

目 录

| | |
|----------------------------------|--------|
| 1. 公司简介 | - 1 - |
| 2. 引言 | - 2 - |
| 3. 服务器安全风险分析 | - 3 - |
| 3.1 存在较多安全漏洞 | - 3 - |
| 3.2 操作系统完整性破坏 | - 3 - |
| 3.3 重要数据失窃密 | - 4 - |
| 3.4 数据完整性破坏 | - 4 - |
| 3.5 缺乏内部攻击的防范措施 | - 4 - |
| 3.6 缺乏统一安全管理 | - 5 - |
| 3.6.1 缺乏统一的身份管理 | - 5 - |
| 3.6.2 缺乏统一的服务器管理 | - 5 - |
| 4. 节点-操作系统安全加固（服务器版）概述 | - 6 - |
| 4.1 节点-操作系统安全加固（服务器版）设计理念 | - 7 - |
| 4.2 节点-操作系统安全加固（服务器版）组成 | - 8 - |
| 5. 节点-操作系统安全加固（服务器版）功能介绍 | - 9 - |
| 5.1 服务器运行安全 | - 9 - |
| 5.1.1 身份鉴别 | - 9 - |
| 5.1.2 执行程序控制 | - 9 - |
| 5.1.3 进程强制访问控制 | - 10 - |
| 5.1.4 服务强制访问控制 | - 10 - |
| 5.1.5 注册表强制访问控制 | - 10 - |
| 5.1.6 网络访问控制 | - 10 - |
| 5.1.7 服务器性能监测 | - 11 - |
| 5.2 服务器数据安全 | - 12 - |
| 5.2.1 自主访问控制 | - 12 - |
| 5.2.2 强制访问控制 | - 12 - |
| 5.2.3 数据完整性保护 | - 12 - |
| 5.2.4 数据保密性保护 | - 13 - |
| 5.3 服务器安全管理 | - 13 - |
| 5.3.1 服务器统一管理 | - 13 - |
| 5.3.2 用户权限控制 | - 13 - |
| 5.3.3 管理员职责分离 | - 13 - |
| 5.3.4 行为监控审计 | - 14 - |
| 6. 节点-操作系统安全加固（服务器版）技术特点 | - 15 - |
| 7. 节点-操作系统安全加固（服务器版）产品优势 | - 17 - |
| 8. 节点-操作系统安全加固（服务器版）产品性能测试 | - 20 - |
| 8.1 测试环境 | - 20 - |
| 8.2 系统比对测试 | - 20 - |

| | | |
|------------------------|----------------|---------------|
| 8.2.1 | 测试执行..... | - 20 - |
| 8.2.2 | 测试值 | - 20 - |
| 8.2.3 | 测试结果..... | - 21 - |
| 8.3 | 操作系统稳定性测试..... | - 21 - |
| 8.3.1 | 测试执行..... | - 21 - |
| 8.3.2 | 测试值 | - 22 - |
| 8.3.3 | 测试结果..... | - 22 - |
| 8.4 | 数据库稳定性测试..... | - 22 - |
| 8.4.1 | 测试执行..... | - 22 - |
| 8.4.2 | 测试值 | - 22 - |
| 8.4.3 | 测试结果..... | - 22 - |
| 8.5 | 中间件稳定性测试..... | - 22 - |
| 8.5.1 | 测试执行..... | - 22 - |
| 8.5.2 | 测试值 | - 23 - |
| 8.5.3 | 测试结果..... | - 23 - |
| 附录 1：产品资质 | | - 24 - |
| 附录 2：公司资质 | | - 24 - |
| 版权声明： | | - 25 - |

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，继续深化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关键技术研究能力、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

随着计算机网络技术的迅速发展和进步，信息和计算机网络系统现在已经成为社会发展的重要保证。信息与网络涉及到国家的政治、军事、文化等诸多领域，在计算机网络中存储、传输和处理的信息包括各种政府宏观调控决策、商业经济信息、银行资金转帐、股票证券、能源资源数据、高科技科研数据等重要信息，其中有很多是国家敏感信息和国家机密，所以难免会吸引来自世界各地的各种网络黑客的人为攻击（例如，信息窃取、信息泄漏、数据删除和篡改、计算机病毒等）。因此计算机网络系统的安全是关系到国家安全和主权、社会的稳定、民族文化的继承和发扬的重要问题。

由于服务器是信息应用的核心，无论是在 C/S 计算模式还是 B/S 计算模式中，它们都是绝大多数用户应用服务的运行中心和数据处理中心，因此，针对服务器的攻击事件层出不穷，攻击手段多种多样，从缓冲区溢出攻击、系统管理员口令攻击到恶意代码攻击，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。今天的商用操作系统，在注重功能性的同时，却严重忽略了安全性保证，比如管理员权限的过于集中、访问控制机制薄弱、身份鉴别机制的易破解性等等。

因此，在由信息和计算机网络系统构成的信息系统中，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。服务器是信息系统中敏感信息的直接载体，也是各类应用运行的平台，因此对服务器的保护是保证整个信息系统安全的基础，而对服务器操作系统安全保障又是保证服务器安全的核心所在。

