



扫一扫，关注官方微信

联系我们

地址：北京市海淀区西二旗大街39号A座三/四层

电话：86-10-57933888

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com



关注企业官方微信

ESAFENET Journal

中国数据安全防护专家



主办：亿赛通

策划：市场部

北京亿赛通科技发展有限责任公司

地址：北京市海淀区西二旗大街 39 号 A 座三 / 四层

电话：86-10-57933888

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com



本刊为亿赛通企业月刊，欢迎交流，禁止转载

CONTENTS 目录

刊首语 PREFACE

2/3 刊首语

行业聚焦 INDUSTRY FOCUS

- 4-7 创新网络安全治理 保障大数据时代国家安全
- 8 Gartner：2018 年全球信息安全产品和服务支出将达到 930 亿美元
- 9 德媒：中国个人数据保护有待加强
- 10-13 七成人担心用“二手空调” 质量问题和信息安全成顾虑

亿赛通动态 ESAFENET NEWS

- 14/15 亿赛通出席 P2SO 南宁站 协同“海上丝绸之路” 构建智慧安全
- 16/17 亿赛通“智慧安全” 武汉站 引领长江经济带打造新一代“智慧城市”
- 18-21 “智时代 智安全” 2017 亿赛通新产品成功发布 领略创新、智能、安全新价值
- 22/23 “智能” 悄然主宰世界？“安全” 决不罢休？亿赛通新产品双重亮相
- 24/25 创新成就价值 亿赛通数据安全市场迎高景气

亿赛通小贴士 ESAFENET PROMPT

- 26/27 别裸了！给你件衣服，穿好.....

典型案例 TYPICAL CASES

- 28/29 中海油田合作亿赛通主动出击 共创企业“智能安全”
- 30/31 亿赛通牵手中核能源 铸就企业坚不可摧的智能安全盾牌

中国数据安全防护专家

智时代·智安全

七月的风牵着记忆章节，纷飞远去，八月，塑造着巍峨。伴随互联网+大数据时代的到来，“漏洞”、“黑客”、“网络入侵”成了人们听起来不寒而栗的词汇。

2017年，严峻的网络安全重大事件悄然袭来：“WannaCry”敲诈勒索病毒、“暗云Ⅲ”变种木马、“Petya”勒索病毒、加拿大贝尔公司190万客户信息泄露、美国中央情报局数千份机密文档泄露……面对这些接连发生的重大数据泄露突发事件，一个全新的智能+、互联互通、全方位的数据安全解决方案才是当下亟需的安全保护网，在这样的背景之下，8月25号，亿赛通召开了“智时代·智安全2017新产品发布会”，体验数据安全领域不一样的感官盛宴，在这里产品的创新、智能、安全和企业多年来一路的坚持所取得的成绩让我们对亿赛通有了不一样的认识……

创新网络安全治理 保障 大数据时代国家安全



2017年5月12日，勒索电脑病毒肆虐全球。这再次警示人们，网络世界风险无处不在，倘若没有安全的甲冑，将危机重重。

网络安全无小事，没有网络安全就没有国家安全。

党的十八大以来，全国公安机关积极应对互联网带来的新机遇新挑战，坚持依法管网与综合治理并举，强化互联网安全管理，推进网络社会法治建设，走出了多条推动网络社会治理能力持续提升的新路径。

从积极构建网上网下相结合的网络社会综合防控体系，到全面提升网上“见警率”和“管事率”；从积极推动互联网企业落实安全主体责任，到进一步深化网络安全执法国际合作……维护网络安全的每一步，公安机关都留下了扎实的脚步。

筑起“防火墙”，还网络一个晴朗天空

互联网时代，个人信息安全尤为牵动公众神经。

2016年，包括徐玉玉被诈骗猝死案在内的一系列电信网络诈骗案件，给人民群众带来了极大的不安全感。网民纷纷表示，大数据时代公民个人信息在网上近乎“裸奔”。

老百姓最痛恨什么犯罪，就严厉打击什么犯罪；老百姓反映什么治安问题最突出，就集中整治什么问题。

2016年4月、2017年3月，公安部两次部署全国公安机关开展打击整治网络侵犯公民个人信息犯罪专项行动，彰显了公安机关突出打击整治网络犯罪的坚强决心。作为网络社会安全管理的主力军，全国公安机关始终把“追源头、摧平台、断链条”作为打击整治网络侵犯公民个人信息犯罪的出发点和落脚点。

针对网络诈骗、黑客攻击和侵犯公民个人信息等高发频发犯罪活动，公安部会同最高人民法院、最高人民检察院制定发布《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》，健全完善网安与各警种案件协作配合机制，依托网络犯罪举报平台，充分发动群众举报犯罪线索，不断加大打击整治力度。

针对网上黄赌毒、“黑拐枪”和售卖黑客工具、“伪基站”和窃听器材等乱象，公安部部署各地网安部门探索建立网上网下合成作战中心，与工商、广电、版权等主管部门建立协作配合机制，依法加强对网站的监管执法，集中整治网上“治安乱点”。

数据显示，2016年以来，全国公安机关累计侦办侵犯公民个人信息案件2894起，抓获犯罪嫌疑人6768名，其中银行、教育、工商、电信、快递、证券、电商网站等行业内部人员727名，查获身份信息、定位信息、出行信息、征信信息、账号密码等各类公民个人信息800余亿条。

实践证明，定期打击整治和专项行动，不仅进一步净化了网络空间，也遏制了网络违法犯罪的高发势头。

铸就安全坚盾 向网络违法犯罪说不

2015年6月，公安部部署全国公安机关普遍建立网警常态化公开巡查执法机制，首批50个省、市公安机关统一标识为“网警巡查执法”的微博、微信和百度贴吧账号集中上线。从此，网警从幕后走向前台，开展网上公开巡查执法工作。

全国372个省市两级公安机关网警大面积“现身网络”，并以公开透明的在线方式监管执法，让人眼前一亮。新形势下，建立网警常态化公开巡查执法机制，正是公安部党委合民心、顺民意、惠民生，贯彻落实全面深化公安改革、依法加强网络社会管理的具体举措。此举有利于依法维护网络社会治安秩序、有利于促进互联网健康发展，更是民心所向。

中共中央政治局委员、中央政法委书记孟建柱就公安机关维护网络安全工作提出要求，全国公安机关要紧围绕建设网络强国目标，深化改革，不断创新，完善网络治理体系，聚焦网络风险防控，切实提高维护网络安全法治化、科学化水平。

如何提高维护网络安全科学化水平？

全国公安机关普遍建立网警常态化公开巡查执法机制作出了有力的回答。网络和现实社会的发展不是两条平行线，网警队伍利用二者的契合点，用“线上工作”去解决百姓呼声高、亟待解决的“线下问题”。

