扫一扫，关注官方微信

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

亿赛通

ESAFENET

ESAFENET

5 月刊

2021 年共 11 期

亿赛通企业月刊　　中国数据安全专家　　www.esafenet.com

亿赛通载誉 2021 中国 IT 市场年会 揽获“新一代信息技术创新企业”殊荣！

联合共赢 | 亿赛通与爱数实现优势互补，共同树立生态合作新标杆

喜报 | 亿赛通专业方案斩获“2020 年度商密产业优秀解决方案”奖

深挖数据安全蓝海，亿赛通入选 IDC2021《中国数据安全市场研究》报告

时势造英雄，亿赛通 2021 全新启程，渠道发展迎来新时代

关注企业官方微信

Esafenet
Monthly magazines

中国数据安全专家

主办：亿赛通

策划：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

加速生态合作扩张，《亿赛通五月刊》全力出击

今天，在数字化转型的驱动下，无论是产业变革和技术迭代都在不断的加速演进，整个企业业务体系正经历着从传统化到业务数据化再到应用智慧化的变革。这种变化背后，在带来更多机遇的同时，显然也对企业提出了全新的挑战，单一力量有限，多数企业选择融合发展，因此合作伙伴通过加速融合和转型，构建多元化的角色和复合化的能力，更完整、更快速的满足企业数字化转型的各种场景需求。

大背景的推动下，以亿赛通为代表的综合安全厂商发展不断深入，推动着产业数字化进程。这其中，亿赛通数据安全产品快速、大范围渗透各大业务场景。凭借技术、服务等方面的优势，获得差异化竞争力，生态合作版全行业扩张，爱数、太平洋保险、中软……生态伙伴与亿赛通实现技术与业务的融合，甚至凭借既有的“朋友圈”让彼此的市场拓展倍速前进。

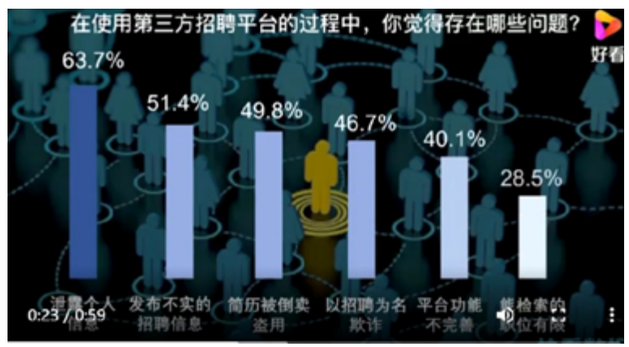
国内

1、105 款 app 通报，警惕个人信息被泄露

摘要：2021 年 5 月 21 日，国家网信办官网发布《关于抖音等 105 款 App 违法违规收集使用个人信息情况的通报》，其中，抖音、快手、360 浏览器、百度浏览器、智联招聘、前程无忧等被通报。

序号	App 名称	版本	运营者	存在的主要问题
1	抖音	15.7.0	北京微播视界科技有限公司	违反必要原则，收集与其提供的服务无关的个人信息等。
2	快手	9.3.30.10424	北京快手科技有限公司	违反必要原则，收集与其提供的服务无关的个人信息等。
3	抖音火山版	11.4.5	北京微播视界科技有限公司	违反必要原则，收集与其提供的服务无关的个人信息等。
4	快手极速版	9.3.30.1295	北京快手科技有限公司	违反必要原则，收集与其提供的服务无关的个人信息等。
5	番子短视频	2.0.5	湖南快乐阳光互动娱乐传媒有限公司	未经用户同意收集使用个人信息；未公开收集使用规则；未按法律规定提供删除或更正个人信息功能等。
6	抖音短视频	1.1.8	北京抖手科技有限公司	未经用户同意收集使用个人信息；违反必要原则，收集与其提供的服务无关的个人信息等。
7	PO短视频	2.0.0	浙江地动科技有限公司	未经用户同意收集使用个人信息等。
8	脸剪短视	2.4.8	广州繁星互娱信息科技有限公司	未经用户同意收集使用个人信息等。
9	爱奇短视频	1.1.3	奇艺有益（重庆）文化传媒有限公司	未经用户同意收集使用个人信息等。
10	快逗短视频	1.1.0.5	北京导体网络科技有限公司	未经用户同意收集使用个人信息；违反必要原则，收集与其提供的服务无关的个人信息等。
11	保护伞短视频	1.4	无锡保护伞信息技术有限公司	未经用户同意收集使用个人信息等。
12	百香短视频	78	贵州贵民（辽宁省）网络文化传媒有限责任公司	违反必要原则和《常见类型移动互联网应用程序必要个人信息范围规定》，收集与其提供的服务无关的个人信息；未公开收集使用规则等。
13	心意红包	2.3.10	深圳市心意创新科技有限公司	违反必要原则和《常见类型移动互联网应用程序必要个人信息范围规定》，收集与其提供的服务无关的个人信息；未公开收集使用规则等。
14	商千	1.1.10.41	北京一觅科技有限公司	未经用户同意收集使用个人信息；未公开收集使用规则等。
15	红包短视频	1.1.6	北京聚贤博众科技有限公司	未经用户同意收集使用个人信息等。
16	推手	4.6.4	北京万合科技有限公司	违反必要原则和《常见类型移动互联网应用程序必要个人信息范围规定》，收集与其提供的服务无关的个人信息；未经用户同意收集使用个人信息；未公开收集使用规则；未按法律规定提供删除或更正个人信息功能等。
17	Like短视频	3.24.2	广州市百果园网络科技有限公司	未经用户同意收集使用个人信息；未公开收集使用规则等。
18	有颜短视频	1.0.6.0	北京流体网络科技有限公司	违反必要原则，收集与其提供的服务无关的个人信息；未经用户同意收集使用个人信息等。
19	1440	3.1.4	贵阳四零科技有限责任公司	未经用户同意收集使用个人信息等。

