

安全牛—亿赛通和太平洋财险签订战略合作协议，共同推出网络安全保险服务



《中国网络安全行业全景图（2021.03版）》发布，
亿赛通九大细分领域强势上榜

亿赛通数据安全产品与飞腾完成产品兼容认证，信创
生态再进一步

聚焦政策法规，数据安全行业喜迎全新局面



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



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



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 赋能企业勒索病毒防护，《亿赛通四月刊》深入了解网络安全保险

行业聚焦 INDUSTRY FOCUS

4-8 国内行业新闻

9-13 国外行业新闻

亿赛通动态 ESAFENET NEWS

14/15 《中国网络安全行业全景图（2021.03 版）》发布，亿赛通九大细分领域强势上榜

16/17 实力认证 | 亿赛通强势上榜《CCSIP 2021 中国网络安全产业全景图》

18/19 亿赛通数据安全产品与飞腾完成产品兼容认证，信创生态再进一步

20/21 安全牛—亿赛通和太平洋财险签订战略合作协议，共同推出网络安全保险服务

22/23 数世咨询—网络安全保险新军亿赛通与太平洋财产保险合作签约

亿赛通小贴士 ESAFENET PROMPT

24/25 从热播剧了解网络安全

26/27 震撼场面，多家行业巨头遭遇数据泄露，数据安全曲突徙薪

28/29 聚焦政策法规，数据安全行业喜迎全新局面

典型案例 TYPICAL CASES

30/31 中国人民财产保险股份有限公司

32/33 深圳市慧择保险经纪有限公司

赋能企业勒索病毒防护， 《亿赛通四月刊》深入了解网络安全保险

近年来，全球范围勒索病毒现象严重，据《2019 威胁态势分析》报告显示，中国勒索病毒的数量居全球榜首，造成业务停摆，声誉下降，且恢复成本巨大。基于此类情况，太平洋财险 & 亿赛通联合推出网络安全保险服务，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。双方的合作进一步拓展网络安全保险生态链，提升客户体验，承担保险发展使命。《亿赛通四月刊》与您详细介绍网络安全保险那些事儿，快来与亿赛通一起体验安全领域不一样的感官盛宴，在这里产品的创新和企业多年来一路的坚持所取得的成绩让我们对亿赛通有了不一样的认识……



国内

1、个人信息泄露引来夺命连环 CALL？ 检察出手了！



摘要：4月22日，最高人民检察院发布个人信息保护公益诉讼典型案例。从发布的11起典型案例看，个人信息泄露真是无处不在。在浙江省温州市鹿城区人民检察院督促保护就诊者个人信息行政公益诉讼案中，温州某儿童摄影公司员工张某某、某儿童培训公司员工卢某某等人就是通过购买、交换等方式，从温州多家医院非法获取1万余条孕产妇个人信息。

2、虚假招聘坑人！58同城超4万条 打工人信息被泄露



摘要：4月20日，广州白云法院对蒋某等人犯侵犯公民个人信息罪一案进行宣判，五名被告人分别被判处有期徒刑二年到十个月不等，并处罚金。经查明，蒋某购买58同城网站的账号后，再指使员工在58同城发布大量虚假招聘信息，以收集应聘者的公民个人信息，再由同伙将这些信息贩卖给他人牟利。经审计，蒋某等人非法获取、销售公民个人信息共计4.2万多条！

3、人脸识别进北京南湖中园社区： 业主称被“默认同意” 担忧信息泄露



摘要：李京（化名）开不了小区的单元门了。门上挂着一个“刷脸”设备，他拒绝录入自己的人脸信息。他是北京南湖中园二区的一名业主，从去年5月开始，小区部分单元门启用人脸识别门禁系统，业主必须采集人脸照片，并提供房产证、身份证、手机号等个人信息——这是业主们打开单元门的唯一方式。“人脸信息与身份证、住址相关联，系统就会对你进行全面监控，万一出现泄露，或者被人倒卖，后果很严重。”李京担忧。

4、根治信息泄露顽疾还需跨过几座“山”

摘要：《经济参考报》记者调研了解到，当前，我国个人信息泄露呈现出“问题频出——公安打击——安全平稳期——问题再次复现”的往复循环的态势，个人信息泄露问题日趋常态化。几乎每个人都被信息泄露带来的问题困扰，信息泄露为何屡禁不止？接受记者采访的专家指出，根治顽疾还需跨过几座“山”，加大处罚力度的同时，亟须划定信息收集红线、强化制度震慑作用，加强重点领域立法补齐监管短板。



5、个人信息泄露，需冻结个人银行账户？ 小心了，这也是诈骗



摘要: 近日，深圳市公安局福田分局通心岭派出所接福田区反诈中心发来诈骗预警指令，在辖区内工作的王女士（化名）正在接听一个境外来电的疑似诈骗电话，时长近1个小时。接到指令后，民警多次拨打王女士手机，一直处于无法接通状态。

6、抓！男子泄露大量市民信息，民警立马闻风而动

摘要: 3月12号，孝感汉川市公安局城关水陆派出所接到一个新建小区内的多名业主反映：一家装修公司的业务员在同一段内向他们推销房屋装修业务，怀疑有人非法侵害公民个人信息。汉川市公安局城关水陆派出所副所长吴家维说：“侦查之后我们发现，其中小区居民接到的有几个电话都是同一家装修公司打出来的，最后我们对这个装修公司进行了突击检查，在现场查获了电子公民信息数据信息，和纸质的公民信息，超过五千多条。”



