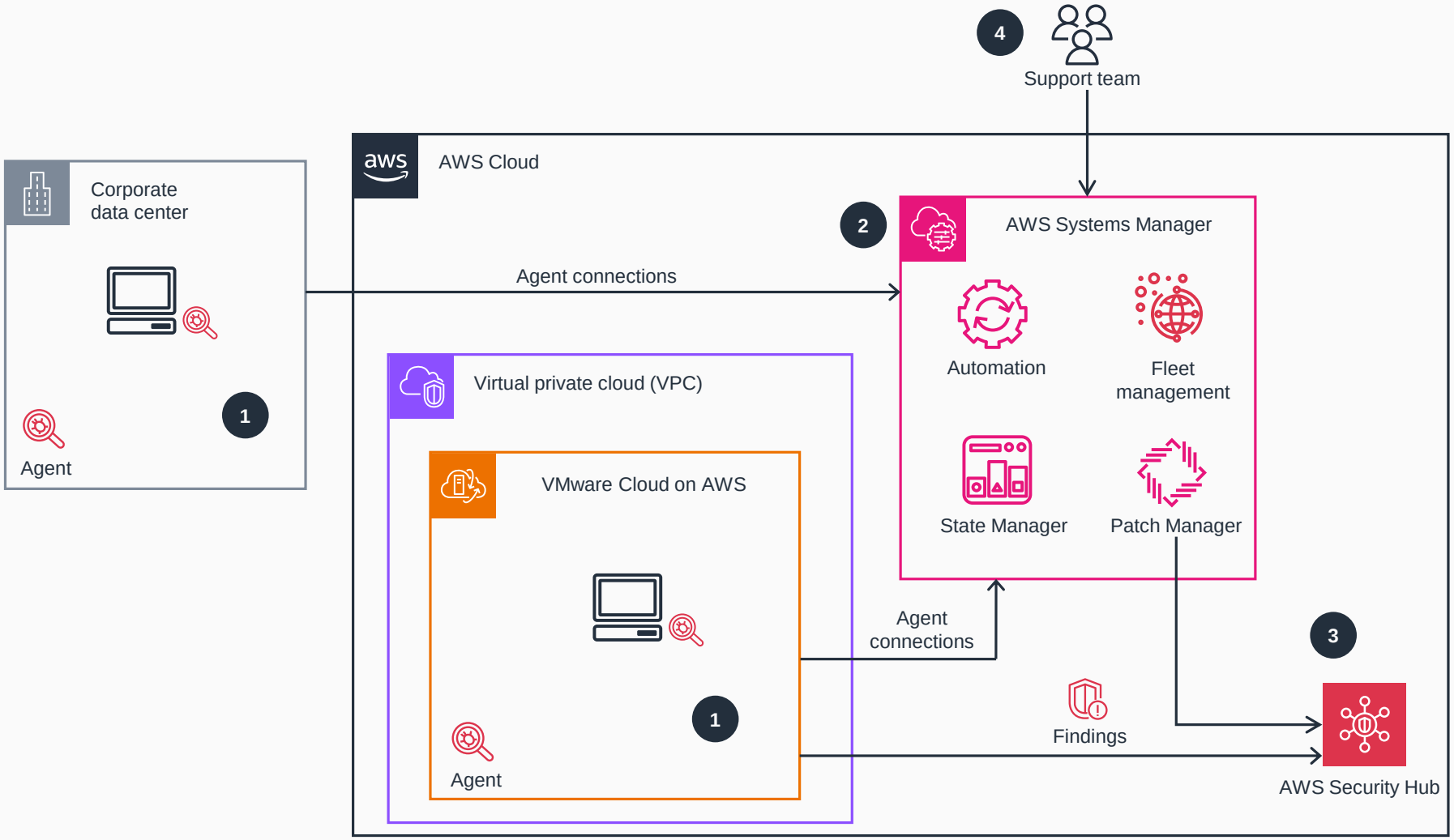
Guidance for Security Compliance and Patching of VMware and Amazon EC2 Workloads

This architecture diagram shows how to set up security compliance and patching of Amazon EC2 and VMware based workloads running on VMware Cloud on AWS as well as on-premises vSphere VMs.



1. This Guidance requires an inventory and data collection from the workloads. **AWS Systems Manager** uses an agent (**SSM Agent**). Install the **SSM Agent** into the **VMware Cloud on AWS** or on-premises nodes to manage. The **SSM Agent** requires communication with the AWS API over standard HTTPS ports. Because the **SSM Agent** always starts the communication, allowing any inbound rules is not necessary (egress tcp ports 443 and 80).

2. **Systems Manager** is the operations hub for your AWS applications and resources and is broken into four core feature groups: Operations Management, Application Management, Change Management, and Node Management.

3. **AWS Security Hub** enables automated checks for standard best practices, such as **AWS Foundational Security Best Practices** (FSBP), **Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 and v1.4.0**, and **Payment Card Industry Data Security Standard (PCI DSS)**.

   Note: At the time of publication of this Guidance, **Security Hub** reports the resource type of all managed nodes as "**Amazon Elastic Compute Cloud (Amazon EC2)** instance." This includes on-premises servers and VMs that you have registered for use with **Systems Manager**.

4. Support teams log in to **Systems Manager** to perform administrative tasks, such as hybrid activations and patch policy creation.

Reviewed for technical accuracy March 6, 2024

AWS Reference Architecture