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

12 月刊

2023 年共 12 期

亿赛通企业月刊　　中国数据安全专家　　www.esafenet.com

高端访谈｜亿赛通宋春岭：数据安全治理：打好“技术 + 管理 + 监管”组合拳

百强第 34 名 | 亿赛通连续五年入选《中国网络安全企业 100 强》

亿赛通登榜 2023 高成长企业 TOP100，破旧立新助力数据安全驱动

亿赛通带你两分钟了解中国数据泄露防护产品市场

荣登安全“奥斯卡”| 亿赛通入选
ISC 2023 创新百强榜单

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

目录 CONTENTS

刊首语 PREFACE

2/3 感恩 2023，冲刺 2024，《亿赛通十二月刊》与您一起温暖跨年

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 亿赛通带你两分钟了解中国数据泄露防护产品市场

16/17 百强第 34 名 | 亿赛通连续五年入选《中国网络安全企业 100 强》

18/19 亿赛通登榜 2023 高成长企业 TOP100，破旧立新助力数据安全驱动

20-23 高端访谈｜亿赛通宋春岭：数据安全治理：打好“技术 + 管理 + 监管”组合拳

24/25 亿赛通出席天津滨海高新区《商业秘密保护主题沙龙》赋能企业数据安全合规建设

26/27 亿赛通解码企业级数据安全治理智能化体系与应用实践

28-33 2023 数据安全与商业秘密保护专业研讨会顺利召开

34/35 当数据安全遇见智能制造，亿赛通硬核产品助力制造企业安全可视化

36/37 亿赛通强势入围《2023 中国网络安全产业势能榜》，制造业成就有目共睹

38/39 荣登安全“奥斯卡”｜亿赛通入选 ISC 2023 创新百强榜单

亿赛通小贴士 ESAFENET PROMPT

40-43 政策速递 | 工信部公开对《工业和信息化领域数据安全行政处罚裁量指引（试行）》征求意见

44/45 首席数据官：驱动组织变革的领导者

46 人勤春来早 学习正当时 | 亿赛通《首席数据官》专业培训正式上线

47 亿说安全之揭秘数据安全的关键一环

48/49 市场洞察：数据泄露防护重要性凸显，市场竞争激烈

典型案例 TYPICAL CASES

50/51 亿赛通智能化数据安全治理体系赋能生物医药企业数字化安全管理

52/53 珠海丽珠试剂股份有限公司

元旦快乐

刊首语 PREFACE

感恩 2023，冲刺 2024，《亿赛通十二月刊》与您一起温暖跨年

不觉间，2023 年已经向我们挥手告别。今年，我国数据和网络安全行业经历了形势严峻的挑战，不仅要应对数量快速增长的安全风险，还要积极应对各项行业政策、标准带来的合规要求。在这样的大环境中，数据和网络安全厂商需要重新制定战术与策略。

亿赛通作为综合数据安全厂商，本年度在“分·放·管·服”数据安全建设理念的基础上，提出了数据安全治理智能化技术体系，通过智能化分类分级工具快速准确地完成组织的业务梳理和数据梳理，并形成规范化的策略库，即主体、客体及两者之间的策略，同时将上述数据根据积累的知识库智能化衔接到技术平台，实现了对组织数据的智能识别、智能防护、智能监测、智能运营，构建可视、可控、可管、可溯的覆盖数据全生命周期的综合解决方案。2024 年，亿赛通愿与全国新老客户、代理商、合作伙伴及同事们携手新一代数据安全技术，同心同行，协同发展，共同见证产业大变革，数据安全产业发展助力！

国内

1、应对大规模数据泄露！中国拟出台应急预案

堵漏　　新华社发 徐骏 作

摘要：中国有关部门 15 日发布了一个包含“四级分类”的应急预案 (征求意见稿)，以应对数据安全事件。此举凸显了中国政府对境内大规模数据泄露和黑客攻击的担忧。在该草案出台之际，中国与美国及其盟友的地缘政治紧张局势不断加剧。中国工信部公开征求对《工业和信息化领域数据安全事件应急预案 (试行)(征求意见稿)》的意见。该案根据数据安全事件对国家安全、企业网络设施和信息系统、生产运营、经济运行等造成的影响范围和危害程度，将数据安全事件分为特别重大、重大、较大和一般四个级别。

2、报告：跨国数字流通与交易中存在个人信息泄露、数字平台垄断等安全威胁

摘要：12 月 21 日，在《亚洲数字经济报告》发布会上，发布了《亚洲数字经济报告》（下称“《报告》”）。明年将重点讨论政府层面与企业层面如何推动数字经济发展，包括推动数字经济与实体经济深度融合，以及进一步推动数字经济创新。《报告》测算称，亚洲数字经济在逆势中实现平稳发展。2022 年，测算的亚洲 14 个国家数字经济规模达到 12.8 万亿美元，同比名义增长 3.5%，占 GDP 比重为 38.5%。产业数字化是亚洲数字经济发展的主引擎，占数字经济比重为 80.6%，其中，第三产业引领行业数字化融合渗透，一二三产业数字经济占行业增加值比重分别为 8.3%、23.1% 和 39.2%。

3、工信部组织开展网络安全保险服务试点工作，数据泄露、服务中断等可获赔偿

摘要：工信部今日发布关于组织开展网络安全保险服务试点工作的通知，加快推进网络安全保险新模式落地应用。通知显示，结合现阶段我国网络安全保险现有险种，本次试点险种主要包括网络安全财产类保险和网络安全责任类保险两大类。

4、300 余万条用户数据泄露，警方提醒！

摘要：前段时间，北京警方接到辖区内一互联网公司报案，称该公司的求职招聘类 App 的短信验证码接口遭受攻击达 1300 余万次。这次攻击还成功匹配注册账号 30 余万个，造成经济损失不说，还危及群众信息安全。北京警方迅速研判，确定这是一起黑客利用网站漏洞非法获取账号信息并用于违法活动的案件。

5、招聘 App 短信验证码接口遭 1300 多万次黑客攻击，致 300 万条数据泄露

摘要：12 月 10 日消息，据央视新闻官微，一求职招聘类 App 短信验证码接口遭遇了 1300 多万次的攻击，警方调查发现 2 名嫌犯利用网站漏洞制作黑客软件并实施“撞库”攻击，获取大量个人信息和公司账号数据在境外出售。

6、小米汽车信息遭泄露，涉事方致歉：开除涉事员工


关于小米汽车信息泄露事件的致歉声明

小米汽车科技有限公司（以下简称“贵司”）：

[illegible]

对汽车事业部员工做出开除处分，永不录用。

[illegible]

摘要：近日，“小米汽车信息泄露事件”引起热议。12 月 20 日，涉事方 ZAKER 和小白买车均发布致歉声明。ZAKER 称，对涉事员工做出开除处分，永不录用。小白买车称，对涉事员工做辞退处理、永不录用。

行业聚焦 INDUSTRY FOCUS

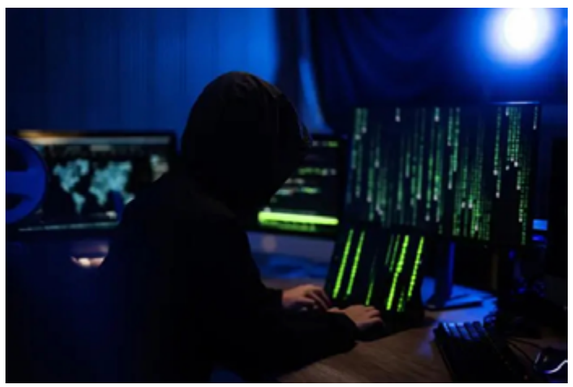
7、鞍钢集团总工程师被罚款 500,000 元，因泄露内幕信息

摘要：2023 年 12 月 25 日，中国证券监督管理委员会山西监管局发布公告，鞍钢集团总工程师林大庆因泄露内幕信息被罚款 500,000 元。公告详细了林大庆的违法事实。林大庆在 2021 年 3 月 18 日实际知悉鞍钢集团拟重组凌钢集团，可能变更凌钢股份实际控制人的内幕信息。然而，他在 2022 年 2 月底、3 月初将这一信息告知其妻子张宁，张宁并未实际参与鞍钢集团重组凌钢集团项目具体工作。

8、医疗信息被泄露，“内鬼”作恶更当严惩

摘要：著名演员周海媚因病去世后，一份疑似是她的抢救电子病历在网上流传开来，病历上显示医院为北京顺义区某医院，并记载了患者个人资料、就诊时间等信息。随后，该医院工作人员证实，网传病历是真实的。日前，北京顺义公安分局发布情况通报：经查，12 月 11 日，符某某（男，36 岁）利用其在顺义区某医院工作的便利，出于炫耀目的，将一名病患的个人病历拍照发至微信群，导致信息扩散，造成恶劣社会影响。目前，顺义公安分局已将符某某依法行政拘留。

9、“人肉开盒”兜售各类隐私，信息泄露源头调查



摘要：《人肉开盒调查：平台成员上万，约 30 种隐私信息公开叫卖》显示，“人肉开盒”参与者众多，30 余种个人隐私被公开叫卖，违法者获得个人隐私信息后，肆无忌惮恐吓、威胁甚至敲诈、勒索明星、名人，普通人也被波及。

10、岚山公安破获一起侵犯公民信息案件

摘要：近日，岚山网警办结一起侵犯公民个人信息案件。豆先生于 2021 年买了套期房，终于等到交房钥匙还没暖热，装修公司、全屋定制、品牌家具等推介电话却接连打来，有时一天多达数十个，让他不堪其扰。更为可怕的是，对方对豆先生的姓名、电话、楼盘位置、单元房号、房屋面积等情况了如指掌……深感后怕的豆先生选择报警。

国外

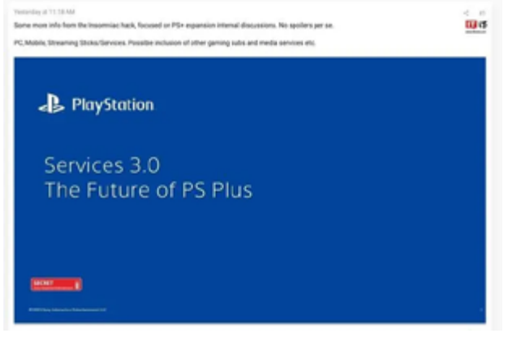
1、英国国防部因电邮泄露待撤离阿富汗人信息被罚款

摘要：当地时间 13 日，英国数据监管机构宣布，因泄露 265 名寻求撤离阿富汗的阿富汗人的个人信息，英国国防部被罚款 35 万英镑 (约 316 万元人民币)。报道称，该错误导致数百人 (包括可能有资格移居英国的阿富汗口译员) 的电子邮件地址，被公开列在邮箱的“收件人”字段中。这些邮件地址本应该被密件抄送，以保护收件人的个人信息。

2、康卡斯特称 3600 万账户数据外泄

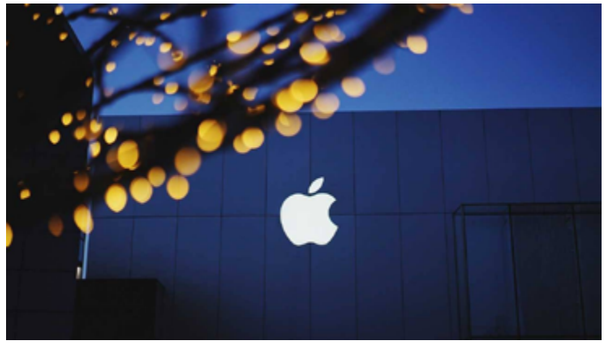
摘要：康卡斯特称，近 3600 万笔美国 Xfinity 账户数据外泄，此次泄露事件发生在 10 月 16 日至 10 月 19 日之间，原因是思杰系统公司（Citrix）生产的软件存在漏洞。

