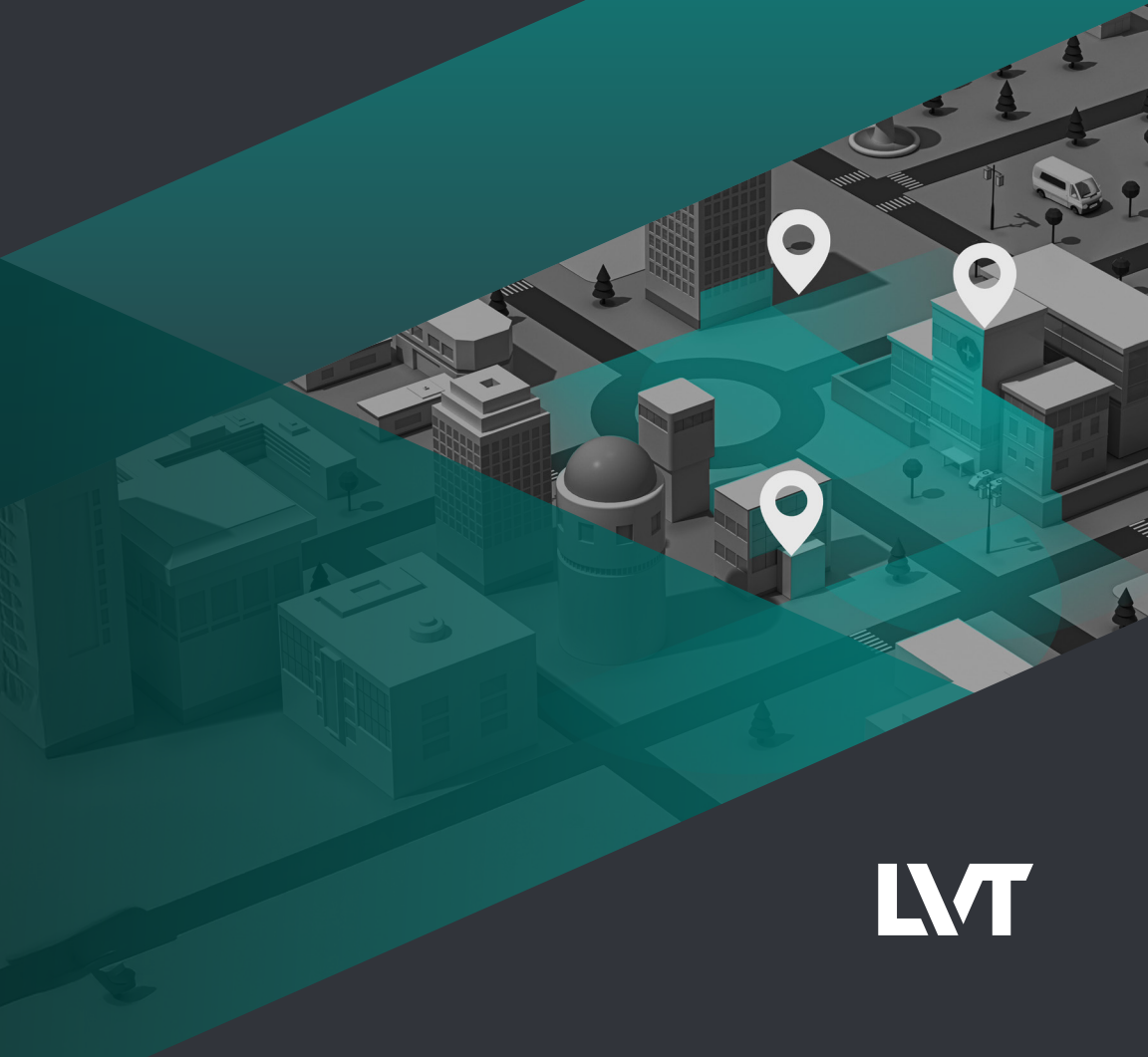


OWN THE OUTSIDE:

Full Site Coverage Buyer's Guide



LMT

With evolving business environments come new threats. Relying on fragmented, reactive security measures is no longer a sustainable strategy. This guide introduces a strategic shift to greater coverage through intelligent site management (ISM). By embracing a unified, proactive security model focused on achieving complete coverage, you can transform your physical security and cut costs.

Discover how to eliminate blind spots, deter threats before they escalate, and unlock critical operational intelligence across your entire enterprise.

