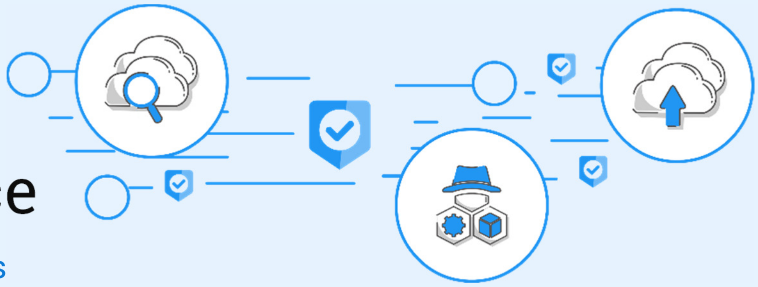
Case Study

CloudFabrix

AWS Security Conformance & Compliance

Network | Identity | Storage | Regulations | IT Controls



Business Profile

Energy Firm Tier-1 (US Based)	**$50B+** Revenue
1500+ AWS Resources	**250+** Applications

Business Impact

- Delayed go-live date by 6-months
- Lost revenue due to limited ability to rapidly onboard new customers
- Increased overall IT costs due to manual operations, onboarding & auditing
- Increased operational overhead
- Credibility and brand at risk due to compliance violations

Technical Challenges

- Complex environment with multiple VPCs, subnets and regions
- Users with varying IAM access levels
- Open S3 buckets, obsolete resources.
- Regulations require keeping tabs on many data points and configurations
- No standardization or conventions
- Increased attack surface. No automation

Business Context

A leading US based energy firm (customer) has recently migrated most of their production workloads to AWS and is concerned about ongoing security conformance and compliance. Specifically, customer wanted to ensure:

- 100% Security Conformance and compliance to industry regulations
- Extend corporate specific IT controls to AWS workloads
- Network Isolation and Inter VPC traffic go through their preferred firewall
- Continuous Security Group monitoring and flow log analysis for threat detection
- Conformance to CIS benchmarks and AWS best practices
- Optimal utilization of resources and reduce unused/under-utilized resources

Customer is in need of an effective Governance and Automation that establishes security posture, provides confidence and robust security controls similar to on-premises and further offers automation to reduce AWS operations spend.

Solution

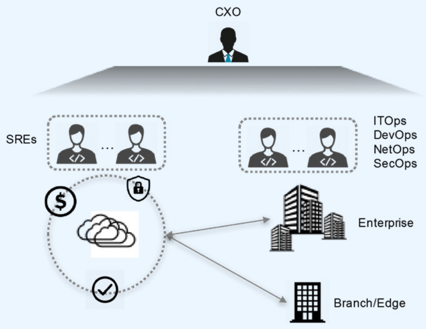
cfxHorizons provides comprehensive AWS Security Conformance and Automation solution. Solution consist of three major components: 1) Multi-source data ingestion & monitoring 2) Real-time insights and intelligence and 3) Automation to correct and remediate. cfxHorizons performed instantaneous assessment and established security baseline and presented list of issues/gaps along with recommendations. Under the hood, cfxHorizons continuously gathered data from multiple sources, cloud services, applications and performed advanced analytics with various rules and compliance checks. With this customer achieved:

- Clear and objective view of current security & compliance posture
- Uncovered hidden security and network isolation issues
- Identified old, unused and under-utilized snapshots, VMs, S3 buckets
- Got to know list of problems and issues with their cloud implementation
- Was presented with list of recommendations to become more secure & compliant

By implementing the recommendations and with ongoing governance, customer realized **98% increase** in security conformance & compliance.

