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

2019 年共 11 期

# 中国数据泄露防护产品市场

# NO.1

数据泄露防护市场需求旺盛，安全保卫战中谁能抢占先机？

《亲爱的，热爱的》火的不止 CP 热恋，还有它……

数据泄露巨额罚单连开，企业应防患于未然

关注企业官方微信

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

# 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




## CONTENTS目录

刊首语 PREFACE

# 《亿赛通七月刊》闪耀登场，独家解析国内数据泄露防护产品市场最新动态

季节的阳光，迈过春天，跨过仲夏，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，2019 年悄然过半。对此，精彩献上亿赛通七月刊……

7 月对于数据安全行业而言，也是历经考验。在随着大数据、人工智能、5G 等新技术的涌现，数据安全市场在这些产业中也将拥有更大的发展空间，安全技术也将上升到又一个新的发展阶段。亿赛通作为中国数据安全防护专家，16 年从未懈怠，专注数据安全领域，引领新技术前沿，开疆扩土，大力开发“安全”市场，制定精准营销战略，满足市场需求变化，不断提高品牌竞争力。近日，国内权威咨询机构——赛迪顾问，经一年多的跟踪研究与市场调研，推出了《中国数据泄露防护产品市场研究报告（2019）》。其中，在品牌竞争力研究中显示，亿赛通在品牌领导力、品牌市场力和品牌专注力等各个方面都处于行业领导者地位，2018 年的整体市场占有率又稳居第一，再一次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 2019 年下半年行业发展趋势……

国内

## 1、贷款应用可暴露数百万国人的位置

摘要：数据库、个人身份信息（PII）以及数百万中国用户的实时位置被阿里云基础设施托管的开放式弹性集群泄露。在申请贷款时，国人使用的 100 多个移动贷款相关应用程序将高度敏感的信息添加到可公开访问的数据库中。根据国外研究机构的报告，最初发现数据泄漏的研究员这些服务器的所有者并不知情，后来阿里云才下架了这些数据库。

## 2、智联招聘员工参与倒卖个人信息 16 万人资料被出售

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、涉 2.9 亿元“套路贷”案主犯一审被判无期，案涉泄露 20 余万条个人信息

摘要：据浙江新闻报道，7 月 1 日，绍兴中院对陈某某等人恶势力犯罪集团犯诈骗、敲诈勒索、侵犯公民个人信息罪一案进行公开开庭宣判，涉及借贷平台“米房”及“壹周金”，主犯陈某某被判处无期徒刑，剥夺政治权利终身，并处没收个人全部财产，罚金人民币 650 万元；判处曹某某等其余 16 人有期徒刑 10 年至 1 年 5 个月不等，并处罚金。

## 4、工信部：网易考拉、小红书、饿了么等未经用户同意收集个人信息

2019年一季度用户个人信息保护检查发现问题的互联网企业名单

| 序号 | 企业名称 | 网站/电话/APP名称（备案号） | 存在问题 |
|---|---|---|---|
| 1 | 北京物源时代数科技有限公司 | 每日+（京 | 未公示用户个人信息收集、使用规则<br>未告知收集、更正信息渠道<br>未提供账号注销服务 |
| 2 | 北京火星九州网络技术有限公司 | 风景FM（京 | 未公示用户个人信息收集、使用规则<br>未告知收集、更正信息渠道<br>未提供账号注销服务<br>未提供有效联系方式 |
| 3 | 杭州千岛信息技术股份有限公司 | 超长书城（京 | 未公示用户个人信息收集、使用规则<br>未告知收集相关信息渠道<br>未提供账号注销服务 |
| 4 | 暴风集团股份有限公司 | 暴风金融（京 | 未公示用户个人信息收集、使用规则<br>未提供账号注销服务 |
| 5 | 北京学而思教育科技有限公司 | 学而思网校（京 | 未公示用户个人信息收集、使用规则<br>未告知收集、更正信息渠道 |
| 6 | 深圳市盛多多网络科技有限公司 | 张多多（京 | 未公示用户个人信息收集、使用规则<br>未提供账号注销服务 |
| 7 | 北京随视文化传媒有限公司 | 酷乐视互连（京 | 未经用户同意收集个人信息 |
| 8 | 北京神州汽车租赁有限公司 | 神州租车（京 | 未明确告知用户业务集、使用规则的目的、方式和范围<br>征得用户同意收集使用个人信息 |
| 9 | 北京猎豹网络科技有限公司 | 猎豹浏览器（京 | 未经用户同意收集个人信息<br>征得用户同意收集使用个人信息 |
| 10 | 杭州贝购科技有限公司 | 贝贝（京 | 未经用户同意收集个人信息 |
| 11 | 上海拉扎斯信息科技有限公司 | 饿了么（京 | 未经用户同意收集个人信息<br>未明确告知用户业务集、使用规则的目的、方式和范围<br>征得用户同意收集使用个人信息 |
| 12 | 北京三快在线科技（上海）有限公司 | 小红书（京 | 未经用户同意收集个人信息<br>征得用户同意收集使用个人信息 |
| 13 | 杭州领车信息技术有限公司 | 51人品贷（京 | 未经用户同意收集个人信息 |
| 14 | 杭州优美网络科技有限公司 | 网易考拉（京 | 未明确告知用户个人信息<br>未明确告知用户收集、使用信息的目的、方式和范围<br>征得用户同意收集使用个人信息 |
| 15 | 北京趣哲征信信息技术有限公司 | 随知卡（京 | 未明确告知用户个人信息<br>未明确告知用户收集、使用信息的目的、方式和范围<br>征得用户同意收集使用个人信息 |
| 16 | 游族网络股份有限公司 | www.yzu.com | 未公示用户个人信息收集、使用规则<br>未告知收集、更正信息渠道<br>未提供账号注销服务 |
| 17 | 杭州飞鸟股份有限公司 | www.cfbyw.com | 未公示用户个人信息收集、使用规则<br>未告知收集、更正信息渠道 |
| 18 | 北京智之星信息技术有限公司 | www.autohome.com | 未告知收集、更正信息渠道 |

摘要：7 月 1 日，工业和信息化部（以下简称工信部）网站发布《工业和信息化部关于电信服务质量的通告（2019 年第 2 号）》，对 100 家互联网企业 106 项互联网服务进行抽查，发现 18 家互联网企业存在未公示用户个人信息收集使用规则、未告知查询更正信息的渠道、未提供账号注销服务等问题，已责令相关企业整改。其中，小红书、猎豹浏览器、饿了么、网易考拉、神州租车等多个 App 及网站存在未经用户同意收集个人信息的问题。

## 5、“宝贝回家”寻子公益论坛遭攻击 导致部分数据丢失


摘要：一个名为“宝贝回家”的民间志愿者寻子公益网站的官方论坛无法正常访问。官方公告称，遭受黑客攻击导致部分数据丢失，目前仍然在闭站维护中。截发稿之时，该网站仍未恢复访问。了解得知，宝贝回家寻子网是隶属于宝贝回家志愿者协会的公益网站，主要宗旨是为帮助寻找失踪儿童及一些流浪乞讨的孩子找家，为孩子家长及志愿者提供一个信息沟通的平台。

