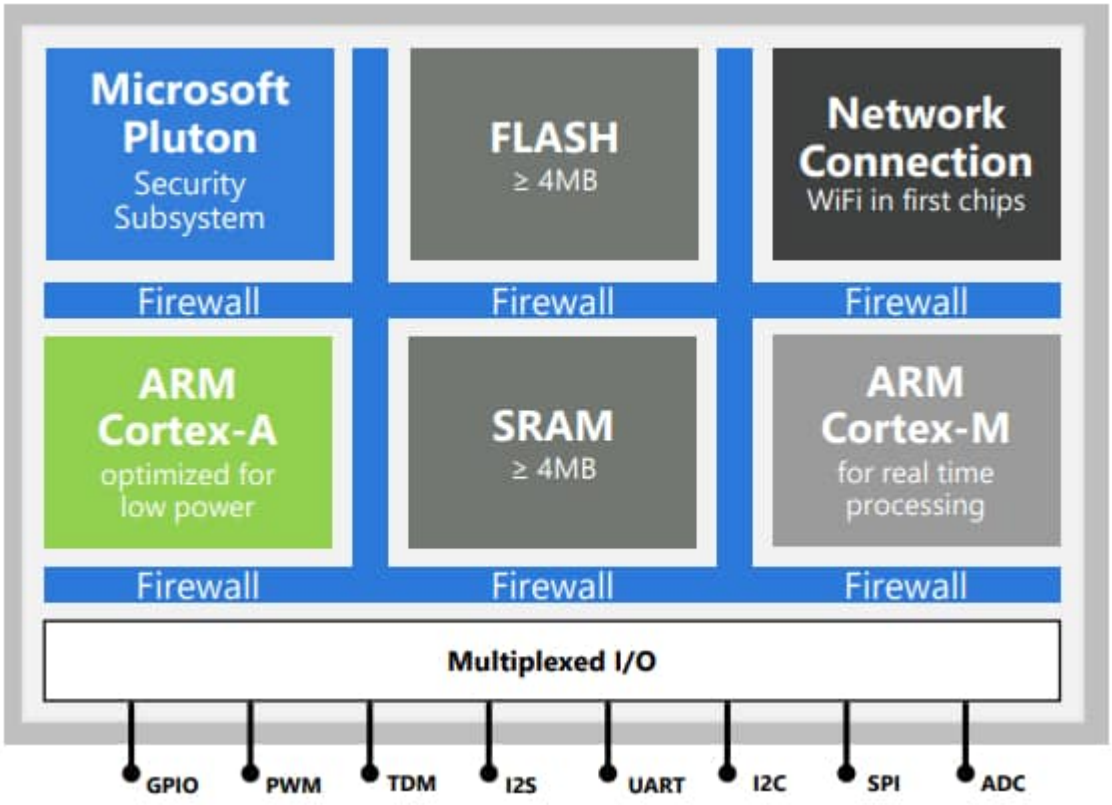
Sécurité : Microsoft pousse Pluton de l'IoT vers les PC

Prochaine étape pour Pluton : les PC. Microsoft vient de communiquer sur ses ambitions en la matière.

L'idée est de placer la racine de confiance matérielle dans le processeur, plutôt que de s'appuyer sur un TPM (module de plate-forme sécurisée). La suppression de cette puce annexe – dont les capacités resteront toutefois accessibles par émulation – est censée réduire la surface d'attaque en éliminant un point faible : le bus de communication avec le CPU*.

Microsoft met déjà cette approche en œuvre sur les microcontrôleurs Azure Sphere. Le sous-système Pluton en gère l'identification et orchestre le démarrage des composants critiques. Il s'appuie principalement sur un cœur de processeur, des moteurs de chiffrement, un magasin de clés et un générateur matériel de nombres aléatoires.



Pluton : aussi sur console

L'architecture de Pluton se reflète dans son nom. Ce dernier ne fait effectivement pas référence à la planète, mais aux roches magmatiques qui se mettent en place en profondeur, par refroidissement. Et qui s'opposent ainsi aux cônes volcaniques, résultats d'une remontée en surface.

Azure Sphere n'en fut pas le premier terrain d'expérimentation. La console Xbox One avait ouvert la

voie, avec l'objectif de lutter contre le piratage des jeux (cf. vidéo ci-dessous).

L'approche ne diffère pas dans l'univers du PC, si ce n'est qu'elle a impliqué une collaboration avec AMD, Intel et Qualcomm. La technologie SHACK (Secure Hardware Cryptography Key) en reste un pilier : Pluton génère ses propres paires de clés pendant la fabrication des composants, sans dépendre d'un HSM. Il doit par ailleurs faciliter les mises à jour de *firmware*, en les intégrant à Windows Update.

***** *Du côté des* datacenters*, on soulignera l'existence d'un projet à visée similaire : Cerberus. L'Open Compute Project en assure la gestion. Son développement répond à la multiplication des ressources de calcul (GPU, NIC, FPGA…). Et des failles potentielles qui en découlent, particulièrement au niveau des communications avec les CPU hôtes.*

Illustration principale © Intel