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 座三 / 四层

电话：86-10-57933888

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　中国数据安全防护专家　www.esafenet.com

09 月刊

2017 年共 11 期

关注企业官方微信

ESAFENET Journal

中国数据安全防护专家

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 座三 / 四层

电话：86-10-57933888

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com

CONTENTS 目录

刊首语 PREFACE

2/3 刊首语

行业聚焦 INDUSTRY FOCUS

4/5 海量数据下暗礁潜藏 “大安全”时代踏浪而来

6/7 网络空间安全 各国怎么管

8/9 也谈政府统计信息安全面临的挑战

10/11 人脸识别不能独立行走 商业化关键在于信息安全

亿赛通动态 ESAFENET NEWS

12/13 多家知名媒体爆料亿赛通“智能 + 安全”新科技 引爆安全领域新风潮

14/15 亿赛通个人版“数据安全卫士”全新推出 敏感数据超凡体验“智能安全”

16/17 慈善融真情 爱心无止 亿赛通 & 绿盟科技参加 2017 北京善行者公益徒步活动

18/19 用大数据建设“安全”生态 亿赛通出席安徽省通信学会大数据学术交流会

20/21 网安则国安 亿赛通出席国家网络安全宣传周 合力共建网络强国

亿赛通小贴士 ESAFENET PROMPT

22/23 某云存储惹祸？大量机密信息遭泄露？小贴士“智能安全”法宝让数据存储更安全

24/25 又来两剂猛料？ 400GB ？半数美国人……敏感数据又遭泄露 好“惨”

26/27 苹果 X 出来啦！有人又开始打量自己的肾了！ 还是亿赛通“安全”小卫士靠谱！今日一波福利又降临

典型案例 TYPICAL CASES

28/29 亿赛通全新“智能安全”方案为研发通讯产业发展护航 实现安全即时通讯智能管理体系

30/31 智能安全引领科技前沿 亿赛通深度打造烽火通信“智能安全”屏障

刊首语 PREFACE

喜迎中秋 歡度國慶

聚焦亿赛通九月刊“信息安全”所有亮点抢先看

金风送爽，天高云淡，花果飘香，我们喜迎中秋欢度国庆。在这个丰收与喜悦的日子里，亿赛通九月刊与大家共话网络安全大事，共建网络安全环境，共创未来安全。

如今社会是一个高速发展的社会，科技发达，信息流通，人们之间的交流越来越密切，生活也越来越方便，而“大数据、云计算、人功智能、互联网”成为了这个高科技时代的产物。对此，数据正在迅速膨胀并变大，它决定着企业、个人的未来发展，人们将越来越意识到数据对企业、个人的重要性，但是威胁同样围绕在我们的身旁。本期月刊，亿赛通与大家共同诠析互联网、大数据、人工智能时代，企业数据究竟潜藏着哪些新威胁？数据安全解决新思路如何采取策略进行防护……

海量数据下暗礁潜藏
“大安全”时代踏浪而来

经过 23 年井喷式发展，互联网已深刻地影响到了中国政治、经济、文化等方方面面。随着互联网加快深入到经济社会各个领域，网络安全形势也面临着更加严峻挑战，海量数据带来的威胁也日益加重。

随着网络化时代的到来，人们的沟通交流更加便捷，各类信息也都逐渐透明，信息技术在人们生活的各方面得到更加广泛的应用。经过 23 年井喷式发展，互联网已深刻地影响到了中国政治、经济、文化等方方面面。

其中大数据正在以一种前所未有的方式对海量数据进行分析，从而获得巨大价值的产品和服务。但是大数据是一把“双刃剑”，人们在因大数据受益的同时，也面临着巨大的挑战，个人隐私保护问题就是其中之一。

大数据时代，任何个人的“小数据”都可能不再安全。与日常隐私保护不同，公众网络上炫富、晒幸福等，都主动贡献了信息，这些看似微不足道的信息，通过大数据分析并与其他信息整合，可能会被犯罪分子利用。

随着互联网加快深入到经济社会各个领域，网络安全形势面临着更加严峻挑战，海量数据带来的威胁也日益加重。数据显示，截至今年 6 月，中国网民已达 7.51 亿人，这其中超过 60% 的人遭遇过不同程度的个人信息泄露，像支付宝目前有超过 4.5 亿用户，而每天交易笔数中有 5% 存在安全隐患。

如今网络安全已经不单单和个人及社会有关，乌克兰大停电、伊朗震网病毒、美国“棱镜门”等事件向世人宣告，网络安全已是国家安全的一部分，网络也已成为可预见的未来战场。

在 9 月 12 日于北京召开的第五届中国互联网安全大会上，与会专家就已明确表示，网络安全不仅是网络本身，而是包含社会安全、基础设施安全、人身安全等在内的“大安全”概念，迫切需要建立与之相适应的保障体系。

工信部网络安全管理局局长赵志国在会上说，网络安全不仅事关社会生活。随着信息技术与工业生产的深度融合，工业互联网、物联网等应用范围迅速扩展，其安全性也应得到足够重视和保障。网络攻击门槛降低，对象广泛，攻击手段更加多样。

缺少了网络的安全，信息化建设就如同空中楼、水中月；缺乏信息化技术的保障，网络安全就成为纸上谈兵，不堪一击。面对新形势工信部将针对国内外形势变化新趋势，开拓网络安全新举措，从法律、制度、标准、技术等方面统筹谋划网络安全的保障体系，并重点建设配套政策等五项举措。

这五项举措具体为：一是推动完善网络安全法律法规和制度标准体系，同步完善危险监测处置、数据保护、新技术、新业务安全评估等行业配套政策；二是持续强化信息通信行业网络安全的防护能力部署和监督落实；三是加大网络环境的治理力度，每年不定期开展网络安全威胁的专项治理行动；四是推进信息行业大数据安全的监管能力建设；五是推动网络安全产业的发展和人才队伍建设，强化基础支撑的保障能力。（新闻来源：中国智能制造网）

