KYLINSOFT
麒麟软件

银河麒麟桌面操作系统 V11 2603

产品白皮书

麒麟软件有限公司（2025 年 11 月）

商标声明

KYLINSOFT 麒麟软件和其他麒麟商标均为麒麟软件有限公司的商标。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受麒麟软件有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，麒麟软件有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容有可能变更，麒麟软件有限公司保留在没有任何通知或提示的情况下对内容进行修改的权利。除非另有约定，本文档仅作为使用指导，并不确保手册内容完全没有错误。本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

麒麟软件有限公司

地址：天津市滨海新区塘沽海洋高新区海缘东路信安创业广场 3 号楼麒麟大厦
网址：https://www.kylinos.cn

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障	**危险** 重置操作将丢失用户配置数据
警告	该类警示信息可能会导致系统重大变更甚至故障	**警告** 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息，补充说明等，是用户必须了解的内容。	**注意** 权重设置为 0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	**说明** 您也可以通过 Ctrl+A 选中全部文件。
-->>	多级菜单递进。	单击**设置-->>网络-->>设置网络类型**。
粗体	表示按键、菜单、页面名称等 UI 元素。	在**结果确认**页面，单击**确定**。
Courier 字体段落	整段命令或代码。	NAME="Kylin OS" VERSION="V10 (Spider)"
Courier 字体	命令或代码。	执行 cd /etc 命令，进入 etc 目录
斜体	表示参数、变量。	*Instance_ID*

目 录

1 概述

银河麒麟桌面 V11 是一款面向桌面应用的图形化操作系统，桌面环境 UI 风格调整、系统功能、安全、应用等易用性获得极大体验提升。

银河麒麟操作系统 V11 定义了全新的架构，即磐石架构，以不可变核心系统为基石，结合面向历史的 KARE 兼容环境，面向未来的开明运行环境而构成。以不可变形式存在的核心系统为用户提供更加稳定、安全和高效的不可变系统架构，提高系统的安全性和稳定性，简化系统管理，使更新、备份、回滚更快速高效，做到“千人一面”。

增加 AI 能力，提供极致的智能好用体验，增强智能内容搜索，既支持根据文件名称检索，也支持根据文件内容检索；文件动态聚合，文件管理高效智能，支持百窗同开；通过 OCR 技术实现在复制粘贴过程中的文转图、图转文；全场景快速记录灵感与会议要点，智能整理繁杂内容、提炼核心，实时语音转写，会议内容全记录，提升工作效率。技术上，结合 MCP 能力实现从“理解”到“执行”的跨越。它不仅能理解你的指令，还能直接操控本地文件与系统工具，甚至联动第三方专业软件，将复杂操作化为一步直达。MCP 赋予 AI 从理解到执行的能力，让它真正成为可思考、可执行的桌面智能助手。

全域可控的安全，实时监测风险、早预警、快响应，确保全链路安全无隙。天御安全域管平台是一款面向企业的高效安全管理平台，专注于提升企业管理效率和安全管控能力。平台聚焦人员管理、设备管理、应用与资源管理、安全管理四大核心场景，打造从身份认证、权限控制、策略执行到审计记录与安全响应的全流程统一管控体系，为企业提供全面、安全、可靠的管理支撑。技术上，KSAF 是创新型突破传统操作系统安全框架，以极简的安全策略语言构建复杂安全功能，轻量开发即可满足复杂安全需求，覆盖全场景主客体与权限控制，全新打造的可控、可信、可扩展的新一代安全框架。

原生开放的生态，全新开明包格式及丰富配套工具，根植系统，底层适配，提供系统级开发稳定体验，兼容性检测、开发部署全方位支撑，化繁为简，排忧解难，辅助开发插件高效协作，让原生开发更简单。可以在不同版本的 Linux 系统中保证软件运行所需要的环境，解决了软件生态针对多个发行版需要多次适配的问题，当系统升级时也无需再重建 或兼容各类软件。开明通过沙箱隔离，让应用软件不依

赖子系统就可以独立运行。这一策略避免了恶意代码对用户隐私数据的访问和对宿主机的破坏，用户可以放心运行各类软件，无需担心数据泄露等安全问题。通过解决兼容性问题，为系统管理员和用户节约了大量时间和精力。系统管理员无 需花费大量时间、资源去适配应用，可以专注于系统升级的主业务，从而降低了系统的维护 成本。同时，用户也可以更加专注于他们的核心业务，无需担心因系统升级导致软件受到影响，提高工作效率。

2 架构

2.1 磐石架构技术

随着个人电脑用户对系统响应速度、安全性和个性化体验的要求日益提高，传统的 Linux 桌面发行版面临着新的挑战：如何更好地实现应用与系统的解耦，以简化更新流程、增强系统稳定性，并提供更加流畅且一致的用户体验。正是基于这样的背景，“磐石架构”应运而生。

磐石架构是围绕“不可变系统”为核心，衍生出来配合“不可变系统”进行用户操作习惯、应用生态保持与演化的一系列技术组合的架构，也可称为磐石系统。

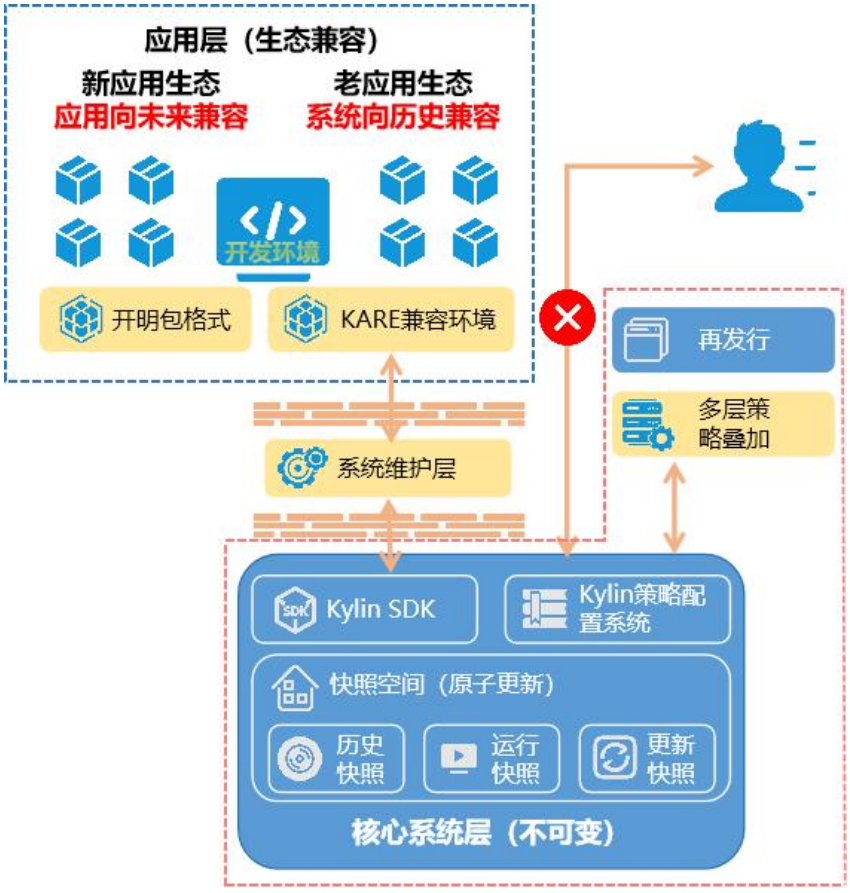

图 1 磐石架构

从系统分层角度来看，系统整体分为三层，从下向上分别是核心系统层、系统维护层、应用及生态兼容层。

为用户提供更加稳定、安全和高效的不可变系统架构，提高系统的安全性和稳

定性，简化系统管理。其内容在运行状态下是固定的、不可被用户及应用程序变更，做到“千人一面”。核心系统层是桌面操作系统最小组成部分，涵盖了传统架构的 Linux 内核、运行时库、系统服务、开发框架、桌面环境。

系统维护层是记录运维人员、高级用户在核心系统外部对核心系统修改的逻辑层。由于核心系统不可变更，因此在调试、运维过程中需要对核心系统做修改都由该层负责接纳，不直接修改核心系统。

