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

07 月刊

2023 年共 12 期

亿赛通企业月刊　　中国数据安全专家　　www.esafenet.com

聚焦投融会 | 亿赛通赋能企业数据安全建设，展示专家风采

亿赛通实力入选嘶吼《时维鹰扬·履践致远 数据安全细分市场调研报告》

亿赛通助力《商业秘密保护与企业高质量发展研讨会》顺利召开，破局行业数据安全新挑战

全面开花 | 亿赛通入选《嘶吼 2023 网络安全产业图谱》23 项细分领域

亿赛通助力某新能源车企打造综合数据安全解决方案，进一步加强企业安全保障能力

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

刊首语 PREFACE

《亿赛通七月刊》全新上线，重点关注企业级数据安全治理

随着新兴技术和人类生产生活交汇融合，各类数据迅猛增长、海量聚集，对数字经济发展、人民生活产生了重大而深刻的影响。数据安全已成为事关国家安全与经济社会发展的重大问题。据 IBM Security 发布的年度《数据泄露成本报告》显示，2023 全球数据泄露的平均成本达到 445 万美元，创该报告有史以来以来最高记录，这表明，企业应对的安全环境变得更加复杂。从泄露成本和政策发展看出，未来几年，数据安全治理是企业重点关注的内容。亿赛通数据安全治理体系从决策层到技术层，从管理制度到工具支撑，自上而下贯穿整个组织架构的完整链条。跟随《亿赛通七月刊》学习数据安全的必备技能—数据安全治理。

国内

1、某科技公司未履行数据安全保护义务 导致存在数据泄露风险隐患被处罚

摘要：2022 年 3 月，广州警方工作发现，广州某科技公司向各地驾校提供的某驾培平台储存处理了驾校培训学员的姓名、证件号、手机号、个人照片等公民个人信息数据被挂在外网售卖。经查，该公司没有建立数据安全管理制度和操作规程，对采集到的个人信息未采取去标识化和加密措施，且系统存在未授权访问漏洞，未落实网络安全等级保护制度，存在数据泄露的重大风险隐患，违反《数据安全法》第二十七条之规定。广州警方依据《数据安全法》第四十五条第一款规定，对该公司作出警告并处罚款人民币 5 万元，该案是广东省首宗适用《数据安全法》进行执法的行政案件。

2、某公司信息系统仅备案未按规定开展等级保护测评被处罚

摘要：广州警方在工作中发现，广州某教育科技有限公司运营使用的“某在线 1 对 1 系统”确定为第二级信息系统，且在 2021 年 7 月到公安机关进行了网络安全等级保护备案。但该系统上线运行前及运行之后，广州某教育科技有限公司一直未按规定对系统的安全等级状况开展等级保护测评，未充分落实网络安全等级保护制度，未履行网络安全保护义务，违反了《广东省计算机信息系统安全保护条例》第十二条之规定。根据《广东省计算机信息系统安全保护条例》第四十条第一款第（二）项之规定，广州警方对该公司作出行政处罚，并责令其限期改正。

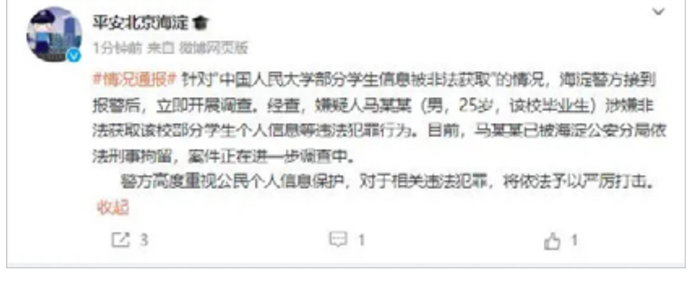
3、一次性至少上传 21 张个人多角度照片 用户担心隐私泄露

摘要：7 月 24 日，记者进入某小程序尝试制作 AI 照片，点击“制作数字分身”后被要求上传一张正面照与 20 张多个角度、表情的照片，记者测试发现，这款小程序需要用户至少上传 21 张个人照片，包括 1 张“五官清晰的正面照片”和 20 张“多光线、多背景、多视角、多表情”的半身照，总共需要 21 张照片。对此，有用户表示，使用这款小程序最担心的就是自己的隐私安全，上传这么多照片，如何储存、使用，以及后期如何处理都待解决。

4、宝坻区委网信办组织开展村务公开个人信息泄露专项治理行动

摘要：日前，宝坻区委网信办组织召开了专项治理行动工作部署会，印发了《宝坻区村务公开个人信息泄露专项治理行动工作方案》，周密部署了行动时间、排查范围和治理任务，逐项细化了责任单位职责分工，要求各单位加强领导、精心组织、强化联动，从提高思想认识、完善审核制度、强化日常监督等方面入手，切实维护公民个人信息合法权益。

5、刑拘！人大学生信息泄露事件，警方通报



摘要：针对“中国人民大学部分学生信息被非法获取”的情况，海淀警方接到报警后，立即开展调查。经查，嫌疑人马某某（男，25 岁，该校毕业生）涉嫌非法获取该校部分学生个人信息等违法犯罪行为。目前，马某某已被海淀公安分局依法刑事拘留，案件正在进一步调查中。

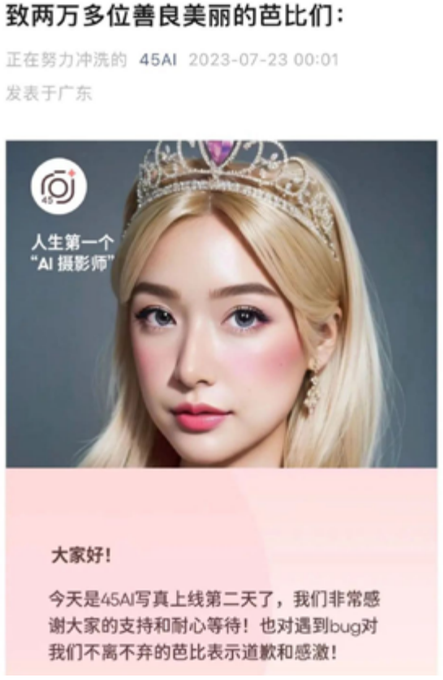
6、还有多少学生个人信息在泄露？

摘要：近日，有媒体梳理了近三年 52 份学生个人信息泄露的相关裁判文书发现，高校学生信息泄露已相当严重。这些个人信息的单价极为低廉，有不法分子仅花费 1 千元就买到 18 万条学生信息，这意味着约等于只花 1 元就可以买到 200 个人的信息。学生信息失窃的成本低的可怕。

7、“代理退保”套路深 “专业培训”别当真

摘要：近期，福建省福州市连江县人民法院判决 6 名涉“代理退保”黑产不法人员犯“敲诈勒索罪”。经调查，涉案人员通过设立信息咨询公司，借助微信、抖音等网络平台发布“可全额退保”的信息，诱导保险投保人委托该公司退保，以杜撰保险公司违规行为的方式编写投诉信，向监管部门恶意投诉保险公司，诈骗钱财。

8、上万网友排队当芭比公主？紧急提醒



摘要：近日，随着《芭比》真人电影的上映，可以生成芭比写真的小程序，在网络走红。该小程序上传的照片可能会因网络攻击或者计算机病毒及木马程序而导致信息泄露。软件使用过程中如果是用户上传本人照片，则视为用户同意软件使用其个人照片，但是软件在使用该等照片并生成“芭比写真”作品后应当及时删除照片素材。如果要存储搜集照片，则需要另行征得上传人同意。

9、逾 12 万条个人信息泄露，竟是“熟人”作案?

摘要：据广东省阳江市公安局消息，7 月 4 日，在广东省公安厅网警总队的指导下，阳江警方侦破一宗侵犯公民个人信息案，打掉一个涉及物业、装修公司、建材家居等多行业的侵犯公民个人信息犯罪团伙，累计抓获犯罪嫌疑人 25 名，涉及公民个人信息逾 12 万条。当日缴获手机 40 部、电脑 6 台和其他作案工具一批。

10、早教机构泄露信息？家长频接诈骗电话后怒了：全家情况摸得清清楚楚

摘要：7 月 18 日，长沙市民王先生向记者反映，他的个人信息遭泄露，高度怀疑是从培训机构泄露而出。王先生说，之所以产生这样的怀疑，是因为他在为孩子报名培训机构时，留下的是他老婆的名字和自己的电话。而诈骗电话多次以该机构名义打来，称机构倒闭，家长可办理退费事宜。“打过来的那个电话里，喊的是我老婆名字。”7 月 18 日，晨意帮忙记者联系了金宝贝儿童多元成长中心（长沙富兴中心）。该机构负责人介绍，机构正常经营，暂未接到其他家长反映相关情况。他将进一步了解相关情况，如属实，将做处理。

国外

1、OpenAI 被韩国隐私监管机构罚款，因未及时报告 ChatGPT 泄露用户信息

摘要：7 月 27 日消息，韩国个人信息保护委员会 (PIPC) 周四表示，对 ChatGPT 的运营商 OpenAI 处以 360 万韩元（约 2829 美元）的罚款。今年 3 月，ChatGPT 上的一个开源库出现了一个现已修补的 bug，造成了一个缓存问题，导致 ChatGPT Plus 用户在 9 个小时的窗口内的支付信息在无意中可见，包括姓名、电子邮件地址、信用卡号码的后四位数字和信用卡过期日期。韩国共有 687 名用户被证实受到影响。韩国个人信息保护委员会表示，OpenAI 违反了在发现信息泄漏后 24 小时内向当局报告的义务，因此对其进行了罚款。

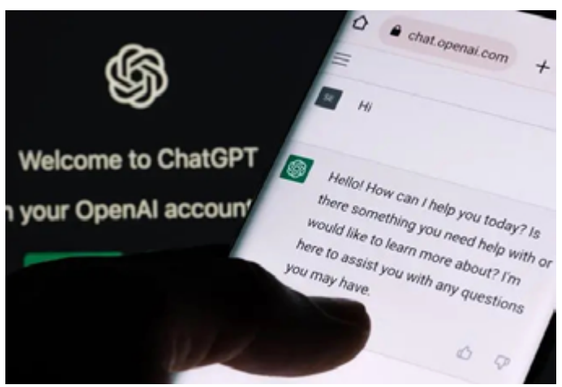
2、IBM：2023 全球数据泄露的平均成本达到 445 万美元 创该报告有史以来以来最高记录

摘要：IBM Security 发布的年度《数据泄露成本报告》显示，2023 全球数据泄露的平均成本达到 445 万美元，创该报告有史以来以来最高记录，也较过去 3 年均值增长了 15%。同一时期内，检测安全漏洞和漏洞恶化带来的安全成本上升了 42%，占安全漏洞总成本的比值也来到史上最高，这也表明，企业应对漏洞的调查和处理正在变得更加复杂。

3、日本现“山寨”政府 App，用户安装后将面临数据泄露风险

摘要：安全公司在日本发现了一系列 SpyNote 恶意木马攻击行动，这些攻击行为专注于安卓用户，黑客发送一系列不同名义的钓鱼邮件，促使用户安装上各种“山寨”政府 App，在安装上后，用户的缴费将被侵吞，还将面临数据泄露的风险。

4、美国 FTC 对 OpenAI 展开全面调查，涉及 ChatGPT 泄露数据、编造答案



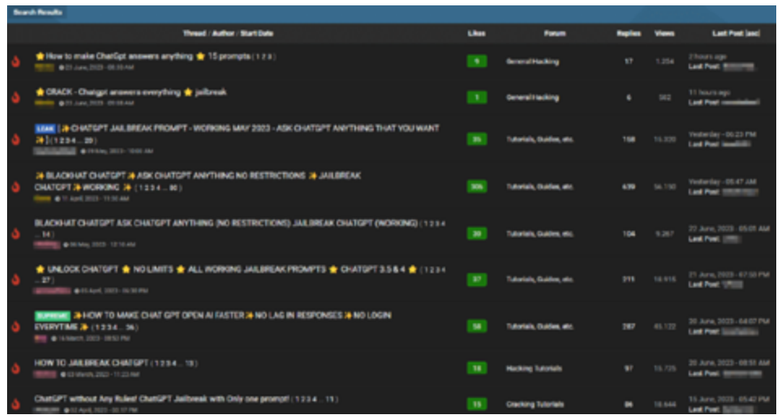
摘要：7 月 13 日消息，据华盛顿邮报报道，美国联邦贸易委员会（FTC）近日对总部位于旧金山的公司 OpenAI 展开了全面调查，原因是该公司开发的流行聊天机器人 ChatGPT 可能违反了消费者保护法，将个人声誉和数据置于危险之中。

