



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



亿赛通深耕数安十余载
——从文档防护到数据安全智能防护



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 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com



本刊为亿赛通企业月刊，欢迎交流，禁止转载

CONTENTS 目录

刊首语 PREFACE

2/3 《亿赛通十一月刊》独家专享“数据安全防护秘籍”

行业聚焦 INDUSTRY FOCUS

4-7 国内行业新闻

8-13 国外行业新闻

亿赛通动态 ESAFENET NEWS

- 14-16 亿赛通深耕数安十余载——从文档防护到数据安全智能防护
- 17-19 【培训服务】某大型集团公司数据安全专题培训课程圆满结束
- 20/21 亿赛通核心产品精彩亮相“天府杯”2019 天府国际网络安全高峰论坛

亿赛通小贴士 ESAFENET PROMPT

- 22/23 国内人脸识别第一案，我的信息泄露谁负责？
- 24/25 云安全 | 12 亿网民信息泄露，究竟谁的“锅”？

典型案例 TYPICAL CASES

- 26/27 民生银行
- 28/29 长城证券有限责任公司

《亿赛通十一月刊》独家专享 “数据安全防护秘籍”

随着互联网越来越多的渗透生活，我们的衣、食、住、行，每一样都离不开互联网，我们的数据都被记载于互联网，记载于每一个APP、每一项移动消费中。一个手机号，一个指纹，一个身份证，N个银行卡密码，互联网支付，家庭住址……这些或物理或生物的身份识别，在互联网时代，在安全与非安全之间，其实只隔了一道“磨砂玻璃墙”——或者看不清，或者一击即破。

近年来，我国数据泄露的频率逐年升高，5年内，网民由于个人数据泄露，而上当受骗，直接或间接造成的经济损失多达805亿元，人均损失近124元；其中，有近4500万网民遭受的经济损失超过1000元。综上所述，数据安全远非像给家门换把锁那么简单的事儿。亿赛通十六年来专注从源头保护用户数据安全，《十一月刊》将独家揭晓专家的“数据安全防护秘籍”。



国内

1、百度 10 月信息安全治理：百家号 Q3 下线低质违规文章超 56 万篇



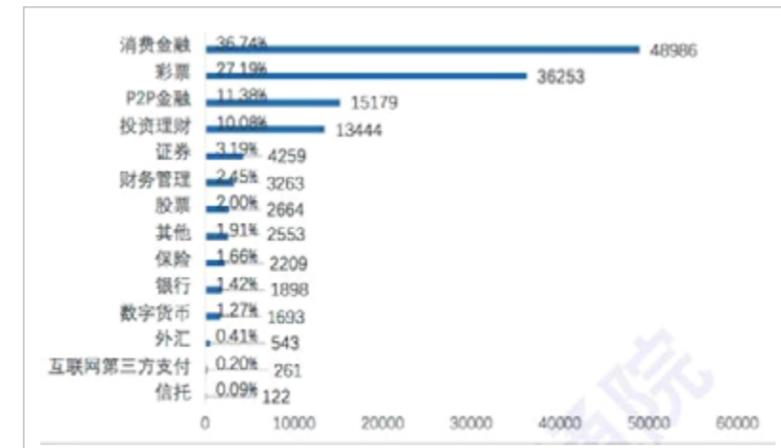
摘要：11月20日，百度发布10月信息安全综合治理月报，向网民周知百度在处理网络虚假有害信息、保护网民权益方面的相关行动和信息。报告显示，10月，百度内容安全中心利用AI人工智能技术挖掘打击色情、赌博等相关有害信息共38亿余条；人工巡查色情、赌博等相关有害信息共544万余条。在网络营销方面，百度10月打击医疗变体词（不法分子为躲避监管，对相关搜索词进行字体替换/顺序改变等）6000万个，拒绝不合规广告4.03亿条。

2、黄牛扫货帅不过三秒，国内首个非法在线抢购平台被端



摘要：平台“Statty sky”已被定性为“国内首个非法在线抢购平台”。尴尬的是，购买“黄牛”服务的用户试图在淘宝天猫平台扫货时，并未体验到所谓的一键“云抢购”。“黄牛”订单刚刚进入系统就被阿里安全的风控团队抓住，专家们把线索交给了警方，最终3名犯罪嫌疑人被抓获归案。

3、信通院评测了 13 万个金融类 App，70% 存高危漏洞



摘要：截止2019年9月11日，中国信通院的报告团队从232个安卓应用市场中收录了133327款金融行业App。从观测对象的地域分布来看，有130022款可以明确归属省份，全国34个省级行政区均有金融行业App生成，平均每个省份生成金融行业App3824款。金融行业App地域分布不均，广东、湖北和北京分别以29.60%、21.30%和12.96%的高占比排名金融行业App生成数量前三，而西藏、青海等6省份总占比仅有0.18%。

4、上亿条个人信息可能被泄露 漏洞在哪？如何保护？

序号	单位名称	漏洞	高危	漏洞详情	漏洞利用	漏洞修复	漏洞来源	漏洞类型	漏洞危害	漏洞等级	漏洞编号
1	广东省公安厅	漏洞	高危	2019/11/15	2019/11/15	2019/11/15	广东省公安厅	远程代码执行	可导致任意代码执行	高危	2019-11-15-001
2	广东省公安厅	漏洞	高危	2019/11/15	2019/11/15	2019/11/15	广东省公安厅	远程代码执行	可导致任意代码执行	高危	2019-11-15-002
3	广东省公安厅	漏洞	高危	2019/11/15	2019/11/15	2019/11/15	广东省公安厅	远程代码执行	可导致任意代码执行	高危	2019-11-15-003
4	广东省公安厅	漏洞	高危	2019/11/15	2019/11/15	2019/11/15	广东省公安厅	远程代码执行	可导致任意代码执行	高危	2019-11-15-004
5	广东省公安厅	漏洞	高危	2019/11/15	2019/11/15	2019/11/15	广东省公安厅	远程代码执行	可导致任意代码执行	高危	2019-11-15-005