网络空间安全 各国怎么管

9 月 16 日，2017 国家网络安全宣传周拉开帷幕。

当今世界，以互联网为代表的信息技术日新月异，创造了人类生活新空间，拓展了国家治理新领域。为了维护网络空间安全，各国纷纷出台了政策法规，“多管齐下”监管。

严格立法 网络犯罪“无处遁形”

新加坡在网络管理方面非常严格。该国的《互联网操作规则》对网站“禁止内容”设立了明确而具体的判断标准。《管理法》规定，在新加坡的网络服务供应商和拥有网址的政党、宗教团体以及以新加坡为对象的电子媒体，均须在新加坡广播局注册并接受管理。

同时，新加坡还将上百个政治性网站列入禁访者清单，不遵守规定的网络服务供应将被吊销执照或罚款，私下访问者也会受到刑罚。政府还鼓励服务供应商开发推广“家庭上网系统”，协助用户过滤不适宜看到的内容。

俄罗斯政府支持并保护互联网的自由，但同时明确强调互联网自由要以道德和法律为基础。《俄罗斯联邦宪法》把信息安全纳入了国家安全管理范围，在此基础上制定颁布了《俄联邦信息、信息化和信息网络保护法》，以此规范俄互联网行为。

此外，俄还专门立法对信息安全进行政策指导并作为司法部门执法依据，以专业机构和地方政府的相关措施作为监管补充，形成了较为完备的多层级信息安全法律体系。

印度政府成立了印度数据安全委员会，专门针对日益增多的网络数据安全问题提供权威监测和管理方法。印度还是世界上为数不多专门为信息技术立法的国家之一。早在 2000 年，印度就颁布了《信息技术法》，并根据实际情况对其进行过多次修订，包括将移动通信纳入监管范畴，加强对网络运营商和个人用户进行适当和有效的管理，规定印度政府有关部门有权查封可疑网站和删除违规内容等。

墨西哥的韦拉克鲁斯州于 2011 年 9 月出台了《动乱法》，标志着该国对网络犯罪的量刑提出了明确界定标准，规定在互联网上制造和发布假新闻的行为构成“破坏社会稳定罪”，将依法追究刑事责任。此外，墨西哥当局近年来不断增加网络安全监管方面的预算开支，聘请更多的网络技术人才来扩建“网络安全军”。

及时应对社交网络常态管理

美国媒体报道称，从 2010 年 6 月起，美国国土安全部分布在各地的“社交网络监控中心”开始执行“社交网络 / 媒体能力”项目，对网上公共论坛、博客、留言板等进行常规监控，多个知名社交媒体及众多热门博客均在监控名单中，搜集的信息会被交给美国国会图书馆收作电子档案。

近年来多发的严重骚乱和日益增多的网络问题也让英国政府逐渐意识到 ,仅仅通过行业自律难以达到治理效果。因此，必须加强网络监管，及时制止把社交媒体用于暴力的行为。

英国要求社交网站保留用户的相关信息记录。据了解，为了调查严重犯罪和恐怖主义、保护公众安全，英国的警察和情报部门能在特定情况下获取通信数据。互联网服务供应商及电信公司还被允许安装硬件，储存通信数据长达一年，社交网站则需要保留用户相关信息记录，以备日后查询。

为了加强对社交网络平台的监管，俄罗斯政府采取了有针对性的措施。一方面 ,加强对本国社交网络公司的管理。此前，俄国家杜马资产委员会专门提交了一项法律草案，旨在通过划定俄战略资产的方式，从法律上排除了外国资本取得俄网络公司控股权的可能性。另一方面，俄政府还通过直接参股等形式加强了对国际新兴媒体的监控。

澳大利亚也把新型社交媒体作为监管重点。澳大利亚国防军公共事务相关负责人认为，在军队中，如何对社交媒体的使用进行监管，使之能够为军方所用，既是机遇也是挑战。此外，越来越多的澳大利亚公司和机构已经开始禁止员工在上班时间使用社交媒体，并且禁止员工下班后在社交媒体网页上对老板进行评论。(新闻来源 : 解放日报)

也谈政府统计信息安全面临的挑战

近年来，随着社会科技水平与网络信息技术的快速发展，计算机技术在政府统计中的运用也越来越广泛。如何加强信息安全建设，管好盘活海量社会经济数据，越来越成为各级统计机构必须解决的重大问题。

政府统计面临的变革

在大数据时代，政府统计的数据采集和数据服务正在发生着巨大的变革。

一是数据获取由“逐级上报”向“网络取数”转变。例如，从政府统计工作实践看，房价调查采用的数据采集模式由“报数”向“取数”转变。2010 年 9 月，国家统计局、住房和城乡建设部联合下发的《关于加强协作共同做好房地产价格统计工作的通知》要求各省以及有关城市住房和城乡建设厅（住房和城乡建设委、房地局）、统计局、国家统计局调查队加强联系和合作，实现数据资源共享、信息资源共用。通过采集网签数据，国家统计局快速实现了对 70 个大中型城市房价指数的统一计算和发布。

二是统计数据由“条数据”向“块数据”转变。政府统计部门作为经济社会发展数据的生产主体，大量宏观和微观数据就像一座座宝库，蕴含着很多有价值的信息、规律和趋势。然而这些数据几乎都是“条数据”，他们彼此割裂、互不融通，最终限制了其在经济社会中应发挥的作用。随着大数据时代图像、文本、视频等非结构化数据的出现，以及统计与工商、税务、质检等部门行政记录的互联共享，通过新数据的汇集和原有数据组合后的衍生数据，将数据链起来、融合起来，让数据金矿富起来，从而真正激活处于沉淀状态的统计数据，挖掘出更高、更多的数据价值，为了解情况、判断形势、制定政策提供重要的参考依据。