An illustration in a dark teal color palette depicting a security scenario. In the foreground, a person in a hoodie is crouching near a car. In the background, several cars are parked on a street, and a few figures are running. Security cameras are mounted on poles and buildings. The overall scene suggests a focus on surveillance and security measures.

The Problem with Piece by Piece Security

Security cameras are typically low-deterrence and only help after an incident.

Security guards are expensive and fallible, requiring scheduled breaks and time off, which can lead to higher overhead.

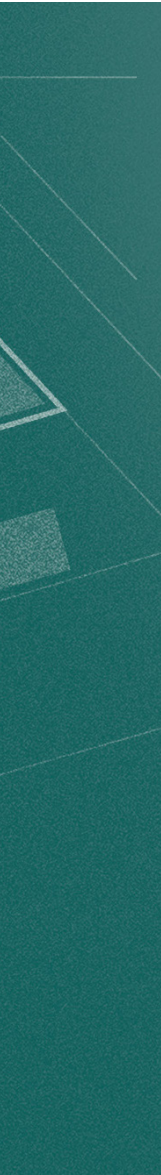
Most organizations today reactively secure their sites with traditional security methods, which create gaps in coverage and operational blind spots.

The flaw in a reactive security strategy is that it involves waiting to respond, a strategy that ultimately leads to greater losses, clean-up costs, and evidence-only outcomes.

A proactive security approach leverages deterrence and detection technology for stronger coverage, which leads to crime prevention, minimized loss, and higher deterrence rates. To achieve this, you should consider a security solution that offers various form factors to meet your site's unique needs. This can look like a unified approach using building-mounted cameras, pole-mounted cameras, and mobile security units (MSUs) to offer full coverage wherever you need it.



The Strategic Shift to Greater Coverage



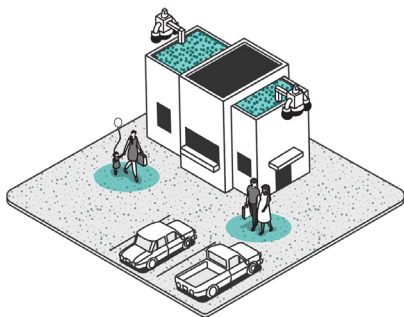
*Companies are adopting an **intelligent site management (ISM)** strategy where security can become proactive in nature and other departments within the organization can unlock new operational and business insights.*

Intelligent site management is a proactive approach to physical security that utilizes AI-powered, rapidly deployable technology to detect, deter, and manage security risks and operational insights across an entire property or organization.

*An ISM strategy is
built out in three
main steps:*

1. Achieve full site coverage with flexible sensors and infrastructure.
2. With this infrastructure in place, proactively deter bad actors and gain intelligent insights.
3. Improve response times across security and other operations, enhancing ROI.

The First Step: Mastering Coverage



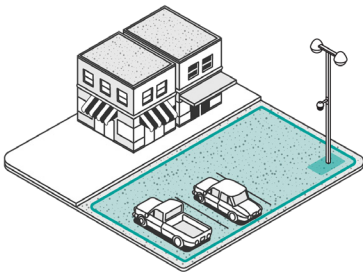
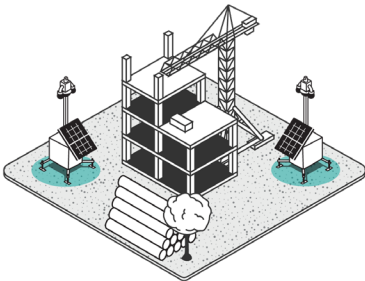
What do we mean by full site coverage? *It means efficiently eliminating all blind spots and ensuring 24/7, uninterrupted visibility for your entire site or sites, even at remote or temporary sites without fixed power or network infrastructure.*

The Challenge of Visibility Across Diverse Sites

Most businesses have multiple sites to secure, and it can be a major challenge to cover diverse environments from one platform with traditional security measures. You need a unified security platform that works across all location types, from the most remote to the most centralized.

