



WEBINAR
Securing Your
Public Cloud Deployments
In the Age of Cloud Transformation



Vigilant-inc.com



Jim Ghormley

VP, Sales

35+ Years Experience In Information Technology & Sales

Jim Ghormley is VP of sales at Vigilant. He has an EECS degree from UC Berkeley and has been a leader in IT solutions and consulting sales for over 35 years, including many years supporting major IBM and Oracle clients and projects.

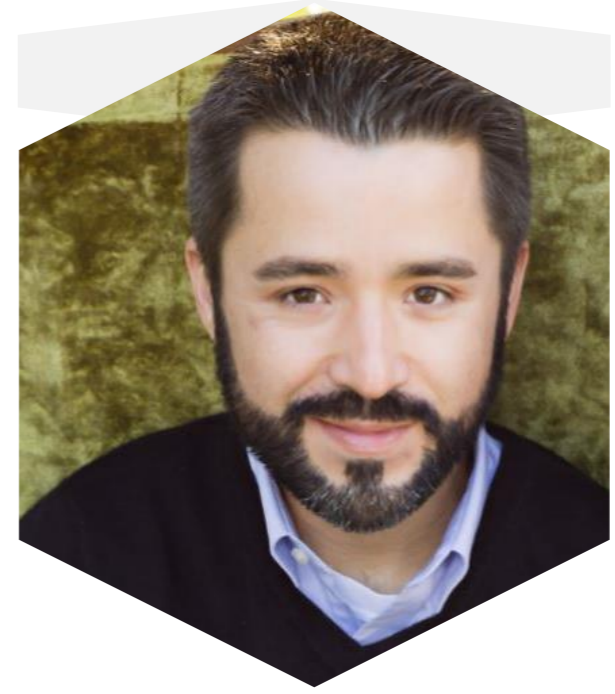


Amrita Mukherjee

Cloud Transformation Specialist

15+ Years Experience In Information Technology & Security

A Cloud Solutions Architect with Vigilant Technologies. Amrita started her career as a programmer, then moved on to become an application, database, and infrastructure admin, and has been a Cloud Architect for the past 15+ years. She has direct experience architecting and moving several types of workloads to the public cloud.



Stephen Clark

Principal, Azure Practice

20+ Years Experience in Enterprise Technology Solutions

Microsoft Cloud Principal, with Vigilant Technologies. Stephen has been focused on hybrid cloud and application modernization for 6-years. Over course of his career Stephen has remained focused on cloud-integration, app-modernization and enterprise identity/security to ensure that public facing workloads follow industry best practices.



