

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



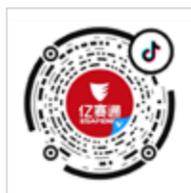
关注官方微信公众



关注官方微信服务



关注官方微信视频



关注官方抖音号

同心同行 一起向未来，亿赛通 20 周年庆典圆满落幕

嘶吼联合亿赛通发布《网络安全服务市场洞察报告》

推动数据安全高质量发展，亿赛通出席 2023 年中国网络和数据安全产业高峰论坛

科创中心“核”动力 | 亿赛通：中国数据安全领域“守护者”

嘶吼专访 | 亿赛通总经理崔培升：“分放管服” 四步双闭环建设数据安全



同心同行
一起向未来

—2023亿赛通20周年庆典—



20周年庆典



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

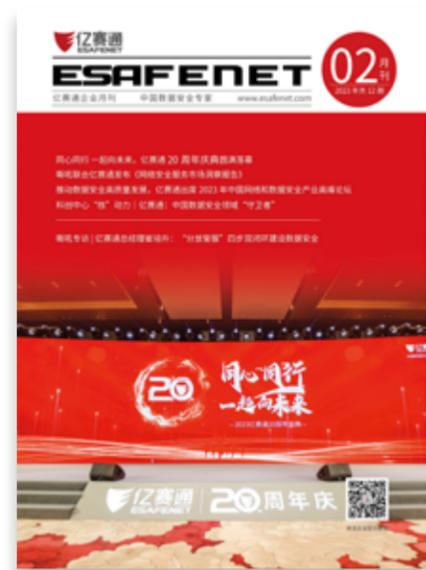
地址：北京市海淀区西二旗大街 39 号 A 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com



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 我们的二十年

行业聚焦 INDUSTRY FOCUS

4-7 国内行业新闻

8-11 国外行业新闻

亿赛通动态 ESAFENET NEWS

12/13 喜报 +1 | 亿赛通连续 5 次上榜 CCSIP 中国网络安全行业全景图

14/15 重磅升级 | 亿赛通“分·放·管·服”数据安全建设理念 V2.0 版正式发布

16/17 嘶吼联合亿赛通发布《网络安全服务市场洞察报告》

18-21 嘶吼专访 | 亿赛通总经理崔培升：“分放管服”四步双闭环建设数据安全

22-24 亿赛通助力“百城千园行”活动，独家分享工业互联网安全建设经验

24/25 亿赛通全力支持首届数据安全大赛，祝贺大赛圆满结束

26/27 亿赛通受邀出席重庆市数据管理能力成熟度评估模（DCMM）宣贯会

28/29 推动数据安全高质量发展，亿赛通出席 2023 年中国网络和数据安全产业高峰论坛

30-32 同心同行 一起向未来，亿赛通 20 周年庆典圆满落幕

33-35 科创中心“核”动力 | 亿赛通：中国数据安全领域“守护者”

亿赛通小贴士 ESAFENET PROMPT

36/37 疑似大量个人信息泄露，快递行业风波再起

38/39 政策解读 | 亿赛通专业解读《关于促进数据安全产业发展的指导意见》

典型案例 TYPICAL CASES

40/41 数据库安全综合解决方案

42/43 商业秘密保护解决方案

我们的二十年



亿赛通 20 周年庆

回首二十年

从 2003 到 2023，是亿赛通卓越而又辉煌的二十年；
 七千日风雨成劲旅，二十年汗水铸辉煌；
 亿赛通从默默无闻淬炼成为行业翘楚！

这是激情梦想、努力拼搏的二十年；这是破茧成蝶、历尽繁华的二十年；
 这是追求卓越、成绩斐然的二十年；二十年，成就了亿赛通今日的荣光！

历程

历史我们不能忘记
 二十年风云变幻，从非结构化数据到结构化数据再到综合大数据，有过成绩和希望，也有过失败和迷茫；
 二十年孜孜以求，从数据资产管理到数据安全防护再到数据安全流转，我们始终将客户的需求与时代脉搏紧密融合；
 二十年卧薪尝胆，从数据泄露防护到数据安全防护再到数据安全专家，我们坚持开拓创新，团结奋进、完成一次又一次历史的锐变；

风雨同舟共进退，戮力同心续辉煌！二十年，我们不忘初心，二十年，我们不畏险阻，亿赛通人用专业彰显自信，用责任践行初心。

感恩

一路走来，是你们不惧风雨，与“我”携手同行；
 是你们不辞劳苦，与“我”共度春秋；
 是你们在晨星交替中，与“我”共度五年、十年、二十年

坎坷磨砺中“我”已经长大，顺境时我们欢呼雀跃，分享成功；逆境时我们不离不弃，亲如一家，任何困难也阻挡不了我们前进的步伐！

展望

海阔凭鱼跃，天高任鸟飞
 让我们把握新机遇、迎接新挑战，在未来的工作岗位上绽放光彩，
 不忘初心，砥砺前行，以竞无止境之心，昂首赢战未来！
 历创业之艰难，庆二十载而流芳
 望未来之峥嵘，树百年基业而辉煌
 新岁序开 共赴新程

同心同行，一起向未来！亿赛通 20 周年生日快乐！

国内

1、“谁泄露了孩子信息”？孩子即将中考，湖南女子突然接到这样的电话 ...



学校招生办曹老师

2月13日 晚上21:45

您好，我是曹老师

以上是打招呼的内容

2月13日 晚上22:04

你已添加了学校招生办曹老师，现在可以开始聊天了。

2月13日 晚上22:15

曹老师好

您好

摘要：近日，长沙家长周女士（化名）每天要接到多个“推销”电话。而打这些电话的人，或自称是职业院校的，或自我介绍是某校外培训机构，但对她孩子的个人信息几乎都是了如指掌。其中有老师向她极力推荐学校的公安消防类专业，还准确掌握了她孩子的身高和视力情况等信息。周女士回忆，2月初新学期开学时，学校老师曾通过一款班级常用的小程序收集过一次学生信息，不仅包括父母姓名、联系方式等，还包括了孩子的身高、体重、视力等信息。没过多久，她就开始陆续接到自称是职业院校和校外培训机构的电话。

2、江苏检察机关依法对曹广晶涉嫌受贿、泄露内幕信息案提起公诉



摘要：近日，徐州市人民检察院就湖北省人民政府原党组成员、副省长曹广晶涉嫌受贿、泄露内幕信息案已向徐州市中级人民法院提起公诉。检察机关起诉指控：曹广晶利用担任原中国长江三峡工程开发总公司副总经理、原中国长江三峡集团公司副总经理、原中国长江三峡集团公司董事长、湖北省人民政府副省长等职务上的便利，为他人谋取利益，利用职权或者地位形成的便利条件，通过其他国家工作人员职务上的行为，为他人谋取不正当利益，非法收受他人财物，数额特别巨大；曹广晶作为内幕信息知情人员，在内幕信息尚未公开前，泄露给他人，致使他人从事与该内幕信息有关的股票交易，情节特别严重，依法应当以受贿罪、泄露内幕信息罪追究其刑事责任。

3、“爱徒”泄露内幕信息，校园“股神”跌落神坛



摘要：林某原是某大学财经学院教授，多年来对证券投资多有研究，是公认的校园“股神”。由于工作和兴趣皆与证券投资相关，闲暇时林某常与陈某等昔日的学生相约登山，谈论股市、投资等信息，林陈二人也因此结下了亦师亦友的深厚情谊。2013年陈某作为C公司重大资产重组项目财务顾问成员，参与筹划Y公司与C公司重大资产重组事项，知悉了重组测算结果，成为该重大资产重组项目的内幕信息知情人。内幕信息敏感期内，陈某与林某保持着频繁的电话联系，向自己志同道合的老师泄露了Y公司重大资产重组的内幕信息，随后在Y公司股票停牌前，林某即利用其多位亲友账户集中交易Y公司股票，累计交易金额890余万元，短短几个交易日获利1,470余万元。

4、2023年考研试题被泄露？大量考生信息被曝光，网友：希望彻查！



摘要：哈尔滨工业大学的学生组成的志愿者团队，竟然能接触到考研的考试袋。这些志愿者不仅拿到考试袋，还可以随意浏览大量考生的信息。更重要的是，这些志愿者竟然将考生的信息以及试卷袋带等都拍照，然后在网络进行发布，所以才引起舆论的争议。公众目前的疑问主要有两个。第一，按照国家的研究生招生规定，任何单位在进行招生试卷的处理过程当中，都是不能够拿手机到相关的场所里面。为何这志愿者却可以这样做，还要把考上的个人信息都泄露出来？第二，目前我们只是看到这些志愿者曝光考试袋以及考生的个人信息。但是从网络的传言来看，部分志愿者可能已经看到内容，特别是考研笔试题里面的答题卡，是否已经出现泄露的问题？

