ONSTAK
The experts for the experts

Cisco Secure Workload Platform

Comprehensive workload security for a multicloud datacenter

Introduction

In this Secure Workload Proof of Value engagement, Onstak will introduce the customer to Secure Workload and provide instruction while guiding them through a set of hands-on exercises that will allow them to gain valuable experience with Secure Workload. They will be able to do so in a safe environment and without requiring utilization of their own applications or infrastructure resources by utilizing Onstak's on-demand cloud application environment. This will allow the customer to immediately begin to gain experience implementing the full breadth of Secure Workload features without risk of impediments that might exist if using their own applications and infrastructure, such as having to wait for maintenance windows for agent installation. The hands-on learning will be coupled with knowledge transfer and mentoring from an experienced Secure Workload architect.

Engagement Overview

The engagement will kick off with a 3-day intensive on-site workshop, where the Onstak architect will review the value and benefits of the Secure Workload platform and gather customer requirements from a business, technical and governance perspective.

Prerequisites

- Mutual NDA with OnStak
- Proxy or direct access allowed to Secure Workload SAAS and Environment
- Limited access to the customers cloud environment

Customer personnel

- Security Operations Engineer
- Network Operations Engineer
- Cloud Operations Engineer

Outcomes

- Participants will get full hands-on experience and mentoring during this workshop
- Will have access to the cloud-based, fully simulated environment with various state-of-the-art applications with different Application and OS stacks like
  - -Windows
  - -Linux and
  - -Container-based
- Will get full knowledge of Secure Workload integrations with external applications as
  - -Cisco NGFW
  - -Active Directory
  - -Kubernetes
  - -Cisco ISE
  - -Cisco ASA
  - -Amazon AWS
- During and Post-workshop, participants will have the environment access to experiment, observe and enable themselves

This will be followed by presentations of the topics to be covered in the hands-on sections of the workshop and mentoring while the customer participants walk through the exercises.

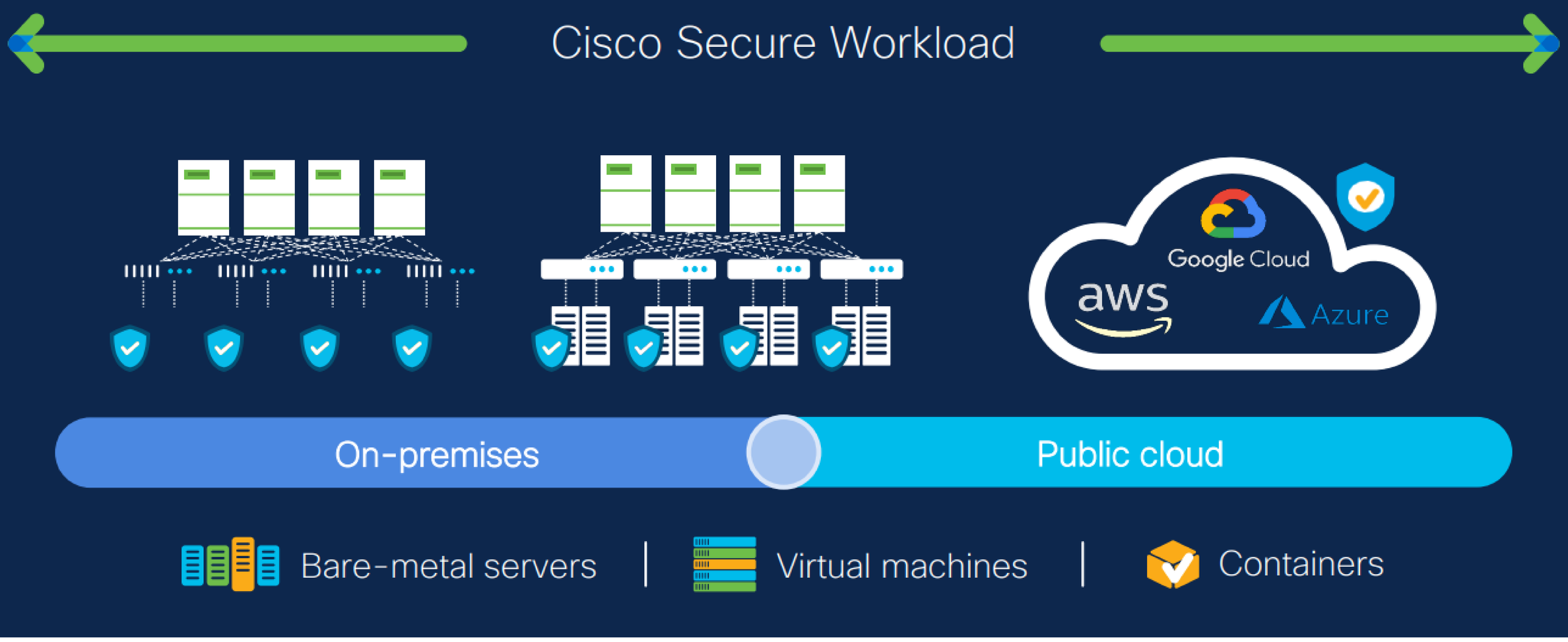
Onstak Inc. 1525 McCarthy Blvd; Suite 1123, Milpitas, CA 95035 USA

Workshop Details

- Introduction to Secure Workload
- Collection Rules
- Agent Installation – Linux
- Agent Installation – Windows
- Agent Config Intent
- Annotations
- External Orchestrators – AWS
- External Orchestrators - Kubernetes
- Scopes
- Ingest Appliance – VPC Flow Logs
- Ingest Appliance – ASA NAT Stitching
- ISE Integration
- Forensics Analysis (Attack & Post Attack)
- Inventory Filters
- Application Discovery & Mapping
- Policy Creation
- Policy Tuning
- Hierarchical Policies
- User-Based Policies
- Enforcement – Linux Application
- Enforcement – Windows Application
- Container Policies & Enforcement
- Security Visibility & Monitoring

****Onstak may add/remove topics as needed based on customer interest

Zero trust microsegmentation



Follow up support

After the workshop, we will conduct three 60-minute follow-up WebEx sessions to review the progress the customer participants have made in completing the Secure Workload work flows, as well as answer any questions that they may have with regard to moving forward with deploying Secure Workload into their own environment. We will conclude the project with a 2-hour, strategy and roadmap session where we will tie the customer's lessons learned from their interaction with the platform to the requirements that were gathered at the beginning of the engagement.

Contact us at info@onstak.com

Onstak Inc. 1525 McCarthy Blvd; Suite 1123, Milpitas, CA 95035 USA