

HITACHI

Inspire the Next



Concerned with Preserving Mission Critical Data?

Then consider the benefits of Hitachi VMP, a complete solution purpose-built for the unique and growing needs of video and the internet of things (IoT)

Terrorism, insider threats, hackers and growing cybersecurity challenges keep security directors up at night. The case for comprehensive and reliable physical security—including video surveillance systems—is more pronounced than ever for the protected premises. Capturing high-resolution images, video streams and intelligent data from thousands of internet of 'things' (IoT) devices is increasingly critical, so it follows that managing, analyzing, storing and retrieving data quickly, completely and securely is paramount. Equally important is having lossless video, the overall size/capacity of storage, speed, fault tolerance and redundancy.

There are many choices and substantial differences in procured solutions. Your choice can make or break your expectations—and results. Hitachi Video Management Platform (VMP) built on certified commercial technologies from selected partners and Hitachi Data System's Virtual Storage Platform (VSP) G Series architecture provides key data management functionality targeted for mission critical applications. This tightly integrated converged platform

combines best of breed storage, network and compute technologies optimized for virtualized environments to support a wide variety of enterprise applications. Hitachi VMP is a purpose built, superior designed solution to meet the needs of the enterprise, government, critical infrastructure and mission critical applications. VMP, through secure and segregated storage, can help physical control requirements around NERC-CIP, PCI, and HIPPA, HITECH and HITRUST regulations.

Security threats are fluid and evolving. Video needs to be accessible at a moment's notice, whether emanating from hundreds or thousands of camera streams. The continued growth of IoT, cameras as data-gathering devices, video analytics, machine learning and artificial intelligence, which require huge amounts of fast, high-quality video, in real-time or from archived storage, further complicates the issue. Still, this market continues its upward spiral. According to the report: The Global Video Analytics, VCA, ISR & Intelligent Video Surveillance Market 2015-2022, the industry's revenues

will pace at a Compound Annual Growth Rate (CAGR) of 18.2 percent, propelled by the video surveillance boom, Safe Cities, technology maturity and price reduction in video analytics. VMP is an answer to deal with the constraints pushed by greater video IoT pressures, while its segregated network environments allow for more control over data storage.

Managing, analyzing and storing video and IoT data correctly presents unique challenges to anyone hoping to keep data safe, access it rapidly and at the highest quality, or even in a way that complies with regulations or reduces risk. This paper will provide readers a look at the unique challenges video and arm users with the right criteria to consider as they design a system that is effective and presents viable options for successfully storing, managing and analyzing critical data.

IoT and Video Growth is Exploding, Along with the Needs to Support It

Cameras are more than a source of video for security, loss prevention and identification.

Today, cameras are evolving to become advanced IoT devices that provide data and real-time intelligence to improve overall operations and business outcomes in smart cities, transportation, retail, industrial and other increasing integrated specifications and environments.

There is a wide range of video management solutions available on the market today to handle all this data. VMS and PSIM aggregate video information and are at their best when they can pull video data from a storage solution that is not impeded by the inherent latency from some of the shared storage solutions that manage all data such as EMC/Dell, HP and IBM.

The Hitachi VMP is more than a static hardware box or server appliance add-on. It is a built-for-video, all-encompassing server, network, storage and management solution that bridges the gap between information technology (IT), operational technology (OT) and physical security. It is the single, all-encompassing solution that can optimize, store and reliably segment data, with the

explode commensurate with the number of camera deployments, higher resolutions and the need for quality streams and faster transmission speeds will compound. These factors, as well as others, require a unified solution that can scale up readily, without compromising stability factors.

Video Data is Different

"The fact of the matter is that video data is fundamentally different from IT data, with very specific requirements," said Pierre Bourgeix, Vice President, SecureState Consulting LLC, in Cleveland, Ohio. "One of the most important criteria is to be able to store petabytes of information and retrieve it safely and optimally. Unfortunately, for the IT decision maker and C-Suite executives, the discussion of storage options has been relegated to an 'apple to oranges' conversation, with the inability to compare solutions only adding to confusion."

The Hitachi VMP solution considers all these critical factors when optimizing a video surveillance specification. Nevertheless, there is more

"The fact of the matter is that video data is fundamentally different from IT data, with very specific requirements,"
-- Pierre Bourgeix,
Vice President,
SecureState
Consulting LLC,
Cleveland, Ohio.

to consider in the video management and storage conversation. It is about liability, risk and potential penalties levied by regulatory agencies and standards bodies for compromised, unobtainable or unusable video. If an incident takes place and you cannot validate that you had proper processes in place documenting the occurrence through video or other IT, OT or physical security safeguards, you may be at risk if a loss occurs. Today's video is part of a holistic approach to security. It is secured in a regulated environment and ensures visual

validation as long as proper protocols have been followed.

