



Possibilities

#CiscoLive

Cisco Intersight

Architecture and Operations

Eric Williams, Principal Engineer

Matt Faiello, Technical Marketing Engineer

DGTL-BRKINI-2534



#CiscoLive





Agenda

- Chapter 1: Intersight Overview
 - What is a Device Connector?
 - Intersight Deployable Architectures
- Chapter 2: Intersight Architecture
 - Behavioral Changes of Policy Enforcement
 - Role-based Authentication
 - Organizations and Tagging
- Chapter 3: Use Cases & Key Features
 - Intersight Managed Mode – Tech Preview
 - Firmware Updates
 - Connected TAC, Advisories, and Contract Status

Chapter 1: Intersight Overview



Cisco Intersight Guiding Principles / Vision



Unified management



SaaS/subscription



No-impact transition



Agile Model



Programmability



Enhanced support experience



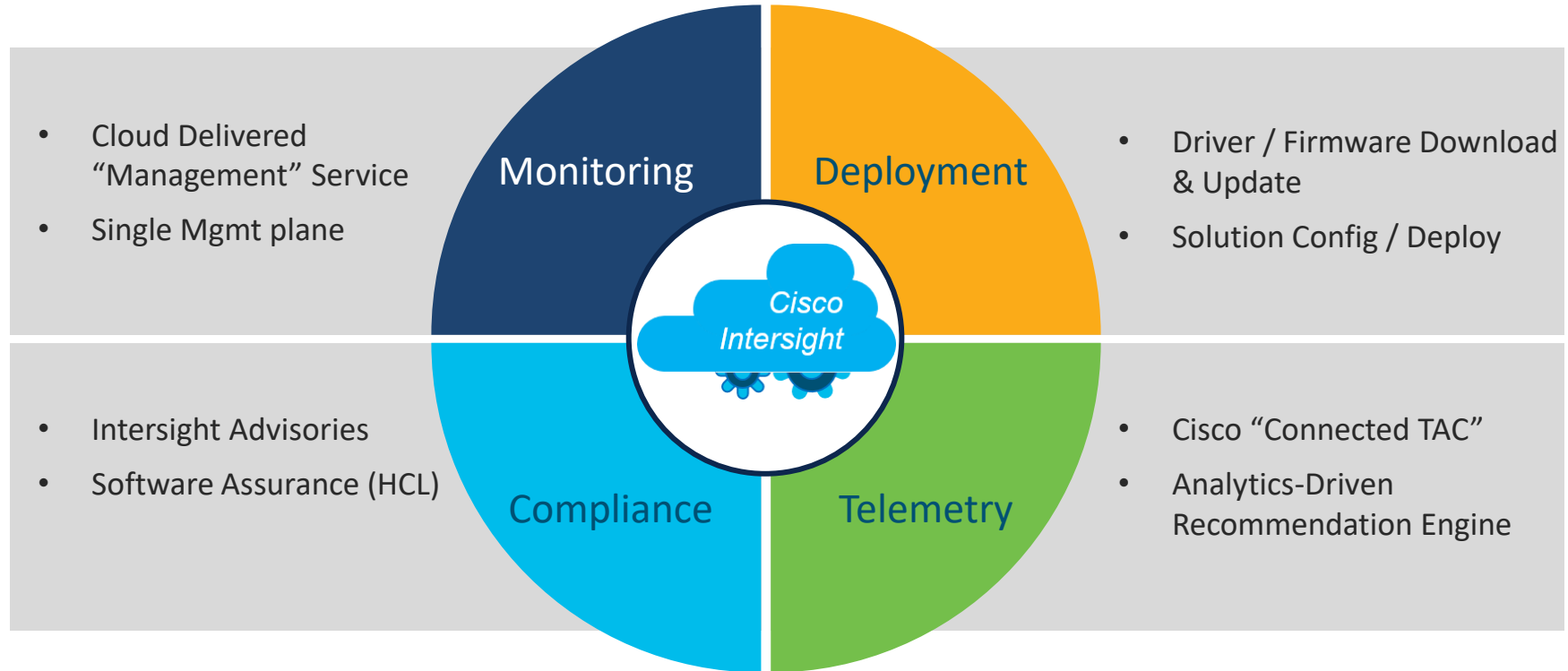
Recommendation engine



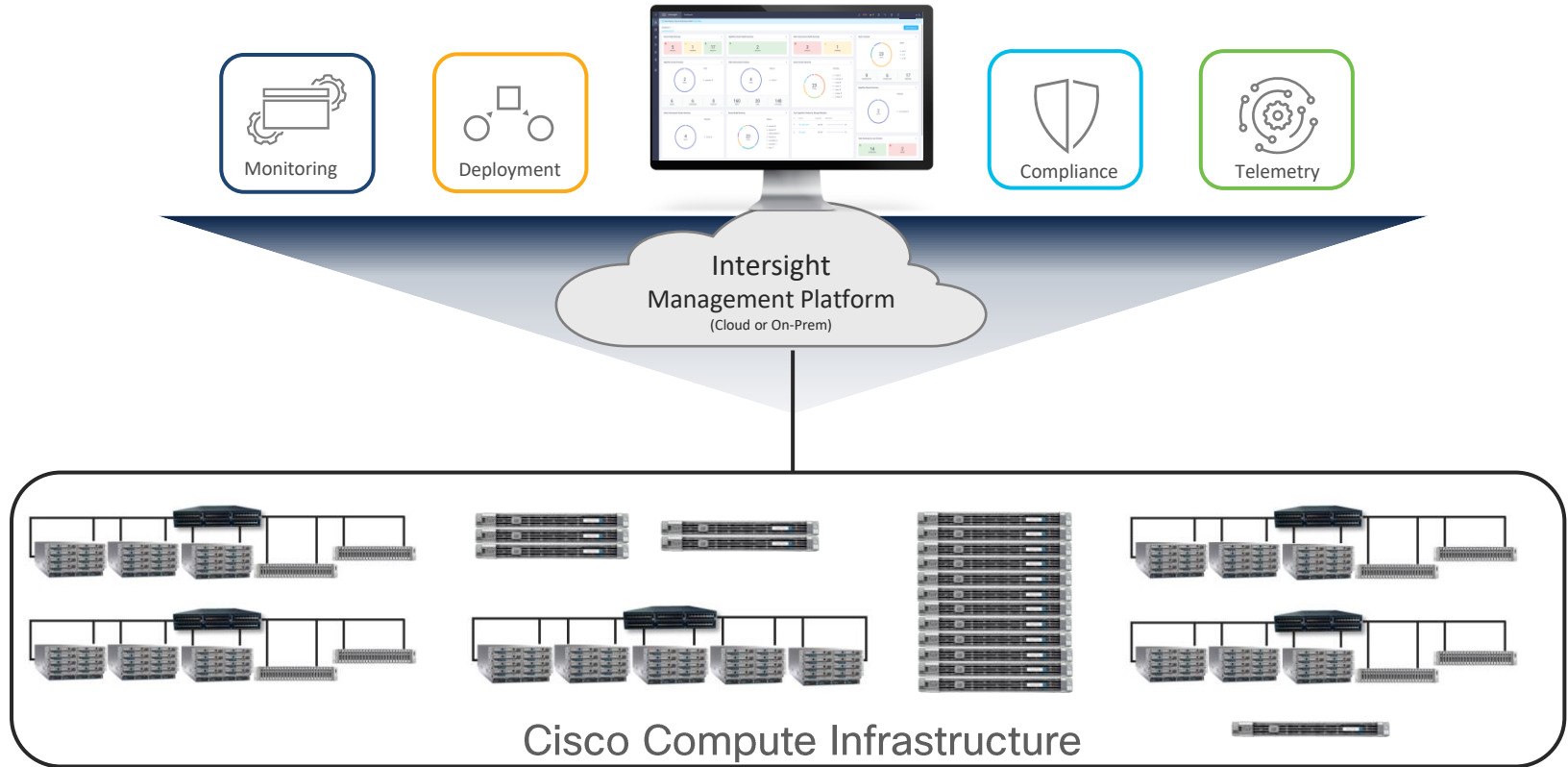
Limitless Scale

Value Proposition – Intelligent Operations

What does Intersight do?



