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

7 月刊

2018 年共 11 期



“企业上云”如火如荼，亿赛通出席山东省“企业上云”峰会暨服务商对接会助力云行业发展

中国数据泄露防护品牌谁第一？CCID 权威数据发布

《我不是药神》刷爆朋友圈，电影背后揭露医疗行业惊人内幕！

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



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

4-10 国内行业新闻

11-17 国外行业新闻

亿赛通动态 ESAFENET NEWS

18/19 中国数据泄露防护品牌谁第一？ CCID 权威数据发布

20/21 “企业上云”如火如荼，亿赛通出席山东省“企业上云”峰会暨服务商对接会助力云行业发展

22/23 亿赛通受邀参加 2018 年株洲市网络安全执法检查工作会议，为公安部网络安全献计献策

亿赛通小贴士 ESAFENET PROMPT

24/25 网盘存储又“作妖”？担心隐私泄露只是因为你少了这个动作

26/27 《我不是药神》刷爆朋友圈，电影背后揭露医疗行业惊人内幕！

28/29 担心个人信息泄露？侵犯公民信息将被判刑！

典型案例 TYPICAL CASES

30/31 共享资源，共建生态 中国数据安全防护专家助力能源行业实现数据资产无泄露

32/33 湘潭电机数据安全体系可靠运行，亿赛通幕后全力支持

CCID

亿赛通数据泄露防护市场

占有率排名第一



15 年在数据泄露防护市场排名 NO.1

市场规模达到 7.8 亿元

2017 年，同比增长 25.3%

刊首语 PREFACE

纯干货！七月刊精彩呈现

季节的阳光，迈过春天，迈过仲夏，遍洒在这七月的原野。午后的蝉鸣，葱郁的树木，万物都在这火辣的七月中加快成熟的步伐，2018 年悄然过半。

7 月，于数据安全行业而言，也是历经考验。随着大数据、人工智能等新趋势在数据安全行业的深度发展，数据安全行业上升新的台阶，拥有更大的发展空间。亿赛通，作为中国数据安全防护专家，15 年从未懈怠，坚持服务数据安全行业。2018 年，继续大展宏图，大力开发“安全”市场，制定精准清晰的战略，满足市场需求变化，继续提高品牌竞争力。据 2018 年 CCID 最新权威报告显示，亿赛通在中国数据泄露防护市场份额连续多年同行业其他品牌厂商中占有率稳居第一，成为数据安全行业的主力军。接下来，让我们一起走进亿赛通七月刊，预知 2018 下半年行业发展趋势……

国内

1、离职员工改网店后台偷红包，检方起诉以盗窃罪判刑



摘要：通过事前掌握的账户名和密码，私自登录他人天猫店铺，28岁的离职员工刘某利用设置购买商品赠送红包、话费、流量的方式窃取21万余元。昨天上午，海淀法院当庭宣判刘某犯盗窃罪，判处其有期徒刑3年6个月，罚款3万元。据悉，这是本市首例通过此种方式盗窃的案件。

2、当涂警方破获特大侵犯公民个人信息案



摘要：7月10日，贩卖公民个人信息犯罪嫌疑男子王某、李某被当涂县检察院批准逮捕。至此，一条侵犯公民个人信息的犯罪产业链被成功摧毁。记者从当涂县公安局网监大队获悉 ,经过缜密侦查、细致工作，辗转重庆、广东佛山、广州等三省五市历时30天，行程万里，先后抓获犯罪嫌疑人3人，查实被盗卖的公民个人信息240万余条，及时破获了这起严重危害公民个人权益的犯罪案件。

3、辽源警方破获部督特大“网络侵犯公民个人信息案”

摘要：7月12日，辽源市公安局召开新闻发布会，宣告由公安部督办的特大“网络侵犯公民个人信息案”成功告破，先后抓获16名犯罪嫌疑人、捣毁7处犯罪窝点、扣押涉案资金200余万元。该案历时10个月，横跨5省8市。该案的成功侦破得到了公安部、省委、省政府、省公安厅、市委、市政府、市公安局领导的高度赞誉，受害人和广大人民群众拍手称赞。



4、慈溪多起侵犯公民个人信息案宣判 购买公民个人信息也是犯罪



摘要：“您家最近需要装修吗？我们的材料质量上乘、价格实惠。”每当家里在装修或者正打算装修时，总会“恰好”接到类似的推销电话，让人不胜其扰。日前，慈溪法院审结几起侵犯公民个人信息罪案件，再次对侵犯公民个人信息行为敲响警钟。

5、女子购物信息遭泄露 被假客服报准确信息骗走 12 万



摘要：近日，郝女士在某电商平台购物后，收到了假冒“客服人员”打来的电话，从而掉入电信诈骗陷阱，被骗 12 万余元。 7 月 10 日，涉事电商平台方面回复称，经查这些消费者账号都存在异常登录情况，怀疑遭到不法分子“撞库”。

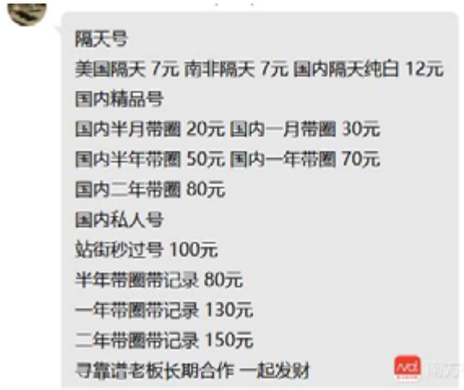
6、4000GB、数百亿条个人信息泄露！大数据行业知名企业数据堂被查

数据堂 Datatang

摘要:7 月 8 日 ,据新华网“新华视点”报道 ,山东日前成功破获一起特大侵犯公民个人信息案 ,共抓获犯罪嫌疑人 57 名，打掉涉案公司 11 家 ,查获公民信息数据 4000 GB、数百亿条。其中 ,国内知名大数据公司、新三板上市公司 “数据堂” 涉案。

