# IP-guard 一体化终端安全管理系统

## 产品详解&应用指南


TEC Solutions Limited

溢信科技

广州 | 深圳 | 珠海 | 北京 | 上海 | 长沙 | 重庆 | 成都
武汉 | 西安 | 郑州 | 济南 | 南京 | 杭州 | 厦门

广东广州科学城科学大道182号创新大厦C3区4楼
400-666-1438　　sales@ip-guard.net
www.ip-guard.net


IP-guard
专注终端安全 保护核心机密

证券代码：870985

# CONTENTS 目录





# PRODUCT IP-guard产品系列

01

IP-guard文档加密系统

02

IP-guard敏感内容识别系统

03

IP-guard终端安全管理系统

04

IP-guard安全网关

05

IP-guard准入网关

06

IP-guard安全U盘

# IP-guard产品概述

## IP-guard文档加密系统

为企业各种类型的电子文档提供高强度加密管理，同时不影响用户的使用习惯。

## IP-guard敏感内容识别系统

对企业海量文件的内容进行精准识别，对高价值文件实施更准确的保护措施。

## IP-guard终端安全管理系统

**文档操作管控**
对文档生命周期内的所有操作进行详尽的审计和严格的控制，保护文档安全。

**移动存储管控**
极大的降低了U盘滥用造成的信息泄露和病毒泛滥等安全隐患。

**设备管控**
防范USB存储、刻录机以及任何新增设备带来的泄密风险，规范设备的使用。

**文档打印管控**
能够保障重要文档不会因文档打印而造成泄密，节约打印资源。

**即时通讯管控**
防止企业内部资料通过QQ、微信、Skype等即时通讯工具外泄。

**邮件管控**
有效防范电子邮件使用过程中的信息外泄风险。

**应用程序管控**
掌握并管理用户对软件的应用，规范桌面操作行为，提升工作效率。

**网页浏览管控**
掌握并管理用户的上网浏览行为，屏蔽存在安全隐患以及于工作无益的网站。

**网络控制**
管理计算机之间的网络通讯权限，同时阻断恶意端口以及下载端口。

**网络流量管控**
掌握终端流量状态，合理分配带宽，保证网络畅通。

**屏幕监视**
严格强大的屏幕记录功能，使得安全审计更加直观。

**资产管理**
为IT资产的高效、集中管理提供方法，实现IT资产的有效利用。

**远程维护**
帮助快速判断并排除故障，保证系统时刻顺畅运行。

**风险审计报表**
对事件日志进行分析统计，及时发现安全隐患，及时风险预警，安全动态全掌控。

**文档云备份**
对终端文档进行集中自动备份，解决企业文档管理难、容易损坏和丢失的难题。

**基本功能（必选）**
提供IP-guard产品架构以及丰富的基础管理功能。

## IP-guard安全网关

通过上传解密、下载加密，防止服务器上的数据外泄，保护服务器上的数据安全。

## IP-guard准入网关

杜绝非法接入带来的信息泄密风险，同时避免PC脱离IP-guard管控。

## IP-guard安全U盘

有效保护U盘内的企业机密信息安全，避免因为U盘丢失造成的资料外泄。

# IP-guard 文档加密系统

IP-guard文档加密系统，加密电子文档、丰富权限设置，在不影响员工使用习惯的前提下为企业构建严密的立体保护体系，保护企业核心电子信息和数据安全。

## 产品模块

**文档透明加密**
为企业各种模式的电子文档提供高强度加密管理，同时不影响用户的使用习惯。

## 产品优势

- **智能缓冲技术，稳定性更出众**
  基于成熟的驱动层兼应用层加密技术，更具独有的智能缓冲技术，让系统保持稳定的同时兼具性能与安全。
- **多种加密模式，满足不同需求**
  强制加密、智能加密与只读加密等多种加密模式，满足用户的多种应用场景需求。
- **三重灾备方案，确保业务不间断**
  双机热备、网络故障应急机制和明文备份服务器，从容应对主服务器无法连接、断网、断电等各种状况。
- **加密管理范围广泛，全面覆盖应用场景**
  权限管理、安全网关、外发管理、离线授权管理四大功能，全面覆盖加密文件的内部流转、服务器上的信息存取、外发给合作伙伴使用、员工离线使用这四大常见应用场景。
- **审计、管控、加密，强强联合整体防护**
  与审计、管控一起组成三重保护信息防泄露整体解决方案，三种强力技术，帮助企业达到一流的信息防泄露效果。

# IP-guard
## 文档透明加密

能够为企业各类电子文档提供高强度的加密管理，确保文档随时随地都处于加密状态，严防信息泄露。

## 功能详解

### 【透明加密】

1、机密文档在授权终端上始终以加密形式保存，文档打开时自动解密，保存时自动加密，不影响用户使用习惯。
2、加密文档即使流传到外部，无法打开及使用。
3、加密文档的使用过程中，用户不能通过复制粘贴、截屏、打印（包括虚拟打印）等方式窃取加密文档中的内容。
4、免费支持各种应用，不论是办公文档、设计图纸、开发代码或是它们的压缩包文件等，都能进行加密保护。
5、支持自定义安全密钥，能自由选择加密算法，安全性尽在用户掌握。

### 【加密模式】

▲ 强制加密
所有文档都进行强制性地自动加密，文档从创建开始，无论修改、移动、复制，全程受到加密保护。

▲ 智能加密
只对重要的文档进行加密保护，加密文档编辑修改另存以后，仍旧是加密文档。普通文档不需要加密，可以和加密文档同时打开使用，修改保存后仍是明文状态。

▲ 只读加密
用户自己产生的文档不用加密，加密文档可以以只读的方式查看，不能对加密文档进行编辑修改。

# IP-guard
## 文档透明加密

细致的应用管理，严防企业重要文档遭到非法外泄，同时也满足企业个性化办公需求。

### 【权限控制】

▲ 文档权限管理
1、为不同的人分配不同的文档权限，严格控制保密范围。
2、根据文档的敏感程度，可将加密文档划归不同的安全区域和级别，建立“分部门分级别”的保密机制，以便让不同部门和职位的用户使用。
3、用户可调整文档的区域和级别，对重要文档可采取提高其级别的方法来禁止普通用户的使用，不同安全区域和密级的文档需要进行交互时，可修改指定加密文档的安全区域与加密级别。
4、用户可以根据文档的重要程度及分享范围，自主决定文档的使用者及其使用的权限，可限制的权限包括阅读、修改、复制、打印、截屏、有效期和解密。

▲ 加密权限USBKEY
通过插入授权USBKEY，临时提升用户的加密授权。

▲ 多级审批机制
1、支持单级、多级、逐级、会签审批，满足多级别办公审批流程需要，保证申请得到各级别管理者复核和审查。
2、支持Web审批，增加工作便利性；且支持Web审批预览及文件下载。
3、移动端安全审批，能在移动端即时接收审批申请通知，可直接预览审批各类申请。

### 【对外交互】

▲ 外发控制
1、可对需要外发的文档进行加密控制，防止二次泄密。
2、可对特定的机器和人员进行授权，只允许授权人员在特定机器上打开并查看外发文档。
3、能够指定外发文档的查看期限、打开次数、打开密码以及复制、编辑、打印、截屏等使用权限。
4、支持外发USBKEY，认证后才能打开外发文档，不需要绑定计算机。
5、外发文档支持过期自动删除，并支持指定进程对指定网络的访问。
6、可以自定义外发模板，方便统一管理。

# IP-guard
## 文档透明加密

丰富的权限管控，帮助企业灵活管控加密文档在内外部的使用和流转。

### 【离线办公】

▲ 出差办公

1、针对人员出差，可对其授予离线策略，确保加密文档在出差期间依然可正常使用，不影响正常办公。

2、可对出差人员设置个性化的离线策略，包括离线时长、加密软件类别以及文档使用权限等。

▲ 离线权限USBKEY

出差时插入离线权限USBKEY，可保证加密功能继续使用。

▲ 移动加密客户端

1、插入设备能打开加密文件，拔出设备不能打开加密文件，不用另外安装加密客户端。

2、可对移动加密客户端进行授权及更新加密策略，授权后的移动客户端才能正常使用。

3、使用移动加密客户端时，需要输入正确的密码才能登录使用。

### 【系统支持】

▲ 支持Windows、Mac OS及Linux操作系统，实现跨平台管理。

▲ 加密文档可在Windows、Mac OS及Linux系统间正常使用，兼容性强。

▲ 支持智能移动端的APP审批，支持通过手机查看器预览加密文件。

### 【系统扩展】

▲ 加密系统接口

通过系统接口可以与各类应用系统进行无缝对接，包括OA办公系统、客户关系管理系统、ERP系统等，提供文档加解密、文档权限控制、身份认证等功能，只要对业务系统做少量的开发就可以与IP-guard服务器对接。

▲ 移动安全SDK

支持为第三方移动应用APP开发者提供SDK，保证其应用可以授权查看加密文档及通过安全网关访问保护的服务器。

# IP-guard
## 文档透明加密

支持各主流系统，方便企业统一管理；多种灾备机制，确保加密系统的正常运行。

### 【灾备机制】

1、硬件灾备

IP-guard服务器支持双机热备，在主服务器出现故障时从服务器可完全接替主服务器的工作，确保加密系统不受任何影响，也可以部署一个或者多个备用服务器，当主从服务器都出现故障时，备用服务器将自动接管加密系统，确保终端可以进行文档加解密操作。

