亿赛通 ESAFENET

ESAFENET

亿赛通企业月刊　　中国数据安全专家　　www.esafenet.com

01 月刊

2024 年共 12 期

启航赴新程

2024 亿赛通

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

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

新年快乐
2024

刊首语 PREFACE

《亿赛通一月刊》2024 启航赴新程

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，2024 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。值此新春佳节之际，亿赛通全体员工祝大家新年快乐！

国内

1、安徽省政协委员王珩：加快医疗健康数据安全治理和要素化开发

摘要：1 月 23 日，正在参加安徽省政协十三届二次会议的安徽省政协委员、安徽医科大学第一附属医院副院长王珩，向大会提交了《关于加快推进安徽省健康医疗数据安全治理 促进数据经济发展的提案》，呼吁重视医疗健康数据的保护、共享、流动以及开发利用。

2、境外机构在我国渤海、东海周边投放大量窃密设备！

摘要：近期，国家安全机关工作发现，多个境外机构以免费提供设备、共享航空信息为诱饵，依托网络社交平台面向境内航空爱好者精准招募“志愿者”，并跨境邮寄设备，指挥“志愿者”在我境内非法采集、向境外秘密传输我国飞行器飞行数据。

3、2023 年数据泄露风险报告：来自金融行业的泄漏最严重

摘要：2023 年，各行业全面数字化，加速业务创新发展的同时，确保大量数字资产及云上业务的数据安全，成为不少企业面临的“两难之境”。因数据泄露问题产生的影响及损失进一步扩大，对各行业关键领域造成严重影响。根据《2023 年数据泄露风险年度报告》，对 2023 年数据泄露风险概况、黑产数据交易市场等进行具体分析，数据显示：

1、2023 年，全网监测并分析验证有效的数据泄露事件超过 19500 起，涉及金融、物流、航旅、电商、汽车等 20 余个行业；

2、金融行业超过物流行业，成为 2023 年公民个人信息泄露事件数量最多的行业；2023 年航旅行业公民个人信息泄露事件数量也出现大幅增长，在公民个人信息泄露的行业分布中首次排名前三。

4、警方通报！案涉百位当红明星

摘要：杭州富阳区网警在日常工作中发现，有人在境外社交平台上建立了一个“个人信息库”机器人，大肆贩卖公民个人信息。网警调查后发现，侵犯公民个人信息的黑客姓韦，19 岁。韦某高中辍学后继续自学计算机，半年前他在境外社交平台上看到一条“个人信息库”寻找合作的消息，想着这不仅能看到别人的个人信息，还能转手赚钱，就联系上了对方。很快上家提供源代码接口，韦某又自制了能够自动进行收费交易的“机器人”，可以大量转发到各类社交群，特别是明星的粉丝群。富阳区公安分局网警大队民警杨名介绍，“信息库中包含了大量明星、网红的数据，当红的明星有一百位左右。你只要输入名字，就会自动返回关联的数据。你输入的信息越多，提供的信息就越精准。”

5、约谈 310 家、关闭 530 个！重庆严厉打击网络违法违规行为

摘要：网信重庆消息，2023 年，全市网信部门不断健全网络执法体系，进一步规范网络执法行为，始终坚持依法治网管网，依法处置各类网络违法违规案件，持续加大网络安全、数据安全和个人信息保护等领域的网络执法力度，全年累计约谈网站 310 家，暂停功能或更新网站 23 家，依法关闭违法违规账号 530 个，警告网站 326 家，关闭违法违规网站 227 家，向有关部门移交案件线索 2840 条，开展行政处罚案件 38 起，其中罚款处罚 10 起。

6、大学生“被法人” 身份冒用几时休

摘要：22 岁的李学，真希望自己没做过所谓的“兼职”。2023 年 7 月，在宁夏上大学的他，因一份需要人脸验证的“兼职”而泄露了个人信息，莫名其妙地成为了四川多家公司的法定代表人或高管。当年 9 月，他在报考公务员考试时无法通过资格审查，没能参加考试。

7、房产推销电话不断！谁在泄露个人信息？住建部公布

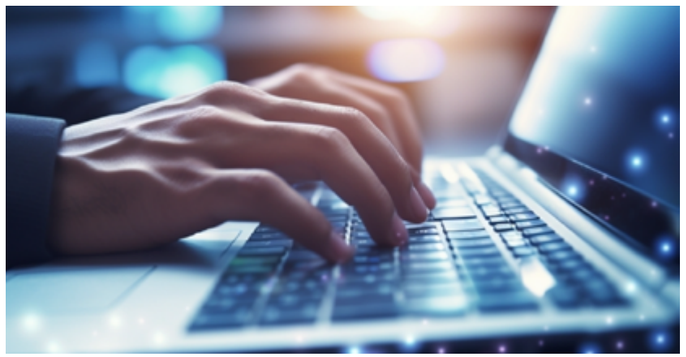
住房城乡建设部办公厅关于
房地产中介行业侵犯公民个人信息
违法违规典型案例的通报

摘要：1 月 22 日上午，住建部官网通报了 5 起房地产中介行业侵犯公民个人信息违法违规典型案例：有人将业主留在中介公司的 12716 条个人联系方式非法出售，有人辗转四家房产销售公司获取楼盘业主 78100 余条信息，还有人利用售楼处工作便利，复印业主的电话后成立房产中介公司做业务……通报信息显示，有人非法获取业主信息 30 余万条，出售获利 150 万元，最终被判处有期徒刑三年，处罚金额 160 万元。

8、QQ 号信息遭泄露，亲朋好友被拉进了诈骗群

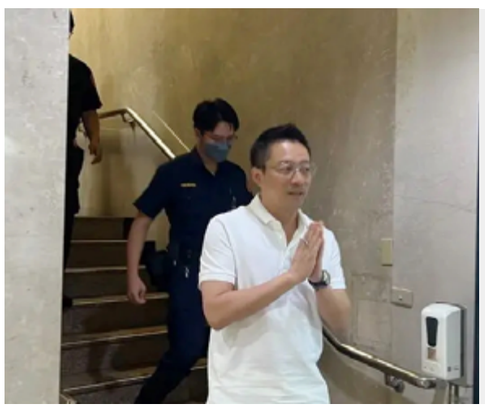
摘要：近日，济南市民赵刚（化名）的 QQ 号被盗，骗子将他的好友们拉进一个群里进行诈骗。赵刚表示，骗子在进行诈骗时，他的 QQ 号还能正常操作，信息不知道什么时候泄露的。网警表示，不法分子盗号后会直接实施诈骗，被害人发觉后尽快修改密码，如果账号里的钱有损失，应保留证据后尽快报警。

9、教培机构员工泄露个人信息被公诉！



摘要：2023 年，虹口区检察院办理了两起公司员工窃取公民个人信息案，两起案件都发生在某教育科技公司。一起是教育科技公司客服人员贾某利用接受客户咨询的职务便利将获取的客户信息，私自发送给外部人员杨某招募学生并获利分成。另一起是汪氏兄弟案，二人里应外合由哥哥入职教育科技公司获取 VPN 账号密码，弟弟则利用“爬虫软件”远程大量频繁访问教育科技公司数据库，爬取信息并转卖获利。这两兄弟中有一人是有侵犯公民个人信息罪前科的人员。

10、汪小菲被台北地检署依法提告 公开大 S 离婚协议涉嫌泄露隐私



摘要：1 月 24 日，据台媒报道，台北地检署依个人数据保护法起诉汪小菲。据悉，汪小菲在网上晒与大 S 的离婚协议，外泄其地址、个人帐号等数据，大 S 对汪小菲进行提告。回顾大 S 和汪小菲的离婚历程，两人于 2021 年协议离婚，但随后双方因财产问题而产生矛盾，2022 年 12 月，两人就财产问题争执不下，甚至在社交媒体上公开交火。

