DATA SHEET

SOC 2 Compliance with Fugue

Developed by the AICPA, SOC 2 is designed to address how organizations should design systems of internal controls to address the security, availability, processing integrity, confidentiality, and privacy of customer data.

CC2.0: Communication and Information

The communications and information criteria of SOC 2 address how service organizations handle internal and external communication and information flows. CC2.1 states that “the entity obtains or generates and uses relevant, quality information to support the functioning of internal control.”

Services such as AWS CloudTrail and Azure Monitor log every API interaction, including which users are taking certain actions. For example, Fugue will check to ensure that CloudWatch log metric filters and alarms are configured properly to alert users to denied connections to CloudFront distributions so users can investigate anomalous traffic.

CC5.0: Control Activities

The control activities criteria of SOC 2 deals with how service organization control activities account for risk management and technology. CC5.2 states that “the entity also selects and develops general control activities over technology to support the achievement of objectives.” This includes that management develops control activities to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity’s assets from external threats.

Access should be granted based on the principle of least privileges necessary to perform job responsibilities. For example, Fugue detects IAM policies that grant full “*:*” administrative privileges and marks them as noncompliant. IAM policies should start with a minimum set of permissions and include more as needed rather than starting with full administrative privileges. The same access principles apply to cloud resources such as SQS queues and S3 buckets.

CRITERIA FOR SOC 2 AUDITS:

The only criteria that are required for SOC 2 audits are those pertaining to security.

- **CC2.0: Communication and Information -** how organizations handle internal and external communication
- **CC5.0: Control Activities -** how organization control activities account for risk management and technology
- **CC 6.0: Logical and Physical Access Controls -** how organization controls implement logical access to IT systems/ credentials to detect and prevent unauthorized access
- **CC 7.0: System Operations -** how organization controls monitor systems for potential anomalies, events and configuration changes
- **CC 8.0: Change Management -** how organizations develop and implement change management approaches to infrastructure, data, software, and policies

CC 6.0: Logical and Physical Access Controls

The logical and physical access controls criteria of SOC 2 concern how service organization controls implement logical access to IT systems/credentials, physical access to facilities, and security measures to detect and prevent unauthorized access.

For example, CC6.1 states that “the entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity’s objectives.” Organizations should identify and authenticate users, consider network segmentation, manage credentials for infrastructure and software, use encryption to protect data, and protect encryption keys.

Here are some rules that Fugue enforces to help prevent unauthorized access to your cloud environments: Fugue checks to ensure that no security group allows unrestricted ingress to port 80, unless it is from an AWS Elastic Load Balancer. Fugue also checks to ensure that CloudWatch log groups are encrypted with KMS Customer Managed Keys (CMKs).

CC 7.0: System Operations

The system operations criteria of SOC 2 address how service organization controls monitor systems for potential anomalies, events, and configuration changes that may carry security risks, and define incident response protocols to contain, remediate, and communicate security incidents.

Fugue provides security and compliance teams with the ability to detect potential misconfiguration risks and noncompliance in near-real time, as well as the ability to set clear and agreed upon baselines, which serve as the basis for automated remediation and drift detection. Fugue promotes compliance with CC7.1 by detecting when CloudWatch and CloudTrail are not enabled and configured correctly. For example, Fugue checks to ensure that a CloudWatch metric filter and alarm is enabled to catch changes made to IAM policies. Monitoring changes to IAM policies helps ensure authentication and authorized controls remain intact.

CC7.2 requires organizations to monitor for malicious acts or anomalies to determine whether they are security threats. Fugue enforces compliance by alerting users to rejected connections in VPC flow logs. With a CloudWatch log metric filter and alarm set up to watch for denied connections to CloudFront distributions, users can investigate anomalous traffic.

CC 8.0: Change Management

The change management criteria of SOC 2 deal with how organizations evaluate and determine necessary changes in infrastructure, data, software, and procedures, which gives them the ability to securely make changes and prevent unauthorized changes.

For example, CC8.1 addresses protecting confidential information - “The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.” The criterion further elaborates that service organizations should create baseline configurations of IT technology and protect confidential information.

Fugue addresses CC8.1 by verifying that DynamoDB tables are encrypted with KMS CMKs. When enabled, DynamoDB encryption secures the primary key, local and global secondary indexes, streams, global tables, and backups in the encrypted table.

Ensuring SOC2 Compliance with Fugue

Fugue provides insights into your SOC 2 compliance posture by detecting cloud misconfigurations and compliance violations, enforcing baselines with codeless auto-remediation, and offering audit reporting with dynamic reports, dashboards and visualizations.

About Fugue

Fugue ensures that cloud infrastructure stays in continuous compliance with enterprise security policies. Our product identifies security risks and automates compliance with out-of-the-box frameworks for the CIS AWS Foundations Benchmark, CIS Azure Foundations Benchmark, GDPR, HIPAA, ISO 27001, NIST 800-53, PCI, and SOC 2. Fugue enforces infrastructure baselines with codeless auto-remediationto self-heal and provide visibility into unwanted changes. Organizations such as AT&T, SAP NS2, and Red Ventures trust Fugue to protect their cloud environments.

aws partner network
Advanced
Technology
Partner