2、网络灾备

可以预设容灾时间，当用户出现网络故障时，在容灾时间范围内，IP-guard加密仍然可正常使用。

3、文档灾备

可将加密文档以明文或密文的形式进行备份，当出现文档损坏或丢失，可从备份中找回相应的明文或密文，避免重要文档遭到损坏。

## 典型应用

【文档加密保护】

- 将设计图纸、开发代码、财务信息、客户资料等重要的电子文档在完全不改变用户的习惯下进行自动加密，即使这些文档被非法带离企业也无法解密和应用。

【部门文档隔离】

- 用户根据文档的重要性设置分享范围，自主设置文档的使用者和权限，可设置阅读、修改、复制、打印、截屏、有效期和解密等权限。

【防止二次泄密】

- 授予客户、合作伙伴等外界对象加密文档外发查看器，限制其在指定客户端上打开文档，规定使用加密文档的打开时间、打开次数等。

【出差办公】

- 对于需要出差的同事，可以给予有限的离线授权，允许外出继续使用加密文档，文档仍能保持加密状态，只能在被授权的计算机上使用。

【移动办公】

- 可以在手机、平板等移动终端正常查看办公类加密文档，满足企业的移动办公需要。

## 常用组合

基本功能+文档加密+安全网关+文档操作管控。

## IP-guard 敏感内容识别系统

IP-guard敏感内容识别模块，能对企业大量的文件进行精准识别和分类，依据先进的内容识别技术，对高价值的数据采取更有针对性的保护措施。

### 功能详解

【敏感内容定义】

1、支持通过关键字建立特征规则，可设置包含内容、排除内容、命中次数、去重和区分大小写等条件。

2、支持通过正则表达式建立特征规则，可设置包含内容、排除内容、命中次数、去重和区分大小写等条件。

3、支持在信息分类中将多个特征规则进行组合，设置每个特征规则的权重，符合规则则进行权重加分，权重相加后阈值达到100，则符合该信息分类。

【敏感内容发现】

1、支持点对点扫描远端计算机上含敏感内容的文档，可指定扫描的敏感内容及文件类型，支持对扫描结果进行加密、解密或变更其安全属性。

2、支持批量扫描全网计算机含敏感内容的文档，可设置扫描对象、敏感信息分类、包含文件类型及排除文件类型、文件大小、性能优先、扫描时段等条件。

【敏感内容监视】

1、新建或下载文档到计算机，支持对文档内容进行实时检测，发现敏感内容，可触发报警、警告、审计和记录屏幕策略。

2、文档通过移动存储设备、网络盘、IM工具、邮件和网页外传时，发现敏感内容，可触发报警、警告、审计和备份副本。

【敏感内容保护】

1、创建、编辑、下载、U盘拷入含有敏感信息的文件时，自动对文件进行加密保护，不含敏感内容的文档不加密。

2、当含有敏感信息的文档发生外传行为时（如拷贝到移动盘、网络盘，发送邮件、IM传送、网页上传等），可触发阻断或锁定计算机的策略。　＊备注：此模块必须配合其他模块一起使用。

【敏感信息日志】

详细记录含敏感内容文档的各种操作类型，包括：复制到移动盘、复制到网络盘、IM传送、发送邮件、网页上传、新建、修改和扫描等，还可以记录操作的计算机、用户、时间、匹配的信息分类、文件名称、路径、文件大小等信息。

### 典型应用

【敏感信息审计】

- 管理员通过批量扫描的方式发现销售部中含有特定关键字的文档。
- 设置公共计算机不允许存在含有敏感信息的文档，如果发现进行报警且记录日志。

【敏感信息防泄露】

- 客服部通过网络（IM工具、邮件）发送含有“敏感信息”的文件，会触发报警提示或进行阻断。
- 财务部从应用系统下载、U盘拷入、网络下载文件到本地，如果文件包含敏感内容，自动对文件进行加密保护。

### 产品优势

- 此技术可忽略不重要的数据，只保护拥有较高商业价值的数据，最大程度削减数据管理的成本，使数据保护更有针对性。
- 全局掌握企业关键数据的分布，进而保护数据资产。
- 含敏感内容的文件落地时，可更加准确地进行加密保护。
- 对涉及敏感内容的文档外传行为进行日志记录、屏幕记录和备份，完整跟踪重要文件的流通情况。

### 常用组合

文档加密+文档操作管控+移动存储管控+设备管控+文档打印管控+即时通讯管控+邮件管控+网页浏览管控+屏幕监视，有效保护敏感信息。

## IP-guard 终端安全管理系统

IP-guard终端安全管理系统，十六大功能模块，全面而细致地对终端进行详尽审计、严格管控和稳定加密，满足企业防信息泄露、员工行为管理、终端系统运维的全面信息安全及管理需要。

### 产品模块

**文档操作管控**

对文档全生命周期内的所有操作进行详尽审计和严格管控，保护文档安全。

**设备管控**

防范USB存储、智能手机、刻录机及任何新增设备带来的泄密风险，规范设备的使用。

**即时通讯管控**

防止企业内部资料通过QQ、微信、Skype等即时通讯工具外泄。

**应用程序管控**

掌握并管理用户对软件的应用，规范桌面操作行为，提升工作效率。

**网络控制**

阻止外来计算机非法接入企业终端获取机密信息，保护网络安全。

**屏幕监视**

严格强大的屏幕记录功能，使得安全审计更加直观。

**远程维护**

帮助快速判断并排除故障，保证系统时刻顺畅运行。

**文档云备份**

对终端文档进行集中自动备份，解决企业文档管理难、容易损坏和丢失的难题。

**移动存储管控**

极大的降低了U盘滥用造成的信息泄露和病毒泛滥等安全隐患。

**文档打印管控**

能够保障重要文档不会因文档打印而造成泄密，节约打印资源。

**邮件管控**

控制邮件收发，有效防范电子邮件使用过程中的信息外泄风险。

**网页浏览管控**

掌握并管理用户的上网浏览行为，屏蔽存在安全隐患以及与工作无关的网站。

**网络流量管控**

掌握企业中流量状态，合理分配带宽，保证网络畅通。

**资产管理**

能使IT资产高效、集中管理，实现IT资产的有效利用。

**风险审计报表**

对事件日志进行分析统计，发现安全隐患，及时风险预警，安全动态全掌控。

**基本功能（必选）**

提供IP-guard产品架构以及丰富的基础管理功能。

### 产品优势

- **立足整体，全面管理内网行为**

  从整体出发，对操作审计、行为管控、系统运维等终端安全项目进行全面管理，严格规范用户的计算机使用行为，大幅优化IT资产的管理，实现安全风险防范，提升工作效率。

- **深度细致，有效管控泄密风险**

  整合运用日志审计、权限管理手段，管理设备、网络、操作、系统4大方面包括可移动设备、IM、文档操作等20种泄密风险，对终端行为进行更精细的管理。

- **统一平台，组合灵活易于管理**

  通过单一控制台对所有客户端进行有效管理和维护，保证系统时刻运行顺畅，让IT为业务发展提供更多动力，保证业务顺利开展；模块化的组合方便用户灵活选择，用户可结合自身的需求，以最小的投入带给用户最大的信息防泄露收益。

# IP-guard
## 文档操作管控

IP-guard文档操作管控模块能完整记录用户电脑文档使用与传播的全过程，发现违规使用行为，防止文档被非法篡改或泄露。

## 功能详解

【文档操作审计】
全面细致地审计存储于服务器、硬盘、光盘、移动盘、网盘等各种位置的文档，详细记录从创建开始到删除文档全生命周期发生的所有操作，保护核心资料的安全。

【文档操作控制】
管理用户的文档使用权限，限制对重要文档的访问、修改和删除。

【敏感操作备份】
在文档被复制、篡改或删除前备份，防止敏感文档损坏，同时留存证据。

【刻录审计】
支持记录刻录操作日志，备份刻录文件副本。

## 典型应用

【审计文档操作】
- 审计指定的文档类型或者特定文件夹下的文档的使用和传播流转情况，帮助发现将重要文档复制到U盘和网络上的非法操作，同时为信息泄密行为提供证据。

【区分操作权限】
- 指定员工对重要文档可读取、修改、删除等操作而其他员工只能访问。

【敏感操作备份】
- 对将离职员工设置删除前备份策略，防止离职人员把重要文件删除。

## 产品优势

- 可对多种类型盘符的文档进行控制和全面详尽的操作记录。
- 对光盘刻录和智能手机等同步操作进行记录。
- 在重要文档被复制、篡改或删除前备份。
- 支持对指定类型文件或者对整个文件夹的操作权限进行统一管理。
- 部分功能支持Mac OS/Linux操作系统。

## 常用组合

文档操作管控+移动存储管控，可实现对移动存储拷贝文档的同步备份。
文档操作管控+即时通讯管控，可实现对通过即时通讯工具传输文档的同步备份。

# IP-guard
## 移动存储管控

IP-guard移动存储管控模块可以分类规范移动存储设备的使用，应用权限控制与移动盘加密可实现“内盘内用，外盘外用”，防范移动存储泄密。

## 功能详解

【移动存储审计】
1、准确识别曾接入到网内的所有移动存储设备，记录设备详细信息，掌握移动存储设备使用情况。
2、支持对移动存储设备进行分类管理，可将企业内部移动存储设备按部门划分。

【移动存储授权】
1、单独控制每一个移动存储设备的读写权限，禁止外来移动存储设备在企业内部使用。
2、部门所属的移动盘，也只能在企业授权的区域内使用，实现专盘专用。

【移动存储加密】
1、可将普通移动存储设备格式化为加密盘，只能在内部使用，如加密盘丢失，内部文件也无法打开。
2、将复制到移动存储上的文件自动加密，加密文档只能在授权计算机上解密使用。

【临时策略申请】
用户可在客户端提交策略变更申请，请求在指定时间段内放开U盘的读或写权限。

【设备注册管理】
对移动存储设备的生命周期的管理，包括对移动存储设备的注册、分类、挂失、注销等。

## 典型应用

【外盘外用、内盘内用】
- 禁止员工的自带U盘在公司内部使用，做到外盘外用。
- 将企业内部U盘制作成专用的加密盘，只能在内部使用，做到内盘内用，U盘不能在外部被打开，防止被动泄密。

