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：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com

亿赛通 ESAFENET

ESAFENET

亿赛通企业月刊　　中国数据安全防护专家　　www.esafenet.com

5 月刊

2018 年共 11 期

关注企业官方微信

Esafenet
Monthly magazines

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：86-10-57933600

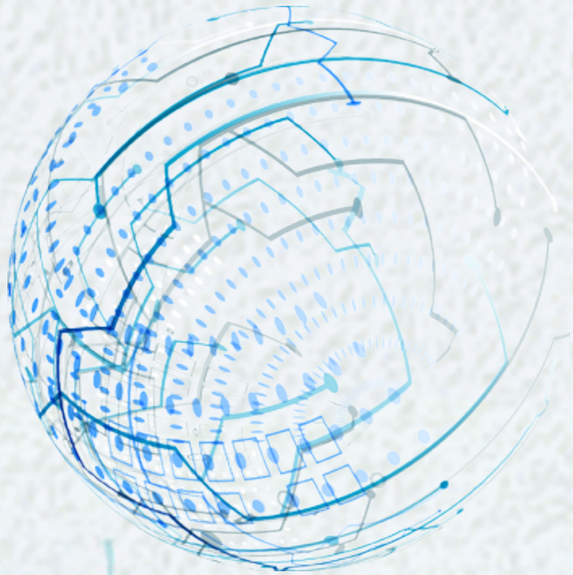
传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com

CONTENTS 目录

面对机遇和挑战
继续开辟新道路



刊首语 PREFACE

5月，正是春末夏初，伴着柔和的阳光，就这样缓缓走过。与温和的天气相比，数据安全市场就显得跌宕起伏。大数据快速渗透到地球的每一个角落，数据安全威胁越发突出，内部隐患和内外联合造成的数据泄密也愈演愈烈，建设数据安全早已刻不容缓……为此，亿赛通五月刊再次新鲜出炉，纵览本月数据安全行业发展最新动态。面对新的信息安全挑战和机遇，数据安全企业如何应对？未来，如何继续开辟新道路？本期月刊犀利为您解读，全新书写数据安全领域新版图……

国内

1、中国银联：超九成电信诈骗源于个人信息泄露

摘要：中国银联日前利用大数据分析向社会发布安全提醒，电信诈骗案、盗窃银行卡、非法套现、冒用他人银行卡、网络消费诈骗形势依然严峻，其中超过 90% 是由于个人信息泄露引致，已成为犯罪主要源头。

2、信息安全行业发展前景分析 2022 年市场规模接近千亿

摘要：信息安全事件带来的越来越高的经济损失加强了企业对于信息安全投入的意愿。根据普华永道对全球 130 个国家 7200 名来自各个行业的管理人员的信息安全状况的调查，有 39% 的受访者认为企业应该加大对信息安全的投入。

行业聚焦 INDUSTRY FOCUS

3、国内首个大数据安全审查标准即将实施

摘要：《GB/T 35274-2017 大数据服务安全能力要求》 标准在 2017 年 12 月 29 日已正式发布，并将在 2018 年 7 月 1 日正式实施。该标准由清华大学、中国电子技术标准化研究院、中国软件评测中心、华为、阿里巴巴、京东、联想等多家单位共同起草。

4、中国工业信息安全产业发展白皮书将发布 产业前景可期

摘要：首届中国工业信息安全大会将召开，会上将发布《中国工业信息安全产业发展白皮书》，该白皮书是国内首份全面系统深入研究分析我国工业信息安全产业发展的报告。

5、顺丰快递员被曝出售用户信息千万余条 你的隐私已被泄露

摘要：日前，湖北荆州中级人民法院宣判一起涉及公民信息泄漏案件。该案以顺丰员工为信息泄露主体，快递代理商、文化公司、无业游民、诈骗犯罪分子等多方参与的黑产链条。在法院判决书中，共公布了 19 人的判决结果。其中顺丰员工 11 人，圆通代理 1 人，顺丰员工家属 1 人，无业人员 5 人，文化公司负责人 1 人。

湖北省荆州市中级人民法院
刑事裁定书

(2018)鄂10刑终84号

原公诉机关湖北省荆州市沙市区人民检察院。

上诉人（原审被告人）杜立明，男，1990年7月25日出生于河北省石家庄市，汉族，初中文化程度，原系河北顺丰速运有限公司快递员，户籍住所地河北省石家庄市藁城区，实际居住地石家庄市藁城区开发区北席小区15栋1单元502室。2016年12月5日被抓获，12月7日被刑事拘留，2017年1月17日因涉嫌犯侵犯公民个人信息罪被依法逮捕。现羁押于荆州市沙市区看守所。

