IP-guard 一体化终端安全管理系统

您是否担心企业内部机密被随意泄露出去？

您是否面临U盘、移动硬盘等外设使用混乱的终端安全管理问题？

您是否有提高企业工作效率、加强运维管理的需求？

终端安全专家IP-guard为您分忧！

IP-guard

专注终端安全 保护核心机密

IP-guard三维智能信息防泄露整体解决方案

保护商业机密，提高企业竞争力

企业信息泄露常见途径：

▶QQ、Email导致重要信息在网络上肆意流传
▶U盘、移动硬盘、打印机等外部设备泛滥，信息被随意传播
▶U盘、笔记本电脑丢失，其中机密随之泄露
▶重要文档被随意浏览，并恶意篡改、删除
▶外发重要文档遭遇接收方泄密
▶ERP等服务器被非法访问，机密亦被顺手牵羊
▶公司内部信息被非法上传到网盘

防止机密文档遭偷窥

对重要文档采用高强度透明加密，通过控制其打开、复制、打印、截屏等权限，随时随地保证机密安全；采取敏感内容识别技术，精准识别高价值文档，实施更准确保护。

防止重要信息被非法操作

控制用户对重要文档复制、修改与删除的权限，在修改或删除时可以自动备份，并通过审计详尽记录文档全生命周期的操作，杜绝非法操作造成企业损失。

防止文档上传网盘泄密

封锁网络上传的行为，防止非法上传重要文件到网页邮箱、网盘等网络服务器。

防止打印泄密

限制用户使用打印设备以及打印程序，并可在打印文件上添加水印，同时详尽记录每一次打印操作。

防止邮件泄密

通过限定收发件人、主题、附件名称及大小等，限制电子邮件发送，并详尽记录邮件来往的信息，杜绝不合规的邮件发送行为。

防止即时通讯泄密

限制文件（可指定类型或指定文件夹）和图片发送，同时完整记录所有IM聊天内容，降低泄密风险。

防止U盘丢失泄密

支持对U盘加密或对拷入U盘的文件自动加密，消除由于U盘被盗或者丢失导致的泄密风险。

支持对U盘接入进行控制，限制读写权限，使U盘的使用更规范。

可记录所有U盘的插拔和拷贝文件的详细情况，对U盘使用情况了然于心。

防止外设泄密

对企业内部U盘、移动硬盘、智能手机、上网卡、随身wifi等外设进行统一管控，禁止随意接入企业计算机，防止非法拷贝和非法外联。

防止未经允许的网络访问

防止内部计算机擅自脱离监管，对试图接入公司内网并访问受保护区域的计算机进行安全状态检查，只有通过检查后才能正常访问目标网络。

震慑拍照泄密行为

支持在计算机屏幕或应用程序上显示水印，有效震慑通过拍照、截屏、录屏泄密的行为。

文档流转追踪

支持在文档中加入显性、隐性水印，或在文档中加入流转标记，以追踪文档在终端的流通记录。

IP-guard一体化终端安全整体解决方案

提高工作效率 加速企业前进

企业行为管理常见问题：

- ▶上班时间炒股、玩游戏、网络闲聊、浏览无关网页，降低工作效率
- ▶疯狂下载电影、歌曲，在线看电影……滥用网络带宽
- ▶访问到黄色、反政府等网站，导致病毒、木马泛滥
- ▶滥用公司打印机，造成资源浪费

禁止访问与工作无关的网页

限制用户访问与工作无关的网页，可以通过设置网站分类，分时段管控用户的网页浏览行为，并通过审计清楚了解用户访问网站情况。

禁止无关工作的IM程序运行

禁止非工作相关的IM帐号登录，并详细记录IM聊天内容，防止闲聊。

禁止游戏、股票等与工作无关的程序运行

禁止在工作时间使用游戏、股票等应用程序，并阻止一切有安全风险的程序运行。

工作时间，禁止下载影音文件

工作时间禁止下载影音文件，并对企业中网络流量使用情况进行分析，及时发现流量滥用问题并进行有效限制，合理分配带宽，保证关键业务的正常带宽，让整体网络更加通畅。

限制软件安装和卸载

禁止员工安装与工作无关的应用程序，禁止卸载与工作相关的应用程序，确保终端应用程序的标准化。

统一的软件安装平台

支持管理员通过软件中心统一上架软件，员工可自行选择安装、升级或卸载软件，既方便运维人员管理软件，又方便用户获取软件。

防止浪费打印资源

灵活控制打印权限，防止无需打印的人员滥用打印资源，并详细审计每次打印操作，统计资源使用情况。

IP-guard资产管理解决方案

让管理化繁为简，省时省力又省心

企业运维管理常见困扰：

- ▶软硬件资产无法确实掌握，人工盘点耗时耗力
- ▶硬件设备被私下挪用、窃取，造成财产损失
- ▶无法及时更新补丁，内部漏洞不能及时修补
- ▶终端频频发生故障，维修工作应接不暇
- ▶管理员与用户交互困难，运维难度大

