INTRODUCTION: VIDEO SURVEILLANCE GOES SMART

The history of video surveillance goes back to the middle of the last century, when closed-circuit television (CCTV) systems – which primarily use cameras to deliver live video feeds to televisions – were introduced. The introduction of recording tapes (video cassettes) was the next major technological leap that enabled the storing of video feeds. The recording as well as storage of video feeds then transitioned from analog to digital formats with the onset of the digital era, significantly increasing video quality and simplifying video storage and access.

Video surveillance technology took another major leap in the current smart era, which is characterized by the advent of transformational technologies such as Internet of Things (IoT), big data analytics, smartphones, cloud computing, 3G/4G/5G networks, edge computing systems, and artificial intelligence (AI). Today, autonomous IP-based cameras have become the norm, and interconnected surveillance systems – specifically cameras, fire alarm systems, and access control systems connected to building management systems – are now commonplace. Advancements in compression technology have increased video resolutions and reduced video file sizes, while advancements in Wi-Fi and mobile networks have enabled faster data transfers and extended coverage areas. At the same time, low-power wide-area networks (LP-WANs) permit battery-operated devices to transmit low bit-rate video data over long distances, extending the potential coverage areas.

With respect to surveillance system back ends, cloud computing models now allow video data to be stored in off-premise locations, while machine learning techniques simplify and increase the effectiveness of data analysis. Computing is also moving towards the edge; IoT devices are increasingly being imbued with analytics and AI features that allow them to capture as well as create data – for instance, cameras can capture video while AI features intelligently add details about a scene (e.g., via object classification or face recognition). The proliferation and increased usage of mobile devices and the evolving mobile app ecosystems have also made remote monitoring more accessible.

The new surveillance ecosystem in the smart era is depicted in the figure below:
FIGURE 1
---
The Surveillance Ecosystem in the Smart Era

Source: IDC, 2019

BENEFITS AND USE CASES

Technology advancements have enhanced video surveillance to a significant degree. These advancements have not only introduced additional features into traditional security use cases but also created potential for a whole host of new use cases. The new security paradigm and the new use cases are dealt with in detail in the following sections.

Use Case 1: District & Building Security

The overall focus on safety and security has only increased over time. Indeed, governments across the world have mandated the use of video surveillance technologies in specific public places due to the opportunities they provide in terms of ensuring public safety. In all Gulf Cooperation Council (GCC) countries today, certain places such as hotels, shopping centers, banks, hospitals, schools, and commercial buildings must have video surveillance systems in place. For example, Dubai had mandated the use of CCTV in important commercial sectors such as hotels, financial institutions, large department stores through Law No. 24 in 2008. This law had detailed specifications on how and where CCTV systems (including the recording devices and cameras) should be provided and in what conditions. This was later amended in 2014 to extend it to ‘important complexes’ which are areas that are an aggregation of residential units or offices which includes buildings, towers and villas. All the GCC countries introduced such laws in last decade. Consequently, there has been widespread adoption of video surveillance cameras across the region; however, facility managers often implement surveillance systems simply to comply with regulations and do not realize the full potential of such solutions.

At the outset, video surveillance had one objective – to enhance the role and importance of security personnel. The smart era has taken this objective to the next level with increased levels of automation. This automation has been made possible through the combination of intelligent devices (cameras, sensors) at the front end, and software (AI-based analytics) at the back end. Together, these devices and software have the capability to ‘understand’ various elements in a video, differentiate and classify them (humans, animals, vehicles, poles, roads, etc.), and detect and track stationary and moving objects. They can also recognize faces and number plates, detect
lines on motorways, and identify various patterns. These features — coupled with rule-based engines at the back end, machine-learning capabilities that learn over time, and automated systems that can trigger specific responses — are collectively taking video surveillance to a whole new level of sophistication.

