Ping32

文档透明加密
全方位数据防泄漏

五大核心价值观，在我们的产品中均有体现。

山东安在信息技术有限公司（安在软件）

山东安在信息技术有限公司（安在软件）是拥有完全自主知识产权的信息安全解决方案供应商，作为中国信息安全领域的创新者，安在软件通过Ping32终端安全管理系统等产品，为企业提供数据防泄漏、统一终端管理、生产力提升一体化管理平台。

安在的产品、解决方案和服务具备高度的弹性和兼容性，被广泛应用于政府、军工、运营商、医疗、金融、教育、能源、制造等行业，既能满足小微企业的需求，也能为中大型企业提供定制化服务，为国内10000多家用户、超过200万台终端提供数据安全保障。

安在通过完善的以客户为中心的研发、客户、销售、市场、渠道组织体系，在北京、上海、广州、深圳、杭州各大区域设有分支机构，覆盖全国的营销及服务战略体系，确保向客户提供提供满意的产品与服务。

营销服务体系

安在凭借前瞻的创新理念、强大的研发实力和业内最全面、丰富、完善的产品线，获得行业内外的高度认可。总部位于山东，以北京、上海、深圳、成都、杭州、沈阳、长沙八大服务中心覆盖全国，为客户提供便捷、便利、高效的服务支持。

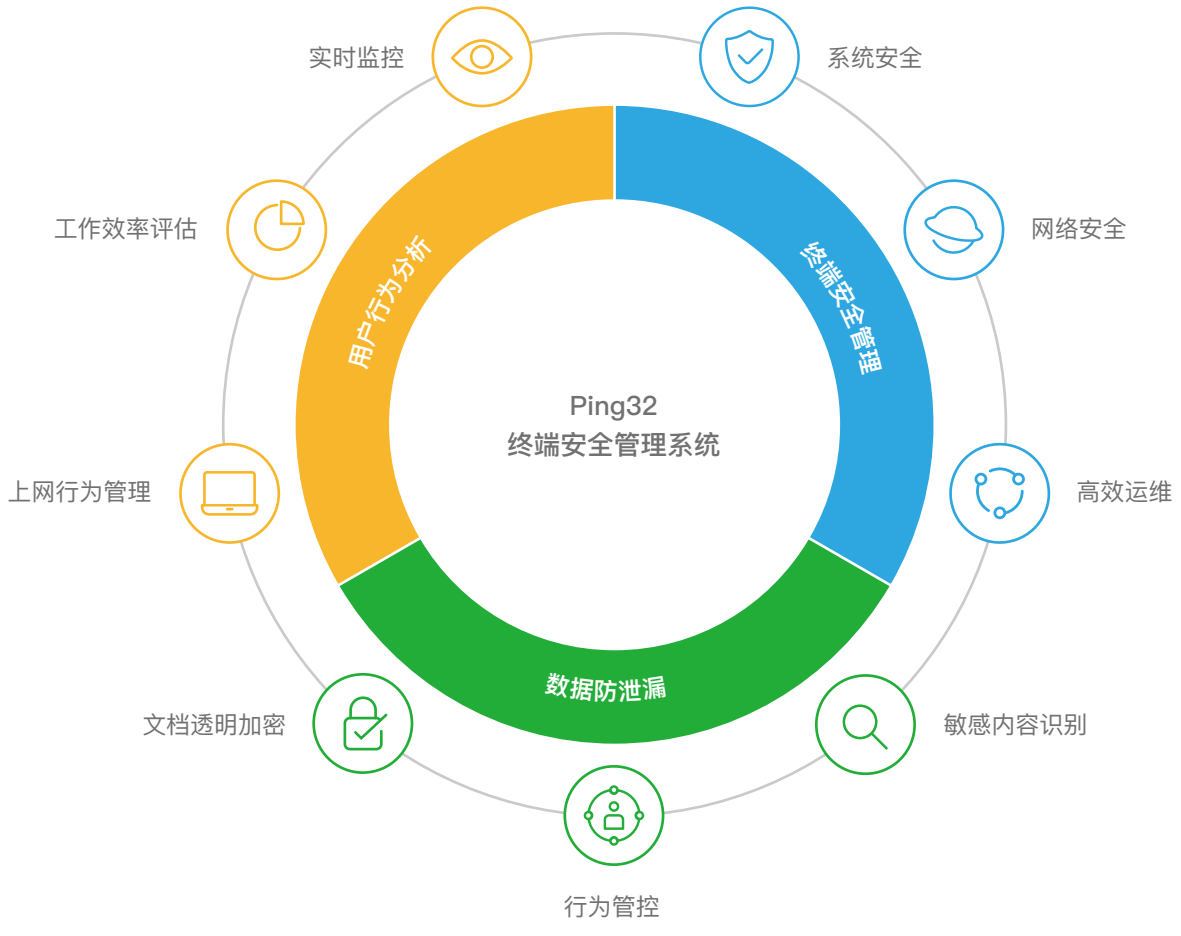
- 创立于2014年专注企业终端安全管理与数据防泄漏
- 自主研发文件透明加密与统一终端管理一体化平台
- 超10000家用户选择，超200万台终端部署
- 八大服务中心覆盖全国，提供高效的服务支持

Ping32 山东总部　　Ping32客户、合作伙伴遍布海内外

企业信息安全
一体化管理平台

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，包括文件透明加密、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。

通过Ping32可以集中管理和维护全网终端计算机，提高IT运维人员工作效率。通过对员工上网行为的监管，防范危险泄密行为，基于先进的机器学习技术，进而对工作效率进行精准评估，提供智能化的工作效率提升建议，提高企业生产力。



