Hyperflex Encryption

Contents

Abstract

Cisco HyperFlex™ offers a range of encryption options, including HyperFlex-native software encryption (HX SWE), hardware-based data-at-rest encryption (DARE) with self-encrypting drives, and support for third-party encryption with vendor-supplied key managers. This brief discusses each of these options, with an emphasis on HyperFlex-native software-based encryption and its storage-saving advantages over other approaches.

Introduction

Cisco HyperFlex™ product components are developed, integrated, and tested using the Cisco Secure Development Lifecycle (CSDL). Secure product development and deployment has several components, ranging from inherent design and development practices, to testing implementation, to, finally, a set of recommendations for deployments that maximize the security of the system.

Various encryption capabilities have been developed with these guidelines in place. These include Self-Encryption Drives (SEDs) and Cisco HyperFlex software-based encryption (HyperFlex SWE), which is a native feature of the Cisco HyperFlex HX Data Platform (HXDP). Both are data-at-rest (DARE) implementations. Cisco has also qualified various key-management solutions using VM-level encryption from third-party partners such as Gemalto and Vormetric (both parts of Thales, as of this writing) for SED-based encrypted clusters. These various key managers are only for SED-based systems. Cisco® software encryption solutions use the Cisco Intersight™ integrated key manager.

SED-based encryption for data-at-rest (DARE) has been a long-standing HyperFlex feature. HyperFlex SWE is a native part of HXDP and is available as of Release 5.0.1(b). Its development and release have followed these rigorous guidelines, and it is ready for tier-1 secure deployments. It offers all the benefits of hardware-agnostic, strong encryption and cloud- based key management while retaining the storage optimizations and capacity savings for which HyperFlex is known.

DARE and deployment challenges

Data-at-rest encryption (DARE)

Data can either be encrypted when it is written to media (persistent tier or caching tier), at which point it is “at rest,” or it can be encrypted on the wire or “in flight” during data transfers between two or more systems. Cisco HyperFlex provides data-at-rest encryption by SED or by software mechanism native within the HX Data Platform filesystem; HyperFlex systems are functionally storage devices with all relevant services rolled into the appliance (compute, memory, and network). Encrypted communication between HyperFlex clusters, for example with backup or replication, is the purview of the intervening network devices and solved using IPSec, VPN, or similar technologies.

Data-at-rest encryption can take place at any of several points in the write I/O process and on various portions of the written data, including the entire content or subsets therein. The types of DARE you might encounter are:

- Application-level
  - Encryption occurs within the application before data is transmitted or stored.
  - Encrypted content in this scenario can have fine-grained boundaries.
    - Example: individual fields in a database

- Database-level
  - Encryption occurs on a subset (tables or columns) or the entire database.
  - Utilizes transparent data encryption from database vendors before data is stored
- File-level
  - Encryption occurs at a file or volume level by agents of the operating system intercepting I/O and applying encryption policies.
- Disk-level
  - Full disk encryption or Self-Encrypting Drives (SEDs) enables encryption in hardware.
  - Encryption occurs at the drive-controller level when data is written to disk and decrypted when data is read from disk.

Cisco HyperFlex–native software encryption naturally takes place at the file level due to integration with the hypervisor. This allows the encryption package within HXDP to take full advantage of the storage optimizations that occur during ingesting and destaging to persistent storage, namely compression and deduplication, respectively.

The challenges and mechanics of deploying HyperFlex encryption

Deploying encryption in practice can pose several challenges:

- Ease of use
- Key management
- Performance overhead
- SED costs
- Storage media type and drive capacities available as SEDs

In other systems, setting up the encryption option for DARE can often be daunting. Cisco HyperFlex, however, makes configuration of DARE using SEDs or HyperFlex SWE a simple operation.

Enabling SEDs is a quick operation using the Encryption Wizard in HX Connect, the HTML 5–based UI for the cluster. SEDs require an existing key-management infrastructure from any of the supported vendors, such as Vormetric, Gemalto, and Entrust, to enable the exchange and secure storage of the key-encryption key (KEK) for the drives. Alternatively, a local key-management option is also available where the KEK is stored by the Cisco UCS® fabric interconnects.

SEDs are specialized hardware and may incur a cost premium over regular drives. They may also be limited in capacity relative to non-SEDs. SEDs, however, have near zero performance penalty for encryption operations because these are performed in hardware and do not consume parent CPU resources.

