



Outdoor Video Security: Nine Success Factors

What You Will Learn

The effectiveness and costs of automated outdoor video surveillance solutions vary widely. This white paper, intended for people who manage and implement outdoor surveillance solutions for perimeters or buffer zones, discusses:

- Sources of nuisance alarms and how to prevent them
- Security violations that human operators commonly miss and how to reveal them
- The value of obtaining precise location information about the target
- The effect of camera range and detection accuracy on overall solution costs

Challenges of Outdoor Video Security

The goal of outdoor video security is to detect an intrusion in time to prevent or minimize harm. Factors that commonly thwart this goal include unreliable results, imprecise information about the intruder's location, and high costs.

Unreliable Results: Cameras That Cry Wolf

Video analytics software offloads the burden of event detection from human operators. When the software detects a possible intrusion attempt, it sends an alert to the operator, who then views the video to decide on a response. Until now, the main barrier to the success of video analytics has been the high volume of false alarms and nuisance alarms, which can be caused by:

- Camera shaking caused by wind gusts and vibrations from trucks, trains, and other sources
- Moving leaves, clouds, rain, snow, and water reflections
- Camera malfunction due to extreme temperature, humidity, dust, or sand

These factors can easily contribute to 10 or more false alarms per camera each day.¹ In a facility with 45 cameras, that's at least 450 false alarms daily, or almost one every three

¹ Consider the U.S. Department of Homeland Security's conclusion that 90% of sensor alerts on the Northern and Southern borders were false alarms. (Source: http://www.dhs.gov/xoig/assets/mgmt/rpts/OIG_06-15_Dec05.pdf)

minutes. As a result, security personnel spend their time unproductively investigating phantom threats. They can become indifferent to nuisance alarms, making it unreasonable to demand accountability. What's more, constant nuisance alarms lead security personnel to distrust the system, and possibly to even turn off the alarms.

Missed Events: Uncooperative Light and Shadows

In the real world, neither ordinary surveillance cameras nor the human eye can detect certain events because of poor lighting, shadows, clutter like shrubbery, light reflection, ripples in the water, and so on. These issues can prevent an operator from seeing intruders.

Lack of Location Information: Where is the Intruder Now?

Most cameras do not report the target's GPS location when sounding an alarm. If they provide location information at all, it's a rough estimate. Nor do most cameras capture the target's size and velocity. Lack of precise information about location, size, and velocity creates several problems:

- **Delayed response:** The time security personnel spend looking for the suspect delays response.
- **Nuisance alarms due to lack of perspective:** Cameras lack perspective, and therefore cannot determine if a detected target has actually entered a defined alarm zone. For example, if a camera detects a target near the fence but does not know its GPS coordinates, it can't determine whether the target is on the side of the fence that you care about.
- **Nuisance alarms from non-human targets:** Without information about a target's size or velocity, the camera cannot perform accurate filtering, or easily determine whether the target is an actual human intruder, a vehicle, or an animal. Without certain knowledge, the only recourse is to dispatch a security officer for an onsite visit, an inefficient use of resources.
- **Inability to find the intruder with PTZ cameras:** If cameras can't relay a target's precise GPS location to a PTZ camera, then security personnel have to manually steer the camera to attempt to find and track the intruder. This is nearly impossible in large areas. Therefore, operators have to treat all targets as threats, which is an inefficient use of resources because many targets might be legitimate visitors such as maintenance personnel.

*Security personnel become
indifferent to nuisance alarms,
making it unreasonable to
demand accountability.*

High Costs

The costs of outdoor video surveillance include the cameras as well as the infrastructure, including mounting poles, video storage, and power and communications lines. The infrastructure cost to support a camera often equals or even exceeds the cost of the camera itself.