7、上海多家“失联”网贷平台用户信息被泄露， 还完贷款却被恶意骚扰

摘要: 近日，多名已经还完贷款的用户进行求助，而求助的原因是他们最近一直被自称为“蓝领贷”的网贷平台委外第三方催收公司恶意骚扰，关键是，关于“蓝领贷”这个网贷平台很多人都不知道，甚至于连“蓝领贷”这样网贷平台名字他们也是第一次听说。那么问题就来了，这些已经偿还完P2P平台贷款的用户个人信息被这些“身份不明”的人非法获取。



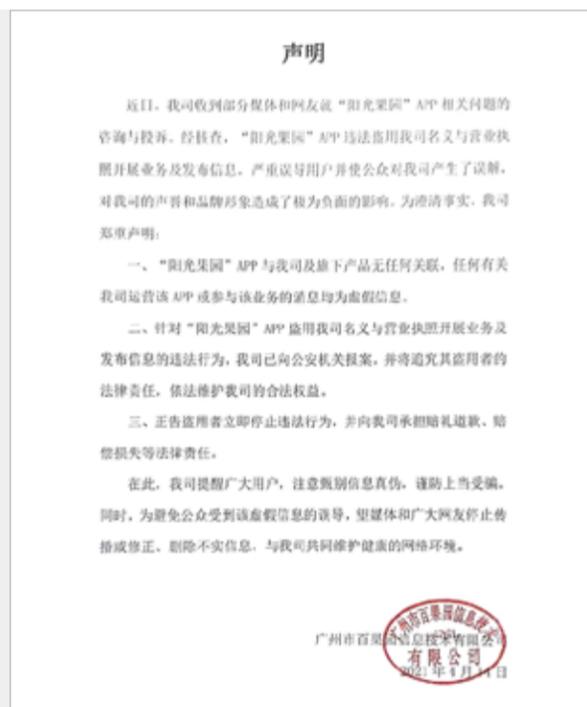
8、广东珠海一中小学生的信息，被泄露“十万” 余条，律师：侵犯信息罪



摘要: 近日，珠海网警在净网二零二一专项行动中发现，珠海某教育培训中心在推广课程时能精准说出学生的个人信息。据了解，该教育培训中心董事长石某某经中间人林某某介绍，认识了一家负责维护校讯通系统的信息技术有限公司员工徐某某，通过徐某某获得校讯通系统中的数据，用于推广公司的培训课程。

9、阳光果园 App 违法盗用的背后是信息泄露及杀猪盘的套路

摘要：近日，多家媒体收到消费者投诉称，“阳光果园”App 登录不上，涉嫌携款跑路。据用户反映，阳光果园客服提供的营业执照显示，平台主体运营公司为广州市百果园信息技术有限公司。记者致电广州市百果园，答复如下：“阳光果园”APP 违法盗用“广州市百果园信息技术有限公司”名义与营业执照，故意误导用户。同时，广州市百果园信息技术有限公司已向公安机关报案，并将追究其盗用者的法律责任。



10、你用的券商 APP 还安全吗？华泰证券被投诉泄露用户个人信息

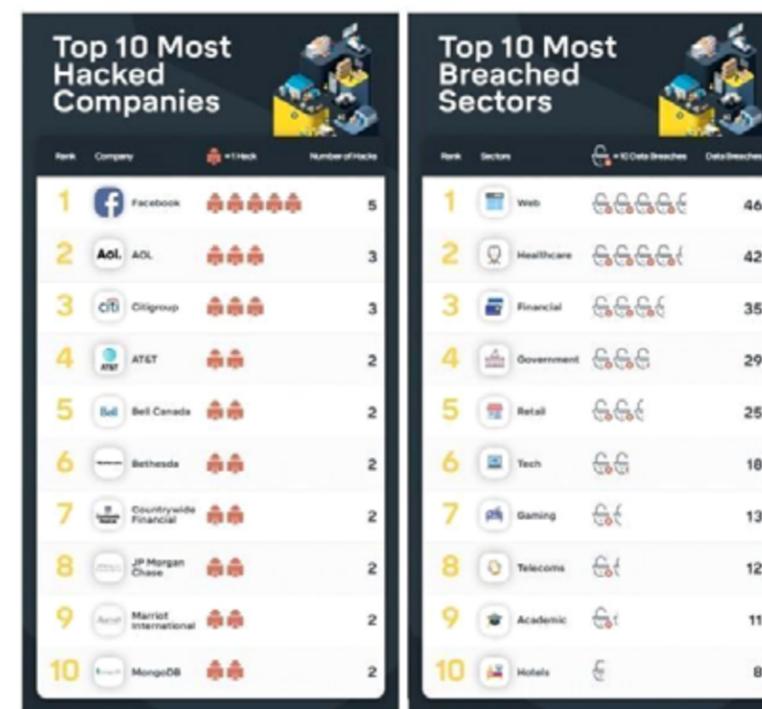


摘要：有投资者对华泰证券泄露个人信息现象进行投诉。该用户表示：“我于 2020 年在华泰证券开户后，就有自称是华泰证券的客户给我打电话拉我进群，我明确说过‘我不需要进入任何投资交流群’。但是近年骚扰电话变本加厉，本周已经 2 个了，严重影响了我的个人生活。希望网信办能彻查‘华泰证券泄露客户隐私’问题，同时查封这两个手机号，不要让更多人上当受骗。”截至目前，该投诉已由聚投诉平台通过邮件转达至华泰证券。

