

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

新年开门红，亿赛通强势入围《中国网络安全细分赛道发展与技术创新趋势洞察报告》

中国信通院《数据治理产业图谱 1.0》发布，亿赛通数据安全治理能力再获认可

深耕安全，实力不菲 亿赛通交上圆满答卷

新征程

大展宏“兔” 亿路同行



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



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 《亿赛通一月刊》乘风破浪迈上 2023 新征程

行业聚焦 INDUSTRY FOCUS

4/5 国内行业新闻

6-11 国外行业新闻

亿赛通动态 ESAFENET NEWS

12/13 新年开门红，亿赛通强势入围《中国网络安全细分赛道发展与技术创新趋势洞察报告》

14/15 荣誉不断，亿赛通入选数据安全共同体计划积极参与单位

16/17 专业能力见证 | 亿赛通多款产品通过中国软件评测中心评测

18/19 深化生态合作蓝图，亿赛通数据库安全审计系统与海量数据库完成产品兼容性互认证

20/21 亿赛通坚持技术创新，成为 2022 北京软件核心竞争力企业（创新型）

22/23 中国信通院《数据治理产业图谱 1.0》发布，亿赛通数据安全治理能力再获认可

24-27 深耕安全，实力不菲 亿赛通交上圆满答卷

28/29 亿赛通数据安全运营管理平台喜获《2022 年网络安全优秀评选》十大明星产品

30/31 深度融合 合作共赢 | 亿赛通正式加入金兰组织

32/33 榜样引领，亿赛通被数专委授予“优秀成员单位”称号

34/35 亿赛通荣获中国网络安全产业联盟 CCIA 2022 年度殊荣！

36/37 培训认证新纪元 | 亿赛通专业化认证培训初具成效

典型案例 TYPICAL CASES

38/39 数据安全分类分级解决方案

40/41 零信任数据安全解决方案

《亿赛通一月刊》乘风破浪 迈上 2023 新征程

当前，数字经济浪潮席卷全球，信息化、数字化、网络化和智能化正在快速覆盖我们的生活、工作中。数据安全产业已成为数字经济发展的前提和保障基石，在国家新兴产业战略中的重要地位得到充分肯定。近年来的一系列政策和配套措施如雨后春笋般发布、实施，数据安全产业的发展春天已经来临。亿赛通在政策的扶持下大力加强技术研发、产品创新、服务升级，2023 年定会获得新的机会和增长点，后续凭借大幅扩增的客户需求顺势而进，承接安全产业红利，助推客户数字化进程。

2023

国内

1、林志玲、小 S、郭台铭、张忠谋手机号等个人信息遭外泄？警方介入



摘要：近日，台湾中华航空（以下简称“华航”）被爆疑似遭到黑客攻击，致使其会员信息泄露，涉及多名政商以及演艺界名人，包括台积电创办人张忠谋、鸿海集团创办人郭台铭、艺人徐熙娣、林志玲等。此后，华航回应称，疑似泄露的个人信息与该公司数据库不符，尚无法确认泄露信息的来源。

3、问界汽车车主信息遭泄露 回应来了 安全气囊未打开话题被转移



摘要：近日，问界汽车车主信息泄露一事登上热搜。据了解，王女士购买了一辆问界M7，1月12日，在驾车中发生追尾事故，诧异的是车辆碰撞安全气囊并没有弹出。随后车辆被拖到AITO授权用户中心杭州国际汽车城店。对此，王女士提出两点质疑，一是刹车为什么偏软，第二个问题气囊为什么没有弹出。随后将这些质量问题反馈给厂家，耐人寻味的是还没接到厂家回复，先接到了单位领导的电话，说有人找过来，给个面子算了。

2、因泄露未公开信息 东方日升被出具警示函



摘要：宁波证监局网站1月28日发布关于对东方日升新能源股份有限公司采取出具警示函措施的决定。2023年1月9日，东方日升员工庄某在微信朋友圈称公司储能业务“23年在手已签4吉瓦时多”，并在评论中与某券商分析师讨论上市公司组件成本、交付价格、未来业绩等，相关事项于1月11日被多家媒体报道、转载。庄某违规泄露上市公司未公开信息，对市场造成不良影响。宁波证监局指出，公司未能有效执行信息披露相关管理制度，规范员工行为，违反了《上市公司信息披露管理办法》第三条的规定。根据《上市公司信息披露管理办法》五十二条的规定，该局决定对公司采取出具警示函的行政监管措施。

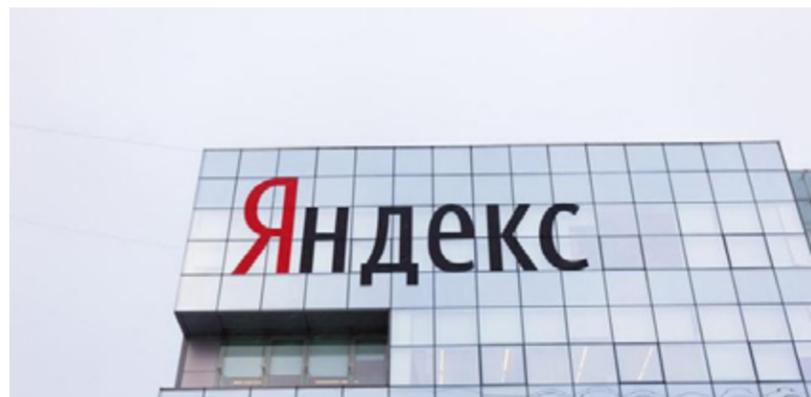
4、“主管”发布“粉丝福利”？警惕追星骗局！



摘要：1月9日晚上，苏州姑苏公安分局友新派出所接到庄女士报警求助，称银行卡里少了15万，疑似遭遇网络诈骗。经了解，前一天晚上，庄女士的女儿小张刷短视频时，发现了一个粉丝QQ群的推广，声称进群就可以获得某明星的“独家信息”。这让小张眼前一亮，赶忙申请进群并表明“铁粉”身份。很快，群里发布消息称该明星将在1月9日举办线上活动，如果要参与，需要与一位“主管”联系。小张随即添加了“主管”QQ，也收到了活动流程内容，并按照“主管”提供的操作步骤申请参与。“主管”告知小张操作不当导致信息泄露，明星所在的经济公司有6万元资金因此被冻结，必须由小张操作挽回损失。小张听后根据对方指引拿了妈妈庄女士的手机开始“挽损”。

国外

1、否认黑客入侵，俄最大 IT 公司内部源码被前员工泄露



摘要：俄罗斯最大的 IT 科技公司之一 Yandex 的源代码仓库据传遭到前员工窃取，相关数据已在某个流行黑客论坛上以 BT 种子形式泄露。1 月 25 日，泄密者发布了一个磁力链接，他们声称这是“Yandex git 源”，其中包含 2022 年 7 月从公司窃取的 44.7 GB 文件。据称，这些代码存储库包含公司除反垃圾邮件规则之外的所有源代码。

2、因泄露个人数据，圣马力诺法院判决脸书缴纳 400 万欧元罚款



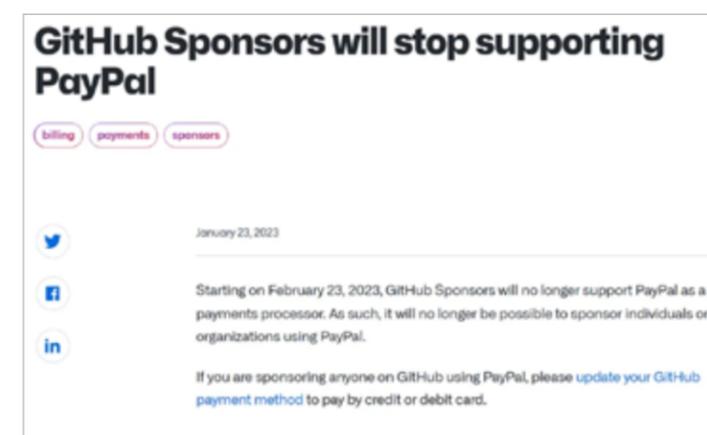
摘要：1 月 26 日有媒体报道，圣马力诺共和国上诉法院 25 日驳回社交媒体网站脸书母公司元宇宙的上诉，判决其向圣马力诺个人数据保护局缴纳 400 万欧元罚款。上诉法院认为，脸书对用户个人数据泄露负有重要责任，其本应采取适当的安全措施来防止用户的个人数据被非法收集。2019 年，因 12700 名圣马力诺公民的脸书账户个人信息被非法泄露，圣马力诺个人数据保护局要求脸书缴纳 400 万欧元罚款，此后脸书上诉至法院要求取消处罚决定。

3、疑似摩萨德情报泄露：俄方、乌克兰和北约特工军官的伤亡数据

| | 俄方 | 乌克兰 | 北约 |
|---------|-------|-------|------|
| 损失飞机 | 23 | 302 | |
| 损失直升机 | 56 | 212 | |
| 损失无人机 | 200 | 2750 | |
| 损失装甲类战车 | 899 | 6320 | |
| 损失火炮 | 427 | 7360 | |
| 损失防空系统 | 12 | 497 | |
| 参战人数 | 41.8万 | 73.4万 | |
| 阵亡人数 | 18480 | 15.7万 | 5360 |
| 受伤人数 | 44500 | 23.4万 | |
| 被俘人数 | 323 | 17230 | |