3.服务器安全风险分析

3.1存在较多安全漏洞

操作系统存在较多安全漏洞，每一年报告给 CERT/CC 的漏洞数量也在成倍增长，如仅在 2009 年一年，微软公司就发布了 72 个补丁修复了近 190 个安全漏洞。而其中很多漏洞会被黑客利用，成为黑客攻击的目标或跳板。对于服务器管理员来说想要跟上补丁的步伐是很困难的。另外，每年都会发现新类型的漏洞。对于新类型漏洞的代码实例分析常常导致数以百计的其他不同软件漏洞的发现。而且，入侵者往往能够在软件厂商更正这些漏洞之前首先发现这些漏洞。

面对操作系统安全漏洞，用户所能做的往往是以“打补丁”的方式为操作系统不断的升级更新。这种方式最大的缺陷是系统补丁的滞后性：（1）从补丁测试到分发，需要较长周期。在此期间，操作系统安全仍然无法得到保障；（2）补丁永远是在漏洞之后，且补丁永远“打不完”；（3）随着发现漏洞的工具的自动化趋势，留给服务器管理员打补丁的时间越来越短。

因此这种事后补救的方式存在着较大的安全隐患，往往在补丁没有发布之前，黑客就已经利用这些漏洞对服务器造成极大的破坏了。

除操作系统外，服务器上的第三方软件也会存在或多或少的漏洞，这些漏洞中有不少可被利用，严重威胁服务器安全。

3.2操作系统完整性破坏

服务器操作系统完整性破坏是当前服务器面临的主要安全威胁。现有服务器操作系统，从开机启动到运行服务过程中，对执行代码不做任何完整性检查，导致病毒、木马程序可以嵌入到执行代码程序或者直接替换原有程序，实现病毒、木马等恶意代码的传播。这些恶意代码一旦被激活，就会继承当前用户的权限，从而肆无忌惮地进行传播，为所欲为地破坏服务器操作系统的完整性，例如在服务器管理员毫不知情的情况下修改或删除服务器中的重要信息，或者破坏服务器操作系统中的一些重要服务，导致服务器操作系统无法正常运作等。

虽然用户在服务器上部署了病毒查杀类产品，但是目前的病毒查杀类产品都是采用病毒库的方式，因此只能防范已知的病毒、木马、攻击程序等恶意代码的攻击，对于未知的病毒、木马、攻击程序等恶意代码是无能为力的，这种被动防御的方式带来的安全滞后性问题将严重威胁服务器的安全。

另外执行程序运行过程中不满足最小权限原则，使得非法操作者和恶意代码能够拥有至高无上的权限，从而给破坏服务器操作系统完整性的行为预留了空间。显然，为了保障服务器的安全，必须防范各种已知及未知破坏系统完整性的攻击，从根本上保证系统的完整可信。

3.3重要数据失窃密

服务器中往往存放着大量的重要数据，而随着信息化的高度发展，重要数据越来越容易被复制和传播，从而导致重要数据的失窃密事件频繁发生，严重损害相应组织机构的形象和利益，甚至威胁到了社会秩序、公共利益和国家安全。例如，首先服务器是对外提供服务的，使其更有可能遭受攻击，即使服务器和互联网隔离，其服务器操作系统仍然可能被病毒、木马入侵或恶意攻击，那么其中的重要数据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服务器安全防护措施，利用现有服务器防护技术的漏洞，通过网络内攻击，恶意植入木马等手段主动窃密。

3.4数据完整性破坏

数据完整性面临的威胁主要指服务器中的重要数据在存储期间被恶意篡改，使得重要数据失去了原有的真实性，从而变得不可用或造成广泛的负面影响，恶意用户可以通过网络或其他方式对没有采取安全措施的服务器的服务器上存放的重要数据进行修改或传达一些虚假信息，从而影响工作的正常进行。

3.5缺乏内部攻击的防范措施

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。由于内部人员可直接接触服务器中的重要数据，并且了解服务器的安全防御措施和管理手段，因此相对于外部用户而言，其更容易规避防护措施，利用服务器系统安全防御措施的漏洞或管理体系不完善的弱点，从内部发起攻击来破坏服务器系统的安全，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服务器系统安全的基本任务。

传统的安全防护措施大多只对来自外部的攻击进行防范，但俗话说家贼难防，所以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，从源头进行治理。

3.6 缺乏统一安全管理

3.6.1 缺乏统一的身份管理

目前服务器普遍存在的问题就是管理员身份单一，致使管理员权限过大，这样会对服务器带来一定的安全隐患。并且出于服务器业务操作和运行维护的需要，服务器经常是混用的，即多人可对同一台服务器进行操作。而服务器操作系统本身只提供用户名/口令认证方式，因此多人不得不共用服务器账户和口令，这样就造成服务器用户身份鉴别不明，难以根据用户的身份和角色分配权限，无法进行严格地访问控制，容易产生误操作；也不能根据用户身份进行行为审计，无法实现事后追查。另外，单纯的用户名/口令认证方式容易受到字典攻击等方式攻击，导致黑客获取口令执行恶意操作。