辩护人耿丽娜，河北纳达律师事务所律师。

上诉人（原审被告人）冯丹，男，1989年6月12日出生于山西省路城市，汉族，大学文化程度，原系河北顺丰速运有限公司市场专员，户籍住所地河北省正定县，曾住地河北省石家庄市新华区。2017年4月14日被抓获，4月15日被刑事拘留，5月24日因涉嫌犯侵犯公民个人信息罪被依法逮捕。现羁押于荆州

6、80 后女辅警泄露公民个人信息，三个月获利 18 万

摘要：在大数据时代的背景下，公民个人信息中蕴含无限商机，伴随而生的是各式各样侵犯公民个人信息的违法犯罪行为。网上非法买卖的公民个人信息种类繁多，涵盖金融、通信、交通、医疗、教育、商业等各个方面。

7、工信部部长苗圩：加快突破智能制造核心装备及工业软件系统

摘要：据工信部 5 月 9 日消息，由中国工程院、工业和信息化部、中国科学技术协会共同主办的“2018 智能制造国际会议”在北京召开。工业和信息化部部长苗圩出席并作主旨报告。

行业聚焦 INDUSTRY FOCUS

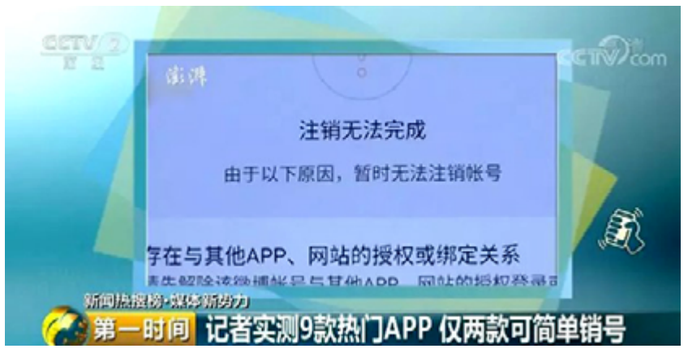
8、物流公司 78 万条个人信息泄露

摘要：通过 qq 群，山东的软件工程师王某和只有小学文化的四川无业游民李某搭上了线，王某负责破解软件，李某利用软件登录快达物流客户端，窃取该公司客户信息，至案发共有 742053 条客户信息失窃。

9、你发前世青年照了吗？当心泄露个人隐私

摘要：五四青年节当天，一款“我的前世青年照”的 H5 产品，迅速引爆深圳人的微信朋友圈，互联网业内人士和法律专家建议，市民需谨慎对待此类需要上传照片等个人信息的软件。

10、央视曝光：APP 注册容易注销难，个人信息或终生被“侵犯”



摘要：“央视财经”微信公号 5 月 7 日消息，随着移动互联网的发展，如今各种手机应用程序层出不穷，如社交类、出行类、购物类等，通常情况下，这些应用程序的账号注册起来非常容易，只要留下我们的一些个人信息即可。但是，账号一旦不用，想要注销起来却不易。

11、中国“网络黑产”规模达到千亿级别 网络安全亟待多维度防御体系

摘要：4 月 20 日召开的全国网络安全和信息化工作会议明确了要树立正确的网络安全意识。习近平总书记强调“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。”

国外

1、索赔 32 亿英镑！ iPhone 用户组织起诉谷歌非法搜集信息

摘要：5 月 21 日，据彭博社报道，在英国，一些 iPhone 用户将谷歌诉至伦敦高等法院，并向其寻求最高至 32 亿英镑（约合 42.9 亿美元）的赔偿。做出起诉的 iPhone 用户组织为“Google You Owe Us”，成员超过 440 万人。

2、中国黑客疑出售超 2 亿条日本网民个人身份信息

摘要：网络安全公司 FireEye 在上周四（5 月 17 日）发布的一份调查报告中指出，该公司旗下的安全团队在地下黑客论坛发现了一组正在被出售的数据集，这些数据集涉及大量的敏感资料，其中就包括了超过 2 亿名日本网民的个人身份信息（Personal Identifiable Information，PII）。

