智慧城市系列: 了解欺诈调查

面向
企业领导者的 RedGuide

James Luke
Tim Cooper
Rob Tucker

- 提高欺诈调查的有效性，实现更好的结果和更低的成本
- 通过证明对欺诈进行主动出击的态势，改善客户关系
- 通过了解系统和流程的弱点，加强对欺诈的防御力

Redbooks

执行概要

欺诈和财务犯罪是公共和私营领域中一项重大、持久且不断演变的挑战。据估计它每年耗费了收入的5-8%[1]，总计达数万亿美元。

除了直接造成财务影响，欺诈和财务犯罪还可能对信誉和客户信任造成长期的损害，以及违法等真实风险，在私营领域遭致罚金和对股东价值造成冲击，以及在公共实体中失去信任。

公众对欺诈和财务犯罪成本的知晓和不接受度也变得越来越高。客户期望通过众多在线和离线渠道进行交互。数据的数量、种类和速度不可避免地在增长，让受到成功攻击的风险在成倍增加。罪犯在探查和利用任何系统或流程弱点方面变得越来越熟练和博学。这些交互的复杂性和零散性本质有效地隐藏了证据。要纵观全局，必须让这些不同的数据源组合起来。

采用前瞻性欺诈响应的企业拥有真正的竞争优势，能带来切实的威慑效果。证明并证实可疑的活动还提供了一种可预防欺诈的强大质疑能力。在某些情况下，此证据会传递给执法部门进行刑事检控。全面揭示欺诈犯罪如何实施欺诈活动，还能加强系统和流程控制，避免重复性损失。

过去，公司通过单点或业务线解决方案来应对攻击。此方法难以管理，常常会遗漏有组织的罪犯所采取的复杂跨渠道攻击。此方法还会使解决方案更为昂贵、更零散且难以管理。

IBM® i2® Fraud Intelligence Analysis提供了一个集成的欺诈调查和发现解决方案。该解决方案支持快速对欺诈和财务犯罪进行备案，为拒付、补救和起诉等活动提供可行的情报。

[1] 注册舞弊审核师协会，2012年国家报告：
http://www.acfe.com/rttn-highlights.aspx

Fraud Intelligence Analysis解决方案的重要功能包括：

► 强大的可视分析，帮助鉴定和了解信息，从而揭示欺诈活动、网络和目标。

► 内置的调查管理和协调工具，让调查工作朝着正确的方向发展并记录关键的发现和决策。

► 数据获取功能，可快速、有效地让调查团队与正确的信息建立联系。

► 报告和仪表板展示了调查的进度和有效性。

► 协作式工具，支持信息共享和通信，将以前孤立的调查活动之间的各个点联系起来。

本IBM Redguide™出版物介绍了Fraud Intelligence Analysis的功能和产品。本指南还探索了如何将Fraud Intelligence Analysis用作更庞大的欺诈和财务犯罪解决方案的一部分。

不同行业中的欺诈和财务犯罪

欺诈活动的多样性和演变性要求一个有效的解决方案必须能足够灵活地处理不断演化且瞬息万变的攻击。

表1 列出了不同行业中欺诈和财务犯罪的一些常见示例。

表1 不同行业中的欺诈示例

行业	欺诈类型
银行业	► 银行卡 ► ATM虚报 ► 检查 ► ACH/电汇 ► 抵押/贷款 ► 会计 ► 无赖/内部交易
保险	► 故意事故 ► 撞车骗保 ► 滑倒 ► 纵火 ► 医疗欺诈 ► 财产欺诈
医疗保健	► 重复索赔/未提供服务 ► 不必要的服务 ► 回扣 ► 服务的分类计价 ► 虚报（服务/商品）
零售	► 退款/退货 ► 折扣 ► 供应商或供应链盗窃 ► 私下协议 ► 收银机贿赂

行业	欺诈类型
电信业	► 订阅 ► PBX 攻击 ► 跨国收入分享 ► 机顶盒破坏 ► 优惠率
中央政府	► 采购 ► 拨款 ► 薪资 ► 税收
地方政府和社会服务	► 住房 ► 收益 ► 采购 ► 薪资 ► 税收

欺诈和财务犯罪的演变和产业化

总体上来讲，可将欺诈和财务犯罪分为两种类型的犯罪：

► 伺机犯罪

通常是个人以一种计划外的方式进行操控，夸大或利用真正的索赔或交易。

► 有组织或复杂犯罪

团伙串通行动，可能掌握知情人士透露的信息，目的在于获得重大的财务回报。可能还会参与其他犯罪活动。

一般而言，会在客户互动过程中尽早地处理伺机犯罪活动。但是，复杂的模式需要结合来自许多不同数据源的信息（通常时间要求很紧迫）才能为调查和补救流程提供支持。

尽管欺诈智能分析常用于调查高价值的伺机犯罪事件，但从本质上将，该解决方案更普遍的使用情况是复杂且有组织的犯罪。

有组织犯罪具有很多形式。团伙可能是当地或地区性组织，通过亲自会面、电话呼叫或电子邮件来组织和实施攻击。也可能在线组建、培训和装备虚拟团伙，然后执行大规模攻击，以期通过勒索来获得直接的财务回报。调查解决方案能灵活地全面调查和揭示所有变化，这至关重要。对如此复杂的攻击进行可靠的防御需要一个整体性解决方案，而Fraud Intelligence Analysis正是其中的一个关键组件。

典型模型是零散的

许多企业，尤其是金融服务领域的企业，在其各种业务线中拥有多个分析系统，每个系统独立检查交易并识别风险。尽管这些系统能满足其特定业务部门的具体目标，但在这些系统之间进行全盘考虑会更有利，这有助于识别和预防跨渠道的威胁。

图 1 显示了一个银行环境中的孤立操作。

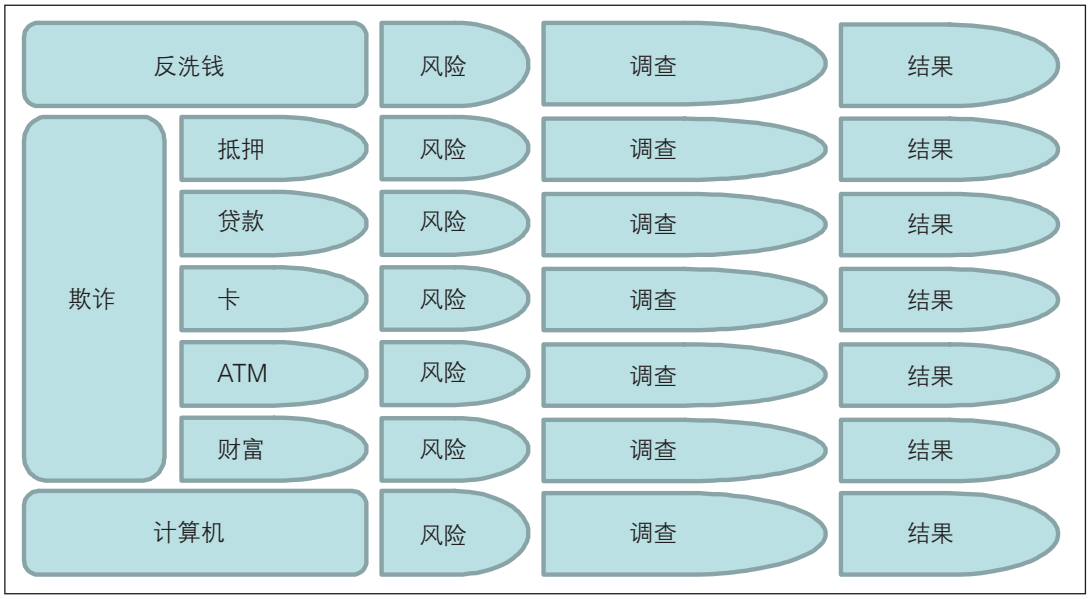

图1 银行环境中孤立且可能很低效的操作

熔合数据和流程孤岛

为了解决零散解决方案中内在的弱点问题，需要一种全新的欺诈解决方案。此解决方案必须从整体上审视企业，以便熔合各个孤岛间的数据。将各个分析和调查孤岛连接起来的需求相当高。这可能是监管方越来越大的压力所造成的直接结果，或者由富有远见的项目从内部推动的。在任何情况下，能够在不同操作单元和地域间调查异常行为，这提供了真正的操作和竞争优势。

