RAMPART™ Distributed End-to-End Embedded Cyber Security

End-to-End Encryption

For Industrial and Government Applications

What is End-to-End Encryption?

Year after year, data is becoming more valuable and used in a wider variety of ways. Securing data has become every organization's utmost priority. Data should be protected at all times, from the location where it is created and stored to the location where it is sent and used. Data breaches affect all organizations, including commercial industries such as financial, healthcare, oil and gas, and research. And government agencies focused on infrastructure, administration, local and national security, customs, law enforcement, emergency services, and homeland security.

One way of protecting and securing data is by employing encryption. The Advanced Encryption Standard (AES) is a standard ratified by the National Institute of Standards and Technology (NIST). The AES specification is approved by Federal Information Processing Standards (FIPS 197) used to protect electronic data. The FIPS-approved cryptographic algorithm converts data or plaintext to an encrypted form called cipher-text and decrypts cipher-text to its original plaintext form.

Based on the standard, government agencies and other organizations may use the specification when sensitive information requires cryptographic protection. Although established for federal government agencies, the standard may be used by any organization to protect sensitive information.

Storage media, such as SSDs (solid state drives) equipped with encryption, only prevent unauthorized access to the data while it is stored. However, data being moved or transmitted from one location to another in a network remains vulnerable to unauthorized access. The most common threat for data being transmitted is the man-in-the-middle attack. It is a type of cyber-attack where the data between the sender and recipient is intercepted and then altered or used, or both.

End-to-End Encryption, encrypts data being transmitted from one location to another therefore preventing anyone in the middle from using or altering the information. End-to-End Encryption or E2EE is considered as the most secure communication method because only the sender and the recipient have access to the data being sent across the network.

What is BiTMICRO® RAMPART Distributed End-to-End Embedded Cyber Security?

BiTMICRO RAMPART Distributed End-to-End Embedded Cyber Security is comprised of RAMPART Cyber Secure Solid State Storage Modules and RAMPART Cyber Secure Management Software. This offering from BiTMICRO provides a unique embedded security solution for data while it is stored and while it is being transmitted.

The RAMPART Distributed End-to-End Embedded Cyber Security solution delivers end-to-end AES-256 encryption. The RAMPART Distributed Cyber Security solution addresses the E2EE challenge by providing the most advanced and distributed, seamless, secure data storage and data transmission environment. Sensitive information is protected by RAMPART Distributed Cyber Security AES-256 encryption when stored and while being transmitted. With RAMPART Distributed Cyber Security, data can be acquired, encrypted and securely stored and transmitted from remote and mobile systems such as: customs inspection scanners, law enforcement and emergency service vehicles, surveillance and border patrol drones, oil and gas exploration vessels, unmanned marine systems, and in-cabin facial recognition scanners.

End-to-End Encryption is created by pairing two RAMPART Cyber Secure Solid State Storage Modules, one at each endpoint (sender and recipient). The remote sender module can be configured to encrypt only during writes and not decrypt during reads, enabling the data to remain in its encrypted form when transmitted to the local receiving module. By encrypting the data during transmission, data will be unusable in the event of a man-in-the-middle cyber-attack. During transmission, the local receiving module receives and stores the encrypted data. The data remains encrypted through the entire data path. Only an authenticated user, with a properly configured system and the correct AES-256 key can access the local receiving module and decrypt the data so it can be used.

RAMPART Distributed Cyber Security is unique because it is true end-to-end AES-256 encryption. Other solutions encrypt data at the OS, link, or network level. But system levels like the memory, CPU, OS and network interfaces can be susceptible to attacks and malware. Network gateways, routers, switches, and transmission signals can also be compromised. Finding and protecting against attacks at all these levels is challenging.

RAMPART Distributed Cyber Security encrypts data at the flash chip/NAND level. As data is written to RAMPART Distributed Cyber Security it is immediately encrypted and stored on the internal flash chips within the solid state storage. The data remains encrypted as it is read from the solid state storage within RAMPART Distributed Cyber Security. The module encryption remains in force as the data passes through the device controller, bus, memory, CPU, OS, and network interface on the remote system. And remains encrypted through the network and transmission links. Even if the physical flash chips are removed from the RAMPART solid state storage and probed, the data will still be encrypted and not useable.

