EN

Hybrid Cloud Guide

Balanced Architecture for Canadian SMBs

PIPEDA/Law 25 · Azure Arc · VPN · Real case -35% costs

On-Prem + Cloud Public = Architecture Hybride

Mars 2026

BOTUM INC. www.botum.ca contact@botum.ca | blog.botum.ca

Hybrid Cloud Architecture for Canadian SMBs: The Balanced Approach

The term "hybrid cloud" is everywhere. Behind the buzzword: workloads running simultaneously on your on-premises infrastructure and a public cloud, orchestrated together through a unified management layer. Not two separate worlds — one coherent system.

Why Canadian SMBs Choose the Hybrid Model

1. PIPEDA and Quebec Law 25 — Constraints on Canadian data residency. Keeping data on-prem or in certified regions (Azure Canada Central) is compliance, not paranoia.
2. Critical application latency — ERP, production databases, real-time systems: these workloads have nothing to gain in the cloud. Network latency adds 5-20ms.
3. Real costs vs. estimated costs — Egress costs. High-frequency object storage costs. Keeping cold data on-prem and using cloud for variable compute: that's where savings materialize.
4. Non-migratable legacy applications — SQL Server 2008, AS/400, bare-metal CAD software. Hybrid cloud lets you maintain them without blocking the organization.

The 3 Hybrid Patterns

Extend — Burst to Cloud

On-prem handles base load. Cloud absorbs peaks. Typical for seasonal e-commerce, nightly batch, dev/test. Pay for cloud only when needed. Tools: Azure Autoscale, AWS Auto Scaling.

Bridge — DR/Backup

On-prem stays primary. Cloud = Plan B: DR, geo-redundant backup, continuous replication. RTO from 4h → 45 min. Monthly cost: $300-800 for a 100-server SMB. Tools: Azure Site Recovery, AWS Backup.

Full Hybrid — Distributed Workloads

Each workload placed by profile. PII data → on-prem. Intensive ML compute → cloud. SaaS for collaboration. Most cost-effective at maturity. Tools: Azure Arc, AWS Outposts, GCP Anthos.

Recommended Tech Stack: Azure Arc, AWS Outposts, GCP Anthos

Platform	Model	Strengths	Ideal for	Cost
Azure Arc	Lightweight agent on your servers	Azure Policy, Defender, Monitor Linux/Win/K8s	Existing Microsoft stack	$0 base + attached services

AWS Outposts	Physical AWS rack in your DC	Ultra-low latency Native AWS services on-prem	Need AWS API on-prem	$10k-30k/month (dedicated rack)
GCP Anthos	Managed multi-cloud Kubernetes	GKE everywhere Integrated Istio Native multi-cloud	Kubernetes-first multi-cloud	$0.10/vCPU-h + infra

Recommendation for Canadian SMBs: Azure Arc for existing Microsoft stacks (M365, Azure AD). Minimal entry cost, unified management without additional hardware.

Hybrid Networking: VPN vs ExpressRoute vs Direct Connect

Option	Bandwidth	Latency	Cost/month	When to use
Site-to-Site VPN	1-10 Gbps	+10-30ms	$30-150	<500 Mbps, tight budget
Azure ExpressRoute	1-100 Gbps	2-10ms	$500-3,000	>1 Gbps, latency-critical
AWS Direct Connect	1-100 Gbps	2-10ms	$500-3,000	>1 Gbps, latency-critical

Practical rule: VPN to start and for DR/backup. ExpressRoute/Direct Connect when bandwidth bill exceeds $200/month or apps need <5ms. Crossover: ~500 Mbps average daily traffic.

Hybrid Security: Unified Identity and Zero Trust

1. Unified Identity

Azure AD/Entra ID (Microsoft stack) or Okta (multi-cloud) as central Identity Provider. SSO for all apps, mandatory MFA, risk-based Conditional Access.

2. Network Segmentation

Micro-segmentation: each workload in its own subnet, strict NSG/Security Groups. East-west traffic (between workloads) must also be inspected.

3. Zero Trust Applied

Just-In-Time access for admins (Azure PIM), secrets in Key Vault, centralized logs in SIEM (Sentinel). Minimum viable: MFA + Conditional Access + privileged access auditing.

Common Mistakes to Avoid

- Migrating everything at once — Approach: pilot 2-3 non-critical workloads, measure, adjust, then scale.
- Ignoring data latency — Rule: apps and data in the same domain (cloud together, or on-prem together).

 Underestimating the network — Minimum network budget: 15-20% of total cloud budget.

 Forgetting cost governance — Azure Cost Management from day 1, budget overage alerts at 80%.

Real Case — BOTUM: 150-Employee SMB, −35% in Costs

Industrial client, 150 employees, Montreal. 40 over-provisioned VMs in Azure, bill: $18,000 CAD/month.

Hybrid stack deployed:

- 12 VMs repatriated on-prem (ERP, production SQL, MES) → Local Proxmox
- Azure Arc on Proxmox servers: unified management, Azure Policy, Defender
- Site-to-site VPN: Fortinet on-prem + Azure VPN Gateway (Active-Active)
- Maintained in Azure: Azure AD, M365, AKS for web apps, cold object storage
- DR: Azure Site Recovery for critical VMs (45-min RTO)

Results after 6 months:

Metric	Before	After (hybrid)
Azure monthly bill	$18,000/month	$11,700/month (−35%)
ERP latency	55ms	3ms
PIPEDA compliance	Partial	100% (data on-prem)
Disaster recovery RTO	4 hours	45 minutes
Unified infra visibility	None	Azure Arc Dashboard

Go Further with BOTUM

Hybrid cloud architecture, migration, security — BOTUM teams support Canadian SMBs.

→ Discuss your project: www.botum.ca/contact

⬇ Download PDF: www.botum.ca/guides/guide-cloud-hybride-architecture-pme-en.pdf