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：86-10-57933600

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　中国数据安全防护专家　www.esafenet.com

8 月刊

2018 年共 11 期

关注企业官方微信

Esafenet
Monthly magazines

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：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com

CONTENTS 目录

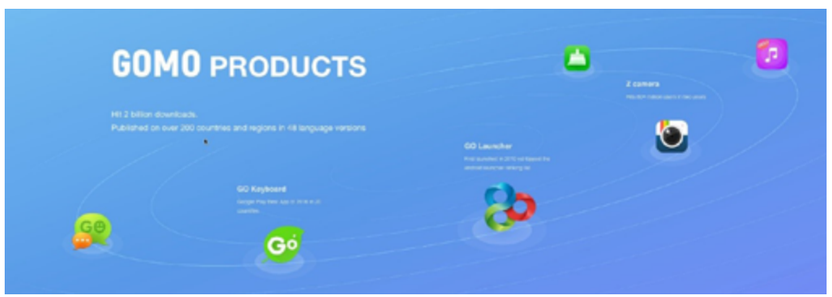
刊首语 PREFACE

《亿赛通八月刊》

近年来，安全事件逐渐成为媒体的宠儿，尤其是个人信息泄露、勒索病毒和黑客攻击事件，时刻牵动着众人的眼球。在公众关注度方面，从近两年的百度指数就能看出，“个人信息泄露”和“黑客”等关键词的整体日均值都在历史中高位波动，信息安全已经不仅仅是技术问题，而是关乎普罗大众的民生问题。与此同时，安全厂商的视角也在慢慢变化，厂商们不再满足于概念性的奔走呼号，真真正正化被动为主动，切切实实关注落地时效和响应时效。从最新发布的赛迪报告中也可看出，安全市场规模在逐年增大，企业用户对数据防护方面的需求日益加深，厂商们未来有较大的市场空间……

国内

1、5050 万久邦数码（GOMO）APP 用户的个人信息遭意外暴露



摘要：久邦数码（GOMO）是全球最大的手机工具软件开发商之一。旗下 GO 系列应用程序包括 GO 桌面、GO 短信、GO 输入法、极相机、S 相机、GO 音乐等，全球下载量超过 20 亿次。久邦数码的应用程序非常受儿童欢迎，这导致当久邦数码因备份配置错误而暴露了超过 5050 万用户的个人信息时，在这 5050 万用户中有很多是儿童。

2、香港卫生署遭勒索软件攻击，官方称暂无资料外泄

摘要：在上个月 20 日，来自联合早报网的消息称，新加坡最大的医疗保健机构——新加坡保健服务集团（SingHealth）的资讯科技系统在今年 6 月 27 日至 7 月 4 日期间遭到了黑客入侵。此次事件成为新加坡历史上“最严重的侵犯个人数据事件”，共造成 150 万名患者的个人资料被窃取，其中包括该国总理李显龙的开药记录。

3、30 亿条信息被盗窃 运营商如何负责用户数据安全？

摘要：根据新浪科技的报道，瑞智华胜及其关联公司整个操作的方法是，从 2014 年开始，他们用竞标的方式，与覆盖全国十余省市的电信、移动、联通、铁通、光电等运营商签订营销广告系统服务合同，为运营商提供精准广告投放系统的开发、维护，进而拿到了运营商服务器的远程登录权限。

4、侵犯公民个人信息形成黑灰产业链相关案件逐年增多

摘要：央广网北京 8 月 23 日消息（记者白杰戈）据中国之声《新闻纵横》报道，侵犯公民个人信息的案件数量逐年上升，形成了非法获取、加工、交易再用于实施犯罪的一条“黑灰产”链条。警方的统计数据显示，两年多来，各地查获的公民个人信息超过 1400 亿条，平均全国每个人有 100 多条信息泄露。

5、台积电不是最后一家！物联网连接数激增背后，隐患不断！

摘要：本月初，台积电遭遇前所未有的重创，“WannaCry”毒如其名，着实让人“想哭”。这个从去年就席卷全球的勒索病毒，曾有过威胁三十多万用户的“辉煌战绩”，造成的资金损失更是数以十亿计。

6、50 元就能买来明星身份证号码，还包教如何查航班信息

摘要：一位“黄牛”（文中特指明星信息贩卖者）还热心告诉澎湃新闻记者，花 50 元购买明星身份证号码，包教如何查询明星航班信息。记者花了好几个“50 元”，就买到了疑似邓超、李易峰、井柏然、易烊千玺等明星的身份证号码，还拿到了迪丽热巴最近的航班信息。记者通过权威渠道核对了其中部分明星的信息，证实不假。

7、30 亿条公民信息被窃，史上最大数据窃取案告破

摘要：如果你的微博关注列表突然出现一堆营销账号，QQ 突然被加进陌生群组，抖音莫名关注某网红，也许黑灰产团伙已经操控了你的账户。近日，浙江绍兴越城区警方成功侦破史上最大规模的数据窃取案，阻止 30 亿条公民信息泄漏。

8、沪一海淘平台信息泄露用户遇电信诈骗 警方及时拦截 38 万存款转账

摘要：两周前，家住浦东顾路地区的市民周女士遭遇惊魂一刻，电信诈骗人员详细掌握了她的个人信息，甚至连她购买眼药水的情况都一清二楚，并利用这些信息设局下套。危急时刻，浦东警方及时上门，阻止了周女士的转账，确保其账户内 38 万元存款安全。

9、小红书时隔一年再曝用户信息泄露诈骗，平台和第三方应如何担责？

摘要：近日，多名小红书用户在社交媒体上爆料，说接到自称小红书客服的电话诈骗，被骗金额从几千到几万元不等。骗子先通过准确说出详细的个人信息和购物信息取得用户信任，再以用户在小红书上购买的商品有质量问题，小红书将按照原价的几倍退款为由，一步步引导用户掉入精心设计的陷阱。

10、浙江省 1000 万学籍数据正在暗网售卖

摘要：8 月 1 日下午，威胁猎人通过暗网监测到，浙江省 1000 万学籍数据正在暗网上售卖。从暗网截图显示来看，售卖的学籍数据覆盖了浙江的大部分市区，被泄露的信息包含了学生姓名、身份证、学籍号、户籍位置、监护人、监护人号码、居住地址、出生地、学校名称等。

11、又双叒叕有医院泄露患者信息，演员林更新中招！

摘要：8 月 12 日，林更新通过微博怒斥“个别无良医务人员公开病人病历资料”。13 日，林更新工作室发出声明，澄清称林更新目前未婚，“相关不实言论纯属个别人员不负责任的错误填写、违法泄露住院记录、手术麻醉系统所涉个人信息造成”。

12、《延禧攻略》全集外泄，网友：5 元买全集

摘要：今年的暑期档热播古装剧《延禧攻略》已经收获了相当高的收视率，很多媒体放出一些消息，5 元可购买全集网盘链接。

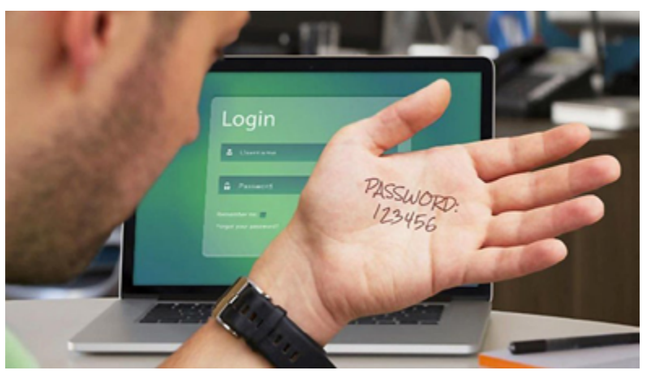
13、华住旗下酒店 5 亿信息疑被泄

摘要：此次泄露的数据数量则总计达 5 亿条，其中华住官网注册资料信息包含身份证、手机号、邮箱、身份证号、登录密码等，共 53G，约 1.23 亿条记录；入住登记身份信息包含姓名、身份证号、家庭住址、生日、内部 ID 号，共 22.3G，约 1.3 亿条；酒店开房记录包含内部 ID 号、同房间关联号、姓名、卡号、手机号、邮箱、入住时间、离开时间、酒店 ID 号、房间号、消费金额等，共 66.2G，约 2.4 亿条。

