

WHITE PAPER

EXTENDING THE VALUE OF PHYSICAL SECURITY SYSTEMS WITH ENHANCED VIDEO SURVEILLANCE

Utilizing surveillance cameras with video analytics can have a major impact on business objectives.



EXECUTIVE SUMMARY

Organizations across industries have relied on video surveillance systems as an important component of their physical security environment for decades. The advent of inexpensive, network-enabled cameras facilitated the growth of these systems to the point where virtually every organization has some video surveillance footprint. Whether limited to critical areas or deployed throughout an enterprise, these cameras collect video footage that organizations historically used for forensic purposes – something went wrong, and video footage enabled security teams to look back to determine what happened.

Video surveillance is undergoing an important evolution. Organizations realize that the cameras they have

distributed throughout their facilities have tremendous untapped potential as sensors in the Internet of Things. Surveillance system deployments enable organizations to move beyond simple forensic investigations and use their cameras proactively to protect people, property and processes.

This white paper looks beyond traditional deployments of video surveillance and identifies ways that video systems can deliver value beyond typical security use cases. It addresses the challenges to implementing these technologies and provides advice on overcoming those challenges through examples from key industries, including retail, education, healthcare and energy and utilities.

Physical Security Solutions

Every organization relies on people, property and processes to achieve its mission. From a hospital treating patients with expensive medical equipment to a retail store offering merchandise to customers, protecting those assets is a crucial component of managing risk and protecting the bottom line. Failure to provide adequate protection increases risk and jeopardizes the organization's ability to achieve its strategic and operational objectives.

Physical security solutions provide the baseline level of control necessary to address these risks, but they also have tremendous untapped potential to deliver additional business value. Organizations now have the opportunity to create this additional value, improving the return on their physical security investments while utilizing their current infrastructure.

Evolution of Video Technology

Video surveillance systems serve as the enabling technology to unlock this additional value. Many organizations originally installed these systems in years past with the goal of providing a forensic tool to support physical security investigations or simply as a deterrent. Using these systems for forensics required time-consuming manual processes that required investigators to spend hours analyzing captured footage, searching for suspicious events. On top of being an entirely reaction-based approach, lengthy forensic investigations could delay the actual response and pursuit of potential criminal suspects.

Humans also quickly became a limiting factor as organizations sought to achieve real-time situational awareness through their video surveillance systems. Typical attempts to do this relied on human operators monitoring live video feeds to react and respond to incidents as they occurred.

Costs quickly mounted as organizations hired additional staff or outsourced this function to security guard services. Firms that chose to make this significant investment found that the reliance on human analysts meant high rates of errors and overlooked events.

The next generation of video surveillance technology incorporates video analytics to reduce this reliance on human intervention, automating the analysis of captured video footage. Enhanced video surveillance (EVS) systems augment existing surveillance camera deployments with sophisticated video analytics tools to enable organizations to move beyond reactive security use cases and leverage their video as a valuable data source for business.

Video surveillance technology saw several key developments over the past decade that are enabling video surveillance to become a source of digital data. First and foremost, the emergence of IP-based cameras allows organizations to cost-effectively replace legacy analog cameras that ran over dedicated coaxial networks with IP-enabled digital cameras that run over shared wired and wireless Ethernet networks. Administrators can now place cameras in locations that were

previously difficult to reach due to electrical wiring limitations. The use of Ethernet cabling with Power over Ethernet (PoE) offers the ability to hang a camera almost anywhere that a Category 5E or Category 6 cable can be pulled and use that single connection for both power and data.

Second, the cameras themselves have gotten smarter. Modern surveillance cameras have computing and storage capability on board the device, allowing them to process video analytics in real time at the edge of the network. The term *camera* itself may be a misnomer in certain cases where it functions as an IoT sensor, capable of generating more than just video.



