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

10月刊

2017 年共 11 期

关注企业官方微信

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

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

十九大

继往开来 砥砺前行

不忘初心跟党走

2017 年 10 月 18 日，举世瞩目的中国共产党第十九次全国代表大会在人民大会堂开幕，习近平代表第十八届中央委员会向大会作了题为《决胜全面建成小康社会 夺取新时代中国特色社会主义伟大胜利》的报告。习主席指出，要善于运用互联网技术和信息化手段开展工作；加强互联网内容建设，建立网络综合治理体系，营造清朗的网络空间；推动互联网、大数据、人工智能和实体经济深度融合。

继往开来，砥砺前行。十九大谋篇布局绘蓝图，战略高远建强国，勾勒出一幅幅激人奋进的壮美画卷，助力中国梦的实现。从分享经济、移动支付到人工智能、“互联网 +”，扬起网络安全和信息化的风帆不仅增强人民对美好生活向往的满意度，而且促进经济平衡充分地发展，提升国家治理体系和治理能力现代化水平，促进创新型国家建设，强有力地推动实现中华民族伟大复兴的中国梦。

信息安全、网络安全、数据安全，安全厂商如何布局？如何砥砺前行？能为中国梦奉献一份力量，期待中.....

雅虎账号泄露达 30 亿
雅虎账号信息安全再成话题

雅虎账号泄露打 30 亿 雅虎账号信息安全再成话题

雅虎去年披露，该公司的数据泄密事件总共影响了 10 亿帐号。截至目前媒体给出最新消息显示，雅虎的全部 30 亿帐户都被泄露，雅虎账号信息安全再成话题。

波士顿安全公司 Cybereason 首席安全官山姆 • 克里（Sam Cuorry）表示，此次数据泄密事件现在已经影响了“半个世界”。不过，由于一个人可能注册多个帐号，所以帐号数量可能多于实际用户数。

根据雅虎披露的消息，被盗的信息包括姓名、电子邮件、手机号码、出生日期、安全问题和答案。同时雅虎还宣布，他们已经向其他受到 2013 年 8 月的数据泄密事件影响的用户发送邮件，向其告知此事。

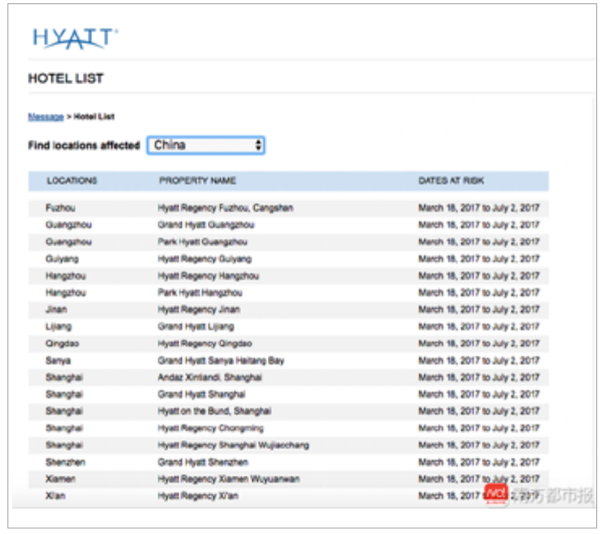
对于邮箱泄密事件，雅虎给出的弥补措施也仅仅是要求用户修改密码，同时废除安全问题，避免帐号遭到入侵。

雅虎泄密事件给 Verizon 造成了很大困扰，该公司刚刚开始投放新的 Oath 子公司的电视广告，而雅虎和 AOL 的服务都被并入这家子公司。

雅虎账号信息全部泄露使账号信息安全再一次成为公众话题，虽然此次出事的雅虎，但不能保证下次出现在我们身上。所以小编建议不要再自己的各个账号保存自己的隐私信息，如有必要云盘是一个不错的选择。

隐私大事件 | 信息泄露不分行业，酒店餐厅又中招

41 家凯悦酒店住客信息遭泄露


HYATT

HOTEL LIST

Message > Hotel List

Find locations affected China

LOCATIONS	PROPERTY NAME	DATES AT RISK
Fuzhou	Hyatt Regency Fuzhou, Cangshan	March 18, 2017 to July 2, 2017
Guangzhou	Grand Hyatt Guangzhou	March 18, 2017 to July 2, 2017
Guangzhou	Park Hyatt Guangzhou	March 18, 2017 to July 2, 2017
Guiyang	Hyatt Regency Guiyang	March 18, 2017 to July 2, 2017
Hangzhou	Hyatt Regency Hangzhou	March 18, 2017 to July 2, 2017
Hangzhou	Park Hyatt Hangzhou	March 18, 2017 to July 2, 2017
Jinan	Hyatt Regency Jinan	March 18, 2017 to July 2, 2017
Lijiang	Grand Hyatt Lijiang	March 18, 2017 to July 2, 2017
Qingdao	Hyatt Regency Qingdao	March 18, 2017 to July 2, 2017
Sanya	Grand Hyatt Sanya Haitang Bay	March 18, 2017 to July 2, 2017
Shanghai	Andaz Xintiandi, Shanghai	March 18, 2017 to July 2, 2017
Shanghai	Grand Hyatt Shanghai	March 18, 2017 to July 2, 2017
Shanghai	Hyatt on the Bund, Shanghai	March 18, 2017 to July 2, 2017
Shanghai	Hyatt Regency Chongming	March 18, 2017 to July 2, 2017
Shanghai	Hyatt Regency Shanghai Wujiaochang	March 18, 2017 to July 2, 2017
Shenzhen	Grand Hyatt Shenzhen	March 18, 2017 to July 2, 2017
Xiamen	Hyatt Regency Xiamen Wuyuanwan	March 18, 2017 to July 2, 2017
Xi'an	Hyatt Regency Xi'an	March 18, 2017 to July 2, 2017

