

安永数据库加密系统

产品白皮书

目 录

一、引言	3
1.1 背景	3
1.2 目的	4
1.3 面向读者	4
二、挑战与机遇	5
2.1 挑战	5
2.2 机遇	6
三、产品介绍	6
3.1 产品概述	7
3.2 产品特点	7
3.3 产品属性	8
3.4 产品体系架构	10
四、产品功能	12
4.1 数据加密与解密	12
4.2 数据搜索与检索	12
4.3 访问控制与权限管理	12
4.4 监控与审计	13
4.5 异常检测与预警	13
4.6 数据备份与恢复	13
4.7 数据完整性保护	13
4.8 灵活的集成和扩展	14
五、产品应用	14
5.1 金融行业	14
5.2 医疗保健领域	14
5.3 政府和公共部门	15
5.4 零售与电子商务	15
5.5 教育机构	15
5.5 企业与组织	15

一、引言

1.1 背景

随着数据规模和流通需求不断增加，数字经济时代将数据视为最主要的生产要素之一。数据的安全性和保护变得尤为重要。在各类系统中，数据库系统扮演着存储和管理信息的关键角色，集中存放着大量敏感数据，并为众多用户直接共享。然而，数据库中的数据通常以明文形式存储，这使得数据容易遭受泄露或遭到破坏的风险。一旦发生数据泄露，不仅会导致企业的业务受损，也会给企业和整个社会带来巨大的损失，甚至危及国家安全。

面对这一现实，必须采取适当的措施来保护数据库中的数据免受未经授权的访问和泄露的威胁。传统的明文存储方式已经不再足够安全，因此需要引入高级的数据保护措施。加密是一种有效的方法，它通过将数据转化为加密形式，使得只有授权的用户才能解密和访问数据，从而提供了更高的安全性。

针对数据库内数据的防护，安永数据库加密系统应运而生。它是一款基于信创安全技术、可搜索加密、硬件可信执行环境和透明加密技术的产品，旨在为敏感数据提供强大的加密存储解决方案。通过使用国产加密算法 SM4，支持细粒度的加密配置，并结合可搜索加密技术，实现加密数据的高效索引和检索功能。此外，产品还采用独立密钥管理方案，支持多种密钥生成方式，并且适配了信创环境，可以在各类国产化环境中高效运行。

安永数据库加密系统的引入将为企业和组织提供一种可靠的数据保护解决方案，确保敏感数据的机密性和完整性，防止数据泄露和未经授权的访问。它不仅满足了企业对数据安全的高要求，还有助于维护国家的信息安全和保护数字经济的可持续发展。

1.2 目的

安永数据库加密系统旨在为组织和个人提供一种强大的数据库防泄漏解决方案，通过综合运用信创安全技术、可搜索加密、硬件可信执行环境和透明加密等先进技术，实现对敏感数据的加密存储和安全访问。本白皮书的目的是介绍安永数据库加密系统的关键特点、功能和应用领域，帮助读者深入了解该系统的价值和优势，并为其在实际应用中提供指导和参考。

1.3 面向读者

本白皮书主要面向以下读者群体：

- 组织和企业的决策者、管理者和技术人员，关注数据安全和隐私保护的专业人士；
- 数据管理和安全团队，负责制定和执行数据保护策略的专业人员；
- IT 从业人员和开发人员，有兴趣了解和集成安全数据库解决方案的技术人员；
- 学术界和研究机构的研究人员，对数据安全和隐私保护领

域感兴趣的专家和学者。

在接下来的章节中，我们将详细阐述安永数据库加密系统的产品特点、体系架构、功能和应用领域。通过介绍系统的关键功能和优势，我们希望读者能够全面了解安永数据库加密系统的潜力，并在实际应用中获得最大的价值和效益。

二、挑战与机遇

数据安全和隐私保护领域面临着一系列的挑战，同时也带来了巨大的机遇。

2.1 挑战

数据泄露风险：随着数据规模和复杂性的增加，组织面临越来越多的数据泄露风险。黑客攻击、内部人员不当行为和外部恶意活动都可能导致敏感数据的泄露。

数据隐私保护：法规和合规要求对数据隐私保护提出了更高的要求。组织需要确保在数据处理过程中遵守隐私规定，同时仍能够有效利用数据进行业务分析和决策。

高效的数据访问：在保护数据安全的同时，组织需要确保合法用户能够高效访问和检索所需的数据，以支持业务需求和决策。

技术复杂性：实现数据加密、访问控制和监控等功能需要综合应用多种技术，包括信创安全技术、可搜索加密和硬件可信执行环境等。这些技术的复杂性和集成难度增加了系统的开发和部署成本。