Achieving Coverage with Flexible Form Factors

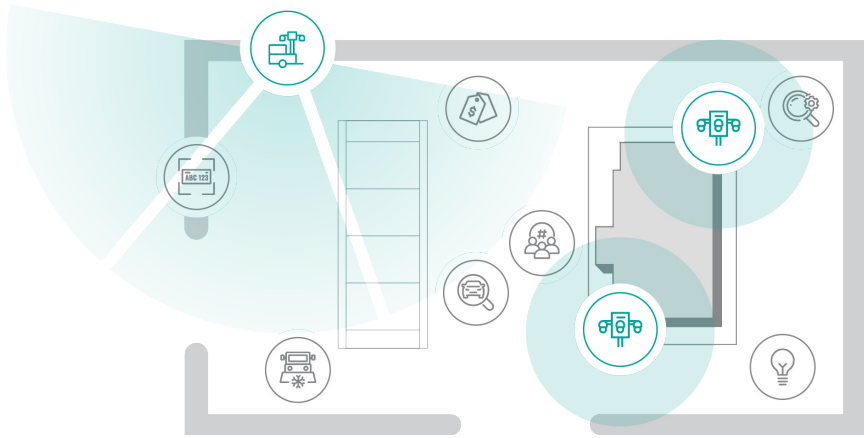
A proactive security approach uses deterrence and detection technology. To offer full coverage wherever you need it, consider a security solution that offers various form factors to meet your site's unique needs. This includes a strategy using building-mounted cameras, pole-mounted cameras, and mobile security units (MSUs).



Conducting a Strategic Site Assessment

When assessing your site for security coverage, you must identify blind spots that traditional, fixed-location cameras can't reach. Below is a quick site assessment checklist:

- 1. Target assets and threats:** What high-value assets are you protecting? Where have past security incidents occurred? Which hours are most vulnerable?
- 2. Map visibility and access:** Where are the blind spots? Where are the main entry and exit points? Are buildings or landscaping obstructing any important viewpoints? What is the lighting situation in this area?
- 3. Define placement and response:** What type of coverage do I need? Is a mobile security unit the best choice, or should I set up building or pole mounted cameras?
- 4. Optimizing cost and coverage:** How can I have full coverage without wasteful overlap? Where can I strategically place the least amount of security solutions to eliminate blind spots and save on cost?



Coverage as a Business Enabler

*Once full site coverage is established, the collected security data is no longer just for evidence—it's a **tool for business improvement and operational efficiency.***

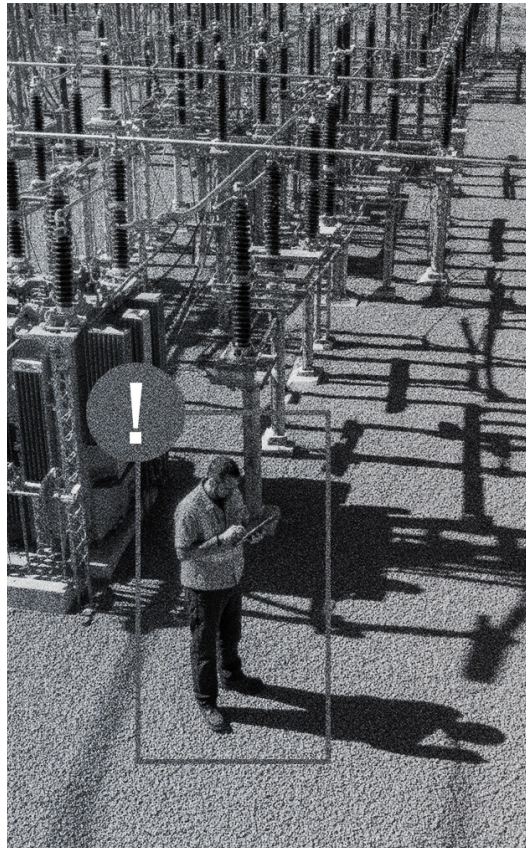
When businesses pursue the intelligent site management approach, they secure all their facilities easily from one platform.

Here are a few examples of how actual businesses can use intelligent site management to improve their operations:

ELECTRICAL SUBSTATION

Security solutions were placed at an electrical substation to prevent trespassing, but those same cameras can also be used to:

- » Alert the site manager of a temperature spike from one of the transformers using thermal camera capabilities.
- » The system then evaluates the area and reviews recent footage to look for anything that might have contributed to the spike in temperature.
- » The system uses data to train itself to predict these spikes earlier.
- » Identify permitted on-site activity
- » Confirm that repairs or work was completed.
- » Monitor for hazards like animal activity, balloons, litter, etc.





