



AI时代企业信息系统 安全计算架构白皮书

version 1

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财务、运营、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，不构成任何要约或承诺，邦彦不对您在本文档基础上做出的任何行为承担责任。邦彦可能不经通知修改上述信息，恕不另行通知。

版权所有 © 邦彦技术股份有限公司2026。保留一切权利。

非经邦彦技术股份有限公司书面同意，任何单位和个人不得擅自摘抄、复制本手册内容的部分或全部，并不得以任何形式传播。



扫码关注官方公众号

基于 NGCC、五业务域与双 AI 助理模型的新一代企业计算参考架构
Secure Enterprise Computing Reference Architecture for the AI Era



构建"计算主权、数据主权、AI 主权、组织主权"统一的
新一代企业计算体系

A Secure Enterprise Computing Reference Architecture for the AI Era

摘要Executive Summary

人工智能、大模型、智能体与云计算的深度融合，正在推动企业信息系统进入新的发展阶段。传统以"终端计算、内网系统、边界防护"为核心的企业IT模式，已难以同时满足数据主权保护、AI能力开放、智能体协同执行与组织效率提升的综合要求。对于科技型企业而言，这一挑战尤其突出：核心代码、研发资料、专利数据、经营数据和组织知识构成长期竞争优势，而研发、销售、财务、供应链等业务活动又越来越依赖AI辅助与Agent自动执行。

为此，邦彦技术提出**"AI时代企业信息系统安全计算架构"**。

该架构以NGCC (Next Generation Commercial Computer, 下一代商用计算机) 为统一计算底座，以五业务域作为安全与业务边界，以七层技术架构作为实现方式，以双AI助理模型作为员工级人机协同范式。



核心架构要素	定义	核心价值
五业务域	S5核心域、S4三链域、S3互联网域、S2 Agent域、S1外部生态域	清晰划定各类数据、业务与AI能力的主权边界
七层技术架构	从终端访问层到外部生态服务层的完整技术能力栈	明确AI时代每一层能力的落位与实现方式
NGCC统一计算底座	下一代商用计算机，提供集中计算与多域隔离	收回计算主权，实现终端零数据与单终端多域访问
企业私域AI平台	私有大模型+企业知识库+RAG体系+专有Agent	沉淀企业内部智能能力，数据主权不出企业
双AI助理模型	私域AI助理+公域AI助理的员工协作新范式	既用企业内部知识，又安全调用公网AI能力

核心观点

AI时代企业最合理的计算架构，不是"在旧系统上叠加AI工具"，而是以云PC统一计算底座为基础、以五业务域为边界、以私域与公域能力分层协同为方式、以双AI助理为员工工作单元的新一代企业安全计算体系。

新一代企业安全计算体系

目录 CONTENT

前言

第一章 AI时代企业计算重构的背景与趋势

第二章 设计思想:四大主权与架构原则

第三章 五业务域:AI时代企业安全与业务边界

第四章 七层技术架构:AI时代企业计算能力实现方式

第五章 NGCC / 邦彦云PC:AI时代企业统一计算底座

第六章 企业私域AI平台:企业内部智能能力中枢

第七章 互联网访问与公有AI能力体系

第八章 双AI助理模型:AI时代员工的人机协同新范式

第九章 三链体系与AI时代企业运行方式

第十章 安全机制:从网闸隔离到AI治理

第十一章 典型应用场景

第十二章 企业建设与改造路线图

第十三章 产业价值与未来展望

附录

01

03

06

10

16

20

23

25

27

30

32

35

39

42

44



新一代 企业计算参考架构

A Secure Enterprise Computing
Reference Architecture for the AI Era

前言 PREFACE

人工智能正在推动企业信息系统进入一个新的时代。过去二十年，企业信息化建设的核心目标是通过ERP、CRM、PLM、MES、HRMS、OA、BI等系统实现业务流程在线化、数据记录电子化和经营管理数字化。企业信息系统更多扮演的是"业务支撑工具"角色，主要解决"信息如何被记录、流转和统计"的问题。

然而，随着大模型、AI Agent和自动化智能系统的快速发展，企业信息系统的角色正在发生根本性变化。它不再只是一个"记录和支撑系统"，而正在演进为企业经营活动的智能协同中枢、企业知识资产的组织和调用平台、企业私域智能能力的运行载体，以及公域AI能力与企业私域能力的安全连接桥梁。

对科技型企业而言，这一问题尤为关键。科技型企业的核心竞争力来自技术积累、源代码与算法实现、产品架构设计、研发过程知识和长期沉淀的组织know-how。这些资产一旦在终端、插件、浏览器或公网AI调用过程中失控，将带来不可逆的竞争损失。因此，AI时代企业信息系统建设，不能只是"在原有IT架构上加一个AI入口"，而必须从计算主权、数据主权、AI主权和组织主权的角度，重新设计企业计算体系。

本白皮书面向正在推进AI转型的科技型企业、研发驱动型企业和高安全要求行业，提供一套完整的企业计算架构参考方法论。

适用对象	典型问题	白皮书能提供的参考
企业CTO / CIO	如何在保护核心知识资产的前提下使用AI	五业务域划分方法与私域AI平台建设指南
信息化负责人	如何避免企业数据在公有模型调用中失控	七层技术架构与AI安全网关部署方案
业务与IT架构师	如何让AI与业务流程和员工工作方式深度融合	双AI助理模型与三链体系协同设计
高安全行业从业者	如何在多域隔离环境下兼顾效率与安全	NGCC统一计算底座与跨域隔离机制详解

第一章
AI时代企业计算
重构的背景与趋势



第一章
AI时代企业计算重构的背景与趋势

1.1 AI正在改变企业信息系统的基本形态

企业信息系统的发展大致经历了三个阶段：信息化阶段、数字化阶段和智能化阶段。

- **信息化阶段** 核心任务是"把线下流程搬到系统中"。企业通过ERP、CRM、PLM、MES等系统实现业务流程在线化、表单化和数据化, 主要价值是提高管理透明度、减少人工统计误差。
- **数字化阶段** 核心任务是"让系统数据可以被分析和运营"。企业开始建设数据中台、BI看板和统一报表平台, 强调数据汇聚、数据质量和经营指标的实时呈现。
- **智能化阶段** 核心任务不再只是"数据可见", 而是"系统具备智能协同能力"。AI可以理解业务数据、参与流程判断, AI Agent可以承担执行任务, 企业知识可被模型检索调用, 人类员工与AI协作成为常态。

这意味着, 企业信息系统的基本形态正在从"业务系统集合", 变成"业务系统+AI平台+Agent能力+统一计算底座"的复合型智能系统。

1.2 传统架构的结构性局限

传统企业IT架构长期建立在三个默认假设之上：终端是主要计算载体；内网是可信的；人是唯一的执行者。在AI时代, 这三个假设都不再成立。

传统假设	在AI时代的失效原因	新的架构应对方式
终端是主要计算载体	终端是主要计算载体终端承载本地数据与AI调用入口, 数据外泄风险被成倍放大	计算迁移到云端, 终端零数据, NGCC统一计算底座
内网是可信的	内网员工可直接访问公网AI, AI调用成为新的数据外泄通道	零信任架构, 持续验证, 基于身份而非位置建立信任
人是唯一执行者	AI Agent可自主执行多步骤操作, 权限扩散和数据访问超出预期	Agent沙箱隔离, 行为全量审计, 最小权限绑定