杜绝漏洞修复延迟

自动检测计算机的补丁安装情况，根据需要及时更新。

实时了解IT资产情况

自动统计企业内部的IT资产，及时更新软硬件变动情况。

统一管理所有终端

单一控制台统一管理内网计算机，集中对所有内部计算机进行远程维护。

及时发现资产异常

对异常的软、硬件变化及时报警，提高资产管理的准确性、及时性和自动化水平。

快速实现软件部署

支持通过控制台统一分发程序、分发文件和可执行文件，使软件派发和文件推送可以快速完成。

IP-guard敏感内容识别解决方案

高效识别敏感内容，精准化防泄密

企业防泄密常见难点：

- ▶无法准确发现和定位企业内部敏感文档的存放位置并加以保护
- ▶员工在工作中既需要对外信息交互，又要防止敏感内容泄露
- ▶员工不清楚文件是否为机密信息，导致无意间泄密
- ▶通过存储设备、网络盘、IM、邮件外传敏感内容，亟需进行更精准的管控

及时发现敏感内容

支持全盘扫描含敏感内容的文档，对发现的敏感文档进行加密保护或进行其他防泄密的处理措施。

针对敏感内容加密保护

从服务器下载或用户新建含敏感内容的文档时，可对含敏感内容的文档可进行加密保护，从源头保护机密数据安全。

敏感内容外传限制

通过存储设备、网络盘、IM、邮件外传文档时，可阻断含敏感内容文档的传输，不含敏感内容的文档可以正常传输。

审计敏感内容传播

记录通过存储设备、网络盘、IM、邮件外传含敏感内容的文档的行为，并可报警、警告和备份。

IP-guard远程办公解决方案

远程办公也安全，无惧任何场景

远程办公常见安全风险：

- ▶ 远程终端的安全基线偏低，容易给内网带来安全隐患
- ▶ 服务器的机密文档下载到远程终端的泄露风险
- ▶ 终端接入内网时权限过大，容易引发安全问题
- ▶ 用户随意外传机密文档而无法追溯
- ▶ 截屏或录屏导致文档内容泄露的风险

远程终端安全基线加固

当远程终端使用VPN接入企业内网时，VPN客户端可检测其是否安装了IP-guard客户端和杀毒软件，如果不符合要求可拒绝其接入内网，以此来强化远程终端的安全性。

文档加密保护

对从内网服务器下载到远程终端的文档自动加密保护，用户无法通过剪贴板、截屏、打印（包括虚拟打印）等方式窃取加密文档内容，未经授权其他人员无法打开加密文档，确保加密文档安全。

加强用户权限管控

对通过VPN接入内网的终端进行权限管控，包括外接设备、移动存储的使用权限、打印权限、文档外传权限等，严格规范用户的计算机行为；还可以通过屏幕水印有效震慑拍照、截屏泄密的行为。

全面审计终端行为

审计远程终端接入内网后的操作行为，包括对文档操作、网页访问、邮件收发、应用程序运行、外设接入、打印、屏幕等进行审计，帮助企业及时发现风险以及对泄密行为进行有效追溯。

水印震慑和追溯

支持在远程终端上启用文字、图片、二维码或点阵的屏幕水印，水印信息包括用户名、计算机名、IP/MAC地址和时间等信息，发生截屏或拍照泄密时，企业可根据水印信息追溯泄密者。

