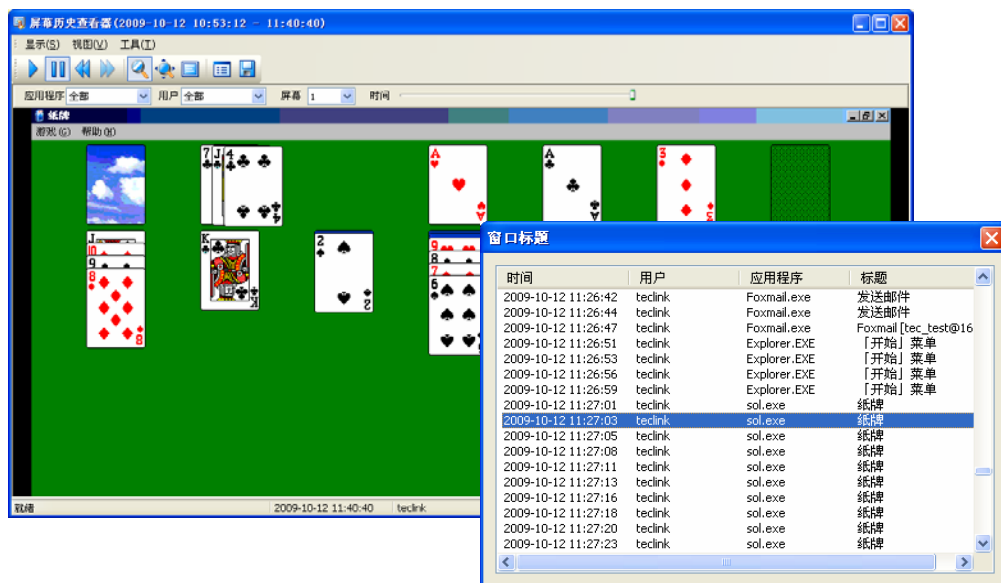


- IP-guard 能通过指定时间范围，网络地址、端口范围、流量方向来限制计算机流量速度范围

## 12、 屏幕监控

屏幕监控模块能远程查看计算机的桌面活动内容，记录桌面活动内容

- IP-guard 能实时查看当前工作的计算机上桌面画面，并能提供实时画面追踪，这个屏幕监控是支持多用户以及多扩展显示器的
- IP-guard 提供多屏监视功能，可以对一组的计算机进行批量集中监控，最多支持同时查看 16 台计算机的屏幕情况
- IP-guard 能根据应用程序或时间间隔频率记录屏幕的历史，这种记录是通过获取屏幕的增量，并进行高速压缩后才储存的，因此能更优化存储空间，同时屏幕录像可以根据应用程序名、时间、标题等进行查询，也可以导出为通用的视频格式



### 13、 远程维护

远程维护模块帮助管理员远程查看计算机的运行信息，并远程解决计算机的故障。

- IP-guard 能远程查看并维护网络内的计算机当前运行的：应用程序列表、进程列表、以及性能，设备管理，系统服务，磁盘管理，共享文件夹，计划任务，用户和组信息等

名称	值
使用率	
CPU使用	4 %
内存使用	72 %
总数	
句柄数	
线程数	
进程数	
物理内存	
总数	
可用数	
系统缓存	
认可用量	
总数	
限制	
峰值	
核心内存	
总数	
分页数	
未分页	

