IBM软件
行业解决方案

IBM i2 Fraud Intelligence Analysis

识别、调查和阻止欺诈

亮点

- 几乎立即发现新出现的欺诈并提醒调查员
- 分析和可视化复杂的跨渠道攻击
- 相关人员和机构参与调查
- 根据职务和责任及时提供简报

欺诈是金融业面临的一个巨大且不断演化的挑战，据估算每年会蚕食掉收入的百分之五到八[1]。犯罪分子越来越善于利用跨多个系统造成的弱点，他们可能与金融业内部员工勾结，试图利用企业数据的孤立性隐藏自己。除了损害资产收益，欺诈行为还对品牌和信誉构成真正威胁，而且对客户、股东和监管机构都有潜在影响。不过，欺诈者每次接触您的系统都会留下一些小的痕迹，凭借这些痕迹，我们就有机会智能地将它们联系起来以识别、侦测和阻止威胁。

企业应对欺诈的传统做法是利用针对某种特定已知威胁的单点解决方案。这种方法可能很难管理，往往漏过有组织犯罪分子渗透的跨渠道和不对称攻击，而且几乎总是会导致解决方案成本变得更高且离散。这种“后视镜”方式也可能难以发现新兴的攻击。

IBM® i2® Fraud Intelligence Analysis设计用于提供关键的洞察，帮助调查复杂事件，生成重要人物和事件的可操作的可视化内容，并记录结果，以便将它们用于潜在诉讼。

如果您不能掌控全局，就不能做出正确的反应

IBM i2 Fraud Intelligence Analysis采用一种全面的方法来应对这一问题，具体途径是:

- 包含几乎所有数据源，提供欺诈活动的全面可视性。
- 对“坏风险”发出及早提醒，帮助更快地实现修复，以支持了解您的客户(KYC)以及客户审查评鉴(CDD)。
- 分布式调查和协作工具，能够利用相关识和技能来丰富调查和改善结果。
- 使用市场领先的分析和可视化工具，对可疑的或异常的活动和威胁进行识别和取证调查。
- 基于职务和责任提供自动化简报更新，让分析师和调查员能够近乎实时地共享证据和分析结果。

监管、风险和合规

欺诈的性质要求由组织的GRC职能部门来执行对欺诈的侦测、管理和处理。风险管理、合规以及内部和外部调查组的要求各有不同且互相关联，它们要求从不同角度观察欺诈活动，最重要的是需要证据来支持决策和行动。

IBM i2 Fraud Intelligence Analysis经过周密设计，使这些企业职能部门能够轻松查看欺诈模式的相应元素，并更有效地进行协作，以便采取适当行动来满足各部门管理和应对欺诈的需要。

分析和可视化

IBM i2 Fraud Intelligence Analysis提供了市场领先的设计分析工具，能够对异常和意外行为进行快速的取证调查。

凭借这个解决方案，用户可以分析来自多个不相关来源的大量数据，并且可以采用多种丰富格式将这些数据可视化，以支持调查。

图2: 关联——谁认识谁，他们有什么联系？

风险提醒

及早发现可能的欺诈能够消除与复杂调查和索赔有关的成本、时间和痛苦。知道“谁是谁”和“谁认识谁”是这个过程的关键。关键欺诈指标将来自黑名单、已知诈骗者和其他相关来源的信息汇总到一个风险评分卡上，提供了风险的可视性，从而帮助实现积极补救措施。

协作和调查

防范欺诈需要您的整个组织的情报和参与。IBM i2 Fraud Intelligence Analysis为相关人员提供了一个直观且安全的接口，便于他们贡献、共享和分析调查数据，从而制定更快、更明智的决策。