**FIGURE 2**

District & Building Security

---

**Components & Ecosystem**

- **Environment Monitoring**
- **Lifts**
- **Camera**
- **Smart Security Platform**
- **Lighting**
- **HVAC**
- **Datacenter**

**Features**

- **Object Detection & Classification**
- **Identification**
- **Facial Recognition**
- **Number Plate Recognition**
- **Motion Detection & Tracking**
- **Open Area Surveillance & Crowd Management**
- **Behavioral / Virtual Fencing & Zoning**
- **Surveillance & Alarm Management**
- **Custom Analytics & Reporting**

Source: IDC, 2019

The key features of surveillance systems in district & building security use cases include:

- **Object Detection and Classification**: As illustrated above, modern surveillance systems can identify and classify objects, recognize faces, and automatically read number plates. These features pave the way for a "teach by example" learning approach to people and vehicle classification and hierarchical labeling. Modern systems can also track people and vehicles by correlating multiple video streams and conduct automatic searches based on descriptive information.

- **Motion Detection**: Modern surveillance systems can understand typical activities in a scene and then detect and flag unusual events. They can also divide areas into virtual zones and create different sets of rules for each zone.

- **Integration with Other Systems**: Video surveillance cameras and other sensors and systems (e.g., building/facility management systems) can form larger, interconnected networks whose combined data can provide valuable insights.

- **Custom Analytics and Reporting**: Different types of users such as security officers and facilities managers can receive custom reports via surveillance dashboards. Custom analytics (e.g., footfall analyses, queue length measurements, and movement patterns) are also available to aid security planning.
Use Case 2: Operations Management

The potential for new use cases that extend beyond security is a major advantage that smart technologies have brought into the video surveillance domain. For example, an advanced video surveillance platform can improve operations management, especially in places frequented by large numbers of people. This use case has a wide range of applications across industries such as bank branches; customer service centers of government departments, telecom operators; hospitals and clinics; entertainment industry that includes exhibition centers, theme parks, museums, stadiums; etc. The section below focuses on the example of a customer service center.

A customer service center is one of the most important premises for a business — an area where the business can either impress customers with its efficiency or face criticism for poor service provision. This is especially true for enterprises with large customer bases (such as banks, telecom operators, hospitals/clinics, and public transportation providers). However, organizations have long struggled with collecting useful data that can help them make their operations efficient and service floors customer friendly.

Today, advancements in video surveillance technology can aid organizations in achieving efficiency. Video cameras, coupled with powerful analytical engines in the back end, can assess footfall, determine the time spent on queueing and receiving actual service, and identify movement patterns or incidents. Surveillance data can therefore be used to reduce waiting times, enhance employee productivity, or redesign the service floor for better service provision. For most customer service centers, video surveillance is mandatory. The use of the right video surveillance solutions can enable organizations to derive more value from existing and planned investments.

FIGURE 3

Customer Service Center: Operations Management

Source: IDC, 2019
Use Case 3: Sales Enhancement and Customer Experience in Retail Stores

Retail stores in the Middle East are going through a turbulent period due to uneven sales and cutthroat competition from new stores and ecommerce players. These retail stores are struggling to achieve their sales targets and increase customer footfall while keeping costs low.

At the same time, the use of video surveillance in retail stores has become common; most surveillance is focused on curbing shoplifting and enhancing security. However, surveillance technology has the potential to offer long-term benefits in areas such as store design, product placement, and in-store promotions. These benefits will in turn enhance customer satisfaction and boost sales. For retailers, the in-store experience is one of the key aspects that drives customer satisfaction and better sales. The placement of products and in-store promotional materials, the amount of time spent standing in queues, and the availability of employees are all crucial parts of the overall customer experience. Video cameras and analytical engines can help retail stores to conduct footfall analyses, investigate movement patterns, determine the time spent in queues, and track employees. Altogether, these capabilities can help store managers make real-time decisions about product placement and promotion management; they can also be used to enhance store design as well as employee productivity.

