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

04 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

《亿赛通四月刊》已送达
与你畅聊安全大事

刊首语 PREFACE

ESAFENET

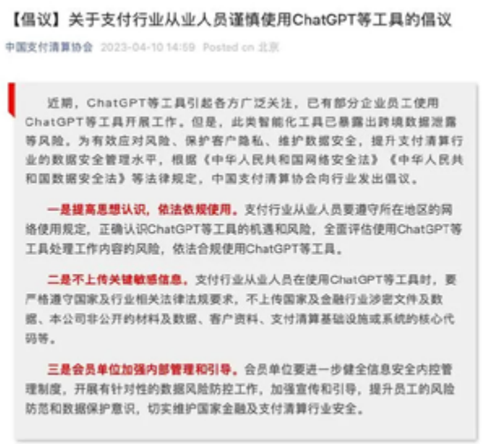
刷脸支付、在线会议、云展览……如今，小到居家出行、大到政务工作，数字技术深刻融入经济社会的方方面面。顺应数字时代浪潮，适应人民新期待，进入新时代，数字中国建设取得了新成就，数字技术不断创造新的可能。伴随着数字中国建设的加速，数据安全的外延越来越大，数据作为第五大生产要素，更要求数据要产生价值，以及保值增值。不同场景下，接触到数据的不同用户，在应用过程当中，有些行为会导致数据的量变引起质变，造成严重的数据安全问题。本次《亿赛通四月刊》带你回顾本月安全圈的精彩瞬间！

国内

1、我国数据泄露事件仍呈现高发态势，数据泄露仍以公民个人信息为主

摘要：近年来，我国数据泄露事件不断增加，其中以公民个人信息为主的泄露事件占比较高。数据泄露给公民个人隐私和财产安全带来了非常严重的风险和威胁。在数据泄露事件中，公民个人信息成为了黑客和犯罪分子的主要目标，这主要是因为个人信息非常珍贵和有价值，可以被用于各种黑色产业链，如假冒身份证、信用卡盗刷、网络诈骗等。

2、中国支付清算协会倡议：从业人员谨慎使用 ChatGPT 等工具



【倡议】关于支付行业从业人员谨慎使用ChatGPT等工具的倡议

中国支付清算协会 2023-04-10 14:59 Posted on 北京

近期，ChatGPT等工具引起各方广泛关注，已有部分企业员工使用ChatGPT等工具开展工作。但是，此类智能化工具已暴露出跨境数据泄露等风险。为有效应对风险、保护客户隐私、维护数据安全，提升支付清算行业的数据安全管理水平，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》等法律规定，中国支付清算协会向行业发出倡议。

一是提高思想认识，依法依规使用。支付行业从业人员要遵守所在地区的网络使用规定，正确认识ChatGPT等工具的机遇和风险，全面评估使用ChatGPT等工具处理工作内容的风险，依法合规使用ChatGPT等工具。

二是不上传关键敏感信息。支付行业从业人员在使用ChatGPT等工具时，要严格遵守国家及行业相关法律法规要求，不上传国家及金融行业涉密文件及数据、本公司非公开的材料及数据、客户资料、支付清算基础设施或系统的核心代码等。

三是会员单位加强内部管理和引导。会员单位要进一步健全信息安全内控管理制度，开展有针对性的数据风险防控工作，加强宣传和引导，提升员工的风险防范和数据保护意识，切实维护国家金融及支付清算行业安全。

摘要：近日，中国支付清算协会发布《关于支付行业从业人员谨慎使用 ChatGPT 等工具的倡议》，引发业内关注。协会倡议业内提高思想认识，依法依规使用；不上传关键敏感信息；会员单位加强内部管理和引导。

3、又有险企员工倒卖客户信息获刑，信息泄露频发该如何防“内鬼”？

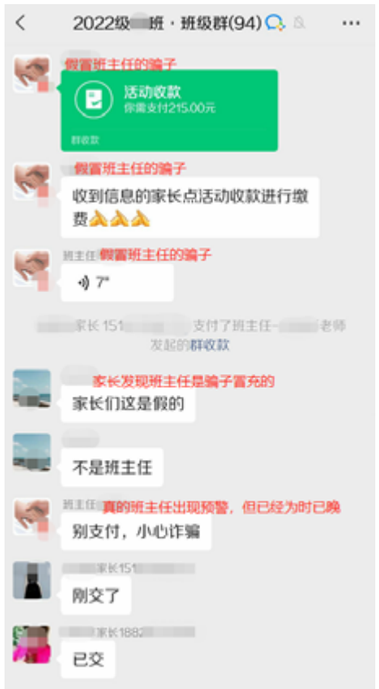
摘要：上海静安区人民法院近期公布一则刑事判决书，将某保险公司多名员工侵犯保险客户个人信息的犯罪细节公布于众。这几位员工利用客服人员的职务便利查询保险客户的个人信息，并售卖给他人赚取利益，从中非法获利超 26 万元，最终得到了法律的制裁。

4、超 1.9 万条个人信息被非法牟利！于法不容！我们并非束手无策！

摘要：作案人杨某是一个资深的游戏迷，他发现在一些网络游戏平台的登录界面，可以用一个人的身份信息绑定 5-10 个游戏账号。抓住了这一漏洞，杨某自以为找到了“商机”。于是，他开始广泛搜集公民个人信息，用以注册游戏账号，并通过出租游戏账户牟利。

5、女演员称怀孕后丈夫多次收涉黄短信，谁在背后泄露了个人信息？

摘要：近日，《巴啦啦小魔仙》黑魔仙扮演者周娇发布视频称，自己孕期及生产后，丈夫多次莫名地收到涉黄短信，周娇表示，这并不是丈夫第一次收到此类信息，之前在自己孕期时，就收到过类似短信，内容大差不差，当时两人都没有当一回事。这次又收到短信，才回过神来，因为自己在怀孕之前，根本就没有发生过类似的事。



6、陕西多名家长已报警！请所有老师和学生家长速速排查

摘要：陕西省公安厅刑事侦查局发布消息称，近期，在榆林市个别学校，接连发生骗子混进班级群、家长群，假冒班主任身份，发布诈骗信息，致使部分家长上当受骗。日前，榆林榆阳区多名家长报警称，他们在子女班级家长群中看到“班主任”在群内发送了一条需要收取所谓的“资料费”215元的通知，让家长们在群内缴纳该项费用。

7、捡到手机拒不归还？法院判赔，包含信息泄露风险损失费

摘要：司女士的手机被孩子遗失在路边，监控录像拍下了一名保洁员将手机捡走的过程。可面对录像、警察和单位的劝说，保洁员始终否认捡到手机，被告上法庭后仍然拒不归还。北京西城法院日前判决保洁员赔偿司女士 2200 元。值得一提的是，法院认定手机中的个人信息、数据损失及个人信息、数据泄露风险的损害也应予以赔偿。

8、突发！新开普董事长涉嫌泄露内幕信息罪被刑拘

新开普电子股份有限公司 NEWCARE ELECTRONICS CO., LTD.　关于公司实际控制人、董事长兼总经理被刑事拘留的公告

证券代码：300248　证券简称：新开普　公告编号：2023-020

新开普电子股份有限公司

关于公司实际控制人、董事长兼总经理被刑事拘留的公告

本公司及董事会全体成员保证信息披露的内容真实、准确、完整，没有虚假记载、误导性陈述或重大遗漏。

新开普电子股份有限公司（以下简称公司）于 2023 年 4 月 24 日收到公司实际控制人、董事长兼总经理杨维国先生家属的通知，杨维国先生因涉嫌泄露内幕信息罪被刑事拘留。

公司于 2023 年 4 月 24 日晚上紧急召开第六届董事会第二次会议，除公司董事长杨维国先生未能出席，其他与会董事一致同意在杨维国先生被调查期间，由董事李玉玲女士代为履行公司董事长及法定代表人职责，以及暂代为履行公司董事会相关委员会成员的职责。由副总经理杨长昆先生代为履行公司总经理职责。

摘要：24 日晚间，新开普发布公告称，于 2023 年 4 月 24 日收到公司实际控制人、董事长兼总经理杨维国家属的通知，杨维国因涉嫌泄露内幕信息罪被刑事拘留。

9、闲鱼被指泄露隐私 用户受电话骚扰 平台称系统自动操作所致

摘要：北京市民小圆女士在某社交平台配图发帖称，自己在闲鱼出售的二手汉服发生退货纠纷，她按要求在 24 小时内修改了隐去个人信息的默认退货地址信息，但闲鱼平台却向买家泄露了她在平台上其他订单的信息，包括手机号码、精确到门牌号的地址等，导致买家打电话骚扰甚至言语威胁她。对此，闲鱼客服先后回复小圆女士及南都记者均表示，信息泄露是系统自动推送所致。

10、小偷盯上了同城婚礼直播 团伙趁婚礼间隙实施盗窃 10 万元被淮阴检方提起公诉

摘要：安某在刷同城视频的时候，看到了被害人张先生的婚礼直播，视频中有很多人拿着现金给新人红包，而且视频中有明确定位，于是便萌生了盗窃的想法。根据视频定位信息，安某找到新房进行踩点，随后联系了同样有盗窃前科的 3 个朋友。4 人于深夜翻墙入院，共窃取现金 6 万余元。

国外

1、美联邦机构被曝数据泄露丑闻：超 25 万消费者隐私被发至私人邮箱

摘要：美国联邦政府下属机构消费者与金融保护局（CFPB）被曝出现严重数据泄露丑闻，一名员工将大约 25.6 万消费者的机密数据发送至私人邮箱。CFPB 表示，该名雇员获得访问这些数据的授权，其中包括来自 7 家机构的消费者身份信息，例如姓名和交易账户等。这些数据被雇员用 65 封邮件发送至个人电子邮箱。

2、菲律宾多个政府机构“大规模数据泄露”？国调局、国税局否认

摘要：4 月 20 日消息，菲律宾一家网络安全公司称，该国超过 120 万条记录在网上泄露，其中包括菲律宾多个政府机构的申请人和雇员的敏感信息。

3、美芯片巨头 20G 数据泄露：芯片后门实锤！ 10nm 芯片技术曝光

摘要：近日，一则美国媒体爆出一个令人震惊的消息：美国某知名芯片巨头的 20G 数据被泄露。据悉，这些数据包括该公司的芯片设计、生产以及供应链信息等敏感数据。更加令人担忧的是，这些数据揭示出了该公司存在着芯片后门的问题，引发了人们对于芯片安全的担忧。

4、新的 Mirai 变体使用了奇特的恶意软件分发方法

摘要：去年跟踪该恶意软件的 Fortinet 研究人员注意到其制造者在不断完善它，首先是增加新的代码确保即使在 PC 重启后也能持续运行，然后是通过远程二进制下载器插入代码进行自我传播。后来，病毒编写者删除了它的自我传播功能，取而代之的是使他们能够持续远程暴力破解 SSH 服务器。

