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

8 月刊

2019 年共 11 期


央采中标 | 亿赛通全线产品再次入围中央政府采购平台

亿赛通签约中国航发沈阳发动机设计研究所

听说你被北大录取了？



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 《亿赛通八月刊》推陈出新，独家分享第一手国内安全快讯

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 央采中标 | 亿赛通全线产品再次入围中央政府采购平台

亿赛通小贴士 ESAFENET PROMPT

18/19 美国银行数据泄露影响上亿人，金融数据急需科技手段安全防护

20/21 起底倒卖明星信息产业链，50 元就能“偶遇”你的爱豆

22/23 听说你被北大录取了？

24-27 科技公司安全事件盘点，亿赛通硬核数据安全解决方案来袭 ~

典型案例 TYPICAL CASES

28/29 东软医疗携手亿赛通将数据安全防护进行到底

30/31 中国航发沈阳发动机设计研究所

# 《亿赛通八月刊》推陈出新，独家分享第一手国内安全快讯

刊首语 PREFACE

虽说立秋已过，但今年盛夏酷暑的滋味，滚烫的感觉却刻骨铭心，似乎盛夏的余威还迟迟不退却。 在这秋老虎盛行的季节，我司隆重推出《亿赛通八月刊》，独家分享第一手国内安全快讯。

随着网络信息技术的持续演进，互联网对整个经济社会发展的渗透、驱动作用越来越明显，带来的风险挑战也在不断扩大。网络安全威胁和风险日益增多，电信网络诈骗等各类违法犯罪活动时有发生，数据安全和侵犯个人隐私问题日益凸显。习近平总书记曾发表重要演讲： 要深入开展网络安全知识技能宣传普及，提高广大人民群众网络安全意识和防护技能。扬起网络安全和信息化的风帆不仅增强人民对美好生活向往的满意度，而且促进经济平衡充分地发展，提升国家治理体系和治理能力现代化水平，促进创新型国家建设。而网络安全接下来又将如何布局？国内安全厂商如何砥砺前行？我们共同期待……

国内

## 1、30 亿条信息泄露，96 家互联网公司遭殃，案子破了！




摘要：“仙人 JUMP”发了一篇文章《连百度都在劝猎头们善良》，说“社会我百度一出手，彻底教猎头如何做人”，其中提到了近期的一起特大侵犯公民信息团伙的案件，在这起案件中，百度公司员工接到竞品公司的猎头骚扰电话，怀疑个人信息遭到泄露，经由公司相关部门携线索向广东警方报案，广东省公安厅组织广州警方侦破了这起案件，抓获犯罪嫌疑人 130 余人，查获公民信息 2 亿余条。

## 2、人大常委会委员：要避免 App 强制收集个人信息

摘要：近日，北京市朝阳区人民法院审理了一起“智联招聘”员工参与倒卖个人信息案。该案涉及公民个人信息达 16 万余份，一份信息被卖 5 元左右。无业人员郑某为了获得公民简历信息，伪造企业营业执照并提供给简称智联招聘工作人员卢某和王某，获得企业会员账号，获取大量公民简历，然后在淘宝上销售。





## 3、工信部：落实网络安全法，强化基础设施保护和数据安全管理




摘要：工信部网络安全管理局副局长杨宇燕表示，当前，随着工业互联网、5G 网络、人工智能等技术不断地发展和大规模的应用，网络安全问题出现了许多新的特点及新的变化，网络安全威胁和风险日益突出。网络安全已经扩展到物理空间，安全边界发生巨大的变化。为此，工信部将从四个方面体系化推进网络安全各项工作：一是完善政策法规；二是健全安全监管机制；三是强化网络安全技术保障；四是推进网络安全产业的发展。

## 4、5G 商用提速 网络安全市场规模将达千亿



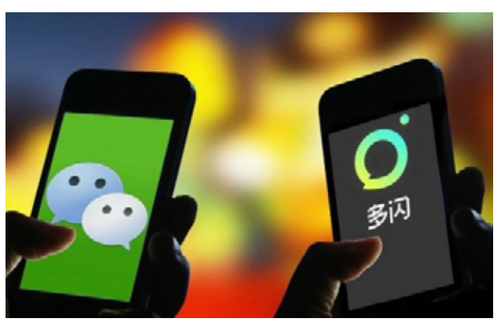

摘要：中国网络安全产业的年复合增长率将超过 25%，到 2021 年市场规模将超过 1000 亿。而随着大数据和人工智能时代的到来，网络安全行业已经成为一个巨大的风口。

## 5、快递企业泄露个人信息或将被列入信用“黑名单”




摘要：中国国家发改委披露的一份文件显示： 未来，如果经营快递业务的企业出现违法收集、使用个人信息；未经被收集人同意，向他人提供个人信息等行为，将有可能被列入信用“黑名单”。中国国家发改委发布了其会同有关部门研究起草了《关于加强和规范运输物流行业失信联合惩戒对象名单管理工作的实施意见（征求意见稿）》，向社会公开征求意见。

## 6、多闪回应窃取通讯录事件：近半投诉者是某公司员工或家属

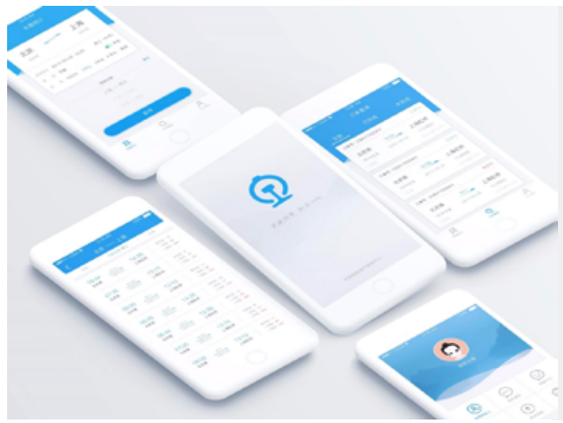



摘要：多闪官方公众号发文说明此前“多闪用户”批量投诉多闪窃取用户通讯录事件疑似为虚假投诉，其中大多数投诉者疑似根本没有注册过多闪，而其中近半投诉的“多闪用户”则是著名互联网公司员工或员工家属。文章称，2019 年 3 月 29 日，多闪收到一起有关部门转来的深圳用户集体投诉案件。14 名深圳“多闪用户”称，在多闪的“可能认识的人”栏目中，系统推荐的一些用户，与微信好友头像、昵称一致，故用户怀疑“多闪”窃取了用户微信通讯录及手机通讯录。





