Automated Compliance and Threat Detection for Telecom Deployments on AWS

Jayavelan Jayabalan

Independent Researcher

University of Madras, India

***Abstract*— The telecommunications industry is undergoing a fundamental shift from traditional on-premises infrastructure to hosted environments in the cloud where cloud-native deployments occur, especially on Amazon Web Services (AWS). This article discusses how telecom organizations can use automated compliance and threat detection frameworks to protect themselves while executing telecom operations in the cloud. It outlines the regulatory challenges faced by telecom companies that are particular for telecom, describes the architectural principles at AWS that support secure deployments, and indicates the various types of AWS native tools available to monitor continuously, leverage behavioral analytics, and enforce compliance. By deploying a combination of services such as AWS Config, AWS GuardDuty, AWS Control Tower and AWS Security Hub, telecom operators will have real-time visibility of their environment, a centralized governance capability, and rapid and effective incident response and automation capability. A practical case study provided a real-life illustration of how to use these tools in a telecom environment to show that the use of automation and intelligence is not a luxury, but rather a necessity in telecom security today. The paper ends with a discussion about the potential role of AI, the future of 5G and edge computing, and the expectation of continuous improvement in the provision of secure cloud-based telecom services for end customers.**

***Index Terms*— telecommunications, Amazon Web Services, automated compliance, threat detection**

1. Introduction

In the past few years, the telecommunications industry has experienced a massive shift as a result of digital transformation, a rapid movement towards cloud-native environments, and increasingly complex network operation environments. As telecommunications providers have transitioned to cloud platforms, such as Amazon Web Services (AWS), and adopted distributed infrastructure models, the security and regulatory rispositions have increased substantially. While cloud adoption provides many benefits, including elasticity, cost-effectiveness, and scalability, it also highlights a multitude of complex security challenges; most notably no clear ownership of my customer's sensitive data, commitment towards the integrity of networks, and meeting regulations. Based on the function of telecommunications workloads, most all process real-time communication and sensitive personal data that is considered as critical data by regulatory bodies. Therefore, these workloads are "high-value" targets for threat actors. This complex position of being required to produce agile operations and have bulletproof security has prompted many organizations in telecommunications to rethink their regulatory compliance and threat detection processes in the context of the cloud [1] [2].

AWS has emerged as a foundational platform for modern telecom deployments. AWS offers a robust array of services—from compute and network to monitoring, governance, and artificial intelligence—that form the foundation for secure and compliant operation. However, the extensive capabilities of AWS create opportunity, but also require that telecom operators take a thoughtful and holistic approach to security. Telecom operators should not just rely on traditional perimeter defenses or manually created compliance reporting when the workloads are ephemeral and in increasingly distributed cloud environments. Operators must design their security architecture to utilize automation, continuous monitoring, and real-time threat detection as first-class components of the security strategy [3].

Automating compliance has become a requirement to keep pace with rapidly evolving industry requirements and no longer just an efficiency. Frameworks like the NIST Cybersecurity Framework (CSF), ISO 27001, and GDPR require organizations to demonstrate both the enforcement of governance policies and expanding upon those with proof of compliance monitoring as well. Within AWS, services like AWS Config, AWS CloudTrail, and AWS Control Tower provide the ability to view and manage infrastructure changes at scale and automatically validate those against established governance baseline [4]. This is particularly important to the telecom sector because changing the network in the wrong way can present service reliability and regulatory risk. By embedding automated governance compliance checks as an event in the infrastructure pipeline, telecom operators can have continuous compliance while reducing the potential for human error and the time to remediate any situations [5].

Simultaneously, threat detection approaches need to shift from static perimeter protection to dynamic, behaviorally-aware monitoring protocols. Some native tools from AWS—such as Amazon GuardDuty, Security Hub, and VPC Flow Logs—collect, correlate, and prioritize security events at scale across the cloud environment. This visibility reveals not only what is happening at the network layer, but also exposes visibility to API-level interactions, identity interactions, and data flow, equipping security teams with the telemetry needed to alert, and respond to anomalies quickly [2]. The incorporation of artificial intelligence with security operations (e.g. Amazon Q and AI-enhanced threat analytics) is allowing the telecommunications provider to switch from reactive to proactive security strategies [6].

This paper examines how telecom operators might utilize an integrated strategy for automated compliance and threat detection using AWS as a cloud provider. In addition to articulating architectural considerations, it presents related AWS services, and strategic frameworks that may streamline the protection of telecom workloads. From this review, it is evident that automation, visibility, and intelligent response create the foundation of any solid cloud security strategy for telecom deployments. The intent is to not only comply with regulatory requirements but to also facilitate secure innovation at the speed required in modern telecom landscape [1] [2] [4].

