datiphy™

案例分析
教育

各大学利用Datiphy智能平台保护数字资产的安全

近年来，越来越多的新闻媒体相继报导大学遭受黑客攻击，导致学生身份证号码和信用卡资料大量外泄，校园内的信息安全饱受威胁。由于每年必须定期举办高考招生和周期性的考试，再加上各种不同的学生活动，因此常会有新数据产生和更新的需求。为了应付大量数据储存的需求，学校的数据库容量必须要够大，而且还需要不断扩增。再者，数据必须能够长期保留，甚至一直到学生毕业后仍不能删除。大学这种大量储存个人数据的宝库，经常会被黑客造访攻击。大学的基础设施必须要能支持教育、科研、学生活动和社区服务各类不同的功能。大一点的大学甚至在校园内还设有实验室、宿舍、收银员、体育馆、食堂、商店、甚至诊所、音乐厅或剧院。这些设施都需要IT的支持来提供各种各样的服务。最麻烦的是这些数据用户经常经常变化；例如，教授经常会被分配到不同的学生来管理员实验室的系统，教授们也会授权学生助教查阅记录成绩的系统。在这样复杂的IT环境中，Datiphy在帮助各大学保护他们的数字资产，扮演了一个关键性的角色。

效益:

- 持续和全面的监控
- 实时电邮、SMS 、 syslog、 SNMP警示
- 用户可以自行设脚本执行管理网路或DB
- 全面和独立的数据库活动记录
- 及时查询支持多种品牌数据库环境

以下举两个在大学经常发生的事件来说明数据安全的隐患。案例一:有些学生为取得好成绩,常用的方法之一就是行贿，其对象往往是有权更动成绩记录的数据库管理员。由于授课的学生人数众多，繁忙的教授大概都不会注意到某些成绩被篡改。借着Datiphy产品的帮助，教授提交出去的原始成绩会受到保护，任何意图更动均会触发警示机制，管理者会收到相关的电子邮件或短信的违规提醒。案例二：大学新生在收到一些本地企业提供免费服务或银行提供开户的电子邮件或电话时，应该注意到使用各种便捷营销服务的同时，个人机密资料是否已经外泄。尽管大学可以实施严格的安全控管，以防止外部威胁：如黑客攻击等等，然而内部的威胁却是防不胜防。数据泄漏事件可能来自一个不法的雇员或某些IT人员对数据的更动或篡改。 Datiphy，提供以数据中心的解决方案，每日可以处理上亿笔的大量数据，迅速检测出可疑的活动，并产生实时警报以告知相关负责人采取因应行动。

现在让我们做个简单的比较表，在上述两种情况下，使用和不使用DatiDNA產品会造成哪些差异。

事发前：	未使用	使用
审计	审计依赖IT或行政人员提供	审计独立,由专职小组操作
符合法规	不经常性、小范围的执行合规审计，需要透过IT人员检查是否合规	持续和完整的数据安全监控，由非IT相关的审计人员操作

学校会审核其IT系统，以防止安全违规，但这种审计通常依赖管IT部门行政人员提供数据。在上述两种情况下，内部人士可能知道审计实践的方法，所以可以轻易规避。 Datiphy DatiDNA的审计独立于常规的IT操作，因此审计可以在监控人员管辖外独立进行。

事发时：	未使用	使用
警示	能力有限，以DB或其他程序登入	即时电邮,SMS, syslog, SNMP
行动	能力有限，以DB或其他程序登入	用户可以自行设脚本执行管理网路或DB

如果没有Datiphy DatiDNA的幫助 ，建立警报触发機制以管制內部違規將不是一件简单的事；更何況內部人员往往知道如何避免触发警示裝置。 DatiDNA提供可自行設定的警示，警報触发政策可以由一个独立的安全团队来管理，因此业內人士的侵权行为更容易暴露。 DatiDNA系统可以由用户自行设定，依照人、事、時、地、物不同層面設定警示政策，并进一步針對行为策略和签名內容政策任意组合警报。若有任何安全违规情形发生，DatiDNA可以实时发送警示和执行预先配置脚本来减轻损害。

事发后：	未使用	使用
回溯	內部违规者可以删除日志或毁灭证据	所有的记录独立而全面记录,且不容被更改
分析	非常费时,即使有日志,但不能支持异种厂牌数据库	组织方式利于立即搜寻,支持多厂牌数据库环境的即时数据提取分析

安全違規事件發生后，进行全面调查，并找到相關责任人是很重要的。不幸的是，往往在事件發生后到调查展開之前，內部肇事者可以通过删除日志和数据改变來掩盖自己犯罪的軌跡。 DatiDNA提供了一种永久的记录，这是不能被改变也不可被否认的证据。因此，行为人将很快被发现和追究相關责任。因为所有記錄是精确而有组织的，所以可以很方便去分析事件及其相关活动，可以用於日後安全策略的改善。

总之，今天大学必須面对外部和內部数据安全威胁和挑戰。在上述情况下，严格的政策法规，如要求对敏感数据访问時作多層级授权或許可以有一些帮助，然而如果有电脑或手机被偷或不小心遗失，这种凭据泄露的突發情况就无法掌控了。此外，教授们因爲忙碌，常要求学生提供临时帮忙，学生素质良莠不齐，這也增加了数据安全控管的难度。Datiphy DatiDNA的数据安全解决方案，运用最尖端的人工智能技术，能够将数据依其特殊性质分类，就如同人类的DNA一样，如果有任何外部病毒细菌意图攻击或者內部细胞异常产生病变，DatiDNA马上会发出警讯，就像人体的免疫系统立即採行防卫抵御攻击，在最快的时间內采取有效的因应措施。DatiDNA的人工智能技术每天能处理数十亿笔的数据，能实时有序的将数据分门别类，易于日后查询，是针对大数据时代需求而产生的尖端安全产品。企业的安全极难做到360度的全面保护，最重要的投资应该放在“以数据为中心”的安全方案才能达到最大的投资效益。

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