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

09 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

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

《亿赛通九月刊》双节同庆，祝网安行业兴盛蓬勃

数字技术多层次的影响着世界经济格局，数据逐渐成为各国新一轮国际政治博弈中争夺的重要资源，加强数据跨境流动管理成为不少国家的共识。面对日益庞大的数字经济规模，保障中国数据跨境安全，维护个人、国家、社会利益的呼声日益强烈。专家认为，要强化网络安全、数据安全和个人信息保护，需要进一步加强中国跨境数据流动监管。9 月的网络安全宣传周，数据跨境成为企事业单位重点关注的内容之一，跨境数据的商业价值进一步凸显。《亿赛通九月刊》就本月业内大事记进行深入分析，快和我们一起了解风起云涌的九月安全圈。

亿赛通全体员工值此双节到来之际，祝愿伟大的祖国神州奋起，繁荣昌盛，国富民强，同祝网安行业创新、奋进、兴盛蓬勃！

刊首语 PREFACE

国内

1、男艺人杨迪电话被“打爆”！保护个人信息安全有多难?

摘要：9 月 4 日下午，男艺人杨迪发文称，自己的个人信息被泄露，由于频繁接到骚扰电话，迫不得已换了手机号码。有网友表示，现如今更换手机号是一件非常麻烦的事情，许多绑定了手机号的社交软件都要一一解绑，随后杨迪也在该评论区下回复：“巨巨巨巨巨麻烦！”

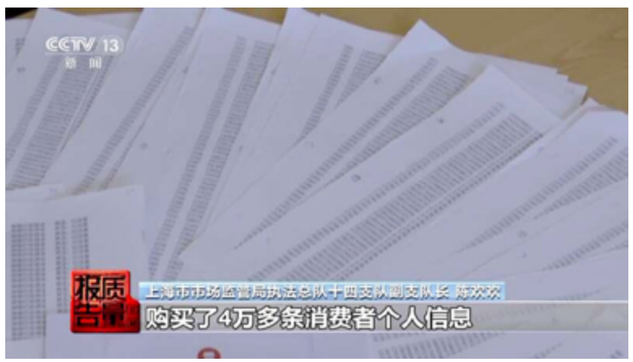
2、近两万条培训学员信息泄露！厦门网警迅速出击 “黑客”获刑!

摘要：今年 2 月底，厦门市某教育培训机构的多名学员和员工接到诈骗电话，存在公民个人信息泄露的情况。厦门市公安局网安支队牵头思明公安分局，迅速介入调查，快速锁定并抓获涉嫌侵犯公民个人信息的犯罪嫌疑人朱某某；同时启动“一案双查”，对不履行数据安全保护义务的教育培训机构及其主管人员处以行政处罚。近期，犯罪嫌疑人朱某某被思明区人民法院依法判处有期徒刑并处罚金，没收全部非法所得。

3、公民个人信息遭境外披露兜售，上海市一政务信息系统技术服务公司被行政处罚

摘要：据“网信上海”公众号消息，前期，据有关部门在跟踪调查中发现，上海市某政府信息系统技术承包商违规将政务数据置于互联网进行测试期间，相关存储端存在高危漏洞，导致大量公民数据泄露，以致成为境外不法分子窃取政务数据的“供应链”入口，2022 年 7 月，相关公民个人信息在境外黑客论坛被披露兜售。针对问题线索，上海市网信办联合有关部门对涉事公司未严格履行数据安全保护义务的违法行为，开展现场网络安全检查。

4、个人信息是如何泄露并被利用的？揭开贷款中介背后的黑灰产业链



摘要：上海市市场监管局执法总队执法人员对贷款中介行业的多家公司初步调查后，锁定了一家贷款中介进行突击执法检查，当场在这家公司负责人的手机和工作电脑中发现大量购买来的消费者个人信息。这个公司的负责人以 2888 块钱的价格购买了 4 万多条消费者个人信息。购买的信息当中包含消费者的姓名、电话、工作单位、家庭住址等一些非常隐私的信息。

5、推行隐私运单 构筑信息安全港

摘要：近日，国家邮政局、中央网信办、公安部三部门就联合召开推进会，持续深入推广应用隐私运单，全力保障邮政快递领域信息安全。一张小小的快递单，究竟能泄露多少个人信息？有调查显示，如果通过快递单上显示的姓名、手机号、地址，基本可以还原出 90% 的个人信息。显然，由此掌握了个人信息的一方，既能转手售出非法牟利，也能满足自身需求。个人信息遭泄露后，轻则引来诸多推销、中介、贷款等行业的骚扰，重则通过手机号有可能查到绑定的微信、支付宝等账号，甚至还能了解到你的兴趣爱好、最近关注等，容易导致人身、财产安全受到危害。

6、拧紧数据“安全阀”！ 德州市自然资源局开展数据异地灾备工作

摘要：9 月 14 日至 15 日，德州市自然资源局组织相关人员前往山东省自然资源数据异地灾备中心（栖霞）开展数据异地灾备工作。据了解，本次数据异地灾备工作包括不动产登记、电子档案、国土空间基础信息平台等重要数据进行备份，旨在更好地落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》等法律关于数据安全管理的规定和《数字强省建设 2023 年工作要点》中关于定期组织开展数据灾备的相关要求，进一步提升德州市自然资源信息化系统数据安全系数，避免因自然灾害或突发事件导致数据丢失。

7、12306 平台发声，警示旅客保护个人信息安全

摘要：据中国铁路官微消息，铁路 12306 从未授权任何第三方平台发售火车票，也不可能给第三方平台所谓的“优先购票权”。第三方平台在旅客朋友购票过程中会保留用户信息，不仅有附加费、加速包、捆绑销售服务等陷阱，还可能存在个人信息泄露风险。

8、利用 AI 散布谣言“杀猪盘”延伸黑链条…… 网络安全防火墙如何筑更牢？

摘要：近年来，各地各部门不断加大打击治理电信网络诈骗违法犯罪力度，有效遏制了案件快速上升势头。然而，仍有犯罪分子铤而走险，不断翻新手段实施诈骗。就以杀猪盘为例，随着技术的更新换代，网络诈骗团伙一方面在境外多地设立多个电信网络诈骗窝点，配备电脑、手机、聊天软件账号等作案工具；另一方面，组建国内洗钱人员、技术维护团队、国内推广引流团队、窝点主管、窝点作案人员，搭建虚假投资理财返利等 App，利用国内公众号或网站推广引流，最终吸引潜在受害者下载指定 App 实施“杀猪盘”诈骗活动。

9、知网（CNKI）被罚 5000 万元!

摘要：根据网络安全审查结论及发现的问题和移送的线索，国家互联网信息办公室依法对知网（CNKI）涉嫌违法处理个人信息行为进行立案调查。经查实，知网（CNKI）主要运营主体为同方知网（北京）技术有限公司、同方知网数字出版技术股份有限公司、《中国学术期刊（光盘版）》电子杂志社有限公司三家公司，其运营的手机知网、知网阅读等 14 款 App 存在违反必要原则收集个人信息、未经同意收集个人信息、未公开或未明示收集使用规则、未提供账号注销功能、在用户注销账号后未及时删除用户个人信息等违法行为。对知网（CNKI）依法作出网络安全审查相关行政处罚的决定，责令停止违法处理个人信息行为，并处人民币 5000 万元罚款。

10、长租公寓住户因拒绝 " 刷脸 ", 进出成难题？上海检察机关出手！

摘要: 因为拒绝“刷脸”，进出公寓对杨女士（化名）来说竟成了件难事。她希望公寓给予门禁卡或其他方式，却遭到拒绝。“为什么我一定要‘刷脸’才能进公寓？”“任何公共场所不得强制将‘人脸识别’作为唯一的门禁出入方式，这不仅侵害了不特定人的个人信息权益，同样损害了个人信息保护领域的社会公共利益。”近日，上海市虹口区人民检察院以检察建议促行政监管，监督公寓整改，保护公民“人脸”信息安全。

国外

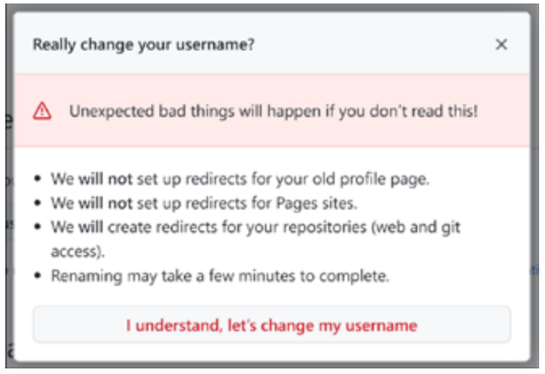
1、马自达服务器被 " 黑 " 或有超 10 万人信息被泄露

摘要：日本汽车制造商马自达发布声明称，最近发现服务器被外部攻击者非法访问，公司管理的部分个人信息可能已泄露。该公司强调，被非法访问的服务器上没有存储任何客户个人信息，这部分信息也没有泄露。对于此次事件可能给相关人员带来的不便和担忧，公司深表歉意。马自达表示，根据外部安全专家的调查结果，确定这次未经授权的访问是利用了公司应用服务器中的一个漏洞。可能泄漏的个人信息包括本公司及集团公司员工、分包商员工、业务合作伙伴部分信息，涉及姓名、电子邮件地址、部门及职务、电话号码等。