Cisco Compute Simplicity – One Framework



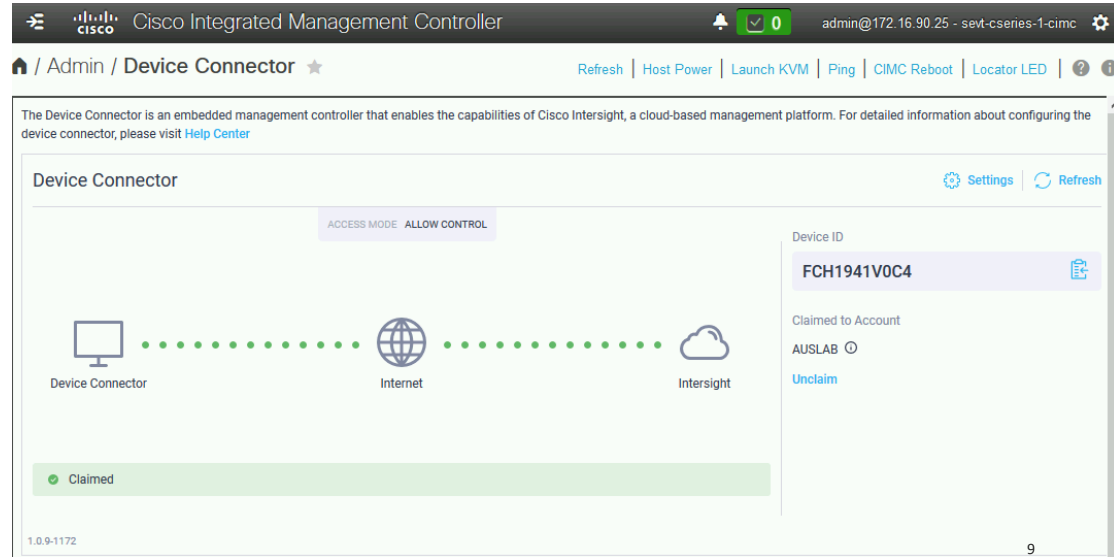
Device Connectors

UCS & HyperFlex become SaaS
Enabled

Intersight Connectivity with Managed Devices

Device Connector:

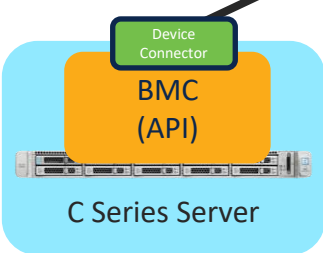
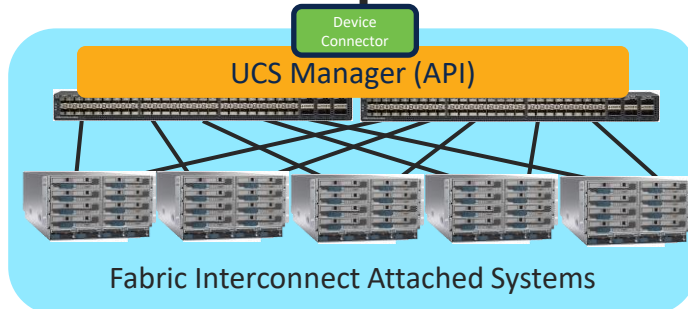
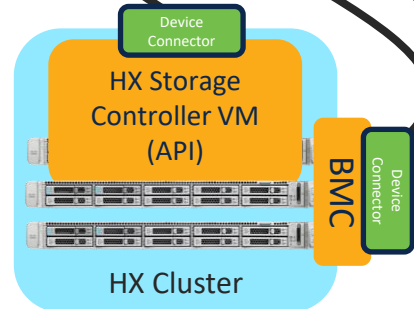
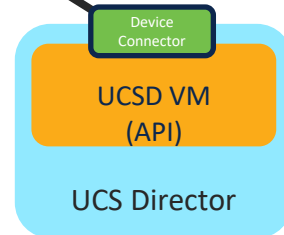
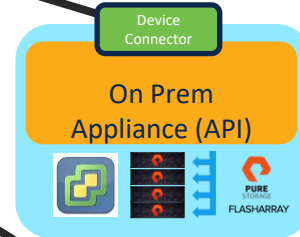
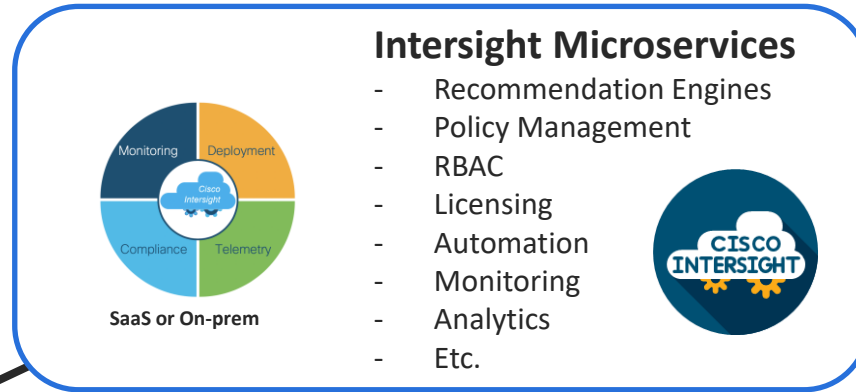
- Bundled in Firmware / Management SW
- Embedded in Management Controller of all new UCS and HyperFlex servers
- Connects to known cloud management location (specific URL)
- DC controls connectivity
 - Device initiated outbound connections
 - HTTPS on port 443 or through proxy
 - MFA
 - Device ID
 - Rolling Claim Code



Intersight – Device Connector Connectivity

DC Connection is:

- Durable WebSocket
- Port 443
- Bottom-up
- Highly Secure



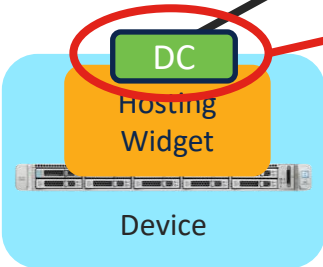
Continuous Integration / Continuous Deployment



Cisco Maintained Services

Paradigm Shift

- Intersight is based on CI / CD Methodology
- It is a SERVICE enabled with Device Connectors
- Traditional Methodology requires software upkeep
- Intersight & Device Connectors are constantly evolving



Device Connector Upgrades

Device Connector reports current version each startup

If Intersight determines an upgrade is needed, UpgradeRequest is created with the desired version

