“白细胞”

可信主动免疫防御体系

产品白皮书

可信华泰

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商标。

01 前言

PREFACE

网络空间已经成为继陆、海、空、天之后的第五大主权领域空间。当前，中国网络空间安全形势非常严峻，面临多维度的安全挑战。随着信息技术的迅猛发展和互联网的普及，移动互联、物联网、大数据、云计算、工业互联网等新型信息系统应用场景迅速推广，信息传播的速度、广度和实时性都达到史无前例高度。信息化应用已经深入国家与社会的各个方面，提供便捷性的同时也带来大量的安全风险，如计算机木马、垃圾邮件、网络攻击等。信息系统在新型网络空间场景的使用，极大扩展了原有信息系统的暴露面，安全形势日益严重。

网络不良信息和网络恶意行为不仅会造成重大的经济损失，而且会严重威胁国家的政治、经济、国防、文化等正常秩序，干扰人民群众的正常生活，甚至会引发国家与社会动荡。当前大部分网络安全防护系统依赖于防火墙、杀毒软件和 IDS“老三样”产品，这种被动的防护方式存在全保障能力欠缺，自身安全机制易被篡改、旁路，管理分散等问题，不足以应对新形式下的安全挑战，近年来大量的重大网络安全事件印证了这一点。

因此，为了抵御潜在威胁，必须从逻辑正确验证理论、计算体系结构和计算工程应用模式等方面进行科学技术创新，解决逻辑缺陷被利用的问题，确保计算任务的逻辑组合不被篡改和破坏，实现计算设备的系统化安全。

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计算 3.0 技术为核心，以国产密码为基础，面向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 ，打造“白细胞”可信主动免疫防御体系系列产品，为用户提供针对基础运行环境及业务应用的全方位安全防护。产品本着开放融合的架构，可协同其他产品共同建立安全体系，为用户构建可信、可管、可控的安全防护环境。

02

可信计算技术是安全防护技术发展的必然趋势

INEXORABLE TREND

2.1 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。2016 年 12 月 27 日国家互联网信息办公室发布《国家网络空间安全战略》，提出了“夯实网络安全基础”的战略任务，强调“尽快在核心技术上取得突破，加快安全可信的产品推广应用”，因此，创新发展可信计算安全技术，推动其产业化，是将我国建设成为“技术先进、设备领先、攻防兼备”网络强国的战略任务。

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。其中第十六条规定，国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

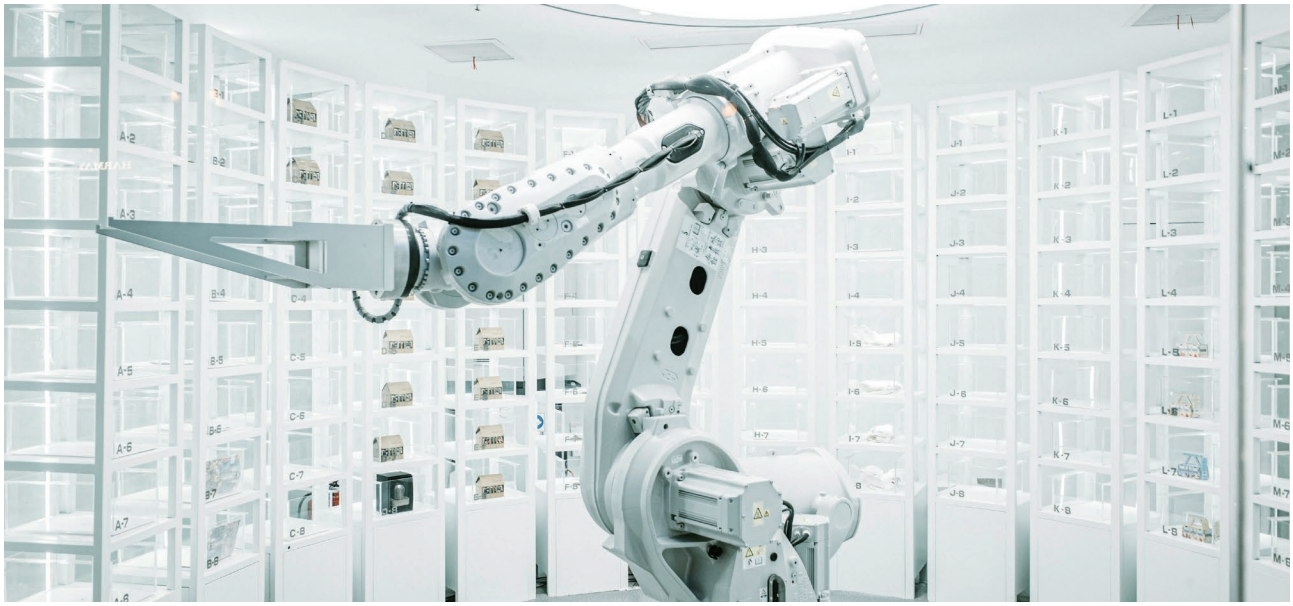
《中华人民共和国网络安全法》提出“国家实行网络安全等级保护制度，对重要行业和领域的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”，这些内容将落实等级保护制度上升到法律层面，更加明确了发展可信计算技术与实施网络安全等级保护制度的重要性。发展可信计算技术与实施网络安全等级保护制度是构建国家关键信息基础设施、确保整个网络安全的基本保障。

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。

2021 年 9 月 1 日《关键信息基础设施安全保护条例》正式施行，其中第十九条例中明确提出了“运营者应当优先采购安全可信的网络产品和服务”，对关键基础设施相关产品的可信功能提出了明确需求。

表2-1 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 安全区域边界 安全计算环境 “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 - 边界防护	无	无	无	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 - 恶意代码防范	无	无	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	/	无	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 - 区域边界 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 - 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。



2024 年 8 月 21 日，中共中央办公厅、国务院办公厅印发的《关于完善市场准入制度的意见》，其中特别强调聚焦人工智能、自主可信计算、信息安全等领域再一次从国家层面强调了可信计算技术的重要性。

