



昂楷静态数据脱敏

AAS-DM-S



让人们放心地享受大数据

为什么需要静态数据脱敏？

敏感数据防泄露防滥用

数据是一笔宝贵的资产，不管企业还是政府单位，每天都有大量的信息在汇集、存储和共享，且规模越来越大。大规模的数据在给社会带来前所未有的应用价值的同时，敏感数据泄露的风险也与日俱增。许多组织在他们例行拷贝敏感数据或者常规生产数据到非生产环境中时，存在被窃取或者泄露的风险，并造成难以挽回的损失。由于缺乏有效的脱敏机制，大量数据不能通过分享来产生价值，对社会造成巨大损失。

政策标准、法律法规要求

《个人信息保护法》

第五章 个人信息处理都义务

第五十一条第三款中提到：采取相应的加密、去标识化等安全技术措施。

《中华人民共和国网络安全法》

第四章42条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

《信息安全技术 个人信息安全规范》

收集个人信息后，个人信息控制者宜立即进行去标识化处理，并采取技术和管理方面的措施，将去标识化后的数据与可用于恢复识别个人的信息分开存储，并确保在后续的个人信处理中不重新识别个人。

《中国银行业信息科技“十二五”发展规划监督指导意见》

加强数据、文档的安全管理，逐步建立数据资产分类分级保护机制，完善敏感信息存储与传输等高风险环节的控制措施，对数据、文档的访问应建立严格的审批机制，对用于测试的生产数据要进行脱敏处理，严格防止敏感信息泄露...

《商业银行信息科技风险现场检查指南》

测试中如需使用生产数据，应对相应数据进行脱敏、变形处理，当使用生产数据测试时是否得到高级管理层的审批并采取相关限制进行脱敏处理...

产品简介

昂楷静态数据脱敏是昂楷经过多年数据库安全产业研发经验积累，结合客户各种应用场景需求，开发的基于对敏感数据进行覆盖、替换、变形等操作的数据库安全产品，可为用户提供高效、稳定、安全、全方位的敏感数据保护解决方案。