3.6.2 缺乏统一的服务器管理

目前大多数服务器仍采用单机管理模式，即服务器管理员对每一台服务器单独进行管理维护，这样的管理模式会存在一定的安全滞后性。服务器要实现真正有效的安全管理，必须能实现对所有服务器的统一集中管理、统一安全策略下发，以及安全事件的统一监控和协同处理，才有可能构建健康的服务器安全管理体系。

4. 节点-操作系统安全加固（服务器版）概述

目前，市面上的服务器安全产品大部分以防外部攻击为主，如防火墙、防病毒软件、入侵检测设备。由于计算机病毒、木马、蠕虫等恶意代码层出不穷，加之外围攻击手法不断升级，致使这些防护系统捉襟见肘、漏洞百出，服务器安全屡屡受到威胁和破坏。即使亡羊补牢，将系统防火墙越做越高、入侵检测越做越复杂、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。其次，由于服务器操作系统自身存在安全漏洞，针对这些安全漏洞的攻击很容易绕过信息安全防线而直接对核心系统和信息发起攻击。第三，根据近年来信息安全事件方面的统计，越来越多的攻击行为是从组织内部发起的，由于内部人员具有合法的权限，同时，对信息安全的保护措施了如指掌，因此，从组织内部发起的攻击对服务器安全造成的破坏程度更为严重。具体来说，是对服务器系统的机密性、完整性和可用性的破坏，重要数据的失窃密等。

并且由于目前服务器操作系统多采用商用操作系统，而现有商用操作系统侧重于系统的易用性。用户登录服务器后可以运行任意程序，查看、修改系统中的任意数据信息，因此在对服务器的机密性、完整性保护方面存在很多不足，无法满足我国对于服务器系统的安全需求。

综上所述，安全服务器操作系统才是保护服务器安全的核心和基础。一旦未经授权的非法用户通过各种手段突破了防火墙等网络安全产品进入到内部服务器，那么安全服务器操作系统将成为最后也是最坚固的一道防线。如果没有安全服务器操作系统的支撑，服务器安全就是无法保障的。黑客可以利用服务器操作系统的漏洞窃取超级用户权限，肆意进行破坏；病毒程序可以利用服务器操作系统对执行程序不检查真实性和完整性的弱点，将病毒代码嵌入到执行代码程序，实现病毒传播、破坏；更为严重的是如果没有安全服务器操作系统，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。还有如果没有安全服务器操作系统的支持，服务器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，自然无法防止内部用户攻击。

因此，通过安全服务器操作系统所提供的安全机制，赋予服务器操作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服务器，从而保证能够访问服务器的用户是可控的；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，确保服务器中的重要数据无法被非法泄露或窃取；通过数据加密保护机制，确保非授权用户无法获取服务器中的的重要数据；通过执行程序真实性和完整性度量，确保服务器操作系统无法被病毒、木

马、攻击程序等恶意代码破坏；通过用户行为审计机制，可以防违规行为的抵赖，做到事后有证可查。因此，安全服务器操作系统在对服务器进行安全保护中起着不可替代的作用。

中软华泰在对攻击手段及传统安全产品详尽分析的基础上，经过多年研发，推出了“节点”系列的服务器加固产品：“节点-操作系统安全加固（服务器版）”。该产品以安全管理平台策略控制为核心，以服务器操作系统安全为基础，通过对现有服务器操作系统进行安全增强，使得管理员能够对服务器进行集中管理和控制，保证服务器始终在可控状态下运行，从根源上有效抑制对服务器安全的威胁，最终达到防止内部用户以及外部用户攻击的目的。

4.1 节点-操作系统安全加固（服务器版）设计理念

服务器是信息系统的主要组成部分，是为网络环境中的客户端计算机提供特定的应用服务的计算机系统，其运行状态将直接影响到应用系统的稳定性。此外，由于攻击和威胁既可能是针对服务器运行的，也可能是针对服务器中所存储、处理和发布的数据信息的保密性、完整性，因此还应对在服务器中存储、处理和发布的数据信息进行安全保护，使其免遭由于人为原因所带来的泄露、破坏和不可用的情况发生；另外服务器安全管理的不完善同样会给服务器的安全带来威胁，所以对服务器的安全保护的功能要求，需要从服务器运行安全、服务器数据安全和服务器安全管理三方面综合进行考虑。

因此，节点-操作系统安全加固（服务器版）产品提出了产品的设计理念，即：从服务器“运行安全”、“数据安全”、“安全管理”三个方面出发，打造服务器全生命周期的安全防护。产品是在现有服务器操作系统基础上，强化了服务器的身份鉴别、执行程序控制、数据完整性保护、数据保密性保护、服务器操作系统完整性保护、服务器性能监控以及行为审计机制，增加了强制访问控制机制，为服务器提供全面的保护。产品整体架构图如下：