以法律法规为方向，目前，国家及各个行业对可信计算的相关要求已具备大量标准及要求。

国家标准情况列表：

表2-2 目前我国可信计算相关标准列表

国家标准名称
GB/T 22239-2019 信息安全技术网络安全等级保护基本要求
GB/T 25070-2019 信息安全技术网络安全等级保护安全设计技术要求
GB/T 28448-2019 信息安全技术网络安全等级保护测评要求
GB/T 20272-2019 信息安全技术 操作系统安全技术要求
GB/T 38638-2020 信息安全技术 可信计算 可信计算体系结构
GB/T 37935-2019 信息安全技术 可信计算规范 可信软件基
GB/T 40650-2021 信息安全技术 可信计算规范 可信平台控制模块
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 可信连接架构
GB/T 29829-2022 信息安全技术 可信计算密码支撑平台功能与接口规范
GB/T 30847.1-2014 系统与软件工程 可信计算平台可信性度量 第1部分概述与词汇
GB/T 30847.2-2014 系统与软件工程 可信计算平台可信性度量 第2部分:信任链
GB/T 38644-2020 信息安全技术 可信计算 可信连接测试方法
GB/T 36639-2018 信息安全技术 可信计算规范 服务器可信支撑平台
GM/T 0011-2012 可信计算 可信计算密码支撑平台功能与接口规范
GM/T 0012-2020 可信计算 可信密码模块接口规范
GM/T 0013-2012 可信计算 可信密码模块接口符合性测试规范
GB 42250-2022 信息安全技术 网络安全专用产品安全技术要求
GB/T 35282-2017 信息安全技术 电子政务移动办公系统安全技术规范
GM/T 0058-2018 可信计算 TCM服务模块接口规范
信息安全技术 办公设备安全规范(代替GB/T 29244-2012,GB/T 38558-2020)
GB/T 信息安全技术 政务计算机终端核心配置规范(征求意见稿)
GB/T 36572-2018 电力监控系统网络安全防护导则

各行业根据国家标准结合行业需求也颁布大量可信计算相关的标准、管理办法及指导文件，标准情况如下:

表2-3 可信计算行业标准列表

中华人民共和国公共安全行业标准
GA/T 1561-2019 移动警务系统 总体技术要求
GA/T 2001-2022 移动警务 可信计算总体技术要求
GA/T 1466.1-2018 智能手机型移动警务终端 第1部分：技术要求
GA/T 1466.2-2018 智能手机型移动警务终端第2部分：安全监控组件技术规范
GA/T 1466.3-2023 智能手机型移动警务终端 第3部分:检测方法
GA/T 1987-2022 执法记录仪接入移动警务系统 技术要求
GA/T 2133.1-2024 便携式微型计算机移动警务终端 第1部分：技术要求
GA/T 2133.1-2024 便携式微型计算机移动警务终端 第2部分：安全监控组件技术规范
公安部可信安全产品检测标准
军队标准
若干项可信相关标准
司法标准
SF/T 0049—2020 司法行政移动执法系统技术规范
建筑行业标准
智慧工地通信网络建设与应用标准（待发布）
通信行业标准
信息系统可信计算能力通用技术要求和测试评价方法（待发布）
通信行业标准
2024-0473T-SJ安全可靠 便携式微型计算机技术要求（征求意见稿）
2024-0474T-SJ 安全可靠 服务器技术要求(征求意见稿)
2024-0475T-SJ 安全可靠 工作站技术要求(征求意见稿)
2024-0476T-SJ 安全可靠 台式微型计算机技术要求(征求意见稿)
2024-0477T-SJ 安全可靠 一体式台式微型计算机技术要求(征求意见稿)
医疗行业
医疗互联互通标准化成熟度测评标准
交通行业
公路水路关键信息基础设施安全保护管理办法

行业采购要求指导文件情况如下表：

表2-4 行业采购要求指导列表

信创产品采购要求
通用服务器政府采购需求标准(2023 版)
操作系统政府采购需求标准（2023 版）
电力行业
火力发电厂工控系统可信验证技术导则(征求意见稿)
电力监控系统主机可信验证技术规范（试行）
电力监控系统网络安全评估指南
电力监控系统可信验证技术要求
传媒行业
广播电视网络安全等级保护基本要求
金融行业
证券期货业网络安全等级保护基本要求