11、TA 们刚出生，信息就被泄露！检察机关斩断贩卖新生儿信息的“幕后黑手”

摘要：江苏省常州市新北区检察院依法办理了一起新生儿信息被泄露案。同年 8 月，经新北区检察院提起公诉，泄露新生儿信息的李某等三人因侵犯公民个人信息罪分别被法院判处有期徒刑三年四个月至三年不等，各并处罚金 21 万元至 8 万元不等。此外，李某等三人还缴纳了民事赔偿金 37 万元，并在省级媒体上公开赔礼道歉。日前，购买新生儿信息并用于影楼推销的黎某等人因涉嫌其他犯罪被公安机关进一步侦查。

12、谁泄露了 300 余万条用户数据？北京网警：坚决打击！

摘要：不久前，北京警方接到辖区内一互联网公司报案，称该公司的求职招聘类 App 的短信验证码接口遭受攻击达 1300 多万次，攻击还成功匹配注册账号 30 多万个。为此，北京市公安局网安总队会同朝阳分局立即成立专案组开展侦查。在侦查中警方发现，这是一起典型的黑客利用网站漏洞非法获取账号信息并用于违法活动的案件。随后专案组在四川省将犯罪嫌疑人喻某抓获。据喻某交代，他在 2022 年 10 月注册了该招聘网站的账号，通过数次尝试验证接口，他发现该网站的签名算法相对单一，于是利用此弱点编写指令，制作黑客软件，对该网站进行撞库攻击。

国外

1、程序员帮捉 Bug 却被判罚 2.3 万元，一切只因帮客户检查出一个恐泄露 700,000 条数据的漏洞


23.6.2021 Datenschutzverletzung | Modern Solution GmbH & Co. KG

Web-Ansicht | webview | Aperçu web | Vista Web | Visualizzazione web

Modern.Solution.

Anzeige einer Datenschutzverletzung

Sehr geehrte Damen und Herren,

mit dieser Nachricht möchten wir Sie über eine Datenschutzverletzung bei der Modern Solution GmbH und deren Umstände informieren.

Was genau ist passiert?
Heute, am 23.06.2021 um 8:09, wurden wir von einem ‚ethischen Hacker' auf eine Sicherheitslücke in unserem System hingewiesen. Aufgrund dieser Sicherheitslücke war es möglich, das Passwort zu unserer Datenbank abzugreifen und auf unverschlüsselte Passwörter und personenbezogene Daten zuzugreifen. Über dieses Datenbankpasswort verschaffte sich der Hacker extern Zugriff auf unsere Datenbank sowie unser Ticketing-System. Inwiefern eine Weitergabe oder weitere Nutzung dieser Daten durch den ‚ethischen Hacker' erfolgt ist und ob es zu weiteren Zugriffen gekommen ist, ist uns derzeit nicht bekannt. Wir arbeiten intensiv an der Aufklärung des Vorfalls.

摘要：1 月 17 日，德国于利希地方法院宣布了一项最新判决结果：“一位独立程序员帮助一家零售公司检查软件问题时，发现此软件存在一个导致近 70 万买家数据会暴露的重大漏洞。为此，该名程序员联系了开发这款软件的公司，却遭软件开发商矢口否认，随后他与一名科技博主将这一漏洞公之于众，受到了广泛的关注。令人没想到的是，后来软件开发商将相关软件进行了下线处理后，也向警方举报了该名程序员，并称之为‘黑客’。由于这种情况，这名程序员现因未经授权访问第三方计算机系统和刺探数据（根据《德国刑法典》（StGB）中所谓的黑客条款 202a 应受到惩罚）而被处以 3,000 欧元（约 2.3 万元）的罚款，同时还必须支付诉讼费用。”

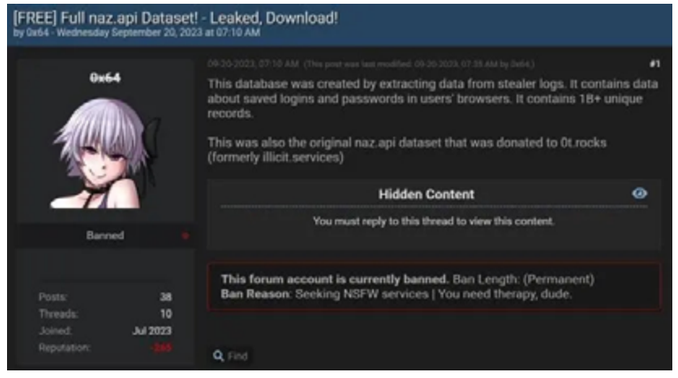
2、向美西方看齐？印度跟风炒作中国设备安全风险，成立情报部门监控中企

摘要：据《今日印度》20 日报道，印度联邦和邦政府办公室（包括敏感部门）安装大量的生物识别考勤系统（BAS），印度安全机构对其中检测到的中国微芯片和硬件可能造成大规模数据泄露的风险感到“震惊”。报道称，印度情报机构在调查中发现，大约有十几家向政府机构提供生物识别考勤系统的印度公司在设备中使用了原产于中国的部件。这些公司正在接受数据泄露（如果有的话）方面的调查。《今日印度》称，近 7500 个联邦和邦政府机构使用了 8 万多个此类生物识别考勤系统。这包括主要的联邦和邦政府机构以及军事和国防办公室。

3、研究人员发现史上最大泄露数据库，包含 260 亿条信息

摘 要： 根据 Security Discovery 和 CyberNews 的研究人员的说法，该数据库大小达到了惊人的 12TB，研究人员认为其由恶意黑客或数据掮客编纂而成，汇集了来自数千次先前数据泄露事件的记录，虽然其中可能包含大量重复数据，但仍让人担忧。该数据库中包含了来自微博以及 Twitter、Dropbox、领英、Adobe、Canva 和 Telegram 等平台的用户记录。而且，数据库中还发现了来自美国和其他国家政府机构的记录。

4、安全领域 2024 开年首炸：7084 万个邮箱账号、1 亿个密码信息泄漏



摘要：安全研究人员发现了有史以来最大的密码泄露事件之一，包含 7084 万个电子邮件地址以及超过 1 亿个密码凭证，至少有超过 40 万 Have I Been Pwned（HIBP）用户受到影响。

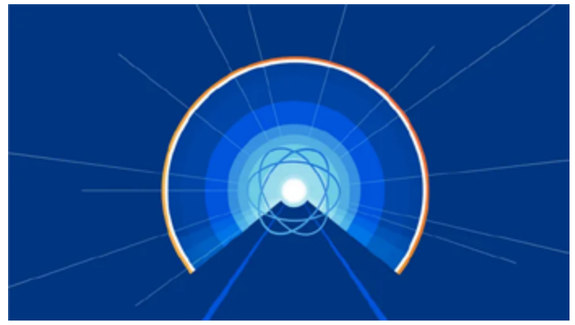
5、多款主流 GPU 被发现漏洞 或泄露 AI 大模型数据

摘要：日前据报道，安全研究人员 Trail of Bits 发现了一个漏洞，有可能从 GPU 内存中窃取“关键数据”，英伟达、苹果、AMD 和高通等多个型号的消费性 GPU 受到影响。该漏洞被命名为“LeftoverLocals”，这个漏洞不只是针对消费者应用程序，而是通过侵入大语言模型（LLM）和机器学习（ML）模型中使用的 GPU 来完成任务。由于模型训练涉及敏感数据使用，因此提取数据更危险。卡内基梅隆大学（Carnegie Mellon University）的专家正在对 LeftoverLocals 进行跟踪，据称该信息已经被受其影响的主要 GPU 供应商共享，其中包括英伟达、苹果、AMD、Arm、英特尔、高通和 Imagination 等。

