CISCO Live!

#CiscoLive

The bridge to possible

Deploying Cisco Secure Cloud Native Security using GitOps

Ed McNicholas
Sr. Technical Solutions Architect - Cybersecurity
BRKSEC-2353

Cisco Webex App

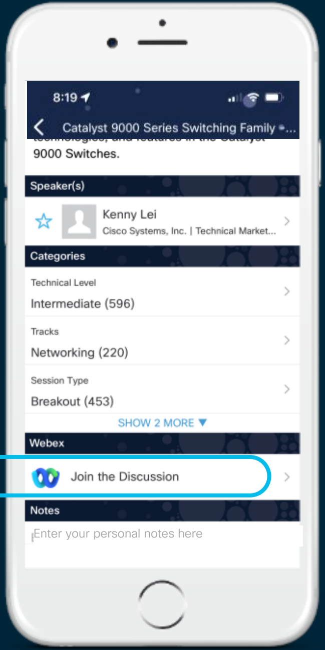
Questions?

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

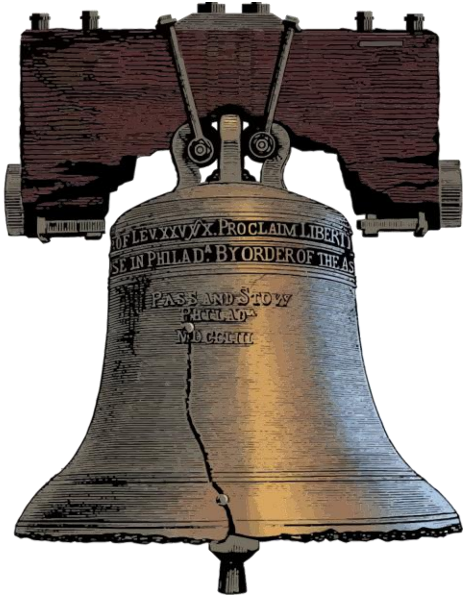
Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2353

About Your Speaker

- Sr. Technical Solutions Architect
- 6 years at Cisco - 20+ years of Network and Security Experience
- Prior to Cisco
  - Product Architect for Manage Service Provider
  - Senior Architect for Financial Services Provider
- Lives in Philadelphia, PA


OF LEV. XXV. V X. PROCLAIM LIBERT
SE IN PHILAD^A BY ORDER OF THE AS
PASS AND STOW
PHILAD^A
MDCCLIII

Agenda

- Introduction
- GitOps and Infrastructure as Code
- Security Analytics and Threat Detection
- Workload Protection
- Cloud Native Application Protection
- Application Security
- Conclusion