近日，凯悦酒店 Hyatt 对外表示，41 家凯悦旗下酒店支付系统被黑客入侵，包括住客支付卡姓名、卡号、有效期和内部验证码等信息遭到泄露。据统计，中国有 18 家凯悦酒店受到影响。

凯悦酒店方面建议，入住受影响酒店的住客随时查看个人支付卡账户信息，一经发现有未授权的消费活动，请立即与发卡机构联系。

在凯悦酒店官网看到，一份名为“来自凯悦全球营运总裁的信”称，在 2017 年 3 月 18 日至 7 月 2 日之间，部分旗下酒店前台手动输入或刷卡消费的宾客的支付卡信息有被未授权访问的迹象，目前问题已经解决。

据了解，造成此次安全事件的原因，经调查是有第三方将恶意软件安装在部分酒店的信息系统中。然后通过酒店管理系统漏洞获取数据库的访问权限，以获得用户的隐私信息。

在凯悦公布的 41 家受影响酒店名单中，中国受到影响最严重 ,共有18家酒店系统被入侵。酒店遍及福州、广州、贵阳、杭州、济南、丽江、青岛、三亚、上海、厦门和西安等 12 座城市。

据悉，总部位于芝加哥的凯悦 Hyatt 酒店集团在国内共有 51 家酒店，旗下有柏悦、君悦、凯悦等品牌。目前，凯悦酒店表示已加强保护措施，并直接向所有高危时段入住受影响酒店的宾客发出通知。

必胜客官网遭入侵 6 万人支付信息或被盗

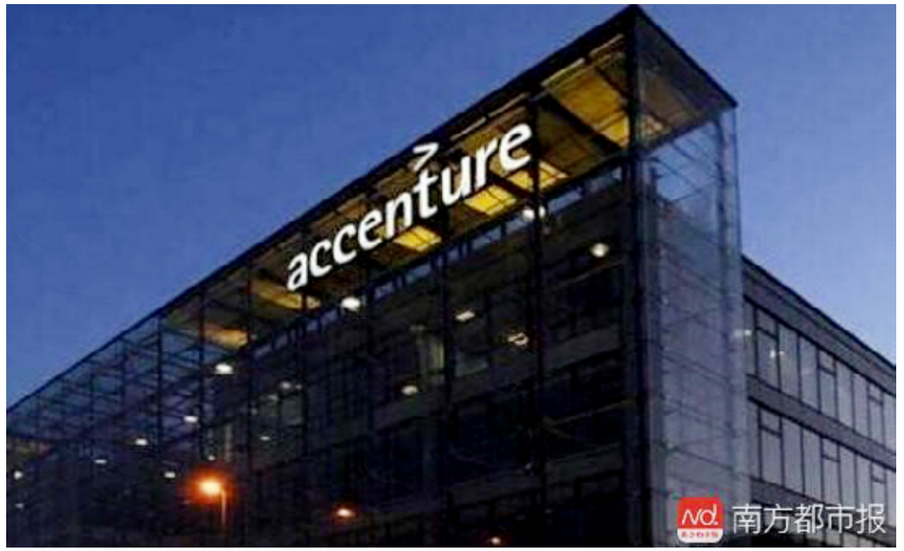
10 月 14 日，必胜客通过电子邮件告知顾客，在 10 月 1 日凌晨到 10 月 2 日中午，通过必胜客官网或移动 APP 下单的顾客的个人信息可能已经被盗用，约有 6 万人受到影响。邮件中称，在意识到被黑客入侵之后，必胜客迅速响应，并采取了相应的缓解措施。此次黑客从必胜客网站上窃取的信息包括：姓名、账单邮编、收货地址、邮箱地址、信用卡数据（包括卡号、有效日期、CVV 码）。

必胜客提醒顾客要小心事后的一些骗局。因为黑客很可能会利用盗取到的信息来冒充必胜客工作人员，以骗取顾客更多的个人信息，比如社会保障卡号码等。

必胜客在黑客攻击网站两周后，才对外公布此事。这让一些用户表示愤怒。15 日，有顾客称，“两周前你丢失了我的信用卡信息，一周后黑客已经在恶意使用了，然后，今天！我才得知这一事件！”

必胜客表示，目前公司正在第三方网络安全专家进行联系，以查明事件背后黑客的身份，并会确保类似的事件不会再次发生。同时，必胜客也称将向受影响的顾客提供一年免费的信用监控服务。

埃森哲曝安全问题 大量敏感数据遭公开



近日，全球最大的管理咨询公司埃森哲被曝出安全问题，大量敏感数据恐遭到泄露。埃森哲放在亚马逊 S3 存储服务上的 4 个云存储服务器数据被公开在网上。

埃森哲企业云平台中存储的数据包括 API 信息、身份验证凭证、加密密钥、客户信息等。因服务器配置不当，在未受密码保护的情况下，任何拥有 web 服务器地址的人都可以访问和下载这其中数百 GB 的数据，并将使埃森哲及其服务的数百家企业客户面临被恶意攻击的风险。