3、前 CIA 情报员被曝将 CIA 代码上传至个人网站

摘要：据外媒 Motherboard 报道，此前前美国中央情报局 (CIA) 情报官员 Joshua Schulte 被怀疑将机密信息泄露给维基解密。近日 Schulte 被怀疑将 CIA 代码上传到一个与他的真实姓名相关的个人网站。

4、欧洲铁路系统遭遇黑客攻击，大量旅客数据泄露

摘要：5 月 18 日，行网站欧洲铁路（Rail Europe）公司已经向客户发布通告表示，有黑客入侵了该公司的机票预定网站，或已窃取了大量敏感数据。

5、美电话追踪公司 Securus 遭黑客攻击：2800 个登录名和密码泄露

摘要：据外媒 cnet 报道，美参议员 Ron Wyden 曾曝光了 Securus 公司为警方提供实时追踪电话的能力。现在，最新消息称，这家公司遭到了黑客攻击。根据 Motherboard 的报道，黑客至少拿到了包含有 2800 个登录名和加密密码的电子表格。

6、Amazon S3 存储桶配置错误暴露数万印度板球球员敏感信息

摘要：在本月早些时候，Kromtech 安全中心的研究人员再次发现了两个因配置错误而在线暴露的 Amazon S3 存储桶。从数据的内容来看，它们似乎归属于印度板球管理委员会（Board of Control for Cricket in India，BCCI）。

7、 2017 年 Equifax 公司数据泄露事件全貌

被盗数据元素	分析标准列	受影响美国用户粗估
姓　　名	名、姓、中间名、后缀、全名	1.466亿
出生日期	出生日期	1.466亿
社保号码	社保号码	1.455亿
住址信息	地址、地址2、城市、州、邮政编码	9900万
性　　别	性别	2730万
电话号码	电话，电话2	2030万
驾照号码	驾照号码	1760万
电子邮件地址（无凭证）	电子邮件地址	180万
支付卡号码与截止日期	支付卡号码与截止日期	20.9万
税　　号	税号	9.75万
驾照状态	驾照状态	2.7万

摘要：5 月 10 日，作为向美国证券交易委员会提交的“8-K”文件的一部分，Equifax 公司公布了其 2017 年内涉及 1.46 亿用户的数据泄露事件全貌。此次受影响的人数众多，几乎有半数美国民众及多家媒体遭到曝光。

8、巴基斯坦数百万公民信息网上公开售卖，售价 1 美元

摘要：根据巴基斯坦“Techjuice”网站在本周一（5 月 7 日）发表的一篇文章来看，数百万巴基斯坦公民的个人敏感信息正在不同的社交媒体平台上被出售，而这些信息在巴基斯坦国内网站上的售价仅为 100 卢比，即 1 美元。

9、澳大利亚最大商业银行遗失 1200 万条用户交易数据

摘要：澳大利亚最大的商业银行澳大利亚联邦银行（CBA）近日发表消息称，他们遗失了包含客户姓名、地址、账号和 2000 年至 2016 年的交易详情记录的两个存储磁带。据悉，这些存储带是在一次数据中心转运中被其分包商 Fuji-Xerox 丢失，其中至少包含 1200 万名用户的银行交易数据。

10、墨西哥多家银行大量资金不翼而飞 官方称或因第三方软件漏洞所致

摘要：据路透社（Reuters）报道，两名接近政府调查的消息人士称，一群劫匪已经从墨西哥银行偷走了数亿比索（墨西哥流通货币，货币编号 MXN），包括排名第二的墨西哥北方银行（Banorte）。

11、美国 Chili’s 连锁餐厅遭遇支付信息破坏

摘要：布林克国际公司于 5 月 11 日发现其旗下 Chili's 连锁餐厅 1600 家门店的顾客支付卡信息受到破坏，这可能导致部分餐厅顾客的支付卡相关信息被非法访问或盗窃。

行业聚焦 INDUSTRY FOCUS

12、美国俄亥俄州河滨城连续两个月 遭遇黑客攻击 涉及警察和消防部门

摘要：河滨城（Riverside）的警察和消防部门再次遭到勒索软件攻击，这意味着该城市仅在几周之后就再次成为了第二起网络攻击的受害者。

13、俄罗斯视频监控公司 iVideon 数据泄露 涉及超过 82 万名用户的个人信息

摘要：Kromtech 安全中心的研究人员在最近发现，一个归属于俄罗斯视频监控公司 iVideon 的 MongoDB 数据库并没有得到保护，并向公众开放。从数据库的内容来看，它似乎涵盖了 iVideon 公司的整个用户群，包括其用户和合作伙伴的登录名、电子邮箱地址、密码哈希值、服务器名称、域名、IP 地址、子帐户以及软件设置和付款设置信息（并不包括任何信用卡数据）。

