



The bridge to possible

Automation & Orchestration Strategies for the Cloud-First Enterprise

Dave Malik, Cisco Fellow, CTO & Chief Architect
Customer Experience (CX) Americas
@dmalik2



Agenda

- Industry Landscape
- Automation & Orchestration Baselineing
- Multicloud Networking
- SASE
- Data Center / Cloud Orchestration
- Cloud Security
- Full Stack Observability
- Key Takeaways

Cisco Webex App

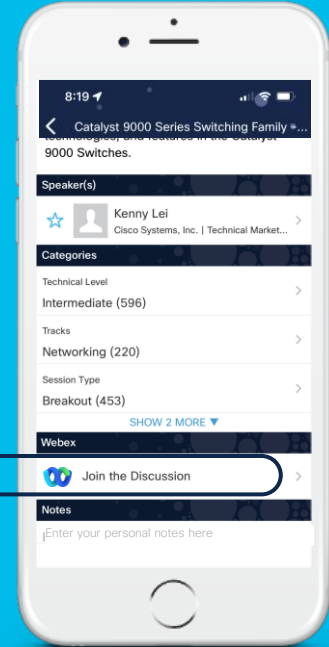
Questions?

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.



Rising expectations
demand a paradigm shift...

Digital Experiences
Automation &
Orchestration
Operations Intelligence

Internet as primary connectivity
Hybrid Multicloud

Lead with Cloud Principles
to
Develop CONTROL POINTS

Foundational Components of ANY Architecture

API as the Primary Interface

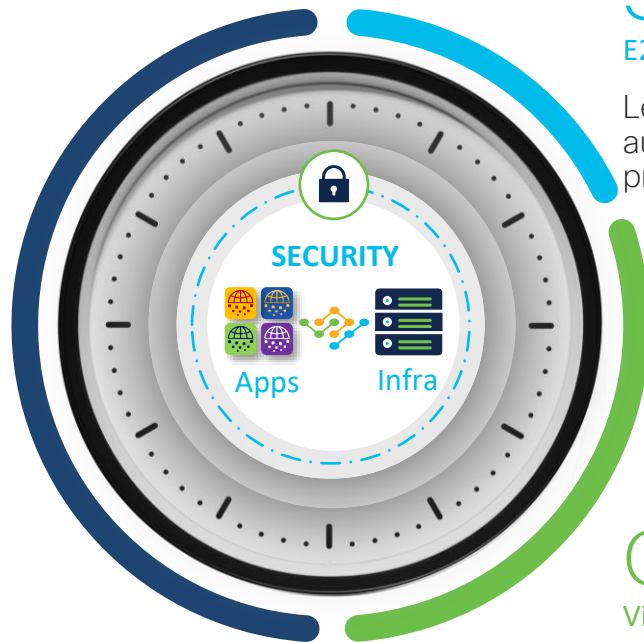
Continuous X

CI/CD/CT

Integrated lifecycle management with automated testing

CI - Continuous Integration
CD - Continuous Delivery
CT - Continuous Testing

CISCO *Live!*



Service as Code

E2E Automation & Orchestration

Leverage programmable infrastructure to automate and orchestrate service intent to provide optimized application experiences

Observability

Visibility & Insights

Infrastructure and application stack real-time intelligence to enable self-optimizing actions

Automation / Orchestration



Automation

The ability to perform individual, repetitive tasks.

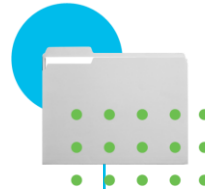
Why do customers want to automate?

“I need to deploy new services quicker; customer demand is drowning me.”

“I have repetitive tasks we are doing manually – I need to free up people to do other value-added work”

“I need to capture intent which can be converted into IP leveraging automated workflows.”

“I have to minimize operational risk”



Orchestration

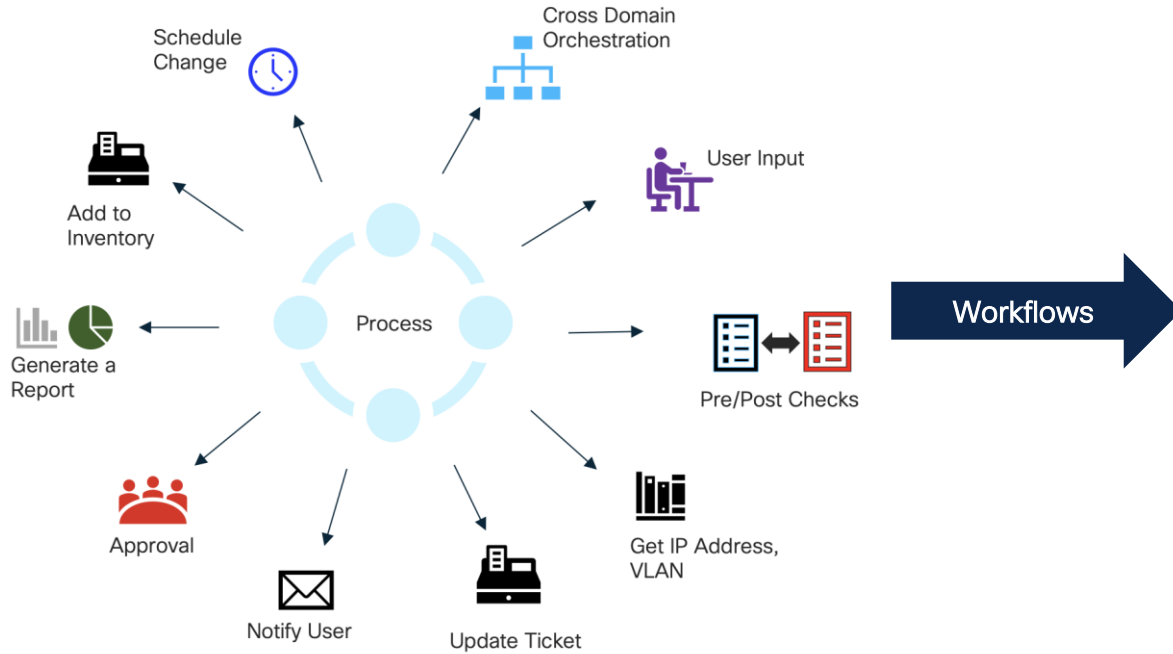
The arrangement and coordination of automated and non-automated tasks, ultimately resulting in a consolidated business/IT process or workflow.

Why do customers want to orchestrate?

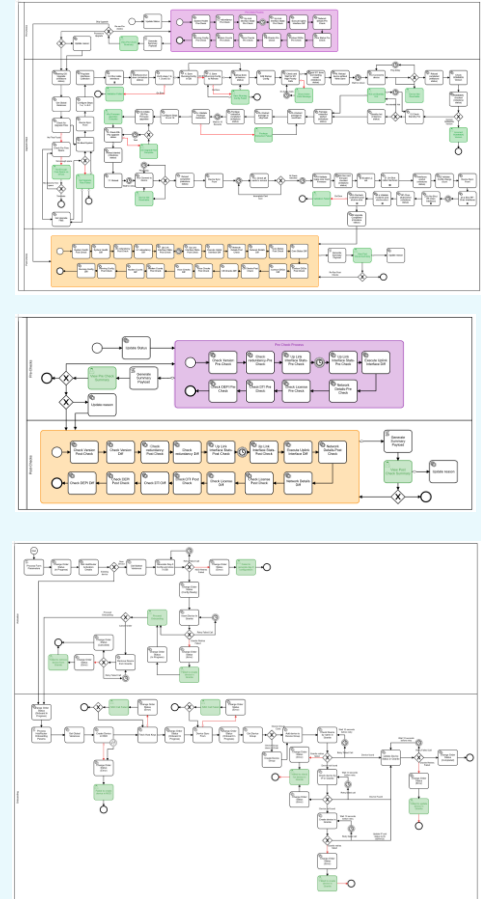
“I want to integrate my systems together to achieve an end-to-end workflow that reflects our service life-cycle – request, implementation, sustainment, modification, decommissioning.”

“Vendors offer many management tools – some do provisioning of services, others do monitoring – why can’t they be integrated together as a solution?”