摘要：最近，江苏淮安警方通报，在公安部督办下，他们以“打链条、打平台、打团伙”为目标，依法打击了7家涉嫌侵犯公民个人信息犯罪的公司，涉嫌非法缓存公民个人信息1亿余条。

5、装修公司频繁电话“骚扰”，原来是#小区业主信息被售楼部倒卖#!你中过招吗?



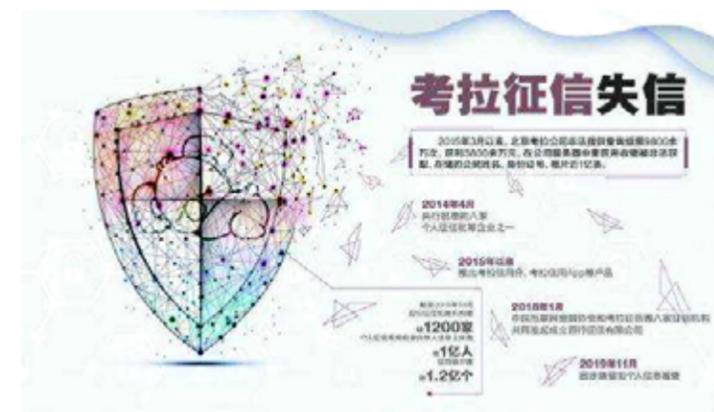
摘要：今年，银川同一个小区多名新购房业主举报，称每天频繁接到装修公司的推销电话，对方还对自己的个人信息了如指掌。民警最终锁定犯罪嫌疑人李某。李某利用职务之便，在售楼部微信群里收藏了一份790人的业主个人信息。随后到装修公司工作时，他将这些信息提供给了同事，经过几次转手，就被涉案装修公司市场部总监李某军买到。民警调查取证发现，涉案的装修公司掌握了大量业主个人信息。此外，装修公司之间还会进行信息互换，导致多家装修公司不停地给这些业主打电话。目前，涉案的五名犯罪嫌疑人已批捕三人，取保候审两人。目前，该案已移交检察机关进行起诉，将继续追究刑事责任。

6、上58同城看房信息泄露



摘要：有杭州市民反映，在58同城上看二手房信息，一周内有50多个陌生号码打来电话，都自称房产中介，说从别处买到了他的联系方式。58同城方面称APP端注册用户是“受隐私保护”的，测试后，确有中介能根据真实手机号回拨电话。录音中，有中介说是从安居客买来的号码，根据数据显示，安居客正是由北京五八信息技术有限公司百分百持股的。

7、泄露个人资料当严惩 勿纵容“考拉征信”们



摘要：考拉征信服务有限公司自2015年3月以来，非法提供查询返照9800余万次，获利3800余万元，在公司服务器中查获并收缴被非法获取、存储的个人信息近1亿条。

8、成都多小区使用人脸识别门禁 业主：我的隐私安全谁负责?



摘要：成都多个小区使用了人脸识别门禁装置。“要实名制，录人像的时候身份证要放在上面。”成都海椒市某小区物管称，是否采集人脸信息全凭业主自愿，主要是为了“方便”。安装后，可以不用带门禁卡，刷脸进门。但也有业主拒绝，张女士说，担心隐私被泄露。

国外

1、男子在使用 App 远程入侵并追踪女友的汽车位置后被指控

摘要：近日，澳大利亚当局指控一名男子在涉嫌侵入前女友的汽车后对其前女友进行刑事跟踪，目的是为了追踪她的下落。他可以在女友不知情的情况下玩弄她的车辆，比如无钥匙进入以及控制点火系统。据推测，该男子建立了一个在线计算机应用程序，允许他利用该陆虎的各种安全漏洞对车辆进行控制。

2、皮尤：大部分美国人认为不收集个人数据是不可能的事情



摘要：据外媒报道，皮尤研究中心的一项新研究显示，对于许多美国人来说，数据收集现在可能已经被视为是其日常生活的一部分。据统计，超 60% 的美国成年人表示他们认为政府或公司不收集他们的数据是不可能的。报告显示，81% 的成年认为广泛收集数据的风险大于益处。不过大多数美国人表示，他们担心自己的数据可能会被公司和政府使用。而超 80% 的受访者表示，他们觉得对自己的数据缺乏控制。超一半的人则表示，他们对数据收集和使用知之甚少。

3、一伦敦男子被指控访问国家彩票用户的帐户



摘要：近日，知情人士透露，一名男子将在 12 月出现在皇家法院，以回答有关他使用黑客程序 Sentry MBA 来访问英国国家彩票在线赌博帐户并从中获利的指控。检察官声称，29 岁的 Anwar Batson 在上一年下载了黑客工具后，于 2016 年 11 月获得了访问国家彩票用户帐户的权限。据说他欺诈性地密谋从这些国家彩票帐户中取钱。