团体标准情况如下表：

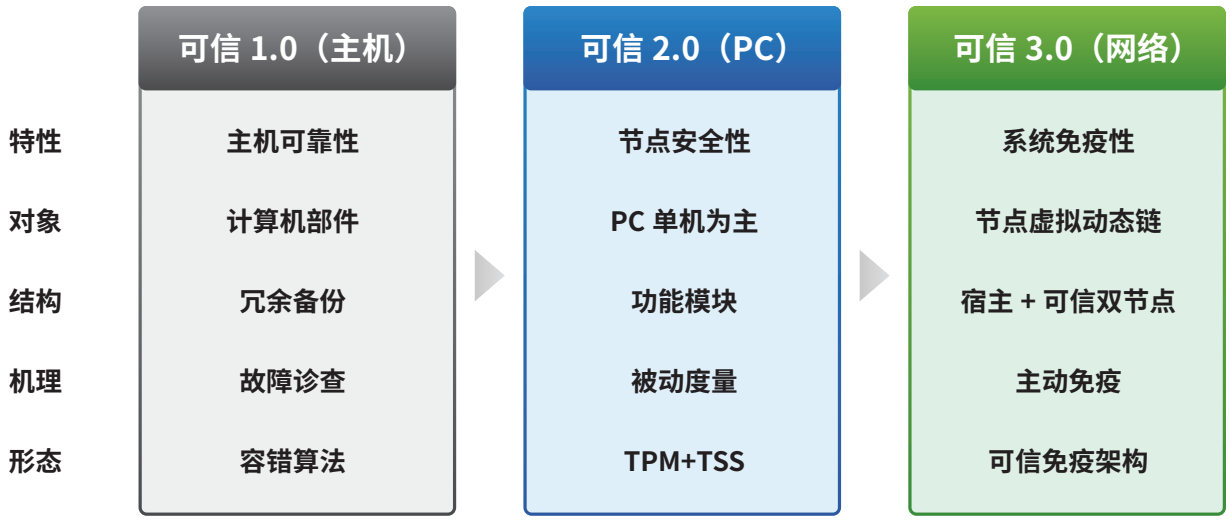
表2-5 团体标准情况列表

中关村可信计算产业联盟
可信计算 办公设备产品技术规范
T/ZTCIA 001—2023 可信计算产品规范
T/ZTCIA 002-2023 可信计算网络安全产品安全可信要求
T/ZTCIA 003-2023 嵌入式可信计算技术要求与测评方法
T/ZTCIA 004-2022 外设产品可信计算技术规范
山东省信息产业协会
T/DSII 006-2023信息安全技术 办公设备打印机技术规范
中关村网络安全与信息化产业联盟
T/ZISIA 04-2024 自主创新型网络安全技术可信计算技术要求
T/ZISIA 01-2024 自主创新型网络安全技术 框架

2.2 可信计算技术发展

可信计算的发展路径可以分为三个阶段，如图 2-1 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，宿主机在运算的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。

图2-1 可信计算发展路径



计算科学、体系结构的发展

可信 3.0 技术基于密码技术从计算体系结构和计算模式方面解决逻辑缺陷，确保完成计算任务的逻辑组合不被篡改和破坏，抵御攻击 , 变被动防御为体系化主动防御。相较于 TCG 组织主推的可信 2.0 技术路线而言，具备更多的技术优势，支持替换为行业合规证书体系、可基于独立系统主动获取度量要素并执行控制、支持基于策略语言描述更复杂的策略场景等更符合国内信息安全防护需求。

表2-6 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 , 理论基础扎实
应用适应面	适用服务器、存储系统、终端、嵌入式系统，适用范围广
安全效果	可抵御未知病毒、未知漏洞的攻击、消除 0day 风险、抵御勒索病毒，安全效果好
保护目标	策略支撑下的数据信息处理可信和系统服务资源可信 , 保护目标可根据策略灵活配置
技术手段	密码为基因，依托双体系架构实现主动度量、主动控制
防范位置	计算环境、区域边界、网络连接
密码证书	密码为国密算法，证书体系支持替换为行业合规证书体系
对业务的影响	在基础环境具备的情况下不需要修改原应用，通过制定策略进行主动实时防护，业务性能影响 3% 以下，对业务系统影响低

03

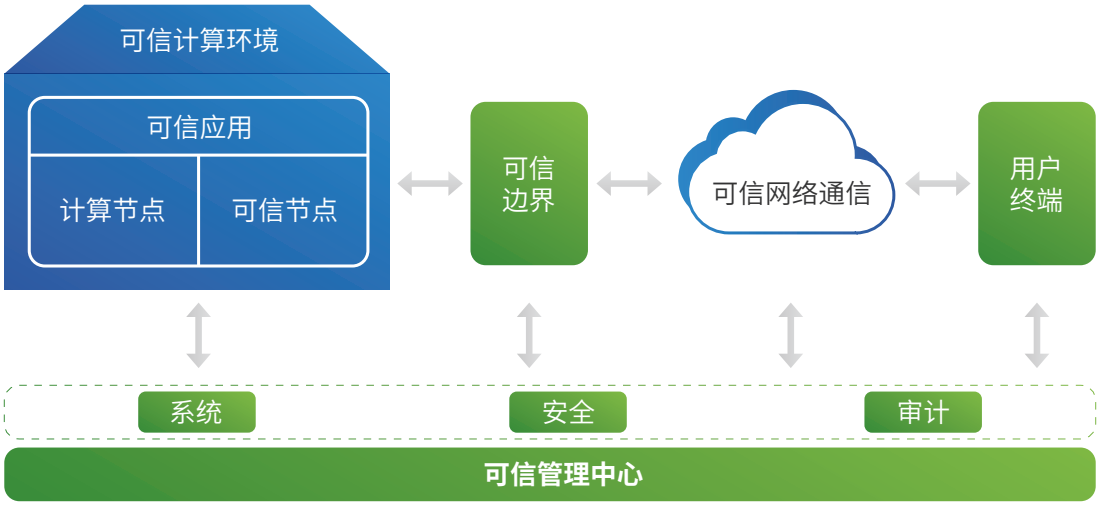
可信计算3.0技术体系架构

ARCHITECTURE

3.1 “一个中心三重防护”纵深防御体系

按照国家等级保护基本要求 (GB/T 25070-2019) 对安全框架的设计需求，信息系统从安全视角可被划分为安全计算环境、安全区域边界和安全通信网络三部分，三部分在安全管理中心的支撑下实现纵深防御体系。基于可信计算 3.0 技术的纵深防御体系，实现由可信管理中心支撑下的可信计算环境、可信区域边界、可信通信网络，使信息系统做到可信、可控、可管。

图3-1 可信管理中心支持下的主动免疫三重防护体系



（一）可信管理中心

可信管理中心实施对可信计算环境、可信区域边界和可信通信网络统一的管理，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）可信计算环境

计算环境是信息系统安全的核心与基础。可信计算环境通过在计算终端上构筑可信计算节点，利用可信计算节点的双体系架构下的主动安全能力形成严密的运行保护环境，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，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）可信区域边界

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，可信区域边界的设备本身也是可信计算节点，自身具备信任链，在可信机制的支撑下进行策略执行，确保不会有违背系统可信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）可信通信网络