3、黑客泄露数据显示索尼有望将 PS Plus 订阅服务扩展至更多平台



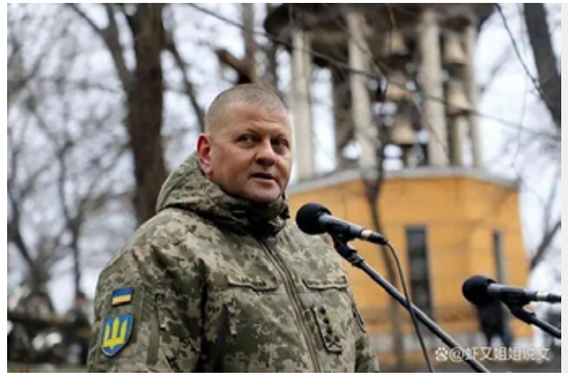
摘要：黑客团队 Rhysida 近日泄露了大量来自索尼游戏工作室“失眠组”（Insomniac Games）的内部数据，其中曝光了索尼内部一项新战略 —— 该公司计划将旗下 PS Plus 订阅服务扩展至更多平台。从黑客泄露文件中得知，索尼实行这一战略的目的是“通过多平台统一订阅方案以吸引更多潜在用户”，该公司计划将 PS Plus 订阅服务从现有的 PlayStation 主机平台扩展至 PC、手机、浏览器及智能电视平台，相关战略名为“服务 3.0（Services 3.0）”。

4、苹果安全部门：今年个人信息泄露事件创新高，黑客呈现“抱团攻击趋势”



摘要：苹果公司安全部门日前联合麻省理工学院研究人员，发布《The Continued Threat to Personal Data：Key Factors Behind the 2023 Increase》报告，就今年个人信息泄露事件进行分析，结果显示，2023 年个人信息泄露事件创下新高。苹果公司声称，今年 1 月至 9 月，美国所发生的个人信息泄露事件，已经比 2022 年全年还多出 20%；从 2013 年到 2022 年，全球信息泄露事件增长了 3 倍，而在过去两年间，有 26 亿条个人信息遭到泄露。

5、乌前高官承认：乌军总部机密信息已经泄露

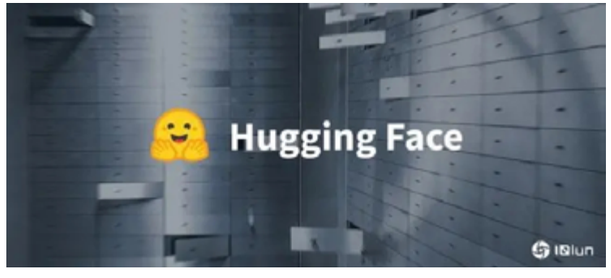


摘要：据俄罗斯 12 月 18 日报道，针对乌克兰武装部队总司令瓦列里·扎卢日内的办公室发现窃听装置一事，乌克兰国防部前副部长汉娜·马利亚尔称，这表明乌军总部机密信息已经泄露。据报道，乌克兰安全局早些时候证实，在乌武装部队总司令扎卢日内的一个可能用于办公的房间内发现了窃听器。乌安全局已根据刑法“非法获取、销售或使用特殊技术手段获取信息”的条款立案调查。

6、外媒：谷歌地图交通信息“泄露”俄军行踪

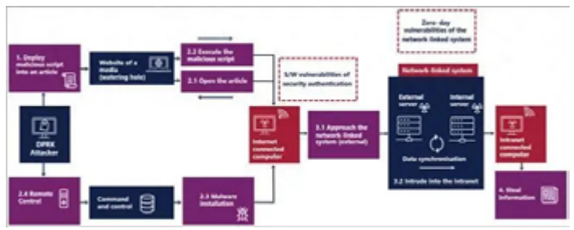
摘要：在俄罗斯总统普京正式宣布开始“特别军事行动”前的几小时，某军事专家就通过谷歌地图识别出俄罗斯出兵乌克兰的明显迹象。美国军事专家，在推特（现 X 平台）上分享了一张谷歌地图的截图，上面显示了乌克兰边境附近的交通堵塞信息，这是俄罗斯出兵的确凿证据。该专家对《法兰克福汇报》说：“它证实了我们的推测，即俄罗斯的一支部队正在这条道路上前进。”谷歌地图上一条简单的交通堵塞信息就预示着一场大规模军事袭击，这乍听起来很荒诞。但中东战争现在也证明，交战各方可以从公开的交通数据中得出军事策略推断。

7、Hugging Face API 令牌暴露，大批生成式 AI 模型岌岌可危



摘要：Lasso Security 的研究人员近日在代码存储库中发现了 1681 个暴露的 Hugging Face API 令牌，这使谷歌、Meta、微软和 VMware 等厂商面临潜在的供应链攻击。Lasso Security 在发布的声明中表示，暴露的 API 令牌使其研究人员能够访问 723 家组织的 GitHub 和 Hugging Face 代码存储库，这些代码库含有大语言模型和生成式 AI 项目方面的高价值数据。数据科学社区和开发平台 Hugging Face 表示，它拥有超过 50 万个 AI 模型和 25 万个数据集。暴露的 API 令牌使众多组织的生成式 AI 模型和数据集面临各种威胁，包括供应链攻击、训练数据中毒和模型被盗。其中 655 家组织的令牌具有写权限，这使得研究人员可以全面访问代码存储库。

8、Lazarus 黑客组织利用 MagicLine4NX 软件进行供应链攻击



摘要：国家网络安全中心（NCSC）和韩国国家情报局（NIS）就与朝鲜有关的 Lazarus 黑客组织活动发出严重警告。该组织利用目前广泛使用的 MagicLine4NX 软件中发现的零日漏洞，发动了一系列复杂的供应链攻击，影响了全球多个实体。MagicLine4NX 软件由韩国 Dream Security 公司开发，是用于安全登录和数字交易的重要联合证书程序。网络攻击者利用该软件中的一个漏洞，在未经授权的情况下访问了目标组织的内网系统，并在此过程中破坏了很多安全认证系统。 联合公告显示，网络攻击者利用软件漏洞未经授权访问了目标组织的内网。他们利用 MagicLine4NX 安全认证程序进行初始入侵，并利用网络连接系统中的零日漏洞进行横向移动，获取更多的敏感信息。

9、敌意僵尸网络发动新的零日攻击，7000 多个路由器和摄像头受到影响

摘要：网络公司 Akamai 的研究人员表示，不法分子正在大肆利用两个新的零日漏洞，将众多路由器和录像机纳入到恶意僵尸网络中，用于分布式拒绝服务（DDoS）攻击。据研究文章显示，这两个漏洞之前都不为制造商和整个安全研究界所知，当受影响的设备使用默认管理凭据时，它们允许攻击者远程执行恶意代码。身份不明的攻击者一直在利用零日漏洞攻击设备感染 Mirai。

10、医疗行业巨头 Henry Schein 公司发生数据泄露

摘要：总部位于美国的医疗保健公司 Henry Schein 本月又遭到了威胁攻击者 “BlackCat/ALPHV” 勒索软件团伙的网络攻击，该公司曾在 10 月份也遭到了同一团伙的攻击。一个多月后的 11 月 22 日，该公司宣布，由于又一次受到 BlackCat 勒索软件的攻击，其部分应用程序和电子商务平台再次瘫痪。包括电子商务平台在内的某些 Henry Schein 应用程序目前也无法使用，公司会继续使用其他的方式来接收订单，并继续向客户发货。

亿赛通带你两分钟了解中国数据泄露防护产品市场

赛迪顾问近期发布了《中国数据泄露防护产品市场研究报告（2023）》。该报告从市场现状、市场趋势与预测两大维度，深度分析了数据泄露防护市场。

亿赛通作为连续 8 年数据泄露防护市场占有率第一的行业代表性厂商，对该报告进行概括，旨在为大众评估市场趋势做出参考。

随着移动互联网、云计算、物联网和人工智能的不断发展和应用，世界经济正加速向以数字经济为重要发展方向的经济模式转变。数字经济一方面极大地促进了经济增长，逐渐成为经济增长的主要动力源泉；另一方面也提高了经济发展的质量，成为促进实体经济转型升级，推动供给侧结构性改革的重要支撑。数据作为生产要素也开始与收益分配，数据以资产形式进入数字经济价值体系，数据价值的重要性愈发显现。此外，数字化转型推动设备间的网络硬件屏障逐渐消失，数据跨界流转的速度越来越快，数据总量正以指数级速度增长，海量数据在采集、存储、传输、共享、交换及销毁的全生命周期都面临着前所未有的数据安全挑战。

据赛迪顾问调研得出，目前国内数据泄露防护市场现状如下：

2022 年，新冠肺炎疫情仍多点散发，对经济行情持续影响较大，数据泄露防护市场增速依然较缓。2022 年，中国数据泄露防护市场规模为 13.0 亿元，增长率为 16.1%。

从区域结构来看，华北、华东、中南地区在整体网络安全防护意识方面都走在前列，企业对数据泄露防护产品的需求较大，保持着较高的市场规模。从行业结构来看，电信、金融、政府等关键信息基础设施行业持续加大对于数据安全系列产品的投入。

01 赛迪顾问对数据泄露防护市场发展趋势分析如下：数据泄露事件频发，数据安全市场备受关注

2022 年，数据泄露事件依然在全球频发，数据泄露事件超过 2 万多件，与 2021 年相比，2022 年的数据泄露事件增长了 14%。数据泄露渠道主要包括网站、电商消费平台、社交平台、交通出行购票平台等，涉及国防、科研、政府机构、跨国集团、金融业、教育机构，医疗等各行各业行业。数据泄露事件的频率、规模和成本都在快速增长。从 Ponemon 发布的《2022 年数据泄露成本报告》来看，2022 年，企业遭受数据泄露事件的平均成本高达 435 万美元，创下历史新高。因此，随着企业组织对数据安全威胁认知度的不断提升，持续加大数据安全投入，加强数据保护，数据安全市场迎来快速发展。

02 数字经济与数据安全相关政策推动数据安全产业快速发展

2023 年，中共中央、国务院发布《关于构建数据基础制度更好发挥数据要素作用的意见》，初步构建了数据基础制度体系的“四梁八柱”。中共中央、国务院发布的《数字中国建设整体布局规划》中明确，数字中国建设要夯实数字基础设施和数据资源体系“两大基础”。数据安全是数据要素市场发展的重要保障，是合法、合规、有序地推动数据使用和价值变现的基础。基于此，近几年我国加快出台数据安全方面的立法进程，加强防范数据安全风险，为数据安全行业的规范化发展、数据安全领域的技术发展和应用深化提供了指导和参考，为数据安全产业的发展提供了良好的政策保障。

03 云上数据防护推动云原生架构的数据泄露防护体系建立

随着企业上云进程的加快，数据安全防护与管理也需要充分考虑云原生、公有云、混合云等场景，在多云的场景下部署数据泄露防护产品，对上云的数据进行分类分级，识别出高风险数据，并制定有针对性的防护策略。因此，要在云原生的架构下解决数据采集、传输、处理、存储全生命周期的安全问题，建立用户和数据的全生命周期管控体系。通过云原生的架构，进行安全融合，解决传统单点数据防泄漏产品中遇到的难运维、高误报、高漏报、无上下文和终端用户体验差的难题是数据泄露防护产品的重要挑战。此外，云原生数据泄露防护需要能够适应多云环境，考虑到不同云服务提供商的数据安全特性和服务，实现跨云的数据安全和保护。

04 从数据流转角度构建数据全生命周期数据安全防护

数据泄露防护应当通过数据治理、安全机制、风险识别和审计溯源等手段识别和控制数据在访问、应用和流转动态过程中面临的安全风险，挖掘数据泄露行为，由被动安全防护转向主动风险控制，高效识别数据泄露风险。从数据流转的角度来监测数据的访问、使用、共享等行为，通过分析操作行为的时间、动作、IP、应用、内容、频率等信息，识别出高风险点。从用户的角度，将数据的生命周期内不同环节所涉及的信息系统、运行环境、业务场景和操作人员等作为围绕数据安全保护的支撑，明确数据防泄露的策略、技术和方法，对数据全生命周期进行数据保护。

05、人工智能技术的运用提升数据泄露防护产品自动化能力

随着数据变得更庞大、多样化和广泛分布，数据安全保护工作会愈加困难。传统的数据泄露防护产品依赖需要以数据分级分类作为应用前提，要基于提前配置的规则过滤来保护数据的流动，手动或半自动化分类数据使得用户很难准确地对全部数据进行识别发现，对用户而言有较高的规则、策略设置要求。现代化的防护手段能够将基于身份的生命周期自动化管理应用于数据安全，利用人工智能和自然语言处理等先进技术提供内容动态洞察，将行为分析技术与数据保护体系相结合的主动、持续、自适应的防御体系，在实现数据安全保护功能的基础上，根据员工的角色变化、所处网络环境的变化自动化调整数据访问权限策略，实现用户行为的可视化监测，判断每个用户的风险等级并快速定位风险用户和高危威胁事件，预测可能会发生的威胁风险事件，从而实现智能化、自动化、高效率的主动防御。