图2给出了一个使用组合视图来调查一次跨渠道攻击的示例。

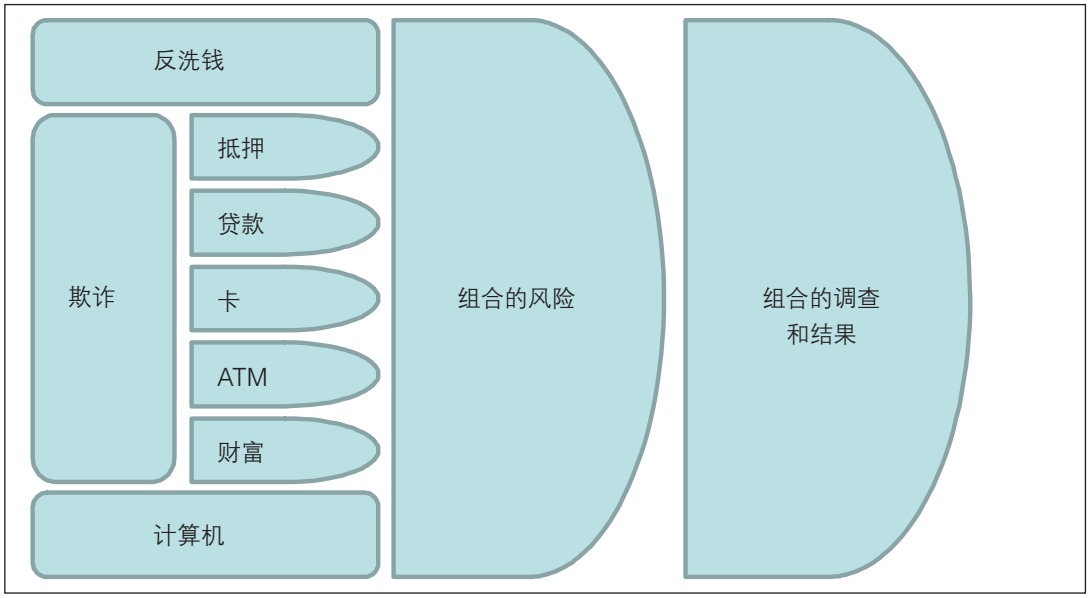

图2 使用组合视图调查一次跨渠道攻击

企业欺诈管理

图3显示出，支持欺诈的完整生命周期需要一种整体行方法，该方法由以下模块化但相互依赖的组件所组成：

► 检测

检测组件用于不断将客户、帐户或交易数据与已知的欺诈案例数据进行比较。这样可在执行支付之前识别可疑的交易。相反且重要的是，有效的交易会得到迅速且更加确定的识别和处理。

► 预防

预防组件阻止不想要的活动发生，让潜在的犯罪者明白他具有明显的欺诈嫌疑，而且与该交易相关的风险很高。预防组件使用发现和调查组件所收集的情报。

► 发现

发现组件是使用一组丰富的分析功能来识别欺诈模式的流程。然后将此信息编码为业务规则、预测模型、异常检测模型和实体分析模型，并且可将它们随时部署到操作系统中，用于实时、近乎实时或用批处理方式进行欺诈检测。调查团队使用此情报确定其活动的优先级。

► 调查

调查组件是构建起诉、恢复或拒绝支付案例的流程。调查的输出是一个链接分析图，其中清晰记录了人员、地点、实体、关系、通信和信息流。

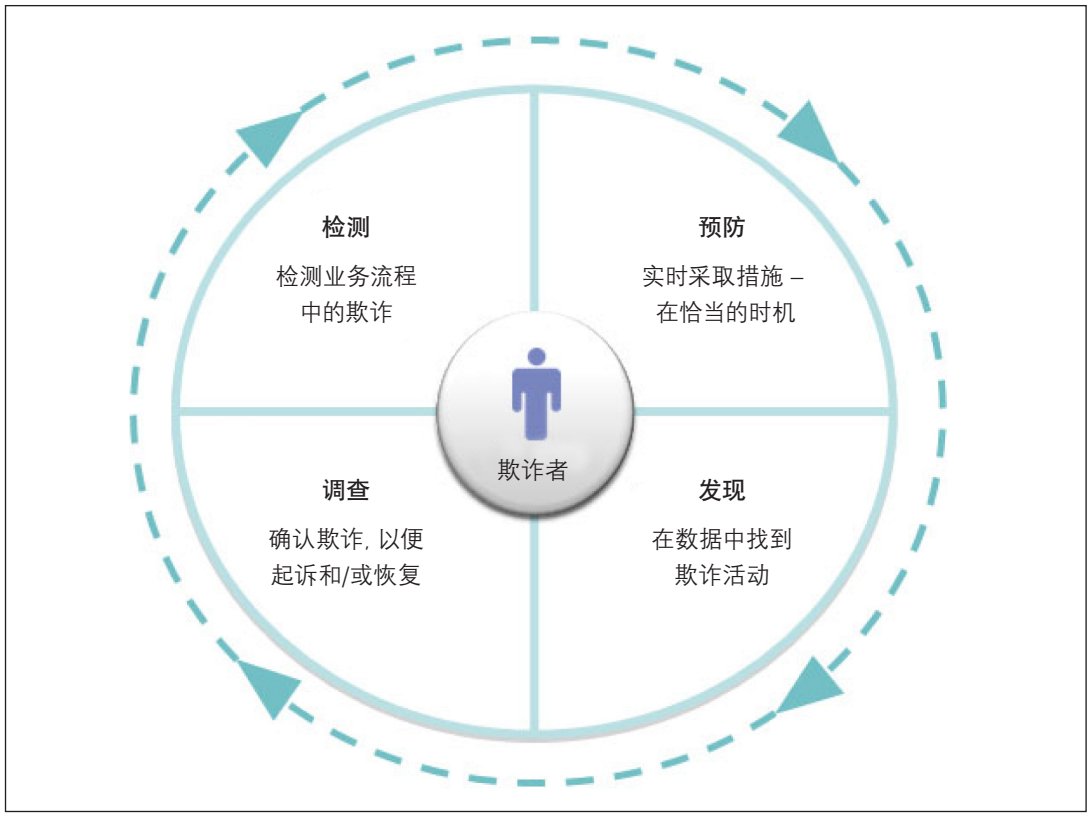

图3 欺诈分析的各个领域

使用分析

由于欺诈活动的产业化导致更高的复杂性，所以有必要采取大量的分析方法来提供完整的解决方案：

- 数据分析用于将不同来源的数据连接、提取并熔合到一个统一的、“适合分析”的表单中
- 实体分析用于在零散的数据集间确定谁是谁以及谁知道谁
- 检测分析用于自动解释潜在的欺诈
- 搜索、查询和警报分析用于快速且有效地获取正确的信息
- 链接（网络）分析用于了解和揭示人员、组织以及事件之间的关系
- 社交网络分析用于确定大型网络中的重要角色
- 报告分析可用正确的格式将正确的信息提供给正确的人

如图4所示，Fraud Intelligence Analysis专注于反欺诈生命周期中的调查和发现阶段。Fraud Intelligence Analysis还与检测、预防和案例管理解决方案进行集成和交互，这些解决方案常常作为一个更大型项目的一部分来部署。

