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

10 月刊

2018 年共 11 期

亿赛通为运营商行业构筑数据安全保护墙

紧急提醒：科技公司高危漏洞，网络安全形式严峻

五角大楼数据被攻击，

黑客认准供应链最薄弱环节……

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

安全圈形势严峻，《亿赛通十月刊》与您共同保障企业数据安全，构建安全网络

近年来，随着用户对数据泄露防护意识的不断增强以及泄露形势的日益严峻，数据泄露防护市场获得了比较快速的发展。市场也已渡过了行业初期的混沌状态，进入到群雄并起阶段。国内数据泄露防护现有的产品及解决方案涵盖了系统监控与审计、电子文档加密、敏感数据防泄漏、勒索病毒防护、网络入侵防御、移动存储介质防护等多个方面。其中，亿赛通凭借长期的研发积累、良好的产品性能和雄厚的资金实力，逐渐占据了相对领先的市场地位。

而信息安全、网络安全、数据安全成为普罗大众的民生问题，安全厂商接下来该如何前行？我们共同期待中……

国内

1、河北破获非法篡改网络数据库、伪造买卖证件案梳理

摘要：10 月 23 日，河北省公安厅对外发布，2018 年 10 月，邯郸市中级人民法院开庭审理一起非法篡改网络数据库、伪造买卖证件案。这是近年来，我省警方侦破的首起非法篡改网络数据库案。经查，该犯罪团伙涉嫌通过网络搜集攻击漏洞、网上发布需求、恶意篡改考试结果、伪造考试合格证书，涉案金额达 600 余万元。专案组奔赴多地进行抓捕，最终打掉这个团伙，16 名犯罪嫌疑人落网。

2、帮朋友个“小忙”泄露报警人信息 辅警被判刑一年

摘要：警务辅助人员，在没有相应职权的情形下，利用职务之便，非法获取并向他人提供报警人手机号码信息，损害国家机关权威以及公众信赖利益的同时，还导致报警人与被报警人双方发生激烈冲突，一人重伤。日前，苏州市虎丘区人民法院对此案依法作出判决，被告人李某犯侵犯公民个人信息罪，判处有期徒刑一年，并处罚金三千元。

3、揭秘河北非法篡改网络数据库案：4 级中间人层层牟利

摘要：河北邯郸警方侦破一起非法篡改网络数据库、伪造买卖假证案，16 名嫌疑人落网。经查，该罪团伙涉嫌通过网络搜集攻击漏洞、网上发布需求、恶意篡改考试结果、伪造考试合格证书，涉案金额达 600 余万元。

4、80 后网警受贿两千万：将查获的源代码交他人开赌场获利 2 亿

摘要：江苏淮安 80 后网警程俊山将办案中查扣的赌博网站源代码提供给犯罪分子开设另一个赌博网站，在赌博网站运营期间，还成为犯罪分子的“保护伞”，通风报信、逃避查处，犯罪分子非法获取暴利高达 2.3 亿元。他自己被法院认定共计收受了 2000 余万元的贿赂。

5、企业内部个人信息泄露危害大 完善管理制度迫在眉睫

摘要：今年 2 月，江苏无锡警方网安部门在网络巡查中发现，某网络软件聊天平台上，有人打出了代查各类信息的广告，发布广告者只是犯罪团伙中的冰山一角。无锡警方发现不法分子通过网络软件、聊天群串联，形成一个完整的非法交易市场。在这里，个人征信、银行账户等数十种公民个人信息被明码标价、挂牌出售。

6、华夏银行技术处长编写病毒植入系统，盗窃 700 余万受审

摘要：利用职务便利，在华夏银行总行核心系统内植入计算机病毒程序，使跨行 ATM 机取款交易不能计入账户，之后成功取款 717.9 万元非法占为己有。

7、株洲警方侦破一起入侵政府网站、伪造国家机关证件连环诈骗案

摘要：近日，株洲市公安局荷塘分局成功破获一起利用非法手段入侵国家政府网站，伪造国家机关证件实施电信诈骗案件，刑事拘留 3 人，涉案金额近六十万元。

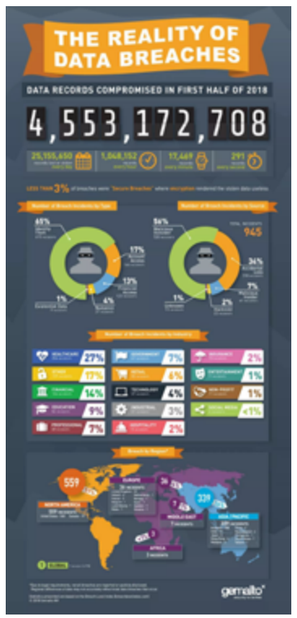
8、国泰航空 940 万乘客数据外泄

摘要：本周三晚上，香港国泰航空公司（CathayPacific）向香港证券交易所告知一起涉及 940 万人的数据泄露事件，乘客姓名、国籍、出生日期、护照号码等个人信息遭泄露。