2、过半受访者发现招聘平台存在信息泄露和发布不实信息



摘要：近日，中国青年报社社会调查中心通过问卷网（wenjuan.com），对 1539 名受访者进行的一项调查显示，信息泄露（63.7%）和发布不实招聘信息（51.4%）是受访者认为存在较多的招聘平台问题。90.3% 的受访者期待对第三方招聘平台进行监管。受访者中，应届生求职者占 33.4%，往届生求职者占 31.4%，在读生占 10.4%，在职者占 24.8%。

3、领英 APP 违规收集个人信息遭网信办通报 曾被曝超 5 亿用户信息泄露

摘要：LinkedIn（领英）遭遇用户信息大规模泄露。一个据称包含从 5 亿个 LinkedIn 用户个人资料的数据档案已在某黑客论坛上出售。泄露的信息包括用户 ID、名称、邮件地址、手机号码、工作信息、性别、其它社交媒体账户。

4、业主信息被开发商销售泄露给装修公司，不胜其扰


【市公安局】业主信息被开发商销售公司泄露给装修公司，不胜其扰 [复制链接] 【投诉】【已回复】 在民生e点通中查看
发表于 2021-3-20 21:41 | 只看该作者
市委书记留言箱
留言类别: 投诉
本人是雅戈尔江上业主，临近交付，平均每天能接到5-6个装修公司电话，不胜其扰。业主群里每位业主都有相似经历。
我们有理由相信：业主信息是被开发商或者销售公司违规卖给了这些装修单位。
请住建局核实，还业主清净

摘要：网友“changfengkimi”在网上发帖《业主信息被开发商销售公司泄露给装修公司，不胜其扰》投诉。根据贴文，该网友自认为雅戈尔江上业主，该业主认为雅戈尔江上开发商将其个人信息违规卖给装修单位，造成其频繁接到装修公司推销电话，不堪其扰，随发帖向市公安局投诉。

5、教育机构网站客户群体信息被泄露，警方净网行动抓捕嫌疑人

摘要：位于海淀区的一家互联网教育机构于今年 3 月报案，称其网站服务器被他人使用恶意手段高频访问，导致公司客户群体信息被泄露。海淀公安分局立即组织警务支援大队、上地派出所等单位成立专案组进行侦查。警方经过排查发现：有一个可疑 IP 对公司网站端口进行多达百余万次网络攻击，疑似以非法手段获取公司客户群体信息。办案民警掌握线索后，立即前往该可疑 IP 所在地侦查，并在当地警方的大力配合下，先后多次进行数据分析，最终锁定了一个名为张某诚的男子具有重大作案嫌疑。

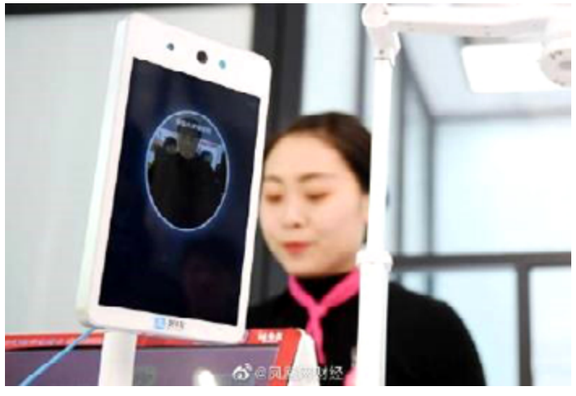
6、宁夏一新冠阳性男子信息被泄露，家人被谩骂，网友各种“问候”

摘要：五月九日，宁夏范某，31 岁，接受新冠病毒检测后，确诊为阳性。随后，他的报告在网上遭到了泄露。这条曝光信息不仅包括范某的活动轨迹，甚至还包括范某及其家人的姓名、身份证号、家庭住址等信息。

7、车主曝零跑车内有摄像头

摘要：金女士有一辆零跑汽车。她说，车子开了快一年，最近经朋友提醒，才注意到车内有个摄像头，而且只要启动汽车，摄像头也自动开启，车主根本无法关闭。

8、人脸识别国家标准征求意见：不得强制刷脸、预测偏好



摘要：近日，《信息安全技术人脸识别数据安全要求》国家标准的征求意见稿的面向社会公开征求意见。人脸识别是近年来的热议话题，现实中未告知情况下获取人脸识别数据、“强制”人脸识别等乱象时有发生。此次拟出台的国标主要为解决人脸数据滥采，泄露或丢失，以及过度存储、使用等问题，对于《个人信息保护法》草案中人脸识别相关的规定也有一定的体现和细化。国标要求，收集人脸识别数据时应征得数据主体明示同意，不得利用人脸识别数据评估或预测数据主体工作表现、经济状况、健康状况、偏好、兴趣等情况。同时，应提供除人脸识别外的其他身份识别方式供用户选择，不应因用户不同意收集人脸识别数据而拒绝数据主体使用基本业务功能等。此外，还对进行人脸识别的开发商提出了技术资质门槛，要求其具备相应的数据安全防护和个人信息保护能力，以防范人脸识别被“活照片”等非法破解。

9、“索取用户隐私”乱象频现 背后隐藏“APP 包上架”灰色产业链

摘要：在互联网应用中，“索取个人隐私”乱象频现，很多用户都在无形中泄露了个人隐私。步入大数据时代，一些 App 强制用户提供各种不相干的隐私权限，所表现出的强权架势不仅令用户反感，也受到监管部门的关注。


下载一款外卖平台软件，却被强制要求获取你的照片信息；看个电视剧，却要你对通讯录授权；浏览网页，多次弹出定位授权……在互联网应用中，类似“索取个人隐私”乱象频现，很多用户都在无形中泄露了个人隐私。步入大数据时代，一些App强制用户提供各种不相干的隐私权限，所表现出的强权架势不仅令用户反感，也受到监管部门的关注。

近日，工信部通报下架90款App，并有多家企业被点名。工信部在关于下架侵害用户权益App名单的通报中称，在近期检测中发现，天涯社区、大麦、途牛旅游等企业在App不同版本中反复出现同类问题，被下架的原因大多是因为企业存在违规收集个人信息、超范围收集个人信息、App过度索权等行为。

