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

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

12 月刊

2017 年共 11 期

亿赛通重磅签约华润置地，
强强联合共创数据安全

亿赛通出击开黑争霸赛，
IT 精英勠力同心王者相见

数据泄露市场潜力巨大，亿赛通深耕
核心数据防护市场

亿赛通喜迎年末收获季企业信誉获政府
认可推举 2017 北京诚信创建企业

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

CONTENTS 目录

刊首语 PREFACE

2/3 刊首语

行业聚焦 INDUSTRY FOCUS

4-7 国内行业新闻

8-15 国外行业新闻

亿赛通动态 ESAFENET NEWS

16/17 亿赛通出击开黑争霸赛，IT 精英勠力同心王者相见

18/19 媒体专访 | 数据泄露市场潜力巨大，亿赛通深耕核心数据防护市场

20/21 荣誉 | 亿赛通喜迎年末收获季企业信誉获政府认可推举 2017 北京诚信创建企业

22/23 荣誉 | 2017 中国软件大会亿赛通数据安全智能管理平台 (DSIP) 喜获“最佳解决方案奖”

24/25 亿赛通荣登“2017 中关村高成长企业 TOP100”榜单

亿赛通小贴士 ESAFENET PROMPT

26/27 保护个人隐私，政府应作出示范

28/29 看《猎场》最重要的不是看职场精英、不是看跌宕爱情、不是看商海沉浮，而是看 " 他 "……

典型案例 TYPICAL CASES

30/31 亿赛通重磅签约华润置地，强强联合共创数据安全

32/33 年末继续发力，再树新功，亿赛通力保京东方数据安全

挥手 2017
迎战 2018

生活就像一场旅行，你经历的，就是最好的风景。如果想站在原地，没有成长就无收获。2017 年转眼过去、挥手告别，2018 年让一切从头再来，我们都已做好准备。

刊首语 PREFACE

“大数据”时代，许多企业和个人掌握了过去只有政府机构才拥有的公民数据，并通过数据挖掘从中获得了大量有价值商业信息。与此同时，用户数据和个人隐私也面临被泄露与侵犯的危险。随着近年来用户隐私泄露事件频发，公民的个人隐私数据保护遇到了严峻挑战。2018 即将是安全企业责任重大的一年。

据统计，2017 年各大科技公司，都在网络领域更通过产品和服务创新、公司并购或者直接将安全列为头等大事。网络安全一直以来都有点像是家庭手工业，由小产品公司、地区 / 全国性服务提供商和少数独角兽公司组成。据估测，从 2017 年到 2021 年的 5 年间，全球网络安全开支将达 1 万亿美元。2015 年，网络犯罪给全世界带来了 3 万亿美元的经济损失；据估计，到 2021 年，该年度损失将达 6 万亿美元。网络犯罪的蔓延，驱动了网络犯罪解决方案市场的发展。再加上合规法令的增多和愈趋严格，未来 10 年，网络安全市场市值将升至令人目眩的高度，面对 2018，亿赛通做好了充分准备，迎战未来。

国内

1、人民法院报刊文谈个人信息的法律保护与合理使用

摘要：个人信息合理的使用，需要做到信息主体自愿提供，自主取消，报酬请求，信息收集者明确收集目的，来源正当，安全保密，不得损害他人合法权益及社会公共利益。

2、教育部印发紧急通知：全面清理和规范学生资助公示信息

摘要：12 月 1 日，澎湃新闻从教育部了解到，为进一步规范学生资助公示工作，切实保护好受助学生的个人信息和隐私，教育部日前印发紧急通知，要求全面清理和规范学生资助公示信息。

3、四川教育厅紧急通知：受助学生信息公示涉及隐私部分全部删除

摘要：近日，有媒体报道个别省份和学校在公示受助学生信息时，含身份证号码、银行卡号等个人信息，严重侵害了学生权益。

4、合肥多所中小学学生信息被倒卖：哪个班、父母是谁明明白白

摘要：合肥一群发短信的公司，从他人处购买了 2 万条学生信息。此后，该公司将这些信息贩卖给培训机构，培训机构又相互交换。近日，检方以涉嫌侵犯公民个人信息罪，对三人提起公诉。

5、安徽几十所学校 7 万条学生信息泄露，涉事公司负责人被控制

摘要：11 月 26 号晚上，一名网友发了条微博，实名举报安徽出众教育皖北地区负责人王磊，非法获取学生家长信息达 7 万条，进行电话销售。

6、人民日报：政府网站泄露隐私引发关注，多地整改升级保护机制

摘要：如何平衡好政务公开与个人隐私保护？政府网站信息发布管理工作该补哪些短板？要更好地完成互联网时代的政务公开工作，这些问题亟待解决。

7、跨 25 省份侵犯公民个人信息系列案：60 元获得一个人的银行信息

摘要：自今年 9 月最高人民法院指定辽宁管辖的跨 25 省份侵犯公民个人信息系列案开槌以来，一些身份为协勤员、银行职员等“内鬼”依靠职务便利并利用监管漏洞，盗卖公民个人信息大肆敛财的事实浮出水面。

8、谁在倒卖用户个人信息？新华社：内鬼是泄露主要渠道

摘要：“新华视点”记者在多地反诈骗中心了解到，目前电信网络诈骗案件 90% 以上是违法分子靠掌握公民详细信息进行的精准诈骗，从已破获案件看，“内鬼”监守自盗和黑客攻击仍是公民个人信息泄露的主要渠道。