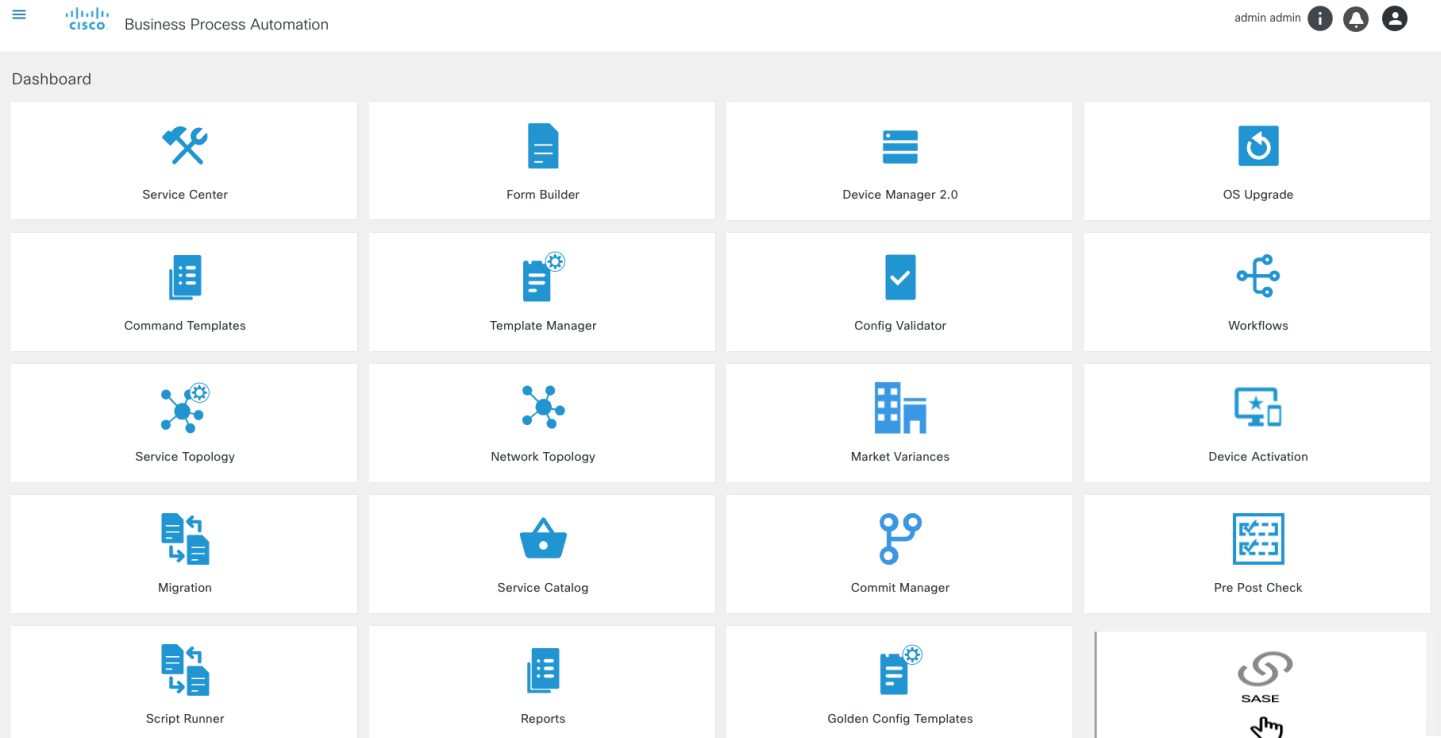
Workflow and Process Automation



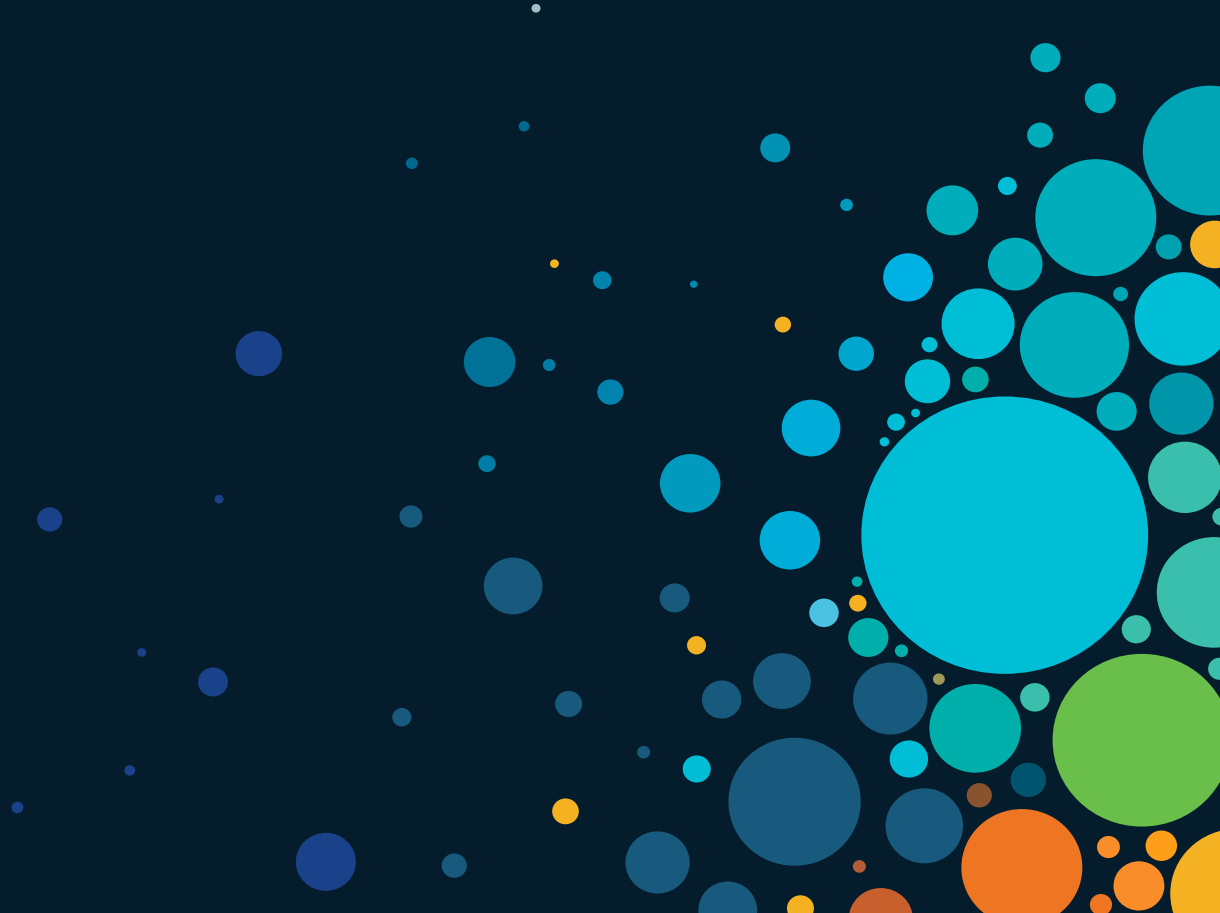
Existing Cox Workflow



Business Process Automation



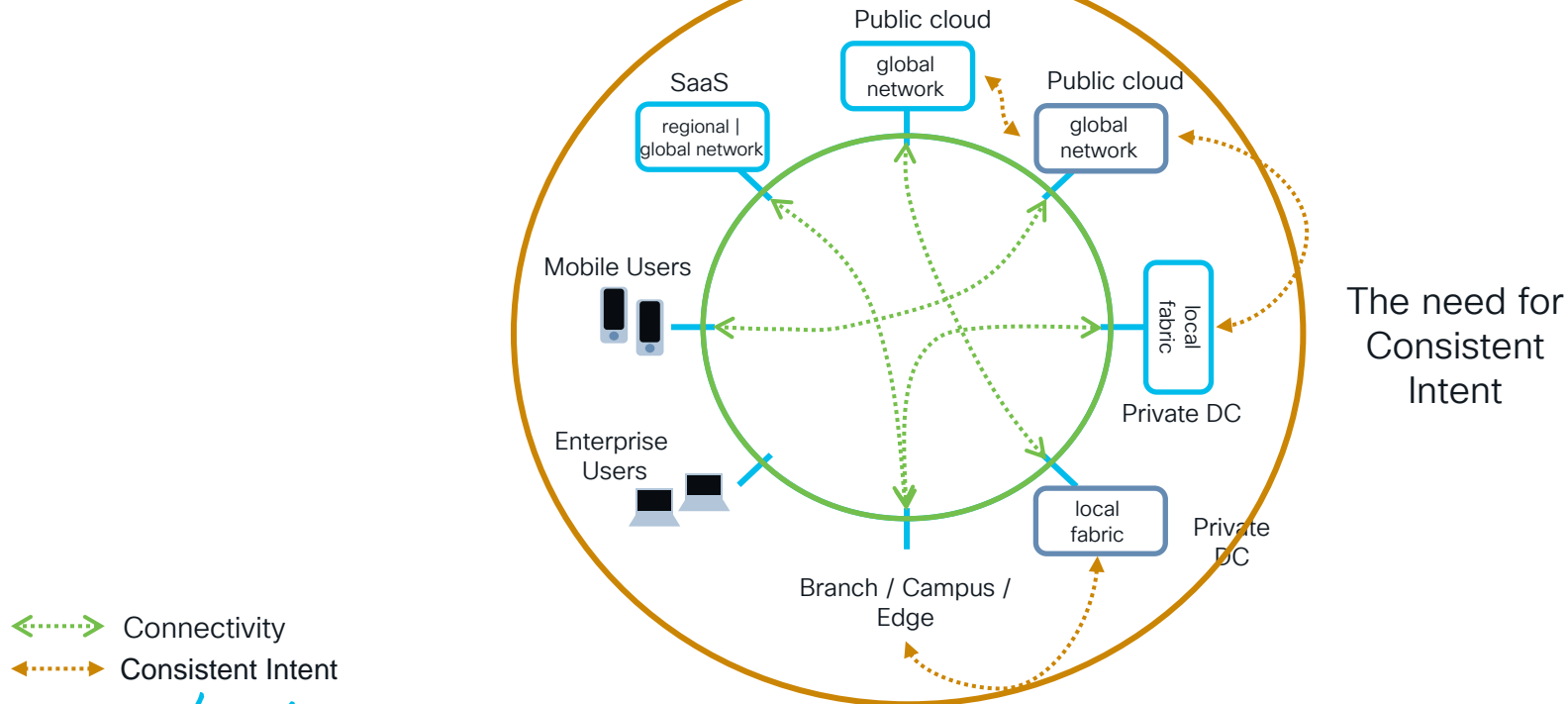
Multicloud Networking



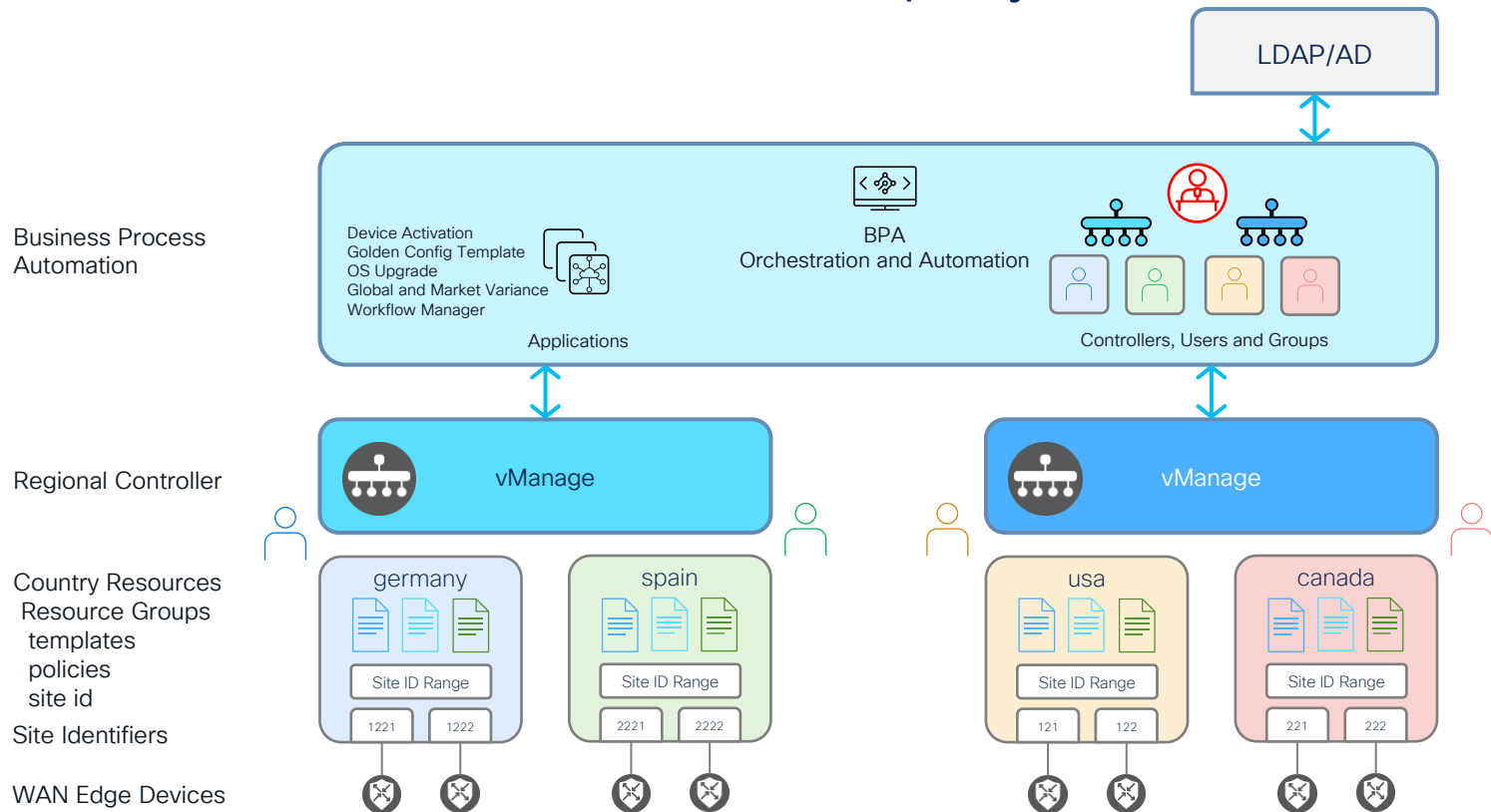
Cloud Networking – Essentials

Hybrid cloud architectures require a more **INTEGRATED**

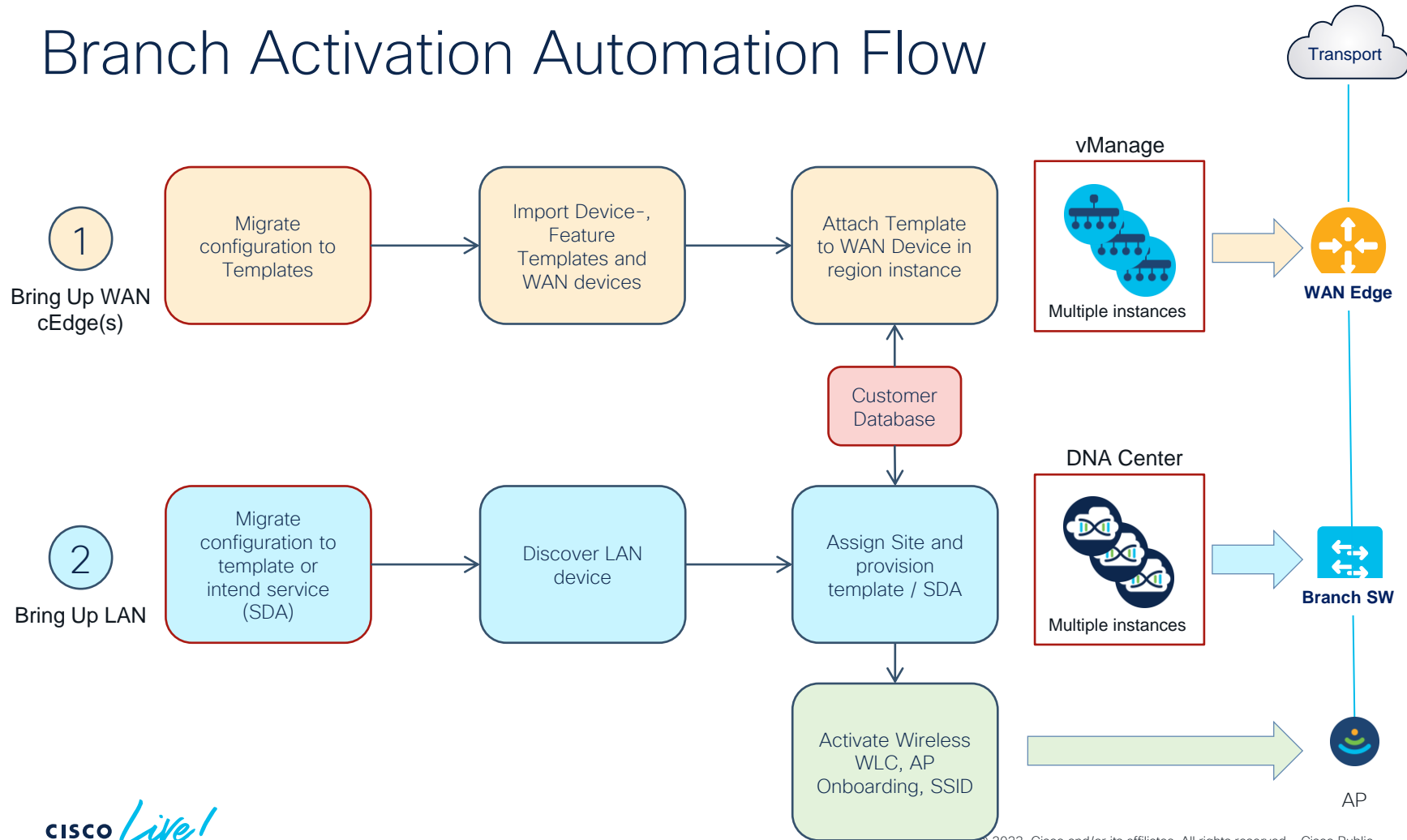
approach



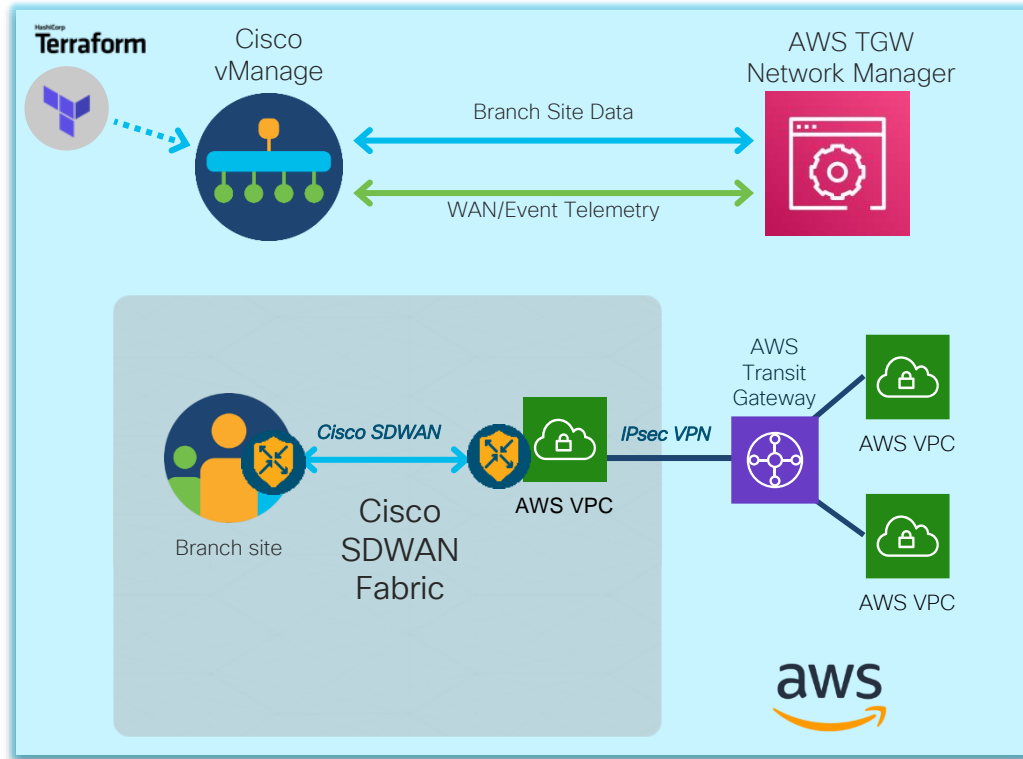
SDWAN Multi-Controller Deployments with RBAC



Branch Activation Automation Flow



Extend SDWAN into the Public Cloud



- Automated provisioning of SDWAN Transit VPC and TGW, route exchange for site to cloud and site to site traffic over AWS backbone
- Full Visibility into inter-regional transit traffic and telemetry with TGW Network Manager
- Consistent Policy and Segmentation across branch and cloud for enterprise class security
- Enhanced end-to-end visibility

Cloud OnRamp Automation

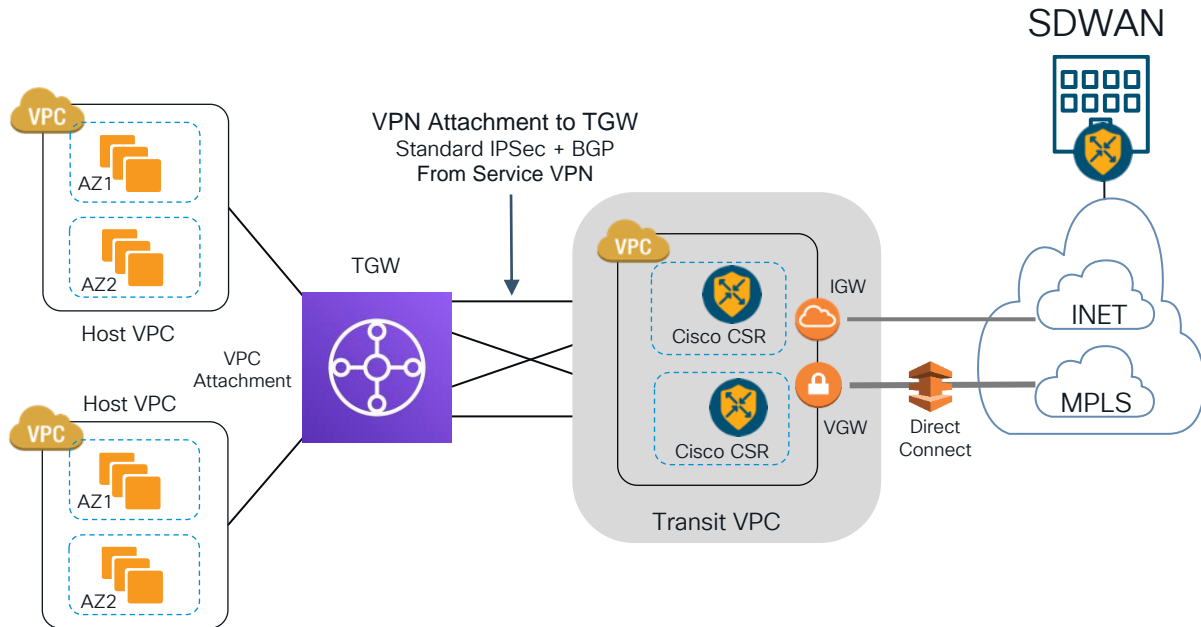
Seamless Access to ANY Cloud

vManage will do the following:

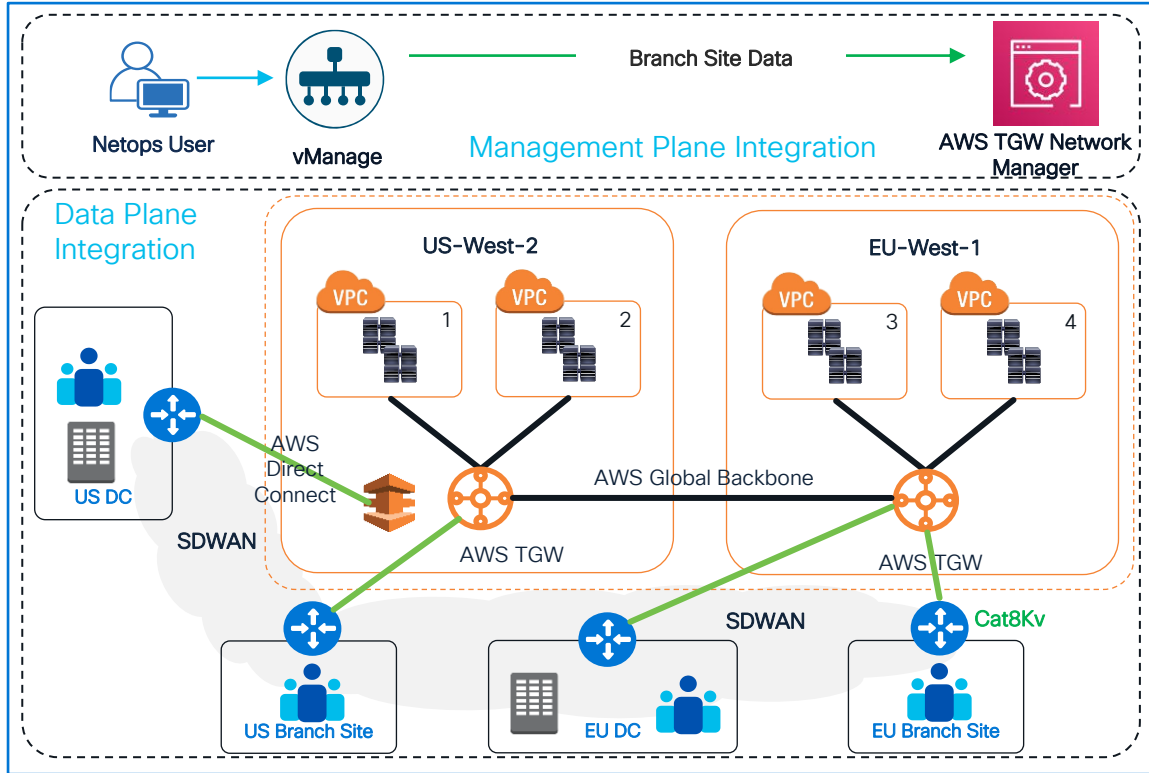
1. Bring up Transit VPC with two CSR running SDWAN image
2. Create TGW
3. Connect TGW and CSR
4. Connect host VPCs

