亿赛通 ESAFENET

ESAFENET

亿赛通企业月刊　　中国数据安全专家　　www.esafenet.com

08 月刊

2022 年共 11 期

关注企业官方微信

联系我们

地址：北京市海淀区西二旗大街 39 号 A 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com

关注官方微信公众号　关注官方微信服务号　关注官方微信视频号　关注官方抖音号

Esafenet
Monthly magazines

中国数据安全专家

主办：亿赛通市场部

北京亿赛通科技发展有限责任公司

地址：北京市海淀区西二旗大街 39 号 A 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com

CONTENTS目录

刊首语 PREFACE

《亿赛通八月刊》探索数据安全运营新生态

习近平总书记曾强调，网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国。数字经济成为我国经济发展中创新最活跃、增长速度最快、影响最广泛的领域，推动生产生活方式发生深刻变革。亿赛通紧跟国家步伐，高度关注国家层面关于数据安全方面的顶层设计、法律法规体系的建设，标准的推行等，结合自身技术优势，推出了一整套从上到下的综合数据安全治理解决方案。《亿赛通八月刊》独家分享企业数据安全运营管理新技能，与企业共同构建信息保护多方参与综合治理的良好生态。

国内

1、突发！ 4850 万上海随申码用户数据遭泄露

摘要：近日，记者发现，有发帖者以 4000 美元（约合人民币 26936 元）拍卖上海随申码数据库，发帖者称其中包含 4850 万用户的上海随申码数据，“自上海随申码推行以来，所有居住和到访过上海的人员信息。”

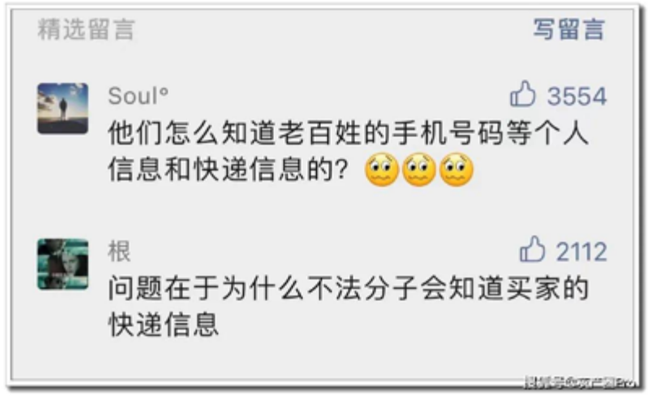
2、查办下游电诈犯罪溯源上游泄露信息“内鬼”

摘要：近年来，电信网络诈骗犯罪多发高发形势严峻，在刑事犯罪案件中占据很大比重。数据显示，自 2021 年 4 月至 2022 年 7 月，全国共破获电信网络诈骗案件 59.4 万起。案件高发背后，非法泄露公民个人信息是网络犯罪链条中关键环节。今年，全国人大常委会办公厅共确定 22 项重点督办建议。其中，加强和创新社会治理，改善人民生活品质方面涉及的 6 项选题中，就包含“严厉打击电信网络犯罪，加强个人信息司法保护”的建议。

3、“中间商”落网！他向境外泄露公民信息 10 万条！

摘要：今年年初，芜湖警方成功捣毁一帮助境外诈骗分子“吸粉引流”的犯罪团伙。团伙头目孔某，为攫取不正当利益，自愿成为其“下线”，为诈骗集团提供“引流”服务。并在网上以“用工为名”招募话务人员，根据诈骗团伙提供的受害人电话号码，要求话务人员冒充证券公司客服，以“加入微信群分享股票信息”为由，成功引流几千人。近日，芜湖市公安局弋江分局办案民警成功锁定该“团伙”上线落脚点，并于 8 月 18 日远赴海南，将嫌疑人欧某抓获归案。

4、500 余万条个人信息从快递站泄露！



摘要：今年 4 月，余姚市发生多起冒充物流网购客服退款赔偿类电诈案件，余姚警方在对这些受害人电话回访时发现，多数的受害人提到，他们的快递都曾停留在一快递始发云仓，民警对该快递始发云仓进行调查后发现，今年 3 月份，曾有一名神秘男子，在深夜翻墙进入过仓库，并对该仓库内一台专门打印快递面单的电脑动了手脚。经侦查民警发现，这个用来打印面单的电脑，被人安装了木马程序。这种木马软件原本应用于企业管理，被犯罪嫌疑人篡改软件功能后，通过植入到打印快递面单的电脑中，便会在电脑后台，将打印信息实时发送出去，以此来窃取快递面单信息。

5、国内某银行疑似数据泄露高达 1679 万条！

摘要：有人在某国外论坛中发帖售卖国内某银行 1679 万笔数据，并放出部分数据样本，数据包括名字、性别、卡号、身份证号、手机号码、所在城市、联系地址、工作单位、邮编、工作电话、住宅电话、卡种、发卡行等等。贩卖者以“8.8BTC”价格在某国外论坛发帖售卖，并放出部分数据样本，数据包括名字、性别、卡号、身份证号、手机号码 、所在城市、联系地址、工作单位、邮编 、工作电话、住宅电话、卡种、发卡行等等。

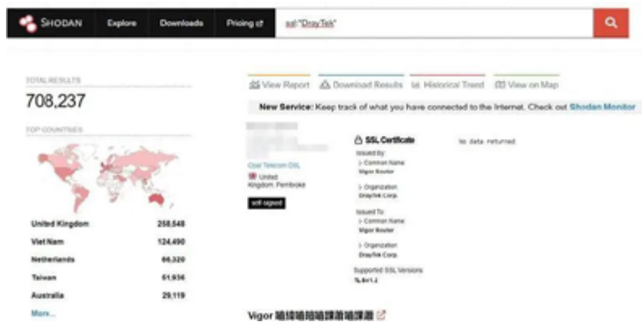
6、“即刻 PDF 阅读器”内置后门收集用户隐私

摘要：近期，有团队发现“即刻 PDF 阅读器”内置后门程序，该后门程序会在用户不知情的情况下，从 C&C 服务器上下载恶意配置文件，再根据配置文件下载恶意模块到用户电脑中。目前发现该病毒会肆意收集用户个人隐私信息，如：QQ 号、淘宝昵称、电商购物记录、电商和搜索引擎搜索记录等隐私数据。

7、超过 8 万台海康威视摄像头受漏洞影响

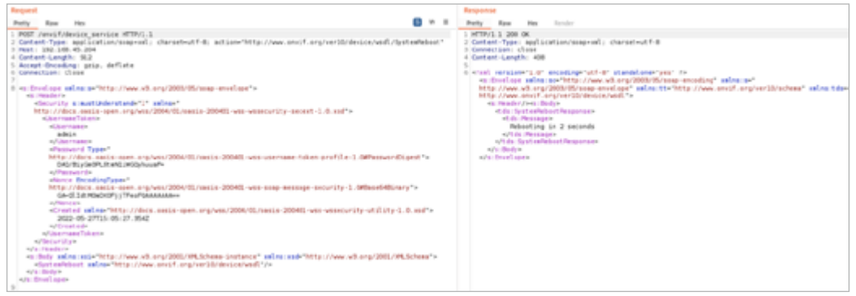
摘要：安全研究人员发现有超过 8 万台海康威视摄像头受到 CVE-2021-36260 漏洞的影响。CVE-2021-36260 漏洞是一个命令注入漏洞，攻击者利用该漏洞可以发送伪造的消息给有漏洞的 web 服务器以实现命令注入。海康威视已于 2021 年 9 月通过固件更新修复了该漏洞。但 CYFIRMA 研究人员发现分布在 100 个国家和地区的 2300 个组织内的数万设备仍然没有应用更新修复漏洞。

8、DrayTek 路由器爆远程代码执行漏洞



摘要：DrayTek 是一家位于中国台湾的网络设备制造商，其生产的设备主要包括路由器、交换机、防火墙以及 VPN 设备等。Trellix Threat 实验室研究人员在 DrayTek Vigor 3910 路由器中发现了一个非认证远程代码执行漏洞，漏洞 CVE 编号 CVE-2022-32548，CVSS 评分 10 分。该漏洞影响多款 DrayTek 路由器设备。如果设备管理接口被配置为 Internet-facing(面向 Internet)，那么该漏洞的利用就无需用户交互。此外，还可以在局域网内默认设备配置下进行零点几攻击。攻击可以完全控制设备，以及对内部资源的非授权访问。

9、CVE-2022-30563：浙江大华网络摄像机安全漏洞



摘要：Nozomi Networks 研究人员在大华部分 IP 摄像机产品 Open Network Video Interface Forum（ONVIF，开放式网络视频接口论坛）标准规范 WS-UsernameToken 认证机制的实现中发现了一个安全漏洞，漏洞 CVE 编号 CVE-2022-30563，CVSS 评分 7.4 分。攻击者利用该漏洞嗅探之前未加密的 ONVIF 交互、在新的请求中重放该凭证，最终实现入侵网络摄像机的目的。

10、银保监会出手，收集、泄露个人金融信息乱象该停了

摘要：8 月 24 日，上证报从业内人士处获悉，银保监会近日下发了《中国银保监会办公厅关于开展银行保险机构侵害个人信息权益乱象专项整治工作的通知》（下称“通知”）。目前已有多家银行、理财公司、保险公司收到通知。

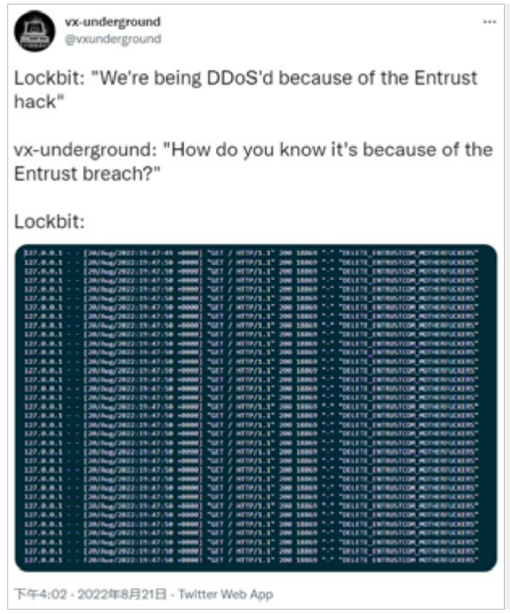
今年以来，多家银行保险机构因违规收集使用个人信息、客户信息管理不善等问题被罚，罚单金额达数百万元。据悉，其侵害个人信息权益乱象大多集中在“个人信息收集”“个人信息存储和传输”“个人信息查询”“个人信息使用”“个人信息提供”“个人信息删除”“第三方合作”七大方面。