1、隐私信息“裸奔”泄露规模呈“指数级”增长：数十亿条个人信息明码标价

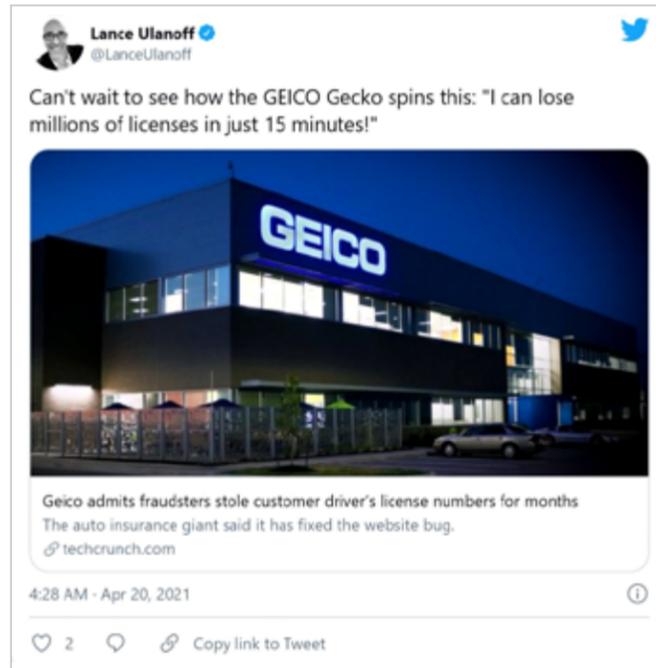
摘要：近期，某记者在 Telegram 上一个名为“社工机器人 & 闲鱼担保交易查档数据某认证群”的社交群上看到，大量的包括户籍、手机号、定位、查人查档、财产调查、开房记录、流水等在内的用户信息被公开售卖，十分猖獗。

2、Facebook 高居数据泄露事件最多公司榜首



摘要：据外媒，软件公司 Intact 对公开数据进行了分析，对过去 16 年里的数据泄露事件进行了统计和分析，Facebook 以最多的数据泄露事件和最多的记录丢失事故位居榜首，根据统计结果，Facebook 在报道期内遭遇了 5 起违规事件，丢失了 86.45 万条记录。其次是万豪国际（505200000 条）、MongoDB（477000000 条）、美国在线（92000000 条）和摩根大通（78600000 条）。

3、美第二大汽车保险公司遭遇数据泄露事故：持续一个多月时间



摘要：据外媒报道，美国第二大汽车保险公司 Geico 最近遭遇了数据泄露事故。Geico 在提交给美加州总检察长办公室的一份通知中披露，今年 1 月 21 日至 3 月 1 日期间公司内部发生了一起安全事故。不幸的是，这个持续了一个多月的漏洞似乎暴露了一些 Geico 客户的驾照号码，但数量不详。

4、俄专家：世界金融部门个人数据泄露的三分之一发生在俄罗斯



摘要：4 月 13 日消息，国际警察协会俄罗斯分会会长尤里·日丹诺夫对俄新社表示，2020 年全球银行、金融和保险公司个人数据泄露的三分之一以上发生在俄罗斯。

5、爱尔兰将调查脸书用户数据泄露事件 或违反 GDPR 多项规定



摘要：当地时间 4 月 14 日，爱尔兰数据保护委员会（DPC）正式宣布，将就 5.33 亿 Facebook 用户数据遭泄露一事展开调查。爱尔兰 DPC 认为，Facebook 可能违反了欧盟《通用数据保护条例》（GDPR）中的一项或多项规定。

6、音频社交平台 Clubhouse CEO 否认有 130 万用户信息被泄露的报道



摘要：据美国科技媒体网站 The Verge 报道，美国音频社交软件 Clubhouse 首席执行官保罗·戴维森（Paul Davison）周日表示，此前那份声称该平台个人用户数据被泄露的报告是“错误的”。此前 Cyber News 报道说，CH 的一个包含用户 ID、姓名、用户名、Twitter 和 Instagram 账号以及粉丝数量的 SQL 数据库被发布到了一个在线黑客论坛上。根据此报道，这些数据可以帮助不法分子针对用户发起钓鱼攻击或身份盗窃，不过信用卡号码等敏感用户信息似乎并不在泄露信息之列。

7、外汇经纪商 FBS 泄露数百万客户数据，潜在风险巨大



摘要：零售外汇及差价合约经纪商 FBS 错误地配置云数据库之后，意外地泄露了超过 20TB 的客户敏感数据。据悉，该数据库包含超过 160 亿条记录，泄露了数百万客户的个人身份信息（包括姓名、密码、电子邮件地址、护照号码、居民 ID、ID 验证扫描、信用卡、水电费账单、金融交易记录等）。

8、警惕！澳洲知名大学现大规模信息泄漏，老师学生姓名、邮箱等全外泄！



摘要：近日，墨尔本一所知名大学被迫道歉，成千上万的员工和学生的个人信息因数据泄露而被分享到了网上。星期五的 Swinburne University 透露了 5200 名员工、100 名学生和 200 个外部的其他人在互联网论坛上提供他们的个人信息。它上个月内发布了这些人的详细信息，包括名字和姓氏，电子邮件地址，甚至联系电话号码。数据漏洞链接到历史活动注册网页，其中来自 2013 年至 2014 年提供的信息。