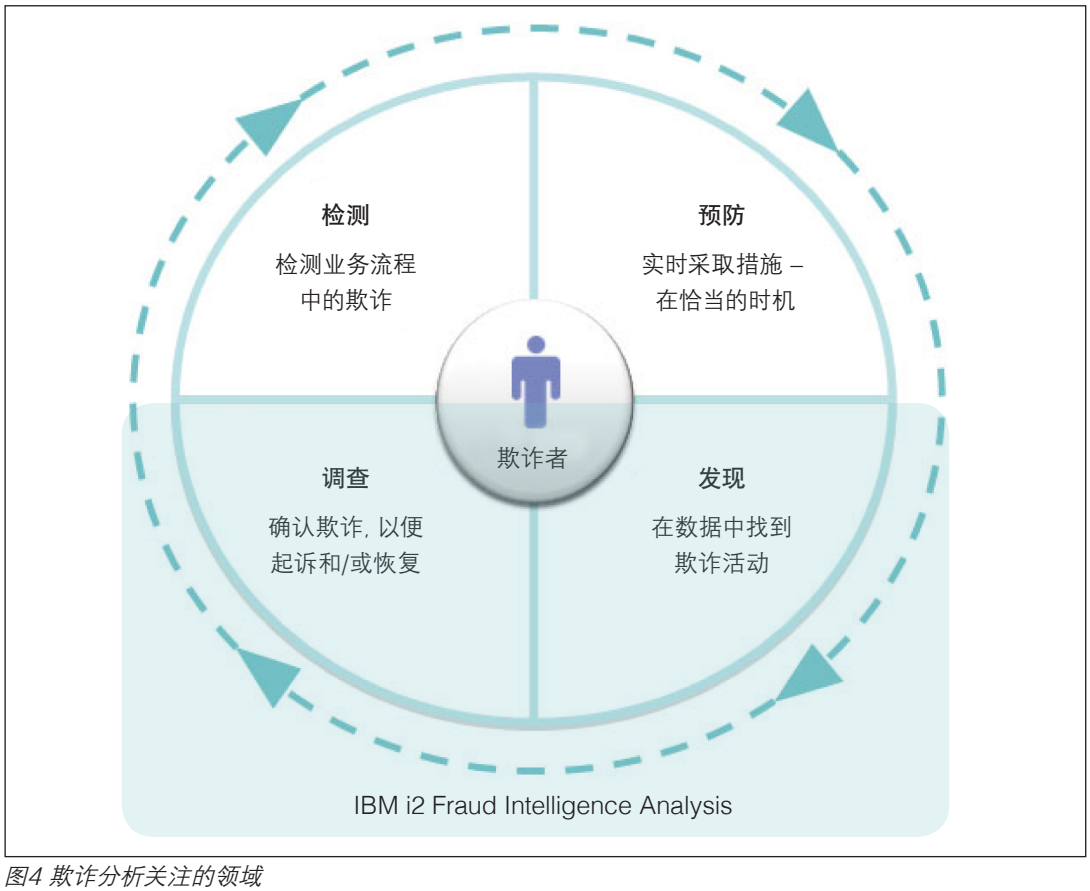

图4 欺诈分析关注的领域

调查流程被视为对检测组件的补充，可揭示并记录欺诈途径和方法。此信息是宝贵的反馈，可用于加强系统流程和策略的执行。

如图5所示，现有的检测分析和规则用于定义可改进检测的各种结果。

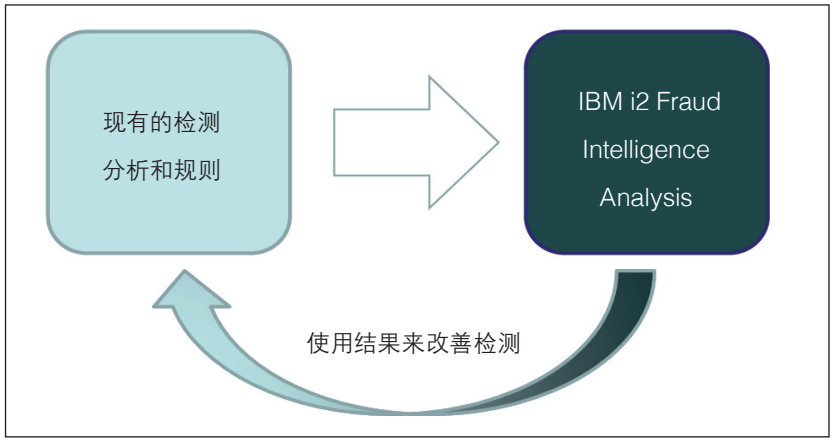

图5 调查的输出有助于定义选择价值

本指南的剩余部分重点介绍Fraud Intelligence Analysis解决方案及其功能，这些功能对更庞大的反欺诈管理提供支持和补充。

IBM i2 Fraud Intelligence Analysis

IBM i2 Fraud Intelligence Analysis帮助调查复杂的事故，生成关键人员和事件的、可行的可视化表示，以及记录拒付和潜在诉讼的结果。

如图6所示，Fraud Intelligence Analysis提供了分布式调查、协作、分析和可视化功能来表示欺诈网络。

Fraud Intelligence Analysis作为一个独立解决方案提供了重要的价值。它也能集成到其他的现有或计划投资中，用来满足更广泛的需求。我们使用取决于行业的重要吸引因素来创建规则和模型，突出风险更高的交易并识别异常。检测工作可实时或批量完成，具体取决于行业和交易类型。