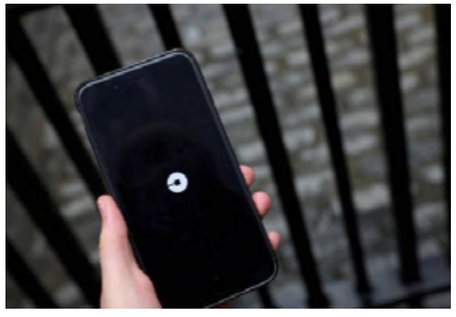
国外

1、谷歌被诉出售逾 500 万 iPhone 用户信息，或赔偿 27 亿英磅

摘要：谷歌被指在 2011 年 6 月至 2012 年 2 月期间收集 iPhone 用户信息。起诉书称，谷歌的做法触犯了《数据保护法案》。预计该案将于 2018 年在高等法院审理。一起集体诉讼指控谷歌利用算法绕过 iPhone 默认隐私设置，收集用户的浏览历史数据。这一诉讼的目的，是使约 540 万名受影响的用户获得赔偿。

2、Uber 数据泄漏事件涉及 270 万英国用户，或将面临巨额罚款

摘要：据外媒体报道，继优步（Uber）披露 2016 年曾掩盖影响 5700 万用户的大规模数据泄露事件后，全球多个国家政府对该公司展开了调查。11 月 30 日，Uber 对英国数据保护监督机构称，在此用户数据泄漏事件中，大约有 270 万用户受到影响，其中泄露信息包括用户名、手机号、和电子邮件地址等。



3、美政府再因亚马逊 AWS S3 配置错误：超 100GB NSA 陆军机密文件曝光

摘要：继数周前美国陆军中央司令部（CENTCOM）与太平洋司令部（PACOM）的敏感数据暴露于不安全亚马逊 AWS S3 服务器后，网络安全公司 UpGuard 研究人员 Chris Vickery 近期再次发现托管在 AWS S3 服务器的 47 份美国陆军情报与安全司令部（INSCOM）机密文件（逾 100GB ）在线曝光，其中竟有 3 份重要文件可任意下载。

4、牛津剑桥俱乐部备份硬盘被盗，涉英国皇室等 5000 名会员数据泄露

摘要：位于伦敦市中心最独特的俱乐部之一的牛津剑桥俱乐部总部发生计算机设备失窃案，包含 5000 多名会员个人详细信息的备用硬盘被盗或导致重大数据泄露，其中包括会员姓名，家庭和电子邮件地址，电话号码，出生日期，照片和一些银行账户详细信息。此外数据库中还包括有大约 100 名工作人员个人信息。

5、重磅！美国国土安全部 24.6 万员工信息泄露

摘要：今年 5 月，美国国土安全部（DHS）一名员工的家用电脑服务器被发现存有 24.6 万名 DHS 员工的个人敏感信息，涉及截至 2014 年底进入 DHS 的雇员。

6、全球航运公司 Clarksons 拒付黑客赎金，内部机密数据或被泄露

摘要： 30 日消息，全球航运公司 Clarksons 发表声明称，公司此前发生“安全事件”被盗的内部机密数据可能会因拒付赎金而被黑客公开，并且对受影响的客户和个人深表歉意。

7、人工智能玩具或侵犯儿童隐私 安全性遭多国质疑

摘要：据外媒报道，法国信息与自由全国委员会警告，近年流行与孩子互动的人工智能玩具安全性不足，可能不利儿童的隐私。

8、前美国国家安全局员工承认非法带走机密文件

摘要：一名前美国国家安全局（NSA）员工 12 月 1 日承认，他非法从该机构非法带走了机密文件，这些文件后来被认为由俄罗斯情报机构的黑客通过互联网从该员工家中电脑当中盗走。

9、PayPal 旗下的 TIO Networks 运营系统存在安全漏洞，逾 160 万客户敏感信息在线泄露

摘要：据外媒报道，全球贸易支付公司 PayPal 于 12 月 1 日证实，公司旗下的 TIO Networks 运营系统存在安全漏洞，黑客已经访问了存储在其服务器中逾 160 万客户的敏感数据，包括用户可识别信息（PII）和部分财务细节。

10、汇丰等知名银行 APP 存在关键漏洞，或致数百万用户易遭黑客中间人（MitM）攻击

摘要：英国伯明翰大学的安全研究人员 Chris McMahon Stone、Tom Chothia 和 Flavio Garcia 近期在佛罗里达州奥兰多举行的 2017 计算机安全应用会议 上发表了一篇学术论文，宣称他们通过测试数百款 iOS 与 Android 设备的不同银行应用程序中发现多家知名银行的主要移动应用程序均存在一处关键漏洞，可导致数百万用户的银行凭证易遭黑客中间人（MitM）攻击，其中受影响的银行包括爱尔兰联合银行、Co-op、汇丰银行、NatWest 和桑坦德银行等。