9、注意自查！新加坡 9 万人隐私疑遭泄露，包括身份证银行卡号



摘要：周五（4月9日），新加坡策安（Certis）集团发声明称，客服邮箱账号遭到恶意攻击，约有 62000 封邮件内容因此疑似遭到外泄，其中有 1.2% 的邮件涉及财务等非常重要的信息。

10、AirDrop 存在漏洞？黑客简单破解就可以获得用户信息？



摘要：网上爆出 iPhone 手机上的 AirDrop 功能可能会泄露用户的电话号码以及电邮地址情况。据悉，iPhone 手机上的 AirDrop 功能开启之后，黑客只要待在距离目标 iPhone 非常近的范围就能获得一张公开分享表，用户的个人信息就会泄露。虽然 AirDrop 为了确定对方是不是已知联络人，会利用一种双向机制来对比双方的电话号码以及电邮地址，但是黑客只要使用简单的技巧就可以快速破解，从而得到用户信息。所以，研究人员认为这个漏洞非常严重，很大程度上造成了隐私泄露，这对于安全性极高的 iPhone 机来说，无疑是一个大漏洞。

《中国网络安全行业全景图 (2021.03 版)》发布，亿赛通九大细分领域强势上榜



3月底，中国网络安全行业专业且具影响力的媒体“安全牛”正式发布《中国网络安全行业全景图（2021.03版）》。亿赛通强势入选数据库安全、数据脱敏、数据防泄露、数据安全管控平台、文档安全、数据安全评估、邮件安全、视频监控安全、勒索软件防护等九大细分领域，并在多款产品中位居前列，数据安全市场一路领跑！

数据安全 | 物联网安全 | 业务与应用安全



亿赛通专业产品霸榜刷屏

本次全景图调研共收到 376 家安全厂商（服务商）申报。为更加科学、规范、全面地展现当前我国网络安全产业的发展状况和企业能力，安全牛对全景图分类进行了优化调整，共分为 14 项一级安全分类，106 项二级细分领域，是甲方用户、安全厂商、投资机构和业界人士共同快速了解产业生态格局、趋势和投资机会的“清明上河图”。

本次全景图的收录产品均需企业自主研发，具备一定特色和技术优势，并且产品要经过实际应用验证，有成熟的市场应用。同时，随着安全行业快速发展，申报安全牛全景图报告细分领域的厂商数量也在快速增长。亿赛通入选全景图，更是充分的说明了亿赛通在业内多年扎根深垦、发展提升自我的能力和魄力，及产品服务的优势。业界一致认可和肯定，是对亿赛通技术实力的最佳见证。

一直以来，亿赛通专注于数据安全领域的深入探索和研究。在数据安全领域中，亿赛通区别于传统数据安全厂商，为客户提供量身定制的数据安全解决方案，用专业化、智能化的产品，帮助客户随时掌控数据资产动态，缓解企业安全风险。同时，公司自主研发的多项产品均已得到广泛推广和应用。未来，亿赛通还将持续为用户提供创新、专业的数据安全解决方案。



实力认证 | 亿赛通强势登榜《CCSIP 2021 中国网络安全产业全景图》



近日，亿赛通数据安全产品成功入选 FreeBuf 《CCSIP 2021 中国网络安全产业全景图》榜单。FreeBuf 是国内领先的网络安全行业门户，发布专业的安全资讯、技术剖析，分享国内外安全资源与行业洞见，是深受安全从业者与爱好者关注的网络安全网站与社区。

本次亿赛通数据安全产品同时入选 FreeBuf 《CCSIP 2021 中国网络安全产业全景图》的四大分类七项细分领域：邮件安全、数据脱敏、数据防泄漏 DLP、数据库安全、勒索软件防护、安全咨询与培训教育、移动终端管理。作为数据安全领域近 20 年的践行者，亿赛通通过自主创新的数据安全产品，对企业核心数据的全生命周期进行有效管理，提供严密的全面防护，已经成功与数万家企事业单位牵手，帮助

企业筑牢数据安全防线。

具体入围领域如下：

01、数据安全



02、网络基础安全



03、移动安全



04、安全服务



现如今，各种内部威胁、外部威胁、恶意程序，以及各种业务安全场景，如薅羊毛、虚假交易、撞库等安全事件频发，很多企业缺乏足够专业的团队和资源去应对，也没有一套快速、标准、流程化地联动各个部门或资源针对威胁采取有效应对措施的系统。

与此同时，政府对数据安全的要求越来越严格，数据安全法、安全等保、行业监管、企业审计等对企业的业务环境要求越来越高。面对安全运营的新形势，亿赛通全新提出“分放管服”数据安全建设理念，配合设计咨询服务、产品方案、工程交付及售后服务四大体系，根据云、网、端三类应用场景对产品线进行扩充，实现数据安全理念建设的可落地执行，从不同维度为用户提供产品和服务，形成一体化智能管理，打造数据安全领域真正意义上的综合解决方案。

当前企业面临日益严重的数据安全治理问题，安全体系建设迎来巨大挑战，亿赛通数据安全全系列产品着眼于数据安全刚需及合规性需求，实现数据全生命周期的安全管控，实现涉密信息、个人信息和重要数据的有效保护。此次入选 FreeBuf 《CCSIP 2021 中国网络安全产业全景图》，是对亿赛通在数据安全相关领域创新和技术实力的又一次认可。未来，亿赛通还将继续深挖数据安全创新技术，以领先的国产数据安全产品保障用户数据资产安全，让数据安全更加高效。

