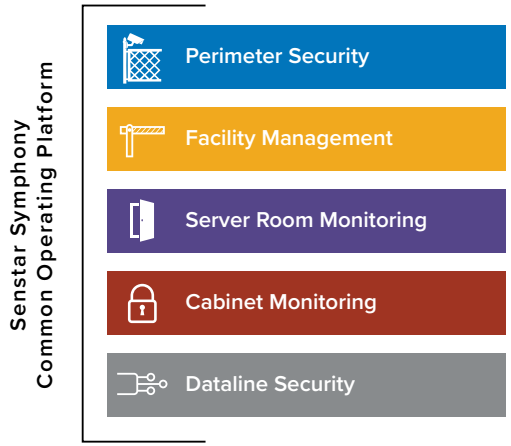
SENSTAR® Physical Security for Data Centers

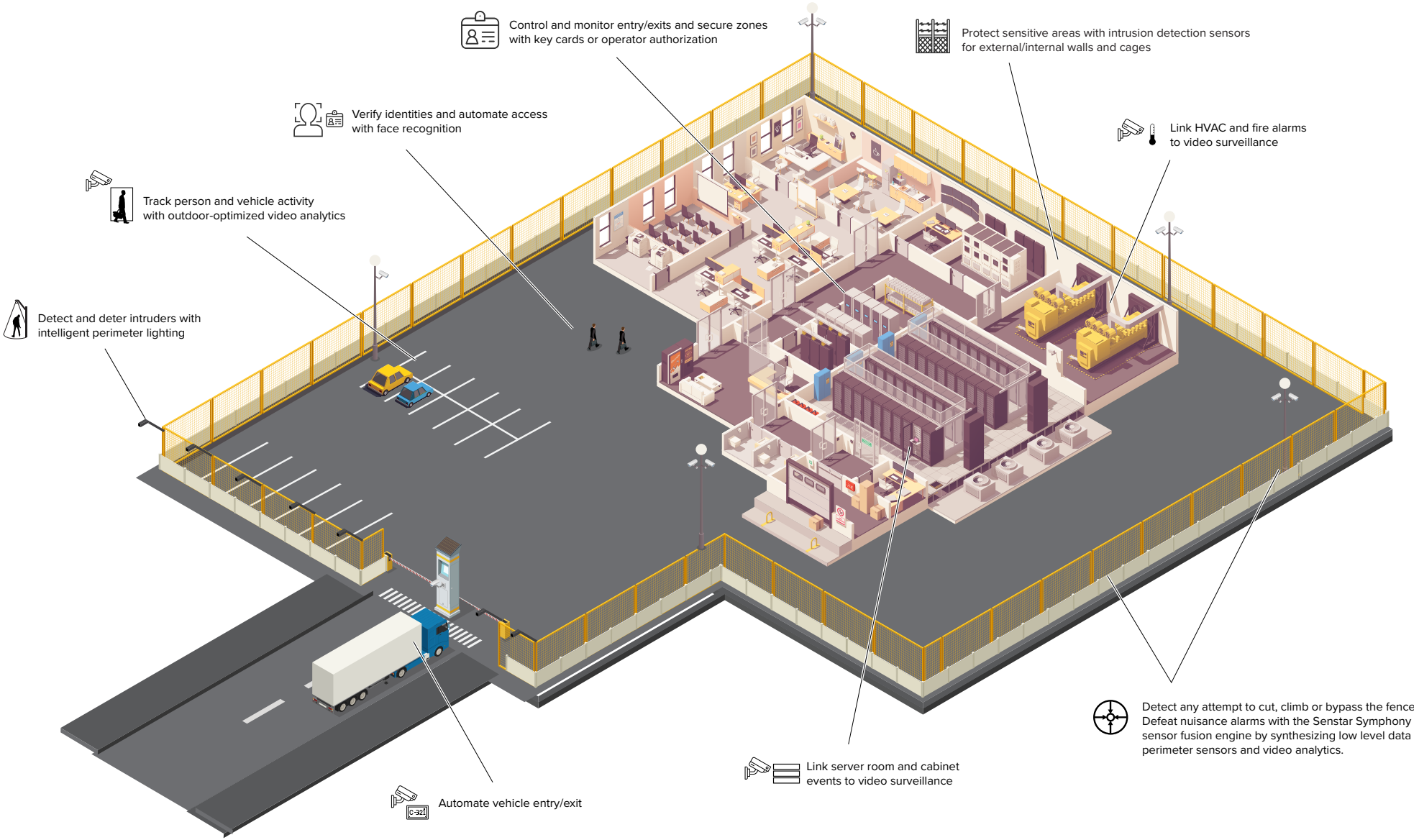
Data centers are the engine that drives the digital economy. Uninterrupted, continuous operation is critical to maintaining the services that an always-connected society relies on. Maintaining customer trust in the protection and availability of their data requires facility operators to offer the highest level of physical security. Physical non-environmental threats include unauthorized access, vandalism, theft, and terrorism. By taking a multi-layered approach to physical security, facility operators can keep customer data secure while meeting business requirements and security best practices.

