NICE Actimize

Datasheet

Actimize Insights Network: Privacy, Security and Compliance for Financial Institutions

Secure, Compliant and Resilient Information Sharing

Fraudsters operate across institutions, yet siloed data limits detection. Financial institutions (FIs) must collaborate to combat fraud, but data privacy regulations and security risks often hinder information sharing. NICE Actimize's Insights Network addresses this challenge by enabling secure, anonymized data sharing across a consortium, ensuring robust fraud detection without compromising sensitive information or regulatory obligations.

Designed for seamless integration with existing solutions, the Actimize Insights Network provides a holistic view across connected systems, leveraging rich transactional data, such as transaction amounts, transaction numbers and account details, to maximize the value of shared intelligence. This comprehensive approach strengthens fraud prevention while maintaining the highest standards of data security and compliance.

Keep Your Data Safe, Without Compromise

The Actimize Insights Network is engineered to uphold the highest standards of data protection while facilitating secure collaboration across FIs. Every layer from data contribution to lifecycle management is fortified with enterprise-grade security, privacy-preserving techniques and regulatory compliance. Data visibility is tightly controlled: participants cannot view data from other institutions, and shared insights are aggregated and anonymized.

Advanced Data Privacy and Anonymization

The Actimize Insights Network ensures sensitive data remains fully protected and anonymized, eliminating exposure risks while maintaining analytical accuracy.

- Sensitive identifiers (e.g., account numbers) are hashed using SHA-512, making them irreversible and non-decryptable.
- Hashing occurs at the source system, ensuring no raw identifiers leave your environment.

Enterprise-Grade Security

The solution delivers a robust security framework with industry-leading encryption, strict access controls and tenant-level isolation, safeguarding data integrity and confidentiality across all interactions.

- **Encryption Standards:** The solution uses TLS 1.3 or higher to encrypt data in transit and AES-256 for data at rest, with support for SSE-S3 or SSE-KMS.
- **Data Isolation:** Data is logically separated per tenant, with strict enforcement of tenant boundaries to ensure no cross-institutional data leakage.

To ensure every transaction call is legitimate and tamper-proof, the Actimize Insights Network enforces multiple layers of authentication.

- **Customer-Specific API Keys:** Access is controlled through institution-specific API keys that are bound to tenant identity.
- **Mutual TLS (mTLS):** This protocol ensures authentication, performed using digital certificates, of both client and server.
- **OAuth 2.0 & JWT Tokens:** These tokens are short-lived, signed and include embedded claims such as tenant ID, role and expiration.
- **IP Whitelisting & Restrictions:** Only pre-approved IP ranges are allowed to initiate API calls.
- **WAF-Protected APIs:** These APIs are protected against SQL injection, cross-site scripting (XSS) and distributed denial-of-service (DDoS) attacks.
- **Role-Based Access Control (RBAC):** This mechanism enforces fine-grained permissions for sensitive operations.
- **Transaction-Level Nonces & Signatures:** Each API call includes a unique nonce and cryptographic signature to prevent replay or forgery.
- **Audit-Ready Authentication Logs:** Every authentication attempt is logged with metadata such as timestamp, tenant ID, source IP and certificate fingerprint.

Compliance and Continuous Monitoring

Meet global regulatory standards while maintaining proactive security through real-time monitoring, audit logs and vulnerability management with NICE Actimize.

- The Actimize Insights Network is certified for ISO 27001, SOC 2 Type II, GDPR, CCPA and APRA CPS 234.
- The solution supports continuous monitoring, audit logs, vulnerability scans, and incident response.

Data Lifecycle and Resilience

Secure data handling from retention to deletion minimizes risk and ensures compliance throughout the data lifecycle. Built-in resilience and high availability protect against downtime and data loss, enabling uninterrupted operations and business continuity.

- Data is retained for 7 years, with secure deletion upon contract termination.
- The solution utilizes multi-region replication, versioning and private buckets to prevent data loss.
- The Insights Network ensures high availability through active-APIs, providing near-zero RTO and RPO for data consumption.

Fast, Secure, Compliant

- Secure, anonymized data sharing across institutions enables FIs to identify bad actors before suspicious activity occurs.
- Compliance with global privacy regulations helps reduce risk exposure.
- Real-time monitoring and alerts for suspicious activity allow immediate threat detection and necessary response.
- Automated data lifecycle management ensures data compliance and minimizes exposure.

The Actimize Insights Network delivers a secure, compliant and resilient platform for collaborative fraud prevention. Identify high-risk actors early and rest assured that your data is protected.

→ **Strengthen Your Fraud Defenses without Compromising Privacy**