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

12 月刊

2018 年共 11 期

荣誉丨2018 中国软件大会亿赛通 DSIP 产品斩获数据安全领域最佳解决方案奖

Google+ 五千万用户隐私数据泄露，强大企业也需专业防护

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

2/3 刊首语

行业聚焦 INDUSTRY FOCUS

4-8 国内行业新闻

9-15 国外行业新闻

亿赛通动态 ESAFENET NEWS

16/17 荣誉 | 2018 中国软件大会亿赛通 DSIP 产品斩获数据安全领域最佳解决方案奖

18/19 强强联手京东方，开启 2019 年超大规模项目新篇章

亿赛通小贴士 ESAFENET PROMPT

20/21 Google+ 五千万用户隐私数据泄露，强大企业也需专业防护

22/23 万豪酒店 5 亿客户信息外泄，酒店行业数据泄露真的无解？

24/25 惊！勒索病毒不要比特币，改“微信支付”？

26-29 年终盘点 | 2018 年引人注目的十大数据泄露事件，信息安全已危及全球！

典型案例 TYPICAL CASES

30/31 亿赛通综合防护解决方案补齐设计制造行业数据安全短板

32/33 亿赛通与信大捷安达成战略合作，为企业数据安全上一把安心锁

刊首语 PREFACE

告别 2018，迎接 2019，《亿赛通十二月刊》亮点纷呈

这是个告别的季节，是个蜕变的时刻， 2018 年转眼过去、挥手告别，所有的辛劳不会白费，2019 年让一切从头再来，我们早已做好准备。

自从信息技术出现以来，对应的安全问题就受到广泛关注，网络安全产业的范畴也随着网络安全保障需求不断延伸而扩展。大众对于一些数据巨无霸公司在使用和保护个人信息方面的担忧日益增强，公众的情绪将成为推动相关法律法规落地的强大助力。不过，尽管我国政府和企业不断重视并加强网络安全保障，但境外针对我国政府等重要领域的有组织网络攻击仍在持续，“互联网 +”、云计算、大数据等新应用也引发着新的安全风险，大型互联网商业平台安全事故呈现高发态势，针对个人数据的网络犯罪呈现组织化和产业化的特征，一系列重大安全事件仍然频发。与之相对的是，我国网络安全企业实力稳步提升，发展态势总体良好，预计到 2019 年，我国信息安全市场总体规模有望达到 48.22 亿美元。未来，网络安全市场市值将升至令人目眩的高度，面对 2019，亿赛通做好了充分准备，迎战未来。

国内

1、培训机构贩卖学生及家长信息，安徽警方摧毁一条灰色产业链

摘要：记者从安徽省滁州市公安局获悉，当地警方近日成功摧毁一条跨市贩卖学生信息的灰色产业链条，累计查获公民个人信息 20 余万条，扣押作案电脑 10 余台。目前，涉案的 4 名嫌疑人已被警方刑事拘留。

2、世界 50 强名校硕士毕业生，为爱成“内鬼”

摘要：全球知名高校研究生胡某，于 2016 年 11 月毕业回国，次年 2 月进入浙江某汽车集团有限公司就职。其男友为一家金融公司的客户经理，为帮助男友获取更多的客户源提高业绩，胡某将工作期间接触的一份车主档案发给男友，其中包含 2 万多条含有姓名、地址、移动电话、车牌、车型等内容的财产性公民个人信息。

3、男子攒 936 万条个人信息赚“提成”获刑四年

摘要：为培训机构招生的何某，通过网络收集公民个人信息，除了替自己的“东家”寻找生源外，还将部分信息与他人交换使用……在案发时，何某的电脑内存储公民个人信息 936 万条，其中百万条涉及法律规定的包括公民财产交易、健康状况等敏感信息。

4、疯狂买卖 300 多万条信息　还能“私人定制”

摘要：12 月 4 日，山东省公安厅举办新闻发布会，就山东网警今年查办的典型案例进行发布，其中公安部督办的一起特大侵犯公民个人信息案，涉及全国 18 个省、33 个市，涉及公民个人信息 300 多万条，涉案金额达到 800 多万元。

5、用户数据泄露多发 工信部将开展移动恶意程序治理

摘要：12 月 3 日，工信部网络安全管理局发布 2018 年第三季度网络安全威胁态势分析与工作综述。第三季度公共互联网网络安全形势依然严峻，发生多起严重危害用户合法权益的网络安全事件。工信部下一步工作重点包括：做好网络安全试点示范项目相关工作；开展移动恶意程序专项治理工作等。

6、西安一男子为报复前任东家破坏计算机系统被公诉

摘要：郭东（化名）在西安一知名信息工程有限公司上班。该公司的呼叫中心在 2017 年 11 月 20 日至 2017 年 12 月 1 日期间，服务器不断遭到攻击，部门内部业务系统频繁异常，数据库被恶意删除、数据监控文件也全部丢失，导致作业系统无法正常使用，造成经济损失 10 万余元。这一切的始作俑者正是已经从公司离职的郭东。

7、安徽破获一跨省侵犯公民信息案近万条车辆信息被非法交易

摘要：日前安徽省马鞍山市公安局破获一跨省倒卖公民信息案，4 名不同省份的犯罪嫌疑人以每条 20 元的价格非法窃取、交易公民车辆信息近万条。

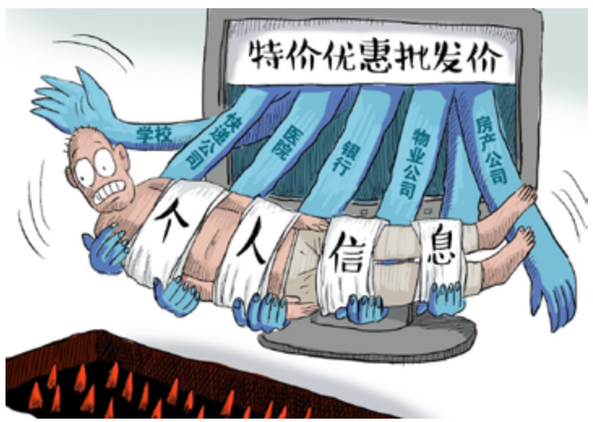
8、“黑客”窃取信用卡信息网上叫卖 非法获利 200 多万元

摘要：繁昌县公安局网安大队民警告诉记者，今年 5 月，他们经过调查，发现繁昌一名网络人员在多个 QQ 群发布信息，称其有高质量的、稳定的“卡料”。所谓“卡料”是专门术语，意思是真实的信用卡信息。这些信息包括信用卡号、安全码、日期、姓名、身份证号、家庭住址等。