OFFICE BUILDING

Security solutions were placed in the office building parking lot to prevent vehicle break-ins, but those same cameras can also be used to:

- » Detect snowfall and accumulation
- » Manage contractors, ie. snow removal crews
- » Verify invoices for contractors based on times they were present on the property
- » Measure and verify employee activity
- » Ensure site maintenance like trash removal and landscaping

RAILYARD

Security solutions were placed to deter cargo theft, but those same cameras can also be used to:

- » Count each train car every time the train enters and leaves the railyard and alert if there is a discrepancy
- » Check that every cargo door seal and lock is intact on every train car
- » If a broken lock/seal is detected, report the car number to a human operator
- » Monitor wheel and axle temperatures
- » Send alert if any extreme temperatures or wheel damage is detected
- » Monitor and verify high-traffic times, backups, slowdowns, and congestion
- » Remotely investigate needed repairs or resources

OIL AND GAS REFINERY

Security solutions were placed to secure perimeters, but those same cameras can also be used to:

- » Monitor remote areas along a pipeline to prevent unauthorized activity
- » Guard high-value equipment on offshore platforms
- » Send instant alerts when equipment is damaged or malfunctioning
- » Report environmental hazards as soon as incident occurs
- » Detect unusual heat spikes
- » Provide insight into working conditions on-site
- » Monitor limited access areas
- » Verify maintenance and repairs are performed

GROCERY STORE

Security solutions were placed in a grocery store parking lot to prevent crime and loitering, but those same cameras were also used for:

- » Detecting an overdose in the parking lot, which led to a timely medical response
- » A bird's-eye view of their store during a severe flood, which enabled corporate leadership to make crucial decisions for recovery and safety
- » Increasing employees' peace of mind and safety during their early morning and late night shifts
- » Count and verify foot traffic, parking lot patterns, busy hours, and staffing needs

The Full Site Coverage Checklist

Here are questions to ask when evaluating vendors for an ISM-focused strategy.



COVERAGE AND PROGRAM COHESIVENESS

- ☐ **Vendor options:** Does the vendor provide a range of solutions (fixed, mobile, specialized) to cover diverse needs across the entire site/enterprise?
- ☐ **System cohesiveness:** Can all camera systems and security assets work together and be managed from a single, unified platform?
- ☐ **Multi-site management:** Can the vendor easily scale deployment from a few dozen to thousands of units/cameras across multiple regions?
- ☐ **Standardization:** Does the vendor offer the ability to mass-update, manage, and remotely access any number of units from one central interface?



PLATFORM RELIABILITY AND UNIT HEALTH

- ☐ **Uptime definition:** How is "uptime" measured across the entire solution, and does it account for all components?
- ☐ **Connectivity guarantee:** Does the vendor offer multi-carrier, multi-SIM connectivity with seamless failover to ensure no data is lost at remote or congested sites.
- ☐ **Predictive maintenance:** Does the system pre-emptively monitor all components for approaching failure conditions? Can it take corrective measures to self-heal without human intervention?



CYBERSECURITY

- ☐ **Network security:** Does the data exclusively operate on a private network, and is it always encrypted (AES-256 at rest and TLS 1.2 in transit)?
- ☐ **Certifications:** Does the vendor possess critical certifications (e.g., SOC2 Type II) to validate their commitment to data security?
- ☐ **Data privacy:** Does the vendor operate on a private cellular network or a public commercial network? Does the customer control which data is shared?



STREAMLINED WORKFLOWS AND INTEGRATION

- ☐ **Unified VMS:** Does the vendor offer a turnkey video management and alert response system that is VMS-agnostic and features an open API for integration?
- ☐ **Alert response:** Can the vendor validate the context of an event and prioritize which ones require human intervention?
- ☐ **Governance (RBAC):** Does the system allow for granular control over who can access the system (designated rights by site, organization, and role) for a multi-layered security team?
- ☐ **Business operations:** Does the system allow for inventory management and manage customer data to provide business intelligence?

Making the Right Choice for Long-Term Security

A full site security program is not an operational expense—it is a critical, long-term strategic investment.

By moving away from piecemeal, reactive systems and moving toward a single, integrated platform focused on full site coverage, your organization achieves true ownership of the outside. This choice shifts your security strategy from a burden that reacts to loss, to a powerful business enabler that proactively prevents incidents, drives operational insights, and protects your brand's reputation.

A unified, flexible solution ensures a high ROI by minimizing remediation costs, reducing security labor overhead, and providing the centralized data needed to maximize operational efficiency across your entire enterprise. It positions your organization to successfully and seamlessly adapt as security challenges and technology inevitably evolve. The time to transition to a proactive, intelligent security program is now.