【移动存储审计】
- 查询指定U盘在各个计算机的插拔和文档操作情况。

【移动存储授权】
- 当员工需要使用U盘时，可以在客户端申请临时放开该U盘的读写权限，审批员根据申请内容以及实际需要决定是否通过。

## 产品优势

- 能对具体的U盘进行识别和区分。
- 提供写入时加密和整盘加密两种加密方式，让移动存储应用的安全性更加有保证。
- 允许对所有移动存储设备分门别类，设定策略更加方便。
- 可以按用户、部门、特定设备等不同维度对移动存储进行授权。

## 常用组合

移动存储管控+文档操作管控，实现对移动存储拷贝文档的同步备份。

# IP-guard
## 设备管控

IP-guard设备管控模块可以对各种计算机外设的使用进行控制，防止企业机密通过外设被非法查看、拷贝与带出。

## 功能详解

【存储设备管控】
管理U盘、移动硬盘、智能手机、光驱、刻录机等移动存储设备的使用，防止内部信息被随意带出公司。
【通讯设备管控】
管理通讯接口、无线网卡、即插即用网卡等网络设备的使用，避免非法外联带来的风险。
【音视频设备管控】
管理声卡、摄像头等音视频设备的应用，避免工作时间分散注意力。
【刻录管控】
1、禁止没有授权的用户使用刻录软件刻录光盘。
2、仅允许用户使用专用的刻录工具进行刻录，禁用其他第三方刻录工具。
【临时策略申请】
用户可在客户端提交策略变更申请，申请在指定时间段内使用指定类型的外接设备。

## 典型应用

【常用设备管控】
- 对常用的外联设备如4G上网卡、USB网卡、蓝牙、U盘、移动硬盘、便携设备、附加硬盘等进行限制，防止信息泄露。

【WIFI连接管控】
- 设置内部计算机只允许连接公司指定wifi热点。

【智能手机管控】
- 禁止手机以便携设备方式、U盘存储方式和手机助手方式接入电脑，禁止通过智能手机外传资料。

【音频设备管控】
- 上班时间限制声卡等设备的使用，休息时间开放，实现人性化管理。

【未知设备管控】
- 禁止其他一切未知新设备的接入，保证公司内部网络的安全。

## 产品优势

- 细化USB设备，能更精准的进行管控。
- 支持对智能手机、4G上网卡以及刻录机等常用外设进行控制。
- 可以用户自主申请临时放开设备使用权限，简化申请审批工作，同时也避免了管理员忘记回收权限带来的安全风险。

## 常用组合

移动存储管控+设备管控，实现对外设的严格管控，不仅可灵活选择控制移动存储设备，还可对移动存储端口及蓝牙、红外等端口进行封堵。

# IP-guard
## 文档打印管控

IP-guard文档打印管控模块，有效审计每一次打印操作，灵活的控制打印权限，防止纸质渠道的信息外泄与打印浪费。

## 功能详解

【打印操作审计】
详细记录每一次打印操作的时间、用户、文件名、页数等信息，方便管理员预防安全风险，追溯打印内容。
【打印内容备份】
获取打印内容映像并以图片形式进行备份。
【打印授权管理】
1、管理用户对各类打印机的使用权限，包括虚拟打印机、共享打印机、本地打印机、网络打印机等，可限制随意使用高成本打印机打印，节省成本。
2、限制能够进行打印的应用程序，防止如ERP等重要程序打印泄密。
【打印水印】
支持在打印纸质文档上显示公司logo，公司及用户信息相关的文字水印、图片水印、二维码水印、点阵水印等。
【临时策略申请】
1、用户可在客户端提交策略变更申请，请求在时间段内放开指定打印机和应用程序的打印权限。
2、用户可在客户端提交策略变更申请，请求在时间段内取消指定打印机和应用程序的打印水印。

## 典型应用

【打印内容审计】
- 批量导出打印记录图片，审计打印内容。

【降低打印成本】
- 限制随意使用高成本打印机进行打印。

【打印程序管理】
- 限制通过ERP、OA等程序直接打印，防止如财务信息等机密信息打印外泄。

【标识版权信息】
- 自定义水印，对打印出的文档申明版权，还可显示打印时间和打印用户。

【打印授权管理】
- 需要临时打印时，可通过申请放开某个实体打印机以及某应用程序的打印权限，管理者审核通过后即可使用。

## 产品优势

- 按照客户需要提供打印水印的功能。
- 支持对OA、ERP等无文档形式的打印内容进行记录。

## 常用组合

文档打印管控+网络流量控制，实现企业资源的合理分配控制。
文档打印管控+文档操作管控，进行严格的信息防泄露。

# IP-guard
## 即时通讯管控

IP-guard即时通讯管控模块，完整地记录QQ、微信、Skype等即时通讯工具的聊天内容，了解用户工作状态，防止重要文件经由即时通讯工具泄露。

## 功能详解

【聊天记录审计】
完整记录QQ、微信、企业微信、钉钉、Skype、TM、RTX、阿里旺旺等数十种主流即时通讯工具的聊天内容，防止有意无意泄密。
【外发文档备份】
能够对外发的文档进行备份，并可以选择备份的文档类型，以供安全审计。
【文档外发控制】
1、能够控制指定类型或指定文件夹的文件发送，控制非法的文件传输。
2、限制通过即时通讯工具外发指定名称或者超过限定大小的文件。
【图片外发控制】
限制通过即时通讯工具外发图片，并可备份被禁止发送的图片。
【限制账号登录】
限制私人QQ的使用，指定登陆工作QQ，增强工作效率，防止公司资源流失。

## 典型应用

【聊天内容审计】
- 通过查询功能，查找用户是否在聊天中涉及敏感信息。

【限制聊天账号】
- 指定登陆公司的QQ账号，可提高员工工作效率的同时也防止了内部资源的流失。

【文档外发控制】
- 禁止通过QQ、微信、Skype等工具外发文档、图片和截屏。

## 产品优势

- 支持QQ、微信、Skype等主流即时通讯工具的审计和管控。
- 支持对文档和图片传输进行记录和控制。
- 支持限制QQ账号的登录。
- 随着即时通讯工具的升级而不断更新，确保管控持续有效。

## 常用组合

即时通讯管控+文档操作管控，实现对通过即时通讯工具传输文档的审计和管控。

# IP-guard
## 邮件管控

IP-guard邮件管控模块帮助企业记录用户收发的电子邮件，发现违规行为，控制电子邮件收发，防止重要信息泄露。

## 功能详解

【邮件信息记录】
完整记录收发邮件的正文、附件、主题、大小、时间等信息，便于企业对邮件的安全使用情况进行统计。
【邮件发送控制】
可通过收件人、发件人、主题、附件名、邮件大小等关键字设置策略来控制邮件收发，防止企业的重要信息通过邮件方式泄露。

## 典型应用

【邮件内容审计】
- 对企业外发邮件的内容进行定期查看，确保邮件的合规使用。

【规范邮箱使用】
- 限定只能使用企业规定的邮箱。

【强制抄送邮件】
- 邮件发送到外部必须抄送部门主管才能发送成功。

【邮件附件控制】
- 禁止发送包含附件的邮件。

## 产品优势

- 能够支持对Lotus邮件、Exchange邮件、普通邮件、网页邮件四种类型邮件审计。
- 能通过限定收发件人、主题、附件名称及大小等，限制邮件的发送。
- 发送邮件时，可以实现必须抄送给相应的管理者才能正常发送。
- 支持对邮件附件内容进行自动备份。
- 支持https协议的邮件监控。

## 常用组合

邮件管控+即时通讯管控，对网络传输文档进行控制。

# IP-guard
## 应用程序管控

IP-guard应用程序管控模块，能帮助管理者清楚了解用户使用了哪些应用程序，直观多样的报表辅助制定黑白名单，防范不良程序风险，有效提升工作效率。

## 功能详解

【应用程序统计】

1、统计用户使用各种应用程序的时长及百分比，并以清晰的图表形式输出统计结果，以了解用户工作情况。

2、可按照部门类型、应用类型等多个角度对应用程序进行分类统计，详细掌握工作状态，进行效率评估。

3、同时支持对应用程序进行自定义分类统计，全面掌握内部动态。

【应用程序记录】

记录各种程序的启动/退出、窗口标题切换等信息。

【应用程序控制】

1、限制用户使用指定应用程序的权限，防止存在安全风险的程序运行。

2、支持对应用程序进行分类控制。

3、支持分时段进行控制，实现人性化管理。

【软件安装/卸载管理】

1、可以限制员工安装工作无关的软件，同时也能禁止员工卸载重要的应用软件，规范员工电脑的软件使用。

2、支持对客户端进行批量卸载软件，同时可通过“可持续”任务对指定软件进行“监控”，卸载之后再次安装也能被卸载。

【屏幕水印】

支持在计算机屏幕或应用程序上显示图片、文字、二维码、点阵水印，防止拍照泄密。

## 典型应用

【工作效率统计】

- 对各种应用程序进行分类，并且通过应用程序统计制作用户计算机应用的报表，分析用户的工作状态。

【应用程序分类】

- 自动收集所有客户端运行过的应用程序，并提供给管理员进行分类管理，然后可根据应用程序的分类进行统计及控制。

【应用程序控制】

- 限制用户在工作时间炒股、打游戏等，休息时间适当放松限制，禁止有潜在安全风险的程序运行。

【防止病毒运行】

- 禁止U盘程序运行，防止U盘病毒。

## 产品优势

- 根据应用程序特征值限制程序运行，即使用户更改进程名，管控依然有效。
- 对安装/卸载应用程序的权限进行控制，使终端的应用程序得到合理控制。支持屏幕水印，防止拍照泄密。
- 统计应用程序使用时长，让管理者详细掌握应用程序的使用行为，为评估工作效率提供了依据。