行业聚焦 INDUSTRY FOCUS

国外

1、黑掉政府网站有多难？ 26% 的西澳政府官员被曝仍在使用弱密码



摘要：西澳大利亚州审计长于本周公布的一份针对西澳大利亚政府的安全审计报告指出，大约有 26% 的西澳政府官员所使用的密码都被归类为“弱密码”，并且在来自 17 个政府机构的 23.4 万个密码中，有 5000 个密码都包含了同一个单词——“password”。

2、面部识别技术成为“照妖镜”，识别非法入境者真身

摘要：随着生物识别技术日益成熟，美国海关与边境保护局（后文简称 CBP）首先使用航班舱单和旅行者文件（主要是护照和签证）在美国境内的飞机上建立所有旅行者的照片库。杜勒斯机场是新的面部扫描技术的 14 个“早期采用方”之一，官方希望这将提高海关检查效率，未来能够普及到全球旅行。

3、垃圾电子邮件活动通过 BEBLOH 和 URSNIF 恶意软件感染日本用户

摘要：最新观察到滥用 IQY 文件的垃圾电子邮件来自 Cutwail 僵尸网络。活动以日本用户为目标，交付了 BEBLOH（检测为 TSPY_BEBLOH.YMNPV）和 URSNIF（检测为 TSPY_URSNIF.TIBAIDO）恶意软件。

4、屈臣氏旗下英国知名药妆店 Superdrug 近 2 万名顾客个人信息遭泄露

摘要：根据英国媒体《每日邮报（DailyMail）》的报道，有黑客在本周一（8 月 20 日）晚上联系了 Superdrug，称他们已经获得了大约 2 万名 Superdrug 顾客的详细个人信息。作为证据，黑客还向 Superdrug 展示了 386 名 Superdrug 顾客的个人信息记录。

5、 供应链攻击袭向韩国

摘要： IssueMakersLab 的安全研究人员发现了 Operation Red Signature，这是针对韩国企业的信息窃取驱动的供应链攻击。研究者在 7 月底发现了这些袭击事件后，媒体报道了 8 月 6 日在韩国发生的袭击事件。

6、 Microsoft Office Publisher 也遭黑客滥用，目标瞄准各大银行

摘要：近日，来自 Trustwave 的研究人员发现了一场目的在于传播 FlawedAmmyy 远程访问木马（RAT）的垃圾电子邮件活动。虽然规模不大，但极具针对性。从电子邮件的收件人地址来看，攻击者的目标似乎是各大银行。

7、 美国奥古斯塔大学因网络钓鱼攻击泄露 41.7 万份记录

摘要：再一次，又一起医疗数据泄露事件暴露了成千上万患者的隐私。这次，受害者主要是居住在美国乔治亚州的公民。据报道，奥古斯塔大学医疗中心（Augusta University Health）在去年曾遭遇了一次网络钓鱼攻击。令人遗憾的是，最新调查结果显示这次攻击导致约 41.7 万份记录遭泄露。

8、 黑客组织 TA505 意图攻击金融机构，利用新型恶意软件 Marap 收集情报

摘要：来自网络安全公司 Proofpoint 的研究人员最近在一场规模相当大（数量达到数百万封）的垃圾电子邮件活动中发现了一种新的恶意软件，主要针对了金融机构。这种被称为“Marap”的恶意软件不仅能够收集系统信息，而且具备下载其他模块或恶意软件的能力。

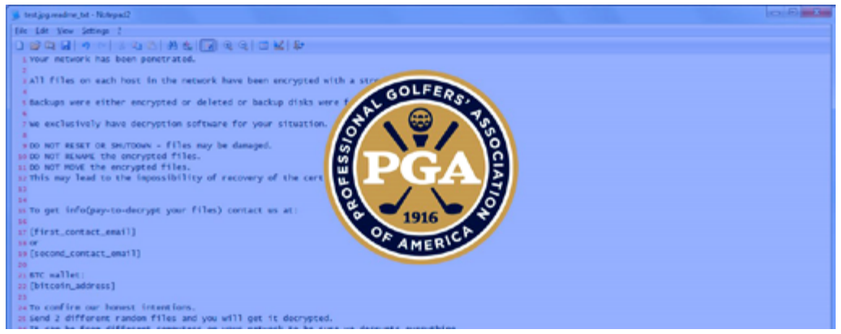
9、 全美第二大互联网服务供应商 Comcast 意外暴露 2650 万用户个人信息

摘要：据发现安全漏洞的安全研究员瑞恩·史蒂文森（Ryan Stevenson）称，Comcast Xfinity 无意中暴露了超过 2650 万名用户的家庭住址和社会安全号码。隶属于这家全美第二大互联网服务提供商的在线客户门户网站上被发现存在两个此前未被报告的漏洞，这使得即使是不具备太多专业技能的黑客也可以很容易地访问这些敏感信息。

10、双尾蝎（APT-C-23）仍在使用 Android 恶意软件攻击巴基斯坦政府实体

摘要：在一年多以前，双尾蝎组织（APT-C-23）开始在中东地区传播其 Android 恶意软件（主要针对的是巴勒斯坦的教育、军事等机构）。从最新发布的一份调查报告的来看，该组织仍在针对巴基斯坦人实施攻击，并在攻击中使用了新的 Android 恶意软件变种。

11、美国职业高尔夫球协会 遭 BitPaymer 勒索软件攻击



摘要：根据 GolfWeek 的报道，美国职业高尔夫球协会办公室的计算机遭到了勒索软件感染。当赎金票据于本周二出现在他们的计算机屏幕上时，受害者才意识到自己被感染了。赎金票据写道：“你们的网络已经被渗透了，网络中每台主机上的所有文件都已经被我们使用一种强大的算法进行了加密。”

12、英空军 F-35 战斗机项目资料失窃，俄罗斯和中国成首要怀疑对象

摘要：据英国《每日邮报（DailyMail）》报道，因为一场“网络美人计”，英国皇家空军（Royal Air Force，RAF）价值 90 亿英磅的 F-35 战斗机项目的机密资料遭到泄露。据调查，间谍人员盗取了英国皇家空军一名现役女飞行员的Tinder账号，并以她的身份添加那些参与 F-35 战斗机项目的英国皇家空军机组人员为好友，进而诱使他们透露有关 F-35 战斗机的机密资料。

13、澳大利亚 SA Health 医院意外暴露 7200 名儿童个人资料

摘要：在上周六，澳大利亚 SA Health 在其官方网站上发布了一篇新闻稿，称旗下位于澳大利亚第五大城市阿德莱德的妇女儿童医院（Womens and Childrens Hospital）因工作人员操作失误，意外暴露了约 7200 名儿童的医疗记录和个人资料。

