思安智云管理系统 v7.0

产品白皮书

- 公司名称：南京思智信息科技有限公司
- 公司地址：南京市雨花台区绿地之窗 C-3 栋 4 层
- 邮政编码：210000
- 公司网址：www.sage.top
- 联系电话：400-089-7028
- 传　　真：025-85567023

目 录

一、引言

1.1 文档主题

本系统通过对企业中各类机密数据信息的加密安全保护，可以显著提高企业中核心数据资产的安全防护能力。同时在对文件安全保护的基础上，又通过对剪贴板的有效控制，可以有效切断内部人员泄漏企业机密信息的途径，防止内部窃密事件的发生，而且一旦发生窃密事件，管理者能够通过日志功能，详细追查到窃密的人员、文件信息、途径等信息，以避免窃密事件的再次发生，从而能在很大程度上提高企业对机密数据信息的安全管理。

本文档主要介绍了思安智云管理系统系统的设计背景、产品概述、产品特点等几个方面内容，并对产品功能也进行了详细的介绍，以帮助读者对思安智云管理系统系统达到快速和全面的了解。

1.2 适用范围

本文档适用于需要对思安智云管理系统系统进行全面了解或以前接触过概念并想做进一步了解的用户。如需要了解产品的其他相关信息，请联系思智信息的销售工程师，由他们对您提出的问题和疑问集中进行解答。

1.3 术语和缩略语

术语、缩略语	解 释
FBI	Federal Bureau of Investigation，美国联邦调查局
CSI	Computer security institute，计算机安全协会
ESG	Enterprise Strategy Group，企业战略联盟
ERM	Enterprise Right Management，企业权限管理
DLM	Data Lifecycle Management，数据生命周期管理
EDRM	Enterprise Digital Right Management，企业数字权限管理
B/S	Browser/Server 结构，即浏览器和服务器结构
C/S	Client/Server 结构，即客户机/服务器结构
PKI	Public Key Infrastructure，公开密钥体系
Load Balance Server	负载均衡服务器

Authentication Server	认证服务器
DRM	Digital Right Management，数字版权管理
受控文件	受系统控制台中受策略限制的文件
受控进程	受系统控制台中受策略限制的应用程序的进程

表 1-1 常用术语及缩略语

二、产品研发背景

2.1 安全重点由外到内的转变

为实现企业内部的机密数据文件信息的安全防护，通常可以采用如设置防火墙，入侵检测，防病毒软件等手段，对来自外部网络的攻击和入侵起到有效的防御。但是，传统信息安全领域主要关注于外部入侵或外部破坏导致的数据破坏和泄漏，而**对于企业网络内部的信息泄漏（如内部人员泄密或其他未授权人员直接接入内部网络导致的泄密等），却没有引起足够的重视。**

据 2006 年 CSI 调查显示，在所有的安全技术应用中，以数据加密传输和加密存储为基础的技术应用所占比率分别达到 66%和 47%。

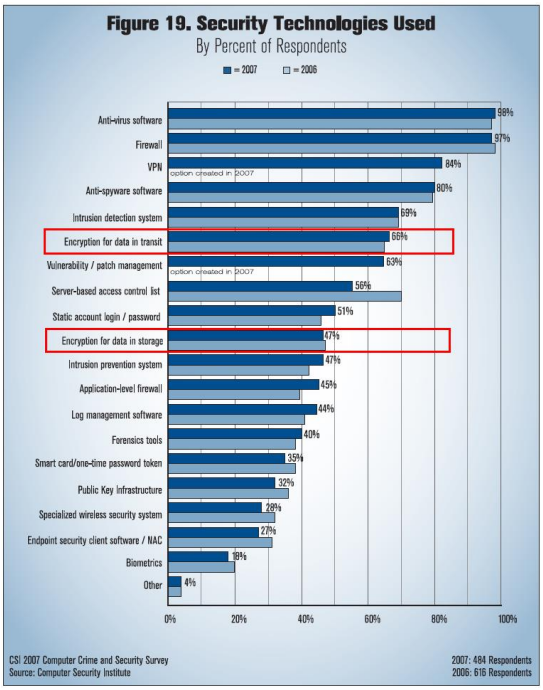

图 2-1 CSI 安全技术应用调查表

通过该调查，我们可以看到数据加密技术正在成为传统安全技术---防病毒系统、防火墙、VPN、反间谍、入侵检测之后的又一具有发展趋势的应用技术。结合各项攻击所带来的经济

损失的变化，可以看到针对于机密信息的安全保护正在成为更多企业新的关注方向。

因此，信息盗窃事件的主谋已经不再单纯是网络黑客和恶意程序，更多的数据信息是被企业和机构的内部员工所泄漏或盗窃。与传统的外部盗窃相比，这种来自内部的恶意泄露更具有针对性和隐蔽性，给企业造成的损失也更大。

2.2 信息泄露事件愈演愈烈

据 CSI 调查显示，2006 年，内部安全事件所占比率为 68%。2007 年这一数据依然保持，为 64%，如图 2-2 所示：

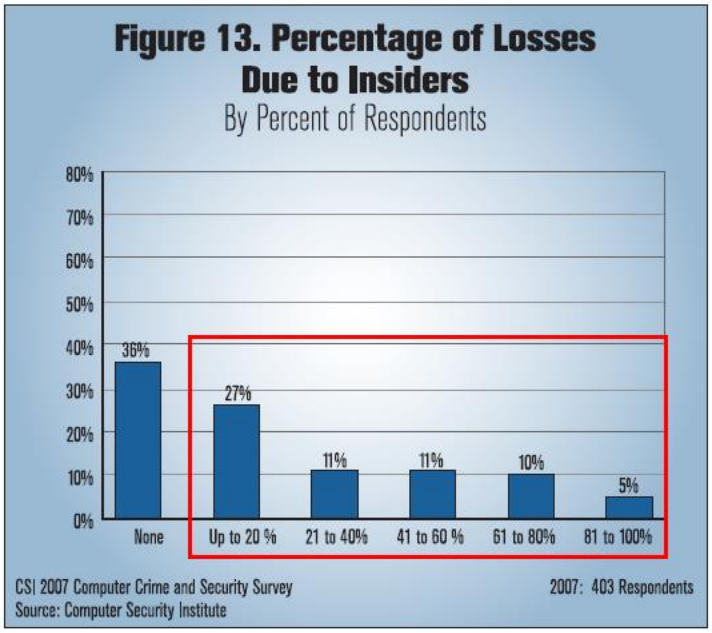

图 2-2 内部安全事件比例调查表

另调查显示，2007 年，由于内部人员窃取机密信息所造成的经济损失累计为 1515 万美元，2006 年的这一数据为 2329 万美元。这一数据的变化说明越来越多的企业开始重视企业内部的机密数据安全。同时，企业内部财务数据的安全性问题日益涌现，对于财务数据来讲，信息的安全和连续性已成为重要的因素，如图 2-3 所示：

