datiphy™

案例分析
金融和银行客户案例分析

金融机构使用Datiphy DatiDNA系统监测和保护数据资产

金融机构在运行日常业务时，常常会产生大量的敏感数据，因此必须设定严格的监管规则让内部员工遵循。另外，在提供客户便捷的服务时，银行业者尚需考虑到如何保护自己的IT系统免于受到一系列的恶意攻击。为了保持运行平稳和安全，许多企业之前都透过防火墙的设置和SIEM（安全信息与事件管理）作为信息安全防护措施，后来才发现这样的安全机制完全抵挡不住内部的威胁，尤其是对特权用户。

现在让我们举一个真实案例来探讨单靠外线信息安全防护（如终端机或是网路安全）可能产生的数据安全漏洞。故事主角是Datiphy的一家银行客户，他们有许多往来超过数十年的老客户。这些客户有些账户因为多年未曾使用而处于停滞状态。这类停滞账户缺乏关注，也没有合法的继承人，所以引起了银行内部经手这些账户的行政人员和数据库管理员的注意。于是他们共谋，想利用本身特权将钱先转账到管辖的临时账户，然后再分批从此账户提取资金，神不知鬼不觉的把钱据为己有。银行的员工对内部的运作非常熟悉，这种非法转账的现象持续了很长一段时间却没有被发现，在取得足够数目的金额后，共犯关闭了原停滞账户和临时账户，分享犯罪所得。虽然银行可以对数据库的访问设置政策和规则，特权用户往往知道如何回避规则并掩盖犯罪证据，如删除更改日志等等。这种犯罪行为防不胜防，甚至连起诉证据都难以备足。

产品效益：

- 审计独立
- 连续完整的合规性监控
- 即时电邮，SMS,Syslog,SNMP警报通知
- 完整独立而不能被篡改的记录
- 即时情报，支持多品牌数据库的异构环境

事发后，为了寻求更安全的保障以杜绝类似威胁事件再度发生，这家银行选用了Datiphy公司具商业智能，获得多项美国专利的数据安全产品：DatiDNA。

现在让我们来探讨在使用Datiphy DatiDNA的事前，事中，和事后各阶段的效益与附加价值。

事发之前：	未使用	使用
审计	以管理员或资讯人员提供的数据为主	审计独立，由另一组人员主导（如CSO资讯安全人员）
合规	非经常性，由资讯人员审核，审核项目受局限	持续而全面性的监控

银行经常会定期审计IT系统的合规性以防止违反信息安全的行为产生。然而这种审计方式必须仰赖IT人员提供数据，而数据的提供者有可能包括意图犯罪的员工。这种依靠人工作业去搜集数据的审计方式既繁琐又耗时，所以不能经常执行。因此，意图犯罪者便有了足够的时间和机会在提供审计报告时掩盖自己的违规行为。Datiphy DatiDNA能独立于一般的IT运营之外，无需耗费额外人力就能自动产出符合法规的审计报告，而这些报告甚至可以不受IT人员的管控以确保其独立性。

事发当时:	未使用	使用
警报	能力有限，通过DB或其他应用程式或日志记录	即时电邮短或信通知，SMS, Syslog, SNMP
行动	能力有限，通过DB或其他应用程式或日志记录	配置可依用户需求自定设定的脚本以执行网络或数据库管理

在没有使用Datiphy产品的情况下，银行的员工可能知道甚至参与设定警报触发器和SIEM的日志系统，因此，他可以轻易规避或逃过检测。 DatiDNA提供精确配置的警报，其警报触发策略可以由一个独立的安全团队（如CSO或风险管理部门）执行，所以内部的员工若有任何违规行为马上就会被暴露出来。 DatiDNA系统的设置可以依据人，事，时，地，物任意组合警报，再加上行为模式分析和签名政策，数据的安全更有保障。DatiDNA还可以依用户需求自定预设的配置脚本，当警报响起后，用户能轻松的依照脚本行动以防止违规事件发生所带来的损害。

事发之后:	未使用	使用
回溯取证	内部人员可以删除日志或湮灭证据	完整独立而不能更动的数据记录
分析	即使日志有记录，搜寻仍非常耗时，若同时拥有不同厂牌的数据库，难度更大	数据即时分类组织，便于立即查询。支持不同厂牌数据库的查寻

在数据安全违规事件发生后，彻底调查该事件发生的原由和追究相关负责人极为重要。不幸的是，往往在调查展开之前，肇事者已经有充分时间可以借由删除日志和改变数据去掩盖自己的罪行。DatiDNA对企业数据作永久的录制并保证其不能被篡改。这些永久记录有利于及时发现犯罪行为，且为日后追究相关责任或采取法律行动提供了充分的证据。DatiDNA对所有的数据作即时而精确的分类归纳，只要输入关键字就能立即搜集到相关数据活动，企业可以用来做必要的事件分析并新制定法规策略以杜绝类似的弊端再度发生。

总而言之，内部威胁是今日一个重要的安全问题。大多数企业持有敏感数据却找不到有效的安控措施。虽说设定严谨的安全法规有助于防止数据安全漏洞：例如，对使用者分级设定不同权限，可以防止企业内部人员对敏感数据的不当使用。然而，在建制内部安控架构时，安全设施部署的便利性也须纳入考量，因为在执行上过于繁琐的方案会降低企业的运营效率。纵观企业多方面的需求，Datiphy获得多项美国专利的创新技术DatiDNA，为企业提供了部署简便，安全性强，灵活度高，又便于日后扩展的全方位数据安全解决方案，是企业选择高效益数据安全解决方案的最佳选项。

欲了解更多信息或下载产品试用，请联系info@datiphy.com或访问www.datiphy.com

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

WEBSITE
www.datiphy.com

SALES
sales@datiphy.com
+1.888.343.9938