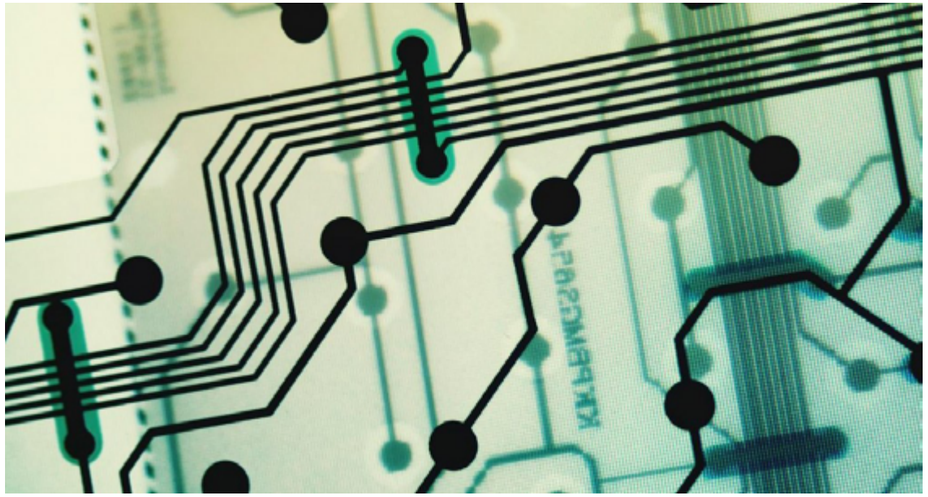
11、特朗普签署新法令，美国政府正式禁用卡巴斯基软件

摘要：据外媒报道，美国总统特朗普于当地时间周二签署了一项法令，接下来各政府部门将不能继续使用卡巴斯基实验室的杀毒软件。这一禁令进一步强化了特朗普政府在今年 9 月发布的一项法令，即民间机构需要在 90 天内删除卡巴斯基软件。

12、暗网暴露 14 亿明文密码库，或成史上最大规模数据泄露案

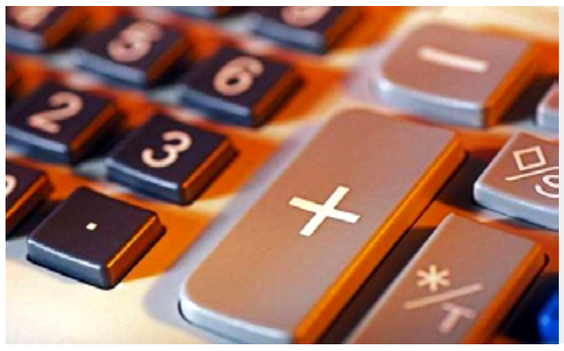
摘要：据外媒报道，美国一家网络情报公司 4iQ 于 12 月 5 日在暗网社区论坛上发现了一个大型汇总数据库，其中包含了 14 亿明文用户名和密码组合，牵涉 LinkedIn，MySpace，Netflix 等多家国际互联网巨头。研究人员表示，这或许是迄今为止在暗网中发现的最大明文数据库集合。

13、普华永道全球信息安全状况调查：中国企业对网络安全投入超全球均值



摘要：普华永道发布了最新的全球信息安全状况调查，调查结果显示，中国内地与香港的企业在网络安全方面的平均投入比全球数值高出 23.5%，受访企业的平均预算达 630 万美元。

14、网络安全产业发展进入新阶段：产业规模不断扩大 核心技术仍需突破



摘要：工业和信息化部副部长陈肇雄表示，我国网络安全产业综合实力已显著增强，但与我国网络设施、融合应用、个人信息等安全保障需求的迅速扩大相比，我国网络安全技术产业的支撑能力仍显不足，网络安全核心技术亟需加快突破。

15、贷款买车也有风险！113 万车主敏感信息泄露

摘要：攻击者可能窃取了包括姓名、地址、车辆信息、车辆识别号码（VIN）、信用分数、贷款金额以及每月付款信息在内的数据。加拿大日产表示，这起事件似乎未涉及支付卡信息。

16、2018 年网络安全趋势展望：垂直行业成主要目标

摘要：2018 网络安全趋势展望第四次工业革命（工业 4.0）带来了前所未有的商机，但同时亦增加了网络攻击的必然性——企业自然需要为此做好准备。这不仅要求企业自起步阶段就将安全措施融入技术中，还需要将安全意识切实引入企业文化当中，同时辅以重要的资金投入。Gartner 公司最新预测数据显示，2018 年全球信息安全产品与服务支出总额将增长到 930 亿美元。

亿赛通动态 ESAFENET NEWS

亿赛通出击开黑争霸赛
IT 精英勠力同心王者相见

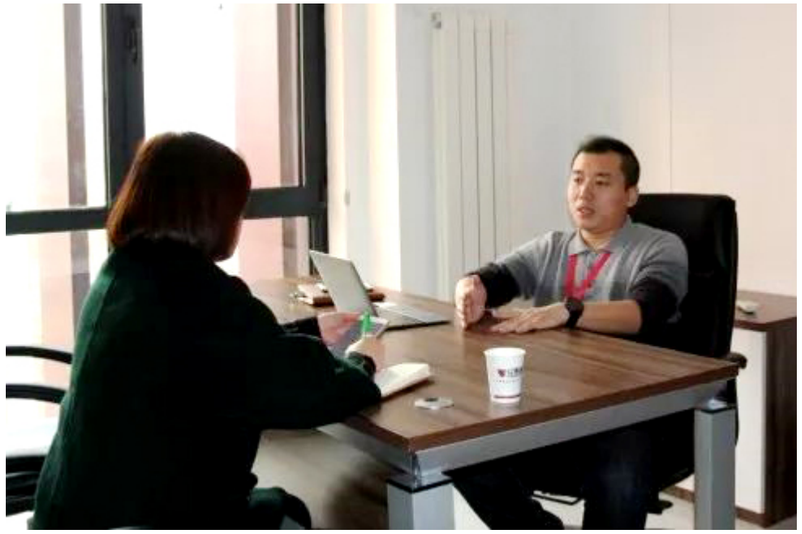
王者荣耀 开黑争霸赛

由苏锡常 IT 经理人俱乐部、亿赛通、小鱼易连、江苏锐视通、太湖慧云联合主办的“王者荣耀开黑争霸赛” 于 2017 年 12 月 17 日盛大开赛。王者荣耀是时下风靡网络的一款多人团队对战手游，吸引很多 IT 界精英人士的目光并大力推崇。俱乐部组建的“王者 IT 荣耀”战队队员数已达一百多人，经过近一年的并肩开黑战斗，在战友的给力表现下，有幸在上赛季从一个菜鸟一步步晋级并荣登王者。新的赛季，更多圈内兄弟姐妹们加入了战队，可以说在这个小圈子里大伙游戏会友，娱乐开黑。亿赛通作为中国数据安全防护专家鼎力赞助，并荣邀参赛，充分发挥团队力量、一鼓作气，赢得团体二等奖。

