

Vehere Bulk Interception Monitoring Center

For National Security Agencies



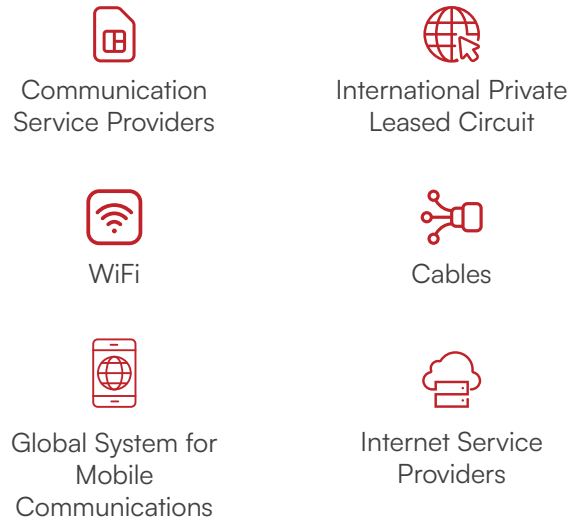
Introduction

Bulk interception is a critical capability that enables National Intelligence and Law Enforcement Agencies to lawfully monitor, analyze, and investigate communications traversing a country's domestic telecommunications infrastructure. Covering 2G, 3G, 4G, 5G cellular networks, fixed-line networks, broadband services, and IP-based communication platforms, the Vehere Bulk Interception Monitoring Center (BIMC) provides nationwide visibility across domestic communication flows. Operating within legally authorized and compliant frameworks, BIMC empowers authorized agencies to process massive communication volumes, uncover hidden networks, identify suspicious activities, and detect emerging threats with speed, precision, and actionable intelligence.

Core Intelligence and Monitoring Capabilities

- Bulk Voice and IP communication interception with selective target monitoring
- AI-assisted intelligence extraction, classification, and investigative analytics
- Unified collection across diverse SIGINT communication sources
- Entity resolution and identification across high-volume, heterogeneous datasets
- Cryptocurrency intelligence for illicit transaction tracing and threat attribution
- Cross-domain identity profiling through correlated shared identifiers
- Advanced behavioral analytics, link analysis, and anomaly detection
- Metadata enrichment and contextual intelligence correlation
- Encrypted traffic intelligence without payload decryption
- Flexible, scalable and cost-effective architecture for national intelligence deployments
- Secure on-premises deployment with complete data sovereignty
- Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), and comprehensive audit trails
- Flexible platform customization with 24×7 mission-critical technical support

Supported Networks



Key Highlights



Use Cases

- Domestic Communications Intelligence
- Counterterrorism and Extremist Network Detection
- Threat Network Discovery and Link Analysis
- Critical Infrastructure Protection
- National Security Surveillance and Strategic Warning

Objectives

- Detect Unknown Threat Actors and Hidden Communication Networks
- Provide Early Warning Through Bulk Communications Intelligence
- Accelerate Intelligence-Led Investigations and Threat Attribution
- Protect Critical National Infrastructure and Public Safety
- Enable Strategic, Operational, and Tactical Decision-Making