Single UI vManage Workflow:

1. have two CSR ready
2. define AWS Account
3. discover host VPCs
4. tag host VPCs as needed
5. enter TGW details
6. deploy and verify



Alternative to SDWAN extension into cloud: Standard IPsec from Branch to AWS



Solution Overview

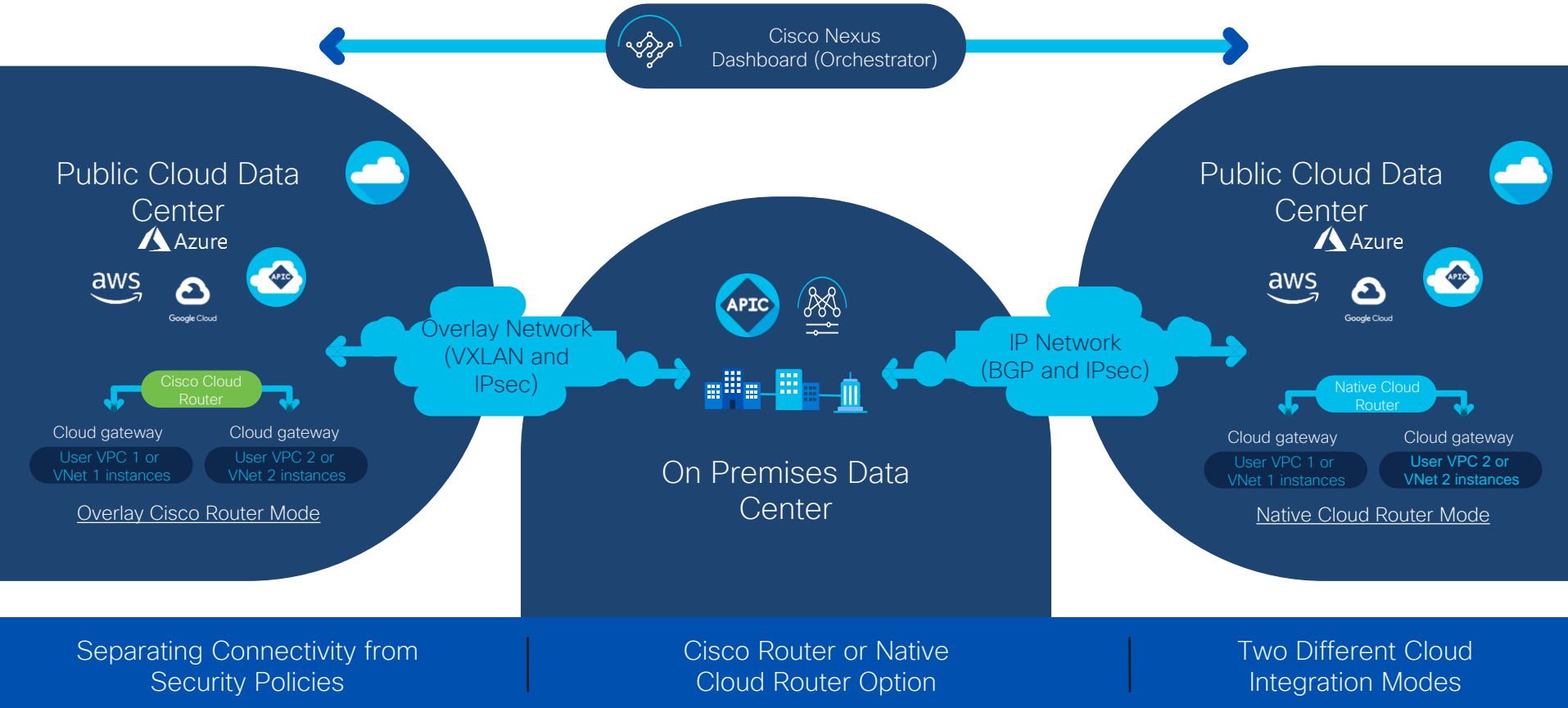
- Management Plane Integration between vManage and TGW-NM Service
- vManage shares branch device data with TGW-NM using APIs calls
- vManage orchestrates branch site router to Transit Gateway (TGW) connection

Customer Benefits

- Network Automation from branch to AWS Cloud via Cloud OnRamp
- Cat8Kv virtual router for multicloud networking with programmatic APIs

