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　中国数据安全防护专家　www.esafenet.com

6 月刊

2020 年共 11 期


# 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

2/3 数据安全隐患凸显，《亿赛通六月刊》带你寻求解决之道

行业聚焦 INDUSTRY FOCUS

4-8 国内行业新闻

9-13 国外行业新闻

亿赛通动态 ESAFENET NEWS

14/15 亿赛通加速释放渠道新动能，2020 全国渠道大会华南站圆满落幕

16/17 亿赛通与中国长城科技集团完成产品兼容认证，助力国产软件生态环境建设

18/19 诚信服务获认可，亿赛通被授予最高级别信用等级评价认证

20-22 赛迪报告权威发布，亿赛通稳居数据泄露防护市场榜首

亿赛通小贴士 ESAFENET PROMPT

23-25 新世纪的“石油和矿产”，我们共同“炼造”

26/27 @ 所有人，远程办公应该这么做……

28/29 黑客攻击瞄准游戏业，核心数据如何防范？

30/31 这些事件“触目惊心”，数据安全行业风起云涌

32/33 如何远离数据泄露的危险漩涡？

34/35 信息化办公企业的“高度风险”——数据泄露

典型案例 TYPICAL CASES

36/37 江苏豪森药业集团有限公司

38/39 长春金赛药业股份有限公司

# 数据安全隐患凸显，《亿赛通六月刊》带你寻求解决之道

受网络强国战略实施、“互联网 +”行动计划推进、网络安全立法、关键基础设施保护强化等国家产业政策和信息安全战略的影响，未来 3-5 年，国内信息安全产业将处于快速发展机遇期，亿赛通也有望实现快速的成长。现在和《亿赛通六月刊》一起回顾本月精彩大事记：

经过赛迪的权威调研，过去的 2019 年，亿赛通再次以傲人的营业额，稳坐中国数据泄露防护市场榜首……

亿赛通数据泄露防护系统经过测试，与中国长城科技集团股份有限公司产品完成兼容认证……

中国中小企业商业协会在本月对上百家企业信用进行考核，我司顺利取得 AAA 等级认证……

亿赛通全国渠道大会第一站顺利召开，与渠道伙伴再相聚，专家解说渠道政策，共议数据安全未来合作发展之道……



刊首语 PREFACE

国内

## 1、《金融数据安全分级指南》标准即将出台

ICS 35.240.40
A 11

中华人民共和国金融行业标准

JR/T XXXXX—XXXX

金融数据安全 数据安全分级指南

Financial Data Security - Guides of Data Security Classification

（送审稿）

（本稿完成日期：2020 年 01 月 13 日）

**摘要：**近日，全国金融标准化委员会发布通告称：《金融数据安全数据安全分级指南》（以下简称《指南》）经过草案稿、征求意见稿等阶段，已形成标准送审稿。《指南》（送审稿）也随该通告同时发布。据移动支付网了解，在今年 1 月《指南》开始对外征求意见，《指南》（送审稿）共分为六个章节，分别是：范围、规范性引用文件、术语和定义、目标原则和范围、数据安全定级、重要数据识别。《指南》详细说明了数据安全分级的原则、方法和流程，并在附件当中给出了《金融业机构典型数据定级规则参考表》。

## 2、《网络安全审查办法》与“新网络安全观”的构建

**摘要：**《网络安全审查办法》正式发布，相比《网络产品和服务安全审查办法（试行）》提供了更具针对性、更为详细明确的审查制度规定，从适用范围，到审查对象、审查机构、审查流程等方面出发构建了偏重供应链自主可控的“新网络安全观”。针对这一审查制度， 网络产品和服务供应链各个环节中符合审查适用范围的企业，从供应商到运营商，如何从自身角度出发把控合规风险和保障网络安全尤为重要。





## 3、两万学生信息遭泄露，高校为何成了重灾区

**摘要：**6 月 6 日，河南郑州某高校多名学生向媒体反映，学校近两万学生个人信息被泄露，以表格的形式在微信、QQ 等社交平台上流传。对此，该校官方微博在回应学生时称，目前已向公安机关报备。报道显示，这些涉及的个人信息覆盖近两万名学生，包括他们的名字、身份证号、年龄、专业甚至宿舍门牌号等，基本上都真实准确。这些隐私信息的四处传播，无疑让学生陷入“裸奔”的状态。


## 4、台湾全省 84% 的人员数据疑似被泄露


**摘要：**研究人员近日在暗网上发现圈内知名卖家“Toogod”放出了一个“台湾全省房屋登记数据库”的数据库，大约 3.5GB，该数据库包含 2000 万条记录。目前中国台湾人口为 2380 万人，这意味着差不多全体台湾人民的个人数据都遭到了泄露。数据库包含个人的全名、邮政地址、电话号码、身份 ID、性别和出生日期，这则泄露将成为有史以来最大规模的公众数据泄露事件之一。到目前为止，它尚无法确定数据泄露的时间，台湾就此事件正在进行调查。据暗网卖家透露，泄密事件始于 2019 年。

## 5、全国人大常委会调整 2020 年度立法工作计划：个人信息保护法、数据安全法草案将提请审议


**摘要：**2020 年 6 月 1 日，十三届全国人大常委会第五十八次委员长会议审议通过了调整后的全国人大常委会 2020 年度立法工作计划。6 月 20 日，调整后的立法工作计划对外公布。计划强调，适应党和国家事业发展需要，为疫情防控和经济社会发展工作提供法律支持，做好国家重大战略法治保障工作，加强重要领域立法。计划提出，围绕构建依法行政的政府治理体系，推进国家机构职能优化协调高效，修改行政处罚法、行政复议法，制定个人信息保护法等。

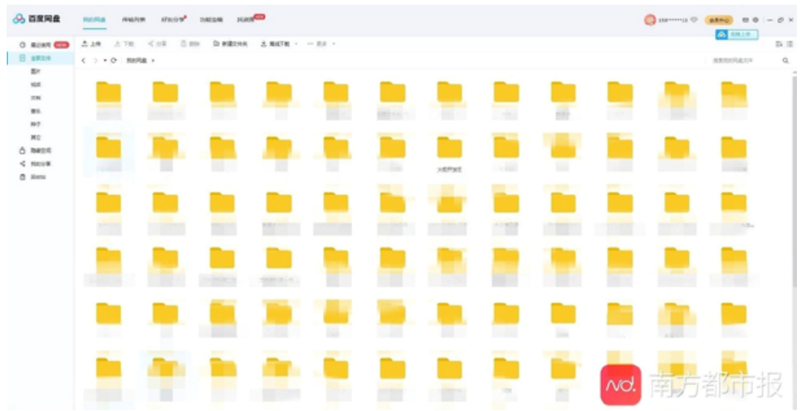
## 6、工信部部署推进 2020 年电信和互联网行业网络数据安全管理工作


**摘要：**近日，为切实做好 2020 年电信和互联网行业网络数据安全管理工作，工业和信息化部印发《关于做好 2020 年电信和互联网行业网络数据安全管理工作的通知》（以下简称《通知》），提出深化行业网络数据安全专项治理、深入开展网络数据安全合规性评估、加快推进网络数据安全制度标准建设、提升网络数据安全技术保障能力等年度行业网络数据安全管理重点工作要求。





## 7、造成 10 亿条个人信息泄露，4 家涉案中介公司被行政处罚




**摘要：**日前，南都记者从珠海市公安局高新分局获悉，该局网安大队在“净网 2020”行动中，成功侦破一宗特大侵犯公民个人信息案，累计查获涉及公民个人房产、车辆、公司法人、个人征信和贷款等公民个人信息数据 10 亿多条，数据量近 330G。并且查获一批作案手机、笔记本电脑及作案用云盘等作案工具，抓获并逮捕 3 名违法犯罪嫌疑人，并在拱北和斗门网安部门的协助下，依法对 4 间中介公司行政处罚。

## 8、贵州男子丢失身份证后被入职 16 家公司


**摘要：**因九年前丢了一张身份证，来自贵州的王伟（化名）近来饱受个人信息泄露的困扰。不久前，他在个人所得税 App 上发现，自己“被入职”了数十家公司，还是其中一家杭州公司的法人代表。不仅如此，调查过程中，他又发现自己被登记成为另一家杭州公司的监事。

## 9、14 万条学生个人信息泄露：非法收集要查清从何而来


**摘要：**据央视报道，江苏无锡江阴市市场监督管理局通报，在对某教育培训机构进行监督检查时，执法人员发现几十个标注了江阴各个中小学名称的 EXCEL 表，涵盖了江阴市绝大部分中小学学生和家长的信息资料，包括学生姓名、性别、所在学校、年级、班级、学生家庭地址、家长姓名及电话等个人信息 14 万余条。

