ACTIONIQ

ActionIQ **Security Brief**

Security at the Center of the CX Transformation

Certified Compliance with Government Regulations and Industry Standards

AICPA SOC aicpa.org/soc4so

CCPA

GDPR

HIPAA COMPLIANT

Table of Contents

Introduction

The Ever-Growing Importance of Security

To meet the demands of today's experience economy, enterprises are transforming to become more customer-centric. Navigating this transformation requires managing:

- Technology stacks that are increasingly complex
- An exponential growth in customer data
- An ever-increasing number of systems hosting and manipulating this data

Simultaneously, enterprises are introducing more cloud-based infrastructure and software-as-a-service (SaaS) alongside their traditionally on-premise systems. This means enterprises must now provide data access to their cloud infrastructure and SaaS vendors. While this unburdens the enterprise from the effort and expense of on-premise management, it requires a new level of trust between organizations and their vendors.

As a result, managing data privacy and security has never been more complex. And with increasing mandates for regulatory compliance—and with privacy critical to maintaining consumer trust—security has never been more important.

Security at the Center of the CX Transformation

ActionIQ has a deep commitment to privacy and security. We employ best practices to keep your data secured and under your control. This security effort applied to technology, processes and people allows your enterprise to remain compliant with external and internal regulations and policies. And to establish and maintain trust between you and your customers.

This security brief provides an overview for IT professionals on the policies, practices and culture at ActionIQ that make up our commitment to keep you and your data safe. This will be described across four key areas of ActionIQ's organization, processes and technology:

1. **Platform architecture:** Security applied across all parts of the ActionIQ Platform
2. **User access, governance & privacy:** Tools and controls required for compliance with all regulations and policies
3. **Company controls:** Security-first practices, procedures and culture
4. **Third party certifications:** Security audit and certification by third party experts

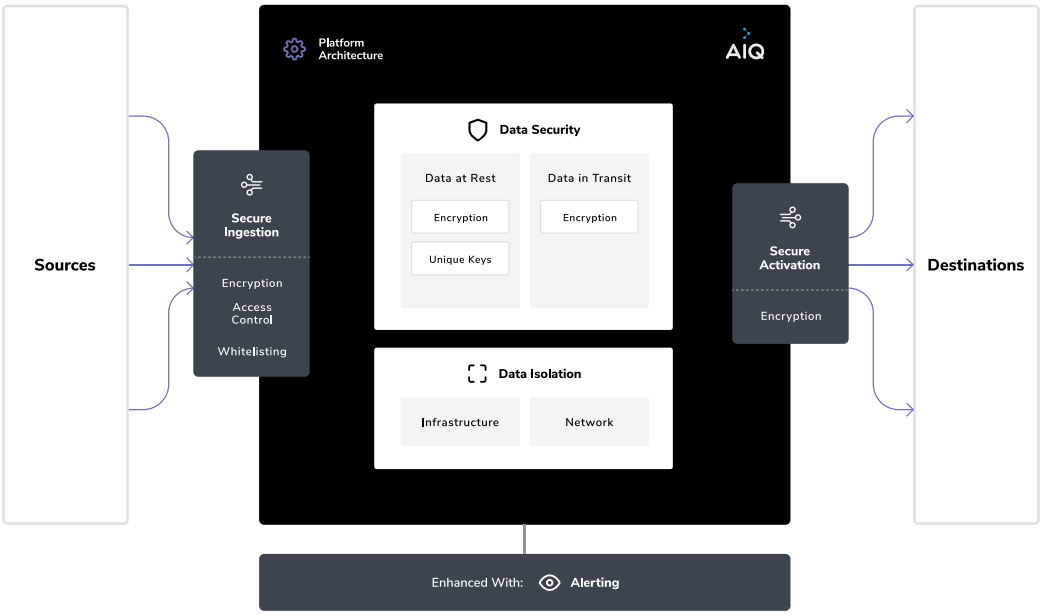
"At ActionIQ, we design technology that enables consumers to have personalized experiences with your brand. At the foundation of those experiences is trust. Trust the PII will be used appropriately and fully secured. Our team is here as your partner in safeguarding that trust so you can remain focused on building loyal and lasting customer relationships."