党的十八大以来，全国网警不断创新工作方法，用更加符合网络传播规律的方式，拉近与网民之间的距离。各地公安机关通过各种途径和手段，扩大队伍，动员社会各界共同开创了网络群防群治新格局。

有专家赞叹：“网上巡查警示制止了一大批违法行为，受理举报处置了一大批网上警情，提升了广大网民防范意识，就像铸就的网络安全坚盾，长期呵护着网络安全。”

设立“监测站”降低“网络PM2.5”污染

众所周知，互联网企业是净化网络环境、防范网络违法犯罪的“第一道防线”。长期以来，各互联网企业积极履职，为维护网络安全发挥了积极作用，但也存在安全责任不落实、能力水平不够等问题。

作为一座创新型城市，深圳拥有一大批高科技互联

网企业和大规模的网民群体。报告显示，2008年6月底，深圳网民人数已经达到483.7万，网络普及率达51%，远高于全国19.1%的平均水平。如何突破互联网管理工作的瓶颈，成为摆在深圳网警面前的一道难题。

警力有限，民力无穷。

“让网安警务工作与互联网产业发展对接，将互联网安全管理的触角延伸到基层的实体单位上，从源头上管理好互联网。”深圳网警从机制上找到了突破口。

深圳“网安警务室”设立以来，互联网监管工作效应不断突显。特别是公安机关网安警务战略性前移，通过派驻民警进行面对面指导和服务，将网警部门的服务和管理带到了社会基层，使企业信息安全状况得到了根本改变，“服务网民、服务群众”的承诺也得到了更好的落实。

深圳“网安警务室”的经验探索恰如一面镜子，照亮的是全国互联网企业参与网络安全治理的全貌。

为进一步加强互联网企业的督促指导，搭建公安机关与互联网企业的快速沟通处置平台，2015年8月，公安部部署全国公安网安部门深入开展网站“网安警务室”建设，在重点网站和互联网企业设立“网安警务室”，第一时间掌握网上涉嫌违法犯罪情况，服务和指导网站提高安全管理防范能力。

据统计，全国目前已建成“网安警务室”1116家，在百度、腾讯、新浪等10家大型重点网站建成了一级“网安警务室”，评选出示范性“网安警务室”63家。2015年以来，各网站配合公安机关依法关闭违法有害信息频发的栏目、群组、店

铺25万家，关停违法账号47万个，在维护网络安全和网民权益方面取得了明显成效。

“网安警务室”提升网络安全感有目共睹。有网友直言，“网安警务室”好似一座座网络安全“监测站”，时刻帮助公安机关监控“网络PM2.5”是否超标。

编织“安全网” 携手构建网络空间命运共同体

人类生活从来没有如此息息相通。

江苏徐州和浙江台州，相距900千米。2013年5月25日，一场抓捕行动在这两座城市同时展开。这不是巧合，而仅仅是一个开始。一场由中美两国警方发起、全球20个国家和地区共同参与的打击儿童淫秽色情网站联合执法行动（代号“天使行动”）悄然收网。历经半年的艰苦侦查，公安机关一举摧毁儿童淫秽色情网站4个，抓获包括网站开办者、版主、重点发帖会员等境内外犯罪嫌疑人250余名。

一场抓捕，折射的是多国携手构建网络空间命运共同体的全球愿景。

互联网跨地域、无疆界，网络恐怖主义、网络淫秽色情等跨国犯罪问题突出，网络犯罪已经成为国际公害。依法打击互联网违法犯罪，切实维护互联网安全，已成为各国执法部门的共同责任。

中国政府高度重视并始终坚持依法打击网络犯罪，坚定维护网络安全。公安部持续通过双边渠道与有关国家开

展了一系列国际执法合作活动，对网络违法犯罪保持高压打击态势。

2015年9月，习近平主席成功访美，两国元首在网络安全问题上达成重要共识，决定建立打击网络犯罪及相关事项高级别联合对话机制。2015年12月、2016年6月、2016年12月，中美双方举行了三次打击网络犯罪及相关事项高级别联合对话，达成了《打击网络犯罪及相关事项指导原则》，建立了热线机制，并就网络安全个案、网络反恐合作、执法培训等展开合作；2016年6月13日，中英举行首次高级别安全对话，双方就打击恐怖主义、网络犯罪等领域合作达成重要共识；2016年9月12日，中国与加拿大举行首次高级别国家安全与法治对话，双方就反恐、网络安全与打击网络犯罪等进行深入磋商；2016年11月23日，中国与白俄罗斯就深化打击网络犯罪和其他跨国有组织犯罪活动等方面达成重要共识……应该说，一个针对网络犯罪的“全方位、宽领域、多层次、讲实效”国际执法合作工作格局已初步形成。

建久安之势、成长治之业。纵观科技发展历史，网络安全治理注定是一场“持久战”和“攻坚战”。公安机关不仅始终冲在最前，而且将全力以赴推进创新治理，保障大数据时代的国家安全。（新闻来源：新浪司法）

Gartner：2018 年全球信息安全产品和服务支出将达到 930 亿美元

根据 Gartner 的最新预测，2017 年，全球信息安全产品和服务支出将达到 864 亿美元，比 2016 年增长了 7%，预计 2018 年将增长到 930 亿美元。

在基础设施保护领域，由于数据泄露频繁发生，以及对应用程序安全测试的需求不断增长，Gartner 预测，新兴应用程序安全测试工具将成为信息安全产品和服务支出增长的一个重要的动力。

安全服务仍然是增长最快的部门，特别是 IT 外包、咨询和安装服务。由于虚拟设备、公共云和软件即服务（SaaS）版本的安全解决方案的普及，硬件支持服务增长将放缓，对硬件支持的需求也将有所下滑。

Gartner 最新信息安全市场预测是以以下假设为前提的：

欧盟一般数据保护条例（GDPR）引起了人们的重视，到 2018 年，将推动 65% 的数到 2020 年，所有管理安全服务（MSS）的合同中，40% 将与其他安全服务和更广泛的 IT 外包项目捆绑在一起，和目前的 20% 翻一番。



到 2021 年，中国 80% 以上的大型企业将利用本土供应商部署网络安全设备。

中国最近批准的网络安全法将有助于中国本土供应商进一步取代美国制造的网络安全产品。

2016 年，亚太地区终端用户在信息安全方面的支出增长了 24%，但由于平均销售价格（ASP）的下降，Gartner 预计，2018 年开始增长率将下降至一位数。（新闻来源：北京时间）

