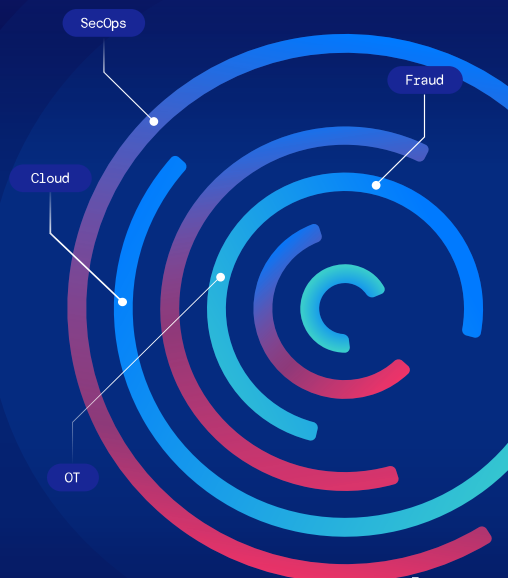
SWIMLANE

The Swimlane Security Blueprint

An in-depth review of Swimlane's industry-leading security and compliance standards



Overview

As the threat landscape evolves and new technologies emerge, it's more important than ever for organizations to protect sensitive data and critical operations through robust security controls. This whitepaper explores Swimlane's comprehensive approach to security and compliance. It details the protocols and industry standards that set Swimlane apart as a secure vendor, demonstrating our commitment to safeguarding customer data. This overview covers Swimlane's compliance certifications, audits, AI data privacy, and proactive risk management strategies.

Robust Compliance and Audit Protocols

Maintaining strict compliance and audit protocols is essential to safeguard sensitive data and uphold regulatory standards. Swimlane's comprehensive approach ensures continuous monitoring, regular assessments, and transparent reporting to meet industry requirements. See the current list of Swimlane's compliance and audit processes below.

Swimlane Compliance Certifications

- SOC II Type II Report covering the American Institute of Certified Public Accountants (AICPA) Trust Service Criteria categories of Security, Availability, and Confidentiality Privacy. Swimlane's latest SOC II Type II attestation was for the May 2023 to May 2024 period.
- Swimlane obtained certification for ISO/IEC 27001: 2022 on June 2nd, 2023. Annual surveillance audits are completed to follow certification requirements. The latest audit was completed on May 7th, 2024.
- Swimlane is compliant with CSA STAR Level 1. The official CSA STAR registry listing can be found here.

Third-Party Audits

- Annual incident response readiness assessment
- Quarterly web application scans
- Annual web application penetration test

Artificial Intelligence Data Privacy & Security

Swimlane Turbine is an AI-enhanced security automation platform. Hero AI is the collection of generative artificial intelligence (genAI) innovations, built on the Swimlane large language model (LLM), that is available within the Turbine platforms. Data privacy, security, and transparency are core to all Hero AI capabilities.

Swimlane does not collect or store any sensitive customer data in centralized storage locations. Only metadata about model usage and performance is retained centrally. Customer data processed by AI or machine learning (ML) models is exclusively stored in the customer's own dedicated database instance which is logically separated from other customer instances. All prompts and features involving customer data are processed using a private Swimlane LLM. Swimlane does not use customer data to train or fine-tune the Swimlane LLM. Customers must "opt-in" to use Hero AI in their instance of Turbine. Individual risk assessments are conducted on all AI/LLM projects before deployment.

Risk Management

Swimlane Risk Management

The Swimlane security team continuously analyzes risks through multiple sources such as Swimlane security operations center (SOC) cases, business continuity and disaster recovery (BC/DR) tabletop exercises, bi-weekly security stand-ups, security incident reports, as well as continuous monitoring for Swimlane products, architecture or asset classification changes. The Swimlane governance risk and compliance (GRC) team manages a risk register that informs Swimlane's annual risk assessment and risk treatment plan activities.