亿赛通数据安全产品与飞腾完成产品兼容认证，信创生态再进一步

随着国家构建安全可信信息技术产业战略布局的全面展开，信息技术应用创新产业发展已经进入快车道，赢得市场的首要因素是生态，即国产软硬件之间的融合问题。亿赛通积极与产业上下游合作伙伴展开适配测试，扩大产品的适配范围，促进信创产业生态共同发展！

近日，北京亿赛通科技发展有限公司（简称“亿赛通”）电子文档安全管理系统与飞腾信息技术有限公司（简称“飞腾”）旗下的 FT-1500A/4、FT-1500A/16 和 FT-2000/4 三款处理器完成产品兼容性互认证。经双方联合测试，亿赛通产品与飞腾处理器良好兼容，系统功能稳定运行。



关于飞腾

• 飞腾公司是国内领先的自主核心芯片提供商，致力于飞腾系列国产高性能、低功耗通用计算微处理器的设计研发和产业化推广，坚持“核心技术自主创新，产业生态开放联合”的发展理念，联合众多国产软硬件生态厂商，提供基于国际主流技术标准、中国自主先进的全国产信息系统整体解决方案，支撑国家信息安全和重要工业安全。

• 基于飞腾 CPU 的整机产品覆盖多种类型的终端（台式机、一体机、便携机、受客户机等）、服务器和工业控制嵌入式产品等，在国内政务办公、云计算、大数据以及金融、能源、通信、人工智能和交通等行业信息系统领域已实现批量应用。

亿赛通作为国内领先的综合数据安全服务商，近二十年发展过程中持续进行技术创新和研发投入，创新提出并落地实践“分·放·管·服”数据安全建设理念，聚焦数据，通过制度主建，技术主战，分放管服，将数据实现分权分责分风险，放管结合，做到要素服务保支撑，持续安全可运营，确保数据有价值的流转，共赢数据安全大生态。

当前，我国信创产业的发展持续加速，亿赛通将继续利用自身优势，积极参与到信创产业生态共建的行动中，与生态伙伴合力，持续助力信创产业加速落地。

此次与飞腾处理器的兼容互认顺利完成，是亿赛通在国产化信息安全上高度重视的体现，标志着亿赛通国产化生态建设步伐再次加速，充分展示了国产信息化生态的协同发展与日臻完善，共同为国家的信息安全提供安全可靠、自主可控的技术支撑。

未来，双方将深化合作，加速实现产品融合、助力国产化信息化生态建设，紧跟数字化转型这一历史机遇，为更多客户提供安全、可靠的服务！

目前，亿赛通全线产品已与统信软件、中国电子、达梦数据库等在内的多家企业完成产品兼容性互认证，未来将与更多合作伙伴开展深度合作，携手推动国产化生态建设。

安全牛—亿赛通和太平洋财险签订战略合作协议，共同推出网络安全保险服务



4月21日，中国太平洋财产保险股份有限公司（以下简称太平洋财险）和北京亿赛通科技发展有限公司（以下简称亿赛通）签订战略合作协议，共同推出太平洋财险亿赛通网络安全保险服务。

本次会议中，太平洋财险网安险项目负责人刘愉对太平洋财险亿赛通网络安全保险服务进行了详细介绍。这是一项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。亿赛通总经理崔培升和CTO朱贺军分别介绍了企业战略合作方针和“文件防火墙”这一防勒索产品。最后双方共同签署了太平洋财险亿赛通网络安全保险服务战略合作协议。本次战略协议签署，是网络安全行业与保险行业跨界浓墨重彩的一笔，是网络安全保险领域的一大前进。



网络安全保险是近年来网络安全的新兴领域，作为金融市场和网络安全行业的新宠，获得了业界的关注。但目前涉足其中的网络安全企业和保险企业均较少，且深度不足。同时，在经济利益的驱动下，勒索病毒成为近年来的主流网络安全威胁之一。由于企业信息化架构基础简单且信息资产大多为核心资产，在受到勒索攻击后，会严重影响日常业务开展。并且企业缺乏专职安全团队，在应对勒索攻击时，没有事件应急响应能力，导致其错过最佳处理时间，加重了不利影响。面对监管合规要求提高、安全风险激增等问题，网络安全保险服务成为企业增强内部保障能力的重要服务。网络安全保险的出现正好填补了保险在网络安全领域的空白。

在对太平洋财险负责人刘愉女士的采访中得知，太平洋财险是布局网络安全保险的保险企业中的佼佼者，目前已在数据安全、身份安全等领域推出保险服务。本次太平洋财险亿赛通网络安全保险服务，结合太平洋财险在保险领域的专业性以及亿赛通在数据安全领域的技术先进性，为广大的金融、政府、智能制造行业的投保单位提供财产保障。

据了解，太平洋财险亿赛通网络安全保险服务包括保前安全检测、保中风险预警以及保后应急响应。亿赛通文件防

火墙是一款基于内核的勒索病毒防护产品，能够对企业核心数据特别是指定的核心文件进行防护。太平洋财险充分借助亿赛通在数据安全、防勒索等领域的优势，有专业数据安全产品的支撑，太平洋财险在精准获客方面优化保险产品和运营模式，进一步拓展网络安全保险生态链，提升客户体验，承担保险发展使命。