2、欧央行“有内鬼”，泄露消息！行长拉加德出狠招：会前没收委员们手机

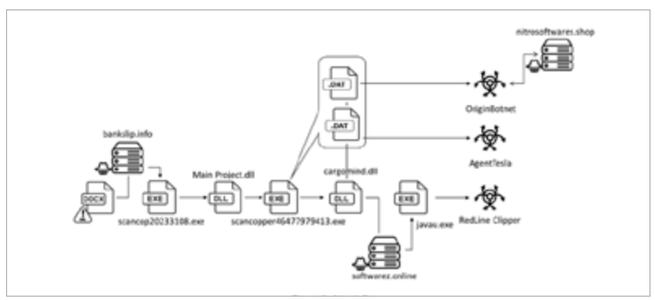
摘要：据路透社报导，欧洲央行行长拉加德在会议上没收了其他政策制定者们的手机，并斥责他们在政策决定前泄露了重要信息。这一史无前例的举措是拉加德为阻止理事会信息泄露而采取的最大胆的一步，这一问题一直困扰着她，让她常被拿来与前任行长德拉吉（Mario Draghi）相比较。知情人士称，周三，也就是央行会议的第一天，欧洲央行管理委员会的 26 名成员被告知交出手机，因为即将任命 Claudia Buch 为欧洲央行单一监事委员会主席。直到会议结束并对外正式宣布此人事任命消息后，委员们才拿回手机。

3、持续性威胁：新漏洞将数千个 GitHub 代码库和数百万用户置于险境



摘要： 近日发现的一个新漏洞让攻击者可以利用 GitHub 的代码库创建和用户名重命名操作中的竞态条件。该技术可用于执行代码库劫持攻击（劫持流行的代码库以分发恶意代码）。这一发现标志着已第四次发现了一种独特的方法，有可能绕过 GitHub 的“流行代码库命名空间退役”机制。这个漏洞已报告给了 GitHub，已得到修复。

4、OriginBotnet 通过恶意 Word 文档传播！

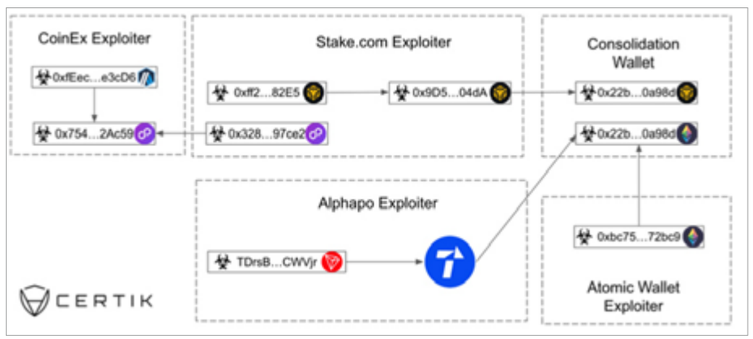


摘要：FortiGuard 实验室捕获了一份 Word 文档，其中包含一个恶意 URL，旨在引诱受害者下载恶意软件加载程序。该加载程序采用二进制填充逃避策略，添加空字节以将文件大小增加到 400MB。该加载程序的有效负载包括用于密钥记录和密码恢复的 OriginBotnet，用于加密货币盗窃的 RedLine Clipper 和用于获取敏感信息的 AgentTesla。

5、MGM 国际酒店集团遭到网络攻击：黑客炫耀中断了四天的服务

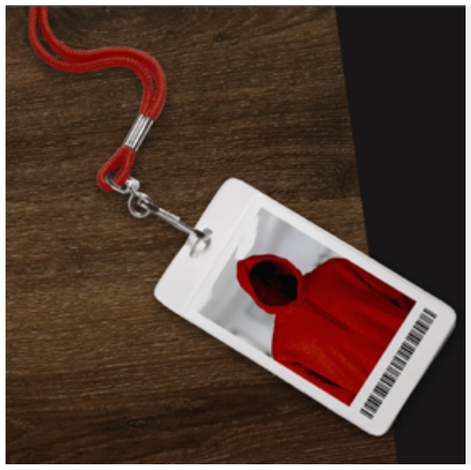
摘要：此次网络攻击迫使美高梅酒店集团（MGM Resorts）关闭了旗下所有的酒店系统。在周日大部分时间里，美高梅的大部分内部网络都处于关闭状态，而这正值其拉斯维加斯大道上的酒店和赌场（如 Bellagio、Aria 和 Cosmopolitan）盛大开业的前一天晚。由于此次技术故障，公司旗下酒店和赌场的自动取款机也出现了大面积的中断，客人们也反应说他们的客房数字钥匙卡和电子支付系统出现了很多的问题。

6、朝鲜黑客组织 Lazarus 成为 Web3 领域主要安全威胁



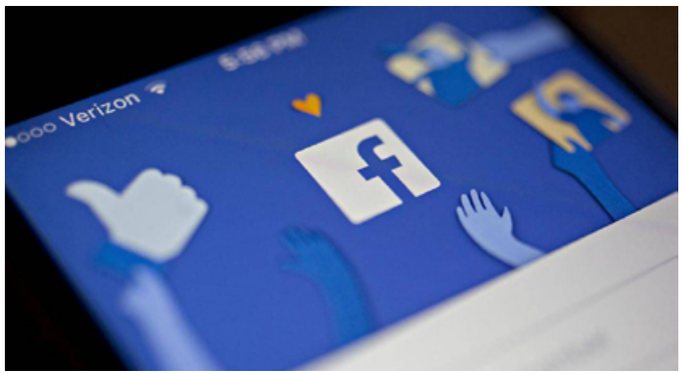
摘要：2023 年朝鲜黑客组织 Lazarus 已窃取超过 3.1 亿美元的数字货币。近年来，朝鲜黑客组织 Lazarus 已成为影响 Web 3 社区最严重的 APT 组织。2022 年，Lazarus 组织造成了至少 7.5 亿美元的损失，占 2022 年加密货币领域被窃总额的 20%。CertiK 分析了 2023 年五起主要的加密货币攻击事件，包括 Atomic Wallet、Alphapo、CoinsPaid、Stake.com 和 CoinEx，造成了 2.913 亿美元的损失。

7、从谷歌到英伟达，科技巨头纷纷招募红队黑客破解自己的 AI 模型



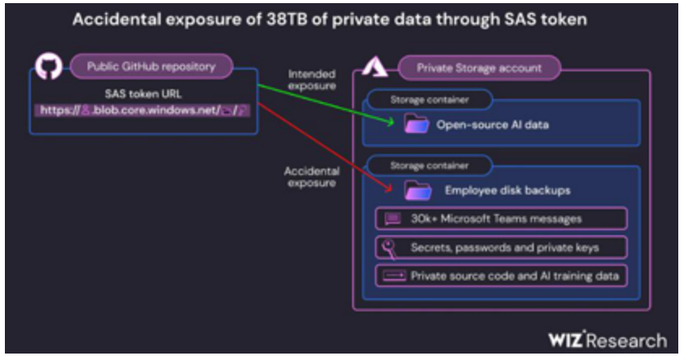
摘要：为了保护 AI 系统避免被人利用，红队黑客站在攻击者的角度思考，对 AI 系统做改动，以发现该技术固有的盲点和风险，以便可以消除风险。随着科技巨头们竞相构建和发布生成式 AI 工具，它们的内部 AI 红队在确保模型供大众安全使用方面起到了越来越重要的作用。比如说，谷歌在今年早些时候设立了一支独立的 AI 红队，8 月份，OpenAI 的 GPT3.5、Meta 的 Llama 2 和谷歌的 LaMDA 等众多流行模型的开发人员参加了一场由白宫支持的活动，旨在让外部黑客有机会破解 AI 系统。

8、越南网络犯罪分子利用恶意广告针对 Facebook 企业账户攻击



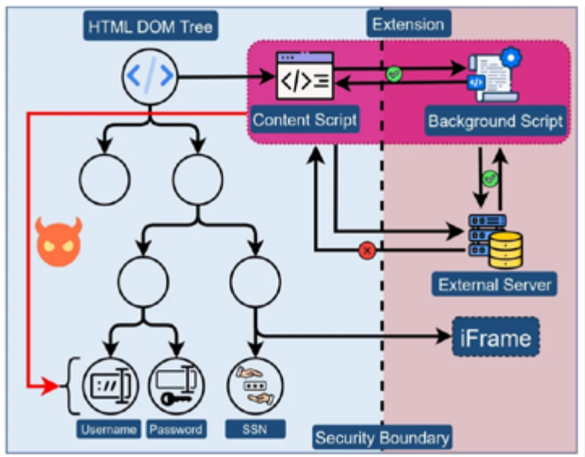
摘要：与越南网络犯罪生态系统有关的网络犯罪分子正在大量的利用社交媒体平台（包括 Meta 旗下的 Facebook）作为传播恶意软件的重要手段。据 WithSecure 的研究人员 Mohammad Kazem Hassan Nejad 称，恶意攻击者一直在利用大量欺骗性的广告针对受害者实施各种诈骗和恶意广告攻击。随着企业越来越多地利用社交媒体发布广告，这种策略使得攻击流程变得更加容易，这同时为攻击者提供了一种新型的攻击方式 -- 劫持企业账户。

9、微软 AI 38TB 数据泄露



摘要：近日，安全公司发布了关于微软人工智能研究部门员工意外泄露 38 TB 数据的研究报告。报告称微软员工在发布开源训练数据时，意外分享了一个包含有泄露的信息的错误配置的 Azure Blob 存储桶（storage bucket）的 URL，其中包含 38 TB 的人工智能训练数据，这些数据本身是用作迁移学习训练的。

10、Chrome 扩展可从网站窃取明文密码



摘要：研究人员发现谷歌、Cloudflare 等知名网站的网页 HTML 源码中都以明文形式保存密码，恶意扩展可从中提取明文密码。威斯康星大学麦迪逊分校研究人员在 Chrome 应用商店上传了恶意扩展 PoC，成功从网站源码中窃取明文密码。

亿赛通亮相 2023 年网络安全宣传周电信日活动，共建数据安全，服务社会民生

9 月 13 日，2023 年国家网络安全宣传周“电信日”活动火热召开，“电信日”活动以“筑牢网络安全屏障 护航新型工业化”为主题，大力推动相关法规宣传，持续推进网络安全知识和技能普及，不断筑牢新型工业化的安全防护屏障，助力制造强国、网络强国、数字中国建设。

