For Your Eyes Only

Blair Semple
CISSP-ISSEP, Director, Business Development, SafeNet

Enhance Data Security with SafeNet and NetApp

More than ever before, your data is outside of your control, whether you know it or not. For a variety of reasons from financial gain to national security, Big Brother, Aunt Cloud, and lots of thieving third cousins are all clamoring for a glimpse at your sensitive information. And because of the sheer amount of data and the rise of virtual and cloud storage, it's pretty easy for them to get to it.

Threats to Privacy and Security

Whether for national security or financial gain, everyone from defense agencies to cybercriminals wants to see your information. Cybercrime rings have grown from accolade-motivated "script kiddies" to multimillion-dollar organizations profiting from the sale of sensitive data. Meanwhile, there are several technical trends that, while necessary to sustain and grow our legitimate businesses, are making it even easier for these adversaries to access our data.

First is the sheer amount of data. Worldwide, the amount of data is growing astronomically, and the percentage of data that's considered "sensitive" is increasing every year. Sensitive data includes government ID numbers, medical records, credit card and payment data, intellectual property, and anything else that could cause harm if seen by unauthorized persons or organizations.

Second is the rise of virtualization, cloud computing, and storage as a service. Virtualization makes it more difficult to keep track of data at all levels of the stack and makes data easier to copy and move. Cloud computing complicates management and control even more, as organizations share layers in a stack among business units or project teams or extend their data center into the public cloud.

You might even be one of the companies capitalizing on this need by offering storage as a service on a pay-for-use basis such as off-site backup and recovery or cloud services. The big issues with both public cloud and storage providers are data ownership and responsibility. Is the onus on the customer or the provider to secure and protect the data? And if a government wants to see the data, does the customer or the provider get the final say on what to hand over? Does the customer even need to be informed?

Secure Your Data with Encryption

The simplest solution to all these security and privacy threats is data encryption. Sure, a disgruntled employee or cloud admin might take data home on a thumb drive, a cybercriminal might steal it, and a government agency might listen in, but all they'll see is a garbled mess, not useful information. Without the encryption keys (which

Explore

Learn More About SafeNet Security Solutions

To learn more about SafeNet's data encryption and key management solutions, download a free white paper:

- Why Encrypt? In Control at Layer 2
- Securing Data in Virtualized Datacenter and Cloud Environments

are stored separately in high-assurance hardware appliances) to decrypt it, the data is meaningless.

After the data repository is encrypted, organizations can hand it off to a service provider with the assurance that even if 10 copies are made, each of those copies is still encrypted. No matter where it goes or how many copies are made, the original owner maintains control of the data by maintaining control of the encryption keys. So even if the cloud provider gets a visit from a government or law enforcement agency looking for your data, they have to come to **you** for the encryption keys. It might not prevent Big Brother from reading your information, but it does make sure that you know where your data is and who is looking at it.

This is a benefit for cloud and storage service providers just as much as their customers. In fact, many service providers are including encrypted storage as a premium tier in their product lineup. If you are a service provider, it not only serves to differentiate you from the competition, but also limits your responsibility for your customers' data. If your customers retain control of the encryption keys, then they retain control of the data, even if it's stored in your environment. This can help alleviate security concerns associated with backup and disaster recovery in the cloud or storing data across country lines and gives organizations the confidence to trust you with 100% of their sensitive data, not just the overflow.

Understanding NetApp Encryption Options

NetApp offers a variety of encryption options to meet specific needs. NetApp's strength (and one of the reasons we at SafeNet like working with NetApp so much) is that they don't try to create a one-size-fits-all solution. NetApp develops different options based on customer requirements and then works with you to figure out which option is right for your specific needs and environment. No matter what your encryption requirement is, NetApp provides a way for you to tackle security. Encryption options include:

- SafeNet StorageSecure for Ethernet-based inline NAS encryption
- NetApp® Storage Encryption (NSE) for encrypting data at rest

SafeNet StorageSecure

The SafeNet StorageSecure encryption appliance protects sensitive data in Ethernet-based NAS deployments (NFS and CIFS). NetApp and SafeNet have partnered to provide advanced encryption services based on high-speed, 256-bit AES encryption and featuring redundant components and clustered failover for high reliability.

