



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

网络从不是法外之地 | 从新冠确诊患者“网暴”看信息泄露

**热点** | 捷报频传！再次荣获百强称号，亿赛通成功入选  
网络安全产业百强榜

亿赛通两大专业方案斩获实力奖项，信创布局正当时



盘点 | 风起云涌的 2020，数据泄露到底有多疯狂？

新规 | 金融行业再添新政策，数据安全必不可少



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 欢乐贺新春，《亿赛通一月刊》祝您新年快乐

### 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 捷报频传！再次荣获百强称号，亿赛通成功入选网络安全产业百强榜

18/19 亿赛通两大专业方案斩获实力奖项，信创布局正当时

### 亿赛通小贴士 ESAFENET PROMPT

20/21 新规 | 金融行业再添新政策，数据安全必不可少

22/23 网络从不是法外之地 | 从新冠确诊患者“网暴”看信息泄露

24-26 盘点 | 风起云涌的 2020，数据泄露到底有多疯狂？

27 勒索不成恼羞成怒，公开电器巨头“背后的秘密”

28/29 原来还能这样牟利，运营商行业数据安全迎来新挑战

### 典型案例 TYPICAL CASES

30/31 医疗行业数据安全解决方案

32/33 江苏豪森药业集团有限公司

34/35 黑龙江珍宝岛药业股份有限公司

牛年  
贺岁



Happy New Year

## 欢乐贺新春，《亿赛通一月刊》 祝您新年快乐

牛年春节到，新春哈哈笑，  
盛世迎宾朋，金牛圣火照，  
千年华夏史，辛丑金秋傲，  
五星红旗扬，四海传捷报，  
和谐春风舞，愿您更美俏！

亿赛通诚挚祝福各位同事、合作伙伴、全国代理商以及全国朋友们  
2021年：身体健康幸福享，美满家庭乐无限！

**放假提醒：**感谢您一年来对亿赛通的信任和支持，我司2021年  
春节放假时间为2月8日~2月21日，共14天，2021年2月22日（星  
期一）正常上班。

国内

# 1、疑似超 2 亿国内已泄漏用户信息在国外暗网论坛兜售



**摘要：**国外安全研究团队 Cyble 在一次日常安全监控中发现了多个帖子正在出售与中国公民有关的个人数据。经分析，这些数据很可能来自微博、QQ 等多个社交媒体，其中还发现了大量湖北省“公安县”的公民数据。其中一个帖子，威胁者公布了公安县 999 名中国公民的户口登记样本数据，以作为黑客攻击的证据。并表示共有 730 万中国公民的数据可供出售，包括身份证，性别，姓名，出生日期，手机号，地址和邮编等记录。专家们还注意到与微博平台用户有关的数据等待出售。

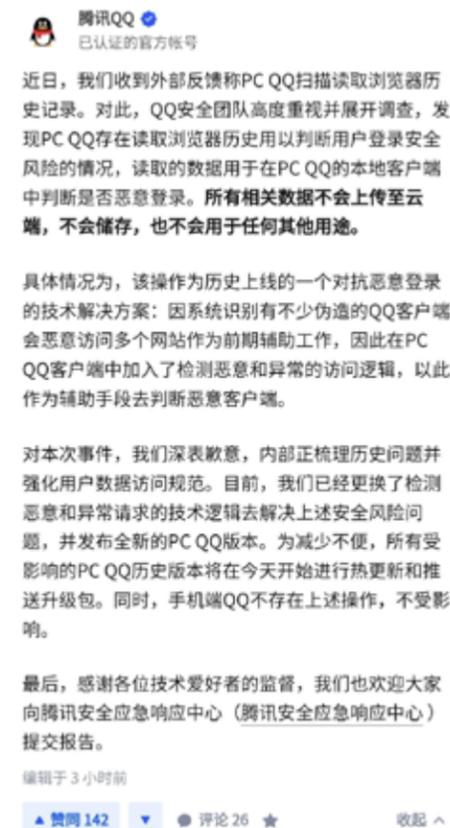
## 2、工信部通报下架 12 款侵害用户权益 APP 名单

| 下架的应用软件名单 |          |                  |         |
|-----------|----------|------------------|---------|
| 序号        | 应用名称     | 应用开发者            | 应用版本    |
| 1         | Wake     | 北京城盛之光网络科技发展有限公司 | 7.7.0   |
| 2         | 场库       | 北京新片场传媒股份有限公司    | 5.8.2   |
| 3         | 玫瑰约会同城交友 | 广州四叶文化传媒有限公司     | 2.5.0   |
| 4         | 海卷吧      | 上海腾云网络科技发展有限公司   | 7.33    |
| 5         | 一罐       | 宁波聚融网络科技有限公司     | 3.12.5  |
| 6         | 猜猜你是谁    | 北京百视悦视文化传媒有限公司   | 1.0.5.1 |
| 7         | 美赞课堂     | 北京美赞科技有限公司       | 2.0.1   |

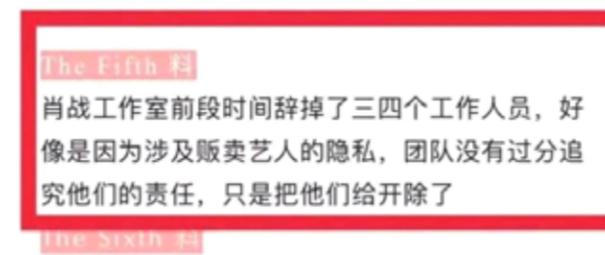
**摘要：**2020 年 12 月 21 日，我部向社会通报了 63 家存在侵害用户权益行为 APP 企业的名单。截至目前，经第三方检测机构核查复检，尚有 12 款 APP 未按照我部要求完成整改。依据《网络安全法》和《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407 号）等法律和规范性文件要求，我部组织对上述 12 款 APP 进行下架。相关应用商店应在本通报发布后，立即组织对名单中应用软件进行下架处理。

## 3、腾讯 QQ 解释读取浏览器历史记录原因：用于对抗恶意登录

**摘要：**技术社区 V2EX 的网友报告 QQ 与 TIM 软件会扫描并上传用户的浏览器历史并搜索购物记录选择性上传引发关注。腾讯 QQ 在知乎的官方认证账号回复了《如何看待 QQ 扫描读取所有浏览器的历史记录？》贴文中确认 PC QQ 存在读取浏览器历史用以判断用户登录安全风险的情况，但读取的数据是用于在 PC QQ 的本地客户端中判断是否恶意登录。所有相关数据不会上传至云端，不会储存，也不会用于任何其他用途。



## 4、肖战信息被泄露！曝为旗下员工故意售卖，工作室已采取行动



**摘要：**艺人信息被泄露是一件很可怕的事情，几乎每个稍微有点名气的年轻艺人都会有这样的苦念，肖战可以说是深受其害了，他的粉丝非常多，相对应的他的私生粉也非常多，他拍摄《王牌》的时候所入住的地方每天都有非常多的粉丝，这使得他不能从正门进出。还有他的航班几乎成了半公开状态，他的黑粉一查就能查到，所以当风车等人会对他的行踪仿佛了如指掌，都知道在娱乐圈中，时常会有员工缘故泄露艺人消息的事情发生，并且这样的事情屡禁不止，几乎成了娱乐圈常态，因为这的确能带来丰厚的收益。

## 5、银行数据泄漏：到底该不该信？



**摘要：**1月8日，有人在国外某论坛上发帖，以8.8个比特币的总价售卖交通银行1679万笔数据。贩卖者还发布了部分测试样本数据，包括客户姓名、账号、开户行、联系地址等。1月12日，交通银行通过官网发布声明称，经系统核查比对，确认与交通银行真实客户信息不符。交通银行郑重声明，不存在黑客入侵，不存在客户信息泄漏。交通银行已就相关违法行为向公安部门报案，依法追究损害商誉行为的法律责任。

