System Monitoring Architecture Guide

Summit Digital Solutions, Inc.

Document Version: 2.4

Last Updated: January 9, 2024

Classification: Confidential

1. Introduction and Scope

1. This System Monitoring Architecture Guide ("Guide") sets forth the authorized system monitoring architecture, protocols, and security requirements for Summit Digital Solutions, Inc.'s ("Company") Peak Performance Platform(TM) and related monitoring infrastructure.

2. This Guide governs all monitoring components deployed within client environments and applies to all Company personnel, contractors, and authorized third parties involved in system monitoring activities.

2. Monitoring Architecture Overview

1. Core Components

- Central Monitoring Server (CMS)
- Distributed Collection Agents (DCAs)
- Analytics Processing Engine (APE)
- Secure Data Storage Layer (SDSL)
- Real-time Alert Management System (RAMS)

2. Architecture Topology

The monitoring architecture employs a hierarchical structure with the following layers:

- Layer 1: Edge Collection (Client Environment)
- Layer 2: Regional Aggregation
- Layer 3: Central Processing
- Layer 4: Enterprise Storage

3. Security and Access Controls

1. Authentication Requirements

- Multi-factor authentication mandatory for all monitoring system access
- Role-based access control (RBAC) implementation
- Minimum 2048-bit SSL/TLS encryption for all data transmission
- PKI infrastructure for client-server authentication

2. Data Protection

- AES-256 encryption for data at rest
- Secure key management system with rotation every 90 days
- Segregated client data stores with logical partitioning

4. Monitoring Protocols

1. Data Collection

- Maximum sampling rate: 1000 samples per second
- Minimum collection interval: 5 seconds
- Buffer size: 256MB per collection agent
- Compression ratio: 10:1 minimum

2. Alert Thresholds

- Critical: Response required within 5 minutes
- High: Response required within 15 minutes
- Medium: Response required within 1 hour
- Low: Response required within 24 hours

5. Compliance and Audit

1. Logging Requirements

- All system access must be logged
- Retention period: 365 days minimum
- Tamper-evident logging mechanism
- Regular log rotation and archival

2. Audit Trail

- Complete audit history of configuration changes

- User activity tracking
- System performance metrics
- Security event logging

6. Disaster Recovery

1. Backup Requirements

- Full system backup every 24 hours
- Incremental backups every 4 hours
- Offsite replication with 15-minute RPO
- Recovery time objective (RTO): 2 hours

2. Failover Procedures

- Automated failover to secondary monitoring infrastructure
- Geographic redundancy across three data centers
- Hot standby configuration for critical components

7. Maintenance and Updates

1. Scheduled Maintenance

- Monthly maintenance window: Second Sunday, 02:00-06:00 EST
- Advance notification required: 5 business days
- Rolling updates to prevent service interruption

2. Version Control

- All monitoring components must maintain version compatibility
- Maximum version deviation: 2 minor releases
- Automated version verification system

8. Legal Disclaimers

1. This Guide contains confidential and proprietary information of Summit Digital Solutions, Inc. and may not be reproduced or disclosed without prior written authorization.

2. The monitoring architecture described herein is protected by U.S. Patents #9,876,543 and #10,234,567 and corresponding international patents.

3. Summit Digital Solutions makes no warranties, express or implied, regarding the performance or reliability of the monitoring system beyond those explicitly stated in the Master Services Agreement.

9. Document Control

Approved by:

- Chief Technology Officer
- Chief Information Security Officer
- Chief Legal Officer

Document Owner: Enterprise Architecture Team

Review Cycle: Annual

Next Review Date: January 9, 2025

End of Document

PROPRIETARY AND CONFIDENTIAL