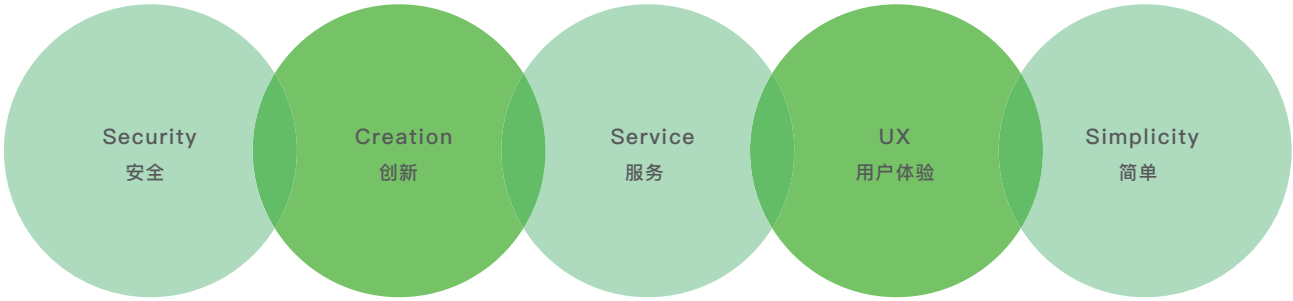
数据防泄密
内网安全
桌面管理
工作效率评估、提升
文档备份
移动存储安全
上网行为管理

产品介绍

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）是拥有自主知识产权的信息安全解决方案供应商。安在软件是中国信息安全领域的创新者，通过 Ping32 等产品，为企业提供数据防泄密、工作效率评估、内网安全管理等服务。

安在的产品、解决方案和服务具备高度的弹性和兼容性，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。

安在通过完善的以客户为中心的研发、客服、销售、市场、渠道组织体系，确保向客户提供满意的服务与产品。

数据防泄密

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。

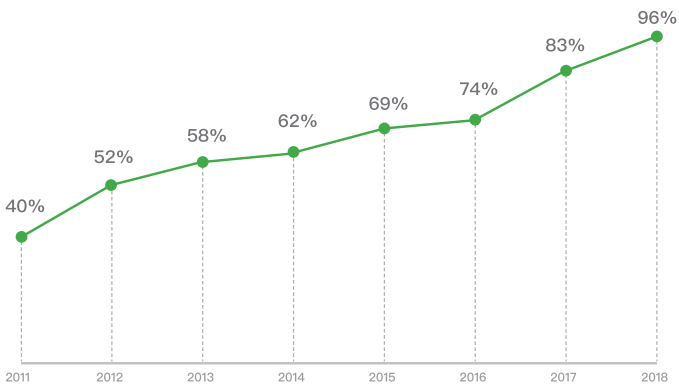
防范商业环境中的数据泄漏，“一夫当关，万夫莫开”。

数据防泄密

了解我们如何与内部职场道德问题作斗争?

背景

保护数据安全、合规，企业数字资产不被外泄从来不是件易事。但是现如今，企业面临的数据泄密威胁日益严重，归根结底在于日常办公、商务沟通中运用的应用程序、设备和平台日益增多。一方面，企业在不断探索提高工作效率和协作效果的方式; 而另一方面, 这种做法无疑增加了员工泄露或盗取企业数据的渠道。



数据泄密的危害

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。

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。

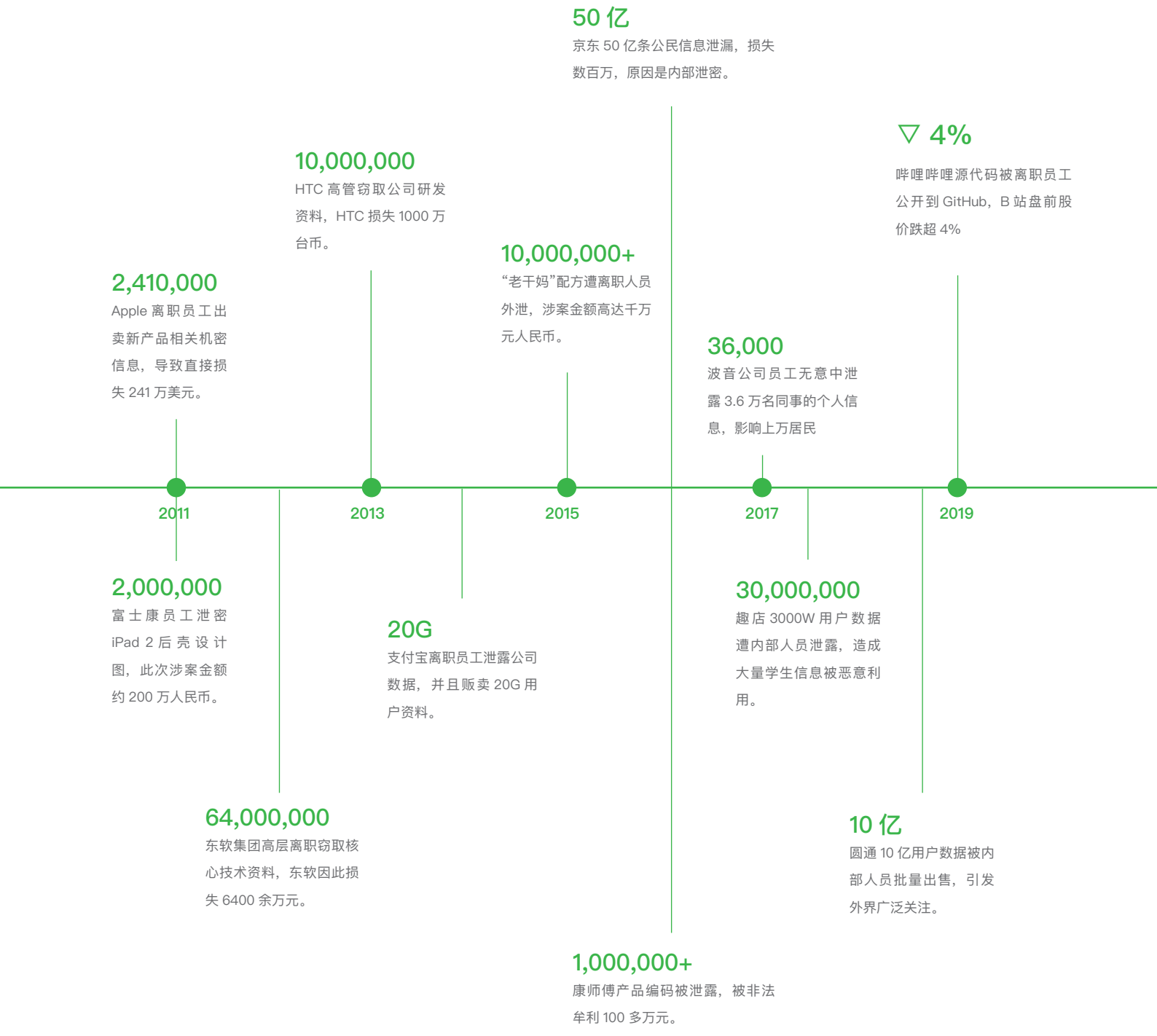
违反法律法规：一些国家涉密领域的数据泄漏，会导致企业违反保密法、网络安全法等法律法规。

