CASE STUDY // PHYSICAL ASSET SECURITY · IoT SURVEILLANCE

Budget-Grade Asset Protection

Self-Storage Surveillance & GPS Stack

Barr Cyber LLC · May 2026 · v1.1

A real deployment. Four independent security layers. Under $300 in hardware sourced same-day from retail. No professional installer. No proprietary ecosystem. No facility cooperation required.

$280	~$60	7 hrs	4
Hardware — One-Time	Monthly OpEx	UPS Runtime	Independent Layers

OVERVIEW

High-value assets stored in unattended environments — self-storage units, construction sites, remote properties, marina slips — are protected by a padlock and a gate code. That is a starting point for a motivated actor, not a deterrent. The standard of security offered by commercial storage facilities was not built for the threat model of a high-value target.

This case study documents a complete physical asset security stack designed, procured, and deployed in under 24 hours using same-day retail sourcing. The architecture is built on four independent layers with no single point of failure. Each layer operates autonomously. Defeating one does not defeat the stack.

“Most people put a padlock on a storage unit and walk away. The cost difference between that and a GPS tracker, two auto-tracking cameras with chained UPS backup, and a dedicated cellular hotspot is a dinner out.”

THREAT MODEL

Controls are matched to threat likelihood. Overspending on low-probability vectors wastes budget and creates false confidence. The following assessment drives hardware selection.

Threat Vector	Likelihood	Primary Mitigation
High-value vehicle theft	HIGH	GPS tracker on independent LTE + motion-alert camera
Opportunistic unit break-in	MEDIUM	Door-facing camera + cloud-stored motion event clips
Power interruption to facility	LOW	Dual chained UPS — 7-hour sustained runtime
Hotspot or WiFi failure	LOW	GPS operates on own LTE — fully independent
Camera tampering or destruction	LOW	GPS continues tracking independently of camera stack
Insurance claim with no evidence	MEDIUM	24/7 cloud-backed video + continuous GPS location history
RF-based GPS defeat	VERY LOW	Requires active scanning equipment outside opportunistic profile — see Known Limitations

BILL OF MATERIALS

Component	Model	Source	Cost	Role
GPS Tracker	LandAirSea 54	Walmart delivery	$35	Vehicle location on independent LTE
Cellular Hotspot	AT&T GoLink 5G	Walmart delivery	$59	Dedicated WiFi for cameras
Prepaid SIM	AT&T Prepaid SIM Kit	Walmart delivery	$5	Hotspot data
Security Camera ×2	Arlo Essential Pan/Tilt 1080p	Walmart delivery	$40 ea.	360° auto-tracking, cloud storage
UPS Backup ×2	APC Back-UPS 450VA BN450M	Walmart curbside	$56 ea.	Power resilience — chained runtime

ONE-TIME HARDWARE TOTAL **$280.44**
MONTHLY OPERATING COST **~$60** (GPS subscription ~$25 + AT&T prepaid data ~$35)

ARCHITECTURE — DEFENSE IN DEPTH

Four layers. Each operates autonomously. No single failure disables the full stack. This is the key design principle: the GPS tracker runs on its own LTE SIM, completely independent of the camera WiFi hotspot. Destroying the cameras does not defeat tracking. Cutting facility power does not defeat cameras. Disabling the hotspot does not defeat GPS.

Layer	Component	Function	Independence
1 — GPS	LandAirSea 54	Real-time vehicle location via LTE. Magnetic, concealed on frame.	Own LTE SIM — fully independent of all other layers
2 — Cameras	2× Arlo Essential Pan/Tilt	360° auto-tracking, motion alerts, live view, cloud storage	WiFi via dedicated hotspot — no facility network dependency
3 — Network	AT&T GoLink 5G Hotspot	Dedicated cellular WiFi for cameras	AT&T LTE — independent of GPS SIM and facility infrastructure
4 — Power	2× APC UPS chained	Sustains cameras + hotspot for 7 hours if facility power is cut	Self-contained battery — no facility power dependency

ADVANCED TIER — LOCAL NVR + SIEM ARCHITECTURE

The base stack relies on cloud-hosted video storage. This creates two dependencies: the camera manufacturer's cloud infrastructure must remain operational, and network connectivity must be available for footage retrieval. For higher-assurance deployments, a local NVR layer eliminates both dependencies and adds a SIEM-style alerting and correlation capability. The advanced tier runs on a Raspberry Pi 5 (16GB RAM) with Debian 12 Bookworm arm64 — a production-grade Linux base chosen deliberately over Raspberry Pi OS for its clean apt ecosystem, full systemd service management, and suitability as a headless security appliance.

