REPERION

OPERATIONAL RESILIENCE. SECURED.

CORPORATE PRESENTATION

July 2023

NEXT GENERATION SECURITY TO PROTECT ASSETS FROM CYBER AND DRONE ATTACKS

Gray Zone Threats Are Multiplying

REPERION RESEARCH CONTINUES TO UNCOVER A DETERIORATING THREAT LANDSCAPE AND BROADENING ATTACK SURFACES

There is a growing focus on opportunities to attack transportation assets, industrial plants, and critical infrastructure using next-generation —

GRAY ZONE METHODS

that put people, assets, and the environment at risk

WHAT IS THE GRAY ZONE?

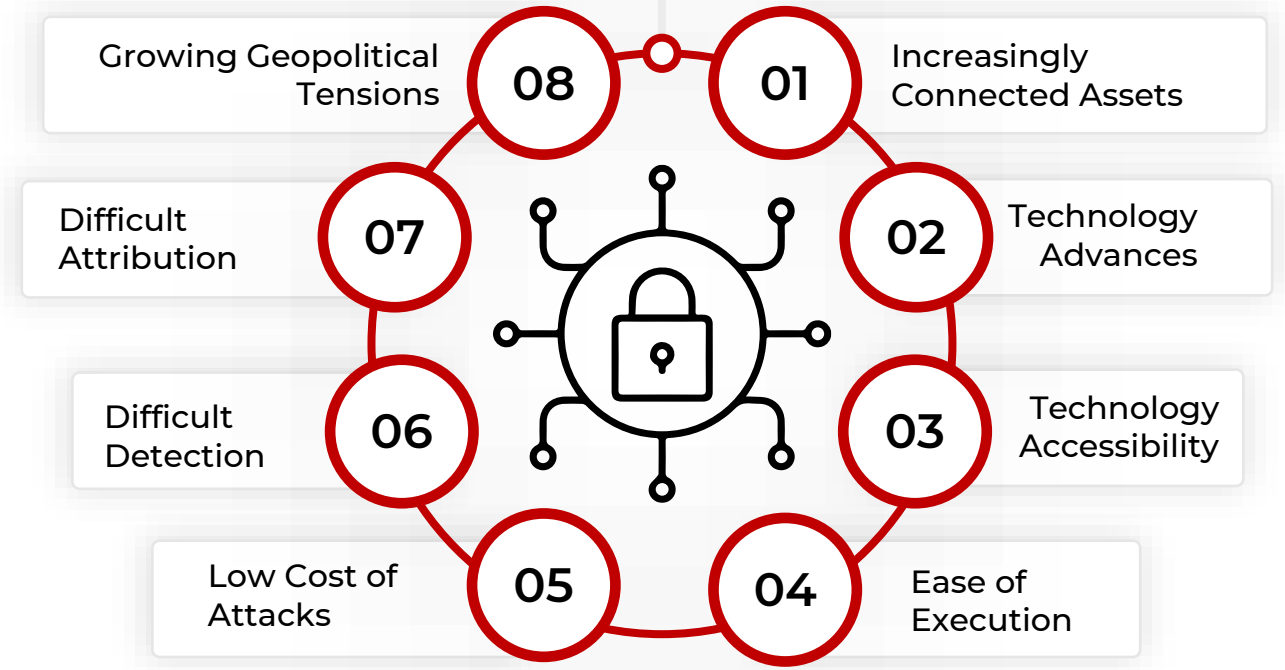
Ever-expanding space between peace and war in which unconventional means are used by state and non-state actors to achieve geopolitical objectives without escalation to armed conflict

Asset Owners And Operators Face A New Dimension of Risk

KEY GRAY ZONE ATTACK VECTORS

Cyber and drone attacks have become the most effective next generation attack vectors on transportation assets and critical infrastructure

KEY DRIVERS



Reperion is a next generation security business that protects transportation assets across sea, land, and air from cyber attacks and critical infrastructure from drone attacks