9、江西宜春警方破获一起侵犯公民个人信息案

摘要：据了解，今年 4 月 3 日，宜春市公安局网安支队在工作中发现，宜春市高安市居民聂某杰在互联网上买卖公民个人信息，包括姓名、身份证、电话号码、地址、芝麻信用分等，非法牟利近一百万元。近日警方抓获犯罪嫌疑人聂某杰、李某志、刚某帽、秦某、陈某丰等 5 人。

10、慈溪破获侵犯公民个人信息案 抓获犯罪嫌疑人 56 名



摘要：近日，慈溪市公安局破获一起侵犯公民个人信息案件，抓获犯罪嫌疑人 56 名，查获公民个人敏感信息数十万条。据介绍，仅本案查获情况就表明，每 5 名慈溪人中，就有 1 人的公民个人敏感信息被泄露。这些信息不仅有公民的姓名、电话，甚至其所购置房屋的楼号、单元、房号都一清二楚。

国外

1、实力“捅熊”：Cylance 揭露 一场针对俄罗斯的网络攻击活动

摘要：在上周，网络安全公司 Cylance 揭露了一场针对俄罗斯关键基础设施建设领域的网络攻击活动。攻击者在过去的三年时间里创建了大量的虚假网站，模仿了二十多个俄罗斯国有石油、天然气、化工、农业和其他关键基础设施机构，包括俄罗斯石油公司（Rosneft Oil）及其子公司。

2、自 9 月份以来，MuddyWater（污水）间谍团伙已攻破至少 30 家组织

摘要：赛门铁克（Symantec）的 MATI 团队于近日发文称，被其命名为“Seedworm（也被称为 MuddyWater）”的网络间谍团伙仍在保持活跃。自今年 9 月份以来，已经有来自 30 家组织的 130 人成为了该团伙的受害者。

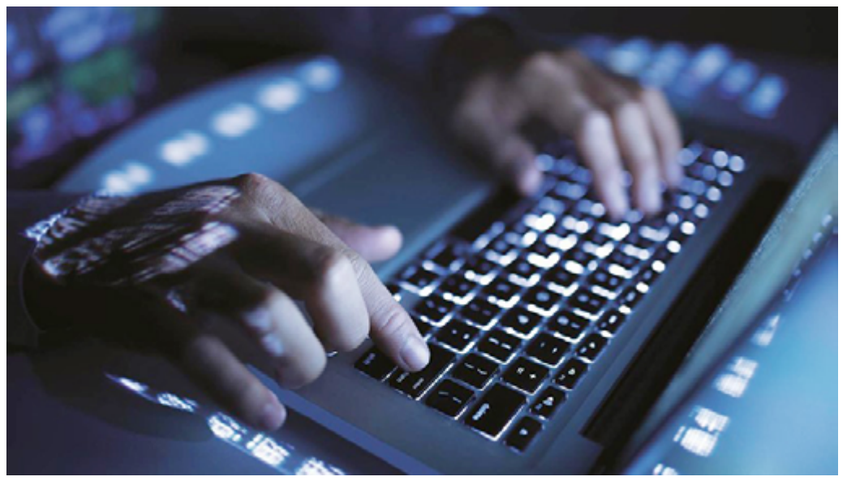
3、 巴西 1.2 亿纳税人信息遭泄露

摘要：一台配置错误的服务器于未知的时间暴露了 1.2 亿巴西公民的纳税人身份证号 (Cadastro de Pessoas Fisicas，简称 CPFs)。巴西国民需要在开立银行账户、创建企业、纳税或获取贷款之前，先申请到 CPF 号码，号码会与所有者的个人和财务信息绑定，此类信息被泄露 / 公开，无疑是一种巨大的风险。根据 InfoArmor 的最新研究，2018 年 3 月，一个 Apache web 服务器被发现配置不当，暴露了存储在其上的数据档案。

4、Facebook API Bug 暴露 680 万用户照片

摘要：Facebook 14 号宣布，它在其照片共享系统中发现了一个新的 API 错误，允许 876 位开发人员访问他们从未在时间轴上共享的用户私密照片，包括上传到 Marketplace 或 Facebook Stories 的图像。

5、 Group-IB：全球约有 4 万多个在线政务服务平台用户账户被盗



摘要：俄罗斯网络安全公司 Group-IB 于近日发布消息称，在过去一年半的时间里，网络犯罪分子利用间谍软件工具和网络钓鱼战术，从全球 30 多个国家 / 地区政府官方门户网站盗走了 4 万多个在线政务服务平台账户。

6、一个新 Bug 泄露 Google+5250 万用户信息

摘要：周一，谷歌公开了 Google+API 中的另一个 bug(11 月 7 日软件更新活动的一部分) 暴露了来自 5250 万个账户的用户数据。

7、微软揭露针对美国智库的网络攻击，疑似由俄罗斯黑客组织 APT29 发起

摘要： 微软的安全专家于近期揭露了一场主要针对美国发起的鱼叉式网络钓鱼活动，其目标包括公共机构和非政府组织，如智库、研究中心和教育机构，以及石油、天然气、化工以及医疗行业的私营企业。这场活动是俄罗斯黑客组织 APT 29（CozyBear，“舒适熊”）发起的，该组织也被微软称之为 YTTRIUM。