Annual Risk Assessment & Treatment Plan

Annually, the Swimlane leadership team conducts a risk assessment and risk treatment plan exercise. This involves assessing the likelihood and impact of potential risks such as compromised cloud access, ransomware attacks, supply chain threats, and more. Each risk requires a treatment plan that indicates if the risk is accepted, transferred, or mitigated. These decisions are based on leadership's analysis of Swimlane's strength of mitigating controls relative to the inherent risk the potential situation poses to the business. Accepted risks require documented approval by Swimlane leadership. Risk treatment plans, for transferred or mitigated scenarios, are documented and tracked by Swimlane GRC in a dedicated compliance management tool. An annual risk assessment report is documented as evidence and distributed to appropriate stakeholders.

Third-Party Risk Management

All Swimlane vendors are tracked and analyzed in a dedicated vendor management tool. Vendors are organized by criticality to the business, types of data stored, inherent risk, and residual risk. Each vendor has their own profile for tracking internal ownership, access to systems, API integrations, data types processed by the system, and results of third-party risk assessments. Business unit leadership is required to review their respective systems annually. This audit process ensures all third parties have been vetted by GRC and that all tools, systems, or integrations are still in use.

Vendor Onboarding and Access Controls

Risk assessments are required before onboarding any new system or vendor to Swimlane's corporate or production environment. The Swimlane GRC team conducts security due diligence on the vendor reviewing their compliance posture, security commitments, and contractual commitments regarding security. All vendors that are deemed high-risk or highly critical to the business are required to have vendor risk assessments refreshed on an annual basis.

In most cases, access to third-party systems is managed through Swimlane's identity access management (IAM) system via SSO/SAML. The Swimlane enterprise IT team provides system access through IAM, while the system owner is responsible for managing roles and permissions for the users. System owners are responsible for ensuring user access is appropriate for the system. Third-party vendor accounts are not permitted unless authorized by Swimlane within the contract or through vendor support channels.

Asset Management

Swimlane tracks all identities, devices, infrastructure, AWS accounts, EC2 instances, third-party systems, and data within the Swimlane configuration management database (CMDB). The CMDB is updated near real-time for all assets.

The Swimlane Privacy Policy

- Notify customers of changes to sub-processors
- Aid customers with transfer impact assessments
- Respond to data requests from government or law enforcement agencies
- Perform data protection impact assessments.

Human Risk Management

Confidentiality Agreement

All Swimlane staff are required to read and sign a Confidentiality, Non-Solicitation, and Assignment of Inventions Agreement on or before their first day with Swimlane.

Background Check

Swimlane performs background checks on all new hires which includes a criminal check, education verification, and employment verification. An authorized member of the Swimlane human resources (HR) team must review each background check prior to extending an offer letter.

Security Awareness Training

Security awareness training (SAT) is required for all employees and contractors during the onboarding process and on an annual basis thereafter. SAT curriculum is custom-made by the Swimlane GRC team and includes the following topics:

- Acceptable use
- Phishing awareness
- Passwords and access control
- Data handling privacy requirements

User acceptance of relevant information security policies is required. Employees who do not complete the training on time are notified and disciplined according to the code of conduct.

Physical Security

The Swimlane security team has implemented physical controls to protect unauthorized or inappropriate access to assets, data, and sensitive information residing in the corporate headquarters, including:

Badge access system that governs all keycard access required for all points of entry

- Required visitor sign-in with the office front desk with a valid ID
- Badge usage monitoring by the Swimlane SOC
- Badge access revocation as part of the employee/contractor termination process
- Badge access is reviewed on a monthly basis
- Server room access restriction to the IT enterprise team
- Camera surveillance and environmental controls implemented by our office partner
- Clean desk and clear screen policy for employees enforced

Infrastructure Security

Change Control Policy

Swimlane has a Change Management Policy to guide personnel on how to implement changes that impact Swimlane's infrastructure. All changes, from code and infrastructure changes to product features and strategic initiatives, are managed via Swimlane's ticketing system. Changes must be tested in a non-production environment before being released to production. All changes require documented approval in the ticketing system before deployment in production.

