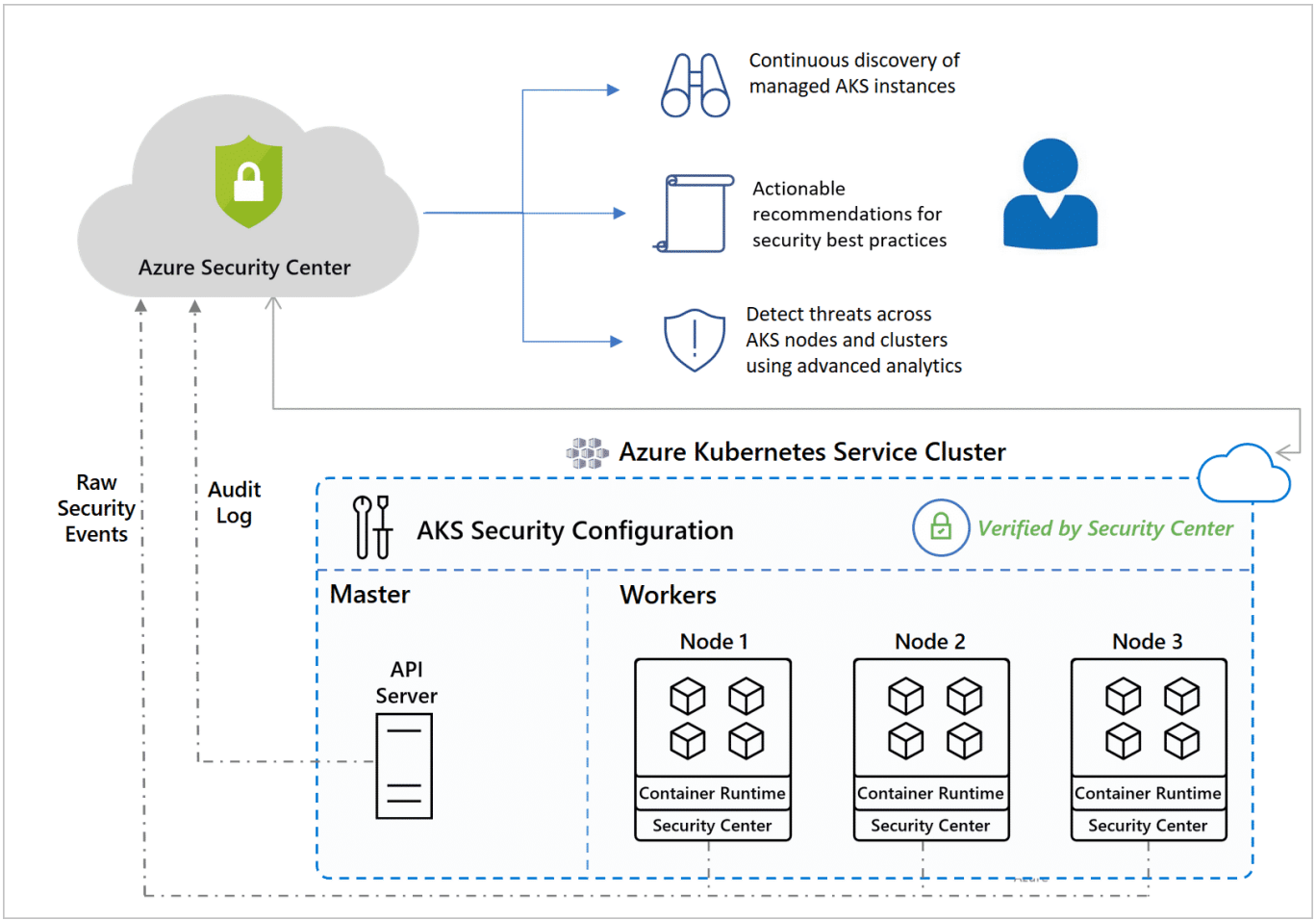
Conteneurs : Microsoft développe une couche de sécurité sur Azure

La « protection contre les menaces pour les conteneurs Azure » entre dans une nouvelle phase.

Microsoft vient d'annoncer la disponibilité générale de cette fonctionnalité accessible avec la version payante du Centre de sécurité Azure.

La tarification n'est pas encore connue. Elle se fera au vCore/h.