典型场景

01 开发测试数据共享时使用敏感数据

业务数据，核心数据脱敏后再给开发、测试使用，防止数据泄露，保证重要数据在开发、测试使用过程中的安全。

02 数据分析时使用敏感数据

数据经过脱敏系统脱敏后，再进行数据分析，保障核心数据、业务数据的安全前提下，有效完成数据分析的工作。

03 替代手工脱敏

对于需要经常对重要文件数据、导出数据进行零散的手工脱敏，进行数据外发和共享时，静态脱敏系统可以替代手工脱敏，高效完成用户脱敏需求。

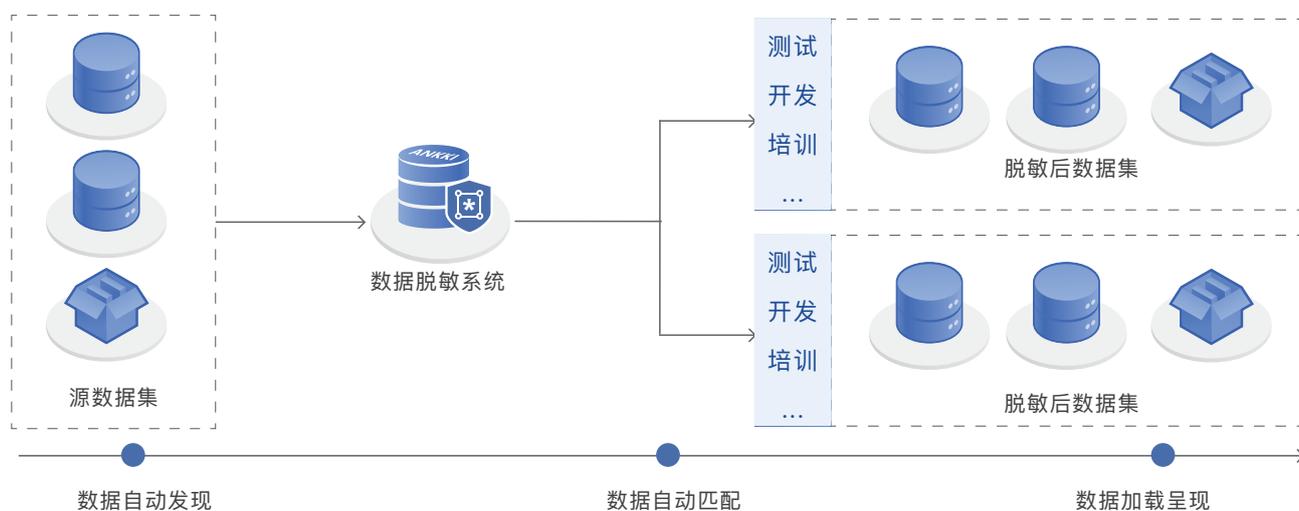
04 数据传输时防止敏感数据泄露

数据在网络传输过程中，容易受到攻击，在离线传输过程中使用脱敏后的数据，解决了敏感数据传输过程中，敏感数据泄露的难题。

05 实时业务数据迁移

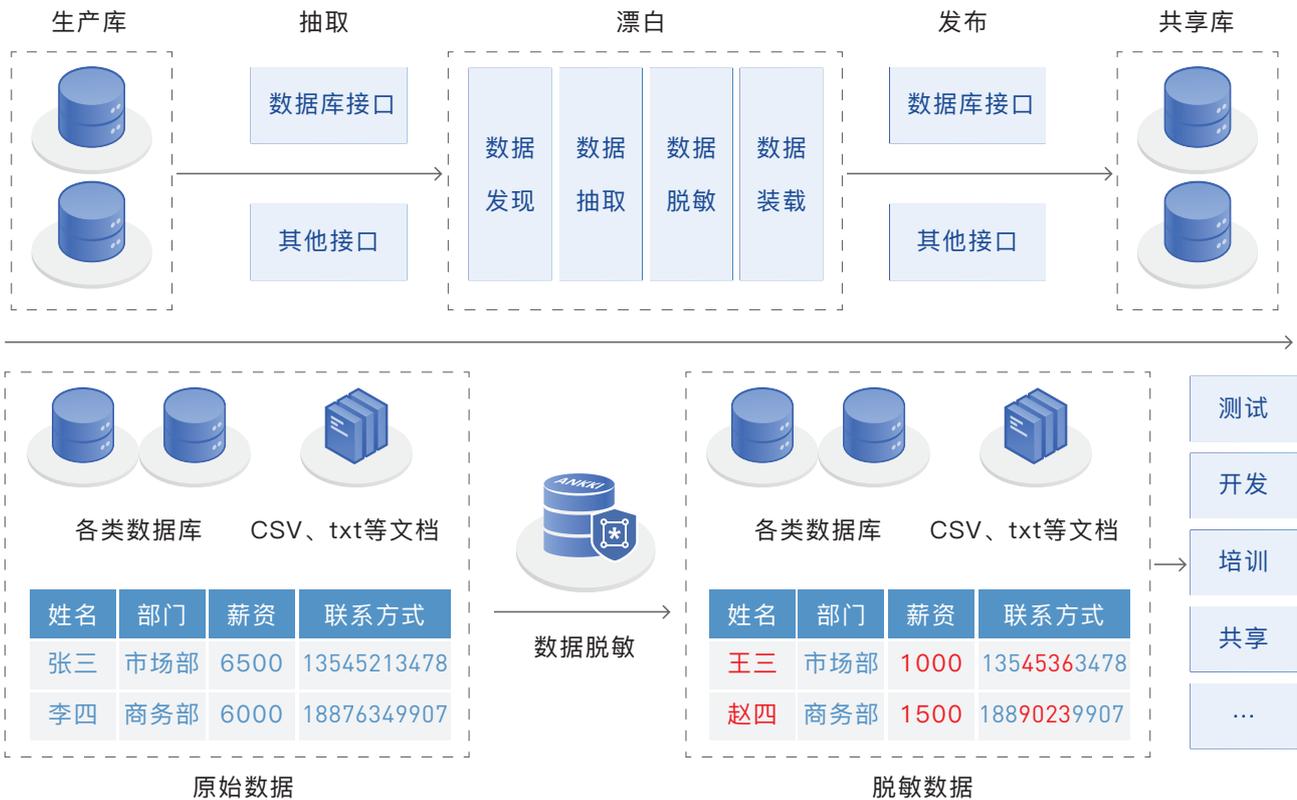
对于需要业务数据在实时迁移过程中的需求场景，提供增量脱敏的功能，一旦源数据库中数据增量变化，做到准实时同步。

部署方式



采用硬件部署方式，独立部署，连接到数据源。

实现原理示意图



产品特性

01 广泛支持多种类型的数据库脱敏

- 支持关系型数据库，如：Oracle、SQL Server、MySQL、DB2、PostgreSQL、sybase、informix、Vertica关系型数据库；
- 支持大数据库，如：Hadoop、Hive、MongoDB、hbase等；
- 支持国产化数据库，如：DM、GaussDB、OceanBase等；