2. Compliance Requirements in Telecom: Risks and Challenges

The telecommunications industry deals with among the most complex regulatory landscapes in the world, created by the requirements of protecting sensitive customer data, service reliability, and complying with legislation. The shift to cloud-native infrastructure has introduced a new level of complexity to an already complicated compliance landscape - one that requires telecom operators to align its security posture with international and regional compliance requirements, while not sacrificing agility and operational flexibility. Cloud computing deployments on platforms like AWS provide a tremendous level of flexibility, but they also introduce new attack surfaces, transient resources, shared responsibility models, all of which require continuous compliance [1][2].

Legal requirements such as General Data Protection Regulation (GDPR), ISO 27001, Federal Communications Commission (FCC) laws in the US, in addition to many national telecom compliance requirements require regulation of how data is collected, managed, stored, accessed, and processed. In the cloud—where the traditional methods of compliance, such as periodic audits, manual reporting, and static control measures—are not functional as the infrastructure can be transient and short-lived, even if automated, and is governed through APIs, telecom operators must be able to move towards continuous compliance with automated governance. In AWS, this is possible through various services such as AWS Config, which tracks and records the configuration of resources; AWS CloudTrail, which records account activity and changes; and AWS Control Tower, which provides extensive governance over multiple accounts at scale [4]

The benefits of working with compliance frameworks such as the NIST Cybersecurity Framework (CSF) to AWS tools is as pertinent as the following. The NIST CSF framework presents an organization with a comprehensive procedure for and managing cybersecurity incidents, which designates functions into five sections identifying, protecting, detecting, responding and recovering. Each of these five function can be contoured to AWS services that inform operators on how to create a complete compliance architecture that is also cloud-native. For example, it associates 'Identify' to AWS Systems Manager Inventory, 'Protect' is IAM policies and AWS Shield, 'Detect' is through Amazon GuardDuty and cloudWatch, 'Respond' when creating AWS Lambda automation workflows, and 'Recover' infers backup and versioning AWS services like AWS Backup and S3 versioning. [5] [6].

To visually illustrate this alignment, the following diagram presents the mapping of NIST CSF Functions to AWS Tools as applicable in telecom compliance automation:

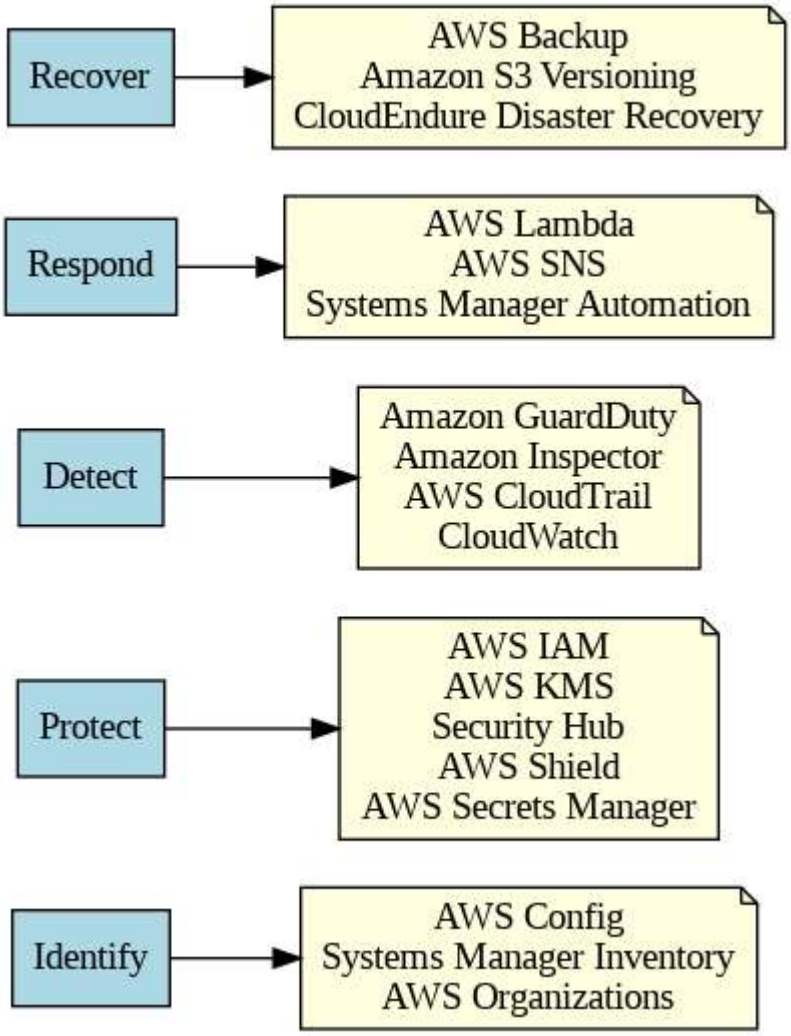


Figure 1: Mapping NIST Cybersecurity Framework Functions to AWS Compliance Tools

This integrated model allows telecom operators to create auditable, repeatable compliance controls while reducing the burden of manual oversight. Moreover, AWS offers specialized tooling for audit preparation and reporting, such as AWS Artifact, which provides on-demand access to security and compliance documentation, and Amazon Q Developer, which supports generative AI-powered compliance dashboards and automated evidence collection [6].

