文德森
wondersun

全面守护企业核心数据

Comprehensively safeguard the security of enterprise core data

目　录

文德森
wondersun

为什么企业需要关注数据安全?

政策驱动

《**中华人民共和国网络安全法**（*2017年6月1日起施行*）》对数据的安全要求

第二十一条 国家实行网络安全等级保护制度。网络运营者应按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经 授权的访问，防止网络数据泄露或者被窃取、篡改。

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据 泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。

第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不 能复原的除外。

《**中华人民共和国数据安全法**（草案）*2020年7月3日提出*》对数据的安全要求

第十九条 国家根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者公民、组织 合法权益造成的危害程度，对数据实行分级分类保护。各地区、各部门应当按照国家有关规定，确定本地区、本部门、本行业重要数据保护目录，对列入目 录的数据进行重点保护。

第四十二条 开展数据活动的组织、个人不履行本法第二十五条、第二十七条、第二十八条、第二十九条规定的数据安全保护义务或者未采取必要的安全措 施的，由有关主管部门责令改正，给予警告，可以并处一万元以上十万元以下罚款，对直接负责的主管人员可以处五千元以上五万元以下罚款；拒不改正或 者造成大量数据泄漏等严重后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

风险驱动 涉及8类软件公司及具体场景

政府与公共事业

政府机构：公民身份信息、国家机密需符合分级保护要求。

能源/电力公司：基础设施数据可能涉及国家安全。

医疗与生命科学

医院/诊所：患者病历、诊断信息。

医药研发公司：临床试验数据、专利配方需防止商业间谍窃取。

互联网公司

软件开发企业：源代码、算法、未发布产品设计需防内部泄露。

大数据公司：用户行为数据、隐私信息需匿名化处理。

制造业

汽车/电子/高端制造：设计图纸、生产工艺可能被竞争对手窃取。

专利持有企业：需监控核心技术的文档流转与访问权限。

政府与公共事业

银行/保险/证券：客户账户信息、交易记录、信用报告等需严格保密。

零售与电商

电商平台：用户订单、地址、支付信息需防数据库泄露。

会员制企业：客户偏好数据是商业竞争核心资产。

专业服务行业

律师事务所/会计师事务所：客户案件、财务数据需保密。

咨询公司：企业战略报告等敏感文档需限制外发。

外包服务

外包公司：接触客户敏感数据（如财务、客服）需严格管控。

共享办公空间：多企业混合环境易发数据交叉泄露。

核心资产-信息数据

设计图纸
技术资料
客户资料
销售数据
生产计划
车间图纸
财务数据
资产信息
人事资料
测试数据
经营数据
机密文档

核心资产泄密的原因及途径

主动泄密

私自拷贝、外带敏感数据
越权访问敏感数据
私自外发敏感数据
私带设备接入内网，下载敏感数据
打印、拍照、录像

被动泄密

设备（电脑、U盘等）遗失、维修、废
程序误操作、误发送
敏感数据保管不当
感染病毒、木马

文德森
wondersun

大家是怎么做的?

数据安全定义：是指采取必要措施，有效保护和合法使用数据，并使数据处于安全状态的能力

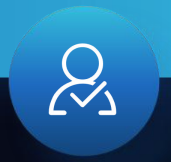
目前市场上通过技术手段解决方案主要有以下四个方面

网络隔离技术

通过虚拟专用网（virtual Private network，VPN）等网络隔离技术，配合防火墙、安全组、网络流量分析等综合手段，保护可信网络区域内的数据库等核心资产

数据加密技术

包括磁盘加密、文件加密、传输加密等技术方案。可以保护数据不受数据泄漏源的影响，也可以在数据离开企业内部后有效防止数据泄漏



权限控制

即身份验证（authentication）、授权（authorization）

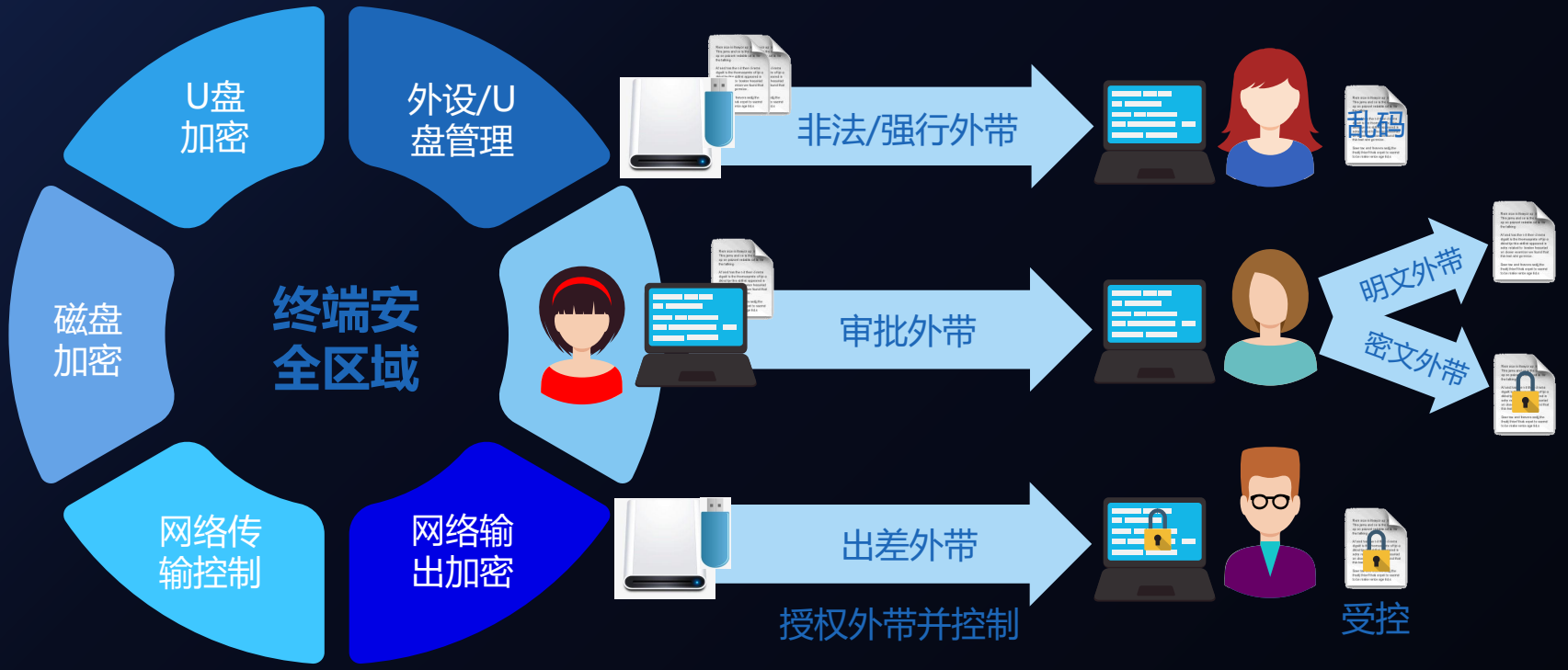
DLP

基于数据内容的防泄漏保护(DLP)。DLP以内容识别为核心，基于敏感数据内容策略定义，监控数据的外部通道，审计或控制敏感数据传输

文德森
wondersun

我们怎么做的?