Before We Start
**A Brief Introduction
to Vigilant**

Vigilant By the Numbers

Satisfied Customers Drive **Two Decades Of Consistent Growth**

200+

Enterprise Clients Served

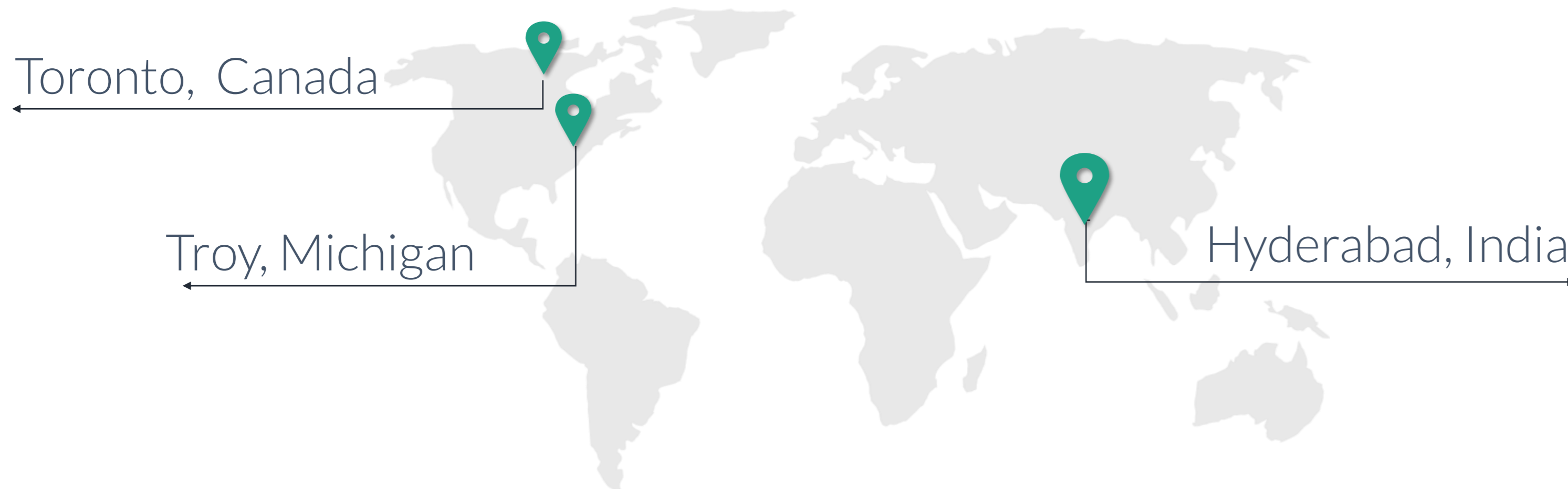
150+

Enterprise Application Projects

75+

Cloud Transformations

Locations



Cloud Services

- Lift and Shift or Hybrid cloud
- Cyber and Enterprise Security
- Workload Assessment
- Application Load Balancing
- Automation and Orchestration
- Governance and Control
- DevOps
- Network Security
- Pen Tests

Certified Experts



200+

Total Clients Served

Client Highlights

We serve large enterprises in a broad range of industries

MANUFACTURING



RETAIL

HEALTHCARE

FINANCE

OTHERS



Today's Agenda

How To Secure Your Public Cloud Deployments

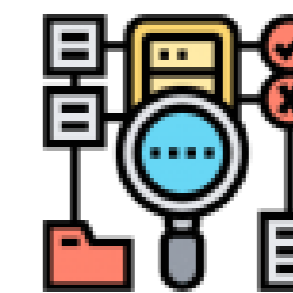


Best Practices



AWS, Azure, GCP, OCI

Tools



Azure & O365

Demo



Cloud Adoption Strategies



Common Roadblocks



Questions



Security on Public Cloud Best Practices

Firewall & Network Segmentation



Virtual Cloud Networks

- Logically isolated private networks
- Virtual networks, as if they were air-gapped physical networks.



Virtual Firewalls

- Stateful firewall components in a public cloud
- Track established connections and only allow return traffic associated with the session
- Access control lists (ACLs)



