



Fundamental Problems in Current Digital Video Security Systems, and Boundless' Solution

Executive Summary

Homeland Security relies on visual information. Unfortunately, current digital video surveillance systems are seriously flawed and provide only the illusion of safety. New digital systems often have even more fundamental problems and vulnerabilities than the old analog systems they replace.

Part of the problem with current digital video surveillance systems results from the fact that the video surveillance industry is changing from components, such as digital video recorders and network video recorders, to systems, where network and Internet connectivity are crucial.

Problems and vulnerabilities in current systems include:

- 1) lack of survivability,
- 2) lack of fault-tolerance and redundancy,
- 3) poor reliability,
- 4) low quality recorded images,
- 5) poor Cyber security of the video system,
- 6) interference with corporate networks,
- 7) inadequate storage duration,
- 8) limited access by first-responders,
- 9) video display problems,
- 10) little archival search capability,
- 11) public misconceptions about the capability of current systems,
- 12) lack of government performance standards, and
- 13) overwhelming reliance on hardware that is proprietary to each vendor, resulting in a lack of interoperability, sustainability and third-party applications.

This White Paper describes these basic problems in current systems and a solution, the ***Boundless Security System™***. The ***Boundless Security System™*** is designed so that if its components or network infrastructure are destroyed, its surviving components will continue operating and will continue to provide live and recorded video to first-responders.

The ***Boundless Security System™*** relies on Boundless' proprietary ***Storage Operating System™*** software. The ***Storage Operating System™*** software runs on industry-standard computers and provides all functions, including video capture, recording, distribution, display-formatting and display. The ***Boundless Security System™*** uses standard CCTV cameras for video input, as well as digital, IP network cameras.

Fundamental Problems – and Boundless’ Solution

1) Lack of Survivability

This document uses “survivability” to mean the ability of a system to continue operating, even if it’s with degraded performance, despite one or more massive, system-level failures. We use “fault-tolerance” to mean the ability of a system to maintain virtually full performance despite the failure of a particular component. We use “reliable” to mean every operation is performed perfectly and continuously.

The question is how to maintain vital video surveillance system functions when man or nature interferes. These vital functions include:

- recording video from cameras
- distributing live video to local and distant users
- providing recorded video to local and distant users
- providing motion detection and other image-understanding functions
- controlling cameras
- providing other information, such as audio and events, to local and distant users

The problem is that video surveillance systems are becoming increasingly centralized. This centralization increases the likelihood that a fault, whether accidental or intentional, can disable the entire system. Having a service center nearby does not solve the problem if the facility housing the video security system has been overrun by persons who are intent on destroying the system, blocking access to its information, and preventing its repair.

The dominant video security system architecture (analog CCTV cameras with digital video recorders and an analog video distribution system), as well as the emerging architecture (network cameras and network video recorders), use a centralized architecture. A common command and control room is often used. As a result, the system can easily be disrupted, and access to it blocked, by a single point of failure, not to mention a terrorist or criminal attack.

The reliance on a single component, and the risk of a single-point failure, have grown as technology has advanced from a system where:

1) each analog, time lapse video recorder stores video from a single CCTV camera, thus the failure of one device affects the recording of a single camera, to

2) a multiplexer selects among a small number of CCTV cameras for recording by an analog, time lapse video recorder, thus the failure of a single device affects the recording of a small number of cameras, to

3) a digital video recorder receives video from often 16 but as many as 96 CCTV cameras and records them, thus the failure of a single device affects the recording of, and often networked video access to, as many as 96 cameras, to

4) an analog video matrix switch or controller that distributes and formats live video from hundreds of CCTV cameras to dozens of video displays and digital video recorders, and provides pan-tilt-zoom control of the cameras and interfaces to access control devices, thus the failure of

the video matrix switch can affect the recording, video distribution, display and control of a massive system, to

5) a network video recorder that receives video from hundreds of network cameras and/or network video servers, thus the failure of one device (an ethernet switch, a server that controls storage, or network attached storage) can affect the recording of a large number of cameras.

In contrast, the ***Boundless Security System™*** was architected from the point of view that things go wrong at the worst possible times. The ***Boundless Security System™*** is an “edge-controlled” architecture that has fully distributed control, like a band of guerilla fighters that picks itself up, regroups, and keeps operating when things go wrong.

See www.BoundlessS.com >> **White Papers and Tutorials** >> ***Architecture Comparison***, for a detailed comparison of digital video recorders, network video recorders and the ***Boundless Security System™***.

The ***Boundless Security System™*** automatically and immediately reconfigures itself to handle problems and continue operation. It was specifically designed to keep operating and remain accessible by first-responders even when major parts of the system and its communications infrastructure, a local area network, are destroyed. It reroutes the handling of both live and recorded video when any of its units detect a problem in itself or its communications infrastructure.