数据泄漏事件

2014

20G

支付宝离职员工泄漏公司数据，并且贩卖20G用户资料。

2015

10,000,000+

“老干妈”配方遭离职人员外泄，涉案金额高达千万元人民币。

2016

50亿

京东50亿条公民信息泄漏，损失数百万，原因是内部泄密。

2018

8, 000+

可口可乐8000名员工的个人信息遭到离职员工违规挪用。

2020

400,000+

圆通快递40万条个人信息遭圆通内部人员非法泄漏。

数据泄密的危害

数据泄密的危害

声誉、信任度受损

一些行业的数据、信息泄漏，会使企业声誉及信任度严重受损，引发舆论危机。

违反法律法规

一些国家涉密领域的数据泄漏，会导致企业违反保密法、网络安全法等法律法规。

知识产权、核心技术流失

代码、技术图纸等数字资产的外泄，会导致企业失去核心竞争力。

巨额财产损失

绝大多数数据泄密事件，市场人员违规，都会给企业造成直接或间接的财产损失。

客户、合作伙伴流失

客户、合作伙伴资料的泄密，一旦被竞争对手获取，会直接影响企业的健康发展。

内部动荡

一场泄密事件背后必然有企业内部各种问题，当企业发生内部数据泄漏时容易引起员工的不信任感，继而影响企业的整体的发展。

数据防泄漏

文档透明加密

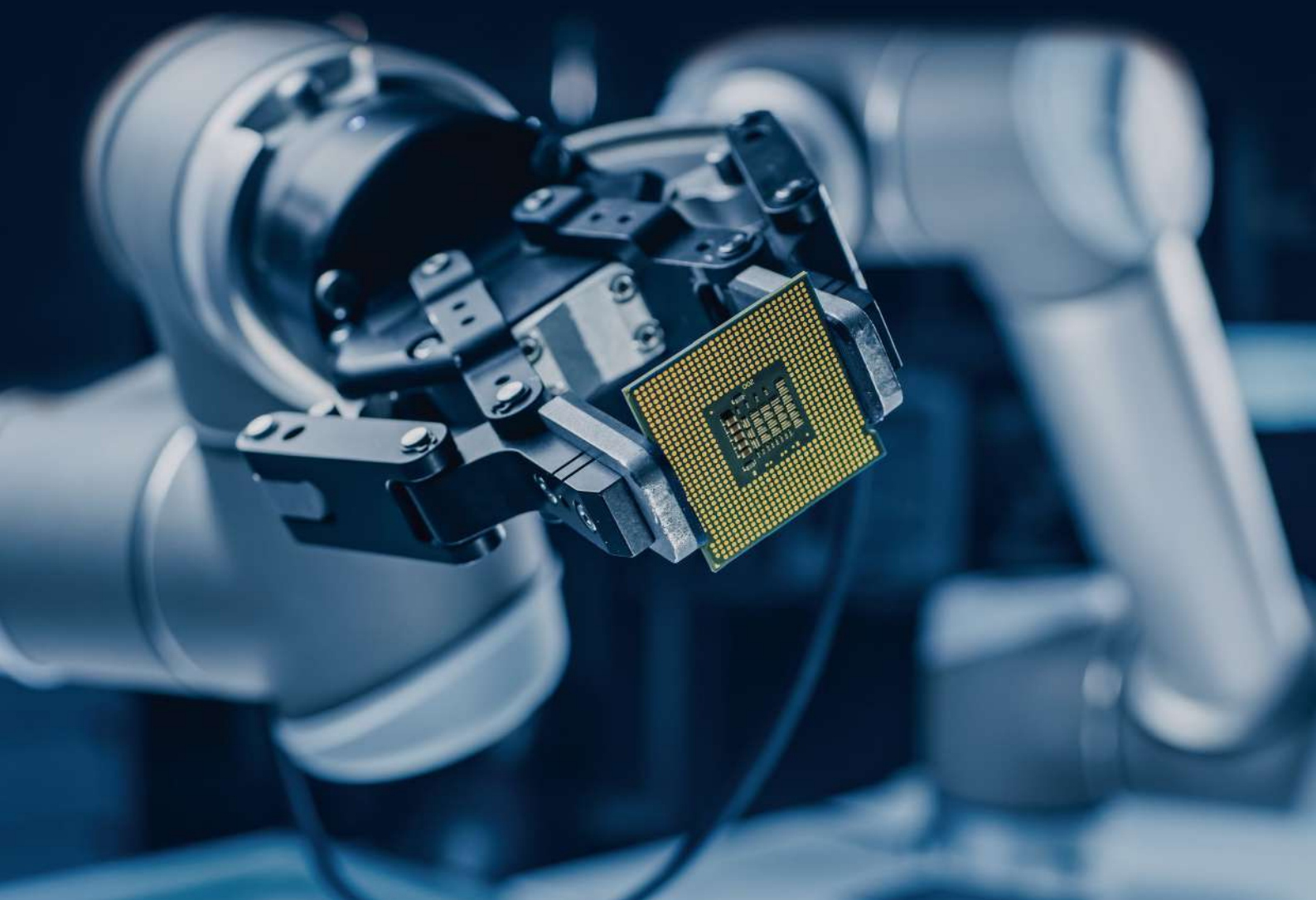
Ping32数据防泄漏以文档透明加密为核心，采用新一代的文件透明加密内核，贯穿文档全生命周期，在不影响员工正常办公习惯的前提下，为企业构建严密的数据泄漏防护体系，即使数据脱离企业，也能做到有效管控。

安全管控

Ping32针对职场道德、内部威胁等因素，采用主动发现-防护的策略，对可能存在泄密风险的途径进行安全防护，及时阻断泄密行为。构建数据安全防护边界，防范全场景的数据泄漏行为，保护企业核心机密，

文档透明加密
强力守护企业核心竞争力

Ping32以文档透明加密为核心，结合敏感内容识别与办公行为管控，构建数据安全防护边界，防范全场景的数据泄漏行为。



Ping32文档透明加密内核

Ping32文档透明加密内核（PFEK：Ping32 File Encryption Kernel）是安在软件通过其在数据安全领域多年的的技术积累、沉淀，基于硬件虚拟化，内核层文件系统隔离微过滤器等技术构建而成的新一代文件透明加密内核。通过用户自定义策略，Ping32支持基于文件的实时访问的透明加解密，数据防泄漏等多种数据安全解决方案。

Ping32文档透明加密内核具有以下特性：

- 按照用户自定义的策略规则，对于新建文件实时透明加密，对于已加密的文件实时透明加/解密。整个过程用户无感知，不影响用户的使用习惯，

- 基于驱动层的透明加密技术，在Windows上，Ping32使用受微软认可的文件系统隔离微过滤器(Filesystem Isolation Minifilters)来实现缓存控制以及同时提供文件数据的原始视图和解密视图。杜绝任何文件损坏事件发生。

- 使用与FIPS 140-2兼容的Microsoft CNG库实现密钥存储和加密算法，CNG工作在内核模式下，提供出色的性能保证。同时，支持国密标准等自定义加密算法。

Enigma是二战时期德国使用的用于加密战争情报的转子机械加密机。迄今为止，加密依然是最有效的用于保护数据、通讯安全的手段之一。

文档透明加密核心功能

新一代文档透明加密技术

基于硬件虚拟化，内核层文件系统隔离微过滤器等技术运行稳定。

支持国密，AES等高强度加密算法，安全可靠。

内置丰富的受控应用。

Ping32文档加密系统基于内核驱动层透明加密技术，对企业内部敏感数据分级管理，针对核心数据、非核心数据实现不同程度的加密保护，实现对外发文件可控、可查、可管理，有效防止企业敏感数据泄漏，实现电子文档的数据安全。

