

## Security Technology Assessment

### Verkada Camera Platform Evaluation

Sample anonymized client report for portfolio use

Prepared for: [Client Company Name]

Prepared by: Danny A Cologero, IT & Cybersecurity Consulting

Date: October 26, 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 Verkada or Axis.\*

### Cover Letter

Dear [Client Name],

Thank you for the opportunity to prepare this complimentary assessment. My goal with this report is to help your organization make an informed, risk-aware decision about the Verkada camera ecosystem as a foundation for your remote monitoring services. As physical security continues to converge with cybersecurity, I want to ensure any technology you deploy protects both your clients' physical assets and their data integrity.

This evaluation is independent and vendor neutral. It outlines the strengths, potential risks, and operational implications of adopting Verkada for your hybrid security model. I have included actionable recommendations and a pilot roadmap that can help your team test the platform's capabilities before full adoption.

I appreciate the trust placed in me to provide this assessment and I look forward to discussing how we can strengthen your technology offerings 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  [Verkada](#) as a video surveillance platform for your remote monitoring program. Verkada's hybrid cloud architecture, combining onboard camera storage with centralized cloud management, simplifies deployment, lowers infrastructure costs, and enhances operational efficiency. However, as with any cloud centric platform, it introduces dependency on the vendor ecosystem and recurring license costs.


Your company currently uses  [Axis Communications](#) camera equipment, which is widely respected for its reliability, open standards, and broad VMS (Video Management System) interoperability. Verkada represents a shift from that open, customizable model toward a managed, cloud based ecosystem focused on simplicity and automation.

**Overall finding:** Verkada aligns well with a security guard company's transition toward technology enabled remote monitoring. It offers scalable deployment, robust analytics, and strong cybersecurity controls. **The main concerns involve vendor lock in, cost predictability, and ensuring data governance policies are in place for AI driven analytics.**

## 1. Platform Overview


**Architecture:** Hybrid cloud (edge storage + cloud management). Cameras record locally and upload metadata for centralized control. This allows live and historical access without the need for on site servers.

### Key Features:

-  [AI based analytics](#): people, vehicle, and license plate recognition
- Secure remote access via web or mobile Command platform
- End to end encryption (in transit and at rest)
- Automated firmware and software updates
- Role based access controls and MFA (Multi-Factor Authentication)

**Relevance to Your Operations:** Minimal on site infrastructure supports quicker installations, lower maintenance, and scalable multi site management suitable for remote monitoring clients.

## Country of Origin and Manufacturing





**Headquarters:** Verkada Inc. is headquartered in San Mateo, California, United States ( [Wikipedia](#)).

**Manufacturing:** Verkada designs its cameras in the United States. U.S. Customs and Border Protection rulings indicate printed circuit board assemblies for Verkada dome and fisheye cameras are of **Taiwan origin**. TAA (Trade Agreements Act) compliant SKUs are available for regulated environments.

**Implication for Your Operations:** These origins align well with NDAA (National Defense Authorization Act) and TAA compliance requirements, which restrict the use of equipment produced in certain countries. Verkada's manufacturing profile supports procurement within regulated U.S. environments, such as municipal and enterprise security projects. For complete assurance, request a **Certificate of Origin** and **Bill of Materials (BoM)** disclosure from Verkada as part of your vendor due diligence.

## 2. Security & Compliance

### Strengths:

-  [SOC 2 \(Service Organization Control 2\) Type II](#),  [ISO \(International Organization for Standardization\) 27001/27017/27018](#), and **FIPS (Federal Information Processing Standards) validated models available (-F SKUs)**
- Encryption in transit and at rest;  [Enterprise Controlled Encryption \(ECE\)](#) available for key ownership
- **NDAA-compliant across the line; TAA-compliant options available for specific SKUs**
-  [FedRAMP \(Federal Risk and Authorization Management Program\) Moderate In Process](#) / [Verkada Achieves FedRAMP In Process Status at the Moderate Impact Level](#)
- Strong audit logging and MFA enforcement


**Historical Context:** Verkada experienced a breach in March 2021. Media and the FTC (Federal Trade Commission) reported that a hacker obtained access to over 150,000 live cameras across multiple customer environments. [Verkada's incident report](#) states that 97 customers had cameras accessed and video or image data viewed. A [2024 FTC action](#) requires Verkada to maintain an enhanced information security program, undergo third-party assessments for 20 years, and pay a 2.95 million dollar penalty related to CAN-SPAM (Controlling the Assault of Non-Solicited Pornography And Marketing) violations.

**Consultant Note:** This incident underscores the importance of vendor access governance and administrative control segmentation. Clients evaluating Verkada should verify support access policies, confirm encryption key ownership, and implement strict least-privilege principles for all connected cloud services.



**Consultant's Assessment:** From a cybersecurity standpoint, Verkada has matured significantly. However, it is important to enforce MFA organization wide, limit support access, and review cloud data storage policies before deployment.