亿赛通作为国内数据泄露防护技术的引领者，无论是市场份额，还是技术创新，都名列前茅。数据泄露防护是亿赛通的主营产品，在数据安全领域全行业积累了大量的用户。接下来，我们会继续打造符合中国国情的本土数据泄露防护产品，持续分享最新的技术发展趋势、成熟的产品和解决方案，与各大行业用户、厂商共同推动中国数据安全产业的发展。

百强第 34 名 | 亿赛通连续五年入选《中国网络安全企业 100 强》

近日，国内第三方专业调研与咨询机构安全牛联合中国计算机学会抗恶劣环境计算机专业委员会、信息产业信息安全测评中心联合发布《中国网络安全企业 100 强（第十一版）》(以下简称百强榜)。亿赛通作为数据安全领域产品方案提供商，凭借创新的产品方案、优异的市场表现和过硬的客户口碑，成功入选综合实力百强榜，位列第 34 名，排名逐年上升，成为数据安全领域的中坚力量。在历年发布的百强名单中，亿赛通至今已经连续 5 年入选！

本年度百强榜调研了国内 300 余家经营网络安全业务的企业，结合企业经营、技术创新、行业应用、信创能力四大维度的企业 2022 年数据进行梳理和评价。据安全牛调研统计，2022 年，我国网络安全企业的整体收入规模约为 927 亿元，相比 2021 年增长约 82 亿元，产业平均增长率约为 9.7%。其中，网络安全产品和解决方案类收入仍是我国网络安全企业的主要营收来源，占比为 59.7%，而服务和运营类收入占比为 24.1%，未来三年或有较大提升增长空间。

作为数据安全领域的中坚厂商，亿赛通始终在产品创新上发力，提出了数据安全治理智能化技术体系，通过智能化分类分级工具快速准确地完成组织的业务梳理和数据梳理，并形成规范化的策略库，即主体、客体及两者之间的策略，同时将上述数据根据积累的知识库智能化衔接到技术平台，实现了对组织数据的智能识别、智能防护、智能监测、智能运营，构建可视、可控、可管、可溯的覆盖数据全生命周期的综合解决方案。

亿赛通认为，数据安全综合管理平台是未来数据安全防护的发展方向。近两年，多家调研机构将数据安全运营管理平台领域单独拆分输出报告。此前，据某调查显示，78% 的受访企业使用 16 种以上的单点安全产品，12% 的受访企业使用 46 种以上的单点安全产品。这意味着大多数企业使用的都是松散、割裂的单点安全解决方案。同时，企业使用的各种单点安全产品又通常都是孤立运行，这导致网络运营团队和安全运营团队无法获得整个企业数据流量的可见性。而亿赛通自主研发的数据安全运营管理平台可以与其他安全产品形成联动，能够将原有的数据库审计、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。

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。亿赛通数据安全运营管理平台能够实现与各个能力组件的配合，结合分类分级结果进行差异化策略部署，兼顾安全与效率。

面对愈演愈烈的安全形势，亿赛通进一步加快技术创新与布局，眼下各行业正加速数字化进程，我司不断夯实自身安全能力，积极研发更多具有行业前瞻性、竞争力的核心产品，紧跟当前数字经济趋势，以承载各行各业持续升级的数据安全需求。

亿赛通登榜 2023 高成长企业 TOP100，破旧立新助力数据安全驱动

近日，由北京中关村高新技术企业协会、中关村创业投资和股权投资基金协会指导，智成企业研究院主办的以“创新聚力 生态赋能”为主题的“2023 高成长企业 TOP100 年度盛典”颁奖典礼暨创新生态发展论坛在北京成功召开，亿赛通作为“高成长企业 TOP100”入选企业出席颁奖典礼并在圆桌论坛环节发表重要讲话。

2023 高成长企业 TOP100 活动自 2023 年 5 月 31 日开启报名征集，经由报名征集、榜单初筛、项目初审、复审路演、走访调研、专家合议等环节，围绕营收成长性、创新成长性、员工成长性、人均营收成长性四个成长性维度，遴选出 100 家最具有发展潜力和行业代表性的高成长科技企业，并于 2023 年 10 月 31 日正式对外发布“2023 年高成长企业 TOP100”名单。亿赛通凭借强劲的研发创新能力和科技实力脱颖而出。

北京亿赛通科技发展有限责任公司专家在圆桌论坛环节与来自相关领域的企业领袖、行业精英共同探讨如何智慧赋能千行百业。他表示随着数字经济的深入发展，数据规模庞大、关联主体众多、流通场景复杂，需求侧对数据安全风险防范手段提出了更高要求。利用人工智能技术，对理论知识和经验沉淀进行深度学习，在技术工具中内化为功能指标，从而完善数据安全基线能力。此外，通过人工智能算法，可实现对数据安全风险的精细预判和数据安全事件的精准溯源，进一步夯实事前防御、事中管控、事后复盘的能力。

数据安全作为加快建设数字中国的重要手段，是企事业单位数字化转型的重要关注点之一，对推动我国数字化、智能化发展具有重要作用。作为国家级专精特新“小巨人”企业，亿赛通在数据安全领域拥有丰富的技术研发、产品创新经验，致力于向政企、金融、制造、生物医药、科教文卫等领域提供完善的数据安全综合解决方案。即通过智能化、自动化工具引擎对业务与数据进行梳理，形成人与数据间的安全策略并导入到安全运营组件。运用独特的安全服务 + 安全产品 + 平台运营的管理体系为客户提供数据安全体系化服务。从业务梳理、分类分级、策略制定、技术管控等方面帮助客户建立全方位的数据安全体系建设。

具体到技术上体现在通过智能化分类分级工具快速准确地完成组织的业务梳理和数据梳理，并形成规范化的策略库，即主体、客体及两者之间的策略，同时将上述数据根据积累的知识库智能化衔接到数据安全运营管理平台，通过整体咨询服务，借助分类分级系统，应用 AI 技术，实现数据安全治理智能化。将各个孤立的安全系统（新一代电子文档安全管理系统、数据泄露防护系统、数据库安全审计系统、数据脱敏系统……）进行资源整合，实现了对组织数据的智能识别、智能防护、智能监测、智能运营，构建可视、可控、可管、可溯的覆盖数据全生命周期的综合解决方案。

对安全厂商而言，业务在变，数据也在变，因此产品技术也要不断升级、创新。为了应对变化，亿赛通持续不断对自身产品技术进行迭代升级，再结合各行业合规政策导向，可适应不同使用场景和环境，并提供具备智能化以及更强安全性能的数据安全治理体系。

高端访谈｜亿赛通宋春岭：数据安全治理：打好“技术 + 管理 + 监管”组合拳

北京亿赛通科技发展有限责任公司高级总监宋春岭

宋春岭简介

宋春岭，自 2007 年起从事信息安全产品研发设计工作。担任企业多项重量级大项目的研发和项目实施，在产品架构部署和数据安全产品研发设计管理中有丰富实战经验。曾荣获中国信息通信研究院云大所数据安全推进计划专家，中国计算机行业协会数据安全专业委员会专家委员，中关村科技园经济技术创新标兵称号。现任北京亿赛通科技发展有限公司高级总监，负责数据安全产品的设计、技术研发方向拟定、技术标准制定。

随着数字经济的蓬勃发展，数据已经成为新时代的重要生产要素，并成为国家基础性战略资源。一方面，构建不同行业、领域规范化数据开发利用场景，提升各行业数据资源的价值，促进数字经济产业集群发展成为大势所趋；另一方面，数据安全和隐私保护问题愈发突出，数据流转过程中暴露面风险急剧加大，面临严峻的数据安全风险防护和合规监管要求形势。在安全风险与监管合规双重驱动下，如何促进数据发展与数据安全的平衡发展，企事业单位也在不断开展数据安全治理工作，防止数据面临的“走光风险”，由于数据频繁产生与流转带来的数据安全防护复杂性，如何在数据释放价值的同时，保障数据安全，推动平衡发展？企事业单位在数据安全治理实践过程中，面临着诸多的痛点和难题。近日，记者与北京亿赛通科技发展有限责任公司高级总监宋春岭围绕数据安全治理现状、数据安全治理难点分析、数据安全治理体系建设及数据安全防护技术研究等内容进行了详细沟通和探讨。

记者：请您谈谈，现阶段数据安全治理状况。

宋春岭：在从业人员方面，中国的数据安全治理现状需要专业人才涵盖多个领域。首先是数据安全专家，他们负责制定数据安全策略、管理数据风险和实施数据安全控制措施。其次是网络安全专家，他们负责保护网络系统免受黑客攻击和恶意软件的侵害。另外，数据隐私专家、法律顾问和数据治理专家也扮演着重要的角色，他们确保数据处理符合法规和道德规范。数据安全治理还有近 200 万人的缺口，为有志从事数据安全的人员提供了足够大的空间。在理论方面，中国的数据安全治理借鉴了国际上的最佳实践和先进的理论模型。同时，中国也基于自身国情和发展需求，制定了适用于本国的数据安全理论和指导原则。其中包括：数据安全风险管理体系、数据分类和标记、隐私保护、风险评估和风险管理、最小权限原则、数据生命周期管理等。已经形成自己的理论体系和标准。在技术方面，中国积极发展数据安全技术。这包括数据加密技术、密码技术、身份认证技术、安全存储和传输技术、数据脱敏和匿名化技术、数据分类分级、泄露防护技术等。同时，中国也在推动人工智能、区块链等前沿技术与数据安全的结合，以提升数据安全的能力和效果。在产品方面，国家相关部门发布了一系列的数据安全法律法规，国家、地方、行业的多级标准和认证体系，促进了数据安全产品的开发和使用。这些产品涵盖了数据生命周期采集、存储、传输、处理、交换和销毁各个阶段，能够满足不同行业和组织的数据安全需求。

记者：请您谈谈，政企单位在数据安全治理方面存在的难点。

宋春岭：政企单位在数据安全治理方面存在以下 4 个主要难点：第一，政企单位需要处理和存储大量的数据，增加了数据管理和安全保护的难度。第二，政企单位涉及多个利益相关方，需平衡各方的权益，并建立合理的数据安全管理机制。第三，缺乏专业数据安全人才，员工缺乏数据安全意识，影响数据安全的管理和保护。第四，数据安全技术和威胁不断演进，政企单位需要持续应对技术的发展带来的不断变化的安全威胁。

如果要解决这些难题，需要综合考虑技术、管理和意识等多个方面的因素，以确保数据的安全和合规，整个数据安全治理过程要从决策层到技术层，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，构建自上而下、全流程、可闭环的完整链条。具体来讲，数据安全治理以“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，建立全面综合的数据安全治理能力。

记者：请您谈谈，对数据安全治理体系的建设和实践的建议。

宋春岭：数据安全治理体系不仅仅是一套用工具组合

的产品级解决方案，它构建了从决策层到技术层，从管理制度到工具支撑，自上而下贯穿整个组织架构的完整链条，打造以“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、增值建立重要保障。

图 1　亿赛通数据安全治理体系框架具体来讲，要制定明确的安全策略和流程。数据安全治理要制定清晰的数据安全策略和流程，包括数据分类、访问控制、数据处理和存储规范等方面，确保相关人员了解和遵守安全策略和流程，以保障数据的安全性。这方面也可以由第三方数据安全咨询公司来梳理和制定。再者，要采用综合技术保障措施，例如加密、防火墙、入侵检测、预防系统、数据泄露防护等。而且要定期进行安全漏洞扫描和渗透测试，及时发现和修复潜在的漏洞和风险。此外，还要建立合理的访问控制和权限管理机制。根据数据的敏感程度和用户的角色，设置恰当的访问权限和控制措施，然后采用强密码策略、多因素身份验证等方式，确保只有授权的人员可以访问和处理数据。需要强调的是，数据安全治理中，加强数据监控和审计也十分必要。建立有效的数据监控机制，能够实现对数据访问和使用进行实时监控，及时发现异常行为，然后定期进行数据审计和日志分析，确保数据的合规性和安全性。对于涉及第三方数据处理和存储的情况，更要进行严格的风险评估和选择，建立合适的合作和监管机制。确保第三方符合安全合规要求，并对其进行有效的监控和审计。另外，还要培养员工的安全意识和技能，加强员工数据安全能力培训，提高他们在日常工作中的安全意识和行为，并定期组织模拟演练和应急演练，增强员工应对安全事件的能力。数据安全治理是一个持续的过程，需要根据实际情况和法规要求进行具体的定制化和调整，从而建设一种先进、自主、灵活、全面、智能的立体化数据安全防护体系，实现企业非结构化数据的有效管理和保护，有效保障数据资产的安全可控。