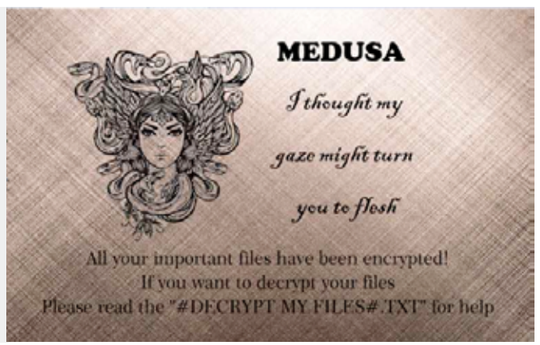
## 7、不同意获取个人信息就“闪退”，网友吐槽 12306 App



摘要：据报道，近日有不少网友吐槽铁路官方 APP“铁路 12306”，称不同意获取个人信息就“闪退”。报道称，最新版本的 12306 App 在首次启动时会显示一个页面，称在使用 12306 时，可能会获取部分必要的个人信息，以提供相关基本服务。这些个人信息包括：定位信息、使用相机、相册和推送权限这 4 项。

## 8、进口勒索“美杜莎” 作祟，盯上国内政企用户

摘要：通过威胁情报关联，本次捕获的 Medusa Ransom 最早于 2018 年 10 月就被编译，但相关的攻击活动却很少，仅在 2018 年 11月国外论坛上出现过一例被勒索的求助信息。直至近日，再次在国内某安全论坛上发现一例该勒索病毒的求助，由此推测，该勒索病毒的运营者很可能将目标转向了中国用户。



## 9、国家网信办发布《儿童个人信息网络保护规定》




摘要：国家互联网信息办公室 23 日发布《儿童个人信息网络保护规定》。规定自 2019 年 10 月 1 日起施行，并明确任何组织和个人不得制作、发布、传播侵害儿童个人信息安全的信息。规定指出，网络运营者应当设置专门的儿童个人信息保护规则和用户协议，并指定专人负责儿童个人信息保护。

## 10、雪球回应“12 万人数据被泄露”：该网传图片为不实信息


针对网传不实信息的声明

雪球已经关注到，今日上午有用户根据来经证实的网传图片，在某平台发帖称雪球数据可能被泄露，并引发部分转发和疑问。对此，雪球严正声明如下：

1、该网传图片为不实信息：（1）雪球不会以任何方式获取和存储用户的股票账户、交易密码、交易记录和持仓数据；（2）雪球采用符合互联网行业主流安全标准的加密算法存储用户的雪球账号密码，不会以明文形式进行存储。

2、雪球非常重视用户隐私，视用户信息安全为生命底线，不断提升技术能力以防范信息泄露，更不允许任何人以任何形式危害雪球用户的信息安全。

变售和贩卖公民个人信息涉嫌违法犯罪，需要承担法律责任，雪球已经就此启动了紧急调查程序，并正在向公安机关进行报案。

最后，雪球呼吁大家不要轻信谣言和传播谣言。

雪球团队

2019 年 8 月 21 日

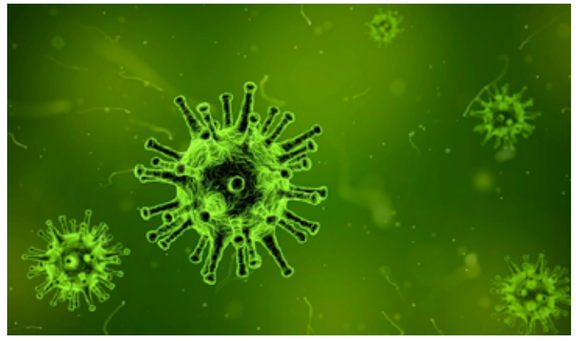
摘要：雪球网数据泄露，涉及 12 万人的数据只卖 75 美元，包含姓名，身份证，手机，账号 / 邮箱，密码，持股前 3 支，持股数，交易风格。针对该消息，雪球发布声明称，雪球不会以任何方式获取和存储用户的股票账户、交易密码、交易记录和持仓数据。此外，公告称雪球采用符合互联网行业主流安全标准的加密算法存储用户的雪球账号密码，不会以明文形式进行存储。





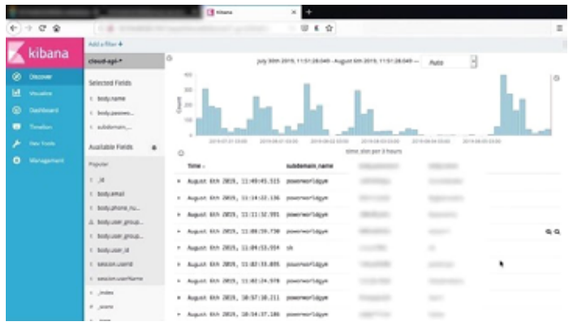
国外

## 1、尴尬了，卡巴斯基反病毒软件存在漏洞允许在线跟踪用户



摘要：美国时间 8 月 15 日，据外媒 the Hacker News 报道，研究人员在卡巴斯基反病毒软件中发现了一个漏洞，该漏洞允许访问过的网站和商业第三方服务在线跟踪用户。这个漏洞为 CVE-2019-8286，存在于卡巴斯基反病毒软件的名为“ Kaspersky URL Advisor”的 URL 扫描模块中。该漏洞暴露了过去 4 年用户访问过的每个网站的关联唯一标识符，该标识符的暴露允许访问过的网站和商业第三方服务在线跟踪用户。

## 2、Suprema Biostar2 安全漏洞导致 100 万人指纹数据曝光！




摘要：近年来发生的多起大规模信息泄露事件，使得网络用户不得不修改那些不再安全的账户密码。但若安全性更高的指纹数据被曝光，那后果就更加严重了。遗憾的是，这正是 SupremaBiostar2 指纹锁身上所发生的事情。据悉，研究人员在 Suprema 的系统中发现了一个安全漏洞，使之能够访问超过 100 万人的身份验证数据。英国指出，这些数据包括了指纹 / 面部识别数据、未加密的用户名和密码、甚至员工的个人信息。