5、上千个 Docker hub 镜像泄露认证密钥和私钥

	Domain	Regular Expressions (Section 5.1.1 / Appendix C) Potential Threat / (Service) Type	(Distinct) Matches (Sec. 5.1.2) Images	Variables	Valid Secrets (Section 5.1.3) Images	Variables	Total
	Private Key	Perform man-in-the-middle attacks, fake identity, …	1,377,336	2	52,107	0	52,107
		PEM Private Key, PEM Private Key Block, PEM PKCS7, XML Private Key	(62,282)	(1)			
API	Cloud	Manage services, create new API keys, reconfigure DNS, access emails / SMS, control voice calls, read / alter private repositories, … *Alibaba[76], Amazon AWS[58], Azure[76], DigitalOcean[76], Github[76], Gitlab (v4, v2)[76], Google Cloud[76], Google Services[58], Heroku[76], IBM Cloud Identity Service[76], Login Radius[76], MailChimp[58], MailGun[58], Microsoft Teams[76], Netlify[76], Twilio[58]*	6,208,995 (74,460)	416 (84)	2,880	67	2,920
	Financial	List / perform payments, inspect / alter invoices, … *Amazon MWS[58], Bitfinex[76], Coinbase[76], Currency Cloud[76], Paydirekt[76], Paymill[76], Paymonge[76], Paypal Braintree[58], Picatic[58], Stripe[58], Square[58], Ticketmaster[76], WePay[76]*	42,901 (543)	4 (2)	23	2	25
	Social Media	Tweet, access direct messages, retrieve relationships, … *Facebook[76], [58], Twitter[58]*	6,365,854 (439,822)	14 (8)	209	4	213
	IoT	Retrieve (privacy-sensitive) IoT data, e.g., track cars, … *Accuweather[76], Adafruit IO[76], OpenUV[76], Tomtom[76]*	297 (117)	0 (0)	0	0	0

摘要：近日，德国亚琛工业大学 (RWTH-Aachen University) 研究人员发现上千个 Docker Hub 上的镜像暴露了机密密钥、软件、在线平台和用户。研究人员分析了 Docker Hub 中 337171 个镜像，聚集了 1647300 层的数据集，发现有 8.5% 的镜像（28621 个 Docker 镜像）中包含敏感数据，包括 52107 个有效的私有密钥、3158 个不同 API 秘密信息。注：以上数据不包括测试密钥、示例 API 秘密和无效的匹配。

6、WormGPT：生成式 AI 被用于发起商业邮件攻击



摘要：近日，在某犯罪论坛出现了上图所示的讨论帖。其中展示了利用生成式人工智能技术应用于钓鱼攻击或 BEC 攻击的可行性。帖子建议邮件使用受害者的本地语言、翻译、然后再反馈给 ChatGPT 这样的接口以增强其复杂性和形式化。该方法表明攻击者即使不熟悉受害者的语言，也可以进行钓鱼或 BEC 攻击。

7、伊朗黑客盯上核安全专家，短短一周内将 Windows 感染链移植到了 Mac

摘要：新的研究表明，威胁分子可以灵活地快速迭代攻击模式，以绕过安全控制措施。安全公司 Proofpoint 对最近一起针对美国一家智库的核安全专家的攻击进行了调查，揭示了资源丰富的攻击者如何迅速改变花招以攻击不同的机器。在意识到最初的攻击载荷无法在 Mac 上奏效后，威胁分子迅速转而采用已知攻击使用苹果硬件的目标奏效的新技术。在这起复杂的行动中，技术娴熟的威胁分子针对一个重要目标设计了一条看似无害的电子邮件链，并在数周内保持联络，以建立信任和融洽关系，然后趁机发动进一步的攻击。

8、被大肆利用的漏洞导致数百个太阳能发电站面临威胁

摘要：太阳能发电厂内数百个暴露在互联网上的设备仍然没有针对一个被大肆利用的严重漏洞打上补丁，该漏洞使得远程攻击者轻而易举就能破坏设施运行或在设施内潜伏下来。这种设备由日本大阪的康泰克（Contec）公司销售，冠以 SolarView 品牌，可以帮助太阳能发电厂内的人员监测产生、储存和分配的电量。康泰克示，大约 3 万个发电站已经引入了这种设备，这些设备根据发电站的规模和使用的设备类型有不同的包装。

9、CryptoClippy 恶意软件窃取葡语用户的加密货币

摘要：Unit 42 最近发现了一个针对葡语用户的恶意软件活动，旨在将加密货币从合法用户的钱包中转移到由攻击者控制的钱包中，该活动使用了一种被称为 CryptoClippy（加密货币剪辑器）的恶意软件，它可以监控受害者的剪贴板，寻找加密货币钱包地址被复制的踪迹，以此来发起攻击并窃取加密货币。

10、芯片巨头台积电面临勒索风波！

摘要：近期，苹果最大的半导体供应商之一台积电将一起数据泄露事件归咎于一家第三方 IT 硬件供应商，这起数据泄露事件导致台积电面临 LockBit 勒索软件团伙索要的 7000 万美元赎金。台积电在通过电子邮件发给安全外媒 Dark Reading 的一份声明中证实了有关这起安全事件的多方报道，但没有表明 LockBit 勒索软件团伙具体访问了其系统中的哪些数据、因此劫持这些数据以索要赎金。不过声明称，这起事件并不影响台积电的业务或客户信息。

聚焦投融会 | 亿赛通赋能企业数据安全建设，展示专家风采

2023 年 7 月 2 日，第十届中国中小企业投融资交易会（以下简称“投融会”）在北京亦创国际会展中心 A 馆盛大开幕。投融会由中国中小企业协会、中国银行业协会、中国期货业协会、中关村发展集团、北京经济技术开发区管理委员会等行业协会、机构联合举办，北京市经济和信息化局协办。本届投融会以“金融活水精准滴灌 专精特新提质增量”为主题，以“搭平台、促交易”为目的，搭建了中小企业与地方政府、金融机构之间的产融结合平台。亿赛通作为国家级“专精特新”小巨人企业，受主办方邀请出席展览并重点展示企业级全生命周期综合数据安全建设方案。

本届投融会展览面积近一万平方米，主要参展机构包括金融机构、地方政府、专精特新企业参与展示，吸引大量中小企业前往洽谈咨询。

数字经济时代，世界百年未有之大变局，新趋势、新机遇、新挑战、新生态、新基建 ... 万象更新，数据安全同样面临着新目标、新需求。国家对“专精特新”企业的要求是新颖化，而亿赛通的技术创新、研发实力、产品性能、服务水平、市场竞争优势、发展前景、综合实力等方面在业内一直保持高水准。公司在数据安全领域深耕 20 年，企业从成立之初就下决心始终专注在这一领域。得益于集“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”于一体的全生命周期防护能力，使我司能够长久的保持生命力和活力，并通过融合行业的需求变化，为用户提供更全方位的综合数据安全解决方案。

并且，亿赛通前瞻性的提出“分放管服”数据安全建设理念，在激烈的行业竞争中脱颖而出，形成了自己的主体特色，在理念的基础上，不遗余力地加大研发投入，保持高度自我迭代和进化。

亿赛通“分放管服”数据安全建设理念

目前亿赛通经过大量的设计、修改和优化，产品已经实现了质的飞跃，企业的数据安全建设必然是从孤立的数据安全产品过渡到体系化能力建设，需要通过一个高度集中化的平台实现数据安全能力的体系化集成，统一汇集围绕数据的资产管理、流动监测、风险分析、事件溯源、风险评估能力，实现合规有序、有效保护、高效运营的数据安全体系构建。

亿赛通将基础数据安全的能力集成在一个平台，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，实现数据安全的闭环管控。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。

在未来的工作中，亿赛通将始终专精于数据安全的建设，在理念、产品和安全的创新方面保持高度自我迭代，推进企业数字化转型，为建设数字强国贡献力量。

亿赛通实力入选嘶吼《时维鹰扬·履践致远 数据安全细分市场调研报告》

2023 年 7 月 4 日，嘶吼安全产业研究院权威发布了“时维鹰扬·履践致远数据安全细分市场调研报告（以下简称《报告》）”。《报告》在数据安全产业变革的关键期，聚焦行业重要领域，通过对行业及安全厂商的整体分析，深挖数据安全的真实发展情况，为资方和甲方提供细节参考。亿赛通基于数据安全领域 20 年方法论及实施经验，入选《报告》多项领域重点推荐厂商。

在实现网络强国的重要思想背景下，我国高度重视、大力推进网络安全和信息化工作，并明确指出，网络安全是实现网络强国战略的四梁八柱之一，网络安全服务业则是网络安全事业前行的基础，为网络强国目标提供技术、人才、资源的支撑。

根据嘶吼安全产业研究院调研数据显示，2022 年数据安全产业市场规模突破 100 亿元，高达 102 亿元，同比增长 15%。数据安全从探索期到启动期，目前已迈入蓬勃期，预计 2029 年实现转折节点。

在数据安全领域，亿赛通凭借业内的良好口碑及客户高认知度，顺利入选报告数据防泄漏、数据脱敏、数据加密、数字水印、数据流动安全、数据访问控制、安全网关、数据交换系统、数据跨境安全检查、数据资产管理平台、态势感知平台、数据安全体系建设、数据安全能力评估、数据库审计、数据库运维安全、数据库防火墙、文件管理与加密、数据泄密溯源取证、数据安全合规、安全人才培养、个人数据隐私等 21 个细分领域。

其中，数据防泄漏、数据资产管理平台、态势感知平台、数据安全体系建设、数据库审计、数据泄密溯源取证、文件管理与加密等领域获得嘶吼重点厂商产品推荐。

在《报告》发布会中，亿赛通专家分享了《企业级数据泄露防护解决方案》主题演讲。在国家政策的支持及约束下，数据安全产业的发展态势日盛，传统安全服务商、专业数据安全服务商层出不穷，产品细分和应用也越来越多，与业务的结合也越发紧密。而数据安全防护在企业的正常运行中起着至关重要的作用。

在亿赛通看来，企业数据安全风险，“内忧”已远远高于“外患”！数据安全防护是平衡利用和保护之间的重要依据之一。近两年，五法一典的推进，让数据安全由“或有”变“刚需”。仅 2022 年，就有共 242 份文件为数据安全工作指明了方向。

从应用场景来看，数据泄露防护分为终端、网络、邮件、存储等场景。随着企业需求的变化，目前甲方视角更多的集中在体系化、集成化产品，避免数据孤岛情况的出现。亿赛通通过数据泄露防护产品的系列组合，综合梳理用户数据，跟踪记录用户行为，集被动审计和主动预防于一体，帮助用户将每一次数据活动与实际用户、设备和应用程序进行关联、监管、审计、识别、记录、溯源，精准识别流动数据是否在被合法使用，以实现数据安全防护价值，建立数据安全防护体系。

以某电力公司项目为例，由于能源行业发展信息化、智能化水平全面提升，电力公司保密工作的对象、内容和

形势、任务发生了深刻变化，面临严峻考验。在这样一个形势下，需要一套有效的平台化数据安全体系，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、消除失泄密事件的发生，确保企业秘密和电网运行安全。

