datiphy™

产品简介
数据行为分析 — DBA

信息安全面临的挑战

目前以网络主体的信息安全架构往往缺乏对数据活动的可视性，以致造成企业信息安全防护网的重大缺失，严重威胁了企业重要资产和敏感数据的安全

Daitphy 产品效益

- 辨识，分类，记录数据库中的数据活动并和人（使用者）事，时，地，物充分连结。
- 根据行为分析和稽核结果可及时采取必要行动。
- 使用者自订的报表内容和规则符合个资法 (PII)，医保法 (PHI)，和信用卡资讯安全保护。
- 提供使用，监控，警示等安全机制给系统使用者，管理者，或程式开发员。
- 对入侵及时分析，所有数据活动全都录，有利于在事发后对异常行为作彻底的剖析
- 事件分析可与其他网络工具作整合，如 SIEM，建制更全面的安全框架。

企业的当务之急是如何增加数据的可视性以确保其使用的安全性。始自应用程式开发周期之初，数据库可能已饱受威胁。这些运行的数据库无论属于结构性或非结构性，部署于公司内部或架构在混合云端，已经提供给意图窃取数据者作案的良机。搜索，分类，保护和记录所有的企业数据资产是防止机密泄露和数据保护的首要任务

一般来说，数据盗窃的主要方法是攻击数据库。数据犯罪的慣窃通常能轻易躲过防火墙，入侵防护系统（IPS），以及终端机的安全装置。完备的企业安全机制必须部署不同层级的保护措施，单一的保护方案无法抵御来自内部或外部的蓄意攻击。

着重于网路流量和使用者分析的安全方案，对企业敏感数据本身的安全缺乏防护。数据库行为分析（DBA）旨在于弥补企业安全机制对数据活动观察和分析不足的缺憾。企业的安全运营有赖于对所有数据的全面控管。了解数据，掌控数据是保护企业信息安全的不二法则。

企业信息安全的新思维

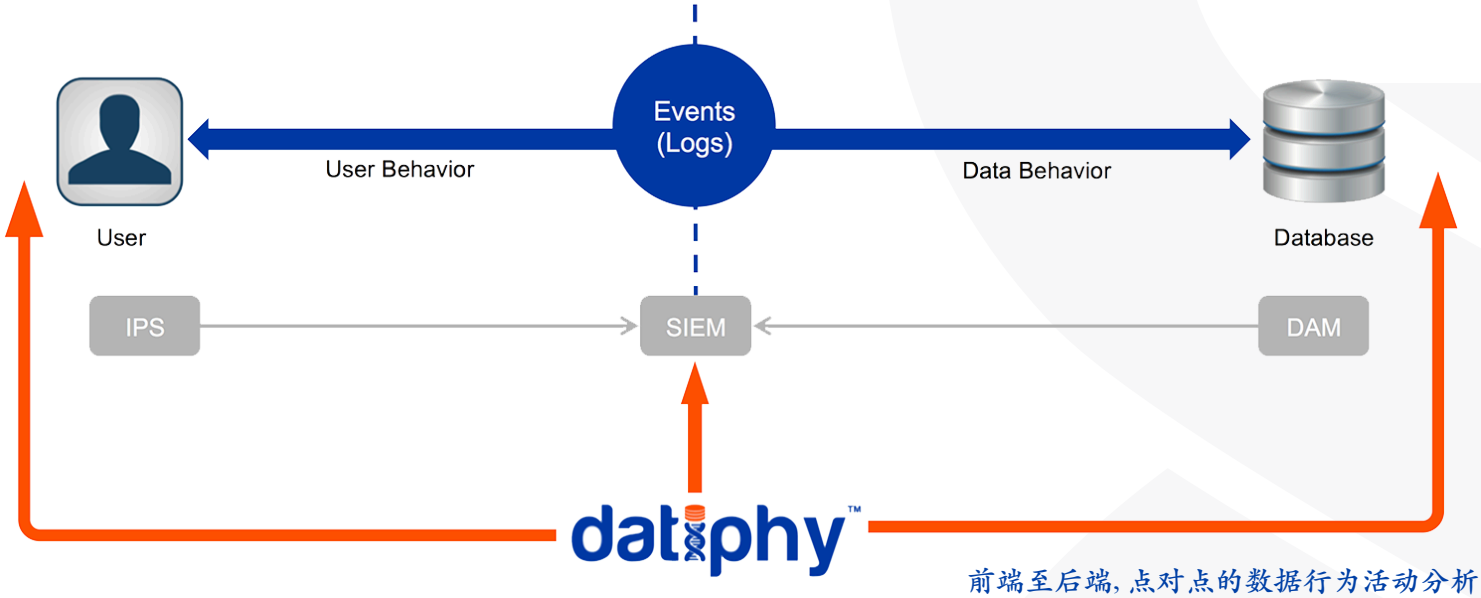
亘古不变的真理 –“你无法保护任何眼睛看不见的东西”– 这个真理至今仍然屹立不摇，尤其处在今天这个诡谲多变的网路世界里。资讯泛滥影响讯息的可视性，也相对造成企业在遭受攻击后有如瞎子摸象，在黑暗中试着大海捞针去找寻攻击的来源和被攻击的标的物。处在大数据信息泛滥的时代中，企业纷纷寻找类似DBA:能充分监控企业数据的一切活动的解决方案。