记者：请您谈谈，对用户在数据安全治理方面的产品选型和能力评估的建议。

宋春岭：首先，用户应确切地了解自己的数据安全需求和目标。这包括需要保护的数据类型、安全合规要求、预算限制等，明确需求和目标将有助于用户更好地匹配和评估相应的产品和解决方案。其次，用户还应综合考虑产品的安全功能和特性。这可能包括数据加密、终端管理、访问认证控制、文件管理、数据存储、泄露防护、流转安全、备份等功能。确保产品提供的安全功能能够满足用户的具体需求。另外，还要考虑选用的产品在规模扩展和系统兼容性方面的能力。用户需要确保产品能够适应未来安全需求的增长和变化，并与现有系统和技术环境兼容。同时，用户应考虑产品供应商提供的服务和技术水平。可信赖的技术服务将有助于用户在使用产品时获得及时的支持和解决问题。需要强调的是，用户在注重产品和服务的同时，也要更加注重关联性的数据安全工具的建设。具体来讲，需要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。亿赛通数据安全运营管理平台遵循 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。

图 2　亿赛通数据安全运营管理平台

记者：请您谈谈，亿赛通在数据安全管理方面的实践。

宋春岭：亿赛通在数据安全管理方面主要包括智能识别、智能防护、智能监测、智能运营。智能识别强调工具智能识别为主、人工配合为辅的理念。通过数据嗅探、网络解析、智能上报等方式梳理网络中的数据库、终端、文件服务、大数据及云数据，形成数据资产清单。

智能防护则依据分类分级结果对不同级别的数据配置不同的安全策略，兼顾成本与安全。基于智能识别结果构建安全智能防护，不同的主体（组织、角色、人员等）对不同级别的客体（终端数据、网络数据、云端数据以及数据库等）采取不同数据防护策略，对绝密数据、机密数据，采取文件加密、数据脱敏、数据水印等高强度管控技术措施，严格限制分享时间，建立数据接收方白名单；对内部不敏感数据只需要进行相关审计。智能监测是对于不同的能力节点的数据进行综合审计分析，形成基于“人”和“事件”的风险画像，完成数据流转过程的高效审计，及时做好全局管理。智能监测通常包括：数据库监测、网络数据监测、终端数据监测、敏感数据分布监测、用户行为监测、API 接口监测、热点应用监测及异常账号监测。智能运营强调数据各个环节的互联、互补、互通，通过对不同能力模块的关联分析来定位风险，通过事件编排处置风险，通过事件追溯完善策略。从而形成覆盖事前预警、事中处置、事后分析的闭环管理。

记者：未来数据安全防护技术将延伸出哪些新的发展特点？

宋春岭：总体来讲，未来数据安全防护技术将延伸至 AI 和机器学习、区块链、边缘计算安全、数据隐私保护、多因素身份验证和融合安全解决方案等方面。这些新的发展特点将为数据安全提供更强大、智能、综合的保护。

具体来讲，AI 和机器学习技术在数据安全领域的应用将进一步扩展。这些技术可以帮助检测和分析大量的数据，识别出潜在的安全威胁和异常行为，并提供更快速、准确的安全响应和预测能力。区块链技术方面，区块链技术逐渐在数据安全领域发挥着重要作用。区块链可以提供去中心化的数据存储和交换，保障数据的不可篡改性和身份验证。未来，区块链技术还将广泛应用于数据保护、身份认证和智能合约等方面，提供更强大、更安全的防护。数据隐私保护方面，数据隐私保护将成为数据安全的重要组成部分。随着隐私法规的加强和用户对个人数据保护需求的提升，数据安全技术将更注重个人隐私的管理和保护，包括匿名化技术、对抗数据分析和差分隐私等手段。多因素身份验证方面，为了增强身份认证的安全性，多因素身份验证将得到更广泛的应用。未来的数据安全技术将推动更多的身份验证方式，如指纹、虹膜扫描、声纹识别等，以提供更强大的身份验证保护。另外，综合安全解决方案也将得到更多关注和应用，以应对不断变化和复杂化的安全威胁。未来的数据安全技术将集成多种安全措施和技术，例如威胁情报、行为分析、入侵检测和响应等，以提供更全面、协同的安全防护能力。

亿赛通出席天津滨海高新区《商业秘密保护主题沙龙》赋能企业数据安全合规建设

11 月 29 日，由天津滨海高新区市场监督管理局指导，天津滨海高新区商业秘密保护协会等单位主办，北京亿赛通科技发展有限责任公司协办的《商业秘密保护主题沙龙》在天津顺利举办。本次活动旨在为企业提供深度洞察和实用指南，助企业在竞争激烈的商业环境中更好地管理和保护企业的商业秘密。与会嘉宾主要为制药行业、工程行业的二十余家企业代表。亿赛通作为中国开发区协会商业秘密保护专委会的发起单位，始终坚持赋能企业数字化转型，进一步提升企业商业秘密保护意识和能力，切实保障企业的合法权益和创新活力。本次，亿赛通咨询顾问受邀为与会嘉宾深入讲解了《企业商业秘密保护之数据安全管理》。

商业秘密是企业通过长期研发投入和市场积累所形成的具有企业私有属性的数据资产，是企业发展的核心竞争力。加强商业秘密保护，是落实反不正当竞争的重要任务，是强化知识产权保护的重要内容，对于优化营商环境，激发市场主体活力和创造力，推动我国经济创新发展具有重要意义。

亿赛通咨询顾问在会中介绍到，现在商业秘密保护实操性不强。与国家秘密不同，商业秘密特别是科技类商业秘密，全部产生于基层，应用于基层。保护工作必须依靠基层人员在实际工作中亲力亲为。由于基层员工没有手段执行。集团公司对企业尚未出台技术手段。从行业来看，政府 / 央企商业秘密保护制度体系与责任体系已基本完善。但在制度落地执行方面，基层员工“不会保，不想保，不敢保”现象突出。

那么，企业应如何进行商业秘密保护呢？数据安全是组织稳健经营的重要因素，亿赛通建议组织通过识别和整改数据安全风险及问题，逐步完善权限管理和数据安全评估等管控流程，覆盖数据生命周期安全防护，严格执行数据日志内部审计和安全备份等制度，建立数据管理应急机制，通过提升安全团队专业化能力来逐步构建企业的数据安全文化，助推企业数据资产价值的不断提升。提出建立有效的技术防护手段是对企业安全意识逐渐强化、培养的过程。落实到具体方案则是以横到边，纵到底为基础，以全周期、全过程、全人员、全威胁保障为目标，从管理、技术、运维、运营四个方面进行建设，逐步建立数据安全立体化防护体系。

亿赛通为企业建设科学先进、自主可信、可扩展同时又满足商密保护合规要求的全方位数据防泄密体系。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。平台部署可有效降低业务运营中的数据风险，提升企业敏感数据防护能力，降低多重安全合规管理成本。

我国商业秘密保护的步伐正在不断加快，其中，数据安全可谓是企业发展的生命线。接下来，亿赛通会再接再厉、开拓创新，奋力协助开创数字政府新局面。继续发挥技术优势，加大研发创新，以过硬的技术和产品持续构筑坚实的数据防御工事，为全面提升企业商业秘密保护能力水平提供可靠的技术支撑。

亿赛通解码企业级数据安全治理智能化体系与应用实践

12 月 2 日，2023 大模型驱动数字安全新实践论坛暨颁奖典礼在北京召开，亿赛通受邀参加并发表主题演讲。本次论坛邀请数据安全领域产学研专家，共同聚焦数字经济时代下，数据安全大模型的现状、关键应用场景、技术创新等内容，探讨产业发展新思路、新篇章，为促进数据安全领域产业高质量发展，推动数据资源有序开发和深度利用，保障数字强国建设夯实基础。

亿赛通 CTO 朱贺军发表主题为《亿赛通数据安全治理智能化体系与应用实践》的演讲。他表示，根据 Ponemon 和 IBM Security 发布的《2023 年数据泄露成本报告》，2023 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 445 万美元，相较过去三年中，违规成本增加了近 15%。数据安全普遍存在外部风险难预防、内部违规难发现、综合攻击新挑战等问题日益凸显。企业核心数据呈现出规模化产生、海量集中、频繁流动交互等特点，已成为提升企业生产力、竞争力和创新力的关键要素，保障数据安全的重要性愈发突出。

当前，数据作为数字经济时代的关键生产要素、国家基础战略性资源，数据改变生活的同时面临的安全问题也日益严峻，亿赛通提出了综合数据安全治理一站式解决方案。通过智能化、自动化工具引擎对业务与数据进行梳理，形成人与数据间的安全策略并导入到安全运营组件。运用独特的安全服务 + 安全产品 + 平台运营的理念为客户提供数据安全体系化服务。从业务梳理、分类分级、策略制定、技术管控等方面帮助客户建立全方位的数据安全体系建设。

亿赛通基于运营管理平台通过整体咨询服务，借助分类分级系统，应用 AI 技术，实现数据安全治理智能化。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。通过智能化分类分级工具快速准确地完成组织的业务梳理和数据梳理，并形成规范化的策略库，即主体、客体及两者之间的策略，同时将上述数据根据积累的知识库智能化衔接到技术平台，实现了对组织数据的智能识别、智能防护、智能监测、智能运营，构建可视、可控、可管、可溯的覆盖数据全生命周期的综合解决方案。

随着我国数字经济的稳步发展，新一代信息技术已经成为引领创新和驱动发展的动力源，为稳经济、惠民生、增活力、促发展发挥重要作用。亿赛通通过体系化的数据安全治理方法论，为客户提供全方位的数据产品和服务，经过多年的探索实践与不断优化，得到业内普遍认可。未来，亿赛通将继续加大在数据安全领域的研究力度，秉持“中国数据安全专家”之使命，以自身丰富的技术经验为依托，持续助力企业数据安全发展。

2023 数据安全与商业秘密保护专业研讨会顺利召开

为切实凝聚数据安全与商业秘密保护共识，构建开放合作的生态体系，深入探讨数据安全和商业秘密保护的政策与制度体系、司法实践、技术体系等的深度融合，2023 年 12 月 14 日下午，由中国开发区协会主办，中国开发区协会商业秘密保护专业委员会、北京网络行业协会、中国技术创业协会孵化分会承办，中关村软件园联合承办，北京亿赛通科技发展有限责任公司协办的“2023 数据安全与商业秘密保护专业研讨会”在北京中关村软件园隆重召开。

中国开发区协会副会长王磊，北京网络行业协会会长袁旭阳出席会议并致辞。

中国开发区协会副会长王磊致辞

中国开发区协会副会长王磊指出，商业秘密是企业通过长期研发投入和市场积累所形成的具有企业私有属性的数据资产，是企业发展的核心竞争力。后续中国开发区协会将指导商业秘密保护专委会继续响应国家和有关部门号召，积极构建政策研究、司法实践、各类服务平台为核心的生态体系。通过专业的服务，切实保障企业和园区的合法权利和创新活力，为国家商业秘密保护体系的建设发挥积极作用。

北京网络行业协会会长袁旭阳致辞

北京网络行业协会会长袁旭阳指出，随着相关政策的发布，商业秘密保护法律体系逐步建立，创新试点工作加速推进。与此同时，在新兴技术广泛应用的情况下，商业秘密呈现“数据电子化、侵权主体多元化、侵权手段科技化、侵权行为复杂化”等特征，物理隔离、事后补救等传统的保护手段难以有效应对新形势下产生的新需要。希望通过专委会构建的生态体系能够持续探讨并形成有效的政策建议，推动商业秘密保护政策和实践的深度融合。