文件名称	PID	时间	CPU	CPU 时间	内存	虚拟内存	基本...	句柄数	线程数	路径
System I...	0		98.4	05:01:12	28 K	0 K	暂缺	0	1	
System	4		0.0	00:01:13	64 K	0 K	标准	344	59	
smss.exe	680	2008-05-14 ...	0.0	00:00:00	60 K	168 K	标准	21	3	C:\WINDOWS\System32\sm...
csrss.exe	736	2008-05-14 ...	0.0	00:00:33	3992 K	2268 K	标准	731	10	C:\WINDOWS\system32\cs...
winlogon...	760	2008-05-14 ...	0.0	00:00:04	4984 K	8444 K	高	539	23	C:\WINDOWS\system32\wi...
services...	804	2008-05-14 ...	0.0	00:03:18	2020 K	4452 K	标准	302	16	C:\WINDOWS\system32\se...
lsass.exe	816	2008-05-14 ...	0.0	00:00:17	3772 K	4280 K	标准	455	21	C:\WINDOWS\system32\ls...
svchost.exe	960	2008-05-14 ...	0.0	00:00:05	1404 K	3324 K	标准	220	19	C:\WINDOWS\system32\sv...
svchost.exe	1032	2008-05-14 ...	0.0	00:00:01	1476 K	2084 K	标准	396	10	C:\WINDOWS\system32\sv...
CCenter.exe	1120	2008-05-14 ...	0.0	00:00:00	868 K	644 K	标准	41	5	d:\Program Files\Risin...
svchost.exe	1136	2008-05-14 ...	0.0	00:08:39	209...	22252 K	标准	1734	71	C:\WINDOWS\System32\sv...
svchost.exe	1184	2008-05-14 ...	0.0	00:00:00	1172 K	1544 K	标准	90	5	C:\WINDOWS\system32\sv...
svchost.exe	1300	2008-05-14 ...	0.0	00:00:00	640 K	1932 K	标准	198	14	C:\WINDOWS\system32\sv...
explorer...	252	2008-05-14 ...	0.0	00:03:37	136...	31976 K	标准	754	15	C:\WINDOWS\Explorer.EXE
nsvsc32.exe	372	2008-05-14 ...	0.0	00:00:00	680 K	3692 K	标准	132	4	C:\WINDOWS\system32\inv...

- IP-guard 能远程连接到客户端桌面，并模拟查看端的鼠标键盘操作，帮助管理人员远程控制客户端计算机，对计算机进行系统维护和故障排除等
- IP-guard 能远程打开指定客户端文件夹进行文件传输，帮助管理员分析远程的文档数据，以及即时派送文件等

## 14、 资产管理

资产管理模块帮助系统统计查询计算机资产，加固系统，防止漏洞

- IP-guard 会在开机后对客户端的资产进行扫描，能自动获取客户端的硬件和软件资产信息，管理者能查询统计各个资产的分布情况，也能对软硬件资产自定义字段来记录相关情况，同时，IP-guard 还支持自定义资产，对一些不能获取的资产进行规范化管理

序号	计算机	操作系统
1	开发部-CAOYL	Microsoft Windows XP Professional
2	开发部-HEFANG	Microsoft Windows XP Professional
3	开发部-HEHUAN	Microsoft? Windows Vista? Business
4	开发部-LIHP	Microsoft Windows 2000 Professional
5	销售部-KUANGJUNXP	Microsoft Windows XP Professional
6	销售部-LIURG	Microsoft Wi
7	销售部-LIURG2003	Microsoft (R)
8	行政部-WLN	Microsoft Wi
9	行政部-WANGLIANG	Microsoft Wi
10	市场部-WINZKS	Microsoft Wi
11	市场部-WL	Microsoft Wi
12	市场部-WUFL	Microsoft Wi

序号	计算机	CPU	内存	硬盘驱动器	网卡
1	test-CAOYL	AMD Sempron(tm)...	AO 512MB	WDC WD800JD-00M...	NVIDIA nForce N...
2	test-WANGLIANG	AMD Sempron(tm)...	AO 256MB   AI 2...	WDC WD800JD-00L...	NVIDIA nForce N...
3	未分组-TEC-HEFANG	Intel(R) Celeron...	DIMM1 512MB   D...	Maxtor 6E040LD...	Realtek RTL8139...
4	未分组-TEC-HEHUAN	Intel(R) Celeron...	DIMM2 1024MB	ST3160815AS ATA...	Realtek RTL8168...
5	未分组-TEC-LIHP	Intel(R) Celeron...	AO 256MB   AI 2...	Maxtor 6T080LD...	VIA Rhine II Fa...
6	未分组-TEC-LIURG	Intel(R) Celeron...	AO 256MB   AI 2...	WDC WD400BB-75F...	VIA Rhine II Fa...
7	未分组-TEC-WT40	CELERON(TM)	BANK_0 128MB	QUANTUM FIREBAL...	Legend DFF-530T...
8	未分组-TEC-WUFL	Intel(R) Celeron...	DIMM1 256MB   D...	Maxtor 6E040LD...	Realtek RTL8139...
9	未分组-TEC-WIN2...	Intel(R) Core(T...	DIMM0 1024MB	ST3160815AS (15...	Realtek RTL8169...
10	未分组-TEC-WUFL	Intel(R) Celeron...	AO 256MB   AI 2...	Maxtor 6Y080LD...	VIA Rhine II Fa...
11	未分组-TEC_GY	Intel(R) Celeron...	DIMM1 512MB	WDC WD1600AAJB...	Realtek RTL8139...
12	未分组-TEST-WIN...	Intel(R) Celeron...	DIMM1 256MB   D...	ST360015A (57GB...	Realtek RTL8139...
13	未分组-TEST-WIN...	Intel(R) Celeron...	BANK_0 256MB	Maxtor 6Y120LD...	D-Link DFE-528T...