## 6、情侣“黑客”入侵教育网站 低价倒卖 网络课程 双双被刑拘

摘要：近日，石家庄鹿泉警方破获一起涉嫌非法获取计算机信息系统数据案，嫌疑人王某和女朋友朱某通过“黑客技术”入侵一家教育公司的网站，低价售卖网络课程获利，致使该机构蒙受很大的经济损失。二人本以为找到了一条赚钱的门路，不想事情败露，6 月 24 日，这对情侣被鹿泉警方刑事拘留。





## 7、明星肖战被私生饭取消值机

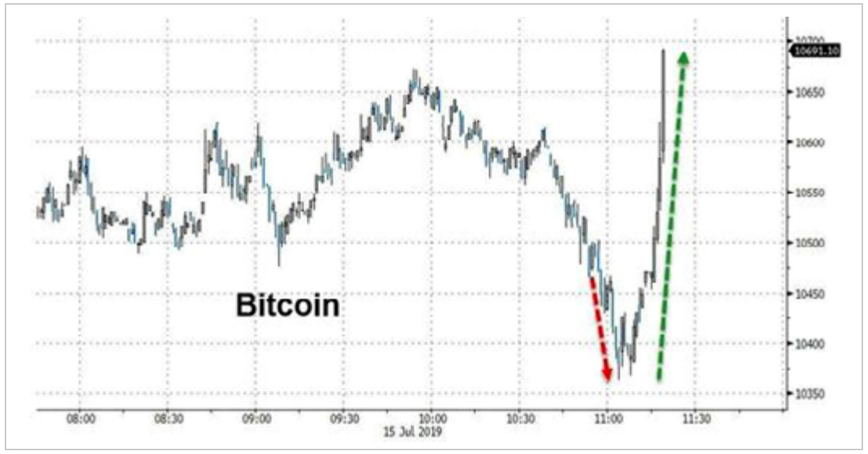
摘要：网曝有私生饭获取了明星肖战的信息，在其本人不知情的情况下，取消了肖战的航班值机，更有其他粉丝爆料称该私生饭是想要逼肖战坐另一班飞机从而方便跟机，今天凌晨时，肖战因此无奈滞留机场。

## 8、QQ 音乐随意清零用户财产

摘要：网友发现自己在 QQ 音乐上充值的虚拟乐币无故被清零，有些余额甚至高达几万元，但是 QQ 音乐并没有给出一个明确说明，就直接对用户的账号进行清零，这直接对用户本身的财产造成了伤害。随后，经过问题反馈之后，QQ 音乐工作人员向用户索要个人身份信息银行流水等私密信息。

国外

## 1、努钦警告 Libra 涉及国家安全问题




摘要：美国财政部长努钦（Steven Mnuchin）对 Facebook 提议的加密货币及其潜在的非法使用表示担忧。在 7 月 15 日的新闻发布会上，努钦称 Facebook 计划中的数字货币 Libra“可能被洗钱者和恐怖主义金融家滥用”，这是一个“国家安全问题”。

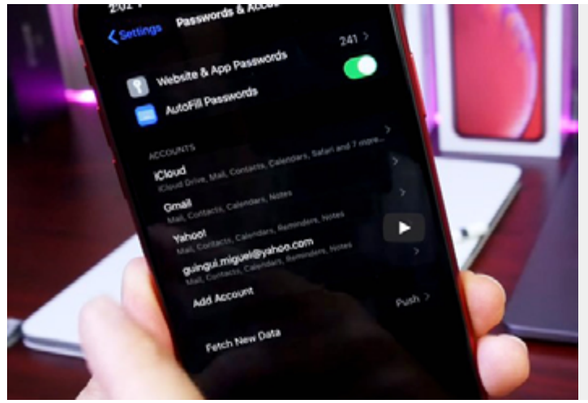
## 2、Evite 1.01 亿账号信息被盗


摘要：电子邀请网站 Evite 发布安全通知，承认部分用户账号信息被盗。名叫 Gnosticplayers 的黑客今年四月在暗网销售六家公司的用户数据，其中一家就是 Evite。Evite 在通知中称，恶意活动始于 2019 年 2 月 22 日，它在 4 月才得知系统被未经授权访问，5 月 14 日它得出结论黑客获取了它的一个不使用的数据存储文件，储存了 2013 年之前的用户数据，其中包括姓名，用户名，电子邮件地址，密码，如果用户填入的话还包括电话号码、出生日期和邮箱地址。





## 3、iOS 13 和 iPadOS 爆安全漏洞：解锁状态下可访问用户名和密码




摘要：援引外媒报道，在 iOS 13 和 iPadOS 的最新测试版本中发现了一个安全漏洞，允许绕过安全机制访问设置应用中的用户名称和密码，用户反复点击“网站 & 应用密码”选项可以绕过 Face ID、Touch IS 或者密码进行访问。不过这个问题对用户的影响并不是特别大，只有用户在解锁状态下访问设置应用才能起效。目前苹果已经收到这个问题的报告，但官方并未做出承认。

## 4、苹果手表个人未经同意或可收听他人 iPhone 信息泄露果真无孔不入


摘要：当地时间 7 月 11 日，据《华尔街日报》报道，苹果通过一家在线门户网站了解到，一苹果用户发现 Apple Watch 上预装的 Walkie-Talkie 应用程序存在安全漏洞，这一漏洞使得个人可以在未获得同意的情况下收听别人的 iPhone 对话。苹果没有透露这一漏洞的性质，并表示，目前尚不了解有用户因此次漏洞受到损害的情况，在解决问题时暂时禁用了该应用程序。

## 5、K12.com 暴露了多达 700 万条涉及学生个人信息的数据库记录


摘要：据 Comparitech 的安全研究人员称，在线教育平台 K12.com 本周无意中暴露了近 700 万学生的个人信息。暴露的数据库包含全名，电子邮件地址，出生日期和性别身份，以及学生就读的学校，同时还可访问其帐户的身份验证密钥和其他内部数据。

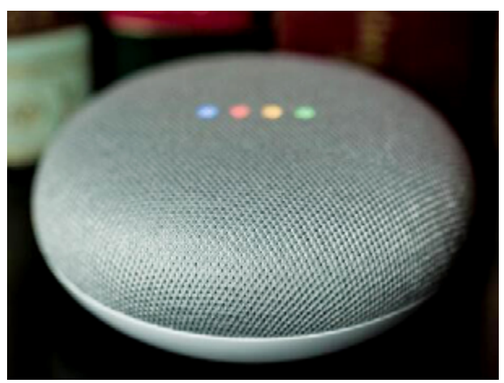
## 6、数据泄露事件达成和解 美政府将向脸书开 50 亿美元罚单


摘要：社交媒体巨头脸书因涉嫌泄露用户数据遭美国政府调查，7 月 12 日，美国联邦贸易委员会（FTC）批准与脸书达成一项 50 亿美元的和解协议，这也是 FTC 有史以来对科技公司开出的最大一笔罚款。综合美媒报道，美国联邦贸易委员会以 3 比 2 的投票结果批准了和解协议，3 名支持者来自共和党，2 名反对者来自民主党。这项协议仍需美国司法部批准，不过司法部很少驳回 FTC 达成的和解协议。一旦核准，这将是联邦政府历来对科技公司开出的最巨额罚款，约占脸书 2018 年收入的 9%。





