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

11 月刊

2018 年共 11 期

第十一届中国档案信息化推进大会：专家齐聚共话数据安全

亿赛通受邀出席 2018 全国企业云服务大会，助力企业“漫步云端”，数据安全落地

《焦点访谈》独家披露：网络攻击严重，提防境外间谍“敲门”

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

4-8 国内行业新闻

9-15 国外行业新闻

亿赛通动态 ESAFENET NEWS

16/17 第十一届中国档案信息化推进大会：专家齐聚共话数据安全

18/19 亿赛通受邀出席 2018 全国企业云服务大会，助力企业“漫步云端”，数据安全落地

20/21 2018 中国网络安全·智能制造大会 11 月 28 日盛大开幕，亿赛通 & 绿盟科技在长沙等您

亿赛通小贴士 ESAFENET PROMPT

22/23 国际顶级银行汇丰再次深陷数据泄露，金融数据急需科技手段安全防护

24/25 企业核心机密被泄露，80% 都和他们有关！

26/27 11 月 22 日《焦点访谈》独家披露：网络攻击严重，提防境外间谍“敲门”

典型案例 TYPICAL CASES

28/29 亿赛通助奥克斯空调实现数据安全严密防护，制造业又一经典案例诞生

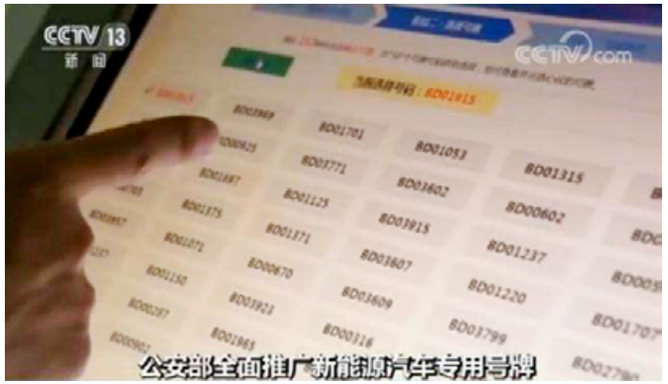
30/31 亿赛通成功签约甘肃电力设计院，构建企业数据安全新防线

企业上云，数据安全不容忽视

现如今，企业管理者们几乎每天都不可避免地看到诸如“大数据”或“云计算”这样的字眼。多云环境变成常态，大数据将通过云端平台深入到多重环境中，云原生应用和无服务器应用架构将愈加成熟。云服务模式已成为大势所趋，在云服务需求迫切的环境下，只有在追随趋势的过程中能准确把握数据资产竞争力，保证企业数据安全，才能在群雄逐鹿当中找到突围路径。对企业而言，云服务确实可以驱动流程创新，但是伴随着越来越多的地方提出“企业上云”行动计划，如何让企业更安全的使用云服务成为社会热议话题……

国内

1、代查车辆信息一条收费 20 元 马鞍山警方打掉网上倒卖公民信息团伙



摘要：马鞍山市公安局雨山分局斩断一条倒卖公民个人信息的黑色产业犯罪链条，抓获钱某等 4 名犯罪嫌疑人，查获非法交易公民信息近万条。据介绍，西部某地车管所一名聘用的工作人员，利用职务之便将每条公民车辆信息以 20 元的价格出售给中间商层层倒卖，在短短两个月的时间非法交易公民信息近万条。

2、“毛巾门”爆料者信息两度遭泄，泄露者或担刑责

摘要：11 月 14 日晚，微博网友“花总丢了金箍棒”（下简称“花总”）发布视频《杯子的秘密》，用 11 分钟偷拍画面揭露了 14 家五星级酒店存在脏浴巾擦杯子擦马桶、用客人用过的面巾擦洗漱台和口杯等卫生乱象。其中，两家酒店（集团）因有员工微信群中泄露“花总”个人护照信息随后致歉。

3、警务人员盗卖个人信息获刑，一审“轻判”遭检察机关抗诉

摘要：雅安市雨城区刑警大队法医庞某、德阳市中江县交警大队辅警黄某某，非法查询公民个人信息并出售给他人，两人均被达州市达川区人民法院判处有期徒刑。达州市达川区人民检察院经审查后认为，原判量刑太轻，遂提出抗诉。近日，该案经达州市中级人民法院公开审理后，依法作出二审判决，该案终于尘埃落定。

4、58 等招聘平台诈骗乱象调查：审核机制失效 数据泄露

摘要：11 月 2 日，西城区法院公开审理了一场泄露公民信息的案件，一位有多年从业经验的猎头，从招聘网站、原单位工作中获取了求职者信息，并在猎头群中互换简历信息，共非法获取了 1852 万条公民个人信息、并将部分信息提供给他人。多位 HR、猎头告诉 21 世纪经济报道记者：“简历的海量下载，买卖、互换，乃至高价值简历交换、企业通讯录共享，已经是这一行业中的普遍现象。”

