

# DeepShield Platform Scalability Architecture

## CONFIDENTIAL AND PROPRIETARY

Document Version: 3.2

Last Updated: January 11, 2024

### 1. Introduction and Purpose

1. This Platform Scalability Architecture document ("Architecture Document") sets forth the technical and operational framework for the scalability components of the DeepShield Industrial Control System Security Platform (the "Platform"), as developed and maintained by DeepShield Systems, Inc. ("Company").
2. This document is intended for internal use and authorized third parties under appropriate confidentiality obligations. All rights reserved. Unauthorized reproduction or distribution is strictly prohibited.

### 2. Definitions

1. "Core Platform" means the foundational DeepShield security infrastructure, including the base threat detection engine, OT network monitoring system, and incident response framework.
2. "Scaling Units" means discrete computational and storage resources that can be dynamically allocated to support Platform operations.
3. "Node Cluster" means a collection of interconnected processing nodes that function as a single system for workload distribution.
4. "Maritime Module" means the specialized Platform component designed for maritime and subsea infrastructure protection.

### 3. Architecture Overview

1. The Platform employs a distributed microservices architecture with the following key components:
  - a) Central Control Plane
  - b) Distributed Processing Nodes
  - c) Elastic Storage Layer

- d) Load Distribution Matrix
- e) Redundant Communication Channels

2. Each component is designed to scale independently while maintaining system integrity and security compliance requirements.

## **4. Scaling Mechanisms**

### **1. Horizontal Scaling**

1.1. The Platform implements automatic horizontal scaling through containerized workload distribution.

1.2. New Node Clusters can be provisioned within 180 seconds of triggering conditions being met.

1.3. Maximum cluster size is limited to 256 nodes per geographic region.

### **2. Vertical Scaling**

2.1. Individual nodes can scale vertically up to 64 CPU cores and 512GB RAM.

2.2. Storage capacity scales from 1TB to 64TB per node.

## **5. Performance Parameters**

1. The Platform shall maintain the following performance metrics during scaling operations:

- a) Maximum latency: 50ms for critical operations
- b) Minimum throughput: 100,000 events per second per node
- c) Data consistency guarantee: 99.999%
- d) Recovery time objective (RTO): 120 seconds
- e) Recovery point objective (RPO): 10 seconds

## **6. Security Controls**

1. All scaling operations must maintain compliance with:

- 1.1. SOC 2 Type II requirements
- 1.2. ISO 27001 standards

- 1.3. NIST Cybersecurity Framework
- 1.4. Maritime cybersecurity regulations (BIMCO Guidelines)

2. Each Scaling Unit must implement:

- 2.1. End-to-end encryption (AES-256)
- 2.2. Hardware security module (HSM) integration
- 2.3. Real-time threat monitoring
- 2.4. Automated compliance validation

## **7. Operational Requirements**

1. The Platform must maintain operational continuity during scaling events through:

- 1.1. Zero-downtime deployment protocols
- 1.2. Rolling updates across Node Clusters
- 1.3. Automated failover mechanisms
- 1.4. Load balancing across geographic regions

2. All scaling operations must be logged and auditable for a minimum of 365 days.

## **8. Proprietary Rights**

1. This Architecture Document and all technologies, methodologies, and implementations described herein are the exclusive intellectual property of DeepShield Systems, Inc.

2. Patents pending: US2023/0123456, US2023/0123457, US2023/0123458

## **9. Document Control**

1. This document shall be reviewed and updated annually or upon material changes to the Platform architecture.

2. All modifications require approval from:

- Chief Technology Officer
- Chief Security Architect
- VP of Engineering

## **10. Execution**

IN WITNESS WHEREOF, the undersigned hereby confirms the accuracy and completeness of this Architecture Document as of the date first written above.

DEEPSHIELD SYSTEMS, INC.

**By:**

Name: Sarah Blackwood

Title: Chief Technology Officer

Date: January 11, 2024

**By:**

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date: January 11, 2024