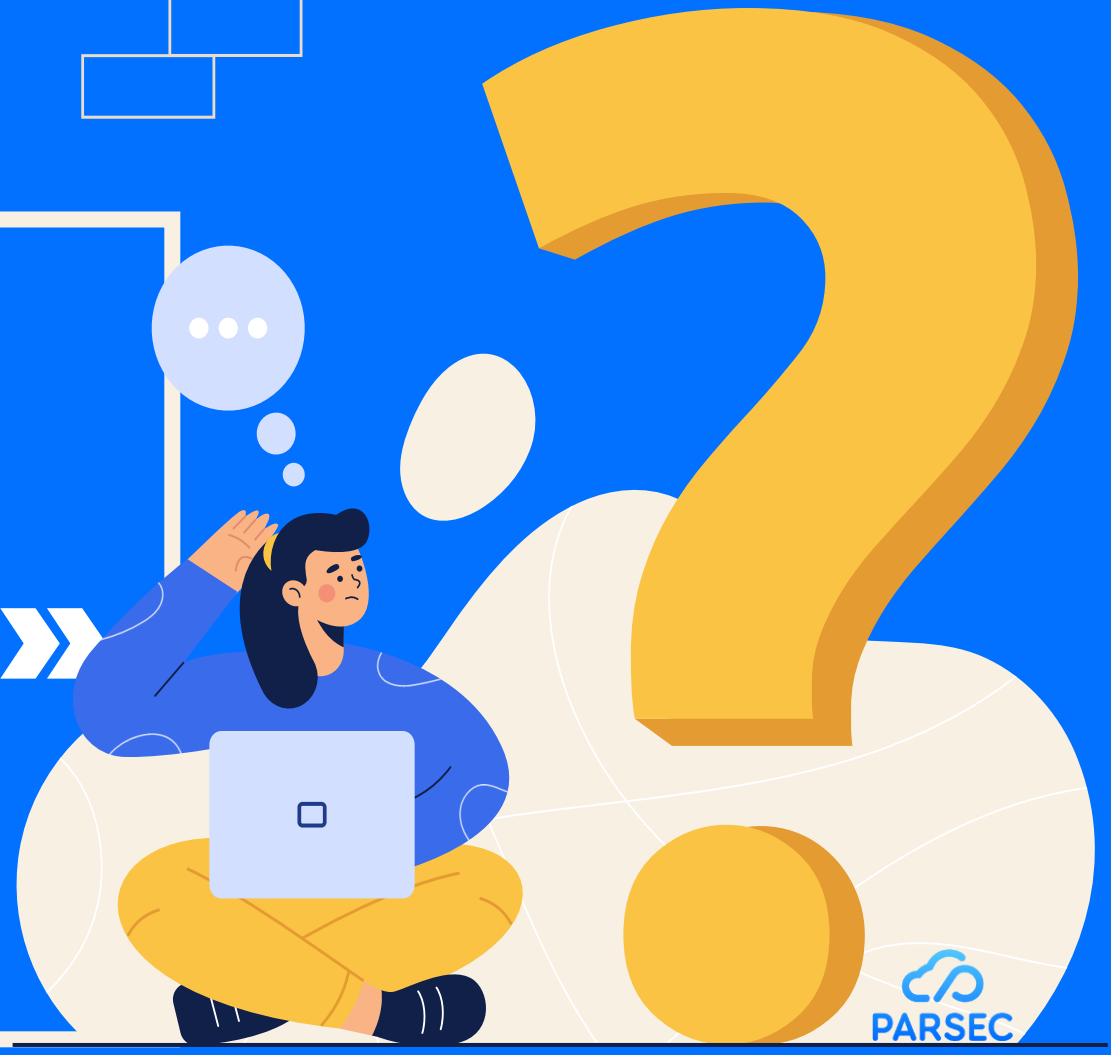
PARSEC

On en parle de plus en plus en ce moment
mais concrètement,

c'est quoi le

« ZeroTrust »