5、宝利国际易主告吹，深交所：内幕信息泄露？

深圳证券交易所

关于对江苏宝利国际投资股份有限公司的关注函

创业板关注函〔2023〕第74号

江苏宝利国际投资股份有限公司董事会：

2023年1月18日，你公司披露《关于筹划公司控制权变更事项的停牌公告》，2月2日你公司披露了《关于控股股东、实际控制人及其一致行动人签署投资框架协议、股份转让协议、表决权放弃协议暨控股股东、实际控制人拟发生变更的提示性公告》，2月12日晚间，公司发布公告称，收到周德洪与周秀凤通知，因江苏东祁提出终止原协议，同时周德洪与周秀凤尚未收到股份转让协议约定的任何转让款项，因此于2月11日与江苏东祁及保证人上海红瑞企业管理有限公司、东台市鑫科新兴产业基金合伙企业（有限合伙）、邓杰、李永红签署了《解除协议》，终止本次控制权变更。我部对此表示高度关注，请你公司核实并说明以下事项：

1. 请你公司详细说明控制权转让终止的具体原因，交易

摘要：2月14日因接盘方“爽约”，宝利国际控制权变更终止，深交所14日向宝利国际下发关注函，追问是否存在内幕信息泄露及信息披露不及时等情形；相关人员是否存在利用内幕信息进行股票交易的情形等。

6、公民个人信息频遭泄露，最高检：将深挖关联犯罪追溯泄露渠道



个人信息

安全学习那些事儿

摘要：2023年2月9日，澎湃新闻从最高检了解到，2019年1月至2022年10月，全国检察机关共批准逮捕涉嫌侵犯公民个人信息犯罪嫌疑人1.3万余人，提起公诉2.8万余人。

7、一个电话就骗走 20 余万元



摘要：日前，福建省福州市反诈中心接到市民阮某某报警，他接到自称支付宝客服的来电，称要为其解决花呗信用问题。听信对方话术的阮某某按照电话里的引导，将22.8万元欠款转账到指定账户，之后才意识到自己被骗。近几个月以来，诈骗团伙冒充金融平台客服人员，以帮助消除不良征信为名实施的虚假征信类诈骗案件数量，一度出现激增。公安部门提醒，公众接到此类电话需提高警惕。

8、新野一医院未严格履行网络安全保护义务被处罚



摘要：近年来，新野县公安局网警大队持续深化网络安全监督检查，强化安全防范意识，督促落实网络安全主体责任，提升单位内部网络安全建设水平。此前，新野县公安局网警大队民警在工作中发现，某医院网络存在信息系统未进行等级保护定级测评、管理制度不完善，未严格履行网络安全保护义务，并且未能按照网络行政执法检查要求整改到位，警方对该医院及相关主体责任人处以行政处罚处罚。

1、美国法警局称曾遭遇安全漏洞事件致敏感信息泄露



摘要：2月27日，美国法警局 (USMS) 发言人表示，法警局于2月17日遭遇安全漏洞事件，导致敏感信息泄露，受影响的系统包含执法方面的敏感信息、法律程序的相关信息以及与美国法警局调查对象、第三方和某些雇员有关的个人身份信息。发言人称，司法部将对此取证调查。

2、时隔近两年，斯坦福大学再遭数据泄露



摘要：2月24日消息，美国斯坦福大学被曝在2022年12月至2023年1月期间发生了数据泄露事件，涉及897名正申请博士学位的研究生。

3、多家科技巨头提醒员工：不要泄露！不要泄露！



摘要：年初以来，在发现 ChatGPT 生成的文本中有疑似商业机密的情况下，不少科技巨头开始提醒自己的员工不要在使用 ChatGPT 时输入敏感信息数据。据报道，在一条从企业内部通信工具 Slack 泄露的信息中，亚马逊的公司律师称，他们在 ChatGPT 生成的内容中发现了与公司机密“非常相似”的文本，可能是由于一些亚马逊员工在使用 ChatGPT 生成代码和文本时输入了公司内部数据信息，该律师担心输入的信息可能被用作 ChatGPT 迭代的训练数据。

4、百事可乐遭遇恶意软件攻击发生数据泄露



摘要：据报道，百事可乐装瓶风险投资有限责任公司遭受网络攻击导致数据泄露，攻击者在百事可乐瓶装风险投资公司的网络中安装信息窃取恶意软件并从中提取数据。

5、因数据泄露和网络中断 韩国运营商 LG Uplus 首席执行官公开道歉



摘要：韩国第三大移动运营商 LG Uplus 为最近的数据泄露和网络攻击事件道歉，并承诺在未来几年每年将投资 1000 亿韩元（7790 万美元）来提高其网络安全能力。在 1 月 2 日被推测为黑客攻击的网络安全事件当中，LG Uplus 的 29 万名客户的个人信息（包括姓名、出生日期和电话号码）遭到泄露。韩国互联网安全监管机构直在调查此案，但数据泄露的原因尚未确定。

6、美国五角大楼内部军事邮件泄露：没有密码，谁都能看



摘要：美国网络安全研究员透露，美国国防部可能出现数据泄露：其在没有密码的情况下，将约 3T（1T=1024G）的内部军事邮件储存在微软专为美国政府提供的 Azure 云端，时间长达两周。这意味着，任何知道该网页地址的互联网用户，都可以浏览其中的内容和相关数据。不过报道指出，由于美军的机密数据无法通过互联网进行访问，现目前可能泄露的数据都不是机密数据。

7、动视暴雪一边被黑客攻击，一边被挖墙角，屋漏偏逢连夜雨



摘要：动视暴雪遭受大规模黑客攻击，导致许多敏感的员工信息和未来游戏计划，有人正在有针对性收集大量游戏源代码和重要文件，有分析称，黑客这次是通过一次网络钓鱼攻击的方式，获得对个人员工详细信息的访问权限，并且顺藤摸瓜，从而导致重要数据遭到泄露。泄露的敏感员工信息可能包含个人详细信息包括：全名、地址、密码、薪水等可能已经泄露。

8、Cl0p 勒索软件团伙声称：使用 GoAnywhere 零日漏洞闯入了 130 家组织



摘要：Cl0p 勒索软件团伙近日声称自己策划了最近利用 GoAnywhere MFT 安全文件传输工具的一个零日漏洞的攻击，表示已从 130 多家组织窃取了数据。该安全漏洞现在被编号为 CVE-2023-0669，使攻击者能够在未打补丁的 GoAnywhere MFT 实例上获得远程执行代码的权限，管理控制台暴露在互联网上，谁都可以访问。

喜报 +1 | 亿赛通连续 5 次上榜 CCSIP 中国网络安全行业全景图



2月1日,网络安全行业门户网站FreeBuf发布《CCSIP 2022 中国网络安全行业全景册》。亿赛通作为数据安全行业的代表厂商,凭借领先的产品技术架构和强大的自主研发实力入选数据防泄漏 DLP、数据安全管控(平台型)、数据安全治理(解决方案)、数据库安全、数据脱敏、勒索软件防护、邮件安全、视频专网、安全咨询与培训教育、风险评估等十大细分领域。

此前 FreeBuf 咨询已累计发布四个版本全景图册,为企业 提供网络安全产品选型参考,帮助企业了解中国网络安全技术与市场的发展趋势。本次第五版全景册改变原有呈现形式,以 PDR 网络安全模型为基础,并参考 IPDRR 安全框架和 P2DR2 模型,在基础的 Protection(防护)、Detection (检测)、Response (响应)三层逻辑上优化

