解决方案简介

京东云与英特尔以可信计算助力 TalkingData 构建安全岛平台 提供高安全性、合规性的数据服务

在数字经济的发展中，大数据平台已经成为企业拓展数据挖掘、预测分析、消费者画像等应用，进而洞悉消费者需求、驱动业务创新的重要方式。要充分发挥大数据平台的价值，联动多源数据，并盘活数据、实现数据的高自由度至关重要，但是，当前复杂的网络安全环境又意味着，数据在流动的过程中，随时可能出现数据泄露的隐患，给企业带来数据资产流失、品牌声誉受损、合规性遭受质疑等诸多风险。

北京腾云天下科技有限公司（TalkingData）依托以“数据智能平台（SmartDP）”为核心的完整数据应用体系，构筑了一套以数据商业化平台、数据服务平台，及数据合作平台为核心的数据生态。为了化解数据融通、应用过程中可能出现的数据安全风险，京东云与英特尔助力 TalkingData 构建了基于可信计算（TEE）的安全岛及数据融通方案，通过使用英特尔® Software Guard Extensions（英特尔® SGX）技术，实现数据在安全可信基础上的更好地进行产业应用与价值挖掘。

“营销场景中数据红利价值发挥的重要前提就是安全，特别是在个人信息保护法、数据安全法等法律法规相继施行的背景下，数据安全更是成为事关企业数据战略成败的关键。通过与英特尔、京东云等伙伴合作，我们以安全岛、数据半岛、隐私安全计算等方式，以数据‘连接’而不是‘拥有’的理念，在安全合规的前提下赋能业务增长。”

— 孙永兵
TalkingData 首席数据产品专家

数据价值挖掘的安全隐忧

数据已经被广泛认为是企业最重要的资产之一，并成为企业增长的关键助推器。但是，对于企业而言，数据价值挖掘却普遍面临相当大的障碍，媒体数据封闭、数据链路断裂、品牌广告效果缺乏量化评估等都可能导致企业的数据战略无法达到预期的效果。

TalkingData 数据平台应运而生，不仅提供了一个开放、兼容、性能强大的大数据平台，而且能够支持企业进行数据收集、管理、挖掘和预测分析，快速实现用户标签梳理、用户画像和精准广告营销，进而实现大数据的变现能力和业务的不断创新。TalkingData 为支持传统行业企业进行私有化部署的第一方大数据管理平台（TalkingData DMP），能够整合企业自身所有渠道的用户行为数据，并能接入企业已有的 CRM 数据、数据仓库数据和 TalkingData 第三方的标签数据，形成 360 度用户视图。

该解决方案能够帮助企业全面了解消费者、挖掘高价值消费者、优化媒介投放策略与执行。但是，实现上述目标的前提是数据合规与安全，传统数据服务模式会存在如下安全问题：

- 传统方案采用数据直接交付的方式，存在个人数据泄露的可能。在《网络安全法》、《数据安全法》、《个人信息保护法》等法律法规相继落地的今天，严格的法律规定对企业的合规性提出了更高的要求；

- 在数据直接交付模式中，数据交付后脱离数据服务方控制，这导致企业对于高价值数据的共享存在顾虑，数据服务方无法依靠高质量的数据持续形成有保障的收入规模；
- 在实现数据交付时，需求方需要提供查询的 ID 给到数据服务方，这样会存在泄漏需求方商业秘密风险，泄漏自己的高质量客户规模与具体客户信息；
- 传统方案项目制、手动、非标准化的交付，造成数据的授权、流动、使用不能做到完全的可追溯、可审计，无法通过技术手段有效地保障数据安全。

上述问题影响了数据的流通和融合，也凸显了隐私计算在联合营销场景的重要价值。中国信通院发布的《隐私计算白皮书（2021 年）》显示，联合营销是当前隐私计算的第二大应用场景，占比达到 27%[1]，其可以帮助机构在不输出原始数据的基础上共享各自的用户数据进行营销模型计算，根据建模结果制定营销策略，实现双赢。

在此背景下，TalkingData 希望通过隐私计算等技术的应用，找到一条高效的数据安全保护之道，能够尽可能地降低数据安全风险，同时化解数据服务方、需求方的顾虑，进而形成良好的数据应用生态，促进产业发展。

集成京东云安全环境以及英特尔 SGX 的 TalkingData 安全岛解决方案

为了化解数据服务中的安全风险，TalkingData 与京东云合作，推出了 “TalkingData 安全岛” 解决方案。该方案是一套基于领先的隐私安全计算技术，实现多方数据的融通、以及价值的挖掘和流通的系统平台，可针对业务需求方的业务需求场景，提供第三方中立可信的安全计算环境以及一站式隐私保护和数据安全保障服务。