在大数据时代，个人信息安全如何保障？在App猖狂“索权”的背后，又隐藏着怎样一条产业链？

10、国家级考试结束，考生信息立马泄露

摘要：会计初级考试结束后，有网友爆料：考试考完第二天就收到了这个消息，不光是我，考完试的室友都收到了。而且考之前也收到各种机构的电话信息，邀请我们报他们的课程。真的很想问作为国家级的考试，泄露我们的个人信息真的好吗？？？虽然是一个大数据时代，但也不至于连国家级的考试都这样吧？

国外

1、2021 数据泄露调查：85% 的违规行为与人为因素有关

摘要：近日，威瑞森发布《2021 年数据泄露调查报告》称，网络钓鱼、勒索软件和 Web 应用攻击成为 2021 年数据泄露主要原因。网络钓鱼的人为违规行为较去年增加了 11%，占比达 36%。Web 应用程序的攻击占比则为 39%。报告还发现，61% 的数据泄露与凭证数据有关。今年与往年一样，人为疏忽仍然是对安全的最大威胁。

2、去年全球数据泄漏超过去 15 年总和，多数与邮件有关

摘要：疫情迫使世界各地的企业迅速数字化，而没有充分考虑在线业务带来的新安全要求。根据 Canalys 的最新报告“网络安全的下一步”，2020 年数据泄露呈现爆炸式增长，短短 12 个月内泄露的记录比过去 15 年的总和还多。勒索软件攻击激增，数据泄露对中小型企业的影响尤为严重。调研表明，员工人数少于 500 的企业，数据泄露的平均成本超过 250 万美元，这对于年收入通常不超过 5,000 万美元的小型企业而言无疑是沉重的损失。其中，电子邮件是勒索软件攻击的主要传播媒介。英国安全部门调查显示，91% 的大型企业遭遇数据泄露的原因是钓鱼邮件攻击，而这种威胁则从 4 年的 72% 已上升到 83%，而这一趋势仍未改变。

3、土耳其加密交易所 BtcTurk 承认超 50 万个用户数据被泄漏

摘要：土耳其加密货币交易所 BtcTurk 周一承认了自 2018 年以来的数据泄露事件，该事件已泄露了超过 50 万用户的敏感信息。根据官方公告，被盗的数据中包含 BtcTurk 用户的姓名，公民身份证号，电子邮件，居住地址，生日和手机号码。被盗的数据于上周五在论坛上首次出售，卖方声称该泄漏信息还包含带有身份证的用户自拍。

4、总部刚曝出 1166 名客户信息泄露 大华银行又因以贷收费被罚 300 多万

摘要：近日，大华银行（中国）有限公司（以下简称“大华银行（中国）”）因向部分借款人收取咨询服务费，收到中国银保监会上海监管局罚款 300 多万元的罚单。据了解，同在 5 月，总部位于新加坡的大华银行有限公司（以下简称“大华银行”）陷入客户信息泄露事件。1166 名中国籍客户的个人信息被泄露。

5、Epic 商店信息可能泄露 包括用户名邮箱和密码

摘要：有外国用户开始收到关于自己 Epic 账户信息有可能被泄露。首先是一位网友收到来自“万事通卡”的预警信息。信息中表示该泄露发生于今年 4 月 22 日，而他们在泄露信息中发现这位网友信息的日期为 5 月 5 日；泄露的信息有 1 亿 635 万 3 千 275 条，其中包括电子邮箱、密码以及用户名。而这位网友的邮箱和密码也包含在其中。

6、曝某大型发行商内部信息大规模泄露，可能包含 E3 计划

摘要：据外媒 VG247 的编辑在推特透露，有一家重量级发行商出现了“前所未有的大规模数据泄露”。他还称，现在就是倒计时阶段，看谁先忍不住把这些泄露内容发出来。目前网友对于这家“发行商”的身份众说纷纭，有些玩家担心是任天堂，还有 Xbox ERA 联合创始人爆料说是 SE。

7、日本婚恋配对 APP 的 171 万个人信息或将泄露

摘要：21 日，运营婚恋配对 app「Omiai」的株式会社 net-marketing 发表遭到了外部的非常访问。确认年龄而提交的约 171 万人的驾照等图像数据有泄露的可能性。4 月 28 日 15 时左右，管理「Omiai」服务的会员情报的服务器检测出了非预期的行为。公司内检查的结果，发现确认用户年龄文件的图像数据有非法访问的痕迹。图像数据包括已经退会的旧会员。对象的个人信息是 2018 年 1 月 31 日～ 2021 年 4 月 20 日期间提交了年龄审核文件的 171 万 1 千 756 件份的年龄确认文件的图像数据。具体包括驾照，健康保险证、护照、My Number Card 等，其中 6 成是驾照的图像数据。

8、爱尔兰卫生部长证实，HSE 的患者数据已经在暗网上泄露

摘要：爱尔兰卫生部长斯蒂芬·唐纳利 (Stephen Donnelly) 证实，HSE 数据已经在暗网上泄露，并补充说，勒索软件的攻击是“广泛的”、“卑鄙的”，对患者造成了“现实世界”的影响。《金融时报》报道称，该公司已看到一些截图和文件，证明 HSE 患者的医疗和个人信息在网上被共享——该公司称，这是自 HSE 勒索软件攻击以来首次确认数据泄露。

9、用户隐私 or 智能监测怎么选，独家：乔布斯生前采访聊用户隐私

摘要：史蒂夫·乔布斯：“保护隐私不意味着不搜集数据，而是要让用户知道你用这些数据干了什么。要用准确、平实的语言向用户取得授权。”

10、攻击美国油管公司的 DarkSide 被查封，现已关闭运营，现已关闭运营

摘要：Recorded Future 研究人员 Dmitry Smilyanets 在黑客论坛上发现了名为 UNKN 的用户发布的帖子，而 UNKN 是 REvil 勒索软件团伙的账号。帖子显示，受执法行动影响，DarkSide 已经无法访问其数据泄露服务器、赎金支付服务器和 CDN 服务器。