根据埃森哲官网介绍，所服务的客户超过四分之三的《财富》全球 500 强企业，业务遍及 120 过个国家，涵盖 40 多个行业。如果这些暴露的数据被黑客利用，进而发起恶意攻击 ,可能给这些知名企业带来无数次财物损失。据悉，埃森哲已采取相应措施应对。

在上个月，四大会计师事务所之一的德勤也曾遭到网络攻击，攻击者利用一个管理员账号，获取德勤的电子邮件服务器的访问权，造成德勤大量数据、机密文档和客户邮件被盗。

亿赛通作为中国数据安全防护专家提醒大家，注意个人隐私数据的保护，不要在网上或是公共场所随意泄露自己信息内容。加强安全意识，筑牢安全防线。商家尽快利用起科学技术，规避泄密风险，全民行动一起抵御黑客的不法行为。

网购盛行 隐私面单如何保障个人信息安全？

“双十一”将至，作为下半年受关注范围最广、单日成交量甚至能够堪比一个国家全年的预估电子商务交易额、并在2016年创下了交易总额178亿美元成绩的消费节日，不难想象，这背后所涉及到的快件量也是无比惊人。

据国家邮政局统计数据显示，2016年全年快递服务企业业务量完成312.8亿件，同比上涨五成有余，而在“双十一”当日，就产生了6.57亿件包裹订单。预计在今年，我国的快递业务量将达到438亿件。

行业聚焦 INDUSTRY FOCUS

由于每一件快递都需要送至指定的地点，可以说任何的快件上都包含着收件人的隐私，若是被盗取，也会对个人日常的生活产生负面影响。曾经有报道称，房产中介翻快递箱并拍摄个人信息的情况确实存在。

根据2016年《中国网民权益保护调查报告》提供的数据显示，在占据4.8亿的网购用户中，有超过半数遭遇过个人信息泄露，而这个约为2.4亿人的数字背后，更会牵扯出数量更加庞大的被信息泄露。有网友曾经做过实验，称一张快递单上面提供的信息，至少可以扩展出三十余条个人信息。

除此之外，有相关调查更显示，约43%的用户认为上门签收会导致个人信息泄露而对安全产生隐患，这也使得快递代收成为了消费者刚需。

面对着来自用户群体的需求，快递公司也不得不推出一系列改变以应对用户对于隐私不被盗取的关注。

日前，顺丰正式宣布上线“丰密面单”服务，新款面单能够隐藏寄件人的姓名、物品相关信息、收件人电话号码等关键信息。

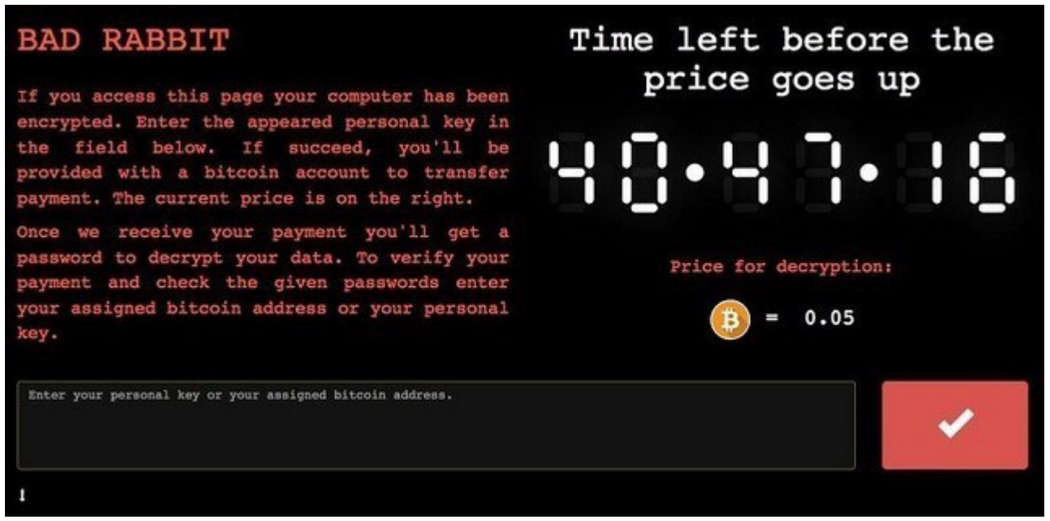
早在今年5月，顺丰的“丰密面单”已经开始试点进行。其中，收件人的姓名、地址、电话等关键个人信息都已经被隐藏起来，而相关地址信息也被编码替代。不仅如此，客户在于快递员进行联系沟通的时候，还可以通过虚拟电话号码进行。

不过，有用户称，目前的顺丰面单能够给予寄件人信息很好的隐藏，但是收件人却只能“抹去”其手机号码的四位。

业内人士分析，隐藏个人隐私信息的新兴面单将会是快递行业在未来的发展大方向，趋势不可逆转。但是，由于成本比一般普通面单高出不少，加上更换快递员移动终端的费用，激增的成本端压力确实会成为行业整体向面单“私隐化”迈进的桎梏，而且因为行业尚未缺乏统一对于面单的标准，在实行起来也会存在一定的困难。