本次专项整治工作以银行保险机构自查为主，监管部门适时开展抽查和督导。有股份行人士透露，当前公司正在围绕上述侵害个人信息权益乱象七大方面开展自查，9 月 20 日前需完成自查整改工作并呈交书面报告。

国外

1、一张乌军伤亡数据泄露，7.6 万人阵亡，4.2 万人受伤，7244 人被俘

摘要：根据外网的消息，一张疑似乌克兰武装部队总司令扎卢日尼向乌克兰安全委员会秘书阿列克谢·丹尼洛夫提供的一份报告被泄露，上面记录了乌克兰军队对内统计的损失数字，日期为 8 月 16 日，编号为 220/1085 号。按照这份文件的描述，截至 7 月 1 日，乌克兰军队已记录了己方的 76640 人阵亡，42704 人受伤、7244 人被俘、2816 人失踪、1610 非战斗减员。这份文件写道这些数字只是乌克兰正规军部队的统计，不包含国民近卫军、领土防卫军、边防局、安全局、警察部队等单位的损失。



2、LockBit 勒索软件团伙称在泄露 Entrust 数据后遭遇 DDoS 反击

摘要：LockBit 勒索软件团伙已经声称对 7 月攻击网络安全巨头 Entrust 的事件负责，但它们也指出遭到了后者的分布式拒绝服务（DDoS）回击。曾于 7 月下旬透露该公司的部分网络遭到了“未经授权者”的访问，但并未证实攻击性质或是否有数据被盗。

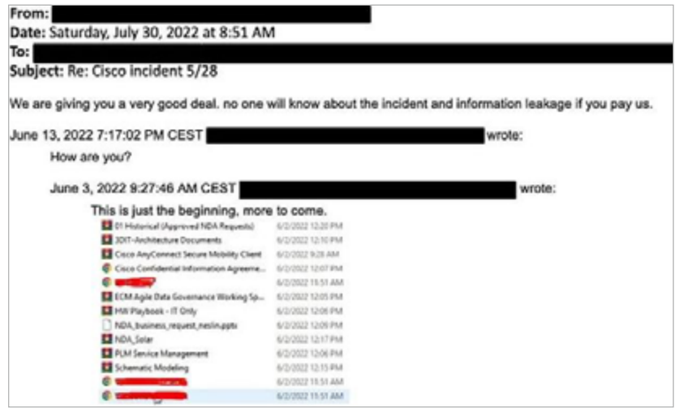
3、南非几乎所有公民征信数据泄露！

摘要：美国征信巨头 TransUnion 的南非公司遭巴西黑客团伙袭击，5400 万消费者征信数据泄露，绝大多数为南非公民，据了解南非总人口约 6060 万人。黑客团伙透露，通过暴力破解入侵了一台存有大量消费者数据的 SFTP 服务器，该服务器的密码为“Password”。TransUnion 公司称，将为受影响的消费者免费提供身份保护年度订阅服务，预计成本将超过 114 亿元。

4、印尼政府正在调查“据称的”国有电信企业数据泄露事件

摘要：印尼通信部周日表示，印尼正在调查国有电信公司 PT Telkom 所属的印尼互联网服务 IndiHome 和国有公用事业 PT Perusahaan Listrik Negara (PLN) 的个人数据泄露事件。

5、思科遭遇勒索攻击，2.8GB 数据泄露，攻击者为 16 岁少年！



摘要：近日，知名网络巨头思科官方证实，今年 5 月曾遭遇勒索攻击，攻击者是一个名为 Yanluowang 的勒索软件集团，攻击者试图以泄露被盗数据威胁索要赎金。

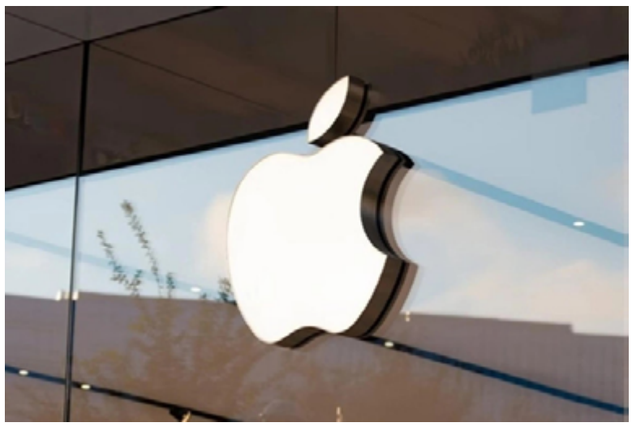
6、确认 540 万账户数据泄露，漏洞已修补

摘要：8 月 9 日消息，据 IT 之家消息，Restore Privacy 报告称，推特因安全漏洞被黑客入侵，共计 540 万个账户的联系方式泄露，泄露的 540 万个账户包括推特 ID 与其关联的电话号码和电子邮件信息，已在一个黑客论坛上出售，价格为 3 万美元。今日，推特已正式确认该攻击已发生，并且该 0-day 漏洞已被修补。

7、亚马逊 Ring 安卓 app 漏洞可窃取个人信息

摘要：亚马逊 Ring 安卓 app 漏洞可以访问摄像头记录。Ring 是亚马逊运行的家用安全环境产品，包含户内外监控摄像头。其中 Ring 安卓 APP 下载次数超过 1000 万次。Checkmarx 安全研究人员在亚马逊 Ring 安卓 APP 中发现了一个安全漏洞，攻击者利用该漏洞可以截取受害者手机中的个人数据、位置信息、和摄像头记录。

8、苹果商业机密被窃取，前工程师对数据泄露事件认罪



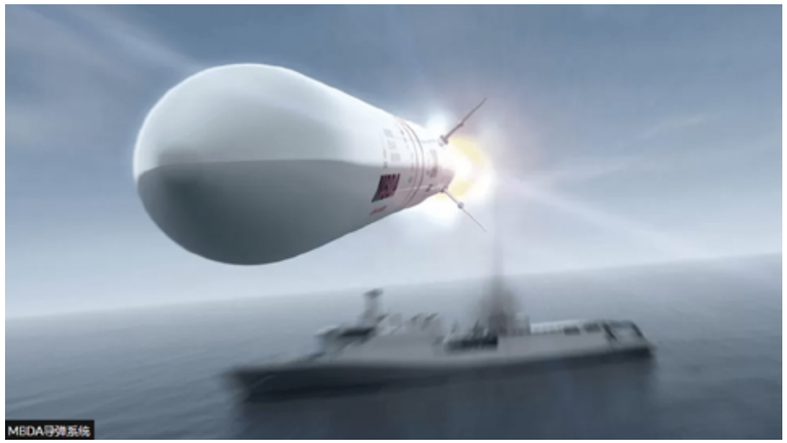
摘要：8 月 23 日消息，苹果公司前工程师张晓浪周一在加州圣何塞联邦法院就一项刑事指控认罪。此前，他被指控在跳槽小鹏汽车前窃取了苹果的自动驾驶商业机密，张晓浪在听证会上承认了一项窃取商业机密的指控。法官已下令将他的认罪协议封存，将在 11 月 14 日作出判决。这项重罪指控将导致他面临最高 10 年监禁和 25 万美元的罚款。

行业聚焦 INDUSTRY FOCUS

9、多米尼加共和国政府机构遭受勒索软件攻击

摘要：多米尼加共和国的多米尼加农业研究所（Instituto Agrario Dominicano）遭到了 Quantum 勒索软件的疯狂攻击，该勒索软件加密了整个政府机构的多项服务和工作站，导致部分工作暂时停滞。

10、北约调查黑客出售导弹公司数据



摘要：北约正在评估黑客组织在线出售的机密军事文件数据泄露的影响。MBDA Missile Systems 是世界上最大的武器制造商之一，这些数据包括北约盟国在乌克兰冲突中使用的武器蓝图。在窃取与欧洲主要武器制造商有关的数据后，犯罪黑客正在出售这些档案。MBDA Missile Systems 承认其数据在其中，但声称这些机密文件都不属于该公司。

数字经济赋能未来，亿赛通 2022 全球数字经济大会大放异彩

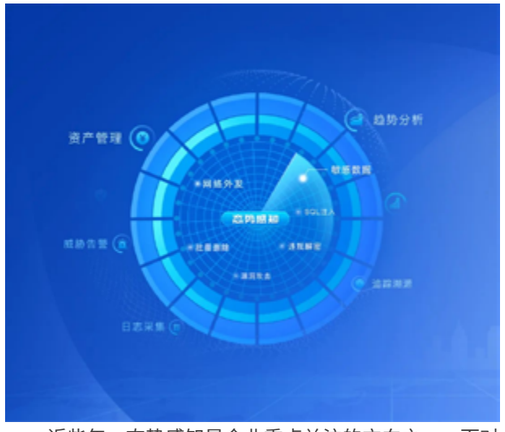
7 月 28 日 -30 日，历经三天，以“启航数字文明——新要素、新规则、新格局”为主题的 2022 全球数字经济大会在北京圆满落幕。大会由北京市人民政府、国家发展和改革委员会、工业和信息化部、商务部、国家互联网信息办公室、中国科学技术协会共同主办，设有六大主题峰会及五十余场专题论坛，亿赛通受主办方定向邀请全方位亮相主论坛与数字经济精品主题展，同世界各国嘉宾、国际机构代表以及知名经济专家学者、全球顶尖企业代表一道，共谋数字经济新发展格局。

