可信华泰
HTTC INFO TECH

WHITE BLOOD CELL

Trusted active
immune defense
system

Technical
white paper

# “白细胞”
# 可信主动免疫防御系统
# 技术白皮书

北京可信华泰信息技术有限公司


## 商标声明

可信华泰和白细胞均为北京可信华泰信息技术有限公司的商标。

## 免责声明

本文档可能含有预测信息，包括但不限于有关未来的产品系列、新技术等信息。由于实践中存在很多不确定因素，可能导致实际结果与预测信息有很大的差别。因此，本文档信息仅供参考，且可信华泰拥有对本文档的解释权，所有根据本文档做出的具体行为和决策，以及产生的后果，可信华泰概不负责。

# TABLE OF CONTENTS
# 目 录

# PREFACE 前言 01

随着各行业信息化的迅猛发展，业务应用信息系统越来越多，计算设备终端作为业务应用信息系统和信息数据的主要承载者，其面临的安全威胁越来越多，从操作系统到CPU逻辑、基于漏洞的攻击不断升级。在面对日益复杂、隐蔽化且有组织的攻击者，传统的依据特征库进行匹配杀毒和拦截等方式的不足性越来越明显。这些传统的安全手段难以应对未知的、新的恶意代码攻击，更不能应对来自有组织的行为攻击，无法有效保障业务应用的安全，易导致信息资产被攻击、业务被中断等大量安全事件的发生。

对于具备大量业务信息系统的行业用户，其首要目标是保障业务系统的连续性、信息数据的完整性和机密性，确保业务应用的正常、安全、稳定地运行。然而业务应用系统的运行依赖于操作系统、硬件平台构成的业务环境。当前计算机体系结构缺乏防护部件，导致操作系统漏洞层出不穷，针对硬件的攻击也时有发生。在开发上由于人们对IT认知逻辑的局限性，不能穷举所有逻辑组合，只能局限于完成计算任务去设计业务IT系统，必定存在逻辑不全的缺陷，从而无法避免人为利用缺陷进行的网络安全攻击。因此，解决承载业务应用系统的软硬件平台的安全性也需要受到极大的关注，构建可信环境是解决系统安全的关键。

北京可信华泰信息技术有限公司凭借多年的技术积累和实战项目经验，以我国自主创新的可信3.0技术为核心，以国产密码为基础，为国家部委及各级政府机构、大中型企业、金融财税机构、云计算服务商、工业企业、能源电力单位、交通运输单位等量身打造，推出了可信华泰“白细胞”可信主动免疫防御系统专业安全防护产品，为用户提供恶意软件防护、系统运行环境保障，以及针对业务应用的全方位安全防护等相关功能和服务。产品本着开放融合的架构，协同建立安全体系，让用户专注业务功能免受安全威胁的困扰，为业务应用构建可信、可测、可控的安全防护环境。

# 02 INEXORABLE TREND
# 主动免疫是安全防护技术发展的必然趋势

## 2.1 安全防护技术的必然选择

可信计算的发展路径可以分为三个阶段，如图1所示。可信计算1.0以世界容错组织为代表，主要特征是主机可靠性，通过容错算法、故障诊断实现计算机部件的冗余备份和故障切换。可信计算2.0以TCG（Trusted Computing Group可信计算组织）为代表，主要特征是PC节点安全性，通过主程序调用外部挂接的TPM（Trusted Platform Module可信平台模块）芯片实现被动度量。中国的可信计算3.0的主要特征是系统免疫性，其保护对象为系统节点为中心的网络动态链，构成“宿主+可信”双节点可信免疫架构，宿主机运算同时可信机进行安全监控，实现对网络信息系统的主动免疫防护。

可信计算3.0其理论基础为基于密码的计算复杂性理论以及可信验证。它针对已知流程的应用系统，根据系统的安全需求，通过“量体裁衣”的方式，对应用和流程制定策略来适应实际安全需要，不需修改应用程序，即可构建积极主动的防御体系，能够抵御未知的病毒和攻击。像“WannaCry”、“Mirai”、“黑暗力量”、“震网”、“火焰”、“心脏滴血”等类型的病毒和攻击将不查杀而自灭，特别适合为重要生产信息系统提供安全保障。

目前黑客在利益的驱使下对企业攻击越来越多，企业“封堵查杀”防御方式难以应对利用逻辑缺陷的攻击，消极被动，防不胜防。目前利用逻辑缺陷的漏洞频繁爆出，如幽灵、熔断，都是因CPU性能优化机制存在设计缺陷，只考虑了提高计算性能而没有考虑安全。由这种底层设计缺陷导致的漏洞难以修补，即使有了补丁，其部署难度也是越来越大。幽灵、熔断的补丁部署后会使性能下降30%。同时，企业的安全防护需要结合自身的业务特点，迫切需要一种有效防护、便于部署并且能够应对多变的安全问题的解决方案。

*图1 可信计算发展路径



可信3.0主动防御从逻辑正确验证、计算体系结构和计算模式等科学技术创新方面，去解决逻辑缺陷被攻击者所利用的问题，确保为完成计算任务的逻辑组合不被篡改和破坏，才能有效抵御攻击。从被动防御向主动防御转变，是一个科学问题，也是技术发展的必然趋势。

*表1 可信计算3.0防御特性

| 分 项 | 特 性 |
| --- | --- |
| 理论基础 | 计算复杂性，可信验证 |
| 应用适应面 | 适用服务器、存储系统、终端、嵌入式系统 |
| 安全强度 | 安全强度高，可抵御未知病毒、未知漏洞的攻击及智能感知 |
| 保护目标 | 统一管理平台策略支撑下的数据信息处理可信和系统服务资源可信 |
| 技术手段 | 密码为基因、主动识别、主动度量、主动保密存储 |
| 防范位置 | 行为的源头，网络平台自动管理 |
| 成本 | 低成本，可在多核处理器内部实现可信节点 |
| 实施难度 | 易实施，既可适用于新系统建设也可进行旧系统改造 |
| 对业务的影响 | 不需要修改原应用，通过制定策略进行主动实时防护，业务性能影响3%以下 |


## 2.2 我国网络安全的法规需求

2014年中央网络安全和信息化领导小组成立，习近平总书记提出“没有网络安全就没有国家安全”，极大地促进了网络安全体系建设。2017年6月1日《中华人民共和国网络安全法》正式施行，作为中国第一部全面规范网络空间安全秩序的基础性法律，是网络安全行业在合规性和强制性方面的重大突破。

《中华人民共和国网络安全法》提出“国家实行网络安全等级保护制度，对重要行业和领域的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”，这些内容将落实等级保护制度上升到法律层面，更加明确指明了发展可信计算技术与实施网络安全等级保护制度的重要性。发展可信计算技术与实施网络安全等级保护制度是构建国家关键信息基础设施、确保整个网络安全的基本保障。

2019年5月13日等级保护2.0核心标准（基本要求、设计要求、测评要求）的发布象征等级保护进入了2.0时代，随着等级保护制度的不断深化发展，等级保护2.0强化了可信计算技术使用的要求，把可信验证列入各个级别并逐级提出各个环节的主要可信验证要求。