8、疑似 MuddyWater 黑客组织在针对土耳其政府的攻击中使用了新后门

摘要： MuddyWater 是一个早已名声在外的网络犯罪组织，自 2017 年以来一直很活跃。其目标群体遍布中东和中亚，主要的攻击手段是使用带有恶意附件的鱼叉式钓鱼电子邮件。最近，该组织被发现与今年 3 月份针对土耳其、巴基斯坦和塔吉克斯坦的一场攻击活动有关。

9、问答平台 Quora 漏洞泄露一亿用户信息

摘要： 互联网最大的问答平台之一 Quora 12 月 4 日宣布其服务器可被非法分子访问并窃取 1 亿用户信息，这几乎是 Quora 平台用户数量的一半。

10、匿名黑客入侵 5 万多台打印机，只为给自己喜欢的主播打广告

摘要： 一位匿名黑客在上周劫持了全球超过 5 万台连接到互联网的打印机，用于打印广告传单，呼吁所有人订阅 PewDiePie 的 YouTube 频道。

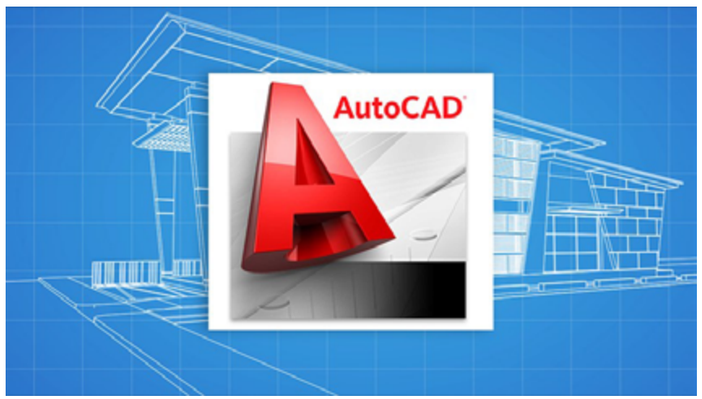
11、巴西 Sky Brasil 公司泄露 32.7 万用户信息

摘要： 独立研究员 Fabio Castro 发现，巴西最大的订阅电视服务公司 Sky Brasil 泄露了 32.7 万用户的信息，包括 28.7GB 的日志文件和 429.1GB 的 API 数据，这些数据显示姓名，家庭住址，电话号码，出生日期，客户端 IP 地址，付款方式和加密密码。

12、未知黑客组织利用 SLoad 恶意软件在意大利开展攻击活动

摘要：网络安全公司 Yoroi 在上周披露，在过去的几个月里，他们观察到了一起针对意大利用户的恶意电子邮件活动。Yoroi 公司已经启用了内部代号“Sload-ITA”（TH-163）来追踪这一威胁。此外，在今年 5 月份，SANS ICS 的研究人员在英国也观察到了类似的活动。类似的恶意软件组件投递方式以及利用压缩文件来隐藏恶意代码的技术，将这两起活动联系在了一起。

13、研究发现新的工业间谍活动，旨在利用 AutoCAD 窃取机密文件



摘要：据外媒 ZDNet 报道，安全专家在最近发现了一起非常独特的恶意软件分发活动，其目标是那些在设计工作中使用 AutoCAD 软件的公司。报道称，该公司在本周早些时候向 ZDNet 分享了这一调查结果。从该公司提供的遥测数据来看，这起活动似乎开始于 2014 年，并一直活跃至今。

14、黑客利用漏洞从美国政府支付系统获利 170 万美元

摘要：近日，网络安全公司 FireEye 证实 Click2Gov 发生了一起安全事件，威胁行为者已经在其中种植前所未见的恶意软件，解析支付卡数据的日志并提取付款细节等详细信息。至少有美国的 46 个城市以及加拿大的一个城市的 294,929 条付款记录遭到了泄露。调查结果显示，在丢失客户数据的城市中，只有不到 50% 的城市知情或公开披露了其网站上发生的数据泄露事件。恶意行为者通过在暗网销售这些信息，至少获利 170 万美元。

荣誉 | 2018 中国软件大会
亿赛通 DSIP 产品斩获
数据安全领域最佳解决方案奖

2018 年 12 月 20 日，由中国电子信息产业发展研究院主办的“2018 中国软件大会”于北京召开。在政府主管部门的指导和支持下，中国软件大会已成功举办多年，大会专注于促进和传播企业级软件技术的创新，已成为引领中国软件和信息技术服务产业发展的风向标。

本届大会以“驾驭数字化转型·走进智能互联时代”为主题，汇聚政府领导、权威专家、企业领袖，就企业数字化转型中的热点问题进行专业的解读和实践分享。同时，围绕大数据、人工智能、区块链等新兴技术创新和落地应用进行深入探讨。

随着宏观经济的发展，特别是数字经济的崛起，以及企业自身转型发展的需要，数字化转型已经成为企业乃至政府的必然发展趋势。如何驾驭数字化转型，使政府、企业在转型过程中不断创新、发展乃至壮大，将成为政府及企业所面临的重要挑战。智能互联时代的到来，将带来更多新的商业模式与机遇。无论是在企业的数字化转型过程中，还是在智能互联时代的发展中，软件都将起到至关重要的作用。特别是，随着大数据、人工智能、物联网以及区块链等新一代信息技术的深入应用，软件的价值和作用将得到更大的体现。

作为 IT 行业的年度盛会，本届大会设置了专业评奖活动，综合企业影响力、创新力、执行力、前瞻力、发展力、贡献力等多项评选指标。通过大会官网在线投票及专家评审，亿赛通数据安全智能管理平台（DSIP）荣获“2018 中国软件和信息服务业数据安全领域最佳解决方案”奖。

产品采用智能分类、智能分级、智能发现、智能防护、态势感知等领先技术，为我国各个领域的政企单位提供全方位综合性的数据安全解决方案，此次获奖是业界对亿赛通产品及服务能力的认可！

在数字化转型的发展趋势下，技术创新是产业发展走向繁荣的前提。作为专业的数据安全服务厂商，亿赛通发展创新的脚步终未停息，研发新产品、引进新技术是企业快速发展的必备筹码。技术的革新与发展推动了企业在数据安全领域独占鳌头的地位，促使亿赛通为广大客户朋友提供中国最佳的解决方案产品，让客户对亿赛通企业认可、产品满意。2018 即将结束，这一年亿赛通用行动和实力取得丰硕成果，2019 企业将会更加努力，继续引领行业前行，做好中国的数据安全防护专家！