9、上海网信办约谈本地 23 个 App 要求整改、加强信息保护

摘要：近日，上海市网信办近期对本地最常用的 23 个 APP 获取用户个人信息等相关权限申请情况开展抽查，发现其中约 30% 与所提供的服务没有对应关系，属于不合理范围。12 日和 15 日，市网信办分别约谈了运营这些 APP 的 23 家企业，要求认真整改。

10、2018 年上半年的数据泄露事件 危及 45 亿条记录



摘要：数据泄露水平指数 (Breach Level Index) 的最新调查结果，分析了 2018 年上半年导致全球 45 亿条数据记录受到侵害的 945 次数据泄露事件。与 2017 年同期相比，虽然泄露事件的总数量略有下降，但丢失、被盗或外泄记录的数量增加了惊人的 133%，表明每次事件的严重程度有所增加。

国外

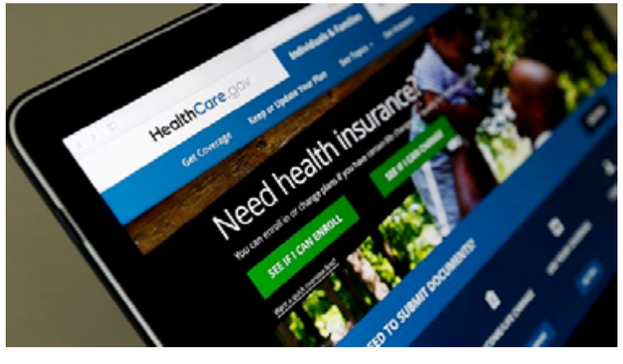
1、英国航空数据泄露受害者远超预期，或将面临 5 亿英镑巨额罚款

摘要：据外媒 ZDNet 报道称，一位安全研究员在 Craigslist 网站上发现了属于加拿大知名电脑零售商 NCIX 的客户和员工数据，且最早创建的数据可以追溯到 10 多年以前。

2、一个归属于美国茶党的 S3 存储桶意外暴露了近 52.7 万选民的个人信息

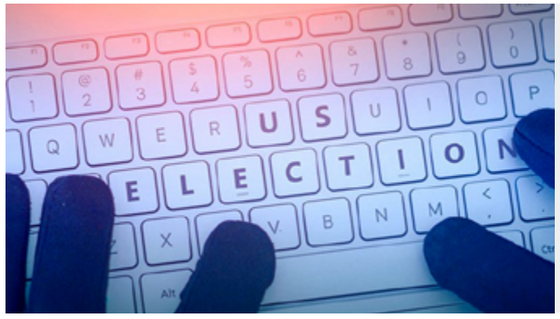
摘要：UpGuard 网络风险团队于近日透露，一个归属于美国茶党爱国者公民基金（Tea Party Patriots Citizens Fund，TPPCF）的亚马逊 S3 存储桶因为一个配置错误，意外暴露了包括全名和电话号码在内的 52.7 万选民的个人敏感数据。

3、美国政府网站 HealthCare.gov 被黑，致 7.5 万人敏感信息泄露



摘要：据负责该政府门户网站的机构称，在本月早些时候，他们在一个与 HealthCare.gov 交互的政府计算机系统中发现了一起黑客攻击行为，导致大约 7.5 万人的敏感个人数据遭到泄露。

4、来自美国 19 个州的 3500 万选民记录被曝正在暗网兜售



摘要：据外媒 ZDNet 报道，两家威胁情报公司于最近发现大约 3500 万美国选民的个人信息正在一个热门的暗网论坛上被兜售，共涉及到 19 个洲。

行业聚焦 INDUSTRY FOCUS

5、美联社：美官员称五角大楼数据泄露事件至少会影响到 3 万名雇员

摘要：五角大楼于本月表示，美国防部的旅行记录因黑客攻击遭到了窃取，这些记录泄露了美国军方和文职人员的个人信息和信用卡数据。数据泄露可能影响了多达 3 万名五角大楼雇员。黑客攻击可能发生在几个月之前，但直到最近才被发现。

6、FitMetrix 健身软件开发公司 119GB 用户数据被指在线暴露

摘要：据外媒 ZDNet 报道，大量 FitMetrix 用户的个人资料被国际网络安全咨询公司 Hacken 的网络风险研究总监 Bob Diachenko 发现通过一组 ElasticSearch 服务器暴露在了网络上，所包含数据的总大小超过 119GB。

