

# Sécurité : Google Capital investit dans CrowdStrike

**CrowdStrike** sera-t-elle la 14<sup>e</sup> société à entrer dans le portefeuille de **Google Capital** ? La firme californienne, qui fournit des solutions de cybersécurité aux entreprises et aux gouvernements, est pressentie pour annoncer, cette semaine, son troisième tour de table institutionnel.

L'opération lui permettrait de lever 100 millions de dollars, sur la base d'une valorisation avoisinant le milliard. Une enveloppe qui s'ajouterait aux 26 millions de dollars injectés en février 2012 par le fonds d'investissement new-yorkais Warburg Pincus. Lequel avait également mis au pot en septembre 2013, aux côtés d'Accel Partners (30 millions de dollars ; source [Crunchbase](#)).

Annoncé samedi par [Business Insider](#), ce tour de financement a été confirmé à [Reuters](#) par [Google Capital](#)... dont c'est la première véritable incursion dans le domaine de la sécurité IT. Depuis sa mise sur pied à l'été 2013, la structure – à différencier du fonds de placement [Google Ventures](#), dont l'activité, beaucoup plus indépendante, se concentre sur les jeunes pousses du secteur des nouvelles technologies – a soutenu 13 sociétés.

Sur la liste, on trouve notamment SurveyMonkey (sondages en ligne), Lending Club (prêts entre particuliers ; entré en Bourse le 11 décembre 2014) et Freshdesk (support client multicanal). Mais aussi InnoLight (technologies optiques pour le data center), Glassdoor (mise en relation des recruteurs et des demandeurs d'emploi) ou encore Duolingo (plate-forme d'apprentissage des langues).

## Opération sécuriser Android ?

Google Capital ne compte pas entrer au conseil d'administration de CrowdStrike. Il s'agit plutôt d'accompagner le développement de ses solutions pour la protection des terminaux Android ainsi que des équipements réseau tournant sous Linux (sur lequel est basé Android).

L'hébergeur Rackspace participerait également à ce tour de table qui permettra à CrowdStrike d'étendre sa présence en Europe, en Asie et au Moyen-Orient... et d'élargir son portefeuille de clients, qui comprend déjà « cinq des dix plus grandes banques du monde ».

L'aventure a commencé il y a environ quatre ans, à l'initiative de George Kurtz (aujourd'hui CEO) et Dmitri Alperovitch (CTO), deux anciens de McAfee. CrowdStrike se positionne aujourd'hui comme l'un des principaux concurrents de Mandiant (filiale de FireEye) avec sa plate-forme cloud Falcon, destinée à aider les organisations à détecter et à stopper les attaques informatiques en temps réel, selon [ITespresso](#).

La principale composante de cette offre se nomme Falcon Host. Il s'agit d'un agent qui s'intègre sur les postes de travail (Windows, OS X ; moins de 10 Mo) et qui exploite l'association big data/machine learning pour détecter des anomalies en analysant « des milliards d'événements ».

Pour CrowdStrike, l'objectif est d'aller « au-delà des indicateurs [classiques] de compromission des

*systèmes* » pour toucher aux indicateurs d'attaques, de la phase de reconnaissance à l'exfiltration de données en passant par l'élévation de privilèges et la contamination du réseau.

Dans le prolongement de Falcon Host, les équipes de CrowdStrike fournissent des détails techniques et stratégiques afin de comprendre l'identité des cybercriminels et leurs motivations. Ce qui doit permettre d'anticiper leurs actions et surtout de mieux allouer les ressources de défense.