The risks of non-compliance are significant and multifaceted, including legal penalties, reputational damage, and service disruptions. For telecom providers, which are essential infrastructure operators, any compliance failure has widespread implications—not only in terms of regulatory fines but also in eroding consumer trust. By adopting AWS-native compliance automation and aligning cloud governance with industry frameworks like NIST, telecom organizations can proactively manage these risks. The move towards real-time compliance monitoring, driven by continuous visibility and automation, is no longer an advantage—it is an operational imperative in today's regulatory climate [2] [3] [5].

3. AWS Cloud Architecture for Telecom Deployments

Establishing a secure and scalable cloud architecture should be the first step for any telecom deployment based on AWS. Telecom operators usually process petabytes of data and have hundreds of services and operations in different geographical areas, so a strong but flexible infrastructure is needed to support their internal requirements while providing resiliency to enable high availability and compliance. AWS provides a solid and flexible architecture model using regions and availability zones, as well as networking components such as Virtual Private Clouds (VPCs), that enables telecom organizations to build enterprise-level cloud deployments according to their operational, regulatory and security requirements [1] [3].

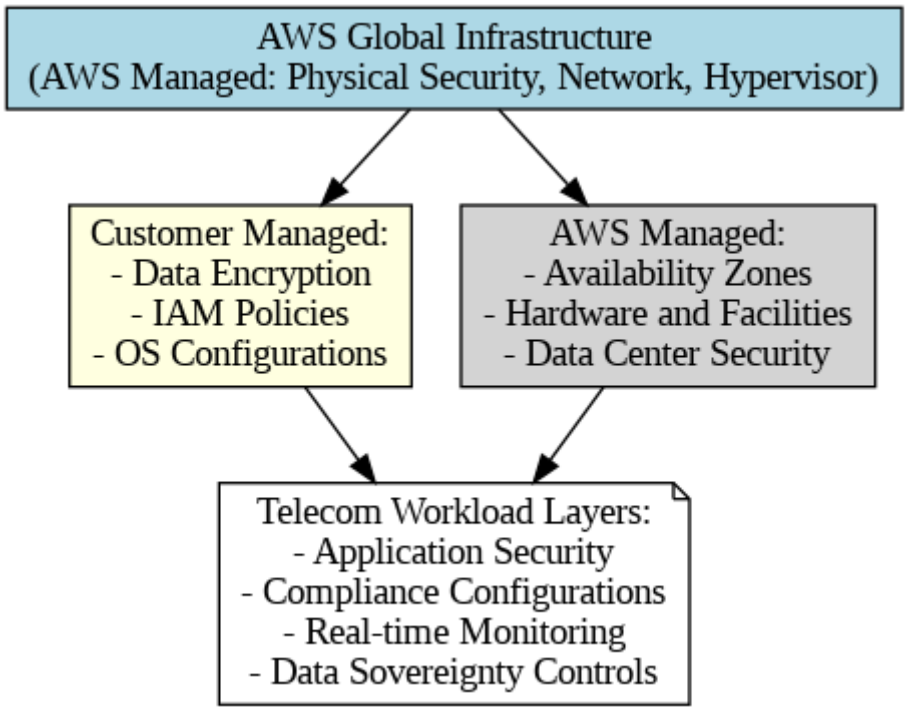
The AWS shared responsibility model is the foundation of this architecture. AWS is responsible for the security of the cloud, including the hardware, networking, and global infrastructure. Customers are responsible for security in the cloud, including data encryption, identity access controls, and security at the application level. This delineation of responsibilities is critical in telecom, which has a strict governance of data flows, customer identity management, and secure processing of workloads. Knowing and designing architecture with this shared responsibility is essential to reduce the risk and enforcing compliance in a multi-tenant cloud environment. [2] [5]

The modular nature of AWS, through Amazon EC2, Amazon S3, AWS Lambda, and Amazon RDS, is one of the advantages to telecom workloads. You can compose and orchestrate workloads that are scalable on call routing, billing, network analytics, and subscriber management. AWS provides the construct to logically isolate workloads, and control the flow of traffic for workloads, through Virtual Private Clouds (VPCs), individual defining subnets, route tables, security groups, and Network Access Control

Lists (NACLs). When developed with thought, these constructs allow telcos to manage east-west and north-south traffic, isolate workloads (for example, billing and customer portals should not share the same network), and reduce blast radius in the event of a breach [3] [4].