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。

96%

《Gartner 2018 数据安全白皮书》中指出，受访的 96% 企业 CEO 承认，由于职场道德、内部威胁等因素，现在面临或曾经发生过数据泄密威胁。

无论用户在何处使用企业敏感数据，Ping32 数据防泄密解决方案都能够发现、监控并保护这些数据。Ping32 可以监控包括：即时通讯、电子邮件、网盘应用、网络通信等途径的数据泄密行为。此外，Ping32 可以对可能存在泄密风险的途径进行安全防护，包括外接设备的管控、行为监控、权限控制以及数据加密。


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。
▽ 4%
哔哩哔哩源代码被离职员工公开到 GitHub，B 站盘前股价跌超 4%
10,000,000
HTC 高管窃取公司研发资料，HTC 损失 1000 万台币。
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。
2,410,000
Apple 离职员工出卖新产品相关机密信息，导致直接损失 241 万美元。
36,000
波音公司员工无意中泄露 3.6 万名同事的个人信息，影响上万居民
2011
2013
2015
2017
2019
2,000,000
富士康员工泄密 iPad 2 后壳设计图，此次涉案金额约 200 万人民币。
20G
支付宝离职员工泄露公司数据，并且贩卖 20G 用户资料。
30,000,000
趣店 3000W 用户数据遭内部人员泄露，造成大量学生信息被恶意利用。
64,000,000
东软集团高层离职窃取核心技术资料，东软因此损失 6400 余万元。
10 亿
圆通 10 亿用户数据被内部人员批量出售，引发外界广泛关注。
1,000,000+
康师傅产品编码被泄露，被非法牟利 100 多万元。

解决之道

采取主动发现 – 防护策略，全方位保护你的敏感数据。

泄密事件不全都是外部窃取，职场中，内部人员泄密是更常见的风险。

常见的泄密场景

- 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；
- 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。

70%

中国公安部统计，70% 的泄密犯罪来自于机构内部，内部人员成为了造成知识产权失窃的首要威胁。

文档安全

文档外发管控

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，结合敏感内容识别，能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。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，防止文档内容被泄露。

泄密追踪

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。同样，结合敏感内容识别，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。

敏感内容分析

敏感内容分析依靠先进的内容识别技术，可以对散落在企业终端的非结构化数据进行分析、整理、归类。对高价值的数据采取更有针对性的保护措施。

水印管理

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。

行为审计

文档操作

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。

浏览器	IE	Chrome	Firefox	QQ	360 等主流浏览器
即时通讯工具	QQ	TIM	微信	企业微信	钉钉	Skype ...
网盘应用	360 网盘	百度网盘	OneDrive	Google Drive 等全部网盘
电子邮件	Foxmail	Outlook 等邮件客户端及各类常见 WEB 邮箱
网络协议	HTTP	HTTPS	FTP	SMTP	POP
移动存储设备	U 盘	移动硬盘	手机等便携设备

HTTPS

Ping32 支持 HTTPS、SSL 加密协议的审计。

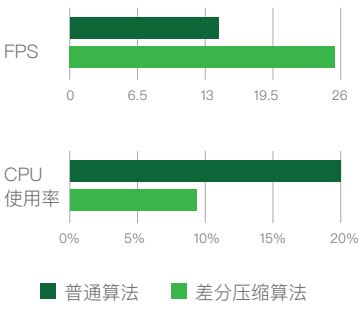
电子邮件

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。同时，Ping32 率先支持对 HTTPS、SSL 加密邮件协议进行审计。

即时通讯

QQ\TIM、（企业）微信、钉钉等即时通讯工具在职场的普及虽然极大提升了工作效率，创造了对外沟通的便利条件，但是也为数据泄露开辟了新的途径。Ping32 的即时通讯审计功能，可以最大限度确保用户沟通内容合规。同时，Ping32 也支持管控用户聊天账号，控制文档外发，内容违规告警等功能。

差分压缩算法在保证流畅度高的前提下，极大地减少了资源占用。



桌面 & 屏幕

Ping32 可以实时查看远程电脑屏幕，直观地了解到用户正在做什么，是否从事和工作无关的事情，以及是否存在泄密等违规行为。实时屏幕使用差分压缩算法，流畅度高，资源占用率低。智能截屏和屏幕录像可以对用户屏幕内容进行记录，方便备案保存。一旦发生违规、违法行为，可以作为事后追责的法律依据。

打印

Ping32 可以精确记录用户每次打印文档的行为，包括打印的文档名称、内容、页数等信息，可以有效防止敏感信息通过打印途径泄露。此外，打印水印模块可以对用户打印的文档添加水印标记，方便发生泄密事故时追溯泄密源。

文档加密

透明加密

Ping32 文档加密是基于内核驱动级别的透明加密技术，支持 AES-256、SEAL、Blowfish 等高强度加密算法。透明加密可以实现受信用户打开文档自动解密，保存文档自动加密，整个过程用户无感知，不影响用户的使用习惯。文档加密可以有效保护文档不被非法窃取，防止内部主动泄露。

50 万美元

Gartner 调查显示，在 Fortune 排名前 1000 家的公司中，每次电子文件泄露所造成的损失平均是 50 万美元。

流程审批

有时，难免需要将一些文件外发或者解密。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。

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，不仅可以防止 Print Screen、QQ、微信等常用的截屏软件，还可以防护 PicPick 等专业的截屏软件。此外，Ping32 还可以审计用户试图截取的屏幕内容。配合屏幕水印模块，可以对用户的截屏内容进行追溯，杜绝敏感内容通过截取屏幕泄密。