2.2 机遇

数据安全意识提高：随着数据泄露事件的频发，组织对数据安全的重视程度不断提高。数据安全解决方案的需求持续增长，为安永数据库加密系统提供了广阔的市场机会。

法规和合规要求：随着数据保护法规的不断出台和加强，组织对数据隐私保护的合规性要求也越来越高。安永数据库加密系统提供了满足法规和合规要求的解决方案，为组织提供了遵守相关法规的机会，提升业务合规性、稳定性和持续性。

数据驱动业务：数据分析和智能决策对组织的竞争力至关重要。通过安永数据库加密系统的高效数据访问和安全保护，组织能够在数据驱动的业务环境中实现更好的业务结果和创新。

技术进步：随着技术的不断进步和创新，安永数据库加密系统能够充分利用信创安全技术、可搜索加密和硬件可信执行环境等先进技术，提供更强大、更可靠的数据安全和隐私保护能力。

在面对这些挑战和机遇时，安永数据库加密系统将不断努力创新和完善，提供高效、安全的数据保护解决方案，为组织应对数据安全和隐私保护的挑战并抓住机遇提供支持。

三、产品介绍

安永数据库加密系统是一款基于可信执行环境、可搜索加密、信创安全等先进技术的数据库防泄漏产品。该系统旨在帮助组织和个人

保护敏感数据的安全和隐私，满足数据保护法规和合规要求。

3.1 产品概述

安永数据库加密系统提供了强大的数据保护功能，包括数据加密、搜索与检索、访问控制与权限管理、监控与审计、异常检测与预警以及数据备份与恢复等。通过综合运用先进的加密算法和安全技术，该系统能够在保护数据安全的同时实现高效的数据访问和管理。

