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

10 月刊

2022 年共 11 期

热烈祝贺

党的二十大胜利闭幕

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

《亿赛通十月刊》喜迎二十大，数据安全重要程度日益加深

中国共产党第二十次全国代表大会已于本月闭幕，奋进新征程、建功新时代。站在“两个一百年”奋斗目标的历史交汇期，加强网络安全工作战略谋划和顶层设计，推动我国网络安全体系不断完善，网络安全保障能力持续提升，网络安全屏障日益巩固，为加快建设网络强国提供了有力支撑和坚实保障。

亿赛通切实结合业务完成数据安全治理顶层设计方案，以“分·放·管·服”数据安全建设理念为基础，针对数据全生命周期过程的治理需求提供完整方案，从数据资产梳理到数据安全防护，进而保障数据可安全流转，建立综合完善的数据安全治理体系。亿赛通产品细分为五大部分：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。

刊首语 PREFACE

国内

1、多家电商平台个人信息被泄！信息泄露造成多大影响

摘要：根据央广网报道，一位从事数据安全保护工作 10 年的工作人员曾接到一个陌生电话，对方能直接详细说出他的姓名、某电商平台的订单信息，并以货品质量有问题，要求他供银行卡号，以便赔偿。

2、钟镇涛 27 岁女儿英国遭遇电话诈骗：个人信息泄漏严重

摘要：近日，钟镇涛 27 岁大女儿钟嘉晴（Chloe）在社交平台上发文，称自己在英国伦敦遇上诈骗集团，被骗走大量个人资料。钟嘉晴在发文中表示，前几天接到自称中国驻英大使馆的电话，先是称有重要文件需要领取，接着告知因为来伦敦时同机有人涉嫌犯罪，需要配合调查，先后通过转接人工电话和视频软件进行询问，并被告之要保密，不能告诉任何人。

她表示自己当时太害怕，都差一点就吓哭了，但最终她发现所谓的大使馆电话是假的，是骗子通过某种渠道取得了自己的个人身份信息，自己的大部分信息已经被泄露了。

3、频频收到亲友网贷逾期短信？你的个人信息可能遭泄露

摘要：2021 年 3 月起，丁先生频繁收到要求其朋友王某归还逾期网贷的催收短信。丁先生拨打短信上记载的联系电话，告知客服该笔借款与他无关，并提出不要再联系他的要求。沟通未果，丁先生依然持续每天收到网贷公司的催债短信。万般无奈下，丁先生将网贷公司诉至法院。

4、医院实习生私转病患就诊信息 法院：泄露隐私，情节严重将追究刑事责任

摘要：小芳在某三甲医院妇产科做人工流产手术，令她没想到的是，医院实习生小勇是她前男友刘大的好友，而她做手术的消息也被前男友获知。刘大向小芳发来医院手术排表的照片，并用污言秽语攻击她，给小芳来了双重暴击。小芳以名誉侵权为由，将医院和刘大起诉至法院。今日，长沙市雨花区人民法院公布了该起典型案例。

5、大数据时代新威胁，女性一定要注意隐私！人脸识别要把自己包严实

摘要：天津一男子带着头盔去房地产看房，这则视频在网上引发了热议，不少人对这样的行为大为不解，甚至还嘲笑这个男子小题大做。但当男子接受采访时说到背后的原因，让人细思极恐。男子说道：地产公司的售楼处都装有人脸智能识别系统，我一个朋友上个月和中介一起来看房，但由于这个人脸识别，被售楼处告知与我朋友长相相似的人独自前往售楼处看房，所以就认定我朋友为自访客户而非中介渠道客户，因此无法享受相关优惠。

6、事关信用卡，北京银保监局发布风险提示

摘要：10 月 25 日，北京银保监局发布风险提示，提示广大消费者非法“代理处置信用卡债务”套路多：假冒专业人士发布虚假广告，夸大宣传；诱导获取消费者个人金融信息，收取高额费用；怂恿消费者虚构事实、伪造证据，恶意逃废债；阻碍有关部门与消费者取得联系，切断正常维权渠道。

7、工信部：前三季度信息安全收入保持较快增长

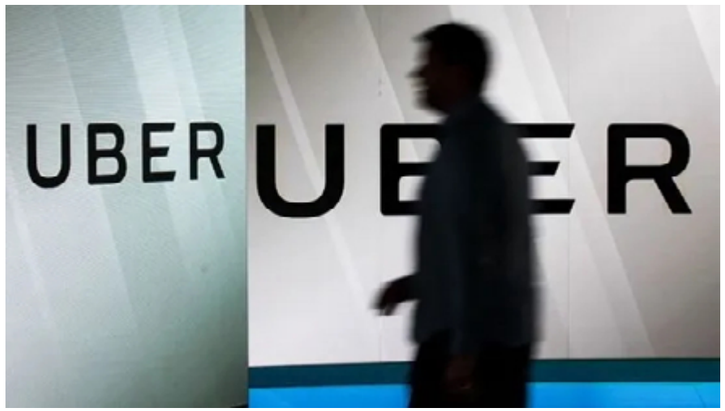
摘要：10 月 26 日，据工信部，前三季度，信息技术服务收入 48681 亿元，同比增长 10.1%，在全行业收入中占比为 65.1%。其中，云计算、大数据服务共实现收入 7138 亿元，同比增长 6.5%。前三季度，信息安全收入保持较快增长，收入达到 1269 亿元，同比增长 12.4%。

8、中航证券：自主可控背景下网络安全重要性凸显 明年市场规模或超 800 亿元

摘要：中航证券发布研究报告称，2018-2021 年我国网络安全行业 CAGR 为 16.04%，预计未来三年我国网络安全市场将保持 15% 以上的增速，到 2023 年市场规模将超过 800 亿元。

国外

1、优步 (UBER.US) 子公司 Drizly 因 2020 年数据泄露问题遭 FTC 处罚



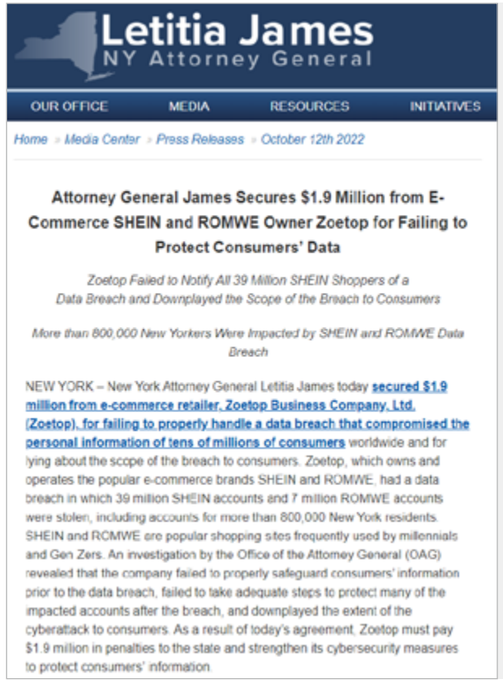
摘要：美国联邦贸易委员会 (FTC) 正在处罚优步 (UBER.US) 旗下子公司酒精运输公司 Drizly Inc. 及其首席执行官 Cory Rellas，原因是他们涉嫌在 2020 年的一次数据泄露安全漏洞问题，那次安全问题泄露了 250 万消费者的个人信息。根据 FTC 周一的一份声明，这项拟议的命令要求现在是 Drizly 销毁不必要的数据，并限制该公司可以收集和保留的信息。它将 Rellas 绑定到数据安全要求中，“因为他在主持非法商业行为中所扮演的角色”。

2、澳大利亚拟加大对出现数据泄露公司的处罚力度

摘要：近日澳大利亚总检察长马克 · 德雷福斯透露，当地政府拟在本周提交相关提案，修订《隐私法》以加大对发生重大数据泄露事故公司的处罚力度。此前在今年 9 月下旬，澳大利亚第二大电信公司 Singtel 旗下的 Optus 透露，其遭遇了安全攻击、并发生数据泄露事故，预计涉及用户数量近 1000 万、约占该国总人口 40%，这也是该国历史上最大规模的数据泄露事件之一。据了解，此次泄露的数据涉及用户的姓名、出生日期、地址、联系方式、驾驶执照、护照、身份证号码等，并且除 Optus 的相关数据外，其曾经的子公司维珍移动和 Gomo 的用户数据也被泄露。

3、超 65000 家公司的 2.4TB 数据遭泄露？微软承认了，但……

摘要：据网络安全供应商 SOCRadar 称，该公司的内置云安全模块检测到微软维护的 Azure Blob 存储配置错误，其中包含来自知名云提供商的敏感数据。分析显示，泄露的文件包括执行证明（PoE）、工作说明文档、发票、产品订单 / 报价、项目详情、已签署的客户文件、POC 工程、客户电子邮件、客户产品价目表和客户库存、客户内部意见、营销策略、客户资产文档以及合作伙伴生态系统详细信息等。



4、Shein 母公司将因数据泄露向纽约州支付 190 万美元

摘要：据 The Verge 报道，超快速时尚品牌 Shein 和 Romwe 背后的公司将向纽约州支付 190 万美元，因为数据泄露影响了数百万客户。罚款源于对 Zoetop 公司的指控，即该公司未能保护客户的数据，没有适当地通知客户数据泄露，并试图对泄露的程度保持沉默。

5、源码被外包误上传到 GitHub，丰田近 30 万数据遭泄露?