亿赛通载誉 2021 中国 IT 市场年会
揽获“新一代信息技术创新企业”殊荣！

2021 年，是“十四五”开局之年，也是中国迈入新数据时代的元年，是全面进行深刻数字化转型的关键之年，数字经济、数字化能力的重要性也日益凸显。在此背景下，5 月 20 日由赛迪顾问股份有限公司主办 2021 IT 市场年会在北京隆重召开。IT 市场年会已连续举办 22 届，是中国 IT 业界延续时间最长的年度盛会之一。

本次会议以“强健产业供应，引领创新发展”为主题，邀请专家学者、企业领袖、行业用户等共同参与，共同探讨新 IT 领域的跨界融合与创新。本次大会重磅发布了“2021 IT 市场权威榜单”，亿赛通荣获 “2020-2021 年度新一代信息技术创新企业”这一重磅奖项。

能揽获此项大奖，得益于亿赛通长期致力于做客户信赖的长期合作伙伴，在数据安全领域深耕多年。同时，亿赛通顺应形势，积极关注国家政策，想客户所想，使得公司能够较为全面、深入地了解客户需求，从而开发出符合客户业务特点的产品与解决方案，为客户提供可感知的价值。

自进入数据安全领域以来，亿赛通一直通过对数据安全领域地不断探索，突破了一系列的技术创新壁垒，实现了产品、服务的全新升级，并拥有了全系列数据安全产品及解决方案。

在数据泄露防护领域，根据赛迪顾问报告，自 2015 年起，亿赛通数据泄露防护系统市场占有率始终保持在国产品牌第一位。目前，亿赛通全系列安全产品与解决方案已广泛应用于金融、制造、央企、运营商、能源、地产、医疗、集团等行业和领域，为客户的数据安全稳定可靠运行持续保驾护航。

匠心经营 18 载，技术创新始终是亿赛通发展和成长的重要驱动力，公司持续加大研发投入，创新体系建设，专注于技术的革新，在发展模式上，采用“渠道 + 直销”的销售模式，依托遍布全国的客户网，持续强化核心渠道建设，在产品研发、工程交付、服务质量管控上不断突破创新。

亿赛通作为中国数据安全行业具有代表性的国有品牌，在以往与客户合作的解决方案中，不断满足客户新的需求，拉动了文档加密、数据泄露防护等专业产品销量呈量级的增加。获得奖项和认可，既是鼓励也是激励，近些年亿赛通也在产品革新上不断尝试调整与增设。未来，亿赛通将继续围绕新一代信息技术加大投入布局，通过提供创新的产品和服务，全面服务经济社会数字化转型和高质量发展。

喜报 | 亿赛通专业方案斩获“2020 年度商密产业优秀解决方案”奖

近日，一场以“因密而安”为主题的密码行业盛会——“2021 密码大兴峰会”在北京国家新媒体产业基地开幕。此次会议由北京市密码管理局、北京市大兴区人民政府、中国电子学会指导，信息安全与通信保密杂志社、中关村中安高速密码产业联盟（筹）联合主办。本次活动围绕《中华人民共和国密码法》的宣传普及，聚焦密码技术、密码产品与服务、密码应用市场及未来前景，汇集行业管理者、专家学者、企业精英及产业同行，问诊密码行业问题和解决方案，共话密码产业成果和未来，致力建设密码行业产业链交流融合的平台，推动密码产业向更好、更快、更健康的方向发展。

其中，“2020 年度商密产业优秀解决方案”评选活动是由《信息安全与通信保密》杂志、数观天下联合众多家商用密码企业发起的针对中国商用密码领域的评选活动，旨在发现和挖掘商用密码领域优秀解决方案，共同携手推进中国商用密码行业和产业持续创新与发展。亿赛通凭借专业项目解决方案荣获“2020 年度商密产业优秀解决方案”奖。

亿赛通遵照相关法规和标准，针对行业痛点及企业的需求进行剖析，具体需求如下：

信息中心和业务部门侧重于整体系统安全防护；

保密办和办公厅由于涉密专人专岗，涉密系统定级整改，所以更侧重涉密信息系统。

亿赛通对其从终端至网络全方位进行防护，管控全面的流出渠道控制，提供完备的事件审计功能等，实现了对数据的安全管理，提高了企业内网数据的安全性，提升企业信息安全等级。

1. 主动泄露防御，分级精准控制

通过部署在内部网络和外部网络连接的出口处的网络 DLP 系统，对进出单位内部网络的所有网络敏感数据进行扫描防护，对敏感数据泄露事件可根据策略进行阻断。

系统能在事件发生时及时响应，包括：阻断、警告、日志记录、邮件通知；

系统能对用户角色和管理员角色进行划分和权限设置，并将权限控制在最小范围内；

支持旁路镜像流量部署；

支持物理串联部署；

支持多层级部署架构，横向扩展能力；

流量捕获设备与内容检查设备为一台设备，支持高可用及扩展；

管理平台及数据库高可用，支持使用多台管理平台构建管理群集，防止单点故障。

2. 明确定位数据，全通道控制

通过内部邮件进行敏感内容防控，并进行增删收件人，邮件正文替换，剥离敏感附件、邮件告警、邮件审批、邮件阻断等操作。

支持按用户、规则、全局设置白名单、审计策略；

可根据 IP、IP 段、域名、URL、关键字、文件类型、文件大小、发送者、接受者的检测等进行多维度灵活组合策略配置；

每条策略可单独设置风险响应办法，包括邮件告警和邮件处理等；

支持策略自定义，策略能够定义不同算法、算法的组合逻辑，如与、或关系。

3. 识别敏感内容，标记敏感级别

通过网络协议的还原和对数据的检测分析，获取此协议承载的数据情况，对违规内容进行安全防泄露处理，并进行违规数据统计和态势分析。

亿赛通为企业建设科学先进、自主可信、可扩展同时又满足央企商密保护合规要求的全方位数据防泄密体系。可提供完整的商密数据资产生命周期风险控制和自动化管理，确保其网内各类涉密信息系统数据下载内容识别、内容保护与审计，针对携带敏感内容的终端电子文档进行管控。系统部署有效降低业务运营中的 IT 风险，提升海关敏感数据防护能力，降低多重安全合规管理成本。

