



中国数据安全防护专家

集团企业 精选案例集

www.esafenet.com



关注官方微信，了解更多内容

北京亿赛通科技发展有限公司

地址：北京市海淀区西二旗大街39号A座3层/4层 100085

电话：86-10-57933888

咨询热线：400-898-1617

网站：www.esafenet.com

中国数据安全防护专家

提供有竞争力的数据资产安全解决方案和服务，持续为客户创造最大价值！



公司介绍

北京亿赛通科技发展有限公司（以下简称“亿赛通”）成立于2003年，是绿盟科技全资子公司，作为国内领先的数据安全业务供应商，是一个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，连续多年获得CCID赛迪权威报告“亿赛通--市场占有率第一品牌”等多项权威称号。

创立至今，亿赛通发扬持续创新的精神，开创了多个业界第一：国内第一套文档安全管理系统、第一套文档透明加解密系统、第一套DLP数据泄露防护解决方案、第一款基于FDE的全磁盘动态加密系统、第一款基于WIN64Bit操作系统的DLP、第一套移动安全接入解决方案、全球第一套Anti-hacking手机应用防破解系统、第一套基于语义识别的智能加密系统……以产品、方案、服务三个方向为主导，逐步构建终端数据防护、网络数据防护、应用数据防护、存储数据防护、介质数据防护和云服务平台等六层防护，以上百项知识产权涵盖了包括：终端、网络、存储、审计等多个方面的几十个数据安全软硬件产品，为建立持续的领航地位提供了核心技术保障。

亿赛通秉承“服务客户、持续创新、勇担责任、专业至上”的核心价值观，凭借卓越的技术和丰富的解决方案，为每一位客户提供最及时、最全面、最到位的服务。近年来，先后为中国移动、中国电信、中国联通、中信证券、招商银行、浦发银行、方正集团、正大集团、艾默生、三星集团等众多国内外知名企业提供数据安全解决方案。亿赛通肩负着“保护数据所有者的信息资产安全”使命，不断进军国内外市场。在国内市场，为党政军、设计制造、金融证券、研发通讯、能源电力、运营商等各大行业万家客户提供产品和服务、拥有过百万终端用户；在国际市场，已将产品及服务部署到十几个国家，过硬的产品和一流的服务，构筑了亿赛通市场占有率连续多年稳居第一的骄人战绩。

亿赛通的卓越发展，离不开求真务实的研发队伍。公司拥有以知名信息安全专家为核心的信息安全咨询团队，以及以清华和北航博士、硕士为核心的产品研发团队。几年来，又与北京航空航天大学 and 北京邮电大学结成“产学研”联盟，为企业发展和人才培养注入源源不断的活力。同时，先后与英特尔、联想、华为等IT巨头达成战略合作伙伴关系，共同开拓终端安全领域的一个又一个新兴市场。截至目前，亿赛通公司已在全国三十余个主要城市设立了分支机构，覆盖全国的营销及服务战略性布局基本完成，为立足国内外市场打下了坚实基础。





目录

Contents

03/ 公司介绍

06/ 目录

07/ 集团企业数据安全综合解决方案

11/ 蒙牛乳业（集团）股份有限公司

13/ 上海德邦物流服务有限公司

15/ 红塔烟草（集团）有限责任公司

17/ 花样年控股集团有限公司

19/ 江西金太阳教育研究有限公司

21/ 深圳市世方商业地产顾问机构

23/ 全友家私有限公司

25/ 华中科技大学

27/ 江西济民可信集团

29/ 北京万泰生物药业股份有限公司

31/ 梅花集团

33/ 部分客户

集团企业 数据安全综合 解决方案

一、行业分析

医药、房产、教育、烟草、物流、食品等行业，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：新产品研发投入大、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。

二、客户需求

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、质量管理体系、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？