亿赛通有幸受邀参加该活动，以数据安全为切入口，全面展示企业在数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务等领域的研究进展，以及我司在电信行业的探索实践。亿赛通专家结合丰富的案例和详实的实践经验为参会领导、到场嘉宾分享了亿赛通在数据安全领域取得的经验及见解。

数据作为数字经济时代最核心、最具价值的生产要素，正在加速成为经济增长的新动力、新引擎，可以说数据正逐渐成为数字经济时代的“石油”。与此同时，客户需求呈现出多元化、个性化的发展趋势，这种个性化和多样化正是企业需要迫切关注的。每一家企业都应认真思考和研究，发挥自身优势，聚焦细分客户群体，为客户创造价值。

随着 5G、大数据、隐私计算等新技术的全面覆盖，电信行业在数字经济的飞速发展下产生了庞大的、多样化的数据。数据的采集、存储、处理的效率不断提高，也促使数据体量变化越来越大，其中包含着大量的敏感信息和用户个人信息，所以如何合理地利用这些数据的同时还能保护数据安全是我们面临的严重挑战。

此时，国家针对个人信息的分类分级和安全技术要求做了明确要求。针对电信行业也发布了《电信领域数据安全指南》、《基础电信企业信息安全责任管理办法 (试行)》、《电信网和互联网信息服务业务系统安全防护要求》等政策，对电信行业相关安全技术要求也做出了详细指引。

在亿赛通看来，电信行业用户需要符合国家信息安全相关标准，对组织、人员、制度整体性管理的建设，独立组织、明确职责、规范流程的可持续优化，全面地帮助通讯行业在庞大的体系管理中达到可持续发展。

我司在电信行业结合企业相关业务应用的运行现状建立数据安全体系，数据安全全生命周期技术防护策略配合标准化的管理制度及流程；可满足现有环境的数据分级安全管理又能保证业务的连续性。

在建设前期通过全面的资产发现方式、灵活的资产梳理规则、深入的资产质量分析，能够有效地帮助企业进行对数据资产的摸底和管理工作；改善传统方式下的资产梳理和管理模式，提高工作效率，保证资产梳理质量，实现资产权责分明；打破数据孤岛，提高获取效率，释放资产价值。以资产发现 - 资产梳理为核心，以资产可视 - 资产可管为目标，致力于提升企业对数据资产的整体管控能力和运维效率。

数据安全建设从来不是一蹴而就的，而需要长期不断进行管理和技术的调整优化。随着管理制度的不断完善，数据安全管控策略也要随之完善优化，通过数据安全工具的日志分析和趋势分析，有针对性地加强各部门安全建设，防控安全风险，也要进行各部门的自查和监督部门的结果性审计检查，同时要做好公司内的培训宣贯，规避常见办公安全风险，贯彻数据安全管理规定。

保障数据安全是电信行业的核心任务之一，全生命周期的数据安全防护是对数据的有效保护手段。用户采用安全、合规的方式方法，有助于企业厘清数据资产、确定数据重要性或敏感度，并针对性地采取适当、合理的管理措施和安全防护措施，形成一套科学、规范的数据资产管理与保护机制，从而在保证数据安全的基础上促进数据流通防护。

网络空间不是法外之地，需要我们增强网络安全意识，提升基本防范技能，亿赛通愿与您一起共建清朗文明的网络空间！

亿赛通荣登《中国经济导报》：提升创新能力 融入全球价值链

中华人民共和国国家发展和改革委员会主管

中国经济导报

CHINA ECONOMIC HERALD

穿透力才是影响力

2023.8.29 星期二 本期共8版 总第4211期

习近平在听取新疆维吾尔自治区党委和政府 新疆生产建设兵团工作汇报时强调

牢牢把握新疆在国家全局中的战略定位 在中国式现代化进程中更好建设美丽新疆

蔡奇出席汇报会

中办国办印发《关于进一步加强青年科技人才培养和使用的若干措施》

三部门联手推动商务信用体系建设高质量发展

经济社会数字化转型快速推进，新应用、新技术在升级迭代的同时，海量高价值数据不断产生，数据安全的战略价值得到各方认可。在社会层次中，中小企业是推动国民经济发展的基础力量，国家对于优质中小企业认定，设置三个层次，即：创新型中小企业、“专精特新”中小企业和专精特新“小巨人”企业。据统计，我国专精特新“小巨人”企业仅 1.2 万余家。

近日，中华人民共和国国家发展和改革委员会主管的《中国经济导报》针对专精特新“小巨人”企业进行报道。亿赛通从 2003 年成立至今，始终专注于数据安全，十几年如一日，早早入选国家级专精特新“小巨人”企业。本次，亿赛通以综合发展的市场表现，产品和技术的创新研发、前瞻性的数据安全建设理念，与《中国经济导报》记者深入交流，探寻亿赛通背后的故事。

资讯 07 INFORMATION

提升创新能力 融入全球价值链

北京朝阳科技创新基金成长中心举行揭牌仪式

在专精特新“小巨人”企业的认证中，要求企业长期专注并深耕产业链，在专业化发展的基础上，创新产品、深化服务。随着企业数字化改革的推进，亿赛通与时俱进，率先提出了数据安全“分放管服”数据安全建设理念和数据安全治理智能化体系，自主研制了电子文档安全管理系统、数据泄露防护系统（含终端、网络、存储等）、API 审计系统、数据库审计系统、数据库防火墙、数据库运维系统、数据脱敏系统（含动态和静态）、数据交换系统及文件防火墙等，覆盖了“云网端”等场景，构建了数据安全运营管理平台、数据安全态势感知平台及数据安全智能管理平台等。

专精特新“小巨人”企业认证对中小企业要求颇高，特别是技术创新能力，尤其看重研发投入和授权专利。截至目前，亿赛通已累计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。

交流中，记者提到，由于数字经济模糊了地域界限，大量的新兴技术和服务会同时被不同国家的用户使用，随着全球生产网络，以及新一轮产业革命与新一代信息技术革命的推动，全球价值链正在成为世界经济的显著特征。

从配套能力看，专精特新“小巨人”企业往往针对全球价值链有自身独特的产品或思考。作为数据安全行业的排头兵，亿赛通在数据安全方面，树立全球化战略意识，根据不同国家、地区的数据安全规定，梳理成安全策略。对还原出的业务内容进行对应的数据安全规定检查，及时发现业务开展过程中的敏感数据，并根据不同规定中数据的敏感程度采取不同的防护策略，以期满足不同国家、地区对敏感数据的安全要求。及时发现网络上不同要求的敏感数据，采取不同的防护方法，降低敏感数据泄露风险，保障数据出境安全。

通过交流发现，亿赛通作为专精特新“小巨人”企业的背后，不仅是始终专精于数据安全的建设，在理念、产品和安全的创新方面保持高度自我迭代和进化的重要印记，更是多年来在融合市场发展需求，与时俱进后一次又一次地全面释放。未来，亿赛通将通过自身的创新力，坚持走好“专精特新”发展之路，为用户带来更高层次的数据安全综合解决方案。

亿赛通支撑太仓市三主管单位完成企业数据出境安全培训

为深入学习贯彻习近平总书记网络强国战略思想，落实《数据出境安全评估办法》相关要求，提高企业员工对数据保护法律的理解和遵守，增强数据保护能力，降低数据出境风险，确保数据出境过程合规性和数据安全性，太仓市委网信办、太仓市工信局、太仓市公安局在 2023 年 9 月 7 日联合主办“2023 年太仓市企业数据出境安全培训”，培训由太仓市互联网协会承办，太仓市数字经济科技发展有限公司及北京亿赛通科技发展有限责任公司协办。全市来自跨国企业、数据处理外包企业、云服务提供商、跨境电子商务企业、跨境金融机构等行业近五十位企业代表参会。

近两年我国已经发布多项数据出境相关政策标准，科学、完备的细化数据出境定义、要求，如：《数据出境安全评估办法》、《数据出境评估申报指南（第一版）》、《网络安全标准实践指南——个人信息跨境处理活动安全认证规范》、《个人信息出境标准合同规定（征求意见稿）》等，上述政策法规命去了数据跨境传输的保护要求及合法路径。除此之外，金融、汽车、医疗健康等行业的主管部门还结合自身行业需求对特定行业的数据跨境流动提出了要求，进一步健全了数据出境流动规则。

太仓市作为对外开放合作的重要城市，数据资源价值逐步释放，数字经济发展态势良好。同时，太仓市地处长三角一体化发展、长江经济带建设、“一带一路”重大战略叠加区，又有“长江第一大港”的港口优势加持，数据出境需求频繁，要求企业在坚持数据出境流动安全性原则的前提下，提升对外贸易经济发展，实现数据出境价值攀升。

此次培训，市网信办组织了北京亿赛通科技发展有限责任公司的相关专家针对数据出境合规政策进行解读，分析了数据出境合规的重要性和影响。重点讲解了数据出境申报指引、数据出境风险自评估工作等。对数据资产分类分级的概念、方法进行介绍，现场解读《装备制造企业重要数据识别指南》（征求意见稿），也对个人信息出境的要求和实践做了介绍。现场与企业代表进行交流和探讨，让现场参会人员对数据出境流动的界定与立法价值，数据出境合规的重要性与必要性、数据出境安全有序流动如何赋能产业发展等方面有了更加深刻的认识。

亿赛通在数据出境安全方面深入钻研政策法规，结合 20 年项目实践经验，可以帮助企业用户对网络 (含邮件) 中的业务进行还原，并对还原出的业务进行内容识别。根据不同国家、地区的数据安全规定，梳理成安全策略。对还原出的业务内容进行对应的数据安全规定检查，及时发现业务开展过程中的敏感数据，并根据不同规定中数据的敏感程度采取不同的防护策略，以期满足不同国家、地区对敏感数据的安全要求。及时发现网络上不同要求的敏感数据，采取不同的防护方法，降低敏感数据泄露风险。