## 10、客户差评后被威胁要泄露开房信息，酒店致歉并处理涉事员工


**摘要：**近日，王女士入住江苏苏州某酒店，因入住体验不佳，给了差评。据王女士称，酒店方为了删除差评，连续多次通过电话、微信协商，让她担心自己的隐私被泄露。昨日，该酒店在其官方微博中发布《致歉函》，称已严肃处理涉事门店的总经理、前厅经理以及当值员工。



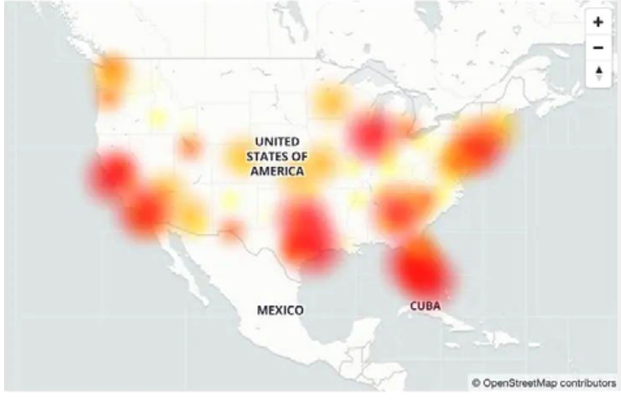


国外

## 1、美国中央情报局数据失窃，网络安全措施失范或为罪魁祸首

**摘要：**据调查，美国中情局前雇员从 “7 号军火库”（Vault 7）中偷走了该局最有价值的黑客工具，网络安全措施失范或为罪魁祸首。维基解密（WikiLeaks）网站公布了大量美国中央情报局（CIA）的内部文件。其中包括 CIA 组织的内部资料，对电脑、手机等设备进行的攻击方法，以及进行网络攻击时使用的代码和真实样本等等。有了这些材料和技术指南，广大电脑技术操作者不仅可以在各平台上的各类操作系统发起入侵攻击，还可以操作智能电视等终端设备，甚至可以通过遥控智能汽车，实施暗杀行动。

## 2、美国移动运营商 T-Mobile 周一通信中断，短信、电话均失效

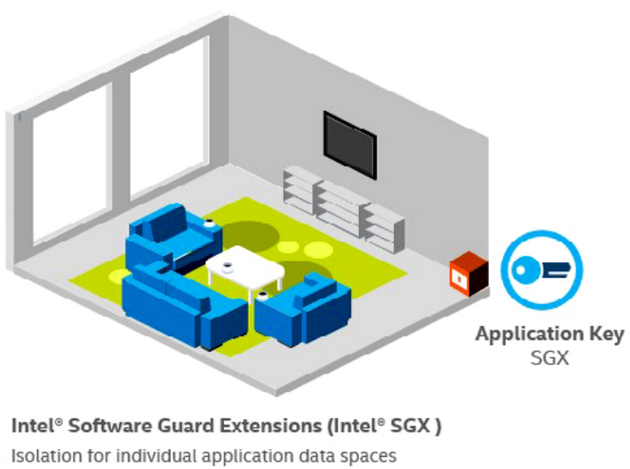



**摘要：**根据 Downdetector 和社交媒体上的用户报告，移动运营商 T-Mobile、Verizon 和 AT ＆ T 的客户在美国各地拨打电话时突发中断，大概时间在美国东部时间下午 2:20。AT ＆ T 表示，其网络“运行正常”，Verizon 亦说，其网络“运行良好”，而问题似乎完全出现在 T-Mobile 上，T-Mobile 承认，正努力修复“已影响到全国各地客户的语音和数据问题。”

## 3、特斯拉废弃零件存泄密隐患，谁为数据泄露买单


**摘要：**特斯拉的车载信息娱乐服务让用户享受非常便捷舒适的乘车环境。然而，在使用特斯拉车载信息娱乐服务前，用户必须输入详细的个人信息。日前，国外黑客发现，尽管这些废弃的媒体控制单元已经被特斯拉技术人员手工销毁，但仍然留有用户大量隐私数据，包括手机通讯录、通话记录、日历项目、WiFi 密码、家庭住址、导航去过的地点等。上述媒体控制单元可在国外交易网站 eBay 上进行交易，且价格并不昂贵。根据上面遗留的用户信息，黑客能够轻松获取到用户的个人信息。

## 4、英特尔处理器又曝两个 SGX 新漏洞攻击者可轻松提取敏感数据




**摘要：**正在英特尔努力消除多个处理器漏洞造成的负面影响的时候，三所大学的安全研究人员再次无情地曝光了 SGX 软件防护扩展指令的另外两个缺陷。对于攻击者来说，这可以让他们相当轻松地提取敏感数据。庆幸的是，新问题可通过积极的补救措施得到修复，且当前尚无新漏洞已在野外被利用的相关证据。

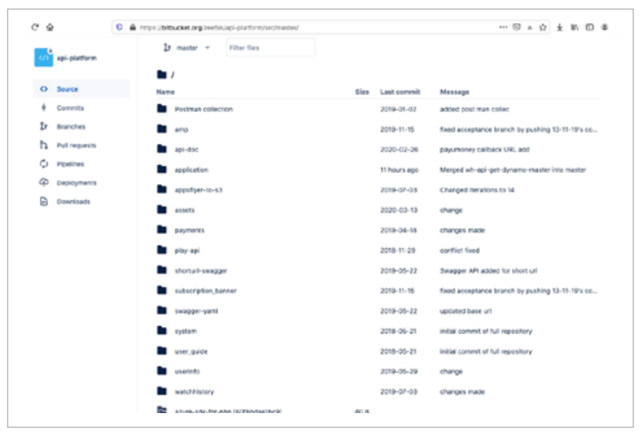




## 5、加拿大特许会计师协会网站遭攻击，33 万个人信息被泄露


**摘要：**加拿大特许专业会计师协会表示，其网站近日遭到网络攻击，据统计将会影响超过 32.9 万名会员和利益相关者的个人信息。该协会表示，这些信息包括姓名、地址、电子邮件和雇主名称，但密码和信用卡号仍会受加密保护不被泄露。不过协会仍警告称，被盗的数据可能会被用于电子邮件钓鱼诈骗，并提醒受影响的人要时刻“保持警惕”。

## 6、印度视频点播巨头 ZEE5 被黑，攻击者扬言出售窃取数据




**摘要：**近日据外媒报道，印度视频点播巨头 ZEE5 遭黑客入侵，同时，攻击者扬言要在网络犯罪地下市场上出售所窃取的数据库信息。早在今年 4 月初，网络安全研究人员在 Medium 上发表了一篇有关数据集的文章，其中包含了约 1023 个针对在线流媒体服务的 ZEE5 Premium 帐户的安全隐患。随后，该事件的起源可以追溯到今年的 4 月 12 日，当时在网上出现了一个名为“Zee5 Premium”的新数据集，其中披露了一些 ZEE5 高级用户的电子邮件地址和纯文本密码。

## 7、任天堂更新“用户账号被黑事件”进展：共有 30 万账号被入侵


**摘要：**这家日本游戏巨头最初披露信息称，共有 16 万个任天堂账号遭到入侵，泄露的个人信息包括账号所有者的姓名、电子邮件地址、出生日期和居住国等。但据任天堂公布的更新声明显示，另有 14 万个账号被泄露。声明称，继续调查的结果使得这一数字上升。任天堂表示，该公司重新设置了这些账号的密码，并与受影响用户取得了联系。声明重申，任天堂的所有账号中仅有不到 1% 受到了此次黑客入侵事件的影响。

## 8、WordPress 中已知漏洞被黑客利用，数百万网站数据库遭到窃取


**摘要：**据外媒报道，近期黑客组织试图利用主题和插件中的已知漏洞从数百万个 WordPress 网站窃取数据库凭据。对于此次 WordPress 面临的威胁，根据 WordPress 安全公司的研究数据，其防火墙在 5 月 29 日至 5 月 31 日之间阻止了超过 1.3 亿次尝试从 130 万个站点收集数据库凭据，请求的数量在 5 月 30 日达到峰值。随后，采访时表示，这些攻击影响了 WordPress 三分之一以上的客户，同时，该公司认为此活动针对的网站总数可能超过 1000 万。