信息传播

实时传送可操作情报有助于确保您的响应团队掌握所需信息。利用包括富文本、图像、表格、统计和图形构件在内的多种组件，可以创建个性化的仪表板。

通过及时和安全地传输信息，用户能够确保使用相关和可靠信息来应对威胁并增强内部意识。

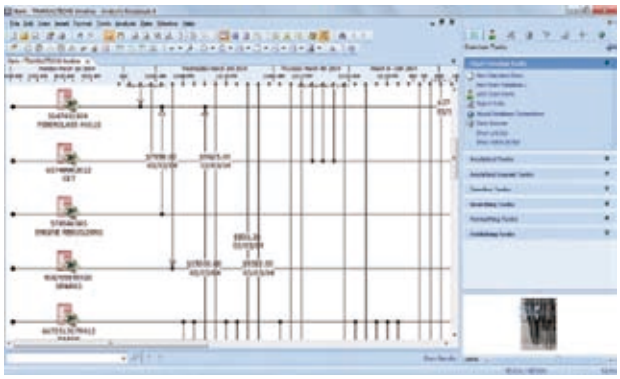


图3: 时序——时间线上的事件和相关方

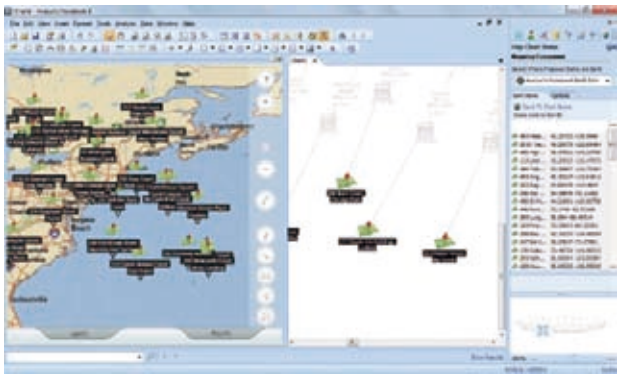
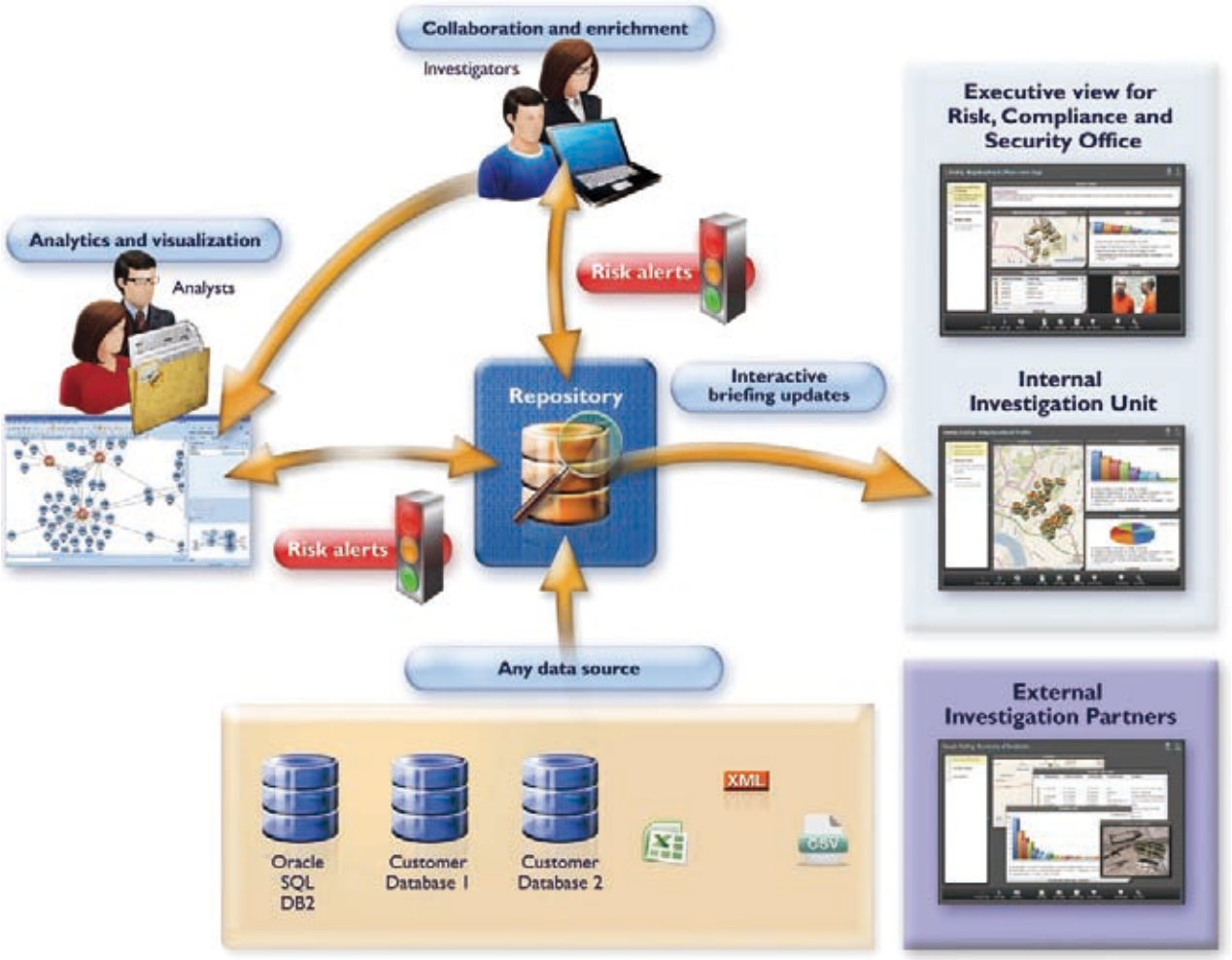