Virtual Appliances

- Fortinet
- CheckPoint
- Palo Alto
- Intrusion Detection & Prevention

Complex Environments

Simple Environments

Firewall & Network Segmentation



Amazon Virtual Private Clouds (VPCs)
Amazon EC2 Security Groups
VPC Network ACLs



Azure Virtual Network (VNet)
Azure Security Center
VNet NACLs



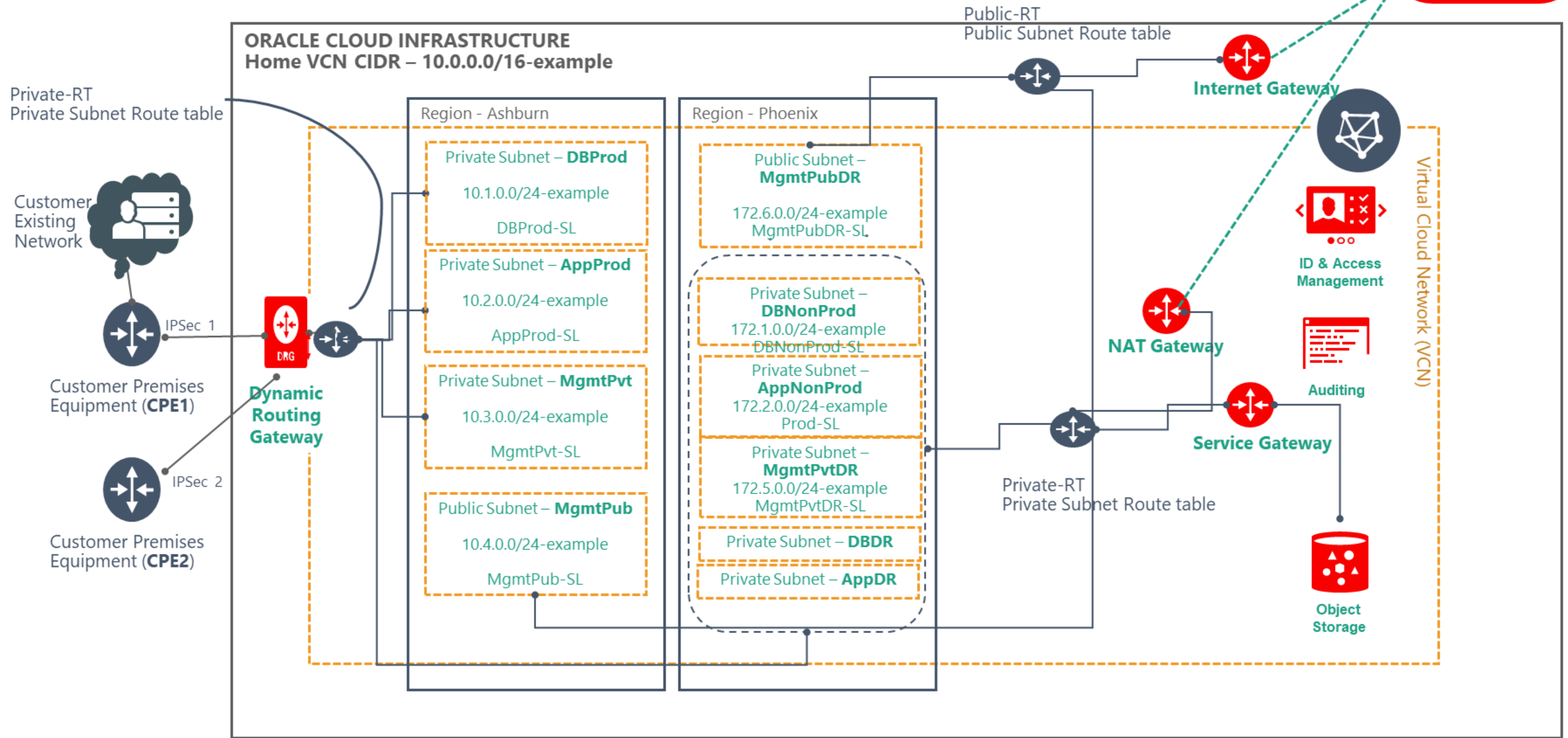
Google Cloud

Google Virtual Private Cloud
Google VPC Service Controls
Google Cloud Armor
Security Command Center



Oracle Virtual Cloud Network (VCN)
OCI Security Lists
OCI Network Security Groups (NSG)

Firewall & Network Segmentation On OCI



Vendor-Supplied Defaults



System Passwords

- Do not use default credentials
- Use cloud provider images wherever possible



OS Hardening

- Use pre-hardened images like CIS Benchmark



Network Hardening

- Follow “Deny-all” rule and only allow access on specific ports for specific protocols

Vendor-Supplied Defaults



Amazon Elastic Compute Cloud (EC2)
AWS CloudFormation
AWS OpsWorks Stacks
CIS Images



Azure Compute
Azure Batch
Azure Blueprints
CIS Images



Google Cloud

Google Compute Engine
Cloud Deployment Manager
Shielded VMs
CIS Images









OCI Compute Cloud
OCI Terraform
OCI Ansible
CIS Images







Pre-built Images On Azure & OCI

Search Compute

Recommended [More](#)

- 
Windows Server
Microsoft
- 
Red Hat Enterprise Linux
RedHat
- 
Ubuntu Server
Canonical
- 
SQL Server 2017 Enterprise
Microsoft
- 
Virtual machine scale set
Microsoft
- 
Container Service
Microsoft

Virtual Machine Images [More](#)

- 
- 
- 
- 
- 
- 

services, and documentation

US East (Ashburn) ⌵ ⌵ 🔔 ? 💬 🌐 👤

Browse All Images

<input type="checkbox"/>	Blue Prism Robotic Process Automation	Blue Prism
<input type="checkbox"/>	CIS CentOS Linux 6 Benchmark - Level 1	Center for Internet S
<input type="checkbox"/>	CIS CentOS Linux 7 Benchmark - Level 1	Center for Internet S
<input type="checkbox"/>	CIS Microsoft Windows Server 2019 Benchmark - Level 1	Center for Internet S
<input type="checkbox"/>	CIS Oracle Linux 6 Benchmark - Level 1	Center for Internet S
<input type="checkbox"/>	CIS Oracle Linux 7 Benchmark - Level 1	Center for Internet S
<input type="checkbox"/>	CIS Ubuntu Linux 16.04 LTS Benchmark - Level 1	Center for Internet S
<input type="checkbox"/>	CIS Ubuntu Linux 18.04 LTS Benchmark - Level 1	Center for Internet S
<input type="checkbox"/>	Charon Virtual SPARC	Stromasys Inc

