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

3 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：86-10-57933888

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com

CONTENTS 目录

刊首语 PREFACE

数据安全

肩负使命

保护数据所有者的信息安全

阳春三月，风和日丽。不知不觉 3 月已经过去，亿赛通 3 月刊精彩呈现，带你一起回顾你身边的安全大事、小事，把握数据安全行业最新动态，深耕企业信息安全，布局关键节点。

目前国内外数据安全行业很不平静 ,数据泄露、信息泄露事件此起彼伏 ,从未消停。国内多家医院又遭勒索病毒、Facebook 遭遇史上最大泄露丑闻、好莱坞再爆艳照门、苹果 icloud 遭内部人员入侵、公务员泄露公民隐私……面对这些接连发生的重大数据泄露突发事件，中国数据安全防护专家——亿赛通，多年来一路坚持守护您的数据安全，肩负“保护数据所有者的信息安全” 的使命，引领数据安全行业飞速发展。

国内

1、公务员利用职务之便泄露 82 万条公民信息 从中非法获利现已被抓获

摘要：南京一公务员利用职务之便泄露了 82 万条公民信息，江苏省南京市鼓楼区人民法院判处其有期徒刑四年，并处罚金 9 万元和没收违法所得。

2、惠州出台大数据试验区建设方案 推动数据共享

摘要：21 日，惠州市政府官网发布《惠州市贯彻落实珠江三角洲国家大数据综合试验区建设实施方案》。

3、“银行分期”买手机被掉包成“网贷” 手机没买成信息被泄露

摘要：温州一男子购买手机，店家工作人员要走他的身份证，在没有征得其同意的情况下用他的身份证办理了网上分期贷款，从而导致其个人信息泄露给了网贷公司。

4、两会声音：要彻底禁止炒作状元

摘要：两会建议，要彻底禁止炒作状元，堵住考生信息泄露源头，扎牢不能炒的制度笼子；严肃问责，就是要加大力度出重拳，扬起不敢炒的惩戒利剑。

5、2017 年有近五分之四的企业（79%）受到了数据泄漏的影响

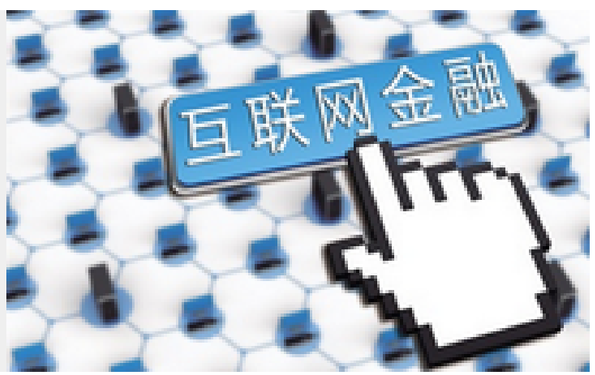
摘要：温州一男子购买手机，店家工作人员要走他的身份证，在没有征得其同意的情况下用他的身份证办理了网上分期贷款，从而导致其个人信息泄露给了网贷公司。

6、北京消费者协会：手机 APP 过度采集个人信息 26.54% 用户信息泄露自认倒霉

摘要：凤凰网 WEMONEY 讯 3 月 7 日，北京市消费者协会发布《手机 APP 个人信息安全调查报告》。调查结果显示，有 89.62% 的人认为手机 APP 存在过度采集个人信息，79.23% 的人认为手机 APP 上的个人信息不安全，41.16% 的人在安装或使用手机 APP 之前从来不看授权须知。

7、上海市消保委：互联网金融安全成投诉新热点

摘要：上海市消保委 19 日披露，互联网金融的安全性成为投诉新热点。该委当日透露了 2018 年 315 期间 (3 月 13 日—15 日) 该委受理投诉的情况。据统计，期间，上海市消保委受理了 3056 件投诉。



8、苗圩：推动互联网、大数据、人工智能和制造业的深度融合

摘要：工信部部长苗圩 26 日在国务院发展研究中心主办的中国发展高层论坛上表示，中国将 加快发展先进制造业，加快发展新材料、生物医药、电子信息、5G、节能环保等新兴产业， 推动互联网、大数据、人工智能和制造业的深度融合。

