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　　中国数据安全专家　　www.esafenet.com

05 月刊

2022 年共 11 期

喜报 | 亿赛通顺利入选“网络安全能力评价工作组”国内首批成员单位

安全牛联合亿赛通发布《数据防泄露 (DLP) 选型指南》，彰显行业龙头地位

专业认可，亿赛通强势入围《2022 数据安全产业竞合力洞察报告》

亿赛通持续扩增能源行业客户版图，助推新奥集团数据安全蝶变升级

关注企业官方微信

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

CONTENTS 目录

刊首语 PREFACE

聚焦《亿赛通五月刊》，了解数据安全行业最新动态

党的十八大以来，以习近平总书记为核心的党中央高度重视“构建以数据为关键要素的数字经济，推动实体经济和数字经济融合发展”。随着企业信息化、数字化建设的不断深入，数据已经成为最有价值的资产，很多业务的命运与关键数据紧密相连，数据已成为一个组织创新与发展的核心。然而，数据在为组织创造价值的同时，也面临着严峻的安全风险。来自内外部的针对数据的窃取、滥用、破坏，可能直接颠覆组织的数字化业务。

据某调研显示，全球大规模数据泄露事件呈逐年递增趋势，泄露事件比往年同时段上涨 33.3%。数据防泄露产品作为满足合规要求的重要手段，产业规模将保持快速增长，市场发展潜力巨大。5 月，安全牛与亿赛通联合发布了《数据防泄露（DLP）选型指南》，帮助企业根据自身的环境和需要进行精准地 DLP 产品选型。除安全牛外，中国信通院、嘶吼、中国软件测评中心、中国计算机行业协会等专业机构均有不同安全动向，具体内容，欢迎查阅《亿赛通五月刊》。

国内

1、上海立法保障因防疫采集的个人信息不得泄露

摘要：5 月 24 日，上海市十五届人大常委会第四十次会议表决通过了《上海市人民代表大会常务委员会关于进一步促进和保障城市运行“一网统管”建设的决定》。这一上海市治理数字化领域的综合性决定共 23 条，主要包括“一网统管”建设目标，“一网统管”运行体系，数据赋能基层治理，发挥治理数字化功能、规范推进疫情防控相关应用场景，加强“一网统管”建设保障等五方面内容。《决定》明确，上海运用治理数字化功能，在疫情防控期间，实行个人疫情防控信息核验措施（即“场所码”或“数字哨兵”等核验措施），核验个人健康信息。

2、消费者投诉：珂润官方旗舰店泄露客户信息

摘要：5 月 24 日消息日前，有消费者在黑猫投诉平台发起投诉称，珂润官方旗舰店存在泄露客户信息问题。消费者称，2021 年双十一期间淘宝店铺“珂润官方旗舰店”购买两支洗面奶，在 2022 年 1 月 22 日，接到假客服电话，对方准确说出消费者所有订单信息，包括真实姓名，手机号，订单号，交易金额和购买产品名称等，导致消费者损失 92000 多元。消费者表示，珂润官方旗舰店存在泄露客户信息的问题，与其反馈后至今未有明确答复。其次，此事最开始出现的日期可追溯至一月十号以前，珂润方面未采取有效措施提醒消费者，致使受骗人数直至今日仍不断上升，涉及金额巨大，但珂润方面态度极其敷衍。

3、云南省严厉打击“不良代理投诉举报”，着力优化营商环境

摘要：部分不良代理组织或个人通过违法买卖公民信息，或利用抖音、淘宝、微信公众号等媒体形式，以“代理退保维权”“专业反催收”“买断理赔”“全额退保退息”等名义发布广告宣传收集客户信息，甚至冒充司法机关、监管部门、金融机构工作人员等骗取信任，诱导消费者委托其“代理维权”，要求消费者提供身份证、保单、银行卡、联系方式等敏感信息，唆使或代理消费者捏造事实进行投诉或举报，并阻止消费者与金融机构、监管部门有效沟通，甚至以缠访闹访等手段施压，以达到其收取高额代理手续费、截留套取资金，唆使消费者转购非法理财产品或参与非法集资等目的。上述非法行为可能导致消费者个人信息泄露、资金受损、失去保险保障，甚至遭受诈骗。

4、网上相亲有风险，个人信息防泄露

摘要：海南省网信办相关负责人表示，近年来，大量婚恋相亲类移动应用程序在各应用商店大量上线，凭借其信息来源广泛、操作便捷易用等功能优势于短时间内迅速积攒大量用户注册并收集用户个人隐私信息，存在较大违法违规收集使用个人信息的风险隐患，亟需通过专项治理、责令整改等方式促使相关企业平台加强行业自律和经营规范。

5、多起泄露疫情信息的案例被通报：他们到底泄露了什么

摘要：某医院 5 名工作人员利用职务便利，私自用手机偷拍并通过微信转发传播该院新冠病毒肺炎感染者病程信息，其中包括患者姓名、详细住址、工作单位、诊疗信息等基本情况，造成恶劣影响，其行为已触犯《中华人民共和国治安管理处罚法》第四十二条第六项规定，被当地公安部门依法给予行政处罚。

6、收到“代理维权”短信：投资者小心被割韭菜 谨防个人信息泄露

摘要：2022 年，A 股大盘波动较大，不少投资者在股票市场亏损回撤较大，股民张力军（化名）也受到影响。几个月前，张力军在上海海能证券投资顾问有限公司购买了投资咨询顾问服务，期间市场下跌，海能投顾的工作人员也向其作出风险提示，张力军也对海能投顾的服务表示认可。但 5 月 12 日，张力军收到一条短信，短信来源显示为某法务协助，内容为若需要追回炒股损失，可以帮其申请维权协助。事实上，金融证券领域“代理维权”早已不是新鲜事。近年来，部分非法社会组织或个人假冒专业律师团队、权威专家或金融机构内部人士等，借“代理维权”之名，捏造“维权”事实，向消费者发布，声称“快速维权”“法律援助”，牟取非法利益。

7、两高两部：未成年人犯罪记录“应封尽封”，泄露将被究责

摘要：日前，最高法、最高检、公安部、司法部会签下发《关于未成年人犯罪记录封存的实施办法》（以下简称《实施办法》），全文共 26 条，对未成年人犯罪记录的定义及范围、保密义务及相关责任等内容作出详细规定，基本上解决了目前未成年人犯罪记录封存中遇到的主要问题。《实施办法》自 2022 年 5 月 30 日起施行。

8、空壳贷款公司骗了 200 多人逾百万元

摘要：成都的一家贷款公司，没有放出过一笔贷款，却有几十名员工，事实上这是一个穿着“贷款公司”衣裳的电诈团伙。江都人张先生，就是他们行骗的对象之一。警方循线追踪，成功端掉这一“网贷”电诈团伙，抓获嫌犯 30 余人，截至被抓获，该团伙已骗走 200 多人逾百万元。

9、微信群聊发原图会泄露隐私？网友：不发了

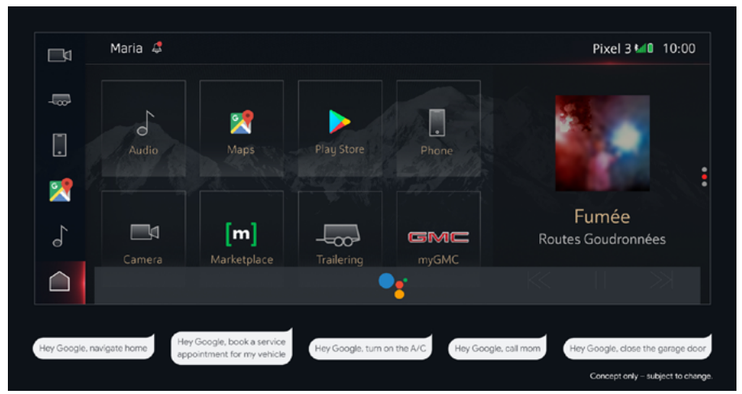
摘要：5 月 25 日，据中国新闻周刊官方微博报道，在微信群聊天时，随意发送照片的原图，会泄露家庭住址等等信息。