行业聚焦 INDUSTRY FOCUS

7、微信号买卖黑产链调查：60 元一个实名号



摘要 : 广东省公安厅通报表示 , 今年 “飓风 5 号” 电信网络诈骗专案在惠州成功打掉 1 个利用微信交友实施诈骗的犯罪团伙，刑拘 239 名嫌疑人，止付冻结资金 3200 万元。

8、4 年半 2379 件侵犯个人信息案宣判 泄露无处不在



摘要：我国近年来侵犯公民个人信息犯罪态势高发。广西律师林仁聪通过法律智能操作系统搜索中国裁判文书网发现 ,2014 年以来 , 全国法院公开的一审宣判侵犯公民个人信息犯罪案件为 2379 件。

9、机场追星成产业链：明星航班信息最便宜只需 15 元



摘要：近两年，多位明星公开批评、斥责行程航班信息被泄露，抱怨不堪粉丝接送机骚扰。昨日，北京青年报记者调查发现，在新浪微博搜索“×× 明星航班”“刷关”等关键词，很多售卖各种明星航班信息的账号会跳出来，如“×××，× 月 × 日，× 地”，并要求买家加微信，最低到达 15 元一条。

10、钦州小伙大学刚毕业，名下却有 130 多家公司！知道真相后他慌了



摘要：小莫是钦州灵山人，今年 7 月份，刚毕业的他入职南宁一家信贷公司。偶然间，他在公司系统中发现，自己竟是 130 多家公司的法人代表！这些公司工商登记所在地均在外省，而成为公司法人代表，要有小莫的身份证才行，但近年他没有遗失身份证，“只是去年 10 月做兼职时，给兼职群里的人发过身份证正反面照片而已。”小莫猜想，应该是那时出问题的。

11、吴宣仪个人信息泄露 公司发声明将追究法律责任



摘要：今日（7 月 2 日）有网友在网上擅自违法晒出吴宣仪私人证件信息，稍后，乐华娱乐发出严正声明，针对个人信息泄露作出回应并表示将采取法律手段。

12、三人倒卖 15 万条公民个人信息获刑 形成信息泄露黑色链条



摘要：近日，山东济南市历下区法院判决一起倒卖公民个人信息案，保险公司业务员、家庭装修推销员非法获取 15.2 万余条公民个人信息并出售，楼盘销售员、无抵押信用贷款电话营销员非法获取信息以推销业务，形成信息泄露的幕后黑色链条。而这些信息的售价，每条不足 1 毛钱。

13、物业贩卖 3 万多名业主信息 泉州警方侦破重大贩卖公民个人信息案



摘要：物业贩卖个人信息，涉及 3 万多名业主的详细个人信息被买卖泄露，在警方的严厉打击下，这起重大贩卖公民个人信息案被成功侦破。

14、大众点评涉泄露用户行踪，你的隐私数据是怎样被滥用的？

大众点评 dianping.com

摘要：7 月 11 日消息，日前有媒体报道，用户用微信登录大众点评后，会将用户关系链与微信等通讯录中的好友捆绑，并将用户在酒店、餐厅等的签到信息、点赞信息或地址信息分享给这些平台的好友。

国外

1、西班牙电信一安全漏洞置数百万用户数据于泄露边缘



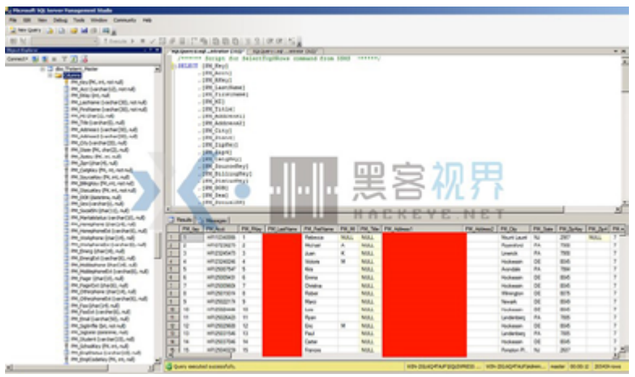
摘要：据 El Espanol 报道，西班牙电信 (Telefónica) 在 7 月 16 日凌晨被西班牙消费者协会 FACUA 发现存在一个安全漏洞。透过这个漏洞能够访问数百万用户的完整个人数据，这意味着这些数据可能早已经被置于泄露的边缘。

2、因员工发错邮件，普渡大学 2.6 万名学生详细信息暴露



摘要：近期，主校区位于美国印第安纳州西拉法叶市的普渡大学 (Purdue University) 发生了一起数据泄露事件，恰恰就只是因为一名工作人员一不小心犯下的一个低级错误导致的。据报道，在这起数据泄露事件中，所涉及的数据超过 2.6 万条。

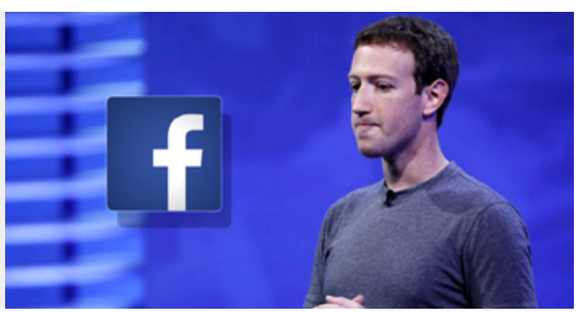
3、医疗软件公司 MedEvolve 因服务器漏洞致 20 多万患者信息泄露



摘要：在过去的几个月里，我们看到了数据泄露事件发生频率的激增，同时也看到了针对对医疗行业的网络攻击显著增加。在上周，另一起医疗数据泄露事件导致了患者的个人信息遭到曝光，并且所涉及的患者数量超过了 20 万。

