

目 录

1. 公司简介	- 1 -
2. 引言	- 2 -
2.1 防内对重要信息系统安全的意义	- 2 -
2.2 防内的主要内容	- 3 -
2.2.1 防重要信息失窃密	- 3 -
2.2.2 防系统完整性破坏	- 3 -
2.3 传统安全技术无法彻底解决防内问题	- 4 -
2.4 安全操作系统在防内中的重要意义	- 5 -
3. “节点一操作系统安全加固”概述	- 6 -
3.1 “节点一操作系统安全加固”设计理念	- 6 -
3.2 “节点一操作系统安全加固”产品组成	- 8 -
4. “节点一操作系统安全加固”功能介绍	- 10 -
4.1 身份鉴别	- 10 -
4.2 执行程序可信度量	- 11 -
4.3 可信代码防篡改	- 11 -
4.4 程序安装控制	- 11 -
4.5 自主访问控制	- 12 -
4.6 强制访问控制	- 12 -
4.7 网络访问控制	- 12 -
4.8 数据完整性保护	- 13 -
4.9 数据保密性保护	- 13 -
4.10 移动介质权限控制	- 13 -
4.11 移动介质加密保护	- 14 -
4.12 终端统一管理	- 14 -
4.13 行为监控审计	- 14 -
4.14 管理员职责分离	- 14 -
5. “节点一操作系统安全加固”技术特点	- 15 -
6. “节点一操作系统安全加固”产品优势	- 17 -
附录 1: 产品资质	- 20 -
附录 2: 公司资质	- 21 -
版权声明	- 22 -

1. 公司简介

北京中软华泰信息技术有限责任公司（Beijing HuaTech Information Technology Co., Ltd）成立于 2000 年（以下简称中软华泰），是专业从事信息安全关键技术研究及产业化实践的国家级高新技术企业，是国内实力雄厚的网络安全产品、可信计算产品、安全服务与解决方案的综合提供商。

公司现有员工 150 余名，其中技术研发和技术支持人员 83 名，拥有博士 9 人，硕士 19 人。十年来，中软华泰秉承“科技兴邦、产业报国”的企业理想，专注于可信计算和操作系统安全的探索实践，首推“计算节点（计算环境）安全”理念，并在关键技术应用方面取得了突破性进展。

近年来，公司成为国家与微软公司源代码级技术合作单位，并先后参与了国家多项重大产业项目。2007 年成为中国可信计算联盟成员之一。2008 年初，公司独立承担了信息安全等级保护国内第一个部委级整改项目，并于当年通过国家测评和验收，同年公司参加了信息安全等级保护 863 课题组，继续深入研究信息安全等级保护关键技术。2009 年公司参加了国家标准 GB/T 25070—2010《信息安全技术-信息系统等级保护安全设计技术要求》的编写工作，同年公司加入信息安全等级保护技术联盟。

为了更好的服务国家，定向输送掌握信息安全关键技术的专业人才，公司坚持产、学、研相结合，2008 年和 2010 年先后与北京交通大学、北京工业大学共同设立“研究生联合培养基地”。在为国家输送大批信息安全专业人才的同时也使公司具有了坚实的技术储备。

经过几年的努力，公司凭借自身一流的键技术研究能力、产业化运作能力和优秀的服务能力赢得了广大客户的支持与信赖，产品已经在各级政府机关和相关涉密企事业单位得到了广泛应用，覆盖政府、金融、能源、电力、军工、企业、教育、医疗、电子商务等众多行业领域。

中软华泰公司总部设在北京，现已设立北京、上海、天津、南京、西安、深圳分公司，吉林、河北、山东、湖北、安徽、贵州办事处，初步建成了较为完善的全国销售和技术服务支持体系。

2. 引言

党的十六大确定了“以信息化带动工业化，以工业化推动信息化，从而全面实现现代化”的基本战略。然而随着信息化的不断推进，信息安全问题是难以避免的，因此应该坚持科学发展的观点，统筹兼顾，做好信息安全保障工作。2003年9月，中共中央办公厅下发了27号文件《国家信息化领导小组关于加强信息安全保障工作的意见》，该文强调“信息安全保障工作要以‘三个代表’重要思想为指导，坚持积极防御、综合防范的方针，全面提高信息安全防护能力，重点保障基础信息网络和重要信息系统安全，创建安全健康的网络环境，保障和促进信息化发展，保护公众利益，维护国家安全”。

“节点—操作系统安全加固”产品是以27号文件为指导，以可信终端为出发点，以重要信息系统安全为目标研发成功。该产品通过加强终端系统的可控性、可管性，使得安全管理员及用户对终端的运行状态心中有数，从而可以有效阻止各种来自网内、网外的攻击，增强了信息系统的安全性。

2.1 防内对重要信息系统安全的意义

内部人员攻击是指获得授权的合法用户从信息系统内部发起的攻击。由于内部人员直接接触重要信息，并且了解信息系统的安全防御措施和管理手段，因此相对于外部用户而言，其更容易规避安保制度，利用系统安全防御措施的漏洞或管理体系的弱点，从内部发起攻击来破坏信息系统的安全，从而达到某种不可告人的目的。据国际权威机构统计，80%的信息安全事故都是内部工作人员或内部工作人员与外部人员相互勾结所为，且这种现象呈上升趋势。一系列的实际案例可以说明，来自内部的数据失窃和破坏，远远高于外部黑客的攻击。因此防止内部用户攻击是保障重要信息系统安全的基本任务。

然而目前传统的安全防护措施大多只针对来自外部的攻击进行防范，而俗话说家贼难防，因此内部人员的攻击更应该作为重点的防范对象。我国主管部门规定重要信息系统网络必须和其他公共网络进行物理隔离，因此对重要信息系统的安全而言，其安全威胁主要来自于内部用户，尤其是内部精通业务、懂技术、会编程的专业人员的主动攻击。分析研究表明，如果信息系统的安全保障措施比较完善，不但能够达到有效防止内部用户攻击的效果，而且该信息系统也能彻底杜绝合法用户因不慎违规操作而造成的信息安全事故，从而整体消除内部用户有意或无意地制造的信息安全事故。可见保护重要信息系统的安全，必须以防内为主，内外兼防为出发点，从源头进行治理。