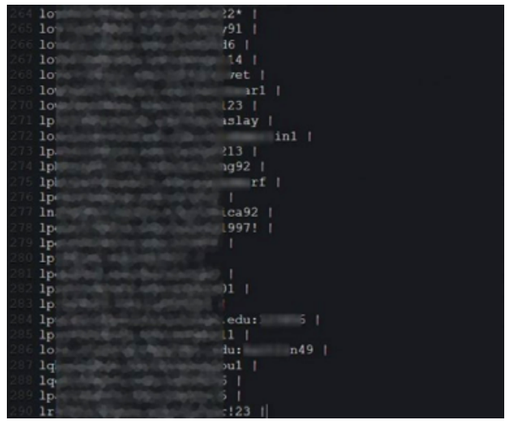




## 9、Foodpanda 发生数据泄露 72 万用户数据遭曝光

**摘 要：** Foodpanda 母公司 Delivery Hero 近日泄露了多达 72 万条用户资料，当中包括香港顾客用户帐号遭外泄的资料包括：姓名、电邮、电话、地址座标等数据该公司正积极展开内部调查事件起因。

## 10、Zoom 漏洞：超 50 万个 Zoom 账户泄露并在 Dark Web 出售



**摘要：** Zoom 被爆出漏洞，在 Dark Web 和黑客论坛上，超过 50 万个 Zoom 帐户可供出售，1 块钱可以买 7000 个。在某些情况下，是免费赠送的。这些凭据是通过凭据注入攻击收集的，其中黑客尝试使用在较早的数据泄露中泄露的帐户尝试登录 Zoom。然后将成功的登录名编译成列表，然后出售给其他黑客。大约 2020 年 4 月 1 日，他们开始在黑客论坛上看到免费的 Zoom 帐户发布，以在黑客社区中获得越来越高的声誉。这些帐户通过文本共享站点共享，黑客在该站点上发布电子邮件地址和密码组合的列表。在以下示例中，免费放出了与佛蒙特大学，科罗拉多大学，达特茅斯，拉斐特，佛罗里达大学等学院相关的 290 个帐户。

# 亿赛通加速释放渠道新动能，2020 全国渠道大会华南站圆满落幕

2020 年 6 月 20 日，”砥砺奋进 感恩共赢”亿赛通全国渠道大会第一站华南站正式拉开帷幕。亿赛通至今已历经十七年风雨沉淀，不断的深入剖析用户痛点，从专业角度出发，融合机器学习、大数据分析、态势感知等新技术，夯实安全服务。本次大会亿赛通与渠道伙伴再相聚，专家解说稳定并不断优化的渠道政策，共议数据安全未来合作发展之道。

近几年，新技术、安全事件、政策法规均推动数据安全产业发展，数据安全发展的核心机会点已经来临。亿赛通抓住关键节点，着眼未来，调整战略布局，依托数据安全领域的丰富实战经验，聚焦安全事件并紧跟行业趋势，研发态势感知、可视化产品。渠道大会中安全专家深入解读亿赛通战略转变的“ 天时、地利、人和 ”，全方位布局亿赛通数据安全新战略。








亿赛通综合解决方案不仅是简单的产品组合，而是针对企业内部部门需求不同，结合多种方案，进行整个企业的安全防护。今年，亿赛通推出“五大产品线”、“九大行业解决方案”，会中，数据安全专家从近年来的数据泄露事件出发，结合当下对数据安全的需求进行分析，探索典型行业的数据安全防护商机，打造“数据安全领域综合专业厂商”的智胜之道。

全球进入数字时代，数据安全重中之重。亿赛通从产品技术方案，到政策法律法规，再到典型客户实施经验，多方向透彻讲解，帮助渠道伙伴深入了解全方位数据安全防护体系，学习如何提供真正意义上全生命周期数据安全管理。同时，面对渠道伙伴，亿赛通严格要求每一个团队人员，对优秀渠道商采取鼓励制度，工程师重点培训，始终坚持以优质的服务标准为原则。今年，我司将继续深化数据安全生态圈合作，扩大与渠道伙伴的合作共建。


亿赛通坚持用专业的态度，认真为每一位客户服务。今后，我司会继续以专业的数据安全技术结合渠道伙伴对行业的深度理解，在这行业的爆发期，让品牌打响每一个角落。亿赛通与时俱进的数据安全解决方案和精准的市场眼光，坚定了渠道伙伴共赢未来的信心，点燃了渠道伙伴抢占市场先机的饱满热情。我们会继续与渠道伙伴携手并进，共谋行业发展蓝海，拓展更大的发展空间，以新布局新视野持续扩大行业优势，创造更多的市场价值。亿赛通渠道大会第一站华南站在紧张有序的环境中圆满结束，为后续会议敲响胜利的钟声，渠道大会第二站华东区即将召开，我们共同期待……

# 亿赛通与中国长城科技集团完成产品兼容认证，助力国产软件生态环境建设

产品兼容性认证

经 北京亿赛通科技发展有限责任公司 与 湖南长城科技信息有限公司 测试，得出以下结论：

北京亿赛通科技发展有限责任公司 的产品 亿赛通数据泄漏防护（DLP）系统 V5.0，与中国长城科技集团股份有限公司的产品 世恒 DF7 系列（FT-2000/4 + 银河麒麟桌面操作系统 V4）、世恒 KF5 系列（FT-1500A/4 + 银河麒麟桌面操作系统 V4）终端和 擎天 CF520（FT-1500A/16 + 银河麒麟服务器操作系统 V4）服务器可兼容。

特此证明！

北京亿赛通科技发展有限责任公司
2020 年 05 月

湖南长城科技信息有限公司
2020 年 05 月

近日，亿赛通的数据泄漏防护（DLP）系统 V5.0 经过湖南长城信息科技有限公司测试，与中国长城科技集团股份有限公司的世恒 DF7 系列（FT-2000/4+ 银河麒麟桌面操作系统 V4）、世恒 KF5 系列（FT-1500A/4+ 银河麒麟桌面操作系统 V4）终端和擎天 CF520（FT-1500A/16+ 银河麒麟桌面操作系统 V4）服务器完成兼容性认证。

测试结果显示，双方产品兼容性良好、性能卓越，系统运行高效稳定，满足用户关键性应用需要。此次，双方产品完成兼容性互认证，将极大促进双方在军工、政府、制造、金融、能源等国计民生重点行业的通力合作，进一步推动关键行业数字化升级和企业智能化转型。

中国长城科技集团股份有限公司（股票代码：000066）作为中国电子信息产业集团旗下网络安全和信息化的专业子集团，是网信产业技术创新大型央企和龙头企业，在计算机、电源、高新电子、金融信息化和医疗信息化等领域，成为中国自主安全信息系统的引领者。中国长城聚焦网信安全核心领域，成功突破高端通用芯片（CPU）、整机系统研发等关键瓶颈技术，筑牢“芯—端—云”网信安全底座，开启中国特色网信事业发展新篇章。

亿赛通数据泄漏防护（DLP）系统 V5.0 是亿赛通自主研发、拥有完全自主知识产权，是早期国产 DLP 产品。产品对企业设计图纸、源代码、合同文本、财务报表等敏感数据进行安全加密软件，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数据的防泄漏意识。

目前，亿赛通与多家国产主流操作系统厂商、国产服务器 / 终端机厂商完成了产品兼容性适配，精心打造满足用户客观需求的国产高效安全解决方案。未来亿赛通会继续完善自身产品，并不断推进与上下游厂商的协同合作，以形成更加安全高效的国产操作系统生态体系，更好地服务于广大用户。亿赛通也期待与更多厂商实现兼容，共同破解生态瓶颈。让我们共同携手，共建完整的安全产业生态圈。

# 诚信服务获认可，亿赛通被授予最高级别信用等级评价认证

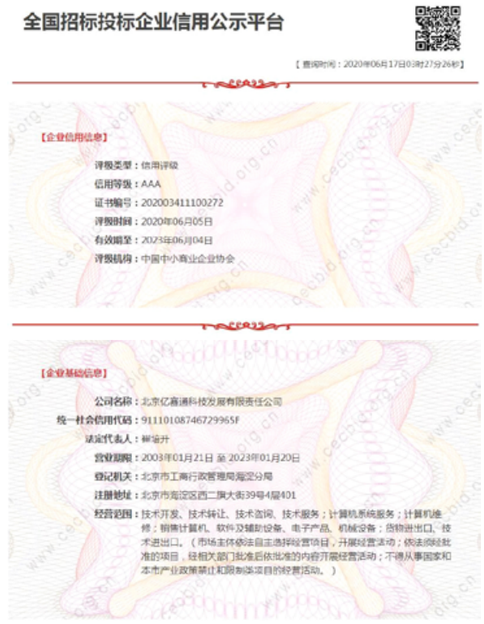

日前，北京亿赛通科技发展有限责任公司（简称：亿赛通），正式通过中国中小商业企业协会的信用状况考核，积极参与信用体系建设和实施，完善企业信用管理，树立信用企业典范，规范合同管理，注重质量、服务水平，特评定为 AAA 企业。

