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

关注官方微信公众号

关注官方微信服务号

关注官方微信视频号

关注官方抖音号

亿赛通 ESAFENET

ESAFENET

亿赛通企业月刊　　中国数据安全专家　　www.esafenet.com

08 月刊

2023 年共 12 期

Esafenet
Monthly magazines

中国数据安全专家

主办：亿赛通市场部

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

目录 CONTENTS

刊首语 PREFACE

2/3 《亿赛通八月刊》剖析汽车行业痛点，助用户解决数据安全危机

行业聚焦 INDUSTRY FOCUS

4-8 国内行业新闻

9-13 国外行业新闻

亿赛通动态 ESAFENET NEWS

14/15 亿赛通总经理受聘为工信部数据安全重点实验室第一届学术委员会委员

16/17 亿赛通亮相 2023 商用密码大会，北京市密码管理局领导莅临展位参观指导

18-20 亿赛通出席南昌市医疗行业数据安全座谈会，合力打造医疗行业深层堡垒

20-22 亿赛通入选《中国数据安全防护与治理市场研究报告（2023）》

23 数据安全能力培训即将开班，帮您实现一次培训拿双证

亿赛通小贴士 ESAFENET PROMPT

24-28 从安全技术视角了解《中国人民银行业务领域数据安全管理办法（征求意见稿）》

28/29 咨询服务 | 企业为什么要开展数据安全风险评估？怎么开展？

30/31 政策速递 | 网信办发布《人脸识别技术应用安全管理规定（试行）》（征求意见稿）

32/33 安全随行 | 智能汽车时代，如何构筑汽车数据的安全围墙？

34/35 数据安全治理：打好安全管理与安全技术的协同之战

36/37 又一高校发生数据泄露事件！罚款 80 万！

38/39 《孤注一掷》火爆热映，揭示了信息泄露的残酷一幕

40/41 信息安全无小事 | 如何防范才能不做“透明人”？

典型案例 TYPICAL CASES

42/43 厦门海辰新能源科技有限公司

44/45 欣旺达电动汽车电池有限公司

刊首语

刊首语 PREFACE

《亿赛通八月刊》剖析汽车行业痛点，助用户解决数据安全危机

近年来，数据泄露往往伴随着企业大量的商业损失、声誉下降，使企业逐渐意识到数据安全防护的重要性与紧迫性。以汽车行业为例，随着智能汽车、新能源汽车的上市，汽车行业开始与数据深度绑定，这给车企带来了多维度的安全挑战，如：车辆数据风险、办公数据风险、业务系统数据风险、跨境数据风险等。在一项有关智能汽车数据安全和个人隐私意识的调查报告中，数据表明 94.6% 受访消费者倾向于选择注重数据安全保护的汽车品牌。值得注意的是，其中 54.6% 的消费者表示一定会购买数据安全保障能力强的品牌。这表示数据安全对于汽车行业的发展有着极其重要的战略意义，同时数据安全也是支撑行业健康可持续发展的坚实基础。本期《亿赛通八月刊》从专业视角分析汽车行业的安全痛点，利用自身经验，为汽车行业用户提供数据安全重要参考。

国内

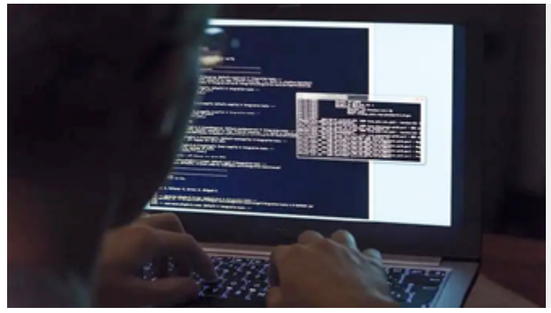
1、北京高院：从严从重惩处行业“内鬼”泄露个人信息行为

摘要：近年来，公民隐私数据泄露问题日益突出，个人信息安全与保护引发全社会高度关注。8 月 23 日，北京市高级人民法院通报近五年侵犯公民个人信息罪案件审判情况，并发布典型案例。数据显示，2018 年以来，北京三级法院共审结侵犯公民个人信息犯罪案件 219 件，判处犯罪分子 294 人。从涉案公民个人信息类型来看，行踪轨迹信息、通信内容、征信信息等高度敏感信息占比突出。

2、罚款 20 万元！北海某公司因泄露约 22 万条个人信息数据被罚

摘要：近日，北海某网站存在数据泄露问题。约 22 万条个人信息数据被挂在境外论坛售卖，该公司及其直接负责人被北海公安机关，分别处以罚款 20 万元、3 万元的行政处罚。

3、抓获“内鬼”2300 余人！从上游堵住信息泄露漏洞



摘要：公安部 8 月 10 日召开的新闻发布会上披露，3 年来公安部部署全国公安机关开展“净网”专项行动，严打侵犯公民个人信息违法犯罪活动，锚定行业内部泄露源头，重拳打击行业“内鬼”，共抓获电信运营商、医院、保险公司、房地产、物业、快递公司等行业“内鬼”2300 余人。

4、侵入多地银行计算机系统窃取储户资料百万余条，两人获刑

摘要：近日，重庆市綦江区人民法院审结一起非法获取计算机信息系统数据案件，被告人封某、陆某利用多地农村信用社联合社网银的漏洞，非法窃取储户资料，企图盗刷银行卡内资金未遂。两名被告人均被判处有期徒刑 3 年 6 个月，并处罚金人民币 20000 元，同时删除非法获取并存储的公民个人信息并在全国性媒体上公开道歉。

5、疑似遭黑客攻击致数据泄露风险 赣州一公司被罚 15 万元

摘要：近日，根据上级部门通报，赣州某信息技术公司业务系统疑似遭受黑客攻击，存在数据泄露风险。江西省通信管理局立即依法组织开展案件调查，查明该公司在开展网络营销代理业务中未有效落实网络和数据安全保护主体责任，未依法采取相应的技术措施保障业务系统数据安全，该行为违反了《中华人民共和国数据安全法》相关规定，省通信管理局对赣州某信息技术公司给予警告、罚款 15 万元，对直接负责的主管人员和直接责任人各罚款 1 万元。

6、黑客窃取个人隐私信息，网警果断出手！

摘要：“净网 2023”专项行动开展以来，福建泉州网安部门不断加大对黑客攻击、侵犯公民个人信息、网络黑灰产业等网络违法犯罪活动的打击力度，成功破获 2 起涉嫌非法控制计算机信息系统案件，抓获 4 名犯罪嫌疑人。

7、斩断简历倒卖黑色产业链 筑牢个人信息保护屏障

摘要：某招聘平台近日被曝假借招聘之名收集简历，高价卖给培训机构并收取佣金，后者则联系求职群体卖课转化客源，双平台以用户个人信息为连接点非法牟利。倒卖简历只是网络招聘黑灰产业链的“冰山一角”，行业内多个平台此前也出现过类似问题，个人信息泄露和违法买卖似成内部“潜规则”。随着就业环境变化，招聘企业核心业务缩小，便开始将目光瞄准个人数据，部分平台释放出早已停止招聘的岗位、诱导用户填写简历，同时私下倒卖用户信息，轻则给广大求职者添堵添乱，重则涉及违法犯罪。

8、大量信息泄露！“内鬼”江某被刑拘！

摘要：8 月 3 日，分局刑警大队在日常摸排工作中，收到线索称：有人推销贷款，且对方知道被推销人单位和所交公积金等信息。接案后，民警敏锐地发现线索的背后，涉及侵犯公民个人信息犯罪。经过摸排后民警发现，嫌疑人就藏在抚州市高新区财富广场某公司内。当日下午 18 时许，民警将犯罪嫌疑人全某霞等 5 人抓获，当场查获了公民个人信息 3 万余条，手机、电脑等作案工具若干。

9、因晒离婚协议泄露大 S 个人信息被告，汪小菲现身出庭说“为一点家事来”

摘要：据报道，汪小菲 17 日现身台北地检署，以被告的身份出庭大 S（徐熙媛）信息泄露案。在面对记者提问为何出庭时，汪小菲仅摆手说“一点点家事”。据悉，汪小菲在去年 12 月曾在社交平台公开了两人的离婚协议书，但在晒离婚协议时，却未将大 S 的地址、汇款账户等私人信息打码。因此被大 S 委请律师搜证，控告他涉嫌违反《个人资料保护法》。

10、揪出楼盘业主信息泄露“内鬼” 宁乡检察：从办理侵犯公民个人信息案到推动行业整治

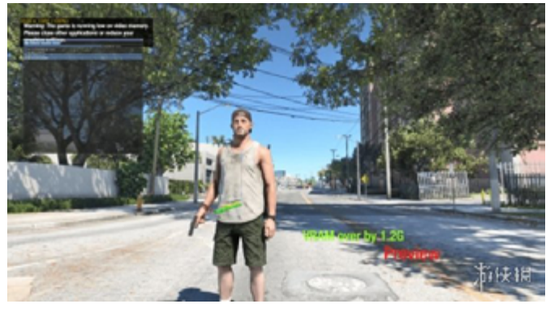
摘要：近日，宁乡市检察院在对某物业公司开展检察建议“回头看”专项活动时，公司物业经理告诉检察官。“案件中被泄露的公民个人信息都用小区楼盘名称命名，并以 Excel 形式在微信群内进行传播，内容包括业主姓名、年龄、详细楼栋单元住址、电话等，甚至还包含家居装修与否等较为私密的信息。” 承办检察官当即对案件进行深入调查，发现部分遭泄露的业主个人信息来源于某小区前物业经理徐某。检察机关引导公安机关及时固定了徐某的微信聊天记录，及聊天中被泄露的业主信息。在微信聊天记录等证据下，徐某很快承认自己曾经利用职务便利，将业主信息主动提供、贩卖给家居、瓷砖等商家。

国外

1、特斯拉 100GB 数据泄露原因查明：内部不法行为，影响逾 7.5 万人

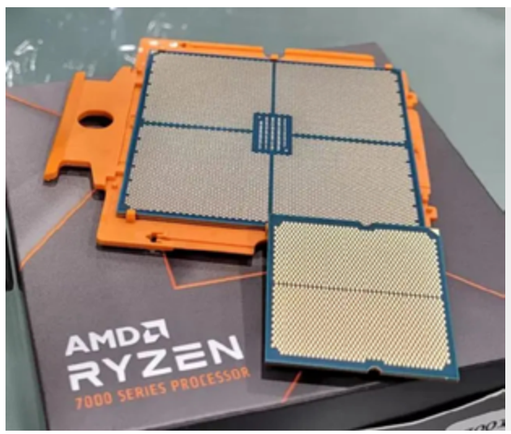
摘要：8 月 21 日，据 BusinessInsider 报道，特斯拉表示，此前发生的大规模数据泄露事件泄露了超过 7.5 万人的个人信息，这是“内部不法行为”的结果。特斯拉在发给员工的通知中表示，被泄露的“特斯拉文件”包含 100GB 的机密数据，其中包括员工的姓名，以及如地址、手机号码和电子邮件地址等联系信息。该通知已与缅因州总检察长办公室共享。泄露的数据还包括大约 2400 起关于特斯拉突然加速的客户投诉，以及另外 1500 起关于刹车问题的投诉。

