WHITE PAPER:

Top 5 Reasons Intelligent Surveillance Appliances Outperform General-Purpose Servers

razberi technologies

According to analysts at IHS Technology, by 2017 video surveillance cameras around the globe will create 859 petabytes of data each day.[1] As the march to IP surveillance continues, security and IT leaders need to work together to intelligently plan their surveillance and network strategy. What if you could reduce IP surveillance data impact on your network by up to 95% without compromising on megapixel quality? Read on.

We're at a crossroads in the surveillance industry. As megapixel cameras that deliver quality beyond high definition go mainstream, the opportunity to provide indisputable evidence with exceptional video quality must be embraced. But high-quality video also has the complicating effect of taxing IP networks like never before.

Streaming megapixel video can bring a network to its knees or require an organization to compromise in quality – neither of which is an acceptable option. And though IP video surveillance is here to stay, security and IT leaders critically have to consider the implications of cybersecurity exposures when network ports for cameras are extended into exposed areas – outside of buildings or down hallways.

Herein lies the meshing of the surveillance and security world with the IP world, requiring a new generation of intelligent technology that's built to overcome the challenges in both the near term and the long run.

This white paper addresses these issues and explains why intelligent network appliances that are purpose-built for video surveillance outperform general-purpose IT servers and systems in today's surveillance environments.

What Is an Intelligent Surveillance Appliance?

An intelligent surveillance appliance is designed and built specifically to capture high-quality megapixel video on surveillance-class hard disk drives (HDDs). It uses Power over Ethernet (PoE) that is right-sized for cameras, processors and operating systems specifically intended to support video processing. It's also typically co-located closer to cameras than a centralized server. A hub-and-spoke connection point for multiple cameras makes an intelligent surveillance appliance more scalable than a 1:1 IP address-to-camera implementation. In fact, numerous cameras can be connected to one appliance, and in an enterprise with thousands of cameras, this scalability is of paramount importance.

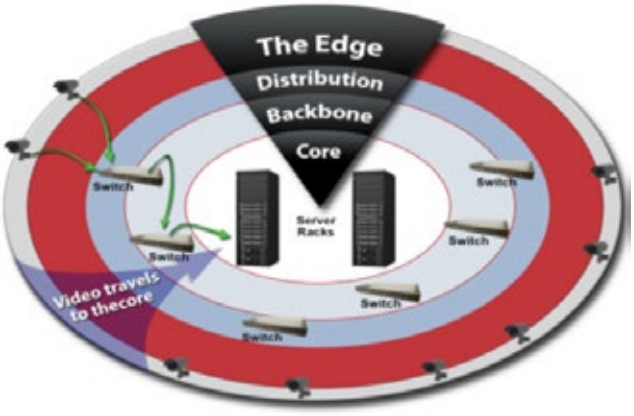
1 Top Video Surveillance Trends for 2015, IHS Technology, 2015

The following are the 5 key reasons that intelligent surveillance appliances outperform general-purpose servers and storage:

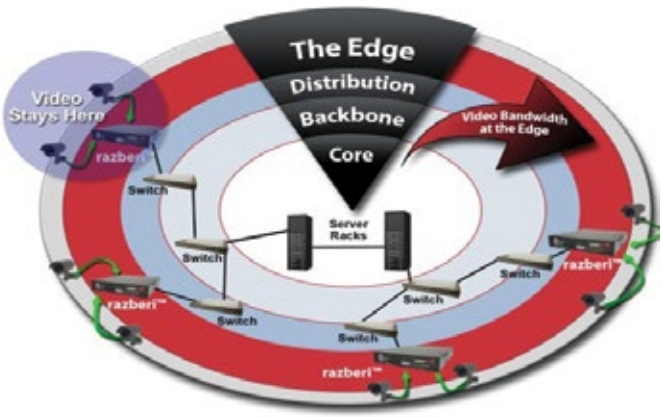
#1 Up to 95% Reduction in Video Surveillance Impact on IP Networks

That's quite a bold claim – and one of the most compelling reasons to consider an intelligent surveillance appliance and distributed architecture over a centralized, general-purpose IT system for streaming video.

In a distributed architecture, appliances record closer to the source, near the cameras. Video only streams over the network when it is retrieved on-demand or in the event of an incident.