图4: 地理空间——地图上的事件



打击跨渠道攻击

数据可能会被锁定在分散且没有联系的数据库中，而且可能以结构化或非结构化的形式进行存储。

IBM i2 Fraud Intelligence Analysis专门设计用于克服这一弊端，它能够跨数据孤岛工作，提供相关事件、人物和对象的“联合”丰富视图。

潜在优势

- 快速。更快的实施和回报，通常只需数周。
- 灵活性。数据可以保留在现有服务器上，调查和报告接口通过瘦客户端交付。
- 统一性。与您的内部信息政策保持统一。根据职务，只需为用户提供适当信息。
- 扩展性。可以与现有系统以及其他IBM解决方案相集成。

金融诈骗用户案例

大型美国保险公司：在三个小时内成功地发现和调查出25万美元的欺诈索赔

美国的一家大型保险公司收到一份可疑的汽车失窃索赔，他们只有30天的时间来确定该索赔是否合法，超出该期限则必须予以赔付。使用IBM i2 Fraud Intelligence Analysis，调查员能够迅速调查与车主关联的社会网络，发现该索赔与一家结构异常的出口公司有关联。通过与美国海关和边境巡逻部门合作进一步开展调查，确定该车辆已经在索赔前数周出口。调查员追踪这辆汽车到意大利并发现了进一步的证据，该车已经在当地进行维修，而且新车主的身份是索赔者的妻子，而且索赔者在当地使用了假冒身份。该索赔被拒付并提交给执法部门。

“使用IBM®i2®Analyst’s Notebook®，我能够在不到三个小时的时间内清晰地判断出是否存在索赔欺诈，如果没有i2产品则可能需要花费数月的时间。”

— Raphael Lawson，欺诈调查部主管。

详细信息

欲了解i2系列产品的更多信息，请联系您的IBM代表，或访问:

www.**ibm.com**

欲了解所有的IBM Smarter Cities解决方案的更多信息，请访问:

ibm.com/smartercities

IBM Corporation Software Group Route 100
Somers, NY 10589
U.S.A.

在中国印制
2012年9月

1 Forrester市场概述: 2010年欺诈管理解决方案。

请循环利用

ZZS03075USEN-00