扫一扫，关注官方微信

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

亿赛通

ESAFENET

ESAFENET

亿赛通企业月刊　　中国数据安全专家　　www.esafenet.com

10 月刊

2021 年共 11 期



Esafenet
Monthly magazines

中国数据安全专家

主办：亿赛通

策划：市场部

北京亿赛通科技发展有限责任公司

地址：北京市海淀区西二旗大街 39 号 A 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com



本刊为亿赛通企业月刊，欢迎交流，禁止转载

CONTENTS 目录

刊首语 PREFACE

2/3 《亿赛通十月刊》教你如何系上信息领域的“安全带”

行业聚焦 INDUSTRY FOCUS

4-8 国内行业新闻

9-13 国外行业新闻

亿赛通动态 ESAFENET NEWS

14/15 亿赛通聚焦数字化安全管理，助力《数据安全法》下的企业安全转型之路

16/17 顶级峰会再起航，亿赛通精彩亮相“天府杯”，共谋安全博弈之道

18/19 亿赛通亮相第十二届中国数据库技术大会，展现专业技术研发实力

20/21 聚焦工业设计数据安全，亿赛通出席中国工业设计软件创新峰会广东站

22/23 2021 全国信创产业发展金华论坛｜共谋信创产业安全发展之路

亿赛通小贴士 ESAFENET PROMPT

24/25 独家科普 | 亿赛通“分▪放▪管▪服”数据安全建设理念

26/27 泄露事件频发，亿赛通揭开数据黑产链中“不能说的秘密”

典型案例 TYPICAL CASES

28/29 东易日盛家居装饰集团股份有限公司

30/31 北京汽车股份有限公司

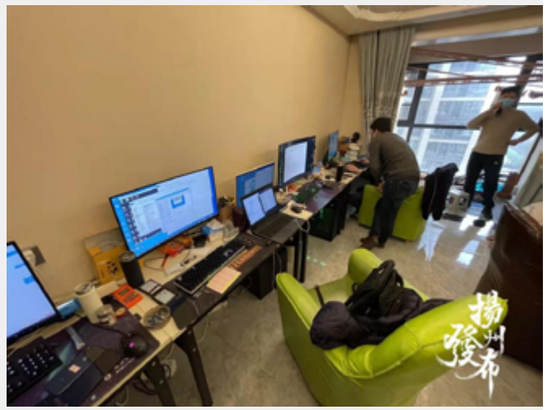
《亿赛通十月刊》教你如何系上信息领域的“安全带”

网络时代，信息安全领域的攻击和防护就像是 “矛”与“盾”的博弈。如今数字化浪潮已经汹涌而至，承载着守护使命的信息安全技术开始受到越来越多的关注，方兴未艾之势逐步显露。知己知彼，百战不殆，延伸到信息安全领域，企业需要洞察行业的发展状态及客户的需求，面对信息安全的威胁才能百战不殆。而每一次安全圈的盛会，都像是一套兵法，可以从中学习和窥探到行业的先机。十月，网安圈的多项大型活动逐一拉开序幕，除了网络安全周、天府杯等大型活动，各个行业论坛、峰会也争相起航，工业设计行业峰会、信创论坛、数据库技术大会……亿赛通在这些会议中分别从安全意识、技术创新，生态建设等方面，与行业专家、领导进行探讨。跟随《亿赛通十月刊》一起，查看本月精彩内容。

刊首语 PREFACE

国内

1、快快网络协助江苏警方破获 1.2 亿条数据泄露案



摘要：近日，厦门快快网络安全团队协助江苏扬州警方成功侦破一起游戏版本数据遭遇泄露的案件，涉案资金近千万元。2020 年，快快网络接到用户举报，有不法分子窃取游戏版本，使得游戏版本数据发生了泄露。接报后，快快网络安全团队立即将情况移交给公安机关，并迅速抽调安全风控团队精英人员组建专项行动小组，连夜赶往扬州协助网安部门对机房相关服务器开展现场勘验，提取木马文件样本。

2、广汽埃安车联网数据泄露，车主的权益和隐私还有保障吗？



摘要：一位车主在购买广汽埃安 Y 后，被 4S 店频繁电话骚扰催要提供新车行驶证和绿本，但为了保证自身信息安全，车主并没有提供相应的证件。除此之外，车主的同事某天下班遇到一台埃安汽车堵住道路，拨打车主预留电话后过来的不是车主而是广汽埃安中心的销售人员。于是车主十分疑惑，4S 店是如何精准找到汽车停在哪里？

3、央视曝光！我的面容信息竟然这么不值钱？



摘要：据央视报道，由于国家开始规范手机卡，所有手机卡都需要实名认证，由于一些不法分子对手机卡需求量巨大，因此动起了歪脑筋，通过伪造他人的人脸视频来通过注册认证。据悉这些不法份子只需要一张静态的半身照，就能通过 AI 人工智能技术将照片里的人物依照输入的指令做出眨眼、张嘴、皱眉等多种精细动作，模仿人物表情变化，从而轻松骗过人脸识别环节。

4、上海市消保委：“蹭网神器”APP 存在信息泄露风险，建议删除！



摘要：上海市消保委表示，“蹭网神器”不仅不能实现蹭网，反而浪费用户流量，观看大量广告。并且除收集 WIFI 密码外，在安装和使用过程中，“蹭网神器”还会索取手机通话记录、位置信息、微信信息、相机、已安装应用软件列表等权限。这些权限明显与软件提供的服务业务没有直接关联，根本目的是索取消费者的隐私信息，极有可能造成个人隐私信息的泄露和滥用。

5、快递业泄露用户信息频发背后：“隐私面单”为何未大规模使用



摘要：记者调查发现，针对印有用户个人敏感信息的快递面单频频遭泄漏的问题，部分快递企业近年来推出了“隐私面单”服务，隐藏了个人姓名、地址和手机号等内容。但隐私保护服务尚未全面普及，不少快递企业在用户寄件时将隐私保护服务作为非常规选项，需要手动勾选才会开启；部分快递企业只有用户线下向快递员叮嘱才会开启隐私保护服务。

6、青海警方查处一起泄露公民个人信息案

摘要：10 月 21 日 9 时许，一则关于“新冠肺炎疫情密接人员的协查通知”在互联网上被大量转发传播。因该《协查通知》涉及紧急疫情及疫情密接人员个人身份信息，极易造成社会恐慌和不良影响，湟源县新冠肺炎疫情防控处置工作指挥部高度重视，要求立即进行查处，接到线索后，局领导抽调警力立即开展调查，同时加大社会舆情的正确引导。经过不懈努力，查证落实董某（男，汉族，现年 36 岁，湟源县人）构成泄露公民个人信息违法行为。

