What is Cloud Data Control (CDC)?

The rapid adoption of cloud technologies has introduced numerous new challenges for security, compliance, and DevOps teams. Although cloud platforms like AWS, Azure and GCP introduce substantial operational benefits, they also introduce new challenges for an organization’s ability to secure data in the cloud and meet an ever-increasing regulatory burden. Unfortunately, many legacy data security and control solutions do not align well with existing and emerging cloud provider technology stacks. In some cases, they do not align at all. Complicating matters are multi-cloud environments that provide disparate cloud security models. Emerging Cloud Data Control (CDC) solutions solve this challenge via a heterogeneous security and control framework across cloud stacks to ensure critical aspects of data security (including audit, identity and access management, data access, and compliance) are effectively addressed in a single provider cloud or multi-cloud implementation.

Introducing the Sonrai Security CDC Service

The Sonrai Security CDC service delivers a complete risk model of all identity and data relationships, activity and movement across cloud accounts, cloud providers and 3rd party data stores. Built from the ground up to address fundamental cloud data security and compliance concerns, the solution delivers the following risk control workflow:

- **Discover**: Automatically, visualize and map data in the cloud.
- **Classify**: Leverage machine learning to determine data type, importance, and risk.
- **Audit**: Continuously map permissions, configuration, and access to data
- **Protect**: Use behavioral controls to detect and prevent theft
Sonrai Security CDC helps companies reduce risk, ensure compliance and increase operational efficiencies.

**Risk and security monitoring**
User configuration risks, public data exposure and excess privilege are reported across cloud providers, accounts, countries, teams and applications.

**Cloud identity and data compliance**
Data sovereignty, data movement and identity relationships are all monitored and reported to ensure conformance to sovereign, GDPR, HIPAA and other compliance mandates.

**DevOps multi-cloud efficiency**
Cloud provider management models are normalized with centralized analytics and views of data across hundreds of AWS/GCP accounts and Azure subscriptions.

---

**Sonrai CDC Reduces Risk and Improves Data Security**

Sonrai CDC is focused on reducing the risk of cloud breach and compliance violations through the introduction of cloud-specific risk management workflow across the following four important categories:

<table>
<thead>
<tr>
<th>Data Exposure</th>
<th>Data Sovereignty</th>
<th>Crown Jewel Protection</th>
<th>Crown Jewel Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sonrai delivers continuous assessment to ensure sensitive cloud-based data is not exposed publicly.</td>
<td>Sonrai ensures data in is not stored or accessed from geographies that are outside security or compliance policy.</td>
<td>Sonrai aligns identity and access security policies with business risk to ensure the protection of crown jewel data is managed.</td>
<td>Sonrai aligns identity and access security policies with business risk to ensure the protection of crown jewel data is managed.</td>
</tr>
</tbody>
</table>
Sonrai Tracks Data Access Within a Cloud Provider and Across Clouds

Implementing controls around what has access to data is fundamental to any data security and compliance program. Although each unique cloud provider delivers services and APIs to manage identity and access to data for their stack, they are not standardized across all the stacks available (e.g., Amazon, Google, and Microsoft), do not address 3rd party data stores, and often require use of low-level tools and APIs. Sonrai CDC resolves this problem through normalized views and control of cloud identity and data access. Example use cases supported by continuous monitoring of access include:

**User Configuration Risk**
- Account password policy violations
- MFA not enabled
- Trust relationships - ability to escalate privilege
- Credential/key/role lifespan
- Separation of duty violations

**Suspicious User Activity**
- Interactive shell and API using same credential
- Failed escalation attempts
- Admin user created account with alternative access
- Account/role created with excessive privilege

**Identity & Access Risk**
- Over permissioned identities that never execute actions allowed
- Assume role and switch role functions that allow privilege escalation if compromised
- VPC with open access
- Host or instance with open access

Figure 1: Example use cases across risk categories assessed by Sonrai Security
Sonrai CDC Ensures Compliance to Key Mandates

Data sovereignty, data movement and identity relationships are all monitored to ensure conformance to sovereign, GDPR, HIPAA and other compliance mandates. Compliance capabilities include:

- **GDPR compliance.** Geographic sovereignty is confirmed and data asset discovery is supported. PII data movement is monitored.

- **HIPAA, PCI and other compliance reporting.** Mandate specific reporting and continuous audit of all identity, developer and privilege access to regulated data assets.

- **Data sovereignty monitoring.** Data classification and location is determined. Movement between geographies and access from alternate geographies is monitored.

- **Data asset inventory.** Unreported data assets will be found, identified and monitored across cloud accounts and developer teams.

- **Continuous monitoring of configuration data.** Cloud configuration data, identity, data access, and data movement are collected, normalized, and available for compliance and audit teams.

- **Configurable frameworks for your company and industry.** Out-of-the-box support is available for major government and industry regulations. Frameworks can be easily customized for unique company requirements.

- **Flexible 3rd party data connectors.** Out-of-the-box support is available for industry leading cloud providers (e.g., AWS, Azure, and GCP) and data stores (e.g., Aurora, Cassandra, Gremlin, MongoDB, MS SQL, MySQL, Oracle, Postgres SQL, SQL, SQL Server, etc.)
Sonrai CDC Increases DevOps and Security Efficiency

Sonrai cloud provider management models are normalized with centralized analytics and views across hundreds of AWS/GCP accounts and Azure subscriptions/resource groups to streamline governance for DevOps and Security teams. Operational capabilities include:

- **Centralized model of identity and data.** Sonrai CDC models all activity and relationships across cloud vendors, accounts and third party data stores. All views pivot on cloud provider, country, cloud accounts, application or data store.

- **Cloud-native query.** Cloud Query Language (CQL) provides rapid interrogation of the complete and centralized model of all data and identity relationships.

- **User and asset reports.** User reports show all privileges and data a particular identity has access to. Similarly, data reports show all those entities with access and history.

- **DevOps and security personas.** DevOps team leaders pivot all functions across teams, applications and data. CISOs pivot on geography, provider and compliance mandates.

- **API’s and customization.** API’s provide access to data and reporting functionality.

**Summary**

The Sonrai Security CDC service has been developed to help businesses improve security, ensure compliance and increase operational efficiencies for their AWS, Azure, GCP and other cloud platforms. Core to the service is the ability to gain a centralized and consistent view into cloud identity and data relationships, activity, and data movement across cloud accounts, cloud providers, and 3rd party data stores.