1.3 科技型企业面临的四重挑战

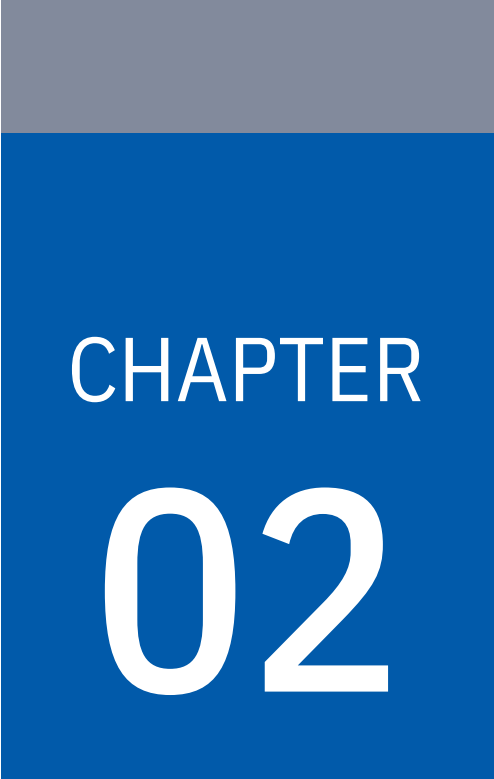
企业信息系统的发展大致经历了三个阶段：信息化阶段、数字化阶段和智能化阶段。

- **核心资产保护挑战** 研发源码、算法实现、专利文档等高价值知识产权，在公网AI调用过程中存在被训练记忆和向第三方输出的风险，传统DLP工具无法有效拦截AI语义层面的数据外泄。
- **AI效率开放需求** 竞争对手已广泛应用AI辅助开发，不用即落后。企业需要在不牺牲安全的前提下，让员工充分享受AI效率提升，两者可以通过架构设计统一实现。
- **多网多域协同困境** 研发网、办公网、互联网在物理上隔离，员工需要多台设备频繁切换，效率损耗巨大，且切换过程本身存在数据传递的合规风险。
- **合规与监管压力** 《数据安全法》《个人信息保护法》《生成式AI服务管理暂行办法》等相继落地，对AI数据处理提出强制性要求，企业必须建立可审计、可追溯的AI治理机制。



本章结论

企业信息系统正在从“业务支撑工具”演进为“智能协同中枢”。传统的终端计算、内网信任、人工执行三大假设在AI时代全面失效。科技型企业迫切需要一套以数据主权保护为前提、以AI能力安全开放为目标的新一代计算架构。



第二章
设计思想
四大主权与架构原则



第二章

设计思想:四大主权与架构原则

2.1 AI时代企业架构的四类主权

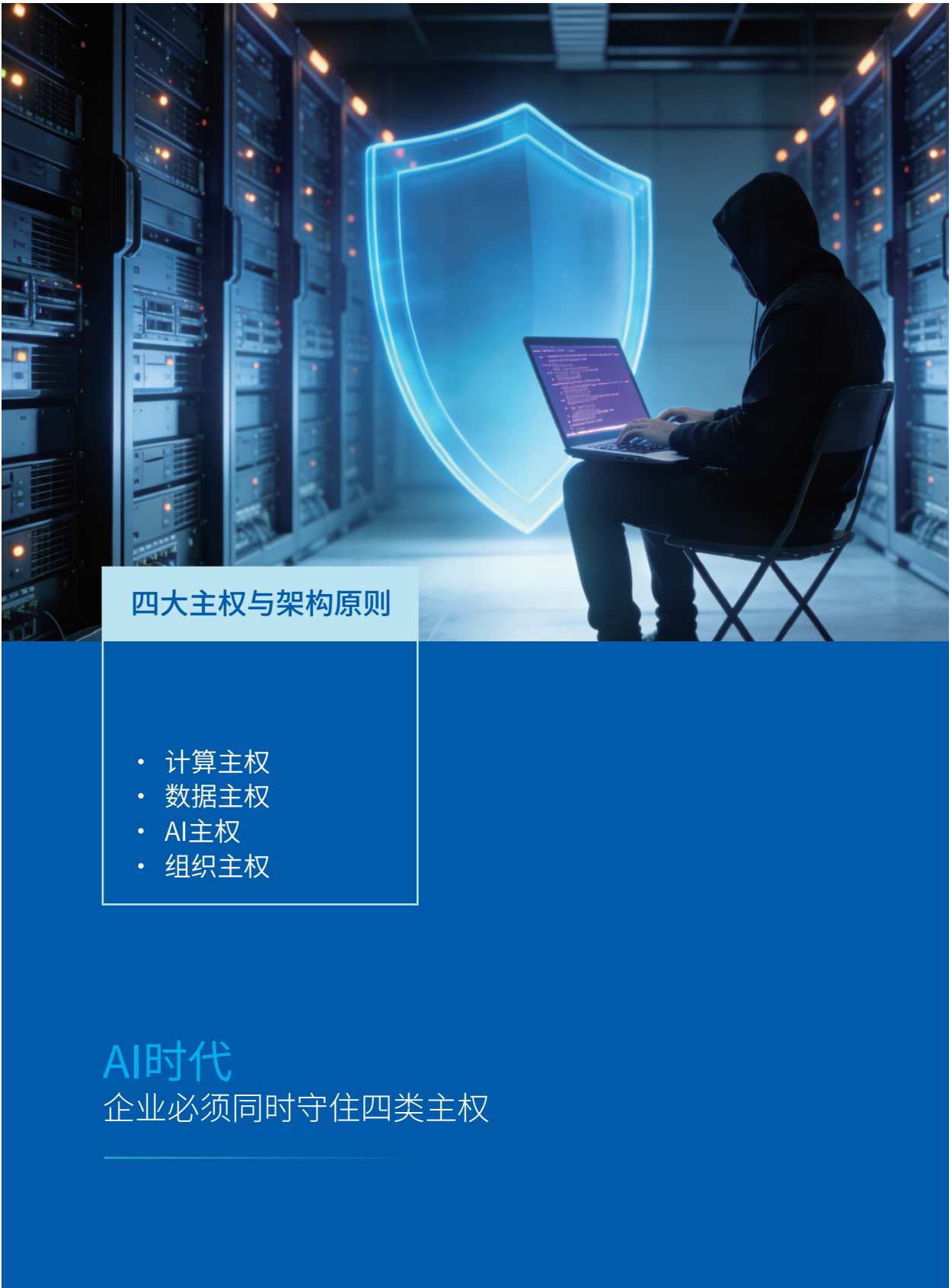
本白皮书将"主权"概念引入企业架构设计,用以描述企业对其核心资产和能力的完整控制权。

AI时代,企业必须同时守住四类主权:

主权类型	核心含义	失控的典型后果	架构应对方式
计算主权	企业计算能力在企业自主控制的基础设施上运行,不依赖难以治理的分散终端	终端本地数据成为泄漏入口,终端管控成本失控	NGCC统一计算底座,计算从终端迁移到云端
数据主权	企业核心数据始终在企业受控环境中处理和存储,不因AI调用而外流	员工调用公网AI时携带原始敏感数据,数据被外部平台记录或训练	五业务域隔离+数据脱敏网关+私域AI平台
AI主权	企业拥有自主可控的AI能力,不完全依赖第三方公有模型,能够沉淀内部智能能力	企业知识资产全部流向外部AI平台,自身智能能力无法积累	企业私域AI平台+私有大模型+企业知识库
组织主权	企业能够自主定义员工与AI的协作方式,AI增强组织能力而非替代组织结构	AI使用零散不可控,无法与组织管理整合,无法形成组织级能力沉淀	双AI助理模型+三链体系+AI工作台统一治理

