

A MARCH NETWORKS WHITE PAPER

---

# Shadow Archiving in Video Surveillance Systems

Fail Safe Recording Options for IP Edge Devices







# Table of Contents

Executive Summary .....	2
Introduction.....	2
Background .....	2
DVR and Server-Centric Solutions.....	3
Shadow Archive Solution .....	4
Storage at the Edge .....	4
Increased Reliability through Shadow Archiving.....	5
Onboard Storage Capacity .....	6
Retrieving the Shadow Archive.....	6
Conclusions .....	8
Glossary.....	8
About the Authors.....	9
About March Networks .....	9
References .....	9

## Figures and Tables

Figure 1 The Shadow Archive .....	2
Figure 2 Server-Centric Architecture .....	3
Figure 3 Shadow Archive Architecture.....	4
Figure 4 Robust Storage Architecture .....	5
Figure 5 Accessing the Shadow Directory .....	7
Table 1 Standard Measures for Protecting Video Systems versus Shadow Archiving.....	5
Table 2 Storage Capacity of a 32GB SD Card.....	6

## Executive Summary

IP video systems can be vulnerable to interruptions caused by network faults, server failures or power outages, and the cost of mitigating these risks has traditionally been high. Shadow Archiving™ introduces a high level of fault tolerance at an economical cost. Onboard memory in IP cameras and encoders is utilized to provide distributed video redundancy and enable direct client software access, as well as compile a mapped directory on the VMS – the Shadow Archive.

## Introduction

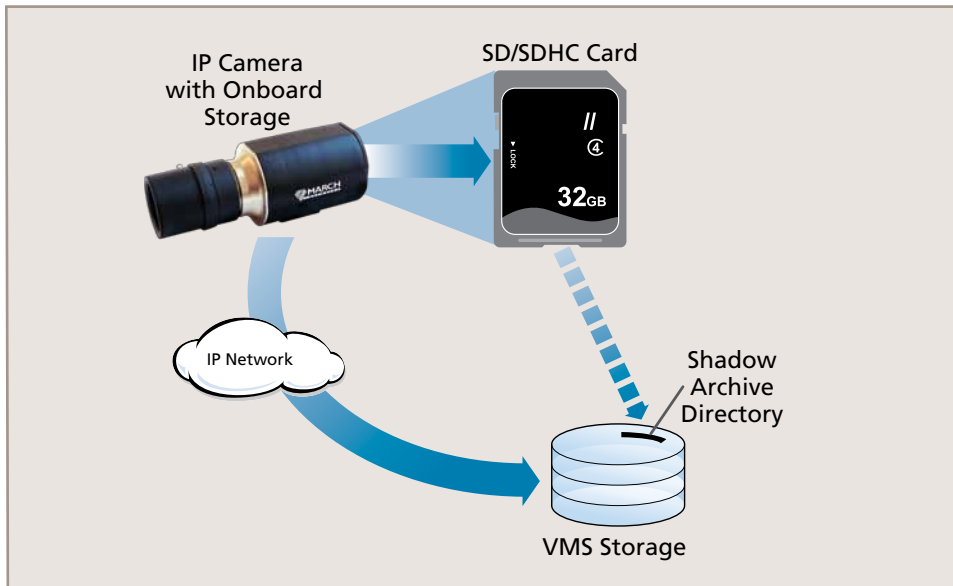
Shadow Archiving is an innovative feature that offers significant benefits to video surveillance systems, and establishes a path for the future development of virtual storage technology.

The Shadow Archive is defined as a directory that maps the video of all onboard edge device storage to a central VMS and is accessible via client software.

That is, it forms a “shadow” on the central VMS archive of all the video data available on IP cameras and encoders with onboard storage and NAS devices.

**The Shadow Archive is defined as a directory that maps the video of all onboard edge device storage to the central VMS and is accessible via the client software.**

**Figure 1** The Shadow Archive



## Background

Several manufacturers have announced IP cameras with a built-in DVR. For the most part, however, these cameras are passive devices that simply have onboard memory. In fact, in some instances the memory is only accessible by manually removing the storage, such as an SD card. Imagine a network outage, or a storage server crash lasting a couple of hours, and then having to physically retrieve the video from 50 or more cameras, some of them in remote locations. The solution is simply impractical. Other camera manufacturers enable access over the network via a web browser interface, and while this may be practical for up to a few cameras, it is hardly a scalable solution. Shadow Archiving eliminates the need to extract video from the cameras manually or to switch to a different software application to retrieve the data.