## 常用组合

应用程序管控+网页浏览管控+网络流量管控，对桌面行为进行严格的管控。

# IP-guard
## 网页浏览管控

IP-guard网页浏览管控模块，能够帮助IT管理人员建立符合企业安全和管理策略的网站访问黑白名单，审计并规范用户的上网行为，有效降低安全风险的同时，更能提高员工的工作效率。

## 功能详解

【网页浏览统计】

1、统计用户访问各网站的时长及百分比，并以清晰的图表形式输出统计结果，掌握用户访问各类型网站的时长和比重。

2、可按照部门类型、网站类型等多个角度对网页浏览进行分类统计。

3、同时支持对网页进行自定义分类统计，合理管控任何类型网页浏览。

【网页浏览审计】

记录浏览网页的标题、网址、时间等详细信息。

【网页浏览控制】

1、控制用户允许访问的网站范围，减少了访问非法网站带来的安全风险。

2、支持分时段、分类别进行上网限制，帮助员工专注核心工作。

3、支持在网址中使用通配符。

## 典型应用

【网站浏览统计】

- 对各种网站进行分类，并通过网页浏览统计制作用户访问网页的行为报表，分析用户网页浏览行为。

【浏览行为审计】

- 查看用户访问的网页标题、地址、时间等，了解用户的上网行为。

【网页访问控制】

- 通过自定义黑白名单，任何时间禁止用户访问违规违法网站，工作时间限制访问与工作无关的网站，休息时间适当放松限制。

## 产品优势

- 全面记录用户所访问的所有网页网址、标题、时间，并能够方便查询。
- 支持包括IE、Firefox、Chrome、360等绝大部分的主流浏览器。
- 可控制Http(s)协议、FTP协议和Tcp协议的上传行为。
- 直观、清晰的网页浏览时间统计，详细掌握用户的上网浏览行为。

## 常用组合

网页浏览管控+应用程序管控+网络流量管控等模块组合，可对桌面行为进行严格的管控。

# IP-guard
## 网络控制

IP-guard网络控制可管理计算机之间的网络通讯权限，阻断恶意端口以及下载端口，防止病毒入侵，保护终端安全。

## 功能详解

【网络通讯控制】
通过对程序、网络端口、IP地址、通信方向等参数限制计算机对内网、互联网等的访问，避免由随意的信息交流带来的风险。
【安全检测的网络控制功能】
根据安全检测结果，对不符合安全检测条件的客户端进行断网控制，可以设置例外地址。一旦客户端计算机符合安全检测条件，则会自动放开控制。

## 典型应用

【网络隔离】
- 建立企业内部的网络区隔，如设置为财务部与研发部的计算机不能互访。

【异常检测】
- 可检测客户端在各计算机运行是否正常，及时发现客户端被非法卸载的情况。

【控制下载】
- 可通过禁止下载端口，让客户端计算机无法使用FTP/Http下载。

【禁止非法网络应用】
- 通过禁止迅雷等P2P下载软件的网络通讯，防止其占用大量网络带宽。

## 产品优势

- 可以控制企业内部每台计算机之间的网络通讯。
- 可自定义安全检测条件，对不满足健康状态的计算机执行网络通讯控制。
- 网络通讯控制功能支持Mac OS/Linux操作系统。

## 常用组合

网络控制+文档操作管控+移动存储管控，防止非法通信盗取重要信息。

# IP-guard
## 网络流量管控

IP-guard网络流量管控模块通过对企业中流量使用情况进行分析，可以及时发现网络滥用问题，合理分配带宽。

## 功能详解

【流量统计】
根据端口、IP地址、流量方向等参数统计计算机或计算机组的流量，并以图表形式输出统计结果，随时了解流量的使用情况。
【流量控制】
根据端口、IP地址、流量方向等参数限制计算机或计算机组的网络流量，合理分配流量，保证关键业务的正常进行。

## 典型应用

【流量优化】
- 分析各项流量使用情况，发现企业是否存在网络滥用问题，对占用网络资源大的计算机的网速进行控制，合理分配企业的网络资源。
- 通过对网络流量的统计，发现占用网络资源的计算机，防止内部网络堵塞。

## 产品优势

- 可根据端口、IP地址、方向等参数分时段限制计算机的网络流量。
- 可控制企业内部任何一台计算机的网络流量。
- 可根据端口与IP地址等参数统计计算机的网络流量。
- 支持以图表形式多维度输出统计结果。

## 常用组合

网络流量控制+应用程序管控+网页浏览管控等模块组合，可对桌面行为进行严格的管控。

# IP-guard
## 屏幕监视

IP-guard屏幕监视模块可以实时查看用户的桌面行为并记录屏幕画面，掌握企业内部真实的工作状态。

## 功能详解

【屏幕查看】
可实时查看一台或一组计算机的屏幕画面，了解用户的工作状态。可根据日志记录直接定位到某时点的屏幕历史，方便快捷。
【屏幕记录】
记录计算机屏幕画面，便于随时查看，记录频率可以自由设定。
【特殊记录】
对指定应用程序进行屏幕记录，只有当指定程序运行时，才进行屏幕记录，保护信息安全的同时，节省数据量。
【触发式屏幕记录】
支持对敏感行为发生时进行屏幕记录，支持的行为包括运行程序、滥用网络流量、浏览网页、网络控制、发送邮件、IM传送文件、网页上传文件、文档访问、修改、移动、复制、删除等，文档打印、敏感内容识别外传、敏感内容识别落地等等。

## 典型应用

【实时监控】
- 管理者可以实时查看客户端的屏幕情况。

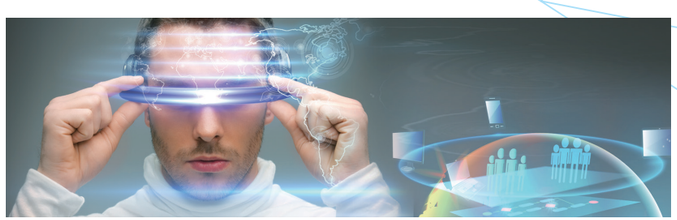
【屏幕历史审计】
- 对重要的程序的使用进行监控，例如财务软件开启的时候进行记录。
- 当审计日志时如发现异常操作，可定位于当时的屏幕记录。
- 发生泄密事件，可翻查屏幕历史，作为追查的证据。

## 产品优势

- 采用增量记录、变频、压缩等技术，保证屏幕记录数据量偏小。
- 对特定的程序进行记录，并且支持自定义记录频率。
- 支持对多显示器的工作站进行屏幕监控与记录。
- 可对终端服务器的客户端进行屏幕记录。
- 可将屏幕历史转换为通用视频格式进行播放。
- 支持Mac OS/Linux操作系统。

## 常用组合

屏幕监视+文档操作管控+网页浏览管控+应用程序管控+文档打印管控等模块组合，实现与日志的同步记录，随时翻查日志记录时的屏幕历史。



# IP-guard
## 资产管理

IP-guard资产管理模块，帮助管理员随时监测和查看各种IT资产及其变动情况，输出资产报表，集中地管理IT资产，防止资产流失。

## 功能详解

【资产管理】
自动扫描监测客户端计算机软硬件IT资产及其变动情况，支持自定义的资产查询和统计及对非IT资产的自定义管理，了解计算机软硬件及其它资产的使用及变更情况。
【版权管理】
对客户端计算机安装的软件进行统计和分类，记录软件采购，统计付费软件的授权使用情况。
【补丁管理】
扫描检测计算机的微软补丁安装情况并集中下载最新补丁分发到各计算机进行安装，防范系统威胁。
【软件卸载】
支持对软件进行强制、批量卸载，支持对任务执行时间段进行设置。

## 典型应用

【资产和版权管理】
- 提供清晰的资产报表，了解IT资产在网内的部署防止发生资产盗窃行为。
- 查看已经购买的Office、ERP等需正版授权的软件License总数和已使用数，获取软件部署情况。
- 集中对违规软件的统一卸载，协助管理员对终端软件安装进行合规管理。

【补丁管理和软件分发】
- 及时为网内所有计算机同步安装最新微软补丁，防范冲击波、已知漏洞等系统威胁。
- 集中部署ERP、Office等软件到客户端计算机，或集中运行脚本程序，提升软件部署效率。

## 产品优势

- 对软硬件资产及变更情况自动收集，支持自定义“保修期”等无法自动获取的资产属性。
- 可以自定义软硬件资产的统计报表。
- 自动收集计算机的补丁，并可集中管理。
- 支持软件分发，可集中部署也可以指定范围部署。
- 支持对打印机、路由器等非IT资产进行自定义管理。
- 资产管理实时化、可视化。

## 常用组合

资产管理+远程维护模块组合，实现系统运维方案，降低系统管理员的工作量，使其拥有更高的工作效率。

# IP-guard
## 远程维护

IP-guard远程维护模块可以帮助管理者为客户端计算机提供远程技术支持，快速响应系统故障。

## 功能详解

【远程信息查看与维护】

1、在控制台上实时查看客户端计算机的运行状态，包括应用程序、系统服务、磁盘及共享文件夹等信息。

2、支持直接对上述信息进行相关操作，如结束进程等。

【远程控制】

远程连接到远端计算机的桌面，并直接对计算机进行操作或示范。

【远程文件传送】

支持管理机与受控计算机之间传送文件，支持断点续传。

【软件管理】

1、在控制台可查看客户端计算机安装的所有软件信息。

2、可远程卸载客户端计算机上安装的软件。

## 典型应用

【远程运维】

- 管理员在控制台远程查看受控计算机基本信息及运行状态，分析故障原因并进行相关维护操作。
- IT管理员直接操作客户端计算机快速排除故障或进行操作演示。
- IT管理员从客户端收集故障样本，或分发文件到客户端计算机。

