



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

数据库安全系统（DAS）产品线

全新上线



数据库安全防护有“他”就够了

信息安防不到位，国泰航空接 50 万英镑罚单



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 《亿赛通三月刊》上线，独特视角解析数据库安全

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 数据库安全防护有“他”就够了

16/17 上海某高校 DAS 虚拟化案例

18/19 你所忽视的数据库安全

20/21 安全力即企业生产力，如何保障企业远程办公数据安全？

亿赛通小贴士 ESAFENET PROMPT

22/23 信息化战“疫”进入关键时期，信息泄露该如何管控？

24/25 信息安防不到位，国泰航空接 50 万英镑罚单

26/27 微博用户泄露引热议，急需为数据筑好最后一道防线

28/29 商场如战场，看《完美关系》你才不是单纯的在看一部职场剧

典型案例 TYPICAL CASES

30/31 中国移动通信集团公司

32/33 中国联合通信有限公司



《亿赛通三月刊》上线， 独特视角解析数据库安全

纵观全球安全态势，数据库持续成为数据窃取者的主要目标之一，而大数据平台的建立与发展更加剧了数据库安全风险。对全球数据库安全风险来说，数据泄露或篡改风险可能导致企业面临无法通过审计导致的资产负债、监管罚款、盈利受损或客户投诉等诸多负面影响。

在现实情况下，引起数据库安全事件频发的原因较多，美国某公司就“核心数据是如何丢失的”做过一次全面的市场调查，75%的数据丢失情况是由于数据库漏洞造成的。另外，数据库安全配置管理措施不够、非结构化数据缺乏安全保护措施是造成数据库安全事件频发的主要原因。

亿赛通着重关注数据库安全，特成立数据库安全产品线，发布数据库审计系统、数据库防火墙及数据脱敏三大产品，让企业实现全面、无感、高效的数据库安全防护……

国内



1、微博泄露 5 亿用户数据？实测：12 元买 201 条用户信息

摘要：近日微博被爆发生用户数据泄露事件。据调查发现，在一些外网交易平台上确实出现了相关的数据买卖，只要缴费即可通过微博账号查询到用户的手机号码及其他更详细个人私密信息。对于这次用户数据泄露，微博方面公开回应称，此次数据泄露应该追溯到 2018 年底。当时，有用户利用微博相关接口通过手机批量上传通讯录，匹配出几百万个账号昵称，再加上通过其他渠道获取的信息一起对外出售。

2、交行分行员工盗取主管账号，利用贷款业务漏洞骗贷 1900 万



摘要：日前，临汾市中院披露一份刑事判决书显示，交通银行临汾分行员工与人里应外合骗取贷款 1900 余万元。梁某芳在交通银行临汾分行担任零贷管理部客户经理协理期间，与李某及其下属 3 名中介人向社会不符合办理贷款条件的客户收取贷款资料，利用梁某芳的职务便利，通过欺骗和盗用该行客户经理和支行行长等人的贷款系统账号密码，擅自利用已办“e 贷通 2.0”业务的 7 家单位名义，非法添加贷款资料，致使交通银行受理 153 人的贷款申请，共计发放 1903.7 万元贷款。

3、工信部：# 健康码要防止数据泄露和滥用



摘要：针对健康码的使用，工信部装备工业一司司长在新闻发布会上表示，阿里、腾讯等科技企业也及时开发了一些小程序，推出疫情防控的“健康码”。这些服务都为复工复产提供了方便快捷的“通行证”。作为监管部门，在数据分析使用的过程中，依据个人信息保护的有关法律法规，严格落实数据安全和个人信息保护的有关措施，切实加强监管，防范数据的泄露、数据的滥用等违规行为。

4、线上学习隐私遭泄露，上海 50 万余条学生信息被倒卖

摘要：近日，上海虹口法院审理一起公民个人信息被交换、倒卖案。三名犯罪嫌疑人都是教育培训机构从业人员，他们倒卖 50 余万条学生个人信息，涉及学籍号、学校、年级、户籍、家庭住址、家长姓名电话等。最终，三人被判处 2 到 3 年不等有期徒刑，并处罚金。



5、黑猫投诉：淘手游泄露个人隐私导致账号被盗

摘要：消费者“匿名”向黑猫投诉平台反映：“我把九游账号挂淘手游卖号。有人在淘手游通过商品给我发信息说他才是号的主人，然后连着好几天给我发信息，然后他就得到了我的手机号码。而我的手机号只有淘手游才有。紧接着那个人就冒充九游给我发信息说我的账号正在被申诉，之后开始不停的发验证码轰炸我的手机最后验证码被破解。密保手机邮箱都换绑了。我申诉找回时账号里面游戏数据没有了，我询问九游客服，客服说被人利用交易猫转移到另一个账号了。我联系淘手游客服，淘手游的一个男客服态度差的要命，代理不搭。泄露我个人隐私，导致账号被盗。我要求赔偿！！！”



6、微信用户注意：这3个“功能”可能导致隐私泄露



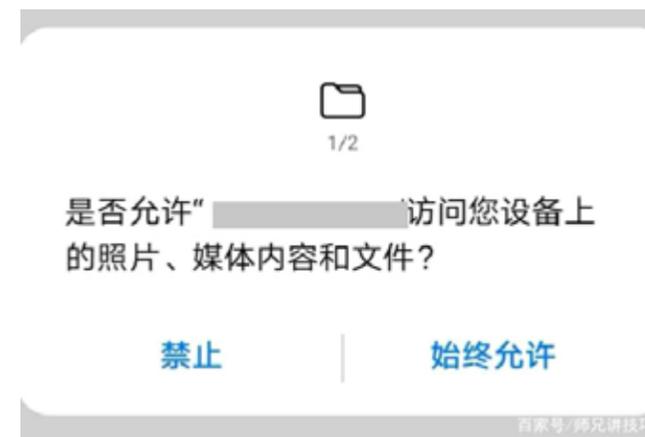
摘要：微信用户一定要注意：这3个“功能”需要注意：1、手机都会设置屏幕锁，防止被偷后，手机隐私泄露、同时还可能造成钱财损失，但是对于微信接收到的信息，还依旧会在屏幕中，显示发信人、及其消息；2、朋友圈的权限关闭“允许陌生人查看十条朋友圈”；3、“授权管理”设置，微信小程序游戏、进入一些网络、链接，都会弹出授权管理的消息。