5、男子入侵近 500 个网站上传色情视频，被抓获刑 2 年

摘要：商河县某单位网站遭到黑客攻击，警方仅凭一条 IP 地址，经过一个多月反复侦查，将犯罪嫌疑人侯某抓获归案。日前，张某以非法侵入计算机系统罪、传播淫秽物品牟利罪被判处有期徒刑 2 年并处罚金 2 万元。

6、检察机关近三年起诉侵犯公民个人信息犯罪 8700 余人

摘要：11 月 8 日，在第五届世界互联网大会“大数据时代的个人信息保护”分论坛上，最高人民检察院检察长张军发言透露，2016 年，中国检察机关起诉侵犯公民个人信息犯罪 1029 人，2017 年起诉 4407 人，2018 年 1——9 月起诉 3283 人，呈增长趋势。

7、售卖公民信息 140 万条 辅警获刑三年六个月

摘要：李某身为交警大队的一名辅警，知法犯法，非法售卖公民个人信息给他人，近日，江西省余干县人民法院审理这起侵犯公民个人信息案，被告人李某犯侵犯公民个人信息罪，判处其有期徒刑三年六个月，并处罚金人民币二十五万元，同时追缴违法所得。

8、四名 90 后倒卖公民个人信息非法获利近 10 万元被刑拘

摘要：近日，徐某明、刘某春、廖某林、叶某扬利用曾当辅警的工作之便，窃取公民个人信息，然后以每条五元、六元不等价格，通过网络向倒卖公民个人信息的代理商出售信息。至案发，共窃取、出售公民个人信息近两万条，从中非法获利近 10 万元。

9、徐州警方破获部督盗取公民信息案 涉嫌倒卖公民个人信息上千万条

摘要：近期，网上出现了“良心卖家”，他们大肆兜售各种低价的酒店客房和机票，从他们手中购得的商品是可以正常使用的，这给不知情的购买者带来了优惠，但也给不法分子带来了巨额利润 . 徐州睢宁警方就破获了这样一起公安部督办的盗取境内外公民信息案，共抓获犯罪嫌疑人 33 名，其侵犯的公民个人信息数千万条，涉案价值在 500 万元以上。

10、入侵政府网站串通招标 这些“黑客”被抓！

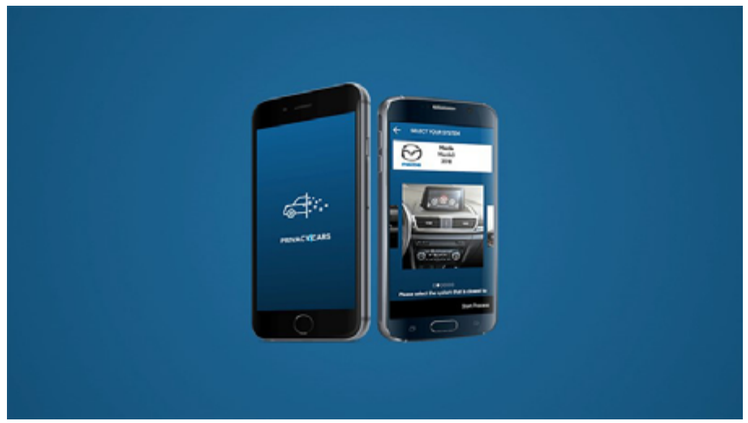
摘要：泸州市公安局网安支队和叙永县公安局网安大队在工作中发现，网民“专业投标支持”频繁在网上联系黑客入侵网站，后侦查发现这是一个专业从事入侵政府公共资源交易网站，获取评标专家名单和文件，串通招投标的犯罪团伙。在泸州、成都、广元、贵州等地抓获杨某权等犯罪嫌疑人 10 人，成功破获泸州首例黑客入侵、串通招投标案，起获四川、重庆、贵州、广东等地评标专家名单上万条，木马程序和黑客工具 52 个，查获大量招投标文件、公司印章。

国外

1、俄罗斯黑客组织 APT29 被指使用 新型恶意软件攻击美国实体

摘要：11 月 16 日，印度安全公司的研究人员发现了一种归属于俄罗斯黑客组织 APT29 的新型恶意软件，它似乎与最近针对许多美国重要实体的攻击有关，这包括军事机构、执法部门、国防承包商、媒体公司和制药公司。

2、汽车蓝牙可能暴露千万司机的私人信息



摘要：Privacy4Cars 公司发现了一款可从车辆中清除 PII 的移动应用程序，其研究人员表示，全球可能会有数千万辆汽车受到影响。风险最高的情况是司机将他们的智能手机与大量租借的车辆（这些车辆被归还后被反复租赁）连接进行数据同步，这样他们的数据极其可能暴露在恶意攻击者视野中。