10、福建 7 月 1 日起施行！出售泄露信息最高罚 10 万元……

摘要：野蛮分拣快件最高罚 3 万元、泄露用户信息情节严重的处 5 万元以上 10 万元以下罚款……省人大常委会会议，27 日表决通过《福建省邮政条例》，自 7 月 1 日起正式施行。

国外

1、通用客户账户遭黑客攻击 部分个人信息泄露



摘要：据外媒报道，通用提交给加利福尼亚州监管机构的一份数据泄露通知显示，有黑客在今年 4 月入侵了部分通用客户的线上账户，黑客可能获得了地址、电话号码和其他个人信息。

2、扎克伯格被美国检察官起诉！涉嫌参与数据泄露决策

摘要：当地时间 5 月 23 日，美国社交媒体平台 Facebook 的母公司 Meta 首席执行官马克·扎克伯格被美国华盛顿特区总检察长卡尔·拉辛起诉，拉辛指控扎克伯格直接参与了导致与剑桥分析公司相关的数据泄露决策。拉辛在一份声明中指出，有证据表明，Meta 的子公司 Facebook 未能保护其用户的隐私和数据，而扎克伯格亲自参与其中，从而直接导致了相关数据泄露事件。

3、Verizon：数据泄露事件 82% 涉及人为勒索软件威胁上升

摘要：Verizon 的研究发现，在截至 2021 年 1 月底的一年中，勒索软件入侵事件增加了 13%，超过此前五年的总和，员工是组织网络安全体系中最薄弱的环节。《Verizon Business 2022 年数据泄露调查报告》发现，在总共 5212 起泄露事件中，有 25% 是由社会工程攻击造成的。Verizon 表示，结合人为错误和滥用特权，违规行为中 82% 涉及人为因素。

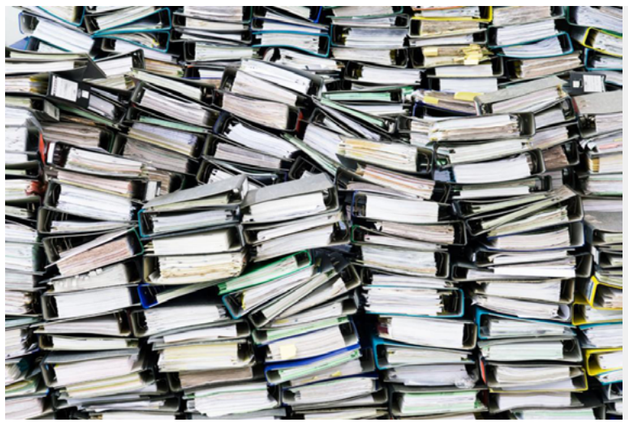
4、揭露“最大规模数据泄露”：上网记录和位置每天被分享七百次

摘要：近日，爱尔兰公民自由委员会（Irish Council for Civil Liberties，ICCL）公布了一份报告，对其认定的一起“史上最大规模数据泄露事件”进行了披露。报告显示，如谷歌、微软等公司会利用实时竞价系统将用户的网络浏览记录和地理位置信息提供给广告商，美国用户每天被分享 747 次，欧洲用户 376 次。谷歌回应称，其一直对与广告商共享用户数据进行严格限制，并要求在投放个性化广告前取得用户同意。

5、68% 的法律部门数据泄露由内部威胁引起

摘要：根据英国信息专员办公室 (ICO) 的官方数据，英国律师事务所超过三分之二 (68%) 的数据泄露事件是由内部人员造成的。NetDocuments 分析了 2021 年第三季度的 ICO 数据。它发现该领域中只有 32% 的违规行为是由外部威胁引起的，例如外部恶意行为者。

6、成人视频网站也遭遇数据泄露



摘要：近日，一家名叫 CAM4 的成人视频网站遭遇数据泄漏，数据内容极其详细丰富，包含 7tb 的姓名、性取向、支付记录、电子邮件和聊天记录——总计 108.8 亿条记录被曝光。

7、为了阻止玩家泄露信息，《绝地求生》开发商疑派出私家侦探

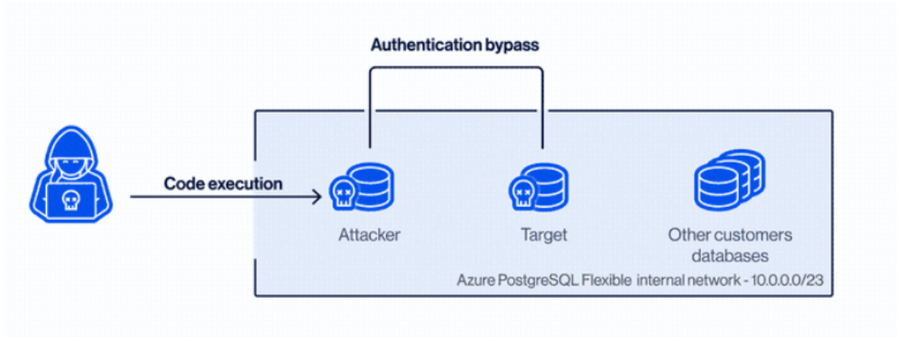
摘要：名为“PlayerIGN”的程序员是《绝地求生》社区的一位知名“舅舅党”，经常曝光一些游戏未来的更新计划和官方信息。之所以获得大量关注，正是因为这位玩家提供的情报极其准确，比如早在一年前，PlayerIGN 就准确预测了 PUBG 即将免费的消息：除了游戏的更新规划，他经常将尚未发布的皮肤图片或者道具信息提前公布，按理说，这样的泄密者应该是所有公司最深恶痛绝的那一类，但由于 PlayerIGN 获得信息的途径是解包游戏数据，所以虽然官方虽然头疼，但苦于找不到泄密者的真正身份，一直没有办法能制止他的行为。

8、安卓预装 APP 被曝高危漏洞，影响数百万用户

```
public void executeSystemCloseProcess(short paramShort, JSONArray paramJSONArray,
    Logger.log("[ExecuteInternal] Executing Close Process", new Object[0]);
    Types.ErrorCode errorCode = Types.ErrorCode.generalError;
    JSONObject jSONObject1 = new JSONObject();
    JSONObject jSONObject2 = new JSONObject();
    try {
      Types.ErrorCode errorCode1;
      String str1 = paramJSONArray.getJSONObject(0).getString("value").trim();
      Shell shell = Shell.getInstance();
      StringBuilder stringBuilder = new StringBuilder();
      stringBuilder.append("am force-stop \"");
      stringBuilder.append(str1);
      stringBuilder.append("\"");
      String str2 = shell.SendCommand(stringBuilder.toString());
```

摘要：微软发现安卓系统中预装 APP 中的多个安全漏洞，下载量超百万。微软在 mce 系统移动框架中发现多个高危安全漏洞，漏洞 CVE 编号分别为 CVE-2021-42598、CVE-2021-42599、CVE-2021-42600 和 CVE-2021-42601，CVSS 评分在 7 到 8.9 分之间。该框架被多个移动服务提供商用于预装的安卓系统 APP 中，攻击者利用这些漏洞可以实现本地或远程攻击。