适逢年末，俱乐部特别策划了本次战队友谊争霸赛，希望借此让战队队友之间线下相聚，相互切磋，同时也希望通过本次争霸赛吸纳更多的圈内会员加入战队后续一起开黑，敞开心扉，交友交流，比赛秉承“娱乐为主，友情第一”的精神。争霸赛现场紧张激烈，局势瞬息万变，兄弟姐妹们如火如荼的为比赛做准备，比赛考验的不仅是选手的技术，更是团队之间的默契协作。小队成员之间互相探讨战术，与对手切磋技术，在这个过程中每个人都收获了快乐，更增进了情谊。

亿赛通——数据安全行业的佼佼者与主办方一起积极参与了此次争霸赛，与众多的业内同行并肩战斗。在激烈比赛的过程中，与队员们交流心得，放松了身心，收获了喜悦。在喜悦的同时，内心也让大家感到一种团队协作的重要性。亿赛通之所以能够历经大风大浪独占鳌头，与公司不可抗拒的凝聚力息息相关，这就是亿赛通人，团结一致朝着一个目标做好数据安全行业，做好中国数据安全防护专家。

媒体专访｜数据泄露市场潜力巨大 亿赛通深耕核心数据防护市场



北京亿赛通科技发展有限责任公司
副总经理 李贺

大数据时代，似乎数据的价值愈凸显，数据泄露事件愈是频频发生。不过，对安全厂商而言，数据泄露可能意味着安全防护方面的机会增加了。据赛迪报告指出，2016 年，我国数据泄露防护市场总规模达到 6.2 亿元，同比增长 21.2% ,预计 2017 年市场规模将达到 7.6 亿元，同比增长 22.3%，市场发展潜力巨大。其中，亿赛通增长势头最为迅猛。

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。记者了解到，2015、2016 年亿赛通通过强化产品技术，持续研发新产品，比如率先发布国内第一套国产 DLP 和基于内容判断进行加密的智能产品，以及通过优化产品服务，为客户提供专业的数据安全体系建设等咨询类服务，不断强化项目管理和交付能力。为此，每年面对市场和客户均开出了优异的“成绩单”。

2017 年的亿赛通在产品技术上面临着更大的革新问题，如何完成业务和指标，进一步巩固在数据泄露防护市场上的领导地位？调整之后的战略是什么？对数据安全市场，亿赛通又是如何理解的呢？近日，北京亿赛通科技发展有限责任公司副总经理李贺接受了《中国电子报》记者的专访，并对上述问题进行了解答。

收购是有益补充而不是加强

“任何企业在发展的过程中都会有这样或那样的问题，企业直面问题，分析并解决问题才能让企业发展的更好更完善。”李贺告诉《中国电子报》记者，面对质疑，亿赛通选择了外部沉默，在目标、营销、产品、服务等方面进行优化调整，最终用业绩说话，兑现了承诺。

“绿盟收购亿赛通，是希望未来向客户提供网络到终端的全方位安全解决方案。” 李贺特意向记者强调。以技术立身的亿赛通，当前正在积极布局大数据数据安全、云数据安全以及同态加密的研究。面对未来，李贺强调，技术优势上还是亿赛通十几年的数据安全技术积累，亿赛通也将一直保持研究院和技术创新的投入，而且绿盟研究院也将是其技术源泉。强强联合，将会开辟出更广阔的市场空间。

2017 年亿赛通已打开全国渠道市场，进行招商加盟。“我们一直秉承‘ 阳光开放 ,合作共赢 ,一同耕耘 ,一同收获’的渠道理念 ,以与合作伙伴实现双赢为宗旨 ,积极贯彻合作、开放、共赢的渠道策略。”李贺认为，保持渠道政策稳定持续，并不断优化对合作伙伴发展、培育、激励、支持政策，才能持续促进建立和谐共赢的渠道环境。他还向记者重点提到了 12371 政策：1 是全国建立统一的渠道销售管理体系 ,2 是两个重要的保障体系即“渠道价格体系”和“渠道认证体系” ，3 是追求三个成就目标“成就客户” “成就伙伴” “成就公司” ，7 是全国分为 7 个销售片区，最后一个 1 是通过努力，合力打造国内第一的数据安全平台。

谈及未来三年亿赛通市场战略以及目标，李贺表示，亿赛通将持续深耕核心数据防护市场，目标是市场覆盖率保持每年 30% 的增长；优化产品线结构，为行业客户量体裁衣提供细分化数据安全产品，预计三年增加 5-6 条新的产品线；深度和绿盟网络安全方案相结合；to C 产品市场的延伸；数据安全咨询服务，协助用户数据治理、数据安全体系建设。