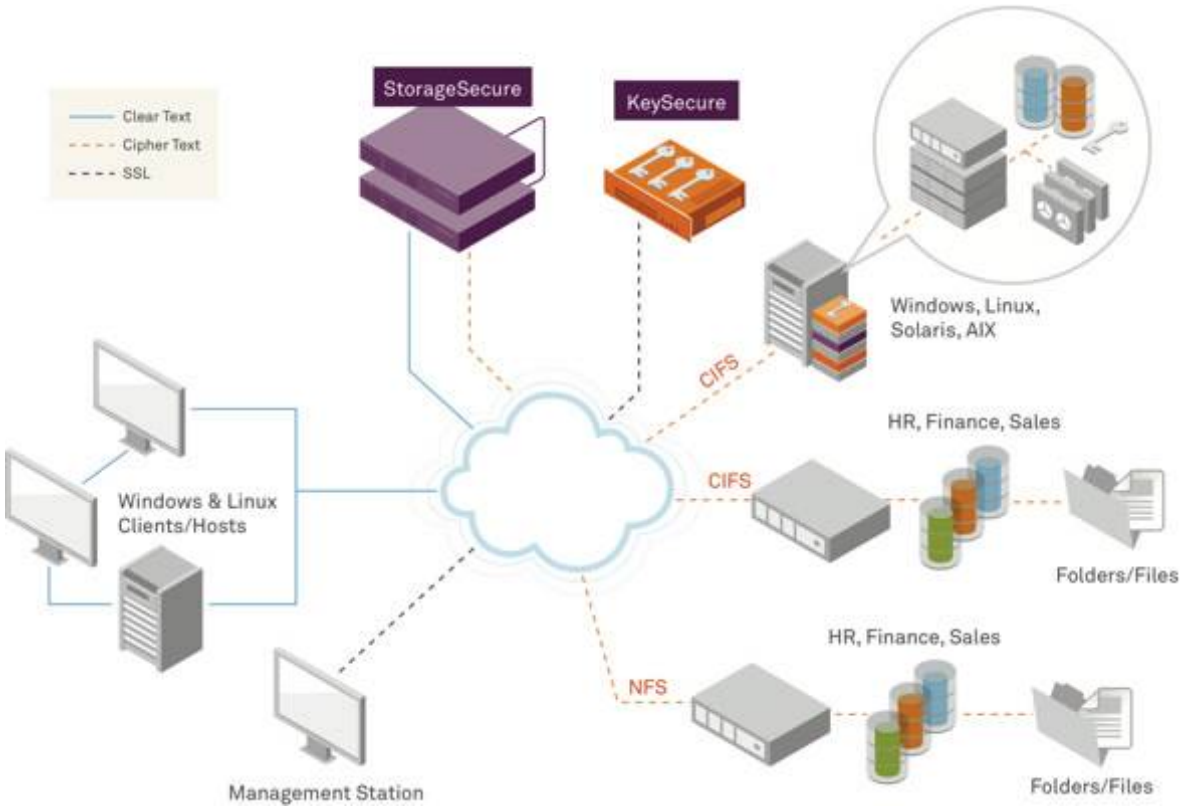

Figure 1) SafeNet StorageSecure and KeySecure provide encryption for NFS and CIFS environments.

Two appliances are currently available:

- SafeNet StorageSecure s220 (GbE network interface)
- SafeNet StorageSecure s280 (10GbE network interface)

These appliances:

- Make sure of data isolation and granular access controls to protected data in shared and virtual environments
- Strengthen existing LDAP, Microsoft® Active Directory®, and NIS controls with an additional layer of access controls
- Protect data for compliance mandates
- Protect offline data in archives from unauthorized access or theft
- Integrate with SafeNet KeySecure for centralized policy and key management

NetApp Storage Encryption

NSE is the NetApp implementation of full-disk encryption (FDE) using self-encrypting drives (SEDs) from leading drive vendors. Because encryption and decryption take place on the drive itself after data is written by Data ONTAP® or before it is read, NSE operates seamlessly with Data ONTAP features such as deduplication and compression. All data on a drive is automatically encrypted, so using NSE is an easy way to make sure that data at rest is protected while maximizing the ROI of your NetApp storage.

The physical drives themselves are tamper proof, and NSE prevents unauthorized access to encrypted data at rest. It prevents someone from removing a drive or shelf of drives and mounting and accessing them elsewhere. In addition, it prevents unauthorized access when drives are returned after a drive failure and simplifies the disposal of drives.

All FDE drives that NetApp sells adhere to the Trusted Computing Group (TCG) AES-256 encryption standard and

are Federal Information Processing Standards (FIPS) 140-2 level 2 validated by the manufacturers, a standard requirement of the public sector. You can find out more about NSE in this recent Tech OnTap® article that explores all of NetApp's drive technologies.

Key Management

Of course, when you encrypt data, you must securely store and manage the encryption keys. One of the things that sets NetApp apart from other storage providers is the fact that it offers a central key management solution, SafeNet KeySecure, so you can easily purchase, integrate, and manage encrypted storage. KeySecure can store and manage encryption keys for NetApp's entire encryption portfolio, including NSE and SafeNet StorageSecure.