*表2 等级保护2.0基本要求——可信相关控制点

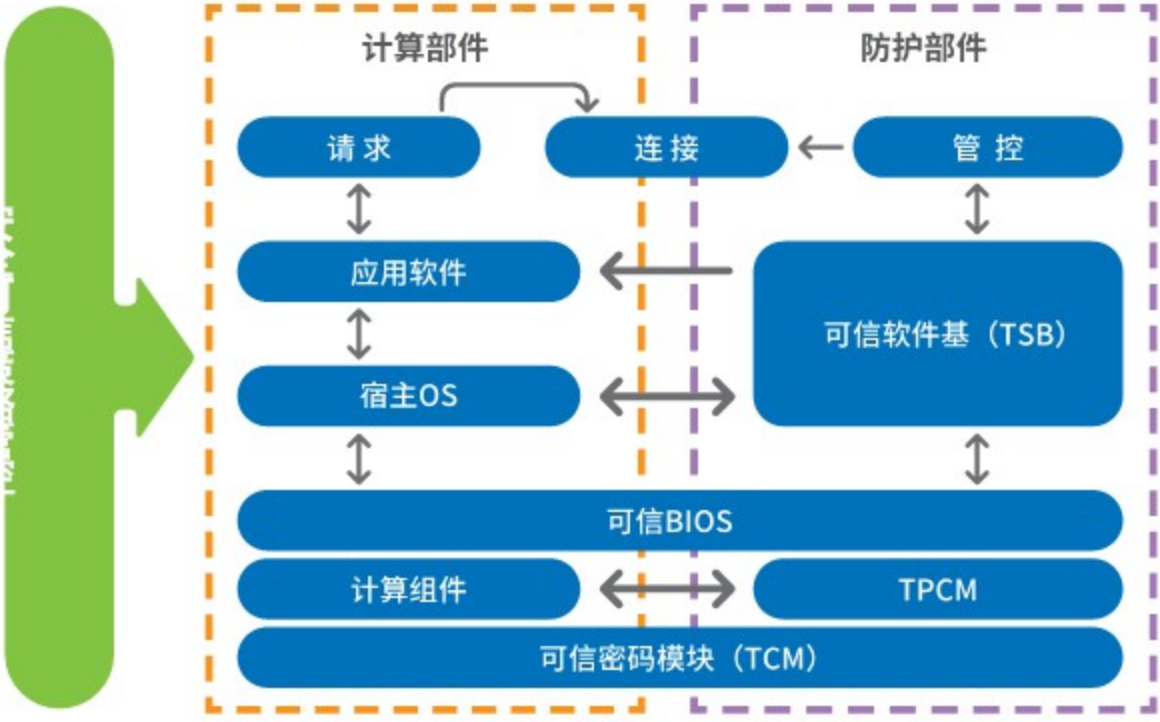
| 要求项 | 一 级 | 二 级 | 三 级 | 四 级 |
| --- | --- | --- | --- | --- |
| 安全通信网络<br>安全区域边界<br>安全计算环境<br>“可信验证” | 可基于可信根对设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。 | 可基于可信根对设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 可基于可信根对设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 可基于可信根对设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。 |
| 安全区域边界<br>-边界防护 | 无可信验证机制要求 | 无可信验证机制要求 | 无可信验证机制要求 | 应采用可信验证机制对接入到网络中的设备进行可信验证，保证接入网络的设备真实可靠。 |
| 安全计算环境<br>-恶意代码防范 | 无可信验证机制要求 | 无可信验证机制要求 | 应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 应采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 |
| 安全管理中心 | ×<br>(一级无此要求项) | 无配置可信验证策略要求 | 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。 | 同三级 |
| 安全区域边界<br>-区域边界<br>访问控制 | / | / | 应在安全区域边界设置自主和强制访问控制机制，应对源及目标计算节点的身份、地址、端口和应用协议等进行可信验证，对进出安全区域边界的数据信息进行控制，阻止非授权访问。 | 同三级 |
| 安全通信网络<br>-可信连接验证 | 通信节点应采用具有网络可信连接保护功能的系统软件或可信根支撑的信息技术产品，在设备连接网络时，对源和目标平台身份进行可信验证。 | 通信节点应采用具有网络可信连接保护功能的系统软件或可信根支撑的信息技术产品，在设备连接网络时，对源和目标平台身份、执行程序进行可信验证，并将验证结果形成审计记录。 | 通信节点应采用具有网络可信连接保护功能的系统软件或可信根支撑的信息技术产品，在设备连接网络时，对源和目标平台身份、执行程序及其关键执行环节的执行资源进行可信验证，并将验证结果形成审计记录，送至管理中心。 | 应采用具有网络可信连接保护功能的系统软件或具有相应功能的信息技术产品，在设备连接网络时，对源和目标平台身份、执行程序及其所有执行环节的执行资源进行可信验证，并将验证结果形成审计记录，送至管理中心，进行动态关联感知。 |

# 03 ARCHITECTURE
# 可信计算3.0体系架构

可信计算3.0是指计算运算的同时进行安全防护，以密码为基因，实施身份识别、状态度量、保密存储等功能，及时识别“自己”和“非己”成分，从而破坏与排斥进入机体的有害物质，相当于为网络信息系统培育了免疫能力。

可信计算双体系架构是主动免疫防御的基础，计算和防护并存的主动免疫双体系架构如图2所示，防护部件由可信密码模块（TCM，Trusted Cryptography Module）、可信平台控制模块（TPCM，Trusted platform control module）和可信软件基（TSB，Trusted Software Base）构成，防护部件拥有独立于主机的软硬件资源，能够主动访问主机所有资源支撑可信验证机制的实施，能够根据可信策略实施主动度量和主动控制，是整个主动免疫防御体系的信任源点。计算部件与防护部件之间具有安全隔离机制，能够确保防护部件的安全性。

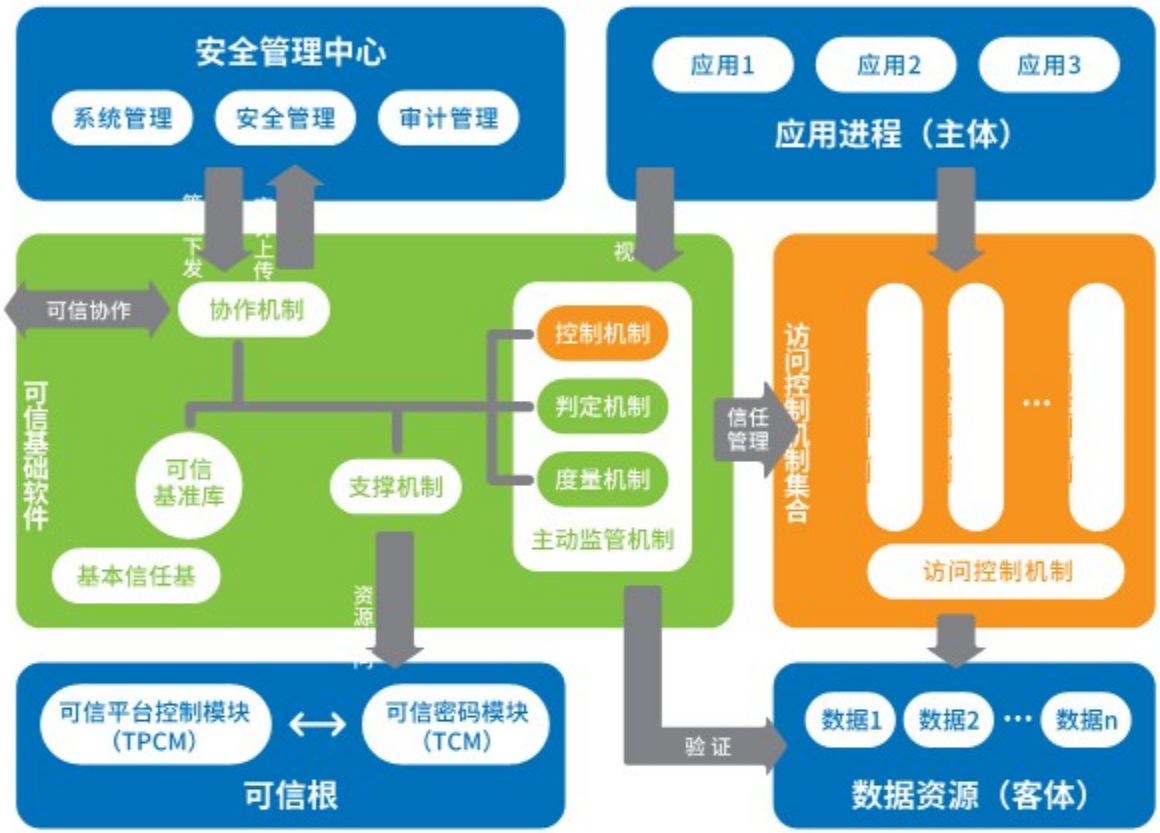
*图2 可信计算双体系架构



## 3.1 可信计算节点

基于可信计算产品构建可信计算节点设备进而打造可信网络。可信节点架构如图3所示：

*图3 可信计算节点架构




可信节点采用双系统体系框架构建，主动免疫是主要的安全特性。通过在计算平台上植入可信平台控制模块TPCM构建可信根，实现了计算和可信的融合（主要通过CPU内置、板载、插卡方式实现）。TPCM在TCM基础上加以信任根的控制功能，采用我国自主密码体系作为免疫基因，实现密码与控制相结合。软件基础层实现操作系统和TSB可信软件基的双重系统核心，通过在操作系统核心层并接一个可信的控制软件接管系统调用，在不改变应用软件的前提下实施对应执行点的可信验证（在验证过程中需可信根支持），达到主动防御效果；网络层采用三层三元对等的可信连接架构，在访问请求者、访问连接者和管控者（即策略仲裁者）之间进行三重控制和鉴别，管控者对访问请求者和访问连接者实现统一的策略验证，将信任由单节点传递至网络，构建可信的信息系统提高了系统整体的可信性。

