中数国科

主机安全加固系统技术白皮书

（网络版）

中数国科集团有限公司

北京市朝阳区外馆斜街泰利明苑写字楼 A 座

电话：13660007444

修订记录

版本号	修订日期	修订内容	修订人

中数国科集团有限公司 地址：北京市朝阳区外馆斜街泰利明苑写字楼 A 座
网址：cdtc@cdtc.com.cn 全国统一服务热线：13660007444

目录

中数国科集团有限公司 地址：北京市朝阳区外馆斜街泰利明苑写字楼 A 座
网址：cdtc@cdtc.com.cn 全国统一服务热线：13660007444

公司概述

中数国科集团有限公司是一家专业从事信息系统安全管理、网络安全产品研发和销售，并提供整体解决方案的北京市高新技术企业及北京市科学技术委员会认定的软件企业，是国内率先提供“可持续发展网络安全整体解决方案”的网络安全服务商。

中数国科集团有限公司位于被称为“中国硅谷”的中关村高科技园区上地信息产业基地。公司与军队系统信息安全研究部门以及国内外信息安全研究领域的众多权威机构建立战略合作关系，并且时刻紧跟国外网络安全方面的最新技术，积极掌握国际、国内信息安全技术的最新发展趋势，提出了一系列的安全体系设计思想和研究理念。中数国科集团有限公司凭借在安全方面的技术实践经验和人员优势，通过设计实施一批国家重点工程，培养了一支技术过硬、品质过硬的高级专业科技队伍，研发出了具有自主知识产权的安全隔离与信息交换系统（以下简称为网闸）、光闸、防火墙、工业防火墙、数据交换平台、网络入侵检测等系列科研成果，为公司在信息系统安全设计、构建、实施、服务领域的发展奠定了坚实的技术基础。

中数国科集团有限公司 地址：北京市朝阳区外馆斜街泰利明苑写字楼 A 座
网址：cdtc@cdtc.com.cn 全国统一服务热线：13660007444

文档介绍

首先，感谢使用中数国科主机安全加固系统（以下简称主机安全加固）!

中数国科主机安全加固由中数国科集团有限公司自主研发的、具有自主知识版权的主机安全加固软件。该系统从保障服务器操作系统安全的角度出发，以可信计算为基础、访问控制为核心，围绕“可信、可控、可管”三个维度构建服务器主动防御体系，从源头上保证服务器安全。

中数国科集团有限公司 地址：北京市朝阳区外馆斜街泰利明苑写字楼 A 座
网址：cdtc@cdtc.com.cn 全国统一服务热线：13660007444

1 背景

1.1 安全隐患

服务器作为信息系统核心组成部分，承载着信息系统关键的业务服务，随着信息化的不断完善，各式各样的业务服务也越来越多，在这些业务服务正常运行的同时，也面临着严重的安全问题。由于目前大多服务器安装的均为国外商业操作系统例如 Windows、Linux、Solaris 等系统，这些系统虽然保证了系统的稳定性，但缺乏必要的安全防护措施，一旦用户使用不当或遭到攻击和破坏，极容易导致服务器无法正常运行，致使国家或企业遭到巨大经济损失。

目前，服务器面临的主要安全风险，如操作系统或应用程序存在漏洞、系统被入侵、病毒木马的感染、系统配置或业务软件配置不当、系统管理员有意或无意的危险操作、缺乏有效的安全审计等安全问题，造成信息系统中服务器在运行过程中出现各种各样不稳定因素，影响业务服务的正常运行。

1.2 安全现状

目前对于信息系统安全防护，用户对基于网络应用的外部防范关注较多，却忽略了服务器自身安全防护。然而在应用系统中最薄弱、易受攻击、而保护力度又相对缺乏的就是对服务器的保护。当前针对服务器的攻击事件层出不穷，攻击手段多种多样，从用户身份伪造、系统完整性破坏到重要数据完整性破坏、泄密，从因特网黑客外部攻击到内部人员攻击，服务器总是处于安全的核心。另一方面，商用操作系统在安全结构上的缺陷，又进一步为服务器攻击提供机会。今天的商