3、美国慈善机构 Kars4Kids 意外泄露了上万名捐赠者的个人信息

摘要：11 月 3 日，网络安全咨询公司 Hacken 的网络风险研究主管发现了一个似乎是可公开访问的 MongoDB 数据库。经过进一步调查，这些数据似乎包含了 21,612 名 Kars4Kids 捐赠者的电子邮箱地址和其他个人信息，以及超级管理员用户名和密码。

4、最大暗网服务商遭受攻击导致 6500 个网站瘫痪

摘要：时至今日，互联网上的网站数量已经超过十亿，试图在全球范围内扩张的网站（包括暗网）仍在不断增加。扩张过程中，执法者与违法者之间不断发生拉锯战，这场不曾停息的战斗中，最大的暗网托管服务商之一——Daniel's Hosting 于上周四被攻击，导致超过 6500 个网站瘫痪。

5、Dharma 勒索软件继续大肆传播，据称已有 100 多家希腊网站沦陷

摘要：近日，一家颇受欢迎的啤酒厂遭到了勒索软件的攻击，而与此同时，一个主要的海港也遭遇了同样的问题，导致进出港口的船只受到影响。调查显示，这两起案件的罪魁祸首都是 Dharma（也称 CrySiS）勒索软件。

6、思科在其软件产品中无意中泄露了 Dirty Cow（脏牛）漏洞利用代码

摘要：思科在上周三发布的安全咨询中表明，该公司无意中在其软件产品中泄露了一个 Dirty Cow 的漏洞利用代码。该公司承认，这是由于 QA 验证步骤失败所导致的，导致其内部用于质量验证目的的漏洞利用代码被意外公布。

7、数百万美国芯片卡数据信息被泄露

摘要： 双子座咨询公司 (Gemini Advisory) 从各种暗网收集的观测数据表明：在过去 12 个月里，有 6000 万张美国卡被盗。其中 93%是 EMV 芯片卡。此外，更重要的是，75%的被盗卡信息是从当面交易中被盗的记录。它们很可能是因为实体交易的支付系统或者 POS 机遭到了恶意软件等方式的破坏攻击。

8、超过 2 万张银行卡数据在暗网兜售，几乎涵盖巴基斯坦国内所有银行

摘要：据巴基斯坦 GEO 电视台报道，几乎所有巴基斯坦银行在最近都受到了黑客入侵的影响，而这一令人震惊的消息已经在上周得到了巴基斯坦联邦调查局（FIA）网络犯罪部门负责人的证实。

9、近 70 万美国运通印度分公司客户个人详细信息遭泄露

摘要：据外媒 ZDNet 报道，近 70 万名美国运通（Amex）印度分公司客户的个人详细信息在最近被一名安全研究人员发现通过一台存在配置错误的 MongoDB 服务器暴露在了网上。

10、汇丰银行再次身陷数据泄露，部分客户个人信息被窃取

摘要：据外媒报道，汇丰银行（HSBC Bank）似乎再一次成为了数据泄露事件的受害者，部分客户的个人和财务信息已经被证实能够被入侵者所访问，这包括客户的全名、邮寄地址、电话号码、电子邮箱地址、出生日期、帐户号码、帐户类型、帐户余额、交易历史、收款人帐户信息和帐单历史记录。

11、尼日利亚国内最大航空公司 Arik Air 遭遇数据泄露

摘要： 据尼日利亚当地媒体《优质时报（Premium Times）》报道，尼日利亚国内最大的航空公司 Arik Air 在上周三公布的数据显示，该航空公司的大量乘客数据因为一个没有得到保护的亚马逊 S3 存储桶暴露在了网上。

12、俄罗斯一家互联网提供商意外暴露了数千名莫斯科富人的个人信息

摘要：据路透社（Reuters）报道，数千名在一家区域互联网服务提供商完成注册的莫斯科富人可能已经暴露了他们的个人信息，这其中就包括他们的姓名、家庭住址和手机号码等。

13、法国一家工程公司 65GB 机密文件被盗，涉及核电站、监狱、电车项目

摘要：据外媒报道，在几个月前发生的一场网络攻击中，超过 1 万份与法国核电站、监狱及电车网络相关的机密文件从 Ingérop 公司的服务器上被窃取，其中一些数据已经被转移到了一台位于德国的租用服务器上。

14、丽笙酒店集团遭遇数据泄露，官方称受影响会员不足 10%

摘要：据英国科技新闻网站 The Register 报道称，丽笙酒店集团（Radisson hotel Group，以下简称“丽笙”）被确认能够被黑客访问的信息有会员的姓名、住址（包括居住国）、电子邮箱地址，以及一部分会员的公司名称、电话号码、丽笙奖励计划会员编号和已存档的常飞顾客编号。