基于可信的原理和理念，在可信防护的同时对应用程序未作干预处理，这是确保能正确完成计算任务逻辑完整性所要求的，正确的应用程序不需要打补丁，减少了打补丁过程中引入新漏洞的情况。

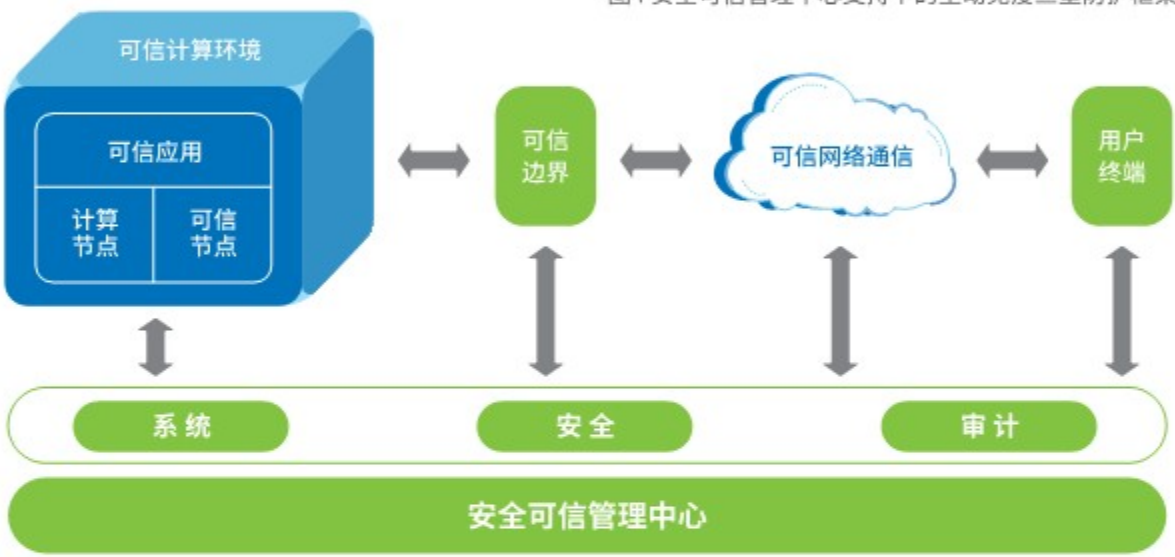
可信安全管理中心支持各种类型的可信节点，支持异构环境为可信计算节点的监控提供可信支撑，提高计算节点自我免疫能力。可信计算节点以物理TPCM和TCM为信任根，实施以TSB可信软件基为核心的可信验证过程，以此支撑业务应用。

架构中的TSB可信软件基由基本信任基、可信基准库、支撑机制和主动监控机制组成。主动监控机制又包括了控制机制、度量机制和判定机制，控制机制是通过监视接口接管操作系统的调用命令解释过程，验证主体、客体、操作和执行环境的可信，根据此执行点的策略要求（策略库表达的度量机制），调用支撑机制进行度量验证，将验证后的结果与可信基准库比对，由判定机制决定处置办法。TSB可信软件基通过主动监控机制，保障业务应用进程行为可信和可信计算节点的安全机制和资源环境可信，实现计算节点的主动安全免疫防护。信任管理是可信机制与其他安全机制的协同防护的方法，通过信任管理将可信的凭据传递到其他安全机制，实现体系化的协同防御。可信协作机制可以实现本地可信机制与其它节点可信机制之间的可信互联，从而实现了信任机制的进一步扩展。管理中心管理各计算节点的可信基准库，并对各个计算节点的安全机制进行总体调度。

## 3.2 纵深防御体系

在可信计算节点主动免疫架构下，将信息系统安全防护体系划分为安全计算环境、安全区域边界、安全通信网络三层，从技术和管理两个方面进行安全设计，建立安全可信管理中心支持下的主动免疫三重防护框架，如图4所示。该框架实现了国家等级保护标准要求（GB/T 25070-2019），做到可信、可控、可管。

*图4 安全可信管理中心支持下的主动免疫三重防护框架




首先在分区分域的基础上，按照信息系统业务处理过程将系统划分成安全计算环境、安全区域边界和安全通信网络三部分，以可信计算节点安全为基础对这三部分实施保护，构成由安全管理中心支撑下的计算环境安全、区域边界安全、通信网络安全所组成的三重防护体系结构，构建纵深防御的信息系统。

(一)安全管理中心

安全管理中心实施对安全计算环境、安全区域边界和安全通信网络统一的安全策略管理，确保系统配置完整可信，确定用户操作权限，实施全程审计追踪。从功能上可细分为系统管理、安全管理和审计管理，各管理员职责和权限明确，三权分立，相互制约。

(二)安全计算环境

安全计算环境是信息系统安全的核心与基础。安全计算环境通过可信计算节点、操作系统、上层应用系统和数据库的安全机制服务，保障应用业务处理全过程的安全。通过在可信计算节点的可信机制和操作系统在可信支撑下的以强制访问控制为主的系统安全机制，形成严密的安全保护环境，通过对程序和用户行为的控制，可以有效防止非授权程序或用户的越权访问，确保数据信息和信息系统的保密性和完整性，从而为业务应用系统的正常运行和免遭恶意破坏提供支撑和保障，构建起信息系统的第一道安全屏障。

(三)安全区域边界

安全区域边界对进入和流出应用环境的信息流进行安全检查和访问控制，安全区域边界的设备本身也是可信计算节点，需要构建自身信任链，在可信机制的支撑下确保不会有违背系统安全策略的信息或连接流经过边界，边界的安全保护和控制是信息系统的第二道安全屏障。

(四)安全通信网络

安全通信网络设备本身也是可信计算节点，在可信机制的支撑下通过对通信双方进行可信鉴别验证，建立安全通道，实施传输数据密码保护，确保其在传输过程中不会被窃听、篡改和破坏，是信息系统的第三道安全屏障。

按照安全可信管理中心支持下的主动免疫三重防护框架，构建积极主动的防御体系，可以达到攻击者进不去、非授权者重要信息拿不到、窃取保密信息看不懂、系统和信息篡改不了、系统工作瘫不成和攻击行为赖不掉的防护效果。

# PRODUCT INTRODUCTION 04
# 产品介绍

“白细胞”可信主动免疫防御系统依据网络安全等级保护系列标准和可信计算3.0相关规范标准进行设计，依托可信计算3.0关键技术，为现有信息系统提供可信支撑，打造可信计算应用环境。使计算机信息系统拥有自免疫能力，以抵御已知和未知威胁攻击。

“白细胞”可信主动免疫防御系统满足GB/T 37935—2019《信息安全技术 可信计算规范 可信软件基》、GB/T 29827—2013《信息安全技术 可信计算规范 可信平台主板功能接口》、GB/T 29828—2013《信息安全技术 可信计算规范 可信连接架台主板功能接口》、GB/T 29828—2013《信息安全技术 可信计算规范 可信连接架构》、GB/T 29829—2013《信息安全技术 可信计算密码支撑平台功能与接口规范》标准，也依据GB/T 25070-2019《信息安全技术信息系统等级保护安全设计技术要求》进行设计，同时满足我国可信密码要求符合GM/T 0011-2012《可信计算 可信密码支撑平台功能与接口规范》、GM/T 0012-2012《可信计算 可信密码模块接口规范》和GM/T 0013-2012《可信计算 可信密码模块符合性检测规范》要求，能够保障系统免受被未知漏洞、未知病毒、未知木马攻击而造成的风险，解决勒索病毒、幽灵、熔断等安全威胁，达到等级保护三级、四级安全需求，为等级保护四级结构化系统建设提供安全支撑和保障。

## 4.1 产品组成

“白细胞”可信主动免疫防御系统主要由可信根、可信软件基（TSB，Trusted Software Base）和可信安全管理中心三个部件组成。其中可信根为硬件部件，TSB可信软件基为软件，可信安全管理中心为管理部件。可信根、TSB可信软件基是部署于节点设备上的可信部件，可信计算节点从安全计算环境、安全区域边界、安全网络通信中三个方面构建，可信安全管理中心是独立部署的管理部件。

*图5 产品组成

### 4.1.1 可信根

可信根依据TPCM、TCM标准进行设计，并集成TCM可信密码模块，能够满足等级保护2.0标准中对可信根的相关要求。其中TCM密码模块符合国家密码局要求，采用国产密码算法SM2、SM3、SM4，依据TCM国家标准提供密码服务和密钥的管理体系。支撑可信计算身份认证、状态度量、保密存储过程中的密码服务。