10 月 22 日，依法将违法行为人董某传唤到案接受询问，董某对自己泄露公民个人信息的违法事实供认不讳。10 月 23 日，因董某违反《中华人民共和国居民身份证法》第十九条第一款之规定，县局依法对其做出行政拘留 13 日并处 5000 元罚款的行政处罚决定。

7、泄露信息上万条，80 余名“内鬼”落网！



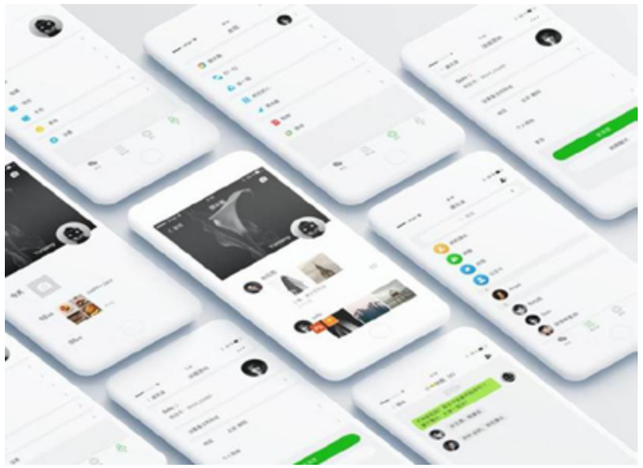
摘要：公安局网安大队在对上级下发线索核查时，掌握到某通讯营业网点存在非法向他人出售个人信息的行为。经大量信息研判和调查取证，发现该网点工作人员在用户不知情的情况下，将新入网用户的手机号码出售给他人注册网络账号从中盈利，其行为涉嫌侵犯公民个人信息罪。警方分 2 次出动 200 余名警力，成功抓获在松滋辖区内以张某、周某、刘某为首的非法买卖公民个人信息的涉案人员 80 余人，一举打掉一个涉嫌侵犯公民个人信息犯罪的团伙。其中采取刑事强制措施 26 人，行政处罚 38 人，教育训诫 10 余人，人员涉及中国移动、中国联通和中国电信营业厅（或代理点）多名工作人员。

8、大量得物用户遭遇信息泄露，网购后被“主动退款”，实际暗藏陷阱



摘要：近日，得物 App 用户秦炜（化名）向记者反映，自己的购物信息被泄露，进而遭遇了诈骗。这并不是孤例。记者在微博、黑猫投诉等平台看到，大量得物 App 用户有相似遭遇。自称得物客服或售后的人员，以“购买物品质量有问题”等为由主动提出退款，但需要用户先开通支付宝备用金或微众银行微粒贷等平台账户，以接收退款。“客服”列举的这几个产品实际都是借款产品，被诱导操作就会背上欠款。

9、用户信息疑泄露，微信引发用户众怒！还有多少“偷窥”我们不知？



摘要： 10 月 8 日，一位微博用户发表一则博文，表示自己在清理应用后台记录的时候发现，微信一直在读取自己的应用，尤其是手机相册，更是读取了很多次。我们都知道，相册里通常有着很多机主的隐私，反复读取相册，难道不是反复“偷窥”个人隐私吗？这位博主质问微信为何要有这样的举动，微信很快解释，之所以会出现反复读取手机相册的事情，是因为苹果 IOS15 系统拥有一个名为“记录 APP 后台活动”的功能，并且严肃表示微信团队并没有私下窃取用户隐私，但是对于这则声明，网友们并不买账，甚至引起了众怒，许多网友纷纷表示自己或多或少都遇到过类似的情况。

10、新密某公司 6 万余条信息被泄露 原来是“内鬼”



摘要： 郑州警方工作中发现，新密市区某公司 6 万余条用户信息遭泄露，存在重大风险隐患。进一步工作发现，新密某装修公司员工慎某龙、慎某明等人手中掌握有该批用户信息。

国外

1、黑客入侵阿根廷政府 ID 数据库，梅西、阿总统等全民身份数据泄露



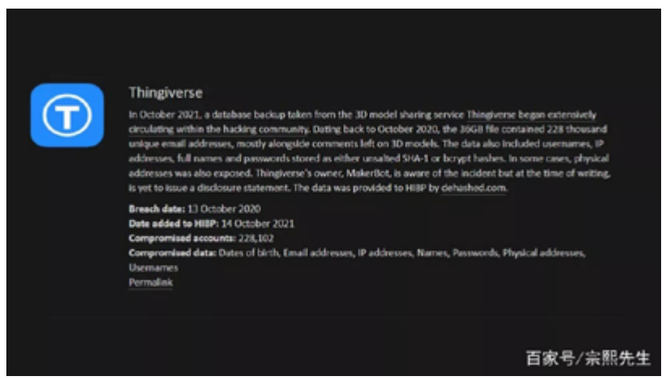
摘要： 今年九月，阿根廷政府 IT 网络遭遇了一名黑客入侵，黑客攻击的目标直指 RENAPER（全称 Registro Nacional de las Personas），即阿根廷国家人口登记处。10 月初，一个名为 @AnibalLeaks 的新注册推特账户，在推特上发布了 44 位阿根廷名人的身份证照片与个人详细信息，一下子就炸开了锅，这也导致 RENAPER 遭到入侵的证据首度浮出水面。

2、260 万个 TikTok、Instagram 用户数据泄露



摘要： 近日，安全研究人员在互联网上发现，超过 260 万的 TikTok 和 Instagram 用户数据被暴露，并下载了这些数据资料。研究人员称，这些数据出自配置错误的 Elasticsearch 服务器上，并且没有任何密码保护或加密。

3、Thingiverse 数据泄漏，黑客声称拥有其 36GB 用户数据



摘要：近日，在某黑客论坛上出现了一个容量为 36GB 数据文件，据称是该网站的用户数据库文件备份。嫌疑包含超过 2.55 亿行数据，具体内容可能为“可公开访问的 3D 模型数据，用户的电子邮件和 IP 地址、用户名、物理地址和全名”等等。

4、脸书 15 亿用户数据泄露，黑客公开在论坛售卖，还表示合法获取?