2、黑客事件曝光：法庭确认 18 岁黑客威胁泄露《GTA6》数据



摘要：近日，英国法庭裁定了一起黑客攻击 R 星，导致《侠盗猎车手 6（GTA6）》90 多段视频被泄露事件。而这起事件原因是一名 18 岁的黑客 Arion Kurtaj 造成的。

3、Inception 漏洞曝光：影响所有 AMD Zen 处理器，可泄露敏感数据



摘要： 8 月 9 日消息，来自苏黎世联邦理工学院的科研团队近日发现了名为“Inception”的攻击漏洞，表示包括最新型号在内，所有 AMD Zen CPU 均存在漏洞。

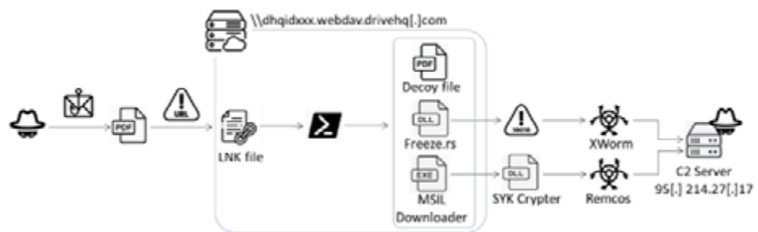
4、英国北爱尔兰警方紧急应对警员信息不慎泄露事件

摘要：英国北爱尔兰警察局 9 日证实，正在调查北爱警方所有员工信息不慎泄露事件，并已成立紧急威胁评估小组。北爱警方 8 日为回应一个信息公开问询时不慎将一份包含当地警局全体员工详细资料的表格发布至互联网，涉及大约一万名警员和文职人员的姓氏、名字首字母缩写、职级、工作地点和部门等信息。相关信息发布到互联网数小时后被撤回。

5、TP-Link 智能灯泡漏洞可窃取目标 WiFi 密码

摘要：研究人员在 TP-Link Tapo 智能灯泡和 APP 中发现 4 个安全漏洞，可用于窃取目标 WiFi 密码。TP-Link Tapo L530E 是一款销量很高的智能灯泡，TP-link Tapo APP 是一款智能设备管理应用程序，谷歌应用商店下载量超过 1000 万。来自意大利和英国的研究人员分析了这款智能灯泡和控制应用程序的安全性，并在其中发现了 4 个安全漏洞，攻击者利用这些漏洞可以窃取目标的 WiFi 密码。漏洞影响数百万智能物联网设备，使得用户数据传输和认证存在风险。

6、攻击者通过 Freeze.rs 和 SYK Crypter 传播恶意软件



摘要：FortiGuard 实验室最近检测到一种用 Rust 编写的新注入器，它可以注入 shellcode 并将 XWorm 引入受害者的环境。虽然 Rust 在恶意软件开发中相对不常见，但自 2019 年以来，已经有几个活动采用了这种语言，包括 Buer loader、Hive 和 RansomExx。FortiGuard 实验室的分析还显示，2023 年 5 月期间注入器活动显著增加，其中 shellcode 可以使用 Base64 编码，并可以从 AES、RC4 或 LZMA 等加密算法中进行选择，以逃避防病毒检测。

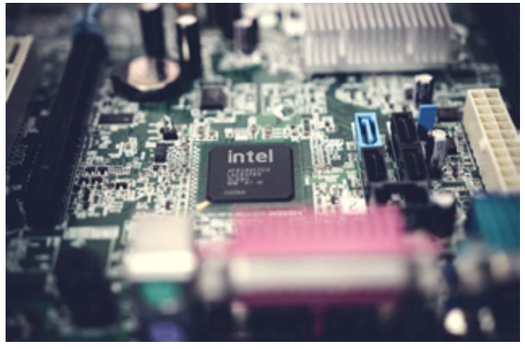
7、几乎所有的 VPN 都容易受到泄露流量的 TunnelCrack 攻击

摘要：研究人员近日发现，影响市面上大多数 VPN 产品的几个漏洞可以被攻击者用来读取用户流量、窃取用户信息，甚至攻击用户设备。实施的攻击从计算上来说开销并不大，这意味着任何拥有适当网络访问权限的人都可以执行攻击，而且攻击与所使用的 VPN 协议无关。即使受害者使用了另一层加密，比如 HTTPS，攻击也会揭示用户在访问哪些网站，这可能是一个重大的隐私风险。

8、Satacom 通过浏览器扩展窃取加密货币

摘要：Satacom 下载程序释放的恶意软件的主要目的是通过对目标加密货币网站进行 web 注入，从受害者的账户中窃取比特币。该恶意软件试图通过为基于 Chromium 的网络浏览器安装扩展来实现这一点，该浏览器随后与 C2 服务器通信，其地址存储在比特币交易数据中。

9、Blackhat 2023：Downfall 攻击可窃取 Intel CPU 加密密钥和数据



摘要：安全研究人员发现了 Intel CPU 中的一个推测执行漏洞，漏洞 CVE 编号 CVE-2022-40982（Downfall）。漏洞影响所有基于 Intel Skylake 和 Ice Lake 微架构的处理器。攻击者利用该漏洞可以从 Intel CPU 中窃取密码、加密密钥、邮件、短信、银行信息等用户个人数据。

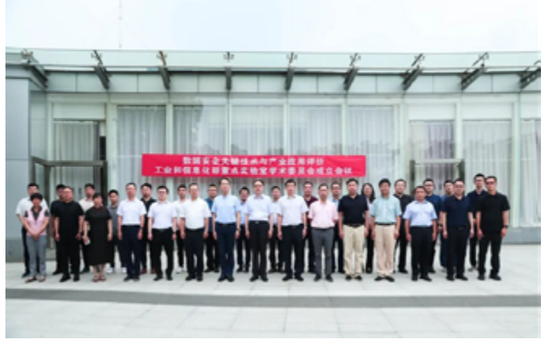
10、搜狗拼音输入法加密漏洞暴露用户输入

摘要：研究人员发现搜狗输入法使用的加密算法存在漏洞，恶意攻击者可解密用户的输入信息。漏洞影响 Windows、安卓和 iOS 平台。漏洞产生的根源是搜狗定制的加密系统——EncryptWall。该系统是敏感流量到未加密的搜狗 HTTP API 终端的安全通道，通过明文 HTTP POST 请求中的加密字段来实现。研究人员分析发现 EncryptWall 系统易受到 CBC Padding oracle 攻击，这是一种选择密文攻击，影响使用 CBC 模式和 PKCS#7 填充的分组加密。网络监听者利用该攻击可以在不知道加密密钥的情况下恢复加密的网络传输的明文，恢复包括用户输入在内的敏感信息明文。

亿赛通总经理受聘为工信部数据安全重点实验室第一届学术委员会委员

7 月 26 日，由工业和信息化部科技司和网络安全管理局指导，赛迪研究院、中关村科学城管委会等单位联合主办，四季慧谷 • 国家网络安全产业园协办的“数据安全关键技术与产业应用评价工业和信息化部重点实验室学术委员会（以下简称“重点实验室”）成立大会”和“数据安全技术产品创新沙龙”在京成功举办。

重点实验室学术委员成立大会（暨一届一次委员会会议）上，为重点实验室学术委员会主任冯登国院士颁发聘书，宣布其出任学术委员会主任，同时为数据安全产业相关专家学者，产业领军企业嘉宾颁发聘书。北京亿赛通科技发展有限责任公司总经理崔培升受聘成为重点实验室第一届学术委员会委员，聘期五年。



会议审议并通过《数据安全关键技术与产业应用评价工业和信息化部重点实验室学术委员会章程》，讨论并通过《数据安全关键技术与产业应用评价工业和信息化部重点实验室 2023 工作要点及实施计划》。

目前国内企业、厂商的数据安全保护意识、安全技术防护手段正在逐步提升。标准需要完善，用户维权困难，管理模式需要更新，人才短缺。基于上述问题，亿赛通提出了“政策 + 标准 + 咨询 + 方案 + 服务 + 人才”相结合的“六位一体”发展思路。其中，我司综合数据安全解决方案能够全方位检测数据安全问题和企业内部存在的脆弱性问题，结合数据资产测绘、数据流转测试、数据平台漏洞、安全配置核查多方面的扫描和检测结果，进行风险评估分析，发现数据分类分级问题、敏感数据存储分布问题、敏感数据异常使用问题、数据组件安全漏洞问题、安全配置问题。解决方案一方面便于检查机构快速发现问题，另一方面也便于企业自身发现安全风险，提早做安全规划，让数据风险可量化，为数据安全防护提供有力支撑。

具体利用机器学习等大量的人工智能技术，对采集到的各类数据进行智能分析和处理，从中提取重要信息，不仅可以在客户网络中自动发现其重要数据资产，同时可依据系统内置的数据分类分级对识别的数据资产进行自动的分类分级处理，打上相应的标签；另外，在自动识别数据资产的同时，系统可以扫描并智能分析客户网络中数据安全风险，对潜在的数据安全风险，通过系统的专家系统进行智能匹配并给出最优的解决方案和建议。

下一步，亿赛通将在重点实验室学术委员会的领导和管理下，夯实履职基础，努力开创委员会工作新局面，在提高企业数据安全保护意识，完善数据安全技术防护手段，系统化培养数据安全保护人才，形成安全保护管理新模式等方面开展工作，为企业数据合规赋能搭建一架专业的服务桥梁。

亿赛通亮相 2023 商用密码大会，北京市密码管理局领导莅临展位参观指导

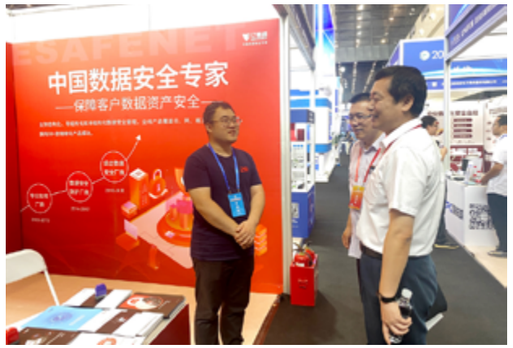
8 月 9 日 -8 月 11 日，2023 商用密码大会在郑州国际会展盛大召开，八方宾客齐聚一堂，共襄商用密码高质量发展。2023 商用密码大会以“密码赋能美好发展”为主题，由国家密码管理局指导，中国密码学会作为支持单位，郑州市人民政府、河南省密码管理局主办，郑东新区管委会承办，旨在推进商用密码创新驱动、前沿交流、产业对接、协同合作，集中呈现我国商用密码理论、技术、产品、服务、应用等最新成果，探讨产业发展趋势，解读政策法规。本次，亿赛通受邀参与大会，集中展示了安全领域的新技术、新产品、新服务，专家现场答疑解惑，让观众近距离感受到数万家企业的安心之选。

密码是国之重器，是保障网络信息安全的核心技术和基础支撑。党的十八大以来，我国深入贯彻习近平总书记关于密码工作重要指示批示精神，全面落实总体国家安全观，大力推进密码应用与创新，着力扶持和壮大商用密码产业。大会现场，大会现场，密码管理局部分领导莅临亿赛通展位参观指导。