Device performs upgrade

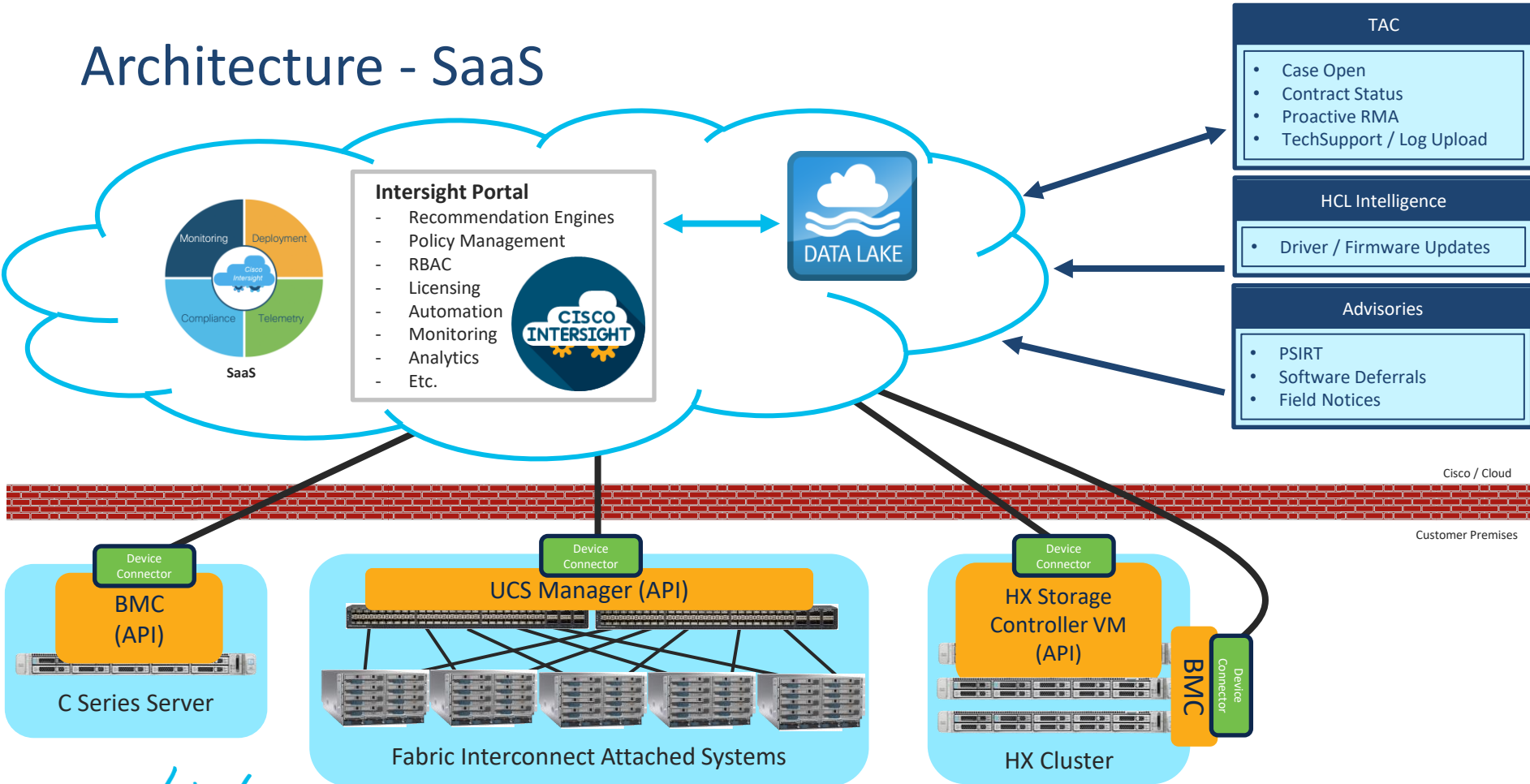
- Only attempted if device is currently connected
- Only impacts Device Connector – Infrastructure, Server, or HyperFlex FW/SW remains user controlled and is not automatically updated

Intersight polls DeviceRegistration to determine upgrade success

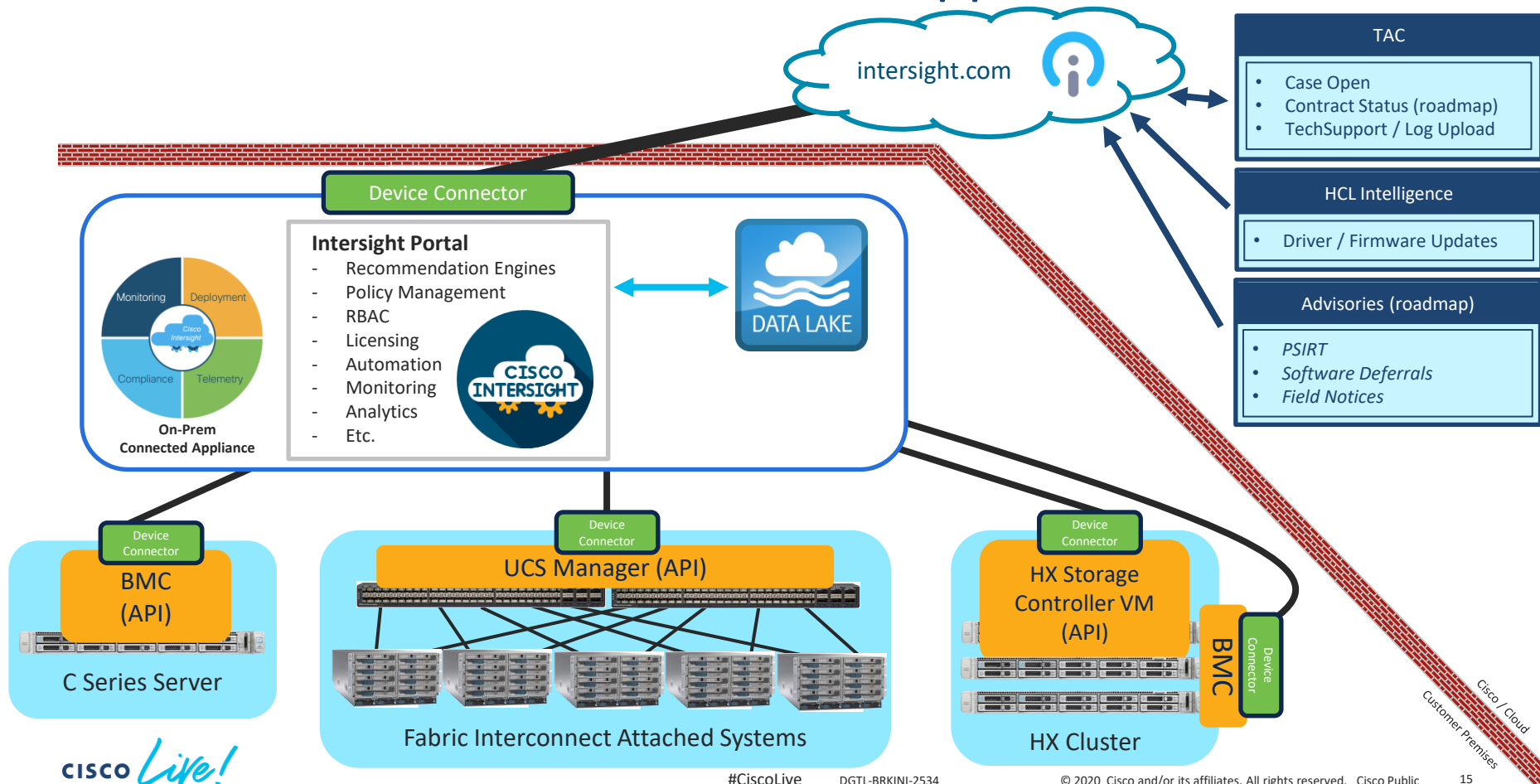
Intersight Architecture:

SaaS and On-Prem Appliances

Architecture - SaaS

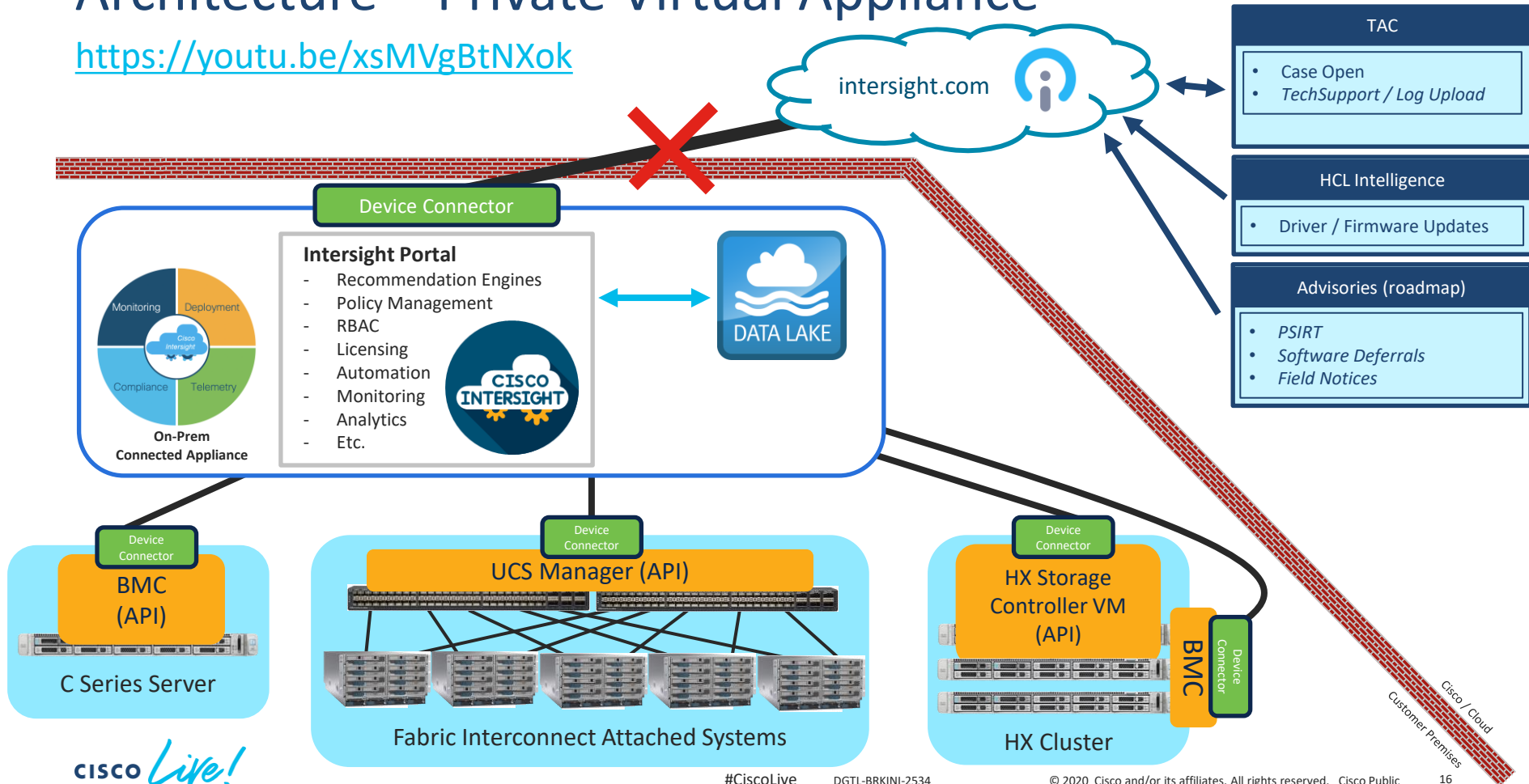


Architecture – Connected Virtual Appliance



Architecture – Private Virtual Appliance

<https://youtu.be/xsMVgBtNXok>





Intersight Licensing:


Base, Essentials, Advantage, and
Premier License Tiers



Cisco Intersight Features - Base Tier License

Base

- SaaS only
- Global monitoring of health and inventory status
- User customizable dashboard
- Virtual Keyboard-Video-Mouse (vKVM)
- Tagging and basic search
- Context launch of element managers (UCS Manager, IMC, HyperFlex Connect, and UCS Director)
- Simplified Cisco HyperFlex installation and upgrades
- Connected TAC: Support Log Collection, Open Case, Support Contract Status
- Roll Based Access Control, Single Sign-On (SAML), Multi-Factor Authentication



Included with each
UCS Server
purchase

Cisco Intersight Features – Additional License Tiers



Essentials

- **All the functionality of the Base Edition**
- SaaS and Virtual Appliance/Private Appliance
- Advanced global search and detailed inventory
- Server HCL compliance check with driver Recommendations
- Service Now Integration
- Cisco Intersight Mobile App
- Cisco Standalone UCS C-Series management (M4 and later)
- Policy-based configuration with Profiles
- FW Management, Servers + S3260, FI's, Blades
- Server Inventory Details
- Server actions (Power On/Off, reboot, etc)
- HX Edge Cluster Upgrade
- HX Storage Capacity Planning (TP)
- Includes UCS Central and IMC Supervisor

Advantage

- **All the functionality of Essentials Edition**
- SaaS and Virtual Appliance
- Tunneled Virtual Keyboard-Video-Mouse (vKVM)
- Claim Managed Devices (Pure Storage and VMware vCenter)
- Storage Widget for Pure Storage
- Storage Inventory Status for Pure: Capacity and Utilization Storage
- Multi-Domain Inventory correlation: Server, Virtualization, Storage
- Operating System Install
- HX Edge + SD-WAN
- Virtualization Inventory
- Advisories & Field Notices (SSD-FN70545)

Premier

- **All the functionality of Advantage**
- SaaS and Virtual Appliance
- Includes UCS Director
- Compute Automation
- Storage Automation
- VM Automation
- Workflow Designer (in Tech Preview)

Complete listing of features are available at:
https://intersight.com/help/supported_systems

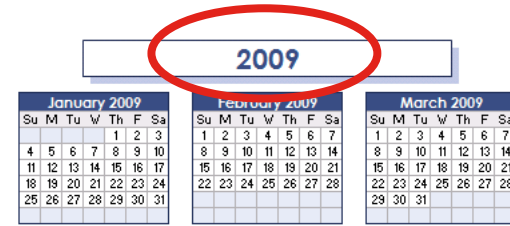
The background is a dark blue field filled with numerous small, semi-transparent squares and dots in various colors including light blue, teal, yellow, orange, and red. These elements are scattered across the frame, with a higher concentration of yellow and orange squares forming a diagonal streak from the top right towards the bottom right.

Chapter 2: Intersight Architecture

Cisco Introduces UCS = Policy-driven Compute

New approach for Model-driven / Stateless Hardware Configuration

- Configuration defined in software → Programmable via API
- Policy-driven Framework
 - Compliance / Security enforcement / Self-governance
 - No configuration drift → Desired state = Current state
- Templatable → Service Profiles



How do we do all of this with a MaaS Solution?

- Cloud-based
- Operations Capabilities
- Model-based
- Extensible
- CI / CD
- Recommendation Engines
- Automation



Intersight Behavioral Changes versus Legacy

Organizations in UCS Manager and Central

- Physical resources arranged in Domain Groups
- Logical resources arranged in organizations
 - Organizations are hierarchical
 - Policies resolved by name via parent relationships up the organization hierarchy
 - Services profiles policy references can be layered across multiple organizations
 - Organization structure and service profiles are not movable across the org structure

Intersight Behavioral Changes versus Legacy

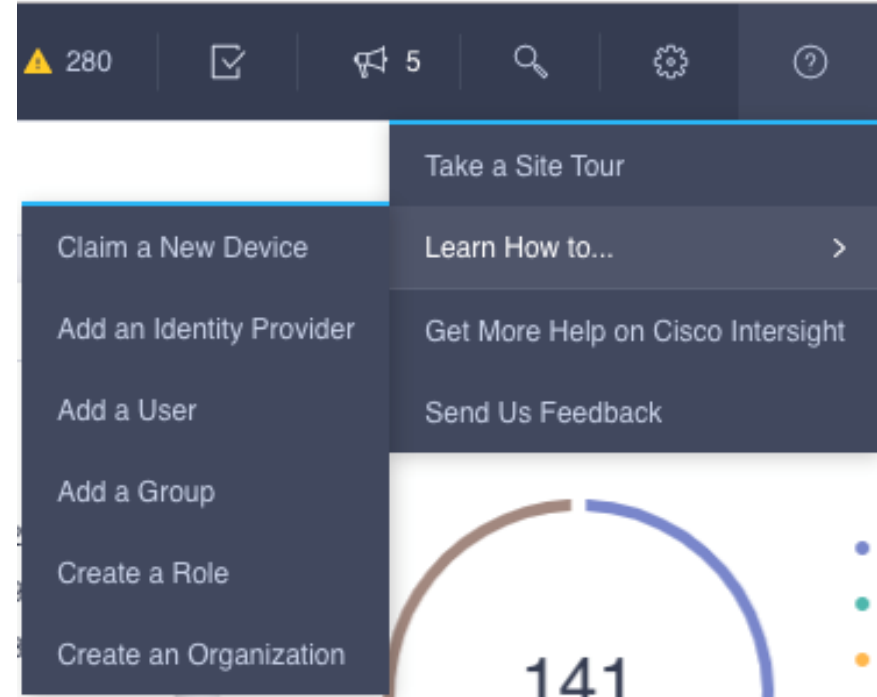
Organizations in Intersight

- Organizations are flat
- Policy references across organizations is not permitted
- Physical and logical resources combined
 - Servers, profiles, templates, policies, and pools
- Policies referenced by managed object ID (MOID) from service profile

Intersight Users/Groups, Organizations, and Role- Based Access Control (RBAC)

Guided Help: ?->Learn How to...