## 6、牛某将「逻辑炸弹」植入某“数据防泄漏系统”：被判18个月



**摘要：**牛某某于2018年6月，在某公司工作期间，在办公室内使用公司给其配发的工作电脑，编写“逻辑炸弹”恶意代码函数并上传至该公司服务器，致该公司“数据防泄漏系统”软件无法正常运行，造成公司直接经济损失人民币13586元。

## 7、国家邮政局：加强快递数据监管 严查泄露信息等行为



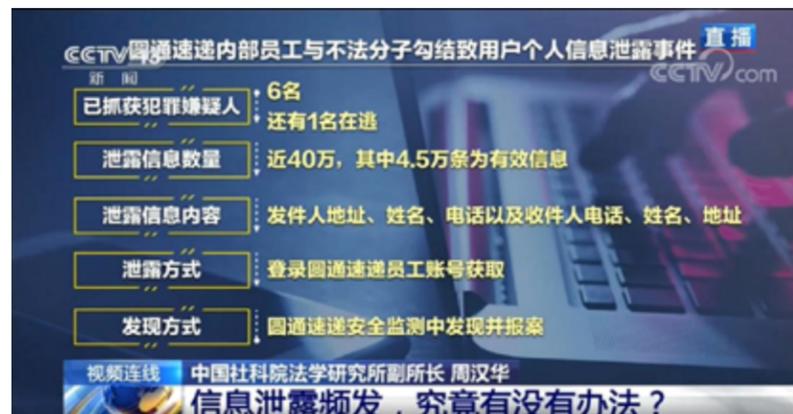
**摘要：**国家邮政局召开一季度例行新闻发布会。国家邮政局将加强对快递数据收集、管理、使用的监管，严肃查处泄露用户信息等违法行为；加快推广信用承诺制度，完善失信行为信息披露机制，对刷单、贩卖快递盲盒等进行清理整顿；狠抓安全监管「三项制度」落实，依托「绿盾」工程加强「互联网++监管」建设，为消费者营造安全的寄递环境。

## 8、银保监会：保险中介机构不得违规向关联企业泄露保单等数据信息



**摘要：**为加强保险中介监管，提高保险中介机构信息化工作与经营管理水平，构建新型保险中介市场体系，推动保险中介行业高质量发展，银保监会近日印发了《保险中介机构信息化工作监管办法》（以下简称《办法》），《办法》的制定出台，将促进保险中介机构加强信息化建设、提高经营管理水平，为加强保险中介领域的事中事后监管、构建新型保险中介市场体系提供有效抓手，在提高风险防范能力的同时，也将推动保险中介行业高质量发展。

## 9、40 万快递数据泄露仅是冰山一角 | 快递业数据资产泄露管控刻不容缓



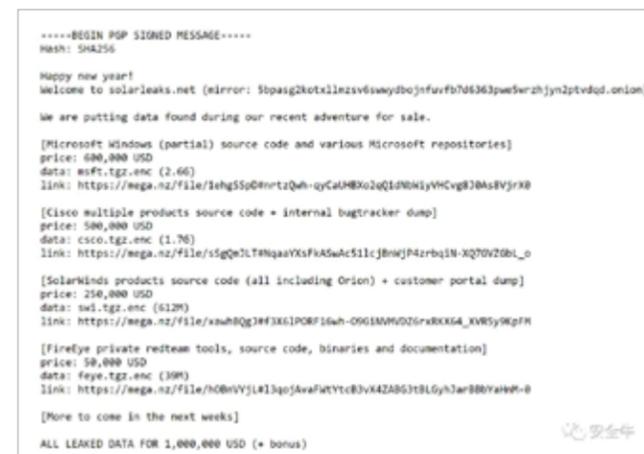
**摘要：**近日，圆通回应内鬼致 40 万条个人信息泄露一事引起了广泛关注。据圆通官方描述，今年 7 月该公司监测到河北省区下属加盟网点有异常查询操作行为，调查后发现疑似个别员工与外部不法分子勾结窃取运单信息，导致信息外泄，并向当地公安报案协助调查，相关犯罪嫌疑人于 9 月落网。

## 10、共享汽车被租后“人车蒸发”成网约车平台前员工泄露关键信息



**摘要：**近日，上海市公安局虹口分局曲阳路派出所，成功破获多起盗用共享汽车从事网约车运营案件，追回被盗车辆 13 辆，车辆总价值近 130 万元，包括被盗车辆驾驶员、共享汽车公司员工等在内共 26 名犯罪嫌疑人因涉嫌盗窃罪被刑事拘留。

## 1、SolarWinds 黑客组织开始销售泄露数据



**摘要：**一个地址为 solarleaks.net 的网站悄然上线，虽然该网站只有一个纯文本页面，但是公布的信息却在网络安全行业引发轩然大波。该网站声称正在出售来自微软、思科、FireEye 和 SolarWinds 的被盗数据。众所周知，所有这些公司都在供应链攻击中遭到入侵。根据网站截图，微软的 Windows 源代码和其他代码库标价 60 万美元，思科多个产品的源代码标价 50 万美元。最先曝光泄露的 FireEye 红队工具标价 5 万美元，而本次供应链攻击的“载体”，SolarWinds 的产品源代码和客户网站拖库数据标价 25 万美元。上述所有泄露数据的打包价格为 100 万美元。

## 2、无孔不入：德国媒体遭受了全国性勒索软件的攻击



**摘要：**德国第三大出版商成为网络攻击的受害者，这次网络攻击影响了其在全国各地的办公室系统。德国媒体（Funke Media Group）发行了数十种报纸（例如 Berliner Morgenpost、Hamburger Abendblatt 和 Bergedorfer Zeitung）、杂志、多家地方广播电台和在线新闻门户。据统计，该公司拥有 300 万的订阅真。

### 3、新西兰央行大量敏感数据泄露：因第三方托管合作商被黑



**摘要：**新西兰中央银行近日表示，某身份不明的攻击者已经成功入侵其内部一个数据系统，并且可能已经访问了商业及个人敏感信息。这家位于新西兰惠灵顿的国家银行在声明中表示，遭到非法访问的是新西兰储备银行用于共享及存储敏感信息的第三方文件共享服务。银行行长 Adrian Orr 表示，违规行为已经得到遏制，该银行的核心职能“仍然保持着健全性及可操作性。” Adrian Orr 说，“我们正与国内外网络安全专家及其他相关机构紧密合作，对此番恶意攻击开展全面调查。”

### 4、美国医疗服务商遭勒索攻击，系统停顿损失数百万美元



**摘要：**据外媒报道，美国佛蒙特州一家医疗服务提供商遭到网络攻击，导致电子健康记录 (EHR) 系统延迟推出，并造成数百万美元的收入损失。总部位于伯灵顿的佛蒙特大学健康网络 (University of Vermont Health Network) 在 2020 年 10 月受到勒索软件的攻击，至今尚未完全恢复。大多数计算机系统已经恢复运行；然而，一些应用程序仍然处于关闭状态，导致了包括放射科在内的各个部门的延迟。该网络服务于佛蒙特州的大部分地区和纽约州北部的部分地区。当攻击者袭击了 6 家网络医院时，佛蒙特州州长菲尔·斯科特 (Phil Scott) 认为情况严重到需要部署佛蒙特陆军国民警卫队的联合网络反应小组来帮助恢复工作。

### 5、网络设备商 Ubiquiti 披露：客户数据遭到未授权访问



**摘要：**据外媒报道，Ubiquiti 是最大的网络设备销售商之一，其销售产品包括路由器、网络摄像头和网状网络。近日，这家公司提醒客户注意数据泄露问题。这家科技公司在周一发给客户的一封简短电子邮件中表示，它意识到第三方云供应商托管的系统遭到了未经授权的访问。

### 6、惨遭“开源”，数百万 Parler 用户数据全部泄露



**摘要：**特朗普的最后社交媒体阵地——美国社交应用 Parler 也被亚马逊、谷歌和苹果公司“拒绝服务”，但本周一更加惊人的消息从 reddit 社区传出，所有 Parler 用户数据（包括参加国会抗议示威活动人员）已经公开暴露，任何人都可查询。