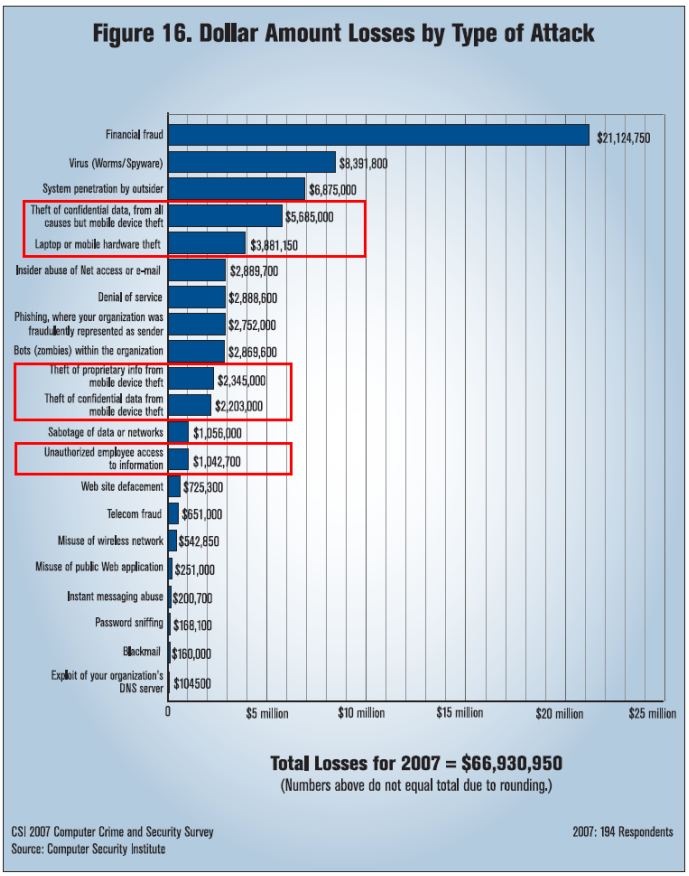

图 2-3 各种攻击所带来的经济损失比例图

由此我们可以得知，企业信息安全已不再单属于技术专家、情报局及学术机构所关注的问题。企业中机密的数据信息的泄漏已经严重影响了企业正常的业务运转。一次数据泄漏事件会严重影响公司的声誉，甚至导致无法预知的巨大经济损失。

2.3 机密信息管理薄弱

企业的核心机密数据就是影响企业未来发展的关键数据信息。每个企业通常都有自己的数据安全管理制度和业务管理流程，但在具体执行管理制度和流程的过程中，策略的执行和监控等多个方面存在很大的缺陷：机密信息监管不力导致内部信息的随意外泄，如高级员工的联系方式及工资待遇、技术部门的设计数据、企业信息化数据、公司的服务操作流程、规章制度等信息的泄漏，都会对企业造成意想不到的损失。

另外，现在大多公司的业务流程已不再是狭窄孤立的，而是一个具有动态性，协作性和广泛性的合作过程。例如：在企业的日常办公过程中，可能需要公司内外的人员通过电子邮件、演示文稿、电子表格或文档的形式来共享机密文件等信息，当然每个人由于担任的角色不同，从而对机密数据也拥有不同的访问和使用权限。这种信息的公开性就给数据的泄漏造成了巨大的潜在威胁。另一方面，公司最具价值的信息又不能完全被封锁起来或拒绝对外流通。这就要求公司的信息安全管理人员在不影响公司竞争优势的前提下，采取积极有效的措

施深刻理解和解决机密文件信息流失的问题。

虽然防火墙、访问控制、网关过滤等技术能够在一定程度上控制用户对机密数据的访问。但这些技术不能为用户提供更加细化的策略权限控制，也就是说它们不能限定用户具体的使用权限，如只读、可打印、可编辑等，这种静态的提供“全部或零”权限的安全工具已经不能满足当今动态的业务需求了。同时，这些内网环境防护技术不能提供对文件内容本身的加密，这就使得文件在外发的过程中也将潜在安全隐患带到了公司之外。

2.4 企业需要建立数据安全管理体系

2006 年《信息安全等级保护管理办法》（国内）和《萨班斯—奥克斯利法案》（美国）两部法案的正式实施对信息安全产业起到了标志性的影响。二者都以法规的形式敦促企业加强内部控制和增强抵御安全风险的能力。作为国家“十一五”计划的开局，2007 年始将是国家各机关部委及企事业单位规划五年发展计划的关键时间，又适逢国家“等级保护”法案实施、萨班斯(SOX)法案的推行，无论从产业发展阶段、国家政策、外部环境来看，还是借鉴国外的发展规律，都预示着我国的信息安全产业将由此迈入一个快速发展的新阶段。

思智信息在这样的大环境下，把握当前信息安全产业的发展形势，从关注企业用户的业务安全需求出发，通过整合自身数据加密技术、数据生命周期管理技术等方面的优势，以数据信息本身的安全保护和应用权限管理为核心，以文件安全策略管理、文件审批流程管理、日志和审计管理、文件自动备份管理为主要组成部分，最终构建完成了一个安全、高效和智能化的企业级应用办公环境——思安智云管理系统系列产品，为企业数据信息的安全防护提供了一个新的选择！

2.5 企业级数据信息安全产品—思安智云管理系统

2.5.1 概念

思安智云管理系统是一个企业级信息安全管理解决方案。它解决的是企业中数字化资产的有效控制和管理问题。

是在当今信息日益激烈的安全挑战下衍生的新生物，是实现信息安全从技术手段向管理手段改进的创新。系统能够全面整合网络访问控制、身份认证、数据通讯机密性、数据存贮机密性、数据使用可控性、数据的使用权限等多项先进的信息安全技术，为企业用户开发的的电子文档提供全新和更为可靠的安全管理解决方案。

系统可以确保企业的数据信息从初期生成、分发使用、编辑、直到最终数据被删除等生命周期的安全性，采用对文件内容本身的加密和细分的文件权限管理，数据无论是在企业内部网络中还是在企业外部，均可有效防止泄密和窃密事件的发生。

通过采用，企业不但可以确保数据信息的安全性，可以将数据资源的应用权限进行全面的细分管理和分配。企业中获得数据信息的一般员工将不再拥有完全的权限，而只将拥有在规定时间内完成某一项特定工作所需的数据信息使用权。

2.5.2 主要内容

对数据信息应用权限的管理过程，就是一个权限区分和细分的过程。

- 权限区分：指的就是对于数据信息使用者的使用权限进行区别对待，区分出哪些人是经过授权的，哪些人是没有经过授权的，做到只有经过授权的用户才可以正常使用数据。这个权限区分的过程，将数据信息的应用范围缩小到了授权人群范围之内。
- 权限细分：是在权限区分的基础上进一步细化。举例来说，企业文档的使用者得到权限区分的授权后，还要再受到权限细分的管理，对文档细分化的应用权限控制包括：只读权限、编辑权限、复制权限，存储权限，完全控制权限、打印权限、解密权限、可以应用的时间权限等等。总之，可以做到让指定的用户在指定的时间对指定的数据信息进行指定的应用操作。

2.5.3 思智信息与思安智云

从企业目前的种种安全状况及企业现阶段发展前景来看，企业内部核心数字资产管理的严重性已经到了无法忽视的地步，这些都要求我们嗜待加强机构内核心数字资产的管理并努力建设一个安全可靠的企业级安全管理体系来提高企业核心数字资产的安全防护，从而有效保护企业核心数字资产并有效进行管理和控制。这些都迫切需要一种革命性的技术出现。

思智信息通过整合自身数据加密技术、数据生命周期管理技术等方面的优势，结合公司理念的产品规划，开发出了一套针对于企业级应用的信息安全管理系统——思安智云管理系统系统，思安智云管理系统系统是理念的完美产品体现。

思安智云管理系统系统定位于以数据信息本身的安全保护和应用权限管理为核心，以客户端管理、文件安全管理、文件审批流程管理、日志和审计管理、文件自动备份管理、消息管理、系统远程管理、客户端为组成部分，构建了一个安全、高效、智能化的企业应用办公环境，从而实现了对企业数据信息的完整安全保护和权限管理。