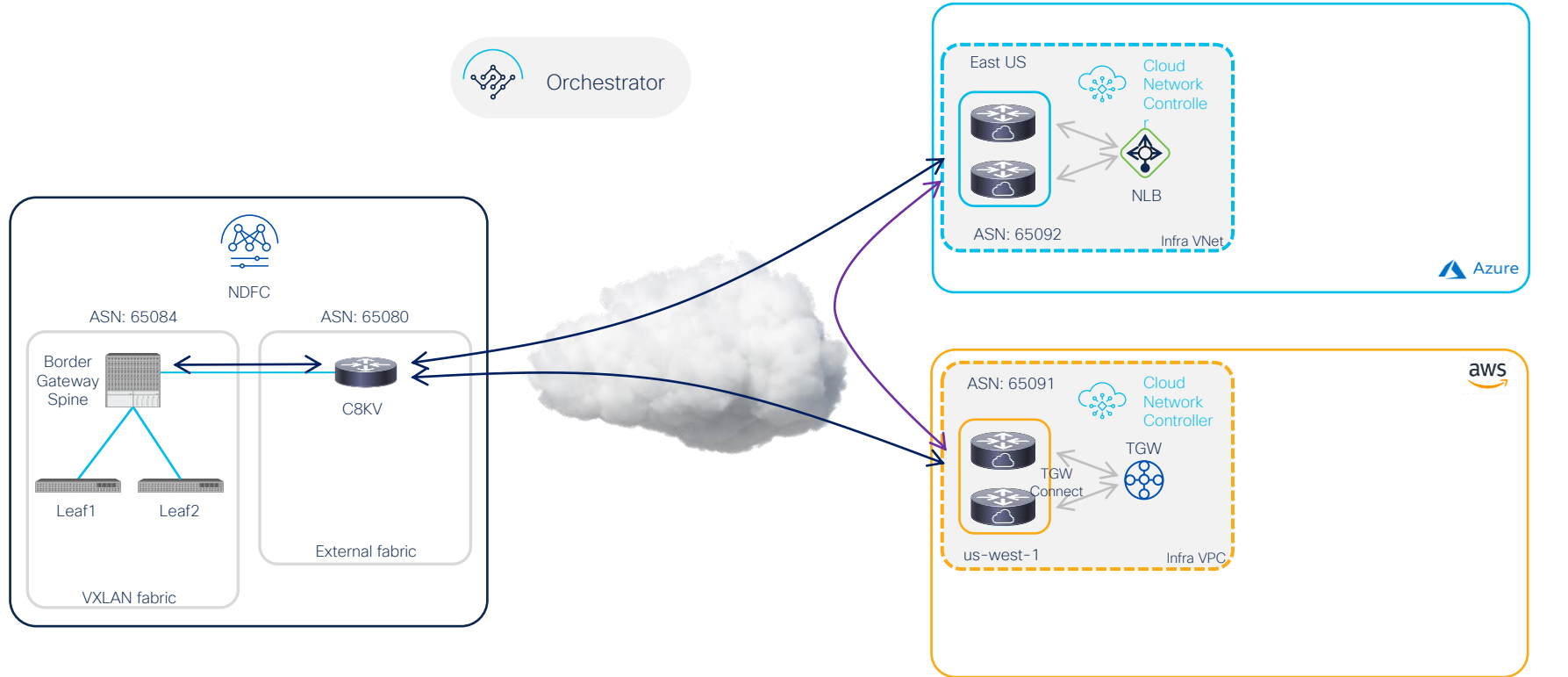


Hybrid Multicloud Networking – Deployment Model



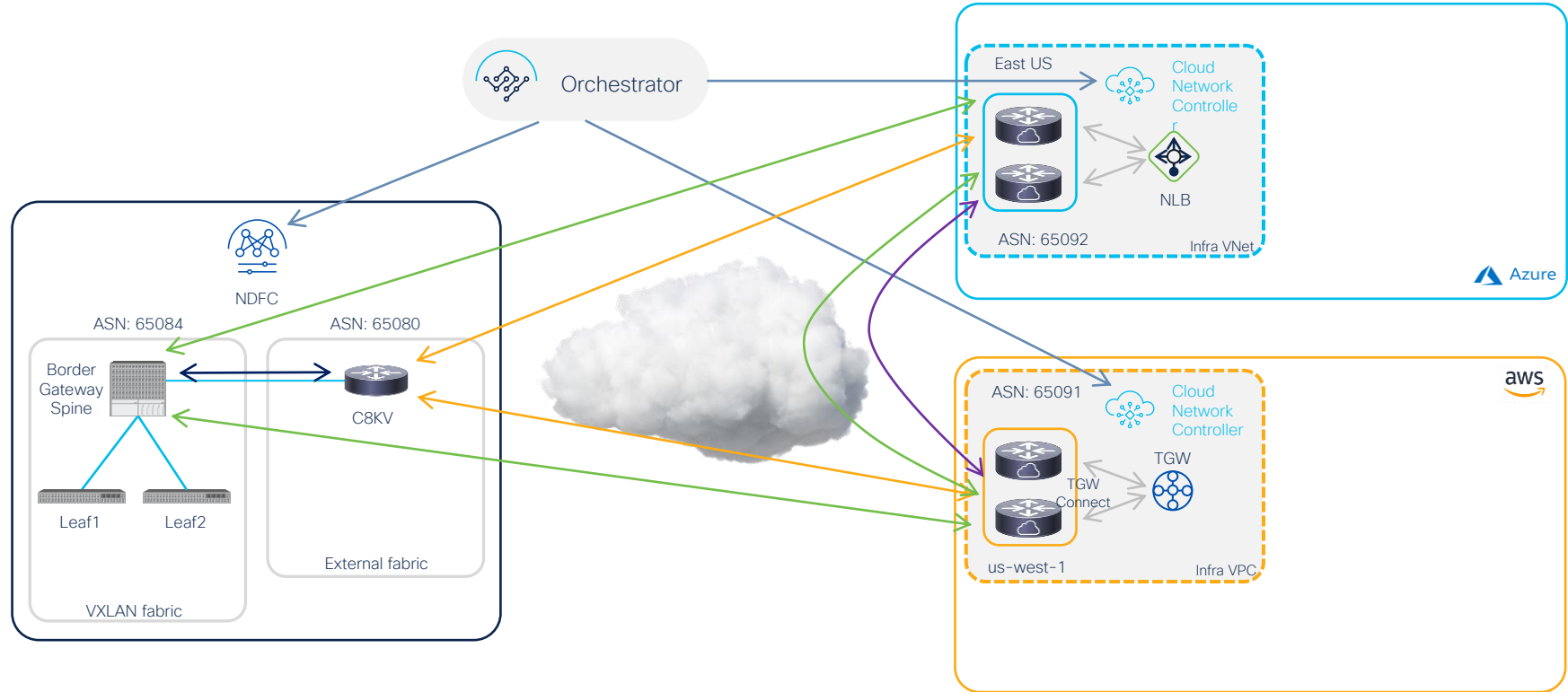
Building Multi-Cloud Connectivity

Building Underlay



Building Multi-Cloud Connectivity

Provision On-Prem to Cloud & Cloud to Cloud Connectivity

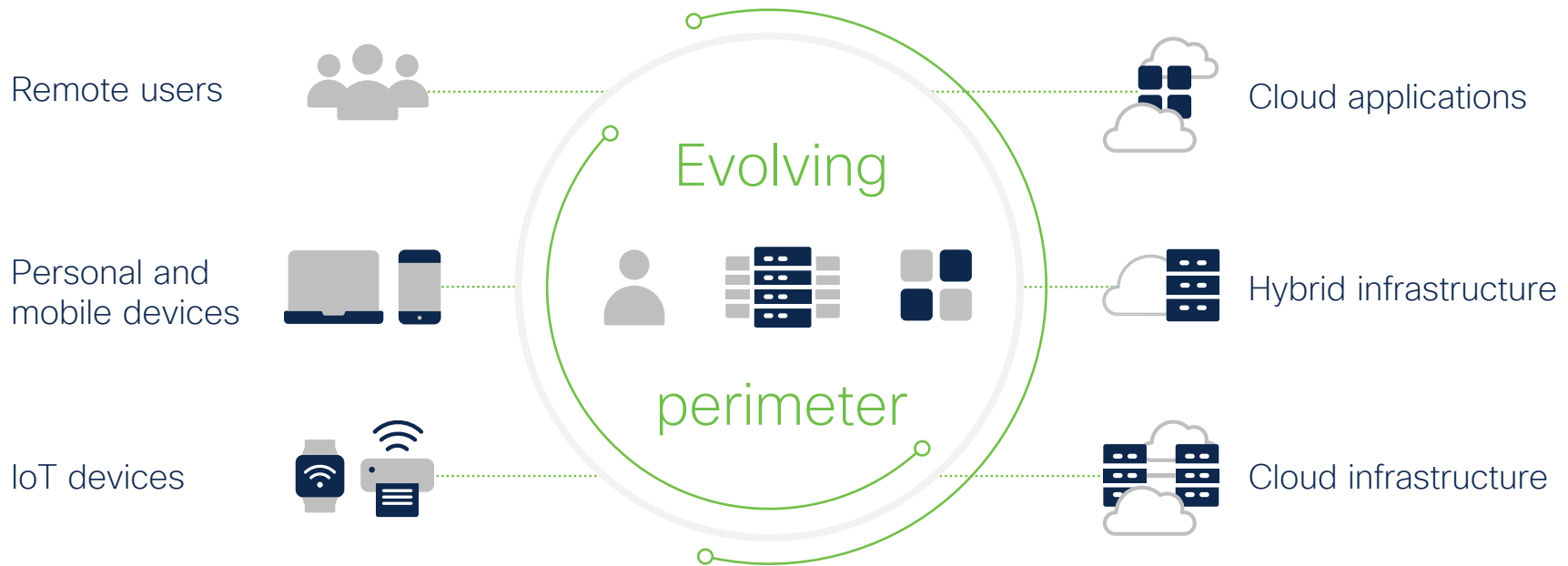


SASE

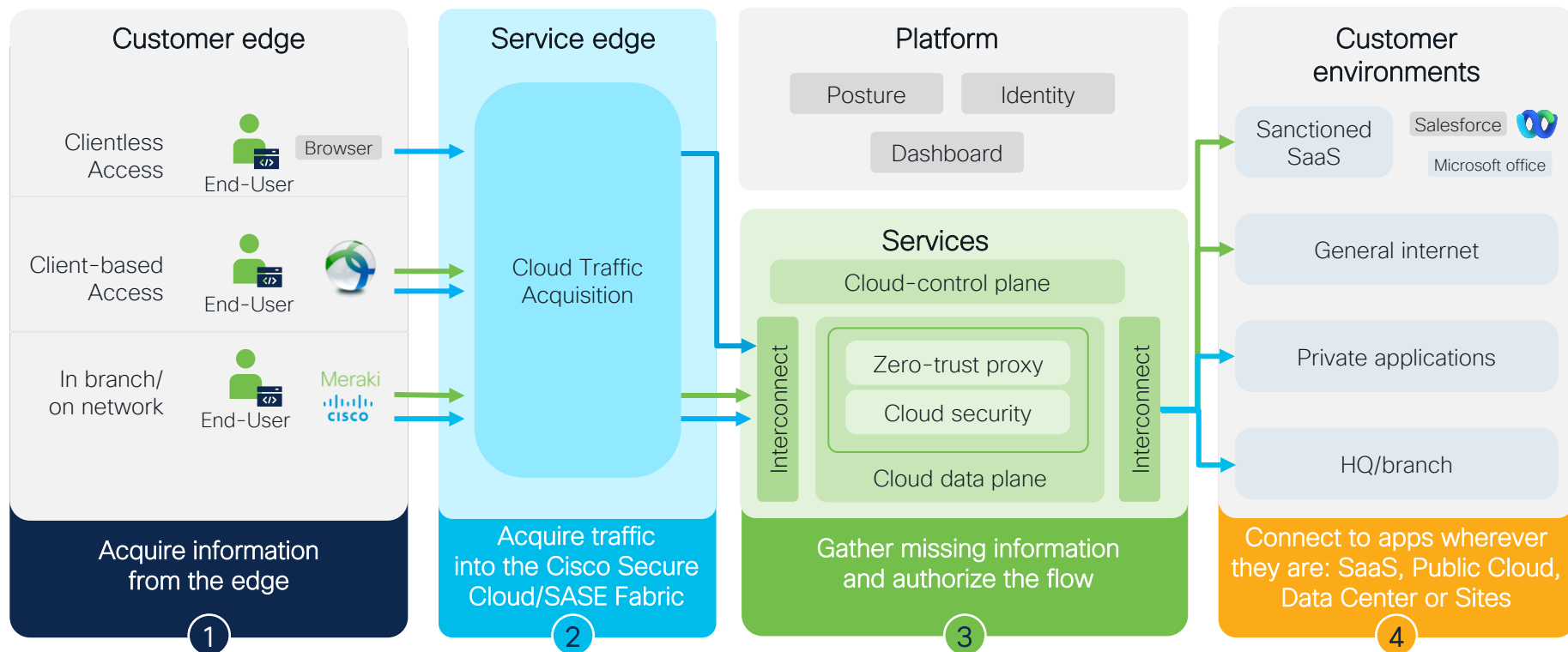


Cloud Experiences are driving major architecture shifts

Users, devices, and apps are everywhere

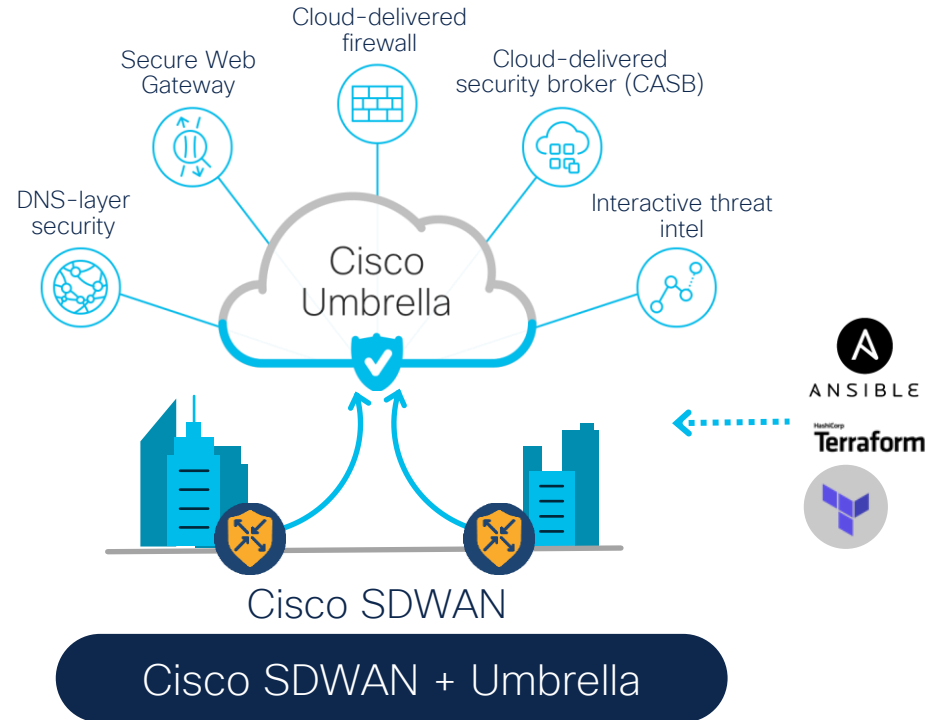


Cisco+ Secure Connect High-level architecture



Cisco SDWAN integrated with Umbrella

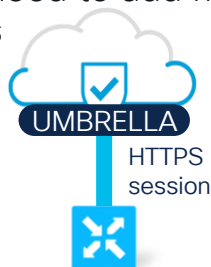
- **Automation:** Deploy cloud security and connectivity across thousands of branches in minutes
- **Instant protection:** defend against threats at the branch with leading real-time threat intelligence
- **Centralized management:** Single pane of glass across all offices and users
- **DevOps:** Integrate into popular tools



Auto-Registration to Cisco Umbrella with SDWAN Edge

Based on Smart Account credentials on both Umbrella and SDWAN

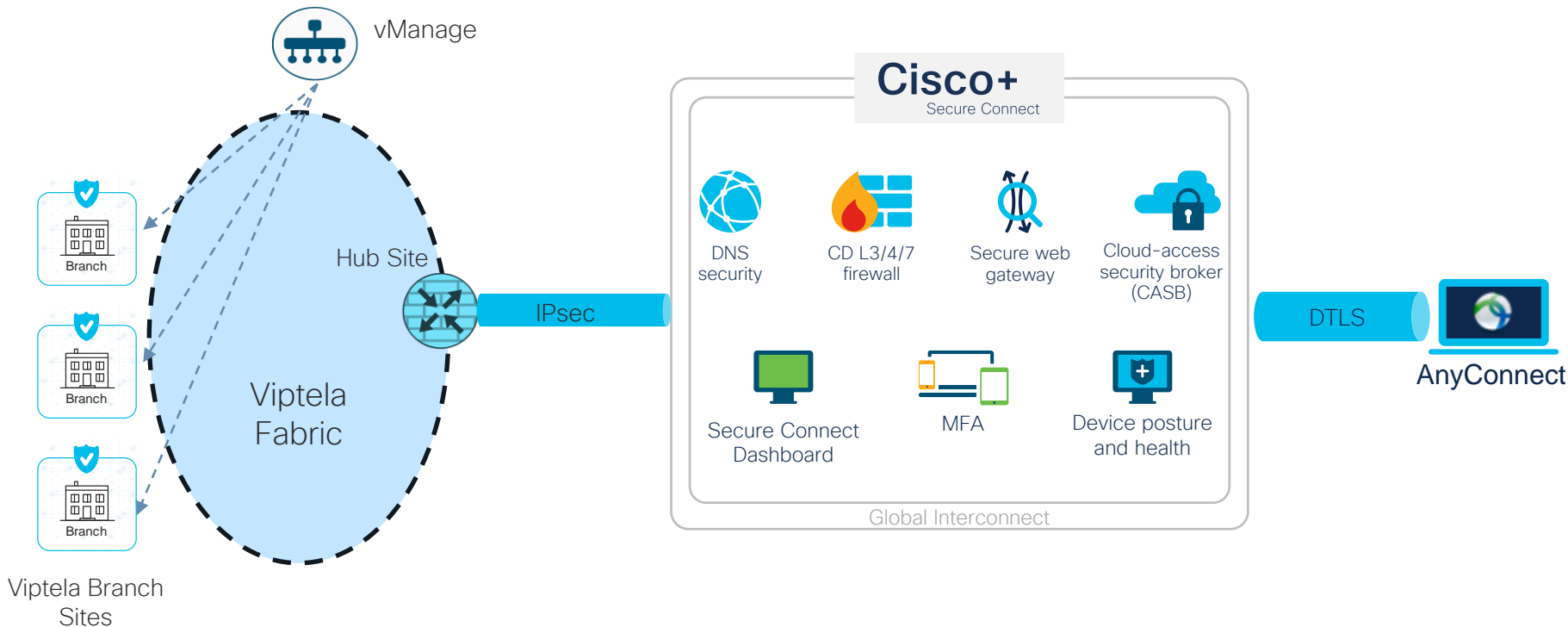
- Registration of Edge Devices to Umbrella is done automatically
- Secure API key is automatically provisioned on the Edge Device through HTTPS session
- No need to add manual API keys



The screenshot shows the Cisco Umbrella Admin interface. On the left is a sidebar menu with options: Reporting, Admin, Accounts, User Roles, Log Management, Authentication, Bypass Users, Bypass Codes, API Keys, Licensing, Investigate, Eric Trolan (ET home), Need Help, Email Technical Support (umbrella-support@cisco.com), Service Status (All services are operational), and Documentation. The main content area is titled 'Admin API Keys' and includes a 'Create' button. Below this is a message: 'Cisco Umbrella generates authentication keys for several types of integrations. These include software, Umbrella-enabled devices, and Cisco network hardware. Click Create, then specify the type of integration key you need.' The main content area also displays a form titled 'What should this API do?' with the instruction 'Choose the API that you would like to use.' The form has four radio button options: 'Umbrella Network Devices' (selected), 'Legacy Network Devices', 'Umbrella Reporting', and 'Umbrella Management'. Each option has a brief description and a note about generating one token.

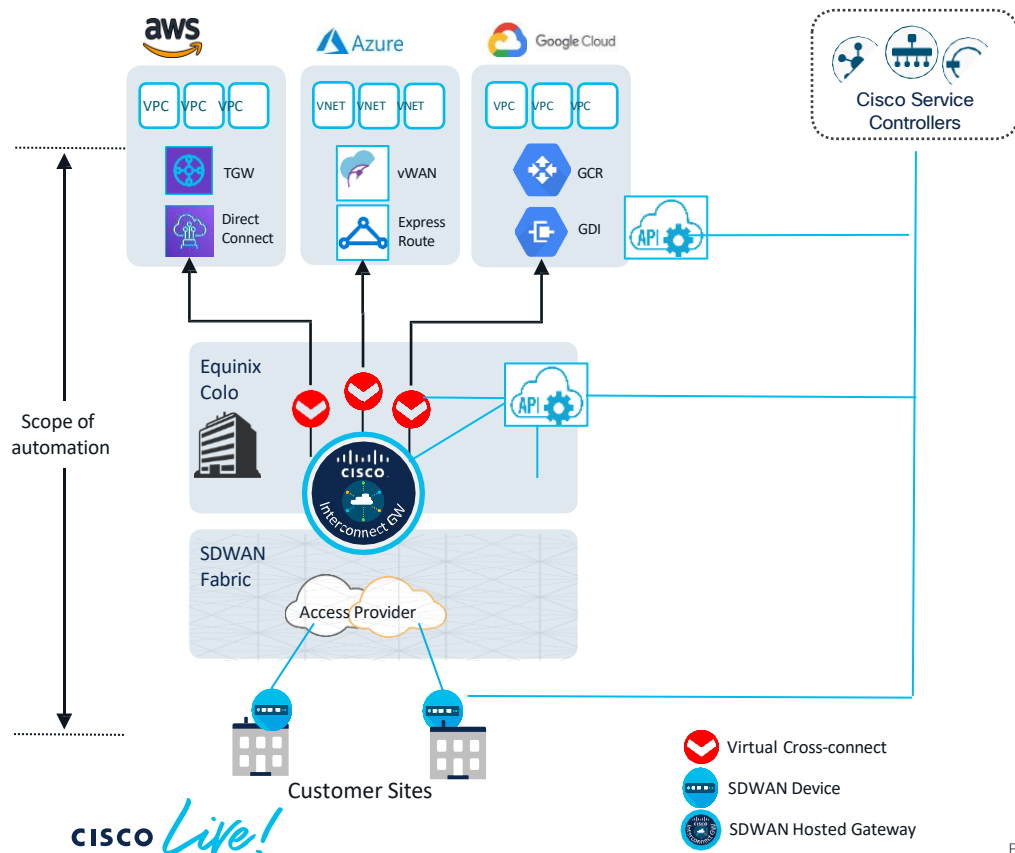
Cisco SDWAN Interconnect

Remote Access Users connecting to Private Applications behind Viptela Fabric



SDCI Detail

Software Defined Cloud Interconnect (SDCI)



Use Cases:

- Site to Site
 - Site to Cloud
 - Backbone on Demand
-
- Hosted SDWAN service at SDCI datacenters
 - Regional Aggregation to Cloud and SaaS
 - Provisioning of all Cloud direct connections in vManage
 - Full-stack network automation
 - Single portal for service creation

Secure Connect Cloud Overview

Enables Auto VPN connectivity with Meraki SDWAN and IPSEC connectivity for private access with Cisco SDWAN.

Dynamically handles bandwidth per Meraki SDWAN network integrating with Cisco+ Secure Connect

Streamlined region based SDWAN fabric integration. Organizations can connect to their closet cloud regions

Eliminates the need for scaling horizontally deploying additional CloudHubs/Connectors.

Decreases the need for large configuration templates.

Supports both RFC 1918 and Public IPs for private access

Data Center/Cloud Orchestration

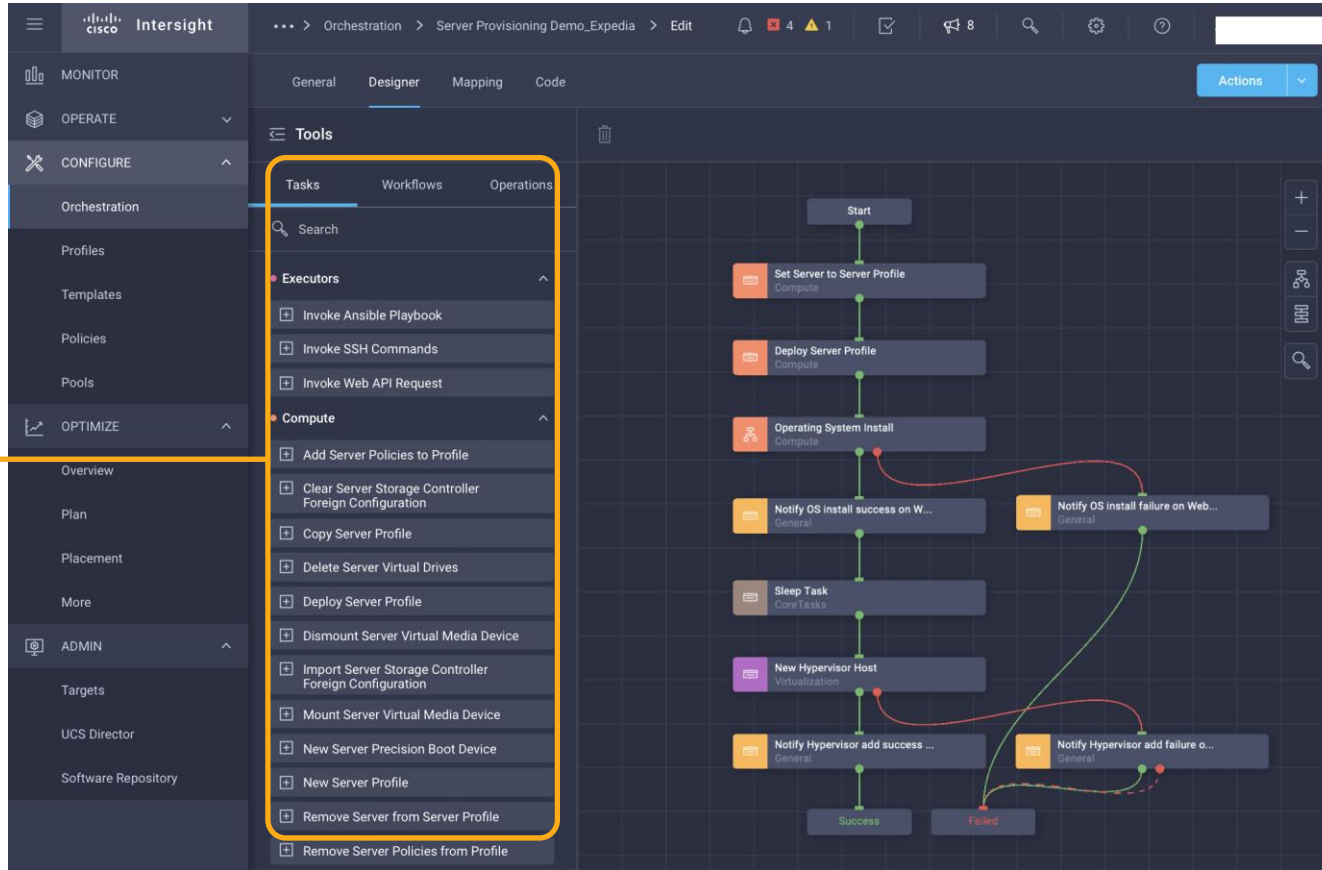


Cross-domain orchestration with workflow designer

Out of the Box



Accelerate hybrid IT delivery with an extensive library of ready-to-use tasks and workflows



Customizable Templates



Create your own custom automation and integration tasks

Simple drag-and-drop workflow authoring

Orchestrating Kubernetes Clusters Deployment

- Simplified workflows for K8s cluster management
- Automate tasks
- Orchestration of complex workflows and accessible via Intersight APIs
- Integration with DevOps tools for release management methodologies

Requests > Deploy Kubernetes Cluster Profile

98

98

33

Sundar Srinivasaraghavan

Details

Status

Success

Name

Deploy Kubernetes Cluster Profile

ID

5fff7cfc696fe2d307b137d

Target Type

Kubernetes Cluster Profile

Target Name

IKSZ

Source

IKSZ (Kubernetes Cluster Profile)