数据出境安全合规可落地


数据出境安全可视化


全面还原网络中的实际业务

下一步，太仓市委网信办将针对企业在申报过程中存在的痛点、难点问题，会同有关部门广泛开展调研，加强资源供给，优化营商环境，进一步服务企业高效申报数据出境安全评估，促进数据出境安全、合规、有序流动，保障重要数据和个人信息安全，推动数字经济健康快速发展。

亿赛通联合华为携手走进甘肃省网络安全宣传周

金桂飘香时节，全国奏起网络安全协奏曲，亿赛通网安之旅再延续。中央网信办于 9 月中旬举办 2023 年国家网络安全宣传周系列活动。甘肃省积极响应国家号召，在张掖举办网络安全周活动，营造网络安全人人有责、人人参与的良好氛围。亿赛通作为数据安全领域的中坚厂商联合华为共同受邀出席本次安全周。

党中央高度重视网络安全建设。没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。国家更是对加快推进新时代网络强国建设作出了全面部署，《国家安全法》、《网络安全法》、《数据安全法》、《个人信息保护法》等法律法规相继制定出台，在新形势下促进网络安全产业新发展。

亿赛通活动现场立体展示我司在协助知名企业进行数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务等方面取得的成就。在展出的一系列相关的安全方案以外，亿赛通专家还与现场观众交流各类网络攻击行为所带来的安全威胁，让观众更直观的理解生活中的网络安全隐患，帮助观众提升网络安全意识。

数据安全对企事业单位来说不仅仅是查缺补漏的工具，而是一个稳健发展的前提。数字化的发展使得数据安全需要一个全新的理念进行整合。除了黑客、漏洞和攻防问题，企业更多面临的是数据在产生、存储、流通中的安全问题。

基于在数据安全市场二十年的经验，亿赛通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。在终端层，基于数据内容进行全量、增量、定期、周期性扫描，对数据进行识别与检测，按照数据分类分级标准制度对数据进行分类分级管理，实现加密、外发审计、审批和阻断管理等措施；在网络层内置全球 IP 地址库，将数据访问发起端和响应端进行 IP 地址比对，识别数据的违规流转、跨境传输、非法出境状态记录、风险告警及流转阻断限制；在数据分散存储时，在终端、服务器端、云虚拟环境、网络端、邮件端可进行全覆盖多点部署，有力保证企业的数据安全建设。

新的经济形势已经出现，数字化进程的加速，业务需求的改变，对安全厂商的考验增加。完全完备的防御手段，对于企业而言也是不可或缺的，应当引起更多的重视，对于企业而言数据安全防护并不是小事，及早防范，更早受益，尽可能尽善尽美，才能为企业后续的发展建设夯实基础。

累足成步，继“网”开来。一直以来，“人民”都是网络安全贯穿始终的关键词，构建网络文明生态，筑牢网络安全防线更是写入数字时代里的“网安大事”。亿赛通希望通过本次网络安全宣传周，提升大众在网络安全方面的意识，并且呼吁大众积极参与到网络安全建设的阵营当中，保护好国家、企业、个人数据信息安全，同时也为净化网络安全环境贡献力量，携手国家合力共建“网络强国”！

亿赛通张艺伟：以服务构建数据安全治理的闭环体系

张艺伟：北京亿赛通科技发展有限责任公司高级咨询顾问。先后从事网络安全行业研究、数据安全战略规划、高级咨询服务顾问，在安全领域具有 10 年的工作经验。围绕数据分类分级、数据安全风险评估、数据出境合规、数据安全治理等方向，主导了政府、金融、央企、能源等多个行业的咨询服务项目。重点参编标准白皮书十余项，在网络安全政策及行业发展、数据安全体系规划与建设方面颇有研究。

2023 年初，工业和信息化部、国家网信办、发展改革委等十六部门联合印发《关于促进数据安全产业发展的指导意见》（以下简称《指导意见》），目标到 2025 年数据安全产业规模超过 1500 亿元。《指导意见》为我国数据安全产业高质量发展指明了方向，将有力推动我国数据安全发展进入了一个全新的阶段。

日前，亿赛通咨询研究部数据安全高级咨询顾问张艺伟在接受安全牛采访时指出，数据安全服务是满足数据安全合规要求、体系化提升数据安全保障能力的重要手段。亿赛通希望将其创新打造的数据安全咨询服务，与传统数据安全技术工具高度整合，从而更好地为各行业用户的数字业务流通赋能。

亿赛通动态 ESAFENET NEWS

数据安全服务浮出水面

当前，以数据为关键要素的数字经济蓬勃发展，经济社会数字化转型持续加速。数据已经成为国家战略资源和新型生产要素，数据安全对国家安全保障和数字经济发展意义重大。随着《数据安全法》《个人信息保护法》的公布与实施，法律规范的不断完善，数据安全的发展也进入了一个新的阶段。

张艺伟认为，《指导意见》作为数据安全产业的顶层规划文件，在贯彻落实国家数据安全法律要求和工作机制，明确数据安全产业发展任务，营造数据安全产业发展生态方面具有重要意义。《指导意见》聚焦数据安全保护和数据资源开发利用需求，提出促进数据安全产业发展的总体要求和阶段发展目标，围绕“产业本身要做什么”，明确了“提升产业创新能力、壮大数据安全服务、推进标准体系建设和推广技术产品应用”四项重点任务，对数据安全企业制定总体战略、发展相关业务、深化相关工作树立了信心、指明了方向。

“1500 亿元”是业界关注的焦点。业内普遍认为，产业规模的大幅提升，意味数据安全产业范围和内涵的扩充。在张艺伟看来，在合规、需求、风险等多因素驱动下，数据安全的内涵已从保护数据载体上的信息安全，转向通过数据安全保护促进数据合法有序开发利用；数据安全的保护对象也从保障数据自身的安全，扩展到数据流通活动安全和数据流通设施安全。

其中，《指导意见》特别强调，要“推进规划咨询与建设运维服务”，“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。”

张艺伟认为，这是充分结合国家监管要求和数据安全内生需要而提出的战略方向。一直以来，企业在开展数据安全工作时，面临数据安全意识和方法论不足、人才短缺、组织内部难协作、管理技术脱节、数据安全状态难持续等痛点，定制化的数据安全服务以及一体化的数据安全解决方案将成为解决这些痛点的有效手段。张艺伟表示，从市场需求来看，用户对数据安全服务的重视度和认可度持续提升，数据安全服务也逐渐从以往的支撑产品销售的打包服务，逐渐脱胎成为独立的新型产品。

构建数据安全治理的闭环体系

研究数据显示，数据安全服务作为近两年发展起来的新兴业务，虽然营收在整体数据安全业务中的占比不高，但增速明显。正是意识到数据安全服务的重要性和需求潜力，数据安全乃至网络安全领域的各方力量，都纷纷加入数据安全服务大军。在此背景下，亿赛通也通过整合资源并利用自身产品技术服务优势成立咨询研究部。

张艺伟认为，数据安全服务是面向组织的数据安全需求，基于数据安全合规要求、专业知识和实践经验，提供的以方案为主、产品为辅的业务形态。它不同于具有硬性指标属性的产品交付，而是基于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

目前国内数据安全服务主要分为咨询规划、认证评估、运营保障三大类：

• 咨询规划是数据安全体系化工程的前期重点工作，是为了瞄准方向、分解目标，并通过搭建数据安全组织、完善数据安全制度等服务，推进后续数据安全工作的开展。目前业内关注度较高的分类分级工作，在服务过程中涉及数据梳理，数据分类分级规则制定、实施，重要数据、个人信息等敏感数据目录编制等，旨在为数据安全管理制度完善、数据安全差异化防护目标和方案确定提供抓手，也被归为咨询规划的范畴；

• 认证评估分为能力认证、符合性评估、风险评估等：能力认证是对用户相关数据安全能力的检验和认可，如 DSMM 认证、数据安全产品认证；符合性评估是基于具体合

规场景和监管要求，对合规项进行逐一检查和打分，最终出具是否合规的评估报告；风险评估是为了识别风险要素、分析风险发生可能性和发生后的影响，以便及时整改；

• 运营保障是基于咨询规划方案和认证评估结果，利用数据安全技术和工具，支撑数据安全管理制度落地，监督技术防护效果，并通过定制化的数据安全培训，从人员层面提升数据安全意识和数据安全专业能力。

在张艺伟看来，这三大类服务与数据安全产品解决方案一起，互为补充和依托，有效打造数据安全状态持续保障的闭环体系。不过需要指出的是，近两年亿赛通在为用户提供服务的过程中发现，用户满足合规要求、体系化提升自身数据安全能力的需求迫切，对接连发布的合规要求理解不到位、对数据安全管理工作重视不到位、对数据资产和安全现状摸排不到位的现象较为严重，这正是未来安全厂商进一步开展数据安全服务工作的动力。

可落地的数据安全服务

张艺伟强调，随着《数据安全法》的颁布实施，“统筹发展与安全”已经成为数据安全工作开展的一个重要原则，“数据分类分级”“数据安全风险评估”等被正式确立为数据安全保护制度。而亿赛通在 2020 年就提出并发布的“分放管服”理念，和这些基础性的重要工作密切相关。

亿赛通之所以提出“分放管服”理念，就是希望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。

“从国家的文件精神可以看出，‘分放管服’理念到今天仍然有很强的实践意义。”张艺伟说，在新时期，亿赛通对“分管放服”赋予了新的意义，并对其进行升级完善:

• 在“分”的理念中补充纳入“合规政策的对标”“数据和安全现状的评估”，形成集“分析对标、分析评估、分类分级、分权分则”于一体的更为完善的工作体系；

• “放”和“管”作为《数据安全法》中“统筹发展与安全”的精神体现，将基于“分”阶段的基础成果，依据差异化的数据安全策略，落实“低敏感数据放行流通”“高敏感数据受控使用”的工作原则；

• “服”的理念则将从偏向后端的产品实施和运维保障逐渐前置，成为覆盖数据安全建设工作全流程的关键活动，不仅包括数据安全工作初阶段的体系规划，也包括安全管理和技术手段落实效果的持续监控评估、事后的应急响应和总结整改等。“服”充分体现亿赛通“以客户为中心”的经营理念，基于客户痛点需求和发展现状，以“有效”和“落地”为最终目标，为用户定制专属的数据安全深化方案。

张艺伟同时也强调，数据安全服务必须具备“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。因此，对于亿赛通公司而言，也将不断整合自身在数据安全领域的理论研究和实践积累，持续提升数据安全服务能力，切实保障数据资产安全，为我国数字强国建设和数据安全产业发展贡献更大力量。

亿赛通入选《2023 年度中国隐私科技厂商图谱》

近日，由上海赛博网络安全产业创新研究院联合上海数据安全协同创新实验室，以及业内专家共同编制的《中国隐私科技厂商图谱》（简称“CPTP 图谱”）正式发布。亿赛通凭借成功入选“数据发现、分级分类与标识”、“数据去标识化、匿名化工具”、“隐私事件响应”三项细分领域。

CPTP 图谱通过对国内隐私科技市场的调研分析，国外代表性隐私科技企业的筛选，旨在用全面、对比的角度展示我国隐私科技产业发展现状，重点聚焦“数据发现、分级分类与标识；数据去标识化、匿名化工具；个人信息授权管理；隐私保护影响评估；数据主体权利管理；数据流动监控；隐私事件响应；数据和隐私合规检测工具；隐私计算平台；隐私科技集成解决方案；隐私科技开源项目”11 个类别。

数据发现、分级分类与标识

通过自动化的数据扫描和策略识别的方式定位数据、分级分类数据，以进一步 实现分级保护。在数据发现过程中基于正则表达式、关键字、UDF 等模式或者 机器智能学习模式，自动将库、表中的数据进行识别和分级分类，并可视化分 级分类结果。基于分级分类结果对字段或表级别打标签。

亿赛通数据安全分类分级系统（简称 :DSCG）是一款提供敏感数据识别规则和数据分类分级标准管理功能的系统。它为资产敏感数据的发现和分类分级打标提供了依据。该系统内置了各行业的分类分级标准，并且用户可以根据实际业务通过自定义的多层级类别进行数据分类管理。通过全面的资产发现方式、灵活的资产梳理规则和深入的资产质量分析，该系统能够有效地帮助企业进行对数据资产的摸底和管理工作。这一过程改善了传统方式下的资产梳理和管理模式，提高了工作效率，保证了资产梳理质量，并实现了资产权责分明。此外，该系统还打破了数据孤岛，提高了获取效率，释放了数据资产的价值。它以资产发现和资产梳理为核心，以资产可视和资产可管为目标，致力于提升企业对数据资产的整体管控能力和运维效率。

数据去标识化、匿名化工具

数据去标识化工具在个体基础上，采用技术手段如假名、哈希、加密等替代对个人信息的标识，保留了个体的颗粒度，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体。数据匿名化工具通过对数据进行随机映射、统一泛化等操作，使其发布的数据无法关联到任何具体个体。数据映射是采用手动或自动的方式帮助企业确定整体数据流，识别企业处理的个人信息，个人信息的来源和去向，存储、传输或处理数据的系统或流程。

亿赛通静态数据脱敏系统（简称 :DMS-S），是一款利用特定脱敏算法对敏感数据去标识与匿名化，实现敏感信息可靠保护的数据脱敏产品。系统自动发现数据源中的敏感数据，针对不同敏感数据类型提供遮蔽、仿真、截断、随机值、固定值、偏移、映射和 HASH 等 30 余种脱敏算法，保证脱敏后数据的一致性和业务关联性。系统同时支持数据库结构化数据与办公类、医疗影像等非结构化数据文件的脱敏，可广泛应用于开发测试环境、数据交换、数据分析、数据共享等场景。

亿赛通动态数据脱敏系统（简称 :DMS-D）是一款高性能、高扩展性的动态敏感数据屏蔽和匿名化产品。系统利用通信协议解析与 SQL 代理技术，实现全透明和实时的敏感数据掩码能力，在无需对生产数据库进行任何改动的情况下，可根据用户的角色和权限，对用户实时访问数据库的返回结果进行屏蔽、隐藏、加密和仿真处理，确保不同角色的用户能根据自身权限合理访问和查看生产环境中的敏感数据。系统可广泛应用于业务访问、开发测试、运维操作等多种数据库访问场景，可低成本、高效率实现企业重要敏感数据的保护。

隐私事件响应

提供符合法律要求的合规应急事件自动化处理，包括向相关方提供隐私事件详情和需履行的事件通知义务，帮助企业应对法律风险。

亿赛通数据安全运营管理平台（简称 :DSOP）采用先进的大数据技术架构，通过采集分析来自于终端、网络、邮件和存储的结构化和非结构化事件日志，基于人工智能算法，以人员和终端行为分析为主线，探测发现威胁企业的数据安全事件，并提供完整追溯取证证据链，全面保障客户数据安全，有效预防、阻断或减少安全威胁事件的发生。

随着互联网的快速发展和技术的不断进步，数据安全和隐私治理变得越来越重要。企业需要找到合适的产品来保护他们的数据和客户的隐私。这需要对市场上的产品进行全面的了解和评估，以便做出明智的选择。

该报告对于企业和厂商来说都具有重要的参考价值，还帮助厂商洞悉隐私科技的发展空间和赛道蓝海，以及了解自身在行业中的位置。通过该报告，企业和厂商都能更好地开展数据安全与隐私治理工作，为未来的发展奠定坚实的基础。

《商业秘密保护进园区系列研讨会》第二期顺利举行，亿赛通护航企业创新发展

为了加强对商业秘密保护的认知，介绍相关政策措施，为广大科技企业提供有效的支持和指导，共同构建良好的商业环境。9 月 12 日下午，在北京市海淀区市场监管局的指导下，由北京海淀中小企业协会、中关村海新联新兴产业促进会主办，北京亿赛通科技发展有限责任公司等公司协办的“商业秘密保护与科技企业支持政策”宣讲会顺利召开。本次会议采用线上、线下相结合的形式开展，会议邀请了众多行业专家就商业秘密保护法规相关内容进行演讲，并针对企业现场提出的疑问进行了详细解答。

为加强商业秘密保护，国内外针对商业秘密保护的研究各有不同。商业秘密已经成为企业的核心竞争力之一，它不仅是企业的核心技术和创新成果，更是企业发展的命脉，是企业在市场竞争中的重要武器。保护商业秘密，对于企业的持续发展具有重要意义。作为《中小企业商业秘密保护规范》团体标准的主笔单位，亿赛通专家结合实际经验对商业秘密保护规范及解决方案进行了介绍和解读。

亿赛通认为通过建立统一的商业秘密安全保护标准，实现商业秘密保护的规范性与统一性。商业秘密安全保护是实现商业秘密保护的重要基础，是支持商业秘密处理活动的重要条件。实现安全保护能力标准化，可以提升企业商业秘密的管理与保护能力，从而更好地对商业秘密在收集、存储、使用、加工、传输、提供、公开、销毁等过程进行规范。通过提升商业秘密质量、提升商业秘密安全性，就是要把商业秘密作为企业的核心竞争力，加强对商业秘密的保护，以保护企业的经济利益。

随着数据大规模流通使用需求的增加，企业面临的数据暴露风险也越来越大。新兴技术如 5G 和物联网的应用，虽然带来了许多便利，但同时也带来了新的安全风险。另外，数据突破边界、流通环节众多，数据的流通路径变得复杂，使得企业对其安全性的可视性降低。此外，人们参与数据处理的程度和能力也存在下降的趋势，这进一步加大了数据安全风险。不同部门之间的协同合作也面临困难，导致组织在数据安全方面的工作效果有限。目前，组织在数据安全工作方面更多地集中在对数据的宏观定义上，而没有深入到特定的业务部门对数据进行有针对性的细分。

为了保护商密数据免受内外部威胁，提高企业核心竞争力，制定一个有效的商密数据安全保护建设方案至关重要。

亿赛通认为商业秘密数据安全保护是一项重要的任务，需要综合考虑现状调研、组织体系、制度体系、技术体系和运营体系等五个方面，形成一套综合的商业秘密数据安全保护建设路径。

1. 现状调研：

在建设商业秘密数据安全保护体系之前，企业应该先进行现状调研，了解当前的风险和威胁。这包括对商业秘密数据流动、存储和使用的整个过程进行全面的调研分析，确定存在的安全漏洞和风险点。

2. 组织体系：

建设一个有效的组织体系对于商业秘密数据安全保护来说至关重要。这包括明确责任分工、设立专门的保密组织和人员，制定相关的保密制度和流程，培养员工的防范意识，提升防护能力。

3. 制度体系：

建设一个完善的制度体系是商业秘密数据安全保护的基础。企业应当制定明确的保密制度和操作规范，明确数据的分类、保护等级和访问权限控制。同时，加强对员工的保密意识教育和培训，确保全员遵守保密规定。

4. 技术体系：

技术体系是商业秘密数据安全保护的关键。企业应采用先进的技术手段，比如建立防火墙、入侵检测系统、数据加密技术等，保护数据在存储、传输和共享过程中的安全。

此外，核心系统和应用程序的安全性要得到特别关注，定期更新和升级技术措施。

5. 运营体系：

建立一个有效的运营体系有助于提升商业秘密数据安全保护的执行力。同时，加强对供应商和合作伙伴的管理，并与其签订保密协议，确保合作过程中的数据安全。亿赛通数据安全运营管理平台是通过提供基础数据安全的能力，把各种安全能力都集成在一个平台，整合数据全生命周期各阶段状态，总览数据资产和安全风险，实现数据安全运营的闭环管控。