文档安全外发

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。

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！

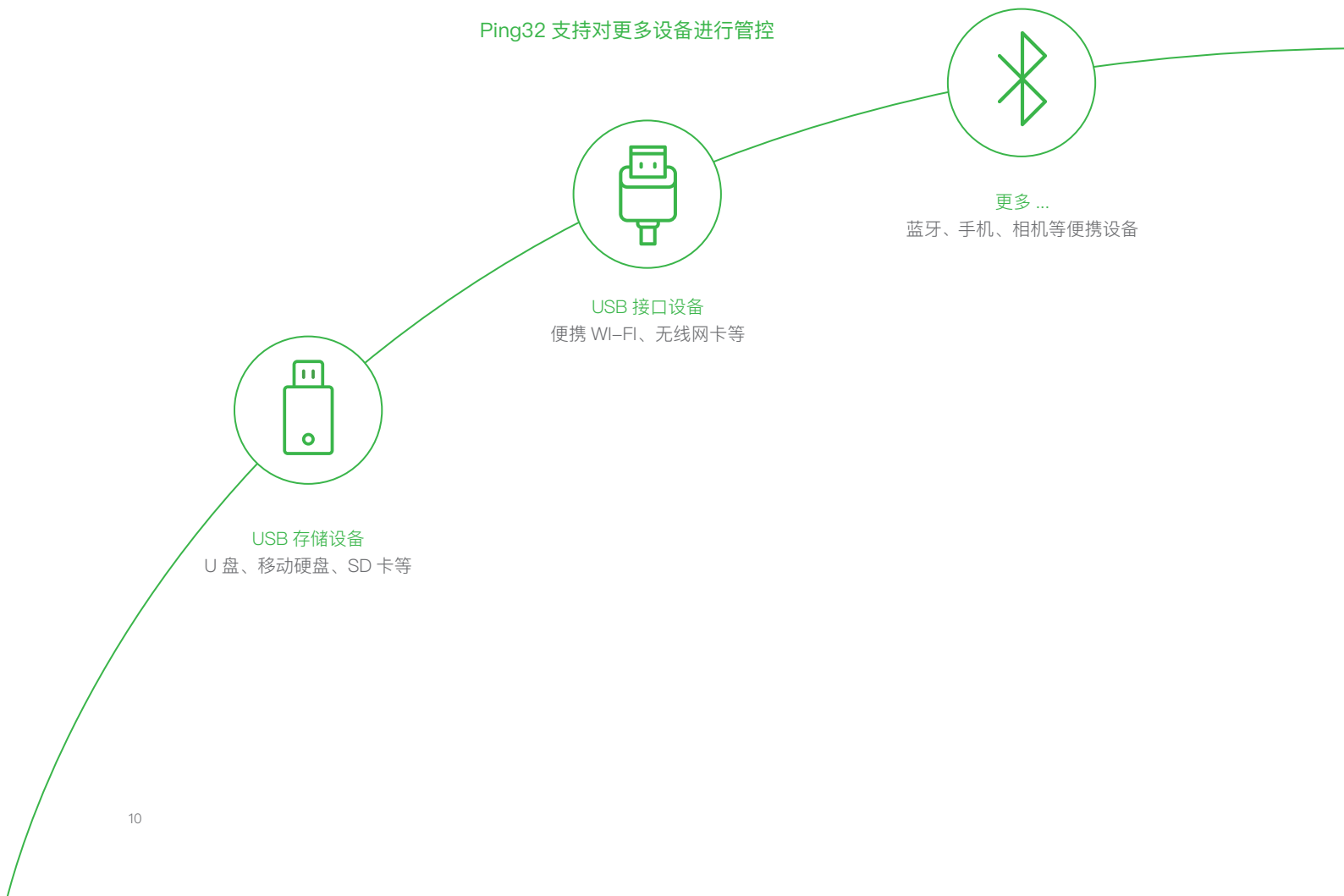
移动存储设备加密

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露怎么办？ 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

你知道吗？除了移动存储设备外，打印机、便携 WIFI、刻录光驱、蓝牙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！

Ping32 支持对更多设备进行管控



收益

保护知识产权，提高核心竞争力

在当今信息化时代，知识产权是企业的核心竞争力，然而这些核心竞争力大部分以文档、图纸的形式存在，所以企业的文档安全保护和知识产权保护面临着巨大的挑战，如果重要文档泄露，会严重影响企业的核心竞争力，以及企业的声誉。为此，企业为了提高核心竞争力、保护知识产权，在不断寻找有效的管控方法。通过 Ping32 能够有效的保护企业重要数据，防止被内部人员有意或无意泄露，从而保障企业的核心竞争力。

泄露跟踪溯源，避免法律商业风险

Ping32 能防止企业内部机密文档如研发代码、设计图纸等核心信息外泄。全方位的信息防泄露解决方案，帮助企业构建 " 事前防御—事中控制—事后审计 " 的完整信息防泄露体系，从而实现信息安全的透明性、可控性和不可否认性目标。除此之外，信息的泄露不仅使企业损失巨额的财产，还可能带来法律上、商业上的风险。通过 Ping32 保护信息安全，有效避免法律商业风险。

提高公众的信任度

当企业中发生数据泄露事件时，公众会降低对企业的信任度，使公众对企业产生不信任感，而这种不信任感会影响公众的选择，因此，数据泄密事件可能会使企业失去一大批已有的或潜在的客户。也可以说，数据信息的安全问题关乎企业声誉、公众信任感，会影响企业的外部竞争力。 因此防止企业数据泄密，能够有效的提高公众对企业的信任度。

规避舆论公关风险

企业发生机密信息泄露事件一旦发生，就会迅速被媒体曝光，并引发人们的讨论与猜想，对企业产生严重的负面影响。因此通过 Ping32 可以帮助你防止企业信息泄露，规避舆论公关的风险。

工作效率

专注目标，
科学评估、提升
工作效率、生产力。

Ping32 会对用户日常的行为数据进行分析，然后通过科学的评估算法测评用户工作效率。结合评估结果，与其他管控模块联动，可以有效避免用户从事和工作无关的活动，比如：屏蔽和工作无关的网站，禁用炒股、娱乐软件等，进而提升工作效率。

工作效率评估

通过用户行为分析
科学地进行工作效率评估

什么是工作效率评估?