6、宝马公司遭受重定向漏洞影响

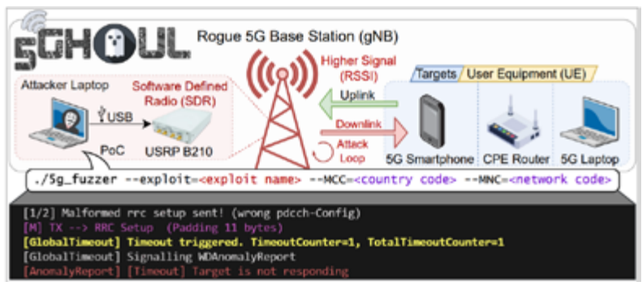
摘要：Cybernews 的研究团队发现，宝马公司的一些子域名很容易受到重定向漏洞的影响，使攻击者能够通过这类漏洞伪造实际上是指向恶意网站的链接。宝马的两个子域名容易受到 SAP 重定向漏洞的攻击。它们被用来访问宝马经销商的内部工作场所系统，为攻击者发动鱼叉式网络钓鱼活动或分发恶意软件提供了便利。

7、KyberSlash 安全漏洞影响量子加密项目安全性



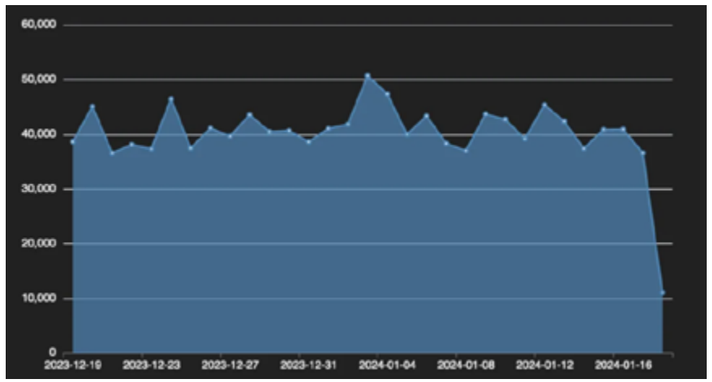
摘要：近日，研究人员发现多个 Kyber 密钥封装机制实现受到 KyberSlash 安全漏洞的影响，攻击者利用这些漏洞可以恢复出密钥。KyberSlash 漏洞属于时序攻击，攻击者在 Kyber 解封装的过程中执行特定除运算时，可以分析执行时间并推算出秘密信息，以破解解密过程。如果实现 Kyber 的服务允许针对同一密钥对的多个操作请求，那么攻击者就可以通过度量时间差异并逐渐计算出密钥。有漏洞的代码存在于 KyberSplash1 和 KyberSplash2 中。

8、5Ghoul 攻击影响着七百多款 5G 手机



摘要：来自新加坡技术设计大学和 A*STAR 的研究人员发现了搭载高通和联发科芯片 5G 设备的 14 个安全漏洞——"5Ghoul"。5Ghoul 攻击可以引发服务暂时中断和网络降级，影响 710 款安卓、苹果 5G 智能手机，以及路由器和 USB 调制解调器。

9、威胁组织利用 Androxgh0st 恶意软件收集云凭据



摘要：近日，美国联邦调查局（FBI）与网络安全和基础设施安全局（CISA）发布联合公告说道，有威胁组织在部署僵尸网络，利用 Androxgh0st 恶意软件大搞破坏。这个恶意软件能够收集云凭据（比如 AWS 或微软 Azure 等云服务的凭据），滥用简单邮件传输协议（SMTP），并扫描查找亚马逊简单电子邮件服务（ASES）参数。

10、苹果、AMD 和高通 GPU 曝出安全漏洞，致使不法分子可以窥探其他用户

摘要：苹果、高通、AMD 和 Imagination 等公司开发的 GPU 驱动程序近日曝出了设计缺陷，这个设计缺陷可能会被共享系统上的不法分子用来窥探其他用户。比如说，不法分子可以观察到处理器为其他用户加速的大语言模型（LLM）及其他机器学习软件。对于那些在云端共享服务器上训练或运行 LLM 的人来说，这将是一个潜在安全隐患。在非共享系统上，设法在系统上运行的恶意软件可能滥用这个弱点来窥视单独用户的 GPU 活动。

11、大批 Linux 设备遭到蠕虫攻击

摘要：研究人员表示，一种新的自我复制恶意软件正肆虐全球各地的 Linux 设备，这种恶意软件并利用复杂步骤隐藏其内部加密货币挖掘恶意软件。这种蠕虫是 Mirai 的定制版本，而 Mirai 是一种僵尸网络恶意软件，可以感染基于 Linux 的服务器、路由器、网络摄像头及其他所谓的物联网设备。

12、云配置错误是黑客首选的攻击目标

摘要：麻省理工学院教授 Stuart E. Madnick 最近撰写的报告中显示，2013 年到 2022 年间，数据泄露事件增加了两倍，2023 年成为创纪录的一年。报告强调攻击者越来越擅长对云配置错误进行攻击，并利用不安全的端到端手机加密，勒索软件越来越猖獗。Madnick 发现，与 2022 年上半年相比，2023 年上半年遭到勒索软件攻击的企业组织增加了近 50%。攻击者还在攻击期间觊觎大批的移动设备，冻结所有通信内容，直到受害者支付赎金为止。

多项荣誉！亿赛通受邀参加海淀区商业秘密保护工作发布会暨服务联盟成立大会

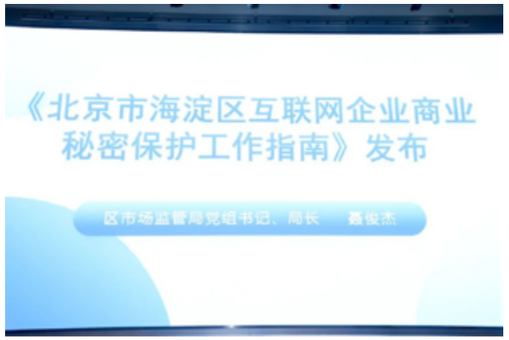
近日，由海淀区市场监管局主办的区商业秘密保护工作发布会暨服务联盟成立大会在中关村自主创新示范区展示中心成功举办。海淀区政府党组成员、副区长徐振涛，北京市市场监管局公平竞争处处长于航，海淀区市场监管局党组书记、局长聂俊杰出席会议并致辞。

大会邀请了中关村科学城管委会、区检察院、法院、司法局、公安海淀分局等相关单位领导，企事业单位、社会团体代表共计 150 余人参加。

徐振涛同志在致辞中介绍了海淀区 2023 年商业秘密保护工作取得的成果，并表示，海淀区将继续开展好商业秘密保护创新试点工作，更加关注制度体系建设，充分发挥政策引导效应，为海淀区提升产业创新生态，促进经济高质量发展提供有力支撑。

于航同志表示，海淀区科研实力雄厚、区位特点突出、互联网企业集中，商业秘密保护需求迫切，在当前我国商业秘密保护制度体系和保护规则尚不完善的大背景下，本次发布的《海淀区互联网企业商业秘密保护工作指南》（以下简称《工作指南》），是制度层面的创新尝试，对互联网行业领域有很强的指导作用。在全市首批 45 个示范基地中，海淀区的企业和园区也充分发挥出了引领作用。同时对海淀区作为全市乃至全国的创新标杆，提出了三点期待：完善保护机制打牢保护根基、发挥区域优势加强理论研究、凝聚多方合力建设服务网络。

