



WHITE PAPER

Security as a Service: Ownership Models, SLAs and Contract Terms

A buyer's guide to managed physical security: ownership models, service scope, SLA design, per-camera and per-door pricing, refresh and exit terms.

By IoT Hybrid Solutions

MANAGED SERVICES

SECURITY AS A SERVICE

SLAS

PROCUREMENT



Executive summary

- Security as a service turns physical security systems into a managed, monthly service. The first decision is ownership: does the customer own the equipment, or does the provider?
- A clear scope is more valuable than a long one. Write down what is covered, what is excluded and who performs third-party work such as electrical, cabling and network changes.

- Good SLAs separate response from restoration, define uptime precisely, and require reporting that the customer can verify.
- Unit pricing by covered camera and door makes cost predictable and scales with the estate. Understand what each unit includes.
- Plan the end at the beginning: refresh, transition and exit terms protect both parties and should be agreed before signature.

What security as a service means

In a managed physical security model, a provider takes ongoing responsibility for keeping video, access control and related systems healthy, current and supported, in exchange for a recurring fee. The model can follow a one-time installation, or it can wrap around systems the customer already owns.

Why organizations choose it

- **Predictable cost:** operating expense in place of irregular repair and upgrade spending
- **Defined accountability:** one party responsible for health, patching and restoration
- **Skills coverage:** access to engineers who know the platforms, without building that bench internally
- **Lifecycle discipline:** firmware, software and hardware kept within support
- **Evidence:** regular reporting for audits, risk reviews and leadership

When it may not fit

Organizations with a large, experienced in-house technical team and a stable estate may prefer to buy time and materials support only. The decision should rest on capability, risk tolerance and how the organization prefers to fund security, not on a general preference for outsourcing.

Ownership models

Two common models exist, and many programs use both across different sites.

Customer-owned assets

The customer buys and owns the equipment, often through a project, and the provider manages it under a subscription.

- Suits existing estates and organizations that prefer capital ownership
- Hardware replacement is typically billed separately or covered by manufacturer warranty
- The customer controls refresh timing and budget
- Requires a clear baseline: the provider should assess and document the estate's condition at onboarding, and exclude pre-existing defects or price their remediation separately

Provider-owned equipment

The provider supplies, owns and maintains the equipment, and the customer pays a recurring fee for the service.

- Suits new sites, temporary sites and organizations that prefer operating expense
- Hardware failure and refresh are the provider's responsibility within the defined scope
- The contract must address what happens to equipment at the end of term: removal, purchase at a defined value or renewal
- Title, insurance and risk of loss should be stated explicitly

Choosing between them

- What is the organization's preference between capital and operating expense?
- How old is the current estate, and how much remediation would onboarding require?
- How long will the site be occupied?
- Who should carry hardware failure risk?

What managed services cover and exclude

Scope disputes cause most managed service friction. A good scope is specific and lists exclusions as clearly as inclusions.

Commonly included

- Health monitoring of devices, servers and integrations
- Remote technical and configuration support during defined hours
- Software and firmware updates, tested before deployment
- Critical incident response and restoration
- Field technician service for covered devices
- Preventive maintenance and periodic health checks

- Configuration backups and documentation updates
- Operator and administrator training
- Regular service reporting and review meetings

Commonly excluded or separately scoped

- Guard services and physical alarm response
- Live video monitoring and alarm monitoring, typically performed by the customer's GSOC or a central station
- New installations, moves, adds and changes beyond a defined allowance
- Damage from vandalism, misuse, environmental events or third-party work
- Electrical work, low-voltage cabling and network or IT configuration, which are typically the customer's trades and IT team unless the provider is contracted for them
- Software licenses and hardware not listed in the covered inventory

Write the covered inventory into the order document, by site and device, and agree a process for adding and removing devices.

SLA design

A service level agreement should describe what the customer will experience and how it will be measured.