9、Azure PostgreSQL 中存在跨账户数据库漏洞



摘要：Wiz Research 在目前已被广泛使用的 Azure 数据库 PostgreSQL 服务器中发现了一系列关键漏洞。这个被称为 ExtraReplica 的漏洞允许对其他客户的 PostgreSQL 数据库进行未经授权的读取访问，绕过隔离保护。如果被利用，攻击者可能已经复制并获得对 Azure PostgreSQL 服务器客户数据库的读取权限。

10、PayPal 0 day 漏洞可窃取用户资金

摘要：研究人员在 PayPal 中发现一个未修复的安全漏洞，攻击者利用该漏洞可窃取用户资金。"www.paypal[.]com/agreements/approve" 中发现了一个安全漏洞，攻击者利用该漏洞只需要点击一次就可以诱使用户完成攻击者控制的交易。www.paypal[.]com/agreements/approve 是为 Billing Agreements 设计的，而且只接受 billingAgreementToken。研究人员分析发现可以传递另一种 token 类型，并从受害者 PayPal 账户窃取资金。

喜报 | 亿赛通顺利入选“网络安全能力评价工作组”国内首批成员单位

为落实《“十四五”信息通信行业发展规划》部署要求，大力推动网络安全产业创新发展，构建网络安全能力科学评价体系，引领网络安全技术产品高质量发展，推动形成人才培养、技术创新、产业发展良性生态，在工业和信息化部网络安全管理局指导下，中国信通院于 2022 年初启动了“网络安全能力评价工作组成员单位（以下简称‘工作组’）征集工作”。日前，第一批工作组成员单位信息已公布，凭借数据安全领域研发创新能力及在行业内近二十年积攒的口碑，亿赛通公司成功入选首批工作组成员单位。

网络安全能力评价工作组（第一批）

编号	单位名称	单位类型	参与工作组和对应联系人员信息				
			体系研究	标准研制	能力评价	示范推进	其他
CS-2022-156	北京亿赛通科技发展有限责任公司	安全厂商	√	√		√	

此次工作组的定位为开展网络安全能力评价体系和方法论研究，推进网络安全能力评价标准体系构建完善，组织开展网络安全技术、产品、服务、解决方案等能力评价，促进先进成果应用示范。工作组以安全企业为创新主体、以重点行业需求为牵引，推动供给质量高、需求释放足的网络安全产业结构优化。亿赛通的入选体系研究子工作组、标准研制子工作组及示范推进子工作组等三个主要工作组，证明了我司的技术领先性和产品创新能力。

随着国家自身区块链、大数据、工业互联网、零信任等新型技术取得重大进展，现阶段无疑是网络安全行业科技创新最好的历史时期。因此，提升技术水平，构筑坚实防线，对于进入“十四五”新时代发展步伐的中国来说，就显得尤为重要。作为中国数据安全行业的先行者，亿赛通致力于帮助用户构建更安全、更完善的数据安全防护体系。

亿赛通基于自主研发的技术和丰富的实战经验，最新总结出八大产品创新亮点：多源异构的综合数据安全、跨网数据分级管控、数据互联互通安全流转、大数据处理能力、全生命周期安全防护、终端平台一体化管理、数据安全态势感知平台、智能安全运营，只为让安全更简单。

近期，我司还发布了新一代电子文档安全管理系统，从制度和技术角度为客户建立数据安全防线，制度主建，技术主战，对数据和人实现分权分责分风险，形成放权管责相结合的态势，做到要素服务保支撑，持续安全可运营，确保数据安全流转产生价值， 共建数据安全大生态。系统可有效减少实施时间，省心省力、稳定可靠、简单运维，并且使用无感知，不改变原始文件格式和状态，运行效率高。使用多达 20 余种丰富的安全策略核心技术，将数据资产分类安全隔离，人员定岗定级精细化分级管控。还提供资产分析 / 解密 / 外发 / 传播 / 违规行为等六大安全审计版块，满足集团大规模应用，实现总部与分部数据互联互通。

亿赛通长期以来在各企事业单位安全建设上勤勉深耕，构建全生命周期安全防护体系。我们近二十年不懈努力，坚持自主研发，成为国内专业的安全领域产品服务供应商，为各行各业构建全面数据安全体系奉献力量。

快来上课吧 | 数据安全职业能力培训报名通道正式开启，预定从速

在数字化转型的浪潮下，企业用户在实践中不断摸索数据安全建设的方法，“强化网络安全，数据安全，个人信息保护”被列为 2022 年重点工作之一。然而在数据安全领域始终缺少一个完整的知识脉络来帮助企业和从业者梳理数据安全建设的内在逻辑、数据安全风险的控制方式、以及数据安全能力建设的演进路线。数据安全成为当前最紧迫和最基础的安全问题，对数据安全人才的需求也愈加迫切，而当前数据安全行业人才缺口高达百万！同时随着企事业单位对数据安全的要求逐步提升，对人才能力的需求也水涨船高，数据安全能力认证也成为用人热点，专业认证的数据安全能力证书更是炙手可热！

为了为全方位满足数据安全人才市场需求， 由工业和信息化部网络安全管理局指导，中国软件评测中心与工业和信息化部教育与考试中心联合推出了数据安全职业能力培训。培训包含：数据安全评估师、数据安全工程师、数据安全咨询师、数据安全架构师、数据安全开发人员、数据安全运维人员的职业能力培训。亿赛通基于在数据安全行业的多年实践经验，受邀加入专家组共同开发培训课程，为数据安全领域人才培养提供支撑！

课程大纲

培训课程由培训教师组中的多位数据安全专家共同探讨，学员通过学习培训可以获得企业进行数据安全保护实践所需的不同知识与技能。

时间	数据安全评估师课程	数据安全工程师课程
第一天	数据安全导论	数据安全导论
	数据安全合规	数据安全合规
第二天	数据安全基础知识	数据安全基础知识
	数据安全技术	数据安全技术
第三天	数据安全应用实践	数据安全应用实践
	数据安全在新兴技术中的应用	数据安全在新兴技术中的应用
第四天	数据安全管理部分评估实施规范	数据安全产品部署与维护
	数据安全技术部分评估实施规范	数据安全管理
	数据安全评估管理	数据安全排查
第五天	考试	考试

师资团队

培训讲师均经过多年安全行业积累，技术深厚扎实、经验丰富。对数据安全有深刻理解，能够结合实际的业务场景，按照现代企业数字化管理要求进行深入剖析，让学员切实学到知识，提升数据安全的各方面能力。