2.2 防内的主要内容

防止内部恶意用户对信息系统安全的破坏，归根到底，是防止其对信息系统中资源的机密性、完整性以及系统可用性的破坏。内部用户可以利用安全防护措施的漏洞来主动泄露重要信息，可以通过植入恶意代码来盗取敏感信息，可以利用操作系统或上层应用的漏洞进行网内攻击，从而获取终端系统的控制权或植入恶意代码。信息系统防内应从以下几个方面考虑：

2.2.1 防重要信息失窃密

随着信息化的高度发展，重要信息越来越容易被复制和传播，从而导致重要信息系统的失窃密事件频繁发生，严重损害了相应组织机构的利益，甚至威胁到了社会秩序、公共利益和国家安全。例如：即使信息系统和互联网隔离，其终端系统仍然可能被病毒、木马入侵或恶意攻击，那么其中的重要信息就很容易被窃取或外泄，造成用户无意失密。另外出于各种利益的驱使，信息系统中的一些合法用户可能有意规避安全防护制度，利用现有防护技术的漏洞，通过网络、移动介质等途径主动泄密，或者通过网内攻击，恶意植入病毒、木马等手段主动窃密。

从信息系统的结构以及失窃密的途径来看，可以将失窃密事件分为如下几类：1) 通过移动存储介质泄密；2) 通过非授权降低重要信息机密级泄密；3) 通过恶意攻击窃密；4) 通过盗取计算机或相应设备泄密；5) 通过网络资源泄密。

可见，为了防止内部用户有意或无意的失窃密行为，必须做到以下几点：1) 严格控制用户行为，对系统中的主体（用户）及客体（文件、目录、移动介质）进行标记并制定级别，实行强制访问控制，严格限制低级别主体访问高级别客体的行为发生；2) 对于重要信息进行完整性及保密性保护，防止被非法篡改、泄密；3) 网络访问控制，防止非授权用户进入信息系统及重要信息非法流出信息系统。

2.2.2 防系统完整性破坏

系统完整性遭破坏是当前信息系统面临的另一安全威胁。如果内部用户无意激活了存储在计算机上的病毒、木马、攻击程序等恶意代码，该恶意代码就继承了当前用户的权限，可以肆无忌惮地进行传播，为所欲为地破坏信息系统的完整性，例如在用户毫不知情的情况下修改或删除信息系统中的重要信息，或者破坏系统中的一些重要服务，导致系统无法正常运作等。

恶意用户的非法操作和植入恶意代码行为能够破坏系统安全的主要原因是当前操作系统在启动执行代码时不对其进行真实性和完整性检查，这给恶意代码的发作留下了可乘之机。因此，为了保障



信息系统的安全，必须防范各种已知及未知病毒、木马、攻击程序破坏系统完整性的攻击，从根本上保证系统的完整及可信。

此外随着网络技术的发展，远程恶意攻击的现象越来越普遍。远程恶意攻击一般都是先通过植入木马来控制目标机器，然后再进行后续攻击，其能够成功的主要原因是被攻击终端操作系统或上层应用存在安全漏洞。虽然我国主管部门规定重要信息系统必须和其他公共网络物理隔离，从而降低了重要信息系统遭受远程恶意攻击的可能性。但是系统中的恶意用户也可能通过网内攻击的手法攻击信息系统中的其他终端，以达到其不可告人的目的。因此为了保障信息系统的完整性，必须加强信息系统的网络访问控制，防止恶意用户利用现有信息系统的漏洞破坏系统完整性。

2.3 传统安全技术无法彻底解决防内问题

目前，市面上大部分的信息安全产品以防范外部攻击为主，如防火墙、防病毒软件、入侵检测设备等等。由于计算机病毒、木马、蠕虫等恶意软件层出不穷，加之外围攻击手法不断升级，致使这些被动防护系统捉襟见肘、漏洞百出，信息系统安全屡屡受到威胁和破坏。即使亡羊补牢，将系统防火墙策略越做越严、入侵检测规则库越做越复杂、恶意代码特征库越做越大，但是由于这些防护手法依赖于攻击手法的特征，致使其防护能力永远滞后于新的攻击，结果仍是防不胜防。产生这种局面的根本原因在于没有对存在不安全因素的终端进行控制，而一味地在外围进行封堵，试图阻止外来的攻击和入侵，对来自内部用户的作案毫无防范能力。

然而，虽然当前也有些产品从终端安全出发，来防范内部用户对重要信息系统的攻击行为，如单一的用户身份认证、文档加密、移动介质控制、网络接入控制、用户行为审计等，但是这些产品只是片面地去解决一些应用安全问题，是头痛医头，脚痛医脚，治标不治本的做法。即使将这些安全产品简单地叠加，同样无法达到全面防内的效果。根据木桶理论，信息安全的防护强度取决于其中最为薄弱的一环，因此不能孤立、片面地思考信息安全问题，而应该将其看成一个整体，从系统的观点、方法来分析信息系统的安全，确定合理的安全体系结构，为信息系统的安全保护提供方法和指导。

另外由于现有主流操作系统在安全保障措施方面的不足，系统安全机制容易被旁路，给病毒、木马、攻击程序等恶意代码留下了可乘之机。例如，现有的一些病毒程序被激活后，会阻止或破坏系统中杀毒软件的正常运行，从而使系统失去病毒防护能力。这样即使利用系统的观点，在现有操作系统基础上给出一系列的安全防护措施，也无法达到整体防内的效果。因此必须从操作系统核心层面出发，增强现有主流操作系统的安全保障机制，保证上层安全机制的正确执行，并且提供安全管理平台，方便管理员制定并强制实施统一的系统安全策略，确保系统始终处于可控状态。