HyperFlex SWE is enabled using Cisco Intersight, Cisco's hybrid cloud operations platform, and is available on all Intersight form factors: software-as-a-service, connected virtual appliance, and private virtual appliance. Regardless of whether a cluster is deployed by Intersight, or imported or claimed in Intersight after deployment, HyperFlex SWE is enabled on the cluster with a simple one-line command after downloading the package. A few clicks under the cluster's "Operate" tab will activate the ability to create encrypted datastores. Key management for SWE takes place in Intersight and is transparent to the end user. The SWE option truly demonstrates "ease of use."

The figure below shows a 2-node edge cluster being claimed in Intersight and using the cluster's device connector (DC) to interface with the Intersight Key Manager.

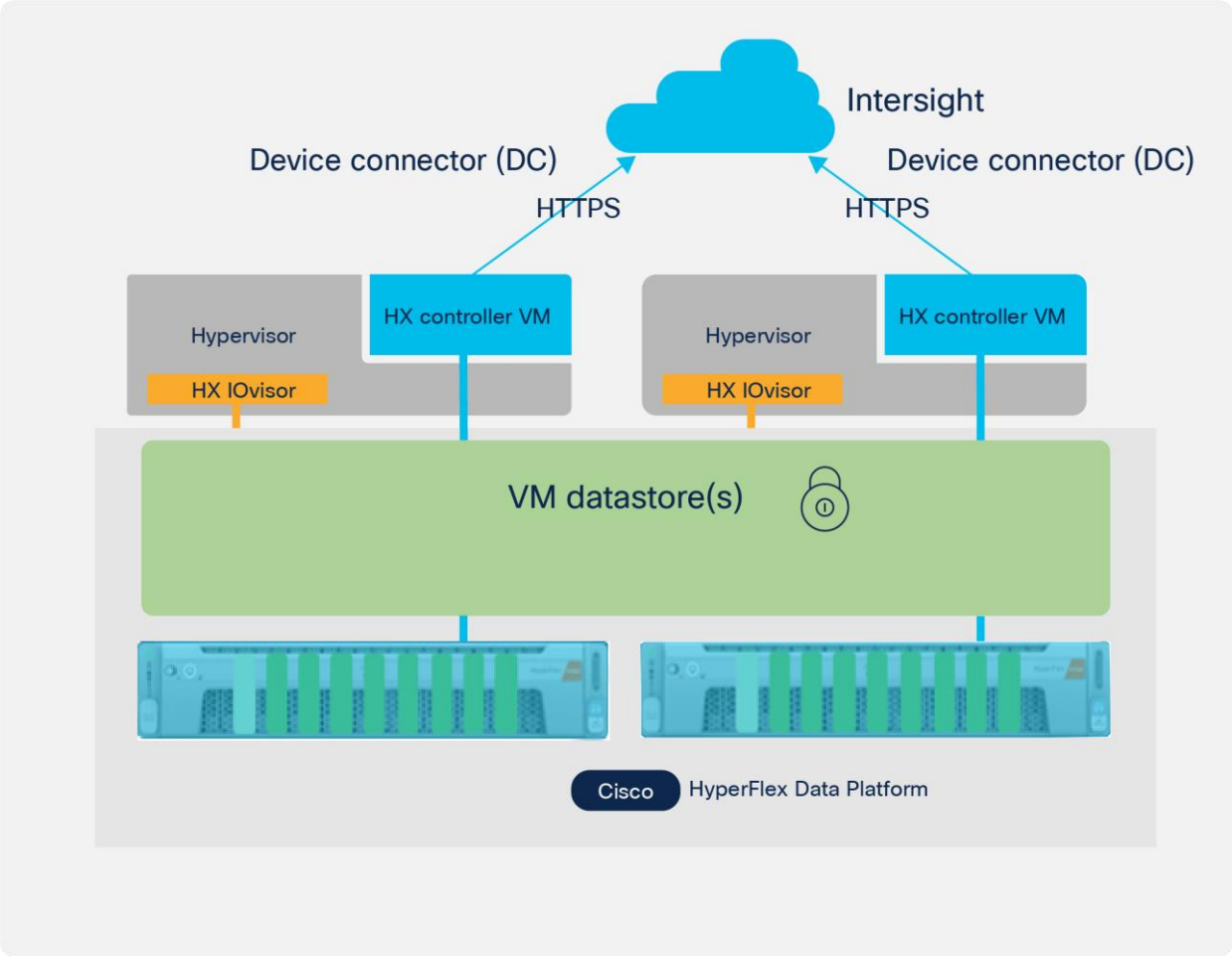

Figure 1.
Secure key exchange with Intersight and 2-node edge cluster through the device connector.

