江民数据保护及防泄漏系统解决方案

北京江民新科技术有限公司

二〇一五年十一月

版权声明

免责条款

本文档仅提供阶段性信息，因市场情况变化迅速，所含内容可根据产品的实际情况随时更新、修改，恕不另行通知。所以，本文档仅供参考使用，不提供任何形式的担保，如因文档使用不当造成的直接或间接损失，本公司不承担任何责任。

信息反馈

地址：北京市海淀区蓝靛厂金源时代购物中心 B 区 2#B 座 701 室
邮编：100097
电话：010-82511166　　传真：010-82511199
邮箱：kvnet@jiangmin.com

目 录

1. 概述与背景

1.1. 信息安全现状

随着信息化的迅猛发展，各行各业都在利用信息化提升企业的核心竞争能力，提升企业办公的效率。由于信息化的灵活和方便，改变了企业传统办公方式，重要核心资产变成电子资料，可以通过 U 盘、邮件、网盘、内部 IM 等多种途径所传播，信息化是一般双刃剑，在享受信息化方便的同时，也需要对安全进行合理规划，在众多数据泄漏事件发生的同时，企业迫切需要一个全面可行的数据防泄漏整体方案。

1.2. 企业数据风险分析

为了更好的理解该方案给企业带来的价值，我们可以先归纳下没有使用该方案时，普通 IT 企业具有哪些数据泄露风险。

1.2.1. 数据存储风险

用户将应用系统上的数据保存到个人笔记本或者本地计算机上 ,数据并没有进行加密保护，如果笔记本发生被遗失，计算机的硬盘被拆卸、报废或者出现故障去进行修理等情况，存储在终端中的核心数据会发生泄露，被不法分子盗取、篡改、甚至公开，将会对公司产生极差的负面影响。

1.2.2. 数据传输风险

邮件系统、公司网站以及内部 OA 是当代企业信息化的三剑客，也是对内以及对外沟通文档的主要途径，特别是邮件系统，几乎是办公人员必备工具；而企业员工经常会主动或者被动将核心资料通过邮件传输给其他无关人员，造成核心资料的泄露。同时还有 U 盘、蓝牙、手机、网络等多种泄漏途径，所以需要一个可以防护所有途径的数据安全方案。

1.2.3. 主动泄密风险

企业系统上具有客户、财务、计费、公司内部通知等多种多样的敏感数据，少数被利益诱惑的员工会利用职务之便，通过 U 盘、QQ、微博等多种途径将公司内部的核心资料泄露给公司外部人员 ,对建筑设计公司造成恶劣的社会影响和重大的经济损失。

员工只要具有文件的所有权，就可以通过截屏、复制文件、拖拽内容、打印等多种方式对内容进行窃取 ,如何防止员工的主动泄密是目前所有中国企业都要面临的问题。

1.2.4. 内部流转风险

企业内部分为市场、运维、采购、财务等多个部门，各个部门各司其职，原则上不同部门的信息不能进行随意共享，但是实际情况中，员工将文件群发给所有人员、或者发送给错误人员的情况比比皆是，甚至有员工利用私人关系直接向其他部门的员工索要核心数据。员工也不清楚什么样的文档可以发给其他同事，同时企业内部具有大量的外协人员长期驻扎在企业总部，由于没有权限划分，核心数据受到严重威胁，必须要对文件的编辑、传输、销毁等全生命周期进行管控，以防止数据的泄露。

1.2.5. 外部交流风险

为了业务的正常流转，企业需要与企业合作伙伴进行频繁地数据交互，在数据传输的过程中重要数据被非法人员进行监控、复制、另存、打印，将会造成不可估量的后果。同时合作伙伴也会有泄漏文件风险，如果管控企业外部合作人员的数据风险也是一个重要课题。

1.2.6. 终端设备混用风险

目前建筑设计公司的员工都使用传统的认证方式，即用户名和密码的方式，这种传统的认证方式极易被破解，使得外部人员可以随意登录核心人员设备，查看核心资料，不仅公司内部的核心数据受到危害，就是个人的隐私数据也面临威胁，外部人员以及内部无关人员登陆他人计算机，招致内部核心数据知悉范围过大，甚至流失。

