SENSTAR | Sensor Fusion Engine

Increase security.
Defeat nuisance alarms.

Nuisance Alarms: An Ongoing Concern

The early detection of intruders, while they are still at the perimeter and away from buildings or sensitive areas, is a key component of a site's security plan. Modern, well-designed perimeter intrusion detection sensors and video analytics have consistently demonstrated a high level of performance and value, protecting critical sites and infrastructure around the world.

However, all individual perimeter intrusion detection technologies have inherent deployment challenges, especially in specific situations. The key difficulty is maintaining a high probability of detection without increasing the nuisance alarm rate (NAR).

	Fence Sensors	Video Analytics / Line-of-Sight Sensors
Detection method	Analyze disturbances of the fence fabric	Analyze changes within coverage area or data signals
Strengths	Limits detection to the fence line, the key demarcation point at which human activity becomes an actualized threat	Detects activity within coverage area and works independently of physical barriers like fences
Challenges	• Stealth attacks • Gate areas • Inadequate fences • Extreme conditions	• Line-of-sight restrictions • Poor visibility conditions • Nearby non-threat activity • Recalibrations due to site changes

These deployment challenges can be mitigated through a variety of methods, including improving physical deterrents, maintaining a sterile perimeter, and careful site design. However, what if there was another way, one that was both highly cost-effective and designed to address these real-world challenges?

A Solution for the Real World

Sensor fusion solves the real-world challenge of nuisance alarms once and for all. By using sophisticated AI techniques, it combines inputs from different sensor types to identify security threats intelligently and reliably. Sensor fusion can defeat nuisance alarms while increasing the Probability of Detection and is ideal for protecting specific areas, zones or situations where existing individual technologies are not sufficient.

High Risk Zones

Zones that are deemed at a high risk of intrusions (for example, remote segments of the perimeter or those with obscured sight-lines) may require a higher level of security.

Noisy Gates

Depending on construction, some gates may generate excess vibrations on or near the moving section(s) during operation as well as during high wind events. Sensor fusion can eliminate the resulting nuisance alarms while maintaining detection capabilities.

Inadequate Fences

Sensor fusion can help compensate for the higher risk level at sites with fences that are inadequate for changing or unforeseen security requirements (for example, those lacking in height or outrigger, as well as those with damaged or loose fence fabric).

Extreme Conditions

Most nuisance alarms generated by strong winds can be mitigated by proper fence maintenance and sensor calibration. However, sites that experience severe storms, irregular gusts, or are in high-vibration environments can deploy sensor fusion along specific perimeter segments that are prone to nuisance alarms.

Sensor Fusion Engine: Perimeter Security Evolved

The Senstar Sensor Fusion Engine is a breakthrough technology that synthesizes data from separate systems to generate actionable information. More than just a simple Boolean logic integration, the sensor fusion engine accesses low level data to intelligently characterize potential risks. Data synthesis enables the system to achieve levels of performance that exceed those of the individual sensors.

How Does It Work?

Senstar's perimeter intrusion detection sensors and video analytic (in-house trained deep learning model) solutions offer industry-leading performance and have proven themselves to be suitable for the most demanding of security applications. However, by synthesizing the raw data from individual sensors and analytic engines, a process which involves the analysis of multiple types of data and sources, the performance of the overall solution is substantially improved, with a particular focus in reducing if not eliminating nuisance alarms.

