INFORMATICA®
The Data Integration Company™

动态数据脱敏最佳实践

实时保护生产应用程序和数据库

白皮书

此版本发布于 2011 年 10 月

目录

引言

财务记录、员工或客户个人信息等敏感数据需要保护，既要避免被未经授权者获知，还需遵守世界各地日益增多的隐私保护法规。与此同时，企业环境正变得更加错综复杂，从而要求为监控与保护企业持有的数据增加开支和加大投入力度。动态数据脱敏（DDM）通过定制数据脱敏、加密级别以及在个体层面进行封锁，以具有成本效益的方式添加额外的数据保护层。借助于 DDM，IT 组织能够为授权用户提供相应的数据访问等级，而不必对代码或数据库进行任何变更。

对动态数据脱敏的需求

支付卡行业数据安全标准（PCI-DSS）、金融现代化法案（GLBA）、BASEL II、欧盟个人数据保护指令、HIPAA 以及其他隐私保护法规均是为了应对同一个不断增长的问题而制订的：针对敏感信息及个人信息的暴露和盗窃。这些法规要求组织基于其用户的业务职能限制数据访问权限。不过，在组织范围内全面执行这一政策并非易事，尤其是在包括了外部用户以及外包和兼职雇员的环境中。

例如：

- 某组织使用 PeopleSoft 来管理人力资源，因而需要向管理员和顾问提供其履行 HR 任务所需的数据访问权限，但同时仅向特许用户提供所有详情。
- 一家大型银行为保护客户隐私而需要对其数据库环境内的账户信息进行匿名化处理，但又不能对设计人员、顾问、承包商、开发人员和 DBA 的日常工作造成干扰。
- 一项关键业务遗留程序因其仅包含最基本的用户权限管理功能，从而给一家主要保险公司的客户保密政策和财务数据安全带来风险。

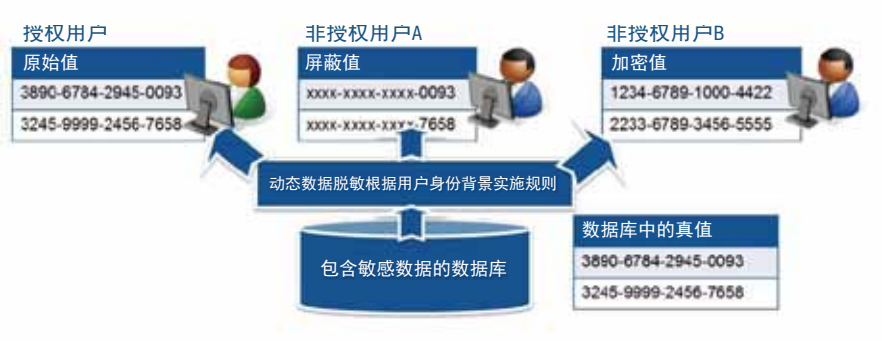
在大多数情况下，针对打包和内部开发应用程序以及开发和 DBA 工具中的敏感信息限制访问权限的成本异常高昂，而且极为耗时。许多数据库访问监控（DAM）解决方案能够审核用户访问记录，并在发生数据泄漏问题后帮助进行识别，但它们无法对敏感信息进行匿名化处理，以便防患于未然。其他技术则要求进行大规模的应用程序变更，导致不可接受的性能问题，且无法为所有需要保护的多种个人信息提供保护。

因此，需要一个与众不同的安全措施，既能够提供更严格的规则、更准确的审计和更细密的访问监控，又能够保留针对用户的透明度。这一解决方案就是 Gartner 在其名为 “2010年应用程序安全卓越供应商（Cool Vendors in Application Security, 2010）”的报告中首创的术语 — 动态数据脱敏。

动态数据脱敏简介

动态数据脱敏是在个体用户层面对数据进行独特屏蔽、加密、隐藏、审计或封锁访问途径的流程。DDM 解决方案是一个代理软件，安装在作为业务应用程序、报表和开发工具及数据库枢纽的单一服务器内。

当应用程序请求通过 DDM 层面时，该解决方案对其进行实时筛选，并依据用户角色、职责和其他 IT 定义规则屏蔽敏感数据。它还能运用横向或纵向的安全等级，同时限制响应一个查询所返回的行数。DDM 以这种方式确保业务用户、外部用户、兼职雇员、业务合作伙伴、IT 团队及外包顾问能够根据其工作所需和安全等级，恰如其分地访问敏感数据。