数据安全解决方案



我们是把杀毒反过来做成防泄密

文德森 wondersun

传统杀毒

解决进来的数据安全问题

- 进入终端的文件自动进行病毒扫描
- 打开可疑文件会自动隔离，阻止其运
- U盘、移动硬盘接入自动扫描
- 扫描文件夹

VS

解决出去的数据安全问题

创新防泄密

- 通过网络外发的文件自动加密
- 拷贝到U盘、移动硬盘的文件自动加密
- 打印文档自动添加水印
- 浏览文件自动添加防拍照水印
- 加密文件夹-自动加密文件，防止明文二次扩散
- 包含传统文档加密所有功能（文件加密、控制打印、时间、次数等等）

控制进来的，叫杀毒；控制一切出去的，这种叫防泄密软件，比如我们

新一代数据防泄密系统- IDLP

- I nnovative 创新
- D ata 数据
- L eakage 泄露
- P revention 防止

我们的产品通过精准定义数据使用范围，结合审计、加密、访问控制等措施强化数据保护。基于风险策略，构建了以数据和用户身份为核心的动态访问控制系统，推动企业安全架构从传统防火墙模式转向更灵活的动态防护。

系统通过分析用户行为，实现数据加密、完整性保护、文件安全、网络监控、打印管控、截屏防护、USB设备管理及固件更新防泄漏等功能，全方位保障数据安全，助力企业稳健发展，促进公平商业竞争。

我们有啥不一样?

稳定高效

核心驱动程序通过微软verifier
认证，运行可靠有保障

高性价比

价格低，化繁为简，赋能中小
企业零门槛加密

全场景封堵

智能围猎12类核心威胁场景：
从离职泄密到APT攻击防御

文德森
wondersun

产品定位与核心价值

基于数据全生命周期的数据安全框架-橙色部分为我司信息安全可控领域

	数据生产	存储	使用	传输		归档	销毁
安全制度	安全策略	资产管理制度	访问控制管理制度	通信安全管理制度		归档管理制度	销毁管理制度
安全组织	信息安全委员会	入职安全管理	安全事件响应机制	密码管理		安全标准管理	销毁流程
安全审计	标准化审计	权限审计	操作审计	手机审计		日志审计	销毁审计
安全运维	标准化管理	权限管理	访问控制	安全事件监控		归档管理	销毁管理
数据安全 应用安全	开发安全工具	数据库安全	云安全	数据防泄漏	邮件安全	备份恢复	数据清除
	应用系统日志监控	数据操作审计	云数据、应用安全	终端DLP	证据收集	数据备份	残留数据清除
	漏洞扫描	文件加密	云服务监控	应用审计	网络DLP	数据集中归档	配置清除
主机安全	补丁管理	虚拟机安全	数据中心防病毒	移动终端安全	主机标准化	准入控制	数据清除
	恶意代码防护	数字证书	云主机安全	操作行为控制	USB控制	安全域	硬盘格式化工具
	双因素认证	物理层加密	云堡垒机	系统审计	打印控制		
网络安全	防火墙	IPS/IDS	APT	数据传输安全	安全态势感知	网络审计	数据清除
	堡垒机	网络隔离	Anti-DDOS防护	网络安全网关	邮件防火墙	VPN	残留数据清除
	双因素认证	应用防火墙		网络漏洞扫描			配置清除
物理安全	视频监控	UPS/空调	物理分区	负载均衡		数控中心	介质处理
	门禁系统	环境监控		设备冗余		灾备中心	打孔设备
	建筑安全					两地三中心	粉碎设备