应用层直接面向用户，为用户提供业务能力。在应用层，提供两套应用安装方案：KARE 兼容环境和开明运行环境。KARE 用于为生态提供面向历史的兼容能力；开明运行环境是新一代软件包格式开明格式的运行环境，为生态提供面向未来的兼容能力。对于历史上已有的生态软件包，安装在 KARE 中，使用开明包格式打包的应用可以直接运行在未来的桌面系统中。

2.2 开明包技术

开明是一种新型软件包格式。它旨在解决传统包格式存在的系统与应用无明确界限、发行版碎片化、兼容性等问题，从而为软件提供高兼容性、高安全性的功能。开明通过在沙箱环境中构建应用，确保软件不受宿主机操作系统的影响，避免因系统升级等问题需重建或兼容运行各类应用。开明通过对沙箱内应用实施细粒度权限管控，以保护用户宿主机的数据安全。

- **跨版本兼容性**

开明通过构建容器机制，可以在不同版本的 Linux 系统中保证软件运行所需要的环境。这一功能解决了软件生态针对多个发行版需要多次适配的问题，当系统升级时也无需重建或兼容各类软件。

- **隐私安全保护**

开明通过沙箱隔离，让应用软件可以独立运行。这一策略避免了恶意代码对用户隐私数据的访问和对宿主机的破坏，用户可以放心运行各类软件，无需担心数据泄露等安全问题。

- **权限管控**

开明通过提供细粒度权限管控，让用户可独立配置开明应用的资源权限管控。这一功能提高了软件的可扩展性、合规性和安全性。

- **提升系统与软件运行稳定性**

开明实现软件运行隔离，软件安装运行不会对宿主系统环境进行修改，提升系统运行稳定性；系统升级不会对软件依赖进行版本改动，提升软件运行稳定性。

● **降低维护成本**

开明通过解决兼容性问题，为系统管理员和用户节约了大量时间和精力。系统管理员无需花费大量时间、资源去适配应用，可以专注于系统升级的主业务，从而降低了系统的维护成本。同时，用户也可以更加专注于他们的核心业务，无需担心因系统升级导致软件受到影响，提高工作效率。

● **deb 转开明**

针对开明软件生态刚起步、生态软件较少的问题,开明提供了 deb 转开明工具，可实现 deb 包到开明包的转换，达到 deb 生态复用效果，降低生态扩充人员编包成本，提升开明生态扩充速度。

2.3 KSAF 安全技术架构

实现 KSAF 可编程动态多策略融合框架和麒麟安全策略语言（KSL），打造下一代安全体系 KSAF2.0，突破传统的访问控制策略机制，能够实现对更全面对象和操作行为进行管控，并通过语言定义软件行为和安全管理，达到软件定义安全的目标，满足多种威胁场景快速响应用户的安全需求，提供高效、稳定、可靠的安全基座。

●可编程安全框架模型：五层安全架构，0 层为安全实施层，1 层为安全决策层，2 层为安全语言层，3 层为安全定义层，4 层为安全交互层，其中 0-2 层实现安全框架，实现稳定的安全基座，3-4 层定义安全功能，基于可编程安全框架灵活进行扩展安全堆栈化，支持更全面的安全管控对象和操作行为客体类别；

●主体身份确认机制： 研究进程/线程主体的身份确定机制，构建系统主体身份模型，并基于进程在进程组、会话组等原生关系，识别内核主体身份，建立安全上下文信息，可有效体现进程的继承关系与转换关系，能够识别不同的编程场景：容器、沙箱、脚本等；

●多元客体身份机制： 研究客体复合身份标记，实现目录嵌套身份的识别，实现动态数据的身份建立和恢复；

●混合语言编程机制：研究利用 C、Python 等通用高级语言本身具备的完备性，来实现约束条件函数的定义。将安全语言与通用高级语言结合，实现安全通用程序设计语言。实现安全语言，即能够表达计算所有图灵可计算安全函数的算法。只要一个安全问题是可以判定的，它的计算过程可以通过符号和算法表达出来；

●动态变量赋值机制：研究安全机制运行态实时动态变量赋值，实现基本类型和复合结构类型的支持编译与策略下发分类；

●内核脚本行为解析：研究解释性语言在内核中的行为，探测脚本管道运行与实际脚本文件的对应关系。

功能及技术架构

KSAF 安全框架从整体上为整个操作系统提供了全方位的安全机制和策略语言支撑，从底层内核开始，向上依次提供了安全实施、安全决策、安全语言、安全定义和安全交互等五个层次。一方面满足了灵活多变的安全需求，另一方面提供了高效的安全功能开发过程。如下图所示：

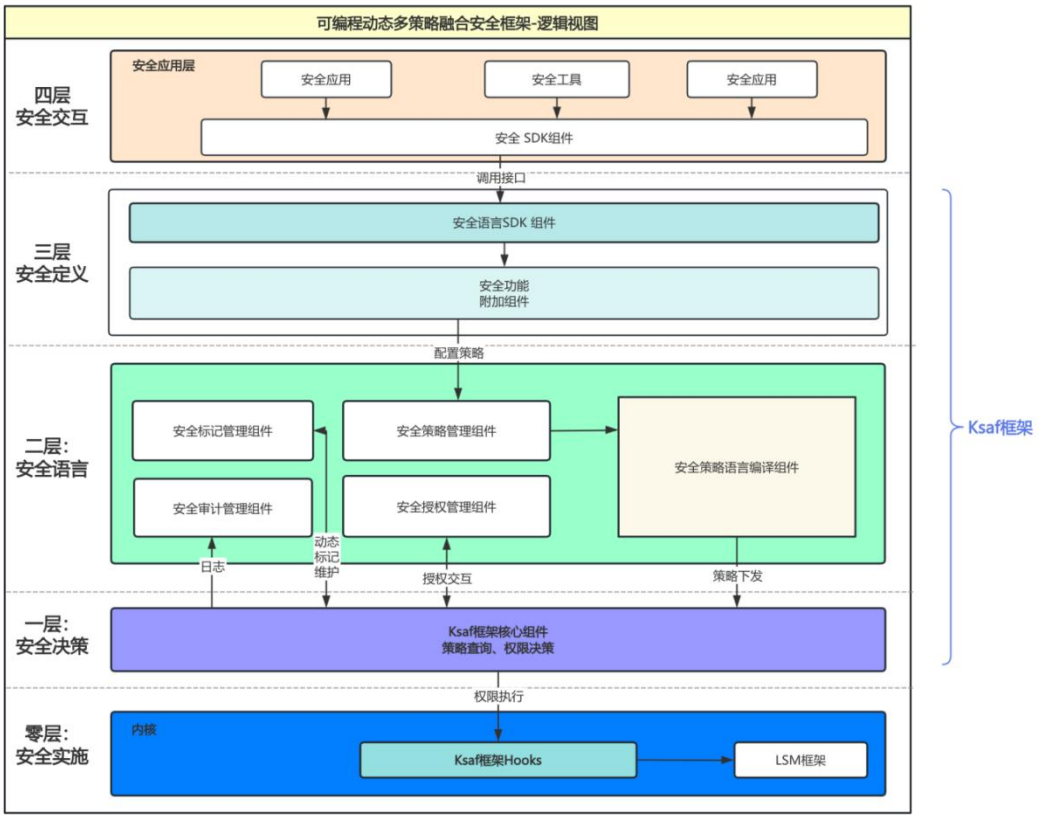

图 2 ksaf 逻辑架构图

2.4 WLCOM 技术架构

WLCOM 是一款基于 wlroots 的 Wayland 合成器，以实现高性能、高安全、易维护为目标，具有渲染性能高、安全性高、生态兼容好、功能可灵活定制、第三方依赖少等技术特性。

● 渲染性能高

在性能上消除了原始窗口管理器的交互开销，同时支持多卡、多输出、多并发渲染加速接口，在不启用动画和装饰性渲染的情况下，渲染后端既支持纯 CPU 绘制，

也支持 OpenGL/ES、Vulkan，大幅提升业务场景渲染能力。

- **X 兼容性好**

目前国内主流应用还处于由 X 显示框架向 wayland 显示框架切换的过渡阶段，特殊 X 接口转换的缺失，导致 X 应用部分功能异常，自研 X 兼容增强插件，通过桥接转换协议打通特殊 X 接口到合成器通路，实现 X 应用广泛兼容。

