亿赛通 ESAFENET

ESAFENET

亿赛通企业月刊　　中国数据安全专家　　www.esafenet.com

12月刊

2022 年共 11 期



联系我们

地址：北京市海淀区西二旗大街 39 号 A 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com

关注官方微信公众号　关注官方微信服务号　关注官方微信视频号　关注官方抖音号

Esafenet
Monthly magazines

中国数据安全专家

主办：亿赛通市场部

北京亿赛通科技发展有限责任公司

地址：北京市海淀区西二旗大街 39 号 A 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com



本刊为亿赛通企业月刊，欢迎交流，禁止转载

CONTENTS 目录

刊首语 PREFACE

2/3 《亿赛通十一月刊》详细揭秘企业的数据安全治理

行业聚焦 INDUSTRY FOCUS

4 国内行业新闻

5-9 国外行业新闻

亿赛通动态 ESAFENET NEWS

10/11 荣耀登顶 | 亿赛通蝉联中国数据泄露防护市场占有率第一

12/13 喜提“金帽子” | 亿赛通荣获 2022 网络安全金帽子年度最佳行业解决方案

14/15 首批入选，网络安全技术与产业发展工业和信息化部重点实验室专项工作组成员名单公布

16/17 星河璀璨 | 亿赛通解决方案荣获中国信通院 2022 大数据“星河”优秀案例

18/19 权威认证：亿赛通安全管理平台成功通过信通院“可信数安”分类分级评估测评

20/21 为亿赛通点赞 | ISC 2022 数字安全创新能力百强亿赛通成功上榜

22/23 又一荣誉榜单实力加冕，亿赛通入围《嘶吼 2022 中国网络安全产业势能榜》

24/25 《ISC 数字安全创新案例报告》发布，亿赛通深挖能源行业新需求，赋能企业安全建设

26/27 2022 年度中国数字安全能力图谱（精选版）| 亿赛通抢占多个细分领域

28/29 2022 年度十大重点成绩单

亿赛通小贴士 ESAFENET PROMPT

30/31 护航数据安全建设第十六期 | 数据安全治理之数据血缘分析系统

31-32 护航数据安全建设第十七期 | 数据安全防护之终端数据安全管理平台

33-35 护航数据安全建设第十八期 | 数据安全防护之新一代电子文档安全管理系统

36/37 护航数据安全建设第十九期 | 数据安全防护之新一代数据泄露防护系统

38/39 护航数据安全建设第二十期 | 数据安全防护之零信任访问控制系统

40-42 护航数据安全建设第二十一期 | 数据安全防护之数据追踪溯源系统

43-44 护航数据安全建设第二十二期 | 数据安全防护之商业秘密管理系统

45-46 护航数据安全建设第二十三期 | 数据安全流转之数据脱敏系统

47 国际乒联服务器出安全问题，数百名乒乓球运动员信息泄露

48/49 国际数据安全市场研究之蓬勃发展的数据安全行业

50-53 政策解读：《工业和信息化领域数据安全管理办法（试行）》

典型案例 TYPICAL CASES

54/55 某储蓄银行数据库安全项目案例

56/57 云数据安全解决方案



告别 2022，拥抱 2023 | 《亿赛通十二月刊》感谢有你，同心同行

刊首语 PREFACE

不觉间，2022 年已经向我们挥手告别。今年，我国数据和网络安全行业经历了形态严峻的发展挑战，不仅要应对数量快速增长的安全风险，还要积极应对各项行业政策、标准带来的合规要求。在这样的大环境中，数据和网络安全厂商需要重新制定战术与策略。

亿赛通作为综合数据安全厂商，本年度在 “分·放·管·服”数据安全建设理念的基础上，细分数据安全治理、数据安全防护、数据安全流传、数据库安全、安全服务五大产品类别，确保数据全生命周期可以有价值的安全流转。2023 年，亿赛通愿与全国新老客户、代理商、合作伙伴及同事们携手新一代数据安全技术，同心同行，协同发展，共同见证产业大变革，数据安全产业发展助力！

国内

1、用软件测颜值？小心隐私泄露！他用伪装软件偷了 1751 张照



摘要：网络科技有限公司软件开发人员李某制作了一款可以窃取安装者手机内的照片的软件，在暗网某论坛售卖。此后，为炫耀技术、满足虚荣心，李某又将其伪装成“颜值检测”软件，以此窃取安装者手机相册照片 1751 张……2022 年 12 月 7 日，最高检发布检察机关依法惩治侵犯公民个人信息犯罪典型案例，其中就包括这起“李某侵犯公民个人信息案”。

2、《关于构建数据基础制度更好发挥数据要素作用的意见》发布

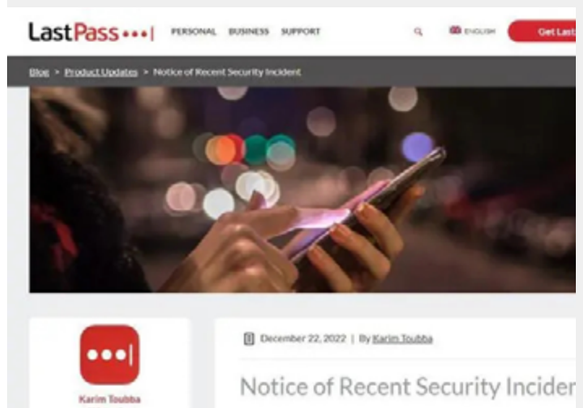
摘要：12 月 19 日，数据要素领域的重磅文件《关于构建数据基础制度更好发挥数据要素作用的意见》（下称《意见》）出台。《意见》指出，数据基础制度建设事关国家发展和安全大局。为加快构建数据基础制度，充分发挥我国海量数据规模和丰富应用场景优势，激活数据要素潜能，做强做优做大数字经济，增强经济发展新动能，构筑国家竞争新优势，提出相关意见。

国外

1、美国联邦贸易委员会与 Epic 达成和解

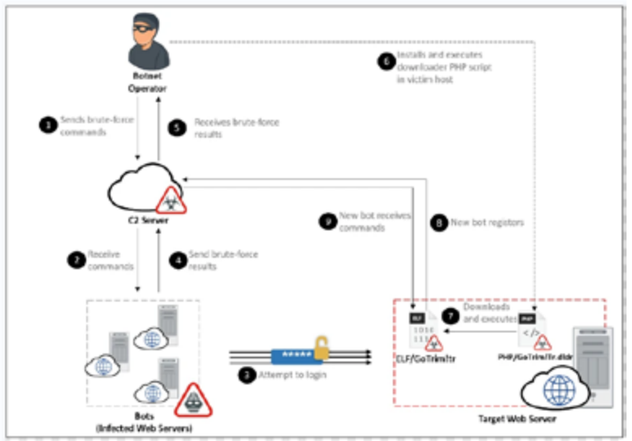
摘要：近日，美国联邦贸易委员会（FTC）已经与《堡垒之夜》等热门游戏的开发商 Epic Games Inc.（Epic）达成和解协议，该公司被指控违反了《儿童在线隐私保护法》（COPPA），并诱导数百万玩家进行计划外消费。Epic 将为此支付总计 5.2 亿美元。这 5.2 亿美元的总金额由两部分组成。一部分是因违反《儿童在线隐私保护法》，支付 2.75 亿美元和解金，这也是美国联邦贸易委员会历史上提出金额最高的一笔罚款。同时，监管还要求公司增强对未成年人的默认隐私设置，确保语音和文字交流默认关闭。另一部分的 2.45 亿美元，是由于公司诱导消费，用于向用户进行退款。这也是目前美国联邦贸易委员会在游戏案件中提出的最大退款金额。

2、LastPass：黑客获得云存储访问密钥，用户信息泄露



摘要：12 月 22 日，在线密码管理器 LastPass 称，有黑客获得了其客户的大量个人信息，包括加密和加密散列密码以及存储在客户保险库中的其他数据。根据调查，黑客利用在 LastPass 今年 8 月的漏洞事件中获得的信息访问了一个基于 云的存储环境。黑客通过一个受感染的开发者账户对 LastPass 开发环境部分的未经授权访问，并“获取了部分源代码和一些专有的 LastPass 技术信息”。通过攻击另一名员工账户，黑客又获得了用于访问和解密基于云存储服务中某些存储卷的凭证和密钥。

3、GoTrim：基于 Go 语言的僵尸网络会重点攻击 WordPress 网站



摘要：FortiGuard 实验室最近遇到了一个以前没有报道过的内容管理系统 (CMS) 扫描器和用 Go 编程语言 (通常也称为 Golang) 编写的攻击破解器。在几个在线论坛上，它被描述为安装在受感染的 WordPress 网站上，但没有公开的分析报告。

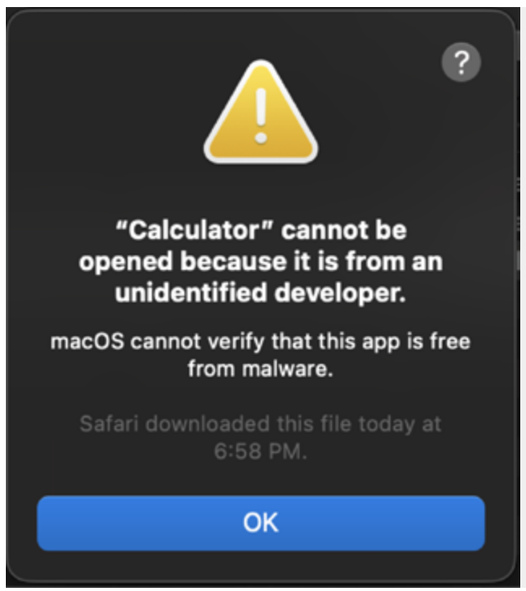
受影响平台：Linux；

影响用户：任何组织；

影响：远程攻击者可以控制易受攻击的系统；

严重级别：严重。

4、macOS 漏洞可绕过安全检查



摘要：微软首席安全研究员 Jonathan Bar Or 在 macOS Gatekeeper 中发现一个安全漏洞——Achilles，漏洞 CVE 编号为 CVE-2022-42821。攻击者利用该漏洞可以在有漏洞的 macOS 设备上绕过 Gatekeeper 的应用执行限制来部署恶意软件。

5、网络攻击者分分钟可将流行的 EDR 工具变成极具破坏性的数据擦除工具



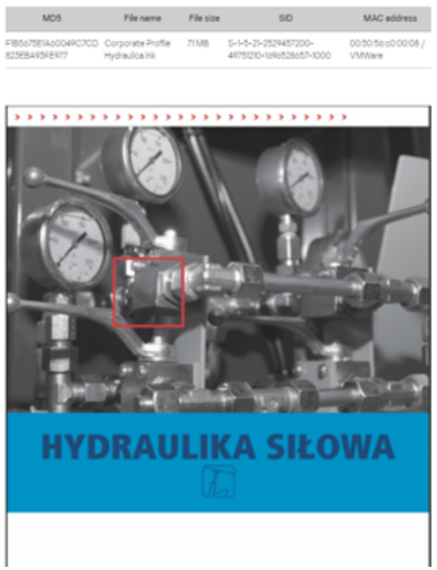
摘要：许多备受信赖的端点检测和响应（EDR）技术可能存在着一个漏洞，使攻击者得以操控产品，从而删除已安装系统上的几乎所有数据。Or Yair 是 SafeBreach 的一名安全研究人员，他发现了这个问题。他测试了多家供应商提供的 11 款 EDR 工具，发现其中 6 款工具（共涉及四家供应商）易受攻击。这些易受攻击的产品包括：微软 Windows Defender、Windows Defender for Endpoint、趋势科技 ApexOne、Avast Antivirus、AVG Antivirus 和 SentinelOne。

6、暗网市场：被盗的个人数据的销售额达到了数百万



摘要：据报道，生产者、批发商和消费者之间的这种数据交易是在暗网市场进行的，暗网市场是非法的网站，与其他合法的电子商务网站一样，只有通过特殊的浏览器或使用授权码的情况下才能进入。仅在 30 个暗网市场上，就发现了有数千名卖家在出售数以万计的被盗的数据。在八个月的时间里，这些数据零售商的销售额高达 1.4 亿美元甚至更多。

7、DeathStalker 使用 Janicab 新变种发起攻击



摘要：Janicab 于 2013 年作为能够在 macOS 和 Windows 操作系统上运行的恶意软件首次出现。Windows 版本将基于 VBscript 的植入作为最后阶段，而不是之前在 Powersing 示例中观察到的 C#/PowerShell 组合。到目前为止，我们确定的基于 VBS 的植入程序样本具有一家族版本号，这意味着它仍在开发中。总的来说，Janicob 显示了与其对应的恶意软件家族相同的功能，但不像 EVILNUM 和 Powersing 攻击那样在攻击生命周期的后期下载多个工具，分析的样本将大部分工具嵌入并混淆在滴管中。

8、勒索软件攻击迫使法国医院转移病人



摘要：由于周六晚上发生了一起勒索软件攻击，位于巴黎郊区的安德烈 - 米格诺特（André-Mignot）教学医院不得不关闭其电话和电脑系统。据这家医院的监事会联合主席 Richard Delepierre 声称，这起勒索软件事件的幕后攻击者已经索要赎金。目前，由于这家医院不得不取消了部分手术，只接受门诊和会诊。据法国卫生和预防部长 François Braun 声称，该医院还被迫将 6 名患者从新生儿和重症监护病房转移到了其他医疗机构。