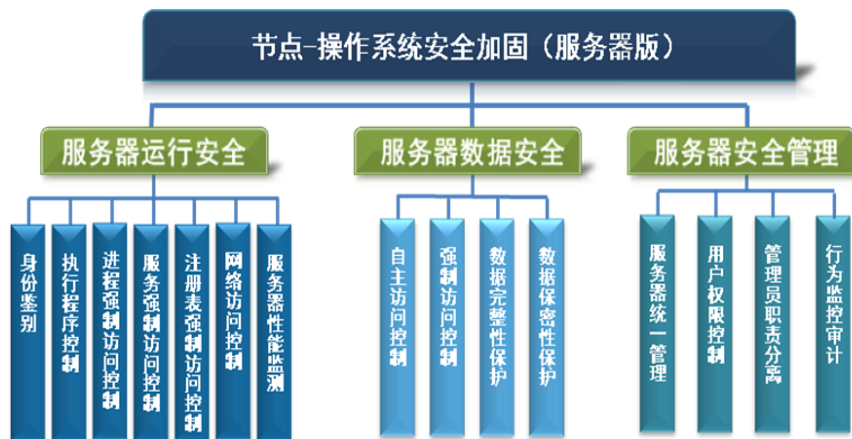


图 4.1：节点-操作系统安全加固（服务器版）产品功能架构图



4.2节点-操作系统安全加固（服务器版）组成

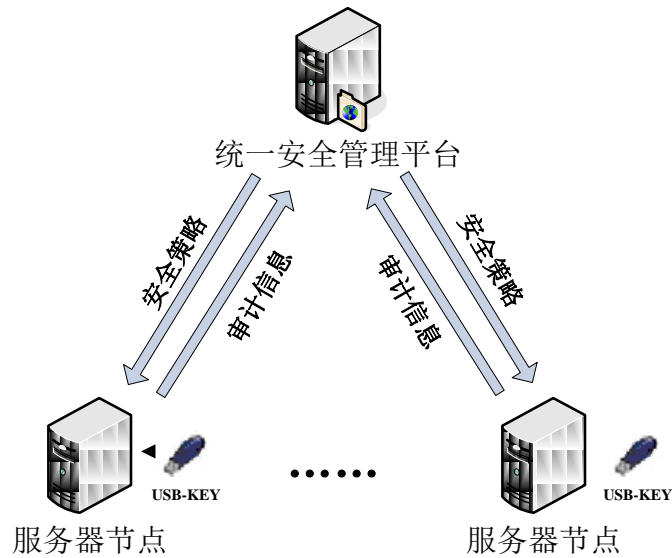


图 4.2: 节点-操作系统安全加固（服务器版）系统组成

节点-操作系统安全加固（服务器版）产品是软硬件相结合的产品，通过硬件 USB-KEY，提高了服务器系统的安全性，克服单纯使用软件防护的局限性；软件部分包括服务器操作系统安全增强软件、服务器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，是加解密运算的介质。

软件部分：（1）服务器操作系统安全增强软件，统一实施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、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）服务器安全代理，主要负责服务器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、服务器主客体安全级别的设定、执行程序策略的制定、服务器网络互联策略的制定等。

5.节点-操作系统安全加固（服务器版）功能介绍

5.1服务器运行安全

5.1.1 身份鉴别

现有的服务器操作系统仍采用单一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（服务器版）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，当用户登录服务器系统时，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，并且输入正确的服务器操作系统口令+ USB-KEY 口令，才能登录服务器。

通过双因子的身份鉴别，将用户身份与 USB-KEY 绑定，可有效防止用户身份伪造事件的发生；对于一个已标识和鉴别的用户，将该用户的身份与该用户的所有可审计行为相关联，以实现用户行为的可查性。

5.1.2 执行程序控制

5.1.2.1 执行程序可信度量

节点-操作系统安全加固（服务器版）产品采用白名单机制，实现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启动。执行程序启动前，节点-操作系统安全加固（服务器版）产品中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（服务器版）产品将禁止其执行，从而阻止了恶意代码继续传播和破坏，降低了服务器操作系统完整性被破坏的风险。通过上述安全机制，节点-操作系统安全加固（服务器版）产品实现了服务器对于已知/未知病毒、木马、攻击程序等恶意代码自免疫。

5.1.2.2 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（服务器版）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。

5.1.2.3 程序安装控制

非法的程序安装行为将有可能给恶意代码入侵服务器提供机会，因此节点-操作系统安全加固（服务器版）产品提供了程序安装接口，仅允许通过此接口在服务器上安装应用程序。通过这种方式将严格控制程序安装行为，禁止未经授权非法在服务器上安装应用程序。

而且通过上述规则，限制了普通用户安装新的应用程序的能力，从而可以有效防止内部精通业务、懂技术、会编程的专业人士对服务器系统安全的威胁。

5.1.3 进程强制访问控制

节点-操作系统安全加固（服务器版）产品提供了进程保护机制，支持自定义进程列表，列表中的进程将自动加以保护，禁止未经授权终止这些受保护的进程。

其次产品提供了严格的进程访问控制，对于进程对重要文件/目录的操作行为进行严格的控制。

5.1.4 服务强制访问控制

节点-操作系统安全加固（服务器版）产品可对应用服务进行严格的控制，禁止非授权服务的启动，实现对于服务的强制访问控制。

5.1.5 注册表强制访问控制

节点-操作系统安全加固（服务器版）产品提供了对于服务器系统的重要注册表项的“只读”保护，系统默认仅允许服务器管理员拥有修改受保护的注册表项的权限，其他任何非授权用户对于受保护的注册表项进行写操作都将无条件拒绝。