9、低价共享单车包月卡网上热销 专家：有个人信息泄露风险

摘要：近期，网络购物平台上有低价版骑行月卡，可以提供向已有共享单车账号里充值月卡服务，6 元左右就能畅行整月，但需要提供共享单车信息。

国外

1、全球知名征信机构 Experian 因大规模数据泄露事件面临政府起诉

摘要：据外媒报道，圣地亚哥市律师 Mara Elliott 已向益百利信用机构（ Experian ）提起诉讼，称该公司未根据加利福尼亚州法律要求将 2013 年发生的大规模数据泄露事件告知其受影响的消费者。 据估计，约有 3000 名消费者可能遭受影响，其中包括圣地亚哥估计的 25 万人。

2、Facebook 史上最大规模数据泄露牵出惊天丑闻

摘要：近日据政治咨询公司“剑桥分析”（Cambridge Analytica）前雇员克里斯多夫·怀利爆料，“剑桥分析”曾在 2016 美国大选期间，利用 Facebook 上 5000 万名用户资料进行分析，最终利用“读心”有术，向 5000 万名 Facebook 用户发送“专属”政治广告。

3、美国在线旅行社 Orbitz88 万客户数据面临泄露风险

摘要：据国外综合新闻平台 PhocusWire 的报道，美国在线旅游巨头 Expedia 旗下的在线旅行社 Orbitz 公司在本周二公开宣布称，其在线旅游预定平台存在一个严重的安全漏洞，而这个漏洞可能会使得大约 88 万名 Orbitz 客户面临数据泄露风险。

4、航运巨头马士基子公司近一半员工个人信息被泄露

摘要：根据《丹麦海军时报（Maritime Danmark）》的报道，航运公司 Svizter Australia 的企业传播总监 Michala Paulli 已经向丹麦海事局证实，该公司已经成为了数据泄露事件的受害者，近一半员工的个人信息被意外泄露到了公司外部，而相关的调查仍在继续进行。

5、英国数百万彩票玩家账户遭窃，1050 万玩家要求修改密码

摘要：据外媒报道，英国国家六合彩管理公司“卡美洛”(Camelot)约有 150 个玩家帐户（总共 1050 万个注册帐户）遭到未经授权的登录，导致玩家信息被外部查看，其中包括姓名以及国家彩票帐户中的金额。

6、医疗机构频遭黑客攻击，2018 年还将面临五大安全威胁

摘要：RSA 近期发布的《数据隐私报告》调查了欧洲和美国的 7500 名消费者。59%的受访者担 心他们的医疗数据受到损害，39%的人担心黑客会篡改他们的医疗信息。

7、 全美第一所公立虚拟大学近 37 万师生信息数据遭泄露

摘要：据多家外媒报道，FLVS 似乎成为了数据泄露事件的最新受害者，近 37 万名师生的个人敏感信息可能已经遭到了外泄。

8、 美国 160 多家 Applebee 餐厅消费者支付卡信息遭泄露

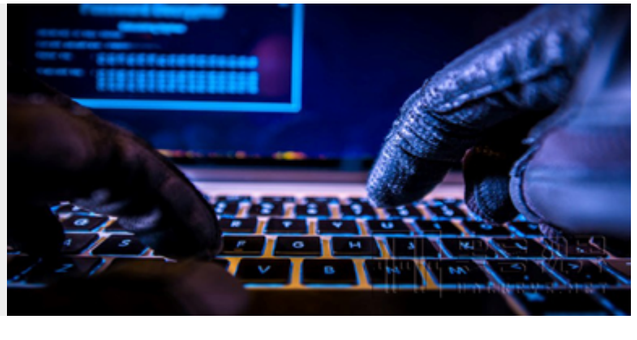
摘要：根据 RMH 特许经营控股（RMH Franchise Holdings）在其网站上发布的公告来看，旗下拥有和经营的 Applebee 连锁餐厅似乎成为了数据泄露事件的受害者。

9、 日本游戏公司 NIS 美国分部在线商城客户信息和财务数据泄露

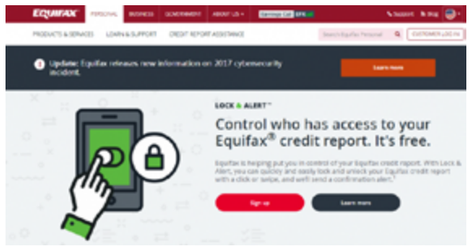
摘要：外媒 3 月 5 日消息，日本游戏开发商 Nippon Ichi Software 透露，其美国分公司 NIS America 的网上商城 store.nisamerica.com 和 snkonlinestore.com 遭受了严重的数据泄露，可能会影响在线客户的个人信息和财务数据。