- Guided help has been updated to provide walk throughs for User, Group, Role, and Organization setup
- Typical setup would be in the following order:
 - Organization
 - Role (Custom Role based on existing Organization)
 - User/Group access to the Custom Role
- Users or Groups can be configured with multiple Roles
- Video Demo: <https://youtu.be/2XzQi-0OUOo>



Users, Groups, and Roles

- Settings->Access & Permissions
 - Used to manage Users and Groups
 - Users can be added using configured Identity Providers
 - Cisco or SAML 2.0 with SaaS
 - LDAP/AD or SAML 2.0 with Virtual Appliance
 - Groups can be added using the Group Name provided by the Identity Provider (groups.cisco.com for managing Cisco)
- Users or Groups can be configured with multiple Roles

Add User

Identity Provider *

Cisco

Email *

Role *

Device Administrator

Role *

Device Administrator

Device Technician

DevNet-Role

Save

Roles

- Settings->Access & Permissions->Roles
 - System Defined Roles created by default in every account
 - Following slides detail system defined roles
 - User Defined Roles can be created
 - Multiple system defined roles can be assigned in a single user defined)
- Only Account Administrators and User Access Administrators can create User Defined Roles



Create Role

Create a user defined role to assign organization and privileges.

General

Name *

DevNet-Role

Description

Custom role for DevNet users and groups

Scope

☒ Select 'All' to allow all the resources in the account or 'Organization' to give access to selected group of resources

☐ All ☒ Organization

Access Control

Organization *

DevNet

Add Privileges

HyperFlex Cluster Administrator x

Server Administrator x

Organization *

default

Add Privileges

Read-Only x

Roles (Predefined User/Group Privilege Sets)

Account Administrator

- Complete access to all services and resources in Intersight. Can perform all administrative and management tasks, including claim and manage devices, create and deploy Server and HyperFlex Cluster profiles, upgrade firmware, perform server actions, cross launch devices, add and manage users and groups, configure Identity providers and more.

Read-Only

- Can view the dashboard, table views of managed devices, change current user preferences, and generate API keys. Cannot claim devices, add or remove users, configure Identity Providers, or perform any server actions.

User Access Administrator

- Can add and manage Users and Groups, view account details and audit logs, manage Identity Providers, roles, sessions, and API keys for non Account Administrator users. Cannot claim a device or perform any device management tasks. Cannot add or manage users or groups with Account Administrator privileges.

Device Administrator

- Can claim and unclaim devices, view device details, license status, and generate API keys. Cannot perform any other management or administrative tasks.

Device Technician

- Can claim devices, view device details, license status, and generate API keys. Cannot perform any other management or administrative tasks.

HyperFlex Cluster Administrator

- Can create, edit, deploy, and manage HyperFlex Clusters, view all cluster dashboard widgets, view cluster details, create HyperFlex policies and profiles, and launch HyperFlex Connect. Cannot claim devices.

Server Administrator


- Can view and manage UCS Servers and Fabric Interconnects, view all server and Fabric Interconnect dashboard widgets, perform server actions, view server details, launch management interfaces and the CLI, create and deploy server policies and profiles, and manage API keys. Cannot claim devices.

RBAC Summary

Privileges	Account Administrator	Read-Only (View Access only)	Device Technician	Device Administrator	User Access Administrator	Server Administrator	HyperFlex Cluster Administrator
Dashboard views	✓	✓				✓	✓
Servers Table view	✓	✓				✓	✓
HyperFlex Clusters Table view	✓	✓					✓
Fabric Interconnect Table view	✓	✓				✓ View details	✓ View details
Service Profiles	✓	✓				✓ Create Server Profiles	✓ Create HyperFlex Profiles
Policies	✓	✓				✓ Create Server policies	✓ Create HyperFlex policies
Devices	✓	✓	✓ Claim and view device details	✓ Claim, view device details, and delete devices		✓ View device details only	✓ View device details only
Alarms	✓	✓				✓	✓
Tasks	✓	✓	✓	✓		✓	✓
Global Search	✓	✓				✓	✓
Settings	✓	✓	✓ View Licensing status, Account details, and generate API keys	✓ View Licensing status, Account details, and generate API keys	✓ Audit logs, Sessions, Licensing, and Settings	✓ View Licensing status, Account details, and generate API keys	✓ View Licensing status, Account details, and generate API keys
Help	✓	✓	✓	✓	✓	✓	✓
User Profile	✓	✓	✓	✓	✓	✓	✓
Cross Launch of Element Managers	✓	✓				✓	✓

Organizations

- Settings->Access & Permissions ->Organizations
 - Enables multi-tenancy by placing devices into logical groups
 - Only Account Admins can create Orgs
 - Devices can be in multiple orgs
 - All devices are in the default Org
 - Devices in a Custom Org are also in the default Org
 - Organization column is in table views (e.g., Servers, Policies, Profiles)



Create Organization

Create an organization to manage access to your logical and physical resources.

General

Name *	Description
DevNet	Infra used in DevNet labs and events

Memberships

Custom All

Select devices to create a Custom Organization. Profiles and Policies that are created within a Custom Organization are applicable only to devices in the same Organization.

Search

63 items found | 50 per page | 2 of 2

<input type="checkbox"/>	Name	Status	Type	Device IP	Device ID
<input type="checkbox"/>	C240-FCH2023V33F	Connected	Standalone M4 Server	10.29.189.107	FCH2023V33F
<input type="checkbox"/>	C220-WZP22420B7P	Unclaimed	Standalone M5 Server	2001:420:282:202f:1...	WZP22420B7P
<input type="checkbox"/>	cc1ucsd.cisco.com	Connected	UCS Director	cc1ucsd.cisco.com	2cdd229f-2d83-4717-a9cd-efd...
<input checked="" type="checkbox"/>	C220-WZP2204097Z	Connected	Standalone M5 Server	172.28.224.106	WZP2204097Z

Intersight Identity Providers and SSO

- Intersight SaaS and the Virtual Appliance support external Identity Providers (IdPs)
- IdPs supporting SAML 2.0 can be configured in Intersight to authenticate users
 - Intersight supports use of IdP groups so that individual users can authenticate through their group permissions (does not require per user config in Intersight)
- [Video demo of SSO setup](#)