Centralized general purpose architecture – all video streams back to central point:

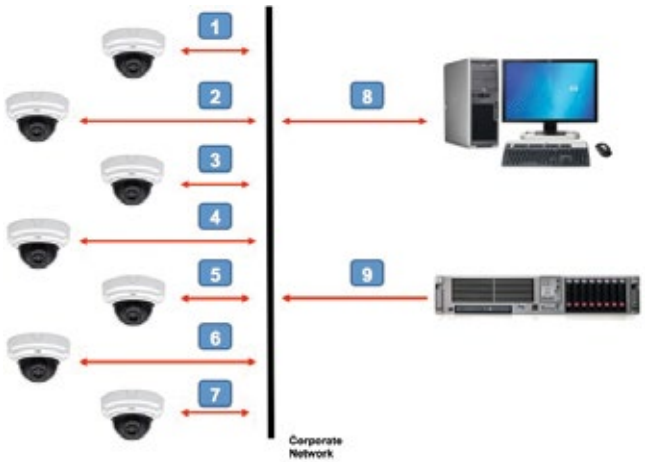


Distributed appliance architecture – video stays closer to the perimeter until requested:

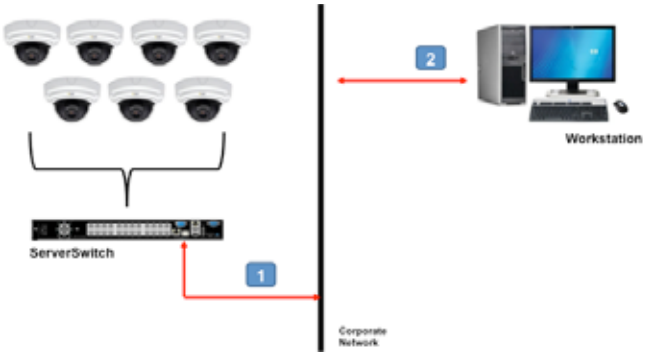
With general purpose IT systems, IP cameras immediately transport the video they capture back to a centralized server or datacenter for viewing and storage. In fact, it's not unusual for video from various sites and hundreds of camera streams to be sent over an organization's network to a server in real time. The bandwidth-intensive video can impact critical network traffic on point-of-sale and other business systems while potentially requiring compromises to the surveillance network in terms of quality. This is one of the key issues for IT with respect to IP video surveillance, leading some administrators to install dedicated and independent networks to reduce impact on existing ones.

In a distributed surveillance architecture, appliances record closer to the perimeter of the surveillance network, near the cameras. There are three aspects to providing a 95% reduction in video surveillance impact on the network: 1) 100% of the constant live video streams stay local for recording; 2) only selective video is streamed back for live viewing; and 3) only selective video is streamed back for archiving. This approach also increases the reliability of the video by disassociating the surveillance video recording from conditions that can affect the health of the network such as network congestion or network outages. Video continues to record when the network goes down, and there are fewer single points of failure.

Another aspect of an intelligent surveillance appliance is that it reduces cost and complexity in surveillance systems by eliminating the need for proliferating IP addresses for each camera on a 1:1 basis. A surveillance appliance requires only one IP address and can create a ratio of up to 24 cameras to one appliance IP address. This reduces IP address requirements by almost 95% and improves network security. General-purpose IT systems typically require an IP address for every camera or component, which is not scalable or sustainable.



Centralized, non-appliance architecture requires IP address for each camera or devices (1:1 ratio)



Appliance architecture reduces IP addresses (up to 1:24 ratio)

#2 Uncompromised Video Surveillance Quality

Given the emergence of high-resolution breakthroughs such as facial recognition, physical security leaders stand to benefit greatly from an intelligent surveillance appliance that allows them to embrace the highest-quality video and applications without compromise. General-purpose systems can require tradeoffs on frame rate and resolution quality to accommodate the limitations imposed by the IP network or by the storage systems, servers and other components that were not built to manage or capture intensive video. By using an intelligent appliance that disassociates video surveillance recording from the IP network until recording is needed, organizations can capture the highest-quality megapixel video without quality tradeoffs and without concerns about burdening the IP network.

The elimination of ongoing video streaming also reduces the risk of quality degradation due to network issues. The potential for missing or frozen frames is mitigated because recording takes place closer to the cameras and does not depend on the quality of the network.

#3 Visibility of the Entire Physical Security Ecosystem – Down to the Camera

The role of the security leader is to reduce risk. This requires visibility and control over the physical security ecosystem, including all sites. But a general-purpose approach only provides monitoring to the server or switch. That's sufficient for most applications such as an email or database server, but not for video surveillance. Visibility is needed beyond the server and switch, down to the source cameras. This allows the security manager to be alerted when cameras are damaged or settings are incorrect leading to the recording of out of focus images, gray screens, or other issues that go undiscovered until it's too late.

An intelligent surveillance appliance provides health monitoring, independent of the VMS (video management system), of the entire ecosystem including the server, switch, storage, PoE and cameras. This monitoring allows greater visibility and better control. It also includes proactive event management and notification 24 hours a day via text message or other communication method in the event of an issue.

An intelligent surveillance appliance provides health monitoring of the entire ecosystem including the server, switch, storage, PoE and cameras.

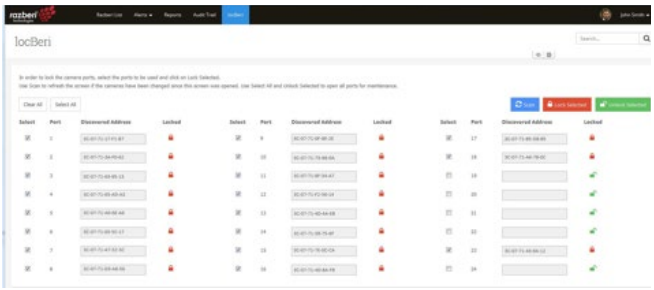
An intelligent surveillance appliance consolidates various systems into one overarching health monitoring system, rather than relying on the fractured monitoring applications a general-purpose system employs. Monitoring of systems health is key to lowering the risk of video loss and unusable evidence.