- **安全性高**

新增 wayland 下防截屏安全协议，支持用户指定窗口防截屏及全屏防截屏，实现对截图内容、区域进行管控，对敏感数据强化保护，并提供 Qt 下防截屏设置接口，方便第三方软件使用等，满足多领域的场景安全需求。

- **功能可定制**

通过整体设计架构改造，解耦系统关联组件，实现插件式框架结构，全插件式管理，支持功能组件灵活裁剪、按需定制，功能实现更高效。

- **第三方依赖少**

既不依赖 KDE、GNOME 等成熟桌面环境，也不依赖 QT、GTK 等 UI 工具包，仅依赖 pixman、libdrm、xkbcommon 等基础库。

2.5 AI PC 技术架构

与传统操作系统不同，AI PC-OS 需要支持 AI 算力芯片、大模型及 AI 应用，因此它是一款面向 AI 设计的桌面操作系统。AI PC-OS 产品拥有本地部署的大模型与个性化本地知识库组合构成的个人大模型，第一交互入口为个人智能体，可实现自然语言交互，AI PC-OS 将通过内嵌 AI 计算单元的方式提供混合 AI 算力，还可以依靠开放生态来满足不同场景的需求。在满足生产力提升的同时，通过本地数据存储和隐私及数据保护协议来保护个人隐私和数据安全。

应用交互层

AI Agent，基于 AI 面向自然语言的新型人机交互，紧跟新人机交互带来的桌面 OS 变革，构建面向 AI 的软件生态体系。传统的终端在交互模式上有着较大的限制。早期的终端设备需要依靠硬件外设才能实现人机信息的传递。图形化操作系统出现后，交互效率实现提升，但可视化程序交互也涉及复杂的菜单和功能操作，有较高的学习成本。而 AI 操作系统能够做到自然语言交互，允许用户以口头或文字形式使用自然语言与操作系统进行沟通，并通过自然语言的方式给予用户反馈，这种交互方式更自然、更直观，更贴近人类沟通本能，替代了复杂繁琐的指令语言。

自然语言交互 UI 的能力主要依赖于常驻其中的 AI Agent（个人智能体），其承担着对用户的意图进行理解与分发任务的重要作用。AI Agent 基于内嵌于终端的本地大模型而打造，当收到用户请求后，本地大模型会精准理解用户意图，并将意图转换为相应的任务组合，分解任务并识别任务完成的路径，从而进一步查询本地知识库、调用设备 API、调用合适的模型或应用来执行相应的任务。设备、模型或应用执行完成任务后，会将相应的结果返回给智能体，智能体完成整合后再反馈给用户。

系统架构层

系统性构建桌面操作系统的 AI 子系统：操作系统架构支持端侧本地 AI 模型推理、统一 AI SDK、云端一体化混合 AI 等能力，桌面操作系统底层能力和架构全面融入 AI 特性。

硬件适配层

构建 AI HAL，兼容各 CPU 架构和 xPU AI 算力芯片，构建 AI PC 硬件生态体系。对 AI PC 涉及的 CPU、GPU、NPU 和云端 AI 算力适配和优化，结合 AI PC 硬件形态面向办公场景提升优化 OS 的 AI 交互体验和工作效率。

3 硬件支持

处理器支持

●麒麟软件与飞腾、龙芯、海光、兆芯、申威等国内主流 CPU 厂商达成良好合作，支持飞腾 D3000M、飞腾 D3000、飞腾 D2000、飞腾 FT-2000/4；龙芯 3A6000 系列、龙芯 3A5000 系列、2K3000、3B6000M；海光 2 号、海光 C86-3G、海光 C86-4G；兆芯开先系列（KX-7000 系列、KX-6000G、KX-6000 系列、KX-5000）、兆芯开胜 KH-40000 系列；申威 SW-831，同时，支持 Intel 和 AMD 等国际厂商的主流处理器，并和厂商深入合作，共同优化，充分发挥其性能。

显卡支持

●麒麟软件与景美、风华创智、摩尔线程、格兰菲、凌久微、芯瞳、象帝先等国内主流 GPU 厂商达成良好合作，支持景美 JM92 系列、JM11；风华 2 号、摩尔线程 S10/S30/S50、X100、X300、格兰菲 Arise-1020、Arise-2030、Arise-GT-10C0t、凌久微 GP201/GP202/GP200S、芯瞳 CQ2040、GB2062、GB2064、象帝先天钧一号、天钧二号等，同时，支持 NVIDIA 和 AMD 等国际厂商的主流显卡。和厂商深入合作，共同优化，充分发挥其性能。

AI 芯片支持

支持格兰菲、芯动力、后摩智能、摩尔线程、此芯、爱芯元智、昇腾、海飞科、天数、沐曦、海光、Intel、AMD 及 NVIDIA 系列 AI 芯片。针对每款 AI 芯片进行了深度优化，在保持系统稳定性的同时充分发挥硬件计算性能，并针对科学计算、AI 推理等典型应用场景进行加速调优，确保在异构计算环境中的卓越表现。

整机支持

银河麒麟桌面 V11 支持大多数基于国产处理器平台的整机，麒麟软件与长城、联想开天、华为、软通计算机、紫光计算机、中科可控、浪潮计算机、江苏七零六、宝德、海康、雷神等整机厂商建立了良好合作。

4 运行环境

4.1 最低配置要求

处理器	ARM64：飞腾 FT-2000/4、飞腾 D2000、鲲鹏 920 X86_64：兆芯开先系列（ZX-C、ZX-C+、KX-5000、KX-6000）、海光 2 号、Intel/AMD 主流在售 CPU 其他：如需使用 AI 子系统及本地模型，需要配备高性能处理器
内存	4GB
存储	建议 128GB 或更大的存储设备 其他：如需使用 AI 子系统及本地模型，需要配备高性能处理器
系统固件	UEFI 安全启动、Legacy BIOS
TPM	支持 TPM2.0
显卡	支持 OpenGL 4.6，支持 OpenCL 2.0(ROCm)、支持 OpenCL 1.1 规范推荐的 GL/CL 互操作接口
显示器	分辨率 1024*768 以上的显示屏

表 1 银河麒麟桌面操作系统最低配置要求

4.2 推荐的配置要求

处理器	ARM64：飞腾 FT-2000/4、飞腾 D2000、飞腾 D3000、鲲鹏 920 Loogarch64：龙芯 3A5000、龙芯 3A6000

	X86_64：兆芯开先系列（ZX-C、ZX-C+、KX-5000、KX-6000、KX-7000）、海光 C86-3G、海光 C86-4G、Intel/AMD 最新在售 CPU
内存	8GB
存储	固态硬盘 512G 其他：如需使用 AI 子系统及本地模型，需要预留 6G 以上存储空间
系统固件	UEFI 安全启动、Legacy BIOS
TPM	支持 TPM2.0
显卡	支持 OpenGL 4.6，支持 OpenCL 2.0(ROCm)、支持 OpenCL 1.1 规范推荐的 GL/CL 互操作接口
显示器	分辨率 1920*1080 以上的显示屏 支持 4K 分辨率以上的显示屏

表 2 银河麒麟桌面操作系统推荐的配置要求

5 内核特性增强

银河麒麟桌面操作系统 V11 基于全新的社区 LTS 6.6 内核开发。银河麒麟桌面操作系统 V11 2603 内核集成了多个自研内核特性、特别是对于内存管理、电源管理、硬件协议、虚拟化和安全模块等核心模块进行了全方位提升，同时吸收上游社区、 openEuler 社区、ubuntu 社区等多个主流内核社区的优秀成果。

除了功能特性，银河麒麟桌面操作系统 V11 2603 在生态兼容方面也做了全面适配，包括国内外主流 CPU、整机板卡等。内核累积合入功能特性项近 100+个，适配 CPU 30+款，适配板卡 60+款，累计更新 patch 30000+个， 修复问题数量 800+个，修复 CVE 漏洞 5163 个，其中 7 分及以上的高危 CVE 漏洞 1308 个。

5.1 内核自研特征

- **前台进程优先调度**

在公平调度基础上，修改调度策略，实现分级调度，确保前台进程拥有优先调度权，限制后台进程的调度，使得前台进程调度延迟降低 90%以上，提升交互流畅度，改善用户体验。