7、Google 因数据泄露关闭 Google+ 消费者版本

摘要： Google 宣布关闭 Google+ 的消费者版本，缘由是缺乏使用率以及 API Bug 可能导致 50 万 Google+ 帐户的个人信息泄露。

8、16 岁澳洲少年黑客侵入苹果公司系统

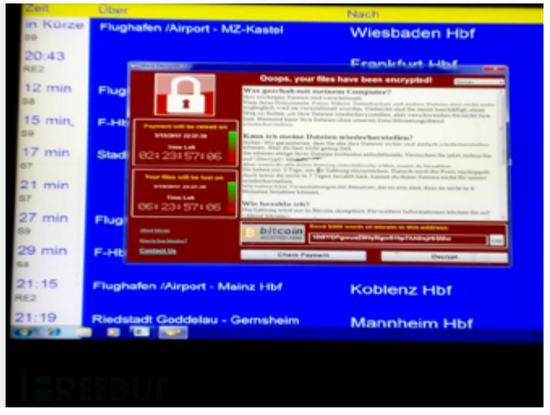
摘要：一名澳大利亚少年承认自己在过去的两年里曾多次侵入苹果公司系统并下载了大约 90GB 的机密文件。根据法庭文件显示，现已成年的被告在入侵苹果公司系统时年仅 16 岁。

9、史上最大数据泄漏案和解，雅虎向 2 亿用户赔偿 5000 万美元

摘要：10 月 24 日消息 ,据 NBC News 报道 ,雅虎已经同意向 2 亿用户支付 5000 万美元（约合 3.47 亿元人民币）赔偿金，并为他们提供为期两年的免费信用监控服务。在此前发生的、有史以来最大的安全漏洞案中，这些人的电子邮件地址和其他个人信息被盗。

10、时至今日 英国卫生部门还在为 WannaCry“擦屁股”

摘要：10 月 12 日据外媒报道，英国卫生和社会福利部公布了一些新进展。它们居然还在为“想哭”（WannaCry）病毒“擦屁股”，去年英国国家医疗服务系统（NHS）的 IT 设施被“想哭”病毒打的“放声大哭”。病毒为 NHS 带来了超过 9200 万英镑的巨额损失。这些损失包括 1900 万英镑的产出损失（NHS 的工作中有 1% 被“想哭”病毒干扰），而剩下的 7300 万英镑都花在“灾后重建”上了。



亿赛通加入广东省粤港澳合作促进会金融专业委员会，阻绝金融数据安全隐患

2018 年 10 月 26 日，广东省粤港澳合作促进会金融专业委员会换届大会正式召开，广东省粤港澳合作促进会是经广东省委、省政府同意，由广东省民政厅批准成立的具有独立法人地位的社会团体，汇聚了粤港澳三地关心和支持粤港澳合作的知名人士和业界代表，是促进和加强粤港澳民间合作的桥梁和纽带。

官方支持，行业认可

多年来，广东省粤港澳合作促进会金融专业委员会的工作，得到粤港澳三地政府和金融界有识之士的高度重视和大力支持，金融专业委员会在粤港澳三地业界的影响力和带动力日益增强，合作取得了新的突破。当前，中央政府加大力度推进粤港澳大湾区建设，委员会以独特角度和角色，肩负促进粤港澳三地金融行业合作的使命，凝聚了三地金融行业上千位业界精英。全力推进粤港澳三地社会、文化、经济等各领域的交流与对接，取得了良好成绩和效果，得到了粤港澳三地行业内的广泛认同，成为促进合作的重要力量。

亿赛通正式加入委员会

亿赛通董事长及精英同事作为委员会特聘成员之一出席换届大会，未来公司将携手粤港澳地区金融行业各大专业机构、事务所、企业共同整合商业秘密保护的管理、法律和信息技术资源。打造金融行业秘密保护的事前风险防范、事中调查取证、事后维权救济的全方位、立体式的保护机制，帮助金融企业建立健全的商业秘密保护体系，解决行业后顾之忧。

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，企业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。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，必定会成为三地金融科技领域数据信息背后有力的保护者，为金融行业的创新建设做出贡献！

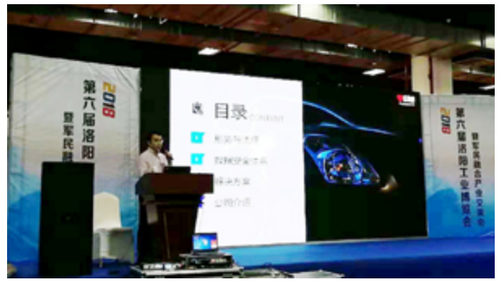
关于亿赛通

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，是绿盟科技全资子公司，十五年风雨兼程，已发展成为国内数据安全、网络安全及安全服务三大业务供应商。拥有完全自主知识产权的软件企业，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。

亿赛通走进洛阳数据防泄漏及涉密计算机安全防护体系建设研讨会

2018 年 10 月 25 日中原军民联合产业联盟在洛阳会展中心举办了“数据防泄漏及涉密计算机的安全防护体系建设”研讨会。

随着信息化建设的不断深入，信息系统的安全性已经成为“军转民、民参军”过程中面对的重要问题，如何防止数据泄漏？涉密计算机如何防护？如何做到军工企业精细化，分类分级管控等合规性要求？这不仅关乎企业的命运，更关乎国家的安全。

