

Guide to Evaluating Video Surveillance Systems

A. Video Recording, Storage, Camera Support and Real-Time Monitoring

Today, in light of the costly investments required to maintain video surveillance systems, it has become critical to optimize equipment and resources. Optimizing video storage, adjusting recording settings by schedules, and using new tools that help with real-time monitoring are just a few ways that make it possible to minimize security costs.

Video Recording

Video recorders that offer a range of recording settings ensure that recording will be optimized around the needs of different types of environments. For example, a retail store may want to capture video at a higher resolution, quality, and number of frames per second during business hours when there is more traffic, but lower video recording settings during non-business hours to optimize the use of storage.

Evaluation Criteria

1. Maximum resolution (across all channels)
2. Maximum frames per second (across all channels)
3. Adjustable resolution, quality, and frame rate settings:
 - 3.1. Adjustable by camera
 - 3.2. Adjustable by time schedule
4. Alarm and other event-triggered recording available
 - 4.1. Adjustable by frame rate, resolution and quality on alarm
5. Continuous Recording
 - 5.1. Adjustable by camera
 - 5.2. Adjustable by schedule
6. Motion-based Video Recording Available

Video Storage

Video surveillance systems are often used to conduct investigations and build cases for law enforcement; therefore, the ability to retain and leverage video storage and key evidence can play a major role in the effectiveness of a video surveillance system for a security environment.

For video storage, security professionals may look for the following:

- **Protection against Data Loss**
Security professionals may look for features such as RAID (redundant array of

independent disks) that help protect against the possibility of hard drive failure and loss of evidence.

- **Advanced Compression for Optimized Storage**

Advanced compression methods are often sought after to optimize storage use, but compressed images and video still needs to be high-quality so that evidence can be used for investigations and law enforcement.

- **Long-term Video Storage**

Long-term video storage may be desired but often cost prohibitive with traditional methods of video storage. Some companies offer non-traditional methods to retain video for multiple years without requiring costly investments in additional storage. The methods differ among manufacturers. Some offer basic video pruning in which video frames are dropped over time (without discerning whether activity is taking place) so that at least some video can be retained for multiple years. Other manufacturers may offer more intelligent video pruning methods in which systems save user-defined types of video (e.g. saving only motion and/or alarm-based activity).

Evaluation Criteria

7. Advanced compression methods available (H.264, MPEG4, MJPEG, etc..)
8. Intelligent storage methods
 - 8.1. Ability to store multiple years of evidence without additional purchase of hard drives
 - 8.2. Ability to adjust storage duration
 - 8.3. Ability to store images by event type (e.g. transaction/POS, motion-based, alarm-based etc.)
 - 8.4. Ability to adjust storage duration by event type
9. RAID storage to prevent data loss
 - 9.1. RAID offered as an upgrade or standard feature

Camera Support

With new camera technologies emerging everyday, security professionals will want to consider video surveillance systems that have the ability to support newer options in addition to their current cameras.

The ability to support these options often drives these requirements and benefits:

- **Flexibility**

It is important to many security professionals to have a video system that can support different types of cameras (such as analog, PTZ, IP, and megapixel). Video systems that do not require the purchase of additional encoders or encoders to support both analog and IP is a benefit.

- **Camera Functionality and User Interface**
Diverse camera support ideally should also be accompanied by a complete range of functionalities and consistent user interface across the different types of cameras. For example, one would want to have the ability to configure both analog and IP cameras on a specific channel.
- **Ability to Incorporate New Camera Technologies**
With new technologies constantly emerging, it is important for video systems to have a camera API that allows one to add new types of cameras or camera functionalities and manage and use these new cameras just as easily as older ones.
- **Scalability**
Security managers may want to purchase video systems that are able to support more IP channels beyond the “set” number of channels without purchasing additional video systems (solving the “17th camera problem) or decoders. Some video systems that offer IP camera support can be expanded to meet these future needs.