在数字经济时代，商用密码、数字安全等话题不仅关系企业、个人，更关系国计民生。如何在当前对互联网和数据信息方面进行有效保护和发展，如何在复杂的国际竞争中保持优势，是我们需要重视并落地解决的问题。

面对不断变化的安全挑战，亿赛通更希望联合企事业单位共建更完善的全生命周期防护系统，提供可靠有效的解决方案的同时，会同客户一起积极探索数据安全的产业价值，助推数字经济安全腾飞。

大会现场，亿赛通全方位展示了立体化、多层次的企业数据安全防护体系，受到现场政府领导、行业专家、权威媒体的极大关注。北京市密码管理局领导特来到亿赛通展位，就公司产品研发、专业方案、技术成果等情况进行深入探讨，并对亿赛通多年来在商用密码行业做出的努力表示认可与支持。



作为一家长期致力于为各行各业、各单位提供全方位数据安全解决方案的企业，亿赛通对此已深耕多年。二十年前，公司正式成立，专注研发文档加密产品，彼时“数据安全”还未被如此广泛知悉和应用。而随着数字化业务发展的多样化，勒索病毒、黑客攻击、内部泄露等安全问题全面爆发，我司以全生命正周期的数据安全解决方案为出口，在为客户提供数据安全防护的同时加入数据库安全审计、网络数据泄露防护、数据安全综合治理等服务，建立起数据安全运营管理平台，亿赛通也再次迎来了高速的市场增长。

以本次展出的全新数据安全产品体系为例，数据安全的首要基础工作是数据治理，即分类分级。基于分类分级结果配置差异化的安全策略和技术保障手段，从而兼顾数据有序流动与安全保障。随后，通过技术与工具的结合（如：文档加密、数据泄露防护、数据库审计、数据库防火墙、数据脱敏……），为防护策略提供能力支持。最终，为安全设备下发统一的策略，达到统一管理、统一调度、一键阻断、协同联动的能力。达到联防联控、追踪溯源。以上，熟悉数据安全工作的业内人士可以看出，这也正是同步规划、同步建设、同步运营，即三同步理念的体现。

政府重视和政策扶持正在不断推动信息安全产业的快速发展，尤其数字经济发展迅猛，加强数据安全是行业大势，势不可挡。展会现场诸多参会人员均反馈，此次参会为商用密码、网络安全、数据安全等行业提供了建设性的思路与实践方向，不虚此行。亿赛通已肩负起保护数据安全，促进数字经济可持续成长的重任，我们会继续努力。

数据安全旨在强调树立正确的数据安全观，在商用密码的基础上加强信息基础设施防护，加强数据安全信息防护手段、平台建设，加强数据安全事件应急能力建设，积极发展安全产业，做到关口前移，防患于未然。这不仅是国家发展的重要战略，也是广大企业发展的历史使命和战略机遇。亿赛通将不忘初心，砥砺奋进，为国家数据安全发展贡献力量。

亿赛通出席南昌市医疗行业数据安全座谈会，合力打造医疗行业深层堡垒

8 月 17 日，南昌市医疗行业数据安全座谈会顺利召开。近年来，数据开始从“静止”走向“流动共享”，随之而来，医疗数据安全也愈加突出，传统的数据安全体系难以周全保障数字时代新的系统架构对数据安全的冲击，风险无处不在。一旦出现数据泄露，不仅会对企业带来紧急损失，还有可能造成极为负面的社会影响。面对数据安全新形势下的诸多挑战与不断强化的监管政策，南昌市各家医院从事信息化工作的数十位同仁出席会议，只为对医疗行业数据安全形势有一个更加清晰的认识。

此次活动由南昌市公安局主办，南昌市网络信息安全协会及亿赛通共同承办。与会嘉宾围绕医疗行业数据安全政策、数据安全治理、数据安全防护体系建设与管理等方面开展专题演讲。望通过系统专业的讲解，进一步强化对医疗行业数据安全相关法律法规政策的理解，形成维护数据安全的新思路、新方法、新举措、新本领，切实提升新形势下安全保障能力。

随着医院信息化建设的网络边界逐渐扩大、信息化为医院提供快速、便捷、有效的服务、管理的同时，勒索病毒、信息泄露、网络攻击也给医疗行业带来了极大的危害。据 IBM 数据泄露成本报告显示，医疗保健、药品、医药等行业数据泄露平均成本占据前列。从全球监管趋势来看，全球 107 个国家和地区已经制定数据安全和隐私保护法律亚洲、非洲只有不到 40% 的国家有相关法律。在中国，自 2016 年起，国家陆续推出网络安全、数据安全相关政策法规，特别是近两年，行业监管条例如井喷式爆发。

针对医疗行业，卫健委发布了《“十四五”卫生健康标准化工作规划》强调健全卫生健康信息标准体系，完善基础类、数据类、应用类、技术类、管理类、安全与隐私类等 6 类信息标准的制定。此后，又发布了《医疗卫生机构网络安全管理办法》，加强了数据收集合法性管理，明确业务部门和管理部门在数据收集合法性中的主体责任。

亿赛通认为医疗行业作为数据密集型行业之一，数据共享流通频繁，数据集中处理、广泛共享、交叉使用是刚性业务需求，对企业的数据安全防护能力和数据治理能力有更高的要求。不同行业有不同的风险，医疗行业在信息化背景下的风险具体如下：

数据量更大

伴随着医疗信息化的快速发展，产生了海量的高通量数据。包括药品的研发数据（基于工程、疫苗、诊断试剂、微生态试剂、血液制品等）、销售数据、市场信息、专利信息、临床试验信息、生产检验数据、药品信息、电力病历、影像信息等等。

数据敏感度更高

医疗健康大数据包含临床大数据、健康大数据、生物大数据、经营运营大数据等，在大数据条件下，这些数据经由系统分析，能够产生新的价值。但是，这其中也直接包含着大量个人信息，一旦被非法第三方获取，则直接对患者隐私造成威胁。

业务系统更复杂

业务流程和运营管理的线上化，包括研发、采购、生产、营销、销售、HR、财务、IT 等多个部门，暴露面更广， IT 面临挑战更加复杂。

数据对外共享更频繁

医疗信息化各项科学研究通常需要大量的样本，单一机构的数据量很难满足这样的需求，跨机构、跨地域、跨国的数据共享非常频繁。各个国家和地区的隐私保护法律法规不同，分享过程数据滥用和泄露风险更高。

针对上述风险，亿赛通遵循 IDPR 能力框架模型，从决策层、管理层、执行层进行组织建设，并进行制度流程管控。始终遵循安全咨询、分类分级、分级管控的治理步骤，将终端、数据库及文件服务器内的数据做梳理，完成分类分级，为数据分级管控做铺垫，最终完成对标合规。

后续通过相应安全技术手段，如：数据库审计、电子文档加密、数据脱敏、数据水印、数据防泄漏、访问控制、关联分析、追踪溯源等，通过人工智能算法，以人员和终端行为分析为主线，发现威胁企业的数据安全事件，提供完整追溯取证证据链。将各个孤立的安全系统进行资源整合，实现数据资产可视、数据威胁可管、数据风险可控、数据血缘可溯。

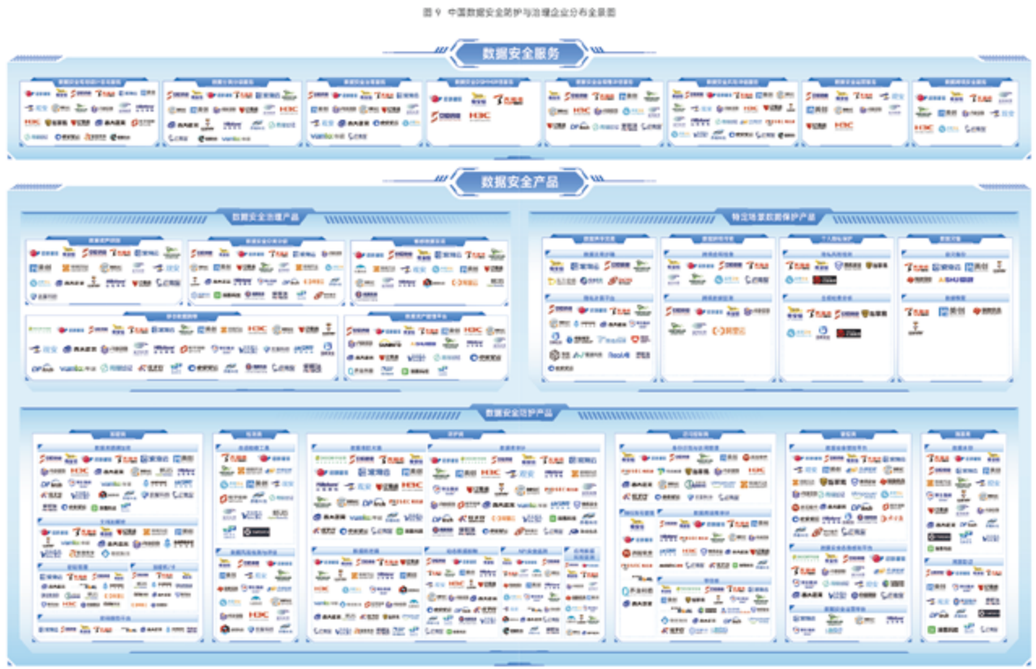
本次座谈会为医疗行业从业人员提供了一个良好的交流平台，就医疗行业政策趋势、数据安全治理、安全运维等难题进行了深入交流与探讨。未来，亿赛通仍将秉持“中国数据安全专家”的职责，成就所托，持续为行业客户的业务顺畅运行保驾护航。

亿赛通入选《中国数据安全防护与治理市场研究报告（2023）》

近日，赛迪顾问发布《中国数据安全防护与治理市场研究报告（2023）》（以下简称《报告》），亿赛通在《报告》全景图中完成数据安全服务、数据安全治理产品以及数据安全防护产品三大类别覆盖，19 项细分领域入选，除此之外，还入围了 4 项细分领域重点企业推荐。

随着数字经济和信息产业蓬勃发展，数据价值持续攀升。据《数字中国发展报告 (2022 年)》统计，2022 年我国数字经济规模达 50.2 万亿元，总量稳居世界第二。海量高价值数据不断产生，数据安全防护、数据安全治理等问题成为继网络安全之后的又一重要安全话题，如何保障数据在创建、采集、存储、传输、交易、销毁的全生命周期安全变得至关重要。

图 9 中国数据安全防护与治理企业分布全景图



数据安全服务	数据安全规划设计咨询服务、数据分类分级服务、数据安全治理服务、数据安全合规性评估服务、数据安全风险评估服务、数据安全运营服务	
数据安全产品	数据安全治理产品	数据资产识别、数据安全分类分级、敏感数据发现、静态数据脱敏、数据资产管理平台
	数据安全防护产品	文档加解密、数据库防火墙、数据库审计、数据防泄漏、动态数据脱敏、数据库运维审计、数据水印、溯源取证

