cisco Live!

#CiscoLive

The bridge to possible

Secure Workloads and Data in the Private Cloud

With HyperFlex, Intersight, and Cisco Secure Virtual Firewalls

Ronnie Chan, Sr. Engineering Product Manager
@ronnielchan

BRKDCN-2706

Cisco Webex App

Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

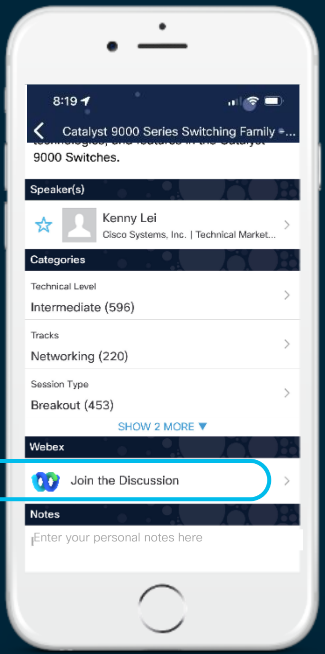
1 Find this session in the Cisco Live Mobile App

2 Click “Join the Discussion”

3 Install the Webex App or go directly to the Webex space

4 Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until June 17, 2022.



8:19

Catalyst 9000 Series Switching Family -...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKDCN-2706

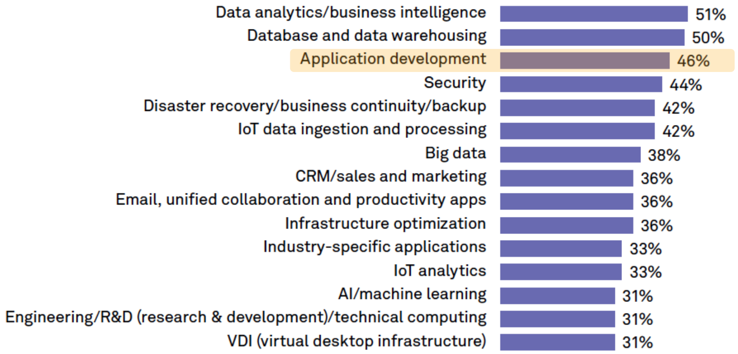
About Me

- 16 years experience in enterprise storage and cloud infrastructure, from startup to Fortune 500s
- Object, Block & File Storage, OpenStack, HCI
- Areas of focus: data platform, security, software-only HX
- Perspectives: systems engineer, field marketing engineer, product manager

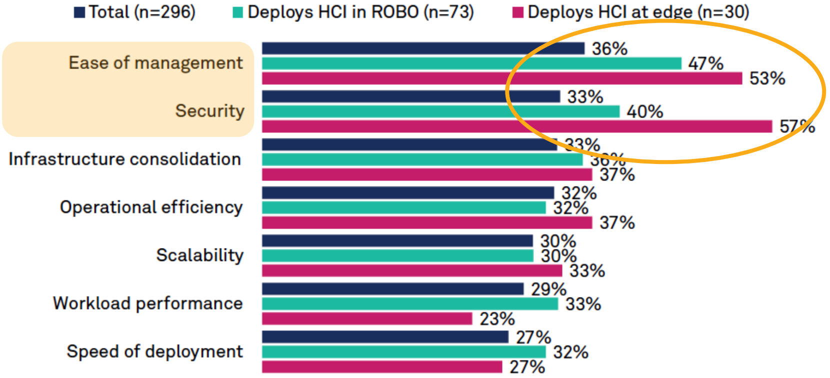
HCI fast-tracks…efforts to implement hybrid cloud because HCI-enabled infrastructure is rapidly deployed and provides one software platform across all environments, whether on- or off-premises.

451 Research

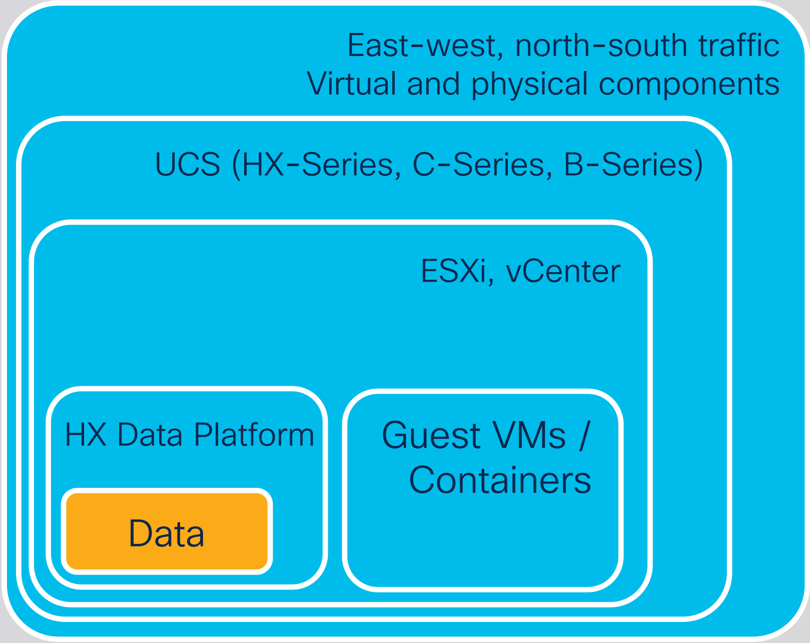
Current and future workload deployed on HCI