- Controller VMs request and receive keys from the Intersight Key Manager through the Device Connector (DC).
- This is known as the "Key Encryption Key" (KEK).
- The KEK is used to encrypt the Data Encryption Key (DEK).
- The DEK is used to encrypt user data.

Cisco HyperFlex systems using SWE are drive-agnostic. They can therefore take full advantage of the range of qualified drive capacities and drive technologies (for example, all-NVMe, all-flash, hybrid-SFF, and LFF). Since SWE takes place in the HyperFlex filesystem stack, there is a small performance impact due to additional CPU utilization in the HyperFlex controller VMs, on the order of 5 to 10 percent, depending on the workload. If your use case is CPU-bound by the controller VMs for performance, you can easily mitigate the issue using HyperFlex "boost mode" whereby additional vCPUs can be assigned to the control VMs.

SWE is supported by the HyperFlex data center (with or without fabric interconnects) and HyperFlex edge cluster configurations. To enable SWE, each HyperFlex converged node system in the cluster must be licensed with either HX Data Platform data center or edge Premier, and with Intersight Essentials (or a higher tier license). In addition, because data-at-rest encryption is an export-controlled commodity, a special, zero-dollar "K9" software PID (HXDP-SW-PKG-SE-K9=) is also required for each converged node in the cluster for which SWE is to be enabled. For more information regarding licensing, refer to the Cisco HyperFlex Software Licensing and Ordering Guide.

Why Cisco for security and HyperFlex SWE

HyperFlex SWE uses industry-standard strong encryption algorithms and is compliant with U.S. Federal certification requirements. It also takes advantage of Cisco HyperFlex's unique features and cloud technologies:

- Utilizes FIPS 140-2 compliant 256-bit AES-GCM inline encryption
- Leverages AES NI acceleration
- HXDP boost-mode compatible
- Encrypts data end-to-end: encrypted at rest (caching and persistent tier) and on the wire during intra-cluster replication (that is, replication factor)
- Manages keys natively with Intersight Key Manager
- Supports encrypted and unencrypted datastores coexisting in the same cluster
- Supports standard data center and edge clusters
- Supports all-NVMe, all-flash, and hybrid drive systems
- Supports HyperFlex inline compression and deduplication optimizations
- Supports KEK rekey
- Supports secure drive erase

HyperFlex Data Platform Software Encryption affords the following additional advantages by virtue of Intersight cloud-based key management.