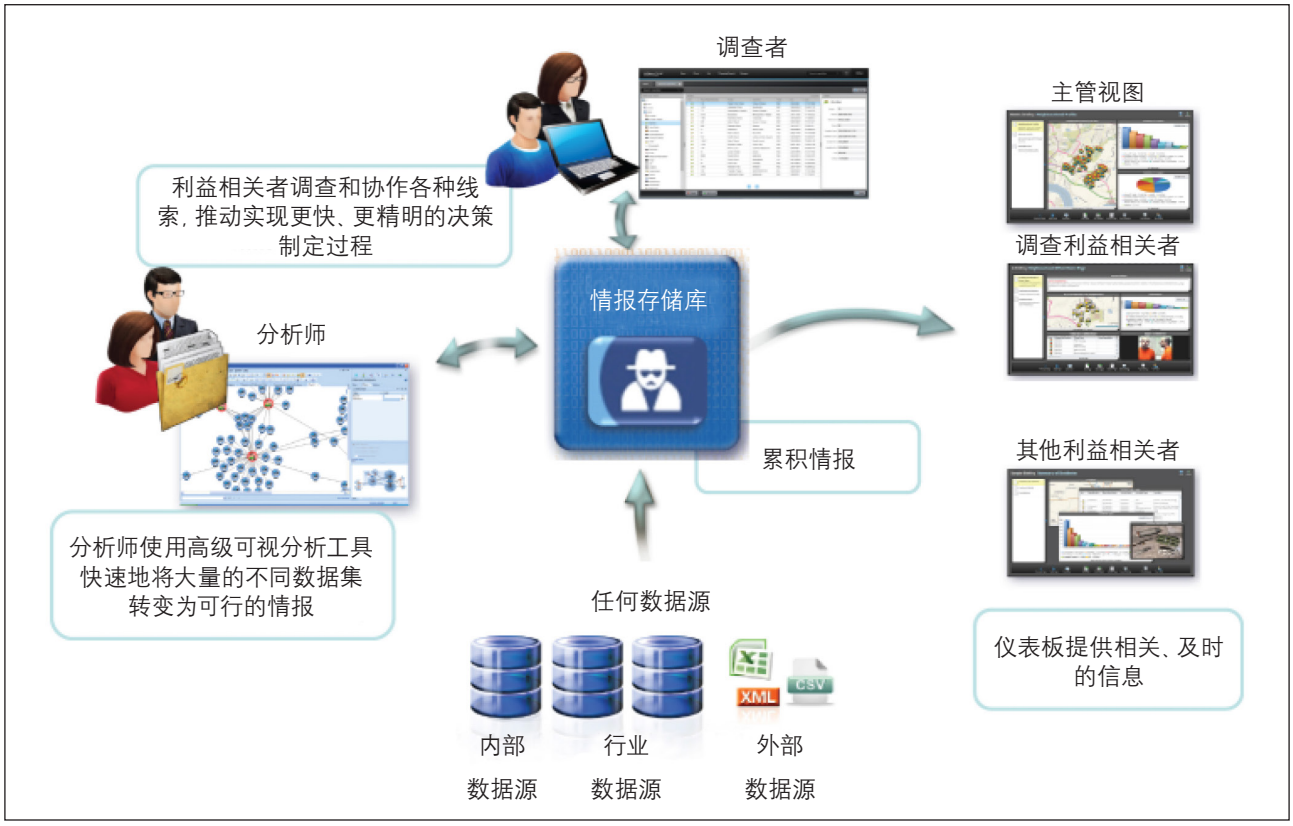

图6 Fraud Intelligence Analysis

连接到数据

数据是调查的血液。以一种尽可能有利的方式将团队与数据建立连接，这至关重要。此方法使团队成员能够将精力集中在揭示和记录可疑活动等任务上。Fraud Intelligence Analysis以各种方式直接连接到必需的数据，并且能够将结构化和非结构化数据源包括在内：

- 通过（外部和内部的）Intelligence Analysis Platform按需获取数据：可将数据源直接连接到调查流程中。可由分析师和调查人员单独搜索、过滤和扩展数据源，与调查相关的数据会保存下来，并添加到累积的情报中。
- 通过连锁搜索按需获取数据：可将数据源分组，然后通过单次搜索有选择性地搜索数据源，还能同时搜索多个数据源。此方法进一步提高了调查流程的效率。会对搜索结果进行排名，并且进一步的预分析最大限度利用了宝贵的分析师时间。
- 数据加载（提取、转换和加载）或数据集的“提前”加载，这些数据都已准备好用于分析。
- 通过灵活且直观的导入程序轻松地将偶尔或不常访问的数据包含在调查中时，可使用临时文件导入。数据格式可以是每种只有一个，或者如果想要更细粒度的导入，可通过以前准备的导入规范（已有分析师创建）来解析某种格式的数据。

处理外部数据

调查几乎不可避免地需要包含外部数据。数据的类型和来源不胜枚举，但至少包含以下数据：

► 监视列表、制裁和政界人士 (Politically Exposed Persons，PEP)

► 公共记录数据

► 信用风险和身份

► 车辆和许可信息

► 业界提供的数据库，如Insurance Fraud Investigators Group (IFIG)、National Insurance Crime Bureau (NICB)和Insurance Fraud Bureau (IFB)

► 开源情报(OSINT)

► 社交媒体，如Facebook和Twitter

灵活的数据摄取模型可确保随时能将数据连接到调查工作，确保调查团队能立即访问他们所需的信息。

使用IBM产品，也可扩展Fraud Intelligence Analysis来应对其他数据挑战：

► IBM Identity Insight提供了身份识别解决方案和跨数据的非明显关系生成。

► IBM Content Analytics从大量非结构化数据中提取关键信息，如文档和网页。

将数据转化为情报

调查工作的最终结果和目标是记录拒付和起诉等可疑活动。该解决方案使调查单位能快速地将看起来无边无际的数据转换为可行的洞察。

以下是一些重要利益相关者：

► 分析师

► 调查人员

► 调查主管

分析师

分析师执行深入的分析调查，核对、分析和可视化信息，减少在复杂数据中发现关键信息所需的时间。

有3类分析师对欺诈分析感兴趣：

► 标准分析师

标准分析师为信息的部门研究、分析和表示提供支持。标准分析师可定义和执行分析战略，通过使用专业的分析工具、数据挖掘、分析和电子索赔文件审核，在所有已分配的传统和复杂的欺诈性索赔中提供反应性的调查数据支持。

► 内部欺诈分析师

内部欺诈分析师的任务是识别公司员工的欺诈行为。内部欺诈分析师对员工提示、合规性和销售审计中找到的异常报告和不法行为执行例行的操作。内部欺诈分析师负责收集证据，编写详细的报告并与员工面谈。内部欺诈部门常常负责开发首选的实践，并向员工教授欺诈感知知识。

► 外部欺诈分析师

内部欺诈分析师主要是对自己公司的员工进行监视，而外部欺诈分析师则处理外部欺诈者，很多外部欺诈者会与目前的员工或以前的员工进行勾结来实施欺诈模式。外部欺诈常常发生在针对一家公司运行各种结算或销售模式的供应商和转包商中。外部欺诈分析师还会调查意欲盗窃敏感信息的借口和社会工程实例。此外，外部欺诈分析师有时会参与检查各种形式的计算机犯罪，包括钓鱼或黑客攻击尝试。

对于每类分析师，Fraud Intelligence Analysis提供以下关键特性：

► 告知和访问新的欺诈案例（手动或通过检测系统触发）。

► 能够快速获取、收集和组合与欺诈案例相关的不同数据。

► 能够探查并理解欺诈案例中的事件、人物、时间和地点。通过使用各种可视分析工具来理解欺诈案例并能从中获取新情报来完成该工作。

► 能够处理“如果……”假设并根据信息进行推理。

► 能够在调查人员和更庞大的利益相关者社区中共享和传播调查发现结果。

IBM Fraud Intelligence Analysis以多种可视格式提供了可行的情报，目的是为整体调查和补救流程提供支持：

► 时间线分析：快速显示复杂的暂时交易。

► 关联图分析：可视化人员、地点和物体之间的关系。

► 地理空间映射：地图实体（例如进入地图上的人员或车辆）。

► 柱状图和热力图：突出峰值并识别定期事件模式。

► 社交网络分析：量化并描绘各种关系，帮助理解复杂的欺诈和欺诈团伙。

图7显示了一些可视分析示例。这些图表可让人们更深入地理解罪犯、恐怖分子和欺诈性网络的操作结构、分层结构和方法。它们还简化了复杂数据的交流工作，支持及时准确地制定操作决策并将结果上报到执法部门。