本次研讨会邀请到了数据安全和商业秘密保护的政策和行业研究专家、司法实践专家、技术防护专家等共同探讨数据安全和商业秘密保护的制度体系和实践案例，以帮助企业提高数据安全和商业秘密保护意识和手段。本次研讨会分为“数据安全”和“商业秘密”两个环节。

中国计算机学会计算机安全专业委员会荣誉主任，公安部第一研究所、第三研究所原所长、一级警监、研究员、中国开发区协会商业秘密保护专委会智库首席专家严明针对《数据安全与信创的几个话题》做主题演讲。他指出，在信息社会中，数据是重要的资源，数据资产化是促进数据要素合规高效流通使用的重要手段。数据将会是构成资本的重要要素。当数据“动”起来的时候，其有效保护和合法利用的状态需要数据安全技术来维持。严明认为自主创新的路，虽然艰难，但是这是中华民族复兴的必然之路。创新是改革开放的生命。

中国网络安全审查技术与认证中心副处长王凤娇针对《数据安全治理背景下的数据安全认证探索与实践》做主题演讲。她指出，在数字经济成为稳增长促转型的重要引

擎这一背景下，数据安全认证发挥着日益重要的时代价值，是支撑法律法规落地的需要，是支撑政府监管、提高监管专业化水平、降低政府成本的需要，也是帮助网络运营者实现合规、促进市场正向发展的需要，符合社会多元主体的利益期待。王凤娇同时还介绍了两项国推数据安全认证（数据安全管理认证、个人信息保护认证）的推进情况，建议有相关需求的企业通过开展相关认证来达到基线合规要求。

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）安全事业部技术总师白利芳针对《数据安全产业政策及发展趋势》做主题演讲。演讲从四个角度分析数据安全产业政策及发展趋势，即看环境、看现状、看机遇和看行动。她认为，重视发展数据安全产业已成大势所趋，我国数据安全产业发展已具备一定基础。并倡导数据安全产业主体应把握四大机遇推动数据安全产业发展，也期待未来大家共同凝聚发展合力，协同打造数据安全产业发展新局面。

清华大学社科学院经济所博士生导师，清华数据要素与数字技术实验室副主任、清华长三角研究院产城融合研究中心主任谢丹夏针对《数据创新经济增长理论及数据要素价值释放》做主题演讲。他指出，近些年来数据量急速增长，数据已成为和土地、劳动力、资本、技术并列的第五大基础生产要素。“数据创新内生增长理论”刻画了数据参与创新的过程，并对数据隐私风险进行统筹分析，根据模型测算，经济增长率可达到 2.90%，比斯坦福大学团队研究结果要高出很多。最后谢教授以跨境电商为例阐述了数据要素价值释放的过程，实践证明，数据创新经济增长理论具有重要的前瞻性和实践意义。

清华大学法学院教授、清华大学法学院知识产权法研究中心主任、国家市场监督管理总局法律顾问、最高人民法院知识产权司法保护研究中心研究员、北京市海淀区人民法院专家咨询委员会委员崔国斌针对《商业秘密独创性标准的证伪》做主题演讲。他指出，企业数据集合与传统商业秘密在内容性质、生产过程和数据规模方面有所区别。他认为商业秘密法的立法目的一是限制背信等违反商业道德的行为，二是降低企业间数据交易的成本，三是避免行业陷入丛林法则，刺激企业耗费更多资源于保密措施，造成社会资源的浪费。我们应当彻底拥抱“实质性投入”标准，即商业秘密的秘密性标准中不应包含创造性的要求。只要数据收集者付出“实质性投入”，就满足了“不为公众所知”的秘密性标准。

最高人民检察院新闻办副处长宋海涛针对《为大局服务，为人民司法，为法治担当，做好涉及侵犯商业秘密知识产权保护工作》做主题演讲。他指出，商业秘密是企业的核心竞

争力，保护商业秘密，既是维护权利人合法知识产权、合法经济利益的需要、更是维护良好市场竞争秩序的必然需要。他结合侵犯商业秘密实践案例讲解了商业秘密认定的三种情形、证据收集的三种情形、并以四个实践案例分析了犯罪数额认定的原则。

北京市海淀区人民法院知识产权庭副庭长李莉莎针对《数据竞争与商业秘密保护》做主题演讲。她指出，数据基础制度构建是当前的重要任务，而数据竞争领域相关规则的构建也成为题中之义。李庭长结合主体、客体、行为手段、损害后果四个方面分析数据竞争类案件特点，并从合法权益、保护范围、法律适用、赔偿数额等方面梳理此类案件的审理要点，希望通过本次分享帮助企业更好利用数据、保护数据，以期维护数据竞争秩序，助力良好营商环境构建。

北京市海淀区市场监督管理局公平竞争科科长周晔针对《商业秘密保护政策及试点工作开展情况》做主题演讲。她指出，商业秘密保护对于推动产业创新发展和企业高质量发展具有重大意义，同时详细介绍了商业秘密的行政保护与司法保护的关系、商业秘密的行政保护的内容以及海淀区商业秘密保护试点工作情况。她希望力争用三年时间，通过高标准建设、高水平保护、高品质服务打造富有海淀区域特点的商业秘密保护特色品牌，推动形成“政府引领、部门协同、企业参与、社会联动”的商业秘密保护工作格局，为海淀区提升产业创新生态，促进经济高质量发展，加快建设北京国际科技创新中心核心区提供有力支撑。

盈科北京律师事务所高级合伙人律师、中国世界贸易组织研究会（CWTO）竞争政策与法律专业委员会（PCCPL）顾问王俊林针对《企业商业秘密保护体系构建及合规管理》做主题演讲。他介绍了商业秘密与专利、知识产权的关系以及商业秘密的概念，并提出了企业应从商业秘密分级管理制度、商业秘密知悉人员管理制度、商业秘密载体防范措施、涉密区域访客制度等十一个方面构建商业秘密保护制度体系。他指出，企业应加强对商业秘密的保护，并对应建立起有效地、适合企业业务需求的商业秘密保护体系及法律保护措施，做到未雨绸缪，才能最大限度地防止商业秘密的泄漏，最大限度地消除法律隐患。

最后，中国开发区协会商业秘密保护专业委员会秘书长张兰兰针对数据安全和商业秘密保护等几个概念之间的关系做会议总结。她指出，数据包含商业秘密，数据和商业秘密的共同点是积极保护，差异点是数据更需要充分流动，商业秘密需要有限流动，终端产生和存储近百分之八十半结构化

和非结构化数据，而这些数据又在网络中流转，所以做好终端和网络数据防护非常重要。中国开发区协会商业秘密保护专业委员会将致力于提供全视角的整体解决方案，以专项和综合服务满足客户需求，创造商业秘密保护的最佳实践，成为最具价值的商业秘密保护服务平台。

中国开发区协会商业秘密保护专业委员会主任崔培升

北京网络行业协会专家邓宏敏，北京网络行业协会专家赵学英，北京网络行业协会专家吴俭，国家市场监管管理总局认研中心中认国证创新中心总监赵广哲，北京大学出版研究院副院长、博士生导师黄国彬，中国科学院计算机网络信息中心研究员、中国互联网络信息中心原副主任王伟，北京柏舟律师事务所高级合伙人、中国开发区协会商业秘密保护专业委员会智库专家胡瑞，北京海淀中小企业协会秘书长申焰，中国开发区协会商业秘密保护专业委员会主任崔培升以及部分网络安全与数据安全企业、律师事务所、软件与信息化服务企业、智库、科技研发、司法鉴定中心等机构代表参加本次会议。

中国开发区协会副秘书长曾召贺主持嘉宾介绍和致辞环节

中国技术创业协会孵化分会秘书长王晓利主持数据安全主题分享环节

中国开发区协会商业秘密保护专业委员会秘书长张兰兰主持商业秘密主题分享

未来，中国开发区协会商业秘密保护专业委员会将通过专业的服务，积极贯彻落实有关部门对商业秘密保护的制度要求，以服务园区和企业为宗旨，为园区提供全流程商业秘密保护服务，切实保障园区和企业的合法权益和创新活力，助力开发区成为深化科技创新、优化营商环境的示范样板。

当数据安全遇见智能制造，亿赛通硬核产品助力制造企业安全可视化

数字经济时代，企业越来越感到前所为遇的困境，企业发展正处在进退两难的十字路口，如何创新管理和商业模式，让企业踏上新的征程，是企业信息化引领者首先需要进行探索和思考的问题。2023 年 12 月 22 日，“云数筑基 企创赋能 2023 年度嘉兴 CIO 峰会”顺利召开。本次峰会以云计算为平台，大数据资源为生产要素，打造“围绕云计算、大数据、人工智能等新兴技术，平台 + 生态”的产业主流模式，催生以新模式，新链接、新生态，新运营为特征的企业创新新模式。亿赛通作为数据安全领域首屈一指的行业专家受邀参会，为嘉兴地区制造型企业信息化建言献策。

制造业是国民经济的基石，是立国之本、兴国之器、强国之基。12 月，国家数据局公布了备受关注的《“数据要素 ×”三年行动计划（2024—2026 年）（征求意见稿）》（以下简称《三年行动计划》），就数据要素 × 的 12 个领域做出原则性部署。其中就有数据要素 × 智能制造领域。希望在制造业能推动数据在不同场景中发挥千姿百态的乘数效应，促进我国数据基础资源优势转化为经济发展新优势。

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。

以本次展出的数据安全治理智能化技术体系为例，亿赛通通过智能化分类分级工具快速准确地完成组织的业务梳理和数据梳理，并形成规范化的策略库，即主体、客体及两者之间的策略，同时将上述数据根据积累的知识库智能化衔接到技术平台，实现了对组织数据的智能识别、智能防护、智能监测、智能运营，构建可视、可控、可管、可溯的覆盖数据全生命周期的综合解决方案。

除此之外，亿赛通还针对数据全生命周期的多场景、高性能、智能化的安全治理需求，历经 20 余年的技术积累和上万个交付项目的沉淀，重点突破了端点数据自适应防护、海量数据内容审计、重要数据深度感知、敏感数据智能防护等关键技术，授权了 50 余项发明专利，达到了国际先进水平，提出了数据安全“分放管服”建设理念，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。峰会现场诸多参会人员均反馈，此次参会为制造业数据安全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。

数据已经成为数字经济时代的最新生产要素，成为国家基础性和战略性资源。加强数据安全成为与整体经济发展与国家安全紧密相关的重要方面。数据安全旨在强调树立正确的数据安全观，在智能制造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。

亿赛通强势入围《2023 中国网络安全产业势能榜》，制造业成就有目共睹

近日，嘶吼安全产业研究院发布《2023 中国网络安全产业势能榜》评选结果，亿赛通凭借行业先进的技术优势、产品的创新能力和成熟的行业标杆案例打造能力，在百余家调研企业中脱颖而出，作为“专精型”厂商荣登制造行业势能榜单。

《嘶吼 2023 中国网络安全产业势能榜》由嘶吼安全产业研究院调研，选取政务、金融、能源、制造、运营商、互联网、电力、教育、医疗、交通十大热门行业以及“综合型”、“专精型”、“创新型”三大类型，历时数月的调研、数据提炼、横向对比，打分复核等阶段，最终评选出 105 名优秀的行业安全厂商，全面激励网络安全产业更加健康有序深化发展。

智能制造已经成为我国经济发展的重要推动力，对于促进数字经济的高质量发展、提振社会经济将发挥重要作用。制造业相关企业逐步将研发、生产、管理、营销等多方面数据进行有效整合，力争全面贯彻落实《中国制造 2025》，实现战略强国目标。数字化转型的基础是数据，数据安全建设大势所趋，重要性日益凸显。而随着数字化持续推进，智能制造业正面临着前所未有的数据泄露风险。特别是在不同业务间、机构间流转的过程中，从技术到管理都面临众多潜在的安全风险，需要加强安全设置和制度保障。

作为国内早期聚焦数据安全领域的专精型厂商，亿赛通针对数据全生命周期的多场景、高性能、智能化的安全治理需求，重点突破了端点数据自适应防护、海量数据内容审计、重要数据深度感知、敏感数据智能防护等关键技术，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。通过智能化分类分级工具快速准确地完成组织的业务梳理和数据梳理，并形成规范化的策略库，即主体、客体及两者之间的策略，同时将上述数据根据积累的知识库智能化衔接到技术平台，实现了对组织数据的智能识别、智能防护、智能监测、智能运营，构建可视、可控、可管、可溯的覆盖数据全生命周期的综合解决方案。

