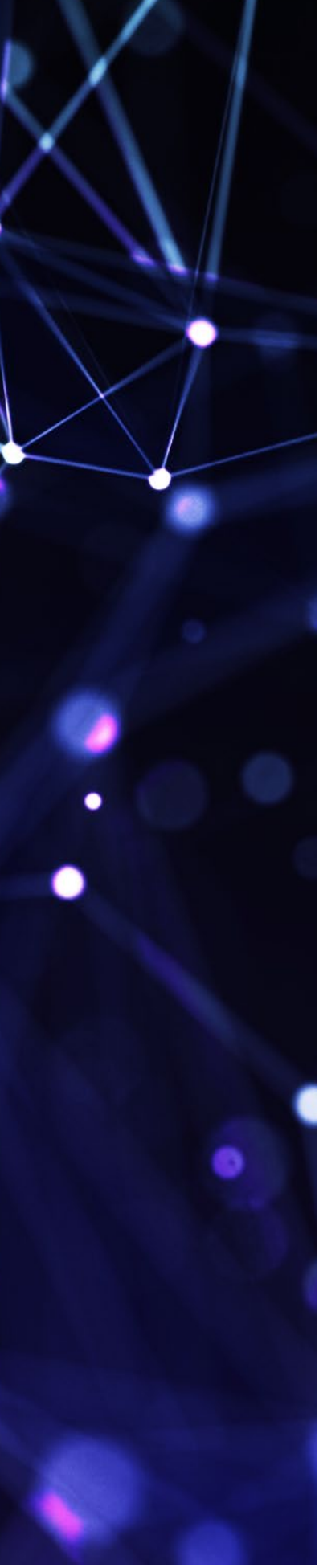
Ping32

制造业

企业数据防泄漏&终端安全管理解决方案



目录

01

项目背景

制造企业制定的文档管理制度和企业员工守则，在落地执行时严重依赖低效的、参差不齐的人员自觉性来遵守，企业内部终端行为审计管理机制的缺失，导致泄密事件发生后才会组织相关人员追查可能已经被不法人员销毁的泄密证据，前期的不法行为活动留痕困难，事后的证据收集困难，导致企业无法对不法人员开展追责严惩，无力维护企业合法正当利益，无法挽回企业损失。

02

企业面临问题

- 如何管控员工在使用企业电脑办公时通过聊天软件、U盘拷贝、打印文件、电子邮件、网盘上传、发布违规信息等行为方式进行泄密、违法、损害企业利益的行为。
- 制造业繁琐的经营生产过程中，重要生产数据需要给上下游合作伙伴交互使用，合作伙伴方的管理缺失和人员流动可能会造成自身企业协同生产数据的泄密风险。
- 企业内部使用的众多办公、设计、制造、生产等软件的使用缺乏规范化管理，违规安装盗版软件、非法软件在办公电脑使用会造成不可控的企业数据损失，甚至会带来软件厂商的法律诉讼风险。
- 如何保障企业核心部门的重要数据在发生泄密行为时，保障重要数据安全，限制住重要数据的企业安全使用环境，降低不法人员损害企业利益的可能。

03

方案设计

围绕核心数据防泄漏和终端行为审计管控留痕为出发点，从以下角度触发提供解决方案：

- 对企业各事业部研发部门产生的工程参数文档及设计图纸进行强制加密，其他部门产生的重要文件数据进行加密保护，划分安全区域和等级，可信范围内的员工可授权访问加密文件。
- 结合多维度的敏感内容识别机制，定位企业现存的敏感数据，帮助提取敏感信息，进而做进一步的数据使用行为的安全管控。
- 结合Ping32聚合搜索，实现相关敏感事件的快速定位，在提供完善数据审计机制的前提下，在海量数据中快速聚合敏感事件相关联数据，还原敏感事件发生的全过程场景记录。
- 完善企业数据备份机制，在监控到不法行为发生的情况下确保核心数据完整性。
- 做好企业网络准入控制，规避非法设备、非法网络接入导致的数据泄漏风险。

04

解决方案

核心数据加密

- 丰富的授信软件库，支持所有应用程序的加密需求，如设计类的Pro/E、AutoCAD、SolidWorks对各部门产生的关键数据进行加密处理。加密后的代码、 文档只允许在内部授信环境下使用，离开授信环境将无法正常访问，杜绝泄密风险。
- 具有强制加密功能，结合制造业各部门实际业务需要，灵活配置加密策略，针对业务线部门终端产生的指定类型的文件会自动完成加密，无需人工参与。

- 针对管理层人员或者其他需降低管控力度的岗位人员使用半透明加密模式，实现可正常查看加密文件，但是自身产生文件不被加密的效果，针对不同人员的岗位职责评估是否使用半透明加密。