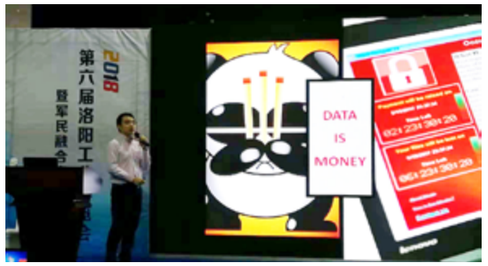


信息化社会中竞争的制胜关键，说到底是核心技术能力的竞争，作为企业领导者，我们都不愿意将自己的核心技术透露给竞争对手，那将直接或间接导致我们在市场中处于下风。本次亿赛通针对企业运营过程中可能出现的数据泄漏和外来攻击，提出了一整套完善的解决方案，受到了许多企业管理者的欢迎。

如何让安全隐患无处遁形？亿赛通相关专家在会中进行“细说数据分析”的演讲，过程中分析了目前互联网安全中国家强力支持的政策法规，企业遇到的威胁，同时针对遇到的安全隐患和攻击，分享亿赛通优秀的数据安全解决方案。其中数据泄漏防护系统充当着保护企业信息安全的角色并且是本次会议的介绍重点。

DLP 助力企业实现数据资产安全智能管控

数据泄漏防护系统基于内容识别技术的综合智能数据安全管控平台。从终端防护、网络防护、邮件防护、数据扫描、数据分析、审计报告等多个环节发现、识别、分类企业敏感数据，监控企业敏感数据使用情况，保护企业敏感数据以防丢失和被窃。亿赛通 DLP 以其自身的先进性、创新性、完整性、拓展性和集成性提供对企业内网综合一体化的防护，做到敏感数据可保护、安全态势可度量、安全事件可追溯，帮助企业提升等级管理建设能力。

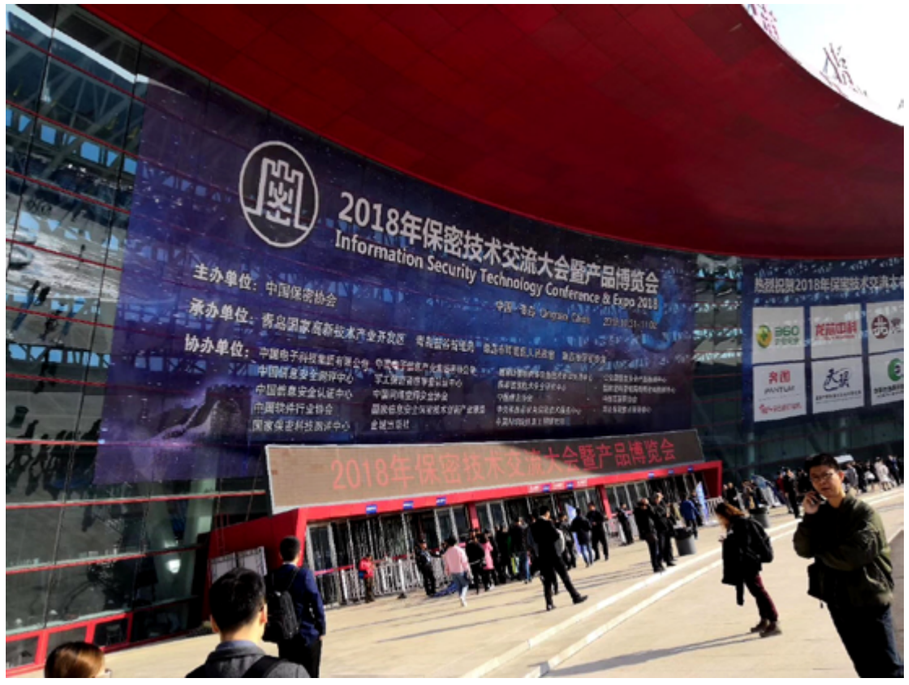


互联网快速发展的大数据时代，每个人几乎每时每刻都在产生数据，信息安全问题引起人们的恐惧和关注。国家加大信息安全的监管，规范网络信息的安全管理，打击违法犯罪活动，在高速发展，信息繁多的大数据时代，网络安全问题成为一个永恒的话题，保护信息安全任重而道远。

亿赛通是国内最早专业从事数据泄漏防护研究的高新技术企业及双软认证，所有核心技术及产品均为自主知识产权，并在全球范围内，提供基于自身核心竞争力的数据安全解决方案，成为最受客户信赖的数据安全公司。15 年客户服务积累，合作客户上万家、保护终端数超过几百万，并在国内各大区域拥有办事处和技术支持中心，为用户提供本地化支持及服务。