Cloud Security Architecture

Infrastructure-as-Code is utilized in Swimlane production environments to manage configuration changes on servers and software. Cloud-Native Application Protection Platform (CNAPP) tools are used to ensure infrastructure and software containers are continuously updated, reconfigured, and/or patched to offer a secure and highly available deployment of the Swimlane Turbine platform.

Tenant Separation

Customer data is logically isolated in all Swimlane cloud and Turbine cloud environments. This is accomplished using a unique ID which includes a range of metadata associated with each customer. Customer data at rest is logically separated in MongoDB in each customer cluster.

Secure Data Centers

The Swimlane cloud and Turbine cloud environments are hosted with Amazon Web Services (AWS). For more information on how AWS protects our product and data in the cloud see AWS physical and environmental controls and AWS compliance.

Access Control

Swimlane manages system identities through an IAM tool. Admin access to the IAM tool is restricted to a small group within the IT enterprise team and the Swimlane chief information security officer (CISO). Predefined user groups that govern access to systems configured with SSO/SAML manage system access. Swimlane uses role-based access control (RBAC) based on predefined user profiles to ensure staff only have access that is appropriate to their respective job role. All new access provisioning is managed through an access request ticket.

The Swimlane SOC has visibility to the IAM identities and user groups, device information, and corresponding HR information. It monitors these accounts for anomalous behavior such as login activity, account changes, and user group changes. These alerts are stored as cases in the Swimlane SOC team's official system of record where they can be easily referenced or audited.

AWS Root Access

Users who are authorized with access to the AWS Root account are restricted to a small group on the Infrastructure team. Authentication to the AWS Root account requires multi-factor authentication (MFA) with a hardware token. Access is de-provisioned on all systems within 24 hours of an employee's termination date. This timeline is reduced to minutes in emergencies deemed by HR or management. Access reviews are conducted quarterly.

Only authorized Swimlane employees have access to customer data stored within customer cloud environments. An approved privileged access request ticket is required before accessing a customer environment.

Network Security

Zero Trust Network Architecture

Access to customer environments by Swimlane personnel requires successful authentication through a VPN which implements Zero-Trust features such as identity and device posture checks. Swimlane personnel must have an active IAM identity and use a compliant corporate-managed device to access AWS.

Administrative access to the Swimlane corporate network is also restricted to a limited number of employees on the Swimlane enterprise IT team. Authentication of the Swimlane network is controlled through a VPN which requires similar IAM and device posture checks listed above.

Corporate Network Firewall

The Swimlane security team created network Domain Name System (DNS) policies that scan, filter, and log network traffic on our corporate environment. Policies such as Internet Protocol (IP) Block lists are configured by Swimlane network administrators.

Network Segmentation

The Swimlane enterprise and office network(s) are on dedicated subnets that are protected by intrusion detection systems (IDS) and intrusion prevention systems (IPS). Wi-Fi at Swimlane headquarters utilizes RADIUS to authenticate all corporate devices. All guests and non-corporate-owned devices (BYOD) utilize a segregated Wi-Fi network.

Customer cloud resources are separated from the Swimlane enterprise and office networks. All Swimlane development environments are separated from production environments on a network level.

Web Application Firewall

IDS/IPS and a web application firewall (WAF) protect Swimlane customer cloud resources. Firewall rules are dynamically updated from the Swimlane SOC using open and closed-source threat intelligence tools.

Data Security

Key Management

Swimlane uses the AWS Key Management Service (KMS) for key management. A custodian is assigned for each vault and is responsible for ensuring the appropriate level of security controls. Anomaly detection is enabled on KMS and sent to the Swimlane SOC for triage.

Encryption of Data at Rest

Customer data and application snapshots are encrypted using the AES256 encryption algorithm before being stored on disk. Passwords for Swimlane user accounts are hashed before being stored using the HMAC-SHA1 algorithm.

