上网行为
文档安全
设备管理
系统 & 网络管理
运维中心
生产力
文档透明加密

Ping32

# 功能模块简介

| 模块 | 功能 | 功能描述 |
| --- | --- | --- |
| 01 浏览网站 | • 浏览网站监控 | • 详细记录终端计算机浏览网页的网址和标题，并提供查询功能。 |
| | • 网站访问控制 | • Ping32 可以对指定的网站 URL 进行封堵。自主研发的高性能过滤引擎，不仅对计算机性能无影响，还支持 HTTPS/SSL 加密协议的过滤。 |
| | • 网站敏感词拦截 | • Ping32 支持网页关键词拦截。 |
| | • HTTP POST 管控 | • 阻断终端通过浏览器 HTTP POST 行为进行的文件上传、支持设置例外 URL。 |
| 02 即时通讯管控 | • 即时通讯监控 | • 完整记录 QQ、微信、Skype、腾讯 RTX、钉钉、企业微信等主流即时通讯软件的对话时间、收发双方、对话内容等信息。 |
| | • 聊天语义告警 | • 定义即时通讯敏感词，对话内容包含了敏感的关键词或语义，如：帐号信息，求职信息等，管理员则会及时收到报警通知。 |
| | • 聊天帐号管控 | • 限制用户登录其它聊天帐号，可以设置指定用户登录管理员设置的聊天帐号。 |
| | • 聊天传输文件 | • 对终端通过即时通讯软件外发的文件进行记录，并对外发的文件进行备份。 |
| 03 邮件管控 | • 电子邮件监控 | • 记录标准协议邮箱、HTTPS/SSL 加密协议邮箱的收发邮件的标题、收件人、发件人、正文、附件等内容。 |
| | • 电子邮件管控 | • 可通过收件人、发件人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。 |

| 模块 | 功能 | 功能描述 |
| --- | --- | --- |
| 04 文档安全管控、审计 | • 泄密追踪 | • 对终端通过浏览器、即时通讯、邮件外发的文件进行记录，并对外发的文件进行备份，提供泄密风险等级评定。<br>• 对终端通过 U 盘、移动硬盘等外接存储设备拷贝文件进行记录，并对外发的文件进行备份，提供泄密风险等级评定。 |
| | • 外发文件敏感内容告警 | • 定义外发文件敏感词，实时分析外发文件正文内容，包含敏感词信息，管理员会收到报警提示。 |
| | • 文件操作监控 | • 记录终端计算机的文件操作信息，包括本地磁盘、移动存储、网络路径、共享目录的所有文档创建、访问、修改、复制、移动、重命名、删除等操作。 |
| | • 文件外发管控 | • 文档外发管控可以封堵常见的文档外发行为，比如：通过电子邮件、聊天软件、网盘等途径外发文件。支持自定义文件类型、大小等。 |
| | • 敏感文档监控 | • 统计终端包含敏感内容的文档，包括：文件名、路径、修改时间等信息。 |
| | • 剪切板监控 | • 监控终端剪切板的文字信息，包括时间，和具体文字内容。 |
| 05 屏幕安全 | • 智能截屏 | • 定期对屏幕进行截屏，智能识别屏幕内容并进行分类，比如：聊天、电子邮件、求职、购物等。 |
| | • 屏幕水印 | • 统一在终端计算机桌面显示自定义水印文字。 |
| | • 窗口水印 | • 指定终端在打开某个应用时添加自定义水印文字。 |
| | • 截屏管控 | • 记录终端截屏内容，并且可以封堵 Print Screen、聊天软件截屏、浏览器截屏插件、以及 PicPick 等专业的截屏工具。 |
| | • 实时屏幕 | • 实时查看终端屏幕内容，支持对多个终端屏幕进行集中监控。 |
| | • 屏幕录像 | • 对屏幕进行不间断录像，并保存成录像文件，方便事后审计。 |
| 06 打印安全 | • 打印监控 | • 详细记录终端打印信息，包括打印标题、时间、页数、内容等信息。支持打印快照查看。 |
| | • 打印管控 | • 管控终端用户使用打印权限。 |
| | • 打印水印 | • 终端打印的文件自动置入自定义水印文字。 |

