VIDEO GUARD

WHITE PAPER

NETWORK SECURITY & ENCRYPTION MODEL

AES-256 ENCRYPTION + SECURE TUNNELING FOR MUNICIPAL VIDEO DATA TRANSMISSION

VideoGuard's security model is designed around encrypted data transport, authenticated access, segmented trust and continuous system oversight. The objective is straightforward: protect video, metadata, credentials and system communications as they move between edge devices, platform services and authorized users.

SECURITY PRINCIPLES

CONFIDENTIALITY

Limit unauthorized access to data.

INTEGRITY

Protect data from undetected alteration.

AUTHENTICATION

Verify devices, users and services.

AVAILABILITY

Maintain dependable access and operations.

ENCRYPTION

PROTECTING DATA IN TRANSIT AND AT REST

The model separates encryption of stored information from protection of data moving across networks. AES-256 is the stated encryption standard for protected data, while secure tunneling protects communications between VideoGuard edge systems, platform services and authorized endpoints.

AES-256 ENCRYPTION

DATA PROTECTION

Applied to protected data stored at the edge and within platform services, according to the deployment configuration.

SECURE TUNNELING

DATA IN MOTION

Encrypted tunnels protect traffic traversing municipal fiber, wired Ethernet, Wi-Fi, cellular or other supported network paths.

WHAT THE MODEL PROTECTS

- **Video and audio streams**
- **Event metadata and analytics results**
- **User credentials and session traffic**
- **System configuration and commands**
- **Relevant clips, exports and archives**