第十一届中国档案信息化推进大会：专家齐聚共话数据安全

11 月 16 日，由中国档案科学技术交流中心、档案安全保护技术专家委员会主办的“第十一届中国档案信息化推进大会暨保密档案安全管理技术与应用交流展”在北京西国贸大酒店盛大举办。交流会齐聚了政府、国资委集团企业、企事业单位、军队军工等重磅机构档案信息部门领导。会中与安全圈行业专家共同探讨档案数据化存储该如何积极加强信息防护与档案安全体系建设；在网络强国建设中如何落实档案信息数据安全与等级保护制度；如何提升涉密信息系统、涉密计算机、涉密载体的安全保密管理；如何构建全方位数据安全防护体系建设等热门话题。

亿赛通数据安全资深顾问建言“DATA IS MONEY”，由此引出档案信息安全管理中数据安全发展的新技术与新应用。我们知道，近年来国内外爆发了多起内部员工窃取核心机密的信息安全事件，从央视 315 曝光国内某些企业内部员工泄露客户信息，到勒索病毒恶意加密企业数据资产、黑客盗取运动员医疗档案等事件的发生，给全球信息中心数据安全拉响了警钟。与此同时，国资委、公安部、部队军工等国家相关部门提出了一系列信息安全相关政策规定，强化档案信息科技风险防范和信息安全保障能力。

针对以上泄露事件亿赛通资深顾问在大会上给予了几点预防建议，分别从基于数据存在的三种形态（存储、使用、传输），对数据生命周期中的各种泄密途径进行全方位的监查和防护，保证了敏感数据泄露行为事前能被发现，事中能被拦截和监查，事后能被追溯，使得数据泄露行为无处遁形，敏感数据无径可出，从而成为真正适用于中国国情的 DLP 数据泄露防护体系。

中央办公厅及国务院办公厅联合发布的《关于进一步加强档案安全工作的意见》中明确提出要进一步把确保档案安全保密作为 “十三五”时期我国档案工作的重要目标；下大力气，建立健全我国档案安全保密体系，不断提高国家政府与企事业单位的档案安全管理水平。完善敏感信息存储和传输等高风险环节的控制措施，对数据、文档的访问应建立严格的审批机制，对用于测试的生产数据要严防敏感数据泄露。

亿赛通按照档案部门的安全体系要求，不断提供满足和引导客户的数据泄露防护解决方案，先后为教育部教育管理信息中心、中共中央办公厅秘书局文印中心、国家外汇管理局、航空工业信息中心、乐清市档案馆、温州市档案局、平阳县档案局等数十家党政军客户提供数据安全保护方案，为档案信息安全的建设提供满足不同客户需求的最优解决方案，科技驱动达到客户信息安全提供强有力的保障。

亿赛通受邀出席 2018 全国企业云服务大会，助力企业“漫步云端”，数据安全落地

现如今，企业管理者们几乎每天都不可避免地看到诸如“大数据”或“云计算”这样的字眼。对企业而言，云服务确实可以驱动流程创新，但是伴随着越来越多的地方提出“企业上云”行动计划，如何让企业更安全的使用云服务成为社会热议话题。为此，2018 全国企业云服务大会于 11 月 8 日在杭州召开，亿赛通作为安全行业领军企业应邀出席大会，并进行“企业上云，安全落地”主题演讲，为企业提供一个上云安全新角度，加快上云步伐，解决企业上云安全隐患，助力企业在新的环境中数据资产安全落地。

企业上云需要安全落地

云服务模式已成为大势所趋，在云服务需求迫切的环境下，只有在追随趋势的过程中能准确把握数据资产竞争力，保证企业数据安全，才能在群雄逐鹿当中找到突围路径。

亿赛通高级咨询顾问于会中做了“企业上云，安全落地”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。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、企业需求进行剖析，精准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“事前主动防御、事中检测响应、事后追踪溯源、全程态势感知“四步巩固“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。

数据安全 = 健康

解决企业上云安全隐患除了需要充分考虑数据面临的各种主动泄密和被动泄密风险，还应考虑系统对企业的业务影响范围，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，并且分别从文件的存储、传输、使用等方面，有效培养并提高员工对敏感文件的保密意识。