| 模块 | 功能 | 功能描述 |
| --- | --- | --- |
| 07 移动存储管控 | • 移动存储使用 | • 对终端计算机的移动存储拔插事件进行记录。 |
| | • 移动存储操作 | • 对终端计算机的移动存储的操作事件进行记录。 |
| | • 移动存储使用告警 | • 针对终端使用 U 盘以及进行文件拷贝时提供实时告警。 |
| | • 移动存储管控 | • 可以对 U 盘进行管控，规范 U 盘的使用，降低信息泄露的风险。同时，还可以对 U 盘进行授权，只有授权的 U 盘才可以使用，安全便捷两不误。 |
| | • 移动存储加密 | • Ping32 使用 AES 等高强度的加密算法对 U 盘进行加密，加密后的 U 盘只能在企业内部使用，如果员工违规带走，在外部无法正常打开使用。 |
| 08 硬件 & 设备管理 | • 硬件变更报警 | • 终端硬件资产变更记录及产生告警信息。 |
| | • USB 端口管控 | • 禁止终端使用通过USB端口连接的设备（键盘鼠标除外），支持设置例外设备 |
| | • 禁用设备 | • 禁用光驱、蓝牙、串口、并口、火线、PCMCIA 总线；禁用打印机、便携 WIFI、无线网卡等，保证系统安全。 |

| 模块 | 功能 | 功能描述 |
| --- | --- | --- |
| 09 系统安全 & IT 资产 | • 系统安全检测 | • 查看全网终端防火墙设置情况、杀毒软件安装情况、来宾用户开启状态、系统多用户使用状态及 Internet 代理使用状态。 |
| | • 系统安全策略 | • 设置系统安全策略，如：禁止安装新软件、禁止共享、禁用注册表、禁用任务管理器、禁用控制面板、禁用安全模式等、禁止修改终端名、禁止修改网络配置、禁用命令提示符、禁用 Windows 管理控制台、禁用自动播放。保证系统始终处于安全状态。 |
| | • 软件资产统计 | • 终端软件资产信息统计，全网终端硬件信息统计。 |
| | • 硬件资产统计 | • 终端硬件资产信息统计，全网终端硬件信息统计。 |
| | • 操作系统统计 | • 终端操作系统安装情况统计。 |
| | • 杀毒软件统计 | • 终端杀毒软件安装信息统计，全网终端杀毒软件安装信息统计。 |
| 10 软件管理 | • 软件资产变更告警 | • 终端软件资产变更记录及产生告警信息。 |
| | • 软件白名单 | • 允许指定的终端计算机在指定的某段时间内使用某种程序。支持进程名、版权信息、安装目录、产品名称等多种匹配方式。 |
| | • 软件黑名单 | • 限制指定的终端计算机在指定的某段时间内使用某种程序。支持进程名、窗口名、MD5 等多种匹配方式。 |
| | • 软件安装白名单 | • 开启禁止安装软件策略后，可通过添加软件安装白名单允许特定软件的安装，支持软件数字签名、版权、产品名称等信息。 |
| | • 软件远程卸载 | • 远程强制卸载终端电脑内已安装的软件。 |
| | • 盗版软件检测功能 | • 实时检测用户安装软件是否为盗版软件，可记录盗版软件名称、版本、开发商、软件安装路径、启动软件时间。 |
| 11 网络管理 | • 网络访问控制 | • 通过对程序、网络端口、IP 地址、通讯方向、协议类型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互带来的风险。 |
| | • 非法外联 | • 检测终端违规外联行为，并可同时阻断违规外联行为。 |
| | • 可信网络 | • 用户可以自定义可信网络环境，离开可信网络支持相应策略联动。 |

| 模块 | 功能 | 功能描述 |
| --- | --- | --- |
| 12 远程工具 | • 分发任务 | • 分发文件、软件、补丁到终端计算机指定路径，支持软件远程安装部署。 |
| | • 远程协助 | • 远程连接到用户计算机的桌面，并直接对计算机进行操作或示范，快速响应系统故障。 |
| | • 文件管理 | • 通过 Ping32 终端安全管理系统的远程文件管理功能，你可以操作远程用户电脑上的文件，比如：浏览、删除、打开、下载等操作。 |
| | • 节能设置 | • 集中对终端进行定时关闭显示器、定时锁定或者定时睡眠，并可设定两次定时关机任务，有效防止能源损失。 |
| | • 工单管理 | • 统计终端工单申请，管理员可及时有效采集终端工单信息并及时做出响应。 |
| | • 发送消息 | • 可以对全网终端用户或指定用户发送通知消息。 |
| | • 时间校准 | • 设置终端计算机时间与服务器时间保持同步。 |
| | • 桌面个性化 | • 对用户电脑自定义设置桌面背景，可禁止用户修改桌面背景，以及可以对用户电脑设置屏幕保护等。 |
| | • 终端负载 | • 统计终端 CPU、内存、硬盘占用率，提供实时负载查看，超阈值预警。 |
| | • 终端活动时间统计 | • 统计每个用户在一段时间内，电脑开机运行时间，空闲时间，用户聊天时间，浏览网站时间等。统计每个终端的上下线时间及离线时长。 |