5、Vice Society 勒索软件如何通过 PowerShell 窃取用户数据

摘要：2023 年初，unit42 团队发现 Vice Society 勒索软件组织使用了一个名为为 w1.ps1 的脚本从受害网络中窃取数据。在本例中，脚本是从 Windows 事件日志 (WEL) 中恢复的。具体而言，该脚本是从 Microsoft Windows PowerShell/Operational WEL 提供程序中发现的事件 ID 4104：脚本块日志记录事件中恢复的。

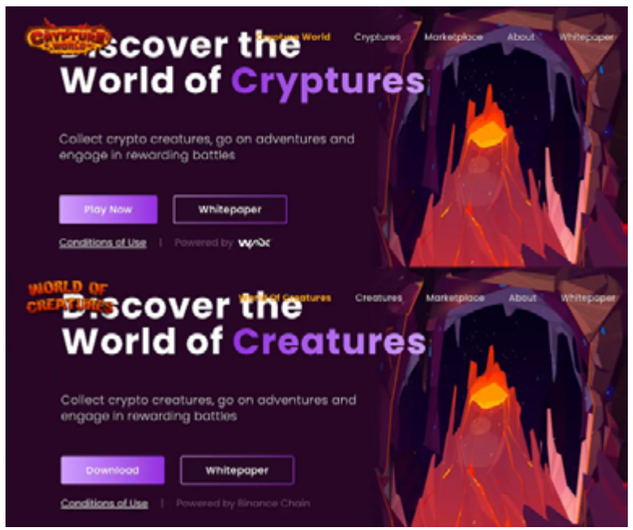
6、间谍软件开发商利用漏洞利用链攻击移动生态系统

摘要：去年，几家商业间谍软件开发商开发并利用了针对 iOS 和安卓用户的零日漏洞。然而，它们的漏洞利用链还依赖已知的漏洞才能发挥作用，这凸显了用户和设备制造商都应加快采用安全补丁的重要性。谷歌威胁分析小组（TAG）的研究人员在一份详述攻击活动的报告中表示：“零日漏洞与 n-day 漏洞被结合使用，利用补丁发布与完全部署到最终用户设备之间的巨大时间差来大做文章。我们的调查结果强调了商业监视软件开发商在多大程度上扩大了以往只有具备技术专长来开发和实施漏洞利用工具的政府才能享用的功能。”

7、黑客针对非洲的智能采矿系统进行攻击

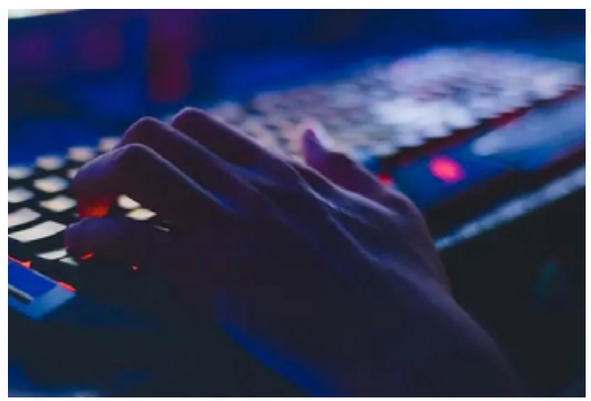
摘要：非洲 IT 集团 CyberAntix 的网络安全运营和合规性负责人 Pierre Jacobs 博士持有一种观点。据他说，网络安全漏洞现在已经达到了一种非常疯狂的程度，这也使得犯罪分子可以有机会在与合法组织相似的条件下实施网络犯罪。

8、Mac 恶意软件 MacStealer 伪装成 P2E 应用程序大肆传播



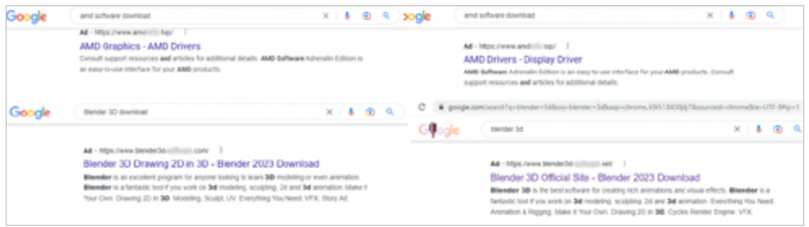
摘要：研究人员检测到 Mac 恶意软件 MacStealer 通过网站、社交媒体和消息平台 Twitter、Discord 和 Telegram 大肆传播。MacStealer，是使用 Telegram 作为命令和控制 (C2) 平台来窃取数据的最新威胁示例。它主要影响运行 macOS 版本 Catalina 以及之后运行在 M1 和 M2 CPU 上的设备。现在该恶意程序又有了新的传播途径，攻击者通过假冒合法的游戏赚钱 (P2E) 应用程序的图片，引诱受害者下载它。P2E 是 Play-to-earn 的缩写，允许玩家通过玩游戏来产生稳定的加密收入。每个游戏的机制可能不同，但奖励通常来自质押、刷游戏币或生成可交易的 NFT 物品。

9、俄罗斯 SolarWinds 攻击者发起新一轮的网络间谍攻击



摘要：4 月 13 日，波兰军事反间谍局和波兰的 CERT 团队向可能受间谍活动影响的目标发出了威胁警报，并且同时还表现出了妥协的迹象。这个被微软称为 Nobelium 的组织，也被 Mandiant 称为 APT29，该组织常年活跃于民族国家的间谍活动中；三年前，它曾发起过臭名昭著的 SolarWinds 供应链攻击。

10、使用搜索引擎作为传播恶意程序的数量大幅增加

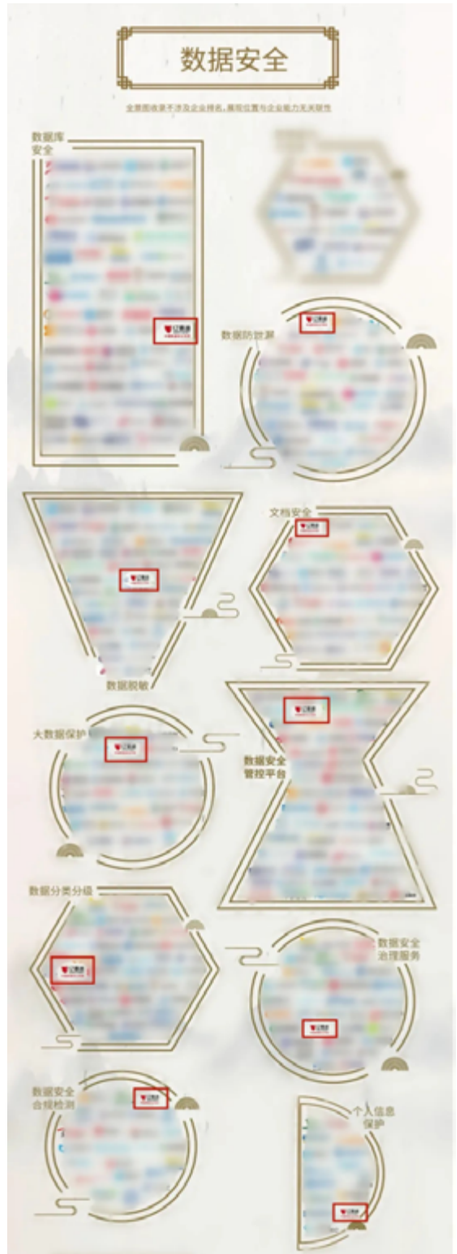


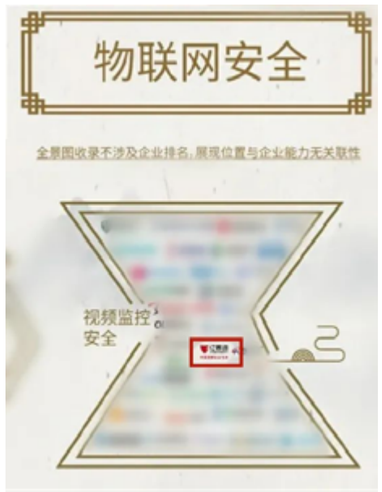
摘要：最近几个月，卡巴斯基实验室的研究人员观察到使用谷歌广告作为分发和传播恶意程序的活动数量有所增加。至少有两个不同的窃取程序，Rhadamanthys 和 RedLine，滥用搜索引擎自我宣传，并向受害者的设备发送恶意负载。它们似乎使用了相同的技术，模仿与 notepad++ 和 Blender 3D 等知名程序相关的网站。

亿赛通网络安全全景图入选十五项细分领域，布局安全新赛道

4 月 7 日，国内权威新媒体安全牛第十版《中国网络安全行业全景图》正式发布。亿赛通基于业内顶尖的技术实力，在数据安全、业务与应用安全、物联网安全、计算环境安全、网络安全服务等 5 大领域中的 15 项细分业务，处于行业领先地位，入选全景图。具体业务领域包括如下：

数据安全	文档安全、数据防泄漏、数据库安全、数据脱敏、数据分类分级、数据安全管控平台、大数据保护、数据安全治理服务、数据安全合规检测、个人信息保护
业务与应用安全	勒索软件防护、邮件安全
物联网安全	视频监控安全
计算环境安全	保密检查
网络安全服务	网络安全保险





本次全景图绘制历时 3 个月，共收录 456 家国内网络安全企业和相关行业机构，细分领域共收录 3180 项，收录领域数量超过 10 项的企业仅有 76 家，占比 16.67%。全景图力求更加科学、规范、全面地展现当前我国网络安全产业的发展状况和企业能力，是甲方用户、安全厂商、投资机构和业界人士快速了解产业生态格局、趋势和投资机会的参考指南。自安全牛第一次推出全景图以来，亿赛通连续 10 次上榜安全牛《中国网络安全行业全景图》，证实公司多年来的自主研发的技术优势和长期以来的客户服务口碑，得到安全行业专业机构高度认可。

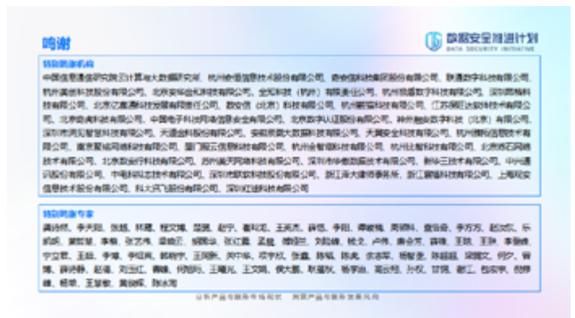
随着我国网络安全产业快速发展，各项客户需求不断涌现，如何从实用性、可用性、技术先进性等维度，研发出真正满足客户安全建设需求的代表性产品，是各厂商企业需要重点研究的问题。