通过该平台，数据提供方能够保证所提供数据源的合法合规性、获得数据主体授权，向平台数据集市开放数据字典与样例数据，并履行数据合约；业务需求方具有对自身运用数据搭建算法模型的知识产权，可以合法合规使用数据提供方的数据；增值服务方提供透明的、可监管和审计的服务，例如算法、模型等。

“TalkingData 安全岛” 平台集成了京东云安全环境以及英特尔 SGX 可信计算平台。可信计算是在计算和通信系统中广泛使用基于硬件安全模块支持下的可信计算平台，以提高系统整体的安全性。可信计算空间（TEE）是主处理器内的安全区域，它保证内部加载的代码和数据在机密性和完整性方面受到保护。

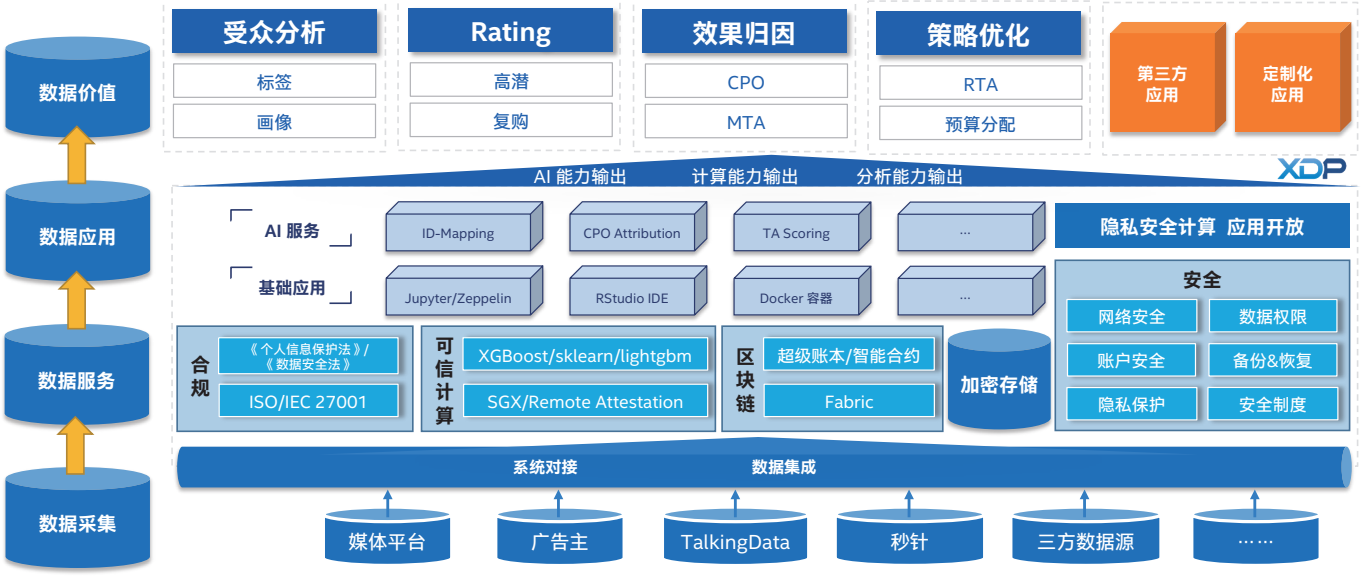

图 1. TalkingData 安全岛平台整体架构

[1] https://www.sohu.com/a/478870037_121124365

TEE 作为一个独立的执行环境，提供了诸如隔离执行、与 TEE 一起执行的应用程序的完整性以及其数据的机密性等安全特性。

英特尔 SGX 能够通过应用程序隔离技术，帮助保护使用中的数据。通过保护选定的代码和数据免遭修改，开发人员可以将他们的应用程序分隔到强化的安全区或受信任的执行模块，以帮助提高应用程序的安全性。例如，开发者可以把应用程序划分到 CPU 强化的 Encalve（飞地）中或者内存中可执行的保护区域，即使在受攻击的平台中也能提高安全性。使用这种新的应用层可信执行环境，开发者能够启用身份和记录隐私、安全浏览和数字管理保护（DRM）或者任何需要安全存储机密或者保护数据的高保障安全应用场景中。