4、高通安全世界移动保险库中的“漏洞”泄露了敏感数据



摘要：近日，Check Point 网络安全研究人员发现，现已修补的高通安全世界虚拟处理器中存在严重的“漏洞”，Secure World 安全隔间可能会被用来泄露财务信息。Secure World 是基于 Qualcomm 的硬件支持的受信任的执行环境（TEE）的一部分，该环境基于 ARM TrustZone，涉及 ARM 体系结构的安全扩展，包括安全的虚拟处理器。

5、ZoneAlarm 论坛遭遇黑客攻击， 暴露成千上万用户数据

```

64 <title>
65
66 Forums -
67
68 ZoneAlarm Community Forums - Your ZoneAlarm Information Source
69 </title>
70
71 <meta name="description" content="vBulletin Forums" />
72 <meta name="generator" content="vBulletin 5.4.4" />
73
74
75
76 <!--[if IE]>
77 <link rel="stylesheet" type="text/css" href="css.php?styleid=6&td=1tr;
78 <link rel="stylesheet" type="text/css" href="css.php?styleid=6&td=1tr;
  
```

摘要：Check Point Technologies 拥有的流行安全软件公司 Zonalar 遭遇了数据泄露，安全漏洞暴露了 ZonAlarm 论坛用户的数据。ZoneAlarm 套件包括面向用户和小型组织的防病毒软件和防火墙解决方案，下载量接近 1 亿。虽然 ZoneAlarm 或者其母公司 Check Point 都还没有公开这次的事件，但该公司本周末悄悄地通过电子邮件警告了所有用户。尚不清楚攻击者何时破坏了 ZoneAlarm 论坛。消息表明，攻击者获得了对论坛成员数据的未经授权的访问，包括姓名，电子邮件地址，哈希密码和生日。好消息是，受影响的用户数量不大，此事件仅影响了“forums.zonealarm.com”域，该域名下大约有 4,500 个订阅者。

6、没人会黑自己？《赛马邮报》数据泄露历史披露



摘要：现任《赛马邮报》(Racing Post) 首席信息安全官的 Johan Pieterse 在任职当时被告知“没人会想黑《赛马邮报》”。2013 年 1 月，Johan Pieterse 入职著名赛马、赛狗和体育博彩消息出版商《赛马邮报》，担任运营总监。入职后不久，Pieterse 向他的直属经理打听公司上一次渗透测试是什么时候做的，被告知“别担心，因为没人会想黑《赛马邮报》的啦”。10 个月后，该公司遭遇了数据泄露。

7、俄罗斯男子因使用 Neverquest 木马偷钱 而被判 4 年



摘要：近日，一名俄罗斯男子 Stanislav Vitaliyevich Lisov 因使用名为 Neverquest 的特洛伊木马从银行账户窃取钱款而在美国纽约南区被判处 4 年徒刑，并被勒令没收 5 万美元且要支付近一百万美元的赔偿。

8、西门子 PLC 隐藏功能可被用于攻击



摘要：西门子公司的一些新型可编程逻辑控制器 (PLC) 存在隐藏功能，使设备面临攻击风险。修复已提上日程。研究人员发现，某些新型西门子可编程逻辑控制器 (PLC) 的一个非正式访问功能可被攻击者当做攻击武器，也可成为防御者的取证工具。

9、西班牙两家公司同天遭勒索软件攻击，引发 WannaCry 级恐慌

摘要：近日，西班牙两家大型公司在同一天内受到勒索软件打击。其中一家是 Everis，这是 NTT Data Group 旗下的 IT 咨询公司，其发言人目前还没有发表正式声明。第二个是西班牙最大的无线网络公司 Cadena SER，其在官网发表了声明，确认公司遭遇了攻击。两家公司都要求员工关闭计算机，并断开网络连接。



10、一年 1.6 千万：财富 500 强公司用户密码泛滥暗网

摘要：网络安全公司 ImmuniWeb 宣称，暗网现存出自财富 500 强公司的 2,100 万 (21,040,296) 被盗用户凭证，其中超过 1,600 万 (16,055,871) 是过去一年中被盗的。个中关键是什么呢？这些凭证中 95% 都包含未加密或已被攻击者暴力破解的明文密码。

Industry	Top 5 Passwords
Technology	password 1qaz!@WSX career01 abc123 password1
Finance	456433 student 00123456 welcome 123456
Health Care	Exigent password pass1 000000 123456
Industrials	12345678 1qaz!@WSX passer comely password
Energy	password 123456 1qaz!@WSX 00123456 789_234
Telecommunications	123456 welcome password 6636455 password1
Retail	1234 1qaz!@WSX 123456789 abc123 password

11、美国某可再生能源发电厂遭到网络攻击



摘要：近日，美国犹他州发生了一起针对可再生能源发电厂的攻击事件。在此次攻击中，黑客成功切断了电厂运营商和发电站之间的连接，这在美国尚属首次。据了解，该事件的受害者是 sPower，其主营业务是通过风能和太阳能进行发电。事件发生后，sPower 的主控制中心与其远程发电站点之间的连接逐渐断开。美国能源部分析师 Matt Tarduogno 表示，攻击者可能利用了思科防火墙中的已知漏洞，以迫使防火墙重启，从而成功切断了二者的联系。然而，此次攻击似乎并非是提前计划好的。有资料显示，在成功瘫痪防火墙后，黑客并没有继续破坏 sPower 的网络。研究人员称，尽管该公司的发电能力并未受到干扰，但此类事件依然为安全人员敲响了警钟。

