G-Cloud 15

Service Definition

CCTV Enhancement & Stability System with CCTV Controller Units (CCU)

M2M Tech Ltd

Lot 2b Software as a Service (SaaS)

Table of Contents

1. Introduction

1.1. Company Overview

M2M Tech is an innovative technology company specializing in intelligent transport infrastructure solutions, focused on transforming legacy systems into modern, cloud-based platforms. We deliver comprehensive Real-Time Passenger Information (RTPI) systems and advanced CCTV security platforms that combine edge computing, AI analytics, and collaborative access management to provide reliable, cost-effective solutions for transport authorities and public sector organizations across the UK.

We focus on breaking down the barriers created by proprietary systems and vendor lock-in, providing transport authorities with flexible, scalable, and future-proof solutions that span passenger information services and intelligent security infrastructure. As a Made In Britain certified member, we are committed to supporting local supply chains and delivering high-quality technology solutions that serve the public sector's evolving needs in both passenger communication and security management.

1.2. Value Proposition

Legacy CCTV systems in the public sector suffer from chronic reliability issues, with many installations experiencing 80%+ camera failure rates in part due to substandard shared installations expensive on-premises infrastructure requirements, and complex access procedures that delay emergency response. Our platform addresses these critical challenges by transforming unreliable legacy camera systems into intelligent, cloud-managed security infrastructure that delivers 99.2%+ uptime, eliminates server costs, and enables seamless multi-agency collaboration.

Our CCTV Controller Units (CCU) revolutionise existing camera installations by adding comprehensive AI capabilities that were previously impossible with legacy systems. Through edge computing integration, older cameras gain access to advanced features including:

- Traffic congestion detection
- Flood and fire monitoring
- Vehicle counting
- Red-light running detection
- Automated incident alerts
- Intelligent privacy masking
- Audio incident detection (collision/collapse/vehicle horns)
- Emergency vehicle siren detection with traffic light priority integration
- Panic audio detection
- Gunfire audio detection with firearm classification

This transforms basic surveillance equipment into sophisticated monitoring infrastructure without requiring complete system replacement.

1.3. What the Service Offers

Our service encompasses a complete ecosystem of integrated solutions for intelligent CCTV infrastructure, designed with flexible deployment in mind. We offer both a comprehensive, full-featured platform for organizations seeking an end-to-end security solution, and individual services that can be selectively integrated into existing third-party systems via robust APIs. This modular approach ensures you can adopt our technology in the way that best serves your operational requirements and existing infrastructure.

Our platform supports both fixed line and wireless CCTV deployments, seamlessly integrating with existing network infrastructure where available, while offering 4G/5G wireless connectivity options for locations without fixed line network access. This flexibility ensures comprehensive coverage across your entire estate regardless of existing infrastructure limitations.

Central to our platform is an advanced automated recovery and remote management system that dramatically improves the reliability and stability of CCTV deployments. Through intelligent health monitoring, predictive fault detection, and automated restorative actions—including remote power cycling and sequential recovery procedures our system maintains exceptional uptime without requiring costly site visits. This self-healing capability, combined with comprehensive remote diagnostics, transforms traditionally unreliable camera estates into robust, dependable security infrastructure.

Unlike traditional CCTV systems that remain passive until an operator views them, our AI analytics continuously monitor every camera feed 24/7/365, even when no human operator is watching. This means your cameras are always working for you, automatically detecting incidents, monitoring infrastructure condition, and tracking traffic patterns around the clock. Human operators are immediately alerted when events require attention, transforming reactive surveillance into proactive security intelligence.

Whether you adopt our complete platform or selectively integrate individual services into your existing infrastructure, our modular architecture ensures you benefit from these capabilities in the way that best serves your operational requirements—delivering maximum value while future-proofing your CCTV systems.

1.3.1 Core Platform Services

Video Ingestion Services	Seamlessly integrate diverse camera feeds into a unified platform, supporting legacy analogue systems, IP cameras, thermal imaging, infrared, and specialized camera types through edge computing transformation
AI Analytics Processing Services	Apply intelligent multi-stage visual and audio analysis including incident detection, environmental monitoring, traffic analytics, and automated threat identification
Video Distribution Services	Deliver on-demand streaming with intelligent bandwidth management, eliminating expensive continuous streaming infrastructure while ensuring rapid access when needed
Edge Device Interface Services	Manage two-way communication with CCTV Controller Units (CCU) Service, enabling secure video retrieval, configuration updates, and real-time health monitoring and recovery
Orchestration & Monitoring Services	Automated rule-based health monitoring, failover management, and restorative actions ensuring 24/7/365 reliability across your camera estate

1.3.2. Sentinel Management Interface

Asset Management System	Complete lifecycle management, real-time monitoring, KPI tracking, remote control, and maintenance management for your entire camera estate
AI Analytics Configuration	Comprehensive control over visual and audio detection algorithms, alert thresholds, and automated response triggers
Multi-Agency Access Management	Collaborative access controls enabling secure cross-organizational sharing between councils, police, emergency services, and contractors
Dashboard, KPIs & Reporting	Real-time operational insights with comprehensive reporting and full audit trails
Privacy & Evidence Management	AI-powered privacy masking, secure video sharing with time-limited access codes, and compliant evidence export
Live View & Operator Controls	PTZ camera control, two-way audio communication with people on-site, snapshot capture, and multi-view layouts
Support Ticket System	Centralized ticket-based support with SLA management, automated notifications, and third-party coordination

1.3.3. CCTV Controller Unit (CCU) Service – Edge Device Interface

Edge Computing Transformation	Modernise legacy cameras with intelligent edge processing, adding AI capabilities without system replacement. Optional 4G/5G connectivity for locations without fixed line network access
Advanced Visual AI Analytics	Real-time detection including traffic congestion, flood/fire monitoring, vehicle counting, red-light running, and infrastructure health assessment
Audio Intelligence Processing	Collision/collapse detection, emergency vehicle siren recognition, panic audio alerts, gunfire detection, and two-way audio communication with people on-site
3D Spatial Awareness	Real-time visual aids including compass headings, asset identification, geolocation extraction, and contextual mini maps
Local Recording & Storage	Local DVR functionality with configurable retention periods and on-demand retrieval
Intelligent Power Management	Remote monitoring, automated fault detection, power cycling capabilities, and backup battery systems

1.3.4. Supporting Utilities & Services

Privacy Masking Engine	AI-powered automatic detection and blurring of faces and vehicle number plates, plus manual privacy zone definition for secure evidence sharing

Video Wall Integration	Professional video wall support for control rooms, plus personal web-based video wall layouts for individual users within Sentinel
UTMC Integration Service	Seamless integration with Urban Traffic Management and Control systems, including emergency vehicle priority integration with traffic light controllers
External Sharing Portal	Secure, time-limited video sharing with external parties via controlled share codes and managed access permissions

2. Core Platform Services

Comprehensive video governance pipeline delivering end-to-end reliability from camera to operator through intelligent edge computing, multi-stage AI analysis, on-demand distribution, secure two-way communication via our CCU Service, and automated health monitoring with self-healing capabilities.

Our entire system is designed around a modular, micro-service architecture, allowing for the easy implementation, update, removal and triage of individual services without affecting the stability and security of the entire system. This enables us to be highly flexible and quick to respond to changes in security requirements and emerging threats.

Video Ingestion Services	Seamlessly integrate diverse camera feeds into a unified platform, supporting legacy analogue systems, IP cameras, thermal imaging, infrared, and specialized camera types through edge computing transformation
AI Analytics Processing Services	Apply intelligent multi-stage visual and audio analysis including incident detection, environmental monitoring, traffic analytics, and automated threat identification
Video Distribution Services	Deliver on-demand streaming with intelligent bandwidth management, eliminating expensive continuous streaming infrastructure while ensuring rapid access when needed
Edge Device Interface Services	Manage two-way communication with CCTV Controller Units (CCU) Service, enabling secure video retrieval, configuration updates, and real-time health monitoring and recovery
Orchestration & Monitoring Services	Automated rule-based health monitoring, failover management, and restorative actions ensuring 24/7/365 reliability across your camera estate

2.1. Video Governance

Video Governance within Sentinel ensures video quality, accessibility, and reliability from camera to operator through a unified pipeline: Video Ingestion Services integrate and transform diverse camera feeds; Video Distribution Services intelligently deliver on-demand content; and Edge Device Interface Services manage two-way communication with CCU Service instances.

2.1.1. Video Ingestion Services

The Video Ingestion Service is the transformation layer for all camera feeds into the Sentinel platform, converting diverse video sources from legacy and modern systems into a unified, cloud-accessible format.