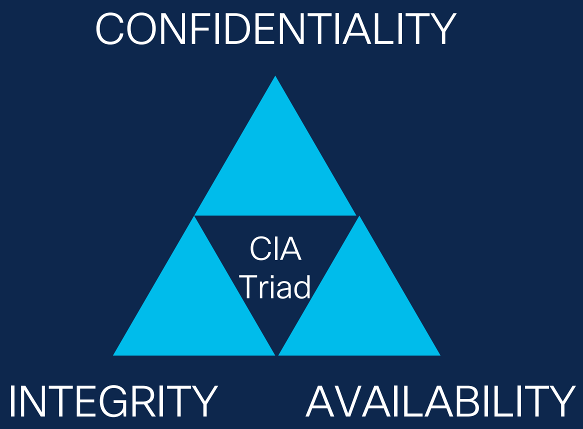


Technical drivers for deploying apps on HCI



“Hyperconvergence” of Security Domains

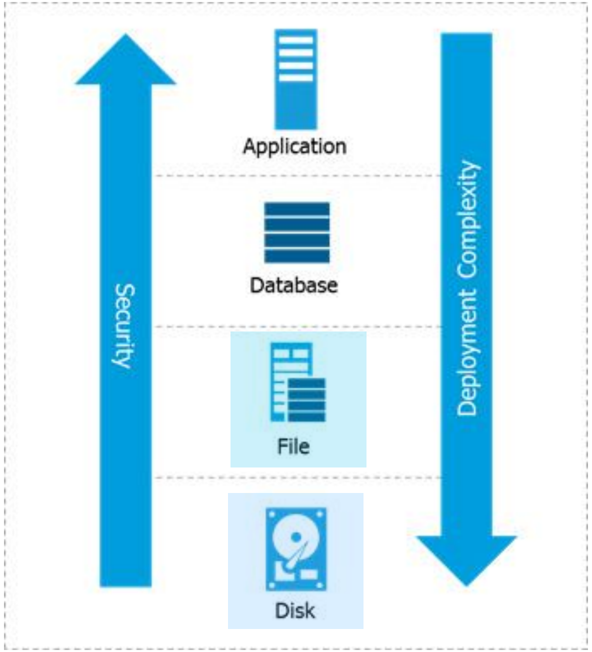

East-west, north-south traffic
Virtual and physical components
UCS (HX-Series, C-Series, B-Series)
ESXi, vCenter
HX Data Platform
Data
Guest VMs / Containers



What We will Focus on Today...

Confidentiality	Data at Rest	Data Access	Mgmt. Access	App Network
Integrity	Root of Trust	Software Authenticity	Cluster Health	Cluster Hardening
Availability	Reliability	Availability	Data Protection	

Data-at-Rest Encryption (DARE) in HyperFlex

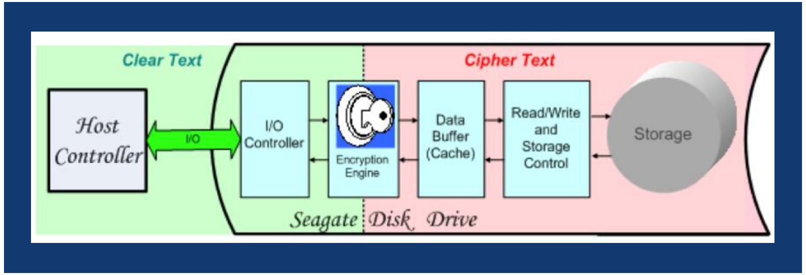


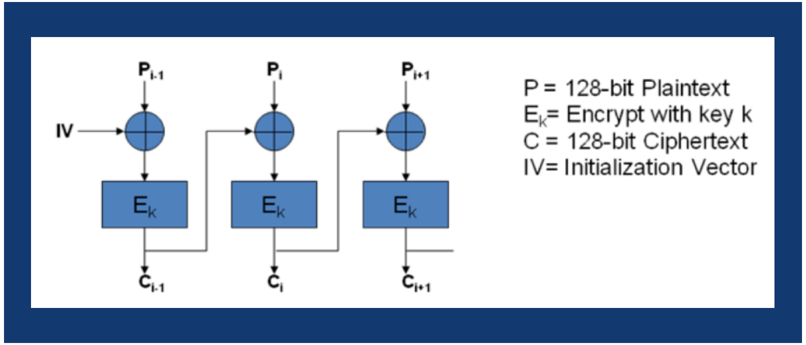
1. Self-Encrypting Drives

2. Software Encryption

- Both protect confidentiality of data at-rest from hardware loss
  - Malicious, e.g., theft of drives, servers, clusters
  - Accidental, e.g., inadequate sanitization when disposing drives
- Neither protects against:
  - Attacker breaches HX controller VMs
  - Exploits upstream of the storage stack: hypervisor, VMs, guest OS, application

DARE with SEDs: A Few Salient Points

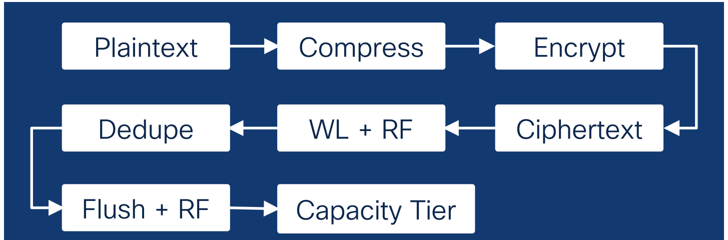




Source: *Enterprise Self-Encryption Drives, User Guide – Part 1 (2015). Seagate. https://www.seagate.com/files/staticfiles/support/docs/manual/Interface%20manuals/100515636b.pdf*

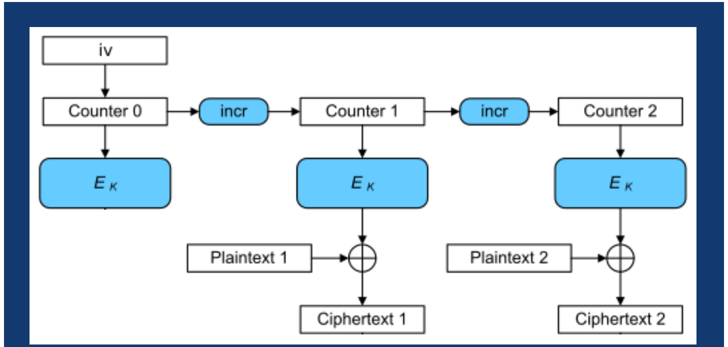
- AES engine encrypts/decrypts data inline with each I/O operation to storage media
- Symmetric key encryption w/ MEK (32-byte random number) known only to the drive
- Once put into locked state, drive must be unlocked with a KEK before I/O can proceed
- 2 KEK options available in HX: **Local Key** (stored in FI), **Remote Key** (stored in KMS)
- Advantages of using SEDs
  - Doesn’t consume host resources
  - Can offer tamper evidence (FIPS 140-2 level 2)
- Disadvantages of using SEDs
  - Many encrypt/decrypt ops per HXDP write
  - Limited drive types and capacities available
  - Can incur a cost premium over non-SEDs
  - Only available in FI-based DC clusters

DARE with HX Software Encryption



Plaintext → Compress → Encrypt → Ciphertext → WL + RF → Dedupe → Flush + RF → Capacity Tier