德媒：中国个人数据保护有待加强

截至去年 12 月，中国有 7.31 亿互联网用户。随着在线服务的快速增长，个人数据保护已经成为一个特别大的问题。

德国《时代》周报网站 8 月 20 日报道称，去年一名山东女学生受骗的轰动案件引发中国媒体关注：她的全部大学学费被一个网络诈骗团伙骗走。犯罪分子使用的诱饵是他们从数据库中获取的有关她——以及其他 60 万名学生——的数据。

中国网民根本不注意保护自己的隐私。外国公司和学者也经常传播这样的观点。的确，很大一部分中国人，特别是年轻人几乎用智能手机支付一切。他们的智能手机通过相应的应用程序与银行账户或信用卡绑定。像滴滴出行等非常受欢迎的服务软件一直要求公开地理位置数据，这对用户来说似乎没有问题。舒适第一，顾虑第二。

波士顿咨询公司 2014 年的一项调查结果显示，只有一半的中国受访用户认为必须谨慎对待分享个人数据，这个比例比另外 10 个国家受访用户的平均水平低 26 个百分点。在具体对待数据方面，中国也显得更轻率：63% 的受访者认同信用卡信息是“相对甚至非常隐私的”。这个比例在美国是 87%，在德国甚至是 93%。

报道称，事实上，在对待数据保护方面，中国的互联网用户行为分裂：在短短几小时内就有数千人参加数字围猎行动，即所谓的“人肉搜索”。他们搜集相关人员的个人信息并在互联网上发布。在受害者的照片、电话号码和住址被公布后，接下来有时还会出现威胁和报复行为。



失密

新华社发 朱慧卿 作

报道称，涉及保护自己的信息时，中国网民则显得更为忧虑。今年 6 月的最新数据泄露事件涉及苹果产品用户，他们大多是中产阶级。一些苹果公司中国区员工以非法手段获取苹果手机关联的公民个人信息，并在网上进行出售，涉案金额超过 5000 万元人民币。自今年年初以来，知乎和天涯等知名社交媒体平台上就经常有人警告不要轻易公布自己的数据，或者给出如何更好保护自己的技巧。

报道称，迄今为止，中国还没有统一的个人信息保护法。2003 年受国务院委托起草的相关法律草案自 2008 年起搁浅。目前生效的是一些相互重叠的行业法规，例如银行业、电子商务或电信领域的法规。

中国政府最近在更有效地保护个人数据方面采取了一些措施。2016 年底，全国信息安全标准化技术委员会将制定个人信息安全规范标准列为重点项目。今年 5 月，该委员会又对外发布了《信息安全技术数据出境安全评估指南（草案）》。（新闻来源：新浪中心）

七成人担心用“二手空调” 质量问题和信息安全成顾虑



共享经济的风口吹得各种“共享”满天飞舞。共享家电也参与其中，除了共享洗衣机和共享彩电之外，第三个共享家电产品——共享空调，开始登场。据了解，某品牌共享空调将在2017年10月1日开始投放，广州为首个试点投放城市。这也意味着，未来你家里用的空调可能都不是你的。

调查数据显示，针对共享空调，有人兴趣浓厚，图的是方便，超三成人士表示会使用；但也有人顾虑很多，超七成人表示最怕“二手货”。还有人担心使用共享空调会存在信息安全问题。因此，共享空调在家庭推广预计有一定难度。



共享空调：可免押金拆装免费 使用1小时1元

“什么？空调也能共享，这个很有意思。”当记者提出共享空调概念的时候，广州市民章女士就很惊讶，也很好奇。她说：“共享单车、共享图书等都好理解，但共享空调算是个新鲜的玩法。”可谓是共享经济是个“筐”，什么都可以往里面装。

近年来，共享单车、共享汽车、共享充电宝、共享篮球、共享雨伞等新形态不断涌现，深刻地影响着人们的消费方式和生活理念。乘着共享经济的风潮，家电业界也开始跃跃欲试。广东一家空调企业将在10月1日开始投放共享空调，广州成为首个试点投放城市。

据解到，该共享空调主要采用物联网、大数据等新技术手段，实现“押金+按时收费”的可消费者支付一定押金之后，可通过扫描二维码充值、开机并使用。循环模式，如消费者下载共享智能空调APP，并实名注册便可以成

为潜在客户，只要发布需求，距离最近的线下服务商接到APP订单后，就会送货上门安装。

推出这一业务的空调企业工作人员称，共享空调目前主要有两种获取方式：“一种是使用现金付押金，暂定为900元；一种是凭借支付宝信用免押金租用。”至于收费问题，工作人员称，目前的使用费是每小时1元。另外，空调的安装和拆卸均不收取费用。

记者测算，除了押金和电费外，使用费每小时1元，如果平均每天使用6个小时，一个月下来就是180元，一般空调使用的高峰期为5~10月，那么6个月算下来费用共计1080元。

共享空调成租房族“最爱”

“共享空调”这一新事物引起了不少市民的兴趣。本报针对“你会使用共享空调吗”的网络调查显示，有不少人对共享空调跃跃欲试，背后图的就是“方便”，对押金的关注排在了第二位。

本报关于共享空调的网络调查共有287人参与，调查结果显示，在受访对象中，有37.98%的人表示“有兴趣”，36.93%的受访者表示“会尝试”。而对共享空调来说，最吸引人的优点是方便，超过45%的受访者（132人）认同这个观点，还有同样数量的人觉得共享空调能减少他们的顾虑，即使经常搬家，也可以轻松使用空调。

“这个空调是怎么共享的，我都想去弄一台试一试。”广州某国企中层管理人士杨先生说，如果是不用押金，像某些共享产品依靠个人信用的话，就可以试一试。

从北方南下的白领赖女士告诉记者，目前她是租房子住，“如果房东没有配空调，自己还得去买，以后换房子了还得搬来搬去。要是能租空调用，还是方便很多。我个人还是很支持的。”赖女士称。

“啥都不用买了，现金为王了！”这是90后小伙子小罗对未来十年共享经济之下的生活想象。他说，房子可以共享，而冰箱、洗衣机和空调在不久的将来，都可能走向共享。

顾虑也不少：质量问题和信息安全

根据记者了解，当前市民对共享空调的顾虑并不少，而担心用到“二手货”的市民竟然最多。一位业内人士指出，实际上，从不同的使用场合，对共享空调的顾虑也是不一样的。如学校、医院、酒店等具有公共属性的共享空调，市民最关心使用二手货可能带来的质量问题，而家用共享空调最担心的是安全。

顾虑一：“二手货”

35岁左右的聂先生正准备在广州经营一家小餐馆。装修时，仅空调就要花费好几万元。不过，他虽然对这种共享空调很感兴趣，但是最担心“二手货”容易出问题。

本报“广调查”数据显示，受访者担心用到二手空调的比例竟然高达76%，有220人选择了该选项。有观察人士就指出，消费者对“二手货”的担忧是可以理解的，因为，二手空调一般使用时间较长，有些是经过翻新的，质量没