IP-guard水印追溯解决方案

文档流转可追溯，泄密者无所遁形

文件追溯常见问题

- ▶ 机密文档被截图、拍照、打印出去，却无法追溯泄密者
- ▶ 文档在哪些终端流转过？最终文档是通过谁的电脑发送出去的

防止打印泄密

限制用户使用打印机的权限，并可在打印文件上添加文字、图片、二维码或点阵水印，可通过纸质文件追溯泄密者。

震慑拍照泄密行为

支持在计算机屏幕或应用程序上显示水印，有效震慑通过拍照、截屏、录屏泄密的行为。

文档流转追踪

支持在文档中加入显性、隐性水印，或在文档中自动加入流转标记，以追踪文档在终端的流转情况。

产品功能模块详细介绍

产品	模块	功能介绍
文档加密系统		**【透明加密 】** √ 重要文档从生成即强制加密，强力守护信息资产 √ 在授权环境中，文档能自动解密，不影响用户原有使用习惯 √ 在非授权环境中，加密文档无法正常打开和使用，严防文档泄露 √ 在加密文档的使用过程中，能够防止用户通过剪贴板、截屏、打印（虚拟打印）等方式窃取加密文档内容 √ 免费提供对各种应用软件的加密支持 √ 可自定义安全密钥，并能自由选择加密算法，安全性尽由用户掌握
		【智能加密】 √ 对于加密文档，编辑、保存后依然为加密文档，不改变文档的加密状态 √ 对于非加密文档，编辑、保存后仍然为非加密文档 √ 用户新产生的文档不会强制加密
		【只读加密】 √ 用户产生的文档本身不加密，只能以只读方式查看加密文档，无法对文档进行编辑和保存等操作 √ 在只读授权环境下，依然可以防止用户通过剪贴板、截屏、打印（包括虚拟打印）等方式窃取加密文档内容
		【权限控制】 √ 文档制作者可对加密文档进行权限控制，可设定文档的访问者，及访问者的阅读、修改、复制、打印、截屏、有效期和解密等权限 √ 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，防止加密文档在企业内部扩散泄密 √ 用户可以调整加密文档的安全区域和密级，对重要文档可采取提高其密级的方法来禁止普通用户的访问 √ 部门间需要进行文档交互时，可修改加密文档的安全区域与加密级别
		【对外交互】 √ 可对需要外发的文档进行加密控制，防止二次泄密 √ 可对特定的机器进行授权，只允许特定机器上打开并查看外发文档 √ 能够对指定外发文档的查看期限、打开次数、打开密码、复制、编辑、打印、截屏等使用权限进行控制 √ 支持外发USBKEY，认证后才能打开外发文档，不需要绑定计算机 √ 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 √ 可以自定义外发模板，方便用户快速配置外发权限

产品	模块	功能介绍
文档加密系统		**【出差办公】** √ 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，不影响日常办公 √ 可对出差人员设置个性化的离线策略，包括授权的离线时长、加密软件类别、文档解密、外发等使用权限 √ 出差时可插入离线权限USBKEY，可保证加密功能继续使用或提升当前的加密权限 √ 出差时，在未安装IP-guard客户端的计算机上插入U盘加密客户端，可正常使用加密文件，拔出U盘加密客户端则不能打开加密文件
		【移动终端查看器】 √ 可以在手机、平板等移动智能终端安装查看器，通过查看器查看办公类的加密文档，满足企业移动办公需要 √ 对移动终端进行授权，授权用户方可使用查看器查看加密文档 √ 管理员可以授权移动终端的加密或解密权限，被授权的移动终端可以在查看器APP中加密或解密文档 √ 管理员可赋予移动终端查看加密文档安全区域和密级的权限，移动端用户只允许查看指定安全区域和密级的文档 √ 可以指定查看器与服务器的认证间隔时间，设定查看器的使用期限，避免脱离管控
		【多级审批】 √ 支持单级、多级、逐级、会签审批，满足多样化审批流程的需要 √ 支持Web审批，增加工作便利性；同时支持通过Web预览及下载文件 √ 移动终端安全审批，支持通过移动终端接收申请通知，可直接预览及审批各类申请
		【系统支持】 √ 支持Windows、Mac和Linux操作系统，实现跨平台管理 √ 加密文档可在Windows、Mac及Linux三个系统平台上正常使用，也支持在智能手机（iOS/Android）上预览加密文档，兼容性强
		【灾备机制】 √ **双机热备** 通过主从服务器实现双机热备，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，确保审批流程正常，日志的收集及查看正常，策略的执行正常 √ **备用服务器** 部署一个或多个备用服务器，当主服务器出现硬件故障时，备用服务器将自动接管加密系统，确保加密客户端正常运行 √ **网络灾备** 预设容灾时间，当用户出现网络故障时，在容灾时间范围内，加密功能仍然可正常使用 √ **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时，可从备份中找回相应的明文或密文，避免遗失重要文档