证书样本

证书由“工信部教育与考试中心”颁发，受国家认可，证明学员的专业技能达到一定水平，意味着拥有了数据安全行业的从业资格，是学员升职加薪的敲门砖。

课程计划

培训时间：首批培训将在 5 月底开班

培训费用：培训考试费 + 证书费共计 11800 元

证书有效期：三年

报名渠道

报名表

扫码下载报名表

填写完毕后发送至负责人邮箱

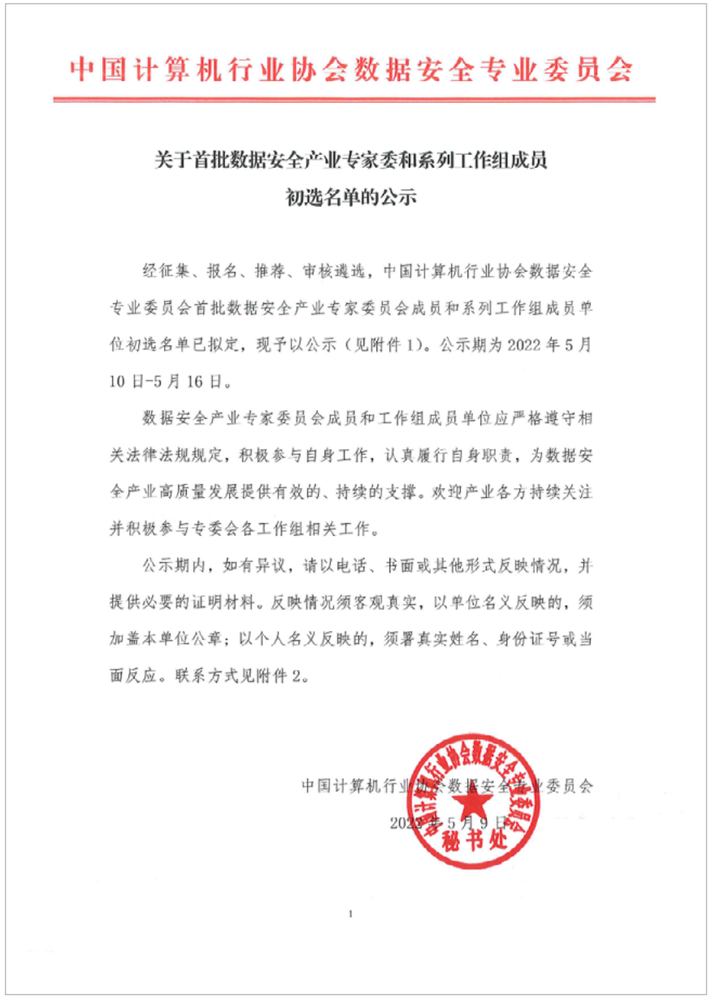
联系单位：北京亿赛通科技发展有限责任公司

负责人：刘慧雯

联系电话：18504569303

邮箱：liuhuiwen@esafenet.com

亿赛通入选首批数据安全产业工作组成员单位，切实推动产业发展良性生态



中国计算机行业协会数据安全专业委员会

关于首批数据安全产业专家委和系列工作组成员初选名单的公示

经征集、报名、推荐、审核遴选，中国计算机行业协会数据安全专业委员会首批数据安全产业专家委员会成员和系列工作组成员单位初选名单已拟定，现予以公示（见附件 1）。公示期为 2022 年 5 月 10 日-5 月 16 日。

数据安全产业专家委员会成员和工作组成员单位应严格遵守相关法律法规规定，积极参与自身工作，认真履行自身职责，为数据安全产业高质量发展提供有效的、持续的支撑。欢迎产业各方持续关注并积极参与专委会各工作组相关工作。

公示期内，如有异议，请以电话、书面或其他形式反映情况，并提供必要的证明材料。反映情况须客观真实，以单位名义反映的，须加盖本单位公章；以个人名义反映的，须署真实姓名、身份证号或当面反应。联系方式见附件 2。

中国计算机行业协会数据安全专业委员会

2022 年 5 月 9 日

秘书处

1

近日，由中国计算机行业协会数据安全专业委员会（以下称“数专委”）组建的数据安全产业专家委员会（以下称“专家委”）首批成员和系列工作组成员单位初选名单已面向社会进行公示。

在数据价值日益凸显，法律监管日趋严格的新环境下，企业数据治理和用户信息安全已经成为影响企业发展潜力和企业竞争力的重要因素。数据安全产业专家委员会的成立，将集聚企事业单位、高校、科研院所中具备数据安全、产业经济等相关领域丰富专业理论、先进技术和实践成果的专家，加快贯彻落实《中华人民共和国数据安全法》，切实提升数据安全保障能力，加速推进国家数据安全建设，实现我国数据安全产业可持续、高质量发展，为产业发展营造良好氛围和安全环境，共同建设开放包容、创新发展的产业生态体系。

亿赛通经组织申报、书面审查、专家评审等多轮考察程序，凭借在安全界内的影响力、技术发展、服务方案等多项优势，成功入选首批专家委数据安全产业研究工作组及数据安全产业人才培养工作组成员单位。

2. 数据安全产业研究工作组（按单位名称首字笔画排序）

成 员 单 位：

北京亿赛通科技发展有限责任公司

4. 数据安全产业人才培养工作组（按单位名称首字笔画排序）

成 员 单 位：

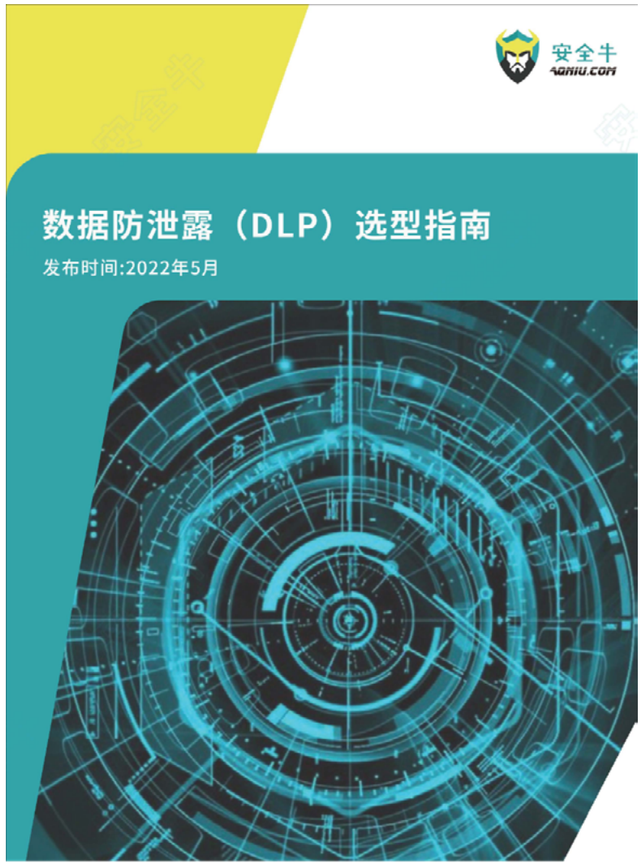
北京亿赛通科技发展有限责任公司

数据安全产业工作组成立的初衷和愿景是加强数据安全创新示范应用，繁荣数据安全产业生态。其中，研究工作组将致力于研究数据安全产业发展政策，攻关数据安全领域前沿技术和产品，夯实产业发展理论基础，推动建设数据安全产业创新体系，实现我国数据安全产业高质量发展。而人才培养工作组将致力于服务国家数据安全治理体系的构建，提高人员数据安全意识，促进数字经济的健康持续发展，培养数据安全专业人才。

各小组将研究构建流程化、规范化的数据安全专业机构服务能力评价体系，并支撑数专委开展相关评价工作；支撑数专委开展组织机构的数据安全能力成熟度评价等相关工作。亿赛通自成立以来，一直聚焦于数据安全方向，致力于成为数据安全行业引领者，此次入选也是对企业数据安全产业的研究及人才培养方向的认可。

通过数专委后续一系列整体举措，必将加快贯彻落实《中华人民共和国数据安全法》，提升数据安全保障能力，引领数据安全技术产品高质量发展，推动形成人才培养、技术创新、产业发展良性生态，加速推进国家数据安全建设。我们将积极配合工作组开展数据安全能力评价体系和方法论研究，推进数据安全能力评价标准体系构建完善，提升行业数据安全建设水平，共同推进数据安全行业发展。