摘要：丰田汽车 10 月 6 日表示：发现在 T-Connect 服务中有 296019 条客户信息疑似被泄露，泄露的内容包含了客户电子邮件地址和客户号码，受影响的客户为 2017 年 7 月以来使用电子邮件地址注册该服务网站的个人用户。关于信息泄露的原因为：从 2017 年 12 月到今年 9 月 15 日，开发 T-Connect 网站的承包商不小心上传了部分带有公共配置的源码。

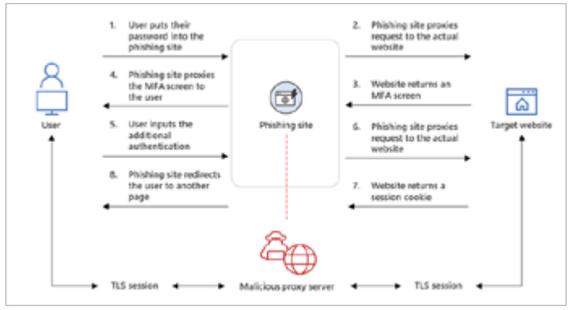
6、或影响上千人：继 Optus 后新加坡电信又一澳洲业务遭遇数据泄露

摘要：新加坡电信（Singtel）在澳大利亚遭遇了另一起潜在的数据泄露事件，其当地 IT 服务咨询公司 Dialog Group 的服务器在一次网络安全攻击中受损，涉及一些客户和员工信息的访问，其中一些样本被发布到暗网上。

7、英国建筑公司 Interserve 因数据泄露被罚款 440 万英镑

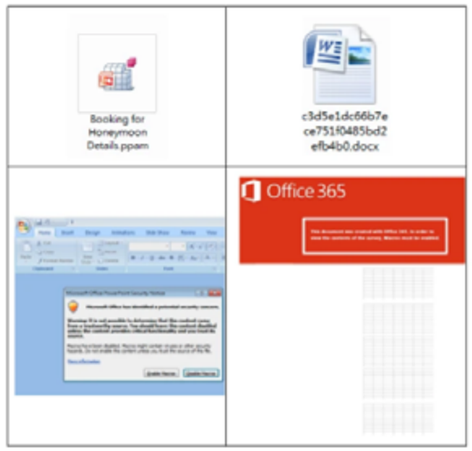
摘要：英国信息专员办公室 (ICO) 因未能保护其 113,000 名现任和前任员工的个人信息安全而对建筑公司 Interserve 集团处以 440 万英镑的罚款。罚款与 2020 年 5 月 2 日发生的数据泄露有关，ICO 认为这是可以避免的——Interserve 对此提出异议。ICO 发现该公司未能采取适当的安全措施来防止网络攻击。黑客能够通过网络钓鱼电子邮件访问多达 113,000 名员工的个人数据。泄露的数据包括个人信息，例如联系方式、国家保险号码和银行账户详细信息。这些数据还包括种族、宗教、任何残疾的详细信息、性取向和健康信息。

8、新的 EvilProxy 服务让所有黑客都可以使用高级网络钓鱼手法



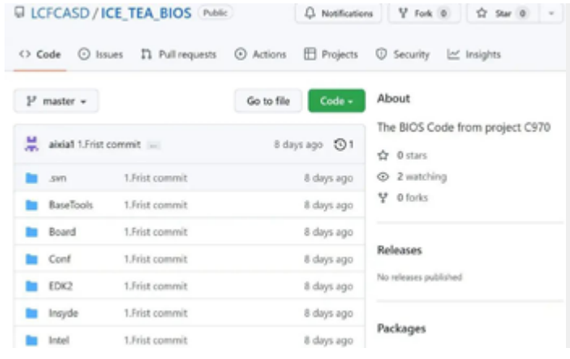
摘要：一个名为 EvilProxy 的反向代理网络钓鱼即服务（PaaS）平台近日兴风作浪，承诺可以窃取身份验证令牌，从而绕过苹果、谷歌、Facebook、微软、Twitter、GitHub、GoDaddy 甚至 PyPI 上的多因素身份验证（MFA）机制。该服务使不知道如何设置反向代理的技能低下的威胁分子也能够窃取原本受到有力保护的在线帐户。反向代理是位于目标受害者和合法身份验证端点（比如公司的登录表单）之间的服务器。

9、攻击者利用 Microsoft Office 文件传播 Agent Tesla 和 njRat



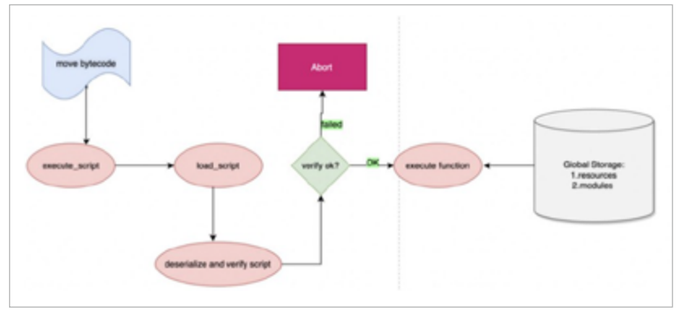
摘要：研究人员最近发现了一些恶意的 Microsoft Office 文件，这些文件试图利用合法网站 MediaFire 和 Blogger 执行 shell 脚本，然后释放 Agent Tesla 和 njRat 的两个恶意变体。Agent Tesla 是一款著名的监视软件，首次发现于 2014 年，它可以从 web 浏览器、邮件客户端和 FTP 服务器中窃取个人数据，收集屏幕截图和视频，并收集剪贴板数据。njRat（也称为 Bladabindi）是 2013 年首次发现的远程代理木马，能够远程控制受害者的设备，记录击键、访问摄像头、窃取浏览器中存储的凭据、上传 / 下载文件、操作注册表等。

10、Intel 确认 Alder Lake BIOS 的源代码泄露



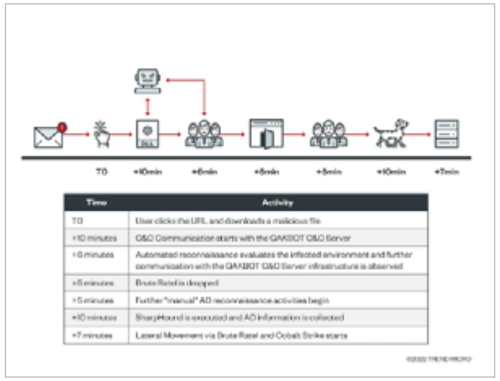
摘 要：Alder Lake 是 Intel 2021 年 11 月发布的第 12 代核心处理器。10 月 7 日，有名为 freak 的推特用户在推特上发布了一个链接称是 Intel Alder Lake 的 UEFI 固件。该链接为名为 LCFCASD 的用户发布的 GitHub 库——ICE_TEA_BIOS。Freak 称 ICE_TEA_BIOS 库中包含 C970 项目的 BIOS 源代码。

11、Move 虚拟机漏洞影响 Aptos 区块链



摘要：近日，新加坡 Numen Cyber Labs 安全研究人员在 Aptos 公链的虚拟机中发现一个非常严重的安全漏洞。攻击者利用该漏洞可以引发 Aptos 节点奔溃，甚至拒绝服务。Move 中有两类程序：module 和 script。Module 是定义结构类型和函数的库。Script 是可执行文件的入口点。Movevm 和 evm 虚拟机原理是相同的，需要将源码编译为字节码，然后在虚拟机中执行。

12、Black Basta 勒索软件组织通过 QAKBOT，Brute Ratel 和 Cobalt Strike 渗透网络



摘要：趋势科技的研究人员最近分析了一个与 QAKBOT 相关的示例，该示例导致了 Brute Ratel C4 和 Cobalt Strike 有效负载，这可以归因于 Black Basta 勒索软件组织。QAKBOT 的恶意软件在短暂中断后于 2022 年 9 月 8 日恢复传播，当时研究人员在这一天发现了几个传播机制。观察到的传播方法包括 SmokeLoader(使用 ' snow0x ' 传播器 ID)，Emotet(使用 ' azd ' 传播器 ID)，以及使用 ' BB ' 和 ' Obama20x ' ID 的恶意垃圾邮件。

亿赛通入选 2022 年度第一批北京市市级企业技术中心创建名单


北京市经济和信息化局

要闻发布 政务公开 政务服务 政民互动 经信数据

关于公布2022年度第一批北京市市级企业技术中心创建名单的通知

来源：科技标准处 发布日期：2022-10-18 11:43

各相关单位：

我局依据《北京市企业技术中心建设管理办法（2021版）》（京经信发〔2021〕72号）和《北京市企业技术中心建设管理实施细则（2021版）》的有关规定，组织了2022年度第一批北京市企业技术中心新创建工作。前期已在拟通过名单予以公示。期间未收到异议。现将2022年度第一批新创建的北京市市级企业技术中心名单予以正式公布。

