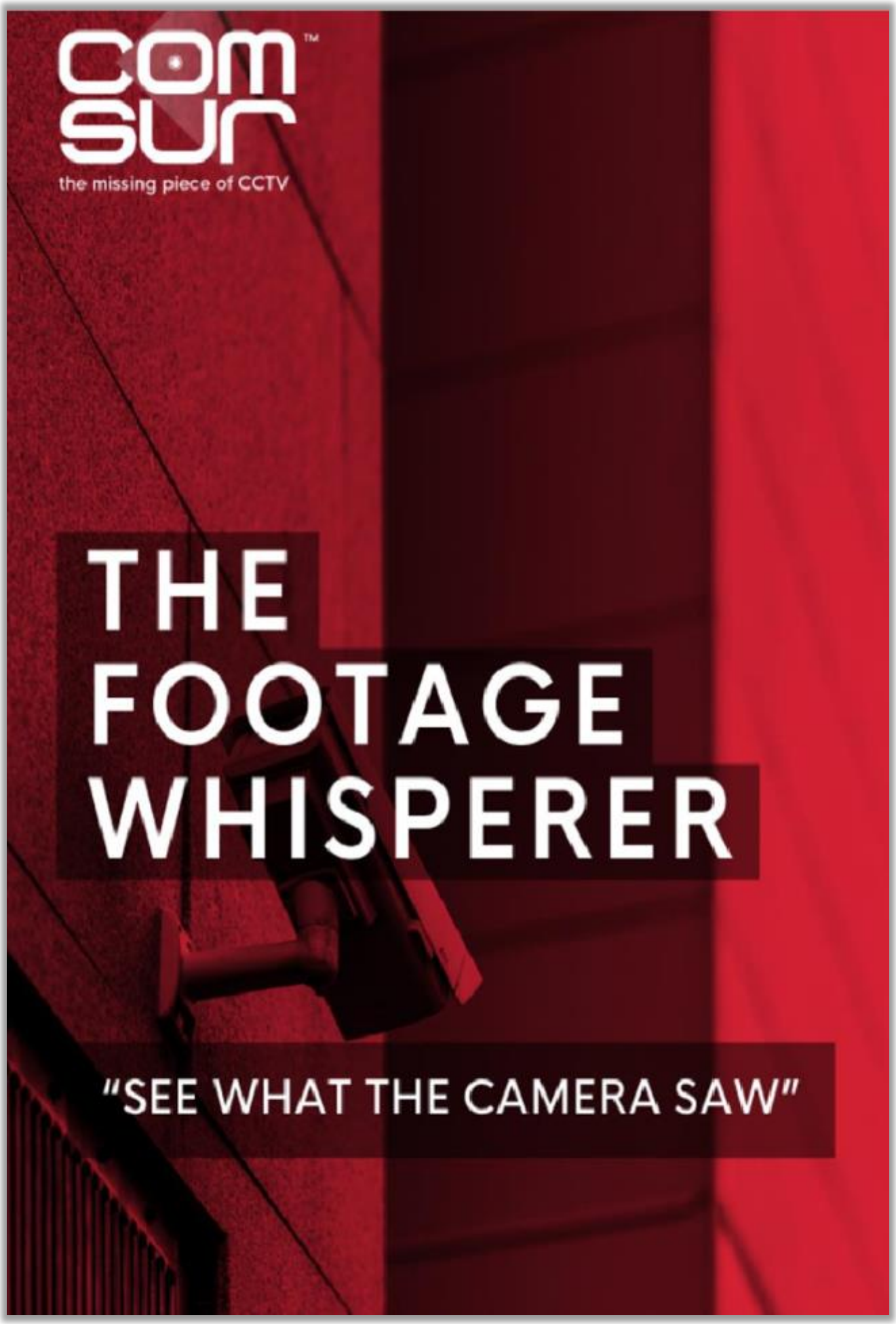
com sur
the missing piece of CCTV
THE FOOTAGE WHISPERER
"SEE WHAT THE CAMERA SAW"

UTILITY VALUE OF COM-SUR™ FOR DATA CENTERS AND SERVER ROOM FACILITIES

WELCOME

AUDIT HOURS OF FOOTAGE IN MINUTES FIND OUT HOW COM-SUR WILL HELP

CCTV surveillance is common in data centers and server room facilities world over, but footage is often only reviewed reactively. Our company realized this problem early-on and has developed the world's only CCTV video footage auditing software that encourages daily auditing (hours in minutes) of CCTV footage, filling the gap for a complete "workflow". The software works with existing cameras and VMS, regardless of type/brand, and provides a standardized approach for intelligent incident reporting. Our software also offers exceptional investigative capabilities.