Risks are Real: Potential Fines Astronomical

For utilities, energy companies, water treatment facilities and other critical infrastructure, reliable video security deployments that protect people, property and assets are not simply good business practice—in regulated markets they are often used to verify procedures and general compliance. Without this proof or documentation, the fines can be hefty. For example, the North American Electric Reliability Corporation (NERC) Reliability Standards fine for lack of functional security plans and systems or missing video files can range from \$7,000 to \$10,000 per day for energy facilities, and if energy delivery is actually interrupted from an attack or inadequate maintenance, the fines can be much higher.

Recent and historical examples of lost, irrecoverable or other unviewable-recorded video streams underscore the need for a turnkey, comprehensive solution that optimizes storage and retrieval in the event of

an incident or terrorist attack. Without uncompromised and high-availability video, there is no evidentiary control and critical infrastructure and other markets risk monetary fines and civil liability penalties.

- In 2009, the Federal Energy Regulatory Commission (FERC) approved a \$25 million civil penalty as part of a settlement with Florida Power & Light Co. (FPL) stemming from a February 2008 blackout that lost power for millions of consumers in South Florida for several hours. FPL also agreed to a broad program of remedial measures to enhance its system and operations to prevent another occurrence. The settlement represented FERC's first civil penalty assessment under its Electric Reliability Standards and its first joint enforcement effort with NERC, the FERC-designated Electric Reliability Organization that oversees daily enforcement of reliability standards.
- In 2013, FERC imposed a \$975,000 civil penalty against Entergy Services for

(NERC) Reliability Standards fine for lack of functional security plans and systems or missing video files can range from \$7,000 to \$10,000 per day for energy facilities, and if energy delivery is actually interrupted from an attack or inadequate maintenance, the fines can be much higher.

27 violations of reliability standards. FERC's Office of Enforcement found the company failed to institute required standards and practices to protect its system from long-term outages. As evidenced in a number of communications outages affecting Entergy's operations, Entergy failed to execute required redundancy in its communications systems and backup power supplies and to adequately test for, plan and respond to these communications outages.

- A sniper attack on Pacific Gas and Electric Company's Metcalf substation near San Jose, Calif., in April 2013 reportedly caused \$15 million in damage. The Metcalf incident was deemed a "sophisticated"

assault on PG&E's transmission substation in Coyote, Calif., as a gunman fired on 17 electrical transformers. PG&E alone pledged to spend \$100 million to improve security at its facilities, while the company, along with AT&T, announced separate \$250,000 rewards to catch the saboteurs.

Energy companies and the U.S. power grid face numerous challenges in securing a significant piece of America's critical infrastructure and regulations continue to evolve. The Critical Infrastructure Protection Reliability Standard for Physical Security (CIP-014-01) R5 and R6 further ensure reliability through a new series of measures approved in November 2014 and effective in January 2015, stemming from

the Metcalf substation attack. CIP-14-1 is a prescriptive standard that outlines the roadmap and requirements for transmission facilities to plan for, eliminate and mitigate many internal and external threats and designed to lessen the likelihood of these scenarios.

Other Vertical Markets

The need for quality images, availability of critical video for evidence and retention and security of data extends to other vertical markets. According to TechTarget, some 60 percent of Fortune 250 companies require video as part of their corporate security strategy, further dictating the importance of reliable surveillance data.

- In manufacturing, security specifications are taking a proactive approach to quality control in the factory floor and widespread concerns over potential threats ranging from food supply contamination to insider espionage of classified information. New regulations have arisen around protecting product manufacturing and distribution, including International Traffic in Arms

The need for quality images, availability of critical video for evidence and retention and security of data extends to other vertical markets.

Regulations (ITAR) and ISO270001 and the threat of product recalls for faulty products from inadequate monitoring of manufacturing process.

- In the retail sector, video cameras provide insights and targeted data by tracking customer activity which can be used to improve sales and customer satisfaction and yield marketing insights. Business intelligence from cameras include dwell time at displays, the frequency of activity in given areas such as end cap display and even automatically count people passing through a defined area in real time. Queue detection is another valuable analytics, detecting groups of people waiting in line and alerting management to send additional cashiers, providing a smoother customer experience.



- In the banking and financial markets, regulations have long been established for security and processes designed to protect sensitive data. Many forms of cyber and physical security controls point to a greater need for data storage and scalability, including the non-standards based Financial Industry Regulatory Authority (FINRA) that make video resolution critical, along with the ability to review and store clear, concise and actionable data in a scalable and stable manner.
- In healthcare, regulations such as Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Health Information Trust Alliance (HITRUST) are changing the way data is stored and exchanged, with compliance requiring physical security such as CCTV, access control and analytics to proactively address possible threats that could cause an information breach or compromise physical security at the protected premises.