亿赛通完整的数据安全产线能够围绕数据安全“事前、事中、事后”三大关键阶段，构建覆盖数据全生命周期的安全防护体系。自主研制了电子文档安全管理系统、数据泄露防护系统、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、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。

此外，亿赛通根据国家政策、法规及标准要求，结合各行业发展趋势，深度调研分析不同用户差异化场景和需求，为用户提供包含数据安全咨询服务、数据安全运营服务、数据分类分级在内的数据安全治理服务。

这已经是亿赛通连续两年入围嘶吼中国网络安全产业势能榜（制造），更加直观的展示了亿赛通在安全领域和制造业的非凡实力。业界的肯定和褒奖也将驱动亿赛通持续深耕数据安全领域，丰富安全产品与方案，提升安全服务能力，为更多行业用户的数字化发展保驾护航。

荣登安全“奥斯卡”|亿赛通入选 ISC 2023 创新百强榜单

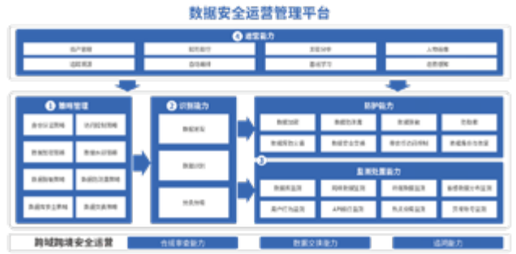
12 月 27 日，ISC 2023 数字安全创新能力百强评选榜单正式揭晓，数据安全运营管理平台再次凭借卓越的核心技术、创新模式和实战应用成果在评选中脱颖而出，以数据与隐私安全领域代表厂商身份入选“ISC 2023 创新百强”并受邀参会讲解。

作为数字安全界的“奥斯卡”，ISC 2023 创新百强评选历时近两个月，来自数字安全行业数百个产品及解决方案参选。此次亿赛通数据安全入选是行业权威资讯机构、行业专家、客户是对我司在数据与隐私安全领域的理论与实践创新价值的肯定。适逢数字安全从被动防御向主动防御转型，具备平台化、体系化、智能化的安全产品将激发企业主动防御的韧劲与潜力。

数据安全风险下的“防护利器”

伴随着数字化变革，企业不断扩张的数字资产让数据风险呈现井喷增长，数字资产“非常规化”、“移动化”、“多样化”的趋势日益明显。资产是安全运营工作开展的基础，如果对资产没有完善整理防护，广泛分布在企业内部，引发的安全风险令人防不胜防。因此，亟需对数据资产进行高效的管理、合理的资源分配以及有效的安全监测和防护。

亿赛通认为，综合管理平台是未来数据安全防护的发展方向。据调查显示，78% 的受访企业使用的仍是单点安全产品。这意味着大多数企业使用的都是松散、割裂的单点安全解决方案。同时，企业使用的各种单点安全产品又通常都是孤立运行，这导致网络运营团队和安全运营团队无法获得整个企业数据流量的可见性。



此次入围的亿赛通数据安全运营管理平台正是可以与其他安全产品形成联动，能够将原有的数据库审计、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。

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，运营实际上就是服务。亿赛通专门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。

亿赛通数据安全运营管理平台能够实现与各个能力组件的配合，结合分类分级结果进行差异化策略部署，兼顾安全与效率。

据了解，亿赛通数据安全运营管理平台已成功为金融、政府、运营商等不同行业的客户提供了管理支持，服务用户单位的数据安全治理建设。面对瞬息万变的数据安全大环境，中国的数据安全治理创新已然迅捷起步，并以乘风破浪的姿态不断向前行进。未来，亿赛通将继续坚持技术创新，并与更多的行业专家、安全从业者等合作探讨、互利共赢，共同绘制数字安全技术创新的新蓝图。

政策速递 | 工信部公开对《工业和信息化领域数据安全行政处罚裁量指引（试行）》征求意见

数据安全行政处罚是督促数据处理者依法依规落实数据安全保护义务、强化数据安全监管的重要手段。《数据安全法》设立专章明确法律责任，对数据处理者的违法行为提出系列处罚措施。为进一步衔接细化《数据安全法》相关罚则规定，构建行业数据安全行政处罚职权体系，统一数据安全行政处罚尺度，指导行业监管部门开展数据安全行政处罚工作，有效提升数据安全监管执法能力，2023年11月23日，工业和信息化部公开对《工业和信息化领域数据安全行政处罚裁量指引（试行）》（以下简称《裁量指引》）征求意见。

本次发布的《裁量指引》由正文及附件《工业和信息化领域数据安全行政处罚裁量基准裁量基准》（以下简称《裁量基准》）组成。其中，正文包括总则、管辖、数据安全行政处罚情形及附则，共五章二十六条；附件共十四条。主要内容如下：

1、明确适用范围与行政处罚裁量权概念

《裁量指引》适用于在中华人民共和国境内开展的工业和信息化领域数据安全违法行为行政处罚裁量工作。

行政处罚裁量权，是指工业、电信、无线电行业监管部门在职责范围内对数据处理活动进行监管处罚时，根据行政处罚原则，在法律、行政法规等规定的行政处罚种类和幅度内，综合考量违法的事实、性质、手段、后果、情节和合规措施等因素，正确、适当地确定行政处罚的种类、幅度或者作出不予行政处罚决定的选择适用权限。

2、明确不同层级的管辖争议解决方式

类别	解决方式
属地管辖	由违法行为发生地的行政处罚机关管辖。数据安全违法行为发生地包括实施违法行为的住所地、实际经营地、工商注册地（工商注册地与实际经营地不一致的，应按实际经营地），网络接入地，取得电信和互联网信息服务相关许可（备案）所在地，网站建立者、管理者、使用者所在地，计算机等终端设备所在地，数据集中存储地、交易地、出境活动所在地等。
交叉管辖	两个及以上行政处罚机关对同一违法行为均有管辖权的，应当由最先立案的行政处罚机关管辖。
指定管辖	两个及以上的行政处罚机关对管辖权有争议的，应当在发生争议之日起7日内协商解决，协商不成的，应当在7日内报请共同的上一级行政处罚机关指定管辖；也可以直接由共同的上一级行政处罚机关指定管辖。
监督管辖	工业和信息化部依职权指导监督工业和信息化领域数据安全违法行为管辖工作。存在下列情况之一的，可以由工业和信息化部指定管辖： （一）数据安全违法行为情节严重的；（二）省级地方行政处罚机关对管辖发生争议，协商不成的；（三）数据安全违法行为或主体涉及不同省级地区、不同行业主管部门的；（四）法律、行政法规、部门规章等规定应当由工业和信息化部指定管辖的其他情形。
移送管辖	行政处罚机关发现案件不属于其管辖的，应当依法依规及时向有管辖权的行政处罚机关移送。 行政处罚机关发现违法行为涉嫌犯罪的，应当依法及时将案件移送司法机关，不得以行政处罚代替刑事处罚。

3、明确两大类行政处罚的情形

第一大类：以《数据安全法》为基准，提出不履行数据安全保护义务、向境外非法提供数据、不配合监管违法行为触发条件

（1）不履行数据安全保护义务的违法行为处罚条件

• 未定期梳理数据，识别重要数据和核心数据并形成本单位具体目录；

• 未建立数据全生命周期安全管理制度，未针对不同级别数据明确数据处理各环节的具体分级防护要求和操作规程；

• 未根据需要配备数据安全管理人员，统筹负责数据处理活动的安全监督管理，协助行业（领域）监管部门开展工作；

• 未合理确定数据处理活动的操作权限，严格实施人员权限管理；

• 未根据应对数据安全事件的需要，制定应急预案，并开展应急演练；

• 未定期对从业人员开展数据安全教育和培训；

• 未开展数据安全风险监测，及时排查安全隐患，采取必要的措施防范数据安全风险；

• 发现可能造成较大及以上数据安全事件的风险后，未按照风险信息报送与共享工作机制向所在地行业监管部门报告并及时处置；

• 数据安全事件发生后，未按照应急预案开展应急处置；

• 数据安全事件发生后，未按照规定向所在地行业监管部门报告；

• 数据安全事件发生后，未按照规定及时告知用户，并提供减轻危害措施；

• 未在数据全生命周期处理过程中，记录数据处理、权限管理、人员操作等日志。日志留存时间少于六个月；

• 重要数据和核心数据处理者未建立覆盖本单位相关部门的数据安全工作体系，未明确数据安全负责人和管理机构，未建立常态化沟通与协作机制；

• 重要数据和核心数据处理者未明确数据处理关键岗位和岗位职责，未要求关键岗位人员签署数据安全责任书；

• 重要数据和核心数据处理者未建立数据内部登记、审批等工作机制，未对重要数据和核心数据的处理活动进行严格管理并留存记录；

• 重要数据和核心数据处理者未按照有关规定做好重要数据和核心数据目录备案管理；

• 涉及重要数据和核心数据的安全事件，未第一时间向所在地行业监管部门报告，事件处置完成后未在规定期限内形成总结报告，每年未向本地区行业监管部门报告数据安全事件处置情况；

• 重要数据和核心数据处理者未按照规定对其数据处理活动每年至少开展一次风险评估，及时整改风险问题，并向有关主管部门报送风险评估报告；

• 重要数据和核心数据处理者报送的风险评估报告未包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等；

• 对于核心数据跨主体提供、转移、委托处理，未按照有关规定进行评估、保护、报批等；

• 其他不履行数据安全保护义务的。

（2）向境外非法提供数据的违法行为触发条件

• 工业和信息化领域中的关键信息基础设施运营者在中华人民共和国境内运营中收集和产生的重要数据和核心数据未在境内存储，或者因业务需要，确需向境外提供的，未按照有关规定进行数据出境安全评估；

• 其他工业和信息化领域数据处理者，在中华人民共和国境内收集和产生的重要数据和核心数据，未按照法律、行政法规等要求在境内存储，或者确需向境外提供的，未依法依规进行数据出境安全评估；

• 非经工业和信息化部批准，向外国工业、电信、无线电执法机构提供存储于中华人民共和国境内的工业和信息化领域数据；

• 其他向境外非法提供数据的。

（3）在各级行政处罚机关依法开展监督检查的过程中，不配合监管的违法行为触发条件

• 在有关行政处罚机关开展数据安全监督检查过程中，未对组织运作、技术系统、算法原理、数据处理程序等进行解释说明，未开放安全相关数据访问、提供必要技术支持的；

• 拒绝提供有关材料、信息的，或提供虚假材料、信息的，或者隐匿、销毁、转移证据的；

• 其他不履行配合数据安全监管义务的。

第二大类：综合涉及数据级别和数量、公共利益损害时间、直接经济损失、影响范围等因素，对数据安全违法行为的危害程度划分为“较轻”“较重”“严重”等情节。

危害程度	具体情节
后果较轻	•1000 万条以下一般数据被篡改、破坏、泄露或者非法获取、非法利用；（数据数量） •对公民、法人和组织合法权益、社会公共利益造成损害的持续时间较短，或直接经济损失在 1000 万元以内；（公共利益损害时间+直接经济损失） •影响范围小，影响对象为单个或少数企业，且不涉及跨地区的；（影响范围） •其他对行业发展、社会稳定和国家安全造成较轻后果的。（数据级别）
后果较重	•超过 1000 万条一般数据被篡改、破坏、泄露或者非法获取、非法利用，或者涉及重要数据、核心数据的；（数据数量、级别） •对公民、法人和组织合法权益、社会公共利益造成损害的持续时间较长，或直接经济损失超过 1000 万元且在 5000 万元以内的；（公共利益损害时间+直接经济损失） •影响范围较大，涉及多个企业，或涉及跨地区的；（影响范围） •其他对行业发展、社会稳定和国家安全造成较重后果的。
后果严重	•超过 1 亿条一般数据被篡改、破坏、泄露或者非法获取、非法利用，或者涉及 2 个以上数据处理者的重要数据、核心数据的；（数据类型、级别） •对公民、法人和组织合法权益、社会公共利益造成损害的持续时间长，或直接经济损失超过 5000 万元的；（公共利益损害时间+直接经济损失） •影响范围涉及多个行业、地区的；（影响范围） •其他对行业发展、社会稳定和国家安全造成严重后果的。