技术为核，安全为魂

一键式安装

无感守护 开箱即用 零学习零运维的安全进化

安全稳定

不封闭网络 不封闭外设端口 不改变文件格式

轻量高效

10MB内存占用 GB文件秒开 业务流畅无延迟

无感知加密

自动加密 操作零干扰

驱动级加解密

技术的特点是自动性透明性和强制性

核心功能模块全景

外发加密

- 用户通过网络外发文件自动加密（亦可根据关键字识别加密），只有授权计算机才可以打开，私自外带或者未授权无法打开

文件夹加密

- 针对任意文件夹进行访问控制或实时自动加密该文件夹及其子目录下所有文件

文件加密防篡改

- 针对任意文件进行加密并可赋予只读、编辑、打印、预览时间范围等权限控制。又可提供防篡改功能，指定加密文件仅通过特定应用系统才能读取

编辑文档自动加密

- 任意文档通过编辑后，保存时自动加密

外设控制

- 针对通过U盘、移动硬盘、手机等外设进行数据传输时，输出数据进行加密，防止信息外泄

屏幕水印

- 出现使用手机、相机等对屏幕进行拍照的风险时，通过隐形水印可以具体到某个终端

外发审批

- 通过流程审批对需要外发的文件进行申请，审批后外发则为明文，保留审批记录

打印水印

- 针对打印的文件自动增加水印，防止非法传播、可溯源

360°守护企业核心数据

离职人员泄密

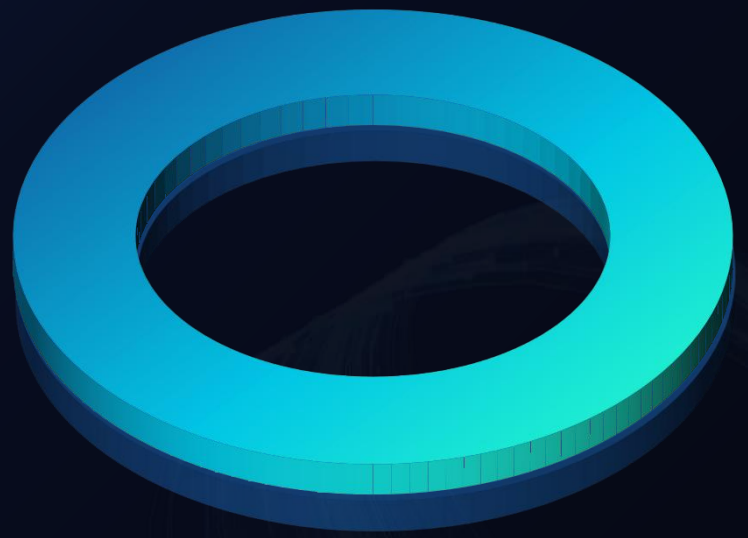
员工离职时设定锁定权限，防止资料外流

越权访问泄密

可以根据需要，设置不同部门、不同操作员的文档阅读权限

商业间谍泄密

国际标准AES加密算法，256位高强度多重密钥，文件破解率为零



外设拷贝泄密

未经授权环境100%不可读

网络传输泄密

数据已加密，保障网络传输过程安全

员工打印泄密

可以设定加密文件禁止打印

文德森
wondersun

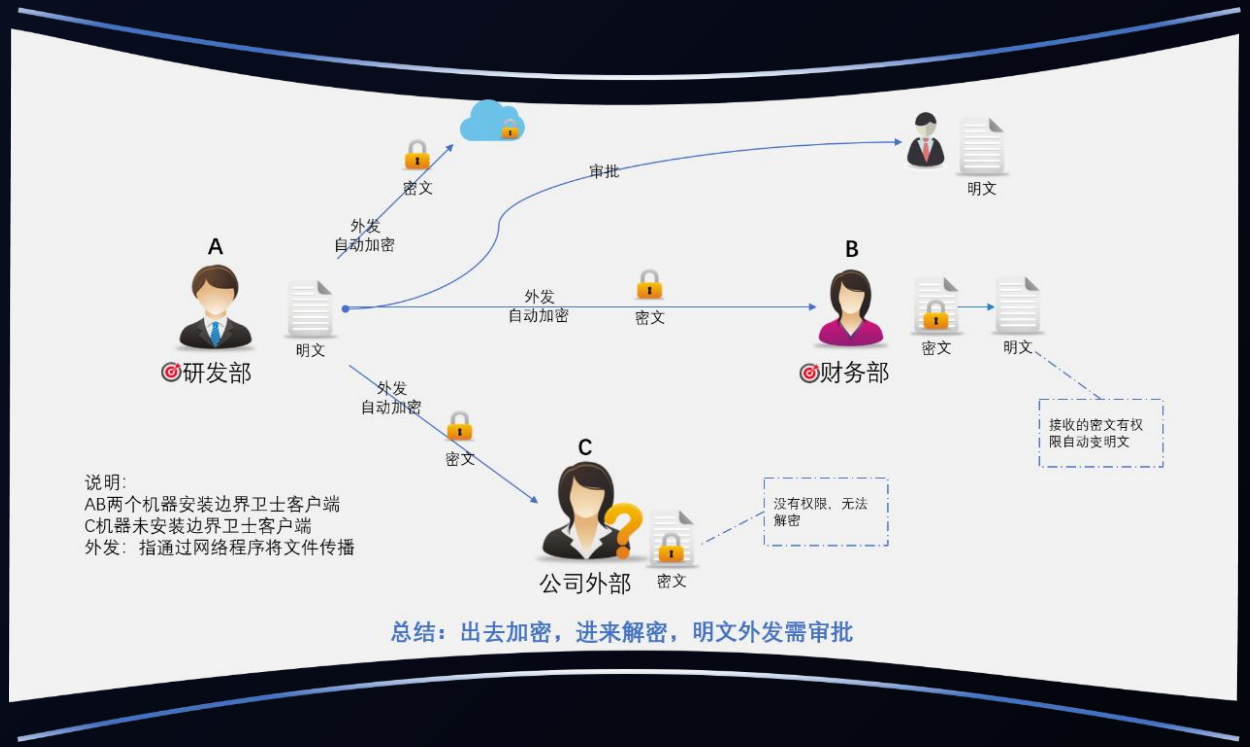
应用场景解析

应用场景-解决员工无意识泄密风险问题

实现效果

员工外发的数据文件都会被强制自动加密（经过审批后可以外发明文），接收端如果有权限解密，则会自动解密，如果没有权限解密，那么接收端收到的数据文件将无法使用。

- ✓可以解决多部门间数据阅读权限隔离的问题；
- ✓可以根据数据需要，设置不同部门、不同操作员的阅读权限，即授权指定部门或用户只能访问指定部门的文件，其他文档即使被获取到，也无法被打开，有效避免因误发文档导致泄密；
- ✓可以识别外发文档内容（office类型或pdf类型）进行关键字查询，然后禁发外发。