安全牛联合亿赛通发布《数据防泄露(DLP) 选型指南》，彰显行业龙头地位



在现今，企业对信息越来越依赖，随着无纸化办公时代的来临，5G 互联网访问也日益普及。但同时而产生的信息泄密问题正影响着企业的正常业务与发展，企业面临日益严重的敏感数据丢失的风险。可以说，数据泄密已经到了人人可畏的地步，数据防泄露工作成为不容忽视的存在。

2021 年，《关键信息基础设施安全保护条例》、《数据安全法》及《个人信息保护法》正式实施，这三部政策法规与 2017 年已实施的《网络安全法》，共同织起了“三法一条例”网络安全保障网，从国家层面，全面加强了对数据和个人信息的安全管理。

行业方面，金融、电信和互联网、医疗健康、汽车等监管机构分别发布了数据安全和个人信息保护的指引和要求，指导企业和单位的数据安全建设。其中，人行发布的《个人金融信息保护技术规范（JR/T 0171-2020）》明确提出“应部署信息防泄露监控工具，监控及报告个人金融信息的违规外发行为”。工信部发布的《电信和互联网企业网络数据安全合规性评估要点（2020 年版）》提出“涉及存储、处理个人敏感信息和重要数据平台系统配备数据防泄露能力，优先从网络侧和终端侧等进行部署，逐步扩大能力覆盖范围。具备对网络、邮件、FTP、USB 等多种数据导入导出渠道进行实时监控的能力，及时对异常数据操作行为进行预警拦截，防范数据泄露风险。”

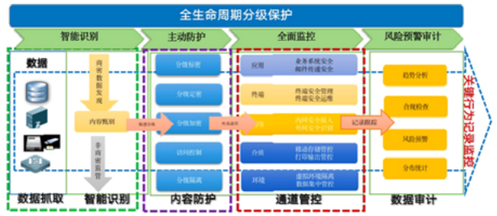
数据防泄露（DLP）技术日臻成熟，成为越来越多组织选择实施的数据安全防护技术手段。数据防泄露产品以深度内容识别技术为核心，在数据存储、传输和使用过程中，发现并监控敏感数据，确保敏感数据的合规使用，防止主动或意外的数据泄露。DLP 产品可以帮助组织降低数据丢失和数据泄露的风险，但是由于 DLP 产品的多样化以及在功能上和性能上的复杂性，导致组织在产品选型时面临挑战，甚至由于选型不当导致部署后无法有效地发挥效用；同时，DLP 厂商也需要花费大量的时间，向组织解释产品选型指标的意义和重要性。

为此，安全牛发起，亿赛通及其他安全厂商联合参编了《数据防泄露 (DLP) 选型指南》研究报告（以下简称为“报告”），供甲方参考借鉴。

亿赛通作为连续六年蝉联中国数据泄露防护市场占有率第一的数据安全厂商，对数据防泄露领域深入钻研，发现目前国内企业普遍存在以下风险：

1. 大量生产设计图纸和技术核心文件没有有效防护；
2. 数据没有合理的分级分类；
3. 终端与其他应用交互时，数据的传输存在泄露风险；
4. 企业安全意识薄弱，没有设立专业的安全管理人员；
5. 与外部单位的合作，对外发出文件数量较多。

亿赛通数据防泄露系列产品包含终端 DLP、网络 DLP、邮件 MailDLP 以及存储扫描 DLP 等，基于企业数据防护方面的需求，提出以事前主动防御、事中检测响应、事后追踪溯源、全程态势感知为设计理念的数据泄露防护解决方案。此方案充分考虑企业业务场景的复杂性，产品易用性，安全管理便捷性以及数据安全与生产效率的最大平衡。最大程度解决企业核心数据难识别、难防护、数据安全难管理的问题。



产品以自然语言处理技术作为内容识别核心引擎，虚拟文件驱动加密作为核心基础技术，可帮助企业对结构化和非结构化数据进行数据治理（文档资产统计、密级标识等）、安全管控（数据加密、权限管理，数据脱敏、边界防护、应用准入、行为审计、数据防护等）、追踪溯源（文档操作、介质操作、用户操作、系统操作等）和态势感知（趋势分析、风险预警、溯源、风险人员画像）。

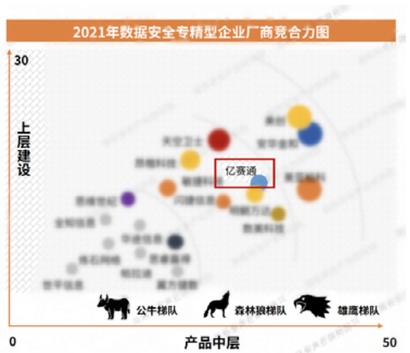
亿赛通数据安全防护解决方案已先后为华润集团、京东方、徐工集团、格力、上海电气集团、千金药业、中国移动、中国电信、中国联通、农业银行、太平洋保险、中信证券、华夏基金、人民银行、零跑科技、长电科技、国家电网、宁波海关、航天科工等众多国内外知名企业进行建设先进、自主、灵活、全面、智能的立体化数据安全防护体系；提供高效、全面、完整、规范的数据安全运营服务。

专业认可，亿赛通强势入围《2022 数据安全产业竞合力洞察报告》

2022 年 5 月 12 日，由嘶吼安全产业研究院撰写的《2022 数据安全产业竞合力洞察报告》（以下简称报告）正式发布。报告通过对参与厂商的竞合力洞察分析，提供了数据安全厂商及其产品、服务和解决方案的竞合视角，深挖数据安全产业的真实发展情况，为资方和甲方提供细节参考。

报告历时两个月的调研、撰写，百余家数据安全厂商踊跃参与，共同深入分析厂商竞合力、盈利模式、发展阶段、典型案例及未来趋势，系统地总结了数据安全产业的市场规模及竞争壁垒，最终成功打造了《2021 年数据安全企业厂商竞合力图》和《数据安全产业需求行为全景图谱》。亿赛通通过在数据安全领域强劲实力与影响力，入围本次两大图谱。

1、成功入围《2021 年数据安全企业厂商竞合力图》



亿赛通以业内产品、解决方案的高认知度，近二十年的技术优势积累及重大项目的丰富实施经验，强势入围数据安全专精型企业厂商。

多年来，亿赛通持续专注于数据安全的技术研究，通过事前主动防御、事中监测响应、事后追踪溯源、全程态势感知四个维度，进行企业数据资产的全流程安全防护。采用人工智能、用户行为分析、大数据分析等创新技术，实现数据资产的分级分类。再根据数据价值和等级的不同，采取不同安全防护手段，确保核心数据重点防护，公开数据或非核心数据轻级管控，实现安全与效率的最大化。

2、成功入围《数据安全产业需求行为全景图谱》

本次《数据安全产业需求行为全景图谱》嘶吼研究院根据自主调研数据，将 2021 年我国数据安全产业主要需求归纳为三大类别、11 个小类。其中，敏感数据共享 / 流通问题、数据安全防护问题、数据资产梳理 / 分级分类问题、数据安全合规问题的厂商数量较多，此类问题具有迫切性和紧要性。亿赛通在图谱中显示，可解决以上四类问题，除此之外，安全人员考核、测评、培训问题、数据安全体系建设问题、数据管理管控问题、数据库相关问题亿赛通也顺利入围。

随着数字经济和信息产业蓬勃发展，5G、零信任、人工智能、区块链等技术加快落地应用，新业态新技术在推动经济转型升级的同时，数据泄露、滥用等风险日益凸显。“十四五”规划等重要文件、《数据安全法》、《个人信息保护法》等法律法规均提出，要推动发展数据战略，统筹数据开发利用、隐私保护和公共安全，规范数据有序流通，保障数据安全。