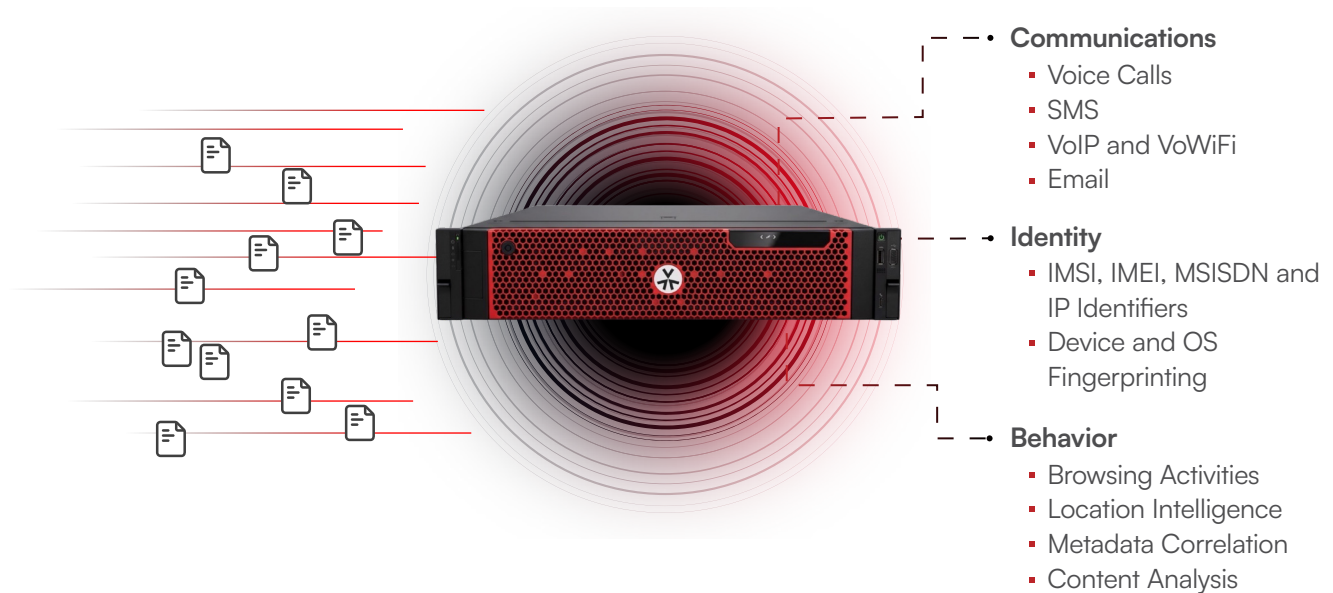


Fig: Intelligence Extracted out of Intercepted Bulk Data

Core Capabilities of Vehere Bulk Interception Monitoring Center



AI-powered Analytics

- AI-powered voice analysis delivers seamless language identification, translation, transcription, and speaker identification and diarization.
- AI-powered email analysis automates category classification and spam detection to significantly reduce operational workload.
- AI-powered behavior profiling to identify suspicious domain and communication patterns by detecting abnormal SIP activities and high-volume data transfers.
- AI-powered SMS Analysis for language identification, keyword extraction, and multilingual translation to accelerate intelligence analysis and investigative workflows.



Crypto Analysis

Detects and analyzes cryptocurrency activity by extracting blockchain- related data from network traffic, delivering detailed insights into transaction metadata and currency types to uncover illicit financial flows.



Visual Link Analysis

Helps identify connections between targets and groups by revealing complex network structures up to 6 layers.



Mass Profiling

Collects, correlates, and categorizes large datasets to detect patterns and anomalies through shared identifiers that may indicate suspicious activities. Identifies potential new leads based on similarity between profiles using location analytics, link analysis, SIGINT behavior and online activity indicators.

Mass Profiling Features and Analytics

- Suspicious behavior patterns
- Clear and encrypted associations
- Geolocation analytics
- Interests
- Routines and Anomalies



Audit Trail

Maintains a granular audit trail of all user interactions, including logins, data access, modifications, and exports to provide complete operational visibility, internal accountability, and regulatory compliance.



Geospatial Analysis

Drives actionable intelligence by visualizing intercepted data points on interactive maps for accurate target location tracking, geofencing, and heatmap generation.

Vehere Differentiators

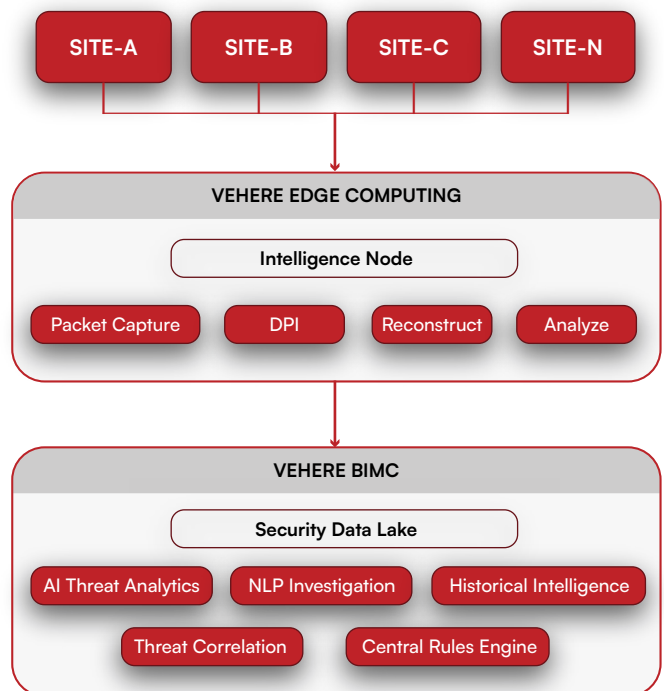
Edge Processing Architecture: Maximum processing in the front-end in terms of enrichment, decoding, and raw data storage, leading to utilization of low bandwidth links, faster query response time and reduced operational costs.