出第 4 层,形成“防护—检测—响应—持续改进”的安全闭环。在核心模型之外,另增加了网络基础安全与业务场景 2 个大类,构建完整的企业网络安全建设链。

1、数据安全



2、计算环境安全



3、物联网安全



4、安全服务

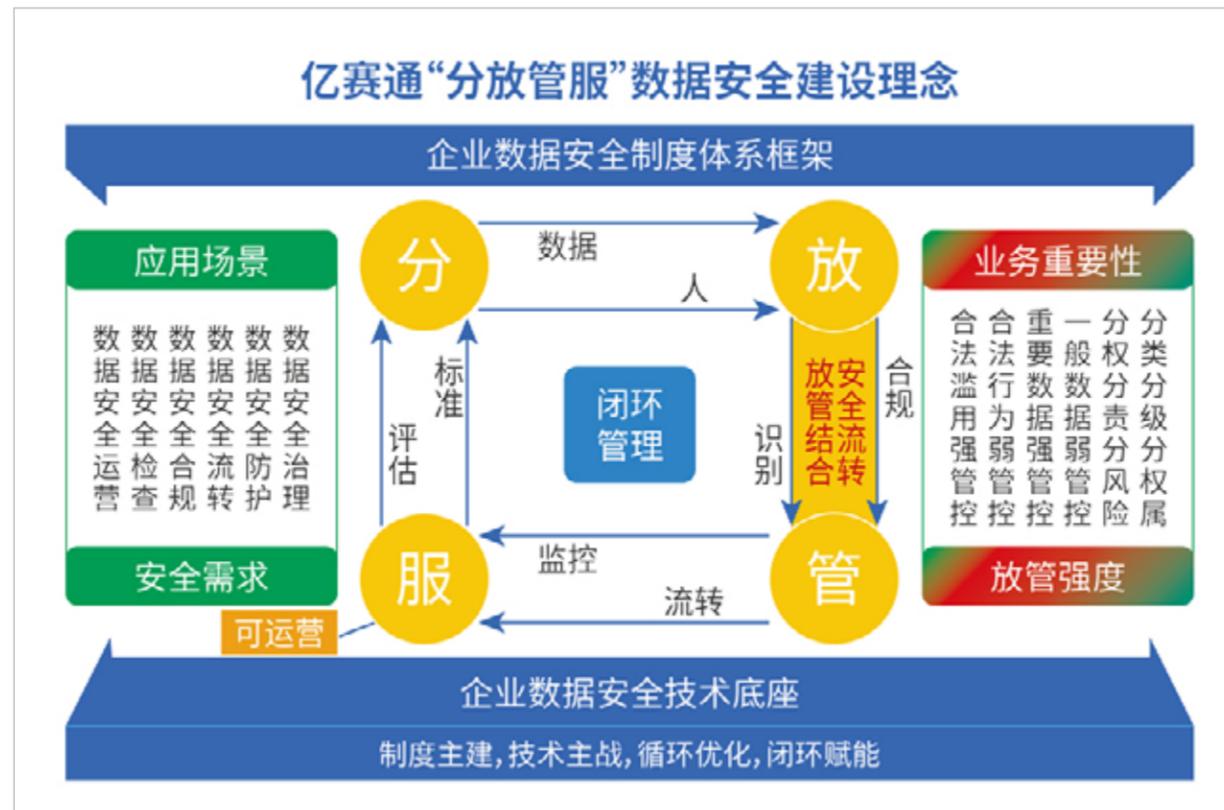


现如今,由于很多企业缺乏足够专业的团队和资源去应对各种内部威胁、外部威胁、恶意程序,以及各种业务安全场景。内部也没有一套完整的系统能快速、标准、流程化地联动各个部门或资源,导致撞库、勒索病毒、内部泄露等事件频发。

与此同时,国家对数据安全的要求越来越严格,安全等保、行业监管、企业审计等标准、法规对企业的业务环境要求也越来越高。面对安全运营的新形势,亿赛通独特的“分·放·管·服”数据安全建设理念,配合数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务等五大属性,根据云、网、端三类应用场景扩充产品线,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,形成一体化运营管理,打造数据安全领域真正意义上的综合解决方案。切实解决了企业数据安全治理难题,因此可以成为多份行业报告、全景图的重要代表厂商。

亿赛通再次上榜 Freebuf 全景图册,充分体现了公司多年来自主研发的技术优势和市场实际应用验证的品牌实力!接下来,亿赛通将继续致力于推动数据安全产业发展,通过对自身技术实力的提升,不断巩固在国内数据安全产业的已有优势,为用户业务提供更强大的数据安全治理能力支撑,借助自身的创新力带动更多行业创造更大价值。

重磅升级 | 亿赛通“分·放·管·服” 数据安全建设理念 V2.0 版正式发布



2020年，亿赛通在业内首次推出“分·放·管·服”数据安全建设理念V1.0版，在理念的指导下，我司细分五大产品属性、六十款+精细化产品。如今，“分·放·管·服”数据安全建设理念V2.0版，正式发布，即将开启亿赛通数据安全体系开发新纪元~

理念V2.0版从基于分、放、管、服四个层面的理解，过度到以“数据和人”为对象的两大革新、四步双闭环体系。

革新一

“分·放·管·服”数据安全建设理念V2.0版以“数据和人”为对象构建的数据治理、防护、流转、运营的双闭环体系，帮助企业形成扎实可靠的综合数据安全能力，为企业数据资产从产生价值到保值、增值的建立重要保障。

革新二

1、闭环一

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、智慧的、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。

2、闭环二

从制度层和技术层同时入手，制度主建指导数据安全体系建设，做到有规可依，技术主战保障制度实施，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。

分的意义

分是把人和数据分开，制定不同的制度，应用不同的技术。对于数据要进行分类分级，识别数据属性、所有权，依法并依据企业实际业务归类，根据敏感或重要程度分级，逐渐形成重要数据资产化，重要信息敏感化，然后根据类和级定策略进行保护。对人要区分对象，分清职责和权限，权责对等，并减少特权账户，根据职责和权限匹配业务策略，匹配数据策略，确保权责和数据重要程度匹配，和业务的重要性匹配，有利于保障业务在保证数据安全的情况下畅通运行。

放的意义

放要建立在“分”的基础上，在做好数据分类分级、账户分权分责之后制定“放”的策略，并且配备有识别机

制根据策略选择放行。有规则 and 标准以及事后管理的，一般数据和合规行为可以放行，但要配备事后审计，问题溯源。“放”是相对的，要与“管”结合来做。

管的意义

管是用行政工具和技术工具管确保对象（数据和人）在约定的范围内按制度运作。“管”的技术工具有很多种，比如DLP、加密、合规审查工具、脱敏、隔离交换、血缘分析工具等等，管理工具和业务场景及业务重要性匹配非常重要，“管”最大的问题是适度，管控强度和业务重要性需要进行适配，一般数据进行放行和弱管控，重要数据强管控，合法合规行为弱管控，合法合规行为滥用强管控。

放管结合

放和管是动态结合的，面对复杂的业务场景、多种类大批量的数据以及频繁变化的接触数据的人，需要及时调整放和管的策略，通过放管结合化被动为主动。

服的意义

服指的是数据安全制度体系和技术手段都是为企业业务服务的，业务数据是核心，确定数据的所有权、使用权和经营权，让数据能够合理合法的被使用和交易，确保数据信息不泄露、数据资产不流失，让数据在保证安全的情况被使用和交易，想更好的为业务本身服务，需要搭建数据安全运营管理平台，建立数据识别能力、防护能力、监测处置能力，搭配安全策略，形成综合运营能力。

整体来说亿赛通“分·放·管·服”数据安全建设理念V2.0版制度和技术的坚持和数据同步的原则，符合“同步规划、同步建设、同步运营”的三同步理论。另外，双闭环体系的可操作性，可高效帮助企业快速提升自身综合数据安全能力，达到数据安全治理、防护、流转和运营的目标，保障数据业务合法合规，业务安全可持续运营，真正实现效率与安全的最佳平衡。

嘶吼联合亿赛通发布《网络安全服务市场洞察报告》

2023年2月8日，嘶吼安全产业研究院联合亿赛通发布了“至人无己 正复为奇：网络安全服务市场洞察报告（以下简称“《报告》”）”。《报告》在中国网络安全产业变革的关键期，聚焦安全服务，通过对行业及安全厂商的整体分析，深挖安全服务的真实发展情况，为资方和甲方提供细节参考。

在实现网络强国的重要思想背景下，我国高度重视、大力推进网络安全和信息化工作，并明确指出，网络安全是实现网络强国战略的四梁八柱之一，网络安全服务业则是网络安全事业前行的基础，为网络强国目标提供技术、人才、资源的支撑。

根据嘶吼安全产业研究院调研数据显示，2022年中国网络安全服务营收达到105亿元，较比2021年的89亿元增长18%。但2022年安全服务在网络安全中的占比仅为12%，和2021年占比水平基本持平，占比率未见明显增长。

在安全服务领域，亿赛通凭借业内的良好口碑、安全服务的高认知度，顺利入选报告安全运营、安全咨询、安全保险、安全培训的领域，且分别收录4个解决方案。

亿赛通「平台&体系化」典型案例

亿赛通「平台&体系化」典型案例

亿赛通「平台&体系化」典型案例

平台化	安全运营中“基础运营”具有平台化特征典型性分析	亿赛通
体系化	安全运营中“定制运营”具有体系化特征典型性分析	亿赛通

亿赛通「流程&标准化」典型案例

亿赛通「流程&标准化」典型案例

亿赛通「流程&标准化」典型案例

流程化	安全运营中“基础运营”具有流程化特征典型性分析	亿赛通
标准化	安全运营中“定制运营”具有标准化特征典型性分析	亿赛通

在《报告》发布会中，亿赛通专家分享了《基于分类分级的数据安全服务建设》主题演讲。在国家政策的支持及约束下，数据安全产业的发展态势日盛，传统安全服务商、云服务商、专业数据安全服务商等层出不穷，产品细分和应用也越来越，与业务的结合也越发紧密。在数据安全的建设中分类分级起着至关重要的作用。

在亿赛通看来数据分类分级是数据治理的基础，是平衡利用和保护之间的重要依据之一。近两年，国家对数据安全要求越来越高，企业在数据合规的过程中发现诸多困境，如：无标准难规范、有标准落地难、已落地难应用等。

而亿赛通数据安全服务就是通过数据发现、数据整理、分类有序等步骤让数据从无序到有序。经过二十年数据安全建设方法论+全行业实施经验，深入了解数据使用业务场景，关注用户数据价值，识别数据安全与风险评估，基于整体数据安全防护规划，进行防护目标的差异化分析，给予综合专业数据安全治理建议，以实现数据安全防护价值，建立数据安全防护体系。