- 具有解密网关功能，无需使用硬件，即可实现与各应用服务器（如OA、ERP、PLM等）实现文件上传自动解密，下载自动加密，保障内部业务正常流通的同时，确保敏感数据文件始终处于安全可控的状态

- 邮件白名单解密、加密文件外发包查看器、U盘安全客户端等多种功能，满足企业重要加密数据对外交互使用场景的灵活管控，其中外发包查看器、U盘客户端可满足重要加密数据外发给上下游伙伴企业的使用限制管控，同时可限制外发文档的查看时间限制、次数、禁止打印、查看显示水 印及其他使用权限，防止二次泄密。

- 针对离网办公人员（携笔记本出差、居家办公）或网络故障等原因引起的客户端离线，设置用户可发起离网审批，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。该方案不需要员工携带离线权限ukey，更便捷，避免离线权限ukey因员工保管不善丢失后造成的不能打开离线文件风险。

- 在加密文档的使用过程中， 能够防止员工通过剪贴板,截屏,虚拟打印等方式窃取加密文档内容。控制授权软件与非授权软件之间的剪切板使用权限，可限制禁止密文复制到明文，密文之间允许复制等权限。 根据不同部门、不同员工岗位级别，可根据需求划分不同的安全域和密级，对于具备 手动解密权限的员工仅可限定解密所属安全域下的加密文件，避免跨部门或者越级沟 通涉密数据导致信息泄密风险

- 具备离线策略，支持服务器出现宕机、故障等意外情况时，所有终端计算机也可以在限定时间内可以正常打开加密文件，确保工作的正常开展。

终端设备管理

- 保证终端系统稳定、可靠运行，对计算机外部设备的使用进行严格管控，特别是对移动设备的管理。

- 移动存储设备审计，详细记录所有通过U盘的文档操作，尤其针对拷贝行为，备份拷贝具体文档，实现事后追溯。

- U盘授权管理，区别外部U盘与企业内部授权U盘，禁止私人未授权U盘接入操作行为。管控读、写、禁止使用等权限。

- U盘加密管理，通过高强度加密算法，有效管控U盘丢失、外带导致的数据泄漏事件，为企业不同部门分配密钥，建议部门专用U盘，实现专盘专用，防范企业内部的数据流转泄密情况。

- 设备管控，限制U盘、移动硬盘、光驱、刻录机等各类存储设备的使用，禁止通讯接口及无线网卡、即插即用网卡、便携wifi等网络设备，避免人为非法外联，禁止其他新增未授权设备的使用，杜绝机密信息从设备外泄的隐患。

终端系统网络&软硬资产统计

- 系统安全策略，禁止共享、禁用注册、禁用任务管理器、禁用控制面板、禁用安全模式、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可控状态。

- 软硬件资产统计，通过对终端的数据盘点，监控终端软件安装运行情况，支持软件名，安装位置、版本等均可导出报表。统计终端包括CPU、主板、内存、硬盘、显卡、显示器等数据可报表导出。

文档安全备份

- 杜绝离职删除内部大量数据，防止数据源丢失，事前备份很关键。借助Ping32提供的备份机制，可对终端计算机中的文件做全盘备份、指定路径备份或者删除备份，备份时支持 文件做解密备份或者密文备份，确保各项业务数据的完整性。

- 针对触发泄密行为的企业重要文件，智能备份到服务器，为企业及时挽会数据泄密损失。

敏感数据识别

- 将散落在终端各处以及实时产生的文本文档进行归类、定位，对Word文档、表格、演示文稿、PDF等类型数据，对涉及的代码文件、技术资料等，标识其敏感级别、所属分类、所在位置、文件大小等，便于对涉密信息做进一步的安全管理。

- 智能扫描指定计算机上的文档，分析是否包含指定的敏感数据类别，分析加密状态，分析出涵盖敏感数据但是当前为非加密状态，可进行进一步的加密处理，确保涉及数据始终处于加密可控的状态。

- 把文档透明加密和敏感内容识别结合起来，做精准文件加密，智能分析文件内容中涵盖敏感内容即做加密处理，不涵盖敏感内容即普通文件不做加密，避免过度管控。
  对于加密文件的存在位置不清晰的情况，可以扫描指定位置或指定类型的加密文档或文件夹，查看加密数据的存在位置、是否加密的状态。可以发现企业网络中的共享服务器，扫描指定网络存储位置的文件，对其加密或解密。

- 针对涉密的文件，通过涉密参数的设置，可以扫描指定计算机上的文档，分析是否包含指定的敏感数据类别，分析加密状态，分析出涵盖敏感数据但是当前为非加密状态，可进行进一步的加密处理，确保涉及数据始终处于加密可控的状态。

