联系我们

地址：北京市海淀区西二旗大街 39 号 A 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com

关注官方微信公众号

关注官方微信服务号

关注官方微信视频号

关注官方抖音号

亿赛通

ESAFENET

ESAFENET

亿赛通企业月刊　　中国数据安全专家　　www.esafenet.com

06 月刊

2023 年共 12 期

关注企业官方微信

Esafenet
Monthly magazines

中国数据安全专家

主办：亿赛通市场部

北京亿赛通科技发展有限责任公司

地址：北京市海淀区西二旗大街 39 号 A 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com

CONTENTS目录

刊首语

ESAFENET

刊首语 PREFACE

《亿赛通六月刊》摆脱单点式防护，建立体系化能力

数据显示，2022 年，我国数字经济规模总量稳居世界第二。数字经济蓬勃发展的同时，数字安全问题不容小觑。非法获取个人信息、网络诈骗等违法犯罪活动，侵害个人财产和隐私安全；网络攻击、网络窃密等行为，给社会治理、国家安全带来挑战。从客户视角来看，客户越来越多关注如何能够在快速理清数据资产等级与敏感度情况下，建立系统化体系化的数据资产防护能力，实现灵活的全面的数据安全保护目标。安全厂商需要顺应客户新的防护需求以及业务场景所面临的数据安全风险问题。《亿赛通六月刊》带来数据安全新模式，给大众带来合规 + 安全的全新体验。

国内

1、上海现新型盗取公民信息案 物流公司电脑竟被植入木马

摘要：6 月 15 日，记者从上海市公安局采访获悉，警方日前从接报的一起电信网络诈骗案入手，在全力破案挽损的同时，循线深挖公民信息泄露源头，经过深度研析和缜密侦查，成功侦破上海市首例在物流公司电脑植入木马非法获取公民信息的系列新型案件，抓获犯罪嫌疑人 9 名。

2、买房后骚扰电话不断！到底谁在泄露我的隐私？

摘要：5 近日，有网友在“问政赣州”平台投诉，新房没交付就遭各种装修电话骚扰，断断续续近两年的时间，望严查公民信息买卖行为，现在提供一个买卖个人信息装修公司线索。1376771**** 赣州华佑装饰。经查，该公司是通过小红书等其他 app 发布视频后，通过观看视频时 , 在视频界面显示的链接信息中所填写的电话号码，公司会根据填写的号码打电话询问是否需要装修房子等需求。民警对该公司负责人进行警告和批评教育，告知其今后联系客户要如实说明取得的联系方式途径。

3、2.8 万余条个人信息泄露！嫌疑人已抓获

摘要：近日，湖北咸宁赤壁市公安局网安大队捣毁两个侵犯公民个人信息犯罪窝点，刑事拘留 3 人，查获提取纸质个人信息 2.8 万余条，有力震慑了非法交易公民个人信息关联犯罪的嚣张气焰。

4、日播时尚回复上交所问询函：不存在内幕信息泄露的情况

2、本次重大资产重组筹划的具体过程、重要时间节点和相关人员如下：

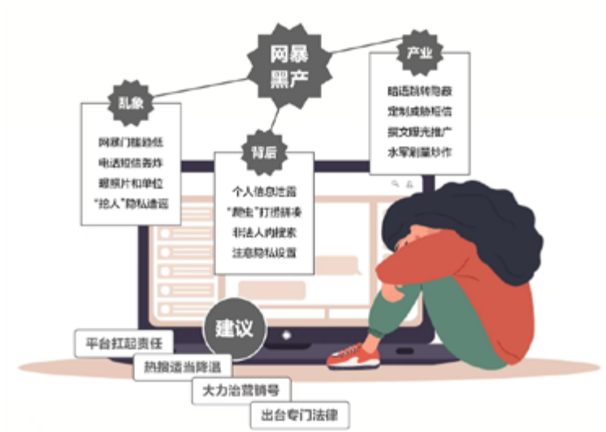
交易阶段	时间	筹划决策方式	参与机构和人员	商议和决议内容
接洽	2023 年 5 月 1 日	现场	交易双方及中介机构相关人员	首次接洽，各方表达重大资产重组意向。
商议筹划	2023 年 5 月 3 日	现场结合通讯（视频）	交易双方及中介机构相关人员	各方确认重大资产重组意向，并商讨重大资产重组意向书的内容，并确定后续事项安排。
形成意向	2023 年 5 月 8 日	现场结合通讯（电话）	交易双方及中介机构相关人员	各方签署《资产重组意向书》，发布重大资产重组继续停牌公告，明确后续事项重要时间节点。
签署协议、召开董事会、监事会形成决议	2023 年 5 月 15 日	现场结合通讯（视频、电话）	交易双方及中介机构相关人员	各方签署《重大资产置换及发行股份购买资产协议》，召开董事会审议相关事项并形成决议，发布重大资产重组预案、复牌公告等相关公告。

摘要：日前，日播时尚就上交所关于公司重大资产置换的问询函作出部分回复。在回复中，日播时尚称“不存在内幕信息泄露的情况”。回函公告中，日播时尚披露了此次重大资产重组筹划的具体过程、重要时间节点。根据公告信息，交易双方及中介机构相关人员首次接洽的时间是 2023 年 5 月 1 日，商议和决议内容是“各方表达重大资产重组意向”；5 月 3 日进行商议筹划，各方确认重大资产重组意向，并商讨重大资产重组意向书的内容，并确定后续事项安排；5 月 8 日“形成意向”，各方签署《资产重组意向书》，发布重大资产重组继续停牌公告，明确后续事项重要时间节点；5 月 15 日各方签署《重大资产置换及发行股份购买资产协议》，召开董事会审议相关事项并形成决议，发布重大资产重组预案、复牌公告等相关公告。

5、中消协开查“强制关注公众号” 律师建议完善立法加大处罚

摘要：6 月 19 日，中国消费者协会表示，针对扫码消费中存在的问题，将在全国开展“反对强制关注公众号”消费监督，消费者可通过电子邮件（ccaxfjd@cca.org.cn）反映。中消协将视情节，采取提示警示、约谈劝喻、支持消费者诉讼、提起消费民事公益诉讼等方式，维护消费者权益。中消协表示，经营者要求消费者关注公众号，并通过公众号下单、结账、开具发票，可获得阅读量和关注量，通过广告和信息推送等方式吸引消费者更多关注和再次光顾，可增强用户黏性。但任何企业的任何商业行为，都必须尊重消费者意愿，维护消费者合法权益。经营者将关注公众号或使用 APP、小程序作为消费者行使权利或享受服务的前提，并在此过程中获取与服务无关的个人信息的行为，已违反《消费者权益保护法》《个人信息保护法》相关规定，侵害了消费者的自主选择权、公平交易权，消费者有权拒绝和举报。

6、给个手机号就能“人肉搜索”？揭秘隐蔽的网暴水军

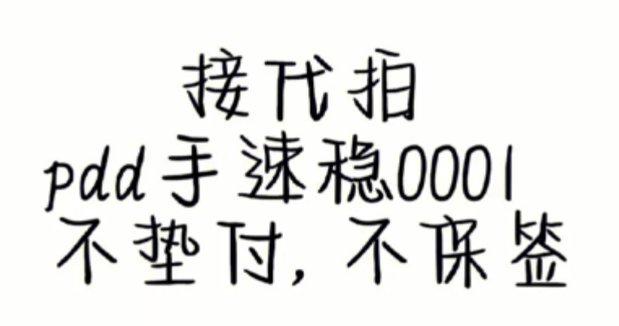


摘要：近日，三部门就惩治网暴公开征求意见。对在信息网络上制造、散布谣言，采取肆意谩骂、恶毒攻击、披露隐私等方式公然侮辱他人等行为依法严惩。记者调查发现，普通人被网暴的门槛越来越低，背后有花钱随意“轰炸”骚扰他人，“水军”推手刷流量等产业。随着政策法规的持续收紧，网暴产业链也越来越隐蔽。

7、谴责虐猫却被曝光信息？隐私泄露魔爪必须斩断

摘要：近日，多位明星针对网络热传的虐猫事件发声，表态反对“处刑式虐待动物”，却被不法分子盯上，个人信息遭到曝光。

8、演唱会等门票实名制后 代拍者要求买家提供个人信息 通过“代拍”抢门票小心泄露个人信息

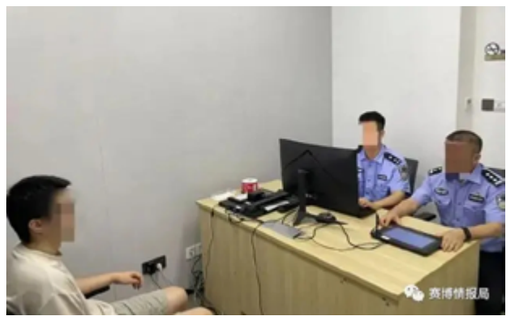


摘要：6 月 15 日，阿根廷国家足球队与澳大利亚国家足球队在北京工人体育场进行一场邀请赛，知名球星梅西将参赛。据了解，该赛事散票座位分六个档位，票价最低为 580 元，最高为 4800 元。第一波官方票开票半小时后，所有门票售罄。6 月 8 日，北青报记者在二手平台搜索关键词“梅西”发现，有卖家加价代拍该赛事门票，一张门票代拍费用从 500 元至上千元不等，抢不到票不收费，但因实名制购票要求，需要用买家的个人信息登录账号抢。

9、上海警方：持续打击涉网犯罪 净化网络空间

摘要：6 月 15 日电，DDoS 攻击，网络勒索病毒，刷量控评，有偿删帖 …… 今天上午，上海市公安局新闻发布会通报，今年以来，根据公安部部署，上海市公安局深入开展“净网 2023”专项行动，持续打击涉网违法犯罪，全面治理网络乱象。行动期间，上海警方紧密结合“砺剑 2023”系列专项打击整治行动，重拳出击、重点打击黑客攻击破坏、网络黑灰产、网络水军等违法犯罪，清理有害信息 1.1 万余条，关停违法账号 320 余个。

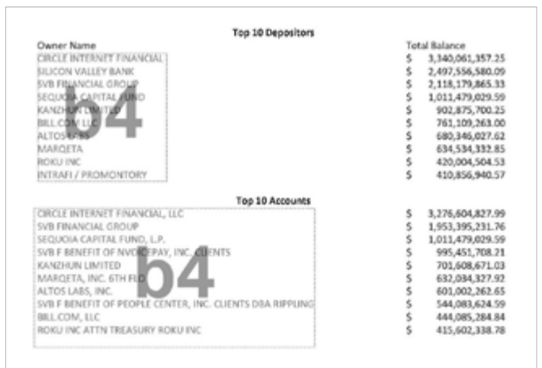
10、国内第二起！浙江某公司为政府部门开发系统时数据泄露，被网安部门罚款 100 万元



摘要：2023 年 6 月 16 日，据报道 2023 年 3 月，浙江温州公安网安部门在查处一起涉数据安全违法案件时发现问题。浙江某科技有限公司为浙江某县级市政府部门开发运维信息管理系统的过程中，在未经建设单位同意的情况下，将建设单位采集的敏感业务数据擅自上传至租用的公有云服务器上，且未采取安全保护措施，造成了严重的数据泄露。浙江温州公安机关根据《中华人民共和国数据安全法》第四十五条的规定，对公司及项目主管人员、直接责任人员分别作出罚款 100 万元、8 万元、6 万元的行政处罚。

国外

1、外媒：FDIC 意外泄露硅谷银行最大客户的详细信息



Top 10 Depositors

Owner Name	Total Balance
CIRCLE INTERNET FINANCIAL	$ 3,340,061,357.25
SILICON VALLEY BANK	$ 2,497,556,580.09
SVB FINANCIAL GROUP	$ 2,118,179,865.33
SEQUOIA CAPITAL FUND	$ 1,011,479,029.59
KANZHUN LIMITED	$ 902,875,700.25
BILL.COM, LLC	$ 761,109,263.00
ALTOS LABS	$ 680,346,027.62
MARQETA	$ 634,534,332.85
ROKU INC	$ 420,004,504.53
INTRAFI / PROMONTORY	$ 410,856,940.57