## 3、英国国家医疗服务的 IT 支出因“WannaCry”攻击而增加 1.51 亿英镑

摘要：据外媒报道，自 2017 年 5 月“WannaCry”袭击以来，英国英国国家医疗服务体系（NHS）在 IT 方面的支出总计增加了 1.51 亿英镑。“WannaCry”勒索软件攻击的目标主要是未修复补丁的 Windows XP 电脑，感染并加密了约 20 万台电脑，其中包括英国各地的 NHS 信托机构，这些机构面临着 7300 万英镑的 IT 账单，以及约 1900 万英镑的病人服务损失。2017 年 5 月“WannaCry”勒索软件攻击后，NHS 的 IT 支出大幅增加，2018/19 财年 65 家 NHS 信托机构支出约 6 亿英镑；2017/18 财年约为 5 亿英镑，2016/17 财年约为 4.6 亿英镑。

## 4、媒大量智能家居数据泄露，技术能力成竞争重点




摘要：据福布斯报道，由 Noam Rotem 和 Ran Locar 领导的网络安全研究团队最近测试了几家智能家居企业的安全能力，发现了一家名为 Orvibo 的智能家居系统发生严重隐私泄漏问题，该数据库无任何密码保护，运行在物联网（IoT）管理平台。大量数据库公开暴露并循环使用，包含了从用户密码到账户重置代码，甚至包含“智能”摄像头记录会话，该智能家居系统的漏洞很多，很多基本的安全措施缺失，更谈不上安全意识和架构。





## 5、国外人气主播账号被黑



摘要： Michael “Shroud” Grzesiek 是国外直播平台 Twitch 上一名《绝地求生》、《Apex 英雄》大主播。最近他的 Twitter 账号被黑，登陆他账号的人威胁要发他和他女友的裸照。据外媒报道，Shroud 的账号在当地时间周一早上被黑，发了很多链接到其他 twitter 账号的推文，威胁发裸照，同时还发布了针对其他 Twitch 大主播的仇恨性言论。

## 6、知名约会软件 3Fun 泄露大量用户隐私和地理定位



摘要：近期，为“好奇和单身人士”服务的 3Fun 手机约会应用被曝出发生了会员数据数据泄露事件，涉及用户隐私和地理定位。3Fun 声称在全球拥有超过 150 万会员。每天会产生超过 18 万条交流信息。有安全研究人员发现，这款约会应用存在几个严重的安全漏洞，导致用户的实时位置和其他敏感数据被泄露。具体数据包括出生日期、性偏好、聊天信息和私人照片。此外，信息泄漏和用户设置无关，即使用户正确地启用了隐私设置，个人数据也会被泄漏。

## 7、新的 Saefko 木马程序窃取您的信用卡、加密钱包

摘要： 在黑暗网络上出售的新木马附带了大量工具来窃取银行详细信息，在线游戏凭证和加密货币钱包。 有研究人员表示，这种名为 Saefko 的新木马是用 .NET 编写的，并且配备了各种功能，使其成为威胁领域的一个危险的新增功能。远程访问特洛伊木马（RAT）通过各种方式渗透系统，包括带有恶意附件的网络钓鱼电子邮件，偷渡式下载，有时作为来自不可靠来源的捆绑软件程序的一部分。

## 8、新西兰航空网络钓鱼攻击中暴露的客户信息




摘要：新西兰航空公司向注册其 Airpoints 忠诚度计划的客户发送电子邮件，警告他们网络钓鱼攻击成功破坏了两名员工的电子邮件帐户，这可能导致攻击者访问个人信息。根据其网站，新西兰航空公司每年运送大约 1700 万乘客到全球 51 个目的地。该航空公司的 Airpoints 计划允许奥塔哥每日时报报道的登记客户约为 200 万美元，用于支付他们通过“航班，Airpoints 商店赠送的礼品以及一系列其他优惠”所获得的 Airpoints Dollars。





## 9、BEC 诈骗者欺骗员工进入客户信息




摘要：企业电子邮件泄密（BEC）诈骗者现在使用新的间接攻击方法瞄准公司的客户，该方法旨在通过询问收集人员的老龄报告来收集有关未来骗局目标的信息。老龄报告（也称为应收账款计划）是一组未完成的发票，允许公司的财务部门跟踪尚未支付服务的客户或允许他们通过信贷购买的商品。

## 10、Fraudster 解锁超过 200 万台 AT ＆ T 手机，支付 100 万美元




摘要：数百万手机被 AT ＆ T 内部人员非法解锁，他们收受数十万美元的贿赂，还在公司内部网络上种植未经授权的工具和设备。在 2012 年至 2017 年之间的五年间，巴基斯坦 34 岁的穆罕默德·法赫德（Muhammad Fahd）在博塞尔（Bothell）的客户服务中心招募了年轻的 AT ＆ T 员工，以取消该公司对解锁手机的保护。专有锁定软件可防止设备与其他网络一起使用，从而使其与全球的移动运营商兼容。法赫德将为锁定在 AT ＆ T 的手机提供国际移动设备身份（IMEI）号码，腐败的员工将禁用该保护。根据司法部的说法，这项活动导致移动运营商　因其服务或支付计划中的设备损失了数百万美元。据称，其中一名同谋通过为期五年的非法协议获得了 428,500 美元。

## 11、当 Skype 翻译器功能处于活动状态时，微软承包商可以获知对话内容




摘要：据外界报道，微软承包商正在收听使用 Skype 翻译功能的用户之间对话。只有当用户在 Skype 中执行翻译功能时，而不是在任何其他典型的 Skype 语音或视频呼叫期间，微软承包商才能执行此操作。收集的信息包括有关夫妻之间亲密对话的 Skype 音频等。

## 12、Twitter 可能未经用户同意与广告合作伙伴共享用户数据




摘要：Twitter 表示最近在其广告平台上发现并修复了一个问题，导致该公司未经用户明确同意而与广告合作伙伴共享一些用户数据。受影响的用户仅包括为移动应用程序点击或查看广告并稍后与该移动应用程序进行交互的用户。暴露数据是从 2018 年 5 月到 2019 年 8 月 5 日，当时它发现并修复了这个漏洞。该漏洞导致共享一些用户数据 - 例如国家 / 地区代码，设备类型和广告详情 - 与 Twitter 用于广告跟踪和衡量目的的广告客户列表。Twitter 分享了其公开的用户广告数据的完整列表，以及可能已收到该信息的广告合作伙伴列表，但它没有透露在其平台上宣传并触发该错误的移动应用的名称。