- IP-guard 能对软硬件资产的变更提供详细的日志信息，并能向管理者提供报警功能，帮助管理者管理企业的资产资源

类型	时间	计算机	资产	描述
增加	2008-03-24 09:14:16	CAOYL	键盘	标准 101/102 键或 Microsoft ...
增加	2008-03-24 09:14:11	CAOYL	鼠标	PS/2 Compatible Mouse
增加	2008-03-24 09:13:46	CAOYL	网卡	NVIDIA nForce Networking Con...
增加	2008-03-24 09:13:41	CAOYL	SCSI设备	Q45810Z WVE884N SCSI CdRom D...
增加	2008-03-24 09:13:15	CAOYL	硬盘驱动器	WDC WD800JD-00MSA1 (71GB, IDE)
增加	2008-03-24 09:13:10	CAOYL		
增加	2008-03-24 09:13:05	CAOYL		
增加	2008-03-21 16:46:03	TEST-WIN2		
删除	2008-03-21 13:17:03	TEC-WIN20		
删除	2008-03-21 13:16:53	TEC-WIN20		
删除	2008-03-21 13:16:48	TEC-WIN20		
删除	2008-03-21 13:16:43	TEC-WIN20		
删除	2008-03-21 13:16:38	TEC-WIN20		
删除	2008-03-21 13:16:08	TEC-WIN20		
删除	2008-03-21 13:15:58	TEC-WIN20		
删除	2008-03-21 11:42:10	TEC-WIN20		
删除	2008-03-21 11:42:05	TEC-WIN20		
删除	2008-03-21 11:42:00	TEC-WIN20		
删除	2008-03-21 11:41:55	TEC-WIN20		
增加	2008-03-21 10:10:50	TEC-WIN20		

类型	时间	计算机	资产	描述
增加	2008-03-25 10:12:55	CAOYL	应用软件	QQ2008 贺岁版
删除	2008-03-25 10:12:54	CAOYL	应用软件	QQ2007II 正式版
变化	2008-03-25 10:11:51	TEC-WUFL	杀毒软件	nod32 2.7 -> nod32 2.7
删除	2008-03-25 09:18:21	TEC-WUFL	杀毒软件	nod32 2.7 -> nod32 2.7
删除	2008-03-25 09:09:47	TEC-WUFL	应用软件	Fetion 2006
增加	2008-03-25 09:09:47	TEC-WUFL	应用软件	Fetion 2006
增加	2008-03-21 17:07:04	TEC-LIHP	应用软件	Lotus Notes 6.5 zh-CN
删除	2008-03-21 17:02:24	TEC-LIHP	应用软件	Lotus Notes 6.5 zh-CN
删除	2008-03-21 16:55:09	TEC-WIN2003...	应用软件	LiveUpdate 3.1 (Symantec Cor...
增加	2008-03-21 16:55:09	TEC-WIN2003...	应用软件	腾讯通RTX 客户端
变化	2008-03-21 14:04:02	TEC-WUFL	杀毒软件	nod32 2.7 -> nod32 2.7
删除	2008-03-21 13:09:08	TEC-WIN2003...	应用软件	LiveUpdate 3.1 (Symantec Cor...
变化	2008-03-21 09:15:09	TEC-WUFL	杀毒软件	nod32 2.7 -> nod32 2.7
增加	2008-03-20 18:03:22	TEC-WIN2003...	应用软件	腾讯通RTX 客户端
增加	2008-03-20 15:11:04	TEC-WIN2003...	应用软件	UltraVNC v1.0.1
增加	2008-03-12 12:13:14	TEC-PC142VISTA	应用软件	Microsoft Visual Studio 6.0 ...
增加	2008-03-12 12:11:04	TEC-PC142VISTA	应用软件	Microsoft Web Publishing Wiz...
增加	2008-03-12 11:55:35	TEC-PC142VISTA	应用软件	Microsoft VM For Java
增加	2008-03-12 11:34:10	TEC-PC142VISTA	应用软件	趋势科技 PC-cillin 2007 网络...
删除	2008-03-12 11:29:32	TEC-PC142VISTA	应用软件	金山毒霸 2008 杀毒套装