可信根是主动免疫可信计算3.0体系的根基，在可信计算体系中所起的作用类似计算体系中的CPU，是安全防护策略的执行者。可信根是可信计算3.0体系的最核心部件，是构建计算任务和免疫防护并行双体系结构的基础，也是区别于国际可信计算的关键创新点。

可信根是可信机制的信任源点，具备隔离保障的资源环境，能够并行获取计算节点中的度量对象信息（例如内存中的数据、I/O等），为TSB可信软件基的可信验证提供了数据获取、控制的重要支撑。

可信根是并行于CPU的防护部件，作为建立和保障信任源点的硬件核心模块，为可信计算提供完整性度量、安全存储、可信报告以及密码服务等功能，能够对总线上的寄存器进行控制，读取内存数据、控制I/O设备，并且读取和控制过程不受计算CPU控制，可信根产品上已集成TCM的相关功能。

在实际构建部署可信根时，可根据不同场景选择CPU内置式可信根、外置式可信根方式（PCI-E插卡、插卡及修改主板）构建在计算设备中。CPU内置方式通常适用于信创，以及其他新建场景；插卡及修改主板的方式适用于定制主板、专用设备场景；PCI-E插卡方式适于用存量设备场景。

#### 4.1.1.1 CPU内置式可信根

基于多核CPU架构采用CPU中的一个核、几个核或内置芯片作为可信根的计算单元，并且针对CPU的多核架构建立资源隔离和交互机制，构建出有隔离保障的可信根单独使用的内存和非易失性存储形成可信专用计算资源。

计算资源与可信计算资源是相互隔离的，可信计算资源可以访问计算资源，但计算资源无法访问可信计算资源，计算资源和可信计算资源在CPU内部的划分可以是固定的，也可以是可配置的。

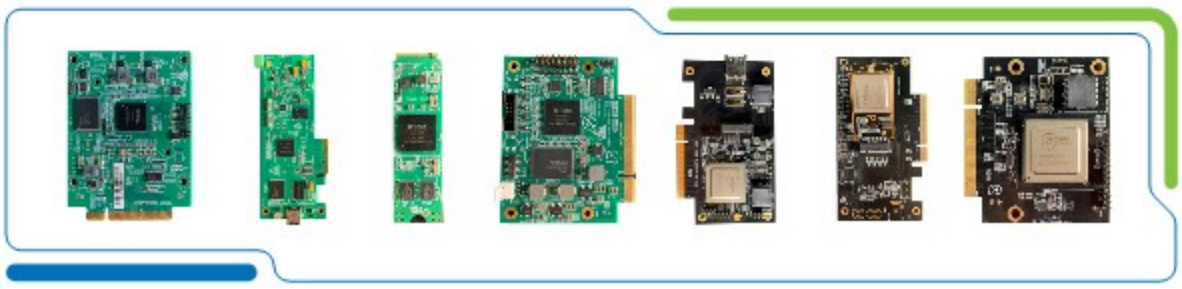
在CPU内部的计算资源主要用于完成计算任务，在CPU内部构建的可信计算资源主要用于对计算子系统进行主动度量（包括静态度量和动态度量）和主动控制，实现完整的可信根功能。

通过CPU内置可信根的方式构建得到双体系结构的可信计算平台，将可信根挂接到内总线上，可信根可以通过内总线获取数据访问和安全控制的能力，实现可信计算的相关工作。

#### 4.1.1.2 外置式可信根

可信根模块以外置模式部署于计算平台主板上，储存证书、算法、密钥、配置信息等重要文件，通过硬件保护避免非法读取和破坏，并提供密码计算服务和主动度量功能，以此为信任根对整个终端建立从启动到运行的信任链。将TPCM的处理器、专有物理内存、持久化存储空间、TCM等集成到PCI-E板卡或模组中得到的可信根。其中，持久化存储区中可以存储有TPCM操作系统、TSB可信软件基程序、密钥等，TCM主要用于为可信根提供加密服务。

外置模式主要有两种方式，一种是修改主板同时通过PCI-E、PCI-E+SPI或M.2与主板相连接，通过修改主板时序电路，使可信根能够先于CPU运行，同时基于SPI或定义的PCI-E、M.2接口改造使得可信根能够读取BIOS等信息，实现主动度量功能并完成启动信任链建立，具体有插卡和板载两种实现方式；另一种方式是不需要修改主板只通过PCI-E总线和主板相连接，进行数据传送，利用PCI-E的DMA机制进行内存度量，这种方式的信任链起点会在BIOS之后，采用标准PCI-E卡实现，多用于存量设备的可信改造。



## 4.1.2 可信软件基


TSB可信软件基是软件层的核心机制，能够动态解析可信策略，截获系统和应用行为，依据策略在可信根的支撑下进行可信验证。TSB可信软件基同时运行在可信体系和计算体系之中，TSB可信软件基的可信验证代理部分，主要实现截获、控制内嵌在计算体系操作系统中，常以内核模块形式存在于操作系统中；同时，部分TSB可信软件基资源运行在可信根中，是可信根的应用层，使用可信根提供的隔离保障的资源进行计算。

TSB可信软件基为终端提供运行时对系统、应用、安全机制的重要度量，并提供安全防护功能，通过TSB可信软件基与可信根的交互保证了终端的安全和自身安全机制的完整，同时将信任传递到应用程序中。TSB可信软件基产品根据不同可信根构建方式进行配套，动态调整采用部分计算资源平衡补充不同可信根构建的差异。

## 4.1.3 可信安全管理中心

可信安全管理中心是对TSB可信软件基、可信根进行策略、基准、日志统一管理的平台，同时也是基于可信数据的服务平台，能够提供可信状态评估支撑可信连接，基于可信日志数据进行数据分析挖掘，呈现可信态势提供可信服务以增强可信计算节点的免疫能力。其中信任管理、关联感知都是在安全管理中心内进行实现。

可信安全管理中心可选择一体机形态的部署方式。可信安全管理中心一体机内置可信根和TSB可信软件基是具备高安全防护的计算节点。也可以采用纯软件方式进行部署，依据用户实际场景选择适合的方式。

# 4.2 主要功能列表

## 4.2.1 可信功能

*表3 可信功能列表

| 功能名称 | 功能描述 |
| --- | --- |
| 信任链建立 | 在可信根的支撑下建立可信计算设备的信任链，依据不同的构建方法信任链的起点不同，CPU内置方式构建的完整信任链，板载和插卡依据具体改造方式构造完整信任链或起点在BIOS的信任链。<br>启动信任链建立的基本思想是，一级度量一级，一级信任一级，保证系统启动的可信性。启动过程中的所有节点都应基于可信根进行可信验证。启动过程包括整个启动链条的逐级度量，构成一个完整的信任链，保障启动以后进入一个可信的计算环境。<br>各环节度量模块根据度量策略的配置由TPCM完整的对度量对象数据获取和对系统的控制，由TCM完成对被度量数据的哈希计算、扩展哈希值到平台状态记录中，由TSB可信软件基完成策略解析基准值比对、度量日志生成等步骤。主要环节为对BIOS/UBOOT/PNOR、OS Loader、OS kernel、TSB可信软件基软件、APP等进行度量。 |
| 静态度量 | 静态度量是采用可信计算技术机制在可执行代码加载前对静态存放数据信息进行可信度量的功能，静态度量先于CPU启动，对系统的硬件配置、固件进行度量，验证之后才将控制权交于CPU，根本上阻止了针对BIOS、BMC等的固件级的病毒、木马攻击。<br>静态度量包括截获、度量、判定、控制四个过程，在不同阶段静态度量采用不同方式截获加载获取度量对象的数据进行度量并依据策略进行控制。<br>APP度量对象：Windows系统的度量对象为可执行文件格式，包括：exe、dll、ocx、sys、com脚本（msi、msu、bat、cmd）等；Linux系统的度量对象为可执行文件格式，包括：脚本（shell、python、ruby、perl、go）、安装包（deb、rpm）、二进制可执行文件、动态库、静态库和内核模块（驱动程序）等的静态度量。 |
| 动态度量 | 需通过CPU，使得对关键内容的度量更为安全可信，并大幅减少在安全度量时对系统资源的占用。<br>主要度量对象包括：内核模块、进程代码段、进程相关共享库、中断描述表、系统调用表、superblock、net_family、socket、net_device、TCP/IP协议栈、内存块等。支持对Linux系统关键信息（包括：中断描述符表、系统调用表、系统模块代码段、系统共享库代码段、应用进程代码段等）和Windows系统关键信息（包括：内核函数表、中断描述符表、全局描述符表、内核进程信息和内核线程信息等）的动态度量。 |
| 可信报告 | 可信报告是终端可信节点对外部提供的终端可信状态数据，包括终端身份和终端状态的信息。终端状态信息通过终端TSB可信软件基的静态度量、动态度量产生相应的数据，再获得相关数据后在可信根的支撑下使用TPCM中的平台身份证书进行签名，外部可信报告使用者可通过验签确定可信报告的身份和可信报告的完整性。可信报告包含报告时间、终端标识、可信状态评估值、非法访问次数、应用程序度量失败次数、内核度量失败次数等，支持HTML格式报告导出。 |