**Shadow Archiving can automatically synchronize the video stored on the edge device with that of the VMS central storage according to well-defined user policies.**

Newer edge devices enable automatic recovery of any missing video by transferring it to the central storage server once network connectivity is restored. Again, for a few devices, this solution undoubtedly functions well, but with many more devices or longer duration outages, such a solution can significantly increase peak network loading, the very issue that manufacturers are trying to avoid by touting distributed storage at the edge.

The implementation of a Shadow Archive avoids such problems, while still permitting the user to download important video evidence either on demand, or according to user-selectable system policies that effectively control network loading.

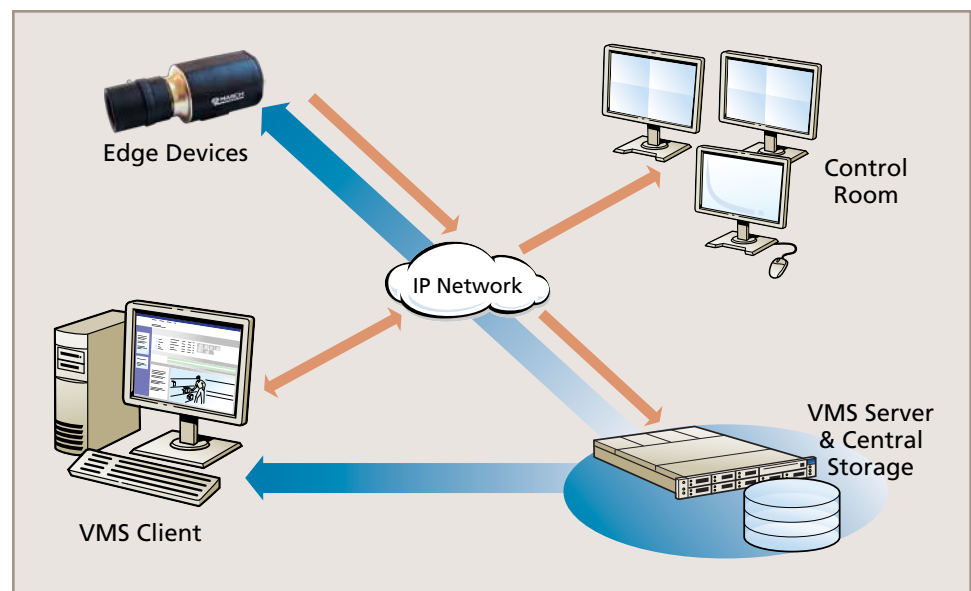
Shadow Archiving can automatically synchronize the video stored on the edge device with that of the VMS central storage according to well-defined user policies. Access to the SD card video is also possible via the central directory. This is the essence of virtual VMS storage.

### DVR and Server-Centric Solutions

Where some leading DVR and hybrid DVR systems have achieved a level of reliability that is unrivalled in the IT sector, server-centric solutions suffer from certain drawbacks. For example, servers tend to be centralized with higher IP camera counts (typically 30 or more cameras on a single server) and, in large systems, even hundreds of cameras route to a central location on multiple servers. Vulnerability to a network outage, server failure or a power outage is therefore significantly increased. DVRs, on the other hand, generally have fewer cameras (usually between 4 and 16) and are deployed in a distributed architecture, such that the risk of a significant failure, and the consequent loss of video, is considerably reduced. Figure 2 illustrates the risk associated with a server-centric solution.