如今，大家都在追求更高的付出回报比，在商业中更是如此。公司业务的发展需要与之匹配的高效率支撑，但与此同时管理人员却很难衡量哪些人是高效的。对用户的工作效率进行客观的评估可以给管理者提供很多参考意见，这就是 Ping32 工作效率评估所做的。通过使用工作效率跟踪、评估，管理者可以轻松查看哪些用户在以更高的效率完成他的工作。参考这些数据，搭配奖罚分明的公司政策，进而以更优雅的方式进行管理。确保公司能以最佳效率运作，在当今激烈竞争的商业环境中极为重要，而 Ping32 出色的工作效率追踪、评估可以助你一臂之力。

刷微博等社交媒体

炒股、做私活

网上购物

20%

据统计，如果不加以管理，职场中用户 20% 的时间会浪费在处理和工作无关的事务。

聊和工作无关的 QQ、微信

看小说、看视频、看球赛

盯着屏幕发呆

职场中常见影响工作效率的行为

如何追踪、评估工作效率?

想象一个场景，如果你观察一个用户使用电脑半个小时，相信你脑海里会对这个用户的行为产生一个直观的评价，工作、娱乐、购物、游戏、炒股……一言以蔽之，Ping32 会对用户行为进行智能分析，通过科学的算法，对用户工作效率进行追踪、评估。

行为数据分析

浏览网站

首先，Ping32 可以对用户访问网络的数据进行过滤，进而协议解析器可以解析 HTTP(s) 数据包，还原用户的浏览网站行为，比如：

John 于 2018 年 8 月 7 日 14:21 – 15:53 在浏览 https://v.qq.com – 腾讯视频。

这条记录具有场景带入感，表面看上去非常普通，实际上包含了我们很多创新。

- **Ping32 支持所有浏览器的 HTTPS**

HTTPS 是 HTTP 的安全版，简单说就是加密的 HTTP 协议。Ping32 支持内核级的 HTTPS 协议的过滤、解析，这并非不负责任的 Shell 层面的取词。也就是说 Ping32 支持所有浏览器的 HTTPS 流量的过滤和解析，记录更加全面、精准。

丰富的评测模型

Ping32 针对不同的应用，适配了不同的评测模型，评测结果更加精准、可依赖。

- **Ping32 支持精准的网站浏览时间记录**

众所周知，HTTP(s) 大多数情况是一种短链接无状态协议，所以只是从协议角度（如：上网行为管理设备），很难测量用户的真实浏览时间。将网络流量过滤引擎的原始 HTTP(s) 记录与用户界面的活动记录进行关联，Ping32 可以精准记录用户真实浏览网站的时间。

软件使用统计

Ping32 提供了多种粒度的使用软件记录，包括：进程活动记录、窗口活动记录等。通过进程活动记录，你可以查询用户计算机指定时间内进程的启动、结束时间；而窗口活动记录，则提供了用户真实的应用软件使用情况。

更多个性化数据

有时，不同的应用，不同的场景需要更多个性化的分析，比如：打开 Word，却没有发生键盘事件显然是低效率的；使用 Photoshop 等做图软件，却没有关联打开设计图纸，也不合理……

所以，Ping32 支持在更多维度对应用进行分析，比如：关联的对象，鼠标事件，键盘事件等，提供个性化的分析结果。

拥有了这些数据，Ping32 的行为分析引擎可以定期进行用户的工作效率评估。比如：用户上班时间花费大量时间在浏览淘宝、天猫等购物网站，那么我们有理由认为，这个用户的工作效率比较低……

等等……真的是这样吗？如果这个企业就是一个电子商务公司，用户花费大量时间浏览淘宝网站是因为在装饰网店，这应该是一个高效率的行为。

因此，想你所想，Ping32 支持对不同的活动事件、行为对象进行个性化评价。

应用、网站评价

Ping32 内置了丰富的策略库，包含了丰富的应用、网站评价规则，用户可以手动调整这些评价规则，以使工作效率评估结果更准确。比如上面的案例，对于绝大多数企业，用户访问购物网站都是一个低效率的行为，但是对于类型是电子商务的企业或者指定的用户，这却是一个高效率的行为。

工作效率排行榜

Ping32 会定期对用户的工作效率进行评估，在此基础上，我们可以进行丰富的扩展。你可以查看指定用户在指定时间内的工作效率评估结果，也可以查看指定时间内，所有用户的工作效率排行榜，甚至还可以查看部门之间的整体工作效率评估结果。

离职风险评估

我们很多案例显示，很多员工在离职前都可能会备份电脑上的文档带走、删除本地文档、恶意删除共享文档搞破坏……Ping32 会对用户的行为数据进行分析，比如：访问招聘网站的频率、聊天语义分析等，进而评估出用户的离职风险。结合离职风险评估结果，你可以制定灵活的策略，比如：文档备份、泄密风险备份……防患未然。

历时 5 年
通过对成功签约的部分企业，约

205,000

台终端数据，回访统计表明

77%	12%	6%	3%	2%
时间用于处理工作事务	时间看新闻、视频、小说 ...	时间炒股、做私活	时间电脑处于非活跃状态	时间用于处理其他和工作无关的事情

提升工作效率

Ping32 的工作效率评估结果可以给你提供详细、精准的数据，让你对企业内用户的工作效率状况一目了然。除此之外，我们还可以给你提供决策依据及建议，帮助你提升企业内用户的工作效率。

内置丰富的网址库和应用库，降低管理员配置成本，并定期自动更新。

网站访问控制

通过网站访问控制，你可以制定灵活的黑名单或白名单规则，你可以禁止用户访问指定的网站，或者只允许访问指定的网站。此外，Ping32 还支持网页关键词拦截。Ping32 的网站访问控制不仅可以确保信息安全合规，更重要的是屏蔽和工作无关的网站，提升工作效率。

软件管控

软件管控同样支持黑名单和白名单两种策略类型。软件管控支持禁用指定的软件，比如各类和工作无关的软件，也支持只允许使用指定的软件。软件管控支持对进程名称、窗口名称、哈希值、厂商名称等各种粒度进行管控。

聊天账号管控

用户工作期间使用私人聊天账号沟通和工作无关的事，不仅存在信息泄密风险，也会极大地影响工作效率。Ping32 聊天账号管控功能可以制定账号白名单策略，只允许用户登录指定的聊天账号，确保每一次沟通都高效、合规。