In addition to compute and storage solutions, AWS has security-focused services like AWS Identity and Access Management (IAM), which can assist telecom providers around defining who can access what resources and how. When IAM is paired with AWS Organizations and Control Tower, IAM allows for central governance across multiple accounts, which is a must-have for telecom: typically, telecom has development, staging and production environments. AWS CloudTrail and Amazon CloudWatch provide visibility into API calls and behavior of infrastructure and are the monitoring and logging layer for real time threat detection and operational troubleshooting [2] [4].

To demonstrate the interrelationship between AWS services and the shared security responsibilities, the next diagram highlights



the AWS Shared Responsibility Model developed for a telecom deployment.

Figure 2: AWS Shared Responsibility Model for Telecom Deployments

This architecture also supports a layered security approach, and better illustrates the boundaries of what AWS controls and what needs to be achieved by the telecom engineer and security architect, which is invaluable as some telecoms migrate from legacy core network elements to cloud-native options. The clarity afforded by this architecture can help to minimize misconfigurations and any audits through gaps in the chain of custody [1] [5].

AWS provides further advantages for telecoms in the creation of multi-region architectures. With services like Amazon Route 53, AWS Global Accelerator, and S3 Cross-Region Replication, operators achieve low latency and geo redundancy for effective compliance with data residency legislation. Using complementary services like AWS Wavelength for 5G edge computing, coupled with a secure, private dedicated link to the telco neck for AWS Direct Connect, telecoms can extend their existing network security and architecture and achieve high throughput and low latency [3] [6].

AWS provides the architecture and tools for telecoms to build secure, compliant, and resilient infrastructure. In combination with industry best practices, standards and compliance frameworks, this cloud architecture can support the operational foundation for secure telecommunications innovation in the age of cloud [2] [4].

4. Threat Detection Strategies in AWS for Telecom

The growth of telecom infrastructure into cloud-native infrastructure has transformed the way in which threat detection must be approached. Reliance on perimeter-based security models leveraging firewalls and a collection of static configurations are insufficient in an AWS system that is dynamic, scalable, and decentralized. In particular, telecom networks with thousands of endpoints, and data flowing in the lots of terabytes of real-time information will necessitate proactive, automated, intelligent detection of threats and intrusions. The systems must also be capable of operating across distributed cloud services and network layers with real-time threat detection capabilities of both known threats and emerging threats [1] [2].

Utilizing a plethora of native AWS tools designed specifically to meet the novel paradigm of cloud security monitoring, weak attack detection can be identified, and remediation can be deployed. Central to this is Amazon GuardDuty, a threat detection service that continuously monitors AWS accounts, workloads and data stored in Amazon S3 for malicious activity and unauthorized behavior. GuardDuty provides both a valuable level of transparency into AWS accounts by providing security alerts and enabling proactive threat detection for AWS cloud deployments. When a threat is detected by GuardDuty, it will analyze logs providing visibility into AWS CloudTrail, AWS VPC Flow Logs, and DNS query logs to identify anomalous behaviours for a host of known threat scenarios such as credential exfiltration, compromised instances, and unauthorized access patterns. For telecom deployments involving workloads with customer identity systems and call data, GuardDuty's ability to identify account compromise scenarios and internal threats is highly valuable [2] [3].

Another essential service is AWS Security Hub since it consolidates and prioritizes security findings from various AWS services including GuardDuty, Amazon Inspector, and Amazon Macie, as well as across third-party tools. For telecom operators with a presence of infrastructure in multiple accounts and regions, Security Hub allows for an aggregated view, providing a dashboard where alerts can be correlated and contextualized. The centralization of visibility, enables security teams to triage threats faster and respond more accurately. Furthermore, connecting Security Hub to automation response systems using something like AWS Lambda or AWS Systems Manager Automation, several rapid mitigations can be automated versus needing to involve human resources at all [3] [4].

VPC Flow Logs add additional context to threat detection, since they will contain IP traffic metadata from network interface(s) within a telecom deployment's VPC. This metadata can help analysts identify unexpected spikes in traffic, port scans, and any data exfiltration activity. A good example would be if a telecom application subnet were to show a heavy amount of rejected outbound connections might indicate that either malware beaconing is occurring on the subnet, or that a botnet (and compromised machines) are attempting to connect to external command-and-control servers. Also, VPC Flow Logs can help when used alongside Amazon CloudWatch Logs and CloudWatch Logs Insights. In conjunction, security teams can query and analyze the patterns from VPC Flow logs and CloudWatch Logs, which can be built into behavior-based detection [2] [5].