Initiator

sunsrini@cisco.com

Start Time

Jan 13, 2021 5:06 PM

End Time

Jan 13, 2021 5:18 PM

Duration

12 m 13 s

Organizations

default

Execution Flow

Deploy Add-ons

View Execution Flow

Jan 13, 2021 5:18 PM

Deploy Cloud Provider

Jan 13, 2021 5:18 PM

Build Cloud Provider

Jan 13, 2021 5:18 PM

Deploy CNI

Jan 13, 2021 5:18 PM

Build CNI Manifest

Jan 13, 2021 5:18 PM

Get Kubernetes Node Group Profile

Jan 13, 2021 5:18 PM

Wait For Connected Cluster

Cluster connected successfully

Jan 13, 2021 5:18 PM

workflow.DeployKubernetesNodeGroupProfile.displaylabel

View Execution Flow

Jan 13, 2021 5:18 PM

workflow.DeployKubernetesNodeGroupProfile.displaylabel

View Execution Flow

Jan 13, 2021 5:18 PM

Deploy Node Pools Batch 0

Jan 13, 2021 5:06 PM

Get Node Pools In Cluster Profile

Jan 13, 2021 5:06 PM

Create Bootstrap Token

Jan 13, 2021 5:06 PM

Create Kubeconfig

Jan 13, 2021 5:06 PM

Configure Essential Add-on Policy

Jan 13, 2021 5:06 PM

New Internal Mgmt SSH Key

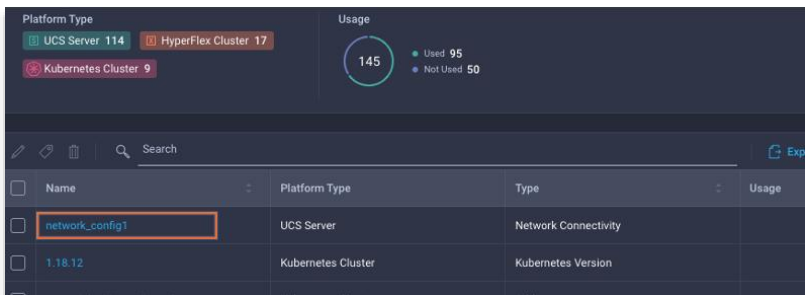
Jan 13, 2021 5:06 PM

Intersight Infrastructure Automation with Terraform

Create module

```
module "iks_example_k8s_network" {  
  source = "terraform-cisco-modules/iks/inte  
  version = "0.9.4"  
  # insert the 2 required variables here  
}
```

Validation in Intersight



Name	Platform Type	Type	Usage
network_config1	UCS Server	Network Connectivity	
1.18.12	Kubernetes Cluster	Kubernetes Version	

Create Terraform execution plan

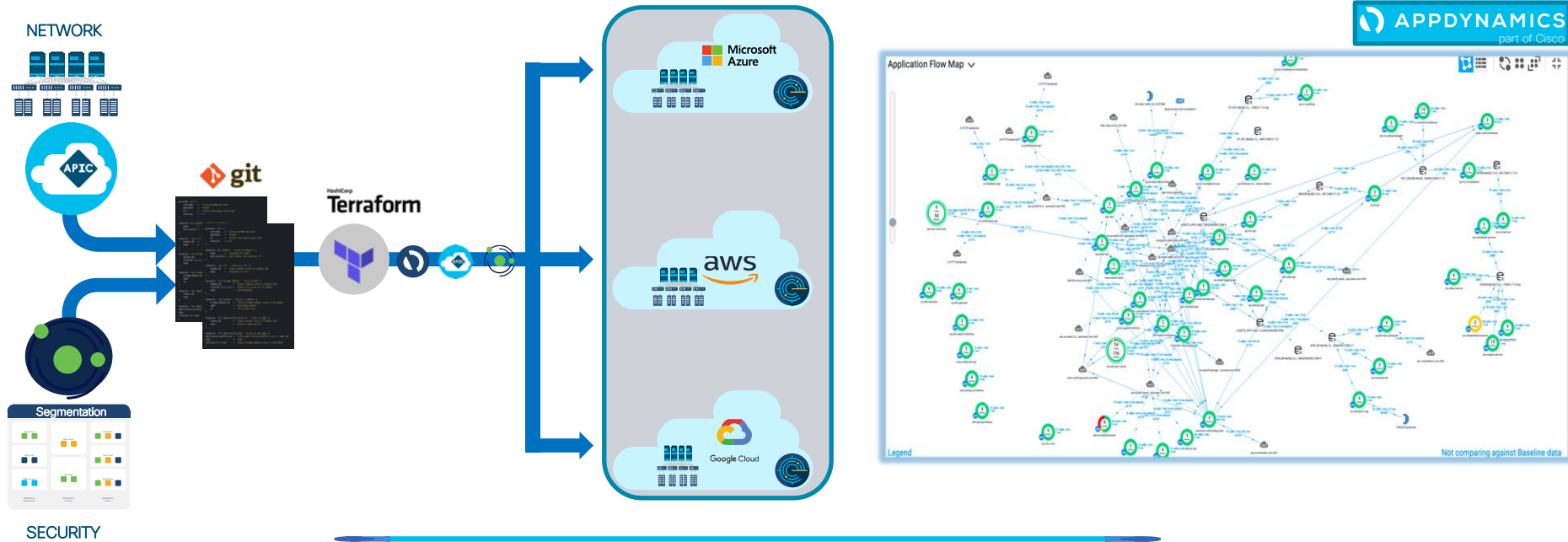
An execution plan has been generated and is shown below.
Resource actions are indicated with the following symbols:
+ create

Terraform will perform the following actions:

```
# intersight_networkconfig_policy.network_config1 will be created  
+ resource "intersight_networkconfig_policy" "network_config1" {  
  + alternate_ipv4dns_server = "10.10.10.1"  
  + alternate_ipv6dns_server = "::<:  
  + appliance_account       = (known after apply)  
  + class_id                = (known after apply)  
  + description             = "test policy"  
  + enable_dynamic_dns      = false  
  + enable_ipv4dns_from_dhcp = false  
  + enable_ipv6            = true  
  + enable_ipv6dns_from_dhcp = false  
  + id                     = (known after apply)  
  + mo_id                  = (known after apply)  
  + name                   = "network_config1"  
  + object_type            = (known after apply)  
  + organization            = [  
    + {  
      + additional_properties = null  
      + class_id             = (known after apply)  
      + mo_id                = "default"  
      + object_type          = "organization.Organization"  
      + selector             = (known after apply)  
    }  
  ]  
  + preferred_ipv4dns_server = "10.10.10.1"  
  + preferred_ipv6dns_server = "::<:  
  + profiles                 = (known after apply)  
}
```

Plan: 1 to add, 0 to change, 0 to destroy.

Hybrid multicloud with automation and app insights



Personalized service

On-demand elastic infrastructure provisioned through portal and/or APIs for self-service business requirements

Infrastructure as code

Common automation and DevOps tools used to safely and efficiently provision and manage service lifecycle with proper release management

Governance and compliance

Multicloud compliance and management to securely provision any workflow to any cloud with workload optimization

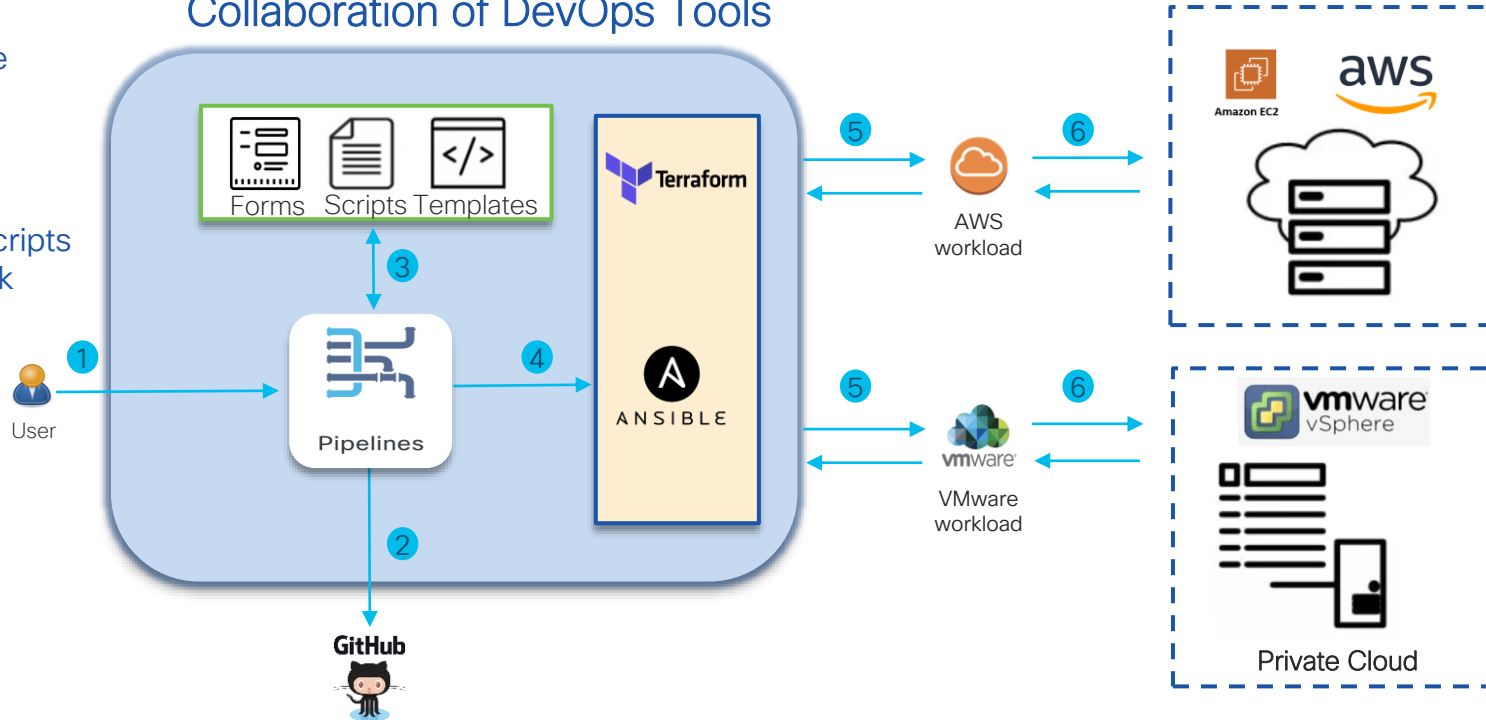
Observability framework

Correlation of deep application insights to infrastructure impact to drive proactive remediation by leveraging event-driven actions

Multicloud Workload Orchestration

Collaboration of DevOps Tools

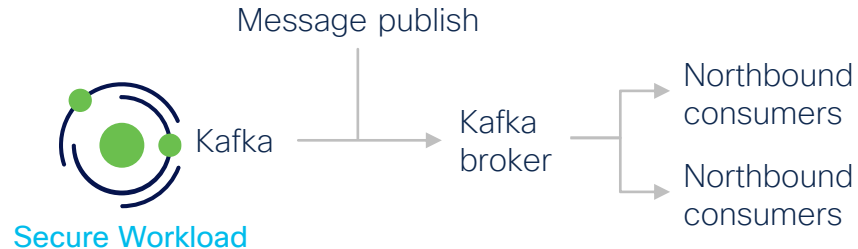
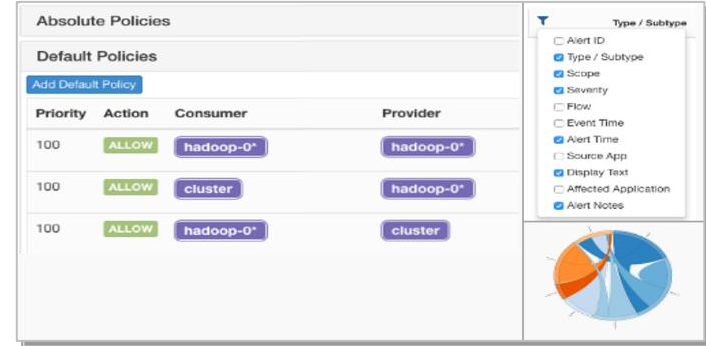
- 1 Request for resource
- 2 Pull scripts from Git
- 3 Process Payloads
- 4 Invokes Terraform scripts and Ansible playbook
- 5 Provision resource
- 6 Deploy



Cloud Security

Orchestrate policy to other enforcement points

- Publish normalized micro-segmentation policy over the Kafka interface
- Updates to the policy are also sent through the same interface in real-time
- Northbound systems can consume this policy and render it in other infrastructure elements such as:
 - Firewall orchestration platforms
 - Load balancers (F5/Citrix)

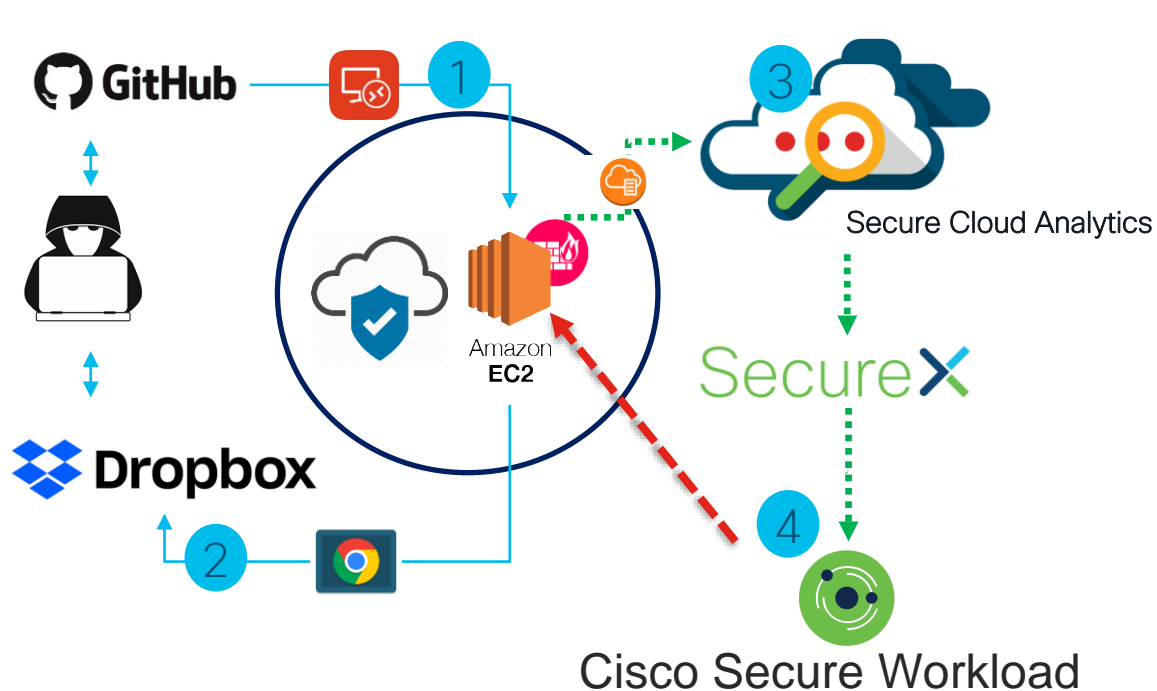


algosec



SKYBOX
SECURITY

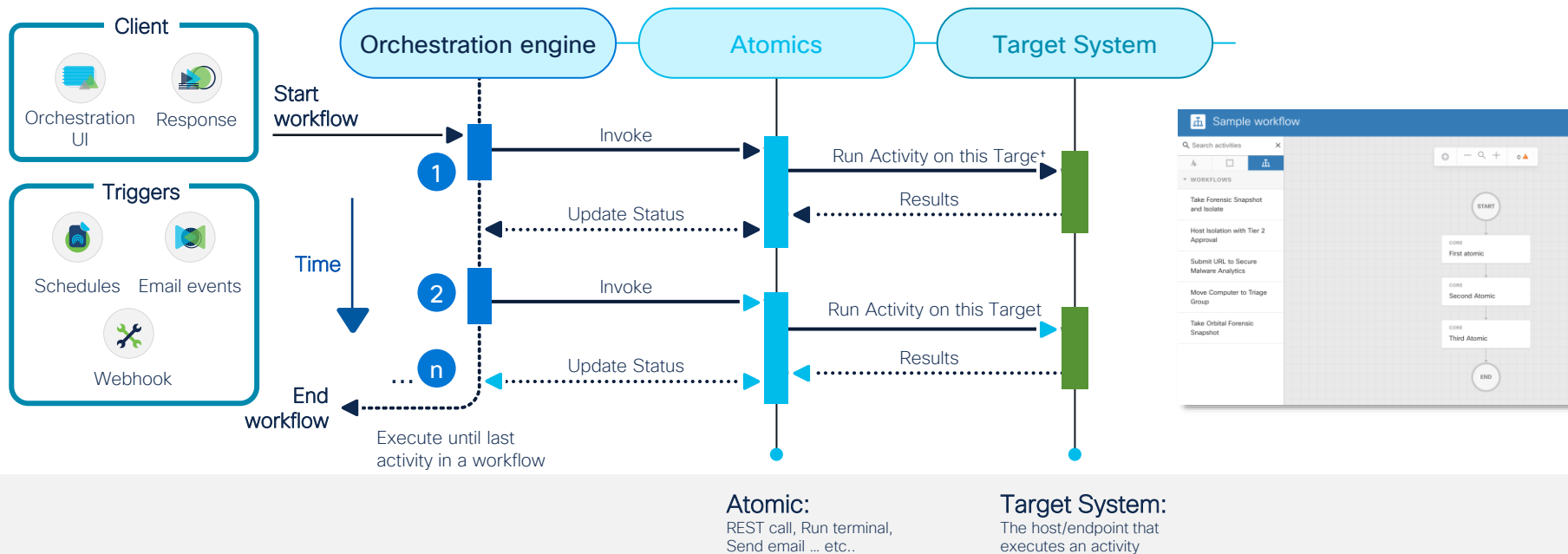
Workload and Security Analytics Workflow



- 1 Attacker Finds Exposed Credentials in Github and breaches over-exposed EC2 VM
- 2 Attacker Begins Exfiltrating Confidential Data from VM to Dropbox
- 3 Secure Cloud Analytics Triggers Alert for Data Exfiltration & Notifies SecureX
- 4 SecureX Orchestrator Quarantines the EC2 instance via Cisco Secure Workload's Multicloud Firewall with One Click in Casebook.