12、T-Mobile 发生数据泄露，影响用户超过 100 万



摘要：据 TechCrunch 消息，T-Mobile 近日出现用户个人数据泄露事件，波及影响用户超过 100 万。该公司向受影响的客户发出了警报，但没有在官方帐户中告知黑客攻击的太多细节。目前其安全团队已经关闭了对预付费数据客户的“恶意、未经授权的访问”。被泄露的数据包括：姓名、账单地址、账号，通话数据等，不包括财务或密码数据。通话数据被视为“客户专有网络信息”，根据电信条例，如果数据泄露，必须通知客户。T-Mobile 称，这起攻击是在 11 月初发现的，并立即关闭了攻击通道。

亿赛通深耕数安十余载

——从文档防护到数据安全智能防护



亿赛通 CTO 朱贺军

近年来，数据泄露事件频发，给个人、企业以及国家造成了巨大经济损失。信息泄露不仅困扰人们生活，甚至威胁生命和财产安全，使人闻之色变。因此，数据安全已经上升到必须解决的社会问题，在这样的背景下，企业对于安全的重视程度也逐渐加深，数据安全市场发展潜力也就越来越大，对于市面上参差不齐的安全技术和产品，用户很难抉择出可靠、成熟的安全解决方案，而亿赛通深耕细作数据安全领域十余年，在数据安全防护层面已取得不菲成绩，使之成为安全领域典型的代表厂商之一。

四年连冠 稳坐数据安全江湖宝座

亿赛通在成立之初，其业务重心是文档加密，经过不断开疆拓土，目前在数据安全防护领域已经取得了不俗成绩。据悉，前不久赛迪 CCID 发布的最新《中国数据泄露防护产品市场研究报告（2019）》显示，亿赛通数据泄露防护产品市场占有率稳居第一，而这把“宝座”已经连续稳坐四年之久。

数据安全体系建设 全面化、智能化 个性化

亿赛通为何能在数据安全防护市场取得如此成绩，对此亿赛通 CTO 朱贺军向我们做了简单介绍：

朱贺军介绍，亿赛通的口号是“中国数据安全防护专家”，作为在数据安全领域深耕细作十几年的厂商，目前已拥有上万余家客户及 400 百多万个终端用户。这样的业绩和地位，靠的不仅是产品的不断升级和推陈出新，更多的是给客户带来了真正的实用价值，其核心优势主要体现在以下几个层面：

首先，亿赛通经过十几年技术的沉淀和积累，研发的文档加密、数据泄露防护、磁盘加密等众多产品，在终端上适配近千种应用，并提供完善的全行业数据安全解决方案，这也是亿赛通数据安全产品的基石。

其次，亿赛通拥有强大的协议分析和处理能力，如支持万兆大流量数据处理、支持丰富的网络应用解析（包括图片内容及语音的识别）、支持旁路与串接及云环境等部署模式、支持 IPv4 和 IPv6、支持 https 内容还原及阻断等，保障了亿赛通在数据库安全领域的核心技术优势，从而快速适应新兴技术的变化潮流。

最后，亿赛通除了深厚的技术积累外，最重要的核心亮点是拥有一套完整的数据安全防护体系建设思路，除了考虑系统的安全性、稳定性、易操作性等基本条件外，还深入聚焦防护产品的全面化、智能化和个性化。

1) 全面化: 从文档加密启程, 不断丰富产品防护范围。目前在 Windows 终端、Linux 终端、MAC 终端、手机终端、

网络、邮件、数据库、存储、业务系统、云端等众多领域实现安全防护功能，并且将这些防护能力统一融入到安全智能管理平台（DSIP），并与众多终端及探针有机结合，为用户带去一体化的全面防护能力。近期，亿赛通又针对客户的数据防泄密需求推出新产品——TIS，该产品属于 UEBA（User and Entity Behavior Analytics）范畴，主要帮助用户解决潜藏在内部更深的数据安全问题，例如商业间谍、安全事件监控与调查，属于高涉密场景下安全机制补充方案，也是对 DSIP 的重要补充。

2) 智能化: 不断改进系统架构及关键领域技术，基于大数据及机器学习能力，融入智能分类分级、行为分析、态势感知、图片及音频识别等技术，极大地增强了产品能力，给用户带去全新的智能防护感受。

3) 个性化: 亿赛通也在尝试推出如面向个人用户的‘数据安全卫士’产品，给用户带来一种新的数据安全防护体验。此外，在结构化数据、大数据、云应用等领域的安全重点发力，新推出数据库审计、数据库防火墙等产品，形成了多源异构化综合安全产品体系。

未来，亿赛通将根据国家法律法规和行业发展战略，利用大数据、人工智能等新技术来规划产品方向，始终坚持以“服务客户、持续创新、勇担责任、专业至上”的核心价值观，为用户提供一流的综合数据安全解决方案。

专家视角话数据泄露防护 DLP 发展趋势

朱贺军作为国内数据安全领域的资深专家，他认为近年来在安全事件和政策的驱动下，国内数据泄露防护 DLP 在技术上取得了长足进步，但同国外相比依旧存在一定差距。

他提到，由于各个厂商原有技术及行业背景不同，导致技术发展选择上的差异。例如一些原来做防火墙产品出身的 DLP 厂商，可能会从网络层面实现 DLP 功能，并结合自己原有的防火墙、网关等产品实现个性功能。还有些厂商主要针对某一类应用做 DLP 防护，如国外的 Mimecast 就主要针对邮件进行防护。国外 Symantec、McAfee 一些传统 DLP