STEVE MCCOLL
ACTIONIQ VP OF ENGINEERING

1. Platform Architecture

Security applied across all parts of the ActionIQ Platform

ActionIQ platform is a cloud-based, Software-as-a-Service (SaaS) platform, built from the ground up with high standards for privacy and security. These standards apply when data is in transit to the ActionIQ platform, while at rest, and while it is manipulated within the platform.



Personally Identifiable Information (PII)

ActionIQ supports a flexible range of PII requirements. The platform can handle PII in order to help directly facilitate communications with downstream systems. Alternatively, the platform can take in encrypted/hashed PII data which is then decrypted by a receiving downstream system.

Ingestion

ActionIQ provides multiple methods to ingest data into the platform, allowing you to choose the best based on the source system type. Each method employs secure data transfer with encrypted network connections. When a source system initiates a data push to ActionIQ, ActionIQ always confirms the sender is legitimate using techniques including IP whitelisting, username and password, and any other required validation.

Data Isolation

INFRASTRUCTURE

All the data entering the ActionIQ environment is transited and stored in a secured infrastructure. ActionIQ services are hosted on Amazon Web Services (AWS), inheriting its comprehensive security and compliance controls. AWS meets enterprise-class security requirements, providing an infrastructure agnostic to underlying data and data processing while offering full control and flexibility over security parameters.

ActionIQ leverages Amazon Elastic Compute Cloud (EC2) to execute its services. ActionIQ configures the platform to support single-tenant customer data for each client, providing a high degree of isolation and protection. The access is controlled via client-specific identity and access management definitions.

NETWORK

Based on your specific needs, ActionIQ sets up a range of services to ensure network isolation. Isolation is enforced using a dedicated Amazon Virtual Private Cloud (VPC) owned by ActionIQ. Client environments are deployed within this VPC. Client instances are shielded from each other using single tenant isolation. To further protect the environment, ActionIQ services are only accessible within a Virtual Private Network (VPN) and via IP addresses previously provided by the client to be whitelisted. Back-end services are maintained in a subnet behind a proxy and firewalls.

Data Security

The infrastructure isolation described in the previous section enforces data isolation, ensuring that one client's data can never come in contact with another's.

DATA AT REST

Data at rest is stored in Amazon Simple Storage Service (S3) buckets with encryption at rest. S3 buckets are encrypted with unique keys.

DATA IN TRANSIT

Data in transit across the ActionIQ platform is encrypted with industry-standard Secure Sockets Layer (SSL) technology. This data remains isolated at all times.

Activation

ActionIQ employs authentication, authorization and encryption techniques to keep data secure when transmitted from the ActionIQ platform to third-party tools.

Alerting

The ActionIQ platform incorporates 24/7/365 monitoring and alerting, to track and notify you of any attempts at unauthorized access to the platform. Permissioning and access are governed by well defined security groups, closely managed access control lists, and IP whitelisting.

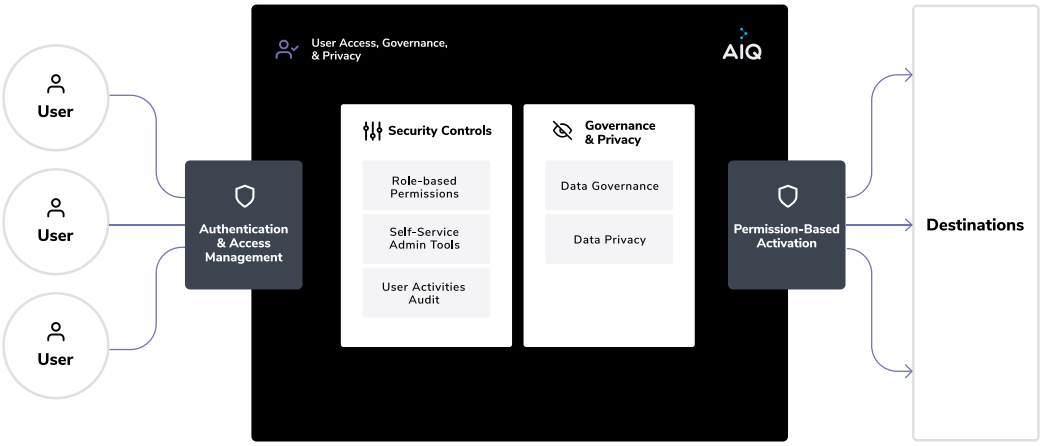
ActionIQ regularly audits security groups to ensure the list of authorized users and their permissions is verified and up to date. We leverage a leading security monitoring tool for access control, credential management, and data access permissions. Because all activities within the platform are logged, ActionIQ can easily configure recurring reports detailing:

- Authorized users within the ActionIQ environment
- Data and access rights
- Data ingested and exported from the ActionIQ environment

2. User Access, Governance, and Privacy

Tools and controls required for compliance with all regulations and policies

Robust policies and procedures that employ industry best practices are instrumental to protecting customer data.



Authentication and Access Management

Only authorized users may access the ActionIQ platform. Authorization begins with an account-based access requiring whitelisting. Across the platform, ActionIQ ensures that authentication, authorization and access controls are put in place to limit data and functionality access to the correct users. These controls are present in the user interface and also extend into the ActionIQ API layer which performs authentication, authorization and input validation prior to servicing requests.

The platform offers a number of options for user authentication. In order of most-to-least recommended, they are as follows:

1. Single sign-on (SSO)
2. Multi-factor authentication (MFA)
3. Login and password combination

Security controls

ROLE-BASED PERMISSIONS

The ActionIQ platform adheres to the principle of least privilege. By default, deny rules prevent general access to ActionIQ. Users must be proactively granted permissions to gain access to various applications, resources and capabilities within the ActionIQ platform. Access permissions can be managed by role (e.g. IT admin, analyst, marketer, etc.) to withhold certain features, and editing or publishing rights from unauthorized user roles.

SELF-SERVICE ADMIN TOOLS

Within the platform, users with designated Administrator status have the authority to update user access permissions via a self-service admin interface. This permissioning capability is facilitated by a role- and team-based permissioning and authorization framework.

USER ACTIVITIES AUDIT

ActionIQ enforces session tracking and audit trails within the platform's service logs. This aids with issue triage and provides detailed usage insights for auditing purposes. All user activities on the platform, including data access, are tracked—but no PII or customer data are recorded in the logs.

Governance & Privacy

DATA GOVERNANCE

With ActionIQ, your IT team maintains control of data governance. Using ActionIQ tools specifically for IT, you can granularly control what data is accessed and by whom, all the way down to the data field level.

DATA PRIVACY, GDPR AND CCPA

ActionIQ plays the role of a data processor. The platform provides tools and processes that aid compliance with regulatory requirements including GDPR and CCPA. The platform provides data portability as a core platform function, with tools to extract and port customer data based on specific selection criteria. Data purging and fine-grained erasure are conducted automatically on a daily basis. Manual data removal is available on-demand.