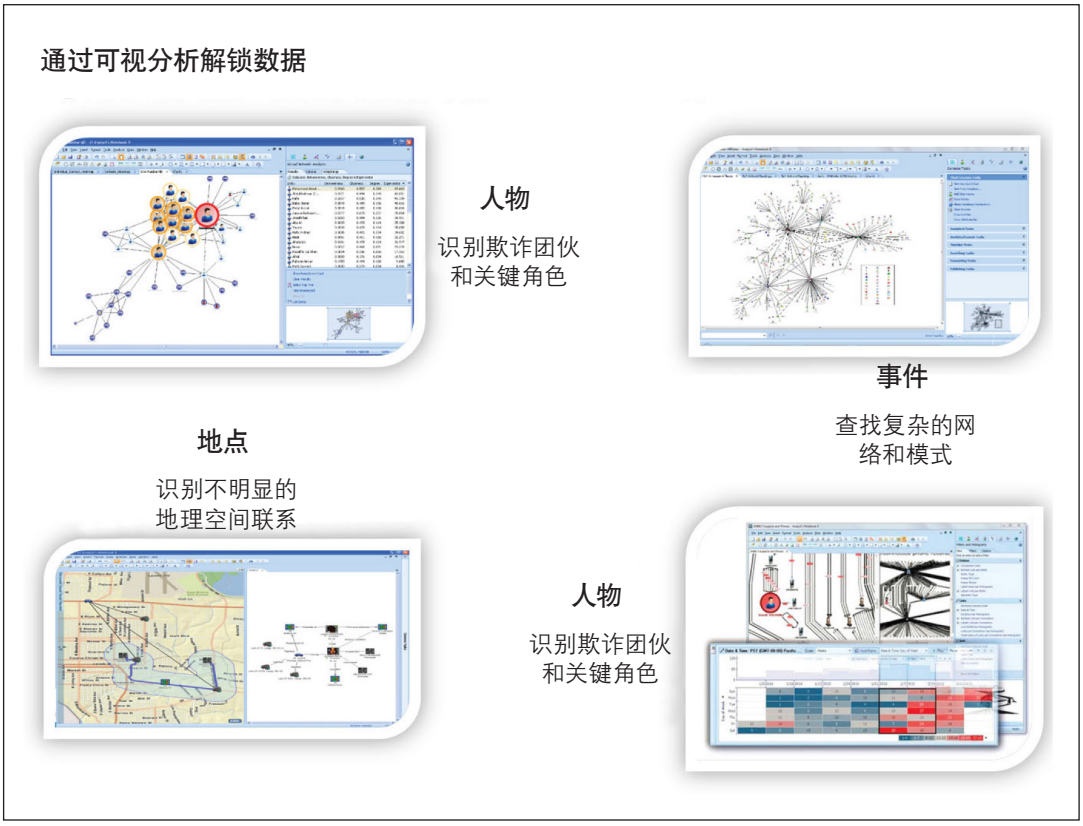

图7 通过可视分析解锁数据

调查人员

调查人员可组织、执行和跟踪涉及承保范围问题和可疑欺诈索赔活动的调查。调查人员可花一些时间抵达各个地方收集证据，执行现场调查和检查。他们还根据既定的最后期限，定期向理算员和相关的第三方报告其调查的状态和结果。

Fraud Intelligence Analysis的智能门户使调查人员能够积极且协作式地参与调查。用户可通过一个简单的界面搜索并浏览案例数据和相关信息，并查看简单的可视化表示内容。

调查人员还可以：

► 获知新的欺诈案例。

► 获取、收集和组合与调查相关的各种数据。

► 与分析师共享和传播调查发现结果。

调查主管

调查主管管理索赔部门的特殊调查职能，向理算员培训欺诈意识，以及与索赔人员和法律人员就诉讼案件进行协调。

协作的力量

复杂欺诈可能触及许多操作流程和系统，而且能够快速识别共谋活动有助于打击复杂、有组织的攻击。Fraud Intelligence Analysis使调查团队能创建和订阅信息集，在添加或修改情报时获得通知。存储库中的内容包括一个完整的版本和变更历史，并且在适当的时候支持进一步咨询。

构建和使用累积的情报

Fraud Intelligence Analysis会存储整个调查过程中的信息。可将情报进行划分，根据角色、调查和权限来提供访问权，并为敏感的调查（例如内部欺诈）提供支持。拥有单个事实来源，再加上警报功能，调查团队能够分享情报。

瓦解各种调查孤岛可得到一个不断更新的、丰富的情报来源，该来源可用于：

- 缩短未来的调查工作。
- 识别共谋和欺诈团伙。
- 通过揭示业务系统和流程中的情报，为检测和预防流程提供支持。

度量进度、成功和结果

Fraud Intelligence Analysis能够创建多种报告和仪表板，以支持操作流程并向更庞大的业务群体演示结果。各种利益相关者都在使用这些报告和仪表板：

- 调查人员和分析师：当前的调查列表、个人绩效与服务水平协议(SLA)的要求对比，以及团队平均绩效。
- 调查主管：按照不同调查类型、调查人员/分析师利用率及针对SLA的调查绩效，监督团队和个人绩效以及趋势。
- 最高层主管/管理报告：总体监督、绩效和趋势，以及财务分析。尽管目标各不相同，但能够证明欺诈和财务犯罪的姿态，是许多企业的一个既定主题。

表2给出了Fraud Intelligence Analysis支持的各种管理官员示例。

表2 Fraud Intelligence Analysis支持的官员

官员	活动
首席风险官	风险减少并针对欺诈提高更有力的姿态，将欺诈者赶到其他保险公司或领域。
首席财务官	更好的财务比率、操作和效率改进。
首席合规官	支持合规性目标，改善与监管者的关系。
首席安全官（调查） 首席信息安全官（计算机犯罪）	更透彻地理解计算机威胁和攻击矢量。
欺诈主管	改进各种调查指标，增加欺诈者转移到更脆弱的目标的可能性。

官员	活动
索赔主管	减少向欺诈性索赔的支付，增加利润。
洗钱报告官 (MLRO) 首席 AML 官	确保在业务小组间整体地解决问题，实现合规性。

提供对操作、绩效和财务可见性，不仅对该流程的日常管理很重要，还有助于将认知扩大到更大的范围，进而扩大到整个企业。

图8总结了Fraud Intelligence Analysis活动。此活动显示为仪表板中的报告、计划和记分卡。

图8 欺诈分析输出报告

IBM i2 Fraud Intelligence Analysis核心组件

Fraud Intelligence Analysis旨在处理3种主要的流程和工作流：

► 分析师工作流

分析师工作流旨在获取、收集、分析、共享和传播情报，以进行欺诈调查。

► 调查人员工作流

调查人员工作流是一种“轻微手动的”（基于字段）工作流，包括情报查找和浏览，以及从一个Web门户输入情报。

► 经理和主管工作流

经理和主管工作流可协调各种调查工作，监视调查进度，以及接收情报报告、更新和趋势。

Fraud Intelligence Analysis围绕3个核心组件来设计：

► IBM i2 Intelligence Analysis Platform

► IBM i2 Analyst´s Notebook Premium

► Intelligence Portal

IBM i2 Intelligence Analysis Platform

IBM i2 Intelligence Analysis Platform是一个企业级、面向服务的解决方案。其设计宗旨是提供调查和分析功能。以下是Intelligence Analysis Platform的重要特征：