亿赛通动态 ESAFENET NEWS

亿赛通精彩亮相第二届中国数据安全治理高峰论坛，专业产品引爆全场

为了减轻企业系统攻击、数据驻留和数据隐私等问题，安全和风险管理领导者应该制定适当的数据安全治理框架，避免安全风险可能给企业带来的信誉流失和经济损失。5 月 22 日由中国网络安全与信息化产业联盟、中国网络安全技术创新产业联盟和中国保密协会产业分会主办，安华金和承办、亿赛通协办的第二届中国数据安全治理高峰论坛正式拉开帷幕。本届峰会以“共享数据价值·共担安全责任”为主题，汇聚了中央部委、地方政府、金融、能源、教育、医疗、互联网等领域安全行业 600 余位资深人士 ,从各自专业视角解读与分享对于数据安全治理的思考与实践经验。以期达成在数据资产时代，既保障数据安全，又促进数据分享、使用的美好愿景。

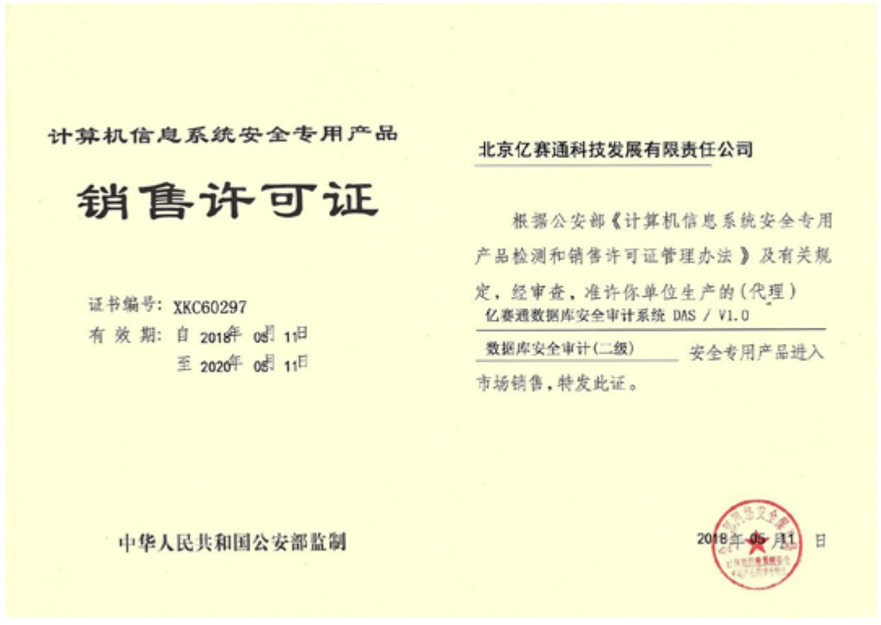
时代革新 技术发展促进企业繁荣

大数据飞速发展的背景下，数据早已成为组织的核心资产，变成新的发展动力和生产资料。数据安全威胁越发突出，内部隐患和内外联合造成的数据泄密也愈演愈烈，建设数据安全早已刻不容缓。在此趋势下，数据安全已经进入新时期，技术发展是产业发展走向繁荣的前提。亿赛通作为数据安全治理委员会的重要成员，始终将技术作为企业的核心竞争力，坚持革新与改进，推动了亿赛通技术在安全领域独占鳌头的地位。

现场咨询人员络绎不绝 ,亿赛通作为行业里的领军企业，以“保护数据所有者的信息资产安全”为使命，一直致力于数据安全行业，以卓越的发展态度，丰富的行业解决方案被广大客户所赞赏；过硬的产品满足更多企业用户的深度需求。未来也会为各行各业提供更加完善、更加周到的数据安全保障服务，不断为广大用户带来更多惊喜！