客户需求

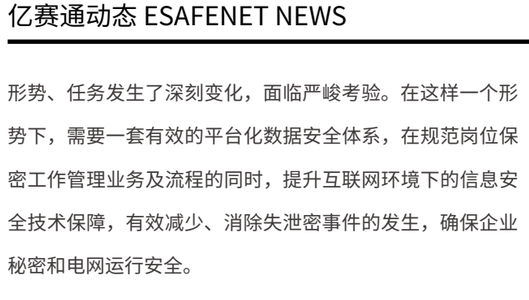
1. 敏感数据管理不足，没有良好的数据梳理，缺乏合规性评审；

2. 风险行为监控不足，内部人员较多，存在日常越权访问、下载和篡改数据等违规操作难以定位和发现；

3. 业务部门日常工作需要与保密相结合，建设保密制度体系，形成完整闭环；

4. 运维人员需要按操作规范或既定方案进行运维操作、非法导出敏感数据、操作行为进行细粒度的审计记录等；

5. 工作资料的存储和传输为明文传输、容易产生数据泄露、篡改。



解决方案

• 涉密文件违规存储管控

通过灵活配置扫描策略，适配内部环境，通过全方位扫描，准确识别涉密数据文件，精确定位。

• 敏感信息发现与管控

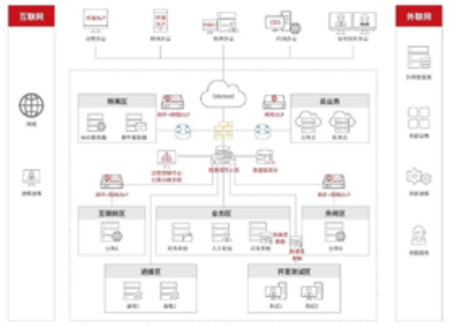
对通过 IM 工具、网络、邮件、网盘等可能造成泄密的外发或上传行为进行实时防护，防护措施包括审计、阻断、告警等，有效阻止数据资产外泄，对企业数据资产进行实时防护，解决无法控制数据资产外泄的困扰。实现平台数据纵向级联，保障省市县三级岗位和业务流程中敏感文件全生命周期智能保密安全防控。

• 风险动态实时监测

省公司统一部署，市县部署监测终端。实时审计用户操作行为，生成敏感信息全生命周期日志记录，动态绘制风险热点地图，为评估风险防控重点提供精确数据支撑。

• 文件自动授权加密

与内网邮件、即时通讯进行深度集成，实现敏感文件自动授权密文传输，防止文件越权查阅。实现对员工日常办公的智能化管控，自动根据规则实现涉密文件的标密、预警、拦截、解密等工作，克服员工对日常保密工作的恐惧，减轻员工工作压力，有效提高员工工作效率。



亿赛通围绕新一代数据防泄露产品强化创新，通过网络、终端、邮件、存储扫描防泄露的一体化管理，构建全面防护屏障，对受控区域内的数据文档进行深度解析、内容还原和敏感数据扫描，及时发现受控区域内通过各类途径泄露数据、传播数据的行为，并进行拦截、告警、审计等措施，保护核心数据不外泄。该项目为银行的数据安全防护建设提供了一个完整、可落地的综合解决方案。

未来，数据安全防护将更加侧重国产化和一体化。亿赛通新一代数据泄露防护系统将国产 DLP 提升到一个全新的高度，即通过“人”与“技术”让安全防护更便捷，帮助企业构建安全有序的数据使用环境，为企业安全赋能。

文章部分内容来源于《报告》

亿赛通助力《商业秘密保护与企业高质量发展研讨会》顺利召开，破局行业数据安全新挑战

当前，我国已转向高质量发展阶段，发展动力从主要依靠资源和低成本劳动力等要素投入转向创新驱动。企业是创新的主体。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。然而，我国企业间商业秘密侵权纠纷多发频发，逐渐成为市场竞争新的矛盾焦点。相比西方发达国家，我国商业秘密保护工作整体起步较晚，制度体系尚不完善，尤其是针对不同行业不同领域的商业秘密保护规则、指引、标准仍有欠缺，因此继续尽快完善相关制度规范和标准体系，对行业健康发展进行引导。

2023 年 7 月 25 日下午，在北京市海淀区市场监管局指导下，亿赛通深入参与并支持由北京海淀中小企业协会、中关村海新联新兴产业促进会主办，北京实创科技投资有限公司、北京京成知识产权研究院、中国开发区协会商业秘密保护专委会协办的商业秘密保护与企业高质量发展研讨会暨《中小企业商业秘密保护规范》团体标准启动会。北京市海淀区市场监管局公平竞争科科长周晔，中关村海新联新兴产业促进会会长肖航出席会议并致辞。

亿赛通作为《中小企业商业秘密保护规范》团体标准的主笔单位，拟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。《中华人民共和国反不正当竞争法》明确规定了商业秘密是指不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息。《中小企业商业秘密保护规范》团体标准的制定，对于维护正常的市场竞争秩序，促进社会主义市场经济的健康发展具有重要意义。

启动仪式

《中小企业商业秘密保护规范》团体标准启动环节合影

启动仪式环节，北京市海淀区市场监管局公平竞争科科长 周晔、中国科学院科技战略咨询研究院、中国科学院大学公共政策与管理学院教授刘海波、北京亿赛通科技发展有限责任公司董事长崔培升、北京和隆优化科技股份有限公司总经理王晓峰、 中科星睿科技（北京）有限公司总经理区东、北京航星永志科技有限公司总经理郭彦军、北京中永律师事务所高级合伙人侯成训和中关村海新联新兴产业促进会会长肖航共同按下标准启动按钮，正式启动标准的研制工作。随后《中小企业商业秘密保护规范》团体标准参编单位和与会企业代表合影留念。

圆桌会谈

圆桌会谈环节，由北京京成知识产权研究院名誉院长谷永久主持，各界大咖齐聚一堂，共同探讨商业秘密与知识产权保护。

亿赛通董事长崔培升表示，企业侧共通的问题一是缺乏对商业秘密与知识产权保护的防范意识，二是缺少关键技术防护手段，三是缺少数据安全专业型人才，导致知识产权侵权和企业核心秘密泄露风险的发生，因此有必要建立一套标准、形成一套方法，帮助企业建立完整的数据安全防护及商业秘密保护体系。同时阐述了亿赛通的制度和体系双闭环理念，提出建立有效的技术防护手段是对企业安全意识逐渐强化、培养的过程。作为行业内深耕多年的综合数据安全解决方案厂商，亿赛通希望运用自身的技术实力及科研优势，助力企业逐步建立完善的商业秘密保护体系，建立公平公正的营商环境。

北京亿赛通科技发展有限责任公司董事长崔培升主旨发言

在主旨发言阶段，中国科学院科技战略咨询研究院、中国科学院大学公共政策与管理学院刘海波、中伦律师事务所的张鹏律师、北京亿赛通科技发展有限责任公司宋春岭、北京亿赛通科技发展有限责任公司专家分别进行了商业秘密保护相关主题分享。刘海波教授在《商业秘密保护与企业经营发展》的主旨发言提倡“商号、商业秘密、商标”是企业的经营基础，商秘是基础的基础，商秘管理要系统部署、全面落实，在经营战略指引下，如何做好创新的商秘化、权利化、和公开化等问题引起了企业家的共鸣和思考；张鹏律师强调保护自身商业秘密的合规体系建设与防止侵犯他人商业秘密的合规体系建设是商业秘密合规的两个面向，对于企业同等重要，不可偏颇；亿赛通宋春岭阐述“分·放·管·服”数据安全建设理念 V2.0，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，保护企业商业秘密和知识产权，引起各企业的关注。亿赛通作为标准的主笔单位，由专家代表标准研制组，对标准研制背景、标准主要内容和标准编制情况进行介绍，并汇报了会议前收到的修改意见以及预处理情况。

《中小企业商业秘密保护规范》团体标准启动会合影

亿赛通是一家致力于数据安全的服务厂商，对政企、能源、金融、通讯、教育、医疗、制造、互联网等行业用户，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、云数据等场景进行全方位多维度管理。我司提出的“分放管服”数据安全建设理念，以“数据和人”为对象构建的数据治理、防护、流转、运营的双闭环体系，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。

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！

重磅出新 | 亿赛通数据库安全审计系统版本升级！

亿赛通数据库安全审计系统版本升级

亿赛通数据库安全审计系统结合多年数据安全领域的技术积累，以及十余个细分行业下各种应用场景实践，经过多次打磨，其版本于近日更新升级。产品于新版本中在扩大了审计防护范围并增强了审计能力的同时，还新增了数据资产管理与数据风险评估能力，安全复合能力的加入能更好的保护数据资产安全，为数据库安全保驾护航。

亿赛通数据库安全审计系统是一款基于数据库协议解析和 SQL 语句还原技术的数据安全产品。可对数据库访问行为进行监控和审计，并对其中危险操作向管理员实时告警提醒。同时，对数据库历史访问行为记录进行多维度统计分析，利用丰富图表进行可视化展示。

新版本亮点

1. 扩充审计类型，增强加密审计能力

新增对 HDFS、Flink、Spark、GoldenDB、TiDB、Solr 等数据库类型审计能力。

增加 MongoDB、PostgreSQL、Hive、Impala 、Inceptor 等加密流量审计能力。

2. 完善审计规则，丰富内置分析报表

新增针对事件序列特征的高级攻击的组合审计检测规则。

新增规则命中分析报告、会话分析报告、失败会话分析报告等内置报表。

3. 管理数据资产，支持数据风险评估

支持数据库扫描以及数据自动分类分级，对不同级别的数据设置对应的保护措施。

支持数据库监控以及风险检测，支持数据库漏洞扫描并提供数据库安全加固建议。

产品价值

1. 满足合规要求

支撑等保二级、三级建设要求，支撑数据安全风险检测建设要求。保障身份标识唯一性识别、非法登录权限管理、数据安全风险检测等安全建设需求的落地。

2. 提高监管能力

准确展示、汇报数据库访问情况、安全风险和执行效率，方便管理和掌控数据库运行情况，提高数据库安全监管能力。

3. 加快响应速度

实时记录、分析和统计数据库访问行为和安全风险，方便管理员在数据库安全事件发生后第一时间采取管控措施，加快对数据库安全事件的响应速度。

4. 解决追责难题

准确的应用用户关联优势，切实、有效地解决了三层数据库部署环境中，安全事件发生后精准定位、追责到人的难题。

产品优势

1. 全面记录访问行为与敏感数据

数据库协议精细解析与专业的 SQL 语法、词法分析；

支持五个大类，累计 40+ 个数据库类型，百余个版本；

数据库资产梳理与数据资产分类分级保护。

2. 准确建立策略与关联用户行为

自动分析建模，准确建立审计基线策略，缩短策略调整时间；

精确定位事件发生前后所有层面的访问及操作请求；

精准发现数据库资产配置、漏洞风险，并提供修复建议。

3. 安全可靠的产品架构与保护机制

超限保护机制确保自身稳定运行，审计数据不丢失；

脱敏敏感数据，杜绝泄密事件发生，避免数据泄密。

4. 兼容众多网络环境与第三方平台

支持多种部署与对接方式，兼容多种网络环境，灵活度高；

提供 8 种系统、风险告警接口，支持 8 个告警接口，按需选择；

基于 API 接口的数据对接与统一管理，具备多种管理对接能力。

亿赛通数据库安全审计系统具备 “全面、准确、安全、兼容”四大产品优势。能够全面记录访问行为与敏感数据、准确建立策略与关联用户行为、具备安全可靠的产品架构与保护机制、兼容众多网络环境与第三方平台，实现“等保合规、安全监控、追踪溯源”的审计效果。我们将以用户需求为导向，持续完善数据库安全产品的安全能力和用户体验，为各行业客户提供更全面、优质的产品与服务。

聚力西北 亿起创未来，2023 亿赛通渠道会精彩直击

7 月 5 日，“聚力西北·亿起创未来——2023 亿赛通渠道会·西安站”顺利举办，数十位数据安全行业专家及渠道伙伴代表齐聚西安，共同探讨合作共赢战略。大会对亿赛通 2023 年渠道合作政策、核心产品及西安地域特点进行详细分析，并邀请到陕西优秀伙伴代表分享与亿赛通的合作体会。