摘要：近日，一份疑似摩萨德情报数据泄露，数据看起来比较像真的战场数据。数据统计，其中北约教官、特工以美英两国为主，死亡 234 人。北约士兵阵亡 2458 人，以波兰、德国、立陶宛为主，其他公开身份雇佣兵死亡 5360 人。

4、泄露 3.5 万用户数据后，微软 GitHub 项目打赏功能不再支持 PayPal 付款



摘要：微软 GitHub 官方博客近日发表简短声明，宣布从 2023 年 2 月 23 日起，GitHub Sponsors 项目打赏功能将不再支持 PayPal 支付方式。赞助人将无法再通过 PayPal 打赏开发者或组织，GitHub 建议赞助人更新支付方式，使用信用卡或借记卡。GitHub 官方对此没有给出更多解释。

5、LOL 源代码被盗，玩家数据会被泄露？ 真正该担心的应该是外挂

摘要：对于任何一个游戏来说，源代码都是极为重要的资产。它不仅展示了整个游戏的架构，而且还展示出了游戏有哪些漏洞。不幸的是，LOL 的研发商拳头游戏日前宣布，《英雄联盟》、《云顶之弈》和一个遗留的反作弊平台的源代码已经被黑客所窃取。看到这个新闻，大多数玩家的第一反应是自己的游戏数据和个人信息会不会也被黑客所窃取。针对这个问题，拳头方面专门进行了回应：玩家的数据和个人信息并没有被泄露。但是在已经被黑客所窃取的源代码当中，包括了许多正在开发的实验性功能。由于拳头方面已经强硬地表示绝不会妥协给钱，这些功能被泄露的概率将大大增加，拳头方面的开发进度可能会因此而被推迟相当长的一段时间。

6、暴雪网易谈判失败，《魔兽世界》等 7 款 游戏大年初二停服，玩家数据如何处理



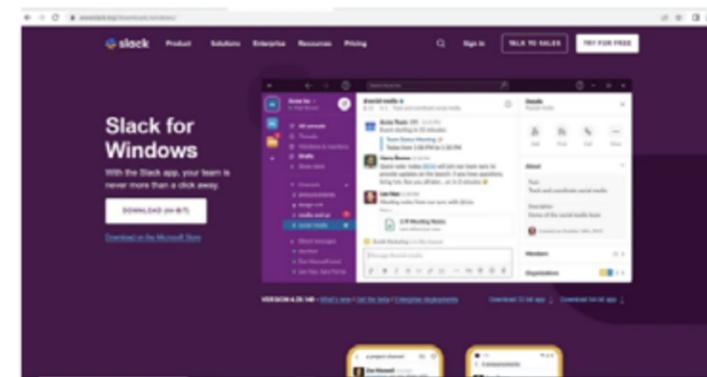
摘要：1月17日，暴雪中国在其官方微博中发布公告称，暴雪于上周再次与网易接触，希望将现有的协议顺延6个月，意在为玩家争取更多时间，同时让暴雪“继续探索未来在国服地区合理而长远的发展道路”。结果是，网易并未接受暴雪关于顺延现有服务的提议，因此，暴雪将遵照网之易的停服公告，仍按原定计划于1月24日0时起正式中止暴雪的国服游戏的一切服务。暴雪要求“续约”的举动，侧面印证了其寻找“下家”的过程并不顺利。而广大玩家关心的账号数据留存问题，也将是网易暴雪接下来的重点工作。

7、T-Mobile(TMUS.US) 正在调查数据 泄露事件 涉及 3700 万个账户



摘要：美国无线运营商 T-Mobile(TMUS.US) 表示，正在调查一起涉及 3700 万个后付费和预付费账户的数据泄露事件，预计将产生与该事件有关的大量费用。该公司表示，它在 1 月 5 日发现了恶意活动并在一天内将其控制住，并补充说，财务信息等敏感数据没有受到损害。不过，该公司称，一些基本的客户信息被获取，如姓名、账单地址、电子邮件和电话号码。该公司表示：“我们的调查仍在进行中，但恶意活动目前似乎已完全得到控制，目前没有证据表明恶意行为者能够破坏或破坏我们的系统或网络。”该公司补充说，已开始通知受影响的客户。

8、IcedID 僵尸网络传播者滥用谷歌 PPC 来传播恶意软件



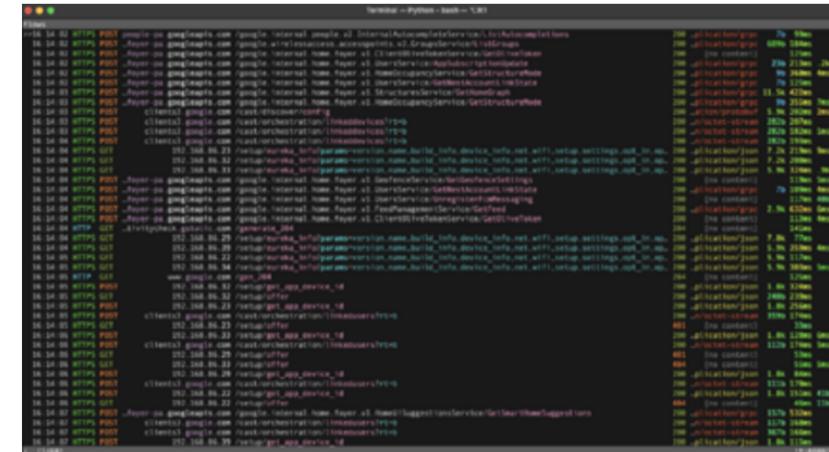
摘要：IcedID 主要针对金融行业发起攻击，还会充当其他恶意软件家族（如 Vatet、Egrogor、REvil）的 Dropper。自 2022 年 12 月以来，谷歌点击付费 (PPC) 广告被攻击者滥用，通过恶意广告攻击传播 IcedID。像谷歌广告这样的广告平台，其目的是使企业能够向目标受众展示广告，以提高流量和增加销售。恶意软件发布者滥用同样的功能，使用一种被称为恶意广告的技术，其中选择的关键词被劫持，显示恶意广告，诱使毫无戒心的搜索引擎用户下载恶意软件。

9、在谷歌和苹果商店中发现了近 300 个恶意的贷款应用程序



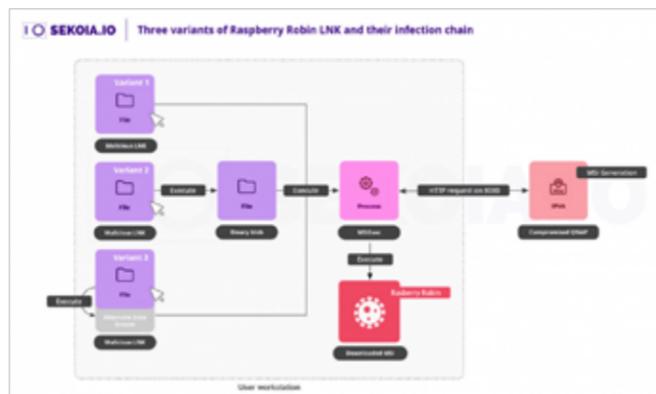
摘要：贷款应用都带有隐性费用和高利率，导致用户的付款额增加，而且这些应用程序还要求用户提供他们移动设备上的敏感信息。网络安全供应商 Lookout 的研究人员说，其中信息包括短信、照片、电话记录和联系人名单，然后用这些来对付受害者。研究人员在一份报告中写道，在某些情况下，从设备中窃取出的数据会被用来敲诈借款人，威胁要向他们的联系人披露这些数据或其他有关债务的信息。

11、Google Home 智能音箱漏洞可监听用户会话



摘要：谷歌发布 Google Home 智能音箱产品。安全研究人员在 Google Home 智能音箱设备中发现了一个安全漏洞，攻击者利用该漏洞可以在受害者设备中安装后门装好，并通过互联网远程发送命令给受害者设备、访问麦克风数据量、在受害者网络中发起任意 HTTP 请求，甚至可能暴露 WiFi 密码，使攻击者访问受害者的其他设备。

10、Raspberry Robin 的僵尸网络迎来第二春



摘要：Raspberry Robin 是一种恶意软件，通过受感染的 U 盘下载，还可能通过网络共享下载。攻击想法很简单：受感染的设备含有 LNK 文件（Windows 快捷方式）。用户插入 U 盘、启动伪装成 U 盘或网络共享的 LNK 后，它会启动 Windows 实用程序 msixexec。