亿赛通未来会继续努力携手更多企业，从技术层面为信息安全保驾护航，防止各种黑客入侵、病毒侵袭、数据泄漏等事件上演。

亿赛通 & 绿盟科技完美亮相青岛保密展，共同保护信息安全产业良好生态



为深入贯彻落实中央关于保密科技创新的决策部署，10 月 31 日至 11 月 2 日，2018 年保密技术交流大会暨产品博览会在青岛国际博览中心举办。大会以“坚持创新驱动，携手打造保密产业良好生态”为主题，全面展示最新信息安全保密技术和科研成果，积极推动产业与用户、企业与企业、国际与国内保密技术合作交流，增强机关单位保密意识，普及公众信息安全保密防范常识，充分发挥保密科技发展政策引领作用、市场资源配置作用、企业创新主体作用，不断提高保密技术研发和产业发展水平。

绿盟科技 & 亿赛通在数据安全行业凭借优秀的品牌影响力、前沿的核心技术、强大的研发能力、广受市场信赖的产品、优秀丰富的数据安全解决方案共同参与本次技术交流大会。

展会上，绿盟科技 & 亿赛通紧扣大会主题，促进信息保密技术行业的交流与合作，针对企业核心数据的泄露防护提出了独到见解。通过了解用户内部 IT 架构、为企业核心数据进行智能识别、明确工作流程及设置安全策略等多维度进行思考。展台前问询观众接连不断，参会人员热情高涨，为每位前来询问的客户提供详尽的解答。整个交流会期间，绿盟科技 & 亿赛通以独特的解决方案和备受关注的技术、产品引爆现场，引起领导和全场观众的重视。

亿赛通作为中国数据安全防护专家，一直致力于为用户提供最优质的数据安全解决方案，以防止企业因无意泄露、故意泄露和恶意泄露所带来的各种风险。如何确保企业在当前 IT 技术越来越发达之时，对核心机密数据进行安全保障，是企业未来迫切需要处理的问题。

在大数据、云计算、互联网、人工智能等等的智能时代与数字经济的大背景下，亿赛通与时俱进、不断自我突破，坚持专注数据安全行业，为国内外企业不断提供最佳方案 ,保障企业实现数据资产安全。保护数据安全，亿赛通竭诚与您携手共进，并继续构筑市场占有率连续多年稳居第一的骄人战绩，继续做好中国数据安全防护专家。

五角大楼数据被攻击，黑客认准供应链最薄弱环节……

“安全”与“漏洞”

在信息化的网络时代，各种失窃行为都已利用高技术、高科技的信息化手段进行非法活动，所以无论企业、个人以及国家，各行各业都高度重视数据资产的保护。频繁发生的泄露事件，一次又一次用刻骨的事实为信息安全管理敲响警钟。在互联网环境中，攻防对抗一直在进行，但很多时候还是存在安全上的漏洞，一直到事件彻底曝光之前，大多数管理者都处于一无所知的黑暗中……

国防部旅行记录暴露 遭黑客窃取

据美联社报道，五角大楼表示美国国防部的旅行记录因黑客攻击遭到了窃取，这些记录泄露了美国军方和文职人员的个人信息和信用卡数据。数据泄露可能影响了多达 3 万名五角大楼雇员。随着调查的继续，这一数字可能还会增加。黑客攻击可能发生在几个月之前，但直到最近才被发现。国防部仍在收集有关这起黑客攻击的规模、范围以及攻击者的信息。

五角大楼发言人约瑟夫·布奇诺中校表示，这起攻击针对的是一家商业供应商，而该供应商只为国防部雇员中的很少一部分人提供服务。黑客将目标放在承包商身上，是因为他们通常被认为是政府供应链中最薄弱的环节。在供应商的服务器系统中，往往存在明显的安全漏洞，让黑客有机可乘。

供应商面临的危险从哪来？

第一：技术安全风险因素

① 重视不够，投入不足。

② 安全体系不完善，整体安全还十分脆弱。

③ 关键领域缺乏自主产品，高端产品严重依赖国外，无形埋下了安全隐患。

第二：人为恶意攻击

相对物理实体和硬件系统而言，精心设计的人为攻击威胁最大。人的因素最为复杂，思想最为活跃，不能用静止的方法和法律、法规加以防护，这是信息安全所面临的最大威胁。

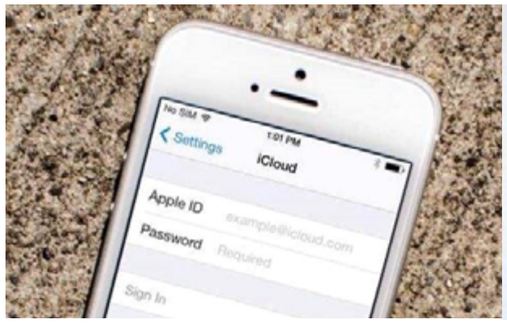
第三：信息安全管理薄弱

信息泄露、破坏信息的完整性、拒绝服务、非法使用（非授权访问）、窃听、业务流分析、假冒、旁路控制、授权侵犯、抵赖、计算机病毒、信息安全法律法规不完善等等，这些情况都会给信息窃取、信息破坏者以可趁之机。