有数据显示，目前隐私面单的普及率仅仅为20%。虽然此前已经有不少的快递企业都迈入了隐私面单的新篇章，但是若要实现完全普及，道阻且长。

欧洲爆发坏兔子勒索软件：赎金 0.5 个比特币



（图片来自 baidu）

日前外媒和多家安全企业报道，在俄罗斯和东欧地区爆发了名叫“坏兔子”（Bad Rabbit）的新型勒索软件，一旦计算机被其感染，“坏兔子”就会在一个黑底红字的界面上显示“NotPetya”风格的勒索信息。

该恶意软件会要求受害人登陆“洋葱路由”下隐藏的某个服务网站，向其交付 0.5 个比特币的赎金来解除勒索。

此外“坏兔子”还会显示一个倒计时界面，声称不及时支付的话，其勒索金额就会水涨船高。目前暂不清楚“坏兔子”攻击的幕后主使者身份、受害者都有谁、以及该恶意软件是哪里产生和如何传播的。

卡巴斯基实验室表示，俄罗斯是“坏兔子”的重灾区，其次是乌克兰、土耳其和德国。该公司称该恶意软件的散布“是一场针对企业网络的有意攻击”。

据了解，“坏兔子”恶意软件的攻击手段与 ExPetr [NotPetya] 期间类似，但现在无法证实它们之间的关系。

另外，安全公司 ESET 指出，该恶意软件还会尝试感染同一本地网络下的其它计算机，比如借助早就曝光的 Windows 数据共享协议（SMB）和开源的 Mimikatz 漏洞利用工具。

勒索病毒“坏兔子”来袭 俄乌等国不幸中招

俄罗斯、乌克兰等国２４日遭到新一轮勒索病毒攻击。乌克兰敖德萨国际机场、首都基辅的地铁支付系统及俄罗斯三家媒体中招，德国、土耳其等国随后也发现此病毒。

法新社２４日报道，新勒索病毒名为“坏兔子”，采用加密系统防止网络安全专家破解恶意代码，与６月底爆发的“NotPetya”病毒有相似的传播方式，但“坏兔子”波及范围不及前者。

在乌克兰，敖德萨机场的旅客服务信息系统２４日下午遭到攻击停止运转。机场发言人说，由于临时改为人工处理乘客信息，造成一些航班延误。机场稍后通过社交网站发布消息说：“机场已强化安全体系，各项服务正常。”

基辅的地铁支付系统当天也遭到攻击，但地铁运营未受影响。

俄罗斯最大的新闻通讯社之一国际文传通讯社、《丰坦卡报》网站及另一家媒体２４日也遭“坏兔子”病毒攻击，国际文传通讯社发稿受到影响。

路透社以网络安全公司ＥＳＥＴ为消息源报道说，超过一半的“坏兔子”病毒受害者位于俄罗斯，这种勒索病毒还蔓延至德国、土耳其、保加利亚、日本等国。

俄罗斯网络安全服务商卡巴斯基实验室２４日发表声明说，“坏兔子”病毒主要攻击对象是公司网络，卡巴斯基正密切关注这一勒索病毒。“坏兔子”病毒是否关联“NotPetya”病毒仍在调查中。

尽管没有受到“坏兔子”病毒影响，美国国土安全部２４日发布警告，提醒公众注意防范新一轮勒索病毒攻击。

６月２７日，欧洲、北美地区多个国家遭到“NotPetya”病毒攻击。乌克兰受害严重，其政府部门、国有企业相继“中招”。

5月１２日，一种名为“想哭”的勒索病毒袭击全球１５０多个国家和地区，影响领域包括政府部门、医疗服务、公共交通、邮政、通信和汽车制造业。

福利分享｜亿赛通个人版数据安全卫士免费送一年激活码

你的数据你做主 个人权益得保障

针对个人 PC 端的重要信息，比如：个人的隐私照片、老师的科研课题、工程师的研发代码、摄影师的参赛作品、设计师的图纸文件等等，需要存储到云端或是将这些隐私数据外发给第三方时，所有者扔可对外发后的数据安全做到有效管控，进而有效避免不法分子侵犯个人隐私，同时保护了数据所有者的合法权益。

您演绎身边的安全故事

视频连接地址：http://v.qq.com/x/page/p0556c3x6r3.html（故事之一）

https://v.qq.com/x/page/c0556l8omnt.html（故事之二）

亮点一：支持多种文件类型。如：文档类、音视频、设计类、图片类、代码类.....

亮点二：支持多种权限控制。如：是否只读、打印、截屏、阅读次数、使用时长、自动销毁.....

亮点三：支持高强度动态虚拟卷加密技术，使文件在外发传输过程中保持加密状态。

亮点四：支持超大文件外发。如外发文件还原成原件，内容仍存在。

使用方法：

第一步：关注亿赛通官方微信；

第二步：回复关键词“激活码”，即可免费领取一年的会员激活码。

重磅 | 2017 年数据泄露防护市场达 7.6 亿 亿赛通迎高景气

近两年重大安全事件频发，局势日益严峻。如 2017 上半年严峻的网络安全重大事件悄然袭来：“WannaCry”敲诈勒索病毒、“暗云Ⅲ”变种木马、“Petya”勒索病毒……面对这些接连发生的重大数据泄露突发事件，2017 年中国工信部首次明确提出信息安全产品纳入目标中，提出到“十三五”末达到 2000 亿元，年均增长 20% 以上。