Identity & Access Management



IAM

- IAM supports password and account policies
- Might need additional Identity Provider



Shared Responsibility

- It is the customer's responsibility to ensure that all password and account policies are configured to meet compliance requirements



Identity Service

- Works with IAM
- Federates with AD

Identity & Access Management



AWS Identity and Access Management
AWS Directory Service
AWS Cognito



Azure Active Directory
Azure AD Domain Services
Azure Information Protection
Azure Key Vault



Google Cloud

Google IAM
Cloud Identity
Managed AD
Cloud Key Management Service
Google Secret Manager



OCI IAM
OCI Identity Cloud
OCI CASB
Key Management
OCI Data Safe
Federation

Azure Identity and Access Management Use Cases

1 I want to provide my employees secure and easy access to every application from any location and any device

2 I want to quickly deploy applications to devices, do more with less and automate Join/Move/Leave processes

3 I need my customers and partners to access the apps they need from everywhere and collaborate seamlessly

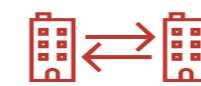
4 I want to protect access to my resources from advanced threats

5 I need to comply with industry regulation and national data protection laws

6 I want to write applications that work with my corporate identities in Azure Active Directory



Azure AD Connect



B2B collaboration



Provisioning-Deprovisioning



Conditional Access



SSO to SaaS



Self-Service capabilities



Connect Health



Multi-Factor Authentication



Addition of custom cloud apps



Access Panel/MyApps



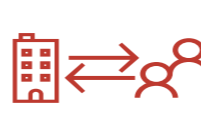
Dynamic Groups



Identity Protection



Remote Access to on-premises apps



Azure AD B2C



Group-Based Licensing



Privileged Identity Management



Microsoft Authenticator - Password-less Access



Azure AD Join



MDM-auto enrollment / Enterprise State Roaming



Security Reporting



Azure AD DS



Office 365 App Launcher



HR App Integration



Access Reviews

Data-in-Transit Encryption

1 **Application Load Balancers**
Native or Appliance

- Offload encryption processing
- Use at least TLS 1.1, preferably TLS 1.2
- Do not use Network Load Balancers

2 **Security Groups and Network ACLs**

- Use to block the use of insecure protocols

3 **Customer Gateways, Virtual Private Gateways, and VPN Connections**

- Use to setup encrypted VPN Tunnels into a virtual cloud network

4 **Cloud Connect**

- FastConnect from Oracle
- Direct Connect from AWS

Data-in-Transit Encryption



- Elastic load balancers
- Network ACLs
- Security Groups
- Customer Gateways
- Virtual Private Gateways
- VPN Connections
- AWS Direct Connect



- Azure Load Balancers
- Azure Application Gateway
- Azure VPN Gateway
- Azure ExpressRoute
- VNet ACLs