3.2 产品特点

1、基于 TEE 技术

密钥管理及使用限定 TEE（硬件可信执行环境）内部，确保密钥在 TEE 环境中安全存储和处理，有效防止密钥被恶意获取。

密钥在内存中不以明文形式存在，提供额外的保护层，防止针对内存数据的攻击。

利用 TEE 技术的可信执行环境，确保加密操作的完整性和安全性。

2、高效加密索引

采用独有且经过工程化验证的可搜索加密技术，保证加密后的数据仍具备高效索引和检索能力。

解决行业痛点，允许用户在加密数据中进行快速查询和搜索操作，提高工作效率。

广泛适用于需要对敏感数据进行保护的行业，如金融、医疗保健和政府部门等。

3、独立密钥管理

支持多种密钥生成方式，包括软件、密码机、加密卡等，用户可根据需求选择合适的密钥生成方式。

密钥独立生成和独立管理，确保密钥的安全性和可控性。

提供灵活的密钥轮换和更新机制，帮助用户实现密钥的定期更新和管理。

4、适配信创环境

兼容各类国产化环境，如龙芯、飞腾、海光、兆芯、鲲鹏等，可在各类国产化软硬件环境实现高效稳定的运行。

充分利用国产处理器的优势，提供性能和安全性的双重保障。

与国产操作系统和硬件平台无缝集成，为用户提供完善的信创环境支持。

以上特点将有助于安永数据库加密系统在保护敏感数据存储和防止泄漏方面提供更全面、可靠的解决方案，满足用户对数据安全的高要求。

通过使用安永数据库加密系统，组织和个人可以有效保护敏感数据的安全和隐私，遵守相关法规和合规要求，降低数据泄露和隐私泄露的风险，提升数据安全和业务信任度。

3.3 产品属性

安永数据库加密系统具备以下核心属性，为用户提供强大的数据保护和隐私保护能力：

高级加密算法：系统采用国产加密算法 SM4，提供高强度的数据加密和解密功能，确保数据在存储和传输过程中的机密性和完整性。

可搜索加密技术：系统应用自主研发的高效可搜索加密技术，允许用户在加密的数据集中进行高效的搜索和检索操作，而无需暴露敏感数据的明文。

硬件可信执行环境（TEE）：系统在关键环节采用硬件可信执行环境，提供安全可靠的数据处理和存储环境，保护关键数据免受物理和逻辑攻击。

细粒度的加密配置：系统支持列级别、表级别和库级别的加密配置，用户可以根据实际需求对不同细粒度的数据进行灵活的加密设置，实现最佳的数据保护策略。

完备的访问控制与权限管理：系统提供灵活的访问控制机制，支持用户级别、角色级别和数据细粒度的权限管理，确保只有授权用户可以访问敏感数据。

实时监控与审计：系统具备实时监控和审计功能，记录数据访问和操作日志，支持对数据使用情况进行审计和追踪，帮助组织及时发现异常操作和安全事件。

异常检测与预警：系统通过先进的异常检测算法，能够实时监测数据访问行为，检测异常操作和潜在的安全威胁，并及时发出警报和预警通知，提高安全响应能力。

数据备份与恢复：系统支持数据备份和恢复功能，定期备份数据以应对意外损坏或灾难性事件，确保数据的可靠性和业务的连续性。

灵活的集成和扩展：系统具备良好的灵活性和可扩展性，可以与现有的数据库系统和应用平台集成，为用户提供便捷的部署和使用体验。

通过这些强大的产品属性，安永数据库加密系统能够为用户提供全面的数据安全和隐私保护解决方案，确保敏感数据得到最高级别的保护，并满足不同行业和组织对数据保护的严格要求。

3.4 产品体系架构

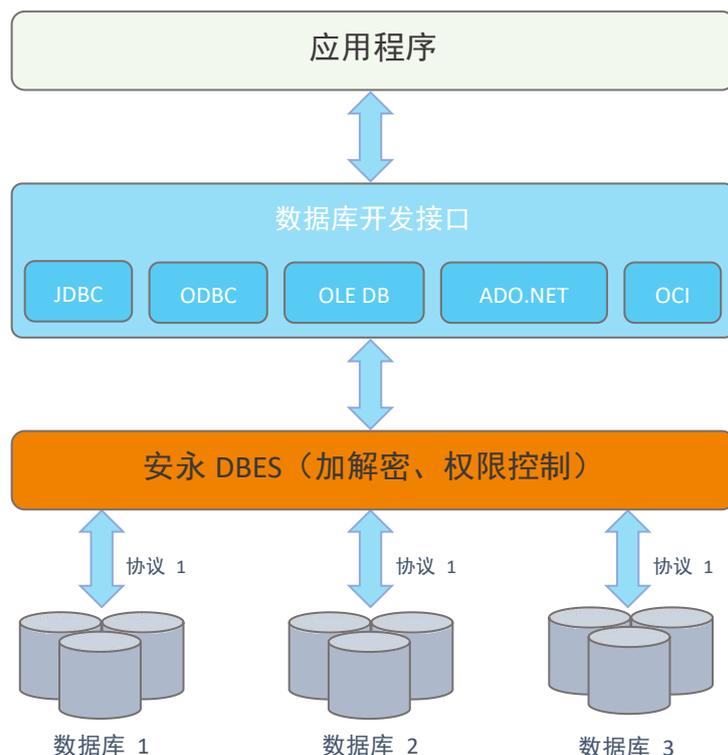
安永数据库加密系统采用先进的体系架构，以保障数据安全和隐私保护。产品的基本体系架构见下页图。

1、用户界面层

用户界面层是系统与用户进行交互的前端界面，提供用户登录、权限管理、配置设置等功能。用户可以通过用户界面层进行对系统的管理和操作。

2、应用服务层

应用服务层是系统的核心处理层，负责处理用户请求并执行相关的加密、解密、访问控制、搜索和审计等功能。该层包括以下组件：



(1) 加密引擎：负责数据的加密和解密操作，采用国产加密算法 SM4 保证数据的机密性和完整性。

(2) 访问控制模块：实现细粒度的权限管理和访问控制机制，根据用户身份和权限策略控制数据的访问权限。

(3) 可搜索加密模块：引入可搜索加密技术，实现在加密数据集中的高效搜索和检索功能，保护数据隐私。

(4) 监控与审计模块：监控用户操作和数据访问行为，记录日志并提供审计功能，帮助组织监测和追踪数据使用情况。

3、数据存储层

数据存储层负责安全存储加密后的数据，确保数据的机密性和持久性。该层采用可信执行环境（TEE）提供安全的数据存储环境，防止数据被非法访问和篡改。

4、外部集成接口层

外部集成接口层允许系统与外部数据库系统 and 应用平台进行集成，实现与现有系统的无缝对接。该层提供标准化的接口和协议，以便与其他系统进行数据交换和通信。

整体架构采用分层设计，通过各层之间的交互和协作，实现数据的安全加密、灵活访问和完整性保护。安永数据库加密系统的体系架构旨在提供高度可靠、高性能的数据安全和隐私保护解决方案，满足用户的各类数据保护需求。

