# Surface d’attaque en environnement Cloud

## 1. Définition

La surface d’attaque correspond à l’ensemble des points d’entrée exploitables par un attaquant pour compromettre un système d’information.

En environnement Cloud, elle est :

- Plus étendue
- Plus dynamique
- Fortement pilotée par les identités et les API
- Accessible via Internet par conception

Dans le Cloud, l’identité devient le nouveau périmètre de sécurité.

---

## 2. Évolution par rapport au On-Premise

| On-Premise | Cloud |
|---|---|
| Périmètre réseau physique clairement défini | Périmètre logique et distribué |
| Pare-feu matériels | Security Groups, NACL, IAM |
| Infrastructure relativement statique | Ressources éphémères et automatisées |
| Accès principalement interne | Accès via Internet et API |
| Sécurité centrée sur le réseau | Sécurité centrée sur l’identité |

Le passage au Cloud ne réduit pas la surface d’attaque : il la transforme.

---

## 3. Principales composantes de la surface d’attaque Cloud

### 3.1 Les identités (IAM)

- Utilisateurs
- Rôles
- Politiques
- Clés d’accès API
- Tokens temporaires

Une compromission d’identité peut entraîner une compromission complète de l’infrastructure.

---

### 3.2 Les API du fournisseur Cloud

Toutes les actions (création, suppression, modification de ressources) passent par des API.

Une clé API compromise permet de piloter l’infrastructure à distance.

### 3.3 Les services exposés sur Internet

- Instances avec IP publique
- Load Balancers
- API Gateway
- Stockage mal configuré
- Bases de données exposées

Une mauvaise configuration augmente immédiatement la surface d’attaque.

---

### 3.4 Le plan de contrôle (Control Plane)

- Console d’administration
- Gestion des comptes
- Organisation multi-comptes
- Infrastructure as Code

Le contrôle du plan d’administration équivaut à un contrôle global.

---

### 3.5 Les workloads et applications

- Machines virtuelles
- Containers
- Images non patchées
- Dépendances vulnérables

Le Cloud n’élimine pas les vulnérabilités applicatives classiques.

---

## 4. Facteurs aggravants en environnement Cloud

- Élasticité : création/suppression rapide de ressources
- Automatisation : propagation rapide d’erreurs de configuration
- Accessibilité mondiale
- Multi-comptes et multi-environnements

La surface d’attaque devient mouvante et évolutive.

---

## 5. Message clé

Dans un environnement Cloud :

- On ne protège plus uniquement un réseau
- On protège des identités

- On protège des API
- On protège des configurations

La mauvaise configuration est aujourd’hui l’une des premières causes d’incident de sécurité dans le Cloud.

---

## Transition pédagogique

Si la surface d’attaque Cloud est principalement liée aux identités et aux permissions, alors la gestion des accès (IAM) devient un élément central de la stratégie de sécurité.

C’est ce que nous allons étudier dans la prochaine partie.