2) Lack of Fault-Tolerance and Redundancy

Current video surveillance systems lack the fault-tolerance of common automobile brake systems. In a car, the primary, front and rear brake systems are coupled but operate independently. If the power brake assist fails, one can pump the brakes. If all else fails, one can pull the emergency brake.

A small amount of fault-tolerance is provided in some current video recording systems by having redundant power supplies. Some systems use a redundant array of inexpensive disks (RAID) to protect against the failure of a single disk. If network attached storage is used, fault-tolerance of the control system for the network attached storage is provided in some systems by a server that has spare internal processors.

However, video from cameras must still travel to these storage components, and users must be able to access live and recorded video.

This component-level of fault-tolerance does not address the vulnerability of an entire cluster of processors, or the computer network that provides access to it, being out of commission.

In contrast, control of the ***Boundless Security System™*** is distributed throughout it, rather than being centralized. Each Boundless ***Multi-Stream DVR*** is responsible for correctly recording the multiple streams of video it produces for each camera. Unlike a DVR, where all storage is internal and the DVR only controls itself, each Boundless ***Multi-Stream DVR*** has two independent subsystems, an acquisition subsystem and a record-and-forward subsystem. As a result, recording can either be inside the ***Multi-Stream DVR*** that produces the streams, in other ***Multi-Stream DVR's***, or in other Boundless record-and-forward servers, called ***Multi-Servers***, on the network.

Each Boundless ***Multi-Stream DVR*** verifies that every packet of every IP-video stream it produces is recorded correctly. If a Boundless ***Multi-Stream DVR*** determines that one of its IP-

video streams is not being recorded correctly, regardless of whether it's a problem in the device doing the recording or a network problem, the **Multi-Stream DVR** switches to another recording unit. If the Boundless **Multi-Stream DVR** finds itself cut off from the network, it records all streams internally until the network is restored.

This constant verification in the **Boundless Security System™** has a side benefit – reduced size video files. Unlike other systems that increase the frequency of key frames to compensate for packet loss, it's not necessary for the **Boundless Security System™** to maintain a high rate of “key frames” in the compressed video to compensate for the loss of packets of video data.

Packet loss is a problem in all networks. It occurs in many places – network switches, network interface cards, and in buffers in servers and workstations. Packet loss is severe when throttled and Wi-Fi wireless network segments, and the Internet are used. It's a particular problem when certain Multi-Stream protocols, such as RTP (Real Time Protocol), and multi-casting are used to send compressed video from network cameras and network video servers to users and network video recorders because there's no feedback as to whether or not each packet was received correctly. It's also a problem when video data rates vary widely, such as when constant quality / variable bit rate encoding is used and a lot of motion occurs, producing a spike in data rates.

The **Boundless Security System™** compensates for packet loss by verifying that every packet is handled correctly throughout the entire systems and its communications infrastructure.

In addition, the **Boundless Security System™** provides redundant storage that guards against the total loss of a storage device. The **Boundless Security System™** does this in a way that does not significantly increase the total amount of storage required.

Each Boundless **Multi-Stream DVR** in the **Boundless Security System™** produces multiple IP-video streams for each camera with different resolutions, frame rates, compression parameters and data rates. Each stream can be stored in the same **Multi-Stream DVR** that produced it, in another **Multi-Stream DVR**, or in a Boundless **Multi-Server**, a record-and-forward server. When different IP-video streams for the same camera are stored in different devices, in different physical locations, the destruction or loss of one recording device or its network segment does not impact the use of the remaining units.

3) Poor Reliability

Many digital video recorders and network video recorders lack redundancy. The failure of a single fan, disk drive or network connection can cause system failure.

There are several levels of reliability in digital video surveillance systems. One is whether a device fails because a hard drive or power supply dies, or its software crashes due to an overload or a bug. A less obvious reliability problem is whether all information from the device is transferred correctly to other devices via a network.

The **Boundless Security System™** uses protocols that ensure that all video recording and distribution are performed correctly. Core functions run under the Linux operating system. Linux, unlike other operating systems, enables the size of critical buffers to be optimized.

Another problem in current systems comes from disk fragmentation. Over time, older video files, unless they have been marked for retention, must be erased to make room for new files. The new and old files will undoubtedly be of different sizes, in which case a given file will be written into a number of locations on disk. This reduces the efficiency of disk read and write operations and

reduces the usable data rate. This ultimately causes data loss unless disk optimization software rearranges file placement, but it is difficult for such software to run while the system operates.

The *Boundless Security System™* is specifically optimized to handle large numbers of video files quickly and reliably, at low cost and with low power dissipation. Minimizing power dissipation of the storage system gives it longer life, reduces the burden on the power system, and reduces the burden on the cooling system.

