Security Technology Assessment

Camius Camera Platform Evaluation

Sample anonymized client report for portfolio use

Prepared for: [Client Name]
Location: [Customer Site / Address]
Prepared by: Danny A Cologero, IT & Cybersecurity Consulting
Date: November 16th, 2025

Note: This is an anonymized example of a real client deliverable, shared for portfolio purposes only. It is not sponsored by or affiliated with Camius or any other vendor.

Cover Letter

Dear [Client Name],

Thank you for the opportunity to prepare this security camera assessment for your business location. Your current system is aging and no longer meets your expectations for image quality, reliability, or remote access. This report focuses on Camius as a potential end-to-end replacement for your existing cameras and recorder.

My goal is to help you make an informed, risk-aware decision about upgrading your video surveillance. Modern systems are no longer just cameras on the wall. They touch your network, your privacy obligations, and your long-term operating costs.

This evaluation is independent and vendor neutral. It outlines the strengths, risks, and practical implications of adopting a Camius Network Video Recorder (NVR) and camera solution at your business location. I have included design considerations, security and privacy points, and a five-year cost outlook so you can decide whether this platform fits your needs for remote viewing, long-term reliability, image quality, cost, and privacy.

I appreciate the trust you have placed in me and look forward to reviewing the findings with you and planning next steps together.

Sincerely,

Danny A Cologero

IT & Cybersecurity Consultant

Disclaimer: This report is provided for informational purposes only and does not represent an endorsement or resale recommendation of any product or vendor.

Executive Summary

This report evaluates Camius as a complete replacement for your existing security camera system at [Customer Site]. Camius offers professional-grade Power over Ethernet (PoE) Internet Protocol (IP) and hybrid camera systems that use a local Network Video Recorder (NVR) for recording, with secure remote access through the Camius View mobile app, computer software, and browser clients (Camius software overview).

Unlike fully cloud-managed platforms, Camius stores video on an on-site hard drive in your NVR. Remote access is provided through encrypted connections and peer-to-peer (P2P) methods, while footage remains on your local recorder (How to watch live Camius cameras).

This model aligns well with your priorities:
- Remote viewing and playback from phone and computer using Camius View (Apple App Store, Google Play)
- Strong image quality with 4K and AI-assisted detection options (Camius IP cameras and systems)
- Long-term reliability with local storage and no required cloud subscription (Video Management Software (VMS) Pro / NVR software overview VMS Pro overview)
- A privacy-forward design that keeps recordings on site, not in a third-party cloud (Real Time Streaming Protocol (RTSP) & local streaming article RTSP/local)
- Cost control through one-time hardware purchase and free client software (Software downloads)

Camius is headquartered in California and states that products are professionally assembled and tested in the United States, shipping from their California facility (About Camius). They also market their cameras and recorders as National Defense Authorization Act (NDAA) compliant, meaning they are designed to avoid manufacturers banned under Section 889 of the U.S. National Defense Authorization Act (NDAA) (Camius FAQ; general NDAA camera guide).

Overall finding:

Camius is a strong candidate for your business location if you want a subscription-free system that emphasizes local control, privacy, and high image quality. The main obligations on your side involve treating the NVR as a critical network device: securing passwords, segmenting it on your network, and keeping firmware up to date.

1. Platform Overview

Architecture

Camius systems are built around an on-site recorder model:

- PoE NVR or hybrid DVR: Cameras connect by Ethernet or coax to a recorder that handles video capture, storage, and management (Camius PoE NVR systems).
- Local storage: Video is written to internal hard drives in the recorder, sized for weeks or months of continuous recording.
- Remote access: You access live and recorded video using:
  - Camius View smartphone app (iOS and Android) (Camius View guide)
  - VMS Pro software on Windows or Mac (VMS Pro how-to)
  - A web browser client via the NVR/VMS interface on the local network (Software overview)

Recording continues even if the Internet is down. Remote viewing depends on your Internet connection and the Camius app or software, but the footage itself stays on your recorder.

