Executive Summary
The very attributes that make network-attached storage environments invaluable to enterprises—their accessibility, centralization of assets, and flexibility—also make them valuable targets to malicious insiders and external criminals, and susceptible to accidental exposure. This paper details why encryption is vital in NAS environments that house sensitive assets, and offers some key considerations for picking the right NAS encryption platform.

Introduction: Why Protecting NAS Environments is so Critical
Network-attached storage (NAS) represents a critical information repository—and a highly prized target for cyber criminals and malicious internal staff. Following are a few reasons:

• **Numbers of records.** As opposed to Wi-Fi hacks or other tactics that may yield a single sensitive record, the effective breach of a NAS environment could yield hundreds or hundreds of thousands of records. When you consider the estimated cost of a breach is about $214 per record, the stakes are clearly very high.

• **Sensitivity of assets.** NAS environments may house any number of sensitive data assets. In a given organization, the NAS may house personally identifiable information, including employee social security numbers and HR records, customer payment and account information, and patients’ medical records. It could also house unregulated information that could nevertheless be detrimental if breached, such as corporate intellectual property or customer email addresses. This sensitive information can be structured (for example, held within a database) or it can be unstructured (residing in Word documents, PDFs, image files, spreadsheets, and so on).

• **Shared access.** To get the most utilization out of their NAS investments, most organizations will have multiple departments and groups using a given NAS system. Consequently, the data of different departments—each of which may have very different policies, risks, and usage requirements—will reside on a common storage system. Given the networked nature of NAS environments, these systems can typically be accessed by many different systems, users, and administrators. As such, they are vulnerable to external attacks, malicious insiders, compromised systems, and lax policies.

• **Distributed.** The fact that most NAS environments are replicated, both on backups and onto offsite locations for disaster recovery purposes, can increase the risks and exposure of sensitive assets that are stored in that environment.

• **Vague legal protections.** For companies that manage their intellectual property digitally, the blurred legal definitions of illegal theft that have surfaced in a recent case further underscore the fact that companies have to protect the digital assets in their NAS environments, and cannot rely on the threat of arrest and jail time as a deterrent to keep employees from stealing those assets. In the case in question, a Goldman Sachs engineer who stole the source code of a proprietary trading application was found not guilty. The court opinion ruled, that in this case, because software code was stolen rather than “physical goods,” the theft was of “purely intangible property embodied in a purely intangible format.”


**Why Encryption is a Critical Requirement**

**Understanding Threats in NAS Environments**

To understand the nature of the threats to NAS environments, it is helpful to first start with a basic definition of NAS: Networked storage that can be accessed by multiple users, often working with heterogeneous clients that use either the CIFS or NFS file sharing protocols. Because of the very nature of NAS environments, they are susceptible to a range of risks:

• If user devices with NAS access privileges are compromised, the NAS system itself can be compromised.

• If networks connected to the NAS are compromised, the NAS can be compromised.

• The NAS system itself can be breached, whether through direct attacks or access.

• NAS media can be stolen or inadvertently exposed, for example, if media devices are lost or stolen in transit to have repairs done or to be destroyed.

• Rogue administrators within the organization could use their existing privileges to gain access to a NAS system.

By and large, the risks outlined above are not effectively addressed by such security mechanisms as antivirus, firewall, full drive encryption, and IDS. It is only through a combination of granular encryption and access controls that organizations can guard against these types of threats.

**Addressing Compliance Mandates**

For any organization that is compelled to comply with regulatory or industry mandates, the need for encryption is often an explicit, direct requirement. For example, the Payment Card Industry Data Security Standard states, “Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person.”

Ultimately, there are two ways to look at the incentives for complying with these types of mandates, the carrot and the stick. The stick is that failure to comply can result in fines and lost business. The carrot is that by complying with these types of guidelines, organizations can strengthen security and effectively guard against breaches. For example, the “2012 Data Breach Investigations Report” indicated that 96 percent of data theft victims that were subject to PCI DSS had not achieved compliance.

Ensuring Control in Outsourced Environments

For the vendors that serve larger enterprises, these compliance mandates can also have a trickle-down effect as larger enterprises and government agencies are increasingly requiring vendors to comply with their mandates. This is especially critical for enterprises that look to cloud providers and outsource IT or development—situations in which NAS systems may need to be accessed or managed by third parties via the Internet.

