

EXECUTIVE GUIDE

Cloud Migration Security Guide

Securing your business through the move to cloud infrastructure — not just after it.

The Shared Responsibility Model

Cloud providers secure the infrastructure — physical data centers, hypervisors, core networking. You remain responsible for securing what you put on top of it: identity, data, configuration, and application security. Most cloud breaches trace back to a gap on the customer's side of that line, not a failure by the provider.

Common Migration Misconfigurations

- Storage buckets or file shares left publicly accessible by default
- Overly permissive identity and access management (IAM) roles granted during setup and never scoped down
- Multi-factor authentication not enforced during the transition period
- Logging and monitoring not enabled until after go-live, leaving a visibility gap
- Legacy on-premises firewall rules not replicated in cloud network security groups

Securing Identity in the Cloud

Identity is the new perimeter in cloud environments. Enforce MFA for every account from day one of migration, apply least-privilege access to every role, and use conditional access policies to restrict sign-ins by location, device health, and risk signals — especially during the migration window when temporary elevated access is common.

Data Protection During Migration

Data is often most exposed mid-migration — moving between environments, sometimes through temporary staging systems with weaker controls than either the source or destination. Encrypt data in transit and at rest throughout the migration, and apply the same data classification and access rules to the destination environment as existed on-premises — don't assume the cloud platform's defaults match your requirements.

Post-Migration Monitoring

Once live, ensure logging, alerting, and monitoring cover the new environment before decommissioning legacy monitoring — a gap here is invisible until an incident occurs. Cyber companies report cloud-focused attacks now significantly outpacing on-premises attacks, making this visibility gap one of the costliest to leave open.

Migrating to the Cloud?

Cenova Cyber helps businesses secure cloud environments before, during, and after migration.

Contact us for a free consultation.

www.cenovacyber.com