Key Features

- - Up to 4K video resolution
- - Power over Ethernet (PoE) for simple single-cable runs
- - High NVR bandwidth to support many high-resolution streams
- - AI-assisted analytics such as motion, human, and vehicle detection on supported models
- - 24/7 continuous recording or motion-based recording
- - Free remote viewing apps and PC/Mac software with notifications and remote configuration

Relevance to Your Business Location

- - Reliable coverage for entrances, exits, parking areas, and interior spaces
- - Better image quality for identifying people, vehicles, and events
- - Remote viewing for you and any trusted staff, directly on phones or laptops
- - No dependency on cloud storage or subscriptions for basic operation

Country of Origin, Supply Chain, and Internal Components

From the Camius About Us page, products are “professionally assembled and tested in the United States” and ship from their California facility (About Camius). Camius also states that its IP cameras, NVRs, and DVRs use NDAA-compliant hardware. (Camius NDAA Compliant Products).

For context, NDAA Section 889 prohibits U.S. federal agencies and many federally funded projects from using certain Chinese-manufactured surveillance equipment (Pelco NDAA explainer; CGP Section 889 overview).

Like most electronics manufacturers, Camius does not publicly disclose the country of manufacture for internal components such as:

- - Image sensors
- - System-on-chip (SoC) processors
- - Network chipsets

Camius' NDAA-compliant positioning indicates that it intends to avoid manufacturers named in Section 889, but chip-level country-of-origin details are not published. Because detailed per-component origin data is not available, the recommended approach is:

- - Obtain an NDAA / Section 889 compliance letter for the specific camera and NVR models.
- - Request a brief bill-of-materials statement identifying the main processor and image-sensor vendors and confirming that none are sourced from banned manufacturers.
- - Request a Certificate of Origin for each hardware SKU as part of the final purchasing documentation.

This keeps the supply-chain documentation defensible if questions arise later.

2. Security and Compliance

Strengths

From a security and privacy standpoint, Camius offers:

- Local recording by default: Video is stored on drives inside your recorder rather than streamed into a third-party cloud (Real Time Streaming Protocol (RTSP)/local streaming article RTSP/local streaming article).
- Encrypted remote access: Remote sessions use Transport Layer Security (TLS) with Advanced Encryption Standard (AES) encryption and Secure Remote Password (SRP)-based authentication via the Camius View app and peer-to-peer (P2P) Device ID, so the password stays on the user's device and the NVR stores a verifier rather than the raw password (Camius app security details).
- NDAA-compliant hardware: Cameras and NVRs are positioned as NDAA-compliant, intended to avoid manufacturers identified in Section 889 (Camius FAQ; NDAA explainer).
- US-based support: Technical support and customer service are based in the United States (About Camius).

Privacy and Security Model

Key aspects of Camius' model:

- Cameras and NVRs are reachable only by accounts you configure with passwords you control.
- Security footage remains on your NVR's hard drive instead of going to a vendor cloud by default (RTSP/local storage).

- Peer-to-peer (P2P) connectivity is used for remote convenience, with encrypted sessions and device authentication (How to watch live cameras; Camius View).
- Optional user-controlled backups of recordings can be configured to cloud storage services like Google Drive or Dropbox, but this is opt-in and managed by the customer (cloud backup instructions).

Combined with sensible network design (segmentation, no unnecessary open ports, Virtual Private Network (VPN) or similar), this supports your goal of remote access with strong privacy.

Known Vendor Incidents and IP Camera Risk Landscape

As of November 14, 2025, there are no widely reported, Camius-specific security breaches or mass exposures of live camera feeds in major news outlets, public vulnerability databases, or vendor advisories that attribute a compromise directly to Camius hardware or cloud infrastructure. A search of recent reporting and Common Vulnerabilities and Exposures (CVE) listings shows numerous IP camera issues for other manufacturers, but nothing clearly attributed to Camius itself.