数字经济时代，基于安全产业的快速变化，数据成为核心资产。亿赛通利用 14 年的技术沉淀，重磅打造数据安全智能管理平台（DSIP），一个全新的智能 +、互联互通、全方位的数据安全技术将上演于国内安全市场。赛迪报告显示，预计 2017 年数据泄露防护市场将达到 7.6 亿，群雄逐鹿、谁与争锋，让我们拭目以待。

创新成就价值

我们知道，2014 年绿盟科技对外宣布收购亿赛通 100% 股权，成功打响在数据安全领域迄今为止最大金额的一次收购案，成功整合的背后，对双方业务的互补延展都起到重要作用，充分实现了为用户提供一站式的信息安全产品、服务和解决方案，“内外兼顾”共同创造新的利润增长点。

据国内权威赛迪报告指出：2015 年，亿赛通以 19.2%的市场占有率，位居中国数据泄露防护市场第一名。2016 年在激烈的市场竞争环境下，继续以 20.6% 占据市场排名第一。14 年来亿赛通不断用“专注”书写着自己在安全领域的历程。

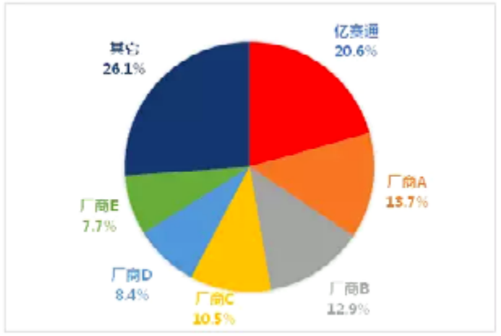


图 1：2016 年中国数据泄露防护市场品牌结构

（来源：赛迪顾问 2017.6）

行业增长分析

数据泄露防护市场充满挑战与机遇，从 2016 年的市场调查报告中得知，2016 年市场总规模达到 6.2 亿元，同比增长 21.2%，预计 2017 年我国数据泄露防护市场规模将达到 7.6 亿元，同比增长 22.3%，市场发展潜力巨大，尤其华北市场占据主力约 31.5%，华东市场次之约 28.6%，华南约 17.7%，西南约 10.3%，华中约 5.0%，东北约 3.7%，西北约 3.0%。如何布局、如何力争站稳脚跟是每一个数据安全厂商应该认真思考的问题。

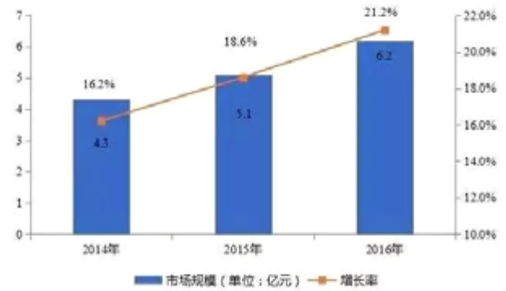


图 2：2014-2016 年中国数据泄露防护市场规模及增长情况

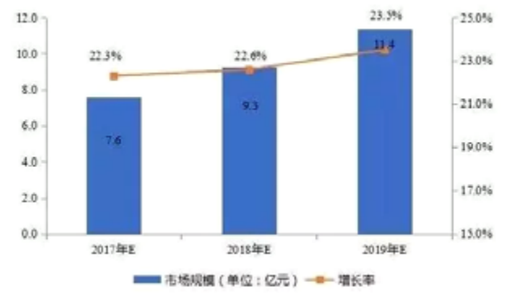


图 3：2017-2019 年中国数据泄露防护市场发展预测

紧贴市场 抢占先机

一个不断“创新”的专业企业，能精准把握市场动态，有了绝佳的“武器”之后，便要布局市场，占领高地。毕竟，市场营销的优秀成绩离不开布局战略，这一次，亿赛通坚持超前创新的服务理念、前瞻性的关键技术、创下了一座又一座新的里程碑“秘诀”。

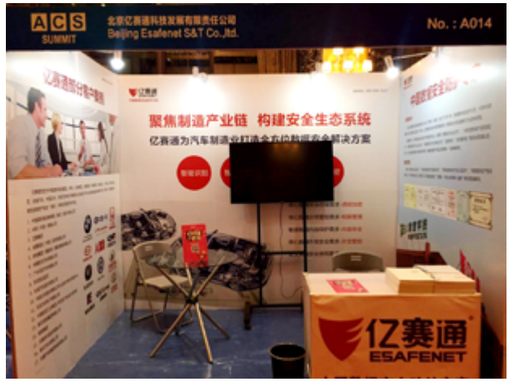
亿赛通数据安全智能管理平台是一款融合机器学习、大数据分析、文档加密、访问控制、关联分析、数据标识等技术的综合性数据智能安全产品，可帮助用户对结构化和非结构化数据进行数据治理（资产统计、分类、聚类、分级、密级标识等）、安全管控（数据加密、权限管理，数据脱敏、边界防护、应用准入、行为审计、数据防护等）、态势感知（趋势分析、风险预警、溯源、风险人员画像等），为用户的核心数据资产从终端、网络、存储、应用等全方位提供全生命周期保护，在确保组织敏感数据安全前提下，不管控、不影响非敏感业务开展的体验度，实现安全与效率的最大平衡。