| 功能名称 | 功能描述 |
| --- | --- |
| 恶意代码防范 | 终端可信计算机制下的可信根、TSB可信软件基能够拦截终端系统上所有的可执行代码，对可执行代码进行判断，拒绝不可信执行代码的运行，具备恶意代码防范能力，能够及时识别“自己”和“非己”执行代码，在无补丁升级，无病毒、木马查杀的情况下，有效防御入侵和病毒等恶意代码行为。 |
| 协同联动防护 | 支持多种可信安全策略的相互联动，协同联动实施可信安全防护。如：可在访问控制和白名单策略中联动动态度量策略，将权限判定与系统所处环境可信状态相结合对行为进行防护，防止恶意攻击的绕过安全控制机制。 |
| 基于信任链的自身防护 | TSB可信软件基在内核保护模块中实现了自保护功能，内核模块可隐藏自身，防止被恶意卸载，防止通信代理通过hook系统杀死命令“kill, kill all”等被恶意杀死等，保护TSB可信软件基程序自身进程不被恶意破坏，防止非法篡改或停止。 |
| 可信连接 | 可信连接是对可信计算节点应用的扩展，同时也是计算节点设备接入网络的控制机制。可信连接在节点接入网络之前，对节点用户的身份进行认证；如果用户身份认证通过，则对节点平台的身份进行认证；如果平台认证通过，则对节点的平台可信状态进行度量。如果度量结果满足网络接入的安全策略，则允许节点设备接入网络，否则将节点连接到指定的隔离区域，对其进行安全性修补和升级。可信连接功能由TSB软件基实现，其中用户身份、平台身份需要可信根支撑完成，平台状态主要由动态度量、可信报告支撑完成。可信连接旨在将节点的可信延伸到网络中，从而确保网络连接的可信。 |
| 策略学习 | 开启学习模式后会记录学习过程中的所有执行程序、所有执行程序对所有目录文件的访问记录、网络上所有的IP和端口访问，通过这三个方面的学习能够使管理员快速了解业务系统的实际现状，并能根据记录转换成策略，制定出针对实际业务环境匹配的可信策略。 |

### 4.2.2 安全功能

*表4 安全功能列表

| 功能名称 | 功能描述 |
| --- | --- |
| 可信标记访问控制 | 支持授权主体（用户级或进程级）配置访问控制策略，支持根据该策略确定主体对客体（文件、数据库表、字段、记录等）资源的访问规则，包括创建、读、写、修改、删除等。<br>支持对主体、客体设置安全标记，在访问控制同时能够对主体、客体和环境进行可信度量，可基于主、客体安全标记和强制访问控制确定用户对文件或数据库表等资源的访问。<br>访问控制功能也可以控制网络，支持远程登录控制、端口控制、IP黑/白名单配置等。 |
| 可信应用防护 | 具备对业务应用的安全防护功能，可对访问业务程序及数据的行为进行控制，对应用所处的目录进行访问控制，设置客体对已添加受保护的关键资源（目录、文件、函数库等）的只读权限，限制修改删除权限，保障业务应用相关的数据不被非法篡改和注入，有效保证业务程序的配置文件、动态库和业务数据的安全。 |
| 移动介质管理 | 支持对U盘、移动硬盘等移动存储介质设备进行注册管理，对注册设备设置标记和权限，包括设备归属人、设备名称、设备ID、权限等。节点TSB可信软件基禁止未注册或无权限设备的接入终端使用，可对已注册设备在不同节点可设置不同的读写权限（可设置读写或只读），防止因非法存储设备造成的数据外泄。 |
| 文件保险柜 | 节点TSB可信软件基提供文件保险柜功能，能够创建文件保险柜设置密码，打开保险柜时可以将重要数据存放于保险柜中；关闭保险柜时将保险柜中的数据，进行安全存储并隐藏。 |
| 文件加密防护 | 节点TSB可信软件基提供基于国密算法的文件加解密功能，加密密钥与节点平台绑定，创建解密口令。用户可以通过解密口令进行数据解密。 |
| 数据擦除 | 节点TSB可信软件基提供数据擦除功能，能够将文件系统上的数据擦除，不被非法恢复和使用，保障数据的彻底删除。 |

### 4.2.3 管理功能

*表5 管理功能列表

| 功能名称 | 功能描述 |
| --- | --- |
| 三权分立管理 | 采用三权分立管理模式，将管理员划分系统管理员、安全管理员、安全审计员。系统管理员对用户身份、平台身份系统资源等进行管理；安全管理员负责可信安全策略的配置、下发、维护等全生命周期的管理，同时负责定义安全级别以及授权等；安全审计员负责制定审计策略，并对审计记录进行存储、备份、查询等。通过“三权分立”的管理模式，使得系统中的不同角色各司其职，相互制约，共同保障信息系统的安全。 |
| 基准管理 | 管理中心存储维护所有节点的基准库，具备采集、编辑、配置基准的功能，能够将基准值下发至各终端节点中的TSB可信软件基，并进行维护使用。终端节点的TSB可信软件基同时具备基准管理功能，能够采集本地终端的基准信息，能够接受管理中心的基准信息，能够在本地存储使用基准信息，同时保障基准信息的存储安全，进行基准使用权限的控制。 |
| | 1、系统基准值采集节点可信根和TSB可信软件基能够采集系统启动过程中的基准值，包括BIOS、OS Loader、OS kernel的基准值。采集后的基准值会上传至管理中心进行存储。<br>2、软件基准值采集<br>支持Linux系统和Windows系统软件包的基准值采集，支持格式包括：Windows：msi、exe、网络插件格式；<br>Linux：deb、rpm、tar.gz格式。<br>在可信安全管理中心提供上传软件包的方式，上传后软件包在管理中心进行存储。同时也提供本地采集软件基准值的工具。 |
| 策略管理 | 可信安全管理中心进行可信策略的制定、下发、维护和存储等，可信策略包括静态度量、动态度量、可信报告、可信连接、访问控制、免疫防护、联动协同、移动设备控制、应用防护等。<br>可信安全管理中心提供策略编辑的页面、支持策略导出、在线策略编辑和文本策略编辑（目前支持xls格式策略编辑），支持策略的批量下发和指定节点下发。<br>终端节点的TSB可信软件基支持策略接收、策略解析和策略配置。TSB可信软件基支持基于策略语言的策略解释器，能够自动解释、配置管理中心的策略，依据不同的策略完成策略配置工作。 |
| 策略模板 | 根据对大量项目案例场景的统计和分析，对常见的应用程序和使用场景，可信安全管理中心提供针对特定场景的安全防护策略模板，用户可根据使用习惯及场景直接选用策略模板，实现策略配置的自动化，同时满足用户高安全的防护效果。<br>例如：登录场景，对用户登录系统（包括远程SSH、telnet和本地登陆等）过程中的所涉及的程序、服务、文件、共享库等进行关联防护，提升用户关键操作场景中的防护能力，提高策略部署的便捷性和准确性。<br>此外，策略模板支持专家模式，可增大安全防护的精度。 |