01

Protect People, Assets, And The Environment From Harm

02

Protect Companies From Financial, Reputational And Business Continuity Risks

Increasingly Costly, Complex, And Common Problems

One Vessel Grounding or Explosion
+$50-800 million

Vehicle Recall
+$1 billion
($500/vehicle)

Fleet Grounding
$500k/day
($20/scooter/day)

Drone Intrusion or Attack
+$1 billion

COLLATERAL RISKS:

LOSS OF LIFE, ENVIRONMENTAL DISASTER, BRAND VALUE DESTRUCTION, AND GEOPOLITICAL TENSIONS

Gray Zone Vulnerabilities Across Sea, Land, and Air

SEA

State-Sponsored GPS Spoofing

UK-flagged tanker Stena Impero, seized by Iranian forces in July after being spoofed to cause the vessel to shift course into Iranian waters.

Rivierramm.com, 30th August 2019

Coordinated Cyberattack

Six vessels simultaneously lost power and navigational control in the Gulf of Oman.

Times of Israel, 3rd August 2021

The Current Cyber Threat

The next Suez Canal blockage could be the result of a hack.

Bloomberg, 30th March 2021

LAND

Costly Vehicle Cyberattacks

US$200 million class action lawsuit settled by Hyundai and Kia to cover losses of over 8 million vehicle thefts using USB chargers.

Wall Street Journal, 19th May 2023

Another Tesla Hack

A Tesla Model 3 was hacked in under 2 minutes...the attack gave hackers deep access into subsystems that control the vehicle's safety...

InsideEVs.com, 27th March 2023

E-Scooter Theft

..each month thieves steal more than 15% of Spin's San Diego [e-scooter] fleet, about 150 of the roughly 900 the company deploys.

Los Angeles Times, 17th April 2023

AIR

Drone Attack on Vessel

Israel linked Mercer Street oil tanker attacked by an armed drone in the Arabian Sea killing 2 crew members.

CNN, 2nd August 2021

Offshore Infrastructure Drone Intrusion

Norway's Petroleum Safety Authority (PSA)...urged oil companies to be more vigilant over unidentified drones seen flying near Norwegian offshore oil and gas platforms, warning they could pose a risk of accidents or deliberate attacks.

Reuters, 26th September 2022

Drone Attack on Vessel

The drone attack on the...Pacific Zircon...off the coast of Oman appears to be part of the long-running shadow war between Israel and its archenemy Iran that has included the targeting of Israeli-linked ships in strategic Mideast waterways.

Associated Press, 22nd November 2022

One Stop Shop For Cutting Edge Operational Resilience

VALUE PROPOSITION

OPERATIONAL TECHNOLOGY CYBERSECURITY FOR TRANSPORTATION ASSETS

More advanced technology than IT or fixed asset OT cybersecurity

COUNTER-DRONE MEASURES AT SCALE

Affordable Military Level Counter-Drone Capabilities

01

SEGMENT COMPETITIVE ADVANTAGE

Integrated solution for mobile assets across sea, land and air

02

SEGMENT COMPETITIVE ADVANTAGE

Larger perimeter protection

STRONGER DEFENSES. SIMPLER RISK MANAGEMENT. REDUCED VENDOR SPRAWL.

