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

亿赛通企业月刊　　中国数据安全专家　　www.esafenet.com

3 月刊

2021 年共 11 期

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

我们心中的亿赛通

我们的祖国

今天已步入富强昌盛的时代

神州 960 万平方公里

到处都有国旗的飞扬

长城内外、大江南北

到处都可以看到中国人自豪的笑脸

到处都飞扬着激昂的歌声

中国的实力

让世人刮目相看

同样　中国的企业

强大已不再是空谈

十八年青葱岁月

是从出生走向成年的标志时光

十八载青春年华

昭示着从青涩迈向成熟

今年，亿赛通十八岁了

十八个春夏秋冬 十八个寒来暑往

我们经历过风雨 沐浴过彩虹

我们品尝过成长的甜美

我们也有过停滞的彷徨

但是亿赛通依然执着向前，顽强生长

十八年春秋见证

多少企业风起云涌

又有多少企业销声匿迹

我们用充满竞争力的机制

为有理想的人搭建创业平台

摩天大楼不是在一天建成

企业的发展也不是朝发夕至

无边落木萧萧下

不尽长江滚滚来

让亿赛通未来的发展

来实践我们对安全的责任

让公司的未来见证我们的荣光

今天，我们相约亿赛通

让梦想指领我们未来

让励志之火照亮我们人生

今天，我们相约亿赛通

在平凡中实践理想

在平庸中追求高尚

相约亿赛通，我们奋斗过，努力过

相约亿赛通

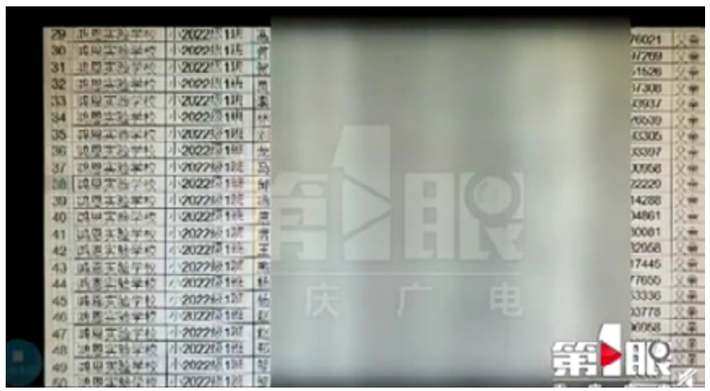
我们将继续为公司的未来　拼搏进取

用百倍的汗水　去创造真正属于自己的水木年华

刊首语 PREFACE

国内

1、培训机构老板爆内幕：学校老师卖家长信息！

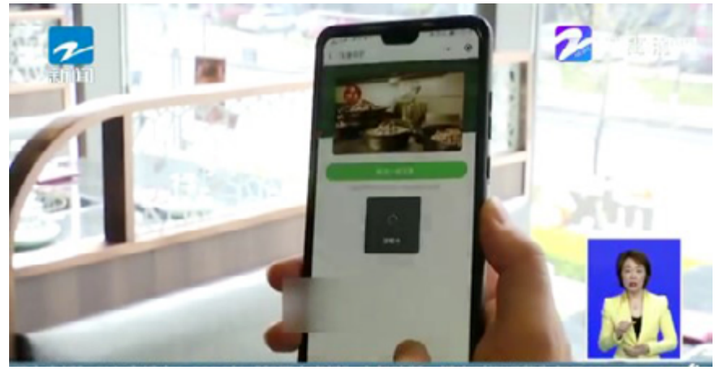


摘要：江北区一家培训机构的老板爆料，说他们花两千元，从一所学校购买了学生和家长的信息，并根据这些信息向家长推销课程。对于信息泄露原因，家长都很关注，江北区鸿恩实验学校却一直无回应，记者多次到学校采访也被拒。由于采访受阻，记者已经把新闻线索提供给警方和教委，事件在进一步调查中。

2、转！曝光！科勒卫浴人脸识别摄像头

摘要：科勒卫浴在全国上千家门店安装了具有人脸识别功能的摄像头，消费者只要进了其中一家店，在不知情的情况下，就会被摄像头抓取并自动生成编号，以后顾客再去哪家店，去了几次，科勒卫浴都会知道。人脸信息属于个人独有的生物识别信息，一旦泄露，将严重威胁用户的财产安全、隐私安全等。

3、扫码点单强制关注公众号涉嫌侵权；杭州整顿“强制关注”行为



摘要：你有过这样的经历吗？只想吃顿饭，却要关注公众号、注册会员。不管服务员忙不忙，就是让你扫码点餐，几顿饭下来，五花八门的公众号和推送来了一大堆。如今看似便利的“扫码点餐”，也正引发关于过度搜集顾客信息、是否存在信息泄露风险的讨论。

4、四川修订物业管理条例，不得强制业主“人脸识别”

摘要：24 日，《四川省物业管理条例（修订草案）》提请省十三届人大常委会第二十六次会议审议。明确了业主委员会及委员、候补委员和物业服务人等主体，不得泄露业主信息或者将业主信息用于与物业管理无关的活动；回应现实中个人生物信息滥用的社会热点问题，明确了物业服务人不得以强制业主通过指纹、人脸识别等生物信息的方式使用共用设施设备。

5、内鬼黑客狂卖个人信息“年产值”上千亿，人均至少被泄露 4 条

摘要：近期，证券时报记者深入多个数据交易千人 QQ 群发现，各行各业的用户隐私数据被肆意贩卖，触目惊心。不时有人在群里喊单，“出一手 GM（股民）、WD（网贷）、BJ（保健）信息，拼多多、淘宝、京东一手网购数据，需要数据的联系我……”这些数据按照行业划分被明码标价。甚至还有采集个人信息的系统展示，号称可以采集全国老板的私人联系方式。还有五花八门爬取数据的软件，“爬”上网站，“嵌”入 APP，“铲”下数据。

6、池子个人信息被泄露处罚结果公布 中信银行收 450 万罚单

摘要：3 月 19 日，中国银保监会下发第 5 号罚单，中信银行被处罚单 450 万元。罚单显示，中信银行的违法违规案由包括：

一、客户信息保护体制机制不健全；柜面非密查询客户账户明细缺乏规范、统一的业务操作流程与必要的内部控制措施，乱象整治自查不力。

二、客户信息收集环节管理不规范；客户数据访问控制管理不符合业务“必须知道”和“最小授权”原则；查询客户账户明细事由不真实；未经客户本人授权查询并向第三方提供其个人银行账户交易信息。