科技创新 成果发布

7 月 30 日，大会以成果发布会作为本次的收官活动，总结回顾了大会的成果与亮点，集中展示全球数字经济标杆城市建设进展成效，发布一批重磅研究成果，推出首创首发企业新品，对大会赛事活动予以表彰。在新品发布环节，“全球数字经济大会创新引领成果、产业创新成果”名单正式公布， 亿赛通数据安全态势感知平台经过专家组多轮调研评定， 最终顺利入选 2022 全球数字经济大会新产品成果发布名单。

态势感知 智能防护

亿赛通数据安全态势感知平台采用先进的大数据技术架构，通过采集分析来自于终端、网络、存储、结构化和非结构化的各类安全设备日志，通过人工智能算法，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。同时能将各个孤立的安全系统进行资源整合，达到系统集中管控、数据关联分析，以揭示海量事件背后隐藏的逻辑关系从而全面监控数据安全状况，指导企业安全管理，有效预防、阻断或减少安全威胁事件的发生。



近些年，态势感知是企业重点关注的方向之一，而对亿赛通的数据安全态势感知平台来说，它不仅仅是一套用工具，而是从决策层到技术层，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。为用户达到：

1、事态可评估

亿赛通数据安全态势感知平台自身能够对采集的日志进行增量分析，对新收集来的数据进行更新比对。并将采集的日志数据通过线图的方式呈现给用户，实现了数据的可视化。除此之外，还能将信息多维度关联，以综合评估数据安全事件。

2、趋势可预测

平台对违规事件趋势、攻击事件趋势、漏洞分布趋势、异常流量趋势进行统计分析，掌握事件的出现规律，并结合安全产品对下次违规事件、安全漏洞、异常攻击进行预测判断出发生的时间、地点、风险级别。

3、风险可感应

平台通过对众多数据安全产品的日志进行多维分析，建立风险响应基线及应对策略，以此基线对后续的风险进行风险建模分析，当偏离此基线时，平台可确认此操作或行为会导致新的更高级别风险，形成对已知、未知风险的感应，并能够快速启动响应策略。

4、知行可管控

通过对数据资产的测绘，将资产、漏洞、攻击、风险等多种数据进行关联分析和计算，通过直观可视化的方式为用户进行呈现，让用户知道自己有哪些资产，哪些资产存在漏洞，哪些资产被攻击，哪些资产存在风险，帮助用户快速定位数据安全风险，精准进行数据安全防护。

为了更好监控和保障数据安全系统运行，及时识别和防范数据安全风险，同时满足国家和行业监管要求，保证数据安全管理工作依法合规，为企业安全管理决策者提供可靠数据支撑，为全行业企业用户做到事前预警、事中监控、事后溯源分析，全面提升数据安全管理与防护水平。

在我国信息化、网络化、数字化发展进程中，数字经济科技创造新力量。作为国产数据安全领域领军企业，亿赛通将乘数字化变革东风，致力核心关键技术创新，为千行百业提供数据安全业务新模式，继续紧跟数字中国的步伐，助力网络强国的目标早日实现。

亿赛通布局渠道与生态合作，凝心聚力书写合作新篇章

2022 年随着数字经济的发展，数字化转型新趋势以及高新技术的广泛应用，数据安全已经上升为国家战略之一，在国家及行业一系列法律法规、政策及标准的驱动下，各行各业对网络安全的重视程度逐年提升。数据安全产业面临着众多新形势、新挑战、新机遇，面对巨大的市场，唯有拥抱合作伙伴，才能紧跟市场变化，为客户创造更多的价值。

2022 年 8 月 9 日，亿赛通在北京总部召开“携手聚亿 创新通赢 2022 合作伙伴沙龙”，围绕数据安全市场机遇，行业政策解读及伙伴政策进行讲解探讨。亿赛通近几年重塑合作体系和管理机制、加大资源投入与赋能，推进渠道与生态体系转型落地，积极布局数据安全市场，显著提升了产品覆盖度和影响力。

北京亿赛通科技发展有限责任公司副总经理张磊在合作伙伴大会上说道，我司生态、渠道合作体系的打造上，严守公平、公正的市场秩序，为合作伙伴构建阳光、透明的商业环境。目前亿赛通已经构建了完善的服务体系，为支撑渠道战略在行业和区域的落地执行，从公司组织架构上深入调整，横纵结合，上下拉通。在任何行业，面对任何客户，合作伙伴们都可以跟亿赛通合作，我们会坚守原则，更主动开放，商机共享，让合作共赢。

亿赛通渠道与生态部负责人表示生态、渠道建设能否成功落地，取决于厂商是否有足够的意愿长期持续投入，为合作伙伴提供市场拓展、技术服务、人力资源等全方位的支持，并对合作伙伴的售前、售后乃至管理人员进行持续培训。亿赛通会利用自身的优势和经验，帮助合作伙伴建设自身能力，培养更加优秀的合作人才。

亿赛体数据安全专家表明，我公司生态、渠道体系和产品体系是紧密相连、相互协同的。此前独家推出的“分·放·管·服”数据安全建设理念，可以融合公司全系列产品，包括数据泄露防护、电子文档安全、态势感知、安全服务等产品服务联动联防，帮助用户进行全生命周期防护体系建设。且产品集被动审计和主动防御于一体，识别数据内容的合法性， 能有效满足客户对敏感数据防泄露的痛点需求。

亿赛通数据安全产品，为用户建设先进、自主、灵活、全面、智能的立体化数据安全防护体系；建设满足合规要求的商密数据保护管理体系；为用户提供完整的数据资产生命周期风险主动控制和自动化管理；可有效降低泄密风险，提升防护能力，提升监管能力的技术体系。

面向各行各业不同的安全需求，亿赛通推出十大行业解决方案。已涵盖市面中的主要行业，针对不同的行业做出产品、方案的适配和优化，向合作伙伴抛出橄榄枝，吸引大家一起投入、拓展市场。

亿赛通把生态、渠道合作战略作为公司的主要战略之一，坚持长期、稳定的合作模式不动摇，以开放、合作、共赢的生态观念，实现客户、合作伙伴和亿赛通的三方共赢。

数据安全产业人才培养沙龙在京召开，助推专业人才培养体系建设

2022 年 8 月 5 日，在工业和信息化部网络安全管理局指导下，由中国电子信息产业发展研究院、工业和信息化部教育与考试中心、中国信息通信研究院共同主办，北京亿赛通科技发展有限责任公司、中国计算机行业协会数据安全专业委员会、路云天网络安全研究院联合承办的“数据安全人才培养”主题沙龙在京成功举办。主题沙龙采取线上线下相结合的方式，线下参会嘉宾 40 余位，线上参会嘉宾 150 余位（具体参会名单附后）。

中国电子信息产业发展研究院党委书记、副院长刘文强、工业和信息化部教育与考试中心副主任刘明亮、中国电子信息产业发展研究院副总工程师安晖、工业和信息化部网络安全管理局杨帅锋、中国电子信息产业发展研究院网络安全研究所副所长、中国软件评测中心主任助理唐刚、北京亿赛通科技发展有限责任公司总经理崔培升、华为技术有限公司中国产业发展与生态部首席数据安全专家刘鑫，北京市京都律师事务所竞争法事务

部主管合伙人王菲等领导出席沙龙并作主旨演讲。

习近平总书记在中央人才工作会议上强调须深入实施新时代人才强国战略，加快建设世界重要人才中心和创新高地；而数据安全关乎国家安全，数据安全人才培育是数据安全产业健康发展的必备前提，是国民经济稳定有序发展的重要环节。为此，本期沙龙聚焦“数据安全产业人才培养”主题，围绕国内数据安全人才培养现状、问题挑战、实践应用等重点议题，研讨数据安全产业人才培养体系建设思路，切实推动数据安全产业高质量发展。

数字经济高质量发展需要数据安全人才

沙龙开场，亿赛通总经理崔培升致欢迎词，他表示目前全球的竞争局势发生巨变，国内数字经济蓬勃发展，企业数字化转型提速，同时，各项法律法规的发布，预示着数据安全成为数字经济发展最重要的基础要素，数据安全发展的高度将决定数字经济的高度。而数据安全的发展又离不开人才的培养，若想满足产业链上下游需求，需要从理念、政策、标准、制度、产品、技术、师资、课程、人才分级等内容不断优化完善。亿赛通在近二十年间，不断为行业输送人才，有责任输出人才培养相关心得、经验，为产业发展贡献力量。

党中央高度重视人才培养工作

随后，中国电子信息产业发展研究院党委书记、副院长刘文强发表致辞，从去年 10 月开始共同合力打造便捷高效的产业合作平台、活动，聚焦数据安全产业标准，凝聚产业各方智慧，围绕人才培养议题，开展深度交流研讨，加快布局步伐。数据安全人才培养是数据安全产业健康发展的前提条件，中央对人才培养工作高度重视，强调深入实施新时代人才强国战略，加快建设世界重要人才中心创新高地。望通过沙龙共同探索人才培养更优路径，学习先进经验，有效推动数据安全产业的人才培养工作，聚集多番力量，携手同心，输送人才。

工信领域数据安全人才培养渠道成熟畅通

工业和信息化部教育与考试中心副主任刘明亮指出，数字经济时代，数据安全关乎国家安全。教育考试中心高度重视数据安全产业人才培养工作，愿意举中心之力做好服务。教育考试中心的核心职责是工业和信息化人才培养与评价，年培养选拔工业和信息化领域技术技能人才 300 余万人次，具体承担国家职业资格考试、工业和信息化人才培养工程、工业和信息化职业技能提升工程、工业和信息化线上培养工程、技术技能大赛等工作。下一步，教育考试中心将从以上五个方面切入，强化岗位课程体系研发，遴选推广优质课程，加强线上培训，提供大赛支持，推动数据安全领域纳入国家职业资格考试。教育考试中心愿充分发挥自身优势，助力数据安全产业人才培养。

