The bridge to possible

Cisco UCS Security

Architecture, Operations and Innovations

Chris Dunk, Principal Engineer, Cisco Networking - Compute

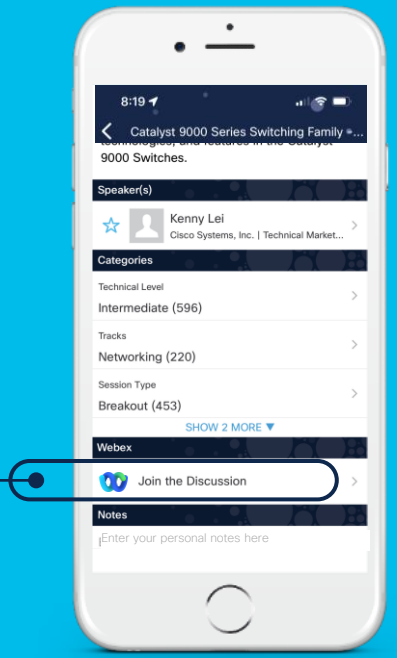
Cisco Webex App

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 until February 24, 2023.

Agenda

- Cisco secure development overview
- Server security foundation and protection
- Cisco innovative system wide security design
- Intersight secure cloud architecture
- Summary

Cisco UCS compute products are designed/tested to Cisco's rigorous security framework, using the latest technologies for prevention. It is part of our Culture and Philosophy

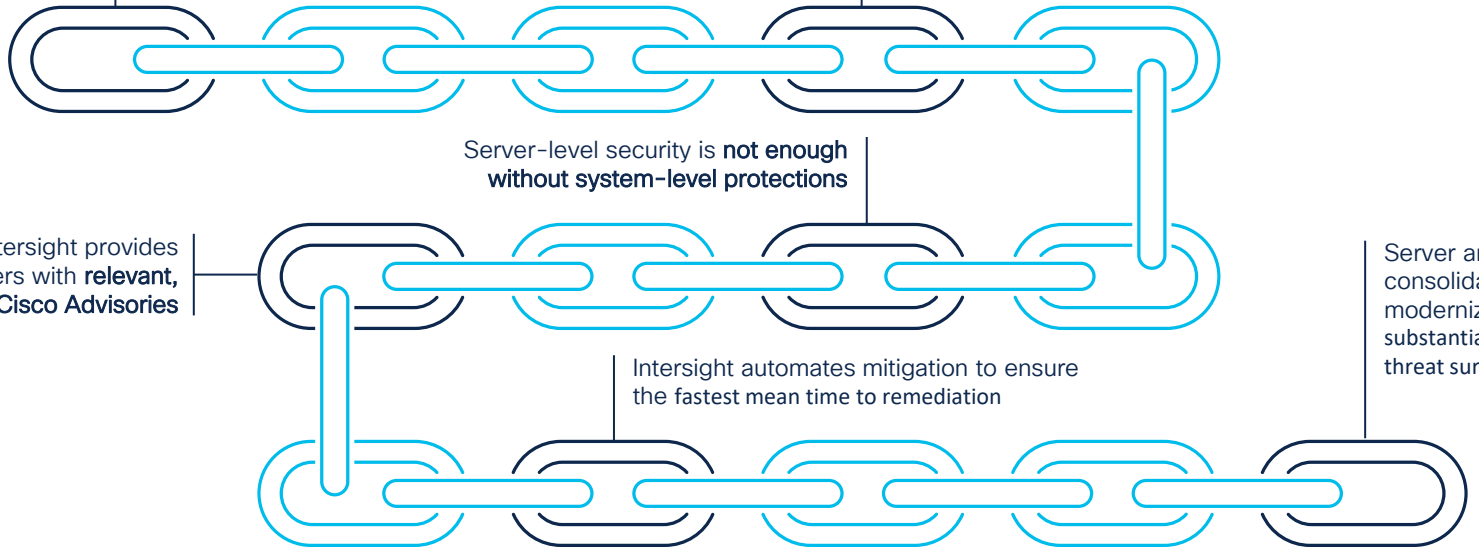
CISCO Trustworthy Systems

Cisco Security Culture

- Supply Chain Management
- Open Source Registration
- Security Training
- Threat Modeling
- Product Security Baseline
- PSIRT Advisories

Cisco UCS Security

Security is only as strong as the weakest link



Cisco UCS Security

Design to Operations – Protections at Every Level

Cisco's security approach begins in the design stage

The server itself contains:

- Chassis intrusion detection
- Fused security keys
- Immutable, multi-layered hardware roots of trust
- Intel Boot Guard – enhanced trust via Intel PCH

Rigorous supply chain certification, evaluation, auditing ensures authentic, secure componentry

At the system level, UCS builds in:

- Multi-stage secure access and authentication
- Granular role-based policies and authentication
- Multi-factor authentication and encryption
- Cisco InfoSec adherence
- BIOS scrub policies
- Trusted compute pools

Cisco Secure Development Lifecycle

Cisco's security approach starts at design time

Design Stage

- Organizations need the comfort of knowing their technology is secure
- Cisco infuses security and privacy awareness into the entire development process
- We call this the Cisco Secure Development Lifecycle (Cisco SDL)
- Cisco SDL employs a secure-by-design philosophy throughout the product life cycle
- Because the security landscape always evolves, so does Cisco SDL
- We constantly review the latest attacks to ensure our security's success

Cisco Secure Development Lifecycle – CSDL

Foundational Policies, Processes, Workflow Tools, Technologies, and Training

Product Security Baseline
Defines security requirements across all on-prem products

Cloud Controls Framework
Defines Security requirements across all cloud offerings

PSB

CCF

ThreatBuilder

TPSCRM

Cisco Threat Modeling Tool
Security threat detection and mitigation

Third Party Software Compliance and Risk Management
Software discovery & management tools

Cisco Security and Trust Organization (S&TO)