## 7、谷歌承认：某些合作伙伴泄露 1000 多份保密对话录音

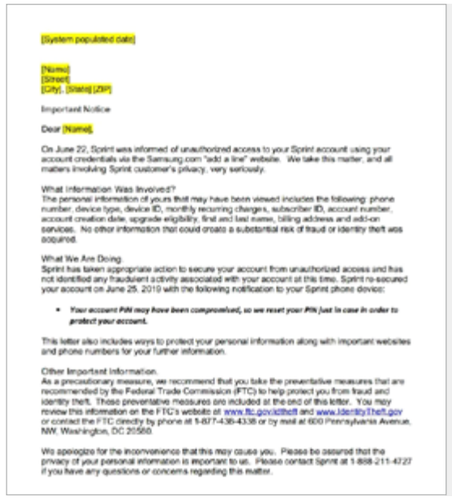


摘要： 7 月 12 日，谷歌承认，某些合作伙伴向一个比利时新闻网站泄露了 1000 多份客户与 Google Assistant（谷歌助手）的对话录音。谷歌和亚马逊等公司利用这些对话来改善其智能助理服务的语音响应功能，而对话信息应该是保密的。但比利时新闻网站 VRT 称，一家承包商向其提供了这种对话的样本，然后该网站利用这些样本找出了其中一些人的身份。VRT 网站还检查了当用户在手机或 Google Home 产品中说“OK Google”时，Google 会收集什么类型的对话信息。另外，VRT 还在对话中听到了客户地址等信息。

## 8、万豪泄露 3.83 亿名客户信息，英国：罚款 1.24 亿美元


摘要：网易科技讯 7 月 10 日消息，据国外媒体报道，国际知名连锁酒店万豪集团因去年发生数据泄露或将被英国监管机构处以高达 1.24 亿美元的罚款。2018 年 11 月，万豪透露，黑客从 2014 年开始入侵喜达屋的客户预订数据库。该公司最初表示，黑客窃取了大约 5 亿名酒店客人的信息。经过更全面的调查，万豪集团后来将信息泄漏的客户总数修正为 3.83 亿。根据对黑客行为的事后分析，黑客窃取了 3.83 亿名客户记录，1850 万个加密护照号码，525 万个未加密的护照号码，910 万个加密的支付卡号以及当时仍有效的 38.5 万张卡号。

## 9、Sprint 发警告：有黑客通过三星官网新办号码页面获取用户数据



[System populated date]

[Name]
[Street]
[City], [State] [ZIP]

Important Notice

Dear [Name],

On June 22, Sprint was informed of unauthorized access to your Sprint account using your account credentials via the Samsung.com "add a line" website. We take this matter, and all matters involving Sprint customer's privacy, very seriously.

What Information Was Involved?
The personal information of yours that may have been viewed includes the following: phone number, device type, device ID, monthly recurring charges, subscriber ID, account number, account creation date, upgrade eligibility, first and last name, billing address and add-on services. No other information that could create a substantial risk of fraud or identity theft was acquired.

What We Are Doing.
Sprint has taken appropriate action to secure your account from unauthorized access and has not identified any fraudulent activity associated with your account at this time. Sprint re-secured your account on June 25, 2019 with the following notification to your Sprint phone device:

- ***Your account PIN may have been compromised, so we reset your PIN just in case in order to protect your account.***

This letter also includes ways to protect your personal information along with important websites and phone numbers for your further information.

Other Important Information.
As a precautionary measure, we recommend that you take the preventative measures that are recommended by the Federal Trade Commission (FTC) to help protect you from fraud and identity theft. Those preventative measures are included at the end of this letter. You may review this information on the FTC's website at www.ftc.gov/idtheft and www.IdentityTheft.gov or contact the FTC directly by phone at 1-877-438-4338 or by mail at 600 Pennsylvania Avenue, NW, Washington, DC 20580.

We apologize for the inconvenience that this may cause you. Please be assured that the privacy of your personal information is important to us. Please contact Sprint at 1-888-211-4727 if you have any questions or concerns regarding this matter.

摘要： 美国移动通讯运营商 Sprint 近日发布警告称，有黑客通过三星官网（Samsung.com）上新办号码“Add a line”页面入侵获取用户账号信息，目前尚不清楚有多少用户受到影响。Sprint 在致受影响用户的信中表示：“6 月 22 日，Sprint 检测到有黑客通过三星官网‘新办号码’页面在未经你知悉和授权的情况下访问了你的 Sprint 账号，黑客可能已经获取了你的个人信息，包括电话号码，设备类型，设备 ID，每月经常性费用，用户 ID，帐号，帐户创建日期，升级资格，姓名，帐单地址和附加服务。”

## 10、保加利亚超 70% 个人隐私信息被盗 黑客还是阿桑奇的粉丝

摘要：据 zdnet 报道，一黑客组织窃取了数百万保加利亚人的个人信息，并通过电子邮件将盗取的数据的下载链接发送给当地媒体。据称，泄露的数据的来自保加利亚国家税务局。该国有关部门已经承认这一事件，并正与保加利亚国家安全局合作调查这起黑客事件。根据当地媒体报道，保加利亚全国人口总共约为 700 万，而黑客表示窃取了其中 500 多人的个人信息，约占比 71.4%。

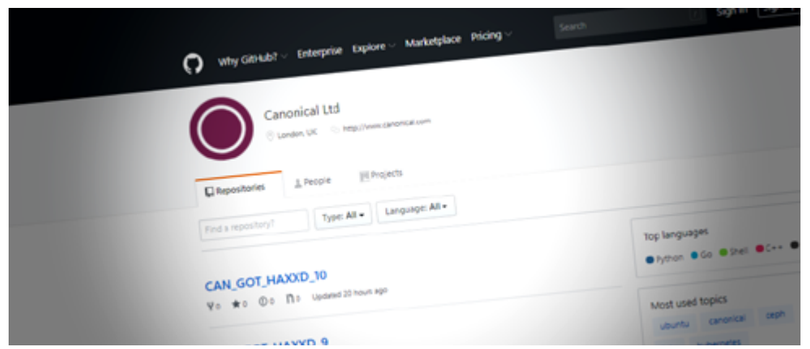




## 11、超 3300 万个邮箱密码泄漏 一波比特币勒索邮件袭来

摘要：腾讯御见威胁情报中心发文称近期捕获到一起挖矿木马攻击事件，该挖矿木马最大的亮点是利用被感染的服务器去分别验证数以千万计的邮箱帐号密码，再群发恐吓勒索邮件。截止目前，该病毒已经攻克了 1691 台服务器，已验证的邮箱帐号超过 3300 万个，包括 Yahoo、Google、AOL、微软在内的邮箱服务均在被攻击之列，最终可能会有上亿个邮箱帐号被验证。