新服务模式打造用户信赖的数据安全解决方案

一个中心：通过管理平台对数据在全场景的分布、流转进行可视化管理，量化数据安全防护成果，提升安全管理工作的效率。

四个领域：从企业的数据安全组织建设、制度流程、技术工具、人员能力方面同步开展建设工作。

六个建设步骤：

- 1. 安全制度建设：**对企业数据资产进行统计，明确定义资产分级标准，梳理重要部门商业秘密清单，明确保护对象，制定完善的数据安全管理制度，敏感操作流程审批制度；
- 2. 安全体系建设：**以数据分类分级为基础，通过梳理合规和安全需求，进行安全体系调整及安全架构分析，体现安全价值的同时保障业务连续性及不改变或不改变员工工作习惯，进行数据质量管理体系建设；
- 3. 风险评估服务：**在漏洞检测、管理、修复、审计和预警的整个过程进行持续监控和闭环管理，提高应急响应质量和效率；
- 4. 安全培训服务：**通过对数据安全法律法规的解读和讲解，帮助企业领导和管理者了解数据安全的红线，数据安全保护的重要性和监管要求；
- 5. 合规对标服务：**依据国家法律法规为基础、行业指标为辅助，最大程度满足企业和国家安全标准的契合，

通过将企业内部的相应合规制度收集和建立起来并遵循合规制度，制定符合国家安全要求、行业安全要求、企业安全要求的相关制度，提高员工安全意识、降低因合规产生的安全风险；

6. 安全复审服务：组织在数据安全建设的工作中，有两大方面需要应对：一方面，是监管机构会对整体的数据安全状况开展检查；另一方面，是监管要求银行需要自查，即通过内部审计或委外审计的方式对自身数据治理进行审计。

安全服务正进行着深刻的产业变革：从服务能力来看，正朝向主动、可感和精细化方向发展；从服务模式来看，价值提供模式得到广泛认可；从服务人才来看，对人才能力的培养与要求同步推进，未来，服务将更加侧重安全的实际落地与项目实施。亿赛通将服务提升到一个全新的高度，即通过“人”与“技术”让安全检测与安全管理更便捷，帮助企业构建安全有序的数据使用环境，为企业安全赋能。

文章部分内容来源于《报告》



嘶吼专访 | 亿赛通总经理崔培升： “分放管服” 四步双闭环建设数据安全

随着《中华人民共和国数据安全法》、《数据出境安全评估办法》、《网络数据分类分级要求》等法律法规和标准的陆续颁布，数据安全发展的政策趋势越来越明朗，但要落实到企业实践当中，还必须有科学的方法作为指导，才能让数据安全和业务融合在一起，数据跑的放心，安全做的有价值。

工欲利其事，必先利其器。近日，亿赛通总经理崔培升根据自身近二十年时间的网络安全行业实践和经验，在实战中淬炼出“分放管服”四步双闭环建设数据安全理念，其超前、系统、全面的数据安全理念，为业界提供了一定的科学指引。



亿赛通总经理 崔培升

为此，嘶吼对他进行了独家专访，深刻解读数据安全建设的最新思路。

“分”是源头

基于安全行业的大好前景及相关了解，崔培升逐步走进网络安全领域。自2015年起，他开始着手管理亿赛通，聚焦更具前瞻性的数据安全赛道。

在崔培升看来，2015年国务院提出的“放管服”的改革理念，从简政放权、放管结合、优化服务三个方面梳理行政权和市场关系，同样可以适用指导从制度和技术层面来建设数据安全。

但是，还有一个前提是必须确定管理对象。从违规角度讲，数据本身不会违规，所有的流动都是人的意志，违规的一定是人，所以也要把对数据进行操作的人管理好。那么做好数据安全就要增加一个“分”字，分清人的行为和数据这两个管理对象，这样就形成了“分放管服”的数据安全建设理念。

对于数据要进行分类分级，识别数据属性、所有权，依法并依据企业实际业务归类，根据敏感或重要程度分级，逐渐形成重要数据资产化，重要信息敏感化，然后根据类和级定策略进行保护。不同行业数据模型有很大差别，基本原则是一样的。

在技术上，首先要建立模型，对数据进行准确的定义以及关联分析。通过机器学习，对已有的数据要具备扫描和鉴别能力，对新的数据打上标签，定义为核心数据；其次结合不同场景，从而进行数据分类分级的精准落地。

崔培升强调，“分”很关键，不能“眉毛胡子一把抓”。比如一般数据处理若增加了审批过程的复杂度，就会降低业务效率；如果把企业核心数据定义为重要数据或者一般数据，降级之后有可能会造成数据泄露的损失。

对于人要区分对象，分清职责和权限，权责对等，并减少特权账户，根据职责和权限匹配业务策略，匹配数据策略，确保权责和数据重要程度匹配，和业务的重要性匹配，有利于保障业务在保证数据安全的情况下畅通运行。

“人”是指内部人员或“内鬼”，而非外部黑客，在每个业务上是不同权限的合法用户。公司应该根据治理安全框架，通过层级，开放权限，赋予“人”不同的权利。一旦发生变动，要及时通过系统预警进行处理。

“分”是源头，非常重要。数据分类分级没做好就会导致乱管，越管越乱，限制了业务发展，阻碍了数据流转，最后业务部门抵制；或者对人的权限职责没有分好，造成突破规则、侵占公共数据、滥用或者泄露重要数据等行为，数据安全得不到落实。

实现“分放管服”双闭环建设

数据安全的外延越来越大，前几年，基本上数据防护要求做到不泄露即可，但是现在数据作为第五大生产要素，更要求数据要产生价值，以及保值增值。

尤其是云端、网端、终端都有数据，数据的暴露面很大。不同场景下，接触到数据的不同用户，在应用过程当中，有些行为会导致数据的量变引起质变，造成严重的数据安全问题。所以，一定要对人和数据进行分类分级，根据不同层级，制定相应的对策，根据业务的匹配程度去实行“放”和“管”。

“放”是明确数据自由流动程度及合规账户能做什么，目的是为了业务的便利性，让数据快速高效的运转服务于业务。“放”一定是有规则 and 标准以及事后管理的，一般数据和合规行为可以放行，但要配备事后要进行审计。

审计的目的有三个：一是防止新的数据和账户未做好合适的分类分级和分权分责，二是防止特殊审批造成数据和账户权限超出安全底线，第三更重要的是审计由量变到质变引发的安全问题，一个合规账户下载一条业务信息是正常处理，下载一百条有可能就超出了正常业务的范围，需要预警和处置。

制定制度是“管”的依据和行政工具，安全产品是“管”的技术工具，分类分级和分权分责是确定对象和范围，用行政工具和技术工具管确保对象在约定的范围内按制度运作

就是“管”。“管”的技术工具有很多种，比如 DLP、加密、合规审查工具、脱敏、隔离交换、血缘分析工具等等。

由于数据爆炸性增长，由静态数据安全做到动态数据安全，由被动数据安全做到主动数据安全，由单一数据安全手段做到智慧综合数据安全，是非常难的，需要一个不断持续加强的过程。这就需要能够时时监测到数据状态的变化以及针对数据的行为，需要“服”来完成。

“服”指的是数据安全制度体系和技术手段都是为企业业务服务的，业务数据是核心，确定数据的所有权、使用权和经营权，让数据能够合理合法的被使用和交易，确保数据信息不泄露、数据资产不流失，让数据在保证安全的情况下被使用和交易，这就是围绕数据做安全在业务层面的意义。



总体来说，“分放管服”数据安全建设理念是一个以“数据和人”为对象构建的数据治理、防护、流转、运营的双闭环体系，帮助企业形成扎实可靠的综合数据安全能力。

第一个闭环是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、智慧的、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。

第二个闭环是从制度层和技术层同时入手，制度主建指导数据安全体系建设，做到有规可依，技术主战保障制度

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。

业务从“单一”走向“综合”

崔培升表示，现在只提供单一安全产品的厂商，面对用户的“一揽子”解决需求，必须拥有一个能够提供完整的解决方案的综合能力。

因为数据的存在形式非常多，针对不同的数据类型，需要不同的应用产品，结合业务，才能满足用户的各种需求。

如何能更好的为业务本身服务？需要搭建数据安全运营管理平台，建立数据识别能力、防护能力、监测处置能力，搭配安全策略，形成综合运营能力。

事前能了解每一条敏感数据从产生到存储使用到流转销毁的全生命周期过程，能了解用户对数据的所有操作，实现数据资产的时时动态分析；事中定期扫描敏感数据和高危行为，及时发现风险，并预警及处置，事后能做溯源取证、关联分析。

亿赛通以文档加密起家，迄今已有 20 多年。目前已经发展成为国内第一家既有结构化数据、非结构化数据和数据平台的安全企业。

崔培升表示，“分放管服”双闭环建设理念符合数据安全建设的三个阶段：数据治理、数据防护、数据流转，与此同时，每个阶段也需要相应的技术产品支持。

在数据安全治理上，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度融合。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；在数据安全防护上，将数据细分为对结构化、非结构化和半结构化，基于云、网、端三类场景对电子文档、数据库进行全方位多维度管理。