10 月 18 日，北京市经济和信息化局发布了《关于公布 2022 年度第一批北京市市级企业技术中心创建名单的通知》，经过对申报材料的严格审查、评审及公示，亿赛通凭借在数据安全领域专业的技术实力成功入选。

当前，新一轮科技革命和产业变革正在向纵深演进，在时代更迭的潮流中，企业的核心竞争力就是产品、技术，如何推动技术创新是每个企业避无可避的难题之一。《北京市企业技术中心建设管理办法（2021 版）》中指出，“企业技术中心”是指企业根据市场竞争需要设立的技术研发与创新机构，主要负责制定企业技术创新规划、开展产业技术研发、创造运用知识产权、建立技术标准体系、凝聚培养创新人才、构建协同创新网络、推进技术创新全过程实施。

北京市企业技术中心是省部级研发平台，是北京市政府对技术创新能力较强、创新业绩成效显著、具有重要示范和导向作用的企业予以的高含金量研发平台类资质，旨在进一步强化企业技术创新主体地位，引导和支持企业增强技术创新能力。

2022 年度第一批北京市市级企业技术中心新创建名单

序号	企业名称
36	[redacted]
37	[redacted]
38	[redacted]
39	北京亿赛通科技发展有限责任公司
40	[redacted]
41	[redacted]
42	[redacted]

本次被认定为北京市企业技术中心，是北京市经济和信息化局对亿赛通科技创新、自主研发、技术应用等综合实力的全面肯定，有利于进一步提升公司的品牌影响力和竞争力，促进公司在行业内起到良好的科技引领和示范作用。

作为成立近二十年的数据安全厂商，亿赛通主动拥抱数字经济时代，积极投身数字中国建设。基于分·放·管·服数据安全建设理念，打造数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务为一体的综合数据安全解决方案，通过 AI 算法、关联分析、密码技术、访问控制、数据标识等多种技术，将企业核心数据的全生命周期进行管控，帮助用户建设从被动防御向主动安全转型的防御体系，确保数据资产可视、数据威胁可管、数据风险可控、数据血缘可溯。

未来，亿赛通将以本次北京市企业技术中心认定为契机，继续聚焦数字经济领域和数据安全建设，一如既往的以创新精神、优质产品、专业服务，为用户提供适用于自身核心竞争力的数据安全产品、安全解决方案和安全服务。

激活企业数据潜能，亿赛通解码数据安全治理

近期，亿赛通与恒申集团合作的数据安全治理 - 分类分级项目经双方努力取得阶段性胜利。作为从“草根工业”发展成为集化工、化纤及新材料为一体的先进制造业企业集团。恒申集团在产业数字化转型过程中，内部产生的数据资产激增，同时，随着国家对制造行业数据安全治理的要求的严控，恒申集团数据安全治理项目随之启动。据悉，恒申集团对项目进行了长期调研，面向全国招标。在选型过程中，也对多家厂商做了全方位的比较及严格的筛选。亿赛通根据恒申集团的实际需求，联合中海创科技集团给恒申集团量身定做出适合其应用的数据安全治理解决方案，最终赢得客户信赖与认可，成功签署项目。

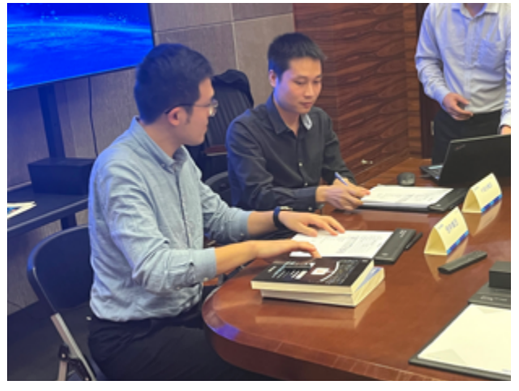
项目已经取得阶段性的成果，双方领导特于 10 月 21 日召开恒申数据安全治理 - 分类分级项目总结会并签署战略合作。会议邀请福建省工信厅及福建省电子产品监督检验所相关领导莅临，对项目双方汇报进行指导。

亿赛通动态 ESAFENET NEWS

在数字经济高速发展的今天，数据安全是各行各业必不可少的助力。制造行业在《网络安全法》、《数据安全法》、《个人信息保护法》的指导下，《工业数据安全评估指南（草案）》、《工业领域重要数据和核心数据识别规则（草案）》、《工业企业数据安全防护要求（草案）》等条例规范对该行业数据安全提出明确要求，应不断强化制造业数据安全治理能力。

亿赛通数据安全专家表示，数据分类分级是数据治理的基础，是平衡利用和保护之间的重要依据之一。数据分类分级可有效果的解决数据战略驱动、数据安全驱动遇到的问题，如：数据资产不清晰、数据管理阻力大、数据价值较难挖掘、数据业务难发展等。在恒申集团项目中，我司首先对集团内部现状进行调研和需求分析，制定信息定级标准，梳理安全管控点。将集团数据按照绝密、机密、内部进行分类分级。随后设计框架，系统建设落地。

亿赛通数据安全治理覆盖数据安全建设全生命周期，涉及梳理、规划、建设和执行等阶段。在数据安全体系建设初期即引入数据分类分级，通过指导企业数据安全体系合规建设，提升数据安全保障能力，同时配合有效的技术工具，使企业数据安全防护能效最大化，整体促进企业数据安全建设发展。



项目初期，是厂商与用户的结合过程，是将理论付诸实践的过程。为确保项目顺利上线，我司为恒申集团专门定制项目响应机制，7*24 小时第一时间响应，优先分配资源。在签署本次战略合作后，双方将重点通过全局部署、统一管理、单独实施等策略，方便、快捷、高效的为恒申集团业务提供数据安全治理支撑服务。

随着数据安全态势愈发严峻化，数据安全治理 - 数据分类分级成为业务的主旋律之一。全面体系化的专业治理方案，是各行业的需求痛点。现有客户对安全的期望也在不断的变化，不仅要通过技术来满足安全需求，更对前期规划及后期实施提出了更高的要求。未来，亿赛通会是恒申集团不断发展与创新中最得力的伙伴之一，有中国数据安全专家为其坚守阵地，恒申集团会创造更加辉煌的明天！

培训 | 给自己“充满电”，亿赛通第三期《数据安全治理工程师》培训课程圆满结课

近日，为期两天亿赛通第三期《数据安全治理工程师》培训课程已圆满结束。参加培训的学员来自全国各行各业的 10 余家企事业单位人员，包括数据安全专员、主管以及信息安全负责人、业务主管等数据安全相关从业人员。

目前国家支持教育、科研机构和企业等开展数据开发利用技术和数据安全相关教育和培训，采取多种方式培养数据开发利用技术和数据安全专业人才，促进人才交流。为了确保培训效果，亿赛通不仅将培训课程做了周密的规划安排，而且派出了具备丰富实战和教学经验的安全专家和高级讲师为学员授课，系统地提升学员在安全治理、管理等方面的专业性和服务能力。

亿赛通人才培养中心目前是国内最具专业实力的人才培养体系之一，汇聚数据安全领域的优势资源，开展数据安全治理领域的学科建设、人才培养和安全技术研究工作，为企业与个人客户提供数据安全培训服务，培养国内一流、专业的安全人才。我司自主开发的《数据安全治理工程师》培训体系，已获得工信部人才交流中心的高度认可。

亿赛通《数据安全治理工程师》培训课程围绕数据安全治理展开，以“让数据更安全”的培训目标，结合当前数据安全领域最新的研究成果，运用国内的数据安全理论、基于实际项目经验，讲解数据与用户权益面临的风险、组织应当如何面对数据安全挑战，确保学员了解大数据时代背景下，数据安全治理的具体特点，并结合安全合规理论与技术方法等内容，让学员充分掌握数据安全治理相关知识。

第四期《数据安全治理工程师》培训课程将于 2022 年 12 月开课，现已正式开启报名通道，小伙伴们赶快加入进来吧 ~

主办单位：北京亿赛通科技发展有限责任公司

招生对象：企业信息安全负责人、数据安全部门工作人员、大数据部门的工作人员、信息安全管理人员、技术支持人员、运维人员、数据管理人员风险管理人员

培训时间：2022 年 12 月 26-27 日

形式：线上直播

培训联系人：卜国东

联系方式： 15979094485

数据安全能力培训 | 一次培训拿双证！第三期数据安全职业能力培训即将开班

由工业和信息化部网络安全管理局指导，中国计算机行业协会数据安全专业委员会与工业和信息化部教育与考试中心联合推出的数据安全职业能力培训第一、二期课程已顺利完成。即日起，数据安全能力培训第三期培训正式开始招生！

数据安全能力培训

中国计算机行业协会数据安全专业委员会与工业和信息化部教育与考试中心为全方位满足数据安全人才市场需求，特联合推出数据安全职业能力培训。培训课程设置数据安全评估师、数据安全工程师、数据安全咨询师、数据安全架构师、数据安全开发人员、数据安全运维人员的职业能力培训。