数据安全市场将是一片蓝海

此前，记者在采访时，工业控制系统安全国家地方联合工程实验室主任陶耀东曾向记者表示，通过他们近两年的统计发现，只有不到 5% 的企业会自发地定期巡检，发现企业信息安全问题，95% 以上的企业是被动告知，甚至有的是在遭受到相关网络安全的问题以后才重视的。可见，企业主动发现数据安全相关问题的意识还较为薄弱。

李贺表示确实有这样的情况存在，特别是很多初创企业往往是在其核心知识产权等重要数据被剽窃之后才想起数据安全防护的问题，这也阻碍了创业者的创新步伐。

但这样的情况也在慢慢好转。随着 2017 年 6 月起生效的《中华人民共和国网络安全法》，企业的安全防护意识也在逐渐增强。“与网络安全相比，企业数据安全目前还只是个小市场，可能都不及网络安全市场的 10%”但李贺依然看好中国的数据安全市场。他认为，数据安全市场是一片蓝海，随着国家对国产化安全要求的提升，军民融合市场的开放，未来数据安全市场份额会上升到网络安全市场的 30%，但是现在市场还有些混乱，市面产品模仿严重，市场格局也没有很好地划分，都是小厂商在做局部市场。但经过大浪淘沙之后，国内将会出现也必须出现一家世界级的数据安全企业 ,我们亿赛通也希望通过自己的努力得到青睐。”李贺最后说道。

荣誉 | 亿赛通喜迎年末收获季
企业信誉获政府认可
推举 2017 北京诚信创建企业

为加快推进我市企业信用体系建设，提高企业诚信意识，规范市场秩序，由市经济信息化委、首都文明办等部门于 2017 年 12 月 22 日在北京渔阳饭店成功举办了 2017 年北京市企业诚信创建活动总结大会。在这场汇聚了各行各业领先企业的盛典中，活动评审团从企业品牌、部门信用信息、司法诉讼信息、金融信贷信息和消费者投诉等信用信息多重角度对企业情况进行实际调查，从而对企业 2017 年企业信誉进行评判。

亿赛通从 2003 年创立至今，十四年品质打造，在行业内已经形成很高的品牌知名度和消费认可度，无论是公司产品技术方面，还是企业形象信誉等方面，2017 年中均取得了优异成绩。最终经信用信息采集、第三方机构征信、行业协会初审、专家组综合评审、社会公示等系列创建程序，亿赛通于本次活动中经过严苛评审、综合考虑，最终脱颖而出，荣获“2017 北京市诚信创建企业”，该结果已报市经济信息化委备案，并纳入全市公共信用信息系统中，足以证明企业在政府及群众中树立起的良好形象，具有举足轻重的地位。

如今，社会关注企业专业技术的同时，更在乎的是企业是否存在信誉、服务漏洞等问题。企业即使拥有一流的产品但公司信誉过低，导致客户的基本权益得不到保障，也不是一家成功的企业。作为数据安全行业的领航者，亿赛通始终保持初心不变，服务客户、持续创新、勇担责任、专业至上，打造专业技术与信誉品质齐飞的一流厂商。面对客户，我们以专业的态度、完善的服务尽力满足客户提出的每一点要求，为其提供全面的解决方案，以保证公司与客户之间的良好关系。

2017 年亿赛通迎接挑战、抓住机遇、充分利用发展新趋势，响应国家新政策，大力开拓业务、签约众多行业大项目、出席重大行业会议、收获多项专业技术资质、成为各界权威媒体的焦点……2017 年是机遇与挑战并存的一年，2018 年亿赛通也会乘势而上，聚力凝心，继续做好中国数据安全防护专家。

荣誉 | 2017 中国软件大会
亿赛通数据安全智能管理平台 (DSIP)
喜获“最佳解决方案奖”

今日热点

2017 年 12 月 21 日，由国家工信部指导，中国电子信息产业发展研究院主办的“2017 中国软件大会暨第十六届中国软件和信息服务”颁奖典礼于新世纪日航盛大召开。大会以“新软件激发产业转型新动能”为主题，是 IT 界最具权威和影响力的评奖活动，吸引了上千位 IT 界著名企业的精英人士前来参会。亿赛通在数据安全领域以卓越的技术、过硬的产品、到位的服务、持续的创新以及丰富的解决方案，连续多年获得国家工信部和赛迪研究院的高度关注并受邀参会。

作为专业的数据安全服务厂商，亿赛通在 2017 年里发展的脚步终未停息，研发新产品、引进新技术是企业快速发展的必备筹码。今年重磅打造的“数据安全智能管理平台（DSIP）”采用智能分类、智能分级、智能发现、智能防护、态势感知等领先技术，为我国各个领域的政企单位提供全方位综合性的数据安全解决方案，得到了 IT 业界政府领导们的极大肯定，特于本次会议上颁发了“最佳解决方案奖”。

初心不变，我们用智能诠释安全

如今，新软件已经成为驱动传统产业转型升级最重要的新动能之一，而且在未来发挥越来越重要的作用。新软件与传统产业的融合 ,不仅会加速传统产业的转型进程，同时也会给 IT 企业、软件企业带来新的发展机会。

亿赛通初心不变，用智能诠释安全，在云计算、大数据、智能制造等新软件的驱动下，DSIP 数据安全智能管理平台可与各类应用系统软件进行有效融合，降低核心数据泄密风险，提高企业数据的可用性和安全性，综合一体化数据安全解决方案孕育而生。因此，这也是亿赛通继 2016 年荣获“杰出企业”和“最佳产品”两项大奖后，2017 年又一举拿下“最佳解决方案”奖，不仅是广大网友对亿赛通的支持，更是行业专家对亿赛通的认可。