亿赛通是一家致力于数据安全的服务厂商，对政企、能源、金融、通讯、教育、医疗、制造、互联网等行业用户，以专利技术为支撑，对综合数据、视频专网数据、工业数据、大数据、云数据等场景进行全方位多维度管理。

近年来，依托技术钻研与产品创新，亿赛通已迈入综合安全厂商发展道路。在数据安全领域，我们规划了完善的“云 + 网 + 端”产品体系，在“分放管服”数据安全建设理念的指导下，拥有着集数据安全治理、数据安全防护、数据安全流转、数据库安全和安全服务等系列共计 60 余款产品、服务、平台，并且产品线还在不断丰富中。亿赛通充分为客户提供全面的信息安全防护，满足客户各类安全防护建设需求。

着眼未来，我们将继续致力于引领数据安全产业发展，加大产品研发，力争为广大行业客户提供更多更好的信息安全产品和解决方案，成为最值得信赖的安全专家！

亿赛通受邀出席《数据安全产品与服务观察报告》发布会



中国信通院云计算与大数据研究所副所长 魏凯

中国信通院云计算与大数据研究所高级业务主管龚诗然发布《数据安全产品与服务观察报告》，介绍了数据安全产品、服务、市场现状，阐述了基于图谱调研信息与多轮专家研讨形成的十项数据安全产品与服务观察观点。

中国信通院云计算与大数据研究所高级业务主管

龚诗然

4 月 11 日，由数据安全推进计划联合中国通信标准化协会大数据技术标准推进委员会举办的《数据安全产品与服务观察报告》发布会在北京成功召开。亿赛通作为参编单位受邀出席本次发布会。

发布会上，中国信通院云计算与大数据研究所副所长魏凯发表了致辞，他指出，数字中国加速发展，数据要素市场建设迅速推进，数据安全广受各方关注，合规要求和内生动力共驱数据安全产业发展，亟需构建供需两侧的对话与交流，回应需求侧关切的痛点问题，推动供应侧产品技术创新，助力数据安全产业与生态良好发展。

报告输出了十个数据安全产品与服务观察观点：

1. 智能化浪潮来临：数据安全技术升级
2. 新技术：深刻影响数据安全产品发展
3. 第三方测评：“以评促建”创造厂商新优势
4. 安全检查工具：供给难以满足市场需求
5. 数据防泄漏：安全防护领域的重点产品
6. 数据安全网关：产品形态缺乏统一共识
7. 数据风险监测：站在“一体化”的“分岔路口”
8. 运营管理平台：“平台化”趋势下的热门产品
9. 安全合规服务：咨询与评估成为业内焦点
10. 分类分级服务：逐渐演变为独立服务品类

近年来，亿赛通积极参与编写了多项行业白皮书、研究报告，主要成果如下：

《我国网络安全保险产业发展白皮书（2021 年）》

《2022 工业互联网行业融合创新应用报告》

《大数据标准化白皮书 2022》

《数据资产管理实践白皮书（6.0 版）》

《数据安全治理实践指南 2.0》

《数据安全管理认证建设白皮书》

《数据安全管理平台应用指南》

《2022 数据安全产业竞合力洞察报告》

数据安全服务是数据安全体系建设的重要组成部分。国家高度重视数据安全服务，其中，工信部等十六部门联合印发的《关于促进数据安全产业发展的指导意见》提出，要壮大数据安全服务，推进规划咨询与建设运维服务。在国家战略与业务需求的双重驱动下，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，推出咨询规划服务、评估服务及运营服务三大类服务，提供基于用户业务需求的全流程服务。通过数据资产盘点、分类分级、数据安全评估等服务项，可以帮助企业全面摸清数据现状、业务现状和安全管理现状，为后续全面的安全体系建设奠定基础。

协同育人 安全赋能 | 亿赛通联合太仓市主管机构开展数据安全培训工作

4 月 14 日，在第八个全民国家安全教育日来临之际，2023 年度太仓市网络安全、数据安全专题培训班在西北工业大学太仓智汇港开班。

此次活动由市委国安办、市委网信办主办，市网络空间安全“双创”人才培养基地及亿赛通共同承办。活动邀请了来自西工大网络空间安全学院、西工大太仓智汇港等相关专家学者，围绕数据安全治理、网络安全防护体系建设与管理等方面开展专题授课。望通过系统专业的培训，来自全市各单位的网络安全官将进一步强化对网络安全、数据安全相关法律法规政策的理解，形成维护网络安全和数据安全的新思路、新方法、新举措、新本领，切实提升新形势下安全保障能力。

数字经济通过不断升级的互联网—云计算—区块链—物联网等信息技术，推动人类经济形态由工业经济向信息经济—知识经济—智慧经济形态转化，极大地降低社会交易成本，提高资源优化配置效率，提高产品、企业、产业附加值，推动社会生产力快速发展，同时为落后国家后来居上实现超越性发展提供了技术基础。数字经济也称智能经济，是信息经济—知识经济—智慧经济的核心要素。正是得益于数字经济提供的历史机遇，使中国得以在许多领域实现超越性发展。

近年来，我国数字经济蓬勃发展，产业规模持续快速增长。新型基础设施建设提速，数字产业化深入推进。大数据、云计算、人工智能加速融入工业、能源、医疗、交通、教育、农业等行业。在《“十四五”数字经济发展规划》中，国家确立了 2025 年的发展目标，明确了信息网络基础设施优化升级、数据质量提升、数据要素市场培育等 11 项重要工程，并从增强网络安全防护能力、提升数据安全保障水平、有效防范各类风险三个方面，明确提出了数字经济安全体系的具体建设要求。

数据资源作为数字经济的关键要素，与土地、劳动力、资本等传统生产要素存在很大区别。数据要素具有“可见性、易理解性、可连接性、可信性、互操作性、安全性、资产性、归属性、开放性”九大特征，每个特征在数字经济中发挥作用的同时都伴随着数据安全风险。

为应对这些新挑战，数据安全工作势必要采取新的思路，用新的方法解决新的问题。在这个背景下，数据安全产业从基于具体应用进行单一防护的 1.0 阶段，迈入了基于数据处理活动场景进行生命周期防护的 2.0 阶段，并正在加速向为数据和业务体系化融合提供安全保障的 3.0 阶段迈进。

亿赛通高级咨询顾问在培训中提到：数据安全建设从以技术防护为主，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。

亿赛通在进行数据安全治理体系建设时，会依据前期资产梳理结果再部署相应的安全能力产品和平台，进而达到风险评估、监控预警、应急处置及持续运营。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，需要覆盖云、网、端等场景。而亿赛通的综合产品能力已经覆盖数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务等方面，能够真正帮助客户实现数据安全策略管理、识别能力、防护能力、监测能力以及运营能力的有机整合。

除此之外，亿赛通率先提出的“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，具有可操作性、高效等特点，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。

本次培训为从业人员提供了一个良好的交流平台，就数据安全治理、安全运维等难题进行了深入交流与探讨。未来，亿赛通仍将秉持“中国数据安全专家”的职责，成就所托，持续为千行百业客户的业务顺畅运行保驾护航。

斩获新誉 亿赛通荣获 2023IT 市场年会新一代信息技术创新产品奖项

2023 年，是数字经济、数字化能力全面爆发的关键之年，数据的重要性逐渐凸显。4 月 20 日由赛迪顾问股份有限公司主办 2023 IT 市场年会在北京隆重召开。亿赛通斩获 “新一代信息技术创新产品”重磅奖项。

本次会议以“数实融创 价值重生”为主题，邀请主管单位领导、专家、企业领袖、科技界精英等共聚一堂，精准把脉行业发展、聚集业界精英力量、剖析行业最新热点、探索 IT 核心价值，共同推动 IT 产业创新发展。同时，大会中重磅发布“2023 IT 市场权威榜单”，旨在推动新一代信息技术的理论、实践创新，表彰取得卓著成绩或者作出突出贡献的个人和集体。

能揽获此项大奖，得益于亿赛通顺应形势，积极关注国家政策，想客户所想，使得公司全面、深入地了解客户需求，从而开发出符合客户业务特点的产品与解决方案，为客户提供可感知的价值。

目前，数字经济迅猛发展，新规定、新场景、新应用层出不穷，对企业来说，数据的获取方法、存储形态、传输渠道和处理方式等不断产生新的变化。这对企业数据安全建设提出了新的要求，并触发了新的安全威胁。同时，国内大部分企业内部人员安全意识落后，导致网络和数据安全层面建设相对滞后，尤其是对重要数据资产的保护，很多企业还无从下手。因此，企业用户受约于行业标准、政策法规的各项要求，数据安全建设成为重要的攻克目标。

在传统的在安全建设模式中，多以单点安全产品为主，企业无法对其进行关联，从而不得不在多点防御系统之间疲于奔命。数据安全建设已经从孤立的安全产品过渡到体系化、平台化能力建设。最终通过一个高度集中化的平台实现安全能力的体系化集成，统一汇集围绕企业的安全管理、流动监测、风险分析、事件溯源、风险评估能力，实现合规有序、有效保护、高效运营的网络和数据安全体系构建。

亿赛通在此大背景下，将人与数据相融合，形成以技术工具为基础的数据安全运营管理平台，并在市场中获得广泛认可。具体从数据治理层面入手，以数据资产为核心，注重对系统数据风险的识别、分析和处置。平台承担了统筹角色，承担识别数据、分类分级等数据安全治理重要工作。同时也成为联动其它数据安全产品，提升整体数据安全能力的重要组件。

平台特色

01 、海量分布式大数据架构

产品使用模块化及分布式架构设计，支持数据采集引擎、大数据存储及分析引擎的分离部署或集中部署， 可通过扩充采集引擎，异地部署或数据节点扩展系统的解析及存储能力。

02、数据汇聚综合分析技术

平台支持多个数据采集引擎，类型包括数据库流量数据、网络流量数据、终端文件数据和网关数据，依靠强大的自研数据流式处理引擎和分布式数据存储中心，从数据的采集、传输、分析、存储等全流转节点对服务器进行横向扩展，可同时统计多种数据类型的海量数据，汇总为直观的统计图或者报表。

03、精准内容检测识别技术

为实现数据智能分级保护，快速定位、准确识别企业核心数据，数据泄露防护系统应拥有内容级识别检测技术，配合机器学习、大数据分析等高级检测技术，实现核心数据事中检测响应的防护理念，以减少数据安全系统的误报 (将并未违规的消息或文件标识为违规) 以及漏报 (未将违反策略的消息或文件标识为违规)

