Empowering Human Capability Through Real-Time Behavioural Insights

iSentry is a video analytics platform focused on improving the ability to effectively manage *in real time* huge amounts of video arriving at a video monitoring center.

iSentry helps to makes tangible the return on investments on CCTV surveillance systems already in place, normally used only for forensic analysis of incidents that have already occurred, rather than to avoid their occurrence.

CORE CAPABILITIES

UNIQUE ANALYTICS

Core Analytics

For years, security experts believed that installing more and more CCTV cameras would deliver enhanced security. There are now over 1 billion video surveillance cameras in the world and that number is increasing. But with more and more cameras to monitor, control room operators are simply unable to cope with the volume of CCTV feeds. It is physically and financially impossible to employ the number of operators that would be required to effectively monitor all CCTV in real-time.

To overcome this problem CCTV camera feeds have been fed into video analysis software. When the software spots something that requires closer monitoring it will be flagged straight away to a control room operator for analysis.

These video analytic solutions perform reasonably well when identifying a handful of pre-defined events that they were programmed to detect. But their rules-based algorithms can neither detect nor manage the majority of abnormal or unusual events that are not covered by specific and preprogrammed rules.

They require heavy configuration prior to use and are resource-intensive demanding massive significant hardware investment, while control room operators waste countless hours analyzing the many false positives flagged by the software.

Traditional video monitoring software does not develop by ‘learning’ from past events. It relies solely on the predefined situations that it has been programmed to look out for. A smarter, AI-powered solution is required. A solution that enables security control room operators to effectively monitor a substantial number of video feeds in real-time. That solution is IntelexVision’s iSentry platform

Self-Learning (Unusual Behaviour)

This is the most important algorithm of iSentry. Detection of Unusual Behavior is driven by an unsupervised artificial intelligence platform. Learning is based on pixel pattern analysis and allows the system to learn how objects normally move in a scene taking into account direction, speed, size and a variety of other factors; after establishing a norm, the system will create an alert on any deviations,

These events are then classified using Deep Learning engine and a logic engine for further contextualization. This allows the system to reduce by 98% to 99% the amount of video to be analyzed by a CCTV operator. A single Self learning license often replaces 5-15 licenses based on Rules Based algorithms.

The self-learning happens amazingly fast. Depending on the complexity of the scenery, the self-learning engine starts getting a smart insight of what is usual already after 48 – 96 hrs of operation

Environmental filtering (TREX)

iSentry is supported by a dynamic learning process based on artificial intelligence called TREX, which creates the ability to acquire and track elements of interest, ignoring environmental factors inherent to CCTV analytics, such as varying conditions of light, rain, snow, wind and even the intrinsic noise of the camera sensor.

Data Enrichment

Applying more than a dozen Deep Learning neural networks, iSentry can enrich the video analysis with detailed information on the alerts generated by the two main "triggers" engines: Self Learning and TREX.

The Deep Learning engine is able to recognize multiple classes of objects, even with difficult camera angles and greater distances using Pixel based learning. The system is constantly improved and updated for specialized areas such as age and gender estimation, fire detection and compliance detection of face-masks, helmets, Guns, Vehicles etc.

Automation (Logic engine)

The iSentry logic engine plays the role of a video surveillance operator and as such can decide for itself whether an alert should be decision. Identified as an alarm or be ignored.

This decision is based on factors such as the number and combination of object types that trigger the alert, the time of day and object size, or even the likelihood of accurate ratings.

Typically, up to 80% of alerts can be handled by the system without requiring human intervention. The inherent risk of automation is largely mitigated by several logical mechanisms, where rules are applied only when their results are highly secure. Key to the iSentry philosophy, all notices that fail the automation test will be placed in front of an operator for further investigation and decision.

Business Intelligence and Forensic Search

iSentry also includes, at no additional cost, a rich Business Intelligence tool, which is available "out of the box" for any customer.

The information generated by this tool is very valuable in terms of operator performance KPIs as well as system and camera performance and operation.

The data warehouse behind this functionality allows our customers to use a range of custom BI tools, should the need arise. In addition, iSentry has a forensic analysis engine, which allows you the search for specific objects that have produced alerts or alarms within a scene, allowing quick verification of all history of alerts by object class and time frame.