摘要：这几天对 Facebook 来说很糟糕。一场停电影响了所有的网站，有举报人称，发现黑客在论坛上公开售卖包含个人数据超过 15 亿的 Facebook 用户数据。数据被盗和公开出售的事实仍然是人们的担忧，这些数据仍可用于危害用户的安全和隐私。特别是，被盗数据包含姓名、电子邮件地址、位置、性别、电话号码和 Facebook 用户 ID 信息。这些数据可以让攻击者获得密码答案，让他们能够拦截一次性登录代码、网络钓鱼、发送诈骗短信等。

5、亚马逊旗下直播平台数据泄露，归咎于配置错误



摘要：亚马逊公司 (Amazon.com Inc .) 旗下的直播电子竞技平台 Twitch 周三指责服务器配置更改中的“一个错误”，该错误可能会让所谓的黑客泄露敏感信息。该平台表示，它仍在评估影响，并已重置了所有流键，即允许影响者和流媒体用户连接和发布内容的代码。《Video Games Chronicle》早前曾报道称，一名匿名黑客声称泄露了 Twitch 的数据，包括其客户端和未发布游戏的源代码和信息。

6、警惕网络疫苗接种证明生成器！重要个人信息瞬间泄漏，已有人被坑



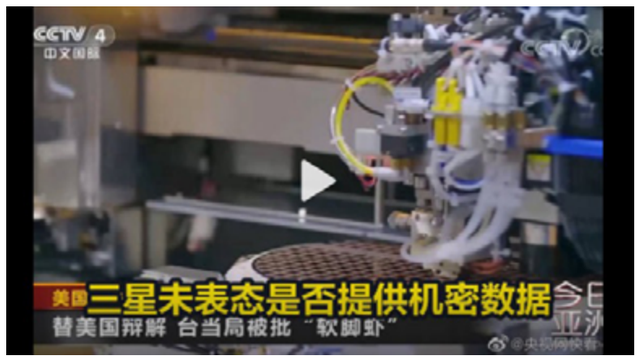
摘要：据 Herald Sun 消息，网络上最近出现了一款新冠疫苗证书生成器，被用来进行疫苗接种证明的伪造。维州反疫苗者们使用这一生成器试图重返工作岗位或进入对应场所。但他们在获得这一生成器的同时也被要求，在不安全的网站上输入个人健康信息，使他们的个人资料非常容易被盗。

7、脸书起诉控告乌克兰程序员，因其泄露 1.78 亿名用户的信息



摘要：据报道，Facebook 已对一名乌克兰男子提起诉讼，理由是控诉该男子收集大约 1.78 亿用户信息，并在市场上出售这些个人数据。在诉讼的文件中显示，被告亚历山大·亚历山德罗维奇·索隆琴科在 2018 年 1 月至 2019 年 9 月期间滥用 Facebook Messenger 功能，从其服务器上抓取大约 1.78 亿用户的信息。

8、美国“抢芯”！ # 台积电将向美国提交机密数据



摘要：今年 9 月，美国政府以提高芯片“供应链透明度”为由，要求台积电、三星等半导体企业在 45 天内交出被视为商业机密的库存量、订单、销售纪录等数据。据台湾“中时新闻网”报道， 此前声称“不会泄露客户机密资料”的台积电 22 日表态称，将会在 11 月 8 日截止日期前，把相关资料提交给美国。

9、新 MacBookPro 设计图曾被黑客盗走，苹果被勒索 5000 万美元赎金



摘要：本月，苹果推出新款 MacBookPro，但就在今年四月份，REvil 勒索病毒团伙攻击了苹果的供应商广达电脑，并窃取了新一代 14 英寸和 16 英寸 MacBook Pro 的设计图纸。之后数家政府机构联手攻击了 REvil，事情得以平息。

10、美媒称俄黑客是攻击辛克莱广播集团的幕后黑手



摘要：据塔斯社 10 月 21 日报道，美国媒体彭博社发布指控材料称，攻击辛克莱广播集团的黑客与俄罗斯有关。彭博社指出，对辛克莱广播集团的攻击是使用 Macaw 勒索软件病毒进行的，这是一种更常见的 WastedLocker 恶意软件的变体，该机构声称它是由 Evil Corp（俄罗斯网络犯罪组织）集团的黑客开发的。

亿赛通聚焦数字化安全管理，助力《数据安全法》下的企业安全转型之路



2021 年 10 月 13 日，为进一步做好新时代企业数字化转型升级与赋能，中国中化控股有限公司数字化部和中化资本主办，亿赛通及指掌易共同在北京策划承办了“数字化转型沙龙 - 数字化安全管理”主题活动。此次活动旨在推动数据安全法律法规的监管落实，促进数据安全技术交流，提升数据安全能力建设。

在活动现场，亿赛通专家以《数据安全法下的行业解决方案》为主题发表演讲，就最新实施的《数据安全法》展开讨论。《数据安全法》充分彰显了其作为数字经济时代特色的部门立法。从《数据安全法》诸多条文中均可以看出，这部法律对于促进企业数据合法利益的保护、开发和利用所体现出的立法保护决心，以及促进数字产业和数据产品的创新和利用所建立起的行业发展信念。



不难理解，安全和稳定是实现长足发展的前提，数据安全亦是如此。企业数据的分类分级、数据安全治理将成为企业今后发展的关键命题。对于企业来说，以更为积极的姿态做好《数据安全法》下的数据安全合规，既是在应对法律规则变化的挑战，更是在积极利用规则开拓的发展机遇，积累与培育新的行业竞争力与市场品牌价值。

