Google Cloud Next 19 : ce qu'il faut retenir de la session de Tokyo

Google Cloud a réuni son écosystème deux jours durant lors de Cloud Next '19 à Tokyo.

À cette occasion, la société américaine a réaffirmé dans un billet de blog contribuer au renforcement de la sécurité numérique des entreprises et à la protection des utilisateurs de ses services. Et ce par le biais de mises à jour et d'améliorations.

Voici 4 annonces mises en exergue par la multinationale :

1. Protection étendue aux entreprises >

La programme de protection avancée (Advanced Protection Program) a été conçu, à l'origine, pour renforcer la sécurité de comptes Google personnels d'individus, tels que des militants et des dirigeants, susceptibles d'être visés par des attaques en ligne ciblées.

Le programme est étendu aux clients de G Suite, Google Cloud Platform et Cloud Identity.

Les administrateurs IT peuvent ainsi autoriser les utilisateurs les plus exposés à s'inscrire au programme. L'utilisation de clés de sécurité certifiées FIDO (dont la clé Titan) et le blocage automatique d'accès aux applications tierces non reconnues comme fiables sont au menu. L'activation de la vérification renforcée des emails entrants l'est aussi.

2. Titan arrive au Japon et en France >

Google a également annoncé étendre la disponibilité à l'international de sa clé de sécurité Titan. Le Japon, le Canada, la France et le Royaume-Uni sont concernés.

La clé, périphérique d'authentification à deux facteurs (2FA), est actuellement proposée au prix de 55 euros l'unité sur la version française de Google Store.

3. Alerte automatique dans G Suite >

Les modèles d'apprentissage machine (machine learning) développés par Google sont conçus pour renforcer la détection de risques de sécurité. Des risques associés au partage de fichiers externes et aux autorisations de téléchargements via Google Drive.

Drive est le service de stockage fourni par Google et un composant clé de G Suite.

Dorénavant, les administrateurs en entreprise peuvent être alertés automatiquement via le centre d'alerte de G Suite des risques potentiels d'exfiltration de données associés à des comportements inhabituels repérés dans Google Drive.

Le service de détection d'activité suspecte est actuellement disponible en version bêta.

4. Accès en un clic à des « milliers » d'apps >

Cloud Identity et G Suite supportent déjà l'authentification unique (ou single sign-on, SSO) pour accéder à différents services utilisant des protocoles tels que SAML (Security assertion markup language) et OIDC (OpenID Connect).

Mais la firme de Mountain View veut aussi améliorer la prise en charge d'applications héritées, dont l'accès nécessite encore un nom d'utilisateur et un mot de passe.

Pour ce faire, Cloud Identity va intégrer « dans les prochains jours » le support d'applications gérées avec des mots de passe. Une avancée qui permettra, selon Google, de faciliter l'accès en un clic des utilisateurs à un catalogue étendu d'applications. Les administrateurs, de leur côté, bénéficieront d'un unique point de gestion et de contrôle.

(crédit photo © Google)