- **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。

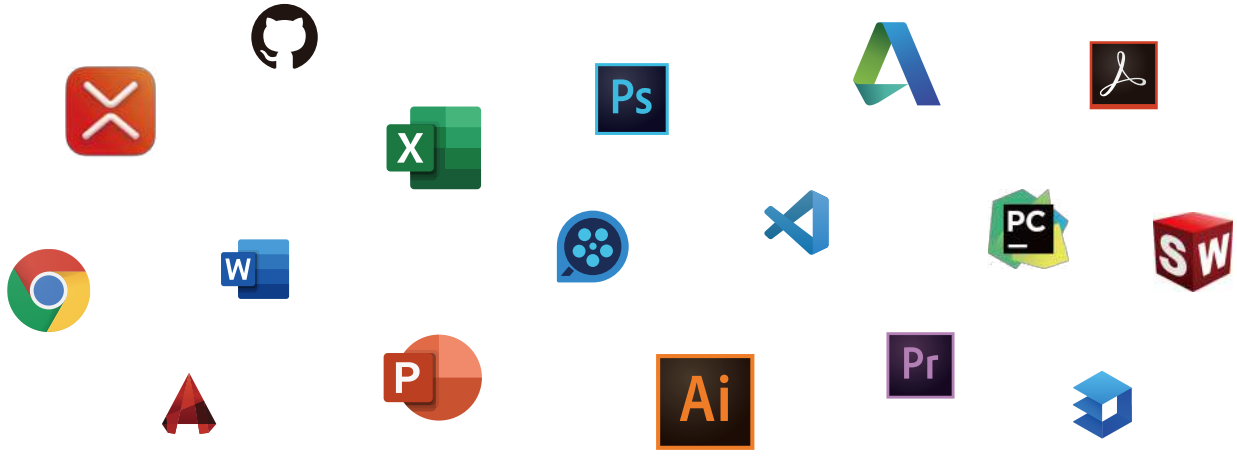
- **手动加解密**

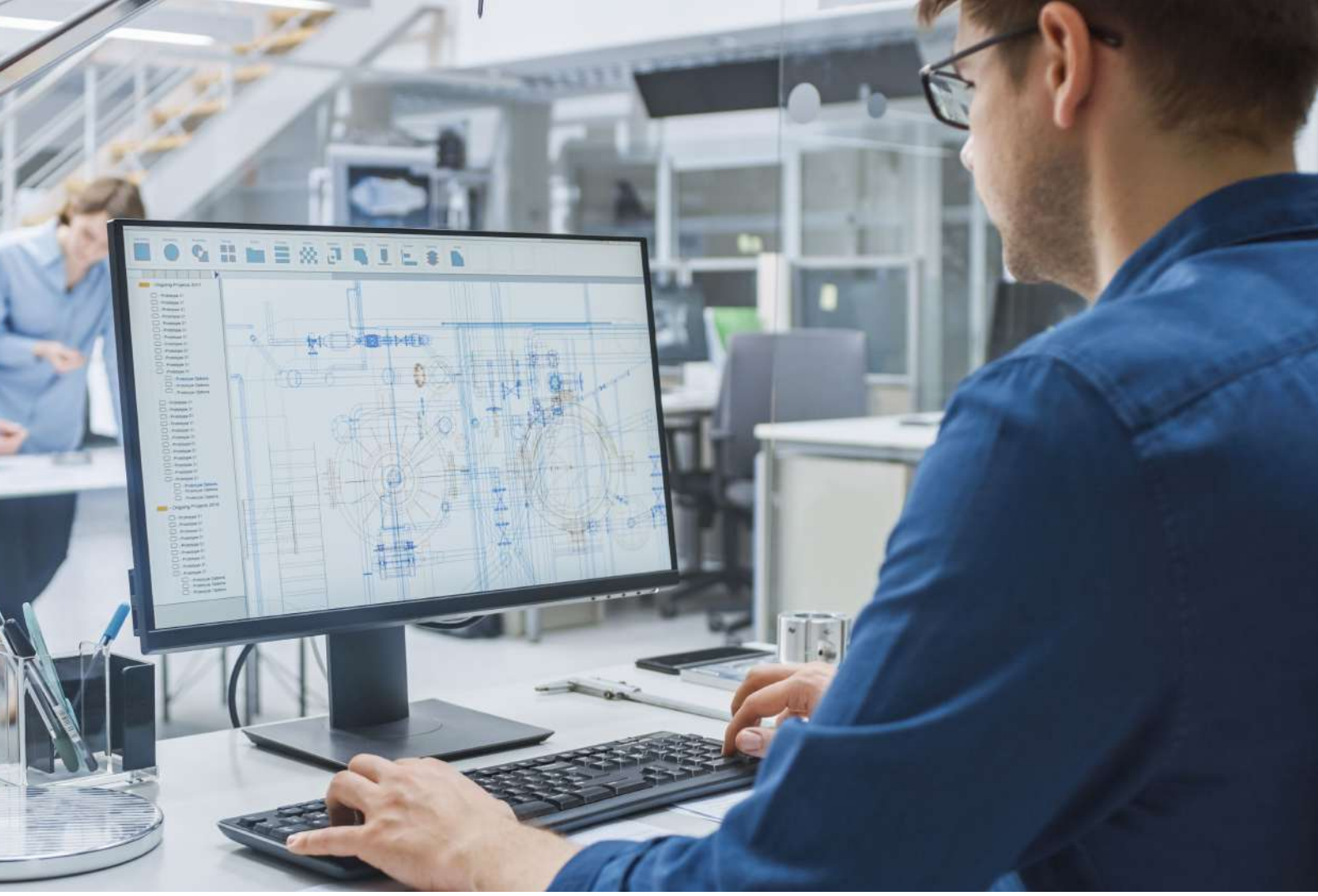
数据使用部门主动对敏感数据加密，防止误操作、外部窃密导致的数据泄漏。

- **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。

丰富的受控应用





386 万美元

2020年 7月，IBM Security发布《2020年数据泄漏成本报告》，揭示了数据泄漏事件给企业造成的平均成本为386万美元，有80%的事件导致了客户个人身份信息暴露。

• 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，识别散落在企业不同位置的机密文件，并对其强制加密，集中管控，保护企业核心数据。

• 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。

• 加密审计

Ping32可以实时记录用户通过透明加解密创建加密文档、使用加密文档，以及主动对文档加解密的操作，记录文档从创建到销毁的整个过程，确保核心数据文件的使用在企业正常管理之下。

安全域

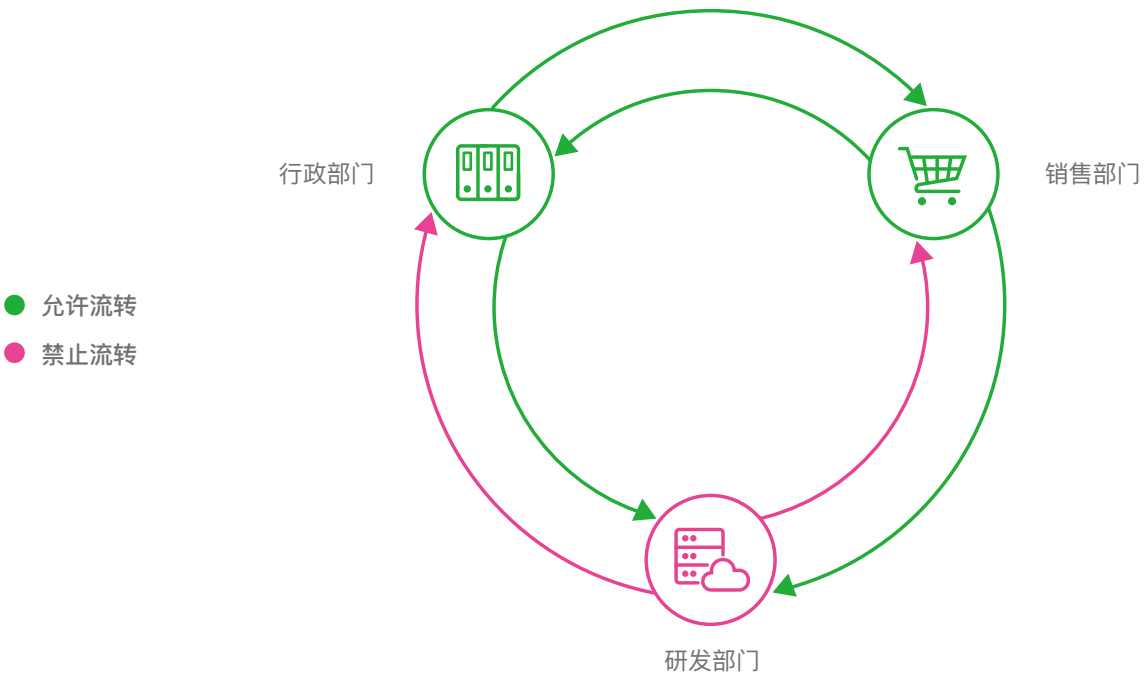
Ping32安全域管理可以设置不同的文件安全域以实现部门之间的加密数据需要安全隔离的管理要求，控制文档流转范围，确保文档在特定范围内使用，比如在财务部、人事部等创建不同的安全区域，防止财务报表流转到其他部门、员工薪酬信息在公司任意查阅。根据用户自定规则，创建符合自身组织机构的安全域，赋予不同人员的操作权限，提高文档安全性，可管理性。

• 安全域

根据企业不同的部门，创建不同的数据安全区域，从而确保不能跨部门访问加密文档。

•安全域权限管理

赋予用户对不同安全域的访问权限，根据用户、部门的涉密程度，部署梯度式的加密防护，控制用户对不同安全域的打开、解密、打印等权限，对核心部门和普通部门的数据分级防护，确保核心文件安全。



