产品简介

Datiphy公司提供领先业界的人工智能数据安全保护方案。Datiphy的核心技术DataNDA得到美国国家专利局多项科技发明奖，其强大的搜索引擎每天可以处理数十亿笔的数据资产。 DatiDNA提供用户即时搜寻特定数据并做关联性比对，能将数据资产立即分门别类确并保其不能被篡改。Datiphy完善的信息保护机制能协助企业做到事前防范，事发时提供预警以采取因应措施，事发后瞬间回溯到问题时间点取证记录，因此数据生命周期的每一个阶段均受到全面的跟踪和保护。

有鉴于传统安全工具只能做到单點保護，对数据变化缺乏前后关联性比对， Datiphy 為用戶提供了“以数据为中心”的安全保护机制，就像每个人拥有不同的DNA 一样，DatiDNA 尖端技术可以找出每个数据獨特的DNA图谱，DNA图谱中的每一个资产会自動搜寻其他关联性交易。这种強大的搜索引擎能掌握敏感数据的动向，真实呈现出数据在企业内部流动时各阶段被使用的方式。

Datiphy的DatiDNA是第一个真正以数据为中心的审计和保护的安全机制，已经广泛应用在大型金融机构、银行、医院、学校、和电商；是企业应付外来攻击、内在威胁、保护敏感数据、审计和符合法规的最佳选择

行为模式管理

随着大数据时代的来临，如何有效管理海量的数据资产是企业最关切的问题。Datiphy 数据安全解决方案了解每一笔数据资产的特性并对其行为模式作关联性的比对和管理，若数据行为有任何变化或异于常态，就会立即被侦测出并发出预警

符合内外审计法规

Daitphy的数据安全解决方案每天能处理数十亿笔数据交易，并将其作实时的分门别类，便于日后搜寻使用。每日数据活动能从“人”、“事”、“时”、“地”、“物”五个层面做剖析比对

安全

数据快速成长严重挑战企业传统的安全政策。 无论企业采用实体机或是云端部署，Datiphy的人工智能技术均能有效的协助企业面对大数据时代信息安全的挑战。

回溯搜证

可使用自然语言搜索任何一笔特定事件、活动、或资产，能立即回溯到事发当时找到关联性的证据。

数据 DNA 和科学行为模式解析

每笔数据交易均会有一系列独特的行为模式。 DatiDNA技术能即时搜寻数据资产并创建索引，并以数据资产之间的科学关系建立数据行为的基准模式。因此每一笔交易均会和模拟样本作比对，任何行为上的变化会立刻被发现，大量减低错误警报發生的可能性。

深层回溯调查降低企业风险

想像Datiphy的数据安全产品如同是数据的录像带，它能够详细取证、实时索引，让用户看到企业的敏感数据在日常运作时各阶段的动向。遇到可疑的攻击时，用户可以重播事件、研究战术、并制定政策,对未来类似的攻击提早发出警报采取行动。

整合数据孤岛的安控措施

企业的数据不断的在各部门流动，传统以部门数据库为中心的安全保护机制已经不能因应大数据时代的需求。Datiphy提供客户“以数据为中心”的安全架构，能够跨越部门的数据孤岛，整合协调各部门数据资料，无论数据呈静止或流动状态， 均能达到高可视性、高安全度的目标。

保护企业声誉

当企业数据被窃的细节在各大媒体相继报导后，一般企业均难以招架，因为他们根本还搞不清楚到底有多少数据流失。Datiphy的安全解决方案能在第一时间点找到相关证据，厘清责任归属，让企业的管理阶层了解真相并立即采取应对措施以作危机处理，降低对企业造成的伤害。

用户比对映射

黑客经常采取的是以盗用账号方式登入数据库窃取数据。从最初的HTTP请求开始，Datiphy专利的用户映射技术便可以将用户和他们的行动全面作有效的连结串联，让黑客难有切入端口。

威胁自动侦测和日志管理

以往企业常使用日志记录作为数据安全管理的手段，然而日志本身数量庞大而且缺乏相互关联性，实非理想的方法。目前大多数企业在面对数据的安全威胁时都不知该如何处理。 Datiphy公司提供人工智能方式自动侦测威胁，弥补日志记录看不到数据内容和缺乏关联性的缺陷，所以企业在面临可疑威胁时能立即采取因应行动。Datiphy 以数据为中心的解决方案大大提高了数据的可视度，企业实时掌握数据的动向，能够有效的检测出各种有针对性、潜伏性、和瞬息万变的攻击的方法。