强强联手京东方，开启 2019 年超大规模项目新篇章

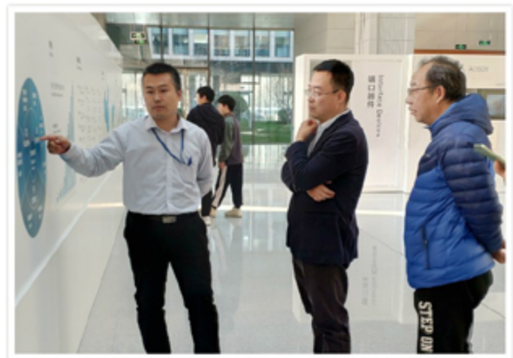
近期 ,亿赛通与京东方合作项目经双方努力取得阶段性胜利。作为半导体显示领域全球领先集团 ,其内部所有核心文件，终端上的数据信息均需严密防护。据悉，京东方对文档加密项目进行了长期调研，面向全国招标。在选型过程中，也对多家厂商的安全产品做了全方位的比较及严格的应用测试。亿赛通根据京东方的实际需求量身定做出适合集团应用的数据安全最佳解决方案，最终赢得客户信赖与认可，签署集团文档加密项目。

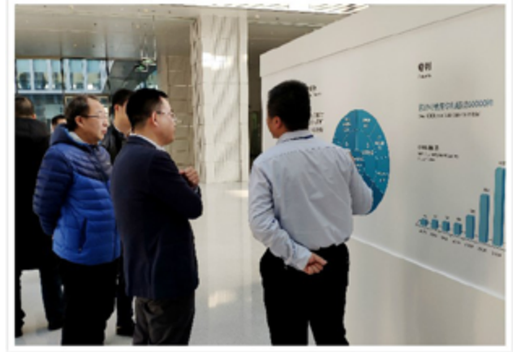
项目一期于京东方总部部署全部终端，后期持续扩增，项目二期范围扩大至各个属地，预计未来 2-3 年内，集团内部所有终端均上线亿赛通加密产品。由于合作具有一定规模，双方领导特于 12 月末召开京东方集团文档加密项目一期总结暨二期启动会。

会中，京东方领导表示，本次部署的亿赛通文档加密产品对集团来讲意义重大，将成为京东方积蓄力量勇往直前的后方保障。亿赛通产品功能强大且易于使用，经过目前总部终端的部署，所有物理端和云环境均实现加密管控，保证公司内部文件在所有涉密终端上无障碍流转，促进了京东方在项目过程中建立跨部门组织，提高内部共享效率的同时，确保文件安全。同时，产品又具有良好的兼容性，在不影响正常操作的同时，最大限度保障系统稳定可靠运行。即使在使用过程中出现问题，亿赛通专业、高效的售后服务体系也可保证企业业务安全运营。未来，有亿赛通为集团坚守阵地，京东方可以更专心投入到市场中，打造半导体行业优质品牌！

随后，亿赛通领导表示，公司向来以产品技术为核心主导 ,项目一期的实施过程 ,是产品与企业的结合过程，是将理论付诸实践的过程。随着数字化、网络化、智能化的快速发展，国内国际制造业文档安全形势越来越严峻，企业内部系统中安全问题的发现更加困难、环境更加复杂，一套完善的加密系统必不可少。

为确保项目顺利上线，公司技术部针对京东方属地多、分布广、业务集成度高等特点，结合亿赛通多年来在安全行业积累的业务经验，设计出更严密的数据安全解决方案。在服务方面更是为京东方专门定制项目响应机制，即“升级 - 开发 - 驻场”服务，7*24 小时第一时间响应，多属地优先分配资源。亿赛通在未来将重点通过全局部署、统一管理、单独实施等策略，方便、快捷、高效的为京东方业务提供数据安全支撑服务。





亿赛通依靠领先的技术，优质的产品，“服务客户、持续创新、勇担责任、专业至上”的核心价值观，赢得了京东方的充分信赖。未来，亿赛通会是京东方不断发展与创新中最得力的伙伴之一 ,有中国数据安全防护专家为其坚守阵地，京东方会创造更加辉煌的明天！

Google+ 五千万用户隐私数据泄露，强大企业也需专业防护

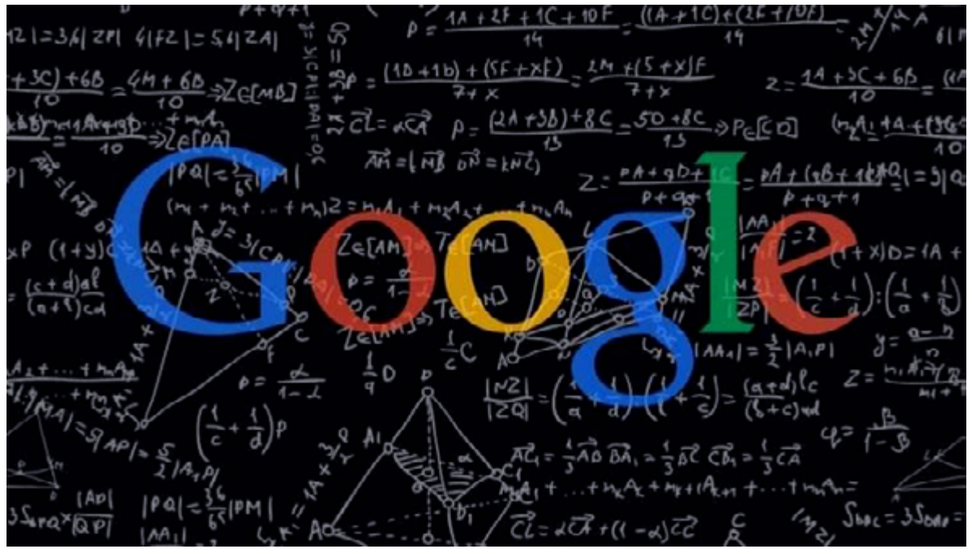
Google+ 要提前关闭？真的假的！

谷歌公司发出官方声明！

Google+ 关闭时间从 2019 年 8 月提前到 4 月！

为什么突然提前关闭时间？

原来仅仅两个月谷歌再次被爆出数据泄露！



Google+ 出现的最新漏洞，让应用开发者使用应用程序接口（API）在 11 月的 6 天时间中，访问 5250 万用户的姓名、电子邮箱、职业和年龄以及其他详细信息。