数据安全行业人才缺口巨大 注重培养综合型人才

北京亿赛通科技发展有限责任公司高级总监孙超表示，从全球视角来看，自 2009 年起数据学科相关学位逐年增加，欧美多所高校已将数据安全相关内容设置为必修课程。而在国内数据安全技术人才则多为社会人员主动进修或转行，数据安全人才培养资源仍然稀缺，相关人才缺口高达百万，这将直接影响数字中国建设，制约数据赋能和数据的安全保护、有序流动和开放共享。因此，要让数据安全人才培训成为一种常态，加快壮大数据安全产业力量，加速组建未来网络安全、数据安全的主力军。当然，数据安全人才的重点，不仅仅是安全技术，也要具备安全意识，掌握政策要求及数据业务场景，综合型人才是数据安全的最终目标。

数据安全知识结构复杂 人才培养需多维度支撑

华为中国产业发展与生态部首席数据安全专家刘鑫对数据安全人才的应用实践进行讲解，他首先指出本世纪最大的财富是人才存储，同时，数据安全人才培养正面临多重挑战：数据要素面临安全环境复杂，超越技术范畴；数据安全技术涉及范围广泛，知识结构复杂；数据安全相关政策频出，合规要求提升。数据安全工作正在全面部署开展，需要大量人才来落实和支撑，数据安全人才培养意义重大。人才的培养需要综合防护、内生安全、安全合规等能力。最终需要职业认证教育与学历教育、职业培训结合，实现人才培养知识体系闭环，制定统一的数据安全“基础体系”教材，同步规划、同步培养、同步使用。

数据安全合规需求旺盛 设立合规师岗位势在必行

北京市京都律师事务所高级合伙人王菲在演讲中提到数据安全合规师岗位。合规师是近几年数据行业经过技术迭代、政策法规的完善及商业新模式下应运而生的技术人才岗之一。该岗位技术人才需要科学系统的方法论及必要完整的知识结构，不仅要了解数据相关法律法规，更要精通数据处理与安全、个人信息保护、数据应用与保护、域外数据法律制度以及重点行业相关的各项数据安全问题。培养出专业的数据安全合规师，能有效推进产业繁荣，企业规范作业，规避数据泄露风险。

工作载体已有效运转 牵头引领培育数据安全人才

中国电子信息产业发展研究院网络安全研究所副所长、中国软件评测中心主任助理唐刚表示，在工业和信息化部网络安全管理局的指导下，组织成立了人才培养工作的载体——数据安全专业委员会人才培养工作组，致力于紧密围绕数据安全产业发展战略，建立完备的培训体系，培养高质量的数据安全产业人才，为数据安全产业人才招聘、评价提供有效参考，推动数据安全产业高质量发展。未来，将进一步提高各地区、各行业领域以及各单位对于数据安全产业工作的重视，加深对数据安全技术和产业发展的了解，推动数据安全产业系列活动开展，构建安全人才的职业发展通路，全面提升数据安全人才专业技术能力。

沙龙讨论环节，与会嘉宾就数据安全人才的需求、面临的挑战、如何推进相关工作、如何完善课程质量等问题展开了深入探讨。

数据安全人才培养需要打通产学研一体化

国家市场监督管理总局信息中心网络安全处处长、中国计算机行业协会数据安全专业委员会委员陈鑫认为，数据本身具有流动性、可复制性和由此带来的权责上的模糊性，这些都给数据治理带来很大的挑战。数据安全产业人才培养需要标准化，建立人才培训体系，并与认证认可体系结合起来，打通产学研一体化。从产业来看，数据安全人才培养不能局限于某一方向，需要包括研发、服务、咨询、测评等各方面的人才；同时，在需求侧的数据安全管理人员缺口同样很大，业内亟需既懂数据又懂安全的人才。数据安全保护工作当前的重点是满足合规要求，首要问题是需要发现问题、定位问题。未来，推进数据安全融合将成为生产力的一部分，更好地支撑数据利用、业务发展是业内努力发展的方向。

医疗行业数据安全综合性服务需求旺盛 亟需制度和人才输入

北京市医院管理中心三级调研员杨建朝谈到，2021年国家发布《关于推动公立医院高质量发展的意见》，对公立医院提出高质量发展的要求。公立医院高质量发展最基础的一个要素便是数据，如互联网诊疗、远程会诊，这些都需要医疗机构在数据安全方面进行支撑。疫情以来，医疗机构数据安全风险压力不断增大：一是互联网诊疗、远程会诊等互联网上的系统暴露的问题较多；二是医疗体系中专业的数据安全的人才缺乏；三是医疗数据安全相关的政策、制度框架尚需健全完善。如何更好的开展数据安全相关建设，需要三个条件：首先需要有编制，能够落实数据安全人才岗位；其次，要有规范指南，有专业的数据安全人才、证书资质要求；第三，有专业的机构进行人才培训。

数据安全产业亟需专业人才 联合搭建平台共同培养

工业和信息化部教育与考试中心信息化处副处长穆步洲谈到，工业和信息化部教育与考试中心一直致力于工业和信息化领域各行业发展提供人才支撑服务，培养选拔工业和信息化领域技术技能人才。当前数据安全产业发展亟需大量的数据安全专业人才，前期由教育考试中心和中国计算机行业协会数据安全专业委员会基于网上学习平台线上培养工程共同推出了数据安全工程师、数据安全评估师两个岗位，相关课程在社会上的反响很好，报名需求很多。未来，教育考试中心将不断健全完善数据安全人才培养标准体系、培养框架，与大家一同搭建产业平台，并竭诚为大家提供服务。

分类型、分阶段、分需求进行数据安全人才培养

最后，部分安全企业代表发表了自己企业对数据安全人才培养的看法。天融信科技集团助理总裁李建彬认为，数据安全产业人才培训需要更加细化、矩阵化的形式培训，一是面向学生，提供全面覆盖数据安全基础知识和安全意识培训。二是面向实践应用，开展场景化的数据安全治理培训。三是面向企业自身业务需求，为企业培养数据安全人才，包括数据安全管理人员和技术人员，主要涉及合规评估、应急处置与响应、部门协调等。数据安全工作覆盖整个业务、整个单位，数据安全人才需要具备系统能力。

路云天网络空间研究院副院长孔勇认为，数据安全人才培养要分阶段、分对象的推进，一些业务与数据强相关的企业已设置了数据安全官及数据安全管理和技术岗位，应加强对这些重点企业的跟踪调研。希望能够在产业内加强数据安全人

才培养，通过在有数据安全需求和重点数据安全保障的单位建立试点，试点先行，推进数据安全人才培养工作的落地。

作为一家数据安全综合服务商，亿赛通多年来为行业培养、输送了大量专业人才。当前，新一轮科技革命和产业变革加速演进，数据安全成为数字产业快速发展的基石，数据安全人才也成为制约产业发展的关键要素。公司以本次沙龙为契机，与各位嘉宾思想聚焦、观点碰撞，希望通过理论课程与企业实践相结合，培养学员对数据合规要求的管理能力以及数据要素开放的应用能力，助力政府、企业与社会的数据安全技术体系建设，赋能数字治理创新发展，共同为培养和壮大综合性数据安全人才队伍贡献力量。

附：参会名单

沙龙现场出席单位

工业和信息化部网络安全管理局

中国电子信息产业发展研究院

工业和信息化部教育与考试中心

中国信息通信研究院

北京亿赛通科技发展有限责任公司

路云天网络安全研究院

华为技术有限公司

北京市京都律师事务所

国家市场监督管理总局信息中心

国家知识产权局专利局自动化部

北京市医院管理中心

北京大学

中国移动通信集团有限公司

中国联合网络通信集团有限公司

中国电信集团有限公司

深信服科技股份有限公司

奇安信科技集团股份有限公司

启明星辰信息技术集团股份有限公司

天融信科技集团

航天科工三院 304 所

中国国际技术智力合作公司培训中心

中电长城网际安全技术研究院（北京）有限公司

北京爱思考科技有限公司

北京卫达云计算科技有限公司

北京永信至诚科技股份有限公司

北京网络职业学院

北京江民新科技术有限公司

北京网测科技有限公司

北京驭安科技有限公司

沙龙线上出席单位

农业农村部信息中心

国家知识产权局专利局电学发明审查部

中国证券监督管理委员会北京监管局

北京市通信管理局

天津市通信管理局

浙江省通信管理局

亿赛通动态 ESAFENET NEWS

福建省通信管理局
河北省通信管理局
湖北省通信管理局
贵州省通信管理局
重庆市经济和信息化委员会
农业农村部农产品质量监督检验测试中心（北京）
外交部机关及驻外机构服务中心
中国司法大数据研究院
中国汽车技术研究中心有限公司
中国电子科技集团有限公司
中铁建设集团有限公司
中国船舶工业贸易有限公司
国能信控互联技术有限公司
中国移动 DICT 综合性实训基地
中国电信股份有限公司天津分公司
北京百度网讯科技有限公司
北京金联融科技有限公司
北京安盟信息技术股份有限公司
北京时代新威信息技术有限公司
北京昆仑联通科技发展股份有限公司
北京亚鸿世纪科技发展有限公司
北京西普阳光科技股份有限公司
北京祥云信安科技有限公司
北京国舜科技有限公司
北京欣正网信科技有限公司
北京盈诚科技有限公司
北京清大华普科技公司
北京华隆辰信息技术有限公司
北京中光文生科技有限公司
北信源软件股份有限公司
神策网络科技 (北京) 有限公司
上海观安信息技术股份有限公司
上海数禾信息科技有限公司
上海优咔网络科技有限公司
浙江新超网络科技有限公司
浙江御安信息技术有限公司
浙江省发展信息安全测评技术有限公司
吉利汽车集团
杭州美创科技有限公司
杭州中尔网络科技有限公司
杭州飞侠网络科技有限公司
杭州安存网络科技有限公司
义乌市华晨网络科技有限公司
常州精研科技股份有限公司
紫光云技术有限公司
宜科 (天津) 电子有限公司
天津荣联汇智智能科技有限公司
天津朗言安全技术服务有限公司
富士康工业互联网股份有限公司
深信服科技股份有限公司
深圳昂楷科技有限公司
深圳市能信安科技股份有限公司
成都安美勤信息技术股份有限公司
长春吉大正元信息技术股份有限公司
长春嘉诚信息技术股份有限公司
大唐东北电力试验研究院有限公司
中原工学院
河南听潮盛世信息技术有限公司
河北千诚电子科技有限公司
陕西正通云计算有限公司
长飞光纤光缆股份有限公司
信通院（武汉）科技创新中心有限公司
山东正中信息技术股份有限公司
山东维平信息安全测评技术有限公司
烟台中科网络技术研究所
广东安创信息科技开发有限公司
福建福诺移动通信技术有限公司
福建海峡信息通信科技发展有限公司
福州优网信息技术有限公司
青创未来集团有限公司
宁夏西云数据科技有限公司
联通云数据有限公司贵州省分公司
贵安新区产业发展控股集团有限公司
贵州奇临一零一科技有限公司
贵州易数科技有限公司
贵州元极科技有限公司
贵州耕云科技有限公司
德勤会计师事务所
Netscout