10、印度国有电信运营商内部网站存漏洞，超 4.7 万员工信息泄露

摘要：据多家国外媒体的报道，法国安全研究人 Robert Baptiste 声称已获得了印度国有电信运营商 Bharat Sanchar Nigam Limited（BSNL）内部网络数据库的访问权，该数据库包含超过 4.7 万名员工的详细信息。



11、美国征信公司信息泄露事件升级，新增 240 万受害者



摘要：据瑞士资讯 3 月 1 日援引法新社报道，美国征信公司伊奎法克斯 (Equifax) 当日表示，关于 2017 年 9 月曝出的 1.4 亿用户个人信息泄露事件，近日又发现另外 240 万名受害者。

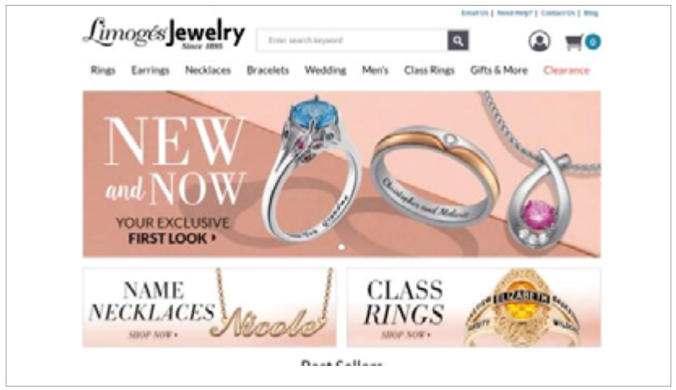
12、苹果用户称 iCloud 遭苹果工作人员入侵并遭威协！

摘要：网友与苹果公司客服人员接触过程中与对方发生口角，没想到该客服利用职务之便，对网友的 iCloud 账户进行入侵，并非法获取隐私资料以此要挟。

13、好莱坞艳照门仍在继续？英国女星乔琪•波特私照及视频曝光

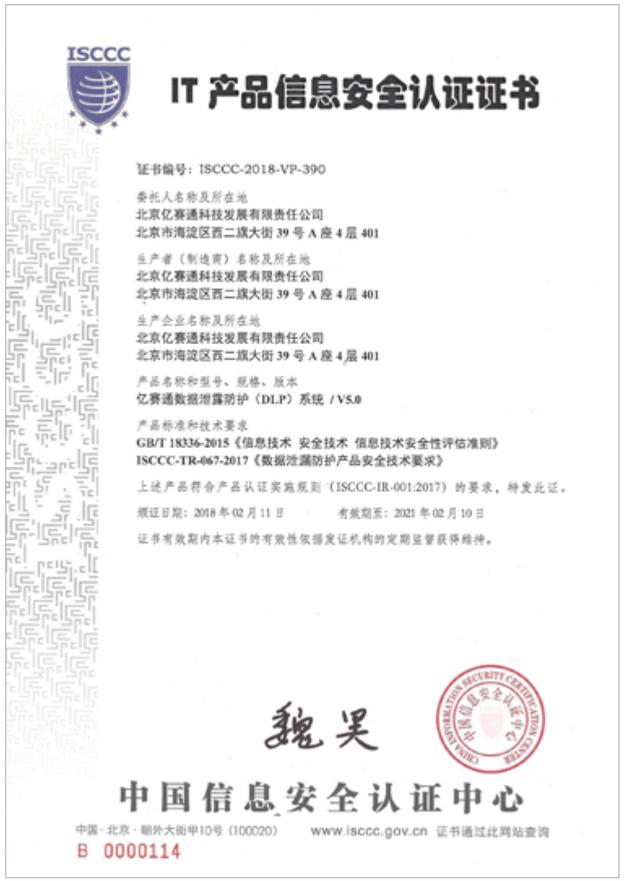
摘要：近日因出演《圣橡镇少年》走红的英国女星乔琪 - 波特（Jorgie Porter）私照及视频又在网络曝光。乔琪 - 波特的私照和视频不仅在艳照门泄露渠道，在成人站点也有流通。