随着越来越多人认识到数据的价值，数据安全将是近几年网络安全的热点。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最佳选择。亿赛通的文件防火墙将为企业勒索软件防护提供第一道屏障，减少企业被勒索的风险；太平洋财险的保险服务将为企业勒索软件防护守好最后一道大门，将企业的勒索损失减到最低。太平洋财险和亿赛通的强强联合，将聚力创新资源，形成发展合力，提供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。

文章来源于安全牛

数世咨询—网络安全保险新军 亿赛通与太平洋财产保险合作签约

4月21日，数据安全厂商亿赛通与太平洋财产保险宣布在网络安全保险项目达成战略合作，并于当天举行了签约仪式。

网络安全保险业务在国际市场上已经处于快速发展的阶段，据市场研究机构 Markets and Markets 发布的统计报告显示，2020年的网络保险费用已达78亿美元，并预计将在2025年增长到204亿美元，年复合增长率21%。

国内市场上的各大保险公司近几年来也在纷纷关注网络安全保险，并与多家网络安全厂商合作，开始涉入这项数字经济带来的新兴保险业务。据数世咨询统计，目前的网络安全保险市场规模接近3亿元。



数世咨询认为，网络安全保险业务的主要挑战有二：

一是保险范围的确定：网络安全涉及的范围很广，如网络运行的保障，内外部商业间谍行为，数据资产的损失，黑客攻击造成的业务损失，以及涉及到的企业声誉、监管罚金等间接损失。因此，没有一个清晰的保险范围划分，无法有效的开展保险业务。

二是保险意识不足：社会各行各业，已经开始接受传统的人身、财产保险业务，但对这种数字经济环境下的新兴保险业务普遍缺乏认知。这里面有着多种因素，如许多机构对网络攻击的认识不足，还有人认为即使发生安全事件损失也可控制，更大的一个背景是国内普遍重业务轻安全的思维惯性并未发生根本性转变。

另据太平洋财产保险网络安全险项目负责人刘愉介绍，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。“这是一个盲点，需要保险公司和业界一起解决。”

针对以上挑战，太平洋财产保险和亿赛通给出了他们的联合解决方案：

首先是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。

再者，刘愉表示，本次与亿赛通合作的网络安全保单“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。



最后，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。此次推出的“防勒索数据安全险”的优势有四个方面，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。

亿赛通总经理崔培升表示，全球范围勒索病毒现象严重，据《2019威胁态势分析》报告显示，中国勒索病毒的数量居全球榜首，造成业务停摆，声誉下降，且恢复成本巨大。因此，此次的合作以防勒索数据安全险为切入点，未来还将推出更多的网络安全保险项目，为客户带来价值为社会做出贡献。

数世点评：

经过几年来的试水，国内已经摸索出基本的网络保险思路。即“安全服务+安全工具+安全保险”的模式。客户方面，可以避免或减少损失。同时，保险公司和安全公司也可共同丰富彼此的业务模式和业务渠道。而保险机构在寻求安全企业的合作伙伴时，最为看重可靠性、安全能力，以及企业级市场的资源，这也是太平洋财产保险选择亿赛通作为合作伙伴的关键原因。

文章来源于数世咨询

从热播剧了解网络安全



作为资深追剧党，小编这段时间沉迷剧情无法自拔，有木有和小编一样，对这部剧欲罢不能的同学，没错，这就是《暴风眼》。该剧在热播期间，引起讨论狂潮！这部电视剧为何可以得到，如此高的讨论度与关注度？让我们一起来看！

“这个世界，这个时代，几乎每时每刻都在延续着没有硝烟的战争，有人决绝地捍卫正义，也有人跌落罪恶的深渊。当你正安享这一切风平浪静的时候，很有可能，你就站在暴风的中央”。

随着电视剧的热播，剧情围绕国际商业间谍展开，牵扯出一系列盗取企业保密技术的间谍案。也许有小伙伴觉得不可思议：商业间谍居然需要发动国安部门？殊不知早在十几年前就有商业间谍给国家带来巨大经济损失，甚至影响国际关系。

追剧时，除了各种高科技手段的使用及各种高明的反侦察技巧，在让人直呼大开眼界的同时，也是在提醒我们：机密可能在不经意间就会被泄露，网络安全的保护比我们想象的还要艰难。

最近几年，有关网络攻击，黑客攻击导致的重要信息泄露，数据丢失等事件频频发生，所以在网络安全形势的严峻下，国家也在重点关注网络安全问题，培养大家的网络安全意识是重中之重。

黑客攻击主要是对服务器的攻击，漏洞发现，植入病毒等。如果我们的移动端，PC端，服务器被攻击了或者是被植入病毒、木马、出现漏洞等，那么会出现什么问题呢？

- 企业敏感信息（如：身份信息、账户名称、银行账户、银行密码等）被窃取或者监视用来贩卖；
- 黑客利用漏洞或者木马病毒远程控制服务端设备，将企业重要的数据文件删除、新建、修改、上传、下载等一系列操作；
- 黑客通过邮件方式带有病毒链接打开时自动被植入控制系统操作，让其设备沦为僵尸主机，打不开等。

亿赛通在为企业服务中，发现企业对于网络安全意识重视程度不同，网络安全意识不是一朝一夕能够转变的，需要贯穿到每一位企业员工，上到领导下到员工。员工的

网络安全意识提高，企业所面临的网络安全风险仍才有可能降低。亿赛通在安全领域注重从源头解决企业困扰，专业程度有目共睹，独家首推的“分放管服”数据安全建设理念，经过多家企业的实施体验，均得到高度认可。