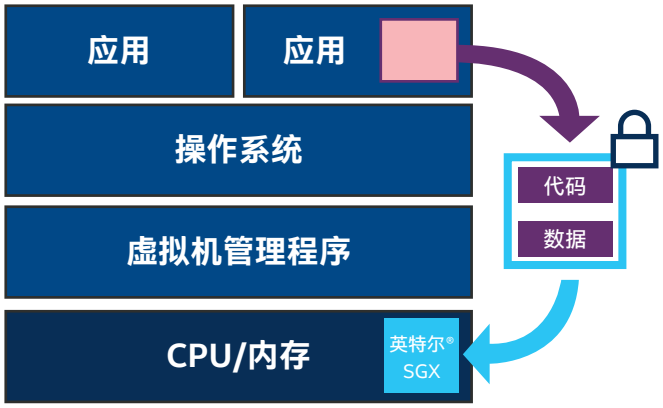

图 2. 英特尔 SGX 能够提升数据的安全性

该方案集成的京东云安全环境提供了远程可信安全验证服务，用于验证、监控、及管理 SGX 可信执行环境，确保 SGX 可信执行环境内的代码和数据可以被远程审计及验证，保障 TEE 方案在逻辑上的安全性。

企业数据与 TalkingData 数据在进行动态加密之后，会将加密数据上传到该可信计算平台，可信计算平台在可信计算安全硬件中会运行三方标签增补、ID-Mapping、TA Scoring 模型、CPO 报告等应用，使用时通过 TLS 链路获得数据解密秘钥，数据的解密及运行过程均在 TEE 上进行，保证数据不出硬件环境，最大限度地保证用户及参与方的数据安全。

为数据服务带来可信计算的安全 “屏障”

集成京东云安全环境以及英特尔 SGX 的 TalkingData 安全岛解决方案能够有效解决数据服务中，数据提供方、数据需求方、算法方、渠道方等多方的安全顾虑，在安全可信的环境下实现数据的融合互通。