14、Palo Alto：不明黑客利用 Bisonal 恶意软件攻击俄罗斯和韩国企业

摘要：Palo Alto Networks 公司旗下 Unit 42 威胁研究团队在近日发表的一篇博文中指出，他们于今年 5 月初发现了一场针对俄罗斯和韩国企业的攻击活动，至少有一家俄罗斯国防公司和一家不明身份的韩国机构成为了目标。

行业聚焦 INDUSTRY FOCUS

15、卡巴斯基：俄罗斯 400 多家工业公司遭遇鱼叉式网络钓鱼攻击

摘要：卡巴斯基实验室 ICS CERT 的研究人员在本周三（8 月 1 日）发表的一篇博文中指出，该团队发现了一系列带有恶意附件的网络钓鱼电子邮件，主要针对的是与工业生产相关的俄罗斯公司和机构。大约有 400 家与工业生产相关的公司成为了此次攻击的目标，这包括制造业、石油和天然气、冶金、工程、能源、建筑、采矿以及物流等。大约有 800 名在这些公司工作的员工遭到了攻击。

立足金融业，实现纵深防护效果！第二十六届国际金融展亿赛通大放异彩

第二十六届中国国际金融展盛大开幕

第二十六届中国国际金融展已于 2018 年 8 月 23 号在北京展览馆正式开幕，亿赛通携手绿盟科技在本次展会上展出的金融行业整体解决方案，将为行业客户诠释金融行业的“科技新发展，创新新气象”。

中国国际金融展是国内主要金融机构参与的国际性金融展览，有“中国金融第一展”的美誉。在绿盟科技 & 亿赛通智慧安全展示区，亿赛通专家现场讲解企业在金融行业的信息安全研究成果、金融行业面临的信息安全风险和信息安全需求，带领到场嘉宾感受亿赛通电子文档安全管理系统、数据泄露防护系统、金融行业解决方案等技术方案。通过展览，与众多业内客户一起探讨、交流、交朋友，共同推进国内金融科技的进步。展览共计 4 天，绿盟科技 & 亿赛通备受关注。

电子文档安全管理系统（CDG）

电子文档安全管理系统（简称：CDG）是一款电子文档安全防护软件，该系统利用驱动层透明加密技术，通过对电子文档的加密保护，防止内部员工泄密和外部人员非法窃取企业核心重要数据资产，对电子文档进行全生命周期防护，系统具有透明加密、主动加密、智能加密等多种加密方式，用户可根据部门涉密程度的不同（如核心部门和普通部门），部署力度轻重不一的梯度式文档加密防护，实现技术、管理、审计进行有机的结合，在内部构建起立体化的整体信息防泄露体系，使得成本、效率和安全三者达到最优平衡，实现电子文档的数据安全。

数据泄露防护系统（DLP）

数据泄露防护系统是基于内容识别技术，对设计图纸、源代码、合同文本、财务报表等敏感文件进行数据安全保护，防止通过邮件、聊天工具、网盘、U 盘拷贝、打印等途径泄露数据，对用户泄密行为进行记录、告警、阻断，并对用户行为进行审计。有效识别敏感数据，监控敏感数据使用情况，防护敏感数据外泄。有效培养并提高员工对敏感文件的保密意识。

亿赛通金融行业解决方案智能洞察行业需求，有机地融入银行业务流程，方案以智能分级、中间件、终端防护等手段，推进金融新服务、新产品，保障新业务模式的探索与创新。同时，亿赛通还致力于按照级别设计，配合金融业务流程进行创新改良，以保证传统银行网点升级后的信息安全，为客户提供更智能、更便捷、更全面的安全服务。

近年来，各类安全事件频发，个人信息泄露、银行资金窃取和勒索病毒的攻击利用等事件，都牵动着众人的眼球。网络安全和信息安全已经不仅仅是一个技术问题，而是关乎普罗大众的民生问题。在传统银行网点不断改革、全面提升人工智能与业务创新的新时代，亿赛通作为数据安全金融行业解决方案供应商，将秉承着“服务客户、持续创新、勇担责任、专业至上”的宗旨，继续坚持自主创新，树立自主品牌，成为金融科技领域数据信息背后有力的保护者，为我国金融行业的创新建设做出贡献！

部分客户

1、中信银行 / 证券股份 / 资产管理有限公司
2、招商银行
3、长城证券有限责任公司
4、中国国际金融股份有限公司
5、泰康资产管理有限责任公司
6、华夏基金管理有限公司
7、民生银行
8、上海浦东发展银行股份有限公司
9、新华人寿保险股份有限公司
10、九江银行股份有限公司
11、宁波银行
12、广发证券股份有限公司
13、中国人民财产保险股份有限公司
14、中国建设银行
15、山西证券股份有限公司
16、北京华控投资顾问有限公司
17、方正资本控股股份有限公司
18、泉州银行
……

亿赛通数据泄漏防护全系列产品成功入围 2018 央采供货协议

日前，2018-2019 年中央国家机关信息类产品（硬件）协议供货采购项目（以下简称为“央采”）中标结果公示结束，亿赛通数据泄漏防护（DLP）系统全系列产品顺利入围，继 2017 年成功中标后再次入选。体现了亿赛通在以技术为基础的数据安全领域强大的产品研发和服务保障能力，也代表着政府行业权威机构对亿赛通产品能力的认可与肯定。


中央政府采购网
www.zycg.gov.cn

2018-2019年中央国家机关信息类产品（硬件）和空调产品协议供货采购项目中标公告

时间：2018-07-24 17:28:36　　发布：佳宇华　　点击：4586

【字体：大 中 小】 打印本页

2018-2019年中央国家机关信息类产品（硬件）和空调产品协议供货采购项目中标公告

1、项目名称：2018-2019年中央国家机关信息类产品（硬件）和空调产品协议供货采购项目

2、项目编号：OC-H61180392

3、招标公告发布日期：2018年6月11日

4、变更公告发布日期：2018年6月27日

5、开标日期：2018年7月12日

本次采购是由中央国家机关政府采购中心组织，是中国政府采购领域级别最高的采购项目之一，覆盖了国家机关、事业单位和社会团体等数万家单位，一直以高标准、严要求、规范化而著称，对于入围厂商的产品品牌、市场口碑、产品品质、技术含量、售后服务均设置了国家级门槛，旨在确保厂商具备提供优质服务的能力，同时也是地方政府采购的风向标。经过严格的检测和评审，亿赛通自主研发的数据防泄漏系统全系列产品，在功能、性能、安全性、可用性等方面，都能够满足中央机关单位在数据安全防护方面的使用需求。


中央政府采购网
www.zycg.gov.cn

今天再次中标央采项目，充分证明政府对亿赛通在数据安全领域的高度认可。同时，在伴随着中央政府对于本土化自主研发产品的采购需求逐步加大，国产化要求越来越高，数据安全产品也被赋予了越来越多的职责。构建以数据为中心的新安全防护体系，不仅是数据安全技术的发展方向，也是我国安全界从领导到专家的普遍共识，其基础和核心地位愈加凸显。本次对外公布的招标内容中，网络安全相关项目备受瞩目。网络安全在近些年进入发展快车道，落地项目呈逐年增加的态势。从本次央采公布结果，可以看出国家对网络安全的大力扶持。。相信在政府的领导下、企业的支持下，网络安全行业潜力愈发巨大。

截止到目前，亿赛通已获得多个资质认证，产品涵盖终端、网络、应用、存储、介质和云服务六层防护，上百项知识产权和几十个数据安全软硬件产品。同时为为国家各企事业单位提供数据泄露防护产品，得到国家直接管辖的各个领域机构的高度认可。