Nine Criteria for Outdoor Video Surveillance Systems

Organizations can overcome the limitations of automated outdoor video surveillance by deploying solutions that provide the following capabilities:

- **Filter out camera motion:** The sensor should not issue an alarm in response to an image change caused by camera movement—say, from a wind gust or passing truck. This is common when cameras are mounted on poles or buildings and looking over great distances. Filtering out this type of nuisance alarm requires image stabilization technology.
- **Filter out non-salient motion:** A different type of intelligence is required to recognize non-salient motion that occurs in nature, such as moving leaves and water reflection. Eliminating this type of nuisance alarm further increases operators' trust in the system, making it practical to hold them accountable for investigating alarms that make it through the filters.
- **Dynamically correct lighting:** The camera must have the intelligence to adapt to lighting changes that occur throughout the day. A good test is whether the sensor can detect moving people or objects in shadows, and distinguish legitimate targets from patterns such as moving clouds.
- **Detect small targets in presence of clutter:** From a distance, the human eye might miss a person walking through plant life. Advanced detection sensors can identify slight movements, even in the presence of scene clutter.
- **Eliminate network intrusion and tampering:** If unauthorized people can access the video surveillance network, they can see what you see. This can enable them to identify and exploit any coverage gaps. The solution is to encrypt video and management commands so that information flowing over the network is useless even if intercepted.
- **Accurately report target location:** Precise location information about a target enables a swift response. Showing the target's location on a map, as opposed to simply reporting its GPS coordinates, makes it easier to dispatch personnel and increases situational awareness. Supplementing the location with information about the target's dimensions and velocity can help the sensor determine if the threat is real—and not a rabbit, for example—before sending an alert.
- **Withstand outdoor environmental conditions:** Many so-called outdoor video surveillance cameras are really indoor cameras with an add-on protective

enclosure. They are susceptible to extreme temperatures, sand, dust, and humidity, which degrade the camera's ability to accurately detect targets and shorten equipment life. Outdoor cameras must be designed from the outset to withstand changing or extreme environmental conditions.

- **Provide accurate coverage over a long range:** The longer or wider the camera's range, the fewer that are needed. This reduces capital expense as well as associated infrastructure costs. However, it defeats the purpose to deploy cameras so far apart that they cannot provide enough visual detail to determine an appropriate response or provide forensic detail. Typically, detail is considered adequate when the camera can zoom in close enough so that the intruder is large enough to be identified.
- **Automatically control PTZ cameras:** Solutions that capture GPS positioning data can use it to steer PTZ cameras to automatically track and zoom in on intruders, making the target large enough to reliably identify. Automatic control is especially valuable for facilities that monitor large areas or use long-range detection cameras.

Information about the target's dimensions and velocity can help the sensor determine if the threat is real — and not a rabbit, for example — before sending an alert.

The table below summarizes the requirements for effective outdoor security.

Goal	Solution Requirement
Practically eliminate nuisance alarms	• Filter out camera motion from wind and vibrations • Filter out non-salient motion in the scene • Set rules to not report on certain targets based size, speed, or area • Dynamically adjust for changing lighting conditions
Enable operators to see what they would otherwise miss	• Detect small targets in the presence of clutter • Provide sufficient detail of target—typically more than 10% of monitor height • Eliminate mis-detects from dust, sand, rain, or snow in camera view • Dynamically adjust for changing lighting conditions
Accurately report target location	• Report GPS target coordinates and display intruder's location on a topology map
Contain costs	• Provide accurate coverage over a long or wide range • Extend sensor life by protecting against environmental conditions

Table 1: Requirements for Automated Outdoor Video Security

SightLogix Outdoor Video Security Solution

Specially designed for perimeter and outdoor area surveillance, SightLogix SightSensor cameras meet the requirements for operator trust and low lifetime costs.

Practically Eliminate Nuisance Alarms

SightSensors are the only outdoor video cameras with multiple built-in Digital Signal Processors (DSPs) that have the intelligence to virtually eliminate nuisance alarms. One DSP is dedicated exclusively to filtering out camera motion. Another filters out other motion such as foliage, fast-moving clouds, and water reflections.