目前已开设数据安全工程师、数据安全评估师课程两项。学员通过培训掌握数据安全基础知识，了解数据安全评估体系，熟悉数据安全评估技术，综合提升数据安全评估能力，使其大幅度提升在数据安全领域工作中的竞争力。同时，也通过考试选拔掌握坚实基础理论和系统专业知识，可以从事数据安全评估、建设工作的高级特定人才，促进数据安全产业发展。

认证情况

学员参与培训且考试合格后将同时获得工业和信息化部教育与考试中心颁发的“工业和信息化职业能力证书”和中国计算机行业协会数据安全专业委员会颁发的“数据安全职业能力证书”。证明学员在相应领域达到相应技术技能水平，且有助于企业参加项目投标活动。学员信息纳入 “工业和信息化技术技能人才数据库”，可在工业和信息化部教育与考试中心官网、工业和信息化技术技能人才网上学习平台、数据安全产业公共服务平台查询。

下期培训安排

培训项目：《数据安全工程师》、《数据安全评估师》

承办单位：北京亿赛通科技发展有限责任公司

招生对象：网络安全数据安全从业者、数据安全顾问、服务人员、IT 从业人员、有意学习数据安全的人员等

培训时间：2022 年 10 月 17-20 日

考试时间：2022.11.3

取证时间：2022.11.17

授课形式：线上直播

费用说明：11800 元 / 人 （含考试费）

报名咨询：卜国东 15979094485

课程名称	课程内容
数据安全导论	数据安全发展背景、数据安全基础知识、数据安全管理框架
数据安全合规	数据安全法律体系、数据安全法规政策、数据安全标准规范
数据安全知识与基础	数据架构、计算机网络、数据库、密码学
数据安全技术	加密技术、脱敏技术、防泄漏技术
数据安全应用实践	数据识别型产品、非结构化数据防泄漏产品、结构化数据防泄漏产品、数据安全加密产品
数据安全在新兴技术中的应用	区块链技术的应用
数据安全产品部署与维护	数据安全防护现状、数据生命周期安全与安全治理框架、数据安全治理防护、数据安全风险TOP10、数据安全治理防护部署
数据安全实施与管理	数据安全法律法规、数据安全管理、数据安全管理制度、数据生命周期安全管理、数据安全应急响应
数据安全排查	红队攻击思路、安全加固基本知识、常见漏洞分析

备注：以上课程内容会根据新技术发展调整，请以最终的课程表为准

课程名称	课程内容
数据安全导论	数据安全发展背景、数据安全基础知识、数据安全管理框架
数据安全合规	数据安全法律体系、数据安全法规政策、数据安全标准规范
数据安全知识与基础	数据架构、计算机网络、数据库、密码学
数据安全技术	加密技术、脱敏技术、防泄漏技术
数据安全应用实践	数据识别型产品、非结构化数据防泄漏产品、结构化数据防泄漏产品、数据安全加密产品
数据安全在新兴技术中的应用	区块链技术的应用
数据安全评估实施	数据安全评估依据与目的、数据安全评估体系、数据安全评估要点、分类分级、数据安全风险分析、数据安全成熟度评估、数据安全成熟度评估实施、数据安全评估技术

备注：以上课程内容会根据新技术发展调整，请以最终的课程表为准

实时战况 -2022 年首届数据安全大赛赛道一 | 数据安全大闯关

数字经济时代，数据安全将面临哪些挑战？企业数据安全如何保障？面对复杂多变的安全形势，数据安全人才培养该如何“与时俱进”？这些问题或将在 2022 年首届数据安全大赛中得到解答。高手同台的顶级数据安全大赛、顶尖技术成果方案展示都将集中呈现。

2022 年首届数据安全大赛由中国电子信息产业发展研究院、中国信息通信研究院、国家工业信息安全发展研究中心、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) 主办，北京亿赛通科技发展有限责任公司等企业协办。共设三个赛道：数据安全大闯关、数据安全产品能力评比、数据安全治理方案。即日起，“2022 年首届数据安全大赛”预赛已正式线上开启。

大赛旨在打造数据安全领域的国家级权威赛事，宣传推广数据安全理念，提高全民数据安全意识，吸引产业要素聚集，激发市场主体活力；选拔优秀示范企业和专业人才，激发更多创新型、专业型数据安全技术企业涌现，加速我国数据安全人才培养；推广可落地的产业化成果，为数据安全产业发展提供新动力；遴选优质产品和治理方案，推动解决行业数据安全实际需求，提升全社会数据安全保障能力。

赛道一数据安全大闯关初赛采用线上解题的方式，数据安全技术人员间进行技术竞技，以考察参赛选手对敏感信息识别、泄露数据溯源、数据文件保护等方面的知识和技能。具体参赛时间、观看地址及晋级规则如下：

正式比赛时间

10 月 25 日 10:00—18:00

10 月 26 日 10:00—18:00

晋级规则

平台将根据各队得分实时展示战况及排名，最终按总分由高至低排名，排名前 100 名队伍晋级到线下总决赛（注：根据最终参赛队伍规模，特将晋级队伍数量由 50 支调整为 100 支）。同一单位或学校（大型企业以同一集团为单位）最多不超过 8 支队伍晋级决赛。

其他信息

其他详细信息，请参阅附件《数据安全大赛参赛手册》。

全新赛程解锁，极限闯关再度升级，更多精彩，让我们共同期待！

附件：数据安全大赛参赛手册

主办单位

中国电子信息产业发展研究院

中国信息通信研究院

国家工业信息安全发展研究中心

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)

协办单位

蚂蚁科技集团股份有限公司

北京安华金和科技有限公司

北京亿赛通科技发展有限责任公司

北京天融信网络安全技术有限公司

护航数据安全建设第四期：数据安全流转

作为安全领域新的风向标，数据安全的关键在于需要具备持久化的安全运营能力。在整个数据安全生命周期中，数据流转阶段是数据安全事故频发重灾区。

对于企业而言，如何在现有的业务数据基础上，从容的应对数据经济下的数据流转过程中产生的一系列安全问题，已成为企业安全建设新的命题。对此，以数据为核心和主视角的数据流安全流转产品崭露头角。

亿赛通数据安全流转通过存储加密、数据变形、访问控制、行为监测等技术手段，针对开发测试环境、数据交换、数据分析、数据共享等情况下的敏感数据处理，防止外部黑客攻击、内部数据窃取、脱库等风险下造成的数据泄露。遵循数据安全合规建设，保证数据存储、流转过程中的安全存储与按需放心流转。数据安全流转类产品如下：数据脱敏系统 DMS、动态数据脱敏系统 DMS-D、静态数据脱敏系统 DMS-S、数据交换系统 DSES、安全网关 FNS、数据跨境安全检查。数据安全流转产品梳理

1、数据脱敏系统 DMS

亿赛通数据脱敏系统是亿赛通自主研发的一款软件数据安全产品，产品可用在发测试环境、数据交换、数据分析、数据共享、业务脱敏、数据运维等场景。亿赛通数据脱敏系统针对每种敏感数据类型均提供了高度仿真的脱敏规则，保证脱

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

2、动态数据脱敏系统 DMS-D

亿赛通动态数据脱敏系统（简称 :DMS-D）是一款高性能、高扩展性的动态数据屏蔽和脱敏产品，在数据库通讯协议层面，通过 SQL 代理技术，实现了完全透明的、实时的敏感数据掩码能力；在不需要对生产数据库中的数据进行任何改变的情况下，依据用户的角色、职责和其他 IT 定义规则，动态的对生产数据库返回的数据进行专门的屏蔽、加密、隐藏和审计，确保业务用户、外包用户、运维人员、兼职雇员、合作伙伴、数据分析、研发和测试团队及顾问能够恰如其分地访问生产环境的敏感数据。

3、静态数据脱敏系统 DMS-S

亿赛通静态数据脱敏系统（简称 :DMS-S），是一款面向敏感数据通过脱敏规则进行数据变形，实现敏感信息的可靠保护的数据脱敏产品。实现自动化发现源数据中的敏感数据，并对敏感数据按需进行脱敏规则变形，避免敏感数据泄露，脱敏后的数据保持了数据的一致性和业务的关联性，应用于开发测试环境、数据交换、数据分析、数据共享等场景。同时对脱敏过程进行监控审计，对数据敏感数据源、敏感数据类型、脱敏任务进行多维度的统计并进行图形化展现。

4、数据交换系统 DSES

亿赛通数据交换系统 (简称：DSES)，部署在不同的隔离网络环境之间，为客户提供数据交换的一体化解决方案。该产品集成安全隔离、访问控制、数据风险识别、交换过程审批、日志审计等多功能于一体，可管控交换过程的同时，大幅提升隔离网络间的交换效率。同时，产品具备架构部署双活，病毒检查，数据定期备份，数据全程加密等安全策略，实现高速、可靠的信息交换服务。在跨网文件交换管控中，实现事前有授权审批、事中有数据泄露防护、事后有审计可追溯的全生命周期管理。