Top 10 Accounts

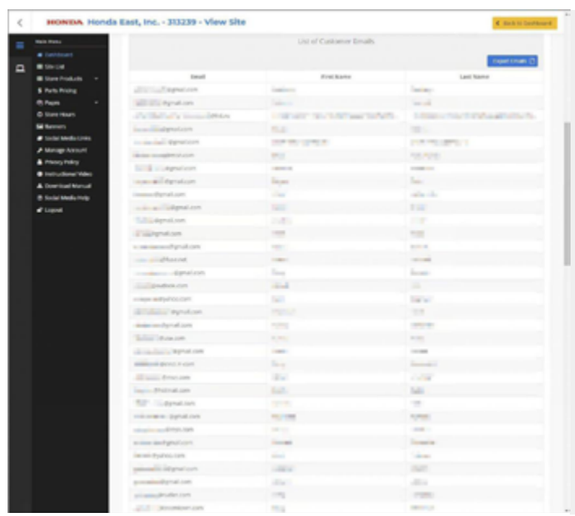
CIRCLE INTERNET FINANCIAL, LLC	$ 3,276,604,827.99
SVB FINANCIAL GROUP	$ 1,953,395,231.76
SEQUOIA CAPITAL FUND, L.P.	$ 1,011,479,029.59
SVB F BENEFIT OF NVIDIAPAY, INC. CLIENTS	$ 995,451,708.21
KANZHUN LIMITED	$ 701,608,671.03
MARQETA, INC. 6TH FLO	$ 632,084,327.92
ALTOS LABS, INC.	$ 601,002,262.65
SVB F BENEFIT OF PEOPLE CENTER, INC. CLIENTS DBA RIPPLING	$ 544,083,624.59
BILL.COM, LLC	$ 444,085,284.84
ROKU INC ATTN TREASURY ROKU INC	$ 415,602,338.78

摘要：美国联邦存款保险公司（FDIC）意外地向媒体透露了硅谷银行最大客户的详细信息。该名单显示，硅谷银行最大的储户包括红杉资本等科技巨头。据悉，彭博社通过《信息自由法》获得了这些新文件，FDIC 在没有事先编辑一些关键细节的情况下意外地移交了这些文件。据该媒体报道，FDIC 要求媒体不要公布这一名单，“因为其中包括机密的商业或财务信息”。尽管如此，获得名单的媒体还是公布了其中的一些细节。

2、因遭黑客攻击 美国数百万人信息泄露

摘要：据美国有线电视新闻网（CNN）当地时间 6 月 16 日报道，在一场全球性的网络黑客攻击中，美国数百万人的信息遭到泄露。据悉，黑客攻击影响了 350 万持有驾照或州身份证的俄勒冈州居民，路易斯安那州所有持有上述文件的居民信息也被泄露。报道称，这场大规模的黑客攻击可能已经暴露了全球数百个组织的数据，危及了包括美国能源部在内的多个美国联邦机构。

3、本田电子商务平台漏洞暴露客户数据



摘要：安全研究人员公开了对本田电动商务平台（用于动力设备、船舶和园艺产品）发现的重大漏洞的具体细节。该漏洞使得任何人都可以重置任何账户的密码，因此存在未经授权的访问风险。这位研究人员在今年年初发现了这些安全漏洞和数据泄露问题，并于三月中旬通知了本田公司他的发现。供应商立即承认了这些问题，并对这位白帽黑客的努力表示了祝贺，但由于缺乏漏洞赏金计划，未对他进行任何赔偿。本田公司表示未发现任何恶意利用的证据。

4、保险业遭受 12 倍以上的网络攻击

摘要：根据 Indusface 的应用程序安全状况报告，保险业是 2023 年第一季度遭受攻击最多的行业，受到的攻击是其他任何行业的 12 倍。同年的另一份报告显示，保险业在 114 个网站上发生了 49,844,877 次网络攻击。平均而言，该行业的每个应用程序都会受到 430,000 次攻击，这与所有行业中每个应用程序平均受到 450,000 次攻击非常相似。

5、数百万新冠疫苗接种数据泄露？印度卫生部否认，信息技术部意见不一

摘要：当地时间 6 月 12 日，印度卫生部公开否认了关于其新冠疫苗接种数据库发生泄露的报道，然而印度政府机构内部的不同声音与印度媒体的报道表明，该数据库是否发生泄露仍然值得质疑与持续关注。

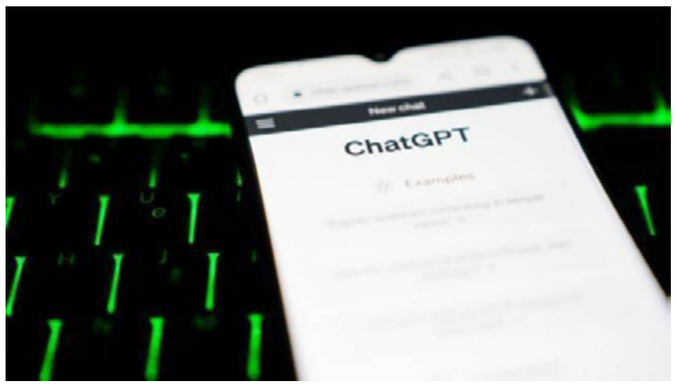
6、RepoJacking 攻击影响数百万 GitHub 库

摘要: AquaSec 安全研究团队 Nautilus 分析了 125 万 GitHub 库，发现其中 2.95% 可能受到 RepoJacking 攻击的影响。GitHub 库总数超过 3 亿，按照 2.95% 的比例，超过 900 万项目受到该攻击的影响。

7、OneNote 文档已成为新的恶意软件感染载体

摘要：OneNote 文档已成为一种新的感染媒介，其中包含在与文档交互时执行的恶意代码。Emotet 和 Qakbot 以及其他高端窃取器和加密器是使用 OneNote 附件的已知恶意软件威胁。目前已观察到使用 OneNote 进行恶意软件传递的电子邮件活动具有相似的特征。尽管消息主题和发送者各不相同，但几乎所有的活动都使用独特的消息传递恶意软件，并且通常不使用线程劫持。消息通常包含 OneNote 文件附件，主题包括发票、汇款、财产和季节性主题 (如圣诞节奖金) 等。2023 年 1 月中旬，安全研究人员观察到演员使用 URL 投递 OneNote 附件，这些附件使用相同的 TTP 执行恶意软件。这包括 2023 年 1 月 31 日观察到的 TA577 活动。

8、10 万多个 ChatGPT 登录凭证被泄露到暗网上



摘要：一家新加坡网络安全公司发现，在过去几年中，有超过 10 万名使用 ChatGPT 等聊天工具的在线用户的登录凭证被泄露并在暗网上进行交易。根据安全研究人员的说法，信息窃取者会非法获取收集任何重要的东西，无论是目标机器的信息、cookies 和浏览器历史，还是文件等等信息。黑客们经常通过在暗网上转售这种信息以及自己使用这种信息来赚钱。例如，一些流行应用程序的受害者的用户名和密码的日志经常会被传送到网络市场。

9、新的 Cactus 勒索软件可自行加密，以逃避反病毒软件

摘要：一个名为 Cactus 的新型勒索软件团伙一直在利用 VPN 设备中的漏洞，对“大型商业实体”的网络进行初始访问。至少从今年 3 月开始，Cactus 勒索软件团伙就一直处于活跃的状态，并向受害者索要大笔赎金。虽然这伙新的威胁分子采用了勒索软件攻击中两种常见的策略：文件加密和数据窃取，但它增添了自己的手法以免被发现。

10、勒索软件攻击者正在利用加密货币矿池进行洗钱

摘要：根据报道，像伊朗这样被制裁的国家已经开始把使用加密货币挖矿，来作为一种防止传统金融系统收缩的方法。在最近的攻击事件中，网络安全公司 Mandiant 还披露了 Lazarus Group（一个臭名昭著的朝鲜黑客组织）是如何将被盗的加密货币，如比特币，然后租赁云采矿服务进行加密货币的挖掘。网络犯罪分子利用偷来的加密货币，然后使用合法的方式开采 " 干净 " 的货币，然后利用不同的业务来洗钱。据 Chainalysis 称，这些常见的网站中有一个是目前还未命名的 " 交易所 "，该交易所已被确认从与勒索软件活动有关的钱包和矿池中收到了 " 大量的资金 "。

亿赛通亮相福建省工业数据安全工作会议，掀起安全新风潮

5 月 31 日，福建省工业数据安全工作会议在福州召开。会议由省工业和信息化厅指导，晋安区政府、省电子产品监督检验所、省数据安全产业发展联盟联合主办。亿赛通凭借良好的客户口碑及业内地位，受邀参与本次工作会议并就新形势下的数据库运维问题展开深入讲解。

福建作为工信部工业数据安全管理试点省，从数据安全管理、防护、评估、产品推广、风险监测等五方面开展试点工作，在数据治理探索和数据产业培育上取得了实质性成果，以总评第一的成绩成功获评 5 个成效突出地区之一。并且会议要求，全省重点工业企业要统筹发展和安全，把安全摆在突出位置，加强管理制度建设，加大人员、资金、技术等投入。通过各方共同努力，全面提升福建省工业数据安全管理能力水平，为数字福建建设、数字经济发展，筑牢数据安全屏障，以新安全格局保障新发展格局。

随着数字经济产业的快速发展和新兴科技在企业的广泛运用，亿赛通顺应企业新的业务场景所面临的数据安全风险问题，对企业数据安全运维能力提出见解，实时推出满足企业需求的数据库运维管理平台，可以及时解决企业在数据库运维过程中所面临的身份认证、数据脱敏、行为审计、统计分析等问题。

01、运维工单管理

运维申请支持：访问源、访问对象、运维行为、执行时间范围等维度细颗粒化行为申请，并支持周期性代理运维的申请与运维执行能力。

02、敏感数据脱敏

通过灵活应用脱敏规则，脱敏规则包含了敏感数据特征以及对于这类数据的脱敏算法。灵活地结合多条脱敏规则、排列优先级，有针对性地满足脱敏需求。

03、身份认证管理

提供多因子运维身份认证机制，包括：Ukey、Web 口令认证、审批口令认证。解决运维身份鉴别及权限安全控制问题。

04、运维行为审计

根据制定的审计规则对捕获的 SQL 语句进行专业的 SQL 语法分析，并根据 SQL 行为特征和关键特征，实现高效精准的审计分析。

05、访问检测防御

针对不同的运维人员，提供敏感表操作权限、访问行数和影响行数控制、限制 NO WHERE 查询更新，同时配合 SQL 黑白名单，对风险行为快速监测防御。

06、行为统计分析

多层面统计与分析，准确掌握数据库安全态势，快速锁定风险目标。支持数据库统计下钻与分析，进一步查看详细的数据库操作行为。

除数据库运维安全管理系统外，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，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。

随着数据安全态势愈发严峻化，现有客户对数据安全的期望也在不断的变化，不仅要通过产品来满足需求，更对前期规划及后期运维服务提出了更高的标准，高质量的数据安全体系建设不仅可以进一步加强客户安全体系的能力，同时也可以加深安全厂商与企业客户双方的粘性，加深对企业的了解，对症下药。亿赛通基于产品的自创研发、安全体系的建设，帮助客户得到智能化的安全体验，与企业实现安全能力共建，为企业安全保驾护航。

亿路同行 | 2023 亿赛通渠道会石门齐聚，一起驶向更远的未来

6 月 7 日，以“同舟共冀 亿路同行” 为主题的 2023 亿赛通渠道会石家庄站顺利召开。亿赛通与渠道伙伴分享渠道战略布局、解读渠道合作政策、剖析商业机会、洞见亿赛通核心产品竞争力，助力渠道伙伴健康稳健发展。

亿赛通石家庄办事处首席代表为大会致辞，他强调，“十四五”提出“加快数字化发展 建设数字中国”，《“十四五”大数据产业发展规划》将“筑牢数据安全防线”作为主要任务之一。市场上产品体系逐渐完善，场景日益丰富。面对数据安全产业新机遇，亿赛通将持续坚持渠道战略不动摇，基于“开放 + 共赢”的渠道理念，为渠道伙伴构建阳光、透明的商业环境，实现用户、渠道伙伴、亿赛通的“三赢”。

作为中国数据安全专家，亿赛通二十年来持续加大研发投入，专注产品开发、技术创新和安全能力研究，具备完整可靠的合规产品矩阵。通过数据安全管理、数据泄露防护、数据库安全、数据安全流转等安全产品的持续赋能，形成针对各场景的解决方案，围绕产品、服务、运营，构建公司核心竞争力，为渠道伙伴提供有力支撑。为进一步实现各场景的精细化覆盖，亿赛通拉动和持续完善数据安全建设框架，助推各行业数据安全建设的实施、落地、完善和持续运营。