Key Benefits

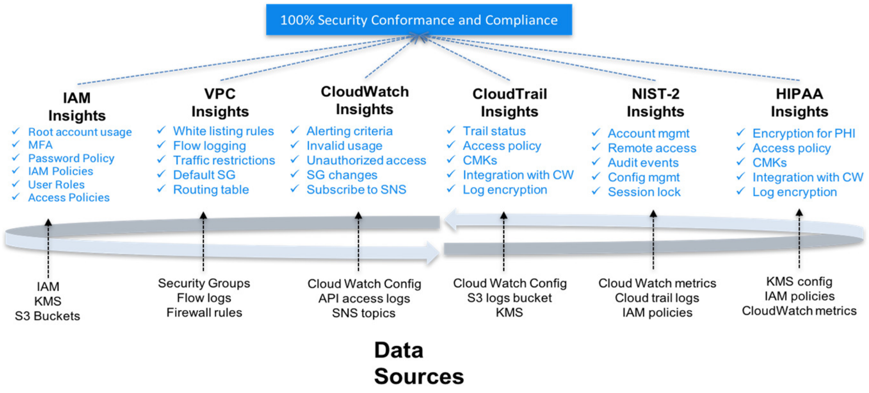
98%	70%	80%
Increase in Security Conformance	Increase in Regulatory Compliance	Unplanned Changes Contained & Audited



> *"Our AWS environment was growing quite large and complex, and frankly getting out of control. Our spend was skyrocketing, and not to mention any inherent security risks and compliance issues that we may not be aware of. We wanted to step back, take a fresh look and identify gaps in our environment to initiate overhaul process.*
>
> *cfxHorizons governance instantly helped us by highlighting security issues/gaps in our environment, along with suggested actions to fix the issues. We incorporated majority of the feedback into our CloudOps processes. In addition, the ongoing governance solution enabled us to effectively keep tabs on our environment all the time"*
>
> **-- Sr. Director, Cloud and IT Ops**

Success Path to 100% Security Conformance and Compliance

1) Define & Monitor: Customer's business objective i.e Outcome of having 100% Security Conformance and Compliance is selected to steer data source selection, Rules and Insights that will be deployed to measure, track and make underlying systems meet the objective. Analytics cover various operational dimensions like Security, **CIS Compliance, PCI DSS Compliance**, Configuration and key AWS service dimensions like VPC, IAM, Security, EC2, S3 etc. This Outcome can also be customized or extended to include any specific **corporate IT/Security controls** or policies.


100% Security Conformance and Compliance

IAM Insights
✓ Root account usage
✓ MFA
✓ Password Policy
✓ IAM Policies
✓ User Roles
✓ Access Policies

VPC Insights
✓ White listing rules
✓ Flow logging
✓ Traffic restrictions
✓ Default SG
✓ Routing table

CloudWatch Insights
✓ Alerting criteria
✓ Invalid usage
✓ Unauthorized access
✓ SG changes
✓ Subscribe to SNS

CloudTrail Insights
✓ Trail status
✓ Access policy
✓ CMKs
✓ Integration with CW
✓ Log encryption

NIST-2 Insights
✓ Account mgmt
✓ Remote access
✓ Audit events
✓ Config mgmt
✓ Session lock

HIPAA Insights
✓ Encryption for PHI
✓ Access policy
✓ CMKs
✓ Integration with CW
✓ Log encryption

IAM
KMS
S3 Buckets

Security Groups
Flow logs
Firewall rules

Cloud Watch Config
API access logs
SNS topics

Cloud Watch Config
S3 logs bucket
KMS

Cloud Watch metrics
Cloud trail logs
IAM policies

KMS config
IAM policies
CloudWatch metrics

Data Sources

cfxHorizons then collects **data** and **monitors** configurational, log, audit and event data from multiple key AWS services and resources and feeds the data into analytics engine. cfxHorizons has **native connectors to all AWS services** to programmatically gather, model and analyze all key data required for auditing and continuously governing target AWS environment. Access of data happens through customer provided read-only 'Security Audit' IAM role and the data collection and retention interval can be changed per needs. cfxHorizons also has extensible **data ingestion** architecture to feed data from any external business or IT systems that contain data relevant for governance/assessment.

2) Analyze & Govern: After data collection and monitoring, cfxHorizons governs AWS environment and provides overall **Governance Index** for the entire environment, which serves like a **score card**. Score ranges between 0 (worst) to 100 (best). Drill down analytics and reports allow reviewing **conformance/compliance per operational dimension** or AWS service or resource. Issues report provides detailed **list of rule violations**, offending resources and recommendations to correct the issues. Insights cover key areas like:

IAM
Root account, MFA, password policy, access policy, privileges, and Key rotation.