“服务客户、持续创新、勇担责任、专业至上”满足各行各业的安全需求，为每一位用户提供最及时、最全面、最到位的服务，是亿赛通的初心；提供领先的技术、专业完善的数据安全方案、稳居市场占有率第一，是亿赛通的动力。不忘初心、励志前行！ 2018 亿赛通将会更加脚踏实地，做好产品、做好服务、持续创新，继续做好中国数据安全防护专家。

亿赛通荣登“2017 中关村高成长企业 TOP100”榜单

资讯：

12 月 26 日，由北京中关村高新技术企业协会与中关村创业投资和股权投资基金协会联合主办的“2017 中关村高成长企业 TOP100”评选活动颁奖典礼在北京友谊宾馆隆重举行。中关村百家高成长企业是一批发展速度快、后劲突出，科技创新与开发能力较强的企业，是中关村成长起来的企业新秀，是所在行业的先锋军。政府领导、行业精英、参选企业、协会代表等 400 余人参加了此次活动，共同见证了这激动人心的荣耀时刻。

TOP100 年度评选活动从 2009 年创办以来，已连续举办了七届。在各级政府及主管单位的关心和指导下，活动得到了社会各界的一致认可与好评，是中关村地区最具权威性和公信力的大型公益性评选活动之一。评选秉承公平、公正、公开、公益的“四公”原则，重点考核企业产业发展方向、持续发展与核心竞争能力、信誉责任与企业收入等方面 ,旨在发掘一批中关村示范区内拥有核心技术、创新能力强、发展速度快、具有良好前景的优秀企业。

此次亿赛通能够榜上有名，标志着政府主管部门对公司的高度肯定，今后亿赛通仍将继续努力加大研发力度和持续创新能力，提高企业核心竞争力，引领产业技术进步和升级。

2017 年亿赛通凭借持续的创新精神，求真务实的研发团队、卓越的技术和丰富的解决方案，突破挑战，抓住机遇，取得骄人佳绩，稳固数据安全行业的鳌头地位。2018 年亿赛通仍然脚踏实地、继续前行，引领数据安全行业快速发展，致力于做好中国数据安全防护专家！

保护个人隐私，政府应作出示范

多地高校国家奖学金名单公示泄露隐私：含身份证号

国家奖学金获奖名单网上公示，也成了个人信息泄露的重灾区。据报道，不少高校近几年在公示国家奖学金候选人或获得者名单时，均披露了学生完整的身份证号码。

安徽多个乡镇社区服务中心信息泄露 目前正进行整改

安徽铜陵市政府信息公开网、合肥市政府信息公开网等官方网站存在泄露个人信息的情况，包括姓名、联系电话、身份证号码等涉及隐私的个人信息均可从上述网站公开获取。

重庆九龙坡区教委官网不慎泄露上千教师个人信息

重庆市九龙坡区教育委员会官方网站同样存在多份文件泄露教师、学生个人信息的情况，当地相关部门迅速进行了整改。

政府网站公开信息中意外涉及个人身份信息

景德镇市人社局官网上，出现一则名为“大学生一次性创业补贴人员花名册”的文件，普通用户无需登录，即可下载。而在表格中，14 名创业大学生的学号、身份证号、手机号码等信息均有载录，但大学生对个人信息被一并发布一事不知情。

近日，多地政府官网频现个人信息等隐私泄露的情况，诸如个人电话号码、住址、身份证号等信息，被主动“公示”于政务网站上，并可任意下载获取，引发人们关注。正如一名网友所说：“信息公开竟成了隐私公开，实在是不应该。”

随着社会生活的日益多元复杂，行政权力更多地向私人领域渗透扩张，公民可通过提供和让渡更多的个人信息给政府，以获取更全面完备的政务服务。政府为了保障公民的知情权和监督权，需要进一步推进政府信息公开。政府信息公开的本质，是将部分个人私权利让渡于公权力的一种“平衡兼顾”。但这样的让渡也预设了一个前提：既要通过信息公开保障公民权利，也要防范信息公开导致隐私泄露而产生一系列问题。

事实上，我国相关法律法规中，早已明确了政府信息公开中“保护个人隐私”的原则。《中华人民共和国政府信息公开条例》第十四条规定：行政机关不得公开涉及国家秘密、商业秘密、个人隐私的政府信息。但是，经权利人同意公开或者行政机关认为不公开可能对公共利益造成重大影响的涉及商业秘密、个人隐私的政府信息，可以予以公开。根据这一规定，在信息公开的过程中，应严格遵守“谁公开谁审查、谁审查谁负责”和“先审查后公开”的原则，对涉及个人隐私的信息进行预先审查。

然而，法律已明确了相关原则，且规范了信息公开的具体流程，为什么还会发生个人隐私信息泄露事件？问题的关键，在于应该进行的审查并未得到严格执行。而且，当个人隐私信息被“晒出来”的错误发生后，仍无人对此亡羊补牢、进行及时的自我纠错。

更重要的是，一些政府工作人员并未树立起个人隐私保护意识，对个人隐私信息的界定和重要性的认知还很模糊，导致在工作中不自觉地泄露个人隐私。其实，政府工作人员若能换位思考，像保护自身隐私安全一样保护每一位公民的个人隐私安全，此类事件发生的概率也许就会大大降低。

从网络安全法提出个人隐私保护的原则和要求，到“两高”司法解释明确侵犯公民个人隐私犯罪的定罪量刑标准；从对网络服务商的隐私条款进行评审，再到网络用户实名制的全面推行……一个寻求多方参与、强调规范治理的个人隐私保护体系日渐完善。