亿赛通渠道业务部高级总监李荣刚向来宾介绍了亿赛通渠道战略发展之路。他强调，渠道战略发展的核心是对公司核心价值观的认可，公司倡导“以专业的产品和服务为客户筑牢数据安全底座”的企业愿景，通过不断优化组织结构、考核体系和系统流程，重塑渠道伙伴体系和管理机制，加大资源投入与渠道赋能，构建公平、公正、公开的渠道架构和政策，以此加速渠道化战略发展落地。下一步，希望通过我们的产品、解决方案、安全运营能力、人才培养体系和专业的安全服务能力与河北的渠道伙伴一起，合力服务客户，实现价值创造共赢。

本次大会汇集了河北地区安全行业的百余位渠道伙伴，通过本次大会，让大家走进亿赛通，了解亿赛通，增进感情，加强信心。同时，会上亿赛通为本年度签约渠道举行了授牌仪式并表彰了优秀渠道。

另外清风网安、河北奇迅两家渠道伙伴代表作为亿赛通优秀渠道伙伴上台发言，他们表示自合作以来，在亿赛通的支持下，打造了行业内多个安全标杆项目，获得了用户的一致好评。伴随着亿赛通渠道体系的逐步完善，接下来也将全力配合，积极投入，希望在不久的将来，双方以及在座的各位新老朋友能展开深层次的合作。

后续，亿赛通数据安全专家对“新一代电子文档安全管理系统”进行了重点介绍，他谈到，目前数据泄露发生的重点行业包括政府、金融证券、运营商、互联网、教育培训、能源、制造业等。随着数据泄露频发造就了行业客户的安全需求升级，因此安全企业自身的能力结构升级势在必行。亿赛通基于二十年安全实践以及对未来数据安全态势走向的深度思考，融入新的安全要素，提出了“分放管服”数据安全建设理念，以理念为指引，构建集“资产盘点、分类分级、溯源分析、加密防护、安全流转、数据水印、介质管控、外发权限控制、系统防护、终端全覆盖”的安全技术能力，达到“数据保护好、场景覆盖全、策略自动化、服务保障快、运维要省心”的防护效果。

最后亿赛通行业解决方案专家为大家针对金融行业、医疗行业及数据出境进行详细讲解。他表示，面对政策、经济、

文化等多方面的背景因素，当下金融和医疗行业的数据安全及数据治理尤为重要。由于金融和医疗数据比较敏感，不仅有市场监管需求，还有内部安全需求的考量。在数字经济飞速发展的当下，数据由“静态”转为“动态”，数据共享流通更加频繁，数据集中处理、广泛共享、交叉使用成为刚性业务需求，对金融和医疗行业的的数据安全防护能力和数据治理能力提出新的要求。亿赛通紧抓各行业发展的重点方向及机会点，以丰富的解决方案与项目落地案例，全面加速推进行业客户合规实践。

石家庄办事处的领导、同事严阵以待，致力为渠道伙伴及客户提供及时、有效的服务，期待大家携手，同舟共冀，亿路同行，赢得更为广阔的数据安全市场。未来，亿赛通将长期坚持渠道战略不动摇，构建多赢的渠道伙伴关系，衷心希望能与所有渠道伙伴共同发展、共同成长、共同服务客户。

亿说安全 | 第一期：数据安全运营管理平台专业讲解

随着各行各业数字化转型加速，“数据化生存”已逐渐成为人类社会运行的常态，数据在公共管理、科学研究、企业营销等领域发挥着重要作用。数据作为当今世界最为重要的资源之一，对于现代社会的发展具有难以估量的价值。但随之而来的数据滥用、个人隐私泄露等问题却令人担忧。为了解决各行业数据安全困扰，亿赛通推出《亿说安全》节目，邀请产品专家定期分享行业发展趋势、热点问题、产品创新方向等内容。

本期邀请亿赛通平台产品负责人详细讲解平台产品的部署革新。

近两年，数据安全开始偏向平台化、体系化发展，您认为企业用户在建设以数据为中心的平台安全中面临着哪些困难？应该如何解决？

企业在进行数据化建设时，主要存在以下三个技术难点。一是：数据识别范围不全。目前的数据安全建设主要针对的是数据库的结构化数据，对于半结构化、非结构数据识别能力不足。二是，数据安全治理的效率和自动化水平偏低。数据安全治理过度依赖人工，虽然安装实施了众多产品，但是能够实际落地的项目少之又少。三是缺乏数据的统一运营和管理能力。数据安全平台体系大多缺乏自上而下的顶层规划，数据接口标准、技术标准等缺乏统一规范，导致各平台多为半封闭状态。

面对这些问题，亿赛通推出了数据安全运营管理平台。首先基于长期在非结构化数据识别的积累，运营管理平台不仅能够管理结构化数据，还能够管理终端及文件服务器中的非结构化数据。其次，针对数据治理自动化程度低的问题，亿赛通提出了数据治理智能化体系 DSIG，采用智能识别引擎完成数据梳理，将策略进行自动导入，实现在识别、防护、监测、运营方面的综合管理，降低人工成本。此外对于统一运营管理，亿赛通数据运营管理平台已经实现与各个安全能力组件的联动，覆盖云、网、端、各个节点的立体化管理。

我们知道亿赛通的数据安全运营管理平台已经投入市场，并且 3 月还入选了安全牛的《数据安全管控平台应用指南》，那在平台发展的这段时间里，数据安全运营管理平台与刚开始的产品相比有哪些明显的升级之处呢？

在今年 2 月份我们平台进行了一次重要版本发布，其中将平台从资产梳理、策略运营、智能分析、响应处置、态势感知 5 大能力进行了全新定义。该版本还对数据分类分级策略关联、自动化编排响应处置做了功能优化，新增了数据血缘分析、僵尸资产分析、数据资产分布态势，集团化分级管理等重要功能，同时还进一步扩充了国产化硬件的支持范围，包括 3 款飞腾 CPU、2 款海光 CPU、1 款国产操作系统。

那根据您的项目经验来看，就是目前哪些行业的客户对咱们平台产品的这个需求是最强烈的。您能否举例给大家介绍一下，不同行业做平台产品的侧重点有什么不同吗？

从当前数据安全发展阶段来看，数据安全治理主要驱动力仍然是合规，同时结合目前我们已经落地的平台项目来看，平台产品客户主要集中在政府、电信、金融、医疗这类行业客户。

政府行业主要是政务大数据局来负责政府数据业务的统筹治理，通过建立数据管理组织体系，解决“数据孤岛”问题，使数据多元联动，发挥更好效用，服务经济，引领产业升级。从建设路径上来看，平台上层建设优先，在完成整体框架建设后向各地方进行能力推进。电信行业存储了大量的个人和企业基础信息，结合电信行业的行业规范，目前的数据安全平台建设仍以数据防泄露为重点，主要关注个人隐私数据的安全建设。

此前我们公司已经有了态势感知平台，如果企业已经部署了态势感知平台，那还需要再部署数据安全运营管理平台吗？

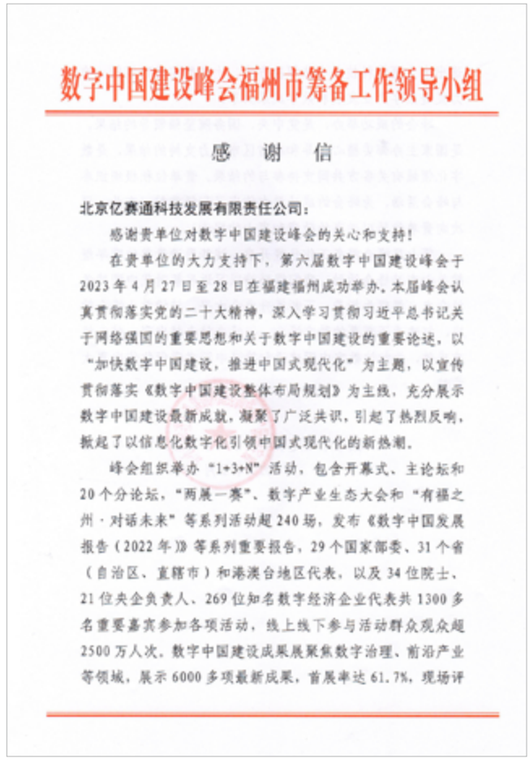
需要，这两类平台并不冲突。企业如果前期网络安全建设时部署了态势感知平台，但是他侧重于网络侧的安全态势监管和运营。我们的数据安全运营管理平台以数据为中心，能力是通过感知云、网、端等多源异构海量数据，实现数据资产管理及分类分级、数据安全策略联防联控、数据安全事件综合分析、数据追踪溯源分析、数据安全风险应急响应及处置、数据安全风险态势感知。

在这一年里，我们看到有很多友商也陆续推出数据安全平台类的一些产品，那么用户应该如何选择合适的方案？有哪些关键的能力指标需要关注？然后我们的一些突出优势有哪些呢？

此前 Gartner 将数据安全平台定义为以数据安全为中心的产品和服务，所以我觉得“平台产品”提供给客户的平台不仅仅是一个产品，而是应该是一套综合的解决方案。这也正是亿赛通的优势，我们具备从业务梳理 - 分类分级 - 策略制定 - 技术管理 - 持续运营全流程的数据安全治理解决方案。

亿赛通产品负责人针对不同行业的需求做出了总结，可以看出我司产品通过这一年的实战已经拥有完善的产品体系。作为中国数据安全专家，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，历经 20 余年的技术积累和上万个交付项目的沉淀，凭借自身的产品技术优势，帮助企事业单位切实做到数据资产可视、数据威胁可管、数据风险可控、数据血缘可溯，为企业守好数据安全防护的大门。

感谢信 | 亿赛通完成 2023 数字中国创新大赛重要支撑工作



数字中国建设峰会福州市筹备工作领导小组

感　谢　信

北京亿赛通科技发展有限责任公司：

感谢贵单位对数字中国建设峰会的关心和支持！

在贵单位的大力支持下，第六届数字中国建设峰会于2023年4月27日至28日在福建福州成功举办。本届峰会认真贯彻落实党的二十大精神，深入学习贯彻习近平总书记关于网络强国的重要思想和关于数字中国建设的重要论述，以“加快数字中国建设，推进中国式现代化”为主题，以宣传贯彻落实《数字中国建设整体布局规划》为主线，充分展示数字中国建设最新成就，凝聚了广泛共识，引起了热烈反响，掀起了以信息化数字化引领中国式现代化的新热潮。

峰会组织举办“1+3+N”活动，包含开幕式、主论坛和20个分论坛，“两展一赛”、数字产业生态大会和“有福之州·对话未来”等系列活动超240场，发布《数字中国发展报告（2022年）》等系列重要报告，29个国家部委、31个省（自治区、直辖市）和港澳台地区代表，以及34位院士、21位央企负责人、269位知名数字经济企业代表共1300多名重要嘉宾参加各项活动，线上线下参与活动群众观众超2500万人次，数字中国建设成果展聚焦数字治理、前沿产业等领域，展示6000多项最新成果，首展率达61.7%，现场评选出十大硬核科技、十佳解决方案、十佳数字普惠案例，有力促进数字产业发展和数字成果共享。

峰会的成功举办，是党中央、国务院坚强领导的结果，是国家主办部委精心指导和各省区市全力支持的结果，是数字化领域有关各方共同支持参与的结果。贵单位积极组织参与峰会活动，为峰会的成功举办作出了积极贡献。在此，再次向贵单位致以崇高的敬意和衷心的感谢！

第七届峰会筹备工作已经开启，诚挚恳请贵单位明年继续关心支持峰会活动。我们将坚持以习近平新时代中国特色社会主义思想为指导，不断提升办会水平，持续放大峰会效应，打造永不落幕的数字峰会，把峰会越办越出彩、越办越有成效，为加快数字中国建设和推进中国式现代化作出更大贡献。

数字中国建设峰会福州市筹备工作领导小组

2023年5月30日

为全面贯彻落实党中央、国务院的决策部署，聚智创新、示范引领，进一步激发社会各界建设数字中国的积极性、主动性、创造性，2023 数字中国创新大赛如期召开。其中，网络数据安全赛道此前已在福州圆满落幕。亿赛通基于在数据安全领域的二十年技术积累，受邀作为赛事支持单位支撑本次大赛，此前，亿赛通接到了主办方的感谢信，感谢信中肯定了“亿赛通在 2023 数字中国创新大赛网络数据安全赛道的支持工作工作中发挥了重要作用，做出了重要贡献。”