行业聚焦 INDUSTRY FOCUS

## 13、美国路易斯安那州宣布进入紧急状态多个学区遭到网络攻击




摘要： 近年来美国地方政府不断受到勒索软件和网络攻击的威胁。继 2018 年 2 月受到 SamSam 勒索软件攻击，导致科罗拉多州交通局被迫关闭运营之后，最近路易斯安那州州长乔恩·贝尔·爱德华兹宣布该州的多个学区遭受了严重的网络攻击。这些袭击事件摧毁了 IT 网络并加密了文件，使其无法访问，目前该地区已经启动了紧急预案，在联邦执法部门提供的帮相下，路易斯安那国民警卫队报告称已派出一个网络团队帮助恢复当地系统并安装防火墙。

## 14、加密货币借贷平台 YouHodler 泄露 8600 万条数据




摘要：据外媒报道，加密货币借贷平台 YouHodler 被爆出数据库漏洞，8600 多万条用户数据记录泄露。泄露数据包括用户姓名、出生日期、电子邮件地址、住址、电话号码、护照号码、信用卡号码及到期日、CVV 验证码、银行详细信息和加密钱包地址等。

# 央采中标 | 亿赛通全线产品再次入围中央政府采购平台




2019 年 8 月 21 日，央采官方公告发布，北京亿赛通科技发展有限责任公司再次入围中央国家机关 2019 年软件协议供货采购项目第十八包：安全软件 - 数据防泄露 DLP 软件和第二十七包：安全软件 - 文件加解密软件两大项。

此次亿赛通全线产品再次顺利入围，“才貌双全”的亿赛通数据安全产品在大家夜以继日的准备下，精诚所至，金石为开。2019 年 8 月，喜讯终于传来：

中央国家机关政府采购中心公布了“中央国家机关 2019 年软件协议供货采购项目”中标公告，亿赛通数据防泄露系统 V5.0 及亿赛通电子文档安全系统 V5.0 双项产品成功中标！





**第十八包：安全软件-数据防泄漏DLP软件**

中标产品：

亿赛通V5.0

**第二十七包：安全软件-文件加解密软件**

中标产品：

V5.0(GP17)

中央政府采购协议供货项目是我国目前高级别的政府采购项目，采购单位覆盖中央直属近万个机关单位，是中国政府采购领域级别高、覆盖面广的采购项目之一。

中央垂直单位会对所有供应商进行一次严格的筛选，最终为地方政府提供一个明确的产品采购方向标。

同时，在伴随着中央政府对于本土化自主研发产品的采购需求逐步加大，国产化要求越来越高，数据安全产品也被赋予了越来越多的职责。构建以数据为中心的新安全防护体系，不仅是数据安全技术的发展方向，也是我国安全界从领导到专家的普遍共识，其基础和核心地位愈加凸显。本次对外公布的招标内容中，数据安全相关项目备受瞩目。数据安全在近些年进入发展快车道，落地项目呈逐年增加的态势。从本次央采公布结果，可以看出国家对数据安全的大力扶持。相信在政府的领导下、企业的支持下，数据安全行业潜力愈发巨大。

本次入围央采，亿赛通数据泄露防护系统及电子文档安全管理系统已经站稳了数据安全系列产品的 C 位。此次能在众多数据安全厂商中脱颖而出，再次获得国家机关及政府行业的青睐，也是对亿赛通数据安全产品的先进性与成熟度的认可与肯定，充分体现了我司的产品研发力和市场竞争力。两项系统将政企的各个业务系统节点安全防护，保障政企业务活动的大动脉，实现关键节点安全对接。

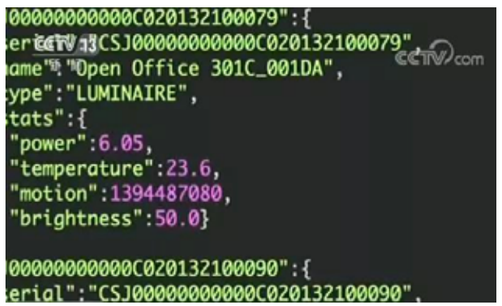
在群雄割据、竞争激烈的数据安全产品市场中，亿赛通作为连续 16 年专注于数据安全市场服务商，一哥地位毋庸置疑。未来，亿赛通的安全产品将持续深耕优化，巩固市场优势，为更多的政企提供优质的产品和服务。

# 美国银行数据泄露影响上亿人，金融数据急需科技手段安全防护

美国第七大商业银行“第一资本”宣布，大约一亿美国人和 600 万加拿大人的个人信息遭一名“黑客”窃取，目前，犯罪嫌疑人已经被逮捕。




根据一份联邦刑事起诉书，黑客名叫 Paige Thompson。Thompson 曾是亚马逊公司云计算部门 Amazon Web Services 的员工。她被控突破“第一资本”的防火墙，访问该银行存储在亚马逊云服务上的客户数据。西雅图联邦检察官称，数据盗窃发生在 3 月 12 日至 7 月 17 日之间。




17 日，一名“源码托管服务公司”的用户看到有人通过网站发布“第一资本”银行客户的个人信息，随后提醒银行可能遭到了黑客入侵。随后，“第一资本”发表声明，证实在 19 日发现系统基础架构的“配置漏洞”，导致大约一亿美国用户的信息在今年 3 月 12 日到 7 月 17 日期间被黑客窃取——其中大部分失窃数据是个人和小企业用户从 2005 年到今年初申请信用卡时所提供的信息，包括：姓名、地址、电话号码、出生日期，以及个人收入等。




如果犯罪分子利用被窃取的信息、以信用最佳客户或富有人群的名字申请信贷，那么“第一资本”被攻击事件的后果可能是灾难性的。

“第一资本”强调说，黑客并没有获得用户的信用卡账号和登录密码，但有大约 14 万美国人的社会安全号码以及与之关联的八万个银行储蓄卡账号被盗；另外还有大约 100 万加拿大人的社会保险号外泄。