2.2 总体设计原则

- **边界优先** 先划清五业务域的安全边界,再在边界内配置AI能力。边界不清晰,任何AI工具的引入都是潜在风险。
- **私域优先** 对于需要接触企业内部数据的任务,优先路由至私域AI平台处理,只有私域无法满足时才考虑经脱敏处理后调用公域AI。
- **底座统一** 用NGCC统一计算底座替代分散终端,是实现多域隔离、终端零数据和双AI助理协同的物理前提。
- **能力分层** 私域AI能力与公域AI能力分层建设、分层治理,通过双AI助理模型向员工提供统一体验。
- **全程可审计** 所有跨域数据流转、AI调用和Agent执行均留存完整审计记录,支持合规检查和事后追溯。

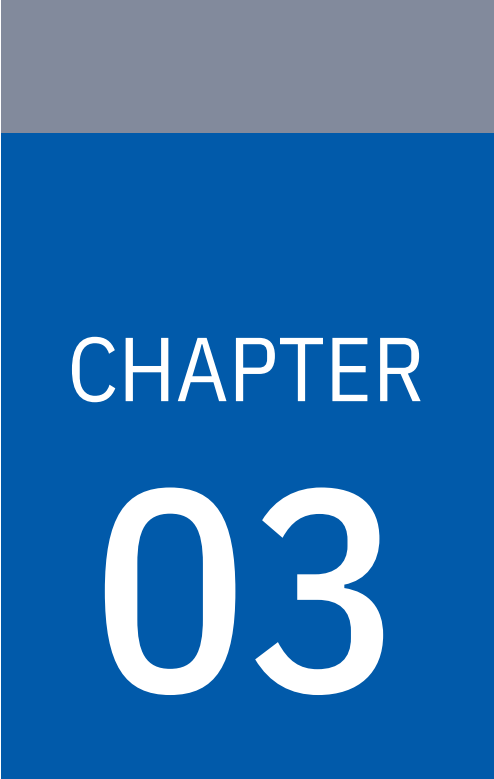


2.3 参考架构总体结构

架构组件	核心作用	在四大主权中的位置
五业务域 (S1-S5)	定义企业安全与业务边界, 明确不同数据和能力的主权归属	数据主权的边界基础
七层技术架构	定义从终端到外部生态的完整能力落位	全部四类主权的技术实现路径
NGCC统一计算底座	集中计算、多域隔离、单终端多域访问	计算主权的物理基础
企业私域AI平台	私有模型+知识库+RAG+专有Agent	AI主权的载体
双AI助理模型	员工级人机协同新范式, 私域+公域双助理	组织主权的具体表达



▲ 图1 AI时代企业计算参考架构总图



第三章
五业务域
AI时代企业安全与业务边界



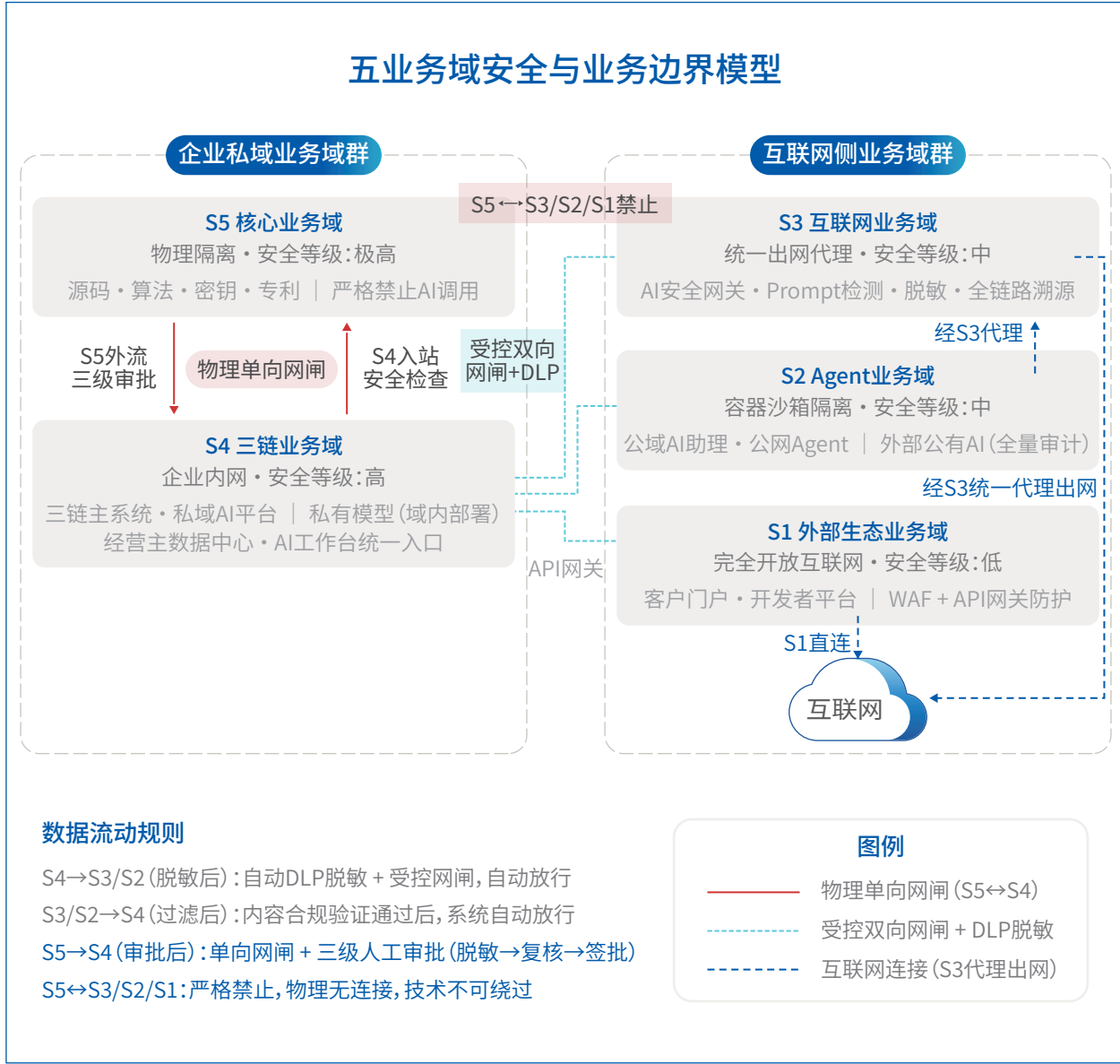
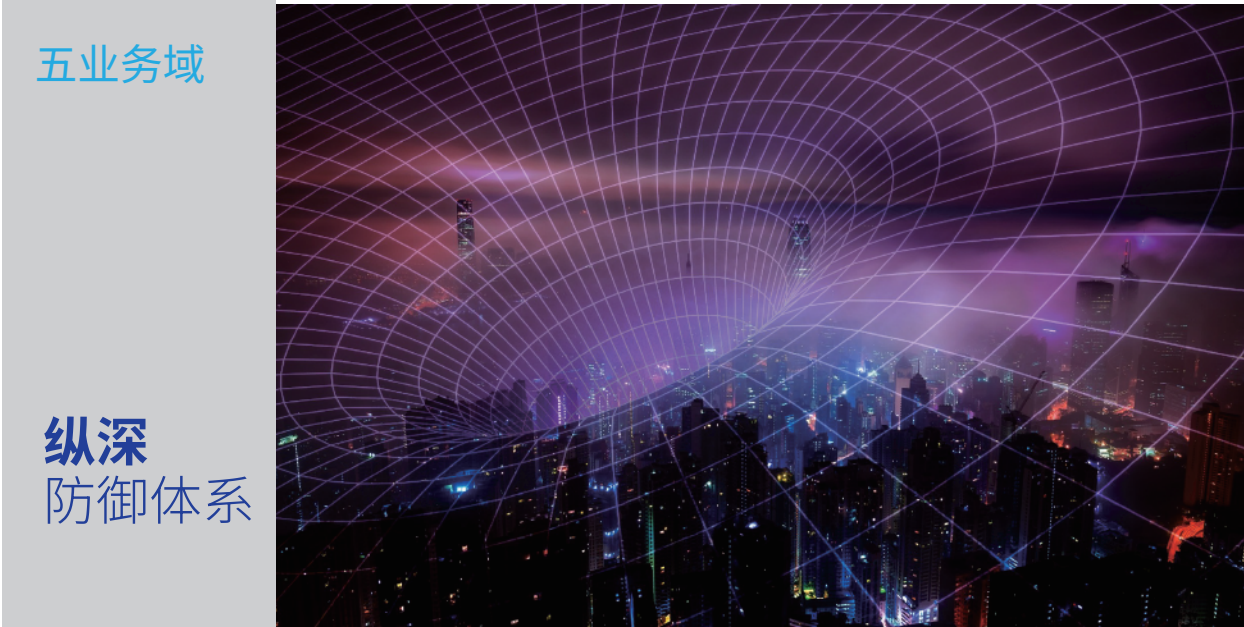
第三章