| 功能名称 | 功能描述 |
| --- | --- |
| 审计管理 | 管理中心支持审计日志的策略编辑、策略下发、日志存储、日志查询、日志导出等功能。<br>终端TSB可信软件基能够接受审计策略、配置审计策略，依据策略采集、上报审计日志。审计日志包括：记录事件ID、事件时间、事件类型、事件内容描述、主体标识、客体标识和事件结果等。<br>审计日志采用可信保护机制，即通过TCM的密钥进行签名，保护审计日志的完整性和安全性，包括系统白名单日志、动态度量日志、应用防护日志、注册表日志、系统日志（管理员操作日志、设置日志）等。<br>审计管理支持安全敏感级别分类，根据敏感级别的不同，提供不同的日志展示方式，如低敏感级别的日志提供查看功能，高敏感级别的日志以弹窗方式进行展示。<br>审计管理支持自定义审计日志策略，可选择成功审计、失败审计、全审计、不审计四个类型。支持日志备份配置，自定义备份周期。支持日志条件检索，提供列表或视图方式的结果展示，并支持xlsx、xls格式日志导出。 |
| 应用软件管理 | 在可信计算的体系中终端节点使用的软件都是经过采集基准后的程序才能运行，所以可信安全管理中心提供对采集后的软件包的存储并提供FTP服务，方便用户能够快速下载安装可信的软件。<br>通过证书技术建立终端软件使用的管理体系，在软件使用前对安装软件包的来源一致性和安全性进行检查，只有通过检查后才能使用，并规范化、简单化终端安装软件包的过程，保证管理员能够及时了解终端安装软件包的情况，可通过管理中心进行采集、效验、下发安装、升级、查看和删除可信软件包等维护工作。 |
| 部署管理 | 1、TSB可信软件基安装包管理<br>TSB可信软件基的Linux版安装包众多，可信安全管理中心依据TSB可信软件基的安装信息（安装包名称、大小、上传时间、系统类型、系统版本、体系架构）进行分类管理提供搜索及查看功能，并支持本地安装包手动导入，设置主（默认）安装包等。<br>2、智能匹配安装<br>支持对网内终端的自动化智能安装部署，支持新建推送模板及模板导入，可采用远程推送或多选推送、智能匹配的方式进行部署，支持图形化和静默安装。可信安全管理中心会推送轻量安装脚本到终端上，通过脚本采集终端操作系统版本信息回传至管理中心，管理中心依据操作系统版本信息选择适合的TSB安装程序进行推送安装。通过录入终端信息，自动匹配并选择推送安装包，可实时展示终端侧的安装进度、状态等信息。 |
| 终端管理 | 可查看网内可信节点信息，包括节点名称、IP地址、操作系统类型、操作系统版本、体系架构、安装时间、在线或离线状态、CPU、内存、磁盘使用率、Windows进程查看等，并支持根据终端名称进行搜索，查看并修改终端信息，终端状态注销及维护等。<br>可对节点可信状态进行评估，查看终端安全可信状态信息等。 |

# 4.3 产品参数

## 4.3.1 适配软硬件平台

*表6 适配软硬件平台

| 形 态 | 类 型 | 性能参数 |
| --- | --- | --- |
| 可信根 | 适配CPU平台 | 支持飞腾、龙芯、兆芯、申威、ARM、X86、Power等多种平台 |
| | 内置CPU平台 | 飞腾2000系列以上CPU、海光CPU、津逮CPU |
| 可信软件基 | 适配操作系统 | 支持麒麟、中科方德、凝思磐石、统信UOS、Red Hat、Centos、Kylin、Ubuntu、Windows7、Windows Server2008、Windows Server2012等主流操作系统 |

## 4.3.2 性能参数

*表7 性能参数

| 类 型 | 性能参数 |
| --- | --- |
| 单台支持最大终端并发 | 支持终端并发数量≤500，（可集群部署） |
| 资源占用率 | CPU＜5%；内存＜5% |
| 其他影响 | 对其他应用软件启动和执行时间的影响＜5% |

# IMPLEMENT DEPLOY 实施部署 05

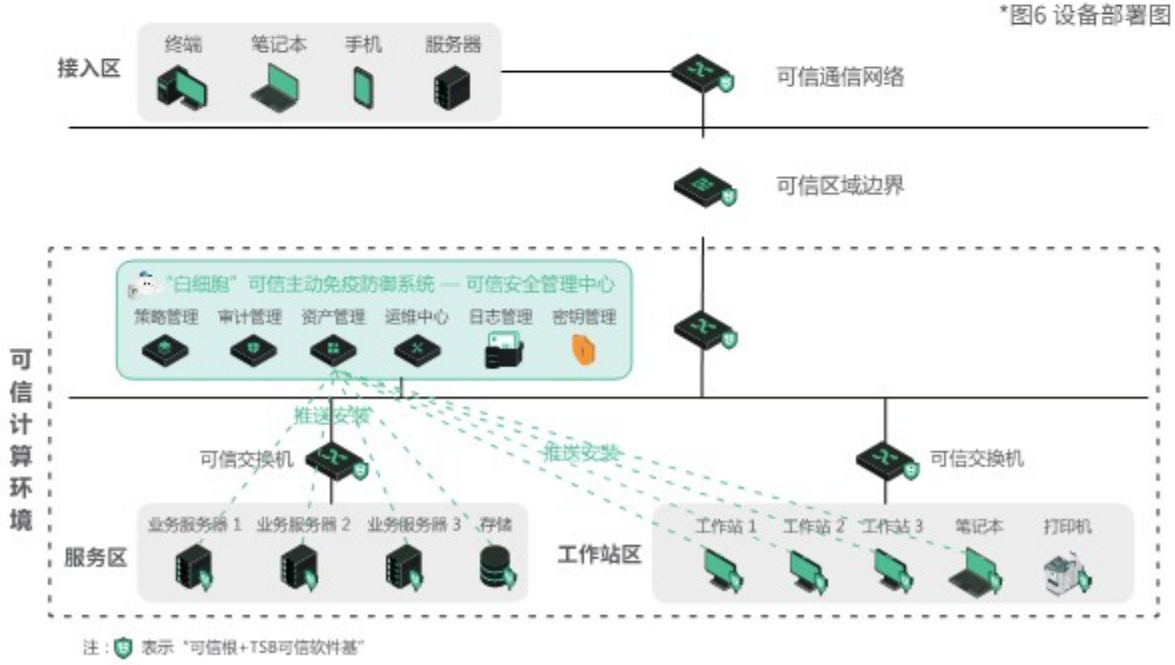
实施可信主动免疫防御系统首先需要确定可信根构建方式，对于新建系统建议采用内置可信的CPU来构建可信根；对于现有信息系统建议采用PCI-E外插卡方式来构建可信根。

第二步在局域网内安全管理域中部署可信安全管理中心，可采用一体机方式部署或软件部署可信安全管理中心，要确保可信安全管理中心的网络可达。

第三步在局域网内的PC终端、服务器、前置机、工作站等终端节点上部署TSB可信软件基，可选用可信安全管理中心的推送功能进行批量部署（推送安装需要知道终端的用户名、密码、IP），安装时TSB可信软件基安装程序会自动匹配出需要安装的版本从管理中心获取并执行安装；TSB可信软件基也可以手动安装程序，如果手动安装需要注意TSB可信软件基版本需要匹配操作系统版本（包括内核版本）。如果采用操作系统预置了TSB可信软件基的模式，可以跳过安装环节。

第四步登录管理中心，依据业务场景的实际需要进行信息采集（收集），开启对业务系统定制的可信安全防护。

*图6 设备部署图



# 06 ADVANTAGES / HIGHLIGHTS 产品优势/技术亮点

## 6.1 基于双体系架构保障计算全程可测可控

基于计算与安全防护并行的主动免疫双体系防御架构，防护部件可主动访问计算部件的所有资源（如存储、I/O等），而计算部件无法访问防护部件的资源，双方只能通过专用的安全通道进行交互，构建了整个主动免疫防护体系的基石，由于不向应用提供服务，极大地减少了安全的暴露面，让防御能力进一步提升，极大地增强了安全防护的能力。

防护部件以可信根为核心和信任源点，能够先于计算部件处理器启动，对计算部件资源和总线进行初始化配置，并通过直接总线共享机制访问主机所有资源，进行静态和动态可信验证，通过验证方能启动或继续执行，否则进行报警和控制，主动抵御入侵行为。

## 6.2 基于可信计算3.0的恶意代码主动免疫防御

采用可信计算3.0主动免疫防御机制能够主动度量系统中的执行程序、执行代码、计算环境等，依据策略基于白名单保护业务程序，阻止非授权及非预期的执行程序运行，免补丁升级，免病毒、木马查杀，同时实现对已知或未知恶意代码的主动防御。

## 6.3 策略语言定制多场景的精准安全防护

结合用户真实场景，将深度分析沉淀的安全成果转化为简单的模板选择，可有效降低用户安全配置难度，无需查看手册进行复杂配置，根据用户需求直接选择相应场景的安全策略，使策略落地更快捷，安全防护更有效。策略学习模式可以最大程度上让可信策略贴近系统的实际情况，制定出的策略能与实际业务有高契合度，减少管理员工作。

针对高端用户可采用策略语言描述安全场景表达安全需求，形成系统安全防护的编码序列，由TSB可信软件基解释和执行，进行可信保障和可信验证，实现动态度量和智能感知，达到主动免疫防御的效果，为构建高等级的动态化（云计算场景）、智能化主动防御体系提供基础支撑。

