Introduction

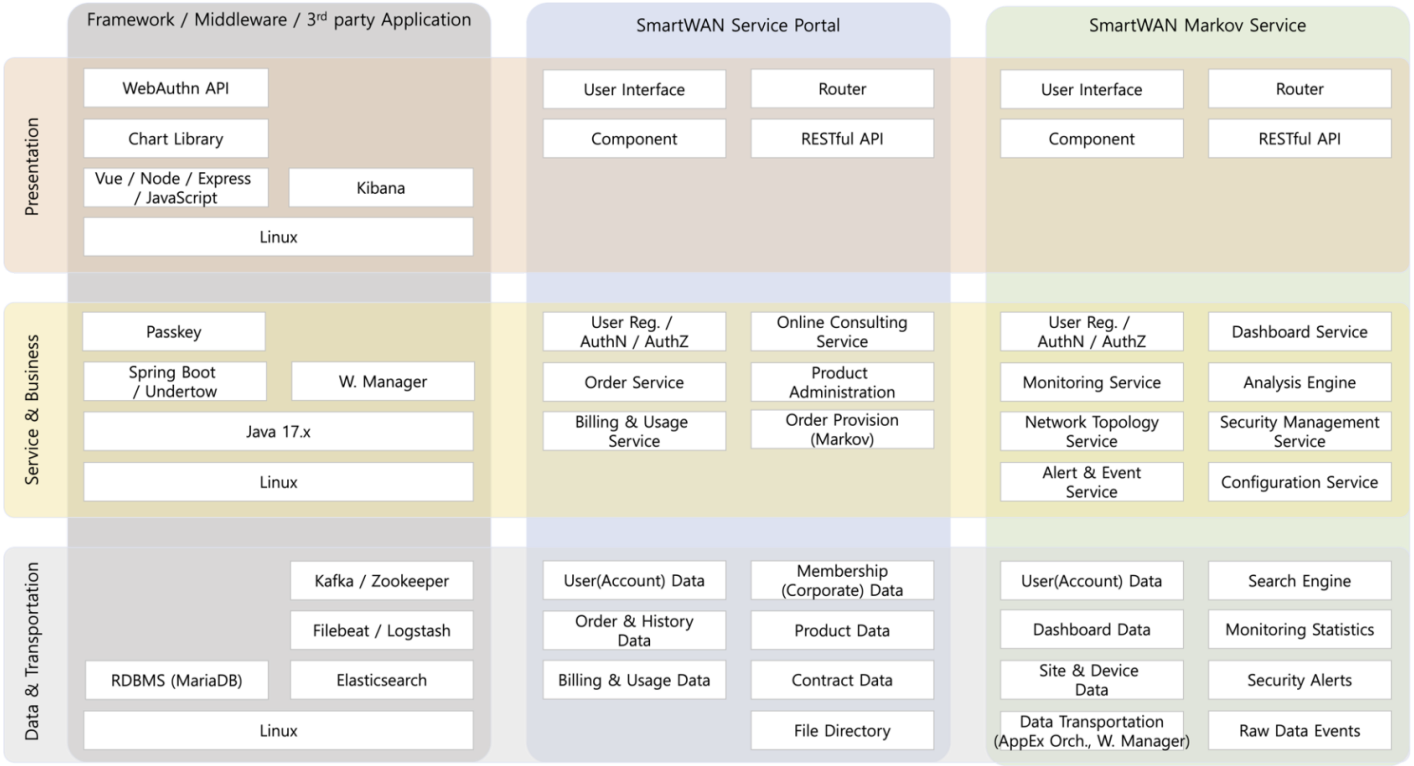
> This document will be continuously updated, and not all the features presented may be fully implemented.
> Some parts of the content are based on the Markov project.

Overview

Unified Security Platform is to provide real-time security monitoring and response services to the customers.
This document describes the key concepts of the platform and provides key features under development.