SecureX Orchestration Workflow Sequence

The orchestration engine runs **workflows** to execute **atomics** on the **target systems**, which returns results and **status**, then the next step in the workflow begins.



SecureX Orchestration Canvas for Developing Workflows

The screenshot displays the SecureX Orchestration Canvas interface for a workflow titled "0010 - Phishing Investigation". The interface includes a top navigation bar with buttons for "VALIDATED", "COMMIT", "VIEW RUNS", and "RUN". A left sidebar lists various activity groups and individual activities. The main canvas shows a workflow diagram with a "START" node, followed by "FETCH GLOBAL VARIABLES", "SET THE ENVIRONMENT URLS", and a loop "FOR EACH ATTACHMENT" containing a decision "IS THIS ATTACHMENT AN EMAIL?". The workflow ends with an "EMAIL" node. A right sidebar provides details for the workflow, including its description, group name, category, and a table of variables.

Drag n' Drop UI

Activity Group

Atomic Action (Activity)

Stacked Activities indicates Atomic Action

Details Pane

Creates Atomic Action

Tags Workflow

Variables

Logical Constructs

Validate & Save Run & Audit

Properties

0010 - PHISHING INVESTIGATION

OWNER

adisanka+ctr-dcloud@cisco.com

DESCRIPTION

This workflow monitors a mailbox for incoming phishing reports. When an email is received, the workflow investigates its attachments and attempts to determine if anything in the email (or its attachments) was suspicious or malicious. If anything suspicious or malicious is found, the user is told to delete the email, and a case is created in the Threat Response system.

☐ DELETE WORKFLOW INSTANCE AFTER SUCCESSFUL EXECUTION

☐ IS ATOMIC WORKFLOW

GROUP NAME

Select

CATEGORY

Select

Variables

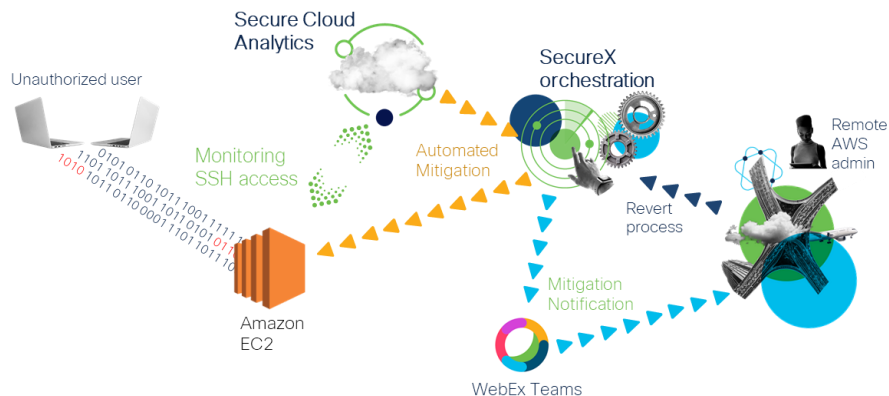
NAME	TYPE	SCOPE	VALUE
Consolidated Headers	String	Local	
Has Email Attachment	Boolean	Local	false
Notification Email Addresses	String	Local	bromide@cisco.com
Number of Clean Observables	Integer	Local	0

Secure Cloud Analytics with Auto-Remediation

Secure Cloud Analytics and AWS

Remediation Workflow

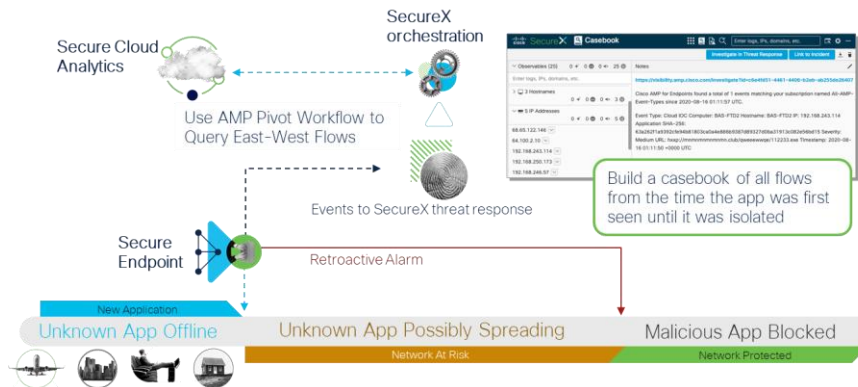
- Mitigation of unauthorized access to EC2 instances on AWS
- Geographically Unusual Remote Access Alert



AMP and Secure Cloud Analytics

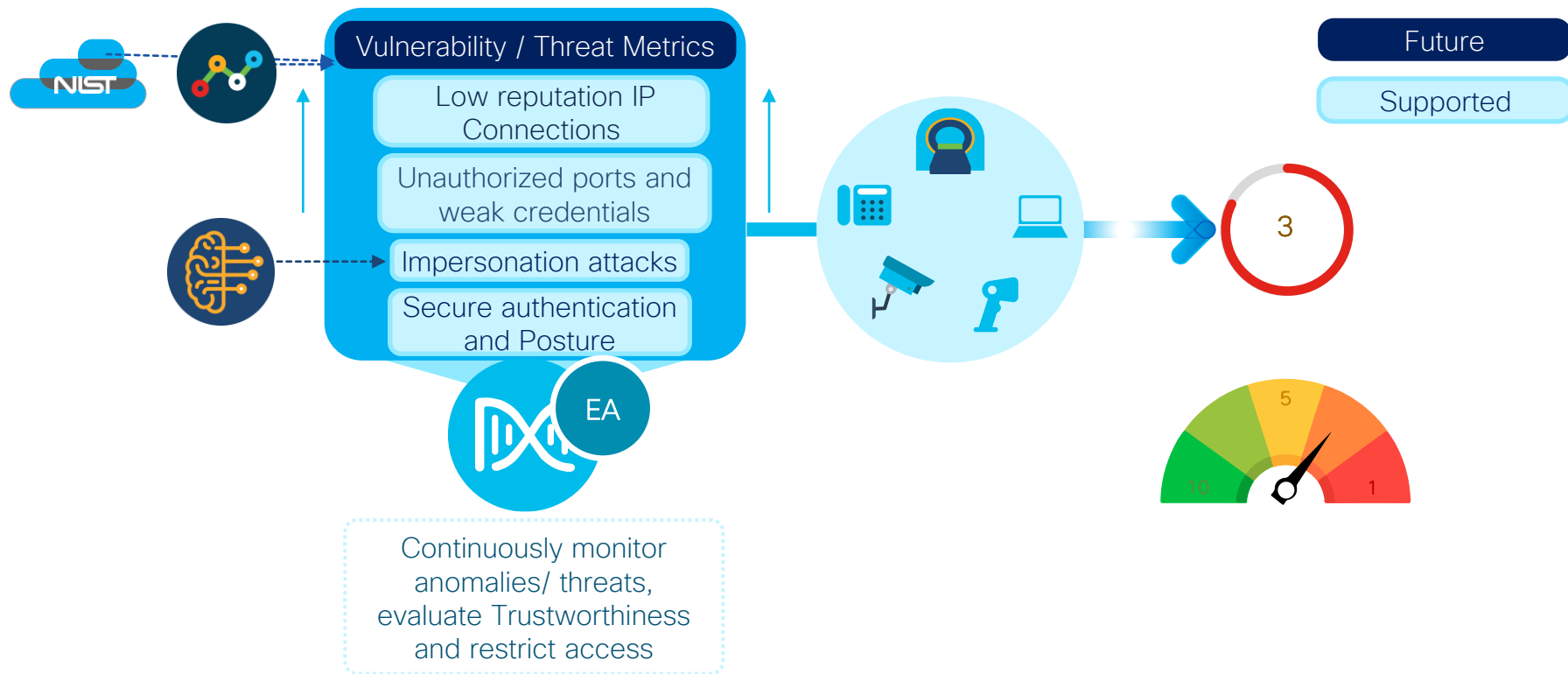
Integration Workflow

- Create Forensic Incident Investigation Casebooks with SecureX and Network Detection and Response (NDR) data

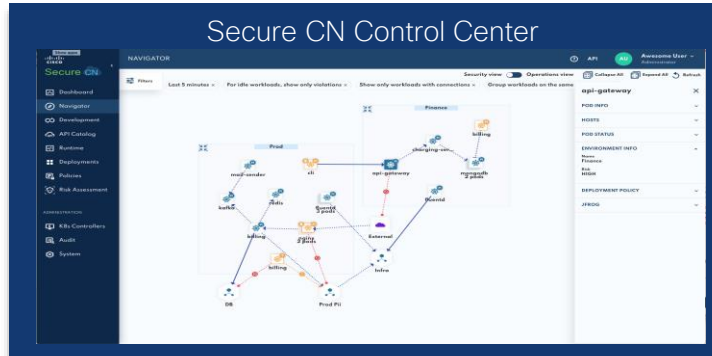
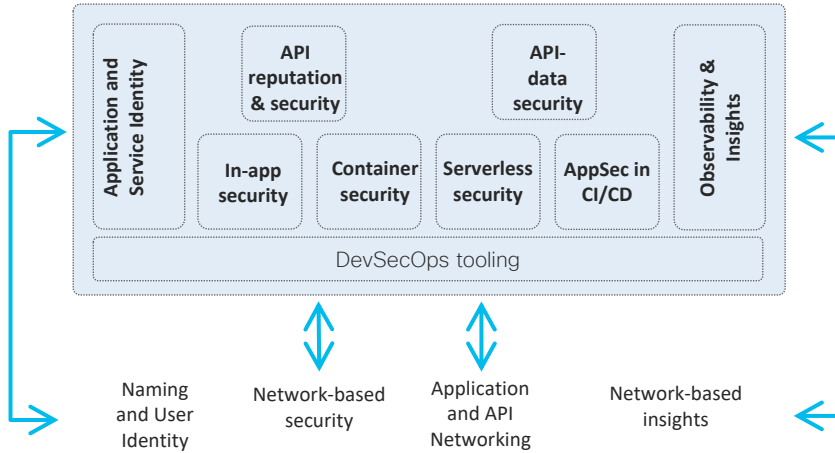


Trust Analytics for Continuous Trusted Access

Continuous evaluation of endpoint security posture



Cisco Secure Cloud Native for DevSecOps



- + Security for various infrastructure ways of building an app – using traditional monolithic methods to cloud native methods
- + Integration of security insights into the CI/CD pipelines
- + API-layer scoring, reputation and security, across any cloud and internally consumable APIs
- + Elements of data security related to API-API and API-Data accesses, Tokenization, and dependency graph visualization
- + Identity for Applications and Services and associate with user identity and policies
- + Security insights at the App and API layer

Observability

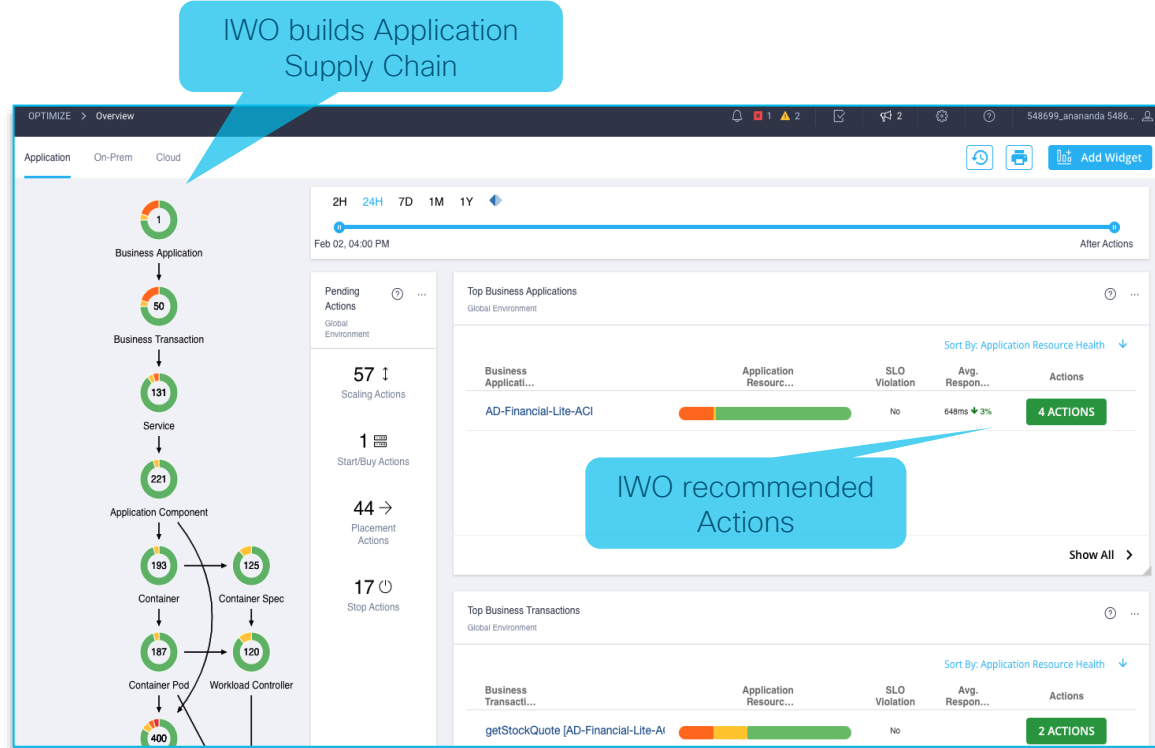
Optimize application experiences

Turn insights into action with Full-Stack Observability



Application Performance Optimization Intersight and AppDynamics Integration

- **Intersight Workload Optimizer** (IWO) provides the application specific supply chain view based on the data provided by AppDynamics
- **AppDynamics** adds Business Application, Business Transaction, Service, Application Component, and Database entities to the IWO supply chain
- **IWO** recommends actions to improve application performance (e.g suspend/provision VMs)



ThousandEyes + AppDynamics Integration

Alerts

Publish ThousandEyes Alerts to AppDynamics

Dashboards

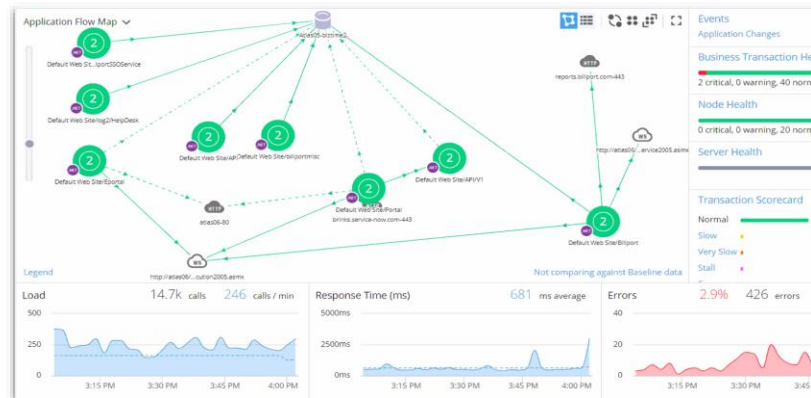
Embed ThousandEyes widgets on AppDynamics dashboards