厂商，可以对终端、网络、邮件、数据库、存储等进行安全防护，技术路线各有千秋。根据对市场的观察和对行业的理解，朱贺军认为未来两年 DLP 领域会出现一些新的趋势：

首先，云安全的重要性将越来越大，很多厂商在设计产品技术路线时，都越来越多考虑云化、零信任。例如云访问安全代理 (CASB) 可以算得上是这两年云安全的热点，Zscaler、Skyhigh 等多家企业都已上市或被并购。

此外，随着人工智能技术的发展，人工智能必将在安全领域发挥越来越大的作用，众多厂商都在寻求将人工智能整合到原有的产品中。例如 Symantec 推出了融入人工智能的安全解决方案，其终端防护产品采用了人工智能和端点行为分析技术以监控端点事件并识别可疑行为，集成了威胁情报、机器学习、恶用阻断、行为分析等技术。

而亿赛通本土化 DLP 在技术发展上，即结合了公司在文档安全领域多年的实施经验，在终端行为分析上采用递归神经网络、场景文本检测等机器学习算法，形成自己独特的智能安全解决方案，不仅可以对非结构化数据进行防护，而且对结构化数据、大数据、云环境等进行安全防护。这些方面，虽然国外厂商比国内厂商投入更早，但国内厂商凭借本土化、行业经验积累等优势，应该说也逐步展现出了自己的特色。

数据安全产品选型布局几点思考

通过在数据安全领域大量技术积累和解决方案得以看出，亿赛通的业务重心不仅局限于最初的文档加密，其在数据安全防护领域亦有着极为成熟的布局，绝非是空谈概念。最后，为了让更多的用户“少走弯路”，亿赛通 CTO 朱贺军认为国内用户在进行数据安全产品选型时应该注意以下几点问题：

数据安全产品对于企业来说是一套综合解决方案，从企业自身需求特性出发，部署整体实施方案，即适合自己尤为重要。

数据安全产品除了可审计和溯源外，对攻击行为的及时发现告警和实时阻断的功能也必不可少，能在发生危害前阻止、减少甚至消除客户损失至关重要。

数据安全产品除了常规的通过事先设置规则判断攻击外，应具备智能机器学习的能力，对非法恶意行为应能自动识别和判断。

【培训服务】某大型集团公司数据安全专题培训课程圆满结束



随着当前信息安全问题的突出，信息安全已经成为影响国家安全、经济发展、社会稳定、企业利益的重要原因。某大型企业为积极响应国家号召，深入贯彻网络强国思想，欲针对技术骨干开展数据安全培训课程，提升其信息安全意识，加大对信息安全人才培养范围和信息安全技能的普及。亿赛通经过该企业的严格选型，作为讲师对企业全国技术人员进行授课，并与企业在数据安全培训方面建立了全面、深度的战略合作关系。

加强技术水平，构筑“安全”优势

根据企业特点，本次数据安全培训在形式上，采用了理论课程+实战演练的模式；在内容上，涵盖了数据安全课程概述、数据安全监管法律法规讲解、数据安全个人信息监管解读、数据安全防护体系介绍、数据泄露防护主流产品技术、数据梳理及分级分类介绍、运营商数据安全审计体系介绍、数据安全能力成熟度模型解析、数据安全治理体系与典型应用、数据库安全威胁、安全产品演进及技术发展趋势、数据库安全防护主要技术介绍、量子加密的原理和应用、个人隐私安全防护讲解、数据安全案例分享及设备实操等课程，充分调动学员积极性，协同配合，实事求是的带领企业全国技术骨干进行了丰富的理论教学以及手把手的实验教学，取得了良好的效果。

亿赛通渠道、技术平台等部门的优秀讲师授课过程中，直击运营商行业数据安全技术痛点，站在运营商角度根据不同课题通过管理和技术手段来讲解，让学员不仅能了解到实践中常见问题更能学到管控方法和工具，学员们对这种学习模式表示认可，认为不仅巩固了自己的所学，还能在交流分享中发现新的问题并解决。



提高技术能力，沉稳应对安全问题

数据安全培训是亿赛通极为重视的一部分，亿赛通专家团队根据多年的专业知识积累，打造“意识提升—技能增强—体系运营”三位一体的数据安全培训体系，针对数据保护开发配套课程，用户可以根据自己企业需增强能力进行针对性学习。

- 对数据安全法律法规的解读和讲解，帮助企业领导和管理者了解数据安全的红线，数据安全保护的重要性和监管要求

- 介绍数据安全体系建设和数据安全保护技术，帮助企业数据如何构建或提升企业的数据安全保护能力，数据安全团队如何通过组织建设，梳理合规和安全需求，设定制度流程，然后通过技术工具和产品进行数据安全建设。

- 持续运营过程中如何明确找出薄弱环节，设置重要检查点，持续评估，有的放矢调整策略，针对性完善制度流程等。

- 介绍数据安全技术的应用和保护方法，从各个场景分享数据安全相关技术和产品的应用，以及来自企业的实际参考案。

- 介绍个人数据安全的保护意义和方法，提高数据安全意识。

专注安全 精深技术

安全是人员、技术、操作三者紧密结合的系统工程，是不断演进、循环发展的动态过程。而安全培训旨在强化客户的安全防护和管理，提高自身应对安全新风险的能力，以减少技术不断发展引起的隐患。通过本次安全培训，提高了该企业技术人员对数据安全的认知，同时对于自身落实安全制度和技术防范措施，建立完善的网络信息安全系统有很好的促进作用。后期，亿赛通将继续专注于人才培养，为加强网络安全强国做贡献。