匠心经营 20 载，技术创新始终是亿赛通发展和成长的

重要驱动力，公司持续加大研发投入，创新体系建设，专注于技术的革新，在发展模式上，依托遍布全国的客户网，持续强化核心销售渠道建设，不断突破创新。

亿赛通作为中国数据安全行业具有代表性的国有品牌，始终践行“中国数据安全专家”使命，洞察数据安全产业变化、围绕客户需求，深入探索数据安全技术，为企业数字化转型增添新的动力。下一步，将依托自主研发的新一代数据泄露防护系统、新一代电子文档安全管理系统、数据安全运营管理平台、数据库安全五件套、数据分类分级系统、数据跨境安全检查工具等核心产品，深化应用，打造数据安全新一代标志产品，深度赋能数字经济高质量发展。

助推数字中国建设 | 亿赛通支撑数字中国创新大赛网络数据安全赛道

2023 年 2 月，中共中央、国务院印发《数字中国建设整体布局规划》，明确数字中国建设整体布局，指出要强化数字中国关键能力，构筑自立自强的数字技术创新体系，筑牢可信可控的数字安全屏障。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，举办 2023 数字中国创新大赛。其中，网络数据安全赛道决赛于 4 月 23 日在福建师范大学开赛，大赛由福建省通信管理局主办，中国电子信息产业发展研究院、工业和信息化部教育与考试中心、中国软件评测中心协办，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并出席决赛现场。

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，历经 7 个小时的激烈角逐，最终评选出 1 名金奖、3 名银奖、5 名铜奖、10 名优胜奖、2 名优秀组织奖、3 名优秀赛题奖、4 名优秀领队奖；决赛成绩排名前 30 的参赛队伍成员获得由工业和信息化部教育与考试中心颁发的数据安全职业能力证书。

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。本届大赛设置网络数据安全赛道，以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。

亿赛通在云、网、端三大应用场景下，对综合数据、商业数据、视频专网数据、工业数据、大数据、云数据等进行全方位多维度管理，打造了集数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务为一体的数据安全领域综合解决方案，能够真正帮助客户实现数据安全策略管理、识别能力、防护能力、监测能力以及运营能力的有机整合。

下一步，亿赛通将继续支撑网络数据安全赛事、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。

亿路同行 | 2023 亿赛通渠道会于津门盛大启航

4 月 27 日，津彩启航 亿路同行 2023 亿赛通渠道会 -- 天津站盛大召开。大会邀请当地渠道伙伴共同探讨数据安全市场新机遇，洞见亿赛通核心产品竞争力，分享亿赛通渠道战略转型的成果，同时赋能渠道伙伴提高产品理解。近百位嘉宾齐聚一堂，共话数安新格局，开启 2023 行业新纪元。

北京亿赛通科技发展有限责任公司天津办事处首席代表在致辞中详细分析天津地域特点，提出渠道布局，愿与渠道伙伴共同打造天津市场数据安全头部品牌，将公司品牌扩大。公司凭借着深厚的数据安全技术积累，全面的数据安全产品体系，成为众多伙伴不二之选。数据安全的深入贯彻需要渠道伙伴共同努力，亿赛通期待与更多新老伙伴建立长期的良性伙伴关系，齐力推动数据安全产业发展，为企业的核心数据创造更大的经济价值。

亿赛通渠道业务部高级总监李荣刚为到场嘉宾详细介绍了 2023 年最新的渠道政策。2023 年亿赛通对全国市场进行调整与规划，继续强化渠道体系建设，增加双方互动，发展核心渠道，通过更加完善的渠道支持政策，实现与渠道的双向共赢。与往年不同的是，公司推出渠道认证技术培训，为所有渠道伙伴提供响应培训认证课程，为长期合作奠定坚实基础。亿赛通以开放心态面对所有渠道伙伴，为其提供强大的平台支撑、公正的业务环境、优质的服务体系、高效的系统支持、多样的市场活动、专业的解决方案、丰富的产品资源，旨在双方共同扩展天津安全生态圈，达到互惠互利，双向共赢。

值得一提的是，大会特别邀请天津智慧城市研究院咨询总监、南开大学信息安全博士、天津职业技术师范大学 “双师型” 博士研究生导师、原西青区网信办副主任张顺博士出席。他提到，全球数据总量高速增长，中国加速进入数字经济时代。中国将成为数据量最大的国家，数字经济占国内生产总值比重从 32.9% 提升至 39.8%，总量连续多年位居世界第二。在数字经济高速发展的前提下，国内外数据安全事件频发，经济社会发展受到巨大影响，政府机构重视数据安全问题，密集出台专项政策法规。

在《数字中国建设整体布局规划》中，明确数字中国建设按照“2522”的整体框架进行布局，即夯实数字基础设施和数据资源体系“两大基础”，推进数字技术与经济、政治、文化、社会、生态文明建设“五位一体”深度融合，强化数字技术创新体系和数字安全屏障“两大能力”，优化数字化发展国内外“两个环境”，“创新体系”与“安全屏障”相伴相生。数据安全总体目标是达到可防、可控、可追溯，在数据安全治理中，确认组织与职责、安全制度、安全标准、响应机制后即可进行数据全生命周期的安全管理，即数据安全技术平台。数据安全管理、运营与技术体系相互促进，以数据安全管控策略为核心，以管理体系为指导，以运营体系为纽带，以技术体系为支撑，构筑形成管理、技术、运营三位一体的数据安全治理框架，全方位支持企业高质量发展。

亿赛通高级咨询顾问在讲解的过程中提到的合规体系日益完善，《“十四五”大数据产业发展规划》、《十六部门关于促进数据安全产业发展的指导意见》都提出完善数据安全保障体系，推进规划咨询与建设运维服务，积极发展检测、评估、认证服务，由此可以看出，深入业务场景提供数据安全服务已成为必然发展趋势。亿赛通构建的数据安全体系具体以技术防护为主，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。全线产品涵盖数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务等五大类别，帮助客户实现数据安全策略管理、识别能力、防护能力、监测能力以及运营能力的有机整合。

大会的最后，亿赛通解决方案专家针对金融、医疗、数据出境详细进行解读分析。对于上述行业来说，数据治理尤为重要。数据由“静态”转为“动态”，金融、医疗作为数据密集型行业，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，对企业的数据安全防护能力和数据治理能力提出新的要求。不同行业有不同的风险，但始终遵循安全咨询、分类分级、分级管控的治理步骤，将终端、数据库及文件服务器内的数据做梳理，完成分类分级，为数据分级管控做铺垫，最终完成对标合规。

而数据出境则较为不同，作为数据领域避不开且极端重要的一个环节，保护数据主权的同时加强跨境数据传输的监管与合作。是政府与企业的重要任务。由于识别标准不一、监管困难、合规建设能力不足，导致数据安全出境困难重重，亿赛通为企业提供“数据出境合规工具箱”，开箱即用，自查合规风险、提高合规能力，并以服务形式输出，给予企业数据出境合规指导，协助企业完成重要数据安全自查。

对数据安全行业而言，政策是基石、产品是保障、监督是手段，星河大海万千点，众志成城共扬帆。数据安全的发展前景广阔已经成为不争的事实。亿赛通将会为推动我国数据安全产业技术发展和行业提升不懈奋斗，依托各自资源和能力，联合创新开展全面合作，我相信，在合作的基础上，我们一定能在数字经济浪潮中一帆风顺，业务蒸蒸日上，更上一层楼！

亿聊安全 | 这些政策新闻，你必须知道

新闻概览

1、中共中央 国务院印发《党和国家机构改革方案》组建国家数据局；

2、中共中央 国务院新闻办公室发布《新时代的中国网络法治建设》白皮书；

3、中共中央 国务院印发《数字中国建设整体布局规划》；

4、中共中央 网信办关于开展网络安全服务认证工作的实施意见；

5、2022 年我国大数据产业规模达 1.57 万亿元；

6、2022 年我国网络安全产业发展现状分析及展望；

7、工业和信息化部办公厅：做好 2023 年信息通信业安全生产工作的通知；

8、工业和信息化部：关于印发《电信领域违法行为举报处理规定》的通知；

9、国家市场监督管理总局、中央网络安全和信息化委员会办公室、工业和信息化部 、公安部联合发布《关于开展网络安全服务认证工作的实施意见》。

01 政策要闻

中共中央 国务院印发《党和国家机构改革方案》组建国家数据局—2023 年 3 月 16 日

组建国家数据局，由国家发展和改革委员会管理。将中央网络安全和信息化委员会办公室承担的研究拟订数字中国建设方案、协调推动公共服务和社会治理信息化、协调促进智慧城市建设、协调国家重要信息资源开发利用与共享、推动信息资源跨行业跨部门互联互通等职责，国家发展和改革委员会承担的统筹推进数字经济发展、组织实施国家大数据战略、推进数据要素基础制度建设、推进数字基础设施布局建设等职责划入国家数据局。

中共中央 国务院新闻办公室发布《新时代的中国网络法治建设》白皮书—2023 年 3 月 16 日

2023 年 3 月 16 日，国务院新闻办公室发布了《新时代的中国网络法治建设》白皮书，系统总结了从 1994 年全功能接入国际互联网以来，中国网络法治建设的理念实践、经验做法。白皮书指出，中国的网络法治建设坚持以人民为中心，通过立法构建公民个人信息权益保护体系，坚持发展和安全同步推进，将网络法治建设融入全面依法治国战略布局，为互联网健康有序发展、网络空间治理提供保障。

中共中央 国务院印发《数字中国建设整体布局规划》2023 年 2 月 27 日

《规划》明确了两大发展目标：到 2025 年，基本形成横向打通、纵向贯通、协调有力的一体化推进格局，数字中国建设取得重要进展。到 2035 年，数字化发展水平进入世界前列，数字中国建设取得重大成就。要实现目标需要强化两大能力、夯实两大基础、推进五位一体，优化两大环境。

中共中央 网信办关于开展网络安全服务认证工作的实施意见—2023 年 3 月 29 日

为推进网络安全服务认证体系建设，提升网络安全服务机构能力水平和服务质量，根据《网络安全法》《认证认可条例》，市场监管总局、中央网信办、工业和信息化部、公安部就开展国家统一推行的网络安全服务认证工作提出意见。

02 行业动向

2022 年我国大数据产业规模达 1.57 万亿元

从日前举行的 2023 中国国际大数据产业博览会新闻发布会上获悉：2022 年我国大数据产业规模达 1.57 万亿元，同比增长 18%，成为推动数字经济发展的重要力量。大数据产业是以数据生成、采集、存储、加工、分析、服务为主的战略性新兴产业，是激活数据要素潜能的关键支撑，是加快经济社会发展质量变革、效率变革、动力变革的重要引擎。

2022 年我国网络安全产业发展现状分析及展望

网络安全是我国总体国家安全观的重要组成部分，积极发展网络安全产业是构建安全、稳定、繁荣的网络空间的重要依托，也是数字时代国家安全的战略基石。2023 年 3 月 27 日，《中国信息安全》杂志根据 2022 年网络安全产业发展现状进行分析并提出展望。