Encryption can play an integral role in gaining the control needed to safeguard assets and address policies in outsourced environments. For example, if a NAS environment is made accessible by external parties via the Internet, encryption provides an invaluable layer of security in the event access methods are compromised.

NAS Encryption: Key Activities

As they set out to embark on NAS encryption initiatives, the following are a few of the key efforts security teams should undertake:

- **Assess risks and business drivers.** Both to ensure the ultimate success of an initiative and to get the required buy-in for any investments, security teams should do an in-depth evaluation of the potential threats surrounding assets on NAS systems, and the potential business risks and costs associated with those threats being exploited.

- **Identify sensitive data and all its locations.** While on the surface, this may sound like an obvious and straightforward exercise, in large enterprises, it is neither. Not only do organizations need to understand what assets reside on the NAS, they also need to understand where else those assets reside. Ultimately, one of the most beneficial outcomes of this kind of exercise is that an organization can identify and eliminate areas where sensitive assets are being stored without a legitimate business reason.

- **Do not rely on users to “do the right thing.”** Generally speaking, end users have been proven to be erratic in complying with maintenance policies, such as conducting consistent backups. Consequently, it stands to reason that users should not be relied on to distinguish between files that need to be encrypted and those that do not. Therefore, an encryption solution must be transparent to users, and should not rely on their active involvement in order to meet corporate policies.

- **Establish ownership and required permissions.** For each type of sensitive asset, security teams need to map rights and permissions of various groups, roles, and individuals. This is a vital first step in ensuring access controls and encryption policies support both business and security objectives.

- **Architect encryption points in accordance with business workflows.** Next, it’s important to design the implementation of encryption to align with workflows within the business. This includes evaluating the different options for storage encryption and ensuring they will accommodate business processes.

- **Implement defense in depth.** In order to ensure optimal security, it’s vital to implement encryption as part of a multi-layered, integrated security framework. This includes coordinating encryption with corporate information security policies and access management systems. After deployment, it is imperative to audit access to sensitive data, and also to routinely perform vulnerability testing so any weaknesses or gaps are spotted before they are exploited.

Key Requirements for Effective NAS Encryption Solutions

When assessing NAS encryption alternatives, there are several key characteristics to look for:

**Centralized, Secure Key Management**

Too often, the efforts and tactics required to secure cryptographic keys are not fully understood when security teams first embark on a NAS encryption initiative. Consequently, lack of visibility, control, and security of cryptographic keys represents a significant vulnerability in many organizations today. Following are some essential ways to optimize administrative efficiency and the security of cryptographic keys:

**Hardware-based Key Storage**

In most organizations, servers play a fundamental role in encryption, acting as a central repository for cryptographic keys. As a result, a breach of these systems can compromise the integrity of the entire infrastructure. Too often, general purpose servers are used, which store keys in software, leaving memory unprotected and keys in clear text. Consequently, keys can be exposed by malicious administrators, software exploits, and a host of other threats. For example, when keys are stored in software, an attacker needs only to find a copy of the server’s backup files and can then exploit a number of vulnerabilities.

On the other hand, purpose-built encryption appliances and hardware security modules (HSMs) can digitally sign hardware-based backups and apply physical security mechanisms to keys. Applications communicate with keys stored in the appliance or HSM via a client—but keys never leave the devices. By leveraging these specialized platforms, many organizations can address a significant gap in their defenses. For the highest levels of security, a NIST (National Institute of Standards and Technology) certification, such as FIPS 140-2 Level 3, is required in order to effectively prevent the exposure of cryptographic material.

**Centralize Keys**

When keys are held on disparate, general purpose systems—often on the very systems containing the sensitive data—they are vulnerable to theft and misuse. And the more locations keys reside in, the more pervasive an organization’s risks. In addition, as keys are backed up, if they are, they often are not secured in transit, which leaves them further exposed.

**Centralize Key Administration**

Encryption management is a vital task, and one typically entrusted to small, resource-constrained groups within the security organization. To effectively address their charters, these security teams have to focus on the most pressing security objectives, and find ways to efficiently deploy and manage their security infrastructures.