适时、科学的建议

Ping32 的独到之处在于，不仅提供了详细的工作效率评估结果，还可以根据评估结果，适时给出合理、科学的决策建议。

上网时间管控

通过 Ping32 的上网时间管控，你可以制定灵活的网络使用策略。可以为用户分配时间配额、流量配额，或者是分时间段管理 , 确保网络高效利用。

收益

工作效率评估

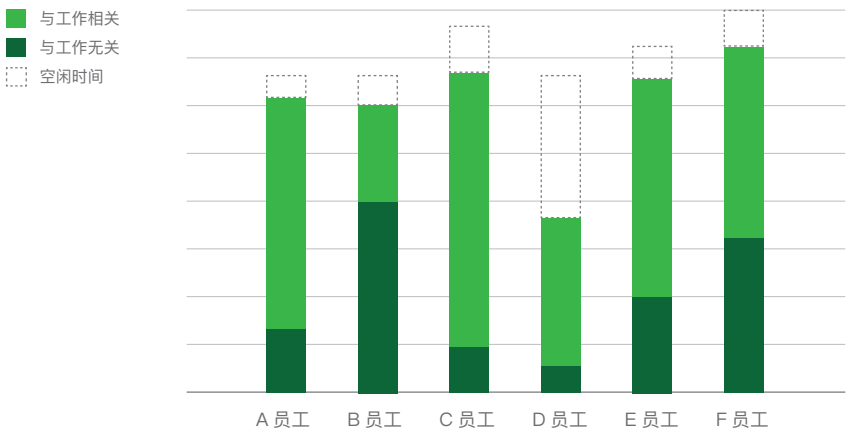
通过 Ping32 工作效率评估系统进行用户行为分析，可以对用户的工作效率进行客观的评估，为管理者做决策提供可参考意见。通过工作效率评估，管理者可以直观的获取对此用户的人物画像，更明确的了解哪些用户正在以高效率的状态工作。借助工作效率评估，管理者制定相关的策略，从而确保员工始终处在高效率工作状态，提高企业核心竞争力。

提高员工工作效率

Ping32 能够审计并且控制员工的上网行为，了解并管理用户对软件的应用，规范桌面操作行为，提高工作效率。既有利于企业的劳动生产效率和经济效益的提高，增加活力，也有利于员工为企业创造更多的经济效益，克服机构臃肿，员工做事浮躁，浪费时间的现象，使企业具有更大的竞争优势。

防范离职风险

人员离职是企业内部的正常人员流动，但是人员离职也暗藏风险，比如一些员工在离职前会拷贝走公司机密资料，恶意删除公司重要数据，这都是人员离职给企业带来的隐患。通过 Ping32 工作效率评估能够对用户进行行为数据分析，智能判断用户的离职风险，从而制定相关的策略，防范员工离职带来的安全隐患，保护企业重要数据。



Ping32 提供了一组实用的内网安全、桌面管理工具。比如：远程协助、补丁管理、远程部署软件等。通过这些工具，可以极大减轻网络运维人员的工作负担。希望对你有帮助，你能喜欢。

一组内网安全、桌面管理工具

“工欲善其事
必先利其器”，
我们提供了一些实用工具。

文档备份

集中备份企业文档
保护重要、敏感数据，防范勒索病毒。

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。

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。

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。

软件分发

如何将 1GB 的软件
快速部署到 1000 台终端电脑?

如何将一个 1GB 的软件快速部署到 1000 台终端？借助 Ping32，你会发现事情原来如此简单。Ping32 的文件分发模块，不仅可以分发文件，也可以分发软件、补丁。独有的子网加速功能，可以从最近的节点获取分发数据，极大减轻服务器的压力。

1GB
3min

通过测试，Ping32 分发 1GB 的文件平均仅需 3 分钟。

特性

自定义目标路径

通过文件分发，可以将你需要的文件、软件发送到客户端指定位置，并且支持自定义目标路径。

可视化任务进度

在文件、软件分发过程中，所有分发任务进度清晰可视，随时可以直接查看各项任务的实时进度。

子网加速

Ping32 文件分发独有的子网加速功能，使终端能够从最近的节点获取分发数据，极大的减轻服务器和网络的压力。

断点续传

如果遇到网络故障，终端会从中断部分继续下载未完成的部分，极大节省下载时间和提高下载速度。

自定义命令行

进行软件部署时，支持自定义命令行，实现软件分发完成后以设定的命令行参数运行。

灵活的分发策略

Ping32 支持用户按照不同的部门、终端制定不同的任务分发策略，满足不同终端对不同软件、文件的需求。

弹窗提醒

支持设置弹窗提醒。分发任务完成时，终端会自动弹窗提醒，提示终端收到新文件。如有需要可以直接点击文件使用。

流量限制

进行文件分发时支持流量限制功能，自定义终端下载此文件的最大速度，节省企业宽带资源，确保企业网络稳定运行。

资产管理

发现、管理数字资产
资产变更告警，防范资产流失。

Ping32 资产管理能够自动检测终端计算机软、硬件资产及其变更情况，支持软、硬件资产自定义查询和统计，

让管理员了解计算机软、硬件资产的使用以及变更情况。

除此之外，如果发生资产变更，Ping32 会第一时间向管理员发起告警。

通过 Ping32 资产管理能够有效提高企业资产管理效率，简化 IT 运维工作。

系统策略、性能监视

系统策略
通过系统策略，你可以调整系统权限。

禁用任务管理器

禁止用户使用任务管理器，确保终端安全稳定运行。

禁用控制面板

禁止用户使用控制面板，实现用户权限最小化。

锁定计算机名称

锁定计算机名称，禁止用户随意修改。

禁止安装新软件

禁止用户随意安装软件，确保用户软件使用合规。

禁用注册表

禁止用户使用注册表，保护注册表不被恶意修改。

禁止修改网络配置

实现 IP\MAC 绑定，禁止用户修改网络设置，防范 ARP 攻击。

禁用安全模式

禁止用户使用安全模式，防止安全防护类软件被恶意删除。

禁用命令提示符

设置命令提示符权限，禁止用户使用命令提示符。

禁止共享文件

禁止用户共享文件，防止数据泄露。

性能监视
通过性能监视，你可以了解系统各项参数。

禁用任务管理器

实时查看用户计算机正在运行的所有进程，支持禁止正在运行的进程。

活动窗口

实时查看用户当前活动窗口，支持关闭活动窗口。

网络状态

实时查看用户当前的网络连接情况，及时发现非法连接。

系统服务

查看用户当前所有的服务运行状态，可以启动、停止任何服务，也可以更改服务启动类型。

开机启动

查看用户计算机的开机启动项，可删除无关启动项，提高终端运行速度。

共享资源

查看用户正在共享的资源，支持取消正在共享的资源，防止数据通过共享资源泄露。

软件信息

查看用户所有安装的软件信息，支持远程卸载非法软件。

硬件信息

查看用户计算机当前硬件情况，如果硬件发生变更，管理员会第一时间收到告警。

硬盘信息

查看用户所有的磁盘信息，支持远程查看用户磁盘内所有文件。

补丁管理

私有补丁数据库
自动修复漏洞，防范勒索病毒。

Ping32 的补丁管理支持多种部署模式，支持内外网隔离环境。通过 Ping32 补丁管理不仅可以进行补丁部署，还可以扫描终端漏洞，识别终端缺失的安全补丁，并立即修复以降低风险。

