Preliminary

BITMICRO
Time - Tested. Verified Rugged. Proven Secure.

Applications

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

Benefits

- Create a highly secure data encryption ecosystem across any private or public cloud
- Simple, portable, and extensible browser-based management application
- Monitor the entire data encryption environment with the browser-based mobile app or use the more comprehensive and intuitive GUI.
- Manage a few to thousands of remote RAMPART-enabled systems
- Integrate encryption key management with other security applications
- Create individual or global encryption policies for data stored and transmitted within the ecosystem
- Secure and authenticated point-to-point communication with remote RAMPART Modules.
- Securely transmit data from dozens of distributed RAMPART Modules to a central host and store that data on a matching number of local Virtual RAMPART Modules.
- Maintain efficiency and longevity with health, utilization, and performance monitoring and reporting

RAMPART™

CYBER SECURE MANAGEMENT SOFTWARE

for RAMPART Cyber Secure Solid State Storage Modules

BiTMICRO® RAMPART Cyber Secure Management Software is a software-configurable framework that is language-neutral, platform-neutral, and extensible. It includes a browser-based application and a more comprehensive intuitive GUI. The management software is designed to manage, configure, monitor, and control the unique RAMPART Cyber Secure Solid State Storage Modules in delivering a powerful embedded security solution for data-at-rest as well as data-in-transit between any two locations. RAMPART Cyber Secure Management Software is essential to configuring the distributed security options available with RAMPART Cyber Secure Solid State Storage Modules.

Feature Highlights:

- Private Cloud (IoET) – An Internet of Encrypted Things
- Browser-based basic interface
- Comprehensive and intuitive GUI
- Scale-out architecture
- Securely transmit data between any two distributed physical RAMPART Modules.
- Securely transmit data from dozens of distributed physical RAMPART Modules to a single host by creating an equal number of local Virtual RAMPART Modules.
- Easy-to-Integrate
- Seamless encryption
- Centralized management
- Secure and authenticated communication
- Health, Capacity, and Performance Monitoring
- Crypto and Secure Erase
- Optional military sanitization

RAMPART Cyber Secure Management Software is available in two product editions:

Configurable Encryption Edition

Enables users to control the Distributed Security configuration of the RAMPART Cyber Secure Solid State Storage Modules. It includes a mobile browser based application for basic configuration and monitoring along with the more comprehensive and intuitive, extendable GUI to view detailed configuration and operational statistics.

Full Suite Edition

Includes the Configurable Encryption Edition and adds military sanitization. Military sanitization includes all the commonly used and approved standard methods of protecting sensitive information from unauthorized access and retrieval.

DTS-MK-068-x02

Preliminary

BITMICRO
Time - Tested. Verified Rugged. Proven Secure.

Product Features

Encryption	
Data Encryption-Stored Data	Included - RAMPART Embedded AES-256, NIST ratified and FIPS approved
Data Encryption-Transmitted Data	Included RAMPART™ Cyber Security - Data remains encrypted during transmission - Embedded, Distributed, End-to-End, AES-256, NIST ratified and FIPS approved

Configurable Encryption Edition

RAMPART Browser-Based Application

Discover RAMPART Modules on the network – assign name and location
Remotely create RAMPART Module Pairs – source and destination
Configure Encryption Method
Monitor status of RAMPART Modules - Paired / Not Paired - Active Pair Status: ➢ GREEN – OK ➢ AMBER – OK with WARNING ➢ RED – ALERT/HALTED – STOPPED FUNCTIONING
Un-pair RAMPART Modules – Return RAMPART Modules to Not Paired status

RAMPART Comprehensive and Intuitive GUI

Centralized Management

Module Management	• Server and Module List • Distributed Security Configuration • Module Information • Health Monitoring • Firmware Upgrade / Downgrade • Crypto Erase Function • Secure Erase Function

Distributed Security Configuration

Security Configuration Pairing	• Module Selection	• Module Pairing
Security Configuration Setting	• A (Encrypt Write / Decrypt Read) • B (Encrypt Write / Normal Read) • C (Normal Write / Decrypt Read)	

Product Information

Module Information	• Firmware Version • Model Name • Product ID • Serial Number	• Vendor ID • Capacity • Performance Statistics

OS Support

Operating System	• Linux	• Windows

RAMPART Full Suite Edition adds Military Sanitization

Military Sanitization

Supported Standards	• NSA 130-2 • NSA 9-12 • US Navy NAVSO P5239-26 • US Air Force AFSSI 5020	• US Army 380-19 • IRIG 106 Chap 10 • NISPOM DoD 5220.22-M

For more information:

Email:
sales@bitmicro.com

Call: +1 (888) 72-FLASH

www.bitmicro.com