4) Low Quality Recorded Images

Many video recording systems discard most of the visual information produced by high quality CCTV cameras. Many recording systems capture video with only 25% of the camera's resolution and compress each frame too much. These problems occur because the recording systems can't provide the amount of computation and storage required for capturing and recording high quality images.

See www.BoundlessS.com >> [White Papers and Tutorials](#) >> *Recording Systems, Not Cameras, Limit Image Quality in Video Surveillance Systems*, for details.

A consequence of compressing each frame excessively to reduce storage requirements is that blocky and other non-linear artifacts are created when JPEG is used. One can see this effect easily in any image editing program that handles JPEG images and enables you to choose varying amounts of compression. A small amount of compression produces no obvious defects in an image but a relatively large file. A large amount of compression produces many defects in the image, especially near sharp edges, but a relatively small file.

These defects in the image may not be apparent when the image is viewed small, but become objectionable when the image is enlarged – such as to zoom in on subject that occupies a small fraction of the field of view. These non-linear artifacts cause severe problems for police forensic image enhancement software that is intended for the relatively smooth images produced by analog video recorders.

Furthermore, JPEG compression operates on non-overlapping blocks of pixels. There are usually blocks of 8x8 pixels for brightness information and 16x16 pixels for color information, using the argument that the human eye is more sensitive to brightness than color. If excessive compression of each frame is used, it may make a difference where a portion of the image of a subject falls within one of the 8x8 or 16x16 blocks. Thus the clarity of an image depends upon exactly where a portion of an image falls upon the image sensor in the camera, and this position changes as the subject moves with respect to the camera.

Wavelet compression give a smoother image at high compression, but loses details. At high compression, the compressed image has much lower resolution than was digitized. At low compression, JPEG and wavelets give comparable image quality for similar size files.

It is important to note that not all frames and frame rates are created equally when one compares the specifications of digital video recorders. First, there may be one relatively low frame rate for recording and a higher frame rate for presenting video on a video display that is connected directly to a digital video recorder. Second, frame resolutions vary from system to system.

In addition, the rate at which frames are recorded may depend on a number of factors. Factors include the rate at which frames are accessed via a local area network, in which case the total recording rate decreases if too many images are being viewed via the network.

Furthermore, the resolution with which a digital video recorder records is often significantly less than is produced by a high quality CCTV camera. The maximum amount of visual information that can be obtained from the sharpest NTSC camera requires sampling an image at the rate of 704 pixels/line x 480 lines/frame.

Often, however, the specification for a digital video recorder defines a “frame,” image,” or “picture” as having resolution of only 320 or 352 pixels/line x 240 lines/frame. This is only ½ the horizontal resolution and ½ the vertical resolution of a high quality CCTV camera. (For NTSC, resolution of “4CIF” is defined as 704 x 480, and “1CIF” as 352 x 240.) To capture all information, a digital video recorder that has 16 video inputs would need the ability to record 16 cameras x 30 frames/second x 4CIF/frame, which totals 480 x 4CIF images per second, or the equivalent of 1,920 x 1CIF images per second.

In contrast, some common digital video recorders record “up to” 60 frames/second with 1CIF resolution. This is a total of 60 x 1CIF images per second, only enough to capture $60/1,920 = 1/32$, or only 3% of the visual information available from 16 cameras.

Multiplexing often affects the aggregate recording rate. Unless the video cameras are synchronized to each other, which is rarely done, frames are lost each time the video capture hardware switches from one camera to another due to re-synchronizing delays. As a result, the aggregate recording rate drops as the total number of cameras recorded increases.

It is becoming increasingly popular for digital video recorders to provide higher aggregate recording ability to improve the quality of recorded images. However, recording with higher resolution and higher frame rates has a price in terms of increased storage and communications requirements. The critical issue becomes how much storage a digital video recorder can manage.

Many digital video recorders vary the recording rate of each camera according to various criteria, such as motion, to reduce the amount of storage required. The risks are that critical information is missed due to failure of the detection algorithm, and that insufficient compression and storage capacity are available if there is substantial activity on many cameras simultaneously.

Note that digital video recorders usually provide only a single choice of resolution for all cameras, and vary only the frame rate with which each camera is recorded.

Some digital video recorders have one or more sets of internal hardware that combines live video from multiple cameras into one standard definition TV signal. This hardware is similar to that found in some video matrix switches. This hardware enables viewing of multiple cameras on a single screen. The limitations are that all cameras desired for viewing on a given screen must be connected to a given digital video recorder, and the number of viewers who want different sets of cameras must not exceed the number of sets of internal video-formatting hardware.

In contrast, Boundless Security Systems, Inc., recognizes that there are different needs for image quality, storage duration, communications bandwidth, display-formatting and display for investigations, monitoring and first-responders. The ***Boundless Security System™*** solves the problem by simultaneously producing multiple, different IP-video streams for each camera, with different resolutions, frame rates, compression parameters and data rates.