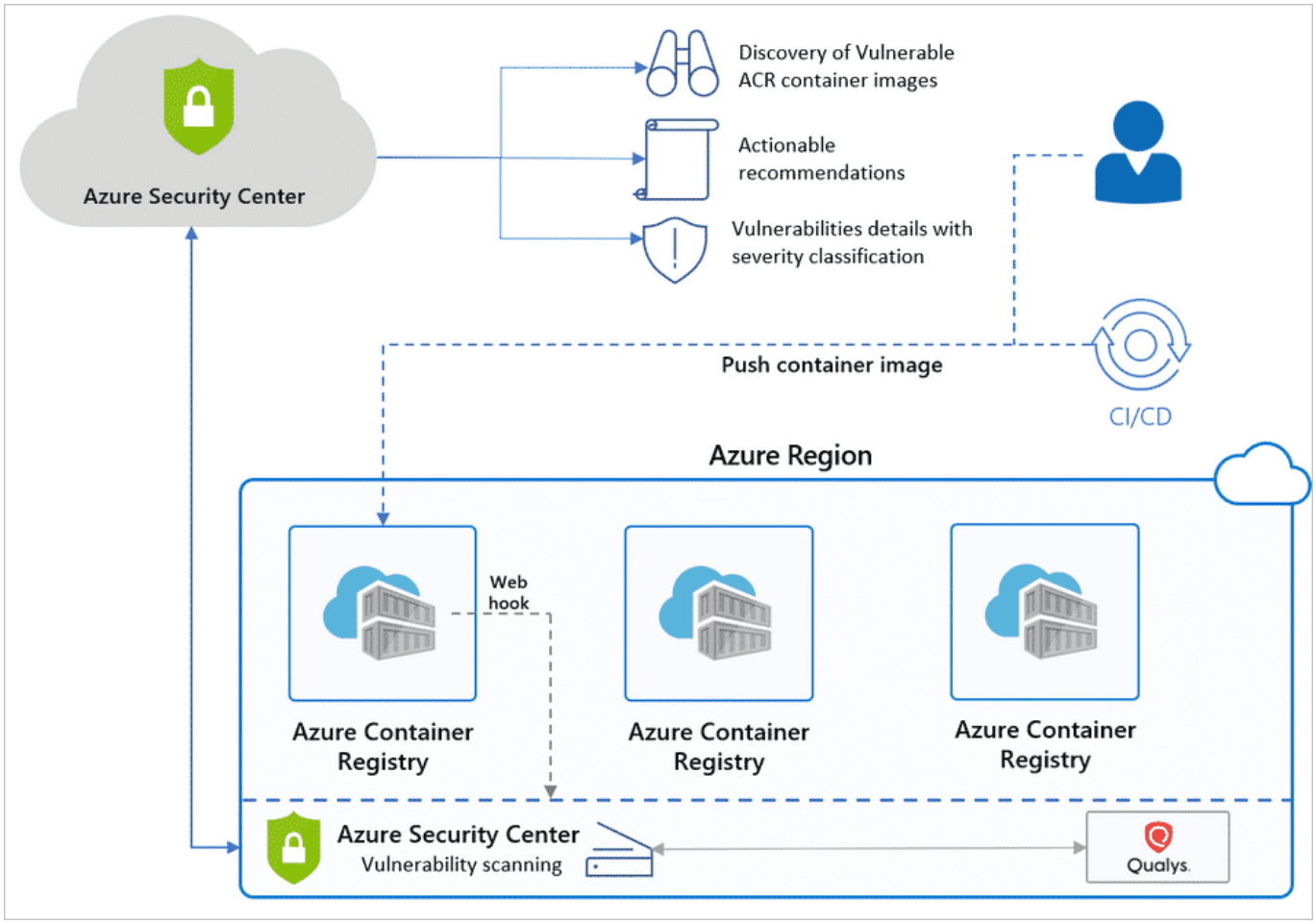
La promesse : sécuriser, à la fois au niveau des hôtes et des clusters, les déploiements réalisés avec AKS, le Kubernetes managé de Microsoft.



Au niveau des hôtes, la protection de base comporte des alertes liées à l'analyse réseau et aux communications avec des serveurs malveillants.
L'installation d'un agent permet d'enrichir les capacités de la solution : détection de commandes privilégiées dans les conteneurs, de demandes suspectes à l'API ou au tableau de bord Kubernetes…

Au niveau des clusters, la protection se fonde sur l'analyse des journaux d'audit de Kubernetes. Elle ne requiert pas d'agent.

Un autre service est en voie d'intégration au Centre de sécurité : Azure Container Registry. La passerelle reste en préversion à l'heure actuelle.



En parallèle, Microsoft ajoute, sur la *marketplace* Azure, l'OS Flatcar.

Ce Linux léger est destiné à la gestion des environnements de conteneurs. Il s'agit d'un *fork* de CoreOS Container Linux, dont Red Hat a annoncé la fin de vie pour le 26 mai 2020.

Le successeur désigné de CoreOS Container Linux s'appelle Fedora CoreOS. Mais il est encore jeune (sorti de bêta en janvier) et ne remplit pas toutes les fonctions de son prédécesseur. Il n'inclut pas, entre autres, de prise en charge native d'Azure.

*Illustration principale © Andrii Stashko*via*Visualhunt.com / CC BY-NC-ND*