14、珠宝零售商 MBM Company 被曝数据泄露 密码竟用明文保存



摘要：近日，珠宝零售商犯了数据安全上的大忌，重要用户资料竟然没有加密，而是用明文保存。130 万用户的个人信息，包括邮寄地址、邮政编码、电子邮件地址和 IP 地址被泄露。

喜讯｜热烈庆祝亿赛通数据泄露防护（DLP）系统 /V5.0 再获国家权威认证



IT 产品信息安全认证证书

证书编号：ISCCC-2018-VP-390

委托人名称及所在地
北京亿赛通科技发展有限责任公司
北京市海淀区西二旗大街 39 号 A 座 4 层 401

生产者（制造商）名称及所在地
北京亿赛通科技发展有限责任公司
北京市海淀区西二旗大街 39 号 A 座 4 层 401

生产企业名称及所在地
北京亿赛通科技发展有限责任公司

产品名称和型号、规格、版本
亿赛通数据泄露防护（DLP）系统 /V5.0

产品标准和技术要求
GB/T 18336-2015《信息技术 安全技术 信息技术安全性评估准则》
ISCCC-TR-067-2017《数据泄露防护产品安全技术要求》

上述产品符合产品认证实施规则（ISCCC-IR-001:2017）的要求，特发此证。

颁证日期：2018 年 02 月 11 日　　有效期至：2021 年 02 月 10 日

证书有效期内本证书的有效性依据发证机构的定期监督获得维持。

魏昊

中国信息安全认证中心

中国·北京·朝外大街甲10号（100020）　www.isccc.gov.cn　证书通过此网站查询

B 0000114

近日，亿赛通数据泄露防护（DLP）系统 /V5.0 通过中国信息安全认证中心的审核，符合 GB/T18336-2015《信息技术 安全技术 信息技术安全性评估准则》以及 ISCCC-TR-067-2017《数据泄露防护产品安全技术要求》双项标准，产品技术水平再受国家权威认可。

数据泄露防护系统（DLP）

一款基于内容识别技术，对设计图纸、源代码、合同文本、财务报表等敏感文件进行数据安全保护，防止通过邮件、聊天工具、网盘、U 盘拷贝、打印等途径泄露数据，对用户泄密行为进行记录、告警、阻断，并对用户行为进行审计。有效地识别敏感数据，监控敏感数据使用情况，防护敏感数据外泄。满足各种不用应用场景需求，为企业数据提供全方位的安全保护和管理。

此次数据泄露防护系统获得 ISCCC 的 IT 产品信息安全认证，说明了中国信息安全认证中心对亿赛通的数据泄露防护系统产品的高度认可以及对亿赛通数据安全产品研发的极大肯定。作为专业的数据信息安全企业，亿赛通始终将支持国家、企业和个人的信息安全保障作为自己的社会责任。未来公司将一如既往地发挥自身优势，做好中国数据安全防护专家，用扎实的技术和不断探索的精神，为保障信息化平台安全稳定地运行、共同维护数据安全贡献更多的力量。

温馨提示

中国信息安全认证中心（英文简称：ISCCC）是经中央编制委员会批准成立，依据国家有关强制性产品认证、信息安全管理的法律法规，负责实施信息安全认证的专门机构。IT 产品信息认证是依据信息技术安全性评估准则和相关技术要求，对 IT 产品的安全性进行评价，旨在保护用户信息安全，维护用户利益。生产企业的 IT 产品获得信息安全认证证书，表明该产品符合相应的标准和技术要求。

亿赛通动态 ESAFENET NEWS

荣誉 | 人工智能开启数字经济新时代，亿赛通 IT 年会实至名归再次获得年度企业奖

2018 年 3 月 22 日，由中国电子信息产业发展研究院主办，赛迪顾问股份有限公司承办的 2018 中国 IT 市场年会于北京香格里拉饭店成功召开，本次大会以“人工智能开启数字经济新时代”为主题。会议邀请了 IT 界千余著名企业精英人士参会。亿赛通作为中国数据安全防护专家一直以专业的态度、过硬的产品以及丰富的解决方案傲立于数据安全市场，连续多年获得赛迪权威报告“市场占有率第一”称号，被赛迪研究院高度关注。2018 年中国 IT 市场年会亿赛通再次荣幸受邀参会，并被授予“2017-2018 中国数据泄露 DLP 市场年度成功企业”权威奖项。

