Preliminary

Applications

- Telemetry
- Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance (C4ISR)
- Avionics and Aerospace

Benefits

- Data can be stored within any remote system and transmitted between systems or to a central host with NIST ratified and FIPS approved AES-256 encryption.
- Data remains encrypted and secure even if transmission links, networks, NICs, systems, memory, operating systems, and, and HBAs are compromised.
- Easy to integrate into any system that supports NVMe storage interface.
- Simple to learn and use, browser based mobile application for remote configuration and monitoring of cyber secure transmission between the data source and the data destination.
- Create Virtual RAMPART Modules on a local central host and receive encrypted data transmitted from dozen of distributed physical RAMPART modules.
- Designed and intended to withstand the harshest remote environments
- Dependable, consistent, and remotely accessible for long-term operation regardless of where and how it is deployed
- Supports nearly all mobile applications where size, weight, and power are important
- Wide range of capacities to address any requirement
- Use on BiTMICRO ACUMEN NVMe over IP connected Networked and Scalable Secure Storage Nodes to secure block-based data reading and writing across any IP Network.

BiTMICRO
Time - Tested. Verified Rugged. Proven Secure.

RAMPART™

EMBEDDED, CYBER SECURE SOLID STATE STORAGE MODULE

M-SERIES for Military Applications

BiTMICRO® RAMPART Embedded Cyber Secure Solid State Storage Modules – M-Series offer a unique embedded security solution for data at rest as well as data in transit between at least two locations. Three security configuration options are available including using a pair of storage modules between at least two different locations. One of the modules is configured to encrypt only during writes and not decrypt during reads, enabling read data to remain in its original encrypted form during transmission to the other paired security module. This other paired security module receives the transmitted data and stores it in its original encrypted form. Once a user is properly authenticated, this storage module will decrypt the stored data so it can be read.

RAMPART Cyber Secure Solid State Storage Modules – M-Series provide an elegant yet effective security solution, permitting remote configuration at different locations at the hardware device level and thus, simplifying implementation in maintenance and management, especially in virtualized or cloud-based computing architectures whether private, public or both.

Feature Highlights:

- Distributed, End-to-End – contiguous and seamless encryption
- Military Grade – Verified Rugged
- Simple to learn and use, browser based mobile application provides centralized management of all local and remote systems.
- View detailed configuration and operational statistics with an extended user interface.
- Embedded AES 256, NIST ratified and FIPS approved
- FIPS 140-2 Level 3 compliant
- Compact size with standard NVMe interface for simple integration
- Up to 16TB of solid state storage capacity per module.
- Create local Virtual RAMPART Modules to securely receive data from dozens of remote physical modules.
- Use with ACUMEN Networked and Scalable Secure Storage Nodes.

Although this powerful embedded security solution is hardware-enabled, it has a software-configurable framework that is language-neutral, platform-neutral, and extensible, reducing the high cost of implementation typically required to protect the entire ecosystem – from host, network, to storage.

In addition, the RAMPART M-Series Line of Embedded Cyber Secure Solid State Storage Modules are manufactured under our Verified Rugged program, tested and screened to operate in rugged and hostile environments. Built-in PowerGuard® technology protects data loss during power degradation or outage.

BiTMICRO maintains provenance of the RAMPART Cyber Secure Solid State Storage Module by controlling all aspects of the product lifecycle, from in-house design to trusted manufacturing and sourcing partners.

Preliminary

BITMICRO
Time - Tested. Verified Rugged. Proven Secure.

Product Specifications

Physical	
Form Factor	U.2
Interface	PCIe 3.0 x4, NVMe 1.2
Dimensions (LxWxH)	100mm x 69.85mm x 15mm *(may vary depending on required storage capacity and NAND type)*
Management	
Mobile Browser Application	Included - Simple to learn and use, browser based mobile application provides centralized management of all local and remote systems.
Comprehensive and Intuitive GUI	Included - View detailed configuration and operational statistics with an extended user interface
Capacity	
Storage Capacity	32GB to 16TB *(utilizing BiTMICRO Altima™ storage)*
Supported NAND Types	SLC, SLC Mode over 3D TLC NAND, MLC Mode over 3D TLC NAND, 3D TLC NAND
Security & Data Protection	
Data Encryption-Stored Data	Included - Embedded AES-256, NIST ratified and FIPS approved
Data Encryption-Transmitted Data	RAMPART™ Cyber Security - Data remains encrypted during transmission - Embedded, Distributed, End-to-End, AES-256, NIST ratified and FIPS approved
TCG Opal 2.0 Compliance	Optional
FIPS 140-2 Level 3 Compliance	Optional
Crypto Erase	Optional
Secure Erase	Optional
Military Sanitization	Optional
PowerGuard® Power Loss Data Protection	Supported
Performance	
Sequential Read / Write	1GB/s Read / 800MB/s Write
Random Read / Write	150K IOPS Read / 130K IOPS Write
Environmental (Operational)	
Temperature	Industrial Extended: -40 to 70 ºC Industrial Wide: -40 to 85 ºC
Power	
Voltage	12V DC
Power Consumption	<25W
Manufacturing and Other Military Option	
Ruggedness Level	Verified Rugged Per Module Manufactured
Connector	Optional Rugged, multi-insertion, and/or environmentally sealed connectors
Solder	Leaded or Lead-free
Potting / Encapsulation	All methods/types
Conformal Coating	All methods/types - including Silicon, Acrylic, Urethane
Warranty	
Standard	1 Year
Extended (Optional)	3 Years

For more information:

Email:
sales@bitmicro.com

Call: +1 (888) 72-FLASH

www.bitmicro.com