基于多年来在数据安全领域的技术积累与实践，亿赛通推出综合数据安全治理解决方案。通过全面的资产发现方式、灵活的资产梳理规则、深入的资产质量分析，能够有效地帮助企业进行对数据资产的摸底和管理工作；改善传统方式下的资产梳理和管理模式，提高工作效率，保证资产梳理质量，实现资产权责分明；打破数据孤岛，提高获取效率，释放资产价值。以资产发现 - 资产梳理为核心，以资产可视 - 资产可管为目标，致力于提升企业对数据资产的整体管控能力和运维效率。

方案优势

1、加快数据治理与应用

系统对企业个人隐私、核心业务等敏感数据进行识别定位，为后续针对关键数据和敏感数据的保护和治理工作提供明确目标；开放底层能力对接可实现接入数据安全防护系统；定位识别能力可实现合规和保护成果验证。充分解决了数据体量大、覆盖区域广、应用场景杂、持续治理难四大难题。

2、助力企业数字化转型

本着整体规划、整体建设、统一协同的思想，为企业数字化转型提供了有力的数据安全支撑，促进业务高效高质量发展。通过分析各类数据特征，标记和定位敏感 / 重要数据，形成数据资产清单、数资产地图，协助企业完成数据资产梳理。

3、满足相关法律法规要求

系统具备静态数据资产分布梳理、敏感数据识别标记、数据分类分级标记等能力，能帮助企业自动化完成常规的数据资产梳理、重要数据识别标记、数据分类分级等工作，输出数据分类分级清单和重要数据清单。满足《网络安全法》、《数据安全法》、《个人信息保护法》等法律法规对数据安全治理的要求。

亿赛通认为，数据安全正在从相对独立的数据安全防护单品向体系化、平台化的数据安全治理演进。这个趋势也和亿赛通多年来的数据安全防护体系建设道路相通，我司提出以“分·放·管·服”数据安全建设理念为核心，以技术为支撑，基于数据分类分级、依托数据安全治理服务，通过数据安全防护产品的联防联控来实现数据全生命周期的防护体系。

亿赛通综合数据安全治理服务将现有的各个独立的数据安全技术和功能整合，为用户提供跨数据类型、存储孤岛和生态系统集成数据的产品和服务，从而实现更简单、一致的端到端数据安全。相较于传统数据安全方案，亿赛通数据安全治理存在更高水平的集成能力、简化的部署模型，统一的策略控制平面，以及对数据、存储、政策和适用法规的一致可见性。

数据安全防护体系的建设是数字经济中数据安全建设的重要组成之一，数字办公常态化促进了数据安全产品的市场需求持续增长。亿赛通持续深耕数据领域，保护企业数据安全，肩负起中国数据安全专家责任，为筑牢数据安全防线贡献力量。

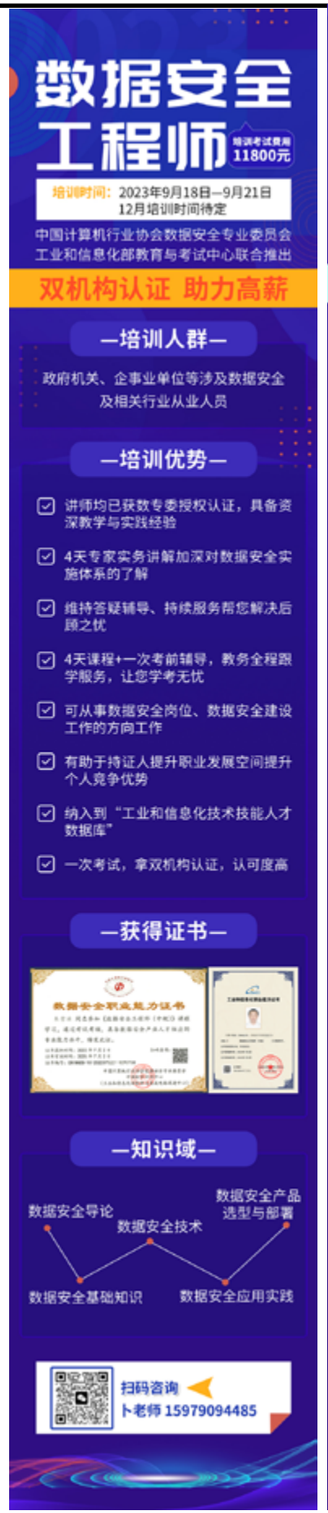
数据安全能力培训即将开班，帮您实现一次培训拿双证

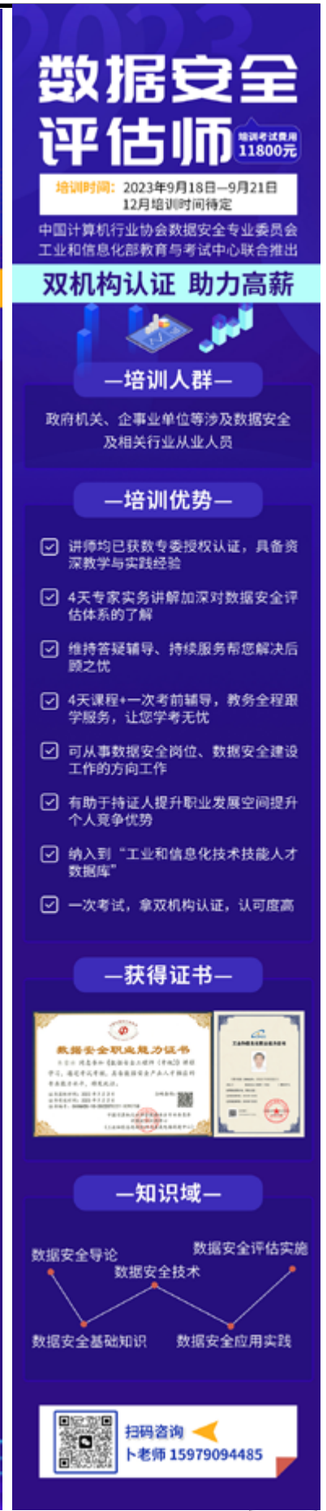
数据安全已经成为当今社会中最重要的挑战之一，随着技术的不断发展和进步，社会迫切需要拥有专业知识和技能的人才来保护我们的数据免受威胁。

由工业和信息化部网络安全管理局指导，中国计算机行业协会数据安全专业委员会与工业和信息化部教育与考试中心联合推出的数据安全能力培训正式开始招生！

目前开设数据安全工程师、数据安全评估师两项课程。学员通过培训掌握数据安全基础知识，了解数据安全评估体系，熟悉数据安全评估技术，综合提升数据安全评估能力，使其大幅度提升在数据安全领域工作中的竞争力。

本次培训不仅仅是为了满足当前的数据安全需求，更是为了培养未来的数据安全专家。让我们携起手来，共同努力，建设一个更加安全的数字时代。





从安全技术视角了解《中国人民银行业务领域数据安全管理办法（征求意见稿）》

继国家金融监督管理总局发文加强金融机构外包网络和数据安全管理后，央行也于近期发布《中国人民银行业务领域数据安全管理办法（征求意见稿）》（以下简称《办法》）。旨在落实《数据安全法》有关要求，加强中国人民银行业务领域数据安全管理。从《办法》预计的生效期来看，或在 2024 年落地。《办法》作为中国人民银行业务领域数据安全规范问题的首个针对性重磅法规，征求意见稿一经发布引发普遍关注。

《办法》分成总则、数据分类分级、数据安全保护总体要求、数据安全保护管理措施、数据安全保护技术措施、风险监测评估审计与事件处置措施、法律责任、附则八章，共 57 条，其中对规范数据分类分级要求、压实数据处理活动全流程安全合规底线、非法获取数据等行为的处理等多个问题指明了方向。

起草背景

《数据安全法》第六条，“工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责”，党中央、国务院也要求认真落实国家法律，进一步细化数据分级分类保护、数据目录管理、全流程数据安全管理、数据安全监测预警和应急处置相关制度。

上述背景下《办法》应运而生，统合了《数据安全法》、《个人信息保护法》以及其他法律法规的相关规定，明确了中国人民银行业务领域数据安全合规底线，填补了本领域数据安全管理制度保障空白。

适用范围

从中国人民银行业务领域来看，数据主要涉及公开政策市场操作数据、跨境人民币数据、银行间各类市场交易数据、金融业综合统计数据、支付清算数据、货币管理数据和数字人民币数据、国库收支数据、个人和企业征信数据、反洗钱相关数据等，这些数据处理者主要是各类金融机构和金融科技公司，也涉及到个人和企业，比如征信数据覆盖面就非常广

管理原则

国内金融行业首次明确在全行业范围要求数据管理、数据安全管理和业务管理要做到三位一体，体现出全行业数据管理和数据安全管理整体能力的提升。

监管模式

条块结合、区域联动的协同监督管理机制。

例：针对违规向国际组织提供数据的行为，中国人民银行及其分支机构将依照《数据安全法》第四十八条第二款规定予以处理；所提供数据涉及个人信息的，依照《个人信息保护法》第六十六条规定予以处理。

此外，中国人民银行及其分支机构执法检查时，若发现数据处理者存在窃取或者以其他非法方式获取数据的行为，会将相关案件信息移送同级公安机关、国家安全机关，并配合其依法依规予以处理。

有何要求

01 数据分类分级

- 分类分级保护总体规划——人行出行标
- 数据分类分级制度规程——机构建制度
- 数据分类要求——指引数据分类操作
- 数据分级要求——指引数据定级操作（三级）
- 数据敏感性分层级——指引数据敏感性分层级操作（五层级）
- 数据可用性分层级——指引数据可用性分层级操作（灾备管理）
- 动态更新要求——每年更新一次

解决方案

亿赛通采用产品结合服务模式，通过服务输出机构内部数据分类分级制度及数据分级管控规程，借助亿赛通数据安全分类分级系统实现数据分类分级梳理及密级标识，通过技术手段将分类分级制度执行落地。

02 数据安全保护总体要求

数据处理者应：

- 责任落实总体要求——压实数据安全责任，明确岗位职责，建立问责处罚制度
- 全流程安全管理制度要求——基于数据分类分级结果，制定数据处理操作规程，指引分级管控落地
- 安全培训总体要求——制定数据安全岗位年度培训计划
- 鼓励创新——积极开展数据安全技术创新应用

03 数据安全保护管理措施

管理制度层面，数据处理者应：

- 人员管理要求——职责分离、权限管理、身份认证、保密协议
- 数据收集保护管理措施要求——签署数据采集协议、征得对方同意、评估数据合法真实性、制定数据暂停使用应急处置方案、材料留存备审 3 年
- 数据存储保护管理措施要求——明确数据存储期限、第三层级以上数据项不得在终端和移动设备中存储，确需存储，执行审批，相关审批资料留存备审 3 年
- 数据使用保护管理措施要求——第三层级数据项不提供导出使用方式，第四层级以上数据项仅提供核验使用方式，确需存储，执行审批，相关审批资料留存备审 3 年
- 数据加工保护管理措施要求——第四层级以上数据项加工，采取风险防范措施并执行审批，数据加工行为相关材料留存备审 3 年
- 促进数据开发利用——使用第三层级以上数据项加工后产生的数据项，执行审批后，可视情降低敏感性层级（有前提），促进数据开发利用
- 数据传输保护管理措施要求——第三层级以上数据项不得通过互联网邮件、即时通讯、在线文件传输、交互性信息服务等互联网信息服务或者通过移动介质交换传输
- 一般性数据提供保护管理措施要求——分情形说明一般性数据提供保护管理措施要求
- 特殊性数据提供保护管理措施要求——分情形说明重要及核心数据提供保护管理措施要求
- 数据融合创新应用管理措施要求——要确保风险可控
- 数据出境限制管理措施要求——数据出境风险自评估、申报安全评估
- 国际组织和外国金融管理部门数据调取——需经中国人民银行和其他有关主管部门批准
- 数据公开保护管理措施要求——第二层级以上数据项公开需执行审批、相关材料留存备审 3 年；第三层级以上数据项需脱敏后公开