亿赛通智能安全系列产品亮相智博会，助力数字经济高质量发展

8 月 22 日，2022 中国国际智能产业博览会（简称“智博会 ") 正式开幕。作为智博会重要参展商之一，亿赛通携数据安全建设理念、产品族、技术解决方案等核心优势和前沿技术成果亮相线上展厅，集中展示如何为数字经济建设保驾护航。

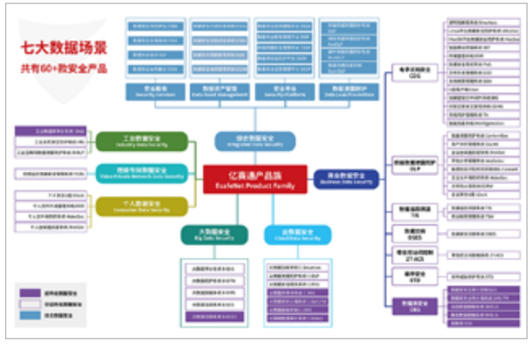
本届智博会线上展示分为六大区域，亿赛通展位位于科技创新展区，运用文字、图片等元素全方位、全景式展

亿赛通展台分为 3 大展示区域，分别为展厅主屏、品牌展示区和解决方案展示区，立体化展示了我公司品牌文化、主营业务、资质荣誉和解决方案，方便线上嘉宾全面深入了解我司在数据安全领域的傲人成绩。

作为中国首批数据安全服务商之一，亿赛通的业务触角已延伸到数据库安全领域、零信任、区块链技术和培训领域，其首创的“分·放·管·服”数据安全建设理念已帮助众多行业客户实现数字化转型升级。

亿赛通认为市场上厂商大都通过提供单一或某几个产品解决客户在某个方面的问题和需求，这样既影响到数据安全体系建设落地，又会增加人力、物力等多方面的成本投入。在“分放管服”理念的指导下，我司通过数据安全产品，基于数据全生命周期各阶段具体情况，梳理数据资产、确定安全风险。

全线产品细分为数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务六大项。对云、网、端等多场景实现数据资产管控、追踪溯源分析、安全态势感知等手段。大力开展数据安全治理、数据资产分级分类、数据安全风险评估、数据应用安全等领域相关工作，建立数据管理长效机制，夯实数据基础工作，支撑数据模型的运行。后续完善重点领域管理能力，管理体系完善建设，加强优化组织、制度、技术、人员闭环管理，推进数据管理各领域工作全面开展和数据安全管理能力全面提升，全面提升企业的数据安全建设成熟度。



随着数据安全态势的革新，全面体系化的专业服务与解决方案，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，咨询、治理、运维的要求越来越高。亿赛通运用近二十年的经验，通过理念 + 工具的开发、安全体系的建设，帮助客户得到智能化的安全服务体验，与企业实现安全能力共建，为企业安全赋能，实现智能防护。

小亿在此诚邀社会观众进入智博会官网线上观展。

（智博会链接详见文末阅读全文）

https://www.smartchina-expo.cn/zbh/index.html

关键基础设施勒索激增，亿赛通助企业守好最后一道防护大门

近日，勒索病毒再次来袭，本次瞄准关键基础设施企业，给国内外很多企业机构带来重大损失。下面我们就近期几起重要的勒索病毒攻击事件进行分析汇总。

1、一医院遭到勒索软件攻击

Centre Hospitalier Sud Francilien（CHSF）是一家设有 1000 张床位的医院，由于遭到了勒索攻击，导致这家医疗中心只好将患者转移至其他医疗机构，并推迟手术预约。CHSF 发布公告：“针对计算机网络的这起攻击导致本医院的业务软件、存储系统（尤其是医学影像）以及与患者入院有关的信息系统都暂时无法访问。”

这家医院的行政管理部门尚未透露有关情况的进一步信息，而导致医院运营受阻的 IT 系统中断仍在困扰着这家医疗机构。需要紧急护理的病人将由 CHSF 的医生进行评估；如果病情需要做医学影像以便治疗，他们将被转移到另一个医疗中心。

法国媒体从执法部门获得信息，攻击 CHSF 的勒索软件团伙索要 1000 万美元（约 6860 万元人民币）的赎金，才肯提供解密密钥。警方知情人士告诉媒体：“巴黎检察官办公室的反网络犯罪部门已对有组织的团伙闯入计算机系统，并企图勒索的非法活动展开了调查。”他还指出“具体已委托反数字犯罪中心（C3N）的警察展开调查。”

2、希腊天然气运营商遭到勒索软件攻击

希腊最大的天然气分销商 DESFA 已证实，它遭到了网络攻击，导致部分数据泄露，IT 系统中断。DESFA 公开声明：黑客企图渗入其网络，但幸好其 IT 团队迅速反应，黑客的阴谋诡计最终未能得逞。然而，一些文件和数据还是被黑客访问了，可能已“泄露”，因此网络确实遭到了入侵，即使范围有限。

DESFA 已关停了许多在线服务以保护客户数据。他们向消费者保证，该事件不会影响天然气供应，所有输入点和输出点均以正常容量运转。目前，DESFA 已通知希腊警方网络犯罪部门、国家数据保护办公室、国防部以及能源环境部，帮助当局在最短的时间解决问题，确保影响最小。并宣称自己绝不与网络犯罪分子联系，因此不会就赎金支付进行谈判。

3、英国水务公司遭遇 Clop 勒索软件攻击

英国一家水务公司因网络攻击而导致其企业 IT 系统出现中断，但声称其供水业务并没有受到影响。同时，所谓的攻击者 --Clop 勒索软件集团声称攻击的对象是另一家更大的水务公司，而该公司则对外声称并没有被攻击。

南斯塔福德郡 PLC 公司是南斯塔福德水务公司和剑桥水务公司的母公司，它在声明中表示它是此次网络攻击的受害者，但并不影响它向所有客户 " 供应安全用水的能力 "，由于一直都有强大的系统对水供应和质量进行控制，团队也迅速应对了这一事件并在预防基础上采取了额外措施，所以供水业务并没有中断。

面对屡屡爆发的勒索攻击，亿赛通联合太平洋保险共同推出“防勒索网络安全保险”。市面上传统的保单中并未明确网络安全风险是否覆盖，即使有些企业具备了一定的网络安全保险意识，但由于缺失明确的预算项目和网络安全经验，保险项目实际操作起来也很难推进。

针对以上挑战，亿赛通防勒索网络安全险给出了解决方案：

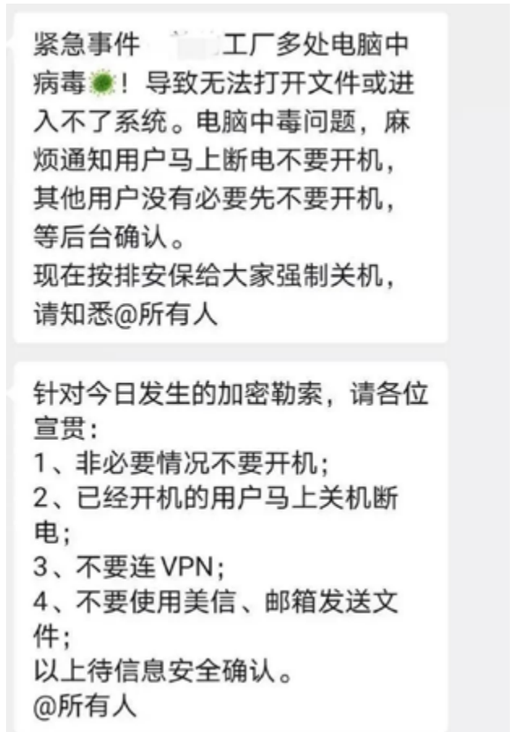
首先聚焦于网络安全中的数据保护，以企业数据资产的保护为切入点，帮助企业避免或挽回损失，推广和提升网络安全保险意识。

保单的保障责任包括，第一方财务损失（如勒索损失），第三方责任赔偿（如信息泄露责任），以及扩展责任（如名誉修复）。保障对象则包括，存储信息、网络收入等。

这份安全保单不仅仅是一份保障合同，更是一项服务承诺，覆盖“保前安全测评、保中安全监控和保后应急响应”三个环节。亿赛通提供自身专业的安全服务和安全工具，在保障用户的数据资产安全的同时，降低出险概率。真正实现数据价值明确、责任认定清晰、鉴定过程简单和“定点防护”，即采用设备与文件防火墙绑定，降低攻击面，为企业守好最后一道勒索软件防护大门。