Our edge computing architecture enables rapid modernization of existing camera infrastructure without complete system replacement. The CCTV Controller Unit (CCU) Service transforms legacy analogue cameras into intelligent, cloud-managed assets capable of AI analytics, with optional 4G/5G connectivity capabilities. For sites with existing fixed line network infrastructure, the CCU Service can connect via Ethernet, fibre, or other fixed line methods, while wireless connectivity options enable deployment in locations without network access.

Camera Compatibility: Our modular design supports diverse camera types and manufacturers including legacy analogue systems, IP cameras with direct cloud integration, PTZ (Pan-Tilt-Zoom) cameras with full remote control, and fixed-position surveillance systems. Specialized imaging technologies are fully supported including night-vision cameras, infrared (IR) illuminated cameras for low-light environments, and thermal imaging cameras for heat-based detection in complete darkness or adverse weather conditions. Both composite and HD-SDI analogue outputs are supported through appropriate video capture interfaces. IP cameras can connect directly to the platform via existing fixed line networks or through the CCU Service's network bridging capabilities.

Two-Way Audio Communication: Cameras equipped with integrated speakers and microphones, or connected to external audio equipment via the CCU, enable operators to communicate directly with people on-site. This capability supports public address announcements, verbal warnings to deter antisocial behaviour, and interactive communication where operators can speak to individuals and hear their responses in real-time. Two-way audio transforms passive surveillance into active intervention capability.

Multi-Camera Site Deployments: The platform fully supports multi-camera installations at single sites, enabling sophisticated coordinated monitoring scenarios. A typical deployment might combine a 360-degree dome camera for continuous situational awareness with a PTZ camera for detailed investigation. AI analytics monitoring the dome camera can automatically detect events of interest and direct the PTZ camera to zoom in on the incident location, capturing high-resolution detail without operator intervention. This intelligent camera coordination maximizes coverage while ensuring critical events are captured in detail.

Encoding and Compression: All video feeds are processed through optimized encoding pipelines supporting H.264 and H.265 compression standards, balancing video quality with bandwidth efficiency. Configurable resolution and frame rate settings enable optimization for specific monitoring requirements and network conditions.

Through the Sentinel interface, you maintain full control over your active camera feeds with manual stream initiation, configuration management, and health monitoring across your entire camera estate or specific groups/individual cameras—essential for managing equipment failures or testing new installations.

2.1.2. Video Distribution Services

Video Distribution Services provide intelligent on-demand streaming with comprehensive bandwidth management and full audit trails. Unlike traditional CCTV systems requiring expensive continuous recording servers, our on-demand model eliminates infrastructure costs while ensuring rapid access when operators need video.

On-Demand Streaming Model: Video streams are initiated only when requested by authorized operators, significantly reducing bandwidth consumption and eliminating the need for expensive always-on server infrastructure. Timed streaming sessions with automatic timeout ensure efficient resource utilization. AI-powered upscaling is available during live viewing to enhance image clarity, particularly valuable for legacy or distant cameras.

Intelligent Bandwidth Management: Adaptive streaming quality based on network conditions ensures reliable video delivery across varying mobile network performance. Automatic quality adjustment maintains viewable streams even in challenging connectivity scenarios. Operators can apply real-time AI enhancement to improve detail visibility during active monitoring sessions.

Priority Access: Critical security events trigger automatic stream prioritization, ensuring operators can access affected cameras immediately regardless of system load. Emergency access protocols bypass standard streaming queues for time-critical situations.

Audit Trail: Comprehensive logging captures who accessed which camera, when, for how long, and what actions were taken during viewing sessions. Full transparency and auditability for compliance and accountability requirements.

2.2. AI Analytics Processing Services

AI Analytics Processing Services apply multi-stage visual and audio analysis to all camera feeds, enabling automated detection, classification, and alerting for security incidents and operational intelligence. Critically, AI analytics operate continuously 24/7/365 regardless of whether a human operator is actively viewing the feed, your cameras are constantly working for you, detecting events and monitoring conditions even when no one is watching.

Visual Analytics Engine: The system processes video feeds through a comprehensive AI pipeline detecting and classifying:

Traffic and Vehicle Analytics: Real-time traffic congestion detection, vehicle counting and classification, red-light running detection, and roadside asset monitoring. Queue length analysis for transport hubs, coach bay occupancy monitoring, and congestion trend analysis. Lane obstruction detection identifies vehicles stopped in active lanes, while wrong way driving detection provides immediate alerts for vehicles traveling against traffic flow.

Environmental Safety Detection: Automated flood detection through water level analysis, fire and smoke detection with thermal signature analysis (enhanced when thermal imaging cameras are deployed), and adverse weather condition identification affecting road safety. Fallen tree and debris detection identifies road obstructions requiring immediate clearance, enabling rapid response to maintain traffic flow and public safety.

Infrastructure Health Monitoring: Detection of shelter and lighting failures, road surface condition analysis, and street furniture damage identification through visual anomaly detection.

Traffic Sign Recognition: Automated monitoring of traffic signage condition including illegible sign detection identifying signs that are obscured, damaged, faded, or otherwise unreadable. Supports proactive maintenance scheduling to ensure regulatory compliance and road safety.

Crowd and Occupancy Analytics: Platform crowd density monitoring for rail stations, passenger counting at bus stops and transport hubs, queue length monitoring for ferry terminals, and general occupancy analysis for public spaces. Loitering detection identifies individuals remaining in designated areas beyond configurable time thresholds, supporting both security and welfare applications.

Security and Perimeter Analytics: Perimeter intrusion detection monitors defined boundary zones for unauthorized entry, with configurable sensitivity and zone definitions. Object removal detection alerts when items are taken from monitored areas, complementing abandoned object detection for comprehensive asset protection.

Audio Analytics Engine: Advanced audio processing capabilities provide detection beyond visual analysis:

Incident Audio Detection: Collision and impact sounds with severity classification, structural collapse audio signatures, and vehicle horn patterns indicating traffic incidents or driver distress.

Emergency Services Detection: Emergency vehicle siren recognition with classification (ambulance, fire, police) enabling automated traffic management integration. Integration with UTMC systems for traffic light priority coordination.

Security Threat Detection: Panic and distress audio recognition using voice stress analysis, crowd disturbance patterns, and verbal aggression detection for public safety applications.

Gunfire Detection: Advanced audio classification identifying gunfire events with firearm type classification, distinguishing between handguns, rifles, and shotguns. Immediate alert generation with location triangulation where multiple cameras are available.

Alert Processing: All detected events are immediately classified by severity, logged with full metadata (timestamp, location, confidence score, classification), and distributed through configured notification channels including email, SMS, and platform alerts. False positive reduction algorithms continuously learn from operator feedback to improve detection accuracy.

2.3. Edge Device Interface Services

Edge Device Interface Services manage two-way communication with the CCTV Controller Unit (CCU) Service, enabling secure video streaming, configuration updates, health monitoring, and remote management.

Communication Architecture: The CCU Service establishes secure outbound connections to the Sentinel cloud platform via fixed line or 4G/5G cellular networks, providing flexibility to match deployment requirements. Fixed line connectivity leverages existing network infrastructure where available, while cellular connectivity eliminates complex network configuration requirements and enables deployment in locations without existing fixed line infrastructure. All communications are encrypted end-to-end using TLS 1.3 protocols regardless of connection type.

Configuration Management: Remote configuration of all CCU Service parameters including video encoding settings, AI analytics thresholds, recording schedules, and alert configurations. Hierarchical configuration inheritance enables estate-wide settings with per-location overrides where required.

Health Telemetry: Continuous transmission of service health metrics including processing utilization, memory usage, storage capacity, temperature readings, network signal strength, power status, and software status. Predictive analytics identify service instances at risk of degradation before impact occurs.

Remote Control: Full remote management capabilities including service/device restart, power cycling, configuration deployment, software updates, and diagnostic command execution. Virtual engineer access provides expert-level troubleshooting without site visits.

2.4. Orchestration & Monitoring Services

Orchestration and Monitoring Services provide continuous, end-to-end oversight throughout the video processing lifecycle and monitor real-time health of all camera assets, maintaining system performance and ensuring 24/7/365 reliability.

Rule-Based Automated Healing: All monitoring and restorative services operate as a highly customizable Rule-Based Machine-to-Machine Hierarchical Finite State Machine (Rule-Based M2M HFSM), ensuring reliable and deterministic detection and healing behaviours. Automated actions include:

Camera Failure Recovery: Detects non-responsive CCTV cameras and initiates sequential recovery steps including remote service/device restart and escalates to power-cycling of CCTV camera via intelligent power management. Escalation to maintenance tickets when automated recovery is exhausted.

Network Failover: Detects degraded cellular connectivity and automatically switches between available network operators where multi-SIM capabilities are deployed. Configurable signal strength thresholds trigger proactive failover before complete connectivity loss.

Storage Management: Priority retention for flagged incidents ensures critical footage is preserved while routine recordings are automatically purged after the desired retention period.