Hardware Efficiency & Flexibility

iSentry has been designed to provide an extremely fast and efficient basic level of video analysis. Very close to real-time analysis and full-motion video alerting.

Key improvements have been made to the use of Intel Open VINO for integrated Deep Learning, and to the introduction of hardware acceleration, incorporating suitable HD graphics or dedicated NVIDIA CUDA GPU decoding hardware to supplement CPU processing.

This results in the ability to manage tens to hundreds of video analytics channels on a single workstation or enterprise server.

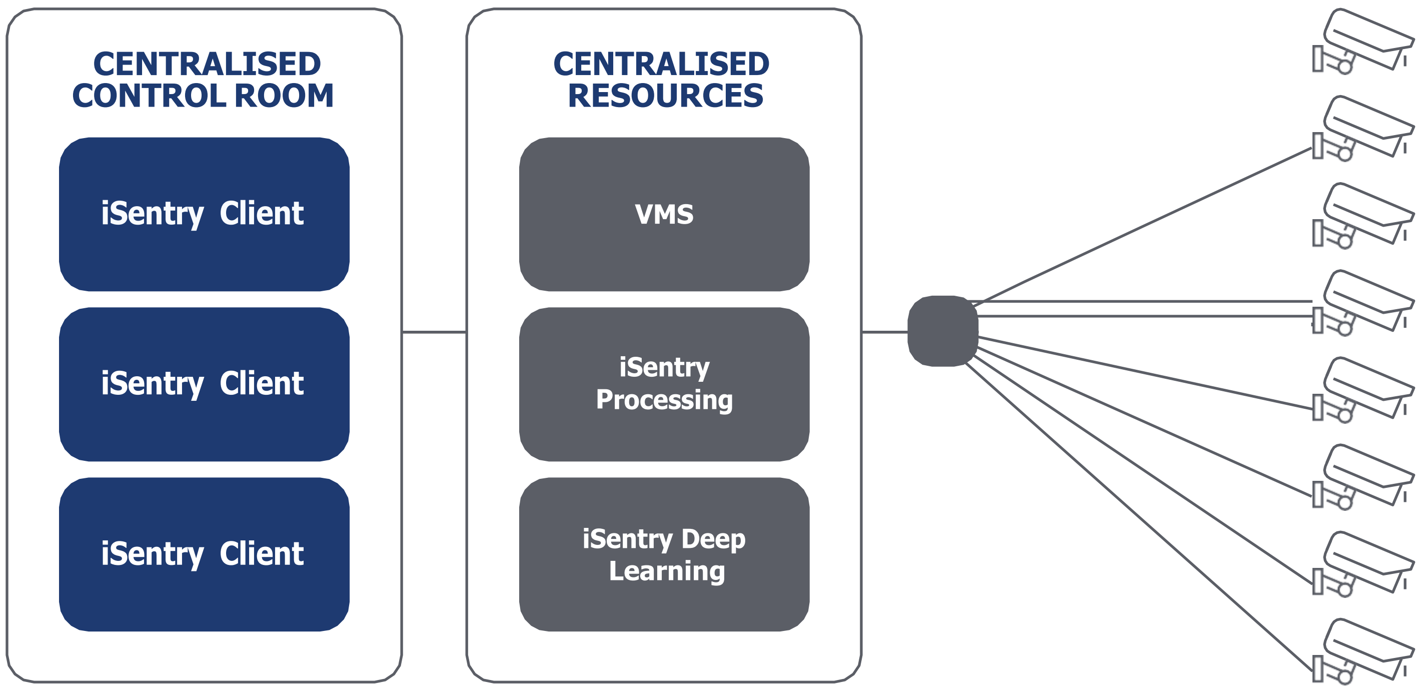
Deployment Options

Both centralised and Edge based architectures are supported by the iSentry system. With flexibility in mind, many of the iSentry system components can be virtualised, combined, or be stand-alone, allowing for resource sharing and optimisationof processing and data flow, when needed and possible.

