



EbizonCloud's Advanced Security Strategies on Oracle Cloud (OCI)

OCI Security Frameworks

A structured breakdown of OCI's robust security frameworks, incorporating foundational and advanced controls, CIS Benchmark integration, and comprehensive multicloud security considerations.



EbizonCloud Enabling the OCI Security Checklist Model



Identity & Access Management

- ✓ OCI Identity Domains (with MFA, Federation)
- ✓ Azure AD / Okta (SAML/OIDC Federation)
- ✓ IAM Dynamic Groups
- ✓ OCI Policy Validator
- ✓ Compartments (Environment-based)



EbizonCloud's Implementation:

- ✓ Federated SSO Integration
- ✓ Enable MFA Enforcement
- ✓ Dynamic Groups
- ✓ Compartment-Based Least Privilege
- ✓ Automated Audits





EbizonCloud Enabling the OCI Security Checklist Model



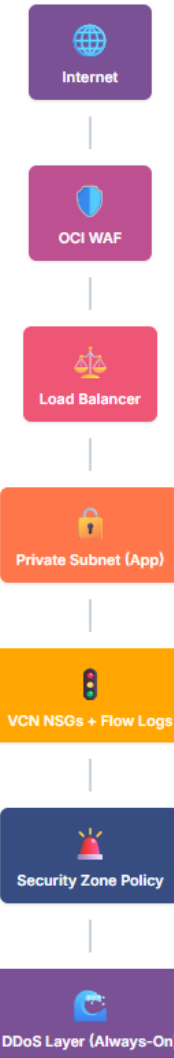
Network Security Architecture

- ✓ VCN with Subnets + NSGs
- ✓ Security Zones
- ✓ OCI WAF + Load Balancer
- ✓ DDoS Protection
- ✓ Flow Logs to Logging



EbizonCloud's Implementation:

- ✓ Security Zones & VCN Templates
- ✓ Deploy OCI resources into pre-approved security zones using IaC to auto-enforce
- ✓ VCN Flow Logs & NSG Monitoring
- ✓ WAF & DDoS Protection
- ✓ TLS Inspection (if needed)