中国数据安全防护专家—亿赛通助力数据所有者实现信息资产的安全，并始终肩负使命为您提供有竞争力的数据资产安全解决方案和服务。

亿赛通解决方案是以数据内容为核心 ,针对数据在使用、存储和流转过程中的安全问题，有机整合亿赛通文档安全管理系统、数据泄露防护系统、终端数据防护（DLP）系统、文档加密安全网关系统、数据资产内容安全管理系统等多个安全产品，打造全方位、立体化、多层次的企业数据安全防护体系，有效的防护企业核心数据资产，保障企业竞争力，提高企业数据可用性和安全性。从而帮您消除技术风险、人为恶意攻击、信息安全管理薄弱等各种困扰；有效的防止敏感数据在打印、刻录、发送邮件、FTP、论坛、网盘、黑客攻击、间谍窃取等等方式泄露出去，同时降低企业运营成本，加强内网、外网一体化的安全意识，提升企业品牌形象。

紧急提醒：科技公司高危漏洞，网络安全形式严峻



作为“安全”防护小贴，

听到这样的消息，

只想原地爆炸，

没错，是原地爆炸！！！

怎么搞的啊？？？

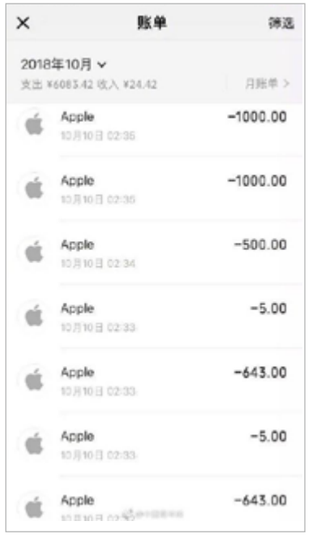
科技公司又爆存在漏洞？

这么多的敏感信息泄露，

后果很严重，很严重，很严重……

爆料 1

支付宝在官方微博发出安全提示称，监测到部分苹果用户的 ID 出现被盗，由此带来相关 ID 绑定支付工具遭到资金损失。在声明中，支付宝称，已经联系苹果公司尽快定位被盗原因，同时建议用户调低免密支付额度以最大限度保护支付宝账户安全。



爆料 2

美国科技公司亚马逊（Amazon）被爆员工通过中间人贩卖内部销售数据、用户邮件地址和一些账户权限等。比如，商家可能通过贿赂亚马逊员工而删除产品的差评。报道称与亚马逊深圳员工有联系的中间人通过微信贩卖亚马逊的机密，信息以 80 美元到 2000 美元不等的价格出售。

爆料 3

Facebook 数据再次遭到黑客入侵，有 5000 万账户信息遭到泄露。黑客可看到账户的全部个人资料，包括家人、朋友的身份信息以及个人隐私照片等。

爆料 4

《华尔街日报》报道称，谷歌今年春季内部调查发现 Google+ 可能导致几十万用户私人数据泄露的软件漏洞，然后随后对公众隐瞒此事。谷歌母公司 Alphabet 宣布一系列用户隐私保护政策，其中包括十个月内逐步关闭消费者版本的 Google+。

这几次事件的发生，仅仅只是科技巨头用户信息安全风险的一个缩影。近年来，Facebook、谷歌等科技巨头安全问题频发，客户隐私屡屡遭到侵害。业内人士指出，“网络环境中的威胁不断升级、进化，2018 年上半年，我们观测到大约 28 亿次攻击，从 2017 年到 2018 年，攻击规模和范围急剧扩大。”

看完几次事件经过，小帖发现均是由安全漏洞引起。有网友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。确实，技术是解决企业安全问题的关键。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苹果、谷歌、亚马逊和 facebook。然后，就算存在安全漏洞导致数据泄露，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。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。

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。

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。

亿赛通为运营商行业构筑数据安全保护墙

运营商行业分析

近年来，业内随着信息安全管控点正在经历从网络安全到内容安全的转变，如何防止内部敏感数据、隐私信息泄露成为安全防护的重点。这就需要从数据内容本身出发，基于目标导向主动寻求一个整体的数据安全解决方案，来满足未来运营商信息化发展中面临的合规及风控需求。

然而，当下信息安全形势日益严峻，随着运营商企业信息化进程推进的同时，企业为了更好的提升员工的工作效率，不可避免地扩展了数据泄露的通道，尤其是内部员工的意外或者是主动泄密更是防不胜防。同时，在行业竞争日益激烈的市场中，难免会有间谍、黑客攻击企业重要数据资料，运营商面临着极大的数据安全威胁。