9、勒索软件团伙攻击了 100 多个组织，获利超过 6000 万美元



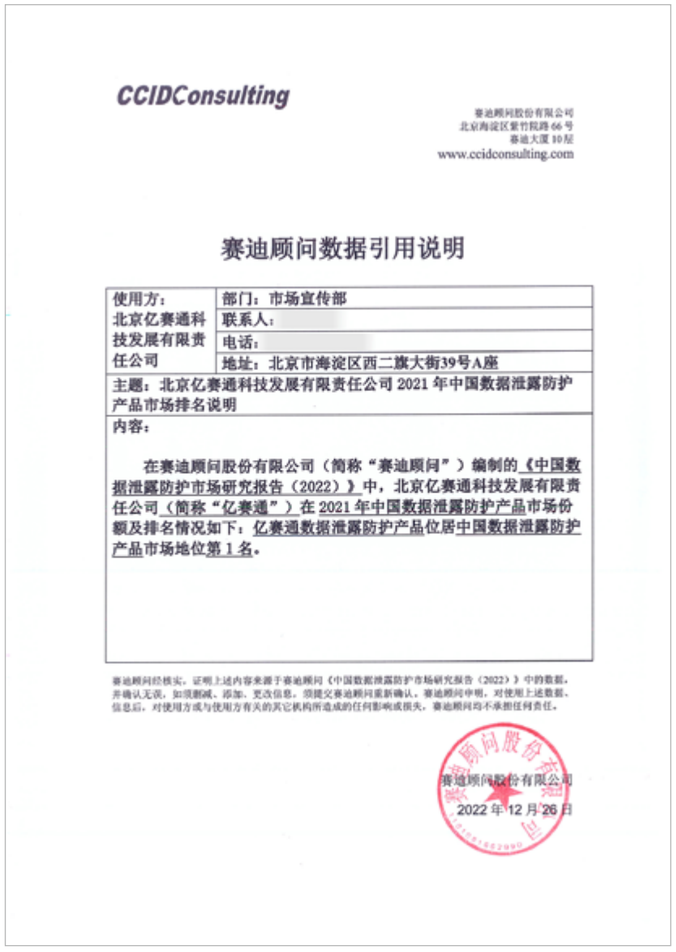
摘要：根据最近的一份联合网络安全咨询（CSA）#StopRansomware，来自 CISA 和 FBI 的警告说，Cube 勒索软件团伙已经攻击了全球 100 多个组织，并已经收到了超过 6000 万美元的赎金。Cube 勒索软件攻击的目标是医疗保健、关键基础设施、金融服务、政府服务等机构。CSA 说，尽管该团伙使用了这个名字，其实该团伙与古巴这个国家没有任何关联。联邦调查局警告说，该勒索软件团伙已经攻击了全球 100 多个目标，并要求支付超过 1.45 亿美元的赎金，现在已经得到了 6000 万美元的勒索款项。

10、UEFI 固件使用 OpenSSL 暴露了软件材料清单（SBOM）的弱点，戴尔、惠普和联想中招

OpenSSL 版本	模块
1.0.2j	DxeCore, Tcg2Dxe, TcgDxe, VariableSmm, SecurityStubDxe, IpSecDxe, IScsiDxe, Setup, PlatformMilestoneHookDxe, PlatformMilestoneHookSmm, LenovoTpmConfigDxe, PlatformInit, PeimBoardInit, PeimBoardInit, PeimBoardInit, Tcg2Pei, TcgPei, PlatformInitPreMem, LenovoPcdInit, LenovoVerifiedBootPei
1.0.0a	FlashUtilitySmm, LenovoCryptService, LenovoCryptServiceSmm, LenovoSvpManagerSmm, LenovoSetupAutomationSmm, LenovoSetupUnderOsSmm, LenovoSecureKeySmm, LenovoDriveEraseSmm
0.9.8zb	InfineonTpmUpdateDxe

摘要：Binarly REsearch 团队近日深入研究了最近的 OpenSSL 安全更新给 UEFI 固件供应链生态系统带来怎样的影响以及 OpenSSL 版本在固件环境中是如何广泛使用的。研究结果不容乐观。科技行业正在积极讨论使用“软件材料清单”（SBOM）来化解供应链安全风险。为了确保供应链安全实践落地，必须加强软件依赖项方面的透明度。以前，任何一款软件作为黑盒子来发布，并不提供与软件依赖项和第三方组件相关的任何信息。

荣耀登顶 | 亿赛通蝉联中国数据泄露防护市场占有率第一



CCIDConsulting

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

赛迪顾问数据引用说明

使用方：北京亿赛通科技发展有限责任公司	部门：市场宣传部 联系人： 电话： 地址：北京市海淀区西二旗大街39号A座
主题：北京亿赛通科技发展有限责任公司2021年中国数据泄露防护产品市场排名说明	
内容： 在赛迪顾问股份有限公司（简称“赛迪顾问”）编制的《中国数据泄露防护市场研究报告（2022）》中，北京亿赛通科技发展有限责任公司（简称“亿赛通”）在2021年中国数据泄露防护产品市场份额及排名情况如下：亿赛通数据泄露防护产品位居中国数据泄露防护产品市场地位第1名。	

赛迪顾问经核实，证明上述内容来源于赛迪顾问《中国数据泄露防护市场研究报告（2022）》中的数据，并确认无误，如须删减、添加、更改信息，须提交赛迪顾问重新确认。赛迪顾问申明，对使用上述数据、信息后，对使用方或与使用方有关的其它机构所造成的任何影响或损失，赛迪顾问均不承担任何责任。

赛迪顾问股份有限公司
2022年12月26日

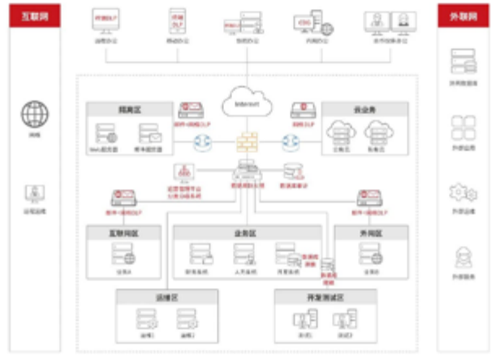
在2022年最后一个工作日，亿赛通收到重大喜讯，据CCID编制《中国数据泄露防护市场研究报告（2022）》（以下简称“《报告》”）显示，亿赛通在中国数据泄露防护产品市场中已连续7年排名第一。

《报告》显示，2021年，多项国家政策，行业标准相继颁布实施，市场监管更为严格。在各路资本支持下不断涌现的初创公司与纷纷扩张其安全版图的传统安全公司使得中国数据泄露防护市场呈现群雄逐鹿的场面。特别是自《关键信息基础设施安全保护条例》、《数据安全法》及《个人信息保护法》实施后，这三部政策法规与2017年的《网络安全法》，共同织起了“三法一条例”网络安全保障网，从国家层面，全面加强了对数据和个人信息的安全管理。数据的安全受到前所未有的重视和保护，导致市场需求激增。

其中，根据《数据安全法》规定，企业要建立全流程数据安全管理制度，这就需要企业在数据安全技术和数据安全管理上建立完整的数据安全治理体系框架和技术架构。数据资产的泄露防护作为数据安全建设的关键技术支撑，大大推动了用户对数据泄露防护产品的采购需求。另外，在《数据安全治理能力评估方法》（T/ISC-0011-2021）中特别提到，数据泄露防护作为数据安全治理的前提，是实现数据分类分级的重要技术工具。

面对复杂多变的应用环境，数据泄露防护产品不但要满足大量合规市场，更需要满足客户的价值需求，品牌优势会助力获得更大的合规市场，技术创新带动行业头部客户的青睐。业务场景和问题挑战的愈发多样，数据泄露防护产品也应该和一些新的数据安全技术相结合，以期为企业提供更为全面的防护。

亿赛通新一代数据泄露防护产品经过不断的研发与创新，产品迭代升级。该产品采用平台化管理，将终端DLP、网络DLP、邮件DLP、存储扫描DLP、API接口DLP进行统一管理，模块化控制。将对数据进行分类分级扫描，实现终端数据资产梳理、文件服务器数据梳理、数据库数据资产梳理、数据加密防护、数据外发监测、终端运维管理、邮件外发控制、数据水印、端口管控。



亿赛通新一代数据泄露防护解决方案已先后为京东方、徐工集团、格力、上海电气集团、千金药业、中国移动、中国电信、中国联通、农业银行、太平洋保险、中信证券、华夏基金、人民银行、零跑科技、长电科技、国家电网、宁波海关、航天科工等众多国内外知名企业建设先进、自主、灵活、全面、智能的立体化数据安全防护体系，提供高效、全面、完整、规范的数据安全运营服务。

在旺盛的社会需求和抢眼的发展市场下，亿赛通作为中国数据泄露防护市场的龙头厂商，重点关注创新和技术的融合及行业应用延伸，产品在市场上反响热烈，市场占有率节节攀升，成为2021年数据泄露防护产品市场占有率第一实至名归。

现在荣耀的成绩只是开始，只有让产品更好地服务客户，推动产品的技术进步才是一个产品持续领先的前提。亿赛通新一代数据泄露防护产品将深入捕捉各行业业务场景需求，继续在诸多领域积极探索。

喜提“金帽子”|亿赛通荣获 2022 网络安全金帽子年度最佳行业解决方案



11 月 29 日，由北京嘶吼文化传媒有限公司主办的“2022 网络安全金帽子年度评选”结果正式公示。本次活动中，亿赛通能源石化数据安全解决方案在年度最佳（能源）行业解决方案赛道高票进入前三，荣获“年度最佳（能源）行业解决方案”奖。作为亿赛通全行业解决方案的重要组成部分，入选最佳解决方案这一殊荣，实乃众望所归。

随着能源创新驱动战略实施，科技类商业秘密已成为能源石化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。做好科技类商业秘密保护，必须结合企业实际，将保密制度、科研业务流程以及法律支撑保障“三要素”相结合，将人防、技防以及岗位制度管理“三环节”相融合，利于科研，便于保密，实现“依规管密，依技防密，依法治密”，全力助推能源企业高质量可持续发展。

与此同时，国家在保障敏感数据安全方面积极制定相关法律法规。《网络安全法》、《数据安全法》、《电力行业网络与信息安全管理办法》等等，都在对能源企业开展数据安全保护提出更高、更严的要求。一方面，能源企业需要通过不断挖掘数据价值以支撑自身服务质量、工作效率和发展需要；另一方面，又要保证数据在复杂的场景、系统之间被安全、合理的访问和使用。

能源电力行业风险分析

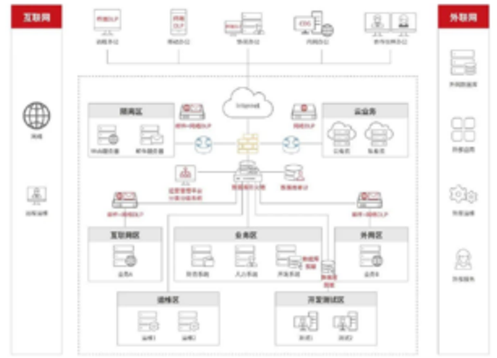
1、 敏感数据管理不足，没有良好的数据梳理；

2、风险行为监控不足，企业庞大造成的日常越权访问、下载和篡改数据等违规操作难以定位和发现；

3、运维人员不按操作规范或既定方案进行数据库运维操作、非法导出敏感数据、数据库操作行为没有细粒度的审计记录等；

4、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。

亿赛通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，能源石化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。

亿赛通能源石化数据安全解决方案基于“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。

亿赛通在能源石化行业已有众多成功落地项目，如：中国石油、中国石化、中海油、华电集团、特变电工、河南电网等。此次获奖，是监管单位、业界专家、行业客户、权威媒体对亿赛通提供的行业解决方案的再次肯定。数据寒冬下，企业面临的挑战和压力与日俱增，我司希望能实际帮助企业提升安全能力，助力企业业务快速发展！

首批入选，网络安全技术与产业发展工业和信息化部重点实验室专项工作组成员名单公布

近日，工信部网络安全产业发展中心公布了网络安全技术与产业发展工业和信息化部重点实验室（以下简称重点实验室）专项工作组成员单位名单。亿赛通首批入选，成为商用密码应用和大数据安全两个工作组的成员单位。



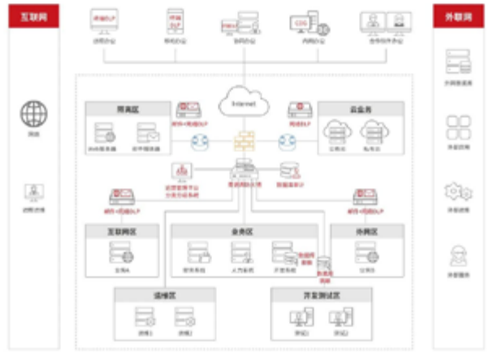
重点实验室是依托工业和信息化部网络安全产业发展中心（工业和信息化部信息中心），聚焦网络安全新模式、新技术、新业态，围绕新一代信息技术与传统产业深度融合，开展信创环境下云安全、大数据应用与安全、人工智能、工业控制安全、密码应用等网络安全新技术在重点领域、重点行业的基础研究、产品开发、方案集成、成果转化及应用推广。近年来，重点实验室逐渐形成了以产业大数据分析和工业互联网平台为基础的产业管理、推进及服务模式，成为网络安全技术创新、合作交流、展示推广、成果转化和产业推进的重要平台。

重点实验室聚焦信创安全运维、密码应用等重点方向开展关键技术创新攻关和产品研发与整体解决方案实现。2022 年初，启动了重点方向专项工作组成员单位征集工作。经过对本次各申报单位的企业能力、行业代表性等方面进行了综合评定，最终认定包括亿赛通在内的几十家单位成为重点实验室专项工作组成员。

商用密码应用工作组对标《密码法》、《网络安全法》等国家法律法规，基于国密算法设计实现覆盖新型云、网环境，保障网络安全、信息安全、数据安全的整体解决方案，突破核心技术、研发国产密码云服务平台、二代数据库加密网关、容器云防火墙、区块链加密机等关键新型密码产品。

而大数据安全工作组则是重点研发数据防护产品，包括数据库加密网关、数据库加密服务器、大数据监管平台、数据安全合规性评估系统。

亿赛通每年进行大量的研发创新投入，且所有产品均符合国家信息安全技术标准，在企业内网域、边界域和外部域三个层面进行重点建设。通过事前主动防御、事中监测响应、事后追踪溯源、全程态势感知四个维度，进行企业数据资产的全流程安全防护。建立多层次防护体系，覆盖终端、网络、存储、业务系统、邮件等层级，同时兼容原有信息系统，在保障技术创新性的同时保证用户使用无感知。