思安智云管理系统系统的特点简单介绍如下：

- 思安智云管理系统系统全面整合了如文件访问控制，数据机密性保护和应用权限细分的电子文档安全管理系统。
- 思安智云管理系统系统用于公司内部电子文档和邮件的安全管理，能有效控制电子文档内容的具体使用权限，例如，哪些人在何时能够对文档进行哪种操作。具体操

作权限包括只读、拷贝、打印、转载、保存和编辑等等。

- 思安智云管理系统系统将权限控制策略直接整合到电子文档中。策略的应用控制直接贯穿到数字信息的整个生命周期，而不仅仅存在与信息的传输和存储等某个单独环节。
- 思安智云管理系统系统采取了和传统安全防护系统不同的信息安全保护方式，它通过保护文档本身来实现机密数据的安全。
- 无论机密信息存储于哪一台计算机上，思安智云管理系统系统具备的访问保护和使用控制策略都能够将文档的应用权限准确分配给不同的使用用户，从而避免机密信息被流失，窃取和非法修改等。
- 思安智云管理系统系统具备集中式管理功能，强大的报表和日志审计功能符合企业管理实际需求，同时通过整合其他 IT 基础结构的主要功能，使产品能够适应现代企业信息安全的需求。

2.6 思安智云管理系统系统给企业带来的好处

信息时代的今天，企业中的核心数据信息已日益成为影响企业发展的关键性因素。企业员工的工作过程，也就是创造数据资源信息的过程，这些数据信息中往往包含着企业赖以生存的关键资源信息，集中体现着一个企业的核心竞争力。从这个层面上来讲，任何企业都需要对自己企业内部的核心数据信息进行安全管理和保护，以防止信息的泄密和窃密。保护好企业的信息安全，就是保护企业的创新、知识产权、商业机密，并可以帮助企业实现现代化的、数字化的、科学有效的管理。

- 思安智云管理系统系统通过整合大量先进的信息安全技术，已经超越了简单意义上的数据信息安全，不再是传统的对文件进行口令管理或是加密，而是第一次从企业的角度来从根本上解决企业信息资源的安全问题。
- 思安智云管理系统系统不仅能够提供对数据信息的安全管理和保护，还可以对企业的业务流程起到有效的支持和推动。通过使用数据全生命周期管理技术，把信息安全融入到企业的管理流程之中，实现技术和管理的高度结合，解决了纯技术手段多年来的不足，从而适应了现代企业的实际安全管理需求。
- 思安智云管理系统系统能够确保信息的授权使用者只能获取自己所必需的应用权限。这样在很大程度上避免了由于电子文档自身的易复制性和易修改性所带来的安全风险。
- 思安智云管理系统系统是对数据信息本身的安全保护，其中整合了身份认证、数据

加密、权限细分、审计等多种技术。相对于目前大量企业所采用的网络边界防护设备和内网行为管理系统，能够更为彻底、有效的保护数据信息，防止信息泄露等安全事件的发生。

- 在维护和应用成本上，思安智云管理系统系统也有着更为突出的优势。对于企业来讲，他们只需集中式的实施和部署一套独立的应用系统；对于用户来说，数据信息的安全保护过程完全是透明的，不改变企业内部员工的操作习惯。但是，如果企业通过其它的信息安全技术实现同样的功能，可就需要采购和实施大量的安全工具进行复合防护。这就为日后的设备兼容性、维护成本、培训成本以及效率成本控制带来了不必要的麻烦，而思安智云管理系统系统则可以实现企业和用户的这种实际应用需求。

三、产品概述

思安智云管理系统系统是针对于企业级的信息安全管理系统。本系统通过对企业中各类机密数据信息的加密安全保护，可以显著提高企业中核心数据资产的安全防护。同时在对文件安全保护的基础上，通过对剪贴板的控制，可以有效切断内部人员泄漏企业机密信息的途径，防止内部窃密事件的发生。而且一旦发生窃密事件，管理者能够通过日志功能，详细追查窃密的途径，避免窃密事件的再次发生。从而提高企业对机密数据信息的安全管理。

3.1 体系结构与兼容情况

3.1.1 体系结构

思安智云管理系统系统采用 C/S+B/S 结构，按照架构可以分划分为三大部分：服务器、控制台与客户端；其中客户端与服务器之间通过 C/S 方式交互，控制台的组织机构管理、策略设置则通过 B/S 的方式与服务器交互实现。

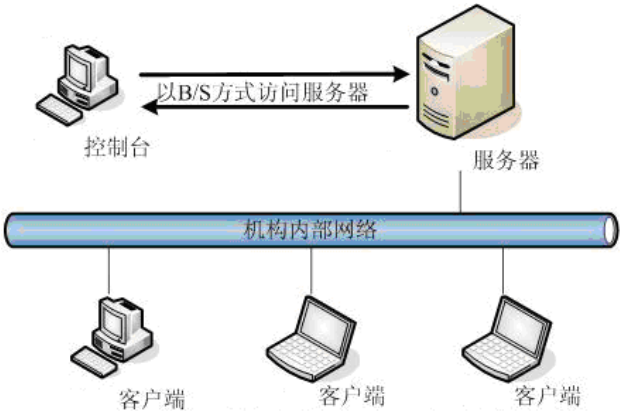

图 3-1 思安智云管理系统体系结构

(一) 服务器

服务器是思安智云管理系统系统运行的基础。服务器主要包括认证服务、负载均衡服务、升级服务、配置服务、文件自动备份服务五部分服务。其中：

- ✓ 认证服务用于用户认证信息的维护和应用；
- ✓ 负载均衡服务用于均衡连接认证和文件服务的用户负载量的应用；
- ✓ 升级服务用于系统相关数据信息的更新升级应用；
- ✓ 配置服务用于控制台的安装配置应用；
- ✓ 文件自动备份服务用于企业机密文件的自动备份应用；

(二) 控制台

为了实现对客户端用户统一管理的目的，思安智云管理系统系统采用了集中化的管理方式和基于角色的权限管理体系，思安智云管理系统系统控制台是整个系统管理和维护的基础平台，是客户端与服务器连接的桥梁。

控制台可以完成如管理员帐号及设置、客户端管理、机构用户管理、策略应用、策略配置、服务器远程管理、系统设置、日志审计管理、文件访问权限管理、文件备份管理的配置及维护等工作。

(三) 客户端

客户端主要是通过执行控制台各角色管理者制定的各种安全管理策略，实现对本地机密文件的安全管理，为企业员工提供稳定、易用的安全信息终端。

3.1.2 网络环境

思安智云管理系统系统可以适用于多种网络环境，如能够在 WINDOWS 域、VLAN、VPN、内网物理隔离的环境中正常安装。从而能确保在不更改各企业现有的网络架构的基础上，满足不同企业的实际应用需求。

	网络环境	支持情况
1.	域	能够与Windows域管理方式相结合，支持域用户漫游的使用方式。
2.	VLAN	支持多 VLAN 网络环境。
3.	VPN	支持使用 VPN 方式接入的网络环境。
4.	内网物理隔离	思安智云管理系统系统支持企业内部多个内网物理隔离的网络环境。

表 3-1 支持多网络环境

注：内网物理隔离是指企业有两个内网，一个内网可以访问 Internet，一个内网不可访问，两个内网之间物理隔离。

3.1.3 兼容情况

思安智云管理系统系统具有良好的兼容性，能够与企业现有大多数软件兼容，能够与多种杀毒软件、数据库、业务管理系统相结合使用。不会因为部署思安智云管理系统系统而需要卸载或更换企业现有软件。

	兼容方面	兼容情况
	杀毒软件	与主流杀毒软件无冲突，且不会被杀毒软件查杀或卸载。如瑞星、诺顿、江民、金山、卡巴斯基等。
	数据库	支持 MYSQL、SQL-SERVER 2000 和 SQL-SERVER 2005 数据库，其他数据库也可以单独定制。
	业务管理系统	能够与 OA、ERP、PKI 等系统兼容。

