3/21/2025

Pennsylvania State University
College of Information Sciences and Technology

IST 554 Graduate Network Security

Project Deliverable 2

Group - 3 : *Aniket Nimbalkar , Gokul Gopakumar, Siddharth Mishra, Sohan Ramalingaiah*

Organization Name : OpenGuardian Solutions
(This is all a hypothetical organization and their current status of where they are as a Startup booming in the IT World)

Organization Abstract

OpenGuardian Solutions has its headquarters in Santa Barbara, California, and presently operates out of one building. It started in 2020 and today employs 62 people, which includes 45 technical staff, 10 sales and marketing specialists, and 7 executives. The vision for OpenGuardian is to empower organizations to secure and automate their digital futures. OpenGuardian's clients include mid-size healthcare providers, fintech start-ups, and e-commerce websites.

Founded by Emilia Perez and Rachel Zegler, OpenGuardian fosters a more in-person work culture, with 30% of its staff having the option to operate in a hybrid model. The company prioritizes continuous learning, heavily investing in industry-recognized certifications such as CISSP and AWS/Azure cloud training to ensure its technical teams maintain top-tier expertise.

Currently, the organization is looking to expand its footprints to Boston, Texas & Canada as their product has been gaining traction over the past 2 years with multiple clients such as Robinhood and Nvidia adopting the products used.

Briefly, the products that OpenGuardian offers:

- SentinelMDR: AI-facilitated threat detection and incident response solution for hybrid clouds.
- CloudFlow Orchestrator: Low-code DevOps automation platform for AWS, Azure, and GCP.
- ComplianceGuard: SaaS compliance monitoring platform (GDPR, HIPAA, PCI-DSS) in real-time.

Since this is a startup, there have been issues that the Security Team has been trying to solve as no organization starts from the most secure system which are discussed in the security structure section.