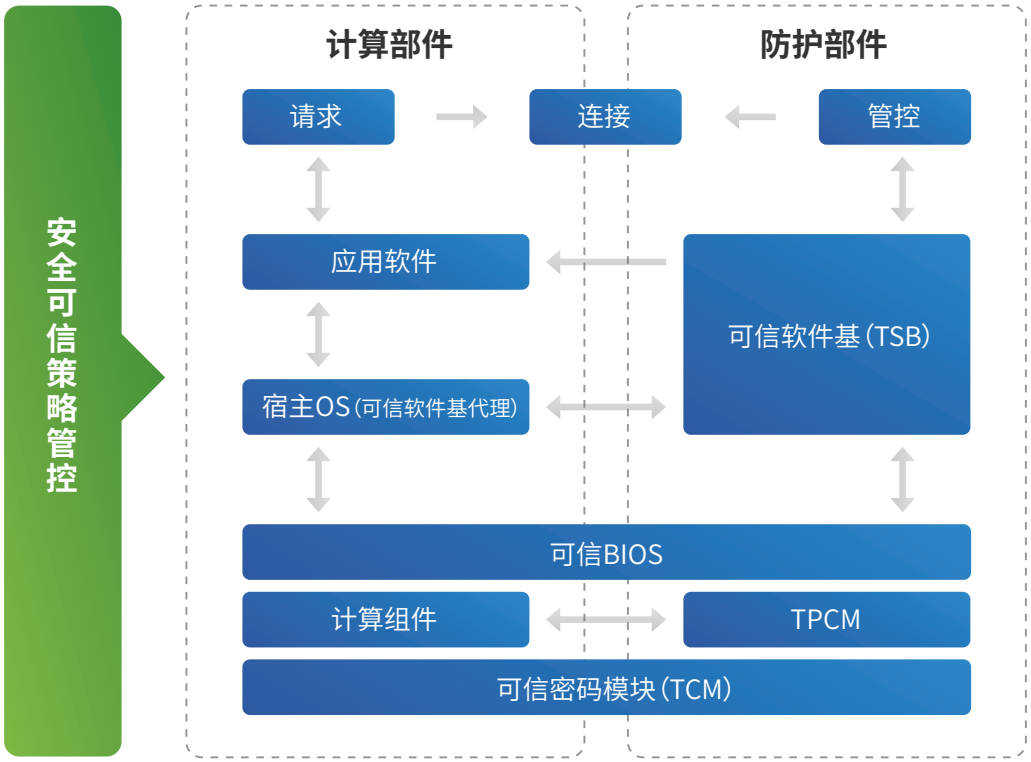
可信通信网络设备本身也是可信计算节点，在可信机制的支撑下通过对通信双方进行可信鉴别验证，建立安全通道，实施传输数据密码保护，确保其在传输过程中不会被窃听、篡改和破坏，是信息系统的第三道安全屏障。

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。

3.2 可信计算3.0双体系架构

可信计算 3.0 技术的纵深防御体系通过将计算环境、区域边界内的各计算节点打造为双体系架构的可信计算节点，实现可信计算环境、可信区域边界、可信通信网络。

图3-2 可信计算双体系架构



双体系架构下计算节点可被分为计算部件和防护部件两部分，计算部件与防护部件之间具有安全隔离机制，计算部件基于计算 CPU 或计算核实现业务逻辑，防护部件基于安全 CPU 或安全核建立一套防护系统，保障计算部件业务逻辑能够正常运行。如图 3-2 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计算部件的软硬件资源，在计算部件中可信软件基代理的配合下主动访问计算部件内资源，实现主动度量和主动控制等机制。

04 产品介绍

PRODUCT INTRODUCTION

“白细胞”可信主动免疫防御体系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，以可信计算 3.0 技术为核心，为信息系统基础运行环境、应用系统提供可信支撑，使应用信息系统拥有自免疫能力，抵御已知和未知威胁攻击。

4.1 产品列表

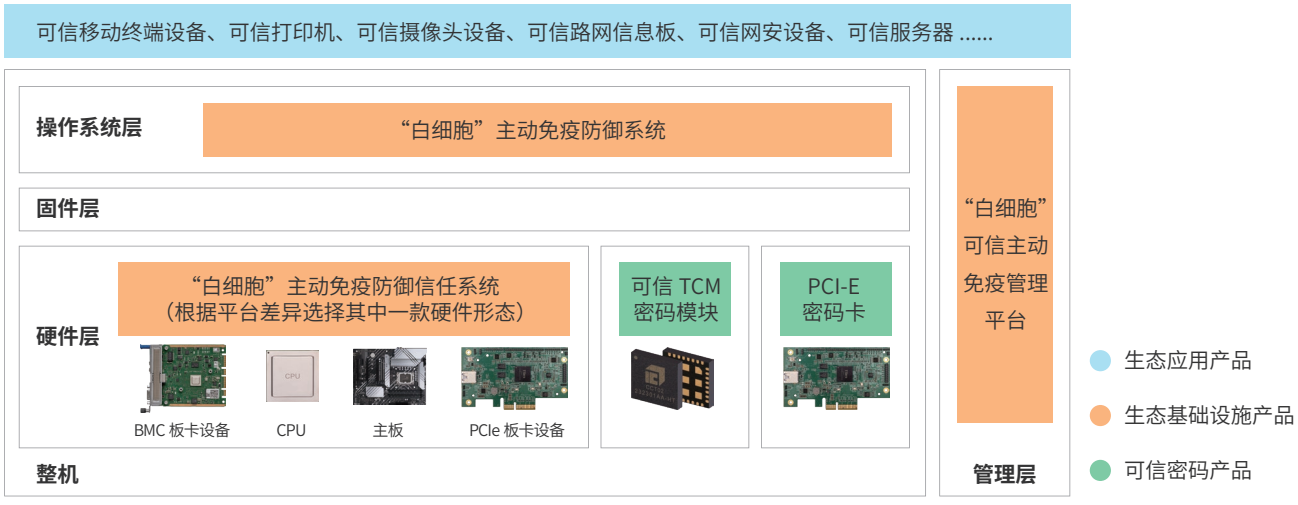
“白细胞”可信主动免疫防御体系产品主要有可信生态基础设施产品、生态应用产品、可信密码产品三个方向。