ARCHITECTURE OVERVIEW

HARDWARE PLATFORM

Raspberry Pi 5 (16GB RAM) running Debian 12 Bookworm arm64 — minimal server install, no desktop environment, no Raspberry Pi OS. Debian was chosen deliberately: clean apt ecosystem, full systemd service management, no Pi-specific cruft, production-grade base for a security appliance. The Pi 5 with 16GB provides sufficient headroom for concurrent Frigate inference, Docker container overhead, MQTT brokering, and WireGuard without memory pressure under sustained load.

OS & SYSTEM ARCHITECTURE

Base OS: Debian 12 Bookworm (arm64) — minimal server, no GUI. Flashed via rpi-imager with custom image or dd from official Debian arm64 image.

Boot: NVMe HAT (Pimoroni or Geekworm) for OS and system partition. USB 3.0 SSD for Frigate recording storage — separated from system partition to prevent recording I/O from affecting OS stability.

Runtime: Docker CE (official arm64 build) manages all application containers. systemd manages Docker. No snap, no flatpak, no Pi-specific package overlays.

Hardening:ufw default-deny inbound, SSH key-only auth, fail2ban on SSH, unnecessary services disabled at boot, auditd for system call logging.

APPLICATION STACK

→ **Frigate NVR (Docker, arm64)** — Ingests RTSP streams from any ONVIF-compatible camera. Records H.264 to local SSD. Object detection via YOLOv8 — person, vehicle, animal discrimination. Publishes detection events to MQTT. Config via YAML. Web UI on localhost only — not exposed externally.

→ **Google Coral USB Accelerator** — USB 3.0 TPU for hardware-accelerated object detection inference. Offloads YOLO from CPU entirely. Frigate Coral integration is native — single config line. Without Coral, Pi 5 CPU handles inference for 2-camera deployments adequately but Coral is recommended for sustained 24/7 operation.

→ **Mosquitto MQTT Broker (apt, systemd)** — Lightweight publish/subscribe broker. Frigate publishes detection events to topics per camera per object class. Python collector subscribes. Runs as a native systemd service — not containerized, lower overhead.

→ **Python Event Collector (systemd service)** — Custom Python script. Subscribes to Mosquitto MQTT feed. Normalizes Frigate event payloads into structured JSON log entries with enriched fields: camera ID, object class, confidence score, clip path, timestamp (UTC), GPS correlation query. Forwards to Wazuh agent via local socket. Runs as a systemd service with automatic restart.

→ **Wazuh Agent (arm64, systemd)** — Ships normalized events and system logs to Wazuh manager on backhaul server. Wazuh arm64 packages are officially supported. Agent handles local log collection (auditd, auth.log, syslog) in addition to the Python collector feed.

→ **WireGuard (kernel-native, wg-quick)** — Kernel-native on Debian 12 — no DKMS, no module compilation. wg-quick manages the interface as a systemd service. All Pi-to-backhaul traffic — Wazuh events, MQTT if remote-bridged, management SSH — routes through the encrypted tunnel. No open inbound ports on the Pi from the public internet.

BACKHAUL SERVER

ZimaBoard 832 or equivalent x86 low-power always-on machine at a trusted fixed address (home lab or VPS). Runs: Wazuh Manager + Elasticsearch + Kibana (Wazuh stack), WireGuard peer endpoint, optional Frigate clip archive mount via SMB or rsync. Wazuh correlation rules fire on compound events — person detection + GPS position change within the same 60-second window elevates alert severity. All events timestamped, retained, and exportable for forensic or insurance use.

WHAT THIS ADDS OVER BASE TIER

Local footage retention completely independent of cloud service status or subscription. Object-

level detection with confidence scoring — eliminates motion-only false positives from wind, shadows, and insects. Compound event correlation across camera and GPS data streams. Full forensic event chain from camera detection through MQTT through Wazuh to export — timestamp integrity suitable for evidentiary use. Encrypted backhaul means monitoring infrastructure is not visible or accessible from the facility network at any point.

HARDWARE COST ESTIMATE — ADVANCED TIER

Raspberry Pi 5 16GB + NVMe HAT + SSD	**~$185**
Google Coral USB Accelerator	**~$65**
Backhaul server (ZimaBoard 832)	**~$200**
Debian 12 + Docker + Wazuh + WG (OSS)	**$0**
ADVANCED TIER TOTAL (one-time add)	**~$450**

INSURANCE REFERENCE — EVIDENCE VALUE

This stack serves a dual purpose: active deterrence and passive evidence generation. Every motion event produces a timestamped, cloud-stored clip. The GPS provides continuous location history. Both directly support an insurance claim.