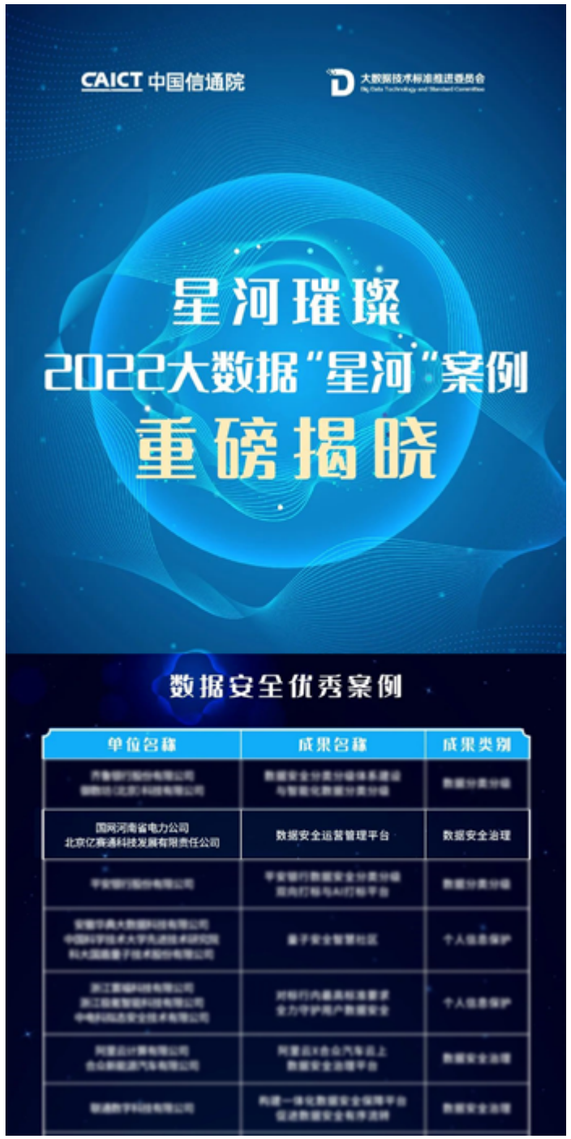


其中数据安全运营管理平台、数据库安全五件套、数据分类分级系统、新一代数据泄露防护系统及新一代电子文档安全管理系统更是亿赛通的核心产品，切实包含了数据的全生命周期防护。整个防护过程从决策层到技术层，从管理制度到技术支撑，将各个独立的数据安全技术和功能整合，为用户提供跨数据类型、存储孤岛和生态系统集成数据的产品和服务，从而实现更简单、一致的端到端数据安全。所有产品套组构建了自上而下、全流程、可闭环的完整链条。相较于传统数据安全方案，存在更高水平的集成能力、简化的部署模型，统一的策略控制平面，以及对数据、存储、政策和适用法规的一致可见性。



数据安全是国之重器，对推动我国数字经济高质量发展、保障国家安全都具有十分重要的意义。加入工作组后，亿赛通将支持工作组开展相关工作，提升数据安全保障能力，引领数据安全技术产品高质量发展，推动技术创新、产业发展良性生态，加速推进国家数据安全建设。

星河璀璨 | 亿赛通解决方案荣获中国信通院 2022 大数据“星河”优秀案例



近日，由中国信息通信研究院（以下简称“中国信通院”）、中国通信标准化协会大数据技术标准推进委员会 (CCSA TC601) 共同组织的第六届大数据“星河（Galaxy）”案例征集活动评选结果已经正式发布。北京亿赛通科技发展有限公司和国网河南省电力公司联合申报的“数据安全运营管理平台”应用成果凭借专业的技术及完善的解决方案，荣获 2022 大数据“星河”案例——数据安全优秀案例。

党中央、国务院高度重视大数据产业发展，推动实施国家大数据战略。《“十四五”规划纲要》围绕“打造数字经济新优势”，做出了培育壮大大数据等新兴数字产业的明确部署。大数据“星河（Galaxy）”案例截止至本次，已成功举办六届，成功推动大数据在社会生产生活中的应用 , 促进了大数据技术产品及相关产业发展。本次案例评选共收到申报项目 595 份，经过形式审查和专家评审最终亿赛通脱颖而出，入选数据安全优秀案例之一。

能源行业是国民经济的基础行业，也是国家支柱性行业，关乎国家稳定与繁荣。伴随着全球数字经济飞速发展，数字化转型加速，传统的业务应用模式发生巨大变革。国家在保障敏感数据安全方面积极制定相关政策法规，对能源企业开展数据安全保护提出更高、更严的要求。本次成果遵循了国家号召和国网河南省电力公司要求，为其提供数据安全治理框架建设和解决方案实施，在能源行业中起到良好应用。

亿赛通数据安全运营管理平台提供基础数据安全的能力，把各种安全能力都集成在一个平台，整合数据全生命周期各阶段状态，总览数据资产和安全风险，实现数据安全运营的闭环管控。主要通过感知云、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。

从应用目标上看，平台以数据安全为核心，涵盖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。

从技术实现上看，平台不仅采集流量，而且进行协议内容还原，更多关注数据内容，从而判断是否存在数据安全的风险。另外包含 UEBA、规则匹配等分析类技术功能。

近年来，亿赛通的数据安全创新能力不断突破，2022 年，更是在全新数据安全建设理念的基础上，结合《数据安全法》、《个人信息保护法》等政策法规要求，对内部各项安全产品更新迭代，整合集数据安全治理、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综合性解决方案，实现了标准化实践，建立了统一的数据安全体系框架。不仅可解决一家能源客户的安全问题，还可实现同行业的复制，提升国家整个能源行业的数据安全水平。



未来，亿赛通将持续围绕“分·放·管·服”数据安全建设理念，推进数据安全体系扩增，促进数据安全治理工作在各企业运营环节的嵌入与防护，提升数据驱动的安全防护能力，助力企事业单位蓬勃发展。

权威认证：亿赛通安全管理平台成功通过信通院“可信数安”分类分级评估测评



2022 年 12 月 8 日，第二批“可信数安”评估评测专家评审会举行。经来自中国信息通信研究院、中国科学院信息工程研究所的专家集中评议后，亿赛通自主研发的安全管理平台继第一批通过“安全运营管理平台”能力测评后，再次通过“分类分级”能力测评。此项权威认证再次证明了亿赛通在数据安全治理、分类分级领域的实力和能力。

“可信数安”评估体系是国内首个面向数据安全需求方及数据安全供应方的体系化、市场化数据安全能力评估体系。创办的初衷一方面面向建设需求方开展企业级、系统级数据安全评估，协助各组织提升安全能力，实现以评促建效果；另一方面面向建设供应方开展产品评测及服务能力评估，筛选优秀的产品与服务，推动技术及服务水平的进步。本次亿赛通能通过测评，是业内对公司在数据安全领域能力与实践的高度认可。

数据分类分级建设方案

数据安全分类分级解决方案：采用服务 + 工具的方式对企业的数据资产进行梳理、分析、标记和持续跟踪。通过对数据全流程的标记，定位企业重要资产，并实施差异化安全防护方案，从而实现企业数据资产可视、数据级别可知、数据风险可控。

数据资产梳理：通过全网资产扫描分析，发现数据库、文件服务、终端的结构化和非结构化数据资产，形成数据资产清单。

数据分类分级：基于数据资产清单，结合服务和工具，按照行业业务属性对数据进行分类，按照风险程度进分级，标识数据资产。

结果清单展示：输出分类分级清单，指导企业依据分类分级结果进行数据安全治理体系化建设。

数据持续运营：分类分级结果支持多种方式向外输出，针对不同安全级别的资产开展不同的安全防护方案，兼顾效率与安全。

分类分级功能特色

亿赛通安全管理平台通过全面的资产发现方式、灵活的资产梳理规则、深入的资产质量分析，能够有效地帮助企业进行对数据资产的摸底和管理工作；改善传统方式下的资产梳理和管理模式，提高工作效率，实现资产权责分明；打破数据孤岛，提高获取效率，释放资产价值。亿赛通安全管理平台的分类分级功能特色如下：

1. 数据源覆盖全面：平台基于数据嗅探技术，能够自动发现网络环境中的数据库、文件服务器。同时系统还支持终端设备，可对终端电脑中的敏感数据进行标识。

2. 识别规则丰富细致：平台提供丰富的敏感数据识别规则和开箱即用的数据分类分级模板，分类分级模板囊括：金融、运营商、医疗、政府、工业、地方政务、汽车、物流等多个行业 10 余种模板，为用户重要数据识别与分类分级提供重要能力支撑。

3. 数据资产直观可视：平台为数据安全提供资产可视化的直观呈现方式，使用户更便捷的了解和管理数据安全，提高数据梳理效率。

4. 数据安全联防联控：平台支持对其它数据安全设备分发分类分级结果，指导其根据不同数据级别，实现差异化策略配置。

本次亿赛通安全管理平台通过评测，是外界对公司在数据分类分级方面取得的成绩的肯定和认可。未来，亿赛通将继续深耕数据安全领域，增强创新能力，提升技术硬实力和服务水平，为我国经济社会数字化转型发展贡献亿赛通的优质产品与方案。

为亿赛通点赞 | ISC 2022 数字安全创新能力百强亿赛通成功上榜



12 月 21 日，由 ISC 平台主办的 2022 网络安全创新能力百强颁奖典礼在北京成功召开，围绕新时代、新安全、新发展遴选年度数字安全创新力量。亿赛通凭借近二十年在数据安全领域的深耕，成功入选 2022 网络安全创新能力百强入榜企业名单。我司的某电力行业解决方案也成功入选《ISC 数字安全创新性案例》报告。同时，我司技术专家受邀出席大会发表《新形势下的综合数据安全防护技术》主题演讲。



伴随着数字经济逐渐深入日常生活，数据泄露事件愈发严重，据统计，2015 年 -2021 年全球数据泄露平均总成本逐年升高，2021 年甚至高达 424 万美元。数据的采集、传输、存储、使用、共享、销毁等全生命周期的安全风险更加严重。企业用户面临着外部风险难预防、内部违规难发现、综合攻击新挑战三大问题。



亿赛通认为，数据安全综合管理平台是未来数据安全防护的发展方向。据 Gartner 调查显示，78% 的受访企业使用 16 种以上的单点安全产品，12% 的受访企业使用 46 种以上的单点安全产品。这意味着大多数企业使用的都是松散、割裂的单点安全解决方案。同时，企业使用的各种单点安全产品又通常都是孤立运行，这导致网络运营团队和安全运营团队无法获得整个企业数据流量的可见性。而亿赛通自主研发的数据安全运营管理平台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，帮助用户准确定位风险源头。

此外，数据安全运营管理平台将视线主要关注到“运营”二字，运营实际上就是服务。亿赛通专门成立了数据安全服务部门，根据用户的经营策略、治理要求、合规要求等，提供顶层设计、IT 安全策略、数据梳理等各种服务。亿赛通数据安全运营管理平台能够实现与各个能力组件的配合，结合分类分级结果进行差异化策略部署，兼顾安全与效率。



作为本次颁奖典礼 2022 网络安全创新能力百强名单的创新企业之一，亿赛通自创立以来始终专注于数据安全技术的钻研与探索，为全行业客户提供数据安全领域综合解决方案，服务用户单位的数据安全治理建设。正因如此，凭借技术驱动创新和安全建设服务方面的优势和经验沉淀，亿赛通在本次“2022 网络安全创新能力百强”评选受到用户单位、评选机构及行业的广泛认可。

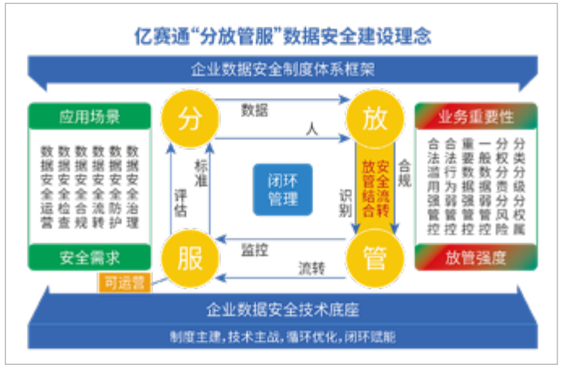
面对瞬息万变的数据安全大环境，中国的数据安全治理创新已然迅捷起步，并以乘风破浪的姿态不断向前行进。未来，亿赛通将继续坚持技术创新，并与更多的行业专家、安全从业者等合作探讨、互利共赢，共同绘制数字安全技术创新的新蓝图。

又一荣誉榜单实力加冕，亿赛通入围《嘶吼 2022 中国网络安全产业势能榜》



12 月 21 日，嘶吼安全产业研究院发布了《嘶吼 2022 中国网络安全产业势能榜》，作为数据安全领域中的排头兵，亿赛通凭实力入选势能榜，获得制造行业的专精型安全厂商荣誉。

2022 年，我国迈入创新型发展国家行列，在国家正确的战略方针指引与驱动下，中国科技在多领域实现了技术革新与突破。十四五也把安全放在首要位置，与发展并驾齐驱。在这创新发展腾飞的时代，随着各行业领域的创新不断提升，网络安全的重要性愈发凸显。政务、金融、能源、制造、运营商等关键行业领域更加依托于真正的安全。



历时近 2 个月的调研、数据提炼、横向对比，打分复核等阶段，嘶吼选取五大热门行业：政务、金融、能源、制造、运营商以及三大类型“综合型”、“专精型”、“创新型”，从参与报名的近 300 家调研信息中最终评选出 84 名优秀的行业安全厂商并颁发荣誉奖杯予以表彰。

亿赛通作为国内首屈一指的数据安全厂商，基于自主研发的“分放管服”数据安全建设理念，打造了集数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务为一体的综合数据安全解决方案。核心产品依托强大的创新能力，不断融合前沿技术，以用户需求为导向进行产品迭代，实现统一管控、平台呈现、安全运营，落实安全闭环管理，建立新一代立体化、纵深防御体系。

此前，亿赛通已陆续入选了嘶吼 2022 网络安全产业图谱、2022 网络安全金帽子年度最佳（能源）行业解决方案，本次又入围嘶吼 2022 中国网络安全产业势能榜，更加直观的展示了亿赛通在数据安全领域的实力和地位，所有的实力加冕，亿赛通都是实至名归。业界的肯定和褒奖也将驱动我司持续深化数据安全建设理念，丰富安全产品与方案，提升安全服务能力，为更多行业用户的数字化发展保驾护航。

《ISC 数字安全创新案例报告》发布，亿赛通深挖能源行业新需求，赋能企业安全建设



近日，《ISC 数字安全创新案例报告》（以下简称“报告”）在 2022 数字安全创新能力百强颁奖典礼上发布。亿赛通凭借《某电力公司电力科学研究院综合解决方案落地实践》入选《报告》生活服务行业优秀案例。

据悉，本次案例征集前后历时近 2 个月，最终成功征集到 600 余份创新案例，在这些海量的案例之中，覆盖了数字安全的方方面面，当把这些创新结晶汇聚在一起，我们看到了数字安全源源不断的创新力和澎湃向上的生命力。而《ISC 数字安全创新案例报告》则是众多案例的精华，极具参考价值。