Driving Security Processes and Technologies Deep into UCS Products

- **ASIG – Advanced Security Initiative Group**
  White hat engineers focused on offensive security – Internal pen testing
- **GCC - Global Cloud Compliance**
  Implements the Cloud Controls Framework (CCF) towards accelerating product certifications for maximum market access
- **PSIRT – Product Security Incident Response Team**
  Manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks
- **SVIC – Security Visibility & Incident Command**
  Provides visibility into security and compliance, performs incident response, and drives root cause analysis to improve Cisco's security posture.
- **VCS – Value Chain Security Trust Office**
  Drives Cisco's supply chain security and anti-counterfeiting technology

Cisco holistic approach to value chain security

We continually assess, monitor, and improve third-party vendor security

Physical security

Camera monitoring, security checkpoints, alarms, and electronic or biometric access controls

Logical security

Encryption, materials and failure analysis, and segregation and scrap weight validation

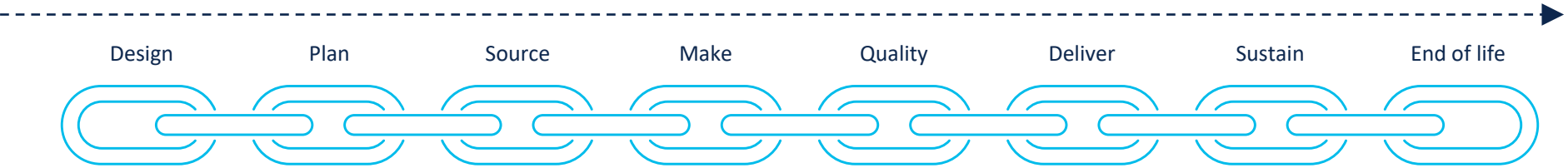
Security technology

Counterfeit detection, terminate functionality, or identify non-authorized components or users (smart chips, data-extracting test beds, and proprietary holographic or intaglio security labels)

Information security

Remote access limitation, configuration management, network segmentation, multi-factor authentication, and data classification

Security at every life cycle stage



UCS Server Security Protection

Cisco Compute Security

Proven Protection for Your Infrastructure

SECURE Anti-Tampering	AUTHENTICATE Anti-Counterfeit	INTEGRATE Across Cisco Solutions	CONTROL Supply Chain & Beyond
• Prevents Malicious FW and BIOS from booting • Multi-Point Secure Installation & Boot with Cryptographically Signed Firmware • Multiple HW Roots of Trust • Secure FW and BIOS verification • Trusted Image failsafe • NIST SP800-147b	• Prevents transfer of insecure/Fake/ Counterfeit HW • Anchored to Cisco Authority • Guarantees Authentic Cisco HW and Code • Continuous Checks with HW and FW handshake • Continuous Assurance of Authenticity	• Secure Boot Anchors another trust level into Cisco HW • Cisco VIC brings additional security over off-the-shelf adapters • Advanced Fabric Security • Enterprise RBAC • Policy-based Security • UCS Intrusion Detection • Disk/BIOS Scrubbing Policy	• Rigorous Cisco Secure Development Lifecycle Methodology (CDLM) • Dedicated Cisco team for threat modeling analysis • Cisco controls FW dev/access/signing • Cisco controls Secured Debug capability • Secure Network Communication

Cisco UCS Security

Design to Operations – Protections at Every Level

Cisco programmatic security measures

Physical mitigations

Multi-tier and end point protection

Access and authentication

Security communications

Policy driven control and accountability

Intersight/ Cisco advisories

Security is designed in from the start, not bolted on and every supplier is held to the highest standards.

Server is protected from malicious activity by bad actors and accidental misconfigurations.

Security controls and policies at every level of infrastructure provide hardware attestation, integrity, and integration with partner solution security features.

UCS fits seamlessly into security best practices with multi-factor authentication, single sign-on, and secure APIs.

UCS provides customizable, secure, and auditable internal communication within the system through encryption, detailed logging, and alerting.

Reduced opportunity for malicious or erroneous exposures and alterations by restricting access to sensitive data and controls.

Increase situational awareness and shorten vulnerability windows through targeted advisories and mitigation automation.

Cisco UCS Versus Widespread Industry Vulnerabilities

Heartbleed
UCS OpenSSL version used not vulnerable

SolarWinds/FireEye
Windows exploit
UCS utilizes hardened Linux
Secure supply chain – not vulnerable

Log4J
UCS Manager/CIMC/Intersight not utilized

Meltdown / Spectre
Servers vulnerable – CPU microcode/OS update
FI/IOM/VIC not vulnerable – no attack vector

Shellshock
UCS Manager & CIMC vulnerable
Fixes available within month of disclosure

WannaCry/NotPetya
Windows exploit
UCS utilizes hardened Linux
Not vulnerable

Apache Struts
CIMC/Intersight/UCSM no Struts

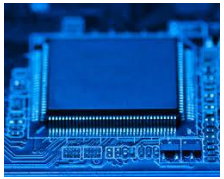
Drupalgeddon
UCS doesn't utilize Drupal

Ripple20
UCS doesn't utilize Treck IP stack

Cisco Security Innovations and Tools

Hardware Anchored Root of Trust and Cryptographic anchored identity

Assure uncompromised Cisco BIOS and OS, withstand physical attacks and parts replacement/tampering



FPGA
Immutable Microloader and Security Keys

Secure Chip
Immutable Identity
Secure Key & Object Storage

Cisco Common Security Modules – Set of modules focused on secure communications and storage of information.