上图展示了 DDM 的运作方式，图中有三名用户对一个内部工资管理系统进行访问。左侧为 HR 经理，该经理获得授权，可查看姓名、账户信息和薪资等全部详细个人信息。中间为兼职的工资管理系统雇员，该雇员仅被授权查看以屏蔽形式显示的数据，以便执行管理任务。右侧则是开发人员、DBA 或生产支持人员，他们出于 IT 方面的用途而需要以相应格式显示的信息，而 DDM 解决方案将为遵守隐私保护法规向他们提供加密过的数值。

动态数据脱敏对比其他安全技术

加密技术可被部署于多种基础设施组件中。但是，虽然终端层面的加密对用户而言具有透明度，它无法在应用程序层面保护数据。同时，应用程序层面的加密要求在使用数据之前进行完全解密，因而为未经授权的访问提供了机会。该技术还要求变更源代码或数据库，令其难以用于常见的打包应用程序，且费用高昂。

存储加密技术只能在静止状态下保护数据，因此无法为应用程序提供隐私保护。数据被解密以供读取并由业务应用程序和工具加以展示，导致数据在使用过程中承受完全曝光的风险。

标记化（**Tokenization**）技术以虚构数据代替数据库中的敏感数据，可保护信用卡号码，但无法对姓名、地址和其他非参考信息进行匿名化处理。此外，标记化技术要求对数据库和源代码做出耗资耗时的更改。

数据库访问管理可针对个人信息的访问时间和访问者创建详细的审核记录，同时还能提供基本的 SQL 请求封锁功能，但不足以达到企业业务应用程序每秒处理数百个 SQL 请求所需的水平。

对比之下，DDM 使用内嵌 SQL 代理程序，在数据库协议层面发挥功能，从而实现完全透明度。对于调用程序来说，DDM 解决方案可看作一个源数据库；对数据库来说，它则是一个应用程序。因此，DDM 适用于所有的打包和定制应用程序、报表和开发工具，无需对数据库进行变更，亦不必访问应用程序源代码。