党的二十大后，数字经济进入新一轮高速发展期，数字经济与实体经济加速融合，而作为数字经济发展的基座，数字安全也走向了各行各业，成为大家关注的重点。《ISC 数字安全创新案例报告》中的成功实践案例覆盖了时下热门的金融行业、政企行业、生活服务行业、教育行业、制造行业等板块，成为数字安全在各个行业的精准施策、高效解决问题的参考，持续挖掘引领行业发展、推动数字中国建设的数字安全创新成果，全方位助力打造中国数字变革的新高地。


“ISC数字安全创新案例报告”
入选结果公布

生活服务行业优秀案例		
序号	案例提供方	案例名称
1	[illegible]	[illegible]
2	亿赛通	某电力公司电力科学研究院综合解决方案落地实践

案例背景

电力公司作为关系国计民生和国家能源安全的重要骨干企业，接触、产生和处理的涉密信息较多，一旦发生失泄密，就可能给电网安全带来隐患，给国家造成重大损失。随着构建全球能源互联网和特高压电网建设不断加快，电网发展信息化、智能化水平全面提升，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

（1）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。

（2）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。

（3）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。

（4）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。

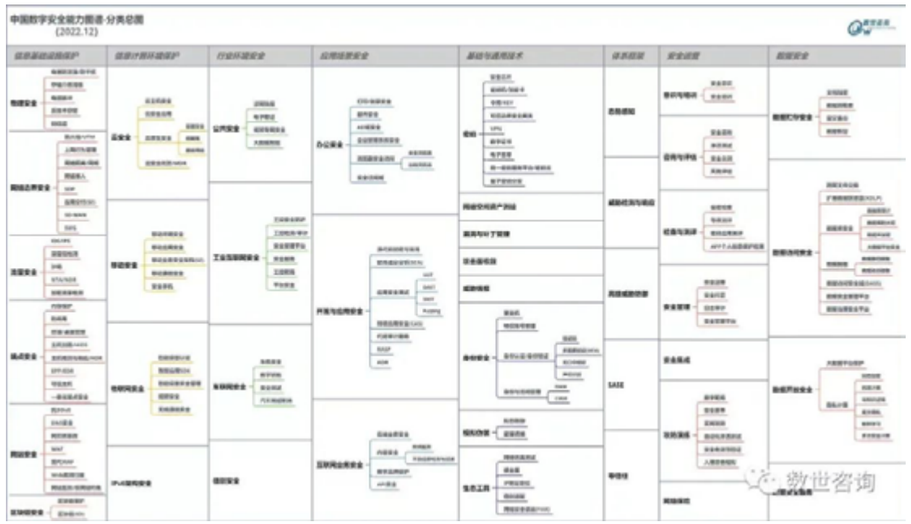
方案价值

电力公司作为关系国计民生和国家能源安全的重要骨干企业，接触、产生和处理的涉密信息较多，一旦发生失泄密，就可能给电网安全带来隐患，给国家造成重大损失。随着构建全球能源互联网和特高压电网建设不断加快，电网发展信息化、智能化水平全面提升，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。



亿赛通为该电力公司提供一套数据泄露防护结合文件加密的安全防护体系，有效地保障了各个环节数据的安全运行，从源头上把控泄密隐患，防止有意、无意的数据泄露事件发生，使保密工作融合到企业业务中，保密制度完美落地。

2022 年度中国数字安全能力图谱（精选版）| 亿赛通抢占多个细分领域



近日，国内数字安全领域中立的第三方调研机构数世咨询正式发布《2022 年度中国数字安全能力图谱（精选版）》（以下简称图谱），凭借技术创新、业务专注及服务能力，亿赛通分别入选 4 个细分领域的代表者与能力者。

图谱从信息技术、业务应用与网络攻防三大支点和位于中心的数据安全共四大维度出发，划分出八大方向。每个方向又包含各自一级或子级的细分领域，以及由数世咨询观察到并予以推荐的数字安全供应商。本年度图谱与 2021 年度图谱最大的区别在于，大幅度削减了数字安全供应商的数量，是精选而不是海选，更不是企业大全，以规避“全能型”原厂商或中小企业占据多条产品线的混乱现象。

在《数据安全法》出台以前，业界传统上将“数据安全”看作网络安全的“子集”。但在本质上，网络安全不是目的，而是手段，保护数据安全才是其核心价值。本版图谱将“数据安全”划分为 4 个一级分类和 1 3 个二级分类。相比 2021 年的能力图谱，本次将“数据安全综合治理”的一级分类更名为“数据安全管理平台”，并划分到“数据访问安全”的分类中。此外，新增了一级分类“数据安全服务”。

亿赛通具体入选细分领域如下：

一级分类	二级分类	身份梳理
数据贮存安全	文档加密	代表者
数据访问安全	扩展数据防泄露	能力者
	数据安全管理平台	能力者
数据安全服务	——	能力者



近些年，随着数字经济的高速发展，客户数据安全的需求发生了前移。客户需求的多样化，导致企业部署各项数据安全产品时需要进行联动，将原有的 DLP、文件加密、数据库安全等各类产品能力集中化管理。



亿赛通在进行数据安全治理体系建设时，会依据前期资产梳理结果再部署相应的安全能力产品和平台，进而达到风险评估、监控预警、应急处置及持续运营。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，需要覆盖云、网、端等场景。而亿赛通的综合产品能力已经覆盖数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务等方面，能够真正帮助客户实现数据安全策略管理、识别能力、防护能力、监测能力以及运营能力的有机整合。



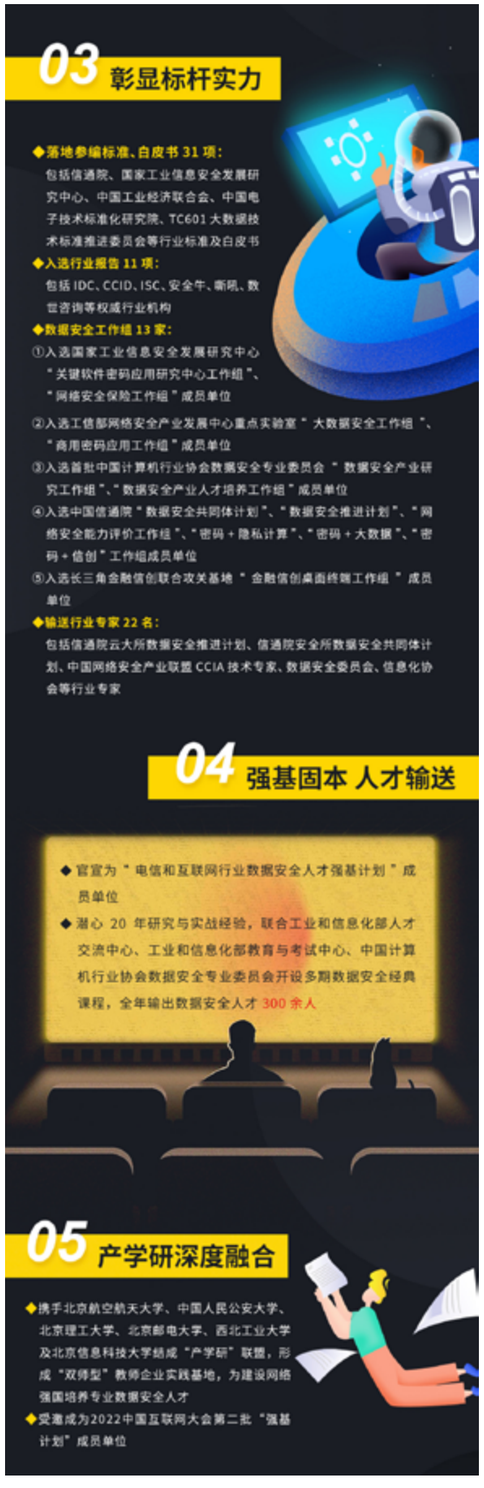
除此之外，亿赛通率先提出的“分放管服”数据安全建设理念，以“数据和人”为对象构建的数据治理、防护、流转、运营的双闭环体系，具有可操作性、高效等特点，让企业步步为营，快速提升自身综合数据安全能力，达到数据安全治理、防护、流转和运营的目标，保障涉数据业务合法合规，业务安全可持续运营。

亿赛通成立之初就聚焦数据安全赛道，凭借对数据安全的深入理解及产品不断更新迭代，以夯实的基础为企业提供持续且可信赖的安全产品与服务。目前，我司产品及服务正在被广泛应用于政府、能源、新能源、金融、运营商、教育、医疗等行业并广受客户好评。

未来，亿赛通将继续发挥自身在数据安全领域技术优势，以优质的产品及服务守护企业用户数据资产安全，为数字中国安全建设贡献力量。

2022 年度
十大重点成绩单









护航数据安全建设第十六期 | 数据安全治理之数据血缘分析系统

在数据的全生命周期中，因加工、融合、流转等产生的数据与数据之间的多种关系，因与人类的血缘关系比较相似，所以被称为数据血缘关系。而数据血缘的特性和应用场景，尽管其当前还未在数据安全治理中广泛应用，但未来必将发挥重要作用。数据血缘分析作为数据血缘的应用方式，不是单纯的一种技术手段或一个工具，而是一个贯穿数据生命周期的过程，涉及流程、技术、产品等多维度的内容。

亿赛通数据血缘分析系统（简称 :DLAS），系统支持对数据在产生与使用过程中对数据的引用关系及流向进行分析，通过对原数据、流动数据进行采集，从数据的归属性、多源性、可追溯、层次性等多方面对数据血缘关系特征进行分析，通过图形方式呈现数据的归属关系及数据的关联关系，帮助企业在数据安全治理时梳理数据的来源和去向、激发数据潜在价值、打下数据安全基础能力。

产品价值

数据追踪溯源

数据血缘分析能够在数据溯源过程中找到相关数据之间的联系，当数据泄露事件发生时，帮助追踪到异常发生的源头及主要原因，平时也能帮助我们追踪数据的来源，追踪数据处理过程。

数据价值评估

数据血缘分析同时可以辅助对数据价值进行评估，数据血缘关系可以从数据的引用数据、关联数据等信息为数据的价值进行评估提供依据。例如：引用数据量大、关联数据量多的数据在企业内部受众度会相对较广。

数据质量评估

通过数据血缘关系图，可以清晰的看到数据产生、流转、使用的整个前后过程，通过数据血缘关系图谱可以方便的了解到数据的处理过程是否符合数据质量处理要求。

关键功能

1、血缘数据采集

数据血缘分析系统支持从各类源数据、流转数据中进行血缘关系采集，当各系统数据血缘关系产生时，血缘分析系统会及时、准确的记录血缘关系并存储下来。

数据血缘分析系统支持关系预定义、实时采集，数据血缘分析系统支持主流的关系型数据库、非关系型数据库、非结构化数据等类型数据源。

2、血缘关系分析

数据血缘分析针对数据流转过程中产生并记录的各种日志进行采集、处理和分析，对数据之间的血缘关系进行系统性梳理、关联、并将梳理完成信息进行存储。数据血缘分析系统可进行系统级血缘、表级血缘、字段级血缘进行关联分析。实现数据来源的精确追踪、流转过程的准确还原、数据去向的精准定位。

3、数据血缘可视化

数据血缘分析系统通过可视化技术将分析结果清晰、直观地呈现给用户，帮助客户进行二次分析和具体应用。系统支持按照数据所有者、数据库、表、字段（列）及数据本身进行血缘关系分析，支持正向分析和反向分析。其不仅展示数据来龙去脉，还定位异常数据影响范围。如影响度分析，也是血缘关系能力的一部分，其用来分析数据的下游流向。

当系统进行升级改造时，能够及时发现上游数据的变化可能会对下游数据产生的影响，并及时告知下游数据使用方。

随着数据的爆发式增长，数据之间的关系也变越发复杂，这为数据安全治理工作带来了巨大挑战。在这样的背景下，数据血缘将在数据安全治理过程中发挥越来越大的作用。数据血缘应用需要依赖丰富的可分析数据、强大的数据采集和血缘分析能力、清晰直观的血缘图谱，是一个贯穿数据生命周期的持续性工程，不仅需要从技术层面重视，更要从数据安全治理的相关流程、制度、意识层面进行配合，才能取得预期的效果。

护航数据安全建设第十七期 | 数据安全防护之终端数据安全管理平台

随着终端产品的广泛应用，促使行业用户对终端数据安全防护提出了更高的要求。如何提高对不同终端设备的统一安全管理能力，及时处理复杂组织下终端设备的安全运维、安全审计等问题已成为当下需重点关注并亟需解决的痛点。

终端数据安全管理平台（简称 TDSP）是用于对企事业单位的终端数据进行安全保护的。系统包含商业秘密文档定密、分类分级、集中管控、安全流转、安全保密、安全外发、终端数据资产梳理、终端应用程序采集、终端设备信息采集等功能，是集终端资产扫描与终端电子文档加密防护于一体的全能产品。

产品价值

1、终端文档加密与数据外发防护识别一体化

终端电子文档加密防护与数据外发内容识别监测相结合，实现从认识数据、分析数据到全方位数据安全防护和风险防控的跨越。

2、内容可审计、文件可溯源

数据标签化，内容可进行敏感识别，文档唯一标识实现溯源分析。

3、数据梳理

梳理数据清单，实现数据可视化，支持以报表形式清晰的给各级保密部门及垂直业务主管部门报送。

4、防护方式多样、灵活

实现数据加密保护，并可不同维度地检索、查询和统计，通过数据行为统计、管理与分析，实时掌握和管理数据动态。

产品优势

1、完整的终端数据管理

实现终端数据资产采集、敏感数据加密防护、关键数据外发监测预警、加密文件外发审批控制。

2、文档加密结合内容识别

静态数据进行内容扫描发现、关键数据进行加密防护、外发数据进行内容识别检测，既保证数据的安全防护，又方便数据进行灵活使用。

3、终端安全管理

对终端信息进行采集，除数据本身外，还可以采集应用程序信息，设备及操作系统信息，使用者信息，资源占用信息，实现终端可视化运维。

4、用户行为可追溯

对用户所访问的数据信息，操作应用程序过程，数据外

发过程等进行事件记录，从访问量，访问时间，数据关联性，数据敏感性进行多维度分析，实现用户行为分析和追溯。

5、终端行为和数据可视化

终端用户使用行为可视化、终端用户数据内容使用情况可视化、终端设备运行状态可视化、风险预警信息可视化。

关键功能

1、文档加密技术

系统采用驱动层加密技术，使用户无法通过常规手段进行强制移除或终止；即使用户通过强制手段破坏了客户端运行环境，系统也有相应的保护措施，确保加密机制的安全、高效和稳定。系统可实现对任意文档自动加密的功能，即文档定稿或归档时进行安全保护，保证数据完整性，同时不改变和影响用户的任何使用习惯及工作效率。支持单个和批量文档加密。

