EN

Cloud Security Guide

Zero Trust, IAM and Compliance for SMBs

BOTUM Audit: 23 critical vulnerabilities remediated in 2 weeks

Zero Trust · **IAM** · **Conformité**

Mars 2026

Introduction: The Myth of Automatic Security

In 2019, Capital One had 106 million customers' data stolen via a misconfigured AWS IAM role. In 2022, Uber suffered a breach via credential stuffing compounded by absent MFA on a VPN account. In 2023, Wiz found 38 TB of Microsoft data exposed on Azure Blob Storage. These breaches share one commonality: none were caused by a provider vulnerability — the attack vector was entirely on the client side.

The Shared Responsibility Model

What the provider manages:

- ✓ Physical datacenter security
- ✓ Hardware and backbone network
- ✓ Virtualization infrastructure
- ✓ Zone/region availability
- ✓ Infrastructure compliance (SOC 2, ISO 27001)
- ✓ OS patches for managed services (RDS, Lambda)

What YOU must manage:

- ✗ Identity and access management (IAM)
- ✗ Security Groups/NSG configuration
- ✗ Encryption of your data (at rest + in transit)
- ✗ OS patches for your VMs (EC2, Azure VM)
- ✗ S3 bucket configuration (public vs. private)
- ✗ Secrets, API keys, certificate management
- ✗ Logs, monitoring, security alerts
- ✗ Regulatory compliance (PIPEDA, PHIPA, OSFI)

Gartner rule: "Through 2025, 99% of cloud security failures will be the customer's fault."

Zero Trust: Never Trust, Always Verify

Zero Trust (formalized by John Kindervag at Forrester) rests on 3 principles:

1. Never implicitly trust — even internal requests must be authenticated
2. Always verify explicitly — who, what device, from where, what sensitivity
3. Assume breach — segment to limit the blast radius

Practical Implementation

- Micro-segmentation: distinct private/public VPC subnets, granular Security Groups per workload
- MFA everywhere: blocks 99.9% of password-based attacks (Microsoft)
- Device trust: AWS Verified Access / Azure Conditional Access + MDM (Jamf, Intune)

- Short-lived sessions: AWS STS temporary tokens (1h max), Azure Managed Identities (zero secrets)

IAM: The Principle of Least Privilege

Identity and access management is the area where SMBs make the most mistakes — and where the consequences are most severe.

Fundamental IAM Rules

- Never *:* (all actions on all resources) — even temporarily
- Granular policies: logs:GetLogEvents not logs:*
- Separate roles by function: dev ≠ ops ≠ security ≠ admin
- Quarterly review: IAM Access Analyzer detects unused permissions 90d+
- Rotate access keys every 90 days maximum
- Prefer IAM Roles over static access keys for EC2/Lambda/Kubernetes
- Mandatory MFA via IAM policy — deny all actions without MFA

Mandatory MFA Policy (AWS):

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

Audit Logs: Your Black Box

- Multi-region CloudTrail: S3 export + alerts on DeleteTrail, LoginWithNoMFA
- Minimum retention: 90 days active + 1 year cold storage
- Separate account for logs — attacker can't delete their traces

Cloud Network Security

Security Groups / NSG

Deny by default, allow explicitly. Close port 22 from internet — use SSM Session Manager or Azure Bastion. Never 0.0.0.0/0 on SSH/RDP.

VPC / VNet Isolation

Isolate by environment (prod VPC ≠ staging) and sensitivity. PrivateLink / Private Endpoints for S3, RDS, Key Vault without internet exposure.

WAF

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

DDoS

AWS Shield Standard (free) + Shield Advanced ($3k/month) for advanced protection.

