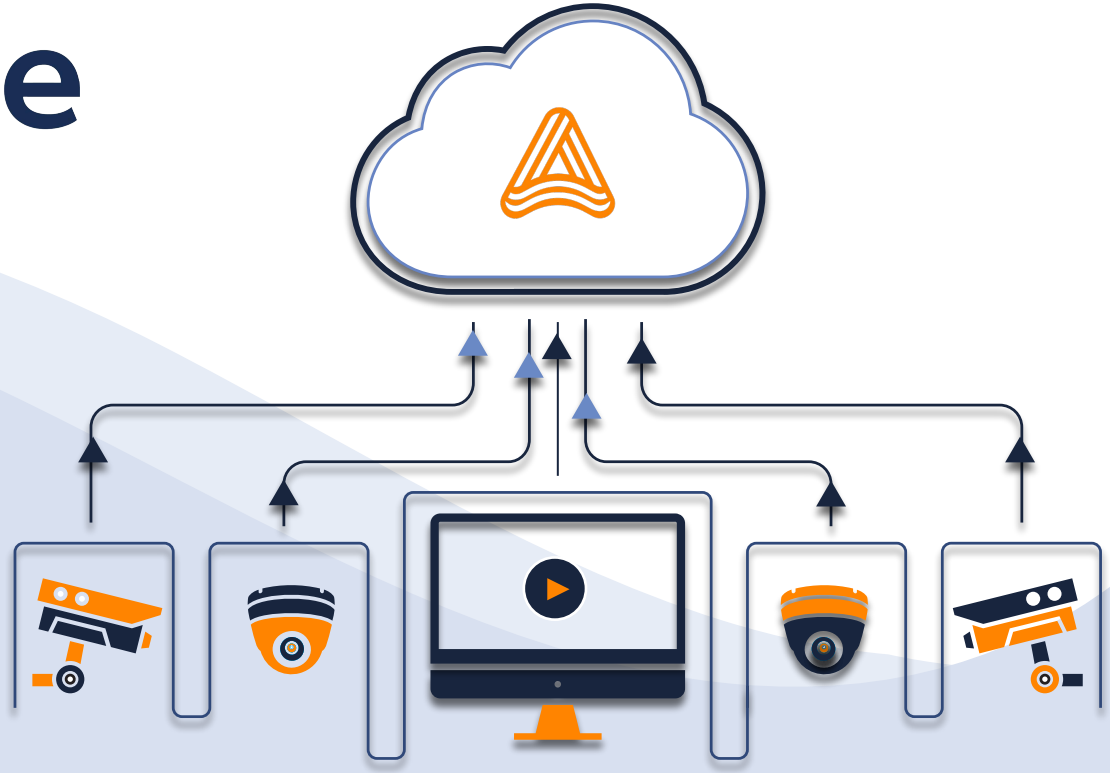
actuate

Products

AI Gun, Intruder, Loitering, and Crowd Detection



Offered Products: Analytics

actuate

Gun Detection

Identifies brandished or held firearms

Intruder (Person/Vehicle) Detection

Identifies a person or vehicle where/when they are not permitted

Loitering Detection

Identifies when a person remains in-frame for a given amount of time

Crowd Detection

Identifies the formation of large groups of people

Additional Analytics (Beta)

- Hard Hat Detection
- Fire Detection
- Vehicle Gate Automation

If interested, contact Actuate at info@actuate.ai for more information.

GUN DETECTION

Product Definition:

Actuate's gun detection AI recognizes both handguns and long guns when brandished on camera, and differentiates between the two when sending alerts. No audio component.

How Does it work?:
Our computer vision algorithms detect guns after having been trained on our proprietary data set of hundreds of thousands images of brandished guns to find common features. Our model then searches for these common features such as shape, texture, and contour of objects in live video to classify guns at a 99% accuracy rate when brandished for 5 seconds.

