Smartronix

EEDS

Expeditionary Encrypted Data Store

Photo Credit: www.af.mil

SECURING DATA AT RISK FOR DEPLOYED MILITARY UNITS & INTELLIGENCE AGENCIES

The current missions and military operations of our Armed Forces require the need for deployable computing systems in both mobile (i.e., aircraft, armored vehicles, battleships, etc.) and fixed strategic locations (i.e., command posts and embassies, etc.) While these Net-Centric systems offer many tactical benefits, protecting sensitive or classified information from the enemy can also pose a challenge. Smartronix, Decru, and Network Appliance have teamed to develop a solution to secure computer systems in theatre. The Expeditionary Encrypted Data Store (EEDS) is the ultimate secure storage solution for military or intelligence organizations.

WHAT IS EEDS?

As a turnkey secure data storage alternative, EEDS is an integrated system that has been designed for rapid deployment and mobilization. The system is comprised of a Decru DataFort encryption device and a NetApp FAS200 series data storage system enclosed in a rugged case designed for remote deployment. Data is always stored encrypted by EEDS using FIPS 140-2 Level 3 AES 256 encryption and its Decru CryptoShred features can be utilized to delete local encryption keys instantly with a push of a button.

This push of the button results in instant sanitization of the entire system since the data is never written in clear text format and the encryption keys are necessary to decrypt the stored data. With EEDS, operators are able to lock down systems temporarily with the removal of a cryptographic “ignition key” stored on a smart card. This unique element facilitates the ability to transport, service, and deploy the system securely and avoid the exposure of mission data to physical or electronic security breaches. For example, a forward deployed data center could be provisioned with pre-staged mission data, but all data would remain in an encrypted format until authorized personnel arrive with the appropriate smart cards.

CAPABILITIES

Boost Secure Storage Consolidation. EEDS can be used to secure storage by consolidating separate groups and/or applications onto one NetApp storage device. Data is compartmentalized into Cryptainer vaults on the Decru Datafort, allowing fine-grain access controls and surgical deletion of data. Stored data is cryptographically partitioned in Cryptainer vaults, which provides an additional layer of threat containment.

Secure Information Sharing. EEDS provides coalition partners and agencies with the ability to share data securely on the same system. Need-to-know access controls and crypto-signed logs guarantee that only authorized personnel can access the shared data. In the field, this offers greater flexibility to military unit leaders and commanders while promoting improved information sharing. With EEDS, data access can be easily provisioned and de-provisioned through sharing partner designation of access control and key management policies.

Stronger Insider Threat Mitigation. All data stored on EEDS can be managed by both Storage and System Administrators, but access to clear text data is not granted to unauthorized personnel. This "role separation" control measure expands options for administrator selection and encourages access to data based on a need-to-know.

COMPONENTS

Network Appliance FAS200 series: The FAS200 series combines the advanced functionality and data protection features of NetApp's storage architecture with high-capacity Fibre Channel (FC) disk drives.

The system features up to 14 FC disk drives per 2U rack-mountable enclosure. Storage capacity can be scaled up to 4TB of raw storage in a single unit and 16TB of raw storage across 4 units, with disk drive sizes from 72GB to 300GB. The FAS200 series supports a variety of server platforms with SAN, NAS and iSCSI.

NetApp leverages SnapMirror and SnapVault software to provide increased data availability and simplify backup and restore operations with automatic and network efficient replication of data. Because encrypted data is mirrored from one system to another, all replicated copies are secure by default. No user or application at the remote site can access the data until a remote Datafort is injected with the correct encryption keys.

Decru DataFort Storage Security Appliances: Decru DataFort appliances wrap strong AES-256 encryption, granular access controls, authentication, and crypto-signed auditing into a high-performance hardware appliance. DataFort's hardware-based encryption runs at wire speed, so there is no performance degradation. DataFort hardware was designed from the ground up for maximum security. At the heart of the system is Decru's Storage Encryption Processor (SEP) a robust hardware engine enabling full-duplex, multigigabit speed encryption and key management. Decru's SEP, clustering, and key management have been validated by the National Institute for Standards and Technology (NIST) for compliance with FIPS 140-2 level 3. DataFort's AES-256, SHA-1, and SHA-256 encryption implementations also have been certified.

Smartronix: As a value added manufacturer, Smartronix offers several configurations for the EEDS solution. For more information, please contact us at 301-737-2800.