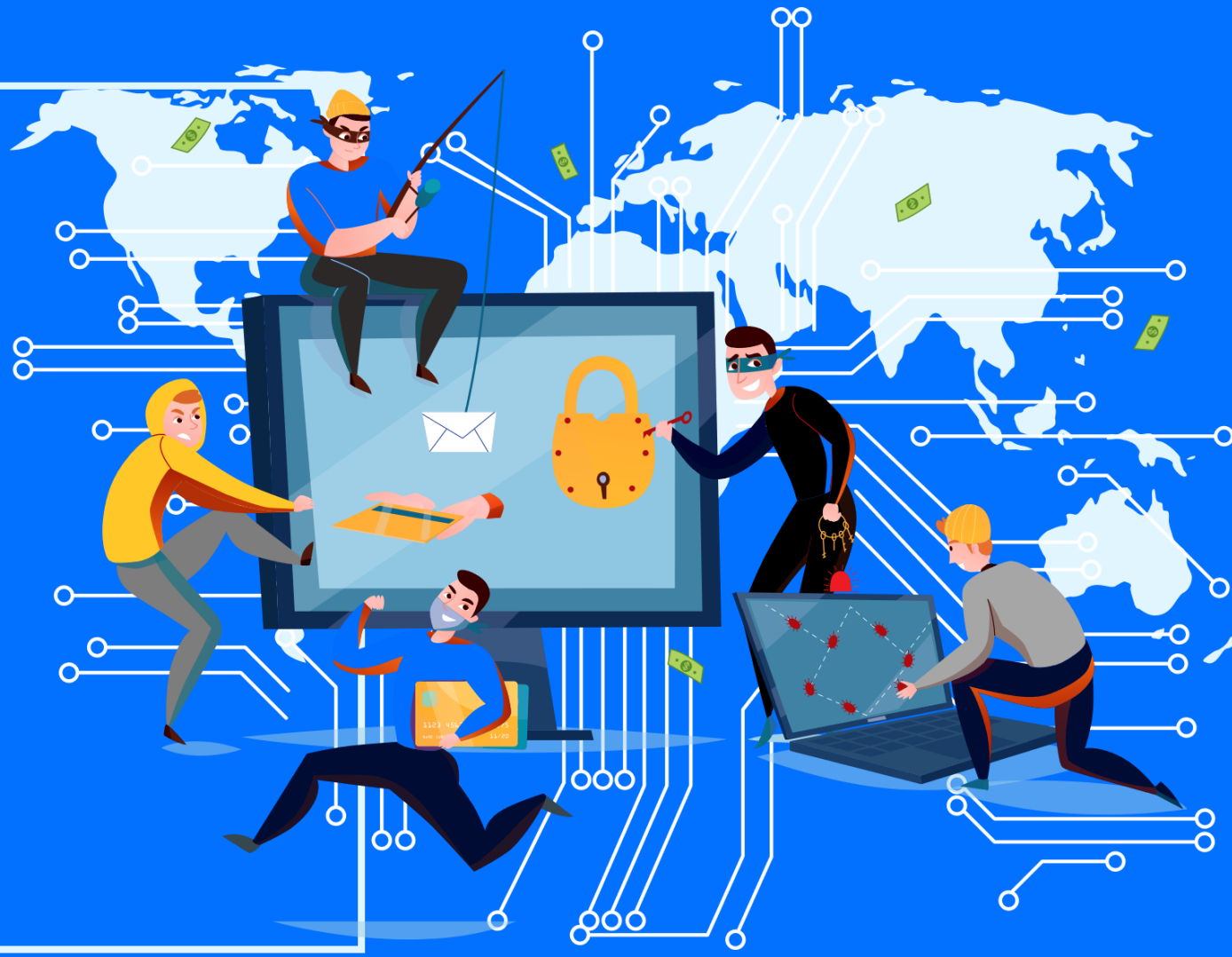
PARSEC

De nos jours avec la vulgarisation d'internet, du cloud et des nouveaux modes de travail en entreprise, on constate en matière de SI que l'on a tendance à croire que la menace vient seulement de l'extérieur et qu'un VPN reste suffisant; les récentes attaques cyber en ont bien démontré les limites.

Le Zerotrust est avant tout un concept SI selon lequel

« Ne faites confiance à personne »

De ce concept, va donc naître des solutions qui vous permettront de bâtir votre sécurité 100% Zerotrust



“Quand il s'agit de la souveraineté et l'intégrité des données sensibles, qu'elles soient partagées et stockées sur un cloud privé ou public, la menace est partout !

PARSEC

L'approche Zero-Trust peut être résumée en cinq points :

1. Tout réseau est considéré comme hostile.

2. Les menaces internes et externes sont présentes à tout moment sur le réseau.

3. **Chaque terminal, chaque utilisateur et chaque flux réseau doivent être authentifiés et autorisés.**

4. Être à l'intérieur d'un réseau interne n'est jamais un gage de confiance absolue.

5. Les politiques de sécurité sont dynamiques et agissent sur chaque sources de données.

PARSEC

Pour mettre en place sa stratégie Zerotrust, une question fondamentale à se poser :

Qui garde la clé ?