密级

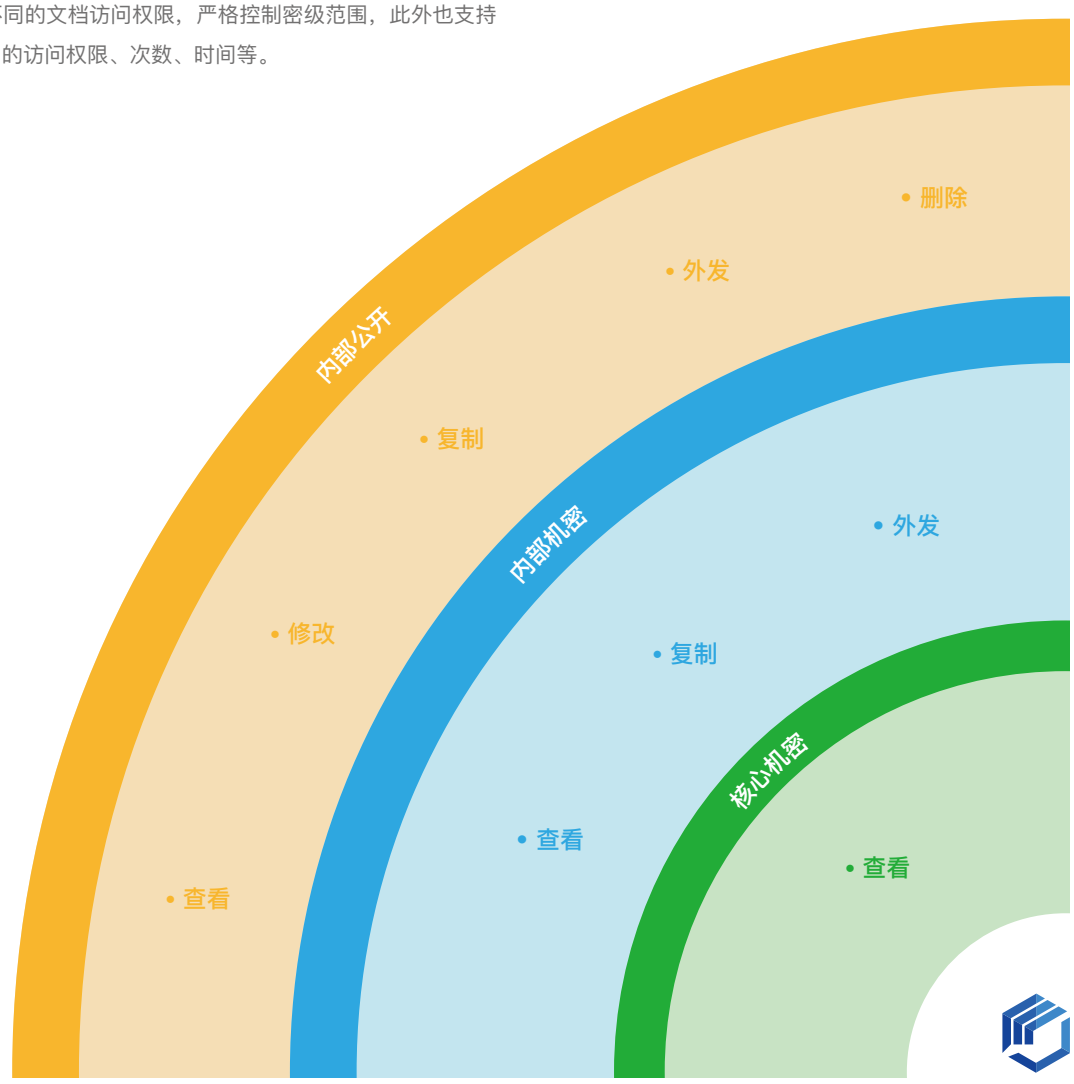
Ping32根据企业各类组织机构与数据密级程度，控制企业核心数据的访问权限，帮助企业加以针对性、灵活性的管控，有效防止非授权访问与越权访问企业敏感数据造成的数据泄漏，实现多元化、安全可控的业务运营。

- **密级权限**

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。

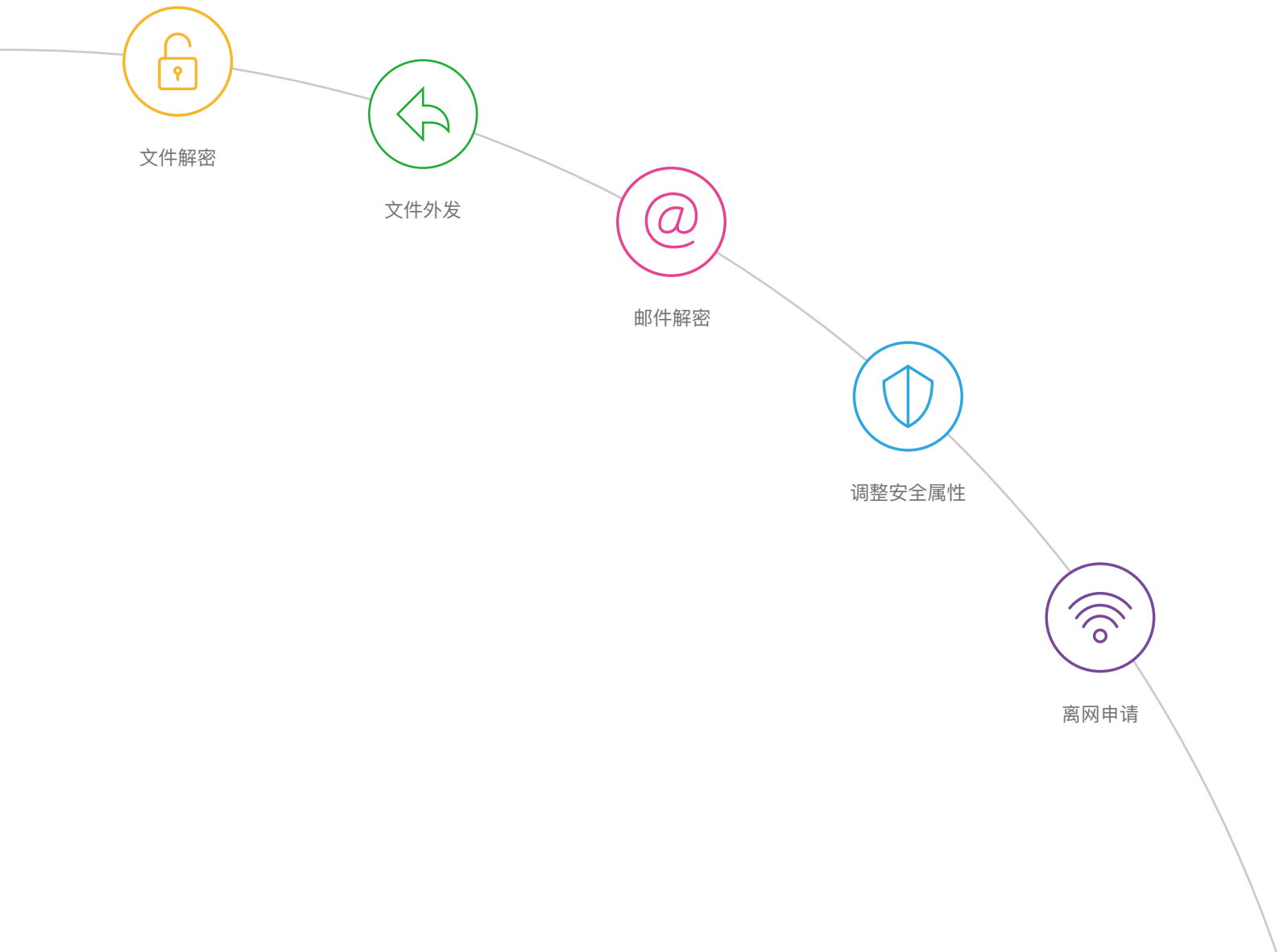
- **访问权限**

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

有时，难免需要将一些文件外发、解密或发送邮件。流程审批提供了便利的审批服务，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文档加密提供了多种离网办公权限管理。