表 3-2 兼容情况

3.2 功能详述

思安智云管理系统系统可以划分为以下功能类，它们分别是：用户管理功能、客户端多元化安装功能、客户端管理功能、策略管理功能、文件访问权限管理功能、离线管理功能、全盘加解密、文件解密审批、系统备份功能、邮件监控、打印控制、日志管理功能、文件远程备份功能以及数字版权控制功能。下面将对此功能进行详细说明。

3.2.1 用户管理功能

功能简述		功能详述及应用效果
1.	组织结构（包括部门和人员信息）的建立	▲功能：在思安智云管理系统系统中可以建立与企业真实组织结构完全相同的组织结构关系，并配置部门和人员等基本信息。 ▲应用：当企业实际人员、部门进行调整时，系统管理者可通过控制台灵活对系统中的组织结构进行更改。 如：王强本隶属于销售 1 部，由于业务需要，可以将其调整至销售 2 部之下。
2.	域管理组织结构导入	▲现状：在企业中可能原已存在 WINDOWS 域管理机制，

		并在域中存在已经建立完善的企业组织结构。 ▲应用：思安智云管理系统系统可以将域中的组织结构通过工具，直接导入到系统中使用，避免了重复录入的烦琐工作。
3.	管理员信息的建立与维护	▲功能：超级管理员(admin)可根据企业的需要，为系统中预定义的用户赋予适当的角色，每种角色所能实现的功能是不同的。 ▲应用：如可设置张三为日志管理员，令李四为文件管理员，命王五为部门管理员等。
4.	自定义用户角色	▲功能：超级管理员(admin)可以自定义用户角色，手动设置其在控制台上可以使用的菜单、策略等。 ▲应用：如新建一个角色“小组管理员”，设置其在控制台上仅可以对其小组内成员进行用户信息修改、策略下发等操作。
5.	双口令登陆认证	▲对系统超级管理员 amdin 的登陆可采用双口令登陆认证方式，以增强超管登陆的安全性。
6.	分级管理功能	▲用户角色分级：不同的用户角色执行不同的管理任务； ▲操作权限分级：解密权限（解密自己、解密本组及解密全部）及解密审批（申请解密审批自己/本部门及所有）分级管理；
7.	一机多用户管理	▲现状：在企业中经常出现一台计算机有多个员工使用的情况。这些员工在一台计算机上分别建立了各自的 WINDOWS 帐户，但他们在企业中受到企业的约束不一定相同。 ▲应用：思安智云管理系统系统支持这种一机多用户的使用情况。分别将员工使用的 WINDOWS 账户与思安智云管理系统系统用户进行绑定，即一旦用户进入了其使用的 WINDOWS 账户，便将接受系统对该用户的指定策略管理。 注：虽然几个员工共同使用同一台计算机，但是每个员工在不同 WINDOWS 账户下接受的系统管理将不同。

表 3.2.1 用户管理功能列表

3.2.2 客户端多元化安装

安装方式		安装方法
1.	本地安装	▲将安装程序拷贝到客户端机器中，在本地直接双击安装程序进行安装。
2.	WEB 安装	▲在客户端机器上服务器访问地址，如 https://192.168.2.53:442，即可实现在线客户端安装。
3.	远程推送安装	▲由系统管理员统一实现对客户端的远程传送与安装，而影响现有员工的目前的工作效率。
4.	域用户透明安装	▲可以在域服务器上统一对所有域用户透明安装客户端。

表 3.2.2 客户端多元化安装列表

3.2.3 客户端管理功能

功能简述		功能详述及应用效果
1.	管理策略执行	▲接收并执行控制台下发的各种功能策略（分 5 大类别近 80 种策略）。
2.	文件剪贴板控制	▲功能：受自动加密保护的文件，具有剪贴板防护的功能和控制，防止受信进程和非受信进程之间的文件互拷。 ▲应用：例如 WORD 为受保护的文件，使用剪贴板控制后，则无法将 WORD 文件中的内容拷贝到聊天对话框或它编辑工具内，但是可以将其他类型文件内容复制到 WORD 文件中来。
3.	文件加解密 ➢ 手动 ➢ 自动	➢ 自动：按照透明加解密策略自动加解密文件。对于加密保护后的文件，无法通过任何复制、粘贴、拖拽等方式，利用邮件、及时通讯工具、论坛等非受信任的执行程序带出到企业之外。 ➢ 手动：根据控制台下发的手动加解密策略，进行手动右键加密和解密操作。
4.	客户端本地文件备份	▲ 功能：客户端具有对加密文件的本地备份机制，每次打开文件均会自动在本地留下文件备份，以防止客户端文件丢失或者遭受恶意破坏。 ▲ 应用：若重要文件遭受意外损坏，可由控制台下发策略“显示本地备份菜单”，同时在客户端右键菜单中选择“打开本地备份文件夹”选项，选择需要恢复的文

		件，拷贝出来后再进行恢复操作。
5.	客户端安全保护	▲功能：防止客户端非法卸载，还可对客户端实行进程监控、进程守护、注册表保护、时间同步、定时与服务器通讯、程序完整性检测等操作，以确保客户端程序安全完整。

表 3.2.3 客户端管理功能列表

3.2.4 策略管理功能

功能简述		功能详述及应用效果
1.	默认用户策略列表(详见附件)	▲应用：系统提供了默认策略列表供用户使用。默认策略分为 5 大类别近 80 种，且可以根据用户实际需求，由思智信息工程师添加特定的默认策略内容。
2.	自定义策略组合	▲应用：根据管理员的实际管理需要，可以将策略列表中的默认策略进行组合，组合成新的策略组，以便于策略整体下发。
3.	策略应用	▲应用：系统管理员根据企业实际管理现状，将相应策略应用于每一个员工或部门。得到策略的员工或部门将按照策略规定，接受相应的策略管理。

表 3.2.4 策略管理功能列表

3.2.5 文件访问权限管理

功能简述		功能详述及应用效果
1.	加密文件夹	▲功能：将非加密文件拖入该文件夹后，实现文件自动批量加密；
2.	文件访问权限不受文件传输方式影响	▲功能：授权后的文档可以通过任何的方式传递给其他受管理人。例如通过局域网的共享，QQ、MSAN 的文件传送，EMAIL 附件等方式传播。 ▲文件在传输过程中仍保持加密状态，只有授权用户才能正常进行访问。

表 3.2.5 文件访问权限管理列表

3.2.6 离线管理功能

功能简述		功能详述及应用效果
1.	长期离线用户管理	▲功能：若员工不能够与企业内网中的服务器相连，可以通过文件交互方式接受思安智云管理系统系统的管理。 ▲应用：例如员工甲长期不在公司，将思安智云管理系统系统客户端安装程序发给他后，其可以自行安装客户端，安装完成后，通过指定工具导出一文件，发送给公司内部管理员。管理员在控制台上将该文件导入，设定用户信息和用户策略后，再导出一文件传送给员工甲。员工甲通过导入此文件至本机，即可按照策略接受管理并根据权限查看其他用户共享给他的加密文件。
2.	短期离线用户管理	▲功能：若员工临时出差在外，可以通过离线策略对其进行管理。 ➢ 为员工下发“离线允许打开自己的加密文件”和“离线允许打开共享加密文件”两条策略，则员工可以在出差期间正常使用加密文件。 ➢ 若需要临时更改策略，操作如下：管理员在控制台为该用户下发其需要的策略，然后导出成一文件形式存储，并发送给员工。员工收到该文件将其导入至本机，则策略修改成功。 ▲应用：例如员工带笔记本外出办公，规定员工某一日期时间内使用受保护的文件，超过规定的时间无法打开这个文件。但是员工在规定的时间内没有完成工作，则可通过上述方式更改离线客户端使用文档的日期和时间。