Le cœur d'une approche ZeroTrust c'est l'utilisateur

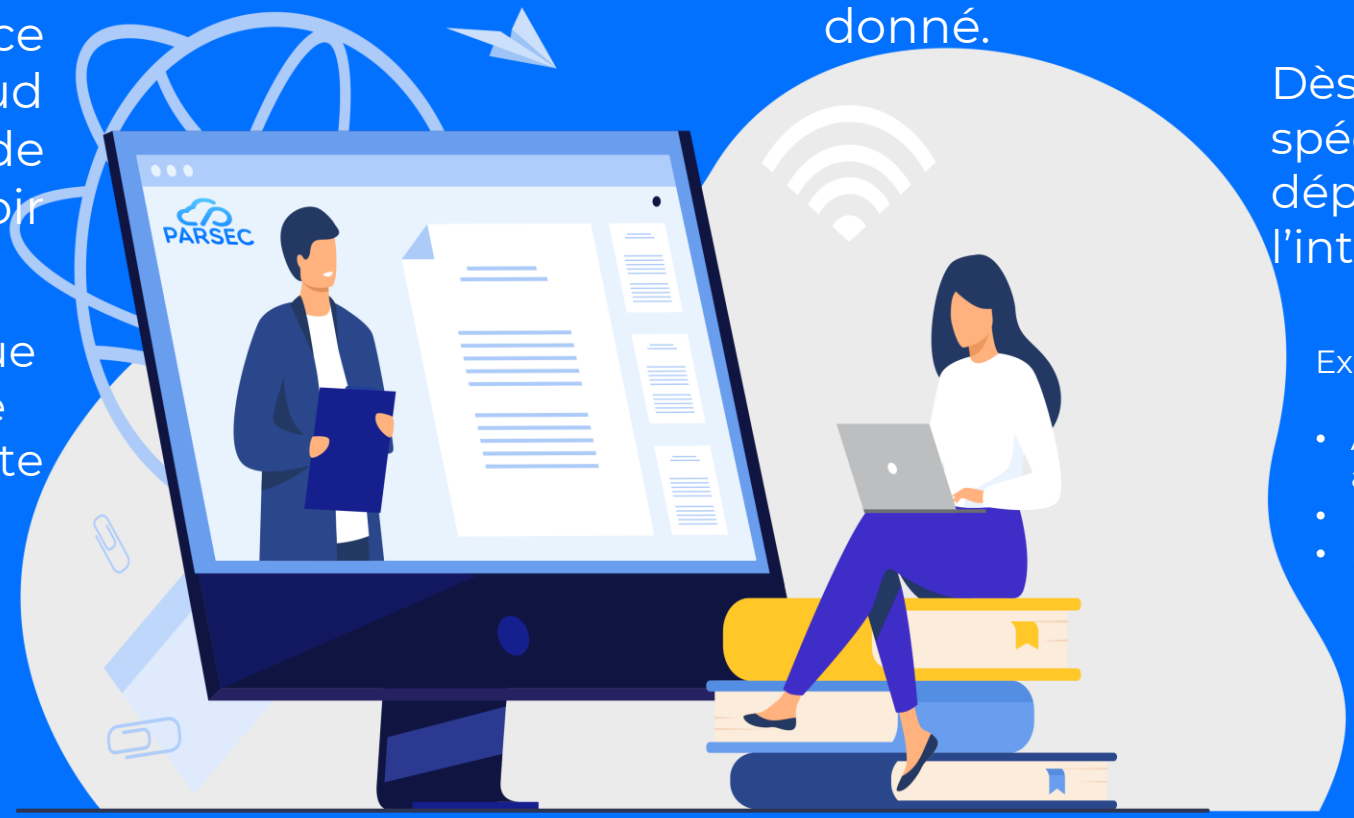
Un modèle de sécurité par l'utilisateur et pour l'utilisateur !

1) Le contrôle des clés par l'utilisateur.

Dans un modèle Zerotrust, seul l'utilisateur détient les clés de chiffrement qui donnent accès à ses données.

Aucun intermédiaire, que ce soit un fournisseur de cloud ou d'une solution de chiffrement, ne doit avoir accès aux clés.

Par conséquent, il est clair que le modèle BYOK, qui consiste à générer ses clés pour ensuite les confier à tiers dans une keybox dont lui aussi détient la clé, n'est pas du tout du ZeroTrust.



2) Le contrôle de l'identité des utilisateurs

La première exigence pour accéder au SI d'une entreprise est basée sur les privilèges d'accès accordés à un utilisateur, à un service ou à un dispositif donné.

Dès lors, des technologie spécifiques doivent êtr déployées afin d'assure l'intégrité des accès.

Exemple :

- Authentification multifacteurs adaptative
- Proxy sans VPN
- Des navigateurs intégrés sécuri

PARSEC

A retenir !

Toujours se poser la question suivante

Qui garde la clé ?

Le ZeroTrust consiste précisément à ne faire confiance qu'à soi-même !