5、安全网关 FNS

亿赛通 FileNetSec 文档加密安全网关系统 (简称 FNS) 是基于动态加解密技术所研发的应用系统文档安全加固产品。从电子文档在企业的使用流程入手，将数据泄露防护与企业现有 OA 系统、文件服务系统、ERP 系统、CRM 系统等企业应用系统完美结合，有效解决文档在脱离企业应用系统环境后的安全问题。FNS9000 是集旁路、串联、网桥等部署模式于一身的综合安全网关产品。它能更加高效、灵活地应用于各种复杂的网络架构中，对用户既有应用系统所产生的电子内容进行安全防护，同时不影响应用系统的工作效率。

6、数据跨境安全检查

亿赛通数据跨境安全检查在满足《数据安全法》、《数据跨境传输管理办法》的基础上，事前采用访问控制、加密、脱敏、防泄漏等工具，对数据跨境处理活动各个环节进行技术管控；事中，通过数据流转监测平台等技术和产品，实现 API 接口监控、数据传输异常告警、数据跨境活动定期审计等功能，并对数据跨境全过程记录，实现动态风控评估，必要时执行流量限制、链路封闭、签名验证、权限迁移等措施；事后，通过流量分析实现事件溯源。

在加快数字化发展大背景下，企业在现有业务结构下，形成体系化的落地治理能力，推动高质量发展的战略举措，是构建企业数字化新发展格局、建设数据安全流转体系的必由之路。作为中国数据安全专家，亿赛通专业的技术手段将持续帮助企业用户加速数字化转型，提升其综合防御能力。

喜迎二十大 | 护航数据安全建设
第一期：数据安全治理

中国共产党第二十次全国代表大会已正式拉开序幕，奋进新征程、建功新时代。站在“两个一百年”奋斗目标的历史交汇期，在喜迎党的二十大胜利召开之际，如何筑牢数据全生命周期的安全问题，成为企事业单位首要关注的焦点之一。习近平总书记曾多次发表重要讲话，加强网络安全工作战略谋划和顶层设计，推动我国网络安全体系不断完善，网络安全保障能力持续提升，网络安全屏障日益巩固，为加快建设网络强国提供了有力支撑和坚实保障。

在此核心思想指导下，安全厂商需要精准把握数据安全新特点、新趋势。保障企业数据安全体系持续稳定运行的关键，是坚持安全顶层设计，确保数据安全管控过程中的各个节点监管到位。亿赛通切实结合业务完成数据安全治理顶层设计方案，并针对数据全生命周期过程的治理需求提供完整方案，从数据资产梳理到数据安全防护，进而保障数据可安全流转，建立综合完善的数据安全治理体系。亿赛通产品细分为五大部分：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。

本期，先和小亿一起了解一下数据安全治理：

亿赛通数据安全治理整体采用大数据技术架构，通过 AI 算法，关联分析、密码技术、访问控制、数据标识等多种技术，采集分析各类安全设备结构化和非结构化日志，探测、预测、发现威胁事件和风险，为敏感数据识别和分级打标提供依据，为用户核心数据提供全生命周期综合性智能管理。产品主要包括数据安全运营管理平台 DSOP、数据安全态势感知平台 DSSA、数据安全分类分级系统 DSCG、数据安全智能管理平台 DSIP。

1、数据安全运营管理平台 DSOP

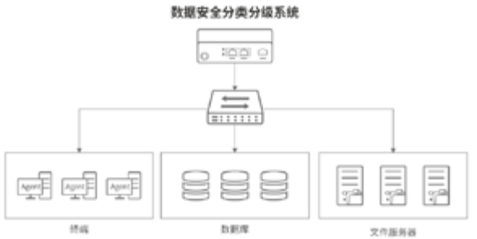
平台采用大数据技术架构、基于 AI 算法，通过采集分析各类安全设备日志，以人员和终端行为分析为主线，探测发现威胁企业的数据安全事件，并提供完整追溯取证证据链，全面保障客户数据安全，有效预防、阻断或减少安全威胁事件的发生，实现可视、可管、可控、可溯。

2、数据安全态势感知平台 DSSA

平台对数据安全产品的数据及日志进行统一收集，通过 AI 算法分析各类事件日志，并将多种异构数据进行归一、聚合、关联分析，感知数据资产当前所面临的威胁，并预测数据资产风险，以整体态势感知当前企业数据安全。

3、数据安全分类分级系统 DSCG

系统提供敏感数据识别规则和数据分类分级标准的管理功能，为资产敏感数据发现与分类分级打标提供依据。以资产发现 - 资产梳理为核心，以资产可视 - 资产可管为目标，致力于提升企业对数据资产的整体管控能力和运维效率。



4、数据安全智能管理平台 DSIP

平台融合机器学习、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数据安全防护产品，以数据为中心，分类分级为基础，为用户数据资产提供事前主动防御、事中实时监测、事后追踪溯源、全程态势感知，基于数据的全生命周期提供全方位、立体化防护。

作为数据安全领域代表厂商，亿赛通站在数据安全高速发展的浪潮中，公司上下始终认真落实国家相关政策决策部署，以最高质量、最严标准持续提升客户数据安全运行和服务质量。在这数字经济赋能产业转型升级的新时代，我们会从严从紧守好最后一道安全阵地，为党的二十大奋进新征程提供坚实可靠的数据安全堡垒，为企事业单位的数据安全持续贡献力量！

喜迎二十大 | 护航数据安全建设
第二期：详解数据安全治理

二十大顺利召开已过半，此前，在习近平总书记关于网络强国的重要思想指引下，我国网络安全工作取得显著成绩，网络安全和信息化一体推进、共同发展，国家网络安全屏障不断巩固，网络安全技术和产业蓬勃发展。数字化进程的加速得益于我国大力推进物联网、区块链等新技术新应用，坚持创新赋能，激发数字经济新活力，数字生态建设取得积极成效，同时在疫情的倒逼下，各行各业加速了数字化进程，“万物互联”势不可挡，然而，数字经济快速的发展也给数据安全带来了前所未有的挑战。

据某机构调研显示，2021 年全球公开披露的数据泄露事件 4145 起，共导致超 220 亿条数据泄露。在企业中，数据的存储、流转、共享已成为常态，一方面信息共享、互联网化、云服务、AI 等高新技术的追求延伸出新的信息安全风险点；另一方面系统多方互通、安全边界模糊，难以系统化设置复杂应用场景中的最小化控制、访问控制及数据持续防护安全策略。

为进一步减少数据泄露情况，国家陆续出台《网络安全法》《数据安全法》《个人信息保护法》等法律持续健全我国数据安全法律法规矩阵，构建了网络空间治理和数据保护的基本法，数据安全步入了强监管时代。

企业面对众多且仍持续颁布的法律法规，需要积极响应相关法律法规及相应的标准规范，落实不同维度、不同侧重的各类治理要求，实现一致性的合规治理。企业数据量大、数据结构复杂，海量多源异构的原始数据量难以对每一条数据进行分类分级管理，导致重要数据识别困难，这是企业当前数据安全治理工作面临的问题。

在亿赛通的观察中，多数客户开始关注从公司内部运营顶层设计的角度建设自己的数据安全治理体系。习近平总书记也曾多次公开强调，网络安全要注重顶层设计，亿赛通响应国家号召，自研自创一整套从上到下的综合数据安全治理解决方案。

我司认为数据安全治理以“人”和“数据”为中心，基于数据安全合规要求、用户的业务发展需要和风险承受能力等多重因素，通过平衡业务需求与风险，制定数据安全策略，对数据分级分类，对数据的全生命周期进行管理，从技术到产品、从策略到管理，提供完整的产品与服务支撑，实现业务与安全的深层融合。

在人为层面，从决策层制定经营策略、IT 策略，帮助企业用户建立数据安全意识，区分职责权限，对企业重要数据进行识别、分类分级、关联分析、追踪溯源、安全态势分析、风险评估等服务，高效理清数据资产，为企业重要数据资产的保护提供专业建议。

在数据层面，运用专业技术支撑，配合数据安全检查工具，通过 AI 算法，关联分析、密码技术、访问控制、数据标识等技术，采集分析各类安全设备结构化和非结构化日志，探测、预测、发现威胁事件和风险，利用技术服务于制度，进而形成技术、制度不断迭代的正循环，建立全面综合数据安全治理能力。

整个数据安全治理过程从决策层到技术层，从管理制度到技术支撑，将现有的各个独立的数据安全技术和功能整合，为用户提供跨数据类型、存储孤岛和生态系统集成数据的产品和服务，从而实现更简单、一致的端到端数据安全，如亿赛通自创自研的数据安全运营管理平台、数据安全态势感知平台、数据安全分类分级系统、数据安全检查工具、血缘关系分析工具、企业重要数据识别。构建了自上而下、全流程、可闭环的完整链条。相较于传统数据安全方案，亿赛通数据安全治理存在更高水平的集成能力、简化的部署模型，统一的策略控制平面，以及对数据、存储、政策和适用法规的一致可见性。

数据已然成为新时代的重要生产要素，为企业业务数字化转型中的重要资产。亿赛通承诺，我司将持续履行中国数据安全专家之责，担当起保护数据所有者信息资产安全之任，帮助企事业单位切实做到数据资产可视、数据威胁可管、数据风险可控、数据血缘可溯。