五业务域:AI时代企业安全与业务边界

3.1 五业务域总览

五业务域是本架构的核心出发点。每个域具有独立的安全信任等级、访问控制策略和AI调用权限，域与域之间通过受控网闸进行数据交换，形成纵深防御体系。

域	安全等级	典型内容	AI调用模式	对外连接
S5 核心域	极高	研发源码、核心算法、专利、密钥	严格禁止	物理隔离，无直接连接
S4 三链域	高	ERP/CRM/PLM、合同、财务、人力	私有模型（域内部署）	单向网闸与S5，受控网闸与S3/S2
S3 互联网域	中	互联网访问代理、公有模型网关	私有+外部（脱敏后）	统一出网代理，全流量审计
S2 Agent域	中	公域AI助理、公网Agent	外部公有AI（全量审计）	经S3安全代理访问公网
S1 外部生态域	低	客户门户、开发者平台、官网	公开API接口	完全开放互联网



数据流动规则

S4→S3/S2(脱敏后): 自动DLP脱敏 + 受控网闸, 自动放行

S3/S2→S4(过滤后): 内容合规验证通过后, 系统自动放行

S5→S4(审批后): 单向网闸 + 三级人工审批(脱敏→复核→签批)

S5↔S3/S2/S1: 严格禁止, 物理无连接, 技术不可绕过

图例

物理单向网闸 (S5↔S4)

受控双向网闸 + DLP脱敏

互联网连接 (S3代理出网)

▲ 图2 五业务域安全与业务边界模型

3.2 各域详细定义

S5 核心业务域 · 安全等级:极高
【定位】 企业知识财富中心, 存储最高价值的知识产权与技术资产。核心域的安全性直接决定企业的长期竞争地位。
【核心内容】 研发源码仓库 (Git私有化); 核心算法与架构文档; 密钥管理系统 (KMS) 主密钥材料; 专利与知识产权档案。
【跨域流转】 与S4:通过物理单向网闸, 向外输出须经三道审批关卡 (自动脱敏初审→委员会复核→负责人签批)。与S3/S2/S1:无任何形式直接网络连接, 物理隔离, 技术上不可绕过。

S4 三链业务域 · 安全等级:高
【定位】 收入链、产品链、支撑链核心生产系统的运行区域, 也是绝大多数员工日常工作的主要数字环境。通过私有化部署确保业务数据不离开企业管控范围。
【核心内容】 收入链: CRM、合同管理、报价系统; 产品链: PLM、需求管理、项目管理; 支撑链: ERP、HRMS、财务管理、供应链管理; AI基础设施: 企业AI工作台、私有大模型、RAG知识库。
【跨域流转】 与S5:通过单向网闸接收经审批脱敏的核心数据。与S3/S2:通过受控双向网闸交互, 业务数据进入S3前自动经过DLP脱敏处理。与S1:通过API网关向外部提供受控服务。

S3 互联网业务域 · 安全等级:中
【定位】 企业互联网访问与公有AI能力的受控中介层, 对内向S4和S2提供统一的互联网能力, 对外以安全代理身份接入各类公共AI平台, 确保敏感数据在接触AI前已完成充分脱敏。
【核心内容】 公有模型统一访问代理 (各主流大模型); AI安全网关 (Prompt注入检测+输出过滤+全链路溯源); SaaS应用统一访问代理; 出网内容脱敏与流量审计。
【跨域流转】 与S4:接受S4推送的脱敏数据后向公有AI发起调用, 向S4返回过滤后的AI响应。与S2:为S2提供经安全审计的互联网访问通道, 所有出入流量全量记录。

S2 Agent业务域 · 安全等级:中
【定位】 AI Agent自动化执行空间。Agent的自主决策与链式工具调用能力在提升效率的同时也引入了权限扩散风险, 本域通过沙箱隔离、权限硬绑定与行为全量录制来管控风险。
【核心内容】 公域AI助理运行环境; 公网研究型Agent (市场情报、竞品监控、技术趋势); 内容生成Agent; 公有模型驱动的自动化任务执行Agent。
【跨域流转】 Agent运行在独立容器沙箱, 权限随任务生命周期动态颁发和销毁。严禁Agent直接访问S4业务数据库或S5资源。所有外部调用通过Egress代理, 受白名单约束, 全程行为录制。

S1 外部生态域 · 安全等级:低
【定位】 企业面向外部世界的数字接口, 承载与客户、合作伙伴、开发者的所有交互。此域完全暴露于互联网, 通过WAF、API网关等机制确保外部访问不能突破到内部系统。
【核心内容】 客户服务门户 (产品激活、工单、知识库自助查询); 开发者API开放平台; 合作伙伴协同平台; 企业官网与市场营销站点。
【跨域流转】 通过WAF拦截OWASP Top10攻击; 通过API网关进行身份鉴权和速率限制; 所有向内部系统的数据请求须通过S4 API代理层中转, S1无法直接访问任何内部数据库。

3.3 数据流动规则

流向	是否允许	控制机制	审批要求
外部生态(S1)→S4	有条件允许	WAF+API网关+身份验证	系统自动 (实名认证通过)
S4→S3/S2 (脱敏后)	允许	自动DLP脱敏+受控网闸	自动放行, 保留审计记录
S3/S2→S4 (过滤后)	允许	结果内容过滤+受控网闸	系统自动 (内容合规验证通过)
S5→S4 (审批后)	有条件允许	单向网闸+三级人工审批	委员会复核+保密负责人双签批
S4→S5 (安全检查后)	允许	单向网闸入站+合规扫描	系统自动 (安全检查通过)
S5↔S3/S2/S1	严格禁止	物理无连接, 技术不可绕过	无审批路径 (禁止操作)