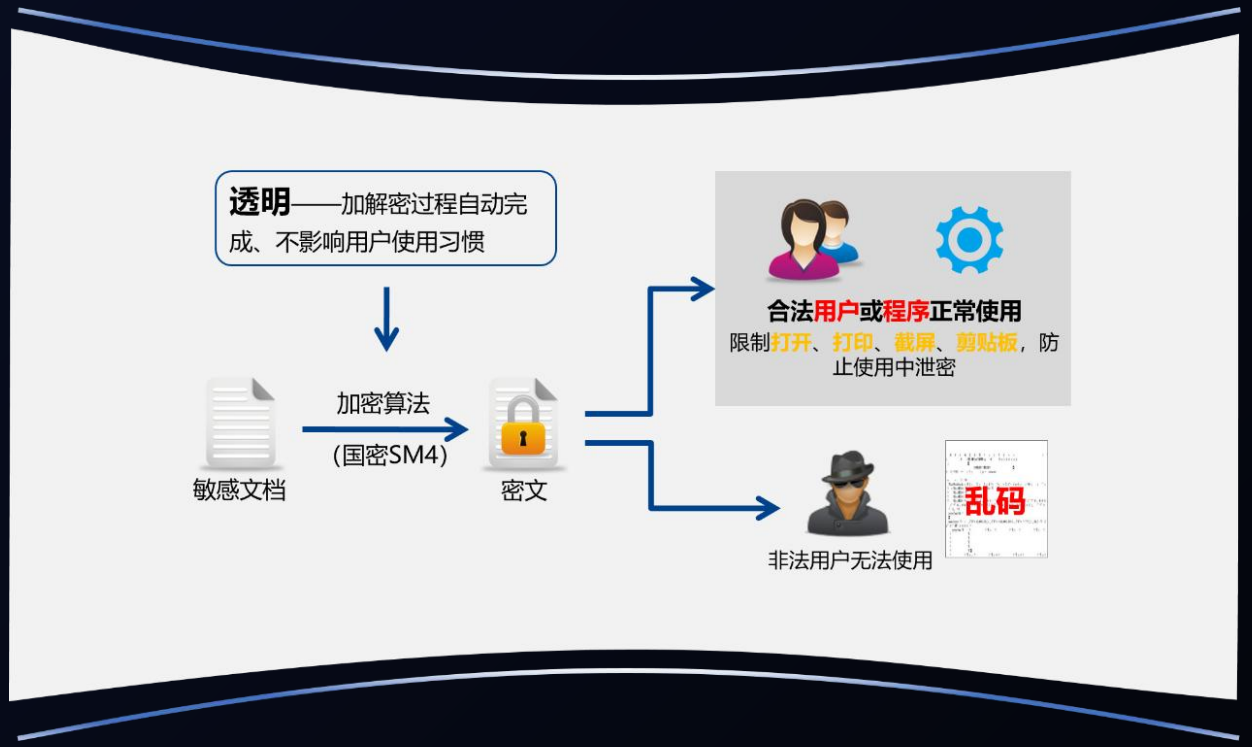


应用场景-解决文档二次扩散泄密问题

实现效果

敏感文件通过手动或自动方式完成加密保护，生成一个加密文件。用户在使用此加密文件时，需要使用账号、密码或硬件绑定打开（没有账号和密码无法浏览加密文件），且打开后受到时间、打印、截屏、拷贝、保存等权限控制。同时，用户使用过程中，系统对时间、IP等日志信息实时详细记录。

- ✓ 解决文档（合同、方案、代码、财务报表等敏感文档）扩散传播泄密问题；
- ✓ 可以绑定U盘编码进行加密。加密数据只能在指定U盘中打开；
- ✓ 可以绑定机器硬件码进行加密，这样加密数据只能在指定机器上打开。



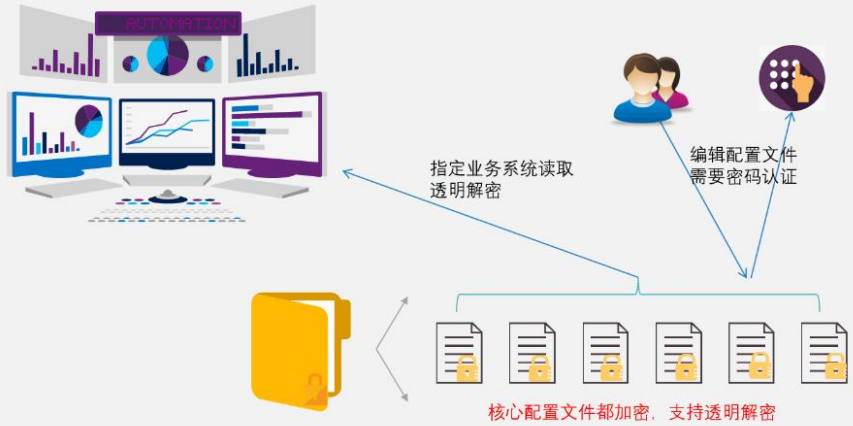
应用场景-解决关键数据安全性问题

实现效果

《关键信息基础设施安全保护条例》自2021年9月1日起施行。目的为了保障关键信息基础设施安全，维护网络安全。法律依据《中华人民共和国网络安全法》。

定义：公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

要求：针对关键基础信息数据进行加密，防止关键数据被恶意篡改或泄密；加密数据编辑时需要使用密码进行认证后才能编辑，编辑的过程中数据始终处于加密状态；当网络出现网络故障，导致防泄密客户端和服务器无法通信时，也要保障业务系统正常使用。



- ✓ 用户可以指定一个或多个文件夹（存储关键数据的）为加密文件夹；
- ✓ 文件夹内文件自动加密，新增文件自动加密；
- ✓ 查看或编辑文件夹内的文件需要账号及密码认证；
- ✓ 查看或编辑文件过程中文件始终保持密文状态；
- ✓ 编辑后保存文件时自动加密，整个过程中不产生任何临时明文文件；
- ✓ 文件夹内的加密文件可以指定任意业务系统透明解密，无需认证；
- ✓ 支持加密文件绑定指定U盘才能打开；
- ✓ 支持加密文件绑定指定电脑才能打开。

应用场景-解决通过手机获取泄密问题

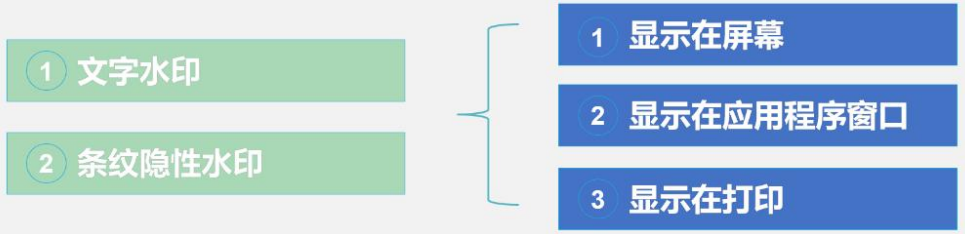
实现效果

实现核心部门终端电脑防手机拍照的泄密风险

随着智能手机的广泛使用，拍照过程从原来的繁琐复杂变为简单易行。在信息安全领域，通过屏幕拍照、录像等手段窃取单位内部敏感信息已逐渐成为当前重要信息泄露的主要途径。

边界卫士系统通过屏幕隐性水印模块，可实现在终端电脑上显示特定隐性水印。非法用户通过手机、相机等对屏幕进行拍照后，通过先进的算法分析，轻松查出泄密电脑，从而在获取照片时，可以追溯源头。

- ✓ 用户开机后，屏幕就会有显性或隐性水印，防止用户拍照泄密；
- ✓ 用户打印文档时可强行添加水印后打印。



应用场景-解决文档传播后溯源问题

实现效果

电子文档隐写是对涉密文档进行处理后传输，保证每份文档的唯一性和扩散路径可控可溯源，能够高效快速查询文档的使用和扩散过程。当泄密事件发生时，能够快速定位溯源，为追责提供依据，从而提高涉密文件的安全性。

- ✓ 系统会主动将诸如文档编写人ID、文档编写时间、终端IP地址唯一标识信息作为隐形数字水印内容添加到电子文档中；
- ✓ 用户将文档进行流转时又会写入新的隐形数字水印；
- ✓ 通过提取整个水印内容，可以展示出整个文档的流转过程。