- **离线时长**

预先设定离线时长，当客户端和服务器因各种原因断开连接时，确保用户可正常使用密文，保证正常办公状态。

- **超时审批**

为应对多变的工作环境，员工离网办公超出预期时间，但仍需要离网办公时，可通过超时审批申请延长离网时间，确保业务持续运行。

文档内容防护

科学有效地管理内部文档

Ping32帮助企业对内部文件精准识别和分类，对高价值的数据提供更有针对性的保护策略，即使文档脱离企业，也能做到有效管控。

文档智能归类

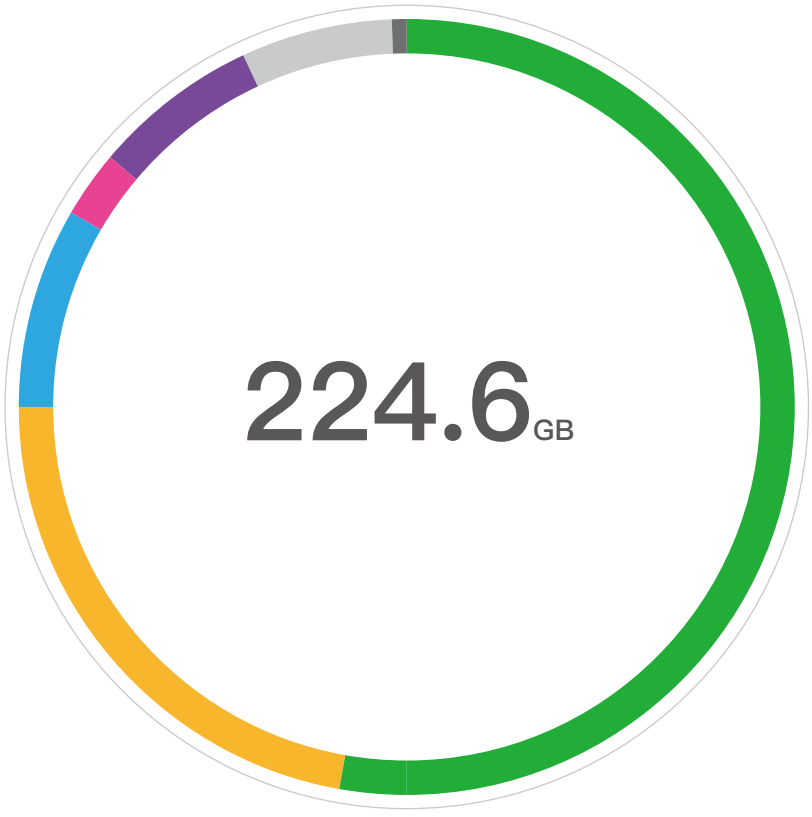
数据泄漏事件遍布于基础设施行业和大型企业，虽然部署了安全防护，但泄密依然源源不断。传统的防护策略已经不完全适应当下的数据安全态势。

企业应更加注重数据集中治理、分类分级防护，建立内部的信息化文件管理库，Ping32文档智能归类系统主要采用自然语言处理、机器学习等技术对分布在不同终端上的文件扫描分析，实现智能归类管理。

- **基于自然语言与机器学习**

不仅是简单的分类识别，更是集深度的机器学习技术、自然语言处理算法有机结合，深度分析文档内容，智能聚类、分类处理数据，进一步提升文档归类的准确性。

智能化的数据归类



机密数据

研发代码	53%
设计图纸	22%

核心数据

商业合同	9%
财务报表	7%
会议记录	5%

普通数据

行政制度	1%
产品资料	3%

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。

• **文档安全查看工具**

Ping32外发文档查看器可以隔离正常办公环境，文件外发时连同Ping32外发文档查看器打包外发，并授权外部人员的使用权限，超出一定时间后自动加密，防护文档内容，防止二次泄密。

• **外发文档权限控制**

文档外发工具可以确保文档在需要流传到外部的场景下安全可控。你可以用Ping32文档外发工具制作外发包，支持设置：打开次数、失效时间、复制权限、截屏权限等参数。外部打开此文件时Ping32会构建一个安全受限的沙盒环境，确保你的文档不存在泄密风险。

• **外发审计**

Ping32可以审计外发文件的行为，提供完整的文件外发日志，包括外发人员信息，外发文件的使用权限信息，确保行为可追溯。

灵活的使用权限控制

文档备份

驱动级的安全防护

Ping32针对备份文档采用了驱动级的安全防护，可以有效防止未授权的访问及勒索病毒攻击。

Ping32文档备份可以对企业散落在各处的文件、数据进行集中备份管理。Ping32支持全盘扫描备份、增量备份，并支持多达1024个历史版本。除此之外，为了降低存储成本，Ping32支持分布式部署，以及与腾讯云、阿里云等云服务商对象存储服务进行整合。

- **实时的数据保护**

Ping32可以提供整机文档的备份还原服务，防止意外的文件损坏、误删、感染勒索病毒等威胁。除此之外，Ping32支持实时捕获全盘或指定路径的文件变化，并进行实时备份，这并非定时扫描文档，因此可以显著降低磁盘I/O。对于变化的文件，Ping32支持增量备份，提升备份效率的同时，可以显著降低存储成本。

- **多达1024个历史版本**

Ping32支持对同一文档进行多版本备份，多版本备份可以进一步巩固企业的数据安全，也方便随时进行历史回溯。你可以随时导出任意版本的历史文件，进行秒级恢复。Ping32支持多达1024个历史版本，对过期版本进行自动清除，节约存储空间。

- **丰富的可视化报表**

Ping32文档备份支持丰富的可视化报表，你可以直观了解备份系统的各项数据，比如：备份日志、备份文件大小、各种类型的备份文件的比例等。

- **支持网络存储**

你可以灵活选择备份位置，Ping32不仅可以支持备份到指定的磁盘分区，也可以备份到网络存储（比如NAS设备、共享分区等）、云服务（腾讯云、阿里云等）等位置。Ping32对于备份文件提供驱动级的防护服务，不仅可以防止未授权的访问，并且建立了牢固的安全防线，使你免受勒索病毒的威胁、困扰。

全面的数据泄漏防护

Ping32数据防泄漏 (DLP：Data Loss Prevention) 解决方案采用了主动发现、防护的策略，可全方位保护你的敏感数据。

移动存储安全

移动存储设备安全管控

• Ping32可以规范、限制U盘、移动硬盘等移动存储设备的使用，为移动存储设备设置不同的权限，比如：只读、完全禁止使用等。这不仅切断了通过这类设备传播病毒的途径，更是杜绝了信息泄密风险。想为不同的移动存储设备设置不同的功能？没问题，通过Ping32 的移动存储设备授权，你可以为不同的移动存储设备设置不同的权限安全、便捷两不误！

移动存储设备加密

• 不想完全禁止移动存储设备的使用，但是又害怕外带导致机密文件泄漏怎么办？Ping32的移动存储加密即是解决之道。Ping32支持AES-256、Blowfish等高强度加密算法，可以确保内部机密文件无法通过U盘等移动存储设备外带泄密。最重要的是整个过程完全透明，用户无感知，丝毫不影响便捷性。

外接设备管控

• 除了移动存储设备外，打印机、刻录光驱、蓝牙、便携WIFI等设备都可能使你的网络面临安全风险。通过设备管控你可以为不同设备做细粒度的权限划分，规范设备的使用，杜绝非法设备的接入。一夫当关，万夫莫开！

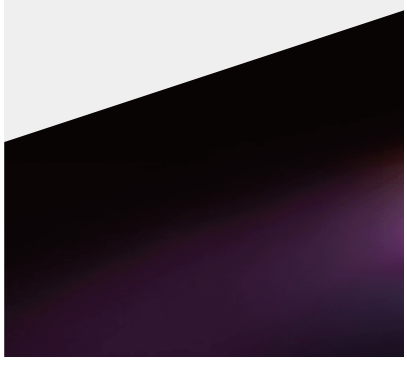
屏幕安全

计算机屏幕是最直观的人机交互界面，通过对屏幕进行安全监管（如：屏幕水印、禁止截屏、实时查看屏幕、智能定时截屏等功能），往往可以更直观地查看、管控存在的内部威胁风险。

水印

Ping32可以对敏感的屏幕内容和打印敏感的文档标记水印。水印是一种可以有效防止用户通过截图、拍照、打印泄密的技术手段。Ping32的水印管理可以对灵活设置各项参数，比如：水印内容、字体、倾斜度、疏密程度等参数。震慑非法泄密行为。