CHAPTER 04

第四章

七层技术架构

AI时代企业计算能力实现方式



第四章
七层技术架构:AI时代企业计算能力实现方式

4.1 七层技术架构总览

层次	层名称	核心技术能力	对应业务域
第一层	终端访问层	云PC客户端、零信任接入、统一身份认证、多域切换界面	S4/S3/S2(入口)
第二层	云PC计算基础设施层	NGCC统一计算底座、智能调度、多域隔离、集中存储	S4/S3/S2(基础设施)
第三层	企业业务与数据中心层	ERP/CRM/PLM等三链系统、数据中台、BI看板、主数据管理	S4核心区域
第四层	企业私域AI平台层	私有大模型集群、企业知识库、RAG引擎、AI工作台、私域Agent	S4 AI基础设施区
第五层	互联网访问与安全代理层	公有模型访问代理、AI安全网关、DLP脱敏引擎	S3核心区域
第六层	公有AI Agent执行层	公域AI助理运行环境、公网Agent沙箱平台	S2核心区域
第七层	外部生态服务层	客户门户、API开放平台、WAF+API网关防护	S1核心区域



▲ 图3 七层技术架构总图

4.2 关键层次详解

- **第二层:NGCC / 邦彦云PC统一计算底座**
NGCC是整个架构的物理基础。其核心价值在于:计算从终端迁移到云端(收回计算主权);终端本地无数据存储(消除终端泄漏风险);单一终端安全访问多个隔离域(消除多设备切换成本);统一的身份认证与行为审计(支撑零信任架构)。
- **第四层:企业私域AI平台**
私域AI平台是企业AI主权的核心载体,包含私有大模型推理集群、企业知识库与RAG体系、私域专有Agent和企业AI工作台。其核心价值是:让AI在"看不见核心数据"的前提下,依然能为业务提供高质量的智能服务——私有模型只处理已脱敏数据,企业知识库中的内容按权限分级访问。
- **第五层:互联网访问与安全代理层**
这一层是企业内部系统与公网AI能力之间的"受控闸门"。AI安全网关提供Prompt注入检测、输入数据二次脱敏、输出内容过滤和全链路溯源四项核心能力,确保企业员工调用公有模型时,敏感数据不会以任何形式出现在发出的请求中。

CHAPTER
05

第五章
NGCC / 邦彦云PC
AI时代企业统一计算底座

第五章

NGCC / 邦彦云PC:AI时代企业统一计算底座

5.1 NGCC的定义与产业定位

NGCC (Next Generation Commercial Computer, 下一代商用计算机) 是邦彦技术自主研发的新一代企业计算基础设施。它不是传统PC的功能升级, 也不是普通的VDI (虚拟桌面基础架构), 而是以"计算位置从桌面迁移到云端"为核心设计理念的结构革命。在NGCC架构下, 员工终端仅作为显示和输入设备, 所有计算、存储、网络处理均在云端NGCC基础设施中完成, 终端本地无任何有价值数据留存。



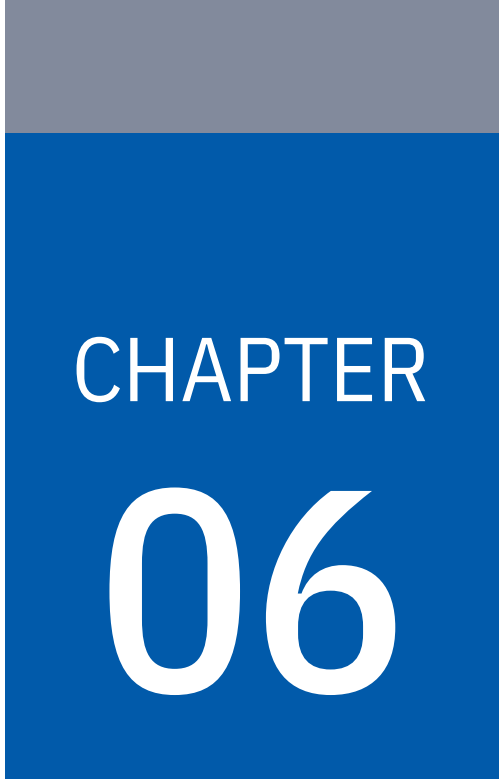
▲ 图4 NGCC统一计算底座示意图

5.2 NGCC与传统VDI的本质区别

维度	传统VDI	NGCC
设计目标	桌面集中化管理, 降低运维成本	计算主权回收, 多域隔离, AI时代统一计算底座
安全设计	以桌面管理为主, 安全是附加能力	以多域隔离和零信任为核心, 安全是首要设计目标
多域访问	通常单一网络环境	单终端同时访问多个物理隔离网络域, 无需多台设备
AI集成	无原生AI集成能力	原生支持私域AI平台和公域AI安全代理的统一接入
终端数据	可能有本地缓存	终端零数据, 技术层面保证数据不落地

5.3 NGCC的四大结构价值

- **计算主权回收** 计算发生在企业自主管控的云端基础设施, 而不是难以治理的分散终端。企业对计算环境拥有完整的管理权和审计权。
- **终端零数据** 技术层面保证终端本地无任何有价值数据存储。员工离职、终端丢失或被攻击, 均无法从终端侧获取企业核心数据。
- **多域隔离访问** 单一终端可安全接入S5、S4、S3、S2等多个网络域, 各域之间计算资源、网络通信和数据存储严格隔离。研发人员可在一台终端上同时处理研发工作和查阅外部资料, 两个环境物理隔离、互不影响。
- **AI协同基础** NGCC为私域AI助理和公域AI助理提供统一的运行基础设施, 使双AI助理模型的落地成为可能——员工在单一工作环境中即可与两个AI助理无缝协同。



第六章

企业私域AI平台

内部智能能力中枢



第六章

企业私域AI平台:内部智能能力中枢

6.1 为什么企业必须拥有私域AI平台

如果企业没有私域AI平台,员工使用AI的唯一方式就是直接访问公有模型。这意味着:所有业务数据必须发送到外部服务器;企业知识无法沉淀为可被AI调用的私有资产;AI使用行为无法统一审计和管控。私域AI平台的本质是:让AI在企业内部运行,而不是让企业数据去AI平台。

6.2 私域AI平台核心组件

组件	核心功能	建设优先级
企业AI工作台	员工访问AI能力的统一入口,整合私域和公域AI能力	最高(先建统一入口)
企业知识库	制度文档、产品手册、研发记录等企业知识的结构化存储	高(支撑RAG的基础)
RAG检索引擎	基于向量检索的企业知识增强系统	高(与知识库同步建设)
私有大模型	部署于企业私有基础设施的大模型,仅处理企业内部数据	高(核心AI能力载体)
私域专有Agent	针对三链典型业务场景的专用Agent	中(平台稳定后建设)

