FR

Guide Sécurité Cloud

Zero Trust, IAM et Conformité pour PME

Audit BOTUM : 23 vulnérabilités critiques remédiées en 2 semaines

Zero Trust · **IAM** · **Conformité**

Mars 2026

Introduction : le mythe de la sécurité automatique

En 2019, Capital One se fait voler les données de 106 millions de clients via un rôle IAM AWS mal configuré. En 2022, Uber subit une brèche par credential stuffing aggravée par l'absence de MFA sur un VPN. En 2023, Wiz trouve 38 TB de données Microsoft exposées sur Azure Blob. Ces brèches ont un point commun : aucune n'est due à une faille du provider — la vulnérabilité était entièrement côté client.

Le modèle de responsabilité partagée

Ce que le provider gère :

- ✓ Sécurité physique des datacenters
- ✓ Hardware et backbone réseau
- ✓ Infrastructure de virtualisation
- ✓ Disponibilité zones/régions
- ✓ Conformité infrastructure (SOC 2, ISO 27001)
- ✓ Patches OS services managés (RDS, Lambda)

Ce que VOUS devez gérer :

- ✗ Gestion des identités et accès (IAM)
- ✗ Configuration Security Groups/NSG
- ✗ Chiffrement de vos données (at rest + in transit)
- ✗ Patches OS de vos VMs (EC2, Azure VM)
- ✗ Configuration buckets S3 (public vs privé)
- ✗ Gestion des secrets, clés API, certificats
- ✗ Logs, monitoring, alertes sécurité
- ✗ Conformité réglementaire (LPRPDE, PHIPA, OSFI)

Règle Gartner : "À travers 2025, 99% des défaillances de sécurité cloud seront la faute du client."

Zero Trust : ne jamais faire confiance, toujours vérifier

Zero Trust (formalisé par John Kindervag chez Forrester) repose sur 3 principes :

1. Ne jamais faire confiance implicitement — même une requête interne doit être authentifiée
2. Toujours vérifier explicitement — qui, quel device, depuis où, quelle sensibilité
3. Supposer la compromission — segmenter pour limiter le blast radius

Implémentation pratique

- • Micro-segmentation : VPC subnets privés/publics distincts, Security Groups granulaires par workload
- • MFA partout : bloque 99,9% des attaques sur mots de passe (Microsoft)
- • Device trust : AWS Verified Access / Azure Conditional Access + MDM (Jamf, Intune)

• Sessions courtes : AWS STS tokens temporaires (1h max), Azure Managed Identities (zero secret)

IAM : le principe du moindre privilège

La gestion des identités est le domaine où les PME font le plus d'erreurs — et où les conséquences sont les plus graves.

Règles IAM fondamentales

• Jamais *:* (toutes actions sur toutes ressources) — même temporairement
• Policies granulaires : logs:GetLogEvents pas logs:*
• Rôles séparés par fonction : dev ≠ ops ≠ sécu ≠ admin
• Revue trimestrielle : IAM Access Analyzer détecte les permissions non utilisées 90j+
• Rotation des clés d'accès tous les 90 jours maximum
• Préférer IAM Roles aux access keys statiques pour EC2/Lambda/Kubernetes
• MFA obligatoire via policy IAM — refus de toute action sans MFA

Policy MFA obligatoire (AWS) :

```
{ "Effect": "Deny", "NotAction": ["iam:EnableMFA"], "Resource": "*", "Condition": { "BoolIfExists": { "aws:MultiFactorAuthPresent": "false" } } }
```

Audit logs : votre boîte noire

• CloudTrail multi-region : export S3 + alertes sur DeleteTrail, LoginWithNoMFA
• Rétention minimale : 90j actif + 1 an cold storage
• Compte séparé pour les logs — l'attaquant ne peut pas supprimer ses traces

Sécurité réseau cloud

Security Groups / NSG

Refuser par défaut, autoriser explicitement. Fermer port 22 internet — utiliser SSM Session Manager ou Azure Bastion. Jamais 0.0.0.0/0 sur SSH/RDP.

VPC / VNet isolation

Isoler par environnement (VPC prod ≠ staging) et sensibilité. PrivateLink / Private Endpoints pour S3, RDS, Key Vault sans passer par internet.

WAF

AWS WAF / Azure Front Door WAF / GCP Cloud Armor : protection OWASP Top 10 + rate limiting anti-bruteforce.

DDoS

AWS Shield Standard (gratuit) + Shield Advanced (3k$/mois) pour la protection avancée.