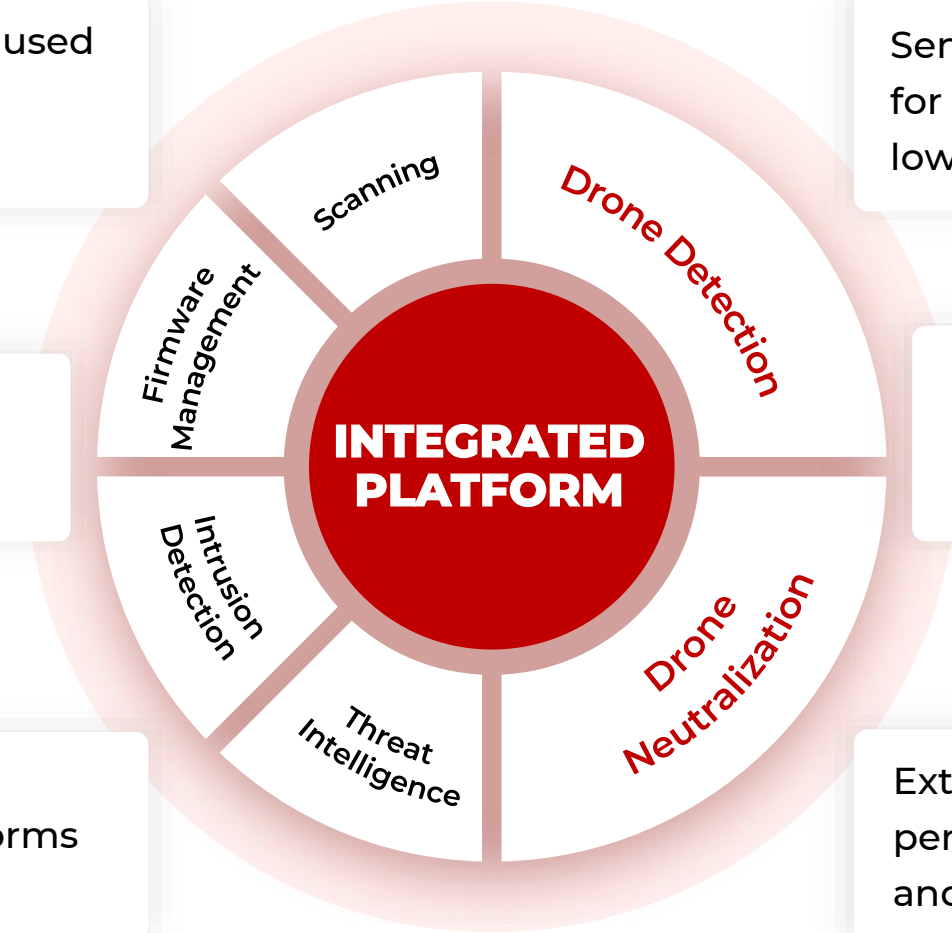
Integrated Technology Platform To Simplify Risk Management

TECH PLATFORM

10x faster protocols than those used to protect fixed assets

Ability to work with black box protocols

Data correlation and cross-pollination for resilient platforms



Sensor-fusion approach (RF/EO/IR) for Beyond Line of Sight detection at low SWaP (size, weight, and power)

Zero dependence on signal libraries for drone detection

Extended coverage range and larger perimeter monitoring due to tech and cost advantages

DIFFERENT ASSETS HAVE DIFFERENT RISK PROFILES

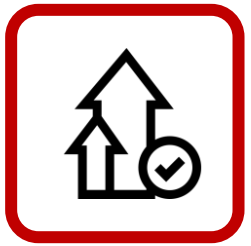
- Asset Type
- Asset Value
- Asset Owner/Brand
- Locational/Regional Political Risk Profile
- Transport Risk Profile (people, assets, environment)
- Cargo risk (where applicable)
- Ease of Attack

MODULAR

Our products are completely independent of each other but individually accretive to achieving defense in depth

RISK-BASED

Product selection can be configured based on asset risk profile



VALUE-DRIVEN

Range of price points and execution complexity to accommodate different risk profiles, client cyber maturity levels, and regulatory requirements

Cybersecurity Platform for Transportation Assets

PROTECTING MOBILE OPERATING ASSETS AT SEA, ON LAND, OR IN THE AIR, IS THE FRONTIER OF CYBERSECURITY

Reperion is building the most resilient cybersecurity platform for transportation assets by offering niche cybersecurity products across sea, land and air

HACKERS

are opportunists who seek to spend the least amount of money and time to achieve success. They focus on the best opportunities rather than specific industries

CYBERSECURITY RESILIENCE IS BEST ACHIEVED BY BEING AS DIVERSIFIED AS HACKERS THEMSELVES ARE

Our competitors across individual transportation segments are narrow niche players