## 12、Canonical 的 GitHub 账号遭入侵，Ubuntu 源码目前安全

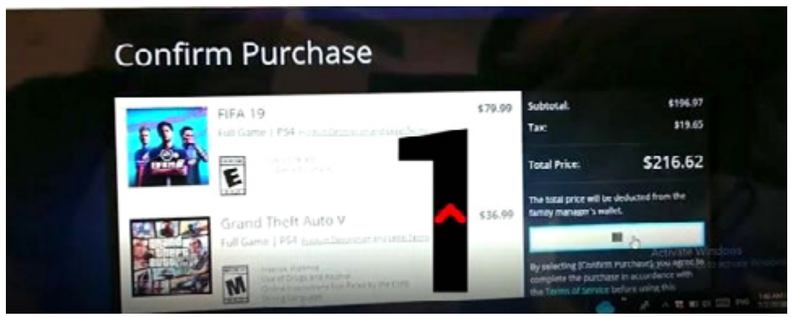



摘要：7 月 6 日，Canonical Ltd. 的 GitHub 账号被黑了。根据被攻击的 Canonical GitHub 帐户的镜像，黑客在官方 Canonical 帐户中创建了 11 个新的存储库。

## 13、英国航空公司将因数据泄露问题面临创纪录罚款处罚

摘要：据外媒报道，英国数据监管机构近日宣布，计划对英国航空公司处以 1.83 亿英镑的罚款处罚，原因是发生在去年的数据泄露事件。信息专员办公室 (ICO) 表示，因为这家航空公司糟糕的安全工作导致 50 万名左右客户的信用卡信息、姓名、地址、旅游预订信息和登录信息被泄露。据 BBC 报道称，这将是成为 ICO 有史以来开出的最高罚单，远高于 Facebook 剑桥分析 (Cambridge Analytica) 丑闻的 50 万英镑罚单。

## 14、外媒曝 PlayStation 严重安全漏洞，黑客可绕过验证盗刷信用卡




摘要：据外媒 MP1ST 报道，一位 Mod 制作者向他们来信称索尼 PlayStation 存在一个多年未修复的安全漏洞，可以让黑客绕过信用卡 CVV 验证进行盗刷，如果黑客们获得了玩家们的账号，却可以通过一个简易的漏洞“获取”受害者的信用卡，甚至可以绕过 CVV 验证使用子账号来消费。外媒调查发现这一漏洞已经大致存在了 5 年之久，让不少人蒙受了损失，但是目前还没能得到修复。





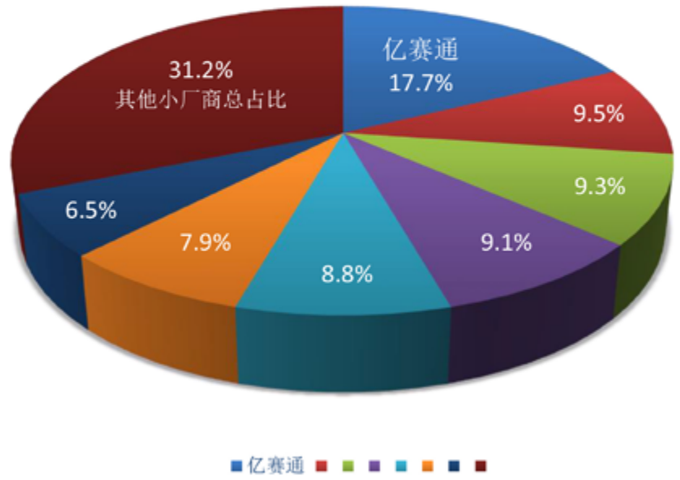
## 15、FCA：网络犯罪事件报告暴增 11 倍

摘要： 英国金融市场行为监管局 (FCA) 2018 年接到金融服务公司上报网络安全事件 819 起，几近 2017 年 69 起的 12 倍。银行是网络攻击的重点目标，由银行上报的网络攻击数量占比超过一半。批发金融市场紧跟其后，上报 115 起；散户投资公司报告 53 起。此外，2018 年里金融服务机构遭遇了 93 起彻彻底底的网络攻击，其中一半是网络钓鱼，20% 是勒索软件攻击。

## 16、以色列安全公司间谍工具可在针对性攻击中获取 iCloud 数据


摘要：微软 OneDrive 用于托管恶意文件的使用率显着上升。根据 FireEye 报告显示，微软 OneDrive 上一季度托管恶意文件的用户数量激增 60% 以上，而此前仅上升了一位数百分点。据 FireEye 称，OneDrive 在托管恶意文件的使用率方面，已经超过 Dropbox、Google Drive 和 WeTransfer 等竞争对手。

# 实力领跑！亿赛通数据泄露防护产品连续四年市场占有率稳居前列




2018 年中国数据泄露防护产品市场仍是“群雄割据”，江湖地位的争夺依旧很激烈。

在赛迪顾问的最新榜单《中国数据泄露防护产品市场研究报告（2019）》（以下简称“报告”）中，亿赛通的数据泄露防护产品市场占有率四年来始终稳居榜首。

论资排辈，亿赛通以 16 年的专业资历成为数据安全领域一哥，市场地位毋庸置疑，自被绿盟全资收购后，也拿出了亮眼的成绩。2018 年凭借 17.7% 的市场占有率，超越了众多国内安全厂商，再次证明了江湖地位。

## 国家政策全力支持

随着近年来国内网络安全事件频繁发生，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。2017 年 6 月 1 日《网络安全法》正式实施，2019 年 5 月 13 日，“网络安全等级保护制度 2.0 国家标准”正式发布，“等保 2.0”是网络安全的一次重大升级，保护对象范围在传统系统的基础上扩大到了云计算、移动互联网、物联网、大数据等。

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，关键信息基础设施运营者的安全保护义务得以进一步明确，对个人信息权的保护在各重要法规中建立了相应的保护机制。将来，国家在法律法规不断完善的基础上会出台各种实施细则，涉及网络安全的配套政策将快速下沉到电信、互联网、工业、教育、农业等各行各业，推动网络安全行业发展。

不过，在报告中有明确指出，虽然国家继续提升在政策层面对数据泄露防护的扶持力度，但由于中国 DLP 市场同质化竞争明显、产品价格走低、获取客户成本增加，导致中国数据泄露防护市场增长放缓，相较上两年，增长率有所降低。


*来源：赛迪顾问，2019.5*

从报告汇总来看，尽管，2018 年市场仅增长 5.1%，但随着国家政策愈发重视、企业与个人对数据资产的保护程度日益加深，数据安全市场依旧会迎来良好的发展机遇。预计 2019 年我国数据泄露防护市场规模将达到 9.8 亿元，同比增长 19.5%。未来三年，我国的数据泄露防护市场复合增长率将达到 20.4%，到 2021 年市场规模将达到 14.3 亿元。