This contrasts with some higher-profile incidents in the broader surveillance industry, for example:

- The Verkada breach in 2021, where attackers gained access to live feeds from over 150,000 cameras in hospitals, schools, prisons, and other facilities by compromising internal admin tools.
- Repeated disclosures of serious vulnerabilities in other camera firmware and cloud stacks (for example, UDP Technology-based firmware used by multiple brands, or third-party peer-to-peer (P2P) software development kit (SDK) issues such as ThroughTek Kalay / Common Vulnerabilities and Exposures (CVE) identifier CVE-2021-28372, affecting millions of devices).

However, the absence of a Camius-named headline should not be treated as proof of superior security. IP cameras as a class remain a high-value target and are frequently misconfigured or left exposed. Recent research by Bitsight's TRACE team found more than 40,000 internet-connected video surveillance devices worldwide (cameras, NVRs, etc.) openly accessible on the internet, many streaming live video with no authentication at all (Bitsight exposed camera research). Malwarebytes and other security vendors have repeatedly documented thousands to tens of thousands of exposed webcams and IP cameras over the last decade, often due to configuration mistakes (Malwarebytes – thousands of private cameras exposed; 2019 webcam exposure study).

Key patterns from that broader research:

- Many devices are reachable over HTTP/RTSP with no password or with default credentials.
- Exposed cameras have been found in private homes, offices, factories, health clinics, places of worship, and other sensitive environments.
- Common root causes include:
  - Default or weak credentials left in place
  - Exposing NVR or camera HTTP/RTSP ports directly to the internet via port-forwarding or Universal Plug and Play (UPnP)
  - Unpatched firmware with known vulnerabilities in shared SDKs or stacks

Camius uses the same fundamental building blocks as other IP camera vendors (Open Network Video Interface Forum (ONVIF), RTSP, web interfaces, P2P connectivity), so it is subject to the same class of risks if installed or maintained improperly.

Consultant's Assessment

From a cybersecurity perspective:

- There are no widely documented, Camius-specific breaches in major public sources at this time.
- The general IP camera threat landscape is noisy and active, with tens of thousands of exposed devices and recurrent vulnerabilities in other brands and third-party SDKs.
- Your actual risk with Camius will be driven less by the brand name and more by how the system is deployed and managed at your business location.

To keep risk low, this project should incorporate at least the following hardening steps:

- - Credential hygiene: Enforce strong, unique admin passwords on the NVR and all cameras, and avoid sharing admin accounts.
- - Network exposure: Do not expose NVR or camera ports directly to the internet (no simple port-forwarding of HTTP/RTSP); prefer VPN or a secure remote-access solution if off-site access beyond the vendor's app is needed.
- - Segmentation: Place cameras and NVR on a dedicated Virtual Local Area Network (VLAN) where possible, with restricted routing to the rest of your network.
- - Patch and lifecycle management: Check for firmware updates from Camius at least quarterly and apply them during maintenance windows; plan for eventual hardware refresh or drive replacement as part of a 5–7-year lifecycle.

If these controls are followed, a Camius deployment at [Customer Site] can meet your requirements for remote access, reliability, and privacy while staying aligned with current camera-security best practices and lessons learned from industry-wide incidents.

3. Integration and Compatibility

Existing Environment

Your current system is an older, outdated security camera solution. For this project, the plan is a full replacement. The old cameras and recorder will be decommissioned. Nothing will be kept in production once the new system is live.

The customer will reuse existing Category 5e (Cat5e) cabling for the new IP cameras, subject to basic validation:

- - Each run within standard Ethernet limits (≤ 100 m / 328 ft).
- - Cable in good condition (no kinks, crushing, or mystery splices).
- - Where practical, runs are tested with a basic cable tester before sign-off; any run that fails continuity or PoE load tests will be remediated or replaced.

Any failed runs will be replaced with new Cat5e or better.

Camius Interoperability

Camius supports:

- Native connection for Camius IP cameras to Camius NVRs.
- Support for third-party IP cameras that are Open Network Video Interface Forum (ONVIF) and/or Real Time Streaming Protocol (RTSP)-compatible on many models (Camius RTSP article; ONVIF/RTSP overview via iSpy).
- VMS Pro PC/Mac software for central monitoring of multiple Camius devices (How to add devices to VMS Pro).