For example, each ***Multi-Stream DVR*** in the ***Boundless Security System™*** can be configured to produce four IP-video streams *simultaneously and continuously for every camera*. All streams are recorded and are available both live and recorded via a local area network. The various streams with 30 frames/second for each camera assist in the formatting of video displays with

images from multiple cameras. The availability of multiple different IP-video streams greatly reduces the CPU burden of the display device to obtain, decode, format and display multiple video streams simultaneously from one or more sites. Typical streams are:

1) for **investigations**: 640x480 resolution @ 5 frames/second with minimal compression for highest clarity and highest data rate, and

2) for **video monitoring**: 320x240 resolution @ 30 frames/second with medium compression and medium data rate, typically used for a quad-display on a TV monitor, and

3) for **video monitoring**: 160x120 resolution @ 30 frames/second with medium compression and medium-low data rate, typically used for a 16-display on a TV monitor, and

4) for **first-responders**: 160x120 resolution @ 10 frames/second with high compression and low data rate, typically used for PDA's and cell phones, or a 64-display on a TV monitor.

In addition, each stream has the IP address of a Boundless record-and-forward server. This server can be co-located within the *Multi-Stream DVR* that produces the stream, can be another *Multi-Stream DVR* on the same or another network, or can be a Boundless *Multi-Server* on the same or another network. These IP addresses can be configured manually or can be controlled by the Boundless *Storage Operating System™* to provide virtually unlimited amounts of disk storage by chaining multiple blocks of storage. As a result of this chaining across multiple storage devices, all disk storage, regardless of where it's located, is treated as a single, seamless pool of storage by the Boundless *Storage Operating System™* when recorded video is accessed.

5) Poor Cyber Security

Video surveillance systems are being tied into computer networks to distribute video within a facility and to provide access to the video via the Internet to corporate personnel, monitoring companies and first-responders. However, access to video from the Internet exposes the computer network to Cyber attack. Many institutions, such as banks, are loath to provide access to video via the Internet for fear of jeopardizing their enterprise data and network security.

Many digital video recorders provide a built-in Web server, an HTTP server, so that one can view images via the network or Internet using a Web browser and Java. The problem occurs when the digital video recorder is on a corporate network because one needs to penetrate the corporate network to access the HTTP server. Furthermore, every digital video recorder acts as an independent HTTP server, hence multiple HTTP servers must be accessed remotely. Another problem is the low performance of Java compared to custom executables and the low frame rates that result.

Many network cameras also function as HTTP servers. Each HTTP server, whether in a network camera or a digital video recorder, requires a hole through a firewall if it is to be accessed from the Internet. This complicates the configuration of the firewall and increases the likelihood that the firewall is configured wrong and the network exposed to Cyber attack.

A Virtual Private Network (VPN) is often used to encrypt sensitive information that is sent via the Internet. However, a VPN does not protect a connection to the Internet from a Denial of Service attack, it complicates the sharing of information with first-responders, and it requires CPU power at the display device to implement.

In contrast, the *Boundless Security System™* is designed with network security and Cyber security in mind. The *Boundless Security System™* implements multiple “network security

zones” that enable first-responders and other authorized users to access live security video without risking Cyber attack of the computer network.

For example, a bank branch could have a pair of firewalls to create a “DMZ” or de-militarized zone. A DMZ is a network segment that can be accessed from the Internet, but which isolates the inner network from the Internet. Each Boundless *Multi-Stream DVR* in the *Boundless Security System™* can be configured to send one or more of its IP-video streams for each camera through the inner firewall to a Boundless record-and-forward server in the DMZ. First-responders, law enforcement and video monitoring companies on the Internet are only able to access live and recorded video streams from the record-and-forward server that is within the DMZ.

Similarly, when there’s only a slow speed connection, such as a cell phone connection, available from a Boundless *Multi-Stream DVR* to the Internet, Boundless’ record-and-forward servers can be located in a web hosting service for the Internet. Such a hosting service provides a very high speed connection to the Internet, providing the digital equivalent of a video distribution amplifier. It also totally isolates the corporate network from remote video access, protecting the corporate network from Denial of Service attacks, corruption of data, and malicious control.

Slow speed communications are not limited to cell phones. DSL and cable modems provide fast download speeds of 1 to 3 Mbps, but typical upload speeds are much lower. In Connecticut, DSL is offered to consumers for about \$35/month. It has an uplink speed of only 128 Kbps and a dynamic IP address. The fastest cell phone networks offer comparable uplink speeds.

Many corporate Intranets provide relatively slow speed connections from each facility to headquarters. Security of the enterprise network is enhanced by the use of dedicated connections within the enterprise, but the connection speed is often limited to reduce cost. A Intranet network segment that operates at 256 Kbps may be perfectly adequate for transferring customer data, but pales compared to the 1 Mbps *or more* per camera that many network cameras require.