End-to-End Performance Tracking: Measures and logs comprehensive performance metrics including stream initiation latency, video quality scores, AI detection processing times, and alert delivery latency. All automated actions and events are logged into event logs for individual cameras and/or the camera estate, ensuring full transparency with real-time and historic data access.

3. Sentinel Management Interface

Sentinel is our web-based, mobile-friendly CCTV management interface for configuration, monitoring, multi-agency collaboration, and remote control of your camera estate.

Asset Management System	Complete lifecycle management, real-time monitoring, KPI tracking, remote control, and maintenance management for your entire camera estate
AI Analytics Configuration	Comprehensive control over visual and audio detection algorithms, alert thresholds, and automated response triggers
Multi-Agency Access Management	Collaborative access controls enabling secure cross-organizational sharing between councils, police, emergency services, and contractors

Dashboard, KPIs & Reporting	Real-time operational insights with comprehensive reporting and full audit trails
Privacy & Evidence Management	AI-powered privacy masking, secure video sharing with time-limited access codes, and compliant evidence export
Live View & Operator Controls	PTZ camera control, two-way audio communication with people on-site, snapshot capture, and multi-view layouts
Support Ticket System	Centralized ticket-based support with SLA management, automated notifications, and third-party coordination

3.1. Asset Management System

The Asset Management System (AMS) provides centralized operational visibility, maintenance management, and remote control across your entire camera estate, delivering real-time and historic insights into asset health, performance, and status.

Real-Time Alerts and Monitoring: Captures comprehensive alerts and events with Email and Text Message notifications, including Automated/Manual Reboots, System/device issues, AI Detection Events, Power events, Network connectivity changes, and Storage capacity warnings.

KPIs and Analytics: Tracks extensive performance metrics for proactive and predictive maintenance:

- CCU Service Metrics: Processing utilization, memory usage, storage capacity, temperature readings, uptime, and software status
- Network Performance: Signal strength, latency measurements, data consumption, and network operator performance comparison
- Camera Health: Video feed quality scores, encoding performance, stream availability, and PTZ functionality status
- AI Analytics Performance: Detection accuracy rates, false positive ratios, processing latency, and algorithm performance metrics

Documentation and Compliance: Complete file repository for compliance documents (site photos, installation certificates, commissioning sheets, maintenance reports), maintenance history tracking, inspection reminders, and modification records for configuration changes.

Remote Management: Hierarchical cascading configuration system (estate-wide to individual camera level), remote commands (Storage Purge, Power-cycling, OS reboot, Configuration deployment), and comprehensive proof of operation via live-stream or recorded footage recall. Includes component-level warranty tracking and maintenance scheduling.

3.2. AI Analytics Configuration

Sentinel provides comprehensive control over all AI detection algorithms, enabling precise tuning of detection sensitivity, alert thresholds, and automated response triggers.

Visual Analytics Configuration: Configure detection sensitivity for each visual analytics module including traffic analysis, environmental monitoring, and infrastructure health. Adjustable confidence thresholds enable balance between detection coverage and false positive rates. Geographic zone definition allows focused analysis on specific areas of camera views.

Audio Analytics Configuration: Fine-tune audio detection algorithms for site-specific acoustic environments. Ambient noise profiling enables accurate detection despite background noise variations. Sensitivity adjustments for each audio detection type (collision, siren, panic, gunfire) optimize performance for deployment environment.

Alert Routing: Configure alert distribution based on detection type, severity, time of day, and recipient preferences. Escalation hierarchies ensure appropriate response based on incident classification. Integration with external systems enables automated workflow triggers.

Learning and Optimization: Operator feedback on detection accuracy continuously improves algorithm performance. False positive flagging trains the system to reduce unnecessary alerts while maintaining detection sensitivity. Site-specific learning adapts algorithms to unique environmental characteristics.

3.3. Multi-Agency Access Management

Sentinel enables secure collaboration between multiple organizations including councils, police forces, emergency services, transport operators, and maintenance contractors, with comprehensive access controls ensuring appropriate visibility and permissions.

Organizational Structure: Hierarchical organization management supports complex multi-agency deployments with distinct access boundaries. Parent-child organizational relationships enable oversight while maintaining operational separation.

Role-Based Access Control: Granular permission sets define precisely what each user role can access and perform:

- Viewing Permissions: Control which cameras, recordings, and live streams each user can access based on organizational assignment, geographic region, or camera grouping
- Control Permissions: Define who can operate PTZ controls, initiate two-way audio communication, initiate recordings, or trigger manual alerts
- Configuration Permissions: Restrict system configuration changes to appropriate administrative roles
- Evidence Permissions: Control who can download, share, or export video evidence

External Sharing: Secure video sharing with parties outside the platform through time-limited share codes. Configurable expiration periods and viewing limits ensure controlled access. Instant revocation capability for emergency access termination. Full audit trail of all external access.

Delegation and Approval: Configurable approval workflows for sensitive actions including evidence export, external sharing, and configuration changes. Multi-party approval requirements for high-sensitivity operations.

3.4. Dashboard, KPIs, Reporting & Audit Trails

The dashboard provides you with a real-time insight into the operational status of the system. The dashboard utilises traffic light colouring systems, graphs and charts to provide performance metrics and alerts for key sub-systems. This enables continuous monitoring and alerting for real-time operational effectiveness.

Dashboard elements consist of, but are not limited to:

- Camera Status Overview: Traffic light counts of online, degraded, and offline cameras across your estate.
- Live Streaming Consumption: Colourised percentage graph showing streaming quota consumption for the billing period.
- Video Retrieval Consumption: Colourised percentage graph showing recorded footage retrieval quota consumption for the billing period.
- AI Analytics Status: Real-time status of each AI detection module with alert counts and performance metrics.
- Alert Summary: Categorized count of active alerts by type (security, environmental, infrastructure, traffic) with severity indication.
- CCU Service/Device Health: Aggregate health status across all CCU Service instances with drill-down to individual location details.
- Network Performance: Mobile network operator comparison showing latency, reliability, and data consumption by carrier.
- Incident Timeline: Chronological view of detected incidents with filtering by type, severity, and location.
- Open Support Tickets: List of open support tickets, categorized by Priority level.

Each dashboard element can take you to a more detailed breakdown of the data, allowing for filtering, report downloads and historical views of the various KPIs, metrics and statuses.

All reports are generated and accessible from Sentinel allowing for unrestricted 24/7/365 access to all data, metrics and KPI outcomes. For contractual obligations to 'deliver' reports, like monthly KPI reports, these will be generated by the system when contractually obligated to, stored in the system, and accessible for download at your convenience. We do not typically generate reports manually or issue reports from outside of the system for reasons of consistency and transparency.

All user movements, modifications and login activity is stored in audit logs, allowing you to review and determine what configurations, settings and data has been changed throughout the system by users, and by automated systems where appropriate. Like other reports, these are accessible 24/7/365 through the Sentinel interface, and as downloadable reports. Video access logs provide complete visibility into who viewed which camera and when, essential for GDPR compliance and security auditing.

3.5. Privacy & Evidence Management

Sentinel provides comprehensive privacy protection and evidence management capabilities, ensuring GDPR compliance while enabling effective security operations and lawful evidence sharing.

AI-Powered Privacy Masking: Automatic detection and real-time blurring of faces and vehicle number plates in both live streams and recorded footage. Multiple masking intensity levels from light blur to complete redaction. Selective unmasking for authorized evidence reviewers with full audit logging.

Manual Privacy Zones: Define static privacy zones to permanently obscure sensitive areas such as residential windows, private property, or locations where surveillance is inappropriate. Privacy zones persist across all viewing sessions and exports.

Evidence Export: Secure export of video clips with configurable privacy masking levels. Chain of custody documentation automatically generated with exports. Digital watermarking ensures evidence authenticity and identifies source. Multiple export formats supporting common evidential standards.

AI-Enhanced Image and Video Upscaling: Advanced AI upscaling tools enhance the quality of snapshots and video footage directly within the Sentinel interface. Original footage is always preserved unchanged, with AI-enhanced versions created as separate derivative copies, maintaining full evidential integrity and chain of custody for both original and enhanced materials.

Secure Sharing: Time-limited share codes enable controlled external access to specific video clips without platform access. Configurable expiration periods (hours to days), maximum view counts, and immediate revocation capability. This eliminates reliance on insecure email attachments or third-party file sharing services, providing a secure, auditable channel for evidence sharing. Full audit trail of all external viewing activity.

Retention Management: Configurable retention policies based on footage type, incident classification, and legal requirements. Automatic purging of routine footage while preserving flagged incidents indefinitely. Legal hold capabilities prevent deletion of footage relevant to ongoing investigations.

3.6. Live View & Operator Controls

Sentinel provides comprehensive real-time camera control capabilities, enabling operators to actively manage surveillance rather than passively observe.