4、Facebook 首次因数据泄密丑闻遭罚款：金额 66.4 万美元

摘要：据报道，Facebook 将因为剑桥分析 (Cambridge Analytica) 数据泄露事件而面临第一次处罚——来自英国的 66.4 万美元罚单。



5、因涉嫌盗窃公司机密，一名苹果前员工被逮捕



摘要：7 月 11 日上午消息 根据美国加州北区法院的文件显示，美国联邦调查局 (FBI) 本周以窃取商业机密罪逮捕并起诉了苹果前雇员张晓朗 (音译，XiaoLang Zhang)。

6、 托马斯库克航空公司置乘客个人信息于泄露边缘

摘要：托马斯库克航空公司 (Thomas Cook Airlines Scandinavia) 是英国的一家包机航空公司，成千上万的度假者依靠该公司提供的服务来完成他们旅程，由于该公司系统在安全方面的不足，正将他们的个人信息置于泄露的边缘。



7、 Timehop 公开数据泄露详细情况，2100 万用户遭受攻击



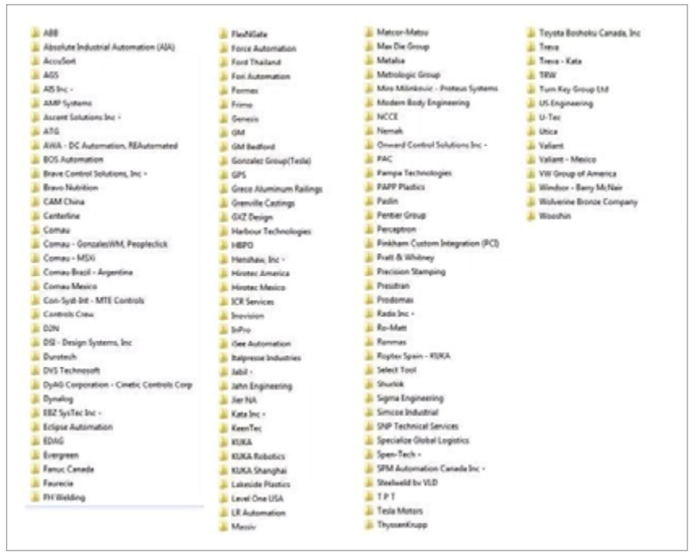
摘要：Timehop 公布了一次涉及 2100 万用户的数据泄露（包括名字和邮件）。大约有五分之一的用户—— 470 万——泄露的账户中附带了手机号码。

8、 国际明星球员洛夫伦被盗号：个人信息全泄漏



摘要：目前在 2018 俄罗斯世界杯上为克罗地亚国家队效力的德扬·洛夫伦 (Dejan Lovren) 已经成功俘获了很多来自全球各地球迷的心。然而，最近有消息称，一名球迷侵入了洛夫伦的社交媒体账户并获取到了其私人信息。

9、重大数据泄漏事件：汽车制造产业上下游 100 多家公司数据暴露在互联网上



摘要：UpGuard Cyber Risk 的安全队伍现在透露，100 多家汽车产业链上下游公司的敏感文件已泄露，这些文件放在属于 Level One Robotics 的一台服务器上。

10、加拿大亚岗昆学院服务器感染恶意软件 超过 11 万条记录遭泄露



摘要：近期，发生一起影响到超过 11 万人的大规模数据事件，而事件中的主角是在加拿大 150 多所学院中排名前五的亚岗昆学院（Algonquin College）。

11、美最大独立医学实验室遭黑客入侵 致数百万客户面临个人信息泄露

摘要：据英国《每日邮报（DailyMail）》报道，LabCorp 在上周末遭遇了一起网络攻击事件，可能存在数据泄露的问题。虽然目前调查仍在进行当中，但有关当局表示 LabCorp 的网络系统的确在上周末遭到了匿名黑客的入侵，而入侵目的很可能是为了获取医疗数据。



12、VPNFilter 恶意软件并未引起重视 许多受影响设备被发现仍存在漏洞



摘要：思科（Cisco）和赛门铁克（Symantec）等全球知名企业相继发出安全预警称，一种新型的多阶段恶意软件“VPNFilter”已经成功感染了分布于全球 54 个国家的 50 多万台路由器。

13、思科发现了一场针对印度的黑客活动 目标指向 iPhone 用户



摘要：思科 Talos 团队的安全专家近日发现了一场“高度针对性”的黑客攻击活动，攻击者使用了一种至少自 2015 年 8 月以来就一直保持活跃的移动恶意软件。安全专家认为，攻击者就位于印度该国，并且只有 13 部 iPhone 受到感染。