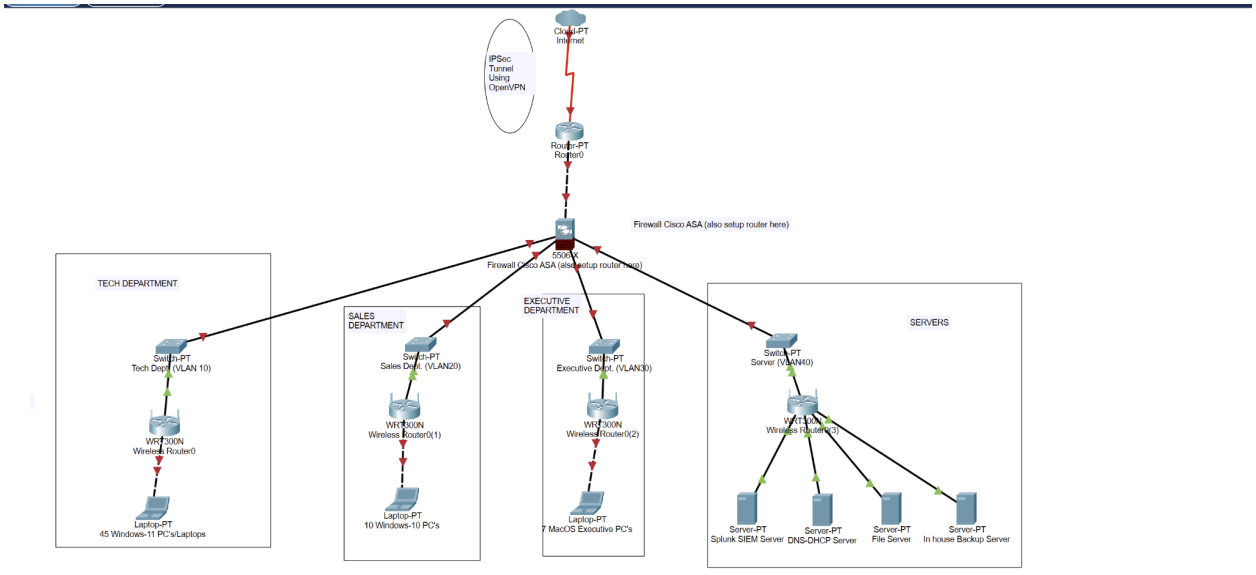
Organization Products

OpenGuardian offers a range of next-generation security and automation solutions that are tailored to suit the requirements of businesses across different sectors. SentinelMDR, one of its flagship products, offers managed detection and response 24/7 with 24/7 continuous network monitoring aimed at detecting and removing threats such as ransomware. For example, a Santa Barbara-based hospital leverages SentinelMDR to detect unusual access patterns in its patient database, automatically isolating compromised devices to prevent data breaches.

The second core product is CloudFlow Orchestrator, which automates deployment of container-based applications into multi-cloud environments with Kubernetes and Docker. Its automation realizes enormous reductions in complexity and deployment time. Example : A Denver logistics startup, for instance, reported a 70% decrease in deployment time after implementing CloudFlow's pre-built templates for AWS ECS, enhancing their scalability and efficiency

To address regulatory compliance challenges, OpenGuardian developed the product ComplianceGuard, a strong solution that searches cloud storage sites like AWS S3 and Azure Blob Storage for unencrypted personally identifiable information (PII). ComplianceGuard provides real-time audit reports to help companies maintain security and compliance levels intact. Example : A Boston-based e-commerce company successfully achieved PCI-DSS compliance within three weeks using ComplianceGuard's intuitive dashboards, streamlining their security and regulatory processes.

Network Architecture



Pic 1. Internal Network Diagram using Cisco Packet Tracer

The network architecture of OpenGuardian Solutions is designed to support its headquarters in Santa Barbara, California. The network architecture is currently designed with VLAN segmentation, including a

Cisco ISR router, a Cisco ASA firewall, router, and a Cisco Catalyst core switch, connecting various departments and servers.

Components

- **Router (Cisco ISR)**: Connects the organization to the internet via an ISP connection and routes traffic between the WAN and LAN.
- **OpenVPN tunnel:** Setup for only users who have successfully created a profile can access the internal network, data and devices.
- **Firewall (Cisco ASA)**: Provides security by filtering incoming and outgoing traffic.
- **Core Switch (Cisco Catalyst)**: Connects all network devices, including access switches, servers, and endpoints.
- **Access Switches**: Connect departmental devices, including PCs, VoIP phones, and wireless access points (WAPs).
- **Servers**:
    - DNS/DHCP Server: Manages IP address assignments.
    - File Server: Hosts internal documents and ComplianceGuard audit templates.
    - Backup Server: Stores local backups.
    - SIEM Splunk Server : Logs from both environments are aggregated in the SIEM server (Splunk) for centralized monitoring and compliance reporting.
- **Endpoints**:
    - 45 Technical Team PCs (Windows 11)
    - 10 Sales/Marketing PCs (Windows 10)
    - 7 Executive PCs (Mac OS)

  Only connected one but symbolizes connecting all the necessaryPC's. Not done to reduce redundancy.