PTZ Camera Control: Full pan, tilt, and zoom control for equipped cameras directly through the Sentinel interface. Preset positions enable rapid navigation to frequently monitored locations. Tour patterns automate systematic coverage of key areas. Smooth control response ensures precise positioning for incident investigation.

Two-Way Audio Communication: For cameras equipped with speakers and microphones, operators can communicate directly with individuals on-site through the Sentinel interface. One-click activation enables immediate public address announcements or verbal warnings to deter antisocial behaviour. Full duplex audio allows operators to hear responses, enabling interactive conversations with members of the public who may require assistance or direction. Audio communication sessions are logged for audit purposes, with optional recording of operator communications.

Snapshot Capture: Instant image capture from live video streams for immediate use in incident reports or sharing. Captured images include timestamp and camera identification metadata.

Multi-View Layouts: Configurable screen layouts displaying multiple camera feeds simultaneously. Saved layout configurations for common monitoring scenarios. Quick switching between layout presets for different operational contexts.

3.7. Mapping and Geospatial Visualization

Sentinel provides comprehensive mapping and geospatial visualization capabilities, transforming camera estate management through intelligent location-based insights and visual network oversight.

Interactive Network Visualization: Advanced mapping interface enables users to visualise the locations of cameras across your entire estate on a comprehensive, interactive map. This

functionality facilitates easy identification and management of camera locations across transport hubs, public spaces, roadways, and key infrastructure points.

Operational Intelligence: The mapping system displays real-time operational status for each camera location using an intuitive traffic light format (green for operational, amber for warning, red for fault), providing immediate visual assessment of estate-wide performance and enabling rapid response to operational issues. Active alerts are highlighted with appropriate severity indicators.

Coverage Analysis: Visual representation of camera coverage areas enables identification of surveillance gaps, overlapping coverage zones, and optimization opportunities. Heat mapping of incident detections reveals patterns informing strategic deployment decisions.

Incident Mapping: Real-time display of AI-detected incidents with geographic clustering and trend analysis. Historical incident mapping reveals patterns across time and space, supporting evidence-based security planning.

Maintenance Planning: Supports efficient maintenance route planning, enables optimization of camera coverage across geographic areas, and facilitates strategic planning for network expansion. Maintenance teams can visualize workload distribution and plan efficient service routes.

3.8. Support Ticket System

Sentinel features a fully integrated, ticket-based support system for centralized operational, maintenance, and query management.

Workflow Control: Full flow control from ticket creation to closure with delegated access for authorized third-party contractors. Configurable Support Ticket Categories (e.g., Camera Offline, Vandalism Damage, AI Detection Issues, Network Connectivity) ensure accurate classification.

Service Level Management: Customizable Priority levels (P0 Critical/Emergency through P6 Informative Only) linked to SLA response timings, configured to your specifications.

Automated Notifications and Evidence Management: Email and Text Message alerts for ticket events (creation, updates, closure) with subscription management by category and priority. Document/image/video upload capability for evidence and diagnostic reports. Automatic ticket raising when automated restorative actions are exhausted, with optional auto-closure upon issue resolution.

Contractor Coordination: Secure ticket sharing with maintenance contractors including relevant camera details, fault information, and site access requirements. Progress tracking through contractor workflow integration.

4. CCTV Controller Unit (CCU) Service - Edge Device Interface

The CCTV Controller Unit (CCU) Service represents the sophisticated edge computing capability of our CCTV ecosystem, providing intelligent transformation of legacy camera systems into modern, cloud-managed, AI-enabled security infrastructure. More than simple video encoding, the CCU Service delivers a comprehensive edge intelligence platform designed to provide advanced analytics,

reliable connectivity, and robust operational capabilities without requiring complete camera system replacement.

Built with reliability and expandability at its core, the CCU Service seamlessly integrates advanced AI processing, intelligent video management, and comprehensive remote management capabilities to transform basic surveillance equipment into sophisticated monitoring infrastructure, while greatly improving stability and reliability.

Edge Computing Transformation	Modernise legacy cameras with intelligent edge processing, adding AI capabilities without system replacement. Optional 4G/5G connectivity for locations without fixed line network access
Advanced Visual AI Analytics	Real-time detection including traffic congestion, flood/fire monitoring, vehicle counting, red-light running, and infrastructure health assessment
Audio Intelligence Processing	Collision/collapse detection, emergency vehicle siren recognition, panic audio alerts, gunfire detection, and two-way audio communication with people on-site
3D Spatial Awareness	Real-time visual aids including compass headings, asset identification, geolocation extraction, and contextual mini maps
Local Recording & Storage	Local DVR functionality with configurable retention periods and on-demand retrieval
Intelligent Power Management	Remote monitoring, automated fault detection, power cycling capabilities, and backup battery systems

4.1. Edge Computing Transformation

The CCU Service fundamentally transforms legacy CCTV systems through edge computing architecture, adding capabilities that were previously impossible without complete infrastructure replacement.

Service Architecture: The CCU Service delivers high-performance video processing capabilities with optional 4G/5G cellular connectivity supporting multi-operator failover, fixed line connectivity options (Ethernet, fibre, or other methods), intelligent power management with backup capabilities, and environmental monitoring. Audio input/output capabilities support two-way communication functionality. The service is designed for deployment across diverse outdoor environments.

Legacy Camera Integration: The CCU Service connects to existing analogue cameras via composite or HD-SDI video inputs, digitizing and encoding video for on-demand streaming and retrieval via the Sentinel platform. This enables organizations to retain functional camera infrastructure while adding modern connectivity and AI capabilities. Specialized camera types including thermal imaging, infrared, and night-vision cameras are fully supported, with AI analytics optimized for each imaging modality.

IP Camera Integration: Modern IP cameras connect to the CCU Service via standard network protocols, benefiting from the same comprehensive AI analytics, cloud management, and remote monitoring capabilities. Critically, the CCU Service adds advanced AI detection features to any connected camera regardless of whether the camera manufacturer natively supports such capabilities—transforming basic IP cameras into intelligent monitoring systems without requiring expensive manufacturer-specific analytics licenses or camera upgrades.

Flexible Connectivity: The CCU Service supports both fixed line and wireless 4G/5G connectivity, enabling deployment across diverse infrastructure scenarios. Sites with existing network infrastructure can leverage fixed line connections for maximum bandwidth and lowest latency, while remote or challenging locations benefit from cellular connectivity without requiring network infrastructure installation. Dual-connectivity configurations provide automatic failover between fixed line and wireless connections for maximum reliability.

Scalable Deployment: Each CCU Service enabled device operates independently, enabling gradual rollout across camera estates without complex interdependencies. Service instances do not impact each other, and replacement deployments can be pre-configured for rapid swap installation. Multi-camera sites can share a single CCU Service instance where appropriate, with AI coordination between cameras enabling automated PTZ tracking of events detected on overview cameras.

4.2. Advanced Visual AI Analytics

The CCU Service processes the full suite of visual analytics capabilities (detailed in Section 2.2) directly at the edge, including traffic and vehicle analytics, environmental safety detection, infrastructure health monitoring, crowd and occupancy analytics, and security and perimeter monitoring.

Edge-based AI runs continuously on every camera, performing automated monitoring 24/7 even when operators are not viewing—ensuring your cameras are always actively working for you. Local processing reduces bandwidth requirements and enables immediate alert generation without cloud round-trip latency.

4.3. Audio Intelligence Processing

The CCU Service processes the full suite of audio analytics capabilities (detailed in Section 2.2) at the edge, detecting incidents and threats that may not be visible on camera or occur outside the camera's field of view—including collision detection, emergency vehicle siren recognition, panic and distress audio, and gunfire detection.

Edge-based audio processing enables sub-second alert generation, critical for time-sensitive security threats where immediate response is essential.

Two-Way Audio Communication: The CCU Service supports full two-way audio when connected to speakers and microphones, enabling operators to communicate with people on-site through Sentinel. The service manages audio encoding, echo cancellation, and synchronization to ensure clear communication quality even in challenging acoustic environments.

4.4. 3D Spatial Awareness

The CCU Service provides sophisticated spatial intelligence features that enhance operator situational awareness and enable rapid incident response.

Compass Heading Display: Real-time compass heading overlay on video streams enables operators to quickly communicate direction information to responding units. Essential for coordinating responses where location descriptions require directional context.

Asset Identification: On-screen identification of known assets within camera view including street names, building identifications, and infrastructure elements. Rapid asset identification supports incident reporting and response coordination.

Geolocation Extraction: Camera position and viewing angle enable approximate geolocation extraction from video content. Clicking locations within the video frame generates geographic coordinates for dispatch to responding units.

Contextual Mini Maps: Picture-in-picture mini map display shows camera location, viewing direction, and surrounding context. Rapid orientation for operators unfamiliar with specific locations.