14、暗网惊现美军 MQ-9“收割者”无人机资料，最低售价仅 150 美元



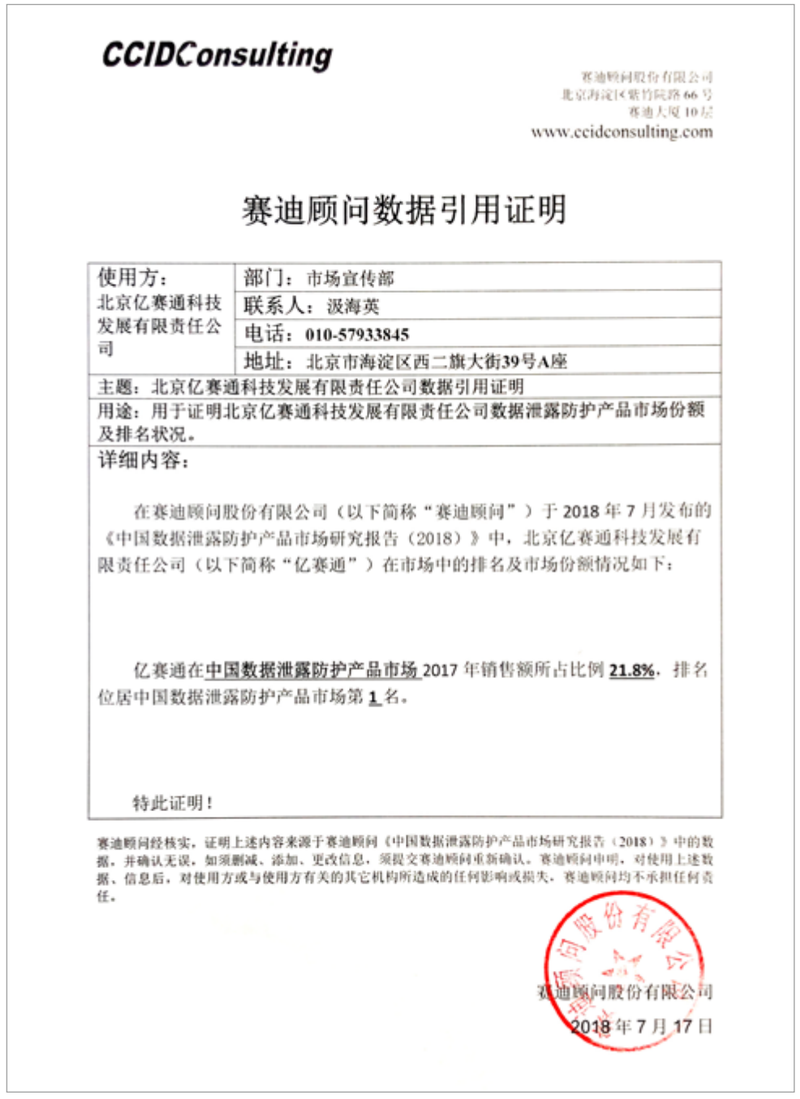
摘要：据多家国外媒体报道，威胁情报公司 Recorded Future 于近日发现，一群黑客正在暗网交易市场销售敏感的军事文件，其中包括了 MQ-9“收割者”无人机的维修手册和飞行员名单。

15、纽约市 9 家 B&BHG 餐厅遭恶意软件感染 致顾客支付卡数据泄露



摘要：据多家国外媒体报道，B&BHG 酒店集团（B & B Hospitality Group）目前已经被证实成为了另一家数据泄露事件受害者企业。

中国数据泄露防护品牌谁第一？CCID 权威数据发布



CCIDConsulting

赛迪顾问股份有限公司
北京海淀区紫竹院路66号
赛迪大厦10层
www.ccidconsulting.com

赛迪顾问数据引用证明

使用方：北京亿赛通科技发展有限责任公司	部门：市场宣传部
	联系人：汲海英
	电话：010-57933845
	地址：北京市海淀区西二旗大街39号A座
主题：北京亿赛通科技发展有限责任公司数据引用证明	
用途：用于证明北京亿赛通科技发展有限责任公司数据泄露防护产品市场份额及排名状况。	
详细内容：	

在赛迪顾问股份有限公司（以下简称“赛迪顾问”）于2018年7月发布的《中国数据泄露防护产品市场研究报告（2018）》中，北京亿赛通科技发展有限责任公司（以下简称“亿赛通”）在市场中的排名及市场份额情况如下：

亿赛通在中国数据泄露防护产品市场2017年销售额所占比例21.8%，排名位居中国数据泄露防护产品市场第1名。

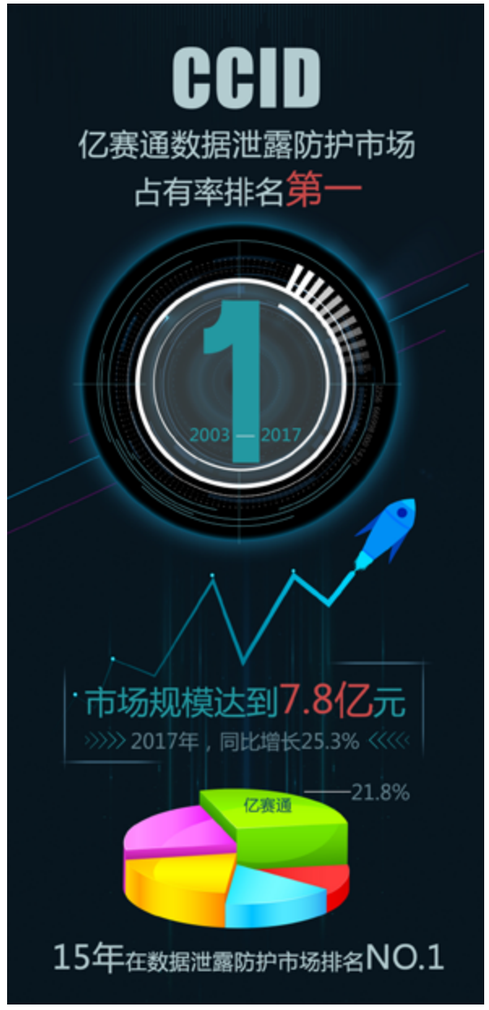
特此证明！

赛迪顾问经核实，证明上述内容来源于赛迪顾问《中国数据泄露防护产品市场研究报告（2018）》中的数据，并确认无误。如须删减、添加、更改信息，须提交赛迪顾问重新确认。赛迪顾问申明，对使用上述数据、信息后，对使用方或与使用方有关的其它机构所造成的任何影响或损失，赛迪顾问均不承担任何责任。

赛迪顾问股份有限公司
2018年7月17日

2018 年 7 月，赛迪顾问股份有限公司发布了《中国数据泄露防护产品市场研究报告》，报告显示亿赛通继续领跑中国数据泄露防护产品市场，这已经是企业连续多年在中国数据泄露防护市场份额中排名第一。