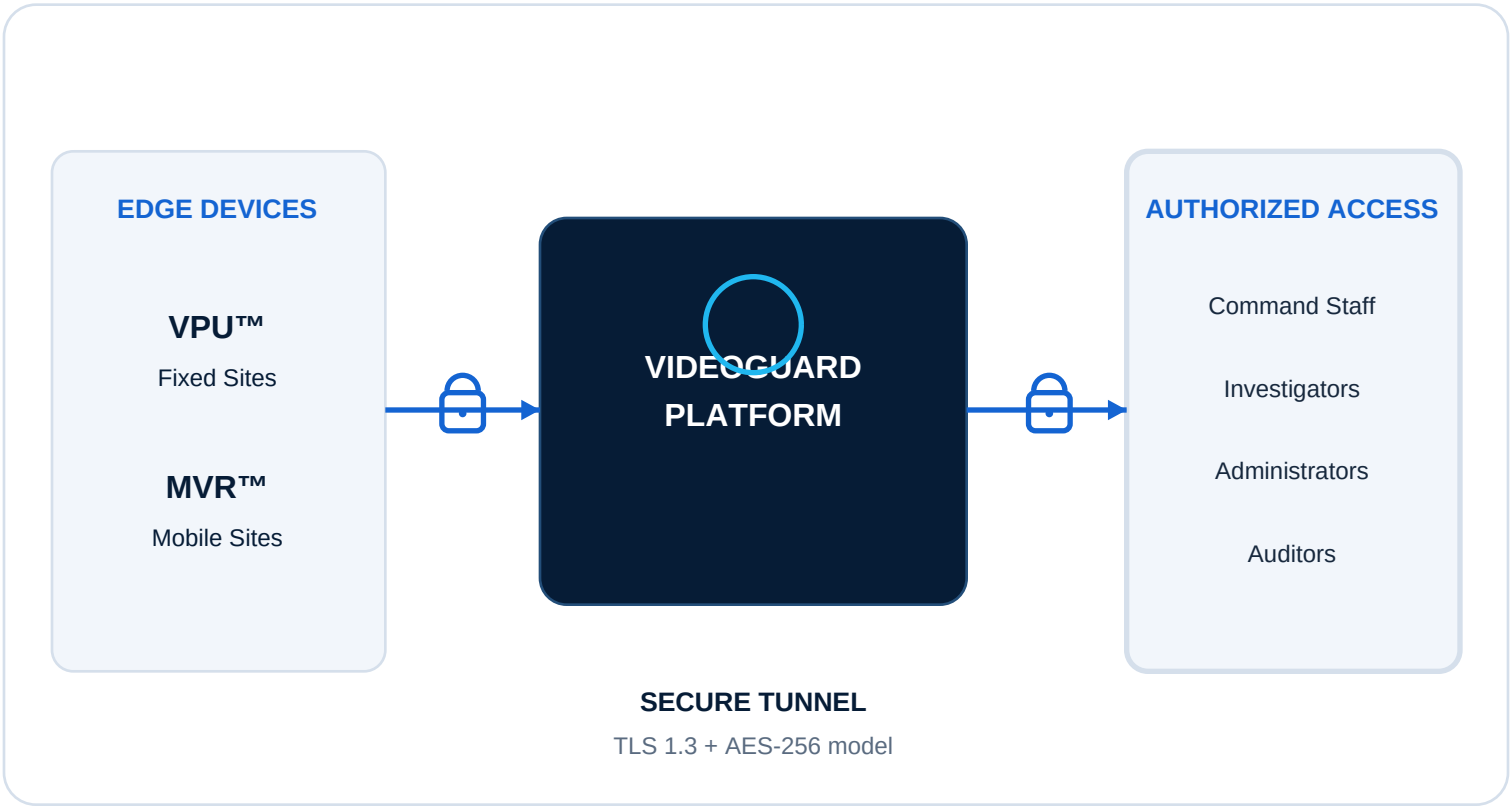
DESIGN PRINCIPLE

Encryption should remain part of the architecture from the edge device through the authorized user's workflow, rather than being treated as a single perimeter control.

ARCHITECTURE

SECURE TUNNEL ARCHITECTURE

VideoGuard's stated model uses encrypted tunnels for communications between edge devices and centralized platform services. Access is then restricted to authenticated, authorized users and administrative roles.



TUNNEL SECURITY FEATURES

TLS 1.3
Encrypted transport

AUTHENTICATION
Verify endpoints

PFS
Limit key exposure

DEVICE IDENTITY
Trust known devices

ENCRYPTED PAYLOADS
Protect transmitted data

HEALTH MONITORING
Maintain visibility

CONTROLS

ZERO-TRUST SECURITY CONTROLS

Encryption is only one layer. The broader model combines identity, least-privilege access, device trust, monitoring and auditability so that network location alone does not establish trust.

01 ZERO-TRUST ARCHITECTURE

Authenticate and continuously validate connections rather than assuming a trusted network.

02 ROLE-BASED ACCESS CONTROL

Grant users only the access needed for their operational responsibilities.

03 MULTI-FACTOR AUTHENTICATION

Add a second verification factor for administrative and remote access where configured.

04 CONTINUOUS MONITORING

Track network, device and user activity for security-relevant changes.

05 AUDITABILITY

Retain security-relevant logs to support review, troubleshooting and investigation.

06 KEY MANAGEMENT

Control key generation, storage, rotation and access as part of system lifecycle management.

STANDARDS & PUBLIC-SECTOR ALIGNMENT

The architecture can be evaluated against applicable agency policy and recognized security frameworks. Relevant references include NIST security controls, NIST zero-trust architecture, FIPS guidance for AES, TLS best practices and FBI CJIS Security Policy requirements where Criminal Justice Information is in scope.

IMPORTANT Final compliance depends on the deployed configuration, agency policy, contracts, access model and operational procedures.

VIDEO GUARD

OPERATIONS

AUDITABILITY, VISIBILITY & OPERATIONAL TRUST

Municipal security systems must remain understandable and manageable after deployment. Security controls should support day-to-day operations, investigation, maintenance and accountability without creating unnecessary friction for authorized personnel.

OPERATIONAL CHECKLIST

- Connection and session logging
- User access and permission changes
- Configuration change visibility
- Security alerts and system events
- Encrypted data transport
- Controlled administrative access
- Device and tunnel health monitoring

SECURE BY DESIGN

ENCRYPTED END TO END

BUILT FOR PUBLIC SAFETY

CONCLUSION

PROTECT THE DATA. PROTECT THE MISSION.

The VideoGuard network security model combines AES-256 encryption, secure tunneling, identity-based access and continuous oversight into a layered architecture intended for municipal and public-safety deployments. The goal is not simply to connect devices - it is to protect the information those devices create and the people who depend on it.

videoguard.ai

SMARTER CITIES. SAFER COMMUNITIES.