VPC
Security groups, subnets, route tables, white listing, traffic restrictions, flow logs, transit VPCs

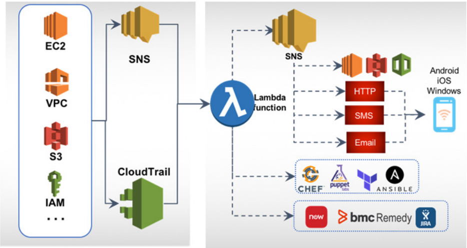
CloudWatch/Trail
Enablement status, log file validation, encryption, access checks, change logging etc.

EC2 and S3
Open buckets, non-standard AMIs, tags …

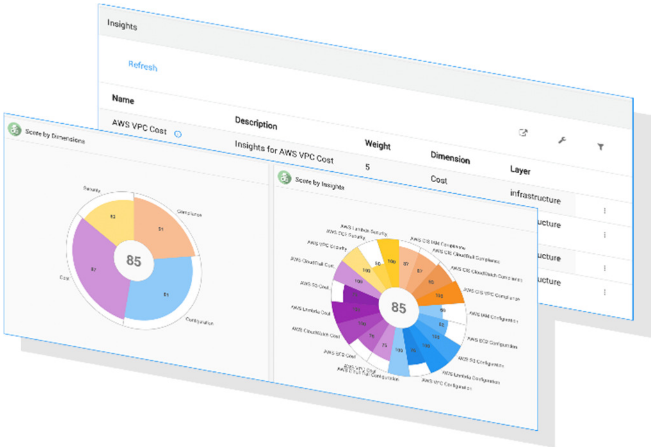
Cost
Unused/under-utilized resources, snapshots …

Compliance
CIS, PCI Dss, NIST, HIPAA etc.

3) Automate & Remediate: cfxHorizons utilizes multi-pronged automation approach, where it integrates with popular **orchestration systems**, like Puppet, Chef, Terraform etc., **native AWS services** like CloudTrail, SNS, Lambda and ticketing management systems, like ServiceNow, Remedy etc..



cfxHorizons automatically deployed **Lambda** functions that listen to key changes/events in customer's AWS environment (Ex: Flow logs, excessive traffic denials, VPC, security groups, too permissive IAM users etc.). Lambda function triggers a config operation, CloudFormation template, trigger a workflow or create a ticket- which all revert incorrect configs, auto-correct or terminate resources. cfxHorizons also automatically **creates SNS topics** that can be further piped upstream to various notification mechanisms like Slack, Twilio, PagerDuty or integrated with corporate IT messaging/control systems.



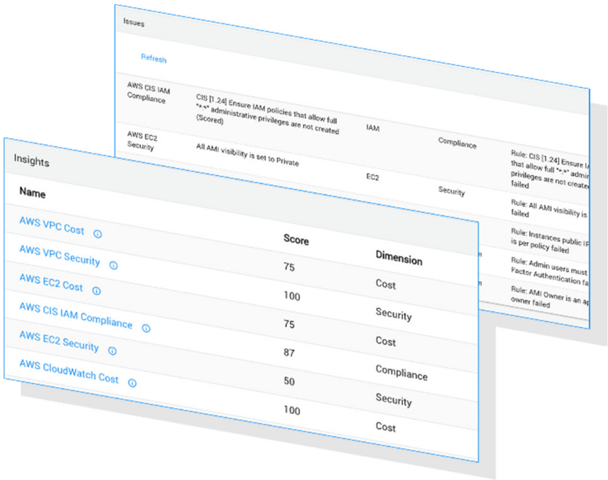
Insights

Refresh

Name	Description	Weight	Dimension	Layer
AWS VPC Cost	Insights for AWS VPC Cost	5	Cost	infrastructure
				ucture
				ucture
				ucture