强化全行业数据安全保障能力，离不开数据安全产业链和生态的有力支撑，在新一轮科技变革和产业变革推动经济发展、我国进入扎实推进共同富裕的关键历史阶段，数据安全生态建设对促进数字产业健康有序发展意义重大。但同时，大批涌入安全行业的厂商给用户的选择造成一定困难，在权威机构进行专业梳理后，为客户提供参考。

本次入围两大图谱，是亿赛通安全技术实力强劲和对市场的深入研究的体现。我们的产品实力已然在网络安全行业内得到了越来越多的关注以及肯定，这将激励着公司继续扎根安全领域，做大做强。

亿赛通与鸿翼联手打造企业内容服务防泄密解决方案，共同探索生态合作新模式

数字时代，信息化水平高速发展，数据成为企业的无形资产，在多数企业中，因发展以及业务需要，各类重要文档资料与企业知识产权相关的数据被高度共享，在企业内部无障碍应用、传输及存储，这些核心数据关系到企业的生存发展以及商业竞争力，一旦泄密，将会给企业造成不可估量的损失。为了保证数据安全，亿赛通与鸿翼融合双方核心产品，推出一套企业内容服务防泄密联合解决方案，旨在解决企业电子资料内部共享过程中，数据资产使用权及所有权的归属问题。

亿赛通经过和鸿翼 ECM 企业内容管理平台的适配，在企业云端以及本地数据共享场景下，针对数据安全性、平台易用性、系统扩展性等问题，制定一整套完善的解决方案，在企业内实现数据文档安全，防止重要资源外泄，提高企业数据安全保护能力，保护单位资源和效益，同时不对日常办公、开发产生负面影响，达到安全与效率的平衡。最终实现以“加密敏感数据”、“控制敏感内容流通”、“规范员工访问行为”为抓手，以“带不走、打不开、读不懂”为控制目标，以平衡效率和安全为原则，基于文件过滤驱动技术实现企业重要数据资产的全生命周期保护，达到合规和安全并行的目标。

方案详情

本次联合方案在鸿翼 ECM 企业内容管理平台的基础上，构建以文件加密为核心，权限管控为辅助的企业内容服务数据防泄密解决方案，实现：

文件加密

对文档进行高强度加密并对使用者透明解密。满足数据安全保护的同时，操作简单，应用方便。

应用灵活

与业务实际情况进行结合、实现对文档灵活的管理。能与鸿翼的工作流引擎结合，灵活调用亿赛通中间件的加解密接口或者外发制作接口，在工作流程中针对文档进行加解密或者外发文档制作操作。

外发控制

根据业务需要，对需要与合作伙伴进行交互的外发文件进行特殊处理，在满足企业正常业务运转的情况下，最大限度的保证文件的安全性。

离线办公

充分适应企业离线应用需求，对出差人员提供离线时长限制，保证离线人员可以正常使用加密文件，同时防止泄密。

日志审计

提供详细的日志审计功能，对管理人员以及终端用户的操作行为进行详细记录。

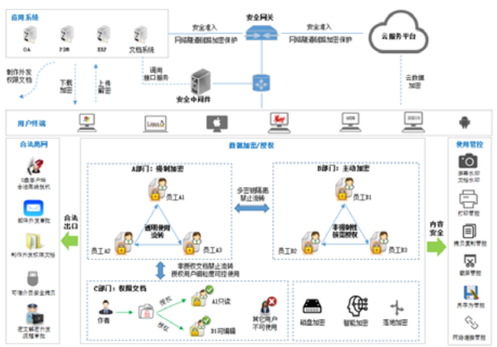
系统集成

与鸿翼以及用户的 OA、代码管理配置平台以及其它业务系统等进行无缝集成，利用动态加解密技术实现服务器中的数据存放明文，下载到终端或离线后的文件自动加密，防止终端泄密或扩散。

分布式部署

部署方式灵活多变，采用异地部署统一管理的模式，适应企业网络环境，同时与企业已有 AD 域进行集成认证，实现单点登录。

方案部署详情



关于鸿翼

上海鸿翼软件技术股份有限公司（以下简称鸿翼），是国内领先的 ECM（企业内容管理）及智能大数据管理服务商。基于先进的非结构化数据获取、存储、管理、安全、洞察和数字化技术而形成的多种产业化应用，构建了完整而又具有开放性的非结构化数据管理体系；融合领先的 NLP 自然语言处理、深度学习、知识图谱、可视化技术以及大数据应用管理技术，打造一系列大数据智能管理解决方案。鸿翼业务覆盖智能制造、工程设计、金融、医药、能源、军工、政府等多个行业，为贵州大数据局、中海油、上汽集团、扬子江药业集团、招商银行等逾 5000 家政企客户提供 ECM 产品及解决方案。

方案实施效果

通过智能动态加解密技术，对终端文件进行强制加密处理，从文件创建开始即可自动加密保护，对鸿翼 ECM 企业内容管理平台下载的文件自动加密，且不同部门可按需进行加密，在保障用户核心数据安全情况下，兼容文档交互效率。通过对核心数据进行全生命周期保护，确保核心数据只可在企业安全域内正常、透明使用，通过任意方式将数据非法带离内部环境将无法正常使用。

当用户通过鸿翼内容客户端上传文件至鸿翼 ECM 企业内容管理平台时，文件在平台中自动解密，不影响员工在鸿翼内容服务平台进行在线预览、在线编辑等操作；同时配合内容安全管控，实现敏感数据文档的拷贝、粘贴、另存、内容拖拽等行为的控制，管控用户操作文件行为规范，对用户的文件操作行为进行审计记录，保障后期追溯能力。

数据安全治理之数据脱敏

售前技术部：马梦续 / 文

数据安全的现状通过社会上的一些重大事件都可以体现出来。一些安全事件，比如 Facebook 的数据泄露、万豪酒店客户信息泄露、特斯拉源代码泄露等，然后是相关的法律法规、还有标准文件的出台，比如《中华人民共和国网络安全法》、《信息安全技术 个人信息安全规范》、《中国银行业“十二五”信息科技发展规划监督指导意见》、《银监会信息科技风险现场检查指南》中都有对数据去标识化，进行脱敏的规定。

看到这些安全现状可以体现出，我们在对数据进行共享流通的时候其实是不畅的，我们想对数据进行挖掘和分析的时候会受到这些东西的制约。但是实际上我们对数据价值释放的期待是非常巨大的，我们依旧需要一些技术手段解决这些问题。

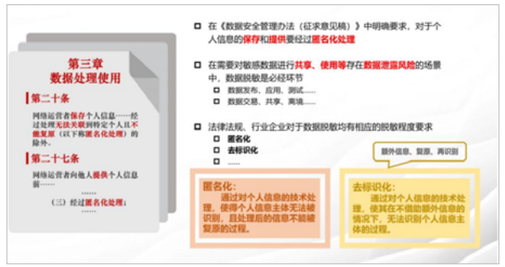


图 1——数据脱敏需求

在各种法律法规文件内容中有要求到，对于个人信息的保存和提供要经过匿名化处理，然而我们在正常生产和使用过程中，很多环节需要对敏感数据进行共享和使用，这时候都是存在一些数据泄露风险的场景，这些场景中数据脱敏是必经环节。法律法规和行业要求，对数据脱敏的时候有相应的脱敏程度要求，比如匿名化、去标识化，其中匿名化是对