其实，早在 2015 年到 2018 年 3 月期间，由于 Google+ API 接口出现的问题，外部开发者利用这些接口直接读取 Google+ 用户私密数据，涉及 50 万名用户数据，但谷歌当时选择瞒报而不是公开此错误。

此前的数据泄露问题让谷歌计划在 2019 年 8 月份彻底关闭面向普通用户使用 Google+，但仍保留企业级用户的版本。但是随着此次新的安全问题出现，谷歌决定将彻底关闭 Google+ 的时间提前到 2019 年 4 月份，并在未来 90 天内，逐步关闭 Google+API 接口的调用。

近两周爆发多起大规模数据泄露事件，从万豪酒店 5 亿客人信息泄露，到陌陌 3000 万数据暗网叫卖，新型勒索病毒爆发要求微信支付赎金 ~

虽然 2018 年已经进入尾声，但……企业切勿放松警惕。不法分子等的就是你放松的那一刻，即使在事后防御也无法挽回损失！不过，当企业核心数据被盯上时，难道真的无力防护？

亿赛通数据安全解决方案

通常敏感信息主要在五种形态下容易被泄露，即数据的存储、使用、传输、外带、外发，中国数据安全防护专家亿赛通针对这五种不同形态下进行数据的保护。

1、数据存储安全

针对场景：竞争对手窃密、员工离职拷贝、内部有意无意泄密、间谍 / 黑客窃密、设备丢失、非法脱机、电脑报废数据丢失、电脑那到第三方去维修信息被窃……

解决方案：以数据加密技术为核心，通过将技术平台与管理体系有效结合，可对任意文档自动透明加密，实现对用户核心数据资产的全方位保护。同时，通过信息安全边界的建立，降低核心数据资产如源代码、设计图纸、财务数据、经营分析以及其他任意信息资产有意或无意泄密风险。

2、数据使用安全

针对场景：涉密文件在企业内部员工流通过程中的使用权限，如有些涉密文件不想被内部某些部门打印、复制、修改，导致信息泄密问题……

解决方案：文档权限管理系统采用多层结构设计，对企业核心电子文档进行细分化的权限设置，确保机密信息在授权的应用环境中，在指定时间内，被指定的人进行指定操作，不同使用者对同一文档拥有不同权限，通过对文档内容的安全保护，实现机密信息分密级且分权限的内容安全共享机制。

3、数据传输安全

针对场景：在数据传输的过程中，遇到网络窃取敏感信息、网络拦截重要信息、网络监听重要信息等非法窃取信息……

解决方案：亿赛通移动终端数据防护系统，主要防止利用移动设备非法获取应用系统数据的智能终端安全防护系统。移动终端数据系统由移动数据防护控制台与移动终端客户端软件两部分组成，系统配置管理采用 B/S 架构，系统部署后不会改变用户使用习惯。

4、数据外带安全

针对场景：企业工作人员在外出差办公携带电脑涉及企业的敏感信息容易被窃取、因工作需要回家加班涉及的公司敏感信息，携带出去带来的风险……

解决方案：离线办公支持，系统提供安全离线办公业务支持，通过离线审核、策略预设及离线补时等功能满足各类离线办公要求，保障离开公司外办公的状态下信息安全操作。

5、数据外发安全

针对场景：针对的是企业外部第三方文档使用者的权限问题，就是当企业将自己的设计图纸、办公文档、视频音频等数据，交接给第三方时，第三方会盗取其中的信息……

解决方案：亿赛通文档外发管理系统，是针对客户的重要信息或核心资料外发安全需求设计的外发安全产品。当客户需要将涉密文档外发给客户（代理商、合作伙伴等）人员时，应用文档外发控制系统生成外发文件发出。当外发文件打开时，用户通过身份认证，方可阅读文件。同时，外发文件可以限定接收者的阅读次数和使用时间等细粒度权限，从而有效防止客户重要信息被非法扩散。

万豪酒店 5 亿客户信息外泄，酒店行业数据泄露真的无解？

万豪国际集团是全球首屈一指的酒店管理公司，拥有遍布全球 130 个国家和地区的超过 6,500 家酒店和 30 个品牌（包括丽思卡尔顿酒店、JW 万豪酒店等）。1997 年，万豪进入中国酒店业市场。

据外媒报道，11 月 30 日，全球最大的连锁酒店——万豪国际酒店集团（以下简称“万豪”）多达 5 亿人次的详细个人信息遭到泄露。

酒店数据库被黑客入侵 ---5 亿信息或外泄

万豪方面表示，集团内部调查发现，自 2014 年以来，一名攻击者一直都能够访问该集团喜达屋（Starwood）部门的客户预订数据库，但公司在近期才发现这一问题。

万豪在声明中称：“公司尚未完成在数据库中识别重复信息的工作，但认为这个数据库中包含了大约 5 亿人次预订喜达屋酒店客人的详细信息。”

万豪国际集团公布喜达屋宾客预订数据库安全事件相关信息

美国马里兰州贝塞斯达－2018年11月30日，万豪国际集团已采取措施调查和处理涉及喜达屋宾客预订数据库的数据安全事件。2018年11月19日万豪国际调查发现，2018年9月10日及之前喜达屋旗下酒店预订数据库中的宾客信息曾在未经授权的情况下被访问。