Snapshots

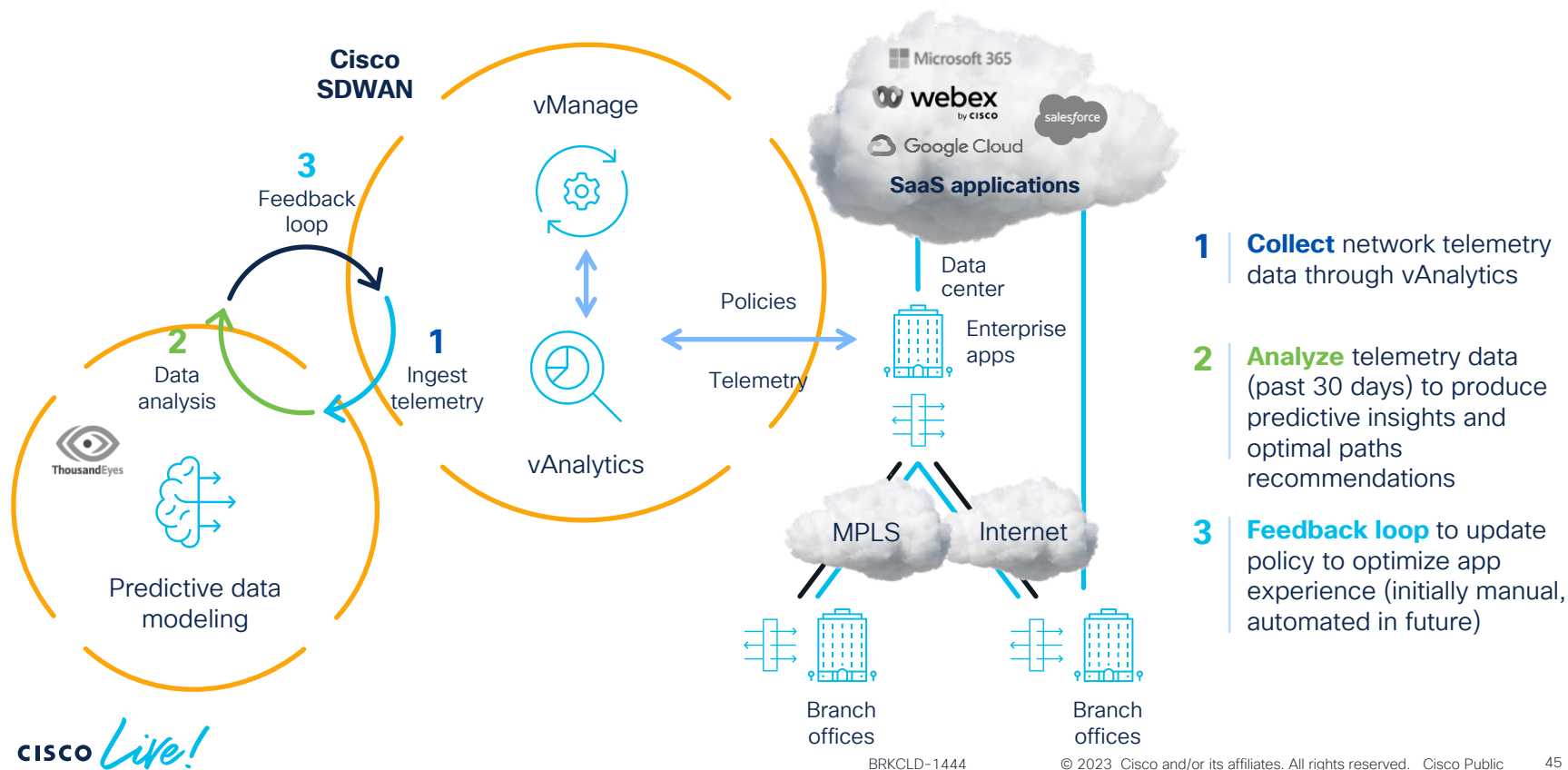
Trigger ThousandEyes snapshots from AppD alert policies

Correlated Data

Make AppDynamics aware of ThousandEyes traffic for correlation



Cisco vAnalytics and ThousandEyes WAN insights



Closed-Loop Integrated Actionable Alerting

Add New Integration

Type: AppDynamics

AppDynamics Instance URL: e.g. thousandeyessinc.saa.s.appdynamics.com

Application Name: Must match the application name from AppDynamics

AppDynamics Username: Username

AppDynamics Password: Password

Severity: Info

Tier: Optional

Node: Optional

Business Transaction: Optional

[Test AppDynamics Integration](#)

[Cancel](#) [Add New Integration](#)

Snapshot Sharing **Export Data**

4 hours of data around SEP 23 19:45 PDT

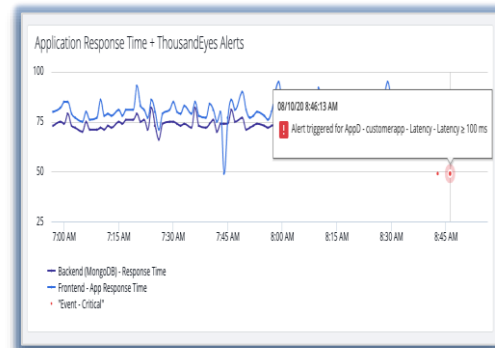
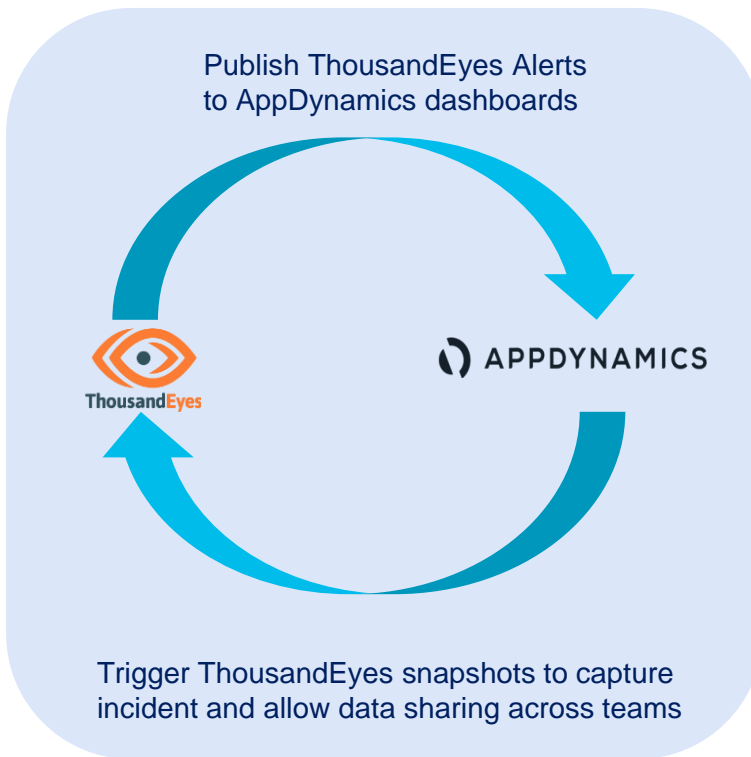
Share this snapshot with

appops@acme.com

Take a look at this data. No network discrepancies observed. Global reachability to the service front door is 100%.

[Link to this snapshot \(anyone can view\)](#)

[Cancel](#) [Share](#)



APPDYNAMICS

ThousandEyes Snapshot - adccapital

Request URL: Method: POST

URL Encoding: UTF-8

Authentication: Type: BASIC

Username: thousandeyessinc@acme.com

Password: [Redacted]

Custom Request Headers: Add Header

Payload: MIME Type: application/json

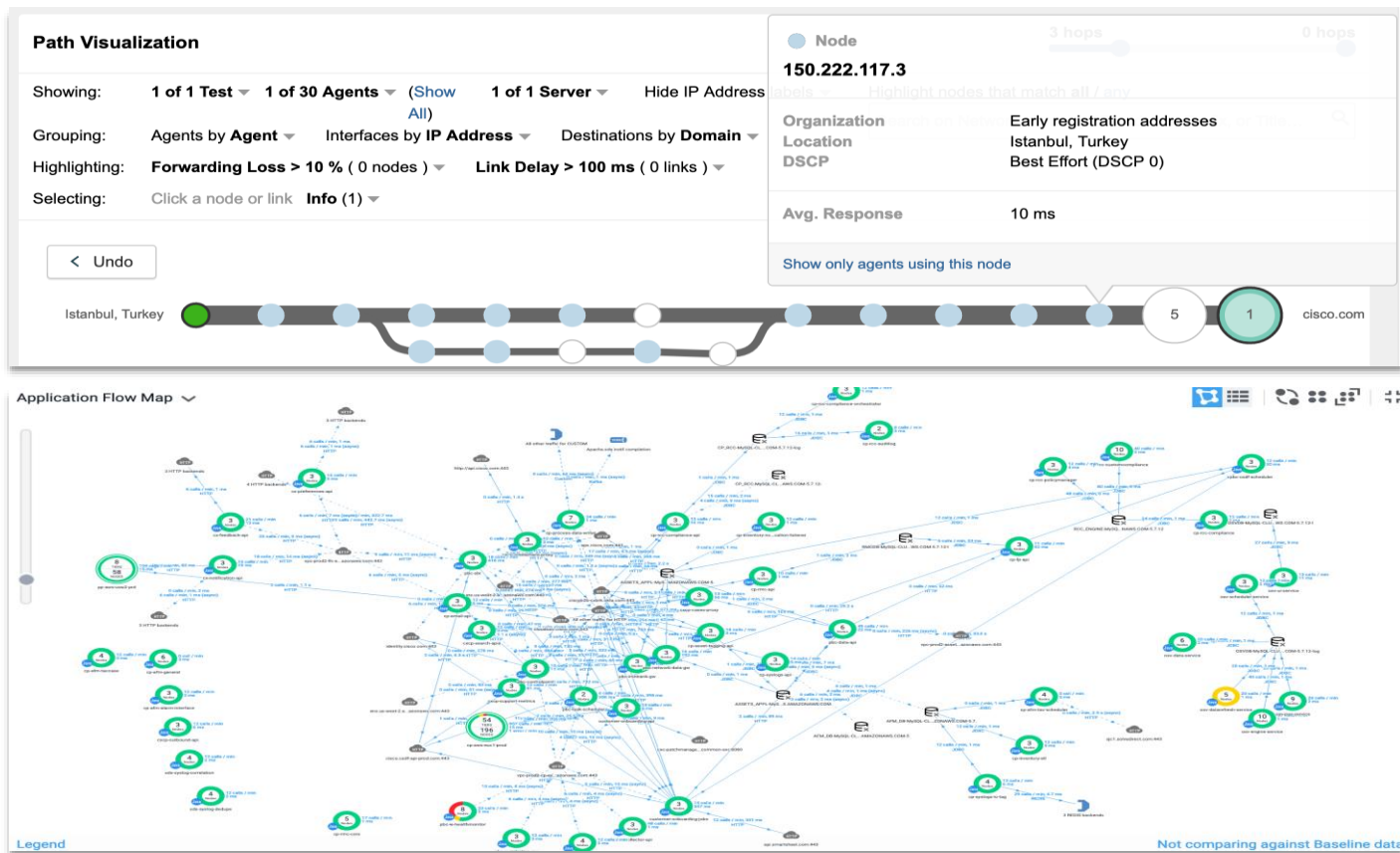
```
{
  "request": {
    "url": "https://api.thousandeyes.com/v4/snapshots.json",
    "method": "POST",
    "headers": {
      "Content-Type": "application/json",
      "Authorization": "Basic thousandeyessinc@acme.com:password"
    },
    "body": {
      "application": "customerapp",
      "business_transaction": "Latency",
      "node": "Frontend",
      "tier": "Optional",
      "severity": "Critical",
      "event": "Latency > 100 ms"
    }
  }
}
```

Application and Infrastructure Event Correlation

WAN/Internet Insights

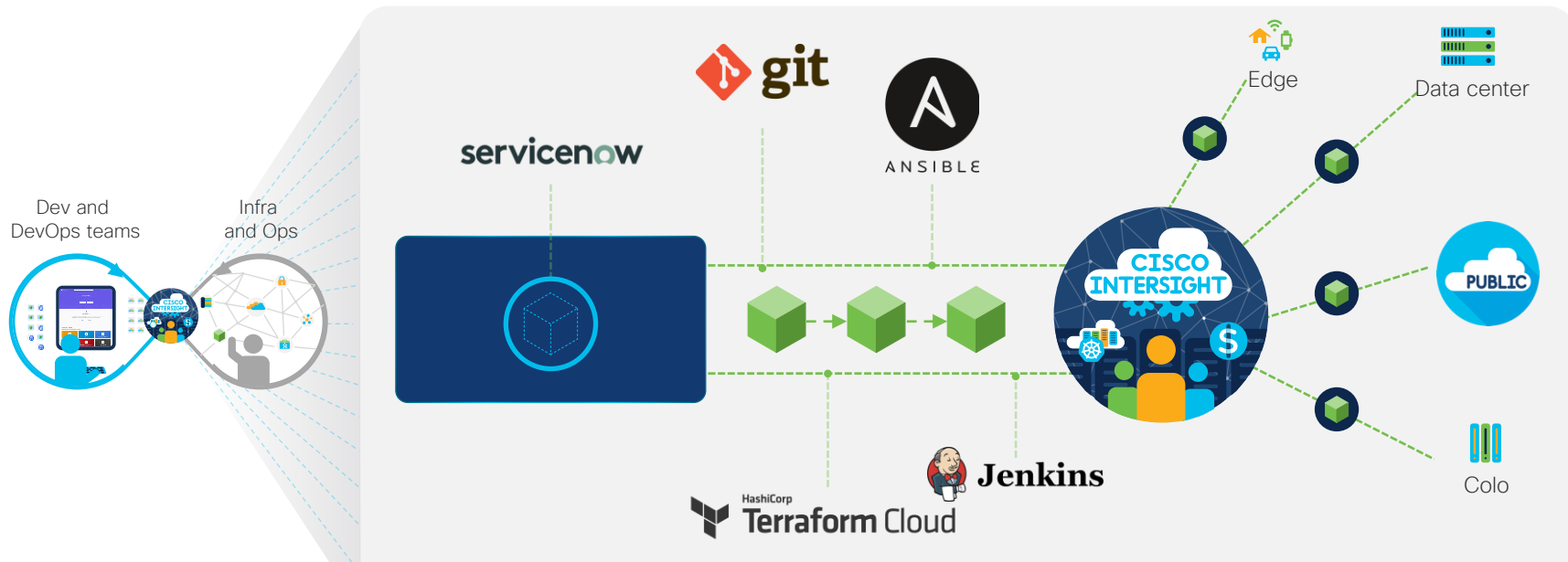


Application Insights



Integrate with DevOps to accelerate application delivery

API as the Leading Interface



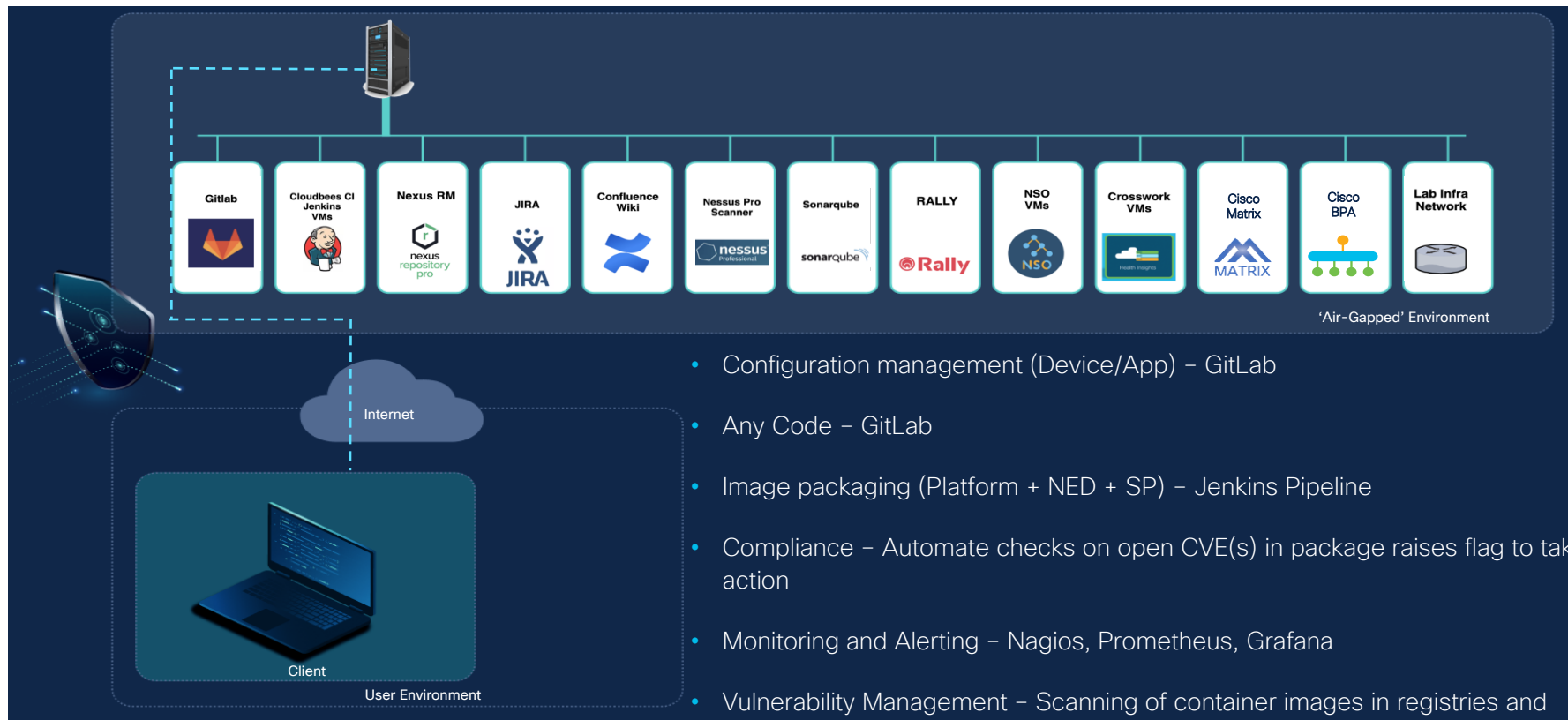
Accelerate CI/CD processes and extend infrastructure as code (IaC) workflows by integrating Intersight into your DevOps toolchains