## 7、面对“智能坐垫”、“厕所计时”，员工的个人信息怎么保护？

**摘要：**近日，一位网友发帖爆料称其所在的公司老板为大家配备了“智能坐垫”，能够实时监测心率、呼吸次数、坐姿、疲劳度以及使用时间，当坐姿不端正或使用时间过长时甚至会提醒使用者注意调整坐姿或使用时间。该网友后续还表示公司 HR 找她谈话，询问每天上午 10 点 -10 点半固定时间离开工位的去向问题。此事一出，网友随即表示自己被智能坐垫“监控”了，就连最基本的如厕时间也会被老板监视！本以为这是老板给大家发的福利，但是在与 HR 的对话后，一切好感戛然而止。还有网友表示，有一些公司对员工上厕所时间也有详细的监控。

## 8、新加坡决定追踪疫情的数据可用于刑事调查，引隐私担忧

**摘要：**近日，据媒体报道，新加坡政府表示，根据《刑事诉讼法》，警察有权使用“TraceTogether”应用追踪新冠患者密切接触者的数据，用于刑事调查。此举引发民众对隐私的担忧。据了解，为追踪密切接触者，2020 年 3 月份，新加坡卫生部推出新冠感染源追踪“神器”App——TraceTogether。使用该 App 时，用户需绑定手机号，打开蓝牙，此时该 App 会自动检测 2 至 5 米内的其他用户。如果接触时长超过 30 分钟，App 会互相记录对方的信息。为保护个人隐私，TraceTogether 会为用户注册账号时使用的手机号随机添加一个 ID 值并进行加密。用户彼此交换的信息，只存储在设备本地。超过 25 天，该 App 将自动删除存储的数据。

## 9、美司法部自曝遭俄黑客入侵，超三千个员工邮箱被访问



**摘要：**美国司法部披露，自身是 SolarWinds 事件的少数重大受害者之一。黑客已经启用 SolarWinds 后门实施了第二阶段行动，向司法部内部邮件系统渗透。美国司法部今天证实，SolarWinds 供应链攻击背后的黑客试图入侵其 IT 系统，包括启用 SolarWinds Orion 软件后门中的木马访问权限，借此遍历司法部内部网络、甚至窃取到部分员工的电子邮件账户。

## 10、支付处理公司 Juspay 发生数据泄露：1 亿用户信息在暗网出售



**摘要：**印度支付处理公司 Juspay 超过 1 亿用户的借记卡、信用卡信息在暗网上销售。Juspay 主要为亚马逊、Swiggy、MakeMyTrip 等公司处理支付业务。本次泄露的数据是以数据转储（data dump）的形式，从一个被入侵的 Juspay 服务器中泄露的。Juspay 已经在其官方博客中确认了此次数据泄露事件，并概述了此次泄露事件的细节。在官方博客中写道：“我们很痛心地向您通知，2020 年 8 月 18 日确实发生了一起数据泄露事件。我们部分用户的非敏感掩码卡信息、手机号码和电子邮件 ID 被泄露”。

# 11、7700 万！ Nitro PDF 用户数据库大规模泄露



**摘要** 包含超过 7700 万条 Nitro PDF 用户记录 (电子邮件地址、用户名和密码) 数据库被盗, 昨天已被黑客免费公开泄露。黑客公布的这个 14GB 的泄露数据库包含 77,159,696 条记录, 其中包含用户的电子邮件地址、全名、bcrypt 哈希密码、标题、公司名称、IP 地址以及其他与系统相关的信息。该数据库已经被添加到“Have I Been Pwned”泄露检测服务中, 该服务使用户可以检查其信息是否在数据泄露中暴露。

# 12、美国位置数据公司通过亚马逊平台进行数据售卖



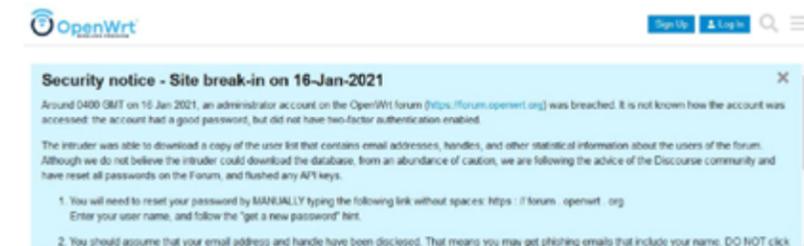
**摘要:** X-Mode Social 是一家成立于 2013 年的美国公司, 总部位于维珍尼亚雷斯顿, 专门从事位置数据的研究。主要通过让 APP 内置其 SDK, 从而进行位置数据收集和分析, 并将其售卖给其他客户, 客户包括美国军事承包商, 该公司从 Muslim Pro 等 (祈祷应用) 中获得了位置数据。而根据研究人员最新发现, X-Mode 公司居然在亚马逊平台上, 公然售卖位置数据, 并且涉及 Covid-19 位置数据, 黑鸟将具体商品截图展示。

# 13、英国国防部个人数据泄露事件同比增加了 18%



**摘要:** 据报道, 英国议会街智库分析的官方数据显示, 2019/20 财政年度, 英国国防部 (MoD) 个人数据丢失事件增加了 18%。英国政府国防部透露, 上个财政年度报告的个人数据丢失事件有 546 起, 高于 2018/19 财年的 463 起。由于其严重性质, 其中 7 起事件已向信息专员办公室 (ICO) 报告。绝大多数 (454 起) 事件记录在未经授权的披露类别下。有 49 个被归类为受保护的政府场所丢失了未充分保护的电子设备, 设备或纸质文件, 另有 19 个报告来自政府场所以外。

# 14、OpenWRT 论坛管理员账号被盗致使用户数据泄露



**摘要:** OpenWRT 是全球最流行的路由器开源操作系统, 而 OpenWRT 论坛作为最大的 OpenWRT 爱好者团体, 近日发生了数据泄露。根据公告, 攻击发生在格林尼治标准时间 (GMT) 04:00 左右, 当时未经授权的第三方获得了管理员访问权限, 并复制了一个列表, 其中包含有关论坛用户的详细信息和相关统计信息。入侵者使用了 OpenWRT 管理员的账户, 尽管该账户具有“良好的密码”, 但是并未启用双因素身份验证 (2FA)。论坛管理员透露, 论坛用户的电子邮件地址已被盗, 但认为攻击者无法下载论坛数据库, 这意味着密码可能是安全的。但是出于安全考虑, 论坛要求所有用户重置密码, 并且撤销了用于项目开发流程的所有 API 密钥。

# 捷报频传！再次荣获百强称号， 亿赛通成功入选网络安全产业百强榜



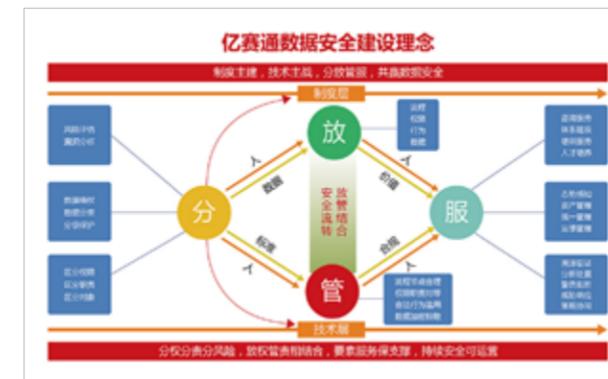
日前，以专业、原创、高端为宗旨的信息安全新媒体嘶吼发布了 2020 网络安全产业百强，亿赛通成功入选 2020 网络安全产业百强企业。

中国网络安全行业 100 强榜单吸引了国内网安产业 300+ 先锋企业积极参与，嘶吼安全产业研究院高级分析师团队根据网安行业市场调研、企业发展策略、影响力、创新能力、融资现状、市值，以及结合网络安全专家指导意见等，多维度综合性总结发布其中全方面领先的 100 个杰出企业。在众多政企领导、业内专家、甲方企业代表以及行业 / 中央媒体的共同见证下，绘制了新趋势下网安行业能力图谱，呈现出中国网络安全行业的核心力量。