客户需求

在数据安全受到极大挑战的行业大环境下，尽管运营商经过多年的信息安全防护体系建设，在系统安全和内容安全方面已经初见成效，但是对于关键用户、关键岗位的数据安全仍存在薄弱环节，需要采用数据资产安全防护手段，有效防止数据通过电子邮件、QQ、web 上传、打印、刻录、文件改名、客户端私自拷贝数据等行为外泄，提升运营商数据内容安全的整体防护能力，有效降低敏感关键信息泄漏风险，因此急需通过防泄漏管理和技术的双重保护。那么，为更好的实现防护，满足业务发展和监管合规要求，必须解决当前数据内容防护层面面临的以下问题：

敏感数据识别难

1) 业支系统数据量大，数据关系复杂，难以进行梳理；

2) 无法判断出哪些数据是重要的；

3) 大量的结构化、半结构化、非结构化数据难于辨识；

4) 缺乏对数据内容的分类和敏感级别分级；

5) 保护措施无法和敏感重要级别挂钩，保护效能和效率较低；

敏感数据定位难

1) 对于重要敏感的数据存放位置无从知晓，保护难以下手；

2) 数据可能存放在电脑、手机、笔记本、业务系统、数据库、存储中；

3) 无法明确某类敏感数据在公司的整体分布情况；

4) 缺乏对不同数据在不同位置的风险评估视图；

重要数据防护难

1) 现有的以加密为主的防护覆盖范围小，因加密导致业务连续影响；

2) 以 DRM 方式为主的手动加密方式用户主动性差，容易防护失效；

3) 从网络、系统、终端多个维度都在管理，防护难以实现紧耦合；

4) 重要敏感的少部分核心数据缺乏整个流通通路的监控审计。

解决方案

亿赛通数据泄露防护系统（DLP）可以支持域同步，将组织架构和人员从业务系统中导出，通过安全准入网关对数据库系统采用准入，非公司人员无法下载文档的同时能够对文档实现“下载加密”功能，保证了数据的使用安全。通过外发插件有效管理，解决了联通某公司业务往来中的外发文档泄密的担忧。该系统可以记录文档、操作、系统等丰富的日志行为，实现对日常行为的审计，方便管理员查看近期情况，提高员工的保密意识。

方案价值

通过解决方案对运营商行业的核心数据和业务系统的数据泄漏风险进行管控，将有效增强数据泄密力度，为企业核心数据安全运行提供了强有力地保障。

部分经典案例

1、中国移动通信集团公司

2、中国联通公司

3、中国电信集团公司

亿赛通为集团企业客户部署最优解决方案，化解敏感信息泄露风险

集团企业行业分析

医药、房产、教育、烟草、物流、食品等行业，在每个集团企业都包括产品的研发、生产和销售环节。近年来这些行业发展速度快，行业成长能力较强，不断吸引国内外企业加入，市场竞争日趋激烈，这也促使了持续的产品研发和技术创新成为企业的发展核心，因此各行业对科技发展的依存度较高，具有高投入、高产出、高风险和高技术密集型等特点。随着市场竞争变得日益激烈，知识产权、经营策略、关键数据等作为核心资产亟需进行加强保护。

与此同时目前大部分集团企业经营过程中面临如下风险：

新产品开发风险：新产品研发投资大、周期长，产品的研发失败后会有丧失市场的风险，将影响到公司前期投入的回收和效益的实现。

行业监管风险：国内对各行业的研发、注册与生产过程都有严格的合规控制，所有企业必须经过合格认证，实行全面质量保证，确保产品质量。

市场竞争的风险：随着近年医药、房产、教育、烟草、物流、食品等行业需求的不断增加吸引更多国内外企业加入，市场竞争也变得日益激烈，知识产权、经营策略、关键数据等作为核心资产要加强保护。

高速成长的管理风险：同时随着公司业务经营规模的扩大，如何建立更加有效内部风险控制体系成为公司管理中面临的挑战，其中信息安全风险应受到重视。

需求分析

办公信息化在医药、房产、教育、烟草、物流、食品等行业中不断的成熟和深入应用，在各行业研发、生产制造和销售过程中，集团企业对管理和经营都依赖于信息化平台，各种内部系统如 OA、ERP、LIMS（实验室信息管理系统）、生产管理系统、质量管理系统、CRM 系统等，这些系统之间集中存放和处理着大量的敏感业务数据，如设计图纸、财务数据、经营数据、知识产权、销售数据、管理经营策略等等敏感数据都是这些行业的核心信息资产，若被有意或无意泄密将对企业的持续运营造成经济、声誉损失，甚至面临更为严重的监管处罚。面对日趋激烈的竞争环境，近年来如何保护这些数据资产在企业经营中的安全，已经成为这些行业的重点关注。企业要想在经营过程中可持续性发展，就必须面对和解决以下问题：