Introduction

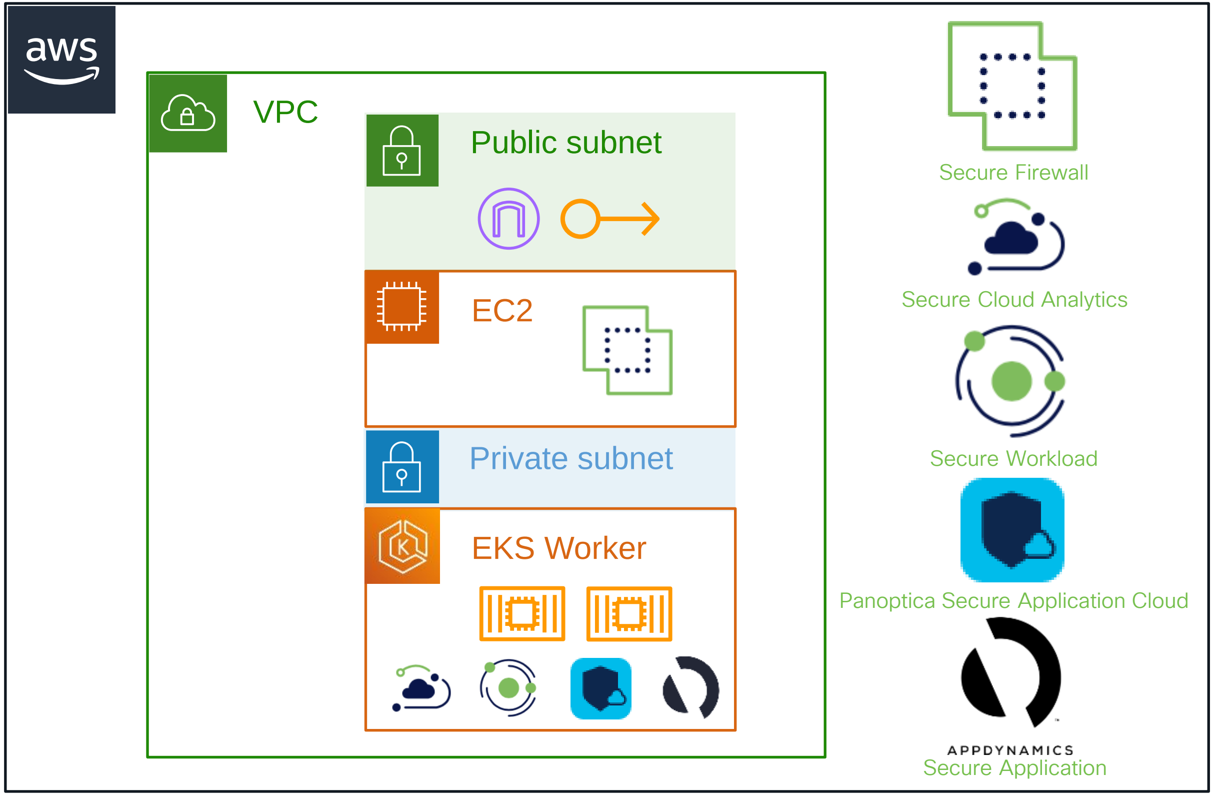
GitHub

https://github.com/emcnicholas/BRKSEC-2353_Deploying_Cisco_Secure_Cloud_Native_Security_using_GitOps

The Design

Securing the Full Stack

- Infrastructure
  - Cloud, VPC, EC2, EKS
  - Secure Firewall
- Security Analytics and Threat Detection
  - Secure Cloud Analytics
  - Secure Cloud Insights
- Workload Protection
  - Secure Workload
- Cloud Native Application Protection
  - Panoptica “The Secure Application Cloud”
- Application Security
  - Secure Application (AppD)



AWS CLI Jenkins GitHub HashiCorp Terraform ANSIBLE kubernetes

GitOps and Infrastructure as Code

What is GitOps?

GitOps is an operational framework that takes DevOps best practices used for application development such as version control, collaboration, compliance, and CI/CD tooling, and applies them to infrastructure automation.

Source:
GitLab

Setting up the Development Environment

- Source Code Repository
- CI/CD Pipleline
- Infrastructure as Code

Demo

Recap Development Environment

- Source Code Repository
  - GitHub: Source Code Management and Version Control
- CI/CD Pipleline
  - Jenkins Multibranch Pipeline Project
  - Jenkinsfile (aka Pipeline as Code)
- Infrastructure as Code
  - Terraform Modules to provision infrastructure
  - Ansible Playbooks and Docker Image to configure Policy

Security Analytics and Threat Detection

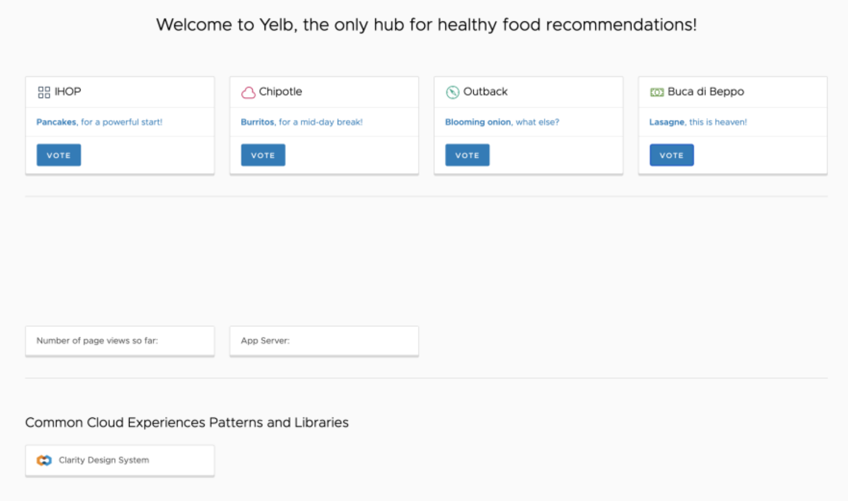
Visibility, analytics, and threat detection of microservice applications