亿赛通小贴士 ESAFENET PROMPT

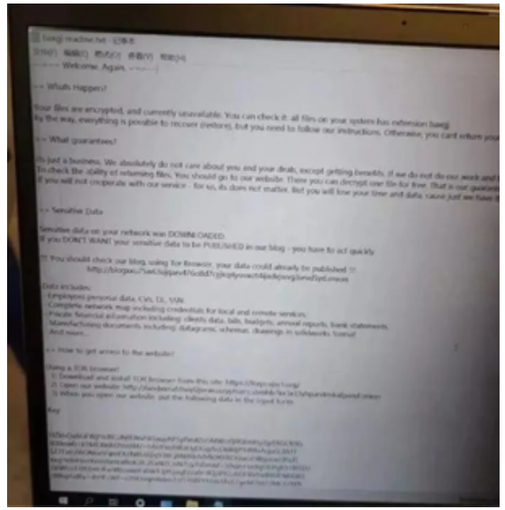
勒索病毒屡次进犯，亿赛通防勒索网络安全险从源头阻断黑手



勒索病毒对于企业来说是极力希望避免的攻击，每次出现都会以全新的面貌示人，让企业两眼一摸黑。目前市面上的勒索病毒主要以邮件、网页挂马、WEB 漏洞、移动介质等形式进行传播，不管是哪种形式的勒索病毒，都具有极其恶劣的性质和极大的危害，一旦感染将给用户带来无法估量的损失。

近日，有网友爆料称国内知名家电企业美的内网遭遇勒索病毒，导致系统无法登录，黑客要求 7 日内汇 1000 万美金到指定账户，另称其是在美的集体年假时趁虚而入。随后，互联网中流传出疑似内部安全部门处理信息的相关消息及疑似中毒的电脑截屏。一时之间，乌云密布，IT 业界激起千层浪。

随后，美的已就此次事件做出回应：仅少数员工电脑受到感染，公司各业务系统未受影响，经营正常进行，也没有收到勒索信息。



请转发以下消息给各自部门所有人：对于811勒索病毒攻击事件，信息安全部正在行动中，因为涉及集团全员，这个病毒是业界见之病毒，而且这个病毒还针对[redacted]刻意做了免杀，处理方案设计多个方面，请大家耐心等待。在此期间，在公司内网办公的员工，如果想要用PC台式机，请拔掉网线，等待通知；如果想用笔记本电脑，请一定断开公司WiFi网络。对于在家的员工，可以通过VPN照常办公。

虽然此次美的已经辟谣，但勒索病毒无孔不入，一不小心就能中招。面对屡屡爆发的勒索攻击，我想大众心中都有一个疑问，勒索病毒真的无解吗？自勒索病毒爆发起，亿赛通一直未放松警惕，致力于对勒索病毒进行研究和防护，推出产品 + 服务体系，有效规避突发性勒索病毒损失，做到事前主动防御，弥补传统安全产品防护的不足。

亿赛通基于对勒索病毒特性及网络安全建设现状等方面分析，最终以企业数据资产的保护为切入点，联合中国太平洋保险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整体解决方案，达到“保前安全检测、保中安全监控、保后应急响应”，大幅度降低了客户安全风险。

我们通过自身专业的安全服务和安全工具，与中国太平洋保险达成战略合作，形成“ 防勒索 + 保险”的整体解决方案， 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。

1、保前安全监测：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；

2、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；

3、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；

未来，数字化触及的领域会不断深入，安全防护的难度也会不断加大。面对全球经济发展不稳定因素急剧增加的发展环境，企业更需要准确把握企业安全防护的发展方向，趋利避害，发挥好新技术、新产品的优势，以规避数字化过程中带来的风险与挑战，亿赛通会持续助力企业数据安全，助推各行业客户长远发展。

数安智库｜数据安全治理体系建设的思路与方法

近年来，《网络安全法》《数据安全法》《个人信息保护法》等法律接连发布，“等保 2.0”、《个人信息安全规范》、《数据安全治理能力评估方法》等标准持续落地，数据安全作为“总体国家安全观”的重要组成部分，成为国家合规监管的重点。同时，数据安全作为数据要素价值化的前提和基础，是各行业健康平稳发展的刚需。Risk Based Security（RBS）《Data Breach Report: 2021 Year End》数据显示，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。在合规建设、业务发展、风险控制等多重需求的推动下，数据安全已经成为关系国家、企业生存发展的重中之重。

随着云计算、5G、物联网、人工智能等创新技术的发展，数据向云、网、端等应用场景不断延伸，数据跨网络边界、业务部门的流转成为常态，单点的安全防护手段缺乏协调联动能力，安全策略全面性弱、一致性差、管控效率低，难以发挥贯穿数据处理全流程的整体防护能力。在国家《“十四五”数字经济发展规划》的不断推进下，为实现大规模的数据共享和业务协同，数据安全必须与业务进行体系化融合，实现全场景、全流程、全链路的安全保障，通过统一的管控平台，推进产品、技术和管理的协同治理，形成数据安全综合治理体系。

数据安全治理体系建设思路与方法

数据安全治理是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，以“数据安全管理和技术能力”为依托，实现业务与安全融合发展的安全建设机制。整个体系以“身份”和“数据”为中心，从决策层到技术层，从管理制度到技术支撑，通过构建自上而下、全流程、可闭环的完整链条，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。数据安全治理工作通常围绕以下四个方面进行能力建设：

1. 构建数据安全统一规划和统筹管理的能力

依据数据安全相关法律法规、标准规范等国家和行业合规要求，结合用户企业的数据安全现状，规划、建设包含数据安全指导方针、数据安全组织体系、数据安全制度体系、数据安全策略体系、数据安全运营体系、数据安全能力体系的数据安全治理总体框架。具体工作可综合考量安全基础、安全预算等因素分阶段进行：

第一阶段包含安全战略方针、组织架构建设、制度流程设计、安全能力规划、建设实施路线等工作，建立切合自身安全需求和发展需要的数据安全管理和制度体系；

第二阶段包含合规基线建立、全量数据梳理、敏感资产盘点、分类分级策略制定和实施、数据风险评估等，进行数据安全方针和策略的落地；

第三阶段包含量化评价指标的建立，并结合评价结果及时完善前期的治理工作，使得数据安全管理制度高效融入业务卡点，保障部署的安全策略持续有效运行。

与此同时，通过定向的培训课程，培养全体人员的安全意识，并以提升安全团队成员的专业能力为重点，进一步赋能数据安全治理体系的高效实施。

2. 构建数据资产可量化、可归类、可评估、可追溯的能力

数据相比土地、资本等传统生产要素，具有规模难量化、类别级别难确定、风险难评估、流向难追溯等特点。解决这些难点，对于后续的数据安全治理工作至关重要。可以通过：

• 调研和工具的方式，详细梳理数据资产脉络，形成数据资产总量和分布视图，实现数据资产的可量化；

• 根据现有分类分级标准要求和行业实践经验沉淀，结合数据的动态和多维度特性，采用“点”“面”结合的分类法，通过预制分类分级规则和平台自动识别，形成分类分级清单，并通过动态校验，持续完善分类分级规则，提升结果的准确度，实现数据资产类别、级别的可确定；

• 针对数据收集、存储、使用、公开等境内处理活动以及数据出境风险，围绕数据本身，运用人员访谈、配置检查、旁路验证等手段，从合规对标情况、管理脆弱性、CIA 威胁识别、已有安全措施等多个角度综合考量，形成数据安全风险评估报告，实现数据安全风险的可评估；

• 通过网络嗅探、细粒度授权管控、用户行为分析等技术，结合数据防泄漏、运维审计、数据脱敏等产品能力，梳理数据从采集、传输、共享到销毁的流向，形成数据流转视图，实现数据资产的可追溯；

3. 构建全场景的数据安全防护能力

数据在与业务融合的过程中，不再局限于文件和数据库的静态使用，而是随着业务发展的需要打破存储空间、系统、应用、网络的边界，走向泛化。在“以边界为核心”的安全框架基础上，建立“以数字身份和数据资产”为核心的新型防护体系，从静态的数据存储和访问安全保障，转向跨系统、跨平台甚至跨行业、跨地域的全场景数据流通保护。具体做法包括：

• 通过驱动级智能加密、数据防泄漏、数据脱敏、数字水印、安全网关、数据库审计等技术和产品的融合，实现数据在生产、测试、应用、运维等场景下的安全保障；

• 以数据资产为中心，利用隐私计算技术，实现数据“拥有权”和“使用权”的分离，确保“数据可用不可见”，实现数据在开放共享过程中的安全使用和流通需求；

• 以数字身份为中心，搭建零信任访问控制系统，通过统一身份、动态鉴权、持续评估，实现跨网融合场景下访问行为的细粒度管控等。

4. 构建一体化的数据安全运营管控能力

传统的数据安全以单点建设为主，围绕数据处理活动，进行分段式保护，在数据流通连续性需求空前高涨的背景下，一旦存在某个薄弱环节，容易导致整体保障工作功亏一篑。通过搭建运营管控平台，集成覆盖数据识别、防护、监测、响应、恢复（IPDRR）各阶段的安全能力模块，向上为组织制度统一贯彻提供能力支撑，向下作为统一调度中心，联动各项安全能力，实现子系统数据的统一汇聚和统筹管理。具体做法包括：

• 以敏感数据为中心，基于分类分级结果，监控全平台数据的流动轨迹，分析业务流向与数据安全的关联关系，绘制数据流转路径，为风险感知和泄露溯源提供信息支撑；

• 以数字身份为中心，基于海量数据挖掘和日志分析结果，构建数字身份画像，并通过标签化管理，形成用户行为基线，为异常行为预判提供理论依据；

• 基于构建的数据流转路径和用户行为基线，通过 SOA 配置编写剧本固化分析场景、处置场景及处置手段，实现智能告警和安全事件自动编排等。

总结

数据安全治理是随着业务数据化和数据资产化，为适应数据安全保障需求而不断更新的产物，其最终落脚点在于“兼顾发展与安全”，实现数据资产在安全保障下的自由流通。基于数据安全治理体系建设框架，从全局层面整合资源，通

过管理和技术手段的结合，形成符合企业现实需要，逐步落地、持续深化的数据安全保障机制。

• 管理层面，进行组织制度建设、安全策略制定、安全意识能力提升等工作，明确数据安全治理的工作方向，夯实安全规范的落地基础，保障管理制度和安全策略的高效运行；

• 技术层面，在数据梳理、分类分级、风险评估、防护策略等工作统筹落实的基础上，执行敏感数据流转的动态监控、综合分析、智能响应，建立及时高效、可持续优化的安全防护和运营体系。