*来源：赛迪顾问，2019.5*

而在此大好形势下，亿赛通如何稳固江湖地位，驰骋数据安全大沙场？

第一招，沉淀经验和服务，蓄势待发。亿赛通数万家的企业客户数量和 400 余万终端的服务经验决定了其征战数据安全江湖的先天优势。16 年的江湖打拼，让亿赛通打下了良好的企业客户基础。

第二招，打造综合型服务，多行业多领域布局。亿赛通自被收购后，全新整合国内市场，整体布局八大行业：制造业、设计行业、金融证券、研发通讯、集团企业、能源行业、运营商等，按行业划分形成了丰富、完整的数据安全服务体系，打造了服务不同领域、不同行业、不同规模企业级客户的能力，成为实力雄厚的 “综合型”选手。

第三招，携手渠道伙伴，构建完善服务体系。亿赛通的认证签约渠道有百余家，分布覆盖全国。公司以夯实基础为渠道建设出发点，以等级梯队制度为技术迭代落脚点。开源是一个公司发展壮大的重要因素，也会带来大量机会。

第四招，加大研发投入，持续创新。随着公司业务的不断壮大，2018 年初，武汉第二研发中心成立，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。研发中心的成立不仅缩短了项目交付时间，还推进了全国客户业务运转。亿赛通研究院又与多所高校结成“产学研”联盟，把实践教学基地建设成为校企之间合作的桥梁和纽带，储备高素质、高效率、创新型的专业人才。

小编相信，在国家政策支持下，数据安全市场将越来越具有优势。亿赛通深厚的实力积淀，全行业布局，丰富的产品体系，强大的研发实力，扎实稳健的发展路线，广泛的客户支撑，成为公司的有力条件，并将支持我司在数据泄露防护领域的发展。未来，亿赛通将继续坚定推动企业数据安全，并向世界级企业迈进。

# 一分钟了解亿赛通视频监控数据安全管理系统

近日，北京亿赛通科技发展有限责任公司自主研发的视频监控数据安全管理系统，获国家版权局计算机软件著作权登记证书。

中华人民共和国国家版权局

计算机软件著作权登记证书

证书号：软著登字第4062815号

软件名称：亿赛通视频监控数据安全管理系统 V1.0

著作权人：北京亿赛通科技发展有限责任公司

开发完成日期：2019年05月06日

首次发表日期：2019年05月06日

权利取得方式：原始取得

权利范围：全部权利

登记号：2019SR0642058

根据《计算机软件保护条例》和《计算机软件著作权登记办法》的规定，经中国版权保护中心审核，对以上事项予以登记。

中华人民共和国国家版权局 计算机软件著作权登记专用章 2019年06月21日

No. 04152358





软件著作权保护是指因为软件具有开发工作量大、开发投资高，而复制容易、复制费用极低的特点，为了保护软件开发者的合理权益，鼓励软件的开发与流通，广泛持久地推动计算机的应用，需要对软件实施法律保护，禁止未经软件著作权人的许可而擅自复制、销售其软件的行为。

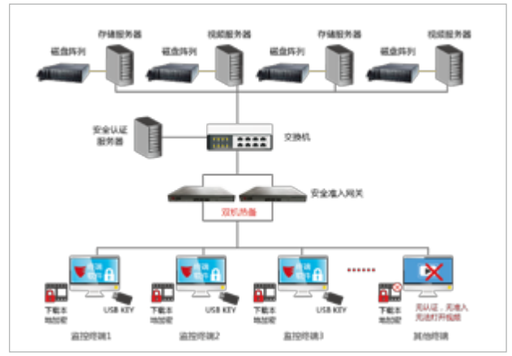
## 视频“监管”与“安全”

目前中国是世界上视频监控设备数量最多的国家，据不完全统计显示，国内公共场所的监控设备超 1.7 亿部，预计在 2020 年左右，我国的监控数量会达到 4.5 亿部。

然而视频监控系统因具有数量众多、24 小时在线、接入带宽高和安全防护差等特点，使其成为不法分子的攻击目标，通过利用弱口令及其它系统漏洞，来实施威胁国家、社会、企业和家庭安全的不法行为。

网络多次爆出黑客破解了家庭摄像头的防火墙，直接窃取主人的私密画面，放到 QQ 群或者其他平台出售：他们利用家庭摄像头存在的漏洞，破解摄像头密码，不仅可以获取摄像头能够拍摄到的内容，还可以对其进行远程控制。

而破解摄像头密码，入侵系统，偷看直播内容，已然发展为一条完整闭环的非法产业链。不法分子将窃取的视频进行“二次加工”，配上极具诱惑性的名字，挂到不良网站出售，成交率非常高。此外，已经有新闻多次报道，现在网络上存在一条灰色产业链，专门交易各种女性生活照。只需十几元，就可以“窥探”许多陌生女性的私密照片。




亿赛通——视频数据安全防护系统，享受国家保密局授权认证、广泛应用于军队和政府保密系统，以视频数据管理为基础，具有成熟的分级管理机制，贴合视频监控平台业务需求，具有独特个性的视频数据安全管控系统：

1、有效控制视频数据非授权下载后的泄密风险；

2、双重加密选择，提高工作效率；

3、屏幕浮水印，从源头管控敏感视频数据；

4、分布式管理模式，降低投入成本；

5、全程监控审计，有效追踪溯源各种终端行为；

6、全程监控所有操作行为，有效防范内部不良人员；

7、部署简单，可做到全网视频数据监控；

8、系统对视频监控平台进行访问二次加密验证控制，可有效防御外部攻击行为；

9、系统可对视频监控平台的权限进行重新定义，便于从源头发现和查处违规使用弱口令，以及数字身份被冒用等问题。

## 株洲市公安局

视频监控系统在株洲市公安系统的广泛应用下，亿赛通视频数据安全防护系统，对全网视频平台使用进行防护。既保证株洲市公安局工作网络较高的可用性、可靠性、保密性，又对核心视频数据有较强的防御、管控能力。提升工作管理建设能力，实现株洲市公安局信息安全监控、合规要求。

# 数据泄露防护市场需求旺盛，安全保卫战中谁能抢占先机？

近日，国内一线权威机构赛迪顾问股份有限公司调查研究的《中国数据泄露防护产品市场研究报告》新鲜出炉。这份数据泄露防护市场报告通过大量的实践调查和研究，详细、系统的分析了国内当下市场发展状况、行业竞争状况、以及未来发展潜力。那么，在互联网等迅速发展的大背景下，数据资产的安全已经上升到各行各业发展的重要战略层面，数据泄露防护作为一套完整的体系，用以解决不同类型用户的不同需求，但由于同质化竞争明显、产品价格走低、获取客户成本增加，导致中国数据泄露防护市场增长放缓。即 2018 年，数据泄露防护市场规模达到 8.2 亿元，同比增长 5.1%。