Flexible Architectures

CENTRALISED ARCHITECTURE

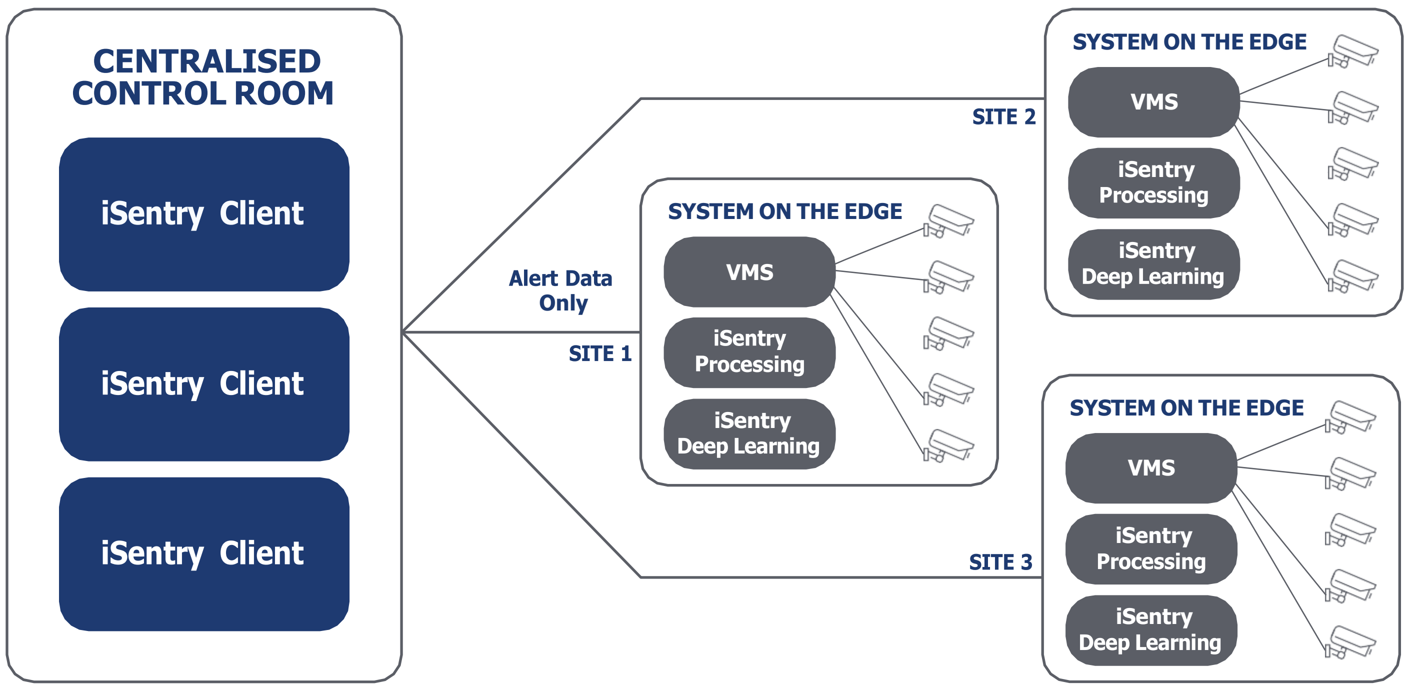
This is the most commonly used architecture in general. The iSentry centralized architecture has the advantage of relatively low complexity and can take advantage of economies of scale, but in the case of a network containing many cameras, it could require significant bandwidth to allow centralization of all the video in a single central location.



CENTRALISED CONTROL ROOM
iSentry Client
iSentry Client
iSentry Client
CENTRALISED RESOURCES
VMS
iSentry Processing
iSentry Deep Learning

DISTRIBUTED ARCHITECTURE

This architecture is suitable where a central control room is required with a number of small and large distributed sites, which need monitoring. This architecture is not limited in terms of camera number and the entire processing requirement is handled on site. This allows for fully autonomous sites, each with the capacity for their own control room, if needed, with records and data stored on site. Only the alert data is transmitted to the central control room and therefore bandwidth usage is limited to just the alert and video data for each alert.