12、一种从未见过的恶意软件感染了成百上千的 Linux 和 Windows 设备

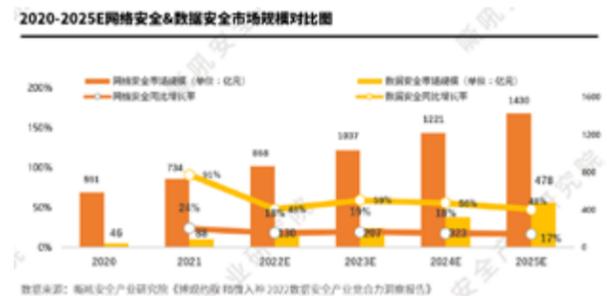


摘要：研究人员近日披露了一种从未见过的跨平台恶意软件，这种恶意软件已经感染了一系列广泛的 Linux 和 Windows 设备，包括小型办公室路由器、FreeBSD 设备和大型企业服务器。称该恶意软件为 Chaos，这个名称在恶意软件使用的函数名、证书和文件名中一再出现。直到 4 月 16 日当第一批控制服务器投入实际使用时，Chaos 才浮出水面。从 6 月到 7 月中旬，研究人员发现了数百个独特的 IP 地址，这些 IP 地址代表受 Chaos 攻击的设备。最近几个月，用于感染新设备的登台（staging）服务器如雨后春笋般涌现，从 5 月的 39 台增加到 8 月的 93 台。截至本月，这个数字已达到了 111 台。

新年开门红，亿赛通强势入围《中国网络安全细分赛道发展与技术趋势洞察报告》

近日，由嘶吼安全产业研究院撰写的《日日新，又日新 中国网络安全细分赛道发展与技术趋势洞察报告》（以下简称报告）正式发布。报告在中国网络安全产业变革的关键期，聚焦五大网络安全重点赛道和五种新兴网络安全技术，通过对参与厂商的整体分析，提供了安全厂商及其产品、服务和解决方案的独特视角，深挖数据产业的真实发展情况，为资方和甲方提供细节参考。

嘶吼从公开数据了解到，2010年-2016年随着“十八大”报告中“国家安全”逐渐引起重视，网络安全行业开始持续大量涌入厂商，在2016年达到峰值，2013年-2020年皆保持在每年成立大于15家的高增长态势，热度居高不下。网络安全行业整体正在向多元化、智能化方向飞速发展，力求满足客户对产品研发提出的更高要求。另外，根据全球网络攻击趋势以及公开调研数据，嘶吼总结五大影响力的网络安全细分赛道，分别是云上安全、数据安全、工控安全、物联网安全、信创安全，未来会进一步在行业内崭露头角。



在数据安全赛道，2022年多因素促使数据安全赛道继续快速发展，市场规模和投融资受大环境影响相对其他较小。2021年，我国数据安全产业市场规模88亿元，预计2022年数据安全产业规模会达到130亿元，预计2025年，数据安全产业有望达到478亿元，用6年时间（2020-2025年）达到传统网络安全20年（1999-2018年）所创造的市场规模。数据安全市场还需要三年达到高速发展期，至少七年达到成熟期，届时生态环境成熟，产业链布局清晰，厂商之间建立起拥有较高认可度的商业合作模式，满足行业的发展需求。

1、成功入围数据安全赛道典型厂商

亿赛通以业内产品、解决方案的高认知度，近二十年的技术优势积累及重大项目的丰富实施经验，强势入围数据安全赛道唯一典型厂商。

多年来，亿赛通持续专注于数据安全的技术研究，通过事前主动防御、事中监测响应、事后追踪溯源、全程态势感知四个维度，进行企业数据资产的全流程安全防护。采用人工智能、用户行为分析、大数据分析等创新技术，实现数据资产的分级分类。再根据数据价值和等级的不同，采取不同安全防护手段，确保核心数据重点防护，公开数据或非核心数据轻级管控，实现安全与效率的最大化。

2、成功入围《报告》多项代表厂商

本次《报告》嘶吼研究院此前发布的《数据安全产业竞争力洞察报告》将数据安全产业主要需求归纳为三大类别、11个小类。其中，敏感数据共享/流通问题、数据安全防护问题、数据资产梳理/分级分类问题、数据安全合规问题的厂商数量较多，此类问题具有迫切性和紧迫性。亿赛通在《报告》中入选数据安全防护问题、数据资产梳理/分类分级、数据安全体系建设等三类安全能力的代表厂商，实力可见。



随着数字经济和信息产业蓬勃发展，零信任、人工智能、区块链等技术加快落地应用，新业态新技术在推动经济转型升级的同时，数据泄露、滥用等风险日益凸显。“十四五”规划等重要文件、《数据安全法》、《个人信息保护法》等法律法规均提出，要推动发展数据战略，统筹数据开发利用、隐私保护和公共安全，规范数据有序流通，保障数据安全。

强化全行业数据安全保障能力，离不开数据安全产业链和生态的有力支撑，在新一轮科技变革和产业变革推动经济发展、我国进入扎实推进共同富裕的关键历史阶段，数据安全生态建设对促进数字产业健康有序发展意义重大。但同时，大批涌入安全行业的厂商给用户的选择造成一定困难，在权威机构进行专业梳理后，为客户提供参考。

在《报告》中显示，数据安全产业预计2025年进入高速发展阶段，这对数据安全厂商而言将会是个转折点，亿赛通将继续钻研安全技术，深入研究市场需求。尽管产品实力在数据安全行业内得到了越来越多的关注以及肯定，我们也一定不骄不躁，让现有的成绩转变为动力，继续扎根安全领域，做大做强。

荣誉不断，亿赛通入选数据安全共同体计划积极参与单位

| 积极参与单位 |
|---------------|
| 北京亿赛通科技发展有限公司 |

近日，由中国信息通信研究院（以下简称“信通院”）发起的“数据安全共同体计划”发布优秀成员单位名单，亿赛通凭借在数据安全领域突出的专业能力，在百余家单位中脱颖而出，获评“数据安全共同体计划积极参与单位”。

“数据安全共同体计划”由信通院发起，旨在“坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展”，落实国家数据安全产业生态建设工作布局。成员单位来自央企、科研单位、高校、互联网企业、安全企业等多个领域，致力于推动数据安全生态链各环节的交流与合作，促进数据安全政策、技术、产品、人才多要素良性互动。2022 年度成员单位已扩增至 200 家，行业领域覆盖范围进一步扩大。

亿赛通在 2022 年作为“数据安全共同体计划”成员单位，积极参与机构组织的各项活动，加速推进数据安全体系建设，服务数据增值，为数据安全能力提升提供助力。

多年来，亿赛通持续创新数据安全建设思路，提出了自上而下的数据治理框架，将产品模块集成平台化输出，形成全新的数据安全运营管理平台。平台主要通过感知云、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等。



综合数据安全运营管理平台可以与其他安全产品形成联动，能够将原有的数据库审计、DLP、文件加密、数据脱敏等各类产品能力集中化管理，策略统一布控，既可以减轻运营人员的工作负担，又能够对各类安全产品进行统一策略的管理与优化，减少无效策略形成的误报。

同时，通过统一的数据安全运营管理平台，还可以对各类安全产品上报的日志数据进行关联分析，解决以往审计日志分析及溯源的局限性，可将一个事件在云、网、端的所有操作进行完整还原，帮助用户进行准确定位风险源头。

强化全行业数据安全保障能力，落实数据安全法律法规政策离不开数据安全产业链和生态的有力支撑，在新一轮科技变革和产业变革推动经济发展、我国进入扎实推进共同富裕的关键历史阶段，数据安全生态建设对促进数字产业健康有序发展意义重大。

2023 年，亿赛通将继续发挥自身能力与经验，积极配合“数据安全共同体计划”工作，为提升全行业数据安全能力，促进数据安全政策、技术、产品、人才多要素良性互动助力。

专业能力见证 | 亿赛通多款产品通过中国软件评测中心评测

近日，中国软件评测中心开展了数据安全产品能力测试。能力测试涉及到数据安全管控平台、数据库审计、数据脱敏、数据防泄露、数据库防火墙等分类。共有 7 款数据安全产品 / 平台通过了数据安全产品能力测试，其中，亿赛通占据 6 款。能力测试过程中使用的测试技术方案及内容依据中国计算机行业协会数据安全专业委员会和中国软件评测中心相关标准规范：《数据库防火墙技术要求与测试方法》、《数据脱敏产品安全技术要求和测试评价方法》、《数据泄露防护系统技术要求与测试方法》、《数据库审计技术要求与测试方法》、《数据安全管控平台技术要求与测试方法》进行评测。亿赛通凭借先进的技术理念和丰富的研发经验，顺利通过了中国软件测评中心的数据安全产品能力测评。

测评结果显示，亿赛通的“数据库安全审计系统（DAS）”、“数据库防火墙系统（DFW）”、“数据脱敏系统（DMS）”、“数据安全智能管理平台（DSIP）”、“存储数据泄露防护系统（存储 DLP）”、“邮件数据泄露防护系统（邮件 DLP）”等产品具备良好的综合技术能力和自身安全防护能力，支持了包含但不限于数据安全治理、脱敏、防火墙、邮件、存储设备端的数据泄露防护等各项能力，且性能较为稳定。