DSL is available to businesses for about \$70/month with a 256 Kbps unlink and a static IP address. A static IP address is required by most software that accesses video surveillance systems. A T1 line provides 1.5 Mbps uplinks and downlinks for about \$1,000/month. These are not only prohibitive expenses for many businesses, but even their speeds are still slow compared to video data rates unless video resolutions and frame rates are reduced, and there is a minimum number of simultaneous viewers.

In addition, many Internet Service Providers do not allow consumers to host a web server. This interferes with the use of digital video recorders and network cameras that make video available via an internal HTTP server, unless a non-standard port address for the HTTP server is used.

Boundless’ architecture not only totally isolates the customer network from users, but enables many users to view live and recorded video simultaneously without burdening a slow speed uplink. Live video can be viewed in real time with low data rate while higher quality recorded video is accessed more slowly. The quality of service of the live streams with low data rates is maintained, even when a recorded stream that would normally consume most of the available communications bandwidth is being accessed.

6) Interference with Computer Networks

Carrying many video streams over an ethernet network is enticing because it has the potential for reducing installation costs. It has the potential for acquiring video from cameras, for moving

video to storage devices, and for moving live and recorded video to display devices, as well as via the Internet for remote viewing.

Fiber optic and wireless network segments have the potential for moving video digitally large distances, far greater than can be achieved with analog transmission on coax cables, without any degradation. The use of fiber optic network segments avoids electrical problems caused by power surges from heavy equipment and lightning.

The problem is that computer networks can easily be flooded with security video. The transmission of security video on a corporate network generally has low priority because it is viewed as an expense and interferes with the flow of enterprise data, which produces revenue.

The problem is put into perspective by looking at how much data is required for security video.

A NTSC color camera with 704 pixels/line x 480 visible lines/frame x 29.97 frames/second x 16 bits/pixel produces 168 million bits per second (Mbps) of raw video data. (NTSC cameras produce 16 bits per pixel, not 24, due to their reduced spatial resolution of color information.) This is much more than the 80 Mbps payload of a 100 Mbps network segment. If 10:1 additional compression is provided in a network camera, 17 Mbps/camera must be carried by the network. This amount of compression, using JPEG, produces sharp images with minimal compression artifacts. It is the amount of compression used in many DV (digital video) camcorders.

MPEG-4 compression, unlike JPEG, removes redundancy between frames. As a result, MPEG-4 gives an improvement of 3:1 to 5:1, or more, depending upon the amount of “motion,” or change in the image from one frame to the next. A 4:1 improvement leaves about 4 Mbps/camera to be carried by the network. This amount of data imposes a significant burden on a 10 Mbps network segment, which has about an 8 Mbps payload. A large system with 100 such cameras requires a total of about 400 Mbps of video traffic under these conditions. A significant upgrade to a network may be required to handle so much data. Or, a dedicated network for video may be needed, especially when the highly variable data rate of surveillance video is taken into account.

There are network cameras, or LAN cameras, that have a Wi-Fi network connection instead of a wired network connection. The argument for using such a camera is attractive, that the camera can be located anywhere there's power, without worrying about running a video cable or a network cable to it. However, an 802.11b Wi-Fi connection provides less than 10 Mbps of payload under ideal conditions. No other Wi-Fi devices can be in its vicinity and a short transmission distance is required unless a special antenna is used, to achieve this data rate.

The ***Boundless Security System™*** avoids this network traffic problem by keeping its IP-video streams within its ***Multi-Stream DVR's*** and local network switches. In addition, the ***Boundless Security System™*** provides multiple IP-video streams per camera, with different resolutions, frame rates and data rates, so only those video streams, with the lowest data rates, that one desires to view at any particular time are distributed via the network. This reduces the data rate required to view live video at 30 frames/second by 75% to 90%.

Furthermore, each ***Multi-Stream DVR*** in the ***Boundless Security System™*** buffers its IP-video streams to handle throttled network segments, and congested and lossy, Wi-Fi network segments. This buffering avoids data loss due to transient network and server overloads.

MPEG-4 supports several ways to encode video. The use of Constant Bit Rate (CBR), or variable quality, encoding attempts to maintain a particular data rate regardless of visual content. The advantage is that the amount of communications bandwidth, storage required and CPU

encode and decode requirements are predictable based on the target data rate. The problem is that sharpness of the image is sacrificed to maintain a given data rate. The use of Variable Bit Rate (VBR), or constant quality, encoding attempts to maintain a specific image quality regardless of data rate required. The advantage is that image clarity is maintained regardless of “motion” or changes in the images. The problem is that the amount of communications bandwidth, storage required, and CPU requirements to encode and decode the video are variable.