Evaluation Criteria

10. Existing camera support
 - 10.1. Hybrid (IP and analog) camera support (without encoders or decoders)
 - 10.2. Hybrid and PTZ camera support (without encoders or decoders)
 - 10.3. Hybrid and megapixel support (without encoders or decoders)
11. User interface and functionality consistent across support of all the different types of cameras supported
12. Camera API
 - 12.1. Ability to easily integrate new camera technologies and/or functionalities through a camera API
 - 12.2. Camera API enables user interface and functionality to be consistent across support of all the different types of cameras supported
13. IP expansion
 - 13.1. IP cameras/channels can be added on top of “filled” channels without purchasing additional video systems or decoders
(e.g. If you are using 16 analog cameras in a 16 channel system, 4-8 additional IP channels can be added)

Live Monitoring

Security managers often monitor live video by viewing multiple camera feeds on single or multiple displays. Other features are also being offered by manufacturers to help security managers monitor real-time surveillance more effectively. For example, motion-based

displays can help security managers focus on only areas of activity, and user-defined alerts can alert managers to potential real-time issues.

Evaluation Criteria

14. Multi-camera viewing

- 14.1. Number of cameras displayed in single screen

15. Virtual matrix

16. Simultaneous recording, live viewing, and remote transmission

17. Separate live video (spot monitor) application

- 17.1. Sequencer and multi-camera viewing available
- 17.2. Alerting capabilities

18. Surveillance activity summary display

- 18.1. Text summary of surveillance vs. still image summary of surveillance

19. Adjustable image sizes for enlarged viewing

20. Ability to create and name camera groups

21. Event naming

- 21.1. Open naming fields and canned pick lists

22. Ability to create alerts

- 22.1. For activity in restricted zones (defined by motion grid)
- 22.2. For activity at restricted times
- 22.3. Send alerts including thumbnails via email

B. Investigations

With growing problems in fraud, theft, and other crimes, investigators are often looking for ways to help reduce loss and improve investigative efficiency and effectiveness.

Investigators often use their video surveillance systems to aid with their investigative work, and here are the qualities and objectives they use to measure the value of their video system:

- **Solved Cases and Stopped Losses**
With improved investigation capabilities, organizations can stop recidivist criminals, identify internal theft patterns and prevent costly future losses.
- **Ease of use**
Investigators prefer using applications that have user-friendly user interfaces and other features that make it easier for them to navigate and find what they are searching for. Also, ease of use reduces investigation time, and user errors; as a result, investigators are more efficient with the DVR/NVR.

- **Reduced Investigative Time**
Many security professionals are looking to newer innovations in the security industry to help reduce overall investigative time. These approaches include deploying video analytics such as motion/object analysis, OCR, and facial recognition. Some DVRs/NVRs combine video analytics with searching capabilities so that investigators can very quickly pull the activity they are looking for, without having to watch live video. For example, an investigator can quickly pull all video in Sept 2007 when objects were removed from a specified area.
- **Improved Management of Case Data**
Traditional DVRs force investigators to store case evidence within a DVR itself, PCs or printed out in a file cabinet. Advanced systems can store cases centrally to enable easier access, streamline management, and improve collaboration.
- **Creating robust and comprehensive cases for law enforcement**
Investigators require case evidence that will be accepted by law enforcement. With features such as central case management and facial surveillance search, investigators can construct more comprehensive cases. Facial surveillance searching allows one to search for a suspect across time and locations despite him/her assuming different identities. Also, facial surveillance analysis requires higher quality face images; therefore, higher quality evidence can be submitted to law enforcement.

Investigative Searches and Case Management

Systems that leverage central case management and robust search tools provide better methods of investigating and reviewing evidence.

Evaluation Criteria

23. Ability to conduct correlated searches (e.g. all motion occurring within 2 minutes of transaction event with transaction ID #23245")
24. Thumbnail image display of search results
25. Ability to search by specific data fields
26. Ability to search for events across systems
27. Ability to search and review face images
28. Ability to search a specific face by similarity
 - 28.1. Across systems and locations
29. Ability to search activity within a specific region
30. Ability to search by direction of motion
31. Saved searches
32. Cases stored and managed centrally
33. Case management and investigation tools can be accessed from a single application

- 34. Cases accessible by multiple investigators simultaneously
- 35. Case exporting
 - 35.1. Export to PC, CD, or email
 - 35.2. Video player included with case or files in a universal format that does not required proprietary video player
 - 35.3. Case export in a format that is easily viewable (e.g. HTML and XML) and able to import into other systems for reporting or analysis.
- 36. Video/image retrieval
 - 36.1. Ability to specify types of events shown in real-time
- 37. Ability to import images, and search against imported images
- 38. Ability to verify authenticity of video and events through watermarking method (e.g. SHA-1)
- 39. Time/Date Overlay

Video Analytics and Facial Surveillance

Video analytics can enable investigators to conduct more powerful investigations.