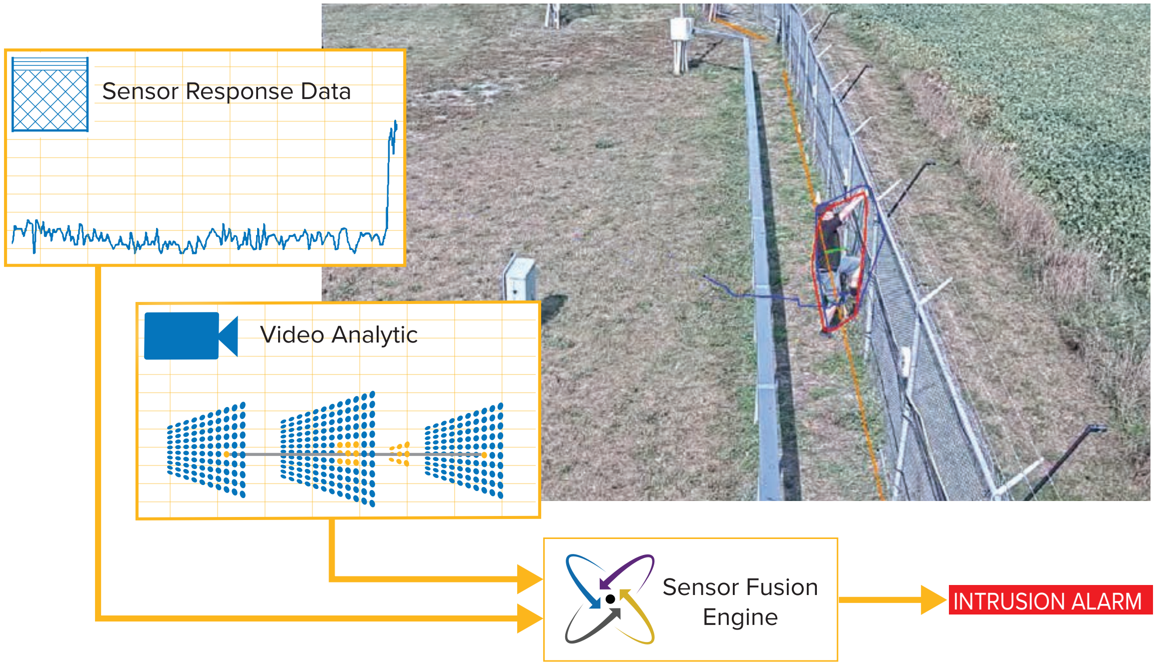
At the same time, sensor fusion increases the Probability of Detection (PD) by allowing the system to react to smaller influences via the use of multi-input probability calculations. A built-in confidence calculation simplifies system configuration while ensuring the optimal performance is achieved.

Built-In Equipment Failure Support

To avoid the potential of incorrect operation as a result of obscured video streams, equipment failure, or a loss of network connectivity, the Sensor Fusion Engine monitors video streams, data flow and communications to determine the health of the sensors. The engine will shift the weighting of the sensors and use only analytics data or sensor data when necessary, and will automatically resume regular operation once sensor functionality and communications are restored. Note that equipment and network issues will also generate trouble alarms to ensure operators remain fully aware of the system's status.

Sensor Fusion vs Boolean Logic

Sensor fusion is not a Boolean logic combination of sensors (e.g. it does not perform logical OR/AND/XOR/NOR operations on individual sensor alarm outputs). Rather, it uses raw data from video analytics and sensors, including time, location and historical values. The fusion process offers better detection capabilities and lower nuisance alarm rates over that of a Boolean logic integration.



Sensor Fusion Engine detecting a daytime fence climb. In this example, the engine is using video from a any ONVIF-compatible surveillance camera (include low-light and thermal). Data from an deep-learning trained video analytic is synthesized with live and historical fence response data from a FlexZone processor to intelligently characterize the risk (valid intrusion attempt).

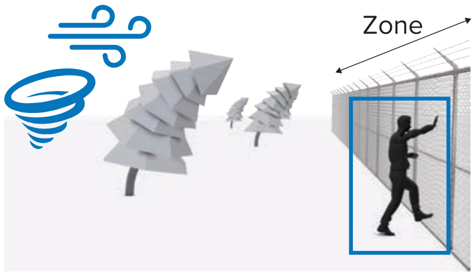
Sensor Fusion vs Boolean Logic Performance

This section looks at different scenarios where there is the potential for valid intrusions as well as nuisance alarms. The perimeter is protected by a fence equipped with ranging fence sensor and a camera equipped with a people tracking video analytic. The results of both a Boolean logic integration and the Sensor Fusion Engine are compared.