## AAA 信用认证的重要意义：

- 提升企业资质，获得国家政府的认可；
- 是企业履约能力、投标信誉、综合实力与竞争力的体现，在市场活动中不断塑造企业的信用形象；
- 获得 AAA 信用企业在工信部中小企业信用信息平台、发改委中国招标投标公共服务平台、中国招标投标信用公示平台、中国中小企业信用信息备案系统四个平台备案公示企业和企业上下游客户随时可查询；
- 所获“信用认证证书、认证标志”可在各类项目招投标、宣传材料等企业形象展示中合法使用。







## 为什么要成为 AAA 企业

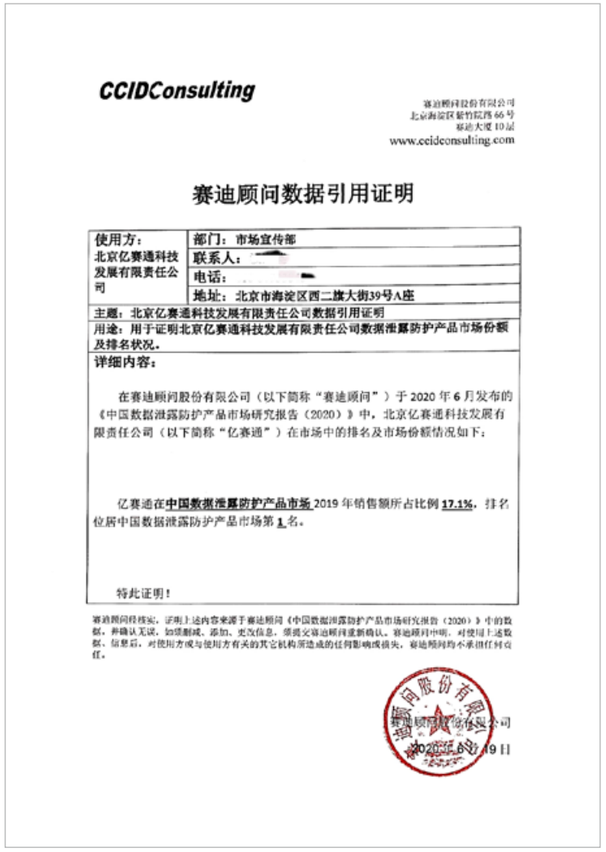
诚信是一个道德范畴，是我们的第二个“身份证”，不论是个人还是企业都应该以真诚之心，行信义之事。人无信而言不立，小信诚则大信立，大信立则赢天下。企业 AAA 认证即企业在信用等级优秀。

除成功认证企业 AAA 等级外，亿赛通一并加入到中国中小商业企业协会，成为其会员单位，为企业在全国范围内业务的进一步拓展开辟了一条新渠道。中国中小商业企业协会作为全国社会组织率先改革的试点单位，坚持打造多元化服务平台，开发点对点服务模式，创造立体式服务结构，逐步探索新常态下企业与协会共同发展之路。


亿赛通完善企业信用体系，从各方面达到了国家级标准，成功认证 AAA 企业，能够更有效保障用户核心数据安全，始终为客户提供最贴心的数据安全解决方案，打造“中国数据安全综合专业厂商”。

亿赛通动态 ESAFENET NEWS

# 赛迪报告权威发布，亿赛通稳居数据泄露防护市场榜首



CCIDConsulting

赛迪顾问股份有限公司
北京海淀区紫竹院南路 66 号
赛迪大厦 10 层
www.ccidconsulting.com

**赛迪顾问数据引用证明**

| | |
|---|---|
| 使用方：北京亿赛通科技发展有限责任公司 | 部门：市场宣传部 |
| | 联系人： |
| | 电话： |
| | 地址：北京市海淀区西二旗大街39号A座 |
| 主题：北京亿赛通科技发展有限责任公司数据引用证明 | |
| 用途：用于证明北京亿赛通科技发展有限责任公司数据泄露防护产品市场份额及排名状况。 | |
| 详细内容： | |

在赛迪顾问股份有限公司（以下简称“赛迪顾问”）于 2020 年 6 月发布的《中国数据泄露防护产品市场研究报告（2020）》中，北京亿赛通科技发展有限责任公司（以下简称“亿赛通”）在市场中的排名及市场份额情况如下：

亿赛通在**中国数据泄露防护产品市场** 2019 年销售额所占比例 **17.1%**，排名位居中国数据泄露防护产品市场第 **1** 名。

特此证明！

赛迪顾问股份有限公司
2020 年 6 月 19 日

赛迪顾问股份有限公司郑重承诺，证明上述内容来源于赛迪顾问《中国数据泄露防护产品市场研究报告（2020）》中的数据，并确认无误，如须删减、添加、更改信息，须提交赛迪顾问重新确认。赛迪顾问对使用上述数据、信息后，对使用方或与使用方有关的其它机构所造成的任何影响或损失，赛迪顾问均不承担任何责任。

## 多年连冠 稳坐数据安全江湖宝座

近日，赛迪顾问发布了《中国数据泄露防护产品市场研究报告（2020）》，报告显示，亿赛通凭借在数据安全领域防泄密产品的市场规模，稳居中国数据泄露防护产品市场占有率第一。

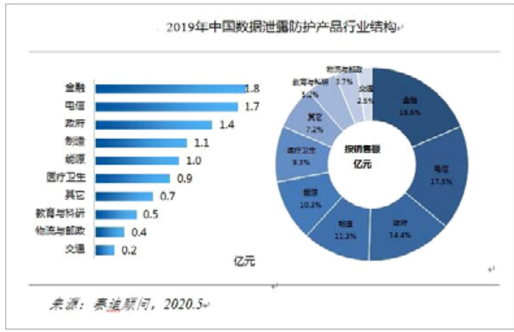
在 IT 数字化转型的进程加速下，政府、制造、运营商、地产、能源、金融、医疗等关键行业和企业信息化建设水平突飞猛进，但不同行业安全管理能力存有差异，现有的防御体系并未全面发挥对数据资产的控制和可见。同时国家层面上对数据安全政策合规性要求不断提升，在行业需求与国家政策浪潮的双轮驱动下，数据泄露防护市场迎来了良好的发展契机。

### 1、市场整体概况

赛迪报告认为，在市场规模上，数据泄露防护产品作为满足合规要求的重要产品，市场需求量快速增长，2019 年达到 9.7 亿元，增速为 18.7%。

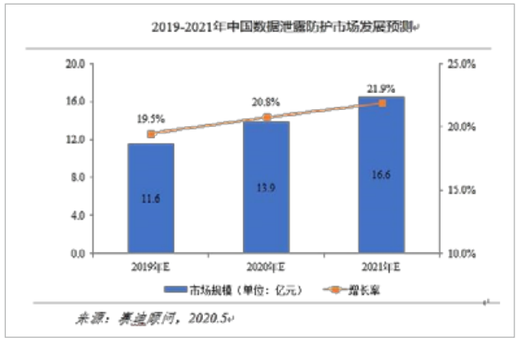

### 2、行业结构分析

在市场结构上，2019 年金融、电信、政府依然是驱动我国数据泄露防护产品市场增长的主导行业。此外，随着制造、能源等行业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。




### 3、未来市场规模

在市场预期上，未来三年，我国的数据泄露防护市场复合增长率将达到 20.9%，到 2021 年市场规模将达到 16.6 亿元。




赛迪同时对 2019 年数据泄露产品市场进行了分析，归纳了四点主要特征：

### 1、国家政策及制度建设推动产品市场需求释放

国家关于信息安全的政策不断出台，多项加强网络安全技术研发、推进产业发展的法律法规和政策措施密集发布，为网络安全产业的发展提供了良好的政策保障。

### 2、大数据的快速发展使得数据安全的需求快速上升

各领域都离不开数据和数字基础设施，各类大数据平台承载着海量的数据资源，大量敏感资源和重要数据的安全保护尤为重要。

### 3、数据安全专项厂商更具市场竞争力

相较于网络安全厂商与系统集成商，数据安全专项厂商，从强制防护手段的传统 DLP 起步，坚持强制加密的核心技术路线，大力推动数据高强力度保护，并经历了多年的发展和变革，在市场中具有显著影响力。