表 3.2.6 离线管理功能列表

3.2.7 全盘加解密

功能简述		功能详述及应用效果
1	全盘加密	能对指定类型的文件执行全盘加密 注：支持按照用户名及文件状态（如未加密、已申请、正进行、未完成等）进行查询，并支持模糊查询。

2	全盘解密	对自己机器上所有的加密文件进行解密
3	前台模式	即扫描界面以前台的形式显示出来
4	后台模式	不提示扫描界面，仅在后台扫描

表 3.2.7 全盘加密实现模式

3.2.8 文件解密审批

功能简述		功能详述及应用效果
1	所有审核者按序审核	即所指定的审核管理员按设定顺序全部审核通过后，文件才可正常解密
2	所有审核者不按序审核	即所指定的审核管理员按任意顺序全部审核通过后，文件才能正常解密
3	部分审核者按序审核	即所指定的审核管理员中的部分（人数可手动设定）按设定顺序全部审核通过后，文件才可正常解密
4	部分审核者不按序审核	即所指定的审核管理员中的部分（人数可手动设定）按任意顺序全部审核通过后，文件才可正常解密

表 3.2.8 解密审批模式

3.2.9 系统备份功能

功能简述		功能详述及应用效果
1.	组织结构备份	▲思安智云管理系统系统中的组织结构能够进行备份并以文件形式保存，今后重新部署思安智云管理系统系统时无需重新再建立组织结构，将该文件直接导入即可。
2.	策略列表备份	▲思安智云管理系统系统中的策略列表可以单独进行备份并以文件形式保存，今后重新部署思安智云管理系统系统时无需重新再建立策略列表，直接导入该文件信息即可。
3.	数据库文件备份	▲对服务器端的配置信息均存储在数据库中，将数据库文件进行备份并以文件形式保存后，当需要迁移或重置思安智云管理系统系统服务器时，通过导入该文件即可直接恢复到上次备份时思安智云管理系统的系统配置状态。

表 3.2.9 系统备份功能列表

3.2.10 日志管理功能

功能简述		功能详述及应用效果
1.	日志管理功能 (logadmin)	➢ 对超级管理员(admin)和所有部门管理员在控制台的操作行为进行统计（审计的内容包括：创建用户，修改用户，删除用户，绑定用户，删除绑定信息，创建部门，撤消部门，调整部门，应用策略，撤消策略，新建用户策略，删除用户策略，修改用户策略，导入导出策略，登陆登出等）。 ➢ 对所有员工进行的文件操作行为进行审计（审计的内容包括：新建文件、复制文件、粘贴文件、保存文件、删除文件、共享文件、文件名称更改、文件路径变更、文件手动加解密操作等）。 ➢ 同时提供以报表形式（柱形、饼型和圆型三种）直观的对操作记录进行统计显示；
2.	记录控制台日志	▲记录所有能够登录控制台的管理员的登录、登出及对用户、部门信息维护的所有操作。
3.	记录客户端日志	▲记录客户端所有在线、离线信息操作。
4.	记录文件操作日志	▲记录客户端对文件的操作日志： ➢ 文件操作信息记录包括：新建、复制文件、粘贴文件、保存文件、删除文件、共享文件、文件名称更改、文件路径变更、文件手动加解密操作的详细记录。 ➢ 离线的客户端日志记录。客户端离线后的操作也全部被记录，当连接到服务器后自动将离线后所有操作的信息上传到服务器。
5.	日志维护	▲对日志信息定期维护，如可以导出或删除日志信息等。
6.	自定义日志查询	▲可以对日志记录进行筛选查看，如通过时间、人员、日志类型进行查询。

表 3.2.10 日志管理功能列表

3.2.11 邮件监控

功能简述		功能详述及应用效果
1	客户端发送附件自动解密	附件发送到指定白名单邮箱里自动解密，否则仍为加密

2	收件箱接收自动解密	在接收人白名单之列的邮箱，收到为明文
3	客户端接收附件自动加密	接收附件到本地时按照提前设置的后缀名类型自动加密

表 3.2.11 日志管理功能列表

3.2.12 打印机控制

功能简述		功能详述及应用效果
1	打印是否可用	可控制是否允许客户端进行打印
2	客户端选择性打印	可设置客户端只能用设定好的打印机进行打印操作
3	打印水印	为保护公司文件版权，可对客户端配置打印水印

表 3.2.12 打印控制功能列表

3.2.13 文件远程备份功能（可选）

功能简述		功能详述及应用效果
1.	设置文件备份服务器	▲由超级管理员设置文件备份服务器的基本信息，如备份服务器名称、IP 地址、备份地址、传输端口等。
2.	文件备份设置	▲功能：通过应用文件自动备份策略，将企业中受保护的文件定期自动备份到文件服务器上，并可以灵活的设置需要文件备份的人员及备份格式、备份文件预留磁盘空间大小等。 ▲备份的文件在服务器上仍以密文的形式进行存贮，并且文件名也是乱码，只有文件管理员才能查看到正常的文件名和文件内容。
3.	文件恢复	▲客户端遇到意外情况，如文件误删、故意删除、或客户端机器硬盘损坏，可以通过文件备份服务器进行恢复。
4.	文件统一集中管理	▲备份后的加密文件由文件管理员集中进行管理。
5.	备份文件查询	▲可按文件名称、用户等分类查询备份文件。

表 3.2.13 文件远程备份功能列表

3.2.14 数字版权控制功能（可选）

功能简述		功能详述及应用效果
1.	第三方共享文件的控制（数字版权控制）	▲现状：在与客户交流过程中，客户常常为第三方的泄密而头疼。有些单位专为第三方企业提供第三方设计图纸、写作方案等等。写好了之后如果以明文的形式交给第三方，第三方有可能把图纸文档再次散发和传播，这必然会给设计的企业带来风险和损失。 ▲应用：通过思安智云管理系统的数字版权控制就可以解决客户的这个需求，给第三方的仍然是密文，第三方拿到密文后只能在指定的计算机中打开，并受到使用这个文档的细致的权限控制。即使第三方不小心将文件传播出去，别人拿到的也是密文信息，也无法正常进行查看。

表 3.2.14 数字版权控制功能列表

3.3 产品特点

3.3.1 基于角色的用户权限管理

思安智云管理系统系统用户管理模块采用基于角色的权限管理体系，在员工、角色和权限之间建立了相互对应的关系，将系统的各种不同操作功能授权给某个角色，加入了该角色的用户就拥有了对应其管辖范围内用户的操作权限，从而实现了用户与权限的逻辑分离。

基于角色的权限管理体系分为两个部分：

- 权限和角色的关联
- 角色与用户的关联

以下为图示说明：

图 3-2 基于角色权限管理模型

基于角色的权限管理能极大的方便管理员的操作。由于角色与权限之间的变化比角色与用户关系之间的变化相对要稳定，并且分配用户到角色不需要太多技术，可以由管理人员来确定，而配置权限到角色的工作较复杂些，需要由具有一定相关技术的专门系统管理员来承担，但是不给他们分配用户的权限，这与现实中情况正好一致。