Architecture

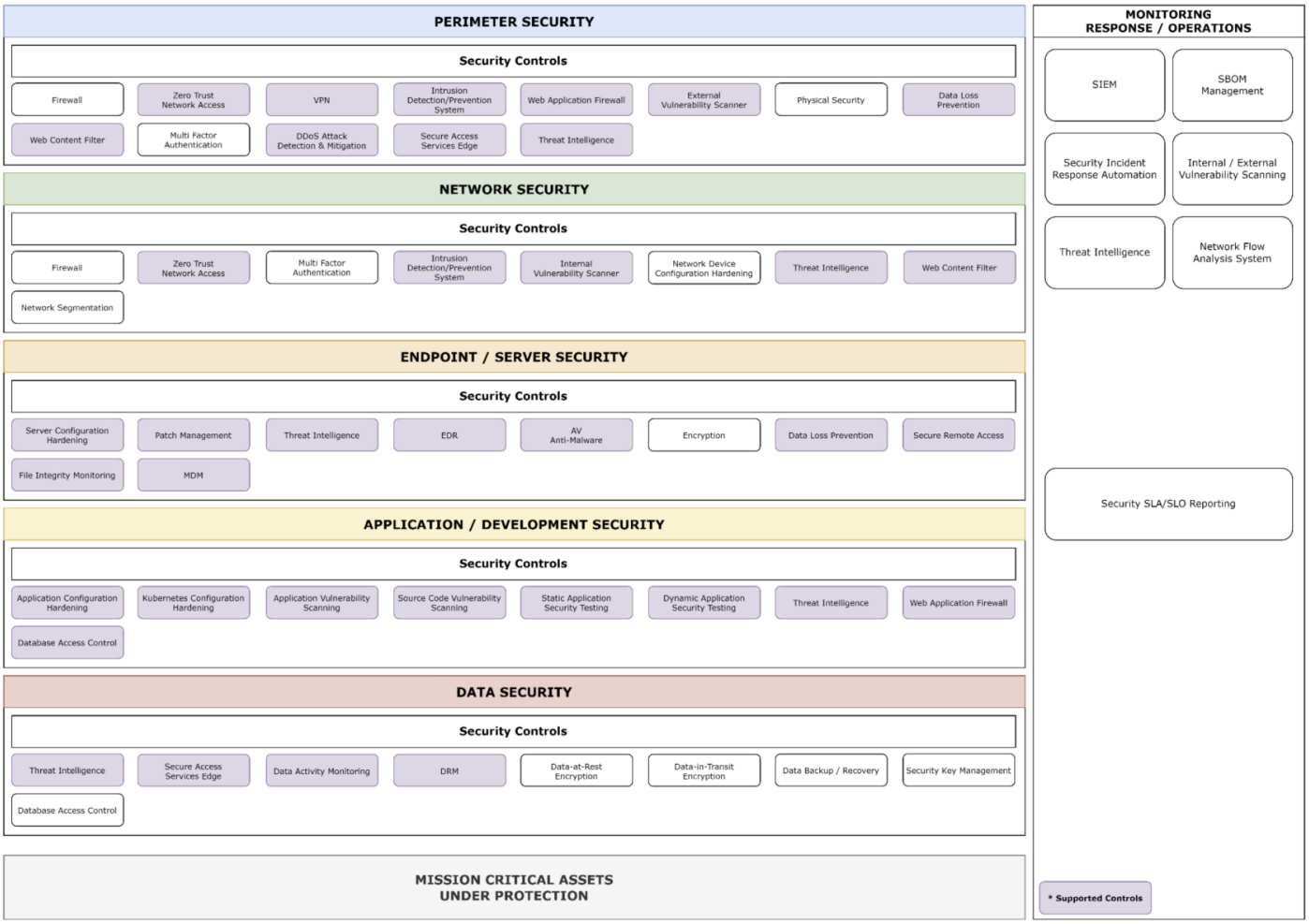
Technical Architecture



This diagram illustrates the end-to-end architecture of the SmartWAN service platform, integrating presentation, business logic, and data layers. The system leverages modern technologies including Vue.js/Spring Boot for frontend/backend, Kafka for real-time data streaming, and Elasticsearch for

analytics. All services are deployed on Linux environments, with RESTful APIs enabling seamless communication between modules.

Defense-in-Depth security model



This architecture diagram maps the key security controls required in each layer of the Defense-in-Depth security model and illustrates how they are supported by this integrated security platform.

The platform is capable of collecting and monitoring logs generated from the security controls highlighted in purple within each layer.

This visual representation clearly demonstrates the scope and capabilities of the integrated security platform across the various layers of the Defense-in-Depth model.

Key Concepts of the Platform

Unified Security Monitoring

The platform integrates traditional on-premises data center security features with cloud environment security capabilities, enabling comprehensive monitoring from a single, unified interface.

This convergence allows customers to maintain consistent security visibility across hybrid infrastructures.

Versatile Data Collection and Analysis

Employing both agent-based and agentless approaches, the platform collects a wide array of log data and vulnerability assessment information.
This multi-faceted data gathering strategy enables thorough security analysis, providing a comprehensive view of the customer’s security posture.

Advanced Security Data Lake

Leveraging a high-performance security data lake capable of sub-second queries on multi-terabyte datasets, the platform offers sophisticated security analytics for network flows.
This capability surpasses traditional security monitoring platforms, providing deep insights into network behavior from a security perspective.

Proactive Security Management

The system incorporates robust vulnerability management features through active security configuration checks and vulnerability identification.
This proactive approach helps customers identify and address potential security weaknesses before they can be exploited.

Streamlined Compliance Management

Offering key compliance management functionalities, the platform facilitates efficient management of compliance evidence.
This feature simplifies the process of meeting regulatory requirements and maintaining audit readiness across various compliance frameworks.

Revision #1
Created 28 April 2025 13:05:43 by □□□
Updated 28 April 2025 13:11:02 by □□□