SiliconMotion

WHITE PAPER

先进的 FerriSSDs®

如何为网络安全提供全面的数据保护

日益增长的网络、基础架构和体系结构的复杂性大幅度增加了连接的数量和种类，并使其成为网络攻击的目标。

日益复杂的威胁和较差的威胁感知使我们很难掌握增长的信息安全控制、需求和威胁的数量。

安全显然是网络安全公司最为关心的问题之一，必须采取相应的预防措施，使硬件不受到黑客攻击或其它未经授权访问的影响，从而防止盗用或滥用。

慧荣科技 FerriSSD 驱动器结合了基于硬件的安全性，符合最新的行业标准并提供一些额外的保护措施。其中包括数字签名固件和篡改响应，范围从生成警报到删除磁盘上的所有内容。

慧荣科技的 FerriSSD 为网络安全提供了安全功能：
保护正常运行的数据

数据中心服务器、联网车辆、医疗设备、游戏系统和例如工厂控制器、监视系统和零售技术的工业计算只是现代生活和工作所需系统的一小部分。存储在系统内存中的数据可能会泄露用户、组织和客户的相关信息，若落他人之手，这些信息可能会产生危害。入侵并意图访问数据的人各有不同动机，如窃取账户和信用卡号码等财务信息、查找医疗记录等机密企业数据或个人信息、窃取知识产权、破坏设备及运行。

防止黑客入侵并保护有价值的数据是一个不断提升的挑战。网络威胁越来越复杂，并且难以预测。如今，无处不在并且“永远在线”的网络连接，以及联网汽车等新兴应用的移动特性，使得保存在硬盘驱动器 (HDD) 或固态磁盘 (SSD) 等大容量存储设备的系统和用户数据很容易受到攻击。

建置网络安全架构

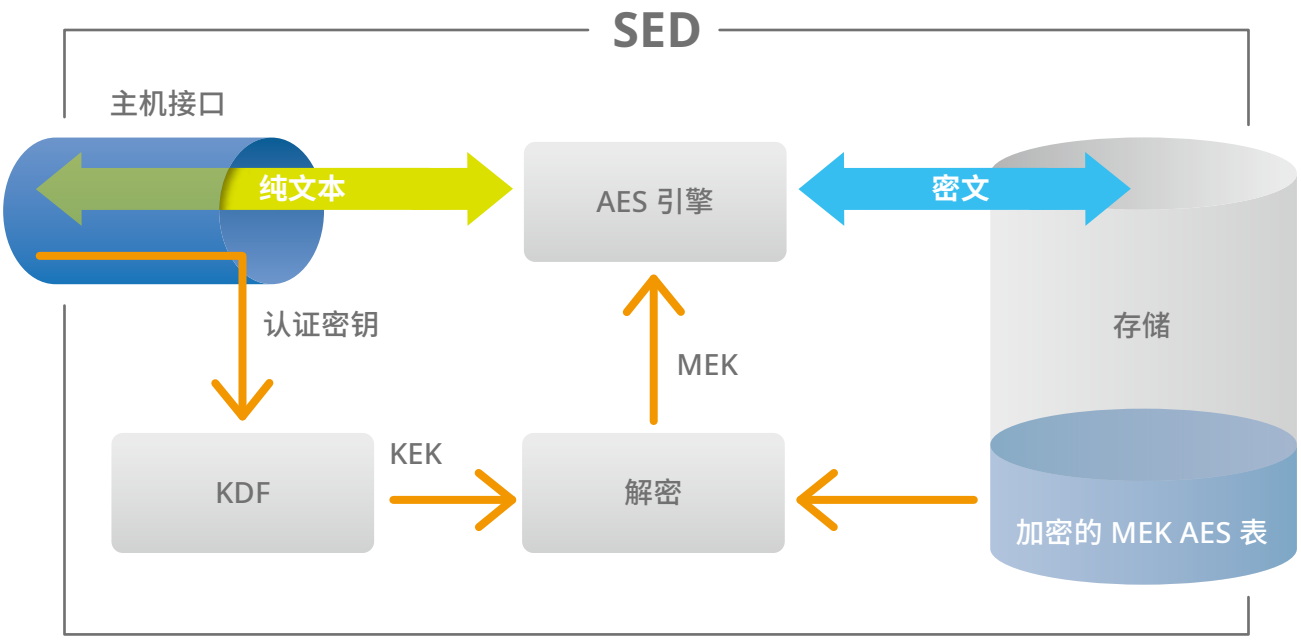
我们需要采取各种保护措施来防止未经授权的数据访问，从而防止盗用或滥用。为了确保这些措施能够实现目标并得到适当实施，行业和监管机构正在建立将网络安全置于新产品开发核心的框架。例如像是汽车行业标准 ISO/SAE 21434:2021 “道路车辆 — 网络安全工程”。这一标准与联合国欧洲经济委员会 (UNECE) 条例 UN 155 密切相关，要求产品开发人员建立一个经过认证的网络安全管理系统。