大会伊始，北京亿赛通科技发展有限责任公司西安办事处首席代表表示，公司作为国内数据安全产品与解决方案提供商的第一梯队，二十年来持续加大研发投入，深耕行业，专注技术创新和安全能力研究。如今已经从专业的文档加密厂商一步步进化为综合数据安全厂商，目前能为用户提供数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务等 60 多款高品质安全产品。其中数据泄露防护系统更是连续 7 年保持国内市场占有率第一。数据安全产业发展已进入“蓬勃期”，数据安全行业持续“高增长”，期待大家携手一起，聚力西北，抢占更为广阔的数据安全市场。

在介绍渠道战略时，亿赛通详细阐述了 2023 年亿赛通渠道伙伴政策。近年来，我司不断优化组织架构、考核体系和系统流程，重塑合作伙伴体系和管理机制、加大资源投入与伙伴赋能、打造面向伙伴的产品体系，以此加速推进伙伴转型落地。在渠道伙伴体系的打造上，通过构建两级伙伴架构，严守公平、公正的市场秩序，为渠道伙伴构建阳光、透明的商业环境。

通过推出培训认证体系、合作合规保障，与渠道伙伴建立了深层次的合作。通过各项改革措施支撑渠道战略的落地执行，和伙伴共赢数据安全行业的丰收。接下来，亿赛通将会更开放地拥抱渠道伙伴，一起同心携手齐奋进，领航安全新征程。

北京亿赛通科技发展有限责任公司数据库安全专家提到，数据安全产业要强化顶层设计，落实相关法律法规和政策标准，在政策驱动的基础之上，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。

亿赛通特别邀请到西安地区优秀渠道进行经验分享，为加快数字化发展，建设数字中国，务必需要加强数据安全保护，提升安全防护能力。新的政策要求和用户需求给数据安全行业带来了新的挑战和机遇。亿赛通一直以来全力助推优质产品、服务及解决方案走进更多渠道、行业伙伴，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，渠道伙伴与亿赛通共同以积极姿态迎接挑战、赢得机遇，聚力西北，亿起创未来。

在产品方面，随着数据泄露频发造就了行业客户的安全需求升级，因此安全企业自身的能力结构升级势在必行。亿赛通基于二十年安全实践以及对未来数据安全态势走向的深度思考，融入新的安全要素，提出了“分放管服”数据安全建设理念，以理念为指引，构建集“资产盘点、分类分级、溯源分析、加密防护、安全流转、数据水印、介质管控、外发权限控制、系统防护、终端全覆盖”的安全技术能力，达到“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”的防护效果。

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。

数字经济加引领经济新发展。站在数据安全的蓬勃期，亿赛通将坚持“分放管服”的数据安全建设理念，围绕企业业务需求做进一步的创新迭代，持续加大在行业内的营销投入；进一步优化对渠道伙伴的差异化、精准化以及多元化的激励政策，牵引伙伴转型和能力提升，与伙伴进行更好的服务利益分享，提升新商业模式下的服务能力和可销售性。

荣耀上榜 | 亿赛通成功入选《中国数据库产业图谱 (2023)》，彰显数据库安全核心实力

随着互联网技术的快速普及和数字化转型的推进，数字经济已经成为全球经济增长的重要引擎。而数据库作为数字经济的基础设施和核心技术之一，对于数据的存储、管理和分析具有重要意义。

2023 年 7 月 4 日 -5 日，由中国信息通信研究院、中国通信标准化协会指导，中国通信标准化协会大数据技术标准推进委员会（CCSA TC601）主办的“2023 可信数据库发展大会”在北京国际会议中心隆重召开。本届大会以“自主·创新·引领”为主题，共设置 9 个论坛，除主论坛外，还涵盖了金融行业、电信行业、互联网行业、汽车行业、云原生与开源数据库、搜索与分析型数据库、数据库运维及生态工具、时序时空及图数据库 8 个分论坛。近百家企业参与本次大会，各行业内专家代表发表主题演讲，共同探讨数据库的技术发展趋势及产业前景，共同推进数据库产业的高质量发展。

大会正式发布了由中国信通院云计算与大数据研究所联合 CAICT DBL 编制的《中国数据库产业图谱（2023 年）》，旨在全面客观展现我国数据库产业中的关键领域、环节和代表企业。作为专注于数据安全领域的专业厂商，亿赛通凭借二十余年的技术实践积累，成功入选该图谱中“数据库安全工具”领域，获得中国信通院、中国通信标准化协会等业界权威机构的肯定与认可。

在当前数字经济的高速发展之下，数据库安全已经成为一个不容忽视的重要话题。随着互联网、大数据、人工智能等技术的不断发展和深入应用，数据已经成为企业和组织竞争的核心资源。而数据库则是存储和管理这些数据的关键组件，它的安全性直接关系到企业的核心利益和用户的隐私权益。如果数据库的安全性得不到保障，数据可能会遭到泄露、篡改或丢失，这不仅会给企业带来巨大的经济损失，还可能导致企业声誉受损，甚至面临法律责任。

此外，数据库面临的安全威胁也在不断增加。黑客攻击、恶意软件、内部人员的不当操作等，都可能对数据库的安全构成威胁。因此，加强数据库的安全管理，采取有效的安全措施，是每一个企业和组织都必须面对的挑战。

亿赛通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。产品主要包括：数据库安全审计系统（DAS）、数据库防火墙系统（DFW)、数据运维安全管理系统 (DOSM)。亿赛通数据库安全解决方案也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。

数字经济时代下，数据库的发展成为推动数字经济发展的重要因素。数据库作为数字经济的基础设施和核心技术，需要不断创新和发展，以应对大数据时代的挑战，满足企业和组织对数据管理和分析的需求。未来，亿赛通将不断提升和完善数据库安全能力，为数字经济的发展提供有力支撑。

全面开花 | 亿赛通入选《嘶吼 2023 网络安全产业图谱》23 项细分领域

2023 年 7 月 10 日，嘶吼安全产业研究院发布了“2023 网络安全产业图谱”。嘶吼分析师根据当前网络安全发展规划与趋势，在原“2022 网络安全产业图谱”基础上进行了再分类，进一步规划网安产业布局。

本次图谱调研成功成功收录 417 家网络安全企业，分为七大类别，共涉及 121 个细分领域。相比于 2022 年新增 22 个细分领域。根据嘶吼安全产业研究院调研数据显示，一级分类 - 安全服务收录占比 32.1%，同比占比增长 3%；一级分类 - 应用与产业安全收录占比 19.4%，同比占比减少 5.6%；一级分类 - 数据安全收录占比 16.2%，同比占比增长 0.8%。相较于去年安全服务、应用与产业安全、数据安全，依然是网络安全产业三大主流方向。

亿赛通作为数据安全领域的头部企业，拥有先进的技术理念和优秀的客户口碑，成功入选图谱数据库安全、数据脱敏、文件管理与加密、数据防泄漏（DLP）、态势感知、数据分类分级、数据安全合规审计、数据综合治理、数据资产梳理、邮件安全、源代码安全、软件管控平台、审计、视频安全、云平台安全管理、移动终端安全、恶意软件防护、勒索病毒专项防护、终端综合管理、安全意识培训、合规检测、技术人才培训、网络安全保险等 23 项细分领域。

根据嘶吼研究院调研发现，网络安全 2022 年的营收增长率有所减缓，但依然处于增长趋势，故嘶吼安全产业研究院仍然看好未来行业趋势，预估从今年开始中国网络安全厂商的安全总营收将迎来平稳增长期，到 2025 年有望突破 1300 亿。

数据安全风险存在于数据采集、传输、存储、使用、外发等各个节点，每年数以万计的泄露数据证明仅采用传统的防护手段难以覆盖所有环节。面对这些问题，作为新一代综合数据安全解决方案及服务提供商，亿赛通以“人”与数据为中心，通过平衡业务需求与风险，制定数据安全策略，对数据分类分级，数据的全生命周期进行管理，从技术到产品，从策略到管理，提供完善的产品与服务支撑。不改变用户使用习惯、不影响业务流程，创建数据的安全使用环境，保证数据内网、外网同样安全可控。

在国家政策的支持及约束下，数据安全产业的发展态势日盛，网络安全服务商层出不穷，产品细分和应用也越来越多，与业务的结合也越发紧密。亿赛通会“积跬步，致千里”，在数据安全领域不断深挖，再创佳绩，再谱新篇。

强化行业数据安全治理，夯实数字金融安全基座

金融业作为关系国家经济稳定运行的“命脉”，数据安全不容有失。作为数据密集型行业，金融业海量数据在释放要素价值的同时，也面临着数据泄露、数据违规收集、传输等安全风险与挑战。

近年来，中国人民银行、银保监会、证监会等国家机构发布了一系列金融行业数据安全相关的政策、规章及标准文件，如中国人民银行发布的《金融科技发展规划（2022-2025 年）》、《金融数据安全 数据安全分级指南》、中国银保监会发布的《关于银行业保险业数字化转型的指导意见》、《监管数据安全管理办法（试行）》及中国证监会发布的《证券期货业数据分类分级指引》等，初步构建了金融领域数据安全的体系框架，为金融数据能力和安全建设提供了依据和指引。

数据安全保卫战已全面打响，金融行业加强数据应用的安全与合规建设迫在眉睫。以金融行业代表机构“银行”举例，银行办公网中运行的程序众多，金融监管机构在对银行的信息安全有硬性规定: 必须将生产网和办公网隔离开来，最大程度上保证生产网的安全。另，银行系统开发测试工作普遍外包，考虑三方人员安全隐患，银行普遍将业务网、办公网、开发测试网建设为隔离的“三网”安全域。

因此，不同网域环境下业务场景不同，所面临的安全威胁亦不同，结合项目经验，金融业数据安全风险主要如下:

网间传输风险

金融机构的生产域、开发测试域、办公域之间通常采用物理隔离或逻辑隔离形式，数据的传输流转根据银监会要求受到严格的管控。通过介质、共享磁盘等外部工具的传输可能产生重要业务数据的泄露风险。

数据未脱敏

金融业务网包含着大量的客户个人信息，这些信息也是被外界窃取的重要数据。生产域经常会导出数据到开发测试网作为开发测试使用，一旦个人金融信息未脱敏而泄露将造成严重的声誉和经济的损失。

业务系统威胁

业务网系统数据库的外部黑客攻击、内部访问权限过度、数据库导出数据没有严格的管控制度都会造成业务数据的严重泄露。

内部办公风险

办公域内存储着大量的行内人员办公文件，其中对于系统的开发测试、财务、监管单位的文件等数据使用、存储安全防护未能完善体系化建设。

外包风险

第三方外包项目在金融业已是非常普遍，人员的管理机制不完善、项目信息和中间开发测试环节获取到的敏感信息，而这些重要信息有意或无意被散播到外界会对银行造成巨大的损害。

为了应对安全风险，亿赛通针对金融行业数据安全治理需求，为用户铸就坚不可摧的安全盾牌。补全四方能力，覆盖六个阶段，建成一个体系——以保障数据安全为中心战略，结合业务场景，基于顶层规划，在现有数据安全治理的建设基础上，从组织体系、制度体系、技术体系、运营体系四个维度补全建设，形成覆盖数据全生命周期六个阶段的整体数据安全保护体系。

金融行业数据安全治理建设规划包含以下四个方面：

组织体系

金融机构需要建立完整的数据安全治理组织架构和人员配置。这包括建立由高层管理者负责的数据安全治理委员会，确定具体责任人，并建立数据安全治理团队，负责执行数据安全治理计划并监控数据安全管理进程。同时，应建立完备的数据安全管理岗位体系，为员工提供相应的岗位培训和教育，提高员工的数据安全意识和技能水平。

制度体系

目前金融机构大多有较完整的安全规范，如分级分类规定，保密规定等，但一方面没有独立的数据安全规范，可执行性不强，另一方面缺乏技术监管手段，落地执行较难。政府部门应加强对金融行业数据安全的监督和管理，制度相关的法律法规来保护数据资产安全。在制度流程建设层面，可根据机构内部组织的特点分期进行建设。