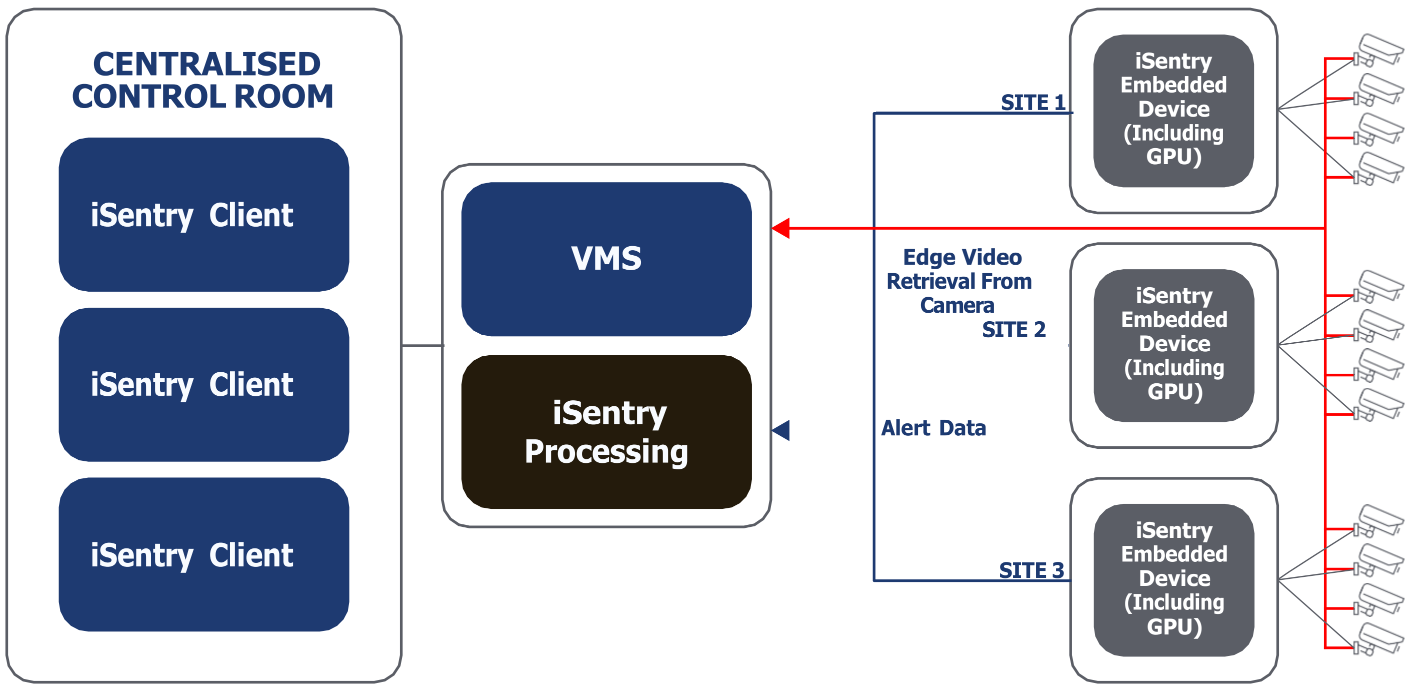


CENTRALISED CONTROL ROOM
iSentry Client
iSentry Client
iSentry Client
Alert Data Only
SITE 1
SITE 2
SITE 3
SYSTEM ON THE EDGE
VMS
iSentry Processing
iSentry Deep Learning
SYSTEM ON THE EDGE
VMS
iSentry Processing
iSentry Deep Learning
SYSTEM ON THE EDGE
VMS
iSentry Processing
iSentry Deep Learning

COMPLETE EDGE ARCHITECTURE

Micro embedded device with GPU

This architecture takes advantage of a central VMS with distributed processing while limiting the bandwidth required to stream live video. In this architecture, all iSentry processing is done on the embedded edge device (such as an NVIDIA Jetson nano), *including the Deep Learning*, importing live video from the cameras and then sending only alert data and alert video to the control room central location.