在激烈的市场竞争中，多变的市场环境下，亿赛通在专注中成为了安全领域最为权威和专业的企业，从而赢得了客户并不断发展壮大。专注成就了企业的成长，使得其对于市场的走向，客户需求的把握更加专业，从而对市场把握更为精准，面对数据泄露防护市场竞争越发激烈的今天，早已布局数据安全领域的亿赛通获得了先机。将销售市场划分为华南、华东、华北、华中、东北、西南、西北七大区域，行业客户遍布党政军、金融证券、研发通讯、设计制造、运营商、能源、企业集团等各个领域，在业内已形成良好口碑。

亿赛通出席 ACS 2017 中国汽车 CIO 峰会 构筑制造产业安全生态系统

为进一步促进信息化技术在汽车产业的应用，10 月 25-26 日“ACS2017 中国汽车 CIO 峰会”在上海成功举办，以“互联网 + 时代的汽车全产业链信息化解决方案”为主题，讨论时下汽车行业发展动向，如何借助信息化技术实行全产业链的优化升级，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。

亿赛通作为中国数据安全防护专家光荣受邀，将制造产业下的生态安全体系建设，智能数据安全、智能数据审计、智能数据加密前沿技术分享给现场 300 余位众多整车、零部件、经销商等全产业链的 CIO 及汽车行业信息化的专家们，大家共襄盛举、共同交流。



亿赛通深耕国内数据防护市场多年，在透明文档加密，内容识别，存储数据防护，应用数据防护，终端数据防护等被动、主动防护方面具有技术优势，并针对特定行业领域细分解决方案，逐步成为“敏感数据识别与主动防护相结合”、“终端 + 网络 + 应用”的全过程全范围数据防护服务提供商。在制造产业中先后为中国国际海运集团、ABB、正泰集团、佳通轮胎、哈电集团、华晨宝马、广州本田、东风悦达起亚、长城汽车、中国北车、东风汽车电子等国内众多知名汽车企业提供数据安全解决方案。肩负着“保护数据所有者的信息资产安全”使命，不断进军国内外市场。

亿赛通总部在北京，同时在全国主要城市设有 30 余家分支机构，可提供全国性覆盖服务。未来，将以产品、方案、服务为主导，融合大数据和机器学习，构建包括终端数据防护、网络数据防护、应用数据防护、存储数据防护、介质数据防护和云服务平台在内的全范围智能数据泄露防护体系，全方位保障用户数据安全。

证券代码：300369　　证券简称：绿盟科技　　公告编码：2017-084 号

北京神州绿盟信息安全科技股份有限公司
关于对全资子公司亿赛通增资的公告

本公司及董事会全体成员保证信息披露的内容真实、准确、完整，没有虚假记载、误导性陈述或重大遗漏。

经公司第三届董事会第六次会议审议通过，公司以重大资产重组配套募集资金人民币 561.5993 万元和自有资金 2,726.0508 万元（合计 3,287.6501 万元）向北京亿赛通科技发展有限责任公司（以下简称“亿赛通”）增资。增资完成后，亿赛通注册资本为 5,000 万元，公司持有其 100% 股权。

本次对外投资金额在董事会审批权限范围内，无需提交公司股东大会审议批准，不构成重大资产重组。本次对外投资不构成关联交易。

一、重大资产重组配套募集资金基本情况及使用情况

（一）重大资产重组配套募集资金基本情况

经中国证券监督管理委员会《关于核准北京神州绿盟信息安全科技股份有限公司向阮晓迅等发行股份购买资产并募集配套资金的批复》（证监许可〔2015〕94 号）核准，本公司非公开发行股票 1,760,712 股，发行价格为每股人民币 94.28 元，本次非公开发行股票共募集资金 165,999,927.36 元，扣除发行费用后募集资金净额为人民币 154,926,055.74 元。以上募集资金已由利安达会计师事务所（特殊普通合伙）于 2015 年 3 月 31 日出具利安达验字〔2015〕第 1025 号《验资报告》验证确认。

（二）重大资产重组配套募集资金使用情况

根据公司《发行股份及支付现金购买资产并募集配套资金暨重大资产重组报告书》募集资金运用方案，本次募集资金主要用于本次交易现金对价和交易费用的支付。若支付本次交易现金对价款和交易费用后仍有剩余资金，将用于标的公司（即亿赛通）运营资金安排。

公司本次非公开发行配套募集资金净额为 154,926,055.74 元，公司向交易对手方阮晓迅等支付交易对价合计 14,940 万元，剩余募集资金 5,526,035.74 元存放于重大资产重组配套募集资金专户。

截止 2017 年 9 月 30 日，重大资产重组配套募集资金专户的余额为人民币 5,615,993.08 元，其中本金为人民币 5,526,035.74 元，利息为人民币 89,957.34 元。

二、本次使用募集资金对外投资事项的审议情况

公司第三届董事会第六次会议审议通过了《关于对全资子公司亿赛通增资的议案》，同意公司使用重大资产重组配套募集资金 561.5993 万元和自有资金 2,726.0508 万元向全资子公司亿赛通增资。本次交易完成后，公司持有亿赛通 100% 股权。

三、投资标的基本情况

1、亿赛通基本情况

名称：北京亿赛通科技发展有限责任公司

注册资本：1712.3499 万人民币

法定代表人：崔培升

住所：北京市海淀区西二旗大街 39 号 4 层 401

成立日期：2003 年 01 月 21 日

经营范围：技术开发、技术转让、技术咨询、技术服务；计算机系统服务；计算机维修；销售计算机、软件及辅助设备、电子产品、机械设备；货物进出口、技术进出口。（依法须经批准的项目，经相关部门批准后依批准的内容开展经营活动。）