近几年，越来越多的电视剧关注网络安全，其最重要的一点就是要宣传网络安全意识，用更年轻化的包装和更好的故事反映当下生活，用大众能理解的表达方式折射时代进程。所以亿赛通最后提醒大家加强网络安全意识，提高识别防范能力，掌握网络安全技能，维护网络的安全！

震撼场面，多家行业巨头遭遇数据泄露，数据安全曲突徙薪

大数据时代，我们的数据信息，被各大公司奉若至宝，各位巨头爸爸们想尽办法把你“扒的干干净净”。近日，多家行业巨头数据库遭受重击……

新加坡最大保安集团泄露数万人隐私信息

新加坡策安（Certis）集团发声明称，客服邮箱账号遭到恶意攻击，约有62000封邮件内容因此疑似遭到外泄，其中有1.2%的邮件涉及财务等非常重要的信息。

策安集团是新加坡最大的私人保安公司。声明表示，本次信息泄露发生在3月中旬。3月16日至3月17日，多人反映收到了策安集团客户服务部门电邮帐号发出的恶意邮件。另外，还有多人收到了包括策安集团信息在内的包裹查询邮件，其中含有诈骗链接。



社交媒体 Clubhouse 130 万用户信息被泄露

社交媒体平台 Clubhouse 发生数据泄露事件，一个包含130万用户个人信息的数据库正在一个人气黑客论坛上免费流传。

遭泄露的用户信息包括用户名、姓名、照片、Twitter 以及 Instagram 关联账户等。Cybernews 表示，尽管被泄露的数据并没有像信用卡信息一类敏感的资料信息，但仍然有被不法分子利用从而进行针对性的网络钓鱼的风险。



5 亿 LinkedIn 用户的数据遭泄露

社区 LinkedIn 领英的数据也遭到泄露，一个宣称包含爬取了5亿条 LinkedIn 个人资料的数据包放在黑客网站上进行出售，良心的卖家还免费赠送了两百万条数据以供查验。

泄露的数据中包含 LinkedIn 用户的信息，包括其全名，电子邮件地址，电话号码，工作场所信息等。根据黑客提供的数据示例来看，数据来源是爬虫。



黑客一般会通过多种手段来利用泄露的数据，掌握了这些信息后，他们可以发起更令受害者相信的网络钓鱼和攻击，甚至对那些已经在黑客论坛上公开过信息的人进行身份盗用。

事实上，在国际的相关法律法规中，早已规定数据泄露的合规要求及惩罚措施。然而，法律已明确了相关原则，为什么还会发生数据泄露事件？问题的关键，在于企业的数据并未得到严格防护。而且，当数据被“晒出来”的错误发生后，仍无人对此亡羊补牢、进行及时的自我纠错。

更重要的是，企业未树立起数据保护意识，对敏感信息的界定和重要性的认知还很模糊，导致在工作疏忽发生数据泄露。企业作为数据的保护者，不仅应身体力行，严格执行遵守数据安全防护的规章制度，更应以身作则，在数据安全防护上率先垂范，充分利用法律武器、利用现代化管理工具，随时随地保护核心数据。

亿赛通——中国数据安全专家，肩负国家数据安全、企业数据安全、个人数据安全的保护使命，为您提供全面而周到的安全服务。

聚焦政策法规，数据安全行业喜迎全新局面



随着信息技术和人类生产生活交汇融合，各类数据迅猛增长、海量聚集，对经济发展、社会治理、人民生活都产生了重大而深刻的影响。数据安全已成为事关国家安全与经济社会发展的重大问题。

中央推动法规定制

按照党中央的部署规划，2020年起草了数据安全法草案并发布意见征询。近日，全国人大常委会法制工作委员会举行记者会，发言人介绍立法工作有关情况并回答记者提问。常委会经过会议讨论对数据安全法草案及个人信息保护法草案进行了初次审议。根据各方面意见，对草案二次审议稿做出几点修改。

数据安全法草案

1. 对草案中的数据安全等用语的含义予以完善。
2. 完善数据分级分类和重要数据保护制度。
3. 充实数据出境安全管理规定。

个人信息保护法草案

- 针对当前个人信息过度收集使用等突出问题，完善个人信息处理应遵循的原则。
- 完善、充实合法处理个人信息的情形、撤回同意、自动化决策、跨境提供个人信息等方面的规则。
- 增加死者个人信息保护的规定。
- 明确国家网信部门统筹推进个人信息保护工作的有关职责。
- 与民法典有关规定相衔接，完善侵害个人信息权益的民事法律责任。

记者会现场，针对个人信息收集乱象问题，发言人回应：个人信息保护事关人民群众的切身利益。2020年10月提请全国人大常委会初次审议的个人信息保护法草案，针对当前个人信息保护领域存在的突出问题，在有关法律的基础上进一步完善相关制度规范：

1. 确立个人信息处理应遵循的原则，强调处理个人信息应当采用合法、正当的方式，具有明确、合理的目的，限于实现处理目的的最小范围，公开处理规则，采取必要的安全保障措施等，这些原则应当贯穿于个人信息处理活动的全过程各环节。

2. 确立以“告知—同意”为核心的个人信息处理一系列规则，要求处理个人信息应在事先充分告知的前提下取得个人同意，不得以个人不同意为由拒绝提供产品或者服务。

3. 设专节对处理敏感个人信息作出更严格的限制，只有在具有特定目的和充分必要性的情形下，方可处理敏感个人信息，并应取得个人的单独同意或书面同意，在事前进行风险评估。

