Pneumatic

Security White Paper

2024

Pneumatic Data Center and Network Security

Physical Security Overview

Infrastructure Hosting & Management

Pneumatic's infrastructure is securely hosted on and managed by Google Cloud. This partnership leverages Google's state-of-the-art data center technology and management, ensuring high levels of reliability and compliance with industry standards. Google is recognized globally for its risk management capabilities and adheres to standards such as ISO 27001, SOC 1 and 2, PCI Level 1, FISMA Moderate, and SOX.

On-site Security Measures

The physical security of our data centers, certified under ISO 27001 and FISMA, includes military-grade perimeter controls, natural boundaries, and nondescript building designs to prevent unauthorized access. Access control is enforced rigorously through professional security guards, surveillance cameras, and advanced intrusion detection systems. Authorized staff undergo multi-factor authentication multiple times for data center access, while visitors are escorted at all times.

Data Center Locations

Our data centers are strategically located within the United States(Oregon) to optimize performance and security.

Pneumatic Data Center and Network Security

Network Security Protocols

Security Response Team

A dedicated team is on standby to address security concerns, reachable via security@pneumatic.app.

Firewall Management

Our network is protected by Google Cloud's firewall systems, which govern access based on specific business needs and security policies. This includes host-based firewalls for added protection and measures to prevent spoofing and sniffing attacks.

Vulnerability Management

Regular security assessments by specialized software platforms ensure ongoing security improvements. Our infrastructure is designed to prevent unauthorized access, including packet sniffing and port scanning, with every incident being thoroughly investigated.

Pneumatic Data Center and Network Security

Network Security Protocols

Penetration Testing and Vulnerability Assessments

Our service provider is security-tested by independent security firms on a regular basis. Findings of all such assessments are reviewed with the assessors, all identified risks are ranked and action is taken to minimize them.

Incident Response

In the event of a security incident, our engineers analyze extensive system logs to address and mitigate the issue promptly.

DDoS Mitigation

Our service provider(Google Cloud) employs advanced DDoS mitigation techniques, such as TCP Syn cookies and connection rate limiting, to protect against denial-of-service attacks.

Logical Access

Production network access is tightly controlled and audited, with multi-factor authentication required for all staff.

Pneumatic Data Center and Network Security

Availability and Continuity

System uptime

Pneumatic maintains an uptime of 99.9%, with ongoing monitoring. Detailed reports are available upon request.

Redundancy and Disaster Recovery

Google Cloud's infrastructure eliminates single points of failure and ensures rapid recovery in the event of an outage, automatically restoring customer applications and databases.

Application Security

Secure Development (SDLC)

Development Practices

Continuous Integration (CI) is implemented via product versioning (Git + Atlassian Bitbucket), the writing of tests, continuous integration with the main product branch, automated testing of new versions (using Ansible + Docker + Jenkins), plus manual E2E and smoke testing by QA before new product versions are deployed.

QA

Our QA department reviews and tests our code base. Dedicated application engineers on staff identify, test, and triage security vulnerabilities in code.

Application Security

Application Vulnerabilities

Code Security

Ongoing static code analysis helps identify and address security vulnerabilities in our codebase.

Product Security Features

Secure Development (SDLC)

IAM

Identity and Access Management are supported.

SAML2

SSO Security Assertion Markup Language is supported.

Others

Two-factor, MFA, and other authorization methods provided by authorization providers (Google, Microsoft, SSO) are integrated through the most secure OAuth 2 Authorization Code Flow at the server level.

Role-based Access Control

Role-based access control utilizes access control lists, meaning that all users have roles at different access levels and before a user can perform any action on an entity, the list of permitted operations that user can perform on that entity is checked. The principle of least privilege is followed at every level.

Transmission Security

All communications with Pneumatic's service provider servers are encrypted using industry standard HTTPS. This ensures that all traffic between you and Pneumatic is secure during transit.

Additional Security Methodologies

Security Awareness

Security Awareness and Training

We have comprehensive security policies in place and conduct regular training and awareness programs for all employees and contractors.

Training

All new employees receive requisite security training. Security Awareness is also part of Pneumatic's routine as updates are shared between all the teams via email, blog posts and in presentations during internal events.

Additional Security Methodologies

Employee Vetting

Background checks

Pneumatic performs background checks on all new employees in accordance with local laws. The background check includes Criminal, Education, and Employment verification.

NDAs

All new hires are screened through the hiring process and required to sign Non-Disclosure and Confidentiality agreements in accordance with local laws.

Pneumatic

pneumatic.app

8350 N Central Expy, Suite 1900, Dallas, TX 75206
support@pneumatic.app