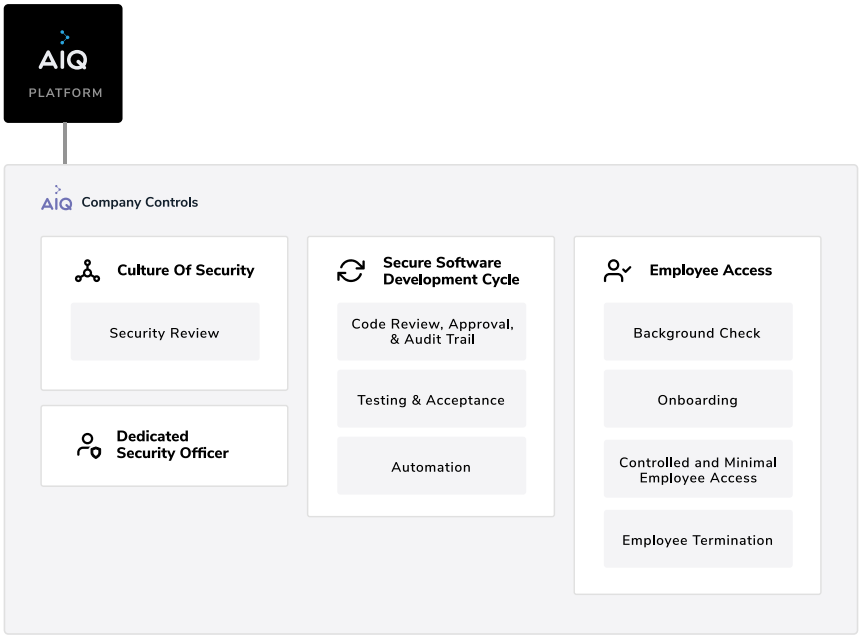
PERMISSION-BASED ACTIVATION

Only permissioned users may extract data from ActionIQ and push it to a destination enabled on the platform. Your IT maintains control over which customer data attributes or behaviors can be used in a channel activation.

3. Company Controls

Security-first practices, procedures and culture

Software and its infrastructure can be rich with security features. But for security to be achieved, the operator of the software must also employ robust security practices down to every individual in the company.



Culture of Security

Since its inception, ActionIQ has invested in developing a culture of security. From the ground up, the ActionIQ team has been built with experts who bring experience working with some of the world's largest datasets within complex, demanding and technically rigorous enterprises. Their knowledge, experience and best practices—as well as those designed in partnership with ActionIQ's customers—have been built into ActionIQ's technology, processes and culture. ActionIQ takes security as an ongoing and continuous commitment. That commitment is reflected in the controls, features and processes described in this document.

SECURITY REVIEW WITHIN ACTIONIQ

ActionIQ conducts periodic risk assessments, information security audits, mandatory training, business continuity planning (BCP), disaster recovery (DR) planning and testing. In addition, ActionIQ subjects itself to regular third party penetration testing performed, SOC 2 Type 2 examination and HIPAA Type 1 examination.

ActionIQ Secure Software Development Lifecycle (SDLC)

ActionIQ employs a secure software development lifecycle (SDLC) to drive the process of building its platform and applications—placing security at the core every design and development effort.

CODE REVIEW, APPROVAL AND AUDIT TRAIL

All software code and infrastructure changes require peer review and pass through an explicit approval procedure before inclusion in a product release. ActionIQ employs tools that make all stage transitions in its SDLC auditable.

TESTING AND ACCEPTANCE

Prior to software release, each release must pass stringent automated and manual testing to validate the correctness of the platform.

AUTOMATION

To minimize the number of individuals with administrative privileges within ActionIQ infrastructure, ActionIQ utilizes automated tools to configure the platform environment and install new product releases.

Employee Access

BACKGROUND CHECK

All employees undergo a successful background check prior to being granted system access.

ONBOARDING

When a new employee joins ActionIQ, they must complete a security awareness training and assessment. This assessment is conducted and scored using a third-party. ActionIQ device management software is installed on each employee corporate laptop and security measures, including disk encryption, password controls, screen lock and more, are set.

CONTROLLED AND MINIMAL EMPLOYEE ACCESS

ActionIQ employees are granted the minimum access required to do their job. Where elevated privileges are required, employees may acquire such privileges using a structured approval process.

To support your ActionIQ implementation, the following ActionIQ personnel are typically provided access:

- **Client Partner** – typically a single support executive who partners with your team to ensure that maximum platform value is being achieved and to offer best practices guidance.
- **Forward Deployed Engineers** – typically two professional services engineers acting in a primary and secondary role.
- **Infrastructure Support Engineers** – a small team of engineers focused on platform health and stability. Typically they rely on aggregated systems metrics rather than direct access to gauge platform health. In support scenarios, they may have elevated privileges to adjust configuration or restart services.
- **Release Engineer** – on a periodic basis (typically weekly) a release engineer is granted temporarily elevated privileges to enable the deployment of a software upgrade.

EMPLOYEE TERMINATION

In the event of an employee's termination, all access to AIQ systems and documents is revoked on the same day.