产品	模块	功能介绍
敏感内容识别系统		√ 通过检索文件内容，帮助企业发现各个客户端上存在的含有敏感关键字的机密文件 √ 可以对所有的客户端进行扫描分析，发现含有敏感关键字的机密文件并进行加密保护 √ 在拷贝、上传或是外发文件时，支持对文件内容进行扫描，阻断含有敏感关键字的机密文件外发出去 √ 当含敏感内容的文件通过移动存储、IM、Email、网页上传时进行日志记录，帮助管理员更加有针对性地对含敏感内容的文件进行审计
终端安全管理系统	文档操作管控	√ 文档操作审计 可记录核心资料流通情况 √ 文档操作控制 管理用户使用文档的权限 √ 对通过U盘、智能手机等设备传送文件，进行操作记录 √ 支持记录刻录操作日志，可备份刻录的文件副本 √ 在重要文档被复制、篡改或删除前备份，防止文档损坏和丢失
	文档打印管控	√ 打印操作审计 预防安全风险 √ 打印内容备份 以图片形式备份打印内容 √ 打印授权管理 节省打印成本防止泄密 √ 打印浮水印 可显示文字水印、图片水印、二维码水印和点阵水印 √ 应用先进的打印映像获取技术，以图片格式记录打印内容 √ 用户可申请临时放开打印权限，或申请临时取消打印水印，也可以通过自我备案登记后进行相关操作
	设备管控	√ 存储设备管理 防止内部信息外泄 √ 通讯设备管理 避免非法外联带来的风险 √ 音视设备管理 避免工作时间分散注意力 √ 新设备管理 规范企业的外设使用 √ 支持控制智能手机、4G上网卡、随身wifi以及刻录机等几乎所有外设 √ 受设备策略控制的用户，可通过申请临时放开指定设备的使用权限，也可以通过客户端自我备案登记后便可进行相关操作
	移动存储管控	√ 移动存储审计 记录设备插拔及拷贝的详细信息 √ 移动存储授权 实现专盘专用 √ 移动存储加密 加密盘只能在企业内部使用 √ 移动存储注册 确保外来U盘无法随意接入企业内网 √ 当客户端移动存储被禁止使用时，客户端可以通过提交申请，请求读、写U盘，也可以通过客户端自我备案登记后便可进行相关操作
	即时通讯管控	√ 聊天记录审计 防止有意无意泄密 √ 外发文档和图片备份 审计更全面 √ 文档外发控制 控制机密文件的传输 √ 图片外发控制 控制发送截图 √ 限制帐号登录 增强工作效率 √ 支持QQ、微信、企业微信、钉钉等主流即时通讯工具的审计和管控 √ 记录QQ、微信、企业微信、钉钉等聊天内容

产品	模块	功能介绍
终端安全管理系统	邮件管控	√ 邮件信息记录 便于企业对邮件的安全使用情况进行统计 √ 邮件发送控制 防止企业的重要信息通过邮件方式泄露 √ 支持对Lotus、Exchange、标准协议、网页邮件进行审计 √ 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 √ 可以对邮件附件进行自动备份
	网页浏览管控	√ 网页浏览统计 详细掌握用户浏览网页的行为 √ 网页浏览审计 记录浏览网页的详细信息 √ 网页浏览控制 减少访问非法网站带来的安全风险和工作效率损失 √ 用图表的方式展现统计结果，各种数据一目了然 √ 支持包含IE、Firefox、Chrome等绝大部分的主流浏览器 √ 可控制http、https和FTP协议的上传行为
	网络控制	√ 通过网络通讯控制，避免随意的信息交流带来的风险 √ 可以控制企业内部每台计算机之间的网络通信 √ 禁止office或wps上传文档到云盘的风险 √ 安全检测不通过，则断网控制，通过则自动放开控制 √ 可检测到外来接入的计算机，可禁止其访问企业的计算机
	网络流量管控	√ 流量统计 随时了解流量的使用情况 √ 流量控制 保证关键业务的正常进行 √ 以图表形式多维度输出流量统计结果 √ 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 √ 可以控制企业内部任何一台计算机的网络流量
	应用程序管控	√ 应用程序统计 全面掌握应用程序使用动态 √ 应用程序控制 防止非法程序运行 √ 软件安装/卸载管理 限制计算机软件的安装/卸载，使计算机的应用程序趋于标准化 √ 自动收集应用程序的特征信息，即使将应用程序改名管控依然有效 √ 用图表的方式展现统计结果，应用程序使用情况一目了然 √ 允许管理者对不同种类的程序进行分时段管理，让管理更加人性化 √ 能根据应用程序的特征值来限制指定应用程序的运行
	软件中心	√ 管理员可通过软件中心上架、发布及下架软件，并可规定终端用户的查看或安装权限 √ 支持终端用户通过软件中心下载、安装、升级或卸载软件 √ 支持http和P2P分发模式 √ 审计管理员的操作行为，包括：登录软件中心、上架软件、添加用户、设置权限、注销退出等
	水印及文档追溯	√ 支持在计算机的屏幕显示图片水印、文字水印、二维码水印和点阵水印，有效震慑拍照、截屏或录屏泄密的行为 √ 通过文档流转标记技术，支持在文档中记录其在各个各节点上流转的时间、用户和计算机等信息 √ 支持在文档中直观呈现显式水印，该水印对用户可见，水印将跟随文档一直存在，更具有震慑效果 √ 支持在文档中呈现隐形水印，该水印对用户不可见，水印也将跟随文档一直存在，可以起到更好的追溯效果

