

**技术简介**

**保护您的驱动器，保护您的数据**

数据帮助我们创新并创造未来的一切。为了帮助保证您的数据安全，西部数据采用了全面的安全方法，涵盖存储设备生命周期的所有阶段：开发、制造、部署和使用。

本文介绍了西部数据针对数据中心和企业级 HDD 和 SSD 以及智能视频和 NAS HDD 的安全方法。通过将安全性集成到固件、硬件和制造过程中，这些驱动器受到保护。我们通过使用加密和访问控制帮助客户保护他们的数据。

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | |
|  | |  | |
| 保护您的驱动器 | | 保护您的数据 | |
|  | **安全制造** |  | **加密** |
|  | **安全启动** |  | **访问控制** |
| **C:\Users\QT\Desktop\1-1.png** | **安全下载** |  | **数据清理** |
| **C:\Users\QT\Desktop\1-2.png** | **安全诊断** |  |  |

**安全目标**

西部数据的安全方法旨在实现以下目标：

●帮助确保驱动器在制造过程中免受外界干扰

●帮助确保驱动器免受第三方攻击的入侵，从而避免损坏或更改驱动器功能

●帮助确保用户在驱动器丢失、第三方物理访问或驱动器停止服务的情况下拥有保护其数据的工具

|  |  |  |  |
| --- | --- | --- | --- |
| 西部数据的安全架构基于安全区域，以确保驱动器从诞生到毁灭都受到保护，免受不必要的入侵。安全区域是一个专用的安全子系统，可在安全功能和其余产品功能之间提供硬件级隔离。  安全区域提供多种加密算法加速器。不可变代码执行初始化、开机自检并建立信任根。安全区域确保设备安全生命周期管理、调试端口管理、非对称和对称根密钥管理，以将密钥树唯一地绑定到设备。所有明文密钥访问仅限于安全区域。 |  | |  | | --- | | **西部数据的安全功能包括**  **硬件：**每个驱动器上都有专用的安全硬件  **固件：**专用安全固件实现  **流程：**安全的制造和诊断过程  **加密：**支持行业标准加密协议  **访问控制：**行业标准协议可防止未经授权访问设备 | |



**保护您的驱动器**

西部数据安全涵盖整个驱动器设计和制造的多个步骤。安全保障措施涵盖客户运输和部署。除了对我们的安全实施进行内部验证之外，西部数据还邀请第三方对各种存储设备的完整性和静态数据保护声明进行审核。这些第三方审计有助于确认我们的架构反映了良好的开发实践，并具有强有力的支持文档和实施。

|  |  |
| --- | --- |
|  | **安全制造：**这些西部数据硬盘是在值得信赖的工厂生产的，具有各种安全的制造特性和保护措施。安全制造驱动器的命令由内部证书颁发机构 (CA) 服务器进行验证，并利用安全质量将这些命令限制为特定的驱动器序列号和一次性使用。此功能仅在 Western Digital 工厂内可用。 |
|  |  |
|  | **安全启动：**安全启动功能可确保驱动器在每次启动时验证固件是否来自经过身份验证的来源，然后再使用。驱动器在启动过程中实现了多阶段加载系统。每个加载器阶段负责在将控制权转移到下一个图像之前加载和验证下一个图像。这在启动过程中建立了信任链。安全区域用于建立信任根并启用信任链。 |
|  |  |
|  | **安全下载：**安全下载功能可确保驱动器仅接受 Western Digital 签名的固件。使用数字签名算法来验证固件签名。为了保证加密分离，不同的客户和安全模型使用唯一的密钥。此外，还提供安全回滚预防和密钥撤销功能。 |
|  |  |
|  | **安全诊断：**当这些驱动器从我们的工厂发货时，所有物理和逻辑调试端口都被禁用。启用驱动器上的任何调试功能的命令均由 CA 服务器进行验证，并利用特性将这些命令限制为特定的驱动器标识（序列号）和一次性使用。有记录显示，现场故障分析能力利用了相同的身份验证机制。 |

