WAVESYS

Ai SURVEILLANCE IN DATA CENTRES

Video surveillance is crucial for data centre security as it provides continuous monitoring, helps deter unauthorized access, and enables prompt detection and response to potential threats. It enhances overall security by integrating with other systems to offer comprehensive protection against physical and environmental risks.

Choosing appropriate video surveillance for your data centre requires assessing security requirements, ensuring integration with current security measures, and opting for systems with advanced functions such as live monitoring, video analysis, and environmental monitoring.

It's essential to choose a solution that complies with relevant security standards and provides scalability for future growth.

The Challenges of Data Centre Security

Data Center Security poses significant challenges in today's digital landscape, with cyber threats constantly evolving and becoming more sophisticated. From physical breaches to malware attacks, data centres must be fortified with robust security measures to protect sensitive information and prevent costly data breaches.

Maintaining a secure environment requires constant vigilance, regular assessments, and advanced technology solutions to stay one step ahead of potential threats. In the face of such challenges, data centre operators must remain proactive and adaptable to ensure the safety and integrity of their infrastructure.

- Preventing physical intrusions and unauthorized access: Unauthorised access to data centres can lead to severe security breaches. WVCA Technology's advanced surveillance systems continuously monitor and alert security personnel to any unauthorised attempts to enter restricted areas.

- Environmental and operational security with integrated monitoring systems: Environmental threats, such as temperature fluctuations or humidity, can impact data centre performance. WVCA Technology's integrated monitoring systems help maintain optimal conditions by providing real-time alerts and insights.

- Compliance issues: Adhering to stringent security regulations and standards is crucial for data centres. WVCA Technology ensures compliance with local and international standards, helping data centres meet regulatory requirements.

By leveraging Wavesys WVCA Technology's advanced solutions, data centres can navigate the complex landscape of security threats, regulatory requirements, and operational challenges with confidence. Our technology not only safeguards your critical infrastructure but also enhances the overall efficiency and reliability of your operations.

Wavesys WVCA ensures Compliance & Privacy

Ensuring compliance with data privacy regulations is a critical aspect of data centre security. That's why our security and video surveillance solutions are designed to meet UK-specific security standards such as GDPR and CPSI / NPSA guidelines.

Moreover, we guarantee international adherence to regulations such as PCI DSS, HIPAA, and ISO/IEC 27001, giving assurance that your data centre operations comply with top security and privacy standards.

Benefits of Wavesys WVCA Technology for Data Centres

Deploying WVCA Technology offers numerous benefits for data centres. Primarily, they can achieve unparalleled security and operational efficiency, ensuring the integrity and confidentiality of their data.

- Using Video Analytics to Enhance Operational Security: Our analytics provides real-time data and insights, allowing security personnel to swiftly identify and respond to potential threats.
- Integrating Environmental Monitoring to Detect Anomalies Early: Early detection of environmental anomalies, such as temperature changes or smoke, helps in preventing potential disruptions or damage to data centre infrastructure.
- Improving Operational Efficiency: Our data centre video surveillance solutions free up resources by automating monitoring and reporting processes, allowing personnel to focus on other critical tasks.
- Video Synopsis Forensic Search: Using our Forensic Search tool, security staff can review hours of footage in minutes and identify potential culprits involved in theft or security breaches.
- Man Down: Data centres operate on a 24-hour basis but quite often with a skeleton staff. In the event of a fall or serious incident in an isolated area with no other staff present, we can create an alert to other staff so they can respond and give aid instantly.

WaveVCA : Intelligence built-in Cameras Analytics

Basic features

Analytics Engine WVCA Technology's advanced tracking algorithm with rich library of detection behaviors
Detection Zones and Rules 40 zones (Multi-segment Polygons and Lines) in total, 60 rules in total as standard
Intrusion Detection Detection of the presence of an object
Tamper Detection Supported as standard


Intrusion Detection


Tamper Detection


Zones & lines

Optional features

Detection Behavior Enter, Exit, Appear, Disappear, Stop, Direction, Dwell filter, Abandoned/Removed object filter, Tailgating
Logical Rules Extends standard rules to allow various combinations of the inputs
3D Behavior Perspective Corrected Size and Speed Filters
Object Classification - Configured Max./Min. object sizes and Max./Min. speeds
Counting Line High accuracy people and vehicle counting, 20 counters in total
Meta Data JSON format, Plain XML format


Enter Filter


3D Calibration


Tailgating Filter


Appear Filter


Counting


Exit Filter


Dwell Filter


Disappear Filter


Removed Object Filter


Stopped Filter


Direction Filter


Logical Rules


Abandoned Object Filter


Counting Lines

Some advantages of using Wavesys smart video perimeter intrusion detection systems

Suggested Features

- Polygon Based detection
- Parking Management- Illegal Parking, Wrong Parking
- Boundary wall crossing, unauthorized entry
- Wrong Way Movement
- Intrusion Detection
- Loitering
- Camera tampering, Video Loss

When it comes to security, artificial intelligence offers great advantages in terms of precision, effectiveness, costs and image processing times, thanks to the nature of self-learning. Here are some examples:

More security: Intelligent security analytics has become the best option to identify potential security threats and intrusions in unauthorized and monitored areas. It is a reliable technology that alerts security teams of possible risks and threats in real-time.

