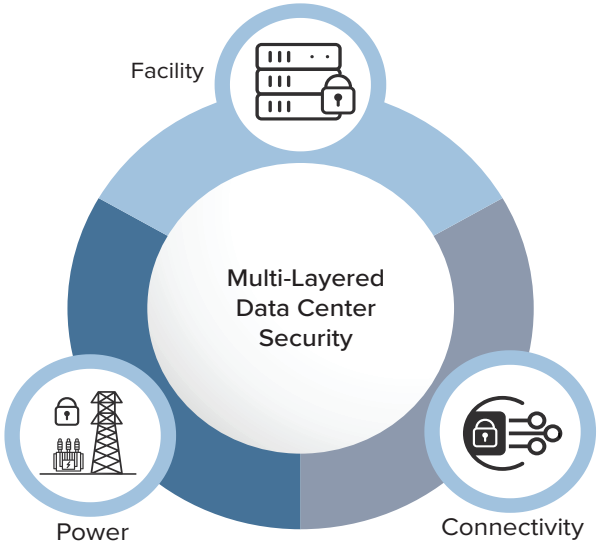
SENSTAR®

Physical Security for Data Centers

Data centers are the engine that drives the digital economy—powering everything from AI and machine learning applications to cloud computing platforms and critical data storage infrastructure. Uninterrupted, continuous operation is essential to maintaining the services that businesses, governments, and consumers depend on daily. Whether supporting real-time AI inference, ensuring 24/7 access to cloud-based applications, or safeguarding sensitive data assets, maintaining customer trust in the protection and availability of these resources requires facility operators to offer the highest level of physical security for the facility itself, its power infrastructure, and external network connectivity.

Physical threats include unauthorized access, vandalism, theft, terrorism, and damage to critical data lines—any of which could disrupt AI workloads, compromise stored data, or bring down cloud services affecting thousands of users. By taking a multi-layered approach to physical security, data center operators can protect these mission-critical computing resources while meeting business requirements and security best practices.



Perimeter Protection for Facility and Power Infrastructure

Protecting the perimeter of a site, be it the facility itself or connected electrical infrastructure, is the first line of defense. Senstar perimeter intrusion detection systems (PIDS) provide early warning of unauthorized entry and offer organizations the following benefits:

- Reliable and effective detection
- Low nuisance alarm rates
- Integration with deterrence devices (lights, sirens) and assessment devices (cameras, analytics, other sensors)
- Effective response to security events using critical information obtained from sensors and surveillance systems

Physical threats	Theft, vandalism, sabotage and trespassing
General deterrence practices	• Security lighting • Perimeter signage and warnings • 2-way intercoms at entrances • Automated PA system • Overt video surveillance

TACTIC	DETERRENCE	DETECTION	DELAY	ASSESSMENT	COMMUNICATION	RESPONSE
Cut, climb or lift fence fabric	Security fence or wall with outrigging Perimeter lighting PA system	Fence sensor LiDAR AI video analytics	High quality, well-maintained security fence or wall	Surveillance system Security lighting 2-way intercom	Automated electronic notifications: - Email - SMS - Mobile app - Clients Site security events linked to specific procedures and contact information	Local security forces
Climb gate	Security gate with outrigging Perimeter lighting PA system	Fence sensor LiDAR AI video analytics	High quality and maintained security gate			
Break or bypass gate lock	Security hardware 2-way intercom Surveillance system	Fence or gate sensor LiDAR Latch contact AI video analytics	Security hardware			
Tunnel under fence or gate	Below-ground fence structure Hardened surface (e.g. concrete) Surveillance system	Buried sensor AI video analytics	High quality and maintained security fence Hardened surface (e.g. concrete)			
Firearms and explosive devices	Ballistic fencing/walls	AI video analytics Audio sensors				
Ladder-assisted climb or elevated position perimeter crossing	Security fence with outrigging	Fence sensor LiDAR AI video analytics	Security fence or wall with outrigging			
Vehicle ramming	Security fence or wall Anti-vehicle bollards	Fence sensor LiDAR AI video analytics	Security fence or wall Anti-vehicle bollards			

Facility Security – Building Management

Facility management encompasses many aspects related to the security, safety, and efficiency of the facility. Senstar, with its innovative portfolio of access control, video analytics, security lighting, and intrusion sensors can ensure any unauthorized access to the building, server rooms, or even individual cabinets is detected and monitored.