**Figure 2** Server-Centric Architecture

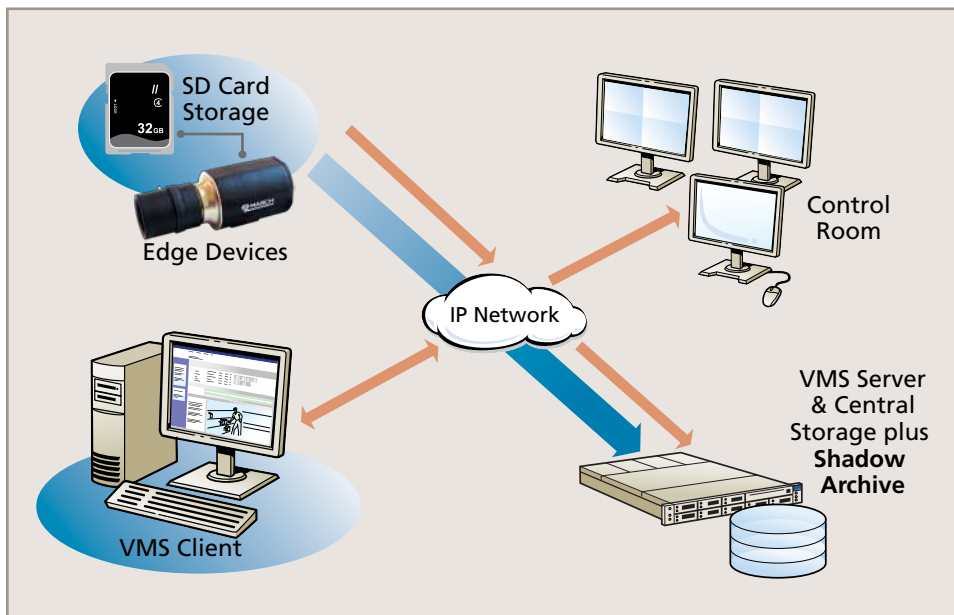
- The server connects to the edge device and requests the video stream
- The VMS records the stream to its local storage
- The server receives a request from the client and streams either live or recorded video
- In the case of a server failure or a network outage, the link between the VMS and edge device is broken and the recording is lost
- With this architecture, server or network redundancy is the only option to ensure that the system keeps recording, which increases cost significantly



## Shadow Archive Solution

Where a server-centric system can potentially suffer from catastrophic failure, the introduction of a Shadow Archive mitigates this risk by distributing a portion of the video storage at the edge. Moreover, Shadow Archive-enabled devices proactively establish contact with the VMS rather than the other way around. As a consequence, the edge device is 'network aware', and essentially operates as a VMS in its own right – **an important distinction from standard edge devices with embedded storage**. See Figure 3.

Figure 3 Shadow Archive Architecture



- Edge devices are equipped with local storage on SD cards
- Edge devices call the VMS and transmit their status
- The central server automatically detects and maps the devices' local storage
- The client connected to the VMS is aware of the current edge device configuration

## Storage at the Edge

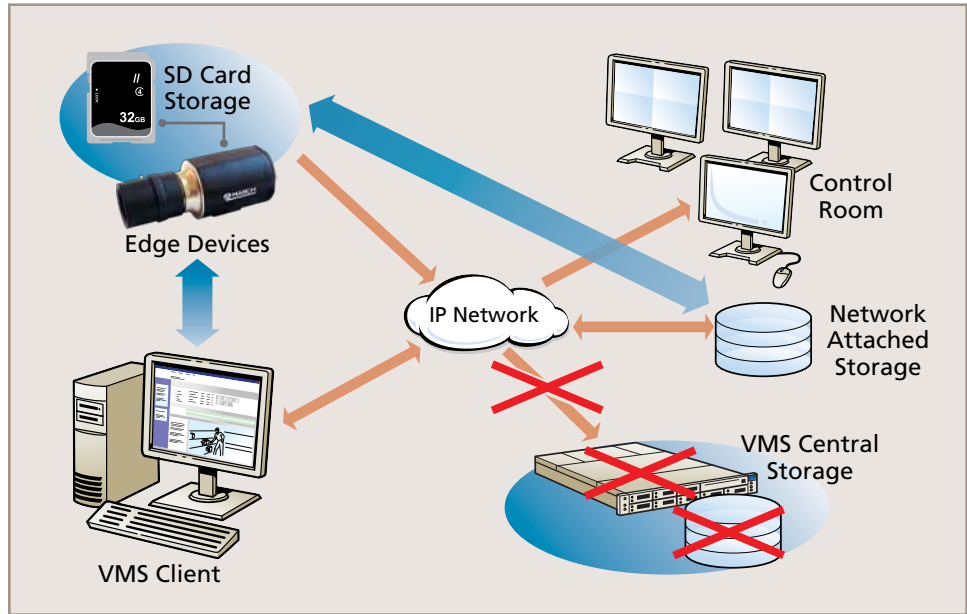
The use of Shadow Archive-enabled devices makes a system particularly robust in the event of a network or server outage. Because of the inherent, standalone capability of such devices, the client software is able to access each edge device independently, not only for live viewing, but also for searching and downloading the video data stored onboard. In addition, video may be streamed to a NAS unit as an alternative storage solution. This differs from server failover because a central VMS is not required, a far simpler method of providing backup storage in the event of longer duration outages. See Figure 4.