课程名称	授课目标
数据安全监管法律法规讲解	企业高管
数据安全个人信息监管解读	
数据安全防护体系讲解	安全技术负责人
数据泄露防护主流产品技术	
数据梳理及分级分类讲解	
企业数据安全审计体系讲解	
数据安全能力成熟度模型解析	
数据安全治理体系与典型应用	
数据库安全威胁、安全产品演进及技术发展趋势	
数据库安全防护主要技术讲解	全体员工
数据安全案例分享和上机实操	
数据安全保护的意义	
个人隐私安全防护讲解	

亿赛通数据安全培训课程

欲了解课程详细信息，请咨询服务热线：

400-898-1617

亿赛通核心产品精彩亮相“天府杯” 2019 天府国际网络安全高峰论坛



为期两天的“天府杯”2019 国际网络安全大赛暨 2019 天府国际网络安全高峰论坛于 11 月 17 日在中国成都西部国际博览城圆满收官，硕果累累。在两天活动中，来自国内外产学研各界的嘉宾，对全球互联网安全进行了丰富的论坛分享和讨论。



活动呈现了一场集政、产、学、研等国内外互联网安全行业人士及企业高层，近千余人的思想和竞技盛宴。本次活动是由清华大学网络科学与网络空间研究院、中科院信息工程研究所等多家行业顶尖单位共同举办。主题为“数字赋能时代 天府护航安全”，论坛将视线聚焦西南地区引领网络安全产业发展所面临的机遇和挑战，国内外行业专家及技术精英共同上演一场互联网信息安全的思想碰撞。

成果展示核心亮相

今年，亿赛通受邀参与大会，作为数据安全领域的龙头骨干企业，携旗下核心产品亮相网络安全成果展，向与会的政府主管部门、顶级企业、国内外行业专家及技术精英们展示技术研发成果，共商解决方案，共谋合作之道。

我司专家在现场就当前新形势下的数据安全体系为参观人员做了全面分析，尤其是现今数据安全已经上升到国家高度的情况下，从国家政策，到等级保护 2.0 中新的规定，再到今年发生的最新数据安全重点事件的安全问题及应对策略做了深入浅出的分析和阐述，简单明了的解释了如何保证数据文件在“内忧”与“外患”中实现精准有效防护。



并且，亿赛通专门为与会人员演示了“定位敏感信息 - 发现敏感信息 - 控制敏感信息 - 监督敏感信息”的完整闭环解决方案，“知”“识”“控”“查”的最新设计理念获得了现场嘉宾的一致认可。

政府助推网络安全，安全圈“火花四溅”

政府重视和政策扶持正在不断推动信息安全产业的快速发展，尤其各大法律条文的出台，更是将数据保护提到了法律高度，加强数据安全是行业大势，势不可挡。在国家政策支持下，数据安全市场将越来越具有优势。

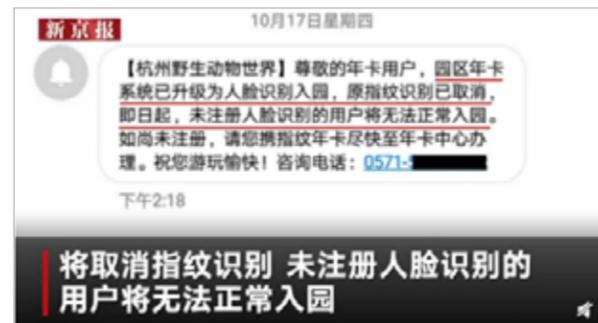
迈入数字经济时代，产业升级，威胁也在加剧，面对不断变化的安全挑战，亿赛通提供可靠有效的解决方案的同时，会同行业伙伴和客户积极探索数据安全的产业价值，助推数字经济安全腾飞。活动现场诸多参会人员均反馈，此次参会为网络安全行业提供了建设性的思路与实践方向，不虚此行。而亿赛通也凭借深厚的实力积淀，丰富的产品解决方案体系及广泛的客户支撑，成为展会现场最亮的星。未来，亿赛通将继续坚定推动企业数据安全，并向世界级企业迈进。

国内人脸识别第一案，我的信息泄露谁负责？

当人脸识别结合着各大互联网巨头的商业布局考量飞速“入侵”我们的日常生活，相应的技术准备与规范真的准备好了吗？

随着人工智能时代的到来以及各种新技术的出现，人们的日常生活得以享受到大量新兴技术带来的便利，这点原本是无可厚非的。但需要指出的是，在新技术的发展、落地过程中，总会出现些许“阵痛”，这也是无法避免的。

浙大法学博士拒绝“刷脸”入园起诉杭州野生动物世界



今年7月，杭州野生动物世界引进了人脸识别技术，应用于年卡使用者的入园检票。10月28日，一位年卡用户将动物世界告上法庭，其质疑：一家动物游乐场也能采集人脸信息，万一信息泄露谁能负责？这位质疑的用户名叫郭兵，他是浙江理工大学特聘副教授，是浙大法学博士。11月1日，法院正式决定立案受理这起案件。“采指纹，我是同意的。但是采集人脸信息，我是拒绝的，难道因为我拒绝人脸信息采集，作为年卡用户的我就不能享受入园的权利吗？”郭兵说。