## 6.4 基于可信计算平台构建协同联动的整体安全防御体系

可信计算3.0的双体系架构将安全机制的度量和控制带到了前所未有的广度和深度，能够获取最真实、最底层、最广泛的信息数据，能够为综合数据分析的安全服务提供有效支撑。

同时可信机制保障了各个安全机制自身的安全不被破坏，通过可信报告信任管理的方式，增强各安全机制的安全判断参考点，使得各个安全部件能够有效联动协同防护，形成整体的防御体系。

## 6.5 与基础软硬件相融合实现应用无感高效防护

可信计算3.0防护机制可内置于基础设备中，可信根可内置于CPU中，TSB可信软件基可内置于操作系统中，内置可信的防御机制与基础软硬件的融合使得安全部署十分容易，在新基础设备中就已经内置的可信机制极大地减轻了用户系统的部署负担。

透明支撑应用系统不需要修改应用从而能够实现有效防护，无需改变用户的使用习惯，让用户在无感的情况下获得高强度的安全保障。可信机制在进行安全运算时不占用业务系统的资源从而使得在安全防护的同时业务系统仍然能够高性能运转。

# 07 CUSTOMER VALUE 客户价值

## 7.1 多维度主动免疫，防护效果更显著

通过建立多维度主动免疫防线，确保系统环境对病毒、木马、漏洞的攻击免疫，从而可以达到攻击者进不去、非授权者重要信息拿不到、窃取保密信息看不懂、系统和信息篡改不了、系统工作瘫不成和攻击行为赖不掉的安全效果。

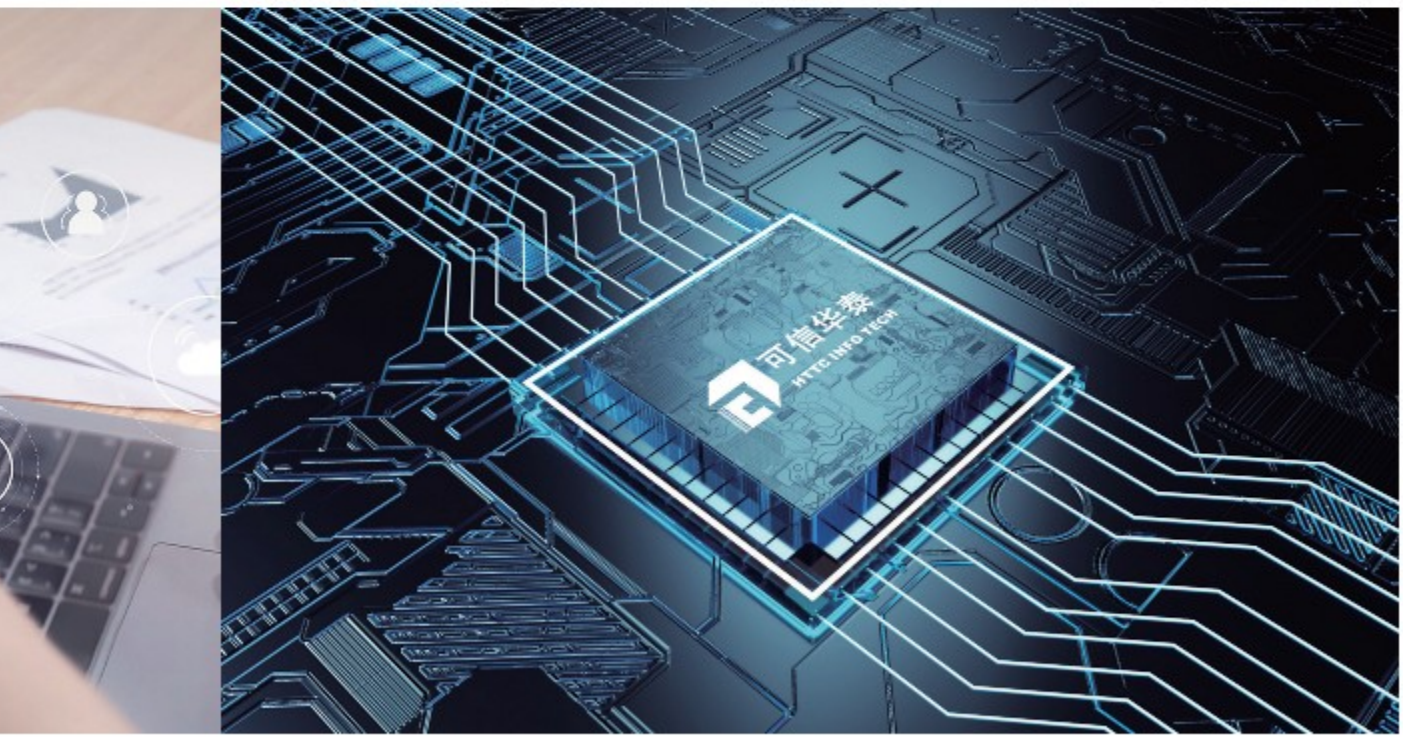
## 7.2 基于可信根设计，满足等保更合规

依据可信计算相关的标准规范进行产品体系和功能设计，符合信息安全技术网络安全等级保护基本要求和设计要求的安全需求，通过灵活的策略配置能够满足等级保护2.0从一级到四级对可信根、可信验证、可信接入等要求，基于可信根能够对所有计算节点实现从开机到操作系统启动，再到应用程序启动的可信验证，并可根据用户需求，在应用程序的关键或所有执行环境中，对其执行环境进行可信验证，支撑基于可信根的可信验证，为用户提供高等级的可信验证功能。“白细胞”可信主动免疫防御系统在为用户构建可信安全操作系统免疫平台的同时协助用户有效落地等级保护，安全更合规。

# CASE INTRODUCTION 案例介绍 08

“白细胞”可信主动免疫防御系统拥有自主知识产权，相关核心技术实现了产业化，已完成在重要领域、重点行业的示范应用和规模化推广，目前已形成了面向全行业市场的产业化推广态势，应用前景极为广阔。

基于可信计算3.0的信息系统安全解决方案主要是在系统关键节点中植入可信根，并部署TSB可信软件基进行实现，其产品具有多种形态和系统版本，可适用于不同的场景和平台。可信根是可信计算3.0和核心组件，也是支撑可信验证功能的主要固件，针对不同类型的设备，在实际构建部署可信根时，可根据不通场景选择CPU内置式可信根、外置式可信根方式（插卡、插卡及修改主板）进行构建。



# 8.1 典型应用

## 某大型国企移动办公安全保障项目

**·背景和需求**

根据等级保护2.0要求和系统在互联网应用过程的实际安全需要，某大型国企组织安全人员制定可信安全方案，实施了可信安全保障示范工程。工程以保障公共服务平台、网络电话、融合通信、分级分权管理、视频会议、必达通知等核心业务安全可信为目标，通过CPU内置的可信计算3.0技术，建立信任链逐步形成网络主动免疫防御体系。

**·方案和价值**

在本项目中，可信华泰协助用户进行移动应用服务器可信计算环境平台建设。通过在移动应用的所有后台服务器中置入可信根，构建双体系的可信服务器，为用户9万多员工提供了可信安全保障，保障了核心服务器安全运行。在项目中采用CPU内置可信根的方式，通过对已有长城服务器（飞腾2000+CPU、麒麟操作系统）的升级将CPU中一个IP核作为可信根的计算单元，并针对CPU的多核架构建立资源隔离和交互机制，构建出有隔离保障的可信专用计算资源；将可信软件基预置在操作系统中，与操作系统进行深度适配整合，为设备建立完整无缝信任链，保障设备安全、运行安全，符合了等级保护2.0标准中可信验证的要求；同时还为业务系统量身定制了安全策略，依据策略在可信根的支撑下进行可信验证，为终端提供运行时对系统、应用、安全机制的重要度量，并提供安全防护功能，同时将信任传递到应用程序中，从根本上提升业务安全能力。

通过疫情期间的稳定运行可信主动防御机制，不仅能够保障业务安全并且对系统资源占用较少，在移动视频业务中安全性能表现优秀。

# 国家电网电力生产调度系统主动免疫防护应用案例

**·背景和需求**

针对国家电网电力生产调度系统高安全系统防护需求，以可信计算为安全基础支撑平台构建安全体系，通过在硬件上引入可信根，从结构上解决计算机体系结构简化带来的脆弱性问题。基于可信根为核心和信任源点，从平台加电开始，到应用程序的执行，构建完整的信任链，一级认证一级，一级信任一级，未获认证的程序不能执行，从而使信息系统实现自身免疫，构建高安全等级的防护系统，是构建积极防御、综合防范的信息安全体系的关键基础。