2.4 安全操作系统在防内中的重要意义

终端是一切不安全问题的根源，终端安全是信息系统安全的源头，如果在终端实施积极防御、综合防范，努力消除不安全问题的根源，那么重要信息就不会从终端泄露出去，病毒、木马也无法入侵终端，内部恶意用户更是无法从内网破坏信息系统安全，内部用户攻击的问题迎刃而解。

安全操作系统是终端安全的核心和基础。如果没有安全操作系统的支撑，终端安全就无法得到保障。黑客就可以利用操作系统的漏洞窃取超级用户权限，肆意进行破坏；病毒程序就可以利用操作系统缺乏对执行程序进行真实性和完整性检查的弱点，将病毒代码嵌入到执行程序中，实现病毒的恶意传播、破坏；更为严重的是如果没有安全操作系统，就不可能有严格的访问控制机制，合法用户就可以进行越权访问，造成不安全事故的发生。并且如果没有安全操作系统的支持，终端上的一切安全机制就如无源之水、无本之木，无法保证自身的完整性，无法从根本上防止恶意代码或黑客攻击，更无法防止内部用户的攻击。

因此，通过安全操作系统所提供的安全机制，赋予终端系统主动防御的能力。如通过身份认证机制可以确保非授权用户无法登录终端，从而保证能够访问信息系统的用户是可控的；通过强制访问控制机制可以限制用户的权限，规定用户能做什么，不能做什么，防止越权访问，确保重要信息无法被非法泄露或窃取；通过数据加密保护机制，可以确保非授权用户无法获取可用的重要信息；通过执行程序可信度量机制，可以确保系统环境无法被病毒、木马等恶意程序修改；通过用户行为审计机制，可以防止违规用户的抵赖行为，以方便事后追查。因此，安全操作系统在防内中起着至关重要的作用。

3. “节点—操作系统安全加固”概述

为了全面解决重要信息系统内部用户攻击的问题，中软华泰在对攻击手段及传统安全产品进行详尽分析的基础上，经过多年研发，推出了“节点”系列的操作系统加固产品：“节点—操作系统安全加固”。该产品以安全管理平台策略控制为核心，以终端节点安全为基础，通过对现有操作系统进行安全增强，使得管理员能够对终端节点进行集中管理和控制，保证信息系统始终在可控状态下运行，从而从根源上有效抑制对信息系统安全的威胁，最终达到防止内部用户以及外部用户攻击的目的。

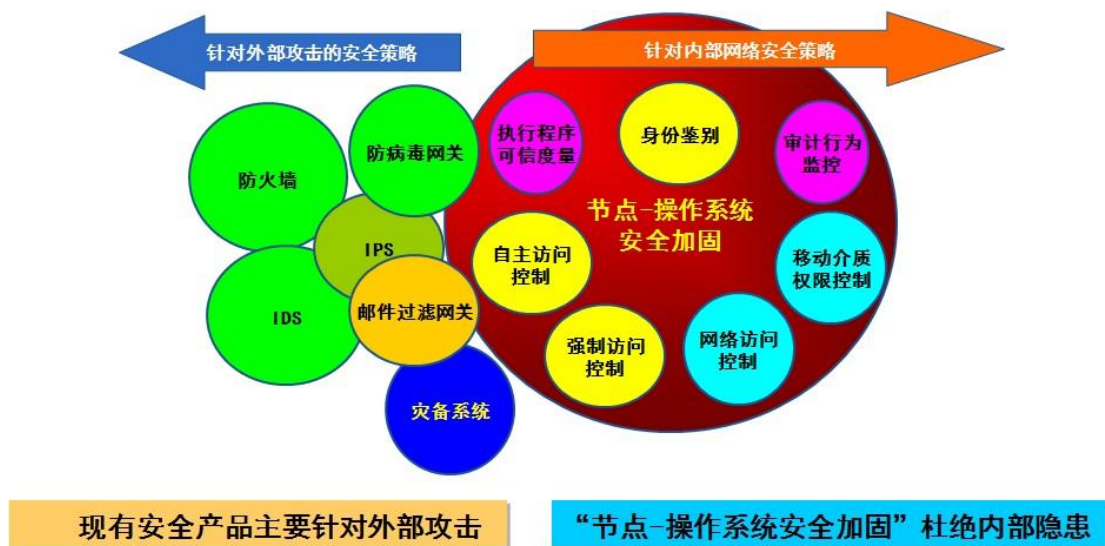


图 3：“节点-操作系统安全加固”产品全面解决防内问题
(本图未列出产品全部功能，具体功能请参考正文介绍)

3.1 “节点—操作系统安全加固”设计理念

产品设计理念：以可信计算为基础，访问控制为核心，构建终端整体安全防御体系，实现“防失窃密”、“防系统破坏”、“确保系统可用”的安全目标。

1) 以可信计算为基础，访问控制为核心

作为商用操作系统，现有操作系统侧重于系统的易用性，用户登录终端后可以运行任意程序，查看、修改系统中的任意信息，因此在对信息的机密性、完整性保护方面存在很多不足，无法保障我国重要信息系统的安全。

近几年来，可信计算技术蓬勃发展。可信计算的基本思想是：首先构建一个信任根，再建立一条信任链，从信任根开始到硬件平台，到操作系统，再到应用，一级认证一级，一级信任一级，把这种信任扩展到整个计算机系统，从而确保整个计算机系统的可信。

访问控制是针对越权使用资源的防御措施，是为了限制访问主体（用户）对访问客体（文件、目录、移动介质）的访问权限，从而使计算机系统在合法范围内使用；决定用户能做什么，也决定代表一定用户利益的程序能做什么。

