WHITE PAPER

Is Onboard Key Storage the Right Corporate Strategy?

Introduction

There has been a recent resurgence in Onboard Key Storage (OKS) offerings from storage vendors such as Dell EMC, Quantum, and most recently NetApp's ONTAP/NSE offering. The key market drivers for this reappearance are focused on several factors, including:

Price: The storage market is evolving in order to find new areas for growth. Most traditional storage vendors are placing more of their marketing efforts towards targeting small to medium-sized businesses, which typically have less budget to spend than larger enterprise organizations. This has driven a demand to reduce price points for onboard key storage solutions, and ensure that any additional functionality, such as key management, also fits within these tighter budget constraints.

Product: To address these pricing concerns, storage vendors need to provide key storage offerings that fit within the new lower price point expectations. One way that storage vendors are looking to address this, is by offering a built-in key management solution. While there certainly are scenarios where a built-in key management solution will appear to suffice in meeting an organizations security and compliance requirements, they must also consider what their 'bigger picture' looks like when it comes to meeting these requirements. This paper will discuss some of the items that an organization should factor into their bigger picture when it comes to making the right choice for a key management solution that meets their needs.

What's "Good Enough" When It Comes to Security and Compliance

The definition of what's appropriate, or 'good enough' for security and compliance is different for every organization. Many factors influence this, from internal IT standards, to industry compliance standards that are related to that company's market such as HIPAA or PCI-DSS, and those mandated by governments at various levels including GDPR. OKS solutions allow companies to use a built-in solution for that storage device. This provides a one-stop shop to resolve storage data encryption, as well as provides basic key availability services on that device - included in one price point. For some companies, this meets the definition of 'good enough'.

For other organizations, their solution cannot be that simple for many reasons, including some of the typical issues that can occur:

- If a company owns multiple storage devices to host their corporate data (or have inherited the storage devices due to a merger or an acquisition of other companies), the OKS model implies that each storage platform would come with different key management offerings. This creates issues with feature parity, as well as making sure each key storage system provides the same key management capabilities. Furthermore, when an enterprise has multiple, different systems that provide the same type of capabilities, but with different features and user interfaces, it is much more prone to user error which can result in data compromise or even loss of data.
- Depending on industry governance, there may be reasons that any keys and data they encrypt must be stored separately. Section 3.5 of the PCI-DSS standard states: "Protect any keys used for encryption of cardholder data from disclosure and misuse." Most storage vendors will state that internal or onboard key management systems protect against unauthorized access to physical storage devices—but not entire storage systems. The keys are embedded and stored within the product itself. If you choose to use an onboard key management system, you should consider that keys, and therefore your data, will be accessible if the entire storage system is compromised.

Take Security and Compliance to Another Level

For companies that are mandated to support items such as FIPS 140-2 compliance (to stop use of encryption algorithms deemed unsafe and tamper proofing of appliances), onboard key storage systems may provide FIPS 140-2 Level 1. This ensures the organization that key algorithms used by the appliance are deemed safe, and comply with FIPS. Achieving FIPS certification can be a lengthy and involved process, so not all storage vendors will certify their onboard key management.

For those that require more than just the disabling of unsafe encryption key algorithms, FIPS Level 2 (storing keys in tamper proof evident hardware) or Level 3 (tamper resistant key storage) external key managers, can help provide that level of security.

Going beyond just the disabling of unsafe encryption key algorithms, higher levels of FIPS will have additional security requirements. For example: Level 2 (storing keys in tamper proof evident hardware), or Level 3 (tamper resistant key storage). External key managers can help provide that level of security.

A well designed external key manager can be configured to meet Level 1 compliance, restricting use of unsafe algorithms, as well as be configured to provide higher levels of assurance. This provides organizations with a future proof system in case their compliance standards change. Combined with the added flexibility of having a key manager that can operate on-premises or in a remote datacenter, as a physical appliance, or virtual appliance (running on a private or public cloud), provides companies with options to meet their budget constraints without sacrificing security.

Key Lifecycle Management

Encryption key management should incorporate some level of centralized policy and control. It's not as simple as creating the key, encrypting the data and forgetting about it, a customer should also be able to perform actions on keys such as:

- Key generation
- Key retirement
- Determining the activation or de-activation of the key
- Key rotation to ensure the key content is updated periodically or as needed
- Destruction (when required)

All of these functions should be part of a company's key lifecycle management strategy.

In the case of onboard key storage systems, assuming they have these capabilities, most of the key management is done through a command line interface. Depending on the scope of key management requirements, a true management console providing a visual interface to the key vault greatly simplifies the required key management.

Deployment Options

When looking at their IT infrastructure, many organizations are being faced with the decision to either maintain various applications (including key management), onsite, or in a remote datacenter and move it to the cloud.

In reality, that choice is based on several factors. For key management, organizations will want to ensure that their solution will function in any of these environments to future-proof their investment. With onboard key storage, companies will not have that flexibility in the deployment – it will tie to the storage platform wherever it is installed. With an external key manager, companies have the ability to manage and store their encryption keys, consistently regardless of the environment.

Audit Trail

To help meet corporate and industry compliance requirements, key management systems can provide signed, validated information on key management, as well as key consumption – detailing who accessed the key, the event time, and the success or failure of the operation.
In addition, alert mechanisms such as SNMP Traps can notify staff if any issues arise with the key management appliance or other appliances communicating with the key manager.

One of the primary benefits of an external key management system, is its ability to help companies streamline their audit reporting. Trying to prove to an external compliance auditor that the keys are secure, protected, and have strong access controls on them, would be much more difficult and costly to do with onboard key storage, especially without consistency between vendors. This would also result in all storage systems to be audited individually.

Support Your Complete Ecosystem

Sometimes, it's difficult to envision how much effort is involved when it comes to managing your sensitive data and where it exists. Databases, CRM/ERP systems, various commercial and in-house applications are among the few places where the proper management of sensitive data needs to be considered. Chances are, most companies have a storage system that will support a portion of these data repositories – so the OKS can help protect this information.

Where there are more dispersed data repositories (as well as different security concerns among lines of business consuming these repositories), a stand-alone key manager helps bring all this disparate effort under one umbrella from a policy management viewpoint. A stand-alone, external key manager that includes technology standards such as KMIP (Key Management Interoperability Protocol), helps provide a consistent interface to applications and appliances interfacing with your external key management system.
Take for example the process of running a system back-up. If keys are residing in the same place as the data, it is possible for a system back-up to contain both the data and

keys. If a tape back-up goes missing, it's possible that the data could then be lost. Loss of a key equals the loss of your data. Having all the keys in one central storage platform that can easily and automatically be backed-up, is much simpler operationally, less prone to error or missed keys, and is more secure.

Separation of Duties

External key management systems have the ability to define permissions for the key administrators, as well as the key consumers. A common example of this is the ability to allow a key administrator to create a key for encrypt/decrypt purposes, but deny the administrator ability to use that key by utilizing LDAP or AD user attributes. Major compliance requirements such as HIPAA, GDPR along with others, require this separation of duties to ensure appropriate data access. Typically, OKS systems will not have this level of granularity in administrative roles – the storage administrator is also the encryption key administrator.

Conclusion

With a variety of OKS offerings available on the market, it's important for companies to examine what their 'big picture' looks like when it comes to making the right choice for a key management solution that meets the needs of their organization. The main question companies should ask themselves is: Is onboard key storage a 'good enough' solution, or is an external key management system something that should be deployed?

While putting a solution in place that has basic onboard key storage capability is a step in the right direction for some companies, they should be considering an external key management solution, which could help take their organizations security and compliance to another level.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com

Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free