在这个体系中，政府作为治理规则的制定者、个人隐私保护理念的倡导者、惩治侵犯个人隐私违法犯罪的执法者，不仅应身体力行，严格执行个人隐私保护的规章制度，更应以身作则，在保护个人隐私上率先垂范，充分利用法律武器、利用现代化管理工具，随时随地保护隐私数据。

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。

看《猎场》最重要的不是看职场精英、不是看跌宕爱情、不是看商海沉浮，而是看＂他＂……

年度大剧，也称史上“国内第一部展现猎头职场生活的作品”《猎场》，已进入剧情高潮，即将迎来精彩大结局。郑秋冬一个背负历史污点，在救赎枷锁中前行，而内心一直坚守原则的人，最终成为猎场精英、职场大腕，走到了职业巅峰。

在剧中，又一次险些走入歧途的郑秋冬，因在内心建立起了强大的道德底线，面对盗取数据可成功能获得18万的诱惑报酬，他最终选择了放弃偷资料，一旦失败，轻的这辈子就被列入黑名单，重的要判刑。

商场如战场

商业间谍在现代战场中已是司空见惯的

有派遣卧底去盗取竞争对手的资料

这些都是不正当竞争

这种“无间道卧底”的情节固然有着编剧的艺术创作成分

但它却向大家展现了一个事实

政企内部人员作案泄密的手段不在少数

……

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。

全球每天超 300 万条信息遭泄

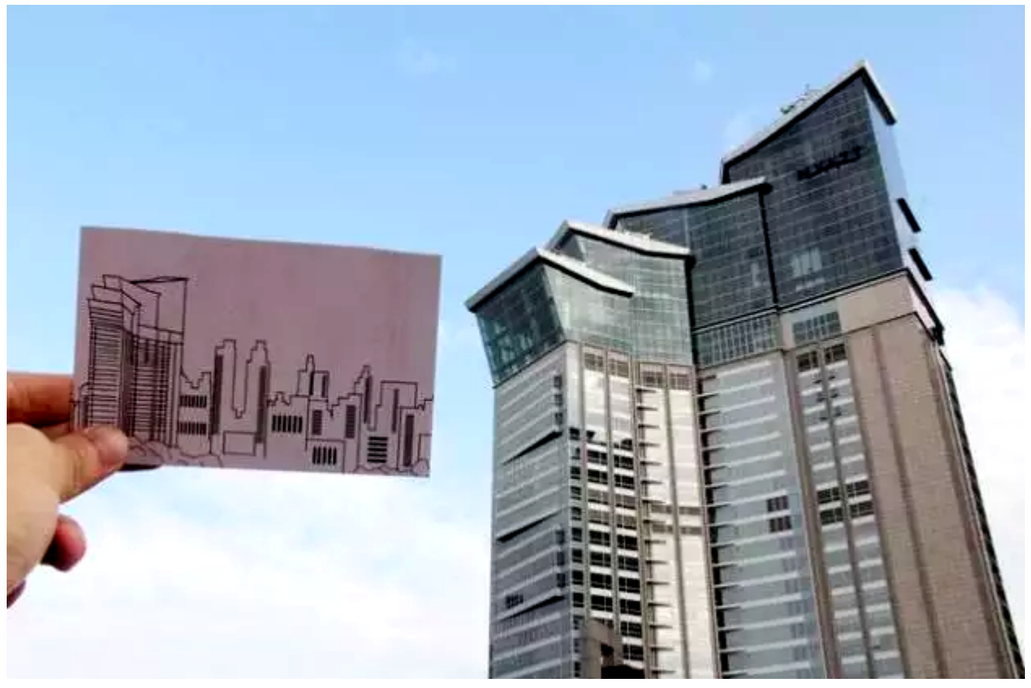
据全球顶级数字安全服务商 Gemalto 最新调查显示，2017 年上半年，19 亿条记录被泄或被盗：比去年全年总量 (14 亿) 还多，比 2016 年下半年多了 160% 多，相当于每天有超过 300 万条个人或私营组织的数据记录遭到泄露。

而我国《刑法》第二百一十九条也规定，盗取、利诱、胁迫或者其他不正当手段获取权利人的商业秘密的。要处三年以下有期徒刑或拘役。而在你倒霉的时候，中介公司早就把自己撇得干干净净。谁的损失大？所以庆幸的是郑秋冬在道德底线面前守住了自己。

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让我们的隐私被暴露在“光天化日”下，而随着由数据的非法获取、网上兜售、甚至违规利用所组成的利益链条悄然形成，无论是企业自身、还是政府机构，包括我们公民自身都需要时刻警惕数据泄露的危险。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政企做好数据安全防护工作。

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 20 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。

亿赛通重磅签约华润置地
强强联合共创数据安全



客户简介

华润置地有限公司（公司简称：华润置地）是财富 500 强企业华润集团旗下的地产业务旗舰，是中国内地最具实力的综合型地产发展商之一。1994 年，华润置地于北京成立，1996 年在香港联交所上市。2010 年，华润置地成为香港 50 家蓝筹股之一。这些均由于华润置地一直秉承着“品质给城市更多改变”的品牌理念，坚持高品质战略的方针。

需求背景

伴随着信息技术的快速发展，各领域数字化、网络化、智能化的水平得到不断提高，华润置地业务得到快速发展，管理及盈利能力不断提升，综合化经营的步伐不断加快。作为房地产行业的龙头企业，数据安全已经成为华润置地业务发展基础和前提。为了加强企业内部管理，提高运营效率，防范数据安全风险，构建一套成熟、稳定、易用、可落地的数据安全防护体系，以增强华润置地数据安全防护能力是企业战略发展的必然选择。