与公司关系：为本公司全资子公司

亿赛通主营业务为研发、生产、销售网络安全 DLP 加密产品和网络内容安全管理产品。

2、投资标的最近一年及一期主要财务数据

单位：人民币元

项　目	2016 年 12 月 31 日/2016 年度（经审计）	2017 年 6 月 30 日/2017 年上半年（未经审计）
资产总额	325,773,113.11	259,029,662.31
负债总额	91,551,314.35	33,219,139.91
所有者权益	234,221,798.76	225,810,522.40
营业收入	142,400,984.24	16,465,930.33
净利润	55,068,492.21	-9,600,095.31

四、本次对外投资的目的、存在的风险和对公司的影响

本次投资主要是补充亿赛通日常营运资金，为研发新技术、生产新产品、开拓市场业务提供必要的资金支持。此次投资也可能面临亿赛通研发投入失败、业务拓展不顺等经营性风险，公司将及时评估风险、控制风险。

特此公告。

北京神州绿盟信息安全科技股份有限公司

董事会

2017 年 10 月 23 日

亿赛通小贴士 ESAFENET PROMPT

信息安全意识小贴士

亿赛通小贴士 ESAFENET PROMPT

信息安全意识小贴士

聚焦产业链 构建安全生态系统
亿赛通为设计制造业打造全方位
数据安全解决方案

一、行业分析

随着制造业信息化的迅速发展，企业信息，尤其是文档信息如何能更有效、更安全的流转和使用成为生产商所关心的问题，文档信息的安全传输也随之成为一项重要的业务需求。 制造业是我国国民经济的重要支柱产业。大部分企业，尤其是制造型企业，随着信息化建设的推进，在网络方面增加了硬件设备，在软件方面，增加了 ERP、PDM、CRM 和 SCM 等专业系统，企业内部的数据流越来越丰富。伴随着愈来愈激烈的行业竞争，数据安全问题就显得尤为重要。

据权威机构调查，80% 以上的安全威胁来自泄密和内部人员犯罪，而非病毒和外来黑客引起。防火墙、入侵检测、隔离装置等网络安全保护对于防止外部入侵有着不可替代的作用，而对于内部泄密显得无可奈何，真正有目的盗取或破坏信息的黑客也许正在隐藏在内部。企业内部的信息安全需要一个整体的策略方案 ,以巩固信息化成果 ,降低企业信息安全风险。

二、客户需求

在制造、设计高度信息化、网络化的趋势带动下，企业引入了大量与生产制造相关的应用系统，而这些应用系统在存储、使用、传输、交互的过程中都会造成数据泄密。具体表现如下：

1、系统内产生的数据和文档有高度保密性、高度敏感性，数据泄露会造成重大危险；

2、企业的认证体系、业务信息系统和办公 OA 系统等应用平台数据交互频繁 ,与合作单位有大量的对外接口；

3、企业内部网络有多种业务平台，移动设备如笔记本电脑、U 盘使用广泛；

4、与外部单位的合作，对外发出文件数量较多；

5、办公网上的信息都未被加密，采用明文传输；

6、办公网的用户权限控制不严密。

三、解决方案

亿赛通数据泄露防护（DLP）是专为企业级用户设计的数据防泄密解决方案，从数据的存储、传输、交换过程中的安全环节，采用了多种加密手段结合的方式保护。从终端、网络和存储三个层次入手，对核心数据的形成、存储、使用、传输、归档及销毁等全生命周期进行安全控制，结合企业特有的业务需求、业务模式和管理文化，为企业制定完整的数据泄漏防护解决方案，实现企业核心信息资产防泄漏的安全目标。

1、加密系统：采用亿赛通数据泄露防护系统（DLP），运用透明加密、主动加密和智能加密的梯度式加密方式，对设计图纸、文档、财务报表、业务合同等核心数据进行保护。从数据的产生，到数据使用传输，数据都处于加密状态，从源头保证数据的安全；

2、采用亿赛通安全准入网关，通过 DLP 系统加准入网关的方式对 OA、MES、SVN 业务系统的安全保护及终端电脑文件的自动加密保护，达到数据安全从源头做起，凡事从业务系统下载下来的数据都已经做过加密处理，员工拿到的数据就已经是加密文件，但服务器中保存的文件仍保持明文状态；

3、采用亿赛通数据泄露防护系统（DLP），对内网使用的多种系统进行统一平台管控。对终端、网络、邮件、移动终端、端口等进行多层次防护，保护文档安全；

4、采用亿赛通数据泄露防护系统的外发管理，可以将外发文档进行统一管理 ,通过设置外发信息的秘钥、权限、机器码绑定等设置，文档是无法打开的，保证了与外部单位合作的外发文档的安全。

四、方案价值

亿赛通数据泄露防护系统（DLP）解决方案与企业的安全理念、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；提供丰富的的审计记录，帮助员工提高安全意识。