三是部门职能由“数库”向“智库”转变。在政府统计的日常工作中，各项业务的顺利开展为决策咨询提供了坚实基础，有效促进了统计科研水平的不断提升。大数据时代，统计部门不仅要建好“数库”，更要做好“智库”，这也是统计工作创新服务的着力点。

信息安全面临的挑战

在大数据时代，数据信息作为政府统计部门掌握的重要资源，随着采集模式、数据类型以及部门职能的转变，统计信息安全也面临资源开放、数据流通和归集带来的一系列风险。

统计数据资源开放带来的风险。目前，在国家统计局联网直报平台上，有企业一套表、采购经理调查、工业生产者价格调查等众多网上直报项目，数以万计的调查样本数据汇聚在一起，就是一个实实在在的统计大数据，这里面蕴藏着许多更加复杂、更加敏感、价值巨大的信息。从样本个体看，具体指标直接反映了其自身生产经营状况；从数据总体看，通过专业分析，透过这些表面数据就能对经济运行的总体状况和未来走势一探端倪，大量统计数据的汇集开放将不可避免地加大数据泄露的风险。

统计数据流通过程带来的风险。在日常工作中，政府统计调查所采集的数据涉及大量企业、家庭和个人的隐私，如企业情况、人员信息、家庭收入、日常支出、消费记录等。大数据应用对数据的完整性、可用性和保密性带来挑战，在防止数据丢失、被盗取、被滥用和被破坏上存在一定的技术难度。首先统计数据采集过程存在数据损坏、数据丢失、数据泄密等安全威胁；其次在统计数据传输过程中，面临数据被截取和篡改等风险。

统计数据资源归集带来安全风险。一方面，在大数据环境下，数据量具有非线性增长的特征，各种数据大集中，尤其是其中 80% 以上的数据属于非结构化的数据类型，现有的存储系统模式仍然不够成熟，存在缺陷及漏洞，容易出现数据存储安全方面的风险。另一方面，由于政府统计数据大量汇集，使得黑客成功攻击一次就能获得更多数据，无形中降低了黑客的进攻成本，增加了攻击“收益率”。

加强信息安全建设的几点建议

一是做好安全规划，提高产品服务的可靠性。大数据时代的信息系统安全问题单凭技术是无法得到彻底解决的，它涉及政策法规、管理、标准、技术等方方面面，对于整个统计系统而言，解决信息安全应从系统工程的角度来综合考虑。首先要规划设计好具有政府统计特色，自主可控的统计网络，从技术、产品和服务等角度重视网络融合、终端使用等安全问题；其次在推进数据系统建设中，要实现建设、应用、管理、安全统筹规划同步设计一体化建设，特别是构建有利于保护数据生产全过程的安全性架构和安全性平台。

二是强化网络管理，保障统计数据安全。对于大数据而言，网络是传输的主渠道，是一切信息安全管理的主要抓手。强化网络基础设施安全保障，一是要通过访问控制，以用户身份认证为前提，通过实施访问策略控制和规范用户在系统中的行为，从而维护政府统计系统安全和保护网络资源；二是要通过科学地划分网络安全域，充分运用各种技术的组合和功能互补，不断完善传输加密、防火墙、入侵检测、入侵防御、漏洞扫描、防病毒等网络安全防护系统，完善身份认证、访问控制、安全审计、信息流控制、补丁分发等网络应用安全防护系统，提高统计信息系统对网络攻击、病毒入侵的防范能力和网络泄密等安全事件的综合响应能力，保证信息化设备与网络的安全稳定运行，切实保障统计数据安全。

三是建立大数据安全标准化体系，强化基础支撑。政府统计部门要研究制定数据基础标准，针对个人隐私、商业秘密、国家安全等率先使用数据安全标准，形成覆盖数据采集、存储、传输、挖掘、公开、共享、使用、管理等全流程安全标准体系。通过完善网络数据安全评估检测体系，提升对大数据网络攻击威胁感知、发现和应对能力。通过数据加密为统计数据的传输服务提供有效保护，利用过滤器监控，自动阻止数据的离网传输。通过系统容灾、敏感信息集中管控和数据管理等产品，实现端对端的数据保护，确保数据损坏情况下的有备无患和安全管控。通过应急恢复，保证在设备或应用软件发生故障时能够迅速恢复，提高重要统计数据的资源可用性和业务连续性。

四是健全大数据安全预警机制，强化监控审计。通过加强在线应用系统的网络安全监控和审计，及时发现网络中存在的安全威胁、安全风险和安全事件等，为制定安全策略、开展安全系统建设提供依据，进而提升自主可控水平和安全防护能力，预防和减少网络安全事件的发生，并可在发生安全事故事件时提供依据，进一步进行安全事件的溯源追查。政府统计信息安全在做好被动防御的同时更应主动出击，通过运用大数据技术和机器学习来提升信息安全防御等级。借助大数据分析，对网络日志数据进行自动分析处理和深度挖掘，对网络安全状况进行全面分析和综合评价感知网络中的异常事件和整体安全态势。利用对统计信息网络数据分析实时展现统计信息系统的访问态势和黑客恶意攻击态势，将那些隐蔽和少见的黑客攻击进行实时展现，同时在面对超级黑客的隐蔽攻击和渗透测试时第一时间识别和发现。最终实现通过大数据建模分析，在总结行为习惯的基础上辅以云端海量的安全威胁情报，达到对黑客可能的行为、网络中可能存在的入侵事件进行提前预警。（新闻来源：中国信息报）

人脸识别不能独立行走
商业化关键在于信息安全

苹果日前新出的 iPhone X 彻底抛弃了指纹识别技术，推出人脸识别功能，使得刷脸科技再次受到关注和热议。事实上，在国内，互金巨头以及大型商业银行都在布局刷脸支付。