亿赛通数据安全解决方案目前已经在央企、集团、金融等多个行业得到了广泛应用，不仅解决了数据安全防护能力薄弱、电子文档管控力度不足等问题，而且对数据进行整体监控、追踪、溯源，有效的支撑运维、规避风险，构建了以数据为核心的服务和安全体系，增强了企业信息安全治理能力。

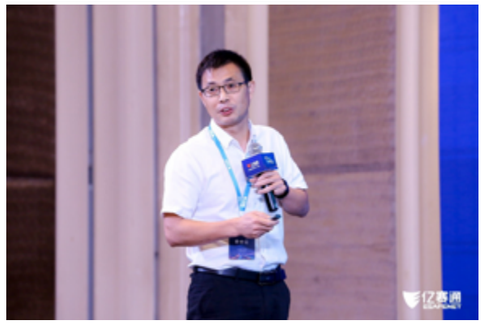
时势造英雄，亿赛通 2021 全新启程，渠道发展迎来新时代

在激烈的市场竞争中，渠道的建设与维护已经成为企业拓展市场的要素，同时，渠道伙伴也是企业产品占领市场的关键。如何建立良性的渠道合作生态体系，做好渠道建设的同时提升渠道伙伴的整体能力，成为了企业发展的重中之重。为此，亿赛通结合自身企业优势，与众多渠道伙伴强强联合，在激烈的市场环境下不断提升综合竞争力。

2021 年 5 月 15 日 -16 日，亿赛通在桂林隆重举办“智慧安全 共创未来”2021 年亿赛通全国渠道大会。来自全国百余位渠道伙伴亲临现场，与亿赛通畅聊产业发展的盛况。本次大会赚足眼球的除了人头攒动的大会现场、专业产品与解决方案的纯干货分享，会中还有 2020 年优秀代理商经验独家揭秘！

亿赛通邀请了所有的渠道伙伴们，一同携手共赢蓝海，一起感受产业变革带来的力量。本次 2021 亿赛通全国渠道大会有哪些亮点呢？快来和小亿一起围观。

在十四五规划的开局之年，要“加快数字化发展 建设数字中国”，加强网络安全保护，提升安全防护能力，在网络应用发展波涛汹涌的浪潮中，网络安全的需求日益凸显，时代赋予了我们展现英雄本色的机会。在如此大趋势下我们如何应势而为？



近几年，数据安全方面无论是基础设施建设还是相关政策都在不断变化，不管是大型企业还是中小型企业都产生了很多新的安全需求，以及对于员工安全意识的需求。亿赛通也因此有针对性的重新优化安全模式，推出全新服务方案及交付流程。对于亿赛通这一数据安全“香饽饽”，产品方案与时俱进，专家表示，公司架构根据十余年专业经验多方面改革：从专业文档加密厂商，到数据安全防护厂商，近两年转变为数据安全综合厂商。亿赛通正向着更纵深、更复合的方向发展，帮助渠道伙伴挖潜市场，从技术赋能帮助企业让管理更智能化、更精细化。

网络技术蓬勃发展，软件应用日新月异，安全面临的威胁亦是愈发严峻。但越是有挑战，越是给了我们彰显技术实力的舞台。在这里，由亿赛通专家解读了数据安全产业发展趋势，在面对现今的安全态势，亿赛通欲善其事，必利其器，通过不断夯实技术能力、构建数据安全生态圈，细分类别、细化行业、拓展区域、抓新方向来优化营销结构。同时针对当前的客户的需求变化进行了详细分析，将产品变成一个个组件，合规化，专业化，组合成个性化的服务给到渠道伙伴及客户，用架构牵引产品的变化以及客户的服务变化，并在变化的时代中，更好的满足客户的需求。

针对目前日益严峻的数据安全形势，基础的技术服务只是服务的开始，在应对突发安全事件时，如何通过服务使安全产品的组合能力发挥到最大？如何通过服务帮助客户快速处置安全问题？战场拼杀离不开趁手的兵刃，商场如战场，我们的渠道伙伴们同样也需要给力的渠道支持政策以及优秀的产品方案支撑。现如今，亿赛通安全服务、产品方案、工程交付一应俱全。公司行业解决方案也在不断更新，分会场中，技术专家详细讲解了制造、医药、地产等领域打造的方案创新，结合应用需求的场景化方案和实践案例。

2021 年是“十四五”规划开局之年，也是全面深化改革、加快形成引领经济发展新常态的体制机制和发展方式的关键之年。站在新一个五年的开端，亿赛通将坚持智慧安全的创新战略，围绕企业业务本身做进一步的组织转型，持续加大在行业内的营销投入；进一步优化对渠道伙伴的激励政策，牵引渠道伙伴转型和能力提升；将持续构建安全服务体系，与渠道伙伴进行更好的服务利益分享，提升新商业模式下的服务能力和可销售性。

深挖数据安全蓝海，亿赛通入选 IDC 2021《中国数据安全市场研究》报告

目前，随着信息革命的深入推进，数据已经成为国家基础性战略资源，数据安全已经上升到维护国家主权的高度，近年来大数据产业快速发展催生数据安全需求增加，国家、企业数据主权面临着潜在隐患和挑战。

对此，全球著名数据公司 IDC 特别针对中国数据安全市场，推出了 2021《IDC Perspective：中国数据安全市场研究》报告，通过对国内外云服务提供商、综合型安全公司、专业型安全公司进行研究，综合产品体系、技术、架构等方面的分析。

而亿赛通，通过最新更新的产品架构，细分的五大产品类别，形成一体可视化态势感知数据安全智能管控平台。本次报告凭借着出色的技术创新能力以及良好的市场口碑，顺利通过 IDC 审查小组的层层审核，成功入选 2021《IDC Perspective：中国数据安全市场研究》报告。