Neighbouring Camera Awareness: Quick access to adjacent cameras enables operators to track incidents across multiple views. Automatic suggestions for relevant neighbouring cameras based on detected incident location and likely movement patterns.

4.5. Local Recording & Storage

The CCU Service provides comprehensive local recording capabilities ensuring footage availability even during network disruptions.

Local DVR Functionality: Continuous local recording with configurable retention periods. Storage capacity options accommodate varying retention requirements from days to weeks of footage.

Intelligent Retention: AI-flagged incidents automatically receive extended retention priority. Routine footage is automatically purged based on configurable age threshold while preserving potentially significant recordings.

Network Resilience: Local storage ensures continuous recording during cellular network outages.

Secure Storage: Encrypted local storage protects recorded footage from unauthorized access. Tamper detection alerts notify operators of potential physical security breaches.

4.6. Intelligent Power Management

Comprehensive power management ensures reliable operation while enabling rapid fault recovery and maximizing equipment lifespan.

Power Monitoring: Real-time monitoring of mains power supply including voltage levels, current consumption, and power quality. Historical trending identifies power supply issues before they cause service/device disruption.

Intelligent Power Management Unit (IPMU): The IPMU is an independent monitoring component with its own battery backup and cellular SIM connectivity, enabling immediate notification of mains power loss events at the moment they occur—even when the main CCU and camera equipment lose power. This ensures operators are alerted to power failures instantly rather than discovering them when cameras become unresponsive, enabling rapid dispatch of maintenance personnel and reducing downtime.

Remote Power Control: Remote power cycling of camera equipment, CCU Service components, and networking equipment enables fault recovery without site visits. Intelligent sequenced restart procedures maximize recovery success rates. The IPMU capability enables targeted power cycling of individual components, allowing precise fault isolation and recovery.

Battery Backup: Optional integrated battery backup for the CCU maintains camera operation during brief power outages, enabling continuous recording and graceful shutdown during extended outages. This is separate from the IPMU's independent battery, which is dedicated solely to power loss notification and remote power control functions.

Automated Fault Recovery: Detection of camera or CCU Service faults triggers automatic recovery sequences including targeted power cycling. Escalating recovery procedures attempt multiple restoration approaches before automatically generating maintenance tickets.

Environmental Monitoring: Temperature and humidity sensors detect environmental conditions that may impact service reliability. Alerts enable proactive intervention before environmental conditions cause failures.

5. Supporting Utilities & Services

Purpose-built utilities extending platform functionality, are also available as standalone services with dedicated interfaces or embedded into third-party systems via robust APIs.

Privacy Masking Engine	AI-powered automatic detection and blurring of faces and vehicle number plates, plus manual privacy zone definition for secure evidence sharing
Video Wall Integration	Professional video wall support for control rooms, plus personal web-based video wall layouts for individual users within Sentinel
UTMC Integration Service	Seamless integration with Urban Traffic Management and Control systems, including emergency vehicle priority integration with traffic light controllers
External Sharing Portal	Secure, time-limited video sharing with external parties via controlled share codes and managed access permissions

5.1. Privacy Masking Engine

Comprehensive AI-powered privacy protection ensuring GDPR compliance while maintaining operational effectiveness for security monitoring and evidence management.

Automatic Detection: Machine learning algorithms automatically identify faces and vehicle number plates in both live streams and recorded footage. Real-time processing ensures privacy protection without operator intervention.

Adaptive Masking: Multiple masking intensity levels from light gaussian blur to complete pixel replacement. Configurable based on sharing context—lighter masking for internal operational use, complete redaction for public disclosure.

Selective Revelation: Authorized users with appropriate permissions can access unmasked footage for legitimate investigation purposes. All unmasked viewing is logged with detailed audit trails including user identity, timestamp, footage accessed and stated justification.

Manual Zone Definition: Static privacy zones permanently obscure sensitive areas regardless of content. Ideal for protecting residential windows, private property boundaries, and areas where surveillance is inappropriate.

Export Integration: Privacy masking automatically applied to all video exports based on configured policies. Export recipients receive appropriately masked content without access to original unmasked footage.

5.2. Video Wall Integration

Professional video wall capabilities transform Sentinel into a comprehensive control room solution for large-scale security operations.

Control Room Video Wall Support: Integration with professional video wall systems for dedicated control room environments. Multi-monitor configurations display camera feeds across large-format displays with centralized control and management.

Flexible Layouts: Customizable multi-camera display configurations supporting diverse monitor arrangements. Drag-and-drop layout creation enables rapid reconfiguration for different operational scenarios.

Automatic Camera Rotation: Scheduled camera cycling ensures comprehensive coverage review across large camera estates. Configurable rotation intervals and camera groupings optimize operator attention distribution.

Alert-Triggered Display: AI-detected incidents automatically promote affected cameras to prominent display positions. Severity-based display prioritization ensures operator attention is directed to highest-priority events.

Multi-Monitor Support: Seamless spanning across multiple monitors for control room deployments. Individual monitor configuration enables optimized display for specific operator roles and responsibilities.

Incident Focus Mode: Single-click expansion of specific cameras for detailed incident investigation. Quick return to standard layout after incident review.

Personal Video Wall: In addition to physical video wall integration, Sentinel provides each user with their own web-based personal video wall interface. Users can create, save, and recall custom multi-camera layouts featuring the cameras most relevant to their role and responsibilities—delivering video wall functionality to any desktop without requiring dedicated control room infrastructure.

5.3. UTMC Integration Service

Seamless integration with Urban Traffic Management and Control systems enables coordinated traffic management and emergency response optimization.

Traffic Signal Integration: Real-time data exchange with traffic signal controllers enables coordinated incident response. Detected traffic incidents can trigger signal timing adjustments to manage congestion.

Emergency Vehicle Priority: Integration with emergency vehicle detection enables automated traffic signal priority. When sirens are detected on approach routes, traffic signals can be adjusted to clear paths for emergency responders, potentially reducing response times.

Data Exchange: Standardized UTMC data formats ensure compatibility with existing traffic management infrastructure. Bidirectional data flow enables both contribution of AI analytics insights and consumption of traffic management data for enhanced situational awareness.

Event Coordination: Major event management coordination between CCTV monitoring and traffic management systems. Crowd detection and traffic analysis inform traffic management decisions during large public events.

5.4. External Sharing Portal

Secure mechanisms for sharing video content with external parties while maintaining control, compliance, and comprehensive audit trails. The External Sharing Portal eliminates the need for insecure email attachments or third-party file sharing services, providing a purpose-built secure channel for evidence sharing that is both easier to use and significantly more secure.

Time-Limited Share Codes: Generate unique access codes for specific video clips with configurable expiration periods. Recipients access content through the secure portal without requiring platform accounts, eliminating complex onboarding processes while maintaining full security and audit compliance.

Access Controls: Configurable viewing limits (maximum views, time-based expiration), geographic restrictions where appropriate, and immediate revocation capability for emergency access termination.

Privacy Integration: Automatic application of privacy masking to shared content based on configured policies. External recipients receive appropriately redacted footage without access to unmasked content.

Audit Logging: Comprehensive logging of all external access including recipient identifier, access timestamps, viewing duration, and geographic location. Full accountability for all external video sharing.

Evidence Packages: Bundle multiple video clips with supporting documentation for comprehensive evidence packages. Chain of custody documentation automatically generated.

6. Data Protection

6.1. Information Assurance

M2M Tech maintains comprehensive information security with Cyber Essentials certification and hosting on Microsoft Azure UK regions. We implement multi-factor authentication, end-to-end encryption, role-based access controls, and continuous security monitoring.

Our security framework includes GDPR compliance, Government Security Classification Policy adherence, regular penetration testing and vulnerability assessments, and regular third-party security audits. We follow public sector data handling standards and transport security best practices with continuous compliance monitoring and comprehensive audit trails for all system access and user activities.

6.2. Data Back-Up and Restoration

Our platform implements robust data protection through multiple layers:

- Local Storage: CCU devices provide local DVR functionality with configurable recording periods for on-site video retention
- Cloud Backup: Automated backup of configuration data, user settings, camera configurations, and metadata to secure cloud infrastructure
- Data Integrity Verification: Automated backup integrity testing and verification processes for both local and cloud storage
- Recovery Procedures: Automated recovery processes for device failures with remote diagnostics and power cycling capabilities
- Testing Schedule: Monthly backup testing and quarterly disaster recovery exercises

Client-specific backup requirements can be discussed and documented in the Order Form, including extended retention periods, additional backup locations, or enhanced recovery time objectives.