7、百度网盘被曝用户隐私文件被泄露，在进行文件分享的时候要注意了



摘要：近日，百度网盘又双叒因为隐私问题受到关注，起因是近期有网友发文称，百度网盘的私密文件存在被第三方引擎抓取并被公开泄露的隐患。据传，此次被曝出的隐私文件泄露不仅包括日常的电话目录以及文件资料，甚至还有证件信息以及个人私密照。而百度网盘官方给出的解决方案是设置分享文件的有效期以及提取码。

8、安装手机 APP 要求允许访问手机文件，APP 会泄露用户个人隐私吗？



摘要：安卓系统的手机容易出现这种问题，之前安卓对于手机用户的个人隐私不够重视，开源的系统，每家手机厂商对于手机系统的而优化各不相同。之前手机应用一般不会出现访问权限确认的弹框，只要在开发软件的时候，在清单文件上注册相关的权限，一般的应用都可以访问手机中的文件等，不需要用户点击确认同意。

9、工信部：截止目前通信大数据分析无个人信息泄露情况



摘要：从3月6日开始，“通信大数据行程卡”上线了境外到访地的查询功能，可对手机用户前14天到访的境外国家或者地区的信息进行查验。3月25日，信息通信管理局局长韩夏表明，目前，累计的查询量已经超过了4.5亿次。行程卡不收集用户身份证号码、家庭住址等信息，而且详细的查询结果，只显示在本人的手机上。并且行程卡是通过通信网络的数据来获取地址信息，不需要个人填报。

10、京东捅了大篓子！女孩表示：看到京东就来气！



摘要：近日，洛阳的王女士在3月19日中午接到一个内蒙古电话，自称是京东金融客服，准确说出了王女士在京东平台的详细信息，王女士对这个所谓的京东金融客服深信不疑，于是就按照电话那头的指示，把京东白条里的额度全部借出来，并打到了骗子的账户上，配合他注销额度，回收到他们公司。王女士表示：“自2015年注册京东账号，没有使用过白条，也没有在任何地方填过京东账号信息”。王女士希望京东能作出回应，为什么这个骗子知道了他的账户信息，并希望京东能作出调查，公司是如何保护用户信息的。

1、加拿大最大的通信公司发生数据泄露



摘要：加拿大ISP Rogers通信公司在官方网站上发布的一份数据泄露通知，Rogers表示，一个包含客户信息的供应商数据库处于不安全的状态，公开暴露在互联网上。此次数据泄露泄露了以下客户信息：地址、帐号、电子邮件地址、电话号码。

2、冠状病毒疫情爆发期间，黑客持续攻击美国公共卫生部门



摘要：近日新型冠状病毒（COVID-19）在美国大爆发，同期，美国重要公共卫生部门遭遇严重网络攻击。截至目前出现了多起黑客事件，旨在减慢该部门网络系统应对疫情的运行速度。在美国安全官员意识到，有人入侵网络系统并且传播有关冠状病毒的虚假信息后，白宫国家安全委员会连夜发布了预警推文表示，在COVID-19响应下网络钓鱼攻击、凭据盗窃、比特币和金融欺诈、勒索软件活动等会持续增加。

3、一波未平一波又起：公主邮轮 承认公司存在数据泄露问题



摘要：据外媒报道，在两艘邮轮爆发了新冠病毒后被迫在全球范围内停止运营的 Princess Cruises（公主邮轮）目前已证实存在数据泄露问题。这份发布在其网站上的通知实际上是在3月初发布的。该份通知称，公司在2019年4月至7月的4个月时间内发现了大量未经授权的电子邮件账号登入，其中一些包含了职工、邮轮工作人员和客人的个人信息。

4、研究发现数以千计的指纹文件 暴露在不安全的数据库中



摘要：一个包含约76000个独特指纹记录的网络服务器被暴露在互联网上，这些不安全的指纹数据，以及员工的电子邮件地址和电话号码，都是由巴西公司 Antheus Tecnologia 收集，该数据库包含近230万个数据点，其中大部分是服务器访问日志。

5、英国多个火车站免费 Wi-Fi 暴露用户数据



摘要：Security Discovery 的一名研究人员发现，与英国多个火车站的免费 Wi-Fi 热点连接的用户数据已存储在非密码保护的数据库中。该数据库包含1.46亿条记录，其中包括电子邮件地址，年龄范围，旅行原因，设备数据和其他日志。

6、国泰航空因 2018 数据泄露事件 被英国 ICO 罚款 50 万英镑



摘要：因2018年在欧盟《通用数据保护条例》（GDPR）生效后发生的一次数据意外泄露事件，国泰航空已被英国数据监管机构处以50万英镑的罚款。据悉，本次漏洞暴露了全球约940万客户的个人详细信息，且其中有111578名来自英国。经过数月的调查，信息专员办公室（ICO）正式宣布了这项惩罚。

7、移动营销平台 Sensor Tower 被爆秘密收集数百万用户数据



摘要：知名 APP 分析平台 Sensor Tower 利用 VPN 应用和去广告应用程序，来收集 Android 和 iOS 平台数百万用户的数据。这些应用程序的全球下载量已超过 3500 万次，但是在应用描述中并没有透露和 Sensor Tower 有联系，或者会收集用户数据给该公司。

8、美国 AI 公司伪造 APP 获取用户隐私数据，Facebook、微博均中招



摘要：人工智能公司 Banjo 秘密创建了一家名为 Pink Unicorn Labs 的公司，借以后者的名义开发多个 Android 和 iOS 应用程序获取社交媒体资源。Pink Unicorn Labs 开发的 APP 包括 One Direction Fan APP、EDM Fan APP、Formula Racing APP。从程序代码可知，被获取资源的社交媒体包括新浪微博、Facebook、Twitter、Instagram、VK（俄罗斯社交媒体）、FourSquare、Google Plus 等。

9、特斯拉、波音、SpaceX 供应商遭勒索软件攻击



摘要：近日，总部位于科罗拉多州丹佛的精密零件制造商 Visser Precision 遭受勒索软件攻击。由于是特斯拉、波音、洛克希德·马丁公司和 SpaceX 等行业巨头的零件供应商，因此该事件引发了不小的震动。黑客威胁说，如果 Visser 不支付赎金，它们就会泄漏与这些公司有关的敏感文件，并且已经泄漏了 Visser Precision 与特斯拉和 SpaceX 签署的保密协议。