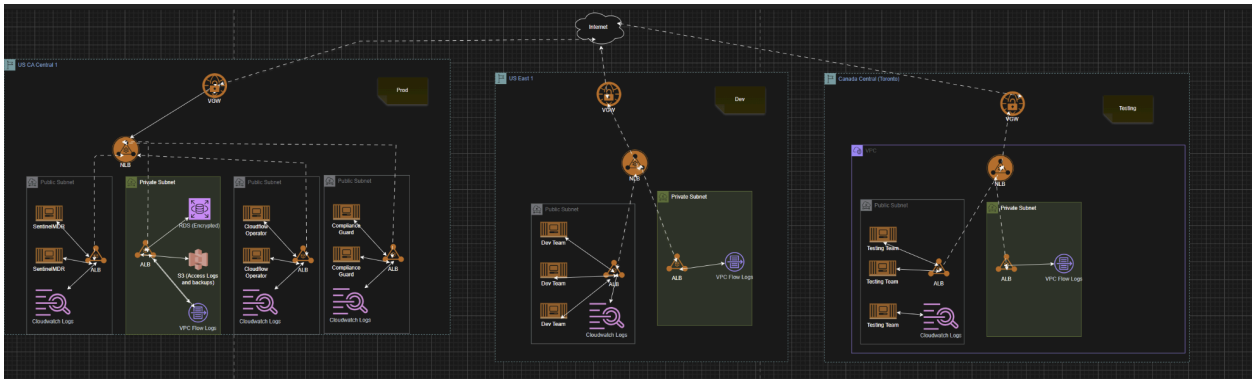
VLAN Segmentation

- **VLAN 10**: Technical Department
- **VLAN 20**: Sales Department
- **VLAN 30**: Executives Department
- **VLAN 40**: Servers (including Splunk)
- **VLAN 200**: Guest Wi-Fi (not setup yet)

Security Measures

- **Firewall Configuration**: The Cisco ASA firewall is configured to restrict traffic but requires regular updates to mitigate ransomware threats.