大会正式发布了《北京市海淀区互联网企业商业秘密保护工作指南》，海淀区市场监管局党组书记、局长聂俊杰从出台背景、主要内容以及下一步工作方向三个方面对《工作指南》进行了全面解读。该指南从商业秘密保护制度、文件数据管理、人员管理、信息网络建设、泄密防范、维权措施等角度，指导企业建立标准和规范，旨在帮助企业迅速建立适应云计算、物联网和大数据等新技术、新应用情况下的商业秘密保护体系。



全市首个商业秘密保护服务联盟“海淀区商业秘密保护服务联盟”也在本次大会上正式启动。该联盟由行业协会、律师事务所、公证处、鉴定所、认证机构、数据安全公司、园区孵化器等 32 家组织机构共同参与发起。联盟以“政府指导、企业自主、行业互助、合作共赢”为宗旨，通过聚集、整合、共享专业服务资源，为海淀区企业商业秘密保护工作提供高标准的专业服务；在宣传普及法律法规、提供专业咨询服务、开展培训交流活动、定制具体解决方案等方面发挥积极作用。作为海淀区商业秘密保护服务联盟轮值单位，亿赛通将以“政策 + 标准 + 咨询 + 方案 + 服务 + 人才”相结合的“六位一体”发展思路，帮助合作企业增强商业秘密保护意识，完善商业秘密保护体系，提高商业秘密安全技术防护手段，系统化培养商业秘密保护人才，形成商秘保护管理新模式，为标准落地和企业赋能搭建一架专业的服务桥梁。

此外，本次大会上海淀中小企业协会发布了《中小企业商业秘密安全保护规范》团体标准，该标准是由北京亿赛通科技发展有限责任公司牵头组织，北京市海淀区市场监管局指导，多家单位共同参与标准制定工作。这一标准为中小企业商业秘密安全保护领域工作的开展提供了指导，填补了相关领域的标准空白。同时会上还为入选北京市第一批商业秘密保护示范基地的企业和园区，以及海淀区商业秘密保护工作站进行了授牌，鼓励示范基地和工作站充分发挥标杆企业的示范作用和自身优势，以点带面辐射带动全区商业秘密保护水平整体提升。

商业秘密是指不为公众所知悉，具有商业价格，并经采取相应保密措施的技术信息、经营信息等商业信息。企业作为创新驱动发展的主体，其商业秘密、创新成果决定了企业的核心竞争力，对企业的生存发展起到决定性作用，加强商业秘密保护，对于优化营商环境，激发市场主体活力和创造力，推动经济创新发展、高质量发展具有重要意义。

海淀区在 2022 年成功入选全国首批商业秘密保护创新试点地区的基础上，区市场监管局积极推进以企业为中心的商业秘密保护体系建设，印发《海淀区商业秘密保护创新试点工作方案（2023—2025）》，统筹全区整体商业秘密保护试点工作，广泛开展商业秘密保护示范基地培育，绿盟科技、亿赛通等 4 家企业和中关村创业大街等 3 个园区成为北京市第一批商业秘密保护示范基地；出台《北京市海淀区互联网企业商业秘密保护工作指南》，助力海淀区互联网企业建立健全商业秘密保护体系；加强与行业协会沟通交流，推动出台自律规范，指导北京海淀中小企业协会发布《中小企

业商业秘密保护规范》团体标准；联合区公安、法院、检察院、司法局、知识产权局等部门，出台《海淀区商业秘密保护联动协作机制》，加强行政保护和司法保护的有效衔接和功能互补。本次大会还对一批商业秘密保护示范基地、工作站进行了授牌。

亿赛通凭借在商业秘密保护工作中的多年积累与沉淀，在众多竞争者中脱颖而出，成功入选《北京市商业秘密保护示范基地名单》，并作为示范基地代表发言。亿赛通表示，成为商业秘密保护示范基地是公司在商业秘密保护提升服务功能的又一重大实践，未来，希望通过建立统一的商业秘密安全保护技术标准，形成商业秘密保护技术的基本统一要求，提升园区企业商业秘密的安全性及对商业秘密的管理与保护能力，为商业秘密权利人和相关主体的合法权益提供规范性依据。

未来，亿赛通将在服务联盟的指导下，继续发挥自己的优势，加大产品研发，把握商业秘密保护市场，夯实基础，并与其他单位一起为园区企业提供专业、高质量的服务，保护企业创新创造，为中国数据安全产业的健康可持续发展贡献出自己的一份力量！

亿赛通出席数专委年度工作总结会，多项荣誉，满载而归

亿赛通此前与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）达成深度合作，双方深化共识，搭建产业生态，为数据要素发展贡献力量。这一年中，亿赛通围绕数据安全治理、数据安全服务、数据治理等方向，积极参与产品评测、案例甄选、人才培养和赛事支撑等工作，持续助力国家数据战略和行业发展的充分融合。

近日，数专委召开了年度工作总结会。会上，数专委总结了 2023 年度工作，展示本年度所取得的成绩以及 2024 年度工作计划，表彰优秀支撑单位。亿赛通作为数专委会员单位，2023 年积极参与数专委各项工作，在大会获得多项荣誉，收获满满。

助力网安产业创新提升 亿赛通积极参与数专委活动

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研究、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。亿赛通深度支撑数据安全大赛及其他数专委相关工作，在大会被授予“赛事工作组 -- 卓越贡献奖”及“研究工作组 - 数据安全研究优秀贡献奖”等多项荣誉。其中，亿赛通赛事工作组及数据安全生态两项荣誉对企业要求极高，表明了数专委对我司相关赛事及生态合作方面的支撑的高度认可。

培养数据安全人才 推进数字经济高质量发展

2023 年，与工业和信息化部教育、中国计算机行业协会数据安全专业委员会开展数据安全人才培养，已开展 5 期共培养优秀数据安全评估人才 200 余人。并且，亿赛通数据安全培训学院已推出七门，服务于市场广大数据安全需求客户群体，培训人数达 2000 余人。本次大会，被人才培养工作组授予“优秀贡献奖”荣誉。

开展数据安全研究 亿赛通深度参与数专委产品测评

产品评测方面，亿赛通多款产品获得了中国软件测评中心数据安全产品检验证书，包括：网络数据泄露防护系统（NDLP）、亿赛通安全管理平台。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。在大会中被授予“数据安全研究优秀贡献奖”荣誉。

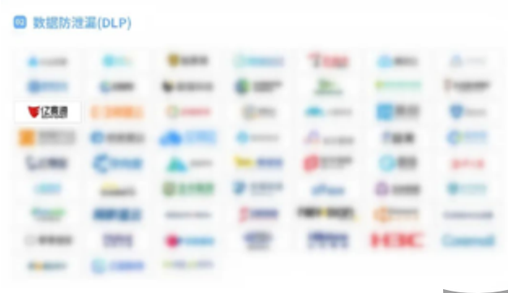
本年度亿赛通的各项荣誉，是数安委对我司在数据安全方向取得的成绩的肯定和认可。2023 年，是我司理论和实践工作的里程碑之年。2024 年，亿赛通将继续与数专委建立长期、稳定的合作关系，在数据安全产业活动、人才培养、赛事保障、标准编制、关键技术与应用场景研究等多方面开展深入合作，充分发挥企业支撑作用，与数专委一道推进数据安全产业高质量发展，为中国的数字经济腾飞保驾护航。