Alongside visibility at the infrastructure layer, AWS also provides host-based threat detection through Amazon Inspector, which operates automated security assessments of EC2 instances and container images. This is especially pertinent to telecom where virtualized network functions (VNFs) and containerized microservices are displacing legacy hardware appliances at a rapid pace. Inspector identifies software vulnerabilities, discovery of sensitive ports, and a deviation from security best practices. These findings are paramount for maintaining continuous compliance with standards designed for this purpose, such as CIS Benchmarks, and PCI DSS - of which both serve as references within telecom regulatory frameworks [1] [6].

To further increase detection capabilities, AWS also provides traffic mirroring, through Elastic Network Interfaces (ENIs) - which allows security tools to capture all packet data for in-depth analysis. The collected data could feed advanced intrusion detection systems (IDS), or forensic platforms more commonly used with telecom workloads that involve signaling and media streams. As the data is collected and security models are created, most likely with leveraging artificial intelligence capabilities offered by services such as Amazon SageMaker or Amazon Lookout, operators can make predictive models that anticipate and potentially thwart security incidents before they occur, or deter the impact of lessons learned from behavior, and current or past anomalous behavior [4] [6].

In the end, threat detection in AWS must be resilient in the lifecycle of telecom infrastructure; from deployment and monitoring to incident response. Implementing and operationalizing a strategy relies on the creation of telemetry; applying alert correlation; and eliciting an intelligent response workflow. Considering that the telecom sector is adopting cloud native architecture, the security of telecom services by implementing versatile detection capabilities using AWS is paramount in general not only for security but also for operational continuity and assurance to regulators [2] [3].

5. Automated Compliance Implementation with AWS Tools

In a cloud-native telecom environment, compliance can no longer be achieved as a milestone determined previously by scheduled audits or periodic reporting. Compliance will need to be embedded into the infrastructure and become an ongoing process that is automated to validate configurations, monitor activities, and enforce policies across the lifecycles of workloads. Telecom operations are inherently complex with aspects of the business related to voice, data, media, billing, and subscriber management. In addition, compliance will need to be multilayered as many services will require a scalable compliance framework that is horizontally integrated across accounts, services, and regions. Finally, telecom organizations will need enhanced compliance enforcement and ongoing monitoring to retain real-time patterns of visibility and actionable governance with the compliance framework. AWS provides a powerful set of capabilities that empower telecom operators to create their automated compliance pipelines to meet both internal business governance requirements and external regulatory requirements [1] [2].

Since compliance will become an ongoing and automated process, a successful compliance program must include services that provide adequate time for identifying and remediating any account, service, or region against a compliance violation. One of the key services in a compliance framework will be AWS Config. AWS Config enables organizations to continuously evaluate, assess, and audit the configurations of AWS resources. AWS Config will compare the real-time configurations in the consumed environment with pre-stated rules regarding configuration configurations. A key benefit of AWS Config will be to detect compliance violations immediately, such as open S3 buckets, misconfigured IAM roles, and encryptions that had been disabled. Identifying compliance violations is critical in a telecom environment where small compliance violations can expose data at large proportions, or even violate regulations. AWS Config integrates directly to AWS Systems Manager so that organizations can also not only detect a non-compliance violation but also automatically remediate a compliance violation [2] [3].

Together, AWS Control Tower establishes a landing zone for standard control over governance across accounts. This is often referred to as an compliance enforcment as this service tracks the relevant user activity in all of your AWS accounts in support for implementing Service Control Policies (SCPs), Declarative guardrails, and a baseline for accounts. While many telecom companies have a federated model and multiple business units or services divisions, Control Tower enables a centerally managed and yert federated governance model. This model is an ongoing support for modified governance implementation for region specific compliances (i.e., GDPR in Europe or CCPA in California). The AWS Control Tower landing zone model can force a constraints for compliance consistently across the global cloud footprint of an organization [4] [6].

AWS CloudTrail provides another log, as it creates logs of every API call across services. These logs represents a record in support of forensic investigation and incident response as well as compliance procedures for audits. Further, when combined with another services like Amazon S3 or utilize AWS Lake Formation, CloudTrail records can be ingested to a "consumptive" data lake. These records can then be queried in parallel across the enormous indexed/recorded repository of event data using Amazon Athena services or running against an OpenSearch service instance. Therefore, compliance team for a telecom company could run queries against billions of record of possible events to find the matters of use violations or provide historical trending against compliance possible events [1] [4].