1、产品在研发过程中的研发数据不同应用场景下如何保护？

2、企业特殊敏感数据如何通过技术手段加密隔离访问

4、员工企业终端和移动终端办公敏感数据如何防止泄密和失密？

5、因业务需要外发到第三方人员或组织的敏感数据如何受控？

6、如何防止企业内部人员有意或无意泄漏重要敏感数据？

7、内部 OA、ERP、LIMS 等系统内关键敏感数据资产如何集中防泄密？

8、集团化企业如何贯彻关键财务及审计数据的统一安全策略？

9、公司的信息安全保密制度如何才能有效落地？

10、敏感数据保护如何从被动防御到主动管理？

解决方案

为确保企业产品从研发、制造到销售环节中敏感数据的安全，确保其在受控范围内安全的流转和使用，亿赛通通过多年的数据防泄密实践经验和产品研究，深入结合业务特点，制定数据泄露防护方案，协助集团企业保护关键资产安全，效果如下：

1、终端数据保护

1）由于研发部门代码、设计文档的特殊性和保密性，采用亿赛通数据泄露防护系统（DLP），确保研发类文档内部安全使用，防止数据的有意无意泄露，从源头保护数据文档安全。

2）对非核心部门采用文档权限加密产品实现数据保护，可以控制敏感数据的用户访问范围、文档使用操作限制，对敏感信息的内部使用实现高细粒度控制。

2、应用系统数据保护

采用文档安全准入网关，实现对 OA、ERP、LIMS 等业务系统中敏感数据保护，对上传到各应用系统中的文档进行解密存储，对从应用系统中下载的文档实现下载加密，且实现业务支撑系统的准入功能，保证了业务系统的数据安全。

3、数据外发安全保护

通过数据泄露防护系统（DLP）的文档外发管理功能实现市场、销售部门对外发送的敏感数据安全保护，有效解决了与外协人员、合作伙伴等的数据交互问题。

4、业务效率保障

1）不改变用户工作习惯和不影响业务工作效率；

2）通过加密网关实现终端与应用系统数据无缝集成；

3）系统内置单级和多级审批流程，让流转操作更快速容易；

4）通过邮件白名单可实现受信用户或伙伴数据自动脱密，降低沟通影响。

5、敏感数据操作行为追溯

所有涉及敏感信息的操作都会产生丰富的记录日志，可定期 / 不定期对员工行为进行审计，提高员工的数据安全保密意识。

方案价值

通过方案部署实施后，可以保障集团企业的数据在任何一个环节使用都安全，并且帮助企业更加有效、有序的管理企业资产，为企业带来更多经济收益。

部分经典案例

蒙牛乳业（集团）股份有限公司

上海德邦物流服务有限公司

云南红塔集团有限公司

花样年集团

金太阳教育

深圳市世方商业地产

成都全友家私

361 度

万科集团

达内时代科技集团有限公司

京汉置业集团股份有限公司

北京建筑大学

北京天地思高教育科技有限公司

北大资源集团控股有限公司

中国民航大学

NDO Technolgy Co,Ltd

长安大学

雅致集成房屋（集团）股份有限公司

亿赛通签约良品铺子股份有限公司

客户简介

良品铺子股份有限公司是互联网休闲零食品牌连锁运营公司，引导并超越休闲食品固有的品牌形象和销售模式。截止至 2014 年 3 月拥有门店数约 1200 家，员工超过 4000 人。12 年致力于休闲食品的研发、加工、分装、零售服务等专业品牌质量与文化的打造，同时深入线下连锁和线上电商同步发展，现已成为全渠道、全品类、O2O 发展的典范，是休闲食品品牌全国第一。

需求背景

随着良品铺子大力推进信息化建设，业务及盈利能力的不断攀升，作为电子商务行业的标杆企业，数据安全早已成为良品铺子经营的基础和前提。为了加强良品铺子企业数据内部流转，保证业务系统的存储及使用安全，防范数据泄露风险，建立一套完善的数据安全防护体系是良品铺子必然的发展战略。

解决方案

1、平台搭建：全新搭建最新正式版文档加密服务平台，新版部署完成后可同时支持 WIN10 及 AD 域。良品铺子通过蓝代斯克产品以及域推送客户端，客户端采用手动安装或者 AD 域推送方式，直接接入加密平台。

2、LINUX 客户端：在 LINUX 操作系统上安装加密客户端，支持 ubuntu、centOS、fedora 等主流版本，实现 linux 平台与 windows 平台加密互通，保障研发代码的安全性。

3、手机客户端：在智能手机上安装客户端，支持 IOS、Android 系统，实现智能移动终端可以正常使用加密文档，同时支持手机审批业务。

4、密级文件管控策略：依据良品商密保护规则，对不同密级文件下发不同策略，进行梯度式全方位管控。

5、审批审计：加密系统平台提供完整的解密审批流程及日志审计体系。

项目成果

亿赛通为良品铺子部署了文档加密系统平台，配合企业现有的保密制度，企业核心文档代码、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，从而规避过错性损失泄密，提升人员保密意识，保障各个环节数据的安全运行，避免了公司敏感数据遭窃的风险，提高数据安全管理，为良品铺子铸就了一道坚不可摧的安全防护基石！