在经过几个月的严格测试、筛选和多方考察后，亿赛通以一流的产品、卓越的技术、贴心的服务和丰富的实战经验赢得华润置地的高度关注。其中，完善的服务和解决方让亿赛通在众多厂商中脱颖而出。最终，华润置地牵手亿赛通共建数据安全智能管理平台（DSIP），共同打造企业数据安全防护系统。

解决方案

亮点功能：

敏感数据发现与管控：实现不同部门、人员上创建对应的管控，如：指纹、关键字、确切数据匹配、正则表达式等。

文件加解密：实现根据部门涉密程度的不同，部署力度轻重不一的梯度式文档加密防护。

磁盘加密：通过实时动态加解密，避免用户使用笔记本外带丢失、被盗后，笔记本硬盘中的数据遭到他人窃取的风险。

介质管控：通过对介质的控制，让用户不能随意使用介质对其重要文档进行备份，只能通过注册后的专用介质进行备份和文件传输。

网络 DLP：可对外网的镜像数据进行内容分析，形成对应的事件，并且做好事件的保留以及报表功能的生成。

项目成果

亿赛通为华润置地提供完善的数据安全智能管理平台（DSIP）解决方案，建立了一套数据安全防护体系，有效地防止员工的不安全行为引入风险，保障了各个环节数据的安全运行，避免了公司敏感数据遭窃的风险，提高数据安全的智能化管理，为华润置地打造了一个良好的信息安全办公环境。

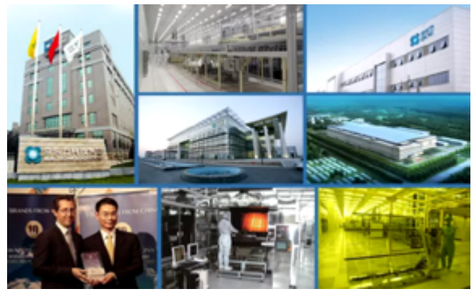
智能化时代发展之际，各行各业都与数据信息深度捆绑，信息安全无疑成为各大领域发展的当务之急，各个行业都应重视起来。亿赛通作为中国数据安全防护专家，14 年来一直肩负着“保护数据所有者的信息资产安全”使命，在未来也会继续数据做数据安全领域的引领者，把数据安全这件事做到更好！

年末继续发力，再树新功，亿赛通力保京东方数据安全

客户简介

京东方科技集团股份有限公司（以下简称“京东方”）是一家物联网技术、产品与服务提供商。核心事业包括显示器件、智慧系统和健康服务。2016 年，京东方新增专利申请量 7570 件，其中发明专利超 80%，累计可使用专利数量超过 5 万件，跻身半导体领域全球第二大创新公司。据 2017 年前三季度市场数据显示，京东方智能手机液晶显示屏、平板电脑显示屏、笔记本电脑显示屏出货量均位列全球第一，显示器显示屏、电视显示屏出货量居全球第二，是全球半导体显示产业的先行者和领导者。

需求背景



作为半导体显示领域全球领先企业，京东方的文件安全是企业最为重视的部分，不仅是财务部、研发部等内部核心文件，还包括专利发明、产品著作权等都是公司的重要资产。数据资产把握着企业的经济命脉，为提高企业内部数据的安全性，实现办公文档内容流转安全可控，文档脱离公司管理平台后能有效防止文件的扩散和外泄，需要建立一套完善的安全管理系统。对此，通过京东方全面的调研与产品测试后，亿赛通无论是领先的产品技术还是完善的服务保障均完全满足了京东方的各项需求。最终，亿赛通力压众多业内同行，与京东方成功牵手共同保护企业数据资产安全。

解决方案

功能亮点

智能加密：智能语义识别根据文档内容进行策略匹配，判断是否为企业核心机密数据，自动筛选进行加密处理；

内容安全防护：防止核心数据通过复制拖拽、截屏录制打印输出以及副本另存等方式泄密；

安全分级控制：实现人员密级、数据密级的安全分级管理控制，满足组织数据分级安全管理要求；

终端防护：确保核心机密数据的内部安全使用、防止数据有意无意泄露，从源头保护数据文档；

审计报表：提供统计分析能力，实现安全现状可度量、事件可追溯、态势可查询；

数据安全传输：数据始终以密文形式传输、存储和使用，保障传输过程中的安全；

权限控制：文档全生命周期管理，如阅读次数、阅读时限及过期自动销毁等保护。文档协同权限、还原及文档内容保护、打印水印等控制。

项目成果

亿赛通智能数据安全管理系统为京东方实现了公司内部文件可以在所有涉密终端上无障碍流转，促进了京东方在项目过程中建立跨部门组织，方便业务交流，安全、高效的完成各项工作，大大的提高了工作效率。同时在数据资产安全保护方面，有效的防止了内部核心信息非法授权阅览、拷贝、篡改等，以达到既防止文档外泄和扩散，又支持内部知识积累和文件共享的目的，高度符合公司所需。

亿赛通深耕国内数据安全市场多年，一直以产品、方案、服务为主导，业务覆盖全国，作为中国数据安全防护专家，始终以顶尖的技术、完善的售后服务，连续占领国内数据泄露防护市场第一的宝座。在着眼于未来之时，亿赛通还将继续肩负“保护数据所有者信息资产安全”的使命，保持创新技术、优质服务、开放合作的传统优势，继续引领数据安全市场前行。