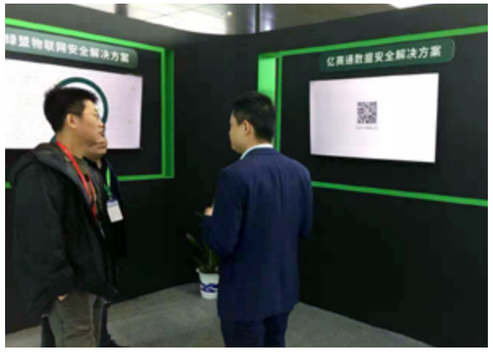
“服务客户、持续创新、勇担责任、专业至上”是亿赛通永成不变的核心价值观，通过领先的技术和丰富的解决方案，为每一位客户提供最及时、最全面、最到位的服务，先后为众多国内外知名企业提供数据安全解决方案。截至目前，亿赛通公司已在全国三十余个主要城市设立了分支机构，为立足中国、迈向全球市场打下了坚实的根基！

2018 中国网络安全·智能制造大会 11 月 28 日盛大开幕，亿赛通 & 绿盟科技在长沙等您

11 月 28 日 -11 月 30 日 2018 中国（长沙）网络安全·智能制造大会在长沙国际会展中心如期举办，该博览会是国内规模最大、级别最高的智能制造产业峰会之一。亿赛通在此次网络安全·智能制造大会中牵手绿盟科技，将网络安全、数据安全以及综合方案等产品进行全方位展示，不仅对全国企事业及制造业单位的重点安全防护领域进行专项宣传讲解，还针对社会公众关注的热点问题进行深入探讨，并着力推进网络安全大会上的相关主题活动，助力国家对全民进行网络安全教育和普及。

强强联合 并肩作战

亿赛通作为信息安全领域的领军企业，不仅为政府军工、制造业、金融、能源、运营商等领域提供专业服务，在个人信息安全建设上也有突出贡献，经过长达 15 年的专业技术领先、经验积累沉淀，已经成为中国最具代表性的信息安全企业。亿赛通在数据安全技术方面也曾开创多个业内第一，一直引领数据安全产业飞速发展。与绿盟科技强强联合后，网络安全与数据安全产品线全面拓展，双方在安全产品及服务上一次次遥遥领先。此次联手参展，无疑成为本届博览会上的最强搭档，充分展现了亿赛通及绿盟科技在网络安全、数据安全、安全服务等方面的领先优势。



展会现场，观展嘉宾在亿赛通精英伙伴详细透彻的介绍下，对其产品和方案产生了浓厚的兴趣。网络安全信息时代下，亿赛通从未止步，其数据安全产品和数据安全解决方案稳居国内安全市场前列。在产品研发上，始终坚持创新，2018 年初更是在武汉成立第二研发中心，正式开启北京、武汉双核研发驱动模式，为企业发展和人才培养注入源源不断的活力。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“网络安全”时代全面化进程做出努力。

移动互联网快速发展的大数据时代，每个人几乎每时每刻都在产生数据，网络安全问题引起人们的恐惧和关注，网络安全将成为一个永恒的话题。国家加大信息安全监管，规范网络信息的安全管理，打击违法犯罪活动，保护信息安全任重而道远。亿赛通 & 绿盟科技继续努力携手更多企业，从技术层面为信息安全保驾护航，防止各种黑客入侵、病毒侵袭、数据泄露等事件上演。

这里有没有你正在苦恼的问题？

敏感数据如何进行有效防护？

内部人员通过 mail 泄密怎么办？

内部人员离职通过 U 盘拷走数据怎么办？

可以拦截内部人员外发泄密信息吗？

是否想知道是谁泄了公司机密？

想监控内部人员外发数据，又不想被他知道怎么办？

长沙网络安全 & 智能制造大会，亿赛通为您指点迷津 ~

11 月 28 日 -30 日，我们在 E1 馆 B2 展位等您！

国际顶级银行汇丰再次深陷数据泄露，金融数据急需科技手段安全防护

近日，汇丰银行（HSBC Bank）部分客户的个人和财务信息已经证实被非法入侵，导致其再一次成为了数据泄露事件的受害者。目前已泄露的敏感信息包括客户全名、邮寄地址、电话号码、电子邮箱地址、出生日期、帐户号码、帐户类型、帐户余额、交易历史、收款人帐户信息和帐单历史记录……

从汇丰银行向加利福尼亚洲总检察长办公室提交的数据泄露通知来看，汇丰银行美国（HSBC Bank USA）部分客户的网上银行账户在 2018 年 10 月 4 日至 2018 年 10 月 14 日期间遭到了未经授权的访问。发现这一情况后，汇丰银行立即暂停了在线账户访问服务，以防止进一步的危害发生。

据知情人士称，此次数据泄露事件发生的原因可能是撞库攻击，登录凭据是从其他数据泄露事件中获取的，这些信息随后被用作对汇丰银行的撞库攻击。

安全专家表示，为了防止凭证填充攻击，网上银行用户应定期更改密码，并尽量在访问不同的网站时使用不同的密码。当攻击者登录用户的网上银行账户时，通常可以在这些账户中找到一些有用的信息，如住址、电话号码、余额、交易记录和帐号等。