SCENARIO

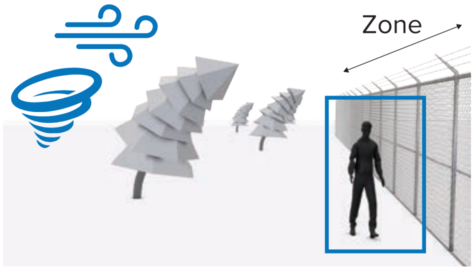
Intruder

An intruder attempts to climb the fence in zone 1 at location 30 m. At the same time, extreme wind conditions create multiple disturbances on the fence at locations 10, 20, and 40. This results in potentially 4 events being generated.



Walker

A person (non-intruder) is walking along zone 1. At the same time, extreme wind conditions create multiple disturbances on the fence at locations 10, 20, and 40. This results in potentially 4 events being generated.



Ladder (Stealth) Climb

A skilled intruder performs a stealth climb using a ladder. In this type of intrusion, there may not be enough data collected for a fence sensor to generate an alarm (typically this would be mitigated through the deployment of fence outriggers like barbed/razor wire and/or a multi-pass cable configuration).

COMPARISON OF RESULTS

Intruder

Boolean Logic Integration

With an AND operation, there are 2 nuisance alarms generated and 1 valid alarm.

Sensor Fusion Engine

Only 1 (valid) alarm is generated (0 nuisance alarms)

Walker

Boolean Logic Integration

With an AND operation, there are 3 nuisance alarms generated. With an OR operation, there are 4 nuisance alarms generated.

Sensor Fusion Engine

0 nuisance alarms generated (the correct response)

Ladder (Stealth) Climb

Boolean Logic Integration

With an AND operation, 0 alarms are generated (the worst possible result!). With an OR operation, there would be 1 (valid) alarm.

Sensor Fusion Engine

1 (valid) alarm is generated

CONCLUSIONS

These scenarios show that:

- AND integrations create a high level of risk: if one sensor does not alarm due to a missed detection or equipment/network failure, no system-level alarm will occur.
- OR integrations increase false and nuisance alarm rates, resulting in the potential for valid alarms to be ignored.
- Sensor fusion will only alarm on relevant events, enabling the operator to focus on important tasks.

Deployment Considerations

The Sensor Fusion Engine is designed to solve specific problems related to high-risk or problematic segments of the perimeter. It may be applied to parts of zones, individual zones, or along the entire perimeter.

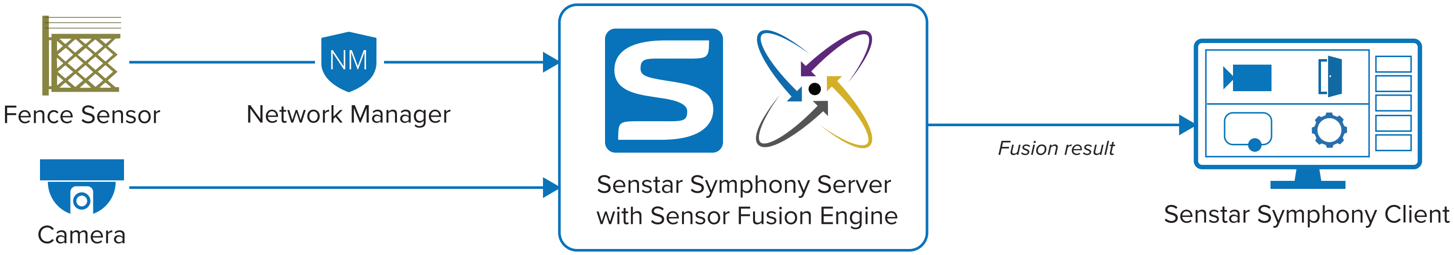
Depending on the site's existing infrastructure, the Sensor Fusion Engine may be deployed as part of a full-featured Senstar Symphony Common Operating Platform solution, or as a drop-in solution that complements the existing third-party security or video management system (SMS/SMS).

To deploy the Sensor Fusion Engine, a site requires:

- Network cameras with perimeter visibility (up to 40 m per detection channel) (for longer zones, multiple detection channels may be used).
- A FlexZone-60 fence sensor with ranging enabled and equipped with Ethernet networking (star topology).
- Sensor Fusion Engine enabled for each camera/sensor segment (either via Senstar Symphony Common Operating Platform software or via Sensor Fusion Engine drop-in solution).