应用场景-解决终端外设（打印机、U口）涉密问题

实现效果

防止用户通过终端打印、U口、蓝牙、拍照等方式进行信息泄密。

- ✓ 在禁止打印或允许打印文档时，系统强制在页眉、页脚、页中添加水印；
- ✓ 允许打印时，系统详细记录每一次打印操作的时间、用户、文件名、页数等信息，方便管理员预防安全风险，追溯打印内容；
- ✓ 通过U盘拷贝数据时，系统可实现：强制加密后拷贝，禁止使用U盘，仅能使用注册U盘；
- ✓ 系统可以禁止终端电脑接入无线网络、蓝牙或便携设备；
- ✓ 在打开加密文件时，系统显示防拍照水印。

应用场景-解决企业文档集中存储、安全共享问题

实现效果

集中存储

通过文档云存储系统，严控企业私有云的文档管理系统，保证企业文件的集中性、私密性和安全性。以集中管理模式改进内部分享效率、降低管理成本，提升合规与安全风险管理水平。系统主要功能包括上传、下载、移动、多维度（目录、标签）管理、全文检索、个人收藏、关联引用、分类排序、版本管理、在线浏览、离线加密等。

安全共享

企业的电子文件资产是日积月累的宝贵经验。为了解决数据安全性，研发资料、技术资料等很多文件仅能在线阅读。如果个别文件一定需要下载阅读，则需要使用边界卫士解密客户端进行打开，阅读过程中通过沙箱技术可防止打印、另存、截屏等泄密动作。

- ✓ 企业各类文档，通过设置权限可线上查阅，实现集中线上管理；
- ✓ 系统将下载文件自动加密，通过解密客户端，实现解密后阅读，同时可实现阅读过程中受禁止打印、另存、截屏水印等数据严控操作；

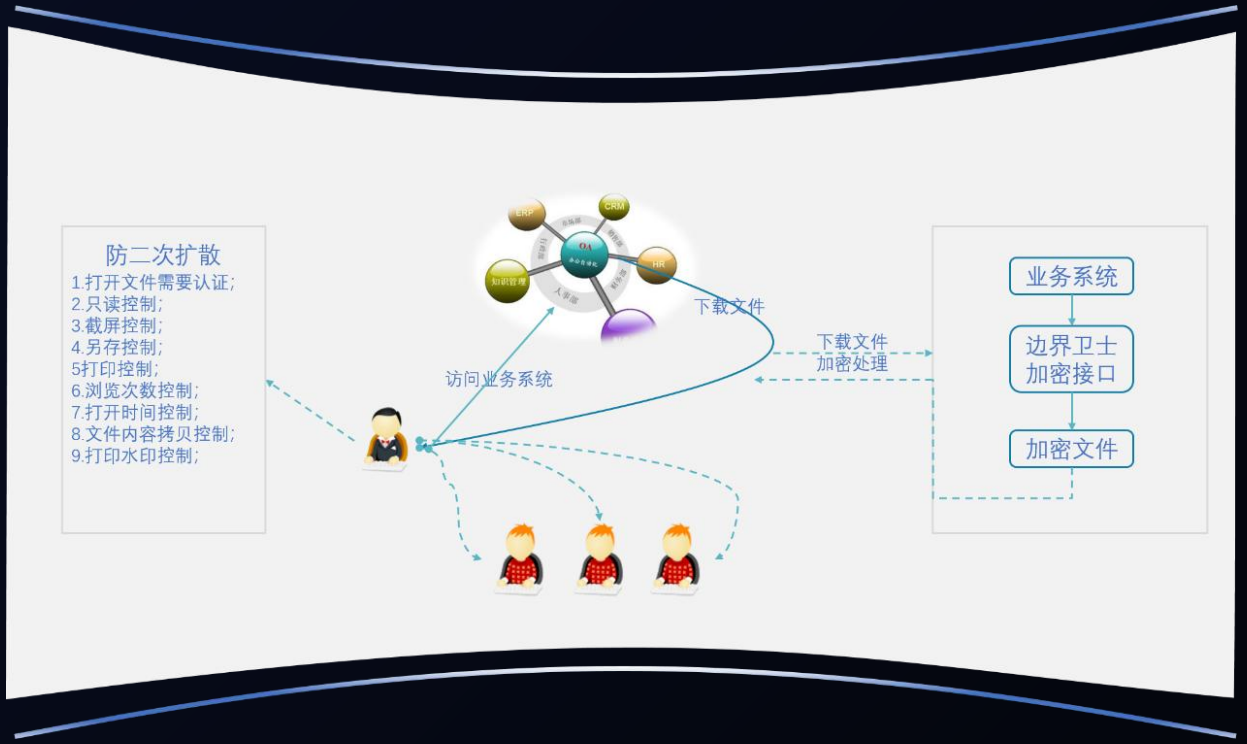
应用场景-解决业务系统（OA ERP等）数据扩散泄密问题

实现效果

待保护的业务系统下载文件时调用边界卫士加密接口，使业务系统下载的文件自动加密，用户拿到下载的加密文件后，必须使用防泄密客户端才能打开，打开加密文件受认证、编辑、打印、截屏、时间等权限控制。

