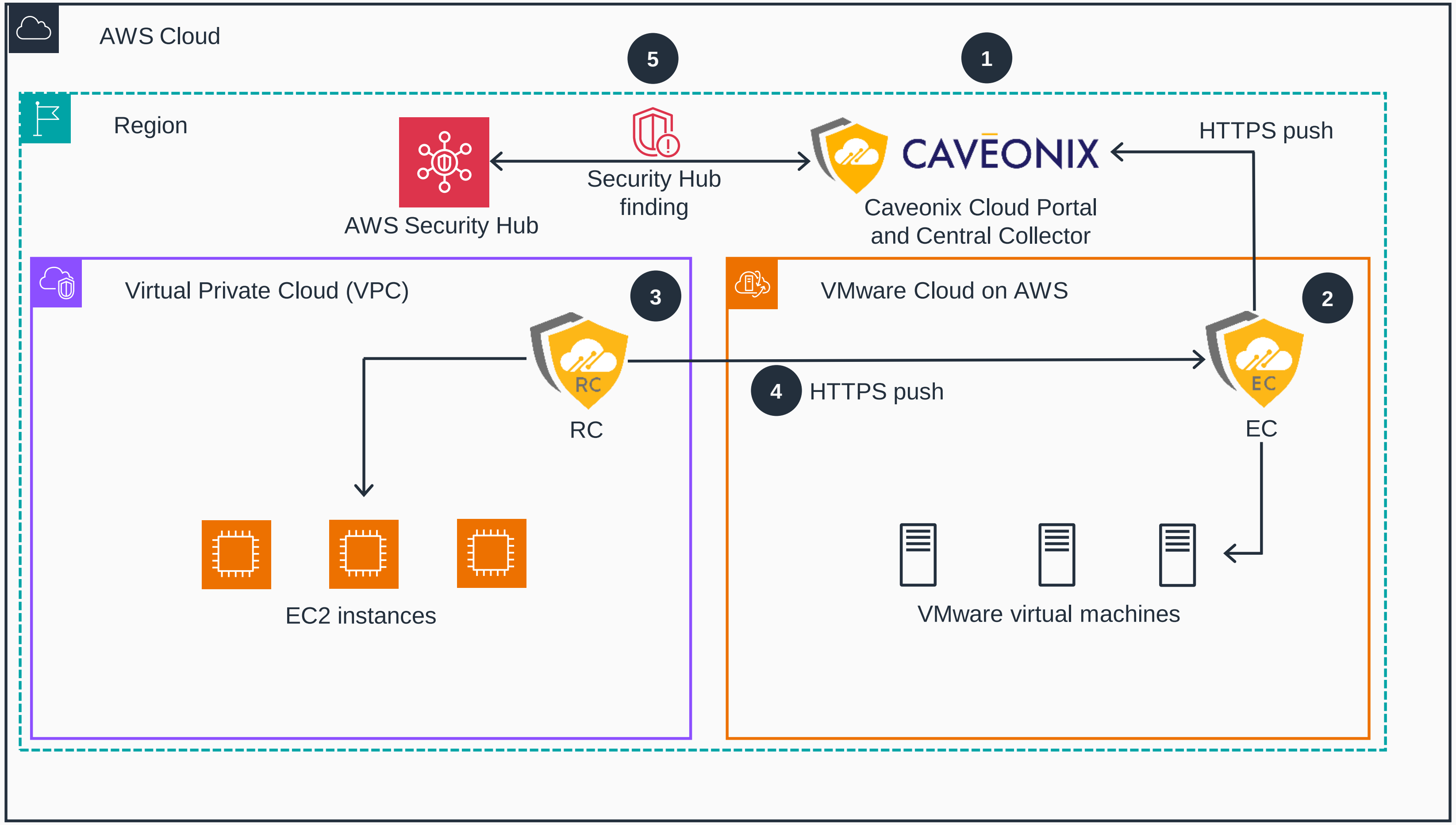
Guidance for Security Compliance and Assurance of VMware and Amazon EC2 Workloads

This architecture diagram shows you how to monitor security compliance and assurance for VMware, AWS, and hybrid workloads.



1 Subscribe to Caveonix Cloud and select the appropriate subscription tier. The product is listed on the **AWS Marketplace**, and private offers are common to negotiate a discount. The Caveonix Cloud Portal and Central Collector are software-as-a-service (SaaS) components managed by Caveonix. The Central Collector queries AWS, **VMware Cloud on AWS**, and other APIs.

2 Deploy an Enterprise Collector (EC) appliance inside the **VMware Cloud on AWS** environment. The EC role performs subnet and virtual machine scanning and includes the Remote Collector (RC) role. A dedicated RC can be deployed in networks unreachable by the EC.

3 Deploy an RC in your **Amazon Virtual Private Cloud (Amazon VPC)** to scan **Amazon Elastic Compute Cloud (Amazon EC2)** instances. The subscription includes unlimited scanning.

4 The RC pushes findings and configuration data to the EC. The EC pushes findings and configuration data to the Central Collector. Data is always pushed outwards using HTTPS, and no firewall ports need to be opened inbound.

5 Caveonix Cloud integrates with **AWS Security Hub** by sending and receiving findings. **Security Hub** can monitor all incidents captured through the Caveonix integration.

Reviewed for technical accuracy November 28, 2023

AWS Reference Architecture