亿赛通实至名归再次拿下年度企业奖

本次中国 IT 市场年会现场，亿赛通与众多 IT 界著名企业共同探讨了人工智能行业新动态、关注 IT 潜在应用领域的发掘、IT 市场创新方向的开拓，以及 IT 产业创新环境的重塑。身为数据安全行业的领军企业，亿赛通从未停止过创新，企业不断加大产品研发力度，提升公司技术服务实力。亿赛通始终以“产品、方案、服务”三个方向为主导，坚持创新，不断探索，为广大客户提供专业的产品技术服务及丰富的解决方案，逐步构建行业领导地位。也正是亿赛通坚持不懈的探索精神、创新成果和市场的广泛赞可让亿赛通在本次中国 IT 年会上再次拿下“2017-2018 中国数据泄露 DLP 市场年度成功企业”奖项。

在人工智能井喷式发展的数字经济时代里，亿赛通也与时俱进、不断自我突破，专注于数据安全行业，为国内外企业提供最佳方案，保障企业数据资产安全。保护数据安全，亿赛通与您携手同行，并继续构筑市场占有率连续多年稳居第一的骄人战绩，继续做好中国数据安全防护专家。

全面打造金融行业深层堡垒，亿赛通出席广东金融 IT 新技术应用分析会

最新资讯

近日，由广东省粤港澳合作促进会金融专业委员会主办的“2018 年广东地区金融系统 IT 新技术应用分析会暨新春联谊”在广州召开。

信息技术的快速发展使银行对电子化的依赖不断加强，数据成为银行的重要资产之一，是现代商业银行的命脉，关乎银行的生存与发展。金融单位既要满足监管部门的合规性要求，又要对企业数据和客户资料进行安全防护，加强信息的安全性。亿赛通 15 年品牌打造，立足服务，全力为金融行业提供最佳数据泄露防护解决方案，帮助银行实现数据安全运行，保护银行数据资产安全无风险，赢得众多国内金融客户的信赖与赞可。对此，亿赛通作为中国数据安全防护专家受邀参加本次交流大会。

亿赛通全面打造金融业坚强堡垒

金融行业伴随着信息技术与互联网的广泛应用，发展速度之快。其业务开展非常依赖于信息技术和互联网，金融服务模式也由传统的柜台服务模式向网上银行、第三方支付等新型服务模式扩展，这种新的转型与发展趋势必然会带来金融数据资产泄露风险。那么，针对新的金融信息安全的出现，本次大会，亿赛通与现场的众多金融客户、IT 精英分享交流了数据安全解决方案：针对终端数据产生、存储及处理采取事先防御思路，防止主动泄密；针对使用中、外带、存储等数据进行内容方面的保护控制，确保关键控制措施。根据防护需求及目标，方案从终端、网络和数据内容三个核心层面让金融行业数据安全防护实现纵深防御的效果。

数据安全建设是一项长期任务，亿赛通作为中国数据安全防护专家，会一直坚持把数据安全这件事做到更好，为各大行业、企业、个人等做好数据资产安全的防护工作。同时，也会继续引领数据安全产业稳健前行，不断创新，迎接更多挑战，满足不同客户的需求，坚持为企业的数据安全作出自身最大贡献。

亿赛通动态 ESAFENET NEWS

3·15 维权日来了，隐私泄露问题成重点，看亿赛通如何守护隐私安全

“3·15”打假日到了

对于广大消费者而言，这至关重要

1983 年

国际消费者联盟组织确定每年的

3 月 15 日为 " 国际消费者权益日 "

其实，连续几年

315 晚会的重点都不只在打假维权

隐私泄露问题

也早已成为 315 关注的焦点

从年初的支付宝账单年度账单泄露

到雷克萨斯 4S 店泄露车主信息

之后的苹果 icloud 内部员工泄密事件

都在警示着我们隐私泄露的严重性

隐私一旦被泄露

会带来巨大的心理、精神以及经济上的巨大损失，

所以隐私被侵犯，其后果不堪设想

这些事件告诉我们

大部分的隐私泄露事件都是“内鬼”泄密造成的

他们利用职务之便，窃取用户个人信息，

从而将获取的大量隐私信息进行非法黑市交易。

亿赛通—中国数据安全防护专家

针对企业用户进行数据泄露防护

从源头守护隐私机密的安全

看到这里，担心个人隐私泄露的宝宝们开始着急了吧

亿赛通坚持 15 年“防盗”