### 4、多场景、精细化、协同化的数据防护用户需求提高

未来将推出更多具备精细管控、全面防护、深度可视、协同防御、智能运维等特点的新一代数据安全产品。态势感知将成为持续安全监测、响应处置、调查分析与溯源的关键决策支撑；大数据安全分析平台作为积极防御的核心，

在结合 EDR 和 NDR 后也将使数据驱动的安全协同成为主流。

在技术发展层面，赛迪给出了四点发展趋势：

### 1、以大数据为核心的泄露防护

通过数据治理、安全机制、风险识别和审计溯源等重点识别和控制数据访问、应用和流转等动态过程中的安全风险。把握大数据环境中数据安全的本质和特点，从静态数据防泄露，过渡到分析挖掘和交易共享等动态使用和数据流动过程中的数据泄露防护。

### 2、产品技术向智能化方向发展

引入机器学习算法，完善数据自动发现与自动分析技术，提高策略设计精准度，提升事件分析效率，解决数据分类管理问题，动态展现敏感数据分布，快速处理海量样本，网络安全是综合性的系统问题，仅仅依靠几款单独的产品很难实现完整的信息安全保护，尤其是面向大中型机构，往往需要结合客户业务系统的实际需求，将多种产品相结合，制定以用户实际 IT 架构需求为基础的整体安全解决方案。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。

### 3、与其他安全产品统一部署

人工智能及机器学习的引入解决了海量日志中心化处理模式中对服务器资源占用大、日志消息堆积导致的安全时效性等问题。对于以日志审计为基础的大数据治理，可以经由人工智能引擎自动对企业数据资产进行采集、范化、增强、敏感数据分布、数据资产分类分级等高级可视化管理能力，进一步提升数据资产管理能力。

### 4、从注重防护走向注重数据治理

企业应该未雨绸缪，从治理层面摸清企业敏感数据分布与流动态势，对重要的数据资产服务器进行重点防护与安全配置检查，进行分类分级、数据脱敏和权限管控，定期进行漏洞扫描与评估等措施。

## 亿赛通为客户赋能，成为业界标杆

在旺盛的社会需求和抢眼的发展市场前，国内数据泄露防护市场呈现群雄逐鹿的局面。近几年，亿赛通重点关注创新和技术的融合及行业应用延伸，产品在市场上反响热烈，市场占有率不断提升，成为 2019 年数据泄露防护产品市场占有率第一。

为适应新环境下的安全分析需求，亿赛通数据泄露防护产品融合了机器学习、大数据分析、态势感知、可视化管理，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，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，实现安全与效率的双向平衡。

凭借技术创新优势，亿赛通数据泄露防护产品快速拓展至党政军、金融、地产、医疗、芯片半导体、运营商、能源等多个行业，为行业客户赋能，帮助客户建立合规、完整、高效的安全保障体系。未来，亿赛通也将始终执着于数据安全以及产品技术的研究，不断加深行业应用，为全局态势感知和业务不间断稳定运行提供安全保障。





# 新世纪的“石油和矿产”，我们共同“炼造”

售前技术部：张哲 / 文

随着互联网、物联网、云计算等新技术的广泛应用，企业在信息化过程中，产生了大量的电子化数据，这些数据已经成为我们企业或组织的重要经济资产，被誉为新世纪的石油和矿产。近两年，国家相关法律法规相继出台，数据防护不仅仅是企业发展的需求，更是企业一份责任和义务。


## 数据泄密无处不在

邮件泄密 -2016 美国总统大选

美国特种作战司令部明文员工数据被泄

WannaCry 勒索病毒全球大爆发

万豪旗下 5 亿客户信息泄露

社交媒体资料数据泄露 – 40 亿条记录

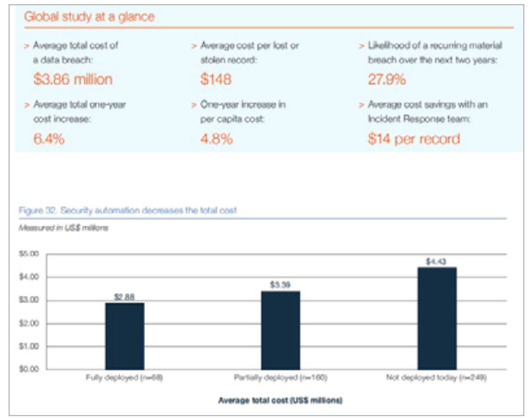
美国金融公司 8.85 亿数据泄露

……

## 泄密让你越来越慌

数据泄露的平均成本从 2017 年的 362 万美元上升到 386 万美元，平均每条失窃记录的成本从去年的 141 美元上升为 148 美元，而未来两年发生重大数据泄露的可能性是也略有上升。此外，事件应急响应团队能够挽回的成本约为平均每条记录 14 美元。

报告还表示，过去一年对于数据泄露事件的 MTTI（平均识别 / 发现时间）是 197 天，平均遏制时间是 69 天。与此同时，对于那些能够在 30 天以内遏制住泄露事件的单位而言，比超过 30 天的单位能够减少 100 万美元的成本。也就是说，“时间就是金钱”。



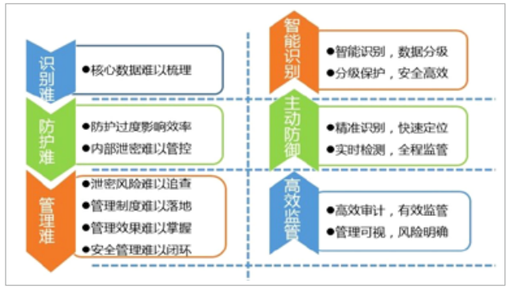

## 习大大带你“飞”

习近平总书记多次就网络安全和信息化工作发表重要讲话，对网络安全工作提出系列新思想、新论断和新要求，为网络与信息安全工作提供了根本遵循，网络与信息安全工作使命艰巨、责任重大。

随着国家“十三五”规划纲要、网络强国、《中国制

造 2025》、“互联网 +”的系列战略部署的推进实施，对网络安全保障提出了更高的要求，网络安全工作的范畴和深度都在不断拓展，迫切要求进一步提升安全保障水平和风险防控能力，更好支撑经济社会健康有序发展。三是近年来，信息通信技术和网络快速发展并加速向传统领域融合，导致安全威胁更加复杂隐蔽，伴生性安全威胁和传统安全威胁更加交织复杂，网络安全预警、应急处置和追踪溯源难度持续加大，互联网与工业等领域融合创新带来的安全问题日益严峻，网络安全管理理念和架构亟待创新完善。


**智能安全时代已经到来**




### 数据资产治理

1、认知关键数据资产：实现关键数据分类分级，制定关键数据管理要求、梳理关键数据责任矩阵，制定关键数据管理矩阵；

2、梳理关键数据资产：网络关键数据自查，重点业务对照自查，关键数据安全现状，不达标项跟踪整改；

3、管控关键数据资产：人员账号权限管控，集中访问控制，数据共享管控，机房设备安全管控；

4、监察关键数据资产：各专业自审计，安全专业审计，智能监察手段提升；

### 安全管理组织机构建设

应规范数据安全保护工作内容和方式，建立健全的数据安全保护工作长效机制，促进数据安全管理工作落地。

### 安全管理制度建设

通过管理手段进一步提升信息系统数据安全管理，具体安全管理制度应根据合规要求及企业业务进行调整和完善。

### 业务安全管理流程建设

根据调研及合规检查的结果，在现有工作流程上进行优化，并根据数据管理新要求，新增相关业务管控流程。

### 人员安全管理建设

对人员进行正确完善的管理，降低人为错误、盗窃、诈骗和误用设备的风险，从而减小了数据泄露的风险。

### 数据安全审计 & 分析

根据企业数据泄露防护建设成果，通过技术手段发现企业数据泄露风险，对日常的核心数据使用进行审计监测。精准定位泄露风险与隐患，帮助安全管理者明确数据安全防护重点，风险重灾区。

### 终端数据安全防护

实现对企业内部终端中数据的安全管控，采用文档加密、权限管控、分级管控、端口管控、外发管理、介质管控、磁盘加密等技术手段，实现终端数据产生、使用、传输等生命周期安全管控。





