The Cisco HyperFlex Security Advantage

Secure your data at rest

- Encrypt data at rest with self-encrypting drives.
- Integrate with enterprise key management software to manage keys.
- Manage your entire security lifecycle with the Cisco HyperFlex™ Connect interface.

Comply with regulations

- Encrypting data at rest provides confidentiality of data to help you achieve compliance with data privacy regulations.

Use a secure platform

- We continuously perform vulnerability assessments to help protect against threats.
- We harden and maintain every component as part of our product development process.

Loss of sensitive data can pose significant business risk. We help you maintain the privacy and integrity of your data.

Easily secure your data at rest on a Cisco HyperFlex™ cluster with data-at-rest encryption using a simple interface. Our policy-based approach to security provides you with the assurance of uniform, consistent, compliant, and secure encryption management and deployment across your cluster.

As you move your enterprise-critical applications to Cisco HyperFlex systems, we are ready with a holistic approach that integrates security deep into our platform. Data-at-rest encryption helps you comply with regulations that require the use of security best practices. We also provide you with a hardened platform based on a secure development lifecycle that protects against vulnerabilities and threats. All these features together make Cisco HyperFlex systems a choice you can trust for your most important business applications.

Secure your data at rest

Data-at-rest security for Cisco HyperFlex nodes integrates the following components to protect your data with high-grade security:

- Self-encrypting drives (SEDs) provide encryption without performance penalty.
- Enterprise key management protects encryption keys.
- The Cisco HyperFlex Connect interface makes configuring and managing data security easy.

High-grade security components

We begin by integrating self-encrypting hard-disk drives (HDDs) and solid-state disk (SSD) drives into each node. With hardware-accelerated cryptographic modules in the data stream, performance impact is minimal as data is transferred to and from the drives. SEDs are supported for both hybrid (HDD and SSD drive) nodes and all-flash nodes.

© 2017 Cisco and/or its affiliates. All rights reserved.

Your data is not secure if you leave the keys under the mat. That is why we have integrated with enterprise key management systems. Your disk encryption keys are kept secure with industry-leading key management solutions, including:

- Gemalto SafeNet KeySecure
- Thales Vormetric Data Security Manager

Key management processes using these solutions are integrated into our platform for secure and simplified encryption. The solutions also provide reporting, compliance tracking, and auditing capabilities. The Cisco HyperFlex system is compliant with Key Management Interoperability Protocol (KMIP) 1.1, so other compatible key management systems can easily be qualified in the future.

You also can use a local key or passphrase using an option built into Cisco UCS® Manager.

Simplified management

Whether you use enterprise key management or local keys, the workflow is controlled entirely through the Cisco HyperFlex Connect interface (Figure 1). This intuitive HTML 5 interface makes the process of enabling, configuring, rekeying, and securely erasing data on the SEDs in your cluster straightforward.

The workflow establishes a certificate-based chain of trust between the Cisco HyperFlex