10、财富 500 强公司 EMCOR 遭 Ryuk 勒索软件攻击



摘要：从事工程和工业建筑服务的 EMCOR Group 近日披露了发生在 2 月份的勒索软件攻击事件，该事件导致其部分 IT 系统瘫痪。该事件发生在 2 月 15 日，已确定所感染的勒索软件属于 Ryuk 家族。目前攻击的详细信息和后果尚未公开，但 EMCOR 表示，并非所有系统都受到影响，只有“某些 IT 系统”受到影响，因此该公司迅速关闭以控制感染。该公司表示正在恢复服务，但未具体说明是否支付了赎金要求或是否正在从备份中恢复。

数据库安全防护有“他”就够了

数据，这个时代的巨量产物，珍贵而无价。越来越多的企业和政府部门将安全的关注重点从传统的边界安全转移到数据安全，保存核心数据资产的数据库系统，毫无疑问的成为防护的关键。数据库防火墙，作为数据库重要的防御工事，自然获得了更多的关注，近年已越来越多的应用在数据库安全防护中。所谓能力越大、责任越大，这句话用来形容数据库防火墙也许应该反过来理解，因其肩负数据库防护重任，社会对于“他”的要求也更加严苛。



亿赛通数据库审计系统 - 防护系列（简称 DAS-FW）是一款基于数据库协议分析与控制技术的数据库安全防护系统。DAS-FW 基于主动防御机制，实现数据库的访问行为控制、危险操作阻断、可疑行为审计。DAS-FW 是一款集数据库 IPS、IDS 和审计功能为一体的综合安全产品。

DAS-FW 四大产品价值

访问权限精细控制

通过分析数据库流量数据，获取权限控制所需关键信息，对相应数据库请求行为进行放行或阻断，达到第三方权限控制的目的。

防止内外高危操作

通过 SQL 注入特征库捕获和阻断 SQL 注入行为；通过限定更新和删除影响行、限定无 Where 的更新和删除操作、限定 drop、truncate 等高危操作避免大规模损失。

防止敏感数据泄漏

限定数据查询和下载数量、限定敏感数据访问的用

户、地点和时间。

审计追踪非法行为

提供对所有数据访问行为的记录，对风险行为进行 SysLog、邮件、短信等方式的告警，提供事后追踪分析工具。

DAS-FW 独特技术优势

精细数据库权限控制

针对数据库表级别提供精细化的访问权限控制，授权对象除了基本的数据库用户以外，还可以对数据库连接客户端进行权限控制，同时可设置权限规则的时间周期及有效时间范围。

全面数据库入侵阻断

提供全面的数据库攻击行为检测和阻断技术，包括：SQL 注入禁止技术、虚拟补丁技术、高危访问控制技术、返回行超标禁止技术、SQL 语句模板技术。

场景化安全策略设置

系统按照不同的防护场景提供预定义策略。

分布式部署集中管理

除了传统的单机部署模式，还支持分布式部署和集中管理模式，可统一下发策略、统一管理、统一展现。

DAS-FW 九大核心功能

- SQL 注入行为检测阻断：通过对 SQL 语句进行注入特征描述，完成对 SQL 注入行为的检测和阻断；
- 防止敏感数据泄漏篡改：针对不同的数据库用户，提供敏感表的操作权限、访问行数和影响行数的控制，以及限制 NO WHERE 查询和更新，从而避免大规模数据泄露和篡改；
- 支持 SQL 语句黑白名单：通过学习模式以及 SQL 语法分析构建动态模型，形成 SQL 白名单和 SQL 黑名单，对符合 SQL 白名单语句放行，对符合 SQL 黑名单特征语句阻断；
- 提供精细访问权限管理：对于数据库用户提供比 DBMS 系统更详细的虚拟权限控制。控制策略包括：用户、终端、对象、时间等元素；
- 支持风险行为控制审计：对数据库访问行为阻断所采取的控制行为，包括：“中断会话”和“拦截语句”两种方式；
- 多种安全策略模型支持：支持许可模型和禁止模型；
- 数据应用访问智能建模：提供学习期以完成对应用访问数据库行为的建模，学习期提供两种模式：初始化模式和完善模式；
- 全面精细审计控制分析：提供全面详细审计记录，告警审计和会话事件记录，并在此基础上实现了内容丰富的审计浏览、访问分析和问题追踪，提供实时访问首页统计图；

- 系统高可用性设计保障：采用高可靠性设计，支持多种高可靠性技术，包括网络 bypass 和双机热备等，充分保障系统运行稳定可靠，对客户现网和业务零影响。

DAS-FW 专业技术，官方认可

亿赛通数据库审计系统 - 防护系列顺利通过国家版权局的检测，取得《中华人民共和国国家版权局计算机软件著作权登记证书》。



用户对数据库防火墙产品的高要求，在传统的防护体系中，补充了对数据库防护这一重要环节，实现了“术业有专攻”的数据库安全防护系统。今天，作为中国数据安全防护专家，亿赛通推出数据库防火墙，保证业务系统在安全状态下正常、高效的运行，为用户提供了安全、无感的体验效果。

上海某高校 DAS 虚拟化案例

DAS 产品线：苏仕红

一、项目背景

上海某高校，是中华人民共和国教育部直属的一所以经济管理学科为主，经、管、法、文、理、哲等多学科协调发展的研究型重点大学；是国家“211工程”、“985工程优势学科创新平台”重点建设高校，国家“双一流”世界一流学科建设高校；入选“国家经济学基础人才培养基地”、“国家海外高层次人才创新创业基地”、“教育部人文社会科学重点研究基地”、“卓越法律人才教育培养计划”、“国家建设高水平大学公派研究生项目”、“中国政府奖学金来华留学生接收院校”、“海外高层次人才引进计划”、“111计划”；是全国首批博士、硕士、学士学位授予单位之一；由教育部、财政部和上海市人民政府三方共建。

二、核心应用场景：

场景 1、审计发现成绩被非法篡改的问题：

审计发现非法用户在非工作时间段修改考生成绩等敏感数据；

场景 2、审计发现非法约课问题：

审计发现课程预约系统中学院热门课程被大量预约后，多次出现取消约课后被另一用户立即补约，疑似利用课程预约进行牟利的问题；

场景 3、审计发现系统疑似盗用问题：

审计发现固定 ip 地址未使用常用账号登陆系统，疑似账号盗用问题。

三、项目目标

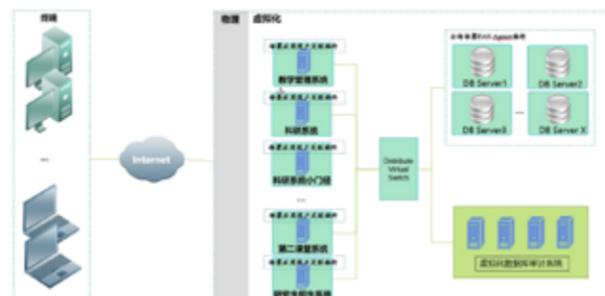
1、快速定位到真正的用户信息

院校全部应用系统采用统一身份认证，对院校门户网站以及下属分院门户和其他业务系统进行统一登陆控制和权限管理，要求 DAS 能在统身份认证环境下快速、有效定位应用用户和 SQL 关联会话。同时针对应用用户，可获取如浏览器、终端操作系统等更为详细的审计信息；