亿赛通小贴士 ESAFENET PROMPT

个人信息处理之后，使得个人信息主体无法被识别。去标识化是处理后不借助额外信息的情况下无法识别个人信息主体的过程。

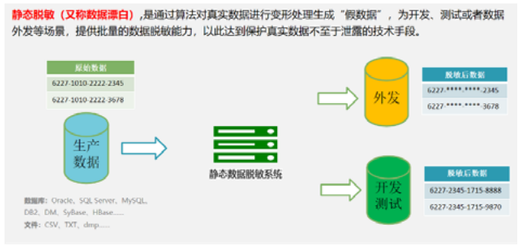


图 2——数据脱敏效果

上面是一个具体的脱敏例子，这是一些身份证号、个人信息等，这些常见的数据一定是敏感数据，这样一串信息需要要进行脱敏会得到右边图上的结果，首先最明显的看到部分信息已经被打码，又或者完全替换成另外一串数字，手机号使用的是常见的中间四位、最后四位掩码，身份证号变成另外一个号码。同时对于身份证号这种有很明显的标准结构的数据进行脱敏的时候，可以使数据维持相应的结构，这样一种脱敏的做法可以保持数据一定的可用性，如果在挖掘分析中需要使用时是很有用的。

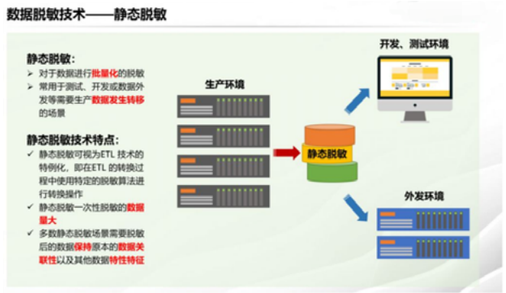
数据的可用范围，正常情况下敏感数据是只能存在于生产环境中，经过脱敏之后就可以在测试环境中存储、在开发环境中存储以及对外部开放访问。敏感数据主要可能有个人隐私数据、企业业务数据，还有数据分级分类之后安全级别很高的核心数据。

还有脱敏涉及的数据源、数据类型，最早的数据源都是关系型数据库，尤其是数据类型部分以结构化的为主，后续也有了大数据体系的数据源，有了更多非结构化的数据。最早数据脱敏的主要是针对数值和文本这种很基本的数据类型，现在对于图片、对音频、视频都有脱敏的需要。

脱敏技术中两个比较重要的概念，一个是静态脱敏，还有一个是动态脱敏。静态脱敏简单说就是对数据进行批量化脱敏，一般用在测试开发或者是对外进行完整的数据集外发的场景中，主要特点是数据会发生批量的转移，静态脱敏这个技术可以视作是 ETL 过程中转换的步骤变成脱敏算法，整体跟 ETL 很像。

数据静态脱敏：

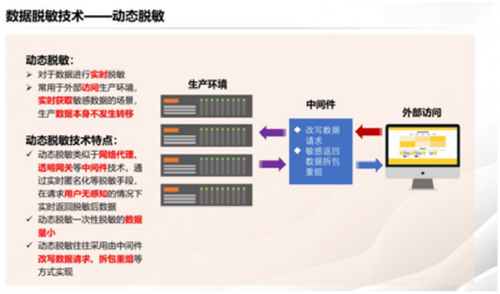
静态脱敏应用的场景，刚才说到有一些结构化的数据或者有一些数据的统计信息，我们希望它能够在脱敏之后继续保持，这个数据集的可用性是不能被破坏的，这个时候静态脱敏的很多算法是能够做到这一点的。



数据动态脱敏：

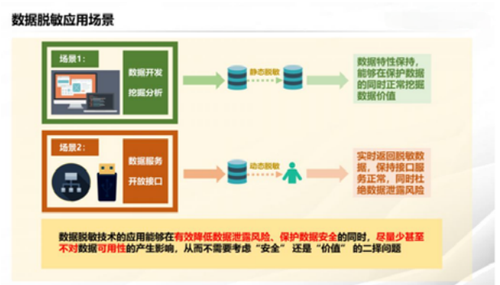
动态脱敏定义是相反的，一般是对数据进行实时脱敏，常用于对外提供访问接口的时候，外部可以访问我们的数据，实时获取数据的场景。有的数据过来，一天有很大的流量，但是单个脱敏的时候，数据量都是比较小的，它的技术实现一般是通过透明网关等中间件技术，使得脱敏方案在用户无感知的情况下给用户返回脱敏后的数据，另外还有改写数据请求的这种方式。

对于动态脱敏有一些场景没有纳入进来，这里说的是比较传统的场景，还会有一些比较新的需求，比如源端流式的数据过来的时候，希望采集过来就能实现脱敏，这实际上也是属于动态脱敏的例子。



具体的脱敏应用场景，以上提到了两个比较典型的，一个是数据开发的时候需要对数据进行挖掘分析，这个时候就用到了静态脱敏，因为我们需要对一个完整的数据集进行脱敏，脱敏过程中还要保持数据的特性，保持数据特性之后才能从中挖掘出数据价值。

另外是动态的场景，比如数据服务，我们要对外提供开放的接口让他访问数据，这个时候显然是动态脱敏的场景，保证正常服务的同时，杜绝数据泄露的风险。从前面对数据脱敏技术的介绍可以看到，数据脱敏可以在有效降低数据风泄露风险、保护数据安全的同时，不对数据的可用性产生影响，从而不需要考虑安全还是价值的二择问题。



亿赛通作为国内早期做数据安全的企业，有着自己独具特色的数据安全能力模型，从终端、存储、网络和云等几个方面对数据安全进行防控。我司的数据脱敏系统面向敏感数据通过脱敏规则进行数据变形，实现敏感信息的可靠保护的数据脱敏产品。产品可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，包含静态脱敏系统（DMS-S）和动态脱敏系统（DMS-D），应用于开发测试环境、数据交换、数据分析、数据共享等场景。

又一次“亡羊补牢”，通用汽车遭撞库攻击致使客户信息泄露

传统汽车行业加速数字化转型。当前，全球汽车制造业正迎来深刻变革，数字化技术快速渗透进汽车制造的各个环节，越来越多的汽车制造商主动拥抱互联网、大数据、人工智能等新一代信息技术。汽车制造商数字商业模式创新勃发，同时，传统汽车制造厂商与数据科技公司合作日趋紧密，欧盟、美国、日本等国家和地区的汽车制造商通过投资并购以及与创新型科技公司合作等方式，积极打造数字化生态系统，提升汽车智能化水平和用户驾乘体验。但是便捷、先进的数字化技术同样给汽车制造商带来不小的麻烦。

近期，通用汽车表示他们在今年 4 月 11 日至 29 日期间检测到了恶意登录活动，经调查后发现黑客在某些情况下将客户奖励积分兑换为礼品卡，针对此次事件，通用汽车也及时给受影响的客户发邮件并告知。为了弥补客户所受损失，通用汽车表示，他们将为所有受此事件影响的客户恢复奖励积分。但根据调查，这些违规行为并不是通用汽车被黑客入侵的结果，而是由针对其平台上的客户的一波撞库攻击引起的。

黑客通过收集网上已泄露的用户和密码信息，生成对应的字典表，并尝试批量登录其他网站后，得到一系列可以登录的用户。经后续的调查，通用汽车表示目前没有证据表明登录信息是从通用汽车本身获得的，“未经授权的用户获得了之前在其他非通用汽车网站上被泄露的客户登录凭证的访问权限，然后在客户的通用汽车账户上重复使用这些凭证。”对此通用汽车要求受影响的用户 在再次登录他们的帐户之前重置他们的密码。