“第一资本”董事长兼首席执行官费尔班克发表声明，对个人信息遭窃取的用户表示道歉，并承诺将“纠正错误”。

“第一资本”的总部位于美国弗吉尼亚州，目前的资产估值为 3736 亿美元。此次数据外泄可能让这家银行今年的经营成本增加 1 亿至 1.5 亿美元，用于赔偿受影响的用户。

这不是美国消费者第一次出现数据遭窃。之前，另一起波及上亿人的征信机构信息泄露事件，刚刚落定处罚和赔偿细节。








信贷报告公司伊奎法克斯公司（Equifax）在 2017 年数据遭窃，受影响人数多达 1.45 亿。该公司刚刚同意支付至少 7 亿美元（约合人民币 48 亿元）了结与此相关的多起诉讼；其中，至多 4.25 亿美元（约合人民币 29.2 亿元）将直接用于补偿消费者。

数据安全形势日益严峻，造成的损失也越来越多，企业也应当更加重视数据安全保护。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。

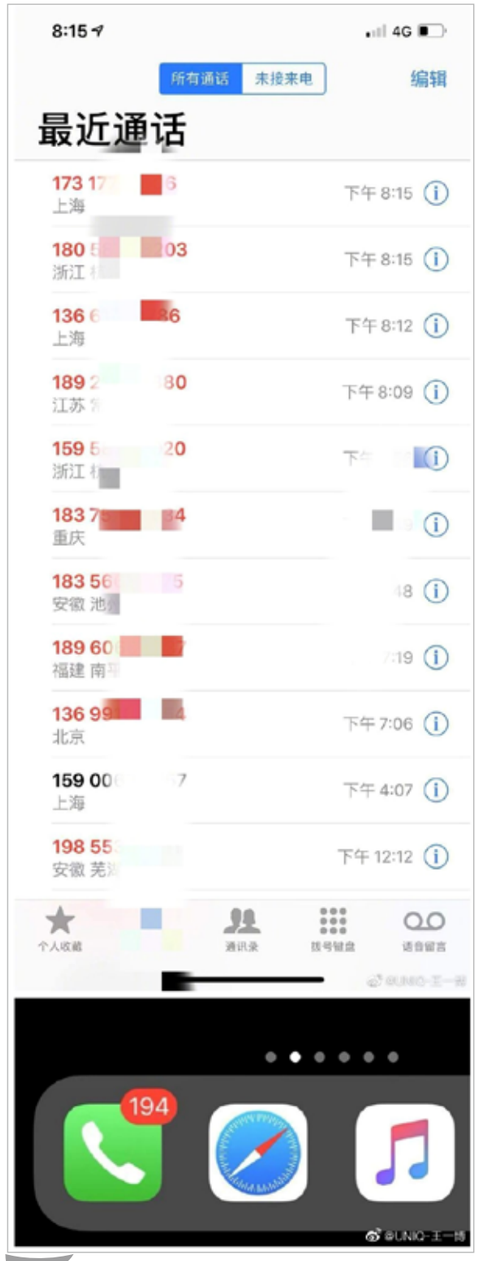
亿赛通根据银行的数据安全风险隐患并结合上级监管部门对银行的信息安全建设要求，提供全面的数据安全解决方案，相信如果从以上几点出发，从内部到边界所有敏感数据进行加密监管，不法份子也不会轻而易举的谋取暴利，危害社会危害他人。

## 典型案例

1、招商银行
2、中国建设银行
3、中信银行 / 证券股份有限公司
4、中国民生银行
5、上海浦东发展银行股份有限公司
6、九江银行股份有限公司
7、中国国际金融股份有限公司
8、中国人民人行清算总中心
9、华夏基金管理有限公司
10、广发证券股份有限公司
11、中国人民财产保险股份有限公司
12、泰康资产管理有限责任公司
13、新华人寿保险股份有限公司
……

文章资讯来源于央视网

# 起底倒卖明星信息产业链，50 元就能“偶遇”你的爱豆




娱乐圈中向来有“私生粉”一说，指的是对偶像私生活过度关心、喜欢跟踪偶像的粉丝。不仅偶像本人生活中会受到骚扰，这种需求还催生了明星个人信息黑产业链的出现。

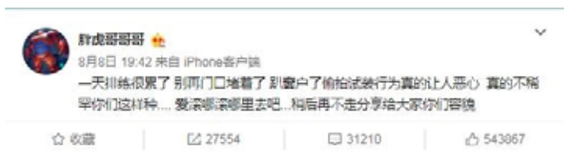
近日，演员王一博发微博称自己电话号码被泄露，遭到粉丝疯狂骚扰，并贴出电话来电记录。

实际上，王一博的遭遇并不是个案。搜索一下即可发现，明星的各种个人信息在微博、微信、闲鱼等渠道被明码标价公开售卖，这些信息价格低廉，从几块钱到 100 元不等，500 元能够打包购买上百位明星的信息。

从航班、酒店、通告到游戏账号、手机号、身份证号乃至户籍，这些明星的个人信息都能被买到。在一位卖家的标价中，吴亦凡的户籍信息只需要 50 元。

还有资深追星族表示，明星信息的买卖在粉丝圈内早已是公开的秘密，如果想去给明星接送机，就可以去买他的航班号或者身份证号进行查询。不少粉丝还会购买酒店信息前去蹲守，制造“偶遇”。

当红偶像易烊千玺助理近日在微博公开怒斥“私生”：一天排练很累了，别再门口堵着了，趴窗户了，偷拍试装行为真的让人恶心，真的不稀罕你们这样种 .... 意指易烊千玺被私生蹲守并偷拍换装。








## 深入思考

### 问题 1：粉丝为何购买 / 用途为何

- 粉丝猎奇心理（即个别“私生饭”的恶趣味）
- 掌握明星的行程，更方便追踪前线消息、接送机等
- 购买与偶像邻座的机票、高铁票
- 入住偶像下榻的酒店
- 少数激进粉丝会拨打偶像电话、蹲守偶像住处等