- **MPTCP 技术**

基线中合入 patch240+，实现 V11 6.6 内核对 MPTCP 功能完善支持；带宽提升可达 8 倍，随着后续的技术更新，MPTCP 未来将最多可以支持 64 个子链路。

- **blk-load 模块优化技术**

通过 NVME 存储器的负载监控及启发式处理进而得出的当前系统 IO 模式，加快 Linux 内存回收，从而极大的提高该类 IO 型存储应用的性能。

- **bonding 优化技术**

实现 bond4 模式下实现 ARP 和 NS 报文双发功能，降低系统性能开销 igb 驱动 bonding 延时优化，达到降低主备网卡切换延时的效果。

- **电源管理技术**

S1、S3、S4、S1 转 S3、S3 转 S4 功能；提供 KPowerInsight 功耗监控工具；国产平台 cpuidle，devfreq，DVFS，Themal Zone 电源管理功能支持。

- **BFQ 调度器优化**

优先调度前台核心应用，从而降低核心应用的 IO 延迟，如 fio 单线缓存写模式下，优化后大型应用启动速度提升 5%以上。

● **LMK 增加优化**

低内存场景时杀进程机制优化，保护核心进程不被杀死，提升系统在大内存压力下的稳定性。

● **内核增强技术**

KABI 兼容技术，内核 KABI 接口统一；muti-size THP 优化，实现 fio 直接读性能 10%。

● **基础性能优化**

基于实际场景或 benchmark 跑分，通过内存管理、进程调度、磁盘 I/O、文件系统、CPU 频率及动态调优等多维度协同优化，提升系统整体效率。

5.2 社区新特征

● **内存管理 folio 特性**

Linux 内存管理基于 page 转换到由 folio 进行管理，相比 page，folio 可 以由一个或多个 page 组成，采用 struct folio 参 数的函数声明它将对整个（1 个或者多个）页面进行操作，而不仅仅是 PAGE_ SIZE 字节，从而移除不必要复合页转换，降低误用 tail page 问题；从内 存管理效率上采用 folio 减少 LRU 链表数量，提升内存回收效率，另一方面，一次分配更多连续内存减少 page fault 次数，一定程度降低内存碎片化。

● **内存管理 mTHP 特性**

其核心目标是提升内存管理效率并减少 TLB 压力。与传统固定 2MB 大小的透明大页不同，mTHP 允许内核更灵活地分配和管理 8KB~2MB 等多种颗粒度大小的内存块。这种灵活性有助于在减少内存内部碎片的同时，让单个 TLB 条目能够覆盖更大的内存范围，从而降低 TLB Miss 的发生频率，提升内存访问性能。此外，通过将多个连续的常规页面整合为一个更大的逻辑单元进行管理，mTHP 还能有效减少系统中活跃的页面数量，这有助于缩短内存回收时扫描 LRU 链表的时间，进而提升内存回收的效率。

● **EEVDF 调度**

EEVDF 全称“Earliest Eligible Virtual Deadline First ”，是一种全新的公平调度器，旨在替代使用了十多年的 CFS（Completely Fair Scheduler）。它的核心目标是在保持公平性的基础上，显著改善延迟敏感型 任务（如实时任务、交互式任务）

的响应性和确定性。具体而言，在保障任 务运行时间分配公平的同时，优先在没有满足应得运行时间的任务中，选择 任务 deadline 最近的任务，从而保障任务的调度时延，解决了原有的 CFS 调度器只能公平分配任务运行时间，不能满足任务时延要求的问题。

● **可扩展编程调度特性 sched_ext**

利用 eBPF 技术，允许动态定义和修改 CPU 调度策略，突破了传统内核调度器的限制。其核心目标是提供极致的可扩展 性和灵活性，让开发者能在生产环境之外安全地实验、定制和优化调度行为。 其关键特性如下：

- 用户态编写调度器：在用户态使用 C 语言或者 Rust 语言，编写调度逻辑， 使用 GCC 或者 CLANG 编译成字节码
- 动态加载与替换：编译后的 eBPF 调度程序可以在系统运行时动态加载到内核，无需重启或重新编译内核，也可随时卸载或替换成另一个调度器
- 加载后的 eBPF 调度程序，通过严格的验证器保证其安全，被 eBPF 虚拟 机在内核态安全、高效地执行

● **WiFi7（IEEE 802.11be）协议**

支持最大 320MHz 的超大带宽（国内为 240MHz），显著提升传输速率；引入 4096-QAM 高阶调制技术，相比 Wi-Fi 6 的 1024-QAM，数据承载量提升显著；新增多链路操作（MLO），允许设备同时在 2.4GHz、5GHz 和 6GHz 三个频段上聚合传输，大幅提升吞吐量、降低延迟并增强连接可靠性；支持 Multi-RU 机制，更灵活高效地调度频谱资源；实现 16 流 CMU-MIMO，通过多接入点协同，为高密度、高要求的应用场景提供极速、低时延网络体验。

● **MPTCP 多路径全量特性支持**

MPTCP 协议诞生旨在突破传统 TCP 协议的单一 路径传输瓶颈，允许应用程序使用多个网络路径进行并行数据传输。这一设 计优化了网络硬件资源的利用效率，通过智能地将流量分配至不同传输路径， 显著缓解了网络拥塞问题，从而提高数据传输的可靠性和吞吐量。 目前， MPTCP 在下述网络场景中已经展现出了其优秀的性能：

- 网络通路的选择：在现有的网络通路中，根据延迟、带宽等指标评估， 选择最优的通路
- 无缝切网：在不同类型网络之间切换时，数据传输不中断
- 数据分流：同时使用多个通道传输，对数据包进行分发实现并发传输，增加网络带宽

- **dm vdo 去重和压缩功能特性支持**

dm-vdo (Virtual Data Optimizer) 是 Linux 内核设备映射器 Device Mapper 框架提供的一个虚拟块设备驱动，它 通过在块存储层透明地实现高级数据缩减功能，显著提升物理存储利用率： 其核心依赖于 vdo 内核模块，利用模块中子模块实时计算数据块哈希值进行 在线去重，仅存储唯一数据块副本并通过指针引用重复块；同时，对去重后 的数据采用高效算法进行异步压缩，将数据打包存入固定大小的物理块中。结合零块消除，它能大幅减少冗余数据、节约存储空间 （尤其在虚拟机、备 份等场景效果显著），且整个过程对上层应用和文件系统完全透明，是高性价 比的理想内核级方案。

- **其他重要更新**
  - 优化唤醒流程，提升系统睡眠唤醒体验
  - 优化睡眠流程，提升系统快速开合盖睡眠体验
  - USB 4.0 V2 的支持
  - 新增硬件与设备驱动过期提示框架。
  - 支持新的 perf 子功能 perf kwork top
  - 新增 TCP Authentication Option 功能
  - 新增 NPU 加速框架
  - 支持 scsi_debug 错误注入功能
  - 新增 block 队列原子限制支持
  - 新增内存分配分析器特性支持
  - 新增 ecryptfs 支持 SM4 国密算法
  - 新增 pidfs 功能特性
  - 支持 kvdd 显示驱动
  - arm64 平台支持 cmdline 动态开关 lse cpu 特性
  - 支持 etmem 内存分级扩展特性
  - 新增 sock 多路转发功能
  - 支持 ICMPv6 Loopback 特性
  - 支持 ext3/ext4 文件系统故障时通过 netlink 上报
  - 新增 SDEI Watchdog 功能支持
  - folio 和 mthp 内存特性增强
  - 支持 Ext4 caseflod 大小写不敏感特性
  - cgroupv1 支持 memcg 的分级管理以及异步回收
  - 支持 arm64 平台下 virtual cpu hotplug