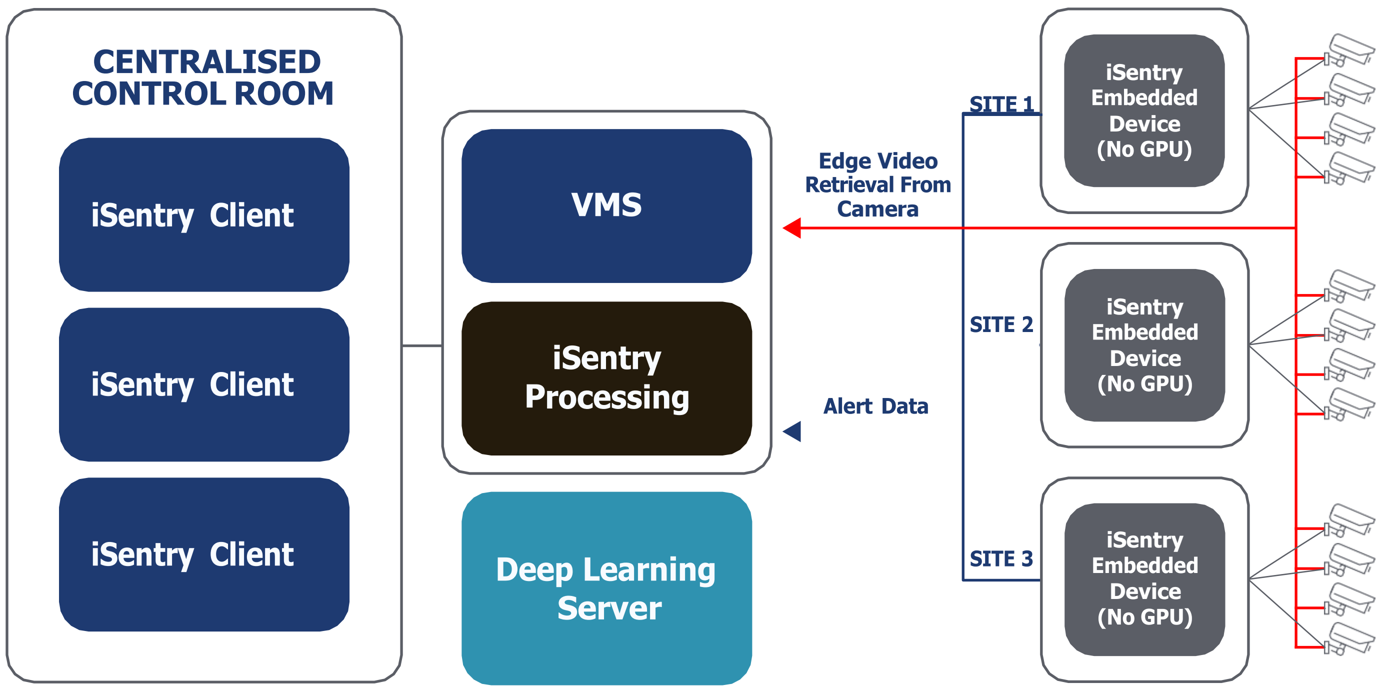


CENTRALISED CONTROL ROOM
iSentry Client
iSentry Client
iSentry Client
VMS
iSentry Processing
Edge Video Retrieval From Camera
Alert Data
SITE 1
SITE 2
SITE 3
iSentry Embedded Device (Including GPU)
iSentry Embedded Device (Including GPU)
iSentry Embedded Device (Including GPU)

PARTIAL EDGE ARCHITECTURE

Micro embedded device without GPU

This architecture differs from the full edge architecture in that only the first processing layer of the iSentry is managed on the edge device (such as a Raspberry Pi) and the subsequent Deep Learning and Rules Engine processing layers are managed centrally. The advantages of this architecture are that Deep Learning processing can be a fully shared resource in the Control Center and that a wider range of embedded devices is supported.