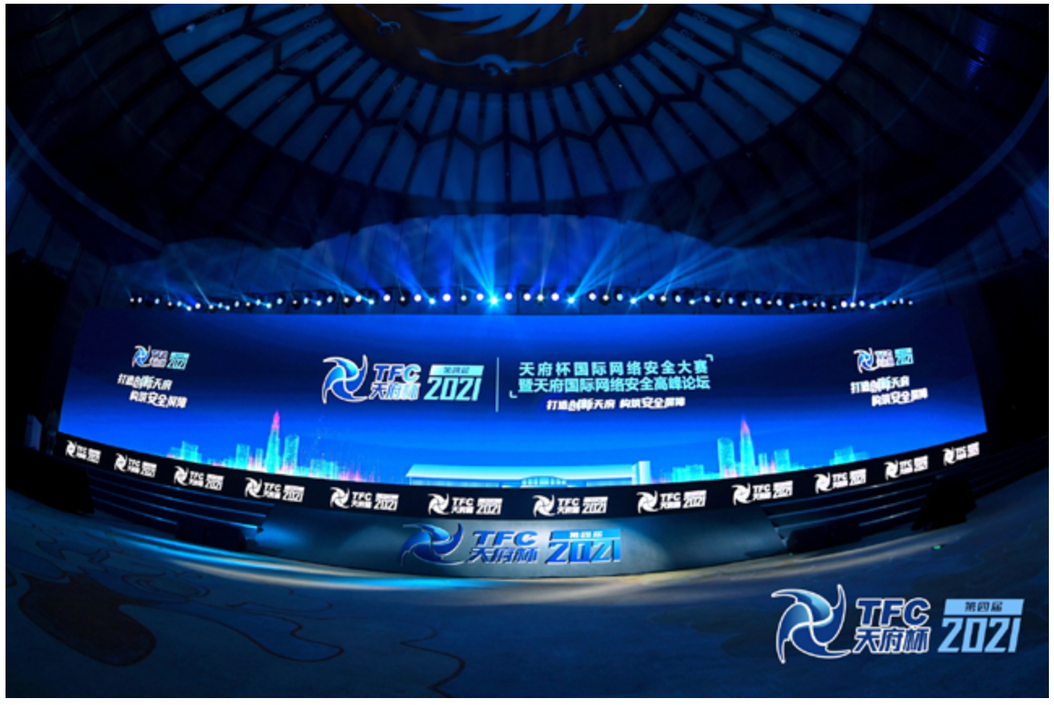


亿赛通的“分▪放▪管▪服”数据安全建设理念中的“分”，即可使企业实现：对政策制度分层合规，对权责访问对象分权分则，对数据分类分级和对资产的分布分析。从整体架构的层面来规划数据安全，是数据安全综合解决方案的基础，没有准确合理的“分”就没有有效安全的数据应用和管控。我司在服务方面为客户提供数据安全体系化服务，帮助企业理清企业数据资产，通过安全产品进行相关敏感数据资产的落地管控，通过全生命周期安全加固和数据治理，从组织架构、制度流程、技术手段、人员能力等方面帮助企业建立全方位端到端的数据安全体系建设，实现数据创造价值，驱动业务发展的安全运营。



身处数字经济发展时代当下，具有标志性意义的《数据安全法》生效，昭示着我国数据安全与治理已经站在了新的起点，开启了新的阶段。数据作为生产要素的战略性地位得到确认，企业在积极探寻数据资产管理方案与价值挖掘的同时，同样意味着应当自觉担负起数据安全保护义务和治理责任，以安全和发展为主题的数字化时代正在踏浪而来。亿赛通也必将紧跟国家与时代的脚步，不断从理论和实践层面完善数据安全建设水平，打造成熟的数据安全建设体系，让数据发挥最大价值，从而推动市场经济高速发展。

顶级峰会再起航，亿赛通精彩亮相“天府杯”，共谋安全博弈之道



一场汇集业界精英、领军企业、前沿学界和政府主管部门的互联网安全峰会迸发出新的火花，同时，也为世界互联网安全贡献出了中国智慧，锚定了未来互联网安全的方向。

10 月 16 日—17 日，为期两天的 2021 天府杯国际网络安全大赛暨天府国际网络安全高峰论坛在中国成都天府国际会议中心盛大开幕。

活动一经开幕，慕名而来的国内外互联网安全行业人士齐聚一堂。全国网络安全领域的专家、学者、科研院所和央企、民企代表，各网络安全参赛战队、选手千余人到场亮相，聚焦政策法规、产业最新发展方向、网络安全热点、前沿防护理念和技术创新、人才培养等行业前瞻热点话题，致力于促进政、产、学、研、用各界在网络安全领域的交流与合作，从而推动我国网络安全保障体系建设，推动网络安全技术产业高质量发展。

亿赛通凭借在行业内深扎多年的数据安全深厚的技术沉淀，受主办方邀约，参与本次展览。与其他与会人员碰撞出具有顶尖水平的网络安全智慧火花，进一步促进对网络安全行业的深入了解，为天府新区实现高质量发展，推动成都市建设中国网络信息安全之城持续注入新活力。



数字经济时代，个人隐私保护、企业信息安全、关键信息基础设施防护等话题不仅关系个人，更关系国计民生。如何在当前对互联网和数据信息方面进行有效保护和发展，如何在复杂的国际行业竞争中保持优势，是我们需要重视并落地解决的问题。

面对不断变化的安全挑战，亿赛通更希望联合企事业单位共建更全面的全生命周期防护系统，提供可靠有效的解决方案的同时，会同行业伙伴和客户积极探索数据安全的产业价值，助推数字经济安全腾飞。

作为一家长期致力于为政府机构、企事业单位提供全方位数据安全解决方案的企业，亿赛通对此已深耕多年。十八年前，亿赛通正式成立，专业研发文档加密产品，彼时“数据安全”还未被如此广泛知悉和应用。而随着数字化业务发展的多样化，勒索病毒、黑客攻击、内部泄露等安全问题全面爆发，我司以全生命正周期的数据安全解决方案为出口，在为政府、企事业单位提供数据安全防护的同时加入数据库审计、网络数据泄露防护、数据资产分析等功能，建立起数据安全智能管控平台，亿赛通也再次迎来了高速的市场增长。

其中以本次展出的全新数据安全建设理念“分▪放▪管▪服”为例，数据安全的首要基础工作是对数据资产的发现和梳理，即分类分级。“分”是从整体架构的层面来规划数据安全，是数据安全综合解决方案的基础，没有准确合理的“分”就没有有效安全的数据应用和管控。如果说“分”是数据安全综合解决方案的基础，“放▪管”则是方案的具体执行，通过各种类型的数据安全工具来达到合理管控的目的。“放”是指数据的流动与应用，而“管”则是指保障数据的安全。两者之间是一个需要动态精准把握的平衡关系。安全服务贯穿了数据安全体系前期的咨询规划、中期的建设和后期的运营，包括相关的人才培训和培养工作。熟悉网络安全工作的业内人士可以看出，这也正是同步规划、同步建设、同步运营，即三同步理念的体现。





政府重视和政策扶持正在不断推动信息安全产业的快速发展，尤其各大法律条文的出台，更是将数据保护提到了法律高度，加强数据安全是行业大势，势不可挡。在国家政策支持下，数据安全市场将越来越具有优势。

活动现场诸多参会人员均反馈，此次参会为网络安全行业提供了建设性的思路与实践方向，不虚此行。而亿赛通也凭借深厚的实力积淀，丰富的产品解决方案体系及广泛的客户支撑，成为展会现场最亮的星。