Evidence Type	Source	Insurance Value
Real-time GPS location history	LandAirSea 54 via LTE	Proves asset location at exact time of loss
Timestamped entry/exit video	Arlo cloud + local NVR	Documents who accessed unit and when
Motion event clips + alert log	Arlo app + SIEM export	Establishes exact incident timeline
Hardware purchase receipts	Retail order history	Proves security measures were in place at time of loss
SIEM event log	Wazuh / Graylog (advanced tier)	Forensic-grade timestamped record of all events

---

KNOWN LIMITATIONS

This stack is designed for the opportunistic threat profile. It is not designed to defeat a technically sophisticated, targeted adversary with unlimited preparation time. The following limitations apply.

RF Countermeasures — Active RF scanning equipment can detect the GPS tracker's LTE transmission. Defeating it requires specialized hardware and knowledge outside the profile of an opportunistic actor. Correct deployment practice — concealed magnetic mount in a location requiring vehicle disassembly to access — raises the bar further. Deployment location is not documented in this publication.

Faraday Shielding — A Faraday bag placed over the GPS tracker defeats LTE transmission. Requires physical access to the tracker location. Mitigated by concealed placement. Not a realistic vector for opportunistic theft.

Camera Blind Spots — Two cameras provide wide coverage but not full 360° of a large unit. Pan/tilt auto-tracking compensates for fixed mounting limitations. Unit layout should be

assessed at deployment.

Cloud Dependency (Base Tier) — Base tier Arlo storage requires active cloud subscription and internet connectivity for retrieval. Local NVR tier (advanced) eliminates this dependency entirely.

Not a Substitute for Insurance — This stack is a deterrence and evidence layer. It does not replace renters or vehicle insurance. Deploy the stack regardless of coverage status, then get the insurance.

BARR CYBER — IMPLEMENTATION SERVICES

Barr Cyber LLC designs, sources, and deploys physical asset security stacks as a contracted service. Every component in this case study — and every tier above it — can be implemented for you, verified end-to-end, and handed over with full documentation and app access. No professional installer required on your end. No proprietary ecosystem lock-in. No ongoing dependency on Barr Cyber unless you want it.

BASE TIER DEPLOYMENT

Hardware sourced and delivered to your location. GPS tracker mounted and activated. Cameras installed and paired to hotspot. UPS units chained and verified. All apps configured on your device. Live feed and GPS ping confirmed before handoff. Flat deployment fee — contact for quote based on location and unit configuration.

ADVANCED TIER DEPLOYMENT

Full base tier deployment plus Raspberry Pi 5 NVR appliance configured on Debian 12, Frigate running with object detection tuned to your camera layout, Mosquitto and Python event collector operational, WireGuard tunnel established to backhaul server, Wazuh SIEM live with compound alert rules configured. Handed over with full architecture documentation and resumption instructions for any future technician.

CUSTOM & SCALED DEPLOYMENTS

The architecture in this document was designed to scale. The same four-layer independence model — GPS on its own LTE, cameras on dedicated cellular, local power backup, encrypted backhaul SIEM — applies identically to construction sites, remote properties, marine assets, agricultural equipment, multi-unit facilities, and small business after-hours monitoring. If the asset has value and sits unattended, the framework fits. Barr Cyber scopes, designs, and deploys to your specific threat model.

WHAT BARR CYBER BRINGS

→ Threat model assessment before hardware selection — controls matched to actual likelihood, not worst-case theater

→ Hardware sourced at cost — no markup on retail components

→ Full deployment documentation — every configuration, every credential, every dependency recorded

→ Insurance evidence architecture built in from day one — not an afterthought

→ Cybersecurity-first design — camera traffic encrypted, management access hardened, no exposed attack surface

→ No ongoing dependency required — you own the stack, the apps, and the data

PRICING MODEL

Hardware is passed through at cost — no markup. You pay exactly what Barr Cyber paid for the components, receipts on file. What you are paying for is the logic: the threat model assessment, the architecture design, the deployment, the configuration, the verification, and

the documentation. Call or email to get a quote on system setup for either the budget build or the advanced tier. Scope and location determine the labor figure. Hardware cost is fixed and transparent.

Call for a quote: 713-882-0902 · warren@barr-cyber.com · barr-cyber.com

---

“The only thing cheaper than deploying this stack is explaining to your insurer why you didn’t.”

This is a practical, repeatable, budget-conscious framework for securing high-value assets in unattended environments. Every component is available at major retail without professional installation, long-term contracts, or proprietary lock-in. The total cost is less than a single month of a commercial monitored security system — with more control, more visibility, and more evidence-grade output.