亿赛通遵循“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，帮助企业形成扎实可靠的综合数据安全能力。

第一个闭环是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于业务的体系，形成“分放管服”的正反馈闭环。

| | | |
|---------|---------|-------------------------------|
| 2 | 企业名称 | 北京亿赛通科技发展有限公司 |
| | 产品名称 | 亿赛通数据库防火墙系统 |
| | 测评项目 | 数据库防火墙 |
| | 产品型号/版本 | DFW/V5.0 |
| 证书/报告编号 | | ZSSJ AQ22120101/SJ AQ22120101 |

| | | |
|---------|---------|-------------------------------|
| 3 | 企业名称 | 北京亿赛通科技发展有限公司 |
| | 产品名称 | 亿赛通数据库安全审计系统 |
| | 测评项目 | 数据库审计 |
| | 产品型号/版本 | DAS/V5.0 |
| 证书/报告编号 | | ZSSJ AQ22112901/SJ AQ22112901 |

| | | |
|---------|---------|-------------------------------|
| 4 | 企业名称 | 北京亿赛通科技发展有限公司 |
| | 产品名称 | 亿赛通数据安全智能管理平台 |
| | 测评项目 | 数据安全管控平台 |
| | 产品型号/版本 | DSIP/V5.6 |
| 证书/报告编号 | | ZSSJ AQ22110801/SJ AQ22110801 |

| | | |
|---------|---------|-------------------------------|
| 5 | 企业名称 | 北京亿赛通科技发展有限公司 |
| | 产品名称 | 亿赛通数据脱敏系统 |
| | 测评项目 | 数据脱敏 |
| | 产品型号/版本 | DMS/V5.0 |
| 证书/报告编号 | | ZSSJ AQ22102601/SJ AQ22102601 |

| | | |
|---------|---------|-------------------------------|
| 6 | 企业名称 | 北京亿赛通科技发展有限公司 |
| | 产品名称 | 亿赛通存储数据泄露防护系统 |
| | 测评项目 | 数据防泄露 |
| | 产品型号/版本 | ScanDLP/V5.1 |
| 证书/报告编号 | | ZSSJ AQ22121601/SJ AQ22121601 |

| | | |
|---------|---------|-------------------------------|
| 7 | 企业名称 | 北京亿赛通科技发展有限公司 |
| | 产品名称 | 亿赛通邮件数据泄露防护系统 |
| | 测评项目 | 数据防泄露 |
| | 产品型号/版本 | MailDLP/V5.1 |
| 证书/报告编号 | | ZSSJ AQ22120801/SJ AQ22120801 |

第二个闭环是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。

在此理念的指引下，亿赛通将产品进行细分归类，共分为：数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务五类，打造完善的数据安全综合解决方案。



数据安全治理

以“人”和“数据”为中心，从技术到产品、从策略到管理，提供完整的产品与服务支撑，实现业务与安全的深度融合。在人为层面，从决策层制定经营策略、IT 策略，帮助企业用户建立数据安全意识，区分职责权限。在数据层面，技术服务于制度，运用专业技术支撑，通过 AI 算法，关联分析、密码技术、访问控制、数据标识等技术，采集分析各类安全设备结构化和非结构化日志，探测、预测、发现威胁事件和风险。进而形成技术、制度不断迭代的正循环，建立全面综合数据安全治理能力。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，构建了自上而下、全流程、可闭环的完整链条。

数据安全防护

数据安全防护将结构化、非结构化和半结构化数据作为防护对象，基于云、网、端三大应用场景，实现对电子文档、数据库进行全方位、多维度管理。在终端侧，基于数据进行全量、增量、一次性、周期性扫描，对数据内容进行识别与检测，按照数据分类分级标准制度，对数据进行分类分级管理，实现加密、外发审计、审批和阻断等管理措施；在网络侧，内置全球 IP 地址库，将数据访问发起端和响应端进行 IP 地址比对，识别数据的违规流转、跨境传输、非法出境行为和敏感数据信息，并进行审计记录、风险告警及流转阻断限制；针对数据分散存储的状态，在终端、服务器端、云虚拟环境、网络端、邮件端支持全覆盖多点部署，为企业数据安全提供保障。

数据安全流转

数据安全流转系列产品通过存储加密、数据变形、访问控制、行为监测等技术手段，针对开发测试环境、数据交换、数据分析、数据共享等情况下的敏感数据处理，防止外部黑客攻击、内部数据窃取、脱库等风险下造成的数据泄露。遵循数据安全合规建设，保证数据存储、流转过程中的安全存储与按需放心流转。

数据库安全

亿赛通数据库安全五件套产品专注数据库安全与核心数据资产防护，通过对数据库进行安全风险评估、操作行为监测、访问控制管理、外部攻击与风险操作防护和敏感数据脱敏。实现全方位立体化的数据库风险管理能力，起到安全风险事前可知、事中可防，事后可溯。在满足等保合规以及数据安全建设的同时，切实有效的避免数据资产被破坏和泄露。

安全服务

涵盖咨询服务、售后服务与培训服务三大体系。利用 20 年数据安全建设方法论 + 全行业实施经验，推出全工作场景、全业务流程、全生命周期的数据安全防护方案，并提供配套专业的安全咨询顾问、实施工程师和培训讲师。售后服务覆盖国内地市级 30 余个办事处，7*24 小时响应，是业内具有端到端安全服务能力的厂家之一。培训服务亿赛通联合中国计算机行业协会数据安全专业委员会、工业和信息化部教育与考试中心、工业和信息化部人才交流中心推出全套数据安全培训课程体系，专注人才建设，并与国内 10 余所名校建立“产学研”联盟，形成“双师型”教师企业实践基地，面向社会不断输送安全人才。

面对数字化变革和数字经济发展的演进，亿赛通将基于“分·放·管·服”理念体系，进一步提升分类分级、安全治理、数据泄露防护、安全服务的纵深防御能力，为客户提供能够满足安全新需求的全品类产品，夯实技术、人才和经验实力，为各行业客户筑好、筑牢坚实的安全底座。

深化生态合作蓝图，亿赛通数据库安全审计系统与海量数据库完成产品兼容性互认证

随着国家构建安全可信信息技术产业战略布局的全面展开，信息技术应用创新产业发展已经进入快车道，赢得市场的首要因素是生态。在此大背景下，亿赛通积极与产业上下游生态伙伴展开合作，联合创新、协作共赢，围绕安全领域展开紧密合作。2022年9月，北京海量数据技术股份有限公司生态发展部总经理到访亿赛通公司，双方怀揣着对数据安全领域未来发展高度一致的良好愿景，确定开展深入合作，充分发挥优势，双向赋能。

双方自全面建立合作伙伴关系起，首先即针对核心产品展开测试。截至目前，亿赛通数据库安全审计系统 DAS V5.0 已经分别与海量数据库 Vastbase G100 管理系统和 Vastbase E100 管理系统完成产品兼容互认，测试结果良好，系统可稳定运行。



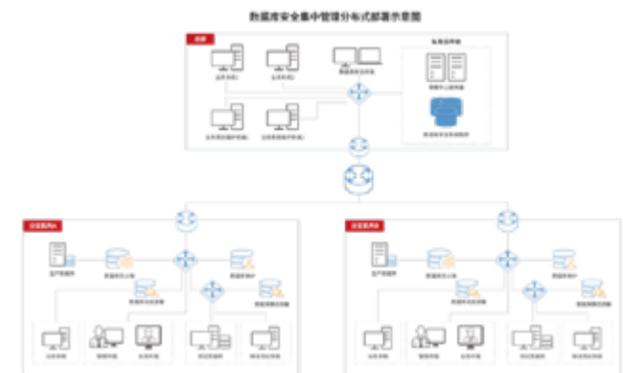
图 亿赛通 & 海量数据库产品兼容认证证书

亿赛通作为综合数据安全厂商，近二十年发展过程中持续进行技术创新和研发投入，创新提出并落地实践“分·放·管·服”数据安全建设理念，聚焦数据，以“数据和人”为对象双闭环管理。

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。

从业务流程入手，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于业务的体系，形成“分放管服”的正反馈闭环。

亿赛通数据库安全审计系统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。



1、满足等保合规需求：帮助客户满足等保分保和行业数据安全合规需求；

2、提升安全监控效率：实时监测数据库风险行为，提供风险趋势分析，帮助客户掌握数据库运行安全状态；

3、加快风险响应速度：提供 SQL 注入和数据库漏洞等攻击行为的实时检测和告警能力，便于客户第一时间采取安全管控措施；

4、解决事件溯源难题：全面记录数据库操作行为，利用准确的应用用户关联能力，切实解决安全事件发生后追责到人的难题。

此次与海量数据库的兼容互认顺利完成，是亿赛通与国产企业生态合作的重要体现，充分展示了企业间生态合作的协同发展与日臻完善。未来，双方将进一步深化资源共享机制，依靠各自的前瞻性思维与技术优势，合作打造融合的生态体系，实现解决方案融合、优势能力融合、技术创新融合和客户体验融合。此次合作，实现了从量变到质变的飞跃，双方将会共同发力，助力企业数字化变革。

目前，亿赛通全线产品已与统信软件、中国电子、达梦数据库、飞腾、海光、中科曙光等多家企业完成产品兼容性互认证，未来将与更多伙伴开展深度合作，携手推动企业生态共建。

亿赛通坚持技术创新，成为 2022 北京软件核心竞争力企业（创新型）



近日，北京软件和信息技术服务业协会发布了《2022 北京软件企业核心竞争力评价报告》，亿赛通凭借在数据安全领域的创新实践强势入选，并被评为“2022 北京软件核心竞争力企业（创新型）”。