赛事遵循开放合作办赛、高规格机构执行、贴近产业应用、多赛道并行的原则，面向产业实际需求，设置了数字党建、数字城市设计、数据开发、信创、产业元宇宙、数字智造、网络数据安全、数字人才、青少年 AI 机器人等 9 个赛道，多角度展现数字中国建设创新成果。赛事聚集了 1000 余支队伍，电信和互联网、金融、能源、教育等重点行业领域的近 3000 余名数据安全专业选手报名参赛。

随着各行业数字化转型步伐推进，数字化面临着复杂多变的网络安全风险挑战。赛事设置网络数据安全赛道旨在切实解决数据安全产业发展中的实际问题为目标，发挥数据安全技术创新、成果转化、人才培养等典型示范带动作用，推广优秀经验和成果，助力我国数据安全产业发展。

亿赛通以专业的产品和服务为客户筑牢数据安全底座，护航各行业用户的数字化安全转型，推进数字经济发展。其中，独特的“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，让企业步步为营，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，保障涉数据业务合法合规，业务安全可持续运营。在理念的驱动下，将产品整合，达到管理和技术并重，再发展成基于用户场景和具体业务提供定制服务，通过组织、制度、技术、人员四大体系的同步规划、同步建设、同步运行，共同保障数据安全。

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，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，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。

下一步，亿赛通将继续支撑国内各项网络数据安全赛事、大会等活动。面向数据安全产业实际需求，进一步激发社会各界建设数字中国的积极性、主动性、创造性，从而更好地赋能经济社会高质量发展。

对话亿赛通梁步庭：浅谈数据库安全产品的革新之路

北京亿赛通科技发展有限责任公司数据库安全产品总监梁步庭

【IT168 评论】近年来，数据泄漏事件层出不穷，来自外部攻击威胁和内部监守自盗愈演愈烈。数据泄露事件对企业以及个人造成了严重经济损失和不良影响，严重的甚至危及国家安全。如某全球知名的硬盘厂商，遭到黑客攻击，攻击者号称窃取了包括大量客户信息，导致大约 10TB 的重要数据泄露。国内某互联网营销解决方案供应商，技术人员删除服务器内数据，导致数百万用户无法正常使用该公司服务，造成超亿元的经济损失。

伴随大数据、人工智能等新型技术的逐步成熟与行业应用，海量数据存储已成为常态。数据库作为最重要的数据存储工具之一，数据泄露事件数量正以惊人的速度逐年增加，数据库安全正面临有史以来最为严峻的挑战。在此大背景下，IT168 走访亿赛通，独家对话北京亿赛通科技发展有限责任公司数据库安全产品总监梁步庭，深刻解读数据库安全产品的革新之路。

数据库安全迎来发展的历史机遇

根据信通院、中商产业研究院整理的‘2017-2022 年，我国数据安全市场规模预测趋势图’ 中显示，2017-2022 年，我国数据安全市场规模由 22.9 亿元增长至 99.2 亿元，复合年均增长率达 32.6%。预计 2023 年我国数据安全市场规模将达 109.5 亿元。

数据库作为主要的数据存储载体之一，承载了大量的核心数据资产，被攻击的可能性和泄露风险越来越高，一旦出现数据泄露所带来的损失不可估量，所以数据库安全至关重要。在梁步庭看来，数据库安全面临的安全威胁，主要有外部威胁和内部泄密两类。外部威胁常见的：数据库系统漏洞、弱密码、SQL 注入等。而内部泄密则主要包括：账号滥用、非法操作、运维不当等内部人员的无意识或主动泄密等行为。以数据库为主体的数据泄露问题，已经涉及金融、电信、教育、医疗、政府、企业等多行业和个人。数据泄露给个人、企业、社会以及国家造成了严重的负面影响及危害。因此，数据库安全也越来越被大众所熟知和关注。

从国家政策角度来看，我国先后出台《网络安全法》、《数据安全法》、《个人信息保护法》、《密码法》、《关键信息基础设施安全保护条例》，旨在进一步提升国家数据安全保障能力，全面维护国家主权、安全和发展利益，以及应对数字经济的快速发展需要。2023 年 5 月 1 日正式实施的《关键信息基础设施安全保护要求》（GB/T 39204-2022），数据安全保护要求更加明确和清晰，包含了数据安全保护计划、数据分类分级、境内存储、重要数据和个人信息保护、容灾备份、数据安全风险评估、数据处理活动全流程保护等多个数据安全保护要求。

梁步庭还提到，早些时间 Gartner 公布的‘2022 年数据安全技术炒作周期图’显示，数据库审计与防护、数据库脱敏、数据泄露监测等数据安全防护技术已经完全成熟脱离周期曲线。但就目前行业化技术应用趋势和更新速度来看，当前成熟的安全技术方案已经越来越难应对和提供更好的安全支撑。未来，随着应用技术和新数据业务的需要和不断拓新，将带动数据库技术的快速更新和发展，数据库安全产品作为数据库侧最主要的安全屏障，需要顺应新的变化进行安全能力的迭代和升级。

解锁数据库安全产品，化解企业选型之难

当前，数据库安全建设已经不再是之前“头疼医头，脚疼医脚”式的单节点防护方式。亿赛通的客户越来越多关注如何能够在快速理清数据库资产等级与敏感度情况下，建立系统化体系化的数据资产防护能力，实现灵活的细粒度的数据安全保护目标。数据库安全产品作为数据库安全防护的最终落地实践工具和建设优略的标尺，如何选择就变得尤为重要，亿赛通深耕数据安全领域二十年，梁步庭作为亿赛通数据库安全产品负责人建议：

1) 构建“合规 + 安全”双轮驱动体系

企业数据库安全建设的基础不仅要满足合规要求，还需要构建“合规 + 安全”双轮驱动的体系化数据库安全整体防护方案。以合规驱动牵引形成数据库安全基线，推动提升数据库安全意识，保证数据库安全技术和防护手段的落地应用与持续更新。亿赛通的数据库安全解决方案已形成数据库安全闭环管理，实现数据库安全的可持续运营和迭代优化，为企业数据库安全建设赋予新动能。

2) 基于安全需求选择合适的安全产品

数据库安全产品截止目前，已经形成了：攻击检测、行为溯源、泄露防护、分析识别等多个细分类型，涉及大数据、云、应用、工控等多场景下的十余种安全产品和相关配套安全服务。由于安全能力侧重不同，企业用户应以自身业务特性和安全需求出发，选取适合企业自身的数据库安全产品，分步骤、分阶段进行数据安全建设。

3) 实践经验和创新能力是选择的关键

随着数据库类型和应用的不断更新和变化，数据库安全产品的选择，除了需要对数据库安全厂商是否有相关技术积累进行考察以外，还需要对数据库安全产品的实践经验和创新能力进行重点关注。如：机器学习、区块链、SSH 通道检测、漏洞检测、工单管理等当前较为热门的安全和管理能力，产品应可以根据用户的数据保护需求，按需模块化进行升级和扩展，不断提升和完善数据库安全能力。

总的来看，数据库安全市场规模在不断扩大，发展情形持续向好。数据安全的特性与业务贴近的比较紧密，当业务发生变化，数据库安全的技术和产品也会随之变化。当前，亿赛通在和客户对接的过程中发现数据库安全正在从单一节点化的产品，向业务化场景的产品变化。此外，多个成熟的安全技术能力还将整合在一起，形成横纵两向。数据库安全大环境的强势利好，企业将会以安全需求为驱动力，保护系统的核心数据资产安全，形成数据全生命周期的安全防护整体解决方案。

数据安全治理智能化 | 亿赛通助力打造工业互联网安全生产示范园区

2023 年 6 月 14 日由工业和信息化部、江苏省人民政府主办的工业互联网大会在苏州开幕，工业互联网“百城千园行”高端论坛同期举办，各地工业和信息化主管部门、通信主管部门、产业界以及新闻媒体 200 余人参会。论坛以“工赋园区·数智未来”为主题，聚焦工业互联网技术创新，赋能中小企业数字化转型，推动工业互联网高质量发展。亿赛通作为数据安全头部厂商，受邀出席论坛并做主题演讲。

论坛由工业和信息化部、江苏省人民政府主办，中国互联网协会与中国信息通信研究院、工业互联网产业联盟承办，中国信通院工业互联网与物联网研究所、《互联网天地》杂志社、中国信通院“智能 + 学院” 联合承办。工业和信息化部信息通信管理局一级巡视员王鹏，中国信息通信研究院党委书记、副院长宋灵恩，江苏省工业和信息化厅副厅长池宇，江苏省通信管理局副局长耿力扬出席论坛并致辞。中国互联网协会副理事长兼副秘书长何桂立出席论坛并作题为《推动工业互联网园区建设 助力数字经济高质量发展》的主旨报告，中国互联网协会副秘书长裴玮作为论坛嘉宾主持。

论坛上亿赛通副总经理张兰兰进行了《数据安全治理智能化体系助力打造工业互联网安全生产示范园区》主题分享。工业互联网数据安全关系总体国家安全，近年工业互联网数据安全事件频发， 针对工业互联网数据安全形势，结合亿赛通数据安全治理体系框架，提出数据安全治理智能化体系，通过分类分级系统，应用 AI 技术等措施实现工业数据安全治理建设的路径。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。

其中，数据安全运营管理平台综合了数据泄露防护、数据加密、数据库安全等多个核心产品，将产品从单一化部署转变为平台部署。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的风险。在一些分析类技术的使用上，例如 UEBA、规则匹配、勒索防护等。

下一步，亿赛通将继续支撑工业互联网“百城千园行”等活动。支持企业加快数字化转型，进一步激发社会各界建设网络强国、数字中国的积极和主动性，从而更好地赋能经济社会高质量发展。

亿路同行 | 2023 亿赛通渠道会相约合肥，群星闪耀共商安全大计

6 月 16 日，2023 亿赛通渠道大会合肥站已顺利召开。本次会议以“皖美绽放 亿路同行”为主题，会上重点分享了亿赛通的渠道战略布局及 2023 最新合作政策，剖析了区域内行业市场商机，并同期举行了渠道伙伴授牌仪式。

会议伊始，北京亿赛通科技发展有限责任公司合肥办事处首席代表在开场致辞中向各位合作伙伴讲述了亿赛通在安徽地区去年所取得的成绩，对过去一年和亿赛通风雨同舟的渠道伙伴们表示感谢。他表示，安徽地区资源禀赋优越，着力打造新型显示、集成电路、新能源汽车、人工智能、智能家电等 5 个世界级战略性新兴产业集群，是全国科教资源大声，并且合肥市综合性国家科学中心之一，未来 3-5 年，安徽的成长空间巨大。亿赛通将本着诚信至上、和谐共赢的原则，在未来的合作中，坚持以市场为导向，以客户为中心，在广阔的营销渠道中建立更多、更持久的利益共同体。

随后，北京亿赛通科技发展有限责任公司专家为与会嘉宾详细分析数据安全行业发展趋势。她提到，数字经济现已成为全球经济复苏和转型发展的关键驱动力。其中，产业数字化是发展主引擎，占数字经济比重 85%。由于数据成为生产要素，因此数据安全内涵不断扩展。数据安全产业顶层规划发布，数据安全治理合规要求日益完善，对数据安全的需求也日益复杂，建设多方联动的组织架构与以数据为中心的数据安全纵深防御技术体系是多数企业当前的工作焦点，长期来看如何培养复合型数据安全人才梯队、如何将安全工作贯穿于企业业务发展当中将是企业未来数据安全工作的重点。亿赛通八大服务模块支撑项目战略规划、组织设计与制度设计。亿赛通数据安全产品功能在向融合化、平台化迈进，将协同数据安全深化服务，助力数字化业务的安全、健康、有序发展。

北京亿赛通科技发展有限责任公司渠道业务部高级总监李荣刚向渠道伙伴介绍了亿赛通渠道战略转型之路，并详细介绍了 2023 年合作伙伴政策。他强调，工信部等 16 部门发布的《关于促进数据安全产业发展的指导意见》提出，到 2025 年，数据安全产业基础能力和综合实力明显增强，数据安全产业规模超过 1500 亿元，年复合增长率超过 30%。到 2035 年，数据安全产业进入繁荣成熟期。数据安全领域正在快车道高速前进。在亿赛通渠道发展过程中，公司不断优化组织架构、考核体系和系统流程，加速推进渠道转型落地，构建公平、公正、公开的渠道架构和政策，聚焦优质伙伴，将全行业全能力开放给渠道伙伴，共享商机，与合作伙伴一起创造价值，共谋发展。