Non-Camius cameras can often be added if they support ONVIF or RTSP and are on the correct network. Enhanced features like AI analytics, PoE power control, and some audio functions may not be fully available for third-party cameras.

Implication for the Customer Site

Because you are doing a rip-and-replace and reusing existing Cat5e cabling, the recommended design is:

- - Standardize on Camius cameras and a Camius NVR for this site.
- - Reuse Cat5e runs that pass testing.
- - Replace any failed or over-length runs.

This simplifies support and ensures all smart features work as designed.

4. Bandwidth and Storage Planning

On-Site Network Load

Camius NVRs support high total throughput across their channels (see product specs on the Camius security systems page (Camius IP camera systems).

For [Customer Site], assuming 8–16 IP cameras in the 4 megapixel (MP) to 4K range:
- Average recording bitrate per camera (H.265, mixed motion): ~2–4 Mbps.
- 8 cameras @ 2 Mbps: ~16 Mbps continuous LAN traffic.
- 16 cameras @ 2 Mbps: ~32 Mbps continuous LAN traffic.

This traffic stays on-site between cameras and NVR and does not consume Internet bandwidth.

Internet Uplink for Remote Viewing

Remote access uses your outbound Internet connection only when you or staff actively view live or recorded video:
- 1 active remote stream: ~2–4 Mbps
- 2–3 simultaneous remote viewers: ~6–12 Mbps

If uplink is limited, remote streams can be throttled or set to lower resolution in the apps/software.

Storage Sizing Example

Rule of thumb for 30 days of continuous recording at 2 Mbps per camera:
- 1 camera → ~0.65 terabytes (TB)
- 8 cameras → ~5 TB

In practice, motion-based recording and variable bitrates reduce this, but budgeting 6–8 TB of NVR storage for 8–12 cameras gives a margin for 30-day retention.

5. Operational Suitability

Advantages for Your Use Case

For a business location that may host events, rentals, or routine operations, a Camius system provides:

- 24/7 coverage of entrances, parking, and interior common spaces.
- High-resolution evidence for incident review and identification.
- Smart detection (human/vehicle) on supported models to reduce noise.
- Remote access for trusted contacts using Camius View and VMS Pro (Camius app guide; VMS playback guide).
- No required subscription fees in order to record and review footage.

Day-to-Day Management

For day-to-day use, Camius is designed so non-technical owners can:
- View cameras and recordings through a straightforward interface.
- Search by time/channel and download clips as needed.
- Receive notifications when motion is detected in defined zones.
- Manage basic NVR functions without deep technical knowledge.

Pairing the technical installation with a short, written operator guide specific to your business location will help ensure smooth daily use.

6. Privacy and Policy Considerations

Even for a single business location, video surveillance can create privacy obligations. With Camius, you already gain a privacy benefit because footage is stored on-site rather than in a vendor cloud (RTSP/local storage article).

For [Customer Site], recommended practices include:
- Signage: Clear notices at entrances indicating that video surveillance is in use.
- Retention policy: Decide how long to keep footage (e.g., 30, 45, 60 days) and configure NVR storage accordingly.
- Access control: Limit who can view live video, review recordings, export clips, and adjust settings.
- Audio considerations: If cameras include microphones, confirm local legal requirements and disable audio where inappropriate.
- Export and sharing: Share incident clips only with law enforcement, insurers, or parties with a legitimate need; keep a simple log.

Even though this is a private installation, documenting these points helps if an incident later involves insurance or legal review.

7. Cost, Licensing and Support

License and Subscription Model

Camius systems are sold as hardware plus free client software:

- You purchase cameras and an NVR/DVR kit.
- Camius View app, VMS Pro, and browser client are provided at no additional license charge (Camius software page).
- There are no required monthly cloud-storage fees to keep recording operational.

This is different from some cloud camera brands that require ongoing licenses simply to retain footage or unlock features.

Warranty and Support

Camius typically offers:

- Limited hardware warranties (length depends on product family).
- Lifetime technical support for registered customers.
- Online manuals, firmware updates, and tutorials via the Camius website and support portal (About Camius; downloads).