- **Endpoint Protection**: Basic antivirus tools are in place (Kaspersky), but patching is irregular.
- **Authentication**: Currently the organization is enforcing MFA using Duo Security or Microsoft Authenticator (depending on the users choice).

AWS Architecture



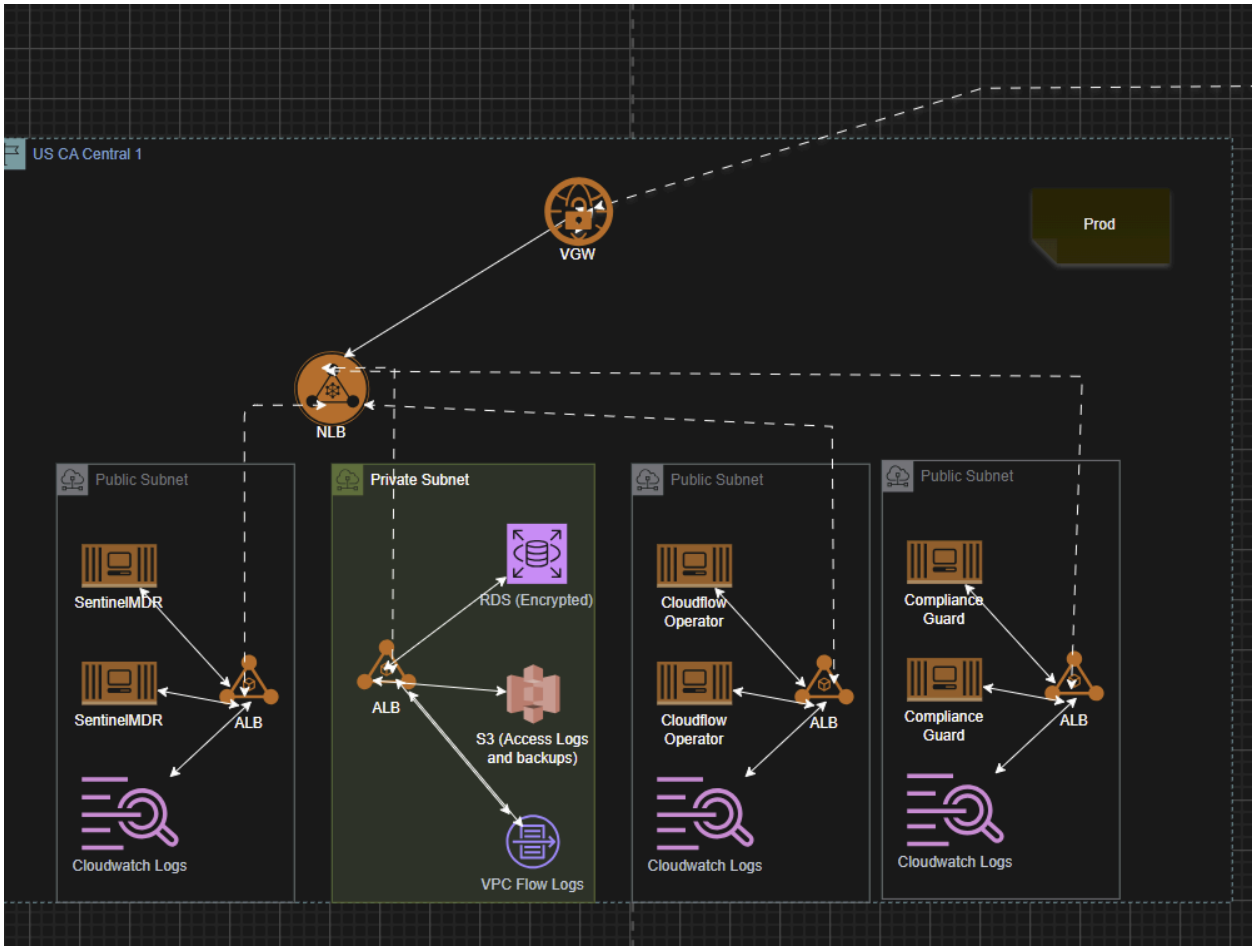
Pic 2. AWS Architecture of the organization