由此“节点—操作系统安全加固”产品采用以可信计算为基础，访问控制为核心的设计思路，在不改变原有操作系统应用的前提下，打造新一代的安全操作系统：以可信计算为基础，在操作系统底层采用白名单的方式，通过对可执行程序的真实性和完整性度量，既能防止用户使用非法程序，又能防止病毒、木马的侵袭；以访问控制为核心，在系统原有自主访问控制的基础上，通过对重要的主体/客体进行安全标记，划分级别，制定访问控制策略，实施强制访问控制，严格控制用户行为，实现对终端操作系统及重要数据的安全保护。

2) 构造终端整体安全防御体系

由于现有操作系统各终端的防御手段、安全配置等参差不齐，其防御能力也各不相同，但任何一个终端遭受攻击，都可能影响整个信息系统的安全。因此，本产品通过构建全系统统一的“安全管理平台”，对系统中的所有操作系统终端进行统一管理、统一配置，审计信息统一存储、统一分析，最终构建一道针对整个信息系统的整体安全防线，有效保护系统中的信息安全。

安全管理员通过规定“哪个用户可以登录哪个终端”以及“哪个终端可以接入网络”，确保非授权用户无法访问内网资源；通过规定终端上的用户“能够做什么，不能做什么”，只赋予其完成任务的最小权限，从而防止重要信息被外泄；通过强制要求终端“在存储过程中对重要信息加密”，从而确保即使重要信息被盗取，信息盗取者也无法获得信息明文；通过确定终端“软件栈的状态，即用户可执行什么软件，软件满足什么样的完整性状态才能被执行”，从而确保恶意代码无法入侵终端，系统环境无法被修改；通过规定“什么样的行为需要纳入审计行列”，从而确保恶意行为痕迹无法被破坏，以方便事后追查。

由此可见，管理员通过制定安全策略，对系统中的终端进行集中管理和控制，“节点—操作系统安全加固”产品构建了终端对于非授权用户的“五不”，即：“进不来”、“拿不走”、“看不懂”、“改不了”、“赖不掉”的整体安全防御体系，系统能够达到防失窃密、防系统破坏、确保系统可用的目的，如图 3.1 所示：

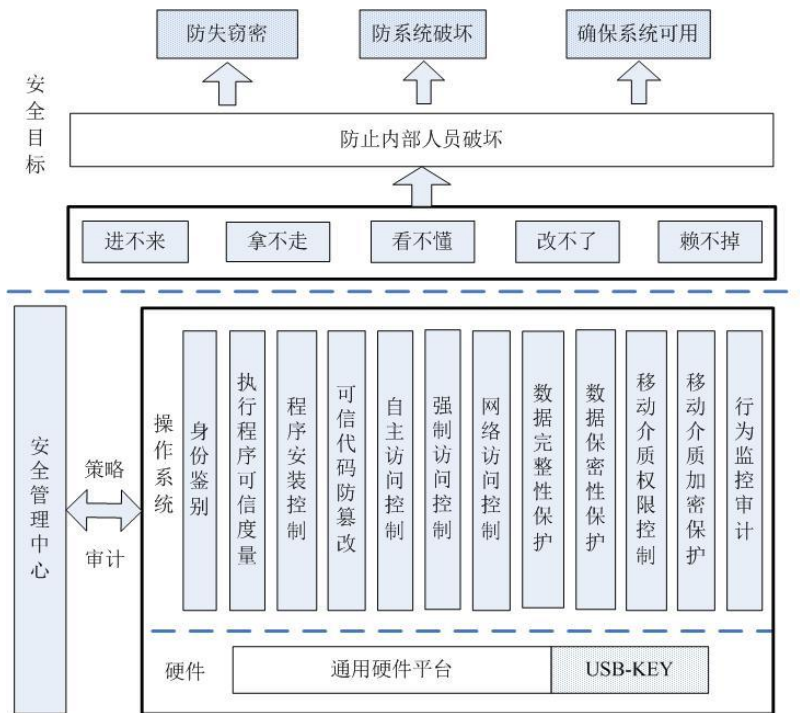


图 3.1: 非授权用户的“五不”的整体安全防御体系

3.2 “节点—操作系统安全加固”产品组成

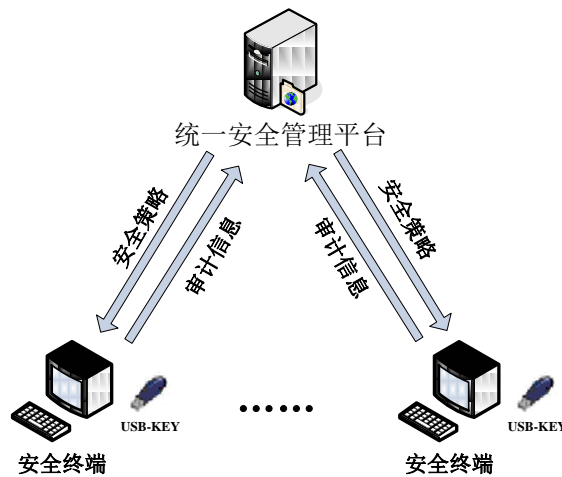


图 3.2: “节点—操作系统安全加固”产品系统组成

“节点—操作系统安全加固”是软硬件相结合的产品，通过硬件 USB-KEY，提高了系统的安全性，克服单纯使用软件防护的局限性；软件部分包括终端操作系统安全增强软件、终端安全代理以及统一安全管理平台软件。

硬件部分 USB-KEY 是一个 USB 接口的可信模块：（1）USB-KEY 是用户身份识别的唯一标识，是用户登录的令牌凭证。（2）USB-KEY 内置了经国家密码管理委员会批准的密码算法，是加解密运算介质。

软件部分：（1）终端操作系统安全增强软件，统一实施统一安全管理平台下发的安全策略，实现用户身份的认证、访问控制、数据保护、审计用户的操作、敏感信息的加解密、网络连接控制等的安全防护控制（2）终端安全代理，主要负责终端与安全管理平台交互，包括安全策略的下载、更新，审计信息的上传以及移动介质的注册等。（3）统一安全管理平台是安全管理员的工作平台，负责系统管理、安全管理、审计管理，主要包括用户 USB-KEY 的发行、用户密钥的管理、终端主客体安全级别的设定、可执行程序策略的制定、终端网络互联策略的制定等。