Percentage of educational institutions and hospitals that plan to upgrade their video surveillance solutions in the next three years¹

As video surveillance systems have evolved into the world of data, they also have moved out of realm of control by organizations' facilities departments. Cameras are now IP-enabled endpoints that connect to enterprise networks and transmit video and data streams back to servers that process and record video to storage devices. All of these devices and systems require cybersecurity controls, and all of this is under the leadership of the CIO. Is it any wonder that organizations, now more than ever, are entrusting their video surveillance systems to IT departments to design, support and, in some cases, operate?

Building the Case for Enhanced Video Surveillance

Enhanced video surveillance platforms combine IP-based video cameras, video analytics technology and artificial intelligence techniques to achieve three key operational security goals: hindsight, insight and foresight. Organizations should view the potential capabilities of their EVS investments through each of these three lenses.

Hindsight provides the ability to forensically examine past events. From a security perspective, this is the traditional use of a video surveillance system and historically can involve a time-consuming manual process of video review. With video analytics, the EVS system can collect metadata about objects seen on recorded video to create a searchable index. This can allow for

keyword searching of video recordings for faster recovery and discovery of events. For example, an operator can search for all instances of cameras seeing a male with a red shirt that occurred on Saturday between the hours of 3 p.m. and 7 p.m. in the parking lot, matching the description of a suspect. Then all video clips from all cameras with matching data can be retrieved, allowing the operator to quickly find event recordings of the suspect in minutes, as opposed to hours.

Insight provides immediate situational awareness that helps organizations improve their real-time operational capabilities. For example, a school might use its enhanced video surveillance platform to assess people entering a secure facility and utilize facial recognition to compare them to a database of known employees, parents and students. If an unknown individual attempts to enter the building amid a stream of known individuals, the EVS system can trigger an alert to security personnel, who can intercept the unknown person.

Foresight applies the lessons learned from video analytics to optimize future performance. For example, a hospital food services team could analyze customer flow patterns in the cafeteria to optimize the staffing of different shifts and the arrangement of employees throughout the cafeteria at different times of the day. This approach not only optimizes costs but also improves patient, staff and visitor satisfaction with the facility.

The shift to enhanced video surveillance today is strikingly similar to past changes in telephony technology. As phones shifted from analog devices with dedicated infrastructure to IP-enabled devices, delivery of telephone service passed from facilities to IT organizations. The technology teams had to shift their capabilities to implement, manage and maintain those systems. Over time, IT teams learned how to help their users realize the value of Voice over IP (VoIP) telephony and integrate the technology into existing productivity and collaboration systems to maximize the return on their investments. EVS systems promise to have this same degree of impact on the field of video surveillance, allowing IT organizations to exploit the value of video data beyond simply physical security.

Where Video Analytics and Data Analytics Meet

Analytics is everywhere in the modern organization.

The rise of advanced analytic techniques and the availability of inexpensive storage and compute capacity allow businesses to harness the value in many different types of data. This makes it important to draw a distinction between data analytics and video analytics.

Data analytics efforts typically seek to analyze the highly structured data sets generated by enterprise technology platforms. Customer relationship management (CRM) solutions, enterprise resource planning (ERP) tools and expense tracking systems are just a few of the many data sources that contribute to this work. The structured nature of these data sets makes them easy to define and integrate with analytics tools.

Video captured by surveillance systems does not fit the neat tabular format of most analytics sources, so typical data analytics tools are not able to derive significant insight from video data streams. Video analytics requires a specialized set of technologies that can ingest video information, detect objects and motion against the normal background in that data source, and generate a set of metadata describing the activity in that stream.

The resulting video metadata does match the structure of other data and thus can be fed into traditional data analytics tools for visualization and correlation with other business data sets.

Overcoming Challenges in Physical Security

As organizations seek to build out their physical security infrastructure, they must integrate a diverse set of technologies and address common challenges that arise with the increased reliance on video surveillance. Fortunately, today's enhanced video surveillance systems are more than capable of addressing these challenges and playing a crucial physical security role. Organizations considering the deployment of EVS solutions should approach the initiative with knowledge of industry best practices.