技术体系

金融机构需要建立严格的数据安全技术体系。这包括建立完善的数据加密、数据备份和恢复的技术，确保应用程序与网络的安全性。银行还需要考虑使用高端数据安全技术，如虚拟化安全技术，区块链，人工智能等，以提高数据安全的能力和水平。技术管控按照生命周期来分，可分为数据采集、数据传输、数据存储、数据使用、数据删除、数据销毁六个方面。根据数据分级分类进行安全环境和边界管控，保障数据的保密性、完整性和可用性。

运营体系

金融机构需要制定完整的运营管理流程，包括漏洞修复、安全应急响应、日志审计、安全培训等多个方面。建立数据安全的监测和评估机制。应当每隔一段时间对网络和计算设备进行信息安全认证和加固，并通过安全事件监测系统来监测安全事件。这样可以及时发现安全隐患并采取措施加以解决。通过有效的监控和管理，能够做到第一时间发现和处理异常情况，保障业务的正常运营。

综上所述，从组织体系、制度体系、技术体系、运营体系四个维度补全金融业数据安全治理的建设，能够让金融机构、银行等在数据安全方面做到全员参与、全方位覆盖。并且通过完善的权限控制、安全检测和应急响应等多个方面的保障，确保了数据的机密性、完整性和可用性，为金融企业的可持续发展提供强有力的支撑。

为有效达成数据安全治理目标，确保金融数据安全解决方案的可行性和合理性，方案设计阶段将严格遵从数据安全治理相关法律法规、标准规范、组织内部管理制度，结合历史项目经验，恪守项目建设原则，聚焦数据安全相关的各个维度上的能力和流程机制，设计数据安全治理建设方案，分阶段提升数据安全治理能力。

构建数据安全治理的项目是一项从无到有、富有挑战且意义深远的工作。对于金融业数据安全治理的建设，将数据安全标准化模型作为数据安全治理建设的总体目标蓝

分期		内容	定位
一期	“建基础”	建立健全：组织体系、制度体系以咨询服务形式，辅助金融机构在原有基础上建立健全数据安全相关组织架构、流程制度，形成满足合规要求、细化岗位职责、可指导工作落地的一整套标准规范。	数据安全治理的保障 •人员保障 •制度保障
二期	“摸家底”	资产扫描、敏感识别、分类分级借助技术工具实现对金融机构内部数据资产的扫描及敏感识别（覆盖结构化及非结构化数据）；以产品结合服务形式，完成数据分类分级梳理及密级标识，输出金融资产梳理报告。	数据安全治理的基础 •摸清家底 •盘明家产
三期	“知风险”	合规梳理、条款解读、评估风险梳理并解读海内外所需遵循的金融行业数据安全相关法律法规及标准规范，评估数据安全合规风险；调研业务场景，结合二期结论，评估现有安全防护措施下的金融机构数据泄露风险。	数据安全治理的依据 •合 9、 规风险 •业务风险
四期	“补短板”	先理后治、补齐短板、精细防护在数据全生命周期的不同阶段，采取适当的安全防护措施对金融机构数据安全加以防护，各阶段需采取的防护措施及对应产品。	安全治理能力的补全 •技防体系建立健全
五期	“持运营”	闭环管理、循环调优、安全运营搭建数据安全运营管理平台，通过多维度量化的指	安全治理能力的提升 •工具联防联控
		标，精准描述金融数据安全的实时风险和整体状况。利用海量的数据分析引擎和模型实现对数据风险的主动发现，精准定位、智能研判、快速处理、严格审计，完成对数据安全工作的闭环处理流程。	•风险提前感知 •探针统一运维 •全面精准溯源

图。而金融业数据安全治理多有一定基础，少有从“0”启建。故需基于机构原有安全能力状况，评估风险，规划升级方案。

总之，金融行业数据安全风险管理是一个复杂且长期的过程，需要金融机构根据实际情况，采取多种措施，从物理到心理，从内部到外部，从安全到合规，全面提高数据安全保障能力。结合行业解决方案，亿赛通可以更加有效地保护金融客户数据隐私和完整性，提升客户的信任度和满意度，实现金融企业持续健康发展。

国外医疗机构遭黑客攻击，千万患者被信息泄露

医疗行业的数据安全问题一直是一个重大挑战。随着医疗信息化的普及和医疗数据的大量产生，保护患者隐私和保障数据安全已成为医疗行业的首要任务。然而，医疗行业在数据安全方面面临许多困难，尤其是黑客攻击的威胁。

【HCA 医疗保健称数据泄露可能影响 20 个州的 1100 万患者】

据美联社 7 月 11 日报道，在美国和英国经营着 180 家医院的医疗巨头 HCA 医疗保健公司表示，在数据泄露事件中，20 个州约 1100 万患者的个人数据可能被盗。包括患者姓名、城市、州和邮政编码、电子邮件、电话号码、出生日期、性别，以及患者服务日期、地点和下次预约日期，被盗数据不包括社会安全号码、支付信息或诊断等临床信息。这些数据样本被一名黑客发布到一个网络骗子喜欢的在线论坛上，试图出售这些数据。总部位于新西兰的杀毒软件公司 Emsisoft 的分析师卡洛 (Brett Callow) 表示，“这可能是今年最大的医疗保健违规行为，也是有史以来最大的违规行为之一”。

医疗行业日益数字化，并面临着与其相关的数据安全风险。医疗数据主要包含患者的敏感个人信息，医疗研究数据以及患者的医疗记录。任何数据泄露、篡改或滥用都可能导致不可估量的损失，对患者隐私和医疗机构的声誉造成危害。因此，确保医疗数据的安全性和完整性是医疗行业亟待解决的问题。

为应对医疗行业的数据安全风险，以下是一些解决方案的措施，用以保护医疗数据的安全：

首先，建立完善的安全管理体系是关键。医疗机构应该建立规范的安全操作程序和安全管理制度，确保医疗数据的安全存储、传输和使用。制定明确的权限管理规定，限制不同人员对敏感数据的访问权限，从而减少恶意行为的发生。定期进行数据安全的风险评估和漏洞扫描，以及建立响应漏洞的紧急响应机制，及时修复和升级系统漏洞，提升安全防护能力。

其次，加强员工安全意识培训也是非常重要的措施。员工是数据安全的关键环节，他们应该了解和遵守保密政策和安全规范。医疗机构应定期对员工开展安全培训，教育他们识别和防范各类网络威胁，提高他们对数据安全的重视和保护意识。同时，建立举报机制和安全事件处理流程，便于员工及时报告异常情况和威胁，减少信息泄露的风险。

第三，加强网络安全防护措施也是非常关键的一方面。医疗机构应该建立强大的防火墙和入侵检测系统，及时发现并拦截恶意攻击。加密存储和传输敏感数据，保护数据的机密性和完整性。使用先进的防病毒软件，及时更新病毒库，预防病毒和恶意代码的入侵。对系统进行持续监控和日志审核，发现和追踪异常操作和入侵行为，及时采取应对措施。

此外，与其他机构建立信息共享和安全合作也是非常有效的措施之一。医疗行业可以与安全机构、技术公司及其他相关行业建立合作关系，以提高整个行业的安全水平。共同研究和开发安全技术和解决方案，共同抵御黑客攻击的威胁。

最后，加强监管和法律保障也是数据安全的重要手段。相关政府部门应该出台相关法律法规，明确对医疗数据安全的要求和规范，建立有效的监管体系，对医疗机构的数据安全进行监督和检查。加大对违法行为的惩处力度，打击黑客攻击和数据泄露行为，形成威慑效应。

作为行业内深耕多年的综合数据安全解决方案厂商，亿赛通为多行业客户提供专业的产品和服务。在“分放管服”数据安全建设理念的基础上，亿赛通数据安全运营管理平台应运而生。平台能力主要体现在综合数据、运营管理两方面，目前数据安全产品能力整体来说可以分为结构化、非结构化和半结构化三类，那么综合数据安全管理平台所管理的数据应当要包含这三类数据。其次是运营管理能力，安全管理平台一定要结合数据安全治理框架模型，从数据的产生到数据的销毁全生命周期都能够进行全流程管控运营。

从应用目标上看，平台以数据安全为核心的保护方案，涵盖了各行业各领域多数场景下的数据安全保护需求，以数据发现和数据分类分级为基础，使用了数据扫描、文件加密、数据访问控制、数据水印、数据脱敏等技术来实现数据安全防护，同时也包含了数据活动监控和数据风险评估等功能。网络安全态势感知平台更多关注的是网络行为，综合分析网络安全要素，评估网络安全状况，预测其发展趋势，并以可视化的方式展现给用户。

从技术实现上看，平台不仅采集流量，而且要进行协议内容还原，更多关注数据内容，从而判断是否存在数据安全的风险。在一些分析类技术的使用上，例如 UEBA、规则匹配、勒索防护等，平台也会用到。

总之，对于医疗行业而言，确保数据安全至关重要。尽管数据泄露和其他安全威胁无法完全消除，但通过采取适当的物理、技术、人员和程序控制措施，医疗机构可以最大限度地降低安全风险，并保护医疗数据的可用性、完整性和保密性。在不断发展的信息时代，医疗行业需要不断提高对数据安全的关注，并与相关利益相关方合作，共同保障医疗数据的安全。

（文章部分数据来源于互联网）

国家首份网络安全保险政策文件发布，推动网络安全产业高质量发展

近日，工业和信息化部、国家金融监督管理总局联合印发《关于促进网络安全保险规范健康发展的意见》（以下称《意见》），提出建立健全网络安全保险政策标准体系、加强网络安全保险产品服务创新等 5 方面共 10 条具体意见，鼓励各方主体积极推进网络安全保险产品和服务创新。

《意见》从政策标准、产品服务、技术、产业需求、发展生态等层面全方位引导网络安全保险健康有序发展，推动网络安全产业高质量发展。

其中，《意见》第二条指出加强网络安全保险产品服务创新。

（三）丰富网络安全保险产品。鼓励保险公司面向不同行业场景的差异化网络安全风险管理需求，开发多元化网络安全保险产品。面向重点行业企业开发网络安全财产损失险、责任险和综合险等，提升企业网络安全风险应对能力。面向信息技术产品开发产品责任险，面向网络安全产品开发网络安全专门保险，为信息网络技术产品提供保险保障。面向网络安全服务开发职业责任险等产品，转移专业技术人员在安全服务过程中因人为操作可能引发的安全风险。

（四）创新发展网络安全保险服务。鼓励网络安全保险服务机构协同合作，探索构建以网络安全保险为核心的全流程网络安全风险管理解决方案。充分发挥保险机构专业优势，联合网络安全企业、基础电信运营商等加快网络安全保险与网络安全服务融合创新。充分发挥网络安全企业、专业网络安全测评机构技术优势，联合保险公司提升网络安全保险服务能力。

• 亿赛通作为中国数据安全专家，此前与中国太平洋保险达成战略合作，共同开展网络安全保险业务，充分发挥各自优势，为用户提供安全可靠的“防勒索数据安全险”整体解决方案。由传统的“事后理赔”模式转变为 “事前防御、事中预警、事后补偿”的全新模式。太平洋保险公司设立“防勒索数据安全险”，针对高价值文件提供防勒索安全保障，这不仅是一份保障合同，更是一项专业责任的服务承诺。

保前安全检测：远程风险测评、制定各项重要数据的保密服务承诺，配备完善全面的保险应急方案。

保中安全监控：对数据持续进行风险监测、预警、发现问题第一时间通知管理人员，快速启动应急处理方案，及时降低安全风险。

保后应急响应：承诺 72 小时达到现场，定责定损，安全专家修复系统、恢复数据。

《意见》第三条指出强化网络安全技术赋能保险发展。

（五）开展网络安全风险量化评估。围绕电信和互联网行业典型事件以及工业互联网、车联网、物联网等新兴场景开展网络安全风险研究。探索建立网络安全风险量化评估模型，加强网络安全风险影响规模预测、经济损失等分析。支持网络安全企业、专业网络安全测评机构等研发网络安全风险量化评估技术，开发轻量化网络安全风险量化评估工具，鼓励保险机构建立网络安全风险理赔数据库，支撑网络安全风险精准定价。