4. “节点—操作系统安全加固”功能介绍

“节点—操作系统安全加固”产品是在现有操作系统基础上，强化了其身份鉴别、执行程序控制、数据完整性保护、数据保密性保护、移动介质控制、网络控制以及行为审计机制，增加了强制访问控制机制，为全面防内提供了基础。

产品功能如下表：

适用范围	功能要求	产品功能
安全功能	身份鉴别	基于 USB-Key 的双因子增强身份认证。
	自主访问控制	提供私有目录保护，保护敏感信息。
	标记与强制访问控制	主、客体的全程标记；基于 BLP 和 BIBA 相结合的二维标识模型的强制访问控制机制。强制访问控制主体类型为用户；客体类型包括文件、目录、移动介质；操作类型包括打开、读、写、改名、删除等。
	执行程序可信度量	通过执行程序的真实性和完整性度量保护系统完整性不被已知/未知病毒、木马、攻击程序等恶意代码破坏。
	数据完整性保护	对标记过的数据进行严格的控制，禁止任何的非法修改行为。
	数据保密性保护	重要文件透明加解密保护、移动介质加密保护。
	可信代码防篡改	可信代码的实时保护和可信校验，实现可信代码防篡改。
	程序安装控制	提供程序安装接口，控制程序安装行为。
	网络访问控制	非法内联控制，非法外联控制。
	移动介质权限管理	移动介质使用许可控制、使用权限控制。
	移动介质加密保护	移动介质存储信息加密保护。
安全管理	系统管理	用户身份、平台资源管理、应急处理。
	安全管理	标记管理、授权管理、策略管理。
	审计管理	审计信息包括主体、客体、操作、成功与否等。审计事件包括用户对文件的访问、对网络的访问、移动介质的使用等。

4.1 身份鉴别

现有的操作系统采用口令认证方式对用户身份进行鉴别，容易受到字典攻击。在“节点—操作系统安全加固”产品中，引入一个硬件 USB-KEY 令牌。该 USB-KEY 为用户身份的唯一标识，当用户登录系统时，需要插入 USB-KEY，然后系统对用户进行双因子身份认证，用户只有拥有合法的 USB-KEY，并且输入正确的操作系统口令+ USB-KEY 口令，才能登录终端系统。

登录成功后，如果用户需要临时外出，可以拔除 USB-KEY，这样安全内核会自动保存用户的工作环境，并且锁定终端桌面。除了持有授权 USB-KEY 的用户外，任何人都不能进入终端环境。由此，“节点—操作系统安全加固”产品实现了基于硬件 USB-KEY 的双因子身份认证，使得非授权用户无法进入终端环境。

4.2 执行程序可信度量

传统病毒查杀类产品采用病毒库黑名单的机制，仅能对病毒库中已知的病毒、木马进行查杀，一旦出现新型未知的恶意代码，这些传统病毒查杀类产品将无能为力，存在很大的安全隐患。因此在“节点—操作系统安全加固”产品中采用特有的白名单主动防御机制，通过对执行程序的可信度量，实现终端对于已知/未知病毒、木马、攻击程序等恶意代码的防御能力。

产品提供执行程序真实性和完整性度量功能。执行程序真实性度量可以确保系统中的执行程序都是合法的，从而阻止非授权程序的运行。执行程序完整性度量用来保证系统所启动的执行程序都是可信的，禁止不符合预期的程序的启动。执行程序启动前，“节点—操作系统安全加固”产品中的核心模块会度量该程序相关模块的真实性和完整性，只有在度量结果和预期值一致的前提下，该程序才允许启动，否则拒绝其执行。因此即使系统中的某一执行程序被病毒或木马感染，由于其不再可信，“节点—操作系统安全加固”产品将禁止其执行，从而阻止了恶意代码继续传播和破坏，降低了终端操作系统完整性被破坏的风险。正是由于上述安全机制，“节点—操作系统安全加固”产品实现了终端对于已知/未知病毒、木马、攻击程序等恶意代码自免疫。

4.3 可信代码防篡改

可信代码通常面临着病毒、木马的破坏以及恶意修改、恶意删除等威胁。因此“节点—操作系统安全加固”产品提供了对于可信代码的实时保护，禁止任何的破坏和非法修改行为，保护可信代码的完整性和可用性不被破坏。

4.4 程序安装控制

非法的程序安装行为将给病毒、木马等恶意代码入侵终端提供可乘之机，因此“节点—操作系统安全加固”产品提供了程序安装接口，仅允许通过此接口在终端上安装应用程序。通过这种方式将严格控制程序的安装行为，禁止未经授权非法在终端上安装应用程序。

4.5 自主访问控制

在现有操作系统中，如果用户以管理员身份登陆，则可以访问系统中的任何文件，用户很难保护自己的隐私。因此在安装“节点—操作系统安全加固”产品后，用户可以拥有自己的文件保密柜，即设置自己的私有目录。安全内核使用用户的私有密钥加密保密柜中的文件，并且禁止本用户以外的其它用户访问保密柜中的文件，从而有效地保护了用户的私有信息。

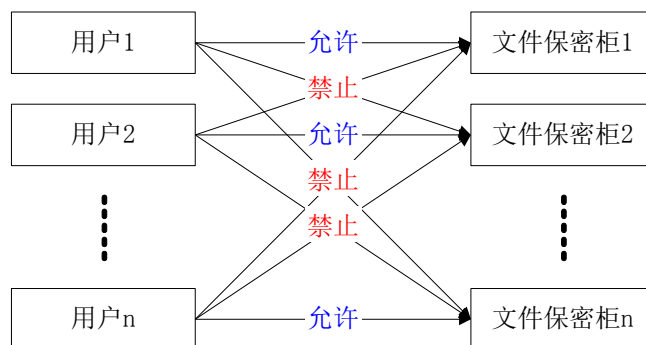


图 4.5: 文件保密柜示意图

4.6 强制访问控制

在自主访问控制的基础上，“节点—操作系统安全加固”产品增加了强制访问控制机制。通过对信息资源的强制访问控制、对移动介质的强制访问控制等机制实现对应用进行安全“隔离”。该机制由安全管理平台对系统中的主体（用户）及客体（文件、目录、移动介质）进行安全标识，根据客体类型的不同，分别制定不同的访问控制规则，从而严格控制用户行为。