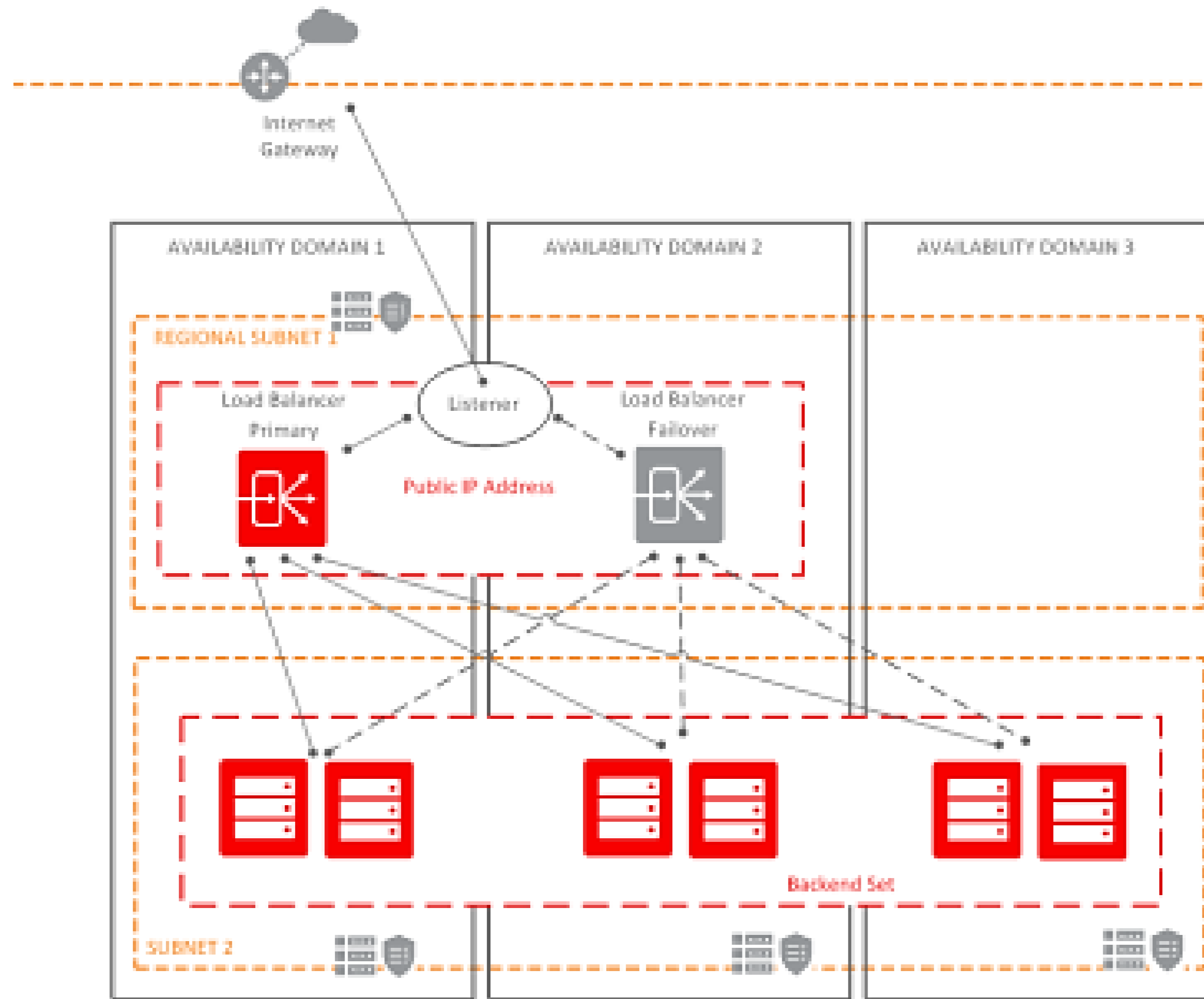


Google Cloud

- Google Cloud Load Balancing
- Google Cloud NAT
- GCP Network Intelligence Center
- Google Confidential Computing






- OCI Load Balancers
- NACLs
- Security Lists / NSGs
- Dynamic Routing Gateways
- NAT Gateways
- Service Gateways
- VPN Connect
- OCI Fast Connect



Application Load Balancer On OCI

Malware & Anti-virus Software

-  You are responsible for ensuring that all instances run appropriate anti-virus scans as well as log and report
-  Same is applicable for Malware protection
-  Cloud Marketplaces offer endpoint security platforms

Audit Trail



Basic Logging



Cloud Resources



Security Information & Event Management (SIEM)



