Google Cloud Platform accélère sur son offre de sécurité

A l'occasion de sa conférence Cloud Next, Google a multiplié les annonces sur son offre de sécurité. Il s'agit, pour la plupart, de services encore en bêta comme ces « machines virtuelles renforcées » qui associent une technologie *secure boot* sur UEFI et une puce TPM virtualisée pour permettre un suivi en temps réel de l'intégrité des VM.

Clé physique et appliances cryptographiques

Autre service : le contrôle contextuel des accès, sur la base d'éléments comme l'identité des utilisateurs, leur localisation et le niveau de sécurité de leur terminal. Une telle fonction était déjà intégrée dans l'offre *Cloud Identity-Aware Proxy*, pour la gestion des accès aux applications SaaS. En la greffant à l'offre *Virtual Private Cloud Service Controls* (mise en réseau gérée avec protection des données sensibles), Google élargit son périmètre aux API, aux outils de la G Suite et aux logiciels tiers.

En version alpha, Binary authorization doit assurer l'intégrité des conteneurs déployés sur Kubernetes Engine. Idem pour Cloud HSM et ses *appliances* cryptographiques destinées à la gestion des clés de chiffrement (à ne pas confondre avec la solution concurrente d'AWS baptisée CloudHSM, sans espace).

Disponible pour les clients Google Cloud, une case est apparue dans la console d'administration pour activer la prise en charge de la Titan Security Key, une clé physique d'authentification à deux facteurs, déclinée en versions Bluetooth et USB.

Crédit photo : © kubais – Shutterstock.com