Cost Baseline

For [Customer Site], your five-year total cost of ownership (TCO) will primarily consist of:
- Up-front hardware: cameras, NVR, hard drives, any PoE switches and mounting hardware.
- Installation labor: mounting, aiming, wiring, configuration, and testing of existing Cat5e runs.
- Occasional hard-drive replacement during the life of the system.
- Electricity for cameras, switches, and the NVR (plus Uninterruptible Power Supply (UPS) if used).

There are no mandatory license renewals to plan for, but it is wise to budget a small yearly amount for maintenance tasks such as firmware updates, health checks, and configuration reviews.

8. Risk–Benefit Snapshot

Category	Strength	Risk	Mitigation
Security	Local storage, encrypted remote access, NDAA hardware	Misconfigured NVR, weak passwords, exposed ports	Strong passwords, network segmentation, VPN or carefully limited remote access, regular firmware updates
Operations	24/7 recording, high-bandwidth NVR, no cloud reliance	NVR is a single point of failure if drive or unit fails	Use quality drives, consider spare drives, keep NVR on UPS, periodic health checks
Privacy	Footage stays on site, no default cloud storage	Risk if accounts are shared or reused	Limit user accounts, enforce device/app security, revoke access promptly when people leave
Cost	No recurring license fees, free apps and software	Up-front capital cost and occasional drive replacement	Treat hardware as a one-time project cost, set aside small annual maintenance budget
Integration	Reuse of Cat5e cabling, ONVIF/RTSP support	Old or damaged cabling can cause instability	Test and replace failed Cat5e runs, standardize on Camius hardware for this site

9. Recommended Next Steps

1. Site Design and Camera Layout

- Confirm priority areas at [Customer Site]: entrances, exits, parking, interior spaces.
- Design a camera layout that balances coverage, privacy, and cost.
- Select appropriate models (4K for critical views, lower resolution where less detail is required).

2. Network, Cabling, and Power Plan

- Inventory existing Cat5e cabling and test each run.
- Reuse Cat5e runs that pass testing and are within length limits.
- Replace failed or suspect runs with new Cat5e or better.
- Plan PoE switching and NVR location in a locked, ventilated closet with Uninterruptible Power Supply (UPS) power.
- Place cameras and NVR on a dedicated Virtual Local Area Network (VLAN) where possible and restrict direct inbound Internet access.

3. Governance and Privacy Setup

- Define who can log in, from which devices, and at what privilege levels.
- Decide on the default retention period and configure the NVR accordingly.
- Draft a one-page surveillance notice and post signage at entrances.

4. System Commissioning and Documentation

- Complete installation and configuration of all planned cameras and the NVR.
- Verify image quality, coverage, motion-detection tuning, and remote access with you on-site.
- Document final camera positions, naming, retention settings, network details, and cabling status.
- Keep a simple runbook with steps for managing users, passwords, firmware updates, and footage exports.

10. Consultant's Recommendation

From an IT and cybersecurity perspective, Camius is a suitable and practical choice for replacing your current outdated camera system at [Customer Site], given your priorities of remote viewing, long-term reliability, image quality, cost control, and privacy.

Key reasons:

- U.S.-based brand with assembly and testing in the United States and NDAA-compliant positioning (About Camius; FAQ; NDAA background; Camius NDAA Compliant Products).
- Strong alignment with privacy by keeping recordings on your own recorder rather than a vendor cloud, with only optional user-controlled cloud backups (RTSP/local storage; cloud backup guide).
- No required subscription fees to maintain recording and remote access, which keeps long-term costs predictable (NVR/VMS overview).
- Adequate tooling for remote monitoring, AI assistance, and evidence export without overwhelming a non-technical owner (Camius View; VMS Pro guides).
- Ability to reuse existing Cat5e cabling where it passes testing, reducing project cost and disruption.

Recommended path forward:

1. Proceed with a focused design for [Customer Site] using a Camius NVR and Camius cameras as the standard, reusing Cat5e cabling where practical and in good condition.
2. Treat the NVR as critical infrastructure on your network and maintain it accordingly (passwords, updates, UPS, documentation).