Elements of a strong SLA

- **Priority definitions:** tie priority to impact, such as a site-wide outage, a critical door or camera, or a single non-critical device.
- **Response time:** how quickly the provider acknowledges and begins work, by priority and by hours of coverage.
- **Restoration target:** how quickly service is restored or a workaround is in place. Restoration matters more to operations than response.
- **Uptime or availability:** define what is measured (platform, server, device class), the measurement window and what is excluded, such as scheduled maintenance or customer-caused outages.
- **On-site attendance:** when a technician must be dispatched and the expected arrival window by region.
- **Escalation path:** named roles at each level, from service desk to account executive.

Reporting

- Monthly report of incidents, response and restoration performance against target
- Device health and availability by site
- Firmware and software currency against the approved baseline
- Open problems, root causes and recommended actions
- Quarterly service review with trends and lifecycle forecasts

Remedies

Service credits are common, but the more important remedy is a corrective action process with named owners. Agree how chronic underperformance is handled. Consult counsel on how remedies interact with the rest of the agreement.

Unit pricing by camera and door

Many providers price managed services per covered unit, most often per camera and per door, billed monthly.

Why the model works

- Cost scales with the estate and is easy to forecast
- Adding or removing devices has a clear, pre-agreed effect
- Sites of different sizes are priced consistently
- Budget owners can allocate cost by site or business unit

What to clarify

- What a "camera" and a "door" include: multi-sensor cameras, readers on both sides of a door, gates, turnstiles, intercoms, LPR cameras
- Whether servers, recorders, controllers and network devices are included in the unit or listed separately
- Whether ownership model changes the unit (customer-owned versus provider-owned)
- Minimum quantities, term commitments and how mid-term changes are handled
- What is billed outside the unit, such as after-hours work or out-of-scope changes

Lifecycle refresh

Managed services should keep the estate supported, not just running.

- Maintain an asset register with purchase dates, warranty and end-of-support dates
- Agree a refresh policy: replace on failure, replace at end of support, or planned refresh by age
- For provider-owned equipment, state when refresh is the provider's cost and when it is a new order
- For customer-owned equipment, ask the provider for an annual lifecycle forecast to support budgeting
- Align firmware and software baselines with cybersecurity requirements, and document exceptions

Transition and exit terms

The start and end of a managed service are where risk concentrates.

Onboarding

- Baseline assessment of the estate and its documentation
- Transfer of credentials, configurations and as-built drawings
- Agreed acceptance of the inventory and its condition
- Defined date from which SLAs apply

Exit

- Return of configurations, documentation, credentials and data in usable formats
- Removal or transfer of provider-owned equipment on agreed terms
- Transition assistance to a new provider or in-house team, with scope and rates defined in advance
- Renewal mechanics: notice periods, auto-renewal and price adjustments
- Termination provisions, including any amounts payable on early termination

Contract terms such as liability, governing law, termination and intellectual property vary by provider and have legal and financial consequences. Review them with your legal and procurement teams before signature.

Questions to ask a provider

- Which platforms and manufacturers do you support, and are you certified on them?
- Do you offer both customer-owned and provider-owned models?
- What exactly does a covered camera or door include?
- What are your response and restoration targets by priority, and how are they measured?
- Who performs electrical, cabling and network work, and how is it coordinated?
- How do you test firmware and software before deploying it?
- What does your monthly report contain? Can we see a sample?
- How do you protect remote access to our systems?
- What happens to our data, configurations and your equipment at the end of term?
- Who are the named roles on our account, from service desk to executive sponsor?

How IoT Hybrid Solutions can help

IoT Hybrid Solutions offers **managed services** for customer-owned and IoTHS-owned systems, priced per covered camera and door and billed monthly. We are platform-agnostic, write scope and exclusions explicitly, and state which work belongs to your electrical, cabling and IT teams. We can also deliver the installation that precedes a subscription through **turnkey installation**.

Next step

If you are comparing ownership models or reviewing a managed service proposal, we can walk through the scope and SLA with you. **Contact us** to start the conversation.