亿赛通亮相第十二届中国数据库技术大会，展现专业技术研发实力



作为国内备受关注的数据库及大数据领域技术盛会，每年一届的中国数据库技术大会于 10 月 18-20 日在北京国际会议中心盛大召开。作为国内安全厂商的领军企业，亿赛通携旗下最新的数据库安全产品：数据库审计系统、数据库防火墙、动态数据脱敏系统及静态数据脱敏系统和最新数据安全建设理念亮相本次大会。

随着各项新兴技术的出现，不断推动数据量高速增长，呈现爆炸式状态，在某些特定时间点某些行业的数据量也会出现并发曲线陡峭的情况，在某一个时间点数据量可能会翻十倍，几十倍。传统的集中式数据库很难适应这些业务场景，企业的数据化变革是发展的重要方向。

据权威机构统计表明，从 2015 年到 2025 年，中国数据以 14 倍的速度扩张。2018 年至 2025 年中国数据以 30% 的年平均增长速度领先全球，比全球高 3%，2025 年将增至 48.6ZB，占全球 27.8%。某调查报告显示，92% 的泄露记录来自于数据库泄密，所以数据库的安全问题成了数据安全管理的核心问题之一。

近几年，国内数据库泄露情况愈发严重，频繁揭露的新闻暴露出数据库产业的短板。由于市场需求的爆发，数据库安全产品也应运而生。



亿赛通作为国内数据安全老牌厂商，在很多人印象里还是“传统”的文档加密厂商。但亿赛通“传 & 统”却不“传统”，坚持技术创新，始终以用户需求为导向推进产品创新和技术的不断发展。

在新的挑战和机遇下，亿赛通公司对建设理念进行了大量探索。“分 • 放 • 管 • 服”数据安全建设理念被首次提出，这是亿赛通一次全方位的升级转型，是从单一的文档加密产品扩展到了数据泄露防护、数据库安全、网络安全、态势感知管控平台等产品线，并站在技术环境变化和企业发展战略的高度，如何将这样的理论有效执行并快速落地，取得市场先机？

“分 • 放 • 管 • 服”引自国务院总理李克强提出的全国深化“放管服”改革优化营商环境指导，亿赛通把其引入到数据安全创新理念之中，是因为二者理论思路相同。在数字化转型的驱动下，数据安全已经成为企业运行和发展的核心资源，整合自身内、外优势，将其作为有利的工具，结合“分 • 放 • 管 • 服”理念，亿赛通拓展了更多的合作伙伴，深耕到更多的行业，针对不同行业客户需求进行细致的安全分级，更好的服务于客户，才是数据时代的创新秘籍。



亿赛通数据库安全产品，基于先进的安全技术监测和管理手段，采用软硬件一体化安全管理模式，全方位分析预警安全隐患，从而有效地进行数据风险管理。大会中，亿赛通通过展示数据库安全相关产品，与众多嘉宾深入探讨、交流，了解数据库产业的进步，三天的展示让亿赛通备受关注。



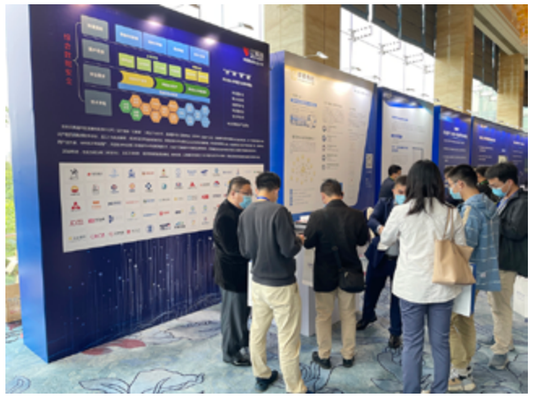
2021 年，在多项安全法律条文的颁布下，数据安全厂商迎来了属于自己的风口，肩负着新时代所赋予的使命。未来，在纷繁的数据安全技术潮流中，亿赛通公司将秉承自主创新的理念，根据市场需求不断打磨产品，以坚实的自主核心技术为基础，做数据安全行业的中流砥柱。

聚焦工业设计数据安全，亿赛通出席中国工业设计软件创新峰会广东站



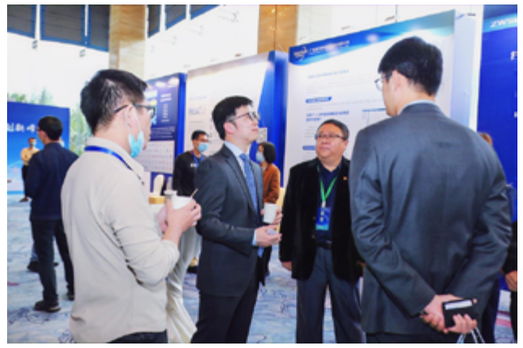
一个行业专家的创新技术往往能引起一个行业的变革，而亿赛通就是这样的革新者。2003 年，亿赛通将文档加密引入到国内，并率先研制出国内第一文档安全管理系统，掀起了行业技术变革。现阶段，亿赛通与中望软件达成战略合作，充分整合和发挥优势资源，加速核心技术的国产化进程。

10 月 22 日，由中望软件主办的主题为“自主工软 生态共赢”的中国工业设计软件创新峰会广东站正式开幕。继北京站深度合作后，亿赛通再次受主办方邀请，作为数据安全领域骨干企业在会中进行独家方案展示。



当前世界经济正处在动能转换的换挡期，新一代信息技术作为新一轮科技革命中，创新最活跃、交叉最密集、渗透性最强的领域，正在引发系统性、革命性和群体性技术突破和产业变革，通过数字化转型实现产业转型升级和高质量发展的两化融合新征程已经开启。工业软件作为设计的关键工具，在企业中的应用场景和需求日趋复杂，与企业的产品创新、智造升级休戚相关。

企业的核心设计方案在流转过程中，极易造成数据泄密。《数据安全法》及其他各项法律条文的诞生及行业需求，使数据安全在工业设计行业需求量攀升。对此，亿赛通与中望在双方专业领域中强强联手，优势互补，通过双方共同打造的设计图纸安全一体化产品解决方案，打造一张最强王牌。