亿赛通作为新一代安全技术领军企业，高度重视产品与技术创新工作，开创、繁荣了数据安全蓝海市场，建立了完整的数据安全建设体系，做到分层治理、放心流转、放管结合、运营保障；在产品上，形成安全服务类、审计检测类、加密防护类、安全管理类、安全平台类等五大产品类别，扩充至四十余项产品模块；在业务范围上，亿赛通已经在医疗、地产、芯片半导体、能源等十大行业展开研究与实践，提供专业的数据安全解决方案！

除了五大产品类别，亿赛通在 2020 年提出新的核心亮点。一个项目的实施中，最易被忽略的环节是工程交付，由于数据安全体系的庞杂，终端环境的千差万别，以及安全部门和 IT 部门、业务部门的交叉，导致交付难度的大幅度上升。为此亿赛通贯彻实施了：流程规范、资料完备，交付技术和交付效率，以及服务态度和用户满意度，六项衡量交付效果的指标。目前，公司已在多个行业积累了大量成功案例，并在各类项目实践过程中结合各行业的客户实际需要和应用场景，有效地提升其安全管理工作的效率和质量。

此次入选 2020 网络安全产业百强是业界对亿赛通技术和实力的认可。未来，我们将持续进行数据安全产品的创新与研究，不断创新，与业界同仁共同努力，构筑坚实的数据安全防线！



# 亿赛通两大专业方案斩获实力奖项， 信创布局正当时

**★安全优秀解决方案★**

| 序号 | 方案名称              | 单位名称             |
|----|-------------------|------------------|
| 1  | 基于飞腾平台的可信系统解决方案   | 北京大唐移动通信技术有限公司   |
| 2  | 信创政务云安全解决方案       | 北京神州绿盟科技有限公司     |
| 3  | 信创云租户安全解决方案       | 浪潮云信息技术股份公司      |
| 4  | 深信服信创云安全解决方案      | 深信服科技股份有限公司      |
| 5  | 同神云安全解决方案         | 同神信息技术(北京)股份有限公司 |
| 6  | 信创系统安全防护解决方案      | 华为技术有限公司         |
| 7  | 面向电子政务的信创安全防护解决方案 | 中孚信息股份有限公司       |
| 8  | 云密码资源池            | 神州龙芯智能科技有限公司     |
| 9  | 信息网格边界安全接入解决方案    | 北京安盟信息技术股份有限公司   |

| 序号 | 方案名称               | 单位名称           |
|----|--------------------|----------------|
| 10 | 基于UOS的数据防护解决方案     | 北京明能万达科技股份有限公司 |
| 11 | 基于信创BIOS的安全技术解决方案  | 中电科技(北京)有限公司   |
| 12 | 基于信创BMC的安全技术解决方案   | 中电科技(北京)有限公司   |
| 13 | 信创电子文档安全管理解决方案     | 北京亿赛通科技发展有限公司  |
| 14 | 基于国产CPU的安全技术解决方案   | 海光信息技术股份有限公司   |
| 15 | 基于密钥技术的新一代数据安全解决方案 | 北京烽火网络技术有限公司   |
| 16 | 金融信创数据脱敏解决方案       | 杭州美创科技有限公司     |
| 17 | 数据库安全审计解决方案        | 北京亿赛通科技发展有限公司  |
| 18 | 基于信创浏览器的安全解决方案     | 北京奇虎科技有限公司     |

| 序号 | 方案名称            | 单位名称             |
|----|-----------------|------------------|
| 19 | 湖南麒麟信创云办公解决方案   | 湖南麒麟信安科技股份有限公司   |
| 20 | 基于信创技术通信安全解决方案  | 深圳奥联信息安全技术有限公司   |
| 21 | 金融支付信创安全解决方案    | 北京中科江南信息技术股份有限公司 |
| 22 | 信创终端安全防护解决方案    | 北京奇虎科技有限公司       |
| 23 | 基于安全区的终端安全解决方案  | 成都卫士通信息安全技术有限公司  |
| 24 | 信创终端数据安全解决方案    | 北京明能万达科技股份有限公司   |
| 25 | 基于信创的身份认证安全解决方案 | 飞天诚信科技股份有限公司     |
| 26 | 采云信创安全监测解决方案    | 中国移动通信集团有限公司研究院  |

| 序号 | 方案名称               | 单位名称             |
|----|--------------------|------------------|
| 27 | 隔网同城数据交换安全解决方案     | 杭州云直云计算有限公司      |
| 28 | 中国电信天翼信创OA安全解决方案   | 中国电信集团系统集成有限责任公司 |
| 29 | 统一身份管理与访问控制解决方案    | 北京众源识人科技有限公司     |
| 30 | 智能化IT信息资产风险管理解决方案  | 北京华顺信安科技有限公司     |
| 31 | 网络空间关键信息基础设施检测解决方案 | 北京华顺信安科技有限公司     |
| 32 | 信创数据审计管理解决方案       | 开普云信息科技股份有限公司    |
| 33 | 信创大数据安全管理解决方案      | 智网安云(武汉)信息技术有限公司 |
| 34 | 信创网络安全应急管理解决方案     | 智网安云(武汉)信息技术有限公司 |

\*排名不分先后

1月28日，由国家工业信息安全发展研究中心主办，北京经开区国家信创园、软件融合应用与测试验证工业和信息化部重点实验室协办的“通明湖信息技术应用创新论坛”系列活动之信息技术应用创新安全优秀解决方案线上发布会成功召开。本次发布会中，信息技术应用创新安全优秀解决方案评选结果正式出炉，评选方案征集由国家工业信息安全发展研究中心组织落实。

经过材料征集、形式审查、专家评审、结果审议等环节，亿赛通“信创电子文档安全解决方案”及“数据库审计解决方案”，以优异表现从众多参评解决方案中脱颖而出，成功入选。

我国信息技术应用创新产业发展已进入战略机遇期，信创产业加速发展，自主软硬件产品能力取得较大提升，产业链、供应链正在逐步形成。与此同时，随着产业纵深发展，信创产品安全能力受到了产业界的广泛关注，构建

信创产品安全保障体系正当其时。本次信创安全优秀解决方案的征集与遴选工作，旨在推动优秀典型案例在行业的应用推广，不断提高企业的安全意识和安全检测能力，探索建立产业多方协同机制，将信创产业做深做实，立足长远，积极推进信创产业发展。

## 铸牢数据安全壁垒，赋能信创体系建设

信创产业的蓬勃发展需要各种网络安全技术、产品和服务保驾护航，信创安全也面临着一些新的问题需要克服，一方面是自身弱、对手强、动机多等严重挑战，另一方面是认知偏差、能力不足、积累不足、实战不足等实际情况。因此，信创安全需要新的发展思路，积极利用新技术、新手段开展网络安全保护。

目前，数据安全行业已经有序、稳定的推进信创工作，从基础架构到应用架构。由于其对业务的连续性和高稳定性要求，各个层次的改造都需要考虑安全风险，同时由于涉及

到众多的操作系统、国产芯片、版本，信创安全产品的兼容性是需要考虑的重点因素。长期以来，亿赛通践行创新理念，为客户提供专业的数据安全产品，助力企业用户解决数据安全防护的关键难点，以多重安全能力深植数据全生命周期各个环节和业务场景，夯实安全基础。近年来，随着国家高度重视信创产业发展，出台各项政策，亿赛通紧跟国家在核心技术创新方面的步伐和企业用户在国产化数据安全产品诉求，持续推进信创安全产品的研发和应用。为积极支持国家信创产业发展，亿赛通电子文档安全管理系统及数据库审计系统早已先后完成与统信软件、达梦、中国长城科技集团等厂商兼容适配。

## 电子文档安全管理解决方案



亿赛通电子文档安全管理系统基于文件过滤驱动技术，通过对用户“有意”、“无意”的泄露行为做统一防护，融合“加密敏感数据”、“控制敏感内容流通”、“规范员工访问行为”为主体的核心技术，配合身份识别、权限控制、终端管理、应用集成、安全接入以及行为审计等功能，形成一整套适合国内数据安全现状及管理目标的全新解决方案。