Using AWS Audit Manager simplifies evidence gathering and reporting even more. AWS Audit Manager maps AWS usage data to control frameworks like NIST 800-53, ISO 27001, and CIS Controls to generate assessment reports for you. In a telecom context, there can be compliance documentation for multiple regulatory bodies, so the implementation of automation with Audit Manager minimizes the manual effort required and improves accuracy [3] [5].

Table 1 provides a summary of how AWS services map to each of the steps in a typical telecom compliance pipeline and the level of automation for each step:

Table 1: AWS Compliance Automation Mapping for Telecom Workloads

Compliance Stage	AWS Service	Function in Telecom Compliance
Configuration Monitoring	AWS Config	Real-time detection of policy violations and misconfigurations
Policy Enforcement	AWS Control Tower	Preconfigured guardrails, SCPs, and multi-account governance
Activity Auditing	AWS CloudTrail	Logs API calls for traceability and audit reporting
Evidence Management	AWS Audit Manager	Generates audit-ready reports aligned to standard compliance frameworks
Data Storage and Analytics	Amazon S3, Athena, OpenSearch	Centralized analysis of compliance logs and historical patterns

Automating compliance will ensure regulatory compliance and provide operational efficiencies. Automation replaces manual processes in audit preparation by eliminating human error and validation time. Most importantly, automation promotes agility – allowing telecoms to develop and roll out services at speed, while not losing sight of compliance. As cloud environments expand in scale and diversity, AWS will ensure that automated compliance remains a pillar of secure, efficient, and sustainable telecom operations [2] [5].

6. Best Practices for Continuous Monitoring and Visibility

Continuous monitoring and visibility are core principles for securing cloud-based telecom environments. Unlike traditional infrastructure where the security of periodic assessments might be enough, the cloud — particularly when supporting essential telecom services — will always be undergoing continuous change. Resources are continuously provisioned and de-provisioned, networks are dynamic with virtually no boundary, and access permissions are designed to be malleable as workloads are constantly scaling. These conditions necessitate a “continuous” visibility approach in real-time, across applications, systems, networks, and data layers. AWS has constructed a series of services to address this core need, to ensure that telecom operators can attain a high degree of situational awareness and enforce a security posture at scale [1] [3].

Centralized log management is a key feature of ongoing monitoring in AWS, with AWS CloudTrail providing a full history of every API call made in the environment. CloudTrail provides a comprehensive audit history to after-the-fact review of user and service activity. This capability is even more necessary in telecom, where an API call made without authorization is usually indicative of a compromise to control planes that manage subscriber identities and network configurations. CloudTrail logs can be streamed to Amazon S3 then analyzed using analytics services such as Amazon Athena or Amazon OpenSearch. This allows security and compliance teams to perform real time queries, discover anomalous patterns, or conduct an investigation without the dependence on batch reports or requirements to send notifications after delays [2] [4].

Further complementing this is Amazon CloudWatch which provides metrics and log analytics for resource utilization, system performance and application-level events. In telecom environments, it is usually a requirement to support continuous high availability or service continuity, and CloudWatch allows proactive monitoring of CPU spikes, memory and traffic patterns that could indicate misconfigurations or an impending failure. CloudWatch's metrics also allow links to automation tools through CloudWatch Alarms and AWS Lambda, automating plans on compromise (for example terminate compromised instances) or to scale on traffic thresholds, allowing for resilient and secure systems [3] [4].

Behavioral monitoring is another key practice, especially around insider threats, account hijacking, and compromised credentials. Amazon GuardDuty provides more visibility by making sense of the CloudTrail logs the organization's actions, the DNS queries, and the VPC Flow Logs to identify concerning behaviors, like attempts to escalate privileges or access from suspect IP ranges. GuardDuty even uses threat intelligence feeds to correlate telemetry in order to leverage enriched alerts; it gives more than the straight log data, it provides information for the required context for investigations or remediations. In the context of telecom deployments, it is impossible to over-estimate the value of being able to point out behavior that emanating from a compromised privileged account. This is especially true, since the compromise of a single privileged account can spark a chain reaction that can either disrupt services or become the risks of a data breach [2] [5].

Centralizing this visibility across the accounts and regions is provided by AWS Security Hub. AWS Security Hub collects findings from GuardDuty, Inspector, Macie, and third-party tools, and presents Security Hub to provide a single view to provide security operations so the analyst can prioritize the threats and response consideration based on severity, compliance, and criticality of the resources. This method of contextual analysis allows a holistic view is invaluable to the telecom industry for identifying threats that share an environment with other organizations while being located in different geographic locations, as well as in a multitenancy allows centralized view amidst geographically dispersed infrastructures. Coupling Security Hub with automated remediation tools offers telecom organizations the ability to create automated response workflows that remediates while igniting prompt; it colludes ICT remediate responses [3] [6].