有办法保证。“要是给我装了个二手货,是很容易出问题的,即使厂家会承担维修费用,但客户体验不好,也会影响生意的。”聂先生称,用过的空调还容易产生安全隐患。

顾虑二：信息安全隐患

广州市民王女士不太接受共享空调,在这位宝妈看来,共享空调信息安全隐患比较大,“现在到处都是共享,个人已经没有什么隐私了,比如去个银行,什么信息都能看到;也没有多少隐私空间了,骑个共享单车,你的行踪人家都知道。现在基本上只剩下家里的一点隐私空间了。如果用了共享空调,你的行踪,作息时间都暴露了。”王女士认为,在当前对信息安全监管还不太严的情况下,虽然共享空调看似方便,但暂时不会使用。

因此,有专家认为,从隐私安全角度看,共享空调最

初可能会在学校、酒店、工厂、博物馆、图书馆等具有公共属性的领域发挥作用,家庭推广暂时有一定难度。

企业：5年可回本

“传统的租赁不同,共享经济的模式就是要应用新科技手段。”美博空调相关负责人表示,共享空调将为家电业创新商业模式探索出一条新路,未来租赁市场也将为共享空调提供广阔的市场前景。

而对企业来说,收回空调成本一般在五年左右。“比如一台空调3000元,按照每小时1元,每天使用6小时,每月使用20天测算,一个月120元,使用5个月计算,每年收回600元,这样计算5年就可以收回成本。”美博共享空调负责人称。

业界：未来潜力大

2017年4月,北京出现共享冰箱发放食物,5月扬州出现首台“共享冰箱”。相比冰箱,很多人对共享洗衣机并不陌生,最常见的就是,高校宿舍投放洗衣机,消费者通过手机APP下单预订,移动支付后就可以使用。

但对于商家和创业者而言,在家电三大件中,共享空调的潜力可能最大。中怡康白色家电事业部总经理魏军称:“空调继洗衣机之后,将在共享家电领域崭露头角。”他分析指出,空调市场规模体量大是共享经济的基础。数据显示,家电三大件中空调价格相对较高,今年上半年空

调零售额为1095.3亿元,同比增长31.9%。冰箱零售额430.1亿元,同比增4.8%。而洗衣机零售额为322.6亿元,同比增10.3%。而且空调的拥有率高,但使用率低。数据显示,2013年到2015年期间,城镇每百户拥有空调分别为102台、107台和115台,而冰箱和洗衣机都在100台以下。因此,他认为,相比冰箱和洗衣机,空调的共享潜力最大。“我们预计2018年共享空调规模在18亿元左右,2019年上涨到25亿元。但到2022年,这个规模有望超过百亿元。”魏军称。

(新闻来源:华龙网)

亿赛通出席 P2SO 南宁站 协同 “海上丝绸之路” 构建智慧安全



广西地处华南经济圈、珠三角经济圈、北部湾经济圈的交汇处，同时作为 21 世纪海上丝绸之路的经济带，将迎来前所未有的历史发展机遇。对此，针对广西数据安全市场现状、发展趋势等情况，8 月 4 号，亿赛通携手绿盟科技于南宁市再次举办了“智慧安全 2.0”大会，并与华南参会嘉宾一起深入探讨：如何让“智能安全”推动华南经济稳健发展，让“一带一路”战略实施顺利通向东盟市场前沿阵地，形成欧亚大陆经济整合的大趋势。



构建智能安全 助推“海上丝绸之路” 经济发展

亿赛通精英伙伴为南宁市与会嘉宾分析到当下智慧城市如何融合“21 世纪海上丝绸之路”战略推进城市经济、文化、政治的繁荣。在新一代信息技术和知识经济的加速发展的背景下，以智慧技术、智慧产业、智慧民生、智慧城市管理等为重要内容，实现城市各功能协调运作，为市民提供更高的生活品质。

亿赛通作为中国数据安全防护专家，根据广西“一轴两带多中心”、“海上丝绸之路”等区域发展战略，为全面建设广西经济发展，提高人民的综合水平，携手广西努力建设“智慧城市”，打造“智慧安全”。如亿赛通伙伴分享到具体的成功案例，其公司智能数据安全加密产品，携手国内众多城市对其网络安全进行智能化方案部署，层层防护，实现对全网数据进行智能化的加密管控，有效的保护了其重要信息的安全，促进了城市信息安全管理更加智能化、有序化，提高了智慧城市的建设能力。面对广西城市建设发展需求，亿赛通更加有信心携手打造“智慧安全”网络环境，实现华南区域经济与社会协调发展，打造真正意义上的智慧城市。



携手华南“安全”领域 共创智慧城市

通过亿赛通精英伙伴详细透彻的介绍，现场嘉宾对公司的产品和方案产生了浓厚的兴趣。在智慧安全信息时代，亿赛通从未止步，持续稳居数据安全市场第一；在核心技术上，坚持创新，拥有业内前沿的技术，带领行业前行。亿赛通数据安全防护产品及方案，坚持通过精心的顶层设计和完善的基础建设，并且从技术、服务、智能化管理手段等方面共同着手，推进“智慧安全”时代全面化进程做出努力。对于未来几年内数据安全市场的发展趋势、面临的挑战等一系列问题，亿赛通精英伙伴和嘉宾也进行了深入的讨论，并坚持与华南区域伙伴一路同行，共同创造华南区智慧城市。

新闻来源：亿赛通华南大区

亿赛通“智慧安全”武汉站 引领长江经济带打造新一代“智慧城市”



8月24号，亿赛通携手绿盟科技举办“智慧安全2.0”全国巡讲活动武汉站再次成功举办。华中区作为长江经济战略发展地带，为促进当地努力对接“一带一路”战略发展，亿赛通“智慧安全”牵手华中区域引领长江中游城市打造新一代“智慧城市”，促使长江经济带成为充分体现国家综合经济实力、竞争力与合作的内河经济带。在武汉大会期间，亿赛通结合当地经济战略发展，深刻的与华中区域的所有与会嘉宾再次分享了智慧安全时代面临的挑战以及未来的发展趋势，并积极探索了如何更好的满足华中市场的需求。



“智能安全”助推长江经济带“智慧”发展

在“互联网+”的迅速发展背景下，新的发展趋势冲击着原有市场的发展状态，智慧安全已经成为当下发展不可逆转的方向。对此，“智能化”成为热议话题。在武汉大会上，亿赛通精英伙伴用智能重新诠释安全。华中区是极具全球影响力的内河经济带，发挥着长江经济发展的独特作用，为推动华中区能够更好、更快的实现产业结构升级、打造世界级产业集群，培育具有国际竞争力的经济带，亿赛通“智慧安全”全力融合区域战略发展，将智能安全产品结合数字化、网络化、智能化技术，为城市信息资源共享、区域经济运转高效、社会服务能力加强，提高“智慧城市”建设的能力，使长江经济带成为推动我国区域协调发展的重要示范。