漏洞自动修复

Microsoft 在每个月第二个星期二为其操作系统和应用程序发布补丁，除此之外，它还会发布安全公告来解决操作系统和应用程序中的关键问题。通过 Ping32，IT 管理人员可以确保所有定期更新的补丁都自动部署到企业内部计算机上，无需任何手动操作。除此之外，Ping32 独有的子网加速功能，计算机可以从最近节点获取补丁，极大减轻服务器压力。

子网加速

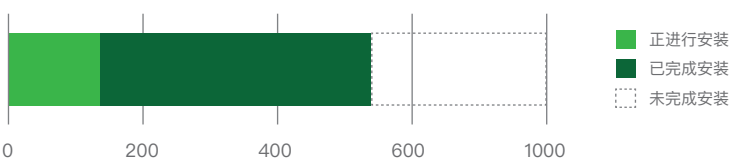
依托于文件分发平台，Ping32 的补丁分发模块同样支持子网加速。确保终端能够从最近节点获取分发数据，减轻服务器和网络压力。

离线补丁修复

Ping32 会扫描所有终端系统以查看操作系统中缺失的 Windows 补丁，Ping32 补丁管理默认会从云端获取补丁数据库，如果终端处于内外网隔离环境中，你也可以手动上传离线补丁数据库进行扫描。扫描完成后 Ping32 会生成漏洞报告，IT 管理员可根据需要更新漏洞补丁。

部署过程可视化

IT 管理员能够通过 Ping32 监控补丁安装结果，并可直观查看已经成功安装的补丁。如果安装过程出现错误，IT 管理员还会收到提示。例如将补丁分发给上千台计算机，IT 管理员无需检查每台机器安装结果，只需要通过查看 Ping32 控制台报告，安装结果一目了然。



部署过程无感知

Ping32 漏洞、补丁管理可以集中处理计算机更新和补丁分发，整个过程并不会影响用户对计算机的正常使用，结合 Ping32 子网加速功能，能够有效的避免企业网络过载或者对计算机性能产生负面影响，不仅如此，你依然可以选择补丁更新避开工作时间，以尽量减少对员工工作效率的影响。

Ping32 的非法外联模块不仅可以检测当前终端是否潜在非法外联行为，也可以对其进行阻断，以确保你的网络环境符合等保合规要求。

网络访问控制

过滤、分析网络流量，阻挡网络攻击，防范数据泄密。

Ping32 网络防火墙是给企业用户计算机使用的网络安全工具，通过对终端计算机进行设定网络安全规则，提供强大的网络访问控制、应用通讯控制等功能。Ping32 可以帮助企业阻止网络入侵和攻击，限制网络的访问、防止数据泄露、保护企业和终端计算机的网络安全。

驱动级的防火墙

Ping32 使用驱动级的防火墙技术，支持进程、端口、网络地址、网络协议、流量方向等多种防护规则。

网络防火墙

通过 Ping32 网络防火墙设置网络访问控制权限，可以管理计算机的网络通讯权限，确保计算机能够进行安全的网络浏览，让计算机在与内部或外部的通讯过程中始终处于受保护状态，让恶意计算机程序无法入侵计算机，从而确保企业内部网络安全。

应用访问控制

通过 Ping32 网络防火墙，可以有效的控制企业内部计算机应用程序访问网络的权限，比如禁止迅雷、比特彗星等 P2P 下载软件的网络通讯，防止其占用大量的网络宽带，造成企业内网瘫痪。这样可以有效的防止企业员工使用违背公司安全策略的程序。

远程协助

媲美商业产品
的跨互联网远程协助服务

例如 QQ，Windows 远程桌面连接都带有远程协助的功能，但是他们的远程协助缺少实用性，并且有很大的局限性，功能也不够强大。Ping32 远程协助实用性强，可操作性好，是一款功能强大的远程协助软件。

快速响应终端故障

计算机故障、系统崩溃和设备故障都会严重影响企业业务的正常开展，当计算机发生任何技术故障，企业 IT 管理员都可以使用 Ping32 远程协助随时随地的协助用户提供远程技术支持，这种方式极大地提高了 IT 管理员的工作效率，取代了费时费力的现场调试服务。Ping32 提供了两种连接方式，首先是向用户发起远程申请，用户同意后即可进行远程控制，再就是直接连接，无需用户同意，直接进行远程控制并解决问题。

跨网络支持

Ping32 可以一对一连接也可以一对多连接，一台电脑控制多台电脑，迅速排除故障，节省维护人员精力，极大提高工作效率。同时 Ping32 实现了内网穿透，在任何能上网的地方使用本地电脑就能对分布于不同地点的终端进行远程协助，快速解决终端故障。

安全、快速、稳定

远程协助最重要的是性能体验，因为远程连接的速度和稳定性直接会影响 IT 管理员的使用效率。Ping32 作为专业的远程连接软件，在传输质量方面进行了大量优化。Ping32 采用了新的传输算法，确保在低宽带的环境下保证连接的快速和稳定性。在安全性方面，Ping32 的传输过程对数据进行了加密处理，确保数据不会被监控，在给企业提供便利的同时也为企业数据安全作出贡献。

身份认证

独立、多模式的身份认证服务

身份认证是管理系统审查终端登录用户的过程，从而确定该用户是否具有登录终端的权限，并且是否具有对资源的访问和使用权限。如果用户身份认证合规，用户可以正常使用终端，相反用户将不具备登录终端和访问内部资源的权限，从而保障企业内部信息安全。

更多的认证方式

Ping32 内置了丰富的认证方式，除此之外，我们还支持定制更多的认证方式，比如：指纹、人脸识别等。

多种认证方式

针对企业不同的需求，并且加强身份认证的安全性，Ping32 提供了多种认证模式，比如口令、UKEY、短信、双因子认证等多种模式，全方位保护身份认证的安全性、可靠性。