'COM-SUR' – THE WORLD'S ONLY CCTV VIDEO FOOTAGE AUDITING, SMART BACKUP, AND STANDARDIZED INTELLIGENT INCIDENT REPORTING SOFTWARE – THE MISSING PIECE OF CCTV

COM-SUR is the world's only CCTV video footage auditing, smart backup, and standardized intelligent incident reporting software that serves as a complete workflow and force multiplier. It helps audit 24 hours of footage in minutes, reduces data size, creates standardized intelligent reports, and delivers business intelligence. COM-SUR helps unlock hidden information in CCTV footage and enables people to gain actionable intelligence, improve homeland security, prevent crime and losses, identify and mitigate threats and hazards, and improve operational efficiency. It empowers people to gain new jobs as CCTV video footage auditors and start new businesses of auditing video footage. Like MS Office, COM-SUR is an enabler that makes it easy to work with CCTV cameras in a standardized way, leading to better decision-making. It also offers exceptional investigative capabilities.

HOW COM-SUR SMARTLY REDUCES 'VIDEO' STORAGE SIZE

COM-SUR employs an innovative approach to smartly reduce the amount of video to be audited and consequently the storage size of videos. Regardless of the video's frame rate, COM-SUR captures a single screenshot of the consolidated 'moment' of 'that' one second, when the I, P, and B frames come together. This method significantly reduces data size without sacrificing vital information. It goes without saying that when multiple cameras are displayed in a grid view, say 4x4, the storage size is further reduced since all the cameras are captured as a single image. Since no suggestion is being made to replace the actual video with screenshots, COM-SUR acts as a wonderful supportive technology both to audit (review) just 86400 frames representing 24 hours and reducing the data size at the same time.

CHALLENGES FACED BY DATA CENTERS AND SERVER ROOM FACILITIES

1. Unauthorized access:

Protecting against unauthorized access is a primary concern. Data centers and server room facilities house sensitive information and systems, and unauthorized individuals gaining physical access can result in data breaches, theft, or sabotage.

2. Theft:

Data centers and server room facilities house valuable equipment, including servers, storage devices, and networking infrastructure. Physical theft of these assets can result in data loss, service disruption, and financial losses.

3. Sabotage and vandalism:

An organization's data centers and/or server room facilities can be targeted for sabotage or vandalism by persons working for competitors or other malicious actors. Damage to equipment, cutting power or network cables, or intentional disruption of services can have severe consequences.

4. Fire and water damage:

Fires and water damage pose significant risks to data centers and server room facilities. A fire can cause catastrophic damage to servers and other equipment, while water leaks or flooding can lead to equipment failure and data loss.

5. Environmental factors:

Temperature and humidity control are crucial for the optimal functioning of data center equipment. Inadequate cooling, improper airflow, or high humidity levels can lead to equipment failures, reduced performance, and increased energy consumption.

6. Worker safety:

Worker safety is a significant challenge in data centers and server room facilities. This includes electrical safety, ergonomic issues, heat and cooling concerns, fire safety, handling hazardous materials, and various security incidents.

7. Compliance issues:

Compliance with regulations and standards poses challenges for data centers and server room facilities. They must adhere to data protection and privacy regulations, security standards, environmental guidelines, occupational health and safety requirements,

accessibility standards, and undergo audits and reporting.

8. Insider threats:

Data centers and server room facilities have to deal with insider threats from disgruntled employees or even unwitting staff who fail to follow proper security and safety measures.