2018年9月8日，万豪国际收到一条内部安全工具发出的关于第三方试图访问喜达屋宾客预订数据库的警报，万豪国际迅速聘请了权威安全专家帮助确定已发生异常情况，万豪国际调查过程中了解到，自2014年起，即存在第三方对喜达屋网络未经授权的访问。万豪国际最近发现未经授权的第三方已复制并加密了其他信息，并试图进行删除等信息移出。2018年11月19日，万豪国际成功解密该等信息，并确定信息的内容来自喜达屋宾客预订数据库。

目前，万豪国际尚未完成对数据库中重复信息的识别，但初步数据库中包含在2018年9月10日或之前曾在喜达屋酒店预订的最多的5亿名客人的信息，这些客人中的有3.27亿人的信息包括如下信息的组合：姓名、邮寄地址、电话号码、电子邮件地址、护照号码、SPG俱乐部账户信息、出生日期、性别、到达与离开信息、预订日期和通信偏好。对于某些客人而言，信息还包括支付卡号和支付卡有效期。但支付卡号已通过高级加密标准（AES-128）加密，解密支付卡号码需要解锁两项密钥。目前万豪国际无法排除该第三方已经掌握这两项密钥。对于其他客人而言，信息仅限于姓名、酷客账户信息和如下数据：邮寄地址、电子邮件地址或其他信息等。

万豪国际集团已向相关执法部门报告此事件，并将继续配合执法部门的调查。我们开始通知相关监管机构。

万豪国际集团首席执行官辛安慧（Arne Sorenson）先生表示：“我们对此次事件表示深深的歉意。我们未能确保全球宾客应该享有的服务，也未能达到对自己的要求。我们正在积极采取行动，不遗余力地帮助受影响的宾客。我们将汲取事件中的教训，未来不断改进。”

“今天，万豪国际集团向全球宾客重申我们的承诺，我们上型力确保宾客能够通过专门的网站和电话服务中心获得有关其个人信息问题的回应，我们会继续全力支持执法部门的工作，并与权威安全技术专家合作进行改进。此外，我们正在投入必要的资源，进步加强喜达屋系统，加速提升网络安全的相关工作。”苏安慰（Arne Sorenson）先生补充道。

宾客支持
万豪国际已采取以下措施，协助宾客监测与保护个人信息：

专门网站及电话服务中心
•我们已建立专门网站(info.starwoodhotels.com)和电话服务中心（400-120-0845），回应宾客对此次事件的咨询。info.starwoodhotels.com 上也将实时更新宾客的常见问题。电话服务中心每周工作七天，以多种语言提供服务。电话服务中心起初可能会长时无量来电，希望您能耐心等候。

邮件通知
•11月30日起，万豪国际集团将向预留了邮箱信息并受此事件影响的喜达屋宾客发送电子邮件，告知此次事件的情况。

免费注册WebWatcher
•万豪国际将为宾客提供一年免费注册WebWatcher监控工具的机会。WebWatcher将监测涉及共享个人信息的网站，如发现宾客的任何个人信息泄露将会向宾客发出风险提示。由于相关法规以及其他原因，WebWatcher或类似产品尚未提供所有市场提供。如欲应用WebWatcher，请前往info.starwoodhotels.com，若该服务国家和地区在列，请注册使用。

万豪国际正向美国证券交易委员会提供8-K报告，其中将有本新闻稿及与本事件相关的其他信息。

*喜达屋旗下品牌包括：W 酒店 (W Hotels)、瑞吉酒店 (St. Regis)、喜来登酒店与度假村 (Sheraton Hotels & Resorts)、威斯汀酒店与度假村(Westin Hotels & Resorts)、源宿酒店 (Element Hotels)、雅乐轩酒店 (Aloft Hotels)、豪华精选酒店 (The Luxury Collection)、臻品之选酒店 (Tribute Portfolio)、艾美酒店与度假村(Le Méridien Hotels & Resorts)、福朋喜来登酒店 (Four Points by Sheraton) 及设计酒店 (Design Hotels)。喜达屋分时度假酒店亦包括其中。

新闻垂询：

万豪国际集团公关部
Media@marriott.com

在 5 亿人次中，有大约 3.27 亿人次的姓名、邮寄地址、电话号码、电子邮件地址、护照号码、账户信息、出生日期、性别以及到达和离开酒店的信息已被泄露。

万豪方面还补充，可能泄露的还包括加密的信用卡信息，且不能排除加密密匙同时被盗的可能性。目前，受此事影响，万豪股价在周五盘前下跌 4.22%。

有网友评论

这是泄露了个干干净净↓

华住旗下酒店大规模数据泄露

事实上，酒店泄露客户信息在国内早就拉响了警报。2018 年就发生不止一起大规模酒店客户数据泄露事件。

今年 8 月底，华住旗下多家连锁酒店开房信息的数据被人在暗网出售，标价 8 个比特币，或 520 门罗币，约等于人民币 37 万元。被售卖的数据共为三部分，分别为华住官网注册资料信息，共 53G，约 1.23 亿条记录；酒店入住登记身份信息资料，共 22.3G，约 1.3 亿人身份证信息；酒店开房记录信息资料，共 66.2G，约 2.4 亿条记录。

酒店信息安全不亚于卫生安全

针对此次事件，某网发表的评论文章中指出：

酒店数据库的脆弱，只是当下个人数据等隐私信息保护不力的冰山一角，或者说它并非是一种特殊现象。很明显，个人信息普遍被数据化又同时泄露常态化的环境中，拿什么捍卫社会的信息安全感，已经不只是一行一业所面临的问题，它需要系统性的法律完善和集体救赎。当前酒店领域的数据库保护系统，应全面升级。其重要性和迫切性，甚至可能超过卫生问题的解决。

一年内发生多起大规模酒店客户数据泄露的惨重事件，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。小亿也想说，如果一切都没有发生，小亿一定把最牛的亿赛通数据加密产品推荐给他们，那么，就算数据库被黑客入侵，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。但是，没有如果，小亿只想说，就算没有如果，现在醒悟也不晚。无论企业或个人都要意识到数据安全防护的重要性，一定要提前采用数据安全防护措施。