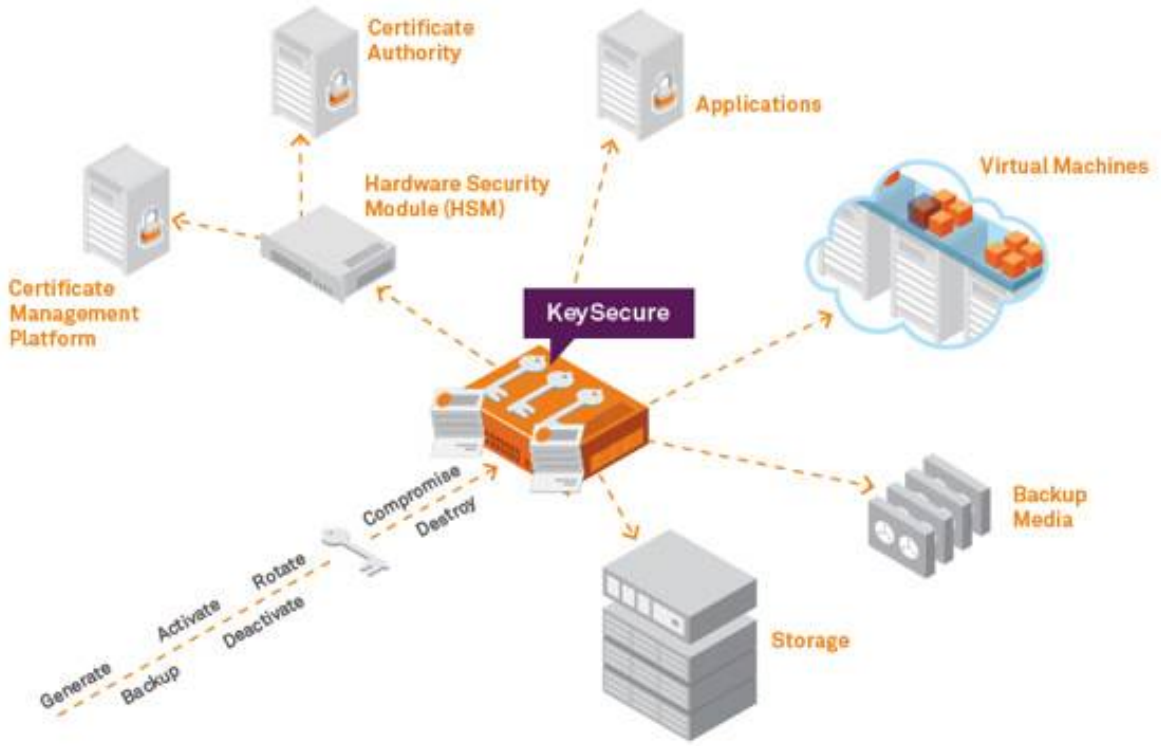

Figure 2) SafeNet KeySecure addresses key security for a wide variety of encryption needs.

KeySecure is built on standard KMIP protocols and can also manage encryption keys for products that aren't in the NetApp portfolio but that might be in your data center. For example, if you're running VMs in your NetApp data center, SafeNet ProtectV enables encryption of VMs, and of course you can use the same KeySecure appliance to manage those keys as well.

Conclusion

Today's adversaries are more skilled and motivated than ever before, and with so much data to manage, organizations have to turn to virtualization, cloud, and storage as a service. Encrypting data in storage environments lets you maintain control of who sees your data, no matter where it's stored, how many copies are made, or who tries to steal it.

SafeNet and NetApp have partnered to better address your security needs. Through this partnership we offer several security solutions:

- NetApp SafeNet StorageSecure Encryption Appliance

- SafeNet KeySecure Key Manager

NetApp FAS systems offer a growing line of self-encrypting drives (SEDs) that use NetApp Storage Encryption (NSE) and the SafeNet KeySecure appliance for data-at-rest encryption.

By Blair Semple, CISSP-ISSEP, Director, Business Development, SafeNet

Blair focuses on information security and, more specifically, storage security. With over 12 years of storage security experience, he is responsible for global outbound communications on the state of the storage security market, emerging standards for storage security, and so on. In addition, Blair works directly with SafeNet and NetApp customers defining the requirements, challenges, and benefits of storage security along with the value that NetApp solutions bring to this environment. Prior to joining SafeNet, Blair was with NetApp for six years in the role of storage security evangelist.

Quick Links

- Tech OnTap Community
- Archive
- User Groups
- PDF