In fact, any number of cameras may be connected to a single NAS, offering a cost-effective alternative to numerous SD cards. Further still, the NAS may also be accessed directly via the VMS client software, and performs exactly the same function as the SD card for the purposes of Shadow Archiving. One obvious exception to this solution would be the loss of a network connection to the NAS array, although SD card recording can be triggered in this instance for critical cameras.

Shadow Archiving combined with NAS recording strengthens system redundancy and video access dramatically, and together serve as early indicators of the evolving importance of edge-based IP video architectures.

Figure 4 Robust Storage Architecture

- In case of server failure or a network fault, a direct connection between the client and the edge device is established, allowing transparent access to all the resources even with the server offline
- An alternative network path may be established between the edge device, a NAS unit and the VMS client



### Increased Reliability through Shadow Archiving

There are a number of standard methods used to mitigate the potential loss of critical video evidence in server-centric systems. Shadow Archiving provides a powerful, economical

Table 1 Standard Measures for Protecting Video Systems versus Shadow Archiving

System Problem	Standard Remedy	Cost	Shadow Archiving Solution	Cost
<b>Storage server down</b>	Redundant or failover server	Moderate	Provides storage redundancy and reduces need for redundant or failover servers. NAS units provide a further storage option.	Low to Moderate
<b>Power outage</b>	UPS or generator backup	High	Most edge devices use PoE. Delivering backup power for PoE devices is far less costly to install and distribute.	Low to Moderate
<b>Network outage</b>	Network redundancy or independent video network	High to Very High	Operates independently of the network. Network redundancy can be reduced to a minimum.	Low
<b>Network congestion</b>	Restrict data rates or increase bandwidth	Low to High	Dual streaming from edge devices means high quality onboard recording and optimized bandwidth streaming utilizing available network capacity.	Low

solution.

### Onboard Storage Capacity

So what storage capacity is typically required for Shadow Archiving purposes? The current maximum capacity of SD cards available today at a reasonable cost is 32GB. For continuous, high quality recording with H.264 compression, Table 2 shows approximate storage times on a 32GB card.

**Table 2 Storage Capacity of a 32GB SD Card**

Bit Rate (Mbps)	Storage Time (Hours)	Frame Rate / Resolution Equivalent
8	9	1080p or 2 MP @ 30 fps
4	18	720p or 1 MP @ 30 fps
2	36	720p or 1MP @ 15 fps
1	71	D1 @ 30 fps
0.5	142	D1 @ 15 fps

At medium quality, storage time practically doubles. Therefore edge device recording policies could include such options as:

- High quality, continuous recording
- Alarm or motion recording only
- Reduced frame rate and/or quality when an outage occurs