据悉，本次报告聚焦北京市行业内业务规模大、效益好、自主创新能力强的优秀企业，旨在通过评价活动助力企业强化品牌建设，推动软件和信息技术服务业构建新的技术和品牌生态体系，赋能北京经济高质量发展。

根据报告显示，入选企业在规模、成长、创新等方面的核心竞争力具有显著优势，均是代表性强，经济社会贡献大，是行业主体。除此之外，报告按照规模型、创新型、成长型、创新创业型四个类别对核心竞争力企业进行了分析。其中，创新型企业在研发费用投入强度上超过规模型企业，并且在产出方面，创新型企业在专利和软件著作权数量上则数倍于规模型企业，是带动全行业技术创新的中坚力量。

经过统计性评价和行业专家评议，亿赛通从数百家企业中脱颖而出，荣获“核心竞争力评价（创新型）企业”荣誉称号。亿赛通自成立以来，积极投入研发创新，建立了完善的研发团队，沿着分类分级、安全防护、数据库安全等产品，持续构建和迭代以“分·放·管·服”数据安全建设理念为核心的综合数据安全治理体系。

作为目前保障数据安全高效、可靠、经济的主要手段，数据安全解决方案在企业发挥着重要的作用。尤其是在倡导无纸化办公的当下，构建高安全性的综合数据安全治理体系已成为各行各业保障其数据资产安全的最后一道防线。

从政策层面来看，近两年出台的各项政策、标准逐渐弥补了国内安全政策的不足。由此来看，建立健全的数据安全治理体系、加强数字基础设施建设是发展“数字强国”战略的必要进程。

数据普遍大规模、高频率流动，如何兼顾数据的“自由疏通”和“安全合规”成为推动企业发展，保障核心资产安全的重要保障。



数据安全保障的具体措施该如何实现？是安全厂商着重考虑的问题。亿赛通针对企业需求、行业政策、实施标准钻研出一套完整的数据安全治理体系，以核心技术工具为支撑，逐步对客户从风险评估、分类分级、体系建设、人才培养、安全运维等多维度指导。技术+工具双重保险，达到有层次的数据分级保护措施，对应落实分级监管职责。亿赛通在不增加用户负担、不改变任何工作流程及使用习惯的前提下，保障客户业务系统的数据安全。

科技创新是企业可持续发展的源泉，未来，亿赛通将继续依托研发团队强大的创新能力，不断通过科研成果的转化推动数据安全技术水平的提升，为科技创新事业发展服务。

中国信通院《数据治理产业图谱 1.0》发布，亿赛通数据安全治理能力再获认可

《数据治理产业图谱1.0》



新年伊始，喜讯一件接一件，由中国信息通信研究院、中国通信标准化协会大数据技术标准推进委员会（CCSA TC601）共同发起的《数据治理产业图谱 1.0》在第五届数据资产管理大会上发布。图谱 1.0 收录了来自 98 家企业的 144 款数据治理产品和 53 项数据治理相关的服务，覆盖超过 15 个行业领域。分为数据治理产品图谱和数据治理服务图谱两部分。亿赛通作为数据安全治理领域头部厂商入榜数据分类分级工具 / 平台板块。



数据治理产业图谱的调研编制，旨在梳理数据治理产业上下游相关企业、产品、服务的分布情况，掌握数据治理市场现状，从而帮助需求方更好的筛选数据治理产品与服务，标齐甲乙双方对于数据治理产品与服务的认知，洞察数据治理产业发展趋势。

此次亿赛通入选数据治理产业图谱，再一次彰显了亿赛通在数据安全治理体系建设上的硬核实力，得到了中国信息通信研究院、中国通信标准化协会大数据技术标准推进委员会的肯定与认可。

当前，数据是促进我国发展数字经济、优化领域资源配置、驱动企业降本增效的关键要素。数据安全的重要性已然越来越凸显。

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。



亿赛通产品服务从管理到实施，从制度建设到工具支撑，已经形成自上而下贯穿整个组织架构的完整链条。将业务梳理、分类分级、策略制定、技术管控、持续运营，帮助企业对数据安全建设进行整体规划。形成一站式的综合数据安全治理能力。最终达到数据资产可视、数据威胁可管、数据风险可控、数据血缘可溯的目标。

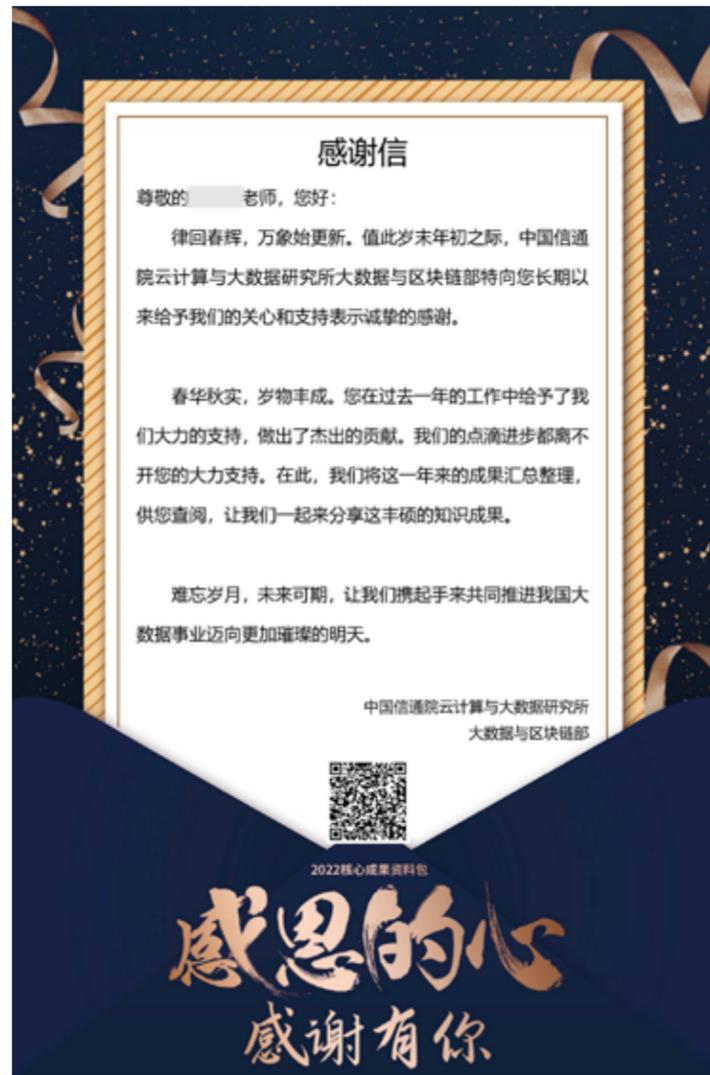
亿赛通“分放管服”数据安全建设理念



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。

亿赛通的产品实力已在数据安全行业内得到了越来越多的关注以及肯定，我们将继续充分发挥自身优势，加大产品研发力度，推动产品与方案、安全技术与服务优化升级，为数据安全产业发展献计献策。

深耕安全，实力不菲 亿赛通交上圆满答卷



亿赛通在 2022 年初与中国信息通信研究院云计算与大数据研究所（以下简称云大所）签署战略合作，双方深化共识，搭建产业生态，为数据要素发展贡献力量。此后，我司又陆续加入 (CCSA TC601) 中国通信标准化协会大数据技术标准推进委员会及 (DSI) 数据安全推进计划。这一年中，亿赛通围绕大数据安全、数据安全治理、数据安全服务、数据治理等方向，积极参与标准定制、图谱研发、产品评测、案例甄选和活动演讲等工作，持续助力国家数据战略和行业发展的充分融合。

云大所是信通院面向互联网新技术、新产业、新模式、新业态不断发展的势态，最新设置的核心业务单元。云大所围绕云计算、大数据、人工智能、数据中心以及关联应用领域的开展技术、标准研究，构建相关技术的测试、试验和统计平台，承担相关服务和产品的测试评估工作，承担相关国家重大科技项目、产业化项目，提供相关技术标准的咨询服务。

CCSA TC601 主要围绕大数据产业发展关键问题，开展大数据技术产品、数据资产管理与流通、大数据行业应用方面的标准预研，宗旨是凝聚产业链各个环节，识别和解决大数据发展面临重大问题，以标准推进工作为纽带，搭建行业交流平台，推动大数据实体经济深度融合。

DSI 数据安全推进计划是公益性合作项目，依托大数据协同安全技术国家工程实验室、中国通信标准化协会大数据技术标准推进委员会、中国互联网协会数据治理工作委员会开展具体工作，致力于打造健康规范的数据安全生态体系，帮助企业了解监管要求，全方位提升企业数据安全能力。

标准定制方面，亿赛通深度参与 CCSA TC601 多项标准编制工作，其中已发布《大数据 数据分类分级工具技术要求》、《大数据 数据审计工具技术要求》、《大数据 数据安全服务能力分级要求》、《大数据 数据防泄露产品技术要求》、《大数据 数据安全运营管理平台技术要求》、《大数据 数据水印溯源产品技术要求》、《大数据 数据安全网关技术要求》、《数据安全治理能力评估方法》等八项标准。