我们希望通过本次大会议能够加强与广大企业之间的沟通与合作，共同面对商业秘密保护的挑战，推动我国科技企业的创新发展。亿赛通相信，未来，在政府的政策支持下，广大企业的共同努力下，商业秘密保护将取得更加显著的成果。

亿赛通亮相 2023 年湖南省数据跨境安全论坛，与行业专家共话数据出境合规服务

9 月 15 日，湖南省国家网络安全宣传周活动 --2023 年湖南省数据跨境安全论坛在长沙隆重拉开帷幕。本次活动由湖南省委网信办主办，国家计算机网络与信息安全管理中心湖南分中心、长沙市委网信办、湖南湘江新区宣传工作部承办，北京亿赛通科技发展有限公司协办，为活动全程提供支撑，助力大会圆满收官。

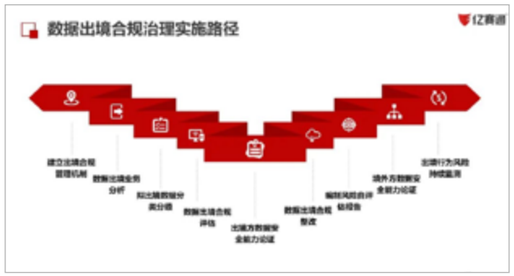
数字经济时代，数据的跨境共享流通已成为全球经济发展的重要推动力。湖南数据安全保障工作的进度和力度不断加快和提升。作为湖南省 2023 年国家网络安全宣传周的重要活动，本次论坛以“保障数据出境安全，推动数字经济繁荣”为主题，邀请来自政府、企业、学术界的领导和专家学者聚焦数字经济这一前沿议题，深入探讨数据出境安全保护的新思路、新观点和新路径，前瞻分析数据出境面临的困难挑战，共同分享国内数据出境管理的最新实践经验，为构建数字经济时代下的数据出境安全与合作作出积极贡献。

论坛分享环节是活动的亮点之一，亿赛通高级咨询顾问在此环节中发表了《数据出境合规咨询服务经验分享》主题演讲。亿赛通认为数据跨境流动和管理正逐渐成为国家博弈、企业合规的关键。数据跨境管理制度、外商投资审查、技术数据出口管制等制度相结合，使数据跨境成为当前国家地区间政策博弈最为复杂的领域之一。企业需同时考虑数据输出地和输入地的数据跨境规则，以满足“双向合规”要求；长臂管辖等因素使得同一法域的数据处理行为需要满足多法域规则，提升合规难度。

立法层面，《网络安全法》《数据安全法》《数据出境安全评估办法》《数据出境安全评估申报指南（第一版）》相继发布确立了重要数据出境传输前应通过安全评估的保护要求；《个人信息保护法》确立了个人信息跨境的三条合法路径，《数据出境安全评估办法》《网络安全标准实践指南——个人信息跨境处理活动安全认证规范》《个人信息出境标准合同规定（征求意见稿）》分别为三条合法路径提供了实施指引。

自《数据出境安全评估办法》实施起，数据出境安全评估申报成为相关企业的迫切工作。对企业而言，数据出境合规治理面临六大难点：重要数据如何判定？出境安全评估路径适用条件如何理解？数据出境风险场景如何辨别？个人信息、敏感个人信息如何识别？出境业务如何梳理？出境合规能力如何评估、论证和整改？

对企业而言，想要做好数据出境安全，首先需要明确数据类型。重要数据是指特定领域、特定群体、特定区域或达到一定精度和规模的数据，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。个人信息是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。亿赛通在帮助企业做数据出境合规治理中，通过数据安全服务对企业数据进行分类分级，确定企业重要数据、个人信息的分布和敏感级别，给出数据出境合规申报路径建议，协助企业完成重要数据安全自查。



企业在数据出境合规治理过程中，为了满足监管需求，需要围绕数据对企业的数据安全管理能力进行整体评估。厂商帮助企业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、数据出境合规评估、出境方数据安全能力论证、数据出境合规整改、编制风险自评估报告、境外方数据安全能力论证、出境行为风险持续监测等步骤进行数据出境合规治理实施。基于上述流程，亿赛通特为相关单位推出一款数据跨境安全检查工具，在产品 + 服务的联动中，辅助组织完成企业数据出境安全风险评估。

数据出境安全有大量的细节需要安全厂商、企业在合规工作中注意，这不是一项能轻易完成但具有重要意义的工作。数据安全的国际博弈才刚刚开始，亿赛通会继续帮助客户实现数据资产在境内、外的安全流转，为保障国家、企业、个人的数据安全尽自己的一份力！

亿说安全之安全治理，服务先行

在以数据为关键要素的数字经济发展的背景下，企业建立数据安全治理体系需要数据安全服务、技术和管理全方位的能力。其中，数据安全服务作为数据安全软能力是数据安全治理能力建设中必不可少的内容。

国内数据安全已经进入强监管时代，企业面临合规压力。业务运营、敏感数据保护带来新的挑战。在多款数据安全相关政策法规实施后，很多企业因存在顶层设计缺乏、标准规范及制度规程不健全、组织架构及人员配备不完备、管控措施覆盖不全等问题，不得不进行数据合规建设，而数据合规离不开数据安全服务。

亿赛通基于数据安全合规要求和风险治理专业实践，以服务的形式向组织用户提供咨询规划、评估认证和安全运营支撑，通过聚焦核心业务和关键需求，摸清全量数据和权属关系，分析安全风险和治理空间，提升运维保障和人员能力，帮助客户改善“信息化建设”与“安全建设”双规并行，“安全管理”与“安全技术”衔接不畅的问题，实现数据安全状态的可持续保障。

以服务带动建设

通过数据资产盘点、分类分级、数据安全评估等服务项，全面摸清数据现状、业务现状和安全管理现状，为后续全面的安全体系建设打好基础。

基于业务的全流程服务

数据安全服务工作的第一阶段将以问卷和访谈调研开展，过程中将详细了解用户数据与业务的关联关系，通过数据盘点、分类分级、方案规划等工作，为用户提供基于其业务需求的全流程服务。

围绕核心业务，保护数据资产价值

随着信息化和数字化建设的推进，各类组织中数据总量大、分散广、类型杂，用户对自身数据资产现状不清，面对数据合规要求和风险隐患无从下手。数据安全服务将聚焦用户核心业务，通过资产盘点摸清数据资产底账，并聚焦核心业务中的敏感数据，提供差异化的安全管理和防护方案，从而以最低的成本达到合规和安全目标。

基于数据全生命周期的数据安全服务

在新技术、新场景的驱动下，数据流转路径不断打破原有边界，从本地场景到云端场景，从存储等单一环节到采集、传输、使用、加工、开放、共享、销毁等全流程，均存在着数据安全隐患。数据安全服务将基于对客户现有数据安全技术和能力现状的总结分析，查漏补缺，在关键风险点帮助用户补足数据安全技术和能力，从而打造数据从产生到销毁的安全体系闭环。

试点先行，形成标准化样板

数据安全服务内容包含组织制度建设、技术体系规划、人员能力提升等，涉及从管理制度到技术框架的整体革新；同时，数据安全能力建设工作也无法一蹴而就，需要分阶段、分步骤逐步落实并持续优化。因此，前期先以单一系统或场景为试点，做好试点的安全服务工作，再“以点带面”，将试点经验复制和完善，形成安全能力的整体提升。

目前，亿赛通数据安全服务已覆盖政府、央企、金融、能源、智能制造等多个行业领域，在安全风险评估、数据资产盘点、数据分类分级、数据防护策略搭建、数据安全检查、数据安全培训乃至全面的数据安全治理工作中积累了丰富的实践经验。面对国家、地区、行业发布的百余项数据安全合规文件要求，帮助客户实现准确对标和深入理解，并将理论要求和实践经验落实到具体工作中，为用户的信息建设和数据管理工作保驾护航。

制造业数字化转型，企业该如何织好数据安全保护网？

随着全球产业调整、技术升级和区域转移向纵深发展，国际装备制造业发展业出现了新的趋势。装备制造业是世界各国争夺的战略制高点。作为“大国重器”的装备制造行业，挺起了中国制造的脊梁，是工业的心脏和国民经济的生命线。在全球产业格局面临重大调整的情况下，我国装备制造业面临发达国家“再工业化”，和其他发展中国家快速进取的双重压力。国家出台了一系列政策来推动装备制造企业与新技术融合，从而增强核心竞争力。

《“十四五”智能制造发展规划（征求意见稿）》——智能制造需立足制造本质，紧扣智能特征，以工艺、装备为核心，以数据为基础，依托制造单元、车间、工厂、供应链和产业集群等载体，构建虚实融合、知识驱动、动态优化、安全高效的智能制造系统。

市场环境：装备制造业客户需求趋于个性化、定制化，亟需加速推进新技术创新、新产品培育、新模式扩散和新业态发展，形成核心竞争力。

社会环境：社会公众的数字化意识逐渐加深，员工对数字化的理解和接受程度不断提高，装备制造企业拥有实施数字化转型的良好社会条件。

技术环境：工业互联网作为新一代信息通信技术与工业经济深度融合的新型基础设施、应用模式和工业生态，构建起覆盖全产业链、全价值链的全新制造和服务体系。

行业趋势：在传统产业链上融合数字化技术、构建贯通企业研发、生产、交易的生产经营流程，重构企业模式，实现产业间的融合与产业生态链的协同发展。

装备制造产业数字化正在蓬勃兴起，覆盖全价值链的数字化转型业务场景。首先，装备制造尤其是高端装备设计、加工工序多、技术密集度大，在各个环节都会产生大量数据且被高度共享使用，同时就存在着大量数据安全风险。其次，装备制造业数据存储和传输的安全风险也不可忽视。随着大数据技术的发展，装备制造企业产生的数据量越来越大，如何安全地存储和传输数据成为一个重要问题。此外，装备制造业数据安全还面临着恶意软件和病毒攻击的风险。恶意软件和病毒攻击的目的是通过篡改、破坏或窃取数据来对企业造成损害。最后，企业员工对社会工程学攻击的警惕性需要提高，避免成为攻击者的目标。

