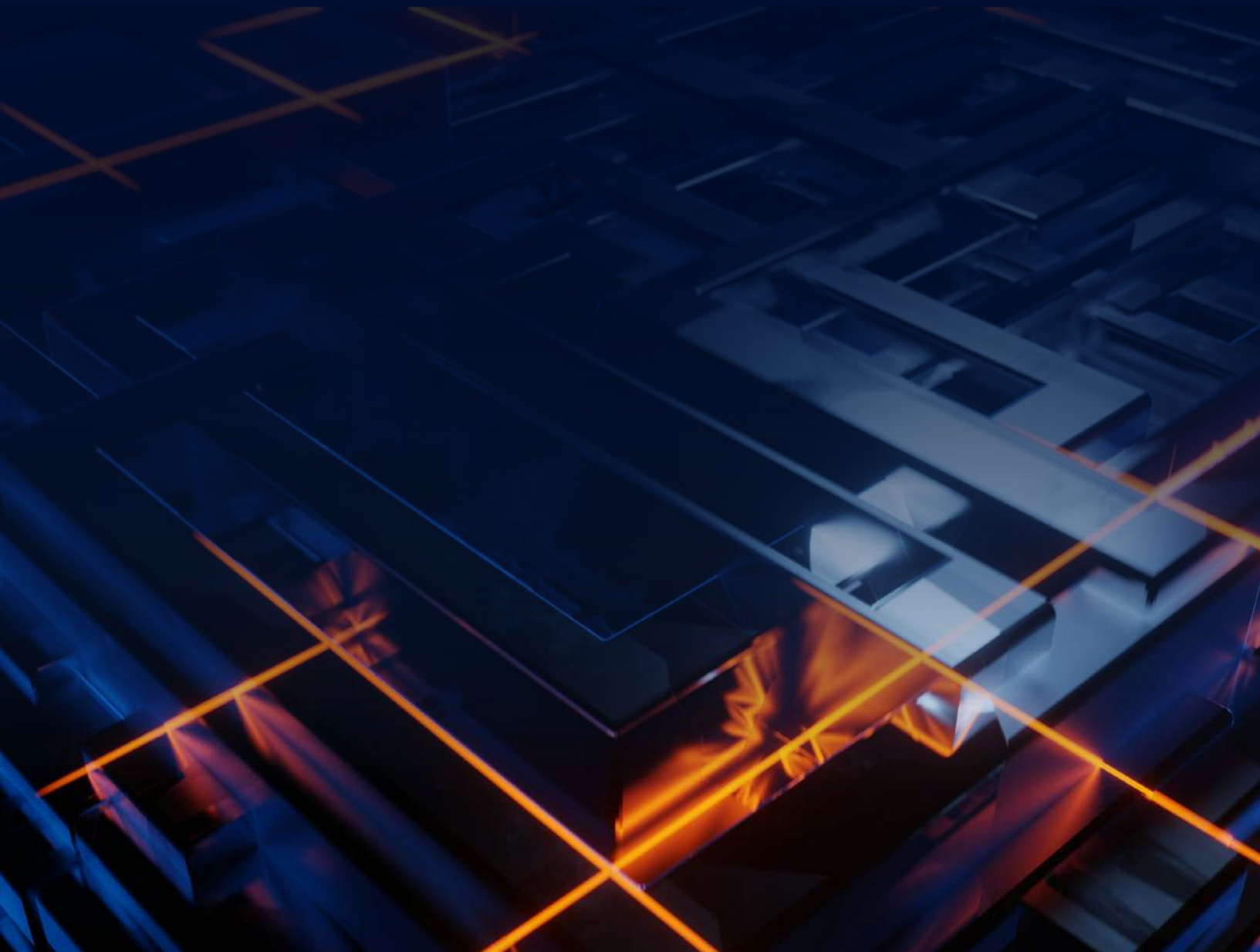
Ping32

Ping32精密零部件制造行业

数据防泄漏&软件合规化管理解决方案



目录

01

行业背景与挑战

精密零部件制造行业是现代工业的重要支柱，其核心竞争力在于对技术资料、设计图纸、设备参数等关键数据的积累与保护。作为一个高度依赖技术创新的行业，设计和研发环节要求企业持续推动技术进步，广泛使用CAD/CAE类软件（如SolidWorks、AutoCAD、UG NX等）创建和修改大量的机密文件，并且核心文件多存储于本地终端或研发服务器，使得数据泄露和丢失的风险进一步加剧。此外，精密零部件制造行业的研发工作还面临以下几项典型的数据安全挑战：