6.3. Business continuity statement/plan

The business continuity plan covers all critical functions of the M2M CCTV Cloud Platform including:

- Cloud infrastructure
- Edge computing devices
- User access
- Emergency response capabilities

Key Business Areas:

- Cloud platform hosting
- CCU device management
- AI analytics processing
- User authentication and access control
- Emergency alerting systems
- Customer support services

Critical Functions:

- Real-time monitoring and alerting
- On-demand video streaming
- AI-powered incident detection
- Cross-organizational access management
- Emergency response coordination

Dependencies:

- Cloud infrastructure providers
- Cellular network connectivity
- Power supply to CCU installations
- Integration points with customer UTMC systems

Acceptable Downtime:

- Cloud platform - target maximum 4 hours per month (99.5% availability)

- CCU devices - individual device failures do not impact overall system
- Emergency alerting - best effort recovery within business hours

Continuity Plan:

- Redundant cloud infrastructure across multiple availability zones
- Automated failover procedures
- Alternative communication channels for emergency alerts

A more detailed plan can be provided/agreed with buyer on request

6.4. Privacy by Design

Our platform incorporates privacy protection from the design phase, ensuring full GDPR compliance:

- Data Minimization: Only necessary data is collected and processed for CCTV security operations, with automatic deletion of older recordings
- Purpose Limitation: Clear definition of data usage purposes with strict controls preventing unauthorized access - data used solely for security monitoring and incident response
- Access Controls: Fine-grained permissions ensuring users only access data necessary for their role and organizational requirements
- Audit Logging: Comprehensive tracking of all data access, modification, and sharing activities
- Consent Management: Clear processes for managing consent and data subject rights
- Privacy Impact Assessments: Regular evaluation of privacy risks and mitigation measures for new features and integrations
- Encryption: End-to-end encryption for all data transmission and storage
- Automated Privacy Protection: AI-powered privacy masking with automatic detection and blurring of faces and number plates, plus manual privacy zone definition for sensitive areas
- Secure Sharing Controls: Time-limited share codes for external video sharing that expire automatically and can be revoked instantly, ensuring controlled access to sensitive footage
- Video Data Privacy: Configurable recording periods and automated purging of video content based on retention policies
- Evidence Management Privacy: Secure, privacy-compliant evidence sharing with automated masking and controlled external access
- Anonymization: Where possible, personal data is anonymized or pseudonymized

7. Using the service

7.1. Ordering and Invoicing

Initial Engagement Process:

To begin using our CCTV Enhancement & Stability System service, prospective customers should email their requirements to info@m2mtechltd.com, please include the following information:

- Number and type of cameras requiring modernization or new installation
- Current infrastructure details and any integration requirements
- User access requirements including cross-organizational needs
- Specific AI analytics or monitoring requirements

- Any additional features or services required
- Preferred implementation timeline and any specific deployment constraints

Order Process:

1. Initial consultation calls to discuss requirements and demonstrate capabilities
2. Technical assessment of current infrastructure and integration needs
3. Customized proposal with pricing and implementation timeline
4. Order Form completion with agreed specifications and service levels
5. Contract execution and project initiation

Invoicing:

- Monthly billing in arrears for standard service subscriptions
- Quarterly billing available for annual commitments
- Professional services billed upon completion of milestones
- All invoicing through standard government procurement channels

7.2. On-Boarding, Off-Boarding, Service Migration & Scope

On-boarding Process:

Our structured on-boarding typically takes 8-12 weeks depending on deployment scale and complexity and includes:

- Kick-off Meeting: Dedicated session with technical team and key stakeholders
- Site Assessment: Comprehensive survey of existing camera infrastructure and network requirements
- Implementation Planning: Detailed deployment schedule coordinated with customer operational requirements
- CCU Installation: Professional installation of CCTV Controller Units with minimal service disruption
- Platform Configuration: User account setup, access permissions, and AI analytics configuration
- Training Delivery: Comprehensive training for all user types including cross-organizational teams
- Go-Live Support: Initial 30-day support period with dedicated technical assistance

Off-boarding Process:

- Termination Notice: 60-day notice period required with engagement to formulate transition plan
- Data Export: Customers can export all configuration data, user settings, and available video content
- Access Removal: Systematic removal of user access with comprehensive audit trail
- Equipment Recovery: CCU devices removed from site or transitioned to customer ownership as agreed
- Documentation Handover: Complete documentation of system configuration and operational procedures

Service Migration: Bespoke migration plans available for transitioning to alternative providers, including data format conversion and technical documentation support.

7.3. Training

Comprehensive training ensures successful platform adoption across all organizational levels:

Training Delivery Methods:

- Web Portal Documentation: 24/7 access to comprehensive help system, step-by-step guides, and interactive tutorials
- Online Training Sessions: Dedicated virtual training sessions conducted via online meetings for all user types and organizational roles
- In-Person Training: On-site training available upon request for complex deployments or specific operational requirements

Training Content:

- Role-Based Training Programs: Specialized curricula for operators and administrators
- Cross-Organizational Training: Multi-agency training sessions designed for police, contractors, emergency services, and other stakeholder groups
- Feature-Specific Training: Focused sessions on AI analytics, audio detection capabilities, emergency response procedures, and collaborative access management
- Administrative Training: User management, access controls, system configuration, and integration with existing UTMC systems

Training Support:

- Training Materials: Comprehensive documentation, quick reference guides, and video tutorials provided for ongoing reference

7.4. Implementation Plan

Our structured implementation approach typically takes 4-8 weeks depending on deployment scale and infrastructure complexity:

Implementation Phases:

- Discovery & Site Assessment: Comprehensive survey of existing camera infrastructure, network requirements, and stakeholder operational needs
- Technical Configuration: CCU installation planning, AI analytics setup, and platform configuration tailored to security requirements
- System Integration: Professional CCU deployment, UTMC integration testing, and cross-organizational access configuration
- User Training & Testing: Role-based training delivery, system testing with stakeholders, and emergency response validation
- Go-Live & Optimization: Phased deployment with performance monitoring, final optimization, and post-implementation support

Key Milestones:

- Week 1-2: Site survey and technical requirements assessment
- Week 3-4: CCU deployment with minimal service disruption
- Week 5-6: Training delivery and integration testing
- Week 7-8: Go-live support, optimization, and handover

A detailed implementation plan can be provided/customised to the buyer on request, including specific timelines, resource requirements, and deployment strategies tailored to organizational security requirements.

7.5. Service Management

Our structured service management practices aligned with industry standards, specifically designed for critical security infrastructure. Our service management approach ensures reliable, consistent service delivery through:

Service Management Framework:

- Incident Management: Structured escalation procedures with defined severity levels prioritizing security-critical functions, emergency response, and camera availability
- Problem Management: Root cause analysis focused on CCU device reliability, AI analytics performance, and multi-agency access continuity
- Change Management: Controlled change processes to minimize disruption to security monitoring and ensure continuity of emergency response capabilities
- Configuration Management: Comprehensive tracking of CCU deployments, camera configurations, AI analytics settings, and cross-organizational access permissions
- Service Level Management: Continuous monitoring of camera uptime, AI detection accuracy, and emergency alerting performance with regular reporting

Service Delivery:

- 24/7 automated monitoring with proactive alerting for camera failures, CCU device issues, and AI analytics disruptions
- Specialized service desk processes for security-specific support including emergency response coordination, evidence management, and multi-agency collaboration
- Regular service reviews with performance reporting focused on security effectiveness, incident response times, and operational resilience
- Continuous service improvement based on feedback, incident analysis, and evolving public safety requirements
- Documented procedures and knowledge base covering CCU management, AI configuration, and emergency response protocols

Customer Integration:

- Monthly service performance reports including camera availability, incident detection rates, and emergency response metrics
- Quarterly reviews available upon request to assess security performance and identify enhancement opportunities
- Escalation procedures for urgent security incidents requiring immediate emergency response coordination
- Change notification processes for planned maintenance affecting critical security infrastructure and emergency capabilities

7.6. Service Constraints

Our CCTV platform operates within defined parameters to ensure optimal performance and reliability for critical security infrastructure:

Availability Constraints:

- Support Coverage: 9 AM - 5 PM Monday-Friday for routine queries (24/7 emergency support available for critical security incidents at additional costs based upon our rate card)
- Response Times: Vary by incident severity with priority given to security-critical and emergency response functions
- Infrastructure Dependencies: Service continuity dependent on cellular network coverage and power supply to CCU installations

Customization Constraints:

- UTMC Integration: Modifications for complex traffic management integration require professional services assessment and development
- Multi-Agency Configuration: Complex cross-organizational access scenarios may require extended security clearance and configuration periods
- Analytics Capabilities: Advanced AI features and custom audio detection algorithms available through add-on services

Deprecation Schedule:

- Feature Changes: 60-day advance notice for any feature deprecation

7.7. Service Levels

Our service levels are specifically designed to meet critical security operational requirements and emergency response demands:

System Availability:

- Cloud Security Platform: 99.5% uptime with redundant infrastructure and automated failover for continuous security monitoring (proven track record over 12 years)
- CCU Edge Devices: 99.2% individual device availability with automated fault reporting and remote diagnostics for camera infrastructure
- Emergency Alerting System: 99.5% availability with best effort recovery during business hours for critical security incidents and emergency response coordination

Performance Standards:

- Video Stream Initiation: Maximum 10 seconds from request to live video display for emergency response situations
- AI Alert Generation: Real-time processing with security alerts delivered within 30 seconds including audio-based incident detection
- Platform Response Time: Maximum 10 seconds for all user interactions and emergency access functions

Support Response Times:

- Critical (P1): 4-hour response, 8-hour resolution target for security system failures and emergency response disruptions

- High (P2): 8-hour response, 2 business day resolution target for camera connectivity and multi-agency access issues
- Medium (P3): 1 business day response, 5 business day resolution for configuration and integration adjustments
- Low (P4): 3 business days response, best effort resolution for enhancement requests and routine maintenance

Service levels can be customized and documented in the Order Form based on specific security operational requirements and emergency response protocols.