产品	模块	功能介绍
终端安全管理系统	屏幕监视	√ 屏幕查看 了解用户的工作状态 √ 屏幕记录 便于随时查看屏幕历史 √ 特殊记录 保护信息安全同时节省数据量 √ 特殊行为记录 当用户通过邮件、IM、网页、打印、拷贝等进行文件传送时，支持记录行为发生时的屏幕画面 √ 采用增量、变频等技术，屏幕记录数据量业内最小 √ 对特定的程序进行记录，并且支持自定义记录频率 √ 可将屏幕历史转换为通用视频格式，更方便查阅
	资产管理	√ 资产管理 了解计算机软硬件信息及变更情况 √ 版权管理 了解计算机安装的软件及授权情况 √ 可以自定义生成软硬件资产统计报表 √ 自动收集网内计算机的补丁安装情况，并可集中管理和安装补丁 √ 支持通过P2P分发软件或补丁，部署效率更高 √ 软件管理 可查看终端所有软件信息，支持批量卸载已安装的非法软件 √ 支持对打印机、路由器等非IT资产进行自定义管理 √ 支持对系统密码复杂度进行检测及控制
	远程维护	√ 远程连接到远端计算机桌面，直接对计算机进行操作或示范 √ 远程文件传送 √ 可查看客户端计算机安装的所有软件信息，可远程卸载软件 √ 可对客户端计算机的运行状态进行实时查看及维护
	风险审计报表	√ 统计表 有效统计用户行为 √ 趋势表 直观展现行为变化的趋势 √ 征兆表 当风险出现时，及时预警 √ 支持软硬件资产统计报表 √ 支持个性化的私人订制报表 √ 支持自动生成周期报表，并且提供邮件订阅功能
	文档云备份	√ 可自动对终端文档进行备份，支持即时备份和定时备份 √ 可设置备份文档类型、排除文件、备份文件大小、备份间隔、备份流量、备份日期和时段等条件 √ 支持设置保留多个历史副本 √ 支持按组织架构的用户列表查看备份库，备份文档以终端实际盘符目录的形式呈现 √ 支持快速检索相关文档，可在线查看备份文档，可设置不同用户对备份文档的查看、下载和删除权限
	基本功能（必选）	√ 统计计算机的基本信息和策略总览 √ 支持限制计算机的系统设置功能，比如：控制面板、网络属性、注册表等 √ 支持对终端计算机进行锁定、注销、重启、关闭等操作 √ 支持对计算机的安全基线进行检查，包括杀毒软件检查、软件安装检查、程序运行检查、系统服务检查、补丁检查、域用户身份检查等 √ 支持角色管理、支持用户系统、支持与AD域同步 √ 支持按用户或计算机两种方式进行权限管理 √ 支持多国语言