三、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。

四、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。

集团企业经典案例集（部分）

一、蒙牛乳业（集团）股份有限公司



客户简介

蒙牛乳业集团（简称“蒙牛”）成立于1999年，总部位于内蒙古自治区，是一家生产牛奶、酸奶和乳制品的生产龙头企业之一，早在2005年时已成为中国奶制品营业额第二大的公司，其中液态奶和冰淇淋的产量都居全中国第一。所以其产品覆盖整个国内市场，产品同时出口到蒙古、东南亚、美国、西班牙及港澳等国家和地区。创业数年，他们创造了举世瞩目的“蒙牛速度”和“蒙牛奇迹”。

需求背景

蒙牛作为国内特大奶制品龙头企业，企业内部敏感资料势必是公司的一笔资产，为此蒙牛非常重视企业的数据安全管理。

解决方案

亿赛通文档外发是针对客户重要信息或核心资料外发安全需求设计的外发安全产品，具体方案如下：

- 1. 丰富兼容接口：**支持常见各种格式电子文档的安全控制；
- 2. 高度的安全性：**采用高强度动态虚拟卷加密与安全沙箱隔离保护技术，外发文件在传输和使用过程中保持加密状态，此外，日志记录确保审计和追溯；
- 3. 细粒度权限控制：**外发文档可控制多种权限，包括浏览次数、使用时间、打印、打印水印、修改、还原、防止内容拖拽、拷屏和设置自动销毁等。
- 4. 详尽日志分析：**详尽记录了登录日志和操作日志。同时，日志收集过来进行集中审计，便于泄密事件发生后的分析和追查。所有

用户的任何操作，系统将自动监控、跟踪并进行记录。另外，通过日志审计功能，管理员可以随时查看系统运行情况，能够及时发现一些异常操作，从根本上降低数据泄露的风险。

项目成果

保障了蒙牛集团文档外发控制系统生成外发文件发出时数据安全，有效的防止了集团内重要信息被非法扩散的风险。



二、上海德邦物流服务有限公司



客户简介

上海德邦物流服务有限公司是一家具有较大规模的专业从事物流服务的专业公司。专营上海至全国各地往返货物运输、货物代理、货物配载、货物配送、仓储等物流业务。逐步形成以公路为主，铁路为辐线的快速运输体系，服务范围覆盖全国各大中小城市。立足上海，覆盖全国，运力雄厚，管理严谨。把服务质量意识深入到公司的每个落，确保高质量完成每一次运输任务。

需求背景

近些年物流行业大量的消费者私人信息泄密事件频繁发生，一旦有快递企业的用户信息泄露事件发生，不仅会给公司带来严重的名誉损害，同时也会给整个社会带来更大经济损失。所以信息安全已经悄然发展成为物流快递业必须高度重视，急需解决的首要问题。有的是一些别有用心不法分子看中其“内在价值”，非法盗用、转卖消费者个人信息谋取私利；有的是个别快递公司无视行业准则，违规泄露客户信息，自动卷入灰色利益链条之中；还有的是消费者个人安全意识不强，给不法分子可乘之机。凡此种种，都提醒我们保障快递信息安全刻不容缓。快递企业应该加强行业自律，加强对内部员工职业道德教育和规范化操作管理，完善保密制度，提升业务管理规范性，以确保物流快递的用户信息安全。

解决方案

- 1. 智能透明加密：**实现对任意文档自动透明加密的同时，不影响用户的使用习惯；
- 2. 内容安全防护：**防止核心数据通过复制拖拽、截屏录制、打印输出以及副本另存等方式泄密；
- 3. 安全水印支持：**通过自动添加安全警示及版权标识信息，来降低屏幕录制和自主打印所带来的泄密风险；