在系统的实际使用中，由于某一角色所能拥有的权限已被限定，所以即使不断变换所对应的实际用户，也不会给已经确定的安全体系带来任何影响。系统管理员可很方便的完成对用户角色的创建和用户角色的分配工作，当员工由于工作需要其职责需要调整时，只需将其加入到对应工作职责的用户角色中即可。例如，对于都拥有日志管理权限的用户，组管理员只对该组内员工的日志具有审计权限，而特权组用户则对全体员工的日志具有审计权限。

3.3.2 安全的身份认证管理

对用户的和合法身份进行认证是企业文件安全系统建设的基础。只有首先区分出哪些用户是经过授权的，并且只允许经过授权的合法用户正常登录内部网络和访问关键的数据信息，才能真正实现到企业级文件安全系统的安全管理。

通过部署思安智云管理系统系统，企业可以确保只有被授权的用户可以正常进入内部网络，进而使用内部网络的资源。在内部网络的结构中，计算机终端既是系统体系主要的组成部分，也是进入内部网络的入口。所以，我们在对内部文件进行安全管理的同时，首先要做的就是加强对终端登录的安全管理和控制。企业中的用户只有经过合法身份认证，才能进入企业内部网络访问企业的内部文件，思安智云管理系统系统采用了双向认证机制，一方面服务器对客户端进行认证，另一方面客户端对服务器进行认证。如下图所示：

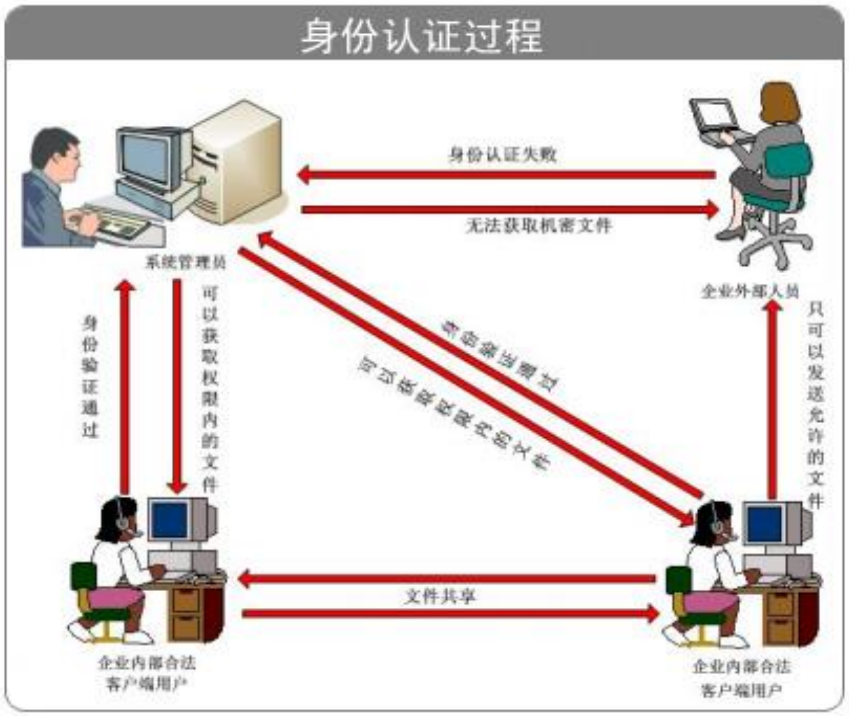

图 3-3 身份认证过程

3.3.3 驱动级的透明加解密应用

目前常用的透明加解密技术分为两种，一种是 HOOK 系统文件操作 API 函数即应用级的

透明加解密，还有一种是在通过文件驱动在驱动层进行处理即驱动级的透明加解密。

目前系统采用的是驱动级的透明加解密实现，和应用层加解密技术相比，具有安全，可靠，稳定，效率高的特点，而透明性则体现了不改变用户使用习惯的特点。

- 对于设置了透明加解密的应用程序，该类型新建和保存的任何文件在从内存写入硬盘前，都将自动进行加密。
- 对于受控制的程序打开的任何文件，在读入内存前，将进行身份认证及权限判定，对合法访问的用户自动进行解密。
- 对于受保护程序新建的任何文件，透明加解密模块都将首先进行加密操作而后打开。
- 透明加解密应用过程并不改变用户文件的默认打开方式，当用户选择使用特定的应用程序打开密文时，如该程序也属于受保护程序范围内，在通过权限验证后，系统也将自动解密，否则将不会自动进行解密操作。
- 文件透明加密过程不改变文件本身的格式和文件管理原有的操作方式。用户在对文件进行安全保护的过程中，不改变文件本身的格式。用户在使用加密文件的过程中，也无需安装特殊的文件阅读器，只需要借助思安智云管理系统系统的客户端程序，直接操作加密文件即可，所有的操作实现透明化。
- 整个加密过程安全、简便、快捷，不会生成任何可能泄密的临时文件，同时对用户的操作也不会产生任何影响。当用户被应用强制加解密策略之后，被加密保护的文件操作可以像操作普通文件一样，文件的加解密转换完全在系统后台完成。并且，在任何存储介质中，被加密过的文件将始终保持加密格式，只有授权用户才能进行解密和应用。

下图即为思安智云管理系统系统透明加解密的示意图：

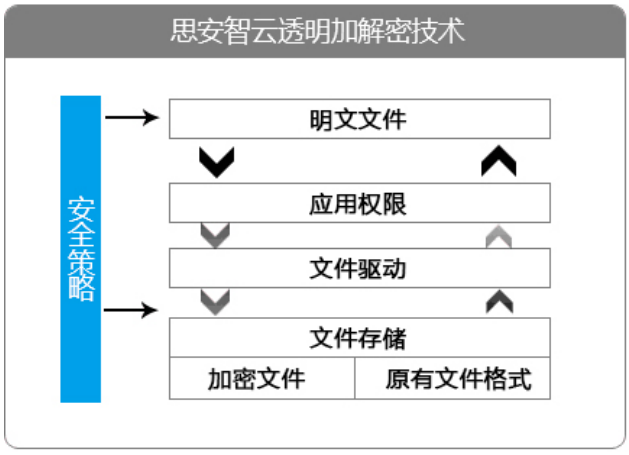

图 3-4 透明加解密图示

透明加解密技术适用于任意类型的信息文件类型，加密的文件格式可以根据用户需要自由设定。在思安智云管理系统系统中，透明加解密的使用策略在控制台由管理员统一设定，

并自动下发到需要应用的客户端，客户端则根据管理员的安全策略设定来执行，从而能够保护在客户端上的机密文件信息。

3.3.4 严密的剪贴板防护技术

作为防止用户主动泄密的重要环节，思安智云管理系统系统提供了剪贴板保护功能。一方面，系统将受透明加解密模块保护的应用程序作为受信进程，其它应用程序作为不受信进程，受信进程内及受信进程之间，基于快捷键、鼠标右键、拖拽操作等各种方式进行的拷贝、剪贴操作，将不会受到任何限制；另一方面，对从不受信进程到受信进程的拷贝、剪贴操作也不受限制，而从受信进程到不受信进程的任何方式的拷贝、剪贴等将被禁止。