三、对客户敏感信息管理不善，致其流出至互联网；违规存储客户敏感信息。

四、系统权限管理存在漏洞，重要岗位及外包机构管理存在缺陷。

行政处罚决定书文号			银保监罚决字〔2021〕5号
被处罚当事人	单位	名称	中信银行股份有限公司
		法定代表人姓名	李庆萍
主要违法违规事实（案由）			一、客户信息保护体制机制不健全；柜面非密查询客户账户明细缺乏规范、统一的业务操作流程与必要的内部控制措施，乱象整治自查不力 二、客户信息收集环节管理不规范；客户数据访问控制管理不符合业务“必须知道”和“最小授权”原则；查询客户账户明细事由不真实；未经客户本人授权查询并向第三方提供其个人银行账户交易信息 三、对客户敏感信息管理不善，致其流出至互联网；违规存储客户敏感信息 四、系统权限管理存在漏洞，重要岗位及外包机构管理存在缺陷
行政处罚依据			《中华人民共和国银行业监督管理法》第二十一条、第四十六条和相关审慎经营规则 《中华人民共和国商业银行法》第七十三条
行政处罚决定			罚款450万元
作出处罚决定的机关名称			中国银行保险监督管理委员会
作出处罚决定的日期			2021年3月17日

7、万店掌创始人回应收集人脸信息

摘要：央视 3.15 晚会，多家知名企业被曝监控摄像头违规采集人脸信息，被点名的万店掌创始人周圣强回应，公司只是帮客户做分析以改善经营，相关数据不会泄露和保留。

8、青岛泄题事件一名嫌疑人已抓获

摘要：28 日，多名网友发文称，青岛市教师招考考试疑似发生泄题。当晚，@ 青岛教育微博 发布说明称，本次泄题事件涉及西海岸新区等六区市的教师招考考试，相关区市已迅速报警，同时向纪检监察部门通报情况。目前，公安部门已经介入。

9、青春有你 3 选手余景天信息泄露被恶意取消值机

摘要：29 日，《青春有你 3》一行 7 名练习生前往参与《王牌对王牌》节目录制，但有网友爆料称，选手余景天疑似被恶意取消值机，一行人中也只有他没能上飞机。

10、人脸信息“裸奔”引全民焦虑，李扬：对生物识别信息的保护应强于一般非敏感信息

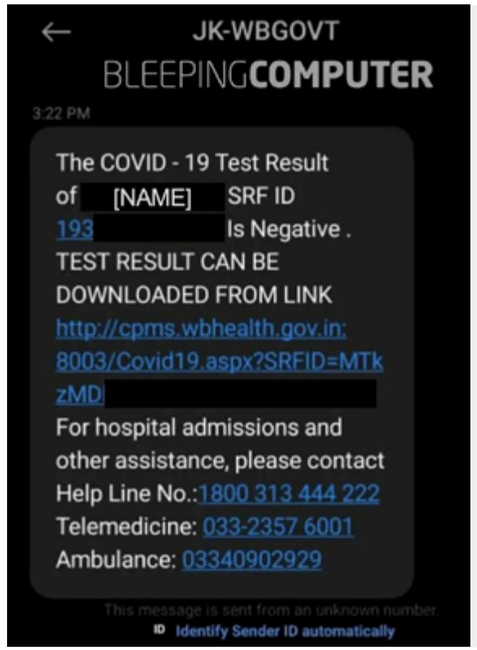
摘要：李扬教授指出，我国目前有关个人生物识别信息保护的规范相对较少。在李扬教授看来，可从多个维度展开。在保护对象上，应当界定个人生物识别的概念边界与法律属性。在保护强度上，对个人生物识别信息的保护强度应当强于一般非敏感个人信息。对其采集、使用应持更强的知情同意原则，坚持特别规制即差异化规制。在保护方式上，对个人生物识别信息应采取多元的保护机制。

国外

1、国家漏洞库 CNNVD：关于 F5 BIG-IP 多个安全漏洞的预警

序号	漏洞名称	漏洞编号	漏洞简介
1	F5 BIG-IP 安全漏洞	CNNVD-202103-770、CVE-2021-22986	该漏洞允许未经身份验证的攻击者通过BIG-IP管理界面和自身IP地址对iControl REST接口进行网络访问，以执行任意系统命令，创建或删除文件以及禁用服务。
2	F5 BIG-IP 安全漏洞	CNNVD-202103-772、CVE-2021-22987	当以设备模式运行时，该漏洞允许经过身份验证的用户通过BIG-IP管理端口或自身IP地址访问TMUI，以执行任意系统命令，创建或删除文件以及禁用服务。
3	F5 BIG-IP 安全漏洞	CNNVD-202103-784、CVE-2021-22991	流量管理微内核(Traffic Management Microkernel, TMM) URI 的规范化可能会错误地处理对虚拟服务器的请求，从而触发缓冲区溢出，导致拒绝服务攻击。在一定条件下，可能绕过基于URL的访问控制，造成远程代码执行。
4	F5 BIG-IP 安全漏洞	CNNVD-202103-781、CVE-2021-22992	在策略中配置了Login Page的Advanced WAF/ASM虚拟服务器在响应恶意HTTP时可能会触发缓冲区溢出，从而导致拒绝服务攻击。在一定条件下，可能造成远程代码执行。

摘要：近日，国家信息安全漏洞库（CNNVD）收到关于 F5 BIG-IP 多个安全漏洞情况的报送。包括 F5 BIG-IP 安全漏洞（CNNVD-202103-770、CVE-2021-22986）、F5 BIG-IP 安全漏洞（CNNVD-202103-772、CVE-2021-22987）等。攻击者可在未授权的情况下远程执行命令、创建或删除文件、开启或关闭服务等。



2、印度 800 万核酸检测结果泄露：网站漏洞过于低级

摘要：近日，印度西孟加拉邦卫生福利部被曝 800 万核酸检测结果报告泄露。而事实上，上月 BleepingComputer 就报道称多个印度政府网站泄露了病人的核酸检测报告。

3、2020 年针对大学的勒索软件攻击翻倍，赎金达 44.7 万美元

摘要：过去一年，针对大学的勒索软件攻击数量同比增加了一倍，随着信息安全团队抵御网络攻击，勒索软件的需求成本也在上升。通过对针对高等教育进行勒索软件活动的分析发现，与 2019 年相比，2020 年针对大学的攻击翻倍，平均赎金达到 44.7 万美元。