节点-操作系统安全加固（服务器版）产品中的注册表访问过滤驱动程序会截获所有对受保护注册表项的读写请求，当截获到注册表项读写请求时检测规则库，并根据规则进行过滤，非授权用户发起的请求将直接丢弃。

5.1.6 网络访问控制

节点-操作系统安全加固（服务器版）产品增强了服务器操作系统的网络访问控制能力，通过对访问服务器的平台身份进行鉴别，防止非授权平台接入服务器。通过可信互联机制，实现对接入的有

效控制。

服务器管理员规定哪些平台可以接入服务器系统。因此在平台尝试接入服务器系统时，安全内核会检查该平台的身份，只有检验通过后，该平台方能与服务器进行网络通信。

同时对于本地服务所提供的远程访问，实行连接限制，订制可信访问列表，对于可信地址则允许其接入服务，非法地址将进行限制连接。

5.1.7 服务器性能监测

节点-操作系统安全加固（服务器版）产品提供了对服务器硬件运行状态信息的远程监测功能，通过统一安全管理平台可以对服务器硬件运行状态信息进行集中的采集和监测。通过监测功能，服务器管理员可以直观的了解服务器的运维情况。具体监测功能如下：

5.1.7.1 服务器 CPU 监测

节点-操作系统安全加固（服务器版）产品提供了服务器 CPU 监测功能，对于服务器 CPU 使用率进行实时的监测。一旦服务器 CPU 剩余率达到警戒值，节点-操作系统安全加固（服务器版）产品会及时向服务器管理员报警。

5.1.7.2 服务器内存监测

节点-操作系统安全加固（服务器版）产品提供了服务器内存监测功能，对于服务器内存使用率进行实时的监控。一旦服务器内存剩余率达到警戒值，节点-操作系统安全加固（服务器版）产品会及时向服务器管理员报警。

5.1.7.3 服务器硬盘监测

节点-操作系统安全加固（服务器版）产品提供了服务器硬盘监测功能，对于服务器硬盘使用率进行实时的监测。一旦服务器硬盘剩余率达到警戒值，节点-操作系统安全加固（服务器版）产品会及时向服务器管理员报警。

5.1.7.4 服务器进程占用资源监测

节点-操作系统安全加固（服务器版）产品提供了进程占用资源监测功能，对于进程占用系统资源进行实时的监测，一旦监测到进程占用过多的系统资源，节点-操作系统安全加固（服务器版）产品会及时向服务器管理员报警。



5.1.7.5 服务器端口监测

节点-操作系统安全加固（服务器版）产品提供了服务器端口监测功能，对于服务器已开放的端口及哪些进程开放的这些端口都有详细的审计记录。

5.1.7.6 交换分区监测

节点-操作系统安全加固（服务器版）产品提供了对于操作系统用来缓冲内存的换分区进行实时监测，当交换分区使用率过大时，及时向管理员提出申请，进行系统资源的整理，防止影响正常应用的使用。

5.1.7.7 网络流量监测

节点-操作系统安全加固（服务器版）提供对网络进出流量的统计。

5.2 服务器数据安全

5.2.1 自主访问控制

现有的服务器经常是混用的，如果用户以管理员身份登陆，则可以访问服务器系统中的任何文件，从而造成敏感数据的泄露。但是安装了节点-操作系统安全加固（服务器版）产品后，可以对服务器上的重要数据设置相应的权限，禁止非授权用户访问这些敏感数据。通过自主访问控制模式来限制用户权限，以达到保护服务器资源安全的目的。

5.2.2 强制访问控制

节点-操作系统安全加固（服务器版）产品提供了强制访问控制机制，通过对执行程序的强制访问控制、对信息资源的强制访问控制等机制实现对应用进行安全“隔离”。该机制由统一安全管理平台对服务器系统中的主体（用户）及客体（文件、目录、执行程序等）进行安全标识，根据客体类型的不同，分别制定了不同的访问控制规则，保证用户的任何行为都在安全策略的支撑下，严格控制“谁”可以“做什么”。

5.2.3 数据完整性保护

对于服务器中存放的重要数据的完整性进行保护也是保障服务器安全的核心问题。节点-操作系统安全加固（服务器版）产品在不改变原有服务器文件系统格式的基础上，通过全路径名对服务器系

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。默认禁止对服务器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，从而全方位地确保服务器重要数据的完整性不被破坏。

5.2.4 数据保密性保护

数据存储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（服务器版）产品支持对服务器重要数据透明加解密，从而达到了服务器重要数据即使被盗取，数据盗取者也“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。这一特性可以保证服务器系统中的重要数据在存储中都以密文的形式存在。

5.3 服务器安全管理

5.3.1 服务器统一管理

节点-操作系统安全加固（服务器版）产品提供了统一安全管理平台，作为所有服务器的统一安管中心，对系统中的所有服务器进行统一管理、统一配置，审计信息统一存储、统一分析，构建服务器系统的整体安全防线，有效保护服务器系统的安全。

5.3.2 用户权限控制

节点-操作系统安全加固（服务器版）产品提供了用户权限控制，用户的任何行为都要受到统一安全管理平台的策略控制，从而有效解决内部有权限的人员有意无意发起的攻击。其次，未经授权的用户不能改变其他用户的状态。包括用户名、密码等相关资源都受到系统的保护。