作为工业的心脏和国民经济的生命线，装备制造业是国家经济安全和军事安全的重要保障。尤其是涉及到国防领域的先进技术和装备。制造业企业的科研数据被泄露或窃取，将对企业带来巨大的经济损失甚至倒闭的风险。基于多年来在数据安全领域的技术积累与实践，亿赛通为客户提供综合解决方案。从数据的存储、传输、交换过程中的安全环节，采用了多种加密手段结合的方式保护，为企业提供数据安全保障。

为了构筑数据安全管理的“三道防线”，亿赛通认为应该建立“事前防御 - 事中控制 - 事后审计”的安全保护机制，实现数据安全的常态化、动态化、精准化、全面化管理。装备制造企业需要了解数据安全的重要性，并加强相关措施的落地。

首先，装备制造企业应在事前加强安全防范，构筑数据安全的第一道防线。企业可以通过制定和完善信息安全管理制度、建立专门的数据安全团队、加强员工安全意识培训等措施来提升数据安全防护能力。信息安全管理制度应涵盖从数据采集、存储、传输到处理等全过程的规范要求，确保企业内部数据资源的完整性、可用性和机密性。数据安全团队的建立旨在提供专业的技术支持和管理，确保数据安全的持续性和可控性。此外，员工是企业数据安全的最后防线，通过加强员工的安全意识培训，使其能够正确处理和保护重要数据，从而降低数据泄密和安全事故的风险。

其次，装备制造企业还应在事中进行实时监控和控制，构筑数据安全的第二道防线。企业可以通过数据安全防护相关系统，实时监测和分析数据安全事件，及时发现和应对潜在的威胁。通过对网络流量、系统日志、用户行为等进行实时监控和分析，可以提供异常检测、威胁识别和响应等功能，帮助企业及时发现和处置潜在的数据安全威胁。此外，企业还可以利用数据分类和权限管理等措施，将数据进行分类和分级，并设置不同的权限和访问控制，实现对数据的细粒度管控，确保数据仅限授权人员访问和使用。

最后，装备制造企业需要在事后进行安全审计，构筑数据安全的第三道防线。企业可以通过建立数据安全审计制度和使用合规的审计工具，对数据安全事件进行溯源和分析，确保安全事件的快速反应和事后追责。数据安全审计制度应明确审计的范围、时机和频率，并制定具体的审计流程和方法。审计工具可以采集和分析关键的安全事件日志和网络数据包，帮助企业了解安全事件的发生原因和影响，及时采取措施加以修复和改进，同时为处理与安全事件相关的纠纷提供证据和依据。

数字化是装备制造产业发展的必然趋势。由此可见，装备制造产业的数据安全是企业生存和发展的重要保障。企业应该建立健全的数据安全管理制度，加强对数据的访问控制、传输和存储的保护，加强网络安全，加强与供应链伙伴的合作，并加强数据安全的监控和应急响应能力。通过这些措施，装备制造企业能够更好地保护自身的数据资产，推进数字化转型，实现可持续发展。

作为一家致力于数据安全建设的企业，亿赛通将继续为建设数字强国贡献力量。我们相信，在数字化转型的过程中，数据安全是企业成功的关键要素之一。我们将继续专注于数据安全的创新和发展，为企业提供可靠的解决方案，助力他们在数字化时代取得更大的成就。

违规存储用户个人信息，知网被罚款 5000 万元

知网被罚款 5000 万

近日，国家互联网信息办公室依据《网络安全法》《个人信息保护法》《行政处罚法》等法律法规，综合考虑知网（CNKI）违法处理个人信息行为的性质、后果、持续时间，特别是网络安全审查情况等因素，对知网（CNKI）依法作出网络安全审查相关行政处罚的决定，责令停止违法处理个人信息行为，并处人民币 5000 万元罚款。

国家互联网信息办公室依法对知网（CNKI）涉嫌违法处理个人信息行为进行立案调查。经查实，知网（CNKI）主要运营主体为同方知网（北京）技术有限公司、同方知网数字出版技术股份有限公司、《中国学术期刊（光盘版）》电子杂志社有限公司三家公司，其运营的手机知网、知网阅读等 14 款 App 存在违反必要原则收集个人信息、未经同意收集个人信息、未公开或未明示收集使用规则、未提供账号注销功能、在用户注销账号后未及时删除用户个人信息等违法行为。

在当下的互联网时代，APP 普遍收集和使用个人信息，这主要是个人信息对于提供个性化服务、和用户行为分析等方面具有重要作用。但也有可能将个人信息用于未经用户同意的商业用途。一些非法分子可能会将用户的个人信息出售给第三方，或者用于精准广告投放。这种行为可能侵犯用户的权益，也可能导致用户接收到大量垃圾邮件、推销电话等骚扰。此外，用户不知情的情况下收集和使用敏感个人信息，例如身份证号码、银行账号等。这种滥用个人信息的行为可能导致个人权益受损，也可能给用户带来不必要的麻烦和损失。

教育部等七部门发布关于加强教育系统数据安全工作的通知，坚持以习近平新时代中国特色社会主义思想为指导，全面贯彻落实党的十九大和十九届二中、三中、四中、五中全会精神，坚持总体国家安全观，根据《中华人民共和国民法典》《中华人民共和国未成年人保护法》《中华人民共和国网络安全法》等法律法规和政策文件要求，建立健全教育系统数据安全治理体系。坚持以人民为中心的发展理念，保障广大师生的切身利益，发挥数据生产要素作用，促进教育事业发展。

其中，《数据安全法》第三十二条：任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。法律、行政法规对收集、使用数据的目的、范围有规定的，应当在法律、行政法规规定的目的和范围内收集、使用数据。《个人信息保护法》：第五条　处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。第十条　任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

数据分析，教育行业攻击事件中 27.8% 导致数据泄漏，泄漏事件中 67% 来自外部，33% 来自内部（其中 1% 是内外勾结，1% 是合作伙伴泄漏），泄漏数据主要是个人信息、凭证信息、内部资料等，92% 的数据泄漏是因为经济驱动，且同样存在职务之便和间谍因素。因此，数据的价值和敏感性使得数据安全成为教育行业的一项重要任务。数据泄露、黑客攻击和不当使用等安全问题都可能会给学校、学生和家长带来严重的负面影响。因此，教育行业需要采取一系列的举措来保护数据安全，维护教育生态的良好运行。

北京亿赛通深耕数据安全行业，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。

亿赛通作为数据安全行业内专业的综合解决方案厂商，一直致力于为客户提供卓越的服务。无论是面对日益复杂的数据安全挑战还是快速变化的市场需求，亿赛通始终将客户的需求放在首位，并积极探索与创新，以满足客户的不断变化的需求。

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，亿赛通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”建设理念和数据安全治理智能化体系，自主研制了电子文档安全管理系统、数据泄露防护系统（含终端、网络、存储等）、API 审计系统、数据库审计系统、数据库防火墙、数据库运维系统、数据脱敏系统（含动态和静态）、数据交换系统及文件防火墙等，覆盖了“云网端”等场景，构建了数据安全运营管理平台、数据安全态势感知平台及数据安全智能管理平台等。

通过采用多种技术措施，可以更好地发现数据源并对其进行分类分级。这样能够更清晰地了解数据资产的存储情况，从而夯实数据安全保障基础。此外，在重点数据交换及使用区域实施数据审计、脱敏、加密以及泄露防护等能力，进一步提升数据安全防护水平。同时，针对数据资产的整个生命周期进行全流程监管，能够及时发现违规操作并进行告警和阻断，以及对数据资产进行全盘态势感知，预知潜在风险。除了以上技术措施，还可以提供安全咨询、安全评估、威胁情报、运维保障以及应急响应等服务。通过这些服务，可以提供专业的支持和指导，确保数据安全治理工作能够得到有效实施。这不仅可以为学校、机构提供安全保障，还能够提升整体数据管理的水平，保护学校的核心信息资产。

教育行业数据安全只有通过建立完善的数据保护体系、加强对个人信息的保护、规范教育资源的管理和使用、加强学生和家长的信息安全教育，以及加强监管和执法，才能确保教育行业数据的安全和可信，为学生提供更优质的教育资源和服务。

在数据安全领域，亿赛通的专业技术和综合解决方案备受认可。通过深入研究和了解客户的业务需求，亿赛通能够提供精确、全面、适用的解决方案，帮助客户应对各种安全风险和威胁。未来，我司将秉承初心，持续创新，切实提升产品防护能力，为全行业客户的数据资产安全保驾护航。

当勒索攻击来“敲门”，企业该如何自保?