- 外发泄露风险高：研发成果需对外协供应商、客户等合作方共享，涉及U盘、邮箱、QQ微信即时通讯软件等多种渠道。
- 远程办公频繁：部分研发岗位出差、在家远程作业常态化，数据传输跨越企业边界。
- 合规要求提高：专利申报、项目投标、军工或行业标准要求加强对核心技术资料的保护。
- 内部防控薄弱：传统手段难以对研发人员操作进行全面、细致、可审计的防控。
- 软件使用合规隐患：部分终端存在安装盗版、破解或非授权软件的行为，带来法律与安全双重风险。

为解决上述痛点，Ping32提供一套以“文档加密、敏感内容分析、数据防泄漏与终端合规管控”为核心的一体化终端安全解决方案。

02

Ping32解决方案概述

核心理念

以“数据与终端双重安全”为核心理念，Ping32通过驱动层加密、敏感内容识别、数据防泄漏、软件资产管理等，构建企业级终端防护体系，保障研发资料、业务数据与终端环境的全方位安全。

终端数据
安全一体化

03

典型场景防护设计

3.1 设计文件透明加密，保障图纸安全

应用场景： 研发人员使用SolidWorks、AutoCAD、UG NX等专业软件绘制设计图纸，并将文件存储在本地终端、文件服务器或业务服务器中。这些设计文件包含了关键的技术资料，如产品结构、加工工艺、设备参数等，是企业的核心竞争力所在。在设计和研发过程中，文件需要与供应商、客户和其他外部合作伙伴共享，通常通过电子邮件、共享平台或U盘等方式进行。随着跨部门协作和远程办公的普及，设计文件的安全性面临更大的挑战。因此，确保设计文件在存储、传输和访问过程中的数据安全至关重要。

解决方案

- 自动透明加密

  对所有由SolidWorks、AutoCAD、UG NX等软件生成的设计文件进行自动透明加密。无论是存储在本地终端、业务服务器，还是外部存储设备中，文件始终保持加密状态。即使文件被盗取或丢失，未经授权的人员也无法读取文件内容。

- 无感知解密

  用户在使用受控的设计软件时，文件会自动解密并可供编辑。此过程对用户而言是无感知的，且不需要改变其操作习惯。这保证了研发人员在进行设计工作的同时，文件安全性不受影响。

- 非授权访问控制

  任何未经授权的用户或程序都无法访问加密文件。即便文件通过U盘、云盘或其他外部介质被复制，未授权设备将无法打开文件内容。这样可以防止机密文件通过不安全的途径泄露或被盗用。

- **离线加密权限配置**

  对于需要远程办公或出差的研发人员，系统支持离线加密权限配置。即使在没有网络连接的情况下，用户仍然可以访问、编辑和保存加密文件，所有操作均在本地加密存储，确保数据安全。出差过程中，文件在传输和使用过程中始终保持加密保护。

- **上传/下载自动加密**

  当设计文件被上传至PLM（产品生命周期管理）、MES（制造执行系统）等核心业务系统时，系统会自动解密文件，确保其可以正常处理。上传过程中，系统会确保加密文件的安全性；在文件从系统中下载时，文件会被自动加密，确保下载的文件也符合加密标准并在存储过程中保持安全。