坚持创新 牵手同行

通过亿赛通精英伙伴详细透彻的介绍下，华中区现场嘉宾对亿赛通“智慧安全”产生了浓厚的兴趣。通过多年打造，亿赛通数据安全市场地位稳居行业前列，坚持从技术、服务、智能化管理手段等方面共同着手，推进“智慧安全”时代全面化进程做出努力。对于未来几年华中区域经济的发展趋势、面临的挑战等一系列问题，亿赛通精英伙伴也与华中区参会嘉宾进行了深入的讨论，亿赛通坚持一路同行，坚持创新发展模式，坚持与华中区共同推进我国腹地经济区域发展。

新闻来源：亿赛通华中大区

" 智时代 智安全 "

2017 亿赛通新产品成功发布

领略创新、智能、安全新价值



如今,伴随互联网+大数据时代的到来,“漏洞”、“黑客”、“网络入侵”成了人们听起来不寒而栗的词汇。2017年,严峻的网络安全重大事件悄然袭来:“WannaCry”敲诈勒索病毒、“暗云Ⅲ”变种木马、“Petya”勒索病毒、加拿大贝尔公司190万客户信息泄露、美国中央情报局数千份机密文档泄露.....面对这些接连发生的重大数据泄露突发事件,一个全新的智能+、互联互通、全方位的数据安全解决方案才是当下亟需的安全保护网,在这样的背景之下,8月25号,亿赛通召开了“智时代·智安全2017新产品发布会”,体验数据安全领域不一样的感官盛宴,在这里产品的创新、智能、安全和企业多年来一路的坚持所取得的成绩让我们对亿赛通有了不一样的认识.....



成大事不在于力量的大小,而在于能坚持多久。

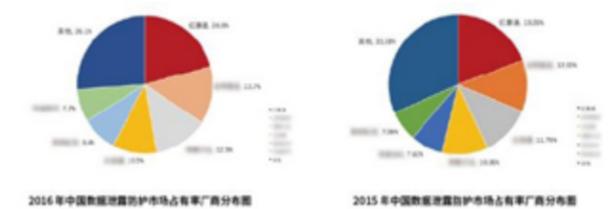
——约翰生

“专注”应万变 “专业”赢市场

之所以说亿赛通新品的推出引人注目,最重要的一点就是这个耕耘中国数据安全防护领域14年的老牌企业,这一次不仅带来了满足市场亟需的产品,更重要的是,蕴含在产品之中的“智能、互联、移动安全”等创新技术、创新应用解决方案让业内对亿赛通有了“新”的认识。

“创新”铸造真价值 智能、移动、互联成关键

作为中国数据安全防护专家,14年来亿赛通都在用“专注”书写着自己在安全领域的历程。截止目前服务的客户超过万家企业,终端活跃用户过百万。业内服务规模覆盖28个省市、4个直辖市,开创11项技术先河,获得了30余项软件著作权及百项荣誉证书。



这些数字已经足以说明,在激烈的市场竞争中,多变的 market 环境下,亿赛通在专注中成为了安全领域最为权威和专业的企业,从而赢得了客户并不断发展壮大。专注成就了亿赛通的成长,使得其对于市场的走向,客户需求的把握更加专业,从而对市场把握更为精准,面对数据泄露防护市场竞争越发激烈的今天,早已布局数据泄露防护领域的亿赛通获得了先机。2015年,亿赛通以19.2%的市场占有率,位居中国数据泄露防护市场第一名。2016年在激烈的市场竞争环境下,继续发力以20.6%市场占有率连续排名第一。

毫无疑问,几近完美的数字,让亿赛通在安全领域备受瞩目,据2017年CCID最新权威报告显示,亿赛通市场份额在同行业其他品牌厂商中占有率连续多年稳居第一,成为数据安全行业的主力军。而创造这些数字的真正“武器”,成就亿赛通实现迅速增长的秘诀,必然是产品和市场战略。总结而言,前瞻性的关键技术、不断创新的产品解决方案和市场销售策略,就是亿赛通在变化莫测的市场快速占领高地,创立了一座又一座新的里程碑的“秘诀”。



智能管理平台 数据安全卫士

在技术和产品方面，互联网、大数据、云计算、人工智能等成为当下行业发展的新趋势，亿赛通又一次发布的产品解决方案结合当前“智能、移动、互联”等新趋势关键词，方案极具前瞻性的尖端技术，整合所有终端模块形成一个统一管理平台，对数据进行智能识别、智能审计、智能加密解密，充分运用智能加密技术。两款新产品分别是数据安全卫士和数据安全智能管理平台。

其中，亿赛通数据安全卫士开启“个人版”新模式，主要是针对“个人”PC端的重要数据和核心资料外发安全需求设计的个人版安全产品。当用户需要将涉密文件发给他人的时候，接收者打开文件首先需要进行身份认证，方可阅读。并且发送者可对外发文件的使用者进行阅读次数、使用时长、内容拖拽、截屏等细粒度安全控制，从而有效防止重要信息在存储中，以及外发、传输给第三方时被有意或无意非法扩散。“简单、易用、安全、可控”是这款产品的最大亮点。免费注册后即可使用。

另一款产品，亿赛通数据安全智能管理平台（简称“DSIP”），是一款融合机器学习、大数据分析、文档加密、访问控制、关联分析、数据标识等技术的综合性数据

智能安全产品，可帮助用户对结构化和非结构化数据进行数据治理（资产统计、分类、聚类、分级、密级标识等）、安全管控（数据加密、权限管理，数据脱敏、边界防护、应用准入、行为审计、数据防护等）、态势感知（趋势分析、风险预警、溯源、风险人员画像等），为用户的核心数据资产从终端、网络、存储、应用等全方位提供全生命周期保护，在确保组织敏感数据安全前提下，不管控、不影响非敏感业务开展的体验度，实现安全与效率的最大平衡。这款产品应用领先的系统构架设计，更加智能化地为用户提供全方位、多层次、高效的数据安全防护。

显然，从两款新产品结合的新趋势和特点，可以分析出，亿赛通下一步的市场战略将立足于打造全方位、立体化、多层次的数据安全堡垒，并且越来越看重智能化，面向的客户群体既有企业又有个人。

占领高地 布局市场快速前行

正如上述所言，一个不断“创新”的专业企业，精准把握市场动态，有了绝佳的“武器”之后，便要布局市场，占领高地。毕竟，市场营销的优秀成绩离不开布局战略，这一次，亿赛通坚持合作伙伴战略和超前的服务理念。