Additional Features:

1. Configurable alert settings for individual cameras + analytics
    - Confidence level, ignore zones, frame thresh, crops
2. Cool-down period fully configurable for each camera
3. Multiple ways to receive alerts
    - Text, email, VMS, monitoring UI, IMMIX. All alerts are sent simultaneously from our end, regardless of how many or what kind of alerting methods are used

TECHNICAL REQUIREMENTS

Min. FPS	Min. Resolution	Detection Range*	Bandwidth Range (50-100% motion)**	SMTP Compatible?	Thermal Compatible?	Fisheye Compatible?
3	720p	20PPF ~50 feet	160-725 kbit/s	No	No	Not Currently Available

1. Gun detection can only be used via RTSP streams or direct integration with VMS systems
   a. NOT COMPATIBLE WITH AI LINK. SmartPSS NVRs also not recommended.
2. Ensure stable internet connection
   a. Unstable connections or frequent outages result in lost frames and detections
3. Higher resolutions and frame rates will not necessarily lead to better detections but will increase bandwidth usage

* Camera resolution and installation will determine actual physical distance detection range
** Per camera using motion filter at min resolution and frame rate

INTRUDER DETECTION

Product Definition:

Actuate's intruder detection AI recognizes when a person or vehicle appears into the camera's view when the camera is armed. When making detections and sending alerts, the model can differentiate between the following five intruder object types: person, car, bike, truck, and bus.

How Does it work?:
Our computer vision algorithms are trained on our proprietary data set of over a million images and searches for personally non-identifiable features such as shape, texture, and contour of objects in live video to detect and differentiate between the five intruder types.

Additional Features:

1. Stationary vehicle filtering
2. Configurable alert settings for individual cameras + analytics
    - Confidence level, ignore zones, frame thresh, crops
3. Cool-down period fully configurable for each camera
4. Multiple ways to receive alerts
    - Text, email, VMS, monitoring UI, IMMIX. All alerts are sent simultaneously from our end.
5. Slicing available for cameras with high resolution for longer-range detections

TECHNICAL REQUIREMENTS

Min. FPS	Min. Resolution	Detection Range	Bandwidth Range (50-100% motion)*	SMTP Compatible?	Thermal Compatible?	Fisheye Compatible?
1	480p	5 PPF	~43 kbit/s	Yes	Yes	Yes

1. Ensure stable internet connection
    - Unstable connections or frequent outages result in lost frames and detections
2. Higher resolutions and frame rates will not necessarily lead to better detections but will increase bandwidth usage
    - However, high resolution may be helpful in certain cases, such as when the camera is covering a large area
3. Intruder model is compatible with all general availability integrations, as well as AI Link.

*Per camera using motion filter at min resolution and frame rate

LOITERING DETECTION

Product Definition:

Actuate's loitering detection AI recognizes when a person enters and remains in a camera's view for a configurable amount of time.

How Does it work?:
Our computer vision algorithms have been trained on our proprietary data set of over 1 million images of people as seen on CCTV footage to find common, non-identifiable human features. Our model then searches for these common features like legs, arms, and whole body figures in live video to accurately identify intruders and track them over a desired amount of time to be classified as loiterers.

Additional Features:

1. Configurable Loitering Time
2. Configurable alert settings for individual cameras + analytics
    - Ignore zones, slicing
3. Cool-down period fully configurable for each camera
4. Multiple ways to receive alerts
    - Text, email, VMS, monitoring UI, IMMIX. All alerts are sent simultaneously from our end, regardless of how many or what kind of alerting methods are used

TECHNICAL REQUIREMENTS

Min. FPS	Min. Resolution	Detection Range	Bandwidth Range*	SMTP Compatible?	Thermal Compatible?	Fisheye Compatible?
1	480p	5 PPF	~43 kbit/s	No	Yes	Yes

1. Loitering detection can only be used via RTSP streams or direct integration with VMS systems
   a. NOT COMPATIBLE WITH AI LINK. SmartPSS NVRs also not recommended.
2. Ensure stable internet connection
   a. Unstable connections or frequent outages result in lost frames and detections
3. Higher resolutions and frame rates will not necessarily lead to better detections but will increase bandwidth usage