双方的联合方案可以满足不同专业、不同复杂应用场景的需求，实现设计经验的有效传承及设计成果的数字化管理。

1. 对文档进行高强度加密并对使用者透明解密，满足数据安全保护的同时，操作简单，应用方便。

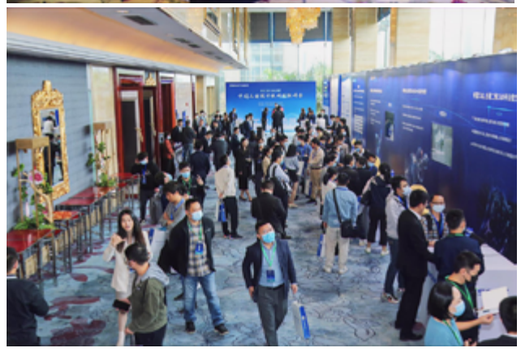
2. 根据业务需要，对需要与合作伙伴进行交互的外发图纸进行特殊处理，在满足企业正常业务运转的情况下，最大限度的保证文件的安全性。

3. 显示水印，对截屏、拍照、录屏、打印等敏感操作进行警示，同时方便进行追踪溯源。

在过去 18 年中，亿赛通实现了从文档加密厂商到综合数据安全厂商的变革。数据安全行业竞争激烈，而亿赛通所以能成为行业头部企业，除了拥有专业的自主核心研发团队外，另一原因是我们紧跟客户现实需求，根据客户需求提供服务。“分 • 放 • 管 • 服”是我们最新提出的的数据安全建设理念，通过制度主建，技术主战，分放管服，将数据实现分权分责分风险，放管结合，做到要素服务保支撑，持续安全可运营，确保数据有价值的安全流转，共赢数据安全大生态。







企业数据安全防护工作任重道远，仍需砥砺前行。亿赛通将以此为契机，向全行业展示安全产品研发实力，解决企业数据安全问题，深耕专业技术，不懈开拓创新，为保护企业网络信息安全贡献力量！亿赛通与中望将更深入的触及客户，发挥双方优势，实现技术、产品、渠道全方位互补，共同探索更广泛的合作机会，共同深化双方产业链价值的发展，推动数据安全系统与服务在更多行业落地，保障客户数据安全的同时促使其业务发展与创新。

2021 全国信创产业发展金华论坛 | 共谋信创产业安全发展之路



10 月 28 日，以“同芯同行 共创未来”为主题的 2021 全国信创产业发展金华论坛在浙江隆重召开。信创是中国坚持走信息技术应用自主创新之路的必然结果，推动信创产业加速落地，已成为产业升级和数字经济发展的重要推动力。目前，我国信创产业进步明显，但是短板依然存在。主办方希望借助大会平台，与行业专家进行深入交流与对话，分享经验、凝聚共识，汇聚各方资源，共同推动信创产业发展。亿赛通作为数据安全行业的佼佼者，并且以近两年在信创行业做出的深入推进受到主办方关注邀请。

伴随着云计算、大数据、人工智能、物联网、5G 等新技术领域的突破，以及新应用场景的逐步拓展，中国自主可控领域取得了显著成绩，为科技企业带来了历史性的发展机遇。“十四五”期间，开好局，起好步。着重强调了发展自主创新技术，要进行关键技术创新。并且信创发展的同时，随着产业纵深发展，信创产品安全能力受到了产业界的广泛关注，构建信创产品安全保障体系正当其时。

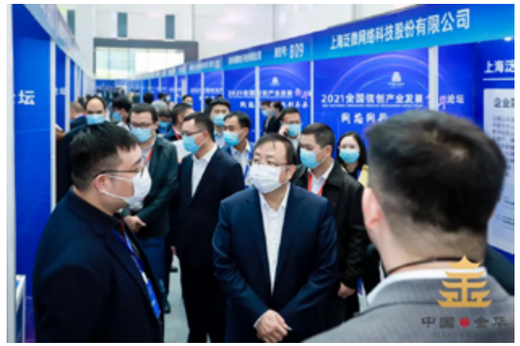
信创产业的蓬勃发展需要各种网络安全技术、产品和服务保驾护航，信创安全也面临着一些新的问题需要克服，一方面是自身弱、对手强、动机多等严重挑战，另一方面是认知偏差、能力不足、积累不足、实战不足等实际情况。因此，信创安全需要新的发展思路，积极利用新技术、新手段开展网络安全保护。



目前，数据安全行业已经有序、稳定的推进信创工作，从基础架构到应用架构。由于其对业务的连续性和高稳定性要求，各个层次的改造都需要考虑安全风险，同时由于涉及到众多的操作系统、国产芯片、版本，信创安全产品的兼容性是需要考虑的重点因素。

长期以来，亿赛通践行创新理念，为客户提供专业的数据安全产品，助力企业用户解决数据安全防护的关键难点，以多重安全能力深植数据全生命周期各个环节和业务场景，夯实安全基础。近年来，随着国家高度重视信创产业发展，出台各项政策，我司紧跟国家在核心技术创新方面的步伐和企业用户在国产化数据安全产品诉求，持续推进信创安全产品的研发和应用。

为积极支持国家信创产业发展，亿赛通早已先后完成与统信软件、达梦、中国长城科技集团、飞腾、爱数、中科曙光等厂商的兼容适配。





信创是中国信息化产业价值的转移，是所有包含中间件在内的 IT 生产要素的调整。随着信创的精准推动，国内 IT 企业将不断成长为信息建设的中流砥柱，解决更多难题。亿赛通作为国内领先数据安全厂商，全线安全产品积极进行信创适配，已覆盖电子文档安全管理系统、数据泄露防护系统、数据库审计、数据脱敏、数据库防火墙等系列产品。未来，亿赛通将继续拓宽生态体系建设，加强技术攻坚，推动信创产业的高质量发展。

独家科普 | 亿赛通“分▪放▪管▪服”数据安全建设理念



万物互联的数据时代，作为信息资产的数据正在从过去局部、静态的属性，向全面、流动的属性过渡。传统的，尤其是单一的数据安全保护工具，已经落后于时代发展的需求。如何从整体统一和业务流动的视角来保护数据，已经成为业界厂商积极探索的共同课题。

亿赛通近年来开始升级转型，从单一的文档加密厂商扩展到了综合数据安全厂商，并站在技术环境变化和企业发展战略的高度，研发业内首个“分▪放▪管▪服”的数据安全综合解决方案的理念。

经过近二十年的数据安全防护经验积淀，亿赛通为客户提供专业的服务，优秀的产品方案及高于行业标准的工程交付体系，满足客户在数据安全建设新时代下的数据安全防护需求。根据数据安全行业发展现状，我司结合客户企业自身的业务开展流程及数据属性提出了全新的“分▪放▪管▪服”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， 与客户携手共建数据安全大生态。