4、软件厂商未及时通报客户产品漏洞，全球百余家机构被黑

摘要：近期网络犯罪组织 FIN11 针对美国软件公司 Accellion 旗下文件共享产品 FTA 的大规模网络攻击，已导致美国华盛顿州审计署、新西兰储备银行、澳大利亚证券和投资委员会、新加坡电信巨头 Singtel 等近百家政企机构敏感数据泄露。

5、Clubhouse 音频数据遭泄露，引发安全性担忧

摘要：据报道，广受欢迎的音频聊天室应用 Clubhouse 曾表示将采取措施确保用户数据不会被恶意黑客或间谍窃取。然而现在，至少有一名网络攻击者证明了 Clubhous 平台的实时音频是可以被窃取的。

6、红杉资本遭钓鱼邮件攻击，投资者数据或泄露

摘要：红杉资本上周五告诉其投资者遭到黑客入侵，黑客使用的是 BEC（商业电子邮件欺诈）攻击，攻击者仿冒红杉员工向投资者发送电子邮件，可能已经访问了投资者的一些个人和财务信息。所谓 BEC 攻击，就是网络罪犯使用恶意账户来模仿员工或受信任的合作伙伴，并发送高度个性化的电子邮件，目的是诱使其他员工 / 客户 / 合作伙伴泄漏敏感信息或转账。

7、2020 年报告的漏洞数量创历史新高，高危漏洞占比达 57%

摘要：近日，根据美国国家标准与技术研究所收集的关于常见漏洞 (CVE) 的数据分析，2020 年全球的安全漏洞报告比以往任何一年都多。托管安全服务提供商 Redscan 的报告显示，2020 年报告了 18,103 个漏洞，其中大多数被列为高度严重级别，占比达 57.1%。实际上，2020 年披露的高严重性和严重漏洞数量超过了 2010 年披露的漏洞总数。

8、巴西一数据库发生重大数据泄露事件：几乎所有巴西人受波及

摘要：据外媒报道，当地时间周二上午，PSafe 的网络安全实验室 dfndr 报告称，巴西的一个数据库发生了一起重大泄密事件，数百万人的CPF 号码及其他机密信息可能遭到了泄露。据这些使用 AI 技术识别恶意链接和虚假新闻的专家们披露，泄露的数据包含有 1.04 亿辆汽车和约 4000 万家公司的详细信息，受影响的人员数量可能有 2.2 亿。

9、WhatsApp 因违反 GDPR 面临最高 5000 万欧元罚款

摘要：根据爱尔兰数据保护监管机构做出的初步判决，WhatsApp 因违反 GDPR 规定将面临最高 5000 万欧元（约合 4400 万英镑）的罚款。根据爱尔兰数据保护委员会（DPC）的调查结果，WhatsApp 未能正确告知欧盟用户其如何与 Facebook 共享数据，在透明性要求上未达标。该判决于 2020 年 12 月确定，然后发送给欧洲其他数据监管机构进行评估。

10、Facebook 被爆以往漏洞泄密，用户隐私信息被出售

摘要：据 Motherboard 报道，有人掌握了包含 Facebook 用户手机号码的数据库，正在使用 Telegram 机器人出售这些数据。安全研究人员 Alon Gal 表示，该机器人的运维人员掌握了 5.33 亿用户信息，信息来自 Facebook 的一个漏洞 (早在 2019 年修复)。

亿赛通各路牛人齐登场，年会 SHOW 出你的样

迎着初春的暖阳，伴着喜庆的氛围，年会或许会迟到，但绝对不会缺席。

亿赛通发展正当时

2020 年是亿赛通综合数据安全厂商的发展之年。在疫情的挑战下，我们仍取得了较满意的成绩。这一年，我们提出了全新的理念，细分了产品条线……这一年，亿赛通人把每一步都走得踏踏实实。

既然是年会，当然少不了颁奖典礼。今年的颁奖典礼有些“特殊”我们要对 2019 年及 2020 年，两年的优秀个人和团队进行表彰。这些工作突出的个人和团队，涵盖职能、研发、销售、宣传等各个部门……

2019 年度优秀新人 &2020 年度明日之星

2019 年度 &2020 年度优秀员工

2019 年度 &2020 年度优秀团队

2019 年度 &2020 年度服务之星

2019 年度 &2020 年度研发之星

2020 年度工程之星

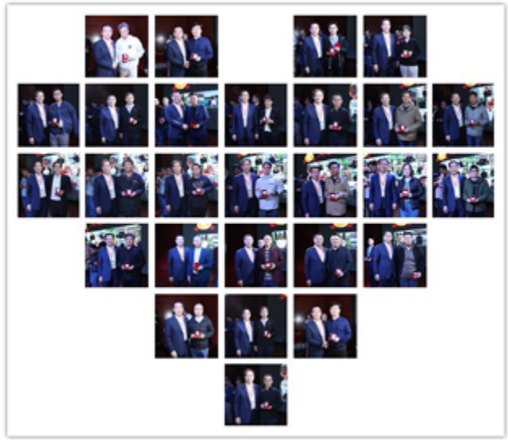
2019 年度销售之星 &2020 年度销售冠亚季军

2019 年度 &2020 年度管理之星

2019 年度 &2020 年度杰出团队

2020 年度重大项目奖

入职五年 & 十年员工感谢奖



年会重头戏——播下希望的种子

一年之计在于春，正值蓬勃朝气的春季，我们齐聚一堂，万众一心，整装待发，签订 2021 年公司全年任务书，开启新的征程！

言出必行，保证圆满完成任务

点亮我们心中的亿赛通

久负盛名的亿赛通天团们，十八般武艺样样皆“牛”。

除了同事们的热情表演，管理层还为大家带来了特别节目，《我们心中的亿赛通》，亿赛通大家庭有你，有我，更有共同努力的我们……

2021 我们已准备就绪，蓝图已描绘，奋斗正当时。“综合数据安全厂商”的华美篇章已徐徐拉起，让我们永葆初心、扬帆远航，迎接亿赛通“新时代”的到来。

圆满保障安全，恪尽职守服务，亿赛通护航客户数据安全运营

感 谢 信

北京亿赛通科技发展有限责任公司：

自保密网络检查监测体系建设以来，贵单位以锐意进取的创新精神、深厚广阔的行业积累、扎实牢靠的技术支持、全面专业的安全服务，有力支撑国网河南省电力公司保密办的各项工作，确保了各项重点任务有序推进，为公司系统保密工作的安全平稳进行提供了坚强支撑。