可信生态基础设施产品涵盖实现可信计算节点的相关生态产品。具体包括：“白细胞”主动免疫防御信任系统、“白细胞”主动免疫防御系统、“白细胞”可信主动免疫管理平台。其中“白细胞”主动免疫防御信任系统产品为硬件或硬件集成形式，部署后形成计算节点的防护部件。“白细胞”主动免疫防御系统在操作系统内集成，部署后形成计算部件下可信软件基代理，两个产品在双体系架构下实现防护能力。“白细胞”可信主动免疫管理平台作为管理部件，独立部署在网络内，实现对可信节点的统一管理，同时支撑可信网络连接等功能。

生态应用产品以可信生态产品支撑下所形成的行业可信应用设备为主，如可信移动终端、可信打印机设备、可信摄像头、可信路网情报系统等。

可信密码产品以支撑可信密码、标准密码运算的相关密码设备为主，包括可信 TCM 密码模块、PCI-E 密码卡。产品以独立板卡或芯片模组形式提供。

图4-1 产品组成



4.1.1 “白细胞”主动免疫防御信任系统

“白细胞”主动免疫防御信任系统依据《GB/T 40650-2021 信息安全技术 可信计算规范可信平台控制模块》、《GB/T 37935-2019 信息安全技术可信计算规范 可信软件基》等国家可信计算相关标准进行设计，是实现双体系架构中防护部件的核心组件，是可信终端设备的硬件可信根。支撑“白细胞”主动免疫防御系统构建可信终端设备主动免疫防御体系。主要功能及具体情况如下：

表4-1 主要功能列表

主要功能	详情
***支撑启动度量**	计算机上电启动后，优先启动可信根，之后逐级度量验证启动过程中各部件，构建信任链。功能可确保系统启动阶段的安全，可有效抵御针对固件、系统内核的攻击。
***支撑主动度量**	主动发起针对系统环境和业务程序运行状态的实时度量。确保关键信息不被非法更改，使系统、业务程序安全稳定运行。
支撑可信存储	提供安全存储区域，保障防护部件自身及相关策略数据的可信性。
支撑可信策略解析	可支持设备在线和离线场景下的可信策略解析，使系统适应不断变化的环境，及时应对复杂场景下的安全威胁。支持用户通过策略实现更高级别的安全需求。
实现各类安全机制	实现判定机制、控制机制、度量机制、支撑机制、协作机制、策略解释、可信基准库、基本信任基等功能，为“白细胞”主动免疫防御系统提供底层支撑。

标*功能部分产品不具备

“白细胞”主动免疫防御信任系统包含内置式、外置式和主板集成式三种产品形态。在实际构建部署时，可根据不同场景选择相应型号产品。

表4-2 可信平台控制模块（TPCM）产品形态

产品类型	产品形态	产品	产品详情		
			TPCM	TSB	TCM
内置式	BMC内置式产品	鲲鹏天池架构平台	●	●	—
	CPU内置式产品	飞腾CPU内置式产品系列	●	●	—/●
		海光CPU内置式产品系列	●	●	●
外置式	PCIe标准板卡式	KXHT T40P-TS	○	○	●
	PCIe非标准板卡式	KXHT T80S-TS	●	●	●
	M.2非标准板卡式	KXHT T80M-TS	●	●	●
主板集成式	电路板模组	KXHT T20H-S	○	○	●
	芯片模组	CCT02-LGA32	○	○	●
		CCT02-QFN40	○	○	●

注：● 表示产品具备该部件，且该部件为完全功能版本 ○ 表示产品具备该部件，该部件为非完全功能版本 — 表示产品不具备该部件

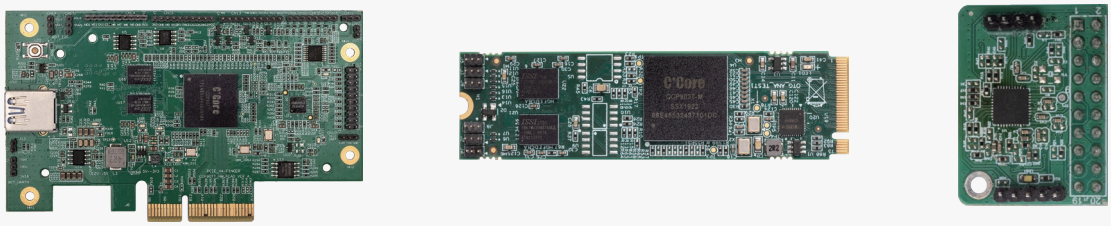
BMC 内置式产品目前仅适用于鲲鹏天池架构平台。BMC 管理系统为基板管理控制器，是通用服务器设备的重要组成部分。BMC 管理系统是一个独立的系统，常规情况下主要支撑服务器运维管理相关工作，它不依赖节点上的其他软件和硬件，优先上电，可以监控主机的状态，控制主机相关的功能。BMC 计算节点在硬件设计和功能设计上满足可信计算 3.0 双体系结构的隔离性要求。BMC 内置式产品利用 BMC 的主动访问控制能力，将其改造为双体系架构中的防护部件，实现基于 BMC 内置式 TPCM 及 TSB，完成对 BMC 业务部件的安全支撑，同时支撑服务器可信计算双体系架构。

CPU 内置式产品适配主流信创 CPU 厂商相关产品线。产品基于多核架构 CPU 中的一个或几个核作为安全计算核，依托多核架构资源隔离、安全交互机制、主动访问和控制能力，实现基于 CPU 内置式产品，完成对计算设备双体系架构的支撑。