惊！勒索病毒不要比特币，改“微信支付”？

近两年来勒索病毒的频繁爆发总是能让各大 BOSS 捶胸顿足，360 度无死角各种防，还是防不过这个互联网时代的攻击套路。只要勒索病毒出现，就会刷爆朋友圈。

近日，又出现新型勒索病毒，但是此次不要比特币，而是绑定微信二维码支付赎金。在短时间的快速传播下，感染病毒的电脑数量越来越多。团伙入侵并利用豆瓣的 C&C 服务器，除了锁死受害者文件勒索赎金，还大肆偷窃支付宝等密码。

据了解，该病毒（Ransom/Bcrypt）为新型勒索病毒，入侵电脑运行后，会加密用户文件，但不收取比特币，而是要求受害者扫描弹出的微信二维码支付 110 元赎金，获得解密钥匙，这也是国内首次出现要求微信支付赎金的勒索病毒。有不少论坛、微博等网友遭遇该勒索病毒的攻击，而该微信二维码以及服务器均已不可使用，这意味着，被病毒感染的用户已经没法支付赎金获得密钥解密。

尽管此次勒索的“水平”不怎么高，但是还是造成了不少麻烦。病毒团伙巧妙地利用“供应链污染”的方式进行传播，已有超过两万用户感染该病毒，而且感染范围还在扩大；该病毒会窃取用户的各类账户密码这才是最大的隐患，网友们即使在解密后，也需更改自己的涉网账户密码，防患于未然！

每次在事件爆发后，很多企业也针对勒索病毒给出了各种应对招数，没错，是管用，但是面对病毒的突然袭击，总是会措手不及，事后的补救也无法挽回损失，为此，中国数据安全防护专家 --- 亿赛通提出应该从根源彻底隔绝各种攻击软件。

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，亿赛通十五年对客户的数据进行安全防护，而今，面对反其道的攻击事件，通过自主研发的勒索病毒防护卫士，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。

欲了解勒索病毒防护卫士详情，请咨询服务热线：400-898-1617

年终盘点 | 2018 年引人注目的十大数据泄露事件，信息安全已危及全球！

2018 年数据安全问题一直备受社会关注，勒索病毒和泄露事件的披露始终占据媒体的头条榜首。据悉，仅仅 2018 年上半年全球数据泄露数量高达 26 亿条，可见，在大数据、互联网迅速发展的全球大背景下，为人类带来无限发展机遇的同时却也催生了大量的信息泄露事件，这些触目惊心的数据让世界警惕信息安全已经危及全球，接下来，亿赛通带您一起回顾 2018 最受关注的数据泄露大事件……

事件一 Facebook：8700 万用户数据泄露

2018 年 3 月 Facebook 公开承认剑桥分析公司不正当使用了 8700 万未经授权的用户私人信息，这也遭到了国外网友的痛斥。今年 9 月份，Facebook 再次通告，黑客利用控制的 40 万个账户获得了 3000 万 Facebook 用户账号的信息。他们可以在不输入密码的情况下，随意登陆这些用户的个人主页，任意拿走想要的数据等。Facebook 爆发的隐私泄露危机至今，公司股价一度蒸发 590 亿美元。

事件二 Under Armour：1.5 亿用户信息泄露

2018 年 3 月，运动品牌 Under Armour 对外表示，旗下健身应用 MyFitnessPal 因存在数据漏洞而遭到黑客攻击，一共有 1.5 亿用户的数据被泄露，这些数据中包含了用户名、电子邮件地址和密码等，不过官方强调，泄密数据并不包含驾驶证号、信用卡号、身份信息等更私密信息。MyFitnessPal 在北美地区颇受欢迎，用户数量最高峰时接近 2 亿，当传出有 1.5 亿用户信息被黑客窃取后，Under Armour 官方表示，立刻要求 MyFitnessPal 用户更改密码。

事件三 Panera Bread：3700 万用户信息泄露

2018 年 4 月，美国面包连锁店 Panerabread 表示，旗下网站 panerabread.com 泄露了 3700 万用户信息，而更可怕的是，在官方没有给出公告前，这种泄露信息行为已经持续了超过 8 个月。随后，安全机构 KrebsOnSecurity 表示，他们在早在 2017 年 8 月 2 日就曾发现了 Panerabread 网站的漏洞，告知对方后并没有进行及时修复，所以造成的结果就是严重的。

事件四 MyHeritage：9200 万用户信息泄露

MyHeritage 是一个家庭基因和 DNA 检测的网站，用户信息中存储不但有私人信息，甚至还有个人的 DNA 测试结果。2018 年 6 月，MyHeritage 给出公告称，网站服务器被攻击，攻击者从中截取了超过 9200 万用户信息，其中包含了电子邮件和 hash 密码。不过 MyHeritag 还表示，用户帐户是安全的，因为密码是使用每个用户唯一的加密密钥进行 hash 处理的，为了彻底解决这种攻击，最终网站启用了双因子身份验证 (2FA) 功能，即使黑客设法解密 hash 密码，如果没有第二步验证码，第一步的破解也将毫无用处。

事件五 AcFun：900 万条用户数据泄露

2018 年 6 月，AcFun 弹幕视频网发出公告称，他们有 800-1000 万左右的用户数据被黑客窃取。黑客攻击 A 站后窃取的用户信息，很快就放在了暗网售卖，并喊出 900 万条用户数据，售价 40 万人民币。如果购买者对信息真实性质疑，那么可以随机抽取测试，此事对用户造成了不小的影响。其实早在今年 3 月份，暗网论坛中就有人公开出售 AcFun 的一手用户数据，数量高达 800 万条，而价格仅为 12000 元，平均 1 元能买到 800 条。

事件六 前程无忧：195 万条个人求职简历泄露

2018 年 6 月，有人在暗网开始叫卖招聘网站前程无忧用户信息，其中涉及 195 万用户求职简历，随后前程无忧方面确认部分用户账户密码被撞库。为了证实泄露数据的真实性，前程无忧方面还进行了一定的测试，结果发现信息是真实可靠的，不过官方强调，数据中绝大部分来自于一些邮箱泄露的账户密码 ,且都是在 2013 年之前注册。对此前程无忧强调，出现这样的情况并非拖库，而是恶意用户通过这些已泄露的邮箱账户及密码，对相应的站点进行登录匹配，然后蓄意倒卖。