方案满足客户在办公中对于文档管理、共享、外发等方面的需求，满足企业信息化、移动化、智能化建设的发展性需要，助力行业用户全面应对跨地域协作与海量文档数据的安全挑战。

## 数据库审计解决方案



亿赛通数据库安全审计系统通过对数据库网络流量的旁路采集，基于数据库协议解析和SQL语句还原技术的数据库安全审计系统。本系统实现对数据库所有访问行为的监控和审计，并对其中的危险操作可通过多种方式进行告警提醒。系统对数据库历史访问行为进行多维度的统计分析，并利用丰富图表进行可视化展现。

## 聚力加速布局信创数据安全

亿赛通作为国内领先数据安全厂商，全线安全产品积极进行信创适配，已覆盖电子文档安全管理系统、数据泄露防护系统、数据库审计、数据脱敏、数据库防火墙等系列产品。未来，亿赛通将继续拓宽生态体系建设，加强技术攻坚，推动信创产业的高质量发展。

# 新规 | 金融行业再添新政策， 数据安全必不可少



国家大力推行数据安全，各行业根据行业特点推出针对性条例，近日，银保监会印发《中国银保监会监管数据安全管理办法（试行）》（以下简称办法），旨在切实加强监管数据安全，防范监管数据安全风险。

办法所称监管数据安全是指监管数据在采集、处理、存储、使用等活动（以下简称监管数据活动）中，处于可用、完整和可审计状态，未发生泄露、篡改、损毁、丢失或非法使用等情况。受银保监会委托或委派，为银保监会提供监管数据采集、处理或存储服务的企事业单位适用于本办法。

## 数据的采集、存储和加工处理

### 数据的采集

按照安全、准确、完整和依法合规的原则进行，避免重复、过度采集。

### 数据的监管

通过监管工作网或金融专网进行传输。因客观条件限制需要通过物理介质、互联网或其它网络传输的，应经归口管理部门评估同意。

### 数据的存储

存储在银保监会机房，并具有完备的备份措施。

### 数据的加工

应在监管工作权限或受托范围内进行。未经归口管理部门同意，任何单位和个人不得将代码、接口、算法模型和开发工具等接入监管信息系统。

监管数据采集、传输、存储、加工处理、转移交换、销毁，以及用于系统开发测试等活动，应根据监管数据类型和管理要求采取分级分类安全技术防护措施。

## 监控数据安全的要求

- 监管数据的使用行为应通过管理和技术手段确保可追溯。监管数据用于信息系统开发测试以及对外展示时，应经过脱敏处理。

- 使用未公开披露的监管数据，原则上应在不可连接互联网的台式机或笔记本等银保监会工作机中进行。因客观条件限制需采取虚拟专用网络等方式使用监管数据时，应经归口管理部门评估同意。

- 因工作需要下载的监管数据，仅可存储于银保监会的工作机中。承载监管数据的使用介质应妥善保管，防止数据泄露。

## 各部门应急处置措施得当

各业务部门及受托机构发生以下监管数据重大安全风险事项时，应立即采取应急处置措施，及时消除安全隐患，防止危害扩大，并于 48 小时内向归口管理部门报告。

- （一）监管数据发生泄露或非法使用；
- （二）监管数据发生损毁或丢失；
- （三）承载监管数据的信息系统或网络发生系统性故障造成服务中断 4 小时以上；
- （四）承载监管数据的信息系统或网络遭受非法入侵、发生有害信息或计算机病毒的大规模传播等破坏；
- （五）监管数据安全事件引发舆情；
- （六）《网络安全重大事件判定指南》列明的其他影响监管数据安全的网络安全重大事件。辖区发生以上监管数据重大安全风险事项时，各银保监局应立即采取补救措施，并于 48 小时内向银保监会归口管理部门报告。

办法的出台在指导并加强监管数据安全，防范监管数据安全风险。亿赛通作为“中国数据安全专家”，通过全新的“分·放·管·服”数据安全建设理念，结合金融数据安全解决方案，为客户提供全方位的数据安全防护体系，提供真正意义上的全生命周期数据安全。

新闻内容来源于银保监会

## 网络从不是法外之地 | 从新冠确诊患者“网暴”看信息泄露



转眼间，已经进入 2021 年。近期疫情的再度来袭，给寒冷的冬天铺上了一层冰。只不过和以往不一样的是，近期的几起病例离奇地在网上卷起了轩然大波。同时，也让小亿亲眼目睹了一场和病毒同样可怕的网络暴力。

日前，在北京市新型冠状病毒肺炎疫情防控工作第 201 场新闻发布会上，发言人介绍，警方在近期的工作中发现，有个别违法人员趁机侵犯公民隐私。

顺义警方接群众报警：其家人信息在多个微信群中泄露传播，对生活和工作造成影响。经警方调查，某航空安保有限公司员工刘某（男，41 岁）在工作期间，将用于筛查密接人员工作的患者初步流调报告，私自拍摄并发至微信群内，导致患者及其家属、同事的姓名、身份证号码、家庭住址、工作单位、手机号码等隐私泄露。顺义公安分局依法对刘某处以行政拘留处罚。



### 疫情以来已出现多起患者个人信息泄露

今年疫情以来国内已出现多起确诊患者及其亲属个人信息泄露的事件：

•2020 年 2 月 21 日，宁波公布新增一例新冠肺炎病例，患者孙某，住宁波市北仑区。而在此之前，关于该患者及其亲属的详细信息在当地微信群中传播，共涉及 16 人，泄露的信息包括姓名、身份证号、家庭住址等。

•2020 年 11 月 20 日，天津市疾控中心报告了瞰海轩小区接连发现 8 名新冠病毒感染者，其中 5 名确诊病例，

3 名无症状感染者。11 月 19 日晚，部分确诊患者和其家人的详细信息和 14 天全部行程，在社交媒体上流传开来，有患者家属反映遭到频繁的电话骚扰。

•2020 年 12 月 8 日上午，成都公布新增 3 例新冠肺炎确诊病例的行动轨迹。其中疑似确诊患者赵某的姓名、身份证号、家庭住址等个人信息在网络平台上流传。

当舆论监督变成了舆论审判，模糊了道德和法律的界线，就会侵犯到他人的合法权益而不得知，还在沾沾自喜，指手画脚。这都是不可取的，新冠确诊，相信政府会采取有效措施隔离确诊者，大范围排查，不久就能回复往常，不要再针对确诊患者，甚至违法了还不得知。

亿赛通医疗行业解决方案为客户提供专业的安全防护手段，保障医疗行业在工作过程中的核心数据安全。除了在一线的医护人员外，我国大量的信息安全专家在这场疫情中，也为隐藏在暗处的网络战争而战斗，逆境之中，我们一直在一起。

# 盘点 | 风起云涌的 2020，数据泄露到底有多疯狂？

2020 年，新冠疫情肆虐全球，催化各行业加速数字化转型，数据的价值在进一步凸显，全球数据的数据泄露也在持续高频发生，企业面临资产与声誉的重大损失，公众深受隐私曝光与骚扰诈骗的困扰。现在，和亿赛通一起回顾 2020 年重大数据泄露事件，看看数据泄露到底有多疯狂？

## “数据泄露索引”网站泄露 23600 个被入侵的数据库

11 月 6 日，大名鼎鼎的数据泄露索引网站 Cit0Day.in 泄露了 23600 个被黑的数据库。该网站收集被黑客入侵的数据库，向其他黑客提供访问权限，包括：用户名、电子邮件、地址、明文密码等。但目前，网站中的全部数据被公开到暗网上，约 130 亿条记录。



## NordPass 称有上万个配置错误的数据库泄露 100 亿条记录

8 月 4 日，NordPass 发现了近万个配置错误的数据库，泄露了 105 亿条来自 20 个国家和地区的数据。据统计，泄露数据最多的三个国家中，法国以 51 亿条位居榜首，中国以 26 亿条紧随其后，美国以 23 亿条位居第三。这些泄露数据库通常包括电子邮件地址，密码和电话号码。