北京亿赛通科技发展有限责任公司咨询顾问与伙伴们针对亿赛通核心产品进行了详细讲解，围绕新基建、勒索病毒、数据泄露等各方面问题，亿赛通设置合规产品矩阵，从数据安全管理、数据泄露防护、数据库安全、数据安全流转等 4 大方向 12 个产品模块对数据进行全生命周期防护。除此之外，单独搭配合规服务矩阵，从咨询规划、评估认证、运营服务对客户实施全面、到位、贴心的服务。在亿赛通合规产品矩阵中，具有突出特点的产品就是新一代电子文档安全管理系统、新一代数据泄露防护系统及数据库安全审计系统。在以上三个核心产品的支撑下，客户可以全局掌控数据资产全生命周期安全态势、多维度审计监测和态势感知报表、场景化多维度预警和审计追溯。达到安全与业务相结合、全面提升企业安全运营能力。

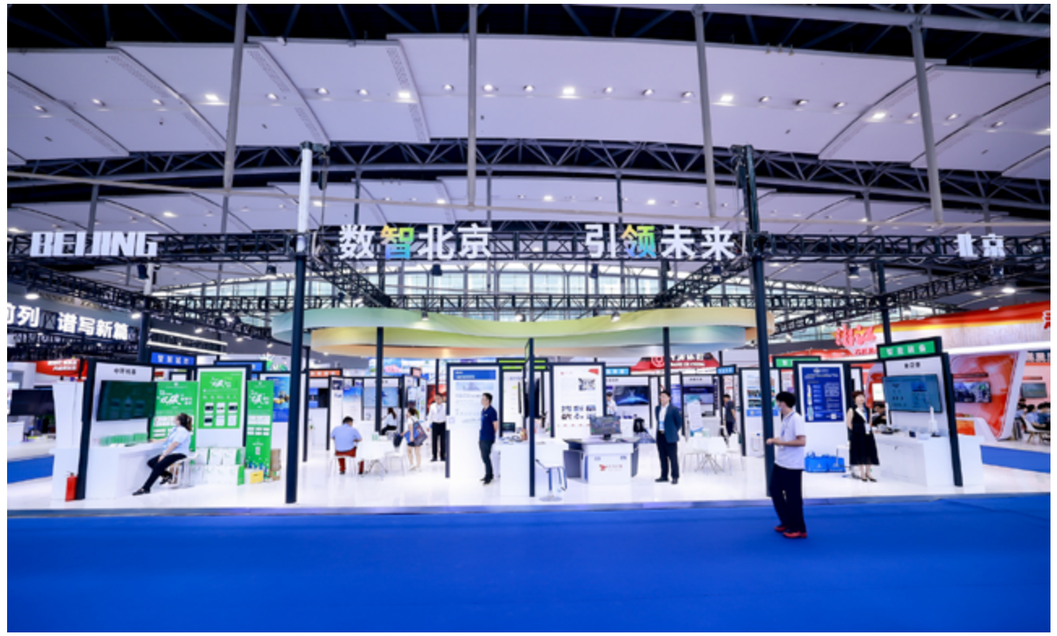
最后，亿赛通从金融、医疗两个行业视角出发，阐述了数字经济时代下如何为客户带来符合客户需求的安全产品。科技正在加速推行数字经济发展进程，企业在以数据为核心加速数字化转型的同时，也带来了区别于传统安全的风险问题，如何用治理方式去解决金融、医疗等行业的数据安全风险成为行业的重要命题。

当前，拥有丰富实践经验的厂商相对于行业用户而言更具有吸引力。亿赛通一直在技术变革中不断进行创新与突破，以客户为中心，构筑能够覆盖各类安全场景的全生命周期产品能力，赋能现代企业数字化发展，为客户提供更为全面、更加优质的数字化服务。

除了精彩的主题分享，亿赛通还在会中为本年度签约渠道举办了授牌仪式。

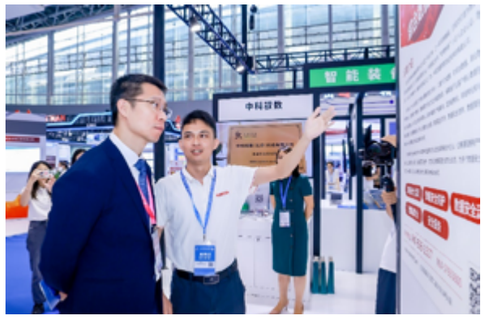
本次大会汇集了安徽区域安全行业的近百位渠道伙伴，通过本次大会，让更多合作伙伴走进亿赛通，了解亿赛通，增进感情，加强信心。未来，亿赛通将长期坚持渠道战略不动摇，构建多赢的合作伙伴关系，衷心希望能与所有合作伙伴共同发展、共同成长、共同服务客户，实现客户、合作伙伴、亿赛通的“三赢”。

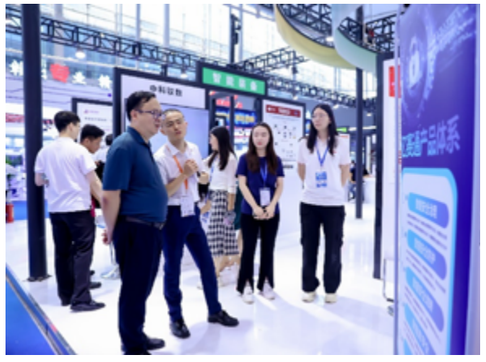
中博会 | 亿赛通携核心产品吹响数据安全冲锋号



第十八届中国国际中小企业博览会（以下简称中博会）于 6 月 27 日拉开帷幕。中博会作为国内外企业“展示、交易、交流、合作”的重要平台，已发展成为我国规模高大、影响广泛的为各企业提供专门服务的国际性展会，成为畅通国内大循环、联通国内国际双循环的重要抓手。智能数据是本届中博会的一大亮点，亿赛通凭借在数据安全领域拥有的 60 余款核心产品及 50 余项专利技术受主办方邀请，此次携综合数据安全解决方案亮相中博会现场。

据了解，到场嘉宾详细询问了亿赛通数据安全全生命周期解决方案的特点、优势及在广东省和全国的应用情况，了解了企业的发展情况及研发实力，并对产品给予了高度评价。





国家大力推行数字经济、数据安全，各行业根据行业特点推出针对性条例，如：建立组织架构，明确董事会、监事会、高级管理层及内设部门等职责要求；数据治理纳入公司治理范畴，建立自上而下、协调一致的数据治理体系；企业应当确立数据质量管理目标，建立控制机制，确保数据的真实性、准确性、连续性、完整性和及时性。由于新兴数字技术组合而成的万物互联，使得网络边界变得非常模糊，因此传统基于内、外网的安全防护模型已经不能够满足企业业务数据在生产、流转、处理等过程中全生命周期的数据安全要求。

而在亿赛通看来，高效的数据应用给企业带来巨大的业务价值，但如果没有数据安全的保障，则时刻面临着巨大的运营风险，两者之间是一个需要动态精准把握的平衡关系。但无论如何，这些企业都会将数据安全放在第一位，数据一定要为使用者而服务，因此这一理念映射出亿赛通具有针对和规划性的将客户需求放在第一位。同时意味着，亿赛通更贴近客户需求，也为营销端提出了新的挑战，面对不同客户对数据不同需求，能更了解客户的管控环境。

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，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，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。

亿赛通基于多年数据安全领域的研究和实践经验，将研究成果转化为持续输出的安全能力，从安全理念到技术落地，为满足客户的特殊需求，形成了一套综合数据安全管理体系，持续不断为用户输出优质的产品和方案。

亿聊安全 | 数安大事全知道

新闻概览

1. 国务院发布《商用密码管理条例》

2. 国家互联网信息办公室发布《个人信息出境标准合同备案指南（第一版）》

3. 国家互联网信息办公室发布《数字中国发展报告（2022 年）》

4. 网络安全审查办公室依法对美光公司在华销售产品进行了网络安全审查，美光公司在华销售的产品未通过网络安全审查

5. 工业和信息化部等九部门近日联合印发《质量标准品牌赋值中小企业专项行动（2023—2025 年）》

6. 工业和信息化部等十四部门联合印发《关于进一步深化电信基础设施共建共享 促进“双千兆”网络高质量发展的实施意见》

7. 国家市场监督管理总局部署开展首届“企业商业秘密保护能力提升服务月”活动

8. 国家市场监督管理总局正式发布实施《信息安全技术 关键信息基础设施安全保护要求》（GB/T 39204-2022）

9. 北京市科委、中关村管委会，市经济和信息化局，市发展改革委会同相关单位制定了《北京市促进通用人工智能创新发展的若干措施（2023-2025 年）（征求意见稿）》

10. 北京市经济技术开发区在京发布全国首个自动驾驶示范区数据安全管理办法

11. 国家互联网信息办公室有关负责人就《关于调整网络安全专用产品安全管理有关事项的公告》答记者问

12. 专家解读｜王小云：贯彻落实商用密码管理条例 推动我国商用密码事业高质量发展

13. 专家解读｜周汉华：商用密码管理法治化的一次重大飞跃——评《商用密码管理条例》修订

14. 专家解读｜杨建军：标准助力商用密码应用发展

15. 专家解读｜张振峰：贯彻《商用密码管理条例》推动商用密码科技创新发展

16. 专家解读｜左晓栋：《商用密码管理条例》修订为维护国家网络安全提供坚强法治保障

一、政策要闻

1. 国务院

（1）国务院发布《商用密码管理条例》—2023 年 5 月 24 日

《商用密码管理条例》于 2023 年 4 月 14 日国务院第 4 次常务会议修订通过，现予公布，自 2023 年 7 月 1 日起施行。

（来源：中华人民共和国中央人民政府）

原 文 链 接：https://www.gov.cn/zhengce/content/202305/content_6875927.htm

2. 国家互联网信息办公室

（1）国家互联网信息办公室发布《个人信息出境标准合同备案指南（第一版）》—2023 年 05 月 30 日

在《个人信息出境标准合同办法》即将实施之际，《备案指南》对个人信息出境标准合同备案方式、备案流程、备案材料等具体要求作出了说明，为进一步指导和帮助个人信息处理者规范、有序备案个人信息出境标准合同的指导性文件。

原 文 链 接：http://www.cac.gov.cn/2023-05/30/c_1687090906222927.htm

（2）国家互联网信息办公室发布《数字中国发展报告（2022 年）》—2023 年 5 月 23 日

按照夯实基础、赋能全局、强化能力、优化环境的战略路径，明确了数字中国建设“2522”的整体框架，从党和国家事业发展全局的战略高度作出了全面部署。

原 文 链 接：http://www.cac.gov.cn/2023-05/22/c_1686402318492248.htm

（3）网络安全审查办公室发布美光公司在华销售的产品未通过网络安全审查结论—2023 年 5 月 21 日

美光公司产品存在较严重网络安全问题隐患，对我国关键信息基础设施供应链造成重大安全风险，影响我国国家安全。为此，网络安全审查办公室依法作出不予通过网络安全审查的结论。按照《网络安全法》等法律法规，我国内关键信息基础设施的运营者应停止采购美光公司产品。

原 文 链 接：http://www.cac.gov.cn/2023-05/21/c_1686348043518073.htm

3. 工业和信息化部

（1）工业和信息化部等九部门近日联合印发《质量标准品牌赋值中小企业专项行动（2023—2025 年）》—2023 年 5 月 26 日

专项行动旨在通过质量提升、标准引领、品牌建设，不断增强中小企业竞争力和发展力，激发涌现更多专精特新中小企业，明确提升企业质量标准品牌意识、建立先进质量管理体系、推广质量管理数字化、提高产品质量水平等 15 项重点任务。

原 文 链 接：https://www.gov.cn/lianbo/bumen/202305/content_6876278.htm

（2）工业和信息化部等十四部门联合印发《关于进一步深化电信基础设施共建共享 促进“双千兆”网络高质量发展的实施意见》—2023 年 5 月 25 日

加快构建新发展格局，落实全面节约战略，以持续提升共建共享水平、促进“双千兆”网络高质量发展为目标，高效发挥“双千兆”网络基础支撑和融合赋能作用。

原 文 链 接：https://wap.miit.gov.cn/jgsj/txs/gzdt/art/2023/art_cd5706ee0fd8417492e42305337c0f6a.html