Network Time Protocol

Audit Trail



AWS CloudTrail
AWS S3



Azure Sentinel
Azure Log Analytics
Azure Blob Storage



Google Cloud

Cloud Asset Inventory
Cloud Audit Logs
Google Cloud Logging



OCI Audit
OCI Log Analytics
OCI Resource
Manager
OCI Tagging
OCI Object Storage

Audit Trail On OCI



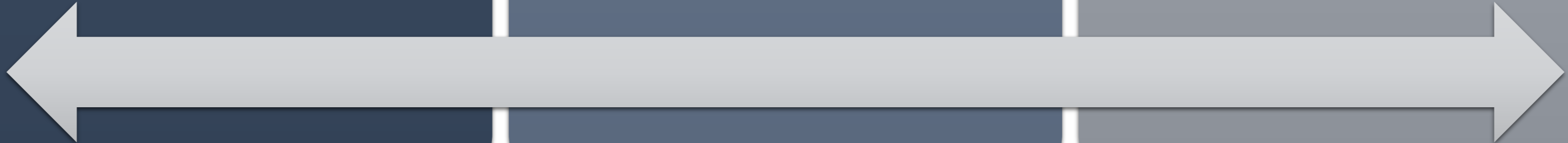
Data Integrity



Maintain
Traceability



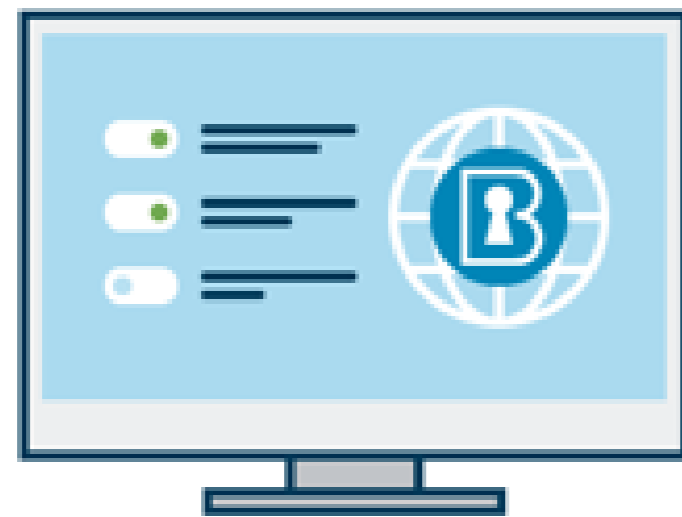
Visibility into
Infrastructure



CIS Hardening

CIS Benchmarks™

Globally recognized
secure configuration
guidelines



Applied to base OS in the cloud

CIS Benchmarks recommendations
are applied to OS and
applications in the cloud



CIS Hardened Images®

Securely pre-configured
CIS Hardened Images meet
requirements of CIS Benchmarks



CIS Hardening – Key Benefits

Helps Achieve Regulatory Compliance

Reduces Cyberthreat Risks

Scalable Deployment

CIS Benchmark Examples for Azure

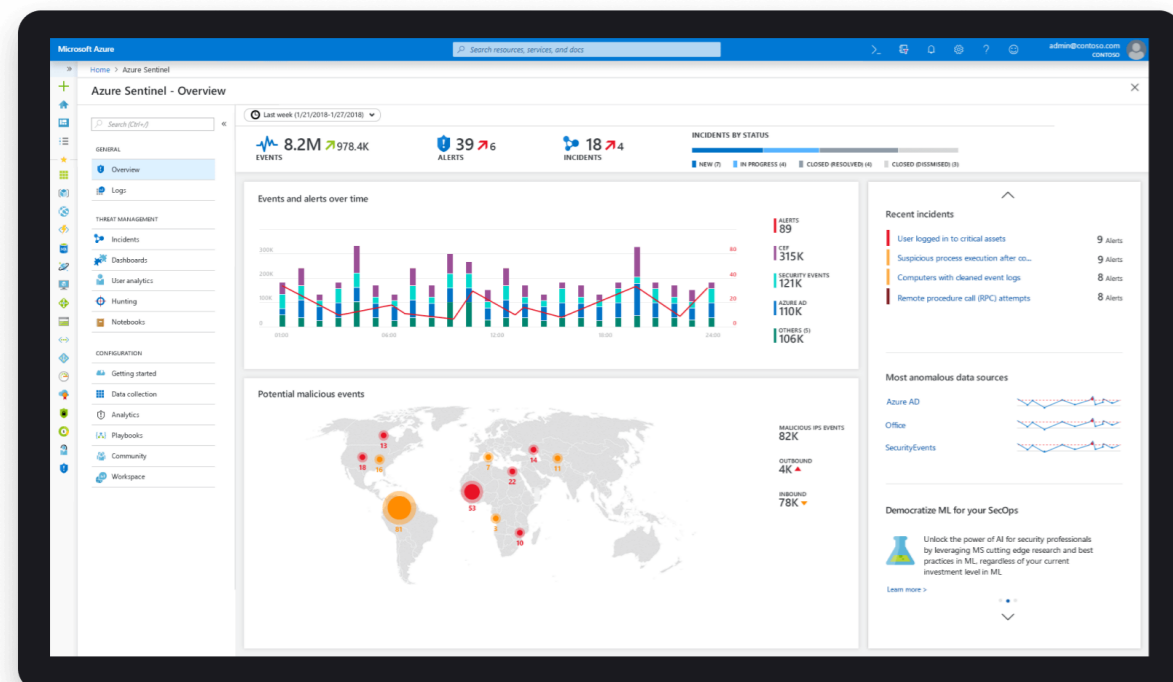
- **Identity & Access Management**
 - Ensure that multi-factor authentication is enabled for all privileged users
 - Ensure that 'Restrict access to Azure AD administration portal' is set to 'Yes'
 - Ensure that 'Users can create security groups' is set to 'No'
- **Security Center**
 - Ensure that 'Automatic provisioning of monitoring agent' is set to 'On'
 - Ensure ASC Default policy setting "Monitor OS Vulnerabilities" is not "Disabled"
 - Ensure ASC Default policy setting "Monitor Network Security Groups" is not "Disabled"
- **Storage Accounts**
 - Ensure that 'Secure transfer required' is set to 'Enabled'
 - Ensure that storage account access keys are periodically regenerated
 - Ensure default network access rule for Storage Accounts is set to deny
- **Database Services**
 - Ensure that 'Auditing' is set to 'On'
 - Ensure that 'Auditing' Retention is 'greater than 90 days'
 - Ensure that 'Advanced Data Security' on a SQL server is set to 'On'
- **Logging and Monitoring**
 - Ensure that Activity Log Retention is set 365 days or greater
 - Ensure the log profile captures activity logs for all regions including global
 - Ensure that Activity Log Alert exists for Create or Update Network Security Group Rule