- 支持 Kmesh 要求的内核网络能力
- 支持混部场景 memcg oom priority 特性
- 支持内核 memory OOM 进程控制策略
- 支持 SMT x86 超线程抢占
- 虚拟网络接收支持 netdim 中断动态调节功能
- 优化大页场景下的内存水位线预留
- 优化 VMA lock 下的缺页错误能力
- 优化 x86 平台下 crash 内核的启动速度
- 优化内存分配信息的统计性能
- 通过引入 mt_dup( ) 接口优化 fork( ) 性能
- 通过降低 vmap/vmalloc 的锁争用优化 vmalloc 多核性能
- 回合上游 slub 分配和内存 compaction 优化特性
- 新增海光 CPU 安全功能，支持 CSV、TPM、TDM、TPCM、CCP、HCT 等驱动
- 新增 BPF arena 特性
- 增加带二维码的 Linux Panic 错误信息显示功能
- 新增 softlockup 中断风暴分析器支持
- 支持 xfs 文件缓存并发写
- 支持 xfs 全新 AF 空间分配算法
- 内核热补丁功能增强
- 支持 ARM8.9HAFT 特性
- 支持 ARM8.6TWED 特性
- vfio 在热迁移中添加 debugfs 功能
- virtio_pmem 支持 SHMEM_REGION 特性
- vDPA 支持用户层查询 virtio 块设备信息
- virtio 添加对 no-reset virtio PCI 电源管理支持
- 虚拟设备 mtty 支持迁移 P2P 状态以及脏页记录
- virtio-net 新增 NETDEV_XDP_ACT_XSK_ZEROCOPY 特性
- 支持显卡优先级设置功能

6 技术指标

银河麒麟桌面操作系统 V11 重要技术指标：

指标类型	指标值
内核版本	6.6
系统运行环境	glibc_2.38 qt_5.92.0 python_3.8.2 perl_5.36.0
Java 版本	openjdk_8u402、openjdk_11.0.21
支持的文件系统	ext3/4、fat、ntfs、btrfs、xfs、udf、gfs2、ufs、ceph、hfs
开发环境	gcc_9.3.0 gdb_9.1 qt_5.92.0 qtcreator_4.14 automake_1.16
X 服务器	Xserver(1.20.9)
grub	2.12
gtk	3.24.41、4.14.2
systemd	255.2
浏览器	奇安信可信浏览器 V1.0

远程登录	openssh-client_8.2p1、openssh-server_8.2p1
文档查看器	atril_1.24
外设	Cups(2.4.7) libjbig(2.1-3.1) libpng(1.6.43) libjpeg(2.1.2)

表 3 银河麒麟桌面操作系统 V11 重要技术指标列表

7 桌面环境

7.1 UKUI

基于 UKUI 4.0“轻量化感知”设计原则基础上，UKUI 4.20 以“更流畅的交互、更智能的体验、更个性化的配置、更安全的基座”为核心目标，通过五大进化方向全面重构桌面体验，为用户带来更高效、更智能、更贴心的操作系统服务。

全局动效优化

UKUI 4.20 完成窗口显示/隐藏动效、应用组动效、桌面图标动效等 46 个交互动效。其中优化的模块包括：

- 通用控件：单选、多选、开关、搜索框、滑动条等 12 个动效
- 窗口类：窗口打开、关闭、居中、最大化、最小化、还原等 11 个新动效
- 功能模块类：图标拖动/悬停、面板显示/隐藏、标签分离/聚合等 23 个动效

UKUI Framework 深度优化

实现开始菜单、任务栏、侧边栏的模块化整合，在保证功能独立性的基础上建立统一交互语言，为轻量化设备与复杂场景提供弹性支撑。

开始菜单

- 智能排序算法：根据使用频率和打开时间智能推算优先级
- 场景化入口：高频功能（如天气、看图、WPS 等）可纳入收藏直观显示
- 任务栏固定优化：支持从开始菜单固定到任务栏操作

任务栏

- 多屏协同协议：自定义主副屏任务栏显示策略（支持多屏显示或镜像模式）
- 托盘精细化管理：图标显示/隐藏自定义，提升多任务管理效率
- 任务栏窗口图标状态优化：非合并状态下新增激活/非激活状态

多任务视图

- 工作区支持自定义命名（如设计/开发/会议）

控制台

- 二级界面联动：网络、蓝牙、声音界面二级联动
- 按钮编辑功能：支持自定义配置按钮，满足个性化需求

文件管理器

- AI 全文搜索：支持文件标签、关键字匹配内容搜索，提供更符合用户期望的搜索结果，提高全局搜索文件效率
- 智能空间管理：随时创建智能空间，支持查看和编辑，融入文管自身搜索与筛选流程，延续用户使用习惯
- 文档理解引擎：智能生成摘要/标签（支持中英双语技术文档；
- 交互体验升级：优化布局，打造简洁、美观的操作界面，对共享与远程体验进行了优化，对地址栏和页签进行了优化

智能模糊搜索

- 融合 AI 能力，支持对图片和文件内容进行识别与检索，无需关键词匹配，即可快速实现定位数据

控制面板

- 蓝牙多设备池：支持多链接技术（Multi-Point），可同时连接多个蓝牙音频设备
- 护眼模式：色温实时预览，告别参数盲调
- 输入法配置：系统级输入法配置，支持添加多种输入法及输入法界面个性化设置
- 任务栏配置：统一托盘区域显示系统图标配置，方便快捷规划托盘功能区域；新增虚拟键盘配置功能，满足不同输入场景
- 背景设置体验优化：将“背景预览”与“背景相关设置”同行显示，可充分利用首屏空间，方便用户浏览更多壁纸，提高用户选择壁纸效率；在用户滚动下方壁纸时置顶显示，方便用户选中不同壁纸后，能随时看到置顶展示壁纸预览，无需滚动到页面顶部，提高用户高频操作的效率
- 字体管理：增加用户添加和查找字体功能，解决新装字体淹没在字体列表里，难以找到的问题
- 音频管理：细化隐私保护场景
- 虚拟键盘：虚拟键盘交互体验优化

通知管理

- 规范系统通知注册机制，方便用户管理系统通知

其他优化

- 窗口管理：最大化按钮鼠标悬停支持分屏
- 新主题框架：引入 UI Design Token，提升显示一致性
- 智能剪切板：新增智能剪切板功能，并对剪贴内容进行分类管理
- 系统监视器：增加磁盘详情读写页
- 远程桌面支持 RDP 协议

7.2 应用兼容

为丰富麒麟应用生态,使用户能够得到和其他平台相同的用户体验。银河麒麟桌面 V11 为用户提供了麒麟移动应用兼容运行环境（KMRE）和麒麟 Windows 应用兼容运行环境（KWRE）的创新技术。

KMRE

麒麟移动运行环境（KMRE）摒弃虚拟机和模拟器方案，真正地将系统和移动环境合二为一，从本质上让系统支持移动应用的运行，从而形成了一套先进完整的移动应用生态迁移解决方案。本地 APK 包支持直接安装，使桌面 PC 与移动设备融合，为用户提供了更加便捷的操作体验，解决用户应用的多样化需求。

●兼容性强：KMRE 目前已经支持飞腾、鲲鹏、海光、兆芯、Intel、AMD 等处理器和 NVIDIA、AMD、Intel、MALI、JJM、GP101、景嘉微等显卡

●融合度高：将桌面操作体验与移动体验进行深度结合，如通知中心、系统托盘、输入法、文件管理等；设备互通，支持键盘、触摸屏、鼠标、手柄等输入；摄像头支持热插拔，支持拍照、视频聊天和视频会议

●平行界面：支持在同一应用中同时开启两个任务界面，查看详细内容时，无需反复跳转，高效省时，充分利用 PC 大屏优势

●易用性高：等比例拉伸窗口、横竖屏切换，支持截图、录屏操作快速分享；可设置游戏按键，快速体验游戏；依据显卡硬件选择性能模式，支持对 AMD、Intel 视频播放硬解码加速，提供安卓应用摇一摇功能，虚拟键盘自适应分辨率

●稳定高效：KMRE 兼容性高、稳定性好、资源开销少、运行效率高；移动应用的使用可从软件商店直接下载，也可直接双击安装 APK 包

●部署简单：易于部署和移植，KMRE 安装 deb 包即可完成部署，无需手动执

行其他脚本

●生态丰富：支持上千款移动应用，覆盖办公、社交、游戏等多种软件类别

KWRE

麒麟 Windows 运行环境（KWRE）是一套跨平台在系统上运行 Windows 应用的兼容环境，支持在多个架构下对所需 Windows 应用进行适配，使得 Windows 应用可以在麒麟桌面操作系统 V11 上运行，满足客户日常办公与生产需要。