2、文档加密授权技术

通过灵活的分级设置，用户可按照部门、项目组、指定用户名等角色设置访问权限，并加上标识，实现对高密级文件进行隔离管理。同时可提供精细化文件权限控制，如文档的阅读、编辑、打印权限，以及阅读次数、阅读时限等文档生命周期的控制管理。

3、内容识别技术和标签

系统采用丰富的内容识别技术（关键词、正则表达式、文件属性、文件指纹、机器学习、文件伪装识别、文件嵌套识别、文件多层压缩、图片 OCR 识别），对数据进行分类分级检测，并进行数据标签化。建立起基于数据分类分级的数据资产管理体系和安全防护体系。

4、数据血缘分析技术

采用数据标签化技术、数据水印技术、数据派生识别技术、机器学习、模型运算技术分析数据的产生，派生，变更，流转，使用过程，分析数据的全生命周期变化过程，并梳理流转途径。

5、同平台管理

系统采用平台化管理，实现管理端平台，客户端一体化，达到一个管理服务端，一套安全客户端，最终为客户提供终端上的信息检测，文档加密，桌面管控，端口管控，水印溯源，整体运维的终端安全目标。

6、风险告警与安全流程管控

系统支持邮件、企业微信、钉钉、syslog、Kafka、sftp 等多种数据风险告警和共享技术，支持 restful 接口对接技术。系统支持邮件审批、企微审批、钉钉审批，实现快捷高效的管理和运营。



亿赛通坚持创新的精神取得了社会各界和客户的巨大认同。特别是自研自创的“分放管服”数据安全建设理念，在理念的支撑下，我司战略部署五大核心业务板块：数据安全治理、数据安全防护、数据安全流转、数据库安全及安全服务，致力以专业的产品和服务为客户筑牢数据安全底座，保障企业保障客户数据资产安全。

护航数据安全建设第十八期 | 数据安全防护之新一代电子文档安全管理系统

近年来，有政府工作报告指出，要促进数字经济发展，加强数字中国建设整体布局，建设数字信息基础设施。同时完善数字经济治理，释放数据要素潜力，更好赋能经济发展、丰富人民生活。数字经济领域，监管治理与促进发展并行。数据要素已成为数字技术进步的助推剂，进而促进生产力的发展。数据的价值只有在有序、规范的流通场景中才能充分发挥。

亿赛通多阶段多维度剖析数据全生命周期管理过程中的问题和风险，为企业管理用户提供直观、全面、实时、动态的安全态势感知大屏，全面保障企业电子文档安全。

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（Windows、Mac 和 Linux 系统平台）、智能终端（Android、iOS）以及各类应用系统（OA、知识管理、文档管理、项目管理、PDM 等），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。



图 新一代电子文档硬件产品展示

产品价值

满足数据合规要求

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

数据分类分级管控

建立数据分类分级保护制度，实行人员定岗定级精细化数据安全管控。

数据安全全面防护

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

数据泄密审计追责

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

产品优势

1、系统部署

支持 Windows 和 linux 部署，支持软硬一体，高效实施、省心省力、稳定可靠、简单运维。

2、分类分级

支持分类安全隔离、数据标密、升降密以及精细化的流程分级管理和内容分级管控。

3、集团管控

支持策略集团统一管理、密钥统一管理、支持策略模板批量快捷分发策略，支持锁定分部策略。

4、中间件服务

支持加解密、外发、移动端、工作流集成，支持 restful/DLl 和 So 库 / 移动 SDK 等多形式灵活部署。

5、国产化适配

支持服务器和终端桌面环境的国产化部署，兼容适配麒麟、统信操作系统，飞腾、海光、麒麟 990、兆芯 CPU，适配 Mysql 和 MOGDB 数据库，实现一套服务端管理平台，兼容 windows、Mac、Linux、国产化、IMT、Usec 多个业务终端，以及中间件和网关服务。

关键功能

文档安全管理系统

聚焦终端核心数据资产加密保护，防范明文泄密风险。

1、透明加密

一种强制自动加密技术，文档加密、解密过程对使用者无感知。主要解决用户核心数据文档明文存储面临的众多泄密风险。

2、半透明加密

一种主动加密技术，实现不同部门按需进行加密，在保障用户核心数据安全情况下，兼具文档交互效率。

3、智能加密

融合透明加密和内容智能识别技术，用户打开文档时基于安全策略对内容进行智能检测，当发现敏感信息时自动加密文档，整个过程使用者无感知。

4、权限管理

数据作者可以设定数据传播范围（用户、部门）和使用权限（只读、打印、修改、阅读次数、阅读时长），控制文档在内部受控使用。权限信息统一存储在后台，管理员可以远程管理文档：再授权、冻结、归档、限制访问、权限转移、离线授权、文档销毁等。

5、内容安全

对用户核心数据文档基于内容上安全保护，防止数据使用者在使用文档内容过程中，通过复制、拖拽、另存、插入、连接（网络）、截屏，造成的文件内容泄密风险。同时，还支持加密文档打印管控、支持阅读水印 / 文档文档 / 打印水印。

6、分类分级

通过密钥对核心数据进行分类标识，拥有分类权限的用户才允许正常使用加密文档，实现数据分类安全隔离；通过文档标密明确数据涉密重要程度，实行数据安全分级管控，能够灵活地根据人员岗位职级对人员分配密级权限。

7、外发管理

采用文件虚拟磁盘技术对数据加密保护，并控制只读 / 打印 / 修改 / 阅读次数 / 阅读时长权限，防范文档外部传播和使用时造成泄密风险。

8、集团管控

采用分部式系统架构能够实现总部与分部间数据互联互通，可以将分部组织架构、密钥、安全策略等定时同步至集团总部，支持密钥集团统一管控；支持制定统一策略模板批量分配给分部；支持总部锁定分部策略实现策略一致性；支持日志分级汇总实现总部集中监管审计。

9、风险预警

终端违规行为、勒索病毒 / 恶意软件、涉密敏感数据大量 效规避设备端口泄密隐患。解密 / 外发 / 传播等，极易引发数据安全泄密风险，系统拥有完善的风险信息获取、分析、研判、预警和阻断机制保障数据安全。

10、安全审计

安全审计包括文件资产统计、全生命周期管理、解密审计、传播监控、外发审计、违规行为审计六大模块，通过精确地终端日志采集能力，全面评估企业数据资产安全态势，为企业构建完善的数据安全审计体系。

11、态势分析

提供统一的数据安全态势感知平台，对资产数量、泄密风险、异常行为等进行全面感知，对预警事件实时披露，以柱状图、饼图和趋势图等多种形式展现，多维度全方位展现企业整体数据安全态势。

12、U 盘客户端

将透明加密客户端植入 U 盘，合法用户可以根据需要将 U 盘插入任意电脑，即可打开和使用加密文档，无需连网加密服务器，无需携带办公电脑，主要适用于员工回家加班、出差等情况。

13、安全网关

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、终端访问日志等多方面进行应用数据安全访问控制，数据加密通过对应用系统核心数据进行上传解密、下载加密，解决企业核心数据离线安全使用。

14、安全中间件

安全中间件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。

终端安全管理系统

聚焦计算机终端用户行为管理、内网系统运维及全面的数据安全管理。

1、资产管理

能够自动化快速采集终端硬件资产和软件资产，方便资产盘点及安全运维管理。

2、软件分发

通过管理平台能够给客户端下发应用软件安装介质，支持静默和非静默安装，支持 exe、msi 类型的软件包。

3、端口管控

可以对计算机端口与存储设备进行安全控制，包括对 U 盘、移动硬盘、各类存储卡、同步软件、软驱、串口、并口、调制解调器、打印机、1394、红外、蓝牙、无线等的安全控制，有终端违规行为、勒索病毒 / 恶意软件、涉密敏感数据大量 效规避设备端口泄密隐患。

4、介质管控

支持介质在线注册申请，由管理员进行统一注册申请审批；支持注册类型包含：签名介质、专用介质。支持介质接入权限控制，只有经过授权的介质才能在内网使用，未授权的介质无法在内网使用。内网专用介质只能在内网使用，在外网无法使用。防止因非法使用介质造成数据泄密。

5、应用管控

管理员可通过平台下发策略，控制终端应用程序的使用，包括：允许运行、禁止运行、强制启动、强制卸载。

有相关数据安全需求的朋友们，请联系：400-898-1617

护航数据安全建设第十九期 | 数据安全防护之新一代数据泄露防护系统

数字化时代，高价值的数据不断产生，数据安全、隐私保护等问题成为继网络安全之后的又一重要安全话题，如何保障数据在创建、采集、存储、传输、交易、销毁的全生命周期安全变得至关重要。

新一代数据泄露防护系统（简称 DLP），以服务企事业单位进行数据资产梳理、数安全防护为目标。系统采用平台化管理，将终端 DLP、网络 DLP、邮件 DLP、存储扫描 DLP、API 接口 DLP 进行统一管理，模块化控制。将对数据进行分类分级扫描，实现终端数据资产梳理、文件服务器数据梳理、数据库数据资产梳理、数据加密防护、数据外发监测、终端运维管理、邮件外发控制、数据水印、端口管控。

系统以《数据安全法》为依据，从认识数据、梳理数据、分析数据（数据分类分级）、使用数据（数据共享与流转）、保护数据（数据加密）、数据交换、数据溯源分析（数据水印和血缘分析）、数据风险识别（机器学习和模型运算）、数据安全管控、用户行为分析，实现数据全生命周期安全（数据安全态势感知）。

产品价值

梳理清晰

数据梳理对象涵盖结构化、非结构化，来源囊括主机、服务器、网络、云端，实现数据资产清单输出和风险数据发现。

分类准确

以国家法律为依据，按照国家标准，参考行业标准，结合企事业单位实际数据特点，应用先进的数据识别引擎进行精准数据分类分级管控。

多方保护

应用行业领先的加解密技术对敏感数据进行加密保护，应用多维度内容识别技术和高效的监测、分析技术在数据外发通道上（网络、邮件、U 盘、光盘、蓝牙）筑起安全识别屏障。

风险追溯

采用水印技术、数据指纹、数据标签化、血缘分析、区块链等先进技术，结合数据多节点监测技术，实现对数据的风险识别、追踪溯源、派生分析、数据流转可视化。

产品优势

1、数据全生命周期管理

数据采集和分析过程涵盖了数据产生、流转、变形、派生、使用和销毁，是行业中唯一真正做到数据全生命周期管理的产品。

2、内容识别与加密防护相结合

安全行业唯一一款将数据内容识别技术与加密防护相结合的产品，全面应用了数据安全防护技术，风险控制无死角。

3、静态数据与动态数据联合分析

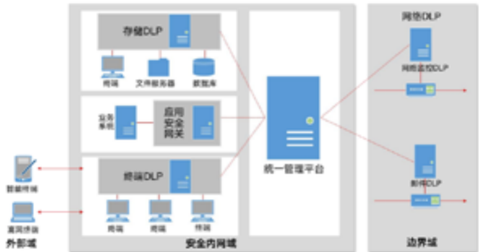
从终端主机、文件服务器、数据库服务器上的静态数据扫描，到网络外发、邮件外发、端口外发等的动态数据进行全覆盖安全防护，并进行数据联合分析和数据风险多场景模型运算和预警。

4、数据可视化、风险可视化

数据资产的可视化、敏感数据的可视化、风险预警可视化、安全态势可视化。

5、数据分类分级与使用者的权限结合管理

检测企业内部风险威胁，可以轻松检测和预测潜在的破坏，数据被盗或相关的异常用户行为。



关键功能

文档加密技术

系统采用驱动层加密技术，使用户无法通过常规手段进行强制移除或终止；即使用户通过强制手段破坏了客户端运行环境，系统也有相应的保护措施，确保加密机制的安全、高效和稳定。系统可实现对任意文档自动加密的功能，即文档定稿或归档时进行安全保护，保证数据完整性，同时不改变和影响用户使用习惯及工作效率；支持单个和批量文档加密。

数据分类分级技术

系统采用丰富的内容识别技术（关键词、正则表达式、文件属性、文件指纹、机器学习、文件伪装识别、文件嵌套识别、文件多层压缩、图片 OCR 识别），对数据进行分类分级检测，并进行数据标签化。建立起基于数据分类分级的数据资产管理体系和安全防护体系。

多数据源安全全覆盖

系统将终端主机数据、文件服务器数据、数据库存储数据、网络流量数据、邮件发送 / 接收数据、API 接口调用数据、数据安全交换数据进行了融汇贯通，联合分析，实现联合风险预警。此外，在基于敏感信息识别的基础上，结合电子文档加密技术实现联防联控，数据安全治理的目标。

数据血缘分析技术

采用数据标签化技术、数据水印技术、数据派生识别技术、机器学习、模型运算技术分析数据的产生，派生，变更，流转，使用过程，分析数据的全生命周期变化过程和并梳理流转途径。

风险告警与安全流程管控

系统支持邮件、企微、钉钉、syslog、kafka、sftp 等多种数据风险告警和共享技术，支持 restful 接口对接技术。系统支持邮件审批、企微审批、钉钉审批，实现快捷高效的管理和运营。

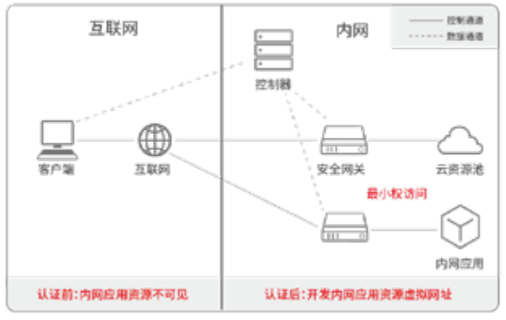
数据泄露防护体系的建设是企业数字化转型中的重要组成之一，促进了 DLP 产品、平台化产品在内的数据安全产品的市场需求持续增长。未来，亿赛通将持续深耕数据防泄露领域，保护企业和个人数据不被泄露和滥用，肩负起数据安全企业责任，为筑牢数据安全防线贡献力量。

