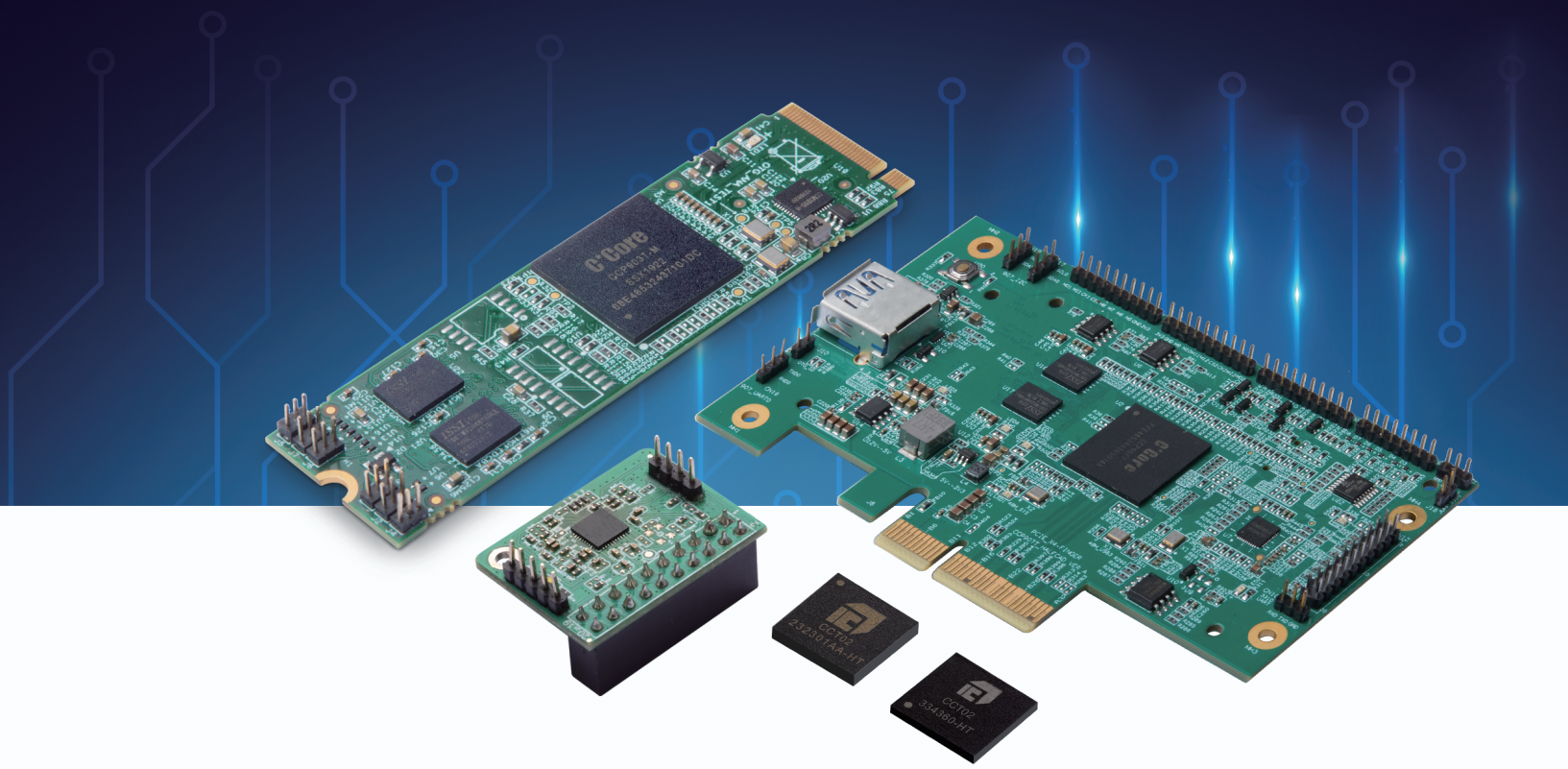
可信华泰



“白细胞”主动免疫防御信任系统

产品介绍
Product Introduction

“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。

“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。具体产品如下：

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

产品功能 Product Function

- 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。系统支持用户通过策略实现更高级别的安全需求。
- 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。

产品优势 Product Advantage

- 可信 3.0 技术具备完整的信任链，可确保防护机制自身安全，能够阻挡已知、未知恶意代码威胁，有效抵御 0 DAY 威胁和勒索病毒威胁，可对计算环境安全威胁提前预警和处理；
- 可信 3.0 技术的主动防护能力可提供超越操作系统权限级别的安全防护；
- 可信功能执行主体及策略受硬件形态的可信根保护，具备更高安全性；
- 可信 3.0 技术可向用户提供更多基于安全硬件的能力扩展；
- 外置式产品硬件具备高计算性能，产品采用多级高速流水线并行方案，主机与设备之间使用高效的直接存储器访问通信方式。
- 可信 3.0 技术满足等保 2.0、关键基础设施条例中对可信相关功能的要求。

独立硬件产品参数 Hardware Product Parameter

产品型号	芯片模组		电路板模组	M.2非标准板卡式	PCIe标准板卡式	PCIe非标准板卡式
	CCT02-LGA32	CCT02-QFN40	KXHT T20H-S	KXHT T80M-TS	KXHT T40P-TS	KXHT T80S-TS
接口	SPI	SPI	非标准	M.2	PCIe	PCIe和SPI
尺寸	5*5MM	5*5MM	27*20MM	22*80MM	64*114MM	64*114MM
功耗	≤1W	≤1W	≤1W	≤4W	≤4W	≤4W
工作温度	0~70°C	0~70°C	0~70°C	0~70°C	0~70°C	0~70°C
密码资质	国家商用密码可信模块产品认证证书					

立即了解更多内容：
公司网站：www.httc.com.cn
联系方式：010-88894990

印刷日期：2024.10

可信华泰