The ***Boundless Security System™*** supports both constant bit rate and variable bit rate methods of encoding, as well as others. Each IP-video stream for each camera can be selected to have a method of encoding that best suits the needs of a given application. Video is encoded in the native MPEG-4 format, not as H.26x that is embedded in a MPEG-4 envelope.

See www.BoundlessS.com >> [White Papers and Tutorials](#) >> *Generations of Video Security Systems*, for details.

7) Insufficient Storage

Current digital video security systems sacrifice image quality, number of cameras recorded, and storage duration for storage capacity. Systems integrators often require the vendors of digital video surveillance systems to take responsibility for the amount of storage bid on a project to hold the vendor liable if the system fails to meet requirements for storage duration.

Vast storage capacity is required. Large-scale video security systems must be able to digitize, record, manage, search, display, and provide local and remote access to a vast amount of video.

Boundless Security Systems, Inc., has developed a simple tool, the “**Rule of Ones™: 1 x 1 x 1 = 1,**” to estimate video storage requirements. When:

- one** video camera is recorded continuously at
- one** million bits/second (1 Mbps, only 1/6th the data rate of a motion picture DVD), for
- one**-quarter of a year, nearly
- one** terabyte of storage is required.

Continuously recording 1,000 cameras under these conditions requires a staggering one petabyte (1,000 terabytes or 1 million gigabytes) of disk space for every three months’ recording.

Note: This calculation is independent of the type of compression used. It is simply a statement of the amount of data produced over a given period of time for a particular data rate.

It is easy to count the number of cameras, the number of days, and the amount of storage. It is hard to estimate data rates because data rates depend on many factors such as the amount of motion, and the complexity and brightness of a scene.

A single digital video recorder that records 32 cameras continuously at 6 Mbps/camera would fill 1 TB in less than ½ day. Thus such a digital video recorder with a seemingly large, 4 TB of storage would have only have enough storage for 2 days under these conditions.

A facility that records 500 cameras continuously with a lower frame rate to achieve a data rate of 2 Mbps/camera would require 1,000 TB of storage for 3 months’ recording. In contrast, the largest network attached storage devices have a capacity of only about 150 TB.

The ***Boundless Security System™*** uses Boundless’ ***Storage Operating System™*** to manage large amounts of storage, and provide survivability and fault-tolerance. It is designed to store

video from many cameras for long periods of time. In contrast, common digital video recorders usually have only a few hundred gigabytes of storage, limiting image quality and storage duration. Boundless' **Storage Operating System™** software requires no special hardware. It pools all storage in Boundless' **Multi-Stream DVR's** and **Multi-Servers** within a given computer network up to a total of 1+ petabyte (1 million gigabytes), or in a national network up to a total of 1+ exabyte (one billion gigabytes), for use by the **Boundless Security System™**.

Massive amounts of storage are required to fulfill Transportation Security Administration (TSA) needs for three years' video storage. The **Boundless Security System™** enables storage to be repaired and expanded while the system operates, avoiding system down-time. Boundless' **Multi-Servers**, record and forward servers, have been specifically designed for video, reducing power dissipation, size and cost. Many terabytes of storage for each Boundless **Multi-Server** can be provided if desired by using the Linux-based **Multi-Server** to host a storage area network.

Furthermore, if a Boundless **Multi-Server**, or its network segment, fails, or the **Multi-Server's** storage is full, every Boundless **Multi-Stream DVR** sending data to it detects the problem within seconds. Each affected **Multi-Stream DVR** redirects its video to an alternate **Multi-Server**, which may be co-located within the **Multi-Stream DVR**, and resends the video that was briefly lost. The display of live video resumes using the new **Multi-Server**. Error reports are sent by every affected **Multi-Stream DVR** and by every display unit that was accessing live or recorded video.

8) Limited Access by First-Responders

One lesson of the 9-11 Commission Report is that first-responders need better access to critical information. First-responders need to assess situations, prepare themselves, and obtain adequate resources to save victims' lives as well as their own. Likewise, police forces need information to assess situations and prepare themselves to eliminate the attackers.

The idea of providing images on image-enabled cell phones and PDA's is well-established. Yet current surveillance systems provide limited access to video to distant personnel because that access usually exposes computer networks to Cyber attacks.

The **Boundless Security System™** simultaneously provides multiple different digital IP-video streams for each camera to meet the competing image quality, storage, communications, display-formatting and display needs for investigations, monitoring and first-responders.

Video from the **Boundless Security System™** can be viewed on handheld devices without any special software. Only a web mini-browser and Java are required. See the section on Cyber security for a description of the ways the **Boundless Security System™** sends video and other information to the Internet that protect computer networks from Cyber attacks.

9) Video Display Problems

Current digital video security systems have limited ability to present live and recorded video, with high resolution, frame rate, and clarity, from multiple cameras on multiple networks, simultaneously, on a given video display. Not only is a switch that can choose any number and any combination of video streams to present on any given video monitor required, but those multiple video streams must scaled and combined into a single video signal for viewing.