6.3 私域AI平台的安全设计原则

- **知识分级访问** 知识库内容按数据安全等级分级标注,不同权限员工只能检索到权限范围内的知识条目, AI工作台在生成响应时自动过滤超权内容。
- **私有模型部署** 私有模型完全运行在企业私有GPU集群上,推理过程不产生任何出网流量,模型版本受企业统一管理,更新前进行安全评估。
- **调用全链路溯源** 每次AI调用生成唯一请求ID,关联用户身份、所属部门、调用模型版本、输入输出内容摘要,支持事后审计和责任认定。

CHAPTER

07

第七章

互联网访问与公有AI能力体系



第七章

互联网访问与公有AI能力体系

7.1 为什么必须区分私域AI与公域AI

很多企业在引入AI时面临两个极端：完全禁止使用公网AI (导致效率损失, 员工私下绕过管控) ;或完全不加管控地使用公网AI (导致数据失控)。本白皮书提出的方案是第三条路：建立受控的公域AI能力体系, 让员工在企业统一管控下安全使用公网AI能力。

7.2 AI安全网关:公域AI访问的核心控制点

AI安全网关部署于第五层 (互联网访问与安全代理层), 是企业内部系统与公网AI平台之间所有流量的必经节点, 提供四项核心安全能力：

- **输入脱敏** 对Prompt内容进行二次语义扫描, 采用语义理解+正则匹配+代码特征检测三重验证机制, 确保敏感信息不随AI请求出网。
- **Prompt注入检测** 识别隐藏在业务数据中的恶意AI指令, 支持多种已知注入模式检测, 置信度低于阈值的请求自动路由至人工复核队列。
- **输出内容过滤** 对公有模型返回内容进行合规性检测, 过滤包含幻觉性敏感信息或不当内容的响应。
- **全链路溯源** 每次公域AI调用生成唯一请求ID, 关联完整调用链路, 支持分钟级事件溯源和取证分析。

7.3 公有AI Agent执行层 (S2)

公有AI Agent执行层 (S2业务域) 专门承载需要访问互联网或调用公有大模型的Agent任务。S2与S4之间严格隔离, Agent在S2中执行公网任务, 成果经审查后再推送至S4的业务系统。典型应用包括：市场情报自动化搜集与汇总、竞品动态监控、行业政策跟踪、外部技术趋势研究等。

第八章
双AI助理模型
AI时代员工的人机协同新范式



第八章
双AI助理模型:AI时代员工的人机协同新范式

8.1 双AI助理模型的提出背景

企业员工的工作天然分为两类:处理企业内部数据、知识和流程(需要访问受保护的内部系统);以及获取外部信息、调用公有AI能力、执行公网任务(需要访问互联网和公有模型)。这两类任务对数据安全的要求截然不同,不能由同一个AI助理承担。双AI助理模型正是基于这一洞察而设计。

8.2 双AI助理的定义与职责分工

维度	私域AI助理	公域AI助理
运行环境	S4企业私域AI平台(私有GPU集群)	S2公有AI Agent执行层(公网沙箱)
能力来源	企业私有大模型+企业知识库+RAG	公有大模型API(各主流大模型)
可见数据	企业内部数据(按权限分级)	仅脱敏后数据和公开信息
典型任务	企业知识问答、内部文档分析、业务数据解读、三链流程辅助	互联网信息研究、竞品分析、技术趋势汇总、公开内容生成
安全管控	企业AI工作台统一调度,数据不出企业网络	AI安全网关全量审计,出入内容脱敏+过滤



▲ 图5 双AI助理模型映射图

8.3 员工标准智能协作单元的重新定义

双AI助理模型将AI时代的员工标准工作单元,从"人"重新定义为:

 人类员工 +  私域AI助理 +  公域AI助理

在这一协作单元中,人类员工负责判断、决策和关系管理;私域AI助理负责内部知识调用、数据分析和流程辅助;公域AI助理负责外部信息获取、公有模型调用和公网任务执行。三者通过企业AI工作台在统一界面下协同,员工无需关注底层安全隔离机制。

CHAPTER

09

第九章

三链体系与AI时代企业运行方式

第九章
三链体系与AI时代企业运行方式

9.1 三链体系的架构意义

三链体系(收入链、产品链、支撑链)是企业价值创造的核心框架。在AI时代,三链不仅是业务流程的组织方式,也是AI能力嵌入的主要载体。

业务链	核心流程	私域AI主要赋能点	公域AI主要补充点
收入链	行业洞察→线索评分→方案生成→合同审批→交付→售后	客户画像、CRM商机汇总、合同风险审查、回款预警	招标信息抓取、竞品动态监控、行业政策跟踪
产品链	需求管理→设计评审→研发实现→测试验收→发布运营	需求解析、代码审查辅助、测试用例生成、缺陷分析	开源框架研究、公开论文汇总、安全漏洞情报
支撑链	战略规划→财务预算→人力→采购供应链→IT运营	预算执行解释、成本趋势分析、人效数据汇总	宏观政策跟踪、薪酬市场对标、原材料价格趋势

9.2 从"系统驱动"到"人机协同驱动"

传统企业运行方式是"人操作系统,系统记录结果"——员工是系统的操作者,系统是业务的记录工具。AI时代的企业运行方式正在转变为"人与AI协同,系统作为执行基础"——员工是业务的判断者,AI是信息处理和任务执行的合作伙伴,系统提供数据和执行能力。五业务域确保AI在安全边界内运行;双AI助理模型定义员工与AI的协作方式;三链体系提供AI嵌入的业务场景框架;NGCC提供安全协同的物理计算基础。



第十章
安全机制
从网闸隔离到AI治理



第十章

安全机制:从网闸隔离到AI治理

10.1 跨域隔离体系

- **物理单向网闸(S5↔S4)** 采用硬件实现的单向隔离网闸, S4单向流向S5, 物理电路层面保证数据只能按规定方向流动。即使软件层被攻陷, 也无法实现反向数据传输。
- **受控双向网闸(S4↔S3)** 可允许采用两个单向隔离网闸进行单向数据流动, 但所有出站数据须通过DLP引擎脱敏处理, 入站数据须经内容安全扫描, 所有操作留存完整审计日志。
- **代理访问(S3↔互联网)** S3通过统一出网代理连接互联网, 所有出站Prompt经AI安全网关处理, 所有入站响应经内容过滤后返回。
- **容器沙箱隔离(S2内部)** Agent在独立容器沙箱中运行, 系统调用受策略过滤, 网络访问受白名单约束, 文件系统访问受严格限制。

10.2 AI专项安全机制

威胁类型	主要防护机制	技术实现层次
Prompt注入攻击	AI安全网关注入检测(规则库+分类器)+私有模型越狱防御训练	第五层 互联网访问与安全代理层
数据外泄(主动)	终端零数据+DLP三重检测+出境审批 workflow+员工行为审计	第一/二层+各域边界
数据外泄(被动)	私有模型全部在企业内网运行+公有模型调用强制脱敏	第二/四/五层
Agent权限扩散	JIT动态授权(任务生命周期绑定)+容器沙箱硬限制+越界自动熔断	第六层 S2 Agent域
供应链攻击	第三方组件成分分析+代码签名验证+沙箱隔离运行	第二/四/六层
内部人员威胁	最小权限原则+全量行为审计+异常基线检测+三权分立	全域统一管控