5.3.3 管理员职责分离

为了方便权限管理，节点-操作系统安全加固（服务器版）产品引入以下三个管理员角色，即：系统管理员、安全管理员和安全审计员。根据最小权限原则，系统只赋予每个管理员完成任务所需的最小权限。

系统管理员具有对服务器进行日常维护的权限，其行为由系统审计机制监控。安全管理员只有完成安全管理任务的权限，即配置服务器系统安全策略等，并且安全管理员的一切操作行为都被记入审计日志。安全审计员只负责审计日志的存取控制，不具有安全管理员和系统操作员的权限。

节点-操作系统安全加固（服务器版）产品通过“三权分立”的机制，使得服务器系统中的不同管理员之间相互制约，每个角色各司其职，共同保障服务器系统的安全。

5.3.4 行为监控审计

从“三权分立”的角度来看，安全审计员主要起监督作用，监督服务器系统中与安全相关的行为，尤其是安全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。具体包括用户对服务器重要数据的操作行为、不可信程序的启动行为、用户的越权访问行为、安全管理员对策略的制定和修改行为、安全操作员对系统的维护行为等。另外只有安全审计员可以修改或者删除审计日志，于是只要恶意用户试图去破坏服务器系统的安全性，其行为就必然会被审计记录，为日后追查留下证据。

6.节点-操作系统安全加固（服务器版）技术特点

1) 采用内核性能优化和安全加固技术

服务器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。当操作系统中的主要物理设备驱动启动后安全防护模块驱动马上启动并对服务器系统实施保护，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：

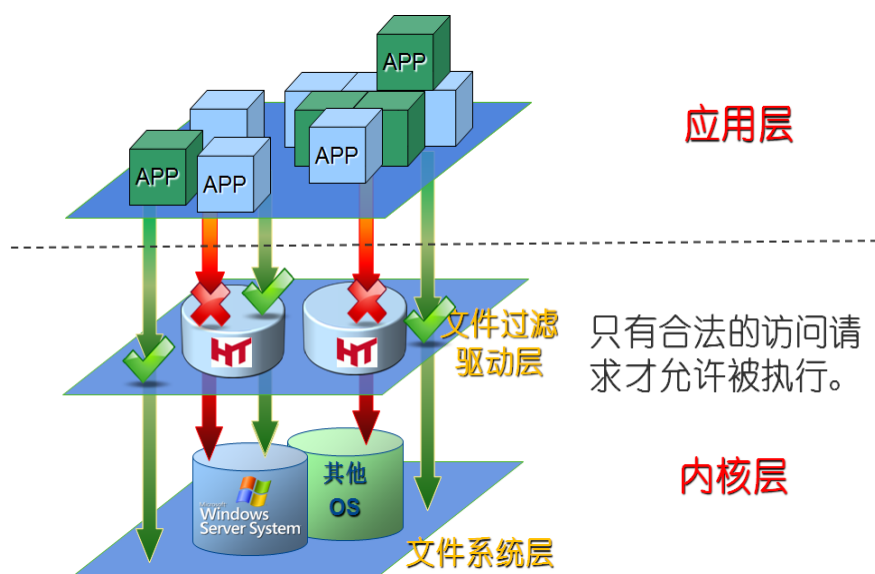


图 6：先进的内核加固技术

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与完整性加以验证，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性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（服务器版）产品将禁止其执行，从而阻止了恶意代码继续传播和破坏，降低了服务器系统完整性被破坏的风险。

3) 以强制访问控制为核心实现对用户行为的严格控制

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、执行程序等）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。保证用户任何行为都在安全策略的支撑下，使得用户登录服务器系统后，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技术

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：加解密速度快、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。

在服务器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，由于缺少解密容器，获取者只能得到密文，从而确保了数据的保密性不被破坏。

7.节点-操作系统安全加固（服务器版）产品优势

1) 先进的设计理念

从服务器“运行安全”、“数据安全”、“安全管理”三个方面出发，打造服务器全生命周期的安全防护。节点-操作系统安全加固（服务器版）产品在保证服务器运行安全的基础上，通过基于主/客体标记的强制访问控制及优化的加解密技术保证服务器中的数据安全，最后通过构建服务器系统统一的安管平台，对系统中的所有服务器进行统一管理、统一配置，审计信息统一存储、统一分析，构建服务器系统整体安全防线，有效保证服务器系统的管理安全。

2) 先进的管理体系

三权分立的管理模式。节点-操作系统安全加固（服务器版）产品对系统管理员、安全管理员和安全审计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，三个管理员之间既相互制约，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”，实现对整个服务器系统的统一管理。



图 7：三权分立的管理模式

3) 对服务器统一管控，构建整体安全防线

构造服务器统一管控的管理体系。信息安全具有“短板效应”，任何一个服务器的安全漏洞都可能对整个服务器系统的安全造成威胁。节点-操作系统安全加固（服务器版）产品构建全系统统一的“安全管理平台”，对系统中的所有服务器进行统一管理、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，有效保护服务器的安全。