四、产品功能

安永数据库加密系统提供一系列强大的功能，以保护敏感数据的安全和隐私。

4.1 数据加密与解密

提供国产加密算法 SM4，实现对敏感数据的高强度加密和解密操作。

支持数据的实时加密和解密，确保数据在存储和传输过程中的机密性和完整性。

4.2 数据搜索与检索

引入可搜索加密技术，允许用户在加密的数据集中进行高效的搜索和检索操作。

用户可以通过关键词或属性进行数据搜索，而无需暴露敏感数据的明文。

4.3 访问控制与权限管理

提供细粒度的访问控制机制，用户可以精确控制数据的访问权限。

支持用户级别、角色级别和数据细粒度的权限管理，确保只有授权用户可以访问敏感数据。

4.4 监控与审计

实时监测数据访问和操作行为，记录数据访问和操作日志。

提供审计功能，支持对数据使用情况进行审计和追踪，帮助组织发现异常操作和安全事件。

4.5 异常检测与预警

使用先进的异常检测算法，实时监测数据访问行为。

检测异常操作和潜在的安全威胁，并及时发出警报和预警通知，提高安全响应能力。

4.6 数据备份与恢复

支持数据备份和恢复功能，定期备份数据以防止意外数据损坏或灾难性事件。

确保数据的可靠性和业务的连续性，快速恢复数据以保持业务正常运行。

4.7 数据完整性保护

采用加密和完整性验证机制，防止数据被篡改或损坏。

确保数据在存储和传输过程中的完整性，防止数据被非法篡改或冒充。

4.8 灵活的集成和扩展

提供与现有数据库系统和应用平台的集成能力，方便用户的部署和使用。

支持标准化的接口和协议，与其他系统进行数据交换和通信。

通过这些功能，安永数据库加密系统能够有效保护敏感数据的安全和隐私，满足组织和个人对数据保护的高要求，并帮助应对各类数据安全挑战。

五、产品应用

安永数据库加密系统可广泛应用于各个行业和组织，以满足数据安全和隐私保护的需求。以下是产品的主要应用场景：

5.1 金融行业

银行和金融机构可以利用安永数据库加密系统保护客户敏感信息，如账户信息、交易记录等，确保数据的机密性和完整性。

适用于遵守金融合规要求和数据安全标准的需求，如 PCI DSS、GDPR 等。

5.2 医疗保健领域

医疗机构和保健服务提供商可以使用该系统加密和保护患者的个人健康信息（PHI），遵守健康保险可移植性和责任法案（HIPAA）的要求。

支持医疗研究和数据共享，确保敏感数据在共享过程中的安全性和隐私保护。

5.3 政府和公共部门

各级政府部门和公共机构可以利用安永数据库加密系统保护公民个人信息和重要机密数据，如社会保障号码、纳税信息等。

支持合规性和监管要求，确保数据的保密性和安全性，维护公众信任。

5.4 零售与电子商务

零售和电子商务企业可以使用该系统保护客户的个人信息、交易数据和支付信息，防止数据泄露和欺诈行为。

提供安全的数据存储和传输，确保客户数据的保密性和完整性，增强消费者对电子商务平台的信任。

5.5 教育机构

学校、大学和其他教育机构可以利用该系统保护学生和教职员工的个人信息和学术数据，遵守教育行业的隐私保护法规。

支持教育数据分析和研究，确保数据的安全和隐私。

5.5 企业与组织

各类企业和组织可以使用安永数据库加密系统保护商业机密、客户数据、员工信息等重要数据资产。

支持合规要求和数据安全标准，如 ISO 27001 等，满足企业数据安全和隐私保护的需求。

安永数据库加密系统的应用广泛而灵活，能够适应各组织和行业的不同需求，为用户提供可靠的数据安全和隐私保护解决方案。无论是保护个人隐私，满足合规要求，还是提升数据安全性，该系统都能为用户提供卓越的保护能力。