Product differentiation, reduced development and certification costs, higher quality and faster response times to vulnerabilities across Cisco products

CiscoSSL

CiscoSafeC

FIPS Object Model

UEFI Security Boot Shim

CiscoSSH

Cisco Runtime Defenses – Use compiler, kernel, and hardware capabilities to reduce exploitation possibilities during runtime

X-Space

ASLR - Address Space Layout Randomization

SSP – Stack Smash Protection

OSC – Object Size Checking

Cisco Server-Level Security

Security is built into every UCS server

UCS server security

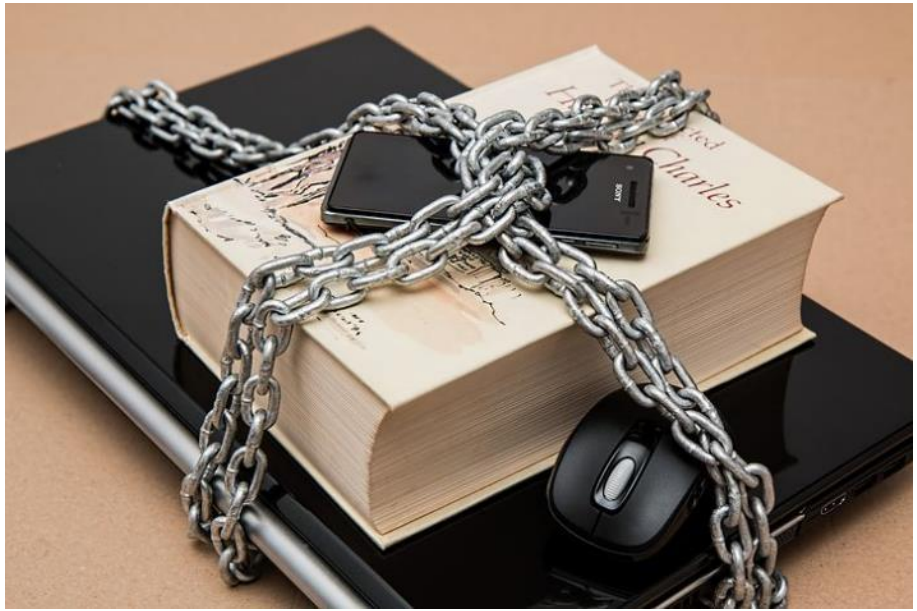
Tainted & counterfeit solutions

- Multi-point secure installation and boot with cryptographically signed firmware
- Immutable, multi-layered hardware roots of trust
- Both firmware and BIOS verification
- FW Update runs under UEFI Secure Boot (using Cisco owned keys)
- Innovative anti-counterfeit measures

Compliance

- NIST SP800-147b-compliant firmware authentication controls on both BMC and BIOS images
- FIPS 140-2 SW Compliance

Secure Boot Starts from Protected Code



Cisco “HW Root of Trust”

Cisco IMC secure boot is handled via HW Root of Trust. Immutable keys are embedded in write-protected devices on every UCS server. Additionally, system BIOS secure boot is also encoded at manufacturing, and Cisco resolves both Firmware and BIOS via HW Root of Trust measures. Cisco also employs anti-counterfeit measures to ensure the physical hardware is authentic and signed by Cisco.

Server-Based Security

UCS M6 Generation Servers

- Anti-Tampering with HW anchored root of trust
  - Cisco IMC: FPGA secure boot
  - BIOS: Intel Boot Guard or AMD PSB
  - OS: UEFI secure boot
- Anti-counterfeit with cryptographic anchored identity
  - Cisco IMC: Immutable ACT2 module

UCS M7 Generation Servers

- Anti-Tampering with HW anchored root of trust
  - Cisco IMC: built-in secure boot
  - BIOS: Intel Boot Guard or AMD PSB
  - OS: UEFI secure boot
- Anti-counterfeit with cryptographic anchored identity
  - Cisco IMC: S&TO enhanced TPM with secure tracking through the supply chain

Cisco Security Protecting the System

Secure & Authenticate

Single Sign-on (SSO)

Multi-factor Authentication (MFA)
Users and managed endpoints

Granular Role-based
Access Control (RBAC)

User Access and Authentication
Assignment of authorizations

Anti-Tampering

Anti-Counterfeit

Intel Boot Guard

AMD Platform
Secure Boot

Server Security protection firmware and booting

Advise & Identify

Policy based enforcement
Drift Prevention

System Lockout

System wide auditing and alerts

Intersight Security Advisories

Node/chassis intrusion detection

Restore & Mitigate

System Erase

Service profile statelessness

BIOS recovery and redundancy

UCS M6/M7 Security Benefits Overview

1. Intel Boot Guard
   AMD Platform Secure Boot
2. Trusted Platform Module (TPM 2.0)
3. Chassis Intrusion Detection
4. Intel Optane DCPMM with Encryption
5. FIPs and Common Criteria modes
6. KMIP Integration
7. Account Lockout
8. IMC FPGA Based Root of Trust or S&TO TPM
9. HTML5 Based UI vs Flash
10. ACT 2 HARSA Certificate

Cisco Global System Security and Control

UCS System Security Innovations

Securing Internal Endpoints

Establishes Ongoing Trust Between BMC & Components
Endpoint Authentication and Attestation
SPDM – Security Protocol and Data Model
MCTP over PCIe VDM Communications

Secure Management Models

Flexible per customer's security requirements
OnPrem - Fully Air-Gapped, Hybrid Connected, Cloud
CIMC / UCS Manager, Intersight – SaaS/CVA/PVA