Administrative efforts, such as key rotation, can help strengthen security; however, this has to happen securely and efficiently. To address these objectives, security teams need to begin moving to a point in which keys are centrally managed across the enterprise, including across heterogeneous NAS platforms, application environments, endpoints, cloud deployments, and more. Following are several benefits of this approach:

- **Decreased exposure of keys.** Centralizing key management offers fundamental advantages in security as it limits the number of locations in which keys reside, minimizing the potential for exposure.

- **Consistent policy enforcement.** Centralized key management makes it practical for administrators to more consistently enforce corporate standards and policies across the organization. For example, an administrator can set user credentials and policies around a specific asset once, and then ensure those policies are effectively employed, whether that data is saved to a database server, NAS environment, or laptop.

- **Streamlined administration.** At the same time, centralized key management also streamlines administration, enabling administrators to make changes and updates once,
and have them propagated across all pertinent areas.

- **Encryption efficiency.** This also represents a more efficient model: As opposed to point encryption, where data on one platform would have to be decrypted and re-encrypted when it is transmitted to another platform. With this approach, a specific asset can be encrypted once and distributed to multiple systems, and only needs to be decrypted when an authorized user needs access to it.

- **Unified auditing and remediation.** Finally, having all keys centralized can also significantly streamline auditing and remediation by housing audit logs that encompass all key-related activities.

Within this context, the Key Management Interoperability Protocol (KMIP) standard, which was ratified in 2010, represents a significant development. The KMIP standard was developed by the Organization for the Advancement of Structured Information Standards (OASIS). KMIP was developed in order to establish a single, comprehensive protocol for standard communication between key management servers and the enterprise-wide cryptographic clients that use these keys. By leveraging technologies that adhere to the KMIP standard, organizations can begin to centralize key management for a number of disparate encryption platforms that may currently be deployed in the enterprise.

**Encryption Platform Deployment**

When implementing encryption in NAS environments, security teams can choose from a broad range of platform types. Following are a few options and considerations:

- **Full disk encryption.** While the simplicity of having a drive that has its own encryption capabilities can sound appealing, the reality is that these alternatives do not give most organizations the kind of control needed to comply with regulations, or prevent employees from accessing sensitive information. For example, if the HR folder and the Finance folder are stored on the same disk or disk array, employees in Finance could have full access to HR files, and vice versa. Full disk encryption ensures that if the drive is physically removed from the data center, no one can access the information. On the other hand, this approach does nothing to protect credit card data, patient information, employee records, or other sensitive information from employees within the organization.

- **Switch-based encryption.** Alternatives that perform encryption within the switch itself can be highly effective. However, this approach is extremely expensive, and, in most cases, requires an extensive infrastructure overhaul to implement.

- **Agent-based encryption.** Many encryption solutions require an agent to be installed on every client that needs to access encrypted data. In larger enterprises, this can result in thousands of clients requiring the installation, administration, and updating of agents, which can pose a number of administrative challenges.

- **Inline encryption.** These encryption alternatives leverage a hardware appliance that is deployed on the network, either inline or connected to a switch, acting as a virtual proxy. The advantage of this approach is that it typically does not require any network changes. Further, it is an approach that can be completely transparent to end users and work with a heterogeneous collection of NAS servers.

Consequently, in a number of organizations, inline encryption alternatives often make the most sense from a security, cost, and administrative perspective.

**Granular Data Isolation and Encryption**

Many alternatives only enable encryption at the volume level. However, it is important to have as much flexibility as possible when it comes to determining which assets will be encrypted. This is important because the more granular control, the more efficient the encryption
deployment. This is true for two key reasons:

- **Performance.** No matter which encryption platform is employed, there's always a computation hit associated with encrypting or decrypting assets. By having granular controls, for example, that enable encryption at the folder level, organizations can ensure that only sensitive assets are being encrypted, and thus minimize the performance cost associated with encryption.

- **Storage efficiency.** Encrypted data cannot be deduplicated or compressed. Consequently, encryption can negate some of the storage efficiencies that NAS platforms deliver. With solutions that enable more granular, folder-level encryption, organizations can encrypt only the folders that contain sensitive data and leave the other folders unencrypted, which helps optimize storage efficiency.

In addition, granular encryption affords higher levels of security, helping ensure that only authorized people can access certain encrypted folders or files. The less granular the encryption, the greater the risk of private data accidentally being exposed to someone without the proper rights. (See the section on full disk encryption above.)