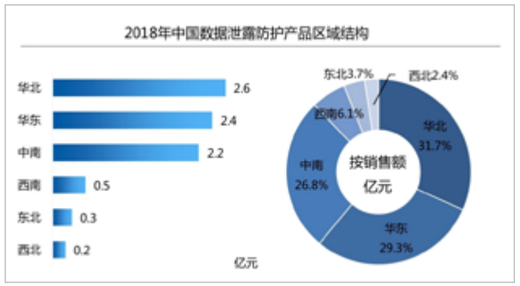
来源：赛迪顾问，2019.5

同时，在国家政策的大力支持和重视下，伴随着我《网络安全法》的实施与等保 2.0 的发布，数据安全需求不断扩大，预计 2019 年我国数据泄露防护市场规模将达到 9.8 亿元，同比增长 19.5%（如图 2），市场发展潜力巨大。

来源：赛迪顾问，2019.5

## 按区域划分市场

报告中调查数据显示，数据泄露防护产品已经成为行业主流安全产品。并且通过调查发现华东、华北、华南（中南）地区是产品的主要需求市场。

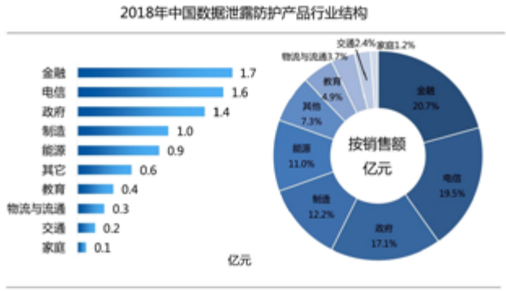




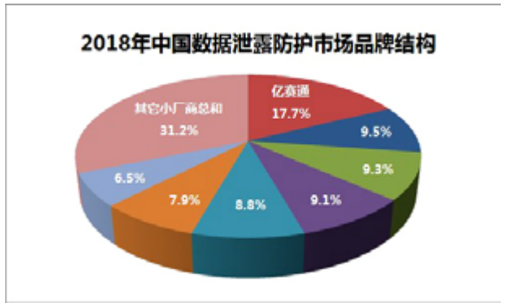



## 按行业划分市场

从行业结构来看，金融、运营商、政府、制造、能源等关系到国计民生的行业，对数据泄露防护产品的需求必不可少，其中以金融、运营商、政府为主。




近些年来，借助我国推进“自主可控”战略的东风，数据泄露防护产品的国产化替代的格局已经开始慢慢形成，也将可能成为未来一个时期的重要特征。同时，国产化的数据泄露防护产品更符合中国国情，而相较于网络安全厂商与系统集成商，数据安全专项厂商，从强制防护手段的传统数据泄露防护产品起步，坚持强制加密的核心技术路线，大力推动数据高强力度保护，并经历了多年的发展和变革，在市场中具有显著影响力。特别是亿赛通在透明文档加密、内容识别、存储数据防护、应用数据防护，终端数据防护等被动、主动防护方面具有技术优势，并针对特定行业领域细分解决方案，逐步成为“敏感数据识别与主动防护相结合”“终端 + 网络 + 应用”的全过程全范围数据防护服务提供商。而其他安全服务提供商往往通过并购等方式建立大而全的产品线，对外宣称各种保护一应俱全，实质上，这类数据泄露防护产品在市场上占有率较低，不是市场的主力，更多是以网络安全作为主营方向。未来，专项数据安全厂商将凭借自身的技术和产品优势，具备较强的市场竞争力。




一个不断“创新”的企业，更能精准把握市场动态，有了绝佳的“武器”之后，便要布局市场，占领高地。亿赛通坚持超前创新的服务理念、前瞻性的关键技术，是创下了一座又一座新的里程碑“秘诀”。

多变的市场环境中，亿赛通在专注中成为了数据安全领域最为权威和专业的企业，专注成就了企业的成长，使得其对于市场的走向，客户需求的把握更加专业，从而对市场把握更为精准，面对数据泄露防护市场竞争越发激烈的今天，早已布局数据安全领域的亿赛通获得了先机。

文章中所有数据均来源于赛迪顾问

# 个人信息违法行为专项执法行动取得阶段性胜利，罚没款超 564 万元


我的个人信息还安全吗？

相信生活中每个人都有过这样的疑问

买房没多久

就会接到装修、家具商家的电话短信

买车没多久

就会接到一堆推销车险的电话

孩子刚上幼儿园

早教培训机构的电话就此起彼伏

……

乱象背后隐藏着一个共同的问题

消费者的信息安全问题

今年 4 月，市场监管总局

在全国市场监管系统部署开展

“守护消费”暨打击侵害消费者个人信息

违法行为专项执法行动

7 月 3 日，市场监管总局对外公布

专项执法行动第一阶段成果

按照总局统一部署，截至 5 月 31 日，为期两个月的第一阶段行动已经顺利结束。各地市场监管部门迅速启动，深入摸排案件线索、强化执法联动，突出房产租售、装饰装修、教育培训等重点行业，查处了一批未经消费者同意，收集、使用，泄露、出售或者非法向他人提供消费者个人信息等侵害消费者个人信息案件。

据统计，在第一阶段行动中各地市场监管部门已立案查处各类侵害消费者个人信息案件 200 件，涉案信息 111 万余条、罚没款 564 万余元，向司法机关移送案件 41 件，抓获犯罪嫌疑人 6 人；组织执法联动 604 次；开展行政约谈 279 次；开展各类宣传活动 3129 次。

下一步，国家市场监管总局将继续推进专项执法行动深入开展，加大对大要案的督查督办力度，指导各地市场监管部门充分发挥执法协作机制作用，积极开展执法联动，切实形成执法合力，进一步强化案件查办；广泛开展专项执法行动成果宣传，进一步提升经营者法律意识，增强消费者维权能力，营造全社会尊重消费者个人信息良好氛围。亿赛通也会继续配合国家专项治理行动，筑牢安全防线。同时提醒商家尽快利用起科学技术，规避泄密风险，全民行动一起抵御不法分子的泄露行为。

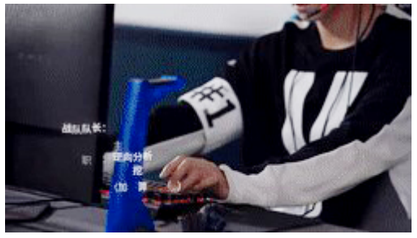
文章来源：国家市场监督管理总局

# 《亲爱的，热爱的》火的不止CP热恋，还有它……


小编日常打开微博热搜，突然看到大批网友吐槽“亲爱的，热爱的电竞赛改成网络安全赛？？？”这条评论成功的引起小编注意。立刻！马上！观看了第一集 ... 的前几分钟。镜头一开始，woo，居然是网络安全大赛，再一看，这么多高颜值小哥哥，仔细一看，编剧你怕是对网络安全有什么误解？网友们纷纷表示“我可能学了个假的网络安全”，虽然小哥哥们一顿操作猛如虎，却输掉了比赛……