那么如何理解全新的“分▪放▪管▪服”数据安全建设理念？需要分别从制度层和技术层面结合做到人与数据的最优管理；人与标准的最佳实践；使数据安全建设在合规的基础上产生最大的价值，真正实现安全与效率的最大化平衡。

分 - 数据安全建设基础

分为分层治理，制度先行，技术支撑；即需要从制度层和技术层两个维度进行分层治理；

制度维度：

1. 分层合规：分层合规是指需要对当前的数据安全相关政策进行分析，进行合规性和安全制度进行对标，符合公司和国家的相关安全制度，做到企业和国家的分层合规。规避法律风险做到有法可依、有据可引。

2. 分权分责：需要指定相应人员负责，做到制度落地有声，追责有人；对相应人员赋予对应的职责和权限进行相关数据资产安全管理。

技术维度：

在技术维度数据资产的发现和梳理是数据安全的首要基础工作。

1. 分类分级：对数据进行确权，把企业杂乱的数据进行分类，分类后的数据实行不同级别的保护。

2. 分布分析：需求了解企业整体的数据分布情况，明确企业数据架构规划，便于发现问题及针对性改善提高。

“分”是从整体架构的层面来规划数据安全，是数据安全综合解决方案的基础，没有准确合理的“分”就没有有效安全的数据应用和管控。

放 - 简化流程保障流通

数据是需要流通才能产生价值，放即是在制度层面放开，使用合理的审批流程规范数据的申请及使用，明确职责后将管理放开，进行行为监察将使用放开，让数据在流转和应用中产生价值。

管 - 放管结合合理监管

☆ 技术监管 ☆

将数据分类分级、流程规范等管理制度落地的具体技术落地，通过端点边界、网络边界及云边界的纵深防控，形成点到面的全面技术防控。

- **端点数据管控：**可实现数据加密、防勒索、磁盘加密、可信介质管控等。
- **网络数据管控：**可实现海量数据防护、邮件外发敏感信息阻断等。
- **云端数据管控：**可实现数据脱敏、敏感挫折防护、敏感系统访问控制等。

☆ 放管结合 ☆

保障数据在流转和应用中的安全，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，企业则时刻面临巨大的运营风险，通过放管结合把握数据制度管理与技术管控的动态精准平衡度，最终可实现安全与效率的最大平衡，在保障数据安全流转的基础上将数据创造的价值最大化。

服 - 高效服务持续运营

在数字化转型的时代背景下，以云计算、大数据、物联网和人工智能为代表的新一代信息革命带来了新一轮的信息化建设浪潮，极大提升生产力的同时也产生了大量的数据资产，这些资产的防护不能再按照传统的数据防护堆积设备或工具就能完成相关防护，更是需要营造及时管理环境，立体运营可持续提升数据资产的防护能力才能在新的信息化产业升级的浪潮中站稳脚跟。这就需要高效的人机结合服务来实现目标，主要从三个角度出发达成持续提升数据安全应用的目标。

1. 安全建设服务：通过数据咨询服务、体系建设、人才培养等整体提高企业内部的安全防护能力基准。

2. 安全态势服务：通过态势感知，资产管理，统一管理运维将风险可视化，分析风险趋势，进行智能风险预估，提供相关可视化数据报表协助企业内部进行安全决策，将风险前移，更加从容的应对风险甚至规避风险。

3. 安全应用服务：通过属于取证，分析处置，策略协调等服务来整体支撑企业的安全运营，使企业安全能力逐步提升实现持续优化的安全运营模式。

整体来说亿赛通数据安全建设理念符合整体的“同步规划、同步建设、同步运营”的三同步理论，经过时间的沉淀相较于传统的相关理论相比，亿赛通“分▪放▪管▪服”理论结合了用户的实际业务应用场景，基于不同的行业可以产生不同的数据保护效果，更贴合实际用户的真实数据防护需求，真正实现效率与安全的最佳平衡，实现企业效益最大化。

泄露事件频发，亿赛通揭开数据黑产链中“不能说的秘密”

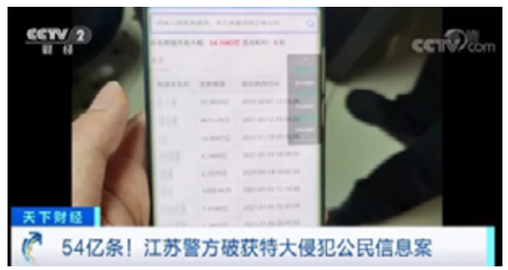
警方破获国内最大公民个人信息案

近日，江苏无锡警方成功破获了一起侵犯公民个人信息案，犯罪嫌疑人非法获取各类公民信息，数据累计高达 54 亿多条，并通过非法网络平台以查询、出售等方式牟利。

今年 3 月份，无锡网警部门在网上巡查时发现，一名卖家利用非法网络平台，为他人查询某大型社交网络账号关联的手机号码等个人信息数据，并将查询信息以每条 1000 美元（约合人民币 6384 元）的价格出售。

经警方调查发现，在贵州遵义有一家网络公司可能与该案有关，该网络公司的法人何某，具有一定的黑客技术，深入侦查发现他自己组建了一个社工库。

所谓社工库就是黑客们将泄露的用户数据整合分析，集中归档的一个地方。何某通过搭建具备查询功能的数据库，并利用非法网络平台提供查询公民个人信息的服务以此获利。经过侦查，无锡警方于近日成功抓获何某、熊某等人，现场查扣涉案服务器 6 台、电脑 2 台，以及非法获取的各类公民个人信息 54 亿余条，是迄今为止国内查获的最大单体量的一个公民个人信息社工库。



央视揭露简历信息黑色产业链

今年 2 月 25 日，四川泸州市合江县公安局接到受害人郑某报警称，他在国内一家大型招聘网站上，向一家公司投递了求职简历。此后，连续接到多家公司的骚扰电话，甚至还接到了大量推销电话，他们都对受害人郑某填写在求职简历上的信息了如指掌，他怀疑个人信息被泄露，于是向警方报案。经过调查，民警很快锁定了一名犯罪嫌疑人。根据这个线索，专案组初步确定这是一个有组织的灰色产业链犯罪团伙。



内部人员泄露疫情防控内部消息

新冠肺炎疫情爆发以来，我们每天都能在第一时间获得权威部门发布的防控措施和医疗救治情况。目前疫情形势已出现向好变化，防控工作取得积极成效。不得不说，在这场硬仗中，信息的及时公开发挥了关键作用。

