Sécurité : Google renforce son cloud avec 20 fonctionnalités

Longtemps, la sécurité des données était le frein le plus souvent évoqué par les entreprises pour ne pas aller dans le cloud. Ce frein est aujourd'hui levé. A grand renfort d'investissements, les fournisseurs s'évertuent même à démontrer que les données sensibles sont davantage à l'abri dans leurs datacenters que sur les infrastructures de leurs clients.

A l'occasion du CEO Security Forum de New York, Google a dévoilé sa feuille de route sur le sujet, annonçant pas moins de vingt nouvelles fonctionnalités et améliorations de dispositifs existants pour renforcer la sécurité de son cloud public, Google Cloud Platform (GCP), et de sa suite collaborative G Suite.

L'annonce majeure porte sur le lancement, en version alpha, de **VPC Service Controls**. Ce nouvel outil de contrôle crée un périmètre de sécurité autour des données sensibles stockées dans les services GCP basés sur les APIs, tels que Google Cloud Storage, BigQuery et Bigtable.

« *Cela permet d'atténuer les risques d'exfiltration de données résultant de la violation d'identités, de mauvaises configurations de politique gestion des identités ou de machines virtuelles compromises »,* précise Jennifer Lin, directrice produit pour la sécurité de GCP.

Également en version alpha, **Cloud Security Command Center** donne un état de santé des services GCP, tels qu'App Engine, Compute Engine, Cloud Storage ou Cloud Datastore. Le service fournit des informations sur l'emplacement où les données sensibles sont stockées, mais également sur les applications susceptibles d'être vulnérables aux attaques de type scripting et injection Flash.

Un bouclier anti DDoS

Pour gérer les politiques de contrôle d'accès, détecter les menaces et les activités suspectes, Google s'associe pour ce service à des spécialistes de la sécurité tels que Cloudflare, CrowdStrike, Dome9, Palo Alto Networks, Qualys et RedLock. Un billet donne une vue exhaustive de ces partenariats.

Avec **Cloud Armor,** Google annonce un service de lutte contre les attaques en déni de service (DDoS) basé *« sur les mêmes technologies et l'infrastructure mondiale* » que Google utilise pour protéger des services tels que Gmail et YouTube.

L'**API DLP** (Data Loss Prevention) permet, elle, de classer, tracer et supprimer des données sensibles sur GCP, un cloud d'un autre fournisseur ou sur les propres serveurs de l'entreprise.

Pour renforcer la confiance de ses utilisateurs, Google propose, avec **Access Transparency**, un journal d'audit venant justifier l'accès de ses équipes d'ingénierie et de support aux services de GCP. Enfin, le géant américain fait de son service managé **Cloud Identity**, présenté en juin dernier, un produit autonome de gestion des identités ou IDaaS (Identity as a Service).

Le machine learning pour lutter contre le phishing

En ce qui concerne G Suite, Google présente toute une panoplie de mesures pour mieux sécuriser sa suite collaborative. Il entend appliquer les modèles de machine learning pour lutter contre le phishing en analysant automatiquement les e-mails provenant d'expéditeurs non approuvés ayant des pièces jointes chiffrées ou des scripts intégrés.

Google renforce également la gestion des terminaux mobiles en instaurant des paramètres de sécurité proactifs par défaut. Plus tôt dans l'année, il avait introduit un centre de sécurité à destination des administrateurs rassemblant les différentes analyses de sécurité et les recommandations de Google en la matière. Ce tableau de bord s'enrichit aujourd'hui de nouveaux graphiques liés à la gestion des mobiles ou au service d'authentification OAuth.

Enfin, Google met en place de nouveaux contrôles de sécurité pour ses Team Drives, ses espaces de travail partagés reposant sur son offre de stockage dans le cloud, en apposant des droits – IRM, Information Rights Management – sur les données sensibles.