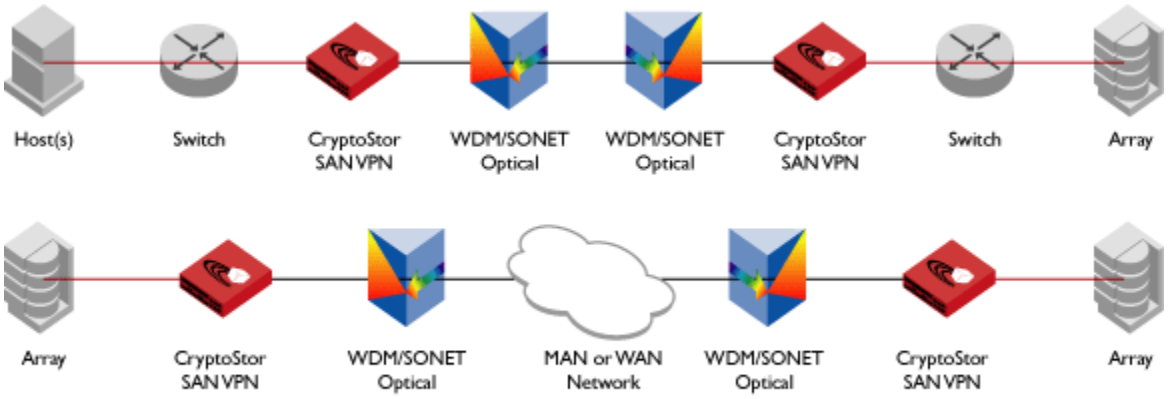
Data Security & Encryption

Business Links has embedded data-security as an integral part of its infrastructure solution offerings. In line with the Data & Storage consolidation trends, organizations have been rapidly adopting aggregated storage technologies like NAS and SAN. The need to consolidate and increase ROI is at the top of every CIO's agenda. Business triggers for enterprise storage consolidation are especially compelling: reduced costs, increased scalability and added ROI. Unfortunately, the aggregation of these storage systems significantly increases the exposure of sensitive data. Especially data from independent application becomes co-resident on a common storage array, and a single internal or external breach can compromise terabytes of data.

Business Links has carefully followed the industry developments as security encryption engines for "Data-at-Rest" and "Data-in-Transit" continue to mature. Our alliances and hands-on deployment experience with emerging encryption & compression technologies makes us a preferred solution provider in this area. When a business's integrity rests on its ability to keep customer or partner data confidential, a complete strategy to secure it in flight and at rest becomes even more critical.

Our solution for securing both "Data-at-Rest" and "Data-in-Transit" includes a field proven technology offering by Neoscale. A typical CryptoStor appliance delivers policy-based storage security, which automatically encrypts data that is in-flight over a storage network, or at-rest on disk, virtual tape, or tape media.



SAN VPN Deployment Options

For example, a primary storage can be secured with virtually no performance impact and with no changes to storage mapping – this ensures that operations can deploy the solution without impacting service level agreements. In addition, the IP Clustering mechanism available as a standard feature with CryptoStor facilitates multiple encryption engines deployed at geographically dispersed sites, thereby providing for alternate-site recovery mechanism for locally encrypted data.