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（服务器版）产品赋予了服务器对恶意代码的主动防御的能力，使得服务器做到了对已知/未知病毒、木马、攻击程序等恶意代码的自免疫，从而有效配合甚至替代传统的病毒查杀类产品。

5) 有效解决系统补丁问题

节点-操作系统安全加固（服务器版）产品在对操作系统安全架构深入理解、安全漏洞深刻分析、攻击手段剖析研究的基础上，通过结合可信计算技术，采用主动防御技术，通过对未知漏洞的有效防御，有效配合甚至代替系统补丁。这种安全机制及安全架构的变革，具有极其重大意义。

➤ 持续安全支撑操作系统的各个版本

鉴于产品周期原因，如微软在新一代操作系统较为成熟后，会相应停止对以前老系统版本支持，不再发布系统补丁。此时，为了服务器系统安全，用户不得不购买新一代的操作系统，进行系统升级。而节点-操作系统安全加固（服务器版）产品的主动防御技术，则可以继续安全支撑这种老版本的操作系统，减少用户投资，节省用户开支。

➤ 延长应用系统的生命周期

许多的应用系统是基于老版本的操作系统开发，而伴随服务器操作系统的更新换代，应用系统也同样面临二次开发问题。由于节点-操作系统安全加固（服务器版）产品支持包括老版本在内的服务器操作系统各个版本，因此避免了服务器系统的重复建设投资，为用户节省了大量二次开发资金。

➤ 用户无需担忧操作系统补丁的“善恶”之分

面对数以百计的服务器操作系统补丁，用户不免会有如下担忧：第一，在解决原有漏洞的时候，是否会引入新的漏洞；第二，服务器操作系统升级过程中，是否会影响服务器的稳定运行；第三，升级过程中，是否会引入病毒木马等。节点-操作系统安全加固（服务器版）产品则解除了用户的担忧，降低了相关的信息安全风险。

➤ 降低对操作系统厂商的依赖性

由于操作系统厂商的升级补丁中，可能蕴含某些商业利益问题，如微软的正版补丁等。这样，就形成了用户一直被系统厂商“牵着鼻子走”的局面。而节点-操作系统安全加固（服务器版）产品的主动防御技术，抛弃了操作系统补丁，降低了用户对操作系统厂商的依赖性。

6) 应用安全隔离及透明应用支撑

节点-操作系统安全加固（服务器版）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、对文件系统的强制访问控制，达到对应用进行“安全隔离”的效果。

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（服务器版）产品在对大量应用的细致分析的基础上，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（服务器版）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（服务器版）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（服务器版）产品采用内核级的安全机制，系统的进程启动管理、访问控制等安全机制均在操作系统核心层实现，安全模块一旦被加载，有效防止恶意程序的非法篡改或卸载；安全模块随服务器操作系统一起加载，安全布控时机早，可有效防止安全机制被旁路的可能；安全机制工作在服务器操作系统内核层，杜绝了旁路和隐通道，增强了安全性，实现对服务器操作系统更有效的保护。

8. 节点-操作系统安全加固（服务器版）产品性能测试

8.1 测试环境

| 项目 | | 测试机 1 | 测试机 2 |
|--------|--|---------------------------------|------------------------------------|
| 硬 件 | 主机类型 | 刀片机 | PC 服务器 |
| | CPU | Intel Xeon E5504 2.00GHz*8 枚 | Intel Pentium(奔腾) D 3.20GHz*2 枚 |
| | 内存 | 6GB (三星 DDR3 1333 MHz) | 2GB (英飞凌 DDR2 533MHz) |
| | 磁盘 | 希捷 ST9146803SS 160G | 迈拓 6L160M0 160G |
| | 阵列卡 | 无 | 无 |
| 软 件 | Windows2003 Enterprise Edition X86 | √ | |
| | Windows2008 Enterprise Edition X86 | | √ |
| | Tomcat6.0 | | √ |
| | Weblogic9.2 | √ | |
| | Apsuic5.1 | √ | |
| | MSSQL2005 | | √ |
| | Oracle10G | √ | |

8.2 系统比对测试

8.2.1 测试执行

- 通过Pcmark5对系统相应参数获得测试值，对系统进行评分。

8.2.2 测试值

| | Windows 2003_cle an | Windows 2003_HT | 性能对比趋势 | Windows 2008_cle an | Windows 2008_HT | 性能对 比趋势 |
|---------------------------|---------------------------|--------------------|---------|---------------------------|--------------------|------------|
| FileDecryption _System | 55.56 | 54.74 | ↓ 1.48% | 69.50 | 69.48 | ↓ 0.29% |
| FileCompressi on_CPU | 9.06 | 9.06 | 0 | 8.01 | 8.01 | 0 |
| FileDecompres sion_CPU | 126.55 | 126.54 | ↓ 0.01% | 126.94 | 126.74 | ↓ 0.16% |
| FileEncryption | 55.97 | 55.75 | ↓ 0.4% | 74.08 | 74.00 | ↓ |