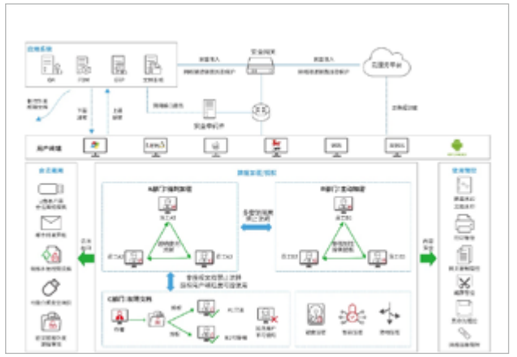
值此二十大胜利召开之际，亿赛通面向央企、国企、大型企业、上市公司推出免费“企业重要数据识别计划”，帮助企业对重要数据进行扫描识别、分类分级、血缘分析、追踪溯源、安全态势等服务。

喜迎二十大 | 护航数据安全建设
第三期：数据安全防护

中国共产党第二十次全国代表大会已经进入尾声，不少不法分子盯紧这一盛事，背后的小动作层出不穷。企事业单位到底该如何完善数据安全体系建设，以顶层设计统筹数据资源，让数据持续发挥其应有的价值显得尤为重要。

数据安全对企事业单位来说不仅仅是查缺补漏的工具，而是一个稳健发展的前提。数字化的发展使得数据安全需要一个全新的理念进行整合。除了黑客、漏洞和攻防问题，企业更多面临的是数据在产生、存储、流通中的安全问题。亿赛通结合自身优势及用户业务需求，从数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务等方面，建立数据安全综合解决方案。

基于在数据安全防护市场近二十年的经验，亿赛通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。在终端层，基于数据内容进行全量、增量、定期、周期性扫描，对数据进行识别与检测，按照数据分类分级标准制度对数据进行分类分级管理，实现加密、外发审计、审批和阻断管理等措施；在网络层内置全球 IP 地址库，将数据访问发起端和响应端进行 IP 地址比对，识别数据的违规流转、跨境传输、非法出境状态记录、风险告警及流转阻断限制；在数据分散存储时，在终端、服务器端、云虚拟环境、网络端、邮件端可进行全覆盖多点部署，有力保证企业的数据安全建设。亿赛通数据安全防护工具主要包括：新一代数据泄露防护 DLP、终端数据安全管理平台 TDSP、新一代电子文档安全管理系统 CDG、零信任访问控制系统 ZT-ACS、数据追踪溯源系统 TIS、商业秘密管理系统 TSM。



1、新一代数据泄露防护 DLP

基于终端、网络、邮件、存储扫描等应用场景，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数据安全防护产品。系统以数据为中心，分类分级为基础，为用户数据资产提供事前主动防御、事中实时监测、事后追踪溯源、全程态势感知，对数据的全生命周期提供全方位、立体化防护。

2、终端数据安全管理平台 TDSP

以“主动防御”为基础，采用模块化的方式实现对各个产品的功能集成；囊括了数据加密、数据泄露防护、桌管、水印、用户行为分析、商业秘密管理、数据追踪溯源等核心安全产品。各业务系统由终端平台统一管理和授权，形成动态扩展产品功能；实现操作系统安全加固及数据文档的自主、可控、可管理，保障终端数据安全，实现终端全方位安全防护。

3、新一代电子文档安全管理系统 CDG

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”两种数据泄漏行为作统一防护，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。

4、零信任访问控制系统 ZT-ACS

针对企业数据边界不清晰、云环境数据部署场景与零信任架构设计。摒弃了传统以网络为中心的被动打补丁的护城墙安全模式，转而以身份为中心进行动态访问控制，客户端作为本系统的唯一登录入口主要实现客户端和控制器之间可信身份认证；控制器根据客户端采集信息对用户 / 应用等进行动态授权，控制器是整个系统的决策中心，提供账号管理、权限管理、终端管理及策略管理，进行集中的应用访问控制，真正做到“主体身份可信、访问操作合规、数据有效防护、行为操作审计”。

5、数据追踪溯源系统 TIS

通过机器学习、大数据分析、溯源取证等技术，对用户、数据、应用、设备进行综合分析，将每一次数据活动与实际用户、设备和应用程序进行关联的数据资产管理和用户行为分析产品。帮助客户进行数据资产管理，勾画员工行为画像，为企业解决数据泄密、内部恶意行为等威胁行为，为企业提供数据资产的实时监控，保护企业数据资产安全。

6、商业秘密管理系统 TSM

用于保护企事业单位商业秘密的安全管理软件，针对安全保密工作中，“定密难，保护难，实施难”等实际问题，调整传统死板的工作方式，通过“以事定密、 以密找人、以人保密“的保密原则，帮助用户实现精准数据定密、定密数据与用户绑定、落实用户责任和义务，从而实现了“员工依技防密，单位依规管密，单位依法治密”的闭环化商业秘密保护管理模式。

时移世易，二十大后，新的经济形势将出现，数字化进程的加速，业务需求的改变，对安全厂商的考验增加。完全完备的防御手段，对于企业而言也是不可或缺的，应当引起更多的重视，对于企业而言数据安全防护并不是小事，及早防范，更早受益，尽可能尽善尽美，才能为企业后续的发展建设夯实基础。

亿赛通小贴士 ESAFENET PROMPT

护航数据安全建设第五期：数据库安全

根据近两年的数据泄露数据显示，国内外每个月发生不少数据泄露事件，数据泄露给人们生产生活带来的恶劣影响不容小觑，数据安全问题已成为广大人民群众最关心、最现实的利益问题之一。

随着国家相关部门出台一系列政策法规保障数据安全，规范数据处理活动，保障数据安全，保护个人、组织的合法权益，维护国家主权、安全；近期，《网络安全法》迎来首次修订，企业安全重视程度再获提升。

企业大量高价值数据以各种形式存放于数据库，数据库安全问题长期以来都是信息安全行业的一大挑战。面对愈发复杂的部署环境，为了更好应对数字经济时代下数据库的安全问题，亿赛通将数据库安全系列产品进行全面更新，为用户提供更直观、高效、可靠的数据库安全防护方案。

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。数据库全系列产品包含：数据库安全防护平台 DBSP、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、易数保 EDG。

数据库安全防护平台 DBSP

亿赛通数据库安全防护平台（简称：DBSP）是一款集成数据库审计、阻断和脱敏功能的综合性数据库安全防护系统，利用审计引擎通过旁路采集数据库网络流量对数据库操作行为进行审计，利用防护和脱敏引擎串接于数据库前端实现对高危数据库操作的实时阻断和对敏感数据访问的实时脱敏，从而达到对数据库安全的实时保护，系统还对数据库历史访问行为和风险操作进行多维度统计，并利用丰富图表进行可视化展示和智能分析。

数据库安全审计系统 DAS

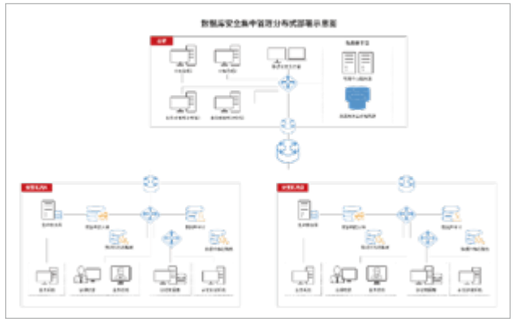
亿赛通数据库安全审计系统（简称：DAS）是一款通过对数据库网络流量旁路采集，基于数据库协议解析和 SQL 语句还原技术的数据库安全审计系统。系统实现数据库访问行为的监控和审计，并对其中危险操作向管理员实时告警提醒；系统还对数据库历史访问行为记录进行多维度统计分析，并利用丰富图表进行可视化展示。系统独立于数据库进行和部署和配置，无需应用系统和用户网络环境改造，提供可靠数据库安全审计服务。

数据库防火墙系统 DFW

亿赛通数据库防火墙系统（简称：DFW）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。

数据运维安全管理系统 DOSM

亿赛通数据安全运维系统（简称：DOSM）是一款具备全面运维管理、数据资产监控、安全合规审计等多能力、综合性数据安全产品。产品可规范数据运维操作流程，监控分析运维活动，主动防御风险行为。产品可进行独立部署与配置，最大限度不改变现网环境的前提下达到运维管理、安全防护和分析溯源的目的。



易数保 EDG

亿赛通易数保产品（简称：EDG）是一款利用数据库流量采集，基于数据库协议解析和 SQL 语句还原技术的轻量安全审计系统。系统在充分理解客户业务系统特点的基础上，针对性的解决工业企业在使用业务系统过程中的数据防泄露、操作事件溯源及合规方面的实际问题。系统对所有数据库访问行为进行监控和审计，识别风险操作并实时告警提醒，对数据库历史访问行为进行多维度的统计分析，利用丰富图表进行可视化展现。

亿赛通数据库安全系列产品自推出以来，受到市场和用户的广泛肯定。未来，亿赛通也将持续加强产品研发和创新，更好的、更切实的满足不同行业、不同客户需求，全力守护数据资产安全！