03 产业调研

工业和信息化部办公厅：做好 2023 年信息通信业安全生产工作的通知—2023 年 3 月 15 日

国家高度重视通信行业安全生产工作，为进一步强化通信行业责任落实、提升治理能力、夯实安全基础，防范化解通信建设工程、网络运行等各环节风险隐患，要求各基础企业加强核心机房、数据中心建设，推动安全生产治理模式向事前预防转型，以高水平安全支撑信息通信业高质量发展。

工业和信息化部：关于印发《电信领域违法行为举报处理规定》的通知—2023 年 3 月 15 日

2023 年 3 月 15 日，政府针对通信行业印发违法行为举报处理规定，规范电信领域违法行为举报处理工作，制定举报处理规则，维护电信市场秩序，保护电信用户合法权益，提升依法处理能力和水平。

04 资质动态

国家市场监督管理总局、中央网络安全和信息化委员会办公室、工业和信息化部 、公安部联合发布《关于开展网络安全服务认证工作的实施意见》-2023 年 3 月 15 日

《实施意见》将推进网络安全服务认证体系建设，强化网络安全服务机构能力水平与服务质量的管控，加强网络安全服务机构认证证书的公信力度，鼓励网络运营者等广泛采信网络安全服务认证结果，促进网络安全服务产业健康有序发展。

05 观点撷英

中国互联网协会副秘书长裴玮：法治力量护航数字中国

网络法治建设是伴随中国互联网发展全过程走过来的，在不同阶段都要应对不同的问题、解决不同的问题。《新时代的中国网络法治建设》白皮书非常全面地、系统地梳理了中国互联网法治建设的经验、道路，也展示了成果，明确了法治建设的方向。

来源：《焦点访谈》

北京社科院研究员王鹏：关于组建国家数据局

地方上的大数据管理局基本是在管政府数据，或者是配合发改委、办公厅系统做政务相关的工作。国家层面的数据局成立后，需要一段时间进行职能的划分与整合，未来应该会重新建立一套从中央到地方，甚至延伸到各部委的一套数据管理系统。国家数据局可包涵的内容很丰富，小到数字政府，大到数字经济，甚至说数据要素市场改革也归口国家数

据局，集中优势资源来实现相关战略目标，对相关行业来说，这是利好消息。

来源：澎湃新闻数字经济新机遇！组建国家数据局，统筹数据资源整合共享开发利用

06 匠心护航

2023 年第一季度国家加强数字中国建设行动可谓是一刻也没有停歇。如上述新闻所说，中共中央、国务院印发《数字中国建设整体布局规划》，提出筑牢可信可控的数字安全屏障，切实维护网络安全，增强数据安全保障能力；组建国家数据局，推动数字化理念深入人心，营造全社会共同关注、积极参与数字中国建设的良好氛围。

作为数字中国建设的支持者之一，亿赛通在数据安全领域发力，助推数字中国及企业数字化转型。目前，亿赛通已是国家认证的双高新技术企业，并取得工信部“专精特新”小巨人企业认证并获得资质荣誉共计 700 余项。曾深度参与《数据管理能力成熟度评估方法》国家标准、9 项团体标准、7 本行业白皮书的编制；入选 IDC 调研机构《中国数据泄露防护市场份额，2021》、《IDC TechScape: 中国数据安全技术发展路线图，2022》等 10 余本行业调研报告；在 CCID 报告中连续 7 年稳居中国数据泄露防护市场占有率第一宝座。与 50 家 + 联盟协会达成深度合作，入选 13 家数据安全工作组，为多个数据安全项目输送行业专家。专业的产品与服务通过行业主管机构的检测，并获得高度认可。

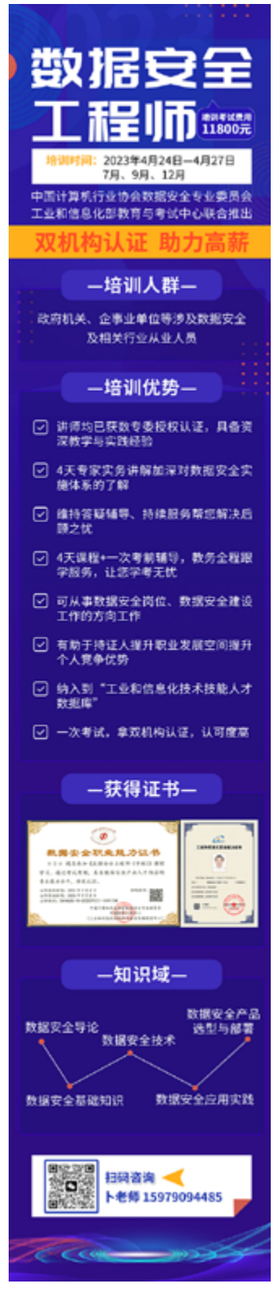
建设数字中国离不开数据安全，下一步，亿赛通会继续助力企业数据安全能力的全面提升，在企业数字化转型过程中帮助其树立牢固安全意识，强化数据安全技术措施同步规划、同步建设、同步使用要求，增强基层数据安全防护能力。

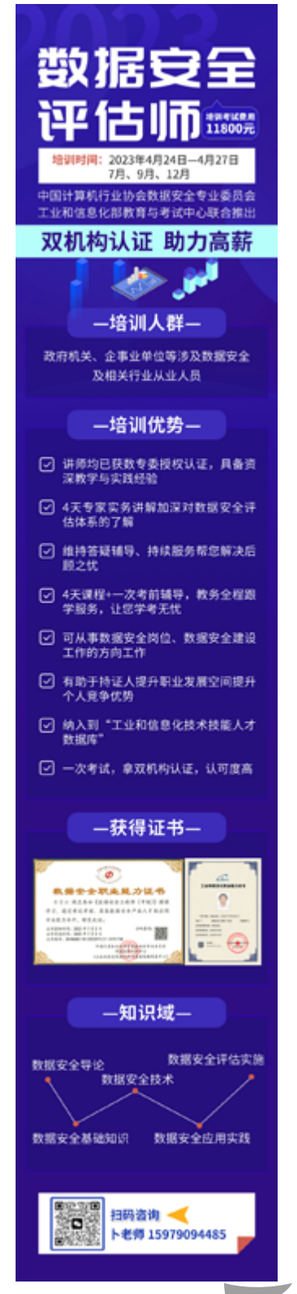
数据安全职业能力培训即将开班，聚焦“数据安全人才培养”

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

由工业和信息化部网络安全管理局指导，中国计算机行业协会数据安全专业委员会与工业和信息化部教育与考试中心联合推出的数据安全能力培训正式开始招生！

目前已开设数据安全工程师、数据安全评估师两项课程。学员通过培训掌握数据安全基础知识，了解数据安全评估体系，熟悉数据安全评估技术，综合提升数据安全评估能力，使其大幅度提升在数据安全领域工作中的竞争力。同时，也通过考试选拔掌握坚实基础理论和系统专业知识，可以从事数据安全评估、建设工作的高级特定人才，促进数据安全产业发展。





数据泄露问题严峻，美国卧底警察起诉市政府

如今，数据安全和隐私保护是各国政府和企业及其注重的问题，一些企业因数据、用户隐私泄露而被开出高额罚单的案例也越来越多。一个名为“杀手警察”（Killer Cops）的网站公布了 9300 名警察的照片、姓名和工作地点。其中，有不少还是卧底警察，4 月 4 日，超过 300 名洛杉矶卧底警察起诉洛杉矶市政府和警察局，因为此次的数据泄露问题，导致他们紧急结束卧底任务，并且自身及家庭受到严重的人身安全威胁。

有消息称，这么严重的实践，洛杉矶市警察局居然没有提前通知他们及时中止卧底任务，而是等到媒体公布之后，这些卧底警察才得知消息。现在，他们已经不能再担任卧底警察，在某些情况下，他们可能无法继续从事警务工作。

虽然每天都会有泄露事件，但此次事件尤其严重，已经威胁警察的生命。在数字经济的发展中，因数据泄露造成的损失也剧增。从全球数据安全发展的角度来看，政府、高新技术企业等单位发生泄密事件的概率普遍较高，那么，数据泄露普遍是什么因素引起的呢？

技术安全风险因素

1. 重视不够，投入不足；

2. 安全体系不完善，整体安全还十分脆弱；

3. 关键领域缺乏自主产品，高端产品严重依赖国外，无形埋下了安全隐患。

人为恶意攻击

相对物理实体和硬件系统及自然灾害而言，精心设计的人为攻击威胁最大。人的因素最为复杂，思想最为活跃，不能用静止的方法和法律、法规加以防护，这是信息安全所面临的最大威胁。

数据安全管理薄弱

数据泄露、破坏信息的完整性、拒绝服务、非法使用 (非授权访问)、窃听、业务流分析、假冒、旁路控制、授权侵犯、抵赖、计算机病毒等等，这些情况都会给数据窃取、数据破坏者以可趁之机。

亿赛通作为中国数据安全专家，一直替您思考该如何管理数据资产，并针对泄露隐患，研发出“分放管服”数据安全建设理念以及一整套数据安全解决方案……

亿赛通“分放管服”数据安全建设理念来源于国务院提出的“放管服”的改革理念，应用到数据安全领域，形成一个以“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。

从业务源头落实对数据分类分级、对人分权分责，制定和实施不同的策略，通过放管结合，构建动态的、主动的、智慧的、可运营的数据安全服务与业务的体系，形成“分放管服”的正反馈闭环。另外从制度层和技术层同时入手，制度主建指导数据安全体系建设，做到有规可依，技术主战保障制度实施，做到有规必依；违规必纠；通过技术不断发现风险补制度漏洞，优化制度，通过制度对技术创新提要求，形成制度和技术的循环优化闭环。

在数据安全建设理念的指导下，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，对数据的全生命周期进行管理。

整个数据安全治理过程从决策层到技术层，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，为用户提供跨数据类型、存储孤岛和生态系统集成数据的产品和服务，从而实现更简单、一致的端到端数据安全，如亿赛通自创自研的数据安全运营管理平台、数据安全态势感知平台、数据安全分类分级系统、数据安全检查工具、血缘关系分析工具、企业重要数据识别。构建了自上而下、全流程、可闭环的完整链条。相较于传统数据安全方案，亿赛通数据安全治理存在更高水平的集成能力、简化的部署模型，统一的策略控制平面，以及对数据、存储、政策和适用法规的一致可见性。

数据已然成为新时代的重要生产要素，是企业业务数字化转型中的重要资产。亿赛通承诺，我司将持续履行中国数据安全专家之责，担当起保护数据所有者信息资产安全之任，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。