- Deploy Cloud Native Application

- Deploy Cisco Secure Cloud Analytics

- Dive into visibility, threat detection and alerting

Yelb – Microservice Application



Welcome to Yelb, the only hub for healthy food recommendations!

IHOP

Pancakes, for a powerful start!

VOTE

Chipotle

Burritos, for a mid-day break!

VOTE

Outback

Blooming onion, what else?

VOTE

Buca di Beppo

Lasagne, this is heaven!

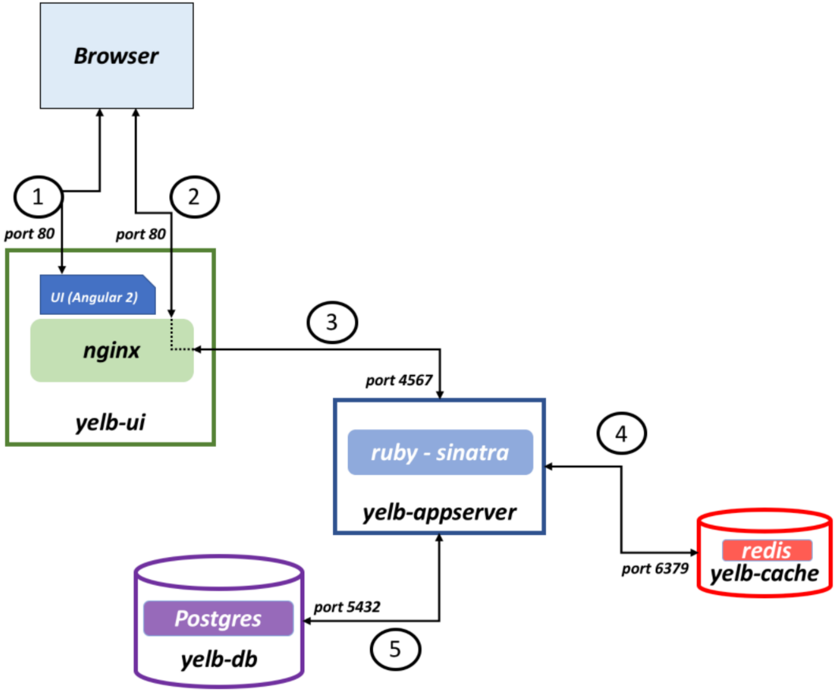
VOTE

Number of page views so far:

App Server:

Common Cloud Experiences Patterns and Libraries

Clarity Design System

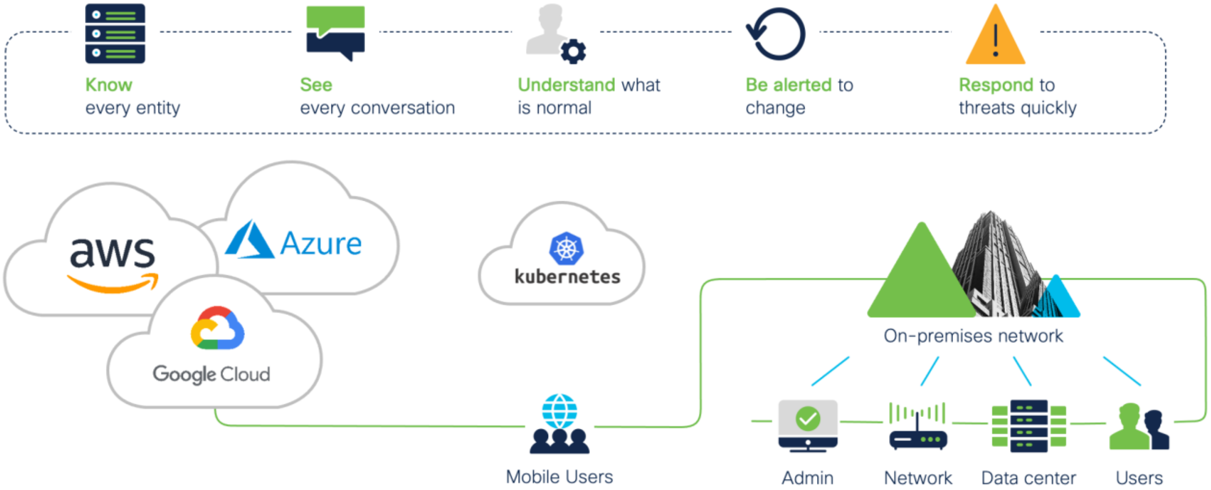


https://github.com/mreferre/yelb

Cisco Secure Cloud Analytics

- Identify all assets in cloud and on-prem
- Visibility into all flows and connections
- Baseline normal activity
- Alert based of Anomalies
- Respond to threats quickly
- Deployed using Terraform

Effective security depends on total visibility



Demo

Recap Secure Cloud Analytics

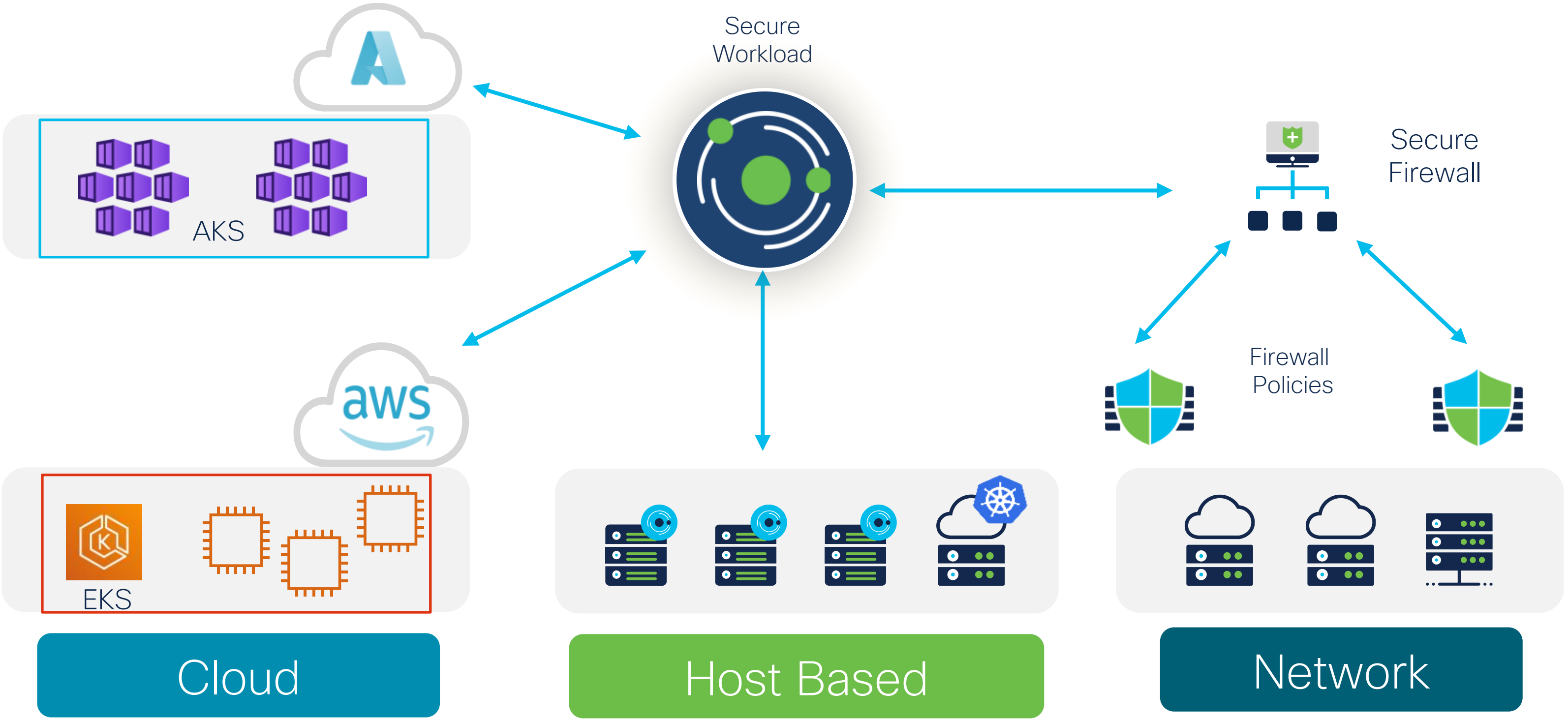
- Deploy Cloud Native Application
  - Yelb - 3-tier microservices application
- Deploy Cisco Secure Cloud Analytics
  - Terraform module – installed using daemonset in Kubernetes cluster
- Dive into visibility, threat detection and alerting
  - Detected IoCs, Insider Threats, Malicious Activity
  - MITRE tactics and techniques
  - Triggered Alerts

