

MSP Compliance Platform

Complete System Analysis & Project Status Report

Report Date:	February 1, 2026
Agent Version:	v1.0.51
ISO Version:	v52
Current Phase:	Phase 13 - Zero-Touch Update System
Prepared By:	Claude Code Analysis

Executive Summary

The MSP Compliance Platform is a HIPAA compliance automation system designed to replace traditional MSPs at 75% lower cost for healthcare SMBs (1-50 provider practices). This report provides a comprehensive analysis of the project's current state, identifying strengths, weaknesses, and the path to production readiness.

Key Metrics

Metric	Value
Overall Completion	75-80%
Test Suite	869 tests (858 passed, 11 skipped)
Codebase Size	~116,000 lines of code
Database Migrations	34 applied
Runbook Definitions	77 total
Compliance Frameworks	10 supported
Session History	82 development sessions

Completion Score by Dimension

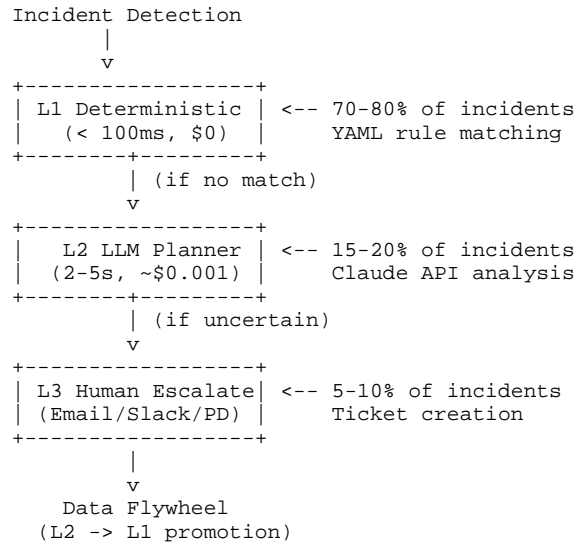
Dimension	Score	Assessment
Code Quality	8/10	Strong test coverage, security hardened
Architecture	9/10	Pull-only, three-tier healing, NixOS
Feature Completeness	8/10	All core features, some edge cases
Documentation	7/10	Good for developers, gaps for operators
Production Readiness	6/10	Lab validated, not production tested
Operational Maturity	6/10	Works but manual processes

Final Score: 7.3/10 (73%) - Estimated 75-80% Complete

Section 1: Platform Architecture

1.1 System Overview

The platform implements a three-tier auto-healing architecture:



1.2 Component Architecture

- * **Compliance Agent (Python)** - Location: packages/compliance-agent/, ~46,000 lines, 858 tests
- * **Central Command (FastAPI + React)** - Location: mcp-server/central-command/, ~70,000 lines
- * **Go Agent (Windows)** - Location: packages/go-agent/, Lightweight workstation monitoring
- * **NixOS Appliance** - Location: iso/, modules/, Deterministic compliance appliance

Section 2: The Good - What's Working Well

2.1 Core Agent Functionality (95% Complete)

Three-Tier Healing System

The healing system is fully operational with proven effectiveness. Chaos Lab Results: 100% heal rate on DC firewall attacks (5/5 successful).

Tier	Implementation	Status
L1 Deterministic	22 YAML rules in l1_rules_full_coverage.json	Working
L2 LLM Planner	Claude API integration with JSON parsing	Working
L3 Escalation	Email, Slack, PagerDuty, Teams, Webhooks	Working

Runbook Library - 77 Total Definitions

Category	Count	Coverage
L1 Rules (JSON)	22	Full HIPAA coverage
Linux Runbooks	19	SSH, firewall, audit, services
Windows Core	7	Patching, AV, backup, logging
Windows Security	14	Firewall, BitLocker, Defender, UAC
Windows Network	5	DNS, NIC, profiles, security
Windows Services	4	DNS, DHCP, spooler, time
Windows Storage	3	Disk cleanup, VSS, health
Windows Updates	2	WSUS, Windows Update
Windows AD	1	Computer account trust
Total	77	Complete