“节点—操作系统安全加固”产品通过分级访问控制的方式对用户权限进行控制。安全管理员通过安全管理平台规定用户以及各终端上客体（文件、目录、移动介质）的安全级，强制终端采用 BLP 和 BIBA 模型相结合的规则限制用户的权限。

通过上述访问控制规则，安全管理员不仅可以规定用户的权限，而且可以依据系统中数据的重要性来制定其安全级，从而确保重要信息只掌握在安全规则允许访问该信息的人手里，以降低重要信息安全性被破坏的风险。

4.7 网络访问控制

“节点—操作系统安全加固”产品增强了操作系统的网络访问控制能力，通过对终端身份的认证和对网络出站的访问控制，达到对接入和外联的控制，实现对应用环境边界的保护，能够防止非法终端接入内部网络，限制终端用户访问网络的权限。

➤ 非法内联控制

在“节点—操作系统安全加固”产品中，安全管理员通过安全策略控制终端的网络通信行为。因此当终端尝试与受保护的终端进行通信时，安全内核检查该终端的身份和安全状态，只有检验通过后，该终端方能与受保护的终端进行通信。

➤ 非法外联控制

“节点—操作系统安全加固”产品可以在操作系统层对网络协议栈进行监控和过滤，禁止任何试图连接公共网络的操作，能够对用户访问 URL、IP 地址进行限制，同时能够限制执行程序访问网络的行为，确保用户无法连接到公共网上，从而在操作系统层实现了物理隔离。

4.8 数据完整性保护

“节点—操作系统安全加固”产品在不改变原有终端文件系统格式的基础上，通过全路径名对终端系统中的重要数据进行标记并制定安全策略。安全内核截获应用层的访问请求后，查询规则库中的安全策略以判断该请求是否允许被执行，实施严格的控制。默认禁止对终端中受保护的重要数据进行任何的非法修改操作，杜绝重要数据被非法篡改、删除、插入等情况的发生，从而全方位地确保重要数据的完整性不被破坏。

4.9 数据保密性保护

数据加密保护是防止信息泄露最有效的手段，“节点—操作系统安全加固”产品支持对重要数据透明加解密，达到了重要信息即使被盗取，信息盗取者也“看不懂”的效果。

所谓透明加解密是指该加解密过程对用户是透明的，这一过程在操作系统层实现，对上层应用透明，用户感觉不到它的存在。这一特性可以保证信息系统中的重要信息在存储和传播过程中都以密文的形式存在，即使意外断电，也不会导致明文信息的外泄。

在“节点—操作系统安全加固”产品中，安全管理员可以根据客体的不同安全级制定不同的数据保护策略，方便信息系统和外界进行数据交换。

4.10 移动介质权限控制

“节点—操作系统安全加固”产品对于移动介质进行严格的控制，所有移动介质在使用之前都需经过授权，未经授权的移动介质一律禁止其使用。对于已授权的移动介质进行标记管理，对其使用行为进行全程的严格控制，从而防止通过移动介质非法拷贝敏感信息等恶意事件的发生。



4.11 移动介质加密保护

“节点一操作系统安全加固”产品可对存放敏感数据的移动介质进行加密保护，只有合法的访问过程才具有解密的权利，从而防止通过移动介质泄露敏感信息事件的发生。加密保护采用透明加解密机制，加解密过程在合法的访问过程中自动执行，既保证了信息的机密性，又不影响正常操作。

4.12 终端统一管理

“节点一操作系统安全加固”产品部署后将建立终端系统统一安全管理平台，对系统中的所有终端进行统一管理、统一配置，审计信息统一存储、统一分析，构建终端系统的整体安全防线，有效保护终端的安全。

4.13 行为监控审计

监督系统中与安全相关的行为，尤其是管理员对安全策略的制定、修改以及授权用户违反安全策略的行为，达到非法行为“赖不掉”的效果。具体包括用户对重要信息的操作行为、对移动介质的使用行为、不可信应用的启动行为、应用的越权访问行为、管理员对策略的制定和修改行为、操作员对系统的维护行为等。

4.14 管理员职责分离

为了方便权限管理，“节点一操作系统安全加固”产品引入三个管理员角色：系统管理员、安全管理员和安全审计员。根据最小权限原则，系统赋予每个管理员完成任务所需最小权限。系统管理员具有对终端进行日常维护的权限，其行为由系统审计机制监控。安全管理员具有完成安全管理任务权限，即配置终端系统安全策略等，并且安全管理员的一切操作行为都被记入审计日志。安全审计员负责审计日志的存取控制，不具有安全管理员和系统管理员的权限。

“节点一操作系统安全加固”产品正是通过上述“三权分立”的机制，使得终端系统中的不同管理员之间相互制约，每个角色各司其职，共同保障终端系统的安全。

5. “节点—操作系统安全加固”技术特点

1) 基于操作系统内核层的安全加固

对终端的安全加固工作建立于操作系统文件过滤驱动层，由于文件过滤驱动工作在系统的核心层，因此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。当操作系统中的磁盘驱动启动后安全防护模块驱动马上启动并对终端系统实施保护，从而杜绝了旁路和隐通道，增强了安全性。系统中用户行为控制、重要资源保护、执行程序控制等安全手段都是从操作系统内核着手。安全模块随操作系统一起加载，安全布控时机早，可有效防止安全机制被旁路的可能。如下图所示：