抛去各种“槽点”“网络安全”“蠕虫病毒”……这些很多观众日常根本不了解的名词，现在出现在热播电视剧里，也着实让“网络安全”火了一把！

最近几年，有关网络攻击，黑客攻击导致的重要信息泄露，数据丢失等事件频频发生，所以在网络安全形势的严峻下，国家也在重点关注网络安全问题。从最近几天热播的《亲爱的，热爱的》电视剧中就可以看出，



宣传培养大家的网络安全意识是重中之重。

黑客攻击主要是对服务器的攻击，漏洞发现，植入病毒等。如果我们的移动端，PC 端，服务器被攻击了或者是被植入病毒、木马、出现漏洞等，那么会出现什么问题呢？

• 企业敏感信息（如：身份信息、账户名称、银行账户、银行密码等）被窃取或者监视用来贩卖；

• 黑客利用漏洞或者木马病毒远程控制服务端设备，将企业重要的数据文件删除、新建、修改、上传、下载等一系列操作；





• 黑客通过邮件方式带有病毒链接打开时自动被植入控制系统操作，让其设备沦为僵尸主机，打不开等。

针对敏感信息来说，主要在五种形态下容易被泄露，即数据存储中、数据使用中、数据传输中、数据外带中、数据外发中，那么，中国数据安全防护专家亿赛通来告诉你如何防范。

## 数据存储安全

针对场景：竞争对手窃密、员工离职拷贝、内部有意无意泄密、间谍 / 黑客窃密、设备丢失、非法脱机、电脑报废数据丢失、电脑那到第三方去维修信息被窃……

解决方案：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。

## 数据使用安全

针对场景：涉密文件在企业内部员工流通过程中的使用权限，如有些涉密文件不想被内部某些部门打印、复制、修改，导致信息泄密问题……

解决方案：文档权限管理系统采用多层结构设计，对企业核心电子文档进行细分化的权限设置，确保机密信息在授权的应用环境中，在指定时间内，被指定的人进行指定操作，不同使用者对同一文档拥有不同权限，通过对文档内容的安全保护，实现机密信息分密级且分权限的内容安全共享机制。

## 数据传输安全

针对场景：在数据传输的过程中，遇到网络窃取敏感信息、网络拦截重要信息、网络监听重要信息等非法窃取信息……

解决方案：亿赛通移动终端数据防护系统，主要防止利用移动设备非法获取应用系统数据的智能终端安全防护系统。移动终端数据系统由移动数据防护控制台与移动终端客户端软件两部分组成，系统配置管理采用 B/S 架构，系统部署后不会改变用户使用习惯。

## 数据外带安全

针对场景：企业工作人员在外出差办公携带电脑涉及企业的敏感信息容易被窃取、因工作需要回家加班涉及的公司敏感信息，携带出去带来的风险……

解决方案：离线办公支持，系统提供安全离线办公业务支持，通过离线审核、策略预设及离线补时等功能满足各类离线办公要求，保障离开公司外办公的状态下信息安全操作。

## 数据外发安全

针对场景：针对的是企业外部第三方文档使用者的权限问题，就是当企业将自己的设计图纸、办公文档、视频音频等数据，交接给第三方时，第三方会盗取其中的信息……

解决方案：亿赛通文档外发管理系统，是针对客户的重要信息或核心资料外发安全需求设计的外发安全产品。当客户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。

# 数据泄露巨额罚单连开，企业应防患于未然

如今，数据安全和隐私保护是各国政府和企业非常注重的问题，一些企业因数据、用户隐私泄露而被开出高额罚单的案例也越来越多。

## 美国政府对脸书开出史上最大罚单

美国联邦贸易委员会（FTC）对 Facebook（脸书）的不当隐私实践进行了长期调查之后，双方最终达成和解，和解金约 50 亿美元。


美国联邦贸易委员会（FTC）的五名委员进行了投票，以 3:2 的投票结果通过了与 Facebook 达成的和解协议，同意以罚款 50 亿美元和其他附加限制条款结束对这家社交媒体巨头的长期隐私调查。

知情人士透露，FTC 中的共和党多数派支持这项协议，而民主党委员则表示反对。此后，这起案件将被转移到司法部下属的民事部门，目前尚不清楚需要多长时间才能最终敲定协议，司法部的审查是 FTC 程序的一部分，但通常不会改变后者的裁决结果。

## 英国航空数据泄露面临 2.3 亿美元罚款

英国计划针对电脑系统遭到黑客攻击，导致客户数据泄露的情况，对英国航空处以 1.834 亿英镑（约合 2.3 亿美元）的罚款，这也是欧盟条例生效以来开出的第一张罚单，欧盟制定这一意义重大的条例，目的就是要求各企业加强反黑客举措的实施。


负责保护数据隐私的英国信息专员办公室（ICO）在声明中表示，去年 6 月到 9 月发生的数据泄露影响客户人数达 50 万人，此次拟议处罚正是针对这一事件发出的。英国航空的母公司国际航空集团表示罚款数额是英国航空 2017 年收入的 1.5%。

ICO 表示此次黑客攻击将英国航空网站流量转移到欺诈网站，并通过该网站收集客户详细信息，这些信息的隐私安全也受到了与网站登录、支付卡、旅行预订细节、姓名和地址信息等相关的保护功能不力的影响。






## 万豪：因泄露 3 亿用户数据，罚款 1 亿英镑

英国信息监管局发表声明称，针对万豪国际集团违反《一般数据保护条例》，开出约 9900 万英镑（约合 1.23 亿美元）罚单。

英国信息监管局发表声明称，2014 年喜达屋酒店集团数据系统遭入侵，2016 年万豪收购喜达屋，但客户信息被窃事件直到 2018 年才被发现。该机构认为，万豪未能在收购中进行充分调查，也未采取足够措施保护数据系统。

声明说，万豪 2018 年 11 月向英信息监管局通报一起始于 2014 年的数据泄露事件，该事件导致全球逾 3 亿条顾客数据被窃取。

信息监管局同时表示，万豪可就该调查结果和罚款进行申诉。

如今，全球各个领域都开始意识到数据资产的巨大价值，保障数据安全就成为了这一时代的刚需。当一家企业无法确保数据安全时，将会给用户以及公司带来巨额的经济损失和信誉损失，甚至是企业难以经营发展面临倒闭的严重后果。

发生数据泄漏通常以窃密、泄密和失密行为所致。窃密主要指外部人员（如间谍、黑客等）通过非法手段恶意窃取信息数据，泄密和失密则是内部人员主观有意或无意造成的信息泄漏。传统的安全防范侧重于对外部的入侵防范，对内部却缺乏有效的管理，据《财经》杂志报道显示，有 80% 的数据泄露是企业内鬼所为，黑客和其他方式仅占 20%。

有一些企业认为，重要的数据信息往往仅在内部网络甚至是涉密网络中运行，黑客窃取数据的难度较高。然而，拥有较高权限的管理人员、维护人员、开发工程师，可能更容易接近这些核心敏感数据，这些人员一旦出现主动或者被动的造成数据泄露，其后果的严重性将无法预估的。