无论是新 iPhone 的“人脸识别”，还是支付宝联手肯德基的“刷脸吃饭”，都因为将“脸”与腰包里的钱挂钩了。顿时感觉人脸识别是不是不安全？有没有风险？作为安防人，小编要和大家探讨探讨“人脸识别”技术引发安全问题。

人脸识别技术不行还是大家在撒谎

一些人工智能公司宣传，他们一般都会把人脸识别的性能吹得非常悬，说错误率已经达到亿分之一的程度等等。虽然这是事实，的确有时候我们发现有一些识别错误率已经低于亿分之一，但这是有前提的，譬如说静态人脸识别：如摆拍等。

还有一种场景是门禁的应用，人们为了过一个通道，然后就盯着摄像头，这时候成像条件都很好。但是对安防而言，更多时候被观测的对象没有意识到自己被观测，它的角度也不是很理想，离相机也比较远，光照也比较复杂。而且整个目标在运动中碰到照片时，它的人脸识别结果也完全不一样了。

很多公司认为人脸识别已经做得很好，但另一方面，如果大家去调查一下如果使用了人脸识别，尤其是使用动态人脸识别的客户，大多数客户都认为误报率太高，而且高到基本上这个系统就没有办法使用。

应用场景的复杂性直接影响到人脸识别的精准性。

针对人脸识别人工智能和人类智能各有所长

做人脸识别它的优点是速度快，一张显卡每秒钟可产生几百张脸的特征，完成数千万张脸的比对，这个目前已经可以做到了。它的成本也低，使得这项技能可以快速复制、大规模地部署，性能很稳定且可持续提升。人工智能的缺点是应对复杂问题应对能力差，除此之外是对环境变化的适应能力弱。

人类的智能跟人工智能相比，几乎是完全相反的。人类智能的优点正好是人工智能的缺点，人类对复杂问题的应对能力和对环境变化的适应能力很强，但缺点就是速度慢、成本高，比较难快速复制、不大可能大规模地部署、性能也不稳定（容易受到精神状态的影响）。

人脸识别不能独立行走

实际上，在今年央视 315 晚会上，人脸识别就被曝出可能存在安全威胁。就此事，专注人脸识别技术的商汤科技和旷视都表示，任何一种安全手段都不是独立的，因此在实际应用中，不会将人脸作为唯一的凭证。就连近日最近媒体频频报道的肯德基杭州“靠脸吃饭”的 KPro 餐厅，也不是单独依靠人脸识别技术单一完成支付认证的。

组合拳在人脸识别应用过程中是常态。现阶段所有涉及支付的系统都不是采取单一“人脸识别”技术，而是要结合短信、验证码、手机尾号等传统验证手段一并使用。

小编认为，采用多样结合的验证方法，表明许多企业在涉及“人脸识别”技术的商业化安全性上，也并没有十足把握。更多的只是把“人脸识别”当成一项新的噱头，尝试吸引着大众的关注。

人脸识别商业化 关键在于“大家的脸”属于谁

看到这里，你或许会一脸懵。如今，许许多多“人脸识别”的应用已经逐渐商业化，走进大众的生活。我们必须要对技术应用中所涉及的隐私和道德问题进行了一番新的思考。蚂蚁金服陈继东曾指出：“从用户隐私上来说，人脸识别和指纹、虹膜相比，属于弱隐私。换句话说，你的脸，早就不是隐私了。”

有关人脸识别商业化所涉及的隐私问题一直备受争议。此前，Facebook 因为未经用户允许而私自储存和使用用户的人脸识别数据而饱受诟病；而 Google 则因隐私政策和舆论压力而禁止 Glass App 使用人脸识别功能。

在中国，不管是“变脸美颜” App，“换装” App 也好，甚至是纳入“人脸识别”支付平台或软件，都无时无刻的“拥有”着大家的脸，每一次使用就将有一份脸部信息“标本”本保存下来。

如果说政府部门录入民众人脸信息“标本”有助于抓捕罪犯、预防犯罪，人脸识别便是鉴权的一种手段。那企业存储和应用这么多人脸，特征隐私数据泄露与否，全凭企业“良心”与“能力”。

人脸识别充当着人工智能的“眼睛”，作为人工智能与外界交互的一项重要技术，人脸识别技术的安全性显得十足重要。小编相信，在人口红利下，人脸识别有着十分庞大的市场空间，但在商业化上数据信息安全依然是所有厂商绕不掉的“门槛”。（新闻来源：星海康智能未来）

多家知名媒体爆料亿赛通“智能 + 安全”新科技 引爆安全领域新风潮

智能时代

黑客覆手为王，想要称霸世界？

家贼背信弃义，

间谍明修栈道，暗度陈仓，

勒索、木马肆意横行，

究竟谁主沉浮？

8 月 25 日，

一场以“智时代 • 智安全”为主题的亿赛通新品发布会震撼袭来，

“智能 + 安全”的新科技登上“智能安全”的舞台。

伙伴们，你们的“数据安全”从此再也不用担心了，

黑客？家贼？间谍？勒索？木马？爬虫？

……

全都 diss 吧，

哪里不安全就用亿赛通智能安全来保护！

你还在犹豫吗？你还在疑虑吗？

No Problem，看过来，

如果你也爱趴新科技，

那就聚精会神看看多家知名媒体如何爆料亿赛通“智能 + 安全”新科技！

央视媒体：CCTV 采访报道

哇喔，

央视媒体直趴“领导”爆料“智能安全”新科技！

优酷媒体独家爆料

亿赛通新品引爆安全领域新风潮

搜狐媒体大爆料

无论何种“病毒”都将被“智能安全”扼杀在摇篮中！

爱奇艺媒体爆料

“个人数据安全”有法宝了！

B 站视频爆料

bilibili 视频抢先看哦！

腾讯媒体爆料

腾讯媒体报道，视频抢先看哦！

亿赛通个人版“数据安全卫士”全新推出 敏感数据超凡体验“智能安全”