- 分析通过即时通讯、邮件、浏览器、云盘等途径外发文件行为。对包含敏感内容的文件传输行为可以进行告警、阻断、审计。

- 分析电子邮件发送行为，对包含敏感内容的电子邮件发送行为可以进行告警、阻断、审计。

- 分析剪切板内容，对包含敏感内容的剪切板使用行为进行审计。

软件管理

- 智能分析终端软件，匹配盗版软件特征，将盗版软件安装情况进行可视化展现。及时告警，执行管控措施，检测功能支持制造行业专业软件适配

- 自动清点企业终端软件资产，识别各版权软件的属性，属于收费版权还是免费版权，统计授权许可使用数量，可远程卸载盗版程序，提供IT运维效率，保障终端使用统一管理。

- 禁止网络通讯，通过网络防火墙，有效控制非法安装的盗版软件恶意访问网络权限，阻断非法安装软件与互联网通讯，保障企业内网安全。

- 为确保员工所安装的软件为正版且来源安全、符合企业软件标准化管理要求的程序，终端用户可自行通过Ping32软件商店下载所需软件。

聚合搜索

- 完整记录经聊天、邮件、U盘、硬盘、网盘、网页、其他应用软件产生的文件、图片、 文字等信息，提供相关备份。存储、管理、分析各类记录事件，在大量记录里需快速 定位到更加精准、有效的敏感信息，快速定位排查相关安全风险事件

- 支持将网站访问记录、即时通讯记录、邮件审计记录、文件操作、文件外发、剪切板等记录、事件，根据关键词进行聚合搜索展示。

- 针对文档、图片、压缩包、组合条件的搜索，支持OCR识别技术，支持压缩包穿透技术，支持通过关键词、正则表达式等多种条件组合进行搜索及筛选，满足多类数据搜索需求。

05

方案优势

一体化平台

提供集文档透明加密、数据防泄漏、统一终端管理、用户行为监控为一体的综合性解决方案。安装客户端及控制台即可实现统一管理。

闭环管理

- 事前防御： 文档透明加密。
- 事中控制： 代码传输途径控制。
- 事后追责： 操作行为审计。
- 智能防护： 敏感内容识别与管控、聚合搜索。

06

方案价值

有效健全企业防泄密管控机制

- 完善公司数据安全监管机制的基础上，通过一体化终端安全管理系统固化企业部门的规范化管理，使企业管理具备预防、审计、管控、留证的信息安全治理能力。

实现企业电脑终端资产的整合、统一管理

- 一体化终端安全管理系统可为企业实现各单位各部门间数据安全风险的可控监管，改变企业终端电脑分散低效管理的情况，实现企业终端统一管理、全程审计、规范维护、等保合规的要求。

聚焦企业中心管理，提供优质高效服务

- 一体化终端安全系统的建设，为企业发展核心竞争优势和保障内网安全等重心工作提供有力的监管措施和坚实的数据保障，打通企业全局电脑终端的安全管理通道，为企业数智化发展打下牢靠基础，充分将数据安全服务于企业各项事业的发展。