Overview

OpenGuardian's AWS architecture is designed to support its cloud-based products and ensure high availability and security. The architecture spans multiple AWS regions, including US-WEST-1 (Cali, US), US-East-1 (Boston), US-West-2 (Texas [in actuality, it is us-east-1-dfw-2a, but for better understanding of architecture, made it West-2), and Canada-Central (Toronto), with each region hosting a Virtual Private Cloud (VPC) for different environments (Production, Development, and Testing Operations).

Components

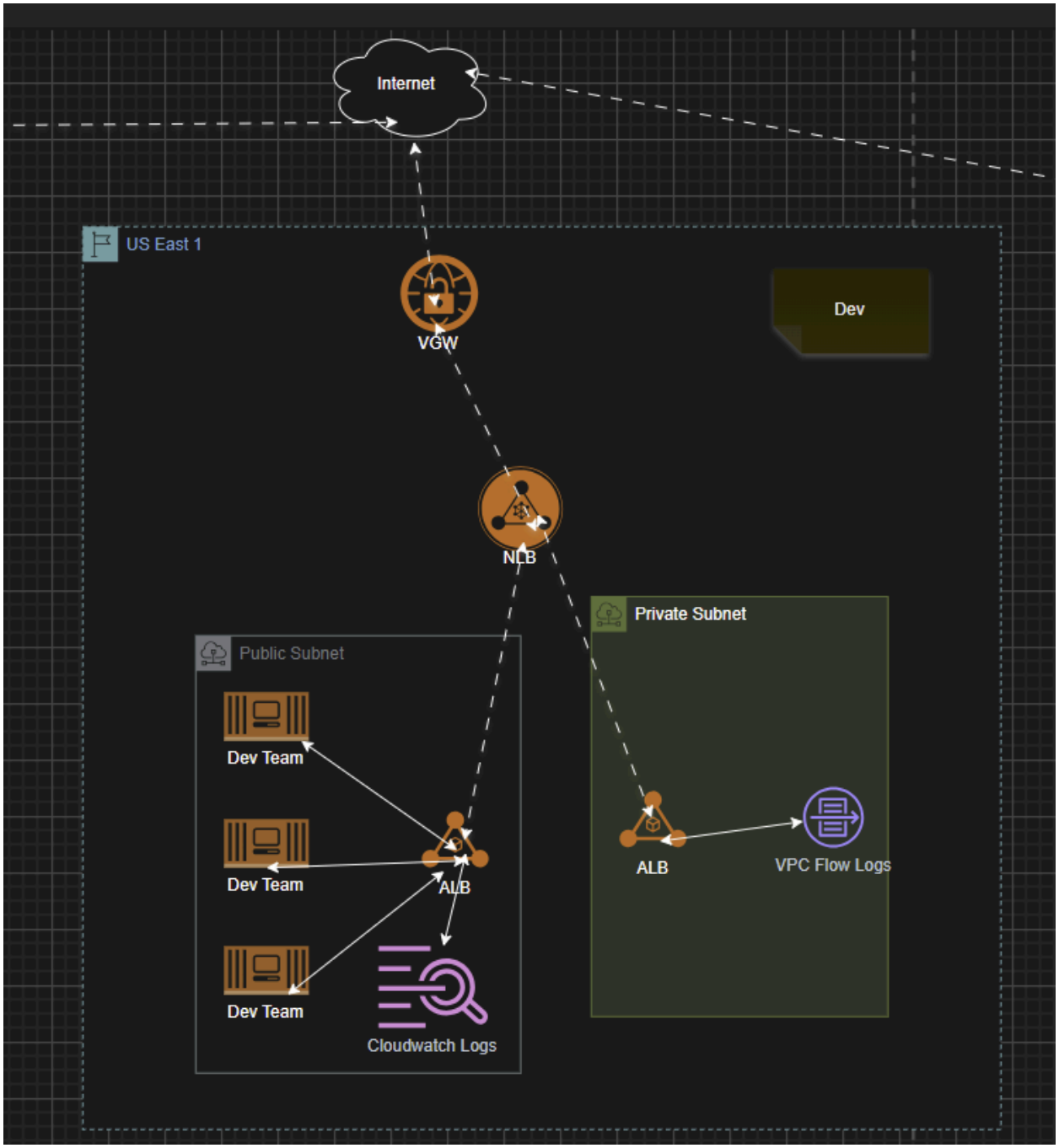
- **Virtual Private Gateway (VGW)**: Connects the on-premises network to AWS via Site-to-Site VPN.
- **VPCs**:
    - **OpenGuardian-Prod (US-WEST-1)**: Hosts production environments with public and private subnets.
    - **OpenGuardian-Prod (US-East-1):** Identical to production environment used for disaster recovery in case any issues with VPC, or AWS Regions occur. Since it is the same, it is not included in the architecture diagram to reduce redundancy.
    - **OpenGuardian-Dev (US-West-2)**: Hosts development environments.
    - **OpenGuardian-Canada (Canada-Central)**: Hosts testing operations.
- **Public Subnet**:
    - **Application Load Balancer (ALB)**: Distributes traffic to EC2 instances running SentinelMDR, CloudFlow Orchestrator, and ComplianceGuard.
    - **EC2 Instances**: Host application services with redundancy.
    - **CloudWatch Logs**: Monitors and logs application performance.
- **Private Subnet**:
    - **RDS Instance**: Hosts the ComplianceGuard database with encryption.
    - **S3 Bucket**: Stores immutable backups following the 3-2-1 strategy.
    - **VPC Flow Logs**: Monitors network traffic for security analysis.