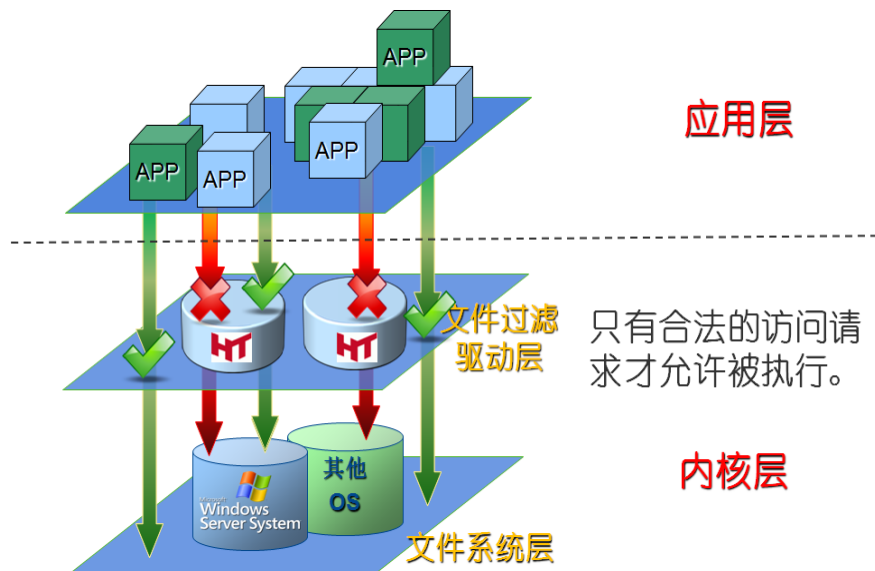


图 5.1：先进的内核加固技术

2) 结合可信计算技术实现对执行程序的可信度量

结合可信计算技术，在操作系统、应用等程序代码运行控制转移过程中，对下一级可执行代码的真实性和完整性加以验证，通过可信链传递模式建立起一个安全可信的系统运行环境。系统通过执行程序的真实度量来判断执行程序是否是合法的；通过执行程序的完整性度量来判断授权程序是否是可信的，禁止不符合预期的程序的启动。即使系统中的某一执行程序被病毒感染，由于其不再可信，“节点—操作系统安全加固”产品将禁止其执行，从而阻止了恶意代码继续传播和破坏，降低了系统完整性被破坏的风险。

3) 以强制访问控制为核心严格控制用户行为

在原有系统自主访问控制基础上，研发基于 BLP 模型与 BIBA 模型相结合的强制访问控制模型，通过对重要主体（用户）及客体（文件、目录、移动介质）的安全标记，控制主体对于客体的访问权限，实施强制访问控制，严格控制用户行为。保证用户的任何行为都在安全策略的支撑下，使得用户登录系统后，其权限受到安全策略的严格限制，不能为所欲为。

4) 基于硬件的系统层加解密机制

通过 USB-KEY 进行加解密，既具备了类似 TPM 功能模块加解密的优势：加密速度快、占用计算机资源少、安全性高等，又无需对现有计算机体系结构进行改造。

在操作系统层实现的加密技术，文档从产生的第一时刻就是自动加密的，避免用户在编写过程中有意或无意地留下明文，且信息被黑客等非法窃取后，由于其没有相应的权限，获取者仅仅只能得到密文，从而确保了数据的保密性不被破坏。

6. “节点—操作系统安全加固”产品优势

1) 先进的设计理念

以可信计算为基础，访问控制为核心，构建终端整体安全防御体系，实现“防失窃密”、“防系统破坏”、“确保系统可用”的安全目标。

产品结合可信计算技术，以可信密码模块为基础，通过可信计算模块提供的服务，来构建可信计算的密码支撑平台，变被动防御为主动防御，通过身份认证、可信度量、数据加密等技术，最终在整个平台中形成了可以有效防御恶意攻击的安全体系。以访问控制为核心，在系统原有自主访问控制的基础上，通过对重要的主体、客体进行安全标记，制定访问控制策略，实施强制访问控制，严格控制用户行为。

综上所述，“节点—操作系统安全加固”产品将安全操作系统的职能从保障单个操作系统安全，转变为支撑整个应用系统的安全，更重要的是保障应用系统中数据的应用、存储安全。在确保应用系统平稳运行的基础上，保证应用系统中的数据安全，确保数据在应用过程中，既不会被非法窃取，又不会遭到病毒、木马等恶意代码的非法篡改。

2) 对终端统一管控，构建整体安全防线

构造终端统一管控的管理体系。信息安全具有“短板效应”，任何一个终端的安全漏洞都可能对整个系统的安全造成威胁。“节点—操作系统安全加固”产品构建全系统统一的“统一安全管理平台”，对系统中的所有操作系统终端进行统一管理、统一配置，审计信息统一存储、统一分析，消除了各个终端由于配置不同造成的安全隐患，最终构建一道针对整个信息系统的整体安全防线，有效保护系统中的信息安全。

3) 三权分立的管理体系

产品在部署后将建立统一安全管理平台，对系统中的终端进行统一管理。统一安全管理平台采用三权分立的管理模式，将管理员分为：系统管理员、安全管理员、安全审计员。产品对三个管理员的权限进行严格的分配和管理，授予其各自完成自己承担任务所需的最小权限，三个管理员之间相互制约，从而防止“超级用户”的形成。通过三权分立的管理体系，为系统设置“保卫部”、“保密室”和“监控中心”，实现对整个系统的统一管理。