黑客入侵通用汽车账户时可获得的其他信息包括汽车里程历史、服务历史、紧急联系人、Wi-Fi 热点设置（包括密码）等。但帐户里不包含出生日期、社会安全号码、驾驶执照号码、信用卡信息或银行帐户信息，因此这些信息没有被泄露。

除了重置密码外，通用汽车还建议受影响的用户向银行索取信用报告，如有必要还可进行账户安全冻结。不幸的是，通用汽车的在线站点不支持双重身份验证，所以其网站无法阻止撞库攻击。不过还有一种做法是客户可以给所有的支付动作添加 PIN 码验证环节。至于受影响的客户数量，通用汽车只向加州总检察长办公室提交了一份通知样本，因此我们只知道该州受影响的客户数量，也就是略低于 5,000 家。

随着各行各业数字化转型的深入，各种内部威胁、外部威胁、恶意程序，以及各种业务安全场景，如薅羊毛、虚假交易，撞库等安全事件频发，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》、《等保 2.0》、行业监管、企业审计等政策法规对企业的业务环境要求越来越高。面对安全运营的新形势，亿赛通独特的数据安全建设理念，配合设计咨询服务、产品方案、工程交付及售后服务四大体系，根据云、网、端三类应用场景对产品线进行扩充，实现数据安全理念建设的可落地执行，从不同维度为用户提供产品和服务，形成一体化智能管理，打造数据安全领域真正意义上的综合解决方案。

当前企业面临日益严重的数据安全治理问题，安全体系建设迎来巨大挑战，亿赛通数据安全产品族全系列 67 款产品着眼于数据安全刚需及合规性需求，实现数据全生命周期的安全管控，实现涉密信息、个人信息和重要数据的有效保护。未来，数字化触及的领域会不断深入，安全防护的难度也会不断加大。面对全球经济发展不稳定因素急剧增加的发展环境，企业更需要准确把握企业安全防护的发展方向，趋利避害，发挥好新技术、新产品的优势，以规避数字化过程中带来的风险与挑战，为企业安全的长远发展保驾护航。

亿赛通持续扩增能源行业客户版图，助推新奥集团数据安全蝶变升级

近期，由亿赛通负责建设实施的新奥集团数据安全项目顺利完成，双方携手共建能源数据安全防护体系。该项目中，亿赛通依托行业专业的项目实施经验、自主可控的数据库安全产品以及优质的响应服务获得客户的肯定和认可，为双方后续深度合作奠定了良好基础。

关于新奥集团

新奥集团以“创建现代能源体系、提高人民生活品质”为使命，致力于成为一家受人尊敬的创新型智慧企业。1989年新奥创立于河北廊坊，以城市燃气为起点，逐步覆盖了分销、贸易、输储、生产、工程智造等天然气产业全场景，贯通清洁能源产业链，为客户提供智能化低碳综合能源服务，助力绿色发展。基于丰富的产业实践，新奥以“场景是基础、物联是关键、数据是资源、平台是载体、智能是目的”为建设思路，搭建了基于物联网的产业数智平台，赋能千行百业，推动产业智能升级。

项目需求

此前新奥集团及各产业公司基于各自运营场景和业务痛点，已经上线过数字化产品，并且进行云端部署，但由于云端部署后数据安全问题就日益突出。特此新奥集团启动了相关数据安全项目，准备采购数据库审计产品，以满足安全管理和监管合规需要。

解决方案

亿赛通数据库安全审计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，具体内容如下：

1、操作记录全量审计

系统对数据库操作行为进行全面的审计，包含操作风险审计和会话事件审计。通过建立审计规则，捕获 SQL 语句进行语法分析 , 实现高效而精准的审计分析。

2、危险操作实时监控

通过规则设置对各类数据库操作访问行为进行实时监测，对网络中的异常数据库操作行为及时进行告警响应。

3、操作行为统计分析

对数据库实例提供多维度和不同时间粒度的审计记录统计功能，帮助用户高效地掌握数据库运行的安全态势并快速锁定风险目标。

4、安全审计合规报表

通过动态报表的方式对数据库操作行为审计结果进行统计分析。系统内置丰富的报表模板，符合 SOX 法案、等级保护等法规标准需求。

5、轻量旁路阻断能力

系统针对某些运维数据链路，若发现有危险操作，可对此数据链路进行通信阻断，防止可疑终端通过此链路进行后续危险操作，从而避免数据库受到损害。

项目成果

项目经过双方团队的配合，实现了对集团数据库的实时监控、全程管理，满足行业合规需求、防止非法数据窃取和破坏，提供数据安全事件溯源和追责依据。确保新奥集团数据库安全、稳定运行，保障核心数据资产的安全性、准确性、权威性。

打造新一代互联网企业安全标杆，亿赛通提升凌迪数字科技敏感数据管控能力

近期，亿赛通签约浙江凌迪数字科技有限公司，建设数据安全治理项目，为企业数据安全驻防。

典型案例 TYPICAL CASES

客户简介

浙江凌迪数字科技有限公司（Style3D）成立于 2015 年 11 月，总部位于浙江杭州，是一家以技术赋能进行柔性快反供应链管理的时尚科技企业，核心产品有服装 3D 数字化建模软件、3D 数字化设计研发管理 SaaS、3D 数字化服装供应链交易平台，致力于以技术赋能进行柔性快反供应链管理，更好地满足新时代的时尚消费需求。

项目需求

作为一家高新技术研发企业，凌迪数字内部管理是典型的互联网管理模式，员工日常工作和应用场景复杂，人为操作不可控等因素越来越多，给内部信息管控带来极大的挑战。为此，凌迪数字为有效进行日常行为规范，达到文件流转合理，文件外发可查，文件流转可追溯，违规事件 / 行为可记录，前端无感知，后端可分析的的目的，联手行业经验丰富的亿赛通，建设凌迪数字数据安全治理项目。

亿赛通凭借领先的技术优势，以及多年来在各行各业积累的经验，并结合客户的特点，为其量身打造了符合国家安全规范及满足企业长久发展使用的产品及解决方案。

解决方案

亿赛通对客户公司进行软探针部署，通过通过机器学习、大数据分析、溯源取证、UEBA 等技术，对用户、数据、应用、设备进行综合分析，帮助其将每一次数据活动与实际用户、设备和应用程序进行关联的数据资产分析管理和用户行为分析产品。对用户进行数据资产管理、数据资产监控、用户实体行为分析，帮助用户解决数据资产监管、暗数据威胁、内部恶意行为、主机检测受损等威胁。

1、行为全记录

对行为全面记录包括操作行为、应用行为、网络行为、数据行为。这些可能包括主文件表记录、事件日志、注册表蜂箱、更改日志、内存快照和其他源。

2、精确快速定位

用户分析数字资产时，系统会消除复杂的手动过程，快速识别出是谁触碰了该资产，并实时自动将移动数据与实际用户关联起来。

3、降低误报

将数据资产自动关联到实际用户可以实现精确的用户分析，最大程度降低误报率，节省大量的人力成本和资源的浪费。

4、日志报表

提供丰富报表呈现功能，可以根据用户需求，多维度、全方面展示用户数据流动、风险等。也可以定制用户独特业务展板，满足企业多元化需求。

项目成果

经过实施部署，凌迪数字已可通过数据分析，进行违规文件流转预警，辅助行为轨迹记录，能第一时间发现违规事件。对内部员工进行规范化统一管理，保护重要信息的无外泄，且操作无感知。项目的建设，有效防止用户“有意”、“无意”数据泄露行为，确保业务的连续性，达到安全性与易用性的深度融合，从而更好的提高用户体验。