▪ 数据删除保护管理措施要求——主动删除、账号核验、介质销毁

解决方案

亿赛通通过数据安全咨询服务，协助数据处理者建立健全数据安全组织体系、制度体系、技防体系及人员能力。包括但不限于明确数据安全管理相关内设部门职责分工，细化定则问责机制，建立健全全流程数据安全管理制度，明确数据差异化（即，分级管控）的安全保护管理和技术措施要求，编制数据处理活动操作规程，明确数据出境安全要求，制定数据安全年度培训计划。

04 数据安全保护技术措施

安全工具应用层面，数据处理者应：

▪ 账号权限保护技术措施要求：第三层级以上数据项的特权账号，涉及人工操作的数据库表删除、修改等操作应当逐一进行事前审查和事后审计；

解决方案

亿赛通数据库运维安全管理系统基于统一管理平台，提供多因子身份认证机制，通过工单管理，约束数据库访问行为，解决特权账号、高危操作等带来的安全隐患。

▪ 数据处理活动日志保护技术措施要求：第三层级数据项如需在数据处理活动日志中记录原则上应当实施脱敏处理，第四层级以上数据项原则上不记录；日志数据纳入分类分级管理；日志数据留存备审 6 月或 3 年（视情况）；

解决方案

亿赛通数据脱敏系统，自动化发现源数据中的敏感数据，并对敏感数据按需进行脱敏规则变形，避免敏感数据泄露，脱敏后的数据保持了数据的一致性和业务的关联性。除脱敏系统外，还需结合上述数据分类分级系统结合应用，方以满足《办法》要求。

▪ 数据收集保护技术措施要求：数据处理者面向个人直接录入方式收集数据时，应当建立健全技术措施，识别法律、行政法规禁止发布或者传输的信息；

解决方案

亿赛通数据泄露防护系统可为数据使用和数据移动提供可见性，根据防护场景分为终端 DLP、网络 DLP、邮件 DLP，用户在对数据执行操作时，系统可根据内容和上下文动态地执行策略。包括监视，提示，告警，阻断，审计和放行等响应功能来解决数据面临的相关的威胁，可以解决有意、无意或事故引发的数据泄露风险以及敏感数据泄露。

▪ 数据存储保护技术措施要求：有效隔离开发测试环境与生产环境数据存储设施设备；第三层级以上数据项实施加密存储；

解决方案

数据加密技术，根据加密队形类型不同分为数据库加密、终端加密，对应亿赛通数据库加密系统、终端电子文档安全管理系统两款产品，加密解密过程性能无损、用户无感，从根源解决数据泄露风险问题。除加密防护外，亿赛通数据安全交换系统置于可信网与非可信网之间，拦截 TCP/IP 连接，过滤丢弃 TCP/IP 协议封装，还原上层应用数据并经安全处理后，以数据摆渡的方式实现应用数据内外网安全交换。在实现数据的往返传输的同时，文件交换平台保证内外网络在任何时候没有联通的电气连接。以上三款安全技术综合应用满足《办法》要求。

▪ 数据使用保护技术措施要求：统一明确第三层级以上数据项的脱敏处理策略；采取数字水印等措施，标识信息系统数据使用信息；针对使用第三层级以上数据项的终端，采取安全沙箱、终端行为管控等安全保护措施；第二层级以上数据项原则上应当经授权并实施脱敏处理后才能用于开发测试；

解决方案

亿赛通数据水印与分发系统可将水印标记嵌入到原始数据中，能够实现数据分发后进行溯源的产品。通过这些嵌入的信息能达到确认版权所有者、追踪泄密用户的目的。除水印系统外结合上述终端 DLP、数据脱敏系统，方可满足《办法》要求。

▪ 数据加工保护技术措施要求：建立统一的加工算法风险评估和控制策略，明确可解释性、脆弱性等风险对应的缓释措施以及退出算法自动化决策的替代方案；

▪ 数据传输保护技术措施要求：动态更新记录不同网络安全区域间正常数据传输对应的网络地址、网络协议通信映射关系，加强安全隔离与终端设备准入控制；

解决方案

亿赛通支持 API 接口自动发现、分类分级梳理，绘制接口画像、监控接口访问轨迹，监测敏感数据流动风险，识别接口异常调用等功能，为 API 使用提供安全保障。除 API 接口安全管理系统外，还需结合上述网络 DLP 综合应用，可满足《办法》要求。

▪ 数据提供保护技术措施要求：并采用前置网关或者应用程序接口方式向其他数据处理者提供数据；提供从其他数据处理者收集获得的数据项，中国人民银行有明确需公开数据来源要求的，应当以显著方式标识来源；

解决方案

数据打标功能是亿赛通数据安全分类分级系统功能模块之一，通过标签可使数据更加便于被搜索、定位、管理。除数据打标外还需结合传输通道加密以及上述的 API 接口安全管理等防护手段联合应用方可满足《办法》要求。

▪ 数据公开保护技术措施要求：明确自身已公开数据是否可被自动化搜集的数据访问控制协议，并采取有效技术措施，保障公开数据不被篡改；

▪ 数据删除保护技术措施要求：建立统一的数据存储介质销毁策略，明确销毁技术方式和过程监督措施——数据加密、数据覆写擦除；

解决方案

数据擦除技术是亿赛通终端 DLP 及新一代电子文档安全管理系统功能模块之一，通过数据覆写技术实现数据永久擦除。

05 风险监测评估审计事件处置

数据处理者应：

▪ 数据处理活动风险监测：采取有效措施，强化数据处理活动安全风险监测和告警，推进违规数据处理活动阻断技术措施建设，及时做好风险隐患的溯源排查处置，并核验技术措施的有效性和可靠性；

▪ 数据安全风险情报监测：加强数据安全风险情报的监测，及时核实并做好必要的数据安全防范处置工作；

▪ 数据安全通报预警监测；

▪ 数据安全风险评估：应当自行或者委托检测机构，每年组织开展一次全面的数据安全风险评估工作，于下年度一季度末前向中国人民银行或其住所地分支机构报送风险评估报告，并按照行政法规要；

求向对应的网信部门报送；

▪ 数据安全审计：数据处理者应当围绕全流程数据安全管理制度和相关操作规程执行情况、数据安全相关投诉处理情况，每年至少开展一次与数据安全相关的合规审计；

▪ 数据安全风险评估与审计的安全保障：建立技术平台，统一建立数据安全风险评估与审计的安全管控策略；

▪ 数据安全事件定级判定；

▪ 数据安全事件响应处置；

亿赛通小贴士 ESAFENET PROMPT

解决方案

亿赛通数据安全运营管理平台通过对安全组件统一纳管，并基于平台实现统一的策略联防联控机制，全网数据综合分析帮助用户构建基于数据安全运营闭环的协同联动防御体系。除此，亿赛通特为监管及被监管单位推出一款敏感数据安全检查和自查自处理的数据安全检查工具箱，可辅助组织完成数据安全风险评估。

法律责任

明确中国人民银行及其分支机构可对数据处理者数据安全保护义务落实情况开展执法检查，以及数据处理者违反规定时对应的法律责任。

亿赛通在 20 年中聚焦数据安全实践，专注技术创新和安全能力研究。从技术到产品、从策略到管理，提出的“分放管服”四步双闭环建设数据安全建设理念与《办法》指引协同一律。

《办法》出台在即，是征求意见期，亦是机构数据安全能力补全建设期。亿赛通以专业的产品和服务帮您筑牢数据安全底座，精准合规，赋能发展。

咨询服务 | 企业为什么要开展数据安全风险评估？怎么开展？

咨询研究部 / 文

咨询服务上篇文章《咨询服务 | 数据安全评估、风险评估、合规评估……概念如何界定？》，我们从组织形式、触发场景、开展阶段、评估结论几个维度，介绍了数据安全评估的几种类型。下面，我们将聚焦数据安全风险评估，对该服务的含义、必要性、评估依据和实施方法进行介绍。

什么是数据安全风险评估？

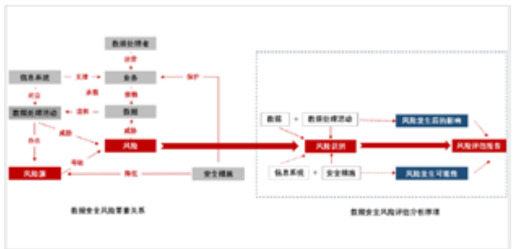
数据安全风险评估是以主动发现潜在的安全风险为目标，基于合规要求和行业优秀实践，运用科学、自动化的方法和手段，识别分析组织数据资产以及在采集、存储、传输、使用、加工、处理、销毁等相关处理活动中面临的风险，最终输出风险等级判断和整改意见的服务。相比数据出境安全评估、个人信息安全影响评估（PIA），数据安全风险评估是日常性、连续性的，评估对象范围更灵活，既可以包含整个数据处理者和处理场景，也可聚焦具体业务场景和数据处理系统。

为什么要开展数据安全风险评估？

数字经济背景下，数据总量爆炸式增长，数据价值凸显、流通场景复杂多样，数据安全风险日益严峻；同时，数据成国家基础战略性资源，数据安全合规体系逐步完善，数据安全监管趋严。各类企业面临满足安全要求和合规要求的双向风险。数据安全风险评估可帮助企业发现数据安全潜在风险、识别数据安全合规差距，并以实现数据安全管理和技术手段有效联动为出发点，提出更有针对性的数据安全工作落地方案。

开展数据安全风险评估有何依据？

当前开展数据安全风险评估可参考依据包括《信息安全技术 大数据安全管理指南》《信息安全技术 信息安全风险评估方法》《网络安全标准实践指南——网络数据安全风险评估实施指引》等通用标准，以及《工业领域数据安全风险评估实施指南（征求意见稿）》《电信和互联网数据安全风险评估实施方法》《互联网新技术新业务安全评估要求 大数据技术应用与服务》等行业标准。综合分析来看，指导标准以确定风险要素、识别风险隐患、形成风险评估报告为整体路径，围绕数据（本身存在脆弱性）、数据处理活动（过程中存在管理或技术脆弱性）、数据安全措施（降低脆弱性被利用的可能性）三大要素展开评估，最终判断风险发生可能性和风险发生后的影响，得出评估结论。