- **文件外发包（Temporary Access）**

  对于需要与外部合作方共享加密文件的情况，Ping32提供了“文件外发包”功能。通过该功能，企业可以为指定的终端授权文件访问，并设置临时权限。具体控制包括：

  指定时间：可以设置文件的有效访问时间，超过该时间，文件将自动失效。

  指定打开次数：可以限制文件的打开次数，超过限制后，文件无法继续访问。

  禁止截图、复制、打印：即便文件被外发给授权用户，也可以设置禁止截图、复制、打印等操作，确保敏感内容不被泄露。此举能够防止外发文件在使用过程中的二次泄露和滥用。

Ping32
文件安全外发

通过透明加密、权限管理等技术有效防止文件外发导致的二次泄密

- **全生命周期保护**

  透明加密技术不仅保护文件在存储过程中的安全，还确保文件在整个生命周期内的安全性。这包括文件创建、修改、存储、外发、下载及最终销毁阶段。每个阶段都受到严格的加密保护，防止文件遭到未授权访问、泄露或篡改。

- **集成多层防护机制**

  为了进一步加强设计文件的安全性，系统支持动态水印和文件审计功能。在文件访问和传输过程中，水印可以动态展示用户身份，防止截图或恶意复制。系统还会记录每次文件操作的详细日志，支持对文件的操作历史进行追溯，从而实现全程审计与风险管理。

3.2 敏感内容识别与分类，精确防护关键数据

应用场景：在设计文档中，常常包含了关键部件的结构、加工参数、项目编号、内部代号、专利信息等敏感内容。这些信息通常涉及到公司的核心技术和知识产权，是企业竞争力的重要组成部分。为了防止这些敏感数据泄露或未经授权的访问，必须对文档内容进行智能识别、分类和保护。在日常研发工作中，设计图纸、BOM表（物料清单）、工艺流程卡等文档是频繁使用和更新的，这些文件中可能包含有害信息，如果未经保护，一旦外泄，将对企业造成严重的损失。

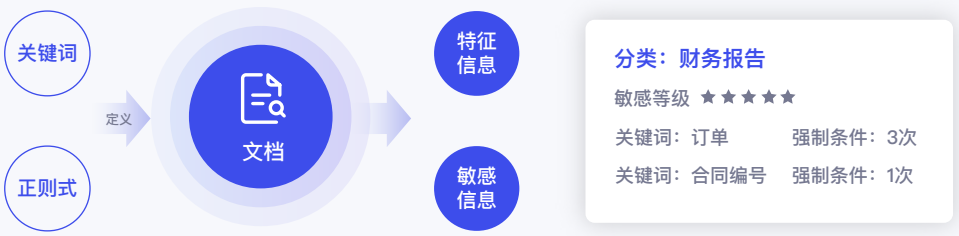
解决方案

- 多维规则识别

  基于关键词、正则表达式、文档指纹等多维度规则，Ping32能够智能识别图纸、BOM表、工艺流程卡、项目计划书等敏感文档。系统能够检测出文档中的特定内容，如项目编号、部件结构、客户信息、专利数据等，自动标记这些文档为敏感文件。

- 自动文档标签、分类和分级

  对识别出的敏感文档，Ping32会自动打上标签，并根据文件的敏感程度进行分类和分级。例如：将文档标记为“内部资料”、“涉密项目”、“关键技术”等，便于后续的管理和审计。分类和分级策略不仅支持手动配置，还能根据文档的内容和重要性进行自动化处理，确保每份文档都按照企业的安全策略进行精确管理。



- 可配置的保护策略

  对于敏感文档，Ping32支持灵活配置智能加密、打印限制、外发控制、复制粘贴限制等策略。可以针对不同级别的敏感文档设置不同的保护措施。

  智能加密：针对高敏感级别文档，自动进行加密处理，确保文件即使被盗取也无法读取。

  打印限制：对敏感文档实施打印权限控制，禁止未授权用户打印敏感文件，减少文件

泄露的风险。

禁止外发：禁止通过邮件、即时通讯软件、U盘等途径将敏感文档外发，确保数据仅在授权范围内流转。

禁止复制粘贴：对文档的内容进行智能识别，限制在复制粘贴时将敏感信息泄漏到其他非授权文档中。

3.3 泄密途径管控全面覆盖，封堵多途径泄密风险

场景举例

- 员工将设计图通过QQ或企业微信发送给个人邮箱；
- 使用U盘将项目文件带出公司；
- 打印大量图纸内容进行外发或归档；
- 上传文档至百度网盘等第三方云存储。