Video surveillance systems that distribute live analog video via video matrix switches use dedicated hardware – video processors – to scale and combine multiple video signals into one for display on standard definition TV monitors. No capability is available in current analog systems

to combine multiple video signals into a format for display on a HDTV monitor, which has sufficient resolution to display six standard definition video signals, each with full resolution, simultaneously.

Digital video surveillance systems, whether they use digital video recorders or network video recorders, have limited ability to display multiple high resolution, high frame rate, digital video signals on a PC video display or TV video display. The reason is that it takes a large amount of CPU power to obtain, decode, scale and display video. A notebook computer can display video from a DVD, and perform other tasks as well, only because compressed video flows from the DVD player to a video graphics chip, that decodes, scales and displays a single video stream.

To put the problem of displaying digital video in perspective, experiments performed by Boundless Security Systems, Inc., show that it takes much of the performance of a 2 GHz Intel Celeron processor to obtain, decode and display one MPEG-4 video stream with full resolution, full frame rate and high clarity. If one wants to see four video signals simultaneously in a quad-display, each stream must also be scaled down. The equivalent of a 10 GHz Celeron processor would be required – an impractical solution.

The ***Boundless Security System™*** solves this problem by providing multiple IP-video streams per camera simultaneously, with different resolutions, frame rates and data rates. Each stream is scaled in a Boundless ***Multi-Stream DVR*** directly from the raw video data, avoiding artifacts that would occur if compressed video were scaled. Each stream is then compressed to MPEG-4.

As a result of the pre-scaling, an inexpensive, 2.2 GHz Intel Celeron processor in a notebook computer has sufficient processing power to obtain, decode and display more than six, MPEG-4, medium-resolution, “monitoring” streams, each at 30 frames/second, simultaneously.

The ***Boundless Security System™*** thus has the ability to reduce the CPU burden to obtain, decode and display video by more than 80%. This provides economical display-formatting and display-driving capability using only standard computer hardware. Boundless’ software is multi-threaded to run on multi-processor machines to drive HDTV displays at full 1080i (1920 pixels/line x 1080 lines) resolution. All video is distributed via an inexpensive local area network; no dedicated cabling or equipment is required.

Boundless’ unique combination of its ***virtual video processor*** at every display device for multi-camera display formatting, and its ***virtual video matrix switch***, provides **universal access** to live and recorded video simultaneously. Each video monitor can display any combination of live and recorded video, from multiple cameras, with multiple resolutions and frame rates, from multiple Boundless record-and-forward servers, on multiple networks, simultaneously.

10) Limited Archival Search Capability

Large amounts of economical, dense, reliable storage with low power dissipation are not sufficient. One must also be able to instantly access any point in the recorded data and quickly search for suspects who may be planning a future attack or participating in a current one.

Current image understanding software generally operates only on raw video. It’s impractical to store raw video for long periods of time due to the massive amount of data required. As a result, recorded video cannot be searched for new content. Currently, the video can be searched only for events that were originally detected. This reduces the utility of recording video for long periods of time.

The ***Boundless Security System™*** provides high quality recorded video and economically stores it for long periods of time. The ***Boundless Security System™*** is an open platform using x86 processors. It is designed for the development of image understanding software by third parties, and for executing image understanding software in parallel on multiple machines to rapidly search vast archives of video.

11) Public Misconceptions

A popular misconception is that cameras are the cause of poor recorded images. The reality is that the #1 cause of poor recorded images is the recording systems, not the cameras. The reason is that many recording systems throw away most of the image quality produced by high quality CCTV cameras. Most recording systems capture video with too low resolution, usually only 25% of the resolution provided by CCTV cameras, and then compress each frame excessively.

Please see www.BoundlessS.com >> **White Papers and Tutorials** >> *Recording Systems, Not Cameras, Limit Image Quality in Video Surveillance Systems*, for details.

Another misconception comes from misleading TV crime-fighting programs that show unrealistic ability to digitally zoom in on a video image to read a license plate or get a sharp image of a suspect.

Furthermore, non-linear artifacts from current digital video recorders cause severe problems for police forensic image enhancement software that is intended for the relatively smooth images produced by analog video recorders.

12) Lack of Performance Standards

The performance of video surveillance systems is subject to many factors. Factors include model of camera, scene background, motion, lighting, physical stability, camera noise in low-light, and the number of users accessing video. However, there are no federal performance tests or standards for video surveillance systems. In contrast, the USAF produced a resolution test chart for still cameras in the early 1950's, and it remains the standard today for still cameras.

Ideally, one would like a repeatable video source that provides raw video data to avoid compression artifacts from the use of MPEG-2 compressed video from DVD's. This is not practical due to the large amount of data and large data rates required. However, Boundless Security Systems, Inc., found that common motion picture DVD's and even inexpensive DVD players provide reasonably high quality analog video that can be used for testing.