见下图所示：

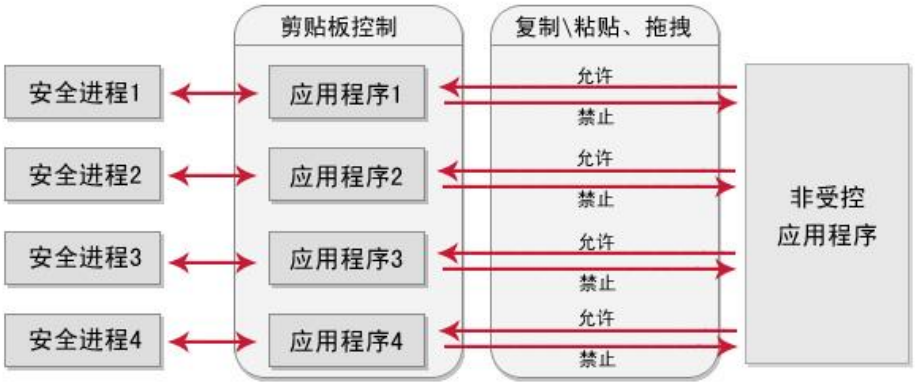

图 3-5 剪贴板防护图示

3.3.5 灵活的策略管理

管理员需要根据企业的管理制度和每个员工的具体操作职能，在控制台为其设置相应的管理策略，设置之后并下发给企业的员工，从而达到对员工操作行为控制管理的效果。

1. 思安智云管理系统文件安全类策略包括：

- 维护及应用“透明加解密策略”
- 维护及应用“文件解密策略”
- 维护及应用“离线文件访问策略”

2. 系统维护类策略包括：

- 维护及应用“任务栏图标显示策略”
- 维护及应用“硬件设备使用控制策略”
- 维护及应用“组间隔离策略”
- 维护及应用“加密文件图标显示策略”
- ……

详细策略内容请查看《策略说明》。

- 行权限设置，不影响企业原有的文件共享的操作习惯。

3.3.7 方便灵活的解密审批机制

思安智云管理系统除对解密文件提供三种直接解密方式外，为配合公司内部管理，还提供了三级解密审批机制：申请审批解密自己、申请审批解密同组及申请解密审批解密全部，每种解密审批级别根据不同情况对不同的用户下发。

该模块可实现指定某些管理员按照何种顺序（顺序或无序）对某客户端的解密请求进行审批，目前实现以下四种审批模式：

- 所有审核者按序审核：所指定的审核管理员按设定顺序全部审核通过后，文件才可解密；
- 所有审核者不按序审核：所指定的审核管理员按任意顺序全部审核通过后，文件才能解密；
- 部分审核者按序审核：所指定的审核管理员中的部分（人数可手动设定）按设定顺序全部审核通过后，文件才可解密；
- 部分审核者不按序审核：所指定的审核管理员中的部分（人数可手动设定）按任意顺序全部审核通过后，文件才可解密；

3.3.8 全面的日志审计管理

思安智云管理系统系统提供了强大的日志审计管理功能，以便系统管理员即时查看用户对文件所做的各种操作，日志审计能够记录以下信息：

- 客户端、控制台的运行状态。
- 对客户端所有的文件操作进行详细的记录，包括：文件新建、打开、关闭，文件复制、重命名、删除、传输等行为，记录内容包括：所操作的文件名、时间、路径等。
- 对所有的日志记录进行查询、分析，提供审计的依据。
- 提供以报表形式（柱形、饼型和圆型三种）直观的对操作记录进行统计显示；

3.3.9 自动的文件备份管理

为实现机密的进一步安全管理，在思安智云管理系统系统透明加解密功能的基础上，还能够对受控的机密文件进行自动备份的管理。

用户在选用文件自动备份管理模块之后，可以通过控制台自由指定需要进行文件备份的用户和部门，并设置其可用的备份空间大小，备份份数等。

- 管理员可以通过控制台指定文档需要自动备份的方式、自动备份的文件格式等信息。
- 客户端会根据提前设定的自动备份条件，将相应的加密文件自动上传到文件自动备份服务器中，而且只有文件管理员通过文件查看器才能对被备份文件进行查看。
- 通过文件自动备份管理模块，管理员可以对文件备份服务器上存储的所有用户文件进行备份，并在必要时执行文件恢复。

3.3.10 便捷的系统远程管理

- 思安智云管理系统系统为客户端提供了“远程推送”安装方式，系统管理员在实际部署过程中，只需要在控制台机器上远程安装，即可以快速完成系统部署及用户组织结构的轻松配置。
- 思安智云管理系统系统在实际部署时，可以根据需要将各个服务分开部署，通过控制台提供的“服务器远程管理功能”，方便地实现对各个服务器集中进行远程管理。
- 对产品发布后所进行的升级工作，用户可通过控制台的升级管理功能完成，从而保证用户的产品的及时更新。

思安智云管理系统系统在安装、应用和维护的过程中无不体现出其卓越的简单易用性和便捷性。

3.3.11 健壮的客户端系统安全

作为确保企业信息安全的重要组成部分的客户端模块，其本身的稳定性、健壮性将直接关系到整个系统的信息安全：

- 思安智云管理系统系统通过进程监控、进程守护、注册表保护、时间同步、定时与服务器通讯、程序完整性检测等方式，确保客户端系统自身的安全。
- 考虑到客户端机器的环境多样性，思安智云管理系统系统能够与主流杀毒软件（瑞星、江民、卡巴斯基、诺顿）、防火墙软件、财务系统、OA 系统等应用系统保持兼容。

3.4 系统运行环境

- **服务器**

操作系统	Windows 2003 Server (SP2)以上
CPU	主频 1.8GHz 以上

内存空间	2G 以上，推荐 4G
硬盘空间	硬件无特殊要求

表 3-13

- **控制台**

操作系统	Windows Xp(SP3)以上
CPU	主频 1.6GHz 以上
内存空间	1G 以上，推荐 2G

表 3-14

- **客户端**

操作系统	Windows XP(sp3)以上
CPU	主频 1.6GHz 以上
内存空间	1G 以上

表 3-15

四、典型应用

4.1 背景介绍

企业内网中，由于机密信息分散存储在企业内网中的各类终端中，这样机密信息在企业内网中就无处不在。如何管理企业内网中的文件本身的安全、又能够使文件能够在内网中共享授权使用，成为企业面临的一大难题。

虽然，企业中的信息安全管理者们已经意识到对企业中文件等数字机密信息安全管理对企业自身的重要性，但单纯的使用管理制度难以实现对企业内部信息全面和有力的保护。如何结合企业的现有管理制度和技术手段，实现企业文件等数字信息的安全，将是目前有信息安全需求的企业迫切需要解决的问题。

4.2 企业需求

- 企业在日常的业务沟通过程中，通常会通过如电子邮件、及时通讯工具、网络上的BBS、演示文稿、电子表格等文档的形式来共享机密数据，这种信息的公开性本身就给数据的攻破造成了巨大的威胁，但是公司宝贵的信息又不能被封锁或破坏。
- 大多的安全系统，像防火墙、访问控制、网关过滤等技术能够准许或拒绝访问，但

他们对可访问的用户都不能提供精细的颗粒度的策略权限，从而限定哪些机密信息能够使用，哪些不能够使用，因此，这种静态的“提供全部或零权限的”工具已经不能满足当今企业，动态的业务需求。

- 大多的文件安全系统，无法提供与实际企业管理流程相一致的管理制度，单纯的实现文件安全，已经无法适应企业的安全需求。如何能够真正从企业文件安全管理出发，从企业文件安全管理者的角度考虑，并能够承载企业文件管理流程的思想，通过企业安全系统的部署，最终保障企业的文件安全管理，并在最大程度为企业创造价值，同时使企业的文件安全得以不断地提高。
- 一般的文件安全系统在对文件加密安全保护的过程中，一旦系统出了故障，或者文件被损坏，无法实现对文件的安全备份和恢复。
- 对于机密性很高的文件信息，如果能够全程跟踪该文件的操作记录，实现对机密文件的安全保护，一旦出现机密文件的泄漏，能够审计到是由哪个环节造成的泄漏。
- ……

