ACTIAN™

DATASHEET

Security, Compliance, and Governance

Avalanche Cloud Data Platform

Overview

Whether your organization is required to comply with General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), Federal Information Security Management (FISMA), Payment Card Data Security Standard (PCI DSS), or the California Consumer Privacy Act (CCPA), the data platform you select to manage your data is critical to your success. Maintaining regulatory compliance requires organizations be able to demonstrate their systems are secure and adequate processes and procedures are in place to quickly address any gaps in security posture and compliance that may arise. Detailed below are some key requirements for data security and compliance and how the Avalanche Cloud Data Platform helps manage these.

Strong Authentication

At a minimum, the Avalanche platform requires users to authenticate their identity using a unique login ID and password. Single sign-on (SSO) using OAuth allows a user to log into multiple independent software systems with one ID and password. This helps ensure that your organization's identity policies are extended to protect your data platform. For added authentication protection, you can leverage your identity provider (IdP) to use multifactor authentication (MFA). This adds an extra level of security by requiring multiple methods of authentication (such as a password and a one-time numeric code sent via SMS to a known mobile phone number) before allowing a user to access the platform.

Key Features

- Single-sign on Using OAuth
- Multifactor Authentication
- IP Allow List
- Role-based Access Control
- Data Masking
- Encryption of Data at Rest and In Motion
- Rekeying of Encryption Keys
- Role Separation
- Audit Logs
- Security Alarms
- Regional Deployment Control
- ISO 27001 Certified
- Compliance with the System and Organization Controls 2 (SOC 2) Framework

Access Control

The core of security compliance is access control. The Avalanche platform limits who can read, write to, and update different data with discretionary and non-discretionary approaches.

The Avalanche platform's discretionary approach uses an "IP Allow" list to limit access to users with approved device IP addresses. When used in conjunction with user authentication, an IP Allow list provides a valuable layer of additional security by precluding access to the data platform when a user's credentials are correct, but the device being used is not recognized.

An unscrupulous individual may have stolen a legitimate user's credentials but won't be able to use them to access the data platform unless the individual also has access to a computer whose IP address appears on the IP Allow list.

A non-discretionary approach to access control is exemplified by support for Role-Based Access Control (RBAC). This technique grants access to resources based on an individual's role in an organization. RBAC does more than just simplify user administration; it can help enforce the principle of least privilege where users have only the privileges they need for their job. This helps comply with privacy and confidentiality regulations. A grant statement can narrow down exactly what user or role is granted a privilege.

Sensitive Data Protection

Because sensitive data masking is a mandatory requirement for achieving PCI DSS, GDPR, and HIPAA compliance, it is a must for data platforms in industries governed by these regulations. This kind of data access control is enabled in the Avalanche platform by dynamic data masking. This is a process by which original data is dynamically occluded by modified content. Dynamic masking is often used to protect fields containing personally identifiable information, sensitive personal data, or commercially sensitive data.

Secure Data Storage and Transmission

Encrypting data at rest (that is, stored in a database) and in motion (in transit on a network) is vital for regulatory compliance and data protection.

The Avalanche platform protects data at rest using AES 256-bit encryption. Additionally, some data may warrant different privacy or security measures. To meet these needs, the Avalanche platform offers the flexibility for both full database encryption and individual column encryption. The Avalanche platform also supports the rekeying of encryption keys where the entire database is decrypted and then re-encrypted with a new encryption key as recommended by NIST guidelines. This is a valuable way to limit the amount of time a bad actor can use a stolen key to access the platform.

Because data in motion (data transmitted from one location to another) is vulnerable to man-in-the-middle (MiTM) attacks, the Avalanche platform can encrypt data while in motion to prevent interception.

Role Separation

By requiring individuals with distinct roles to work together to complete critical or sensitive tasks, you create a checks-and-balances mechanism that can reduce security risks and facilitate compliance with regulatory mandates such as SOX, HIPAA, PCI DSS, and GDPR—as well as with industry regulations such as ISO 17799.

The Avalanche platform ensures role separation. The idea is based on the principle of separation of duties where more than one person should be involved when completing critical or sensitive tasks. For example, role separation in the Avalanche platform could require that the person who determines what to audit (DBSSO) must be different from the person who monitors the audit trail (AAO), and both must be different from the person who is responsible for the operations of the database server.

Audit Support

The Avalanche platform's audit logs form a critical part of data protection and compliance because they record all or specified classes of security events for the entire installation. Selected classes of events, such as use of database procedures or access to tables, can be recorded in the security audit log file for later analysis. Criteria can be selected that apply to a single object or across an entire class of installation objects.

The security alarm capability enables you to specify the events to be recorded in the security audit log for individual tables and databases. Using security alarms, you can place triggers on important databases and tables. If any user attempts to perform an access operation that is not normally expected, the security alarm will raise an alert.

Data Sovereignty

To support data sovereignty, the Avalanche platform lets you define the geographic region where your data is deployed. Data sovereignty means that data is subject to the laws and governance structures from where it's collected. For example, a business in the United States must comply with GDPR if data was collected anywhere in the European Union. Likewise, if the business collected data from a customer located in California, the business has to comply with CCPA.

Trust

Actian's ISO 27001 certification proves compliance with global best practices for quality in information security management systems.

The Avalanche platform operates in compliance with the System and Organization Controls 2 (SOC 2) framework, demonstrating that it maintains a high level of information security. We have passed an on-site audit, showing that we have taken all steps necessary to keep the Avalanche platform, and the valuable information contained therein, safe from breaches.

Be sure your cloud data platform provides the features and functions to help you comply with the ever-increasing requirements your business faces today. You can trust your data with Actian and the Avalanche Cloud Data platform. Delivering robust security and compliance is a core aspect of Actian's design principles.

About Actian

Actian transforms business by simplifying how people connect, manage, and analyze data. The Avalanche Cloud Data Platform gives customers a flexible and comprehensive solution that enables fast innovation by gaining real-time insights, leveraging native data integration, and deploying anywhere. The Actian platform offers maximum interoperability by combining data integration, management, and analytics solutions across systems, while its partnership model makes scaling fast, efficient, and effective. Customers benefit from its always available support that proactively detects and solves potential issues, which is also a crucial feature for data intensive enterprises. For more information, please visit **www.Actian.com**.

Toll Free +1 888 446 4737 Tel +1 512 231 6000 330 Potrero Ave, Sunnyvale, CA 94085 **Actian.com**

ACTIAN™