在过去的一年里，频繁发生的数据破坏、数据泄露等安全事件，将“数据安全”的理念提升到一个新的层次，受到各行各业的高度重视，市场需求不断增加。而 IDC 认为企业需要根据自身的发展情况，从企业级加密与数据保护；新兴数据安全防护；数据可见性、控制和报警三个维度考虑数据安全建设方案。

亿赛通近二十年来，一直专注于数据安全的技术创新，累计已经服务医疗、金融、政府、运营商、研发通讯、地产、芯片半导体、能源、设计制造、集团企业等十大行业数万家客户。

针对数据安全的特殊性，我们以“分 ▪ 放 ▪ 管 ▪ 服”为数据安全建设理念，将数据实现分权分责分风险，放权管责相结合，做到要素服务保支撑，持续安全可运营，不断打造保护核心数据安全的精品，经过长期的积累，打造出对数据全生命周期进行防护的综合解决方案。

作为数据安全领域的优秀供应商，亿赛通紧跟国家战略，致力于自主研发、技术变革、产品创新，在数字化转型的大潮下，全力协助客户实现数据安全管理创新与有效安全防护，助力客户数字化经济安全转型。

联合共赢 | 亿赛通与爱数实现优势互补，共同树立生态合作新标杆

5 月 26 日，亿赛通与上海爱数信息技术股份有限公司（以下简称：爱数）在 2021 天津城市论坛签署战略合作协议。双方将充分整合各自在产品、技术、服务等方面的优势，形成紧密、全面、可持续的战略合作伙伴关系。

亿赛通与爱数正式签订战略合作

作为中国数据安全行业领军企业，亿赛通产品覆盖政府、金融、能源、运营商、地产、医疗等重要行业的六百余万终端，已构筑起全方位、多层次、立体化的数据安全管理管理体系。

而作为一家领先的大数据基础设施供应商，爱数致力于为政府、公共事业及企业的数字化转型赋能，以开放平台架构，与合作伙伴共建数字能力生态，帮助各行各业在数字化浪潮中充分释放数据价值，实现即时、随时、实时的数据服务。

综上，双方在数据安全、基础设施建设相关行业市场、技术研发与产品服务方面均具有良好的合作基础。

随着互联网时代的飞速发展，越来越多的企业开始成为数据的工厂和载体，这些数据的安全管控与企业的正常运营紧密相关，对于高度依赖数据、数据高度集中的企业而言，如何降低“各种意外”对其数据的安全威胁已成为当前急待解决的重要问题！

基于本次生态合作，旨在帮助企业在纷繁复杂、危机四伏的大环境中更好地保障数据安全，亿赛通与爱数联合推出“电子文档安全管理系统 +AnyShare Family 7”解决方案。

双方产品的融合可实现最大化优势互补：一方面，通过亿赛通电子文档安全管理系统对本地终端文件进行管控；另一方面，AnyShare 可实现云端文件管理，真正做到线上线下全方位管控。同时，基于策略驱动的安全管控体系能支持更多的安全管控场景，满足客户不同的安全管控需求，从而维系企业相关业务工作的正常运转，为企业的数据安全与业务的正常运转保驾护航。

除本次合作外，亿赛通还将与爱数在安全领域展开深度技术合作，通过方案融合，产品升级等模式，持续完善、提升数据安全相关产品与解决方案，共享资源、共建生态、共同发展，为广大客户提供更加完善、高效、可靠的信息安全技术、产品与服务保障！

亿赛通牵手太平洋产险
为网络安全加颗“定心丸”

近些年，“网络安全保险”一词逐渐进入人们的视野。顾名思义，网络安全保险保障的是由于网络安全事件给企业带来的直接财产损失，以及第三方客户提出的索赔责任。在网络威胁不断加剧的今天，企业在购买网络安全产品与服务，做好自身网络安全能力建设的同时，再加上网络安全保险的保障，可进一步减少损失，转移剩余风险。

在欧美国家，网络安全保险行业经过多年的发展，已趋于成熟。无论是从险种设计、理赔方案等来看，还是与网络安全保险相关的政策法规的完善，网络安全保险行业运行在国外已形成了成熟的体系。据统计，目前美国已有超过 500 家保险公司可以提供网络安全保险服务。当下，全球网络安全保险市场发展迅猛，有机构研究显示，2021 年全球网络安全保险市场预计将激增 21%，市场规模达到 95 亿美元，到 2025 年，预计将达到 204 亿美元。而国内网络安全保险行业还处于初期发展阶段，市场规模还较小。但随着企业数字化转型步伐的加快，“十四五”规划纲要中也强调要进一步加强网络安全建设，同时，企业对网络安全风险带来的影响认识也在逐步提升，尤其是数据泄露、勒索软件等造成的直接经济损失，让企业越来越意识到防范并化解风险的重要性。

数据显示，中国平均每年由于网络安全问题造成的损失高达 600 亿美元，居亚洲首位、全球第二。那么，网络安全保险作为转移风险的重要手段，是否会成为一片新的蓝海呢？

日前，数据安全厂商北京亿赛通科技发展有限责任公司（以下简称“亿赛通”）与中国太平洋财产保险股份有限公司（以下简称“太平洋产险”）达成战略合作，将共同开展网络安全保险业务，发挥各自优势，为企业提供基于亿赛通“文件防火墙”产品的保险服务。

随着企业网络业务的不断增多，网络安全问题越来越受到重视。在网络安全事件频发的环境下，保险作为企业机构风险转移的重要手段也越来越得到关注，当前正迎来可观的发展机遇。据太平洋产险网安险项目总负责人刘愉女士介绍，太平洋产险作为国内开展网络安全保险业务的先行者，已在金融、医疗、工业互联网等领域为企业提供了涉及数据安全、身份安全、文档安全等方面的保险服务。本次合作将借助亿赛通在数据安全防护方面的过硬实力，并结合太平洋产险在保险领域雄厚实力与专业服务能力，同时整合双方在各自行业的客户资源，更好的促进网络安全保险业务的发展。刘愉表示，在国家相关政策法规的支持下，以及客户对网络安全保险认识与认可的提升，行业将进入一个快速发展期。不过，国内的网络安全保险业务还有一些需要完善的地方，例如保单内安全风险覆盖不明确导致操作困难、理赔时定责定损等问题。术业有专攻，今后太平洋产险会持续深入的跟网络安全企业进行合作，以获得网络安全能力方面的专业支持，进一步完善网络安全保险服务，帮助客户企业健康稳定运行，助力国家数字经济发展。