系统实现被下载文件的阅读记录日志。

- ✓ 可以实现企业业务系统下载的数据是加密的，用户进行查看加密数据时受到时间、地点、软硬件、打印等权限控制。

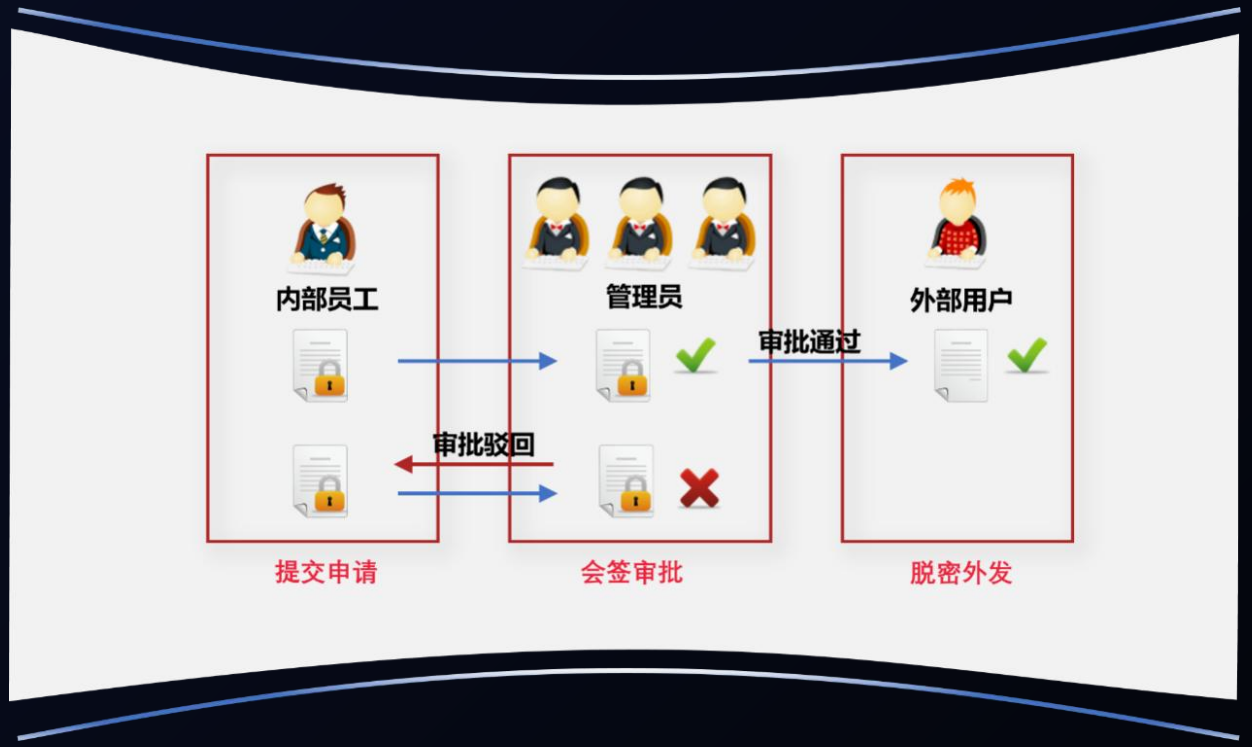


应用场景-解决文件外发/脱密审批问题

实现效果

数据明文外发/密文脱密须经审批后执行，审批过程遵循严格的审批流程和制度约定，同时可对审批行为及脱密的数据进行审计，并对审计记录进行集中管理。

- ✓ 流程审批即时消息提醒，提高了流程审批效率；
- ✓ 流程审批可以通过企业微信进行推送，且可直接在企业微信消息中进行审批和查看待审批文件；
- ✓ 支持Web审批方式，提高流程审批便捷性；
- ✓ 支持移动终端（如：iPad、iPhone）流程审批；
- ✓ 审批人员审批时需要输入合法口令，提高审批安全性；
- ✓ 可查询所有发起审批、待审批、已审批等信息；
- ✓ 审批时可在线查看或者下载文件内容。