期间，贵单位选派的毕[illegible]、刘[illegible]、雷[illegible]三位同志以高度的责任感和饱满的工作热情全身心投入国网河南省电力公司的保密网络体系建设工作。在保密网络检查监测工作中，三位同志充分发扬奉献拼搏精神，履职尽责，严格遵守公司要求，出色完成了保密网络检查监测任务，表现出扎实的技术能力和出色的专业素养，得到我单位各级领导和同事的一致好评。

在此，谨对贵单位给予我公司的大力支持，对三位同志付出的辛苦努力表示诚挚的感谢！希望在后续工作中再接再厉、砥砺前行，共同为公司保密建设作出新的更大的贡献！

国网河南省电力公司电力科学研究院

2021年 [illegible]月 [illegible]日

近日，国网河南省电力公司电力科学研究院向亿赛通发来感谢信，以感谢亿赛通在项目实施过程中各项重点任务进行中的的大力支持和有力保障，为公司保密工作的安全平稳进行提供了坚强支撑。

多年以来，亿赛通一直在不断强化着对合作单位和客户的技术支持能力，将工程交付与服务输出提升至和产品输出同等重要的地位，让员工在专业素养和服务意识两方面能够并行成长，从培养先进个人到建设先进团队，通过专业、高效的服务向客户呈现更加完善、优质的合作体验，为双方建立长期合作打下更加坚实的基础。

数据安全运营服务及工程交付往往是被业界普遍忽略的痛点问题，由于数据安全体系的庞杂，终端环境千差万别，安全、IT 及业务部门的交叉，往往导致交付难度大幅度上升，用户体验感较差。亿赛通过 10 余年数据安全建设方法论 + 全行业实施经验，深入了解数据使用业务场景，关注用户数据价值，识别数据安全与风险评估，基于整体数据安全防护规划，进行防护目标的差异化分析，给予综合专业数据安全治理建议。并实施了流程规范、资料完备，交付技术、交付效率、服务态度和用户满意度等六项交付效果指标。服务了小到几千点大到十几万点的客户，在各类项目实践过程中结合各行业的客户实际需要和应用场景，有效地提升其安全管理工作的效率和质量。

尽心尽力保安全，技术服务获认可

在本次项目支撑中，技术人员在充分了解国网需求后，依托公司专业资源优势，积极配合做好系列技术服务工作，保障了项目实施工作的顺利进行。亿赛通服务用户的专业认真，在业界早已深入人心。近年来，我们曾先后收到多家企事业单位的感谢及优秀供应商证明，客户均对亿赛通给予了高度评价。

这种全心全意为客户服务的工作宗旨，也正是亿赛通长久以来所秉承的企业文化精髓，客户的感谢及认可既是我们的荣幸，更是公司继续前进的动力！亿赛通还将以更加完善的服务、更加专业的技术和更加认真的态度，为客户提供更加优质的安全产品和服务，与广大行业客户精诚合作、携手共赢！

破局金融数据安全，亿赛通打造专业金融数据安全解决方案

3 月 23 日，2021 年贵州农信系统 IT 新技术应用交流会已成功召开。此次会议由广东省粤港澳合作促进会金融专业委员会主办，北京亿赛通科技发展有限责任公司协办。亿赛通作为安全厂商受邀出席会议，并在会上发表题为《金融数据安全的变革与创新》的精彩演讲。

现代信息化科技建设的大力发展下，金融行业在日常经营活动中积累了大量数据，这些数据除了支持前台业务流程运转之外，越来越多被用于财务报表、客户信息、绩效考核、决策支持等领域。银行日常经营决策过程背后实质是数据产生、存储、传递和利用的过程。充分挖掘这些数据资产的使用价值，可以为金融生产带来极大的经济效益和竞争优势。然而，业务数据一旦丢失、损坏或泄露，则有可能造成巨大的经济损失，或在社会、法律、信用、品牌上对企业造成严重的不良影响。在金融行业转型和发展的过程中，平衡数据使用的便捷性和安全性成为极大的挑战。

金融行业数据安全迫在眉睫

金融行业相关机构要想实现安全的管理和运营，就必须满足国家上级监管机构要求的数据安全合规性建设，这种需求项目大、周期长、客户要求较高。通常需要先进行整体体系建设的交流，以及成功案例的经验分析，对客户进行分阶段的规划，然后取得建设思路的一致，才能逐步开展组织架构、数据体系制度流程的建设、数据的分级分类、数据安全产品技术落地等。

沉着应对金融数据安全挑战

目前金融机构大多有较完整的安全规范，如分级分类规定，保密规定等，但一方面没有独立的数据安全规范，可执行性不强，另一方面缺乏技术监管手段，落地执行较难。传统的安全理念是“七分管理，三分技术”，随着数据量的指数级增长，仅仅依靠管理很难对数据进行全方位管控，而在实践中技术工具占据了越来越大的比重。传统的咨询项目交付物是大量的文档，而数据安全的项目真正能够落地执行离不开技术工具的管控。技术管控按照生命周期来分，可分为数据的采集、传输、存储、使用、删除、销毁六个方面。根据数据分级分类进行安全环境和边界管控，保障数据的保密性、完整性和可用性。亿赛通分别从制度和技术角度为客户建立数据安全防线，制度主建，技术主战，对数据和人实现分权分责分风险，形成放权管责相结合的态势，做到要素服务保支撑，持续安全可运营，确保数据安全流转产生价值， 共建数据安全大生态。

在本次交流会中，亿赛通凭借在金融行业数据安全解决方案上的创新突破，获得了与会嘉宾的高度认可，这也是对公司一直以来践行方案创新的肯定。亿赛通也将会继续不断发挥工匠精神，在数据安全领域不断探索前沿技术。近日，亿赛通已细分五大类产品技术特点“审计检测类、加密防护类、安全管理类、安全平台类、安全服务类”，拥有 40 余项精品产品板块。未来，我司将继续帮助企业推动数字化转型，实现企业全生命周期数据安全保障。