4. 国家市场监督管理总局

（1）国家市场监督管理总局部署开展首届“企业商业秘密保护能力提升服务月”活动—2023 年 5 月 22 日

保护商业秘密是保护企业核心竞争力的重要举措。市场监管总局将指导各地市场监管部门，聚焦企业商业秘密保护面临的困难和问题，通过开展开展商密保护服务月活动，帮助企业提升商业秘密保护意识和能力，打造商业秘密保护“生态圈”。

原 文 链 接：https://www.samr.gov.cn/xw/mtjj/art/2023/art_af94181ba5674bb9a04a10127bce13c6.html

（2）国家市场监督管理总局正式发布实施《信息安全技术 关键信息基础设施安全保护要求》（GB/T 39204-2022）—2023 年 5 月 1 日

《关保条例》中明确了关键信息基础设施范围： 公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域。同时规定监管部门、保护工作部门、关基运营者三层责任分工，以及网络安全服务机构的责任和义务。

《关保要求》是配套支撑《关保条例》的核心国家标准之一，适用于指导运营者对关键信息基础设施进行全生存周期安全保护。

原 文 链 接：https://www.sohu.com/a/671956371_244641

5. 北京市经济和信息化局

（1）北京市科委、中关村管委会，市经济和信息化局，市发展改革委会同相关单位制定了《北京市促进通用人工智能创新发展的若干措施（2023-2025 年）（征求意见稿）》—2023 年 5 月 12 日

北京市科委、中关村管委会，市经济和信息化局，市发展改革委会同相关单位制定了《北京市促进通用人工智能创新发展的若干措施（2023-2025 年）（征求意见稿）》，

《若干措施》针对加强算力资源统筹供给能力、提升高质量数据要素供给能力、系统布局大模型技术体系持续探索通用人工智能路径、推动通用人工智能技术创新场景应用、探索营造包容审慎监管环境五大方向，明确组织机制，提出 21 项具体措施。

原 文 链 接：http://kw.beijing.gov.cn/art/2023/5/12/art_2418_4626.html

6. 北京市经济技术开发区

（1）北京市经济技术开发区在京发布全国首个自动驾驶示范区数据安全管理办法—2023 年 5 月 12 日

智能网联汽车是汽车与电子信息、通信、交通等产业交叉融合发展的主要载体，其功能实现依赖于海量数据，却也存在数据安全合规风险。办法填补了国内自动驾驶示范区级数据安全管理的空白，明确了在市自动驾驶办公室统筹指导下，企业负数据安全主体责任，构建示范区企业数据能力提升及共享机制。

原 文 链 接：https://mp.weixin.qq.com/s/HfVIlzgKzbYP6IjUVRrIRw

二、资质动态

1. 国家互联网信息办公室有关负责人就《关于调整网络安全专用产品安全管理有关事项的公告》答记者问—2023 年 5 月 8 日

解答需要按照《公告》要求开展安全认证或者安全检测的网络安全专用产品、具备检测资格的认证检测机构范围及安全认证和安全检测依据的标准等。再次明确自 2023 年 7 月 1 日起，《计算机信息系统安全专用产品销售许可证》停止颁发，产品生产者无需申领。

原 文 链 接：http://www.cac.gov.cn/2023-05/08/c_1685191060504925.htm

三、观点撷英

《商用密码管理条例》修订版于 2023 年 5 月 24 日正式公布。这是《条例》自 1999 年 10 月 7 日发布和施行以来，首次迎来修订，也是贯彻实施 2020 年 1 月 1 日起施行的密码法的重要举措。《条例》在完善商用密码管理体制、促进商用密码科技创新与标准化建设、健全商用密码检测认证体系、规范商用密码进出口管理及促进商用密码应用等多方面提出具体要求，形成商用密码产业的基础框架。

1. 专家解读｜王小云：贯彻落实商用密码管理条例 推动我国商用密码事业高质量发展—2023 年 5 月 21 日

原 文 链 接：http://www.moj.gov.cn/pub/sfbgw/zcjd/202305/t20230519_479177.html

2. 专家解读｜周汉华：商用密码管理法治化的一次重大飞跃——评《商用密码管理条例》修订—2023 年 5 月 24 日

原 文 链 接：http://www.moj.gov.cn/pub/sfbgw/zcjd/202305/t20230519_479174.html

3. 专家解读｜杨建军：标准助力商用密码应用发展—2023 年 5 月 24 日

原 文 链 接：http://www.moj.gov.cn/pub/sfbgw/zcjd/202305/t20230519_479170.html

4. 专家解读｜张振峰：贯彻《商用密码管理条例》 推动商用密码科技创新发展—2023 年 5 月 24 日

原 文 链 接：http://www.moj.gov.cn/pub/sfbgw/zcjd/202305/t20230519_479169.html

5. 专家解读｜左晓栋：《商用密码管理条例》修订为维护国家网络安全提供坚强法治保障—2023 年 5 月 24 日

原 文 链 接：http://www.moj.gov.cn/pub/sfbgw/zcjd/202305/t20230519_479166.html

监管执法 | 《网信部门行政执法程序规定》于 2023 年 6 月 1 日正式实施

2023 年 3 月 23 日，国家互联网信息办公室发布了《网信部门行政执法程序规定》（以下简称“规定”），于 2023 年 6 月 1 日正式实施。《规定》是对 2017 年发布的《互联网信息内容管理行政执法程序规定》的全面修订，修订后的《规定》调整完善了网信部门行政执法的法律依据和适用范围，进一步规范了网信领域行政处罚等执法活动。

《网络安全法》、《数据安全法》、《个人信息保护法》等法律法规作为基础性实体法，对网络运营者、数据处理者、个人信息保护者等相关主体在网络运营、数据处理以及个人信息保护方面的权利义务及法律责任进行了详细的界定和规范，同时明确了网信部门在网络安全、数据安全、个人信息保护方面的统筹监管职责。而《规定》从程序上强化了数据执法，为各级网信部门开展执法活动提供了具体的程序规范，使数据执法有法可依、有法必依。

《规定》包括总则、管辖和适用、行政处罚程序、执行和结案、附则五章，共 58 条。其中行政处罚程序依次为立案、调查取证、听证、行政处罚决定和送达。本文将对《规定》文本内容进行解读，以供大家参考。

法律依据

依据《中华人民共和国行政处罚法》、《中华人民共和国行政强制法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》制定。这意味着网信部门的执法范围从原来的网络信息内容管理，扩大到网络安全、数据安全、个人信息保护等领域。

管辖和适用

《规定》第八条至第十四条内容，对地域管辖、指定管辖、级别管辖、移送管辖等相关制度作出了明确规定。

行政处罚程序

行政处罚程序依次为立案、调查取证、听证、行政处罚决定和送达、执行和结案。

类别	条款要点
地域管辖	第 8 条规定：“行政处罚由**违法行为发生地**的网信部门管辖”；
级别管辖	第 9 条规定：“**县级以上网信部门**依职权管辖本行政区域内的行政处罚案件”； 第 11 条规定：“上级网信部门认为必要的，可以直接办理下级网信部门管辖的案件，也可将本部门管辖的案件交由下级网信部门办理”，还明确设区的市级以下网信部门发现其所管辖的行政处罚案件涉及国家安全等情形的，应当及时报告上一级网信部门，必要时报请上一级网信部门管辖。
指定管辖	第 10 规定：“对当事人的同一个违法行为，两个以上网信部门都有管辖权的，**由最先立案的网信部门管辖**； 两个以上网信部门对管辖权有争议的，应当协商解决，协商不成的，报请共同的上一级网信部门**指定管辖**；也可以直接由共同的上一级网信部门指定管辖。”
移送管辖	第 12 条规定：“网信部门发现受理的案件不属于其管辖的，应当及时**移送有管辖权的网信部门**”； 第 14 条规定：“网信部门发现案件属于其他行政机关管辖的，应当依法移送有关行政机关”。

01、立案

第十八条规定了行政处罚立案的条件：（一）有涉嫌违反法律、行政法规和部门规章的行为，依法应当予以行政处罚；（二）属于本部门管辖；（三）在应当给予行政处罚的法定期限内。同时明确了符合立案条件后的程序。

02、调查取证

第十九条

网信部门进行案件调查取证，应当由具有行政执法资格的执法人员实施。执法人员不得少于两人，并应当主动向当事人或者有关人员出示执法证件。必要时，可以聘请专业人员进行协助。

首次向案件当事人收集、调取证据的，应当告知其有申请执法人员回避的权利。

向有关单位、个人收集、调取证据时，应当告知其有如实提供证据的义务。被调查对象和有关人员应当如实回答询问，协助和配合调查，及时提供依法应予保存的网络运营者发布的信息、用户发布的信息、日志信息等相关材料，不得阻挠、干扰案件的调查。

第二十条

网信部门在执法过程中确需有关机关或者其他行政区域网信部门协助调查取证的，应当出具协助调查函，协助调查函应当载明需要协助的具体事项、期限等内容。

收到协助调查函的网信部门对属于本部门职权范围的协助事项应当予以协助，在接到协助调查函之日起十五个工作日内完成相关工作；需要延期完成或者无法协助的，应当及时函告提出协助请求的网信部门。

第二十一条

执法人员应当依法收集与案件有关的证据，包括书证、物证、视听资料、电子数据、证人证言、当事人的陈述、鉴定意见、勘验笔录、现场笔录等。

电子数据是指案件发生过程中形成的，存在于计算机设备、移动通信设备、互联网服务器、移动存储设备、云存储系统等电子设备或者存储介质中，以数字化形式存储、处理、传输的，能够证明案件事实的数据。视听资料包括录音资料和影像资料。存储在电子介质中的录音资料和影像资料，适用电子数据的规定。

证据应当经查证属实，方可作为认定案件事实的根据。

以非法手段取得的证据，不得作为认定案件事实的根据。

第二十二条

立案前调查和监督检查过程中依法取得的证据材料，可以作为案件的证据使用。

对于移送的案件，移送机关依职权调查收集的证据材料，可以作为案件的证据使用。

第二十三条

网信部门在立案前，可以采取询问、勘验、检查、检测、检验、鉴定、调取相关材料等措施，不得限制调查对象的人身、财产权利。

网信部门立案后，可以对涉案物品、设施、场所采取先行登记保存等措施。

第二十四条

网信部门在执法过程中询问当事人或者其他有关人员，应当制作询问笔录，载明时间、地点、事实、经过等内容。询问笔录应当交询问对象或者其他有关人员核对确认，并由执法人员和询问对象或者其他有关人员签名。询问对象和其他有关人员拒绝签名或者无法签名的，应当注明原因。

第二十五条

网信部门对于涉及违法行为的场所、物品、网络应当进行勘验、检查，及时收集、固定书证、物证、视听资料和电子数据。

第二十六条

网信部门可以委托司法鉴定机构就案件中的专门性问题出具鉴定意见；不属于司法鉴定范围的，可以委托有能力或者有条件的机构出具检测报告或者检验报告。

第二十七条

网信部门可以向有关单位、个人调取能够证明案件事实的证据材料，并可以根据需要拍照、录像、复印和复制。

调取的书证、物证应当是原件、原物。调取原件、原物确有困难的，可以由提交证据的有关单位、个人在复制品上签字或者盖章，注明“此件由×××提供，经核对与原件（物）无异”的字样或者文字说明，注明出证日期、证据出处，并签名或者盖章。

调取的视听资料、电子数据应当是原始载体或者备份介质。调取原始载体或者备份介质确有困难的，可以收集复制件，并注明制作方法、制作时间、制作人等情况。调取声音资料的，应当附有该声音内容的文字记录。

第二十八条

在证据可能灭失或者以后难以取得的情况下，经网信部门负责人批准，执法人员可以依法对涉案计算机、服务器、硬盘、移动存储设备、存储卡等涉嫌实施违法行为的物品先行登记保存，制作登记保存物品清单，向当事人出具登记保存物品通知书。先行登记保存期间，当事人和其他有关人员不得损毁、销毁或者转移证据。