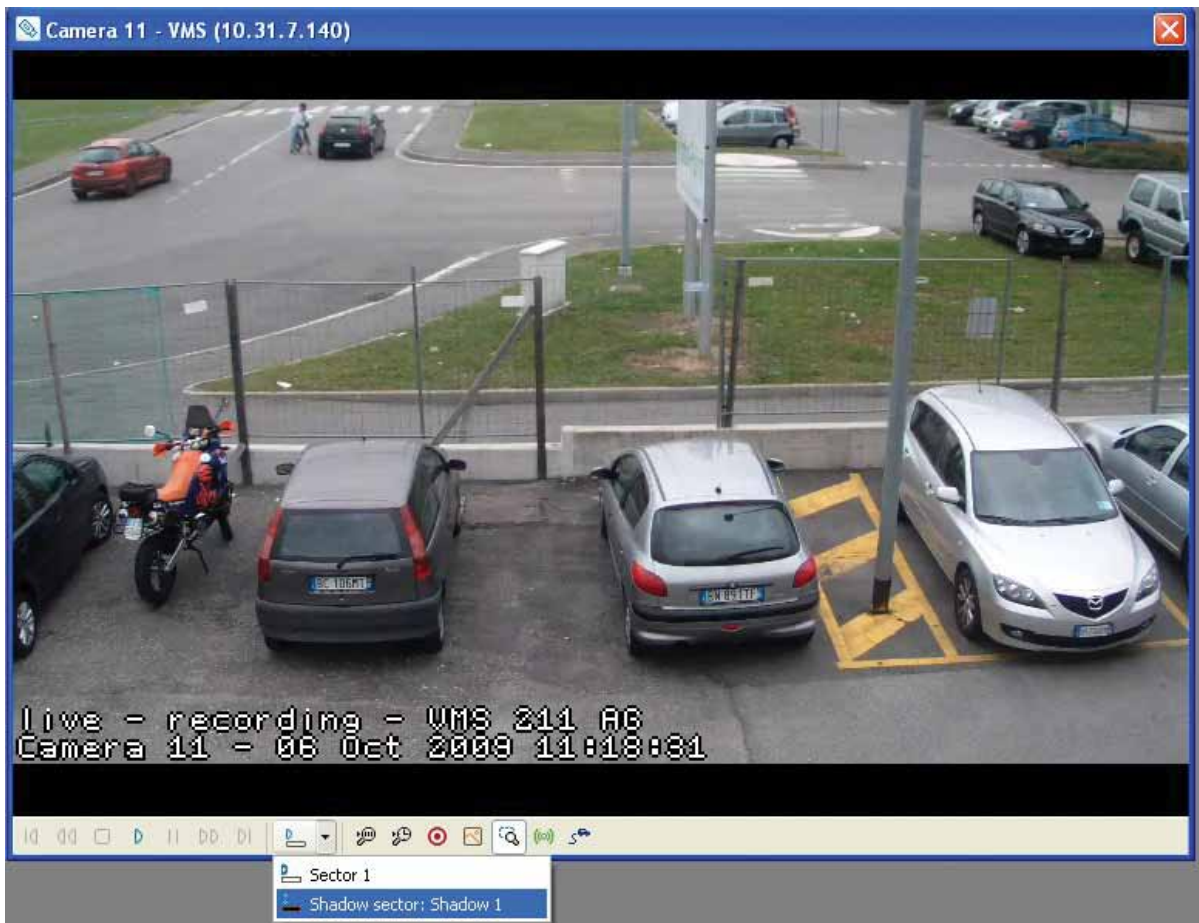
These video retention times will cover most disruptions in service. For example, in North America, carrier network outages of two minutes or more are typically registered for immediate action, and any outage over 30 minutes is considered severe. Of course, many issues can occur on the LAN, which will depend on corporate resources to restore service in a timely manner. Shadow Archiving is not intended in its primary form to replace local or central (long-term) storage devices, although such a concept is easy to envision in the future as flash memory, such as SD cards or micro SD cards, increase in capacity and decrease in cost.

### Retrieving the Shadow Archive

Fast access to the video stored in onboard memory is an important characteristic of Shadow Archiving. In general terms, users should experience little delay in accessing recently recorded video. For short duration outages of less than two minutes, which might occur upon a VMS server reboot or failover for example, the Shadow Archive on the VMS enables normal user access via the client software and the VMS Shadow Directory. A single click opens the edge device's recording window to enable the immediate review or retrieval of the video. If direct NAS recording is used, then it can either backup or be used instead of a central VMS archive.



