安腾方案：
企业数据安全/泄密防护解决方案

安腾为您的业务提供合终极数据安全保护，保护您免受信息泄密的威胁

文档加密与数据泄密防护方案

安腾能帮您解决企业中的以下问题：

- 技术员工离职带走核心资料，导致重大隐患
- 重要图纸文档被盗，核心竞争力遭严重威胁
- 客户资料、财务数据外泄，影响企业正常经营
- 给外部单位的重要文档无法控制，造成诸多麻烦
- 封USB端口、锁机箱，企业机密文档仍然被泄露

400 000 3720

ITEN

企业数据安全新挑战：

精明的公司明白在当今由数据推动、高度分布化的环境中，有很多严重的威胁亟待解决，其中超过 85% 的安全威胁来自企业内部数据泄密，企业安全本质是以保护技术图纸、财务数据、销售资料、客户信息和经营信息为主的公司机密数据和信息为对象。

核心文档遭遇内部泄密 企业80%的信息安全威胁来自于内部,其中又以内部员工泄密为主。公司多年的研发图纸、科研资料、财务数据、经营数据和客户资料等机密信息公开的存在于服务器和员工电脑中,公司网络内每台电脑就是一个信息流通的水龙头,信息泄密就如开水管。

机密文档流出核心团队 公司最重要的核心资料和文档,需控制在核心的研发小组成员或者核心团队内部使用,如过多人员包括公司其他部门人员的的获取可能会造成不必要的泄密。

外部交流造成信息泄密 与外部的交流必不可少,又需防范核心资料在交给外部人员后造成二次泄密,必须做到不影响正常交流下的读写、打印时效等可管理外发文控制

外设端口泄密如何杜绝 USB端口、打印机、绘图仪等外设无法控制无法保证重要文档图纸的安全,虽然采取了封U口、锁机箱等措施,但文档还是泄露了出去。

缺失信息安全管理规范 信任不等于放任,对员工和管理层的信任并不能成为借口,来掩饰企业时刻面临的安全威胁,建立完善的信息安全保障体系才是企业长治久安之计。

系统概述

安腾反泄密软件以PHOENIX加密技术为核心，集文档加密、权限管理、身份认证、U盘管控、打印控制、外发文控制、内容保护、手机安全、文档备份、日志审计等多种安全功能模块于一体，是解决设计院企业图纸文档泄密问题的专业解决方案。

事前主动防御:反泄密软件对已有的或正在生成的CAD、Office、PDF等各种格式的图纸和文档进行加密保护，被加密的文档图纸只能被授权用户在授权环境（如企业内部）中应用，文档在创建

、存储、应用、传输等环节中均为加密状态,未经授权或脱离授权环境，加密文档均无法打开使用。

事中有效控制: 反泄密软件的加密过程不会因修改程序或进程名，更改保存文件后缀等作弊手段而失效，同时加密文档的复制/剪切/拖放/粘贴等操作也受到限制,向非加密文件中拖放/拷贝/粘贴的操作将被自动禁止。除此以外，安腾反泄密软件对打印机、U盘等存储工具,笔记本电脑均有控制措施，并借助分组策略和身份权限的认证管理等技术进行更细化的设置和保护。

事后溯源补缺:安腾反泄密软件提供日志审计和自动备份功能，前者可以将指定的操作过程详细、完整地记录下来，方便监督检查和问题溯源;后者可以在文件被有意或无意删除或损坏时，通过备份资料及时恢复。文件在备份的传输、存储和恢复过程中均以加密形式存在。

主要功能

功能模块	功能说明	备注
终端安全	移动存储设备管控	可以针对各种移动存储设备进行入与出分开的开放、禁止、加密与不加密的策略设置，同时不影响键鼠等非存储设备的使用
	打印设备管控	可以针对终端打印机、绘图仪等打印设备端口的允许使用操作进行管控
文档加密（文档安全）	透明加密	针对受控终端的文档进行强制加密，无需人工干预，加密文档仅在内部授权环境内可以正常使用，拿到外部无法打开
	智能加密	可以分别针对不同终端的每个程序设置单独设置不同的加密策略，包括打开加密、修改加密、智能加密和不加密四种方式
	手动加密	提供手动对文件进行加密功能，满足特殊人员或者特殊情况下实现文档的保护
	批量加/解密	提供批量对部门和终端的指定类型文件加密与解密功能。可自定义扫描策略
	打印属性	根据安全策略，对被保护文档进行打印控制
外发文安全	权限控制	控制外发文件的只读、另存、打印、截图权限和有效使用时间
	增强管控	实现外发文件绑定电脑、绑定介质（如U盘）、打开次数、打开密码等控制权限
	水印保护	实现打开、打印文档时显示如授权信息等水印功能