► 在用户数量、数据量和分析性能方面具备极高的可伸缩性。

► 基于一种强大且灵活的实体、链接和属性(ELP)数据模型，具有出色的数据格式和模式灵活性。这包括支持结构化和非结构化信息。

► 具有完整的事件审计记录和回放功能，实现了更高的可靠性。还能够实例化新的分析服务。

► 更好的可扩展性和集成，通过为服务API和数据使用开放标准、可扩展的应用程序框架和插件客户端功能来实现。

如图9所示，在Intelligence Analysis Platform的核心平台中有4种不同的服务类。

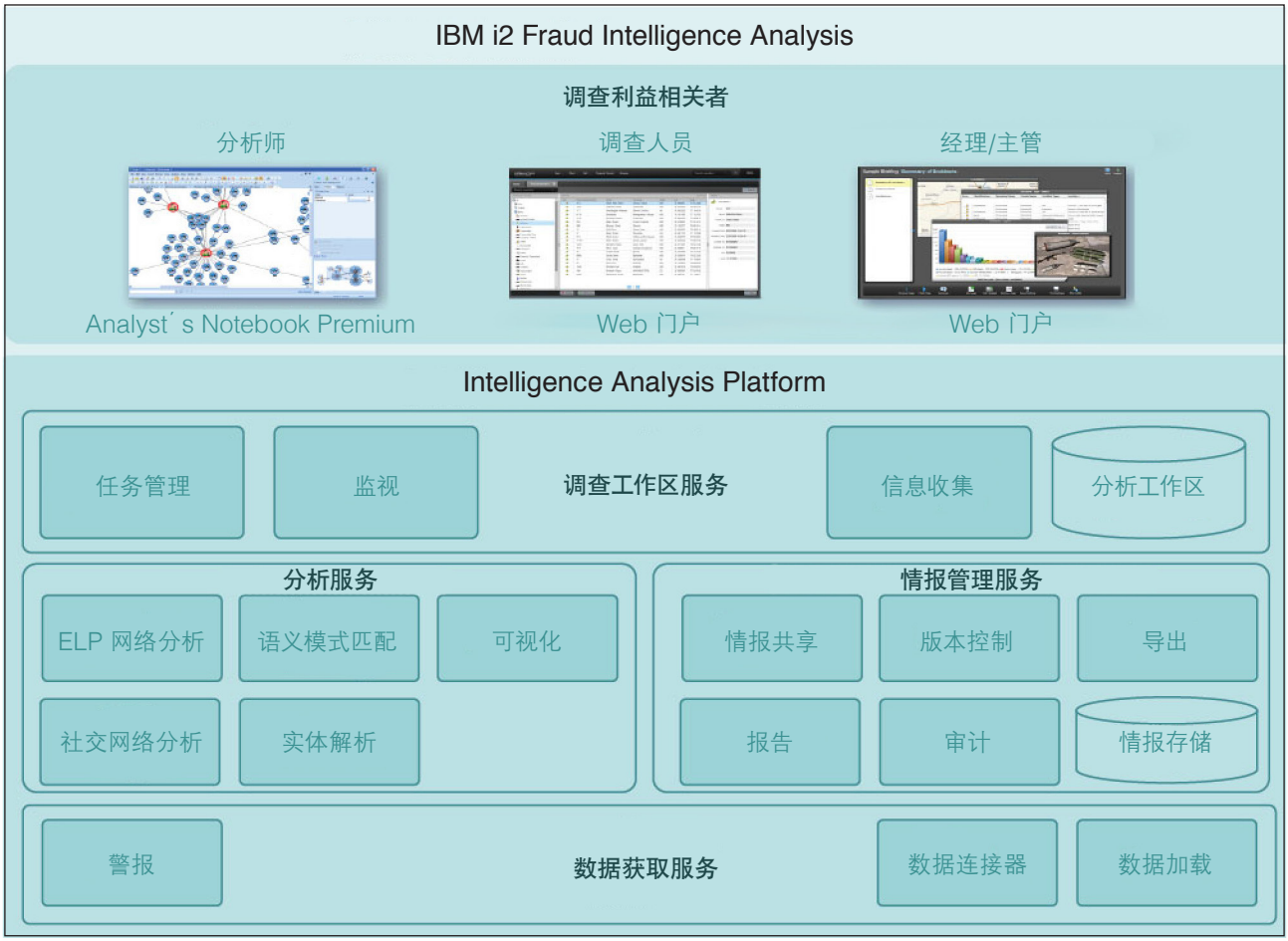

图9 Intelligence Analysis Platform架构

► 数据获取服务

数据获取服务将信息获取到Intelligence Analysis Platform中。有两种可用的方法：

– 数据连接服务支持按需访问外部来源中的数据。用户可根据需要，通过搜索、检索和扩展操作来从数据源请求信息。Fraud Intelligence Analysis支持在多个数据源间进行连锁访问。

– 数据加载服务支持“提前”将信息摄取到Intelligence Analysis Platform中。信息已预先填充到Intelligence Analysis Platform中。

► 分析服务

分析服务可增强并协助浏览、理解和分析信息：

– 实体、链接和属性(ELP)网络分析服务支持核心信息的交互和分析命令，如数据探索和查找网络路径。

– 语义模式匹配服务为Intelligence Analysis Platform中的信息提供丰富的ELP查询匹配功能。

– 可视化服务提供了信息的交互式、可视表示，帮助人们理解和分析信息。

– 社交网络分析服务可分析ELP网络，确定其中的“重要角色”。

– 实体解析服务可查找ELP网络中匹配的实体和不明显的关系。

► 调查工作区服务

调查工作区服务在调查人员和分析师使用Fraud Intelligence Analysis执行调查和分析活动过程中提供支持：

– 任务管理服务支持对Fraud Intelligence Analysis中的活动进行组织和跟踪。此服务可与一个案例管理系统相集成，实现更广泛的协调操作。

– 监视服务提供了调查的关键绩效指标和进度指标。

– 信息收集服务提供了收集、核对和分析调查活动信息的途径。

► 情报管理服务

情报管理服务为Fraud Intelligence Analysis中的以下调查和分析活动的分享和发布提供支持。

– 情报共享服务可共享、关联和重用通过调查和分析所收集的情报。

– 版本服务提供了共享信息的完整更新历史记录。

– 导出服务支持将情报信息推送到其他系统中。

– 报告服务提供报告和仪表板，用以传达通过调查和分析所收集的情报。

– 审计服务记录Fraud Intelligence Analysis中的用户交互和数据更改。

IBM i2 Analyst’s Notebook Premium

IBM i2 Analyst′s Notebook Premium是一个桌面应用程序，提供了一个功能丰富、交互式的可视分析环境。Analyst′s Notebook Premium连接到Intelligence Analysis Platform，以增强和扩展其功能。

Analyst′s Notebook Premium以IBM i2 Analyst′s Notebook的功能为基础，提供了对情报数据的访问能力。Analyst′s Notebook Premium可收集、管理并组织信息和情报。无需首先将内容放入图表中，即可查看和编辑存储库中的数据。使用分析存储库，可轻松地揭示不同数据类型之间的关系、路径和网络。

Intelligence Portal

Intelligence Portal为Analyst′s Notebook Premium提供了补充性功能，可供调查人员、经理和主管们使用。它通过连接到Intelligence Analysis Platform来运行。

性能和可伸缩性

Fraud Intelligence Analysis解决方案使用IBM DB2®、IBM WebSphere® Application Server和IBM WebSphere MQ。此中间件以及解决方案架构支持垂直（在服务器内添加流程）和水平（在服务器间执行负载平衡）扩展解决方案。

该解决方案的组件在大量场景中经过了广泛测试，已部署在全球一些最大型的金融机构中。得益于Fraud Intelligence Analysis的灵活扩展功能和内部架构，现在可以提供大容量功能。

可用性

Fraud Intelligence Analysis解决方案架构支持定义一种部署架构，这种价格可消除软件的单点故障。解决方案组件可分布在一个集群中，如果集群中的一个成员发生故障，其他成员可继续操作。

一个全面集群化的解决方案利用了WebSphere提供的工作负载管理和平衡功能。WebSphere Application Server通过主动处理集群规划的节点来实现高可用性，而DB2通过心跳信号监视和自动化的磁盘接管来提供高可用性。

所有备份和还原计划都通过实用程序来处理，如IBM Tivoli® Storage Manager。在针对客户需求提供量身定制的灾难恢复架构方面，IBM拥有广泛的经验。一般而言，客户倾向于在其所有运营部门采用一种通用的灾难恢复战略，目的是保持该战略的一致性。

安全

信息至关重要，而且业务部门可能需要分类这些信息，根据“需要知道”的原则来限制访问。Intelligence Analysis Platform存储库中的信息可分类为4个级别：