外置式产品基于 PCIe 板卡板载独立计算、存储能力及 PCIe 通用总线 DMA 访问能力，完成对计算设备双体系架构的支撑。外置式产品分为 PCIe 标准板卡式和 PCIe 非标准板卡式，非标准式需要厂商根据参考设计修改主板，相较标准式具有更完善的功能，“白细胞”主动免疫防御信任系统运行早于计算环境 CPU 运行，可实现 BIOS 启动前的启动度量能力，提供更完整的可信链。

主板集成式分为电路板模组、芯片模组两种类型，均需要厂商根据参考设计修改主板并将产品集成至主板。由于总线速率原因，目前该类型产品暂不支持系统下的主动度量能力。

图4-2 外置式可信根图片



KXHT T80S-TS、KXHT T40P-TS、KXHT T80M-TS、KXHT T20H-S

4.1.2 “白细胞”主动免疫防御系统

“白细胞”主动免疫防御系统按照国家可信计算相关标准所规范的可信体系架构进行设计，部署于上层操作系统，在可信根的支撑下，建立可信终端设备的主动免疫防御体系。为可信终端设备提供系统、应用的安全可信防护功能。

*表4-3 可信软件基代理功能列表

主要功能	详情
静态度量	对应用程序进行白名单完整性检查，防止病毒、木马等未知恶意程序运行。
动态度量	可定期对运行环境进行检查，确保程序运行阶段的安全。
可信报告	依据启动情况、静态度量、动态度量、审计信息等可信状态信息生成可信报告，并定期上报终端安全状态；支撑用户或其他信息系统及时知晓终端的可信状态，避免安全风险。
自身防护	产品具备自保护能力，可防止安全机制被旁路，导致安全功能失效。
可信密钥	可信密钥基于可信根向用户提供符合国密要求的密码计算能力，支持多种密钥类型，能够覆盖用户业务场景的密钥应用。
可信存储	可信存储基于可信根的硬件安全存储区域，为用户提供证书、密钥、配置文件等敏感文件的安全存储空间，确保用户获得硬件级别的高安全存储空间。
可信连接	通过可信连接功能可将设备的可信状态扩展整个信息系统，确保非可信设备和可信状态异常的设备无法接入内部安全网络。
可信访问控制	根据策略配置实现系统内关键文件、关键目录、网络端口的访问权限，确保非法应用无法读取、破坏、盗窃系统内重要数据。支持用户在更复杂的场景下，通过策略实现更高级别的安全需求。

“白细胞”主动免疫防御系统产品支持麒麟、中科方德、凝思磐石、统信 UOS、EulerOS、CCLinux、RedHat、Centos、Ubuntu 等主流操作系统。

4.1.3 “白细胞”可信主动免疫管理平台

“白细胞”可信主动免疫管理平台按照国家可信计算相关标准所规范的可信体系架构进行设计，基于“一个中心，三重防护”的防护理念，实现对部署了“白细胞”主动免疫防御系统的可信终端设备的统一管理。“白细胞”可信主动免疫管理平台支持以一体机形式进行部署或以软件形态部署于可信计算节点，可以支撑可信终端设备间可信连接的建立，是网络可信安全体系的关键基础设施，可实现用户对全局的可视、可管、可控，保障终端系统安全稳定的运行。

可信安全管理中心一体机内部集成“白细胞”主动免疫防御信任系统及“白细胞”主动免疫防御系统，具备完整的可信安全防护能力。

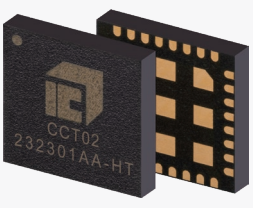
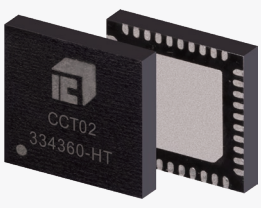
表4-4 可信安全管理中心功能列表

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。通过“三权分立”的管理模式，使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	存储维护业务网络中可信设备的基准库，具备存储和配置基准的功能，“白细胞”主动免疫防御系统依据该基准进行可信验证；向用户提供相较终端更权威的可信状态判定结果。
策略管理	进行可信策略的制定、下发、维护和存储等，可信策略包括启动度量、静态度量、动态度量、访问控制、可信连接、业务进程执行保护等。提供策略配置、支持策略的批量下发和指定可信终端设备下发。
平台管理	支持设置可信终端设备的全局策略，启动度量、启动度量控制、动态度量、静态度量的开关等，便于用户更灵活的使用。
软件管理	“白细胞”可信主动免疫管理平台提供对采集基准后的软件包进行集中存储并提供推送服务，可向用户提供便捷的软件下载。
资产管理	可查看网络中的可信设备信息，包括 可信设备名称、IP、操作系统类型、操作系统版本、处理器架构、在线 / 离线状态等，支持用户对可信设备名称搜索，可信设备信息查看。
可信连接	配置可信连接相关策略，支撑用户利用“白细胞”可信主动免疫管理平台的统一管理能力，通过可信连接功能可将设备的可信状态扩展整个信息系统，确保非可信设备和可信状态异常的设备无法接入内部安全网络。
可信验证	支持查看可信终端设备的 TPCM、TCM 等信息，提供可信终端设备可信报告、启动度量、动态度量等策略及结果的查询，确保接入的可信终端设备真实可信，向用户及内网信息系统提供可信状态的查看能力。
审计管理	支持对可信终端设备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，可以监督和追踪系统及用户的行为，记录所有数据处理和访问活动 , 确保运行数据及管理操作可追溯。
部署模式	支持负载均衡模式和双机热备模式部署，可靠性高。

4.1.4 可信TCM密码模块

可信 TCM 密码模块符合 GM/T 0012-2020《可信计算可信密码模块接口规范》、GM/T 0028-2014《密码模块安全技术要求》和 GM/T0008-2012《安全芯片密码检测准则》的检测规范。可信 TCM 密码模块可作为防护部件核心组件，为可信平台控制模块（TPCM）提供可信密码服务；也可作为独立模块，支撑可信计算密码支撑平台实现安全功能。产品具有低功耗、高性能、多功能及高安全性等特点。产品内置高等级安全特性的硬件算法协处理器，支持国家商用密码算法及国际标准算法。支持工业级温度范围（-40℃～ 85℃），可用于苛刻的工业环境。产品规格如下：

