# L’architecture Zero Trust

Par Patrick Sentinel – 29a.ca

## 🧱🚫 "Zero Trust : parce que même ton clavier pourrait être un traître"

Imagine un monde où ton réseau est un magasin sélectif. Pas de passe-droit, pas de copinage, pas de "c’est correct, c’est Roger du marketing". Non. **Tout le monde montre patte blanche.** À chaque porte. À chaque fois. Bienvenue dans le **Zero Trust Architecture (ZTA)** : Un monde où **personne** n’est digne de confiance par défaut. Pas même toi. Pas même ta souris. Pas même ton Wi-Fi. (Même ton *toaster* connecté IoT pleure un peu.)

## 😳 "Mais… j’ai déjà un pare-feu!"

Oui, et c’est bien… Mais dans un modèle classique, on fait souvent confiance à l’intérieur du réseau. C’est comme si ta maison avait une super porte blindée… mais que tout le monde à l’intérieur pouvait aller dans le frigo, lire ton journal intime ou vendre ta PS5 ou regarder si tu as caché de l’argent entre les deux matelas (il y en a encore qui font ça ?).

Le Zero Trust, lui, dit :

"Non. Même si tu es déjà dans la maison, tu dois redemander la clé à chaque pièce."

## 🧠 Les grands principes du Zero Trust:

🔐 1. Ne jamais faire confiance par défaut

- Ton propre serveur? Suspect.
- Ton collègue? Suspect.
- Toi-même? Doublement suspect.

🆔 2. Vérification continue

Chaque demande d’accès doit prouver :

- Qui elle est;
- Pourquoi elle est là;
- Si elle a le droit d’y être;
- Si elle s’est bien lavé les mains.

### 🧱 3. Micro-segmentation

Le réseau est découpé en petites zones bien cloisonnées. Un peu comme une prison… mais avec des badges de sécurité partout et un agent qui te regarde de travers si tu vas à la cafétéria.

### 👀 4. Surveillance constante

Tout est journalisé, audité, analysé. C'est la version numérique de *"je t'ai vu Roger, t'as encore cliqué sur un lien étrange."*

### 🌓 À quoi ça ressemble en pratique ?

- Un utilisateur ne peut pas accéder à une application sans authentification forte, même s'il est déjà connecté au réseau, oui Monsieur !
- Les droits d'accès sont granulaires, limités à ce qui est strictement nécessaire. Si t'as pas besoin de voir la donnée 'Y' alors tu n'auras pas les accès pour la voir, *as simple as that*;
- Chaque accès est réévalué en temps réel selon le contexte : lieu, heure, appareil, humeur du système;
- Même les connexions internes entre services doivent être authentifiées et chiffrées. On ne fait confiance à rien, je vous l'avais déjà dit 😉 ?

## 💣 Et les avantages?

- Moins de mouvements latéraux pour les attaquants. « *T'as réussi à compromettre un poste ? Bravo… Mais tu en restes là, pas de bonus* »;
- Moins de dégâts en cas de brèche (*"Un utilisateur s'est fait hameçonner? Pas grave, il avait seulement accès à 3 boutons et une imprimante."*);
- Un meilleur contrôle sur qui fait quoi, quand, où et pourquoi.

### 😟 Mais… Ce n'est pas un peu parano 😳?

Oui, totalement! Et c'est précisément le but. Le ZTA (Zero Trust Architecture), c'est la cybersécurité **sous caféine et avec un passé traumatique.** Mais dans un monde où tout peut être compromis — y compris les outils de cybersécurité eux-mêmes — **la paranoïa devient une stratégie**.

### En conclusion… Parano 😉

Le Zero Trust Architecture, ce n'est pas juste une mode *buzzword*. C'est une philosophie. Un style de vie en sécurité. C'est dire à chaque octet :

*"Je ne te connais pas. Identifie-toi. Sinon, pas de passage et pas d'information."*

Alors oui, ça demande du travail, de la gestion, des politiques, du monitoring, des règles, des logs, etc. Mais quand un hacker tente de passer par la porte du serveur RH ou tente de dérober les coffres forts numériques d'une entreprise et qu'il se fait recaler comme un ado sans carte d'identité… Tu sais que ça valait la peine.

---