4. 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账号信息的自动完整同步和单点登录认证集成等；

5. 离线办公支持：可通过离线审核、策略预设及离线补时等功能满足各种离线办公要求；

6. 安全水印支持：通过自动添加安全警示及版权标识信息，来降低屏幕录制和自主打印所带来的泄密风险。

项目成果

截止 2015 年 11 月德邦物流 5600 多个分支机构均已全部投入亿赛通 DLP 数据防泄露体系，数据安全无论是内部办公、网络办公、移动办公均实现了文档安全统一管控，可分类、分级、分权使用文档，防止用户信息外泄，这份安心值得我们信赖。先后北京亚太物流中心、近铁国家物流、深圳年富供应链等等多家物流快递公司，纷纷也都牵手亿赛通，实现对企业敏感数据安全审计，对终端和网络数据进行完全监控，根据安全需求进行加密、阻断、告警与审计，建立了全方位信息安全管理机制，从而保证了物流快递企业的用户信息安全，这不仅是对物流快递企业的一份保障，也是对我们个人用户一份安心快递的选择。

三、红塔烟草（集团）有限责任公司



客户简介

红塔烟草（集团）有限责任公司成立于1956年，1958年为了向国庆十周年献礼，第一包“红塔山”香烟诞生了。在经过20余年艰难的行进，1997年“红塔山”被国家工商总局认定为“中国驰名商标”，“红塔山”因此成为“中国民族工业的一面旗帜”。近年，红塔集团积极推进“大市场、大企业、大品牌”战略，以品牌的整合扩张，推动重点工业企业联合重组，拥有坚定的信念，同时也致力于制定务实的、以市场为导向的和高度有效的战略。

需求背景

红塔烟草作为一驰名品牌，数据安全与否把握着公司生存发展状况，然而其公司庞大的业务在数据传输的环节存在瑕疵，容易被泄露，红塔烟草选择与亿赛通联手合作打造企业数据安全。

解决方案

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。

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。

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账号信息的自动完整同步和单点登录认证集成等。

详尽日志分析：详尽记录了登录日志和操作日志，同时。日志收集过来，进行集中审计，便于泄密事件发生后的分析和追查。所有用户的任何操作，系统将自动监控、跟踪并进行记录。另外，通过日志审计功能，管理员可以随时查看系统运行情况，能够及时发现一些异常操作，从根本上降低数据泄露的风险。

项目成果

保障了红塔烟草集团内部人员邮件外发的过程，通过审计分析，确保中间传输环节数据安全不可被窃取。

四、花样年控股集团有限公司



客户简介

花样年控股集团有限公司起步于1998年，总部设立于深圳，为中国领先的以金融为驱动、服务为平台、开发为工具的金融控股集团，致力于成为有趣、有味、有料的生活空间及体验的引领者。2009年11月，花样年控股在香港联交所主板成功上市，股份代号为HK1777。至2013年，花样年控股资产规模超过人民币300亿元，拥有员工1.2万多名。

需求背景

信息化爆炸时代，面对数据安全问题的巨大挑战以及企业庞大的人员规模和业务规模，花样年集团的总部与总部、总部与分支机构之间的信息传输和资源共享的信息安全问题显得尤为重要。因此，花样年集团一直把信息安全管理作为首要目标，把数据安全作为抓住机遇、迎接挑战的有效途径。

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：可使从花样年集团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，每周最多解密5篇权限文件，如超过该值会向管理员进行预警。不可解密文件只能由指定专人进行解密。

3. 全盘加密安全U盘：

①强身份认证：保护合法用户访问U盘文件加密区。

②加密密钥：为U盘里本身加密的数据穿上第二层防护衣。

③账号保险箱：杜绝银行账号、系统密码等涉密信息的泄密风险等。

项目成果

通过以上防范手段，不仅为花样年集团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。

五、江西金太阳教育研究有限公司



客户简介

江西金太阳教育研究有限公司（简称“金太阳”）创建于1996年，是一家集教育研究、出版发行于一体大型基础教育研究和教辅出版发行企业。公司自创办以来，在教材教法、学生学法、考试研究、学生心理健康、教考信息等方面都展开了卓有成效的研究工作。公司编写的金太阳系列丛书、金太阳系列试卷在全国影响深远。金太阳的发展，一年一大步，五年上台阶，经历了产品创新阶段和品牌创建阶段，目前正处于全面腾飞阶段。