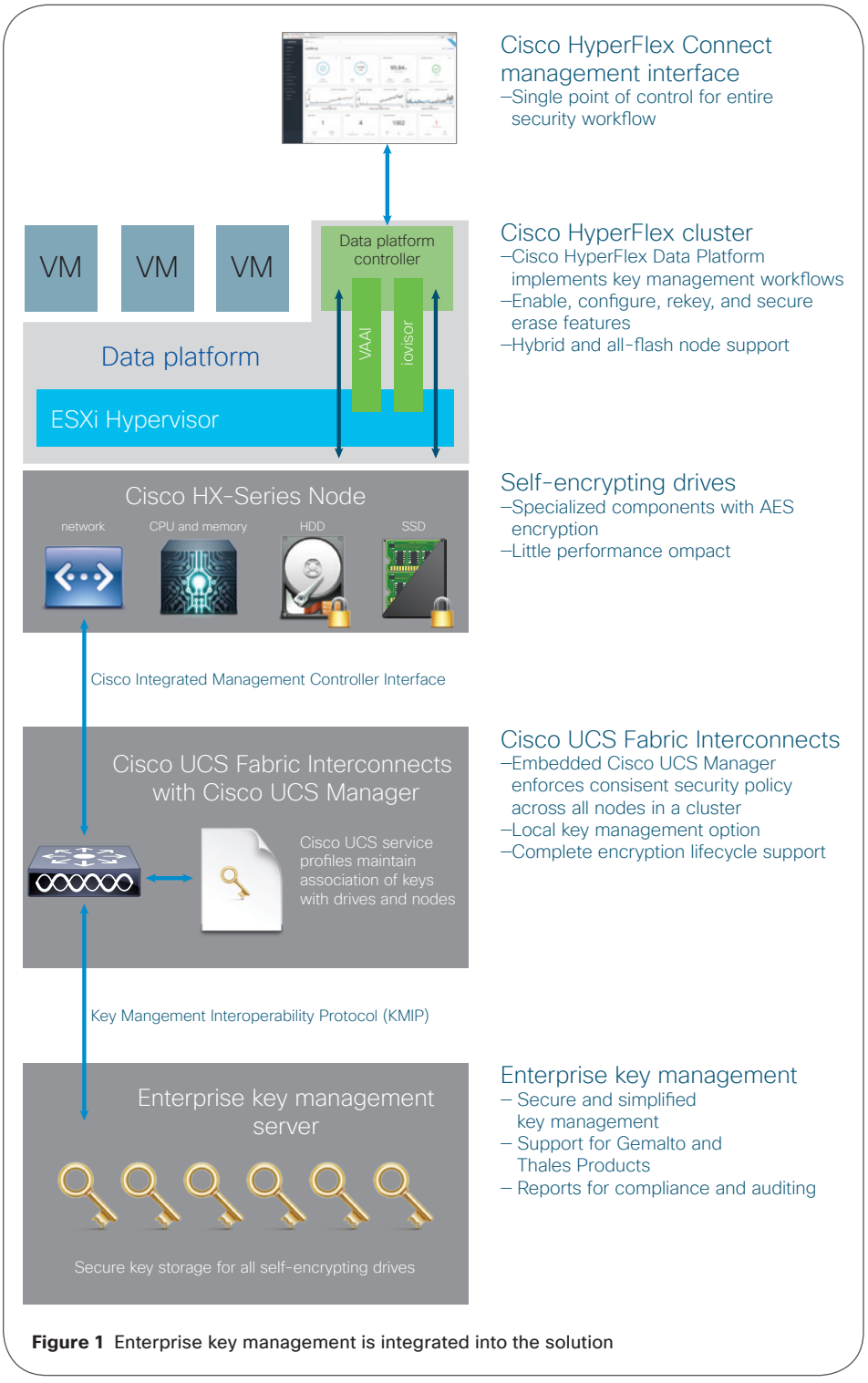

Figure 1 Enterprise key management is integrated into the solution

© 2017 Cisco and/or its affiliates. All rights reserved.

Secure your data at rest

- Encrypt data at rest with self-encrypting drives.
- Integrate with enterprise key management software to manage keys.
- Manage your entire security lifecycle with the Cisco HyperFlex Connect interface.

HX Data Platform and the key management server. Using this connection, the nodes can securely transfer the encryption keys necessary to unlock the drives.

Operational security

Our approach to security establishes and enforces policies so that encryption and key management are deployed uniformly and consistently across the cluster. This approach eliminates worries about inconsistent security practices that could compromise security. Because policy implementation is automated, configuration is repeatable across the many nodes and SEDs that populate a cluster.

Cisco UCS Manager uses Cisco Unified Computing System™ (Cisco UCS) service profiles to specify the interaction among security policies, the data platform, and the key management software. With these profiles plus the more than 100 identity, configuration, and connectivity variables that Cisco UCS Manager sets for each server, you are assured of a consistent and compliant deployment across every node. With automated configuration and deployment, the process of expanding your cluster with new nodes is simple and straightforward.