Evaluation Criteria

- 40. Ability to add analytics as software upgrades
- 41. Adding analytics does not require buying additional hardware
- 42. Embedded analytics supported
- 43. Facial Surveillance Analysis Available
- 44. Directional Motion Analysis Available
- 45. Regional Motion Analysis Available
- 46. Object added/removed Analysis Available
- 47. License Plate Recognition Available
- 48. Analytic-triggered alerts
- 49. Search by analytics (outside of alerts)
(e.g. search in a region, or search for a specific person where no alert has been set)
- 50. Analytics used for intelligent storage
(see "Video Storage > Data Longevity")

C. APIs and System Integration

New innovative technologies are quickly appearing on the scene, and it is important that security video systems have the capabilities to extend their technologies in a seamless

manner. Systems with ample processing power and APIs based on standard protocols are integral to supporting 3rd party analytics and integrating with other systems (e.g. POS, teller, ATM, live video etc.) DVRs used in banking should allow users to search transactions on specific cameras and by specific fields (e.g. amount, account, etc.)

External System (non-analytic) Activity API

Evaluation Criteria

- 51. API to integrate data from external, non-video system such as transaction, POS, and access control
 - 51.1. Web standard protocol (e.g. SOAP)
 - 51.2. Supported integration methods (e.g. IP, serial)
- 52. Integration with DVR/NVR's UI and Functionality
 - 52.1. Integrated data events have same functionality as other surveillance activity in system (e.g. date/time/camera/system searching, correlated searching).
 - 52.2. Data events seamlessly integrated into UI
 - 52.3. Data events fields customizable
 - 52.4. Data events stored centrally
 - 52.5. Data events can be stored separately and longer than video
 - 52.6. Ability to search by specific fields and details (e.g. account #, sequence #, transaction type, or other fields)

External Analytic API

Evaluation Criteria

- 53. API to integrate 3rd party software analytics and/or hardware into DVR/NVR or support remote analysis hardware
 - 53.1. Web standard protocol (e.g. SOAP)
- 54. Integration with DVR/NVR's UI and Functionalities
 - 54.1. Integrated data events have same functionality as other surveillance activity in system (e.g. date/time/camera/system searching, correlated searching).
 - 54.2. Data events seamlessly integrated into UI
 - 54.3. Data events fields customizable
 - 54.4. Data events stored centrally
 - 54.5. Data events can be stored separately and longer than video

Event Syndication

Evaluation Criteria

- 55. Ability for 3rd parties receive data from DVR/NVR according to specified criteria
 - 55.1. Use of standard web protocols (e.g. RSS)
 - 55.2. System events are encoded in format for easy parsing, transformation, or rendering (e.g. XML)
 - 55.3. Customize feeds for any set of data and also alerts

D. Enterprise and Systems Management

Enterprise deployments where many video systems are distributed across different locations are becoming prevalent. Thus, the ability to easily manage all of these distributed systems as well as its users is crucial. Features such as central health monitoring and central configuration of systems are important to keeping maintenance costs down, reducing downtime of systems, and increasing administrative efficiencies.

