Ciphertex family of Secure Portable Storage Systems

Ciphertex is the leading provider of secure, portable data storage systems using advanced AES 256-bit encryption hardware, guaranteeing the highest level of data security and performance. Computer forensics and cyber investigation agencies use Ciphertex encrypted hard drives and storage systems for evidence collection and to ensure successful representation of data when called on as a forensic data expert witness.

Single Drive Systems

Ciphertex encrypted hard drives are the cornerstone of any computer forensic investigation or data security strategy. Portable data storage must be protected from cyber stalking, theft, and loss. Hardware implementation of the advanced AES 256-bit encryption algorithm provides the fastest performance possible, Ciphertex portable hard drives can be purchased in capacities from 500GB to 2TB or in an encrypted SSD (Solid State Drive) from 80GB to 160GB. Securing data and forensic evidence collection are made easy by high performance, interoperability with any Operating system and application, and easy connectivity via USB 2.0 and eSATA.

Network Attached Storage

Ciphertex provides secure mobile Network Attached Storage (NAS) for demanding forensic data collection applications when data mobility and security are required with capacities up to 40TB and 1GgE to 10GbE connection speeds with file system access and AES 256-bit encryption.

When data is brought from the work site to the processing location, Ciphertex also offers a rack mount version of their industry leading secure, portable storage. Offering the same AES 256-bit highest level of encryption, Ciphertex rack mounted NAS storage is the perfect resource for quick turnaround of deliverables with up to 48 TB of storage capacity operating at up to 1,000 MB/s throughput. These rack mounted systems expand to 72 data drives via JBOD expansion enclosures for virtualized or clustered workgroup applications.

All Ciphertex NAS storage systems provide built-in advanced RAID management with hot-swap design, simple-to-use sophisticated system management tools driven from a web-based GUI, AES 256-bit hardware encryption, and high network bandwidth allowing these systems to easily drop into any architecture.

Ciphertex secure, portable data storage systems are designed for Digital Forensic applications and address the special demands of successful civil and criminal investigations. Designed with input from the FBI and other pioneering forensic organizations, Ciphertex secure storage systems are engineered from the ground up to meet the exacting requirements of law enforcement and investigative personnel. This ensures data extraction with the highest integrity for proper unaltered presentation in a court of law.

Ciphertex offers three critical differentiating capabilities for use by modern government agents, information technology specialists, and private investigators in the process of evidence collection, handling, analysis, chain of custody, and archiving. These are safe secure data transport, easy data access and fast data collection.
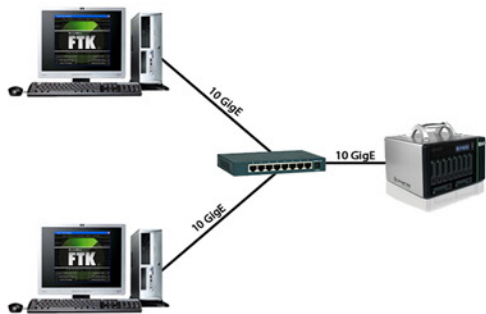
Secure Data Transport

Digital evidence can be altered, damaged, or destroyed due to improper handling or examination. At no stage during the transit of the electronically stored evidence can intercession by a third party be possible. Failure to do so may render the data unreadable, inadmissible, or lead to an inaccurate conclusion. All Ciphertex secure, portable storage systems are designed to the highest quality standards and incorporate the industry's most powerful AES 256-bit encryption system to arm investigators with powerful tools to protect digital evidence and to assure the data is secure from tampering during transit, awaiting presentation, or stored for later access.

Ciphertex also implements a unique separate hardware key. When the system is booted without the key, the data on the disks cannot be accessed. By limiting access to the encryption keys, custodial control of the evidence can be strictly enforced. The encrypted data on the disk drives is safe from hackers or any system security breach as evidence data cannot be accessed, manipulated or altered when stored on Ciphertex secure, storage systems.

Ciphertex also offers portable, multi-drive systems that implement RAID data protection. RAID protects data from corruption and mechanical failure so there is no degradation of evidence over time and the original evidentiary copy is maintained.

Easy Data Access

At the scene a forensic expert must quickly ascertain how to best access the suspect's systems to sequester an original copy of the suspect's data. It is also critical during the extraction and acquisition process to use a reliable means of accessing the suspect information without alteration or corruption. Ciphertex secure portable storage systems address this need by providing a broad range of interchangeable, high speed connectivity options enabling investigators to quickly capture evidence data at a suspect's location. Ciphertex offers direct connection to storage devices through eSATA, USB 2.0 or 3.0, and FireWire. When there's a network, Ciphertex NAS systems can connect

to the network at 1GbE or 10GbE to access all devices on the network. Connecting in a way that is native to the target system helps ensure data structure and content is unaltered from the original thereby demonstrating a higher degree of trustworthiness in data authenticity.
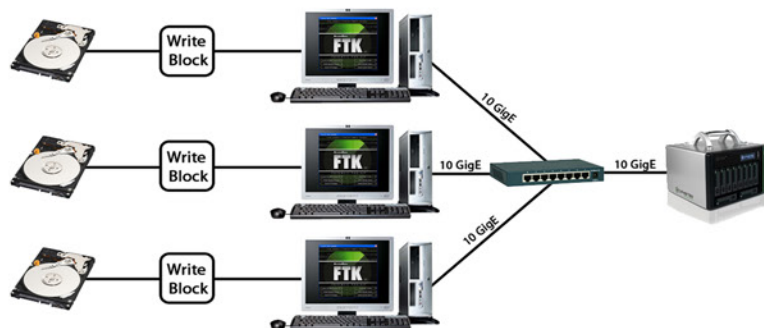
Fast Data Collection

Reducing on site time in the collection of data reduces the overall cost of investigation. Ciphertex uses scalable storage (500GB to 40TB) with the fastest available processors, memory, and networking in their class. This along with AES-256 bit encryption ensures the best possible performance. Furthermore, this encryption algorithm takes advantage of system infrastructure eliminating processing bottlenecks while still providing the fastest most secure encryption system in the world.

Ciphertex multiple drive RAID and NAS systems allow quicker access to multiple sources simultaneously, reducing the time required to collect and ingest data. High speed disk drives and high speed network interfaces (that can reach speeds up to 10 gigabits per second - billion bits per second) create the highest performing systems for electronic forensic data collection. These devices are also compact with an integrated carrying handle for easy transportation and portability.

eDiscovery

Ciphertex secure, portable storage systems enable good faith effort during the discovery process providing advantages to both parties easing the burden of data collection for the defendant and providing for a secure transmission and storage for the plaintiff. Easy network access and high performance systems reduce the cost of producing the evidence and enable ready compliance with delivering timely native data and metadata. Encrypting the data and providing a separate physical encryption key ensures the data cannot be altered or accessed by unauthorized parties. This provides total protection if a drive is lost or stolen while being transported to meet judicially mandated discovery requirements.

Single Drive Evidence Failure

Data security, easy connectivity, and speed of capture are clear advantages for Ciphertex secure, portable data storage. E-forensic investigators also avoid the single drive evidence failure if a failure occurs when the suspect use the largest drives currently available. Since best practice forensic data collection requires the collection of all native data with metadata intact, the forensic information from the collection software, and the hash or digital finger print. The total data will exceed the size of a given single drive of the same capacity. If the suspect's data drive is the largest on the market a similar size drive cannot capture the data. Ciphertex solves this problem by providing multi-drive storage systems that can be partitioned into sizes corresponding to the size of data that needs to be collected plus any data