2、审计虚拟化、集中管理化

目前学院部分业务系统已经实现虚拟化部署，后续全院业务系统将全部完成虚拟化部署的过渡。要求 DAS 可以支持虚拟化环境，同时要求具备集中化管理能力，实现后续 DAS 的平滑扩容和保证审计日志留存周期超过一年；

四、部署图



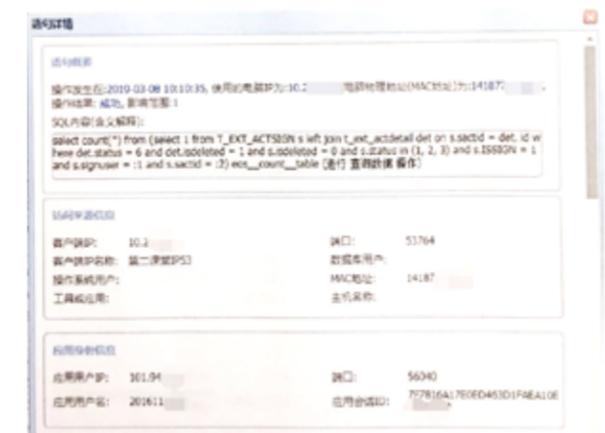
五、核心价值

1、统一身份认证下的应用用户关联审计

采用统一认证方式管理门户网站与各子业务系统时，用户只需一次登陆认证后，访问院校其他子业务系统将无需进行二

次认证。而常规应用用户关联审计只能针对门户网站进行用户关联审计，子业务系统由于免认证机制导致应用关联插件无法正常获取登陆信息，造成应用关联审计下沉失败，用户信息缺失，存在重大审计漏洞。亿赛通数据库审计系统通过与统一身份认证系统对接，以及与子业务系统登陆标签进行绑定和信息获取，进行主动关联绑定完成应用用户关联审计下沉，实现在统一身份认证环境下快速、有效、无误的应用关联审计，满足了客户在三个核心审计场景的要求。

如下为实际部署运用界面截图：



2、虚拟化分布式部署

分布式部署将 DAS 的审计引擎及管理中心进行分离，管理中心统一负责亿赛通数据库审计日志数据的存储和分析，审计引擎负责 SQL 会话与相关信息的采集、解析和审计，一个审计中心可管理多个审计引擎。满足了用户对亿赛通数据库审计的集中化管理要求，减轻了用户后续运维压力，同时也兼顾了后续 DAS 平滑扩容和审计日志超长留存的要求。

你所忽视的数据库安全

售前技术部：梁伟

在互联互通的世界里，保护关键信息与数据变得愈发重要。在保证可用性与运行效率的前提下，需要确保数据中心的实体基础设施能够迅速适应变化，满足未来物联网以及在云端与边缘增长的需求。因此数据库的运行安全、系统安全越来越受到企业的关注。

数据库面临的安全威胁：

数据库安全包含两层含义：第一层是指系统运行安全，系统运行安全通常受到的威胁如下，一些网络不法分子通过网络，局域网等途径通过入侵电脑使系统无法正常启动，或超负荷让机器运行大量算法等破坏性活动；第二层是指系统信息安全，系统安全通常受到的威胁如下，黑客对数据库入侵，并盗取想要的资料。数据库系统的安全特性主要是针对数据而言的，包括数据独立性、数据安全性、数据完整性、并发控制、故障恢复等几个方面。

据 Verizon 的数据泄露调查分析报告和对发生的信息安全事件技术分析，总结出信息泄露呈现几个趋势：

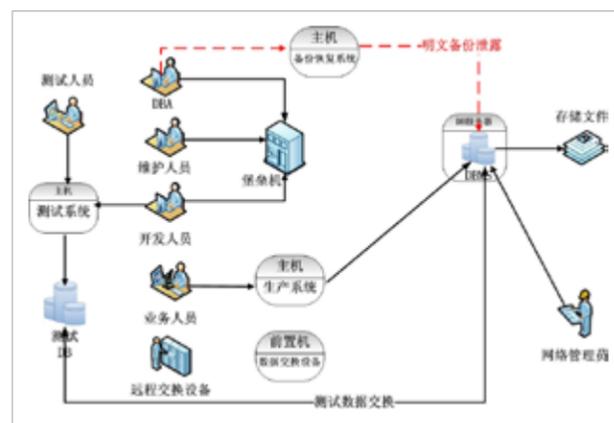


1、黑客通过 B/S 应用，以 Web 服务器为跳板，窃取数据库中数据；传统解决方案对应用访问和数据库访问协议没有任何控制能力，比如 :SQL 注入就是一个典型的数据库黑客攻击手段。

2、数据泄露常常发生在内部，大量的运维人员直接接触敏感数据，传统以防外为主的网络安全解决方案失去了用武之地。

3、业务系统风险，业务系统在调试过程中测试数据库数据泄露，导致大量未脱敏或半脱敏敏感信息泄露。

数据库成为了这些泄露事件的主角，这与传统的安全建设中忽略了数据库安全问题有关，在传统的信息安全防护体系中数据库处于被保护的核心位置，不易被外部黑客攻击，同时数据库自身已经具备强大安全措施，表面上看足够安全，但这种传统安全防御的思路，存在致命的缺陷。



(传统方案的缺陷)