## 泰国最大的移动运营商泄露 83 亿条用户数据记录

5 月 27 日，泰国移动运营商 AIS 的 ElasticSearch 数据库暴露在公网上，泄露 83 亿条记录。此次泄露事件影响了数百万名用户，泄露 4.7 TB 数据。研究人员在公共网络上发现该数据库，并且无需密码即可访问，包括查询 DNS 和 Netflow 数据。

| Name              | Health | Status | Primary | Replicas | Size (bytes) | Storage size |
|-------------------|--------|--------|---------|----------|--------------|--------------|
| shv-2020-05-02-01 | green  | open   | 3       | 1        | 114483610    | 25.0gb       |
| shv-2020-05-04-03 | green  | open   | 3       | 1        | 48814513     | 10.0gb       |
| shv-2020-05-04-10 | green  | open   | 3       | 1        | 48813802     | 10.0gb       |
| shv-2020-05-04-18 | green  | open   | 3       | 1        | 45713040     | 10.0gb       |
| shv-2020-05-04-25 | green  | open   | 3       | 1        | 43718868     | 10.0gb       |
| shv-2020-05-04-21 | green  | open   | 3       | 1        | 43814871     | 10.0gb       |
| shv-2020-05-05-01 | green  | open   | 3       | 1        | 41448018     | 14.7gb       |
| shv-2020-05-05-02 | green  | open   | 3       | 1        | 40716676     | 14.3gb       |
| shv-2020-05-08-22 | green  | open   | 3       | 1        | 50480154     | 14.7gb       |
| shv-2020-05-07-12 | green  | open   | 3       | 1        | 58374402     | 14.7gb       |
| shv-2020-05-07-13 | green  | open   | 3       | 1        | 58214642     | 14gb         |
| shv-2020-05-04-17 | green  | open   | 3       | 1        | 58213546     | 14.0gb       |
| shv-2020-05-07-11 | green  | open   | 3       | 1        | 58742330     | 13.7gb       |
| shv-2020-05-07-03 | green  | open   | 3       | 1        | 58602802     | 13.7gb       |
| shv-2020-05-04-15 | green  | open   | 3       | 1        | 58213232     | 13.7gb       |
| shv-2020-05-04-16 | green  | open   | 3       | 1        | 58113248     | 13.7gb       |
| shv-2020-05-07-05 | green  | open   | 3       | 1        | 58982817     | 13.7gb       |
| shv-2020-05-07-02 | green  | open   | 3       | 1        | 55740180     | 13.0gb       |
| shv-2020-05-08-10 | green  | open   | 3       | 1        | 54883708     | 13.7gb       |

## 德国购物网站 windeln.de 数据库暴露，泄露 60 亿条记录

9 月 18 日，研究人员在网上发现了一个暴露的数据库，属于德国在线购物网站 windeln.de。网站暴露了 6.4TB 的数据，其中包含 60 亿条记录，泄露了超过 700000 名客户的个人信息。此次事件的泄露信息包括个人身份信息 (PII) 和其他数据，例如发票、全名、IP 地址、内部日志、电话号码、电子邮件地址、家庭地址、密码、付款方式和用户的孩子个人信息等。



## Keepnet Labs ES 实例泄露超过 50 亿条记录

3 月 23 日，英国安全厂商 Keepnet Labs 的一个 Elasticsearch 实例泄露了超过 50 亿条数据记录，这些记录是 2012 年至 2019 年之间发生的泄露事件中的记录。该数据库由两个集合组成，一个包含 50.88 亿条记录，而另

一个实时更新的集合则包含超过 1500 万条记录。泄露的记录包括哈希类型、泄露年份、密码（哈希、加密或明文格式）、电子邮件、电子邮件域名以及泄露源（包括 Adobe、Last.fm、Twitter、LinkedIn、Tumblr 和 VK 等）。

| id | hostname     | ipaddress    | password     | username | email              | domain       | source       |
|----|--------------|--------------|--------------|----------|--------------------|--------------|--------------|
| 1  | 192.168.1.1  | 192.168.1.1  | admin:admin  | admin    | admin@192.168.1.1  | 192.168.1.1  | 192.168.1.1  |
| 2  | 192.168.1.2  | 192.168.1.2  | root:root    | root     | root@192.168.1.2   | 192.168.1.2  | 192.168.1.2  |
| 3  | 192.168.1.3  | 192.168.1.3  | user:user    | user     | user@192.168.1.3   | 192.168.1.3  | 192.168.1.3  |
| 4  | 192.168.1.4  | 192.168.1.4  | test:test    | test     | test@192.168.1.4   | 192.168.1.4  | 192.168.1.4  |
| 5  | 192.168.1.5  | 192.168.1.5  | admin:123456 | admin    | admin@192.168.1.5  | 192.168.1.5  | 192.168.1.5  |
| 6  | 192.168.1.6  | 192.168.1.6  | root:123456  | root     | root@192.168.1.6   | 192.168.1.6  | 192.168.1.6  |
| 7  | 192.168.1.7  | 192.168.1.7  | admin:123456 | admin    | admin@192.168.1.7  | 192.168.1.7  | 192.168.1.7  |
| 8  | 192.168.1.8  | 192.168.1.8  | root:123456  | root     | root@192.168.1.8   | 192.168.1.8  | 192.168.1.8  |
| 9  | 192.168.1.9  | 192.168.1.9  | admin:123456 | admin    | admin@192.168.1.9  | 192.168.1.9  | 192.168.1.9  |
| 10 | 192.168.1.10 | 192.168.1.10 | root:123456  | root     | root@192.168.1.10  | 192.168.1.10 | 192.168.1.10 |
| 11 | 192.168.1.11 | 192.168.1.11 | admin:123456 | admin    | admin@192.168.1.11 | 192.168.1.11 | 192.168.1.11 |
| 12 | 192.168.1.12 | 192.168.1.12 | root:123456  | root     | root@192.168.1.12  | 192.168.1.12 | 192.168.1.12 |
| 13 | 192.168.1.13 | 192.168.1.13 | admin:123456 | admin    | admin@192.168.1.13 | 192.168.1.13 | 192.168.1.13 |
| 14 | 192.168.1.14 | 192.168.1.14 | root:123456  | root     | root@192.168.1.14  | 192.168.1.14 | 192.168.1.14 |
| 15 | 192.168.1.15 | 192.168.1.15 | admin:123456 | admin    | admin@192.168.1.15 | 192.168.1.15 | 192.168.1.15 |
| 16 | 192.168.1.16 | 192.168.1.16 | root:123456  | root     | root@192.168.1.16  | 192.168.1.16 | 192.168.1.16 |
| 17 | 192.168.1.17 | 192.168.1.17 | admin:123456 | admin    | admin@192.168.1.17 | 192.168.1.17 | 192.168.1.17 |
| 18 | 192.168.1.18 | 192.168.1.18 | root:123456  | root     | root@192.168.1.18  | 192.168.1.18 | 192.168.1.18 |
| 19 | 192.168.1.19 | 192.168.1.19 | admin:123456 | admin    | admin@192.168.1.19 | 192.168.1.19 | 192.168.1.19 |
| 20 | 192.168.1.20 | 192.168.1.20 | root:123456  | root     | root@192.168.1.20  | 192.168.1.20 | 192.168.1.20 |

## Whisper 数据库可公开访问，泄露约 9 亿条记录

3 月 12 日，匿名秘密共享应用 Whisper 由于数据库可公开访问，导致约 9 亿条记录泄露。数据库中存储的数据是从 2012 年该 APP 发布一直到现在的所有数据。尽管记录中不包含用户名，但其中包含昵称、年龄、种族、性别、家乡、团体成员关系以及与发帖相关的位置数据。



## 雅诗兰黛泄露 4.4 亿数据记录

2 月 13 日，雅诗兰黛因一个数据库未设密码，导致 4.4 亿条记录泄露，其中包括纯文本电子邮件地址（包括来自 @estee.com 域的内部电子邮件地址）和 CMS、中间件的日志内容。但记录中没有包含客户的付款数据或敏感的员工信息。