KWRE 一键安装技术让用户在银河麒麟桌面操作系统 V11 上安装 Windows 应用程序变得非常简单。只需在软件商店中搜索对应的应用程序，无需进行任何配置，KWRE 环境就会部署在系统中。

●兼容性强：支持丰富的硬件平台，支持主流处理器如：飞腾、龙芯、海光、兆芯及通用 X86 等处理器

●融合度高：支持与系统文件互通，Windows 兼容软件中文档和银河麒麟桌面操作系统文档之间可无缝剪切和粘贴，实现跨平台的快捷键和窗口管理；支持设备互通，声音互通，视频互通

●病毒防护：应用感染病毒后的传播仅在 KWRE 运行环境中，不会对桌面操作系统造成影响

●生态丰富：目前已经适配办公类、社交类、工具类等 50 余款常用应用

7.3 AI 能力

AI 子系统

麒麟 AI 子系统分为云端模型配置、本地模型配置、自定义模型配置三个部分。

第一部分是云端模型配置，用户通过网络访问使用。该配置支持大语言模型、视觉模型和语音模型的灵活配置，用户可以通过设置关键参数，快速接入云端 AI 服务，实现高效的模型调用与数据处理。

第二部分是本地模型配置，安装在本地设备上，无需网络连接即可运行。这种配置方式特别适合对数据隐私和实时性要求较高的场景，用户可以在本地设备上直接调用 AI 模型，确保数据安全性和响应速度。

第三部分是自定义模型配置，针对局域网部署，或者其他接入方式的 AI 能力，提供自定义模型配置功能，满足个性化使用场景。

此外，麒麟 AI 子系统支持自定义模型调用优先级，用户可以根据实际需求选择

优先使用云端模型、本地模型或者自定义模型，从而灵活应对不同的应用场景。

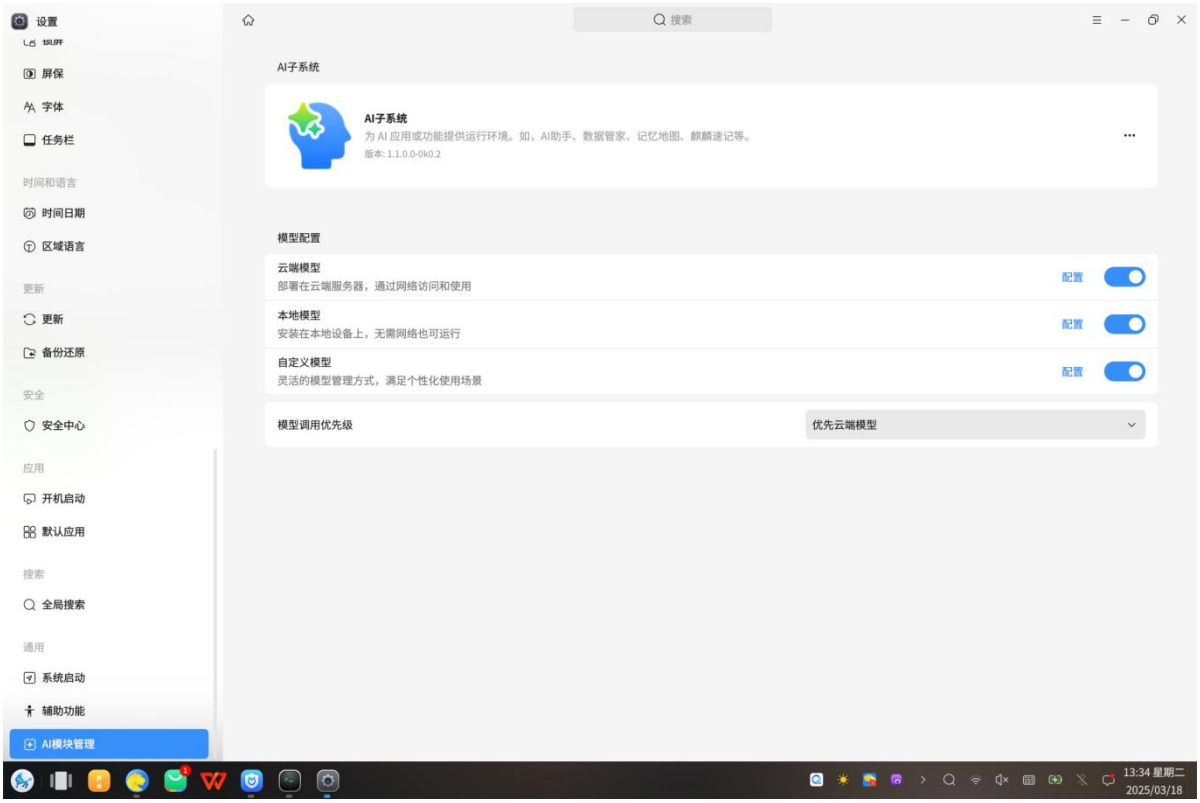

图 3 AI 子系统

说明：使用 AI 子系统，需要预留 6G 以上存储，以及配套高性能硬件支持。

AI 模型

云端文本类模型免费试用账号上线。为进一步降低用户在模型配置环节的门槛，助力用户更便捷地体验 AI 能力，云端模型新增文本类模型免费试用账号。通过该免费试用账号，用户无需复杂配置即可快速接入文本类 AI 模型，轻松体验智能问答、文本处理、生成等核心功能，轻松感受 AI 技术带来的高效与便利。

AI 功能应用

AI 功能应用是基于多种端侧和云端模型混合调度的应用程序，支持通义千问、百度-ERNIE-Bot-4、讯飞 Spark Max、Deepseek 等主流大模型。

AI 助手

AI 助手宛如一位 24 小时待命的全能顾问，不仅能快速响应各类常规问题，精准解答知识疑惑，还能基于深度学习积累的丰富经验，针对复杂的工作场景、学术难题等提供专业且极具可行性的建议。无论是文案创作时的灵感枯竭，还是代码编写过程中遭遇的技术瓶颈，AI 助手都能通过智能分析，结合行业最佳实践，给出个性化的解决方案，有效节省用户时间与精力。

记忆地图

记忆地图打破传统记忆模式，以直观、形象的可视化方式梳理知识脉络。它能将零散的知识点构建成逻辑清晰的知识网络，帮助用户快速把握知识体系的整体架构与内在联系。无论是备考复习，还是学习全新领域的知识，记忆地图都能让用户更高效地理解、记忆信息，同时激发创新思维，促进知识的灵活运用与拓展。

智能模糊检索

智能模糊检索彻底革新传统检索方式，突破了精确关键词匹配的限制。当用户无法清晰表述需求、输入模糊信息时，该功能能够通过语义理解、联想分析等技术，精准定位到与之相关的各类资源。无论是查找文献资料时对某一概念的大致描述，还是搜索历史记录中模糊的事件片段，智能模糊检索都能快速、准确地返回结果，显著提升信息获取的效率与便捷性。

麒麟速记

麒麟速记则是办公与学习场景下的高效记录利器。在会议、讲座、采访等需要快速记录信息的场景中，它能够实时、准确地将语音转化为文字，支持多种语言与方言，且具备强大的自动纠错、标点添加功能。麒麟速记还能对记录内容进行智能分类、标注重点，方便用户后期编辑与整理，大幅减少手动记录的工作量，让用户专注于内容本身，有效提升沟通与信息处理效率。这些 AI 应用功能相互协作、相辅相成，全方位为用户的工作、学习与生活赋能，开启智能时代的全新篇章。

7.4 安全防护

KSAF 安全框架

KSAF 是麒麟全新自研的一套可编程动态多策略融合的安全框架技术，实现系统机制与策略分离，提高安全功能的可靠性、灵活性和易用性，满足不同业务场景下对操作系统的多样化安全需求。

安全中心

安全中心是一款系统安全图形管理工具，包含安全体检、病毒防护、账户保护、防火墙、漏洞修复、隐私安全、可信度量和安全工具等功能。

●安全体检对系统账户安全，系统配置安全，系统软件漏洞等进行多项检测，及时发现和修复系统安全隐患，并且可针对单项异常进行专项修复，保障系统运行安全和稳定

●病毒防护通过对系统的病毒查杀保护系统健康，快速查杀、全屏查杀、自定义查杀可满足不同场景下的查杀任务，配合标准或高速扫描模式，将潜在风险隔离至特定区域

●账户保护提升了账户和登录的安全性，自定义设置密码强度、密码连续输错次数、用户锁定时间，防止密码被暴力破解导致数据丢失，同时提供根账户远程登录限制开关，可防止高权限远程访问