据了解，2017年亿赛通不断努力完成在行业市场的突破、地市业务的创新。截至目前，亿赛通已经在全国三十余个主要城市设立了分支机构，覆盖全国的营销及服务战略布局基本完成。渠道体系的建设已经成为了亿赛通稳步前行的基石。当然，伴随着亿赛通全国招募的近百家渠道的合作开展，规范的渠道政策和渠道管理方式也在逐步成型，而吸引渠道合作伙伴的最大动力集中在三点“好产品、好价格、好服务”。另外，近年来，亿赛通也同很多云服务厂商合作，共同开拓新型数据安全战场。



开花结果获殊荣 成就未来

在客户服务上，14年来，亿赛通已经服务了包括党政军、研发通信、金融、能源、设计制造、运营商、各大企业集团等领域的客户，这些领域的众多企业一直同亿赛通保持着良好的合作关系。这与亿赛通专业而完善的服务体系相关。

今天，依靠坚实的合作伙伴渠道架构和客户服务体系，亿赛通获得了国家、媒体、客户授予的众多荣誉，在2017年上半年，亿赛通荣获智能时代·数字经济“2016-2017中国DLP市场年度成功企业”；再次获得B级军用信息安全产品资质证书；由国家公安部颁发的亿赛通数据泄露防护（DLP）系统V5.0、亿赛通电子

文档安全管理系统V5.0、电子文档安全管理（一级）销售许可证和亿赛通安全网关V5.0、亿赛通虚拟终端管理系统V2.0两款产品的软件著作权登记证书。更是一举成为中国大数据产业联盟，中国保密协会，中国商用密码保护协会，全国信息安全标准化技术委员会的高级会员。

总之，这一路的荣誉、良性成长，客户拓展，融汇着亿赛通员工的汗水和付出，更指向着亿赛通的未来前进方向。中国数据安全问题任重道远，继续打造“智能安全，智慧未来”，将是亿赛通持续发展的方向。

“智能” 悄然主宰世界？ “安全” 决不罢休？ 亿赛通新产品双重亮相



在互联网迅猛发展的时代，信息泄露事件逐年成倍增长，信息安全是如今社会人们关注的焦点。近年，互联网、大数据、云计算、人工智能是发展热潮，数据安全行业必须结合新趋势，才能阻断遏制数据安全面临的新威胁。因此，一个全新的智能+、互联互通、全方位的数据安全解决方案才是当下亟需的安全保护网。

企业级智能安全管理平台

在此背景之下，2017年8月25号，亿赛通在北京香格里拉酒店召开了“智时代·智安全 2017 新产品发布会”，针对企业级用户重磅推出“数据安全智能管理平台”，用智能诠释安全，以智能发现、智能防护、态势感知、领先技术、安全可控等全新功能亮点引爆全场，独一无二的前沿技术再一次开创先河，重新定义了数据安全市场，旨在更好地满足企业对信息资产的安全保护需求，让各行各业的数据真正实现“智能安全管控 态势感知威胁”。

亿赛通“数据安全智能管理平台”是一款融合机器学习、大数据分析、文档加密、访问控制、关联分析、数据标识等技术的综合性数据智能安全产品，可帮助用户对结构化和非结构化数据进行数据治理、态势感知，为用户的核心数据资产从终端、网络、存储、应用等全方位提供全生命周期保护。



个人版数据安全卫士

如今，数据安全市场上更多目光投向各大行业、企业级的数据资产安全防护。在针对个人信息安全保护方面无论个人意识、信息安全解决方案都重视不够、投入不足。此外，由于在互联网时代新的安全威胁不断衍生，突发性、多样性、高级化等威胁特性让大家防不胜防，给个人带来了不堪重负的信息泄露担忧。

亿赛通数据安全卫士是针对个人 PC 端的重要信息或核心资料在外发、分享、存储中的安全需求而设计的个人版安全产品。当您需要将涉密文件发给他人时，接收者打开文件首先需要进行身份认证，方可阅读。并且发送者可对外发文件的使用者进行阅读次数、使用时长、内容拖拽、截屏等细粒度安全控制，从而有效防止重要信息在存储中，以及外发、

传输给第三方时被有意或无意非法扩散。

再也不怕个人知识产权被别人窃取
再也不怕电脑丢失而使数据被泄密
再也不怕个人网盘存储数据不安全



技术大咖对话

据媒体报道，亿赛通技术大咖坐镇发布会，阐明“全新智能安全产品是亿赛通采用领先的技术，并对用户、应用程序和基础架构所生成的数据进行实时跟踪、监督，防护敏感数据外泄，有效的对客户敏感数据进行智能化综合防护管控”。此次两款企业级与个人版产品的推出，将对数据安全领域的技术革新起到举足轻重的作用，又一次成为智能时代的缔造者。

创新成就价值 亿赛通数据安全市场迎高景气



近两年重大安全事件频发，局势日益严峻。如 2017 上半年严峻的网络安全重大事件悄然袭来：“WannaCry” 敲诈勒索病毒、“暗云Ⅲ”变种木马、“Petya”勒索病毒……面对这些接连发生的重大数据泄露突发事件，2017 年中国工信部首次明确提出信息安全产品纳入目标中，提出到“十三五”末达到 2000 亿元，年均增长 20% 以上。

基于安全产业的快速变化，2017 年 8 月 25 日一个全新的智能 +、互联互通、全方位的数据安全技术大会震撼上映，亿赛通“智时代·智安全 2017 新产品发布会”在北京香格里拉酒店成功举办，在这里体验了一场不一样的感官盛宴，产品的创新、智能、安全和企业多年来一路的坚持所取得的成绩让我们对亿赛通有了不一样的认识……

创新成就价值

我们知道，2014 年绿盟科技对外宣布收购亿赛通 100% 股权，成功打响在数据安全领域迄今为止最大金额的一次收购案，成功整合的背后，对双方业务的互补延展都起到重要作用，充分实现了为用户提供一站式的信息安全产品、服务和解决方案，“内外兼顾”共同创造新的利润增长点。

据国内权威赛迪报告指出：2015 年，亿赛通以 19.2% 的市场占有率，位居中国数据泄露防护市场第一名。2016 年在激烈的市场竞争环境下，继续以 20.6% 占据市场排名第一。14 年来亿赛通不断用“专注”书写着自己在安全领域的历程。