事件七 圆通：10 亿条用户信息数据被出售

2018 年 6 月，某用户公然在暗网兜售圆通 10 亿条快递数据，按照卖家的说法，这些是 2014 年下旬的数据，数据信息包括寄 (收) 件人姓名，电话，地址等信息，都是圆通内部人士批量出售而来 (只要快递单信息进入电脑他们就可以获取)。随后，有网友验证了其中一部分数据，发现所购“单号”中，姓名、电话、住址等信息均属实。按照当时售价来说，用户只要花 430 元人民币即可购买到 100 万条圆通快递的个人用户信息 (10 亿条数据 1 比特币)，而 10 亿条数据则需要约 43000 元人民币。能够泄漏如此多用户信息，且准确率如此之高，外界普遍认为来源是圆通内部级别较高的工作人员。

事件八 华住旗下多个连锁酒店：2.4 亿入住记录泄露

2018 年 8 月，网上突然出现华住旗下多个连锁酒店入住信息数据售卖的行为，数据涉及 5 亿条的用户个人信息及入住记录，而这些泄密的数据中，包含的不少私密信息，比如身份证号、家庭住址、银行卡号等等。经过排查泄露的用户数据多达 2.4 亿条 (66.2G)，这是酒店入住的记录 ,还有约 1.3 亿条入住登记身份信息 (共 22.3G) 和约 1.23 亿条官网注册资料 (共 53G)，而这些数据中把用户的姓名、银行卡号、手机号、邮箱、开房人、家庭住址等等核心信息全部泄露出来。

事件九 顺丰：3 亿条用户信息数据被出售

2018 年 8 月底，某用户在暗网上公然售卖顺丰快递数据，其中牵扯到了 3 亿用户数据信息，售价 2 个比特币，而这些信息中包含了寄件人、收件人的姓名、地址、电话等，为了证明数据的准确性，购买者可以选择先“验货”，验货数据量 10 万条，验货费用 0.01 个比特币。从交易情况来看，至少有超过 90 万条疑似顺丰快递用户个人信息流向了市场。从一些匿名测试用户反馈的数据来看，随机抽选 50 个，准确率在 90% 以上。

事件十　万豪喜达屋：5 亿客户的用户信息泄露

2018 年 11 月，万豪对外发出公告称，旗下喜达屋酒店预订系统 2014 年起遭网络“黑客”入侵，泄露大约 5 亿客户的用户信息。经过复查后得知，万豪泄露的这 5 亿用户信息中，用户的姓名、住址、电话号码、电子邮件地址、护照号码、信用卡等所有核心的信息统统被泄露出去，性质十分恶劣。美国诉讼集团代表众多消费者向万豪提起诉讼，索赔金额高达 125 亿美元。

数据安全任重道远，如何在互联网发展的大潮下同时确保信息安全，已经成为全世界各行业普遍关注的焦点问题。亿赛通作为中国数据安全防护专家提醒大家，无论企业或个人一定要意识到数据安全保护的重要性，提早采取防护措施。未雨绸缪，防患未然！

亿赛通综合防护解决方案补齐设计制造行业数据安全短板

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。

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。

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。

设计制造数据安全综合解决方案

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，凡是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。

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。

部分经典客户

1、京东方科技集团股份有限公司
2、中国国际海运集装箱（集团）股份有限公司
3、南通中集罐式储运设备制造有限公司
4、ABB（中国）有限公司
5、中国石油工程建设公司
6、佳通轮胎（中国）投资有限公司
7、哈电集团（秦皇岛）重型装备有限公司
8、鞍山钢铁集团公司
9、江苏沙钢集团淮钢特钢股份有限公司
10、招商局重工（江苏）有限公司
11、华晨汽车集团控股有限公司
12、华晨宝马汽车有限公司
13、广州本田汽车有限公司
14、东风悦达起亚
15、长城汽车股份有限公司
16、中国北车股份有限公司大连电力牵引研发中心
17、海马汽车有限公司
18、河南奔马股份有限公司
19、东风汽车电子有限公司
20、正泰集团
……

典型案例 TYPICAL CASES

亿赛通与信大捷安达成战略合作，为企业数据安全上一把安心锁

郑州信大捷安信息技术股份有限公司（简称“信大捷安”）成立于 2004 年，是一家专业从事安全芯片创新设计、云安全服务平台研发，提供移动 • 物联安全服务保障的高新技术企业。企业作为公安部准入公安移动安全接入的民营企业，先后参与了 9·3 阅兵、上合峰会、河南省人大会议、G20 杭州峰会、河南省党代会等重大活动的移动通信安全保障工作，并获得了各方的高度肯定。

需求背景

信大捷安作为一家移动信息安全企业，一直非常重视企业内部数据核心资产的共享利用、版本归档、以及安全保护。2017 年初在全公司范围内实施了内外网隔离，员工使用两台 PC 进行办公，防止内网研发数据泄密。不过最终隔离效果并不理想，决定选用专业数据安全厂商进行核心数据加密防护，经过长达半年的测试和选型，最终选择亿赛通作为其核心代码数据保驾护航。

解决方案

亿赛通安全产品具体帮信大捷安实现了如下功能：

1.所有研发终端（ windows、linux ）产生的代码及文档，强制加密保护，内部透明使用；

2. 由终端提交到 SVN，GIT 服务器的代码及文档，自动上传解密。SVN,GIT 服务器下载到终端的代码，自动下载加密；

3. 未安装及非授权使用客户端的用户无法访问 SVN、GIT 代码系统。

项目成果

亿赛通针对信大捷安业务模式设计的特色安全保护方案，为公司提供了安全屏障，也为用户资料提供了安全保护，更让信大捷安的整体安全提升了一个台阶。亿赛通产品的稳定性、安全性以及高效的售后服务，也获得高度的认可。