面对网安行业内卷严重的现状，崔培升说到，一定要减少恶性竞争。安全行业是一个持续增长的行业，像跑步一样需要耐力，需要踏踏实实。

用心做好安全产品，真正了解用户的需求，除了必须具备解决客户现有问题的能力之外，还要拥有预判力，有梯度地进行规划建设。采用“分放管服”四步双闭环建设数据安全，从而系统性地解决问题，实现产业共赢。

人物简介

崔培升，毕业于清华大学，获得工程管理硕士 MEM；清华大学 - 北卡罗莱纳大学 EMBA，获得北卡罗来纳大学凯南商学院工商管理硕士学位。从事网络安全和数据安全行业近二十年，深入洞察产业趋势，现任中国开发区协会商业秘密保护专业委员会主任、海淀中小企业协会副会长、中关村海新联新兴产业促进会副会长、中国信息通信研究院数据安全共同体计划专家、北京亿赛通科技发展有限公司总经理，全面负责公司经营及管理工作，带领公司取得工信部“专精特新”小巨人、双高新技术企业等多项国家级资质认证。在业内率先提出“分·放·管·服”数据安全建设理念，不断延伸技术优势，从单一的文档加密厂商扩展到综合数据安全厂商，保持公司业绩长期稳定增长。

亿赛通助力“百城千园行”活动，独家分享工业互联网安全建设经验



近日，2023年成渝工业互联网一体化进园区“百城千园行”重庆活动在西彭工业园区顺利召开。工业互联网领域权威专家、知名学者和数据安全行业翘楚相聚齐聚重庆，深入贯彻党的二十大精神和习近平总书记重要讲话精神，聚焦“工业互联网+数智园区”路径，加快提升工业园区信息化赋能水平，促进企业数字化、网络化、智能化转型。

本次活动是由重庆市经济和信息化委员会、重庆市通信管理局、重庆市九龙坡区人民政府、中国信息通信研究院（以下简称“中国信通院”）共同主办，活动发挥桥梁纽带和引领作用，为政府、园区、企业搭建供需对接、产业协作、资源共享、合作共进的平台，加快推动工业互联网与经济社会各领域深度融合。亿赛通作为国内数据安全领域的龙头企业，也是首批百城千园行合作伙伴，聚力汇智协同推进工业互联网信息化赋能，本次受邀出席并分享了《构建工业互联网安全防护体系》心得。

亿赛通提到根据 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%。而国内为落实各项关于网络、数据安全管理的规定，近些年大力推进各项政策法规的实施，国内网络、数据安全领域步入新纪元。并且，根据部分已实施的法规来看，建立健全的数据安全治理体系、加强数字基础设施建设是发展“数字强国”战略的必要进程。



随着 IT 环境越来越复杂，企业原有的业务架构和网络边界被打破。数据之间的交互越来越多、敏感数据分散化、数据窃取手段层出不穷，同时数据安全合规监管越来越严格，亟需体系化的数据安全技术框架来应对新兴场景的数据安全挑战。



亿赛通在 2023 年初发布“分放管服”数据安全建设理念 V2.0 版，分别从制度层和技术层面结合做到人与数据的最优管理；人与标准的最佳实践；使数据安全建设在合规的基础上产生最大的价值，真正实现安全与效率的最大化平衡。



在“分放管服”数据安全建设理念的基础上，数据安全运营管理平台应运而生。平台能力主要体现在综合数据、运营管理两方面，目前数据安全产品能力整体来说可以分为结构化、非结构化和半结构化三类，那么综合数据安全管理平台所管理的数据应当要包含这三类数据。其次是运营管理能力，安全管理平台一定要结合数据安全治理框架模型，从数据的产生到数据的销毁全生命周期都能够进行全流程管控运营。

具体从应用目标上，平台以数据安全为核心的保护方案，涵盖了各行业各领域多数场景下的数据安全保护需求，以数据发现和数据分类分级为基础，使用了数据扫描、文件加密、数据访问控制、数据水印、数据脱敏等技术来实现数据安全防护，同时也包含了数据活动监控和数据风险评估等功能。网络安全态势感知平台更多关注的是网络行为，综合分析网络安全要素，评估网络安全状况，预测其发展趋势，并以可视化的方式展现给用户。

从技术实现上看，平台不仅采集流量，而且要进行协议内容还原，更多关注数据内容，从而判断是否存在数据安全风险。在一些分析类技术的使用上，例如 UEBA、规则匹配、勒索防护等，平台也会用到。

亿赛通工业互联网领域解决方案及相关产品紧跟政策法规的指导思想，明确发展目标和实施路径，部署战略规划和展路线，指导推进我国工业互联网数据安全发展。通过建设工业互联网数据安全运营、治理等技术的实践，形成核心技术创新发展优势，以数据安全奠定基石，释放数据价值，构建协调发展的工业互联网数据安全产业生态。

亿赛通全力支撑首届数据安全大赛，祝贺大赛圆满结束



2月21日，在工业和信息化部网络安全管理局的指导下，中国电子信息产业发展研究院、中国信息通信研究院、国家工业信息安全发展研究中心、中国软件评测中心（工业和信息化部软件与集成电路促进中心）联合主办、北京亿赛通科技发展有限公司协办的“2022年首届数据安全大赛”赛程已圆满结束。

大赛为深入贯彻落实《数据安全法》，加速我国数据安全人才培养，推广数据安全优秀产品和解决方案，推动解决各行业领域数据安全实际需求，提升全社会数据安全保障能力，促进数据安全产业高质量发展，为建设网络强国和数字中国，保障数字经济健康发展提供有力支撑。

本次大赛中，运营商、金融、公安、海事等政府部门以及全国多家高校受邀参赛。上千支队伍经过预赛的激烈角逐，最终有100支参赛队伍300余名专业选手进入决赛。大赛在中国电子信息产业发展研究院的指挥下，顺利圆满落幕，所有选手均展现了专业水准，赛出风格。大赛颁奖典礼于2月23日在中国网络和数据安全产业高峰论坛数据安全产业生态建设主题论坛举行。届时可通过线上线下等多渠道参加，共襄盛举。数据安全产业论坛举办时间、地点、报名方式详见如下链接：

惊喜面对面！来2023年中国网络和数据安全产业高峰论坛·数据安全产业论坛



作为赛事协办方，亿赛通共参与了赛道二及赛道三双赛道竞选，经过激烈角逐，我司战队各技术骨干分工明确，团队依靠多年对敏感信息识别、泄露数据溯源、数据文件保护的经验和优势。在整个比赛环节中表现出了亿赛通专业的、过硬的技术实力。最终凭借专业的产品和丰富的数据实施服务经验，成功夺得赛道二数据安全识别方向的铜牌。

随着数字经济的高速发展，数据安全事件爆发频率与规模越来越大，对国家和社会的影响也将愈发明显，数据安全事件的预警、应急处置就愈发重要。

亿赛通作为国家级“专精特新”小巨人单位，承担了多项重点项目、基金和课题的开发和实施，整合公司的技术、产品、服务等能力，针对用户需求快速梳理、研究、分析用户细节，根据用户特性，形成防护能力，提供可落地的安全防护方案，依托覆盖全国的安全服务团队，帮助企业尽快对信息系统作出合规性分析。在数据的全生命周期中，通过有效的制度流程、组织管理及技术手段，为企业提供多阶段、多层次、多形式服务，有效降低安全事件造成的影响和损失，提升企业应对威胁的能力。



亿赛通深耕数据安全事业二十载，在安全技术研究和活动支持上有着丰富的积淀。除了提供赛事支撑外，还从技术保障、赛事题库、人才培养等多方面进行全方位的支撑。未来，亿赛通将再接再厉，持续创新，不断积累，为企业信息化建设贡献力量！

亿赛通受邀出席重庆市数据管理能力成熟度评估模型（DCMM）宣贯会



当前，数据已经成为数字经济时代的基础性资源、重要生产力和关键生产要素。习近平总书记强调，数据基础制度建设事关国家发展和安全大局，要统筹推进数据产权、流通交易、收益分配、安全治理，加快构建数据基础制度体系。近日，中共中央、国务院印发《关于构建数据基础制度更好发挥数据要素作用的意见》（以下简称“数据二十条”），系统性布局了数据基础制度体系的“四梁八柱”，历史性绘制了数据要素发展的长远蓝图，具有里程碑式的重要意义。此外根据国务院印发的《关于加快推进国有企业数字化转型工作的通知》要求，明确指出了数据治理是企业数字化转型的必经之路，企业数字化转型方兴未艾，数据治理被推向了“风口浪尖”。

重庆市在 2021 年出台《重庆市数据治理“十四五”规划（2021—2025 年）》指出数据是数字经济发展的关键要素，加快推进数据治理工作是保障数字经济高质量发展的重要前提。近日北京亿赛通科技发展有限公司受邀参加了重庆市数据管理能力成熟度评估模型（DCMM）宣贯会，会上重庆办负责人做了“构建数据安全能力体系”的主题演讲。

DCMM 宣贯会由重庆两江新区管理委员会产业促进局和重庆市工业信息安全发展研究中心共同主办，旨在通过数据管理能力诊断评估推动重庆市企业数据管理能力提升，加快推动数据基础平台建设、强化数据目录管理、打造数据治理能力中台、持续提升数据质量、强化数据安全治理，支撑重庆市“智造重镇”“智慧名城”的建设。