亿赛通签约中国国际海运集装箱（集团）股份有限公司

客户简介

中国国际海运集装箱（集团）股份有限公司（简称“中集集团”），是世界领先的物流装备和能源装备供应商，总部位于中国深圳。公司致力于集装箱、道路运输车辆、能源和化工装备、海洋工程、物流服务、空港设备等，提供高品质与可信赖的装备和服务。其市场占有率而言，中集有 10 多个产品持续多年保持全球第一，作为一家为全球市场服务的跨国经营集团，中集在亚洲、北美、欧洲、澳洲等地区拥有 200 余家成员企业，客户和销售网络分布在全球 100 多个国家和地区。

需求背景

随着中集集团业务快速扩展，集团经营规划、行政办公、技术研发资料愈发重要，集团需要统一梳理核心数据并明确各级数据保护规范和要求。集团下属 50+ 分公司，研发资料、项目文档技术保护手段和管理存在缺失，资料外泄情形屡有发生，核心重要资料容易被竞争对手窥视，许多重要资料随着人员离职等大量流失。集团出现部分数据泄密事件后审计无从做起，相关职责划分不明确，缺乏技术手段。

解决方案

亿赛通数据泄露防护（DLP）系统是一款基于内容识别技术的保护系统。

终端防护：防止敏感数据通过打印、刻录、聊天工具、发送邮件等终端方式泄露出去。

网络防护：防止敏感数据通过邮件、网盘、微博、FTP、论坛等网络方式泄露出去。

数据扫描：通过扫描和分类的方式，随时随地发现企业敏感数据分布，并保护静态数据。

邮件防护：防止敏感数据未经任何检查通过企业邮箱泄露出去。

数据分析：基于规则和中文语义的智能数据分析，对数据进行高效敏感检查。

审计报表：提供统计分析能力，实现安全现状可度量、事件可追溯、态势可查询。

项目成果

亿赛通完善的数据泄露防护（DLP）解决方案，为中集集团建立了一套数据资源保护标准，防止员工的不安全行为引入风险，以及保障了各个环节数据的安全运行，并且使得员工了解与自己相关的数据安全保护责任，强调数据系统安全对企业业务目标的实现、以及业务活动持续运营的重要性。

亿赛通签约 ABB（中国）有限公司

客户简介

ABB 集团是全球 500 强企业之一，总部位于瑞士苏黎世，在苏黎世、斯德哥尔摩和纽约证券交易所上市交易，是全球电力和自动化技术领域的领导企业，致力于为工业、能源、电力、交通和建筑行业客户提供解决方案，帮助客户提高生产效率和能源效率，同时降低对环境的不良影响。ABB 集团的业务遍布全球 100 多个国家，拥有 15 万名员工。

需求背景

ABB 集团是全球大型级上市企业，其业务遍布全球，工作内容往来都是通过电脑操作，为了防止如此庞大的业务数据、公司重要信息泄露出去，ABB 集团通过与多家数据安全企业沟通、了解其解决方案，最终在这些数据安全企业中选择与亿赛通携手合作，将亿赛通优秀精准的数据安全解决方案展开部署，实现 ABB 数据安全运行管理。

解决方案

电子文档安全管理系统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数据资产，对电子文档进行全生命周期防护。

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；

内容安全管控：截屏录屏控制文档、阅读水印文档、打印水印、拷贝粘贴控制；

安全分级控制：实现人员密级、数据密级的安全分级管理控制，满足组织数据分级安全管理要求；

身份认证集成：统一身份认证平台进行无缝集成，如实现组织构架及用户账号信息的自动完整同步和单点登录认证集成；

安全水印支持：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动打印所带来的泄密风险；

权限控制：每个用户都设有文件收件箱、发件箱、还原箱，方便对权限文档的使用和管理。用户还可以通过在线申请的方式向作者申请文档权限，申请和审批流程简单。同时考虑到文档离线使用情况，系统还可生成离线权限文件，并可设定文件的阅读次数和使用时长。

项目成果

亿赛通电子文档安全管理系统促使了 ABB 集团整个工作效率的大幅度提高，并且让庞大的工作体系更加有序进行，也同时加快了项目进展、加强了所有员工的数据保密意识，让 ABB 所有员工在一个安全、高效、有序的环境中积极热情的工作。

亿赛通签约佳通轮胎（中国）投资有限公司

客户简介

佳通轮胎是中国最大的高品质轮胎的制造商和供应商，总部位于上海。公司可提供全系列型号的轮胎，并通过中国境内庞大的销售网络进行销售。同时，公司的产品出口到世界 80 多个国家和地区。佳通轮胎目前致力于作为中国面向世界最大的轮胎市场的主要供应商。佳通轮胎有 5 家世界级工厂，并拥有国际级的优质产品和成本竞争优势，这些都使得佳通轮胎能在轮胎制造行业内跻身世界前 13 强。

需求背景

通轮胎由于企业规模庞大，分支机构繁多，信息管理难度较大。并且企业信息环境复杂，应用系统数量庞大，产业链较长，设计外部数据信息接入以及对外交互数据信息需求频繁。同时，在数据安全管理和数据应用效率两方面难以均衡。如何才能更好保障企业数据安全、有序的管理数据？佳通轮胎从众多数据安全厂商中选择亿赛通与其共同管理企业的数据安全。

解决方案

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。

可以实时记载用户对文件的操作记录；

可以根据用户的需要设置不同的安全级别；

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；

文件加解密过程均自动完成，对用户完全透明；

文件从制作完成到生命结束都是以密文形式存在。

项目成果

佳通轮胎通过部署亿赛通文档安全管理系统后，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。