Workload Protection

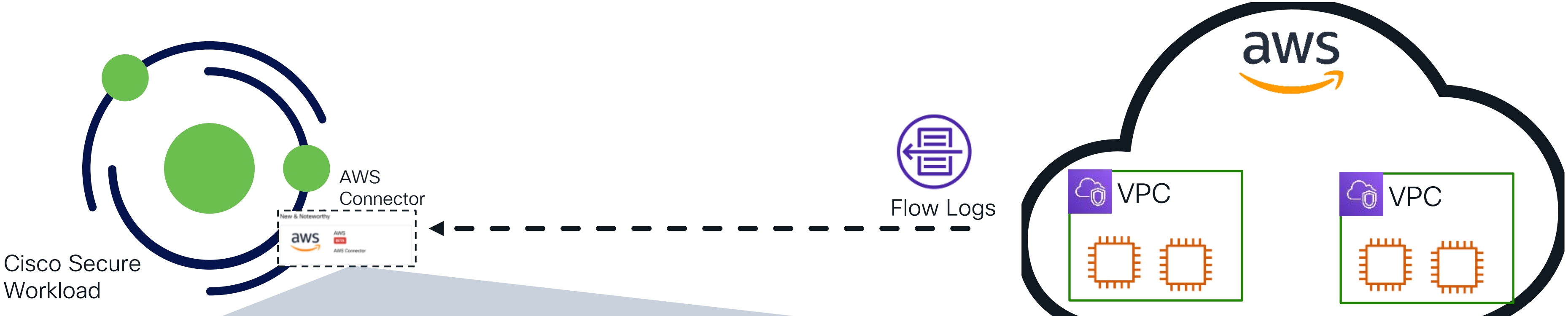
Micro-segmentation for Microservice Applications

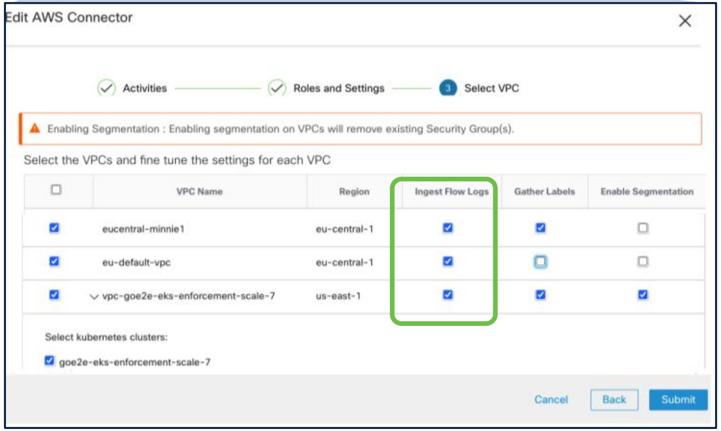
- Deploy Cisco Secure Workload
- Define annotations for pods and services
- Deploy micro-segmentation policy as code
- Enable enforcement