### 网络数据安全防护

实现对企业网络传输数据的安全管理，从泄密源头管控、防止数据泄露发生。同时监控核心数据流通过程，掌握数据流向，实现对数据的全程监管需求。

### 存储数据安全防护

DLP 提供的检测手段包括实时分析以及数据发现。实时分析针对当前被访问的文件或者内容，通过快速的检测得到结果。

### 数据安全可视化

解决安全管理员无法明确核心数据在公司的整体分布以及流向的问题，解决传统安全管理系统无法对核心数据进行风险评估的问题。整体可视化界面可以体现多层面的数据管理效果以及风险趋势分析效果。最终实现数据风险看得见、企业安全看得见的效果。

## 亿赛通不断前行

### 占领高地、布局市场快速前行

一个不断“创新”的专业企业，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，亿赛通坚持合作伙伴战略和超前的服务理念。

据了解，近几年亿赛通不断努力完成在行业市场的突破、地市业务的创新。截至目前，亿赛通已经在经成为了亿赛 通稳步前行的基石。当然，伴随着亿赛通全国招募的近百家渠道的合作开展，规范的渠道政策和渠道管理方式也在逐步成型，而吸引渠道合作伙伴的最大动力集中在三点“好产品、好价格、好服务”。另外，近年来，亿赛通也同很多云服务厂商合作，共同开拓新型数据安全战场。

### 开花必结果

在客户服务上，17 年来，亿赛通已经服务了包括党政军、研发通信、金融、能源、设计制造、运营商、各大企业集团等领域的客户，这些领域的众多企业一直同亿赛通保持着良好的合作关系。这与亿赛通专业而完善的服务体系相关。

今天，依靠坚实的合作伙伴渠道架构和客户服务体系，亿赛通获得了国家、媒体、客户授予的众多荣誉。

总之，这一路的荣誉、良性成长，客户拓展，融汇着亿赛通员工的汗水和付出，更指向着亿赛通的未来前进方向。中国数据安全问题任重而道远，继续打造“智时代，智安全”，将是亿赛通持续发展的方向。

# @ 所有人，远程办公应该这么做……


2020 年，由新型冠状病毒引发的肺炎疫情成为全民焦点，从防疫一线的各级医疗机构人员、到支撑社会正常运转的各行各业从业者，都在这场防疫战中贡献着自己的力量。

为减少人员聚集，企业大都采用远程办公的工作形式，各类在线化办公解决方案成为防疫战中的重要组成部分。但企业如何满足核心业务的远程正常运转，且让关系公司命脉的核心业务和数据在远程办公环境下，避免受攻击和被泄露，做到安全可控、行为合规，是远程办公中的难题：

## 远程办公安全风险

众所周知，企业的数据资产中包含大量的办公文档、核心技术资料、研发代码等。一些数据存储在办公终端，而很多重要的业务数据还存储在应用系统上，而这些系统数据也是黑客最喜欢窃取的重要资产，所以我们面临的主要风险主要分为内部风险和外部风险。





## 内部风险分析

### 1. 远程桌面或专网接入办公

员工通过远程桌面软件或 SVN 接入内网远程办公，由于员工使用不当或恶意行为，导致重要文件非法下载、使用、扩散，使企业面临经济或荣誉上的损失。

### 2. 公司电脑在家办公

员工携带公司办公电脑在家办公，如果终端上公司重要文件没有防护措施，员工电脑丢失、感染病毒等，或其他有意、无意行为，都可能导致重要文件外泄。

### 3. 使用第三方软件流转文件

员工使用第三方 IM 软件办公、沟通，传输工作重要文件，文档以明文进行传输，这些包含公司重要信息的数据可能被外泄，给企业带来经济损失。

### 4. 人员安全意识薄弱

员工在家多数会使用私人电脑做为主要办公电脑，但私人电脑多以娱乐为主，家庭成员的安全意识薄弱造成的电脑漏洞百出，甚至装满了不同类型的木马病毒，极易造成数据泄露。

## 外部风险分析

### 1. 数据库、应用系统权限过度

远程访问中权限过度，没有细粒度权限划分，以及远程办公、远程教学等业务所需的大规模数据采集和分享，都使得企业应用系统和数据安全的受攻面成几何级数放大。

### 2. 桌管端口防护范围有限

远程办公后企业数据运行的环境失去了桌管的端口管控、杀毒软件的病毒查杀。现有的 VPN 通道和安全认证方式防护范围有限，无法满足数据应对攻击和有意无意的泄密风险，造成了企业面临复工之后数据泄密风险并发症。

基于企业数据防护方面的需求，亿赛通提出了以事前主动防御、事中检测响应、事后追踪溯源、全程态势感知为设计理念的数据泄露防护解决方案。此方案充分考虑企业业务场景的复杂性，产品易用性，安全管理便捷性以及数据安全与生产效率共存。极大程度解决企业核心数据难识别、难防护、数据安全难管理的问题。

结合商密秘密保护标准，以 “依法规范、企业负责、预防为主、突出重点、便利工作、保障安全”为指导方针，整体遵循管理与技术并重原则、分级分域管理原则、数据生命周期管理原则和分步实施原则。

产品以自然语言处理技术作为内容识别核心引擎，虚拟文件驱动加密作为核心基础技术，可帮助企业对结构化和非结构化数据进行全生命周期的安全防护、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）、追踪溯源（文档操作、介质操作、用户操作、系统操作等）和态势感知（趋势分析、风险预警、溯源、风险人员画像）。

融合基于风险管理的数据安全咨询服务，从数据产生开始，覆盖数据使用、存储、传输、共享，实现全生命周期管理数据安全。同时，防护范围覆盖终端数据、存储数据、网络数据、业务系统数据、邮件数据。最终实现掌握数据分布、风险看的见、泄露防的住的整体效果，帮助企业建立立体化数据安全防护系统。

数据安全从来都不是一蹴而就，数据安全的建设是一项从无到有、富有挑战且意义深远的工作。亿赛通远程办公解决方案为客户提供专业的安全防护手段，保障远程办公过程中企业的核心数据安全。经过多位专家评审，此解决方案已成功入选 IDC 咨询机构《新冠疫情下，IT 安全提供商如何保障企业业务稳定运行》报告。

疫情已经逐渐过去，在有效的控制下，我国大量的信息安全专家在这场疫情中，也在为这隐藏在暗处的网络战争而战斗，逆境之中，我们一直在一起。

# 黑客攻击瞄准游戏业，核心数据如何防范？


近 10 年间，互联网的迅猛发展，带动了多种行业的崛起，游戏业是其中之一。热衷于游戏的你一定听过任天堂，该公司在其游戏火爆的同时，也让黑客盯上了它的核心数据。

游戏大火，黑客也伺机出动，任天堂数据被上传到论坛，泄露的资料是任天堂中古主机的信息，总数据量达到了 2 TB 。多款游戏主机被波及，源代码、开发文档，技术演示等内容，都被发布到论坛上。

## 如此核心的资料是来源于哪呢？

根据推论，资料可能来自任天堂的一家合作公司，该公司被聘请开发任天堂大部分硬件和软件。黑客攻击其服务器，从而获得了重要信息，包含 Wii 各个部分的框图和 Verilog 文件。后者用于描述电子电路和系统，具有适当专业知识的人员，可以从该数据中重新创建 Wii 的每个组件。





## 数据如何防泄密？亿赛通干货来袭！

亿赛通的数据安全管理平台可帮助用户对数据进行治理、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，实现安全与效率的双向平衡。

### 资产分析

通过部署安全探针，基于监督式学习或非监督式学习的方式，实现对终端数据资产进行快速分类、统计并生成数据资产地图，帮助用户即时掌握企业核心数据资产数量及分布情况并提供可视化数据分析展示平台，数据资产情况一目了然。

### 文档安全

对用户数据资产进行智能分级保护，将数据防护焦点聚集在重要数据资产上，对不同重要程度数据资产施行不同强度的防护手段，帮助用户精准防护企业数据资产。同时支持用户对外发数据进行权限控制，保护脱离企业内网环境的数据文档安全可控。

### 敏感信息泄露防护

智能识别数据资产中所含有的敏感信息，对通过 IM 工具、网络、邮件、网盘等可能造成泄密的外发或上传行为进行实时防护，防护措施包括审计、阻断、告警等，有效阻止数据资产外泄。

### 数据发现

对企业数据资产进行智能识别检测，可对 PC 终端、文件服务器、数据库进行智能检测，检测规则支持关键字、正则表达式、文档指纹、向量机等多种数据识别技术，帮助用户一键检查敏感数据违规存储，管理违规存储行为。