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，亿赛通对此已深耕二十年。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，我司为客户提供数据安全防护、数据库审计、网络数据泄露防护、数据安全综合治理等全生命周期的数据安全解决方案和全方位服务，建立起数据安全运营管理平台。

亿赛通提出了“分·放·管·服”全新数据安全建设理念及全系列产品，数据安全的首要基础工作是数据的分类分级。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。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。



二十大提出建设网络强国、数字强国，认真学习贯彻习近平总书记重要讲话精神，加强数据安全是行业大势，更是国之大势，势不可挡。面对不断变化的安全挑战，亿赛通希望联合企事业单位充分激活数据要素潜能，高质量发展数字经济，增强经济发展新动能，助推数字经济安全腾飞，构筑国家竞争新优势。

推动数据安全高质量发展，亿赛通出席2023年中国网络和数据安全产业高峰论坛



为深入贯彻习近平总书记关于网络安全的重要指示精神，落实党的二十大报告关于强化网络和数据安全保障体系建设的要 求，按照党中央、国务院决策部署，工业和信息化部系统推进网络和数据安全保障体系和能力建设，大力促进网络和数据安全产业创新发展。2月23日至24日，中国网络和数据安全产业高峰论坛暨数据安全产业生态建设主题论坛在四川省成都市成功举办。

本次论坛由工业和信息化部、四川省人民政府主办，中国电子信息产业发展研究院、中国软件评测中心（工业和信息化部软件与集成电路促进中心）、中国计算机行业协会数据安全专业委员会联合承办，工业和信息化部网络安全管理局副局长杜广达、中国电子信息产业发展研究院党委书记兼副院长刘文强、四川省经济和信息化厅副厅长郎利影、四川省通信管理局副局长刘小文、工业和信息化部网络安全管理

局数据安全处处长雷楠、中国电子信息产业发展研究院副总工程师安晖出席论坛并进行致辞。论坛汇聚全国网络和数据行业龙头企业及专家，围绕国家政策解读、前沿技术和行业安全实践，深入交流构建行业高质量发展的产业生态。

亿赛通凭借在行业内深扎多年的数据安全深厚的技术沉淀，参与并支持本次数据安全产业生态建设论坛，成为数据安全产业生态战略合作伙伴，并在中国网络和数据安全产业高峰论坛·数据安全产业生态建设论坛发表主题演讲。

论坛上，公司总经理崔培升作了“‘测研用’联动，助推数据安全产业高质量发展”的主题演讲，为参会人员深入剖析数据安全产业生态建设双闭环管理体系，揭秘亿赛通数据安全治理的破局之法。



总经理崔培升主题演讲

数据安全产业生态建设主题论坛同时举行了数据安全产业生态战略合作签约仪式，作为数据安全领域的优秀解决方案提供商，亿赛通参与签约成为数据安全产业生态战略合作伙伴，并将在未来积极发挥自身在数据安全领域的优势及业务发展积累，赋能数据安全产业高质量发展。



生态合作的签约仪式



生态合作的签约仪式 - 签约单位代表合影

随着2022年首届数据安全大赛决赛圆满落幕，作为论坛的压轴环节，为所有获奖单位和个人举行了盛大的颁奖仪式。亿赛通在赛道二经过激烈角逐，依靠多年对敏感信息识别、泄露数据溯源、数据文件保护的经验和优势，成功夺得数据安全识别方向的铜奖。在整个比赛环节中表现出了亿赛通专业的、过硬的技术实力！



数据安全大赛颁奖现场

此外，亿赛通在数据安全产业生态建设主题论坛设立展台，展示了亿赛通在数据安全领域取得的先进研发成果和成功应用案例，产品备受瞩目，吸引与会人士驻足交流，现场咨询者络绎不绝。



展台现场交流

二十年的实践总结与提炼，亿赛通为客户数据安全治理提供技术支点及完善的产品解决方案，并不断推出全新理念、前沿技术与创新型产品，为产业提供新的视角，以前瞻性的研发创新伴随整个数据安全产业的发展。未来，亿赛通将继续拓宽生态体系建设，加强技术攻坚，为推动数据安全产业的高质量发展作出贡献，促进数字经济时代的安全共赢。

同心同行 一起向未来，亿赛通 20 周年庆典圆满落幕



绿盟科技集团党委书记、总裁胡忠华出席庆典，代表集团对亿赛通 20 周年表示祝贺。他在讲话中指出，政策法规、安全事件、技术创新、市场竞争等关键性因素正推动产业健康稳步发展。目前，安全产业正处在一个关键的时间节点，安全产业能够发挥的力量与作用越来越大，对厂商来说风险与机遇并存。集团希望亿赛通能持续贯彻落实持续创新战略，力求完善技术、产品及服务，继续丰富产品线和安全体系，为客户提供优质服务。



随后，亿赛通总经理崔培升回顾了亿赛通的发展之路。崔总表示，公司是在一次次的考验中不断总结经验教训成长起来的。在公司的发展历程中，也经历了非常多的困难和坎坷，环境不断变化，愈来愈多的不确定性带来更新的挑战。未来，亿赛通会继续推陈出新，无论是产品技术，还是市场布局，我们会持续发力，产学研、项目支撑、人才培养、生态合作多方发力，全面开花，为亿赛通人开启更美好的起点。



产品是公司发展的根基和命脉，创新是公司发展的动力，创新研发承载着公司的腾飞和梦想！亿赛通成立以来，在产品研究的道路上一步一个脚印，踏实前行，建立起完善产品体系。亿赛通 CTO 朱贺军在庆典做出承诺，未来会继续深挖数据安全领域的前沿技术，打造以顶层设计为主体、数据安全治理框架为导向、核心工具深度融合的技术创新体系，为亿赛通的核心竞争力和持续创新能力提供有力保障。



回望过去，从成立之初的几十人初创团队到如今的规模，公司资产、业绩也实现了倍数增长。20 年间，有付出也有回报，辛苦与快乐并存，未来的路仍然艰辛。小亿小赛们在此宣誓，正式开启新的征程，践行责任，聆听宣言，领会榜样的精神与力量，再创佳绩！

从 2003-2023，是一个又一个小亿小赛们，共同缔造了今天的亿赛通！在他们之中，有人亲身经历并见证了这家公司的发展历程，也有人在亿赛通度过了至今全部的职业生涯，还有人在工作期间完成了从子女到父母的人生蜕变…二十年

2003 年，中国互联网迎来高速发展期，当年 1 月 21 日，亿赛通在北京成立。

2023 年，见证中国数据安全行业发展的亿赛通迎来了 20 周岁生日，以成年人的姿态奋进在下一个 20 年的新征程上。

2 月 25 日，同心同行 一起向未来，亿赛通 20 周年庆典在北京精彩上演。活动总结了公司 20 年可歌可泣的发展历程和取得的宝贵成绩，对公司未来发展进行了展望。亿赛通各区域五百余名员工齐聚北京，共同见证属于小亿 20 周年的华彩！



春夏秋冬，我们一次次通过了数据安全行业的大浪淘沙，从无到有、逐渐壮大，最终留下的、最为宝贵的，是“亿赛通人”这个名字。庆典中，公司对在不平凡的两年间，各自岗位上取得优异成果的个人及做出突出贡献的团队，分别进行了嘉奖与表彰！

伴随优秀新人、优秀员工、服务之星、研发之星、工程之星、管理之星、销售 TOP、优秀团队、杰出团队、重大项目奖、重大签约项目奖、重大标杆案例奖、新产品突破奖、五年感谢奖、十年感谢奖等一系列奖项花落，亿赛通完成了对 2022 年的总结，正式开启了 2023 年的全新征程！



华灯初上，光影激荡，舞台之中，谁与争锋。庆典最后，各位才艺、颜值均在线的小亿小赛们十八般武艺样样显神通。有活力四射的舞蹈，婉转动听的歌声，悠扬飘荡的朗诵……精彩纷呈的节目，承接了现场一轮又一轮的尖叫！



二十岁，是人生中最好的年华，风华正茂、朝气蓬勃、青春洋溢，也是一家公司经历岁月沉淀后，厚积薄发的黄金时代。走过的路程可以计数，发挥的价值却难以衡量，20 岁的亿赛通，已成为备受客户信赖、有责任感的中国数据安全专家，正在以更加成熟的姿态迎接机遇和挑战，创造更多奇迹。

展望未来，正值蓬勃之期的亿赛通，将依托 20 年坚实基础，在大家的鼎力支持下，继续保持高质量、可持续发展，用青春与汗水浇筑出绚烂辉煌的小亿梦。下一个二十年，亿赛通初心依旧，热情不减，将继续为数据安全的健康发展贡献力量，以竞无止境之心，昂首赢战未来！

科创中心“核”动力 | 亿赛通：中国数据安全领域“守卫者”



数据作为一种新型生产要素，正深刻影响着国家经济发展。有了法律依据后，数据安全保障能力是国家竞争力的直接体现。近年来，数据安全不仅是国家安全的重要方面，也是促进数字经济健康发展提升国家治理能力的重要议题。