- 屏幕水印
- 窗口水印
- 文字
- 二维码
- 点阵



防截屏

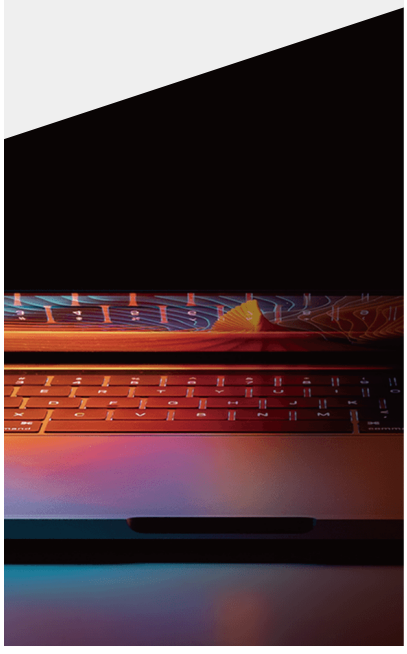
Ping32防截屏模块，可以有效保护屏幕内容不被违规、非法窃取。防截屏基于驱动级的GDI防护技术，有效防护各类截屏操作，审计用户试图截取的屏幕内容。追溯泄密场景，杜绝敏感内容通过截取屏幕泄密。

- 聊天软件
- 浏览器
- 截屏软件
- Print Screen

屏幕监控

通过Ping32，您可以远程查看屏幕的实时画面，方便您清晰地了解用户正在做什么，是否从事和工作无关的事，以及是否存在违规行为。

- 智能截屏
- 屏幕录像
- 实时屏幕



打印安全

Ping32支持对本地、网络、共享、虚拟打印机的使用权限进行控制，监控用户打印行为，结合打印水印附加技术、打印快照获取，记录打印操作关联的用户信息，包括：涉密终端、涉密人员、打印时间、涉密打印机等信息，对打印行为精准定位，有效追溯，有效防止涉密信息通过打印的方式向外泄漏。

• 打印管控与审批

管控用户对各类打印机的使用权限，限制非法与浪费公共资源的打印行为，员工可通过打印审批向管理员提交打印申请，管理员审核后方可使用，降低打印成本，防止机密信息打印外泄。

• 打印水印

在纸质文档上显示自定义水印，如添加企业logo加强企业文化宣传，添加包含用户信息的文字水印震慑、追溯泄密行为。

文件外发审计

52%

52%的企业承认：员工是他们最大的IT安全弱点，粗心的行为或缺乏知识会严重损害企业的IT安全战略。

通过电子邮件私下联络客户做私单。

通过微信将客户资料发送给竞争对手。

将公司内部文件备份到网盘。

离职将机密文件拷贝到U盘带走。

Ping32可以记录包括存储于服务器、硬盘、光盘、移动盘、网络盘等各种位置的文档从创建到消除整个生命周期内发生的所有操作。此外通过泄密追踪分析引擎可以对用户的日常操作进行深度分析，识别存在泄密风险行为，包括但不限于通过即时通讯、电子邮件、网盘等途径外发文件，将敏感资料拷贝到U盘带走等场景。

- **泄密追踪**

可以对用户存在泄密风险的行为进行跟踪、追溯。无论用户将图纸、代码拷贝到U盘带走，还是将客户资料上传到网盘，亦或是将销售数据通过电子邮件发送给竞争对手，在Ping32的泄密追踪中全部有迹可循。

- **发现泄密时告警**

在审计的同时，Ping32提供弹窗、短信、邮件等多种形式的文件外发告警通知，如：某员工在1分钟内用微信向外发送几十个文件，那么我们有必要认定这是一个具有违规泄密的行为。当用户行为触发预设规则时，管理者可以在第一时间收到存在泄密风险行为的告警通知，以便进行相关管控。

- **敏感内容分析**

敏感内容分析依靠先进的内容识别技术深度分析员工外发文件中是否包含涉密信息，根据不同办公行为、办公软件引起的文件外发提供不同等级的泄密风险评定。在海量的文件外发行为中准确定位违规行为。

文件外发管控

通过聊天软件、电子邮件随意外发公司内部文档，甚至将工作文档违规上传到私人网盘，可能会引发严重的数据泄漏事故。Ping32可以对文档外发行为进行严格的监控，以及对包含重要数据的文档建立严格的传输控制策略，保护企业的核心竞争力。

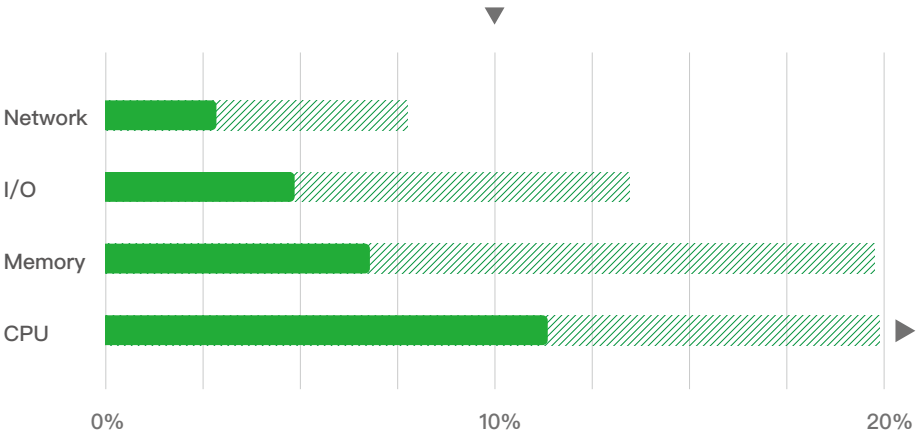
- **文件外发管控**

文档通过QQ、微信、电子邮件、网盘等途径外发是常见的泄密途径。Ping32文档外发管控可以设置文档的外发权限，用户可以按照进程类型、文件类型、文件大小、URL等粒度进行管控，保障文档的安全性，防止文档内容被泄漏。

- **敏感内容拦截**

Ping32敏感内容识别支持关键词和正则表达式等多种定义敏感信息的方式。含有敏感内容的数据进行流转时可进行审计或阻断，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。

资源占用



Ping32敏感内容分析引擎可以从语义层识别文本中的敏感内容，构建基于自然语言的神经网络，相较于传统的文本识别方法，内容识别更精确，通过不断智能训练语义分析模型，多线程处理技术，极大减轻服务器计算压力。

邮件审计

电子邮件为对外沟通提供了便利的同时，也引入了数据泄漏的隐患。大约有94%的企业、机构已经意识到了“邮件危机”，保护邮件安全不泄漏，需从“监管”两手一起抓。

对用户收发电子邮件进行审计可以确保邮件内容安全合规，杜绝信息泄密风险。Ping32不仅支持对主流的Web邮箱进行审计，也支持对Foxmail、Outlook等邮件客户端以及用户企业邮箱进行审计。