Chiffrement : at rest + in transit

- At rest — AES-256 : activer sur tous volumes (EBS, Disk), buckets (S3 SSE), bases de données (RDS)
- In transit — TLS 1.3 minimum : désactiver TLS 1.0/1.1. mTLS entre services internes.
- AWS ACM : certificats TLS gratuits avec renouvellement automatique
- KMS (AWS) / Key Vault (Azure) / Cloud KMS (GCP) : gestion centralisée des clés
- Rotation automatique annuelle des clés KMS, 90 jours pour les secrets applicatifs

Conformité canadienne

LPRPDE / PIPEDA

- Consentement explicite avant collecte des données personnelles
- Notification de brèche si risque réel de préjudice grave
- Droit d'accès et de correction des individus

Résidence des données au Canada

AWS ca-central-1 (Montréal) · Azure Canada Central (Toronto) + Canada East (Québec) · GCP northamerica-northeast1 (Montréal). Vérifiez que sauvegardes et logs restent au Canada.

PHIPA (Ontario — données de santé)

- Health Privacy Agreements avec vos providers cloud
- Audit logs de tous les accès aux données de santé
- Notification du Commissaire en cas de brèche (24-72h)

OSFI (institutions financières fédérales)

- Évaluation de risque formelle avant tout engagement cloud
- Droit d'audit des providers cloud
- Plans de résilience et de sortie documentés
- Notification au BSIF pour services "matériels" dans le cloud

AWS vs Azure vs GCP — Outils de sécurité natifs

Catégorie	AWS	Azure	GCP
IAM	IAM, Access Analyzer, SCP	Entra ID, RBAC, PIM	Cloud IAM, WIF
Secrets	Secrets Manager, KMS	Key Vault	Secret Manager, Cloud KMS
Détection	GuardDuty, Security Hub	Defender for Cloud, Sentinel	Security Command Center
Réseau	Security Groups, WAF, Shield	NSG, Azure Firewall, WAF	VPC Rules, Cloud Armor
Conformité	Config, CloudTrail, Artifact	Azure Policy, Compliance Mgr	Audit Logs, Assured WL
Chiffrement	KMS (CMK), ACM, CloudHSM	Key Vault, Azure HSM	Cloud KMS, Cloud HSM

Vulnérabilités	Amazon Inspector	Defender for Servers	Artifact Registry Scan

Erreurs communes qui ouvrent la porte aux attaquants

Clés AWS hardcodées dans Git

Des bots scannent GitHub en continu et récupèrent les clés en moins de 4 minutes. Solution : git-secrets en pre-commit, IAM Roles pour éliminer les clés statiques.

Buckets S3 publics

Base de données clients, sauvegardes, configs exposées. Vérifier avec aws s3api get-bucket-acl ou AWS Config Rule s3-bucket-public-read-prohibited.

Logs désactivés

Impossible de retracer un incident. CloudTrail coûte quelques dizaines de dollars/mois — son absence lors d'une brèche peut coûter des centaines de milliers.

MFA absent sur root/Global Admin

Un phishing donne accès total immédiat. Activez le MFA aujourd'hui.

Security Groups trop permissifs "en attendant"

La règle "temporaire" reste des mois. AWS Config Rule restricted-ssh détecte automatiquement.

Cas concret BOTUM : 23 vulnérabilités critiques remédiées en 2 semaines

Agence de marketing digital québécoise, 45 employés, stack AWS. Audit demandé "juste pour voir où on en est". Ils pensaient être en bonne forme.

Résultats de l'audit (semaine 1) :

- 3 clés AWS actives dans des repos GitHub publics (dont 1 AdministratorAccess active depuis 8 mois)
- 2 buckets S3 publics contenant des exports de bases de données clients
- 17 règles Security Group autorisant SSH/RDP depuis 0.0.0.0/0
- CloudTrail désactivé dans us-east-1 (60% des workloads)
- Aucun MFA sur 6 comptes IAM humains dont 2 avec AdministratorAccess
- Clés d'accès non-rotées depuis 3 ans
- RDS exposé sur internet (port 3306 depuis 0.0.0.0/0)

Total : 23 vulnérabilités critiques/élevées — CVSS composite 9.1/10

Plan de remédiation (semaine 2) :

- Révocation immédiate des 3 clés + audit CloudTrail des 8 derniers mois
- Migration vers IAM Roles pour toutes les applications — zéro clé statique

- Blocage public access tous les buckets S3 + notification clients (LPRPDE)
- CloudTrail multi-region activé, 90j rétention, export vers compte séparé
- Fermeture toutes règles SSH/RDP publiques — passage à SSM Session Manager
- MFA obligatoire via IAM Policy sur tous les comptes humains
- Fermeture port RDS, migration accès privé via VPC uniquement

Résultat : 23 vulnérabilités critiques → 0 en 14 jours. Surface d'attaque réduite de 87%. Coût potentiel d'une brèche : 500 000 à 2 000 000 CAD (LPRPDE + légal + réputation).

Conclusion

La sécurité cloud n'est pas optionnelle pour une PME en 2024. Les outils natifs existent, la plupart sont inclus dans vos frais d'infrastructure. Un audit de 2-3 jours révèle systématiquement les problèmes critiques. Les corriger prend rarement plus de 2 semaines.