护航数据安全建设第六期 | 数据库安全五件套之数据库安全防护平台

数据，这个时代的巨量产物，珍贵而无价。企事业单位越来越多的将安全的关注重点从传统的边界安全转移到数据安全，保存核心数据资产的数据库系统，毫无疑问的成为防护的关键。作为数据库重要的防御工事，数据库防护获得了更多的关注。因为数据库肩负的重任，社会对于它的安全要求也更加严苛。亿赛通凭借自身专业技术、实施经验、创新能力，自创自研数据库安全五件套产品，今天，我们来了解一下数据库安全防护平台。

亿赛通数据库安全防护平台（简称：DBSP）是一款集成数据库审计、阻断和脱敏功能的综合性数据库安全防护系统，利用审计引擎通过旁路采集数据库网络流量对数据库操作行为进行审计，利用防护和脱敏引擎串接于数据库前端实现对高危数据库操作的实时阻断和对敏感数据访问的实时脱敏，从而达到对数据库安全的实时保护，系统还对数据库历史访问行为和风险操作进行多维度统计，并利用丰富图表进行可视化展示和智能分析。

1、产品价值

满足合规需求

帮助客户满足等保分保和行业数据安全合规需求。

提高监管能力

实时监测数据库风险行为，提供风险趋势分析，帮助客户掌握数据库运行安全状态。

全面阻断风险

提供 SQL 注入、数据库漏洞和风险操作等攻击行为的实时检测和阻断能力，提供敏感数据实时脱敏能力，保护数据库安全。

综合数据安全

多维度保护数据库安全，既能实时阻断数据库高危操作请求，也能对返回结果敏感数据实时脱敏，还能利用全量数据库操作记录进行多维统计和智能分析，实现风险趋势的预测。

2、产品优势

全面记录访问行为

平台基于数据库协议解析和专业的 SQL 语法、词法分析，提供全面的数据库访问审计能力，具体表现在以下几个方面：

- 支持的数据库类型全；
- 解析的 SQL 语句类型全；
- 记录的审计日志内容全；
- 全面支持 IPv4、IPv6 协议。

事前中后纵深防护

平台通过数据库资产扫描组件发现数据库资产分布、使用、数据流向及数据安全状态，通过数据库风险扫描组件发现潜在的数据库漏洞风险，实现事前防御。

平台利用数据库防护，阻断高危风险数据库操作；通过数据脱敏，对数据的敏感信息进行有效遮蔽，防止敏感信息外泄，实现事中控制。

平台利用数据库审计组件全量日志记录，对风险事件操作进行还原，审计三层关联功能，精确定位到实际终端用户，解决追责到人的难题。

智能规则联动分析

平台利用融合的智能管控技术，将数据库安全保护从单点保护演进为整体保护，并形成数据库安全保护中各安全产品和组件的智能联动。

一方面，通过数据安全智能扫描，获取重要数据的静态存储位置和动态数据流动路径。系统根据获取相关信息制定针对性的数据安全保护策略，自动向数据保护产品和组件下发对应的数据保护，包含审计、阻断以及脱敏的规则，从而实现对重要数据的保护。

另一方面，通过全量的数据审计以及制定的审计规则监测并发现风险数据操作，对高风险操作通过平台直接向数据库防护引擎下发阻断指令，阻止危险数据操作的执行，从而保护数据库的安全。

3、关键功能

数据库资产自动发现

系统通过对数据库网络流量的采集和数据解析，利用各数据库类型私有通信协议各自特征，实现对不同类型数据库的自动识别，同时还可从协议内容获取到更为精确的数据库参数，比如数据库版本号、协议版本号、通信端口等信息。

数据库访问行为记录

系统支持多种国内外主流数据库类型，采用旁路镜像或者软探针方式采集数据，经过对数据库私有通信协议的解析和 SQL 语法分析，获取数据库会话和操作行为相关信息，形成数据库操作行为记录，保存信息日志。

数据库运行状态监控

系统对数据库操作访问行为进行全面监控，实时掌握数据库访问状态，监控数据库访问源、访问工具和访问路径，对数据库运行状态进行风险和性能评估，提前对数据库运行状态进行预警。

数据库精细权限控制

针对数据库管理对象，提供独立的第三方权限控制管理能力。可针对数据库表级别提供精细化的访问权限控制，授权对象除了基本的数据库用户以外，还可以对数据库连接客户端进行权限控制，同时可设置权限规则的时间周期及有效时间范围。

数据库入侵行为阻断

平台提供业界最为全面的数据库攻击行为检测和阻断技术，包括：

1. SQL 注入禁止技术：提供 SQL 注入特征库；
2. 虚拟补丁技术：针对 CVE 公布的漏洞库，提供漏洞特征检测技术；
3. 高危访问控制技术：提供对数据库用户的登录、操作行为，提供根据地点、时间、用户、操作类型、对象等特征定义高危访问行为；
4. 返回行超标禁止技术：提供对敏感表的返回行数控制。

敏感数据多类型脱敏

对于数据库存放的敏感数据，通过此功能将数据脱敏，在数据安全的前提下，保障业务的正常开展。脱敏类型包括:

1、业务脱敏

可对不同业务系统帐号进行脱敏，在业务系统本身无法限制业务人员查询信息时，可通过数据动态脱敏系统针对不同业务人员进行访问权限管控。

2、运维脱敏

对于 DBA 等数据运维人员，可限制其在操作某些敏感表或越权操作其他数据表时，返回的数据为非真实数据，并且对于运维人员恶意或过失的高危操作时进行阻断，防止其危害数据库。

数据库风险统计分析

系统对数据库审计对象提供多维度统计功能，分别从风险、语句、会话和访问来源多个层面进行统计与分析，帮助用户高效地掌握数据库运行安全态势并快速锁定风险目标。

数据库审计合规报表

系统内置丰富的报表模板，满足等级保护、SOX 法案等法规标准对信息系统的审计需求。另外用户也可以根据自身的实际需求选择审计对象、报表内容和审计周期，编辑并生成自定义审计报表。

国内曾有发布报告称，国产化兼容中最具弹性的是数据库，在国内数据库这个百亿级的大市场里，国外品牌占有 90% 以上份额。结合已有资料与产业调研，国内数据库市场规模约 300-400 亿元 / 年，国产化数据库替换市场总体存量规模约 3000 亿元。亿赛通数据库全五件套产品与国内极具实力的多家数据库厂商完成国产化兼容认证，如：达梦、人大金仓。并且相关产品已取得国产化相关资质。

数据库作为业务系统数据的重要载体，若其安全防御不完善、防护强度不够，将可能成为攻击者的重要突破口，对此，亿赛通建议各行业用户单位进行数据库防护建设，加大数据库的安全防护投入，保证核心业务数据库在安全状态下正常、高效的运行。

某国有银行新一代数据防泄露防护案例

场景介绍

由于自身数据安全需要以及监管机构对行业数据安全监控要求。为解决办公终端、存储、网络、邮件以及其它应用软件传送敏感数据可能产生的泄露风险。银行启动数据泄露防护建设。在全集团范围内对办公网、研发网、生产网的终端、网络、邮件、存储设备实现数据防泄露的统筹建设和统一管理。

客户需求

1、 实现全集团范围内的立体联动，同时支持信创终端。对常用办公软件，如：Office、WPS、PDF、Zip、7Z、.C/C++、Python、IDEA、eclipse、点钞机、清分机等产生的文件进行内容识别或过滤，实现全网数据立体发现和泄漏风险防范预警。

2、 实现终端、网络、应用数据防泄露统一管理，通过数据挖掘和关联分析，形成以“人“和敏感数据为主线的泄露风险关联和画像，预防和追溯泄露风险；

3、 客户另外对新一代数据泄露防护系统和管理服务器集群的高可用性、易用性等方面提出需求；

解决方案

双方根据项目需求，经过多轮沟通讨论，最终确定采取总分的分布式部署。系统集群部署实现高可用性，保障业务连续性，产品易用性按照一般习惯性操作方法针对使用场景和操作习惯进行修改。同时，把数据防泄露的事件、预警和日志接入新系统，通过与客户 OA 系统对接实现组织架构同步和登录认证。

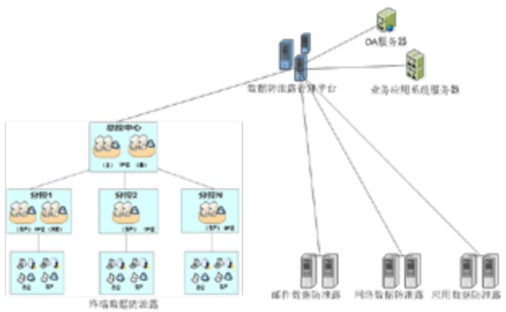


图 1 新一代数据泄露防护系统

新一代数据泄露防护系统部署逻辑拓扑如图 1 所示。把终端、邮件、网络和应用数据统一管理和展示，通过综合关联分析其数据泄露事件风险，形成用大屏展示以“人“和敏感数据为主线的泄露风险和轨迹。对终端电脑上发现的数据提脱敏、删除、加密等处理方法，并将处理结果上报，管理员可以对处理情况进行检查和管理反馈，实现敏感数据滚动迭代的常态化检查和效果评估。邮件、网络、应用数据防泄露采用热备部署方式，实现业务连接性。