需求背景

金太阳是一家集教育研究、出版发行于一体大型基础教育研究和教辅出版发行企业。在市场竞争如此激烈的情况下，加上其产品可复制性非常强的产品特征，金太阳意识到必须要有一种强有力的管控手段，才能保障企业自身的核心竞争力。

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，对于核心数据，需要控制数据过程使用安全时，采用透明加密控制方式控制数据的安全使用，实现内容安全防护、安全浮水印、统一身份认证、离线办公安全、日志审计等功能，确保文件内容不会因为文件数据体扩散而扩散。

项目成果

金太阳借助亿赛通文档透明加密系统产品自身良好的稳定性、兼容性，在不影响用户工作习惯及业务效率的同时，实现了企业内部电子文件的加密存储，有效防止企业核心信息资产外泄风险。

六、深圳市世方商业地产顾问机构



客户简介

深圳市世方商业地产顾问机构成立于 1993 年，是深圳商业地产策划代理行业的启蒙者，也是是中国商业地产策划代理行业的知名企业机构，由世方投资控股、世方商业地产顾问、世方市场营销策划、武汉世方、合肥世方、世方红广告等多家公司及万商会、中华专业市场两大网络平台共同组成，在全国设立华南、华中、华东、华北、西南等五大区域，已涉足全国 18 个省份，70 余个城市，典型案例超过 200 个，被誉为深圳商业地产的“黄埔军校”。

需求背景

世方地产在信息化发展的道路上上线了 KM（知识管理）系统作为企业最为核心的信息化共享平台，其愿景是打造知识汇聚中心、经验交流中心、能力提升中心；通过积累知识资产，并不断传承创新，形成世方不可复制的知识竞争力，为客户提供更卓越的服务。但是另一方面，随时知识管理系统的运用越广泛，越来越多的信息资料包括客户信息、营销策划方案、市场调研报告、财务报表被员工随意下载、复制、拷贝、外泄。如何确保 KM 系统中的数据资源在内部高度共享的同时又能防止随意外泄的课题被提上重要议程。

解决方案

- 1. 应用安全准入：**针对制定的应用系统进行通路数据加密，即任何用户访问系统时获得的数据都是加密的。只有在 PC 终端上安装强化身份认证的解密软件，才能正常阅读应用系统中的数据；
- 2. 系统标准加密：**在文件下载过程中，数据加解密网关会自动实现文件的加密，加密的文件在合法的系统用户中可正常使用。而对非系统用户则是不可用的；

3. 文件授权管理：针对实际业务应用的不同情况，系统在文件授权提供不同的授权模式，文件分级权限及文件群组授权；

4. 统一外发管理：在系统用户管理和认证体系下，只有系统合法用户根据安全策略才能获得文件外发的使用权。发起人的文件自动上传给系统，同时系统会在服务器制作外发文件，且将外发文件和使用说明书文件共同形成一个 ZIP 压缩包，该压缩包可通过用户随文件上传时预约的邮件地址发给接收人，也可由发起人通过该链接下载后再以其他形式发出。

项目成果

知识管理库中下载的文档经 TrustArmour 网关自动生成成为权限文档，TrustArmour 网关通过双机热备确保知识管理系统的高可用性，同时针对用户组织架构划分文档的权限，用户需安装 TrustArmour 客户端并验证身份的合法性之后才可以按用户等级查看权限文档；目前项目覆盖华南、华中、华东、华北、西南各分支机构，使用用户达 400 余人。

七、全友家私有限公司



QUANYU 全友家私
FURNITURE

客户简介

全友家私有限公司创建于1986年，经过二十余载的励精图治，已发展成为中国研、产、销一体化大型家具龙头企业。作为中国规模最大的家具制造企业，公司拥有共计占地6000余亩的四大制造基地，30多个专业分厂、20多个驻外销售服务机构、3000多家专卖店。公司产品连续多年畅销全国，并远销欧美、东南亚多个国家和地区，产品销量在全国同行业中连续多年遥遥领先。



