Stitchflow Security Whitepaper

Last revision: January 2024

Contents

Introduction

Stitchflow eliminates the grunt work involved in maintaining your Cloud IT environment by bringing all of your tools into a single pane of glass.

Stitchflow does this by integrating with 40+ IT-specific tools, no-code dashboards for every IT task, and the ability to share data, take bulk actions, and set alerts and automate repetitive tasks.

Stitchflow's implementation of security & compliance controls offer significant advantages to its customers so they can improve their IT operations without compromising on security. In this paper, we will cover how Stitchflow approaches the following areas of :

- Security Governance
- Data Center Security
- Compliance & Privacy
- Vendor Risk Management
- Personnel Security
- Product Security

Security Governance

Dedicated Security Team

Stitchflow has a security committee that partners with security personnel to provide oversight and strategic decision-making. The team includes a dedicated security lead responsible for corporate security & compliance.

The security committee team proactively:

- Pursues strategies to develop secure applications, ensure the security of the SaaS infrastructure, and establish protected and stable data storage
- Is a stakeholder in the software development lifecycle process with approval authority for code review and proper release management
- Mitigates security risk to the environment through outreach, awareness, assessment, policy, and best practices
- Participates in monitoring of systems and infrastructure to protect against and detect malicious activity
- Audits the environment identifies vulnerabilities, and recommends resolution strategies
- Responds to security events to contain the incident and improve protocols

The security leadership committee at Stitchflow drives continuous assessment and improvement of Stitchflow's security program and fosters a security culture within the organization.

Incident Management

Stitchflow’s engineering team includes dedicated incident management resources to effectively respond to and handle security and operational issues. Incident response procedures are defined, documented, and approved by management. We're proactive about monitoring security and operational incidents.

Data Center Security

Stitchflow is delivered using state-of-the-art, innovative architectural and engineering approaches. Cloud computing technologies are utilized from Google Cloud Platform data centers in the United States.

Physical Security

The data center facilities have implemented a robust physical security and environmental protection program to ensure adequate safeguards for equipment. The facilities are located in non-descript locations, maintain professional security guard personnel 24 hours a day with video surveillance monitoring, and feature electronic access controls to control access at the perimeter and building ingress points.

Environmental Security

Environmental protections prevent impact from fire, loss of power, flood, humidity, and temperature changes. This includes automatic fire detection and suppression equipment, uninterruptible power supply (UPS) units for backup power in the event of an electrical failure, climate control to maintain atmospheric conditions at optimal levels, and leakage detection and removal mechanism.

Data Center Compliance

Google Cloud Platform has achieved and continues to maintain a multitude of certifications, compliance, and attestations for globally recognized laws, regulations, and frameworks.

An independent third-party auditor has granted Google Cloud Platform a formal certification, attestation, or audit report based on an assessment that affirms compliance with ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701, SOC 1/SSAE 16/ISAE 3402 (formerly SAS70), SOC 2, SOC 3, PCI DSS, HITRUST CSF, FIPS 140-2 Validated, FedRAMP among others. To learn more about Google Cloud Platform compliance programs, please visit https://cloud.google.com/security/compliance.

Compliance & Privacy

Stitchflow was designed to comply with global data protection regulations and is compliant with major regulatory requirements out of the box. Stitchflow has chosen the AICPA's SOC2 framework as the basis for its security & compliance program with control criteria including security, confidentiality, and availability.

Service Organization Controls (SOC)

Stitchflow's leadership team has adopted a security control governance model consistent with the SOC 2 audit standard. Stitchflow has engaged an independent auditor to evaluate its conformance with the trust services criteria relevant to security, availability, and confidentiality as set forth in the 2017 Trust Services Criteria for Security, Availability, and Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Stitchflow is SOC 2 Type II compliant and plans to engage in annual audits. Stitchflow's leadership team is committed to partnering with trusted leaders in the cybersecurity industry to further support Stitchflow's information security and risk management strategy.