点燃安全之火，亿赛通数据库安全审计系统获信息技术产品安全测评证书

近日，经过多轮严格信息安全评估，亿赛通数据库安全审计系统通过中国信息安全测评中心 EAL3+ 级测试，获得《信息技术产品安全测评证书，级别：EAL3+》。

网络的快速发展使得网络安全问题日益突出，越来越多的用户更加重视信息资产安全，并部署了软硬件多种安全产品保护数据安全。但是不可预测的安全威胁，以及更高级网络技术的不断涌现，促使网络安全防护需要不断更新升级，对于安全产品的选择也要有较高安全保证能力的要求。

亿赛通数据库安全审计系统是亿赛通推出的一款通过对数据库网络流量的采集，基于数据库协议解析与还原技术的数据库安全审计系统。实现对数据库所有访问行为的监控和审计、对其中的危险操作进行多种方式的告警、对数据库访问行为进行多维度的统计并进行图形化展现。

六大特色让数据库审计更可靠

业务系统无感审计

系统主要采用旁路镜像方式部署，将客户数据库的网络流量单向引出，能做到对客户业务网络零影响，对客户业务系统无感知，从而保证客户原有业务系统的稳定运行。

终端用户审计能力

系统利用 WEB 插件关联技术，将应用层和数据库层的访问操作请求关联，可以追溯到应用层的最初访问数据及请求信息，可直接定位到业务终端用户。

大数据架构和设计

系统采用大数据计算和存储架构以及数据热交换技术，大大提高了实时数据处理效率，使得数据检索不仅范围更广，能实现全库检索，而且查询效率更高，对于客户常用的查询和检索场景，均能实现秒级响应。

数据类型全面审计

系统支持数据库类型丰富全面。不仅支持市场主流关系型数据库，还支持国产数据库和大数据审计。

机器智能模型学习

系统具备在目标网络中的数据库自动发现能力，并且支持自动对象参数配置，同时系统具备特定数据库的数据访问模型学习能力，可自动归纳学习数据库访问模型。

审计部署方式灵活

系统采用大数架构及分层模块化设计，具备极强的伸缩性，既支持硬件一体机方式，也可完美支持分布式部署，同时还支持纯虚拟化环境部署。

“中国信息安全测评中心”是国内专门从事信息技术安全测试和风险评估的权威职能机构，拥有一流的信息安全漏洞分析资源和测试评估技术装备。此次 EAL3+ 评估测试过程中，亿赛通数据库安全审计系统历经数月多轮严格的评估检验，一次性全部成功通过测试。获此信息安全产品 EAL3+ 级认证，意味着亿赛通在数据库审计方面能提供最安全稳定的服务，其产品自身、开发环境、管理过程都达到了 EAL3+ 级别的要求，具备了相应级别的安全性，也标志着亿赛通可以为用户数据库提供更高级别的安全保障。

30 秒了解亿赛通：

北京亿赛通科技发展有限责任公司（以下简称“亿赛通”）成立于 2003 年，是绿盟科技（证券代码：300369）全资子公司。亿赛通作为国内数据安全行业的供应商，是一个拥有完全自主知识产权的高科技软件企业，并已取得“高新技术企业证书”、“涉密信息系统产品检测证书”、“军用信息安全产品认证证书”、“商用密码生产定点单位证书”等多项资质认定。

亿赛通从专业的文档加密厂商，逐步发展为数据安全防护厂商，近两年成为综合数据安全厂商，更是在业内首提“分．放．管．服”数据安全建设理念，公司全线产品从应用场景出发，分为云、网、端三类，细分五大产品类别，包括：安全服务类、审计检测类、加密防护类、安全管理类、安全平台类，同时涵盖 40 余项产品板块，形成一体可视化态势感知数据安全智能管控平台。

史上最大隐私诉讼案迎来和解，巨额赔偿金引起关注

2020 年各种“泄露事件”不断上演，2021 年如期而至，我们希望今年是风平浪静的，希望各种“门”都锁好，不要再被破门而入让您措手不及、损失巨大。然而，理想很丰满现实很残酷！泄露事件仍然频繁上演，无论个人或企业都难逃隐私泄露的魔手。

近日，Facebook 再次登上热搜榜，成为各国关注的焦点，对于 Facebook 来说，也是新春过后的一件喜事，隐私侵犯事件正式落下帷幕！

美国加州地方法官批准了 Facebook 人脸识别侵权集体诉讼案的和解协议，并要求 Facebook 尽快向索赔的 160 万名诉讼成员支付共 6.5 亿美元的赔偿金。

这起集体诉讼于 2015 年 4 月在伊利诺伊州发起，涉及 Facebook 在其照片标记功能中使用的面部识别技术，用户指控 Facebook 未经许可创建并存储他们的面部扫描图像，违反了《伊利诺斯州生物特征信息隐私法》。

此前，Facebook 曾以用户没有遭到金钱损失等“明显的具体损害”为由申请撤销诉讼，但被法院驳回请求。之后，再次提出了 5.5 亿美元赔偿金的庭外和解方案，试图结束这起诉讼。然而，法院认为这笔赔偿金额过低，驳回了其提出的和解方案。直至 Facebook 将赔偿金额增加至 6.5 亿美元之后，法院初步批准了双方达成的和解协议。

根据和解协议，三名原告代表将每人获得 5000 美元赔偿，其他原告预期将获得至少 345 美元赔偿。法官表示：“这项 6.5 亿美元的和解是一个里程碑式的结果，是有史以来针对隐私侵犯诉讼规模最大的和解之一。”

随着人脸识别的大范围普及，我们的隐私信息被轻松爆出，难道隐私信息、生物信息不应该被层层武装，运用各种信息安全防护手段去保障吗？那么，当下千千万万的企业来讲，他们的信息安全防护手段远没有 Facebook 缜密，其信息安全程度也就可想而知了。

在当今的信息化迅速发展的时代，企业的数据信息就是企业一笔巨大的资产，假设公司将人脸识别出的面部特征、绑定的身份信息等等这些保密性的资料一旦被泄露出去，会造成巨大损失。那么作为企业，我们应该如何去加强防护自己的敏感信息呢？亿赛通小贴士为您献上锦囊妙计：亿赛通的“分、放、管、服”数据安全建设理念，改变原有理念，通过数据的风险评估，漏洞分析进行数据的分类分级；利用技术手段做到“安全流转、放管结合”；最后实现数据的统一管理、溯源取证、策略协同。