ULTRAHUNT: Target tracking at scale: Designed to manage and monitor 2 million concurrent targets in less than a millisecond

Compatible with any Hardware: Adaptable deployment as the software can be installed on customer- provided hardware (COTS) or on Vehere-certified hardware systems.

On-Premises by Design: Keeps sensitive interception data and communications intelligence within sovereign infrastructure, ensuring data sovereignty, security, access control, and retention while enabling low-latency, resilient processing for mission-critical bulk interception.

NEXT-GEN BULK INTERCEPTION DEPLOYMENT



Why is Vehere trusted by Defense and National Intelligence Agencies?



On-premises deployment with complete air-gapped data sovereignty



Protocol-agnostic architecture supporting 5000+ protocols



AI-powered Network Intelligence for language and speaker identification, text translation and summarization and email analysis



400+ metadata attributes help analyze encrypted IP traffic



Lossless continuous packet capture preserves every packet for complete visibility, investigation, and session reconstruction.



Terabit-speed packet capture with petabyte retrieval in seconds



Classification and concealment of sensitive information using advanced PII detection



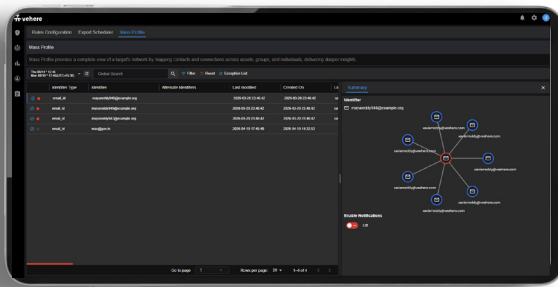
Seamless integration with third-party platforms



Granular forensic analysis to uncover evidence, timelines, associations, and anomalies

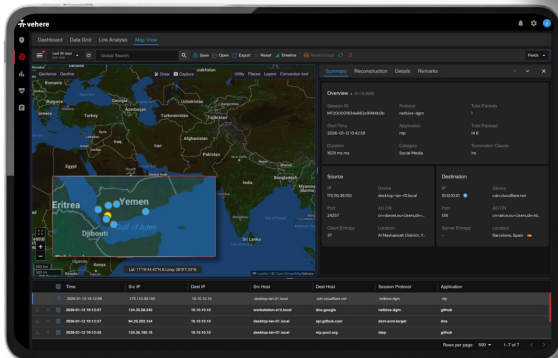
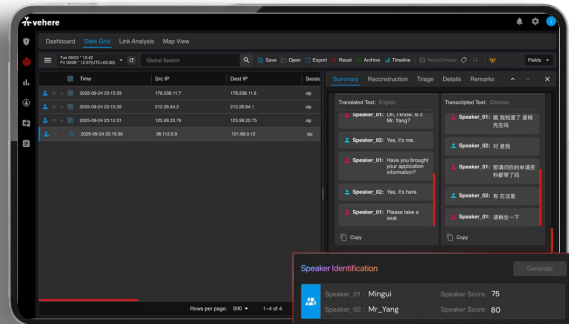


Supports wide range of bulk interception use-cases



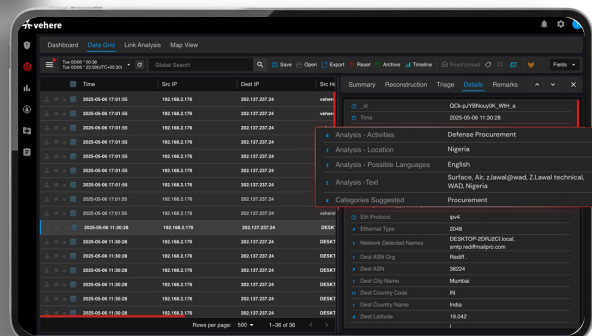
> Mass Profiling

AI-powered Speaker Identification <



> Geospatial Analysis

AI-powered Email Analysis <



About Vehere

Vehere is an AI cyber defense company operating at the intersection of national security and enterprise security. Our AI-powered Network Intelligence platform processes petabytes of network data at terabit speed, empowering government agencies with real-time intelligence, advanced analytics, and actionable insights. From preventing emerging threats to accelerating investigations, Vehere helps governments and law enforcement agencies protect national sovereignty and strengthen public safety.