Comply with regulations

Data privacy

Privacy is essential for regulatory compliance—and encryption enables data privacy. Cisco HyperFlex systems with data-at-rest encryption help you achieve compliance for many industry-specific regulations. There are many such regulations, and these are some examples:

- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI-DSS)
- Federal Information Security Management Act (FISMA)
- General Data Protection Regulation (GDPR)
- Sarbanes-Oxley Act

The Cisco HyperFlex Connect management interface enables you to easily configure your data-at-rest encryption and manage the entire security lifecycle. Cisco HyperFlex Connect uses the power of Cisco UCS service profiles to dictate the configuration and security characteristics of each node. This feature reduces the risk of configuration drift, which can cause downtime and introduce security vulnerabilities.

Certifications

For data-at-rest security, Cisco HyperFlex systems use

© 2017 Cisco and/or its affiliates. All rights reserved.

Comply with regulations

- Encrypting data at rest helps provides confidentiality of data to help you achieve compliance with data privacy regulations.

self-encrypting drives and integrate with enterprise key management systems that are validated for FIPS 140-2.

Cisco HyperFlex systems are also undergoing Common Criteria certification for Evaluation Assurance Level (EAL) 2 for Information Technology Security Evaluation Criteria (ITSEC).

Cisco has extensive security expertise across the company, and our Global Certification and Common Security Modules team has developed an innovative approach to FIPS certification. The group has developed a cryptographic module that is already FIPS validated and can be embedded in a range of trusted Cisco® products. The compliance process verifies that the product has implemented cryptography according to standards. Cisco HyperFlex Systems use of this module has undergone a compliance review.

Use a secure platform

IT organizations trust Cisco security because we have made it an integrated part of the software lifecycle. Security is built into products from the beginning and is continually improved and hardened through the Cisco Secure Development Lifecycle implemented by our software development teams.

Platform hardening

All the software that is integrated into Cisco HyperFlex systems has undergone substantial hardening: Cisco UCS Manager, Cisco HyperFlex HX Data Platform, and the hypervisor itself.

We have used the Secure Technical Implementation Guide (STIG) for hardening and applied recommendations from certification standards. For example the system has been validated implementing Cisco HyperFlex best practices and several VMware ESX Server security recommendations.

Ongoing vulnerability assessment

To keep our hardened systems secure over time, we implement regular vulnerability assessment using Nessus scans with frequently updated vulnerability databases.

Management security

The management of your Cisco HyperFlex system has been secured from the beginning. Using the Cisco HyperFlex Connect interface, you can manage all aspects of your cluster operations, including the end-to-end lifecycle of data-at-rest encryption. Cluster management is secured with your enterprise authentication and authorization mechanisms integrated with vSphere single sign-on (SSO), including Microsoft Active Directory and Lightweight Directory Access Protocol (LDAP).

© 2017 Cisco and/or its affiliates. All rights reserved.

Use a secure platform

- We continuously perform vulnerability assessments to help protect against threats.
- We harden and maintain every component as part of our product development process.

For more information

For more information about Cisco HyperFlex Systems, visit http://cisco.com/go/hyperflex.

Using role-based access control (RBAC), you can specify which administrators can modify configurations and which have read-only permission for monitoring purposes. Changes performed through the Cisco HyperFlex Connect interface, representational state transfer (REST) APIs, or the command-line interface (CLI) are audited so that any unauthorized changes can be traced back to their sources.

Behind the management interfaces, Cisco UCS Manager implements consistent configuration and key management across the cluster.

Conclusion

Cisco HyperFlex systems are ready to support your enterprise applications with a holistic approach to security that:

- Secures data at rest
- Helps you comply with regulations that require data privacy
- Protects against active attacks with a secure platform

The security that we have built into Cisco HyperFlex systems is part of a long history of integrating security into the software lifecycle at Cisco. With security built into the lifecycle of your Cisco HyperFlex system, you too can experience the benefits of a long tradition of security excellence.

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

LE-60301-00 07/17