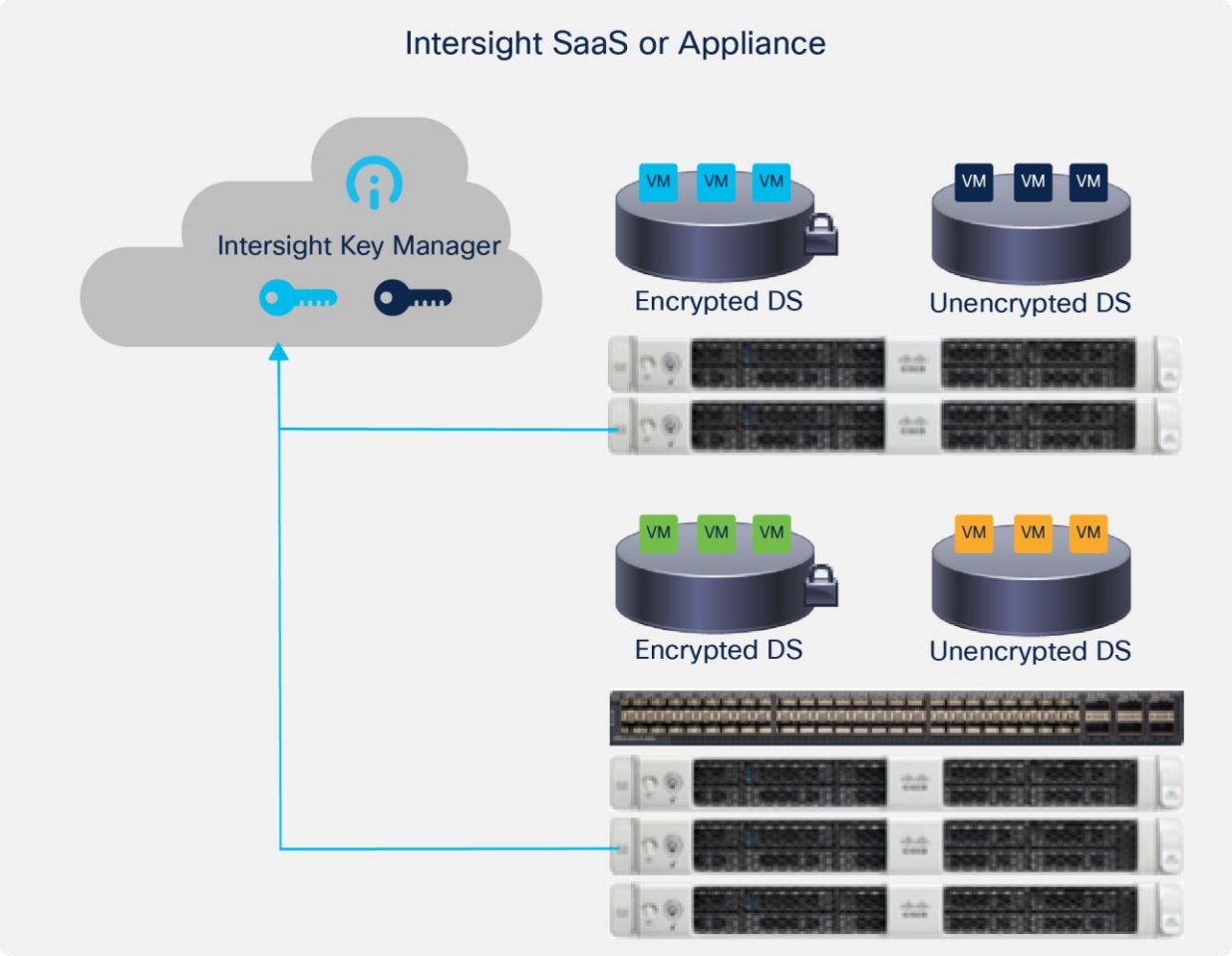

Figure 2.
Standard cluster key exchange with Intersight Key Manager.

- Protects confidentiality of data at rest from theft of storage media
  - Theft of drives, servers, even clusters
    - Simply unclaim the cluster in Intersight. It cannot be reclaimed and you cannot regain access to the KEK stored in Intersight without your original passphrase.
  - Drives disposed without adequate sanitization
    - Unreadable without access to the Key Encryption Key (KEK), which only the HyperFlex system can access from Intersight

A distinguishing feature of HyperFlex SWE is its ability to work with HyperFlex storage optimizations that have been available from day 1. Using post-process encryption such as transparent clients on guest VMs or application-level encryption cannot afford the advantages that HyperFlex SWE offers in this regard, because they take place once data is written to disk. Inline encryption in the write I/O path offers all of the HXDP storage optimizations that are otherwise present in unencrypted, or SED-based deployments.

- In most cases, for a block of data, encryption occurs once.
  - An exception is partial writes.
- Data is stored encrypted in the write log.
- Data is stored encrypted in the persistent tier.
- Data is already encrypted before redundant replication (RF) occurs.

While encryption is extremely important for an overall excellent security posture, it is not a catch-all. Encryption does not protect against direct breaches of the HyperFlex controller VMs or for exploits that occur upstream of the storage stack, for example, in the hypervisor, guest VMs, or VM-based applications. Protection of these software assets are a normal part of regular due diligence and are mitigated by the timely patching and hardening of these components.

SED: general information overview

SEDs

A cluster is designated as SED-capable or not at installation based on whether or not the cluster contains SED-capable drives. After installation, this designation cannot be altered. For a cluster that is SED capable, encryption can then be enabled or disabled at will. You are free to move between the two states whenever you want. The components for an encrypted cluster consist of the SED-capable HX nodes with the Cisco Unified Computing System Manager (UCSM) and the key management infrastructure.