权限控制

通过 Ping32 身份认证，可以有效的对用户进行权限控制，指定用户能够登录的终端，根据用户级别也可以设定对企业网络资源的访问权限。严格管理企业内部资源的访问权限，最大可能保护企业内网安全。

公共终端管理

企业对于公共终端的管控，无法做到追根溯源，所以在公共终端发生安全泄密事件时，企业无法定位违规人员。通过 Ping32 身份认证，系统要求用户必须进行身份认证后才能够登录公共终端，同时对用户的所有操作进行审计，审计记录和用户身份进行关联方便回溯追查。

终端实名制

为了防止终端被恶意登录，发生泄密事件，使用 Ping32 身份认证能够有效的实现终端“实名制”登录问题，设置终端只能允许指定用户登录，用身份认证信息来标识终端使用人员的身份，保证只有合法用户才能登录内网终端。用户无论通过哪种认证方式登录终端，Ping32 都会对终端的操作行为进行基于登录用户的审计关联，确保能够准确定位到终端的使用者，可有效降低违规、泄密事件的发生。

节能设置

制定合理电源计划
为绿色星球贡献一份力量

如今的信息化时代，企业内部计算机数量越来越多，在用户计算机合理使用方面也面临着很多问题，比如用户离开工位没有锁屏习惯，长时间不使用计算机不对其进行睡眠或关机处理等等，这些情况不仅仅会浪费能源，也可能会导致潜在的安全风险，比如数据泄露等。由此可见，依靠规章制度的约束，不如使用 Ping32 节能设置的功能，以上问题迎刃而解。

节约能源

Ping32 节能设置，能够智能监测用户的工作状态，如果检测到用户处于空闲状态，会自动对空闲计算机进行关闭显示器、锁屏等操作。当然你也可以手动设定电源节能设置，通过设定的时间阈值，如果超过时间阈值计算机没有进行操作，那么计算机进行自动关闭显示器、锁定屏幕等操作。你也可以设定定时任务，比如每天在下班之后，为防止用户忘记关闭计算机，Ping32 可以强制对此计算机进行关机操作，或者是对用户进行提醒，让用户来手动选择是否关机，从而达到节约能源的目的。

防止数据泄露

用户正常工作过程中屏幕会显示很多工作相关资料，可能会包含企业重要数据。如果用户离开工位时并没有进行计算机锁定或睡眠操作，那么企业就会面临数据泄露的危险，借助 Ping32 节能设置，实时检测计算机是否处于空闲状态，一旦计算机空闲，Ping32 将会对此终端进行关闭显示器，锁屏操作，并不会影响用户正在处理的文档，节约企业能源的同时也降低了企业数据泄露的风险。

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、内置动态域名服务、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。

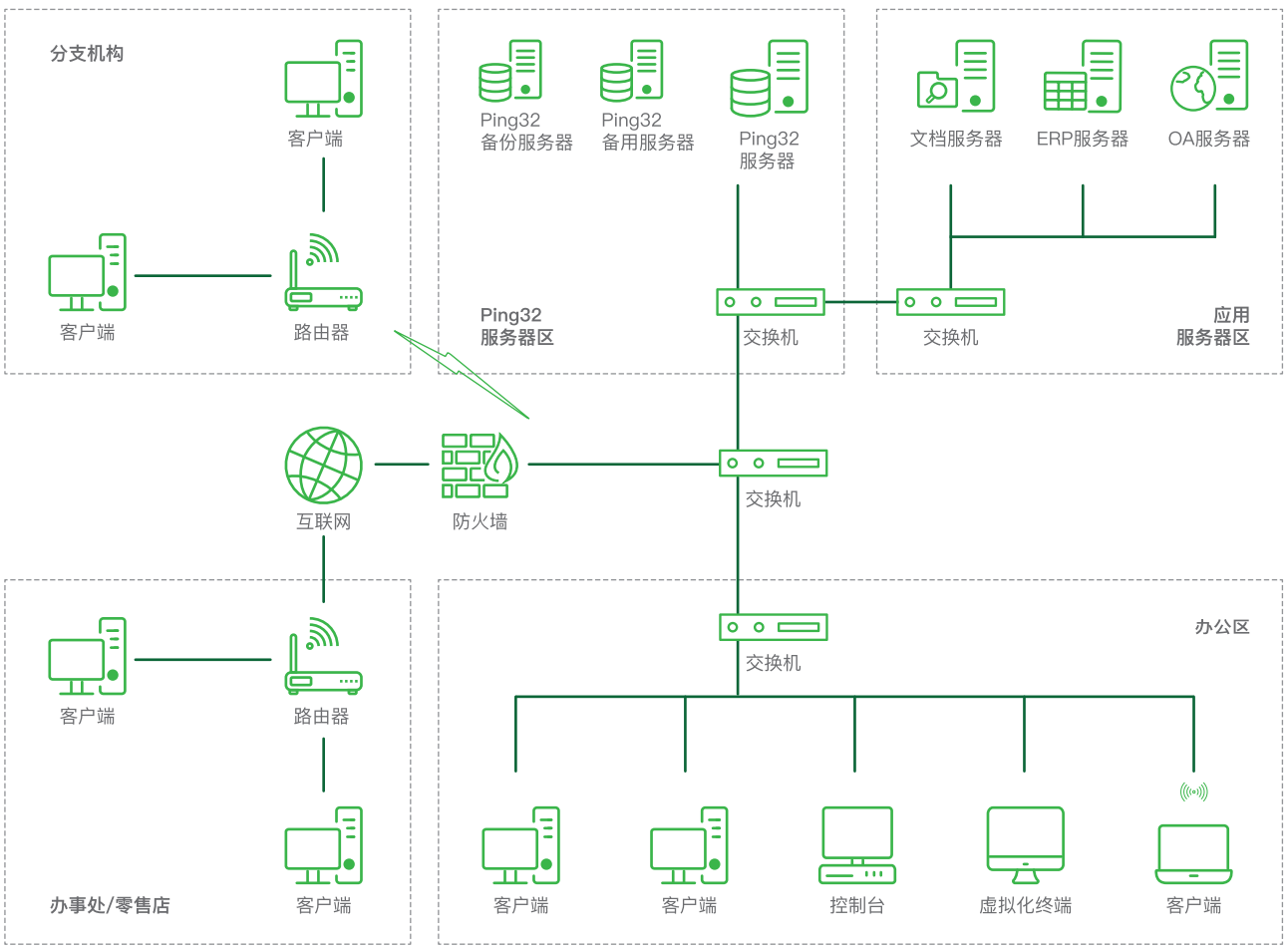
基础架构

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。



异地轻松管理

内置动态域名服务
随时，随地远程管理

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。

报表

详细、清晰、多维度、可视化

数据可视化一直是我们致力研究的目标，Ping32 内置了丰富的报表模板，无论你是自己查看，还是导出、打印给其他管理者作为绩效管理依据，Ping32 都可以提供灵活、详细、直观的可视化数据。此外，我们还进行了数据分析，比如：如果一个员工工作期间频繁访问招聘网站，那么他的离职风险将会显著增加，这些都会在报表系统中展现。