如何开展数据安全风险评估

数据安全风险评估实施工作包括评估准备、信息调研、风险识别、综合分析、评估总结五个环节。评估准备阶段，通过确定评估目标、明确评估范围、组建评估团队等前期准备工作，制定数据安全现状调研表和整体评估方案。信息调研阶段，对数据资产、数据处理者、数据处理活动、业务和信息系统、安全防护措施展开调研，输出数据资产清单、数据处理者基本情况、数据处理活动清单、业务信息系统清单、数据安全措施使用情况等一系列调研结果。风险识别阶段，基于特定的风险评估清单，采用文档查阅、安全核查、人员访谈、技术检测等手段，从管理、技术、应用等方面开展风险识别，形成识别结果。综合分析阶段，基于识别结果，整体考虑数据价值、风险隐患严重程度、安全措施有效性和完备性等因素后，给出存在的主要问题、数据安全风险情况和整改建议。评估总结阶段，对项目各阶段交付物内容总结、分析，形成《数据安全风险评估报告》和《数据安全下一步建设方案》。

在实施过程中，确定数据安全风险评估范围和深度，根据实际情况完善风险评估模板，形成适用于具体行业、具体企业的风险评估项和风险分析策略至关重要。对企业的数据安全管理能力进行整体评估，针对关键系统、重要场景、高敏感数据的技术防护能力进行专项评估，以可能引发的安全事件为判定视角，以细粒度完善数据安全管理流程、聚焦性补齐数据安全技术措施为整改原则，有助于提高数据安全风险评估工作的效率和效果。

咨询服务下篇文章，我们将为大家呈现亿赛通数据安全风险评估方案，并分享从实际项目中获得的经验，敬请期待~

政策速递 | 网信办发布《人脸识别技术应用安全管理规定（试行）》（征求意见稿）

咨询研究部 / 文

随着大数据、人工智能等新兴技术的快速发展，人脸识别技术被广泛应用于金融、安防、医疗等领域的具体场景中，给我们的生活带来了许多便利，但技术滥用的安全问题也显而易见，对个人隐私和社会安全造成一定的威胁。为规范人脸识别技术应用，保护个人信息权益及其他人身和财产权益，维护社会秩序和公共安全，8 月 8 日，国家互联网信息办公室发布了《人脸识别技术应用管理规定（试行）（征求意见稿）》，向社会公开征求意见。

在此之前，我国也出台了许多关于人脸识别数据规范使用相关或专门的国家标准，如《信息安全技术 个人信息安全规范》（GB/T 35273-2020）、《信息安全技术 人脸识别数据安全要求》（GB/T 41819-2022）、《信息安全技术 个人信息处理中告知和同意的实施指南》（GB/T 42574-2023）、《网络数据安全标准实践指南——人脸识别支付场景个人信息保护安全要求（征求意见稿）》等，具体内容不再呈现。未来，这些标准可以支撑《规定》的落地实施。

根据 2022 年 10 月发布的《信息安全技术 人脸识别数据安全要求》（GB/T 41819-2022）相关内容，对人脸识别数据、人脸识别技术及人脸识别技术应用场景的定义如下：

人脸识别数据是指可识别自然人身份的人脸图像或人脸特征。

人脸识别技术是指通过人脸图像或人脸特征信息识别身份的一种生物识别技术。

人脸识别技术应用场景包括机场、火车站使用人脸识别数据进行认证比对；移动智能终端、应用程序使用人脸识别数据实现解锁、支付等功能；公园、居民小区等使用人脸识别数据核对人员身份 ……

一、法律依据

《规定》根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律制定。

其中《个人信息保护法》第二十六条明确：“在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外”。

二、适用范围

在中华人民共和国境内利用人脸识别技术处理人脸信息，提供人脸识别技术产品或者服务。

三、要点内容

该《规定》共二十五条，对人脸识别技术使用者处理人脸信息提出了具体的安全要求。

1. 明确了处理人脸识别数据的总体原则

第四条明确：只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，方可使用人脸识别技术处理人脸信息。存在其他非生物特征识别技术方案的，应当优先选择非生物特征识别技术方案。

2. 明确了在不同场所使用人脸识别技术的要求

第六至九条分别对隐私场所、公共场所、组织内部管理、经营场所使用人脸识别技术的要求作了规定。

场所	要求	条款
隐私场所（如旅馆客房、公共浴室、更衣室）	不得安装图像采集、个人身份识别设备	第六条
公共场所	可以安装图像采集、个人身份识别设备，但限于维护公共安全，相关单位对获取的个人图像、身份识别信息负有保密义务	第七条
组织内部管理	应当根据实际需求合理确定图像信息采集区域，采取严格保护措施	第八条
经营场所（如宾馆、银行、车站）	在法律、行政法规规定内可以使用人脸识别技术验证个人身份	第九条

3. 明确了人脸识别技术使用者处理人脸信息的安全要求——人脸识别数据采集、存储、处理、监管等方面的具体要求

第十五条明确：人脸识别技术使用者处理人脸信息，应当事前进行个人信息保护影响评估，并对处理情况进行记录。

第十六条明确：在公共场所使用人脸识别技术，或者存储超过 1 万人人脸信息的人脸识别技术使用者，应当在 30 个工作日内向所属地市级以上网信部门备案。

第十七条明确：除法定条件或者取得个人单独同意外，人脸识别技术使用者不得保存人脸原始图像、图片、视频，经过匿名化处理的人脸信息除外。

第十八条明确：应当尽量避免采集与提供服务无关的人脸信息，无法避免的，应当及时删除或者进行匿名化处理。

第十九条明确：应当每年对图像采集设备、个人身份识别设备的安全性和可能存在的风险进行检测评估，并根据检测评估情况改进安全策略。

4. 明确了相关监督检查主管部门

第二十一条明确：网信部门会同电信主管部门、公安机关、市场监管部门等有关部门依据职责，加强对人脸识别技术使用的监督检查，指导督促人脸识别技术使用者履行备案手续，及时发现安全隐患并督促限期整改。

5. 明确了违反本规定需要承担的责任

第二十三条明确：人脸识别技术使用者或者相关产品、服务提供者违反本规定的，由网信、电信、公安、市场监管等有关部门在职责范围内依照《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规进行处罚。违反《治安管理处罚法》的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

违反本规定，给他人造成损害的，依法承担民事责任。

四、小结

该规定聚焦人脸识别技术应用方面的安全管理，对人脸识别技术使用者、提供人脸识别技术产品或服务提供者提出了具体的安全要求。《规定》的发布表明国家对人脸识别技术应用合规监管的重视，相关者应提高重视，并结合规定的相关内容及《信息安全技术 个人信息安全规范》（GB/T 35273-2020）《信息安全技术 人脸识别数据安全要求》（GB/T 41819-2022）、《信息安全技术 个人信息处理中告知和同意的实施指南》（GB/T 42574-2023）、《网络数据安全标准实践指南——人脸识别支付场景个人信息保护安全要求（征求意见稿）》等国家标准，规范相关行为，避免因不合规而遭到相关处罚。

安全随行 | 智能汽车时代，如何构筑汽车数据的安全围墙？

汽车行业是一个国家制造业软件实力和硬件实力的双重标杆，因为汽车制造产业规模大、技术含量高、产业链长、辐射面广、带动性强，在国民经济中战略地位突出。中国作为汽车制造业大国，汽车制造行业在随着社会技术的不断进步和创新，也在不断的创新与发展中，特别是新能源汽车上升为国家战略，无人驾驶等新技术早已崭露头角，产业互联网蓬勃发展下，针对汽车制造过程的控制变得日益复杂，也令数据的高效、合理使用及其安全防护需求愈发凸显。

根据 Ponemon 和 IBM Security 联合发布的《2022 年数据泄露成本报告》，2022 年全球数据泄露规模和平均成本均创下历史新高，数据泄露事件的平均成本高达 435 万美元，在过去两年中，违规成本增加了近 13%。这些安全事件的发生突显很多企业缺乏足够专业的团队和资源去应对，也没有一套快速、标准、流程化地联动各个部门或资源针对威胁采取有效应对措施的系统。

与此同时，政府对数据安全的要求越来越严格，《数据安全法》、《个人信息保护法》、行业监管等政策法规对企业的业务环境要求越来越高。

2022 年 12 月 13 日，工信部发布《工业和信息化领域数据安全管理办法（试行）》，这是为了规范工业和信息化领域数据处理活动，加强数据安全管理，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家安全和发展利益而发布的行业性质的数据安全管理顶层设计。管理办法明确了开展数据分类分级保护、重要数据管理等具体要求，构建工业和信息化领域数据安全监管体系。

2022 年 3 月 7 号，工信部为落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》等法律要求，加强车联网网络安全标准化工作顶层设计而发布了《车联网网络安全和数据安全标准体系建设指南》，指南针对车载联网设备、基础设施、网络通信、数据信息、平台应用、车联网服务等关键环节，提出了覆盖终端与设施安全、网联通信安全、数据安全、应用服务安全、安全保障与支撑等方面的技术架构。

我国汽标委（SAC/TC114/SC34）下设的“汽车信息安全标准工作组”已分 4 批次累计开展了 15 项标准制定及研究项目，其中《车载信息交互系统信息安全技术要求及试验方法》《汽车网关信息安全技术要求及试验方法》等 4 项推荐性国家标准已正式发布。强制性国家标准《汽车软件升级通用技术要求》《汽车整车信息安全技术要求及试验方法》已立项，推荐性国家标准《电动汽车充电系统信息安全技术要求》已进入报批阶段；《汽车诊断接口信息安全技术要求》等四项标准已提交立项。

汽车行业数据安全解决方案

智能时代的到来，将会凸显很多安全问题，比如：研发设计数据明文存储，无管控；文档数据明文外发使用泄密风险；应用系统 / 数据库无访问控制手段，非法访问窃取数据；邮件外发机密信息；网络外发风险；终端数据明文存储泄密风险；外部使用泄密风险等一系列数据安全的问题。一旦汽车行业遭遇信息安全危机，遭遇危险的可能就不仅仅是企业甚至会殃及那些使用汽车的人，而危险的程度甚至会超出普通的泄露事件，可能还会祸及人的生命。面对如此敏感的信息安全问题，汽车行业必须时刻提高警惕。

亿赛通服务于诸多汽车公司，全面解决近些年来发生的多起电子文档、设计图纸泄露并扩散的安全事件，根据客户自身业务系统进行安全规划，为客户制定完整的数据泄露防护解决方案，实现企业核心信息资产防泄露的安全目标。

从组织体系层面看，汽车制造企业应设立数据安全管理部门或委派专人负责数据安全工作，并建立数据安全团队。该团队负责制定数据安全策略、规程和标准，并监督执行。其次，汽车制造企业应加强内部培训，提高员工的数据安全意识和技能。此外，应建立合理的数据权限控制机制，对敏感数据进行分类管理和访问权限控制。

从制度体系层面看，汽车行业需要制定相应的数据安全管理制度和规范。企业应建立数据安全管理制度，明确数据安全的管理流程和责任分工。例如，制定数据分类分级保护制度，制定数据备份和恢复制度，以及制定紧急事件响应程序等。此外，汽车行业可以借鉴其他行业的通用数据安全标准和规范。

从技术体系层面看，汽车行业需要采用一系列的技术手段来保障数据安全。首先，汽车行业应加强网络安全防护，包括建立防火墙、入侵检测和防御系统，加密通信，隔离内外网和关键数据的网络等。其次，汽车行业需要加强数据加密技术的应用，包括对数据传输和存储进行加密保护，确保数据的机密性。此外，汽车行业还需要建立可靠的身份认证和访问控制机制，以防止非法访问和数据篡改。