1.2.7. 病毒木马窃取破坏数据风险

网络病毒木马肆虐，虽然公司已经采购国际国内知名品牌的杀毒软件来保护各个终端的安全，但是由于杀毒技术的滞后性，病毒以及木马并不能完全被杜绝。当病毒木马发生时，最可怕的不是对终端操作系统的破坏，而是对核心文件的破坏以及窃取，需要有一种技术可以保证核心文件不能被病毒以及木马所破坏和窃取。

1.2.8. 人员离职风险

由于外围人员变动频繁，涉及业务较多，当出现有人员突然离职的情况，会造成该人员掌握的业务资料没有进行交接，业务资料被遗失，同时该人员获取原有的公司内部资料没有进行销毁，会对核心数据的保密安全工作埋下隐患。

1.2.9. 人员出差风险

由于企业正常业务的需求，企业用户难免会出差进行工作，由于网络环境以及地域问题，造成公司很多的制度，在出差阶段都出现执行不到位的情况，员工可能利用出差的机会将员工本地的资料泄露给非法人员，或者非法使用企业核心数据，需要一

种方法保证员工出差时既不会泄露企业核心数据，同时也可以正常使用核心数据。

1.2.10. 事件追溯风险

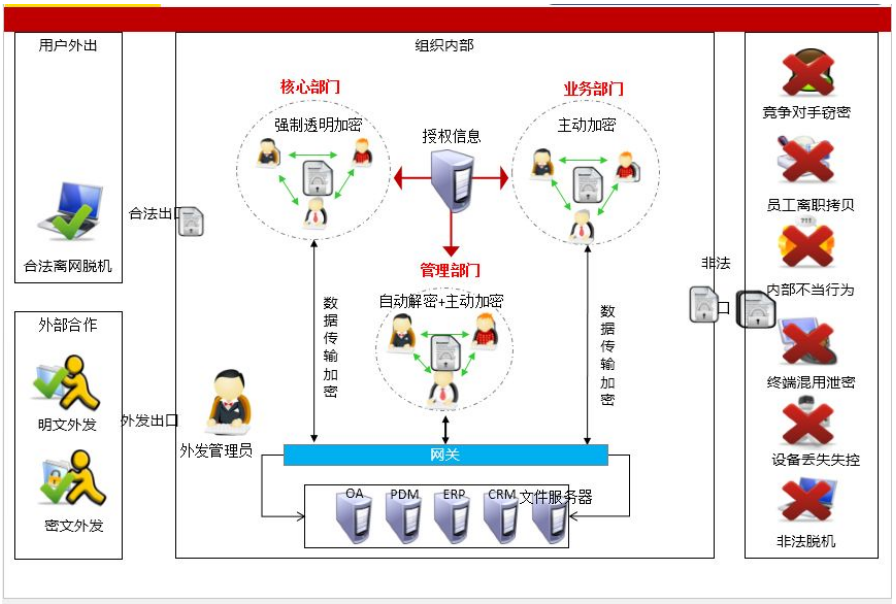
由于信息化迅猛发展，数据不仅具有多种多样的传播途径，而且还具有非常惊人的传播速度，QQ、论坛、微博、微信、视频等各种互联网工具已经让大家能实时获取当前发生的事情。任何企业发生数据泄露事件都会是影响巨大的，如果发生泄露事件后，还无法对泄露的人员、文件内容、时间、泄露途径等详细信息进行查询。从而无法对事件的原因以及责任进行追溯和定位。

2. 数据防泄漏解决方案

2.1. 方案概述

产品以数据加密为核心，结合身份认证、授权管理、设备管理、数据保护以及监控审计等技术，创建数据安全为中心的多层次安全模式，保护数据整个生命周期的安全。

系统自动对核心文件进行加密保护，用户无需关心怎样加密和何时加密，同时禁止用户对核心文件的内容进行复制、截屏、打印等非法操作。提供设置对核心文件的编辑、打印、复制等权限进行管控。自动对流转文件进行加密处理，无论文件通过QQ、邮件、U 盘等任何方式传输出去，都是加密文件，只有管理员授权的人员才能对文件进行解密查看。支持对合作伙伴使用的文件进行加密以及权限管理，客户和合作伙伴无需安装客户端也可以使用外发文件，同时受权限的管控，对合作文件进行浏览次数和天数的限制，超过浏览时间限制的文件将自动销毁。