### 介质管理

对介质进行管理控制，防止因非法介质接入造成数据外泄的风险，同时也可对认证介质做加密保护，帮助用户避免因主动或被动行为造成的泄密风险。

### 磁盘加密

对 PC 端磁盘存储区加密保护的功能，从源头保障终端数据存储的安全性，帮助用户解决因终端丢失、失窃、维修等意外情况造成数据泄露的风险。

### 端口管控

对 PC 端口进行实时管控，严防企业核心数据外泄，端口管控范围包含蓝牙、光驱、串口 / 并口、USB 接口、WIFI 接口、调制解调器、红外设备等，帮助用户实时防护终端数据安全，降低数据安全风险。

### 态势感知

提供用户对企业数据安全态势进行实时感知，通过大数据智能分析海量数据日志，聚焦安全事件并可视化数据呈现，帮助用户掌握企业安全态势，为安全运营提供可靠的信息数据支撑。

# 这些事件“触目惊心”，数据安全行业风起云涌

## 1、美国地方警局 269GB 数据泄露

所谓的 BlueLeaks 是一个名为 Distributed Denial of Secrets（DDoSecrets）的黑客组织发布的 269 GB 的数据，包括了 200 多个警局 24 年的数据。泄露数据包含高度敏感的信息，例如 ACH 路由号码、国际银行帐号（IBAN）和其他财务数据，以及个人身份信息（PII）、嫌疑人图像（RFI）、其他执法和政府机构报告。调查结果表明，泄露文件可追溯到 24 年前的 1996 年 8 月，而此次泄露是因为德克萨斯州休斯顿的软件开发公司 Netsential 发生的数据泄露。


## 2、社交 APP 云泄露数十万用户 845GB 敏感数据

近日，9 家流行约会软件曝光了 845 GB 的照片和聊天等信息，泄露了数十万用户的隐私数据。此前某安全研究人员在扫描开放的互联网时，偶然发现一组公开可访问的亚马逊网络服务“桶”。每一个都包含了来自不同约会应用软件的数据信息，这些应用包括 3somes、Cougary、Gay Daddy Bear、 Xpal、BBW 约 会、casual alx、SugarD 和 GHunt 等。共找到 845 千兆字节和近 250 万份记录，可能代表了数十万用户的数据。

据悉，这些被泄露的信息特别敏感，其中包括照片和录音，同时研究人员还发现了来自其他平台的私人聊天截图和付款收据，这些数据都是用户在应用内发送的，是他们在应用内建立约会关系的一部分。专家表示，这是一次数据不正当保存而引起的信息泄露。研究人员无法确定是否有人在他们之前发现了这些暴露的隐私数据。

## 3、甲骨文引发今年最大的数据安全漏洞

科技巨头甲骨文（Oracle）花费了数十亿美元投资并购初创公司，以建立自己的用户网络浏览数据全景图，其中一家公司叫 BlueKai，在 2014 年用 4 亿多美元将其收购，鲜为人知的一面是，它已经成了美国最大的网络跟踪数据公司之一。

据外媒披露， BlueKai 服务器有一段时间内处于不安全状态且没有密码，网络跟踪数据不慎泄露到了开放的互联网上，从而使数十亿条记录可供任何人查找，在这些数据库中可找到用户的姓名、家庭住址、电子邮件地址和其它可识别的数据，数据还显示了敏感用户的 Web 浏览活动，从购买商品到新闻资讯的订阅等。

甲骨文发言人回应：“甲骨文已经意识到了这个安全漏洞与某些 BlueKai 记录可能会在互联网上公开。” “虽然研究人员提供的初始信息没有足够的信息来识别受影响的系统，但是 Oracle 的调查已经确定是因为旗下两家公司没有正确配置他们的服务网络导致的。Oracle 已经采取了其他措施来避免再次发生此类问题。”

不过甲骨文并没有说明这些额外补救措施是什么，这个公开数据库的庞大规模可能是今年最大的数据安全漏洞之一。根据欧洲的《通用数据保护条例》，甲骨文可能因违反数据保护和披露规则而面临占其全球年营业额高达 4% 的罚款。


## 4、Facebook 起诉开发人员窃取用户数据

据法庭文件显示，Facebook 正在起诉一名开发人员，该名开发人员参与了一场数据搜集活动并从中窃取了数千人的个人信息，该公司在诉讼中要求被告提供 7.5 万美元的赔偿。

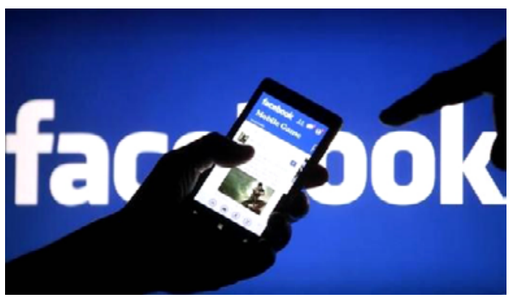
此行为被指违反了《计算机欺诈和滥用法案》。网站向客户提供了从 Facebook 好友处获取数据的能力，其中包括电话号码、性别、出生日期和电子邮件地址等。所有这些数据都是由 Facebook 用户公开发布的，但据称 Zaghar 网站提供的自动化将使人们能够以更快的速度、更大规模地获取这些信息。数据搜集活动从 4 月 23 日持续到 5 月 6 日，约有 5500 人注册了这项服务。

在得数据者得天下的今天，数据对企业单位业务深度和广度的扩展具有重要的意义，数据安全是企业单位生存和发展的根基，当今数字社会需要的是以“体系”为中心的数据安全治理时代。上述事件用自身的经验告诉所有企业，与其把数据放在他人手里，不如攥在自己手中。

## 扬技术专长，给数据穿上防护衣

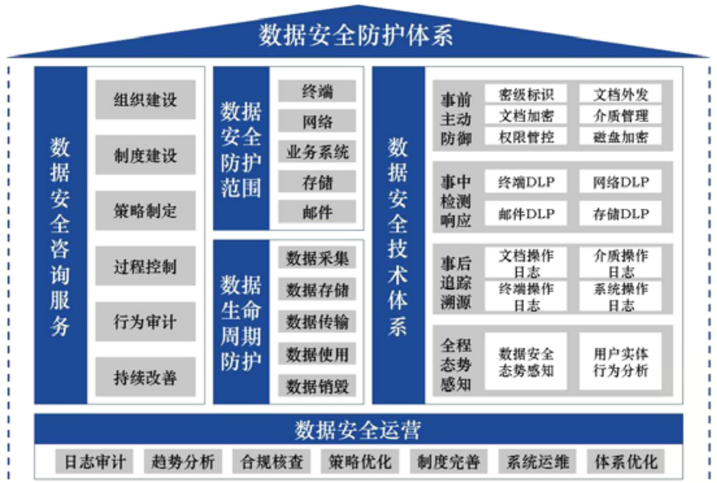
体系化的安全要求不再是纯产品技术层面上的安全，而是要求组织规范 + 技术的完美整合，以呈现整体的安全。亿赛通全系列综合防护解决方案，系统定制化功能强大，可适应广泛较复杂的应用场景，产品实施对现有系统改造程度小，易于部署，且能极大限度保护系统数据文档，另外在组织制度的规范化方面，可对文档权限灵活控制，并有全面的日志跟踪记录，便于事后追查，配合数据安全防护制度，提高员工的数据安全保护意识。

曾经，企业的数据安全意识淡薄，认为安全是成本，企业无暇兼顾数据的安全问题，但数字社会的时代背景下，数据安全问题已经成为一个致命伤。善用数据，保护数据将会是未来全世界需要长期重点研究的课题。亿赛通将继续其企业使命，为客户提供有竞争力的数据资产安全解决方案和服务，持续为客户创造价值。



# 如何远离数据泄露的危险漩涡？

产品管理与解决方案部：张兴堂 / 文




随着各类信息的“数据化”，如何保护个人“数据”等信息的安全，变得日益迫切；如何满足群众在生产生活中对数据使用的合理需求，也变得更为迫切。正在审议中的《数据安全法（草案）》，或许能够满足人们对数据安全和使用顺畅的双重需求。

《数据安全法（草案）》，在本月举行的十三届全国人大常委会第二十次会议迎来初次审议。《数据安全法（草案）》的内容主要包括：

确立数据分级分类管理以及风险评估、监测预警和应急处置等数据安全管理各项基本制度；

明确开展数据活动的组织、个人的数据安全保护义务，落实数据安全保护责任；

坚持安全与发展并重，规定支持促进数据安全与发展的措施；

建立保障政务数据安全和推动政务数据开放的制度措施。

保护公民和企业的数据安全，需要掌握个人信息的单位、部门的权责和业务，对依法获取个人信息数据的单位、部门，则有职责和义务保障数据不被非法泄漏。依法打击掌握个人数据信息的“内鬼”和其下游产业链，需要从法律层面、制度层面进行框架设计，是堵塞源头、防范违法的重要步骤。