7.8. Outage and Maintenance Management

Our comprehensive approach to service reliability ensures continuous security monitoring and emergency response capabilities through:

Proactive Outage Prevention:

- Redundant cloud infrastructure across multiple availability zones with automated security continuity and emergency response failover
- Automated failover procedures with health monitoring for CCU devices and critical security functions
- Proactive monitoring with failure detection for camera systems, AI analytics, and multi-agency access points
- Advanced predictive maintenance for CCU hardware and camera infrastructure to prevent security coverage gaps

Service Performance Planning:

- Capacity planning based on security usage patterns, emergency response requirements, and multi-agency collaboration growth
- Regular performance testing and optimization for video streaming, AI analytics, and emergency alerting systems
- Network bandwidth optimization through on-demand streaming model ensuring efficient emergency response access

Downtime Measurement:

- Real-time monitoring with automated incident detection for security systems and emergency response capabilities
- Monthly availability reports with detailed incident analysis
- Root cause analysis for all security service interruptions and improvement recommendations
- Continuous improvement based on incident learnings and emergency response effectiveness analysis

Ad-hoc Service Support:

- Emergency response team available for critical security incidents and emergency coordination (24/7 availability at additional cost)
- Rapid deployment capabilities for urgent camera replacements and emergency security coverage during incidents
- Flexible resource allocation during security events, emergency situations, and multi-agency response scenarios

- Disaster recovery procedures with business hours response for features and emergency response capability restoration

8. Provision of the service

8.1. Customer Responsibilities

Our partnership approach requires clear customer responsibilities to ensure optimal service delivery and operational excellence:

Infrastructure Provision & Environmental Requirements:

- Provide secure physical locations for CCU installation with appropriate environmental protection
- Ensure adequate power supply (240V mains electricity) to designated CCU installation points with appropriate surge protection
- Coordinate site access for installation, maintenance, and emergency response personnel as required
- Maintain secure physical access controls and environmental monitoring for critical equipment installations

Operational Requirements:

- Provide timely feedback during implementation, testing, and system optimization phases
- Maintain current contact information for emergency alerts, security notifications, and critical system communications
- Ensure availability of key personnel during implementation phases, system updates, and emergency response situations

Security & Compliance Management:

- Ensure compliance with organizational data protection policies, privacy regulations, and surveillance legislation requirements
- Maintain appropriate user access controls with regular security reviews and permission audits according to established protocols
- Report security incidents and unauthorized access attempts promptly according to escalation procedures and regulatory requirements
- Comply with acceptable use policies for surveillance system access, monitoring activities, and evidence management
- Coordinate with law enforcement agencies and emergency services for incident response and evidence sharing protocols

Operational Continuity & Risk Management:

- Participate in disaster recovery testing and business continuity planning exercises as required for critical security infrastructure
- Provide advance notice of planned operational changes that may affect surveillance coverage or emergency response capabilities
- Maintain backup procedures for critical security monitoring processes during system maintenance and upgrades

- Ensure trained personnel availability during system updates, security incidents, and emergency response coordination

8.2. Technical Requirements and Client-Side Requirements

Our CCTV Enhancement & Stability System integrates seamlessly with existing security infrastructure while providing advanced upgrade pathways for comprehensive surveillance capabilities:

Hardware and Platform Requirements:

- Client-side access via modern web browsers (Chrome, Firefox, Safari, Edge) on desktop workstations, tablets, or mobile devices
- No additional server infrastructure required - fully cloud-based solution with scalable architecture
- Optional video wall configurations supporting multiple monitors or projectors with standard video inputs for enhanced control room viewing
- Mains electricity supply to CCTV installation points (240V standard UK supply) with appropriate surge protection

Personnel and Resource Requirements:

- Designated system administrator with security clearance for user management, system configuration, and access control
- Trained operators for daily surveillance monitoring, incident response, and emergency coordination
- Technical liaison personnel for integration with existing traffic management systems and emergency services
- Site security coordinator for installation access and ongoing maintenance coordination

Customization and Integration:

All specific technical requirements, integration specifications, and customization needs can be comprehensively discussed and documented in the Order Form as mutually agreed between M2M Tech and the customer organization.

8.3. Outcomes/Deliverables

Our comprehensive CCTV Enhancement & Stability System delivers measurable security outcomes through integrated platform capabilities and continuous performance optimization:

Core System Access & Functionality:

- Fully functional cloud-based CCTV management platform with secure web portal access and multi-device compatibility
- CCU edge computing devices professionally installed and configured for all designated camera locations with optimal performance settings
- Advanced AI analytics suite with automated monitoring, intelligent alerting, and comprehensive audio detection capabilities
- Sophisticated audio incident detection system for collision/collapse/vehicle horn alerts with automated visual tracking and response coordination
- Emergency vehicle siren detection with seamless integration to traffic light priority management systems and emergency response protocols
- Advanced panic audio detection for crowd safety monitoring with automated alerting and incident escalation procedures
- Gunfire audio detection with advanced firearm classification capabilities for enhanced security response and threat assessment
- Cross-organizational access controls configured for all stakeholder groups including police, emergency services, and authorized personnel
- Comprehensive integration with existing UTMC systems including emergency vehicle priority control and traffic management coordination

Measurable Operational Outcomes:

- Dramatic improvement in camera reliability achieving 99.2%+ uptime through proactive monitoring and automated fault detection
- Complete elimination of expensive on-premises server infrastructure requirements with fully cloud-based architecture
- Significantly streamlined access procedures reducing emergency response times and improving incident coordination
- Enhanced collaboration capabilities with police, contractors, and emergency services through secure, privacy-compliant video sharing
- Advanced privacy-compliant evidence management with automated masking and controlled external access for legal proceedings
- Comprehensive audio-based incident detection reducing response times for collisions, emergencies, and security threats
- Automated emergency vehicle priority management through intelligent traffic light integration and real-time coordination
- Complete audit trails for all system access and control actions ensuring compliance and accountability

Comprehensive Business Benefits:

- Significant operational cost reduction through automated fault detection, predictive maintenance, and streamlined processes
- Extended hardware lifecycle for existing camera investments through intelligent optimization and performance enhancement

- Improved operational efficiency through intelligent monitoring, automated alerting, and advanced audio-based incident detection
- Enhanced emergency response capabilities with precise geolocation, spatial awareness, and sophisticated audio incident classification
- Proactive threat detection through advanced gunfire and panic audio monitoring with immediate escalation protocols
- Substantially reduced emergency response times through automated siren detection and intelligent traffic priority management systems

8.4. Development life cycle of the solution

M2M Tech employs a robust Agile development methodology with continuous improvement cycles specifically tailored for security and surveillance systems:

Structured Development Framework:

Phase-Based Development Approach:

1. Requirements Analysis: Continuous engagement with security professionals and emergency services to identify operational challenges, threat assessment needs, and surveillance system requirements
2. Strategic Planning: Sprint planning with prioritized feature development based on security feedback, regulatory compliance, and law enforcement best practices
3. Security-Centred Design: Collaborative design approach incorporating stakeholder input, privacy standards, and operational security optimization
4. Iterative Development: Systematic development with regular security testing, quality assurance, and compliance validation throughout the development process
5. Comprehensive Testing: Multi-tier testing including unit tests, integration testing, penetration testing, and real-world security scenario validation
6. Controlled Deployment: Continuous deployment with automated testing, security verification, rollback capabilities, and minimal operational disruption protocols
7. Ongoing Enhancement: Continuous monitoring, support, and platform enhancement based on security feedback and emerging threat landscape requirements

Release Management & Platform Evolution:

- Monthly Platform Updates: Regular feature releases and security improvements delivered automatically with minimal service disruption and comprehensive testing protocols
- Critical Security Updates: Immediate deployment of security patches and urgent bug fixes with comprehensive validation and regulatory compliance verification
- Security Feedback Integration: Systematic incorporation of security professional requirements and operational insights into development roadmaps
- Regulatory Compliance: Ongoing platform updates to maintain compliance with surveillance regulations, privacy standards, and law enforcement requirements

8.5. After-sales Account Management

Every client is assigned a dedicated account manager who serves as your primary point of contact throughout the entire service lifecycle. This ensures continuity, personalized service delivery, and a deep understanding of your specific transport operational requirements and strategic objectives.