Write Operation with SE



AES-GCM encryption

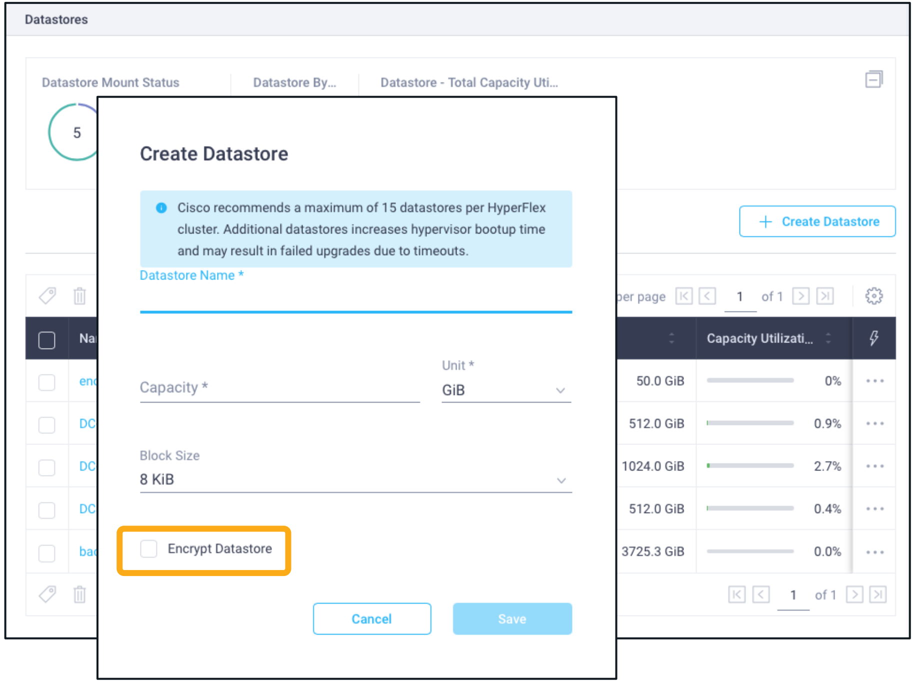
- FIPS 140-2 compliant, 256-bit AES encryption
- Optimized for HX distributed data model = Fast!
- 3 clicks to enable SE with Intersight Key Manger
- Manage encrypted and unencrypted datastores in Intersight and HX Connect
- Software-based encryption = hardware agnostic:
  - ✓ DC (FI and FI-less), Stretched, Edge clusters
  - ✓ All-NVMe, All-Flash and Hybrid systems
  - ✓ M4, M5 and M6 systems

Demo: Enable SE with Intersight Key Manager

```
Last login: Fri Mar 11 10:57:09 on ttys000
bilroth@BILROTH-M-F1ST ~ %
```

Manage Encrypted Datastores

Intersight



Datastores

Datastore Mount Status | Datastore By... | Datastore - Total Capacity Uti...

5

Create Datastore

Cisco recommends a maximum of 15 datastores per HyperFlex cluster. Additional datastores increases hypervisor bootup time and may result in failed upgrades due to timeouts.

Datastore Name *

Capacity *

Unit * GiB

Block Size 8 KiB

□ Encrypt Datastore

Cancel | Save

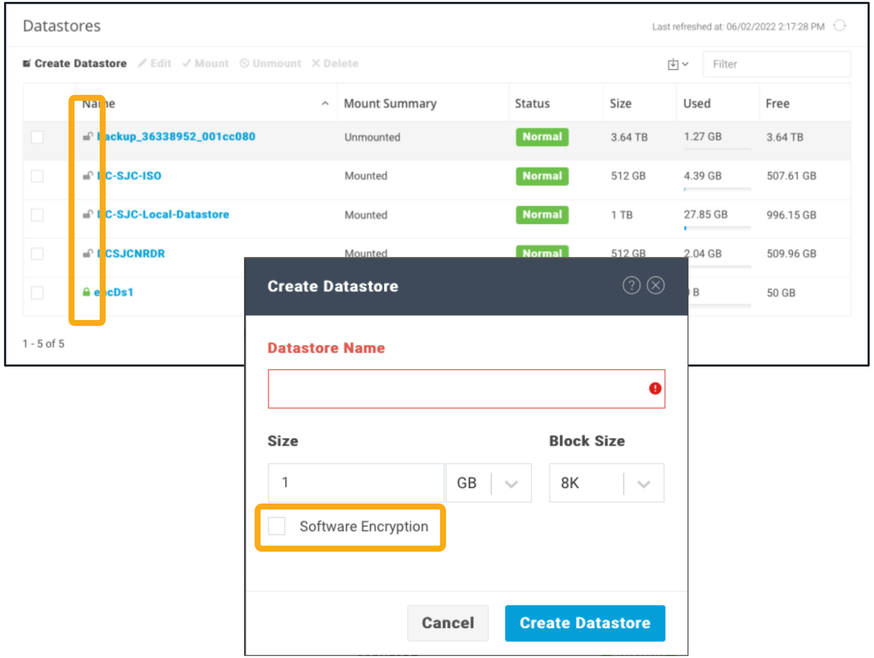
+ Create Datastore

per page 1 of 1

Na		Capacity Utilizati...
en	50.0 GiB	0%
DC	512.0 GiB	0.9%
DC	1024.0 GiB	2.7%
DC	512.0 GiB	0.4%
ba	3725.3 GiB	0.0%

1 of 1

HX Connect



Datastores

Last refreshed at: 06/02/2022 2:17:28 PM

Create Datastore | Edit | Mount | Unmount | Delete

Filter

Na e	Mount Summary	Status	Size	Used	Free
ackup_36338952_001cc080	Unmounted	Normal	3.64 TB	1.27 GB	3.64 TB
C-SJC-ISO	Mounted	Normal	512 GB	4.39 GB	507.61 GB
C-SJC-Local-Datastore	Mounted	Normal	1 TB	27.85 GB	996.15 GB
CSJCNRDR	Mounted	Normal	512 GB	2.04 GB	509.96 GB
e cDs1				B	50 GB