但是也有一些关于泄露疫情信息的案例通报。其中，有些当事人被免职。

亿赛通小贴士 ESAFENET PROMPT

某市政府拟恢复部分受到疫情影响的公交线路。在参与方案讨论过程中，该市公交公司运营管理部部长在方案未经上级批准的情况下，擅自将《关于恢复部分公交线路的通告（讨论稿）》发布至公司微信群。在没有证实信息准确性的情况下，公司 5 名中层干部在朋友圈进行了转发，造成了不良社会影响。该市公交公司党委决定对范某给予免职处理，其他 5 人给予诫勉谈话处理。



频繁的泄露事件告诉我们，社会已经进入“数据为王”的时代，核心数据资产是企业的主要竞争力，对于企业发展具有重大意义。企业为了保护自己的核心资产，一套完整的综合数据安全解决方案需求越来越高，亿赛通“分•放•管•服”的数据安全建设理念提出正符合时宜。作为中国数据安全专家，亿赛通通过制度主建，技术主战，分放管服，将数据实现分权分责分风险，放管结合，做到要素服务保支撑，持续安全可运营，确保数据有价值的安全流转。

信息时代，掌握数据等于掌握了企业的命脉，也正因此，数据的买卖给一些不法分子提供了便利。亿赛通作为国内早期的数据安全解决方案提供商，以推动信息安全技术发展、加强信息安全管理、保护商业秘密为已任，我们将继续为客户提供有竞争力的数据资产安全解决方案和服务，持续为客户创造价值。

东易日盛家居装饰集团股份有限公司



客户简介

东易日盛家居装饰集团股份有限公司始创于 1997 年，目前已发展为一家专业化、品牌化、产业化的大型上市家装集团公司（股票代码：002713），连续多年居于《中国最具价值品牌 500 强》家装行业前列，品牌价值高达 275.61 亿元。23 年来，东易日盛集团一直专注家装产业的创新发展。近年来，东易日盛集团启动科技化转型，已拥有近百项专利，是家装行业中通过国家认证的高新技术企业、国家装配式建筑产业基地。东易日盛集团秉承源回报社会的理念，始终坚持慈善事业的发展，于 2015 年正式创建东易慈善基金，开展乡村芭蕾、东易图书馆、润琪老人关爱计划、心灵公益、幸福密码等 5 大核心项目。迄今已在全国范围拥有 87 家分会，2000 余名志愿者，受益人群达到 2 万余人。

需求背景

家居装饰企业中人员防泄密和设计图纸安全是两个比较棘手的问题，设计行业的特殊性导致了人员流动较大，因设计人员手中都会或多或少的掌握部分公司重要图纸信息，这部分人员如果存在离职或缺乏保密意识，将会直接导致公司的经济损失。企业对内部核心数据的安全管控是很有必要的。

解决方案

电子文档安全管理系统利用驱动层透明加密技术，通过对东易日盛电子文档的加密保护，解决企业数据资产外泄问题。

智能加密：可根据文档的内容进行语义识别，判断是否为企业所定义的加密数据并自动进行加密处理；

内容安全管控：可对数据实现截屏录制控制、文档阅读水印、文档打印水印、拷贝粘贴控制；

文档权限管理：可对数据进行细粒度权限控制、模板批量授权、文档权限管理；

文档外发管理：可进行用户身份认证、使用权限控制；

流程管理：实现文件解密审批流程、文件外发审批流程、离线办公审批流程和文件还原审批流程；

审计跟踪：可以进行邮件外发审计、文件解密审计、文件打印审计、流程全文检索审计和违规操作预警。

项目成果

通过对东易日盛的使用、存储、流转、审计等各个环节安全把控，为企业构筑了立体化的安全防护体系。系统充分融合了环境兼容性和功能扩展性，可无缝地满足日益变化的用户需求和环境变化需求，在实现安全管控的情况下，又实现工作效率与管理效率的提升。

北京汽车股份有限公司



客户简介

北京汽车股份有限公司成立于 2010 年 9 月 28 日，由北京汽车集团有限公司等六家大型企业发起组成。致力于发展高端制造业，加快北京市汽车工业的优化升级，全面推进北京汽车自主品牌的发展战略。北京汽车股份有限公司以国内市场为基础，同时大力开拓国际市场；以基于萨博技术的自主品牌轿车和越野车为龙头，发展成为乘用车产品线齐全、产业链完整、企业结构和布局合理、管理高效、盈利能力强、具有核心竞争能力，自主品牌乘用车产品具有较大市场占有率的公司，成为国内一流、具有国际影响力的大型汽车公司。

典型案例 TYPICAL CASES

需求背景

北京汽车集团有限公司为了防止企业内部的研发、设计、市场等部门的重要资料在无任何防护措施的情况下被内部员工泄露到企业外部，从而影响北京汽车在激烈的汽车行业中的竞争力，因而启动了数据泄露防护项目。亿赛通对北汽集团所使用数据泄露防护系统的现状进行了充分调研和论证，并最终决定按照北汽集团的模式进行数据泄露防护系统的部署和管理。

解决方案

签约产品：亿赛通文档透明加密系统 SmartSEC、文档外发管理系统 ODM

1. 文档透明加密系统：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；另外，只有被系统授权许可，才可使用这些加密的文件，如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体扩散而扩散；

2. 文档外发管理系统：为客户实现在文档外发文件打开时，用户需通过身份认证，方可阅读文件。同时，外发文件可以限定接收者的阅读次数和使用时间等细粒度权限，从而有效防止了客户重要信息被非法扩散。具体如下：

①文档加密：采用高强度加密技术对外发数据进行加密保护，防止非法用户暴力破解泄密。

②身份认证：外发文档提供多种安全身份认证机制，包括：密码口令认证、机器绑定认证、硬件 USB-KEY 认证及混合认证等，在身份认证通过后才可正常、安全打开外发文档。

③权限控制：外发文档提供细粒度权限控制保护，包含文档使用权限如只读、打印、修改等控制；文档生命周期管理如：阅读次数、阅读时限及过期自动销毁等保护；文档协同权限如修改、还原以及文档内容保护、打印水印等控制。

④内容防护：为防止使用者恶意将文件内容扩散，系统对其内容进行高强度安全控制，如内容剪切保护、禁止截屏、禁止另存为及打印控制等。

项目成果

亿赛通采用高效加密技术，对北汽 OFFICE 文档、研发设计图纸等文档访问自动加密，外发安全控制等功能，实现了北汽内部涉密文档的信息的安全访问与流转等功能。