Improved situational awareness: by constantly monitoring activity around a perimeter, security personnel can gain a better understanding of what is happening in their environment and make better decisions about how to respond to potential threats.

Quicker response times: By automatically detecting and alerting security personnel to potential threats, intelligent video analytics can help to reduce response times to incidents.

Cost savings: automated video surveillance systems help reduce the need for security guards. This reduces costs for companies and organisations. What's more, the technology used by smart video analytics perimeter security systems gives superior coverage to other protective systems that require extensive cabling, fences, sensors, etc.

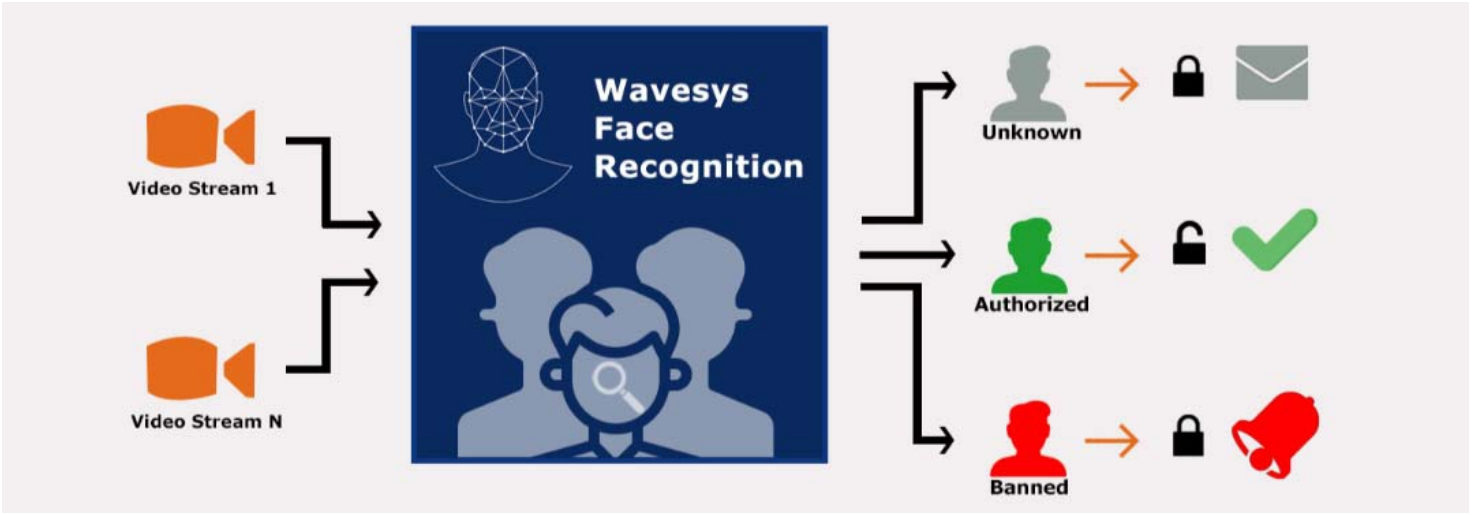
Improved security: Intelligent video analytics can help to improve the overall security of a perimeter by providing a more comprehensive and effective security system.

Additional Analytics that Can be Implemented at Server Level

SUPPORTED ANALYTICS	
Deep Learning Object and People Tracking	Deep learning trackers for highly accurate detection and classification of people, hands, vehicles types and objects. Optimised for business intelligence and metadata generation.
Event Rules	Intrusion detection, Tamper, Enter & Exit filters, Appear & Disappear filters, Stopped filter, Dwell filter, Direction & Speed filters, Counting, Abandoned & Removed object filter, Zones & lines, 3D calibration, Tailgating filter, Aggressive Behaviour, Fall Detection, Logical rules.
Object Detection, Tracking and Classification	Robust object tracking engine tracks through occlusion. Deep learning classification for reduced false positive rate. Multiple modes permit optimization for intrusion detection.
Object Counting	Accurate people and vehicle type counting, even in dense scenes.
Event Actions	E-mail, TCP, HTTP, Arm/Disarm.
Tamper	Camera Tamper Alert, Loss of Video Input Connection Alert.

Facial Recognition

The Wavesys Face Recognition system for WVMS Professional and Enterprise servers offers biometric identification and authentication.



Key Features

- Quick and simple installation with a ready-to-go database
- DNN Technology based database matching
- Solution support Multiple cameras simultaneously
- Customised actions for triggered Faces

Follow us

Wavesys Global | 16192 Coastal Highway | Lewes, DL-19958, County Of Sussex, |United States of America

www.wavesysglobal.com | sales.americas@wavesysglobal.com