护航数据安全建设第二十期 | 数据安全防护之零信任访问控制系统

零信任的雏形源于 2004 年成立的耶利哥论坛 (Jericho Forum)，2010 年零信任被 Forrester 正式使用。2014 年开始，谷歌基于内部项目 Beyond Corp 构建零信任架构，成功地摒弃了对传统 VPN 的采用，确保所有来自不安全网络的用户能安全地访问企业业务。

零信任理念是不区分内外网，针对核心业务和数据资产构建一体化的动态访问控制体系。在访问者和被保护资源之间建立动态的信任关系，根据信任的程度持续进行授权和权限调整。

亿赛通零信任访问控制系统（简称：ZT-ACS），主要针对数字化转型时代企业数据边界不清晰、云环境数据部署场景设计，产品的典型部件包括：客户端、网关、控制器。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。



产品价值

1、主机身份可信

通过统一企业应用访问的认证入口来确保主体身份唯一性，通过多种认证方式相结合来确保身份基础信息真实可信，以细粒度的应用、接口、数据等资源为核心保护对象，遵循最小权限原则，构筑端到端的逻辑身份边界。

2、数据防护全面

通过对数据发现和分类、数据活动监控、数据安全分析以及与身份的集成提供端到端的零信任覆盖。通过发现敏感数据所在的位置，可制定符合安全性、合规性和隐私目标的数据安全和治理策略。

3、访问操作合规

零信任以动态方式围绕每个连接进行防御，根据风险状态调整访问权限和其他特权，通过身份、数据安全和其他关键工具不断提供有关每个用户、设备和连接的上下文，可以构建配置文件，发现可能存在风险的人或事物，确保每个数据访问连接操作合规。

4、行为审计完善

系统提供完善的日志管理能力，按照经典“5W1H”方法详细记录系统操作及业务操作日期和时间、用户、事件类型、事件是否成功及其他与审计相关记录，方便事后追溯，完全满足《等保 2.0》、《关键信息基础设施网络安全保护基本要求》等文件关于安全审计的相关要求。

产品优势

1、减少业务暴露

在云原生时代，安全边界不再是数据中心边缘和企业网边缘的某个硬件盒子；且企业“内部”可能现在已经在公有云或混合云上了，不是完全可控的“内部”了。通过部署零信任访问控制系统后，业务无需暴露任何 IP 和端口，业务系统完全隐藏，恶意扫描、账号暴破等手段无法触达到业务服务器。

2、集中式运维管控

传统的安全防护体系采用白名单授权方式，这会造成白名单人数越来越多，管控压力越来越大。且白名单采用比较粗放的授权方式，无法实现细粒度授权。系统实现了统一业务访问入口，统一身份管理，统一权限管理，平台统一策略下发，减少运维压力。

3、弱身份强管控

过去，企业 VPN 访问密码被盗往往导致企业数据丢失，这是因为 VPN 通常允许用户对整个网络进行广泛的访问，从而成为弱身份、密码与访问管理中的薄弱环节。系统针对网络划分的每个逻辑单元制定独特的安全策略与规则，增强网络访问安全性。

关键功能

1、身份管理

以身份为基础，支持对组织、用户、终端、应用多种身份的统一管理。能汇聚多个身份源数据，通过对自然人、终端、应用的标识、凭据、属性等信息的分类管理，实现身份数据的归一化管理。

2、认证管理

主要基于身份管理构建身份认证模型，并可基于场景、因素、方式构建丰富、个性化的认证策略，能实现多种认证方式的认证服务，实现前端可信认证、后端权威核验。

3、分级管理

通过分布式部署、分级网关管控，可以将部署的所有网关纳入到控制中心进行统一管控，在控制中心可以管理多个网关，不同网关负责不同的应用代理和转发，实现应用与日志在集团和二级、三级公司的分级管控。

4、授权管理

零信任访问控制系统对接入的资源（应用、数据）进行集中权限管理，践行责任分离、最小化授权和数据抽象原则，通过建立基于角色的授权模型帮助管理人员实现对各类人员的权限最小化、集中授权与分类分级管理。

5、安全隧道

基于安全隧道、反向代理等技术实现为可信终端用户构建安全的应用访问隧道，隧道通信时采用高安全的加密算法，并可以定期更换秘钥，保证通信安全性，防止数据泄露，且通信时，报文无法中间篡改，针对不可以信终端、连接，直接采取默认丢弃请求报文，尽最大可能构建安全隧道。

6、应用隐身

产品采用预验证和预授权技术，实现客户端、应用间之间的地址、端口隐藏，让业务服务器、应用服务器的网址和端口只对授信的客户端可见，对非授权的客户端、其他工具完全不可见，最大程度减少内网应用资源暴露面。同时对端口扫描工具、SQL 注入等攻击起到一定的加固防护作用。

7、审计日志

依据相关法律法规，通过零信任访问控制系统记录账户、应用之间的访问日志记录，可记录应用访问时间、用户、操作行为、操作对象、操作结果等内容。

8、安全域隔离

根据用户类型和权限配置要开放的网络域 IP 和端口资源，用户终端登录 ZT-ACS 后，针对不同的用户下发不同的网络域访问权限，实现测试域和生产域安全隔离。

传统访问控制中，访问主体通过角色属性获取相应权限，但不适合当今快节奏、多样化、基于云的环境的需要。但是在零信任架构下，相对封闭的网络环境已经越来越少，逐步向开放式发展，亿赛通零信任访问控制系统，基于我司近二十年的实践经验研发，真正做到了“主体身份可信、访问操作合规、数据有效防护、行为操作审计”。

护航数据安全建设第二十一期 | 数据安全防护之数据追踪溯源系统

数据溯源是对目标数据衍生前的原始数据以及演变过程的描述。在数字经济时代，海量的数据和数据挖掘分析的需要，实际使用的数据大多是经过多次数据处理后的衍生数据。在数据使用时，常常需要通过追溯数据的来源，确认数据的确切含义、数据计算和错误排查等。

亿赛通数据追踪溯源系统（简称：TIS）是通过机器学习、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。

对数据资产和用户活动进行上报、分析、跟踪，可以为企业提供可视化的用户肖像，为企业提供完整数据资产全景以及用户效率分析。让企业数据行为可视化，为保障企业安全运营提供强有力的保障。



产品价值

系统以终端数据采集能力为核心，结合行为分析建模、UEBA、威胁行为检测、关联分析、机器学习、可视化等能力，帮助用户构造全天候数据安全态势感知系统的建设需求。

1. 数据资产发现：自动收集用户数据资产信息，自动收集用户历史操作文件信息。

2. 用户行为监控：通过对用户操作行为的监控，可以直观和准确确定用户行为威胁。

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

4. 数据追踪溯源：实现数据可视化展示，分析数据流转的全生命周期流转过程。

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

产品优势

1、记录每次数据移动

终端支持丰富的行为数据抓取，包括数据操作、数据轨迹、网络行为、用户行为、应用行为等。所有的行为可以生成可视化的数据和文本，可以直接进行查阅，并与用户活动相关联。

2、强大数据整合能力

TIS 将 UEBA、机器学习和大数据技术的精华整合为一个以数据为中心的综合审计和保护平台。通过对数据的重新构筑和关联，我们提供了一个强大的解决方案，首次缩小了实时世界和分析世界之间的差距。我们将运维团队从繁琐的手工工作中解放出来，并授权您的 IT 和安全团队用更少的资源做更多的事情。

3、行为和效率分析

基于用户操作行为数据，提供强大的数据和行为分析能力，帮助用户发现数据泄露、欺诈、滥用等安全问题，并可以发现员工之间潜在数据流通，通过用户行为数据的分析还可以分析用户工作时长、工作内容以及用户操作等，可以为企业提供用户完整数据活动轨迹。

产品优势

1、数据资产收集

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。

2、数据资产扫描

通过对用户终端数据数据扫描，发现终端存储存在的数据资产，可以帮助用户梳理和查看企业内部的数据资产。可以查看数据文件的文件名称、文件位置、文件类别、文件类型、文件属性、文件大小、文件指纹等数据的详细信息。通过探针对系统日志进行提取，收集用户历史操作行为。分析用户历史操作行为是否存在操作风险。

3、操作行为监控

终端探针对终端用户的操作行为进行监控并进行日志上报，可以通过服务器端查看用户终端的操作行为，如文件上传行为、文件下载行为、WEB 访问行为、U 盘拷贝行为、网络共享行为、文件删除行为等行为。可以查看用户操作文件的终端信息、文件名称、文件位置、文件类型、文件大小、应用进程、操作动作、操作时间、文件属性、文件指纹等信息。

4、操作录屏监控

系统支持对终端进行进行屏幕操作录制，可以通过服务器对终端录屏进行查询，除了可以对终端用户、终端信息、录制时间、URL 地址、应用软件等常规查询，我们还可以通过屏幕出现过关键字进行录屏查询，可以快速定位发现用户的操作行为。

5、用户行为分析

用户行为分析是通过对用户，设备，资产，应用程序事件进行关联分析，TIS 使用无监督和监督的机器学习和统计分析来建立正常行为的概况并检测异常。分析涉及统计分析，模糊相关，预测和顺序学习，机器人模式检测以及其他技术。任何与正常行为的偏差都会立即被标记并分配风险评分，提供企业用户风险评估依据。

6、风险行为分析

系统通过对用户操作行为进行配置，可以从用户海量的操作日志中提取用户风险操作行为。风险规则可以支持操作行为、操作时间、用户信息、终端信息、风险等级等的配置，用户可以细粒度配置企业内部不同部门的差异化的风险行为。

7、违规行为分析

系统通过对用户操作行为进行规则组配置，对用户特定操作泄密行为实现点滴式泄露监控，帮助用户发现企业内部蚂蚁搬家式数据泄露行为。

8、异常行为分析

系统采用大数据分析技术和神经网络等先进技术，对用户行为进行自动化学习，当用户行为与系统学习结果产生偏差时，系统会把相关的异常行为上报，同时系统还支持用户模型的增量学习来提高精准度。通过查看异常行为可以看到用户用户当时操作软件顺序与模型预测的操作软件顺序的差异，用于分析用户的异常行为。

9、用户威胁态势

通过对企业内部威胁行为检测结果，依照威胁类型，标识数据的数据类型、数据位置等，并支持威胁事件分类分级结果的报表展示。为企业提供了统一数据得统计、分析、稽核和展示。

10、用户行为画像

以“人”为中心刻画“数据”用户画像，依托用户威胁行为基线分析用户数据的异常访问行为。如图所示：用户状态、用户威胁分数、违规行为趋势、风险软件使用趋势、风险操作趋势、用户在线时长、用户空闲时长、数据资产分布等信息。

11、数据追踪溯源

通过对内部数据操作行为进行关联分析和溯源，查看某个数据流转全生命，同时也可以发现用户存在数据违规操作行为。系统还可以支持数据多级数据溯源。

通过关键字或者关键证据图片对企业内部操作进行溯源，可以帮助用户在海量的录屏视频中快速有效的定位用户威胁的操作行为。

12、数据统计分析

系统可以通过灵活的可视化配置，不仅展示企业数据资产全景，还可以根据客户的个性化需求进行自由配置。

利用强大的数据分析功能，所有数据结果都可以转化成视图，视图样式丰富如仪表盘、柱状图、趋势图、饼图和数据列表等，通过仪表盘面板中丰富的视图，能够以最直观的方式呈现企业关心的业务和数据，充分展现企业各方面的运行状态。

13、系统维护

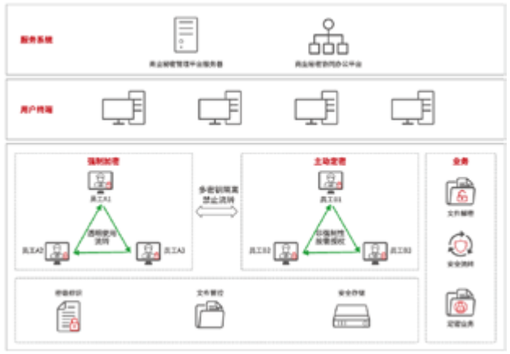
系统可以监控终端和服务器状态，在终端发生异常时，可以进行及时预警。

护航数据安全建设第二十二期 | 数据安全防护之商业秘密管理系统

商业秘密保护与企业的生存与发展息息相关，《民法典》明确将商业秘密纳入其中予以保护。强化商业秘密保护成为《中美经贸协议》的重要部分，直接推动了《反不正当竞争法》修订实施，最高院连续出台了一系列关于商业秘密的司法解释及其他规范性文件，提高商业秘密保护水平。尽管法律保护力度空前，但是企业对商业秘密的保护水平仍然很低，随着人才流动频繁，技术手段不断迭代，“员工跳槽”、“核心流失”、“另起炉灶”、“删库跑路”、“技术失窃”等事件层出不穷，不少人员漠视法律，致使企业丧失竞争优势的事例比比皆是。为此，亿赛通专门研发了商业秘密保管理系统，旨在助力企业的商业秘密保护和管理体系建设。

商业秘密管理系统（简称 TSM）是用于保护企事业单位商业秘密的安全管理软件。系统包含商业秘密文档定密、分类分级、集中管控、安全流转、安全保密、安全外发、商密用户评分等功能，完成对商业秘密文档的保护。

本系统的特色是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。



产品价值

定密准：确保商业秘密数据资料，全部按照保密制度要求，实施定密及加密技术防范措施保护；

责任实：落实相关保密协议书、保密责任书、竞业限制协议书等责任认定文档；

数据清：梳理数据清单以统计报表形式清晰展示给各级保密部门及垂直业务主管部门；

防护严：实现商业秘密数据加密保护，并可不同维度地检索、查询和统计，通过商秘数据行为统计、管理与分析，实时掌握商业秘密的管理情况动态。

产品优势

1、完整的商密业务管理

在商业秘密使用的同时，通过对流程的管理，有效的减少用户因违规操作而导致的泄密风险。

2、商业秘密安全保护

通过文件加密技术对商业秘密全生命周期的保护，有效减少了商业秘密泄露的风险。

3、商业秘密集中管理

通过保密盘技术和云安全技术对商业秘密的多样化、碎片化进行统一有效的管理，有效的保护了商业秘密因遗失导致的泄密风险。

4、用户行为可追溯

检测企业内部风险威胁，可以轻松检测和预测潜在的破坏，数据被盗或相关的异常用户行为。

5、商业秘密可视化

实现企业内部商业秘密可视化，展示企业商业秘密概况。

关键功能

1、文档加密技术

系统采用驱动层加密技术，使用户无法通过常规手段进行强制移除或终止；即使用户通过强制手段破坏了客户端运行环境，系统也有相应的保护措施，确保加密机制的安全、高效和稳定。系统可实现对任意文档自动加密的功能，即文档定稿或归档时进行安全保护，保证数据完整性，同时不改变和影响用户的任何使用习惯及工作效率。支持单个和批量文档加密。