需求背景

家具行业竞争激烈，产品更新换代快，需要不断创新，销售策略不断改进。人员流动大的同时，竞争对手潜伏现象普遍。所以公司的战略规划、管理方法、商业模式、财务信息、投融资决策、产购销策略、资源储备、客户信息、招投标事项等经营信息。设计、制作工艺、制作方法、技术诀窍等技术信息容易被泄露。

解决方案

主动防御：将对核心信息进行全生命周期强制加密保护，防止核心信息在内部共享、流转、使用时所带来的数据扩散泄密；

三权分离：系统管理、文档管理和日志管理权限及职责的有效分离，在保障体系协同运转的同时实现管理制约及监督；

分级管理：亿赛通 DLP-CDG 采用权限分离、管控分级的信息安全管控理念，将系统管理维护、终端管理、日志审计等权限有机分离，避免由于管理人员权限过大而导致的泄密隐患。

项目成果

该项目运行期间，全友家私遇到一次竞争对手攻击情形，但由于企业内部部署数据安全防护手段，竞争对手未曾窃取任何文件。

八、华中科技大学



客户简介

华中科技大学计算机科学与技术学院具有计算机科学与技术一级学科博士学位授予权（计算机系统结构、计算机软件与理论、计算机应用技术和信息安全四个二级学科均具有博士学位授予权）和一级学科博士后流动站；同时一级学科也是湖北省重点学科，其中，计算机系统结构为国家重点学科、湖北省高校特色学科。该学科是中国计算机学会常务理事单位、湖北省计算机学会理事长单位、“211工程”和“985工程”重点建设学科。2012年在教育部学位与研究生教育发展中心组织的一级学科评估中排名全国第十。

需求背景

作为计算机科学与技术学院，每年都会研发出一些新的技术和专利，其设计图纸、重要代码、编程内容等信息非常重要，如果重要数据被窃取，这些技术和专利所有的研发成果都全军覆没，损失惨重。所以，为了防止重要研发数据被泄密，华中科技大学计算机科学与技术学院迫切需要加强数据安全保护。

解决方案

亿赛通可信介质安全管理体系是针对移动存储介质使用范围、使用方式及数据安全存储进行科学控制的安全管理系统。

1、从介质访问控制、终端注册授权、介质注册授权、介质存储数据安全保护、介质使用权限控制、介质离线审批与权限控制、介质使用安全审计以及结合终端端口控制、终端光盘刻录监控与审计等方面对存储介质进行数据泄露防护管理，用技术手段实现存储介质的安全使用及存储的数据安全保护；

2、通过对介质的访问控制与注册授权，实现非注册介质接入内网计算机上不能使用，内网专用介质接入非内网计算机上不能使用；

3、数据始终以密文形式存储在专用介质上，非授权用户不能解密，保证涉密介质丢失后不会造成泄密事故。详细的介质使用审计日志，确保介质可追踪等。

项目成果

通过部署亿赛通可信介质产品，帮助华中科技大学计算机科学与技术学院达到如下效果：

- 1、**进不来**：非注册介质不能在单位内部计算机上使用；
- 2、**拿不走**：内部注册专用U盘不能在单位外界计算机上使用；
- 3、**读不懂**：内部专用U盘数据进行加密存储，非授权用户不能解密；
- 4、**改不了**：数据存储在专用U盘上，非法用户无法更改数据内容；
- 5、**走不脱**：详细的U盘使用日志，泄密事件可追踪，犯罪分子无处可逃。

九、江西济民可信集团



客户简介

江西济民可信集团 2000 年正式成立，是以医药为核心、健康地产和医疗康复产业为两翼的大型健康产业集团。集团现有员工 6000 余人，总资产逾 100 亿元。在江西、北京、江苏、香港等地设有 9 家全资子公司，86 家销售分公司遍布全国各主要省市，产品远销东南亚及欧美市场。

需求背景

集团各区域分支的地理分布决定了数据管理者的管理思路，另外再加上早期出现了几起移动设备的丢失并造成了一定的影响，更加使济民可信的管理者坚定部署数据防泄密管理系统的决心。