产业图谱方面，亿赛通积极配合云大所《数据安全产品与服务图谱》调研工作，总结数据安全产品及服务的特点、发展现状，深化数据安全产品服务调研，洞察数据安全市场发展趋势。最终，亿赛通多项产品及服务入选，具体包括：数据分类分级、数据资产管理、数据防泄漏、数据库审计、态势感知、运营管理、合规咨询、数据安全运维等八项细分领域。



数据安全推进计划
DATA SECURITY INITIATIVE

数据安全产品与服务 图谱 2.0



产品评测方面，亿赛通多款产品通过了“可信数安”专项能力测评，包括：数据库安全审计系统（DAS）、数据脱敏系统（DMS）、数据安全运营管理平台（DSOP）、数据泄露防护系统（DLP）、网络数据泄露防护系统（NDLP）。权威认证再次证明了亿赛通在数据安全领域的实力和能力。



此外，CCSA TC601 组织了大数据“星河（Galaxy）”案例征集活动，活动一经发布，就受到了各大厂商的广泛关注 and 踊跃报名，共收到申报项目 595 份。其中，亿赛通和国网河南省电力公司联合申报的“数据安全运营管理平台（DSOP）”应用成果凭借专业的技术及完善的解决方案，荣获 2022 大数据“星河”案例——数据安全优秀案例。

| 单位名称 | 成果名称 | 成果类别 |
|--|-------------------|--------|
| 亿赛通科技股份有限公司 国网河南省电力公司 | 数据安全运营平台 | 数据安全治理 |
| 平安银行股份有限公司 | 平安银行数据安全运营平台 | 数据安全治理 |
| 安徽中鑫大数据科技股份有限公司 中国科学技术大学先进技术研究院 科大讯飞股份有限公司 | 量子安全管理平台 | 个人信息保护 |
| 浙江数盾科技有限公司 浙江数盾网络科技有限公司 中核集团核工业安全技术有限公司 | 核能行业数据安全运营平台 | 个人信息保护 |
| 阿墨云计算有限公司 金山网络汽车技术有限公司 | 阿墨云计算汽车云上数据安全运营平台 | 数据安全治理 |
| 数盾数字科技有限公司 | 数盾—一体化数据安全运营平台 | 数据安全治理 |

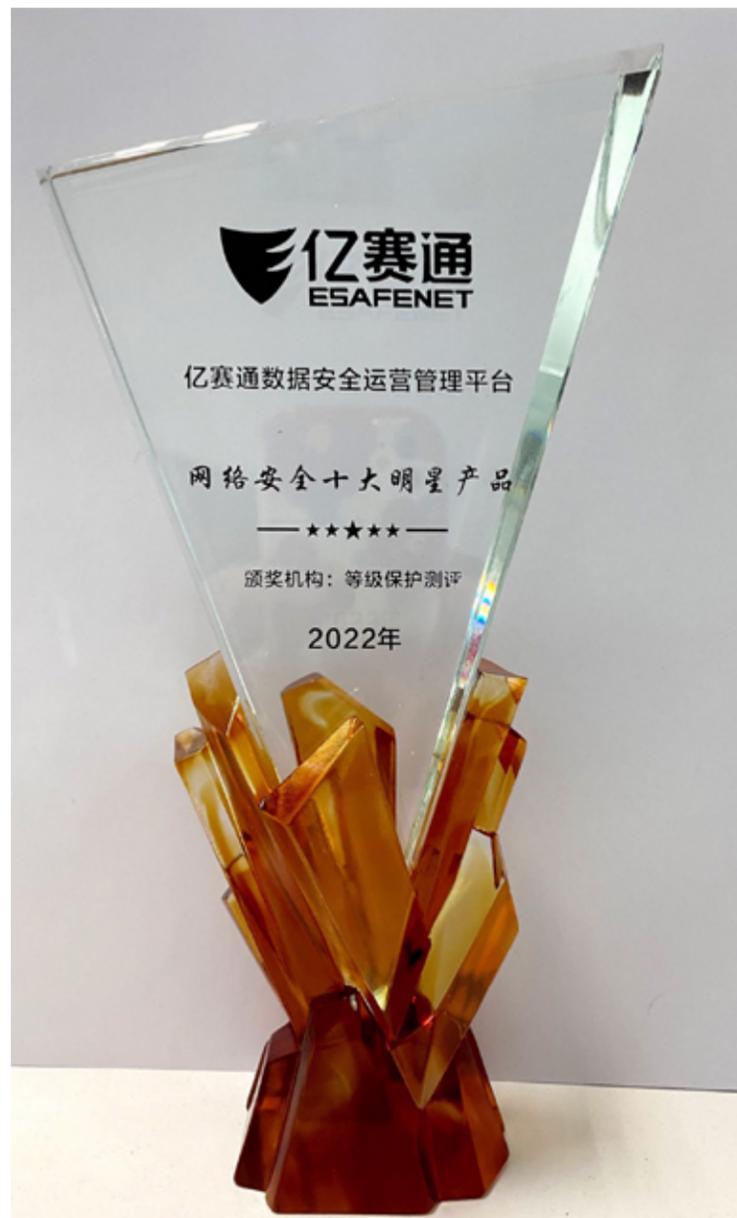
在国家明确要加强数据安全等基础通用标准的研制的情况下，信通院重磅发布《数据资产管理实践白皮书 6.0》《数据安全治理实践指南 2.0》报告。亿赛通作为中国数据安全专家，高度重视行业相关研究，结合广泛的实战经验和技術积累深度参编上述两项报告。云计算与大数据研究所向亿赛通多位同事在数据资产管理领域的支持表示感谢，愿未来继续携手共同推进大数据事业蓬勃发展。



亿赛通还为 DSI 数据安全推进计划“数安智库”输送多位行业专家，且发表《数据安全治理体系建设思路与方法》，独家分享数据安全思考和经验。多次参与 DSI 数据安全推进计划组织的沙龙及峰会，如：“数安 Talks”——数据安全风险管理及 2022 年大数据产业峰会等，均在会中发表重要演讲。

本年度亿赛通的各项荣誉与标准参编，是云大所、CCSA TC601 及 DSI 数据安全推进计划对我司在数据安全方向取得的成绩的肯定和认可。2022 年，是我司理论和实践工作的里程碑之年。未来，亿赛通将继续坚持自主创新，不断强化自身优势，提供以安全为核心的咨询、评估、实施、建设、交付服务，用专业可靠的服务和技术创造出标杆项目及专业产品。

亿赛通数据安全运营管理平台 喜获《2022年网络安全优秀评选》 十大明星产品



近日由等级保护测评主办的“2022年网络安全优秀评选”活动圆满结束，优秀企业及产品案例名录隆重发布。评选过程依托专家评审评分（占60%）与大众投票数量（占40%）的评选机制，亿赛通数据安全运营管理平台凭借其出众的能力在100余项申报项目中脱颖而出，成功入选“2022年网络安全十大明星产品”。

此次评选中的大众投票体现出亿赛通数据安全运营管理平台在客户侧的认可，一直以来亿赛通本着客户至上的原则，深入各个行业，解决客户实际需求与问题，帮助用户建立统一的数据安全运营管理体系，实现数据安全全局分析和动态监控。目前亿赛通数据安全运营管理平台已经在金融、医疗、政府、运营商等行业广泛应用。

金融行业

数字信息是金融产业发展的基础元素，此类数据包含大量用户个人信息和交易数据等敏感信息。金融数据具有复杂性、隐蔽性和易扩散性，为保障数据泄露、数据污染等一系列潜在风险，根据《JR/T 0223-2021 金融数据安全 数据生命周期安全规范》要求在数据采集、传输、存储、使用、删除及销毁全过程建立安全监测及防护。

结合金融行业的数据特点，平台将“人-过程-技术（PPT）”三者有机地集成和协同起来，对某银行进行全面的数据安全建设。平台通过机器学习、关键字识别、正则、文件指纹识别等技术对结构化和非结构化数据实现数据自动、精准的分类分级，并基于分类分级结果进行差异化策略配置。平台还利用大数据分析技术，对数据操作行为进行智能分析，构建用户安全行为模型，预知用户泄密风险并预警。同时提供丰富的报表展示功能，实时动态展示数据安全关键业务指标，让安全可视化、事件可追溯、态势可感知。

政府行业

某部委数据共享交换平台归集各个业务系统的数据，数据情况复杂、每天新增及访问量较大，对海量的政务数据进行安全监测、安全防护困难。基于共享交换平台的特点及客户的需求，通过部署亿赛通数据安全运营管理平台对共享交换平台的全量数据资产进行了盘点。扫描发现数据库总量40余个，表单总量800余张，单个表单的数据字段在40余个，单表最大数据量约40G。

进一步，根据数据安全相关的法律法规并结合部委自身业务特点，厘清数据资产，制定数据分类分级基本规则，并且使用数据安全运营管理平台进行数据分类分级及打标。在数据分类分级结果的基础上进行数据安全