10.3 合规与审计框架

- **等保2.0三级** 五域隔离架构满足安全区域边界要求;RBAC/ABAC满足访问控制要求;WORM不可篡改日志满足安全审计要求;全链路国密加密满足数据保密性要求。
- **数据安全法/个保法** 数据分级分类体系满足分类分级保护要求;S5物理隔离满足重要数据保护要求;出境三级审批满足数据出境安全评估要求。
- **生成式AI管理暂行办法** AI安全网关内容过滤满足内容安全要求;全量AI调用日志(建议留存不少于12个月)满足使用记录留存要求。

CHAPTER

11

第十一章

典型应用场景



第十一章

典型应用场景

以下八个典型场景展示了五业务域架构和双AI助理模型在不同业务部门的具体落地方式。

场景 1 | 研发场景:AI辅助核心算法优化

- **核心痛点** 研发工程师希望借助AI分析核心算法代码的性能瓶颈,但代码属于最高安全级别资产,不允许以任何形式离开核心域。
- **架构方案** 工程师在AI工作台打开代码助手→DLP自动识别代码敏感特征→结构化脱敏(保留代码框架,替换具体实现逻辑)→脱敏后的"结构骨架"提交至S4私有模型→获得基于最佳实践的优化建议→工程师在核心域本地参考建议自行实现,原始代码全程未离开S5。
- **业务价值** 核心算法实现零外泄;工程师获得有价值的性能优化指导;全程操作留存完整审计日志。

场景 2 | 销售场景:AI生成大客户定制化技术方案

- **核心痛点** 销售团队需要在短时间内完成高度定制化的技术方案,传统方式严重依赖少数核心售前人员,效率瓶颈明显。
- **架构方案** 销售经理在AI工作台创建"方案生成"任务→私域AI助理从RAG知识库检索产品规格、成功案例摘要和架构模板→调用私有模型生成方案初稿(全程在S4内)→售前协同批注修改→DLP确认无超级别内容→审批后加密发送至客户。公域AI助理同步在S2中搜集客户行业信息和竞品动态供销售经理综合参考。
- **业务价值** 方案生成效率大幅提升;内容安全全程DLP覆盖;内外部信息有机融合,方案质量更高。

场景 3 | 财务场景:智能经营分析与预警

- **核心痛点** 财务部门大量数据分散在多个系统,跨系统经营解释依赖大量人工整理,管理层难以快速获取经营洞察。
- **架构方案** 财务人员在AI工作台以自然语言提问(如"本季度某产品线利润率为何下降")→私域AI助理联动ERP财务数据、回款情况、供应链成本、项目延期数据→生成结构化经营解释报告→财务人员审核确认。全程数据在S4私域AI平台处理,不调用任何外部AI。
- **业务价值** 财务工作从"数据搬运"升级为"经营洞察生产";分析响应时间从数小时缩短到分钟级;数据安全完全可控。

场景 4 | 供应链场景:智能预测与异常预警

- **核心痛点** 供应链同时受销售预测、研发BOM变化、成本和库存多重因素影响,传统人工方式难以实现实时预测和主动预警。
- **架构方案** 私域供应链AI助理持续分析ERP/SCM中的需求预测、物料齐套、库存健康度,自动生成预警报告和排程建议。公域供应链AI助理在S2中实时监控公开供应商信息、原材料价格趋势和物流风险,将外部风险信号推送至供应链团队。
- **业务价值** 供应链从"被动响应订单"升级为"主动感知风险";内外部信息融合提升预测准确度。

场景 5 | 法务合规:智能合同审查

- **核心痛点** 法务部门每月处理大量合同,核心工作是识别非标条款和法律风险,传统人工逐一审阅效率低且一致性差。
- **架构方案** 合同上传至S4合同管理系统→私域AI助理提取结构化文本,与标准模板库和历史风险案例对比→生成逐条风险报告(红/橙/绿三色高亮)→法务人员对AI分析结果进行确认和修改。全程在S4私域AI平台处理,满足保密协议要求。
- **业务价值** 初审工作量大幅降低;风险识别一致性提升;法务人员精力集中于复杂风险判断和谈判策略。

场景 6 | 人力资源:组织能力建设支持

- **核心痛点** HR部门不仅需完成传统事务管理,还需思考哪些岗位适合AI增强、如何设计人机协作模式,传统工具无法支撑此类分析。
- **架构方案** 私域HR AI助理分析企业内部人员结构、人效数据、培训记录,辅助生成岗位说明书草稿、人力需求分析和梯队报告。公域HR AI助理在S2中跟踪人才市场趋势、薪酬对标数据和劳动法规动态。
- **业务价值** HR从"事务管理"升级为"组织能力建设支持";岗位设计充分考虑AI增强因素;人才策略更科学。

场景 7 | 高安全行业客户:既要AI效率,又要数据主权

- **核心痛点** 政务、金融、能源、医疗等高安全行业,既需AI提升效率,又有极高数据安全和合规要求,两者看似矛盾。
- **架构方案** S5+S4构成高安全私域体系,核心业务数据和AI交互全程不出企业网络;NGCC保证终端零数据和多域隔离;私域AI平台在满足等保要求的受控环境内提供AI能力;S3/S2的安全代理机制允许在边界清晰的前提下使用公域AI能力。
- **业务价值** 既拥抱AI,又不牺牲数据主权与合规要求;架构天然满足等保2.0三级要求;可作为向同类行业客户输出的参考方案。

场景 8 | 科技型企业整体改造:从传统IT走向AI时代计算体系

- **核心痛点** 大量科技型企业已有较完整的系统基础,但AI使用零散、出网不可控、员工工作方式未升级,需要系统性改造。
- **架构方案** 按照"底座先行、边界先立、能力渐进、组织跟进"的五阶段路线:先用NGCC收回计算主权→按五业务域划清边界→在S4建设私域AI平台→建立互联网访问与公有AI能力体系→最终推行双AI助理模型,重构员工工作方式。
- **业务价值** 改造结果不是"多上一套AI系统",而是把企业整体运行方式切换到AI时代,实现效率与安全的统一。

第十二章
企业建设与改造路线图



第十二章
企业建设与改造路线图

12.1 总体建设思路

企业AI时代计算体系建设必须坚持渐进路线,正确的建设顺序是:
底座先行 → 边界先立 → 能力渐进 → 工作方式跟进。

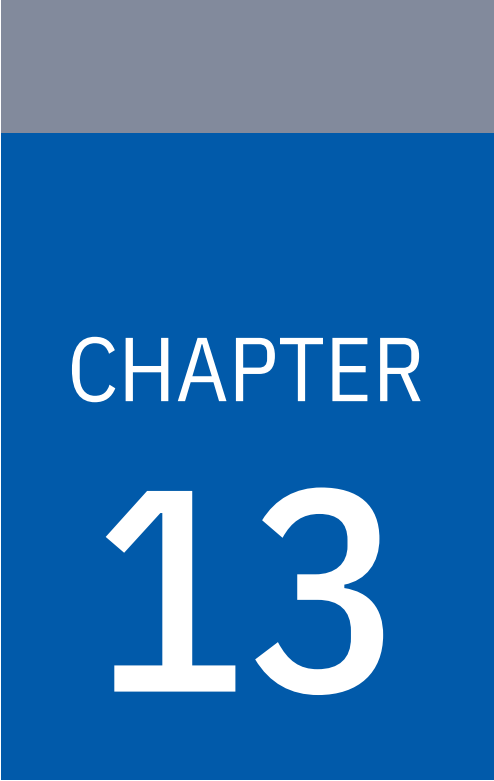
阶段	核心目标	主要建设任务	验收标准
第一阶段 统一计算底座	把企业计算主权从分散终端收回到云端底座	建设NGCC/云PC基础平台、统一身份认证、终端接入体系;完成高安全岗位的云PC迁移试点	建立统一计算底座;关键岗位实现一端多域访问试点
第二阶段 划清业务边界	建立五业务域结构,明确主权边界	完成五业务域总体划分、数据分级分类体系、业务系统归属映射、域间连接规则规划	企业有正式五业务域定义;S5/S4与S3/S2/S1的边界已建立
第三阶段 建设私域AI	在S4之上构建企业私域智能中枢	按"先知识体系→再私有模型→再AI工作台→再私域Agent"顺序建设私域AI平台	企业有统一私域AI工作台;关键知识库可被AI调用
第四阶段 释放公域AI	在私域能力稳定后,统一纳入公域AI访问能力	建设S3互联网访问与安全代理层、AI安全网关、S2公有AI Agent执行层	公有模型访问实现统一代理;公域AI助理有独立运行环境
第五阶段 重构工作方式	让AI真正转化为员工日常工作方式	定义岗位级双AI助理配置;将AI工作方式写入岗位模型;将AI使用纳入绩效和培训体系	关键岗位形成双AI助理工作模式;员工AI使用从"尝试"走向"依赖"