最终随着实践经验的积累，以及创新技术和应用的成熟，持续加强安全与业务的深层融合，最大化实现“安全保发展”的战略目标。

浅谈医疗行业数据安全的必要性

售前技术部：马梦续 / 文

医疗信息属于用户的个人隐私信息，相比其他的业务信息泄露更加能够对用户生活产生影响，疫情期间的医疗行业，由于患者流调数据泄露引发的网络暴力，充分显示了信息化时代的数据泄露给个人带来的后果。

成都、沈阳等一系列地区的新冠患者个人信息泄露，在医院就诊时，被记录的除了真实姓名、电话号码等个人信息外，还有身份证号码、行动轨迹、家庭住址、个人照片等相关信息被公开，在网上一度引发热议。不管指责还是同情，对于患者都是二次伤害，在这个过程中，医院是否尽到相关的监管责任？是否切实保护患者个人数据安全？

《数据安全法》

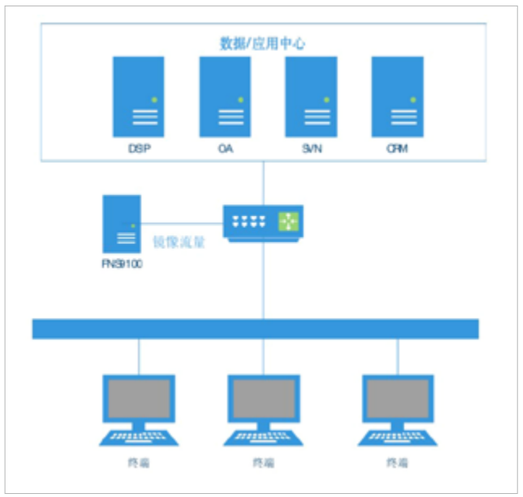
第四章数据安全保护义务，第二十七条开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

从提供诊疗服务的医疗机构来看，首先必须健全相关的诊疗信息安全保障制度，从网站、APP 等环节入手，从根源上防止信息泄露；其次是加强诊疗人员的隐私保护意识，必要时建立相关的人员管理制度文档。

部分医院的数据安全意识薄弱、场景复杂、权限混乱、数据海量、防护薄弱，针对一系列的问题，亿赛通提出有效的解决方案。

1、数据安全准入网关

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



2、数据分级管控

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

方案收益

1．建设先进、自主、灵活、全面、智能的立体化数据安全防护体系；

2. 建设满足合规要求的分级分类数据保护管理体系；

3．提供身份访问控制安全和审计溯源管理；

4．提供可有效降低泄密风险，提升防护能力，提升监管能力的技术体系；

5．提供可有效提升企业数据安全审计、管理、风险分析的可视化管理平台；

6. 提供高效、全面、完整、规范的数据安全运营服务。

MS-D：数据合规亿赛通有妙招

售前技术部：刘子宇 / 文

不知不觉，距离某打车平台 APP 下架被查已经过去了整整一年了，就在大家逐渐淡忘的时候， 网信办发布公告：“国家互联网信息办公室依据《网络安全法》《数据安全法》《个人信息保护法》《行政处罚法》等法律法规，对该公司处人民币 80.26 亿元罚款，对该公司董事长兼 CEO、总裁各处人民币 100 万元罚款。”

国家互联网信息办公室有关负责人答记者问时，将其违法行为归纳为 8 个方面，具体可以简化为六大类型：

1. 违法收集数据

主要是违法收集用户手机相册中的截图信息 1196.39 万条。此举违反了《数据安全法》第三十二条规定：“任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。”

目前，软件违规搜集资料的方式还不清楚，但估计不是侵入式的，否则将构成非法取得电脑资料的罪名。另外，违规搜集用户的手机相册中截屏内容的行为业侵犯了用户的隐私，此举也属于民事侵权。

2. 过度收集用户（个人）信息

具体包括：剪切板信息、应用列表信息、乘客人脸识别信息、年龄段信息、职业信息、亲情关系信息、“家”和“公司”打车地址信息、精准位置（经纬度）信息、司机学历信息等。

其中大多数属于用户个人信息，其过度收集行为未能限于实现处理目的的最小范围，违反了《个人信息保护法》中关于遵循必要原则等相关规定。

3. 违法储存公民个人信息

具体是指以明文形式存储司机身份证号信息。

之所以此举会被处罚，是因为我国《个人信息保护法》要求对于身份证号码等敏感个人信息采取严格采取严格保护措施，《信息安全技术个人信息安全规范》也明确应采用加密等安全措施。但是显然，明文形式存储不符合严格保护措施的要求。

4. 在未明确告知乘客情况下分析个人信息

主要包括乘客出行意图信息、常驻城市信息、异地商务／异地旅游信息等。不知道对用户个人信息进行分析是为了得出用户画像还是什么原因，但是对用户个人信息进行分析之前必须以显著方式、清晰易懂的语言真实、准确、完整地向个人告知。

尽管平台在收集相关数据时也许告知并取得了用户同意，但是如果告知范围不包括分析以上数据，那么仍然属于超范围处理个人信息，构成违法行为。

5. 频繁索取与提供服务无关的终端功能

《移动智能终端应用软件预置和分发管理暂行规定》，生产企业和互联网信息服务提供者所提供移动智能终端应用软件，不得调用与所提供服务无关的终端功能，该软件频繁向乘客索取无关的“电话权限”，违反了规定要求。

6. 未准确、清晰说明部分个人信息处理目的

根据《个人信息保护法》的相关规定，处理个人信息的前提是信息主体知情同意，因此个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知个人信息的处理目的、处理方式，处理的个人信息种类、保存期限等基本内容。

个人信息保护涉及个人隐私权，也涉及公民个人财产的安全，还涉及网络国家安全。个人信息处理者告知义务履行不到位的，不仅可能自缚手脚导致后续处理行为违法，而且模糊告知行为本身，也是违法行为。

个人信息保护应当全流程全链条全覆盖，从普通员工到高管，从入职到离职，从生产到运营与销售，从内部提取搜集到外部交换，从制度防范、物理防范到技术防范，从专项合规到常态化合规。

平台公司在数据合规方面得到了应有的教训，而其他公司也应以此为鉴，及时自查，填补自身的数据合规缺口。亿赛通动态数据脱敏系统（简称 :DMS-D）通过对数据的梳理与分类分级，脱敏与加密、机器学习等技术，及时发现数据所承载的系统、业务、网络、终端中的安全威胁，提前做好防范与合规措施，让泄密风险看得见、信息泄漏防得住、数据使用合规定，帮助企业正确使用资源，合法使用数据，保护公司的良性发展：

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。DMS-D 具有如下价值：

1. 满足业务需求

亿赛通动态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，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. 保护隐私数据

亿赛通动态数据脱敏系统内置了丰富的敏感数据发现规则，通过简单而灵活的配置即可对敏感数据进行扫描、脱敏。而且能够提供通用、定制要求的脱敏规则，在不需要投入更多的人力物力的基础上快速部署实施。

3. 满足合规需求

通过使用亿赛通动态数据脱敏系统，可以有效防止企业内部的敏感数据随意导出，防止在敏感数据在未经处理的情况下从开放的环境中被复制、流出、泄露等。提高企业的敏感数据防护能力，提升企业整体的安全等级，满足合规性要求。

在平台公司这个例子上，DMS-D 可以在应用侧让脱敏后的数据保留原有数据的特征和分布，无需改变相应的业务系统逻辑，实现了企业低成本、高效率、安全的使用生产的隐私数据；在运维侧，对敏感数据进行遮蔽处理，既不影响正常运维工作，又能够保证敏感数据，如用户个人隐私信息安全。监顾了数据使用的合规性和高效性。

从国家这几年对于安全方面的立法中，我们可以看出国家鼓励数据发展，但也强调安全作为前提，不再是之前粗放式的经营与管理，愈加重视数据安全合规。我们也能看到自平台事件开始，阿里腾讯字节等大厂也开始审视自身的数据安全。未来，数据与个人信息合规将成为所有企业尤其是所有互联网企业必须正视的重要工作之一，不论这个企业是头部的，还是独角兽，还是初创的小微企业。也许一个时代正在开始，一个数据安全的时代正在兴起。

亿赛通入选《工业互联网融合创新应用白皮书（2022 年）》，助推大数据安全稳定发展

此前，以“加快工业数字化转型，推动经济稳中求进”为主题的 2022 年（第四届）全球工业互联网大会暨工业行业数字化转型年会（以下简称大会）在浙江桐乡乌镇举办。为不断提升制造业核心竞争力，更好总结工业互联网领域阶段性发展成果、继续推进工业数字化转型工作，本次大会围绕全球工业互联网数字化转型，聚焦数字化转型在工业企业中的实际应用等问题，邀请了国内外院士、工业领域专家、学者和企业高管共聚一堂，共同探讨。大会现场除了论坛交流外，还发布了《工业互联网融合创新应用白皮书（2022 年）》（以下简称《报告》）。

《报告》深入贯彻落实习近平总书记关于网络强国的重要思想，统筹发展和安全，积极推进新基建下数字产业化、产业数字化，引导数字经济和实体经济深度融合，挖掘网络安全产品和服务在各领域的融合创新应用场景，培育优质网络安全企业，推动网络安全产业高质量发展，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）在 2021 年提前开展了网络安全产品和服务优秀案例征集活动。亿赛通经过多轮专业评审成功入选网络安全领域解决方案。

网络安全关乎国家安全、企业生产安全、人民生活安全，是工业互联网技术高质量发展最大的保障，也是我国工业化高质量发展的坚实壁垒。本次活动中，工业和信息化部信息中心在网络安全领域数百家优秀案例中，精选 17 个具有创新性和代表性的应用案例，代表了国内网络安全各细分领域的最新的技术方向，体现网络安全领域发展的最新趋势。

其中，亿赛通的大数据安全解决方案作为网络安全领域代表之一顺利入围。我司解决方案能够全方位检测数据安全问题和大数据平台存在的脆弱性问题，结合数据资产测绘、数据流转测试、大数据平台漏洞、安全配置核查多方面的扫描和检测结果，进行风险评估分析，发现数据分类分级问题、敏感数据存储分布问题、敏感数据异常使用问题、大数据组件安全漏洞问题、安全配置问题等。产品一方面便于检查机构快速发现问题，另一方面也便于大数据企业或机构自身发现安全风险，提早做安全规划，让数据风险可量化，为数据安全防护提供有力支撑。