表4-5 可信密码模块TCM产品规格

产品型号	CCT02-LGA32	CCT02-QFN40
CPU	C*CORE C0	
主频	100MHz	
尺寸	5*5MM	
工作温度	-40℃～85℃	
工作电压	1.8V~3.3V	
典型功耗	25mA@100MHz	
低功耗	2uA	
ESD	2KV	
接口	SPI	
存储保护机制	存储加密，总线加扰	
物理防攻击	支持	
安全检测与防护单元	TD/VD/FD/AD等	
随机数	GM/T 0005-2012真随机数标准 FIPS 140-S标准	
算法性能	SM2签名：6.6ms/次 SM3：46.5MB/S SM4加密（ECB）：24.3MB/S	
密码资质	国家商用密码可信模块产品认证证书	
封装		

4.1.5 PCI-E密码卡

产品遵循国家密码局发布的《GM/T 0018-2023 密码设备应用接口规范》《GM/T 0028-2014 密码模块安全技术要求》标准，可为各类安全平台提供多线程、多进程和多卡并行处理的高速密码运算服务，满足其对数字签名 / 验证、非对称 / 对称加解密、数据完整性校验、真随机数生成、密钥生成和管理等功能的要求，保证敏感数据的机密性、真实性、完整性和抗抵赖性。

4.1.6 可信生态产品

可信生态产品是可信华泰支撑生态厂商形成的大量具备可信能力，符合双体系架构的合作产品。目前已经应用的包括：可信移动终端设备、可信打印机、可信执法记录仪、可信摄像头设备、可信路网信息板、可信网安设备、可信服务器。

图4-3 部分生态产品图

图4-4 华为可信服务器兼容性认证证书

05 实施部署

IMPLEMENT DEPLOY

可信主动免疫防御体系需部署系列产品。

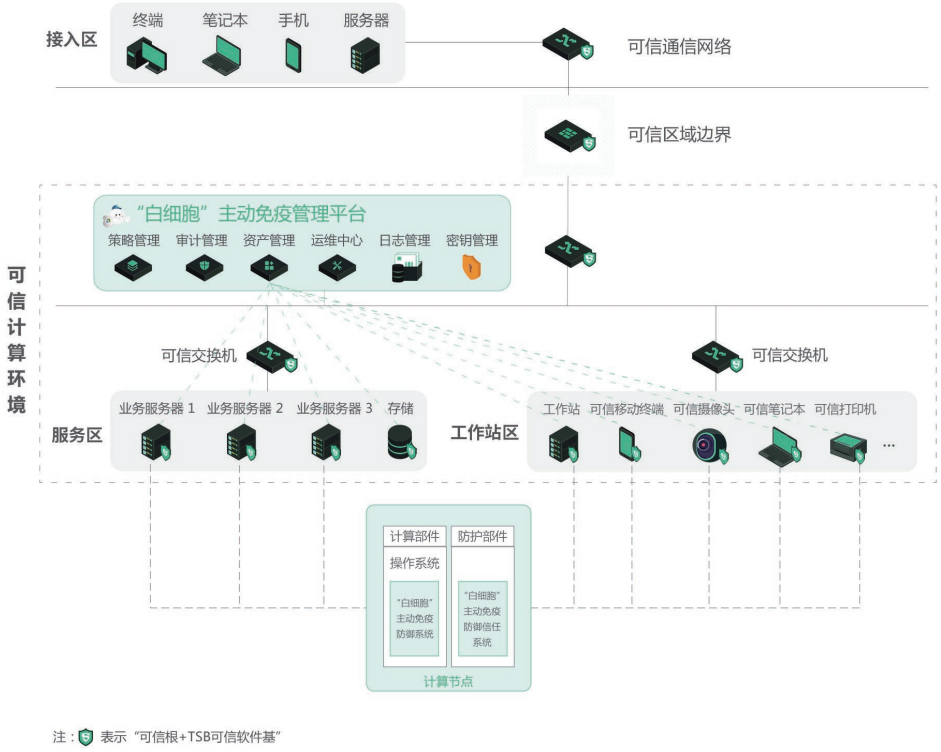
首先，基础硬件平台需集成“白细胞”主动免疫防御信任系统，对于新建系统建议采用 BMC 等内置式“白细胞”主动免疫防御信任系统产品。对于现有信息系统可根据需求选用“白细胞”主动免疫防御信任系统相应类型产品。

其次，在设备操作系统下部署“白细胞”主动免疫防御系统，也可选用已经集成“白细胞”主动免疫防御系统的操作系统进行安装。

最后，在局域网内安全管理域中部署“白细胞”可信主动免疫管理平台，可采用一体机方式部署或软件部署，要确保网络可达。

对于生态应用产品等可信应用设备，如可信移动终端、可信打印机设备、可信摄像头等都可直接接入网络由“白细胞”可信主动免疫管理平台进行统一管理。

图5-1 部署网络图例



注：表示“可信根+TSB可信软件基”

06

产品优势/技术亮点

ADVANTAGES / HIGHLIGHTS

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，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，依据策略保护业务程序，阻止非授权及非预期的执行程序运行，实现对已知或未知恶意代码的主动防御。

6.3 策略化支持多场景的精准安全防护

符合用户真实场景应用，提供多种策略配置方式有效降低用户安全配置难度，最大程度上让可信策略贴近系统的实际情况符合业务实际需求，提高安全性的同时，降低管理工作难度。

支持基于策略语言描述更复杂的策略场景，实现对复杂场景的防护构建高等级的主动防御体系。

6.4 基于可信管理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 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，有效满足用户合规需求的同时切实保障信息系统安全性。

07

重点应用案例介绍

KEY CASES

“白细胞”可信主动免疫防御系列产品拥有自主知识产权，已完成在重要领域、重点行业的示范应用和推广，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。