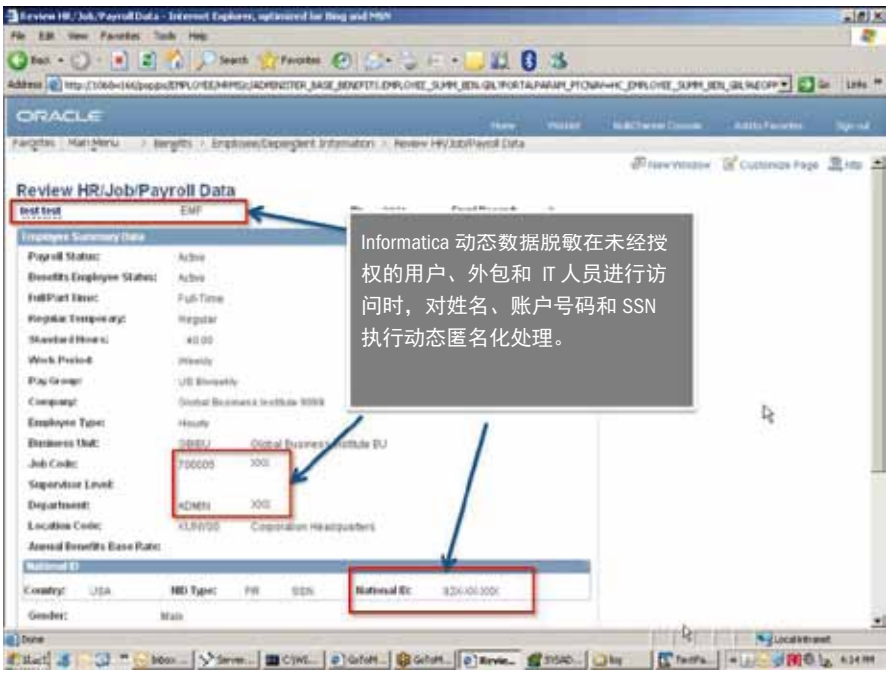
动态数据脱敏最佳实践

通过遵循本步进式流程采取最佳实践方法，组织可在几天之内安装、测试和部署 DDM 实施方案：

1. 将数据按三项类别划分，以确定哪些数据需要保护：
   - 高度敏感数据（信用卡号码、护照号码、姓氏、地址、账户号码、社保号码等）
   - 中等敏感数据（名字、出生日期、财务记录等）
   - 非敏感数据
2. 确定使用隐私数据的应用程序。任何包含个人验证信息（PII）的应用程序都是 DDM 方案的潜在对象。优先考虑涉及最大数量的敏感数据和用户的应用程序。
3. 界定可接受的假想情况。您的 DDM 实施方案将如何确定需要屏蔽的内容以及接受屏蔽保护的对象？在这一步骤中，您将决定需要对哪些应用程序、报表和批量处理进行保护、应该对哪些字段进行屏蔽、数据脱敏标准以及需要加以配置以便能够始终接收未经屏蔽数据的流程。
4. 通过将这些假想情况按 DDM 解决方案的登录和审计模式运行，对数据进行映射。
5. 制订并检测屏蔽规则，证实这些规则能够有效应用于适用的应用程序和工具中的所有相关筛选功能。
6. 测试应用程序功能。如果 DDM 实施方案影响了其他应用程序功能或破坏了参考完整性，那么它便是没有用的。为维护性能，可考虑限制针对每项应用程序的屏蔽数量。
7. 审核流程。为了达到合规性目的，对被屏蔽数据的访问者和访问时间进行跟踪的能力至关重要，在同时聘用了内部和外包员工的公司内尤其如此。
8. 将数据脱敏规则从生产环境扩展到克隆、备份与培训环境，从而在全企业范围内增强数据安全。

全面动态数据脱敏解决方案

Informatica 动态数据脱敏是首个在市场上推出的 DDM 产品。它是一个为企业级客户设计的应用程序和数据库供应商混合解决方案，这些客户需要实现快速的实时数据脱敏和数据库访问监控，同时又要将对网络性能的影响降至最低。Informatica DDM 可在短短五分钟内完成安装和配置，并与常用的企业业务应用程序天衣无缝地集成，其中包括 Siebel、PeopleSoft、SAP、Oracle Apps ERP Suite、Clarify、Cognos 及其他多种程序。



正如此处 Oracle 的 PeopleSoft Enterprise 应用程序内图例所示，Informatica 动态数据脱敏操作具备终端用户透明度

Informatica 采用的数据脱敏方法基于终端用户的网络权限实时进行，与现有的 ActiveDirectory、LDAP 和 Identity Access Management 软件配合无间，确保每名用户的个人网络登录均会针对该用户有权访问的信息类型，触发响应的数据脱敏规则。这一验证流程能够随着终端用户数量的增长，轻松地扩展至额外的数据库中，所造成的延时仅为 0.15 毫秒，几乎不对网络资源产生任何可觉察的影响。

Informatica DDM 使用多种数据脱敏、加密和封锁方法，这些方法可根据组织的安全需求单独或共同应用：

- 数据替换 – 以虚构数据代替真值
- 截断、加密、隐藏或使之无效 – 以“无效”或 *****代替真值
- 随机化 – 以随机数据代替真值
- 偏移 – 通过随机移位改变数字数据
- 字符子链屏蔽 – 为特定数据创建定制屏蔽
- 限制返回行数 – 仅提供可用回应的一小部分子集
- 基于其他参考信息进行屏蔽 – 根据预定义规则仅改变部分回应内容（例如屏蔽 VIP 客户姓名，但显示其他客户）

此外，Informatica DDM 还具备针对终端用户等级的访问进行监控、登录、报告和创建审计跟踪的功能。该功能可简化遵守数据隐私法规和内部报告需求的流程，同时显著降低数据侵害风险。