2.2.功能设计

通过对客户的需求进行分析，数据防泄漏解决方案包含并设计了数据透明加解密、文件内容保护、文件权限管理、外设管理、可信进程管理、终端安全登陆、文件全周期审计等多个功能。

2.2.1.数据实时透明加解密

使用数据透明加解密功能对存储的文件进行永久加密 ,防止因笔记本的丢失以及硬盘恢复造成的数据泄露问题，合法用户可以解密浏览，不合法用户无法查看，不改变用户使用习惯，自动监控数据的创建、编辑、使用、传输等流转过程，实时分块对数据进行加解密，对机器性能影响较小，同时在数据每个生命周期都保持加密状态，保证数据的保密性。

2.2.2.外发管理

可以管控企业外部流转文件的权限，包括编辑、复制、打印、另存等权限，还可以限制文件的浏览时间以及次数，超过时间和次数将销毁文件，防止合伙伙伴对文件的二次泄密，同时提供多种外发格式，完美与邮件网关、杀毒软件兼容。

2.2.3.计算机外设/端口控制

对蓝牙、串口、并口、1394、USB 等外部设备进行控制，可以禁止核心文件通过以上端口进行传输，该功能可以对 U 盘进行注册管理，管理员可以对已注册的 U 盘进行授权，设置 U 盘可以使用的计算机范围，同时还可以将普通 U 盘制作为安全 U 盘，防止因 U 盘丢失而造成的数据泄露事件发生。

2.2.4.可信进程管理

用户可以通过设置黑白名单的方式定义可信进程和非可信进程。系统将禁止非可信进程对核心文件的使用，防止病毒木马对核心文件内容的窃取，同时还可以禁止 QQ 等网络进程对核心文件的使用 。默认可信进程的数据不能被复制到非可信进程中，非可信进程的数据可以被复制到可信进程中。

2.2.5.文件内容保护

文件内容保护可以阻止用户对数据的主动泄露行为。防止用户对文件内容进行复制、拖拽、打印、截屏等内容泄密操作，同时提供灵活的打印管理，对于特殊用户可以放开打印功能 ,文件打印时将会被自动添加用户名、文件路径、公司名等打印水印，方便事后追溯。

2.2.6.终端安全登陆

使用双因子认证代替传统的用户名和密码认证方式，除了知道密码之外，还需要具备手持令牌，没有手持令牌将无法登陆解密程序，同时拔出令牌后，计算机将进入待机状态，任何非法用户都无法登陆系统，最终防止外部人员以及内部无关人员对他人终端的非法登陆，进而防止因登陆风险而造成的文件泄露事件发生。

2.2.7.离线办公策略

支持使用离线和在线两种策略，自动探测是否与企业内网进行连接，出差的用户可以执行离线策略，既可以在出差的环境下进行文件使用，同时又可以防止文件被泄露。

2.2.8.文件全周期审计

文件全周期审计可以帮助用户随时随地查看核心文件的使用以及违规情况，可以对文件的编辑、复制、打印、重命名等使用状态进行记录，同时可以记录所有文件的使用者、使用时间等详细信息，方便用户对数据泄露事件发生后进行查询和追溯。

2.3. 安全设计

2.3.1.三权分立管理制度

由于系统的管理员具有设置用户使用、传输文件等权限以及其他管理功能，在整体解决方案中具有重大的权利，所以在安全上考虑将管理员进行分权管理，可以分为系统管理员、操作管理员与审计管理员，每个管理员管理范围没有重叠，互相监督，保证了管理制度的可靠性与安全性。

2.3.2.自身安全防护

数据防泄漏系统应该具有自我保护的功能，对自身文件、进程以及注册表等相关项目上具有防破坏功能，防止任何病毒、木马以及用户主动地终止系统的运行，阻碍数据泄露的防护功能。

2.3.3.业务连续性保护

安全系统的容错以及应急措施应该完备，系统应该具有双机热备的功能，防止因服务器硬件等问题造成的业务中断问题，使用双机热备功能可以保证业务连续性，保障业务的正常运转。