【软件管理】

- 管理员在控制台远程查看受控计算机安装的软件的信息，并可以卸载非工作需要的软件。

## 产品优势

- 可实时查看客户端计算机的运行状态信息。
- 对计算机进行远程控制，及时解决客户端故障。

## 常用组合

远程维护+资产管理，实现高效率的系统运维。

# IP-guard
## 风险审计报表

IP-guard风险审计报表能多维度地统计用户行为，从宏观角度发现用户行为变化趋势，并通过预先设置行为阈值，及时发现潜在的安全风险。

## 功能详解

【统计表 有效统计用户行为】

基于IP-guard强大的审计日志，可以对用户的打印、电子邮件、移动存储、文档操作、应用程序、上网浏览、即时通讯等行为进行报表统计，快速掌握内网计算机运行情况。

【趋势表 直观展现行为变化】

通过统计用户行为，可以直观展现某段时间内用户行为的变化趋势（如上网行为趋势是上升？还是下降？），并可为管理者后续完善管控策略提供直观的依据。

【征兆表 及时预警潜在风险】

对打印、电子邮件、移动存储、文档操作、应用程序、上网浏览、即时通讯等行为，管理员可预先设置征兆阈值和报警级别（如文档打印，可设征兆阈值：打印次数≥10次，报警级别=严重），当用户行为达到设置的阈值时，报表系统会自动产生、统计相应的征兆事件，并启动报警。

【私人报表 个性订制】

可根据企业内部需要，自定义报表统计条件，获取个性化的私人订制报表。

【周期报表 自动生成发送】

可设定时间周期（年、季度、月、周或自定义），自动生成周期报表，并可以通过邮件订阅，将周期报表定时发送给相关人员。

## 产品优势

- **多样化：**支持详尽的统计报表、清晰的趋势报表、针对性的征兆报表，以及个性化的私人订制报表。
- **智能化：**支持自动生成周期报表，并且提供邮件自动订阅功能。
- **简单易用：**安装方便快捷，操作界面友好，使用简单明了。
- **传播灵活：**报表支持打印、导出及邮件自动订阅。

## 常用组合

风险审计报表+文档操作管控+网页浏览管控+应用程序管控+文档打印管控等模块组合，可视化内网安全。

# IP-guard
## 文档云备份

IP-guard文档云备份模块能够帮助企业管理者对终端计算机上的文档进行集中存储和管理，解决企业文档管理难、容易损坏和丢失的难题。

## 功能详解

【自动备份】
1、强制对终端文档进行备份。
2、支持对终端文档进行即时备份、定时备份和全盘扫描备份。
【云存储机制】
1、支持文档存储容量的无限扩充。
2、支持依据文档的类型、大小等条件进行备份，支持通过判断文档的内容和大小，防止重复备份，减少存储冗余。
【版本管理】
支持保留一个文档多个备份版本，有利于追溯历史备份文件。
【文档检索和恢复】
1、终端用户可在线检索自己的备份文档。
2、可将备份文档下载到终端电脑。
【磁盘空间管理】
1、磁盘空间剩余量达到阈值时，支持发送警报和停止备份的措施。
2、当磁盘空间容量小于设定的阈值时，可执行自动清理的措施。

## 典型应用

【恢复丢失的文件】
- 用户误删除文件，或硬盘损坏，导致文件无法找回，可从文档云备份服务器将文件恢复到终端。
- 终端文件被病毒破坏或被勒索病毒加密，导致文件无法再使用，可将正常的文件从文档云备份服务器恢复到终端。

【文档快速检索】
- 文档云备份服务器聚集所有用户的文件，可以通过检索快速查找到所需的文件，实现快速的查询和分享。

## 产品优势

- 实现对文档的统一管理，降低企业文档面临丢失、删除和破坏等风险。
- 支持文档快速检索，有效帮助用户快速、准确地从海量文档中快速定位目标文档。
- 可直观查看用户备份的文件。

## 常用组合

基本功能+文档云备份+文档操作管控+文档打印管控，保障企业内文档安全。

# IP-guard
## 基本功能（必选）

IP-guard基本功能模块提供集中的终端管理平台架构，简化大量重复性的基础管理工作，帮助总揽终端全局。

## 功能详解

【信息查询】
可查询客户端计算机的基本信息和策略总览，随时掌握了解客户端计算机基本信息。
【基本控制】
能够在控制端对网内任意客户端计算机进行锁定、关闭、重启、注销和发送通知信息等，发现不安全行为时，可及时采取措施进行制止。
【系统策略设置】
设置客户端计算机的控制面板、网络属性、系统还原等配置工具的操作权限，如有违规变动，可以报警并警告。
【日志记录】
记录客户端计算机在执行策略时的操作日志，便于进行安全审查。
【实时报警与阻断】
当非法的文档操作行为发生时，在控制台即时弹出气泡告知管理员，以便及时阻断非法操作行为甚至锁定计算机。
【安全检测的检测功能】
检查客户端的状态是否与控制台设置的检测条件相符，检测内容包括：杀毒软件使用、补丁、软件安装、系统服务状态和其他条件（注册表等）。

## 典型应用

【限制视听功能】
- 工作时间通过ActiveX控件限制在线视听、游戏等无关应用。

【系统实时报警】
- 当发生硬件异动，存储设备和通讯设备插拔，软件安装卸载，系统信息和网络配置变化时，发出实时警报。

【节省电力】
- 管理员可设置定时关机策略，节省IT能源。

## 产品优势

- 支持角色管理，支持与AD域同步，支持与第三方用户系统同步。
- 支持终端服务器模式和无盘启动模式。
- 支持绑定IP/MAC地址，防范ARP攻击。
- 可按用户或计算机两种方式进行权限管理。
- 细致的管理员权限划分和部门管理。
- 支持多国语言。

## 常用组合

基本功能模块为购买其他模块的必选模块。

# IP-guard 安全网关

安全网关是一款专业的保护服务器数据安全的硬件系统，通过对访问服务器的计算机进行安全控制，实现服务器数据下载强制加密，防止服务器机密外泄。

## 功能详解

【服务器文档上传解密下载加密】

安全网关结合IP-guard加密客户端，对服务器重要数据进行保护。

1、服务器文档下载加密：服务器数据下载到本地都将自动强制加密，防止服务器数据下载外泄。

2、加密文档上传解密：终端上的文档上传到服务器时自动解密，服务器以明文存储所有文档，确保服务器上文档的安全。

【杜绝非法访问服务器】

杜绝非法计算机和非法进程对服务器进行访问，有效保障服务器的安全。

## 产品优势

【部署简便】

- 无需改变服务器配置和终端用户操作习惯。
- 无需增加或升级网络设备和改变原有网络结构。
- 支持串接和旁路部署方式。

【支持多种服务器类型】

- 支持企业常用信息管理系统OA、PLM、SVN、ERP等。
- 支持网络共享服务器。
- 支持B/S、C/S两种服务器访问方式。
- 支持http/https协议的附件加解密。

【终端系统支持】

- 支持Windows全系列，Mac OS，Linux，Android和iOS操作系统。

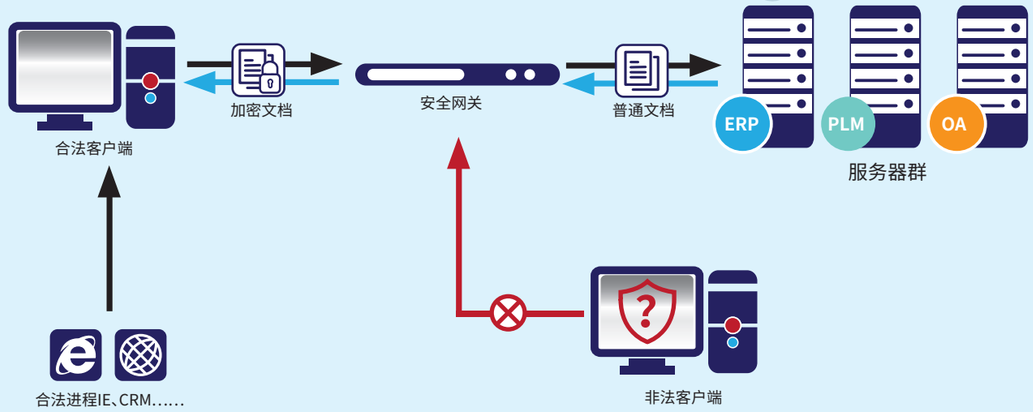
## 典型应用

【有效防范内部应用系统文档外泄】

¤ 为了避免加密的数据对原有的OA、ERP等服务器系统造成影响，安全网关确保上传到服务器的文档以明文存储。同时对服务器下载的文档强制加密，防止服务器文档下载泄密。

【安全便捷实现部门间数据共享】

¤ 部署了加密的部门将加密文档通过安全网关，上传至共享文件夹时，加密文档自动解密为明文，确保未部署加密的其他部门正常使用。当部署了加密的部门员工下载共享文件夹上的文档时，文档将自动加密，防止文档泄密。




## 系统型号和参数

| 安全网关系统 | IPG-1600S | IPG-2600S | IPG-3400S | IPG-3600S | IPG-4400S | IPG-4800S | IPG-5X00S |
|---|---|---|---|---|---|---|---|
| 适用范围 | 小型企业 | 小型企业 | 中小型企业 | 中型企业 | 大中型企业 | 大中型企业 | 大型企业 |
| 参考用户数 | <30 | <100 | <300 | <600 | <1000 | <2000 | <5000 |
| 标准接口 | 准千兆电口 | 千兆电口 | 千兆电口* | 千兆电口* | 千兆电口* | 千兆电口* | 千兆电口* |
| 支持Bypass | | Y | Y | Y | Y | Y | Y |

