Governance & Compliance

Steven Moran
TECHNICAL INSTRUCTOR

Are We There yet?

Traffic Control

...let in desired traffic and drop the rest?

Traffic Protection

...secure appropriate traffic sessions?

Traffic Awareness

...create automated monitoring and response procedures?

...implement procedures for responding to significant events?

What else is there?

Almost There...

How can we actually verify that our environment is configured according to plan?

How can we ensure that our environment won't be inappropriately modified?

The Admin Attains Wholeness in the Correct Governance of the Services

Governance = Control

Establishing systems to ensure that organizations are following the "rules".

Compliance = Proof

Demonstrating that organizations are, in fact, following the "rules".

Who Makes the Rules?

- Organizations establish procedures to:
  - Ensure objectives are efficiently met
  - Ensure risks are identified and mitigated
- Nations establish laws to protect the interest of citizens.

Through 2025, 99% of Cloud Security Failures Will Be the Customer's Fault

"CIOs can combat this by implementing and enforcing policies on cloud ownership, responsibility, and risk acceptance. They should also be sure to follow a life cycle approach to cloud governance and put in place central management and monitoring plans to cover the inherent complexity of multicloud use."

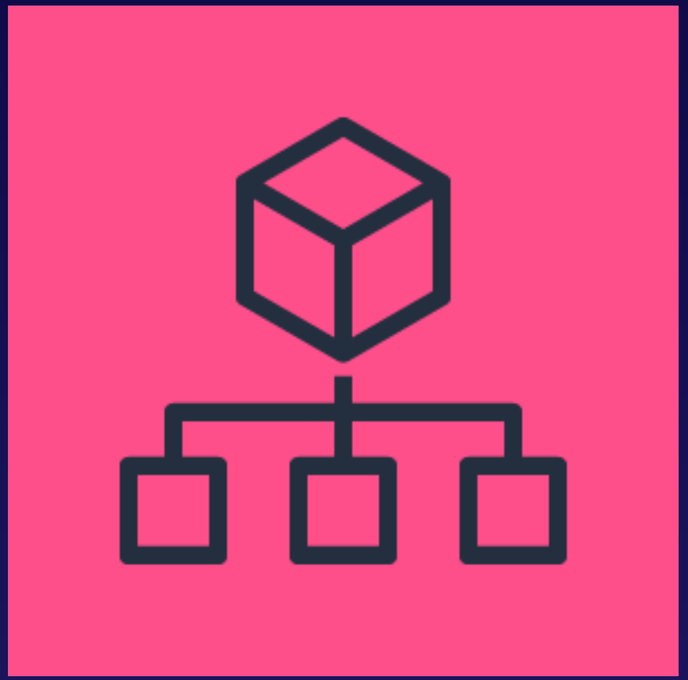
Gartner, Inc.
"Is the Cloud Secure?"

AWS Identity and Access Management

- Access control to AWS services.
- All AWS API calls must be authenticated and authorized.

AWS Organizations

- Allows centralized management of multiple AWS accounts.
- Apply Service Control Policies (SCPs) onto child accounts to define the maximum applicable IAM permissions.
  - Child account principals may only perform actions allowed by both AWS account IAM policies *and* Organizational SCPs.

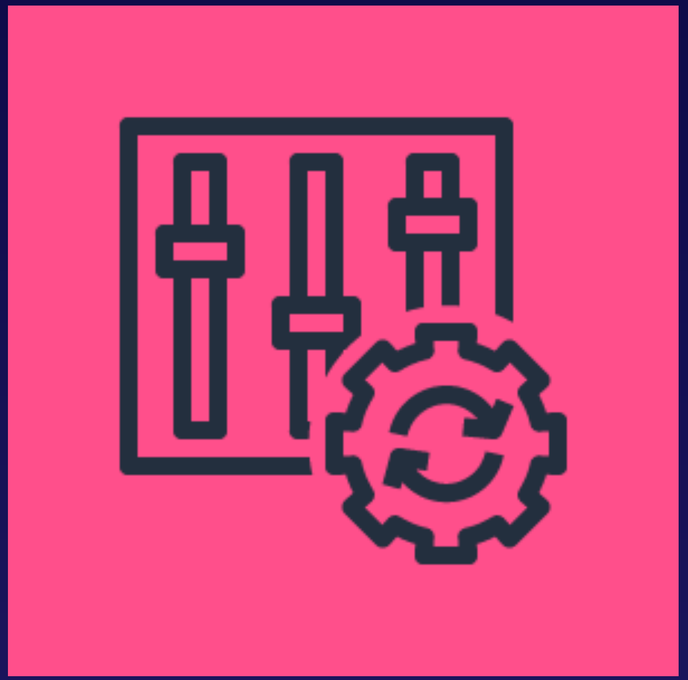


AWS CloudTrail

- AWS API-call auditing service.
- Audit trails from multiple accounts can be sent to a single S3 bucket.
- Integrated with CloudWatch Events.
- Does NOT monitor network traffic.

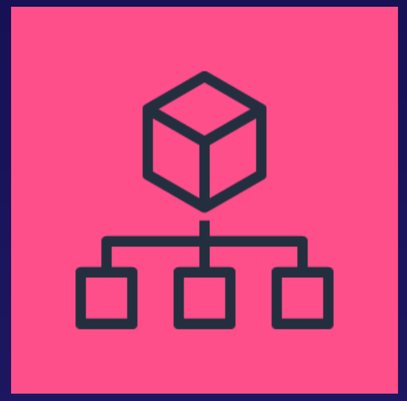
AWS Config

- Monitors the configuration of your AWS resources.
- Tracks configuration changes.
- Applies remediation rules.
- Integrates with CloudTrail.