Enhanced Video Surveillance Components

EVS implementations rely on technology components that come either as core components of the EVS solution or are realized through integrations with existing enterprise infrastructure and applications.

The video management system serves as the central control point for an EVS platform. This system is responsible for

managing the cameras deployed throughout the organization as well as the storage and retention of the massive amounts of data generated by those systems. The management system also provides the foundation for video analytics software capable of reaching into video streams and producing the metadata required for advanced analytics capabilities. It's crucial that organizations identify a video management system that offers the analytics capabilities necessary to achieve their short-term and long-term physical security objectives.

The video management system, in turn, relies on two types of dedicated video hardware. First are the IP-enabled cameras that serve as sensors for the surveillance system. Modern video management systems are capable of receiving, processing and analyzing video feeds from virtually any camera device, but the ability to actively manage cameras depends on the compatibility of the video management system and the hardware devices. The second crucial hardware component is the storage infrastructure supporting the EVS. While it is possible to use standard enterprise storage for these purposes, the EVS will operate more efficiently if it is paired with a storage solution designed specifically to support video operations.

All of these components also require the support of enterprise-wide technology services. These include the network infrastructure and cabling necessary to carry video streams as well as the enterprise identity and access management infrastructure required to perform access control for the video system, limiting access to authorized individuals and ensuring that those individuals are not able to exceed the limits of their authority.

Finally, EVS systems may also integrate with physical security access control systems to provide enhanced levels of insight and intervention. For example, an integration between these systems can automatically trigger a security response when an individual uses an ID card to gain access to a facility but the face of the person using the card does not match existing images of the card's owner. Similarly, integrations between the EVS system and environmental sensors can detect students vaping

85
MILLION

The number of security cameras that will be in place in the United States by 2021²

in a school setting or sounds associated with aggressive behavior in a hospital emergency room environment.

EVS Adoption Challenges

As organizations plan enhanced video surveillance deployments, they often encounter three common areas of challenge to their efforts: storage, management and cybersecurity.

Storage is one of the core requirements of an EVS system. EVS platforms manage massive amounts of video and must be able to do so efficiently. The crucial nature of this challenge is evident in the fact that video is the fastest-growing driver of enterprise storage consumption. Organizations can manage this challenge and control the growing costs of storage by setting parameters around their use of video. Some key questions to ask regarding storage consumption include:

- How many cameras are necessary to achieve security and business objectives?
- What resolution and frame rate of video will the organization record and store?
- How long will the organization retain video?

Altering any one of these parameters can have dramatic effects on video storage requirements.

After addressing storage requirements, organizations often find themselves tackling questions focused on the **management** of stored video. These are sometimes policy decisions and sometimes technical ones. Here are some of the important questions organizations should ask regarding video management:

- Where will data be stored?
- Who is allowed to access data and for what purposes?
- What tools will be used to analyze video data?

Organizations may choose to tier storage in different categories to reduce costs. Short-term storage may occur on the camera itself, and long-term storage may be handled by less expensive classes of on-premises storage or by cloud solutions.

These management concerns lead directly to **cybersecurity** issues that must be considered. Organizations must pay attention to the physical security of video surveillance cameras. An IP camera with a weak or default password is vulnerable; hackers can utilize unsecure cameras as an attack surface from which to launch other cyberattacks across the network. Intruders who are able to disable or bypass cameras pose a serious risk to the physical security infrastructure. Video streams and metadata may need to be secured in transit and at rest, whether it's stored on-premises or in the cloud.

On the other side of the coin, there is an opportunity to unify a person's identity across both electronic and physical domains through integration of physical security and cybersecurity access management. This could lead to more natural multifactor authentication methods — such as the combination of facial recognition plus a card key or passcode — and greater visibility and control over who has visibility into both company physical and electronic assets.



Cloud Connected Cameras

Cloud computing is revolutionizing virtually every aspect of IT, and video surveillance systems are no exception. Organizations can leverage cloud-based Video Surveillance as a Service (VSaaS) solutions to achieve many of the same benefits that the cloud brings to other areas of their technology stack. These include scalability, manageability, ease of deployment, automated updates and increased visibility.