智能化时代发展之际，各行各业都与数据信息深度捆绑，数据安全无疑成为各大领域发展的当务之急，各个行业都应重视起来。在未来，亿赛通将继续数据做数据安全领域的引领者，为各行业客户提供安全稳定的数据防泄漏安全服务，亿赛通的未来之路会越来越好！

“设计•融合”2018 山西设计行业数据安全研讨会顺利召开

设计业与互联网如何融合发展？

设计行业作为国家传统行业之一，基础扎实，转型升级愿望强烈，设计企业对互联网应用有庞大的市场需求。为了数据安全和设计业的融合创新实践，2018 年 8 月 24 日，亿赛通在太原成功举办了“设计·融合”2018 山西设计行业数据安全研讨会。会议着重分享了设计业与互联网跨界融合创新模式和实践成果，研讨融合创新发展新路径，加快设计信息建设，举办该活动对推动设计业转型升级，具有特殊意义。

设计•融合 信息安全是核心

随着互联网加速与传统产业融合，互联网新技术和新模式不断催生孕育新的经济增长点。推动设计业与互联网融合，有利于形成叠加效应、聚合效应、倍增效应，加快新旧发展动能和生产体系转换。设计业与互联网融合创新是作为产业探索转型发展之道的重要选择，是志在必行的前进方向。

我们了解到，设计行业在大力发展信息化的同时，在远程异地办公、设计应用图纸和协同办公等领域，已逐步形成了一整套覆盖设计行业各个业务流程和管理领域的信息化体系，完全依赖于计算机和网络技术。因此在设计企业的局域网内存在着大量重要数据信息资料，这就使得数据安全变得尤为重要。

本次分享大会在重视“设计与互联网”融合发展的同时，特别强调了信息安全是核心问题。如何保障企业在融合互联网和设计行业的创新实践中信息安全运行？亿赛通精英伙伴在大会上讲到，作为中国的数据防护企业，亿赛通研发的数据防泄漏体系强力支持和保障设计行业的数据安全问题。通过推动建立设计业与互联网融合发展新生态，充分释放互联网的力量，改造提升传统动能，加快推动产业信息化增效升级，亿赛通有责任去保障广大企业降低核心信息资产的有意或无意泄密风险，提高互联网信息安全水平，为企业在互联网的创新发展下，提供一个健康安全的环境。

通过亿赛通精英伙伴详细透彻的介绍，现场嘉宾对其产品和方案产生了浓厚的兴趣。在大数据信息时代，亿赛通从未止步，在数据安全领域特别是数据安全产品和数据安全解决方案市场稳居市场前列，并在国内的安全市场占据了一席之地。在核心技术上，坚持创新，拥有业内前沿的技术，带领行业前行。亿赛通数据安全防护产品及方案，坚持通过精心的顶层设计和完善的基础建设，并且从技术、服务、智能化管理手段等方面共同着手，结合人工智能、云计算、区块链等新兴技术做出努力，助力更多企业拥抱互联网，实现转型升级。对于未来几年内数据安全市场的发展趋势、面临的挑战等一系列问题，我们也深入的和现场嘉宾进行讨论。同时，相信在公司的发展下，将为客户提供更加完善、更加周到的数据安全保障服务，不断为广大用户带来更多惊喜！

守护医疗信息安全，亿赛通出席上海医药行业数据安全建设交流会

2018 年 8 月 23 日，由医谷携手亿赛通公司举办的“2018 智时代·新安全上海医药行业数据安全建设交流会”在上海国际医学园区成功举行。本次活动邀请到数名业内专家分享医药行业数据安全建设行业管理经验，共有来自医药行业的近百名高管、IT 部门人员参会。亿赛通公司具备企业级安全服务资质，一直深耕数据安全行业 15 年时间，积累了众多客户与行业经验，本次大会受邀会中进行了精彩演讲。

亿赛通动态 ESAFENET NEWS

当前，医疗行业信息化建设方兴未艾，伴随移动医疗、智能设备和云端解决方案等智能化建设持续升温，以医疗管理信息系统、临床信息系统、医院运营管理系统等信息化设备为体系的医院信息集成平台正面临着数据泄露、黑客入侵、非法登陆等信息安全挑战。如何按照国家相关规定落实信息安全等保工作，建立完善的医疗信息化安保体系，以确保医疗信息系统和网络安全成为众多医疗机构所面临的难题。因此医谷携手业内主流 IT 厂商群策群力，会议中为医疗信息安全建设提出了优秀的解决方案及建设性意见。

应对当前医疗行业常见的患者医疗数据泄露、黑客入侵医疗设备以及移动医疗信息安全难题，北京亿赛通技术部专家为参会大众带来了企业数据资产安全防护案例，介绍了市面上常见的数据防泄密产品，包括数据隔离、数据分级、数据识别，并以签约典型医疗行业客户为例阐述各个企业在数据安全建设工作中值得借鉴的经验。

他表示，医院信息系统以及信息数据泄露直接影响到医疗信息化安全建设，立足实际，从全局角度出发，构建起以数据安全防护、移动安全防护与行为追踪等为体系的智慧医疗全局态势感知与监管架构，才能为打击医疗黑产源头，维护医疗信息数据安全，确保医疗信息化安全建设提供稳定可靠的技术支撑，确保医疗信息化建设安全稳步推进。

作为国内领先的数据安全厂商，应对医疗信息化安全建设难题，亿赛通通过对医院信息化现状调研、分析，研发覆盖数据安全、系统安全等多方面的医院信息数据安全解决方案，以提高医院信息系统管理水平，减少安全隐患，保障网络和信息数据运行安全。目前，亿赛通数据安全解决方案已在全国多个地区的医药企业得到广泛应用，并获得了广大用户的充分认可。

亿赛通走进河南 CIO 俱乐部，数据安全新理念引企业 CIO 共鸣

8 月 4 日，由河南省 CIO 俱乐部主办，北京亿赛通科技发展有限责任公司、中国联通洛阳分公司协办的 2018 河南 CIO 夏季峰会在云台山—云台天阶国际饭店盛大开幕。本次峰会聚焦了河南省各企业 CIO，共同探讨“软件定义一切”、“数据驱动管理”、“安全保障发展”的行业规律。亿赛通作为河南省众多企业的合作伙伴受邀出席，分享企业在工业信息化环境下，如何保障核心数据资产的安全，以及在大数据、物联网、云计算、移动应用等最新信息技术的应用中，CIO 领袖们所面临的数据安全建设、肩负的数据安全使命等问题。

融合创新、智能安全已成企业新时代下的未来趋势、广泛大数据平台建设后企业深刻认识到数据安全重要性的背景下，简单数据防护已不能解决现阶段企业的问题。数据安全正在从管控型向服务型转变，于众多企业而言，大数据治理的目标是提供统一智能的数据工作环境，建设和布局安全的工业互联网平台。

本次论坛期间，主办方邀请亿赛通参加了主题演讲，并为行业众嘉宾交流分享了数据安全领域的经验之谈、行业发展情况。以及亿赛通资深顾问也为与会的各大行业精英人士在“细说 2018 年的数据安全与数据泄露防护”进行了实践分享。并介绍到：当前工业信息安全已成为制造强国和网络强国建设的重要基础支撑，已成为工业互联网发展进程中的“必修课”，是工业互联网健康发展的重要前提。