Narrow niche player focus limits cyber-resilience

BROADER PERSPECTIVE

DEEPER INSIGHTS

STRONGER DEFENSES

Our cutting edge cybersecurity products can be plugged into existing IT or OT cybersecurity platform

Cybersecurity Product Summary

CYBERSECURITY PRODUCTS

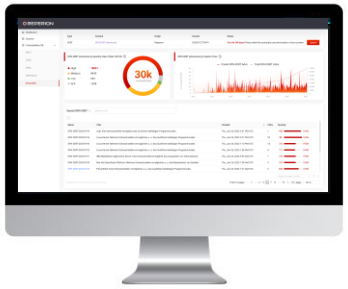
Scanning

Scanning tools are used to identify vulnerabilities before anomalies are detected

- These tools can be used to uncover network vulnerabilities, to assess cyber-maturity, to detect unauthorized devices, and to assess the cybersecurity of plugged-in devices
- A light touch, high impact method of securing assets

01

Intrusion Detection

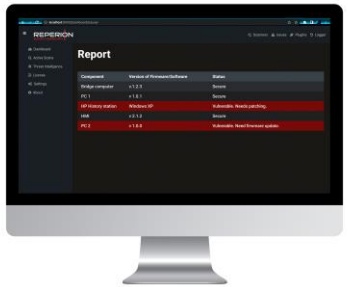


Intrusion Detection Systems are used to identify anomalies in IT/OT network traffic

- Software installed on an asset's existing hardware or a separate IIoT component
- Protect the mobile asset at the key gateway to detect passively any illegal connection to the asset or any anomalous activity on the asset's network

02

Firmware Management



System to ensure that firmware which controls hardware components is up to date and cybersecure

- Reperion's firmware management systems are industry-specific and customized to asset types
- Reperion is capable of patching without source code without interrupting asset operations

03

MDR & Intelligence Tools

Security Incident & Event Management to analyze data and respond to incidents

- *SIEM:* Correlating and cross-pollinating event data powers effective Management, Detection, and Response and and identifies threats at a Client's Security Operations Center
- Threat Intelligence (maritime): early detection of potential attacks targeting specific locations, specific companies, or specific types of assets