＊备注：3400S以上系列支持扩展卡，可扩展千兆光口、千兆电口、万兆光口、bypass等。

## 常用组合

安全网关+文档加密+基本功能，为客户提供低成本、高回报的加密解决方案。

# IP-guard 准入网关

IP-guard准入网关，通过对访问指定网络设备的计算机进行身份验证，有效防止非法计算机对指定网络设备进行非法访问，并可避免内网计算机脱离IP-guard管控。

## 功能详解

【网络访问 准入控制】

计算机接入企业内部网络对服务器、互联网等访问时，需经过准入网关严格的审核，只有合法的计算机才能连入访问，非法计算机可根据需要将其引导至隔离区进行修复，或者完全阻断其访问。

【安全状态 合规检查】

对通过准入网关连入网络的PC进行安全状态合规检查（如：是否安装指定软件、杀毒软件，病毒库、系统补丁是否更新等），满足条件则允许接入网络，否则拒绝访问并发出警告提示，并强制跳转至隔离区进行相关修复。

【外来访客 账号登录】

对于临时来访的外来PC，因工作需要接入企业内部网络时，可以设定访客账户，通过WEB浏览器输入账号密码进行身份认证，通过后方可连入网络。

支持设置访客账号禁止访问的IP地址或IP地址段，防止访客PC随意访问内部敏感资源。

管理员可以对访客账户的访问时间、登陆IP、登录注销等进行日志审计。

【防止内部PC脱离管控】

可以有效防止内部PC通过重装系统、安装多系统、虚拟机等方式脱离管控，保证终端安全策略可以有效的执行。

【状态信息】

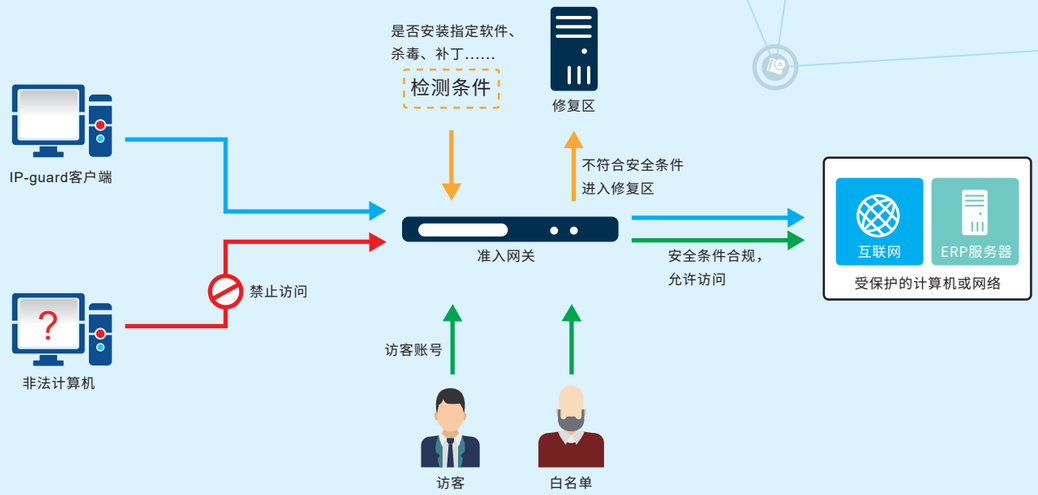
支持显示准入网关的实时流量和时间段内的流量信息，支持统计CPU、内存和磁盘的使用率。

## 典型应用

- 置于服务器集群之前，防止非法计算机访问重要服务器。
- 置于互联网出口之前，阻断未安装客户端的计算机访问互联网，预防用户私自重装系统。
- 结合IP-guard网络控制模块，禁止外来计算机对内网计算机的非法访问，保护内部网络计算机的安全。

## 产品优势

- 极其便捷的安装方式：支持串接、旁路两种模式，无需改变企业网络环境。
- 多种认证方式：授权、信任、白名单、例外地址等，适合企业不同的管理需求。
- 容灾能力强：具备ByPass功能，确保企业网络高效稳定。




## 系统型号和参数

| 准入网关系统 | IPG-1500F | IPG-2500F | IPG-3300F | IPG-3500F | IPG-4300F | IPG-4500F | IPG-5X00F |
|---|---|---|---|---|---|---|---|
| 适用范围 | 小型企业 | 中小型企业 | 中型企业 | 大中型企业 | 大中型企业 | 大型企业 | 大型企业 |
| 参考用户数 | <100 | <300 | <600 | <1000 | <2000 | <5000 | <10000 |
| 标准接口 | 准千兆电口 | 千兆电口 | 千兆电口* | 千兆电口* | 千兆电口* | 千兆电口* | 千兆电口* |
| 支持Bypass | | Y | Y | Y | Y | Y | Y |

＊备注：3300F以上系列支持扩展卡，可扩展千兆光口、千兆电口、万兆光口、bypass等。

## 常用组合

准入网关+网络控制+应用程序管控+资产管理，实现准入条件检测和更加完善的准入功能。

# IP-guard 安全U盘

IP-guard安全U盘凭借安全的身份鉴别机制，灵活的分区管理，完善的生命周期管理，为企业内外部文件流通保驾护航，让U盘传输数据再无后顾之忧！

## 功能详解

【密码保护U盘读写】
安全U盘具有多重密码安全保护方案，在外部使用时，需要先通过密码认证，方可使用安全U盘。

【详尽记录U盘操作】
安全U盘无论是在公司内部使用，还是在公司外部使用，都会详细地记录U盘的使用和U盘文档的所有操作。管理员可以对U盘使用进行可视化管理。

【有效防范木马病毒】
安全U盘通过专用资源管理器进行访问操作，禁止其他程序直接访问，有效防止木马病毒。

【内外分区确保安全】
安全U盘通过保密区和交互区进行存放数据。保密区只允许在公司安全客户端的机器上使用，外部不显示；交互区可以在公司内部和公司外部使用，使用时需要通过专用资源管理器进行访问，并且需要通过密码认证，即使U盘丢失，数据也无法被他人窃取。

【有效防止U盘格式化】
安全U盘通过硬件芯片级保护，禁止非授权的格式化操作，保证U盘的安全性和可靠性。

## 典型应用

【分区管理 灵活使用】
- 内部文档在公司内需要通过U盘流转时，可以使用安全U盘的保密区，保密区在公司外部无法访问。
- 公司文档对外流通时，可以使用安全U盘的交互区进行交互。

【有效防止U盘丢失导致泄密】
- 安全U盘在外使用时，需要通过专用资源管理器访问交互区数据，并且要输入密码认证，因此即使U盘无意丢失，捡到的人员也无法查看U盘上的文件，确保数据安全。

## 产品优势

- 分区管理，保密区内部使用，外部机器无法查看；交互区内外都可用。满足企业对U盘多样化的需求。
- 独创U盘全方位日志审计，无论是在公司内部还是外部，都可以完整记录U盘的使用情况和U盘内文档操作情况。
- 专用资源管理器、强制密码验证和芯片级防格式化，多管齐下保证U盘数据的安全。

## 常用组合

安全U盘+文档操作管控，实现对文档流转全过程的审计。

# SOLUTIONS 常用解决方案

02 终端安全解决方案

03 移动存储管理解决方案

01 信息防泄露整体解决方案

04 资产管理解决方案

05 终端文档云备份解决方案

# IP-guard信息防泄露整体解决方案

## 保护商业机密

IP-guard信息防泄露整体解决方案基于统一平台，以审计洞察业务流程和安全风险，以丰富的权限控制功能降低网络、外设、文档流转等多种渠道的泄密风险，必要时应用透明加密加固保密体系。通过整合运用“强力审计-权限控制-透明加密”三种强力技术，形成层次分明、轻重有别、易于调整的整体防御体系。

| 您是否担心： | IP-guard帮您解决： |
| --- | --- |
| 重要文档被随意浏览，并恶意篡改、删除等，却无法有效监测。 | 对文档进行全生命周期的操作审计，包括创建、访问、修改、复制、删除等，及时发现危险性操作，在文档被修改或删除时，可设置自动备份，防止有意无意的敏感操作造成损失。 |
| QQ、Email、网络共享等网络渠道不受控制，公司内部信息被随意外泄。 | 对即时通讯、电子邮件、网络上传等行为进行详细审计及管控，有效威慑泄密行为，并能提供泄密证据。 |
| U盘、移动硬盘、打印机、刻录机等外部设备泛滥，信息安全无保障。 | 对打印机、移动存储等设备使用进行详细的审计及设置细致而严格的控制策略，防止敏感信息被随意外泄。 |
| 重要文档被非法带离企业。 | 对核心机密进行高强度的透明加密，确保机密信息随时随地都处于加密状态，即使被带离企业也无法被打开使用。 |
| 外发的重要文档遭遇接收方泄密。 | 把机密文档设置为外发格式，指定外发文档的使用权限，防止重要信息被二次泄露。 |
| 包含敏感信息的文档泄露出去。 | 对包含敏感信息的文档进行加密，在文档外传时，对敏感内容进行检测，并实施具有针对性的控制和审计措施。 |
| ERP等服务器被非法访问，其上机密亦被顺手牵羊。 | 对访问服务器的终端进行严格的身份认证，防止非法访问带来的风险，同时防止下载到本地的文档被二次泄密。 |

### 方案优势：

**★ 基于整体防泄露理念，综合运用审计、权限控制、加密三大防泄密技术。**

**★ 通过文档敏感内容识别技术，精准识别高价值文档，综合实施保护措施。**

**★ 丰富的控制策略，提供灵活可控的防护，真正实现精细化管理。**

**★ 统一平台集中管理，极大提高了IT管理效率。**

**★ 可视化的行为审计，效果直观。**

推荐模块：

基本功能　文档加密　安全网关　文档操作管控　敏感内容识别　移动存储管控
设备管控　邮件管控　网络控制　文档打印管控　即时通讯管控　应用程序管控
准入网关　屏幕监视　安全U盘　网页浏览管控　网络流量管控　风险审计报表