Privacy Regulations

Among the global privacy & data security requirements that Stitchflow tracks, the European Union's General Data Protection Regulation and California Consumer Privacy Act are a core focus.

Stitchflow has employed legal counsel and privacy experts to help build a foundation for a privacy program that considers existing and emerging laws and regulations aimed to protect consumer personal information.

Vendor Risk Management

Stitchflow expects critical vendors to observe industry standard security practices and, where applicable, provide assurance that they comply with global privacy regulations. Stitchflow's security team has implemented a process to evaluate the security posture of its data centers and service providers used in delivering the Stitchflow service. All vendors are subject to a risk assessment and annual review of security, however, different focus and scrutiny are applied based on the service being provided by the vendor.

If a review has identified a potential risk to customers or other areas of concern, Stitchflow will work closely with the vendor to develop a remediation plan. For a list of Stitchflow's current data centers and service providers used in delivering the Stitchflow service, please reach out to the security team at security@stitchflow.io.

Personnel Security

Stitchflow's security strategy starts with our people. Our recruiting process was developed to ensure we attract and retain a competitive workforce that prioritizes secure development and data security while mitigating the risks of code loss or data mishandling. To those ends, we have incorporated the following:

Background Checks

We pride ourselves on recruiting highly capable and qualified people at Stitchflow. We also recognize that people are a critical part of upholding a secure environment. When each new employee joins Stitchflow, a background check is completed prior to granting access to company systems.

Security and Privacy Training

All employees are required to participate in an Information Security and Privacy orientation when hired and annually thereafter. Awareness training provides our staff with skills to prevent, detect and respond to common security threats and includes topics such as password management, phishing, social engineering, physical security, data security, global privacy regulations and how to report security incidents.

New hires are required to acknowledge corporate policies, including their expectations regarding their conduct, and sign non-disclosure agreements as part of their onboarding process to ensure they understand their responsibilities while performing work for Stitchflow.

Access Control

Internal user accesses are granted using a role-based access control model that follows the least-privilege principle and requires a documented request and approval. We observe a similar procedure to manage access for individual contractors that perform work on behalf of Stitchflow and require access to corporate systems.

If an employee or contractor changes roles, their access is reviewed to ensure excess privileges are removed. In the event that an employee is terminated, access is removed.

User entitlement reviews are performed quarterly for privileged accounts and every 6 months for non-privileged accounts for critical systems, applications and infrastructure. User access reviews are focused on identifying access errors, removing overlapping or excessive permissions, and removing orphaned accounts.

Product Security

Stitchflow incorporates application security by design, allowing Stitchflow customers to build natively secured applications. Key aspects include:

Multi-factor Authentication

With multi-factor authentication (MFA) support for the Stitchflow, customers can secure their environment by requiring a second layer of identity verification at sign-in using one-time password (OTP) applications such as Google Authenticator.

Encryption

To protect data in transit between users and Stitchflow servers, Stitchflow uses Transport Layer Security (TLS) version 1.2 or better, creating a secure data transmission. Connections to the service that do not utilize this level of encryption are not permitted.

Data uploaded to the Stitchflow service is encrypted at rest using AES-256 in primary and backup data stores. Data storage spans multiple data centers to provide fault-resistant availability.

Access and Authentication

Stitchflow brings cloud-native IT management that leverages both built-in fine-grained security as well as standards-based authentication.

- Role-based access authorization and privilege management restrict a user's access to data and actions within the application
- Native authentication via 3rd-party market leaders
    - Out-of-the-box integration with Google Workspace Single Sign-On (SSO) integration

Penetration Testing

Stitchflow engages third party firms to perform annual penetration testing against its applications to evaluate the defenses against the most critical security risks for web applications. If a vulnerability is detected or other security concern, please report your findings immediately to security@stitchflow.io.

Conclusion

Stitchflow was founded by engineers and product visionaries who believe in the need for security as a core business tenet and is led by an executive team that has built products where security is paramount. At Stitchflow, we prioritize continuing work on our security practices to ensure that, as our product evolves, it continues to offer best-in-class safeguards for customer data.