# BeyondProd : l'approche de Google pour sécuriser les microservices

Comment permettre à des utilisateurs de travailler depuis des réseaux non approuvés sans avoir besoin d'un VPN ?

En 2011, Google avait commencé à se pencher sur la question dans le cadre d'un projet nommé BeyondCorp.

Il s'agissait, à l'origine, d'une initiative interne. Le groupe américain l'a depuis lors ouverte à tous ses clients cloud à travers la solution « Accès contextuel ».

BeyondCorp applique un modèle de sécurité fondé sur des réseaux « zéro confiance ». Il offre un contrôle d'accès non plus au niveau du périmètre réseau, mais au niveau des utilisateurs et des appareils individuels.

Google applique la même approche aux architectures de microservices (dites « cloud-native ») à travers un autre projet : BeyondProd.

Le postulat : tout comme les utilisateurs sont mobiles et se servent de différents appareils à différents endroits, les microservices se déplacent et sont déployés dans différents environnements.

## Changement d'identité(s)

L'approche « zéro confiance » est mise en œuvre avec une solution personnalisée de sécurisation de la couche de transport : ALTS (Application Layer Transport Security).

Proposant un système d'authentification mutuelle et de chiffrement des données en transit, elle s'exécute au niveau de la couche d'application pour protéger les communications RPC (appels de procédures à distance) sur l'infrastructure Google Cloud.

Dans ce modèle de confiance, les identités sont liées à des entités plutôt qu'à un nom de serveur ou à un hôte spécifique. Ce qui facilite la réplication des microservices, l'équilibrage de charge et la replanification entre les hôtes.

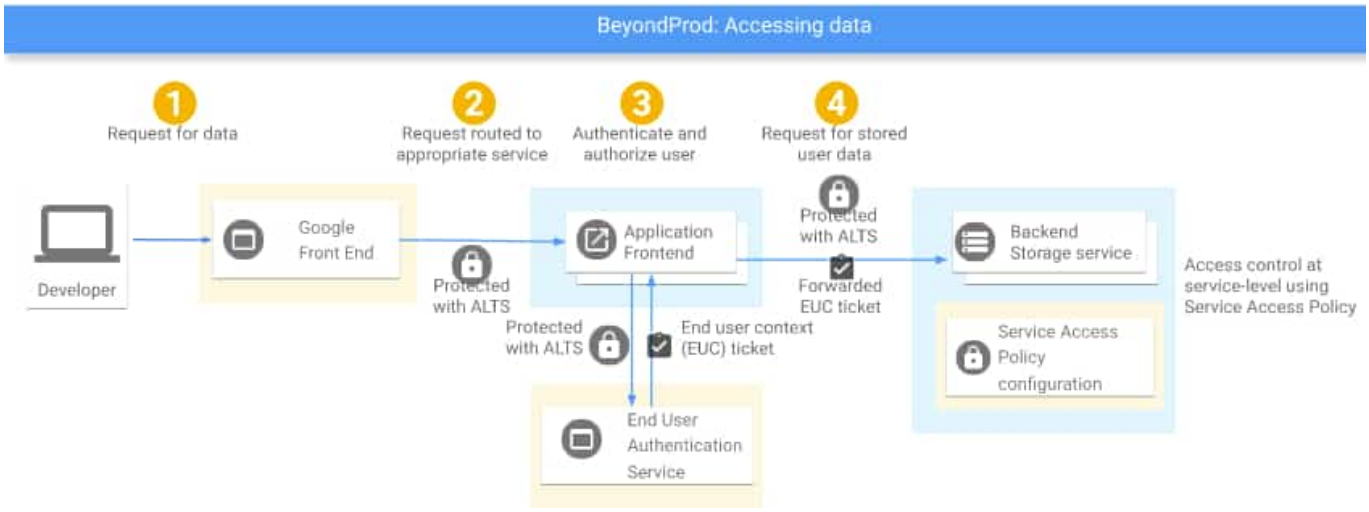
BeyondProd, c'est aussi, entre autres, une nouvelle approche en matière d'isolation des tâches. Aux mécanismes « traditionnels » de séparation physique ou par hyperviseur, Google substitue gVisor, son bac à sable pour Docker et Kubernetes.

La vérification d'intégrité du code et des machines a également son importance. Elle se reflète, en particulier, dans les nœuds GKE protégés.
Ces derniers vérifient leur intégrité tout au long de leur cycle de vie, par l'intermédiaire de fonctions telles que :

- Le démarrage sécurisé : vérification de la signature numérique de tous les composants de

démarrage à l'aide d'un magasin de clés approuvées.

- Le démarrage mesuré : un vTPM (module de plate-forme sécurisée virtualisée) détermine une référence pour un démarrage sain et y compare les mesures provenant des démarrages suivants.



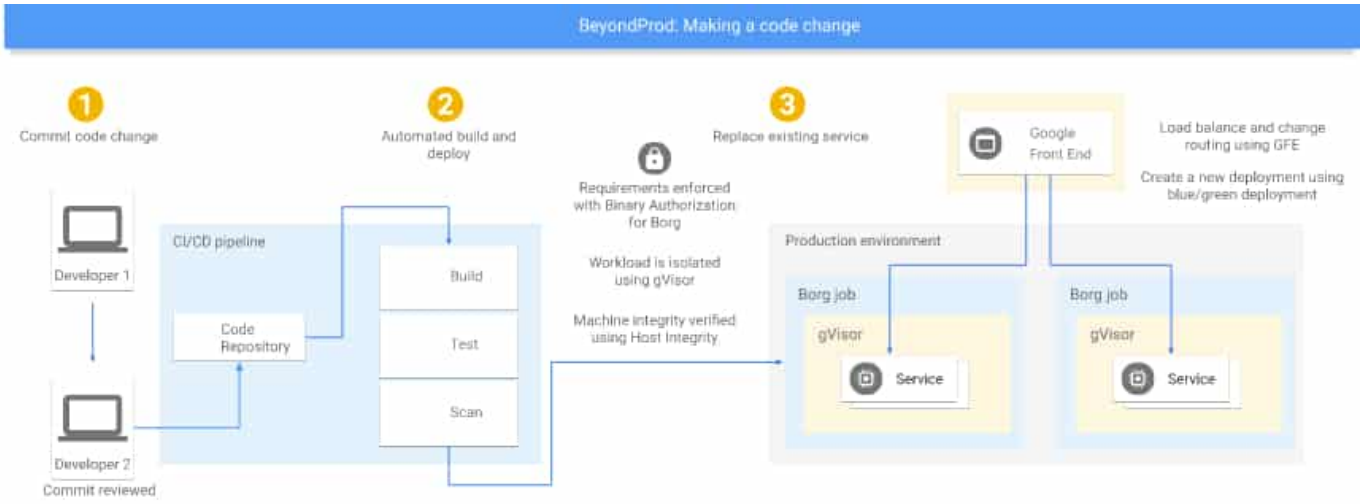




*Photo d'illustration © Macrovector – Shutterstock.com*