●防火墙帮助识别网络访问，设置防火墙访问规则，在使用公共场所的网络时，保护系统网络安全性；提供一键关闭远程访问功能

●漏洞修复提供漏洞库更新功能、漏洞扫描功能、漏洞查询功能，联动更新完成漏洞修复功能

●隐私安全通过限制应用访问权限，保护系统隐私资源安全和个人隐私

●可信度量兼容支持兆芯主板内置 TPM、海光 CPU TPM/TCM、飞腾 kyee 可信启动度量，依据信任传递的思想，实现对可信根、TPCM/TPM/TCM、可信固件 UEFI 、GRUB 引导程序、系统内核文件与关键配置文件进行逐级度量，构建完整可信信任链，为设备启动建立初态的可信执行环境

●安全工具下包含了一系列全面保障系统安全性的工具：

- ■ 应用程序来源检查：设置未知来源应用安装策略
- ■ 进程防杀死：保护特定进程在运行过程中不被意外或恶意终止
- ■ 内核模块防卸载：防止系统内核中的特定模块被非法或意外地移除
- ■ 文件防篡改：确保文件在存储和传输过程中不被非法修改
- ■ 应用程序执行控制：设置应用执行策略，保护系统运行环境
- ■ 设备安全：提供外部设备接入的多重防护控制功能，有效防止系统重要数据意外丢失和恶意盗取
- ■ 应用联网控制：设置应用联网控制策略，在未授权的应用或服务访问网络时，可及时拦截并提醒

文件保护箱

文件保护箱是具有数据隔离与加密保护的特殊目录，支持通过文件保护箱管理工具和文件管理器进行新建、删除、打开、锁定、密码修改、重命名等操作。达到一箱一密、一文一密的控制粒度，并结合系统其他安全属性，实现数据的绝对隔离与加密保护。支持密钥加密保护箱和透明加密保护箱，支持保护箱导入导出，支持

密码强度检查和防暴力破解安全机制，支持自动锁定和定时锁定，支持注销、锁屏时自动锁定，锁定、注销时清除文管里保护箱文件访问记录。支持基于 TPM 的密钥保护。支持保护箱删除后彻底抹除文件数据。

日志查看器

日志查看器是一款集中展示系统日志的工具，包含系统日志、启动日志、认证日志、应用日志、内核日志和安全日志，提供复制、刷新、导出、搜索、排序等功能，实现对日志内容的分类显示和结构化解析。

- 扩展日志内容搜索范围，支持对详情信息的搜索
- 优化支持海量日志数据管理
- 系统远程登录的日志，检测到远程用户登录情况与记录
- 记录麒麟安全、崩溃日志和审计日志
- 支持日志轮替和日志轮替规则设置

磁盘加密

- 支持磁盘分区加密、取消加密、解锁、锁定；支持系统分区和非系统分区加密；支持保留数据加密和非系统分区格式化加密
- 支持磁盘加密密钥管理，支持通过备份密钥重置密码，支持口令、TPM、TPM+PIN 等解密方式
- 加密密码支持复杂度配置，支持防暴力破解

统一认证

统一认证在支持人脸、指纹、指静脉、虹膜、声纹等生物特征的前提下，加入远端账号认证和安全密码设备认证机制，通过微信扫码或 Ukey 证书认证方式授权登录。

双因子认证

支持使用用户密码和作为第二因子的 OTP 或 Ukey 来完成更安全的双因子认证，支持系统登录和授权。

7.5 系统更新

银河麒麟桌面 V11 系统更新模块将用户所需所想的更新功能全面展现。

源更新管理

银河麒麟桌面 V11 更新时检测系统异常后自动修复异常信息，包括自动更换用户使用的软件仓库，自动更换用户可更新应用列表，自动修复用户系统包数据库异常等，保证用户使用无异常。银河麒麟桌面 V11 支持软件源服务器多个地址以优先级顺序访问；支持多种定制版本的区分推送以及灰度推送，使更新更精准更全面。

推送机制

银河麒麟桌面 V11 具备多种检测更新模式，包括开机更新检测、定时错峰检测、周期检测、用户手动检测，同时用户可选择开启自动下载和更新。支持多种推送方式与推送区域控制，管理员可选择区域全部推送，区域部分推送，静默推送，可选推送、精准推送等。根据用户服务序列号在管理端配置升级列表，包括静默更新列表和可选更新列表。管理员可通过管理端设置对这批序列号全部推送、部分推送或单个推送。管理员设置为部分推送时可自定义部分推送的百分比数量。

更新保障

银河麒麟桌面 V11 支持下载更新限速功能，防止过多占用用户网速；支持更新保护机制，对更新全流程进行监控,在更新前自动检测当前环境，更新过程中不允许关机、重启、休眠等操作，确保更新顺利完成，不受非常规操作干扰，如遇更新异常可回退至更新前版本。更新完成后支持查看更新历史，让用户了解银河麒麟桌面 V11 的每一次更新，伴随银河麒麟桌面 V11 的每一次进步。

7.6 软件商店

软件商店是一款内容丰富的图形化软件管理工具，为用户提供软件的搜索、下载、安装、更新、卸载一站式管理服务。软件商店作为应用分发平台，为用户推荐常用软件和优质软件，用户不仅可以快速搜索需要的软件，还可以根据具体需求，通过商店的分类查找相关的软件。每款上架的软件都有详细的软件信息以供参考，可根据实际需要进行下载安装。

- 支持原生软件、Windows 兼容软件、移动应用、驱动多种类型软件
- 支持多种专题推荐模块，多软件并行下载，同类型软件推荐，优质软件推荐，采用智能算法为用户推荐当前热度较高的软件，满足用户多种软件需求
- 使用麒麟 ID 登录软件商店进行软件评分与评论，对他人评论进行点赞，互动丰富，同时支持查看云安装历史，一键安装云端软件