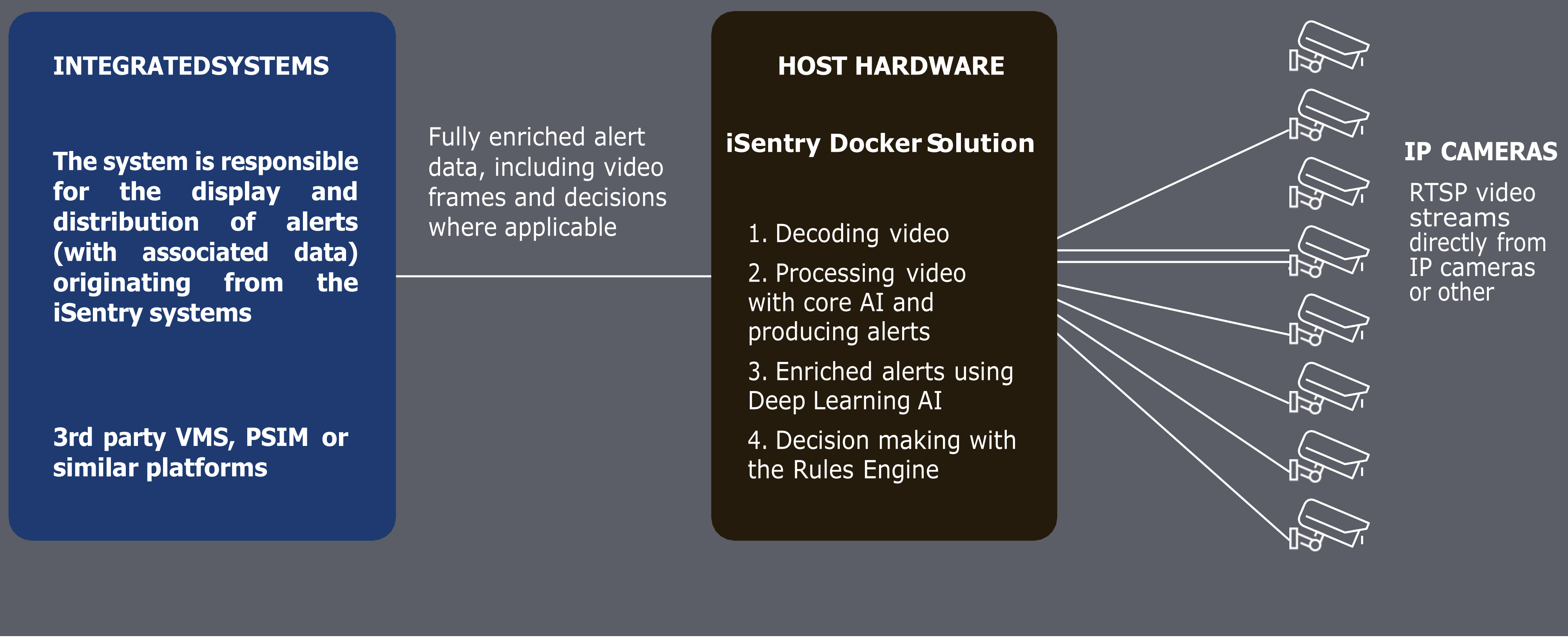


CENTRALISED CONTROL ROOM
iSentry Client
iSentry Client
iSentry Client
VMS
iSentry Processing
Deep Learning Server
Edge Video Retrieval From Camera
Alert Data
SITE 1
SITE 2
SITE 3
iSentry Embedded Device (No GPU)
iSentry Embedded Device (No GPU)
iSentry Embedded Device (No GPU)

Other Integration Options

The iSentry core system is also available in an API form, which can be integrated into VMS and PSIM platforms.

The iSentry core is available as a Nvidia docker, or Linux-based service.



INTEGRATEDSYSTEMS

The system is responsible for the display and distribution of alerts (with associated data) originating from the iSentry systems