Intersight Security Advisories

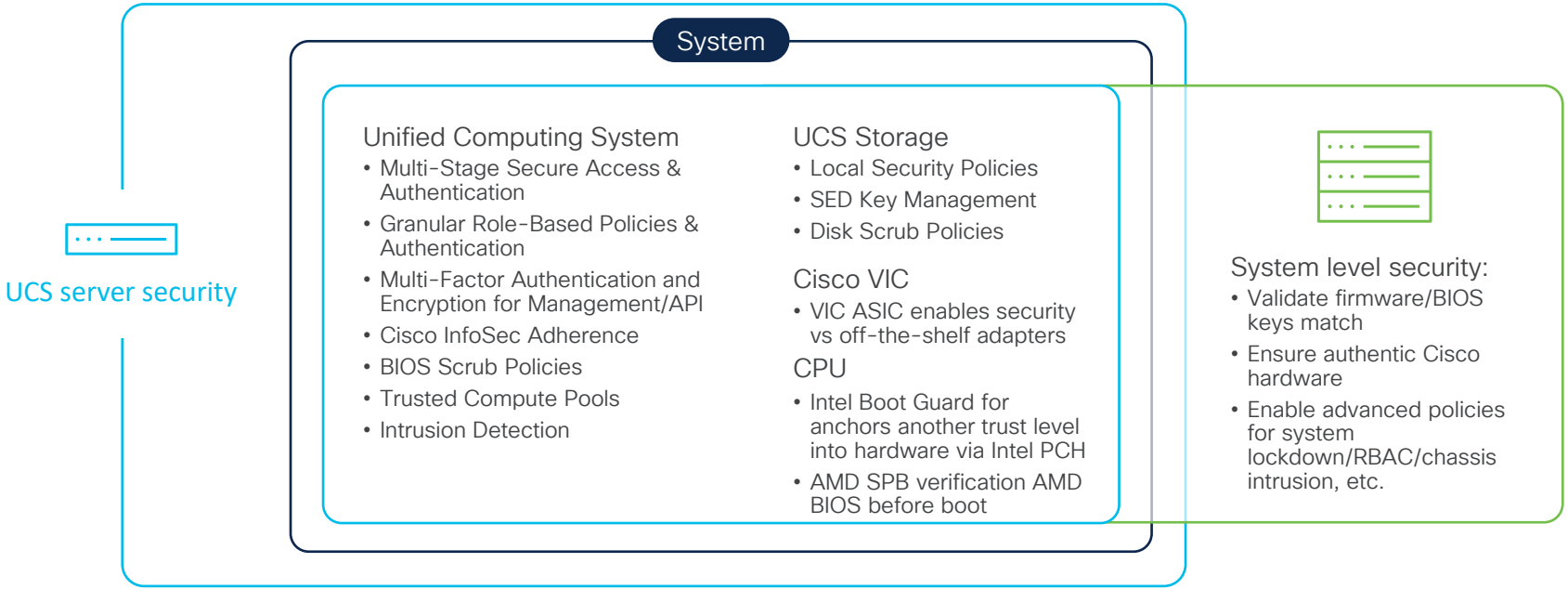
Proactive alerting of security advisories
CVE IDs, devices impacted, and severity
Drilldown for comprehensive information

Template, Policy, & Profile Configuration

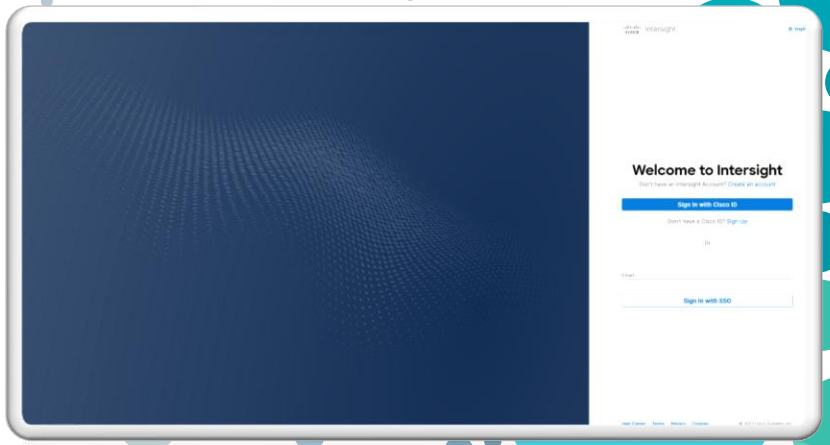
Security through physical and logical abstraction
Associating repeatable secure baselines to target systems
Centralized add/change/delete reducing audit footprint

Cisco System-Level Security Innovations

Security is also built in at the system level



UCS Intersight Cloud Security



cisco Live!

Intersight Privacy and Security Standards

- All Data sent to Intersight is Encrypted
- All Data exchanged via HTTPS
- Connections initiated outbound from devices
- Devices can use HTTPS proxy servers to avoid direct internet access

- UCS Devices verify the authenticity of Intersight portal with signed certificates
- Portal must present a signed Certificate Authority (CA) via X.509 digital certs
- Will connect only if presented with signed certificate

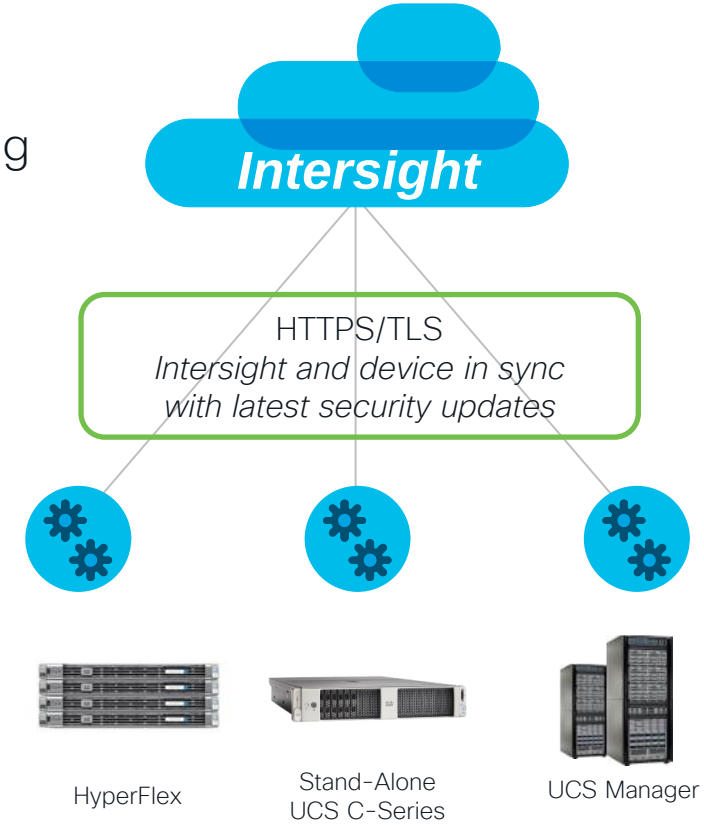
- Meets/Exceeds InfoSec
- Long term data stores with Data at Rest encryption
- All user access to portal and account data authenticated
- Firewalled user accounts; Intersight services can't access across accounts
- Vault used for key/access and Intersight Admin (Cisco Admin access)