文档权限控制	自动部门文件隔离	实现文档的精细化权限管控。生成的加密文档根据策略自动加入权限信息，如：文档在不同部门的打开、编辑、打印等权限控制
	手动部门文件调整	可以手动指定某份文件的权限，如哪些人可以看，哪些人可以修改，哪些人可打印等。亦可对原有文档权限作出调整
内容安全	复制粘贴保护	实现加密文档内容无法向未加密文档内复制粘贴，但不影响未加密文档内容向加密文档内复制粘贴
	截屏控制	防止终端通过截屏等方式泄露受保护的文档内容
	虚拟打印保护	控制通过虚拟打印机方式输出的文档
	增强打印保护	详细记录打印日志，并对打印文档首页拍照留底
流程审批	单级审批	实现对涉密文档的解密、外发、权限调整等操作的流程审批，可自定义审批人的管理权限
	多级审批	可实现多级审批、审批与解密分离等的复杂特殊流程
	异地审批	支持跨地域分布式部署结构的审批流程
	自定义审批流程	可以根据企业的需要，可自定义审批流程
应用安全	业务应用系统安全	防御应用系统落地数据的泄密风险，提供上传解密下载加密兼容方案
移动安全	移动安全	保护涉密文档在移动端的安全使用，同时提供安全水印、防复制等安全保护控制
移动审批	手机审批	可通过手机实现在公司以外随时实地的对解密进行审批管理
离线管理	离线策略管理	根据出差情况，允许用户在出差笔记本中继续使用加密文件。并设置周期管理，权限管理。限制离线操作，确保安全性
邮件白名单	邮件白名单	对符合白名单的邮件发送者或接收者，自动解密其发送的附件
程序管理	程序黑名单	设置终端程序黑名单，控制程序运行，辅助管理员工行为
授信介质管理	U盘白名单	对符合白名单的U盘，其不受移动存储设备策略所控制
审计与泄密分析	日志审计	提供客户端、审批端、服务器端详细操作日志，方便后期监督检查和问题溯源。
	文件审计	查询文件流水日志，回溯员工创建、拷贝、流转文件数据等操作痕迹，深度发现、识别企业内部数据安全层面各类风险，精准追溯事故源头。
	数据安全态势分析	支持用户行为分析与意图预警，展示用户风险 行为报告，检测终端异常行为，安全事件发生之前，预警风险。
系统兼容	认证平台	支持按硬件号认证用户，也支持AD域、OperLDAP及其他第三方认证方式，根据需要采用混合认证模式
	平台集成	可与多种应用系统如PDM、PM、OA、CRM、ERP等兼容集成

部署效果

在不改变原有工作习惯和工作流程的情况下，保护机密数据安全的同时，保证员工的工作效率，确保内部文档数据安全，防范数据泄密并确保遵从合规性。

1）切断泄密途径，控制U口，**重要图纸文档拿不走**；

2）实时文档加密，带到外面打不开，**拿走也没有用**；

3）重要文档外发控制权限，**虽给对方却能控制；**

4）操作记录解密情况记录在案，**随时追查审计**；

5）**规范管理**流程，责权更清晰，管理更流畅。

资质证书客户案例

政府机关

海南核纪委监察厅

广西人大常委会

南宁国土资源局

珠江水利委员会西江局

集团用户

中国移动

中国黄金集团

中光学集团

中铁大桥局

教育

清华大学天津高端装备研究院

郑州大学综合设计研究院

河南理工大学

生产制造

力神电池股份有限公司

牧羊集团有限公司

瑞丰钢铁（集团）有限公司

国盾量子通信

医药行业

正大天晴药业集团

上海现代制药股份有限公司

国药集团川抗制药有限公司

设计研究院

中国科学院

中国地质科学院

林产工业规划设计院

河南省城乡建筑设计院有限公司

关于安腾

安腾（ITEN）软件有限公司长期专注政府和企业计算机信息反泄密研究，为企事业单位提供领先的计算机信息反泄密解决方案。安腾(ITEN)是中国计算机信息反泄密软件和文档加密软件的始创者和领导品牌，旗下拥有"文档守望者"、"凤凰卫士"、"安腾"等多个品牌产品线，产品涵盖文档加密、移动介质管理、内网安全、终端安全、外发文安全、数据备份、信息安全等领域，能够满足不同行业和规模客户的信息安全保密需求。

安腾（ITEN）始终专注于透明加密软件的研发，是国内最早从事文档、图纸、代码等透明加密的研发厂商，对于加密软件有着深刻的理解。 安腾力求产品的部署快速、使用简洁、功能实用、运行可靠，十几年来得到客户的广泛认可和信赖，客户遍布政府、军工、设计研究院、电力、机械、电子、化工、服装、广告等诸多行业。安腾（ITEN）已成为信息安全领域"计算机反泄密软件"的代名词。

安腾（ITEN）坚持走专业化发展的道路，坚持"技术领先、服务先导"的经营理念，走自主研发和持续创新之路，保持产品和技术的领先。致力成为中国信息安全领域的标识型高科技企业。

"用专业技术保信息安全，为保护用户的利益而不断创新"是安腾一直坚持的使命。安腾从深刻理解企业信息安全与知识产权保护需求出发，以先进的技术、专业的服务，满足用户需求，为用户创造价值为己任致力成为用户信任的信息安全技术专家和长期合作伙伴。

联系我们

安腾（ITEN）软件有限公司

地址：郑州市西三环283号国家大学科技园（东区）11号楼14层
热线：400-000-3720　传真：0371-65751007
网址：www.iten.com.cn

安腾微信公众号