防护产品建议：

基于数据安全保护设计

基于数据库保护设计，满足商业数据保护与合规建设需求；

灵活的产品组合使用

根据客户实际需求，产品可独立使用或组合使用，产品功能使用更灵活；

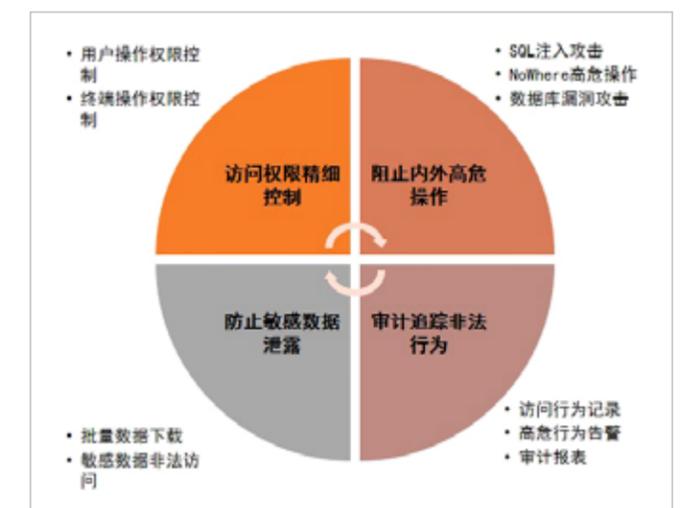
可视化的安全管理

采用数据可视化技术，对数据库状态，访问情况，操作风险做可视化处理，提升数据保护工作效率；

采用大数据架构设计

采用大数据架构，充分利用硬件性能，数据处理效率高，全量数据检索更快。

关注的防护功能：



安全力即企业生产力，如何保障企业远程办公数据安全？



近期，由突发事件导致的企业运营方式调整，企业已在家办公多时，既维护了企业的正常运转，又保障了员工的安全。可同时，与之相对应的却是安全问题频出，不法分子利用此次危机对企业进行攻击，窃取机密等。与在公司有专业的网络管理员不同，员工在家办公的网络和工具要更开放、更多样，因此产生的安全问题也往往更容易被忽略。

远程办公看似外表平静，实则对数据的安全威胁暗流涌动。这段时间内，多次发生以各类疫情相关文件为名，借全国人民对疫情的关注度，制作并传播远控木马

病毒。既具有高迷惑性且紧跟疫情热点，吸引不明用户点击执行，从而达到控制中毒电脑的目的。

数据时刻面临高危泄密风险

1、内部人员主动或被动泄密

主动泄密：将企业内部文档私自拷贝外带及复用泄密(USB/网络/即时通讯/刻录)；盗用他人账号及设备非法访问数据泄密；私自携带笔记本设备接入内部网络非法下载数据泄密；对敏感数据的恶意传播及扩散泄密等。

被动泄密：存储设备遗失或失窃导致数据泄密；邮件或

网络误操作、误发送引起的泄密；设备和硬盘等维修、废弃时引发的泄密等。

2、危险网络

在外远程办公的无线路由器形形色色，其中不乏存在大量不安全网络，造成了数据在传输过程中“裸奔”，毫无安全防护的使用企业内部敏感数据。

3、家庭电脑

近期，大多数员工都使用家庭电脑办公，企业数据运行的环境失去了管控、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。

4、趁火打劫

发生重大公众事件后是不法分子的作案高峰期，伴随着重大公众事件的发酵扩散，生成了大量的恶意软件传播和网络欺诈行为。随着新冠肺炎疫情引发全球关注后，一系列的恶意软件和攻击手段都蜂拥而至。

不同类型的企业、不同定位的安全部门，如何结合企业自身情况，在平衡安全和效率的前提下，保护数据资产的安全呢？

专业方案解决远程办公困扰

亿赛通加密软件可通过联网客户端、离网客户端、U盘客户端等不同组合方式确保企业员工加班、出差、在家办公等业务连续时实现对核心数据的安全保护，通过提供完整、安全、可靠的多种形式办公方案，确保用户在紧急出差、出差延期以及网络瘫痪时业务连续及数据安全。

• 透明加密

以数据透明加密技术为核心，通过信息安全边界的建立，降低核心信息资产的有意或无意泄密风险，如源代码、设计图纸、财务数据、经营分析等。文档透明加密系统遵循加解密透明、管理强制和使用无感知的设计原则，有效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。

• 权限管理

对企业核心电子文档进行细分化的权限设置，确保机密信息在特定授权范围内合法操作，同一文档可以针对不同用户设置不同权限。通过实时权限控制，为用户提供安全授权下的机密信息共享机制，实现机密信息分权限的内部安全共享。

• 外发管理

当客户需要将涉密文档外发给客户时，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，用户需要通过身份认证，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。

• 移动终端

通过移动终端用户身份认证、移动终端数据存储和访问控制等手段，实现对移动终端的数据使用安全控制。

限时活动：亿赛通数据安全软件限时免费使用中，详情请来电咨询：400-898-1617。

信息化战“疫”进入关键时期， 信息泄露该如何管控？

近日，全国各地正在陆续返程，为做好疫情联防联控工作，单位均在落实人员申报登记制度。与此同时，个人信息泄露现象在各地频现，如何在疫情防控与个人信息保护之间求得平衡？政府应依法公开哪些信息？如何在公布涉疫个人信息与保护公众健康权、知情权之间做好“平衡术”？成为目前急需解决的问题。

中央网络安全和信息化委员会办公室发布的《关于做好个人信息保护利用大数据支撑联防联控工作的通知》强调“收集或掌握个人信息的机构要对个人信息的安全保护负责，采取严格的管理和技术防护措施，防止被窃取、被泄露”。



疫情期间侵犯隐私违反法律

疫情期间，各地在排查上报返乡人员和确诊患者信息时，一份份包括个人信息的文件在微信、微博等社交平台上被疯狂转发，内容包括相关人员的姓名、照片、工作单位、就读学校、家庭住址、手机号码、身份证号码及车票、航班信息等。信息泄露给返乡人员及确诊患者的生活带来极大的困扰，不少人甚至接到骚扰电话和谩骂短信。

针对疫情期间的个人信息保护问题，国家有关部门发布了相关通知。

交通运输部发布通知，明确要求依法严格保护个人隐私和信息安全，除因疫情防控需要，向卫生健康等部门提供乘客信息外，不得向其他机构、组织或者个人泄露有关信息、不得擅自在互联网散播。《关于做好个人信息保护利用大数据支撑联防联控工作的通知》中明确，除国务院卫生健康部门依据《中华人民共和国网络安全法》《中华人民共和国传染病防治法》《突发公共卫生事件应急条例》授权的机构外，其他任何单位和个人不得以疫情防控、疾病防治为由，未经被收集者同意收集使用个人信息。

疫情期间收集信息需参照规范，坚持最小范围原则

《关于做好个人信息保护利用大数据支撑联防联控工作的通知》中表明，收集联防联控所必需的个人信息应参照国家标准《个人信息安全规范》，坚持最小范围原则，收集对象原则上限于确诊者、疑似者、密切接触者等重点人群，一般不针对特定地区的所有人群，防止形成对特定地域人群的事实上歧视。