此外，《裁量指引》还明确了行政处罚裁量权适用规则，包括明确行政处罚实施流程、依据和综合裁量原则；规定不予处罚、从轻或减轻处罚、从重处罚的适用情形；从处罚种类、幅度两方面明确不予处罚、减轻处罚、从轻处罚、从重处罚的具体内容。

总结

《裁量指引》衔接和细化了《数据安全法》相关罚责规定，使行政处罚机关实施行政处罚有了具体依据。在监管形势不断趋严的情形下，企业务必做好数据安全合规工作，以避免因合规问题遭到行政处罚。

首先，《裁量指引》明确了不履行数据安全保护义务的违法行为处罚条件，主要涉及数据资产梳理、数据分类分级、数据安全管理制度、数据安全人员、数据安全教育培训、数据安全风险监测、数据安全事件风险信息报送等方面。同时针对重要数据和核心数据的处理者明确要建立数据安全工作体系，明确职责与分工，至少每年开展一次风险评估等。为避免因违反数据安全保护义务而触发行政处罚，企业应当严格履行数据安全保护义务。

针对上述合规要求，亿赛通凭借自身在数据安全领域多年的实践经验，构建了数据安全咨询服务体系，推出了基于用户业务需求的咨询规划、评估服务及运营服务等全流程服务。通过数据资产盘点、分类分级、组织建设、制度建设、人员能力培养、数据安全风险评估、数据安全检查、数据安全培训等服务项，可以帮助组织更好地应对数据安全建设和管理中的问题，全方位夯实数据安全保障能力，打造全面的数据安全管理运营体系。

其次，《裁量指引》明确了向境外非法提供数据的违法行为触发条件，涉及数据出境安全评估。

针对上述合规要求，亿赛通深入研究相关政策法规文件精神，能够为相关机构提供数据出境合规咨询服务，通过建立出境合规管理机制、数据出境业务分析、拟出境数据分类分级、数据出境安全合规评估、出境方数据安全能力论证、数据出境合规整改、境外方数据安全能力论证、编制数据出境安全合规评估报告、出境行为和风险持续监测九个步骤，帮助相关企业落实数据出境监管要求，掌控敏感数据流向，完善数据安全体系化能力，从而最终实现数据资产的放心流转，加强关联主体间的信息共享，保障出境业务的高效流通。

首席数据官：驱动组织变革的领导者

数字经济时代，数据被认为是企业的核心资产之一。随着数据量的不断增长，许多组织正在寻求将数据转化为商业价值的方法。首席数据官 (CDO) 作为企业中的重要角色，负责领导和管理数据战略和数据治理，以确保组织能够有效地利用数据。

首席数据官是企业中负责管理和指导数据管理和分析的领导者。他们的职责包括制定和实施数据战略，确保数据的可用性、准确性和可靠性，以及推动数据驱动的决策制定。CDO 通常拥有广泛的业务知识和技术背景，能够将数据转化为商业洞察力，并利用这些洞察力来推动组织变革。

首席数据官在组织中扮演着至关重要的角色。他们通过制定和实施数据战略，推动数据驱动的决策制定，帮助组织实现商业价值。CDO 还需要建立和维护与各个部门的合作关系，以确保数据的准确性和可靠性。他们的存在使得组织能够更好地理解和满足客户需求，提高生产效率，降低成本，并最终实现商业成功。

随着数据的不断增长和技术的发展，首席数据官的角色将会变得更加重要。未来，CDO 将需要更加关注数据的实时性和准确性，以便更好地支持组织的业务需求。他们还需要更加关注数据的安全性和合规性，以遵守不断变化的法规和标准。此外，CDO 还需要与更多的利益相关者合作，包括客户和供应商，以实现更广泛的商业价值。

此前，北京政府机关发文通知，将全面推进首席数据官制度，工作方案鼓励各区级政府在选取有条件的下级单位开展试点工作，积极鼓励各类企业设立首席数据官。并且市场监督总局认研中心提出要加强 CDO 高质量体系建设；加快企业首席数据官制度的普及应用，用各方力量开展首席数据官人才的评价和培养，邀请业内众多顶级专家学者制定科学合理的首席数据官培训课程体系，开展涵盖数据安全相关法律法规、隐私保护相关合规、数据安全评估实施、数据安全策略、数据安全技术、数据安全咨询实践等内容，充分讲解数智时代数据安全的重要性，加快培养 CDO，通过这类人才充分激活数据要素价值以确保企业的竞争力。

总之，首席数据官是组织中非常重要的领导者。他们通过制定和实施数据战略，推动数据驱动的决策制定，帮助组织实现商业价值。随着数据的不断增长和技术的发展，CDO 的角色将会变得更加重要。未来，亿赛通将更加关注数据的实时性、准确性和安全性，以便更好地支持市场监督总局认研中心的业务需求。

首席数据官培训咨询热线如下：卜老师　18210488262

关于亿赛通培训学院

亿赛通数据安全培训学院自成立以来，不断深挖全球大数据和数据安全相关政策，分析企业需求人才需具备的能力素养与技术能力，以培养数据安全专家人才培养为目标，扩展课程研发方向，并建设 60 余人的高级讲师师资团队。学院目前主要开展两大培训工作分别是人才认证方向及企业数据安全意识培训。

人才认证方向主要包括：1）工信部人才交流中心开展的“亿赛通数据安全专业人才认证 (EDSP) ”目前已开展 10 期，共培养数据安全治理人才 400 余人。2）与工业和信息化部教育、中国计算机行业协会数据安全专业委员会开展数据安全人才培养《数据安全评估师》、《数据安全工程师》两门课程，已开展 5 期，共培养优秀数据安全评估人才 235 人。3）与市场监督总局认研中心合作的《首席数据官》、《商业秘密保护工程师》、《首席安全咨询师》三门课程已经录制上线，即将服务于市场广大数据安全需求客户群体。

企业数据安全意识培训主要服务于：企业各单位人员数据安全意识方向的培训，目前服务于行业包括政企、能源、互联网、教育等，曾为百余家客户群体提供过服务，线上线下培训人数达 5000 余人。

人勤春来早 学习正当时 | 亿赛通《首席数据官》专业培训正式上线

为强化数据资源管理，挖掘数据资源价值，保障数据安全，助力“数字中国”建设，国家市场监督管理总局认证认可技术研究中心 (以下简称“市场监管总局认研中心”) 联合国家发展和改革委员会国际合作中心 (以下简称“国家发展改革委国际合作中心”) 共同开展了首席数据官人员能力验证工作，推动数据基础设施建设，为数字经济前沿产业持续提供坚实的人才保障。

首席数据官人员能力验证是指按照相关规定或标准，根据考核验证规则，采取专业知识学习、能力素质考核、结果分析比对及验证等方式，对首席数据官的专业能力进行验证的合格评定过程。市场监管总局认研中心邀请业内诸如亿赛通的众多顶级专家学者制定科学合理的首席数据官培训课程体系，开展涵盖数据安全相关法律法规、隐私保护相关合规、数据安全评估实施、数据安全策略、数据安全技术、数据安全咨询实践等内容。

1、报名条件

① 从事于数据安全、网络安全行业从业者、数据信息使用者等从事相关岗位及有意从事相关岗位的工作人员；

② 年满 18 周岁，有一定学习基础的学员。

2、学习方式

平台录播视频学习，凭《学时证明》可以申请参加能力验证考试，并获取《人员能力验证证书》。

3、考试时间及报名取证

①人员能力验证工作原则上在每个季度最后一周的周六为“人员能力验证日”，具体验证时间以官网通知为准，每年共计安排 4 次考试；

②考试结束后成绩公布在 1 周左右公布查询方式。课程学习完，可在平台个人中心查询学时电子版证明，纸质版“人员能力验证证书”证书会在考试后 2 个月拿证。

4、人员能力验证结果优势

① 市场监管总局认研中心是国家市场监督管理总局直属正司级事业单位，具备着从业人员能力提升、监管辅助和认证认可的相关职责；

② 人员能力验证属于从业人员能力提升考核验证的全新模式，目前市场处于空白期，发展前景向好，市场潜力大；

③ 通过人员能力验证的培养培训和验证结果，学员可以清晰掌握目前的自身能力水平处于行业哪个位置，也可以提高在某行业的自我认知。有助于学员提升自我专业能力和水平，了解到行业发展趋势和方向，协助自身做好职业规划；

④ 人员能力验证项目采取了 " 考培 " 分离的模式，相关开展通知由市场监管总局认研中心统一印发通知文件，公示培养培训及能力验证费用。同时只有在市场监管总局认研中心人员能力验证综合服务平台公示的合作单位才具备招生资格，规避了层层代理带来的各类市场乱象；

⑤ 国家市场监管总局认研中心发布的人员能力验证管理办法中指出：应积极协调政府部门、行业协会、用人单位等，鼓励企业采信人员。随着人员能力验证结果的不断被采信，持证人将持续获得更多赋能，对其本人求职、晋升等提供更大帮助。

课程联系人：卜老师 18210488262

亿说安全之揭秘数据安全的关键一环

今年，数字化和智能化的发展依旧迅猛，ChatGPT、大语言模型不绝于耳，创新技术甚嚣尘上，这些新技术被广泛应用于企业服务之中，它们在给企业带来新机遇的同时，也让企业、社会面临着巨大的安全风险。与此同时，用户对于产品和服务的要求越来越高，数据安全服务已成为目前国内安全市场增速最快的赛道。

数据安全服务践行着从经验主义—实用主义—创新主义的演进过程。具体表现为通用安全服务（如：安全运营、安全咨询、安全培训等）到细化落地的行业安全服务（如：等保咨询、商用密码评估等）。国家明确规定要以新安全格局保障新发展格局，作为大安全观下细分的数据安全服务正踩在时代的节点上。通过某咨询机构数据显示，在通用安全服务细分市场中，安全运营占比达到 52%。安全服务处于迭代演进阶段，整体呈现往前推进态势。

作为数据安全领域极具用户信服力的厂商，亿赛通认为数据安全服务是基于数据安全合规要求、专业知识和实践经验，通过数据安全理论和实践的积累，由服务人员利用专业知识，辅以数据安全工具，帮助组织分析现有问题、找到应对方案、实现方案落地的过程。在了解客户需求的过程中可以发现，客户方满足合规要求、体系化提升自身数据安全能力的需求迫切，对合规要求理解、数据安全管理工作重视程度、数据资产和安全现状摸排存在一定问题。

基于上述情况，亿赛通提出的“分放管服”数据安全建设理念，即可帮助客户从整体统一和业务流转的视角，在对数据敏感程度、人员职责、访问权限进行精细化分析的基础上，把握“放”和“管”的平衡，重视产品实施和运营保障服务，从而帮助用户夯实数据安全能力。同时，亿赛通认为数据安全服务还必须具备“可落地性”，要善于联动数据安全技术和工具，为用户提供可闭环的数据安全解决方案，实现数据安全状态的可持续。

公司以产品 + 服务的模式，通过专业的安全咨询团队、优质且完善的安全服务，深入客户业务，贴近客户需求，快速安全分析，全面深度分类。让客户在专注业务增长的同时保持严格的安全策略，深度赋能企业的管理运营，增强客户粘性，发挥并实现安全产品能效的最大化。此前，亿赛通已经连续两年入选数据安全服务前五家企业名单，完成客户重大项目（如：文旅部、中外运等），参与多项国标、行 / 团标编写、制定工作，积累了丰富的实践经验，在业界收获了良好口碑。

作为数字化转型领域的重要参与者与推动者，亿赛通将继续站在数据安全的前沿，坚持以建设数字中国的重要思想为指导，加大技术研发力度，不断提升产品、解决方案及安全服务的“硬实力”，深度赋能多行业的安全生态，帮助更多企业更快实现数字化转型目标，为重要信息系统运营者提供有力支撑和坚实保障，为促进数据安全服务行业健康有序发展贡献积极力量。