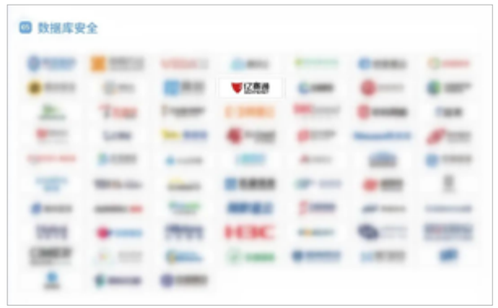
全景图 +1 | 细分领域逐步扩增，亿赛通打响开年第一枪

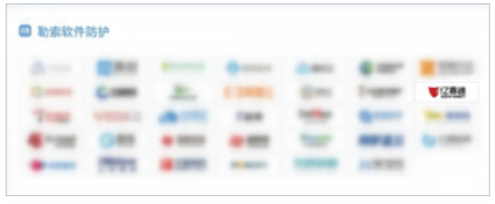
近日，网络安全行业门户网站 FreeBuf 发布《CCSIP 2023 中国网络安全行业全景册（第六版）》。亿赛通作为数据安全领域的代表厂商，凭借先进的产品技术架构和强大的自主研发实力入选数据防泄漏 DLP、分类分级、数据库安全、数据脱敏、勒索软件防护、数据安全治理（解决方案）、数据安全管控（平台型）、商用密码、邮件安全、防火墙、安全咨询与培训教育、风险评估、视频专网等十三大细分领域。

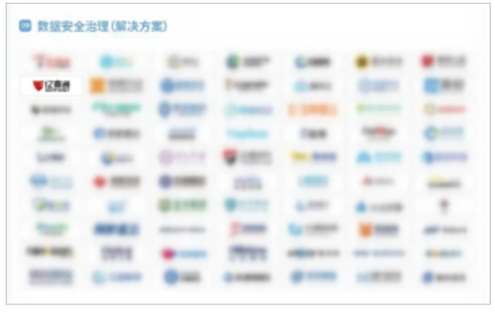
此前 FreeBuf 咨询已累计发布五个版本全景图册，为企业提供网络安全产品选型参考，帮助企业了解中国网络安全技术与市场的发展趋势。本次第六版全景册以 PDR 网络安全模型为基础，并参考 IPDRR 安全框架和 P2DR2 模型，在基础的 Protection（防护）、Detection（检测）、Response（响应）三层逻辑上优化出第 4 层，即“持续改进”，形成“防护—检测—响应—持续改进”的安全闭环。在核心模型之外，另增加了网络基础安全、业务场景、前沿技术 3 个大类，构建完整的企业网络安全建设链。

数据安全

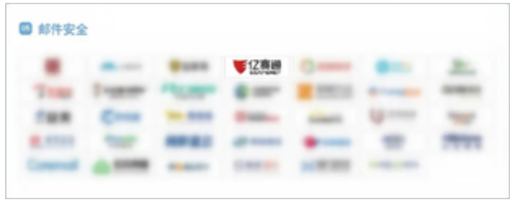




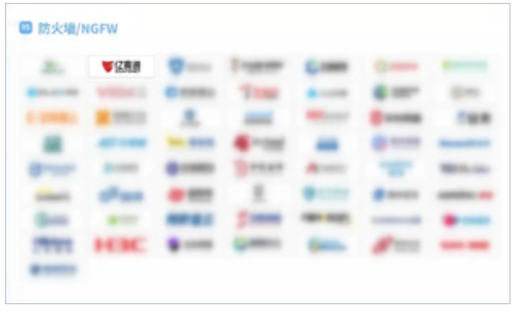




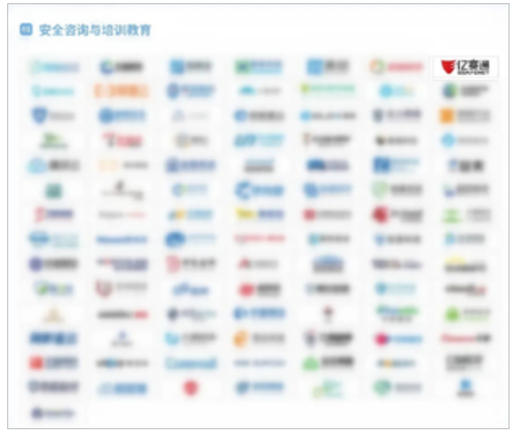
应用防护



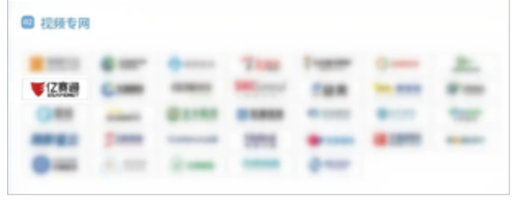
边界访问控制



安全服务



物联网安全



现如今，由于很多企业缺乏足够专业的团队和资源去应对各种内部威胁、外部威胁、恶意程序，以及各种业务安全场景。内部也没有一套完整的系统能快速、标准、流程化地联动各个部门或资源，导致撞库、勒索病毒、内部泄露等事件频发。

与此同时，国家对数据安全的要求越来越严格，安全等保、行业监管、企业审计等标准、法规对企业的业务环境要求也越来越高。面对安全运营的新形势，亿赛通独特的数据安全治理智能化技术体系，通过智能化分类分级工具快速准确地完成组织的业务梳理和数据梳理，并形成规范化的策略库，即主体、客体及两者之间的策略，同时将上述数据根据积累的知识库智能化衔接到技术平台，实现了对组织数据的智能识别、智能防护、智能监测、智能运营，构建可视、可控、可管、可溯的覆盖数据全生命周期的综合解决方案。根据云、网、端三类应用场景，实现数据安全理念建设的可落地执行，从不同维度为用户提供产品和服务，形成一体化运营管理。切实解决了企业数据安全治理难题，因此可以成为多份行业报告、全景图的重要代表厂商。

亿赛通再次上榜 Freebuf 全景图册，充分体现了公司多年来自主研发的技术优势和市场实际应用验证的品牌实力！下一步，亿赛通将继续致力于推动数据安全产业发展，通过对自身技术实力的提升，不断巩固在国内数据安全产业的已有优势，为用户业务提供更强大的数据安全治理能力支撑，借助自身的创新力带动更多行业创造更大价值。

重磅新誉 | 亿赛通荣获“2023 年度先进私营企业”称号

为表彰优秀，鼓励先进，海淀私个协举行 2023 年度总结表彰大会。海淀私个协各分会负责同志和会员企业、个体工商户代表共 130 余人集齐聚一堂，集思广益、凝心聚力，共谋私个协高质量发展大计并对以北京亿赛通科技发展有限责任公司为首的 90 家私营企业予以表彰，授予“先进私营企业”称号。

此次评选表彰活动经过遴选推荐、初评初审、终审打分等流程，是对亿赛通近年来研发创新、高质量发展所取得成果的一次全面检验，也是对亿赛通多年以来推动区域经济发展所做贡献的高度肯定和鼓励。

在新型数字化背景及政策的支持和帮助下，亿赛通在技术创新、业务拓展、人才培养等方面不断强化提升，加强企业市场竞争力。积极帮助用户落实行业数据合规各项要求，并取得阶段性进展。公司主营产品的技术水平和市场占有率逐步增长，助力各行业高质量发展。

作为扎根数据安全领域的综合数据安全厂商，亿赛通将全面落实新发展理念，以技术创新为驱动，以安全管理为保障，以关键人才为支撑，各项工作全面协同赋能业务发展，全力打造以以专业的产品和服务为客户筑牢数据安全底座的产业生态，为实现成为“中国数据安全专家”的品牌战略目标不断奋斗，为加快建设数字中国贡献亿赛通力量，持续为数字经济发展蓄力赋能。