- 公共

  非敏感的信息，如果公开披露，不会危害业务。例如一家股份有限公司的公司董事长姓名。

- 内部

  可由所有员工访问的信息。此信息不适合公开披露。例如，处理可疑欺诈性保险索赔的推荐流程。

- 机密

  公司的敏感信息，仅应按照“需要知道”的原则进行访问。例如，欺诈性保险调查的可疑目标。

- 受限

  公司中价值最高的信息，如果公开披露该信息，将会损害业务。例如，公司内高级员工执行的可疑内部欺诈活动。

这些分类拥有一种继承关系，这意味着如果某个人能访问机密信息，那么他也能访问“内部”和“公共”类别的信息。

Fraud Intelligence Analysis集成

Fraud Intelligence Analysis可集成到现有客户端或更庞大的IBM反欺诈管理解决方案中。有许多集成领域值得考虑，如图10所示。

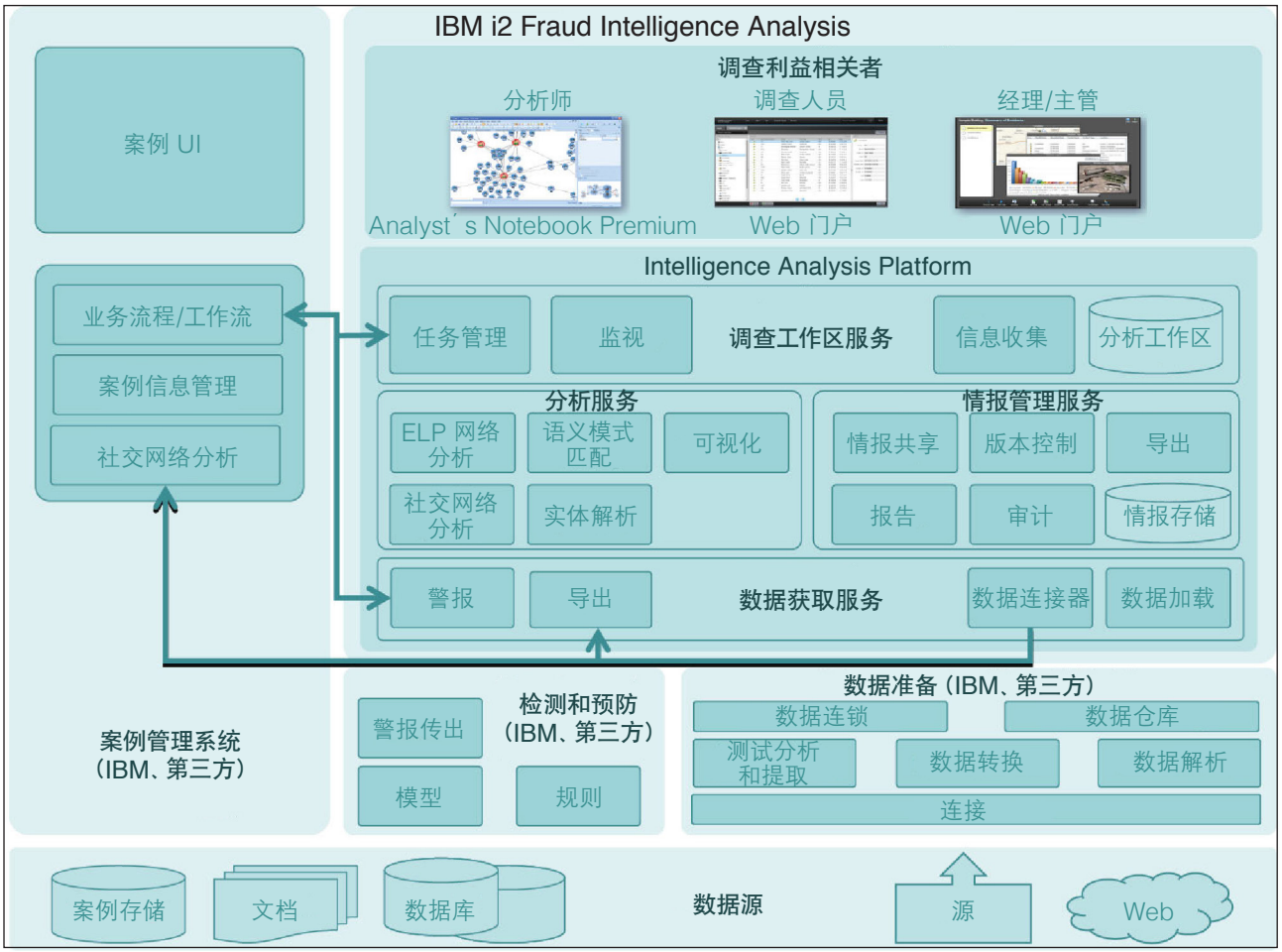

图10 Fraud Intelligence Analysis集成区域

案例管理集成

Fraud Intelligence Analysis可与外部（IBM或第三方）案例管理系统相集成，提供协调、工作流和案例材料管理支持。有3个集成点：

► 任务集成

任务集成是在案例管理系统中创建的任务，与Fraud Intelligence Analysis解决方案中对这些任务的处理和跟踪之间进行同步。

► 信息集成

可在Fraud Intelligence Analysis中访问案例管理系统内的信息，以执行调查和分析。也可将Fraud Intelligence Analysis中生成的最终情报导出到案例管理系统中。

► 警报集成

可在创建新任务或信息时，通过案例管理系统生成Fraud Intelligence Analysis警报。

检测系统集成

通过检测系统检测到一种潜在的欺诈情形时，可使用该系统启动Fraud Intelligence Analysis中的调查和分析工作。集成点包括：

► 警报集成

进行检测时，可将警报发送到Fraud Intelligence Analysis以通知调查人员。可使用警报中的信息来识别与警报相关的关键信息，以帮助进行检测。

► 信息集成

与检测相关的信息可通过数据加载服务加载到Fraud Intelligence Analysis中，或者通过数据连接服务按需进行访问。

在有案例管理系统的地方，检测系统可集成到其中，而不是集成到Fraud Intelligence Analysis中。这样进行检测之后，会在案例管理系统中生成警报和任务。然后可使用案例管理系统与Fraud Intelligence Analysis之间的集成，将调查人员和分析师与工作流建立联系。

数据源集成

Fraud Intelligence Analysis可连接到业务线或外部数据源，为调查人员和分析师提供他们所需的信息。信息可根据需要获取或预先安装，如IBM i2 Analyst′s Notebook Premium一节中所述。客户的各种需求和数据环境要求最佳的数据源集成方法，可能需要更多的产品来准备要使用的信息。

数据准备集成

IBM提供了许多技术来帮助准备信息，使调查和分析更加有效和高效。此领域的常见需求包括：

► 非结构化数据

IBM Content Analytics提供了强大的工具来从文本中挖掘和提取知识。

► 零散的数据

对于多个来源中零散或相互重叠的信息，IBM Identity Insight提供了一种途径来解析和整合这些信息。

► 大数据

对于客户拥有大量信息的情况，IBM InfoSphere®可提供帮助。

扩展Fraud Intelligence Analysis

可通过丰富的IBM或第三方技术轻松扩展Fraud Intelligence Analysis，增加它的功能：

- 在调查中使用面部识别

  尽管许多欺诈和财务犯罪是在线实施的，但人员交互是许多犯罪活动中的重要阶段，例如在零售和银行领域。可随时扩展Fraud Intelligence Analysis，通过摄像头获取面部信息，并将其与数据库匹配。可在事件发生后完成此操作，目的是为调查提供支持，或者在操作中实时完成，为犯罪预防提供支持。

- 实现流程合规性

  Fraud Intelligence Analysis包含IBM Operational Decision Manager，它集成了业务事件和规则，在流程和应用程序之间实现决策自动化。它提高了反复制定的、与交易和流程相关决策的质量，确定了每个事件、合作伙伴和内部交互的恰当行动过程。

- IBM SPSS®用于识别可疑和异常的活动并确定调查活动的优先级。IBM SPSS结合了领域专家经验和高级分析，可寻找已发生的可疑和异常交易。集成到您的操作流程中后，IBM SPSS能更好地预防不想要的交易，将高风险交互的信息传递给调查团队。与警报相关的信息与额外的相关内容相结合，能够全面揭示并可视化欺诈活动。此外，可快速识别并处理非可疑交易，从而降低操作成本并超越客户的预期。

- IBM Q1/QRadar®用于检测内部和共谋欺诈，以及计算机攻击。内部欺诈及系统和特权的滥用是主要的损失来源，可能会吸引监管人员进行调查。QRadar是一个领先的安全信息和事件管理器。它有效、实时地组合了整个企业的日志记录，并将这些记录与业务规则相关联，从而识别威胁、风险和异常行为。这些警报与内部人员和共谋犯罪活动相关，可传递给调查团队，此外还有传统的外部系统和网络威胁。