Add Identity Provider

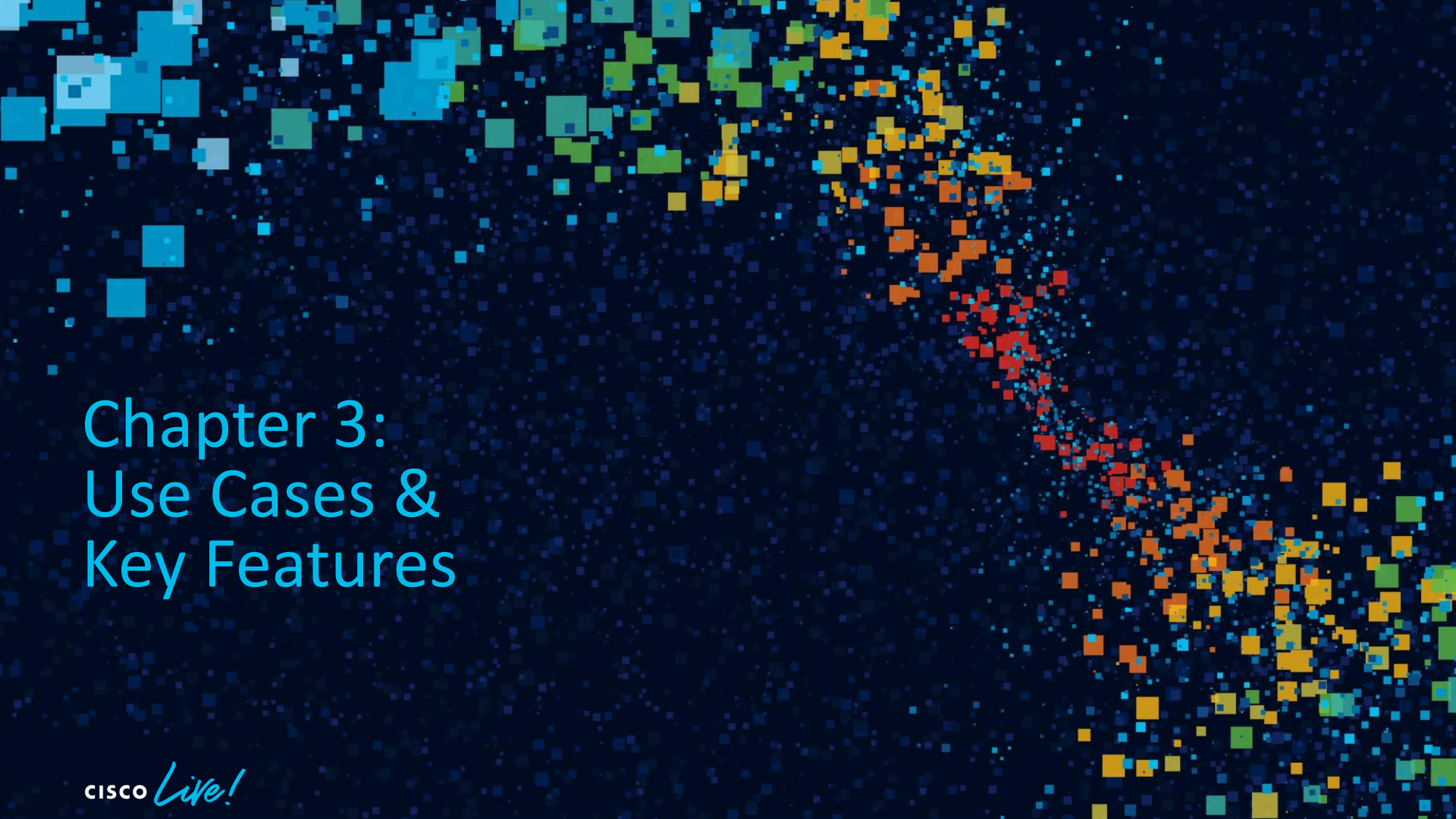
Name *
T

Domain Name *

Organization IdP Metadata *
Browse No file selected

Cancel Save

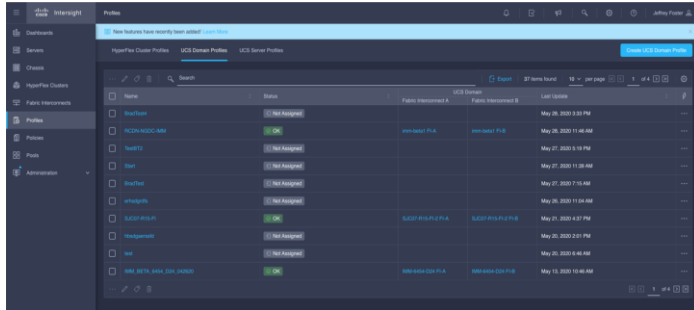
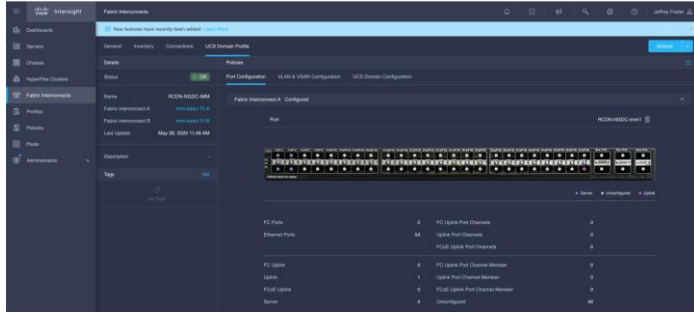
Click Name
Enter a name for the Identity Provider.
6 of 9 Continue

The background is a dark blue field filled with numerous small, semi-transparent squares and dots in various colors including light blue, green, yellow, orange, and red. These elements are scattered across the frame, with a higher concentration of yellow and orange squares forming a diagonal streak from the top right towards the bottom right.

Chapter 3: Use Cases & Key Features

Intersight Managed Mode

Intersight Managed Mode Summary



What is it?

- Brand new software stack (Alternative to UCSM)
- Foundation of UCS Management
- Standards based approach

Why are we doing it?

- Unify management experience
- Standardize our platform
- Enable automation

How is this rolling out?

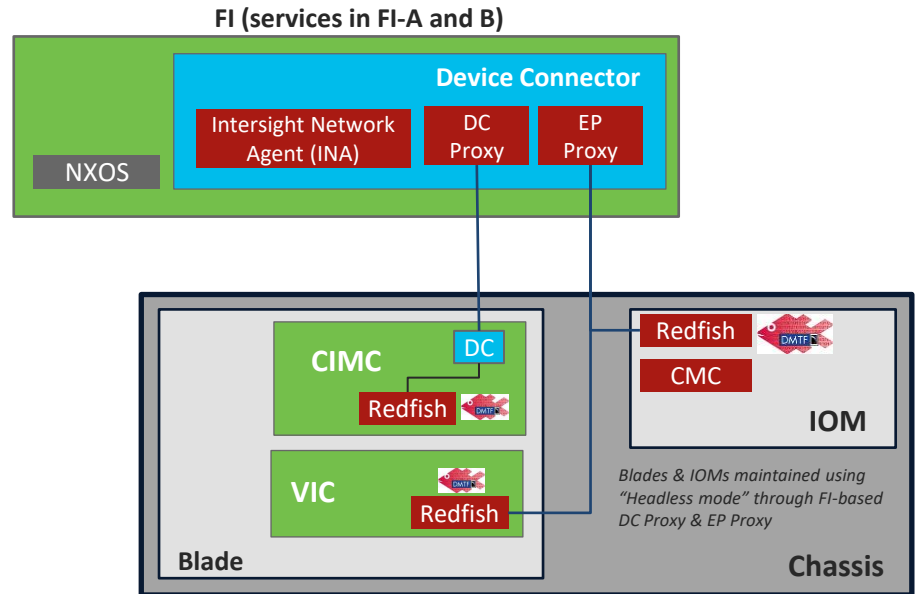
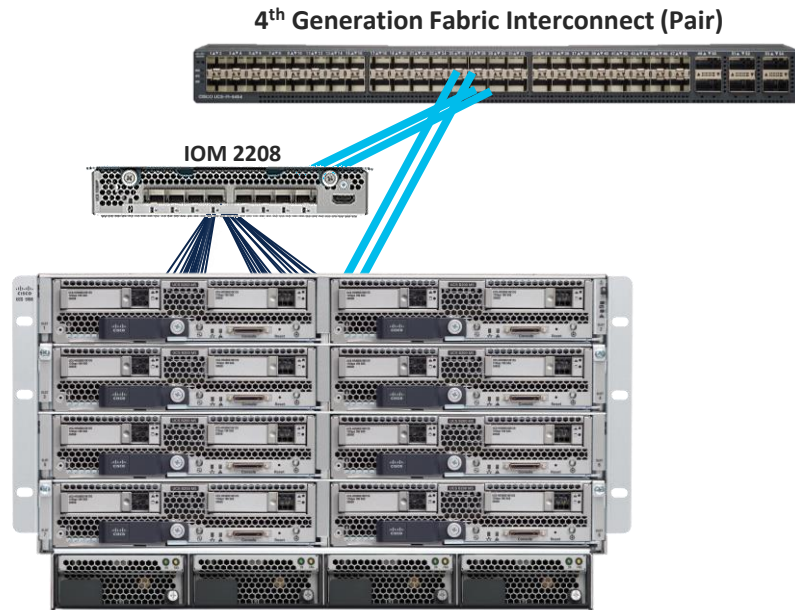
- Customer Tech Preview enabled now!
- Will continue to be enhanced until Tech Preview moniker is removed in Intersight