2、文档加密授权技术

通过灵活的分级设置，用户可按照部门、项目组、指定用户名等角色设置访问权限，并加上标识，实现对高密级文件进行隔离管理。同时可提供精细化文件权限控制，如文档的阅读、编辑、打印权限，以及阅读次数、阅读时限等文档生命周期的控制管理。

3、安全存储保护技术

系统自动在当前用户物理机硬盘中创建一个隐藏的加密空间，即“保密盘”，以供用户存储个人及企业重要文件使用。退出系统后此空间将隐藏在物理硬盘中，免受他人恶意窃取或黑客攻击。“保密盘”采用数据单向隔离及重定向技术，确保数据的安全隔离。

4、文件集中管理技术

建立高效、安全的商密协作云平台，实现内部文档通过统一系统进行管理和传递。商密协作云平台支持用户流程操作、业务操作、安全共享、内部共享、外链分享等功能，实现数据与业务双传递。

5、流程管控技术

系统支持商密项目与商密行为配置和管理，建立商密保护流程和评价体系，包含商密项目管理、商密保密承诺书签署、商密文件定密以及商密行为量化考核，流程方式灵活可配，保证客户业务的快速响应。

亿赛通小贴士 ESAFENET PROMPT

护航数据安全建设第二十三期 | 数据安全流转之数据脱敏系统

随着数据存储和使用场景复杂程度的大幅提高，隐藏在数据背后可被挖掘的信息也逐渐丰富，数据面临的泄露风险与日俱增。国家、行业主管部门对于数据安全的管理制度愈加严格与完善，同时在数据共享使用的一些场景中对于脱敏数据的仿真程度、脱敏效率等要求也越来越高。为了适应这些变化和需求，专业的脱敏产品应运而生。

亿赛通数据脱敏系统（简称：DMS）是亿赛通自主研发的一款软件数据安全产品，产品可用在开发测试环境、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。

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

产品能力

脱敏数据源

1、支持多种数据库类型，涵盖主流关系型、NoSQL、大数据和国产化数据库类型；

2、支持云数据脱敏，支持 RDS 数据库。

敏感数据发现能力

1、支持身份证号、银行卡号、手机号码 、地址、税号等 34 种敏感数据的发现能力；

2、支持正则式、算法文件、特征字典等多种方式的自定义数据扫描规则；

3、支持对内置、用户自定义的数据扫描规则进行数据识别测试。

脱敏算法

1、支持数据遮蔽、随机字符串、重置固定值、加盐 Hash 四种通用脱敏算法；

2、支持特征字典、随机字典、算法文件等多种方式的添加自定义脱敏算法；

3、支持对所有的脱敏算法进行脱敏效果测试。

脱敏方案

1、能够制定丰富的脱敏方案；

2、脱敏方案能够提供多种多样的方案配置；

3、可支持业务脱敏和运维脱敏。

静态数据脱敏

静态脱敏主要通过脱敏规则进行数据变形，实现敏感信息的可靠保护，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。

动态数据脱敏

动态脱敏主要通过实时对流量中数据库协议解析，可以实时对数据库相应数据进行脱敏，可针对对人员、权限、客户端、主机、时间等不同维度配置脱敏策略，针对待脱敏数据可以进行替换、屏蔽、数据偏移、数字随机化等方式进行脱敏处理。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。同时针对高危操作，还可进行阻断。保护敏感信息，不被违规查询泄露，防止恶意操作和误操作，提升数据安全性。

国际乒联服务器出安全问题，数百名乒乓球运动员信息泄露

近日，由于国际乒联的服务器出现安全问题，数百名乒乓球运动员的护照细节和疫苗接种证明等被泄露。其中，中国运动员马龙和樊振东的护照信息也在其中。

对此，国际乒联发言人回应称，“一位独立的技术专家提醒我们注意服务器上的一个安全问题。国际乒联在得知后立即获得了访问权限。文件只在此处存储了很短一段时间，我们没有证据表明在相关报道之前有人访问过个人信息。”该发言人还表示，机构对这一事件感到遗憾，并正在联系受影响的相关成员协会。安全和数据隐私对国际乒联来说是最重要的。目前乒联已经实施了额外的安全措施，并将监控可疑活动且正在进行彻底的安全审查和调查。如今，全球各个领域都开始意识到数据资产的巨大价值，保障数据安全就成为了这一时代的刚需。当一家企业无法确保数据安全时，将会给用户以及公司带来巨额的经济损失和信誉损失，甚至是企业难以经营发展面临倒闭的严重后果。

有一些企业认为，重要的数据信息往往仅在内部网络甚至是涉密网络中运行，黑客窃取数据的难度较高。然而，拥有较高权限的管理、运维、工程师等角色，可能更容易接近这些核心敏感数据，这些人员一旦出现主动或者被动的造成数据泄露，其后果的严重性将无法预估的。

纵观国内外被公开的数据泄露事件，对企业和组织带来的损失将是多方面的，这其中除了经济损失，还存在品牌信誉和业务影响。数据泄露的根本原因都在于企业数据安全体系的不完整，数据作为企业的源动力，其安全防护应结合企业特定环境，形成适合企业的纵深防护体系。

其实，在国际乒联这件事情上，根本原因是内部防护不到位，数据安全意识薄弱，未来务必要将安全意识和技术手段结合起来共同保护运动员隐私信息。不仅仅是国外机构，国内亦如此。在数字经济的快速发展下，亿赛通不断提升产品品质及提高服务能力，全新推出“分·放·管·服”数据安全建设理念，并在理念指导下，研发 60 多款精细化产品，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。

亿赛通数据安全综合解决方案管理可以有效支撑企事业单位数据资产管理业务，提升安全工作的发现、管控能力与处理效率。若要详细了解亿赛通数据安全综合解决方案，保障企业数据安全，可咨询服务热线：400-898-1617。

文章内容部分来源于互联网

国际数据安全市场研究之蓬勃发展的数据安全行业

行业研究部 张艺伟 / 文

从数字经济发展的洪流中可以看到，全世界数据安全行业产业呈现蓬勃发展之势，前进趋势不可阻挡。那么，国际数据安全市场目前究竟如何呢?

数据安全和隐私立法普及呈现鲜明的“国情特色”

世界主要国家高度重视数据和安全，但对于数据安全的理解，总体上与各国发展阶段和数字化程度密切相关，并不存在统一认知与概念界定，政策实践亦呈现鲜明的“国情特色”。根据联合国贸易发展组织（UNCTAD）统计，除中国外，截至 2022 年 2 月 21 日，全球约 80% 的国家已完成数据安全和隐私立法，其中包括欧盟成员国、美国、俄罗斯、印度、澳大利亚、加拿大和日本等。在立法精神方面，世界主要国家和地区基于自身所处国际局势、技术、产业发展情况等因素，呈现出或开放或保守或平衡的数据安全战略。

1、美国鉴于自身的技术和产业优势，从发展利益出发，对数据持积极开放的态度，坚持以市场为主导、以行业自律为手段，总体呈现“相对宽松”的政策导向。比如，在数据跨境方面，美国坚持“促进型”政策，主张在保障国家安全的前提下促进数据最大程度地自由流动。

2、欧盟虽然将数字产业发展列为实现未来竞争力的战略方向，但目前来看规模有限，其对数据安全的关注更多从“理念”与“规则”塑造层面入手，提出将价值观、个人权利和市场价值相结合的“欧洲数据理念”。比如 2018 年，欧盟发布《通用数据保护条例》（GDPR），明确用户对属于自己个人的数据具有绝对掌控权，规定欧盟所有成员国企业在收集、传输、保留、使用个人信息上都必须取得用户的同意，为全球其他国家和地区的相关政策制定提供了高价值参考。

3、俄罗斯从维护国家安全的角度出发高度重视数据安全，不断收紧对数据的整体控制，并呈现出从数据本地化向“断网行动”转变的极端趋势。比如，《俄罗斯联邦个人数据法》规定，所有运营商须确保俄罗斯公民的个人数据通过位于俄罗斯境内的数据库进行记录、存储、调整、提取等操作，且须永久存储。

4、中国基于总体国家安全观，数据安全政策整体比较务实平衡。一方面将数据作为重要生产要素和基础战略资源，提出建设全方位的数据安全保障体系；另一方面加强政策引领，推动数字经济和实体经济深度融合、实现经济转型。

合规需求驱使下全球数据安全市场蓬勃发展

随着数字化进程的加速，数据上升为国家基础性、战略性资源，以数据作为关键生产要素的数字经济成为当前各国高质量发展的新引擎。在新经济体高速发展的同时，网络数据呈现指数级增长，数据暴露面持续加大，数据安全风险形势日益严峻。2021 年全球数据总量高达 320ZB，数据泄露的平均总成本达 424 万美元。在此背景下，数据安全成为 IT 行业中最热门的领域之一。市场规模方面，2021 年全球数据安全市场价值约为 190 亿美元，预计到 2027 年将达到 542.3 亿美元。融资并购方面，2020 年，国际“数据安全”方向融资金额占比 13%，仅次于“风险管理与合规”，排名第二；数据安全的并购活动占比显著提升，2020 年占比 7%，排名第六。资金投入方面，2021-2026 年，全球数据安全市场投资规模增长率将达 CAGR13.3%，2026 年投资额将高达 149.5 亿美元。

敏感数据识别、数据脱敏技术向智能化、场景化发展

1、敏感数据识别技术

该技术在国际市场智能化应用成熟，已实现全面商业化。在传统的关键字识别基础上，通过引入规则匹配、自然语言处理等扩大识别范围，提高识别精度。同时，结合聚类分析等机器学习技术，通过大数据的累积训练提升敏感数据识别的智能化程度。针对数据的使用、存储、传输等数据泄露高风险阶段，通过将组件部署在企业数据流动的关键节点,实现对数据泄露行为的预警发现和拦截处置。

2、数据脱敏技术

数据脱敏技术根据业务场景及需求，在保密、群体信息统计、数据可逆需求场景下获得差异化应用。在保密场景下，使用加密技术对数据进行脱敏，有效保护个人数据；在群体信息统计场景下，使用数据失真技术，实现个人信息去标识化，同时输出统计结果数据；在数据可逆需求场景下，采用位置变换、表映射等方式实现数据脱敏，最大限度保障数据的可用性。

数据匿名化、新型加密技术的落地实践应用取得初步成效

1、匿名化技术

根据特定算法对数据进行变换，在保证数据可用性的同时确保数据无法定位到个人且无法还原，从而达到保护个体隐私信息的目的，主要包括差分隐私、K 匿名等。近年来，数据匿名化技术得到业界广泛关注并在数据交换、数据分析等环节初步开展应用。

2、新型加密技术

量子加密、后量子加密等新型加密技术涌现，探索实践工作获得初步成效。随着云计算、量子计算等新兴技术的发展以及计算机处理速度的提升，传统加密算法的效率与强度逐渐难以满足业务需求，被破解失效的风险日益提升。在此背景下，量子加密、后量子加密等新型加密算法被不断提出。

综上所述，全球数据安全市场处于高速发展阶段，中国作为全球最大的数字经济国家之一，“数据安全”已成为当下以及未来发展的趋势。从技术角度来看，新型加密技术、敏感数据识别及脱敏技术将是数据安全行业发展的重要能力之一。亿赛通在数据安全防护技术上以“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。

而敏感数据识别、加密技术及脱敏技术更是亿赛通数据治理和数据安全的组件，采用敏感数据识别，助力企业厘清重要数据资产、确定数据重要性或敏感度，并针对性地采取适当、合理的管理措施和安全防护措施，形成一套科学、规范的数据资产管理与保护机制，从而在保证数据安全的基础上促进数据流通防护。

政策解读：《工业和信息化领域数据安全管理办法（试行）》

行业研究部 张艺伟 / 文

12 月 13 日，《工业和信息化领域数据安全管理办法（试行）》在工信部官网公开发布，并于 2023 年 1 月 1 日起正式施行。《办法》作为工信领域数据安全管理顶层制度文件，共八章四十二条，重点解决工业和信息化领域数据安全“谁来管、管什么、怎么管”的问题。主要内容包括七个方面：一是界定工业和信息化领域数据和数据处理者概念，明确监管范围和监管职责。二是确定数据分类分级管理、重要数据识别与备案相关要求。三是针对不同级别的数据，围绕数据收集、存储、加工、传输、提供、公开、销毁、出境、转移、委托处理等环节，提出相应安全管理和保护要求。四是建立数据安全监测预警、风险信息报送和共享、应急处置、投诉举报受理等工作机制。五是明确开展数据安全监测、认证、评估的相关要求。六是规定监督检查等工作要求。七是明确相关违法违规行为的法律责任和惩罚措施。其将与《工业领域数据分类分级指南（试行）》（2020.2）《工业互联网企业网络安全 第 4 部分：数据防护要求（征求意见稿）》（2022.11）等文件一起，成为工业领域数据安全保护工作的合规指南。

发布背景

2021 年 9 月 1 日，《数据安全法》正式施行，依法开展数据安全工作踏上了新征程。工业领域作为《数据安全法》中提及的行业领域之首，是当前强化数据安全保障的重要领域。随着企业上云、工业 APP 培育等工作持续推进，工况状态、产能信息等数据向云平台加速汇聚，高价值的数据资源池成为不法分子的攻击目标。此外，新一代信息技术与制造业融合发展模式下，工业生产环境互联开放趋势加快，工业数据的流向、路径、汇聚点等都发生了变化，数据从流向企业本地孤立的业务系统，到流向外部的边缘节点、大数据中心等，贯穿了企业控制网、管理网、专用网、互联网等各个网络，数据安全涉及设备层、控制层、网络层、平台层及应用层各个层面，数据暴露面加大，数据安全风险点增多，数据安全影响面更广。