How we achieved PCI compliance for one of our clients

1. Moved them from on-prem datacenter to the cloud, where you can piggyback on a cloud provider like AWS or Azure's Attestation of Compliance, thereby reducing the number of controls to be met
2. Rearchitected the web servers to be front ended by Application Load Balancers so all communication is encrypted with TLS 1.2
3. Used CIS Benchmark compute images to ensure OS is properly hardened and not using any default passwords or security parameters
4. Used cloud backup storage to leverage data-at-rest encryption provided by all major cloud vendors
5. Used Checkpoint Virtual Appliance to achieve IDS/IPS capabilities
6. Used Network Security Groups and subnets to achieve network segmentation
7. Federated with ADFS to supplement Cloud Identity Service capabilities

Azure & O365 Demo

- Office365 Service and Trust Center
- Azure AD
- End Point Protection Manager



In conclusion...

- **Encryption** should be based on accepted industry standards for both structured and unstructured data
- **Contextual Access Control** for corporate data in the cloud, based on user, device and geographic location
- **Application Auditing** of cloud usage and automatic alerts for anomalous (potentially malicious) use
- **Data Loss Prevention** for cloud data should include blocking of disallowed actions, alerting, and encryption
- **Extend cloud security**, governance and compliance policies to data as it moves between cloud services



Cloud Adoption Strategies

1 Termination and Data Retrieval

Termination clauses may be inadequate or may bring the potential for vendor lock-in.

Security 2

Evaluate the compliance and security certifications.

3 Data Privacy

Compliance and data privacy standards like HIPAA or PCI

Liability 4

Negotiate higher limitation of liability.

5 Cloud Repatriation

Verify T&Cs to bring data from public cloud to hybrid environment.









Data Retrieval Charges 6

Data retrieval and migration without the proper provisions may become challenging from a cost and support perspective.

7 Post termination Assistance

Incorporate clauses regarding assistance required during the termination period.

Common Roadblocks


-  Tightly coupled legacy architecture
-  Unsupported and deprecated platform and software versions
-  Lack of downtime or maintenance windows
-  Heavy customizations and integrations
-  Reluctance to adopt new skillsets
-  Inability to balance risk and reward
-  Financial considerations for OpEx
-  Compliance & Regulatory restrictions

What are some of the causes of failures?

- Insufficient Planning
- Organizational Bias
- Incorrect skillsets

Contact Us

For more than two decades Vigilant has been building relationships on trust and results—driving powerful IT outcomes. Our experts are here to help you navigate your next move.



Vigilant Technologies
1050 Wilshire Drive
Troy, Michigan 48084



mabdullah@vigilant-inc.com



(313) 777-8023



www.vigilant-inc.com