1 - 5 of 5

Create Datastore

Datastore Name

Size 1 GB

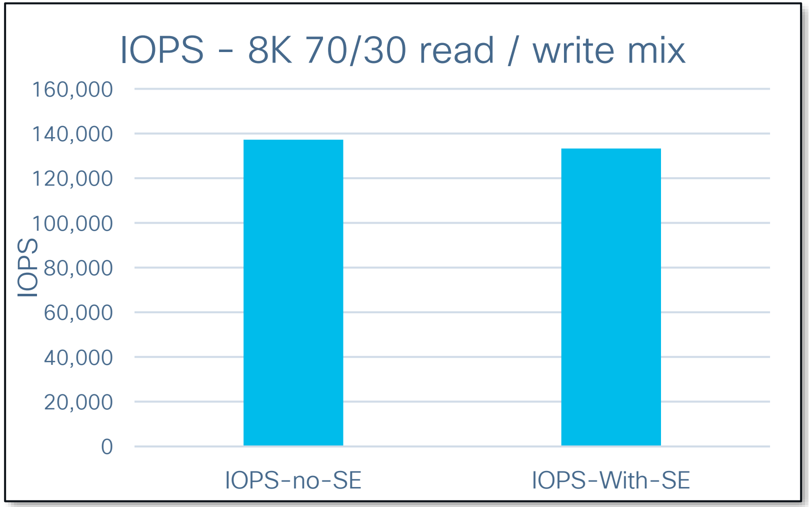
Block Size 8K

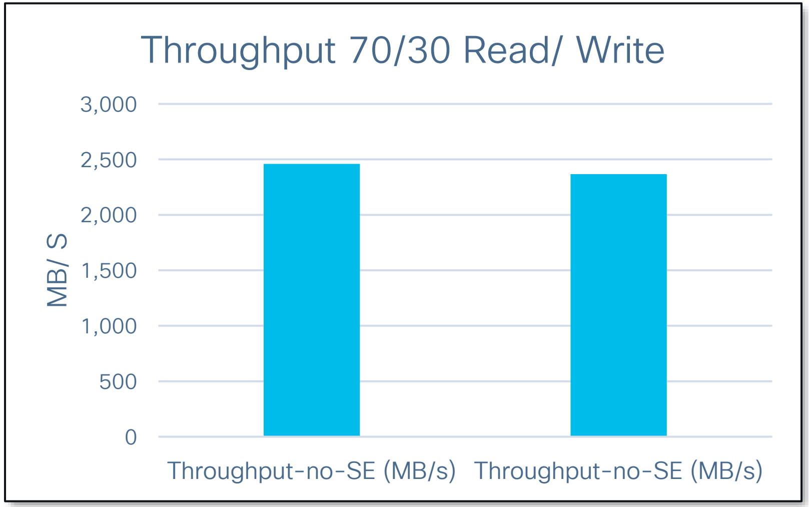
□ Software Encryption

Cancel | Create Datastore

Software Encryption Performance

HXAF 240 M6 cluster (HX Boost Mode not configured)

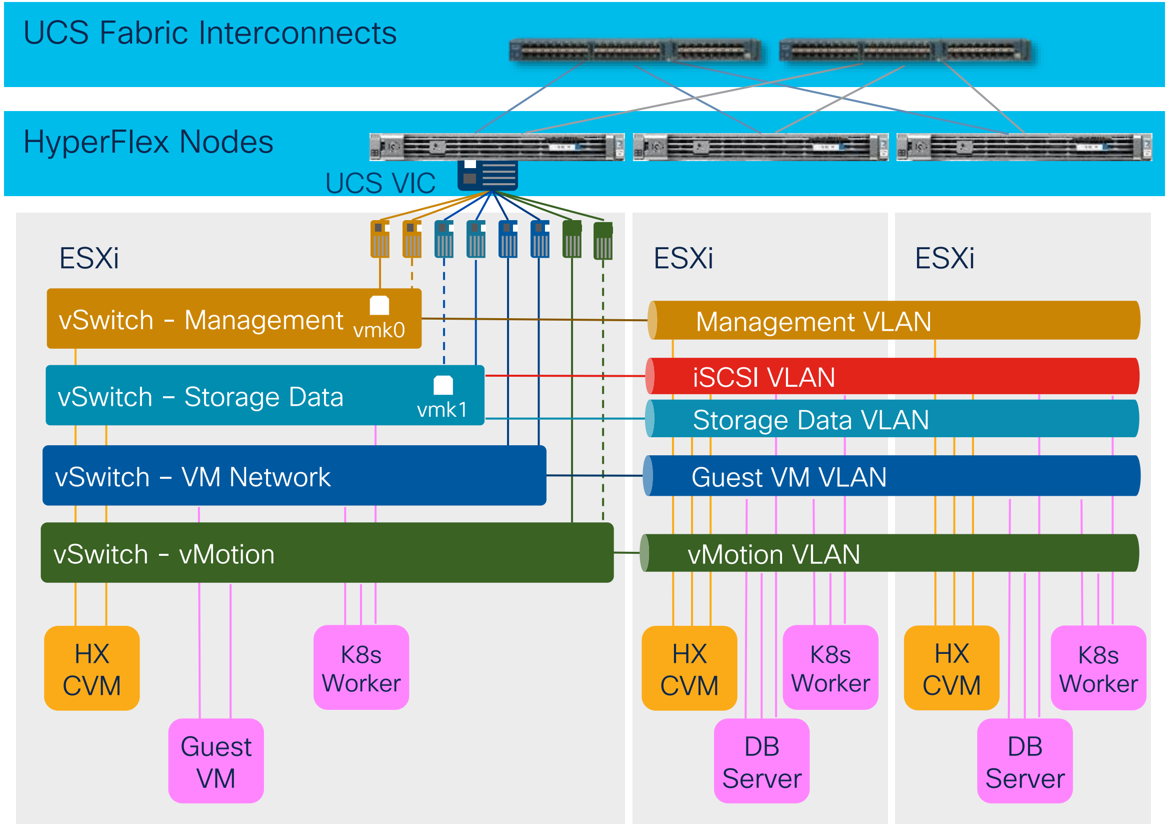




8K Workloads	Impact of SE
8K 100% Read	-3.6%
8K 70/30 Read/ Write	-2.8%
8K 100% Write	-7.2%

64K Workloads	Impact of SE
64K 100% Read	0.4%
64K 70/30 Read/ Write	-3.7%
64K 100% Write	-4.0%

Network Segmentation and Traffic Isolation



- Physical EW fabric, uplinks to TOR switches for NS traffic
- Virtualized interfaces, single cable mgmt. by Cisco VIC
- Automated and consistent configuration with UCS service profile templates
- Traffic segmentation via dedicated vNICs
- Storage and management traffic localized to fabric for optimal performance
- QoS policies (e.g., no-drop, jumbo frames) for well defined and predictable service

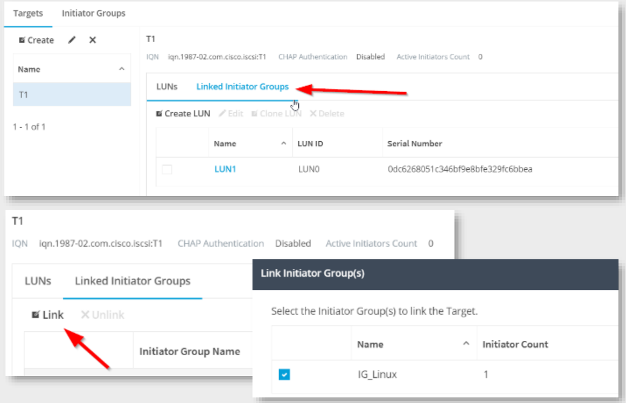
Confidentiality

Data Plane Access Controls

Datastores – IOvisor manages access to datastores from HXDP

Isolated, private VLAN dedicated to datastore traffic

Hosts must be on allowlist to mount datastores



Targets | Initiator Groups

T1

IQN iqn.1987-02.com.cisco.iscsi:T1 CHAP Authentication Disabled Active Initiators Count 0