解决方案

- Ping32 可全面识别并审计终端用户通过 QQ、微信、邮箱、浏览器等常见渠道进行的文件外发行为。系统可基于设定的规则，对传输内容进行智能判定：

  内容识别维度：支持对文件内容进行深度解析，识别是否包含敏感关键词、敏感段落、特定正则规则、图纸特征、个人信息等。

  格式类型匹配：可限定拦截特定格式类型（如 Office、PDF、CAD、图像文件等），按需精细化管理不同业务场景。此外，Ping32 还可溯源原始文件格式，确保即使用户尝试将敏感文档改名或伪装为普通格式（如将 .docx 改为 .txt），系统依然可以识别真实格式并按规则拦截，从而实现精准、不可绕过的文件类型控制策略。

  传输途径识别：精确识别传输通道（如 QQ、微信、Outlook、Web邮箱、各类浏览器、网盘上传操作），确保不遗漏高风险外发途径。

当命中上述规则时，系统可自动拦截文件外发操作，并同步记录完整行为日志，支持行为溯源与风险告警。

外设管控：禁止接入未经授权的U盘、移动硬盘；支持专用加密U盘使其只能在企业内部使用并记录读写日志；

水印与截屏防护：在受控应用中强制展示用户身份动态水印，阻止屏幕截图和虚拟打印等操作。

打印管控：支持对打印操作进行审计、动态水印添加及按文件密级控制权限；可基于敏感内容识别拦截打印行为，并阻断虚拟打印机操作。

3.4 软件合规管控，防止盗版风险与安全漏洞

场景举例

- 员工擅自安装破解的设计软件、绘图工具或插件，企业因此面临法律责任、信息泄漏和IPO审查等多重风险。

- 企业往往难以及时掌控员工的违规行为，许多盗版使用行为由员工私自实施，最终却由企业承担全部法律后果。
- 大量盗版软件存在向境外IP回传数据的情况，极可能被植入木马、后门，带来严重的信息安全隐患。

解决方案

为应对盗版软件引发的法律风险与信息安全隐患，Ping32提供业内唯一的专业级盗版软件检测解决方案，已在制造、设计、能源、军工等多个行业客户中成功落地，并获得一致好评。该方案基于先进的机器学习算法与终端防护机制，实现对盗版软件的精准识别与自动化控制。

核心能力与优势包括：

- 覆盖广泛的识别能力

  基于先进的机器学习模型与行为特征识别技术，Ping32 已可精准识别 1000+ 种常见盗版软件，覆盖 Adobe、SolidWorks、Autodesk CAD、西门子等主流设计、建模、工业类工具。系统识别能力持续迭代升级，可快速适配更多垂直行业的专业软件，帮助企业有效防范合规风险与资产浪费。

- 响应式适配机制

  针对客户环境中尚未支持的新型或行业特殊软件，Ping32 提供 48 小时定向适配机制，可快速分析软件行为特征并下发识别规则，确保系统始终具备高覆盖率与场景适应性。

- 自动化的处置能力

  系统支持对识别出的盗版软件进行策略化、自动化响应，包括但不限于：

  自动禁用可疑程序运行

  断网隔离终端设备

  弹窗告警提示用户违规行为

  自动通知管理员并生成事件报告

  通过“识别 → 控制 → 追踪”的闭环机制，Ping32 实现了对盗版软件使用行为的即时阻断与可追溯管理，帮助企业从容应对合规审计与法律风险。

04

平台化管理与审计能力

聚合搜索：让审计从“找不到”到“瞬时命中”