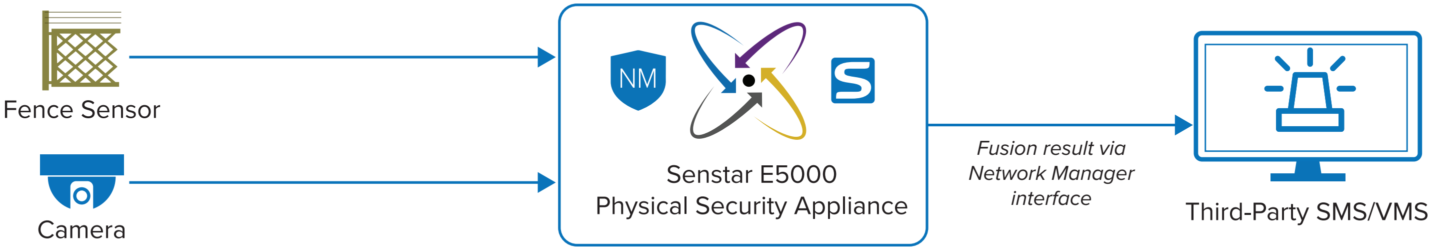
FULL-FEATURED SENSTAR SYMPHONY COMMON OPERATING PLATFORM SOLUTION

In this configuration, the sensor fusion engine is deployed within a full-featured Senstar Symphony solution, enabling operators to receive sensor fusion alarms alongside video and events from other perimeter intrusion detection sensors, access control devices, and video analytics.



SENSOR FUSION ENGINE DROP-IN SOLUTION

In this configuration, the Sensor Fusion Engine is preinstalled on a physical security appliance (PSA) and integrates with an existing SMS/VMS. Alarms from the Sensor Fusion Engine are communicated to the SMS/VMS via the Network Manager's Alarm Logic Engine (ALE), which supports all major SMS/VMS platforms and offers a range of integration options.


Fence Sensor
Camera
NM
Senstar E5000 Physical Security Appliance
Fusion result via Network Manager interface
Third-Party SMS/VMS

Technical Specifications

	Senstar Symphony Common Operating Platform		Drop-in Solution
	Server Farm	E5000 Physical Security Appliance	(for use with existing SMS/VMS)
DESCRIPTION			
Hardware platform	R-series or other supported hardware	E5000 Physical Security Appliance	E5000 Physical Security Appliance
Senstar Symphony version	Standard or Enterprise (R-series includes Symphony device licenses, other hardware may require separately purchased licenses), v8.5 or newer	Standard license included, v8.5 or newer	NA
Sensor Fusion Engine SKU	S8SW2091-XXY (sensor fusion engine only)	S8SW2091-XXY (sensor fusion engine only)	S8SP0303-001 (includes PSA hardware and software)
Sensor Fusion licenses	1 per channel (separate NMS and ranging sensor software licenses required)	1 per channel (separate ranging sensor software license required)	1 per channel (includes 1 video stream and 1 ranging sensor connection)
Number of sensor fusion channels	Dependent on server resources	4 per appliance (maximum)	4 per appliance (maximum)
Network Manager license	Not included (v2.55 or newer)	Included (v2.55 or newer)	Included (v2.55 or newer)
Ranging sensor license	Not included	Not included	Included
Maximum zone distance	40 m (131 ft)	40 m (131 ft)	40 m (131 ft)
Supported camera type	Fixed only (no PTZ)	Fixed only (no PTZ)	Fixed only (no PTZ)
Recommended camera resolution	720p (minimum)	720p (minimum)	720p (minimum)
Video management	Yes	Yes	No
Access control	Yes	Yes	No
Security management	Yes	Yes	No
Additional video analytic support (with license)	Yes (number dependent on server resources)	Yes. Up to 4 video analytics, including sensor fusion channels.	No
ONVIF server	Yes	Yes	No
Network Manager integration options	Yes	Yes	Yes

Copyright © 2023. All rights reserved. Senstar and FlexZone are registered trademarks of Senstar Corporation. Windows is a registered trademark of Microsoft Corporation. Senstar Symphony is a trademark of Senstar Corporation. R4-04/23

SENSTAR®