随着近年来国内网络安全事件地频繁发生，我国政府对于信息安全防护建设意识逐渐加强，政策支持力度不断上升。



近三年来，国家在关键信息基础设施安全保护制度方面及个人信息和重要数据保护制度方面出台了众多法律法规。企业在数据泄露防护体系建设上的投资不断增加，加强数据安全和隐私保护并提升基础设施保护、防御能力成为数据泄露防护产品市场发展的主要推动力。

2017 年，随着企业用户对数据防护方面的需求日益加深，中国数据泄露防护市场高速增长。2017 年，数据泄露防护市场规模达到 7.8 亿元，同比增长 25.3%；预计 2018 年我国数据泄露防护市场规模将达到 9.6 亿元，同比增长 23.1%；到 2020 年，市场规模将达到 14.7 亿。

亿赛通再度成为 DLP 行业主力军

作为中国数据泄露市场领军企业，亿赛通的产品及服务在市场排名中遥遥领先。产品能够连续十五年得到市场青睐，充分显示了亿赛通在数据泄露防护领域的产品、服务及解决方案等方面强大的综合实力。2018 年公司更是在武汉成立研发中心，有利于吸纳国内最优秀的科技类人才，促进产品研发更新的快速开展，为公司下一代产品的核心竞争力提供技术支持。

现今数据安全市场日渐成熟，用户对于产品性能和稳定性要求越来越高。亿赛通作为数据安全领域领先企业的市场价值也会越来越明显，政策法规也给国内厂商带来了很多机会。特别是在信息安全方面，国内的政府部门和关键行业呈现出“外退内进”的局面，国内软件企业对国外企业的替代效应日益明显。因此，国内企业具有很大的空白市场，发展空间大。与国外厂商相比，国内的数据泄露防护软件企业在客户选型时会有一定优势，他们更为了解中国企业所面临的问题，有针对性地进行开发与设计，能够为国内企业提供性价比更高的安全服务。未来数据安全专项厂商市场机遇更加突出。

公司无论在市场份额、品牌知名度上都一直名列前茅，通过准确把握当前数据安全发展态势，推动数据安全先进技术手段建设，促进专业产品实施应用，越来越受到更多客户的认可。作为专注于 15 年数据安全领域的厂商——亿赛通当仁不让，一直遥遥领先同行厂家，有望在快速增长的安全市场获得更大份额，未来的市场空间将会更巨大。

亿赛通经过多年耕耘，为政府、军队、金融、运营商、能源、教育、企业等行业提供了完善的数据泄露防护解决方案，帮助客户建立了完善的安全保障体系。到目前为止，公司用户遍及全国，客户超过 15000 家，服务终端用户过 200 万。企业将始终执著于数据泄露产品以及对技术的创新和研究，致力于提供具有国际竞争力的自主创新的防护产品和最佳实践服务，秉承“专注产品品质、注重客户服务”的研发使命，在数据泄露防护技术创新的道路上不断前行。

“企业上云”如火如荼，亿赛通出席山东省“企业上云”峰会暨服务商对接会助力云行业发展



“互联网 +”时代 ,以云计算、物联网、大数据、智能制造为代表的新兴技术和模式中蕴含着大量既有安全方案容易忽视、不能发现、不能应对的新型信息安全问题。

为更好地应对网络和信息安全新挑战，聚合互联网产业领域与网络安全行业的力量。由山东省经济和信息化委员会、山东省财政厅指导，山东省企业上云服务联盟主办的山东省“企业上云”峰会暨服务商对接会于 7 月 3 日在济南隆重举行。会议邀请山东省 200 多家云服务商、200 多家中小企业以及来自全国的近百家安全厂商参与。亿赛通作为安全厂商中的行业领军企业，受邀在会议中进行主题演讲并与“山东安全云”平台现场签约入驻。



“山东安全云”平台签约仪式

按照山东省企业上云工作的总体部署，促进综合云平台服务商、行业云平台服务商、云应用服务商的有效对接。会上同时进行了“安全云”平台发布会，全方位助力山东省企业上云。 平台聚合国内优秀的安全厂商，在相关政策指导下，协助所入驻的安全厂商打通线上线下资源。亿赛通参与现场签约仪式，与平台达成良好协议，形成共享、共生、共赢的合作生态。



企业上云，数据安全如何落地

亿赛通高级咨询顾问于会中做了“企业上云，数据安全如何落地”的主题演讲，在云平台、大数据的快速发展应用中，企业信息安全工作也迎来了新的挑战。会议上，亿赛通结合企业工作的业务场景，从现实出发从我们身边的故事出发，对办公环境进行剖析，指出每种办公环境下存在的数据安全隐患，并给出相应的解决方案。通过数据防护，分别从文件的存储、传输、使用等方面，采用核心加密技术，巩固“企业上云”安全建设，确保在各种复杂业务场景下企业核心数据资产不被泄露和非法窃取。完美的方案展示，精彩的发言，获得了与会领导和在座专家的充分肯定。



彰显领先技术，塑造品牌形象

解决数据安全隐患需充分考虑数据面临的各种主动泄密和被动泄密风险。同时，还充分考虑系统对企业的业务影响范围，即保证敏感数据在加密状态下不改变和影响用户使用系统和工作效率，让安全性和可用性之间保持一定的平衡。亿赛通针对各种敏感文件进行数据安全保护，有效识别敏感数据，监控敏感数据使用情况，防护敏感数据外泄。有效培养并提高员工对敏感文件的保密意识。确保在各种复杂业务场景下企业核心数据资产不被泄露和非法窃取。

