# Sécurité multicloud : un socle désormais solide chez Microsoft ?

Protéger les clusters Kubernetes connectés à Azure Arc ? Defender for Cloud le permet désormais. C'est l'une des deux fonctionnalités introduites ce mois-ci sur cette offre née de la fusion d'Azure Security Center (CSPM, gestion de la posture de sécurité) et d'Azure Defender (CWP, protection des charges de travail).

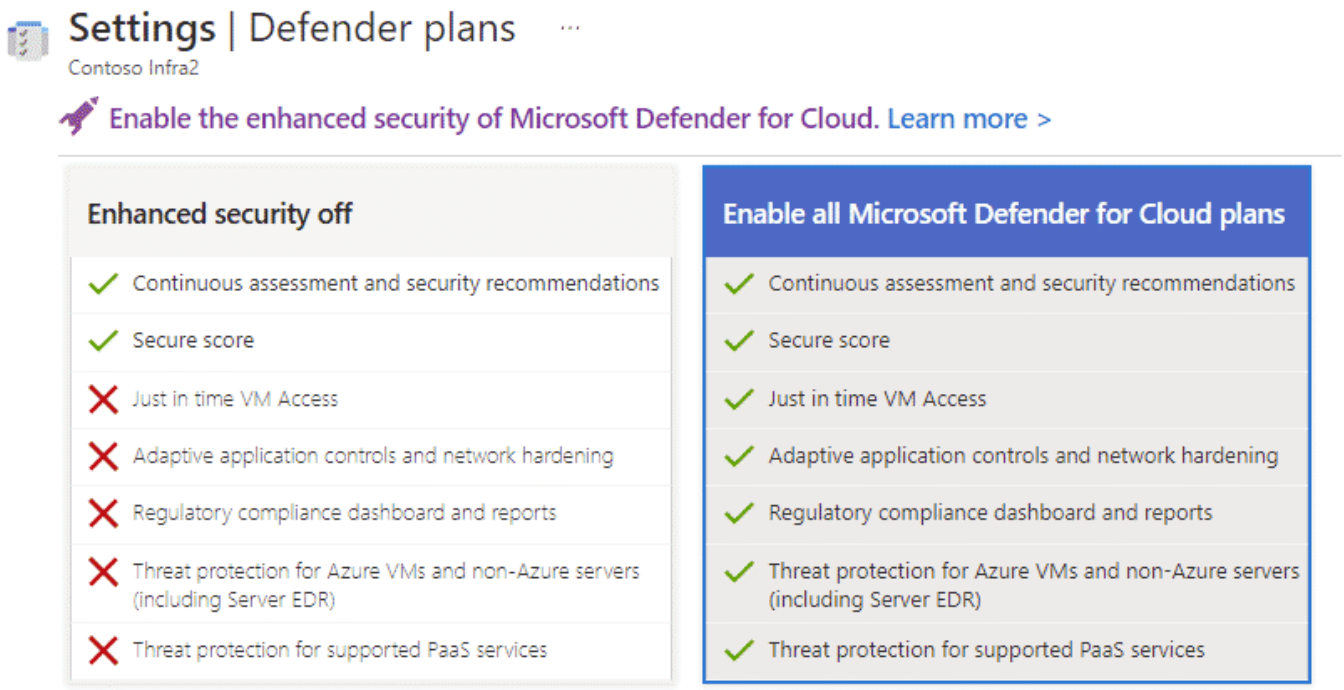
L'autre fonctionnalité cible les environnements Google Cloud. Elle est censée simplifier leur intégration à Defender for Cloud. Et donner accès à davantage d'options de protection.

Jusqu'ici, l'intégration de GCP se faisait nécessairement par l'intermédiaire de connecteurs. Il existe désormais une page spécifique. Le même système est en place pour AWS depuis quelques mois. Avec lui, une fois connecté le compte de gestion, les comptes membres – existants et nouveaux – peuvent s'ajouter automatiquement à Defender for Cloud.

La composante CSPM est utilisable sans agent. Elle évalue la posture de sécurité sur la base de standards (CIS pour GCP et pour AWS ; avec également, pour ce dernier, PCI DSS et FSBP). Il en résulte un « score de sécurité » multicloud englobant aussi les éventuelles ressources Azure et les machines enrôlées *via* Azure Arc.

Sur la partie CWP, on est globalement à parité fonctionnelle entre AWS et GCP. Cela commence avec la protection des VM. À l'appui, notamment, de Defender for Endpoint (EDR) et de la techno Qualys pour le scan de vulnérabilités. Côté conteneurs, les clusters EKS sont pris en charge sur AWS. Sur GCP, Defender for Cloud couvre les clusters GKE Standard.

L'usage de la brique CSPM n'occasionne pas de coûts supplémentaires. Pour le CWP, il y a une panoplie d'options – payantes – à activer en fonction des ressources qu'on souhaite couvrir (Defender for servers pour les VM, Defender for Containers pour les conteneurs…).




Certaines des fonctionnalités disponibles pour les environnements Azure ne le sont pas sur AWS et GCP. Par exemple, l'accès JIT aux VM, le contrôle d'accès aux applications et les alertes de sécurité réseau.

La « nouvelle expérience » de connexion des VM GCP ne dispense pas d'y installer l'agent Azure Arc. Un processus qu'on peut choisir d'automatiser au moment de créer le connecteur.

*Illustration principale* via *Adobe Stock*