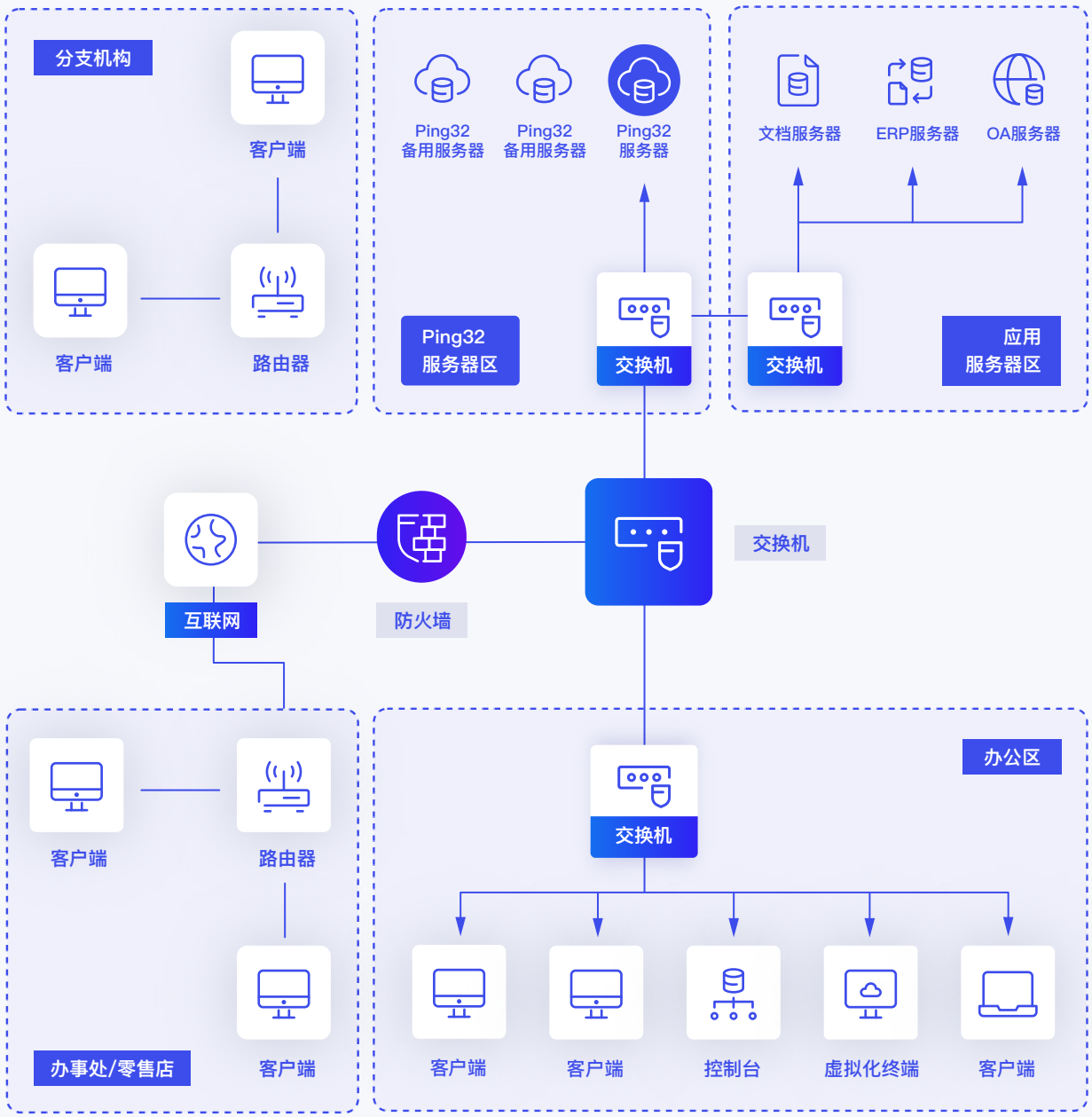
一体化终端使用的灵活性

- 按需选择功能模块：按实际业务需求，灵活选择需要使用的模块，自由组合。
- 方案可拓展未来需求：安装一个客户端，既能满足当前的业务需求，又可以在未来的需求中做拓展。
- 部署使用易用便捷：安装一个管理端平台，即可以实现所有客户端的集中管理。
- 可根据管理需要，分配给多人以不同的管理员权限，具备灵活的权限管理。

07 | 系统架构

- Ping32是基于C/S架构设计的，系统主要由三个模块组成，客户端模块、服务器模块和控制台模块。
- 客户端：安装在被管控的计算机上，执行管理者设定的管控策略，采集计算机运行的各项数据并上传给服务器。
- 控制台：供网络管理员、企业负责人用来管理终端计算机，审计操作使用。管理者通过控制台设置管理策略，查看日志和各项统计信息。控制台操作界面简洁易用，支持多个管理员登录。
- 服务器：安装在系统内的一部高性能计算机上。存储系统的管理策略和客户端上报的数据，向客户端计算机下发管理策略。

系统架构图


分支机构
客户端
客户端
路由器
Ping32
备用服务器
Ping32
备用服务器
Ping32
服务器
Ping32
服务器区
交换机
文档服务器
ERP服务器
OA服务器
交换机
应用
服务器区
互联网
防火墙
交换机
办公区
交换机
客户端
路由器
客户端
办事处/零售店
客户端
客户端
控制台
虚拟化终端
客户端

公司简介

山东安在信息技术股份有限公司成立于2014年，是一家以研发信息安全类产品及提供相关服务为主营业务的技术驱动型公司。是中国领先的、拥有完全自主知识产权的信息安全产品和服务解决方案专业提供商。

安在软件自主研发的Ping32终端安全管理系统，构建了全生命周期的一站式信息安全产品与整体解决方案平台，包括文档透明加密、办公行为审计、操作管控、敏感内容识别、终端系统安全、运维管理等功能，有效防护由于不正当的办公行为造成的数据泄漏。

Ping32凭借优异的信息安全管理方案以及良好的用户体验受到广泛好评。被广泛应用于政府、金融、军工、运行商、制造、能源、教育、医疗等行业的大型知名单位和机构，涵盖衣食住行各行各业，为国内10000多家用户，超过200万台终端提供安全保障。

400-098-7607
nsecsoft.com

济南
高新区经十路7000号汉峪金谷
互联网大厦12层
—
support@nsecsoft.com

NSecsoft 安在软件