熟悉企业内数据活动的行为模式并侦测到异常行为是保护数据的唯一有效方法。了解网页使用者如何连结到数据库是侦测异常行为的重要依据。另外，了解应用程式的服务器如何与数据库连接交换数据亦有等同的重要性。另外，诸如数据库管理员，程式开发员，网路工程师等等能够看到大量信息的高权限使用者可能是造成数据受威胁的潜在因素。

数据分类

識別環境中的所有數據庫之後，可以开始对储存敏感數據的 數據庫進行分類。针对使用者自行定义的内容的属性可过滤并找出具有各种敏感性的数据，如信用卡號碼，身份证号码，駕駛证照信息，醫療記錄，銀行賬戶或護照號碼。安全专家均希望能够针对自行定义的数据模式进行监控。 监控范围并不仅仅限于数据库本身，还涉及到敏数据的准确位置 - 数据库，列表和栏位的可视性。

敏感的数据被确定之后，下一个主要步骤是跟踪和分析所有的用户行为。这可能包括 Web 应用程序的用户，数据库管理员，应用程式开发人员或 DevOps 工程师。具体监控的对象必须包含对所有敏感数据有访问权限的用户，亦即监测已被授权和未被授权所有用户对数据使用的行为总览。



前端至后端，点对点的数据行为活动分析

数据安全的防护

一旦敏感数据被界定，保护和管理相对容易。集中管理和权限控制访问仅仅是数据保护的其中一环。了解行为模式，然后发现环境中的动态变化才是关键。最常见的攻击来自于用户帐号被盗用或内部权限的滥用。此种情况下，虽然用户被完全授权访问数据库，但是，这种恶意用户和一般使用者的行为模式会有不同之处。僭越权限侦测是另一个防护要点 - 即一个未经授权的 IP 附属 网僭越权限访问数据库。

如果一个应用程式每次只探访一个数据库，在预设的时间里做固定的资料查询，比如说每次只查询单张信用卡，那么有心人士可以在政策和报警的预设上允许同时汲取多笔信用卡数据。这是利用 SQL 注入应用程式以窃取敏感数据的惯用手法。另一个可能的攻击方式是由真正的应用程式 Datiphy DatiDNA 安全防護系統不僅能檢測出有哪些數據被盜用，同时确实记录取证，并提供线索以修补信息安全使用者利用在查询单笔数据时，倾倒整个数据库的内容作 SQL 注入的漏洞。很多时候，企业和政府机构因信 息外泄的丑闻而感到尴尬不已，品牌信誉度大幅下滑，甚至影响到年营收。确实掌控数据信息，加强信息安全防范意识能够协助企业实现最佳运营效率。大数据时代的数据信息成等比级数增长，以数据为中心的安全考量将对实体或云端数据库提供最佳的可视性。

DATIPHY 公司简介

Datiphy 产品弥补了单点式资安工具的不足，它提供一个高透视度的平台，在数据流的各重要关卡部署侦测站，检视企业数据的生命周期的各种活动。 Datiphy 技术核心是其专利的数据行为模式（也称为 DatiDNA ）它能够及时分析数据库中所发生的事件，并提供相关的科学证据。使用者仅仅下一个指令就能启动集中管理数据库和自然语言查询，在几秒钟内即能搜寻到任何一笔数据资产，并看到它和所有其他相关数据资产之间的互动变化。

如果您想了解更多 Datiphy 的产品信息或是安排产品演示，请联络我们或造访我们的网址 www. datiphy.com

datiphy™

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

WEBSITE
www.datiphy.com

SALES
sales@datiphy.com
+1.888.343.9938