	Name	LUN ID	Serial Number
□	LUN1	LUN0	0dc6268051c346bf9e8bfe329fc6bbea

T1

IQN iqn.1987-02.com.cisco.iscsi:T1 CHAP Authentication Disabled Active Initiators Count 0

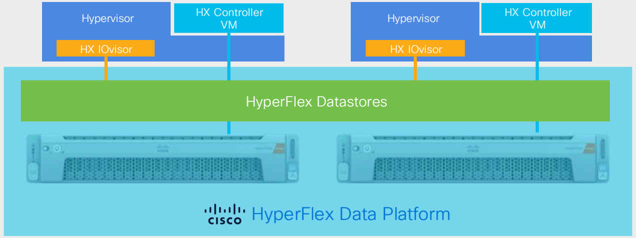
Link Initiator Group(s)

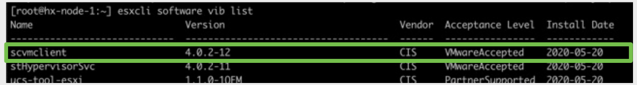
Select the Initiator Group(s) to link the Target.

	Name	Initiator Count
☑	IG_Linux	1

Optionally, authenticate initiators using CHAP

Initiator attempting to login to the HX Target must present the Challenge Handshake Authentication Protocol (CHAP) password for the target





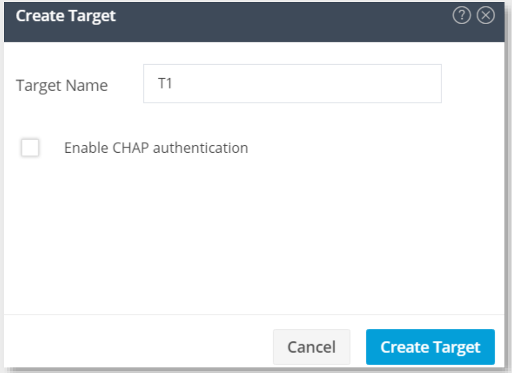
```
[root@hx-node-1:~] esxcli software vib list
Name                          Version                                Vendor  Acceptance Level  Install Date
----------------------------  -------------------------------------  ------  ----------------  ------------
scvmclient                    4.0.2-12                               CIS     VMwareAccepted    2020-05-20
stHypervisorSvc               4.0.2-11                               CIS     VMwareAccepted    2020-05-20
ucs-tool-esxi                 1.1.0-1OEM                             CIS     PartnerSupported  2020-05-20
```

Block or Container Storage – Storage access controlled by iSCSI initiators and targets

Initiator's IQN is verified

Access to LUNs is restricted to linked initiator for a target

Initiator from outside iSCSI VLAN must be added to allowlist



Create Target

Target Name: T1

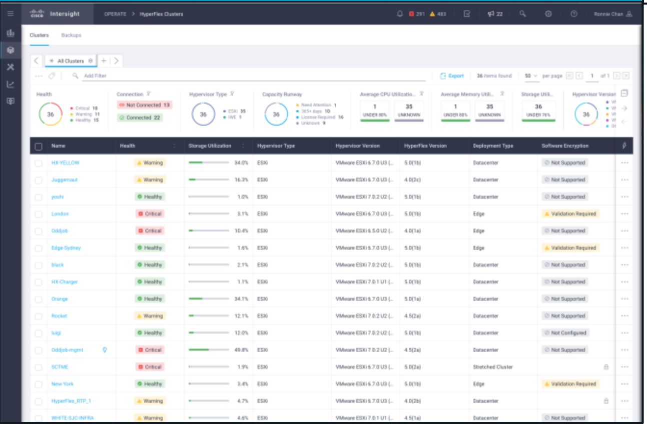
□ Enable CHAP authentication

Management Plane Access Controls

Intersight: single-pane-of-glass global management

Support Zero-Trust with SSO and MFA (cisco.com or on-prem IdP)

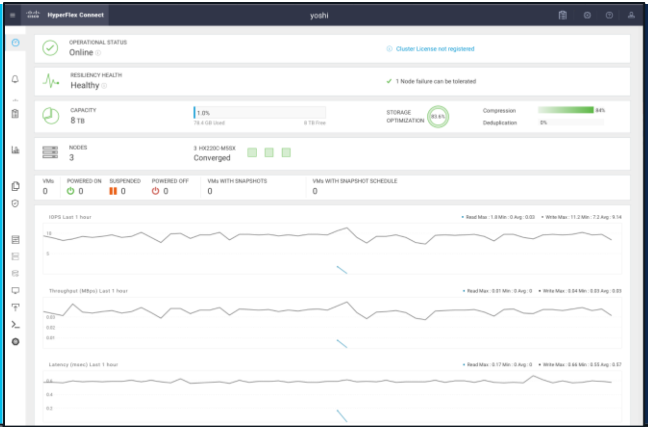
Secure channel (WebSocket) between Intersight and HX via embedded Device Connectors



HX Connect and REST APIs: local cluster management

Authentication for local (admin) and AD users and groups (latter requiring vCenter integration with AD)

RBAC: 2 roles (admin, read-only), enforced across UI, CLI and API

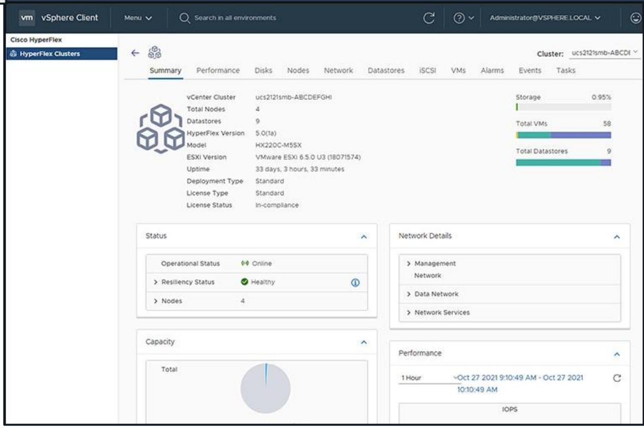


HX Plugin: manage HX clusters from within VMware vCenter

Perform Day-2 cluster operations and monitoring directly from vCenter

Signed package from CCO and automated install

Traffic between plugin and HX protected by TLS



Confidentiality

Protect App Networks with Cisco Secure Firewall (FTDv, ASAv) running on HX

North-South Security with Cisco Secure Firewall

(formerly NGFW)

Broad Visibility

- Secure Firewall at data center edge
- Visibility into Internet, branch, campus
- Attribute based policies

East-West Security with Cisco Secure Firewall

Coarse Control

- Segment within your data centers
- Handles workloads without agents
- Single/multi site public cloud
- Physical/virtual form factors

Workload Security with Cisco Secure Workload

Fine-Grained Control

- Provides detailed inter-application controls, software-based
- Supports rapid automation

Closer to application

Cisco Secure Firewall Threat Defense Virtual on HX

FTD Version	FTD 7.0 or later
FMC Version	FTD 7.0 or later
FTDv Cores	4, 8, 12,16 core vCPU
VMware vSphere Version	7.0
HX Data Platform Version	HX 4.5(1a) or later
Supported vNICs	VMXNET3 - FTDv on VMware now defaults to vmxnet3 interfaces when you create a virtual device.