在终端安全与数据防泄漏领域，审计能力直接决定了问题定位的效率与响应速度。Ping32突破传统架构，构建了业内领先的“聚合搜索”能力，为安全审计带来质的飞跃。

4.1 Ping32聚合搜索的五大核心能力：

- 无需预设关键词，按需即时搜索

  管理员可随时输入感兴趣的关键词（如“138****8888”或“ZJ-2024合同”），系统即可从所有审计数据中高速提取并聚合相关记录，操作简洁，体验极佳。

- 极速响应，搜索级数据库架构

  相比竞品仍依赖传统关系型数据库（如SQL Server、MySQL），Ping32采用搜索引擎级数据库架构，从根本上解决了数据查询效率低、格式割裂等问题。

  查询效率：检索1000万条审计数据，Ping32仅需0.5秒，竞品平均耗时达10分钟以上。

- 支持检索文档正文内容

  除文件名外，Ping32可深度分析.doc/.pdf/.xlsx等常见文档类型的正文内容，快速锁定合同编号、客户名称、参数信息等隐藏数据。

- 集成OCR图像识别，打通图片检索盲区

  针对截图、扫描件等图像泄密行为，Ping32可通过OCR技术将图片中识别出的文字内容纳入聚合搜索范围，实现“图文一体化审计”。

- 分布式搜索架构，支撑PB级实时查询

  Ping32构建了分布式搜索集群，轻松支撑大中型企业PB级审计数据的实时调取与多维检索，保障查询时效性与稳定性。

Ping32
聚合搜索

4.2 行为审计与追踪

自动记录所有与文件相关的操作日志（如打开、修改、复制、删除、打印、外发等）；
支持生成可视化报表或触发异常告警，例如某员工短时间内集中导出图纸的行为；
可对任意可疑行为回溯原始文件、操作者身份、终端信息与操作路径，全面支撑内部稽查与责任认定。

4.3 策略集中配置

提供统一的可视化策略管理平台，支持按角色、岗位、终端或项目组灵活配置加密策略、通道权限、外发限制等；
与企业AD域无缝集成，实现组织架构同步、策略继承与分级授权，便于大型企业集中运维与权限管控。

4.4 合规性支持与日志留痕

满足 ISO 27001、等保2.0、军工保密资质等数据合规要求；
所有关键操作、策略变更、告警触发均可完整留痕，形成可导出、可审计的合规日志；
支持对接第三方监管与合规系统，如SIEM、安全态势感知平台、数据资产审计平台等。