Reveal Movement You Might Miss

SightSensors perform specialized processing to detect movement that shadows would otherwise hide. In Figure 1, the left image shows two targets detected within small clutter and moving foliage that a human operator would likely miss. The right image shows how the SightLogix SightMonitor reports the intruder and location by superimposing the target on a topology map.

Prevent Snooping with Encryption



Figure 1: Special Processing Reveals Target Despite Clutter and Non-Salient Motion

SightSensors encrypt video, metadata, and commands with AES (Advanced Encryption Standard), preventing would-be intruders from seeing what you see. Attempts to tamper with cameras are logged and immediately reported as alarms.

Do a Better Job with Fewer Cameras

Used to protect perimeters, SightSensor cameras can detect a human intruder at 1,500 feet, approximately three times farther away than most sensors. Used to create buffer zones, SightSensors can cover approximately nine times more area than other cameras. Figure 2 shows the coverage area for SightLogix cameras compared to cameras with a smaller coverage area.

With their longer range and greater detection accuracy, SightSensors reduce camera, infrastructure, and storage costs by one-third, as shown below in Table 2.

Outdoor Security Task	Cost of SightLogix cameras and infrastructure	Cost of nearest competitor's cameras and infrastructure	Savings using SightLogix
Monitor 4-mile perimeter	15 cameras spaced 1,500 feet apart: \$395,000	45 cameras spaced 500 feet apart: \$831,000	\$436,000
Monitor buffer zone of 168,750 square feet	2 cameras, \$43,000	8 cameras, \$108,000	\$65,000

Table 2: Longer Range Significantly Reduces Camera Costs

Report Target GPS Location

SightSensor cameras use a unique “georegistration” technique to capture the GPS location of intruders and superimpose them on a map of the facility (Figure 3). Security personnel can continuously track and report the intruder’s exact location in relation to the facility. The GPS information is also used to automatically steer a PTZ camera to follow the target, zooming in so that the intruder fills at least 10% of the screen. This provides sufficient visual detail for intruder identification and later forensic analysis.

Endure Outdoor Conditions

Enclosing an indoor surveillance camera in a protective enclosure might protect against some conditions, such as rain, but it does not protect against humidity, sand, and extreme temperatures. SightLogix SightSensor cameras are specially designed for outdoor use. A sealed, nitrogen-filled NEMA 4X-compliant enclosure keeps grit, dust, or humidity from getting in, and an auto lens defogger ensures crisp images and range even in humid conditions. SightLogix cameras are currently in operation in the Canada Oil Sands at -58° F and in the Middle East at 158° F.

Conclusion

Realizing the promise of automating outdoor video security requires a solution that is trustworthy, reveals what the human eye would miss, and is cost effective. The SightLogix solution meets these requirements by using unique technology to:

- Virtually eliminate nuisance alarms so that operators trust the system and managers can demand accountability
- Accurately report target location information as well as target size and velocity, superimposing the information on a facilities map
- Cover approximately three times the distance of other sensors, reducing capital and infrastructure costs

About SightLogix

SightLogix is an established technology leader in proactive, long-range and wide-area automated surveillance solutions specifically designed to protect critical outdoor infrastructure and key assets. The company's open-architecture, Intelligent Video Surveillance system provides full situational awareness to increase the effectiveness and efficiency of security manpower.

Information and Resources

- To perform an online perimeter security design of your facility in minutes, visit: www.sightlogix.com/sightsurvey.html
- To read more about SightLogix SightSensor technology, visit: www.sightlogix.com.
- To request a meeting with a solution specialist, email info@sightlogix.com or call 609.951.0008.

Contact SightLogix

Call: +1 609.951.0008
Email: solutions@sightlogix.com
Visit: www.sightlogix.com
SightLogix, Inc.
745 Alexander Road
Princeton, NJ, USA 609.951.0008

© SightLogix, Inc. All rights reserved. SightLogix, SightSensor, SightSurvey and the SightLogix logo are trademarks of SightLogix, Inc. All other trademarks or registered trademarks contained herein are the property of their respective owners