当然除了企业之外，也要守护个人隐私的安全

所以呀

数据安全卫士来啦

TA 不仅能帮你加密私密照片、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，没有你的权限允许，谁也拿不走

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

亿赛通福利大派送

现在关注亿赛通官方微信公众号“esafenet2003”，

回复“激活码”，即可获得价值 366 元 / 年的数据安全卫士激活码，软件免费使用啦！

助考诈骗团买千万条信息诈骗考生，遇电信诈骗该怎么办？

热点话题 # 助考诈骗团卖“真题”骗财

近些年来，国内发生多起不法分子向考生发送诈骗信息谎称可以提供考试试题、考试答案、考试改分，实施电信网络诈骗犯罪的案件。某翻译考试考生一月被骗万元：据考生回忆，“起初是收到一个手机短信，说是卖翻译考试资料的，就加了对方 QQ。”当时对方表示，只要 840 元就能提供资料，转账后，对方又打来电话，要考生收取邮箱内的考试资料，但需要密码查看，同时还附有一份保密协议。此后，对方称需要交纳 4000 元保密保证金，于是考生用支付宝转账上述款项。对方继续提出要收取风险承担金，考生再次用支付宝转账 6000 元。当对方又提出索要 8000 元风险承担金时，考生才意识到上当受骗。

收购考生信息发诈骗短信

首先，电信诈骗团伙在此前已非法获取包括公民个人信息 4000 余万条。从中挑取考生的信息，诈骗团伙雇人发送短信，以出售真题信息、提供试题为由，通过短信、互联网骗取考生钱财。诈骗成功后，给团队成员每人最低 35% 的提成。也有不法分子通过网络承揽了诈骗短信的各项业务进而再购买短信群发器，向公民发送诈骗短信。

如何辨别电信诈骗

为什么会收到诈骗短信（电话）？遭遇电信诈骗都是在信息泄露的基础上，由于现今互联网高度发达，全民手机党，都在网上购物，玩游戏，或者网站注册登录等。这些任何一种情况都会导致身份信息泄露，这种情况无法避免。我们需要学会的是如何辨别这些事情的真假？

第一：通常情况下，全国重点考试国家禁止发放任何考试真题，凡是告知可以提供试题，均为诈骗。

第二：收到诈骗短信后，要注意核实对方身份，尤其是对方要求转账时，不要轻易转账。

第三：收到短信或留言需要加 qq、微信等，不要随便添加好友。

对于电信诈骗这样的骗局，一般情况相关部门都快速地作出了反应，但措施大都局限在“事后提醒”上。所以，有关单位必须要从源头消除类似事件发生，保护考生隐私信息。亿赛通作为数据安全行业的领航者，15 年来专注打造客户信息安全，既保证业务的可用性、可靠性、保密性，又对内部核心数据有较强的防御、管控能力，有效地对文件进行事前防御、事中控制、事后追踪，全面防止泄密。保护隐私信息安全，亿赛通从不懈怠，一直做好中国数据安全防护专家。

国内多家医院已中招？
亿赛通怒怼勒索病毒

焦点头条

据媒体报道，国内多家医院服务器疑似遭最新勒索病毒攻击，导致系统瘫痪，同时数据库文件被加密破坏，已严重影响医院的正常就医秩序。“医院信息系统遭受了勒索病毒攻击，导致长时间瘫痪。”某儿童医院相关负责人说。

连医院信息系统也中招了！面对性质如此恶劣的网络安全事件，难免会引起不少单位对网络安全方面的恐慌。针对近期有爆发趋势的勒索病毒事件，亿赛通扛起行业责任，怒怼勒索病毒！

领先技术，怒怼勒索病毒

本次事件的爆发，究其根源面对的对象是数据文件，勒索软件可以无任何顾虑的光顾你的电脑，对数据文件进行加密，加密后随之勒索解密。谈起数据加密，亿赛通十几年都用其对客户的数据进行安全防护，而今，面对反其道的攻击事件，亿赛通决定重拳出击此类恶意勒索软件，通过自主研发的驱动数据防护核心技术，将数据实体与访问应用进行智能隔离和验证，屏蔽勒索软件读取终端上存储的数据，让勒索软件无论如何变种，都无法接触到用户数据，从而无法加密用户数据，使勒索行为化为泡影。相比其他保护方式，用户无需系统补丁，无需病毒库样本支持，与传统亿赛通电子文档安全产品一样，终端用户无需改变任何工作习惯，真正的从源头上保护用户的数据安全。另外针对没有加密保护需求的用户，此功能也可以对明文文件进行安全保护。