- IP-guard 能自动扫描各个客户端计算机的补丁情况，并能同步微软的官方网站，下载最新的系统补丁，然后即时分发给没安装补丁的计算机，自动安装补丁

- IP-guard 会自动扫描客户端的安全漏洞情况，对存在的安全漏洞提供详细的分析报告和解决方案

The screenshot displays two windows from the IP-guard software interface:

**补丁管理 (Patch Management):**

序号	严重级别	公告号	补丁ID	名称	未安装数
52	未知		934737	Excel Viewer 2003 Service Pack 3 (SF3)	0
53	严重	MS05-036	901214	Windows XP 安全更新程序 (KB901214)	0
54	重要	MS07-012	924667	Windows Server 2003 安全更新程序 (KB924667)	0
55	严重	MS07-009	927779		
56	中等	MS05-032	890046		
57	严重	MS06-070	924270		
58	严重	MS07-040	933654		
59	未知		936984		
60	重要	MS08-012	946254		
61	重要	MS07-007	927802		
62	重要	MS07-067	944653		
63	重要	MS07-041	939373		
64	重要	MS07-034	929123		
65	未知		110806		

**漏洞管理 (Vulnerability Management):**

序号	严重级别	名称	有漏洞数量	无漏洞数量
1	严重	未限制匿名连接	3	9
2	严重	没有重命名管理员账号	12	0
3	严重	Guest账号未禁用	4	8
4	信息	共享资源权限	3	9
5	严重	拥有系统管理员权限的用户过多	2	10
6	一般	登陆时显示上一次登陆的用户名	12	0
7	严重	密码的最小长度限制过短	12	0
8	严重	不是所有硬盘的文件系统都是NTFS格式	9	3
9	一般	未启用系统自动更新	8	4
10	严重	用户密码不会过期	12	0
11	一般	补丁需要重新启动才能更新	3	9

Below the vulnerability management window, a summary table shows the status of various clients:

序号	名称	有无漏洞
1	WANGLIANG	存在漏洞
2	TEC-LIHP	存在漏洞
3	TEC-HEFANG	存在漏洞
4	TEC-LIURG	存在漏洞
5	TEC-HEHUAN	无漏洞
6	TEST-WINZKTCNSP	存在漏洞

- IP-guard 能向客户端自动分发文件、应用程序和安装程序，自动分发各种文件会存放在指定的目录下，分发支持断点续传，支持后台安装和交互安装

---

## 四 IP-guard 的运行环境与性能指标

### 1、 IP-guard 基本软硬件配置要求:

	计算机基本要求	
数据库	SQL Server 2000 SP4 / MSDE SP4 / SQL Server 2005 SP1 / SQL Server 2005 Express SP1	
客户端模块	操作系统	Windows 2000 / XP / 2003 / Vista
	建议配置	Pentium4 / 512MB 内存 / 1GB 可用硬盘空间
控制台模块	操作系统	Win98 / Me / NT4 / 2000 / XP / 2003 / Vista
	建议配置	Pentium 4 / 512MB 内存 / 1GB 可用硬盘空间

### 2、 IP-guard 服务器建议配置

- **超过 100 台工作站:**  
服务器: Pentium 4 2G HZ CPU/ 2G 内存/ 120GB 或以上的可用硬盘空间/ 100MB 网卡
- **超过 500 台工作站:**  
服务器: 双核或双 CPU/ 4G 内存/ 160GB 或以上的可用硬盘空间/ 100MB 网卡
- **超过 1000 台工作站:**  
服务器: 四核 CPU/4G 内存/400GB 以上可用硬盘空间或使用硬盘阵列/ 1000MB 网卡

### 3、 IP-guard 数据量分析

天数 8 小时/天	工作站 数量	屏幕历史 记录间隔 (秒)	网络负荷 (服务器) (Mbps)	网络负荷 (服务器) (在 100MB 网络中所 占用网络带宽的百分 比)	屏幕记录 数据量 (GB)	日志记录 数据量 (MB)
1	100	15	1.1	1.1%	3.2	100
1	100	30	0.53	0.53%	1.6	100
1	100	60	0.27	0.27%	0.8	100
1	200	15	2.2	2.2%	6.4	200
1	200	30	1.06	1.06%	3.2	200
1	200	60	0.54	0.54%	1.6	200
1	500	15	3.3	3.3%	16	500
1	500	30	1.59	1.59%	8	500
1	500	60	0.71	0.71%	4	500
1	1000	15	11.00	11.00%	32	1000
1	1000	30	5.3	5.3%	16	1000
1	1000	60	2.7	2.7%	8	1000