策略配置，并且可以根据安全监测情况动态调整防护策略，为政企行业客户提供全面的数据安全技术支撑保障能力。

医疗行业

医疗行业HIS、LIS、CIS、PACS系统集中存储的大量的电子病历、个人敏感信息，一旦遭到篡改、破坏和泄露，势必对医疗机构的声誉、个人隐私安全等构成严重威胁，甚至影响社会的安定和谐。

为保障某医院数据安全，依托亿赛通数据安全运营管理平台对数据安全能力组件进行统一的配置和管理，包括分类分级、操作审计、访问控制、数据脱敏、数据防泄露等，将各个策略依据数据分类分级的结果进行应用到对应的人员/角色与数据资源，建立相应的权限对应关系。

此外，平台通过在每个节点部署探针来分析上报日志数据，探测发现威胁医院的数据安全事件，并提供完整追溯取证证据链，全面保障医院数据安全。

运营商行业

电信运营商的网络和业务系统作为与人们的生活、工作密切相关的信息载体，承载着海量而又敏感的资料内容。频发的客户信息泄露事件让电信运营商更加关注数据安全。

某电信运营商通过分阶段的方式进行终端、网络、存储全方位的数据安全防护建设，数据安全运营平台接收所有终端、网络、存储上报的日志，通过运营管理平台安全编排及响应处置对海量日志进行预处理，并根据丰富的安全运营经验固化处置流程，降低风险事件的处置时间，减少安全风险对业务带来的影响。

亿赛通数据安全运营管理平台能够在众多产品中脱颖而出，离不开专家及客户对产品能力的肯定和认可。荣誉与肯定既是鼓励，也是激励继续前行的动力。未来，亿赛通将继续深耕数据安全领域，不断打磨产品，为更多客户提供贴合业务特点、解决客户问题的优秀产品及方案。

深度融合 合作共赢 | 亿赛通正式加入金兰组织



近日，亿赛通正式加入金兰组织，相互支持，共同发展。合作双方本着联合创新、协作共赢的原则，充分发挥自身优势，围绕安全领域展开紧密合作。

金兰组织是由人大金仓发起，并联合国产基础软硬件及行业头部企业共同成立的生态合作组织。其宗旨是协同产业链上下游企业、行业专家及用户等相关创新力量，实现优势互补、资源共享、技术攻关，共同打造安全、好用、开放的产品与解决方案，在产品适配、市场推广、联合营销，人才培养等方面展开深入合作，助力国产软件和信息技术服务产业的高质量发展，促进合作组织成员的共同发展，共建包容、繁荣的信息技术生态系统。

作为国内数据安全专业厂商，亿赛通深知一人难挑千斤担，众人能移万座山的道理。多年来，已与数十家企业、机构开展生态合作，构建先进的生态体系，全力推动行业数字化转型，搭建开放、弹性、安全的平台。本次我司加入金兰组织，双方基于人大金仓与亿赛通核心产品，逐步开展合作，对产品充分适配、研发联合解决方案、打造专业领域的人才培训、组织成员间渠道建设、资源共享，共同将合作成果推向各行各业。

随着近年数字经济的快速演进，无论是政府部门还是企业组织，均响应发展趋势，积极运用数字化手段挖掘数据价值，释放数据红利。然而，伴随着指数级增长的数据量，近几年大规模数据泄露事件也频频爆发，并呈现逐年递增趋势。面对这一现状，如何在打通数据孤岛、释放数据价值的同时保障数据安全，成为企业用户的棘手问题之一。尽管对数据安全治理具有强烈需求，但不少用户无法对此投入大量人力物力，与专业的数据安全服务商合作，便成为性价比较高的选择。



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“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治理，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。

作为行业的翘楚，亿赛通加入金兰组织必将产生1+1>2的效果。未来，双方将进一步深化资源共享机制，共同助推国产化解决方案在性能和稳定性等方面的不断提升，运用新一代信息技术，共建创新、合作、共赢的数字经济美好未来！

榜样引领，亿赛通被数专委授予 “优秀成员单位”称号

优秀成员单位名单（排名不分先后）

北京亿赛通科技发展有限公司

上海观安信息技术股份有限公司

上海斗象信息科技有限公司

北京安华金和科技有限公司

杭州美创科技股份有限公司

2023年1月12日，中国计算机行业协会数据安全专业委员会（以下简称“数专委”）工作组年度工作会议在京顺利召开。作为数专委会员单位，亿赛通2022年积极参与数专委各项工作，被授予“优秀成员单位”称号。

助力网安产业创新提升 亿赛通积极参与数专委沙龙活动

近两年国家政策表明要大力发展数字经济，并明确提出数据安全为新兴数字产业。在此背景下，数专委凝聚数据安全领域各方力量，建立数据安全产业开放生态和联合创新的交流平台，在会、展、赛、训、平台、系列沙龙等方向开展了数据安全产业系列沙龙、数据安全能力评定及产品测评工作、数据安全大赛、数据安全产业发展成果、数据安全人才培养、数据安全标准提案征集及标准编制、数据安全产业大会等各项产业活动。

培养数据安全人才 推进数字经济高质量发展

8月，在工业和信息化部网络安全管理局指导下，由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、中国信息通信研究院共同主办，北京亿赛通科技发展有限公司、中国计算机行业协会数据安全专业委员会、路云天网络安全研究院联合承办了“数据安全人才培养”主题沙龙。此外，还作为支撑单位，参与第二期（8月）和第三期（9月）“数据安全职业能力培训”，开展数据安全工程师和数据安全评估师两个方向的教研和培训工作。

厚积薄发，专业加持 亿赛通参与数专委两项标准制定

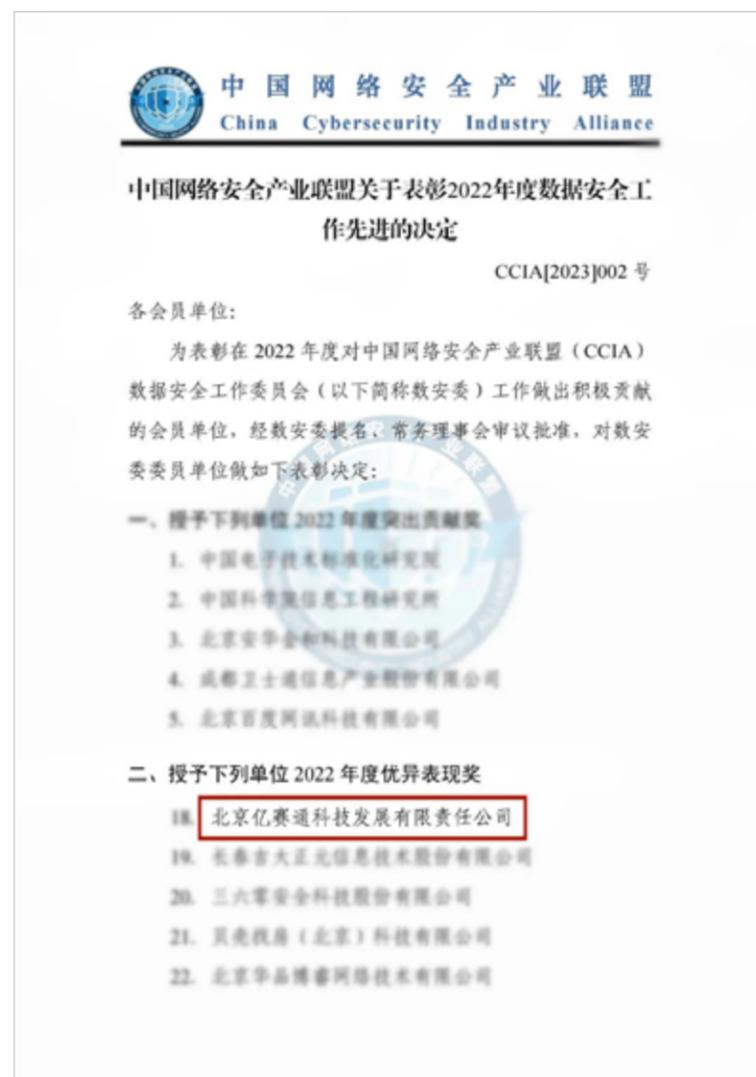
作为国内首批专注数据安全领域的厂商之一，亿赛通20年来砥砺前行，形成了集数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务为一体的产品板块。多年来的技术累积及口碑，也赢得了数专委的高度认可。在专业的加持下，全年积极参与标准制定工作，目前已参与计算机行业协会两项标准的制定：《邮件数据安全防护技术评价标准》及《电子文档安全的技术要求和评价标准》。

开展数据安全研究 亿赛通深度参与数专委研究项目

亿赛通围绕数据安全热点和难点应用场景的技术攻关，开展相关工作，联合部署重点实验室结合亿赛通丰富的行业推广和应用实践，开展相关的技术研发与研究工作。并参加2022年数据安全产业成果系列征集（第二期）-先进技术应用案例征集活动等工作。

2023年，亿赛通将继续与数专委建立长期、稳定的合作关系，在数据安全产业活动、人才培养、赛事保障、标准编制、关键技术与应用场景研究等多方面开展深入合作，充分发挥企业支撑作用，与数专委一道推进数据安全产业高质量发展，为中国的数字经济腾飞保驾护航。

亿赛通荣获中国网络安全产业联盟 CCIA 2022 年度殊荣!