Our comprehensive account management approach ensures sustained security value delivery and strategic partnership development throughout the service lifecycle:

Strategic Security Relationship Management:

- Quarterly Security Reviews: Comprehensive performance assessments including system security metrics, incident response analysis, and operational security improvement opportunities
- Annual Strategic Security Planning Sessions: Collaborative security roadmap development aligned with organizational security strategies and threat landscape evolution
- Regular Security Performance Check-ins: Proactive security satisfaction monitoring and value realization assessments with dedicated security-focused account management support
- Multi-Level Stakeholder Engagement: Security relationship management including technical security teams, operational security managers, and strategic security decision-makers

Customer Success & Security Enhancement Strategy:

- Proactive Security Service Enhancement: Continuous identification of value-adding security services and operational optimization opportunities based on threat analytics and security industry developments
- Security Innovation Updates: Early notification and demonstration of new platform security features, capabilities, and industry-leading surveillance technologies
- Security Expansion Support: Strategic assistance with deployment scaling, additional security service integration, and multi-site security implementation coordination
- Security Best Practice Sharing: Knowledge transfer sessions and security benchmarking insights from similar security organizations and surveillance deployments

Continuous Security Value Optimization:

- Security Performance Analytics: Regular analysis of threat detection metrics, incident response effectiveness, and security system utilization indicators
- Security Feedback Integration: Systematic incorporation of security insights into service improvements and platform security development priorities
- Security Technology Evolution: Ongoing assessment of emerging security technologies and their potential integration into existing surveillance infrastructure
- Threat Landscape Monitoring: Continuous evaluation of evolving security threats and proactive platform adaptations to maintain security effectiveness

8.6. Termination Process

Our comprehensive termination framework ensures seamless service conclusion while protecting security infrastructure continuity and organizational interests:

Termination Rights & Contractual Framework:

- G-Cloud No-Fault Termination: In accordance with G-Cloud framework requirements, buyers may terminate this service for any reason with 30 days written notice, ensuring procurement flexibility while allowing adequate transition planning for security infrastructure and emergency response capabilities
- Standard Termination Notice: Either party may terminate with 30 days written notice for standard service agreements outside the G-Cloud no-fault provision, ensuring comprehensive transition planning for security infrastructure and emergency response capabilities
- Immediate Termination Rights: Material breach or insolvency situations permit immediate termination with appropriate safeguards for ongoing security monitoring and emergency response functions
- Customer Convenience Termination: Customer organizations retain rights to terminate for convenience with appropriate notice periods aligned with security operational requirements and emergency preparedness protocols
- Security Service Continuity: M2M Tech maintains full-service quality and security monitoring standards throughout the entire notice period including emergency response capabilities

Comprehensive Data Protection & Migration Support:

- Structured Data Export: Customer data facilitated in multiple standard formats (CSV, JSON, XML) including security configurations, camera settings, access controls, and incident analytics
- Extended Data Retention: 30-day secure data retention period following termination for recovery purposes and security transition support
- Certified Secure Deletion: Secure data deletion certification provided upon request with comprehensive audit trails, compliance verification, and evidence management protocols
- Security Migration Assistance: Technical assistance with data migration to alternative security systems including format conversion, access control transfer, and emergency response integration support

Financial Settlement & Commercial Terms:

- Pro-rata Service Billing: Payment obligations limited to services rendered up to the termination date with transparent security service accounting
- Unused Service Refunds: Pro-rata refunds provided for unused prepaid services where applicable, calculated on daily usage basis for security platform access
- No Penalty Termination: No early termination penalties applied for termination for convenience, supporting organizational security strategy flexibility
- Outstanding Services Settlement: Settlement of any remaining professional services, security integration, or technical support charges according to agreed schedules

Transition Support & Security Continuity:

- Phased Security Reduction: Gradual service reduction implemented to minimize operational disruption to security monitoring and emergency response capabilities

- Technical Security Migration: Comprehensive technical assistance with data export, security system migration, and alternative platform integration including CCU device transition
- Security Knowledge Transfer: Structured knowledge transfer sessions ensuring continuity of security operations, emergency response procedures, and technical understanding
- Extended Security Support: Post-termination technical support available for 60 days covering security transition queries, emergency response continuity, and operational assistance

Service Agreement Considerations:

Customers acknowledge service commitment for the Minimum Period (typically 12 months) and subsequent Renewal Terms as defined in the Certificate or Order Summary. Early termination may result in loss of volume pricing benefits or preferential security service terms, though no financial penalties apply for convenience termination.

G-Cloud Renewal Requirements:

In accordance with G-Cloud framework requirements, service renewals must be agreed with comprehensive transition and continuity plans established at least 8 months prior to the end of the contract period. This ensures adequate time for:

- Strategic planning and budget approval processes
- Technical transition planning if changing providers
- Continuity of security monitoring and emergency response capabilities
- Stakeholder engagement and training requirements
- Compliance and security clearance processes for new service arrangements

M2M Tech commits to proactive engagement with customers regarding renewal planning, providing advance notice of contract expiration dates and supporting strategic planning discussions to ensure seamless continuation of critical security infrastructure services.

9. Our experience

9.1. Case Studies

9.1.1. Case Study 1: Oxfordshire County Council - Legacy CCTV Transformation

Challenge: OCC operated 60 PTZ cameras monitoring highways and carriageways with only 12 devices functional (20% uptime). Fixed cameras failed within 24-48 hours requiring site visits, while complex access procedures (VM access, then VNC/web connections) caused operational delays. Network conflicts with traffic light controllers forced camera disconnection, impacting critical traffic management systems.

Solution: M2M Tech deployed CCTV Controller Units (CCU) transforming the legacy system into a wireless, cloud-managed platform. CCU devices eliminated network conflicts by providing wireless connectivity, while on-demand streaming eliminated expensive server infrastructure requirements. The platform enabled collaborative access for multiple departments and external organizations including police and contractors.

Results: Achieved 99.2%+ uptime across entire camera estate, transforming system reliability from 20% to near-perfect availability. Eliminated 24-48 hour failure cycles through automated self-monitoring and fault reporting. Reduced operational costs by eliminating server infrastructure while enabling advanced AI capabilities including traffic monitoring, flood detection, audio-based incident detection, emergency vehicle siren detection, and emergency response features. Enhanced multi-agency collaboration through fine-grained access controls and evidence management capabilities.

9.1.2. Cast Study 2: County Council Network Deployment - Multi-Agency Collaboration

Challenge: Large county deployment requiring coordination between traffic management, highways maintenance contractors, and law enforcement agencies. Existing systems provided limited access capabilities and no integration between organizations, leading to delayed incident response and inefficient evidence collection.

Solution: M2M Tech implemented comprehensive multi-organizational access controls with role-based permissions. Traffic department maintains full system access, highways contractors receive live streaming capabilities for obstruction clearing, while law enforcement agencies access video recall and evidence download features. Integrated AI analytics provide automated alerts for all stakeholder groups.

Results: Streamlined emergency response through coordinated access and advanced audio AI detection capabilities, reduced incident response times through automated detection and alerting including collision/collapse audio alerts and emergency vehicle siren detection, improved evidence collection efficiency with privacy-compliant sharing capabilities and comprehensive audit trails, and enhanced operational coordination between multiple agencies within unified platform with secure external video sharing via time-limited access codes.

9.2. Clients

Our client base includes leading public sector organizations across the UK:

Local Authorities:

- Oxfordshire County Council - 100+ CCTV Cameras
    - Shared Access with Milestone Infrastructure Group
    - Shared Access with Doncaster Security Operations Centre

Key Client Sectors:

- County councils and unitary authorities
- Public Transport organizations
- Highway maintenance contractors
- Emergency services requiring evidence collection capabilities

10. Contact Details

Primary Contact:

- Name: Mathew Sunderland
- Email: info@m2mtechltd.com
- Phone: (+44) 01235 819890

Business Hours:

- Monday - Friday: 9:00 AM - 5:00 PM GMT

Business Address:

- Unit 4 Harrier Park, Hawksworth, Didcot, Oxfordshire, OX11 7PL

Our dedicated G-Cloud team provides comprehensive support from initial enquiry through implementation and ongoing operation, ensuring successful deployment and optimal platform utilization for all customer requirements.