中数国科集团有限公司 地址：北京市朝阳区外馆斜街泰利明苑写字楼 A 座
网址：cdtc@cdtc.com.cn 全国统一服务热线：13660007444

用操作系统，在注重功能性的同时，却严重忽略了安全性保护，如管理员权限过于集中、程序运行控制机制薄弱、核心进程及关键目录的防护控制不足等等。

针对服务器操作系统存在的诸多安全问题，我公司经过对服务器存在的安全隐患进行认真分析，结合自身多年的操作系统安全加固经验，开发了主机安全加固系统，该软件从 防止病毒木马入侵、恶意软件启动、系统漏洞利用、配置参数不合规、管理人员违规访问等方面入手，为 Windows、Linux、Solaris 等系统提供基于可信的程序可信检测、核心目录防篡改、移动介质权限控制、网络通信控制、核心进程防护、远程运行控制和统一集中管理（系统管理、安全配置、安全审计）等安全技术。针对服务器“运行安全、数据安全、安全管理”三个层面进行安全防护设计，打造服务器全生命周期的安全防护，全方位保障服务器的安全。

2 设计思路

2.1 产品概述

本产品从保障服务器操作系统安全的角度出发，以可信计算为基础、访问控制为核心，围绕“可信、可控、可管”三个维度构建服务器主动防御体系，从源头上保证服务器安全。

产品在安装部署后，提供操作系统内核级加固、核心进程防护、关键目录保护等安全机制，逐步建立完善的服务器操作系统级安全管理体系，给予服务器主动防御的能力，保障服务器的运行安全、数据安全及安全管理，为服务器提供全面的安全防护。

中数国科集团有限公司 地址：北京市朝阳区外馆斜街泰利明苑写字楼 A 座
网址：cdtc@cdtc.com.cn 全国统一服务热线：13660007444

2.2 产品价值

2.2.1 降低服务器被攻击风险

本产品以用户身份可信、执行程序可信为基础，通过限制程序及目录的访问控制，实现对目录及程序进程的行为的限制，从而从身份、权限以及安全审计三个层面建立服务器自身主动安全防御机制，降低服务器自身被攻击的风险。

2.2.2 满足行业政策及标准要求

本产品从访问控制、移动存储控制、安全审计、恶意代码防范、入侵防范等几个方面对操作系统都进行了有效加固，满足等级保护基本要求、等级保护安全设计技术要求、分级保护、以及各行业标准等对主机安全的要求，能够提高操作系统等级保护、分级保护以及行业标准的符合性，适用于等级保护二级、三级、四级主机安全应用场合。

2.2.3 提高服务器安全运维效率

本产品提供服务器安全集中管控中心，以 B/S 架构部署，支持服务器基线配置、安全策略下发、安全策略同步等功能，减少管理员重复工作，大大提高管理员安全运维效率。

中数国科集团有限公司 地址：北京市朝阳区外馆斜街泰利明苑写字楼 A 座
网址：cdtc@cdtc.com.cn 全国统一服务热线：13660007444

2.3 产品优势

（1） 可信计算技术

随着可信计算工作组在国家信息中心宣告成立以及可信计算技术的开发、应运和部署，一种构建可信计算技术体系应运而生。借鉴这种可信思想并将这种思想应用于实际产品中，在操作系统底层建立一个信任根，从信任根开始到硬件平台，再到应用进程、文件等，一级认证一级，一级信任一级，建立一条信任链，从而把这种信任扩展到整个服务器系统，提高服务器系统的安全性。

（2） 主动防御技术

采用主动防御技术，当有恶意代码启动时进行有效的拦截并进行审计，从中了解黑客意图、手段，通过对启动程序进行分析取证找到破坏的根源，以保证服务器的操作系统安全，将恶意事件控制在源头。

（3） 内核级安全加固技术

服务器的安全加固工作建立于操作系统内核层，既能准确全面的截获应用层的访问请求，又降低了系统安全机制被旁路的危险，这也为系统的安全模块自我保护、防卸载等构筑了坚固的防线。

（4） “控制与防护”结合的加固策略

服务器的安全加固一方面通过对非可信的程序控制，外设存储控制防止病毒木马入侵、恶意软件启动、系统漏洞利用、配置参数不合规、管理人员违规访问的控制策略，另一方面通过白名单机制对可信的核心程序和关键目录予以保护，通过”控制与防护”结合的加固策略全方位实现对服务器系统的加固。

2.4 设计思路

“可信”即以可信认证为基础，构建一个可信的业务系统执行环境，即平台、程序、进程都是可信的，确保病毒无法执行、入侵行为无法成功。可信的环境保证业务系统永远都按照设计预期的方式执行，不会出现非预期的流程，从而保障了业务系统安全可信。