近日, 中国网络安全产业联盟 (CCIA) (以下简称联盟) 针对 2022 年度对联盟工作做出积极贡献的会员单位进行了表彰。作为 CCIA 委员单位, 亿赛通积极参与配合联盟各项工作, 凭借优异的工作表现, 荣获 2022 年度“优异表现奖”。

联盟由积极投身于网络安全产业发展, 开展网络安全理论研究、技术研发、产品研制、测评认证、教育培训、安全服务等相关业务的企事业单位以及用户单位自愿组成, 属于全国性非营利行业组织。旨在搭建产业创新平台, 聚合产业势能, 营造良好产业发展环境, 促进产业创新发展, 加强行业自律, 提升网络安全技术产业和服务水平, 推动网络安全产业做大做强, 提升中国网络安全产业竞争力和国际话语权, 维护用户网络安全和利益, 为实现网络强国战略提供坚实保障。

作为联盟的委员单位, 自加入联盟以来, 亿赛通积极投身联盟各项工作, 始终践行中国数据安全专家的使命担当, 助力数据安全产业的发展。

全年, 亿赛通参与联盟举办的多场线上活动和方案评选, 被推选成业界具备领先竞争力、较高成长性以及较强发展潜力的标杆企业。联盟面向安全企业发起公开调研, 评选“2020 年 CCIA 中国网络安全竞争力 50 强 / 成长之星 / 潜力之星”榜单以及“网络安全服务情况调研”、“2022 网络安全优秀创新成果大赛”等活动。亿赛通凭借在管理团队、外部资源、技术能力、产品竞争力、经营数据等多项指标的优异表现, 得到联盟认可。

未来, 亿赛通将持续增强在数据安全、个人信息保护等方面的专业能力, 积极响应联盟号召并配合开展各项工作, 践行中国数据安全专家的社会责任与使命担当, 进一步推动产业结构化升级, 助力我国数据安全产业的高速发展。

培训认证新纪元 | 亿赛通专业化认证 培训初具成效

2022年，在国家高度重视和有力领导下，我国数据安全法规政策陆续出台，数据安全产业初具规模，创新能力不断增强，产品体系逐步建立，但也存在产业供给水平不高、应用需求有待培育、产业生态尚待健全、专业人才缺口大等问题。在此大背景下，亿赛通培训学院迎来有意义、有价值、有收获的一年，岁末年终，再回首这一年，培训认证工作取得了初有成效的进展。

亿赛通与中国电子信息产业发展研究院（赛迪研究院）、工业和信息化部人才交流中心等权威单位展开合作，联合推出数据安全职业能力培训体系、工信人才 & 亿赛通 - 数据安全专业人才认证两大体系共6门课程。课程自推出以来获得社会各企事业单位高度认可，并积极参与培训，取得卓有成效的成绩，共为数据安全行业输出300+人才。



亿赛通培训学院由亿赛通数十位专家级别讲师授课，旨在为数据安全行业储备精兵强将，培养一批高技术高能力专业人才。亿赛通具备行业数据安全方面的体系构建、安全规划、政策规范解读及前瞻技术研究，为行业用户引导设计安全规划、安全建设管理，提供体系化的安全解决方案和一体化的安全规划设计。通过培训让学员具备掌握场景化、体系化、标准化的解决方案能力，

了解数据安全、数据安全治理、数据治理、安全服务等主流安全解决方案，以及数据安全专家需掌握的必备技能及结构化的知识体系。

培训特点

| | |
|-------------|------------------|
| 需求驱动 | 以岗位能力需求建立人才培养方案； |
| 实践教学 | 以实际工作内容构建教学内容； |
| 虚实结合 | 构建真实的企业数据安全环境； |
| 立体合作 | 构建安全人才培养生态圈； |

2022年培训认证情况

| 课程名称 | 认证课程 | 第一期 | 第二期 | 第三期 | 第四期 |
|---------------|-------------|-----|-----|-----|-----|
| | 《数据安全工程师》 | 10 | 8 | 12 | 11 |
| 《数据安全架构师》 | 15 | 9 | 14 | 16 | |
| 亿赛通数据安全专业人才认证 | 认证课程 | 第一期 | 第二期 | 第三期 | 第四期 |
| | 《数据安全治理工程师》 | 19 | 25 | 25 | 18 |
| | 《数据安全运维工程师》 | 18 | 20 | 30 | 20 |
| 《商业机密保护工程师》 | 12 | 10 | 19 | 10 | |

新的一年亿赛通认证培训将开启全新征程，以培养产业和岗位终身学习为核心；以培养优秀的应用型数据安全人才为宗旨；以面向数据安全行业发展需要，提供完整的培训课程体系为目标；努力实现数据安全培训工作新纪元。

亿赛通培训学院联系人：卜老师 15979094485

2022 部分参与培训单位

- 江苏汉联网络科技有限公司
- 南京里恩特电子科技有限公司
- 上海适云信息科技有限公司
- 苏州德斯克信息技术有限公司
- 上海智游网络信息科技有限公司
- 深圳市艾美斯信息技术有限公司
- 广东安客信息科技有限公司
- 深圳市晶盛通科技有限公司
- 广州市锦锐信息科技有限公司
- 广州市安鼎信息科技有限公司
- 洛阳沃克网络科技有限公司
- 上海华垞信息技术有限公司
- 合肥融思信息科技有限公司
- 北京金联融科技有限公司
- 杭州中尔网络科技有限公司
- 深圳市网安计算机安全检测技术有限公司
- 中国软件评测中心
-

数据安全分类分级解决方案



行业需求

数据分类分级是数据安全的基础性工作，最终目标是基于分类分级结果配置差异化的安全策略和技术保障手段，从而兼顾数据有序流动与安全保障。数据分类分级在数据安全治理中至关重要，数据的分级是数据重要性的直观化展示，是组织内部管理体系编写的基础、是技术支撑体系落地实施的基础、是运维过程中合理分配安全管理资源的基础。

伴随着《网络安全法》、《数据安全法》、《个人信息保护法》的相继出台并实施，为应对日益严峻的数据安全形势，如何建立科学全面的数据安全治理体系，更加有效地保障数据安全，支撑以数据为关键要素的数字经济发展，已成为国家、全社会以及政府部门、行业机构、企事业单位等各类组织需要面临的共同挑战。

风险分析



建立数据资产分类分级清单，掌握数据的重要程度，成为数据安全首当其冲需要解决的问题，也是数据安全治理的基础。

解决方案



方案收益

数据安全分类分级满足金融、运营商、政府等行业数据分类分级标准要求，帮助客户对标分类分级标准，对客户数据进行分类分级治理，制定合理的安全保护策略，为数据的安全与利用之间找到平衡点。



零信任数据安全解决方案



行业需求

随着信息技术的快速发展，云计算、大数据、物联网、移动互联、人工智能等新兴技术为政府部门及各类企业的信息化发展及现代化建设带来了新的生产力，但同时也给信息安全带来了新挑战。一方面，云计算、移动互联导致的企业边界瓦解，难以继续基于边界构筑企业的安全防线；另一方面，外部攻击和内部攻击愈演愈烈，以 0day 漏洞、APT 攻击为代表的高级持续攻击仍然能找到各种漏洞突破企业的边界，同时，内部业务的非授权访问、雇员犯错、有意的数据窃取等内部威胁层出不穷；另外，国家和行业层面对企业安全的监管力度逐步加强，也对企业安全提出了更高的要求。只有充分的认识到这些新 IT 时代的安全挑战，才能更好的进行应对。

风险分析

远程办公

从安全趋势上看，内网安全基于边界的安全已经不是那么牢不可破，数字化办公发展导致没有边界内网。核心的爆发点还是来自于疫情带来的物理隔断，大家远程办公，这是最基本的适用场景，人们已经不得不使用这种架构。

运维管理

“删库跑路”作为一种历史悠久、后果严重的公司资产损坏事故，一旦发生，后果难以估量，轻则业务短时间不可用，重则公司倒闭关门，甚至有人为此坐牢。虽然这些破坏计算机信息系统的不法分子已经受到应有的惩罚，但对于企业来说，已经遭受的损失、给企业带来的负面影响却无法挽回。

业务上云

同时，云计算业务天然需要零信任。云计算的快速发展和普及应用，包括应用云化，基础架构的异构化和混合化，业务的数字生态化以及接入网络及设备的多元化因素都推动了更多的企业开始通过部署零信任架构来建立能够适应云时代的全新安全体系。

解决方案



亿赛通零信任数据安全解决方案打破了传统的认证即信任、边界防护、静态访问控制、以网络为中心等防护思路，遵循零信任安全理念，通过对数据资产盘点梳理并分级分类，建立起一套以身份为中心，以识别、持续认证、动态访问控制、授权、审计以及监测为链条，以最小化实时授权为核心，以多维信任算法为基础，认证达末端的动态安全架构。

- 1、重要资产隐身，规避网络扫描、渗透行为
- 2、先认证后准入，以用户权限为中心，权限最小化
- 3、保护应用群及服务器之间最小细粒度安全给予划分

方案收益

基于“持续验证，永不信任”理念，默认不信任企业