Encryption of Data in Transit

TLS 1.2/1.3, and HTTPS, are used to protect data in transit. Swimlane encrypts data between the Swimlane application server and client browsers, and MongoDB from Swimlane tenant and API services.

Secure SDLC

The Swimlane engineering team reduces security risks in the software development lifecycle (SDLC) process by implementing the following controls:

- All application and infrastructure changes are defined and managed within our ticketing system.
- Automated security checks, including Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and quality tests are performed as part of the continuous integration and continuous delivery (CI/CD) pipeline.
- All code changes must be reviewed by a peer, independent of the individual who developed the code.
- Swimlane code repositories are scanned for vulnerable third-party dependencies and secrets.
- Identified vulnerabilities must be fixed before all version releases.
- Annual developer security awareness training is mandatory.

Product Security

Customer Application Logs

Swimlane audit logs report events in the Swimlane Turbine application. The customer administrator user can access logs in the customer application. Customers also have the option to retrieve logs from the Swimlane API. The full list of audit log fields and their definitions can be found at Swimlane Knowledge Center.

Customer Authentication

Swimlane cloud products offer several features for secure authentication, including:

- Two-factor authentication on user accounts
- SAML/SSO integration
- Configurable session timeout parameters
- Configurable password parameters for expiration and complexity

Additional information on authentication and session security in Turbine can be found in the Swimlane Knowledge Center.

Customer RBAC

Role-Based Access Control (RBAC) can be applied at every level within workspaces, dashboards, reports, applications, records, and fields ensuring only the appropriate users have access to data within Turbine.

Secure APIs

APIs are accessible to all Swimlane customers for seamless data access, ensuring system compatibility and smooth data transferability. Swimlane employs secure and standardized network protocols for data management and transfer to maintain high security and reliability.

Logging, Detection, and Response

Log Monitoring

Swimlane has implemented measures to protect and retain audit logs, monitor security events, and alert stakeholders as necessary. Access to audit logs is restricted to authorized individuals to ensure accountability. The Swimlane SOC analyzes logs for unusual activities and responds promptly to any anomalies detected. The time of all Swimlane systems is synchronized for consistency. Swimlane defines and periodically reviews the scope of

events that must be logged. The Swimlane security team generates audit records containing essential security details and protects these records from unauthorized interference. Swimlane has a well-established system for reporting anomalies, ensuring immediate notification of responsible parties.

Observability

The Swimlane security team collects metric information regarding Swimlane systems which include central processing unit (CPU) usage, memory usage, and latency. This information is stored in a database which can be graphed to set up alerts about specific thresholds. All audit logs are stored in an Elasticsearch, Logstash, and Kibana (ELK) stack which are also monitored. We utilize tools such as Cloud-Native Application Protection Platforms (CNAPP) to be able to detect any anomalous behavior in our systems.

Vulnerability Scans & Assessments

The Swimlane security and risk team has developed, and annually revised, policies to defend Swimlane-managed assets against malware. This includes established routine and emergency procedures for responding to vulnerabilities according to their risk levels. The Swimlane team updates detection tools and threat indicators regularly (at least weekly) and identifies updates for software that uses third-party or open-source libraries in line with the Swimlane Vulnerability Policy.

The Swimlane GRC team conducts annual independent third-party penetration tests of the web application. Daily vulnerability scans are run on cloud assets and corporate devices. Swimlane vulnerability fixes are prioritized using a risk-based approach and a recognized framework, with all vulnerability management activities, including stakeholder alerts, being tracked and communicated.

MDM & EDR

Devices connected to the Swimlane network are polled on an hourly basis and cross-referenced with our various mobile device management (MDM) and endpoint detection and response (EDR) solutions. The Swimane enterprise IT team uses these tools to ensure devices meet minimum requirements for anti-malware, encryption, operating systems (OS) versions, device locking policies, etc. The Swimlane SOC team manages all MDM and EDR alerts.