Encryption: At Rest and In Transit

- At rest — AES-256: enable on all volumes (EBS, Disk), buckets (S3 SSE), databases (RDS)
- In transit — TLS 1.3 minimum: disable TLS 1.0/1.1. mTLS between internal services.
- AWS ACM: free TLS certificates with automatic renewal
- KMS (AWS) / Key Vault (Azure) / Cloud KMS (GCP): centralized key management
- Automatic annual rotation of KMS keys, 90 days for application secrets

Canadian Compliance

PIPEDA

- Explicit consent before collecting personal data
- Breach notification if real risk of significant harm
- Individual right of access and correction

Data Residency in Canada

AWS ca-central-1 (Montreal) · Azure Canada Central (Toronto) + Canada East (Quebec) · GCP northamerica-northeast1 (Montreal). Verify backups and logs also stay in Canada.

PHIPA (Ontario — Health Data)

- Health Privacy Agreements with cloud providers
- Audit logs of all health data access
- Privacy Commissioner notification on breach (24-72h)

OSFI (Federal Financial Institutions)

- Formal risk assessment before any cloud engagement
- Right to audit cloud providers
- Documented resilience and exit strategies
- OSFI notification for "material" cloud services

AWS vs Azure vs GCP — Native Security Tools

Category	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
Detection	GuardDuty, Security Hub	Defender for Cloud, Sentinel	Security Command Center
Network	Security Groups, WAF, Shield	NSG, Azure Firewall, WAF	VPC Rules, Cloud Armor
Compliance	Config, CloudTrail, Artifact	Azure Policy, Compliance Mgr	Audit Logs, Assured WL
Encryption	KMS (CMK), ACM, CloudHSM	Key Vault, Azure HSM	Cloud KMS, Cloud HSM
Vuln Scan	Amazon Inspector	Defender for Servers	Artifact Registry Scan

Common Mistakes That Open the Door to Attackers

AWS Keys Hardcoded in Git

Bots scan GitHub continuously and retrieve keys in under 4 minutes. Solution: git-secrets pre-commit hook, IAM Roles to eliminate static keys.

Public S3 Buckets

Customer databases, backups, configs exposed to internet. Check with aws s3api get-bucket-acl or AWS Config Rule s3-bucket-public-read-prohibited.

Disabled Logs

Impossible to trace an incident. CloudTrail costs tens of dollars/month — its absence during a breach can cost hundreds of thousands.

No MFA on Root/Global Admin

One phishing attack grants total immediate access. Enable MFA today.

Overly Permissive Security Groups "Temporarily"

The "temporary" rule stays for months. AWS Config Rule restricted-ssh detects automatically.

BOTUM Real Case: 23 Critical Vulnerabilities, Remediated in 2 Weeks

Quebec digital marketing agency, 45 employees, AWS stack. Security audit requested "just to see where we stand." They thought they were in good shape.

Audit findings (week 1):

- 3 active AWS keys in public GitHub repos (including 1 AdministratorAccess active for 8 months)
- 2 public S3 buckets containing customer database exports
- 17 Security Group rules allowing SSH/RDP from 0.0.0.0/0
- CloudTrail disabled in us-east-1 (60% of workloads)
- No MFA on 6 human IAM accounts including 2 with AdministratorAccess
- Access keys unrotated for 3 years
- RDS exposed to internet (port 3306 from 0.0.0.0/0)

Total: 23 critical/high vulnerabilities — composite CVSS 9.1/10

Remediation plan (week 2):

- Immediate revocation of 3 keys + CloudTrail audit of last 8 months
- Migration to IAM Roles for all applications — zero static keys
- Block public access all S3 buckets + customer notification (PIPEDA)
- Multi-region CloudTrail enabled, 90-day retention, export to separate account

- Close all public SSH/RDP rules — migrate to SSM Session Manager
- Mandatory MFA via IAM Policy on all human accounts
- Close RDS port, migrate to private VPC-only access

Result: 23 critical vulnerabilities → 0 in 14 days. Attack surface reduced by 87%. Potential breach cost: $500,000 to $2,000,000 CAD (PIPEDA penalties + legal + reputation).

Conclusion

Cloud security is not optional for an SMB in 2024. Native tools exist, most are included in your existing infrastructure costs. A 2-3 day audit systematically reveals the most critical issues. Fixing them rarely takes more than 2 weeks.