网信部门实施先行登记保存的，应当通知当事人或者持有人到场，并在现场笔录中对采取的相关措施情况予以记载。

第二十九条

网信部门对先行登记保存的证据，应当在七个工作日内作出以下处理决定：

（一）需要采取证据保全措施的，采取记录、复制、拍照、录像等证据保全措施后予以返还；

（二）需要检验、检测、鉴定的，送交具有相应资质的机构检验、检测、鉴定；

（三）违法事实不成立，或者先行登记保存的证据与违法事实不具有关联性的，解除先行登记保存。

逾期未作出处理决定的，应当解除先行登记保存。

违法事实成立，依法应当予以没收的，依照法定程序实施行政处罚。

第三十条

网信部门收集、保全电子数据，可以采取现场取证、远程取证和责令有关单位、个人固定和提交等措施。

现场取证、远程取证结束后，应当制作电子取证工作记录。

第三十一条

执法人员在调查取证过程中，应当要求当事人在笔录和其他相关材料上签字、捺指印、盖章或者以其他方式确认。

当事人拒绝到场，拒绝签字、捺指印、盖章或者以其他方式确认，或者无法找到当事人的，应当由两名执法人员在笔录或者其他材料上注明原因，并邀请其他有关人员作为见证人签字或者盖章，也可以采取录音、录像等方式记录。

第三十二条

对有证据证明是用于违法个人信息处理活动的设备、物品，可以采取查封或者扣押措施。

采取或者解除查封、扣押措施，应当向网信部门主要负责人书面报告并经批准。情况紧急，需要当场采取查封、扣押措施的，执法人员应当在二十四小时内向网信部门主要负责人报告，并补办批准手续。网信部门主要负责人认为不应当采取查封、扣押措施的，应当立即解除。

第三十三条

案件调查终结后，承办人认为违法事实成立，应当予以行政处罚的，撰写案件处理意见报告，草拟行政处罚建议书。

有下列情形之一的，承办人撰写案件处理意见报告，说明拟作处理的理由，报网信部门负责人批准后根据不同情况分别处理：

（一）认为违法事实不能成立，不予行政处罚的；

（二）违法行为情节轻微并及时改正，没有造成危害后果，不予行政处罚的；

（三）初次违法且危害后果轻微并及时改正，可以不予行政处罚的；

（四）当事人有证据足以证明没有主观过错，不予行政处罚的，法律、行政法规另有规定的，从其规定；

（五）案件不属于本部门管辖，应当移送其他行政机关管辖的；

（六）涉嫌犯罪，应当移送司法机关的。

第三十四条

网信部门在进行监督检查或者案件调查时，对已有证据证明违法事实成立的，应当责令当事人立即改正或者限期改正违法行为。

第三十五条

对事实清楚、当事人自愿认错认罚且对违法事实和法律适用没有异议的行政处罚案件，网信部门应当快速办理案件。

03、听证

第三十六条

网信部门作出下列行政处罚决定前，应当告知当事人有要求举行听证的权利。当事人要求听证的，应当在被告知后五个工作日内提出，网信部门应当组织听证。当事人逾期未要求听证的，视为放弃听证的权利：

1. 较大数额罚款；
2. 没收较大数额违法所得、没收较大价值非法财物；
3. 降低资质等级、吊销许可证件；
4. 责令停产停业、责令关闭、限制从业；
5. 其他较重的行政处罚；
6. 法律、行政法规、部门规章规定的其他情形。

第三十七条

网信部门应当在听证的七个工作日前，将听证通知书送达当事人，告知当事人及有关人员举行听证的时间、地点。

听证应当制作听证笔录，交当事人或者其代理人核对无误后签字或者盖章。当事人或者其代理人拒绝签字或者盖章的，由听证主持人在笔录中注明。

除涉及国家秘密、商业秘密或者个人隐私依法予以保密外，听证公开举行。

听证结束后，网信部门应当根据听证笔录，依照本规定第四十二条的规定，作出决定。

04、决定与送达

第三十八条

网信部门对当事人作出行政处罚决定前，可以根据有关规定对其实施约谈，谈话结束后制作执法约谈笔录。

第三十九条

网信部门作出行政处罚决定前，应当填写行政处罚意见告知书，告知当事人拟作出的行政处罚内容及事实、理由、依据，并告知当事人依法享有的陈述、申辩等权利。

第四十条

当事人有权进行陈述和申辩。网信部门应当充分听取当事人的意见，对当事人提出的事实、理由和证据，应当进行复核；当事人提出的事实、理由或者证据成立的，网信部门应当采纳。

网信部门不得因当事人陈述、申辩而给予更重的处罚。

网信部门及其执法人员在作出行政处罚决定前，未依照

本规定向当事人告知拟作出的行政处罚内容及事实、理由、依据，或者拒绝听取当事人的陈述、申辩，不得作出行政处罚决定，但当事人明确放弃陈述或者申辩权利的除外。

第四十一条

有下列情形之一，在网信部门负责人作出行政处罚的决定之前，应当由从事行政处罚决定法制审核的人员进行法制审核；未经法制审核或者审核未通过的，不得作出决定：

（一）涉及重大公共利益的；

（二）直接关系当事人或者第三人重大权益，经过听证程序的；

（三）案件情况疑难复杂、涉及多个法律关系的；

（四）法律、行政法规规定应当进行法制审核的其他情形。

法制审核由网信部门确定的负责法制审核的机构实施。网信部门中初次从事行政处罚决定法制审核的人员，应当通过国家统一法律职业资格考试取得法律职业资格。

第四十二条

拟作出的行政处罚决定应当报网信部门负责人审查。网信部门负责人根据不同情况，分别作出如下决定：

（一）确有应受行政处罚的违法行为的，根据情节轻重及具体情况，作出行政处罚决定；

（二）违法行为轻微，依法可以不予行政处罚的，不予行政处罚；

（三）违法事实不能成立的，不予行政处罚；

（四）违法行为涉嫌犯罪的，移送司法机关。

第四十三条

对情节复杂或者重大违法行为给予行政处罚，网信部门负责人应当集体讨论决定。集体讨论决定的过程应当书面记录。

第四十四条

网信部门作出行政处罚决定，应当制作统一编号的行政处罚决定书。

行政处罚决定书应当载明下列事项：

（一）当事人的姓名或者名称、地址等基本情况；

（二）违反法律、行政法规、部门规章的事实和证据；

（三）行政处罚的种类和依据；

（四）行政处罚的履行方式和期限；

（五）申请行政复议、提起行政诉讼的途径和期限；

（六）作出行政处罚决定的网信部门名称和作出决定的日期。

行政处罚决定中涉及没收有关物品的，还应当附没收物品凭证。

行政处罚决定书必须盖有作出行政处罚决定的网信部门的印章。

第四十五条

网信部门应当自行政处罚案件立案之日起九十日内作出行政处罚决定。

因案情复杂等原因不能在规定期限内作出处理决定的，经本部门负责人批准，可以延长六十日。案情特别复杂或者情况特殊，经延期仍不能作出处理决定的，由上一级网信部门负责人决定是否继续延期，决定继续延期的，应当同时确定延长的合理期限；国家网信部门办理的行政处罚案件需要延期的，由本部门主要负责人批准。

案件处理过程中，听证、检测、检验、鉴定、行政协助等时间不计入本条第一款、第二款规定的期限。

第四十六条

行政处罚决定书应当在宣告后当场交付当事人；当事人不在场的，应当在七个工作日内依照《中华人民共和国民事诉讼法》的有关规定，将行政处罚决定书送达当事人。

当事人同意并签订确认书的，网信部门可以采用传真、电子邮件等方式，将行政处罚决定书等送达当事人。

05、执行与结案

第四十七条

行政处罚决定书送达后，当事人应当在行政处罚决定书载明的期限内予以履行。

当事人确有经济困难，可以提出延期或者分期缴纳罚款的申请，并提交书面材料。经案件承办人审核，确定延期或者分期缴纳罚款的期限和金额，报网信部门负责人批准后，可以暂缓或者分期缴纳。

第四十八条

网络运营者违反相关法律、行政法规、部门规章规定，需由电信主管部门关闭网站、吊销相关增值电信业务经营许可证或者取消备案的，转电信主管部门处理。

第四十九条

当事人对行政处罚决定不服，可以依法申请行政复议或者提起行政诉讼。

当事人对行政处罚决定不服，申请行政复议或者提起行政诉讼的，行政处罚不停止执行，法律另有规定的除外。

当事人申请行政复议或者提起行政诉讼的，加处罚款的数额在行政复议或者行政诉讼期间不予计算。

第五十条

当事人逾期不履行行政处罚决定的，作出行政处罚决定的网信部门可以采取下列措施：

（一）到期不缴纳罚款的，每日按罚款数额的百分之三加处罚款，加处罚款的数额不得超出罚款的数额；

（二）依照《中华人民共和国行政强制法》的规定申请人民法院强制执行。

网信部门批准延期、分期缴纳罚款的，申请人民法院强制执行的期限，自暂缓或者分期缴纳罚款期限结束之日起计算。

第五十一条

网信部门申请人民法院强制执行的，申请前应当填写履行行政处罚决定催告书，书面催告当事人履行义务，并告知履行义务的期限和方式、依法享有的陈述和申辩权；涉及加处罚款的，应当有明确的金额和给付方式。

当事人进行陈述、申辩的，网信部门应当对当事人提出的事实、理由和证据进行记录、复核，并制作陈述申辩笔录、陈述申辩复核意见书。当事人提出的事实、理由或者证据成立的，网信部门应当采纳。

履行行政处罚决定催告书送达十个工作日后，当事人仍未履行处罚决定的，网信部门可以填写行政处罚强制执行申请书，向所在地有管辖权的人民法院申请强制执行。

第五十二条

行政处罚决定履行或者执行后，有下列情形之一的，执法人员应当填写行政处罚结案报告，将有关案件材料进行整理装订，归档保存：

（一）行政处罚决定履行或者执行完毕的；

（二）人民法院裁定终结执行的；

（三）案件终止调查的；

（四）作出本规定第四十二条第二项至第四项决定的；

（五）其他应当予以结案的情形。

结案后，执法人员应当将案件材料按照档案管理的有关规定立卷归档。案卷归档应当一案一卷、材料齐全、规范有序。

第五十三条

网信部门应当依法以文字、音像等形式，对行政处罚的启动、调查取证、审核、决定、送达、执行等进行全过程记

录，归档保存。

第五十四条

网信部门实施行政处罚应当接受社会监督。公民、法人或者其他组织对网信部门实施行政处罚的行为，有权申诉或者检举；网信部门应当认真审查，发现有错误的，应当主动改正。

《规定》的发布实施开启了我国网络信息内容管理、网络安全、数据安全和个人信息保护领域行政执法工作的新篇章，标志着网信部门行政执法常态化时代的来临。在监管形势不断趋严的形势下，企业务必要在网络安全、数据安全和个人信息保护方面做好安全合规工作，以避免因合规问题遭到行政处罚。

@ 高考考生 | 事关个人信息保护，高考生不能松懈

各位考生请注意！这些东西千万不能发朋友圈等社交平台，例如准考证、个人身份证、考生号及密码、填报志愿纸质表、成绩单或查询页面截图、个人录取通知书等，这些东西包含一些考生重要个人信息，千万不要泄露出去！如果被别有用心的人获取到可以拿来实施精准诈骗。我们要时刻注意保护个人信息，不让不法分子有可趁之机。

今年的高考已经结束，考生们经历了漫长而艰苦的备考过程，但是高考结束后的信息防护也是一项关键的工作，因为信息泄露可能会给考生带来不必要的麻烦。

高考结束，这些高考类诈骗套路千万别信

1、伪造虚假查分网站

不法分子通过短信发送带有木马链接的虚假查分网址，从而获取手机所关联的银行卡信息，或者声称可帮助提前“有偿查分”的方式诈骗钱财。警方提醒：考生及家人查分时应认准教育部门指定的官方查分网址和查询方式，不要轻易点击来历不明的链接。

2、伪造录取通知书

不法分子通过伪造虚假高考志愿填报平台，冒充高校招生办人员，向考生寄送伪造的录取通知书，让考生将学杂费等打入指定的银行账号。警方提醒：考生和家长在登录学校和教育部门网站时，要通过官网认证的链接进入，转账汇款时要通过多种途径核实账号真伪。

3、声称有内部指标

不法分子谎称有特殊关系可获得高校“内部指标”“计划外指标”，引诱家长花钱“打点”。警方提醒：正规的招生录取不会产生任何附加费用，凡是需要收取保证金、录取费、指标费的“招生指标”，都是诈骗！

除此之外，冒充名家辅导志愿填报、谎称可以更改高考成绩等也是高考期间常见骗局。广大考生和家长要提高警惕，注意甄别，凡是涉及转账的事项一定要反复核实，如遭遇此类诈骗，请第一时间报警。

高考考生信息保护措施

尽管高考考生信息保护存在风险，但是我们可以采取一系列的措施进行保护。首先，高考办公室应该建立健全的信息保护体系。包括对考生信息的存储、传输、查询等方面进行彻底的保护。对网上成绩查询系统的安全性进行必要的加固措施，防止网络攻击、信息泄露等问题的发生。其次，可以通过对考生信息加密的方式提高信息安全性。比如在成绩查询系统中设置双重验证机制，通过验证码或指纹等方式加强认证，确保信息安全性。此外，还可以采取实名认证制度，对考生进行身份验证。并且在网上成绩查询系统上设置访问日志，对所有访问者进行监控，防止恶意攻击和信息泄露。

高考考生自我保护措施

作为高考考生，我们也应该主动采取一些措施来保护自己的信息安全。首先，不要随意将个人信息泄露给他人。比如不要将自己的身份证号码、学籍信息等随意透露给陌生人，避免给自己带来经济损失或身份盗窃等问题。其次，注意保管自己的账号和密码，设置强密码，定时更改密码，避免网络账号被黑客攻击、窃取个人信息。最后，加强安全意识，警惕各种网络欺诈和诈骗，向身边的人寻求帮助和支持。

总之，高考考生信息保护问题需要得到重视和关注。高考办公室应该建立健全的信息保护体系，采取一系列的措施确保网上成绩查询系统的安全性。考生本身也应该注意保护自己的信息安全，加强防范意识，避免信息泄露。只有通过共同的努力，才能够最大程度地保护考生的个人信息安全。

最后，亿赛通祝所有考生前程似锦，金榜题名！

小贴士 | 网络攻击手段你了解多少?