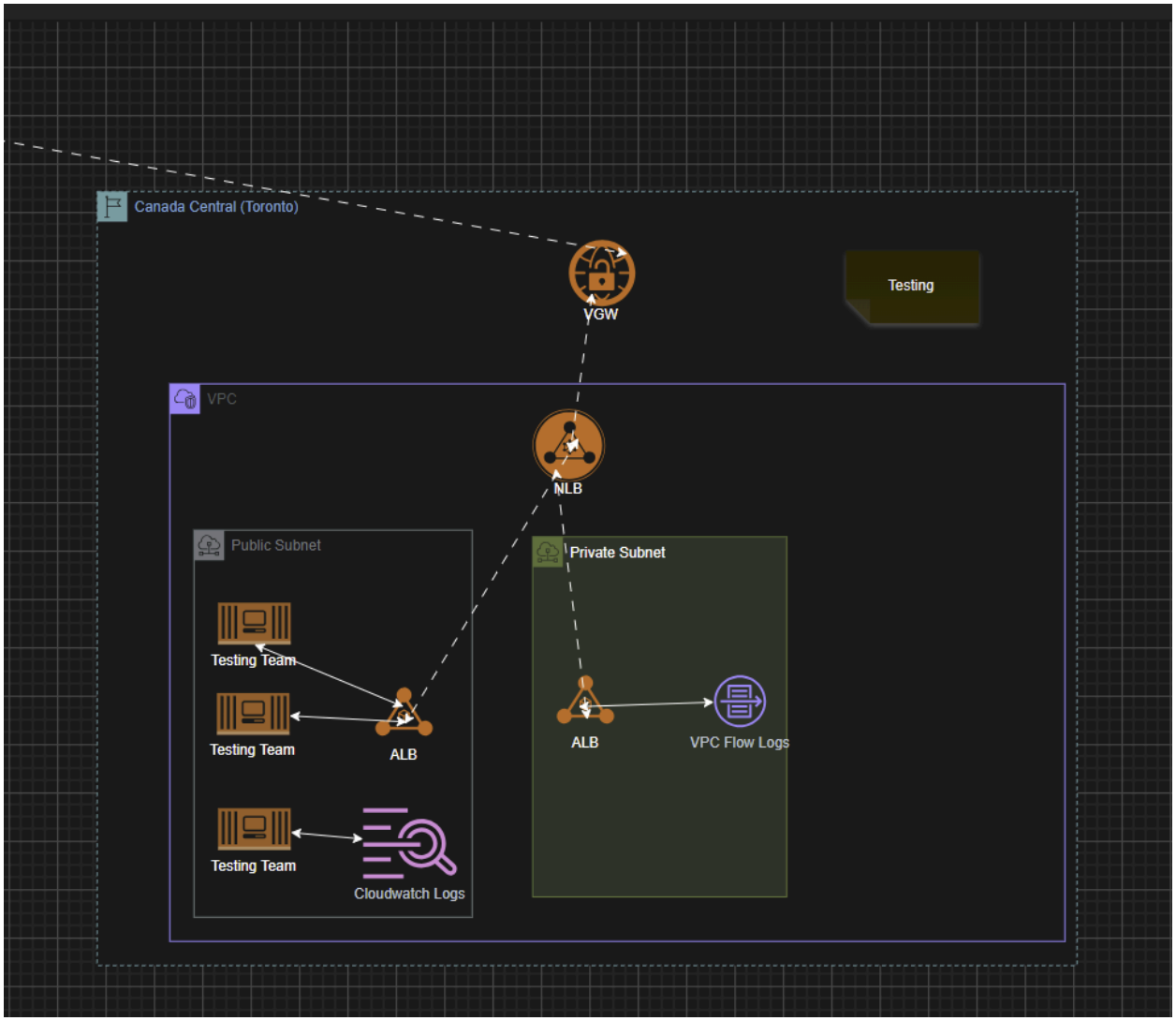
Pic 3. AWS Architecture of the Production Environment

Note : The identical architecture is used in Region US-East-1 for disaster recovery purposes.

Note :  Logo is meant to be any resources mainly computing that is required for that environment



Pic 4. AWS Architecture of the Dev Team environment



Pic 5. AWS Architecture of the Testing Team environment

Security Measures

- **Security Groups**: Restrict access to authorized IPs.
- **Encryption**: Data at rest and in transit is encrypted. (Transit using VGW, NLB, Security Groups and ALB) (Rest using RDS DB AES-256 Encryption algorithm with keys from AWS KMS refreshed every 120 days)
- **CloudTrail**: Logs database access for audit purposes.
- **VPC Flow Logs**: Provides visibility into network traffic.
- **IAM Security:** Restricts access to resources according to user privileges (Least privilege methodology used)

Backup Strategy

The AWS architecture implements the 3-2-1 backup strategy, with immutable backups stored in S3 buckets across multiple regions. This ensures data redundancy and protection against ransomware.