04

Counter-Drone Capabilities

Counter-Drone companies are typically defense industry players

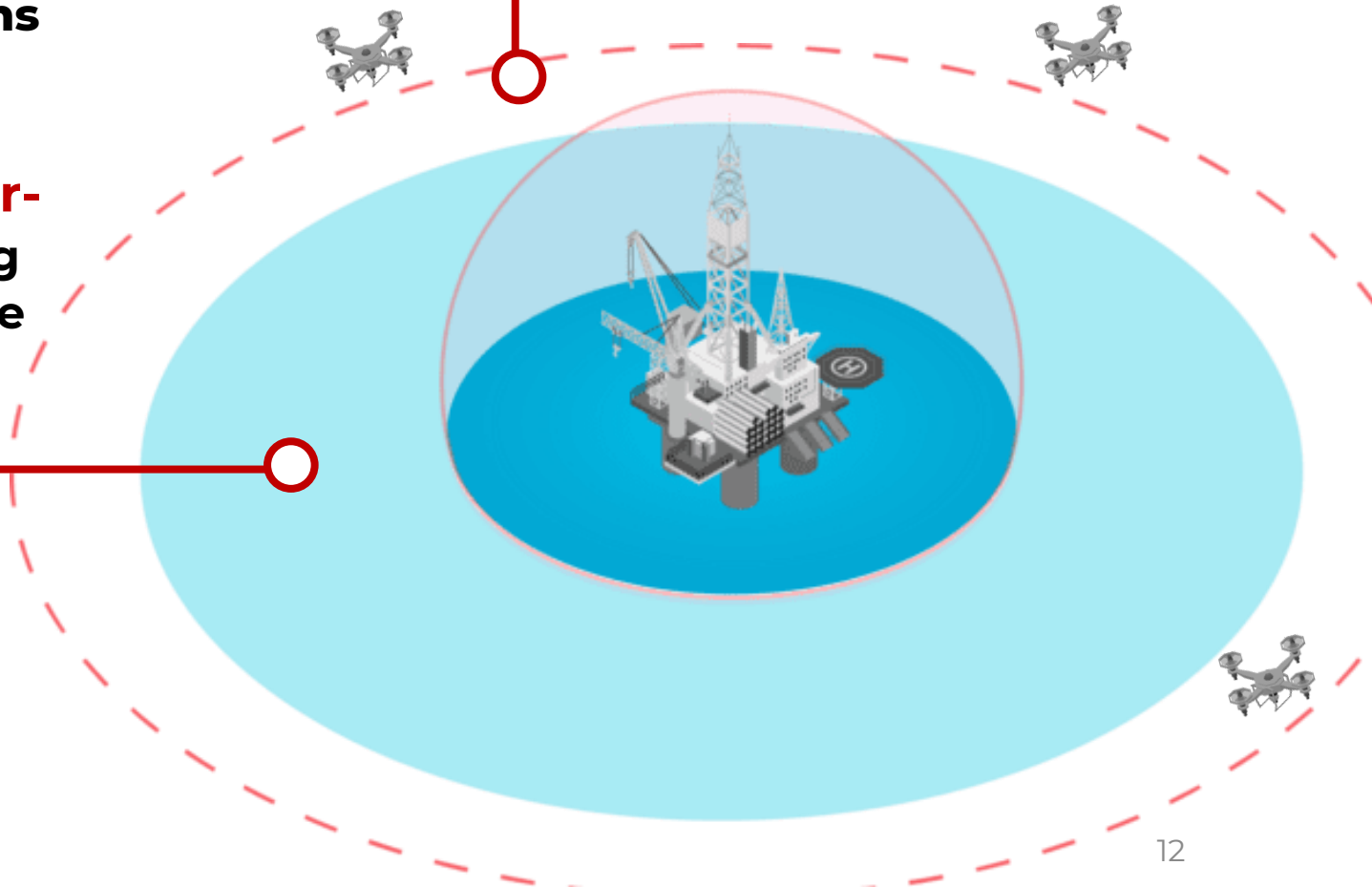
Defense Industry Pricing

Regulatory Restrictions

We are solving the problem of counter-drone protection at scale by offering affordable Military Level Counter-Drone Capabilities

Due to a significant cost advantage over military grade solutions, our military level advanced detection allows mass scale deployment and increases the perimeter of secured airspace

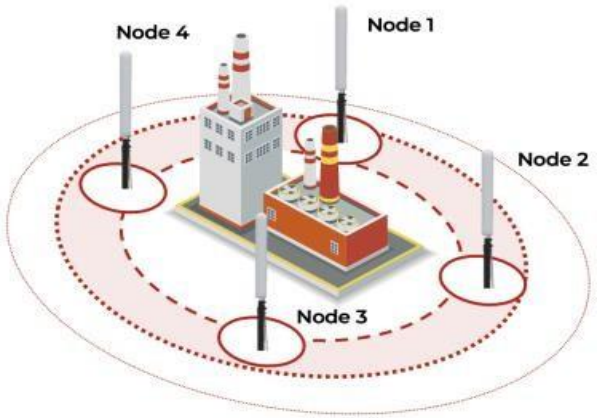
Military level – Long Range DETECTION



Counter-Drone Product Summary

COUNTER DRONE CAPABILITIES

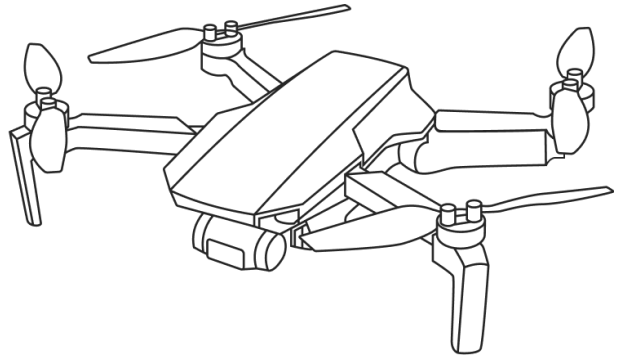
DRONE DETECTION



A hardware-software complex

- Detect unauthorized drones in controlled airspace leveraging RF direction finding,electro-optical, infrared, and acoustics technology