数据安全开启“个人版” 亿赛通全国首推

亿赛通全新推出“个人版”数据安全卫士，主要是针对个人 PC 端的重要信息或核心资料在外发、分享、存储中的安全需求而设计的个人版安全产品。即当您需要将个人的重要资料如工作资料、代码、保密照片、个人设计 / 摄影作品、书籍 / 自传、视频 / 音频资料、财务数据等等敏感信息外发给合作伙伴时，接收者打开文件首先需要进行身份认证，方可阅读，可以有效的防止重要信息在存储中，以及外发、传输给第三方时被有意或无意非法扩散或二次使用。

免费注册 拒绝套路

都说城市套路深，NO ！亿赛通拒绝套路！我们只为您的数据安全保驾护航。亿赛通数据安全卫士免费注册，过程甚是简单，操作绝对安全。轻松动动手指，就能尊享终身“安全”。伙伴们，让亿赛通数据安全卫士成为您“贴”身的数据安全小卫士吧！

简单 易用 支持近百种文件类型

面对智能时代的发展，亿赛通数据安全卫士迎合潮流让产品使用过程更加智能、安全、简单、易用。即采用高强度智能动态虚拟卷加密技术与安全沙箱隔离保护技术 ,具有高度的安全性。那么 ,问题来了 ,有小伙伴开始担忧，我想保密的文件类型有好几种，肿木办？难道需要格式转换再加密？ Oh,NO ！这么搞多不智能啊 ,不管你有多少种格式，亿赛通数据安全卫士包您满意，因为它可以支持近百种文件类型，如文档类、音频 / 视频类、设计类、图片类、代码类……全都鼎力支持。伙伴，总有几款需要你倾心呵护的秘密资料，交给亿赛通数据安全卫士帮您守住秘密吧！

外发文件想据为己有？ NO Way ！

伙伴，现实社会水很深，“知人知面不知心”说的总有几分道理的。当重要的个人资料发给朋友、或者客户时，然后你告诉对方一定要保密，鬼知道他扭头干了什么事，总有图谋不轨之人想把资料据为己有，甚至到处扩散，从而带来巨大损失。别担心，亿赛通数据安全卫士可以控制多种权限，包括浏览次数、使用时间、打印水印、修改、还原、防止内容拖拽、拷屏和设置自动销毁等等，无论在网盘存储，或者传输、外发都可保证您的数据绝对安全。没毛病，数据安全卫士就是这么屌，伙伴，文章都看到这里了，你还不行动吗？

慈善融真情 爱心无止
亿赛通 & 绿盟科技参加 2017
北京善行者公益徒步活动

2017 年 9 月 9 日 -10 日，北京善行者公益徒步活动在北京居庸关长城开走，有数百支队伍、三千余人以 50 公里、100 公里的徒步同时出发，体验行走的力量。亿赛通 & 绿盟科技携手共建和谐家园，用爱凝聚，践行公益的承诺，共同参加善行者公益徒步活动。

善行者是中国扶贫基金会于 2014 年发起的一项徒步筹款活动，旨在以“每一步都会带来改变”的信念，动员身边的人以实际行动支持公益，助力贫困地区儿童全面发展。亿赛通作为中国数据安全防护专家，秉承“勇担责任”的企业优秀文化，以“仁者爱人，老吾老，以及人之老，幼吾幼，以及人之幼”的慈善之心，在把企业做强做大的同时，不忘回馈社会，不忘关心贫困地区需要帮助的儿童，积极投身于公益活动。

以行动成就爱心，让慈善走进生活！

阳光慈善聚人心，亿赛通 & 绿盟科技携手慈善，与爱同行。

德化万物，泽备十方，爱心的传递如生命之花生生不息。每一个企业都应有一颗爱心，有一颗实现中国梦的爱心，感恩社会，感恩一切。亿赛通会坚持做社会公益事业，它不仅是企业优秀文化的传递，更是构建社会主义和谐社会的内在要求，同时也体现着亿赛通企业一直以来的高贵品质和关心公益事业、勇于承担社会责任、为社会无私奉献的精神风貌。用爱心作帆，用善良作桅，齐心协力，众志成城，开动慈善的大船，载着每一个中国人的梦想，驶向幸福美好生活的彼岸，亿赛通不忘初心，与大家一路同行！

用大数据建设“安全”生态 亿赛通出席安徽省通信学会大数据学术交流会

2017 年 9 月 17 日，安徽省通信学会大数据分会第四期学术交流活动在合肥举行，本次活动由安徽联通承办，会议规模之大，权威之高。并邀请到了中兴通讯首席架构师、中国大数据专家委员会委员等国内引领大数据前沿技术的 150 多家权威企业代表、德高望重的技术专家坐镇学术交流大会现场。亿赛通作为数据安全行业的佼佼者，运用大数据、互联网、云计算等新科技，采用国内外先进的信息安全技术，采取有效的安全策略和技术手段，建立覆盖终端、网络、存储、审计等各个方面的统一、安全、稳定、高效的信息安全大数据智能安全管理体系，保证系统安全稳定运行，推动大数据生态圈的健康发展。对此，亿赛通被特别邀请出席了本次权威大会，并与众多参会精英企业、技术专家等就大数据时代“潜藏哪些新威胁、机遇、解决方案等话题进行了深度的交流与分享。