纵观国内外被公开的大型数据泄露事件，对企业和组织带来的损失将是多方面的，这其中除了经济损失，还存在品牌信誉和业务影响。数据泄露的根本原因都在于企业数据安全体系的不完整，数据作为企业的源动力，其安全防护应结合企业特定环境，形成适合企业的纵深防护体系。

解决数据安全隐患亿赛通自主研发出一整套解决方案，可通过数据防护，分别从文件的存储、传输、使用等方面，采用核心加密技术，巩固企业数据安全建设，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。并且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。除此之外，亿赛通针对各种敏感文件进行有效识别敏感数据，监控敏感数据使用情况，防护敏感数据外泄，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。

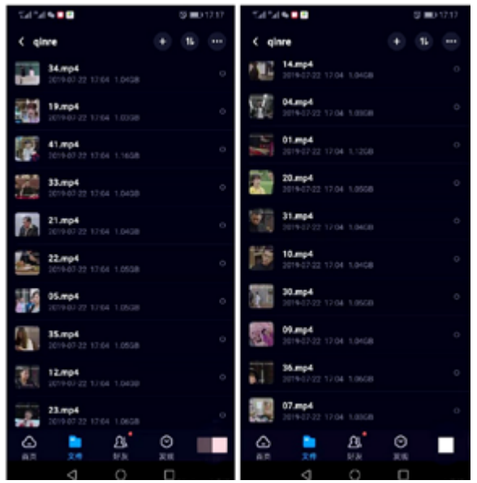
要知道，数据安全政策法规不只欧盟有 GDPR；也不止外国企业才会因数据泄露等安全事件而被问责和处罚。在中国，《网络安全法》早已实施，等保 2.0 也已发布，年底即将实施，而《个人信息保护法》《数据安全法》等紧密相关的法律法规也正在积极制订中。新环境下，保障数据安全已成为中国企业实现持续健康发展的重要前提和基础。亡羊补牢代价太高…为何不防患于未然?

# 天了噜，热播剧全集遭泄密，官方超无奈

说起近期热播剧，非《亲爱的，热爱的》莫属，真是掀起全民追剧热潮～但最近不少网友称已经看完该剧全集内容！什么情况？


电视剧《亲爱的，热爱的》从开播伊始就备受关注，这两天却遭遇了全集泄露事件。该剧的全部 41 集高清视频非法资源在互联网被下载、传播，此外，还有不少所谓投机的商家，公然对该资源进行非法售卖。

经在网上搜索，小亿发现确有多个平台已经上传了《亲爱的，热爱的》全集资源。而在微博、贴吧等社交网站，也有多人发布相关网盘资源。




相较于电视播出的剧集，泄露版的视频画面上标注有“仅限东方卫视查阅”以及时间轴的字样，但视频内容和预告片中的一样。这不禁让人联想，难道是内部人员造成的资源泄密？






日前，女主角杨紫在微博公开呼吁大家尊重版权，维护优秀作品的权益。这一声明得到了广大粉丝、观众的理解与支持，同时，也印证了未播剧集遭泄露的传言。


网友、粉丝们纷纷表示：抵制盗版，坐等更新


目前泄露原因并未查清，但据内部人士分析，影视剧比较普遍泄露环节有两种，一种是在拍摄、制作和发行的某个环节，泄露者属于剧组内部员工或者合作方员工，这些人大多都有合同在身，他们这种行为就是违反了合同的约定，应承担违约责任。

另一种可能泄露的方式，是影片在经相关部门的审查过程中，由于工作人员故意或者疏忽产生的泄露，属于他们失职或者滥用职权的行为。

不过泄密事件的发生，其原因主要还是安全防护工作做得不够扎实。

亿赛通自主研发的个人版“数据安全卫士”，可对 PC 端的重要信息或核心资料在进行全面防护，即当您在将个人的重要文件、照片外发或上传网盘之前，对文件进行加密保护。接收者打开文件首先需要进行身份认证，方可阅读，可以有效的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或二次使用。

无论何时，安全意识都需常在心间，绷紧防护弦，如若不然，稍有不慎就会被有心者所利用造成社会危害。老铁，将你倾心呵护的秘密资料，交给亿赛通数据安全卫士吧！

## 福利回馈

各位小伙伴们，现在关注“亿赛通”微信公众号，回复 “激活码”，即可获得价值 366 元一年的数据安全卫士会员版使用特权，机不可失，快快领取吧！

# 中核能源科技有限公司


## 客户简介

中核能源科技有限公司成立于 2003 年，是在原国防科工委的支持和推动下，由中国核工业建设集团公司与清华控股有限公司（清华大学）共同出资组建的核能高科技企业。中核能源的使命是围绕实现股东各方的战略目标，集聚整合股东各方在研发设计、工程实践、产业配套等方面的优势资源，发挥产学研结合的体制优势，发挥企业主体和产业化平台的积极作用，推动我国具有自主知识产权的高温气冷堆、低温核供热堆两大先进核能技术实现产业化。



典型案例 TYPICAL CASES

## 需求背景

由于中核能源在庞大的业务体系下，数据管理还存在一些不完善的地方，为此中核能源通过在众多的数据安全企业中甄选，选择与亿赛通合作帮助企业实现数据安全管控。

## 解决方案

亿赛通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。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

亿赛通文档安全管理系统帮助中核能源实现一体化的数据安全管理，为企业铸就了坚不可摧的安全盾牌。

# 国家核电技术公司


## 客户简介

国家核电技术公司 ( 简称“国家核电”) 成立于 2007 年，是国有重点骨干企业之一。根据《国务院关于组建国家核电技术有限公司的有关问题的批复》（国函（2007）35 号）的要求，国家核电是受让第三代先进核电技术，实施相关工程设计和项目管理，通过消化吸收再创新形成中国核电技术品牌的主体；是实现第三代核电技术 AP1000 引进、工程建设和自主化发展的主要载体和研发平台；是大型先进压水堆核电站重大专项 CAP1400/1700 的牵头实施单位和重大专项示范工程的实施主体，成为具有国际竞争力的核电投资运营商和能源工程技术服务商。





## 需求背景

随着国家在战略层面对核电发展大力支持，国内核电项目不断兴起，信息安全作为保障核安全的有机组成部分，成为国家核电关注的焦点。如何建立信息安全管理体系及落实信息安全解决方案？亿赛通文档安全管理系统为国家核电信息安全提供了具体实施部署方案。

## 解决方案

1、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、统一身份认证平台进行无缝集成，如实现组织构架及用户账号信息的自动完整同步和单点登录认证集成；

3、每个用户都设有文件收件箱、发件箱、还原箱，方便对权限文档的使用和管理；

4、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；

5、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；

6、提供“密文 / 明文”切换模式，保障业务涉密数据安全处理的同时，不影响用户个人数据的处理。

## 项目成果

从内部和外部两个方面保障国家核电数据安全，有效的保护企业核心数据资产，保障企业竞争力，提高企业的数据可用性，降低运营维护成本，加强了员工的安全意识，提升了企业的综合品牌形象。