| 模块 | 功能 | 功能描述 |
| --- | --- | --- |
| 13 生产力 | • 生产力评估 | • 智能统计、分析员工使用电脑的时间，并根据员工行为自动划分高效工作时间、低效工作时间 |
| | • 生产力排行 | • 通过获取员工使用的软件，以及每个软件所使用的独立时间，计算员工的生产力评分，形成生产力效率排行榜。 |
| | • 活动分析 | • 对所有终端的软件应用类型进行统计，并根据类型划分使用时长及占比，以软件类型维度分析整体的活跃度和评分。 |
| | • 时间跟踪 | • 可以查看所有终端的软件应用及详细信息，并可对每个应用自定义个性标签，形成更智能化的统计图表。 |

| 模块 | 功能 | 功能描述 |
| --- | --- | --- |
| 14 文档透明加密 | • 透明加解密 | • Ping32 通过多种高强度加密算法，对企业散 落在各处的文件透明加密，实现受信用户打开文档自动解密 ，保存文档自动加密 ，整个过程对用户毫无感知，并且丝毫不会改变用户的使用习惯。文档加密可以有效保护文档不被非法 窃取、防止内部主动泄漏。 |
| | • 半透明加解密 | • Ping32 半透明加密技术针对企业不同部门的 密级管理程度，使得非核心部门在需要的情况 下可以正常使用核心部门加密文档，但不会造 成非法的数据泄漏，自身非加密文档不受影响， 避免过度管控降低工作效率。 |
| | • 手动加解密 | • 数据使用部门主动对敏感数据加密，防止误操作、外部窃密导致的数据泄漏。 |
| | • 穿透加解密 | • Ping32 穿透加密技术可对压缩包中的原始文件进行加解密操作，全盘加密无遗漏。 |
| | • 智能加密 | • Ping32 将敏感内容分析与文档加密技术结合， 实时或定时扫描终端文件，对全网涉密信息进行针对性防护 ，敏感内容分析支持关键词 ，正则表达式等匹配规则，防止敏感内容，业核心数据。集中管控，从而避免过度管控，影响工作效率。 |
| | • 敏感词库 | • Ping32 内置符合各行业敏感数据的识别库，如金融行业所涉及的公民个人信息 : 身份证号、手机号、银行卡号 ; 或者财务部门涉及的合同、订单 ; 又或者是研发部门的逻辑代码等等 ..... 通过 Ping32 敏感词库您可以建立属于自己的 核心数据识别体系，将散落在企业不同位置的 敏感文档智能加密，维护企业核心知识产权。 |
| | • 文档权限 – 安全域 | • Ping32 安全域管理可以设置不同的文件安全 域以实现部门之间的加密数据需要安全隔离的管理要求，控制文档流转范围，确保文档在 特定范围内使用。 |
| | • 文档权限 – 密级 | • 对重要文档分级管控，并且对不同用户赋予不 同的密级权限，密级权限低的用户无法打开高 密级文档，确保文档权限安全可控。可灵活为不同用户设定不同的文档访问权限，严格控制 密级范围，此外也支持对指定文档设置其他用 户的访问权限、次数、时间等。 |
| | • 流程审批 | • Ping32 不仅可以支持自定义的审批流程、审批人，还支持自定义的审批通过条件。Ping32 支持客户端、管理端、网页、手机 APP 等多种审批方式。 |
| | • 离网办公 | • 针对出差人员或网络故障等原因引起的客户端离网 ，用户可以可发起离网审批 ，确保终端密文在出差过程中保持可用状态，不影响日常办公。Ping32 文档加密提供了 |

| 模块 | 功能 | 功能描述 |
| --- | --- | --- |
| | | 多种离网办公权限。 |
| | • 文档安全外发 | • 为满足对外业务的正常交互，Ping32 文档安全外发结合透明加密、权限管理等技术，对需要外发的文档加密控制、指定外发文档的使用权限，在不影响正常办公的同时防止二次泄密。 |
| | • 邮件白名单 | • 基于先进的机器学习技术实时分析邮件包含的敏感内容，根据用户既定策略，对邮件无感知透明加解密，确保可信范围内邮件正常传输，自动拦截带有敏感信息的邮件，防止核心数据外泄。 |

# 增值服务

| 模块 | 功能 | 功能描述 |
| --- | --- | --- |
| 15 身份认证 | • 身份认证 | • 自定义系统登录用户或使用 Windows 用户，统计登录用户操作审计信息。 |
| 16 文档备份 | • 文档备份 | • 文档备份可以将分散在客户端的文件进行集中备份管理，整个备份过程对系统资源占用极少，用户无感知，可以设置多个历史版本。文档备份并非定时全盘扫描备份，而是会识别用户的修改文件操作，当用户保存文件的一瞬间，记录文件变化，发起备份请求。终端进行文件删除操作时自动对被删除的文件进行备份。 |




**安在软件**
济南
高新区新泺大街 2008 号
银荷大厦 C 座
—
400-098-7607
support@nsecsoft.com