4. 明确个人在个人信息处理活动中的各项权利，包括知情权、决定权、查询权、更正权、删除权等，强化个人信息处理者合规管理和保障个人信息安全的义务。

5. 设置严格的行政、民事法律责任。

响应国家政策，亿赛通蓄势待发

上述法律规范以保护个人信息权益为核心，以严格规制个人信息处理活动为重点，将为防范和遏制违法收集、使用个人信息行为提供强有力的法律保障。亿赛通作为综合数据安全厂商，近二十年发展中，一步步稳扎稳打，先后共计积累客户数万家，服务实施终端用户六百多万，已成为在数据安全产业里的先头翘楚，在国家安全政策春风的沐浴下，为各行各业的数据安全体系建设做好充分准备。

中国人民财产保险股份有限公司



客户简介

中国人民财产保险股份有限公司（简称“中国人保财险”），是“世界500强”中国人民保险集团股份有限公司（PICC）的核心成员和标志性主业。中国人保财险与共和国同龄，在与国家共同成长的历程中，始终践行“人民保险 服务人民”的历史使命，积极投身于“保障人民高品质生活”的崇高事业，以“做人民满意的保险公司”为共同愿景，秉承“风雨同行 至爱至诚”的核心价值观，坚持以市场为导向、以客户为中心，积极履行优秀企业公民责任，为经济发展、社会稳定、国家强盛、人民幸福提供了强大的保险保障。

需求背景

信息系统安全是中国人保财险持续稳定发展的重要基础。因此为防范化解保险公司信息系统安全风险，完善信息系统安全保障体系，确保信息系统安全、稳定运行，保护信息在采集、传输、交换、处理和存储等过程中的可用性、保密性、完整性和不可抵赖性，中国人民财产保险股份有限公司联手亿赛通共同打造信息安全运行的高效工作环境。

解决方案

亿赛通文档安全是以数据透明加密技术为核心，通过信息安全边界建立，降低核心信息资产的有意或无意泄密风险。

智能透明加密：采用第四代VFS技术，实现对任意文档自动透明加密。不改变和影响用户使用系统和工作效率。

智能半透明加密：可实现对本地文档不影响情况下，无障碍使用密文文档，对本地敏感文档可手动加密。

内容安全防护：防止核心数据通过复制拖拽、截屏录制、打印输出、副本另存等方式泄密。

离线办公支持：系统提供安全离线办公业务支持，通过离线审核、策略预设及离线补时等功能满足各类离线办公要求。

端口安全管控：可对软驱、光驱、串口、并口、pcmcia、红外设备、1394火线、wifi接口、蓝牙设备、调制解调器、usb移动存储设备端口进行管控，防止核心数据通过外设端口泄密。

细粒权限控制：不仅可细化设置文档的阅读、编辑、复制、打印等组合权限，还可根据管理需要设定文档生命周期，同时提供灵活的二次授权管理、归档管理、交接管理及版本变更管理等功能。

项目成果

中国人保财险通过部署亿赛通文档安全产品，有效的抵御了来自企业内部或者外部的各种数据泄露可能，并且为其构建了完善的数据安全管理体系，提高了工作效率，增强了员工的数据保护意识。

深圳市慧择保险经纪有限公司



客户简介

深圳市慧择保险经纪有限公司 2006 年正式成立，是经保监会早期批准获得保险网销资格的网站之一；是第三方互联网保险服务平台的创立者。经过 13 年的发展，慧择网已与 80 余家保险公司合作，提供近千款保险产品服务，产品线涵盖了健康险、人寿险、意外险、旅游险、企业险等全险种产品，服务用户超过 3000 万。

需求背景

在互联网保险运作的新趋势下，慧择网业务亦向互联网发展，产生大量的核心技术、专利、重要客户信息以及财务数据等方面的电子文档。为提高企业内部数据协同和高效运作，防止一切人为或非人为风险，实现内部文档的流转安全可控，实现文档脱离内部管理平台后能有效防止文件的扩散和外泄，因此慧择网必须加强信息安全管理。

解决方案

- 1、统一身份认证：**支持同时同步深圳总部的 AD 域及合肥分公司 AD 域；
- 2、透明加密：**对慧择网公司的源代码、办公软件等做透明加密保护；
- 3、业务系统集成：**与慧择网的各种应用系统无缝集成，实现数据的上传解密、下载加密功能；
- 4、半透明加密：**特殊岗位人员可自主选择是否加密，对公司核心部门加密文档可正常使用；
- 5、流程审批：**对于普通员工采用流程审批解密，特殊岗位人员及高层领导分配右键特权解密功能；

6、支持手机 APP：高层领导安装手机客户端，一方面方便审批解密文档，另一方面可直接在手机上查看加密办公文档；

7、支持 MAC 端：部分高层领导使用 MAC 系统，主要是保护办公核心文件；

8、文件外发安全：对于机密文件制作外发加密文件，根据文件安全程度及外部用户可信程度设置权限，可控制是否只读、时间、次数、是否可打印等权限控制，打开认证方式可采用密码、机器码绑定、KEY 认证等方式，从而保证外发出去的文档安全控制。

项目成果

项目的成功实施大力保障了深圳市慧择保险经纪有限公司代码、财务数据、客户信息等核心数据安全；保障深圳总部跟分部合肥分公司数据交互安全，建立信息安全边界，有效防止企业核心信息资产外泄的同时，不影响用户工作习惯及业务效率，同时提高了员工的数据安全保护意识。