There is also the increasingly integrated security environment: in Safe Cities, for example, body-worn cameras are also big users of video, as are dashboard cameras.

Adding to the conundrum is the rapid growth of video analytics for operational intelligence, as well as security alerts that also rely on robust compute and storage for real-time alerts and historical data. In smart city operations, traffic detection that counts vehicles on highways, streets and parking garages and vehicle counters, when not specifically designed for this activity and resist false alarms, can add to storage requirements. License plate recognition, used to match plates and compare against stored lists, can also consume large amounts of data and is increasingly deployed in urban environments.

Solutions that allow users to reliably store data and retrieve it in these applications and others presents a stronger value proposition for the user, who can gain easy access to the information and use it for a variety of purposes including security, business intelligence and operational process improvement and even machine learning. Video analytics promotes a proactive element, allowing users to identify potential data and get alerts before an incident. There is also the increasingly integrated security environment: in Safe Cities, for example, body-worn cameras are also big users of video, as are dashboard cameras. Access control often piggybacks with video to trigger cameras if someone with an expired credential or other unauthorized party tries to gain entrance.

"For mission critical and other markets, the most important element is the ability to store and manage petabytes of information reliably and retrieve it in a way that allows users to visualize the information in a secure and segmented manner," commented Pierre Bourgeix.

Hitachi VMP Meets the Challenges

So just what is the most efficient solution? One that manages, segments, stores, scales and secures data to enable the consistent mitigation and management of threats. Again, not all solutions are created equally. In fact, many of the video management systems on the market suffer from low-resolution playback; difficult retrieval processes; the inability to comply with high-availability requirement mandates; an inability to scale readily and cost-effectively; and are non-segmented or segregated solutions that interfere with the network infrastructure. If video data resides on a shared IT network, it could burden the network infrastructure.

The ideal solution will:

- Keep all data available, secure and uncorrupted.
- Comply in regulated markets like energy, healthcare and government and increase the value proposition for unregulated verticals and business users.

- Allow users to view their data anytime, without slowing the network, reducing availability or degrading quality.

Without the ability to store increasingly high amounts of data streams, users will find latency and impingements on the IT environment, causing the inability to grow the solution, resulting in potential gaps in security. There is a greater reliance on the cloud, but that too comes with a higher price tag than a one-time, non-proprietary solution like Hitachi VMP. A purpose-built VMP that considers

Without the ability to store increasingly high amounts of data streams, users will find latency and impingements on the IT environment, causing the inability to grow the solution, resulting in potential gaps in security.

the consequences of growing data can actually reduce risk and liability, provide for business process improvement and result in a lower total cost of ownership over time. For end users, obtaining the correct solution is understanding how the business uses video data to manage its operational environment and the growth plan of that business to build in storage requirements. Hitachi has the most advanced calculator in the industry to determine scale and capacity today and tomorrow.

The Hitachi VMP is an enterprise level, converged solution that seamlessly incorporates compute, networking and storage within a virtualized environment. Designed as a vendor-agnostic platform, it is optimized to host multiple DVMS (digital video management systems) and video analytics systems. It bridges the gap between information technology, operational technology and physical security with its ability to store and segment data and scale cost-effectively. With Hitachi VMP, data does not have to reside on the IT or corporate network and as such will not compromise network resiliency.

Competing solutions in the market today are not designed from the ground up for video and other IoT data, and are usually pieced together from various vendors, resulting in inadequate integrations and finger-pointing if anything goes wrong. With Hitachi VMP, customers get a single, integrated solution built specifically for video, and one that is completely supported by a single, established partner that can expand the solution over time as your needs grow.

Finding the Right Solution

Deciding which platform to specify takes careful research and team consideration. Here are four key parameters to remember:

1 Video and IoT data is fundamentally different from traditional IT data. It is becoming mission critical for security and operational intelligence and with increasingly deployed video analytics equals a high-demand ratio.

2 Video data requires higher network speeds and intensive storage system utilization.

3 Risk and liability from non-compliance can be astronomical in fines and devastating in loss of business continuity and downtime.

4 Because of all those factors, you need the right equipment and tools for the job.

Business IT and C-Suite users need to keep their video available, secure and uncorrupted. Optimization is key when looking to comply in regulated markets like energy, healthcare and government, as is the ability to easily and readily view video anytime and without compromising the network.

After factoring in all these considerations, the Hitachi VMP solution is a smart option to meet all your technology, security and compliance needs.



Hitachi Insight Group
Global Headquarters
3315 Scott Boulevard, 4th Floor
Santa Clara, CA 95054-3103 USA
www.HitachiInsightGroup.com
community.HDS.com/community/IoT

Regional Contact Information
Americas: +1 877 765 1832
International: +1 408 471 4999
info@HitachiInsightGroup.com