EbizonCloud Enabling the OCI Security Checklist Model

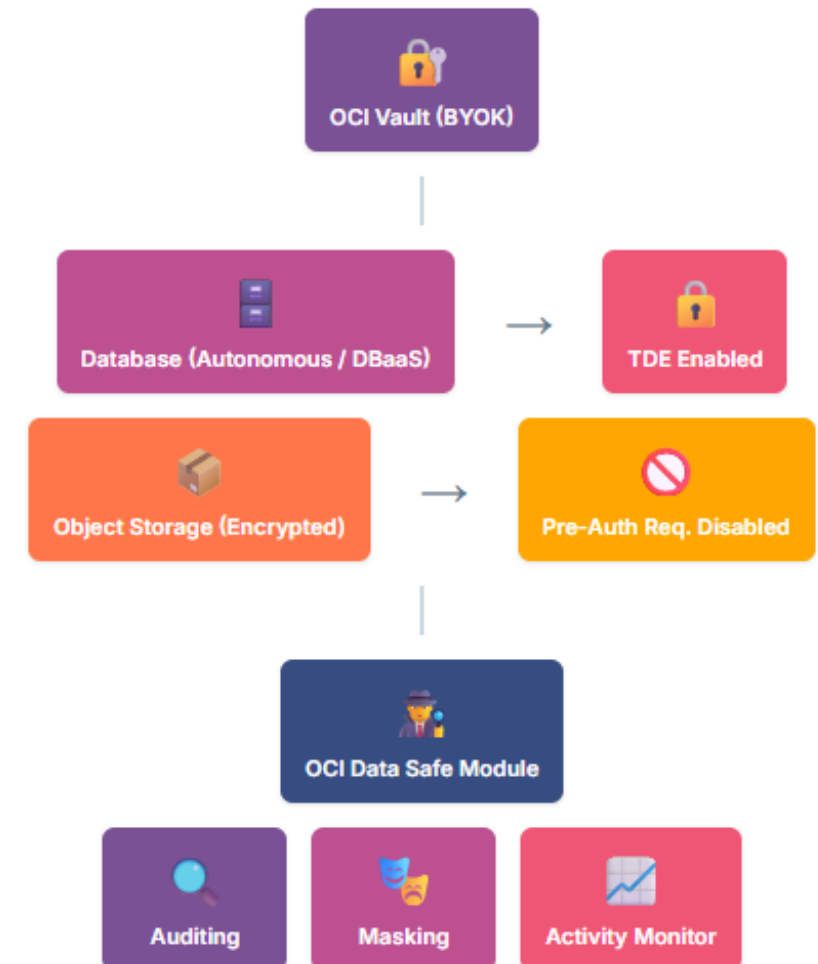
Data Protection Architecture

- ✓ OCI Vault (BYOK)
- ✓ Block/Object Storage (Encrypted)
- ✓ Autonomous DBs (TDE Enabled)
- ✓ OCI Data Safe
- ✓ Policies to Block Public Buckets



EbizonCloud's Implementation:

- ✓ BYOK with OCI Vault
- ✓ Transparent Data Encryption (TDE)
- ✓ Object Storage Encryption
- ✓ OCI Data Safe Integration





EbizonCloud Enabling the OCI Security Checklist Model

Monitoring & Threat Detection Architecture

- ✓ Cloud Guard (all compartments)
- ✓ Detector + Responder Recipes
- ✓ Service Connector Hub
- ✓ Streaming to SIEM (Splunk, Sentinel)
- ✓ Alarms (IAM changes, VCN modifications)



EbizonCloud's Implementation:

- ✓ Enable Cloud Guard Everywhere:
- ✓ Forward Logs to SIEM
- ✓ Critical Alarm Policies
- ✓ Vulnerability Scanning Service (VSS):





EbizonCloud Enabling the OCI Security Checklist Model



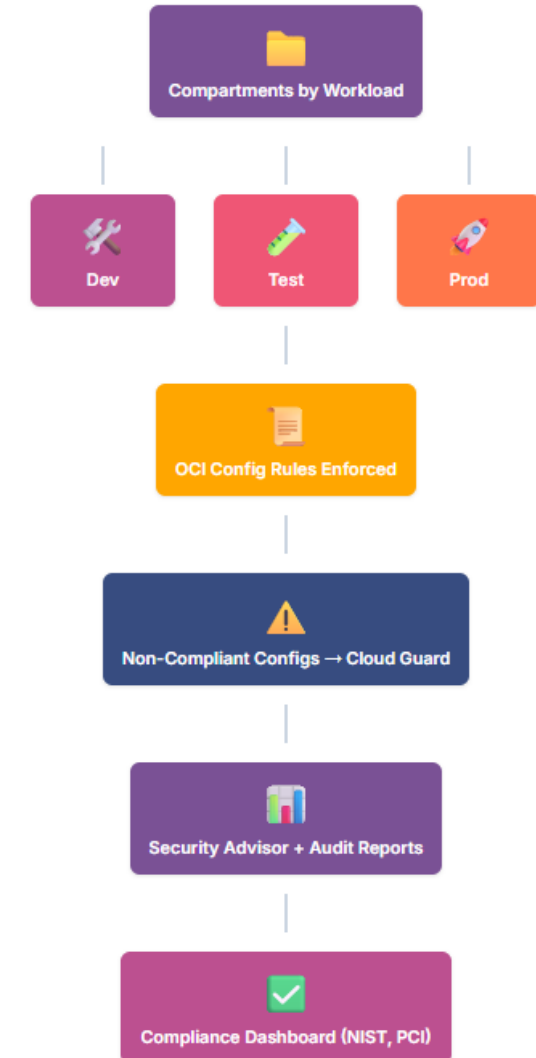
Governance & Compliance Architecture

- ✓ OCI Compartments (Workload Segmentation)
- ✓ OCI Config Rules
- ✓ Security Advisor Reports
- ✓ Compliance Mapping (PCI, HIPAA, NIST)



EbizonCloud's Implementation:

- ✓ Compartmentalization Strategy
- ✓ OCI Config Rules:
- ✓ Deploy OCI Config with enforced policies like:
- ✓ Compliance Mapping:
- ✓ Run Security Advisor