Systems Management

Evaluation Criteria

- 56. Enterprise management of systems (i.e. single sign on ability to manage distributed systems centrally)
- 57. Remote configuration of systems
 - 57.1. Ability to adjust all types of recording settings (such as resolution, quality, fps, motion-based or continuous recording) remotely
 - 57.2. Ability to adjust global camera settings remotely (e.g. frame rates across all cameras)
 - 57.3. Ability to adjust individual camera settings remotely
 - 57.4. Ability to configure storage settings (such as RAID configurations) remotely
- 58. Ability to upgrade “over the wire” for easier hardware and software updates
- 59. Saved configurations in case of system failure
 - 59.1. Automatic backup of individual appliance configurations, enabling quick restoration of settings on a replacement box.
 - 59.2. Number of past configuration versions saved

- 60. Saved system and camera templates available, which can be applied to systems/sites and cameras
- 61. Remote troubleshooting
 - 61.1. Remote reboot available
 - 61.2. Live video check available
 - 61.3. Testing connectivity of servers available

62. NTP Time Synchronization

User and Role Management

Evaluation Criteria

- 63. Ability to centrally manage users and roles across sites/systems
- 64. Ability to remotely manage users and roles
- 65. Ability to create users
 - 65.1. Ability to grant access to specific regions and/or systems
 - 65.2. Ability to assign roles with specific permissions (e.g. creating an investigator role, which allows one with an investigator role to edit cases but not configure system settings)
 - 65.3. Ability to enable automatic password expiration
 - 65.4. Ability to enable automatic password renewal

Health Monitoring

Evaluation Criteria

- 66. Remote health monitoring
- 67. Enterprise health monitoring
- 68. Health alerts available
 - 68.1. Cameras health alerts
 - 68.2. Camera or camera connection failure
 - 68.3. Camera added or removed
 - 68.4. Network connection failure
 - 68.5. System not recording
 - 68.6. Software update needed
 - 68.7. External data not received (e.g. data from transaction system not received)
 - 68.8. Email alerts customizable by type of alert and recipient

- 68.9. Intelligent filtering of nuisance alerts
- 69. Reporting
 - 69.1. Ability to view summary of health alerts
 - 69.2. Ability to run customized report of system issues
 - 69.3. Ability to create and run customized summary of systems' health (to meet end-user's security standards) including system and channel configurations and transaction events being received.

E. Network and Network Security

IT departments evaluating video surveillance systems expect that the DVRs/NVRS won't leave their network and video surveillance vulnerable to attack. They will also endorse DVRs/NVRS that have features that minimize disruption to the company's network.

Network Optimization

Evaluation Criteria

- 70. Bandwidth throttling available
 - 70.1. Minimum throttle level (e.g. 56Kbps) for acceptable real-time monitoring purposes (the lower the better)
- 71. Ability to adapt (still an acceptable real-time monitoring tool) to lowered bandwidth rate by network (not by user) through adaptive frame dropping and/or thumbnail-only transmission
- 72. Bandwidth scheduling available (e.g. the ability to lower bandwidth consumption during business hours when overall network usage is heavier)

Network Security

Evaluation Criteria

- 73. Operating System
 - 73.1. If embedded/proprietary OS
 - 73.1.1. Vulnerability testing completed; types of tools used and standards met
 - 73.1.2. On-board firewall present
 - 73.1.3. Restriction of open ports to only those required to run DVR/NVR
 - 73.2. If standard (Windows XP Professional, Vista, etc.) OS
 - 73.2.1. Process for security updates: DVR-vendor-supplied or OS-vendor-supplied
 - 73.2.2. Types of firewall and anti-virus software approved

74. Applications

- 74.1. Application connections to DVR through proprietary protocol to reduce risk of virus attacks

75. Network Services

- 75.1. Restriction of network applications such as Internet Explorer or Telnet clients
- 75.2. SMTP support limited to sending emails and not receiving emails to minimize vulnerability.

76. Anti-virus Strategy

- 76.1. Explicit signing of all software installed so that sniffing/interception/modifying transmission is not a risk
- 76.2. Antivirus scanning (only applies for standard OS)

F. Hardware

Evaluation Criteria

77. Flexible channel configurations (4-32 channels etc.)

78. Additional encoders/decoders not necessary to support IP and analog cameras.

79. Hard drives

- 79.1. Field replaceable
- 79.2. Hard drives are specifically built for surveillance environments (e.g. for longer storage, more reliable)

80. RAID

81. CD/DVD Rewritable Player

82. Hard-wired inputs for alarm and access events

- 82.1. Number of hard-wired event inputs

83. Warranty for system hardware

84. Warranty for system software