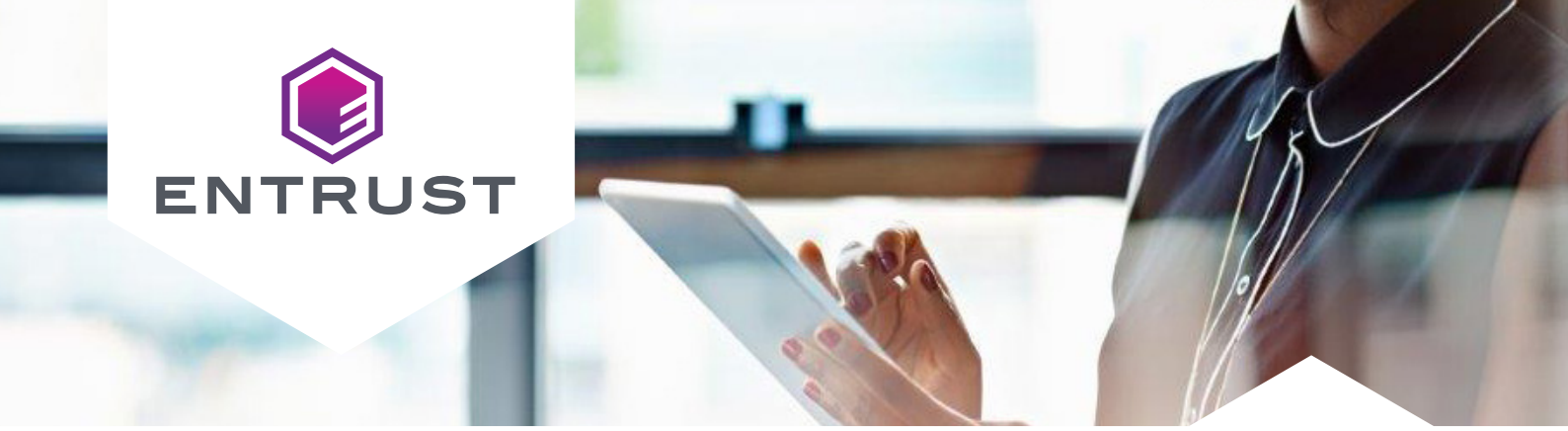

nShield Database Security Option Pack

Microsoft SQL 服务器数据库与高度安全的 nShield 硬件安全模块无缝集成

精彩亮点

深受 Microsoft SQL 服务器数据库部署信任

- 通过经 FIPS 和 Common Criteria 认证的最佳实践硬件安全模块 (HSM) 保护数据库加密密钥
- 保护单元级别加密和透明数据加密 (TDE)
- 防止组织关键数据泄露

在大多数组织中，数据库是敏感信息的重要存储库。企业数据库包含客户的信用卡数据、保密竞争信息和知识产权。数据丢失或被盗会让组织陷入声誉危机，损害品牌形象，同时面临巨额罚款。通过保护关键数据免受内外部威胁的侵害，组织可以减轻数据泄露的风险，遵守支付卡行业数据安全标准 (PCI DSS) 等法规和立法要求。实际上，最新 PCI DSS 标准 (v3.2.1) 第 3.6 节规定："加密密钥必须安全地存储在硬件安全模块等安全加密设备中。" 此外，第 3.6 节还概述了根据硬件安全模块功能 (例如双重控制) 实现密钥管理的良好实践。

利用最高级别的保障，守护数据库安全

加密数据库中的数据可以保护数据，同时解锁数据的加密密钥也必须受到保护。使用硬件安全模块 (HSM) 可将密钥与数据分开存储，另行存储在安全且可信任的平台上，以此保护加密密钥。nShield 硬件安全模块实施的内部安全策略要求基于角色的授权以及将安全和数据库管理分开，从而更容易向审计人证明合规性。

可充当单个服务器的专用 PCIe 卡或虚拟化环境的共享网络设备。

nShield Database Security Option Pack (适用于 Microsoft SQL Server) 又称为 SQLEKM 提供商，是专为 Microsoft SQL Server 提供的可扩展密钥管理 (EKM) API。

nShield Database Security Option Pack

Microsoft SQL Server 附带了两个内置的加密功能，可保护您的数据：TDE 和单元级加密。借助这些功能，您可以保护整个数据库或仅保护敏感数据库字段，并且可在不中断当前应用程序、数据库结构和流程的情况下激活。