Unified Policy across host, network and cloud



Secure Workload Cloud Connector





⚠ Enabling Segmentation : Enabling segmentation on VPCs will remove existing Security Group(s).

Select the VPCs and fine tune the settings for each VPC

□	VPC Name	Region	Ingest Flow Logs	Gather Labels	Enable Segmentation
☑	eucentral-minnie1	eu-central-1	☑	☑	□
☑	eu-default-vpc	eu-central-1	☑	□	□
☑	∨ vpc-goe2e-eks-enforcement-scale-7	us-east-1	☑	☑	☑

Select kubernetes clusters:

☑ goe2e-eks-enforcement-scale-7

- AWS Connector consolidates:
  - VPC flow logs ingestion
  - Context gathering (AWS tags and labels)
  - AWS cloud-managed Kubernetes orchestration (Kubernetes object labels and annotations)
  - Agentless Enforcement – Enforce segmentation using AWS Security Groups

Demo

Recap Secure Workload

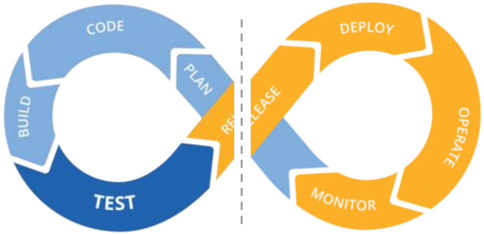
- Deploy Cisco Secure Workload
  - AWS Connector
  - Daemonset deployment script
- Define annotations for pods and services
  - Create Inventory Filters
- Deploy microsegmentation policy as code
  - Terraform module – deployed segmentation policy
- Enable enforcement
  - Segmentation policy applied and reviewed traffic flow inside the Kubernetes cluster