Dedicated Security Officer

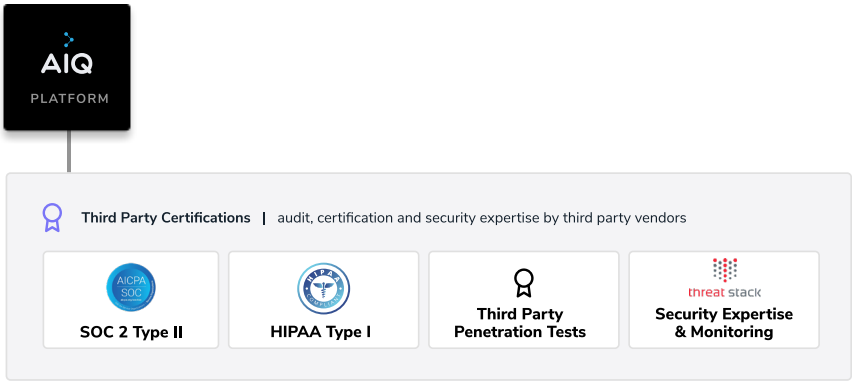
ActionIQ employs a full time Director of Information Security who oversees and implements the company's security program. The director:

- Owns the definition and execution of ActionIQ's security strategy and underlying policies
- Interfaces with clients to demonstrate our security expertise
- Manages relationships with security vendors and partners
- Works with client IT to audit systems and ensure compliance
- Develops and delivers security education to employees

4. Third Party Certifications

Security audit and certification by third party experts

As an additional, objective check on ActionIQ security measures, ActionIQ contracts with multiple third party security experts who regularly audit and certify the company's systems, procedures, policies and software.



SOC 2 Type 2 Examination

ActionIQ's SOC 2 Type 2 examinations are conducted annually by a leading independent third-party cybersecurity and compliance firm. SOC 2 Type 2 is one of the most stringent compliance standards in the industry, established by the American Institute of Certified Public Accountants (AICPA). The standard covers security, processing integrity, availability, confidentiality, privacy and more. What's distinctive about SOC 2 Type 2 examination is that it isn't something ActionIQ "gets done". Rather, it is an ongoing commitment to a secure mode of operating that is strengthened, improved, and re-validated with every examination.

As an enterprise going through vendor selection for your CDP, working with a vendor partner who subjects themselves to SOC 2 Type 2 examination provides added confidence that the solution will pass your internal security review. It also helps boost trust that your customer data will be managed and protected to a high standard of best practices.

ActionIQ subjects itself to an annual SOC2 Type 2 examination.

HIPAA Type 1 Examination

In addition to the baseline for data security practices that SOC 2 Type 2 provides, ActionIQ successfully completed its first independent third-party HIPAA Type 1 examination. Enforced by the U.S. Department of Health and Human Services, the Health Insurance Portability and Accountability Act (HIPAA) establishes national standards for maintaining the security and privacy of electronic health information, setting rules for privacy, security and breach notification in order to maintain the integrity of protected health information. Besides undergoing HIPAA audits, ActionIQ also periodically trains employees on HIPAA awareness to reinforce compliance.

By meeting HIPAA compliance guidelines, ActionIQ is ready to implement safeguards to ensure the confidentiality and integrity of sensitive healthcare data. Our customers can confidently manage health information knowing they're partnering with a HIPAA Type 1-certified vendor.

Third Party Penetration Tests

ActionIQ engages an external security company to assess source code and perform yearly penetration tests against the platform. Should issues arise during an assessment, they are remediated in a timely fashion based on issue severity.

Additional Security Expertise and Monitoring by Threat Stack

Threat Stack is utilized as an additional, independent, security monitoring and alerting layer across ActionIQ's SaaS environment. Threat Stack detects, triages and issues alerts ActionIQ regarding security issues and suspicious activity.

About ActionIQ

ActionIQ is at the center of a data-driven revolution that is changing the way brands think about customer experience, digital transformation and the value of customer data as a core corporate asset. We concentrate on solving enterprise data challenges so that teams are empowered to create authentic customer experiences across all brand touchpoints. ActionIQ helps G2000 companies by connecting their first-party customer data, providing an easy-to-use interface for business users to access customer insights, and enabling customer experience orchestration across channels. We are helping brands like Morgan Stanley, The New York Times, Pandora Media, The Hartford, Shopify, American Eagle Outfitters and others grow customer satisfaction and revenue.