首例！非法获取车辆信息被判刑

随着汽车保有量增加，我国停车需求也进一步上升，加上停车位利用率不足，“停车难”成为城市发展亟待解决的问题。在智慧城市的建设中，运用互联网技术和大数据、云计算而打造的智慧停车成为应对之策。现如今，信息技术不断发展，智能停车场管理系统已经覆盖了全国许多城市的商场、酒店、小区等场所。但是便捷、先进的数字化技术同样给汽车行业带来不小的麻烦。犯罪分子会通过停车缴费的公众号、小程序以及 APP 来查询临时停车缴费信息，并组建车辆查询系统，通过访问各个智能停车管理系统收集车辆停放信息。

近日，全国首例全链条打击“非法获取公民车辆位置信息”案，在南京市鼓楼区人民法院公开开庭审理并当庭宣判。法院经审理查明，2020 年 6 月起，被告人黄某伦、李某两人，明知他人从事非法寻车业务，仍制作、提供“JTC”等程序并从中牟利。非法寻车业务经营者利用两名被告提供的“JTC”等程序，可绕过某些停车平台系统的安全防护机制，非法获取车辆停车位置信息，或者根据客户需求在车辆底部等位置安装 GPS 设备，非法跟踪车辆行踪轨迹。被告人黄某伦就接受了寻车业务人委托，给指定车辆安装 GPS 设备。经统计，截至 2022 年 5 月归案，黄某伦非法获利 113 万多元，李某非法获利 24 万多元。

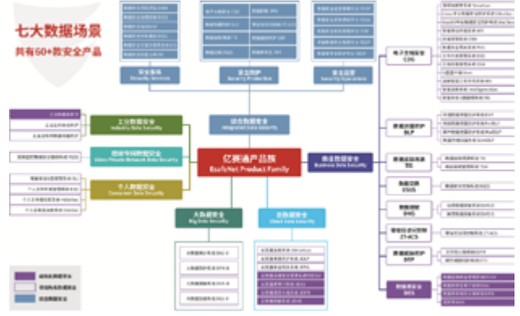
最高人民法院、最高人民检察院《关于办理侵犯公民个人信息刑事案件适用法律若干问题的司法解释》规定：“公民个人信息”，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等

南京市鼓楼区人民法院认为，停车信息及车辆行踪轨迹，反映特定自然人的生活、工作等活动情况，属于公民个人信息，应受法律保护。两名被告人明知他人非法获取公民车辆位置信息并从中牟利，仍制作软件程序，供他人使用，情节特别严重，且黄某伦还参与了给指定车辆安装 GPS 等下游犯罪。两人的行为已构成侵犯公民个人信息罪。法院当庭作出判决。被告人黄某伦、李某因犯侵犯公民个人信息罪分别被判处有期徒刑四年十一个月和三年三个月。据了解，该案涉及的非法寻车业务人、安装 GPS 人员、拖车人员等已陆续归案，相关案件正在进一步审理中。

据了解，该案涉及的非法寻车业务人、安装 GPS 人员、拖车人员等已陆续归案，相关案件正在进一步审理中。

随着设计制造业信息化的迅速发展，企业信息，尤其是文档信息如何能更有效、更安全的流转和使用成为生产商所关心的问题，文档信息的安全传输也随之成为一项重要的业务需求。制造业是我国国民经济的重要支柱产业。设计制造型企业在信息化的迅速建设下，在日常办公中大量的设计图纸、技术资料等核心数据散落的存储在企业终端、服务器、数据库等位置。伴随着愈来愈激烈的行业竞争，数据安全问题就显得尤为重要。

创立至今，亿赛通持续创新，以“分·放·管·服”数据安全建设理念为核心，以技术为支撑，对综合数据、商业数据、视频专网数据、工业数据、大数据、云数据等进行全方位多维度管理，保障各行业客户核心数据资产安全。全线产品覆盖云、网、端三大类应用场景，60 款 + 精细化产品模块，支持结构化、非结构化和半结构化数据安全管理，打造集数据安全合规、数据安全治理、数据安全防护、数 据安全流转、数据库安全、安全服务为一体的数据安全领域综合解决方案。



未来，数字化触及的领域会不断深入，安全防护的难度也会不断加大。亿赛通将继续加强研发投入，满足相关政策法规要求，响应监管重点，不断对原有产品、解决方案进行突破，打造真正意义上的数据安全领域综合解决方案，帮助客户提升安全能力，持续助力企业数据安全，助推各行业客户长远发展。

（部分内容来源于互联网）

信息泄露现象严重，网络“安全漏洞”何解？

随着信息技术的飞速发展，“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。近些年发生了多起严重的数据泄露事件，给很多企业造成严重的负面影响。接下来，让我们看看都有哪些典型案例！

某单位数据泄露案

2022 年，凉山州某单位将本应储存在单位内部信息系统的数据，违规提供给第三方公司，因第三方公司服务器被入侵导致数据泄露，且该单位存在诸多不履行网络信息安全管理义务问题。凉山公安机关依法对该单位处以警告并罚款 100 万元，对直接责任人处以警告并罚款 1 万元的行政处罚。

李某间谍案

2021 年 10 月以来，眉山籍人员李某通过 QQ 寻找“捞偏门”挣快钱的方法，被境外情报人员策反，为对方拍摄我国某港军事基地及军舰视频、照片（经国家权威部门鉴定为 6 件机密级、3 件秘密级），前后获取非法收入 14 万元。2022 年 2 月，眉山市公安机关成功侦破该案，对李某依法刑事打击，及时消除了安全隐患，有效遏制境外敌对势力渗透策反窃密的猖獗势头。

员工信息泄露案例

大数据平台员工电脑遭 Stealer log 病毒木马攻击，造成数据泄露。2023 年 3 月 1 日，有公司在暗网发现有黑产出售某大数据平台的数据，包含 50W+ 条 Json 格式涉及姓名、手机号、部门等字段的数据。该公司情报研究员根据过往黑产发布的信息分析发现，绝大部分数据都是从数据库获取，涉及国家、行业广阔，大概率是通过 MongoDB、MySQL 等数据库弱口令或未授权等方式获取。经专家分析和溯源，发现该数据泄露事件由 Stealer log 导致。起因是员工个人电脑中过病毒木马，连接过公司的 PostgreSQL 数据库被 Stealer log 记录了下来，因该数据库可被公网访问，黑产直接连接数据库即可窃取。

快递运单信息泄露

有公司监测到，Telegram 上有黑产在出售某快递的运单信息数据，字段包含运单编号、产品类型、收件人地址、手机号、姓名，派送员姓名等，一天可提供的数据 5 万 + 条，价格为 0.9 元一条。通过调查，根据黑产透露的后台带水印的截图，定位到此次数据泄漏事件由于离职员工账号权限未及时收回导致。目前，该快递平台已收回离职员工权限并反馈警方，窃取数据的黑产已拘捕在狱。

从以上的案例可以看出，在大数据时代，隐私数据泄露所涉及的范围日益扩大，这不仅侵犯用户的隐私权、侵害公民生命财产安全，还将对互联网企业自身造成不可预估的经济损失，数据泄露后对企业声誉的负面影响也很难消除。

二十年来，亿赛通主要涉及数据安全、网络安全及安全服务三大业务，以数据资产防泄密为核心，以网络安全为基本框架，以协议识别解析为技术支撑，对数据进行智能识别、智能分类和智能加密，保障企业核心数据资产安全无泄露，打造数据安全领域的综合解决方案。

亿赛通数据安全运营管理平台（简称 :DSOP），产品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。

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，平台也会用到。

共建网络安全

随着数字化经济高速发展，各行各业都与数据信息深度捆绑，信息安全无疑成为各大领域发展的当务之急，各个行业都应重视起来。亿赛通作为中国数据安全防护专家，将凭借自身的产品技术优势，多年的数据安全实践经验，继续为客户做好安全服务，保障用户核心数据无泄露。

菲律宾政府多部门数据遭泄露，安全问题刻不容缓

4 月 20 日消息，菲律宾一家网络安全公司称，该国超过 120 万条记录在网上泄露，其中包括菲律宾多个政府机构的申请人和雇员的敏感信息。

这次大规模的数据入侵暴露了 817.54GB 的申请人和雇员记录，涉及的机构包括菲律宾国家警察 (PNP)、国家调查局 (NBI)、厘务局 (BIR)、特别行动部队 (SAF) 等多个国家机构，将数百万菲律宾人的个人信息置于危险之中。暴露的记录包括高度敏感的数据，例如指纹扫描、出生证明、纳税识别号 (TIN)、纳税申报记录、成绩单，甚至护照复印件。此外，此次泄露的数据还包括针对执法人员的内部指令。

撰写报告的网络安全研究员写道：“这些是来自最高领导层的命令，内容涉及如何执行哪些法律以及哪些优先事项或需要的额外培训等。我无法进一步确认或验证该数据库中包含的这些文件的准确性或真实性。因此，我无法保证文件内容准确或可靠。”

他补充道，这些政府文件存储在一个不安全、不受密码保护的数据库中。他说：“个人可以通过互联网连接轻松访问并且容易受到网络攻击或勒索软件的攻击。当执法人员的个人文件被曝光时，他们将面临风险，但此类袭击并未发生。”

他最后表示：“任何泄露属于警察和执法人员或其他官员的个人信息的数据泄露都可能是危险的。数据泄露的个人可能成为身份盗用、网络钓鱼攻击和一系列其他恶意活动的潜在受害者。政府记录在不安全的数据库中的可用性引发了对潜在国家安全问题的担忧。暴露的记录还可能允许犯罪分子以执法人员为目标进行勒索或其他计划。”

根据该报告，该数据库被暴露了至少六个星期。然而，该研究员建议进行全面的取证审计，以“充分了解漏洞的程度和影响”。

在信息化的网络时代，各种失窃行为都已利用高技术、高科技的信息化手段进行非法活动，所以无论企业、个人以及国家，各行各业都高度重视数据资产的保护。频繁发生的泄露事件，一次又一次用刻骨的事实为信息安全管理敲响警钟。各国普遍重视安全领域的立法，对关键信息基础设施保护、个人信息安全保护、数据安全管理等方面事项进行法律规定。在与其他国家进行合作和竞争过程中，如何保障国民和企业利益是各国政府高度重视的问题。

亿赛通曾与众多重要行业携手打造客户信息安全，既保证企业业务较高的可用性、可靠性、保密性，又对内部核心数据有较强的防御、管控能力，如电子文档安全管理系统，实现了企业内部电子文件的加密存储。无论是由人工生产还是由应用系统生成的，只要写在磁盘上就是加密形式，倘若未经合法许可将加密文件数据体带走，加密文件内容将不能够被正常打开，从而确保文件内容不会因为文件数据扩散而泄密。同时，通过信息安全边界的建立，降低核心数据资产如源代码、设计图纸、财务数据、经营分析以及其他任意信息资产有意或无意泄密风险。此外，配合完善的信息安全咨询服务，对企业的业务进行梳理和流程建立，保障企业的核心业务正常运转，同时不影响用户工作习惯及业务效率。