DRONE NEUTRALIZATION



Drone neutralization service to tackle airborne threats

- Long-range and short-range C-UAS non-destructive neutralization along with directed UAV landing
- Neutralize non connected drone using GPS spoofing and jamming

Maritime: Vessel Cybersecurity Applications

MARITIME CYBERSECURITY PRODUCTS

NORTRANS

First vessel IDS deployment, pending activation in 3Q23

Discover Vulnerabilities, Assess Cybersecurity Maturity

VSAT Scanner

- It's important to strengthen defenses of VSAT infrastructure because ~90% of successful attacks penetrate vessels through satellite communication
- Since VSAT infrastructure vulnerabilities can largely be mitigated by onboard personnel, vulnerability levels indicate cyber-maturity levels
- **Key Advantage**: No specific satcom subscription or hardware required

Gain Visibility in IT and OT Networks

Intrusion Detection System

- Reperion's Intrusion Detection System monitors traffic on IT/OT networks passively to detect and flag anomalies
- Our IDS has a proven capability of working with black box protocols and not interfering with operating systems
- **Key Advantage**: Our system is already certified by Kongsberg Maritime, a leading maritime tech OEM

Strengthen Safety and Security

Firmware Management System

- Prevent accidents caused by corrupted firmware installed on critical vessel operating components. Firmware cybersecurity is critical to achieving defense in depth
- **Key Advantage:** Binary firmware patches without access to source code that can eliminate vulnerabilities without affecting vessel operations

Become Proactive with Situational Awareness

Maritime Threat Intelligence

- Reperion has developed the leading database of maritime signatures, using a maritime specific honeynet system
- **Key Advantage**: Reperion's Maritime Threat Intelligence is the first of its kind

Maritime: Port Cybersecurity Applications

Crane Protection

- Protect cranes from unauthorized RF communication to block different types of attacks (replay, command injection, e-stop, re-pairing, re-programming)
- **Key Advantage:** Can be combined with drone detection

Firmware Management System

- Prevent accidents caused by corrupted firmware installed on critical components of port vehicles and cranes. Firmware cybersecurity is critical to achieving defense in depth
- **Key Advantage:** Binary firmware patches without access to source code that can eliminate vulnerabilities without affecting vessel operations

Intrusion Detection System

- Reperion's intrusion detection system, installed on an asset's hardware such as the key gateway to detect any illegal connection to the asset or any anomalous activity on the vehicle's network
- Our IDS has a proven capability of working with black box protocols and not interfering with operating systems
- **Key Advantage**: Reperion's intrusion detection system was the first (and one of only two) to be approved by Kongsberg Maritime– a global leader in maritime technology

Improve Port Defense in Depth

- Vessels plugging into a port's wi-fi network whilst moored at the quayside create vulnerabilities for the port
- A port can mitigate its cyber-risk by scanning a vessel before its arrival to assess and mitigate its cyber risk. The port could generate revenue by charging the vessel for the scan
- **Key Advantage**: No specific satcom subscription or hardware required

Become Proactive with Situational Awareness

- Reperion's Maritime Threat Intelligence tool is an early detection system to identify and assess potential threats in a port's local or regional vicinity
- Our maritime threat intelligence is based on our database of +23,000 signatures and strategically deployed honey nets
- **Key Advantage**: Believe to be the only company offering this product