02 敏感数据自动识别

可通过预定义敏感数据特征库，在任务执行过程中通过智能匹配识别敏感数据，最大限度的实现脱敏工作自动化，简化以手工方式按字段名定义敏感数据的繁琐工作。

03 支持丰富的脱敏算法

内置同义替换、数据遮蔽、随机替换、偏移、随机化、可逆脱敏等多种脱敏规则，可根据实际的应用场景灵活使用。

04 支持数据库和文件异构脱敏

- Oracle、MySQL、MS SQL Server、MongoDB、Teradata等。
 - 支持TXT、EXCEL、CSV等数据格式文件脱敏，支持库到库、库到文件、文件到库、文件到文件的脱敏。
 - 静态数据脱敏支持同库（脱敏源和脱敏目标是相同数据库）和异库（脱敏源和脱敏目标是不同数据库）脱敏。
-

05 黑白名单脱敏

内置黑白名单管理，指定表中一些信息的显示与否，较敏感的数据，例如公安部红名单等信息可选择黑名单配置；特意选择查看的数据或其他可选择白名单配置。

06 支持水印溯源功能

支持水印嵌入，并提供水印溯源的能力。支持智能筛选可嵌入水印字段。并根据可嵌入水印字段类型的差异，分别选择对应的水印嵌入算法。采用独创的水印嵌入算法，在业务系统性能、水印的健壮性、鲁棒性之间取得平衡。

07 高可用性

在复杂环境中，昂楷静态数据脱敏系统支持断点续脱功能，确保这种场景下能从上次脱敏意外终止的地方继续进行，节省系统资源和人力成本。

08 支持增量脱敏功能

提供工具化的手段完成脱敏，一旦源数据库中数据增量变化，脱敏系统可以提供增量脱敏的功能，做到“准”实时同步。增量脱敏的周期可以达到分钟级。

产品优势

01 分布式扩展

采用自主研发的代理架构，在单台设备容量或者性能达到瓶颈时，可以通过级联多台设备搭建分布式集群环境，满足大规模数据场景下的需求。

02 智能自动发现

内置针对不同行业的预定义敏感数据特征库，能够自动发现如姓名、身份证号、电话号码、银行账户、日期、地址、税号、金额等敏感信息，减轻用户面对海量数据库手动挑选敏感数据的工作量。

03 高效数据梳理

可自动发现敏感数据，对数据关联关系进行智能分析，将敏感数据关系图谱清晰的呈现给用户。

04 脱敏方式的多样性

适应性，内置 五种以上的脱敏 式， 持 定义，配置简单，灵活度 ，满 不同场景的需求。

05 广泛的数据脱敏能力

满 传统关系型数据库的同时， 持HBase、Hive、Teradata、mongodb等 数据库NoSQL环境脱敏， 持阿 云 数据库环境， 持数据增量式脱敏，满 多样化 需求。

昂楷部分资质与荣誉

Time To Platform Will Be Reached: 0 = 2 yrs, 1 = 3-5 yrs, 2 = 5-10 yrs

Data Security Platforms

- Identify data security capabilities that are not fit for purpose in your environment, and retire them after selecting corresponding capabilities from a leading DSP vendor. Good candidates for replacement are:
 - Data security controls that scale box by box, not feature by feature.
 - Products that need customized middleware maintained using professional services.

Sample Vendors
 ANKKI, IBM, Imperva, PKWARE, Prolegity, SecuPI

Analysis By
 Joerg Fritsch, Brian Lowans

Gartner Recommended Reading

昂楷数据安全综合治理平台入选Gartner《2021数据安全技术成熟度曲线》DSP中的国内唯一标杆性厂商

哈尔滨工业大学(深圳) - 昂楷数据安全治理联合实验室

哈工大(深圳) - 昂楷数据安全联合实验室

涉密信息系统产品检测证书

2018年贵阳大数据攻防演练“安全防卫奖”

ISO/IEC 27001信息安全管理体系认证证书

ISO9001质量管理体系认证证书

ISCCC中国国家信息安全产品认证证书

IPv6 Ready Logo 认证证书

2017贵阳大数据及网络安全攻防演练活动安全防卫奖

高新技术企业证书



地址：深圳市前海深港合作区南山街道桂湾五路123号前海大厦T2栋6楼
电话：400-622-8990
网址：www.ankki.com
E-mail：support@ankki.com

关于本出版物

本刊物仅供参考，不构成任何承诺或保证。本刊物中的商标、图片、标识均归深圳昂楷科技有限公司或拥有合法权利的第三方所有。
版权所有 © 深圳昂楷科技有限公司2021 保留一切权利

版本号：ANKKI-[AAS-SIMP]-20211220-V2.0



官方微信