Security and Compliance Architecture

Author: Hari Krishna Potluri

HIPAA and NIST Controls

For this architecture, my top priority was aligning every design choice with HIPAA and NIST 800-53 Moderate controls. I enforce encryption everywhere—using TLS 1.2+ for all data in transit, and AWS KMS with customer-managed keys for data at rest (covering S3, EBS, RDS, etc). I configure IAM with least-privilege, centralized SSO, and strong role separation, making sure access is only ever granted when necessary. Every action is logged using CloudTrail and integrated with GuardDuty and a third-party SIEM, so audits and compliance checks can be performed at any time.

Implement Zero Trust

I don't assume trust between any two systems—whether in AWS, between accounts, or with on-prem. Every route is explicitly defined via TGW, and all ingress/egress is filtered and inspected in a dedicated VPC with NGFWs. Identity is managed centrally with SSO (SAML/MFA), and only necessary resources are accessible from any role. This not only meets compliance requirements, but actually reduces operational risk in day-to-day work.

Secure Secrets and Key Management

I never hard-code secrets or credentials; instead, I store everything in AWS Secrets Manager, with automated rotation and tight, auditable access policies. Encryption keys are managed in KMS, and key usage is strictly limited to designated services. I monitor key usage with CloudTrail and make sure every sensitive operation is logged for later review. This means incidents can be quickly detected and resolved, and secrets never sprawl beyond what's needed.

Network Boundaries

My design funnels all network traffic through an Inspection VPC equipped with next-gen firewalls and packet inspection. I set up WAF on CloudFront and ALB for all web entry points, and make sure every VPC and endpoint is isolated by design. All network flows—internal and external—are logged and visible to GuardDuty, so any anomaly or attack can be detected fast.

Monitoring, Auditing, and Access Review

I centralize logs and metrics using CloudWatch, OpenSearch, and GuardDuty, with strict access controls to logs and audit data. I recommend (and automate) quarterly access

reviews for all privileged roles and secrets, to enforce least privilege and maintain compliance. With this architecture, audit readiness is ensured.