05 | 客户收益

- All–in–One一体化价值

  统一高效：一套平台整合加密、防泄密、终端管控、审计等核心能力，显著降低多系统采购与管理复杂度及成本。

  用户体验：新一代 Ribbon 风格 UI 界面，美观大气，功能布局合理，用户可以通过直观的标签和菜单快速找到所需操作。

  全局可视：打破数据孤岛，安全事件统一关联分析，提供全景视图，提升威胁响应效率。

  联动防护：各模块深度协同（如盗版识别–>自动处置–>审计追溯），构建闭环纵深防御，提升整体有效性。

- 筑牢核心资产防线

  透明加密与智能防护显著降低设计图纸等研发成果外泄风险。

- 实现全流程透明审计

  对研发人员操作、文件流转、软件使用进行可视化追溯，提升管理规范。

- 加密无干扰，协作更安全

  研发操作无感知，外发文件自动受控。

- 规避泄密多重损失

  有效防护关键数据，减少经济损失，维护客户信任与品牌声誉。

- 消除盗版合规风险

  精准识别管控盗版软件，规避法律纠纷与安全隐患。

06

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

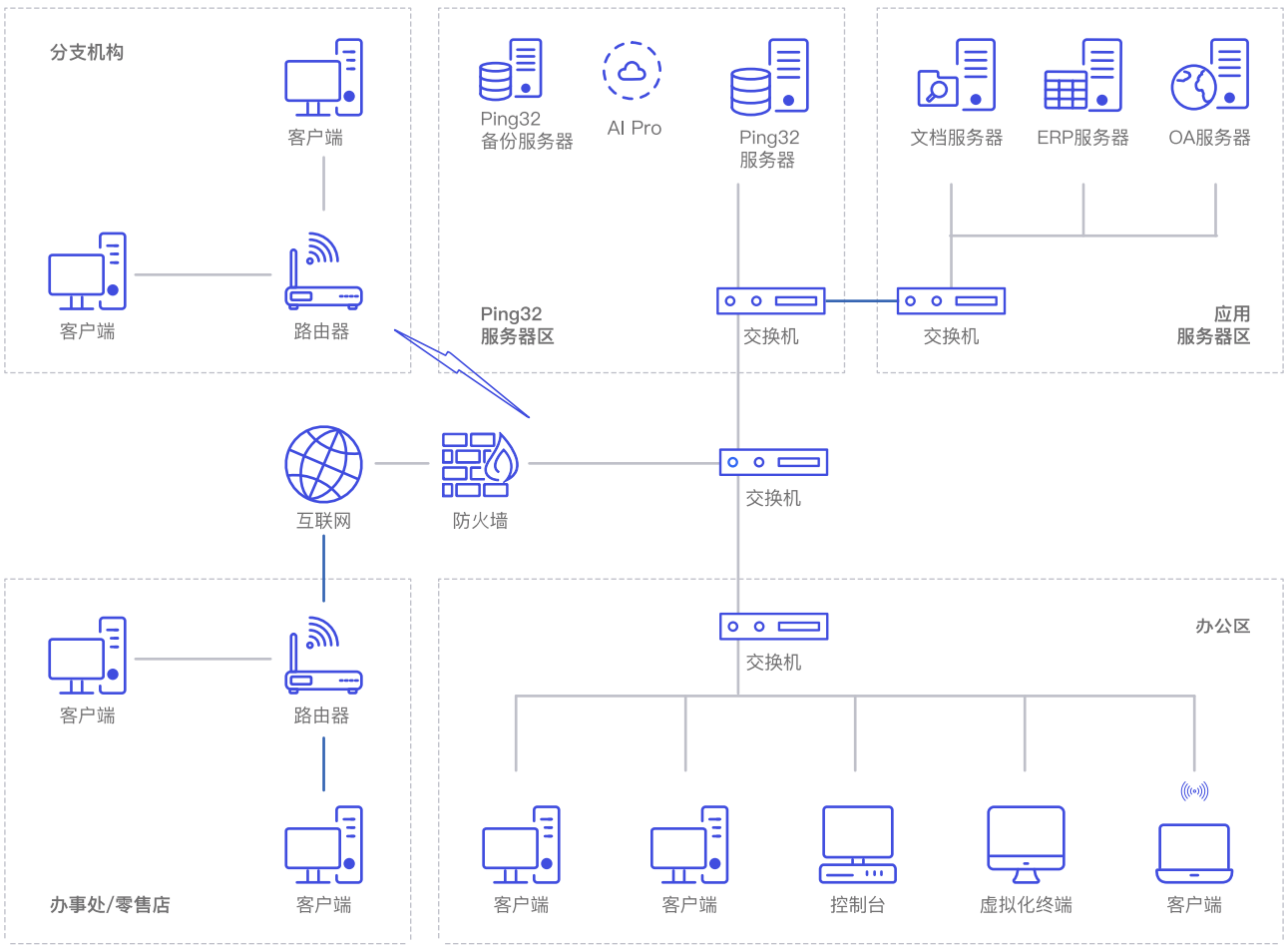
安装在被管控的计算机上，执行管理者设定的管控策略，采集计算机运行的各项数据并上传给服务器。

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

安装在系统内的物理服务器上，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。



Ping32在技术架构上的特性

- 云服务与本地代码结合的混合架构：

  Ping32采用了云服务与本地服务结合的架构，充分利用云端的强大计算与存储能力进行日志分析、数据处理与威胁监控，同时保持本地部署的安全性，确保敏感数据在本地环境中的保护和管理。这种架构能够灵活应对各种企业需求，提升系统的可扩展性