Integration of Network and AWS Architectures

Site-to-Site VPN

The on-premises network is connected to AWS via Site-to-Site VPN, ensuring secure communication between the headquarters and cloud environments. The Virtual Private Gateway (VGW) in each AWS region facilitates this connection, providing a secure tunnel for data transfer.

- The VPN tunnel uses IPSec to encrypt data in transit between the on-premises network and AWS.
- The tunnel ensures that all communication between the headquarters and AWS is secure and compliant with data protection regulations.
- The Cisco router and AWS VGW are configured to advertise and accept routes for the respective networks.

Data Flow and Security

Data flows between the on-premises network and AWS are encrypted and monitored. The Cisco ASA firewall and AWS Security Groups work in tandem to restrict unauthorized access. VPC Flow Logs and CloudWatch provide continuous monitoring and logging of network traffic in the Cloud, whereas Splunk stores and monitors all logs including the internal network logs.

Compliance and Monitoring

The integration supports compliance with industry standards such as GDPR, HIPAA, and PCI-DSS. The SIEM server (Splunk) on VLAN 100 aggregates logs from both on-premises and cloud environments, providing a centralized view of security events.

Benefits of Integration

1. **Seamless Connectivity**: Employees can access both on-premises and cloud resources seamlessly, improving productivity.
2. **Scalability**: AWS provides scalable infrastructure to support OpenGuardian's growing product offerings and client base.
3. **Disaster Recovery**: The integration enables robust disaster recovery capabilities, with backups stored in AWS S3 and redundant resources across multiple regions.
4. **Centralized Monitoring**: The use of Splunk for centralized logging and monitoring ensures that security events are detected and responded to promptly.

Compliance Status of OpenGuardian Solutions

GDPR, CCPA, and PCI-DSS Compliance

- **Data Protection**:
    - Encryption of data in transit and at rest ensures compliance with GDPR, CCPA, and PCI-DSS requirements.
- **Access Controls**:
    - Strict access controls and audit trails help meet compliance requirements for data access and monitoring.
- **Data Deletion**:
    - Mechanisms for data deletion, as provided by **ComplianceGuard**, ensure compliance with GDPR and CCPA.

HIPAA Compliance [NOT]

While the current setup is not fully HIPAA compliant, the integration of on-premises and AWS architectures provides a foundation for achieving compliance. Key steps include:

- Signing **Business Associate Agreements (BAAs)** with healthcare clients.
- Implementing **HIPAA-specific workforce training**.
- Enhancing audit trails for PHI access.

Future Enhancements

1. **Automated VPN Failover**: Implement automated failover for Site-to-Site VPN connections to ensure continuous availability.
2. **Enhanced Encryption**: Explore the use of **AWS Direct Connect** for private, high-speed connectivity between the headquarters and AWS.
3. **Advanced Threat Detection**: Integrate **AWS GuardDuty** with the on-premises SIEM server for advanced threat detection across hybrid environments.
4. **HIPAA Compliance**: Implement additional controls, such as PHI-specific access logging and encryption, to achieve HIPAA Compliance for future endeavours.

Conclusion

The integration of OpenGuardian Solutions' on-premises network with its AWS architecture is a well-designed, secure, and scalable solution that supports the organization's business objectives. By leveraging Site-to-Site VPN, encryption, access controls, and centralized monitoring, OpenGuardian ensures seamless connectivity, data protection, and compliance with GDPR, CCPA, and PCI-DSS. While the setup is not yet HIPAA compliant, the foundation is in place to achieve this goal with targeted enhancements. This integrated architecture positions OpenGuardian to continue its growth and deliver secure, innovative solutions to its clients.