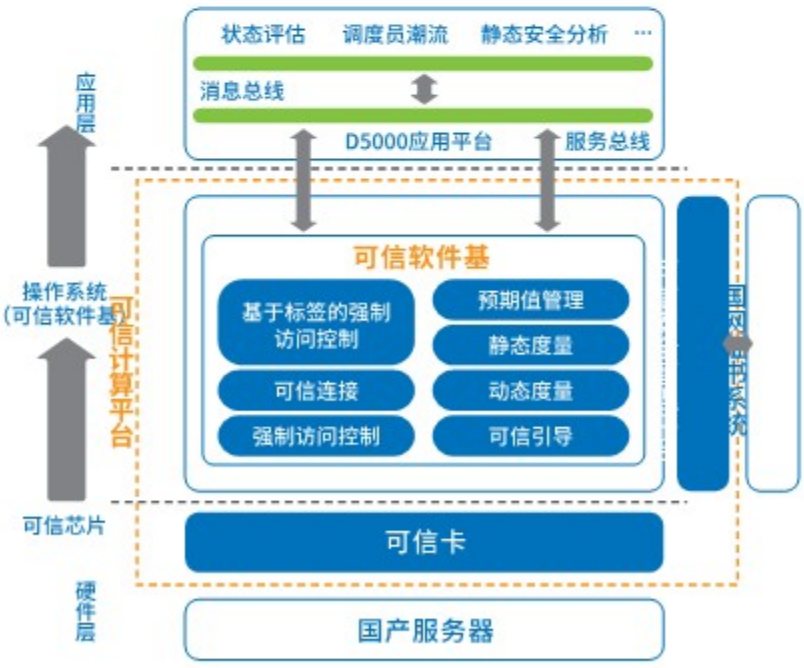
本方案采用可信计算3.0技术体系，建立新一代电力调度系统安全计算环境，实现电调系统底层基础安全，是有效防止来自未知领域、未知途径、未知方式、未知手段、未知空间攻击的最佳方案。

方案服务于国家电网电力调度系统，使国家电力调度系统达到国家等级保护四级的安全要求，同时符合GB/T22239基本要求和GB/T25070设计技术要求。

**·方案和价值**

本方案中的智能电网电力调度系统，其组织架构为国调、省调及地调的树形层次型分级结构。可信华泰通过将可信根部署在计算节点，实现智能电网电力调度控制系统对恶意代码的免疫和智能电网电力调度控制系统基础平台及其高级应用的版本管理，保障系统稳定和可靠的运行。

*图7 国家电网电力调度系统可信加固方案



# 主要功能

### 可信代码度量

TSB可信软件基通过可信度量技术，提供执行代码的主动度量和控制，实现了对恶意代码主动防御的能力，使得各计算节点对已知或未知病毒、木马、攻击程序等恶意代码的自免疫。

### 强制执行控制

TSB可信软件基中，强制执行控制基于DTE模型实现。将系统公有库及基本应用划分为公有域，同时，将不同应用划分为不同的私有域集合。并通过公有域不能执行私有域中的代码；私有域间不允许互相调用进程；通过特权调用策略允许其他域中的进程对私有域中初始进程的启动请求及私有域间合法通信请求等策略保护程序执行安全。

### 动态度量

在系统运行期间通过定时设定、手动触发等操作方式对系统的重要执行路径、内核模块、进程代码段等进行检测，可发现系统隐藏的木马、rootkit等恶意程序的破坏行为，并对其进行恢复。

### 预期值管理

可信安全管理中心辖区内所使用的软件及生成的安全策略，不仅可以使用TSB可信软件基已有的完整性保护，还可以结合智能电网电力调度系统现有的CA生成的签名一起使用。

### 透明支撑

根据智能电网电力调度系统的访问控制逻辑，基于智能电网电力调度系统现有的标签体系生成可信控制的标记，结合TSB可信软件基的可信控制功能，对系统的主客体进行识别，对访问控制行为进行判定。用户的可信性通过可信身份认证、可信平台认证及可信平台安全状态认证来保证，服务的可信性由动态可信度量来保证。

## 可信网络连接

可信连接提供对接入可信网络的请求发起者进行可信状态评估，先对接入者的用户身份进行合法性认证，通过后进而对接入的计算平台的平台身份、可信状态进行验证，确定接入者可信之后，将允许其接入，否则拒绝其接入。

该方案主要部署在国家电网电力调度系统服务器、SCADA、前置机和工作站，目前已完成34个省、市的可信计算规模化部署，通过对部署后的计算环境进行测试和网络分析得出：应用系统适配性良好，整体性能影响在3%以下，能够有效抵御未知病毒木马的攻击。可信计算密码平台规范了电力调度系统中软件使用的权限边界，对应用软件、业务软件实现了统一的版本管理和使用权限管理，将安全保护提前到从引导阶段开始，并建立了硬件级的可信根和基于可信连接的网络连接访问保障机制，整体提升了电网电力调度系统的安全防护和免疫能力。

*表9 可信计算对性能的影响

| 应用 | CPU使用率 | 列1 | 列2 | 内存使用率 | 列3 | 列4 | 计算时间 | 列5 | 列6 |
|---|---|---|---|---|---|---|---|---|---|
| | 加载前 | 加载后 | 影响度 | 加载前 | 加载后 | 影响度 | 加载前 | 加载后 | 影响度 |
| 应用1 | 2.92% | 2.95% | 1.03% | 11.00% | 11.00% | 0.00% | 69s | 69.9s | 1.30% |
| 应用2 | 2.30% | 2.33% | 1.30% | 6.90% | 7.00% | 1.45% | 24.6s | 25.1s | 2.03% |
| 应用3 | 2.80% | 2.85% | 1.79% | 7.80% | 7.90% | 1.28% | 18.9s | 19.4s | 2.65% |

## 8.2 应用案例

### 政府及企事业单位

- 中央国家机关政府
- 国家发展和改革委员会
- 中华人民共和国水利部
- 国家体育总局
- 国家信息中心
- 国家计算机病毒应急处理中心
- 湖南省委
- 云南省委
- 上海市政府
- 河北省人民政府
- 辽宁省委办公厅
- 中央电视台
- 宁波市人民政府
- 中山市人民政府
- 北京市民防局
- 北京市规划委员会
- 北京市交通委员会
- 广东省经济和信息化委员会
- 安徽省经济信息中心
- 安徽省社保基金管理局
- 江西省药品监督管理局
- 合肥市民政局
- 武汉新港管理委员会
- 天津市宝坻区环保局
- 台州市人力资源和社会保障局
- 故宫博物院
- 中国电子信息产业集团有限公司
- 中国电子科技集团公司

### 公检法

- 中华人民共和国公安部
- 中华人民共和国司法部
- 北京市公安局公安交通管理局
- 洛阳市公安局公安交通管理局
- 金华市交通运输局
- 北京市东城区公安局
- 广西南宁市公安局
- 广西省河池市公安局
- 河北省廊坊市人民检察院
- 衡阳市蒸湘区交警支队
- 浙江省德清法院
- 浙江省南浔法院

### 能 源

- 中国石油
- 国家电网
- 中国南方电网
- 三峡水利发电厂
- 全球能源互联网研究院
- 珠海博威智能电网



可信华泰
HTTC INFO TECH

## 金融保险

- 中国人民银行
- 中国农业银行
- 中国银联
- 华夏银行
- 上海保险交易所
- 山西省农村信用社
- 安徽省农村信用社联合社
- 阳光保险集团股份有限公司
- 中国保险信息技术管理有限责任公司
- 阳光渝融信用保证保险股份有限公司
- 中煤财产保险股份有限公司
- 资和信控股集团股份有限公司
- 邯郸银行股份有限公司

## 医疗

- 北京积水潭医院
- 北京友谊医院
- 包头市卫生和计划生育委员会

## 教育

- 北京邮电大学
- 北京工业大学
- 北京信息科技大学
- 淮北师范大学
- 宁波工程学院
- 中国科学院信息工程研究所
- 山东凯文科技职业学院
- 兰州职业技术学院
- 北京西普阳光教育科技股份有限公司

## 其它

- 数据通信科学技术研究所
- 武汉电子口岸有限公司
- 中国电信股份有限公司

扫描二维码关注
**可信华泰**

可信华泰
HTTC INFO TECH

www.httc.com.cn

**地 址：**
北京市海淀区闵庄路3号
清华科技园玉泉慧谷二期2号楼

**联系方式：**
010-88894996