3rd party VMS, PSIM or similar platforms

Fully enriched alert data, including video frames and decisions where applicable

HOST HARDWARE

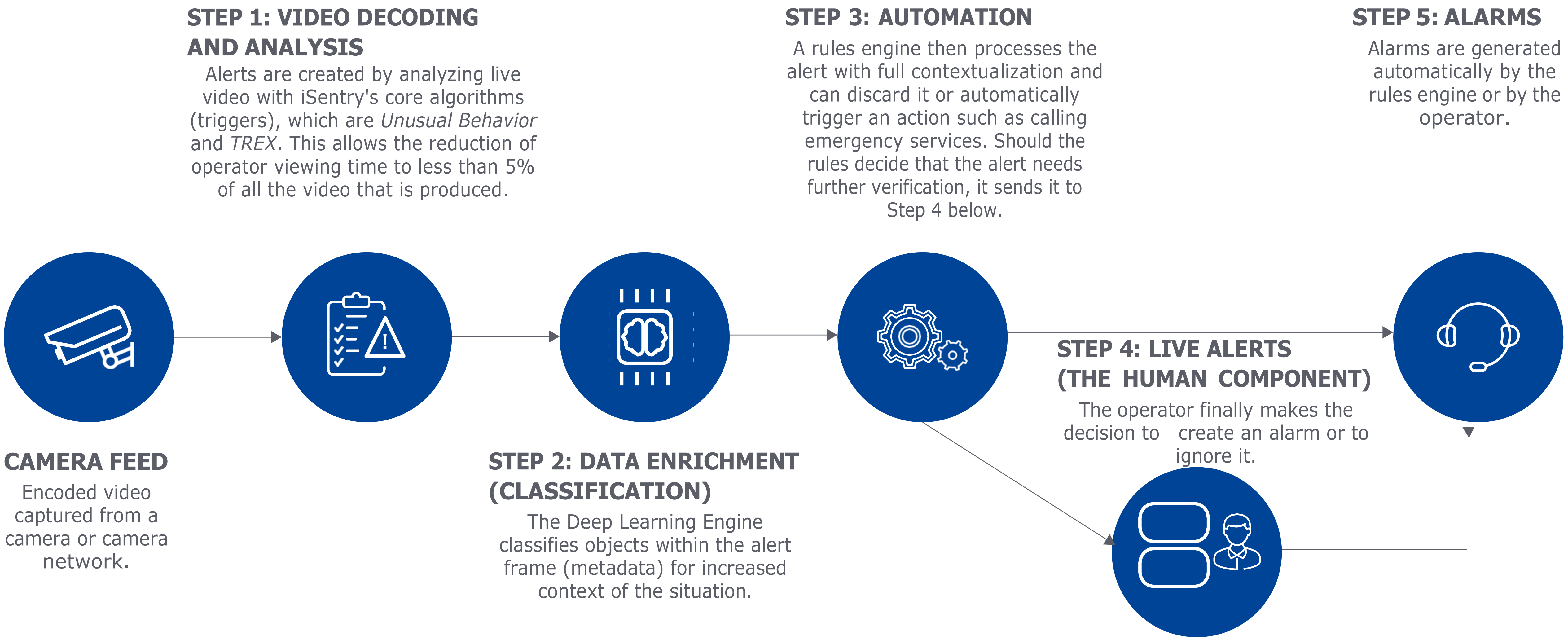
iSentry Docker Solution

1. Decoding video
2. Processing video with core AI and producing alerts
3. Enriched alerts using Deep Learning AI
4. Decision making with the Rules Engine

IP CAMERAS

RTSP video streams directly from IP cameras or other

The iSentry Process



STEP 1: VIDEO DECODING AND ANALYSIS

Alerts are created by analyzing live video with iSentry's core algorithms (triggers), which are *Unusual Behavior* and *TREX*. This allows the reduction of operator viewing time to less than 5% of all the video that is produced.

STEP 3: AUTOMATION

A rules engine then processes the alert with full contextualization and can discard it or automatically trigger an action such as calling emergency services. Should the rules decide that the alert needs further verification, it sends it to Step 4 below.

STEP 5: ALARMS

Alarms are generated automatically by the rules engine or by the operator.

CAMERA FEED

Encoded video captured from a camera or camera network.

STEP 2: DATA ENRICHMENT (CLASSIFICATION)

The Deep Learning Engine classifies objects within the alert frame (metadata) for increased context of the situation.

STEP 4: LIVE ALERTS (THE HUMAN COMPONENT)

The operator finally makes the decision to create an alarm or to ignore it.