自 WannaCry 勒索病毒爆发以来，近些年勒索病毒如雨后春笋般席卷全球，黑客窃取企业数据和文件并以此进行勒索，带给企业严重破坏，造成了巨大损失，令人头痛不已。此次亿赛通以独有的防勒索产品“文件防火墙”与太平洋产险进行网络安全保险合作，既从防护端为企业提升安全能力，同时也为企业减轻损失，减小风险。亿赛通总经理崔培升表示，现在网络安全威胁给企业带来的损失并不亚于企业设备的损坏或者金融风险等其他方面带来的损失，所以企业现在越来越重视网络安全问题。尤其是像金融行业、互联网、智能制造等对资金损失或业务连续性较为敏感的领域，遭受网络攻击或勒索病毒攻击，后果不堪设想。在做好网络安全能力建设的同时，购买网络安全保险能进一步有效防范并化解风险，降低企业的损失。

据亿赛通 CTO 朱贺军介绍，亿赛通文件防火墙是为防止勒索病毒对企业的核心数据进行恶意攻击的安全防护软件，其加入到网络安全保险的合作模式为“保险 + 避险工具”——由传统的服务模式“事后理赔”转变新的服务模式“事前防御、事中预警、事后补偿”，具有数据价值明确、责任认定清晰、坚定过程简单、定向定点防护等优势。

目前，数据安全法（草案）、个人信息保护法（草案）都已进入二审阶段，关键信息基础设施保护条例也将很快出台，相信今后有关部门也会制定关于网络安全保险方面的政策法规，规章制度的完善势必会促进网络安全保险行业更快更好的发展。崔培升表示，未来亿赛通会结合自身业务优势，继续与保险领域合作，尝试开拓更多方向的网络安全保险业务。

在各方面不断完善发展的背景下，网络安全保险将会成为产业生态不可或缺的重要组成部分。我们相信这片蓝海不久即将迎来风口，成为我国数字经济发展的必然助力。

最高调的勒索攻击，美国进入紧急状态

目前，有研究表明，网络犯罪分子仍在持续不断地进行勒索活动，只要成为勒索软件攻击的目标，自己将很快无法开展业务，不法分子会索要比以往更高的赎金。

网络犯罪分子之所以封锁网络，原因在于这是从被攻陷的组织中赚钱的最快、最简单的方式。攻击者要求支付赎金，以换取文件的解密密钥。近几年，勒索要求不断上升，勒索软件团伙定期向受害者索要数百万美元的比特币。

亿赛通小贴士 ESAFENET PROMPT

但不幸的现实是，勒索软件的不断得逞，在于因为大量受害者屈服于勒索要求的罪犯支付赎金。虽然官方倡导不应付钱给犯罪分子，但多数企业领导者觉得这是恢复网络和防止长期经济损害的最快和最简单的方法。

近日，美国关键基础设施遭遇了迄今为止最严重网络攻击。该公司的工业控制系统 7 日遭到网络攻击，被“勒索软件”要求支付赎金，否则其数据将被公开或删除。由于输油管线遭到网络攻击，美国总统拜登宣布美国 17 个州和哥伦比亚特区进入国家紧急状态。

这起罕见的黑客攻击事件充分暴露出高度网络化的基础设施体系具有的脆弱性，也凸显了国际社会合作应对非传统安全威胁的必要性。

勒索软件是企业的主要威胁，但企业可以通过采取相对安全、保险的措施来保护自己免受其害。太平洋保险 & 亿赛通联合推出一款网络安全保险服务，针对勒索病毒专门针对企业高价值文件防勒索的保险产品，为投保人高价值文件提供保障。

现今，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。

我们应该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。这份网络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。

作为数据大国，网络安全保险大势所趋。勒索病毒由于具有明确的定损数额，是在数据安全领域进行保险试水的不二选择。亿赛通的文件防火墙 + 保险服务，为企业勒索软件防护提供封闭式屏障，减少企业被勒索的风险，将企业的勒索损失减到最低。此次跨领域的协同机制与技术支持，加速相关产业的创新发展，产生示范效应， 在网络安全保险领域具有里程碑式重大意义。

谈之色变，印度航空惨遭黑客攻击

即便是不愿承认，但当我们在享受互联网带来的快速，便捷，智能的时候，有意或无意间，已经卖掉了自己隐私。

近日，印度航空官网发布消息，大约 450 万名客户的数据遭黑客窃取，黑客窃取的数据包括乘客的姓名、信用卡信息、出生日期、联系信息、护照信息、机票信息。

据了解，本次攻击损失了过去十年在印度航空公司注册的乘客的数据（2011 年 8 月至 2021 年 2 月 3 日）。目前已采取了相关措施，调查数据安全事件、保护被破坏的服务器、聘请外部数据安全事件专家、通知信用卡发卡机构并与之联络，以及重新设置印度航空公司 FFP 项目的密码。

针对此次黑客攻击事件，印度航空公司并不是唯一的受害者，其他星空联盟成员也受到了影响，其中包括新西兰航空，国泰航空，芬兰航空，济州航空，汉莎航空，马来西亚航空，SAS 和新加坡航空。而泄露的 450 万客户信息也只是刚刚开始，因为这种影响会持续很长一段时间在全球蔓延，受到牵连的企业和个人数量可能还会扩大数倍。

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人员、维护人员、工程师，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大型数据泄露事件，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，在印度航空这件事情上，根本原因是公司安全防护不到位，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客户隐私信息。不仅仅是国外企业，国内亦如此，中国数据安全专家亿赛通，与众多重要行业携手打造客户信息安全，既保证企业业务网络较高的可用性、可靠性、保密性，又对内部核心数据有较强的防御、管控能力，如亿赛通电子文档安全管理系统，实现了企业内部电子文件的加密存储。倘若未经合法许将加密文件带走，其文件内容将不能够被正常打开，从而确保文件内容不会因为文件数据扩散而泄密。