面对这些随时都在发生的攻击事件，亿赛通作为中国数据安全专家提醒大家，无论企业还是个人，都要注意隐私数据的保护，企业尽快利用起专业技术，规避泄密风险；个人不要在网上或是公共场所随意泄露自己信息内容，加强安全意识，筑牢安全防线。

（部分内容来源于互联网）

亿赛通助某银行全方位打造数据安全解决方案，提升企业数据安全保障能力

数据是银行的重要信息资产，包括业务数据、生产运维数据和办公文档等。随着信息化技术的快速发展和广泛应用，各类生产经营和安全运行相关的文档数据增长迅速且愈发关键。为满足《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《商业银行内部控制评价指南》、《银行业金融机构信息科技外包风险监管指引》等法律法规和监管要求，实现某银行重要文档数据的安全管控目标，计划引入文档加密防护、权限控制等技术措施，有效防范信息泄漏风险。

根据某银行电子文档数据安全管控需求，亿赛通采用电子文档加解密安全防护产品，对文档数据进行加密和权限管控，确保银行电子文档数据只能在通过员工身份认证的电脑、手机等终端环境中进行授权的阅读、编辑等操作；外发电子文档数据只能通过申请、审批、授权后才能制作和外发使用，并可根据需求设置外发电子文档数据的密码、使用时限、使用次数等安全策略。

亿赛通新一代电子文档安全管理系统（简称：CDG）是一款融合文档加密、数据分类分级、访问控制、关联分析、大数据分析、智能识别等核心技术的综合性数据智能安全产品。产品包括透明加密、智能加密、权限文档、数据分类分级、终端安全管理、文件外发管理、集团管控、数据安全网关、加解密接口中间件、U 盘客户端十大核心组件，保护范围涵盖终端电脑（Windows、Mac 和 Linux 系统平台）、智能终端（Android、iOS）以及各类应用系统（OA、知识管理、文档管理、项目管理、PDM 等），能够对企业核心数据资产从生产、存储、流转、外发到销毁进行全生命周期保护。通过对“有意”、“无意”两种数据泄漏行为作统一防护，采用“事前主动防御，事中实时控制，事后及时追踪，全面防止泄密”的设计理念，配合身份鉴别、数据分类、密级标识、权限控制、应用集成、安全接入、风险预警以及行为审计等能力，全方位保障用户终端数据安全。

图 新一代电子文档硬件产品展示

项目需求

1、目前行内文档均为明文存储，数据的随意外发及使用有很大的数据泄露隐患。

2、业务人员通过报表系统、大数据平台等下载数据，在办公网终端环境消费数据。

3、将亿赛通 CDG 流程申请与银行 OA 系统集成对接，实现通过 OA 待办任务机制进行流程审批。

4、CDG 加密系统中的组织部门和用户信息需要定期从银行系统中同步。

5、为提高企业内部数据协同和高效运作，实现内部办公文档内容流转安全可控，实现文档信息再传输、交换、外发等过程中的保密性和完整性。

项目实施

文档透明加密

采用全透明强管控策略，对程序产生的办公文件编辑保存后自动加密，其余全行采用半透明加解密策略对程序产生的办公文件和存量的历史文件进行加密，用户可根据需要行内数据安全管理规范选择对敏感文件进行加密，降低核心信息资产的泄密风险。

业务系统上传下载加解密（网关）

使用安全网关来完成员工上传密文到业务系统，根据设置的安全策略进行文件加解密处理，保证整个系统上传下载文件的安全，防止有人非法盗取业务系统中的数据，有效地保障了业务系统的连续性和服务数据的安全性。

解密流程集成 OA

实现文件解密审批流程，仅处理该银行组织架构（即同步的组织架构）的申请、审批推送。

人员组织架构同步系统

CDG 系统与银行系统对接同步，实现自动和手动完整同步人员组织架构及用户信息。

文件外发安全

亿赛通拥有手机客户端，可实现手机上流程审批及加密文件预览（支持安卓和苹果系统及鸿蒙 2.0）。核心数据对外发布时，通过对数据进行加密和授权封装，保障数据在外部环境的存储及使用安全。

项目成果

1、对银行办公环境中的文档数据安全进行加密控制，针对内部生成文档进行更好的安全防护。

2、实现文件上传到应用系统时自动解密，保障文档可正常在应用系统页面进行预览使用，下载到终端时自动加密，保障业务系统中重要文档在传输中的安全。

3、实现核心数据在使用、流转、存储等各个环节的安全可控，做到“事中全程控制、事后有据可查”。

4、完成电子文档安全管理系统的文档解密流程等审批流程与银行 OA 系统的待办任务等流程模块对接，实现申请人发起文档解密流程后，审批人可在 OA 中收到解密申请的待办审批消息，点击后可跳转到电子文档安全管理系统的审批页面执行审批动作。

5、完成电子文档安全管理系统与银行系统组织架构和用户信息的同步，实现银行涉密数据安全，达到项目建设目标

现代数字化经济高速发展下，银行和金融机构在日常经营活动中积累了大量数据。充分挖掘这些数据资产的使用价值，可以为金融行业带来极大的经济效益和竞争优势。然而，一旦这些业务数据丢失、损坏或泄露，则有可能造成巨大的经济损失。为保障银行数据资产安全，亿赛通提供稳定可靠的文档加解密能力、丰富的权限分配能力和灵活的策略配置能力的解决方案，从而提升企业内部信息安全建设水平，保障企业核心竞争力。

金融行业部分客户案例

农业银行 | 北京银行信用卡中心 | 人民银行

宁波银行 | 中国邮政银行 | 泉州银行

中英人寿保险 | 上海国际集团 | 太平洋保险

中信信托 | 华夏基金 | 华泰证券 | 中信证券

亿赛通联合文旅部加强数据安全合规建设，深化数据分类分级管理

数据分类分级是数据合规治理工作的重要环节，是完善数据安全保护的重要步骤，是推进政务信息共享的重要保障，是提升数据使用价值的重要手段。《国务院办公厅关于建立健全政务数据共享协调机制加快推进数据有序共享的意见》《全国一体化政务大数据体系建设指南》《政务数据共享管理条例（草案征求意见稿）》连续强调，政务部门要建立数据目录分类分级管理机制，明确数据分类分级等具体制度和要求，加强政务数据分类管理和分级保护，切实保证政务数据共享安全。

“文旅部共享交换平台数据分类分级项目”以文旅部共享交换平台为试点，在现有的数据分类分级合规要求和方法理论的基础上，聚焦共享交换平台中汇聚、存储、流通的全量数据，通过数据盘点分析、数据分类分级策略的制定和实施，理清平台数据内容，明确敏感数据类别和安全等级，进而为共享交换数据定制差异化安全防护要求，“以点带面”，为文旅部提升数据管理水平和安全防护能力，全面推进数据安全工作提供有价值参考。

亿赛通作为《文化和旅游部政务数据共享交换平台数据分类分级研究》课题的承接单位，基于文化和旅游部的数据安全保障需要，提供的数据资产盘点、数据分类分级、数据差异化安全防护能力建设规划等服务获得文化和旅游部信息中心的高度认可。根据文旅部需求，我司通过数据资产盘点，厘清平台数据内容，明确敏感数据类别和安全等级，完成数据分类分级策略的制定和实施，进而为共享交换平台的数据制定差异化安全防护方案，例如《共享平台数据资产清单》、《共享平台数据分类分级规则》、《共享平台数据分类分级清单》、《共享平台数据安全管理规范》、《文化和旅游部系统数据分类分级工作方案》等。

亿赛通数据安全分类分级系统（简称 :DSCG）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。

项目实施

在分类分级策略实施的过程中，亿赛通数据安全分类分级系统通过丰富的敏感数据识别规则和灵活的类别级别匹配模型，为策略的高效实施和成果的完美展现提供了重要支撑。

在数据资产盘点阶段，通过端口扫描和流量分析，高效探查数据存储位置，精细识别多种数据源，自动化生成数据资产清单，帮助用户明确数据内容、类型、范围等必要属性，摸清数据底账，为下一步制定数据分类分级策略打好前期基础。

在分类分级策略执行阶段，通过邮箱、身份证号等明显特征数据的预定义，以及内置的行业标准和业务模版，结合为用户方定制的分类分级策略，采用语义分析、内容指纹匹配、机器学习等技术，对数据进行批量化分析处理，生成细颗粒的数据分类分级清单。

在分类分级结果审核校验阶段，通过自定义范围扫描和策略下发，配合人工进行分类分级清单的稽核完善。再依据行业实践经验的不断总结和识别规则的持续沉淀，不断调整数据分类分级逻辑框架，实现内置模型的持续优化。

项目亮点

1、在分类分级、敏感数据保护合规要求的基础上，基于用户业务特点、共享交换数据内容、数据安全建设现状，定制数据分类分级策略、数据安全管理方案和数据分类分级整体推进方案。

2、数据资产盘点工作以“数据”和“业务”为双中心，在对数据总量、结构、存储方式、流转路线摸排的基础上，将每项数据归集到具体司局和业务，实现数据与业务贯穿的整体路线图。

3、充分考虑后续的数据体量、数据内容、数据使用方式、合规要求等变化因素，提供可持续优化的分类分级策略方案。

4、分类分级输出成果细化到字段，并针对用户数据治理工作不完善的情况，提供相应的改进方案，充分保障分类分级结果的准确性。

5、针对数据的分级情况，落实差异化的数据安全管理制度和技术防护解决方案。

项目价值

1、数据分类分级是政务数据合规治理工作的重要环节。

文化和旅游部政务数据共享交换平台承载的数据来源广泛、种类繁杂、安全管理手段不一，通过数据分类将相同属性或特征的政务数据归集在一起，形成以类别为框架的数据资产目录; 再通过数据分级为分类后的数据评定安全等级，从而理清数据资产，并制定统一的安全管理和技术防护策略，对不同级别的数据实行更有针对性地保护，是提升数据使用质量、优化安全管理的基础性工作。

2、数据分类分级是完善数据安全保护的重要步骤。

文化和旅游部政务数据共享交换平台作为政务数据汇聚的中心，在经济和战略层面具有极大价值。

3、数据分类分级是推进政务信息共享的重要保障。

为响应国家政策号召，释放政务数据可开发、可利用的潜能，进一步提升文化和旅游领域政务数据共享比例，保证各家单位共享数据的安全，需要在已建立的政务信息资源目录基础上，制定更加细化的数据分类分级规则，通过配套差异化的安全控制措施，保障政务数据在共享开放过程中的可监测、可追溯。