银行该如何保障自身数据安全

针对此次银行数据外泄事件，亿赛通作为中国数据安全防护专家，结合多年来给国内众多知名银行实施过的安全项目，从丰富的实施经验中给予几点防护建议，即对银行内部系统如何管控(业务办公网)、银行外网如何管理(网络及邮件) 以及对移动存储介质如何做到有效监管、如何充分利用现代信息化手段，全方位保护银行的数据安全，把泄密风险降到最低。亿赛通从里到外为银行部门提出了一套一体化的数据安全解决方案，不仅可以有效保证银行业务的正常运转 ,而且也对公民的信息安全贡献一份力量。

办公网数据安全防护：在各大银行企业办公环境中，诸多电子文档采取明文存储，可以通过移动存储介质或者互联网等方式轻松带离企业环境，而且文件外发途径多种多样（邮件、网盘、移动存储设备等等）造成很难通过封堵的方式去解决电子文档外泄问题。因此，亿赛通通过加密技术对核心电子文档进行管理，保障数据只有在合法终

端上可使用，如果数据脱离企业合法环境，均将处于不可用状态。

终端敏感数据智能防护：通过对所有数据进行内容识别扫描，对文档进行分类分级，智能加密处理，非敏感数据不受加密影响，防止一刀切的加密方式。使办公业务更加智能更加快捷。

网络及邮件数据防护：在确保正常的互联网应用及邮件的正常使用的前提下，对向外发布信息进行敏感性过滤，监管向外发布敏感信息行为及内容，一旦触发安全事件，可以直接追溯到相关责任人。正确的宣导和告警可以避免和减少安全事件的发生。

移动介质数据防护：目前部分银行在网络拓扑中已经实现了内外网隔离，办公终端没有互联网条件，那么计算机终端的外设端口就成为数据外泄的重要通道，对于移动存储设备的管控，其重心在于移动设备的识别与管控及数据传输监控。

亿赛通根据银行的数据安全风险隐患并结合上级监管部门对银行的信息安全建设要求，提供全面的数据安全解决方案，相信如果从以上几点出发，从内部到边界所有敏感数据进行加密监管，不法份子也不会轻而易举的谋取暴利，危害社会危害他人。

一个好的社会环境不是等来的，也不是靠老百姓忍受苦难能救赎的，而必须是通过有关各方的积极治理才能臻于完善。一味指责不法分子的全无底线，或者一味强调信息保管单位的无能无力，不如下决心打造一个界限明确、放心可靠的制度环境，用技术手段用科技手段做到安全防护，银行管理者的工作任务已经迫在眉睫。

企业核心机密被泄露，80% 都和他们有关！

近日，北京市海淀区某离职员工又舔了全国吃瓜群众的屏，登上热搜榜，各大科技公司 BOSS 深受内伤！下面小编带你领略这件现实版的内鬼窃密事件！

哪些敏感数据被内鬼窃取？

今年 3 月，海淀区某科技公司员工陈某在离职之前私自开通公司多个重要技术项目权限，下载公司独立开发的三个项目源代码，离职后将代码带出，倒卖后，共获利 800 万元。

内鬼如何获取项目源代码？

陈某是该科技公司原运维主管，在职期间，通过非法手段提高自己系统操作权限，从而获取大量自己本无权限接触到的核心代码，并通过自己的账号进行下载。调查中，通过梳理该科技公司系统的电子日志，专案组民警发现曾有人在未经授权的情况下擅自登录后台数据库，对一个账号进行非法权限提高。

源代码真的能获利这么多？

源代码在各大科技公司是相当受欢迎的，这个价值就不用多说了。源代码倒卖利润颇为可观，一些源代码还被用来二次开发，制作私服和外挂。再则技术人员离职如果带走源码，也可以开发同类产品与前东家竞争。