Physical threats	Theft, vandalism, sabotage, data theft and trespassing
Operational risks	• Efficient movement and routing of vehicles • Strict access control requirements • Door access to individual server cabinets • HVAC/temperature/fire alarms
General practices	• Multi-zone access control • Security lighting • Automated PA system • Vehicle routing • Equipment monitoring (digital I/O)

CATEGORY	OPERATIONAL REQUIREMENT / RISK	SOLUTIONS
Access control (building and server rooms)	Access via false or misappropriated credentials	Access control system 2-factor authentication Face recognition or other biometric system
	Passback detection	Access control system Face recognition or other biometric system
	Human tailgating	Video analytic + access control system
	Visitors /manual door override	Linked cameras with on-screen door controls 2-way intercom
Vehicle managment	Automated enter/exit	Automatic license plate recognition (ALPR)
	Gate routing	ALPR with delivery management integration
	Parking lot monitoring	Vehicle tracking analytic
	Fire escape obstacles	Left and removed object detection
	Pedestrian/vehicle accidents	AI video analytics
	Safety/night illumination	Instant-on perimeter lighting
	Vehicle tailgating	Video analytic + access control system
Server room security	Human presence	LiDAR (room detection zones)
	Intrusion detection for walls	Wall-mounted sensor (cable, fiber, or accelerometer)
	HVAC/fire/temperature alarms	Monitor third-party HVAC and fire equipment (event-driven video surveillance via auxiliary I/O)
	Temperature verfication	Thermal camera with temperature alerts
Cabinet security	Unauthorized accesss	Monitor door latches (event-driven video surveillance via auxliliary I/O) LiDAR (cabinet detection zones)

Data Line Security

Physical damage to fiber optic cables and communication lines can result in catastrophic data loss, extended downtime, and service disruptions. Whether caused by accidental construction activity, natural disasters, or deliberate sabotage, severed or compromised data lines represent one of the most serious vulnerabilities in data center operations.

Senstar's FiberPatrol FP1150 fiber optic sensor detects third-party interference (TPI) to fiber optic data links and other cable infrastructures before damage occurs. FiberPatrol requires just one optical fiber to detect potential TPI events anywhere along the cable's pathway, determining and reporting the precise location of each event with pinpoint accuracy. Classification abilities can indicate the nature of the intrusion, including the presence of heavy machinery, vehicle traffic, machine and human digging, and direct tampering of the cable conduit—enabling security and operations teams to respond proactively before critical communications are severed.

Beyond intrusion detection, FiberPatrol can serve a vital role by verifying the actual location of buried communications infrastructure and ensuring that redundant data paths do not overlap or exist in close proximity to each other. Many data centers assume their backup communication routes are geographically separated, only to discover during an outage that both primary and redundant cables were damaged in the same construction incident. FiberPatrol enables precise mapping and ongoing monitoring of all cable pathways, confirming true route diversity and protecting against common-mode failures that could compromise data center resilience and business continuity.

Physical threats	Machine and human digging Deliberate tampering Accidental damage
Operational risks	Service interruptions

CATEGORY	OPERATIONAL RISK	SOLUTIONS
Datalink integrity	Machine and human digging	FiberPatrol FP1150 fiber optic sensor
	Deliberate tampering	FiberPatrol FP1150 fiber optic sensor
	Accidental damage from nearby maintenance	FiberPatrol FP1150 fiber optic sensor
Data path verification	Incorrect documentation	Contact Senstar
	Non-redundant paths	Contact Senstar

KEY SPECIFICATIONS

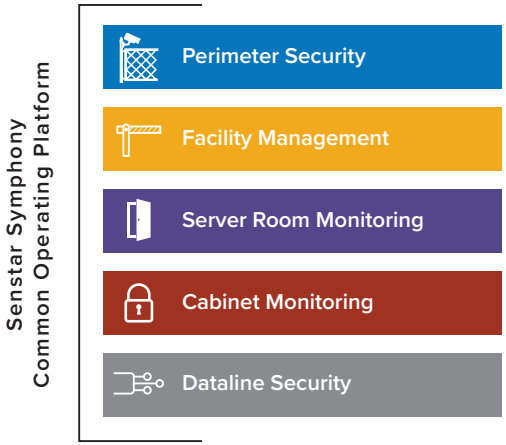
- Up to 50 km (31.06 mi) of TPI detection processing per sensor channel, 100 km (62.1 mi) total
- Detection accuracy: ±4 m (13 ft) typical
- Report threat location by zone, cable distance, or GPS coordinates
- Cut immune configuration
- Use existing communication fiber(s) (assuming performance specifications are met)

FiberPatrol for data conduit detects and locates any disturbance to the communcations conduit, including nearby machine and human digging.