数据被誉为新世纪的“石油和矿产”。足以说明，“数据”是企业非常重要的资产，一旦泄露，意味着企业面临巨大的灾难，甚至破产的可能。那么企业的数据威胁来自哪些方面？主要分为两个方面，其一是来自外部的威胁，其外部威胁的主体为黑客、恶势力、竞争对手；盗取方式为漏洞、病毒、木马、社会工程；他们的行为是攻击、窃取机密信息或商业秘密。其二，内部威胁的主体通常是内部人员；泄露方式就是利用工作的便利“拿”；其行为同样是破坏、窃取机密信息或商业秘密……

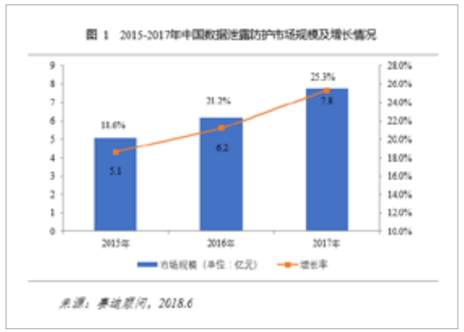
亿赛通丰富的技术积累，依托“知、识、控、查”的四大建设思路，通过统一的数据工作环境，为企业提供多种数据安全服务。结合会上的焦点论题，专业人员分别从数据泄漏途径、目前的安全形势、技术水平等方面进行考虑，为企业提供一套周密的安全保护方案，最终实现资源的有效配置，清晰、明了的规划思路，赢得了与会人员的高度称赞。包括在场的河南省领导以及河南省各企事业 CIO 等领导，就两化融合，数据安全管控等问题与亿赛通进行了深入交流和探讨。

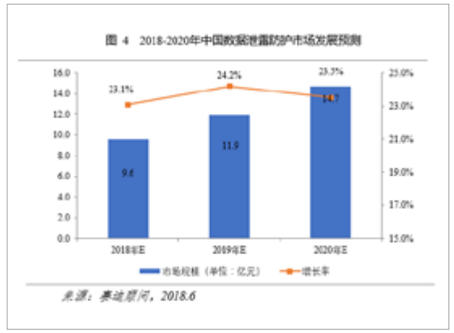
目前北京亿赛通科技发展有限责任公司已经在河南地区发展多个战略合作伙伴，同时公司非常重视自主研发，业务涉及到设计制造、金融、党政军……等行业，无论是产品质量还是公司员工的服务质量，均获得客户以及同行业人士的交口称赞！

2018 年数据泄露防护市场格局分析：亿赛通占据强势地位

市场潜力巨大

近日，国内一线权威媒体赛迪顾问股份有限公司调查研究的《中国数据泄露防护产品市场研究报告》新鲜出炉。这份 DLP 市场报告通过大量的实践调查和研究，系统、专业的分析了当下国内 DLP 市场发展状况、行业竞争状况、以及未来发展潜力。那么，在互联网等迅速发展的大背景下，数据资产的安全已经上升到各行各业发展的重要战略层面，DLP 作为一套完整的体系，用以解决不同类型用户的不同需求，促使中国数据泄露防护市场保持快速增长。即 2017 年，数据泄露防护市场规模达到 7.8 亿元，同比增长 25.3%（如图 1），同时，在国家政策的大力支持和重视下，数据安全需求不断扩大，预计 2018 年我国数据泄露防护市场规模将达到 9.6 亿元，同比增长 23.1%（如图 4）。

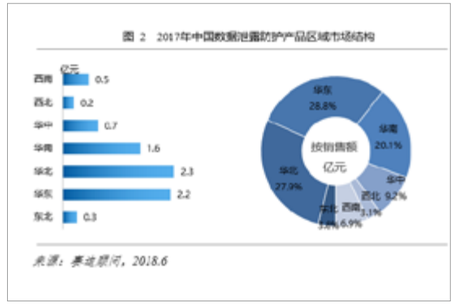




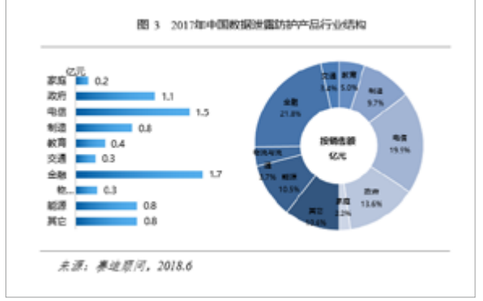
政策支持激发市场活力

从全国范围看，数据安全产业正处于快速发展阶段。随着中国数据信息化的不断发展，广大企业对数据安全的重视程度也日渐提升，中国的数据安全产业开始进入高速发展时期。产业信息化为数据安全产业提供了极具潜力的市场，数据泄露防护产品的不断突破则成为支撑产业发展强有力的技术保障。数据资产信息化、互联网技术的普及，给数据泄露防护市场带来新的变革。

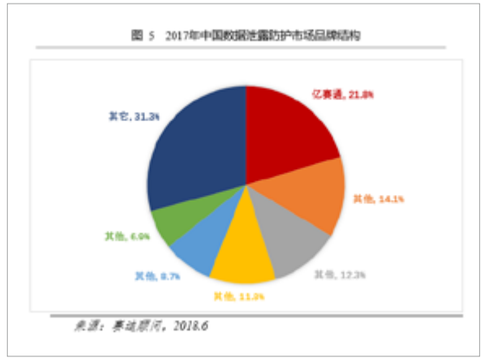
此外，国家持续提升在政策上对 DLP 的扶持力度，也进一步激发 DLP 市场的活力，制定了各种标准和法规，明确国家秘密、商业秘密以及个人隐私的保护。各项政策和支持均为数据安全产业营造了有利的发展环境。预计到 2020 年，中国数据安全产业总规模将超过 14.7 亿元。



从各项调查数据显示中，我们不难看出 DLP 产品已经成为安全行业主流产品。并且通过调查发现 2017 年依然是华北、华东、华南地区保持较高的市场规模（如图 2），对安全方面的需求较大。细分到具体行业来看，金融行业、电信行业、政府等关系到国计民生的行业，是数据泄露防护的主导市场。此外，能源行业、制造业方面随着对数据安全的认识逐渐加深，数据泄露防护产品未来有较大的市场空间（如图 3）。



那么，随着近年来数据安全需求强烈的同时，DLP 市场竞争也越发激烈，国内的数据安全防护（DLP）细分市场划分为两大类：一类是专项的数据安全提供商（如亿赛通等）；另一类是从传统防火墙、IDS、防病毒领域拓展切入 DLP 领域的服务提供商，这些数据安全品牌企业努力开拓创新，保障好各大行业的数据资产安全。其中，亿赛通在数据泄露防护领域的布局早，市场推广力度较大，2017 年，亿赛通的 DLP 市场占有率排名第一，而其他品牌企业依靠其在传统安全、硬件防护、管理平台、数据分析等方面的专业性优势，在数据泄露防护领域拥有比较稳固的市场地位（如图 5）。所以，在激烈的市场竞争格局下，促使 DLP 产品逐步标准化，技术门槛逐步提高，市场集中度也逐步提升，安全厂商加强实力、加大创新，显得尤为重要。



DLP 厂商竞争激烈

近些年来，由于国外的数据防泄露产品主要针对的是防丢失的方面，而国内则更侧重于防泄密，防护数据在全生命周期的安全性，更符合中国的国情，强制有效的保护数据，是国内 DLP 市场明确的需求，也是国内 DLP 所具有的战略性优势，因此国内产品的销量在逐年上升当中。