In addition to the technical instrumentation noted above, continuous monitoring in telecommunications relied to a significant degree on defined operational procedures and clear escalation processes. Continuous monitoring uses AWS services like AWS Systems Manager and AWS Config Rules to support operational maturity, which includes remediation runbooks, inventory visibility, and conditions that enforce compliance with configuration policies. These systems allow an organization to completely understand what they are monitoring, not just the detection of unknowns, but also reinforce consistency, standardization, and quick response to protect the practice of continuous monitoring practice across all cloud service provider assets [1] [5].

Continuous monitoring helps telecom sectors stay ahead of threats, improve security posture, compliance, and operational efficiency. Continuous monitoring processes combine existing AWS logging policies, metric events, behavioral analytics, and centralized dashboards across the organization so they can detect threats early, respond quickly, and comply with industry standards. As telecom networks increasingly rely on cloud services, and customer-facing services depend on digital services, the systematic view, insight, and continuously monitoring of consciousness is not an optional activity, but should be amongst the most important planning to secure and resilient telecommunications strategy [2] [4].

7. Case Study: Implementing Telecom Security with AWS

In order to see how the perspectives of automated compliance and threat detection can be applied in a real-world telecom scenario, it helps to study organizations that have utilized various AWS services to secure their organizations. One example, is a large telecommunications operator that adopted AWS Control Tower, AWS Config, and GuardDuty to centralize governance and improvement in threat detection across many regions/accounts. This not only strengthened the overall security posture of the organization, but also provided the organization with faster audits whilst reducing the manual compliance effort, which is a key consideration in the heavily regulated telecommunications environment [1] [2].

The organization started with the AWS Control Tower to establish its cloud landing zone. Control Tower provided the telecom operator a common governance model with auditing or Hypothetical - development, staging, and production environments. Service Control Policies (SCP) were required to implement the governance model to prevent access to least-privilege access and prevent actions like disabling logging, or disabling parts of the network without authorization. Centralized policy enforcement practically eliminated the risk of configuration drift, a likely contributor to vulnerabilities in environments of scale like telecom. The pre-packaged guardrails that came with Control Tower clearly mapped to industry standards. The telecom operator was able to establish a compliance-as-design methodology from the very start [2] [4].

To complete the solution, AWS Config was also inserted to provide continuous monitoring and assessment of the configurations of resources. The company established compliance rules guided by the CIS AWS Foundations Benchmark ensuring that critical configurations from encryption at rest and secure access policies to multi-factor authentication were enforced on all accounts, and AWS Config provided near real-time notifications when there were deviations, and it executed automatic remediation actions via AWS Systems Manager. Given that the organization had implemented an automated approach, it was no longer reliant on periodic checks; therefore, it could now be audit-ready at all times. For a telco company subject to regulatory frameworks such as ISO 27001 and national telecom data retention legislation, the automation provided assurances in terms of accuracy and operational performance [1] [3].

The organization expanded their threat detection function with the use of Amazon GuardDuty. GuardDuty ingested several logs, including VPC Flow Logs, AWS CloudTrail Logs, and DNS query logs, to identify anomalous behaviours that raised concern about compromised instances or unauthorized data exfiltration. For example - one of the interesting features of GuardDuty involves it identifying EC2 Instances that are communicating with a known bad IP address . When GuardDuty identified this and the automatic response was triggered to quarantine the instance using AWS Lambda, the incident had a significant impact on the company's mean time to detect (MTDD) and mean time to respond (MTTR) metrics. These metrics were important to the company for protecting its telecom network and preserving customer trust [2] [5].

Additionally, the company was using AWS Security Hub, which found a way to capture Threat Detection Findings from GuardDuty, Inspector and its third-party SIEM tools into one single view. The security operations team could simply identify any incidents of critical severity and incidents with a compliance impact, of which, an incident related to open S3 buckets in a critical billing environment was reviewed and escalated for remediation immediately. The Company's compliance status was further supported by the AWS Audit Manager, who retrieved and logged evidence of the unresolved incidents, which would help the company with future audits and regulatory reviews. The AWS provided end-to-end and automated threat detection and compliance loop was an example of successfully embedding security into the security fabric of cloud-native deployments for telecoms [3] [6].

This case study showcased how AWS is helping telecommunications companies evolve from reactive security and static compliance. By encapsulating governance frameworks, threat detection, monitoring, and automation into a singular approach, telecommunications organizations could build or leverage solid, scalable and audit-ready cloud production environments. As the telecommunications industry continues to increase its adoption of the cloud, such implementation models could serve as a design model for other organizations facing similar issues [1] [2].