目前信息的“数据化”引发了一系列的安全风险：传播途径广、传播速度快、拷贝 / 复制操作无痕迹及易携带等特性，普通的网络边界防护措施已无法有效控制有内部人员参与的泄密事件的发生。一旦发生机密数据或者信息资产泄密，带来的损失和法律责任，将无可计量。如何保证企业中的核心数据资产安全是关系到企业生存发展乃至国家安全的重要问题，亿赛通自主研发的全套数据泄露防护方案可以解决您的燃眉之急。

一个成熟的数据安全体系应当做到技术、管理相结合。同时结合企业当前数据安全管理现状，需要解决分散控制、过度防护等带来的防护效果和业务影响问题。实现企业复杂业务场景下的全面数据安全防护，形成数据安全的事前、事中、事后、全程把控的技术体系，将技术体系作为工具辅助安全管理。

数据安全体系解决数据利益攸关者之间的责、权、利问题，明确数据安全治理的目标以及安全策略，通过安全管理流程实现数据治理的目标，落实各项安全策略，保障数据不被窃取、破坏和滥用。构建包括系统层面、数据层面和服务层面的数据安全框架，从技术保障、管理保障、过程保障和运行保障多维度保障数据安全。

从系统层面来看，保障数据安全需要构建立体纵深的安全防护体系，通过系统性、全局性地采取安全防护措施，保障数据系统正确、安全可靠的运行，防止数据被泄密、篡改或滥用。

从数据层面来看，数据应用涉及到采集、传输、存储、处理、交换、销毁等各个环节，每个环节都面临不同的安全威胁，需要采取不同的安全防护措施，确保数据在各个环节的保密性、完整性、可用性，并且要采取分级分类、加密、脱敏等方法保护用户个人信息安全。

从服务层面来看，加强数据的安全运营管理、风险管理，做好数据资产保护，确保数据服务安全可靠运行，从而充分挖掘数据价值，提高生产效率，同时又防范针对数据应用的各种安全隐患。

亿赛通基于数据安全防护体系的解决方案，实现安全管理与技术手段相结合的目的，通过主动防御、检测响应、追踪溯源、全程态势感知的整体防护理念，帮助企业建立完善的整体数据安全管理体系。

建设先进、自主、灵活、全面、智能的立体化数据安全防护体系；

建设满足合规要求的数据保护管理体系；

提供完整的数据资产生命周期风险主动控制和自动化管理；

提供可有效降低泄密风险，提升防护能力，提升监管能力的技术体系；

提供可有效提升企业数据安全审计、管理、风险分析的可视化管理平台；

提供高效、全面、完整、规范的数据安全运营服务。

# 信息化办公企业的“高度风险”——数据泄露

售前技术部：梁伟 / 文

数据安全近年来是任何国家、政府、部门、行业都必须重视的问题，是不容忽视的国家安全战略。2009 年央视 315 晚会曝光的个人信息泄露产业链，数据安全再一次进入公众的视线。进入网络时代后，数据安全保障工作的难度大大提高。面对日益严重的网络安全威胁：网络的数据窃贼、黑客的侵袭、病毒发布者，甚至系统内部的泄密者。数据安全已经成为各行业信息化建设中的首要问题。

围绕数据安全的需求，我司总结大多数企业数据安全建设难题如下：

1. 海量数据识别难：缺乏对数据内容的分类和敏感级别分级；保护措施无法和数据重要级别挂钩，保护效能和效率较低；

2. 敏感数据定位难：敏感数据存放位置无从知晓，保护难以下手；数据存放在电脑、笔记本、存储等地无法定位；缺乏对不同数据的交互场景进行风险评估视图；

3. 重要数据防护难：现有的安全防护措施，大多基于病毒防护、桌面管理、边界安全等，无法对数据本身进行有效保护，实现网络、应用系统、终端多个维度统一数据安全管控；

4. 数据外发追溯难：现有系统难以对数据的全生命周期实现日志、事件等详细记录，对泄密途径、行为等方式无法进行追溯；

企业信息化建设的核心目标是提高业务效率，数据的高效传输、分享和交换是实现这个目标的重要途径。而绝大多数传统的数据防泄露手段，是阻碍数据的高效传输、分享和交换的。亿赛通通过多年的数据安全防护经验，提出了企业数据安全的最佳实践方法“知”“识”“控”“察”。



结合商密秘密保护标准，以“依法规范、企业负责、预防为主、突出重点、便利工作、保障安全”为指导方针，整体遵循管理与技术并重原则、分级分域管理原则、数据生命周期管理原则和分步实施原则。

产品以自然语言处理技术作为内容识别核心引擎，虚拟文件驱动加密作为核心基础技术，可帮助企业进行数据治理、安全管控、追踪溯源和态势感知。融合数据安全咨询服务，从数据产生开始，覆盖使用、存储、传输、共享，实现全生命周期管理数据安全。

典型案例 TYPICAL CASES

# 江苏豪森药业集团有限公司


## 客户介绍

豪森药业成立于 1995 年，是在中国排名前列的研发驱动型制药公司。二十余年来，始终秉承“做优民族医药，做强中国创造”的企业使命，致力于在中国市场临床需求缺口巨大的中枢神经系统、抗肿瘤、抗感染、糖尿病、消化道和心血管等六大领域的创新发展。欧兰宁、普来乐等八种主要产品在多方治疗领域占据市场领先地位。公司建有两个研发中心，分别位于连云港和上海，拥有研发人员 1200 多名，拥有多个国家级研发称号，包括国家级技术中心、博士后科研工作站及国家重点实验室。

## 需求背景

随着豪森药业的大步伐扩张，积累了太多重要的关于核心知识产权的文档，如像企业的客户信息、药品研发数据、生产数据和运营信息等等，组织不希望这些价值资料离开内部网络环境，甚至不允许在网络外部传递与交流。但现代组织不能拒绝互联网的交互，不能将机构封闭在一个信息孤岛。而员工在上传下载和发行网络中文件的同时，可能会有意或无意将组织的许多重要信息流通到网络外部，从而使重要的知识产权受到安全威胁。

## 解决方案

1. 文档安全管理系统：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等，防止文档信息泄密。

2. 文档加密安全网关：可使从豪森药业应用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。不可解密文件只能由指定专人进行解密。

## 项目成果

通过以上防范手段，不仅为豪森药业各业务部门部署合理的数据安全防护体系，同时使得该集团相关业务流程更为合理化、流程化、规范化。在数据传输上既保证了内部业务网络较高的可用性、可靠性、保密性，又对内部核心数据有较强的防御和管控能力。

# 长春金赛药业股份有限公司


## 客户简介

金赛药业是中国基因工程药物质量管理示范中心，国家基因工程新药孵化基地，国家科学技术进步二等奖获得者，拥有亚洲重组人生长激素生产基地。金赛药业是长春高新控股子公司，行政总部和生产总部设于长春。



典型案例 TYPICAL CASES

## 需求背景

近年来越来越多的数据泄露事件，给企业造成不少的压力。金赛药业为避免药品研发中心、财务部、客户服务等重要部门的核心文档、资质文件和支持产权，因内部人员有意或无意泄密，或外部人员攻击，而给企业造成重大经济损失，在经过严苛选型测试后，最终签约亿赛通公司数据安全管理体系。

## 解决方案

组织内部分部门控制。如对研发、设计部门采用强制加密，对管理、财务和营销等部门采用主动加密，实现重要文档高效、安全管理。

防止内部员工通过邮件、MSN、QQ、FTP 下载等网络端口发送重要文档，防止复制、拖拽、拷屏、打印、另存为、剪贴板盗取和内存窃取等手段盗取文档内容；

文档操作强制日志审计，确保事后可追溯；

防止硬盘被盗、笔记本和移动存储设备丢失后导致的信息泄露；

邮件发送可信对象时自动解密，提高工作效率；

员工出差或离开时，配置脱机策略设定时间并可补时，确保离线终端安全可控等。

## 项目成果

亿赛通加密产品，为其研发、财务等核心部门的格式文档强制加密，并且实现内部自由使用，通过灵活的权限设置使不同员工拥有对应的操作权限，既加强了内部文档的安全管控又保证了企业员工的灵活使用。