从运营体系层面看，汽车行业应建立完善的数据安全运营管理流程和监控机制。企业应建立数据安全审查机制，对重要数据的采集、传输和存储进行安全审查，确保符合相关法律法规和行业标准。同时，汽车制造企业应建立定期的数据安全检查和评估机制，及时发现和解决潜在安全隐患。此外，汽车制造企业还应与相关合作伙伴建立数据安全保障机制，确保数据在合作和共享过程中的安全性。

亿赛通数据安全解决方案是专为企业级用户设计的数据防泄密解决方案，从数据的存储、传输、交换过程中的安全环节，采用了多种加密手段结合的方式保护。从终端、网络和存储三个层次入手，对核心数据的形成、存储、使用、传输、归档及销毁等全生命周期进行安全控制，结合企业特有的业务需求、业务模式和管理文化，为企业制定完整的数据安全防护解决方案，实现企业核心信息资产防泄露的安全目标。

未来，亿赛通将继续积极顺应时代环境和用户需求的变化，找准自身定位，持续创新升级产品和技术，探索制定战略规划，为行业带来更多惊喜！

汽车行业案例

零跑 | 一汽解放 | 上海汽车

东风日产 | 比亚迪 | 长城汽车

欣旺达 | 江铃汽车 | 广州汽车

数据安全治理：打好安全管理与安全技术的协同之战

8 月 16 日，国家安全部发布消息，针对武汉市应急管理局地震监测中心的网络攻击事件，联合调查组已取得新进展，发现了符合境外情报机构特征的后门恶意软件。

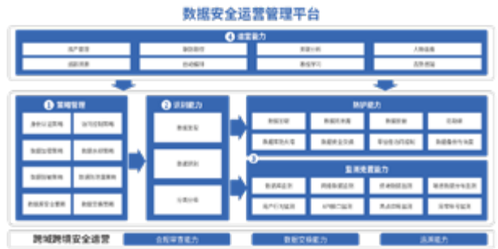
近年来，一些境外组织机构对我国重要数据安全的觊觎屡屡见诸报端。国家聚焦网络攻击活动新动向，跟踪网络攻击技术新特点，组织开展打击危害网络和数据安全犯罪等系列专项行动，依法严惩非法侵入、控制、破坏计算机信息系统等行为，抓获并阻止一大批犯罪嫌疑人，切实维护网络秩序和民众合法利益。

数字经济时代，数据的重要性是无可争议的。特别是在习近平总书记关于网络强国的重要思想指引下，我国网络安全、数据安全工作取得显著成绩，网络安全和信息化一体推进、共同发展，国家安全屏障不断巩固，网络安全技术和产业蓬勃发展。同时，数字化进程的加速得益于我国大力推进物联网、区块链等新技术新应用，坚持创新赋能，激发数字经济新活力，数字生态建设取得积极成效，然而，数字经济快速的发展也给数据安全带来了前所未有的挑战。据 IBM Security 发布的年度《数据泄露成本报告》显示，2023 全球数据泄露的平均成本达到 445 万美元，创该报告有史以来以来最高记录，这表明，企业应对的安全环境变得更加复杂。

对企业而言，数据的安全体系建设中，数据安全治理是基础，在海量高价值数据资产面临各种内外威胁面前，数据安全更需要体系化的建设思路。目前，企业用户对数据安全治理的认知度和接受度已经有较大提高。从需求来看，用户真正需要的是安全能力、安全效果的提升，而不是安全设备、软件等产品的堆砌。目前数据安全市场主流产品品类繁多，例如数据防泄露、数据脱敏、数据加密、数据水印等，但是随着企业部署的数据安全单点产品数量的增多，越来越多缺乏关联性的数据安全工具正在成为企业数据安全治理面临的最大挑战之一。

亿赛通认为，数据安全治理是以“人”和“数据”为中心，基于数据安全合规要求、用户的业务发展需要和风险承受能力等多重因素，通过平衡业务需求与风险，制定数据安全策略，对数据分级分类，对数据的全生命周期进行管理，从技术到产品、从策略到管理，提供完整的产品与服务支撑，实现业务与安全的深层融合。

落实到产品、服务，则需要企业从制度体系建设、安全设备搭建、安全意识培训等方方面面采取行动，这是一个从点到线、再从线到面的过程。正如亿赛通数据安全运营管理平台的能力特点，平台遵循 IPDRR（识别、防御、检测、响应、恢复）能力框架模型，可以为客户提供一个中心、多种安全管理和防护能力，帮助安全管理人员落地安全管理和技术体系的结合，达到数据安全运营管理工作闭环，最终实现数据安全可视、可管、可控、可溯的目标。



这也正符合我公司提出的“分放管服”数据安全建设理念，从业务源头落实对数据分类分级、对人分权分责，制定和实施不同的策略，通过放管结合，构建动态的、主动的、智能的、可运营的数据安全服务于业务的体系，形成“分放管服”的正反馈闭环。从制度层和技术层同时入手，制度主要指导数据安全体系建设，做到有规可依，技术主要保障制度实施，做到有规必依，违规必纠；通过技术不断发现风险，以填补制度漏洞，优化制度，通过制度对技术创新提要求，形成制度和技术的循环优化闭环。

总的来说，面对愈发突出的数据安全风险挑战，数据安全逐渐成为客户关注的焦点。现有客户对安全的期望也在不断的变化，不仅要通过技术来满足安全需求，更对前期规划及后期实施提出了更高的要求。亿赛通承诺，我司将持续履行中国数据安全专家之责，担当起保护数据所有者信息资产安全之任，帮助企事业单位切实做到数据资产可视、数据威胁可管、数据风险可控、数据血缘可溯。

又一高校发生数据泄露事件！罚款 80 万！

近期，南昌公安网安部门工作发现，南昌某高校 3 万余条师生个人信息数据在境外互联网上被公开售卖。南昌公安网安部门立即开展一案双查，成功抓获犯罪嫌疑人 3 名。同时，网安部门对涉案高校不履行数据安全保护义务违法行为开展执法检查。

经查，涉案高校在开展数据处理活动中，未建立全流程数据安全管理制度，未采取技术措施保障数据安全，未履行数据安全保护义务，导致学校存储教职工信息、学生信息、缴费信息等 3000 余万条信息的数据库被黑客非法入侵，其中 3 万余条教职工、学生个人敏感信息数据被非法兜售。南昌公安网安部门根据《中华人民共和国数据安全法》第四十五条的规定，对该学校作出责令改正、警告并处 80 万元人民币罚款的处罚，对主要责任人作出人民币 5 万元罚款的处罚。

随着信息技术的发展和互联网的普及，教育行业正面临着越来越多的数据安全挑战。数据是学校的核心资产和战略资源。高校业务系统之间的数据流通打破数据孤岛，实现数据流动共享，为学校的日常教学、后勤、财务和安防等工作的开展提供有力的数据支撑。将松散的数据沉淀为科学有效的学校数据资产，同时数据安全风险问题也开始突显。

日常数据使用泄露风险

学生信息、家长信息、资助信息等高敏感数据泄露会带来巨大的个人、家庭和社会影响。学生群体的社会经验不足， 易被煽动和洗脑，是诈骗机构、国外反动机构的重要目标。学生往往心智不够成熟，受骗后容易产生严重的不良后果。

黑客攻击风险

校内部分学生缺乏法律意识，为了满足技术好奇心和黑客技术尝试，甚至出于尝试篡改考试成绩等目的，在校园网内通过暴力破解等手段攻击财务、教务等重要的数据库资产，掌握 root 密码后随意的篡改数据，窃取敏感数据。这种行为防不胜防，风险高，后果严重。教务系统由于特殊情况开放公网访问权限，存在学生想毕业，买通黑客篡改考试成绩的事件，风险较大。

内部管理工具混乱风险

学校信息系统和数据库的内部管理工具混乱，很容易引起病毒感染，造成数据库中勒索病毒，导致数据丢失，后果严重。

内部和第三方窃取数据风险

内部和第三方运维人员往往具有高权限的账户，或者没有清理的测试账户，并且能够方便的进出内部网络访问数据库。权限过大、操作不受控的同时，出于外部黑市诱惑、好奇心驱动、同学请求帮助等原因，利用各种便利条件达到窃取数据、篡改数据的目的，防不胜防。

信息公开、发布缺少控制措施风险

学校按要求在门户网站上，发布和公开信息，如奖励信息、资助信息、惩处信息、班级信息、招生考试结果等。由于缺乏有效的技术手段进行控制，很容易由于人为疏忽造成包含了未经脱敏遮蔽的个人隐私信息被公开，引起隐私数据泄露，被追责。

匠心打磨 20 年，亿赛通提出了数据安全“分放管服”建设理念和数据安全治理智能化体系，自主研制了电子文档安全管理系统、数据泄露防护系统（含终端、网络、存储等）、API 审计系统、数据库审计系统、数据库防火墙、数据库运维系统、数据脱敏系统（含动态和静态）、数据交换系统及文件防火墙等，覆盖了“云网端”等场景，构建了数据安全运营管理平台、数据安全态势感知平台及数据安全智能管理平台等。针对学校、机构的数据进行资产扫描、分类分级，加密防护，最后确定管控策略、持续长期运营，形成完整体系构建。

通过多种技术措施发现数据源，对学校数据进行分类分级，对敏感数据存储情况进行识别、定位，能够清晰的掌握数据资产台账。夯实教育行业数据安全保障基础，在重点数据交换及使用区域实现数据审计、脱敏、加密、泄露防护等能力。面向数据资产生命周期进行全流程监管，及时发现违规操作并进行告警和阻断，同时对数据资产进行全盘态势感知，预知潜在风险。通过安全咨询、安全评估、威胁情报、运维保障、应急响应等服务，助力学校各部门协同完成数据安全治理可持续运营。

教育行业数据安全是一项长期而复杂的任务，需要教育机构和政府部门的共同努力。通过加强数据安全措施、加大人员培训和技术投入，可以有效保护教育行业的数据安全。

未来，亿赛通将继续发挥工匠精神，在数据安全领域不断探索前沿技术，提供满足不同客户需求的最优解决方案，为行业客户数据安全提供强有力的保障。

《孤注一掷》火爆热映，揭示了信息泄露的残酷一幕

电影《孤注一掷》正在热映中，影片以真实案例为背景，揭开了境外诈骗全产业链骇人惊闻的内幕，警示观众小心踩坑，不要上当受骗。影片中骗钱夺命的惨案在现实生活中仍不断上演。

随着技术的不断发展和普及，越来越多的人使用互联网进行各种活动，同时也增加了个人信息泄露和被盗的风险。在电影《孤注一掷》中，一个引人深思的主题就是人们信息安全保护的重要性。如今，我们生活在一个数字化的时代，个人信息的泄露和滥用问题日益严重。因此，保护个人信息已经成为我们每个人的责任。