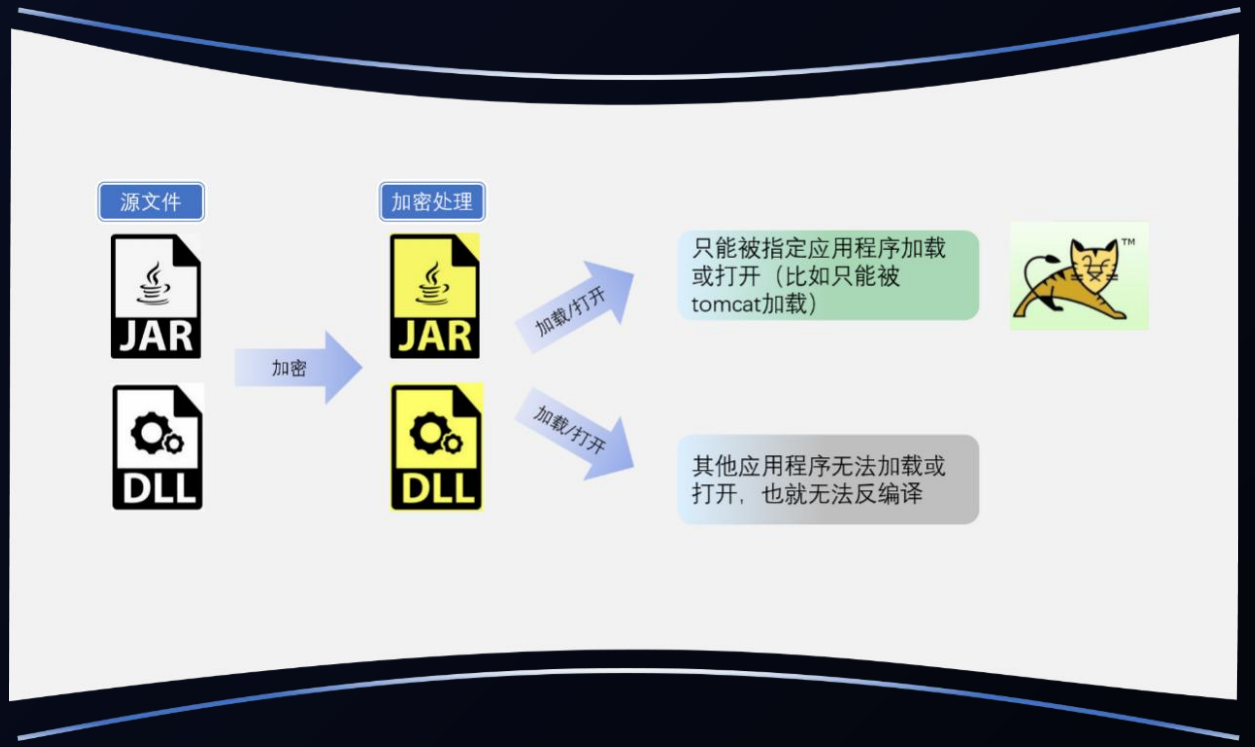
应用场景-解决代码被反编译泄密问题

实现效果

系统可实现各种代码混淆加密、防止反编译

系统可实现多种加密技术，快速完成代码保护，防止反编译和篡改。

系统解决软件厂商核心代码被破解、反编译等问题。



应用场景-解决核心资产服务器准入控制/运维安全问题

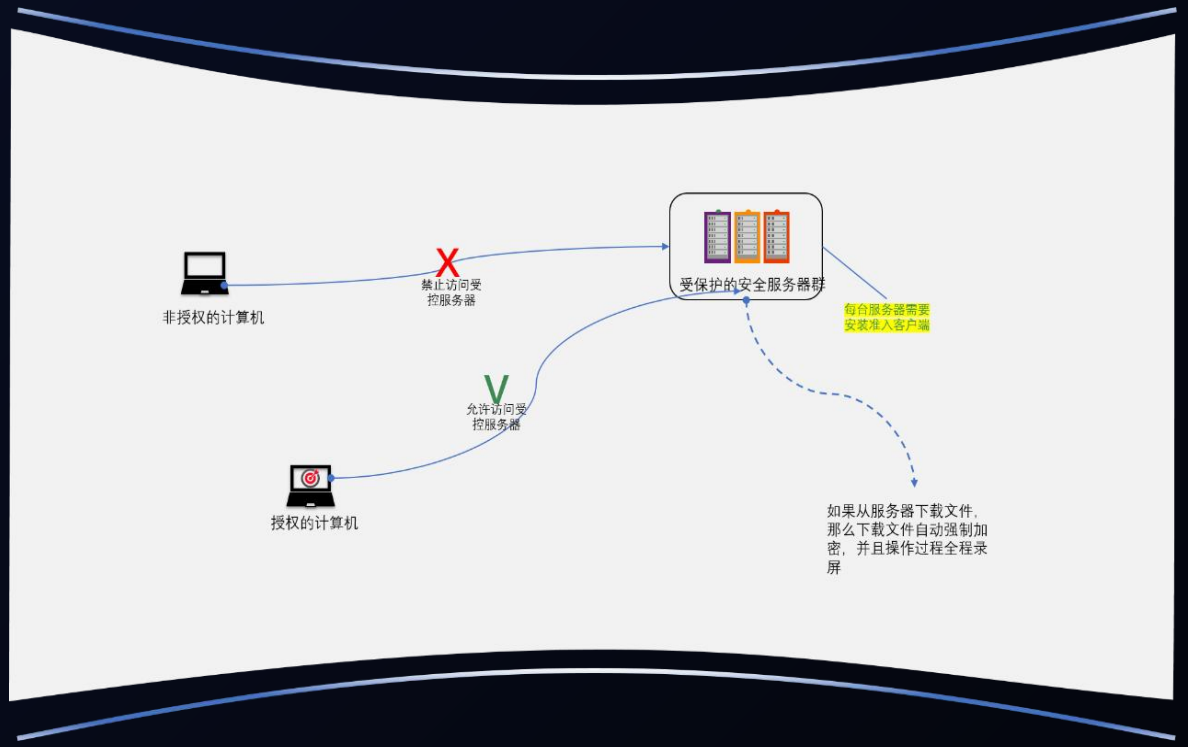
实现效果

解决核心资产服务器数据泄密风险问题：

用户无需改变任何网络结构，仅在服务器安装部署准入软件，即可实现仅有经过授权的计算机才能访问服务器指定端口，且轻松实现将服务器下载的数据自动加密，加密文件仅能在指定的电脑终端和时间内使用。

解决运维过程数据泄密问题（如：移动、联通、电信及其三产公司服务器数据泄露问题）

运维的终端计算机必须安装防泄密客户端才可以进行运维，运维过程中受录屏、拷贝加密等权限控制，被拷贝数据以作加密处理。



系统可定制数据包括：

在指定的硬件设备上使用；

定制数据使用期限。

解决方案对比

技术方案	方案要点	安全性	用户体验	优缺点	说明
物理隔离	1、对网络进行隔离，不允许连外网 2、使用专用终端，如专用电脑或桌面云 3、封堵U盘、打印机、随身WiFi等外设外联	高	较好	成本过高	1、用户操作体验较好，基本不受影响 2、效率略微降低，需在不同环境切换 3、整体方案重，仅适用于极少数特定场景
DLP控制	1、基于策略，识别并阻断敏感数据外发 2、可从终端、网络、邮件层面进行控制 3、需要先进行数据的梳理，并制定策略	一般	较差	难落地	1、周期长、难度大、工作量大 2、误报、漏报问题普遍，大量无用告警和日志 3、用户体验和工作效率均受较大影响
传统加密	1、传统的终端防泄密是以加密为主，对磁盘中的文件进行逐一加密 2、基于核心应用生成的文件进行加密	高	一般	易落地	1、非授权终端、环境无法打开加密文件 2、特殊文件、应用加密效率低，影响正常工作
我	1、只对输出文件进行加密或审计 2、对敏感文件提供加密工具	高	较好	易落地	1、用户使用过程无感知 2、只要不外发文件，用户在使用过程中，是没有改变任何使用习惯的