解决方案

1. 文档透明加密系统

文件加密：对文档进行高强度加密和对使用者透明解密。实现盗走了，拿走了，没法用；操作简单，应用方便，现场无痕；

外发控制：对外发文件能控制文件的打开方式、权限控制、操作记录；

应用灵活：根据业务实际情况进行结合、使对文档灵活的管理。达到“多方适应，技管结合，兼顾现状”的系统应用机制；

审计报表：实现对身份、操作行为的完整记录、报表分析与查询，以便审计。

2. 文档外发管理系统

文档加密：采用高强度加密技术对外发数据进行加密保护，防止非法用户暴力破解泄密。

身份认证：外发文档提供多种安全身份认证机制，包括：密码口令认证、机器绑定认证、硬件 USB-KEY 认证及混合认证等，在身份认证通过后才可正常、安全打开外发文档。

权限控制：外发文档提供细粒度权限控制保护，包含文档使用权限如只读、打印、修改等控制；文档生命周期管理如：阅读次数、阅读时限及过期自动销毁等保护；文档协同权限如修改、还原以及文档内容保护、打印水印等控制。

内容防护：为防止使用者恶意将文件内容扩散，系统对其内容进行高强度安全控制，如内容剪切保护、禁止截屏、禁止另存为及打印控制等。

项目成果

通过部署文档透明加密系统和文档外发管理系统后，让江西济民可信集团庞大的工作业务系统的数据得到优化管理，无论其内部、外部威胁环境都无法窃取企业敏感的医药数据，让集团所有员工都能够高效的进行安全工作。

十、北京万泰生物药业股份有限公司



客户简介

北京万泰生物药业股份有限公司隶属于养生堂有限公司，是从事生物诊断试剂与疫苗研发及生产的高新技术企业，以“科学为本，关注健康”为理念，以“质量求生存，科技创新求发展”为宗旨，以“为人类的健康事业做出贡献”为追求，将生物技术成果转化为优质产品服务于社会大众。

需求背景

诸多数据泄密事件，着实给企业造成不少的压力。万泰生物药业为避免技术部、研发中心等重要部门的成果性自主知识产权文档，因内部人员有意或无意泄密，而给企业造成重大经济损失，经过近一年选型，最终签约亿赛通公司数据安全管理体系。

解决方案

1. 文档透明加密系统：

实现了企业内部电子文件的加密存储。无论是由人工生产还是由应用系统生成的，只要写在磁盘上就是加密形式；另外，只有被系统授权许可，才可使用这些加密的文件，如未经合法许可将加密文件数据体带走，加密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体扩散而扩散。

2. 文档外发管理系统：

在文档外发文件打开时，用户需通过身份认证，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，从而有效防止了客户重要信息被非法扩散。

项目成果

亿赛通加密技术，为其 Office、WPS、PDF、JPG 等格式文档的强制加密和内部自由使用，通过灵活的策略管理使不同角色拥有不同的操作权限。既加强了内部文档的安全管控又不会增加用户太多的额外工作量。



十一、梅花集团



客户简介

梅花集团是全球领先的氨基酸营养健康解决方案提供商。公司通过为全球 100 多个国家和地区多家知名客户提供各类氨基酸产品及使用解决方案，让全世界用户享有技术的全方位沟通。公司成立于 2002 年，注册地为西藏自治区拉萨市，全称“梅花生物科技集团股份有限公司”，2009 年完成股份制改造，2010 年底在沪市 A 股上市，办公地址位于河北省廊坊市，是目前国内氨基酸综合品类最多、产能最大的生产企业之一。

梅花集团拥有生物发酵行业中最完整的、最长的产业链和配套设施，通过全系列的研、产、供、销服务，灵活满足全球不同客户的差异化需求以及快速创新的追求，专注于打造生物发酵和生物制药的高端产业平台。2015 年梅花集团实现营业收入 130 亿，员工总数 1.2 万，目前已完成河北、内蒙、新疆、山西等多区域布局。

需求背景

随着梅花集团的大步伐扩张，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、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：