Score by Dimensions

Score by Insights



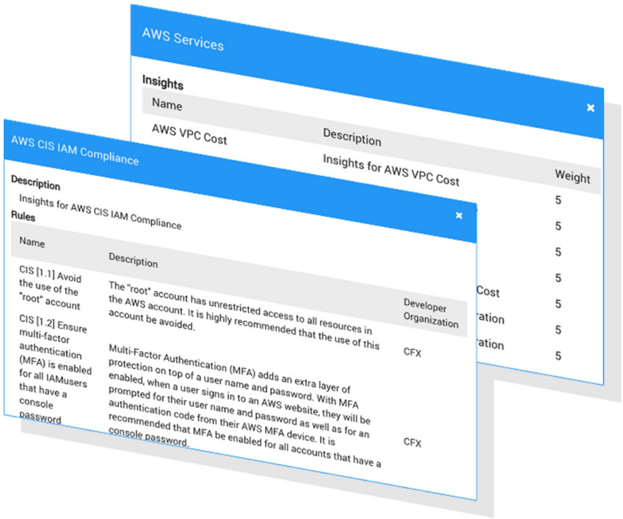
Issues

Refresh

AWS CIS IAM Compliance	CIS [1.24] Ensure IAM policies that allow full "*:*" administrative privileges are not created (Scored)	IAM	Compliance	Rule: CIS [1.24] Ensure I that allow full "*:*" admir privileges are not create failed
AWS EC2 Security	All AMI visibility is set to Private	EC2	Security	Rule: All AMI visibility is failed
				Rule: Instances public IP is per policy failed
				Rule: Admin users must Factor Authentication fa
				Rule: AMI Owner is an ap owner failed

Insights

Name	Score	Dimension
AWS VPC Cost ⓘ	75	Cost
AWS VPC Security ⓘ	100	Security
AWS EC2 Cost ⓘ	75	Cost
AWS CIS IAM Compliance ⓘ	87	Compliance
AWS EC2 Security ⓘ	50	Security
AWS CloudWatch Cost ⓘ	100	Cost



AWS Services ✖

Insights

Name	Description	Weight
AWS VPC Cost	Insights for AWS VPC Cost	5
		5
		5
	Cost	5
	ation	5
	ation	5
		5

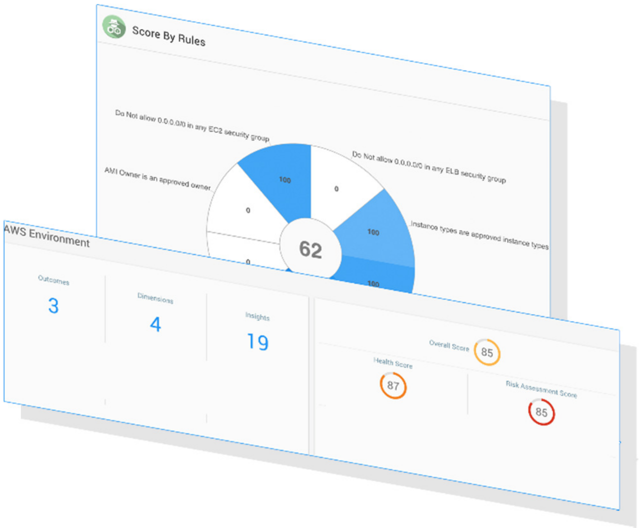
AWS CIS IAM Compliance ✖

Description

Insights for AWS CIS IAM Compliance

Rules

Name	Description	Developer Organization
CIS [1.1] Avoid the use of the "root" account	The "root" account has unrestricted access to all resources in the AWS account. It is highly recommended that the use of this account be avoided.	CFX
CIS [1.2] Ensure multi-factor authentication (MFA) is enabled for all IAMusers that have a console password	Multi-Factor Authentication (MFA) adds an extra layer of protection on top of a user name and password. With MFA enabled, when a user signs in to an AWS website, they will be prompted for their user name and password as well as for an authentication code from their AWS MFA device. It is recommended that MFA be enabled for all accounts that have a console password.	CFX



Score By Rules

Do Not allow 0.0.0.0/0 in any EC2 security group
Do Not allow 0.0.0.0/0 in any ELB security group
AMI Owner is an approved owner
Instance types are approved instance types
100
0
0
100
0
100
62

AWS Environment

Outcomes	Dimensions	Insights
3	4	19

Overall Score 85

Health Score 87

Risk Assessment Score 85