Intersight Managed Mode

Enabling Modernized Compute



Intersight



Intersight Managed Mode Demo

Intersight Firmware Updates

Intersight – Firmware Upgrades

...				
Search				
<input type="checkbox"/>	Power On	Health	Management IP	Model
<input type="checkbox"/>	Power Off	✓	Unavailable	UCSB-B200-M4
<input type="checkbox"/>	Power Cycle	✓	Unavailable	UCSB-B200-M4
<input type="checkbox"/>	Shut Down OS	✓	Unavailable	UCSB-B200-M4
<input type="checkbox"/>	Hard Reset	✓	Unavailable	UCSB-B200-M4
<input type="checkbox"/>	Reboot IMC	✓	Unavailable	UCSB-B200-M4
<input type="checkbox"/>	Turn On Locator	✓	Unavailable	UCSB-B200-M4
<input type="checkbox"/>	Turn Off Locator	✓	Unavailable	UCSC-C220-M5SX
<input type="checkbox"/>	Upgrade Firmware	✗	172.22.249.75	UCSC-C220-M5SX
<input type="checkbox"/>	D23-UCS1-1-8	✓	10.29.131.185	UCSB-B200-M3
<input type="checkbox"/>	D23-UCS1-1-7	✓	10.29.131.185	UCSB-B200-M3
<input type="checkbox"/>	D23-UCS1-1	⚠	10.29.131.185	UCSC-C240-M5S
<input checked="" type="checkbox"/>	C240-WZP21340YNQ	✗	10.29.131.134	UCSC-C240-M5SX

Upgrade Firmware

Network Share Utility Storage

NFS CIFS HTTP/S

Remote IP *

Remote Share *

Remote File Name *

Firmware will be installed and the device will be rebooted immediately.

Cancel

Upgrade

Upgrade Firmware

Network Share Utility Storage

Utility storage includes FlexUtil cards for the M5 servers.

Firmware Version *

3.1(2b)

Image Name

ucs-c240m5-huu-3.1.2b.iso

Release Date

October 5, 2017

Size

487 MB

Supported Models

UCSC-C240-M5S, UCSC-C240-M5L, UCSC-C240-M5SX, UCSC-C240-M5SN

Description

Cisco UCS Host Upgrade Utility

On clicking upgrade below, firmware download to FlexUtil will begin immediately. Installation will start on the first boot after the download has successfully completed. Installation can be initiated once the server Firmware Status is "Ready for Upgrade" by performing a Host Reboot on the server.

Cancel

Upgrade

- Firmware upgrades available via Network Share or Utility Storage
- Network upgrades reboot host immediately and begin upgrade
- Utility Storage upgrades are staged – firmware is downloaded and then upgrades on next reboot

Legacy UCS FW Upgrades – From Intersight

- Intersight Essentials Tier now includes ability for legacy UCS Domains to have FW (Infrastructure, Blade, Managed C-Series, Managed S-Series) upgrades driven directly from Intersight
 - Cisco UCS C-Series M4 and M5 servers that are configured in standalone mode.
 - Cisco Fabric Interconnect-attached UCS B-Series, C-Series, S3260 M3, M4 and M5 servers.
 - Cisco Fabric Interconnect-attached Cisco UCS S3260 chassis
 - Cisco UCS Fabric Interconnects Series 6200, 6300 and 6400 in a Cisco UCS Domain.
- Workflow Driven, Direct Upgrades – not Policy Model Driven
- UCSM/UCS Central Service Profiles cannot be attached to Updating Templates nor have assigned FW policy (conflict with new FW pushed from Intersight)
- Maintenance User-Acks automatically a part of the Intersight FW Upgrade Workflow
- Currently not available for the Intersight Connected Virtual Appliance

Intersight Firmware Upgrade Demo

Intersight Support: Connected TAC

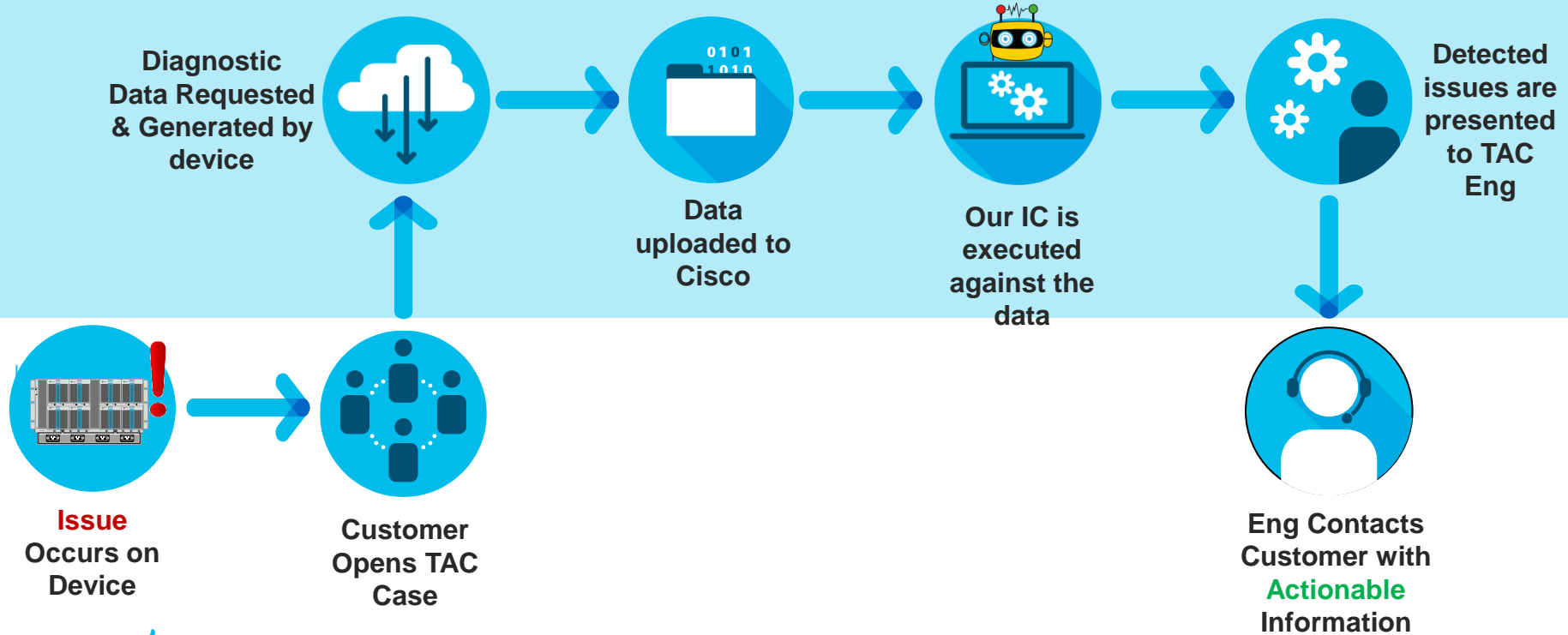
“No Customer should ever be impacted by an issue we know about or could predict”