中国社会科学院法学研究所副研究员认为：发布确诊病患确诊前的行动轨迹应该尽可能详细，有助于密切接触者自我观察、及时就医，有的地方还发布了确诊病例的感染路径分析，便于公众加强自我防护。类似的信息公开只要没有指名道姓、不能识别特定的人，就没有侵犯公民的隐私权，而且尽到了善意提醒的作用，有助于寻找密切接触者和提示有关人员自我观察。

目前，基于大数据技术，公民可以查询实时防疫地图，这种直接或间接不可能识别公民个人身份的公开是没有问题的。此类信息公开已经能够达到抗击疫情的必要性要求，没有必要再变成可识别的公民个人身份信息。如果政府有关部门、医疗机构需要相关人员的个人信息，但信息公开要有底线，不得用于其他用途。

疫情防控期间，为了保障个人信息安全，应当在收集和保管时采取严格的保护措施，防止信息被泄露。任何单位和个人未经被收集者同意，不得公开姓名、年龄、身份

证号码、电话号码、家庭住址等个人信息。同时，疫情期间发布个人信息时，要尽量避免涉及个人；疫情结束后，应对相关个人信息进行封存。同时，专家认为，被侵犯个人隐私的当事人也要学会维护自己的权利。传播的信息若不属实，可要求传播者进行更改；电话号码公开后被骚扰，可要求公布者进行修改。

亿赛通十七年专注于数据安全领域，始终以客户的安全为第一位，为其提供具有针对性的数据安全解决方案。凭借十余年的技术优势、业务领域的丰富经验和高品质的服务，为客户提供强有力的技术支持和安全保障，获得了市场及客户的青睐。

疫情防护期间，亿赛通免费推出远程办公数据安全解决方案，保障企业办公安全，详情请咨询：400-898-1617。

文章资讯来源于互联网

信息安防不到位，国泰航空 接 50 万英镑罚单

近日，英国资讯委员会办公室（ICO）公布一项处罚决定：由于国泰航空有限公司未能保护客户个人数据的安全，对其罚款 50 万英镑（约 450 万元人民币）。

ICO 称，2014 年 10 月至 2018 年 5 月期间，国泰航空的计算机系统缺乏适当的安全措施，导致全球 940 万人的个人信息被泄露，其中 111578 人来自英国。被泄露乘客的个人信息包括：姓名、护照和身份信息、出生日期、电子邮件地址、电话号码和历史旅行信息等。

19. In total, approximately 9.4 million data subjects were affected by the data breach. Of these, 233,234 were from the EEA, and 111,578 were from the UK. 199,714 passport numbers issued by an EEA Member State were accessed. The breach encompassed a variety of types of personal data (in a variety of quantities), namely: passenger names, nationalities, dates of birth, phone numbers, email addresses, postal addresses, passport and identity card numbers, frequent flyer membership numbers, customer service remarks and historical travel information.¹

国泰航空在 2018 年 3 月意识到可疑活动，当时其数据库遭到暴力攻击，提交了大量密码或短语，希望最终能够正确猜出，他们随后向 ICO 报告了这一事件。

国泰航空是一家设在香港的航空公司，但在英国拥有分支机构，而且提供航班服务，过程中直接处理相关数据。国泰航空的系统是通过连接到互联网的服务器输入的，并安装了恶意软件来获取数据。

ICO 调查期间发现了一系列错误，包括：未受密码保护的备份文件；网上服务器没有进行最新更新；使用开发人员不再支持的操作系统以及防病毒保护不足。



ICO 调查主管史蒂夫·埃克斯利（Steve Eckersley）表示：“当人们向公司提供他们的个人信息时，他们理所当然地期望这些信息将保持安全，以确保他们免受任何潜在的伤害或欺诈。但事实并非如此。”

国泰航空系统中基本的安全缺陷数量众多，使得黑客很容易获得访问权限。调查中发现的多个严重缺陷远远低于预期的标准。从最基本的角度来看，该航空公司未能满足国家网络安全中心的基本网络基本要求中的五分之四。

根据现有披露的信息来看，未经授权使用国泰航空系统的最早日期是 2014 年 10 月 14 日，最早的未授权访问个人数据的日期是 2015 年 2 月 7 日。这项违法行为必须采取适当的技术和组织措施，防止未经授权或非法处理个人数据。ICO 对国泰航空罚款最终为 50 万英镑，除此之外，国泰航空还可能会被股东处以 4.7 亿英镑的罚款，占其全球年营业额的 4%。

关于英国资讯委员会办公室（ICO）

英国资讯委员会办公室（ICO）是英国的数据保护和信息权利法独立监管机构，维护公共利益的信息权，促进公共机构的开放性和个人的数据隐私。

其实，在国泰航空这件事情上，根本原因是公司安全防护不到位，数据安全意识薄弱，未来必须从源头消除类似事件发生，要将安全意识和技术手段结合起来共同保护客户隐私信息。不仅仅是国外企业，国内亦如此，中国数据安全防护专家亿赛通，与众多重要行业携手打造客户信息安全，既保证企业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、管控能力，如亿赛通电子文档安全管理系统，实现了企业内部电子文件的加密存储。倘若未经合法许可将加密文件带走，其文件内容将不能够被正常打开，从而确保文件内容不会因为文件数据扩散而泄密。

亿赛通数据安全管理体系可以有效支撑国家信息空间管理业务，提升国家公共安全工作的发现、管理能力与处理效率，为客户国家安全贡献重要技术力量。现阶段，亿赛通免费推出数据安全解决方案，保障企业数据安全，详情可咨询服务热线：400-898-1617。

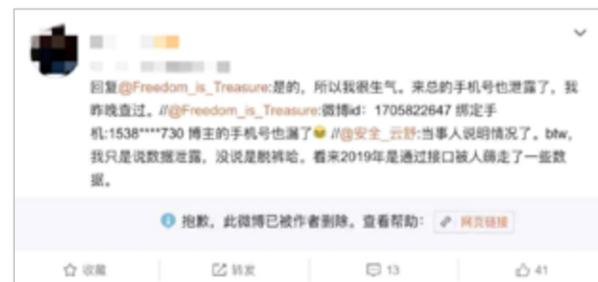
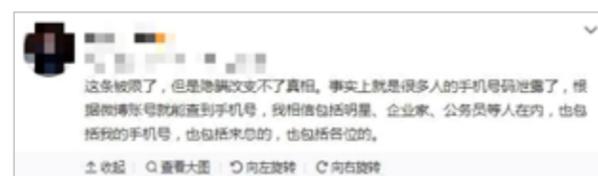
微博用户泄露引热议，急需为数据筑好最后一道防线