Intersight Layered Security

Layered security architecture includes the following

- Industry Standard protocols (e.g., HTTPS)
- Encryption of all data during transport
- Management/Production network separation
  - No production network data flows to or from Intersight
- Identify, Authenticate, and Authorize
  - During claim process and all subsequent transfers

Device drives all management tasks (No device inbound connections)



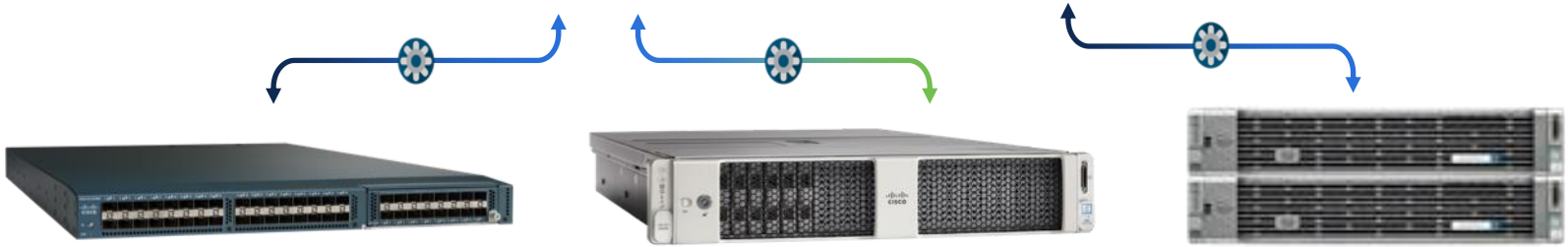
Device Connector: Overview

A very light and autonomous piece of software allowing:

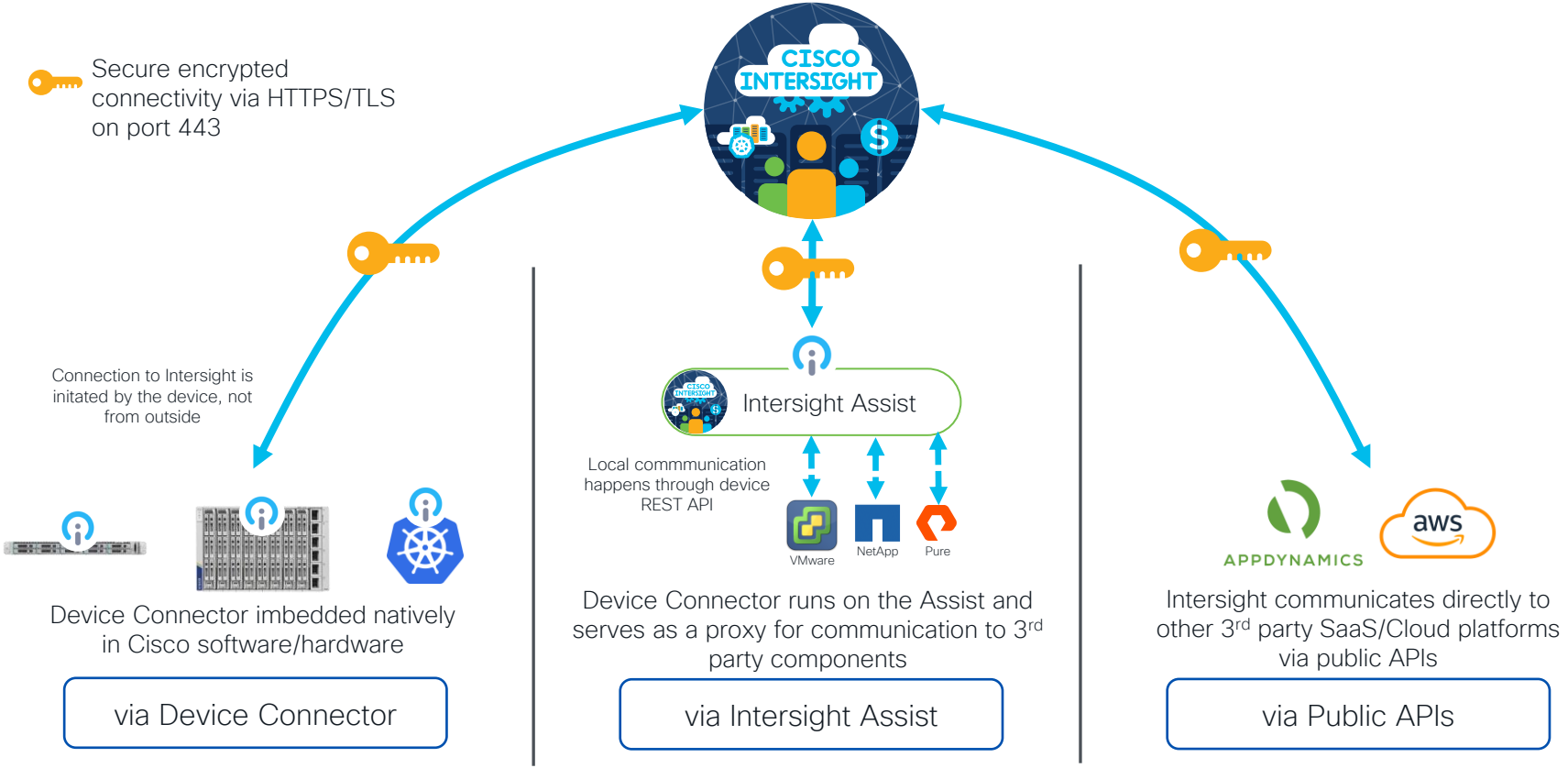
- Communication with the Intersight portal, wherever the portal is.
- Capability of inserting tasks / calls against the infrastructure (UCS Manager, Cisco IMC Software, HyperFlex, UCS Director) via the pluggable / extensible framework

Key Features

- Bundled with Firmware
- Embedded Product Feature
- Secure Communications
- Self Updated
- Autonomous Check-In



