

Data Encryption

By David Wilkins
SARCOM Senior Enterprise Engineer

Read the news today and you might think that encryption will solve all your security needs. Storage encryption is being praised by industry experts across the globe as the solution to data encryption both in transit and at rest. This, however, is seldom true. Encryption is actually a function of the internal and external processes that affect data.

Why Data Encryption?

SANs today are susceptible to internal and external threats that require security. Regulatory requirements on classifying data, monitoring access to the data and securing the data are causing storage teams to incorporate increased security measures.

The SAN has often been seen as an isolated environment that has been immune to attackers. Storage managers have previously thought through the use of fiber channel in their environment they wouldn't be noticed. Today this assumption is no longer true as the fiber channel gap has been bridged through the use of IP storage devices attached to fiber channel storage networks.

Threats that expose different vulnerabilities will require various lines of defense. The security strategy that has been used in the network world for years will have to transcend to the storage arena. A proper defense will be one that covers identity, policies, access control, securing hosts, securing storage devices and securing their interconnects.

Implementing these changes alone may not work. The issue of security doesn't only cover storage, but also translates to all other facets of a technology infrastructure. Corporate security teams will have to begin to work closely with the storage teams to create an effective data security practice.

Encryption is only as good
as the authentication layer
it's built upon.

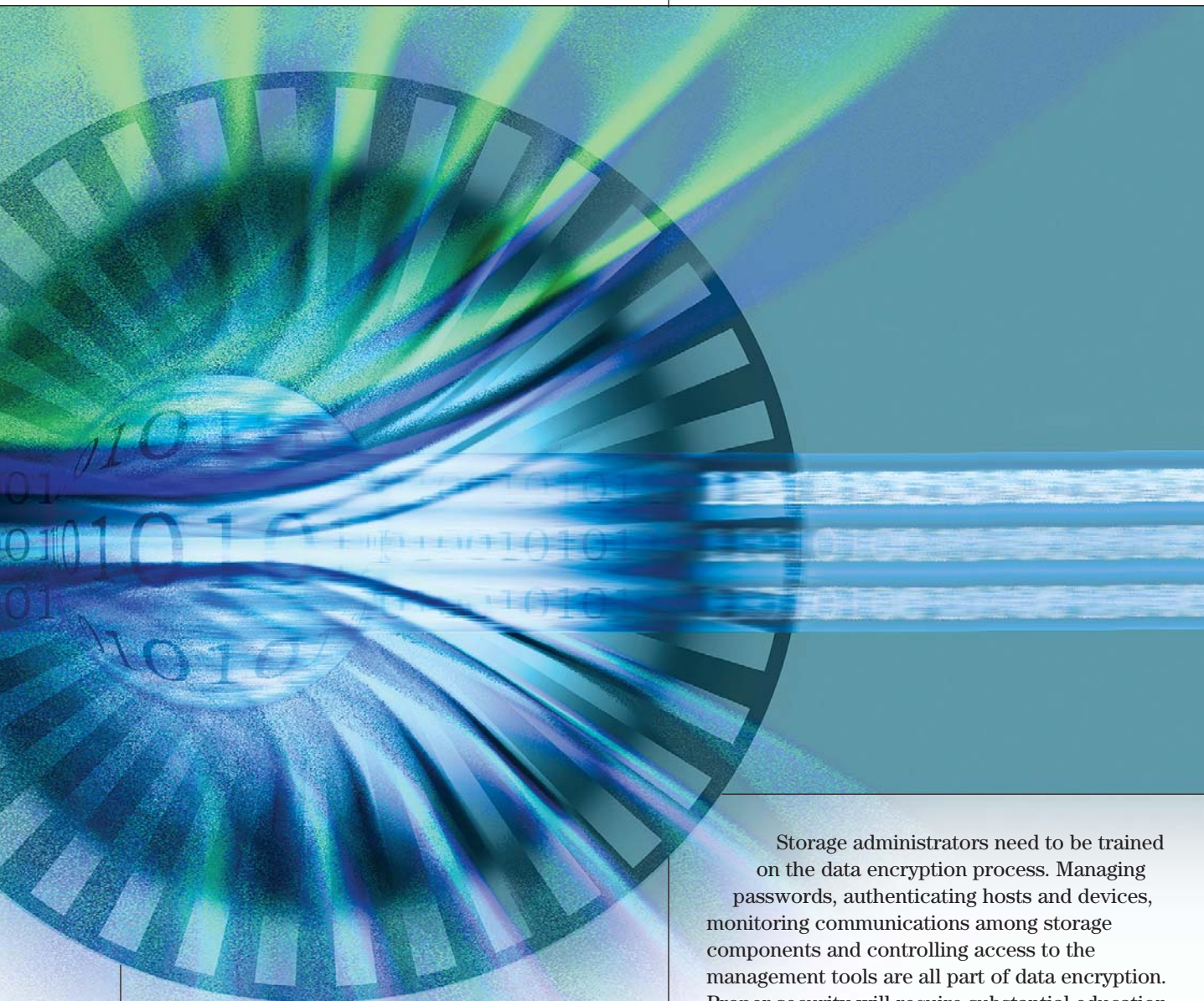
010001011110001010101
010001011110001010101
010001011110001010101

Why organizations aren't using Data Encryption

The three major obstacles to storage encryption are: cost, latency and key management. Storage encryption can be expensive when utilizing some of the encryption appliances on the market today. Precious CPU cycles are consumed during the encryption process and lead to latency. Key management is complex and expensive, requiring more administration time to maintain and support.

Access control for storage is currently limited because role-based access control is almost non-existent. Role-based security needs to mature and become more common place. Identity management is another key component that is lacking in which the storage managers have no direct control over. The storage team often sees the responsibility of identity management fall into the area of application developers or DBAs.

The disparity of responsibilities leads to breakdowns that in turn are likely to cause security breaches. A proper solution is to have the corporate security, storage, network and application groups define a set of policies and procedures.



The main issue with policies and procedures is: Who drives them? Cooperation among all the players will be needed. The storage team can implement basic security measures, but an overall policy at the corporate level is required.

Basics that a good data encryption system will cover

The core security building block to any SAN is proper authentication. Encryption is only as good as the authentication layer it's built upon. Data encryption is not necessarily meant for every type of data, but could be used for certain data sets that go offsite or contain sensitive information. The impact on backup and recovery should be evaluated when considering encryption.

Storage administrators need to be trained on the data encryption process. Managing passwords, authenticating hosts and devices, monitoring communications among storage components and controlling access to the management tools are all part of data encryption. Proper security will require substantial education which increases costs.

An investment in expensive hardware based encryption devices will be required. Encryption appliances can start at around \$30,000. An investment in additional authentication, firewall and intrusion detection systems will be needed, however, these devices will not be a storage centric device, but a shared infrastructure expense.

There is no real single solution to the storage security problem. Identity management, authentication and encryption will all play an important role. Corporate security, network and application groups have tasks required that are beyond the realm of the storage team. Actions listed within SNIA's "Introduction to Storage Security" whitepaper can begin to be implemented, but storage security requires a corporate-wide effort.