# IP-guard终端安全解决方案

## 提高工作效率

凭借优异的统计分析能力，IP-guard让企业管理者对内部的工作情况了如指掌，灵活的控制策略还能够帮助企业实现人性化管理，限制与工作无益的行为，帮助企业职员专注于本职工作，提高工作效率。

| 您是否担心： | IP-guard帮您解决： |
| --- | --- |
| 上班时间炒股、打游戏、使用与工作无关的应用程序，影响工作效率。 | 限制用户在工作时间使用与工作无关的应用程序，休息时间可适当放开。 |
| 玩网络游戏、浏览与工作无关的网站、进行与工作无关的网络聊天。 | 控制对终端用户访问的网站、允许使用的网络应用程序。 |
| 疯狂下载电影、歌曲、程序，在线看网络电影、听音乐，滥用内部网络带宽。 | 对终端用户使用的网络带宽和网络流量进行合理分配。 |
| 无意或有意访问到黄色、反政府等非法网站，造成病毒、木马泛滥。 | 禁止一切黄色、反动、挂马等非法网站，降低内部遭受病毒、木马入侵的风险。 |
| 缺乏对员工上网、桌面行为的了解，无法掌握员工的业绩和工作状态。 | 提供清晰的应用程序和访问网站记录的统计报表，掌握内部的操作动态。 |

### 方案优势：

**★ 一目了然的统计报表，掌握内部行为**

IP-guard提供直观清晰的统计报表，方便企业管理者详细掌握内部行为。

**★ 分时段内容过滤，劳逸结合**

IP-guard分时段管理不同类型的网站，令用户在工作时专心工作，休息时尽情娱乐。

**★ 实时智能警告，人性化管理**

IP-guard对执行非法操作的用户发送实时警告，提醒用户注意，人性化的管理令用户倍感尊重和自由，符合现代企业管理要求。

推荐模块：

基本功能　设备管控　远程维护　文档操作管控　敏感内容识别　移动存储管控
邮件管控　网络控制　准入网关　即时通讯管控　文档打印管控　网页浏览管控
屏幕监视　资产管理　安全U盘　应用程序管控　网络流量管控　风险审计报表

# IP-guard移动存储管理解决方案

## 确保设备安全使用，防止机密泄露

IP-guard可以对各种移动存储设备进行集中管理，帮助企业使设备使用更加规范，遏制外来病毒入侵，防止内部重要信息泄露。

| 您是否担心： | IP-guard帮您解决： |
| --- | --- |
| U盘丢失，导致内部机密泄露。 | 将普通U盘格式化为加密盘，该加密盘只能在内部使用，即使丢失，外部人员捡到也无法正常使用。 |
| 外部手机、数码相机等随意接入，盗取重要资料。 | 禁止USB移动存储、蓝牙、红外、光盘刻录及任何新设备，有效防止移动设备泄密。 |
| U盘泛滥，病毒感染屡禁不止。 | 限制首次接入的移动存储设备自动播放，防止病毒扩散至企业内网。 |
| 财务部、设计部、开发部的重要文档通过U盘随意流传到其他部门。 | 限制各部门U盘的使用范围，只能在企业授权允许的区域内使用。 |
| 个人U盘内外混换使用，暗含丢失、损坏、格式化、资料外泄风险，且不便于管理。 | 安全U盘满足内外不同场景，无法被非法格式化，保证盘中数据完整性，全面记录文件操作记录，发现潜在风险。 |

### 方案优势：

**★ 管控全面**

IP-guard可管控USB设备、蓝牙、红外、光盘刻录、移动硬盘、智能手机以及其它一切新设备。

**★ 细粒度控制**

对外来设备、公司不同部门的设备以及公司内不同授权的设备进行管理，满足多样化的需求。

**★ 分类管理**

对内网所有移动存储设备进行分类，管理者可以按照类别来设定使用权限，让管理更便捷、轻松。

**★ 详尽的审计**

IP-guard详细记录接入网内的移动存储设备的相关信息与插拔使用记录，方便审计使用情况。

推荐模块：

基本功能　文档操作管控　敏感内容识别　移动存储管控
设备管控　文档打印管控　风险审计报表　安全U盘

# IP-guard资产管理解决方案

## 化繁为简，省时省力又省心

IP-guard拥有出众的集中管理能力，通过单一控制台就能够对成百上千台计算机进行有效的管理和维护，保证系统时刻运行顺畅，支持业务顺利开展。

| 您是否担心： | IP-guard帮您解决： |
| --- | --- |
| 单位的PC数量越来越多，无法集中管理，一旦大规模出现问题，影响效率的同时还危及企业信息安全。 | 通过单一控制台，对内网PC进行统一管理，通过远程支持，集中管理和控制内部所有计算机。 |
| 计算机软、硬件数量无法确实掌握，盘点困难。 | 自动统计企业内部的IT资产，同时及时更新软硬件变动情况。 |
| 硬件设备私下挪用、窃取，造成财产损失。 | 对异常的软件、硬件变化进行及时报警，提高 IT 管理的准确性、及时性和自动化水平。 |
| 无法及时更新微软的补丁，造成内部漏洞越来越多，安全风险大。 | 自动检测PC的补丁安全情况，根据需要及时更新。 |
| 软件单机安装浪费人力，应用软件版本不易控制。 | 支持程序分发、程序修复、文件分发，方便网内计算机进行软件部署。 |

### 方案优势：

**★ 集中化**

通过IP-guard单一控制台即可对内部庞大计算机进行集中维护。

**★ 简易化**

IP-guard自动统计IT资产信息并以列表形式显示，大力节省人力物力。

**★ 智能化**

自动发现新增计算机软硬件的变动情况，确保随时掌握最新IT资产情况，省力更省心。

**★ 清晰化**

管理员只需点击IP-guard控制台的相应界面，所有资产信息均会以分类的形式清楚地呈现眼前。

推荐模块：

基本功能　资产管理　远程维护　风险审计报表

# IP-guard终端文档云备份解决方案

## 备份终端文件，保证文档安全

IP-guard支持将终端的文件上传到文档云备份服务器，进行集中存储和管理，帮助企业更好保护文档，防止终端文档丢失而无法找回。

| 您是否担心： | IP-guard帮您解决： |
| --- | --- |
| 计算机硬盘损坏，电脑丢失，导致机密文件丢失泄密。 | 对终端计算机上的数据进行备份，统一上传到文档云备份服务器，进行集中存储和管理。 |
| 员工离职时，恶意删除计算机上的文件。 | 文档云备份服务器和终端的备份目录相同，终端文件一旦遭到破坏或者遗失，可从文档云备份服务器快速恢复，使数据得到还原，并且目录和原来保持一致。 |
| 员工计算机上的文件感染勒索病毒或其他病毒，文件遭到破坏，无法还原。 | 管理员可以从文档云备份服务器上快速检索到所需文件，实现快速查找和分享。 |
| 重装操作系统时不小心格式化数据盘，计算机磁盘损坏，无法恢复文件。 | 通过定时备份和实时备份，保证文档云备份服务器始终保存终端最新的文档，一旦终端数据出现风险，可将损失降到最低。 |

### 方案优势：

**★ 集中存储**

企业所有终端计算机上的数据，都可以全部备份到同一台文档云备份服务器上，便于集中存储和管理。

**★ 备份及时**

终端软件对数据进行自动监控，一旦检测到终端数据有变化，便实时、准确的备份到文档云备份服务器中，数据安全性更高。

**★ 快速恢复**

终端数据出现损坏，可从文档云备份服务器恢复，找回误删或者损坏前的数据。通过恢复保证数据的完整性。

推荐模块：

基本功能　文档操作管控　文档云备份

## 建议解决方案与产品选择

| 产品 | 模块 | 推荐解决方案 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| | | 信息防泄露整体方案 | 终端安全管理方案 | 移动存储管理方案 | 上网行为管理方案 | 文档加密方案 | 资产管理方案 | 终端文档云备份方案 |
| IP-guard文档加密系统 | 文档加密 | √ | | | | √ | | |
| IP-guard敏感内容识别系统 | | √ | √ | √ | √ | √ | | |
| IP-guard终端安全管理系统 | 文档操作管控 | √ | √ | √ | | | | √ |
| | 移动存储管控 | √ | √ | √ | | | | |
| | 设备管控 | √ | √ | √ | | | | |
| | 文档打印管控 | √ | √ | √ | | | | |
| | 即时通讯管控 | √ | √ | | √ | | | |
| | 邮件管控 | √ | √ | | √ | | | |
| | 应用程序管控 | √ | √ | | √ | | | |
| | 网页浏览管控 | √ | √ | | √ | | | |
| | 网络控制 | √ | √ | | √ | | | |
| | 网络流量管控 | √ | √ | | √ | | | |
| | 屏幕监视 | √ | √ | | √ | | | |
| | 资产管理 | | √ | | | | √ | |
| | 远程维护 | | √ | | | | √ | |
| | 风险审计报表 | √ | √ | √ | √ | √ | | |
| | 文档云备份 | | | | | | | √ |
| | 基本功能（必选） | √ | √ | √ | √ | √ | √ | √ |
| IP-guard安全网关 | | √ | | | | √ | | |
| IP-guard准入网关 | | √ | √ | | √ | √ | | |
| IP-guard安全U盘 | | √ | √ | √ | | | | |