“服务客户、持续创新、勇担责任、专业至上”是亿赛通永成不变的核心价值观。领先的技术和丰富的解决方案，为每一位客户提供最及时、最全面、最到位的服务，先后为众多国内外知名企业提供数据安全解决方案。截至目前，亿赛通公司已在全国三十余个主要城市设立了分支机构，为立足中国、迈向全球市场打下了坚实的根基！

亿赛通受邀参加 2018 年株洲市网络安全执法检查工作会议，为公安部网络安全献计献策



为贯彻《2018 年湖南省网络安全执法检查工作方案》要求，做好株洲市网络安全保卫工作，株洲市公安局于 7 月 3 日召开 2018 年株洲市网络安全执法检查工作会议，全面部署开展网络安全执法检查工作，加快推进网络安全监测预警通报处置体系建设。会议邀请株洲市重要领导、各重点网站及互联网企业负责人参会。亿赛通在业内凭借优秀的数据安全解决方案得到众多合作企业的称赞与肯定，株洲市公安局特邀亿赛通出席大会并展示专业解决方案。





亿赛通相关专家在会上就当前新形势下的的数据安全体系做了全面分析，尤其是现今数据安全已经上升到国家高度的情况下，从国家政策，到等级保护 2.0 中新的规定，再到 2018 年发生的最新数据安全重点事件的安全问题及应对策略做了深入浅出的分析和阐述，简单明了的解释了如何保证数据文件在“内忧”与“外患”中实现精准有效防护。会中 ,亿赛通专门为与会人员演示了“定位敏感信息 - 发现敏感信息 - 控制敏感信息 - 监督敏感信息”的完整闭环解决方案，“知识控查”的最新设计理念获得了与会的各部门领导的一致认可。

亿赛通作为国内知名的数据安全防护专家，全力支持保护各企事业单位信息安全，以及加强网络安全管理。对此，针对国家对网络安全政策的出台与实施，与当下网络安全面临的“内忧外患”，亿赛通加大技术投入力度，研发出一整套数据安全解决方案，从终端防护、网络防护、邮件防护、数据扫描、数据分析、审计报告等多个环节发现、识别、分类企业敏感数据，监控企业敏感数据使用情况，保护企业敏感数据以防丢失和被窃，让窃密者无空可钻。同时，降低企业运营成本，加强内网、外网一体化的安全意识，提升企业品牌形象，打造最完美的数据安全防护解决方案，以及专业的安全咨询服务。

目前，亿赛通为八大行业，万余家企业服务，200 余万终端用户铸就了坚不可摧的安全盾牌，有效提高了客户数据安全管理水平，优化重组了工作流程、服务效率和信息共享的能力，协助保障了社会安全有序的运行，从而促进国民经济和社会可持续发展。

另外，在数据安全防护领域，亿赛通面向全国各个行业客户建立新型安全防护模型，使企业客户的信息系统能够对安全策略进行持续优化。亿赛通愿与株洲公安局一起，为株洲建立和谐、安全的互联网环境助一臂之力。

网盘存储又“作妖”？担心隐私泄露 只是因为你少了这个动作



“听说了么，又有网盘出事儿了！”

“对啊，国外某知名网盘被媒体曝出上万条账号信息被公开。”

“啊啊？那这些信息里都有什么呀？”

“是用户名、密码和文件名的数据。”

“密码都被公开了，那信息是不是就被泄露了呀？”

“可不是么，被泄露信息的账号全部都显示登录异常，里面的文件都被泄露了。”

“Oh,myGod! 那可怎么办呢？难道就没办法能避免网盘泄露吗？”

“当然有了，亿赛通有一个数据安全卫士就能解决这个问题”

“这么厉害啊，具体给说说呗！”



数据安全卫士

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。

更多优势

1、免费注册，简单易用：该产品采用了高安全动态虚拟卷加密技术和细粒度权限访问控制，因此访问者只有经过合法身份认证后才可打开受控文件，可有效控制数据被非法扩散或二次使用；

2、多文件类型支持：支持近百种文件类型，如文档类、音频 / 视频类、设计类、图片类、代码类……全都鼎力支持。

小伙伴们，当重要的个人资料上传网盘或者发给客户时，尽管你告诉对方一定要保密，但总有图谋不轨之人想把资料据为己有，甚至到处扩散，从而带来巨大损失。别担心，亿赛通数据安全卫士可以控制多种权限，包括浏览次数、使用时间、打印水印、修改、还原、防止内容拖拽、拷屏和设置自动销毁等等，无论在网盘存储，或者传输、外发都可保证您的数据绝对安全。没毛病，你有你的网盘存储，我有我的数据安全卫士，不是很屌，但够安全，安排！！！

各位小伙伴们 ,现在关注“亿赛通”微信公众号 ,回复“激活码”，小编就会为大家推出“数据安全卫士”激活码，领取后的小伙伴，就可以为您的敏感资料安全保驾护航啦！

《我不是药神》刷爆朋友圈，电影背后揭露医疗行业惊人内幕！



“你怎么笑了？”

“因为它真。”

“你怎么又哭了？”

“因为它血淋淋的真。”

近期一部感人的电影刷爆朋友圈

《我不是药神》

影片是根据真实事件改编

围绕着慢性白血病救命药「印度格列宁」

上演了各种真实却又荒诞的感人故事

瞬间看疼了无数人的心

“我吃了三年的药，吃掉了房子，吃垮了家人。可我还是想活。谁家还没个病人了？”