Managed Device / Service Communication



Note: Intersight Appliance can also act as Intersight Assist

Intersight Device/Browser Connectivity

Cloud Portal

User Access

- Cisco.com used to create accounts
  - Becomes the “root” user
  - Invite other Cisco.com or SSO users

Device Access

- DNS required - must resolve **svc.ucs-connect.com**
- Intersight always provides CA signed x509 certificate
- Two Factor Authentication for device claim
  - Device Serial Number
  - Device Claim Code

User Browser Traffic

HTTPS (port 443) or proxy

Certificate Authority (CA) Signed Certificate

HTTPS (port 443) or proxy

Device Traffic

Certificate Authority (CA) Signed Certificate

TLS v1.2 (or higher)

HTTPS (port 443) or proxy

Outbound Initiated Only (from Device)

Off Premises

1. Operations/ Administration

Customer Premises

1. Account Setup/Creation
2. Device Claiming
3. Operations/ Administration

Fabric Interconnect Device Connector

C-series (IMC) Device Connector

HX Device Connector

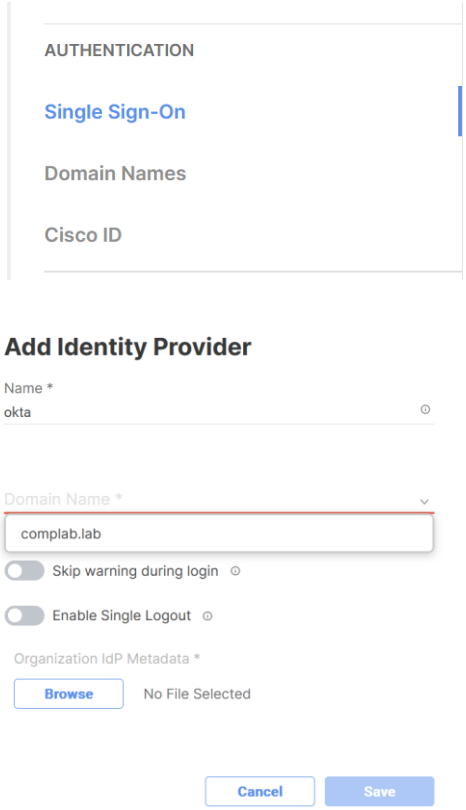
Intersight Identity Providers and SSO

SSO allows using corporate credentials instead of Cisco ID

Multi-Factor Authentication on Cisco ID users

Identity Providers (IdPs)

- Cisco SSO or SAML 2.0 with Intersight SaaS
- LDAP/AD or SAML 2.0 with Intersight Virtual Appliance



Intersight Role-Based Access Control

Resource Groups

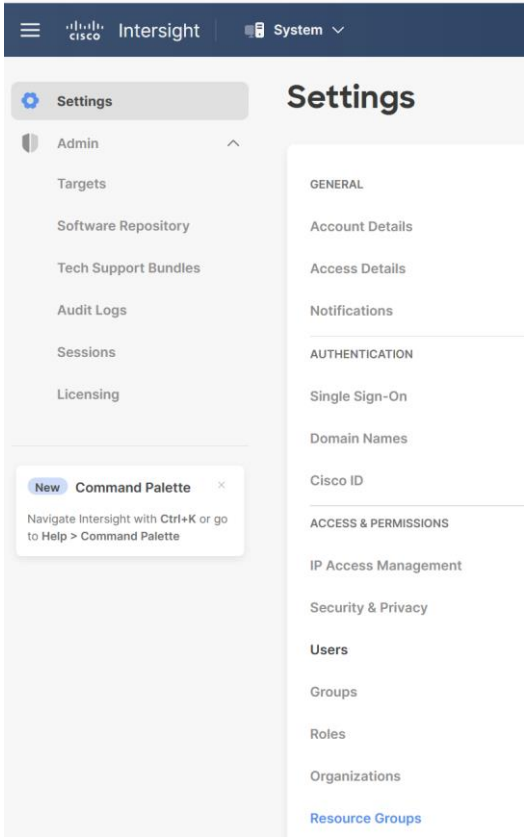
- Collection of managed resources (targets)

Organizations

- Enables multi-tenancy by placing devices into logical separated resource groups

Roles and Privileges

- System defined or user defined roles
- Roles are tied to sets of privileges to perform operations specific to a role
- Privileges can be based on areas of responsibility
  - UCS Domain, Virtualization, Storage, Network

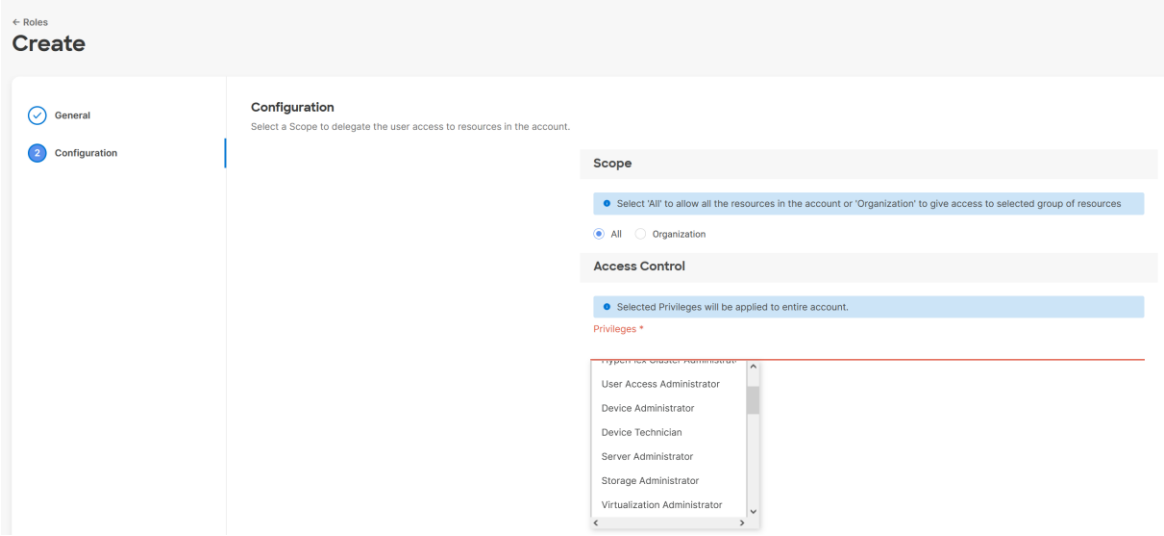


Video Demo: [Cisco Intersight Organizations and Role-Based Access Control - YouTube]