当前，数据作为数字经济时代的关键生产要素、国家基础战略性资源，数据改变生活的同时面临的安全问题也日益严峻，亿赛通提出了数据安全治理智能化技术体系，通过智能化分类分级工具快速准确地完成组织的业务梳理和数据梳理，并形成规范化的策略库，即主体、客体及两者之间的策略，同时将上述数据根据积累的知识库智能化衔接到技术平台，实现了对组织数据的智能识别、智能防护、智能监测、智能运营，构建可视、可控、可管、可溯的覆盖数据全生命周期的综合解决方案。

亿赛通会以本次表彰为契机，振奋精神、提升信心、争当先进、发挥作用，争做爱国敬业、守法经营、创业创新、回报社会的典范，为促进海淀区个体私营经济高质量发展和实现海淀区发展的战略目标做出新的更大贡献。

关于亿赛通

北京亿赛通科技发展有限责任公司成立于 2003 年，二十余年风雨兼程，已成功打造为数据安全领域专业的综合数据安全厂商，是国家双高新企业，并获得国家级“专精特新”小巨人企业认证。签约用户过万家、800 余万终端用户，连续多年获得 CCID、IDC、中国信通院等专业机构的高度认可。

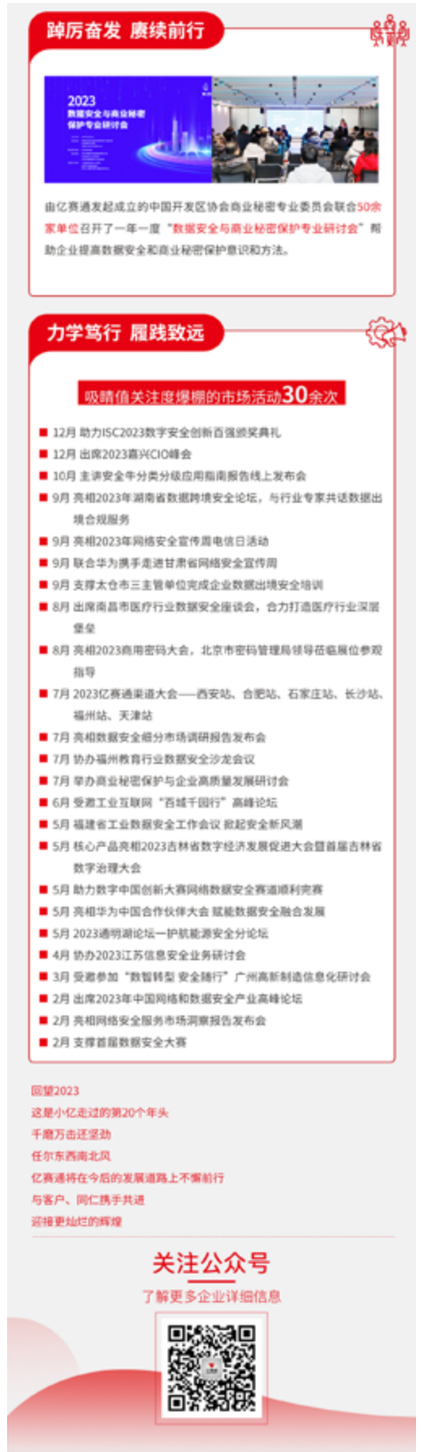
亿赛通针对数据全生命周期的多场景、高性能、智能化的安全治理需求，历经 20 余年的技术积累和上万个交付项目的沉淀，重点突破了端点数据自适应防护、海量数据内容审计、重要数据深度感知、敏感数据智能防护等关键技术，授权了 50 余项发明专利，达到了国际先进水平，提出了数据安全“分放管服”建设理念和数据安全治理智能化体系，自主研制了电子文档安全管理系统、数据泄露防护系统（含终端、网络、存储等）、API 审计系统、数据库审计系统、数据库防火墙、数据库运维系统、数据脱敏系统（含动态和静态）、数据交换系统及文件防火墙等，覆盖了“云网端”等场景，构建了数据安全运营管理平台、数据安全态势感知平台及数据安全智能管理平台等。

2023 年终大事记


2023
年终大事记
一夜荣华春秋意
年月回首却思量
亿赛通吹响年终冲锋号
2023成绩单高光来袭
一起回顾专属于我们的精彩瞬间
披荆斩棘 永攀高峰
1
重大签约项目
100+项
2
新增终端
100+万点
3
新签同比增长
11%
广东移动 重庆联通 电信国际 移动国际
农银人寿 重庆银行 江西银行 华泰证券
中国中化 中核工业 大唐集团 清华大学
宁德时代 一汽大众 中环领先 立臻科技
广联达 和记黄埔医药 江西省公安厅 重庆市公安局


前沿技术 匠心精神
修炼内功蓄力成长，全年完成20余款产品迭代和技术升级，只为给您更好的产品和服务
❶ 数据安全治理系列
新品发布-数据安全检查工具箱系统
技术升级-数据安全运营管理平台、数据分类分级系统
❷ 数据安全防护系列
新品发布-终端资产采集系统
技术升级-新一代电子文档安全管理系统、终端数据泄露防护系统、网络数据泄露防护系统、数据安全网关
❸ 数据安全流转系列
技术升级-数据交换系统、动态数据脱敏、静态数据脱敏
❹ 数据库安全系列
技术升级-数据库安全审计系统、数据库防火墙系统、数据库运维安全管理系统
标准报告 落地有声
落地国标 行标、团标 12项
参编 行业白皮书 13项
国家市场监督管理总局 国家标准化管理委员会 中国信通院、海淀中小企业协会 中国电子技术标准化研究院
中国信通院 中国电子技术标准化研究院 国家工业信息安全发展研究中心 世界互联网大会
IDC 入选 专业机构 5项
入选 权威媒体 7项
硬核实力 熠熠生辉
❶ 新增硬核实力证书50个
授权发明专利 24个
重要企业资质 26个
数据安全服务能力评定资格证书


❷ 新增荣誉奖项
企业/人物奖（11项）
① 北京市商业秘密保护示范点
② 北京市发明专利奖三等奖
③ 2023年数据安全服务前五家企业
④ 2023中关村高成长企业TOP100
⑤ 2022-2023年度数据安全服务领航企业
⑥ 2022-2023信息技术应用创新榜-数据安全信创领军企业
⑦ 2023行业信息技术应用先锋人物
⑧ 中国计算机行业协会数据安全专业委员会优秀成员单位
⑨ 黑龙江省网络安全协会优秀行业企业
⑩ 2023年中国网络安全与信息产业金智奖-创新企业奖
⑪ 第八届“海英”人才
产品奖（5项）
① 2023年CCF科技成果奖-科技进步三等奖——数据安全智能防护关键技术及应用
② 中国信通院数据安全共同体计划《数据安全产品名录》（数据泄露防护系统（网络型）V5.1、数据库防火墙系统V5.0、动态数据脱敏系统V5.0、数据库安全审计系统、安全管理平台V2.0、数据资产安全分析系统V1.0）
③ 2022年首届数据安全大赛 赛道二“数据安全产品能力-数据识别”钢奖
④ 喜获《2022年网络安全优秀评选》十大明星产品—数据安全运营管理平台
⑤ 获评IT市场年会2023年新一代信息技术创新产品奖—数据安全运营管理平台
解决方案奖（6项）
① 新奥集团荣获IOC CSO20大安全项目
② 华工集团荣获IOC CSO20大安全项目
③ 2023年网络安全服务阳光行动优秀应用案例
④ 2023中国数字化优秀方案集-信创篇案例征集
⑤ 2022-2023信息技术应用创新榜-信创卓越解决方案-网络数据泄露防护解决方案
⑥ 2023网络安全全明子年度评选-解决方案赛道第一名
安全牛15项
CCSIP 10项
数说安全6项
信通院2项
入选60+细分领域
2023年百强榜，排名逐年提升
安全牛34名、大众点评23名、ISC百强榜十强
春风化雨 孜孜不倦
1
7门
认证课程
2
50+位
高级讲师师资团队
3
2000+人
参与培训人数
亿赛通联合工信部人才交流中心、工信部教育考试中心、中国计算机行业协会数据安全专业委员会、市场监督管理总局认研中心成立数据安全培训学院。能力培训课程包括【《数据安全评估师》《数据安全工程师》《数据安全治理工程师》《数据安全运维工程师》《数据安全咨询师》《首席数据官》《商业秘密咨询师》】。
踔厉奋发 赓续前行
由亿赛通发起成立的中国开发区协会商业秘密专业委员会联合50余家单位召开了一年一度“数据安全与商业秘密保护专业研讨会”帮助企业提高数据安全和商业秘密保护意识和方法。