### 3. Integration & Compatibility

#### Existing Environment:

Your company's current  [Axis based infrastructure](#) uses open standards like ONVIF (Open Network Video Interface Forum) and supports multiple VMS platforms. This architecture provides flexibility and long-term control but requires more maintenance and technical oversight.

#### Verkada Interoperability:

- Primarily closed ecosystem; integrates via  [ONVIF Profile S](#) and RTSP (Real Time Streaming Protocol)
- **RTSP is LAN-only and does not traverse the Verkada cloud. Command Connector requires LAN reachability and specific ports; dynamic NAT or L3 translation is unsupported.**
- Command Connector enables some third party camera ingestion
-  [API \(Application Programming Interface\) support](#) for automation, alerts, and data export

#### Implication:

Verkada's approach trades openness for simplicity. It excels in unified cloud operations but may not integrate seamlessly with existing Axis environments. **This system is best suited for new deployments or clients seeking minimal infrastructure and centralized management.**

## 4. Bandwidth & Storage Planning

- **Idle bandwidth:** ~20–50 Kbps per camera
- **Active streaming:** 300 Kbps–3 Mbps per camera
- **Local retention:** 30–365 days onboard
- **Cloud backup:** 30 days included; optional paid extensions

Cloud backup includes 30 days for most cameras by default, with some compact models offering 15 days by default. Extended cloud retention is available as a paid option.

**Example:** A 24-camera site requires ~1 Mbps steady state uplink and 10–20 Mbps for active monitoring.

## 5. Operational Suitability

### Advantages for Remote Monitoring:

- Rapid deployment (no NVRs (Network Video Recorders) or servers)
- Unified dashboard for multi site management
- Easy incident sharing with time stamped video links
- Built in AI for quick search and threat detection


### Challenges:

- Subscription based model increases long term cost
- Limited third-party VMS integration
- Cloud dependence requires redundant connectivity (LTE (Long-Term Evolution) backup recommended)

## 6. Privacy & Policy Considerations

Facial recognition and “Person of Interest” alerts require clear governance. You should define:

- Who can create and access watchlists
- Data retention timelines
- Signage and consent procedures
- Audit review schedules

Establishing a written **PIA (Privacy Impact Assessment)** and adopting  [Feature Manager](#) controls will align the system with privacy best practices.

## 7. Cost, Licensing & Support

- **License Model:** Per camera, 1, 3, 5, or 10 year terms (includes firmware and support)
- **Warranty:** Up to 10 years
- **Cloud Backup:** Optional tiered pricing
- **Support:** 24/7 technical support, auto firmware updates

**Consultant's Note:** Plan license renewals 60–90 days prior to expiration to prevent service disruption. Include license renewal management in your internal processes.

## 8. Risk–Benefit Snapshot

Category	Strength	Risk	Mitigation
Security	Encryption, MFA, key control, SOC2	Prior breach history	Enable ECE, enforce MFA, conduct quarterly audits
Operations	No NVRs, auto updates	Cloud reliance	Use LTE failover, UPS (Uninterruptible Power Supply) backup
Compliance	NDAA, FIPS, ISO	Privacy and face data concerns	Define retention and signage policies
Cost	Low infrastructure cost	License renewals	Multi year planning
Interoperability	Some ONVIF support	Closed ecosystem	Maintain RTSP and export backups

## 9. Recommended Next Steps

1. **Pilot Program (30–60 days):** Deploy a mixed camera set (indoor, outdoor, PTZ (Pan-Tilt-Zoom), LPR (License Plate Recognition)) to measure performance, bandwidth, and alert accuracy.
2. **Governance Setup:** Establish user access policies, privacy guidelines, and chain of custody procedures for video evidence (in the case of a security incident).
3. **Network Design:** Segment camera VLANs (Virtual Local Area Networks), restrict inbound traffic, and enable outbound only communication to Verkada's cloud.
4. **Cost Modeling:** Build a 5 year Total Cost of Ownership (TCO) and camera monitoring cost analysis comparing Verkada, open VMS alternatives such as Axis, and physical guard services, normalized to the same operational outcomes (identical coverage, hours, and response objectives).
5. **Post Pilot Review:** Evaluate operational efficiency, false alert rate, and operator satisfaction.

## 10. Consultant's Recommendation

Proceed with a controlled pilot to validate Verkada's technical fit and operational value. From a security and compliance standpoint, **Verkada is viable when paired with clear data governance and redundancy planning**. If the pilot confirms reliability and operator satisfaction, it can be scaled confidently.

As a next step, I recommend a **side-by-side operational comparison** between your current camera systems (Axis, etc.) and Verkada to objectively assess maintenance, cost, and monitoring efficiency. This approach will allow you to identify if a hybrid model, leveraging multiple camera solutions, might provide optimal flexibility and performance.

\*Sections detailing commercial engagement phases and consulting terms have been intentionally omitted from this portfolio version.\*