大数据时代潜藏的新威胁

如今社会是一个高速发展的社会，科技发达，信息流通，人们之间的交流越来越密切，生活也越来越方便，而“大数据”成为了这个高科技时代的产物。对此，数据正在迅速膨胀并变大，它决定着企业的未来发展，人们将越来越意识到数据对企业的重要性，但是威胁同样围绕在我们的身旁。因此，在本次学术交流大会上，亿赛通高级安全顾问专家深刻的与大家分享了“大数据平台的数据安全解决思路”。那么，在大数据时代，企业数据究竟如何潜藏着新威胁？亿赛通高级安全顾问专家分析到，首先，因为权限管理与控制不当，导致敏感数据被随意处置；其次，因为流程设计与管理问题，导致敏感数据被不当获取；再者，因为安全管控措施落实不到位，导致敏感数据发生泄露，所以敏感数据难以得到保护。

智能安全 助推大数据引领时代发展

如何防护大数据时代下的数据安全？亿赛通高级安全顾问专家提出“智能安全”防护的新思路和方案。亿赛通全新“智能安全”解决方案是一套融合机器学习、大数据、数据分析、密码学、访问控制、语义分析、数据标识等技术的综合性数据安全体系，可以实现对用户数据资产进行事前主动防御、事中检测响应、事后追踪溯源、全程态势感知，协助企业构建全方位数据安全体系。

大数据时代，保护数据安全非常重要，亿赛通坚持用大数据构建“大安全”生态，利用前沿技术对企业敏感数据进行识别 ,提高敏感数据的识别精度 ,从而进行全方位智能防护。

新闻稿来源：亿赛通华中大区

网安则国安 亿赛通出席国家网络安全宣传周 合力共建网络强国

随着互联网的高速发展，网络安全成为各大行业、企业、个人等发展的重灾区。国家高度重视网络安全的问题，对此，出台了《网络安全法》，成为我国第一部网络安全的专门性综合性立法，具有里程碑意义。

亿赛通出席 2017 国家网络安全宣传周

9 月 16 日，由中央宣传部、中央网信办、教育部、公安部、中国人民银行等九部门于上海成功举办了网络安全宣传周大会。亿赛通作为数据安全行业的权威厂商、专家，一直坚持服务于中国数据安全领域的防护，通过不断的创新、突破各种新的挑战，用全新智能安全解决方案为国家各大支柱行业提供专业的服务，保障其数据资产的安全。为此，作为安全领域的领航者，亿赛通被邀请出席了本次大会。本次国家网络安全周是《网络安全法》颁发执行后的第一次网络安全周，党中央高度重视，具有极大的权威性。

用“智能安全”铸造网络强国

在“网络安全周”交流会上，各大企业、领导与亿赛通就网络安全防护问题进行了深度的交流。亿赛通坚持响应习近平总书记“网络强国战略思想”，贯彻《网络安全法》政策，积极维护网络安全，并且按照网络安全等级保护制度的要求，亿赛通履行安全保护义务，保障各大行业网络免受干扰、破坏、攻击，防止网络数据泄露或者被窃取、拷贝。对此，在“网络安全”技术、产品、研发上，亿赛通加大创新力度，应对各种新的安全挑战，为各大企业分享了企业数据安全智能防护方案和智能加密技术，博得众参会嘉宾的一致认可和称赞。

维护网络安全是一项长期任务，亿赛通作为数据安全领域的引领者，会一直坚持把数据安全这件事做到更好，努力保护好各大行业、企业、个人等数据资产安全。同时，也会继续带领数据安全领域稳健前行，不断创新，迎接更多挑战，满足不同客户的需求，坚持为国家数据安全作出自身最大的贡献，并携手国家合力共建“网络强国”。

某云存储惹祸？大量机密信息遭泄露？小贴士“智能安全”法宝让数据存储更安全

A：有媒体报道，亚马逊的云存储服务器又出乱子了

B：啊啊啊啊？不会吧，上次是被玩家上传小电影测试，信息被泄露，这次是咋回事？

A：据说这次是安全配置错误

B：信息泄露了吗？

A：报道称，安全公司 UpGuard 在亚马逊云存储上发现了文件中包含了一些美国军方和情报人员简历信息，还含有大量与美军合作的伊拉克、阿富汗公民的信息。很多资料已经被不少网友看到。

B：Oh, my God! 机密信息被泄露可能会被带来巨大的损失啊！有什么方法能避免无论是有意或者无意识机密信息被泄露的方案吗？

A：当然有了啊，亿赛通数据安全卫士和数据智能安全管理平台你知道吗？

B：听过啊，好像是刚新推出的两款智能产品，据说很屌呢，具体我不清楚，你能说说嘛？

A：是的，他们刚推出的智能安全新品，我首先介绍一下他们推出的“数据安全卫士”，这款产品主要针对个人重要数据实现智能安全加密，操作超级便捷，能保证咱们个人的数据在云盘存储、传输、外发等情况下数据安全。

B：哇喔，太棒了，我个人的很多作品需要加密保护的，他们这个产品有格式和文件大小的限制吗？

A：格式这个基本都能满足，数据安全卫士支持上百种格式呢，加密文件大小可是超级大啊 4T，所有足足够保密咱们的文件啦！

B：那另一款产品呢？

A：数据安全智能管理平台，这款产品是很对企业级的加密产品，能够智能防护、高效识别、并且采用业内领先技术，能够实现安全与效率的最大平衡。

B：666 啊，我怎么才能注册使用亿赛通产品呢？

A：喔，我把这个链接给你，很方便，很智能，很安全，你点击链接地址

http://www.2c.esafenet.com/index.html，查看详情哦！

B：好嘞，谢谢啦，这就去弄啦！

亿赛通数据安全智能管理平台

亿赛通数据安全智能管理平台（简称“DSIP”），是一款融合机器学习、大数据分析、文档加密、访问控制、关联分析、数据标识等技术的综合性数据智能安全产品，可帮助用户对结构化和非结构化数据进行数据治理、安全管控、态势感知，为用户的核心数据资产从终端、网络、存储、应用等全方位提供全生命周期保护，在确保组织敏感数据安全前提下，不管控、不影响非敏感业务开展的体验度，实现安全与效率的最大平衡。