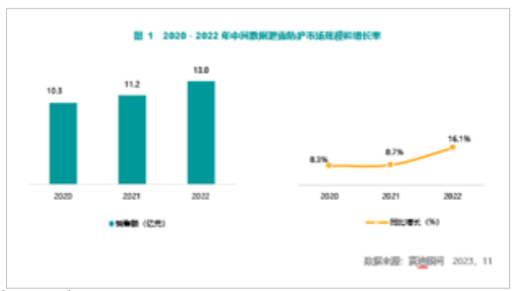
市场洞察：数据泄露防护重要性凸显，市场竞争激烈

随着数字经济发展的不断推进，数据安全已成为党和国家重点关注的问题。从安全发展的角度来看，数据安全是数字经济建设中的底座，是护航数字经济稳定发展、数据要素价值释放的基础保障。数据安全的防护目标是保护数据的机密性、完整性和可用性，未经授权的访问、篡改或破坏数据。

近年来，数据泄露依然是全球发布最频繁的安全事件，涉及制造业、教育、通信和政府等多个领域，对个人隐私和企业安全都造成了严重影响。因此，无论是在公共部门还是在商业领域，都需要加强数据加密、访问控制、员工培训和漏洞修复来保护敏感信息和减少数据泄露风险。

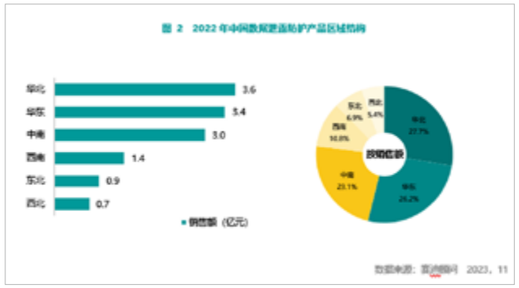
01、整体行业分析

我国《数据安全法》和《个人信息保护法》已经颁布施行两周年，数据安全标准化工作加速推进，数据安全审查与监管措施逐步完善，数据安全技术发展迅速，数据安全市场需求不断增长。中国数据泄露防护产品作为数据安全重点产品之一，2022 年市场规模达 13.0 亿元，增长率为 16.1%。



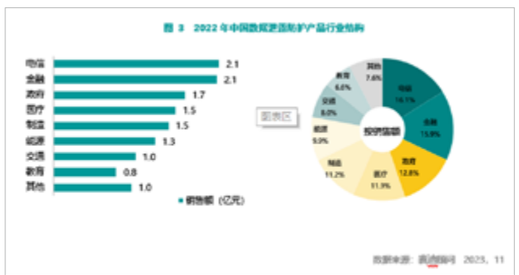
02、区域结构细分

从区域结构来看，华北、华东、中南地区对数据泄露防护产品的需求较大，保持着较高的市场规模。西南、东北、西北近几年对数据安全的重视度逐年提升，数据泄露防护产品的需求增速较快。

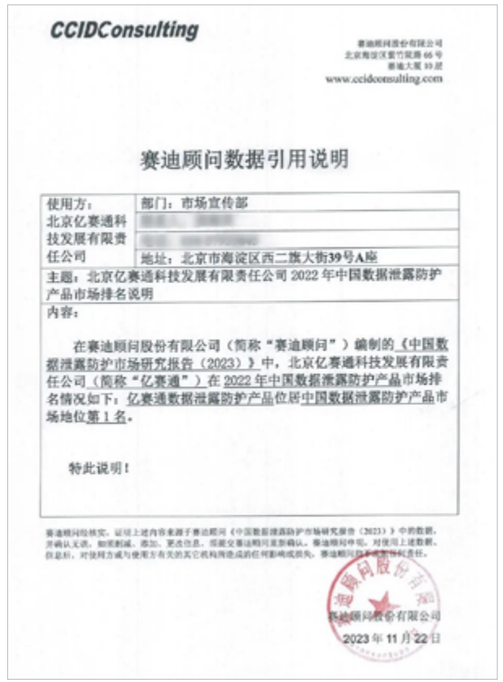


03、行业结构细分

从行业结构可以看出，电信、金融行业一直以来对数据泄露防护产品保持较高需求，而政府、医疗等关键信息基础设施行业系统中也包含了大量的个人隐私信息与敏感数据，网络与数据安全相关的投入逐年增大，数据泄露防护产品需求也在不断显现。



在大环境整体向好的趋势下，数据安全政策的密集发布，国内布局数据泄露防护产品的厂家也越来越多，市场竞争较为激烈。2022 年，亿赛通的数据泄露防护产品在市场中占有率排名第一。


CCIDConsulting

赛迪顾问股份有限公司
北京海淀区紫竹院路 66 号
赛迪大厦 10 层
www.ccidconsulting.com

赛迪顾问数据引用说明

使用方：北京亿赛通科技发展有限责任公司	部门：市场宣传部 [redacted] [redacted] 地址：北京市海淀区西二旗大街39号A座

主题：北京亿赛通科技发展有限责任公司 2022 年中国数据泄露防护产品市场排名说明

内容：

在赛迪顾问股份有限公司（简称“赛迪顾问”）编制的《中国数据泄露防护市场研究报告（2023）》中，北京亿赛通科技发展有限责任公司（简称“亿赛通”）在 2022 年中国数据泄露防护产品市场排名情况如下：亿赛通数据泄露防护产品位居中国数据泄露防护产品市场地位第 1 名。

特此说明！

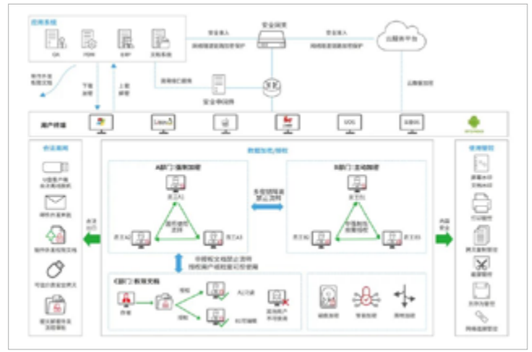
赛迪顾问股份有限公司
2023 年 11 月 22 日

亿赛通的数据防泄露产品主要包括终端数据泄露防护系统（DLP）、网络数据泄露防护系统（NETDLP）、邮件数据泄露防护系统（MailDLP）及存储扫描数据泄露防护系统（ScanDLP）。

1. DLP 基于内容识别技术，对企业设计图纸、源代码、合同文本、财务报表等敏感数据进行安全加密，防止通过邮件、聊天工具、网盘、U 盘拷贝、打印等途径泄露数据，对用户泄密行为进行记录、告警、阻断，并对用户行为进行审计；

2. NETDLP 是基于网络协议分析、敏感信息识别、网络行为控制于一体的安全防护系统；

3. MailDLP 是基于邮件数据安全防护和敏感识别、数据防泄漏的安全防护系统，可以实现邮件数据分析、敏感数据识别审计、邮件数据脱敏处理、邮件审批管理、阻断策略响应访问控制等；



4. ScanDLP 是基于网络共享协议分析与控制技术的安全防护系统，实现了网络共享数据的扫描采集、敏感数据识别审计、数据资产扫描发现和分析。

近年来，业内提倡根据数据全生命周期进行安全防护，亿赛通将各个孤立的安全系统进行资源整合，形成集资产管理、策略运营、智能分析、响应处置、态势感知等功能为一体的数据安全运营管理平台。采用大数据技术架构，通过采集和分析来自于终端、网络、存储的各类安全设备日志，以此掌握全网数据安全态势情况。同时可对数据安全能力进行集中化、标准化、规范化、常态化、场景化管理，全面掌握全域敏感数据资产情况，有效监控敏感数据流转路径和动态流向，通过集中的数据安全策略管理，实现数据分布、流转、访问过程中的风险识别与防护。

未来，随着数据量的爆发式增长，如何发挥出数据要素的价值是推动未来数字经济发展的关键，而数据安全问题作为数据价值发挥的前提逐步被政企用户所重视，将成为优先考虑的重点问题。赛迪顾问预计，未来三年，我国的数据泄露防护市场复合增长率将达到 15.2%，到 2025 年市场规模将达到 19.9 亿元。

亿赛通智能化数据安全治理体系赋能生物医药企业数字化安全管理

生物医药作为21世纪优先发展的战略性产业，各国政府高度重视生物产业发展。近年来，各国围绕生物技术制高点占据，加强顶层设计，相继发布了加快医疗生物技术创新突破的政策举措。

生物医药产业数字化正在蓬勃兴起，新药研发数字化、AI 辅助新药研发、临床研究管理数字化、真实世界数据应用、数字化生产、供应链数字化管理、电子处方流转、医药数字化营销、数字化医生服务、数字化患者用药服务等领域都得到了较快发展。

对国民而言，生物医疗研究中包含大量的个人敏感信息，例如通过几十个统计学上独立的基因点位，很大程度上就可以确定一个个体，售价最高可达个人身份信息的六倍。据某调研机构数据显示，生物医药产业 2022 年数据泄露成本已挤入前十。

亿赛通认为生物医药产业数据共享流通频繁，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，生物医药产业普遍存在以下风险：

伴随着生物医药的快速发展，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、药品信息等等。据 IDC 预测，到 2025 年人类生产和复制的总数据量将达万亿 GB。

企业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。

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。

基于生物医药数据的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。

据亿赛通分析，生物医药产业数据安全的核心需求主要有临床研究数据加密需求、内部人员权限管控需求、敏感数据外发管控需求、敏感数据溯源审计需求。

针对上述需求，亿赛通提出了数据安全治理智能化技术体系，帮助生物医药企业通过智能化分类分级工具快速准确地完成组织的业务梳理和数据梳理，并形成规范化的策略库，即主体、客体及两者之间的策略，同时将上述数据根据积累的知识库智能化衔接到技术平台，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，实现了对组织数据的智能识别、智能防护、智能监测、智能运营，构建可视、可控、可管、可溯的覆盖数据全生命周期的综合解决方案。

亿赛通基于多年在数据安全领域的专业能力，已形成数据安全治理咨询规划、数据安全产品技术、数据安全综合运营在内的完整的产品方案及服务，帮助生物医药产业筑牢数据安全基座，护航数字化转型发展！

珠海丽珠试剂股份有限公司

客户简介

珠海丽珠试剂股份有限公司（简称“丽珠试剂”）创立于 1989 年，是上市公司丽珠医药集团（股票代码：SZ000513）旗下第一家高科技子公司，专业从事体外诊断试剂及配套设备的研发、生产和营销。丽珠试剂作为坚守耕耘 30 余年的体外诊断试剂生产企业，膺获“国家高新技术企业”，“广东省省级企业技术中心”，“广东省丽珠体外诊断工程技术中心”，“广东省创新型企业”，“珠海市专精特新企业”等诸多殊荣，获批设立“博士后科研工作站”，“广东省博士工作站”及“广东省博士后创新实践基地”。

需求背景

伴随着医疗行业信息技术的快速发展，丽珠试剂业务得到快速发展，版图扩增明显，管理及盈利能力不断提升，综合化经营的步伐不断加快。作为丽珠集团旗下的高科技子公司，数据安全已经成为丽珠试剂业务发展基础和前提。为了加强企业内部管理，提高运营效率，防范数据安全风险，构建一套成熟、稳定、易用、可落地的数据安全防护体系，以增强丽珠试剂数据安全防护能力是企业战略发展的必然选择。

解决方案

亿赛通帮助丽珠试剂实现终端数据安全管控：

资产管理：一种能够自动化快速采集终端硬件资产和软件资产，方便资产盘点及安全运维管理。

介质管控：支持介质在线注册申请，由管理员进行统一注册申请审批；支持注册类型包含：签名介质、专用介质。支持介质接入权限控制，只有经过授权的介质才能在内网使用，未授权的介质无法在内网使用。内网专用介质只能在内网使用，在外网无法使用。防止因非法使用介质造成数据泄密。

软件分发：通过管理平台能够给客户端下发应用软件安装介质，支持静默和非静默安装，支持 exe、msi 类型的软件包。

应用管控：管理员可通过平台下发策略，控制终端应用程序的使用，包括：允许运行、禁止运行、强制启动、强制卸载。

端口管理：可以对计算机端口与存储设备进行安全控制，包括对 U 盘、移动硬盘、各类存储卡、同步软件、软驱、串口、并口、调制解调器、打印机、1394、红外、蓝牙、无线等的安全控制，有效规避设备端口泄密隐患。

项目成果

亿赛通为丽珠试剂提供完善的新一代电子文档安全解决方案，有效地防止员工的不安全行为引入风险，保障了各个环节数据的安全运行，避免了公司敏感数据遭窃的可能，提高数据安全的智能化管理，为丽珠试剂打造了一个良好的信息安全办公环境。