**保护您的数据**

为了确保用户数据的机密性和完整性，有三个关键要素协同工作。这些功能可防止未经授权的方访问用户数据，无论是读取（机密性）还是写入（完整性）。

|  |  |
| --- | --- |
|  | **加密：**西部数据提供带有和不带有用户数据硬件加密功能的驱动器。启用加密的驱动器使用 AES-XTS-256 加密静态用户数据。 |
|  |  |
|  | **访问控制：**西部数据硬盘提供加密和非加密两种型号，均采用行业标准的访问控制方法。 |
|  |  |
|  | **数据清理：**所有接口（SATA、SAS、NVMe™）的驱动器均提供清理功能，如果使用得当，这些功能与 IEEE 标准 2883™-2022 文档“存储清理标准”中描述的“清除”功能一致。 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 驱动器类型 | 静态加密数据 | 数据访问控制 | 首选清除-擦除 | 认证 |
| 东南 | 不 | ATA 安全  （仅限 SATA） | 清理覆盖 (HDD)  清理块擦除 (SSD) | 不适用 |
| ISE | 是 | ATA 安全  （仅限 SATA） | 加密擦除 | 不适用 |
| TCG | 是 | TCG-SSC | 加密擦除  恢复 | 不 |
| TCG-FIPS | 是 | TCG-SSC | 加密擦除  恢复 | NIST 认可实验室的 FIPS 140-2 验证  （FIPS 140-3 正在进行中） |

**摘要**

|  |  |  |  |
| --- | --- | --- | --- |
| 在当今环境下保护数据需要多层保护。西部数据将安全性集成到固件、硬件和制造流程中，以帮助确保物理硬盘得到保护。  通过启用行业标准数据加密协议和数据访问控制，我们使客户能够保护其数据。西部数据对安全性的承诺以及帮助客户保护其创建内容是我们产品的核心。  **了解更多关于西部数据安全解决方案的信息**  www.westerndigital.com/solutions/data-security |  | |  | | --- | | **提供的安全类型：**  **安全擦除 (SE)：**SE 硬盘不提供用户数据加密。使用标准 ATA 安全功能集（SATA 硬盘）提供用户数据访问控制。硬盘清理通过使用标准 ATA 安全擦除、SCSI 清理或 NVMe 清理命令执行，并采用覆盖 (HDD) 或块擦除 (SSD) 方法。  **即时安全擦除 (ISE)：**ISE 硬盘的数据在静态时加密。使用标准 ATA 安全功能集（SATA 硬盘）提供访问控制。启用数据加密的优势体现在清理步骤中。硬盘可以使用 ATA、SCSI 或 NVMe 标准命令进行清理，但采用即时加密擦除，而不是要求硬盘被覆盖或进行块擦除过程。也支持覆盖/块擦除。  **可信计算组 (TCG)：**TCG 硬盘的数据在静态时加密。访问控制通过 TCG-SSC 协议处理：TCG Enterprise、TCG Opal 或 TCG Ruby，具体取决于型号。硬盘清理可以使用 Revert 命令即时完成。也支持加密擦除和覆盖/块擦除。  **TCG-FIPS：**TCG-FIPS 硬盘在功能上与 TCG 硬盘相同，但经过 NIST 认可实验室验证，符合美国联邦信息处理标准 [FIPS]。此外，硬盘采用防篡改功能，以确保硬盘在部署或使用过程中不会被物理修改。 | |



|  |  |
| --- | --- |
| 5601 Great Oaks Parkway  美国加利福尼亚州圣何塞 95119  www.westerndigital.com | © 2023 Western Digital Corporation 或其附属公司。保留所有权利。  Western Digital、Western Digital 设计、Western Digital 徽标是 Western Digital Corporation 或其附属公司在美国和/或其他国家的注册商标或商标。NVMe 字标是 NVM Express, Inc. 的商标。所有其他标志均为其各自所有者的财产。本出版物中提及的某些产品、功能或服务并不意味着它们将在所有国家/地区提供。 |