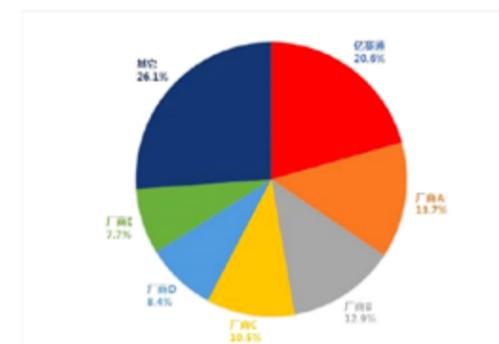


图 1：2016 年中国数据泄露防护市场品牌结构（来源：赛迪顾问 2017.6）

行业增长分析

数据泄露防护市场充满挑战与机遇，从 2016 年的市场研究报告中得知，2016 年市场总规模达到 6.2 亿元，同比增长 21.2%，预计 2017 年我国数据泄露防护市场规模将达到 7.6 亿元，同比增长 22.3%，市场发展潜力巨大，尤其华北市场占据主力约 31.5%，华东市场次之约 28.6%，华南约 17.7%，西南约 10.3%，华中约 5.0%，东北约 3.7%，西北约 3.0%。如何布局、如何力争站稳脚跟是每一个数据安全厂商应该认真思考的问题。

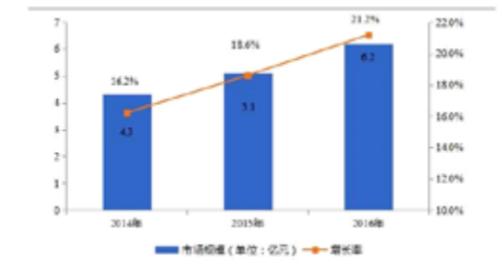


图 2：2014-2016 年中国数据泄露防护市场规模及增长情况

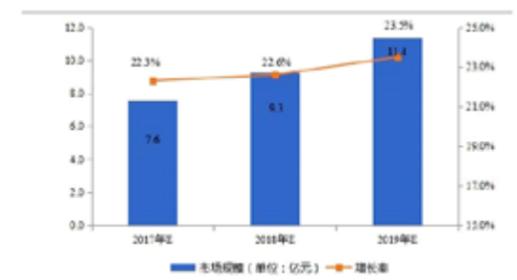


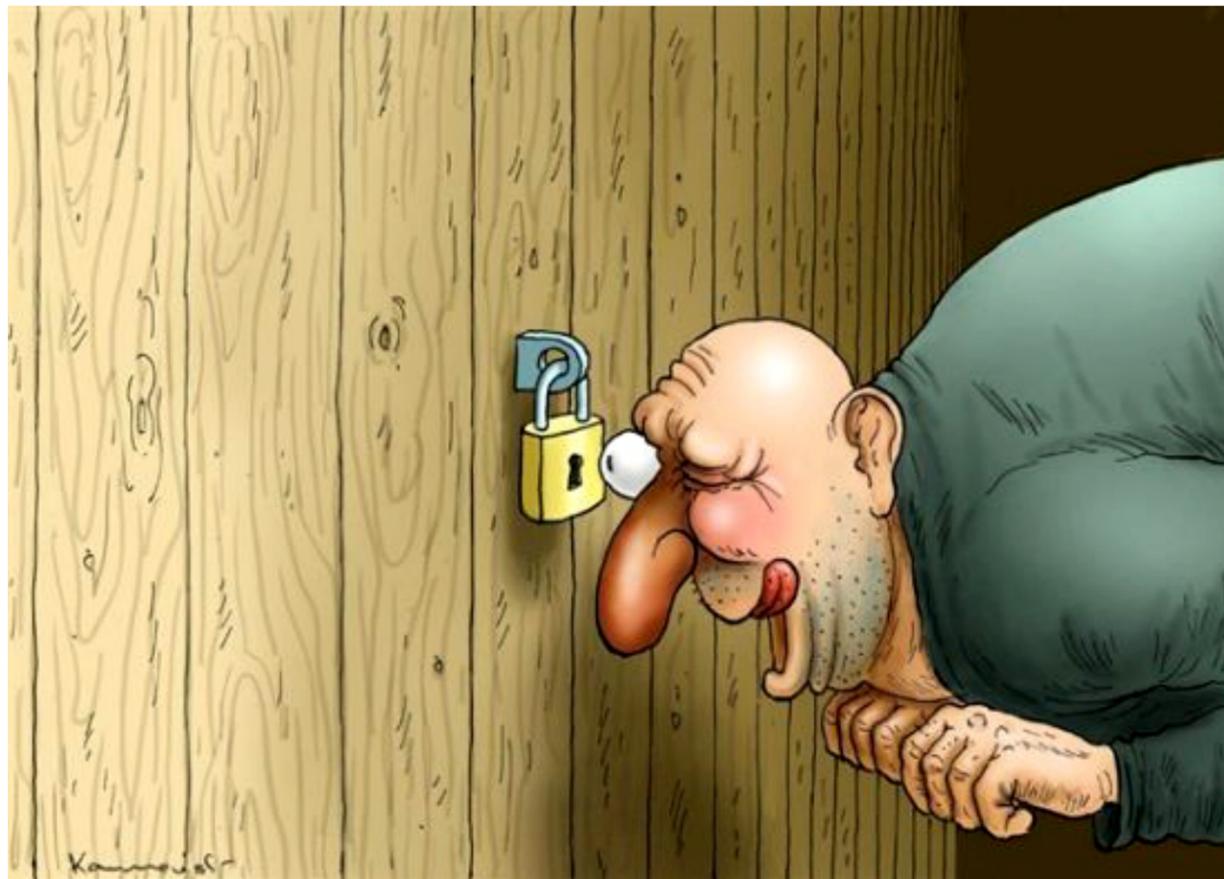
图 3：2017-2019 年中国数据泄露防护市场发展预测

紧贴市场 抢占先机

一个不断“创新”的专业企业，能精准把握市场动态，有了绝佳的“武器”之后，便要布局市场，占领高地。毕竟，市场营销的优秀成绩离不开布局战略，这一次，亿赛通坚持超前创新的服务理念、前瞻性的关键技术、创下了一座又一座新的里程碑“秘诀”。

在激烈的市场竞争中，多变的 market 环境下，亿赛通在专注中成为了安全领域最为权威和专业的企业，从而赢得了客户并不断发展壮大。专注成就了亿赛通的成长，使得其对于市场的走向，客户需求的把握更加专业，从而对市场把握更为精准，面对数据泄露防护市场竞争越发激烈的今天，早已布局数据安全领域的亿赛通获得了先机。将销售市场划分为华南、华东、华北、华中、东北、西南、西北七大区域，行业客户遍布党政军、金融证券、研发通讯、设计制造、运营商、能源、企业集团等各个领域，在业内已形成良好口碑。

别裸了！给你件衣服，穿好.....