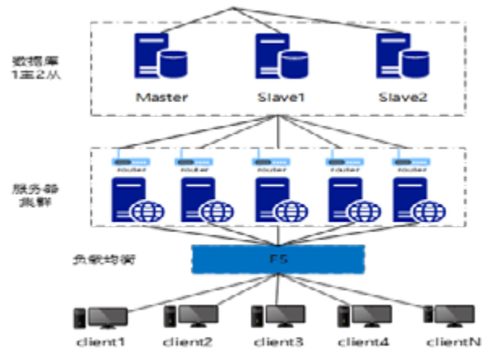


图 2 分控中心管理服务器部署拓扑

在数据防泄露建设中，分控中心的服务器集群部署如图 2，应用服务器负载均衡，数据库主从模式。实现服务器高可用性。先盘点存放的数据文件情况，按照“应删尽删”原则对涉敏文件进行治理。同时，若确因工作需要存放数据文件，采取加密授权进行密文存放，并根据重要性对密文的使用范围、操作权限进行设置。另外，文件加密授权可设置有效期，当该文件达到有效期后不能再被使用。

方案在操作系统的适配性和稳定性、终端扫描的速度提升、电脑终端与使用电脑的用户分离、权限文件处理机制的稳定性、数据安全全员可参与执行的技术实现，以及服务器的高可用性和稳定性等方面在产品方案的基础上进行了明显地创新和提升。图 3 分别给出大屏、“人”的轨迹画像、事件关联、终端和网络的展现示例。

“人”的轨迹画像

事件关联

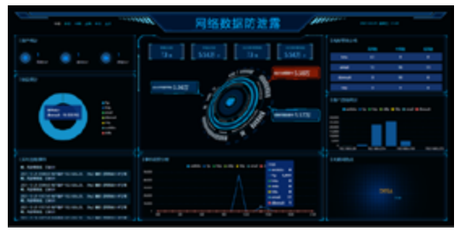


图 3 新一代数据泄露防护系统示例展现

方案价值

1、 立足产品方案制定项目方案，围绕以客户为中心的企业价值观。

2、 方案围绕银行项目实际，在保持总体目标不变的前提下。针对客户关注的安全风险调整项目步骤，首先解决客户面临的重点风险。分阶段按步骤排序制定项目计划并组织实施。

3、 在满足监管合规的基础上，对终端、网络、应用间的数据流转使用方面的安全要求，以及技术措施方面具备实际应用价值。

4、 通过系统实现数据防泄露的综合关联，满足跨产品的扩展联动。

5、 通过项目的制定和组织实施，逐步形成满足客户实际的数据防泄露解决方案。由于其场景的复杂性和客户需求的代表性，为同类客户的数据防泄露建设提供较好借鉴。

总结

亿赛通围绕新一代数据泄露防护产品强化创新，通过网络、终端、邮件、存储扫描防泄露产品的组合构建屏障，对受控区域内的数据文档进行深度解析、内容还原和敏感度扫描，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。该产品为数据安全防护提供了一个完整、可落地的综合解决方案。

某制造业数据安全管理认证案例

1、案例背景

随着各行业数字化转型升级进度加快，特别是 5G、人工智能、物联网等新技术的快速普及应用，全社会数据总量爆发式增长，数据存储、计算、传输和应用的需求大幅提升，数据安全建设已成为支撑各行业“上云用数赋智”的重要新型基础设施。

大数据、人工智能的广泛应用虽然打通了数据孤岛、实现了数据共享，但数据的非法调用以及数据的滥用带来了更严重的数据安全问题：数据价值被提炼，核心资产被泄露。由于电子信息传播途径广、传播速度快、拷贝 / 复制操作无痕迹及易携带等特性，普通的网络边界防护措施已无法有效控制有内部人员参与的泄密事件的发生。根据国家安全机关的统计，现在泄密事件超过 80% 的发生均与内部人员有关，暴露出了内部监管手段的薄弱以及安全管理体系的缺乏。

2、解决方案

数据安全合规评估

为客户持续提供业务流程风险梳理、现有管理制度存在的漏洞、流程管理制度是否得到执行。认知关键数据资产：实现关键数据分类分级，制定关键数据管理要求、梳理关键数据责任矩阵，制定关键数据管理矩阵，梳理关键数据资产：网络关键数据自查，重点业务对照自查，关键数据安全现状，不达标项跟踪整改。

海量数据风险识别

现代信息化建设中，任何业务的运行都离不开网络。网络使用率越高，其数据泄露风险概率也越大。通过网络外发途径众多，数据中心应该重点关注网络边界的监管建设，基于核心数据重要程度，对不同级别的核心数据进行不同的响应处理方式，形成针对网络传输中海量数据的风险识别能力。从泄密源头管控、防止数据泄露发生。同时监控核心数据流通过程，掌握数据流向，实现对数据的全程监管需求。为用户的数据外发把好最外层的安全防护门。

核心数据加密保护

通过透明和非透明、半透明三种模式对核心数据加固防御，实现数据产生、使用、传输、外发、存储、销毁各环节安全防护。比如日常工作中起草的重要公文，通常都是以 word、pdf 等形式存储。在公文传递及使用中，因未对其进行主动防御加固，比如文档加密或者权限管控，公文很容易被黑客或非法人员窃取。

敏感数据访问审计

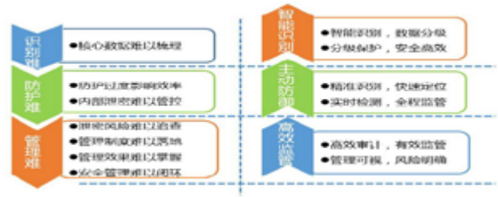
针对业务环境下的数据库操作行为进行细粒度审计并合规管理，通过对业务人员访问数据库的行为进行解析、分析、记录、汇报，用来帮助用户事前规划预防，事中实时监视、违规行为响应，事后合规报告、事故追踪溯源，同时加强内外部网络行为监管、促进核心数据资产的正常运营。

数据安全态势感知

通过数据安全运营管理平台建设，掌握核心数据分布、流向、外发等情况。量化数据安全防护成果，提升安全管理工作的管理效率。使数据安全态势变得可视化，数据泄露风险分析变得有据可依。方便管理者进行事件查看分析及处置。

3、案例优势

通过应用亿赛通综合数据安全解决方案，实现安全管理与技术手段相结合的目的，通过事前主动防御、事中检测响应、事后追踪溯源、全程态势感知的整体防护理念，帮助用户建立完善的整体数据安全管理体系。实现数据泄露防得住、数据风险看得见、安全管理好落地的整体效果。



4、案例效果

数据全生命周期风险评估

数据全生命周期安全评估指从数据的产生、使用、传输、共享、存储和销毁六个存在的状态进行评估，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，在设计和制定数据保护管理制度以及技术措施时，融入和覆盖数据全生命周期的各个环节。

海量数据安全防护

根据数据安全方案建设，通过技术手段发现数据泄露风险，对日常的核心数据使用进行审计监测。精准定位泄露风险与隐患，帮助安全管理者明确数据安全防护重点，风险重灾区。实现对网络传输数据的安全管理，实现包括 SMTP、FTP、HTTP、IM、HTTPS、SMB 等大量的常用传输协议。实现从泄密源头管控、防止数据泄露发生。同时监控核心数据流通过程，掌握数据流向，实现对数据的全程监管需求。

存储数据安全防护

方案提供的检测手段包括实时分析以及数据发现。实时分析针对当前被访问的文件或者内容，通过快速的检测得到结果。数据发现则是面向存储容器中大量的数据而言，通过一定的扫描方式定位敏感数据的位置，提前对敏感数据进行梳理，做好相应安全防护措施。

业务系统安全防护

通过应用系统安全准入控制，可以实现对内部业务系统的准入防护或者业务系统中数据的存储保护。

保护内部合法人员正常访问数据中心业务系统的需求，对于非法访问和恶意访问行为，通过安全准入控制阻止其对数据中心内部系统造成威胁。

通过对业务系统中数据加密、解密来保护业务系统中存储的数据安全，以及离开业务系统后数据在终端的使用安全。

数据库安全防护

数据库审计与溯源系统还原网络流量中的数据库语句操作，提供全流程语句操作审计，并内置漏洞模型与 SQL 注入模型，可对侵入行为进行审计与告警，风险事件发生后可根据审计日志进行溯源追责。

数据库安全防护与控制系统可进行访问权限控制，阻止高危操作，并结合虚拟补丁功能，保障中心数据库的业务调用及运维安全。

数据库敏感数据共享防护主要通过敏感数据匿名化、去标识化等技术解决数据在开发测试、交换、分析、共享环节中敏感数据安全风险，有效避免敏感数据泄露，同时满足数据共享、数据挖掘、数据分析等场景的使用需求。

数据安全可视化

数据安全运营管理平台提供了丰富的可视化界面，方便管理者进行事件查看和分析。每一个安全事件不仅记录了事件摘要，也包含了详细内容，可以完整追溯。整体可视化界面可以体现多层面多场景的数据管理效果以及风险趋势分析效果。最终实现数据风险看得见、数据安全看得见的效果。