中国数据安全防护专家—亿赛通助力数据所有者实现信息资产的安全，拥有数据安全行业领先技术和丰富的解决方案。帮助众多企业打造全方位、立体化、多层次的企业数据安全防护体系，有效的防护企业核心数据资产，保障企业竞争力，都到各大行业和企业的拥护和信任。

随着信息技术的快速发展和演进，数据安全行业不断诞生新的发展趋势和新的问题。亿赛通智能安全产品，融合大数据分析、文档加密、访问控制、关联分析、数据标识等技术，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，从而做到事前预防、事中控制、事后审计于一体化防护，可效防止重要信息被有意或无意非法扩散。

Facebook数据泄露持续发酵，现已到生死关头？

近日，当全国人民都沉浸在春天的温暖天气中，讨论去哪儿出游时，Facebook 让吃瓜群众们放下了计划，开始舔屏。到底是怎么回事呢，且看小编给你具体分析。

事件回顾

事件的起始要追溯到 2014 年，27 万 Facebook 用户下载了平台上一款个性分析测试的应用软件 (App)，该软件的开发者透过这 27 万用户通过滚雪球的方式获得了 5000 万脸书用户的隐私信息并将资料私自卖给了某数据分析公司。这家数据分析公司充分利用获取的用户资料建立分析模型，精确推送信息甚至是假信息，从而影响用户的选择。

事件是如何发生的呢？

事件目前还在持续发酵中，广大网友们都在意的是数据分析公司对 Facebook 造成了巨大的伤害，但是小编想说的是，Facebook 的用户数据泄露才是这次事件的起因，Facebook 的用户遍布全球，人数超过 20 亿，但是用户资料却没有进行严密的防护，给不法分子留下了一个可乘之机。

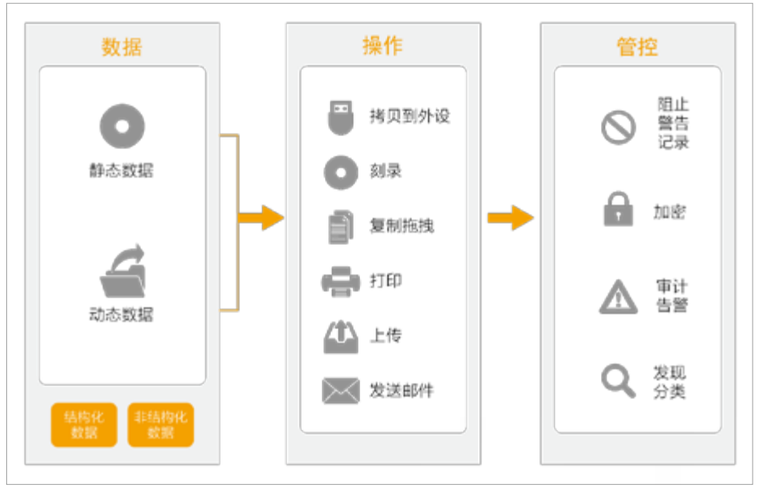
此次事件也是给各位 Boss 们敲响了警钟，数据资产是一个企业的命脉，可当下各种数据的泄露事件频繁发生，且越演越烈，对各大行业造成不可损失的后果。对于数据泄露问题，亿赛通具有成熟的数据泄露防护产品，各种需求的数据安全系统，提高企业的工作效率，降低成本，保护数据资产，降低风险损失，消除用户安全隐患，有效的防止核心数据资产的外泄。亿赛通作为国内专业的数据安全行业领军企业，15 年来一直以保护国家、企业的数据安全为己任，坚持做好中国数据安全防护专家。

重磅｜春暖花开 亿赛通党政机关领域又一经典案例诞生

客户简介

徐州市国土资源局，为市政府主管全市国土资源管理秩序的责任，组织指导全市国土资源行政执法工作，依法查处国土资源违法案件的工作部门。承担规范国土资源管理秩序、优化配置国土资源的责任。负责规范国土资源权属管理、矿产资源开发以及管理地质勘查行业和矿产资源储量，是国家级行政机关。