（六）加强网络安全风险监测能力。开展网络安全保险全生命周期风险监测，覆盖事前、事中、事后等重要环节。鼓励网络安全企业、专业网络安全测评机构等充分发挥网络安全风险监测技术优势，充分利用安全技术手段，针对网络安全漏洞、恶意网络资源、网络安全事件等开展网络安全威胁实时监测，及时发现网络安全风险隐患，提升网络安全风险监测预警、应急处置等能力。

• 亿赛通“防勒索数据安全险”整体解决方案可通过对可信应用和访问数据文件进行一键收集，形成安全防护策略。保护数据文件只能被可信进程访问和使用，非法进程不能访问和使用，可以有效防止病毒、木马勒索软件等对数据文件的篡改和破坏。

• 启动防护后，如检测到非法进程访问被保护数据文件，立即拒绝应用进程的访问，并记录违规访问记录。违规访问记录内容包含违规访问进程名称、进程位置、访问时间、访问数据位置等信息，帮助用户及时有效定位勒索病毒信息，同时也可以逐步丰富安全防护策略，减少过度防护。

• 通过全面识别安全风险，对安全意识进行测评和培训等教育服务，降低人员隐患，消除潜在安全风险，综合提升用户的安全风险识别能力、突发安全事件应对能力和事后数据恢复能力，形成风险闭环管理的运营机制。“防勒索数据安全险”在投保者遭遇勒索后，确保企业获得足量的保障赔偿，在一定程度上降低和补偿因勒索病毒带来的经济损失。

《意见》第四条指出促进网络安全产业需求释放。

（七）推广网络安全保险服务应用。面向电信和互联网、能源、金融、医疗卫生等重点行业，以及工业互联网、车联网、物联网等新兴融合领域，围绕网络安全与信息技术产品服务供给侧和需求侧两类主体，充分发挥网络安全产业、网络安全保险相关联盟协会等作用，开展网络安全保险服务试点，形成可复制、可推广的网络安全保险服务模式，促进网络安全保险推广应用。

（八）推动企业网络安全风险应对能力提升。鼓励重点行业企业完善网络安全风险管理机制，推动电信和互联网、制造业、能源、金融、交通、水利、教育等重点行业企业积极利用网络安全保险工具，有效转移、防范网络安全风险，提升网络基础设施、重要信息系统和数据的安全防护能力。支持中小企业通过网络安全保险服务监控风险敞口，建立健全网络安全风险管理体系，不断加强中小企业网络安全防护能力。

• 亿赛通的文件防火墙将为企业勒索软件防护提供第一道屏障，减少企业被勒索的风险；太平洋财险的保险服务将为企业勒索软件防护守好最后一道大门，将企业的勒索损失减到最低。太平洋财险和亿赛通的强强联合，共同守护企业核心资产安全。

网络安全保险在当前的网络安全环境下具有重要的意义和价值。个人和企业应认识到网络安全风险的严重性，保险公司也应加强网络安全保险产品的开发和推广，为个人和企业提供更加全面和有效的网络安全保护。未来，在《意见》的推动下，亿赛通将结合自身业务优势，持续创新，深化合作，尝试开拓更多方向的网络安全保险业务，为广大客户提供更加完善、高效、可靠的网络安全产品与服务！

敏感数据检查难？数据安全检查工具箱系统 - 单机版来安排！

近日，国家金融监督管理总局办公厅向各银保监局、银行保险机构等下发《关于加强第三方合作中网络和数据安全管理的通知》，要求各银行保险机构对照通报问题，深入排查供应链风险隐患，切实加强整改。

7 月 14 日，国家金融监督管理总局发布的行政处罚信息显示，浙江农商联合银行因存在 11 项主要违法违规行为，依据《中华人民共和国银行业监督管理法》第四十六条第一项、第三项、第五项；《中华人民共和国商业银行法》第七十五条第二项，被银保监会浙江监管局罚款 380 万。

据了解，本次浙江农商联合银行违法行为中包含了“数据安全管理缺失”，关于数据安全管理问题，此前某大行也曾因“数据安全管理较粗放，存在数据泄露风险”等违法违规行为被开出巨额罚单。从数据安全管理的角度看，四大行在近 2 年均有相关罚单。

针对金融行业日益突出的数据安全管理问题，在《网络安全法》、《数据安全法》、《个人信息保护法》等法律法规要求指引下，亿赛通自主研发了数据安全检查工具箱系统 - 单机版。

数据安全检查工具箱系统 - 单机版外观

数据安全检查工具箱系统单机版采用 U 盘一体化形态，即插即用，无需安装部署。单机版内置金融行业检查规则，可随时随地帮助用户提前对办公终端电脑中存量的数据文件进行合规性、安全性自检。除满足数据自检工作外，单机版检查工具亦具备文件自处理能力，即可帮助用户提前发现数据安全风险并对数据进行处理。

数据安全检查工具单机版功能界面

数据安全检查工具系统单机版兼容 Windows、Linux 等操作系统，满足不同终端场景下客户的敏感数据检查需求。单机版工具既支持独立使用，也可与数据安全检查工具箱系统管理平台进行联动，将多个数据安全检查结果统一汇总并分析，输出数据安全合规性综合报告，帮助金融客户面对监管部门抽查时，改变被动接受检查的局面。

护航金融行业数据安全，数据安全检查工具箱系统利刃出鞘！未来，亿赛通将继续深耕数据安全领域，不断打磨产品，为更多行业客户提供贴合业务特点、解决客户问题的优秀产品及解决方案。

欲购请联系服务热线：400-898-1617

政策速递 | 央行发布《中国人民银行业务领域数据安全管理办法（征求意见稿）》

咨询研究部 / 文

7 月 24 日，中国人民银行发布《中国人民银行业务领域数据安全管理办法（征求意见稿）》（以下简称《办法》），并向社会公开征求意见。

01/ 制定背景

《数据安全法》第六条明确规定：“工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责”，党中央、国务院也要求认真落实国家法律，进一步细化数据分级分类保护、数据目录管理、全流程数据安全管理、数据安全监测预警和应急处置相关制度。

在此背景下，中国人民银行组织起草了《办法》，全面衔接《数据安全法》，细化明确中国人民银行业务领域数据安全合规底线要求，填补本领域数据安全管理制度保障空白。《办法》对指导数据处理者优质高效合规开展中国人民银行业务领域数据处理活动，履行数据安全保护义务，保障消费者和企业用户的合法权益，促进数据要素市场高质量发展具有重要的意义。

02/ 适用范围

根据“谁管业务，谁管业务数据，谁管数据安全”基本原则，《办法》明确适用范围为中华人民共和国境内开展的，中国人民银行承担监督管理职责各类业务相关的数据处理活动。此类业务涉及的数据处理者，开展对应数据处理活动时，应当遵守《办法》提出的管理要求。

本办法所称中国人民银行业务领域数据，指根据法律、行政法规、国务院决定和中国人民银行规章，开展中国人民银行承担监督管理职责的各类业务活动时，所产生和收集的不涉及国家秘密的网络数据。

当前，《办法》约束的数据处理活动主要包括：货币政策业务、跨境人民币业务、银行间各类市场交易业务、金融业综合统计业务、支付清算业务、货币管理和数字人民币业务、经理国库业务、征信业务、反洗钱业务等领域的数据处理活动。

03/ 主要内容

《办法》分成总则、数据分类分级、数据安全保护总体要求、数据安全保护管理措施、数据安全保护技术措施、风险监测评估审计与事件处置措施、法律责任、附则八章，共五十七条，主要内容包括：

一是规范数据分类分级要求。强调数据处理者应当建立数据分类分级制度规程，梳理数据资源目录标识分类信息，在国家数据安全工作协调机制统筹协调下，根据中国人民银行制定的重要数据识别标准，统一对数据实施分级，严格落实网络安全等级保护和风险评估等义务，并在此基础上推动各数据处理者进一步做好数据敏感性、可用性层级划分，以便在全流程数据安全管理中更好采取精细化、差异化的安全保护管理和技术措施。

二是提出数据安全保护总体要求。强调数据处理者应当压实数据安全责任，建立数据安全问责处罚制度和数据处理活动全流程安全管理制度，制定数据安全培训计划。

三是压实数据处理活动全流程安全合规底线。针对收集、存储、使用、加工、传输、提供、公开和删除各环节，

向数据处理者明确采取哪些安全保护管理和技术措施后，可视为总体满足尽职尽责的合规底线要求。

四是细化风险监测、评估审计、事件处置等合规要求。强调数据处理者应当建立数据处理活动安全风险监测和告警机制，加强数据安全风险情报监测、核查、处置与行业共享，制定数据安全事件定级判定标准和应急预案，规范应急演练、事件处置、风险评估和审计等工作。

五是明确中国人民银行及其分支机构可对数据处理者数据安全保护义务落实情况开展执法检查，以及数据处理者违反规定时对应的法律责任。

数据出境安全：保护国家基础性战略资源的新路径

在这兵马未动，数据先行的时代，数字经济模糊了地域界限，大量的新兴技术和服务会同时被不同国家的用户使用，产品技术的跨国界流动同时意味着数据的流动，数据是国家基础性战略资源，对于这种有着重要意义的“数字石油”，各国都在推动和参与数据出境规则的制定。

近两年我国已经发布多项数据出境相关政策标准，科学、完备的细化数据出境定义、要求。首先，针对数据出境的定义，国家网信办发布的《数据出境安全评估办法》及《数据出境评估申报指南（第一版）》明确指出，数据出境是指“数据处理者向境外提供在中华人民共和国境内运营中收集和产生的重要数据和个人信息”。

数据出境具体包括三种情形：

1. 数据处理者将在境内运营中收集和产生的数据传输、存储至境外；

2. 数据处理者收集和产生的数据存储在境内、境外的机构、组织或者个人可以查询、调取、下载、导出；

3. 国家网信办规定的其他数据出境行为。

数据处理者：数据处理者是指在数据处理活动中自主决定处理目的和处理方式的个人和组织。

境外和境外接受者：“境内”“境外”中的“境”是以司法辖区为依据，包括港澳台地区。

我国在政策层面，数据出境的政策指导要追溯到 2021 年，国家“十四五规划”强调，要加强数据安全评估，推动数据跨境安全有序流动。

立法层面，《网络安全法》《数据安全法》《数据出境安全评估办法》《数据出境安全评估申报指南（第一版）》相继发布确立了重要数据出境传输前应通过安全评估的保护要求；《个人信息保护法》确立了个人信息跨境的三条合法路径，《数据出境安全评估办法》《网络安全标准实践指南——个人信息跨境处理活动安全认证规范》《个人信息出境标准合同规定（征求意见稿）》分别为三条合法路径提供了实施指引。

除此之外，金融、汽车、医疗健康等行业的主管部门还结合自身行业需求对特定行业的数据跨境流动提出了要求，进一步健全了数据出境流动规则。

目前，数据出境安全已经从“加速立法”进入“从严执法”阶段。在应对全球数据监管和遵守国家相关法规的前提下，现阶段，企业合规能力并未跟上加速立法的节奏。对客户来说，数据出境安全仍然面临着如下困难：

- 员工缺乏安全意识，有意无意违规操作；
- 缺乏统一标准，重要数据范围存在争议；
- 未结合业务，安全产品不符合实际场景需求，形同虚设；
- 想要合规，但并不知如何合规，迷茫。

想要做好数据出境安全，首先需要明确什么是重要数据。依照目前已发布的《信息安全技术 重要数据识别指南（征求意见稿）》、《信息安全技术 网络数据分类分级要求（征求意见稿）》、《工业和信息化领域数据安全管理办法（试行）》、《工业数据分类分级指南（试行）》等相关国家与行业标准对地区、行业重要数据进行细化定义、识别和防护规范。重要数据是指特定领域、特定群体、特定区域或达到一定精度和规模的数据，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