- ① 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。
- ② 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；
- ③ 文档操作强制日志审计，确保事后可追溯；
- ④ 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；
- ⑤ 邮件发送可信对象时自动解密，提高工作效率；
- ⑥ 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。

2. 全盘加密安全 U 盘：

- ① 强身份认证：保护合法用户访问 U 盘文件加密区
- ② 加密密钥：为 U 盘里本身加密的数据穿上第二层防护衣
- ③ 账号保险箱：杜绝银行账号、系统密码等涉密信息的泄密风险等。

3. 电子文件保险箱：

- ① 应用程序安全保护：当用户访问受该产品保护的文件时，因受到文件保险箱的应用程序的保护，只允许插入 key 的合法用户运行使用，杜绝非法用户使用。
- ② 即时通讯数据安全保护：用户可将 QQ、MSN、ICQ、UC、Skepe 等网络即时通讯工具的通讯记录，设定保存在安全保险箱中，只有合法用户才能看到隐私数据，防止他人偷窥或利用。
- ③ 机密与隐私数据安全保护：对电脑机密与隐私数据进行强加密保护，防止电脑以外危机所带来的泄密风险。
- ④ 专业数据保护：用户可为企业财务数据、分析报告、设计文件等重要数据建立专属文档，电子文件保险箱将对专属文件进行加密保护。
- ⑤ 电子邮件内容安全保护：可为 Outlook、Foxmail 等邮件系统提供内容保护。

项目成果

自梅花集团建立这三重防护体系后，极大程度上实现了泄密问题的精准定位以及核心数据精确保护！

部分客户

- 1、蒙牛乳业(集团)股份有限公司
- 2、上海德邦物流服务有限公司
- 3、云南红塔集团有限公司
- 4、花样年控股集团有限公司
- 5、江西金太阳教育研究有限公司
- 6、深圳市世方商业地产
- 7、全友家私有限公司
- 8、华中科技大学
- 9、江西济民可信集团
- 10、北京万泰生物药业
- 11、梅花集团
- 12、万科集团
- 13、北陆药业
- 14、达内时代科技集团有限公司
- 15、京汉置业集团股份有限公司
- 16、北京建筑大学
- 17、北京理工大学雷达与对抗技术研究所
- 18、北京天地思高教育科技有限公司
- 19、北大资源集团控股有限公司
- 20、沃斯坦热力技术(北京)有限公司
- 21、JFE 贸易(北京)有限公司
- 22、河北永辉房地产开发有限公司
- 23、河北天山实业集团有限公司
- 24、河北永康房地产开发集团有限公司
- 25、卓达房地产集团有限公司
- 26、内蒙古信元网络安全技术股份有限公司
- 27、青岛银盛泰房地产有限公司
- 28、东辰控股集团有限公司
- 29、山西中天信科技股份有限公司
- 30、中国民航大学
- 31、倍索企业管理咨询(上海)有限公司
- 32、上海东方传媒集团有限公司
- 33、旭辉集团股份有限公司
- 34、上海宋海佳律师事务所
- 35、上海放心酒业连锁有限公司
- 36、盛威科(上海)油墨有限公司
- 37、依工(中国)投资有限公司
- 38、昆山高科电子艺术创意产业发展有限公司
- 39、江苏天目湖旅游股份有限公司
- 40、浙江工业大学信息工程学院
- 41、近铁国际物流(深圳)有限公司
- 42、NDO Technology Co,Ltd
- 43、长安大学
- 44、深圳富瑞集团
- 45、西藏藏医学院
- 46、雅致集成房屋(集团)股份有限公司
- 47、众环海华税务师事务所有限公司
- 48、国防科学技术大学
- 49、中昊晨光化工研究院
- 50、重庆融汇地产(集团)有限公司
- 51、西安曲江文化旅游股份有限公司
- 52、河南龙成煤高效技术应用有限公司
- 53、广州市南方人力资源评价中心有限公司
- 54、莆田市城厢区凯特图文服务中心
- 55、安徽岳森贸易有限公司
- 56、重庆金阳房地产开发有限公司
-