“可控”即以 IP、端口访问控制技术为核心，实现远程登录控制。同时基于白名单技术，实现对程序的运行控制。保证所有的执行操作行为均在可控范围之内进行，在防范内部攻击的同时有效防止了从外部发起的攻击行为。对核心进程，关键目录进行防护，可以确保系统中的核心资源不被篡改，保证了核心资源的安全可控。

“可管”即通过构建集中管控、最小权限管理与三权分立的管理平台，为管理员创建一个工作平台，使其可以进行技术平台支撑下的安全策略管理，从而保证信息系统安全可管。

中数国科集团有限公司 地址：北京市朝阳区外馆斜街泰利明苑写字楼 A 座
网址：cdtc@cdtc.com.cn 全国统一服务热线：13660007444

3 功能简介

3.1 可信

3.1.1 执行程序可信

基于可信计算技术，采用白名单机制，提供执行程序可信度量，阻止非授权及不符合预期的执行程序运行，实现对已知/未知恶意代码的主动防御，降低操作系统完整性及可用性被破坏的风险。

采用可信程序保护机制，禁止任何程序或用户对可信程序进行篡改，保障服务器中的程序能够稳定运行；支持基于可信计算技术对服务器中运行的业务程序或其他可信程序进行防篡改检查；拦截以任何方式对服务器中业务程序的删除、修改等危险操作；记录可信程序变更记录，并支持在得到授权允许时恢复可信程序；与可信检测平台联动，通过自动下载可信检测平台中对应程序的保护策略，实现程序防护策略动态调整。

恶意代码防御

提供基于可信计算技术的恶意代码防御机制，对执行程序进行可信检测，确保恶意程序或与业务无关的程序无法在服务器中运行；拦截服务器中可执行程序执行请求，只允许经过可信验证的安全程序才能在服务器中运行，有效拦截已知、未知病毒、木马及其他恶意软件；与可信检测平台联动，通过自动下载程序可信检测平台中的程序知识，转化为服务器本地的安全运行策略，并能够将服务器中的未知程序（即不在白名单里的程序）信息发送给可信检测平台，由可信检测平台进行可信安全分析。

中数国科集团有限公司 地址：北京市朝阳区外馆斜街泰利明苑写字楼 A 座
网址：cdtc@cdtc.com.cn 全国统一服务热线：13660007444

3.2 可控

3.2.1 核心进程防护

核心进程的防护是主机加固的重中之中，系统支持对核心进程的单独防护模块。可以防止该进程被非法结束，从而保证核心进程的正常运行。

3.2.2 关键目录保护

对关键目录提供基于文件级的目录保护机制，提供关键目录的专项保护策略，防止目录及其下的文件（夹）被恶意篡改,防止目录内容的添加及修改。保证关键目录的正常访问。

3.2.3 远程登录控制

提供基于网络层的远程登录访问控制，支持对远程登录的允许和禁止操作控制，可实现同一主机服务器的基于源 IP 地址的远程登录控制，满足了特定远程控制许可的业务需求。当出现非授权 IP 操作时，拒绝操作，并记录安全事件告警。

3.2.4 程序运行控制

基于白名单技术实现对应用程序的保护，纳入程序白名单的程序是安全可信的。禁止非白名单应用程序的运行安装，从而有效控制非法程序运行安装带来的主机安全威胁。

3.2.5 外设存储控制

通过禁止或允许移动存储设备在服务器上使用，有效防止移动存储设备的随意接入对服务器系统的安全威胁。

提供移动介质授权管理，移动介质在使用前均须经过授权；禁止非授权外设

中数国科集团有限公司 地址：北京市朝阳区外馆斜街泰利明苑写字楼 A 座
网址：cdtc@cdtc.com.cn 全国统一服务热线：13660007444

存储的接入。有效防止由于非授权移动存储接入而产生的攻击。

3.2.6 网络通信控制

按照等保 2.0 的要求提供基于 IP，端口，协议的多维网络通信控制，提供网络访问控制，IP 白名单和 IP 黑名单三种控制规则。

将 IP 白名单列入可信列表，将 IP 黑名单列入非可信列表，当出现非授权 IP 通信请求时，拒绝操作，并记录安全事件告。

3.2.7 执行程序监控

对指定目录下可执行程序运行实现有效的拦截，审计控制。对受控主机的执行程序进行有效的监控，防止非法程序的执行。并为主机加固策略提供有效的依据。

3.2.8 强制访问控制

本产品提供基于 BLP 模型的强制访问控制，强访问控制首先对主体(用户)和客体（文件）进行安全级别定义，然后对不同的安全级别的主客体制定读写的基本访问控制策略。BLP 模型的基本安全策略是“上读下写”，高安全级别主体只可以读安全级别比它低的客体，低安全级别主体只可以写安全级别比它高的客体，同级别主客体间可读写，“上读下写”的安全策略保证了数据流向中的所有数据只能按照安全级别从低到高的流向流动，从而保证了敏感数据不泄露。