近期，重大勒索攻击事件不断爆雷。从某银行宕机事件、房企遭勒索病毒索赔 400 万美金到美国最大燃油管道运营商遭勒索病毒攻击，再到近日的香港消费委遭勒索 50 万美元 ..... 种种痛心的案例表明，勒索病毒正在不断升级攻击手段，扩大攻击范围，从某种意义上来说，所有的系统都有被攻击的风险！破坏力也在快速升级！

香港消费委遭勒索 50 万美元

香港消费者监管机构成为黑客攻击的最新受害者。据香港《星岛头条》9 月 22 日报道，香港消费者委员会 9 月 20 日遭黑客入侵，时间长达 7 小时，八成系统被破坏，系统较正常流量多出 65GB。黑客窃取了消费委的员工、月刊用户数据，以及其他内部资料。攻击者向香港消费委勒索 50 万美元赎金。

香港数码港遭黑客入侵部分数据泄露 特区政府：已要求堵塞漏洞

香港数码港管理有限公司 (以下称“数码港”) 近日遭黑客入侵，致使部分数据泄露。香港特区政府创新科技及工业局局长孙东 13 日就此会见媒体时表示，特区政府对这次网络攻击事件予以高度关注。他已要求数码港全面提升对相关网络系统和敏感数据文件的保护措施，堵塞各种漏洞。香港数码港是香港数码科技旗舰及创业培育基地，汇聚超过 1900 家社群企业。今年 8 月中旬，数码港发现系统被入侵。事件发生后，数码港立刻采取措施展开调查、报警处理并向执法部门寻求协助，并于 8 月 18 日通报香港个人资料私隐专员公署。据港媒报道，本月 6 日，有疑似与该事件有关的资料在“暗网”上被披露，包括疑属数码港人事部内部资料，例如员工相片、身份证、手机号码、申请入职履历、银行资料等，数量达 400GB。数码港 12 日发表声明公布事件最新情况，表示留意到相关资料被披露，已直接联系可能受影响人士并为他们提供协助。

毋庸置疑，如今勒索病毒已成为各类政企的头号威胁，令人防不胜防。黑客攻击可以采用多种形式，包括但不限于网络钓鱼、恶意软件、拒绝服务攻击等。这些攻击手段旨在获取机密信息、破坏系统、窃取财务信息等。一旦黑客入侵，个人和企业都将面临巨大的风险。个人可能面临身份盗窃、财务损失等；而企业则可能面临财务损失、声誉受损、法律诉讼等长期影响。

除了做好网络防护和杀毒之外，如何在遭受勒索病毒攻击后，能快速恢复企业的业务系统，解除勒索病毒的封印？如何把勒索病毒攻击带来的影响降到最低？这已成为各大政企密切关注的问题。

亿赛通通过自身专业的安全服务和安全工具，与中国太平洋保险达成战略合作，形成“防勒索 + 保险”的整体解决方案，由传统的“事后理赔”模式转变为 “事前防御、事中预警、事后补偿”的全新模式。太平洋保险公司设立“防勒索数据安全险”，针对高价值文件提供防勒索安全保障，这不仅是一份保障合同，更是一项专业责任的服务承诺。

亿赛通文件防火墙 (简称 : EDFW) 是一款为防止勒索病毒对企业的核心数据文件进行攻击而研发的防勒索病毒软件，主要是对文件进行保护，不允许非法进程访问受保护的文件，防止非授权进程如病毒、木马、勒索软件等对指定文件类型或路径下文件的篡改、破坏和窃取。该产品支持对已知勒索病毒和未知勒索病毒的防护能力，阻止勒索病毒加密、删除文件 ; 并且基于数据的操作系统内核级防护技术而非病毒特征库技术，无需更新病毒特征库即可防御新型勒索病毒攻击。

“防勒索 + 保险”的整体解决方案，由传统的“事后理赔”模式转变为 “事前防御、事中预警、事后补偿”的全新模式。太平洋保险公司设立“防勒索数据安全险”, 针对高价值文件提供防勒索安全保障 , 这不仅是一份保障合同 , 更是一项专业责任的服务承诺。

保前：我们提供远程风险测评服务，以及制定各项重要数据的保密服务承诺,配备了完善全面的保险应急方案，以确保在任何紧急情况下，能够迅速采取措施保护客户的数据安全。

保中：我们对数据进行持续的风险监测，并及时进行预警，以便在发现问题时第一时间通知管理人员，快速启动应急处理方案，以降低安全风险，保护客户的利益。

保后：我们承诺在发生安全事故后的 72 小时内到达现场，定责定损，并派遣安全专家修复系统、恢复数据。我们致力于在最短的时间内恢复正常运营，确保客户的业务不受影响。

作为中国数据安全专家，亿赛通将充分发挥自身优势，为用户提供安全可靠的“防勒索数据安全险”整体解决方案，共同维护网络空间的秩序和安全。

亿赛通为某物流行业央企提供数据安全服务，助力用户数据安全迸发新活力

数据安全服务是数据安全体系建设的关键一环。通过数据安全服务解决数据安全建设难题，得到越来越多的重视。数据安全服务市场正在步入快速发展的黄金期，各厂商纷纷布局，同时，数据安全服务品类也呈现出多样化趋势，包括：数据安全风险评估、数据安全治理咨询、数据安全培训、数据安全体系建设、数据分类分级、数据安全检查工具等。

亿赛通作为中国数据安全专家，本次将以物流行业央企的实际项目为例，为大家独家揭秘亿赛通的数据安全服务指南。

项目背景

近年来国家对于数据安全愈加重视，陆续颁布了多项法律法规，对数据在采集、传输、存储、处理、交换、销毁全流程中涉及的数据保护、个人隐私保护、数据安全问题等做了明确规定。某物流行业央企对 IT 系统依赖性极高，在长期的经营生产过程中也产生了大量的数据。该公司在前期的网络安全治理中对于边界防护，审计等进行重点建设，但在数据安全技术体系的建设上存在很大差距。因此，集团把数据安全治理作为一个重点工程，力争通过试点逐步建设起该公司的数据安全防护体系，确保业务的顺利开展。

解决方案

1. 数据安全组织建设服务

在该公司已有的网信安全组织基础上，加入相关数据安全保护职责并在数据安全技术体系建设过程发挥管理、指导、协调等作用；

2. 数据安全管理制度建设

在该公司《网络信息安全管理办法》基础上，制定数据安全政策、形成企业级数据安全解决方案、数据分级分类规范以及详细的操作流程、作业指导书等；

3. 数据安全试点应用

选择跨境电商业务线相关项目为试点，采用总体规划、分步实施、稳妥推进、确保公司业务安全为指导原则，快速建立该公司数据安全技术体系框架，将管理制度、技术平台组件通过跨境电商业务线指导规划，形成企业级的数据安全解决方案。

亿赛通按照该公司整体网信安全管理和技术防护体系规划，以业务高效开展和数据安全流通为目标，以“风险防范”与“安全合规”为抓手，打造了数据安全保护体系。

通过“一个战略规划”、“两个安全支点”、“三个行动方向”、“四个能力维度”的治理思路，以及为期三年有序推进的实施计划，实现网络安全、数据安全、业务安全的一体化组织保障，以及数据安全核心能力的稳步提升。

项目成果

最终，此项目通过对该公司数据安全组织、数据安全管理情况的调研，为客户定制数据安全组织架构图、数据安全管理办法、数据安全服务协议（中英文版本），并针对数据出境欧盟的需求特点，编制了相应服务承诺，以推动集团内部的数据出境合规治理和自评估工作。同时，通过对跨境电商业务系统的试点研究，全面梳理用户数据、制定《数据分类分级规范》及《数据出境管理办法》；结合现有数据安全建设痛点问题，提出《跨境电商业务线企业级数据安全解决方案》；针对业务情况和后续数据安全建设需求，与用户联合编制《三年规划建议书》，从管理手段到技术手段，从规范文件到实施方案，为用户提供了体系化的数据安全能力建设服务。

目前，提供数据安全服务的厂商百舸争流，各有所长，如何选择数据安全服务厂商，用户需从数据安全服务经验、对行业业务场景的认知、团队项目实施经验等进行综合考量。亿赛通根据自身专业能力和技术优势，围绕用户实际业务需求，在数据安全服务方面积累客户实践经验，引领数据安全服务市场先进思想，释放数据动能，助力各行各业数字化转型升级。

中国国际海运集装箱（集团）股份有限公司

客户简介

中国国际海运集装箱（集团）股份有限公司（简称“中集集团”），是世界一流的物流装备和能源装备供应商，总部位于中国深圳。公司致力于集装箱、道路运输车辆、能源和化工装备、海洋工程、物流服务、空港设备等，提供高品质与可信赖的装备和服务。其市场占有率而言，中集有 10 多个产品持续多年保持全球前列，作为一家为全球市场服务的跨国经营集团，中集在亚洲、北美、欧洲、澳洲等地区拥有 200 余家成员企业，客户和销售网络分布在全球 100 多个国家和地区。

需求背景

随着中集集团业务快速扩展，集团经营规划、行政办公、技术研发资料愈发重要，集团需要统一梳理核心数据并明确各级数据保护规范和要求。集团下属 50+ 分公司，研发资料、项目文档技术保护手段和管理存在缺失，资料外泄情形屡有发生，核心重要资料容易被竞争对手窥视，许多重要资料随着人员离职等大量流失。集团出现部分数据泄密事件后审计无从做起，相关职责划分不明确，缺乏技术手段。

解决方案

亿赛通数据泄露防护（DLP）系统是一款基于内容识别技术的保护系统。

终端防护：防止敏感数据通过打印、刻录、聊天工具、发送邮件等终端方式泄露出去。

网络防护：防止敏感数据通过邮件、网盘、微博、FTP、论坛等网络方式泄露出去。

数据扫描：通过扫描和分类的方式，随时随地发现企业敏感数据分布，并保护静态数据。

邮件防护：防止敏感数据未经任何检查通过企业邮箱泄露出去。

数据分析：基于规则和中文语义的智能数据分析，对数据进行高效敏感检查。

审计报表：提供统计分析能力，实现安全现状可度量、事件可追溯、态势可查询。

项目成果

亿赛通完善的数据泄露防护（DLP）解决方案，为中集集团建立了一套数据资源保护标准，防止员工的不安全行为引入风险，以及保障了各个环节数据的安全运行，并且使得员工了解与自己相关的数据安全保护责任，强调数据系统安全对企业业务目标的实现、以及业务活动持续运营的重要性。