7.1 典型案例

7.1.1 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，通过选择“白细胞”主动免疫防御信任系统 CPU 内置型产品，并配套使用“白细胞”主动免疫防御系统，建立形成系统主动免疫防御能力。

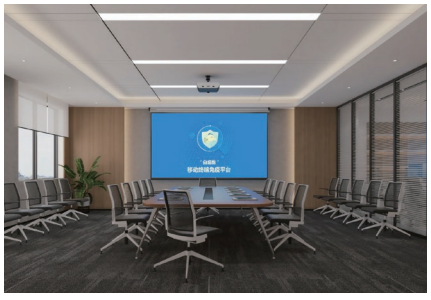
方案和价值

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部署产品，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。项目在长城服务器（飞腾 2000 CPU、麒麟操作系统）中选择“白细胞”主动免疫防御信任系统 CPU 内置型产品，在服务器上部署“白细胞”主动免疫防御系统（基于麒麟操作系统），为设备建立完整无缝信任链，符合了等级保护 2.0 标准中对计算环境的可信验证相关要求。

产品在实际应用中不仅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。

行业图例

图7-1 政企行业图例



7.1.2 国家电网电力生产调度系统主动免疫防护应用案例

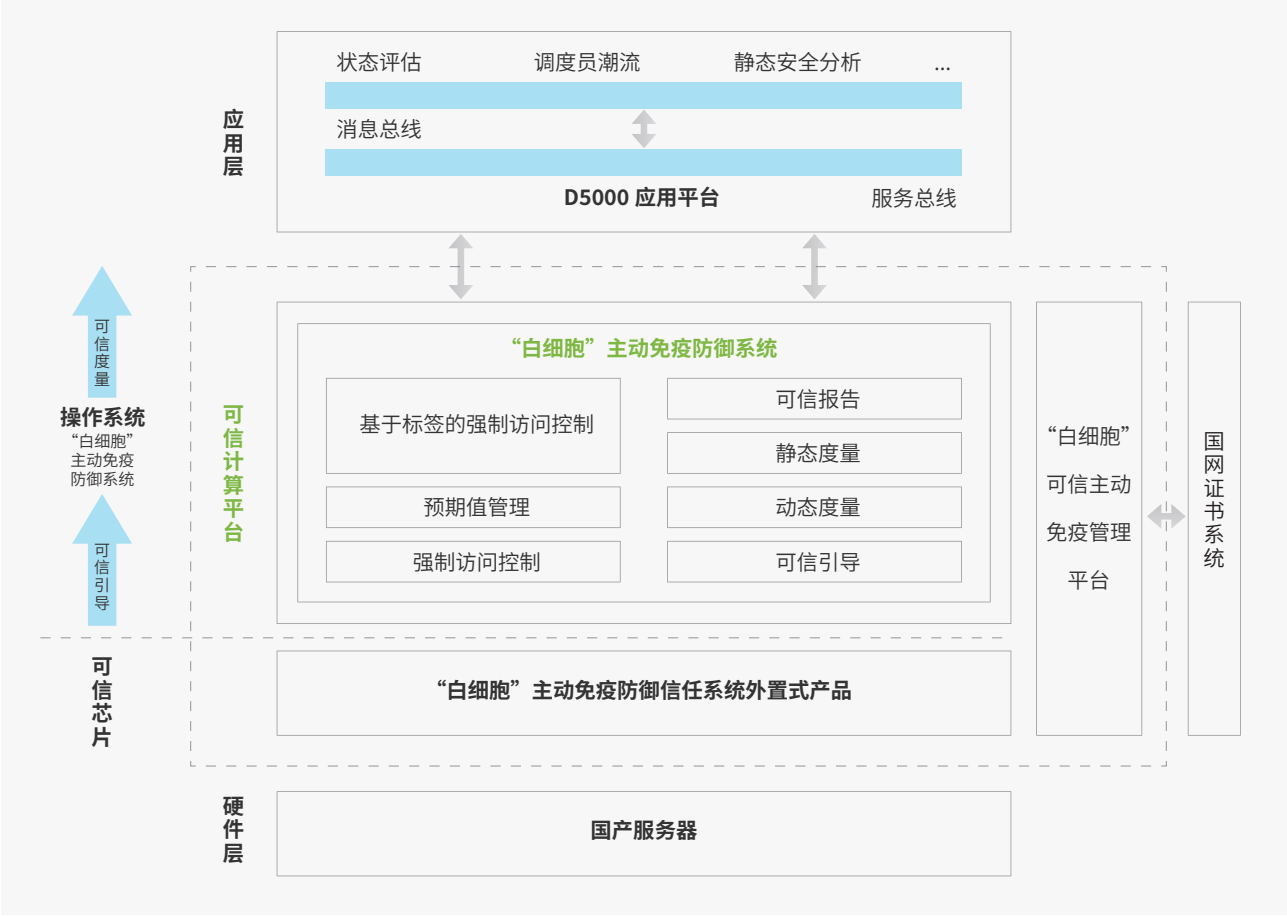
背景和需求

针对国家电网电力生产调度系统高安全系统防护需求，方案采用可信计算 3.0 技术体系，在新一代电力调度系统中通过部署“白细胞”主动免疫防御信任系统外置式产品、“白细胞”主动免疫防御系统及可信主动免疫管理平台建立电力生产调度系统主动免疫防御能力，实现电调系统基础设施安全，使国家电力调度系统达到国家等级保护四级的安全要求。

方案和价值

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。可信华泰通过相关产品的部署实现智能电网电力调度控制系统对恶意代码的主动防御能力，保障系统稳定和可靠的运行。

图7-2 国家电网电力调度系统可信加固方案



行业图例

图7-3 电力行业图例

扫描二维码关注
可信华泰

北京可信华泰信息技术有限公司

公司地址：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

公司网站：www.httc.com.cn

联系电话：010-88894996