To maximize control and efficiency, encryption platforms should offer the flexibility to assign different encryption keys and policies to an individual share, folder, or file. This is vital for enabling security administrators to provide segregation of encrypted storage between users, groups, and, in the case of service providers, clients and other entities.

**High Availability**

When encryption is employed, the importance of having encryption and decryption capabilities continuously available cannot be overstated. Quite simply, if the encryption platform goes down, users cannot access encrypted data, which is often comprised of some of the organization's most vital resources. Consequently, it's important to leverage encryption platforms that ensure continuous availability of critical cryptographic processing and data. Toward that end, look for encryption offerings that provide the following capabilities:

- **Clustering.** Look for encryption platforms that offer capabilities for clustering multiple appliances, which helps organizations ensure vital encryption capabilities and encrypted data are always available when needed. With these capabilities, all keys, policies, and configuration information can be shared among appliances within a cluster, so that if a primary appliance goes offline, a secondary appliance in the cluster can take on the required workload.

- **High throughput and minimal latency.** It is important to leverage an encryption platform that is based on a dedicated, robust security appliance. This appliance should feature specialized hardware and parallel processing in order to deliver the scalability and responsiveness required. Further, look for solutions that offer support for 1 and 10 gigabit Ethernet networks, ensuring organizations can meet both their near- and long-term security and throughput needs.

- **Support for Disaster Recovery.** The ability to instantaneously access the necessary encryption keys at a remote site in order to access critical data after a disaster is vital. This means the encryption keys must be replicated to a remote location as soon as they are created, rather than as part of a daily backup cycle.

With the above capabilities, organizations can enjoy the security benefits of encryption, while minimizing the implications encryption can have on network reliability and performance.

**Granular, Efficient Access Controls**

The extent to which an encryption platform integrates with and supports existing access control infrastructures and policies is a vital determinant to the ultimate success of the encryption deployment. Following are a few of the features to look for in supporting this
objective:

- **Support for two-factor authentication.** To maximize the security of an encryption deployment, it is vital to leverage encryption platforms that support two-factor authentication. This can be a vital line of defense, for example, if a client with NAS access is compromised.

- **Integration with authentication frameworks.** Depending on the specific objectives and infrastructures of a given organization, it can be highly advantageous if a security platform can be configured to leverage an existing authentication framework, such as Active Directory, LDAP, or NIS. This can help security teams more seamlessly leverage existing policies and administrative efforts within the domain of access to encrypted data, which helps ensure administrative efficiency and consistent policy adherence.

- **Independent access control lists.** In addition, it may be important to consider encryption platforms that can be configured to have their own access control lists—whether run independently or to augment those of the existing authentication framework. By leveraging a platform that can work independent of any existing authorization scheme, organizations can implement safeguards that, for example, could offer protection against a rogue Active Directory administrator, preventing them from using their administrative privileges to decrypt sensitive data that they are not authorized to access.

**Conclusion**

Done correctly, deploying encryption in NAS environments can boost security and strengthen compliance. Done improperly, it can be a costly exercise that offers limited security and hampers business productivity. By leveraging the guidelines outlined above—including deploying an encryption platform that centralizes cryptographic keys, delivers high availability, offers granular encryption and access controls, and more—organizations can maximize the chances of success with their NAS encryption initiatives.

**About SafeNet Storage Encryption Solutions**

SafeNet StorageSecure is a network encryption appliance that offers optimal protection of data at rest in physical, virtual, and cloud-based storage environments. Due to its deployment model, StorageSecure facilitates fast and easy deployments, and streamlines ongoing administration. StorageSecure ensures the confidentiality of sensitive data on NAS file servers, encrypting information based on defined business policies, while minimizing encryption’s impact on ongoing operations.

**About SafeNet**

Founded in 1983, SafeNet, Inc. is one of the largest information security companies in the world, and is trusted to protect the most sensitive data for market-leading organizations around the globe. SafeNet’s data-centric approach focuses on the protection of high-value information throughout its lifecycle, from the data center to the cloud. More than 25,000 customers across commercial enterprises and government agencies trust SafeNet to protect and control access to sensitive data, manage risk, ensure compliance, and secure virtual and cloud environments.