丰巢智能柜引进人脸识别系统紧急下线



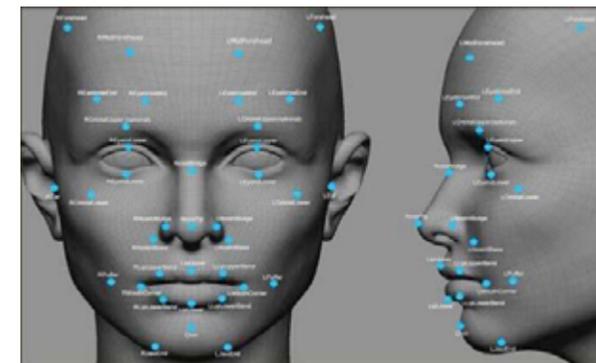
除上述事件外，前段时间，嘉兴上外秀洲外国语学校402班科学小队在一次课外科学实验中发现，在使用丰巢智能柜“刷脸取件”的时候，只要用一张面部打印照片就能够打开智能柜，根本无需快件人本人在场。随后，相关部门对该结果进行的验证表明，丰巢智能柜确实存在普遍的只要用照片就能打开的情况。

尽管丰巢随即就紧急下线了“刷脸取件”功能，并称此次只是小范围测试，并未导致用户损失，但这次事件无疑将“人脸识别”痛点披露，社会目光聚焦到“刷脸”过程中所存在的种种隐患：“刷脸支付的安全性”、“面部信息泄露的隐患”、“是否有规范的监管”等都成为大众所担心的问题。

“刷脸”进入、“靠脸”结账……当人脸识别结合着各大互联网巨头的商业布局考量飞速“入侵”我们的日常生活，相应的技术准备与规范真的准备好了吗？

刷脸一时爽，安全火葬场？

两起事件中的“刷脸取件”使人们对“人脸识别技术”表示疑虑，更令人担忧的是在支付场景下“刷脸”的安全性和隐私性。



因为“刷脸”的基本原理是将终端硬件采集到的用户信息与云端存储的信息进行比对，看信息是否一致，然后解锁完成人脸支付，所以若云端生物数据库信息发生泄露或采集端信息容易“伪造”，则用户的个人隐私就会失去保障，刷脸支付就可能面临比较大的风险。

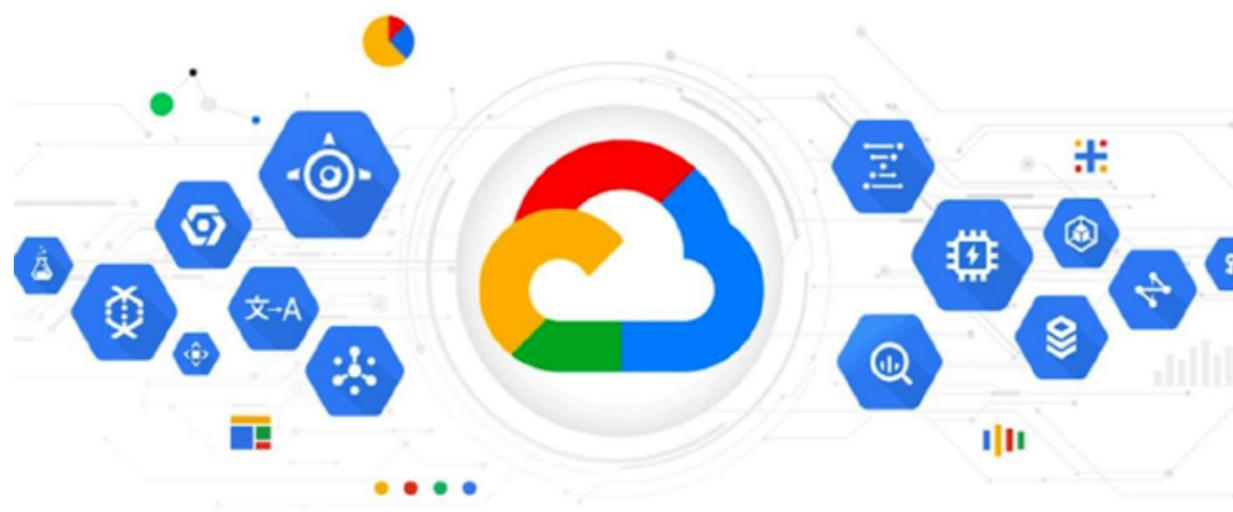
推广人脸识别，数据安全是关键

鉴于人脸等生物识别信息具有唯一性和不可更改性，相关信息一旦发生泄露，就会造成不可逆转的潜在危机及风险。因此，相关监管部门应该尽快出台生物信息采集、使用规则和标准，支付机构也应不断提升技术水平以增加应用安全性，防治云端数据泄露，相关企业在向客户推广刷脸支付方式时，理当尽最大限度确保数据安全。

诚然，“人脸识别技术”的发展和應用正有效地推动着大量行业的进步，但随之暴露出的很多潜在风险也应当引起足够的重视。“用户面部特征采集的安全性及隐私性”、“用户信息的泄露与恶意买卖”、“法律法规不健全”等等问题，“刷脸”真正实现普及还有很长的路要走。中国数据安全防护专家亿赛通也在此呼吁大家，“刷脸”需谨慎体验，防止某些不法分子窃取你的信息实施各种非法活动，推广数据安全，我们一直在路上……

新闻来源：新京日报

云安全 | 12 亿网民信息泄露， 究竟谁的“锅”？



日前，一个汇总了 12 亿用户个人信息的数据库被发现毫无保护的存在于某个服务器上，这些个人信息中包括社交媒体帐户、电子邮件地址和电话号码。到目前为止还不清楚该数据库出现在这个服务器上的原因。