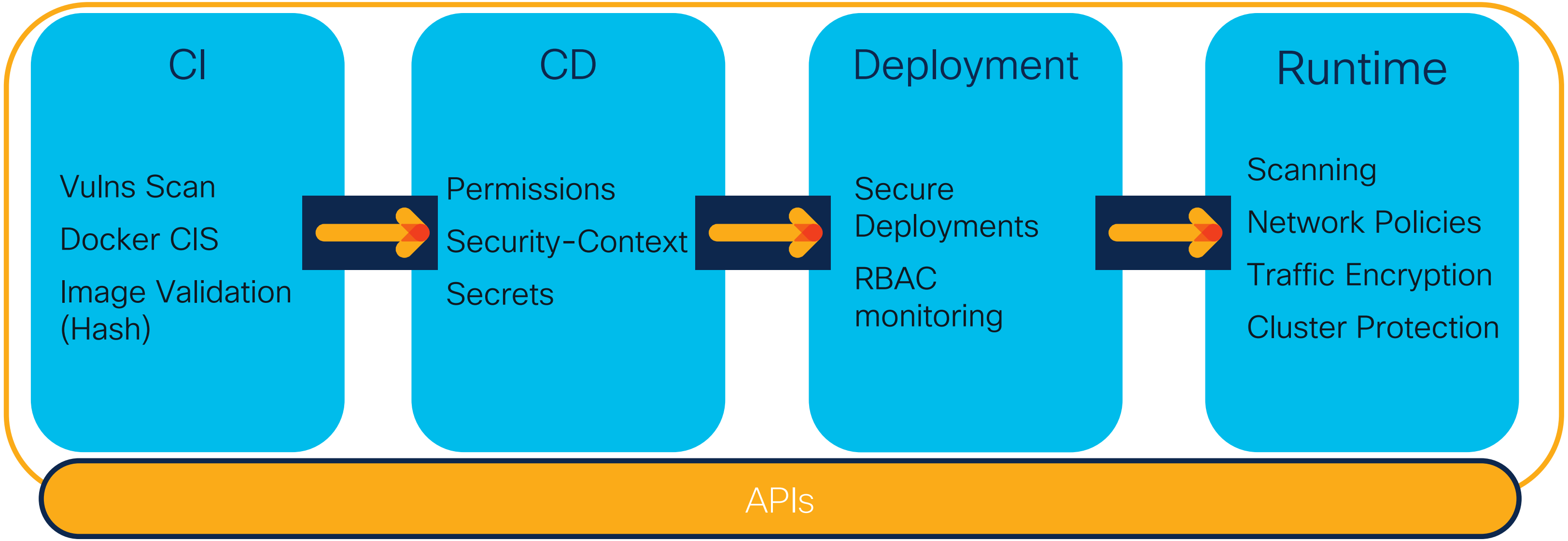
Cloud Native Application Protection

Securing Kubernetes, Containers, Pods and APIs

- Deploy Panoptica “The Cisco Secure Application Cloud”
- CI/CD Plugins
- Runtime Policies
- Risk Assessment

Panoptica





CI

Vulns Scan

Docker CIS

Image Validation (Hash)

CD

Permissions

Security-Context

Secrets

Deployment

Secure Deployments

RBAC monitoring

Runtime

Scanning

Network Policies

Traffic Encryption

Cluster Protection

APIs

Demo

Securing Kubernetes, Containers, Pods and APIs

- Deploy Panoptica
  - Terraform – Istio Service Mesh and Secure App Cloud Controller
- CI/CD Plugins
  - CI – Jenkins
  - CD - Terraform
- Runtime Policies
  - Deployment, Connection, Event, and API
- Risk Assessment
  - K8Shield – Mapping to MITRE

Application Security

Secure Applications at Runtime

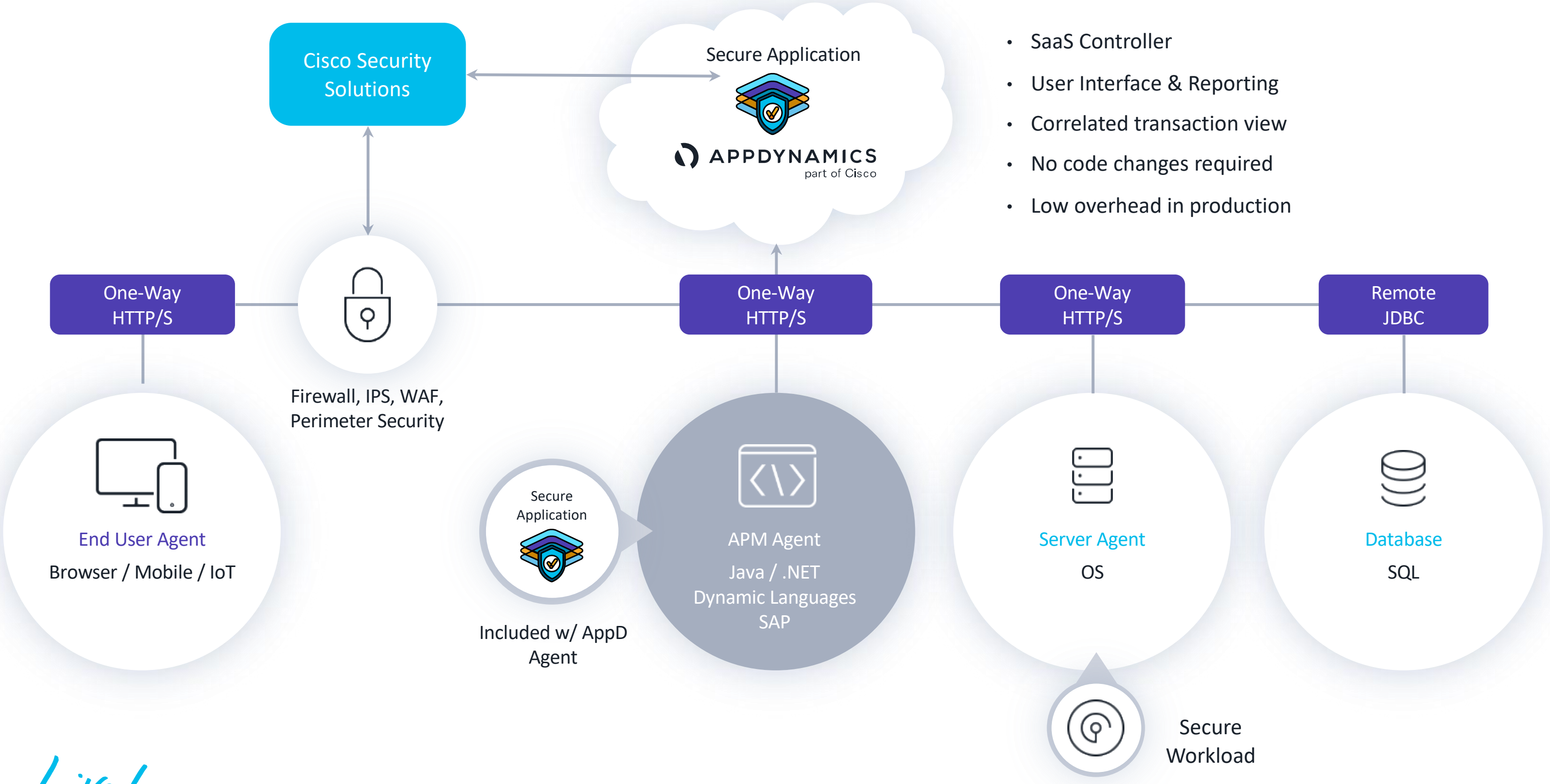
- Deploy Cisco Secure Application (AppD)