- IBM Advanced Case Management提供了一种机制来存储书面证据、准备案例，以及根据调查来执行临时工作流。Advanced Case Manager为调查提供支持，作为Investigate and Discover子系统的一部分为Fraud Intelligence Analysis提供补充。

- IBM Identity Insight提供实时的帮助来预测财务犯罪并实现先发制人，方法提供一个人的身份、它熟知的人和这些人执行了哪些操作等全面信息。高级识别算法用于从企业交易数据中提取实体，并将这些实体与其他数据（监视列表、社会安全记录等）相结合。这为犯罪分子尝试隐瞒身份的情况提供了具有统计参考价值的身份数据。此数据能在交易早期提供警报，预防高风险的交易。此数据对调查流程也非常有用，它使团队能集中精力将高质量的实体信息与其他相关内容相结合，从而记录犯罪活动。

- IBM Content Analytics使用非结构化数据来捕获必要的信息，这些数据占企业总内容量的80%，保存在注释字段、电子邮件、CRM系统和其他业务线应用程序中。此内容包含大量高价值的情报，能为欺诈和财务犯罪调查提供支持。将您的分析师和调查人员直接与此内容建立联系，能带来切实的操作优势，使团队能够将海量的非结构化数据转变为可行的洞察，从而为他们的调查工作提供支持。
- IBM InfoSphere Streams支持摄取、分析和关联来自多个实时数据流的数据。

总结

Fraud Intelligence Analysis提供了至关重要的洞察来帮助人们调查复杂的事故。这会生成一种可行的可视化表示内容，其中包括关键人员和事件，以及已记录的拒付和潜在诉讼结果。分布式调查、协作和可视的结果有助于优化和证明调查团队的价值。

Fraud Intelligence Analysis解决方案作为一个独立解决方案增添了即时操作价值，而通过使用现有投资将其集成到一个整体的解决方案中，还能带来了更大的优势。

其他资源中的更多信息

- IBM Fraud Intelligence Analysis产品页面

  http://www.ibm.com/software/products/us/en/fraud-intelligence-analysis/

- IBM i2 Intelligence Analysis产品组合出版物

  http://www.ibm.com/support/docview.wss?uid=swg27024896

- IBM产品信息页面

  http://www.ibm.com/common/ssi/index.wss?request_locale=en

  在此页面上，输入IBM i2 Fraud Intelligence Analysis，选择信息类型，然后单击Search。在下一页上，按地理位置和语言缩小搜索结果范围。

作者

本指南由IBM i2专家与国际技术支持组织 (International Technical Support Organization, ITSO) 合作编写。

James Luke是位于英国的首席架构师。他在分析领域拥有20年的经验。他拥有University of Southampton人工智能和信息运营方向的哲学博士学位。他擅长的领域包括数据挖掘、数据熔合、人工智能和文本分析。他还编写了大量有关实际分析应用的著作。

Tim Cooper是位于英国的产品线经理。他在 IT 行业拥有20多年的经验。他拥有Open University计算机科学和心理学学位。他擅长的领域包括互联网技术、网络安全、系统和流程变更，以及调查欺诈和财务犯罪的解决方案。

Rob Tucker是位于英国剑桥的IBM i2产品组的Product Advancement for Intelligence Products负责人。他是一位经验丰富的软件架构师、用户体验设计师和业务分析师，擅长具有丰富可视化和分析功能的软件。他还拥有线索开发、用户体验和业务分析团队方面的工作经验。Rob在IBM工作已有13 年，负责开发执法、军队、国家安全和商业行业所使用的情报分析和调查管理软件。

感谢以下人员对本项目做出的贡献：

Esther Boal和Joanna Lockhart

IBM软件部，行业产品部

Marcela Adan和Debra Landon

国际技术支持组织，罗契斯特中心

现在您也可以成为出版作家！

现在您有机会让您的技能备受关注，发展您的事业，并成为出版作家——所有这些可一步实现！欢迎加入ITSO实习项目并帮助您针对您所擅长的领域编写一本图书，同时使用前沿技术磨砺您的经验。您的努力将帮助提高产品的认可程度和客户满意度，您还能扩大您的技术联系人和关系网。实习项目持续2到6周，您可亲自参与，也可作为远程实习生在家中工作。

要了解有关该实习计划的更多信息，浏览实习索引并在线申请，请访问：

ibm.com/redbooks/residencies.html

随时关注IBM Redbooks

- 在Facebook上找到我们：

  http://www.facebook.com/IBMRedbooks

- 在Twitter上关注我们：

  http://twitter.com/ibmredbooks

- 在LinkedIn上查找我们：

  http://www.linkedin.com/groups?home=&gid=2130806

- 使用IBM Redbooks®每周时事通讯浏览最新的Redbooks出版物、实习计划和研讨会：
  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm
- 通过RSS源随时关注最新的Redbooks出版物：
  http://www.redbooks.ibm.com/rss.html

声明

本信息适用于在美国提供的产品和服务。

IBM可能不会在其他国家/地区提供本文档中所讨论的产品、服务或功能。有关您所在地区提供的产品和服务，请与当地IBM业务代表联系。对IBM产品、程序或服务的任何引用并非暗示只可以使用该IBM产品、程序或服务。也可以使用任何不破坏IBM知识产权的类似产品、程序或服务。但是，对任何非IBM产品、程序或服务操作的评估和验证操作是用户自己的责任。

对于本文中描述的主题内容，IBM可能具有专利或正在申请专利。本文档内容未赋予您对这些专利的任何许可。您可以用书面形式将许可查询发送给：

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

以下段落不适用于英国或这些规定与当地法律不一致的任何其他国家（地区）：国际商业机器公司“按原样”提供本出版物，不含任何明确或暗示的担保，包括但不限于非侵权、适销性、特定用途的适用性的所有隐含担保。某些国家在某些事务中不允许明确或隐含担保的免责声明，因此，此声明可能不适合您。

本信息可能包含技术错误或排版错误。这里的信息会定期变更，这些变更将合并到本出版物的新版本中。IBM可能随时对本文介绍的产品和/或程序做出改进和/或变更，恕不另行通知。

本信息中对非IBM网站的引用仅出于方便考虑，不能以任何方式看作是对这些网站的认可。这些Web站点上的内容不是本IBM产品资源的一部分，使用这些Web站点时风险自负。

IBM可能以它自己认为合适的方式使用或分发您所提供的信息，同时不会承担对您的任何责任。

这里给出的性能数据是在受控环境中实现的。因此，在其他操作环境下获得的实际结果可能变化很大。在开发级系统上可能进行了一些度量，我们不保证这些度量值将会与一般可用系统上的度量值相同。此外，有些度量值可能是通过推断估计的。实际结果可能有所不同。本文档的用户应该针对他们的特定环境验证适用的数据。

有关非IBM产品的信息是通过这些产品的提供商、他们发布的公告或其他公开来源获得的。IBM没有测试过这些产品，无法确认与非IBM产品相关的性能、兼容性或任何其他声明的准确性。关于非IBM产品功能的问题应该由这些产品的提供商解决。

本信息包含日常业务运营中使用的数据和报告示例。为了尽可能完整地阐释它们，这些示例包括了个人、公司、商标和产品的名称。所有这些名称都是虚构的，如果同实际企业使用的名称和地址雷同，纯属巧合。

版权许可：

本信息中包含了以源语言格式编写的示例应用程序，演示了在多种操作平台上的编程技巧。为了开发、使用、推广或分发符合操作平台应用编程接口（示例程序正是为之编写）要求的应用程序，您可以用任何形式复制、修改和分发这些示例程序，无须向IBM支付费用。这些示例未在所有环境中经过彻底测试。因此，IBM不能保证或暗示这些程序的可靠性、有效性或功能。

本文档（编号REDP-5037-00）创建或更新于2013年11月11日。

商标