多起内鬼泄密事件引起社会关注

其实内鬼窃取公司情报事件 ,早已发生过不止一次，每次都会给企业带来不可磨灭的损失。据某杂志统计，有80％的数据泄露是企业内鬼所为，黑客和其他方式仅占20%。

1、苹果供应商内部员工离职窃取商业机密

苹果 A 系列芯片的供应商台积电公司技术副理将 16nm，10nm 等机密文件通过打印的方式保存，准备辞职后带入新公司，从而获取苹果订单。

2、医院职工窃取产妇信息

某医院后勤人员用手机拷贝产妇信息出售给儿童写真影楼。其窃取的文档里面标注着新生儿姓名、出生日期、家庭住址以及孩子父母联系方式，信息数量多达上千条。

3、教育、通信企业职工利用职务之便非法获取公民个人信息

李某利用“校讯通”业务代理的职务之便 ,非法从“校讯通”系统中复制西昌市 17 所学校的学生数据 4 万余条并非法出售给教育培训机构。

以上几起案件告知我们，企业核心机密泄露的案件中，大量的数据均是以电子文档的形式存在并被窃的。在公司内部其台式电脑中都会大量涉及企业商业秘密的核心部门资料。

内鬼泄密亿赛通有妙招

然而，所有的企业内部员工泄密事件完全是可控的，只要企业从数据内部和外部两个方面进行严格管理数据，就会让“内鬼”无空可钻。那么针对外部和内部的隐患，亿赛通研发了一整套数据防护解决方案，保障数据在存储中的安全、使用中的安全、传输中的安全、外带中使用时的安全、外发中的安全。

首先，在内部方面，以数据加密技术为核心，通过将技术平台与管理体系有效结合，可对任意文档自动透明加密，实现对用户核心数据资产的全方位保护。同时，通过信息安全边界的建立，降低核心数据资产如源代码、设计图纸、财务数据、经营分析以及其他任意信息资产有意或无意泄密风险。此外，配合完善的信息安全咨询服务，对企业的业务进行梳理和流程建立，保障企业的核心业务正常运转，同时不影响用户工作习惯及业务效率。数据加密技术是很多公司电脑采购的标配产品。其次，在保障外发数据安全方面，针对客户的重要信息或核心资料，当员工需要将涉密文档外发给客户（代理商、合作伙伴等）人员时，应用文档外发控制系统生成外发文件发出。当外发文件打开时，用户通过身份认证，方可阅读文件。同时，外发文件可以限定接收者的阅读次数和使用时间等细粒度权限，从而有效防止客户重要信息被非法扩散。

总之，亿赛通“数据防护”解决方案可以做到智能识别、动态加密，实现加密数据无感知、加密数据脱离使用环境无法读取、非法获取数据后无法使用，无边界全方位保护数据安全。在信息化之路上，保障数据安全亿赛通与你一同携手共进，净化数据安全环境，让内鬼不在兴风作浪，让企业安全便捷放心的使用。

11 月 22 日《焦点访谈》独家披露：网络攻击严重，提防境外间谍“敲门”

在互联网技术高度发展和广泛应用的今天，网络与国家安全息息相关，没有网络安全，就没有国家安全。而在现实中，互联网这个看不见的战场并不平静，境外间谍情报机关通过各种手段窃取国家机密，危害国家安全的事件时有发生。

某网络科技公司因为具有涉密邮件管理系统建设资质，在全国 1500 多家客户中，很多是党政机关等涉密单位。这些单位每天通过该公司搭建的电子邮件系统进出大量重要文件。然而，就是这样一家有着涉密邮件管理系统建设资质的公司，发生了一起规模庞大的网络窃密事件，近千家客户包括重要党政机关单位的地理位置、邮件系统账号密码和网管人员的联系方式被窃取。调查发现，该科技公司的核心应用服务器先后被三家境外间谍情报机关实施了多次网络攻击，窃取了大量敏感的数据资料。

这一切是如何发生的呢？原来，该公司为了方便员工查询信息，把客户的地理位置、网管人员身份、远程登录方式和账号密码等敏感信息储存在内网服务器中，并在内网和外网之间搭建了一个连接通道，这样即使不在公司，通过一个 VPN 账号就可以随时登录内网进行查询。他们自以为这样做毫无风险，不曾想，早已有人密切关注他们的一举一动，随时寻找可乘之机。

该公司缺乏保密意识，为了工作便捷建立的通道，同时也为境外间谍网络窃密活动打开了方便之门，由于重建设轻管理，重应用轻安全，给相关单位带来了严重的损失。事件发生后，该公司被责令停业整改，并被有关部门依法进行了处罚，同时，国家安全机关要求该公司逐一对此次事件涉及的用户单位进行安全加固，消除危害影响。

近年来间谍很重视通过网络实施技术窃密和情报搜集活动，对国家秘密安全和网络安全造成严重危害，当前，我国面临的网络攻击窃密敌情形势异常严峻复杂。2018 年以来，境外间谍情报机关对党政机关、科研院所、军工单位等实施了多轮次大规模的网络攻击窃密活动，造成我国境内数百台计算机设备被攻击控制，数十万份文档资料被窃取，涉及政治、经济、军事、外交、科技等多个领域。

相关专家认为发生这种时间主要原因有三点：第一点是管理人员敌情意识比较淡薄，总认为网络攻击这种事情离自己很远，大部分是在电影电视这种影视作品里面会出现，远离自己的这种日常环境；第二点是防范能力不足，主要反映在对这种网络安全的知识不具备；第三点就是相关重点单位的防范体系不足，管理不到位。