▲ 图6 企业建设与改造五阶段路线图

12.2 三个常见误区

- **误区一:先上模型,再谈架构** 在没有划定五业务域、定义数据边界和建设统一入口之前,先购买GPU和大模型,导致AI快速失控或被边缘化。正确顺序是先建底座和边界,再建AI能力。
- **误区二:只做私域,不管公域** 只建私域AI平台而不建设受控的公域访问体系,员工会在架构外自行使用公网AI,反而形成更难管控的灰色地带。
- **误区三:只建平台,不改组织** 平台上线后不将AI能力落实到岗位、流程、培训和绩效体系,平台的技术能力无法转化为组织实际效率提升。



第十三章
产业价值与未来展望



第十三章 产业价值与未来展望

13.1 从产品到企业计算方法论

本白皮书提出的架构，其意义已超越单一产品的范畴。它不是在推荐某个软件工具或某个模型，而是给出了一套结构性解法：用五业务域解决业务与安全边界问题，用七层技术架构解决能力落位问题，用NGCC解决统一计算底座问题，用私域AI平台解决内部智能沉淀问题，用双AI助理模型解决员工工作方式升级问题。

13.2 NGCC的产业定位升级

通过本白皮书的完整架构论述，NGCC的产业表达已从“云PC产品”上升为“AI时代企业统一计算基础设施”。NGCC同时服务于五业务域、七层技术架构、企业私域AI平台、公有AI Agent执行层和双AI助理模型，成为整套方法论的物理基础。基于这一定位，邦彦的市场方式也相应从“销售产品”转变为“输出企业计算方法论”。

13.3 三阶段演进路线

- **第一阶段(近期):企业内部架构成立** 当前,这套架构首先服务于企业自身的信息系统建设和AI平台建设,在实践中持续验证和完善各组件的技术实现细节。
- **第二阶段(中期):企业级解决方案形成** 随着内部实践成熟,将架构抽象为面向客户的解决方案,包括企业AI计算总体方案、五业务域规划方案、NGCC统一计算底座方案、私域AI平台方案和双AI助理工作方式方案。
- **第三阶段(远期):行业参考架构输出** 进一步成为高安全行业参考架构和科技型企业AI转型参考架构,从“提供产品和项目”走向“定义企业AI时代计算架构的方法论与行业语言”。



附录

核心术语表 · 架构映射表 · 参考标准

附录A 核心术语表

术语	英文/缩写	定义
下一代商用计算机	NGCC	邦彦技术研发的新一代企业计算基础设施,以"计算从终端迁移到云端"为核心理念,提供集中计算、终端零数据、多域隔离和单终端多域访问能力
五业务域	Five Business Domains	将企业信息系统按安全等级和业务属性划分为S5-S1五个独立域,每个域具有独立的访问控制策略、AI调用权限和跨域数据交换规则
双AI助理模型	Dual-AI Assistant Model	为员工配置私域AI助理和公域AI助理的人机协同范式,形成"人类员工+私域AI助理+公域AI助理"的标准智能协作单元
企业私域AI平台	Enterprise Private AI Platform	部署于企业私有基础设施的AI能力中枢,包含私有大模型、企业知识库、RAG检索引擎、AI工作台和私域专有Agent
AI安全网关	AI Security Gateway	部署于互联网访问层的专用安全控制点,提供Prompt注入检测、输入脱敏、输出内容过滤和全链路溯源四项核心功能
单向隔离网闸	Data Diode	仅允许数据单方向流动的硬件安全设备,通过物理电路设计在硬件层面消除反向通信可能性
检索增强生成	RAG (Retrieval-Augmented Generation)	将向量数据库语义检索与大模型生成结合的AI架构,使模型在推理时能动态检索企业知识库中的最新知识
即时授权	JIT (Just-in-Time Provisioning)	在需要时才动态颁发临时权限凭证,任务完成后立即撤销,消除长期静态权限积累带来的权限扩散风险
三链体系	Three-Chain System	企业价值创造的核心框架,包含收入链(市场到回款)、产品链(研发到交付)和支撑链(财务/人力/供应链等)

附录B 五业务域安全等级与架构映射

域	名称	安全等级	互联网连接	AI调用策略	对应技术层
S5	核心业务域	极高	物理隔离,无法直连	禁止任何AI直接调用	无(物理隔离)
S4	三链业务域	高	仅通过S3代理访问	私有模型(域内部署)	第三层+第四层
S3	互联网业务域	中	统一出网代理,全流量审计	私有+外部(脱敏后)	第五层
S2	Agent业务域	中	经S3安全代理,白名单约束	外部公有AI(全量审计)	第六层
S1	外部生态域	低	完全开放互联网	公开API接口	第七层

附录C 参考标准与法规

类别	名称 / 编号	与本架构的关联
国家标准	GB/T 22239 网络安全等级保护基本要求 (等保2.0)	第十章 合规框架——等保三级系统建设的核心依据
国家标准	GB/T 20279 网络和终端隔离产品安全技术要求	单向隔离网闸选型与评估依据
国家标准	GB/T 37964 个人信息去标识化指南	数据脱敏技术规范依据
密码标准	GM/T 0002/0003/0044 (SM4/SM2/SM9)	全链路国密加密实现依据
法律法规	中华人民共和国数据安全法 (2021年施行)	数据出境管理与分级保护法律依据
法律法规	中华人民共和国个人信息保护法 (2021年施行)	个人信息DLP与访问控制法律依据
法律法规	生成式人工智能服务管理暂行办法 (2023年施行)	AI服务合规与使用记录留存依据
国际框架	NIST SP 800-207 零信任架构	零信任设计原则的国际最佳实践参考
行业规范	OWASP LLM AI Security Top 10 (2025版)	AI安全威胁分类与防护措施的行业参考

文档版本信息

版本	发布日期	说明
版本 1.0	2026年3月28日	本白皮书第一版，完整阐述构建"计算主权、数据主权、AI主权、组织主权"统一的新一代企业计算体系，经邦彦技术内部审核发布。

邦彦技术股份有限公司
BANGYAN TECHNOLOGY CORP., LTD.
版权所有 © 2026