- **正文标题审计**

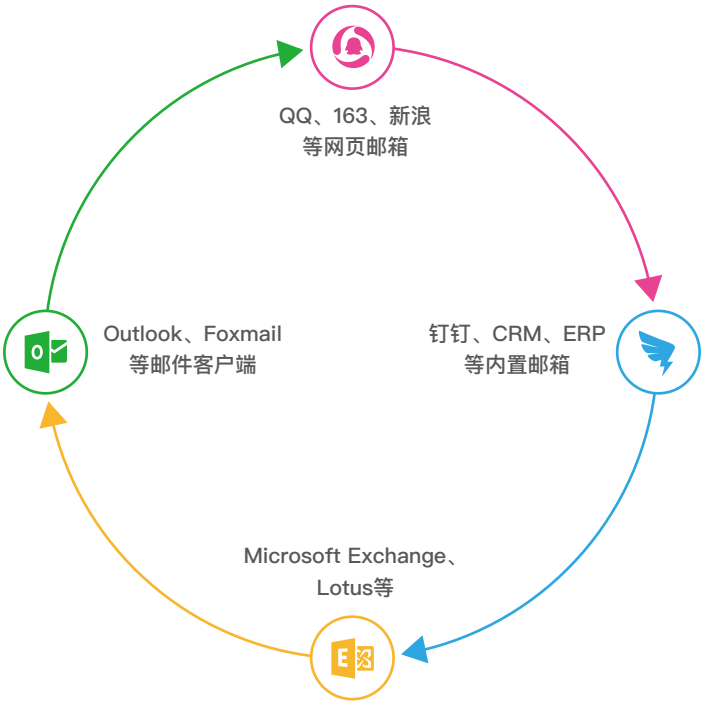
对邮件收发进行场景化还原，详细记录收发件人、标题、正文、时间等信息。

- **邮件附件**

相比即时通讯软件，邮件附件支持超大附件的传输与中转，根据策略设置，Ping32可以审计、备份邮件附件内容，作为事后回溯的依据。

- **敏感词告警**

支持自定义敏感词，分析邮件标题、正文、附件，一旦触发敏感词告警，管理员会收到短信、弹窗、邮件等形式的告警，随时随地查看告警信息。



Ping32邮件审计

支持多种邮箱协议，不论是Web邮箱还是邮件客户端均可轻松应对。

邮件管控

适配多种邮件服务

Ping32邮件审计支持多种邮箱协议，不论是Web邮箱还是邮件客户端均可轻松应对。

基于机器学习技术

Ping32邮件审计和拦截基于大数据深度学习技术，可对往来邮件进行智能识别或拦截。

支持HTTPS、SSL 加密协议

大多数邮件会使用加密协议来确保安全性，Ping32率先实现了对加密协议的支持。

Ping32邮件数据防泄漏解决方案具备完整的邮件安全审核功能，通过对互联网邮件协议的解析、敏感内容识别以及透明加密技术，在邮件数据在传输过程中审批、审计、分析、拦截、加密等多项管控，确保邮件数据安全合规。

- **强制抄送**

邮件发送必须抄送指定人才能够发送成功，邮件使用增加审核环节，确保邮件传输更加安全。

- **限制接收邮箱**

限制邮件收件人，员工只能将邮件发送到指定接收人，适用于企业只允许使用邮件进行内部沟通等场景。

- **限制发送邮箱**

限制员工只能使用企业规定的邮箱发送邮件，除此之外的邮箱均不可使用，配合邮件审计，实现邮件的合规使用。

- **邮件安全网关**

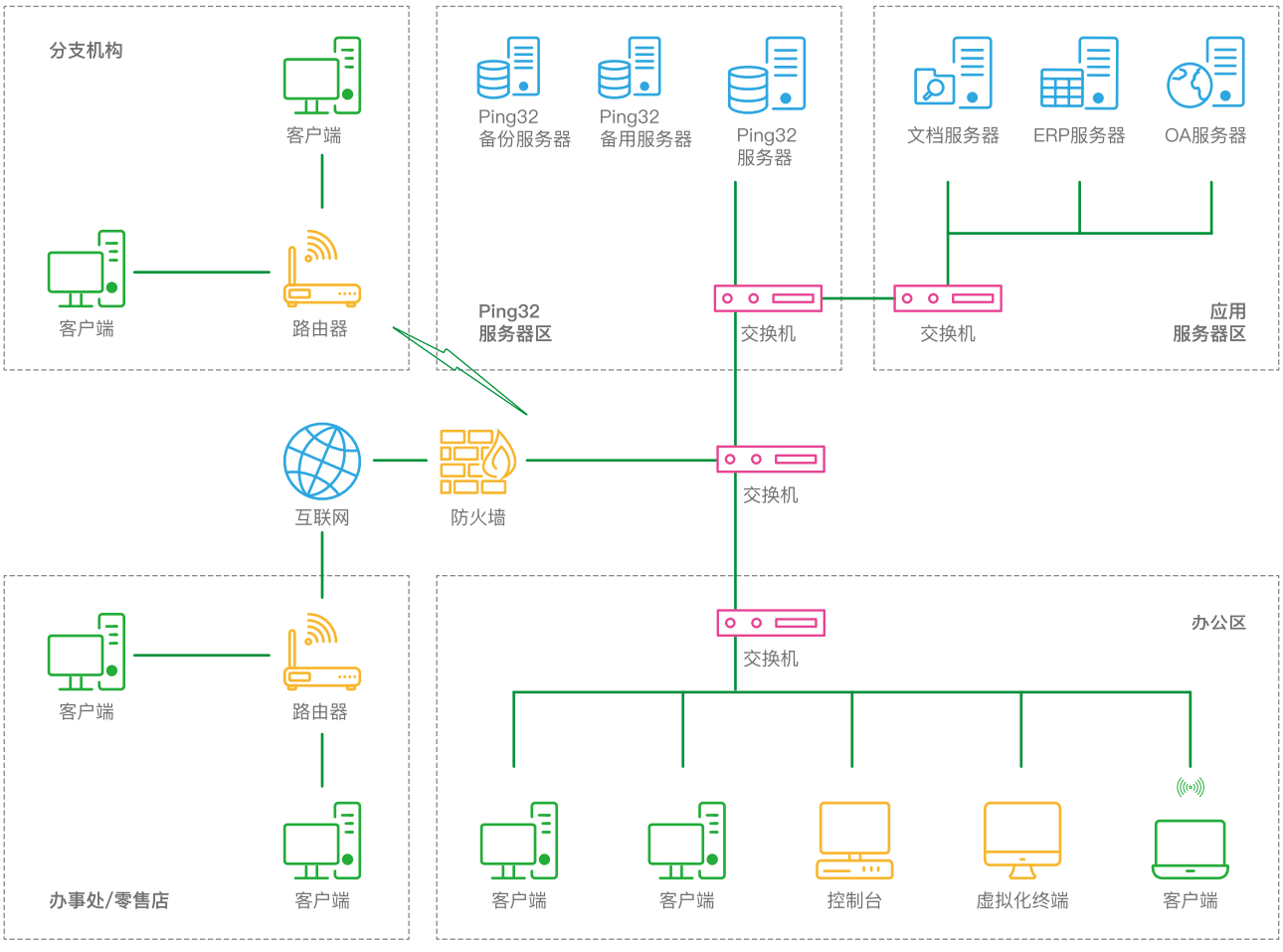
基于先进的机器学习技术实时分析邮件包含的敏感内容，根据用户既定策略，对邮件无感知透明加解密，确保可信范围内邮件正常传输，自动拦截带有敏感信息的邮件，防止核心数据外泄。

架构·特性

Ping32包含了很多技术创新及安全特性，比如：私有的加密通信协议、与业务系统集成、动态域名服务、负载均衡等。Ping32技术架构具有高度的弹性和伸缩性，既可满足创业公司的需求，又可适应大型企业的使用场景。

基于TCP/IP协议的标准网络架构

Ping32基于TCP/IP协议的网络架构，可以灵活地从本地网络扩散到远程网络和异地网络。
远程计算机也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管控。