亿赛通动态 ESAFENET NEWS

热烈庆贺亿赛通数据库审计产品获取双项权威资质



计算机信息系统安全专用产品

销售许可证

证书编号：XKC60297

有效期：自 2018年 05月 11日

至 2020年 05月 11日

北京亿赛通科技发展有限责任公司

根据公安部《计算机信息系统安全专用产品检测和销售许可证管理办法》及有关规定，经审查，准许你单位生产的（代理）

亿赛通数据库安全审计系统 DAS / V1.0

数据库安全审计（二级） 安全专用产品进入市场销售，特发此证。

中华人民共和国公安部监制

2018年 05月 11日

近期，亿赛通数据库安全审计系统 DAS/V1.0 数据库安全审计（二级），该产品同时获得《计算机信息系统安全专用产品销售许可证》和《中华人民共和国国家版权局计算机软件著作权登记证书》双项国家资质。

公安部销售许可证是产品必须通过国家网络与信息系统安全产品质量监督检验中心、公安部计算机信息系统安全产品质量监督检验中、公安部信息安全产品检测中心的专业测试，产品需完全符合信息安全技术中通用渗透测试检测条件均达到标准的质量要求，可充分满足各个行业对数据库安全审计产品的需求方可获得。

中华人民共和国国家版权局

计算机软件著作权登记证书

证书号：软著登字第2567567号

软件名称：亿赛通数据库安全审计（DAS）系统
[简称：DAS]
V1.0

著作权人：北京亿赛通科技发展有限责任公司

开发完成日期：2018年01月29日

首次发表日期：2018年03月20日

权利取得方式：原始取得

权利范围：全部权利

登记号：2018SR333467

根据《计算机软件保护条例》和《计算机软件著作权登记办法》的规定，经中国版权保护中心审核，对以上事项予以登记。

中华人民共和国国家版权局 计算机软件著作权登记专用章 2018年05月14日

No. 02567567

该产品在获得公安部销售许可证书的同时获取了计算机软件著作权登记证书，该证明是国家保护软件著作权人合法权益的依据。授予单位中华人民共和国国家版权局是国务院著作权行政管理部门，主管全国的著作权管理工作。

此次亿赛通数据库审计系统同时获得双项专业资质，是政府对亿赛通的数据库安全产品、研发能力以及公司在数据安全行业成绩的充分肯定；表明亿赛通在数据安全产品研发领域的竞争力和知名度进一步提升。今后，亿赛通将会继续致力于为用户提供优质的数据安全产品、高效的售后服务、完备的行业解决方案，为国内数据安全行业做出更多的贡献。

亿赛通参与太仓企盟信息技术发展中心理事会选举，深层次展示企业核心竞争力

2018年 5月 12号，太仓企盟信息技术发展中心举办了第三届理事会选举，旨在加强公司管理体系。该机构成立于 2009年 6月，是由 10位太仓外企的 IT负责人自发组织成立。连续 5年承接太仓市民政局的公益创投项目，并以再生电脑公益行项目与太仓企业达成定点教室的援建，4次获得太仓市公益创投项目优秀项目的荣誉及优秀执行团队荣誉，2016年获得江苏省青年公益项目大赛一等奖。此次理事会选举，特邀请中国数据安全防护专家亿赛通参加，在会中共同探讨企业信息化数据安全问题。

企业目前普遍存在数据安全问题，担心防护不严密 ，起不到效果。为此，亿赛通精英人士为与会人员介绍了公司专业产品：电子文档安全管理系统及网关。针对太仓外企数据国内加密国外不加密的特点，提出可将少量文件发给国外，直接采取白名单策略，方便实用；批量数据可采用上传到指定服务器落地解密，但针对落地解密中的风险，采取双服务器机制，即国内员工上传到的文件服务器不做解密，但文件同步传到国外服务器时落地解密。该解决方案引起到场人员探讨，各位 IT负责人认真聆听，并不时提出问题。会议结束后，与会人员都认为这样的研讨才真正有意义，对企业数据安全问题有实实在在的帮助。

在数据安全市场，大到国家，小到个人，对安全意识都在不断提高，各行各业也对自身的核心数据提到了前所未有的重视高度，但是数据安全的风险却一直存在，如何避免、如何防控 ?数据安全的工作任务还是任重而道远，中国数据安全防护专家作为领军企业会扛起行业大旗，为各行各业提供更加完善、周到的服务。