这句虐心的台词催人泪下

其实

每一个生命都值得被尊重

但是

不法分子

却利用他们的病进行诈骗

再一次打击他们已经脆弱不堪的心

……



医疗行业的电信诈骗、信息泄露、医疗骗保等情况屡见不鲜

体检诈骗

湖南株洲的王某到马来西亚旅游，被当地被检查出癌症，花62.5万元打抗癌针。最近单位组织体检王某各项指标正常，无癌症病征...近日，警方侦破了该起海外医疗诈骗案。

手术诈骗

6月，某村通过大队广播告知村中老年人，唐山某医院可免费体检，50名老人被接走。检查后，称得了肌瘤，需要做激光手术，费用3000元。

医保诈骗

刘某因患急性心肌梗死住院，在此期间认识医生杨某并在其帮助下接受手术。手术结束后，因刘某本人没有参加新型农村合作医疗，很多费用需要自理。医生杨某授意刘某使用刘某姐姐的身份证到某医院农村合作医疗办公室登记。事情办妥之后，医生杨某收取刘某给予的9000元现金。刘某到某医院农合办使用刘某姐姐的手续报取95059.45元治疗费用，杨某、刘某已经构成诈骗。

信息非法销售

更早之前，上海20万条新生婴儿信息被上海疾控中心、黄浦区疾控中心两名工作人员窃取，并贩卖给婴幼儿保健品经营企业。

电话诈骗

部分艾滋病感染者接到诈骗电话，诈骗者事先已掌握他们的个人信息，包括姓名、身份证号、联系方式、户籍、确诊时间、随访医院或区县疾控等，由于信息真实，导致其中多人被骗。



互联网时代，数据呈现方式的多样化，以及获取渠道的多元化都导致我们的隐私随时被暴露在“光天化日”下，而随着由信息的非法获取、网上兜售、甚至违规利用所组成的利益链条悄然形成。在上述涉及公民隐私数据泄露的问题上，相比遭遇黑客攻击而造成的损失，内部泄露造成的数据被盗占有更大的比重。



亿赛通凭借多年终端管控及文档加密的经验，加入智能识别分类和内容感知技术，创造了新一代数据安全智能防护体系。该体系将终端数据防护、网络数据防护、应用数据防护、存储数据防护及介质数据防护有机结合在一起，融合了亿赛通 21 个产品应用组件，每一个组件都可以作为一个独立的方案帮助客户解决数据安全问题，同时这些组件也可以任意组合形成更智能化的联动方案，满足用户复杂的数据安全需求，还可以为用户的信息安全规划分阶段制定个性化的数据安全解决方案，帮助客户建立智能化的数据安全防护体系。作为 IT 服务厂商，中国数据安全防护专家——亿赛通有义务也有责任帮助各大医院做好数据安全防护工作。

担心个人信息泄露？
侵犯公民信息将被判刑！



日常生活中，这样的场景你一定经历过：刚买完车，各种保险公司不停地打电话；刚买完房，就会接到多家装修公司、贷款机构的电话；给孩子报课外班，接到很多培训电话，甚至知道孩子的名字，比这些更令人深恶痛绝的还有电信诈骗、黑客勒索等更为严重的犯罪。

最近四年，全国法院公开宣判的公民个人信息犯罪案件超过 2000 件以上。专业人士认为，最重要的就是要加快推进个人信息保护相关法律法规的出台，从源头上保护个人信息。2018 年开始，不论国内国外，多个信息保护条例相继出台，信息安全已经成为国家最为重视的事情之一。

案件数量增长迅速

2018 年上半年，警方法院抓获判决多起大型信息泄露事件。

事件一、顺丰员工非法出售快递单获刑

湖北荆州中级人民法院公布了一起涉及公民信息泄露的案件，此案涉及顺丰快递代理商和多名顺丰员工。此案涉嫌被泄露的公民个人信息达千万余条，涉及金额高达 200 余万元。被告人冯某、杜某等 19 人为谋取非法利益，利用微信、QQ 等软件平台，出售、提供、非法获取包含顺丰快递单号、面单（即包含顺丰快递单号、地址、电话号码的图片）等公民个人信息。19 名嫌疑人被判 1-3 年不等的有期徒刑。

事件二、装修公司联合物业窃取业主信息

湛江麻章区法院近日审理了一起某小区 4700 余位业主信息泄露的案件。被告人肖某是湛江某装饰公司法定代表人。为承揽生意，肖某联系到了某小区的物业经理何某，要求何某向其提供业主信息，并承诺若接单成功，会给何某“提成”。何某发给肖某 4700 多条业主信息。案发后，何某到公安机关投案自首，肖某被抓获归案，两人均构成侵犯公民个人信息罪，被判处有期徒刑六个月，并处罚金人民币五千元。

事件三、民警知法犯法查询公民信息

日前，民警詹某擅自利用公安信息系统帮人查住址，导致女子赵某被前男友况某找上门并杀死在暂住地内。法院经审理认为，詹某违反国家有关规定，向他人提供公民信息，情节特别严重，其行为已构成侵犯公民个人信息罪，判处有期徒刑 1 年 3 个月，缓刑 1 年 6 个月。

事件四、员工利用职务之便出售企业信息

近日，南京中院对一起侵犯公民个人信息案作出宣判，刘某利用职务便利，非法获取企业信息并出售给被告人严某、郭某。三名被告人分别被判处一年三个月至四年不等的有期徒刑，并处 4 万至 9 万元不等的罚金。

事件五、律师泄露案件内幕消息

蚌埠市中级人民法院依法对原安徽皖瑞税务师事务所有限责任公司负责人陈某一案作出公开宣判，以陈某犯内幕交易、泄露内幕信息罪，判处其有期徒刑七年，并处罚金 1.5 亿元，违法所得金额予以没收。



上述事件仅仅是很少的一部分，据统计，近三年信息泄露安全案件审理数量成倍增加，特别是 2017 年，对信息泄露案件的惩戒力度到达最高。近两年新增加的信息安全法律中明确规定：非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息 50 条以上的；非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息 500 条以上的；非法获取、出售或者提供前两项规定以外的公民个人信息 5000 条以上的，违法所得 5000 元以上的，属于情节严重。