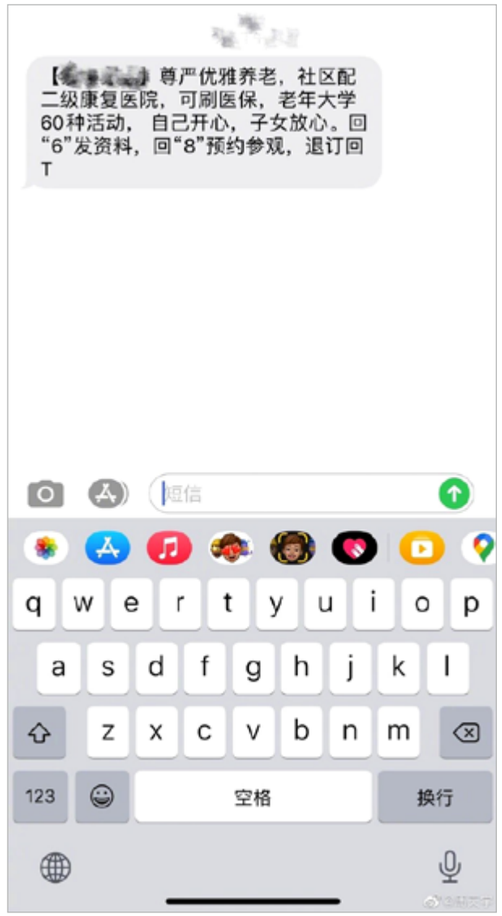
诚然，“人脸识别技术”的发展和应用正有效地推动着大量行业的进步，但随之暴露出的很多潜在风险也应当引起足够的重视。“用户面部特征采集的安全性与隐私性”、“用户信息的泄露与恶意买卖”、“法律法规不健全”等等问题，“刷脸”真正实现普及还有很长的路要走。中国数据安全专家亿赛通也在此呼吁大家，“刷脸”需谨慎体验，防止某些不法分子窃取你的信息实施各种非法活动，保障数据安全，我们一直在路上……

垃圾短信成“流行趋势”，背后的安全问题你知道吗？

这是一个无处不网、无人不网、无网不媒的时代。我们的个人信息安全在大数据时代日益凸显，隐私泄露层出不穷，垃圾短信、骚扰电话现象频繁发生。

聚光灯下的明星难逃隐私泄露

3 月 3 日下午，演员马天宇在个人社交平台晒出一张短信截屏，并附文写到：“不出意外的话，又收到了养老院的信息，是你们给我报的名么？要回复 6 还是 8？在线等 ~”。其实，对于马天宇来说这已经不是他第一次收到养老院信息了。去年 11 月底，马天宇就晒出一张苦笑表情包并透露最近天天收到养老中心的电话。



个人信息泄露无处不在

收到垃圾短信现在已经成为生活中很平常的事情，像马天宇一样，很多人确定并没有在某平台、公司预留手机号码，却总是收到推销短信。实际上，我们的个人信息早就在不知道的情况下被转手倒卖了好几次了。我国手机网民规模庞大，移动互联网时代，个人信息和用户数据成为重要的商业资源。一些企业和个人为牟取经济利益，私自倒卖信息数据，导致垃圾短信、骚扰电话频发。

可能有人会说，在现在社会现实中，苛求公民身份证号、手机号不被他人知晓，根本就是天方夜谭。“五毛一张打包带走，总共两万套，不议价。”、“人脸数据 0.5 元一份、修改软件 35 元一套”……当下，在不少社交平台、电商平台上，通过搜索特定关键词，就能找到专门出售人脸数据和“照片活化”工具的店铺。连人脸数据都能轻易买到，更何况随时随地都能被收集到的手机号码。

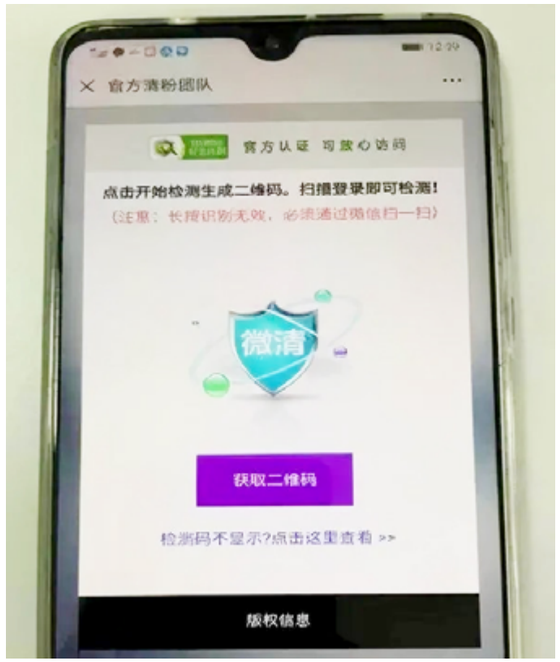
无视不是解决的良策

据一项调查显示，在信息泄露后，接到骚扰和诈骗电话、短信时，71% 的被调查者选择掐断电话或不予理睬，63% 选择拒接及拉黑，仅有 20% 左右被调查者选择了举报、投诉、报警等积极应对措施。个人信息泄露、遭到垃圾短信的骚扰，本质上是对公民隐私权的侵犯。

当然，骚扰电话、垃圾短信背后是庞大的数据泄露灰色产业链，事关不少经营主体的切身利益。还公众“私人生活安宁”，必须从源头抓起，扼住信息泄露的“喉咙”。就目前而言，APP 授权、快递单等都是泄露个人信息的主要渠道。因此，在保护个人信息安全方面，网络平台和企业都扮演着重要角色：要合理合法地收集业务所必需的信息，而不是越权、越界收集其他信息；提高平台的安全系数，强化其信息保护能力，防止信息被泄露甚至被恶意窃取。

另外，亿赛通提醒您针对各种侵权行为，用户应及时投诉维权，便于对侵权行为及时追责。唯有多管齐下，解决公众对信息泄露无可奈何的痛点，才能还互联网时代公众私生活一片祥和安宁。

如此明显的骗局，你还敢“清粉”吗？



微信已经成了很多人的主要联系方式。微信通讯录的数字越来越多，但其实里面大部分人都很少联系。于是，一种所谓微信“清粉”的服务应运而生。然而，这种方式可能威胁到你的信息安全。