热烈庆祝研发·双核时代 亿赛通武汉研发中心落成庆典圆满成功

2018 年，对亿赛通是如此特别！企业的全面发展，离不开公司求真务实的研发队伍。从 2003 年成立至今，亿赛通在技术领域不断突破，先后开创业界多个第一。同时，在不断以产品、方案、服务为导向的发展过程中，凭借卓越的研发技术水平，早已成为数据安全领域不可或缺的标杆企业。

如今，公司着眼未来，在武汉建立研发中心，有利于吸纳国内最优秀的科技类人才，促进相关业务的快速开展，为公司下一代产品的核心竞争力提供技术支持。同时，该研发中心选址武汉东湖高新区（位于中国光谷核心地段），与各大科技公司毗邻，利于公司融入外部创新、开放、包容的文化环境，为企业注入创新活力和发展动力提供便利条件，特于 5 月 31 日举行了“研发 . 双核时代“落成典礼，标志着亿赛通武汉研发中心正式建成并投入使用。

亿赛通公司总经理、副总经理、全体核心研发人员、武汉高新区政府领导以及亿赛通众多合作伙伴，共同见证这一重要时刻。希望亿赛通在今后的技术发展道路上，构建出更高效的研发技术团队、提供出更专业的技术方案、打造出更优质的产品和服务，迎合时代需求，继续引领数据安全市场快速发展。

2018 新起点·再出发

在会议中，亿赛通公司总经理崔培升介绍，面对数据安全市场带来的挑战，亿赛通将加大市场及研发投入、规范运营体系，实现北京、武汉双研发模式。

标杆项目签约仪式

本次活动，亿赛通特举办项目签约仪式，标杆项目代表与亿赛通企业代表签署合作协议，标志着双方合作将会实现双赢的局面。从此以后，亿赛通将与该企业在技术实施、产品服务等多领域，展开深度合作。

知识控查·数据安全体系新思路

我们知道，亿赛通 15 年来始终坚持自主研发，在近两年的产品研发及投入上不断加大筹码，很多安全产品、安全理念、安全服务早已超越同行。亿赛通公司副总经理李贺分别从数据安全体系、产品方向、整体解决方案等视角向在座同仁传递前沿技术，打造越来越多创新的、更具竞争力的行业解决方案，从而为最终用户创造更多价值。

数据安全时代站上风口浪尖

亿赛通高级咨询顾问为到会人员分析了数据安全目前面临的机遇与挑战以及典型客户案例，针对信息泄密的途径及防护措施，详细分析了数据安全产品原理与技术，并从重点典型签约客户出发，分别就客户需求、项目落成、产品部署等方面证明了亿赛通的专业实力，彰显企业核心竞争力，为合作伙伴提供了丰富的实战经验。

走在奋斗的路上 永不止息

披荆斩棘，砥砺前行，为研发奋斗、为创新而生；亿赛通武汉研发中心秉承“专注产品品质、注重客户服务”的研发使命，在数据安全技术创新的道路上不断前行。

个人信息安全规范正式实施，亿赛通为您深层解读那些必须 Get 的条文

近年来，APP 默认勾选协议、大量收集用户隐私权限、不当与第三方共享且导致信息外泄的现象经常发生。互联网时代，作为被迫用部分隐私交换便利的用户，你该如何保护自己的信息安全？当企业收集你信息时，需要如何告知及征得你同意？如果涉及到与第三方共享数据，又该向你做出怎样的确认？

针对 APP 默认勾选、手机用户隐私权限等问题，《规范》明确指出：在间接获取个人信息时，作为接收方的企业有义务要求提供方对相关个人信息的来源进行说明并确认其合法性，同时还应当了解个人信息主体对于提供方的授权范围 ,包括使用目的、个人信息主体是否授权同意转让、共享、公开披露等内容，若接收方处理个人信息超出上述范围的，还应在合理期限内另行征得个人信息主体的明示同意。

不只上述提到的问题，信息泄露时有发生，近期的外卖平台数据泄露事件；前世青年照泄露信息；我们更是经常接到推销电话，对方能准确报出你的姓名、职业和需求；微信群发了“砍价拼水果”的购物链接，帮朋友砍价时下载了 APP、填写了姓名和手机号，结果没几天就收到了带自己姓名的诈骗短信，以及扫描二维码获取话费、转发某个广告领取红包、点赞领取礼物……面对这些信息泄露情况，我们究竟该怎么办呢？