明确重要数据后，还需要进行重要数据识别与分类分级，明确企业重要数据分布与数据级别，完成内网数据总量统计，厂商根据统计结果给出数据出境合规申报路径建议，协助企业完成重要数据安全自查。这一环节必不可少的就是合规自查工具箱。

亿赛通数据跨境安全检查工具可以实现对网络（含邮件）中的业务进行还原，并对还原出的业务进行内容识别。根据不同国家、地区的数据安全规定，梳理成安全策略。对还原出的业务内容进行对应的数据安全规定检查，及时发现业务开展过程中的敏感数据，并根据不同规定中数据的敏感程度采取不同的防护策略，以期满足不同国家、地区对敏感数据的安全要求。及时发现网络上不同要求的敏感数据，采取不同的防护方法，降低敏感数据泄露风险。

数据出境安全合规可落地

帮助有数据出境需要的企事业单位或监管机构对照自查或检查出境数据的合规情况。通过对不同国家、地区数

据安全要求（如：欧盟的 GDPR、美国的 ADPPA、日本的 APPI 等）的梳理分析，形成符合要求的敏感数据检查策略和防泄露措施，实现满足不同国家、地区数据安全的合规要求，促进数据出境安全合规的可落地。

数据出境安全可视化

企事业单位跨境数据流转中的敏感数据可被及时发现，并根据不同国家、地区的数据安全要求采取相应的技术防护措施。通过对不同敏感数据流转的轨迹画像，实现敏感数据出境的安全风险可视化。

全面还原网络中的实际业务

通过数据跨境安全检查工具，实现对网络中的业务全面还原，作为网络业务的全量备份。通过数据挖掘和关联分析，可以全面还原网络中的业务场景，实现“什么人”在“什么时间”通过“什么方式”发了“什么数据”给“什么人”触发了“什么敏感信息”完整业务过程。


数据出境安全合规可落地


数据出境安全可视化


全面还原网络中的实际业务

数据出境安全有大量的细节需要安全厂商、企业在合规工作中注意，这不是一项能轻易完成但具有重要意义的工作。数据出境安全，目前还是一个成长中的孩子，数据安全的国际博弈才刚刚开始。亿赛通会继续帮助客户实现数据资产在境内、外的安全流转，为保障国家、企业、个人的数据安全尽自己的一份力！

咨询服务 | 数据安全评估、风险评估、合规评估……概念如何界定？

咨询研究部 / 文

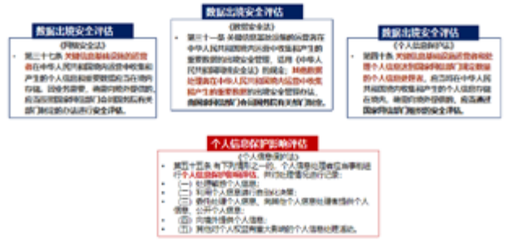
2021 年起，数据安全进入“强监管”时代。重要数据泄露，个人信息收集、处理不当等事件一旦发生，组织将面临监管重罚。在此背景下，各类组织用户对数据安全评估的需求愈发旺盛。那么什么是数据安全评估？数据安全风险评估、数据安全合规评估、个人信息保护影响评估等工作又有什么区别和联系呢？

目前来看，“数据安全评估”尚无统一定义，一般提到这个词汇，是对于评估服务的一个泛指，依据不同的维度，其可以细分为多种类型。

依据评估结论展现形式的不同，数据安全评估可以分为“合规评估”和“风险评估”两大类。合规评估以证明组织数据安全工作符合合规性要求为目标，开展评估工作时，评估项往往基于国家和行业主管机构发布的合规要求而拟定，并在一定程度上达成了共识（比如网络安全评估中的等保评估）。评估结论是一个打分结果，分为符合、不符合，或优、良、中、差等。风险评估以主动发现潜在的安全风险为目标，在评估工作中需要基于较为复杂的判断方法以及专家的主观经验，评估结论不仅会呈现对风险等级的判断，并会附带一系列整改意见。我国《数据安全法》中提到的，“重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告”中的要求，就属于此类。

依据组织形式的不同，数据安全评估可分为主管部门组织的评估和自行开展的评估两大类。主管部门在国家政策的引导下，以合规检查为重点，依据既定的检查项，在监管领域履行数据安全检查职责，视为主管部门组织的评估。目前金融、电信、医疗等重点行业的监管部门，都在落实和深化数据安全检查工作。自行开展的评估即数据处理者自行组织、开展的评估工作，可依托组织内部的有关部门（比如数据管理部、合规管理部）开展，也可委托第三方测评机构来进行专业评估。值得一提的是，2023 年 4 月，国家编制出台了《信息安全技术 数据安全评估机构能力要求（征求意见稿）》，以进一步规范第三方数据安全评估机构的专业能力。

依据触发评估的场景的不同，数据安全评估可分为数据出境安全评估、个人信息保护影响评估、APP 个人信息安全测评等。数据出境安全评估是在《网络安全法》《数据安全法》《个人信息保护法》的要求下，因业务需要，向境外提供在境内运营中收集和产生的个人信息和重要数据的关键信息基础设施运营者，以及向境外提供重要数据或规定数量个人信息的其它数据处理者，须在出境前开展的评估活动。数据出境安全评估包括自评估和主管部门（网信办统筹）评估两个阶段，目前已存在一套完整的标准和流程，《数据出境安全评估办法》《数据出境安全评估申报指南》等文件对此提供了具体指导。个人信息保护影响评估（PIA），是依据《个人信息保护法》第五十五条要求，在处理敏感个人信息、利用个人信息进行自动化决策、委托处理个人信息、向境外提供个人信息等可能对个人权益有重大影响的个人信息处理活动发生前须进行的评估。目前开展个人信息保护影响评估可依据《信息安全技术 个人信息安全影响评估指南》等参考标准来开展。



依据开展阶段的不同，数据安全评估可分为事前评估、事中评估和事后评估三大类。事前评估是组织类用户依据合规要求或实际需要，在特定数据出境、加工、共享等情形发生前开展的安全评估工作。具体工作包括理清数据资产、评估平台或系统的数据安全风险，确保数据活动符合法律法规、标准的规定，查验现有数据安全防护的管理和技术手段是否完善等。事中评估是为保障信息系统和数字化工作的稳定有序进行而开展的数据安全状态监控工作。具体工作包括实时感知系统或平台运行时的风险行为，确保各项管理流程、技术措施在数据活动环节的有效，数据泄露、滥用等风险行为的监测预警等。事后评估是当安全事件发生后，对事件发生路径进行溯源分析，以找出事件发生原因、制定整改方案为目标的一系列活动。依据国家的合规文件精神，企业应开展集事前、事中、事后为一体的持续评估工作，尤其是重要数据和大量个人信息处理者，应打造体系化的数据安全管控能力，以保障数据流通各环节的安全闭环。

除上面提到的评估分类以外，数据安全评估还包括以评估组织数据安全整体能力为目标的数据安全能力评估，如数据安全管理能力成熟度评估（DSMM）、数据安全治理能力评估（DSG），以评估数据安全厂商技术和产品能力为目标的数据安全技术产品测评等。各类评估工作将彼此配合、互相补充，在数据安全“强监管”的背景下，成为组织用户落实数据安全监管要求，提升数据安全管控能力，赋能数据健康有序流通的基础性、关键性工作。其中，“数据安全风险评估”通过“以数据为中心”，对网络数据安全保护和数据处理活动情况中存在的风险源进行识别和分析，是助力分类分级策略与技术工具实现统一联动，深化落实数据安全治理工作的关键环节和重要抓手。

咨询服务下篇文章，我们将聚焦“数据安全风险评估”这一具体服务项，详细讲解该服务的实施路径，敬请期待。

构建强固安全防线，助力芯片半导体行业安全防御体系建设

芯片产业是整个信息产业的核心部件和基石，也是国家信息安全的最后一道屏障。当前芯片产业发展已被列入我国重点科研工程，是未来国家战略的重要一环。除了前所未有的机遇和挑战，还有外国势力对中国芯制造的持续施压。由于半导体芯片的加工工序多、技术密集大，在制造的各个环节都会产生大量数据；伴随设备与工艺的不断提升，针对制造过程的控制变得日益复杂，也令数据的高效、合理使用及其安全防护需求愈发凸显。

在这个万物互联的时代，数据安全的“飓风”正在袭来。三星被曝芯片机密代码遭 ChatGPT 泄露、HTC 被曝遭一员工窃取 HTC SENSE 6.0 之 UI 接口程序的商业机密、日产公司近 20GB 源代码遭到泄露、苹果代工厂「广达」MacBook Pro 设计图纸被黑客窃取、联发科芯片产品机密信息被前员工盗窃泄密等等，这些事件的发生都在向各企业敲响警钟。由于现代芯片和半导体技术的复杂性，攻击者有可能通过恶意软件、硬件漏洞或其他技术手段，获取、修改或破坏芯片半导体中的数据。这样的攻击可能导致用户隐私泄漏、系统瘫痪、知识产权泄露等严重后果。因此，保护芯片半导体数据的安全性至关重要。

基于数据安全领域的各项基础法律，近年来一系列配套法规和部门规章也陆续进行意见征集或正式颁布实施。伴随着《网络安全法》、《数据安全法》、《个人信息保护法》的相继出台并实施，为应对日益严峻的数据安全形势，如何建立科学全面的数据安全防护体系，更加有效地保障数据安全，支撑以数据为关键要素的数字经济发展，已成为国家、全社会以及政府部门、行业机构、企事业单位等各类组织需要面临的共同挑战。《集成电路布图设计保护条例》、《集成电路布图设计行政执法办法》、《集成电路布图设计保护条例实施细则》等保护条例的发布是为了保护集成电路布图设计专有权，鼓励集成电路技术的创新，促进科学技术的发展。

半导体芯片设计、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。

设计业务场景分析

1）因行业发展需要，芯片企业包含大量重要信息的电子资料，如设计图纸、SVN 等服务器，为设计提供支撑，但自身明文存储，未采用访问控制手段，可能导致非法用户访问服务器，窃取明文数据。这些核心数据关系到公司的生存发展以及商业竞争力，一旦泄密，将会给公司造成不可估量的损失。

2）芯片行业企业数据库存放关键数据，敏感操作无审计，无追溯；且对数据访问或者下载时无防护措施。

3）芯片核心数据明文在部门之间流转、以及在员工终端上使用留存。在数据资产的使用、传输、 保管、销毁的过程中存在较多安全风险，增加了信息安全管理工作难度。

办公场景分析

1）ERP、OA 是办公核心业务系统，涉及到物资、人力资源、财务资源等核心数据。对于信息系统、业务平台、网络通讯、办公终端以及存储介质中的数据均以明文形式存在，会有泄露风险。

2）邮件是与外界沟通的重要途径。从内到外，容易造成数据泄露。

3）核心数据明文在办公部门之间流转、以及在员工终端上使用留存。对于信息系统、业务平台、网络通讯、办公终端以及存储介质中的数据均以明文形式存在，在数据资产的使用、传输、保管、销毁的过程中存在较多安全风险。

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，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，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。

为了构建强固的安全防线，我们需要从芯片设计、加密技术以及安全管理等方面综合考虑，不断加强数芯片半导体数据的安全保护。只有如此，我们才能确保数据在传输和处理过程中的完整性和保密性，实现真正的数据安全。加强数据安全保护不仅需要技术的创新和突破，也需要全社会共同努力，合力打造一个安全可靠的数字化环境。