Land Cybersecurity Applications

VEHICULAR CYBERSECURITY PRODUCTS

VEHICLE USE CASES

- **Firmware Scanner**
  Assembly Line Scanner positions vehicles for a cybersecure start to their useful lives and facilitates compliance with ISO/SAE 21434
- **Aftermarket Cybersecurity Platform**
  Scans the vehicle to ensure that devices plugged into vehicle are approved and certified by the OEM for cybersecure use.
- **IDS**
  To protect assets from hacks across all segments

SIEM and **ANALYTICS SUITE** to power Management Detection and Response from a Security Operations Center (SOC)

Our products improve the cybersecurity of assets and enable our customers to improve safety outcomes

MOTORBIKE AND SCOOTER USE CASES

- **Firmware Scanner**
  Evaluate existing equipment and potential equipment acquisitions before procurement
- **IDS**
  To protect assets from hacks across all segments
- **Road Safety**
  Combine cybersecurity with road safety feature

REVENUE OPPORTUNITY:

OEMs generate revenue by charging Accessories Manufacturers to have their products verified and certified on an Aftermarket Cybersecurity Platform

Air Cybersecurity Applications

OUR PRODUCTS PREVENT AIRBORNE ASSETS FROM BECOMING TARGETS OR TOOLS OF CYBERATTACKS.

HELICOPTER/VTOL USE CASES

- **Firmware Scanner**
  to evaluate existing equipment and potential equipment acquisitions before procurement
- **IDS**
  to protect VTOLs and helicopters

SIEM and **ANALYTICS SUITE** to power Management Detection and Response from a Security Operations Center (SOC)

Drone Detection Applications

Mitigate against corporate espionage and unauthorized surveillance

Mitigate attacks on urban, industrial, and critical infrastructure

Reinforce border patrol and perimeter security in controlled airspaces

COLLATERAL RISKS:

ESPIONAGE: LOSS OF IP

INFRASTRUCTURE ATTACK: INJURY AND LOSS OF LIFE

SUPPLY CHAIN DISRUPTION

CIVIC DISRUPTION

GEOPOLITICAL TENSIONS

Drone Detection Applications

LAND

01 Buildings and other Urban Structures

02 Industrial Plants

03 Critical Infrastructure

04 Borders and other Government Controlled Airspace

MARITIME

01 Port Infrastructure

02 Offshore Infrastructure

03 Vessels

Use Case: Modular Approach to Vessels

VESSEL TYPE	VESSEL TYPE	VESSEL TYPE	VESSEL TYPE
1,800 TEU Containership	Offshore Dive Support Vessel	LNG Vessel	24,000 TEU Containership
CARGO RISK	CARGO RISK	CARGO RISK	CARGO RISK
LOW	NOT APPLICABLE	HIGH	MEDIUM
TRADING PATTERN RISK	TRADING PATTERN RISK	TRADING PATTERN RISK	TRADING PATTERN RISK
LOW	HIGH	HIGH	HIGH
SUGGESTED SECURITY	SUGGESTED SECURITY	SUGGESTED SECURITY	SUGGESTED SECURITY
VSAT Scanner	VSAT Scanner Intrusion Detection Counter-drone measures (depending on location)	VSAT Scanner Intrusion Detection Drone Detection & Neutralization	VSAT Scanner Intrusion Detection Drone Detection & Neutralization

Use Case: Integrated Approach to Ports

OUR INTEGRATED APPROACH ENABLES DEFENSE IN DEPTH FOR CUTTING EDGE RISK WITH SIMPLIFIED RISK MANAGEMENT AND REDUCED VENDOR SPRAWL

Use Case: Securing the Oil & Gas Value Chain

Offshore Oil Platform

- Intrusion Detection
- Drone Detection
- Drone Neutralization

Offshore Vessel

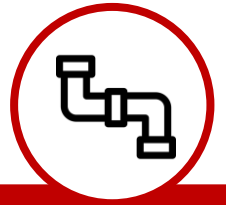
- VSAT Scanner
- Intrusion Detection

Tanker

- VSAT Scanner
- Intrusion Detection
- Drone Detection
- Drone Neutralization

Refinery

- Drone Detection
- Drone Neutralization
- White listed drones vs Intruder drones