目前金融、电信、教育等行业会接触到大量的公民个人信息，除此以外，快递、房地产及酒店等服务行业也会存储大量个人信息。那么这些行业内的某些企业、个别员工为了获取非法利益，将在工作中获得的公民个人信息资料出售或提供给他人，对公民的人身、财产安全及正常工作生活造成了严重威胁。亿赛通——中国数据安全防护专家，肩负国家数据安全、企业数据安全、个人数据安全的保护使命，为您提供全面而周到的安全服务。

共享资源，共建生态 中国数据安全防护专家助力能源行业实现数据资产无泄露



能源行业分析

能源是国家的基础和支柱行业，是我们日常各项工作和生活的基础与保障。随着现代化建设的迅速发展，各行各业需求日益强劲，尤其是对能源行业的依赖也越来越强，它的发展和建设关系到国计民生，是整个国家安全保障体系的重要一环。随着能源工业的发展和业务规模不断扩大，各大企业实现业务过程中，总部与各个分支机构需要实时信息传输和资源的共享。在数据传输上既要保证内部业务网络较高的可用性、可靠性、保密性，又要对内部核心数据有较强的防御和管控能力。

典型案例 TYPICAL CASES

客户需求

随着业务的发展，大量的核心技术、专利、重要客户信息以及财务数据等方面电子文档的生成。为提高企业内部数据协同和高效运作，实现内部办公文档流转的安全可控，实现文档脱离内部管理平台后能防止外泄，可对内部文档的使用范围、文档权限等进行控制管理，以防止内部核心信息非法授权阅览、拷贝、篡改，既防止了文档外泄和扩散，又支持内部文件共享的目的，需从以下几个方面给予解决：

1、怎样确保跨区域网络环境数据统一安全管理问题；

2、如何保障化工配方和技术文档交互的安全；

3、如何保障终端数据的离线安全；

4、如何解决与外协人员、合作伙伴等的数据交互安全；

5、如何保障移动设备（笔记本）、存储介质（U 盘、移动硬盘）的数据安全；

6、如何保障各应用、办公系统等数据的存储和使用安全。

解决方案

企业内部数据安全体系建设，需要突出重点，切实关注文件外带保密需求，充分考虑敏感性数据面临的各种主动泄密和被动泄密风险。同时，应充分考虑系统对设计人员的业务影响范围，尽可能降低安全行为带来的系统性能损耗和应用约束，在安全性和可用性之间保持合理的平衡。

方案价值

本方案实现了数据本地保护，涉密路径控制，事后行为审计的一种总体的解决方式，最大限度的保证数据安全。实现从数据的生命周期（创建、处理、交换、保存、流转）安全管控，降低数据泄密风险，提高企业员工的保密意识。数据的有效防护，配合系统的数据安全管理制度，进一步增强了企业的核心竞争力。

部分经典客户

中国石油天然气股份有限公司

中国石油化工股份有限公司

中海油田服务股份有限公司

特变电工股份有限公司

国家核电技术公司

中核能源科技有限公司

英利能源

艾默生网络能源有限公司

北京 TSC 海洋石油装备有限公司

中材科技风电叶片集团

中煤北京煤矿机械有限责任公司

洲际油气股份有限公司

中国电力投资集团有限公司

中国电能成套设备有限公司

中联煤层气国家工程研究中心有限责任公司

新奥集团股份有限公司

……

湘潭电机数据安全体系可靠运行，亿赛通幕后全力支持

湘电股份

客户简介

湘潭电机股份有限公司是以全球供应链高端市场为经营目标，目前营销网络覆盖全国各地，出口美欧等世界 24 个国家和地区，为名列前三甲的跨国公司提供产品服务。各类型电机产品稳步进入跨国公司全球采购系统，成为跨国公司在国内采购的首选品牌。

典型案例 TYPICAL CASES

需求背景

现代企业的竞争是以核心技术为基础的整体实力的竞争。企业成功上市后，湘潭电机就围绕如何提升企业核心技术竞争力，打造 " 湘电 " 品牌进行了一系列的改进工作。公司的电机电器成套技术、电力推进技术和电动车辆制造技术三大核心技术，保持了主导产品在国内市场的领先地位。为保障企业的核心竞争力，公司开始陆续加强了内网信息化的安全建设 ,经过多次调研沟通 ,以及两轮测试环节，最终湘潭电机采购了我司的文档防泄漏产品。

解决方案

文档安全管理系统部署方案：

部门控制：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；

员工控制：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 ,防止复制、拖拽、拷屏、打印、另存为、剪贴板盗取和内存窃取等手段盗取文档内容；

审计控制：文档操作强制日志审计 ,确保事后可追溯；

存储控制：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；

外发控制：邮件发送可信对象时自动解密，提高工作效率；

终端控制：员工出差或离开时，配置脱机策略设定时间并可补时，确保离线终端安全可控等。

项目成果

湘潭电机于 18 年 3 月份开始进行整体项目实施，项目访范围覆盖湘电 11 个分支机构的技术中心，主要对企业核心技术资料进行安全防护。项目开展的有声有色，灵活的系统不改变用户网络结构和客户的使用习惯，保障了每一个输入、输出的数据安全运行。部署加密产品后的国企焕发出了新的朝气与活力！

设计制造行业部分经典案例

江苏沙钢集团淮钢特钢股份有限公司

招商局重工（江苏）有限公司

海马汽车有限公司

南通中集罐式储运设备制造有限公司

京东方科技集团股份有限公司

湘潭电机股份有限公司

佛山电器照明股份有限公司

广州市百库电子科技有限公司

珠海光宇电池有限公司

江苏共创人造草坪有限公司

湘潭电机股份有限公司

东风汽车电子有限公司

杭州东芝水电有限公司

珠海格力电器股份有限公司

中国航空工业集团公司沈阳飞机设计研究所