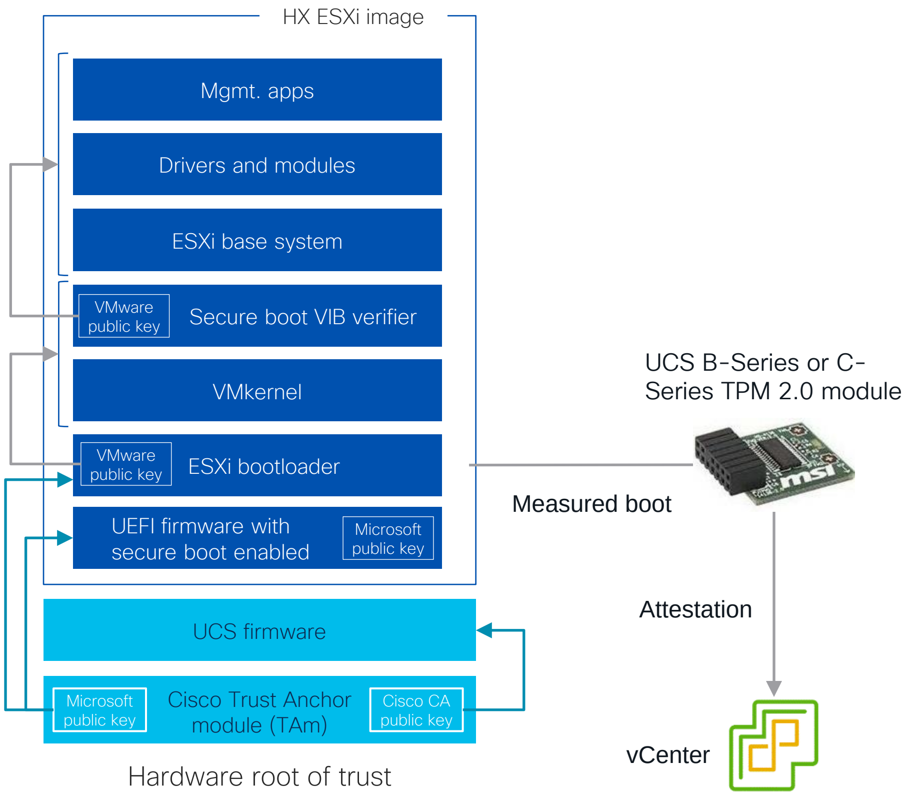
Cisco Secure Firewall ASA Virtual on HX

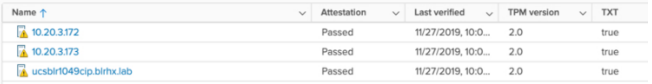
ASAv Cores	1, 4, 8, 16 core vCPU
ASAv Version	9.17 or later
VMware ESXi Version	7.0
HX Data Platform Version	4.5(1a) or later
Supported vNICs	VMXNET3 - ASAv on VMware now defaults to vmxnet3 interfaces when you create a virtual device.

Integrity

UEFI Secure Boot Support in HX

- Detects ESXi boot code issues with public keys stored in write-protected hardware trust anchor (“silicon root of trust”)
- Built-in capability in UCS rack and blades; no additional hardware required
- Ensures only a trusted HX ESXi image, including drivers, is booted by verifying signatures
- Supports attestation of secure boot by vCenter; requires min. ESXi 6.7 and TPM 2.0 hardware module
- UEFI Secure Boot mode is enabled by default on freshly installed clusters running HX 5.0 or later



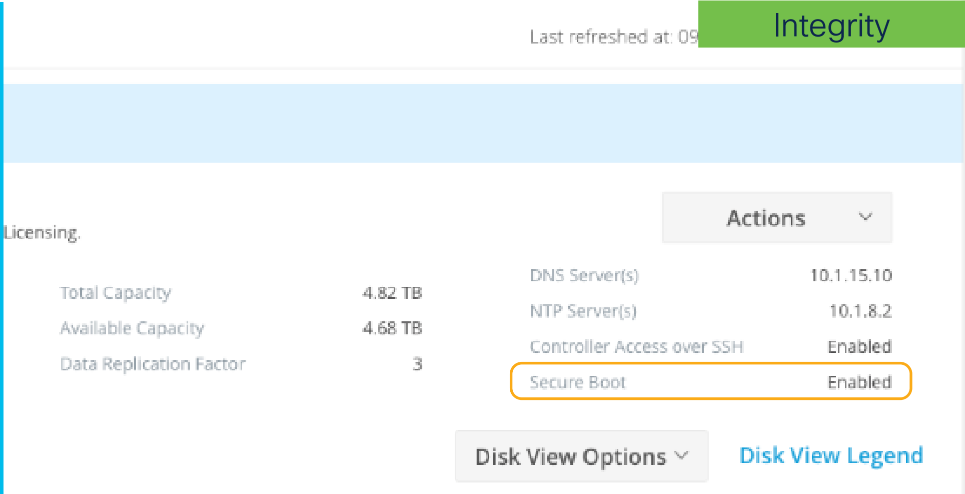


Name ↑	Attestation	Last verified	TPM version	TXT
10.20.3.172	Passed	11/27/2019, 10:0...	2.0	true
10.20.3.173	Passed	11/27/2019, 10:0...	2.0	true
ucsblr1049cip.blrhx.lab	Passed	11/27/2019, 10:0...	2.0	true

Seamlessly change boot mode from Legacy BIOS to UEFI Secure Boot on brownfield clusters

After upgrading to HX 4.5 or later, a “Secure Boot mode” upgrade type becomes available on HX Connect