- Security Visibility in Application Native Context

- Vulnerability Assessment and Remediation

- Attack Detection and Protection

Cisco Secure Application



- SaaS Controller
- User Interface & Reporting
- Correlated transaction view
- No code changes required
- Low overhead in production

Demo

Recap Secure Applications at Runtime

- Deploy Cisco Secure Application (AppD)
  - Application Performance Monitor (APM) on Java Virtual Machine (JVM)
- Security Visibility in Application Native Context
  - Full map of Application
- Vulnerability Assessment and Remediation
  - Vulnerable libraries and Remediation versions
  - Policy rules to dynamically patch
- Attack Detection and Protection
  - Attack types, Event triggers, Commands and Stack Traces

Conclusion

Security up the stack

- Built cloud native infrastructure using GitOps
  - DevOps tools – Jenkins, GitHub, Terraform, Ansible, Kubectl, AWS CLI
- Security Analytics and Threat Detection
  - Cisco Secure Cloud Analytics – Visibility, detection and alerting
- Workload Protection
  - Cisco Secure Workload – Micro-Segmentation and visibility
- Kubernetes and Container Security
  - Cisco Secure Application Cloud – CI/CD integration, container and API policies
- Application Security
  - Cisco Secure Application (AppD) – App visibility, vulnerabilities, attacks and events

Resources

- Cloud Native Security Blogs and Videos
  - https://blogs.cisco.com/tag/cloud-native-security
- GitHub Repository
  - https://github.com/emcnicholas/BRKSEC-2353_Deploying_Cisco_Secure_Cloud_Native_Security_using_GitOps
- FREE
  - Secure Firewall AWS: https://aws.amazon.com/marketplace/pp/prodview-mpk3c2gkda3w4
  - Cloud Analytics https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html
  - Secure Workload Sandbox: https://devnetsandbox.cisco.com/RM/Diagram/Index/e95caf39-0b4a-45da-9305-49a65f8dce97?diagramType=Topology
  - Panoptica: https://panoptica.app/
  - Cisco AppDynamics: https://www.appdynamics.com/free-trial/

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