方案采用大数据分析和集中统一控制总线技术，建立集实时数据流处理和离线大数据分析相结合的统一数据处理平台，实现以数据为中心的审计与安全防护。基于数据安全治理的原则，将数据安全策略中的控制要求在非结构化，半结构化和结构化数据库进行实现。同时，利用机器学习或行为分析能力，通过行为监控和智能分析提供更高层次的洞察力。具体技术包括以下几个方面：

数据分类和发现

根据相关政策内置字典或搜索算法，如 PCI，HIPAA 或 GDPR。具备特定 DBMS，文件类型，Hadoop 或云平台搜索的能力。此外，支持在数据库中的二进制大对象（BLOB）或字符大对象（CLOB）中搜索数据。

数据安全策略管理

提供统一管理控制台的能力，可以控制所有数据存储仓库的安全策略。将角色和责任在数据安全治理过程中统一起来，策略的应用基于通过第三方产品（如 AD 或 LDAP）进行身份验证。策略管理人员定义对特定数据的访问策略，并支持授予多个用户组访问多个数据单元的多对多的能力。

监控用户权限和数据访问行为

制定安全策略来管理和监视所有可访问特定数据集的应用用户和管理权限。通过监控 AD 成员资格的变化或个别权限的更改，以确保它们符合业务角色、数据类型或数据存储位置相关的要求。检测数据修改、权限提升和更改安全警报的功能，并拦截各种管理员在数据和应用层的非法访问。

审计和报表

合规性将需要各种监控功能的审计跟踪，例如异常用户行为，数据更改，违反政策或更改权限。在发生违规或安全事件的情况下，重要的是能够进行审计日志分析来追溯所有行为，包括数据访问、修改或权限更改。

行为分析，警报和阻断

警报机制，包括控制台显示器的告警、对关键安全人员、数据所有者或业务人员的自动消息传递。通过一些关联分析来检测异常行为。分析历史访问趋势的能力将提供越来越重要的洞察力以检测不适当的行为。

数据保护

通过加密，令牌化和数据脱敏提供独立的数据保护能力。实现透明的数据库加密可以防止系统管理员的访问，通过数据库服务器上的代理应用数据动态脱敏，并通过 AD 链接，可以用于防止数据库管理员访问，加密或令牌化字段可以保护正在活动或存储的数据元素。

另一方面，从数据处理流程上，方案对于数据采集，利用交换机网络镜像、网络旁路分光以及 Agent 探针方式将网络流量数据和主机数据引入数据处理平台。网络流量数据经过网络协议解析、业务数据提取合成统一数据格式的日志记录，供实时处理和离线分析使用。

对于数据处理，包括实时数据处理和离线数据处理两部分，实时数据处理通过高性能软硬件并结合先机的模糊比对算法实现海量数据的特征识别和比对；离线数据基于标准的大数据分析算法，实现用户行为分析和画像等功能。

对于数据存储，利用 Elastic Search 大数据集群存储原始数据记录，并实现高效的检索和分析。

本解决方案的技术创新主要体现在以下两个方面：

首先，利用机器学习等大量的人工智能技术，对采集到的各类数据进行智能分析和处理，从中提取重要信息，不仅可以在客户网络中自动发现其重要数据资产，同时可依据系统内置的数据分类分级对识别的数据资产进行自动的分类分级处理，打上相应的标签；另外，在自动识别数据资产的同时，系统可以扫描并智能分析客户网络中数据安全风险，对潜在的数据安全风险，通过系统的专家系统进行智能匹配并给出最优的解决方案和建议。

工业互联网安全和数据安全治理之路任重道远，亿赛通数据安全解决方案，经过多年的探索实践与不断优化，得到业内普遍认可。未来，我们将继续加大在工业互联网和数据安全领域的研究力度，以自身丰富的技术经验为依托，持续助推工业企业数据安全发展。

某国有银行终端数据防泄露案例

场景介绍

由于监管机构检查出的办公终端上存放着重要敏感数据文件，且以明文形式存储，以及终端电脑缺少数据泄露防护技术措施，甲方特开启终端数据防泄露建设项目。项目计划在全集团范围内对办公网、研发网、生产网的办公终端、生产终端、共用中转终端，以及分子公司实现数据防泄露建设。在建设的同时，同步制定相应的终端数据安全管理制度和规范。

客户需求

客户根据项目计划，提出以下主要需求：

1、 终端电脑部署范围接近 40 万；

2、 对 Windows 系统进行终端数据防泄露管控，同步开展信创终端的适配支持；

3、 支持对常用办公软件，如：Office、WPS、PDF、Zip、7Z、.C/C++、Python、IDEA、eclipse、点钞机、清分机等软件产生的文件进行内容识别或过滤；

4、 终端用户能够对检查出敏感文件进行判断和处理；

5、 客户端还对服务器的高可用性、产品的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，最终决定采取总分的分布式部署。服务器采取集群部署实现高可用性，产品的易用性根据一般习惯性操作方法进行修改。在项目产品的功能方面结合客户的使用场景和操作习惯进行修改，从客户角度考虑解决方案并制定开发交付计划，逐步达到项目预期目标。

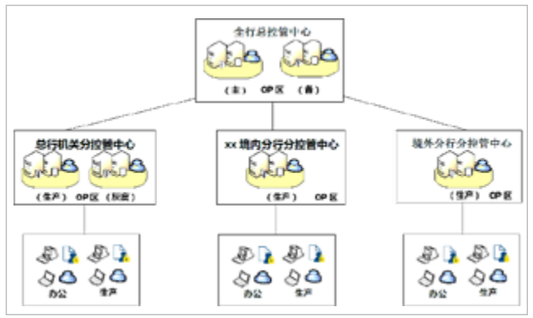


图 1 分布式部署拓扑

全行管理服务器分布式部署方式如图 1，通过各分控中心实现近 40 万终端电脑的管理、策略和事件等功能，达到终端数据防泄露的技术防护效果。全行总控中心实现对各分控中心的管理、各分控中心的敏感事件上报与用户组织架构同步。

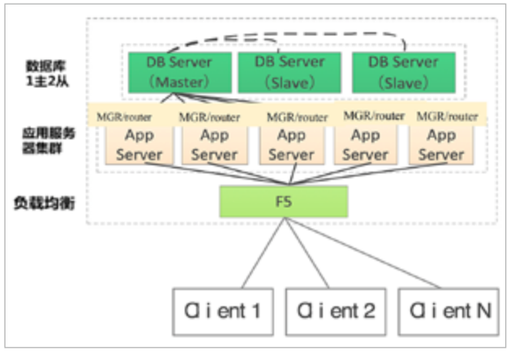


图 2 分控中心的集群部署模式

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。

经过双方沟通讨论，在保持项目目标不变的前提下，对项目步骤进行了调整。主要先盘点终端电脑上存放的敏感数据文件情况，再对涉敏文件进行治理，按照“应删尽删”原则开展终端数据安全治理。同时，对于确因工作需要在终端电脑上存放敏感数据文件，采取加密授权对存放的敏感文件进行密文存放，并根据文档重要性对密文的使用范围、操作权限进行设置。

首创性地把“数据安全是全员的事，而不仅是安全管理部门的事”通过技术手段进行实施布局。同时，为保障重要敏感文件的安全性，还增加了敏感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。在项目开展进度的基础上，按需分析设计其它有数据防泄露需要的业务应用系统在数据文件脱离原业务系统时的“离岸”数据文件防泄露能力。

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。

方案特色

1、降低数据泄密风险，保障数据资产安全

基于银行的数据全生命周期，依据数据类别、级别采取有差别、针对性的精准化防护，从终端、网络、邮件、业务系统、移动存储设备等全面构建数据安全防护体系，降低银行数据泄密风险。

2、事件追踪溯源及责任认定

全面记录客户对敏感数据的操作行为，结合屏幕监控技术，实时对敏感信息泄密行为进行拍照留存，形成完整事件证据链，确定相关责任人。

3、提高数据安全的运维效率

从资产分布、敏感数据流转、敏感数据使用、数据泄露事件、用户数据访问行为等数据安全信息，利用可视化技术进行呈现，帮助客户全面掌握全网数据安全态势，达到“底数清、情况明”的应用效果，降低运维成本。

方案价值

1、 立足产品方案制定项目方案，与客户沟通讨论达成项目目标的分解，体现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，对终端数据安全和敏感数据文件在终端间流转使用方面的安全要求，以及终端数据防泄露技术措施方面具备实际应用价值。

4、 通过项目的制定和组织实施，逐步形成满足客户实际的终端数据防泄露解决方案。还因为项目规模及场景的复杂性和客户需求的代表性，为其它同类客户的终端数据防泄露建设提供较好的参考借鉴。

客户评价

通过本次项目方案，首先帮助客户解决银行业监管合规要求。另外解决多年分散在电脑终端上数据文件模糊不清的情况，实现对所有终端的数据文件盘点，摸清敏感文件在电脑终端上的分布情况，及时识别风险并采取相应的防范措施，全员共同参与终端数据安全的盘点与防护。

甲方领导在项目阶段总结会中对亿赛通给予好评：“项目开展过程中虽然有各种各样的不足，但是厂商能够及时响应并积极分析解决。即使因为疫情采取园区封闭措施，厂商也安排了相应技术人员与我们一起封闭保障项目开展。使我行的终端数据安全不仅满足监管要求，也在实际工作中起到了安全防护作用。希望厂商能够继续保持，直到达成项目目标。其它信息安全项目的建设可以参考借鉴终端数据防泄露建设的思路和方法。”

亿赛通围绕全系列数据泄露防护产品强化创新，至今已取得丰硕成果。通过网络、终端、邮件、存储扫描防泄露产品的组合构建屏障，对受控区域内的外发数据流量进行深度解析、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。目前已为数千家客户筑起坚固的堡垒。