4.3 产品部署应用

思安智云管理系统系统的部署将帮助企业从根本上解决上述问题。见下图所示的思安智云管理系统部署结构示意图：

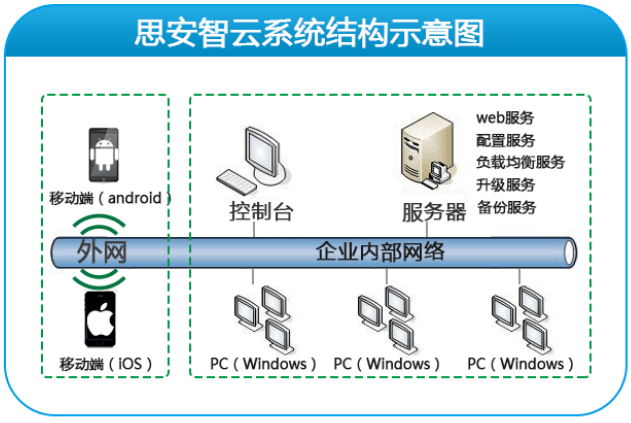

图 4-1 思安智云管理系统系统部署示意图

思安智云管理系统系统在企业内网部属完之后，为了实现企业内网中机密文件等数字信息的安全，企业可以通过以下几个步骤来来实现文件信息的安全管理目的：

1. 根据企业的人员组织机构设置，同时结合思安智云管理系统系统的产品结构，在控制台建立与真实组织机构相一致的部门结构。
2. 通过思安智云管理系统系统的控制台的远程系统管理功能，为企业员工远程推送安

装客户端程序，不会影响员工的正常工作。

3. 按照企业的安全管理制度，管理员在控制台制定相应的安全策略：

1) “透明加解密策略”设置及应用

- 策略设置，为了保护企业内网中的机密文件安全，首要任务是实现内网中文件的自动加密存储。所以企业管理者需要制定出哪些文件类型需要进行安全保护，然后通过思安智云管理系统系统控制台提供的强制加解密策略，并添加相应的受保护文件的应用程序的进程。
- 应用效果，应用该透明加解密策略的员工，只要使用本策略定义的应用进程，应用该应用程序的进程打开的所有格式的文件就强制被自动加密。本策略支持所有的文件应用进程。见下图示意：

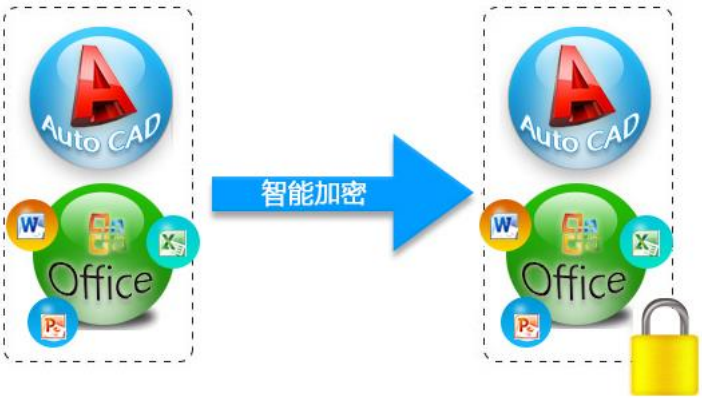

图 4-2

2) “剪贴板控制策略”设置及应用

- 在企业内部工作中，越来越多的沟通工作都依靠邮件系统、及时通讯工具、网络工具来完成。虽然给我们的工作带来了便利，也在一定程度上，加大了对企业中文件等数字信息安全的隐患。经常会有内部员工，通过邮件系统、及时通讯工具把公司的机密文件内容，泄露到内网之外。为了控制企业员工对主动对文件等信息的泄密，思安智云管理系统系统控制台提供了“剪贴板控制”策略。可以在“剪贴板控制策略”中，添加对剪贴板受保护的应用进程。
- 应用该策略的用户，无法从受“剪贴板控制策略”限制的应用程序进程打开的文件中复制、粘贴文件的任何内容到未受“剪贴板控制策略”的应用程序进程打开的文件中。包括及时通讯软件的对话窗口、上传空间，拷贝和粘贴

机密的信息内容和地址等。从而保证了企业员工在正常使用这些工具进行工作的同时，杜绝员工通过及时通讯工具、上传下载工具，外泄企业中的文件等数字机密信息。见下图所示：

图 4-3

3) “手动解密策略”设置及应用

- 在企业内网的日常的业务工作过程中，可能会有与外界进行沟通的文件传输和共享。思安智云管理系统系统控制台提供了客户端主动解密的策略。
- 应用该策略的员工，在实际工作过程中对受控文件可以进行主动解密，解密之后的文件再进行传输和共享，从而保证正常工作。而没有应用该策略的员工，则无法对受控文件进行解密查看。这样即使拥有加密的文件，并通过邮件系统发送到内网之外，对方接收到的文件也是加密的格式，文件的内容无法泄露。

4) “移动硬件设备控制策略”设置及应用

- 为了防止企业员工通过移动硬件设备盗取企业中的机密数字信息，泄露企业的核心资产，可以通过思安智云管理系统系统控制台提供的硬件设备控制策略，定义禁止使用某些硬件设备及使用时间限制等。
- 应用该硬件控制策略的员工，在策略定义的时间范围内，则无法使用策略定义中的硬件设备。

图 4-4

5) “文件访问权限的细粒度的控制”设置及应用

- 设置：为了防止企业员工通过通用的文件访问权限把企业中该员工不应该看到的机密数字信息泄露，可以通过思安智云管理系统系统控制台提供的文件访问权限的控制，设置何种级别的用户能够访问某一类文件的权限。文件访问权限设置包括，复制/粘贴、可打印、访问时间、只读等。

- 应用：应用控制台对文件访问权限的设置之后，客户端按照管理者设置的文件访问权限控制进行文件访问权限的设置，设置完成之后，同时需要经过管理者审批之后，客户端才能够按照文件访问权限的设置进行访问。

6) “文件自动备份管理”的设置和应用

- 管理者可以通过控制台，设置文件备份的方式，是自动还是手动备份；设置文件备份的格式，哪种文件需要进行备份等信息。
- 用户在选用文件自动备份管理之后，客户端根据设定的自动备份条件，将相应的文件上传到文件自动备份服务器中。同时，管理员可以对文件备份服务器上存储的所有用户文件进行备份，并在需要时进行恢复。

7) “日志审计管理”的设置和应用

- 在控制台管理者能够查看到包括客户端、控制台的运行状态，客户端所有的文件操作进行详细的记录，还可以实现对所有的日志记录进行设置、查询、分析，提供审计的依据。
- 日志管理员还可通过查看报表（柱形、饼型及圆型）直观的查看操作统计报表记录；
- 每个客户端按照控制台设置的日志记录并上传的级别，记录各自客户端的操作行为，并定时上传到服务器上。管理者通过上传到服务器的每个客户端日志信息，进行日志的维护、查询、分析工作。

8） “文件解密审批”的设置和应用

- 在控制台由管理员指定审批管理员角色，并针对某用户或组设置专门的审批规则，即由哪些人按照何种审批顺序对解密请求进行审核。
- 审核管理员界面会及时弹出客户端自动提交的解密审批请求，根据情况对文件进行审核（批准或驳回）。
- 提交解密申请的客户端可随时查看解密请求的审核通过情况。

4.4 实施效果

通过思安智云管理系统系统的部署，完全能够杜绝现阶段企业内网环境中无法控制的机密信息对外泄露。同时，本产品在对企业中的机密文件信息进行保护的过程中，灵活的实现了受保护的企业机密文件在企业内外网中的正常使用。在极大地方便企业内网员工日常工作的同时，又保护了企业机密数字信息的安全管理。