Not only does RAMPART Distributed Cyber Security provide seamless end-to-end AES-256 encryption, it can also securely erase RAMPART Distributed Cyber Security stored data if needed

or completely wipe the RAMPART solid-state storage using secure erase or other sanitization standards. Data can be erased and sanitized on any remote or local module.

How is BiTMICRO RAMPART Distributed Cyber Security deployed and managed?

RAMPART Cyber Secure Solid State Storage Modules are NVMe devices that are available in a variety of storage capacities. They can be installed into any system that uses the NVMe protocol. The modules retain data in a fully AES-256 encrypted state while data is stored, transmitted, or transported between any two RAMPART Cyber Secure Solid State Storage Modules.

RAMPART Cyber Secure Solid State Storage Modules do not necessarily require an operating system. They can be deployed on a larger variety of remote systems. All that is needed from the connected system is the ability to receive a command and send that command to the NVMe connected RAMPART Cyber Secure Solid State Storage Module. RAMPART Cyber Secure Solid State Storage Modules are not only compact, secure, and energy efficient, but also verified rugged. They resist shock, vibration, wide temperature ranges, altitude, humidity, power outages, and power degradation.

RAMPART Cyber Secure Solid State Storage Modules, although a hardware-based solution, are managed by a software-configurable framework. It is language/platform-neutral and extensible, simplifying and lowering the high cost of implementation typically required to protect the entire ecosystem – from the host, network, to storage.

In addition to the end-to-end encryption solution with its seamless AES-256 encryption implementation, RAMPART Distributed Cyber Security provides an option to securely erase data on any module using secure erase or other data sanitization standards.

RAMPART Cyber Secure Solid State Storage Modules are offered with the RAMPART Cyber Secure Management Software to manage the security configuration and authentication, as well as the execution of data sanitization.

RAMPART Cyber Secure Management Software:

- Finds and manages all RAMPART Cyber Secure Solid State Storage Modules with one interface
- Displays module health, performance, and usage information
- Supports multiple users, hosts, RAMPART Cyber Secure Solid State Storage Modules
- Manages distributed security configuration
- Manages “secure-erase” and sanitization of the RAMPART Cyber Secure Solid State Storage Module stored data.

RAMPART Distributed Cyber Security Conclusion

As data continually grows and moves in different directions, data breaches are becoming more prevalent and widespread. Cybercriminals are becoming more creative and innovative in penetrating private or government organizations to access sensitive and confidential information. The effect is costly and damaging.

Implementing an end-to-end encryption solution addresses the need to secure data while it is stored and while it is being transmitted. By storing and encrypting data from a RAMPART module in the sending system, across a network, to a RAMPART module in the receiving system, true end-to-end encryption is ensured and man-in-the-middle attacks are prevented.

RAMPART Distributed End-to-End Embedded Security simplifies end-to-end encryption. By deploying distributed embedded security at the RAMPART Cyber Secure Solid State Storage Module level, there is less need to manage costly cyber security solutions at all the system and network levels susceptible to attacks. With its advanced technology, data will be encrypted from the sender system upon acquisition, during transmission, and upon receipt and storage at the recipient system.

NOTES:

Artificial Intelligence

RAMPART Distributed Cyber Security with BiTMICRO ACUMEN™ for AI on the EDGE

RAMPART Distributed Cyber Security can be used in conjunction with BITMICRO ACUMEN™ – AI on the Edge. ACUMEN Ruggedized Supercompute AI Platform is a low SWaP, compact, portable and rugged platform for remote AI, supercomputing, or data recording applications. BiTMICRO ACUMEN AI Platform and BiTMICRO RAMPART Distributed Cyber Security can be combined to provide a secure and powerful military-grade solution delivering security and intelligence to the edge of your infrastructure.

Solid State Storage

RAMPART Distributed Cyber Security with BiTMICRO ALTIMA™ Solid State Storage

RAMPART Distributed Cyber Security utilizes up to 16TBs of BiTMICRO Altima™, verified rugged, solid state storage. Altima solid state storage supports all popular SSD NAND types and includes features to ensure durability and reliability.