- 数据安全与隐私保护

  本地部署的服务确保了对敏感数据的严格控制与保护，避免数据泄露的风险。云端架构专注于数据分析与处理，不存储敏感数据，保证了数据隐私和合规性。通过加密传输和本地存储的双重保障，确保数据的安全性与完整性。

- 高效的日志分析与实时监控：

  云端系统提供强大的日志分析功能，能够对各类日志数据进行实时分析，快速识别潜在的安全风险和异常行为。通过云端的强大计算能力，Ping32能够在海量数据中精准挖掘出安全威胁，为企业提供高效、全面的安全监控和预警。

- 分布式架构与可扩展性

  Ping32采用分布式架构，能够支持大规模企业环境中的多终端管理。系统可根据需求灵活扩展，满足不同规模企业的需求，确保在复杂环境下仍能保持高效稳定的运行。

- 智能化运维与自动化管理

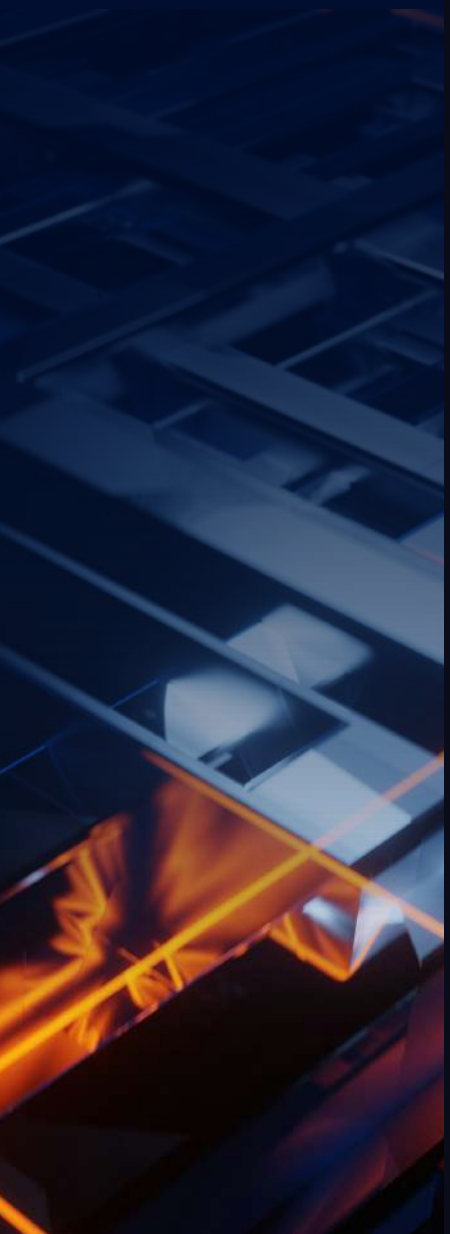
  Ping32的架构设计注重智能化运维与自动化管理，通过自动化的威胁识别、日志分析与事件响应，减轻IT团队的负担。管理员可通过统一控制台进行集中管理和实时监控，提升响应速度和管理效率。

- 灵活的部署选项

  支持云端、私有云和本地部署等灵活的部署方式，能够根据企业的不同需求和IT环境进行定制化部署。无论是在需要严格控制本地数据的环境中，还是希望利用云端计算能力的企业，Ping32都能提供最佳的解决方案。

07 | 总结（结语）

Ping32精密零部件制造行业数据防泄漏与软件合规管理解决方案已广泛应用于机床制造、轨道交通、工业设备、工程机械等精密零部件制造类企业，成功帮助客户构建了研发核心资产与终端环境的“最后一道防线”。通过文档加密、数据防泄漏、敏感内容分析、软件合规与行为审计等手段，为企业技术成果构建了可落地、可运营、可审计的终端安全闭环体系。



联系我们

support@nsecsoft.com

400-098-7607

安在软件

济南高新区经十路7000号汉峪金谷
A5-5 政金大厦6层

nsecsoft.com