典型案例 TYPICAL CASES



需求背景

随着国土资源局大力推进信息化建设，作为国家行政机关，数据安全早已成为国土资源局的重点防护对象。为了加强国土资源局的信息化重建，保证业务系统的存储及使用安全，防范数据泄露风险，部署一套完善的数据安全防护体系对国土资源局来说迫在眉睫。

经过多家方案技术对比，几个月的实施测试，亿赛通在众多数据安全厂商中脱颖而出，以完善的解决方案、丰富的市场经验、一流的售后服务，通过国土资源局的甄选，为其数据安全体系保驾护航。

解决方案

亿赛通数据泄露防护（DLP）系统是一款基于内容识别技术的保护系统。

1、终端防护：防止敏感数据通过打印、刻录、聊天工具、发送邮件等终端方式泄露出去。

2、网络防护：防止敏感数据通过邮件、网盘、微博、FTP、论坛等网络方式泄露出去。

3、数据扫描：通过扫描和分类的方式，随时随地发现企业敏感数据分布，并保护静态数据。

4、邮件防护：防止敏感数据未经任何检查通过企业邮箱泄露出去。

5、数据分析：基于规则和中文语义的智能数据分析，对数据进行高效敏感检查。

6、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。

项目成果

亿赛通为徐州市国土资源局提供了完善的数据泄露防护系统解决方案 ,有效地保障了各个环节数据的安全运行，避免了敏感数据遭窃的风险 ,提高数据安全的智能化管理，为徐州市国土资源局打造了一个良好的信息安全办公环境。

亿赛通作为中国数据安全防护专家，15 年来一直引领数据安全领域，接下来也会继续肩负着“保护数据所有者的信息资产安全”使命，把数据安全这件事做到更好！

亿赛通签约上海德邦物流服务有限公司

客户简介

上海德邦物流有限公司是一家具有较大规模的专业从事物流服务的专业公司。专营上海至全国各地往返货物运输、货物代理、货物配载、货物配送、仓储等物流业务。逐步形成以公路为主，铁路为辐线的快速运输体系，服务范围覆盖全国各大中小城市。立足上海，覆盖全国，运力雄厚，管理严谨。把服务质量意识，深入到公司的每个落，确保高质量完成每一次运输任务。

典型案例 TYPICAL CASES

需求背景

近些年物流行业大量的消费者私人信息泄密事件频繁发生，一旦有快递企业的用户信息泄露事件的发生，不仅会给公司带来严重的名誉损害，同时也会给整个社会带来更大经济损失。所以信息安全、数据安全已经悄然发展成为物流快递企业必须高度重视，急需解决的首要问题。有的是一些别有用心的不法分子看中其“内在价值”，非法盗用、转卖消费者个人信息谋取私利；有的是个别快递公司无视行业准则，违规泄露客户信息，自动卷入灰色利益链条之中；还有的是消费者个人安全意识不强，给不法分子可乘之机。凡此种种，都提醒我们保障快递信息安全刻不容缓。快递企业应该加强行业自律，加强对内部员工职业道德教育和规范化操作管理，完善保密制度，提升业务管理规范性，以确保物流快递的用户信息安全。

解决方案

1、智能透明加密：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；

2、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。

3、安全水印支持：通过自动添加安全警示及版权标识信息，来降低屏幕录制和自主打印所带来的泄密风险。

4、身份认证集成：支持与基于 Ldap 和 OpenLdap 协议的统一身份认证平台（如 AD、ED、TDS 等）进行无缝集成，如实现组织架构及用户账号信息的自动完整同步和单点登录认证集成等。

5、离线办公支持：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。

6、安全水印支持：通过自动添加安全警示及版权标识信息，来降低屏幕录制和自主打印所带来的泄密风险。

项目成果

截止 2015 年 11 月德邦物流 5600 多个分支机构均已全部投入亿赛通 DLP 数据防泄露体系，数据安全无论是内部办公、网络办公、移动办公均实现了文档安全统一管控，可分类、分级、分权使用文档，防止用户信息外泄，这份安心值得我们信赖。先后北京亚太物流中心、近铁国家物流、深圳年富供应链等等多家物流快递公司，纷纷也都牵手亿赛通，实现对企业敏感数据安全审计，对终端和网络数据进行完整监控，根据安全需求进行加密、阻断、告警与审计，建立了全方位信息安全管理机制，从而保证了物流快递企业的用户信息安全 这不仅是对物流快递企业的一份保障，也是对我们个人用户一份安心快递的选择。