### 问题 2：倒卖背后的根源

畸形的追星文化：偶像的意义在于通过其作品所形成的艺术人格来引领某种积极的品质或潮流。偶像通过粉丝的实际支持获得更大的创作动力，粉丝通过偶像的艺术作品获得更多的精神共鸣，这本应是一种积极的共生关系。但“私生粉”的追星行为打破了这种默契，干扰了艺人的正常生活，也破坏了社会的正常秩序。

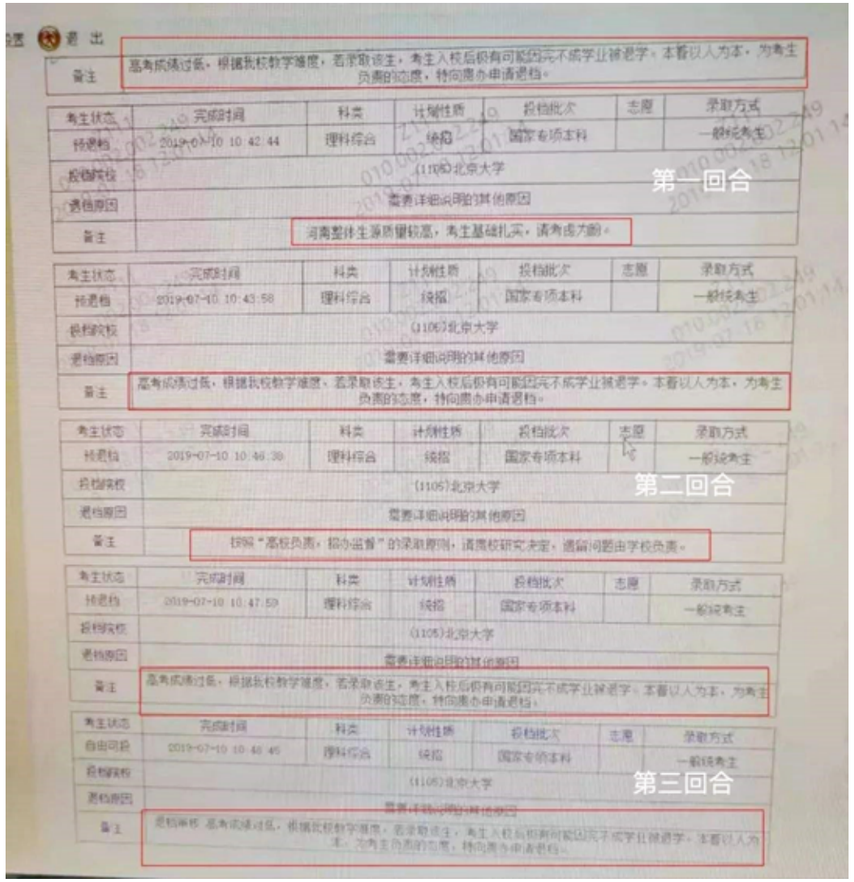
流出渠道管控不严：户籍信息、航班、手机号等明星个人信息本不该曝光于公众之下，但其背后所对应的管理机构，如户籍部门、航空公司、电信公司，均难逃其咎。个别工作人员利用职务之便，通过倒卖明星信息来牟取暴利，暴露了这些人员职业道德的缺失和单位信息管理的疏漏。

在王一博号码被泄露及易烊千玺被私生蹲守事件中，网上以负面情绪为主。不管是明星还是普通百姓，信息泄露都是困扰众人的一大烦恼。伴随信息泄露而来的是，各种垃圾电话、垃圾短信轰炸及个人财产安全隐患。如何保护个人信息安全是生活在互联网时代大家共同面临的问题。




有安全专家提出，新技术不断发展的同时，安全威胁也随之而来：信息系统并不是独立运营的，信息与各相关单位均联网共享，存在被黑客入侵、网络攻击的风险；单位员工共用账号的现象也非常严重，对内部工作人员的管理不够严谨，导致“内鬼”有机可乘。要避免个人的关键数据及隐私信息被黑客、内部人员所窃取，除了必须要加强员工的安全意识之外，还需要通过技术手段提高身份认证的安全性，并做到安全追溯、责任到人。亿赛通始终站在您的背后，成为守护信息安全的坚实臂膀，努力建设和谐的信息安全环境。

# 听说你被北大录取了？




此前，北京大学三次退档河南省考生事件引发网友热议，该考生考了 536 分，虽说稳过一本线，但考不到 680 分以上，进不了北京大学。幸运的是，他报考了提前批录取的“国家专项计划”，第一志愿为北大，而且在河南省 8 个招生名额中，恰好排第八。因为满足专项计划的招生要求，所以这名考生被顺利投档，也就是俗称的“捡漏”。但是北大“拒绝捡漏”，三次退档该河南考生。此举激发众怒，事件曝光后舆情迅速发酵，大家为这个已经准备回去复读的寒门学子鸣不平。

但是近日，一则“河南籍考生北大退档流程图”在微博上疯传。








河南省招生办发布消息，经与北京大学招生办公室协商沟通，两名国家专项计划退档的河南考生补录工作完成。消息同时称，针对网络流传的考生退档过程信息，省招办通过网传“退档流程图”IP 锁定该信息来自某县招办工作用机。系县招办工作人员疏忽大意，考生退档过程信息被他人擅自拍照并上网传播。为此，省招办约谈并致函该县有关部门，要求进一步调查核实情况并依规依纪进行处理。

此事简直是峰回路转，同时也有网民质疑，为什么本应该是系统内部消息的提档退档记录，会被截图，并且还流传到网上？因为工作疏忽导致应当保密的工作流程信息泄露的工作人员应当承担什么处罚？

根据我国教育部在 2014 年公开的《普通高等学校招生违规行为处理暂行办法》第十条规定：招生工作人员存在“泄露尚未公布的考生成绩、考生志愿、录取分数线等可能影响录取公正信息的，或者对外泄露、倒卖考生个人信息的”的情形，其所在单位应当立即责令暂停其负责的招生工作，由有关部门视情节轻重依法给予相应处分或者其他处理；涉嫌犯罪的，依法移送司法机关处理。

此外，对于普通高校招生工作中可能存在的招生违规问题，教育部此前曾以下发规定和实施暂行办法的方式予以规范。

教育部在今年 3 月下发的《2019 年普通高等学校招生工作规定》中指出，除按规定应向社会公开公示的信息外，对属于考生个人信息及有关录取过程中需要阶段性保密的工作内容，任何单位和个人不得擅自向他人提供或向社会公开，严禁非法传播、出售。