Recognizing that different facilities face different security requirements, Senstar offers a wide range of video management, perimeter intrusion detection, access control, and video analytic solutions. Individually, they provide best-in-class protection; used in combination and managed under the Senstar Symphony Common Operating Platform, they form an integrated, multi-layered solution.



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.

SENSTAR'S PORTFOLIO OF VIDEO MANAGEMENT, VIDEO ANALYTICS, ACCESS CONTROL AND PERIMETER INTRUSION DETECTION PRODUCTS PROVIDES OPTIONS FOR MANAGING RISK AT DATA CENTERS



Perimeter Security

Protecting the perimeter of a site 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 Outdoor people tracking analytic	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 or gate sensor Outdoor people tracking analytic	High quality and maintained security gate			
Break or bypass gate lock	Security hardware 2-way intercom Surveillance system	Fence or gate sensor Latch contact Outdoor people tracking analytic	Security hardware			
Tunnel under fence or gate	Below-ground fence structure Hardened surface (e.g. concrete) Surveillance system	Buried sensor Outdoor people tracking analytic	High quality and maintained security fence Hardened surface (e.g. concrete)			
Firearms and explosive devices	Ballistic fencing/walls	Outdoor people tracking analytic Audio sensors				
Ladder or other assisted climb	Security fence with outrigging Perimeter lighting PA system	Fence or gate sensor Outdoor people tracking analytic	High quality and maintained security gate			
Vehicle ramming	Security fence or wall	Fence or gate sensor Outdoor vehicle tracking analytic	Security fence or wall			
Elevated position perimeter crossing	Security fence or wall with outrigging	Outdoor people tracking analytic	Security fence or wall with outrigging			

Facility Management & Server/Cabinet Monitoring

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
	Tailgating	Access control system ALPR video analytic
	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	People and vehicle tracking analytics
	Safety/night illumination	Instant-on perimeter lighting
Server room security	Intrusion detection for walls	Wall-mounted sensor
	HVAC/fire/temperature alarms	Monitor third-party HVAC and fire equipment (event-driven video surveillance via auxliliary I/O)
	Temperature verfication	Thermal camera with temperature alerts
Cabinet security	Unauthorized accesss	Monitor door latches (event-driven video surveillance via auxliliary I/O)

Dataline Protection

Senstar's FiberPatrol fiber optic sensor detects third-party interference (TPI) to fiber optic data links and other cable infrastructures. FiberPatrol requires just one optical fiber to detect potential TPI events anywhere along the cable's pathway, and determines and reports the precise location of each event. 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.

The sensor can also be used to verify the location of buried communications infrastructure and ensure redundant paths do not overlap or exist in close proximity to each other.

Physical threats	Machine and human digging Deliberate tampering
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
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
- Up to 1,440 software-definable detection zones
- 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.

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. Highly cost-effective, Senstar Symphony is licensed per security device (camera, door, or sensor). 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 cloud 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.

- Intelligent search and investigation
- Moveable between cameras
- Future-proof with edge analytics

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
- Complete alarm and event management
- Customizable for your environment

UNIFIED ACCESS CONTROL WITH VIDEO SURVEILLANCE

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'S SENSOR FUSION ENGINE

The Senstar Symphony™ Common Operating Platform's sensor fusion engine 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.

For security applications, this has direct, practical benefits, namely the ability to maximize the strengths of individual sensor technologies while avoiding their shortcomings. When signal response data from outdoor sensors is synthesized with video analytic data, nuisance alarms generated by wind or debris are virtually eliminated while maintaining the system's high probability of detection.

info@senstar.com • senstar.com

Copyright © 2025. All rights reserved. Features and specifications are subject to change without notice. Senstar and Senstar Symphony are trademarks of Senstar Corporation. 05/22.