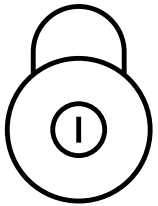
Setting up Roles and Privileges

System->Settings->Roles

- System Defined Roles created by default in every account
- 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



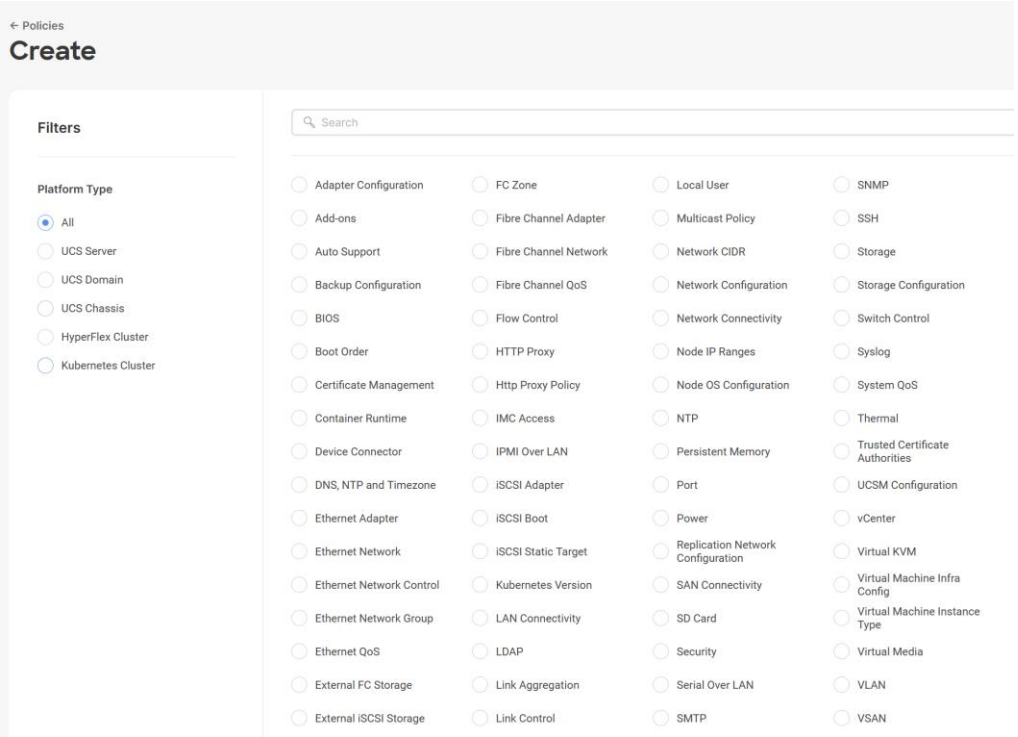
UCS Policies and Security



Policies = Security Rules

Policies enforce configuration settings on endpoints

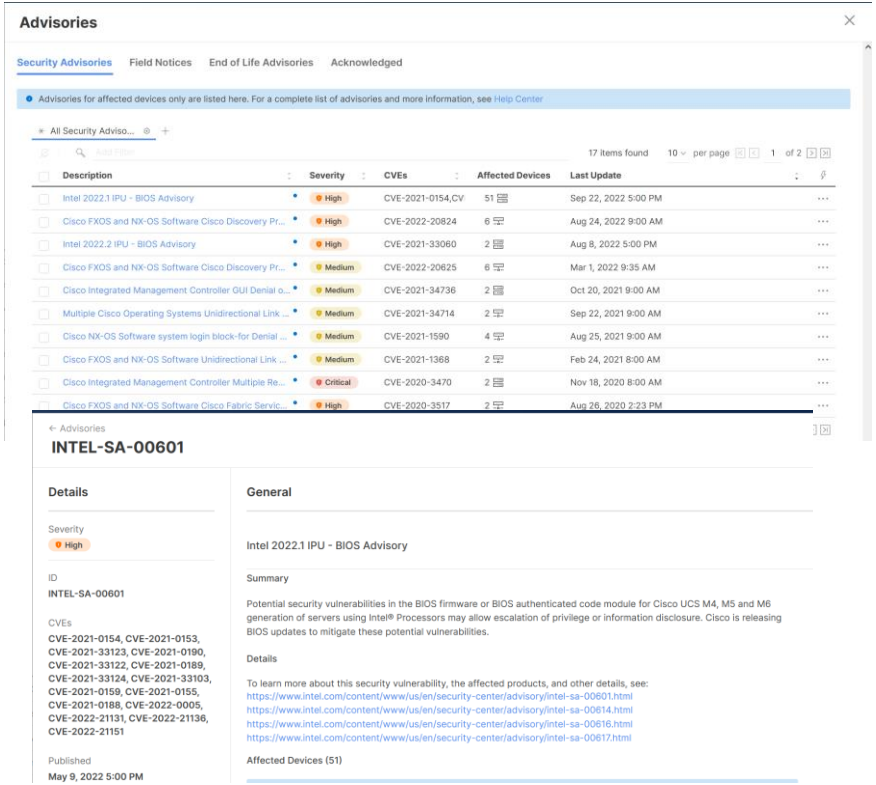
Cannot change without explicit authorization



Intersight Security 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 un-acknowledge Advisories



Intersight Compliance/Certifications

The Intersight infrastructure is colocated in tier-1, SAS70 type II / SSAE16 certified datacenters

Intersight meets or exceeds InfoSec's requirements for a wide range of Security Certifications including the following:

- ISO 27001:2013 and ISO 27017:2015
- SOC 2 Type 2, SOC 3
- FIPS 140-2

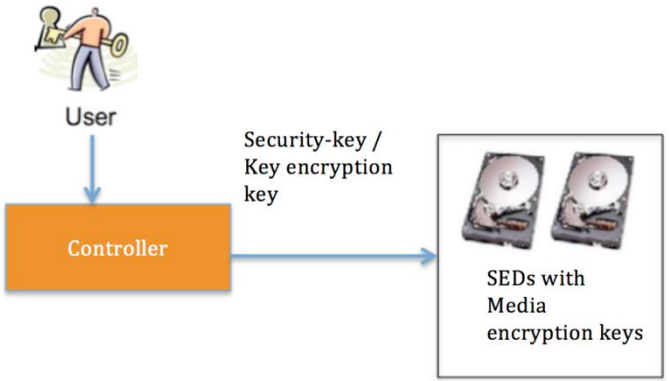
Cisco Integrated Management Controller / UCSM

Key Management Interoperability Protocol (KMIP) Integration with SEDs

Local vs Remote Key Management

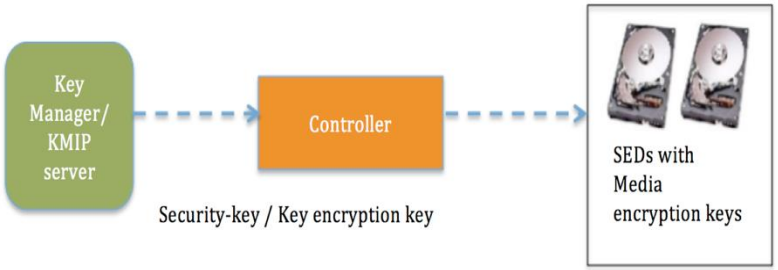
KMIP Local Key Management

- Security key identifier and key stored locally
- The SED security key is provided by the user
- User is responsible for remembering the key information



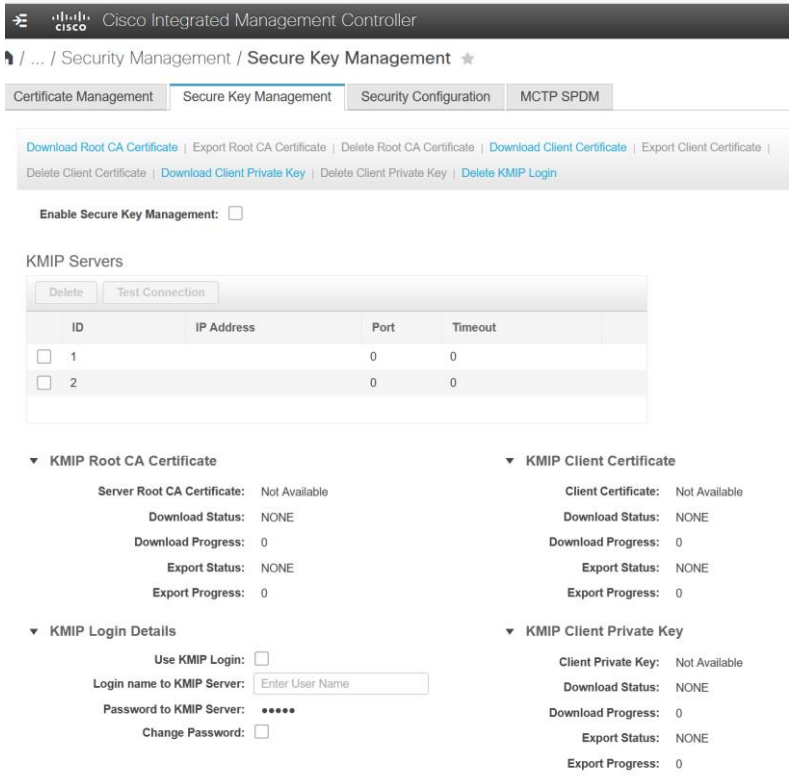
KMIP Remote Key Management

- The security key is created and fetched from a KMIP server
- User's responsibility is to configure the KMIP server on CIMC
- Key manipulation is completely on the KMIP server side



CIMC Key Management

- Cisco IMC contains integrated KMIP client that communicates with KMIP Server
- KMIP client/server uses TLS to negotiate mutually authenticated connection – client and server must have access to certificate information
- KMIP is an OASIS standard – Organization for the Advancement of Structured Information Standards – same consortium handling XML
- Compatible with any KMIP compliant key manager – official support for Safe Net and Vormetric



Summary

Cisco UCS Security

Design to Operations – Protections at Every Level

Cisco security culture

Cisco Security Development Lifecycle Process

Layered Value Chain Security Approach

Constant Threat Modeling and Scanning

Policy driven control and accountability

Policy Based Configuration Consistency

Auditing Controls and Reporting

Role-Based User Groups and Privileges

Communications

External and Internal Alerting, Logging, Reporting

Customizable Secure Communication Transports

Common Criteria and FIPs Security Modes

Access and authentication

Multi-Factor Authentication

Certificate Based Access

Single-Sign-On and Legacy Systems

Multi-tier protection

Continual Hardware Root of Trust Hardening

System and BMC Secure Boot

Industry Leading Endpoint Protection

Physical mitigations

Chassis Intrusion Detection

Locking Security Bezel

Fused Security Keys

Cisco UCS Security Team – Many Facets

Bringing it all together

Features / Functionality

Technology updates and deprecation
Feature submission
Requirement definition
Design and usability

Compliance / Regulations

Tracking and research
Cisco Product Security Baseline (PSB)
Project management
Domain definition
Test bed acquisition and delivery

Vendor Management

Technology reviews
Feature requests, design, usability, integration

Proactive and Reactive Remediation

Customer vulnerability reports
Industry disclosures
Cisco Product Security Incident Response Team (PSIRT)
UCS Quality Assurance

Education, Communication, Coordination

White papers
Mailer queries
RFP responses

Presentations
Multi-team coordination
Documentation
Standards bodies

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

The bridge to possible

Thank you

cisco Live!

CISCO Live!

ALL IN