踔厉奋发 赓续前行
2023 数据安全与商业秘密保护专业研讨会
由亿赛通发起成立的中国开发区协会商业秘密专业委员会联合50余家单位召开了一年一度“数据安全与商业秘密保护专业研讨会”帮助企业提高数据安全和商业秘密保护意识和方法。
力学笃行 履践致远
吸睛值关注密集曝光的市场活动30余次
12月 助力ISC2023数字安全创新百强颁奖典礼
12月 出席2023嘉兴CIO峰会
10月 主讲安全牛分类分级应用指南报告线上发布会
9月 亮相2023年湖南省数据跨境安全论坛，与行业专家共话数据出境合规服务
9月 亮相2023年网络安全宣传周电信日活动
9月 联合华为携手走进甘肃省网络安全宣传周
9月 支撑太仓市三主管单位完成企业数据出境安全培训
8月 出席南昌市医疗行业数据安全座谈会，合力打造医疗行业深层堡垒
8月 亮相2023商用密码大会，北京市密码管理局领导莅临展位参观指导
7月 2023亿赛通渠道大会——西安站、合肥站、石家庄站、长沙站、福州站、天津站
7月 亮相数据安全细分市场调研报告发布会
7月 协办福州教育行业数据安全沙龙会议
7月 举办商业秘密保护与企业高质量发展研讨会
6月 受邀工业互联网“百城千园行”高峰论坛
5月 福建省工业数据安全工作会议 掀起安全新风潮
5月 核心产品亮相2023吉林省数字经济发展促进大会暨首届吉林省数字治理大会
5月 助力数字中国创新大赛网络数据安全赛道顺利完赛
5月 亮相华为中国合作伙伴大会 赋能数据安全融合发展
5月 2023通明湖论坛—护航能源安全分论坛
4月 协办2023江苏信息安全业务研讨会
3月 受邀参加“数智转型 安全随行”广州高新制造信息化研讨会
2月 出席2023年中国网络和数据安全产业高峰论坛
2月 亮相网络安全服务市场洞察报告发布会
2月 支撑首届数据安全大赛
回望2023
这是小亿走过的第20个年头
千磨万击还坚劲
任尔东西南北风
亿赛通将在今后的发展道路上不懈前行
与客户、同仁携手共进
迎接更灿烂的辉煌
关注公众号
了解更多企业详细信息

打造完善数据治理屏障，驱动数据安全流通

近日，国家数据局指出，推进数据要素市场化价值化，需关注顶层设计与实践探索相结合、数据基础设施、分配机制兼顾效率与公平、适应数据特点的安全治理模式等四方面的问题。

将数据作为生产要素，是我国首次提出的重大理论创新。国家数据局正在推进的重点工作之一，就是充分发挥数据的基础资源作用和创新引擎作用，不断做强做优做大我国数字经济。数据作为新型生产要素，是价值创造的重要源泉；构建以数据为关键要素的数字经济，是释放数据价值的关键动力；当前，为促进数据要素流通，还需要在制度建设、流通利用方式、安全治理等方面深化研究。

目前国内的数据安全治理现状借鉴了国际上的最佳实践和先进的理论模型。同时，中国也基于自身国情和发展需求，制定了适用于本国的数据安全理论和指导原则。如：数据安全风险管理体系、数据分类和标记、风险评估、数据生命周期管理等，已经形成自己的理论体系和标准。

在技术方面，我国积极发展数据安全技术。这包括数据加密技术、密码技术、安全存储和传输技术、数据脱敏和匿名化技术、数据分类分级、泄露防护技术等。同时，也在推动人工智能、区块链等前沿技术与数据安全的结合，以提升数据安全的能力和效果。

在产品政策方面，国家相关部门发布了一系列的数据安全法律法规，国家、地方、行业的多级标准和认证体系，促进了数据安全产品的开发和使用。这些产品涵盖了数据生命周期采集、存储、传输、处理、交换和销毁各个阶段，能够满足不同行业和组织的数据安全需求。

据亿赛通分析，对国内企业而言，用户通常需要处理和存储大量的数据，涉及多个利益相关方，建立合理的数据安全管理机制；并且缺乏专业数据安全人才，员工缺乏数据安全意识，影响数据安全的管理和保护；数据安全技术和威胁不断演进，企业需要持续应对技术的发展带来的不断变化的安全威胁。

那么这些问题又该如何解决呢？亿赛通认为需要综合考量分析，整个数据安全治理过程要从决策层到技术层，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，构建自上而下、全流程、可闭环的完整链条。

具体来讲，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层融合。

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，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， 提出了数据安全治理智能化技术体系，通过智能化分类分级工具快速准确地完成组织的业务梳理和数据梳理，并形成规范化的策略库，即主体、客体及两者之间的策略，同时将上述数据根据积累的知识库智能化衔接到技术平台，实现了对组织数据的智能识别、智能防护、智能监测、智能运营，构建可视、可控、可管、可溯的覆盖数据全生命周期的综合解决方案。

此外，当前数据安全治理是各方高度关注的问题。数据元素一旦被泄露或滥用，可能带来个人隐私、商业秘密等数据泄露问题，影响隐私保护、产业发展，甚至可能对国家安全带来挑战。亿赛通持续帮助用户以合适的安全成本，实现良好的防护效益，助力企业提升数据安全管理能力，构建兼顾活力与秩序的数字治理体系。

解决方案 | 大数据局数据安全防护新思考

近年来，在国家引导和技术驱动下，我国数字政府迅猛发展，以政务大数据为核心的“数字政府”已成为“数字中国”建设的重要组成部分。政务大数据为提升政务服务水平和社会运行效率、促进释放市场活力提供了创新“原材料”。目前国家数据局正式揭牌，数据的重要性更为凸显，作为重要资产，在成为发展新动能的同时，也带来了巨大风险。数据安全、隐私保护乃至信息基础设施均面临新威胁与新风险，数据窃取、数据干涉、非法侵入、间谍软件、身份盗窃、黑客攻击、网络犯罪和网络窃密等互联网安全事件频发 , 对大数据安全工作提出了新的要求。

随着《网络安全法》、《数据安全法》、《网络数据安全标准体系建设指南》以及《个人信息保护法》等一系列法规政策的出台，对政务大数据平台数据资源全生命周期的保护提出了更明确的要求，需要切实保障政务信息资源在开发利用、分享交换等过程中的数据安全。