数据安全中间件

现在，企业为规范业务流程实现业务数据和资源共享，提升企业运营效率，引进多种企业应用系统，而存储在OA、CRM、ERP上的数据资产安全正受到严峻的挑战。

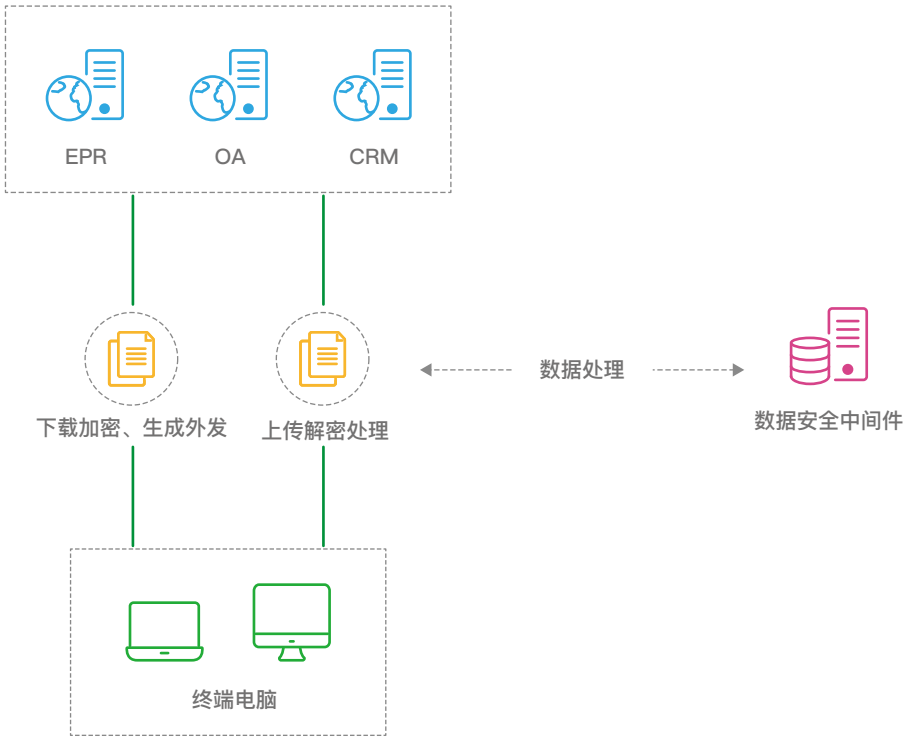
Ping32采用先进中间件技术与企业各类应用系统无缝对接，在不影响用户正常操作行为、不改变企业网络架构的情况下，对企业各类信息数据集中管控、协作共享，满足企业信息化建设，有效避免离线使用业务系统造成的泄密风险。

- **透明加解密**

不改变用户原有的操作行为，在上传到业务系统时自动解密，下载到本地自动加密。

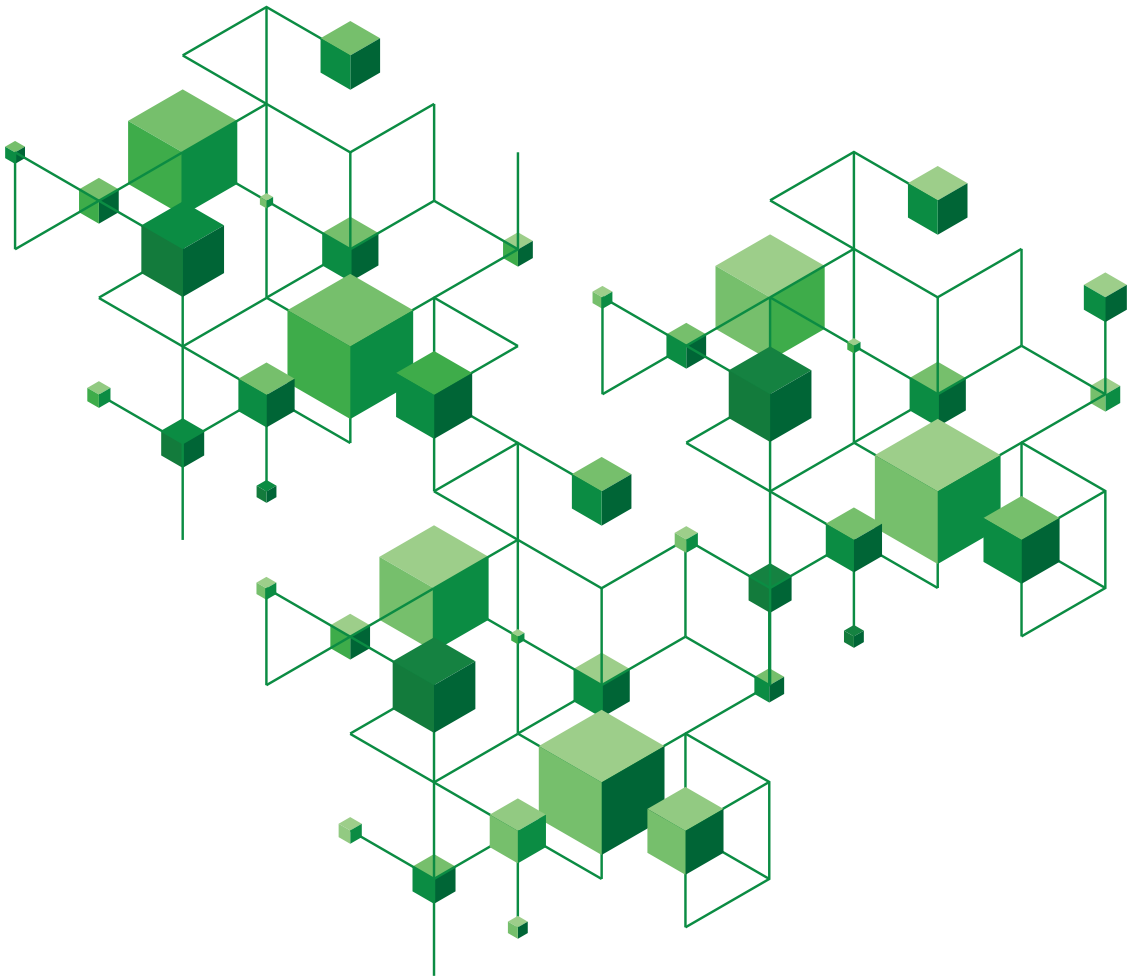
- **权限控制**

中间件实时获取Ping32终端安全管理系统中当前用户文档操作权限，确保业务系统文件安全。



集成云计算能力

随着企业业务的增长，伴随企业各类应用系统逐步启用，企业结构化数据与非结构化数据数据量几何级数的增长，Ping32集成主流云计算平台，借助云存储、图像识别、文字识别、数据处理与分析等AI服务，确保数据安全合规的同时，进一步扩展数据安全防护能力。



动态域名服务

很多时候用户有跨互联网，管理异地电脑的需求。Ping32想你所想，不需要固定的公网IP，也不需要云服务器。Ping32内置了动态域名服务，你可以随时随地进行跨互联网管理，极大的简化设置，降低成本，提升效率。而且，数据不会经过任何服务器中转确保你的数据足够安全，可控。

更多特性

- **安全性**

安全性是我们设计产品和服务的基础。Ping32以完全私有化部署模式，内部加密的私有通讯协议等技术手段来保证你的数据安全、合规。

- **完全私有化部署模式**

无须借助任何第三方服务，以完全私有化的部署模式、私有的通信协议等特性，你的数据只属于你，确保数据安全可控。

- **Webhooks**

有时客户会有需求，希望能使用Ping32的数据，与自己内部的其他业务系统进行集成。鉴于此，Ping32提供了Webhooks机制，方便你获取需要的数据。

- **良好的用户体验**

此外Ping32更注重用户的使用体检，Ping32以匠者之心精心打磨产品，简洁、大气的用户界面，能够帮助企业快速投入到运营的当中，降低学习成本，一度受到各行业客户好评。

- **安全态势感知**

数据可视化与良好的用户体验一直是我们致力研究的目标，Ping32以详细、清晰、多维度的态势感知平台提供精准用户行为分析，报表统计。

从大企业到创业公司，深受规模各异的众多企业信任。

国家电网 STATE GRID

DEEP COOL

货拉拉

青蛙王子

丰桔出行

同程旅游 LY.com

咪咕

五粮液

新氧

Zong Mu

新天药业

LYNK&CO

UCC

甘源

中银国际证券

更多案例...

nsecsoft.com/customers

即刻开始

1 下载

前往www.nsecsoft.com/trial，选择所需版本下载，你也可以联系我们的经销商获取相应版本。

2 安装

运行已经下载完成的Ping32，按照提示直到安装结束，恭喜你Ping32已经安装完毕。

3 激活

使用我们提供的License激活Ping32，你会看到成功激活的提示，Ping32现已激活且可供使用。

知识库
www.nsecsoft.com/support

下载中心
www.nsecsoft.com/trial

产品介绍
www.nsecsoft.com/products

我们网站www.nsecsoft.com拥有完善的知识库和与产品相关的全部新信息，包括产品的系统要求等更多详细信息。

NSecsoft
安在软件

nsecsoft.com

Contact us : design-team@nsecsoft.com

安在软件
济南
高新区经十路7000号汉峪金谷
A5区5栋6层
—
400-098-7607
support@nsecsoft.com