七大原则保障个人信息安全

★权责一致原则—对其个人信息处理活动对个人信息主体合法权益造成的损害承担责任。

★目的明确原则—具有合法、正当、必要、明确的个人信息处理目的。

★选择同意原则—向个人信息主体明示个人信息处理目的、方式、范围、规则等，征求其授权同意。

★最够用原则—除与个人信息主体另有约定外，只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时根据约定删除个人信息。

★公开透明原则—以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督。

★确保安全原则—具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性。

★主体参与原则—向个人信息主体提供能够访问、更正、删除其个人信息，以及撤回同意、注销账户等方法。

亿赛通从事数据安全防护领域十五年，已发展成为国内数据安全、网络安全及安全服务三大业务供应商，以上百项知识产权涵盖了包括：终端、网络、存储、审计等多个方面的几十个数据安全软硬件产品，坚持为广大客户提供核心技术保障。对于《网络安全法》的正式实施，亿赛通强力支持国家政策，并且努力从技术方面持续为大家的数据安全保驾护航，携手国家政策共同致力于建设安全、高效、文明、和谐的网络安全环境。

亿赛通为江苏沙钢集团淮钢特钢股份有限公司部署最佳解决方案，全方位建立数据资产安全管理体系

淮钢特钢

客户简介

江苏沙钢集团淮钢特钢股份有限公司始建于 1970 年，前身为清江钢铁厂，经历了淮阴市冶金工业公司、江苏淮钢集团有限公司等改制过程。多年来，公司坚持协调发展、创新发展、绿色发展，做到以人为本、尊重科学、创新驱动、追求卓越，致力于将淮钢建设成为“内享工作快乐，外受社会尊敬”的具有国际竞争力的新型特钢企业。

需求背景

近些年发生的诸多行业数据泄密事件，着实给企业的信息化造成不少的压力。江苏沙钢集团作为具有国际竞争力的现代化大型国际竞争企业，为避免设计部门、生产部门、财务部门等重要部门的核心资产，因外部或内部人员有意、无意泄密，而给企业造成重大经济损失，经过长时间沟通实施，最终签约亿赛通公司构建数据安全管理体系。

解决方案

亿赛通电子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；以及对技术部门采用强制加密；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。

亿赛通电子文档安全管理系统帮助淮钢特钢股份有限公司实现一体化的数据安全管理，产品经过了多年的实践证明成熟度比同行要高出一截。有效的保护企业核心数据资产，保障企业竞争力，提高企业的数据可用性，降低运营维护成本，加强了员工的安全意识。使企业的整体保密强度和水平显著提高，为企业铸就了坚不可摧的安全盾牌。

亿赛通签约招商银行

客户简介

招商银行北京分行成立于 1994 年。16 年来，坚持贯彻总行的经营管理理念，实现了效益、质量、规模、结构协调发展，呈现出盈利能力强、资产质量优、业务结构好、发展可持续、品牌形象佳的特点。

需求背景

随着信息化建设的发展，大量的信息化文档生成，如银行办公资料、客户资料、业务数据等重要文档资料分散在各 PC 机上，如何保证这些重要数据的安全和实现统一安全管理，是招商银行绝对不容小视的问题。

解决方案

1. 防截屏软件（定制）：

屏蔽用户计算机上使用一切防截屏软件，对涉密信息进行截图处理。

2. 全盘加密安全 U 盘：

①强身份认证：保护合法用户访问 U 盘文件加密区；

②加密密钥：为 U 盘里本身加密的数据穿上第二层防护衣；

③账号保险箱：杜绝银行账号、系统密码等涉密信息的泄密风险等。

3. 可信介质安全管理系统：

①从介质访问控制、终端注册授权、介质注册授权、介质存储数据安全保护、介质使用权限控制、介质离线审批与权限控制、介质使用安全审计以及结合终端端口控制、终端光盘刻录监控与审计等方面对存储介质进行数据泄露防护管理，用技术手段实现存储介质的安全使用及存储的数据安全保护；

②通过对介质的访问控制与注册授权，实现非注册介质接入内网计算机上不能使用，内网专用介质接入非内网计算机上不能使用；

③数据始终以密文形式存储在专用介质上，非授权用户不能解密，保证涉密介质丢失后不会造成泄密事故。详细的介质使用审计日志，确保介质可追踪等。

项目成果

亿赛通数据安全防护系统在招行银行运行稳定，已经实现招行银行北京分行全员部署，通过数据泄露防护体系的建立，为招商银行信息安全树立了安全屏障。