北京亿赛通科技发展有限公司（以下简称：亿赛通）以专业的产品和服务为客户筑牢数据安全底座，位于海淀区的北京亿赛通科技发展有限公司成立于 2003 年，作为绿盟科技全资子公司，是一家拥有完全自主知识产权的安全服务商。



亿赛通从发布国内第一套文档加密系统后，便开始在数据安全领域开疆拓土，不断扩充产品线，陆续在全国各地成立办事处及服务网点，已发展成为集数据安全、网络安全和安全服务于一体的综合安全服务商。



近两年，亿赛通又结合人工智能、大数据、区块链、5G 等新兴技术，在新产品研发上进行深度融合，智能化、专业化、标准化，是未来亿赛通发展的重要目标。

做数据安全守护者 用产品诉建设理念

亿赛通提出“分放管服”数据安全建设理念，以“数据和人”为对象构建的数据治理、防护、流转、运营的双闭环体系，帮助企业形成扎实可靠的综合数据安全能力，为企业数据资产从产生价值到保值、增值的建立重要保障。



全线产品覆盖云、网、端三大类应用场景，60 款+精细化产品模块，支持结构化、非结构化和半结构化数据安全治理，打造集数据安全合规、数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务为一体的数据安全领域综合解决方案。



精准把握需求 解决企业痛点

企业在传统数据安全建设中，多以单点安全解决方案为主，无法将大量数据信息关联起来，造成数据安全监测技术和体系化运营规划困难，成为数据防护中的普遍痛点。



亿赛通全新推出综合数据安全运营管理平台

企业里的重要数据资产可以通过大平台进行可视化治理、这个平台上的功能模块可以自己组合有联动效果，进而全方位的可以对敏感数据进行流动监测、提前预知泄露风险、迅速锁定泄漏源头。



新一代数据泄露防护系统 DLP

新一代电子文档安全管理系统 CDG

数据安全运营管理平台 DSOP

数据库安全五件套

数据跨境安全检查工具

.....

亿赛通打造的一系列明星产品在国产化适配上先后与华为、飞腾、统信软件、麒麟软件、中科曙光、达梦、中国电子、海光、人大金仓等多家国产厂商完成产品兼容认证。

推进传统产业转型升级 助力企业数字化转型之路



亿赛通凭借 20 年数据安全建设方法论，始终坚持以数据安全流转为中心，形成一体化智能安全管理体系，打造数据安全领域真正意义上的综合解决方案。



记者了解到，亿赛通签约用户已过万家，800 余万终端用户，覆盖金融、能源电力、设计制造、新能源、芯片半导体、医疗教育、研发通讯、运营商、互联网等十大行业客户。



截至目前，亿赛通拥有 100 余项发明专利、商标注册权及企业资质证书，300 余项软件著作权及产品资质证书。同时在信创发展道路上与麒麟、飞腾、中科曙光、通信软件、达梦、长城科技等多家完成国产化兼容认证，并成为光合组织成员单位。

拓宽生态体系建设 加强核心技术攻坚

亿赛通仍将紧跟时代步伐，以民族责任感不断激励自主创新，为客户创造真正所需价值服务，为我国信息安全产业贡献更大力量，致力于成为最受信赖的中国数据安全专家。

海淀企业加油!

《科创中心“核”动力》挺你!

《科创中心“核”动力》

指导单位：北京市海淀区人民政府

出品单位：北京市海淀区融媒体中心

本期视频《亿赛通：中国数据安全专家》

出品人：佟志伟

总策划：张庆洁

总编导：卫东

总监制：张东旭

统筹：韩娟娟

监制：郝冰

编导：金山

记者：杨钰倩

摄像：佟金库、杨靖

后期：贾荣暖

本期推文

记者：杨钰倩 编辑：罗雨涵 实习编辑：张靖雨

疑似大量个人信息泄露，快递行业风波再起

近些年来，发展数字经济已经成为世界主要大国和地区提升经济竞争力的共同选择。中国数字经济正在蓬勃发展，并推动互联网、大数据、人工智能和实体经济深度融合，中国将全面步入数字经济时代。

然而，在数字经济快速发展的同时，个人信息保护问题受到了日益广泛的关注。数据是数字经济的生产资料，数字经济的发展离不开数据。因而对于企业来说，数据即财富，谁拥有了数据就相当于拥有了生产资料，数据可以直接转化为利润。由此，不法分子将视线盯上了含有庞大数据量的快递行业。

日前，有消息称，疑似约45亿条国内个人信息在“暗网”被泄露，包括真实姓名、电话与住址等，引发各界关注。



2月12日晚，Telegram 各大频道突然大面积转发某隐私查询机器人链接。网传消息称该机器人泄露了国内45亿条个人信息，数据包大小达435GB，疑似电商



或快递物流行业数据。用户仅需输入手机号，即可通过该机器人查询到姓名、手机号和详细的收货地址等隐私信息。

某专家经过验证确认数据泄露的时间不早于2021年11月份，最晚不晚于2022年12月份。不法分子将泄露的用户数据整合分析、集中归档到“社工库”，通过社工库便可以获得相关信息。此次的数据泄露较为广泛，类型较多，涉及多家平台的相关快递信息。由于信息泄露规模庞大，暂时无法判断其泄露具体原因。

在亿赛通看来，快递行业掌握着大量消费者数据，是个人信息最密集的地方之一。并且，快递行业数据泄漏事件屡屡发生。一方面，快递行业相对滞后的信息安全建设，频繁遭受外部攻击，而另一方面企业内部人员职责、操作流程不明确，第三方维护人员的操作监控失效，非法盗用转卖客户信息等问题，让数据安全隐忧倍增。快递行业的数据安全治理建设既要满足行业相关政策法规的要求，又能满足产品高效可用。

而亿赛通数据安全运营管理平台恰好满足快递行业的相关需求。平台将亿赛通自主研发的数据库审计、DLP、文件加密、数据脱敏等各类产品能力集中化管理，策略统一布控，既可以减轻运营人员的工作负担，同时又能够对各类安全产品进行统一策略的管理与优化，减少无效策略形成的误报，满足行业合规需求。



同时，通过统一的数据安全运营管理平台，还可以对各类安全产品上报的日志数据进行关联分析，解决以往审计日志分析及溯源的局限性，可将一个事件在云、网、端的所有操作进行完整还原，帮助用户准确定位风险源头。

此外，数据安全运营管理平台将视线主要关注到“运营”二字，成立了数据安全服务部门，根据用户的经营策略、治理要求、合规要求等，提供顶层设计、IT安全策略、数据梳理等各种服务，兼顾安全与效率。

本月，国家邮政局明确强调邮政快递领域用户个人信息保护事关国家安全、公共安全和人民群众生命财产安全。后续将依法严厉打击泄露、买卖寄递服务用户个人信息等行为，督促寄递企业加强网络安全数据安全和个人信息保护工作。未来，快递行业信息安全定会得到安全防护。亿赛通数据安全治理解决方案可以有效帮助企业进行数据资产管理业务，提升安全工作的发现、管控能力与处理效率。

欲详细了解解决方案内容，保障企业数据安全，可咨询服务热线：400-898-1617。

政策解读 | 亿赛通专业解读《关于促进数据安全产业发展的指导意见》

此前，工信部等 16 个部门发布《关于促进数据安全产业发展的指导意见》（以下简称《意见》），提出了数据安全产业的概念，确立了推动数据安全产业高质量发展的指导思想、基本原则和发展目标，并从提升产业创新能力、壮大数据安全服务、推进标准体系建设、推广技术产品应用、构建繁荣产业生态、强化人才供给保障、深化国际交流合作和加强保障措施等方面明确了数据安全产业的发展任务。内容要点如下：

要点一：明确数据安全产业的独立地位

《意见》提出，“数据安全产业是为保障数据持续处于有效保护、合法利用、有序流动状态提供技术、产品和服务的新兴业态。”数据安全产业既要满足数据处理者履行数据安全保护责任义务的需要，也要满足促进数据资源开发利用、激活数据要素价值的需要。

要点二：提出四个“坚持”的发展原则

《意见》提出，坚持创新驱动、坚持以人为本、坚持需求牵引、坚持开放协同。以创新为动力，以需求为导向，以人才为根本，加强核心技术攻关，加快补齐短板，促进各领域深度应用，发展数据安全服务，构建繁荣产业生态。

要点三：确立两个阶段的发展目标

2025 年，数据安全产业规模超过 1500 亿元，年复合增长率超 30%，并在核心技术、应用推广、产业生态、人才培养等方面实力明显增强。

2035 年，数据安全产业进入繁荣成熟期，政策体系、

核心技术、重点产品、服务能力跻身世界先进行列。

要点四：推动数据安全创新

技术创新：支持科研机构、高等院校、企业等主体共建高水平的重点实验室、研发机构、协同创新中心等，围绕新计算模式、新网络架构和新应用场景，加强数据安全基础理论研究，攻关突破数据安全基础共性技术、核心关键技术、前沿革新技术。