新浪微博蝉联热搜榜单

近日，新浪微博也连续登上“热搜榜”，因 APP 数据泄露一事引发热议。其实这也不是新浪第一次侵犯用户隐私，不知 CEO 王高飞是否会难为情？

前几日，某用户转发微博时称：“很多人的手机号码泄露了，根据微博账号就能查到手机号……已经有人通过微博泄露查到我的手机号码，来加我微信了。”

随后，该网友在微博下的留言中进一步表示，他通过技术查询，发现不少人的手机号已被泄露，当中涉及不少微博认证的明星、官员、企业家。“来总的手机号也被泄露了，我昨晚查过。”（“来总”代指微博 CEO 王高飞）



该微博一出，立马引发网友关注，毕竟涉及网络安全问题，网友都炸开了锅，纷纷留言表示自己也疑似遭遇了数据泄露，更有网友表示，发现 5.38 亿条微博用户信息在暗网出售，其中，1.72 亿条有账户基本信息。涉及到的账号信息包括用户 ID、账号发布的微博数、粉丝数、关注数、性别、地理位置等。



对此，新浪微博回应称：
• 自 2011 年来，微博一直提供根据通讯录手机号查询微博好友昵称的服务，用户授权后可以使用该服务。
但用户仅能查询到相关账号昵称，也可随时取消授权。

站方发现，此前黑客通过手机号比对服务获得多个平台的用户信息，例如通讯录好友微博昵称、QQ 号、邮箱等，并抓取微博用户个人主页上的公开数据，以“5.38 亿微博用户绑定手机号数据，其中 1.72 亿有账号基本信息”的名义进行售卖。

对此，站方已加强安全策略，并将详情上报给司法机关。此次非法调用微博接口匹配出的信息为微博账号昵称，不涉及身份证、密码，对微博服务没有影响。

发现异常后，我们及时加强了安全策略，今后还将不断强化。

但网络安全圈有很多大牛对微博的回应并不认可。

此后，工信部也就此问题约谈新浪微博负责人，新浪微博仍是“官方口吻”表示，“公司高度重视数据安全和个人信息保护，针对此次事件已采取了升级接口安全策略等措施，后续将按照工信部要求，落实企业数据安全主体责任，切实做好用户个人信息保护工作。”

微博多次发生侵犯用户隐私问题

此前，新浪微博也多次发生侵犯用户隐私的行为。

新浪数据库漏洞至大规模账号泄露

新浪曾存在 sql 注入漏洞，利用漏洞可读取数据库内内容。包括明文密码在内的 7000 多 W 新浪用户信息。可以通过构造数据库查询语句获得用户 uid=1303977362 的 uid、login、email、passwd 等信息，通过修改字段还可以获取其他信息。

脉脉信息安全纠纷事件

微博还曾与脉脉发生一起网络安全纠纷，因脉脉非法抓取使用新浪微博用户信息，虽然最后新浪微博胜诉，获得 200 万元赔偿，但这也暴露出新浪微博在保护用户隐私信息方面存在漏洞。

新浪微博用户密码库曾被泄露，并提供电驴下载地址，并且 Techweb 对该数据进行了下载验证，显示有部分用户名和密码可以登陆新浪微博或者邮箱，文件显示，泄漏总量超过 400 万。

本次事件中新浪微博 CEO 王高飞的电话号码也被泄露，简直引起尴尬癌。作为微博技术型高管，网友表示“他的主要问题是管理方面”，没想到这次微博数据安全问题如此轰动。

固定布局

从企业以数字化的方式存储信息开始，数据泄露就没有停止过。实际上，只要在计算机保持记录并存储信息，就有可能存在数据泄露。这时候，就需要一道坚固的防御工事来守好数据的阵线。

亿赛通数据库安全产品可通过分析数据库流量数据，获取权限控制所需关键信息，进行放行或阻断；使用过程中限定数据查询和下载数量、限定敏感数据访问的用户、地点和时间；提供对所有数据访问行为的记录，对风险行为进行 SysLog、邮件、短信等方式的告警，事后可进行追踪攻击。此次中国数据安全防护专家亿赛通全新推出的数据库安全产品线，为你的数据筑起最后一道坚固的防御工事。

文章资讯来源于互联网

商场如战场，看《完美关系》 你才不是单纯的在看一部职场剧

电视剧《完美关系》已经精彩大结局，这是一部讲述公关人的电视剧，在一个个危机公关事件中，逐渐发现人性的真善美。

江达琳是在 DL 危急时刻，临危受命的总裁，这个海龟学子，有着单纯的心思，缺少职场的敏感度和决策力。好在公关界牛人卫哲，为了报恩江达琳的父亲江远鹏，而选择帮助江达琳和 DL 渡过危急时刻。

商场如战场，商场间谍在战场中已是司空见惯的。买通内鬼盗取竞争对手的资料，成为影视剧中常见手段类似“无间道”情节固然有着编剧的艺术创作成分，但它却向大家展现了一个事实

.....

在剧中，DL 内鬼将公司标书内容泄露给竞争对手，后续调查过程中发现，只有在印刷厂才会出现标书泄露的过程，随即前去指定印刷厂询问当天情况。印刷厂工人表示，谭新凯嘱咐当 DL 的人走后，多打出一份，给了后面来的女士。

涉及公民隐私数据泄露的问题上，相比遭遇黑客攻击而造成的损失，内部泄露造成的数据被盗占有更大的比重。



泄露商业机密将遭严惩

我国《刑法》第二百一十九条也规定，盗取、利诱、胁迫或者其他不正当手段获取权利人的商业秘密的，要处三年以上有期徒刑或拘役。而在你倒霉的时候，竞争对手早就把

自己撇得干干净净，谁的损失大？

互联网时代，数据呈现方式的多样化，以及获取渠道的多元化都让我们的隐私被暴露在“光天化日”下，而随着由数据的非法获取、网上兜售、甚至违规利用所组成的利益链条悄然形成，无论是企业自身、还是政府机构，包括我们公民自身都需要时刻警惕数据泄露的危险。作为 IT 服务厂商，中国数据安全保护专家——亿赛通有义务也有责任帮助政企做好数据安全保护工作。

数据篡改、内鬼泄密事件的爆发，令用户已经普遍意识到企业数据库访问疏于监管所带来的巨大危害。那么，亿赛通数据库审计产品，能让你得到什么呢？你可以放心的使用各种数据库类型，第一时间获得数据库操作行为，随时监控，操作全面审核、统计分析……系统自身也会进行监控和管理。