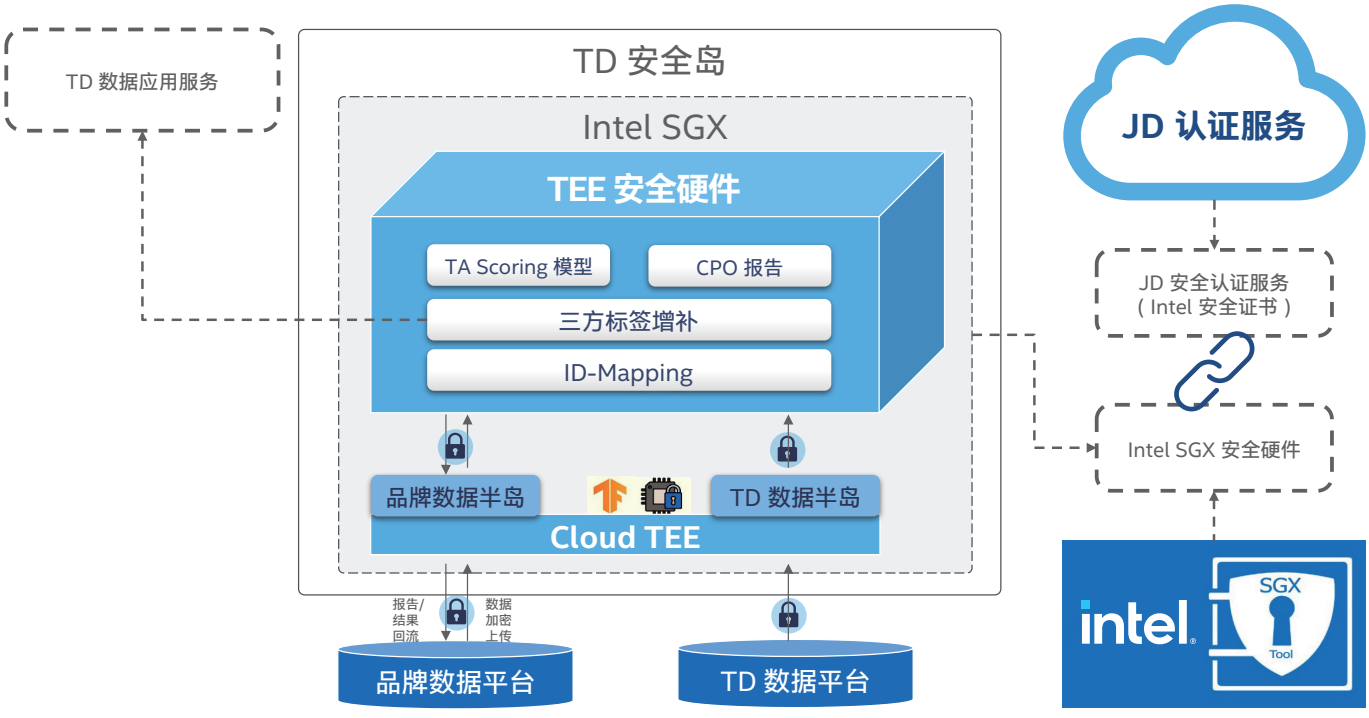

图 3. TalkingData 安全岛平台安全交付示意图

得益于安全可信能力的集成，TalkingData 安全岛平台提供了如下优势：

- **平台化：**在平台范围内提供了多方管理能力，形成数据流通生态闭环，实现数据收集、治理、服务、计算在云端的数据全生命周期管理。
- **合规化：**已获取合法授权的数据会在脱敏加密后进入平台进行处理，全程保证数据可用而不可见，原始数据不被泄露，能够满足合规性的需求。
- **线上化：**提供了便捷的线上操作流程，企业能够通过全套云安全技术及隐私安全计算技术，实现安全的线上应用。

目前，TalkingData 安全岛解决方案已经在零售、快消等行业领域得到了广泛应用。以某食品行业标杆企业为例，该企业通过安全岛平台实现基于安全可信环境的 ID-Mapping，构建了用户标识体系，联动公域媒体广告触达数据和商品购买数据，同时为一方会员和购买人群补充第三方标签，丰富人群洞察分析，从而帮助该企业构建高潜模型，持续提升转化效果。

数据安全为数据价值挖掘保驾护航

在数据安全合规性要求不断提升、网络安全环境持续复杂化的今天，通过可信计算环境的构建来降低数据泄露风险已经成为大势所趋。TalkingData 安全岛平台的构建与应用实践将证明，安全可信技术能够通过成熟合规的技术方案，严格确保品牌方数据安全，依托数据联动能力，实现以场景驱动营销业务增长，赋能数据应用落地和价值产出。

面向各行各业对于可信计算的需求，京东云与英特尔合作构建的基于可信硬件的隐私计算解决方案正在持续落地，保障数据计算和建模过程中的数据资产安全，并且对数据的使用和流转进行存证，做到数据可追踪，资产可确权，实现数据融合过程中的 “数据可用不可见”，打破数据孤岛，为金融风控、智能定价、精准营销等场景赋能。双方还计划围绕隐私大数据、云原生数据安全隐私保护进行进一步合作创新，协同助力用户在安全的前提下充分挖掘数据价值。

图 4. 通过安全岛平台生成的用户画像

关于 TalkingData

TalkingData 成立于 2011 年，是国内领先的数据智能服务商。TalkingData 秉承 “数据改变企业决策，数据改善人类生活” 的愿景，围绕 TalkingData SmartDP 数据智能平台（TalkingData 数据中台）构建 “连接、安全、共享” 的数据智能应用生态，致力于用数据 + 科技的能力为合作伙伴创造价值，帮助商业企业和现代社会实现以数据为驱动力的智能化转型。

关于京东云

作为京东集团面向企业、政府等机构的技术服务品牌，京东云是更懂产业的数智化解决方案提供商，致力于为企业、金融机构、政府等各类客户提供以供应链为基础的数智化解决方案。依托公、专、混的全栈式云产品矩阵，京东云融合了人工智能、大数据、物联网等前沿科技，在零售、物流、健康、智能城市、金融科技等行业领域为客户提供了丰富的产品与数字化解决方案，帮助客户降低成本、提升效率，是值得信赖的产业数字合作伙伴。

关于英特尔

英特尔（NASDAQ: INTC）作为行业引领者，创造改变世界的技术，推动全球进步并让生活丰富多彩。在摩尔定律的启迪下，我们不断致力于推进半导体设计与制造，帮助我们的客户应对最重大的挑战。通过将智能融入云、网络、边缘和各种计算设备，我们释放数据潜能，助力商业和社会变得更美好。如需了解英特尔创新的更多信息，请访问英特尔中国新闻中心 newsroom.intel.cn 以及官方网站 intel.cn。

intel 京东云

实际性能受使用情况、配置和其他因素的差异影响。更多信息请见 www.Intel.com/PerformanceIndex

性能测试结果基于配置信息中显示的日期进行测试，且可能并未反映所有公开可用的更新。详情请参阅配置信息披露。没有任何产品或组件是绝对安全的。

英特尔技术可能需要启用硬件、软件或激活服务。

具体成本和结果可能不同。

英特尔未做出任何明示和默示的保证，包括但不限于，关于适销性、适合特定目的及不侵权的默示保证，以及在履约过程、交易过程或贸易惯例中引起的任何保证。

英特尔并不控制或审计第三方数据。请您审查该内容，咨询其他来源，并确认提及数据是否准确。

© 英特尔公司版权所有。英特尔、英特尔标识以及其他英特尔商标是英特尔公司或其子公司在美国和/或其他国家的商标。

文中涉及的其它名称及品牌属于各自所有者资产。