8. Conclusion and Future Directions

The telecommunications sector currently finds itself at a monumental crossroads, driven by blurring paradigm shifts associated with exponential digital transformation and increasingly complex threat conditions. As telecommunications players migrate to cloud-native technology stacks, especially on AWS, it is critical to implement integrated, automated, and intelligent security frameworks. Instead of responding to adverse outcomes through centralized threat detection and compliance management processes that our legacy environments often relied on that were often manual, siloed, and reactive in nature, telecommunication organizations must innovate and leverage the capabilities of AWS to not only meet, but exceed the security and compliance requirements of telecommunications organizations in the digital world.

Automated compliance through AWS services such as AWS Config, Audit Manager, and Control Tower allows telecom service providers to sustainably and continuously demonstrate compliance with world-wide regulations like ISO 27001, NIST, and GDPR. By injecting compliance checks into infrastructure deployments and by providing automated remediation workflows, organizations can achieve a continuous state of compliance, which is a significant cultural shift away from audit readiness, in that it decreases operational overhead and increases accuracy and agility. The ability to generate audit ready evidence, its uniform adherence to policy across distributed settings means that telecom operators can go beyond demonstrating compliant behavior toward resilient behavior in the face of legal and regulatory obligations which are in a constant state of evolution, given the pace of change in the world today.

With respect to threat detection, AWS services such as GuardDuty, Security Hub, Cloud trail, and VPC Flow logs give telecom operators both deep and continuous visibility into their cloud operations allowing the detection of—at near-real time—anomalous behavior affecting their system, unauthorized access into their systems, and breaches into their cloud systems. The combination of behavioral analytics, AI-enhanced threat intelligence, and automated responses all contribute to transforming security operations from a purely reactive function into fully-blown proactive functions. For telecom networks, where service uptime, customer trust, and data privacy are paramount, these capabilities are critical for not only sustaining operational integrity, but also for securing customers' trust.

The practical application of these principles, as seen in the case study, bolsters the legitimacy of AWS as an all-in-one platform for secure telecom operations. AWS is a one-stop shop for private & public network operations, allowing a user to manage network traffic and users, to monitor behavior of applications, and to properly enforce governance across accounts. AWS is a singular ecosystem able to fulfill the promise of end-to-end security and compliance that can scale out with your business, grow in response to new threats, and innovate with the rapid pace of technological change.

In the future, the enhancement of AWS security services with artificial intelligence and machine learning capabilities opens up new opportunities for telecom operators. There is a suite of services including Amazon Lookout for Metrics and Amazon SageMaker, that can be trained with historical threat patterns, operational data and also become capable of predicting threats with automatic updates to adjust or optimize security on behalf of the operator. Also, with the growth of support for edge computing and 5G, AWS solutions for 5G and edge computing solutions like AWS Wavelength allows telecom to create new secure, low-latency telecommunication services deployed as close to the end user as possible.

Ultimately, AWS supplies telecom operators with the infrastructure as well as sophisticated tools required to build trusted, compliant and future-proof cloud environments. The shift toward automation, continuous monitoring and smart threat detection is no longer an option. It is the new way to do business. As telecom operators migrate further into the transformation made possible by automation, those operators who will deliver services trusted by consumers and regulators alike, will be those who will

embrace automation, security and compliance as the framework to do so. The future of telecom in cloud as it converges with technology, security and automation has possibilities that are safe and attainable.

9. References

[1] Amazon Web Services. (2025). *Enhancing telecom security with AWS*. AWS Security Blog. https://aws.amazon.com/blogs/security/enhancing-telecom-security-with-aws/

[2] Szili, D. (2019). *Building a threat detection strategy in AWS*. SANS Institute & AWS Marketplace. https://pages.awscloud.com/rs/112-TZM-766/images/Threat%20Detection_SANS%20and%20AWS%20Marketplace%20whitepaper.pdf

[3] Amazon Web Services. (2024). *Overview of Amazon Web Services*. AWS Whitepaper. https://docs.aws.amazon.com/pdfs/whitepapers/latest/aws-overview/aws-overview.pdf#security-services

[4] Shackleford, D., Butler, J. M., & Szili, D. (2019). *Threat Detection Best Practices in AWS*. SANS Institute. https://d1.awsstatic.com/Marketplace/solutions-center/downloads/Threat-detection-AWS-Marketplace-eBook.pdf

[5] Kim, F., Shackleford, D., Szili, D., & Pescatore, J. (2019). *Practical Guide to Security in the AWS Cloud*. https://tinyurl.com/58k5feab

[6] Woo, N., Robinson, M., & Woo, R. (2025). *Key Governance, Risk, and Compliance Sessions at re:Inforce 2025*. AWS Cloud Operations Blog. https://aws.amazon.com/blogs/mt/key-governance-risk-and-compliance-sessions-at-reinforce-2025/