去年九月，南通市通州公安破获全国首例利用微信“清粉”软件非法获取微信用户信息的案件，八名犯罪嫌疑人落网。本月，该案进行了集中宣判。

八名被告人犯非法获取计算机信息系统数据、非法控制计算机信息系统罪而获刑。被害用户当初扫描这款“清粉”二维码，目的是想给微信好友通讯录“瘦身”，释放内存空间，不料造成个人信息泄露。被告人则以刷阅读量、售卖微信群聊二维码等方式非法获利 200 余万元。

为图省事和方便，现在很多微信用户会选择“清粉”服务。事后，发现有陌生人通过二维码扫码进群，或者自己被拉入了一些广告群。其实，微信朋友圈和群聊中散播的“清粉”软件存在很大安全隐患。

嫌疑人获取的群二维码

“清粉”软件的原理，是通过应用集群控制软件控制微信账号，自动向所有好友群发消息，再由软件自动识别哪些是“僵尸粉”并予以删除。但不法分子在取得微信账号的控制权限后，借机非法获取用户微信群聊二维码信息，并将这些群聊二维码以图片形式保存在服务器上，倒卖给下游的诈骗、赌博等犯罪团伙获利。

有“组织”有“纪律”

经过调查，该“清粉”团伙分工明确，由张某、刘某、何某负责系统开发和维护，李某负责出售二维码牟利，谭某负责为微信公众号引流牟利。据众人交代，所谓的官方认证、放心访问只是为了降低使用者的警惕心理，他们并没有获得官方授权，而是租用服务器自行搭建系统，在骗取用户授权登录后，通过这些外挂软件系统批量获取微信群聊二维码，批量关注、阅读、点赞等。

短短 3 个月时间，该团伙共非法获取用户微信群聊二维码 2000 余万个，均出售给了诈骗、赌博犯罪团伙，同时还为他人批量关注微信公众号和刷阅读量、刷赞，先后获利 200 余万元。

该团伙从非法获取微信用户的相关个人信息，到下游的广告、营销和其他网络犯罪，相关的网络黑灰产已经形成一个各环节相互独立又紧密协作的产业链。

亿赛通中国数据安全专家提醒，“清粉”授权不法分子将轻易获取相关个人信息，建议广大网友不要使用非法插件和软件，有效规避可能遇到的安全风险，做到“不信、不扫、不传播”！！！

痛批个人信息泄露的“新病”，数据安全该何去何从？

一年一度的“3·15”国际消费者权益日如期而至，其实，连续几年，315 晚会的重点都放在“个人信息泄露”的问题上！“谁偷了我的‘脸’？”“伸向个人简历的黑手”“老人手机里的安全陷阱”……今年的 3·15 晚会揭露了侵权违规行为——个人信息泄露的“新病”。

个人信息安全问题曝光率最高，如何加强保护成为痛点

与往年相比，今年曝光的个人信息安全问题同样不容小觑。智联招聘号称视用户信息安全与隐私保护为自己‘生命线’，背后却大肆贩卖求职者个人信息，只需支付 7 元，就能买到一份内容详尽的求职者简历，卖家还可以根据用户要求对简历按照年龄、地域、毕业院校等信息进行精准筛选，已经形成了个人信息泄露、买卖、精准诈骗的黑色产业链。此问题在曝光后，智联招聘表示，已成立专项团队进行调查处理，并进行后续整改工作。

人脸信息成主要泄露数据

同样引发关注的还有对人脸识别信息的窃取。人脸信息涉及公民隐私和财产安全，我国法律明确规定，未经允许不得随意获取人脸识别信息。然而，某公司旗下卫浴门店等多家企业安装人脸识别摄像头抓取包括性别、年龄在内的个人信息。

数字经济时代，“信息”成为宝贵的财富资源。如何加强个人信息保护已成为当前亟待解决的痛点问题。《民法典》专设‘隐私权和个人信息保护’章节，规范了个人信息使用应当遵循合法、正当、必要原则，不得过度处理，如果自然人发现信息处理者违反法律、行政法规的规定或者双方的约定处理其个人信息的，可以请求信息处理者及时删除。

同时，消费者应增强维权意识，学会利用《民法典》及相关消费者权益保护法律规定，维护其自身隐私和个人信息。此外，还应从监管层面着手，明确“人脸采集”等个人信息采集的许可证制度，规范数字经济的发展。

消费者个人敏感数据被存储到企业后，企业必须承担安全管理责任。由于数据保护措施不到位、审核流程不完善，极易给不法分子可趁之机，导致企业“内鬼”信息泄露事件。作为数据安全领域一流的解决方案供应商，我们以咨询服务、产品方案、工程交付三个体系为主导，全新提出“分．放．管．服”数据安全建设理念，即分层治理、放心流转、放管结合、运营保障。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，放权管责相结合，做到要素服务保支撑，持续安全可运营，确保数据有价值的安全流转。

文章资讯来源于互联网

文件加密在 HVV 行动中的应用

售前技术部蒋李 / 文

随着大数据、物联网、云计算的飞速发展，同时 5G 技术为各种新型技术赋能，加上各种新型技术在日常生成上的应用，企业信息化水平不断提升，逐步实现无纸化电子化办公及线上协同，提高企业生产效率；如今，网络已成为企业乃至国家发展不可缺少的一环，网络安全直接影响到企业乃至国家安全，特别是国家关键信息基础设施建设也面临无形威胁，为了加强国家关键信息基础设施的安全，特别是在中美对抗这一特殊时期，我国应当化被动为主动，提升主动防护水平，未雨绸缪做好网络防护、网络攻防演练及应急响应，由此由公安部组织的“HVV 行动”应运而生。

2021 年 HVV 行动将于 4 月正式拉开帷幕，各抽中参与演练单位已陆续收到行动通知；在 HVV 行动中常用的攻击方式是社会工程学攻击，以下分享某航空公司被攻击方拿分案例。

首先是红方队伍选定好攻击目标后通过采用邮箱攻击获取到了内部员工即时通讯的账号和密码，通过内网渗透扫描出该航空公司内部信息化系统，同时发现了该航空公司的 FTP 服务器；攻击者通过分析拿到的即使通信软件的聊天内容，对该名员工的行为及语言组织方式进行学习模仿，同时分析通讯录可能拥有核心敏感信息的好友信息，并在工作日最为忙碌的时间段内对航空公司员工发起社会工程学攻击，用日常语调使用即使通信攻击进行聊天寒暄，并在不经意间咨询其同事 FTP 账号密码，并成功拿到 FTP 账号及密码登陆进入 FTP 服务器，发现众多机密文档，不限于当天航班信息、飞行安排及其他系统的账号密码信息文件。至此裁判直接判定红方得分。