In urban areas, communication lines may be installed in legacy service tunnels and be relatively unprotected from nearby maintenance or construction activities.

Centralized Management of Security and Operations

The Senstar Symphony™ Common Operating Platform with sensor fusion is a modular solution for video management, video analytics, security management, access control and data intelligence. Modules can be used individually, added when needed, or combined as a complete integrated solution. All managed devices report to a shared rules and alarms management system, enabling operators to perform site security or operational functions from a 'single pane of glass'.



INTELLIGENT VIDEO MANAGEMENT

An open platform, Senstar Symphony supports cameras from all major vendors and easily scales to any size. With intuitive operator clients, simple per-camera licensing, and built-in high availability, it is the ideal high-performance video management solution.

- Scalable, high-performance architecture
- Open ecosystem
- Easy to use operator interfaces
- Browser-based administrator client
- Centralized management
- Privacy and security

AI-POWERED VIDEO ANALYTICS

By leveraging existing video surveillance infrastructure, Senstar Symphony video analytics are a highly cost-effective means to augment security with new detection capabilities, direct attention to key events, automate access control and other facility functions, and collect data on customer behavior.

- Object classification and tracking
- Intelligent search and investigation

INTEGRATED INCIDENT AND ALARM MANAGEMENT

A full-featured security management system (SMS), Senstar Symphony delivers a consolidated view of incidents from any source, including intrusion sensors, video analytics, access control, other security devices and general-purpose I/O. Its visual, map-based interface provides a streamlined user experience for operators handling everything from daily routines to crisis situations.

- Streamlined map-centric interface
- Complete sensor integration
- Customizable alarm and event management workflows

UNIFIED ACCESS CONTROL

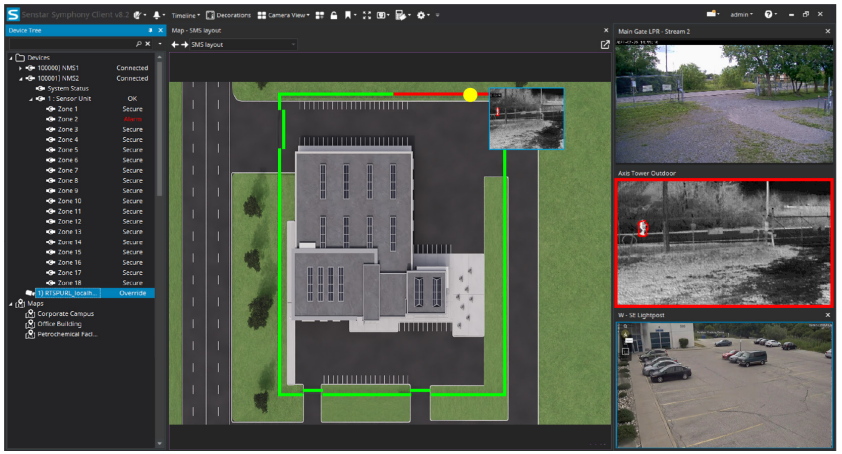
A complete access control system, Senstar Symphony supports industry standard hardware and fully integrates access control events with video and alarm management.