隐私保护

在电影中，主人公为了追溯一起案件的真相，涉及到许多他人的隐私。隐私保护是信息安全的核心内容之一。个人信息的泄露可能导致身份盗窃、诈骗，甚至犯罪行为。因此，我们需采取措施保护个人隐私。首先，我们应该使用强密码，并定期更换密码以保护个人账户的安全。同时，谨慎对待来自陌生人的电子邮件和信息，避免点击可疑链接或下载未知附件。另外，保持软件和操作系统的更新也是非常重要的，因为这些更新通常包含了修复已知漏洞的补丁，有助于防止黑客入侵。同时，政府和法律机构也应加强对违反隐私保护的行为打击，制定严格的法律保护隐私权。

数据安全

数据是信息时代最宝贵的资源之一。电影中的情节揭示了数据被窃取的危险以及其带来的后果。为了保护数据安全，企业和个人需采取措施，包括备份数据，使用加密技术，限制数据的访问权限等。此外，政府应完善相关法律法规，确保企业和机构履行对数据的安全保护义务，并加强对数据盗窃和滥用的惩处力度。

网络安全

电影中的黑客入侵揭示了网络安全的重要性。以网络攻击为手段进行犯罪行为已经成为全球性威胁。为了保护网络安全，个人和组织需增强网络安全意识，关注密码安全、防火墙设置、软件更新等细节。政府应加强网络安全的监管，建立健全的网络安全管理体系，提供技术支持和培训，打击网络犯罪行为。了解不同类型的网络诈骗是非常重要的。常见的网络诈骗手段包括钓鱼网站、电子邮件欺诈、虚假网络销售以及社交媒体欺诈等。钓鱼网站是指那些伪装成合法网站的虚假网站，目的是诱使用户提供个人信息。电子邮件欺诈则是通过发送虚假电子邮件来获取用户的敏感信息。虚假网络销售是指以低价销售商品诱骗用户支付，但实际上并不会发货。社交媒体欺诈则是利用社交媒体平台上的漏洞进行信息窃取和欺诈活动。

面对日益增长的网络诈骗威胁，我们每个人都有责任保护自己的个人信息。通过了解不同类型的网络诈骗、加强个人信息防护以及教育自己和他人，我们可以更好地应对这一挑战，确保我们在网络世界中的安全。

作为国内专业的数据安全专家，亿赛通历经二十年的技术积累和上万个交付项目的沉淀，坚持服务于各行各业，不断自我迭代、创新升级产品服务，以“分·放·管·服”数据安全建设理念为核心，对七大数据场景：综合数据安全、视频专网数据安全、工业数据安全、大数据安全、云数据安全、商业数据安全、个人数据安全进行全方位多维度管理，保障各行业的核心数据资产安全。

亿赛通以“人”和“数据”为中心，从技术到产品、从策略到管理，提供完整的产品与服务支撑，实现业务与安全的深层融合。在人为层面，从决策层制定经营策略、IT策略，帮助企业用户建立数据安全意识，区分职责权限。在数据层面，运用专业技术支撑，通过 AI 算法，关联分析、密码技术、访问控制、数据标识等技术，采集分析各类安全设备结构化和非结构化日志，探测、预测、发现威胁事件和风险，利用技术服务于制度，进而形成技术、制度不断迭代的正循环，建立全面综合数据安全治理能力。整个数据安全治理过程从决策层到技术层，从管理制度到技术支撑，将现有的各个独立的数据安全技术和功能整合，构建了自上而下、全流程、可闭环的完整链条。

亿赛通“分放管服”数据安全建设理念

信息安全是当代社会的重要议题，影片《孤注一掷》引发了我们对信息安全保护的思考。隐私保护、数据安全和网络安全是保护信息安全的关键要素。我们应加强对个人隐私的尊重，注重数据的安全处理和传输，同时提高网络安全意识。

亿赛通将会与您共同努力，保护好自己的信息安全，才能真正生活在一个安全、可靠的数字世界中。

信息安全无小事 | 如何防范才能不做“透明人”？

李雷：我真的好喜欢大明星呀，好想知道他的行程，去看看他！

小亿：快停止你的想法！你最近没看热搜吗？

李雷：什么？我没注意呀！

小亿：高铁员工贩卖明星行程信息被判刑了，你快看看新闻，还有好多信息泄露事件 .....

在当今数字时代，我们的个人信息正面临着越来越大的隐私风险。信息泄露事件频频发生，隐私保护的挑战也在不断增加。众所周知，我们的个人信息是一项非常重要的财产。诸如姓名、身份证号、电话号码、银行卡账号等个人信息往往被用于身份认证、交易结算等重要场景，一旦泄露或被不法分子利用，将可能导致财产损失。以身份证号为例，通过持人身份证号和其他个人信息进行诈骗活动的案例层出不穷，这些案例给个人信息安全提出了迫切的要求。

信息安全无小事！不让自己成为“透明人”！

一、加强个人信息的保密意识。

保护个人信息始于个人，加强个人信息的保密意识是非常重要的。在我们日常生活中，应该养成不将个人敏感信息随意透露给他人的习惯；在互联网上，要注意不在不可信的网站上留下个人信息，尤其是涉及到金融和账户密码等敏感信息。此外，还应当注意不随意公开个人信息，特别是在社交网络上。

二、使用强密码和多因素认证。

在互联网时代，密码是我们保护个人信息的第一道防线。为了提高密码的安全性，我们应当使用强密码：包含大写字母、小写字母、数字和符号，长度不少于 8 位。此外，为了增加账户的安全性，可以开启多因素认证功能，例如手机短信验证码或指纹识别。

三、谨慎使用各类应用程序和软件。

随着智能手机和应用程序的普及，我们的个人信息越来越容易被泄露。因此，在下载和使用各类应用程序和软件时，我们应当谨慎选择，并且在选择之前，应该查看应用程序的用户评价和隐私政策，谨防个人信息被滥用。

四、定期备份和更新个人数据。

在进行电子交易、使用各类应用程序时，我们的个人数据非常重要。为了防止个人信息损失，我们应该定期备份重要的个人数据，并且及时更新软件和应用程序，以保持最新的安全性。

五、关注个人信息的泄露事件。

个人信息泄露事件时有发生，我们应当密切关注这些事件的发展和处理情况。如果发现个人信息被泄露，我们应及时采取措施，如修改密码、报案等。

六、了解个人信息保护的法律法规。

我国有一系列关于个人信息保护的法律法规，如《中华人民共和国网络安全法》等。我们应该充分了解这些法律法规，知道自己的权益和义务。当遇到个人信息泄露等问题时，可以依法维护自己的权益。

作为中国数据安全专家，亿赛通一直专注于产品开发、技术创新和安全能力研究，在自主研发的“分放管服”数据安全建设理念指引下，建立数据安全防护技术手段，分别从数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务五个层面为企业提供全系列数据安全防护产品：电子文档安全管理系统、数据泄露防护系统（含终端、网络、存储等）、API 审计系统、数据库审计系统、数据库防火墙、数据库运维系统、数据脱敏系统（含动态和静态）、数据交换系统及文件防火墙等，覆盖了“云网端”等场景，构建了数据安全运营管理平台、数据安全态势感知平台及数据安全智能管理平台等。通过资产盘点、分类分级、溯源分析、加密防护、安全流转等技术，增强数据的可用、可信、可流通、可追溯水平，实现数据流通全过程动态管理，在数据合规使用中激活数据价值。

二十年风雨兼程，亿赛通已成功打造为数据安全领域专业的综合数据安全厂商，以专业的产品和服务为客户筑牢数据安全底座。数据，关乎发展；科技，理应美好。未来，亿赛通将秉承持续创新的理念，肩负起“保障客户数据资产安全”的使命，引领数据安全产业发展，与更多企业一起打造安心无虞的数字经济世界。

厦门海辰新能源科技有限公司

客户简介

厦门海辰新能源科技有限公司，是厦门引进的百亿级重点项目、福建省重点项目和国家高新技术企业。公司专业从事锂电池核心材料、磷酸铁锂储能电池及系统的研发、生产和销售，拥有核心技术知识产权，致力于以客户为中心，为全球提供安全、高效、清洁、可持续的绿色能源解决方案。

需求背景

随着互联网的快速发展，数字化已经深入到经济社会的各个领域，如何在数字经济新形势下加强对新能源信息的安全防护成为了当下能源企业的重要工作之一。作为福建省重点项目，能源产业的核心及枢纽，海辰新能源对数据安全更为看重，需求也尤为迫切。为此，海辰新能源选择携手行拥有上万家客户且实施经验丰富的亿赛通，共同建设数据保护措施增强优化新能源数据加密系统。

解决方案

1、新一代电子文档安全管理系统：

实现了企业内部电子文件的加密存储，无论是由人工生产还是由应用系统生成的，只要写在磁盘上就是加密形式；

只有被系统授权许可，才可使用这些加密的文件，如未经合法许可将加密文件数据体带走，加密文件内容将不能够被正常打开；

可根据客户需要调整安全等级，可自主设置加密解密。

2、应用安全网关：

通过对经流设备的数据文件进行智能分析，根据设置的安全策略自动进行访问控制和文件加解密处理，将数据安全与企业现有应用系统完美结合，有效地保障了业务系统的连续性和服务器数据的安全性。

项目成果

该项目中，亿赛通采用新一代电子文档安全管理系统的现有功能模块，根据海辰新能源数据保护措施增强优化内部软件加密层级的需求，进行客户化系统开发工作，并结合海辰新能源现有业务系统的相关功能，最终形成一套可实现敏感数据管理、数据追溯的数据安全管理体系建设方案。数据安全管理系统通过移动存储介质管理、数据加密、敏感数据识别、外发管控等相关技术手段，实现终端数据在存储介质交互使用过程中的安全。

欣旺达电动汽车电池有限公司

客户简介

欣旺达电动汽车电池有限公司（简称欣旺达 EVB）成立于 2014 年，是一家集电芯、模组、BMS 和 PACK 研发、生产和销售于一体的全球领先的综合性新能源科技公司，致力于为新能源行业提供具有竞争力、场景化的动力电池解决方案及储能电芯。

需求背景

欣旺达电动汽车电池有限公司专注于便携储能、家庭储能、网络能源、电力储能及智慧能源等领域，以满足客户多元化能源需求为宗旨，提供包括锂电池储能产品、多场景集成方案、能源投资运营等多类型综合能源服务模式。因此，公司内部产品研发、技术数据就是企业生存和发展的命脉，一旦把重要资料泄露，对企业造成的损失后果不堪设想。为了提高其内部数据协同和高效运作，欣旺达选择中国数据安全防护专家—亿赛通作为合作伙伴，共创企业数据安全。

解决方案

1、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；

2、半透明加密：用户能正常打开加密文件，未加密文件不强制加密，也可以根据用户需求与透明加密策略组合使用；

3、打印控制：支持虚拟打印机和物理打印机用户权限和设备控制；

4、权限管理：通过对文档加密授权及角色对应，控制文档在内部受控使用，避免越权使用带来的泄密风险。

5、安全中间件：以接口的方式为应用系统提供加解密能力，应用系统可以根据需要选择加密接口、解密接口、流程接口等进行联合开发；

6、外发管理：通过对文档加密、授权及封装，控制文档在外部传播和使用时造成的泄密风险

项目成果

亿赛通不仅为欣旺达电动汽车电池有限公司部署合理的电子文档安全管理系统，同时使得该企业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。