优秀的安全性

在保护企业数据安全的同时，自身也拥有优秀的安全性。

安全性是我们设计产品和服务的基础，

我们非常重视产品的安全性，因此我们做了很多工作来确保你的数据的安全性，

你的数据只属于你，任何人都没法查看或窃取。

完全的私有部署模式

完全私有的部署模式，无须借助任何第三方服务，确保你的数据安全可控。

加密的私有通信协议

私有的通信协议，支持数据加密、压缩等特性，极低的网络负载，极高的安全性。

灵活的权限体系

Ping32 支持细致的管理权限设置，可以满足不同的管理角色、管理场景需要。

操作行为支持审计

所有管理员的操作都会记录审计日志，可以随时查看是否违规。

完善的证书、资质

Ping32 拥有相关软件著作权十余项，通过了公安部信息安全产品的安全检测，并取得信息安全产品销售许可证。

Webhooks

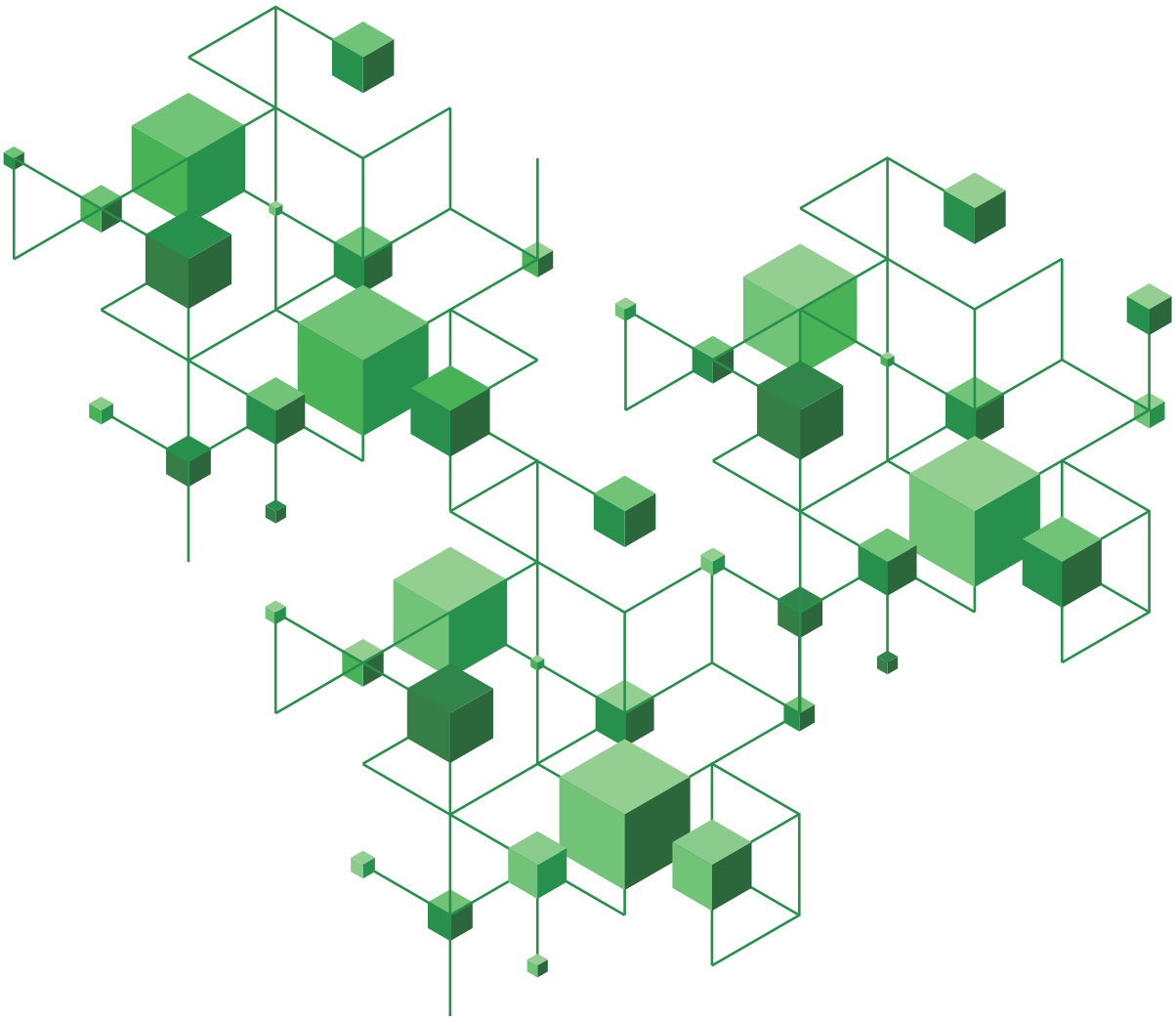
连接数据，打通自己的业务系统。

首先，Ping32 做了很多工作来确保你的数据足够安全、合规，你的数据只属于你，比如：

完全的私有化，本地化部署方式；通信协议加密，不被第三方窃取；数据不经过第三方中转，确保绝对安全可靠……

除此之外，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。



从大企业到创业公司，深受规模各异的众多企业信任。

gameloft

VOLVO

中通快递 ZTO EXPRESS

国家电网 STATE GRID

货拉拉

同程旅游 LY.com

中银国际证券

中国石油

UCC

更多案例...

nsecsoft.com/customers

即刻开始

既然你已经了解了 Ping32 是如何工作的，能帮你解决哪些问题，
那么现在你需要了解如何安装部署 Ping32。
安装部署 Ping32，你只需三步。

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.com

Contact us : design-team@nsecsoft.com

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