Intersight and Terraform Cloud provide end-to-end, cross domain coverage for the management, orchestration and consumption of your private and public cloud environments

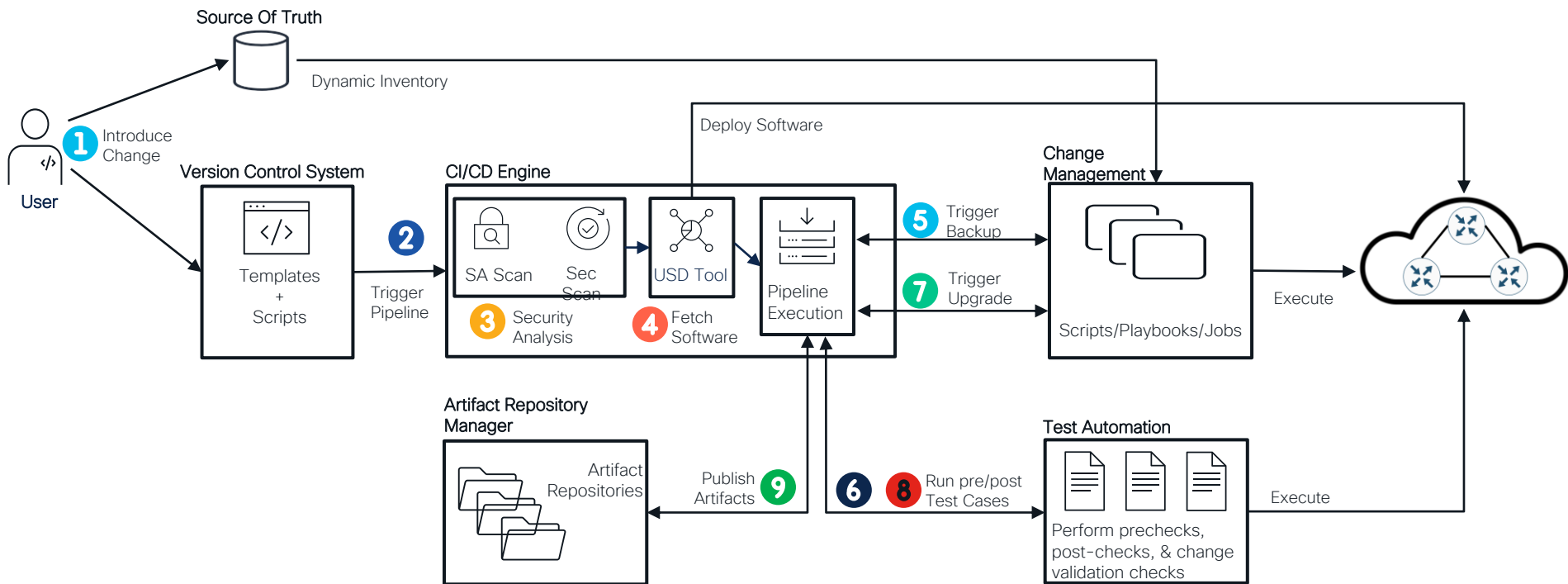
Intersight is a next-generation, hybrid cloud operations platform that visualizes, optimizes, and automates applications and infrastructure

DevSecOps Pipelines for Service Release Management

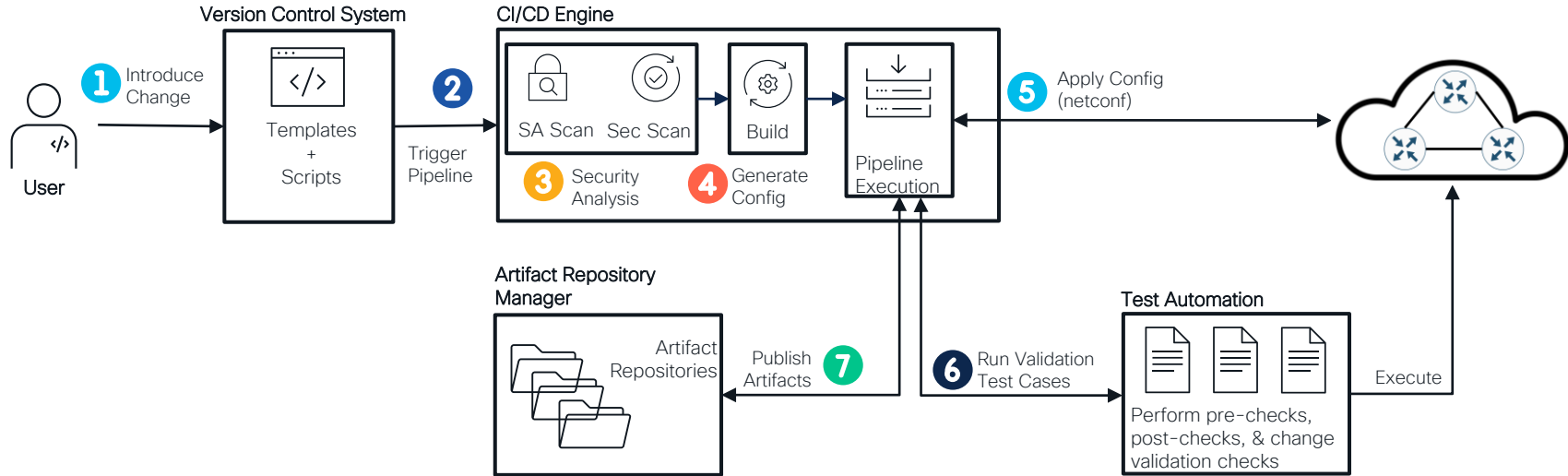
Accelerate Infrastructure Lifecycle



Automated Pipeline for Device Software Upgrade Example



Pipeline for Configuration Deployment Example



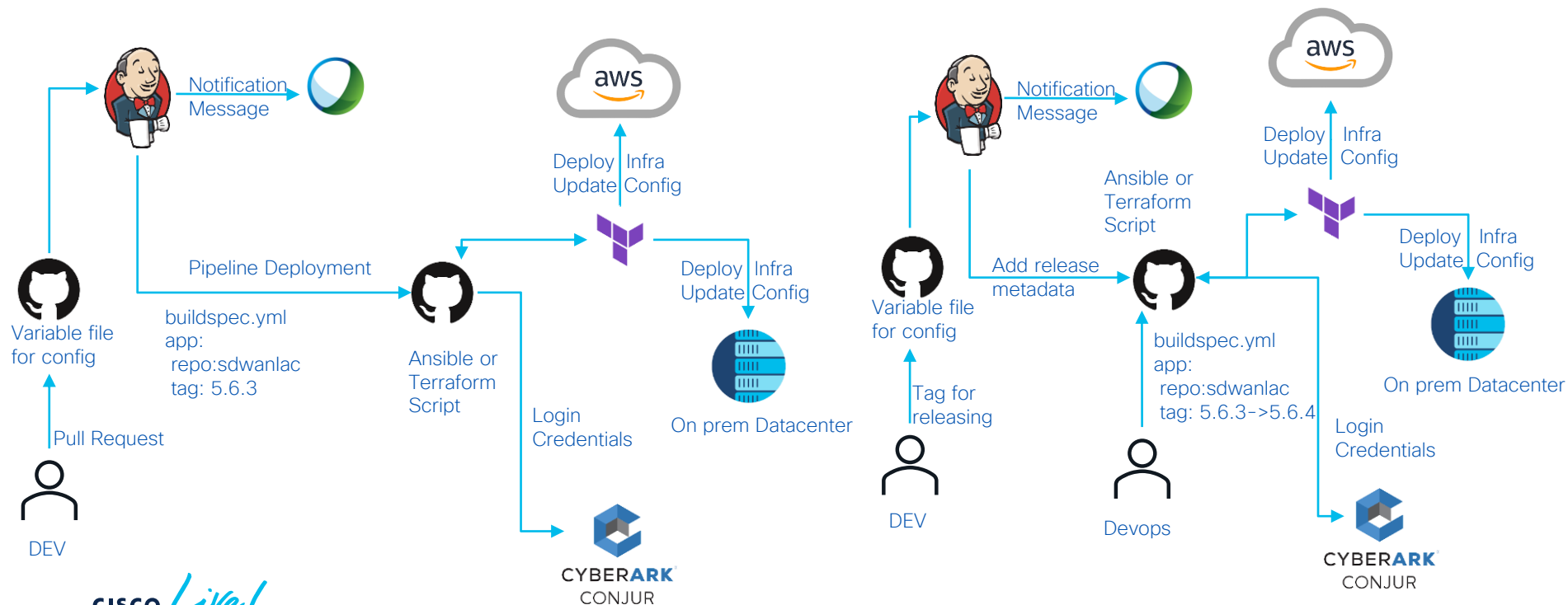
Service Release Management Flow Example

Build

Lab deployment and Testing

Release

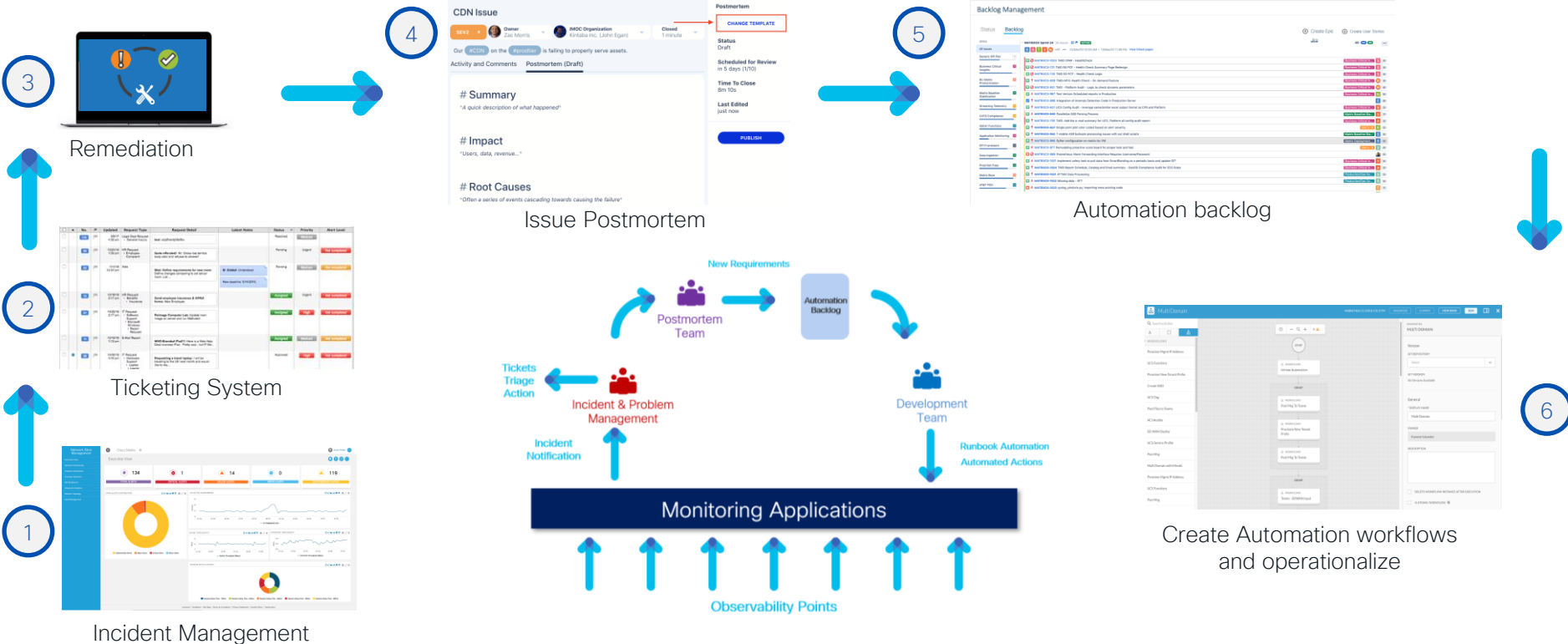
Production Deployment and Testing



Site Reliability Engineering

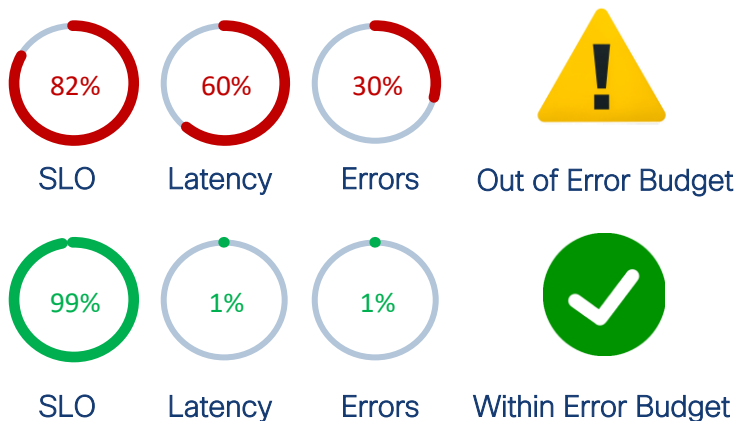
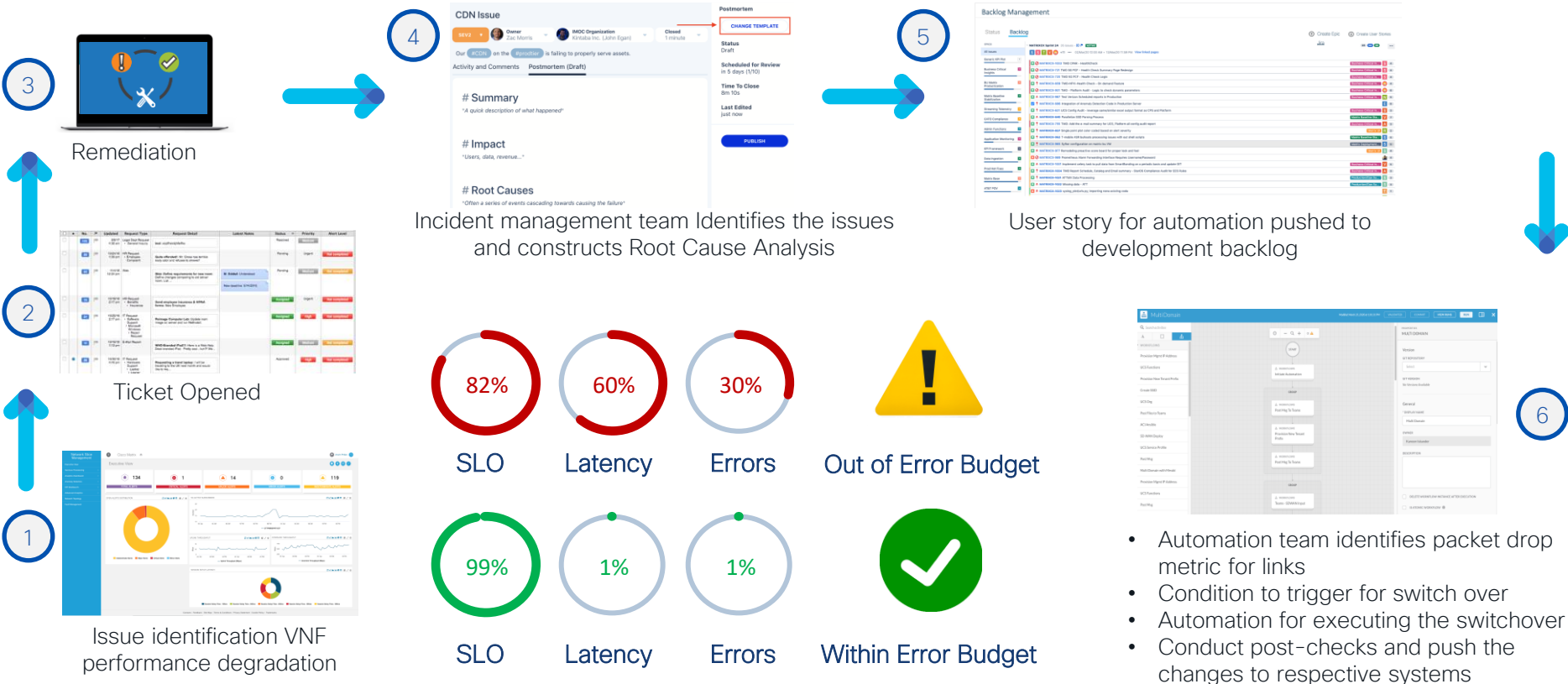


Incident Remediation – Codify to Improve Resilience



Continuous improvements through codification to reduce MTTR

Incident Remediation – Codify to Improve Resilience Example



- Automation team identifies packet drop metric for links
- Condition to trigger for switch over
- Automation for executing the switchover
- Conduct post-checks and push the changes to respective systems

Key Takeaways

Key Takeaways



Automation & Orchestration establish control points



DevSecOps and CloudOps practices are embedded in service delivery



Network intelligence enables visibility and insights for action



Cloud-First Mindset



Speed with Safety



Full-Stack Observability

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is 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!*

ALL IN