

# Panguard AI - soc2 Compliance Report

## SOC 2 Trust Services Criteria

---

Generated: 2026-05-19

Organization: Acme Corp (Sample)

# Executive Summary

---

## Overall Compliance Score: 55%

Total Controls: 10  
Passed: 4 | Failed: 3 | Partial: 3 | N/A: 0  
Total Findings: 5  
Critical: 0 | High: 2

### Key Risks:

- System Boundary Protection
- Transmission Encryption
- Anomaly Detection

### Key Achievements:

- 4 controls fully compliant
  - No critical findings
-

# Findings

---

HIGH

FW-001

## Firewall disabled

macOS Application Firewall is disabled. System is exposed to inbound connections.

---

HIGH

NET-PORT-001

## Risky services exposed

The following services are listening on network interfaces: Redis (6379), Redis (6379), PostgreSQL (5432), PostgreSQL (5432). These should be firewalled or disabled.

---

MEDIUM

MON-LOG-002

## System logging may be impaired

Could not verify macOS unified log status.

---

MEDIUM

IR-NOTIFY-001

## No notification channels configured

Panguard has no notification channels (Telegram/Slack/Email) configured. Incident alerts cannot be delivered.

---

MEDIUM

PATCH-001

## 2 pending system updates

There are 2 pending macOS software updates. Security patches should be applied promptly.

---

# Compliance Overview

Control ID	Title	Status	Findings
CC6.1	Logical and Physical Access Controls	Pass	-
CC6.2	User Registration and Authorization	Pass	-
CC6.3	Access Removal and Modification	Pass	-
CC6.6	System Boundary Protection	Fail	2 findings
CC6.7	Transmission Encryption	Fail	1 finding
CC7.1	Infrastructure and Software Monitoring	Partial	1 finding
CC7.2	Anomaly Detection	Fail	2 findings
CC7.3	Security Event Evaluation	Partial	2 findings
CC7.4	Incident Response	Partial	1 finding
CC8.1	Change Management	Pass	-