Searched 1209 of 1209 shards. 440339996 hits. 2.656 seconds

| visualization.title                  | visualization.visState                    |
|--------------------------------------|---|
| [eCommerce] Sales by Category        | {\"title\": \"[eCommerce] Sales by Ca     |
| [eCommerce] Sales by Gender          | {\"title\": \"[eCommerce] Sales by Ge     |
| [eCommerce] Markdown                 | {\"title\": \"[eCommerce] Markdown\",     |
| [eCommerce] Controls                 | {\"title\": \"[eCommerce] Controls\", \"t |
| [eCommerce] Promotion Tracking       | {\"title\": \"[eCommerce] Promotion T     |
| [eCommerce] Total Revenue            | {\"title\": \"[eCommerce] Total Reven     |
| [eCommerce] Sold Products per Day    | {\"title\": \"[eCommerce] Sold Produc     |
| [eCommerce] Average Sales Price      | {\"title\": \"[eCommerce] Average Sell    |
| [eCommerce] Average Sold Quantity    | {\"title\": \"[eCommerce] Average Sol     |
| [eCommerce] Average Sales Per Region | {\"title\": \"[eCommerce] Average Sell    |
| [eCommerce] Top Selling Products     | {\"title\": \"[eCommerce] Top Selling     |

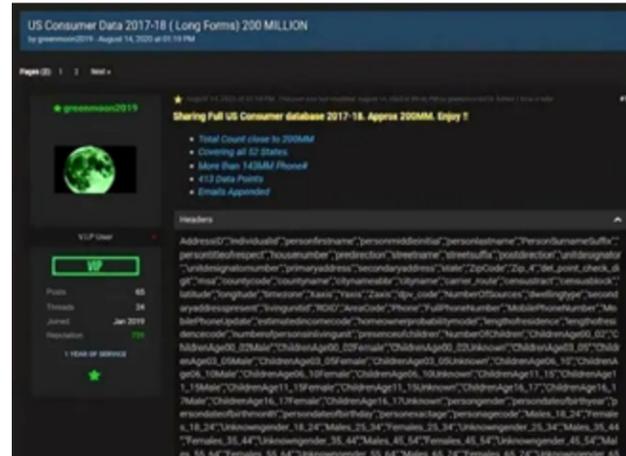
### 黑客在暗网公开 wattpad 的 2.7 亿条用户数据

7月7日起，暗网以十个比特币的价格出售包含2亿多条记录的 Wattpad 数据库。该数据库的记录包含用户名、名称、哈希密码、电子邮件地址和一般地理位置。通过与泄露数据的用户联系，可以确认列出的信息是准确的。



### 黑客在暗网出售美国超 2 亿选民数据

10月27日，黑客在暗网出售了超过2亿美国人的个人识别信息，包括姓名、电子邮件地址、电话号码和选民登记记录等。这些数据是由近年来企业遭到各种攻击所泄露的数据以及从政府网站检索的公开数据组成的，可用于社交媒体、电子邮件网络钓鱼以及文本和电话诈骗活动和虚假信息宣传活动。



### 巴西公司 Natura 数据库暴露泄露 1.92 亿条用户信息

5月21日，Natura 暴露了两个配置错误的 AWS 数据库长达数周之久，泄露了 1.92 亿条用户信息。此次泄露的是在该公司网站购物的超过 25 万名客户的信息，包括用户性别、姓名、国籍、出生日期、电话号码、以前购买记录、MOIP 帐户详细信息、母亲的姓、邮件欢迎模板、用户名和昵称、电子邮件地址、实际地址、用于 wirecard.com.br 的访问令牌、API 凭证（包括未加密的密码）、Natura.com.br 登录凭证（包括哈希密码）。



如何在互联网发展的大潮下同时确保数据安全，已经成为全世界普遍关注的焦点问题。亿赛通作为中国数据安全专家提醒大家，无论企业或个人一定要意识到数据安全保护的重要性，提早采取防护措施。未雨绸缪，防患未然！

文章资讯来源于互联网

# 勒索不成恼羞成怒，公开电器巨头“背后的秘密”

近日，勒索软件瞄准电器企业，某电器巨头遭遇黑客组织攻击，因该公司拒付赎金，导致黑客将窃取的数据发布至公共平台。

惠而浦公司于近日遭到勒索恶意软件攻击，幕后黑客 Nefilim 勒索软件，在其网站上发布了（Whirlpool）惠而浦公司的部分数据，包括员工福利、住宿要求、医疗信息及其他相关信息。

黑客表示：“数据泄露归咎于 Whirlpool 惠而浦公司高管不愿维护公司员工的利益支付赎金，并且其网络安全防护非常脆弱，这使得我们在谈判失败后进行第二次攻击活动。”



就所有勒索事件来看，电器、芯片半导体等行业一直深受黑客青睐，哪怕产品研发技术再先进，也难挡黑客攻击，由此来说，企业更应重视自身的安全防护。研发是一个极为复杂的过程，由于其中涉及不少复杂的数据信息，多个环节的协调不可避免要与网络相连接，这也给黑客提供了便利。

亿赛通文件防火墙是为防止勒索病毒对企业或个人的核心文件进行攻击，主要是对文件进行保护，不允许非法进程访问受保护的文件夹，防止非授权进程如病毒、木马、勒索软件等对指定文件类型或路径下文件的篡改、破坏和窃取。

### 1、智能学习

自主选择需保护目录进行学习，可学习到被保护目录下文件的合法访问进程及文件路径信息。

### 2、数据防护

通过学习到的合法进程访问相应路径下的文件，生成文件防护策略；

启动防护后，软件将对被保护路径下的文件进行防护；

如检测到非法进程访问被保护目录下文件，文件防火墙立即拒绝应用进程的访问，并记录违规访问记录；

拒绝未在学习范围内的合法进程的访问，可根据违规记录进行过滤；

对指定的文件类型或目录只能被指定的进程访问，其它进程不能访问。

数据作为信息化建设的主机，其重要性不言而喻，对于企业来说更要对网络病毒攻击打起万分警惕，才能保证产业链的正常运转。欲了解亿赛通文件防火墙产品详情，请拨打：400-898-1617。

# 原来还能这样牟利， 运营商行业数据安全 迎来新挑战

在这之前，宝宝先来张这样的照片



实在看不下去了，能不能别裸啦!!!

# 营业厅看到详细上网数据 #

词条迅速登上热搜，原来营业厅可以看到这么详细的上网数据!

除此之外，手机卡、银行卡、甚至你的身份证号，都被记录在册。

小编不禁害怕，如此庞大的数据，被泄露会发生什么?



我的天呐



近日，多名广东运营商“内鬼”，通过盗用他人信息获利，警方根据线索抓获 11 人，查获两处代营点，由于总公司对营业点有业绩指标要求，未达标会被处罚。员工为了完成指标赚取绩效奖金，在未征得客户同意的情况下，私自盗取他人信息完成业绩任务，后续一临时员工在网上与人联系后，将手机卡以 80 元一张卖出获利，警方对涉案 9 人进行刑事拘留，2 人教育训诫处理。

## 运营商行业威胁与日俱增

近年来，运营商行业随着信息安全管控点正在经历从网络安全到内容安全的转变，如何防止内部敏感数据、隐私信息泄露成为安全防护的重点。企业为了更好的提升员工的工作效率，不可避免地扩展了数据泄露的通道，尤其是内部员工能轻易获取客户信息使得企业防不胜防。同时，在行业竞争日益激烈的市场中，难免会有间谍、黑客攻击企业重要数据资料，运营商的数据安全威胁与日俱增。

## 敏感数据识别难

- 1) 业支系统数据量大，数据关系复杂，难以进行梳理；
- 2) 无法判断出哪些数据是重要的；
- 3) 大量的结构化、半结构化、非结构化数据难于辨识；
- 4) 缺乏对数据内容的分类和敏感级别分级；
- 5) 保护措施无法和敏感重要级别挂钩，保护效能和效率较低；