随着网络技术的飞速发展，网络攻击成为了一个不可忽视的问题。有许多黑客试图获取用户数据，窃取个人隐私，并利用它们进行非法活动。虽然网络安全是一个广泛的话题，但是仍然有很多人对如何保护自己的数据感到困惑。

【艾克斯 - 马赛大学遭受重大网络攻击】

据法媒 6 月 7 日报道，今天上午，法国艾克斯 - 马赛大学遭受一次重大的网络攻击，导致内部和外部网站访问出现严重问题。据该大学内部一位消息人士透露，整个计算机网络在上午被关闭，以限制或避免潜在的数据泄露。该大学的通信部门证实，网络已经被封锁，学校管理层已要求员工回家，预计计算机网络在今天结束前不会恢复。

【英国 BA、BBC 和 Boots 遭黑客攻击，数万名员工个人数据泄露】

据路透社 6 月 5 日伦敦报道，英国航空公司 BA、英国药店连锁店 Boots 和英国 BBC 这些公司周一确认其数万名员工个人数据被泄露。BA、BBC 和 Boots 表示，违规行为发生于他们的薪资服务提供商 Zellis，加拿大新斯科舍省政府也受到了此次违规行为的影响。Zellis 和新斯科舍省政府的数据是通过使用 MOVEit 文件传输软件而暴露的。Zellis 拒绝透露有多少客户受到影响，新斯科舍省政府没有立即回复置评请求。新斯科舍省网络安全和数字解决方案部长科尔顿勒布朗在一份声明中表示，他的居民“会有疑问，我们也会有疑问”。

随着信息技术的迅猛发展、大数据技术在各行各业的逐步落地，在大数据为业务带来巨大价值的同时，也带来了潜在的安全风险。一方面，传统数据中心面临的安全风险如网络攻击、系统漏洞等依然存在；另一方面，针对大数据的数据集中、数据量大、数据价值大等新特点的安全风险更加凸显，一旦数据被非法访问甚至泄露，造成的损失非常巨大。

常见的网络攻击手段

1、口令入侵：不法分子非法登录你的账户，然后再实施攻击活动。

2、电子邮件攻击：不法分子不停地发送垃圾邮件到你邮箱，让系统瘫痪，然后进行非法获取数据。

3、安全漏洞：许多系统都有安全漏洞（Bugs），比如我们常用的 windows 操作系统经常要打补丁，就是为了弥补出现的安全漏洞。这些漏洞如不补上，就会被坏人利用，获取你的电脑权限甚至电脑里的信息数据。

4、黑客软件：不法分子能非法取得用户计算机的终极用户级权利，对其进行完全控制，除了能进行文件操作外，还能进行桌面抓图、取得密码等操作。

5、MITM 攻击：中间人 (MITM) 类型的网络攻击是指网络安全漏洞，使得攻击者有可能窃听两个人、两个网络或计算机之间来回发送的数据信息。在 MITM 攻击中，所涉及的两方可能会觉得通信正常，但在消息到达目的地之前，中间人就非法修改或访问了消息。

……

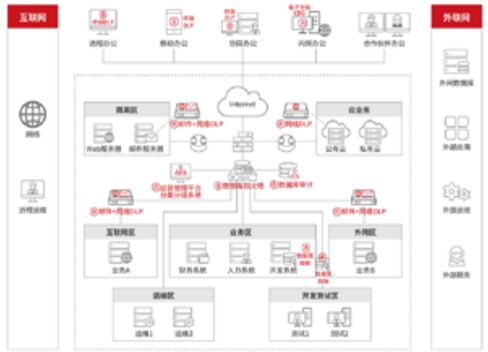
亿赛通小贴士 ESAFENET PROMPT

面对庞大的冗杂数据和众多数据场景结合的现状，为保障数据安全，让数据得到更好的防护和流转，亿赛通独家提出数据安全建设理念，以专业的产品和服务为客户筑牢数据安全底座。

亿赛通提出 “分·放·管·服”核心数据安全建设理念，分别从制度和技术角度为客户建立数据安全防线，制度主建，技术主战，对数据和人实现分权分责分风险，形成放权管责相结合的态势，做到要素服务保支撑，持续安全可运营，确保数据安全流转产生价值，循环优化，闭环赋能。

“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，为企业数据资产从产生价值到保值、增值的建立重要保障。这样的双闭环体系非常具有可操作性，并且非常高效，可以让企业步步为营，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。

除此之外，亿赛通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，全方位保障用户终端数据安全。



网络攻击是一个严重的问题，我们需要采取一些措施来保护我们的数据安全。谨慎打开附件和链接，使用防病毒软件以及备份数据。我们必须时刻保持警惕，避免冒险行为，以确保我们的数据不受损失。

作为中国数据安全专家，亿赛通二十年专注数据安全，以专业的产品和服务为客户筑牢数据安全底座。未来，我司将持续深化数据安全建设理念，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。

海关总署

客户简介

海关总署与国家紧密联系，所涉及信息带有机密性，所以其信息安全问题，如敏感信息的泄露、网络资源的非法使用以及勒索病毒等，都将对其信息安全构成威胁。尽管已经采用了安全防护措施等方式来提高信息安全等级，但在数据防泄露部分，大多还是以明文存储在服务器、终端及各种存储介质中，数据泄露的风险时刻存在，另外也无法做到对数据在内部使用权限和范围的管控。

需求背景

海关总署于 2007 年成立安全组织机构，2008 年制定海关等保标准，各直属海关完成系统定级。经过调研，海关的风险主要对于网络中传输的数据没有监控和审计；对于邮箱应主动或无意外发敏感文件没有必要的防护措施。因此有必要加强对海关信息系统，电子信息数据的安全防护。特别是对敏感信息资源进行保护。双方沟通后，具体数据安全需求分为两部分：信息中心和业务部门的系统安全，这部分更侧重于整体系统安全防护；以及主要针对保密办和办公厅两部门的内容安全，两部门由于涉密专人专岗，涉密系统定级整改，所以更侧重涉密信息系统。

解决方案

针对海关总署问题痛点，亿赛通在其内网区域旁路部署数据泄露防护系统：

1、主动泄露防御，分级精准控制

通过部署在内部网络和外部网络连接的出口处的网络 DLP 系统，对进出单位内部网络的所有网络敏感数据进行扫描防护，对敏感数据泄露事件可根据策略进行阻断。

2、明确定位数据，全通道控制

对海关总署内部邮件进行敏感内容防控，并进行增删收件人，邮件正文替换，剥离敏感附件、邮件告警、邮件审批、邮件阻断等操作。

3、识别敏感内容，标记敏感级别

对海关总署通过网络协议的还原和对数据的检测分析，获取此协议承载的数据情况，对违规内容进行安全防泄露处理，并进行违规数据统计和态势分析，在设备部署过程中，网络数据泄露防护系统部署在核心交换机取旁路镜像数据流，对终端访问业务系统和外发时下载的数据进行内容识别和敏感信息审计，数据泄露防护系统只取镜像数据，不影响网络数据的正常传输。

项目成果

亿赛通为海关总署建设科学先进、自主可信、可扩展又满足央企商密保护合规要求的全方位数据防泄密体系。具体实现了与海关与建设或正在建设的第三方平台对接，特别是与海关的安管中心。以 SNMP 或 SYSLOG 方式上传系统运行状态和安全事件；整合后，可共用组织机构、人员、岗位等信息，把用户、组织同步到 DLP 系统。现有的内网邮件系统也进行了整合，从而实现所有通知信息均可通过邮件的方式进行通知；设置了数据识别策略后，保证了系统对报关单仓单的敏感数据库文件的数据保护业务；并且定期调整数据识别策略，以降低误报率和漏报率，是之符合实际工作和事件处置需要。本次系统部署可有效降低业务运营中的 IT 风险，提升海关敏感数据防护能力，降低多重安全合规管理成本。

国家信息技术安全研究中心

客户简介

国家信息技术安全研究中心是遵照中央领导重要批示，经中央编制委员会办公室批准组建，中央网信办所属的国家事业单位，履行科研技术攻关与网络安全保障双重职能，主要开展网络安全核心技术研究、国家网络安全现实保障及网络安全技术服务等业务，现有各类科技人员 200 余人。自 2005 年成立以来，中心以服务国家网络安全为使命，秉承“国家网络安全因我而不同”的建设发展理念，践行“忠诚、团结、创新、务实、高效”的文化精神，承担国家重大活动网络安保、党政机关和重要行业关键信息基础设施安全防护、网络和信息技术产品安全检测、自主可控技术产品研发，以及网络安全发展战略研究等任务。在执行国家重大活动网络安保任务中发挥核心作用。先后执行上百次国家重大活动安全保障任务，牵头组织和参与多项网络安全应急处置任务，受到国家有关部门的充分肯定和表彰。

需求背景

国家信息技术安全研究中心拥有数量大、价值高的数据资源，通过开放共享发挥这些数据资源的潜在价值，是数字时代促进经济社会发展的必然要求。但在当今的大数据时代下，个人及重要隐私数据保护超越了传统隐私权保护的范畴，这就导致传统隐私保护制度无法进行全面保护。一旦遭遇不法分子攻击威胁，泄露的形式更是多种多样。因此，需加快构建与数字时代相适应的政企机构数据安全保障体系，提升数据安全合规检查能力，可以有效防范和化解政企机构数据泄露带来的风险，构建数据安全。

解决方案

1. 记录每次数据移动

终端支持丰富的行为数据抓取，包括数据操作、数据轨迹、网络行为、用户行为、应用行为等。所有的行为可以生成可视化的数据和文本，可以直接进行查阅，并与用户活动相关联。

2. 强大数据整合能力

TIS 将 UEBA、机器学习和大数据技术的精华整合为一个以数据为中心的综合审计和保护平台。通过对数据的重新构筑和关联，我们提供了一个强大的解决方案，首次缩小了实时世界和分析世界之间的差距。我们将运维团队从繁琐的手工工作中解放出来，并授权您的 IT 和安全团队用更少的资源做更多的事情。

3. 行为和效率分析

基于用户操作行为数据，提供强大的数据和行为分析能力，帮助用户发现数据泄露、欺诈、滥用等安全问题，并可以发现员工之间潜在数据流通，通过用户行为数据的分析还可以分析用户工作时长、工作内容以及用户操作等，可以为企业提供用户完整数据活动轨迹。

项目成果

亿赛通数据安全防护体系保障了国家信息技术安全研究中心的办公资源安全，以及建立了一套真正适合其单位的信息安全体系，有效的防止了内部员工有意或无意泄密和外部人员非法窃取企业的核心数据资产的风险。