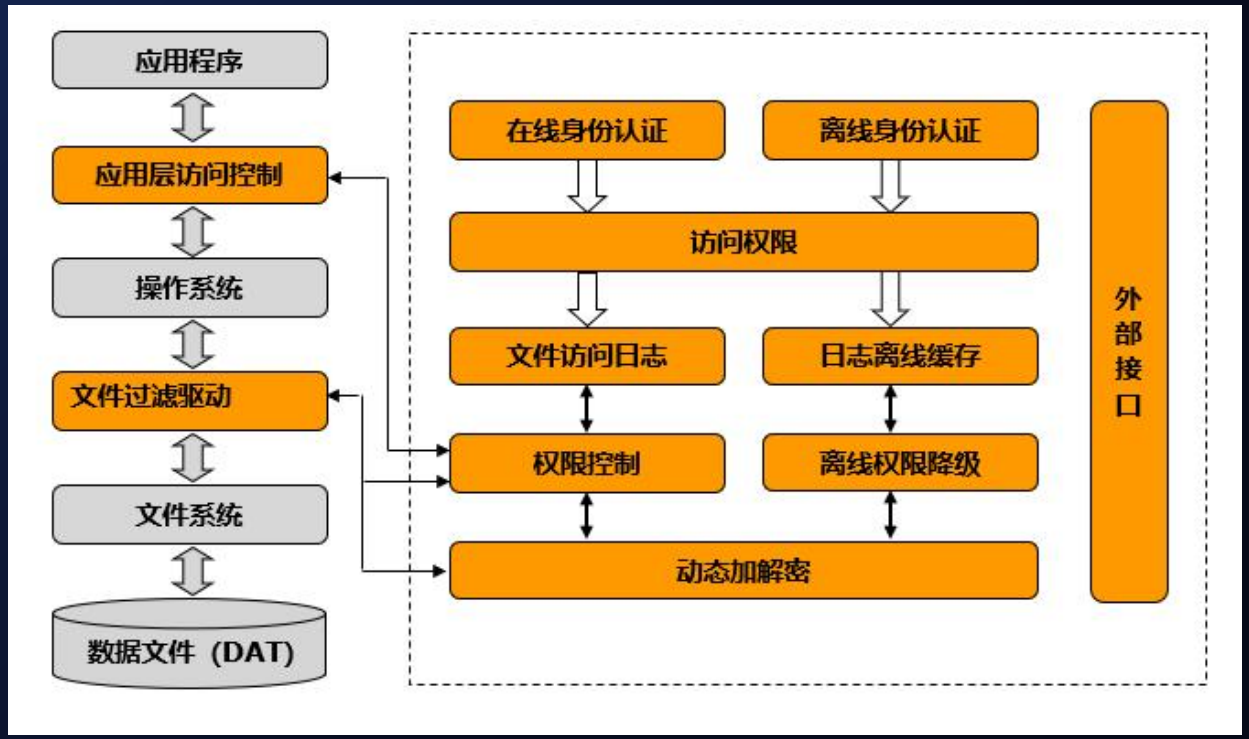
解决方案对比

技术方案	方案要点	安全性	说明
应用层加密	应用层加密通过windows的钩子技术，监控应用程序对文件的打开和保存，当打开文件时，先将密文转换后再让程序读入内存，保证程序读到的是明文，而在保存时，又将内存中的明文加密后再写入到磁盘中	低	与应用程序密切相关，它是通过监控应用程序的启动而启动的。一旦应用程序名更改，则无法挂钩。同时，由于不同应用程序在读写文件时所用的方式方法不尽相同，同一个软件不同的版本在处理数据时也有变化，钩子透明加密必须针对每种应用程序、甚至每个版本进行开发。应用程序为了防止黑客入侵设置了反钩子技术，这类程序在启动时，一旦发现有钩子入侵，将会自动停止运行，所以应用层加密很容易通过反钩子来避开绕过。应用层透明加密技术（钩子透明加密技术）开发容易，但存在技术缺陷，应用程序版本变更容易产生不兼容，而且容易被反Hook所破解。
驱动级加密	驱动层透明加密技术工作在windows的内核层，他工作于windows API函数的下层	高	当API函数对指定类型文件进行读操作时，系统自动将文件解密；当进入写操作时，自动将明文进行加密。由于工作在受windows保护的内核层，运行速度更快，加解密操作更稳定，但开发难度大。

实施前后对比

管控内容	实施前	实施后
终端边界出口防护	用户可以通过网络、usb口、串口、蓝牙、打印机等方式将数据泄密	用户通过网络方式传输文件可以做到审计、禁止、强制加密等控制手段 通过usb口可以做到审计、禁止、强制加密等控制手段以及授权认证企业内部u盘方式，让用户只能在企业内部用户特定u盘 禁用蓝牙传输 识别串口传输数据，禁止疑似源码数据外泄 打印机可以控制禁止打印、指定账户打印、打印加水印等方式实施控制
数据加密	数据传播无法控制	可控制数据的知悉范围，做到从数据的产生到销毁的全生命周期管理 打开需要授权认证，浏览有监控，操作有限制（禁止拷贝、复制、另存等等），超过使用周期自动销毁
数据或配置文件防篡改	大型系统，比如铁路运行图的配置文件，可以任意修改	对核心的配置文件进行加密处理，用户如果编辑必须通过账号密码认证后才可以修改 加密的配置文件针对大型系统是透明的，读取时会自动解密
数据使用时绑定usb设备	usb内的数据可以任意拷贝，导致扩散	数据只能在指定u盘内使用，离开u盘后无法打开 数据被使用时，无法拷贝、截屏、录屏、另存 可定制数据使用时间范围，以及使用时是否显示屏幕水印
档案管理/OA等业务系统定制开发	公文系统起草文件无法有效控制其泄密	公文系统从起草文件开始，实施全过程正文及附件加密处理，防止公文发布前提前泄密
终端文档云备份	终端文档无法有效分类归档，员工离职后，工作成果无法有效保留	根据文件内容、页眉、页脚等内容自动进行识别分类归档到云空间进行备份，可有效收集员工工作成果
usb口控制	政府或企业终端u口没有管控，用户随意使用各种u盘，导致病毒及数据泄密	只能使用指定u盘，并记录使用记录，或禁止任意u盘使用

技术架构



- 通过文件过滤驱动技术，实现动态、透明加解密功能；
- 结合内核文件过滤驱动技术和应用层访问控制技术，实现细粒度的权限访问控制功能；
- 记录用户对文件的访问操作，定时传送到加密系统统一存储、分析、展现；
- 通过外部接口，统一从加密系统获取权限信息，并进行用户的身份认证和单点录。

技术应用

文件过滤驱动技术	内嵌至操作系统内核层，可对除操作系统文件以外的其他任意文件类型进行加解密处理
磁盘过滤驱动技术	利用磁盘设备过滤驱动，可对包含操作系统在内的任意存储扇区数据进行加解密处理
虚拟磁盘驱动技术	通过内核驱动程序将文件虚拟成独立的逻辑盘，该逻辑盘具有与普通磁盘相同的特性
内核HOOK技术	通过HOOK内核有关组件， 能够对USB存储设备进行动态加解密和控制各种计算机外设
网络过滤驱动技术	利用网络过滤驱动实现对网络的完全控制，有效防止非法网络接入、外联
网络协议过滤技术	通过过滤网络协议，能够根据安全策略对网络数据动态加解密和细粒度的控制
沙箱隔离技术	采用主流的沙箱技术，实现应用进程之间的隔离，防止数据传输

文德森
wondersun

部署与运维方案

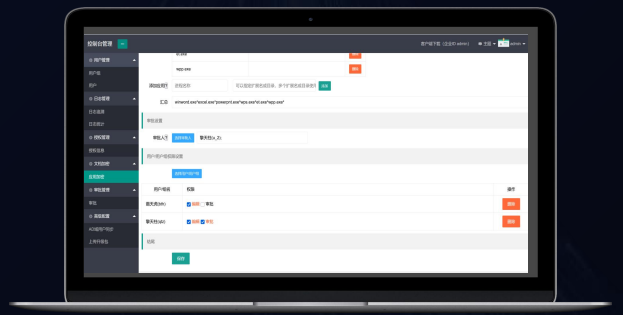
组成架构

一台本地或云端服务器 windows server版本

- ✓ 存储系统数据
- ✓ 管理系统策略

任意电脑浏览器

- ✓ 查看系统数据
- ✓ 制定管理策略



终端电脑安装防泄密客户端

- ✓ 执行系统策略
- ✓ 收集数据，形成日志

文德森
wondersun

谢谢 观看