中国作为全球最大的“信息化产品”市场之一，未来三年，我国的数据泄露防护市场将持续处于高速发展阶段，增速保持在 20% 以上，DLP 行业发展前景将大放光彩。同时，“大数据”的时代已经到来，数据安全成为核心资产信息化的重要目标，代表了未来产业发展方向，既是国家政策大力扶持的重点，也是当下市场的热点。结合大数据分析技术，推动数据泄露防护的智能化发展，DLP 产品将实现用户行为分析与数据内容的智能识别，实现数据的智能化分层、分级保护，并提供一个体系化的安全解决方案。产品在为企业提供便捷服务的同时，客户也给数据安全行业带来新的发展契机，市场前景值得期待。

注意！最新朋友圈套路来袭，“砍价”有风险，帮忙需谨慎

从年初开始，微信朋友圈中兴起了一股砍价热潮

活动方宣称，只要将想要的商品链接分享到朋友圈

邀请微信好友进行砍价

就可以不花一分钱，直接把商品带回家

世上竟有如此好事！

因此不少网友选择将活动信息转发到微信

没想到，能拿到商品的寥寥无几

大部分网友最终都落得个竹篮打水一场空

更有甚者，还陷入了微信诈骗的陷阱

白忙活：砍到 0 元，却领不到商品

“我距离免费拿这套化妆品就只剩 100 元了，麻烦大家来帮忙砍一下价！”张小姐日前就发动朋友们“帮砍一刀”，以便赢取免费获得一套化妆品的机会。然而等到她邀请了所有朋友，将化妆品“砍”到 0 元，后按规定提交了个人信息后，却没领到所谓活动方寄来价值 1999 元的化妆品，联系客服也没有得到任何回应。

“我所有加入的群都发布了这条信息，总共有几百名微信好友一起帮忙砍价，还发动了朋友的朋友帮忙，最终，这套化妆品被砍到了 0 元，但是却没有得到物品，白忙活一场。”张小姐说。

好无奈：参与砍价信息被泄露

年初时看见自己的好姐妹们都在玩砍价免费拿的活动，一时心痒的李女士很快也在好姐妹的劝说下参加了活动。

“点开页面，要求我输入手机号和个人身份证信息进行实名制注册，我一开始有点怀疑，但看身边的人都照做了也没什么影响，就照做了。”好不容易等到验证程序过关，李女士开始转发链接。但她很快发现，所谓的砍价暗藏玄机，即使你成功将其砍到 0 元，但是由于参与人数的限制，只挑选前十位幸运网友发放商品。

意识到可能是个骗局之后，李女士删掉了该条朋友圈，但是没想到几天过后，李女士身边的不少好友发来信息，称都收到了留有李女士姓名发来的借钱短信，而李女士也频频接到某贷款机构打来的骚扰电话。

李女士这才知道自己的个人信息可能被泄露了。于是李女士怀疑，可能是参加的“砍价”活动泄露了自己的信息。

心好累：匿名砍价群 骗取入会费

如此高额的利润诱惑，很多人都乐此不疲地尝试，但是人脉的限制导致砍价失败，为此一些人选择加入砍价互助群。李先生告诉记者，自己在转发砍价链接后，看到有人在自己的微信底下评论，可以帮忙拉自己进专门帮忙砍价的群。考虑到自己的商品需要砍价的次数，李先生被人拉进了一个砍价互助群。

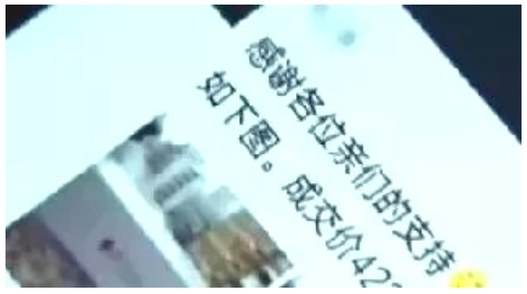
“群里有 300 多人，很多人都在里面分享自己的砍价链接。”刚一进群，李先生就被一个自称为是群主的人艾特了，群主表示在群里砍价有先来后到的顺序，李先生刚进群，只能先帮人砍价后找人帮忙。考虑到自己的砍价时间有限，李先生添加了群主说明情况。没想到群主表示，要想优先让人帮忙砍价，必须先发红包。

李先生考虑了一下，就给群主私发了 20 元的感谢红包，没想到红包刚被领取，李先生就被群主拉黑，移出了群聊。“虽然损失的钱不多，但是吃一堑长一智，不能轻易相信网上的陌生人。”最终李先生也没能成功拿到商品。

很费神：优惠幅度有限

有部分人的确通过“砍价”活动获得了一些实惠。市民刘先生介绍，之前在买电器时看到只要下载该电器品牌的app，邀请朋友砍价就可以额外得到一些优惠。

刘先生说，虽然不能零元购机，但只要转发到微信群中，通过别人帮助砍价，还可以得到最高 500 元的实惠，由于每人只能帮刘先生“砍”几毛钱到几块钱，最终也只是比原价便宜 300 元左右。谈到砍价，刘先生表示很费神。



据介绍，事实上，微信“帮砍价”活动起初只是用于营销。不少商家通过这种活动吸引人们在朋友圈转发关注，从而吸引了一大圈粉丝，短时间获得了大量关注度，实现不错的营销效果。

但是后来，这种成本低，操作简单，而且受众容易上当的的活动给不法分子盯上了，通过朋友圈砍价，收集个人信息和骗钱，演变成了一种新型的骗局，充斥着整个朋友圈，参与过的用户会收到大量的广告短信和诈骗短信。

这几种微信陷阱需警惕

1、微信红包别乱抢

有种“红包病毒”，设计的页面跟微信钱包十分相像。红包一旦被点开、输入手机号码，即被安装木马程序，自动窃取手机里的通讯录资料，并冒充中毒手机号码给朋友发送“红包病毒”短信，让朋友中招。一旦输入银行卡信息，木马程序就会转走卡内资金。面对“微信红包“，一定要分辨链接是不是第三方的，如果第三方，就有可能是假红包，最好别点。

2、免费清理僵尸粉

清理僵尸粉，结果很有可能会出现微信号被盗、好友信息被窃取，甚至手机会中木马病毒等严重后果。

3、微信群别乱进

微信让我们找到了失散多年的老同学、老同事，不知不觉微信里面全是各种群聊，也不记得谁给你拖进去的，也不知道这群都是干嘛的。有个案例，一个公司的会计，进了一个公司群里，结果除了自己，别人都是假的，稀里糊涂地给冒充老总的骗子转了钱！