ISO/SAE 21434 的范围涵盖了产品从设计到使用年限结束的整个生命周期，包括了分析漏洞和落实安全措施的规定，以确保最全面的网络安全。此标准评估包括风险评估、识别和解决网络安全漏洞，以及测试软件和硬件组件的应用，从而降低风险。预计在 2024-2026 年间，车辆电子系统的合规将成为强制性规定。慧荣科技正在与 SGS 合作，以确保所有工艺都符合 ISO 21434 标准，并将在 2023 年第四季之前由第三方进行认证。

IntelligentGuard - 加密：第一道防线

SSD 正逐渐成为大量存储需求的选择。SSD 没有主动组件，带来了无噪音、抗震动、可靠性高、坚固耐用、低耗电等优点。同时，高性能和快速的系统回应，可缩短数据读写时间。用户通常会将存储在 SSD 上的数据进行加密以保护隐私，以防黑客窃取并对设备进行破坏或干扰 SSD。传统的全磁盘加密是由操作系统中的软件模块执行。数据以加密的形式在磁盘中进行检索，并通过 PCIe/SATA 接口传输，然后在计算机中解密。

可支持 AES 256 位硬件加密技术的自加密驱动器 (SED) 也是另外一种选择。自加密驱动器 (SED) 是一种将加密硬件内建于控制器的驱动器。SED 会自动加密写入所有数据，并对读取驱动器的数据解密。存储在 SED 的数据一律会使用媒体加密密钥 (MEK) 进行完整加密保护。MEK 也可以利用用户指定的验证密钥予以加密，借此锁定和解锁 SED。SED 控制也有专有的方法。



不同于传统由操作系统中软件模块执行的方法，SED 是即时加密或解密的，主系统 CPU 上没有处理负载。当从磁盘检索时，数据在 host 端解密，并通过 PCIe/SATA 接口不加密地传输到计算机。在移动和便携设备中，基于硬件加密的方法效率更高，有助于提高能源效率并延长电池寿命。

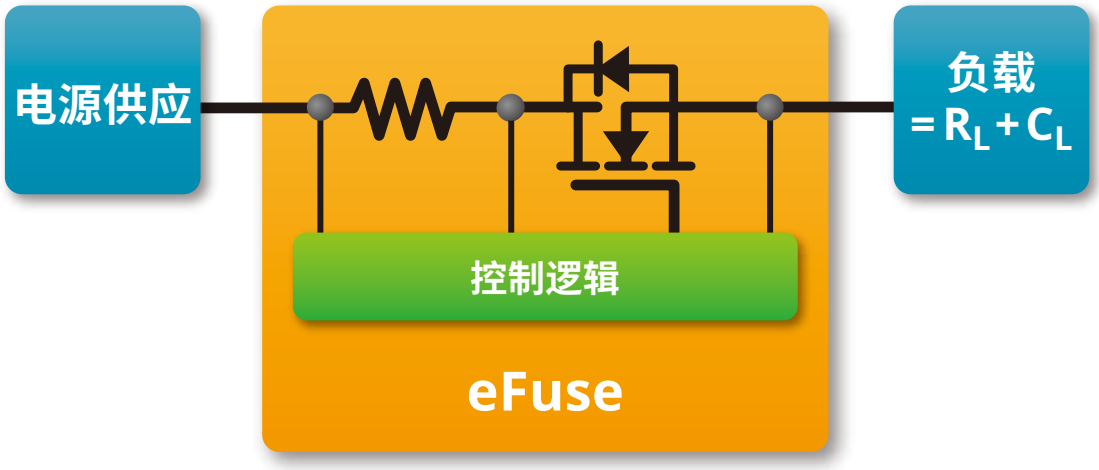
FerriSSD 固态硬盘符合 TCG Opal 2.0 并搭配 AES 256 位加密。遵循此标准有助于确保驱动器尽可能安全，防止未经授权的访问查看存储在磁盘上的数据。AES-256 位加密技术，符合行业标准的 256 位加密算法，也是业界广泛使用的加密演算法之一，是美国政府用于机密数据的加密标准，由于 AES 的密钥是随机产生的，即使制造商及用户也无法得知其密钥密码，其演算法极端复杂，至今仍未有任何破解。