亿赛通数据安全卫士

亿赛通数据安全卫士是针对个人 PC 端的重要信息或核心资料在外发、分享、存储中的安全需求而设计的个人版安全产品。当您需要将涉密文件发给他人时，接收者打开文件首先需要进行身份认证，方可阅读。并且发送者可对外发文件的使用者进行阅读次数、使用时长、内容拖拽、截屏等细粒度安全控制，从而有效防止重要信息在存储中，以及外发、传输给第三方时被有意或无意非法扩散。

又来两剂猛料？ 400GB ？半数美国人……敏感数据又遭泄露 好“惨”

作为“安全”防护小贴，

听到这样的消息，

小贴只想原地爆炸，

没错，是原地爆炸！！！

怎么搞的啊？？？

400GB ？？？半数美国人？？？

这么多的敏感信息泄露，

后果很严重，很严重，很严重……

有铁粉三脸迷茫？不知道小贴在生哪门子的闷气，

好，小贴再爆两剂猛料！！！

爆料 1

近日，相关媒体报道，墨西哥增值税退税网站 MoneyBack 因数据库配置错误导致大量客户敏感信息遭遇外泄。据悉此次数据泄露因一套 ApacheCouchDB 数据库存在配置错误而起，其中包含有约 50 万名客户的护照信息、信用卡号码以及旅行票据等等。专家们发现超过 400GB 敏感数据可通过网络进行公开访问，如此庞大的信息当中囊括有 45 万 5038 份扫描文档（包含护照、ID、信用卡以及旅行票据等等）以及 8 万 8623 条注册或者扫描形式的惟一护照号码。

爆料 2

美国信贷机构 Equifax 近日被黑客入侵了公司系统，导致了约 1.43 亿美国消费者的个人信息泄露，这也是近年来最大和最具威胁性的数据泄露之一。Equifax 披露本次黑客获得的信息主要包括姓名、社会安全号、出生日期、地址（这是申请信用最重要的四项信息）以及驾驶执照号码。此外，黑客还获取了大约 20 万美国消费者的信用卡号码。

Equifax 还发现黑客还获取了某些英国和加拿大居民的个人信息。

看完这些信息泄露的惨重事件，有铁粉说如果他们提前采取数据安全保护措施，就不会酿成今天的悲惨结果。小贴也想说，如果一切都没有发生，小贴一定把最牛亿赛通数据加密产品推荐给 MoneyBack、美国信贷机构 Equifax，然后，就算数据库配置错误导致数据泄露，就算黑客脑洞在大，数据丢失、窃取、拿走……亿赛通智能加密产品完全可以防护，让对方无法查看，无法获取。但是，没有如果，小贴只想说，就算没有如果，现在醒悟也不晚。无论企业或个人一定要意识到数据安全保护的重要性，一定要提前采用数据安全防护措施。

亿赛通智能安全产品，融合大数据分析、文档加密、访问控制、关联分析、数据标识等技术，可帮助用户对数据进行数据治理、态势感知、智能防护，为用户的核心数据资产从终端、网络、存储、应用等全方位提供全生命周期保护，从而做到事前预防、事中控制、事后审计于一体化防护，可效防止重要信息被有意或无意非法扩散，让客户再也不担心数据被泄密、存储不安全。

苹果 X 出来啦！
有人又开始打量自己的肾了！
还是亿赛通“安全”小卫士靠谱！
今日一波福利又降临

亿赛通数据安全卫士

产品亮点：注册简单 存储安全 加密分享

产品概述

亿赛通数据安全卫士是一款专门防止您的私人数据资产，在分享、外发、存储过程中，被他人非法窃取或使用的安全产品，该产品采用了高安全动态虚拟卷加密技术和细粒度权限访问控制，因此访问者只有经过合法身份认证后才可打开受控文件，可有效控制数据被非法扩散或二次使用，是 您“贴”身的数据安全小卫士。

产品优势

简单 易用 灵活 更安全 更可控 更智能

安全分享：让您的数据在外发或分享时，更安全、更可控（系统支持：xp/win7/win10）。

细粒度权限访问控制：可以对外发文档进行只读、打印、截屏、阅读次数、使用时长、自动销毁等控制。

多文件类型支持：多格式支持保障您的文件安全、轻松外发。如：文档类、音视频、设计类、图片类、代码类……

高度安全：采用高强度动态虚拟卷加密技术，外发文件在传输和使用过程中保持加密状态。

应用场景

主要应用于普通大众（个人 PC 端）和企业，针对重要文件、图纸、设计、作品、专利、视频 / 音频文件、财务报表、薪资等等数据在外发、传输给第三方或者网盘存储中数据的安全管控。

再也不怕个人知识产权被别人窃取了

再也不怕电脑丢失而使数据被泄密了

再也不怕个人网盘存储数据不安全了

注册使用

亿赛通“数据包安全卫士”会员注册详细介绍		
特权	普通用户	会员
价格	免费	46/月 | 366/年
多文件制作	支持	支持
单个文件大小	<=100M	<=4G
外发文件总大小	<=100M	<=1T
外发文件还原	不支持	支持
权限模板	不支持	支持
指定机器打开外发文件	不支持	支持

亿赛通数据安全卫士50个“激活码”大派送				
Y6xe	K76v	yPlD	4QtX	e3QW
ZRTQ	Thz2	yECO	cdpW	5sgN
BJRa	H9MN	VXrq	m1Dn	gLfM
YlQK	K6wU	r7Oa	WQ98	cjQ9
2eOa	P5yb	U8nR	Xhzt	27FK
iwzh	9Dvw	GxLh	Ums4	CBAQ
1SGW	RXnP	Mtft	UD2W	UemW
kI5M	03Th	81Mn	vzUD	GYzN
hEeu	bHEh	olVI	GU6I	uWK
ADEz	mNMG	zeSx	fLAl	y1Bc