产品	模块	功能介绍
安全桌面		√通过沙盒技术将普通桌面和安全桌面进行隔离，保护安全桌面中的敏感数据，无需重启计算机即可自由切换，高效兼顾机密和普通办公环境 √将涉密程序限制在安全桌面中运行，防止核心数据外泄 √为安全桌面开设专属的网络共享目录，普通桌面无法访问 √安全桌面默认禁止访问任何网络，可根据需要开通访问部分IP地址或域名 √安全桌面默认禁止连接任意外设，可根据需要放开部分外设的使用 √安全桌面默认禁止连接物理打印机、网络打印机和共享打印机，但可根据需要允许开放使用某台打印机 √从安全桌面导出文件加密，导入文件解密，保证核心数据安全 √支持记录安全桌面登入登出及文件导入导出的日志
安全网关	硬件网关	√服务器文档下载加密：服务器数据下载到终端自动加密，防止服务器数据下载泄密 √加密文档上传解密：终端的文档上传到服务器时自动解密，服务器以明文存储，确保良好的兼容性 √杜绝非法计算机和非法程序对服务器进行访问，有效保障服务器的明文文件的安全 √支持串联、旁路两种部署方式 √支持企业常用信息管理系统OA、PLM、SVN、ERP等 √支持B/S、C/S两种服务器访问方式 √采用高强度的通讯加密技术
	软件网关	√适用于云服务器的保护，对不方便架设硬件网关的传统物理服务器，也可通过软件网关进行保护 √杜绝非法计算机和未授权程序访问服务器，保障服务器的访问安全 √服务器文档下载到终端自动加密，防止服务器文档下载泄密 √终端文档上传到服务器自动解密，服务器以明文存储，确保良好的兼容性 √支持企业常用的各类应用系统OA、PLM、SVN、ERP等 √支持B/S、C/S两种服务器访问方式 √采用高强度的通讯加密技术 √可用于保护Linux服务器，也可以通过反向代理保护其他操作系统的服务器
准入网关		√计算机访问服务器或互联网时，需要经过准入网关的严格审核，只有合法的计算机才能访问受保护的资源，非法计算机将被引导至隔离区进行修复，或完全阻断其访问 √支持对终端计算机进行安全状态检查，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修复 √对于临时来访的外来计算机，可以建立访客账号，通过Web浏览器输入账号密码进行身份认证，验证通过后，可访问受保护的资源 √防止内部计算机通过重装系统、安装多系统、虚拟机等方式脱离管控 √支持串联、旁路和镜像三种部署方式
安全U盘		√密码保护 U盘读写，需要密码认证才能使用安全U盘 √详细记录 U盘的使用和U盘文档操作的记录 √使用专属的资源管理器，可有效防范木马病毒 √区分保密区和交互区，通过内外分区，确保U盘使用安全 √采用芯片级保护，有效防止非授权的U盘格式化

IP-guard七大产品18大模块功能

IP-guard 文档加密系统

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	文档打印管控	设备管控	移动存储管控
即时通讯管控	邮件管控	网页浏览管控	网络控制
网络流量管控	应用程序管控	软件中心	水印及文档追溯
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 安全桌面

IP-guard 安全网关

IP-guard 准入网关

IP-guard 安全U盘

各行业标杆企业一致信赖IP-guard

oppo　vivo　华为终端 HUAWEI Huawei Device　小米 xiaomi.com　ZTE中兴

CATL 宁德时代　长江存储　SMIC 中芯国际　TIANMA 天马微电子　北斗星通 BDStar Navigation

上上电缆 SHANGSHANG CABLE　Galanz 格兰仕　AUX 健康空调奥克斯　Panasonic 松下电器　inspur 浪潮

SANY　FANUC 发那科　东风小康 DFSK　广汽集团 GAC GROUP　恒大集团 EVERGRANDE GROUP

SANGFOR 深信服科技　饿了么　唯品会 vip.com　途牛 tuniu.com　watsons 屈臣氏

中国移动通信 CHINA MOBILE　中国石油　ICAC　中南市政院　深圳发改委

中山大学 附属第三医院 THE THIRD AFFILIATED HOSPITAL, SUN YAT-SEN UNIVERSITY　上海长海医院　MY LIKE 美莱整形　老百姓大药房 LBX PHARMACY　CSPC 石药集团

ochirly 欧时力　博时基金 BOSERA FUNDS　BCS 长沙银行 BANK OF CHANGSHA　泰康资产 TAIKANG AMC　海大集团 HAID GROUP

TEC Solutions Limited
溢信科技

广州 | 深圳 | 珠海 | 北京 | 上海 | 长沙 | 重庆 | 成都 | 合肥
武汉 | 西安 | 郑州 | 济南 | 青岛 | 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