*Per camera using motion filter at min resolution and frame rate. For a more accurate calculation for a specific camera see this calculator

CROWD DETECTION

Product Definition: **Actuate's crowd detection AI recognizes the formation of large groups of people. The model's definition of crowd is configurable on the number of people, the distance (in feet) between them, and the allotted time (in seconds) that a crowd is in the camera's view before alerting.**

How Does it work?:
Our computer vision algorithms have been trained on our proprietary data set of over 1 million images of people as seen on CCTV footage to find common, non-identifiable human features. Our model then searches for these common features like legs, arms, and whole body figures in live video to accurately identify larger formations of people.

Additional Features:

1. Configurable crowd time, number of people that qualifies as a crowd, crowding distance
2. Configurable alert settings for individual cameras + analytics
    - Ignore zones, slicing
3. Cool-down period fully configurable for each camera
4. Multiple ways to receive alerts
    - Text, email, VMS, monitoring UI, IMMIX. All alerts are sent simultaneously from our end, regardless of how many or what kind of alerting methods are used

TECHNICAL REQUIREMENTS

Min. FPS	Min. Resolution	Detection Range	Bandwidth Range*	SMTP Compatible?	Thermal Compatible?	Fisheye Compatible?
1	480p	5 PPF	~43 kbit/s	No	Yes	Yes

1. Crowd detection can only be used via RTSP streams or direct integration with VMS systems
   a. NOT COMPATIBLE WITH AI LINK. SmartPSS NVRs also not recommended.
2. Ensure stable internet connection
   a. Unstable connections or frequent outages result in lost frames and detections
3. Higher resolutions and frame rates will not necessarily lead to better detections but will increase bandwidth usage
4. While configuring, start low - 15 second crowd time, 2.0 6ft multiple (crowd distance), and 3 people (crowd number) until we get enough alerts to verify that it is working.
5. Cameras that don't send enough motion may inhibit alert reception.

*Per camera using motion filter at min resolution and frame rate. For a more accurate calculation for a specific camera see this calculator

GLOSSARY

- **PPF (Pixels Per Foot)**
  - Metric determined by width of the field of view and resolution of camera. Can calculate if customer stands in view with an object of known size.
- **Frame thresh**
  - The number of frames/seconds that the model must detect an analytic on before an alert is sent. The standard for most analytics is 2 detections per 5 frames received.
- **Cool down period**
  - A set amount of time between generating alerts to prevent overloading a system. The standard period is 30 seconds but is configurable on our end.
- **Minimum confidence level**
  - The lowest confidence the model can have in an object classification before a detection is made. 50% - 65% minimum confidence levels on most analytics to reduce FPs while staying sensitive to true positives.
- **Crops**
  - A tool that allows us to zoom in and only run analytics on a selected part of the frame. Increases performance at long distance. Can not be used with slicing
- **Slicing**
  - A tool that breaks the camera frame into a grid pattern and has the model analyze each grid piece individually before stitching back together. Increases model performance at a distance without the restriction of crops. Only available for intruder and vehicle detection.
- **IoU (Intersection over Union)**
  - The amount of overlap between the bounding box of a detection on one frame and on the next. If there is a large overlap, the object is likely not moving, while if it is small, the object is likely moving. Is in effect on all cameras, but is used by the stationary vehicle filter as well.
- **Stationary vehicle filter**
  - When enabled, the model will filter out and ignore all stationary vehicles, preventing sending false positive alarms. There is also a Vehicle Filter, which prevents any vehicle from being detected.

Optimize Existing Security Systems with Actuate AI

actuate

Actuate is a real-time, cloud-based AI video analytics company that offers industry-leading leading threat detection software.

Accurate, real-time detections	Requires no new or additional hardware	Real-time, informative quick alerts	Wide variety of use cases
Drastically reduce false positives	Cost-effective, software-only, system agnostic integration	Turns security video footage into actionable intelligence, minimize response time	Central stations, industrial facilities (construction sites, etc) and private/public spaces (schools, retail establishments, etc)