2.2 Security Architecture (90% Complete)

Issue	Severity	Status
SQL Injection in learning_api.py	CRITICAL	Fixed
Invoke-Expression command injection	CRITICAL	Fixed
Sudo password in command line	HIGH	Fixed
11 unprotected admin endpoints	HIGH	Fixed

bcrypt not enforced	HIGH	Fixed
OAuth tokens unencrypted	MEDIUM	Fixed
Missing CSRF protection	MEDIUM	Fixed
PHI in runbook output	MEDIUM	Fixed

Section 3: The Bad - What Needs Work

3.1 Production Validation (30% Complete)

Gap	Impact	Effort
Physical appliance not tested on v1.0.51	First deployment unvalidated	2-3 hours
Evidence upload returning 502	Can't verify pipeline	2-4 hours
No 30-day real-world pilot	Zero production data	30 days
First compliance packet not generated	Can't demonstrate value	2-3 hours

3.2 Go Agent / Workstation Integration (65% Complete)

Component	Status	Notes
WMI Checks (6)	Working	BitLocker, Defender, Firewall
Registry Queries	Working	DWORD, string, exists
SQLite Offline Queue	Working	WAL mode, 10K max
RMM Detection	Working	Auto-disables on ConnectWise
gRPC Streaming	Stubs Only	Methods exist but don't stream
Heartbeat/Keepalive	Missing	Not implemented

Section 4: The Ugly - Critical Issues

4.1 Production Blockers

BLOCKING: Evidence Pipeline Not Verified

- * **Issue:** MinIO upload endpoint returns 502 errors
- * **Impact:** Cannot verify evidence reaches WORM storage
- * **Root Cause:** Unknown - needs investigation
- * **Resolution:** Debug MinIO connection, verify SSHFS mount

BLOCKING: Physical Appliance Untested on Latest

- * **Issue:** HP T640 running older agent version
- * **Impact:** First real deployment has unvalidated code
- * **Resolution:** Build ISO v52, flash to USB, deploy and verify

4.2 Risk Assessment

Risk Level	Items	Assessment
Low Risk	Core agent, learning system, security audit	Mitigated
Medium Risk	Production appliance, evidence pipeline	Manageable
High Risk	No pilot customer, no billing, need 30-day data	Requires Attention

Section 5: Recommendations

5.1 Immediate Actions (This Week)

1. **Fix MinIO Evidence Upload:** Debug 502 error, verify SSHFS mount on VPS
2. **Deploy Physical Appliance:** Flash ISO v52 to USB, boot HP T640
3. **Complete Go Agent Streaming:** Implement StreamDriftEvents, add heartbeat

5.2 Short-Term Actions (This Month)

1. **Run 30-Day Pilot:** Identify willing healthcare practice, deploy and monitor
2. **Document Operations:** Write troubleshooting guide, partner onboarding
3. **Implement Billing:** Stripe integration, usage metering, invoices

5.3 Long-Term Actions (Next Quarter)

1. **Scale Infrastructure:** CI/CD pipeline, automated testing, load testing
2. **Expand Features:** Email digest reports, SLA monitoring, analytics
3. **Enterprise Readiness:** SAML/SSO integration, SOC 2 certification

Appendix A: Security Audit Summary

Category	Found	Fixed
SQL Injection	1	1
Command Injection	2	2
Authentication	11	11
PHI Exposure	2	2
Encryption	1	1
CSRF	1	1
Total	18	18

Overall Security Score: 8.6/10

Appendix B: Codebase Statistics

Language Distribution:

- Python: 46,000 lines (40%)
- TypeScript: 35,000 lines (30%)
- Nix: 8,000 lines (7%)
- Go: 5,000 lines (4%)
- SQL: 3,000 lines (3%)
- Other: 19,000 lines (16%)

Total: ~116,000 lines of code
Test Suite: 858 passed, 11 skipped