Figure 5 Accessing the Shadow Directory



In instances of longer duration outages without a VMS, the client software connects directly to the individual devices, from which the video may be viewed live or downloaded. Furthermore, upon restoration of the VMS server, a number of user-selectable policies ensures that network traffic is carefully controlled through automated recovery sequences using intelligent streaming. Such policies include selecting the specific cameras and the time interval, or the option of downloading all video recorded during an outage one camera at a time. The sequence would include a download schedule and automatic insertion of the specified video segments into the main VMS archive, an important feature for compliance with video retention policies that exceed the capacity of the SD cards on the edge devices.

## Conclusions

Shadow Archiving combines the scalability of central archiving with the fault tolerance of distributed archiving. It is an effective and economical method for reliable video backup in server-centric video surveillance systems.

Its key benefits are:

- Network fault tolerance
- Redundant video storage at the edge
- Rapid access to critical video evidence
- Automated video recovery

**Shadow Archiving combines the scalability of central archiving with the fault tolerance of distributed archiving.**

## Glossary

<b>DVR</b>	Digital Video Recorder
<b>NAS</b>	Network Attached Storage
<b>NVR</b>	Networked Video Recorder
<b>PoE</b>	Power over Ethernet
<b>RAID</b>	Redundant Array of Independent Discs
<b>SD</b>	Secure Digital
<b>SDHC</b>	Secure Digital High Capacity
<b>UPS</b>	Uninterrupted Power Supply
<b>VMS</b>	Video Management System



## About the Authors

**Fabrizio Colciago** is March Networks' Chief Technology Officer and Managing Director of operations in Europe, the Middle East and Africa. Combining these two roles, Mr. Colciago guides the company in the evolution of intelligent IP video technology that delivers innovation and practical applications to customers in key markets. Prior to joining March Networks, Mr. Colciago was founder and Chief Executive Officer of Milan-based CIEFFE, a developer of high performance IP video surveillance solutions. Through his leadership, CIEFFE grew to serve an international base of commercial-industrial and government customers and garnered multiple industry accolades. CIEFFE was acquired by March Networks in 2008.

**Philip McDouall** is Director of Solutions Marketing for March Networks, and holds a BSc(Eng) from the Royal Military Academy of Science, U.K. Mr. McDouall spent the early part of his career in signals and communications in the British Army, and then in test and measurement engineering, before moving on to telecommunications. He has worked for March Networks since 2001, authoring a number of papers on video technology. Mr. McDouall is a member of the American Public Transportation Association's CCTV standards committee, helping define video surveillance standards for the transportation industry.

### About March Networks

March Networks® (TSX:MN) is a global provider of intelligent IP video solutions. For close to a decade, the company has helped some of the world's largest commercial and government organizations transition from traditional CCTV to networked video surveillance used for advanced security, loss prevention and risk mitigation. VideoSphere®, the company's enterprise-class video management portfolio, includes open-platform VMS software complemented by high-definition IP cameras, encoders, video analytics and recording platforms, as well as outstanding professional and managed services. March Networks systems are delivered through an extensive distribution and partner network in more than 50 countries.

### References

1. March Networks News Release; *Enhanced Video Access and Redundancy, Key Features of Expanded VideoSphere Solution*; September 21, 2009
2. VideoIQ; *Why Intelligent Storage in Cameras will Transform IP Video Surveillance*; 2009
3. IP Video Market Info; *Should You Use Cameras With Built In Storage?*; June 2009
4. IP Video Market Info; *SD Card's Future for Video Surveillance Storage*; August 2009

Shadow Archiving™ and Shadow Archive™ are trademarks of March Networks Corporation. March Networks has a patent pending on Shadow Archiving technology.

---

North America ————— 1 800 563 5564  
Latin America ————— +1 613 591 8181  
Europe, Middle East and Africa ————— +39 0362 17935  
Asia Pacific ————— +61 1300 089 419  
[www.marchnetworks.com](http://www.marchnetworks.com) PN 060-3053-00-B

March Networks EMEA  
Via Laboratori Autobianchi, 1  
Edificio 23  
20033 Desio - Milano - ITALY  
Phone: +39 0362 17935  
Fax: +39 0362 1793590

March Networks  
Corporate Headquarters  
303 Terry Fox Drive  
Ottawa, Ontario - CANADA K2K 3J1  
Phone: +1 613 591 8181  
Fax: +1 613 591 7337