Recommend pre-flight test (“Test Upgrade Eligibility”) before proceeding

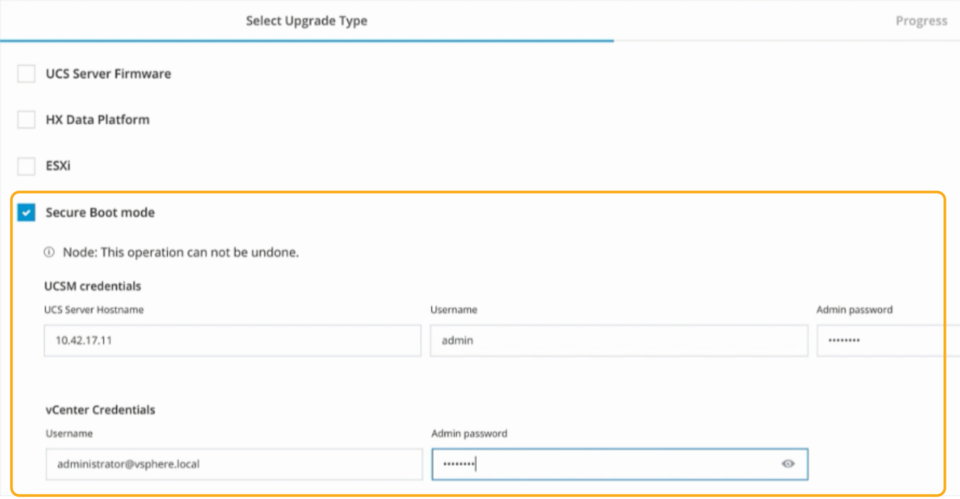


Last refreshed at: 09

Integrity

Licensing.

Total Capacity	4.82 TB	DNS Server(s)	10.1.15.10
Available Capacity	4.68 TB	NTP Server(s)	10.1.8.2
Data Replication Factor	3	Controller Access over SSH	Enabled
		Secure Boot	Enabled



□ UCS Server Firmware

□ HX Data Platform

□ ESXi

☑ Secure Boot mode

ⓘ Node: This operation can not be undone.

UCSM credentials

UCS Server Hostname	Username	Admin password
10.42.17.11	admin	••••••••

vCenter Credentials

Username	Admin password
administrator@vsphere.local	••••••••

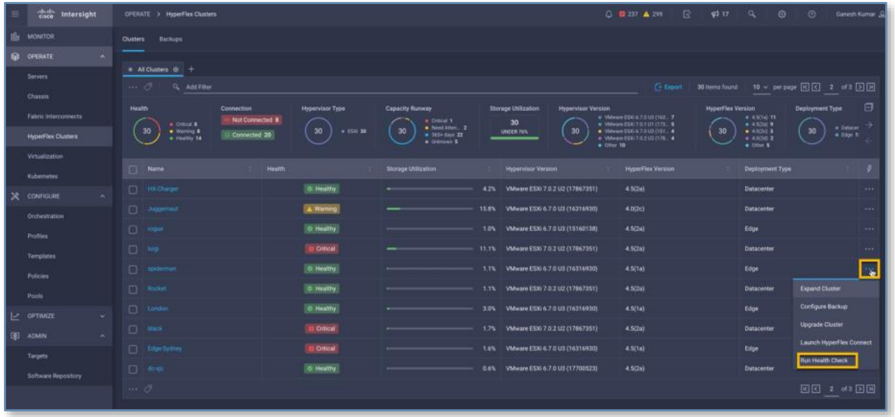
Status indicator shows if all nodes (converged and compute-only) in the cluster has secure boot enabled

“Check Secure Boot Status” action button reports if boot mode on any node was changed out-of-band

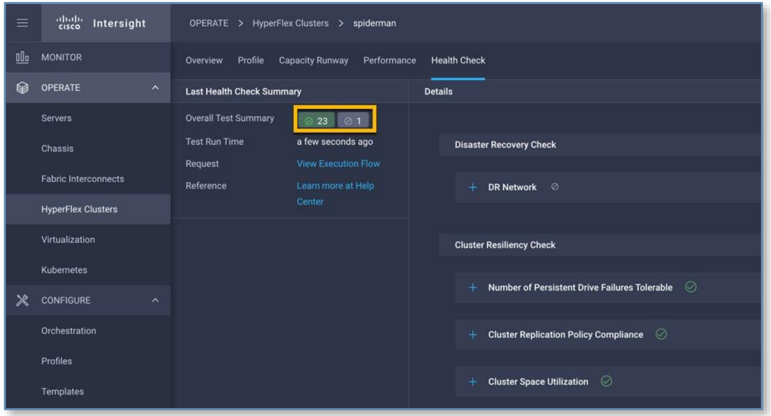
Integrity

HyperFlex Health Check

- Initiate from Intersight, runs locally on cluster
- More than 20 comprehensive checks, to be run in full or partially
  - Granular results and actionable recommendations
  - New security checks show statuses of security-related configurations per latest best practices



Name	Health	Storage Utilization	Hypervisor Version	HyperFlex Version	Deployment Type
HX-Charger	Healthy	4.2%	VMware ESXi 7.0.2 U2 (17867351)	4.5(2a)	Datacenter
Juggernaut	Warning	15.8%	VMware ESXi 6.7.0 U3 (16316930)	4.0(2c)	Datacenter
rogue	Healthy	1.0%	VMware ESXi 6.7.0 U3 (15160138)	4.5(2a)	Edge
luigi	Critical	11.1%	VMware ESXi 7.0.2 U2 (17867351)	4.5(2a)	Datacenter
spiderman	Healthy	1.1%	VMware ESXi 6.7.0 U3 (16316930)	4.5(1a)	Edge
Rocket	Healthy	1.1%	VMware ESXi 7.0.2 U2 (17867351)	4.5(2a)	Datacenter
London	Healthy	3.0%	VMware ESXi 6.7.0 U3 (16316930)	4.5(1a)	Edge
black	Critical	1.7%	VMware ESXi 7.0.2 U2 (17867351)	4.5(2a)	Datacenter
Edge Sydney	Critical	1.6%	VMware ESXi 6.7.0 U3 (16316930)	4.5(1a)	Edge
dc-spi	Healthy	0.6%	VMware ESXi 6.7.0 U3 (17700523)	4.5(2a)	Datacenter



Last Health Check Summary

Overall Test Summary: ✓ 23 ⊘ 1

Test Run Time: a few seconds ago

Request: View Execution Flow

Reference: Learn more at Help Center

Details

Disaster Recovery Check

- + DR Network ⊘

Cluster Resiliency Check

- + Number of Persistent Drive Failures Tolerable ✓
- + Cluster Replication Policy Compliance ✓
- + Cluster Space Utilization ✓

Integrity

HyperFlex Hardening

Follow Hardening Guides

HX Data Platform HG (refreshed to HX 5.0)

vSphere Security Configuration Guide

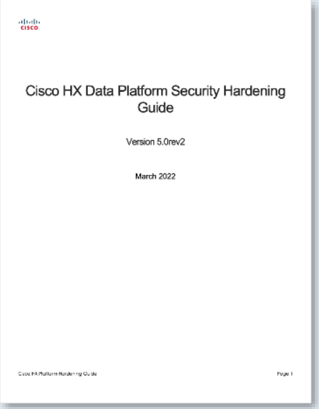
UCS Hardening Guide

Patching

HX being in user space means ESXi and vCenter patches are independently supported and can be applied independently of HXDP

Upgrade ESXi with HX Connect or Intersight; neither VUM nor vLCM is HX cluster aware!