网络领域的竞争是当前国家间最重要的竞争领域之一，维护网络安全和国家秘密安全，是各级涉密单位、各大安全厂商乃至全社会的共同责任。各国普遍重视网络领域的立法，对关键信息基础设施保护、个人信息安全保护、数据安全管理等方面事项进行法律规定。今年 4 月，十九届中央国家安全委员会第一次会议审议通过了《党委（党组）国家安全责任制规定》，对涉嫌违反《反间谍法》、《网络安全法》、《保密法》等法律法规，以及渎职犯罪者，国家安全机关将联合检察机关等有关部门依法追究刑事责任。

国家安全无小事，千万不能掉以轻心。通过加强我国网络安全领域的立法和执法，不断完善相关规定，积累网络管理经验，将社会各群体的权益法定下来，能够为今后国际合作竞争中保障国家和国民利益争取更多主动。国内专业专项信息安全厂商也迎来大好发展时机，亿赛通作为中国数据安全防护专家，全力支持国家政策，不断为企业、党政机构提供切实有效的安全防控解决方案，对数据在使用、存储和流转过程中的安全问题，有机整合多个安全产品，打造全方位、立体化、多层次的企业数据安全防护体系。可以发现、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。其部署效果集终端数据防护、网络数据防护、应用数据防护、存储数据防护、介质数据防护、云服务平台等一体化的企业综合数据安全防护体系，使得数据窃密行为无处遁形，敏感数据无径可出，从而真正意义上保护企业的安全。

亿赛通助奥克斯空调实现数据安全严密防护，制造业又一经典案例诞生

客户简介

奥克斯空调股份有限公司隶属奥克斯集团有限公司。自 1994 年成立以来，历经 20 年专业制冷历程，现已成长为中国空调行业的领导品牌，中国企业 500 强，拥有奥克斯姜山国际产业园、奥克斯南昌工业园、天津武清工业园三大产业基地，空调年产突破 1000 万套，销售额超 100 亿，员工 10000 余人。

需求背景

奥克斯空调作为行业领导品牌，数据是否安全影响着公司生存发展现状，其庞大的业务数据在部门关键流程节点存在泄露风险，敏感数据容易被拷贝。奥克斯急需完善保密体系，提升业务管理规范性，以确保企业信息安全。

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，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

亿赛通为奥克斯空调股份有限公司成功建立了一套数据资源保护标准，防止员工的不安全行为引入风险，以及保障了各个环节数据的安全运行，并且使得员工了解与自己相关的数据安全保护责任，强调数据系统安全对企业业务目标的实现、以及业务活动持续运营的重要性。

亿赛通成功签约甘肃电力设计院，构建企业数据安全新防线

中国能建甘肃院

客户简介

中国能源建设集团甘肃省电力设计院有限公司（简称“中国能建甘肃院”）始建于 1958 年，现为中国能源建设集团有限公司所属Ⅱ级企业，是甘肃省内一家甲级电力设计院。中国能建甘肃院 2015 年成功进入国家电网公司输变电工程设计承包商资信评价前 20 名行列，总承包工程项目发展迅速，历经 15 年的蓬勃发展，先后承揽新能源发电、送变电工程总承包项目百余项，合同额约 65 亿元，连续多年位列中国勘察设计协会公布的全国工程总承包 100 强行列。

需求背景

随着网络信息技术的信息发展，中国能建甘肃院在信息化各个领域进行了大量的投入，中国能建甘肃院充分发挥专业技术优势，积极服务国家、地方电网建设，先后承担大批省内外的电力工程勘测设计和工程总承包项目，是国内第一家承担 750 千伏变电和同塔双回路输电线路工程设计任务的省级设计企业。在企业持续保持市场竞争力的情况下，需要对企业的研究成果进行保护。为此，中国能建甘肃院携手经验丰富的亿赛通对企业的设计图纸、研究报告等数据资产进行保护。

解决方案

电子文档安全管理系统，采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，杜绝了外部人员非法窃取企业数据资产，并对生产的文档进行全生命周期的防护。

透明加密：对指定格式的文件进行透明加密，有效的保护了企业的数据资产；

文档安全网关：解决了企业设计图纸集中存储的安全问题；

离线办公策略：可通过离线审核、策略预设及离线补时等功能满足各种离线办公要求；

内容安全管控：截屏录屏控制文档、阅读水印文档、打印水印、拷贝粘贴控制。

部分经典案例

中国能建甘肃院使用亿赛通电子文档安全管理系统，有效的保护了企业的设计图纸、科研成果。既解决了文档使用安全问题，又通过文档安全网关解决了企业大量内部资料集中存储的安全问题。亿赛通助力中国能建甘肃院在市场上保持了持续的竞争力。