数据内容的关联性

市面上有许多工具宣称他们可以让用户一窥企业的数据资产，然而他们却缺乏一个完整性的故事； 就如同你可以看见一张张的照片，却无法得知照片拍摄的时间和每张照片之间的关联性。使用Datiphy以数据中心的解决方案，用户看到的是犹如播放录像带的视频，不仅可看到数据资产前后的关联性，甚至还能够全盘了解这些资产如何在各部门间流动和交互使用。

看见数据所有的变化

由于Datiphy能够记录每一个数据交易的细节，所以在意外发生时，用户可以使用Datiphy的搜索引擎立即找出相关事件并检视事件发生的真实情况，进而采取适当的方法迅速而完整的恢复事发当时状况。

简易的事件搜寻和取证

由于Datiphy实时标示了每一笔数据交易的细节并将其依特性分门别类，所以事发当时对相关事件搜寻或事发后的取证也相对容易。事件调查小组随手就能够找到问题发生的原因并且有足够的证据佐证，搜索和报告能从“谁”、“在什么时间”、“从什么地点”、“用什么方法”、“窃取什么数据”等各层面来搜证叙述。

知道谁在看你的数据

一般拥有读取权限的人比拥有修改权限的人多。 Datiphy记录了所有阅览过敏感数据的轨迹，无论这些敏感数据本身是否被更动过。

有效验证威胁的真实性

由于企业往往分不清楚威胁警报的真实性，因此在人力物力无法负荷的状况下，企业对这些威胁警报通常会采取置之不理的态度，不愿意展开调查工作。但是如果攻击事件属实，企业往往丧失了有效对抗攻击、降低损失的黄金时间。Datiphy的数据安全解决方案可以针对警报立即提供相关细节，让调查人员能够迅速验证实际威胁的真实性并采取因应措施。

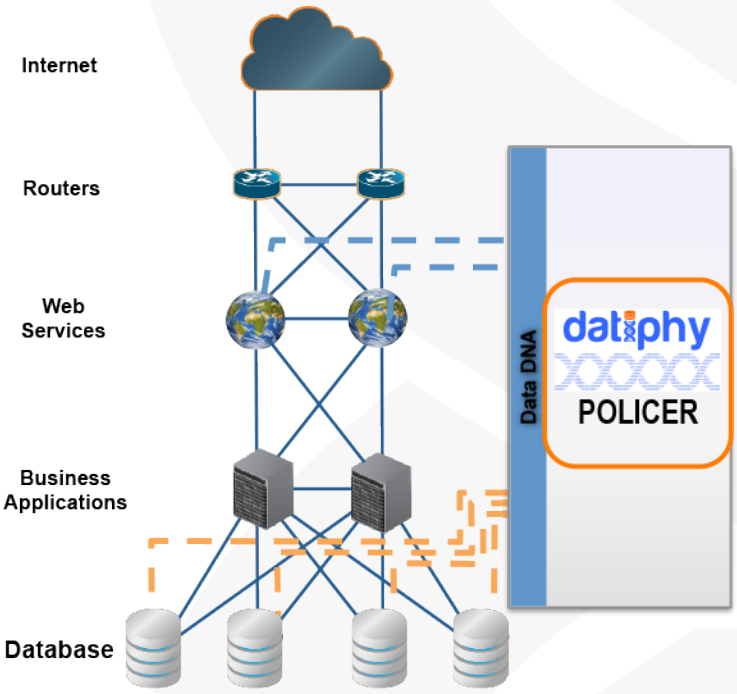
有效采取应对措施

Datiphy 能够协助企业过滤假警报以避免人力物力的浪费。调查小组调查范围只限于对事实的调研，所以调查的进行能够实时而迅速，避免攻击者有足够的时间湮灭证据或覆盖攻击的轨迹。

有效预防类似事件再度发生

当可疑的攻击事件发生时，Datiphy的人工智能可以立即侦测到是否有曾经发生过的类似攻击行为，并立即比对其间的相互关系。Datiphy可以通知用户立即阻断该攻击，确保其攻击行动无法顺利进展下去。

欲了解更多信息或索取产品演示，请访问：
www.datiphy.com/schedule-demo/



以上的图片代表典型的产品部署方式

ADDRESS
2290 N. First Street, Suite 204
San Jose, CA 95131

WEBSITE
www.datiphy.com

SALES
sales@datiphy.com
+1.888.343.9938