3.3 可管

3.3.1 安全状态展示

提供对整体环境的安全现状展示，展示数据动态实时更新。提供注册资产总数、异常资产总数等资产信息，最新安全事件及详细信息、待办安全事项、持续

中数国科集团有限公司 地址：北京市朝阳区外馆斜街泰利明苑写字楼 A 座
网址：cdtc@cdtc.com.cn 全国统一服务热线：13660007444

拦截威胁总数、系统安全风险指数、安全事件分类统计、安全事件趋势、安全事件最近一周发生趋势等多个维度展示主机安全状态。为整体运行环境安全风险分析提供参考。

3.3.2 节点管理

节点管理模块是给系统管理人员提供一个节点资产维护的统一视角，通过该模块，运维人能够方便的查看某台主机服务器名称、操作系统、在线状态、位置、资产标签等信息，同时平台可提供对主机资产的统计管理。能够实时对服务器节点的操作系统，在线状态，位置等资源信息进行采集；支持查询服务器历史资源信息。

3.3.3 安全基线配置

提供基于操作系统的安全基线配置功能，能够一键配置启用系统安全基线，使操作系统自身安全机制充分发挥作用，从而提高系统运行环境安全，简化安全管理配置工作；支持对管理账户的安全基线配置，同时支持根据业务或运维需求，将系统安全基线一键还原到系统默认状态。

3.3.4 多种控制模式

本系统的部分控制分为保护模式，监视模式，关闭状态三种模式。为用户提供方便灵活的控制策略。

3.3.5 安全审计

本产品提供操作系统审计功能，审计内容包括：提供用户登录审计、程序运行控制审计、文件访问控制审计、可信程序保护审计、进程防护审计、外设存储审计、网络通信审计、执行文件审计等同时支持日志的检索和导出功能。

中数国科集团有限公司 地址：北京市朝阳区外馆斜街泰利明苑写字楼 A 座
网址：cdtc@cdtc.com.cn 全国统一服务热线：13660007444

系统还提供了向特定邮箱发送告警日志的功能。

3.3.6 等保评分

产品不仅从访问控制、移动存储控制、安全审计、恶意代码防范、入侵防范等几个方面对操作系统都进行了有效加固，满足等级保护基本要求，并从身份鉴别，访问控制，安全审计，入侵防范，资源控制等多个视角对所有受控终端安全现状进行等保评分分析，并以图形化，数值化的方式直观的将分析结果投放给用户。终端等保情况一目了然。

3.3.7 基线扫描

基线配置是主机安全的基本保障，系统支持对终端节点基线配置项信息的自动获取，将基线结果清晰呈现给用户。并为用户提供了一键配置操作，完成对基线配置项的合理设置。大大降低了用户的配置难度和配置过程。

3.3.8 卸载控制

为防止受控节点的有效性，产品提供客户端的卸载申请，只有提交卸载申请并获得管理中心卸载码的客户端才可以对客户端进行卸载。有效防止由于受控节点随意卸载客户端程序而产生的安全威胁。