相关人员表示，数据库中的大多数数据是由一家名为人员数据实验室（People Data Labs）的公司收集的。

人员数据实验室自称可以提供多达 15 亿人的工作电子邮件和社交媒体帐户详细信息。该公司的网站称，数据通过多种来源获得，购买数据的用户可以据此来接触“美国、英国和加拿大超过 70% 的决策者”。

本次未受保护的数据并非是存放在人员数据实验室的服务器上，而是出现在一个 Google Cloud 服务器上。

人员数据实验室的首席执行官表示：只有一部分数据来自他的公司，他怀疑这些数据是由另一家公司汇总收集的。10 月份在例行扫描未受保护的数据时发现了这个数据库，并向美国联邦调查局报告了这个 4TB 数据库及其位置。这次事件再次暴露了，用户对公有云的最大担心——数据安全。

目前美国云计算领域的竞争日益激烈，企业上云也是主流趋势之一，但是，云服务是否对得起用户的信任和买单呢？对于用户而言，只要云服务品牌有保障，并且符合大多数企业需求就可以了。

但是近年来，云厂商确实经常出现数据泄露的情况，从阿里云函数计算挂掉、直接导致国内半个互联网瘫痪、到本次谷歌云存储未经保护的数据库……企业上云后的安全如何保障？成为云厂商急需解决的问题。

亿赛通数据安全卫士是针对 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安全产品。当您需要将数据文件上传云端时，先用安全卫士设置保护，不法分子企图盗取您云端的重要数据后，想打开首先需要进行身份认证。此软件可以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或二次使用，这样就可安心上传到云盘。

中国民生银行



客户简介

中国民生银行成立于1996年，是一家主要由民营企业发起设立的全国性股份制商业银行。成立20多年以来，伴随着中国经济的快速发展，在广大客户和社会各界的支持下，中国民生银行充分发挥“新银行、新体制”的优势，从当初只有13.8亿元资本金的小银行，发展成为一家核心资本超过3200亿元、资产总额超过5.2万亿元、分支机构近3000家、员工近6万人的大型商业银行。中国民生银行致力于实现“长青银行、百年民生”的宏伟愿景，坚持“以客户为中心、以市场为导向、以创新为动力”的发展理念，锐意变革创新，加速战略转型，努力成为中国银行业的标杆性银行，为客户创造更大的价值，为投资者实现更高的回报。

需求背景

针对互联网安全新形势，民生银行面临着信息安全威胁与风险，其中来自外部的安全形势日趋复杂和严峻，如APT攻击、多态变形的恶意软件攻击、0Day攻击等多种手段层出不穷，民生银行内部的安全系统监测呈逐渐攀升的状态。所以，民生银行非常重视对企业内部的敏感数据保护。

解决方案

亿赛通文档透明加密系统以数据透明加密技术为核心，通过信息安全边界建立，有效的防止企业核心信息资产外泄的同时，不影响用户工作习惯及业务效率。

智能透明加密：采用第四代VFS技术，实现对任意文档自动透明加密。不改变和影响用户使用系统和工作效率。

智能半透明加密：可实现对本地文档不影响情况下，无障碍使用密文文档，对本地敏感文档可手动加密。

开放式策略库：用户可根据业务及管理需要进行安全策略自定义或策略导出导入，开放、灵活的策略配置，无须二次开发，有效降低企业后续维护成本。

身份认证集成：支持与基于Ldap和OpenLdap协议的统一身份认证平台（如AD、ED、TDS等）进行无缝集成，如实现组织架构及用户帐号信息的自动完整同步和单点登录认证集成等。

项目成果

民生银行通过部署亿赛通文档安全技术，建立了专业化的信息安全平台，完善了安全制度和规范，提升了信息安全技术的支撑能力，完善了信息安全的响应机制。

长城证券有限责任公司



客户简介

长城证券有限责任公司，成立于1995年11月。公司现注册资本20.67亿元。股东分别是中国华能集团公司、深能源、招商局、中国核工业集团公司等国内知名大型国有企业集团。公司经营范围是为客户提供证券代理买卖、证券发行与承销、收购兼并、改制重组、财务顾问、资产管理、证券咨询等证券投、融资全方位服务。公司控（参）股长城基金管理公司及景顺长城基金管理公司。公司在国内20个城市拥有营业部网点24家。

需求背景

长城证券服务模式正由传统的柜台服务模式向网上银行、第三方支付、P2P小额贷款、企业网络融资等新型服务模式扩展。信息化金融已逐渐成为金融业的发展方向。但与此同时，由于这种新型服务方式虚拟化、业务边界模糊化、经营环境开放化等特点，无论是从组织内部还是外部而言，都使得金融业务面临网络攻击、非法窃取交易信息、客户信息泄露等新的信息安全问题。如何利用信息技术的优势加强长城证券公司的内部控制，防范和化解敏感信息泄密风险，是当前长城证券信息安全关注的重点和难点。

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平衡，实现电子文档的数据安全。

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。

文档权限管理：细粒度权限控制、模板批量授权、文档权限管理。

文档外发管理：用户身份认证、使用权限管控。

流程管理：文件解密审批流程、文件外发审批流程、邮件外发审批流程、离线办公审批流程、文件还原审批流程。

审计跟踪：邮件外发审计、文件解密审计、文件打印审计、流程全文检索审计、违规操作预警。

项目成果

长城证券有限责任公司通过部署了亿赛通文档安全产品保证了文档敏感信息的安全，使得员工在使用过程中内部透明，使用无感知；外部用户非法获取内部文档无法使用；合法用户获取内部文档优先使用。