9. Humongous growth of surveillance video:

The exponential growth of surveillance cameras has resulted in an unprecedented surge in surveillance video. Effectively managing this data has become a daunting challenge due to the massive storage capacity required, especially considering the prolonged retention periods necessary for security, incident investigation, or legal purposes. Furthermore, the prevalence of high-resolution video with increasing megapixels compounds the storage demands, making efficient data management an urgent priority for organizations grappling with the immense volume of surveillance footage.

COVID-19 PANDEMIC

The pandemic had a significant impact on the operations of data centers and server room facilities worldwide. The increased demand for digital services, the need for enhanced business continuity planning, the shift to remote management and monitoring, and supply chain disruptions were among the key effects. Staffing and workforce challenges, cybersecurity concerns, and the adoption of health and safety measures also emerged. Guidelines were issued to prevent the spread of COVID-19, but outbreaks still occurred.

USE OF VIDEO SURVEILLANCE AT DATA CENTERS AND SERVER ROOM FACILITIES

Most data centers and server room facilities have video surveillance covering the following areas:

- Entry and exit points
- Lobby and reception areas
- Equipment rooms
- Server aisles
- Areas housing the network infrastructure
- Critical infrastructure areas such as power supply areas, backup generators etc.
- Restricted access areas
- Corridors and common areas
- Parking and other outdoor areas

Further, the concerned stakeholders at data centers and server room facilities generally need to review and analyse recorded CCTV video footage from time to time for investigating incidents and/or accidents, and other issues in order to corroborate evidence as well as assist Police/other Law Enforcement Agencies.

USE OF THERMAL CAMERAS

Thermal cameras detect and capture infrared radiation emitted by objects and individuals based on their heat signatures. They are used in data centers and server room facilities for the following purposes:

1. Temperature monitoring:

Thermal cameras are used to monitor the temperature of critical equipment and infrastructure in data centers and server rooms. They can detect hotspots or abnormal temperature variations, allowing operators to identify potential issues and take preventive measures to avoid equipment failure or overheating.

2. Fire detection:

Thermal cameras are effective in early fire detection within data centers and server rooms. They can detect heat signatures associated with fires or overheating equipment, enabling swift response and timely evacuation to prevent further damage.

3. Energy efficiency:

Thermal cameras help identify energy inefficiencies by detecting areas of excessive heat or poor insulation. This information can be used to optimize cooling systems, airflow management, and overall energy consumption in the facility.

4. Security monitoring:

Thermal cameras can be used for security purposes in data centers and server room facilities. They can detect human presence or movement based on body heat signatures, allowing operators to monitor and identify unauthorized access or potential security breaches.

LIVE MONITORING – CHALLENGES

Several data centers and server room facilities have a dedicated control room with operators, set up for live monitoring of CCTV cameras. However, live monitoring comes with its own set of challenges of video blindness, poor attention span, boredom, operator bias, false alerts, and so on.

Moreover, these cameras continuously capture and record humungous amounts of video data. It therefore becomes a daunting task for the operators to review and analyse this data whenever the need arises. Thus, it may be noted that benefits from video surveillance systems can accrue only when they are used optimally, suggestions for which are enumerated further on, in this document.

COMPLIANCE - GENERAL

Conformity or compliance in any organization means adherence to laws and/or rules and regulations, various standards, as well as data storage and security requirements as laid down by government bodies, governing bodies of the respective industry, or the management of the organization. When an organization complies with the requirements mandated by government and/or governing bodies, then it is termed as ‘regulatory compliance’ which enables the organization to run in a legal and safe manner.

COMPLIANCE - AUDITS

Several organizations carry out compliance audits on a regular basis to avoid the potential consequences of non-compliance.
A compliance audit examines how well an organization adheres to compliance requirements. Some organizations use video surveillance to monitor compliance issues and audit recorded CCTV video footage from time to

time for investigating and preventing compliance issues. Auditing CCTV provides actionable insights on the level of compliance within the organization.

