DATA SHEET

Cloud Security and Compliance for Federal Agencies

As Federal agencies migrate to cloud-based technologies, new and complex security and compliance challenges are being identified every day. In order to operate and maintain information systems, Federal agencies are required to comply with the guidelines and recommendations developed by the National Institute of Standards and Technology (NIST). These guidelines establish standards that address security controls for government information systems.

To meet these standards, Fugue identifies security and compliance violations in cloud infrastructure and ensure they are never repeated. Fugue helps to address the following NIST guidelines: Configuration Management (CM), Audit and Accountability (AU), Identification and Authentication (IA), Access Control (AC), and System and Communications Protection (SCP).

Configuration Management (CM)

Fugue's automated remediation feature reverts all unauthorized changes back to an original approval state for enforcement of configuration policy. While preventing unauthorized changes, Fugue also implements approved asset changes where proposed modifications go through a defined process. As part of this process, Fugue's "dry run" feature provides a preview of the changes that will be made to infrastructure before they are implemented.

BENEFITS

- Quickly identifies and automatically remediates policy violations to ensure compliance
- Provides detailed records for audits and accountability
- Enforces multi-factor authentication for non-privileged and privileged accounts
- Ensures only designated users can make allowable configuration changes

Audit and Accountability (AU)

Fugue provides detailed records of changes to cloud infrastructure for audits and accountability. The records include the type of change, when it occurred, where in the environment and to what specific resource, and who made the change. If the change was made through the organization’s official modification process, it will be deemed successful and implemented. If the change was unauthorized, then it will be marked as having failed and the infrastructure is restored to its original configuration ensuring compliance.

Fugue aggregates all cloud infrastructure audit records from multiple sources into a centralized location for easy viewing and access. The audit data is stored in an environment protected against tampering. All inbound network ports are closed and all traffic is encrypted and executed via Cloud Provider queueing service such as AWS Simple Queue Service (AWS SQS) or push notification services such as AWS Simple Notification Service (AWS SNS). To help with correlation across multiple log sources, Fugue can also send audit data to a centralized log aggregation system such as Splunk.

Identification and Authentication (IA)

Fugue enforces identification and authentication policies for users accessing cloud infrastructure. Fugue ensures that users have enabled multi-factor authentication for accessing cloud infrastructure services, both for privileged and non-privileged accounts. Fugue also enforces specific password policies for cloud infrastructure such as minimum password complexity, prohibiting password reuse for a certain number of generations, and disabling passwords after an inactivity period.

Access Control (AC)

Fugue’s RBAC features define rules specifying whether designated users can make configuration changes to cloud infrastructure. By design, an account is prohibited from taking any action unless a rule explicitly permits the action. Fugue also enforces various access control mechanisms such as the reporting of atypical account activity, encryption of remote access session traffic, and the routing of network access traffic through specific control points.

System and Communications Protection (SCP)

Fugue enforces controls that protect system network boundaries and enforce data encryption. For example, Fugue ensures that logging is enabled for resources such as load balancers and content delivery networks, and that inbound network traffic is prohibited for specific components. Also, Fugue requires that encryption be enabled for resources such as databases, storage buckets, logs, and server storage volumes.

Securing Your Infrastructure with Fugue

The NIST Framework provides federal agencies with guidelines and recommendations on how to protect and secure their networks and infrastructure. Fugue identifies and remediates cloud infrastructure risks. Fugue’s Conductor feature automates remediation of unathorized changes and provides an accurate view of all infrastructure components. Auditing of infrastructure changes is made simple with a centralized view of all audit records from aggregated sources. Fugue enforces specific identification and authentication policies such as multifactor authentication, and Fugue’s RBAC features ensure that any changes made to privileged accounts are made by approved users are authorized.

About Fugue

Fugue is a security and compliance solution that identifies and eliminates cloud risks. Our patented software automatically remediates misconfigurations and policy violations in near real time and ensures they are never repeated. With Fugue, cloud resources are always provisioned according to a single source of truth – and stay that way throughout the resources’ lifetime.