How Do These Services Help You Govern?

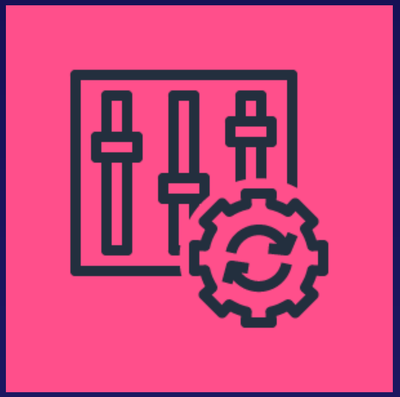
- Follow IAM best practices:
  - Secure the root user
  - Use multi-factor authentication
  - Authorize roles instead of users
  - Grant least privilege



- Enforce organizational policies with AWS Organization SCPs.

How Do These Services Help You Govern?

- Automate responses to audited API calls using CloudWatch Events.
- Automate configuration change remediation with Config rules.
- Investigate the cause of events to determine follow-up actions.



How Do These Services Help You Govern?

- Require that common resources be created using CloudFormation templates.
  - CF authorized to manage resources via IAM role.
  - Users only given permission to use CF templates.

AWS Service Catalog

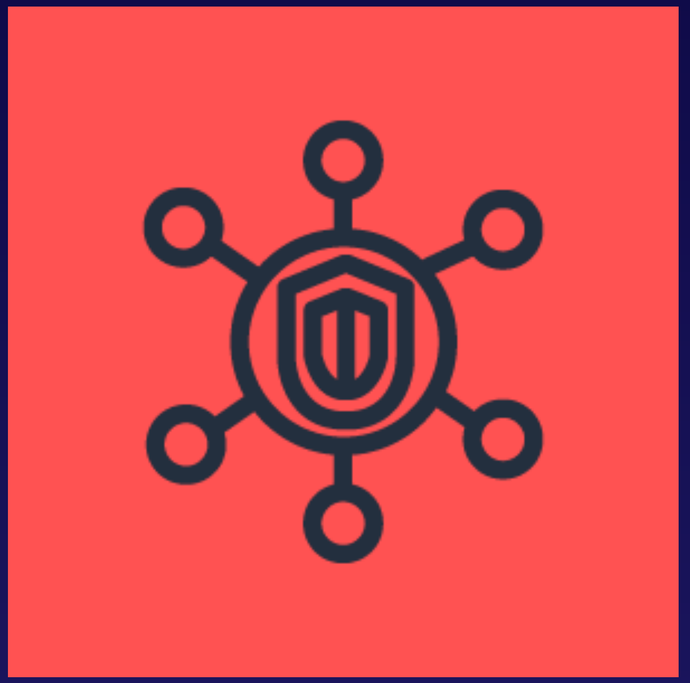
- Controls and standardizes deployment of AWS services.
- Catalog administrators define products using CloudFormation templates.
- End users may deploy products that they have been granted access to.

AWS Firewall Manager

- Provides AWS Organizations an interface to centrally enforce deployment of:
  - WAF ACLs
  - AWS Shield Advanced protection policies
  - VPC security groups
- Reports findings to AWS Security Hub (if enabled).

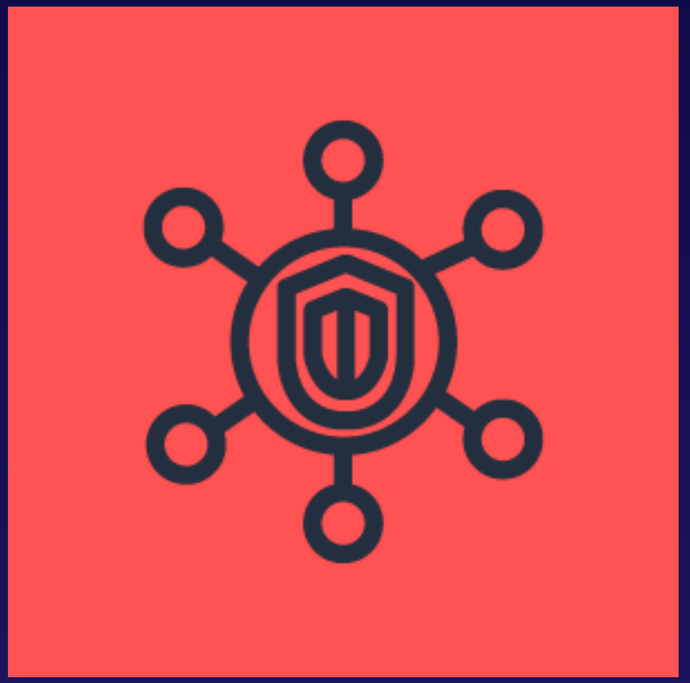
AWS Security Hub

- Centralized security and compliance monitoring service.
- Gathers data from AWS and supported third-party products.
- Consolidates information across multiple accounts.
- Runs account configuration and compliance checks.



AWS Security Hub

- Imports findings from Amazon GuardDuty and Amazon Inspector.
- Receives findings from AWS Firewall Manager:
  - WAF policy non-compliance
  - AWS Shield Advanced not protecting resources
  - AWS Shield Advanced identifies an attack
  - VPC Security Group configuration issues
- Integrates with CloudWatch Events.



Fast Takeaways

Know what your compliance obligations are.

Leverage automated governance processes wherever possible.

Follow security best practices.