同时，卸载控制可以按需由管理员进行开关的设置，提高了产品的灵活性和适用性。

4 部署方式

本产品采用 C/S 部署模式、B/S 管理模式。支持单机版和网络版两种部署方

中数国科集团有限公司 地址：北京市朝阳区外馆斜街泰利明苑写字楼 A 座
网址：cdtc@cdtc.com.cn 全国统一服务热线：13660007444

式。

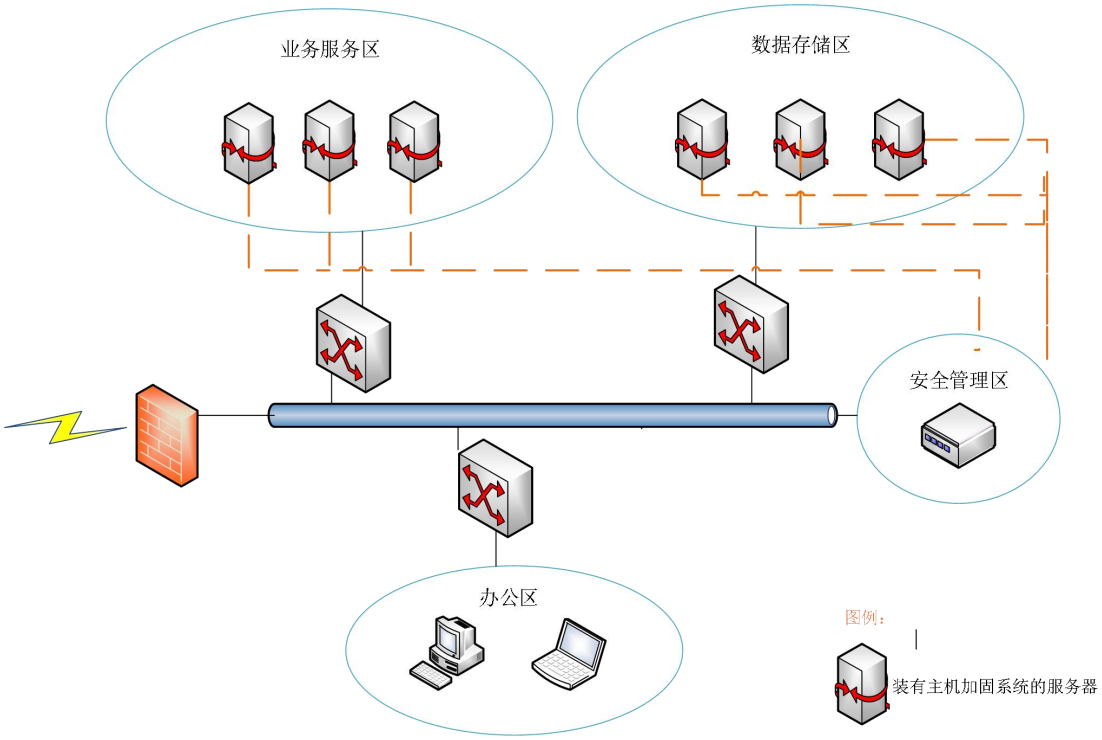

图 4.1 部署结构图

5 安全防护效果

■ 抵御各种入侵行为

通过对服务器的操作系统进行安全加固，从系统底层为出发点，以可信计算技术为基础、访问控制为核心，保证服务器的安全，形成严密的安全保护环境，抵御病毒木马等恶意代码的入侵行为。

■ 提高整体防御力

通过对操作系统本身的安全加固，打造服务器本身的免疫系统。可以有效的规避因打补丁给服务器带来的风险，切断黑客的攻击途径。同时，本方案通过主

中数国科集团有限公司
网址：cdtc@cdtc.com.cn
地址：北京市朝阳区外馆斜街泰利明苑写字楼 A 座
全国统一服务热线：13660007444

动防御和防网络攻击等功能弥补了传统安全产品的不足，避免出现信息安全的短板效应，提高了系统的整体防御能力。

■ 构建统一安全管理平台，集中管控全部服务器

通过构建统一安全管理平台（安全管理中心），对整个网络系统的服务器统一管理、集中控制，保证各项安全机制的高度协调统一。消除各个服务器由于配置不同造成的安全隐患，最终构建一道针对整个服务器系统的整体安全防线，有效保护服务器系统中的信息安全。

■ 防止摆渡木马感染

摆渡木马非常隐蔽，但该木马要运行发作，就需要通过移动介质进感染系统，并常驻系统中。安装配置操作系统进行安全加固以后，可以保护系统不被移动介质中的病毒感染。

■ 免疫木马病毒的破坏

主机加固系统软件不从特征上来判断病毒或者木马，而是根据配制信息从行为上判断其是否会破坏系统和应用，只要其破坏主机安全加固系统软件就阻止，所以无论是已知或未知病毒木马都是无法运行的。

■ 提升操作系统安全等级

主机安全加固系统软件不需要改变任何原有系统结构以及应用流程，从内核层保护系统和应用的关键位置不被恶意破坏，可按需求配制保护策略，从而保证业务系统的正常运行。

中数国科集团有限公司 地址：北京市朝阳区外馆斜街泰利明苑写字楼 A 座
网址：cdtc@cdtc.com.cn 全国统一服务热线：13660007444