Network Security Architecture & Data Flow Diagrams

Summit Digital Solutions, Inc.

Document Classification: CONFIDENTIAL

Last Updated: January 9, 2024

Version: 3.2

1. Introduction & Scope

This document details the network security architecture and data flow diagrams for Summit Digital Solutions, Inc.'s ("Company") core technology infrastructure, including the Peak Performance Platform and associated enterprise systems. This documentation is considered confidential and proprietary information of the Company.

2. Network Security Architecture Overview

2.1 Physical Infrastructure

The Company maintains primary data center operations in AWS US-East-1 (Virginia) and US-West-2 (Oregon) regions, with disaster recovery capabilities in EU-Central-1 (Frankfurt). All data centers maintain SOC 2 Type II and ISO 27001 certifications.

2.2 Network Segmentation

The network architecture implements the following security zones:

- DMZ (Public-facing services)
- Application Zone (Web/API servers)
- Data Zone (Database clusters)
- Management Zone (Administrative access)
- IoT Gateway Zone (Sensor data ingestion)
- Analytics Zone (ML/AI processing)

2.3 Security Controls

Primary security controls include:

- Next-generation firewalls (Palo Alto Networks)
- Web Application Firewalls (AWS WAF)
- Intrusion Detection/Prevention Systems (IDS/IPS)

- DDoS protection (AWS Shield Advanced)
- Zero Trust Network Access (ZTNA) implementation
- Multi-factor authentication (MFA) enforcement

3. Data Flow Architecture

3.1 Client Data Ingestion

a) Web Application Data

- TLS 1.3 encryption for all client connections
- API Gateway with request validation
- Rate limiting and anomaly detection
- Load balancing across application clusters

b) IoT Sensor Data

- Dedicated IoT gateway infrastructure
- MQTT protocol with TLS encryption
- Device authentication via X.509 certificates
- Edge preprocessing capabilities

3.2 Internal Data Processing

a) Peak Performance Platform

- Microservices architecture with service mesh
- Event-driven processing via Apache Kafka
- Real-time analytics pipeline
- Automated scaling based on workload

b) Machine Learning Operations

- Containerized ML model deployment
- GPU cluster for training workloads
- Model versioning and A/B testing
- Automated retraining pipelines

3.3 Data Storage

a) Operational Data

- Multi-region database clusters
- Automated backup and recovery
- Point-in-time recovery capability
- Data encryption at rest (AES-256)

b) Analytics Data

- Data lake implementation (S3 + Athena)
- Data warehouse (Snowflake)
- Time-series optimization
- Retention policy enforcement

4. Security Monitoring & Response

4.1 Security Information and Event Management (SIEM)

- 24/7 Security Operations Center (SOC)
- Log aggregation and correlation
- Real-time threat detection
- Automated incident response playbooks

4.2 Compliance Monitoring

- Continuous compliance scanning
- Configuration drift detection
- Automated policy enforcement
- Regular security assessments

5. Disaster Recovery & Business Continuity

5.1 Recovery Objectives

- RPO (Recovery Point Objective): 15 minutes
- RTO (Recovery Time Objective): 4 hours
- Regular DR testing and validation
- Automated failover capabilities

5.2 Backup Strategy

- Multi-region data replication
- Daily incremental backups
- Weekly full backups
- 90-day retention period

6. Legal Disclaimers

This document contains confidential and proprietary information of Summit Digital Solutions, Inc. The architecture and systems described herein are protected by various intellectual property rights. Any unauthorized disclosure, copying, or distribution is strictly prohibited and may result in civil and criminal penalties.

The security controls and architectures described in this document are subject to change based on evolving security requirements and threat landscape. The Company reserves the right to modify any aspect of the security architecture without prior notice.

7. Document Control

Document Owner: Chief Technology Officer

Security Classification: Confidential

Review Frequency: Quarterly

Next Review Date: April 9, 2024

8. Approval

APPROVED BY:

Michael Chang

Chief Technology Officer

Summit Digital Solutions, Inc.

Date: January 9, 2024

James Henderson

Chief Digital Officer

Summit Digital Solutions, Inc.

Date: January 9, 2024