大数据局作为政务数据管理的核心单位明确在开展数字政府体系建设中需加强数据安全保障体系建设，实现全网数据全生命周期安全的全面、统一、高效管控，解决敏感数据泄露问题，形成常态化数据安全评估与监督检查机制，实现数据安全能力的不断扩展、强大，满足大数据平台长期、持续性数据安全需求，确保安全合规与风险可管可控。

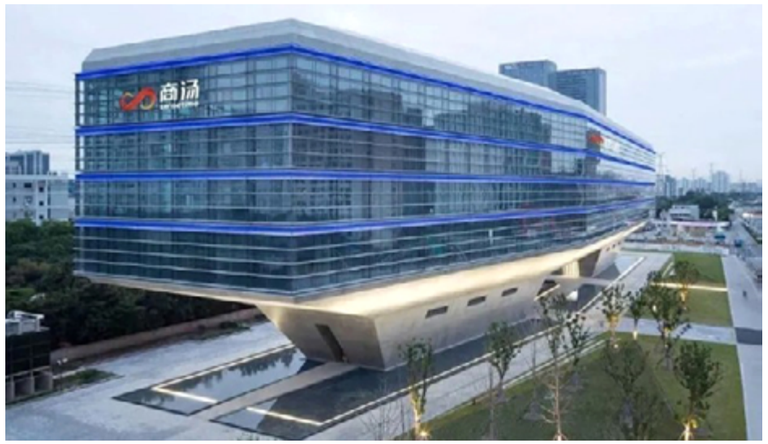
亿赛通认为大数据局数据安全也是对数据获取、存储、分析、演变、归档、销毁等全生命周期的数据进行识别、分类与分级，并关注不同环节的安全风险点。首先是数据咨询，即数据分类分级，基于分类分级结果配置差异化的安全策略和技术保障手段，从而兼顾数据有序流动与安全保障。数据分类分级工作既需要国家层面根据数据重要敏感程度建立相应的保护制度，又要求行方全面落实政务数据分类分级管理工作，落实主体责任“三步走”。

开展组织架构建设时，需要考虑大数据局组织层面实体的管理团队及执行团队，也要考虑虚拟的联动小组，组织架构从上到下各部门均需要参与其中。除了人员配置外，完善的数据安全技术框架能够为政务大数据安全提供可行性保障，大数据局在技术工具的布局与应用方面加强数据安全技术规划，防护布局由“点”向“面”趋势渐显。产品结合服务，将终端、数据库及文件服务器内的数据做梳理，完成结构化数据 + 非结构化数据安全管控。

在亿赛通技术体系中，技术层借助于数据安全运营管理平台，对大数据局核心资产、敏感数据进行识别定位，为后续针对关键数据和敏感数据的保护和治理工作提供明确目标; 开放底层能力对接可实现接入数据安全防护系统定位识别能力可实现合规和保护成果验证；运营层通过数据安全咨询服务，个性化定制分类分级规范及分级管控制度，完美展现产品 + 服务配置。

保护大数据局数据安全需要搭建统一的数据安全管理体系，通过分层建设、分级防护，达到平台能力及应用的可成长、可扩充，创造以数据为核心的安全管理体系框架。这也是全行业用户在数据安全进程中应具备的基本能力，亿赛通基于沉淀的治理经验和产品能力，提供更为专业、全栈的产品与服务，助力企业用户数据更安全！

上海商汤科技开发有限公司



客户简介

作为人工智能软件公司，商汤科技以“坚持原创，让 AI 引领人类进步”为使命，旨在持续引领人工智能前沿研究，持续打造更具拓展性更普惠的人工智能软件平台，推动经济、社会和人类的发展，并持续吸引及培养顶尖人才，共同塑造未来。 商汤科技拥有深厚的学术积累，并长期投入于原创技术研究，不断增强行业领先的多模态、多任务通用人工智能能力，涵盖感知智能、自然语言处理、决策智能、智能内容生成等关键技术领域，同时包含 AI 芯片、AI 传感器及 AI 算力基础设施在内的关键能力。

典型案例 TYPICAL CASES

需求背景

人工智能行业竞争激烈，产品更新迭代快，需要不断创新，销售策略不断改进。人员流动大的同时，竞争对手潜伏现象普遍。所以公司的战略规划、管理方法、商业模式、财务信息、投融资决策、产购销策略、资源储备、客户信息、招投标事项等经营信息容易被泄露。商汤在此大背景下，公开招标数据安全厂商，为其数据信息保驾护航。

解决方案

①满足数据合规要求：遵从《数据安全法》《信息安全技术网络安全等级保护基本要求》，全面提升安全内控、数据安全体系建设。

②数据分类分级管控：建立数据分类分级保护制度，实行人员定岗定级精细化数据安全管控。

③数据安全全面防护：从数据收集、存储、使用、加工、传输、提供、公开等实现全生命周期管理，对数据流通各环节进行安全防护。

④数据泄密审计追责：全面记录数据传播轨迹、终端异常操作行为，对重要数据资产的解密、外发、打印等详细审计。

⑤日常网络检测：网络 DLP 产品部署完成后，会对经过系统的网络流量进行 7 层协议分析，分析粒度达到内容级，在分析过程中实现对网络协议数据的内容敏感性匹配，满足内容级审计需求。审计数据长期保存，支持对数据的浏览，查看，统计分析，趋势分析，报表生成等。

项目成果

亿赛通的部署使得商汤科技内部文件可以在所有涉密终端上无障碍流转，如需将文件发送到第三方公司必须由本部门文档管理员解密，并且对于每天大批量的数据文件需要委托给第三方，在发送前将电子文件转化成外发加密文件，从而保障数据文件不会被第三方公司泄密，确保了商汤科技所有数据管理有序、安全运行。

上海小牛互娱智能科技有限公司

客户简介

上海小牛互娱智能科技有限公司创立于 2018 年 7 月，是一家专注于创新技术发展的移动互联网科技公司。小牛互娱致力于成为中国互娱产业领导者，目前公司已经在应用工具、游戏运营、游戏研发等领域布局，每天都有千万级用户通过小牛互娱旗下的各类产品获取内容与服务。公司的核心团队由来自腾讯、阿里、网易等互联网巨头的产品及技术专家组成。在核心团队的带领下，公司利用自身的技术优势和买量发行能力，不断推出符合市场需求的优质互联网产品，深耕互联网行业。

典型案例 TYPICAL CASES

需求背景

在国内，因互联网公司引发的种种信息泄露隐患，加剧了数据安全问题的恶性影响力。小牛互娱中保存了大量游戏账号、个人隐私的详细信息，极易变成不法分子的攻击对象。小牛互娱为避免企业内部业务流转存在漏洞，提高企业各环节的数据安全防范能力，开展数据安全体系建设工作。

解决方案

①数据资产发现：自动收集用户数据资产信息，自动收集用户历史操作文件信息。

②用户行为监控：通过对用户操作行为的监控，可以直观和准确确定用户行为威胁。

③用户行为分析：通过 UEBA、数据关联分析等技术结合，自动识别用户异常风险，并进行预警。

④数据追踪溯源：实现数据可视化展示，分析数据流转的全生命周期流转过程。

⑤数据安全分析：利用可视化数据平台，展示用户数据资产流向、资产地图、风险行为帮助企业立体全面了解内部风险态势。

项目成果

与亿赛通合作后，小牛互娱对游戏图纸、账号信息等企业重要资料进行行为监控、人员访问权限管控、用户行为分析等获得更高级别的安全保障，实现核心数据资产的有效积累和流转。同时，部门间的资料共享、汇总分发等协同工作效率也将得到极大提升。