场景	解决方案
IIC 设计网	**数据库审计系统** 数据库审计系统是一款通过对数据库网络流量的采集，基于数据库协议解析与还原技术的数据库安全审计系统。本系统实现对芯片半导体企业数据库所有访问行为的监控和审计、对其中的危险操作进行多种方式的告警、对数据库访问行为进行多维度的统计并进行图形化展现。
	数据库加密系统 利用加密技术，有选择性的加密数据库内敏感字段内容，保护数据库内敏感数据。将数据库内大量设计资料，电子数据等敏感数据由明文存储改为密文存储，解决敏感数据明文存储引起的数据泄密、内部高权限用户或者黑客入侵的数据窃取等问题。
	数据安全网关 数据安全网关是一种软件服务集成平台，通过 WebServices 接口、DLL 动态库、SO 库等方式可以方便地与应用系统无缝集成，提供文件加密、文件解密、外发文档制作以及流程审批等能力，还能够支持手机移动端文件加解密，有效保障了芯片半导体行业应用系统数据使用安全。
	CDG 文档权限管理 电子文档安全管理系统以数据资产防泄密为核心，涵盖文档安全、终端安全、防勒索、安全态势、集团管控五大板块，实现对用户电脑终端、移动办公、各类应用系统上的数据从生产、存储、流程、外发到销毁进行全生命周期保护。
	透明加解密 通过对文档加密授权及角色对应，控制文档在内部受控使用，避免越权使用带来的泄密风险。
	数据安全交换系统 针对两个网段业务数据跨网交换这类型要求，用数据安全交换系统，由系统自动进行数据甄别、管控、传输到另外网段，再由干系人获取。
办公室	**数据库防火墙** 数据库防火墙系统是一款通过对数据库网络流量实时处理，基于数据库协议分析与控制技术的数据库安全防护系统。系统基于主动防御机制，实现数据库的访问行为控制、危险操作阻断、可疑行为审计，是一款集数据库 IPS 和审计功能为一体的综合安全产品。

办公室	**数据库加密系统** 利用加密技术，有选择性的加密数据库内敏感字段内容，保护数据库内设计文件、电子信息等敏感数据。将数据库敏感数据由明文存储改为密文存储，解决敏感数据明文存储引起的数据泄密、内部高权限用户或者黑客入侵的数据窃取等问题。
	数据库审计系统 数据库审计系统是一款通过对数据库网络流量的采集，基于数据库协议解析与还原技术的数据库安全审计系统。本系统实现对芯片半导体行业数据库所有访问行为的监控和审计、对其中的危险操作进行多种方式的告警、对数据库访问行为进行多维度的统计并进行图形化展现。
	数据安全网关 数据安全网关是一种软件服务集成平台，通过 WebServices 接口、DLL 动态库、SO 库等方式可以方便地与应用系统无缝集成，提供文件加密、文件解密、外发文档制作以及流程审批等能力，还能够支持手机移动端文件加解密，有效保障了应用系统数据使用安全。
	邮件数据泄漏防护系统 邮件 DLP 系统，是一款基于邮件数据安全防护和敏感识别、数据防泄漏的安全防护系统。邮件 DLP 集被动审计和主动防御于一体，实现邮件数据传输过程中邮件协议数据分析、敏感数据识别审计、邮件数据脱敏处理、邮件审批管理、阻断策略响应访问控制。
	网络数据泄漏防护系统 网络 DLP 系统是一款基于网络协议分析与控制技术的安全防护系统。网络 DLP 集被动审计和主动防御于一体，实现网络数据传输过程中各应用协议分析、敏感数据识别审计、阻断策略响应访问控制。网络 DLP 产品不仅能识别网络行为的合法性，还能深入到 7 层网络协议，识别网络数据内容的合法性，能有效满足对敏感数据防丢失泄漏的痛点需求。
	数据安全智能管理平台 以数据为中心，分类分级为基础，融合机器学习、关联分析、密码技术、访问控制、数据标识等多种技术的综合性终端数据安全防护产品。
	文档安全管理系统 电子文档安全管理系统以数据资产防泄密为核心，涵盖文档安全、终端安全、防勒索、安全态势、集团管控五大板块，实现对用户电脑终端、移动办公、各类应用系统上的数据从生产、存储、流程、外发到销毁进行全生命周期保护。

亿赛通助力某新能源车企打造综合数据安全解决方案，进一步加强企业安全保障能力

数据安全是汽车行业日益关注的问题，特别是随着企业存储和使用越来越多的数据来驱动联网汽车功能。随着车企行业向软件定义车辆过渡，并采用新技术实现数字化和个性化客户体验，保护敏感信息变得越来越重要。国家对于汽车行业发布了明确的数据安全管理规定，既是对目前智能汽车发展过程中的数据安全问题的监管回应，也是对汽车行业的合规要求。而亿赛通积极布局汽车行业客户，深入研究汽车数据安全问题，从而更好地为全行业车企及产业链伙伴提供智能汽车数据安全体系建设。

此前，某新能源车企由于此前使用的加密系统在运行中存在着诸如虚拟打印机打印文件格式、大型文件通过 smb 上传到 liunx 服务器无法自动解密，下载自动加密等问题，影响员工办公使用，因此需要进行加密产品的更换。为建立核心数据安全管理系统，针对数据安全性、平台易用性、系统扩展性等问题，结合该公司现有的系统环境，制定一整套完善的解决方案，在公司内实现图纸、代码等数据的安全，防止重要资源外泄，提高公司数据安全保护能力，保护公司资源和效益，同时不对日常办公、开发产生负面影响，达到安全与效率的双向平衡。

亿赛通结合有关制度、管理体系和应用模式，采用了自主研发的新一代电子文档安全管理系统，将透明加密、权限管理、文档安全防护、服务器安全加固、日志审计等技术完美地结合在一起，有效防范数据泄密。

需求分析

为了加强公司对终端电脑电子文档的保护，防止公司重要数据泄漏，电子文档资料是公司核心资产，需要有系统管理举措，确保其完整、安全、有效、保密。

需要符合以下几项要求：

1. 符合相关法律法规合规要求；

2. 对知识产权、 专利数据资产进行有效保护；

3. 对敏感数据进行强保护，防止内部员工有意和无意的数据外泄行为；

4. 对外发敏感数据设置特定权限策略和审批流程，有效保证只有授权人员能够获取并阅读外发文件；

5. 采用的防泄密技术不会降低工作效率；

6. 安全策略可根据部门或组分别定义，灵活管理；

7. 可与现有的业务系统等进行集成；

8. 旧加密文件可以无缝替换；

9. 文件操作审计记录，可进行事后追溯。

解决方案

（一）域用户导入

通过域信息配置，实现将 AD 域中的组织关系以及用户同步导入到加密系统的数据库中，与域控服务器关联，客户端登录时自动去域服务器中做认证。

（二）无缝替换

通过技术手段，可将历史加密文件自动转换为亿赛通的新加密文件，当历史的旧加密文件所在的文件夹被打开时，当前窗口所显示的文件会自动被替换为亿赛通加密文件，并且同步替换加密厂商信息。

（三）流程审批

域同步时会将 AD 域组织关系同步到加密系统管理后台，审批员可以按此组织结构进行设置审批关系，当有文件需要外发时，可以通过设定的审批关系提交流程解密文件。

（四）策略放开限制

CDG 客户端和服务器端可以配合项目实施放开限定策略的限制。

（五） 自动加密

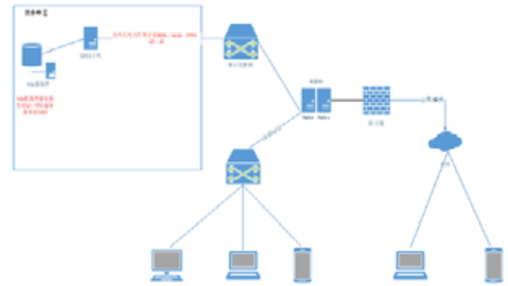
通过加密策略统一控制，可实现上传到 HPC 服务器、OA 系统中的数据上传时自动解密上传，下载时自动加密下发，即保证数据库的可靠性与安全性的同时，也可以兼顾正常的业务流转。

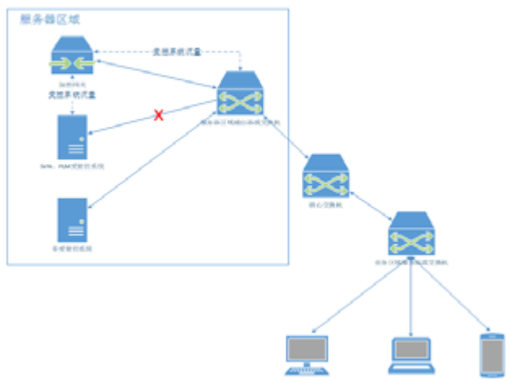
（六）多终端配置

安装手机客户端、MAC 端和 Linux 客户端，其中手机客户端适配安卓系统、苹果系统，鸿蒙系统；linux 客户端为文件夹加密。

（七）网关准入

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 SVN、PLM 系统提供安全准入防护，安全准入通过终端身份识别、传输隧道加密等多方面进行应用数据安全访问控制，使得未安装客户端的用户无法访问 SVN 、PLM。





项目价值

- 服务器和客户端都完成加密软件安装，客户端实现单点登录，确认收取到部门策略，对文件进行自动加密；
- 服务器可查看用户操作日志和审批流日志，查看具体时间等信息；
- 服务器数据库定期自动备份，和密钥一起保存在其他服务器中，保证系统可及时被灾难恢复；
- 用户了解并能自己使用加密软件，熟悉解密审批和外发审批流程，知晓加密文件和非加密文件的区别；
- 通过网关做准入控制实现未安装加密客户端的用户无法访问指定的业务系统，保障业务系统的安全；
- 通过中间件与 OA 系统做集成，实现文件的上传自动解下载自动加，保证系统正常运行。

项目成果

亿赛通通过一体化部署，不改变集团现有使用习惯，零感知替换原有加密软件，通过对数据进行识别解析，内置规则策略进行智能加密；在项目中对接人才培养、业务集成等重要环节，并对第三方系统实行上传解密、下载加密等手段，及时有效识别用户异常行为并进行防控。项目实施后，从技术层面帮助零跑汽车实现对于数据的加密防护，规避各类风险，满足企业合规及自身数据管理要求，全方位提高该公司数据安全管控和风险防御能力。

部分车企客户展示

一汽解放 | 上汽集团 | 华晨宝马 | 广州本田

东风日产 | 北京汽车 | 海马汽车 | 江淮大众

广汽集团 | 比亚迪 | 长城汽车 | 江铃汽车

长城汽车股份有限公司

长城汽车
时尚 科技 精美

客户简介

长城汽车是一家全球化智能科技公司，业务包括汽车及零部件设计、研发、生产、销售和服务，旗下拥有哈弗、魏牌、欧拉、坦克及长城皮卡。长城汽车面向全球用户，致力提供智能、绿色出行服务，加速向全球化智能科技公司转型。长城汽车的业务包括汽车及零部件设计、研发、生产、销售和服务，并在氢能、太阳能等清洁能源领域进行全产业链布局，重点进行智能网联、智能驾驶、芯片等前瞻科技的研发和应用，旗下拥有哈弗、魏牌、欧拉、坦克及长城皮卡。

典型案例 TYPICAL CASES

需求背景

长城汽车的业务包括汽车及零部件设计、研发、生产、销售和服务，有着智能网联、智能驾驶、芯片等前瞻科技的研发应用等核心技术。为了防止企业内部研发、设计等重要资料的泄露，保障企业的核心竞争力，公司开始陆续加强了内网信息化的安全建设。因此，长城汽车签约亿赛通新一代电子文档安全管理系统，共同保护企业数据资产安全。

解决方案

新一代电子文档安全管理系统是一款电子文档安全防护软件，该系统利用驱动层透明加密技术，通过对电子文档的加密保护，防止内部员工泄密和外部人员非法窃取企业数据资产，对电子文档进行全生命周期防护。

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

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

文档权限管理可对数据进行细粒度权限控制、模板批量授权、文档权限管理；

文档外发管理:可进行用户身份认证、使用权限控制;

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

项目成果

亿赛通为长城汽车提供了完善的电子文档安全管理系统解决方案，通过对数据的使用、存储、流转、审计等各个环节安全把控，避免了公司敏感数据遭窃的风险，提高数据安全的智能化管理，为长城汽车构筑了立体化的安全防护体系。