亿赛通数据安全管理体系可以有效支撑国家信息空间管理业务，提升国家公共安全工作的发现、管理能力与处理效率，为客户国家安全贡献重要技术力量。若要详细了解亿赛通数据安全解决方案，保障企业数据安全，可咨询服务热线：400-898-1617。

长鑫存储技术有限公司

客户简介

2016 年 5 月，长鑫存储的事业在 “创新之都”——安徽合肥启动。作为一体化存储器制造商，公司专业从事动态随机存取存储芯片 (DRAM) 的设计、研发、生产和销售，目前已建成第一座 12 英寸晶圆厂并投产。DRAM 产品广泛应用于移动终端、电脑、服务器、人工智能、虚拟现实和物联网等领域，市场需求巨大并持续增长。长鑫存储将凭借值得信赖的产品和服务满足不断增长的市场需求，致力于成为技术领先与商业成功的半导体存储芯片公司，以存储科技赋能信息社会，改善人类生活。

需求背景

因长鑫存储发展及业务需要，各类包含大量重要信息的电子资料，如源代码、设计图纸、财务报表、技术文档等与公司知识产权相关的数据被高度共享，数据安全保护依赖某 DLP 产品，但其产品本身存在安全漏洞，这些核心数据关系到公司的生存发展以及商业竞争力，一旦泄密，将会给公司造成不可估量的损失。非核心数据安全保护层面的措施仅限于传统网络安全、存储冗余和文件服务器管理等层面，对于信息系统、业务平台、网络通讯、办公终端以及存储介质中的数据均以明文形式存在，在数据资产的使用、传输、保管、销毁的过程中存在较多安全风险，增加了信息安全管理工作难度。

解决方案

根据长鑫存储现有情况，以及对文档安全管控的实际需求建立电子文档加密系统解决方案。

多秘钥隔离：系统采用多密钥加密隔离方式，对不同类型的电子文档设置不同的密钥，密钥之间相互独立；

加解密中间件：提供加解密接口、外发接口给自研等业务系统，实现文件上传解密、下载加密、外发加密功能；通过策略方式实现指定业务系统 IP 的文件上传解密、下载加密功能；

策略模式切换：通过终端用户桌面悬浮窗口方式，用户自主切换策略模式，系统管理员在服务平台设置好策略模式对应密钥关系后，下发给终端用户。

加密锁图标显示：用户在同一台终端上，不同密钥加密的文件显示不同颜色加密锁图标， 加密文件在云盘里的图标能够共存显示，一个系统可支持多种密钥锁图标；

密钥打印控制：用户在同一台终端上，不同密钥加密的文件可区分控制是否允许打印，不允许打印的加密文件，可申请打印审批流程，审批通过后方可打印。

项目成果

长鑫存储解决方案成功部署后，保障公司内部电子文档的使用安全，支持多种文档类型加密保护，防止用户通过剪切板拷贝、拖拽、另存为、截图等操作行为泄密；进行了文档权限管控，按照组织架构（部门、用户等）对文件进行授权管理，同时控制文档的使用权限及生命周期；通过对外发文档授权封装，保障数据在企业外部环境的使用安全; 加密系统服务平台支持双机热备软件,提供高可用、安全性保障。

北京兆易创新科技股份有限公司

客户简介

兆易创新成立于 2005 年，是一家领先的无晶圆厂半导体公司，致力于开发先进的存储器技术和 IC 解决方案。2016 年 8 月，公司在上海证券交易所成功上市。公司在多个国家和地区均设有分支机构和办事处，营销网络遍布全球，为客户提供优质便捷的本地化支持服务。在质量管理方面有严格的标准与要求，已获得 ISO 9001、ISO 14001 等国际质量体系认证，同时积极推进产业整合，拓展战略布局，在已有的微控制器、存储器基础上，布局物联网领域人机交互技术，并与全球多家领先晶圆厂、封装测试厂达成战略合作伙伴关系，通过加强产业上下游合作、优化供应链管理，共同推进半导体领域的技术创新。

需求背景

当前大数据、云计算是行业大趋势，网络边界变得越来越模糊，企业自身已经无法完成所有的安全防护；同时，新的攻击手段层出不穷且目的性更强，攻击手法也经过精心设计，很难发现其特征。所以企业对威胁的防御已经不可能再是简单部署安全设备。将各种安全防护手段和信息整合起来，既要防止新的漏洞和应用方式引入风险。

解决方案

亿赛通电子文档安全管理系统具体帮企业实现了如下功能：

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

2. 内容安全管控：可截屏录制文档阅读水印、文档打印水印、拷贝粘贴控制；

3. 工作模式切换：提供“密文 / 明文”切换模式，保障业务涉密数据安全处理的同时，不影响用户个人数据处理；

4. 安全浮水印支持：为保证核心数据的打印安全以及可追溯性，系统提供对加密文档的阅读和打印浮水印功能，通过自动添加安全警示及版权标识信息来降低屏幕录制和自主打印带来的泄密风险，水印支持自定义；

5. 多密钥隔离：可实现部门动态加密文档相互隔离禁止交叉打开，管理人员可以打开各部门文档，自身文档可自动或半自动透明加密，密钥可以独立或某个部门相同；

6. 文档权限管理：可以细粒度权限控制、模板批量授权、文档权限管理；

7. 文档外发管理：可进行用户身份认证、使用权限管控；

8. 流程管理：可以进行文件解密审批流程、文件外发审批流程、邮件外发审批流程、离线办公审批流程、文件还原审批流程。

项目成果

通过信息安全边界建立，以数据加密为核心，以数据的安全技术管控保障为落实关键，结合单位业务发展规划及保密条例与等保合规要求，构建完善了单位数据安全保护体系。降低了兆易创新核心信息资产的有意或无意泄密风险，保障文档在存储、使用过程中的安全，加强了系统保密管理工作。