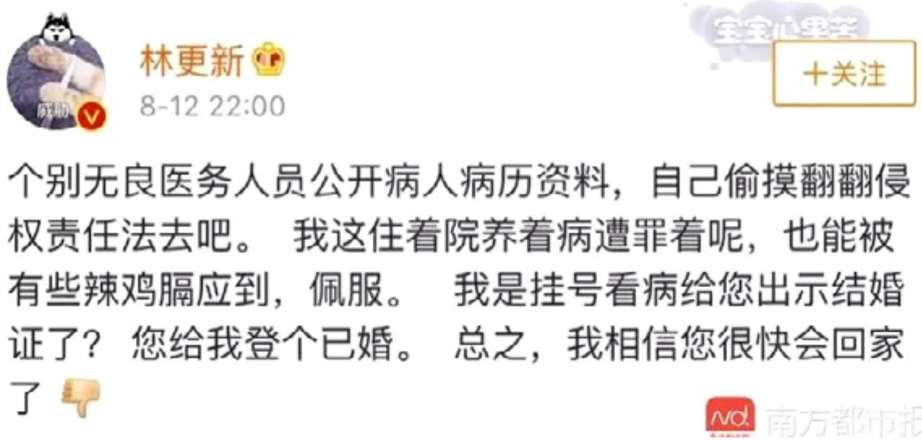
4、链接别瞎点

微信群中，陌生人发送的链接、二维码截图、压缩包等一定不要点击；安卓系统的微信用户收到后缀名为 .apk 的文件，一定谨慎点击下载和打开。

亿赛通小贴士提醒

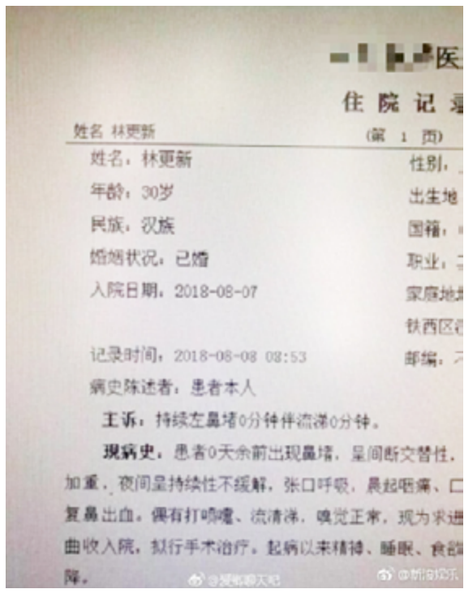
大家要对朋友圈发布的砍价赢大奖类似的营销保持高度警惕，切勿轻易填写个人信息，特别是敏感信息千万要谨慎填写；对于要求转账汇款的一定要核实好对方具体身份后才汇款。在遇到诈骗后一定要保存好聊天记录、转账汇款后及时报警。亿赛通 -- 中国数据安全防护专家，肩负国家数据安全、企业数据安全、个人数据安全的保护使命，为您提供全面而周到的安全服务。

麻醉医生曝光患者信息，林更新怒斥无良医务人员



林更新是大家熟知的演员，特别是从《楚乔传》播出之后，更是进入一线大咖的行列。但是人红是非多，日前，林更新在微博上公开怒斥某医院医生泄露个人信息，这一消息在网络上疯狂传播。

我们都知道林更新是演喜剧出身，本人礼貌幽默，经常在微博上和大家互动。从未听说林更新公开斥责某人，此次突然爆出的病历隐私，让他本人和粉丝都无法接受，并且最重要的是，这又是一次“内部”人员泄露个人信息事件，网友们纷纷表示“不能忍了”！



从被曝的病历中看，姓名到家庭住址，全部无打码曝光。泄露者是医院医生，据说，这个医生是林更新的粉丝，利用职务之便就偷偷地照下了林更新的病历。

公民的隐私权和个人信息在法律中明确规定：病历属于个人敏感信息。根据执业医师法，医师在执业活动中应保护患者的隐私，如果泄露患者隐私造成了严重后果，还须承担法律责任。


中日友好医院关于患者隐私泄露事件的声明

近日，林更新先生在我院就诊过程中，病历资料被泄露，给林更新先生造成了伤害与困扰。事件发生后，医院密切关注，深度重视，内部立即进行调查核实，目前仍在进一步调查中。

关于病历首页中林先生婚姻状况，系医务人员未完成的病历模板，现经与林更新先生本人核实，其婚姻状况为：未婚。

通过此事件，我们将加强患者信息安全的管理工作，同时采取相关措施，切实改进工作机制与流程，避免同类事件再次发生。

中日友好医院

2018. 08. 14

医院及时回复

此次事件，医护人员已经明确触犯了法律，医院方面也及时给出了回复：其病历首页上的婚姻状况问题是医务人员未完成的病历模板，经与林更新本人核实其婚姻状况为未婚，信息泄露情况目前内部仍在进一步调查中，未来将加强患者信息的安全管理。

林更新的明星身份，让他的斥责备受关注。但事实上，医疗行业的信息泄露事件，此前已发生过多起：

1、深圳孕妇信息丢失案

深圳某医院上千名接受产检和分娩照护的女性，接到月嫂和婴儿产品公司的骚扰电话和短信。

据称，涉事受害者的信息，被明码标价售卖。由已经泄露出来的孕妇信息显示，疑是卖方通过医院内部存储孕检信息的电脑取得。

2、艾滋病人接到诈骗电话

全国超过 330 位艾滋病感染者称接到了诈骗电话信息，诈骗者自称是政府人员，通知患者领取疾病补助，并以此索要手续费。

因在电话中直称其名，对艾滋病感染者近期的就诊时间、在哪里拿过药、身份证号码，以及工作单位等等信息都掌握精准。因此不少感染者上当受骗。

3、洛杉矶长老会医院遭敲诈

洛杉矶长老会医院遭黑客攻击，全部电子病历数据无法使用。

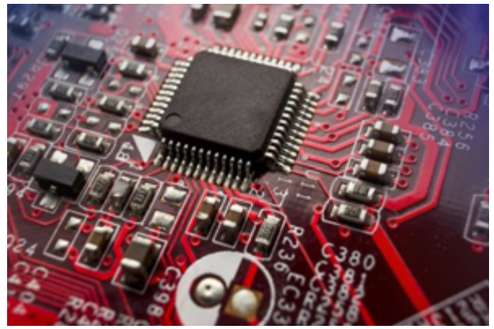
医院负责人声称，黑客并没有非法利用上述数据，但以解锁密钥作为要挟，向医院索取赎金。在尝试各种办法都无法恢复系统之后，只好向黑客支付了 40 比特币（一种虚拟电子货币，当时价值 1.7 万美元）才得以恢复正常运行。

相关专家提出，医疗信息化不断发展的同时，安全威胁也随之而来：医院的信息系统并不是独立运营的，信息与各相关单位均联网共享，存在被黑客入侵、网络攻击的风险；医护人员共用账号的现象也非常严重，对内部工作人员的管理不够严谨，导致“内鬼”有机可乘。层出不穷的安全事件时刻提醒着我们，安全线就是生命线，要避免医院的关键数据及病人隐私信息被黑客、内部人员所窃取，除了必须要加强员工的安全意识之外，还需要通过技术手段提高身份认证的安全性，并做到安全追溯、责任到人。

亿赛通数据安全产品，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。

三天亏 10 多亿！
台积电中毒表示难受“想哭”

据台湾媒体 8 月 5 日报道，台积电在 2 日傍晚遭勒索病毒入侵，并于当晚 10 时许扩散至三大厂区。台积电公告推算，事件发生后约 40 小时已恢复八成机台生产作业，预计在关键的 60 小时“排毒行动”后有望全数排除电脑病毒。但比原先预期慢了约一天，受冲击营收也比预期大，将冲击第三季度营收约 3%，约为 87 亿元新台币（约合人民币 17.7 亿元）。



台积电是世界 500 强的半导体制造公司，隶属于设计制造行业。此次遭受勒索病毒也为制造业企业敲响了警钟，台积电在数据安全处理上，在制造业方面一直以严谨出名，这次发生的病毒入侵事件导致电脑宕机，甚至是晶圆厂产线停摆事件，让业界非常震惊。

安全圈专业人士认为，连龙头级大厂都会遇到此问题，且是一次好几个晶圆厂同时被瘫痪，实属异常，其他业者更是要小心应对，尤其要引起制造业内部的警戒，未来应更为重视数据安全问题。

Wanna Cry 记忆犹新

这次病毒是勒索病毒 WannaCry（“想哭”）的变种， 想必去年的 Wannacry 爆发事件，大家还记忆犹新，受到该病毒攻击的电脑出现蓝屏，各类重要文档、数据库被锁定，无法正常打开和使用，众多业务系统出现瘫痪。