AUTOMATED SOFTWARE – WHY THEY WILL NOT WORK IN ISOLATION

In the wake of the Christchurch shooting incident, several high-profile places of worship considered deploying gun detection technology. However, there are concerns about its efficacy, since it may not be able to detect all types of weapons, or the perpetrator could still create damage before being detected. Similarly, automated systems like video analytics, AI/ML can only detect what they have been programmed for. What about the rest? Again, these technologies are prone to triggering huge amounts of false alarms. Also, since the permutation combinations of exceptions can be vast and varied, it becomes almost impossible to automate every kind of exception. Facial recognition technology also raises ethical and privacy concerns, and has been found to produce inaccurate results, especially for certain ethnic groups. Therefore, experts suggest that while automated technologies will continue to grow, human intervention and intelligence will still be necessary to verify alerts and ensure their efficacy.

"CCTV IS NOT ENOUGH – WE MAKE IT WORK FOR YOU"

While it is not being suggested that optimal usage of video surveillance can cure all issues, several issues of the following kind can be addressed by doing just a little 'more' with respect to making the optimal use of video surveillance systems:

- Operational issues
- Recces/suspicious movements/activities
- Insider job/security lapses
- Equipment malfunction/other technical issues
- Violence and vandalism
- Unauthorized/unlawful activities/visitors
- Health and safety issues
- Compliance issues
- Accidents/Causes of potential accidents
- Potential causes of fires
- Loss/theft
- Intrusions, especially by animals
- Inattentive staff (e.g. guard sleeping)
- Unruly staff/security guards
- Unclaimed/unattended objects
- Issues with female staff
- Cameras/recorder malfunctions

So, what is the 'more' that needs to be done?

1) AUDIT CCTV VIDEO FOOTAGE DAILY AS A STANDARD OPERATING PROCEDURE

'Auditing' means 'seeing' what the cameras 'saw'. Auditing of CCTV footage should be done

daily (continuous investigation) to identify potential issues and threats. Auditing is a dedicated and systematic process that helps address challenges related to live monitoring and alert-based systems. Auditing helps in evaluating analyzing incidents to improve existing policies, procedures, and processes. Concerned personnel should be trained to become CCTV video footage auditors, and the audit teams should be rotated to avoid complacency/collusion. Daily auditing of CCTV footage can also help in adhering to the principles of Kaizen and TQM for business improvement.

2) DOCUMENT AUDIT FINDINGS/INCIDENTS

Audit findings/incidents should be documented in a standardized template to find the root cause to prevent future recurrences. Historical data of such findings/incidents can reveal patterns that can help take better informed corrective and preventive action. If all data centers and server room facilities report incidents in a standardized template, relevant authorities can derive business intelligence from the data and take action for the collective benefit of all data centers and server room facilities.

3) ENSURE DISASTER RECOVERY OF CCTV VIDEO FOOTAGE – LIKE A 'BLACKBOX'

CCTV video footage must be stored at multiple locations in order to ensure that even if the recorder is stolen, destroyed or tampered with the data is never lost. Further, any backed-up data must easily be searchable and retrievable; else, it is going to be a nightmare finding the relevant video.

4) DISPLAY DYNAMIC INFORMATION AT RELEVANT PLACES

Document and display details of information that is dynamic in nature in relevant areas. For example:

1. List of authorized staff.

2. List of authorized security personnel deployed at the data center or server room facility.

3. List of potential suspects/miscreants likely to visit the premises of the data center or server room facility (a 'Watch out' list).

5) USE A POWERFUL NEW SIGNAGE

"WE AUDIT CCTV VIDEO FOOTAGE EVERYDAY".

One size, one color, one powerful message. Across the nation.

DE-CENTRALIZED SURVEILLANCE + CENTRALIZED SURVEILLANCE = OPTIMAL RESULTS

Organizations with multiple locations struggle with centralized video surveillance due to infrastructure cost, internet bandwidth, and operator limitations. De-centralized surveillance offers higher accountability at each location and better situational awareness, leading to more chances of discovering exceptions.

CONCLUSION

"You see, but you do not observe" is a quote by Sherlock Holmes in A Scandal in Bohemia (1891, written by Sir Arthur Conan Doyle).

COM-SUR makes 'observation' far effortless and effectual leading to superior results.

"Cameras don't lie" - but how will you know unless you 'see' what the cameras 'saw'?
Audit CCTV - why suffer!

Get award-winning COM-SUR now.
Don't wait for things to go wrong!