## 敏感数据定位难

- 1) 对于重要敏感的数据存放位置无从知晓，保护难以下手；
- 2) 数据可能存放在电脑、手机、笔记本、业务系统、数据库、存储中；

- 3) 无法明确某类敏感数据在公司的整体分布情况；
- 4) 缺乏对不同数据在不同位置的风险评估视图；

## 重要数据防护难

- 1) 现有的以加密为主的防护覆盖范围小，因加密导致业务连续影响；
- 2) 以 DRM 方式为主的手动加密方式用户主动性差，容易防护失效；
- 3) 从网络、系统、终端多个维度都在管理，防护难以实现紧耦合；
- 4) 重要敏感的少部分核心数据缺乏整个流通通路的监控审计。

亿赛通专业方案可以支持域同步，将组织架构和人员从业务系统中导出，通过安全准入网关对数据库系统采用准入，非公司人员无法下载文档的同时能够对文档实现“下载加密”功能，保证了数据的使用安全。通过外发插件有效管理，解决了业务往来中的外发文档泄密的担忧。该系统可以记录文档、操作、系统等丰富的日志行为，实现对日常行为的审计，方便管理员查看近期情况，提高员工的保密意识。通过解决方案对运营商行业的核心数据和业务系统的数据泄露风险进行管控，将有效增强数据泄密力度，为企业核心数据安全运行提供了强有力地保障。



# 医疗行业数据安全解决方案

## 一、行业背景

“互联网+医疗”、“智慧医疗”等新兴产业强势进入医疗行业各个环节，高效的信息交互提供了医疗系统的办公效率，同时在数据安全方面也面临巨大的挑战。移动医疗、AI 医疗影像、电子病历等等数字化程序的普及，使大量个人信息、医疗数据被窃取售卖用于推销，内部人员造成的官方遗嘱和处方的泄露也让医院造成极大的经济损失。而且，一些医药公司紧随其后，大力发展信息化办公的同时，如何保护核心医药技术资产已经成为不少医药企业的重点关注。

《关于印发国家健康医疗大数据标准、安全和服务管理办法（试行）的通知》正式下发，医疗行业互联网安全生态产业的数据安全从数据分类分级、分级管理、身份认证、审计溯源四大方面都做出了明确指引。

## 二、医疗数据安全风险分析

1) 由于医疗数据的个体价值巨大，医生或者护士只需简单地获得权限之内的数据就可以获得巨大收益。终端对

个人的身份认证及访问审计是内部人员泄密的一大风险；

2) 在医疗行业，业务系统一般依托于软件开发厂商的服务和外包运维人员来开发和管理，医疗系统和数据对第三方厂商也存在着泄露的风险。

3) 医患关系冲突事件加剧，医嘱相关资料的防篡改、防销毁达到有效的溯源取证防抵赖也是数据安全建设的必要环节。

4) 外部攻击风险，由于医疗数据有着得天独厚的价值，从而很容易引起大量黑客攻击行为。

5) 医药核心技术资料容易泄露，对企业经济造成极大损失。

## 三、解决方案

### 1、数据安全准入网关

通过软硬一体化结合的方式为应用系统提供安全保障，应用安全网关可以为应用系统提供安全准入和数据加解密双重防护，安全准入通过终端身份识别、应用系统仿冒、传输

隧道加密等多方面进行应用数据安全访问控制，数据加密通过对医疗业务核心数据进行下载自动加密，解决医疗机构核心数据易泄露、被篡改、非法访问的安全问题。



### 2、数据分级管控

依照《关于印发国家健康医疗大数据标准、安全和服务管理办法（试行）的通知》相关数据安全要求，必须对数据分类分级管理，通过“密级标识”、“透明加密”及“权限管控”模块，实现根据数据价值等级，自动进行分级管控。对高价值等级的数据，例如制药配方、关键医疗科研成果等，进行严格的权限管控，防止泄密的同时，限制其在医院内部的使用范围；对于一般价值等级的数据，例如医嘱、处方、个人信息等进行加密管控、防止泄露后对医院及病患造成损失；对于可公开的文件，选择不对其进行管控，满足业务使用需求，平衡安全与效率。



## 四、方案收益

1. 建设先进、自主、灵活、全面、智能的立体化数据安全防护体系；
2. 建设满足合规要求的分级分类数据保护管理体系；
3. 提供身份访问控制安全和审计溯源管理；
4. 提供可有效降低泄密风险，提升防护能力，提升监管能力的技术体系；
5. 提供可有效提升企业数据安全审计、管理、风险分析的可视化管理平台；
6. 提供高效、全面、完整、规范的数据安全运营服务。

# 江苏豪森药业集团有限公司



## 客户简介

豪森药业成立于 1995 年，是在中国排名前列的研发驱动型制药公司。二十余年来，始终秉承“做优民族医药，做强中国创造”的企业使命，致力于在中国市场临床需求缺口巨大的中枢神经系统、抗肿瘤、抗感染、糖尿病、消化道和心血管等六大领域的创新发展。欧兰宁、普来乐等八种主要产品在多方治疗领域占据市场领先地位。公司建有两个研发中心，分别位于连云港和上海，拥有研发人员 1200 多名，拥有多个国家级研发称号，包括国家级技术中心、博士后科研工作站及国家重点实验室。

## 需求背景

随着豪森药业的大步伐扩张，积累了太多重要的关于核心知识产权的文档，如像企业的客户信息、药品研发数据、生产数据和运营信息等等，组织不希望这些价值资料离开内部网络环境，甚至不允许在网络外部传递与交流。但现代组织不能拒绝互联网的交互，不能将机构封闭在一个信息孤岛。而员工在上传下载和发行网络中文件的同时，可能会有意或无意将组织的许多重要信息流通到网络外部，从而使重要的知识产权受到安全威胁。

## 解决方案

1. 文档安全管理系统：可以实时记载用户对文件的操作记录；可以根据用户的需要设置不同的安全级别；对于需要打印的文件强制在打印界面加载打印时间、IP 地址及用户信息；文件加解密过程均自动完成，对用户完全透明；文件从制作完成到生命结束都是以密文形式等，防止文档信息泄密。

2. 文档加密安全网关：可使从豪森药业应用系统上下载下来的文件带有权限，在企业内部可自由使用，泄露到企业外部无法使用。该权限文件分为可解密文件和不可解密文件两类，其中，可解密文件由内部人员解密时，需提交解密理由并通知相关人员，同时留下解密日志。不可解密文件只能由指定专人进行解密。

## 项目成果

通过以上防范手段，不仅为豪森药业各业务部门部署合理的数据安全防护体系，同时使得该集团相关业务流程更为合理化、流程化、规范化。在数据传输上既保证了内部业务网络较高的可用性、可靠性、保密性，又对内部核心数据有较强的防御和管控能力。

# 黑龙江珍宝岛药业股份有限公司



## 客户简介

黑龙江珍宝岛药业股份有限公司是致力为人类健康提供优质产品与服务的大型上交所上市企业。企业坚持以“平台，合作，共享，共赢”为发展理念；以“创新创造、高质发展”为经营总目标，经过 20 余年的科学管理与稳健发展，现已形成了集科技研发、制药工业、中药产业、金融投资四大主导产业为一体的国际化全产业链大健康产业集群企业。

## 需求背景

随着珍宝岛药业企业信息化的发展，电子文档已成为公司在行业内竞争力保障资源，在公司的运营和发展中有着举足轻重的作用，为加强和规范公司的电子文件管理，保护公司的利益不受侵害成为珍宝岛药业迫切需要解决的问题。建立一个电子文件加密系统，在保证足够的安全水平和良好性能的情况下，使公司电子文件得到有效的保护。

## 解决方案

亿赛通电子文档安全管理系统：以数据透明加密技术为核心，对于核心数据，需要控制数据过程使用安全时，采用透明加密控制方式控制数据的安全使用，实现内容安全防护、安全浮水印、统一身份认证、离线办公安全、日志审计等功能，确保文件内容不会因为文件数据体扩散而扩散。

## 项目成果

珍宝岛药业在部署亿赛通加密产品后，在不影响员工工作效率的基础上，使得文档信息顺畅交流，强有效的保护电子文件信息的保密性、安全性和可用性；实现应用系统运行稳定、使用方便、管理集中、恢复快捷，提供企业科研、生产、办公各环节的电子文件安全保障。