Informatica 动态数据脱敏的实际运用

下述三个范例展示了 Informatica 动态数据脱敏如何在业务应用程序与生产数据库中，快速平稳地提供实时隐私保护：

保护生产环境

对于全球最大的电信公司之一而言，为其客户提供高水平的服务是理所当然之事。这意味着该电信公司的开发人员、数据库管理员、应用程序设计人员及顾问需要不受限制地访问生产应用程序和数据库，以便从速解决重大问题。然而，多项隐私法律禁止生产支持人员访问客户地址、信用卡号码和其他敏感的个人信息。通过采用 Informatica DDM，该电信公司现已能够实时对敏感数据进行完全屏蔽或加密，让 IT 部门可以快速识别并解决问题，却不会为客户隐私带来风险。此外，该电信公司如今还可为数据管理与合规性保存全部审计跟踪记录。

将外包风险降至最低

一家大型跨国制造业公司依赖成百上千名外包和海外雇员来开展业务，这些雇员使用应用程序屏幕、打包报表以及开发和 DBA 工具访问生产数据。如今，该制造商采用了 Informatica DDM 对这些雇员进行身份验证，从而在他们进行访问时实时屏蔽和加密所有敏感数据。此项技术帮助该企业维持对其最宝贵的资产 — 信息的严密监控，同时满足针对保护个人可识别信息的法律和法规要求。

保护通用账户

某一组织认识到，虽然拥有诸如“Billing”或“Apps”等通用登录账户便于开发人员与 DBA 访问和监控生产数据库及业务应用程序，但同时也为访问关键业务系统和敏感数据大开方便之门。不过，此类通用账户对于运行重要的经营报表来说必不可少。该组织通过利用 Informatica DDM 设立审计和安全操作规则，堵塞了这一安全漏洞。现在，从通用账户登录数据库的途径已被封锁，并向用户显示警告信息，要求他们以自己的专用账户登录，与此同时数据处理工作仍在继续运行，丝毫不受影响。该 DDM 解决方案还为合规性目的提供了详尽的审计跟踪记录。

总结

在今日竞争激烈的市场中，数据安全和快捷性能缺一不可。凭籍动态数据屏蔽，组织将能够快速升级扩展，为敏感和隐私信息提供实时保护，而不必迫使 IT 部门对应用程序和数据库进行昂贵且耗时的变更，从而避免影响生产效率，更重要的是，不会干扰员工履行其职责的能力。

Informatica Dynamic Data Masking 作为市面上首个真正的 DDM 解决方案，不仅在 Gartner 于2010年发布的 “Cool Vendors”报告中备受赞誉，而且也是2011年的 SC 杂志奖项（SC Magazine Awards）中的信息安全创新类入围产品。其技术充分利用了 Informatica 具有高度可扩展性的灵活数据集成体系架构，并已在全球多家最大型企业和最复杂的 IT 环境中获得了实际验证。

Informatica Dynamic Data Masking 和业界领先的 Informatica Persistent Data Masking（用于非生产环境）组成了本公司的全套隐私保护解决方案，旨在保护数据并保证IT环境中的全方位合规性，从开发和测试直到最苛求的生产业务应用程序。运用这些 Informatica 产品来实施数据脱敏最佳实践，将能帮助贵组织确保唯有授权用户可依据“须知”标准访问敏感数据。

了解更多

了解更多有关 Informatica 平台的信息。请访问我们的网站 www. informatica. com/cn 或致电 +86-10-5879-3366。

关于 Informatica

全球领先的独立企业数据集成软件提供商 Informatica（纳斯达克代码：INFA）让世界各地的企业拥有经营业务所需的及时、准确和可靠的数据，从而赢得竞争优势。全球有 4,630 多家企业依赖 Informatica 提供的数据集成、数据质量和大数据解决方案来访问、集成和信任传统企业内外以及云中的信息资产。有关详细信息，请致电（+86-10-5879-3366）（在美国请拨打 1-800-653-3871）或访问我们的网站 www.informatica.com/cn。如欲直接联系 Informatica，请登录：http://weibo.com/informatica、http://www.linkedin.com/company/informatica 和 http://blog.sina.com.cn/informatica。

INFORMATICA®
The Data Integration Company™

www.informatica.com.cn

北京办事处

地址：北京市朝阳区建国门外大街乙 12 号，LG 双子座大厦
西塔 EF 层 06 室　　邮编：100022
电话：86-10-5675 2000　　传真：86-10-5675 2030

上海办事处

地址：上海市浦东世纪大道 201 号渣打银行大厦 5 楼
邮编：200120
电话：86-21-6182 6825　　传真：86-21-6182 6755

1844（10/27/2011）