Sentinel

Focoos AI

The Next Generation of Video Surveillance

Sentinel is Focoos AI's technology designed to analyze video in real time and support monitoring systems, live streaming, video surveillance, and advanced operational workflows.
Unlike systems that merely generate alerts or detect presence and movement, Sentinel interprets video content to help operators, platforms, and applications better understand **what is happening, what truly matters, and which events deserve attention.**

Three Core Features

Live Sense

Real-time video stream understanding.
Live Sense monitors the live stream and returns a higher level of event interpretation, useful for monitoring, security, supervision, and decision-support applications.

Smart Filter

Intelligent alarm and event filtering. Smart Filter helps reduce operational noise by distinguishing higher-priority alarms from less critical ones, supporting operators and systems in managing large volumes of alerts.

Deep Trace

Natural language event database query. Deep Trace allows exploration of events, metadata, and structured content generated by Sentinel through an LLM layer, simplifying search, analysis, and information reconstruction.

Key benefits

Semantic Understanding Brings semantic understanding to existing video infrastructures.	**Streams & Clips** Supports live streams, alarm clips, recorded video, and application pipelines.	**Reduced Operational Load** Reduces the operational burden and eliminates unnecessary manual checks.	**Event Prioritization** Helps identify and prioritize the most relevant events.
Fast Integration Integrates quickly with workflows, VMS, and third-party systems.	**No Dedicated Training** Does not require customer-specific training datasets	**Flexible Deployment** Adapts to edge, workstation, and server-side deployments.	**Production-Ready** Designed for real-world production scenarios.

Input Modes

Sentinel can be fed from live streams, alarm clips, recorded video, or triggers generated by third-party systems. Video ingestion can occur either via a frontend interface or directly through a backend API.

RTSP Stream

Supported video formats: H.264, H.265

Alarm Clips

Video files in AVI, MP4, MPG format

Recorded Video

Batch or post-event analysis

Video Segments from Third-Party Systems

From VMS, NVR, or custom pipelines

Available Outputs

Sentinel returns structured outputs designed to be consumed directly by application platforms, operational workflows, monitoring systems, or investigation modules.

Event Classification

Supported video formats: H.264, H.265

Priority / Relevance Score

Ranking of alarms and events by operational significantly

Structured Metadata

Associated with streams, clips, or specific events

REST API and JSON Output

Programmatic access for integration into any platform or workflow

Event Database Access

Via LLM layer for natural language querying and investigation

Licensing Model

Annual All-Inclusive License

Software usage rights

Maintenance, updates, and support included

Minimum 2-year commitment

Ideal for rapid activations. Lower recurring cost.

Perpetual License + Maintenance

One-time cost for software usage rights

Optional annual maintenance fee on a 3-year basis

Standard support

Maximizes return on initial investment.

Hardware performance

Certified hardware	10s video length		30s video length		Parallel Live Streams
	Response time (s)	# alarms handled	Response time (s)	# Alarms handled	
Orin NX 16GB	—	—	—	—	1/2
RTX 4070 Super workstation	2s	6	3s	2	6
RTX 5070 workstation	2s	12	3s	4	12
2× RTX 5070 workstation	2s	24	3s	8	24
RTX PRO 5000 workstation	1s	48	2s	16	48
2× RTX PRO 5000 workstation	1s	96	1s	32	96

** Alarms handled = maximum number of clips processable within the stated time under standard operating conditions. The number of parallel live streams depends on video resolution, FPS, bitrate, model configuration, and deployment architecture.*

*** The Orin NX 16GB configuration is typically suited for embedded deployments, real-time applications, and single live stream scenarios.*

Use cases enabled by Sentinel

By understanding behaviour and context, and not just detecting motion or predefined rules, Sentinel unlocks entirely new classes of applications.

Workplace Safety

Detects unsafe behaviours in real time, such as missing PPE, hazardous proximity to machinery, and anomalous actions.

Vandalism Detection

Identifies intentional damage actions such as striking, breaking, and tampering with objects.

Aggression & Violence

Recognizes suspicious interactions or escalation between individuals, including physical altercations, abnormal postures, and rapid movements.

Intrusion Detection

Goes beyond simple perimeter crossing by understanding intent and behaviour, such as loitering and suspicious movement patterns.

Break-ins & Forced Access

Detects attempts to access restricted areas through anomalous actions such as forcing doors and tampering with locks.

Museums & Sensitive Environments

Monitors interactions with artworks or protected assets, preserving integrity without invasive systems.

Retail Theft & Suspicious Behaviour

Identifies pre-theft patterns such as item concealment and anomalous browsing behaviour, not just the theft itself.

Multi-Step Event Understanding & Operational Compliance

Tracks sequences of actions over time and verifies that procedures are followed correctly - useful in industrial or regulated environments.

Banks & Financial Institutions

Protects counters, vaults, and critical areas from attacks, fraud, and unauthorised access by recognizing early warning signals.

Behavioural Monitoring

Analyses complex activity patterns over time, enabling deep understanding of workflows, anomalies, and intent in any monitored environment.

> Sentinel behaves like a **smart virtual operator**, active 24/7 - it doesn't just detect signals, it understands situations.