产品创新：鼓励数据安全企业紧密围绕产业数字化和数字产业化过程的数据安全保护需求，优化升级传统数据安全产品，创新研发新兴融合领域专用数据安全产品；面向重点行业领域特色需求、中小企业个性化需求，以及数据开放共享、数据交易等开发利用场景，加快适用产品研发；加强数据安全产品与基础软硬件的适配发展，增强数据安全内生能力。

服务创新：鼓励数据安全企业、第三方服务机构由提供技术产品向提供服务和解决方案转变，发展壮大数据安全规划咨询、建设运维、检测评估与认证、权益保护、违约鉴定等服务，推进数据安全服务云化、一体化、定制化等服务模式创新。

要点五：推动数据安全产业满足数据安全保护需求

打造“产学研用”合作生态：积极拓展产业合作渠道，建设数据安全产业公共服务平台，组织数据安全产业会议、展览、赛事、学术研讨、产业沙龙等活动，促进数据安全企业与数据处理者强化交流合作，推动供需精准对接和产业信息共享。

开发基于场景的适用性产品方案：支持数据安全企业深度分析工业、电信、交通、金融、卫生健康、知识产权等领域数据处理者的合规需求和保护需求，梳理典型应用场景，发展、提升相关产品和服务的功能性能，特别是面向重点行业领域、新型应用场景及中小企业特色需求，开发适用性产品或解决方案。

坚持合规、需求双驱动：引导数据处理者围绕落实《数据安全法》和行业数据安全要求，梳理自身数据安全保护需求，科学合理制定数据安全保护规划，持续强化数据安全保护能力；同时，与数据安全企业加强互动反馈，以数据安全最新需求牵引技术产品和服务的迭代升级。

打造示范引领效应：鼓励各地区规划建设数据安全创新应用先进示范区，组织本地区相关单位和企业部署应用数据安全保护产品，对特点鲜明、成效显著的产品和解决方案予以推广，形成示范效应。

要点六：持续培育和壮大数据安全专业队伍

基础教育方面，推动普通高等院校和职业院校加强数据安全相关学科专业建设，强化课程体系、师资队伍和实习实训等。

职业教育方面，制定颁布数据安全工程技术人员国家职业标准、实施数字技术工程师培育项目，并鼓励科研机构、普通高等院校、职业院校、优质企业和培训机构产教融合、协同育人。

人才选拔、培养和激励机制方面，开展职业资格评价、职业技能等级认定、专项职业能力考核等工作，推广优质数据安全培训项目，打通人才供给通道。

人才引进方面，鼓励企业择优引进海外优质人才与创新团队，扩充数据安全人才力量。

近两年，亿赛通从管理和技术双管齐下，全面贯彻“分·放·管·服”数据安全建设理念，充分利用和发挥各种

关键技术、服务，贴合用户需求，实现产品创新、服务升级、人才培养，构建全场景、全周期、可信任的数据安全纵深防御体系。



产品创新方面，亿赛通根据行业及用户需求的变更，将产品实现平台化集成，形成数据安全运营管理平台。平台是数据安全治理的中枢，向上为制度服务提供技术支撑，向下作为统一调度中心，驱动各类数据安全产品实现数据安全管控。通过将各个孤立的安全系统进行资源整合，利用人工智能算法，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。

服务升级方面，亿赛通拥有一个中心、四个领域、六个步骤，包含全工作场景、全业务流程、全生命周期的数据安全服务方案。在基于科学性、实用性、稳定性及扩展性的数据分类分级原则基础上，建立组织保障、梳理数据资源、确定分类分级策略、长期数据运营。

人才培养方面，亿赛通与中国电子信息产业发展研究院（赛迪研究院）、工业和信息化部人才交流中心等权威单位展开合作，联合推出数据安全职业能力培训体系、工信人才 & 亿赛通 - 数据安全专业人才认证两大体系共 6 门课程。2022 年为行业输出 300+ 高技术高能力专业人才。

下一步，亿赛通将在《意见》的指导下，帮助企业明确数据安全组织职责，深化产品、技术创新，加强解决方案设计，为数据安全工作落地执行提供强有力的人力资源保障。

数据库安全综合解决方案



行业需求

随着计算机和网络技术发展，信息系统的应用越来越广泛。数据库做为信息技术的核心和基础，承载着越来越多的关键业务系统，渐渐成为商业和公共安全中最具有战略性的资产，数据库的安全稳定运行也直接决定着业务系统能否正常使用。

围绕数据库的业务系统安全隐患如何得到有效解决，一直以来是 IT 治理人员和 DBA 们关注的焦点。

风险分析

- 1) 外部黑客重要数据窃取
- 2) 内部人员面临的安全隐患
- 3) 第三方维护人员的威胁
- 4) 最高权限滥用风险
- 5) 违规行为无法控制的风险

解决方案



采集及引擎组件层是数据采集以及执行数据安全指令的执行组件，包括数据库透视、数据库审计、数据库防火墙、数据库加密、数据库脱敏、数据库水印以及数据库运维等组件。

存储及计算能力层

系统的存储分为两个部分，其中 MySQL 数据库存储系统元数据、系统配置参数等信息，ES 大数据存储集群用来存储数据安全的相关审计日志记录，用于系统的离线数据分析。

功能服务组件层

功能服务组件层提供数据库安全的基本服务，包括数据梳理、数据监测、数据防护和智能分析四大模块功能集，其中：

数据梳理完成数据资产梳理、数据分级分类、数据风险评估、数据静态环境评估和数据动态流转评估以及数据血缘图谱等功能。

数据防护包括数据的细粒度访问控制、数据访问身份认证、数据加密、数据防泄漏、数据脱敏以及数据水印等功能。

数据监测包括数据审计、数据拥有者溯源、数据动态轨迹跟踪、数据风险识别、数据风险预警以及数据安全态势感知等能力。

智能分析服务包括用户行为分析（UEBA）、用户行为画像、基于机器学习的智能基线建立、风险趋势智能预测、智能辅助决策服务以及数据安全的智能联动等功能模块。

业务展现层

业务展现层是系统与用户的主要接口，集中向用户提供系统管理和业务展现的能力。在系统业务管理上，提供统一策略管理和统一流程管理，使用户能够在更高层次上实现对其数据安全的管控。

系统管理及接口

系统管理及接口是业务处理平台的管理以及对外接口部分，包括平台元数据管理、三方数据接入管理、数据共享接口、数据安全联动 API 等。

方案收益



商业秘密保护解决方案



行业需求

随着改革开放的不断深化和信息化的快速发展，企业在发展中产生了大量的数据资产。这些拥有自主产权的数据资产已成为企业竞争力的根本基础，那么如何保护企业核心数据资产安全，如何维持自己的研发创新力，已成为关乎企业生存发展的重要问题。

同时，党和政府高度重视数据应用及安全保障相关工作。《中华人民共和国国民经济和社会发展第十三个五年规划纲要》明确指出，要“加快推动数据资源共享开放和开发应用”；要“加强数据资产安全保护”，“保障安全高效可信应用”。十九届四中全会报告也指出，“健全以公平为原则的产权保护制度，建立知识产权侵权惩罚性赔偿制度，加强企业商业秘密保护”。

风险分析

- 1) 数据资产识别不充分，无法有效定位到真正的数据资产
- 2) 业务部门对数据安全感知度不高，管理方法落地难；
- 3) 一旦出现数据泄密问题后，溯源取证难。

解决方案

数据安全治理

提供一套灵活的商密项目管理、人员管理、数据管理作为支撑，帮助用户可以快速有效支撑商密数据安全治理落地。

数据安全管控

保障数据操作安全，数据使用安全，对数据内容转储行为进行安全控制。

数据安全流转

保障企业商密数据内部流转以及外发。

数据安全存储

有效保证内部数据的安全。

安全闭环管理

通过全面的行为审计、详细的商密数据统计分析，清晰的获取企业整体商密数据安全态势。逐渐安全管理体系与安全管理技术，进而实现对未发生的风险预警，感知未知风险。将数据泄露隐患从源头遏制，防范于未然。

方案收益

本方案的有效实施将帮助企业获得以下收益：

1) 商密数据业务管理

用户使用商业秘密的同时，通过对项目、用户、数据的管理，有效的减少用户因违规操作而导致的泄密风险。

2) 商密数据安全保护

通过文件加密、权限控制、安全存储等技术对商业秘密全生命周期的保护，有效减少了商业秘密泄露的风险。

3) 商密数据集中管理

协作办公云平台对商业秘密的多样化、碎片化数据进行统一有效的集中管理，同时降低用户因硬盘损坏、误删、人员离职、病毒攻击等导致的数据丢失问题，有效保护了商业秘密数据的安全性、完整性，提升用户办公效率。

4) 商密数据透明可视

统计和分析企业内部商密数据资产，实现企业内部商业秘密可视化和透明化，展示企业商密数据资产概况。为组织提供有效数据支撑。

5) 商密行为威胁检测

利用大数据分析和 UEBA 技术，通过用户操作行为日志检测企业内部风险威胁，可以轻松检测破坏数据被盗或者用户异常操作行为。