适用范围

在中华人民共和国境内开展的工业和信息化领域数据（工业数据、电信数据、无线电数据等）处理活动（数据收集、存储、使用、加工、传输、提供、公开等）及其安全监管，应当遵守相关法律、行政法规和本办法的要求。军事领域、涉密领域、政务数据的处理活动，按照有关规定执行。

监管职责

工信部负责监督指导地方工业和信息化主管部门、地方通信管理局、地方无线电管理机构等地方行业监管部门开展数据安全监管工作，地方行业监管部门分别负责对本地区工业、电信、无线电数据处理者的数据处理活动和安全保护进行监督管理。

内容要点

一、术语定义

1、工业数据

工业各行业各领域在研发设计、生产制造、经营管理、运行维护、平台运营等过程中产生和收集的数据。

2、电信数据

在电信业务经营活动中产生和收集的数据。

3、无线电数据

在开展无线电业务活动中产生和收集的无线电频率、台（站）等电波参数数据。

4、工业和信息化领域数据处理者

数据处理活动中自主决定处理目的、处理方式的工业企业、软件和信息技术服务企业、取得电信业务经营许可证的电信业务经营者和无线电频率、台（站）使用单位等工业和信息化领域各类主体。按照所属行业领域可分为工业数据处理者、电信数据处理者、无线电数据处理者等。

二、数据分类分级管理

1）、职责分工

1、工信部负责制定标准、指导工作、明确重要数据和核心数据具体目录。

工信部部组织制定工业和信息化领域数据分类分级、重要数据和核心数据识别认定、数据分级防护等标准规范，指导开展数据分类分级管理工作，制定行业重要数据和核心数据具体目录并实施动态管理。

2、地方行业监管部门负责本地区管理、明确本地区重要数据和核心数据具体目录。

地方行业监管部门负责识别分别组织开展本地区工业和信息化领域数据分类分级管理及重要数据和核心数据识别工作，确定本地区重要数据和核心数据具体目录并上报工业和信息化部，目录发生变化的，应当及时上报更新。

3、数据处理者负责定期梳理数据、识别重要数据和核心数据。

工业和信息化领域数据处理者应当定期梳理数据，按照相关标准规范识别重要数据和核心数据并形成本单位的具体目录。

2）、数据分类规则

1、分类判定因素

行业要求、特点、业务需求、数据来源和用途

2、分类维度

包括但不限于研发数据、生产运行数据、管理数据、运维数据、业务服务数据等。

3）、数据分级规则

1、分级判定因素

根据数据遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益等造成的危害程度，综合判定安全级别。

2、分级框架

工业和信息化领域数据分为一般数据、重要数据、核心数据三个级别。

3、一般数据判定标准

- 对公共利益或者个人、组织合法权益造成较小影响，社会负面影响小；
- 受影响的用户和企业数量较少、生产生活区域范围较小、持续时间较短，对企业经营、行业发展、技术进步和产业生态等影响较小；
- 其他未纳入重要数据、核心数据目录的数据。

4、重要数据判定标准

- 对政治、国土、军事、经济、文化、社会、科技、电磁、网络、生态、资源、核安全等构成威胁，影响海外利益、生物、太空、极地、深海、人工智能等与国家安全相关的重点领域；
- 对工业和信息化领域发展、生产、运行和经济利益等造成严重影响；
- 造成重大数据安全事件或生产安全事故，对公共利益或者个人、组织合法权益造成严重影响，社会负面影响大；

亿赛通小贴士 ESAFENET PROMPT

- 引发的级联效应明显，影响范围涉及多个行业、区域或行业内多个企业，或者影响持续时间长，对行业发展、技术进步和产业生态等造成严重影响；
- 经工业和信息化部评估确定的其他重要数据。

5、核心数据判定标准

- 对政治、国土、军事、经济、文化、社会、科技、电磁、网络、生态、资源、核安全等构成严重威胁，严重影响海外利益、生物、太空、极地、深海、人工智能等与国家安全相关的重点领域；
- 对工业和信息化领域及其重要骨干企业、关键信息基础设施、重要资源等造成重大影响；
- 对工业生产运营、电信网络和互联网运行服务、无线电业务开展等造成重大损害，导致大范围停工停产、大面积无线电业务中断、大规模网络与服务瘫痪、大量业务处理能力丧失等；
- 经工业和信息化部评估确定的其他核心数据。

4）、重要数据、核心数据备案规则

1、数据处理者向本地行业监管部门备案。备案内容包括但不限于数据来源、类别、级别、规模、载体、处理目的和方式、使用范围、责任主体、对外共享、跨境传输、安全保护措施等基本情况，不包括数据内容本身。

2、地方行业监管部门二十个工作日内审核备案申请。若审核通过，将备案情况上报工信部。若审核未通过，及时反馈备案申请人并说明理由。备案申请人应当在收到反馈情况后的十五个工作日内再次提交备案申请。

3、备案内容发生重大变化的，数据处理者应当在发生变化的三个月内履行备案变更手续。重大变化是指某类重要数据和核心数据规模（数据条目数量或者存储总量等）变化30%以上，或者其它备案内容发生变化。

三、数据全生命周期安全管理

1）、总体安全要求

1、一般数据处理者

建制度：建立数据全生命周期安全管理制度，针对不同级别数据，制定数据收集、存储、使用、加工、传输、提供、公开等环节的具体分级防护要求和操作规程；

配人员：根据需要配备数据安全管理人员，统筹负责数据处理活动的安全监督管理，协助行业监管部门开展工作；

确权限：合理确定数据处理活动的操作权限，严格实施人员权限管理；

定预案: 根据应对数据安全事件的需要，制定应急预案，并开展应急演练；

开培训：定期对从业人员开展数据安全教育和培训；

留日志：记录数据处理、权限管理、人员操作等日志。日志留存不少于六个月。

2、重要数据和核心数据处理者

明确数据安全责任人：建立覆盖本单位相关部门的数据安全工作体系，明确数据安全负责人和管理机构，建立常态化沟通与协作机制。本单位法定代表人或者主要负责人是数据安全第一责任人，领导团队中分管数据安全的成员是直接责任人；

明确关键岗位和职责：明确数据处理关键岗位和岗位职责，并要求关键岗位人员签署数据安全责任书，责任书内容包括但不限于数据安全岗位职责、义务、处罚措施、注意事项等内容；

建立内部登记、审批等工作机制：对重要数据和核心数据的处理活动进行严格管理并留存记录；

开展风险评估：自行或委托第三方评估机构，每年对数据处理活动至少开展一次风险评估，及时整改风险问题，并向本地区行业监管部门报送风险评估报告。

2）、各环节处理活动安全要求

处理环节	一般数据	重要数据	核心数据
收集	遵循合法正当原则 采取分级安全措施	加强收集人员、设备管理 记录收集来源、时间、类型、数量、流向等信息 间接获取数据，数据处理者和提供方须签署协议并明确双方责任	
存储	依法依约存储	采取校验、密码等安全存储技术 实施容灾备份 实施存储介质安全管理 定期开展恢复测试	
使用加工处理	保证自动化决策公平透明 涉及电信业务的数据处理，应取得电信业务经营许可	加强访问控制	
传输	按照数据类型、级别、应用场景，制定安全策略，采取保护措施	采取校验、密码、安全传输通道或安全传输协议等措施	
提供	明确范围、类别、条件、程序	与数据获取方签订安全协议 核验获取方数据安全保护能力	评估安全风险 采取安全措施 经本地区行业监管部门审查上报工信部
公开	对国家安全、公共利益存在重大影响的不得公开		
销毁	建立数据销毁制度 明确销毁对象、规则、流程、技术要求 记录销毁轨迹	禁止恢复 履行备案变更手续	
出境	境外工信领域执法机构获取数据，须获得我国工信部批准	法律法规有境内存储要求的，在境内存储 确需出境的，申请数据出境安全评估	
转移	明确转移方案 通知受影响用户	履行备案变更手续	评估安全风险 采取安全措施 经本地区行业监管部门审查上报工信部
委托	签订合同协议，明确委托、受托双方责任义务	核验受托方数据安全保护能力和资质	评估安全风险 采取安全措施 经本地区行业监管部门审查上报工信部

四、数据安全监测和应急管理

1、工信部

1、建立数据安全风险监测机制，组织制定监测预警接口和标准；

2、建立数据安全风险信息上报和共享机制，统一汇集、分析、研判、通报风险信息；

3、制定数据安全事件应急预案，组织协调重要、核心数据安全事件应急处置。

2、地方行业监管部门

1、建立本地区数据安全风险监测机制，组织开展安全风险监测，及时发布预警信息；

2、汇总分析本地区数据安全风险，将可能造成重大安全事件的风险及时上报工信部；

3、开展本地区数据安全事件应急处置工作，涉及重要、核心数据的安全事件立即上报工信部。

3、数据处理者

1、开展数据安全风险监测，及时排查安全隐患，采取必要措施防范风险；

2、将可能造成较大安全事件的风险上报本地行业监管部门；

3、按照应急预案及时开展应急处置，涉及重要、核心数据的安全事件第一时间上报本地区行业监管部门，并每年上交事件处置总结报告。

某储蓄银行数据库安全项目案例



一、项目背景

某储蓄银行是中国领先的大型零售银行，目标是服务社区、服务中小企业、服务“三农”，致力于为中国经济转型中最具活力的客户群体提供服务。同时，邮储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。本项目为公司数据安全项目重要组成部分，实现对银行内所有重要数据库操作进行全面记录和审计，发现其中的高危风险操作行为并及时上报，以便及时响应，减少和避免银行相应损失。

二、项目目标

目标一：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。

目标二：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。

目标三：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；

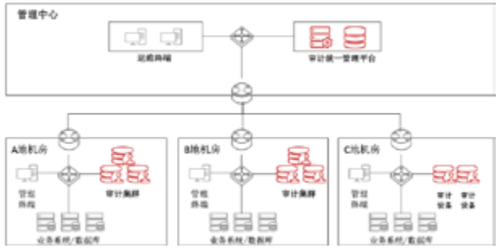
2) 总部为分公司提供有效工具和方法，赋予分支机构数据安全风险管理的能力。

三、项目方案

项目通过对银行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。

1. 部署情况

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：



2. 重点技术支撑

本项目为异地多中心部署模式，在交付过程当中，根据客户自身的行业特点和管理机制，对实施方案进行了较大的改进，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。

3. 项目规模

主要数据库类型：Oracle、openGauss。

重要数据库实例：200+，审计流量：>5Gbps，日志量：20 亿条 / 天。

两地三中心，两级管理部署。

1 个统一管理平台，2 个审计集群，共 8 个审计节点。

四、客户价值

价值一：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，同时满足银行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。

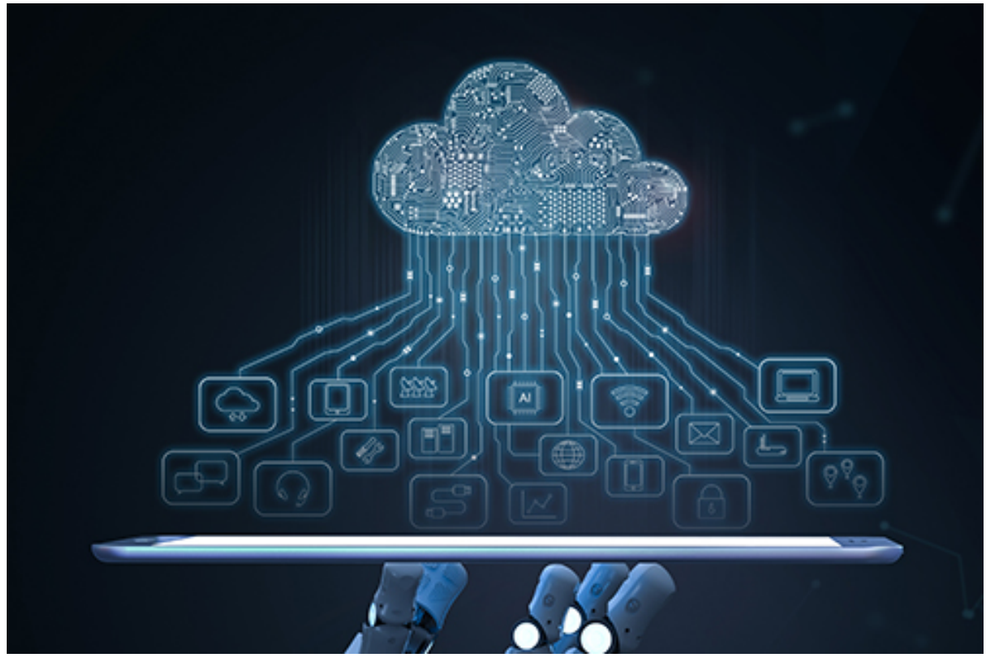
价值二：实现数据安全监管与赋能

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。

价值三：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。

云数据安全解决方案



行业需求

随着企业上云越来越朝着多样化发展，数据安全管理和保护方面的挑战日益凸显。在云计算环境下，网络架构已不同于传统网络，打破了传统的信息安全保障体系设计、实现方法和运维管理体系。云端数据安全则是云安全中最核心的问题之一。不同于本地部署，在云端还需要考虑云计算网络环境中虚拟化部署的场景、云端环境的多租户场景等。

典型案例 TYPICAL CASES

风险分析

1、云端数据面临来自租户自身内部人员的威胁，租户内部人员可最大权限对云端数据进行增删改查；

2、数据库漏洞攻击、SQL 注入、拖库、撞库等；

3、云端数据下载到本地终端后，数据不再受控，容易导致敏感数据泄露；

4、内部人员、开发、测试使用云端敏感数据未做脱敏处理，造成数据泄露。

解决方案

亿赛通云数据安全解决方案支持各大公有云和私有云平台，满足用户数据上云后，数据在云平台的全生命周期安全；产品支持 VMware、Openstack 等多种主流云平台架构。

云数据安全防护能力包括：云数据安全运营管理平台、云数据库审计、云数据库防火墙、云数据脱敏、云安全网关、云网络数据审计、云数据加密等，帮助用户满足合规性要求。



方案收益

为用户提供从数据识别到数据防护、异常行为分析检测等一套完整的数据安全防护能力，让云上用户能够清晰的了解到自己的数据存放在哪里，被哪些人访问，是否存在安全风险等等，以提升云上用户整体数据安全水平，有效降低敏感数据泄露风险。