Wannacry 病毒在 2017 年 5 月肆虐全球之后，不少用户已采取了数据备份或杀毒软件进行防护。但由于一些用户没有及时更新的习惯，或是许多用户在使用已经停止备份、查杀等操作，无法对数据进行防护，因此，仍有许多用户终端面临该病毒侵袭的威胁。

勒索病毒的爆发，究其根源面对的对象是数据文件，勒索软件可以无任何顾虑的光顾你的电脑，对数据文件进行加密，加密后随之勒索解密。谈起数据加密，亿赛通十五年都用其对客户的数据进行安全防护，而今，面对反其道的攻击事件，亿赛通决定重拳出击此类恶意勒索软件，通过自主研发的勒索病毒防护卫士公益版，将数据实体与访问应用进行智能隔离和验证，让勒索软件无论如何变种，都无法接触到用户数据，从而无法加密用户数据，使勒索行为化为泡影。相比其他保护方式，终端用户无需改变任何工作习惯，真正的从源头上保护用户的数据安全。

目前此产品已全面上线，用户可拨打我们的服务热线进行咨询：400-898-1617，或访问亿赛通官网了解具体信息，我们竭诚为您服务！

一、服务概述

信息网络技术在金融证券业行业的普及和应用层次的不断深入，各金融单位之间的竞争也日益激烈。为了适应这种发展趋势，金融单位在改进服务手段、增加服务功能、完善业务品种、提高服务效率等方面做了大量的工作，以提高金融单位的竞争力，争取更大的经济效益。而实现这一目标必须通过实现金融电子化，利用高科技手段推动金融业的发展和进步，网络的建设为金融行业的发展提供了有力的保障，并且势必为金融单位的发展带来巨大的经济效益，从而对数据安全的也提出更高要求。

信息技术的快速发展使银行对电子化的依赖不断加强，就在银行业务不断信息化的过程中，银行所面临的系统安全问题越来越多。金融单位既要满足监管部门的合规性要求，又要对企业数据和客户资料进行安全防护，加强信息的安全性迫在眉睫。因此 如何提高金融系统的信息安全性，最大限度保护金融系统信息安全，成为金融业务系统的重中之重！

二、服务介绍

客户需求

随着金融单位业务的发展，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的生成。为提高企业内部数据协同和高效运作，实现内部办公文档内容流转安全可控，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。对于内部文档使用范围、文档流转等进行控制管理 ,以防止文档内部核心信息非法授权阅览、拷贝、篡改。既防止文档外泄和扩散，又支持内部知识积累和文件共享的目的。内部的数据安全需从以下几方面解决：

1. 怎样确保跨区域网络环境数据统一安全管理问题；
2. 硬盘故障后进行数据恢复，导致数据泄漏；
3. 如何保障终端数据的离线安全；
4. 如何解决与外协人员、合作伙伴等的数据交互安全；
5. 如何保障移动设备（笔记本）、存储介质（U 盘、移动硬盘）的数据安全。
6. 如何保障各应用、办公系统等数据的存储和使用安全。

解决方案

企业内部数据安全体系建设，需要突出重点，切实关注文件外带保密需求，充分考虑敏感性数据面临的各种主动泄密和被动泄密风险。同时，应充分考虑系统对设计人员的业务影响范围，尽可能降低安全行为带来的系统性能损耗和应用约束，在安全性和可用性之间保持合理的平衡。

终端防护：通过透明加密、主动加密、智能加密和权限控制对文档进行梯度式、多层次、全方位的保护，从文档的产生到传输一直处于保护状态，有效保护终端安全。

移动介质管理：对移动介质进行注册签名和分类，保证移动介质正常使用的同时还能够有效保证数据的安全，并提供了丰富的审计功能。

邮件敏感数据泄露防护：能够对邮件服务器中的邮件有效管控，并能够及时向管理员报警和丰富的事件审计，杜绝邮件发送敏感事件的发生，有效保护数据安全。

回家办公：即插即用设计原理，当 U 盘移动客户端插入个人电脑并认证通过后，系统自动进入密文模式，可提供与企业内网终端完全一致的安全防护效果，确保企业加密数据外部使用安全；当 U 盘移动客户端移除或退出用户登录后，客户端将自动完成环境移除并关闭加解密功能，不对用户处理个人数据产生任何影响；

智能分类分级：通过对敏感信息的识别分析，对文档进行智能分类分级和标示密级，对文档进行方便有效的管理。

准入网关：通过安全准入、链路加密等技术，全面解决企业移动业务数据安全问题。

安全中间件：为业务系统开发者提供了标准易用的业务安全接口。

三、客户收益

通过亿赛通数据泄露防护系统 (DLP) 解决方案，系统定制化功能较强，可适应广发较复杂的应用场景；网关系统实施对现有系统改造程度较小，易于部署，且能最大限度保护系统数据文档；可对文档权限灵活控制，并有全面的日志跟踪记录，便于事后追查。通过一系列技术手段，配合数据安全防护制度，提高了员工的数据安全保护意识。

部分客户

1、中信银行 / 证券股份 / 资产管理有限公司
2、招商银行
3、长城证券有限责任公司
4、中国国际金融股份有限公司
5、泰康资产管理有限责任公司
6、华夏基金管理有限公司
7、民生银行
8、上海浦东发展银行股份有限公司
9、新华人寿保险股份有限公司
10、九江银行股份有限公司
11、宁波银行
12、广发证券股份有限公司
13、中国人民财产保险股份有限公司
14、中国建设银行
15、山西证券股份有限公司
16、北京华控投资顾问有限公司
17、方正资本控股股份有限公司
18、泉州银行
……

亿赛通签约中信银行/证券股份有限公司

客户简介

中信银行、中信证券股份有限公司都属于中信集团。中信集团系三大机构中信银行、中信证券、中信信托。其中，中信银行原称中信实业银行，创立于 1987 年。中信银行是中国的全国性商业银行之一，总部位于北京，主要股东是中国中信股份有限公司。而中信证券股份有限公司是中国证监会核准的第一批综合类证券公司之一，于 1995 年在北京成立。中信证券第一大股东为中国中信集团公司。

需求背景

自 2009 年开始，中信证券上线知识管理系统（KM）。为了防止从该系统下载的离线文件被内部人员泄露到企业外部从而损害企业利益及形象，中信证券于当年 6 月与亿赛通签署了数据泄露防护系统定制开发及授权使用合同。由于此项目的成功实施，中信证券又分别于 2011 年 6 月、2011 年 12 月、2015 年分别签约亿赛通，不断夯实企业数据信息安全管理机制。

解决方案

1. 文档安全管理系统，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。

①可以实时记载用户对文件的操作记录；

②可以根据用户的需要设置不同的安全级别；

③对于需要打印的文件强制在打印界面加载打印时间、IP 地址及用户信息；

④文件加解密过程均自动完成，对用户完全透明；

⑤文件从制作完成到生命结束都是以密文形式存在。

2. 文档加密安全网关，可使从 KM 系统上下载下来的文件带有权限，在企业内部可自由使用，泄露到企业外部无法使用。该权限文件分为可解密文件和不可解密文件两类，其中，可解密文件由内部人员解密时，需提交解密理由并通知相关人员，同时留下解密日志，每周最多解密 5 篇权限文件，如超过该值会向管理员进行预警。不可解密文件只能由指定专人进行解密。

项目成果

亿赛通数据安全解决方案，有效保护企业数据信息安全。客户后续持续新的需求，都由亿赛通定制开发，项目应用取得的良好的成果，此次项目，也有效树立了金融证券业的安全风尚标！