然而，仅靠加密技术无法对所有可能的攻击提供全面保护。FerriSSD 还搭配附加数据保护机制，来防范这些不可预期的攻击风险。针对数据保护与增加存储设备可靠度层面，FerriSSD 具有多项独特技术，包含如下。

安全数字签名验证机制

其它常见的攻击包括通过加载恶意软件来控制 SSD。这可能迫使磁盘解密存储的内容，从而暴露敏感数据或激活勒索软件。为了阻止这种类型的攻击，FerriSSD 产品支持安全数字签名验证机制，以在系统启动时提供安全的数字签名。利用电熔丝 (eFuse)，为 FerriSSD 固件与软件加入数字签名（Digital Signature）功能；简言之，eFuse 是一个外人无法碰触的保护机制，一组独有的密钥，使得黑客就算入侵 FerriSSD，也会碍于无法通过数字签名验证程序，因而无法窜改固件，更无法擅自启动 SSD。若是验证签名失败，会导致系统向主机处理器传送安全性警告。

安全数字签名还允许将固件更新远程应用到 FerriSSD 单元。



主动式的保护：IntelligentScan™ & DataRefresh™

经过验证的主动数据保存可以抵抗物理攻击

FerriSSD 提供高达 1TB 的存储容量，采用 16mm x 20mm 表面贴焊 BGA 封装技术。这可以安装在靠近主机处理器的电片或主板上，与传统的外部 SSD 相比，可确保有更好的保护，以防止物理篡改。

黑客也可能试图通过假装紧急不定期的维护来攻击目标。透过慧荣独有的 IntelligentScan 智能扫描功能，可依主机访问行为与工作环境的变化，自动启动扫描作业，检测 NAND 闪存区块与单元的状况，并结合 DataRefresh 功能，自动修复或替换存在失效风险的闪存单元，维持整体存储设备的可靠性与稳定性。

此外，所有 FerriSSD 都支持安全快速清除功能，如果检测到干扰，可以立即删除所有数据。还提供临时断电保护机制以触发数据刷新序列，在突然断电等意外事件期间安全地存储用户数据。

结论

SSD 固态硬盘提供节能、小巧和高性能的大容量存储，其强大功能适用于各种企业、医疗和汽车计算应用。为防止黑客窃取数据，对于维护存储数据的安全至关重要，其加密方式包括在主操作系统中的软件或磁盘本身内嵌的硬件进行全磁盘加密。

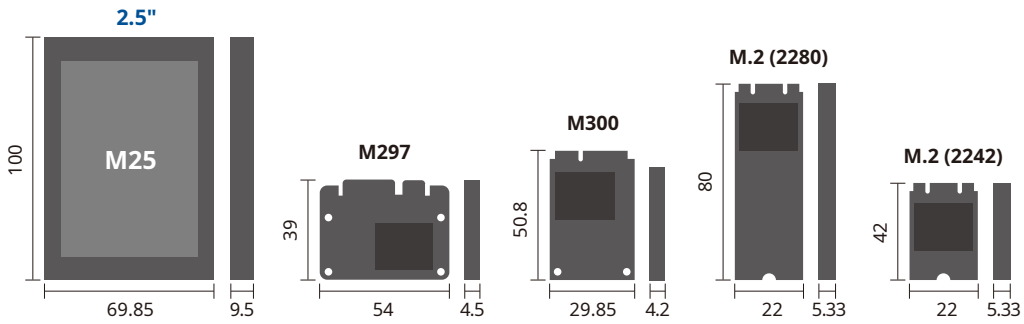
慧荣科技的 FerriSSD 支持硬件加密技术，在不增加主系统 CPU 负载的情况下运行，因此提高了便携应用的性能、能源效率和电池寿命。为了增强和增加加密提供的保护，从而针对当今的网络威胁提供最有效的安全，FerriSSD 使用了数字签名、篡改检测和紧急擦除等附加技术，可在发生窃取攻击时提供固件保护。

FerriSSD® BGA SSD 解决方案

规格	
主机接口	SATA Gen3 PCIe Gen3x2;Gen4 供于 2023 年第 1 季
容量	SLCmode:10/20/40/80/160GB;320GB 供于 2023 年第 1 季 TLCmode:32/64/120/240/480GB;960GB 供于 2023 年第 1 季
外观尺寸	20mm x 16mm BGA
绿色产品	符合 RoHs / 无卤
支持的温度	商用级温度 (0°C 至 70°C) 工业级温度 (-40°C 至 85°C)

FerriSSD® 模块解决方案

外观及尺寸



要了解更多有关 Ferri 家族产品的信息，请访问
www.siliconmotion.com 或发送电子邮件至 **ferri@siliconmotion.com**