- Integrated operator interface
- Cardholder histories
- Access zones, levels and schedules
- Full-featured administration client
- Unified, seamless integration

OBTAIN OPERATIONAL INTELLIGENCE

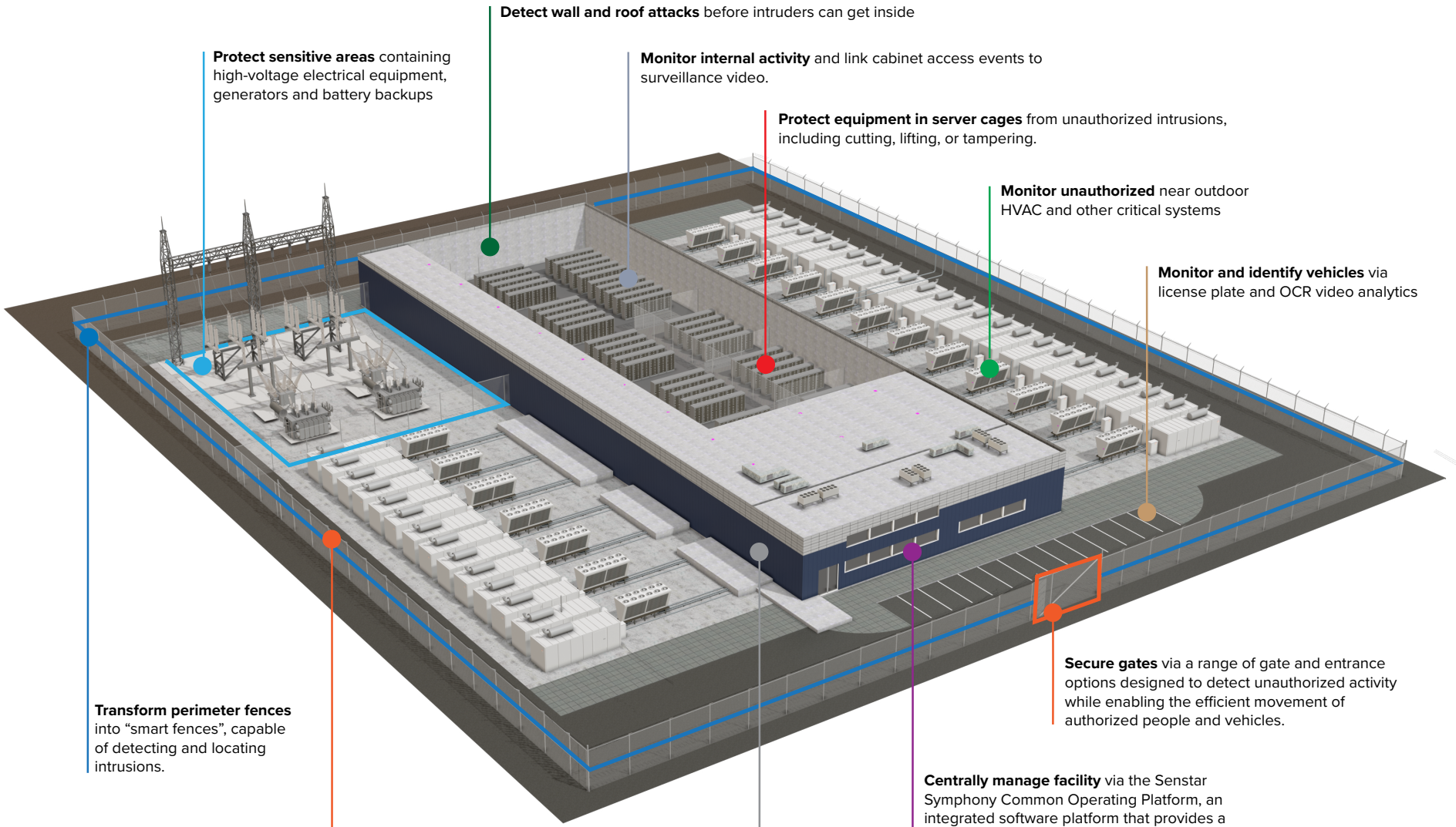
By combining video surveillance with analytics, security sensors, and data from manufacturing or logistics systems, organizations can monitor operations, detect abnormalities, and implement corrective actions.

- Monitor on-site vehicles
- Link video to process events
- Monitor operations
- Empower employees



Senstar Symphony provides a unified interface for all video surveillance, security management, and access control functions. Its support for open interfaces enables it to be integrated with third-party security and I/O devices.

MITIGATE RISK VIA SENSTAR'S PORTFOLIO OF VIDEO MANAGEMENT, VIDEO ANALYTICS, ACCESS CONTROL AND PERIMETER INTRUSION DETECTION PRODUCTS



info@senstar.com • senstar.com