通过此案例可以看出，提高员工的安全意识固然重要，但在这种场景下，员工对于熟悉的人难免会有松懈，导致敏感信息泄漏，如何去杜绝敏感信息泄漏，常见的敏感信息防护手段有两种，第一种为限制泄漏渠道，这种防护方式缺点为不能将所有的外发渠道锁死，容易产生疏漏，不然文件应用在效率上将大打折扣，不利于内部办公；第二种方式是采用文件加密方式，从文件本身上杜绝敏感文件泄漏，是安全和效率较高的一种防泄密方式。亿赛通电子文档安全管理系统采用的驱动层透明加解密技术，可以保证员工在日常办公中无感使用，但脱离本地的安全环境后文档将无法打开，如果以上航空公司 FTP 服务器中存储的文件都已加密文件进行存储，那么红方即使拿到了相应的敏感文件也无法打开使用，保障敏感信息安全。同时在 HVV 行动中常见的攻击方式还有 XSS 攻击，这种攻击方式可以做到对电脑权限进行提权，直接获取电脑盘符的存储文件并可以进行下载到攻击者本地，如采用加密方式进行文件存储，即使攻击者拿到了相应的文件也无法打开使用，保障敏感信息泄漏。

在整个数据安全行业中亿赛通已连续八年获得数据安全市场占有率第一的殊荣，国内第一套数据安全加密防护软件来自于亿赛通，成立至今已有 18 年历史，通过十八年的技术积累已获得数据安全领域九项国家专利，亿赛通以其深厚的技术实力为蓝方用户敏感信息文件加上一把坚不可摧的安全之锁，势必将在 HVV 行动中守好数据安全的最后一道防线。

蜂巢能源科技有限公司

客户简介

蜂巢能源科技有限公司的前身是长城汽车动力电池事业部，自 2012 年起开展电芯的预研工作，2016 年 12 月成立电池事业部，2018 年 2 月独立为蜂巢能源科技有限公司。公司总部位于江苏省常州市。我们致力于下一代电池材料、电芯、模组、电池系统、BMS 储能系统和太阳能技术的研发、制造及创新。公司拥有超过 2200 名员工，包含 1100 名研发人员。到 2020 年研发投入约 30 亿元，到 2025 年全球工厂建设计划投入超过 260 亿元。

典型案例 TYPICAL CASES

需求背景

现代企业的竞争是以核心技术为基础的整体实力的竞争。企业独立后，蜂巢能源就围绕如何提升企业核心技术竞争力，打造 " 蜂巢 " 品牌进行了一系列的改进工作。公司的电池材料和系统、太阳能技术研发设计和储能系统等核心技术，保持了主导产品在国内市场的领先地位。为保障企业的核心竞争力，公司开始陆续加强了内网信息化的安全建设，经过长期沟通选型，以及多轮测试环节，最终蜂巢能源采购了我司的文档加密产品。

解决方案

文档透明加密系统改变了传统意义上的文档安全保护模式，在对文件加密的同时不改变用户的任何使用习惯，让用户在不知不觉中享受安全。通过透明加密和内容智能识别技术，用户打开文档时，客户端根据服务器下发的安全策略，对文档内容进行检测，如果检测到敏感文档中还有机密信息，则会自动加密，整个过程对使用者来说是无感知的。

通过为应用系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。通过对文档加密、授权及封装，控制文档在外部传播和使用时造成的泄密风险。数据作者可以根据需要设定文档的查看权限（只读、打印、修改、阅读次数、阅读时长），外部用户拿到文档后需要通过安全身份认证后才能查看该数据，没有通过认证的无法查看和使用数据。

项目成果

蜂巢能源文档加密项目开展的有声有色，灵活的系统不改变用户网络结构和客户的使用习惯，保障了每一个输入、输出的数据安全运行。首先极大的解决了企业信息环境高度安全性与信息安全整体解决方案高成本之间的突出矛盾。其次，最大程度的保障了企业庞大的数据体系，为企业打造出安全良好的工作环境。，主要对企业核心技术资料进行安全防护。

四川省电力公司信息通信公司

客户简介

国网四川省电力公司信息通信公司是国网四川省电力公司直属单位。国网四川信通公司于 2012 年 6 月 21 日成立，下设 4 个职能部门和 3 个业务机构。承担了特高压一级通信干线的属地化运维任务，以及三大特高压安控系统第二、三通道和直流控制保护业务二通道的通信传输任务。公司成立以来，为国网四川公司现代化管理、电网安全稳定运行提供了信息通信技术坚强支撑。在通信、信息领域取得多项重大科研成果，多次获得中国电力、四川省、国家电网公司、国网四川省电力公司科技创新一等奖。

需求背景

国网四川信通公司创新管理模式，优化业务流程，构建了集约化、扁平化、专业化的信息通信体系，为了防止企业内部的财务、设计、市场等部门的重要资料在各种有意无意的情况下被泄露到企业外部，从而影响公司在行业中的竞争力，因而启动了数据安全防护项目。亿赛通对国网四川信通公司的现状进行了充分调研和论证，并最终决定按照根据其工作模式进行相关的部署和管理。

解决方案

1. 文档加密安全网关：通过加解密网关进行业务系统的安全保护，可使从业务系统上下载下来的文件经过加密处理，在企业内部可自由使用，泄露到企业外部无法使用。有效控制了业务系统流出文档的安全性。

2. 文档透明加密系统：实现了企业内部电子文件的加密存储。所有文件只要写在磁盘上就是加密形式；只有被系统授权许可，才可使用这些加密的文件，如未经合法许可将加密文件数据体带走，加密文件内容将无法正常打开。透明加密，保护企业终端电脑办公文件安全，具有高适用性，灵活性。可根据客户需要调整安全等级，可自主设置加密解密。

项目成果

亿赛通提供的解决方案与国网四川信通公司的安全理念、安全需求高度融合，从根本上解决了企业存在的信息泄密隐患；通过高效先进的数据安全技术手段，解决了企业数据的存储、使用和传输中可能存在的泄密问题，帮助员工提高安全意识。