该规定同时对高考报名、考试、录取等招生各环节出现违法违规行为的处罚做说明。考生、考试工作人员、社会其他人员在高校招生的报名、考试、录取等各环节出现违规行为的，严格按照刑法、教育法等规定（办法）确定的程序和规定严肃处理，依法依规追究当事人及相关人员责任；涉嫌犯罪的，应及时移送司法机关追究法律责任。对公职人员违规违纪的，将按照相关规定严肃处理。

在这个体系中，教育部作为规定（办法）的制定者、学生隐私保护理念的倡导者、惩治侵犯个人隐私违法犯罪的监督者，不仅应身体力行，严格执行颁布的规章制度，更应以身作则，在保护学生隐私上率先垂范，充分利用法律武器、利用现代化管理工具，随时随地保护隐私信息。

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。

# 科技公司安全事件盘点，亿赛通硬核数据安全解决方案来袭 ~

## 苹果将不再保留 Siri 互动录音并致歉




近日报道称，苹果公司会有专门审查 Siri 语音记录的工作人员，在审查录音的过程中获得用户私人信息。

几小时后，苹果公司正式在其官网上致歉称，“我们知道客户近期一直为苹果人工审查 Siri 录音感到困扰，这是我们提高 Siri 使用质量的一部分，我们称之为‘评级’。当我们得知了用户的担忧之后，立即停止了所有人工对 Siri 的‘评级’的项目，并对所有的环节和政策进行了一个全面的评估。我们决定对 Siri 做一些改变。”




对于具体的改变，苹果公司承诺，将减少从 Siri 语音记录中搜集到的用户数据，也不会将存储在服务器中的数据，作为销售用途。

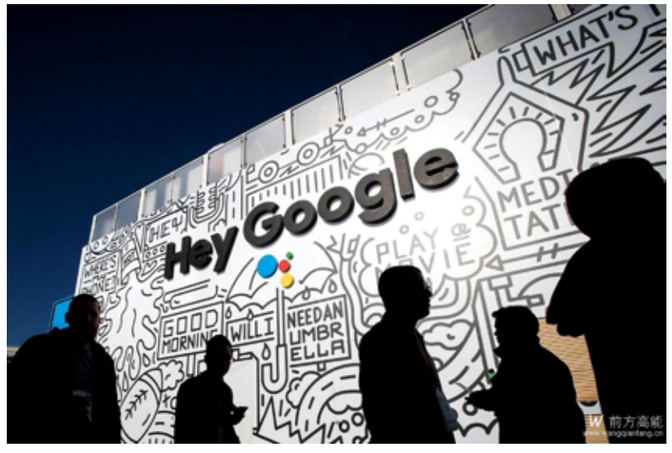
此外，苹果还承诺，用户可以选择自己使用 Siri 时的录音是否被人工审查，这项功能可被人工关闭，而非默认选项。“如果您不想保留 Siri 录音的转录，您可以在设置中禁用 Siri 和听写。”苹果称。对于审查录音的工作人员，苹果公司指出，仅指派公司内部员工，而非外部聘用的合同工。

美国媒体报道，陷入“窃听门”事件的科技巨头，并非仅苹果一家。在经媒体报道披露之后，谷歌暂停了人工审查录音的项目；亚马逊也调整了设置模式，使用户在使用 Alexa（亚马逊语音助手）时，可选择录音不被审查；Facebook 也叫停了人工审查用户录音片段的项目。

上述这些改进措施是在媒体揭露了“窃听门”的数月后，科技巨头才做出的改变。这些人工审查项目对于大众来说也是一个提醒，在科技产品的背后不仅有无形的算法和人工智能，也有人工参与的合作，帮助其提升产品质量。

虽然科技公司需要引入人力成本，去做与语音科技相关的工作，但是科技公司应该采取更多的措施，保证用户的录音不存在泄露隐患。

## Chrome 浏览器将内置数据泄露通知功能




有消息指出，Google 正在向 Chrome 浏览器添加内置的数据泄露通知服务，该服务会在用户使用已泄露的凭据登录网站时发出警告。

此前 Google 已经发布了一个 Password Checkup 扩展，它也提供了类似的警告，通过对该扩展数据的调查，Google 发现，大约 1.5% 的用户数据已经被泄露，而其中有 26% 的用户在收到警告后更改了密码。考虑到这种功能的重要性与普遍性，Google 这一次直接将其集成到 Chrome 中，作为一项内置特性存在。

值得一提的是，此前 Mozilla 在 Firefox 中也整合黑客网站 Have I Been Pwned（HIBP）推出了类似功能的服务，在用户电子邮件账户被泄露时也会发出警告。HIBP 是一个可以查询用户的邮箱是否被泄漏的网站，其数据库包含数十亿个已经被网络攻击套取的邮箱账户。

# Hostinger 数据泄露影响了近 1400 万客户

主机提供商 hostinger 今天宣布，在最近的一次安全漏洞允许未经授权访问客户端数据库之后，它重置了 1400 万客户的登录密码。

事件发生在 8 月下旬，第三方能够访问用户名、哈希密码、电子邮件、名字和 IP 地址。

## 未经授权的服务器访问

服务器有一个授权令牌，允许访问和权限提升到一个 RESTful API，该 API 用于查询客户及其帐户，包括电话号码、家庭地址或业务地址，已被未经授权的第三方访问。保存客户机数据的相应数据库表包含大约 1400 万主机用户的信息。

密码重置操作是一种预防措施，主机客户端收到了有关如何重新访问其帐户的通知和详细信息。该公司表示，金融数据和网站没有受到任何形式的影响。托管服务的支付是通过第三方提供商完成的，内部调查发现，有关网站、域、托管电子邮件的数据“未受到影响”。

随着全球经济产业调整的转变，高科技公司得到了充足的发展，高技术产业的信息化之路已经步入正轨。从整个行业生态的角度来看，高技术含量的企业发生泄密事件的概率普遍较高，例如互联网 IT 行业、电子通信行业、设计行业以及金融业等都是泄密高发行业。随着市场的饱和，行业竞争加剧，竞争升级催生各行业更高的保密需求。我们知道，数据就是企业的核心资产，一旦泄露，后果不堪设想。亿赛通作为中国数据安全防护专家，一直替您思考如何管理数据资产，并针对数据隐患，研发出六层防护体系以及一整套数据安全解决方案……