Datacenter TAC's North Star

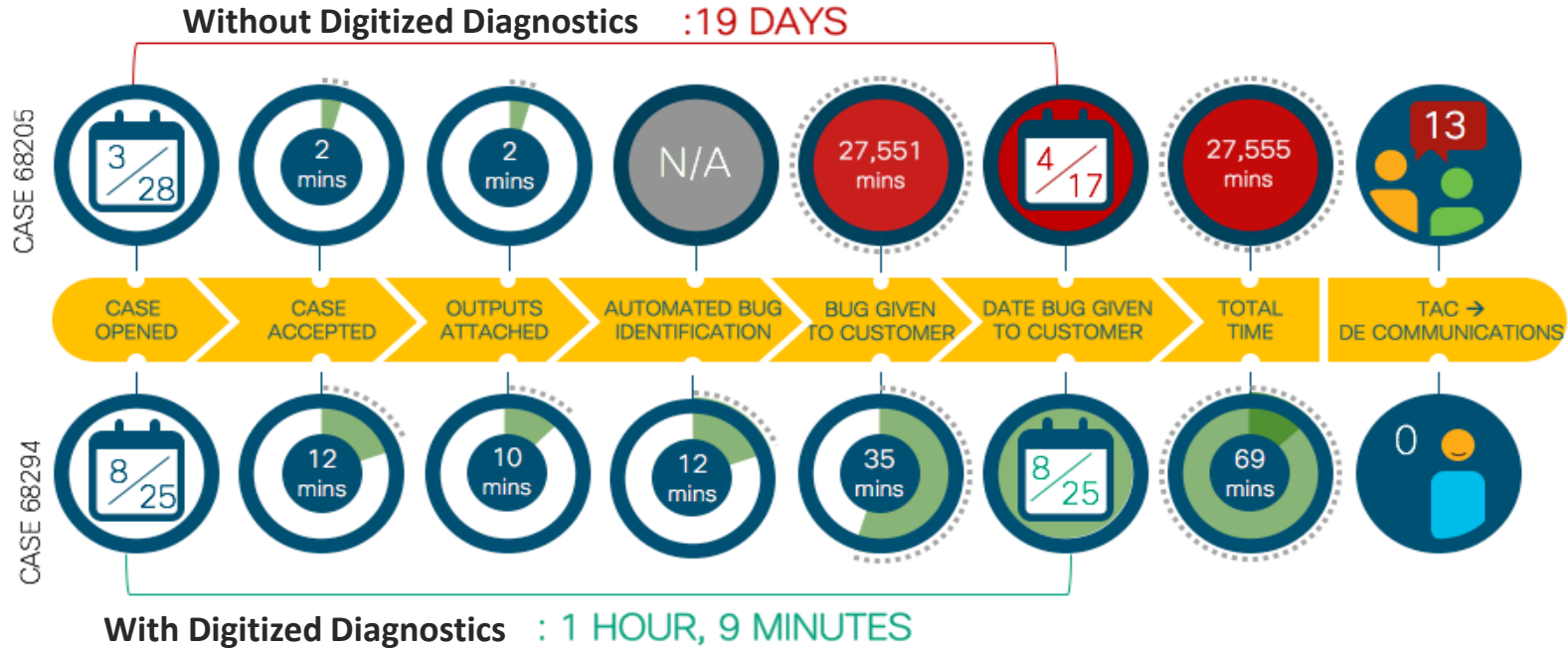


Connected TAC Workflow

Automatic Actions



Accelerate Issue Resolution: From Days to Minutes



Examples – Time Saved



Case opened



Diagnostic data
automatically collected



Diagnostic results
automatically gathered



RMA delivered
and part replaced

Root Cause: Part Failure – Average time to Solve: 1 day

Case opened:
XXXXXX162
2019-03-DD 08:11



+11 Minutes



+13 Minutes

0:00 Hours Failure
+1:59 Hours (RMA)
+7:06 Hours (DIMM replaced)

Root Cause: Software Defect – Average time to Solve: 2.1 days

Case opened:
XXXXXX244
2019-03-DD 01:25



+12 Minutes



+16 Minutes

Total: 28 minutes from
case opening to solution
(SW defect)

Advisories (CVEs)

- Intersight displays devices impacted by Cisco Security Advisories
 - Advisories available in the menu bar of the UI
- CVE IDs and links for more information are provided
- User can acknowledge (hide) and unacknowledge Advisories



Security Advisories > CVE-2017-5715

1957 353

2

David Soper

Details	General
Severity Medium	CPU Side-Channel Information Disclosure Vulnerabilities
CVE CVE-2017-5715	
Published Oct 8, 2019 9:01 PM	
Last Update Oct 9, 2019 2:16 PM	

Acknowledge

Details

To learn more about this security vulnerability, the affected products, and other details, see:
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180104-cpusidechannel>

Affected Devices (29)

29 items found 10 per page 1 of 3

Search

Name	Type	Model / Type	Firmware / Version
CC7UCS1-3-4	Server	UCSB-B200-M4	3.1(1e)
CC7UCS1-1-5	Server	UCSB-B200-M4	3.1(26i)

Summary

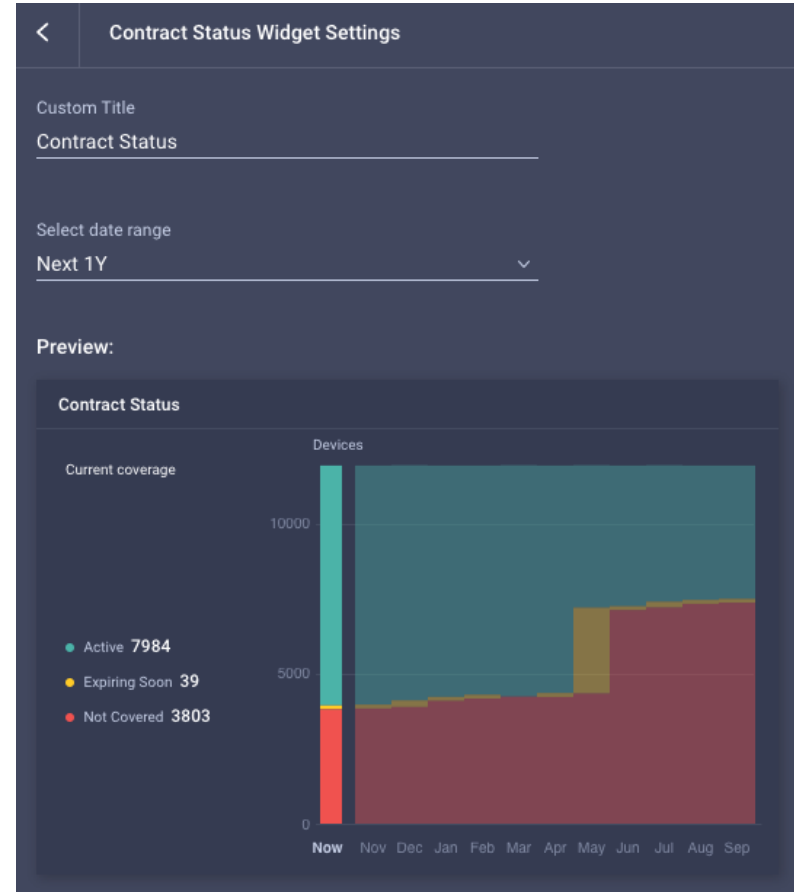
Details

Affected Devices (29)

Workarounds/Solutions

Service Contract Status

- Dashboard Widget and Table View column display current Contract Status
- Categories: Active, Expiring Soon (next 30 days), Not Covered
- Widget provides custom date range for planning (1 or 5 year status displayed)



Intersight – Next Steps for Connected TAC



**Diagnostic Data
Following RMA**



**Streaming data
during case lifecycle**



**Direct, live CLI
Interaction**

Thank you



Possibilities

#CiscoLive