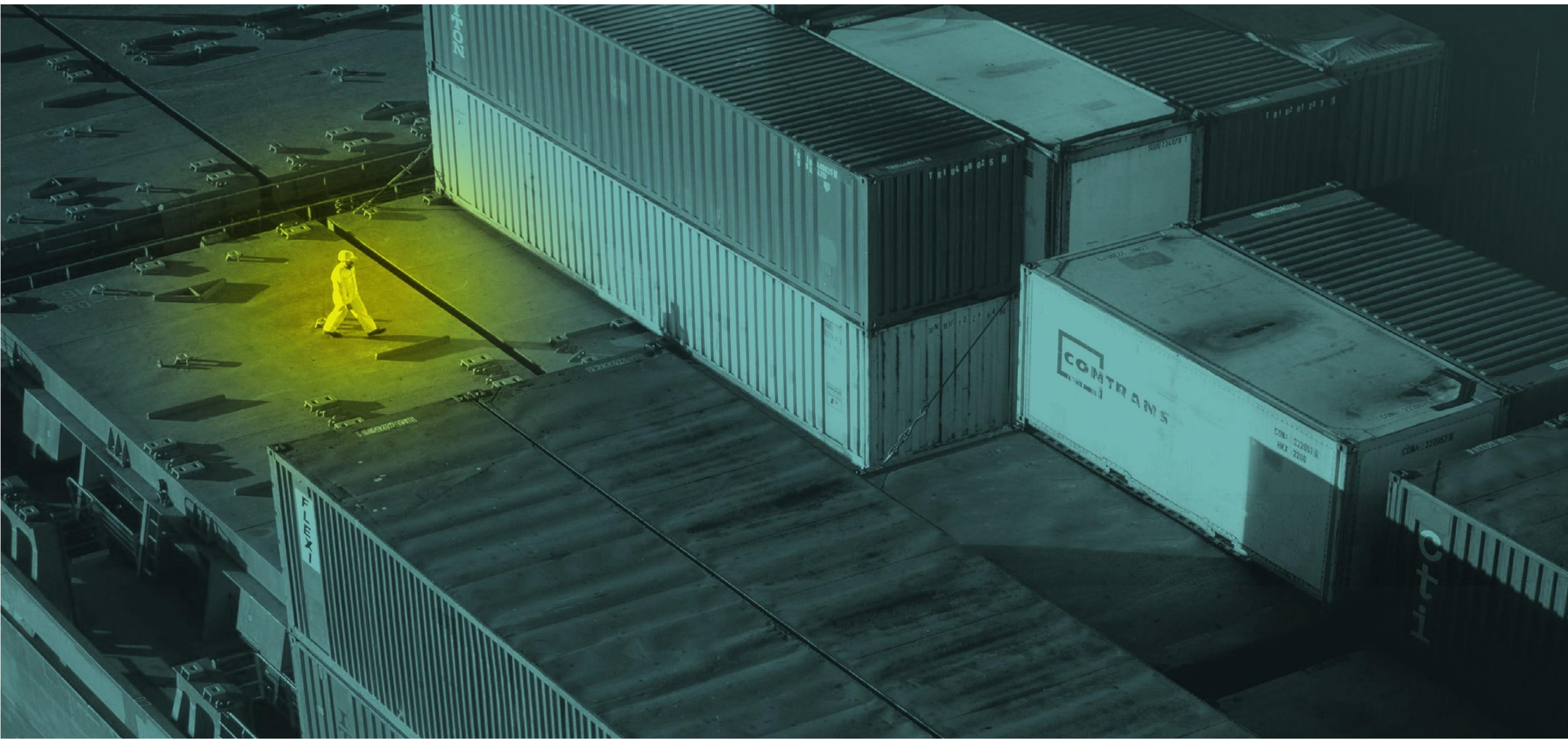
1 iSentry efficiently decodes multiple video streams which are then analyzed by one or more of the analytics based on Artificial Intelligence, resulting in an "alert", which will then start the iSentry process.

2 A certain number of detected frames, extracted from the alert video, are analyzed by the GPU-based Deep Learning server. This process maximizes processing efficiency and gives the system a much greater understanding of the alert.

3 Due to the greater understanding, from step 2, the system will automatically dismiss many alerts or raise some to an alarm, many of these with a high level of certainty.

4 Alerts that are not automatically elevated to alarm in step 3 are presented to the operator as a list of current alerts, each containing classified images and a +/- 5-10 second video clip. The operator then decides whether an alert is important (escalating to alarm) or not, thus eliminating most false positives.

5 Once an alarm is generated either automatically by step 3 or by the human in step 4 the iSentry process is now complete. All data associated with the alarm including video, classifications, metadata and operator input, is included with the alarm to be processed.



IntelexVision is a provider of unparalleled unusual behavior and threat analytics solutions through its AI driven iSentry platform.

Admirals Offices, Main Gate Road
The Historic Dockyard
Chatham, ME4 4TZ
United Kingdom

info@intelexvision.com