## 亿赛通硬核解决方案来袭

### 终端数据防护

终端防护通过利用透明加密技术，对文档进行防护，防止内部员工泄密和外部人员非法窃取企业核心重要数据资产，对文档进行全生命周期防护，用户可根据部门涉密程度的不同（如核心部门和普通部门），部署力度轻重不一的梯度式文档加密防护，实现技术、管理、审计进行有机的结合，实现文档的数据安全。

### 网络数据防护

网络数据防护通过 web 代理转发到网络 DLP 系统，对网络中传输的数据进行扫描和防护，可用于监控 SMTP 或 HTTP/HTTPS/FTP 协议外发的敏感数据；对进出单位内部网络的所有网络敏感数据进行扫描防护，对敏感数据泄露事件可根据策略进行阻断，保护敏感数据安全。

### 介质数据防护

存储介质防护是针对移动存储介质使用范围、使用方式及数据安全存储进行科学控制的安全管理系统。MediSec 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，以及内网专用介质接入非内网计算机上不能使用。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。

### 存储数据防护

存储数据防护可以对企业的文件服务器和数据库进行扫描，检查并标识存储文件服务器和数据库上暴露或常驻的企业敏感数据。对敏感文件进行报告，对泄密行为进行警告、阻断、审计等操作。防止通过文件服务器及数据库泄露企业敏感数据。

### 应用数据防护

应用数据防护将数据泄露防护与企业应用系统完美结合，有效地保障了业务系统的连续性和服务器数据的安全性。

### 文档安全云服务

文档安全云服务将服务器部署到云端，企业文档安全防护和“云”的有效结合，一方面可以降低企业核心数据的泄密风险，另一方面能够减少企业成本投入，同时区别于其他公有云服务，可以有效地防护企业数据在云上的存储安全，为企业打造安全高效的文档云服务。

# 东软医疗携手亿赛通
# 将数据安全防护进行到底




## 客户简介

东软医疗系统股份有限公司（以下简称“东软医疗”）是中国大型高端医疗设备的推动者之一。东软医疗目前拥有CT、MR、DSA、XR、PET/CT、RT、US、IVD、影像云九大产品线，能够提供放射影像、常规检查、放疗与核医学、临床应用解决方案。目前，东软医疗在中国设有 10 个大区、25 个省级办事处，美国、迪拜、秘鲁、俄罗斯、巴西、肯尼亚、德国设有 7 个海外子公司，越南设有 1 个办事处。产品遍布全球 110 余个国家，为 9000 多家医疗机构提供医疗设备与服务，践行“创新成就价值”理念，致力于成为全球医疗服务的最佳价值创造者！



典型案例 TYPICAL CASES

## 客户需求

随着东软医疗大力推进信息化建设，作为全球知名医疗服务商，数据安全早已成为其重点防护对象。在信息化融入到全球社会化迅速发展的时代，黑客数据攻击与威胁频发、安全漏洞隐蔽性强，泄露风险聚集、扩散性并存，构成行业数据安全风险态势严峻。为了加强东软医疗的数据安全建设，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东软医疗来说迫在眉睫。

经过多家方案技术对比，严格的实施测试，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、专业的售后服务，通过东软医疗的甄选，为其信息安全保驾护航。

## 功能亮点

亿赛通电子文档安全管理系统是一款电子文档安全防护软件，该系统利用驱动层透明加密技术，通过对电子文档的加密保护，防止内部员工泄密和外部人员非法窃取企业核心重要数据资产，核心功能如下：

1. 智能加密：可根据文档的内容进行语义识别，判断是否为企业所定义的加密数据并自动进行加密处理；

2. 内容安全管控：可截屏录制文档阅读水印、文档打印水印、拷贝粘贴控制；

3. 文档权限管理：可以细粒度权限控制、模板批量授权、文档权限管理；

4. 文档外发管理：可进行用户身份认证、使用权限管控；

5. 流程管理：可以进行文件解密审批流程、文件外发审批流程、邮件外发审批流程、离线办公审批流程、文件还原审批流程；

6. 审计跟踪：可进行邮件外发审计、文件解密审计、文件打印审计、流程全文检索审计、违规操作预警。

## 项目成果

亿赛通为其提供了完善的、适合其环境的数据安全解决方案，东软医疗安装电子文档安全管理系统后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，为其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，16 年来一直引领数据安全领域，服务于数万家企业，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，坚持把数据安全这件事做到更好！

## 集团企业部分典型客户

1、华润置地有限公司
2、蒙牛乳业 ( 集团 ) 股份有限公司
3、北京汽车研究总院有限公司
4、上海德邦物流服务有限公司
5、云南红塔集团有限公司
6、花样年集团
7、金太阳教育
8、深圳市世方商业地产
9、成都全友家私
10、361 度
11、江西济民可信集团
12、北京万泰生物药业
13、梅花集团
14、万科集团
15、北陆药业
16、达内时代科技集团有限公司
17、京汉置业集团股份有限公司……

欲了解解决方案应用详情，请拨打服务热线咨询：400-898-1617

# 中国航发沈阳发动机设计研究所




## 客户简介

中国航发沈阳发动机研究所（简称国发动力所，代号六 O 六所），始建于 1961 年 8 月，首任所长为刘苏少将，是国内大中型航空发动机设计研究中心，先后研制 11 种型号的涡喷、涡扇发动机。昆仑、太行两大发动机的成功研制，走出了一条中国自主创新研制航空发动机的道路，更实现了我国航空发动机研制历史上的伟大跨越。



典型案例 TYPICAL CASES

## 需求背景

航发沈阳所在庞大的业务体系下，为了防患于未然，让研发数据资产的安全能够做到事前预防，事中控制，事后审计与一体化的智能安全管理，对此航发沈阳所通过在众多的数据安全企业厂商中甄选，最终选择与亿赛通合作帮助企业实现数据安全管控。

## 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

电子文档安全管理系统的成功部署促进了航发沈阳所在项目过程中建立跨部门组织，方便了业务交流，加快了项目进展，并实现了对流程各级节点提供业务代办提醒及审核结果通报等的支持。