EbizonCloud's Audit Readiness Using CIS OCI Benchmarks

(Based on CIS OCI Foundations Benchmark v1.2/v1.3)



Critical Checks

- ✓ 1.1: Ensure no root user API keys exist
- ✓ 1.4: Ensure MFA enabled for all human users
- ✓ 2.1: Ensure no Object Storage buckets are publicly accessible
- ✓ 3.1: Ensure VCN flow logging enabled in all VCNs
- ✓ 3.3: Ensure WAF policies applied to public endpoints
- ✓ 4.2: Ensure Block Volumes encrypted with Customer-Managed Keys (CMK)



Tools for CIS Compliance

Native

- ✓ OCI Config → Compliance Rules (auto-remediate CIS failures)
- ✓ Cloud Guard → Detect CIS violations (e.g., public buckets)

Third-Party

- ✓ Prowler (OSS): `prowler oci --cis-level2`
- ✓ Wiz/Lacework: Continuous CIS posture assessment

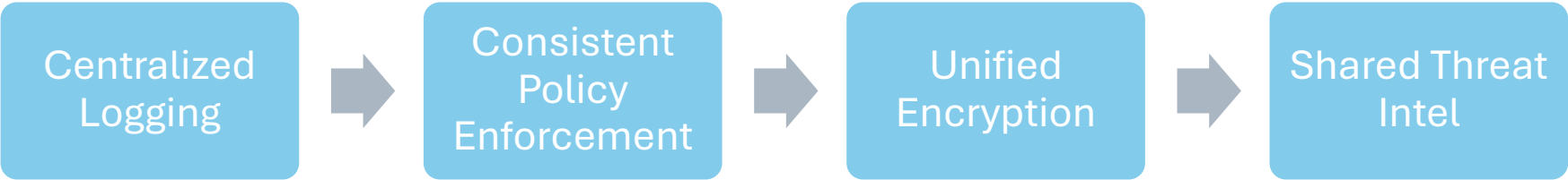
EbizonCloud's Multicloud Architecture Security Framework

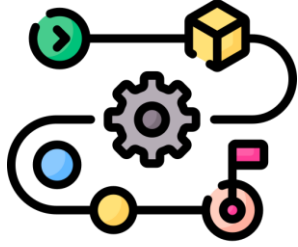
(Extending controls to AWS / Azure / GCP)

Cross-Cloud Security Checklist

Domain	OCI Native	Third-Party Integration
Identity	OCI IAM + SAML federation	PingFederate/SailPoint (centralized RBAC)
Network	OCI FastConnect + NSGs	Zscaler/Twingate (unified ZTNA)
Secrets Mgmt	OCI Vault	HashiCorp Vault (multicloud sync)
Threat Detection	Cloud Guard + OCI SIEM	Microsoft Sentinel (ingest OCI logs)
Compliance	OCI Security Zones	Wiz (CNAPP for OCI+AWS+Azure)

Key Multicloud Security Patterns





Implementation Roadmap



1. Assess

CIS Benchmark scan (Prowler / OCI Config),
Map workloads to shared responsibility model.



2. Harden

Deploy Security Zones for new workloads,
Enable Cloud Guard + VSS.



3. Extend to Multicloud

Implement central SIEM (e.g., Sentinel),
Deploy CNAPP (e.g., Wiz).



4. Automate

Use OCI Resource Manager,
Integrate third-party tools via OCI API.



Critical OCI-Specific Advantages to Leverage



Network Isolation: Physical separation of control/data planes provides enhanced security.



Always-Free DDoS: 8Tbps+ scrubbing with no additional cost for L3/L4 attacks.



Oracle DB Security: Native Data Safe for advanced masking and auditing capabilities.



Bare Metal Governance: Cloud Guard scans on-premises databases via OCI Agents for consistent security.



Regulated Workload Tip: For PCI/HIPAA, combine OCI Security Zones + HashiCorp Vault + Splunk for end-to-end audit trails.



Multicloud Benefit: Multicloud deployments benefit most from third-party CNAPP/SIEM unification.