#4 Protecting Against Cyber Attacks

In late 2016, a massive distributed denial of service (DDoS) attack caused outages of major web sites such as Amazon and Twitter. Hackers hijacked an estimated 100,000 devices, including network security cameras, into a botnet for the attack.[2] Protecting surveillance systems from hackers and cyber attack has become an increasingly difficult challenge, and external camera and entry ports prove to be ideal access points for hackers to reach the corporate network and wreak havoc. For hackers, it can be as easy as unplugging a camera on the outside of a building and plugging in a laptop.

Most general-purpose systems don't provide protection against cyberattacks at the camera level, or they provide protection that often proves prohibitively difficult to implement. Dedicated camera networks, 802.1x and MAC address binding (or port security) are all options to help secure the network and they should be considered, but they can be complex to set up and maintain.

An intelligent surveillance appliance includes a cybersecurity protection mechanism as a priority and provides the opportunity to easily set up a virtual LAN (VLAN). The security leader can lock down camera ports on a switch with a single click to prevent hackers from gaining access to the surveillance system and ultimately to the corporate network itself. If a device with a different MAC ID address is plugged into the camera or access port, it cannot gain entry into the network and will be locked out. The intelligent appliance also provides a web-based interface to unlock ports for maintenance and camera changes.



Lock down ports to reduce cyber threats

#5 A Scalable, Open, Space-Saving Solution

An intelligent surveillance appliance replaces the server, storage device, network switch and PoE camera power of a general-purpose system, combining the functionality of all of these (along with a suite of intelligent software features) into a single appliance built specifically for the surveillance industry. It delivers the following characteristics to outperform general-purpose systems.

2 http://www.csoonline.com/article/3126924/security/here-are-the-61-passwords-that-powered-the-mirai-iot-botnet.html

SCALABLE:

There are two aspects of scalability to consider when evaluating general-purpose systems versus intelligent surveillance appliances. The first is the adding and removing of cameras, which is to be expected in an ever-changing environment. Intelligent appliances have a clear benefit of making this easy before, during or after installation, unlike general-purpose systems that may require significant reconfiguration to make changes. The second involves the misperception that appliances are only suitable for smaller businesses or implementations. In fact, intelligent surveillance appliances are purpose-built for scalability to the largest enterprises and deployments; they provide a simplified, network-friendly architecture, as well as better ecosystem visibility, monitoring and oversight of hundreds and thousands of sites and cameras.

OPEN:

When selecting an appliance for surveillance, it is important to identify open systems that are video management software (VMS) agnostic. This allows the selection of the best-of-breed VMS that is right for the application and implementation. An intelligent appliance is pre-certified to work with leading VMS solutions but does not lock the security leader into one option.

SPACE-SAVING:

A general-purpose system can require more components and a larger physical footprint than an intelligent surveillance appliance.

In many environments such as retail, education and distributed organizations, space is at a premium. General-purpose security components take up valuable space adjacent to a manager's desk in an already crowded office. In large-facility installations, they can fill racks of air-conditioned space or require costly building reconfiguration. An intelligent surveillance appliance is an all-in-one device with a small footprint that fits easily in the available space and saves cooling and energy costs.

Making the Best Choice for High-Performance, Cost Effective IP Video Surveillance that Delivers

This paper serves as a framework to evaluate the right approach to a high-performance, reliable and cost-effective IP video surveillance solution – one that takes into account network bandwidth and IP impact, health performance monitoring, cybersecurity, openness, scalability, and space constraints. Because surveillance is intersecting with IP networks today, system integrators, security managers, and IT leaders need to work together to determine the best architecture and technical solutions. Organizations can reduce security risks and future-proof their security investments with intelligent network appliances built for the demands of video surveillance.

razberi™ technologies

Contact Razberi Technologies today to request a demonstration and discover what the intelligent surveillance appliance can do for you at razberi.net/demo.

Razberi makes intelligent surveillance appliances that record closer to cameras, improving video quality while reducing capital, bandwidth, and space costs. By deploying Razberi ServerSwitchIQ™ appliances in a distributed architecture near the network's edge, enterprise security leaders and integrators can reduce megapixel video impact on the network by up to 95 percent. Combining a PoE switch, server, storage, and intelligence, the scalable platform is open-architected to work with top video management systems (VMS) out of the box. Razberi VyneWatch™ health monitoring software alerts security pros to issues 24x7 while Razberi LocBeri® cybersecurity features lock down vulnerable ports. For information, visit razberi.net.

Americas: 469-828-3380
UK/EMEA: 0203 773 3689
salesinfo@razberi.net

wpia20170127