在这之前，
宝宝先来张这样的皂片，



大哥，实在看不下去了，能不能别裸啦！！！！

你真觉得你 PC 端上“秘密”存储的资料分享给他，
他扭头就帮你守住了灵魂？
别无邪了，
除了他可能出卖你的秘密资料之外，
在“秘密”外发传输的环节，还有“盗贼”期间抢劫，
哎呦，妈呀，咋就没意识到呢？
还有更无邪的呢，
你敢说，你那啥啥网盘里不存点小小小秘密？
咋，你是不是想歪了.....



宝宝说的是“秘密”，
大哥，别傻了，那啥啥网盘里搁的秘密真的不“安全”，
宝宝这么跟你说，
譬如你那裸皂、avi、与某某的亲密 cp 皂、重要数据、
客户资料.....
这些事重大的秘密放在自己申请的某网盘里，
就相当于“皇帝的新装”，
啊哈哈，
“皇帝的新装”
懂吗？
懂吗？
懂吗？
小学知识点啊！！！！



“你”谁啊，有什么资格说俺的东西放那啥啥网盘里
不安全，
宝宝坚持 14 年专业负责“防盗”，
所以啊，
重点 ZAI 这里，<http://www.2c.esafenet.com>
数据安全卫士
数据安全卫士v1.0
就是这款东西，
TA 不仅能帮你加密那些灰常灰常秘密的小视频，事关
你“钱”途发展的重要资料、独门技术、专利、理财数据
等等等等等等等等等等的保密资料，
用它加密，
就算有人盗走你的资料，甚至想背叛你将你发送的保
密资料扩散，没有大哥你的权限允许，天王老子也拿不走，
呵呵.....从此，
再也不怕个人知识产权被别人窃取了，
再也不怕电脑丢失而使数据被泄密了，
再也不怕个人网盘存储数据不安全了！
宝宝说了这么多，
不知道大哥明白了这其中的良苦用心了没，
不说了，反正这款东东免费注册、使用超简单，
关键是能让你的“秘密”更加安全的存储、传输、外
发和分享安全！！！！
再说一遍下载地址：<http://www.2c.esafenet.com>
说一万遍都不如大哥亲自体验一把！
今日宝宝福利大特派，价值 366 元 / 个的激活码，抢
先领，手慢全无~~

亿赛通数据安全卫士“激活码”赠送活动									
89Wf	THmZ	vELU	XixZm	a8Pd	z5cW	uT5z	4v4v	59Ae	NRvQ
Cb3o	OqOq	K7aY	VUmC	WHdQ	KusM	xsx6	hqCG	g63f	ZvM2
C93o	jE2z	hyli	YChC	2n7e	ybdM	C2IQ	xpAu	NnhN	uKYy
mluT	vq6h	g84Q	RERW	x9fE	vAID	3xqv	EkHf	DVCc	LD0w
Hbea	piou	ze8U	jQZr	2hTd	2MVI	XPBZ	Fo6N	B3qc	hvla

中海油田合作亿赛通主动出击 共创企业“智能安全”



客户介绍

中海油田服务股份有限公司（简称“中海油”）是亚洲最具规模的综合型油田服务供应商。服务贯穿海上石油及天然气勘探，开发及生产的各个阶段。中海油拥有亚太地区最强大的海上石油服务装备群。公司的服务区域涵盖中国海域，并拓展至亚太、中东、美洲、欧洲四大区域，覆盖全球 30 多个国家和地区。

需求背景

中海油作为亚洲最具规模的油田特大公司，服务业务范围广、业务量巨大，数据就是企业生存和发展的命脉，一旦把



重要资料泄露，就完全失去了对文档的管理控制，接收方获取文件后可以任意的传播，对企业造成的损失后果不堪设想。为了提高中海油内部数据协同和高效运作，实现文档脱离内部管理平台后能有效防止文件的扩散和外泄。对于内部文档使用范围、文档流转等进行控制管理，中海油选择中国数据安全防护专家—亿赛通作为合作伙伴，共创企业数据安全。

解决方案

电子文档安全管理系统是一款电子文档安全防护软件，该系统利用驱动层透明加密技术，通过对电子文档的加密保护，防止内部员工泄密和外部人员非法窃取企业数据资产，对电子文档进行全生命周期防护。

智能加密：可根据文档的内容进行语义识别，判断是否为企业所定义的加密数据并自动进行加密处理；

内容安全管控：可对数据实现截屏录制控制、文档阅读水印、文档打印水印、拷贝粘贴控制；

文档权限管理：可对数据进行细粒度权限控制、模板批量授权、文档权限管理；

文档外发管理：可进行用户身份认证、使用权限控制；

流程管理：实现文件解密审批流程、文件外发审批流程、离线办公审批流程和文件还原审批流程；

审计跟踪：可以进行邮件外发审计、文件解密审计、文件打印审计、流程全文检索审计和违规操作预警。

项目成果

通过对中海油数据的使用、存储、流转、审计等各个环节安全把控，为企业构筑了立体化的安全防护体系。系统并充分融合了环境兼容性和功能扩展性，可无缝地满足日益变化的用户需求和环境变化需求，在实现安全管控的情况下，又实现工作效率与管理效率的提升。

亿赛通牵手中核能源 铸就企业 坚不可摧的智能安全盾牌



客户简介

中核能源科技有限公司成立于 2003 年，是在原国防科工委的支持和推动下，由中国核工业建设集团公司与清华控股有限公司（清华大学）共同出资组建的核能高科技企业。中核能源的使命是围绕实现股东各方的战略目标，集聚整合股东各方在研发设计、工程实践、产业配套等方面的优势资源，发挥产学研结合的体制优势，发挥企业主体和产业化平台的积极作用，推动我国具有自主知识产权的高温气冷堆、低温核供热堆两大先进核能技术实现产业化。



需求背景

中核能源在庞大的业务体系下，为了防患于未然，让企业数据资产的安全能够做到事前预防，事中控制，事后审计与一体化的智能安全管理，对此中核能源通过在众多的数据安全企业厂商中甄选，最终选择与亿赛通合作帮助企业实现数据安全管控。

解决方案

亿赛通文档安全管理系统部署方案实现对任意文档自动透明加密的同时，不影响用户的使用习惯；以及对研发、设计部门采用强制加密；对管理、财务和营销等部门，采用主动加密，实现重要文档高效、安全管理。防止内部员工通过邮件、MSN、QQ、FTP 下载等网络端口发送重要文档；通过文档操作强制日志审计，确保事后可追溯；防止硬盘被盗、笔记本和移动存储设备丢失后导致的信息泄露。

项目成果

亿赛通文档安全管理系统帮助中核能源实现一体化的数据安全管控，为企业铸就了坚不可摧的安全盾牌。