| | | | | | | |
|-----------------------------------|----------|---------|---------|---------|---------|------------|
| _CPU | | | | | | 0.11% |
| FileDecryption _CPU | 55.38 | 54.74 | ↓ 1.16% | 69.60 | 69.56 | ↓ 0.06% |
| ImageDecomp ression_CPU | 27.94 | 27.94 | 0 | 25.92 | 25.87 | ↓ 0.2% |
| AudioCompres sion_CPU | 2899.39 | 2938.16 | ↑ 1.34% | 2154.83 | 2152.10 | ↓ 0.13% |
| MemoryRead- 16 MB | 8971.704 | 8984.02 | ↑ 0.13% | 5959.53 | 5952.90 | ↓ 0.11% |
| MemoryWrite- 16 MB | 5312.08 | 5247.63 | ↓ 1.22% | 4048.73 | 4046.90 | ↓ 0.05% |
| MemoryCopy- 16 MB | 6525.77 | 6524.10 | ↓ 0.03% | 4422.55 | 4406.62 | ↓ 0.16% |
| MemoryLatenc y-Random 16 MB | 6.14 | 6.11 | ↓ 0.49% | 8.01 | 7.96 | ↓ 0.63% |
| HDD-XP Startup | 8.92 | 8.82 | ↓ 1.12% | 7.96 | 7.88 | ↓ 1% |
| HDD-Applicat ion Loading | 6.20 | 6.21 | ↑ 0.16% | 6.05 | 6.10 | ↑ 0.82% |
| HDD-General Usage | 5.48 | 5.51 | ↑ 0.55% | 5.13 | 5.15 | ↑ 0.39% |
| HDD-Virus Scan | 102.00 | 101.30 | ↓ 0.69% | 91.77 | 91.48 | ↓ 0.32% |
| HDD-File Write | 10.12 | 10.13 | ↑ 0.1% | 9.58 | 9.80 | ↑ 2.3% |

8.2.3 测试结果

- 根据以上获得的数据，安装后与初始的操作系统并未查看到明显的评分差。安装前后的分差浮动较小，对系统影响在**1.5%**以内，并未造成明显的差异。

8.3 操作系统稳定性测试

8.3.1 测试执行

- 使用super_pi程序运行不同位的运算的获得操作系统的稳定性。
- 分别运行不同的位数继续获得是否会导致系统崩溃，如未崩溃则增加运行位数。
- 运行最大 π 位为3355万位。

8.3.2 测试值

| 测试系统 π 运算 | Windows2003 _clean | Windows2003 _HT | Windows2008 _clean | Windows2008 _HT |
|--------------|-----------------------|--------------------|-----------------------|--------------------|
| 838 万位 | 04:01 | 03:59 | 07:27 | 07:52 |
| 3355 万位 | 19:05 | 19:03 | 34:47 | 34:56 |

8.3.3 测试结果

- 通过以上测试结果运行结果：在所设定的操作系统中均能正常运行最高π 位，测试通过。

8.4数据库稳定性测试

8.4.1 测试执行

- 通过LoadRunner的Java vuser调用已经写好的数据库jdbc连接插入查询类进行时。
- 运行行为10个用户并发测试 持续运行72小时以上。

8.4.2 测试值

| 测试系统 数据库 | Windows2003 _HT | Windows2008 _HT | Windows2003 _HT 平均响应时 间 | Windows2008 _HT 平均响应时 间 |
|-------------|--------------------|--------------------|-------------------------------|-------------------------------|
| Oracle10G | 4768843 次 | 2997591 次 | 0.024 | 0.188 |
| MSSQL2005 | 2575528 次 | 2580202 次 | 0.06 | 0.059 |

8.4.3 测试结果

- 测试中未遇到系统崩溃或无法收到反馈消息的情况。消息反馈时间与性能比对测试时所获得的数据偏差轻微。

8.5中间件稳定性测试

8.5.1 测试执行

- 通过LoadRunner的web协议 调用导入的页面。
- 运行行为10个用户并发测试 持续运行72小时以上。

8.5.2 测试值

| 测试系统 中间件 | Windows2003 _HT | Windows2008 _HT | Windows2003 _HT 平均响应时间 | Windows2008 _HT 平均响应时间 |
|---------------|--------------------|--------------------|---------------------------|---------------------------|
| Tomcat6.0 | 2456558 次 | 2446719 次 | 0.004 | 0.004 |
| Jboss4.2.3.GA | 2593042 次 | 2579439 次 | 0.003 | 0.003 |
| Websphere6.0 | 2534354 次 | 2585096 次 | 0.003 | 0.003 |
| Weblogic9.2 | 2614757 次 | 2573632 次 | 0.003 | 0.003 |
| Apusic6.0 | 1759472 次 | 1834990 次 | 0.283 | 0.202 |

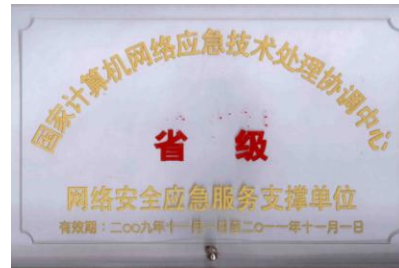
8.5.3 测试结果

测试中未遇到系统崩溃或无法收到反馈消息的情况。消息反馈时间与性能比对测试时所获得的数据偏差轻微。

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