4、数据分类分级是提升数据使用价值的重要手段。

文化和旅游部业务系统众多，数据总量、在线数据量、数据月增量庞大，通过开展数据分类分级工作，综合考虑数据属性、特点、数量、质量、格式、重要性、敏感程度等因素，对这些数据进行分类分级管理，梳理出非敏感、低风险等级、权属相对明确的数据资源，以要素形式优先流入数据

交易市场，同时明确在市场交易过程中应配备的安全保护措施，可以在兼顾数据安全和个人隐私保护的同时，最大限度地释放数据价值。

在数字经济时代，亿赛通在为客户护航数据安全建设的道路上从未止步。未来，我司将基于文旅部的数据安全管理需要，通过数据安全分类分级系统与数据安全管理平台和防护组件的联动，为文旅部提升数据管理水平和安全防护能力，全面推进数据安全工作提供有价值参考。

亿赛通牵手新奥集团保障信息安全无懈可击，共同助力能源行业安全发展

能源是国家的基础和支柱行业，是我们日常各项工作和生活的基础与保障。随着能源行业的发展和业务规模不断扩大，各大企业实现业务过程中，总部与各个分支机构需要实时信息传输和资源的共享。在数据传输上既要保证内部业务网络较高的可用性、可靠性、保密性，又要对内部核心数据有较强的防御和管控能力。新奥集团为河北省头部企业，1989 年创立于河北廊坊。为配合监管机构对数据安全的监管，防止重要数据外泄，提高集团数据安全保护能力，集团计划在云平台上建设统一数据库审计能力，供集团下属企业使用，保护集团数据资源和效益，同时要求不影响日常办公和研发产生。

关于新奥集团

新奥集团以“创建现代能源体系、提高人民生活品质”为使命，致力于成为一家受人尊敬的创新型智慧企业。

1989 年新奥创立于河北廊坊，以城市燃气为起点，逐步覆盖了分销、贸易、输储、生产、工程智造等天然气产业全场景，贯通清洁能源产业链；为了人民对美好生活的向往，新奥拓展了置业、旅游、文化、健康等业务，打造品质生活栖息地。

面向数智时代，新奥为客户提供家庭品质生活和企业安能碳管理的数智城市服务。基于丰富的产业实践，新奥以“场景是基础、物联是关键、数据是资源、平台是载体、智能是目的、安全是保障”为建设思路，聚焦“气 - 能 - 碳 - 安 - 城 - 质”产业场景，链接需求侧和供给侧，通过“恩牛 + 行业数智平台”，将场景数据、产业最佳实践共建打造成为产业智能产品，助力产业智能升级。

亿赛通数据库安全审计系统（简称：DAS）是一款通过对数据库网络流量旁路采集，基于数据库协议解析和 SQL 语句还原技术的数据库安全审计系统。系统实现数据库访问行为的监控和审计，并对其中危险操作向管理员实时告警提醒；系统还对数据库历史访问行为记录进行多维度统计分析，并利用丰富图表进行可视化展示。系统独立于数据库进行部署和配置，无需应用系统和用户网络环境改造，提供可靠数据库安全审计服务。

项目需求

1、建设统一集团数据库审计能力

在集团云平台上构建统一数据库安全审计能力，提供下属企业和单位使用。

2、满足安全监管要求

满足集团和下属企业在等级保护建设中对数据安全审计的合规要求。

3、满足自身数据安全要求

1）利用数据库审计能力，实时监控数据库访问行为，及时上报高危风险；

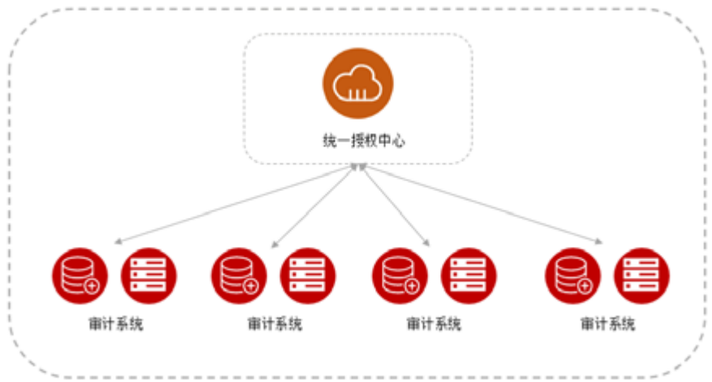
2）利用数据库审计，全面记录数据库访问操作行为，为风险事件事后溯源提供依据。

项目实施

亿赛通数据库安全审计系统实现对数据库所有访问行为的监控和审计，并对其中的危险操作可通过多种方式进行告警提醒。系统对数据库历史访问行为进行多维度的统计分析，并利用丰富图表进行可视化展现，具体内容如下：

1、操作记录全量审计

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



2、危险操作实时监控

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

3、操作行为统计分析

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

4、安全审计合规报表

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

5、轻量旁路阻断能力

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

项目成果

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

项目价值

价值一：满足集团客户等保合规数据安全方面需求

通过建设集团统一数据库审计系统能力，满足集团各子公司在等级保护等合规方面的监管和测评需求。

价值二：实现了集团数据库安全统一建设和管理

在满足集团各子公司合规需求的同时，实现了集团数据库安全能力的统一建设和集中管理，实现了数据库实例的集中授权管理和灵活分配。

价值三：满足了自身数据库风险监测和上报需求

满足集团对数据库使用行为记录和安全风险监管的要求，准确展示和汇报集团 / 分公司各数据节点的访问情况和安全风险，提高数据安全监管能力。

项目意义

本项目可作为综合性企业集团以及能源行业头部企业，首个云上数据安全运营增值项的标杆型案例，助力新奥集团在数据库审计能力上更上一个台阶。

成都农商行签约亿赛通定制化安全策略，合力打造金融行业安全堡垒

随着成都农商行的高速发展和信息化工作的推进，越来越多的涉密文档以电子化的形式流转，一方面极大地提高了工作效率，另一方面也令泄密风险俱增，这些文档一旦失控，损失将会难以估计。而企业现有的涉密数据管理仍然集中在存储环节，流通环节则缺乏有效监管，无论是在公司内部还是外部，分发出去之后的文档没有得到全程控制，形成相当严重的安全隐患，建立一个架构于全企业的文档安全管理体系已经成为一个非常关键和迫切的任务。

成都农商银行

成都农村商业银行股份有限公司（以下简称：成都农商银行）是在原成都市农村信用社基础上改制成立的股份制商业银行，于 2010 年 1 月 15 日挂牌开业。2011 年完成增资扩股，注册资本达到 100 亿元。2020 年 6 月，完成股权结构调整，回归市属国企属性。

目前，全行设有各层级机构 654 家，其中总行营业部 1 家，分行 8 家，支行 205 家，分理处 440 家。在山东、江苏、福建、河北、四川、云南、新疆等地发起设立了 39 家中成村镇银行，形成跨区域发展。截至 2022 年末，全行资产总额 7200 亿元，各项贷款余额 3600 亿元，各项存款余额 5065 亿元。

项目需求

近年来，成都农商银行在金融行业的合规要求下，启动信息安全系统的建设，旨在强化行内终端信息安全的管控力度。并且随着业务的不断发展，行内日常工作和应用场景的日益复杂，保密意识欠缺造成的日常人为操作等不可控因素越来越多，给银行信息安全管控带来更大的挑战。为此，成都农商银行为有效防范重要业务数据因主动或被动原因造成的泄漏风险，联手实施经验丰富的亿赛通，建设银行数据防泄露系统项目。

项目实施

应用到银行办公网下总行及其分支行下所有部门：

1、办公文档发送审计

采用 DLP 文件类型策略：关联办公文档的文件类型，即可对办公文档通过系统适配的渠道发送记录进行审计。

2、含敏感关键字的文档及图片文件外发审计

采用 DLP 关键字策略：可设置敏感关键字，及关键字出现的阈值，对文档内容进行检查，对图片文件进行 OCR 识别，符合规则的文档或图片进行审计处理。

3、邮件白名单

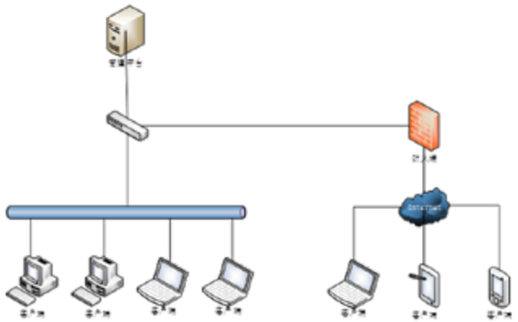
针对行内邮件地址设置邮件目的地址白名单，通过邮件客户端（FOXMAIL、OUTLOOK）发送的加密附件自动防护。

4、应用系统防护

采用终端 DLP 系统，对邮件客户端，共享文件，QQ、腾讯通等途径外发的信息进行防护，只有安装了 DLP 系统的终端才能解密查看，即保证业务系统不受影响，同时保证终端文件安全可控。

5、流程审批申请

采用终端 DLP 系统，用户可以通过实现设定的流程进行解密流程申请，（流程解密申请与行内工单系统进行开发对接，流程在工单系统内进行单向审批，审批结果回馈至 DLP 系统）流程审批后才可以正常外发。



项目成果

基于内容识别技术，亿赛通终端 DLP 系统对敏感文件进行数据安全保护，对员工的外发的敏感数据进行关键字审计，定期扫描重要部门的敏感数据，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，有效识别敏感数据，监控敏感数据使用情况，防护敏感数据外泄，也可有效培养并提高员工对敏感文件的保密意识。

亿赛通新一代数据泄露防护系统（简称 DLP），以服务企事业单位进行数据资产梳理、数安全防护为目标。系统采用平台化管理，将终端 DLP、网络 DLP、邮件 DLP、存储扫描 DLP、API 接口 DLP 进行统一管理，模块化控制。将对数据进行分类分级扫描，实现终端数据资产梳理、文件服务器数据梳理、数据库数据资产梳理、数据加密防护、数据外发监测、终端运维管理、邮件外发控制、数据水印、端口管控。DLP 是一款融合机器学习、关联分析、密码技术、访问控制、数据标识等多种技术的综合性数据安全防护产品，该产品以数据为中心，分类分级为基础，为用户数据资产提供事前主动防御、事中实时监测、事后追踪溯源、全程态势感知，基于数据的全生命周期提供全方位、立体化防护。

亿赛通围绕新一代数据泄露防护产品强化创新，至今已取得丰硕成果。未来，我司将持续深耕数据防泄露领域，保护企业和个人数据不被泄露和滥用，肩负起数据安全企业责任，为筑牢数据安全防线贡献力量。

金融行业部分客户案例

农业银行 | 北京银行信用卡中心 | 人民银行

宁波银行 | 中国邮政银行 | 泉州银行

中英人寿保险 | 上海国际集团 | 太平洋保险

中信信托 | 华夏基金 | 华泰证券 | 中信证券