Pipeline

- Drone Detection
- Drone Neutralization

OUR INTEGRATED APPROACH ENABLES DEFENSE IN DEPTH FOR CUTTING EDGE RISK WITH SIMPLIFIED RISK MANAGEMENT AND REDUCED VENDOR SPRAWL

Use Case: Integrated Approach to Government

01 Drone detection for urban centers

02 Drone detection for utilities and other critical infrastructure

03 Government-mandated road safety and cybersecurity protection for motorbikes and scooters

04 Vehicular cybersecurity protection for government vehicles

05 Extended perimeter drone detection for airports and borders and other controlled airspaces

Reperion Company Background

COMPANY BACKGROUND

Reperion is a Singapore-headquartered next generation security business that protects transportation assets from cyberattacks across sea, land, and air as well as critical infrastructure and controlled airspaces from drone attacks

Reperion's tech leadership team holds relevant positions at University of Bristol and Carnegie Mellon University; we are at various stages of collaboration with:

University of Bristol

Singapore University of Technology and Design

Imperial College London

ADSC

NUS National University of Singapore

Carnegie Mellon University CyLab Security and Privacy Institute

CYBERSECURITY AWARDS

- Midnight Sun CTF 2020 Quals (1st place)
- 1st place at Midnight Sun CTF Quals 2018
- 1st place at Midnight Sun CTF Finals 2018
- 1st place at CTFZone 2017
- 1st place at CTFZone 2017 Finals
- 1st place at CTFZone 2018 Quals
- 1st place at OpenCTF 2016
- 1st place at Meepwn CTF Quals 2018
- 1st place at 0CTF 2016 Finals
- 1st place at 0CTF 2017
- 1st place at Insomnihack 2019
- 1st place at Real World CTF 2018 Finals
- 1st place at WhiteHat Grand Prix 2018 - Final Round
- 1st place at TUM CTF 2016

Leadership Driving Visibility, Product, and Revenue Pipeline

Key Management Team

Andrew W. Sallay

CEO & CO-FOUNDER

Entrepreneur with finance background. Founded and headed companies and projects across B2B Enterprise services and industrials. Raised in excess of US$20 million for startups and ventures. MBA from University of Chicago. BA from Swarthmore College

Dr. Dmitry Mikhaylov

CSO & CO-FOUNDER

Cybersecurity thought leader and academic. Co/authored 10 books and obtained 15 patents in cybersecurity. United Nations Expert. PhD in Cybersecurity from National Research University MEPhI. MBA from University of Warwick. Most recently, Visiting Associate Professor at National University of Singapore (NUS Enterprise)

Kushagra Dixit

HEAD OF TECHNOLOGY & PRODUCTS

Top cryptography researcher in the UK and part of the University of Bristol's world-renowned Cryptography Research Group in England. Visiting Researcher at Carnegie-Mellon University. Leading our drone segment because of his defense background

The team comprises 15 FTEs including a VP with an automotive background, a Head of Research, and a development resource base in India

Key Advisory Board Members

Head of Cybersecurity Business

LEADING AMERICAN BIG DATA ANALYTICS COMPANY

Digital Forensics and Incident Response Expert with cyber experience in finance and big data industries. Track record of sales to corporates and governments. Extensive network in Middle East and Europe

Head of Strategy & Tech

LEADING CYBERSECURITY THREAT INTELLIGENCE COMPANY

20 years of cybersecurity experience in strategy and implementation roles; deep experience in product development and customer. Tenures at BHP, Deloitte and Accenture

Stephane Degenne, Head of Origination and Structured Trade

GUNVOR

De facto CEO of Gunvor, 4th largest global commodities trader. 29 years in Oil & Gas trading including tenures at Total, Elf, and Addax. Extensive top level O&G network in Middle East, Europe, Africa, and Asia