Boundless Security Systems, Inc., uses a number of common motion pictures DVD's that have scenes and scanning methods that stress the ***Boundless Security System™***. A variety of motion pictures is used to get some that were photographed with progressive scan and some that were photographed with interlaced scan.

These DVD's can be used to perform repeatable testing of systems. This testing can be performed when new systems are introduced, as well as when system software is modified.

Boundless Security Systems, Inc., believes that the video security industry needs a suite of video surveillance test scenes from a third-party certification organization to run repeatable qualification tests and regression tests, and to compare systems from multiple vendors.

13) Lack of Interoperability

Today, every vendor's digital video recorders are different. There's a multitude of vendors, compounding the problem. Expanding and maintaining video security systems over time is difficult or impossible as models become obsolete quickly. Software that controls, or accesses video from, one vendor's family of digital video recorders generally can't operate another vendor's digital video recorders.

The problem today in the video surveillance industry is far worse than the problem in the mini-computer industry 25 years ago. Then, a relatively small number of computer manufacturers such as Data General, Digital Equipment Corporation, Prime Computer, and Varian, tried to lock customers into their proprietary hardware, software and service. Often, a customer risked voiding the computer's warranty by installing an interface board that came from another vendor.

It took IBM, Intel and Microsoft to develop the Personal Computer, which promoted interoperability of software and hardware.

Boundless Security Systems, Inc., uses the lesson of the Personal Computer Industry. The ***Boundless Security System™*** uses only industry standard computers for the *entire system* – video capture, recording, distribution, display-formatting and display – to assure a continuing source of supply for all components. The ***Boundless Security System™*** uses standard, new or existing, CCTV cameras as video sources.

Currently, network cameras and network video recorders promote a degree of interoperability, but at the expense of high network traffic when video resolution and frame rates are high. Unless a dedicated network is used for video, network video recorders may be best-suited for applications where a few frames per second per camera, at moderate resolution, are adequate, and thus a minimum amount of network traffic is created.

14) Lack of Applications

The lack of interoperability, and the use of closed computing platforms for digital video recorders, results in a lack of third-party software that runs on, or interacts with, digital video security systems.

Image understanding, such as face recognition, reading of license plates, and object identification and tracking, currently requires expensive proprietary platforms. Most of the image understanding is limited to operation on live video, not on archives of recorded video. This is due in large part to problems using compressed video rather than raw video.

The ***Boundless Security System™*** uses an industry-standard, x86 computing platform throughout. The ***Boundless Security System™*** has been designed as a platform for third-party software to facilitate operations on both live and recorded video. Its “investigations” IP-video streams are compressed with very high quality, minimizing the artifacts seen in other systems and facilitating image understanding on recorded video.

The Boundless ***Storage Operating System™*** in the ***Boundless Security System™*** can build massive video data bases (exabyte – a billion gigabytes) to handle high quality video from large numbers of cameras over long periods of time, and to enable it to be searched quickly by third-party software.

The ***Boundless Security System™*** unconditionally records all video, ensuring that no information is missed. Rather than having software that detects a particular event in real time and

only records that segment of video, unconditional recording enables one to search the same recorded video multiple times with different algorithms and different search criteria.

The ***Boundless Security System™*** enables live and recorded video to be embedded in third-party applications. Boundless' ***Video Player*** software is multi-threaded so that many instances, each handling a single video stream, can run efficiently concurrently on a given machine. The ***Video Player*** can be invoked by third-party software multiple times. Each instance selects and places a single video stream on a screen with a programmable size and location.

The Boundless ***Multi-Stream DVR, Multi-Server*** and ***Display Server*** can be packaged in a wide variety of industry-standard housings, such as book-PC, mini-PC, desktop, tower and rack-mount cases. Units that handle extremes of environmental conditions can be provided. The same core, Boundless software is used in all units, assuring compatibility and the interchange of information.

Conclusion

Homeland Security relies on visual information. Unfortunately, current digital video surveillance systems are seriously flawed and provide only the illusion of safety. New digital systems often have even more fundamental problems and vulnerabilities than old analog systems they replace.

The ***Boundless Security System™ with Boundless' Storage Operating System™*** from Boundless Security Systems, Inc., in Monroe, CT, uniquely satisfies these diverse and difficult requirements. It is a fault-tolerant, redundant, fully networked, enterprise-class, digital video security system. It has been architected specifically to satisfy the difficult needs of large-scale, enterprise-class, video security systems. It simultaneously satisfies the competing imaging needs for image quality, storage, communications, and display for investigations, monitoring, and emergency response. It provides the utmost image quality, survivability, capacity, accessibility and Cyber security. Its non-proprietary hardware avoids sole-source supply, maintenance and expansion problems, and enables local content to be used overseas.

###