六大特色让数据库审计更可靠

▶业务系统无感审计（稳）：系统主要采用旁路镜像方式部署，将客户数据库的网络流量单向引出，能做到对客户业务网络零影响，对客户业务系统无感知，从而保证客户原有业务系统的稳定运行。

▶终端用户审计能力（准）：系统利用 WEB 插件关联技术，将应用层和数据库层的访问操作请求关联，可以追溯到应用层的最初访问数据及请求信息，可直接定位到业务终端用户。

▶大数据架构和设计（快）：系统采用大数据计算和存储架构以及数据热交换技术，大大提高了实时数据处理效率，使得数据检索不仅范围更广，能实现全库检索，而且查询效率更高，对于客户常用的查询和检索场景，均能实现秒级响应。

▶数据类型全面审计（全）：系统支持数据库类型丰富全面。不仅支持市场主流关系型数据库，还支持国产数据库和大数据审计。

系统支持 SQL 语句、参数、函数全面审计。记录内容全面，包括人员、时间、位置、动作、对象、工具、结果等七要素的全面审计。

系统支持网络协议完整。能完美支持 IPv4、IPv6 双栈网络协议数据流量的混合审计。

▶机器智能模型学习（智）：系统具备在目标网络中的数据库自动发现能力，并且支持自动对象参数配置，同时系统具备特定数据库的数据访问模型学习能力，可自动归纳学习数据库访问模型。

▶审计部署方式灵活（灵）：系统采用大数架构及分层模块化设计，具备极强的伸缩性，既支持硬件一体机方式，也可完美支持分布式部署，同时还支持纯虚拟化环境部署。



商场如战场的今天，黑客和竞争对手都在觊觎你的数据库资产，一不小心就造成巨大的商业利益损失！ DAS 数据库安全审计系统可以全面审核、监控数据库操作信息，数据库审计产品选择亿赛通，这波稳了。

中国移动通信集团公司



客户简介

中国移动通信集团公司（简称“中国移动”）成立于 2000 年，是一家基于 GSM，TD-SCDMA 和 TD-LTE 制式网络的移动通信运营商。中国移动是根据国家关于电信体制改革的部署和要求，在原中国电信移动通信资产总体剥离的基础上组建的国有骨干企业，公司全资拥有中国移动（香港）集团有限公司，由其控股的中国移动有限公司（简称“上市公司”）在国内 31 个省（自治区、直辖市）和香港特别行政区设立全资子公司，并在香港和纽约上市。除原有“动感地带”、“神州行”、“全球通”、“动力 100”、“G3”外，在 2013 年公布了与正邦合作设计的 4G 品牌，标志着中国移动 4G 业务的正式启动。2016 年中国移动位列财富世界 500 强之一。

需求背景

中国移动作为通信行业的市场龙头之一，业务系统遍布全国各个角落，因此其业务支撑系统包含了很多重要的信息资料，如业务支撑网络积累和掌握了大量的客户信息、生产数据和运营信息等，如果重要信息一旦泄露，造成的损失非常之大，所以中国移动在原有的数据管理基础上进一步强化数据安全中存在的缺陷问题，如人员流动性大、外出工作、打印、邮件往来等都有可能对数据安全造成威胁。

解决方案

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；

内容安全防护：防止核心数据通过复制拖拽、截屏录制、打印输出、副本另存等方式泄密；

多密钥隔离例外：可实现部门动态加密文档相互隔离禁止交叉打开，管理人员可以打开各部门文档，自身文档可自动或半自动透明加密，密钥可以独立或与某个部门相同；

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；

数据安全传输：数据始终以密文形式传输、存储和使用，保障传输过程中的安全；

终端自我保护：全球首创底层 Anti-hacking 技术，防止移动终端应用程序被反编译或破解；

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。

项目成果

亿赛通文档安全管理系统帮助中国移动公司保障文档数据存储的安全，提高了公司的整体数据管理能力，极大的实现了业务无障碍操作运转。

中国联合通信有限公司



企业简介

中国联合通信有限公司成立于 1994 年，拥有 843 亿元净资产，2129 亿元总资产的大型国有骨干企业，是我国提供全面电信基本业务的综合性电信运营企业，并在纽约、香港、上海三地同时上市的电信运营企业，世界 500 强企业之一，拥有覆盖全国、通达世界的通信网络，在国内 31 个省（自治区、直辖市）和境外多个国家和地区设有分支机构，主要经营 GSM 和 WCDMA 制式移动网络业务、固定通信业务，国内、国际通信设施服务业务，卫星国际专线业务、数据通信业务、网络接入业务和各类电信增值业务。

需求背景

随着电信市场竞争的日益激烈，客户资料、企业运营数据、营销策略文件等各类信息资产已成为核心资产。近年来，电信运营商敏感信息数据泄露安全事件频繁发生，泄密事件给中国联通公司敲起了警钟。认识到了自身在数据安全方面的不足之处，如下：

- 1、缺乏有效的数据防泄密手段和数据的访问控制措施；
- 2、地市的离线数据下载和 C/S 结构的数据查询成为数据安全隐患，数据无法控制，基本处于失控状态；
- 3、对涉密数据的生命周期缺乏有效管理手段等。

根据工业和信息化部相关文件以及总部《中国联通集团内网信息安全体系和工作思路》的要求，中国联通开始对数据泄露防护项目的前期调研及选型，经过 3 个多月的测试，最终选择了亿赛通公司产品作为其核心电子数据保驾护航，并且四省联通正式启动 BSS 系统数据防泄密项目，已加强对敏感数据的保护及管理。

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数据保护系统，主要发现、识别分类企业敏感数据；监控企业敏感数据；保护企业敏感数据以防丢失和窃取。

网络防护：防止敏感数据通过邮件、网盘、微博等网络方式泄露出去；

终端防护：防止敏感数据通过打印、刻录、聊天工具等终端方式泄露出去；

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；

审计报告：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

通过强制加密策略，能够获取到用户资料、经营分析资料的部门及员工实现强制自动加密处理，未安装客户端的电脑则需要经过审批才能拿到文件；通过对 BSS 业务系统的安全保护，凡是从系统中下载的文件已经过加密处理；通过数据集中、网络改造、数据加密、日志审计等手段，达到事前预防；控制集中数据提取、权限控制等手段，达到事中监控；从数据提取到数据分发加密控制并全程日志记录，对涉密数据全生命周期管理，达到事后可查的目的。