亿赛通全新“智能安全”方案 为研发通讯产业发展护航 实现 安全即时通讯智能管理体系

研发通讯行业分析

信息化时代的企业都在最大化地利用信息技术以提高企业的运营效率，致使企业百分之九十的知识产权如：程序代码、设计图纸等，都是以电子数据的形式存在企业的内部网络中。研发通讯企业在制定安全策略与具体执行这些策略的能力之间还是存在很大的差距，现存的网络安全技术大都是对外防护的问题，而且没有构筑出一个能彻底解决企业内部网络安全问题的平台，所有以电子形式存在的企业知识产权信息均有可能会以电子邮件，文件传输等形式轻而易举地流出企业。如何才能有效的将网络安全防线，从企业网络的边缘扩展到企业所有的网络节点之上？如何控制企业内部人员的主动或非主动的泄密风险？如何从源头上保证涉密资料的安全？如何避免其他内网安全软件的各种漏洞？成为研发通讯中各个企业急需解决的首要问题。

客户需求

为提高研发通讯产业内部信息管理的安全性，实现内部核心源代码存储、流转安全可控，有效防止文件的扩散和外泄，需要建立一套完善的智能数据保密及授权访问系统，即对于企业内部电子文档，就其使用范围、用户权限、用户操作、文件流转进行智能控制管理，以防止文档内部核心信息非法授权阅览、拷贝、篡改。

综上所述，为了安全和效率的平衡点，构建内网数据安全可从以下几方面防护：

1）防止内部重要电子文档被泄密；

2）防止离职或内部员工泄密；

3）数据安全系统能否支持应用的复杂性；

4）数据安全系统是否改变应用习惯；

5）数据安全系统是否改变应用流程；

6）数据安全系统是否能保障应用的安全性；

7）数据安全系统是否能支持应用系统升级。

解决方案

亿赛通数据泄露防护（DLP）系统专为企业级用户设计的数据防泄密解决方案。它不但能够对源代码、Office等进行加密保护，并且能够对加密的文件进行细分化的应用权限设置。确保企业的机密数据只能被经过授权的人，在授权的应用环境中（例如企业内部），在指定的时间内，进行指定的应用操作，并且整个过程会被详细、完整的记录下来，以便您对数据的访问记录进行安全审计。

方案价值

可有效的提高员工的保密意识，并且配合企业现有的保密制度，企业核心代码、设计图纸、财务数据、重要数据等都可获得有力的保障，业务系统的安全也得到提升，从而促使研发通讯产业实现内部信息智能化的管理和业务系统的高效运转。

智能安全引领科技前沿
亿赛通深度打造烽火通信
“智能安全”屏障

客户简介

烽火通信于 1999 年 12 月 25 日成立，是国内优秀的信息通信设备与网络解决方案提供商，国家科技部认定的国内光通信领域唯一的“863”计划成果产业化基地和创新型企业，曾承担从“六五”到“十一五”期间光通信领域几乎所有的重大科研课题，累计取得了五百多项具有自主知识产权的重大科研成果，多次荣获国家、科技部、邮电部科技进步奖，是国内光通信领域中的龙头企业。

需求背景

烽火通信防扩散系统项目是烽火通信科技股份有限公司信息安全改造项目的重要组成部分。本次项目是通过对烽火集团内部运行环境进行安全改造，按照集团公司信息安全总体框架，全面提升系统的安全水平，对内网系统中的涉密数据达到事前有管理、事中有控制、事后有审计，规避信息安全事故风险。

解决方案

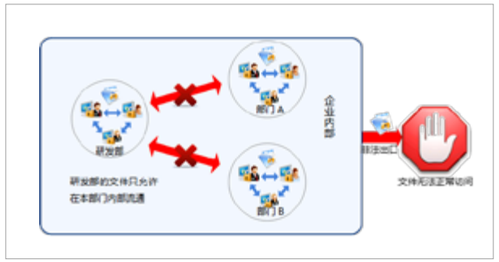
亿赛通智能加密产品具体帮企业实现了如下功能：

1. 对加密文件进行必要的权限管控，如复制，打印，截屏等，让使用过程更可控；对加密文件进行细粒化授权管理；让数据在合法可控的前提下提供给第三方使用，并可以对使用权限进行精细化控制；

2. 所有合法终端（已部署加密客户端）访问业务应用系统时，上传解密，下载加密，所有非法终端（未部署加密客户端）将禁止接入业务应用系统；

3. 系统采用驱动级透明加解密技术，对终端使用完全透明，用户无任何感知；

4. 研发数据脱离终端保护区域与外界交互时，系统可提供对外发文档进行加密保护和权限控制保护（如可实现对外发文档设置：只读、打印、修改、只读次数、过期销毁以及打印等）,防止重要研发数据外部非法二次扩散；



5. 系统提供详细日志审计功能，终端上用户对核心文档的相关操作（如打开、修改、删除、加密、解密等）系统均可完整追溯。

项目成果

1. 业务管理系统（PLM）的核心数据访问及存储安全，实现后端明文安全存储、前端密文安全访问；

2. 数据集中存储服务器的数据安全存储及访问，实现文件上传自动解密、文件下载自动加密；

3. 版本管理系统（SVN/CVS）的后台数据明文安全存储，并与联合编译工具、终端用户之间实现前端密文安全访问；

4. 不影响与应用系统相关的业务流程执行、业务效率；不改变应用系统部署架构，不改变应用系统后台数据存储形态和规则；不改变或不过多改变用户访问应用系统的工作方式习惯；

5. 提供完整、通用的集成解决方案，同时对不同应用系统进行统一集成，并具备有良好的拓展性，降低后续维护成本。