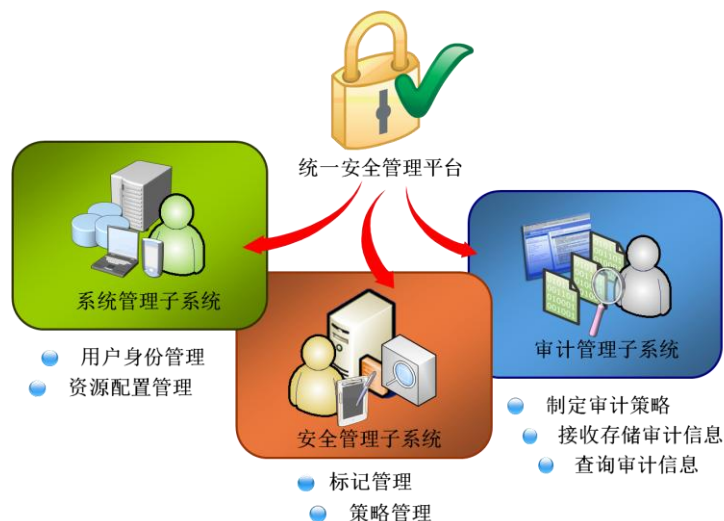


图 6：三权分立的管理模式

4) 恶意代码自免疫

通过可信度量技术，“节点—操作系统安全加固”产品赋予了终端对恶意代码的主动防御的能力，使得终端做到了对已知/未知病毒、木马、攻击程序等恶意代码的自免疫，从而有效替代或配合传统的病毒查杀类产品。

5) 完善的安全防护体系

“节点—操作系统安全加固”产品不是只针对安全功能中的某一点或几点进行保护，而是为系统构筑整体的安全防护体系。系统中的各种安全机制相互联系、相互制约，构筑了一个整体的安全保护环境，实现终端对于非法用户“进不来”、“拿不走”、“看不懂”、“改不了”、“赖不掉”的安全目标，因此从整体上保证了终端系统的安全。

6) 应用安全隔离及透明应用支撑

“节点—操作系统安全加固”产品通过对执行程序的强制访问控制、对用户行为的强制访问控制、对网络访问的强制访问控制、对重要数据的强制访问控制，达到对应用进行“安全隔离”的效果。

产品兼容现有系统的全部应用：现有操作系统的应用多种多样，“节点—操作系统安全加固”产品在对大量应用的细致分析的基础上，得到应用系统运行的一般规律，通过与应用无关的透明支撑设计，使得产品能兼容现有系统的全部应用，且不影响原有应用系统的效率。

不改变现有应用：“节点—操作系统安全加固”产品部署后，无需改变现有应用的应用模式、网络部署等，通过透明支撑，既使得用户在原有应用中感觉不到安全操作系统的存在，又实现了对应用的安全保护。

7) 优化的加解密机制

“节点-操作系统安全加固”产品采用基于硬件的透明加解密，占用系统资源少，安全性高，加解密动作对用户及应用透明。

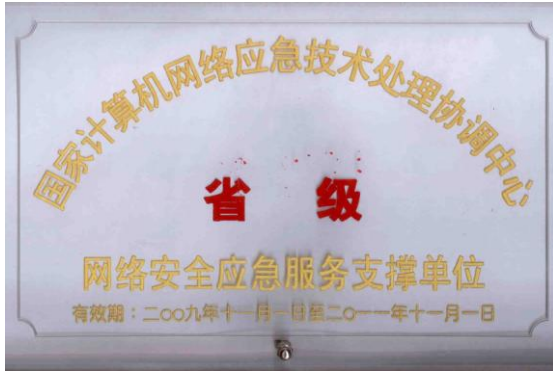
8) 足够的安全强度

“节点-操作系统安全加固”产品采用内核级的安全机制，系统的访问控制等安全机制均在操作系统核心层实现，采用文件过滤驱动技术，安全布控时机早，降低安全机制被旁路的危险，有效防止安全模块被恶意篡改或卸载。

附录 1：产品资质



附录 2：公司资质



版权声明

本手册的所有内容，其版权属于北京中软华泰信息技术有限责任公司（以下简称中软华泰）所有，未经中软华泰许可，任何人不得仿制、拷贝、转译或任意引用。本手册没有任何形式的担保、立场倾向或其他暗示。

本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，中软华泰恕不承担另行通知之义务。

版权所有 不得翻印© 2000-2010 中软华泰公司

公司联系方式:

用户可以通过如下的联系方式详细了解该产品:

北京中软华泰信息技术有限责任公司

- 地 址: 北京市海淀区远大路1号金源时代商务中心B区写字楼705-706室
- 邮 编: 100097
- 网 址: <http://www.huatechsec.com.cn>
- 电 话: 010-62191614、62198781、62144177、62133838
- 传 真: 010-62133939

北京中软华泰信息技术有限责任公司上海分公司

- 地 址: 上海市静安区延平路三和大厦15B1
- 邮 编: 200042
- 电 话: 021-62462228、62462229

北京中软华泰信息技术有限责任公司南京分公司

- 地 址: 南京市玄武区成贤街50号成贤大厦308室
- 邮 编: 210018
- 电 话: 025-83699268

北京中软华泰信息技术有限责任公司西安分公司

- 地 址: 陕西省西安市高新区高新一路25号创新大厦F7室
- 邮 编: 710075
- 电 话: 029-88839373

深圳中软华泰信息技术有限公司

- 地 址：深圳市福田区八卦一路鹏基商务时空大厦 2408-2409A
- 邮 编：518029
- 网 址：www.szhuatechsec.cn
- 电 话：0755-22200019、0755-22200026

北京中软华泰信息技术有限责任公司天津分公司

- 地 址：天津市华苑产业园区华天道海泰信息广场 D 座 601 室
- 邮 编：300384
- 电 话：022-83716303, 83711786, 83718234

北京中软华泰信息技术有限责任公司武汉办事处

- 地 址：武汉市洪山区雄楚大道 229 号春林庭苑 C-1702
- 邮 编：430070
- 电 话：027-87397339

北京中软华泰信息技术有限责任公司东北办事处

- 地 址：吉林省长春市亚泰大街繁荣路东南阳光小区 5 号楼 3 门 406
- 邮 编：130000
- 电 话：0431-85332050

北京中软华泰信息技术有限责任公司贵州办事处

- 地 址：贵阳市延安中路 1 号振华科技大厦 24 层 A-B 座
- 邮 编：550001
- 电 话：0851-6907223