Threat Intelligence

Swimlane utilizes multiple public and private threat intelligence feeds to alert, enrich, hunt, and inform the security & GRC teams on current Indicators or Tactics, Techniques, and Procedures (TTPs) that could impact our operational risk management program. Multiple detect and prevent use cases are set up to accomplish this, which include the ingestion and enrichment of the following feeds.

- Weaponized domains and URLs
- Command and control
- Exploits in the wild
- Threat actor retro-hunts
- Known tor infrastructure
- Emerging & novel malware
- Active RAT C2 infrastructure
- Fast flux hosts
- Dynamic DNS hosts
- Potentially undetectable malware
- Potentially abused domains

Incident Response Plan

The Swimlane security team has established, and annually updated, policies for prompt and efficient handling of security incidents. Swimlane regularly performs a third-party gap assessment of our incident response plan to ensure its continuous improvement. The incident response plan involves all relevant parties, including Swimlane's supply chain, and is regularly tested and revised to ensure its continued effectiveness.

Swimlane monitors and assesses security incident metrics to improve response strategies. Processes for prioritizing and managing security events are in place, ensuring a structured approach to event triage. Swimlane has established procedures for notifying relevant parties of security breaches, in compliance with customer agreements and global regulations such as GDPR. Additionally, Swimlane maintains updated contact information for regulatory and law enforcement agencies to ensure timely communication in the event of an incident.

Bug Bounty Program

Swimlane utilizes OpenBugBounty to triage, validate, and process any web vulnerability findings on swimlane.com. Swimlane does not have a Bug Bounty Program for the Swimlane or Turbine automation platforms. See https://swimlane.com/.well-known/security.txt for further details.

Business Continuity and Disaster Recovery

Swimlane maintains a written BC/DR plan that documents the processes for triaging, remediating, and recovering from catastrophic incidents or disasters that may affect critical business processes. The BC/DR plan contains playbooks for stakeholder communication and restoration activities. The plan is reviewed, updated and approved annually. Swimlane performs and documents disaster recovery tabletop exercises which involve key personnel discussing simulated disaster scenarios in an informal setting to assess the effectiveness of the plan, identify gaps, and improve response strategies. Additionally, Swimlane cloud backups are tested at least annually to verify data is accessible and readable.

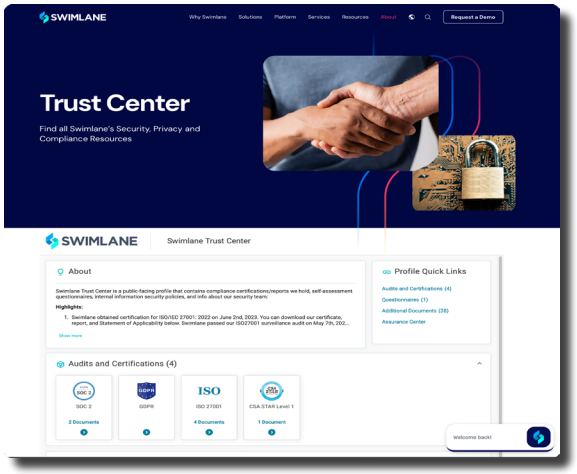
The Swimlane Shared Responsibility Model

Security is a shared responsibility between Swimlane, Amazon Web Services (AWS), and our customers. Customers should avoid sending any of the following types of sensitive personal information to Swimlane:

- government-issued identification numbers
- specific financial information, such as credit or debit card numbers, any related security codes or passwords, and bank account numbers
- information related to an individual's physical or mental health
- information related to the provision or payment of healthcare

Introducing the Swimlane Trust Center

Swimlane is committed to maintaining the highest levels of security and compliance to protect our customers' data and operations. For further information and documentation regarding our security measures, please visit the Swimlane Trust Center.



SWIMLANE

Swimlane is the leader in AI security automation. Swimlane unifies security operations in-and-beyond the SOC into a single system of record to reduce process and data fatigue while quantifying business value and security effectiveness. The cloud-scale Turbine platform combines human and machine data into actionable intelligence for security leaders. For more information, visit swimlane.com.