●提供浅色与深色两种主题，并支持自动跟随系统主题风格

●可设置自动更新软件商店及已安装软件，静默无感知、便捷更高效

●可设置软件安装后自动创建桌面快捷方式

●增加企业资质认证、个人资质认证，支持软件数字签名验签，建立面向开发者的多级软件安全审核机制，确保进入软件商店的软件安全稳定

●支持软件适配质量评级

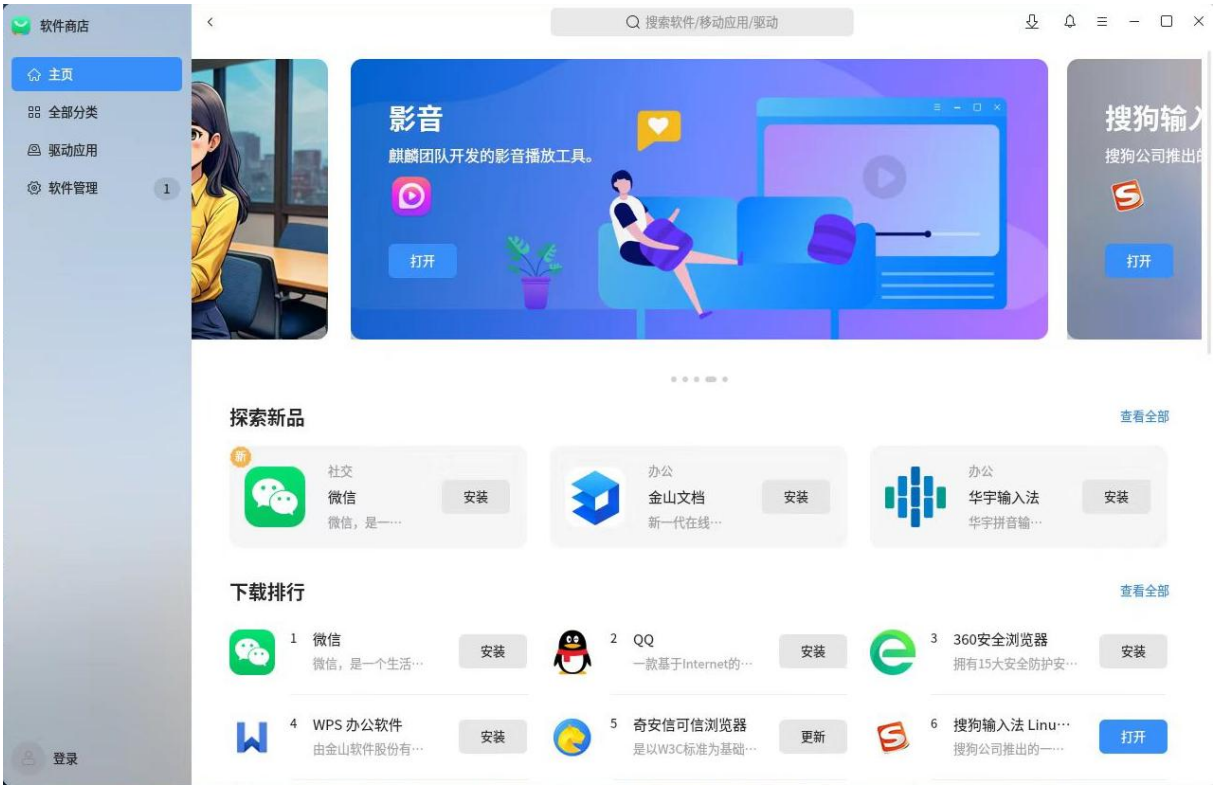

图 4 软件商店登录界面

7.7 Kylin SDK

为开发者提供统一便捷的开发工具和接口，构建基于银河麒麟操作系统及国产硬件平台的原生应用，降低开发成本，提升开发质量与效率，让信创开发更简单！

目前 SDK 版本已迭代更新到 3.0 版本：合计提供各类接口超过 2600 个，具有兼容性强、部署灵活、控件优质、接口丰富的特点， 麒麟 SDK 主要包含以下功能层级及模块：

●应用支撑：基础窗体控件，对话框控件，按钮控件，滑动条控件，进度调控件，消息提示控件，应用行为控制等

●系统能力：系统时间报时，CPU、网卡等硬件信息，内存、swap 分区等资源信息，系统名称、版本、激活等信息，文件管理，OCR，系统属性及系统主题控制

等

●安全管控：设置管控，电源管控，设备管控，应用管控，数据管控，网络管控等

●基础开发：日志管理，定时器，链表模块，配置文件操作，单位进制转换，C 语言字符串扩展等

●通用中间层：读卡器接口，扫描仪接口，打印机接口，手写板接口，高拍仪接口等

●AI 能力：文字识别、语音识别/合成、文本/图像向量化、文本生成、图像生成

●开发工具：提供可视化打包工具、兼容性扫描工具等功能丰富、使用便捷的开发、打包发布、适配工具

此外，SDK 还提供了配套文档材料，以降低开发者入门门槛，其中包括：开发环境部署文档，开发工具使用文档，开发规范指导文档，应用开发指导文档，应用迁移指导文档，均可在开发者平台中获取。

8 配套方案

8.1 软件商店私有化部署

当前自主创新已深入各重点行业及领域，部分企业对于网络安全有着极高的要求，在日常办公环境中只允许访问内部网络，不允许访问互联网。目前大多数软件商店的仓库源都是部署在公网环境下，在企业只能访问内网的情况下，无法访问到公网的软件商店仓库源，需要在企业内部单独部署软件商店的仓库源，进而满足用户的内网需求。

麒麟软件商店管理平台（私有化版）本着简单、适用、高效的原则，贴合实际使用需求，采用 B/S 与 C/S 架构相结合的方式，即普通用户使用 C/S 架构的软件商店客户端进行软件下载、安装等，管理员使用 B/S 架构的软件商店管理平台进行软件的上架、下架、更新等运维管理。提供一套完整、标准的软件商店（私有化版）解决方案，以解决内网环境下无法下载软件、管理软件的问题。

麒麟软件商店管理平台（私有化版）产品，包括软件商店客户端、软件商店管理平台、仓库源 3 大核心模块。实现软件的全生命周期管理，软件包的上下架管理，软件信息维护管理，数据统计管理等功能。提供了从软件上架、软件包推仓、到最终客户端下载安装的一体化服务。

图 5 软件商店架构图

私有化部署的优势：

- 服务运行在企业内部服务器上
- 信息存储在企业内部服务器上
- 企业自主掌控所有数据和权限
- 可实现内外网隔离安全性更高
- 个性化强企业可按需定制功能

8.2 终端安全管控

麒麟天御安全域管平台（简称“麒麟天御”）是一款面向企业的高效安全管理平台，专注于提升企业管理效率和安全管控能力。平台聚焦人员管理、设备管理、应用与资源管理、安全管理四大核心场景，打造从身份认证、权限控制、策略执行

到审计记录与安全响应的全流程统一管控体系，为企业提供全面、安全、可靠的管理支撑。

麒麟天御采用 B/S 与 C/S 混合架构，包含服务端与客户端两大核心模块，兼具灵活性、扩展性和高效操作体验。服务端提供一体化 WEB 管理控制台，覆盖组织、用户、终端的全方位安全管理。同时，服务端可基于银河麒麟容器云平台构建，支持多种单双园区高可用部署方案，保障业务系统高效、连续运行。客户端深度融合麒麟通用桌面操作系统，集成入域退域、数据同步、策略执行与撤销、日志同步、消息提醒等核心功能，有效解决统一认证、策略控制及维护升级等关键需求，为业务信息系统管理提供可靠支撑。

图 6 麒麟天御产品架构图

● **集中化身份和访问：**麒麟天御提供了集中化的身份验证和访问控制，使管理员能够统一管理和控制用户账户、组策略和访问权限。简化了用户管理和安全管理，减少了重复工作和管理复杂性。

● **组织人员与权限管理**

支持 ldap(ldap over tls、ldaps）、Kerberos 等多种认证与数据同步协议；提供对外 LDAP 服务进行认证与数据同步；提供对外 SSO 服务（包括：系统级与 B/S 应用级单点登录）并进行白名单管控；提供 OpenAPI 服务推送和拉取域控基础数据并进行应用级授权管控；支持域用户权限管控细化到命令级和文件级，并可自定义权限的有效期。

● **终端管理与远程维护**

支持终端自动分组及动态同步，可自定义 8 条匹配规则；新增终端公共机属性，隶属公共机相同组织人员均可登录；多终端间安全 VNC 远程协助，可远程自动拉起目标方 VNC 服务，未使用时自动静默。

● **统一策略与任务协调**

支持 200+管控策略项，全面覆盖终端细粒度策略管控；全新策略模型，兼顾继承、强制、例外、优先级、临时取消。

● **安全威胁全方位防控**

集成系统安全类解决方案：隐私文件访问权限控制、进程保护、文件防篡改；集成网络安全类解决方案：流量与流速控制、应用联网管控；集成数据安全类解决方案，包括：文件外发管控、敏感打印管控、公共机敏感数据清理和磁盘加密等。

● **日志报表与数据监控**

全方位统计形成运维报表，包括：资产信息、在线时长、资产统计、终端健康度统计、流量流速统计、策略视图、软件应用统计等；终端全方位关键操作日志采集与外发，包括主机行为、DNS 日志、硬盘接入、管控异常告警、监控指标告警及定向采集；监控大屏中支持应用使用统计、紧急事件通报及告警变化趋势可视化展示。

● **性能与高可用**

单项目终端纳管规模可突破 12 万，7×24 小时高压负载稳定运行；支持单园区及同城/异地双活等多种部署架构，提供自研存储高可用方案 KylinFS，具备节点健康实时监控能力，核心故障可 1 分钟内告警；支持一键巡检、一键恢复、一键还原、一键升级功能，故障自愈机制快速响应、运维更智能便捷；高中低三级部署方案，从小规模验证到超大型部署全覆盖，硬件资源智能配比，功能模块两种组合，完美平衡成本与性能。

● **兼容性**

云桌面兼容：中兴、华为、紫光、深信服、锐捷云桌面兼容纳管；认证同步兼容：支持竹云、鑫盾、信安、派拉等 4A 的认证对接与数据同步；兼容阿里云平台高可用环境；兼容国产数据库，包括达梦数据库、OceanBase；兼容基础网络服务，如 ZDNS。