Industry Literature : Overview of Similar Infrastructure

The 2025 Fortra State of Cybersecurity Survey and The 2025 State of Cloud Report highlight the growing adoption of hybrid cloud strategies across industries. These reports reveal that:

- 60% of organizations currently employ a hybrid cloud strategy, allowing them to use either cloud or on-premises infrastructure based on specific needs.
- 22% of organizations plan to accelerate hybrid cloud adoption over the next 12-24 months. [3]

Many organizations, including those in sectors like media (Netflix, Hulu), ride-sharing (Uber), and accommodation (Airbnb), leverage hybrid IT architectures, combining on-premises infrastructure with cloud resources for flexibility and cost-effectiveness.

Netflix and Hulu use hybrid cloud storage to handle spikes in demand during popular series releases, combining on-premises storage with cloud services like AWS [1]

Netflix found that Amazon was the partner that they needed. Instead of investing a lot of money in servers and storage machines, they used Amazon's infrastructure. At that time, transmitting vast data such as video over the Internet was still something not secure for many reasons, including bandwidth quality; therefore, servers needed to be located near the regions, where many customers used the service, while Amazon was investing in a lot of server regions across the United States of America. [2]

AthenaHealth, a leading healthcare technology company, has embarked on an ambitious journey to modernize its technology stack by leveraging AWS's hybrid cloud solutions. This transformation aims to enhance scalability, performance, and developer productivity, ultimately improving the quality of care provided to its patients. AWS allows AthenaHealth to scale its infrastructure dynamically to handle fluctuating workloads, such as peak times for patient data processing. By migrating critical workloads to AWS, athenahealth improved the performance of its EHR and patient engagement portals. [4]

OpenGuardian Solutions, as a startup specializing in security and automation solutions in the Cloud, can draw valuable lessons from the hybrid cloud transformations of AthenaHealth into their own architecture and the broader industry trends highlighted in the 2025 Fortra State of Cybersecurity Survey and The 2025 State of Cloud Report.

Like AthenaHealth's EHR system and Netflix's demanding platform, SentinelMDR requires a scalable infrastructure to handle increasing workloads, such as monitoring multiple client environments for threats. Leveraging AWS for scalable compute and storage resources can enhance SentinelMDR's performance and reliability.

AthenaHealth's use of AWS to improve developer productivity mirrors OpenGuardian's goal with CloudFlow Orchestrator. By leveraging AWS's cloud-native tools (e.g., ECS, EKS), OpenGuardian can further streamline DevOps workflows and reduce deployment times for clients.

By integrating AWS services like CloudTrail and Config, ComplianceGuard can provide real-time audit reports and ensure compliance with GDPR, PCI-DSS, and HIPAA.

These examples provide a roadmap for OpenGuardian to enhance its infrastructure, improve compliance, and scale its operations effectively.

References

(1) [2022] AWS Customer Stories, "Netflix Catalogs Objects Across Hybrid Cloud Storage Systems", https://aws.amazon.com/solutions/case-studies/netflix-storage-reinvent22/

(2) [2024] Hugo Humbert, "Case Study: How Netflix Leverages Cloud Computing for Success", https://medium.com/@hugo-humbert/case-study-how-netflix-leverages-cloud-computing-for-success-6964283e1b6e

(3) [2025] “2025 Fortra State of Cybersecurity Survey Results Guide”, https://www.fortra.com/resources/guides/fortra-state-cybersecurity-survey-results?_gl=1*1p7zqre*_ga*MTk5NDg3Mjk2Ni4xNzQyNjEzNjYw*_ga_NHMHGJWX49*MTc0MjYxMzY1OS4xLjAuMTc0MjYxMzY1OS42MC4wLjA.*_gcl_au*Nzg2MTY0NDQ3LjE3NDI2MTM2NjA.

(4) [2024] AWS Architecture Blogs, https://aws.amazon.com/blogs/architecture/hybrid-cloud-journey-using-amazon-outposts-and-aws-local-zones/

(5) [2024] Technative Blog, https://technative.io/state-of-application-strategy-2024-navigating-hybrid-it-trends-2/