In a VSaaS deployment, cameras automatically stream video directly to the cloud, where management and analytics processing takes place. Hybrid approaches combine cloud-based services with on-premises hardware in an integrated approach.

Source:² The Wall Street Journal, "A World With a Billion Cameras Watching You Is Just Around the Corner," Dec. 6, 2019

Key Considerations for Deploying Enhanced Video Surveillance

Organizations in the planning stages of an EVS rollout may smooth their implementation work by answering several key questions related to the capabilities and challenges of EVS solutions:

- What are we trying to protect?
- Where do we need to place cameras?
- What kind of cameras do we need?
- Will the current network infrastructure support this system?
- Will the current storage infrastructure support EVS?
- What business goals are we hoping to achieve?
- How can we use video analytics for greater hindsight, insight and foresight?

The answers to these questions will provide crucial guidance and direction for the EVS initiative.



Addressing Privacy Concerns

No discussion of video surveillance is complete without considering the privacy implications of these solutions. Individuals and regulators remain deeply concerned about the impact of this potentially intrusive technology into everyday lives, and organizations should take steps to ensure that they don't run afoul of privacy advocates or regulators.

The most important thing to remember is that video footage and metadata that identify individuals definitely constitute personally identifiable information under both the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Footage should be treated with care, and organizations should make sure that they notify individuals who are subject to video monitoring while on the organization's premises.

The laws and regulations surrounding video surveillance are complex and vary from jurisdiction to jurisdiction. As organizations deploy EVS platforms and cameras, they should consult with attorneys with specific surveillance expertise to make sure that they don't wind up on the wrong side of the law.

There are many methods available to protect privacy while utilizing video surveillance systems. It is possible to mask parts of the field of view of a camera, for instance, to ensure that the camera does not capture the work area of a medical records technician and accidentally expose patients' personal information. Other mechanisms can provide automatic privacy masking of individuals, pixelating or blurring their images in live and recorded video. This masking can be permanent or liftable only by someone with the necessary level of security access. These privacy tools can ensure that organizations get the security and operational benefits of EVS without compromising the personal privacy of those who happen to be caught on camera.

Use Cases for EVS and Physical Security Systems

Enhanced video surveillance platforms promise to improve physical security programs and realize new business value at organizations in almost every industry. This is particularly true for businesses engaged in retail sales, educational institutions, healthcare providers and energy and utility companies.

Retail Use Cases

The retail industry may be the industry that has already taken the greatest advantage of EVS technology. The physical security applications of video surveillance in retail operations are obvious. Retailers lose millions of dollars each year to inventory shrinkage, and video surveillance can help identify shoplifting and internal loss as it happens, enabling security personnel to then intervene while the offender is still in the store.

Physical security applications are only the tip of the EVS iceberg in retail environments, however. Retailers can dramatically increase the return on their video surveillance investment by taking advantage of video analytics to build heat maps of customer traffic in retail locations, analyze customer dwell times in different parts of the store and implement queue detection and line-busting procedures to make store operations more efficient. These uses of video surveillance technology improve the customer experience and streamline retail operations.

K-12 Education Use Cases

The safety of students and faculty is paramount in today's K-12 school environment. Both districts and individual schools are investing in technology to dramatically improve school security. EVS solutions are capable of monitoring school activity in real time, integrating with other environmental sensors to provide multiple streams of data that facilitate rapid threat detection. For example, schools trying to enforce no-smoking policies on campus may deploy vape-detection sensors in bathrooms and locker rooms, which may integrate into their video monitoring system to include their environmental monitoring and alert processes with their physical security procedures.

EVS platforms can also use facial and license plate recognition technology to automatically notify security personnel of the presence of threats or unwelcome individuals on campus. These could include estranged parents under restraining orders, suspended or expelled students and known violent offenders. The system can notify relevant personnel the moment that an unauthorized individual is detected on school grounds.