SEDs provide native data-at-rest encryption, typically using AES 256. Some qualified disks are FIPS 140-2 Level-2 validated components for data-at-rest encryption. The hardware encryption is built-in, thereby incurring no deployment overhead. The performance is comparable to that of a non-SED system and is transparent to data-optimization functions (dedupe, compression).

Several encryption keys are associated with a SED implementation:

- Media (disk) encryption key – data is always stored in encrypted form.
- Key encryption key secures the media encryption key.

SEDs provide a mechanism for secure erase, ensuring security during decommission.

SED key management

Configuring SED-encryption services supports both local and remote key configurations. If you are not using local keys, then you need to configure a KMIP server. KMIP server key handling is performed through encryption partners (for example, Thales Vormetric, Gemalto SafenNet, Entrust). The server specifics are entered using the encryption workflow in HX Connect.

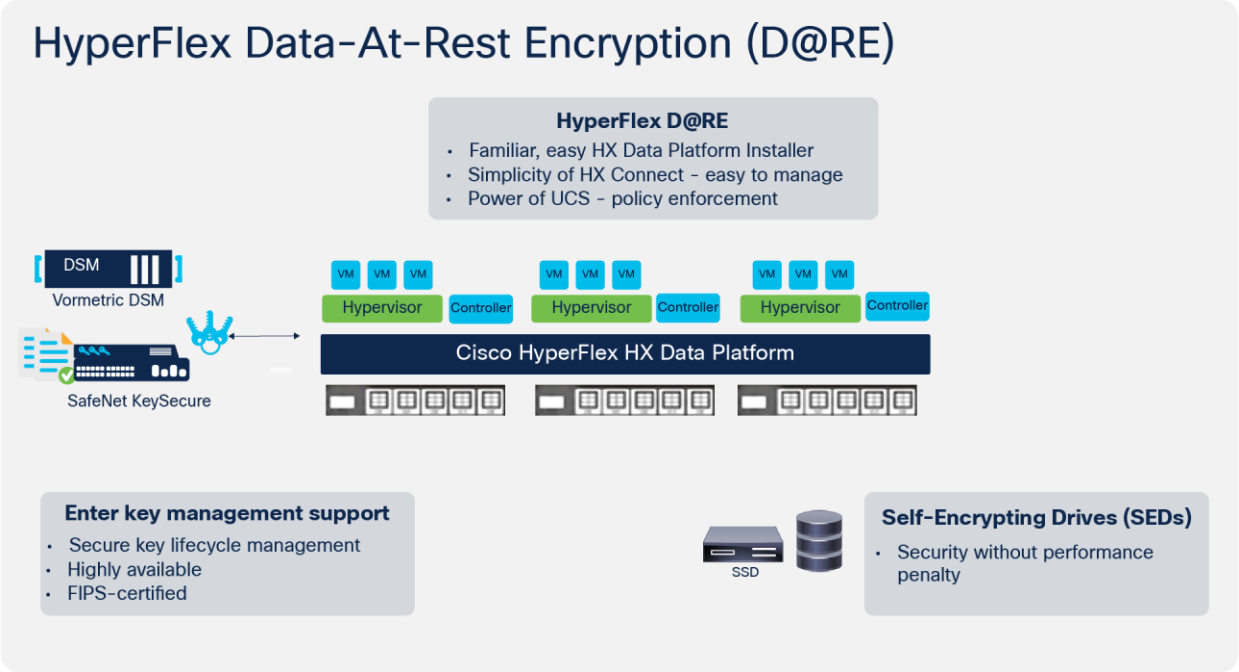

Figure 3.
SED-based cluster using third-party key management.

Third-party encryption support

Cisco HyperFlex systems are KMIP 1.1 compliant. HyperFlex supports several key- management-server vendors. Recent industry consolidations have seen vendors such as Thales Vormetric (DSM), Gemalto (KeySecure), and HyTrust (KeyControl) subsumed by Entrust. Entrust's KeyControl (formerly HyTrust) and any server vendor that supports KMIP 1.1 should function as expected, but qualifications for newer vendors are always under way.

VMCrypt from VMware is also supported as a hypervisor storage policy. VMCrypt requires an external key manager (see the vendors above). This is a VM-level encryption scheme and does not offer the storage optimizations that HyperFlex native SWE can provide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C11-3053402-00 07/22