# IP-guard系统架构

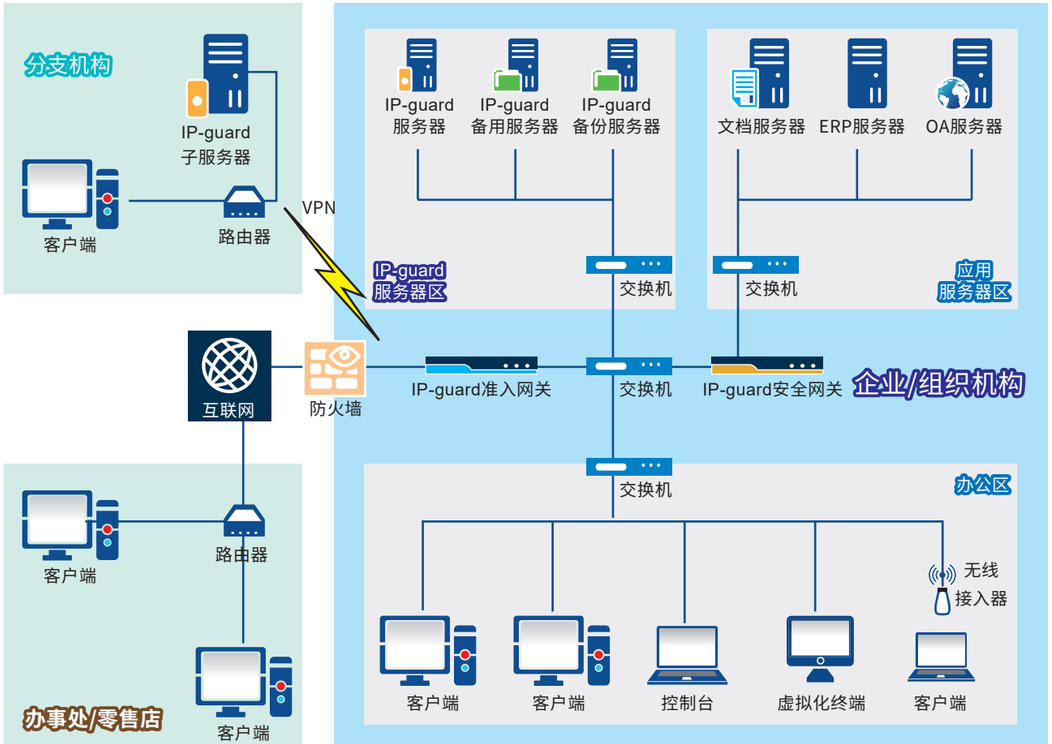
IP-guard基于TCP/IP协议的网络架构，可以灵活地从本地网络扩展到远程网络和异地网络。远程的计算机可以通过虚拟专用网（VPN）或互联网连接到服务器，实现大规模复杂网络的集中管理。控制台也可以通过互联网等方式连接到异地的服务器，实现对分支机构的远程监控。

IP-guard系统由三个部分组成：客户端、服务器和控制台。

**服务器**安装在系统内的一部高性能的计算机上，存储系统的管理策略和客户端采集的数据，向客户端计算机传递管理规则和指令。服务器是系统的管理核心。

**控制台**安装在管理者的计算机上。管理者通过控制台设置管理策略，查看日志和各类统计数据。

**客户端**程序安装在每一台被管理的计算机上。执行管理者设定的各种管理策略，采集计算机运行的各项数据并传送至服务器。




# 优秀的系统性能

| | |
|---|---|
| 高安全性的系统 | |
| | 客户端与服务器的通讯采用高强度的AES加密算法，有效保护通讯的数据不被窃取和伪造。 |
| | |
| | 所有的管理员操作都会记录在系统审计日志中，管理员的操作行为可以得到详细的审计。 |
| 高效率的系统 | |
| | 应用先进的通讯数据压缩技术，数据通讯效率更出众。 |
| | |
| | 具备优异的按天存储机制，处理海量数据更方便、更快速；每天数十G的数据存储也能够轻松应对。 |
| | |
| | 客户端运行时仅占用较小的计算机资源，平均CPU消耗<1%，平均占用内存< 25M。 |
| | |

# 全面的系统支持

| | 操作系统 |
|---|---|
| 客户端 | Win 2000以上各32/64位Windows版本<br>Mac OS X 10.6以上64位系统<br>Linux Ubuntu/CentOS/Fedora/Redhat/Debian等各系列32位/64位系统 |
| 服务器 | Win 2000以上各32/64位Windows版本 |
| 控制台 | Win 2000以上各32/64位Windows版本 |
| 移动智能APP | Android 4.0及以上<br>iOS 6.0及以上 |

# 溢信科技

## 极富创新力的终端安全管理解决方案提供商

广州市溢信科技股份有限公司（以下简称“溢信科技”），始创于2001年7月，是中国较早从事终端安全领域的企业之一，创立之后一直专注于终端安全领域的发展和创新，已成为行业优秀的终端安全整体解决方案提供商，并于2017年在新三板成功挂牌上市。（证券代码：870985）

溢信科技经过十多年的技术研发及经验积累，掌握了文档操作监控、网络驱动、系统调用劫持、虚拟磁盘保护、智能缓冲、沙箱隔离等核心技术，公司及子公司（广州全安软件有限公司）拥有61项计算机软件著作权，并以此为基础致力于为用户提供包括信息防泄露、行为管理、网络审计及资产运维管理等丰富功能在内的一体化终端安全整体解决方案。

旗下自主研发的一体化终端安全管理系统IP-guard，凭借其完善的整体架构，灵活的扩展性，极佳的易用性和稳定性，获得包括奔驰汽车、华为终端、中国移动、香港廉政公署、佳能在内的超20,000余家客户的一致信赖。

## 专业技术团队，提供优质服务与技术支持！

溢信科技分支机构众多，在北京、上海、长沙、深圳设立分公司，在华南、华北、华东、华中、西南等各大区域都设有办事处。

专业的研发团队、咨询服务人员，实现咨询、定制方案、安装部署和解决技术问题一步到位；完善的服务和售后支持网络，为用户提供电话技术支持、故障排除、上门处理等各种服务，帮助客户获取更强的竞争力。

广州 深圳 珠海 北京 上海 长沙 重庆 成都

武汉 西安 郑州 济南 南京 杭州 厦门

行业标杆 一直信赖

| 电子光学 | 纺织服饰 | 互联网/游戏 |
|---|---|---|
| 欧姆龙 | 欧时力 | 途牛网 |
| 艾默生 | E·LAND | 唯品会 |
| 长江存储 | 宏珏时装 | 乐逗游戏 |
| 松下 | 江博士 | 东方博雅 |
| 索尼 | 博洋家纺 | 广州捷游 |
| 佳能 | 七匹狼 | 梦工厂 |
| 蓝思科技 | 波司登 | 墨麟科技 |
| 正晶光电 | 九牧王 | 软通动力 |
| 科沃斯机器人科技 | 海澜之家 | 广州菲音 |
| 保伦电子 | 美特斯·邦威 | 吉比特网络 |

| 机械/重工 | 医疗/卫生/药品 | 政府部门/事业单位 |
|---|---|---|
| 三一重工 | 中南大学湘雅二医院 | 湖南省财政厅 |
| 小松制作所 | 天津医科大学总医院 | 中国海事服务中心 |
| 特变电工 | 中山大学附属第三医院 | 重庆市地理信息中心 |
| 盾安集团 | 台北市联合医院 | 广州司法局 |
| 三菱电机 | 神威药业 | 上海航务管理署 |
| 中国重汽 | 新华制药 | 宁波市环保局 |
| 大洋电机 | 仁和药业 | 深圳市罗湖区国税局 |
| 沪东重机 | 老百姓大药房 | 重庆市勘测院 |
| 日立电梯 | 益丰大药房 | 常德市地方税务局 |
| 徐工集团 | 无限极（中国） | 苏州规划局 |

# 他们信赖IP-guard

| 日用/化工 | 数码/通讯 | 汽车/汽配 |
|---|---|---|
| 资生堂 | 华为终端 | 奔驰 |
| 大宝 | 中兴通讯 | 大众 |
| 相宜本草 | 小米集团 | 保时捷中国 |
| 珀莱雅 | OPPO | TOYOTA |
| 建霖家居 | VIVO | 普利司通 |
| 威露士 | 展讯通信 | 本田汽车 |
| 乐扣 | TPK | 长安汽车 |
| 贝亲 | 新普科技 | 长城汽车 |
| 联塑科技 | 瑞仪光电 | 北汽集团 |
| 玫龙纸业 | TCL集团 | 东风汽车 |

| 金融行业 | 科研/设计院 | 矿产/冶金 |
|---|---|---|
| 汇添富基金 | 中国航空动力控制 | 宝钢集团 |
| 长沙银行 | 国家测绘局大地测量数据处理中心 | 中国石化 |
| 中信银行 | 天津电力设计院 | 中钢集团 |
| 百年人寿 | 国家海洋局第二海洋研究所 | 中国神华 |
| 马上消费金融 | 北京市测绘设计 | 新余钢铁 |
| 博时基金 | 中国家用电器研究院 | 日本神钢 |
| 广东农信 | 中国电子集团38研究所 | 长庆油田 |
| 安联财产保险 | 上海市城市规划设计研究院 | 浦项制铁 |
| 中国国际期货 | 重庆市规划设计研究院 | 兖州煤业 |
| 上海汇付数据 | 广州机械科学研究院 | 海亮集团 |

| 能源/电力 | 家电/家居 | 食品/零售 |
|---|---|---|
| 广东电网 | 海尔 | 金龙鱼 |
| 葛洲坝集团 | 三菱空调 | 娃哈哈 |
| 宁德新能源科技 | 艾美特 | 伊利 |
| 阿尔斯通 | 万宝集团 | 屈臣氏 |
| 君正能源化工 | 小熊电器 | 周黑鸭食品 |
| 华能国际 | 大金空调 | 雪花啤酒 |
| 三洋能源 | 小鸭集团 | COSTA咖世家咖啡 |
| 亿纬锂能 | 松下家电（中国） | 益力多 |
| 顺特电气设备 | 罗浮宫家居集团 | 钱大妈 |
| 京瓷太阳能 | 生活家.巴洛克地板 | 拉法耶特百货 |