Healthcare Use Cases

EVS platforms offer tremendous benefits in many healthcare settings. In a hospital environment, EVS can improve patient health outcomes. Fall detection technology can identify when a patient requires assistance and immediately dispatch emergency response personnel. Boundary detection capabilities can detect unauthorized individuals in sensitive areas of the hospital. Traffic management features can monitor traffic flow and alert security staff to anomalies that could affect operations, such as illegally parked vehicles or blocked ambulance lanes.

In the pharmacy setting, EVS platforms offer many of the same benefits as they do in other retail environments. Pharmacies can also use facial recognition to correlate image data from multiple locations to catch prescription fraud committed by criminals using different identities to illegally obtain opioids and other controlled prescription drugs.

Senior care centers may also benefit from the deployment of EVS platforms where the technology can assist overworked staff in the monitoring of residents for safety and security issues. EVS technology can keep a close eye on entrances and exits and use facial recognition technology to identify memory care patients who are attempting to exit the facility alone, putting their safety at risk.

Energy and Utility Use Cases

Energy and utility operations must offer dependable and reliable service to their customers, and EVS platforms are able to improve the safety, efficiency and reliability of these facilities without adding staff.

For example, in older plants, visual inspection may still be the standard operating procedure for monitoring and recording the values on analog gauges and valves. Cameras can be used to monitor these valves remotely, sparing instrument technicians from having to trek across a facility for routine data collection.

Video analytics can be used to monitor the position of a gauge needle with an alert when it crosses a given threshold.

Heat-detecting cameras can spot the early signs of equipment overheating before it is obvious to other sensors. This approach provides early warning of impending equipment failures, reducing downtime and extending the useful life of expensive equipment without requiring additional preventive maintenance staff.

EVS systems can provide visual confirmation of safety-critical situations, such as verifying that a breaker is open or closed before staffers enter an operational area. Cameras with video analytics can monitor restricted areas and alert when a worker wanders into these areas, triggering both an audible alarm and notifying the safety officer on duty.

These examples are just a starting point for integrating EVS technology into virtually any environment. While retail, educational, healthcare and energy organizations are well positioned to benefit from EVS technology, the same is true of many other industries. Manufacturers can leverage video surveillance to quickly spot issues on a production line. Logistics firms can automatically detect the arrival of important shipments. Airport operations teams can track the flow of people in the terminal and aircraft on the tarmac. The potential applications of EVS technology are virtually limitless.

CDW: We Get Security

CDW stands ready to serve as your organization's enhanced video surveillance partner. Our team of engineers, architects, and consultants have decades of subject matter expertise in physical security and are able to help you achieve your physical security objectives and optimize your use of EVS to realize additional business value.

CDW helps organizations find the right physical security solutions and services to meet their needs. Our IT consulting services team will work closely with you to determine your security needs and develop a range of EVS options that fulfill those requirements while fitting within the constraints of your budget. Our consultants are prepared to assist with site surveys, solution design, video management and access control systems, and the selection and placement of cameras and other sensors.

CDW Can Design, Orchestrate and Manage a Comprehensive Infrastructure Strategy

CDW's simple, smart, scalable and flexible services portfolio provides a fully automated and managed infrastructure across your entire network, whether on-premises, hybrid or in the cloud.



DESIGN for the Future

Consult with our team of technology experts to plan a solution that fits your unique needs and optimizes business impact.



ORCHESTRATE Progress

CDW Amplified™ Infrastructure services help you build and deploy your custom infrastructure utilizing best practices.



MANAGE Operations

Our world-class, certified staff monitors and manages your infrastructure 24/7/365 to ensure operational efficiency and security.

Sponsors



Want to learn more? Check out the Solution Spotlight “Enhanced Video Surveillance Drives Better Business Outcomes” from CDW.

CDW®, CDW.G® and PEOPLE WHO GET IT® are registered trademarks of CDW LLC. All other trademarks and registered trademarks are the sole property of their respective owners. Together we strive for perfection. ISO 9001:2000 certified MKT42701 – ©2020 CDW LLC