Cisco scans weekly for CVEs and fixes are rolled into the next HXDP patch release (turnaround within 90 days depending on SIR)



Cisco HX Data Platform Security Hardening Guide

Version 5.0rev2

March 2022

Cisco HX Platform Hardening Guide Page 1

Hardening Automation

HX CLI command automates application of supported vSphere, ESXi and VM hardening settings (with reference to Secure Technical Implementation Guides)

HyperFlex Availability & Data Protection

Data Integrity & Reliability

Block checksums protect against media errors

Flash friendly layout maximizes media life

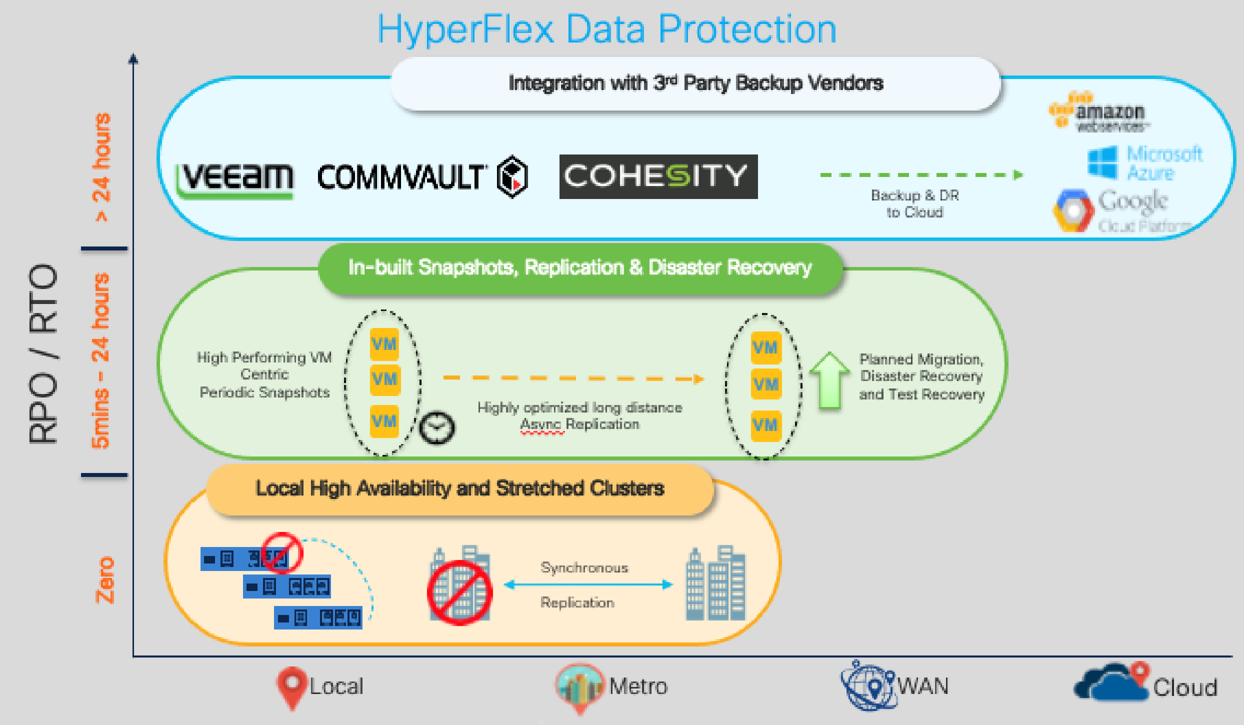
Zero overhead, instantaneous snapshots for data protection

High Availability

Fully-striped architecture helps with faster rebuilds

Fine grained data-resync and rebalance

Non-disruptive rolling upgrades



HyperFlex Data Protection

Integration with 3rd Party Backup Vendors

Backup & DR to Cloud

In-built Snapshots, Replication & Disaster Recovery

High Performing VM Centric Periodic Snapshots

Highly optimized long distance Async Replication

Planned Migration, Disaster Recovery and Test Recovery

Local High Availability and Stretched Clusters

Synchronous Replication

Session Summary

HCI creates a convergence of security concerns across compute, storage and networking

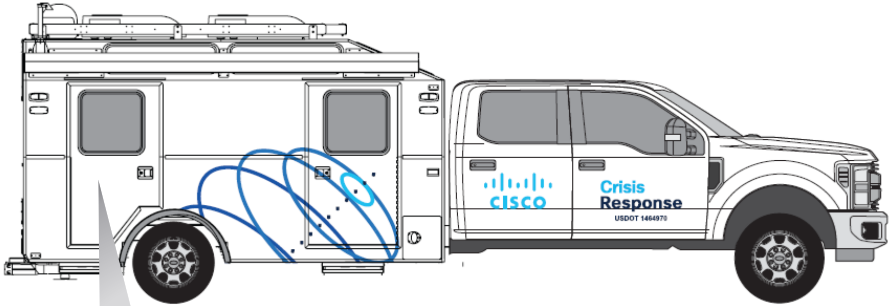
With an appliance-based and network-integrated approach, HyperFlex, UCS and Intersight help address security challenges across the entire stack

Leverage the power of Cisco-on-Cisco, such as Cisco Secure Firewall Virtual, to secure the application networks on HyperFlex whether in the Datacenter or at the Edge

Tour the Network Emergency Response Vehicle

Powered by Cisco HyperFlex

- Providing **free and secure emergency communications to first responders** after a disaster
- **Equipped with a HyperFlex edge cluster** for workloads that might include:
  - Drone Image processing
  - Video surveillance
  - Network, collaboration and cybersecurity applications
  - **Take a tour!** Located at back of hall, near Broadcast Studio



"Reestablish and provide secure network and satellite communications for emergency responders in a disaster zone"

Cisco HyperFlex Edge Clusters

For info on Cisco Crisis Response scan the QR code.

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

The bridge to possible

Thank you

cisco Live!

#CiscoLive