保护您的品牌和数据

Entrust nShield 硬件安全模块已通过 FIPS 和 Common Criteria 等最高安全标准的验证，即使在最具挑战性和最苛刻的安全情况下，也可以随时保护您的数据。nShield 硬件安全模块的精细访问权限控制可供您管理 Microsoft SQL Server 的加密密钥。如需强制实施策略，必须将安全功能与管理功能区分开来。

Entrust nShield 硬件安全模块带来以下功能：

- **硬件密钥保护** – 将数据库加密密钥存储在安全的防篡改环境中，防止密钥被复制或破坏
- **强制实施用户和角色管理** – 强劲控制 Microsoft SQL Server 中加密数据的访问权限
- **严格的密钥控制** – 使用管理员的智能卡身份验证，实现对数据库加密密钥的强大控制
- **角色分割** – 将重要任务和流程的责任拆分开来，分配给多个管理员
- **轻松设置和集成** – Entrust nShield 硬件安全模块可与 Microsoft SQL Server 无缝集成，实现以下功能：
  - TDE 和单元级别的加密模式，带有适用的加密密钥保护

nShield 硬件安全模块可进行扩展，以满足您不断变化的需求，可与其他领先的企业应用程序（包括 Web 和应用程序服务器以及公钥基础结构 (PKI)）直接集成。

基于网络的 nShield Connect 硬件安全模块可以在多个服务器之间共享，这些服务器提供：

- **虚拟化环境支持** – 基于硬件的密钥存储供 Hyper-V 和 VMware 等虚拟服务器使用
- **故障转移集群支持**包括 AlwaysOn 可用性组
- **简化管理** – 管理多个数据库的加密密钥以及其他应用程序使用的密钥
- **故障转移功能** – 在具有高可用性的重要环境内，用户可以选择在某个硬件安全模块不可用时，自动切换到另一个硬件安全模块
- **灾难恢复** – 简单、安全的密钥存档和恢复流程
- **经济高效的资源** – 跨多个服务器共享模块，降低硬件、许可证和运维成本

nShield Database Security Option Pack

技术规格

支持的配置

- 需要 nShield Security World Software v12.40.2 或 v12.60.x 或更高版本。
- Microsoft SQL Server 版本（企业版）2019 x64、2017 x64
- Windows Server 操作系统支持 2019 R2 x64、2016 R2 x64
- 支持的硬件安全模块
  - 与所有 nShield Solo 和 nShield Connect 硬件安全模块型号兼容

支持的加密算法

- 非对称 - 包括 RSA 2048、3072 和 4096 位密钥长度
- 对称 - 包括 AES 128、192 和 256 位密钥长度

支持的 NSHIELD 功能

将 nShield 硬件安全模块与 Microsoft SQL 服务器集成后，即可使用以下功能：

功能	支持
N 个卡集之 1	是
N 个卡集之 K	否
软卡	是
仅模块密钥	否
密钥恢复	是
密钥导入	部分[1]
负载均衡	是
故障转移	是
强劲的 FIPS（FIPS 140-2 3 级）支持	是[2]

1. 密钥导入功能仅支持导入 nCore 密钥。nCore API 是 nShield 模块
2 的原生应用程序编程接口。查看发布说明和用户指南，了解详细信息。

进一步了解

如需进一步了解 Entrust nShield 硬件安全模块，请访问 **entrust.com/HSM**。如需进一步了解 Entrust 的身份、访问权限、通信和数据数字安全解决方案，请访问 **entrust.com**

如需进一步了解 Entrust nShield 硬件安全模块

HSMinfo@entrust.com
entrust.com/HSM

关于 ENTRUST CORPORATION

Entrust 支持受信任的身份、付款和数据保护，为世界的安全运转保驾护航。如今，无论是处理跨境业务、购买商品、访问电子政府服务还是登录公司网络，人们都比以往更加需要顺畅安全的体验。Entrust 提供了无与伦比的数字安全和凭证颁发解决方案，直接打通这些交互的核心。Entrust 在 150 多个国家/地区拥有 2,500 多位同事以及巨大的全球合作伙伴和客户网络，因而深受全球大多数托管组织的信任。

如需进一步了解，请访问：
entrust.com/HSM

ENTRUST

联系我们：
HSMinfo@entrust.com