## 五 IP-guard 的安装和部署

### 1、 服务器的安装

服务器一般安装在性能较高、容量较大的计算机上，建议安装服务器版的操作系统上，服务器安装之前必须首先安装 SQL Server 系列的数据库。

### 2、 客户端的安装

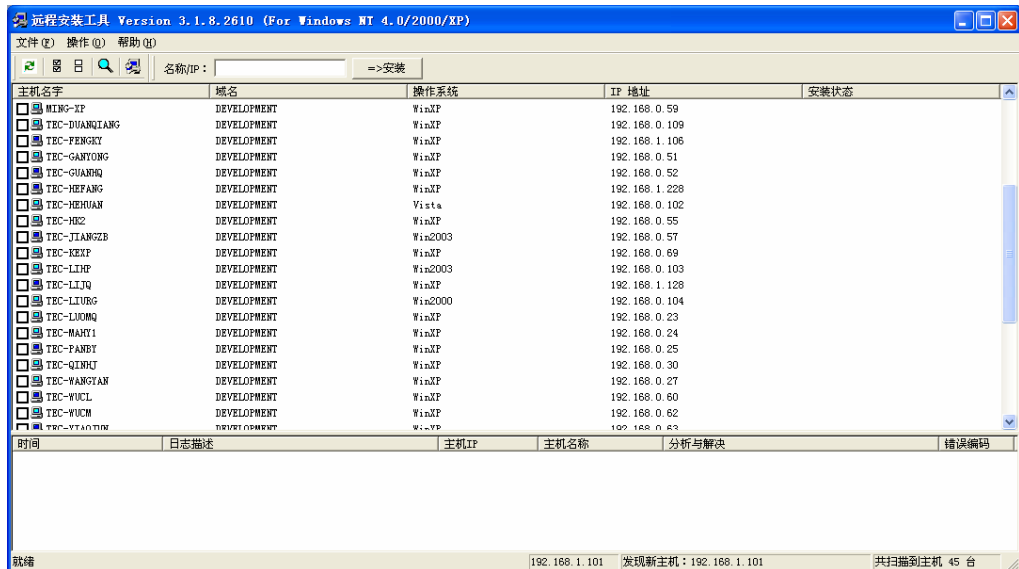
客户端程序部署于受管控的计算机上。客户端的安装需要有计算机的管理员权限，客户端的安装提供一下三种安装方式：

- 手工安装

手工安装适合在计算机的数目不多，而且相当分布集中的企业环境下。手工安装通过在服务器生成客户端安装程序，安装程序在需要进行安装的计算机上运行，则客户端安装完毕

- 远程推送方式安装

远程推送安装方式适合计算机数目较多，而且计算机分布相对分散的企业环境，远程安装工具能扫描指定网段内的计算机，并向其远程推送客户端安装程序进行安装



- 域脚本安装

域脚本安装方式适合部署有域环境的企业，通过修改域用户的登录脚本，在域用户登录域的时候安装客户端程序

### 3、 控制台的安装

控制台一般安装在企业相关管理人员计算机上，控制台能根据服务器的 IP 地址或计算机名进行访问

---

## 六 关于广州溢信科技有限公司

广州市溢信科技创立于 2001 年 7 月，是国内最早开始内网安全产品开发的企业之一，始终致力于对企业内网安全问题的研究和解决，专注于内网安全软件的研发，目前其自主研发的《IP-guard 内网安全管理系统》成为屈指可数的能够提供内网安全管理整体解决方案的产品之一，溢信科技也成长为当之无愧的领先的内网安全产品提供商。

发展中，溢信科技秉持专注和持续创新的信条，并以快速响应客户需求、为客户提供有效的内网安全保护作为不断前进的动力。专注成就专业，短短八年，溢信科技先后开发出 any@mail、any@web 和 IP-guard 三个系列的内网安全产品，其中屏幕监视、应用程序使用统计、网页浏览统计等多项功能都是由溢信科技率先实现并引入企业应用，每款产品都凭借其专业的品质赢得客户的广泛好评。持续创新的精神和以客户需求为主导的原则使得产品始终保持先进性，在信息化的各个时期都能很好的满足客户的需求，为客户提供更多价值。

如今，我们的客户遍布全国各行业、各类型组织，海外客户也不断增多，在帮助客户保证安全从而获得成功的同时，我们也积淀下了丰富的内网安全实践经验，愿与更多的组织分享，帮助更多组织实现信息化环境下的健康快速发展。