FIGURE 4

Retail Shop: Sales Enhancement and Customer Experience

Source: IDC, 2019
The new smart video surveillance ecosystem and the potential new use cases present significant opportunities and advantages to organizations that are ready to embrace new platforms or upgrade existing systems. However, the new technology paradigm – with its myriad of connected things and ever-changing regulatory requirements – also poses significant challenges. These challenges mostly fall under four broad areas:

- **Storage:** First and foremost, the vast amount of data generated by connected things is a key challenge. By 2025, IDC expects the IoT ecosystem to generate 79.4 ZB (or 79.4 billion terabytes) of data. This data explosion will largely be driven by video surveillance use cases, which will account for almost 90% of all generated data. As such, how to store, scale, and manage this data is an important concern. This data is the fuel that flows through the entire surveillance system and feeds various components, smartening video surveillance and enabling new security use cases.

- **Computing:** The days in which video surveillance was simply about capturing data from cameras, or security personnel either actively monitoring screens or accessing recording data when needed, are long gone. Surveillance systems are now automated and smart; they can analyze data in real time and automatically provide alerts to security personnel, thereby making security monitoring much more effective and intelligent. Importantly, the gap between the growing volume and sophistication of data on one hand and the transformation required to make that data useful and valuable to organizations on the other is narrowing. However, this process needs software with significant analytical capabilities and a staggering amount of computing power. Tackling this problem will require organizations to make significant investments that may require a long term to generate ROI.

- **Cybersecurity:** According to the results of IDC’s Middle East CIO Survey 2019, maintaining security remains the top technology-related priority of CIOs in the region. Indeed, security is a key challenge organizations are facing considering the rapidly growing sophistication of cybercriminals, the expanding number of environments and devices to protect, the rising number of security tools and new compliance regulations, and the scarcity of qualified information security professionals. However, security solutions are also evolving to address these challenges. The new cybersecurity model uses IoT devices and AI-powered analytics to collect and index sources of information, derive insights from threat dynamics, and initiate proper responses to mitigate threats and harden the network. In fact, IDC predicts that 50% of legitimate security alerts will have automated responses by 2021 (i.e., responses produced without human intervention). With increasing numbers of endpoints, organizations are faced with new cybersecurity challenges and threats, but many are not equipped with the latest security solutions required to address them.

- **Regulations:** Rapidly evolving technologies have created major opportunities for public safety, but have also raised cybersecurity and privacy concerns. Public safety is a major aspect that needs to be addressed; accordingly, governments around the world are taking advantage of advancements in video surveillance to bolster civilian security. As noted earlier, video surveillance in certain areas is now mandatory in many countries, including all GCC countries. In addition, government regulations keep evolving – for example, stipulations that require new areas to be added to a surveillance system are routinely introduced. Moreover, additional stipulations can extend retention time (i.e., the minimum duration that a recorded feed must be kept) or require certified providers to install/manage surveillance platforms. With respect to the ever-growing privacy concerns, legal guidelines such as the General Data Protection Regulation (GDPR) have also come to the fore. Unfortunately, the existing regulatory paradigm makes it difficult for organizations to keep up with the breakneck speed of advancements and remain compliant; this model may also force organizations to underutilize technology or keep outdated platforms.
THE APPROACH MATTERS: THE BENEFITS OF CLOUD

Since its advent in the last decade, cloud computing has emerged as the essential foundation for digital innovation in every industry and the preferred services and information consumption model for businesses. Cloud platforms have become the primary launchpads for digital technology innovations in AI, security, digital infrastructure, data services, IoT services, and more. According to IDC’s 2018 Global CloudView Survey of more than 5,700 firms, 81% of companies currently use or plan to use public cloud, and 86% private cloud. This represents an increase of more than 30% from the previous year’s results.

Traditionally, organizations have taken an on-premise approach to video surveillance by locally maintaining all components, hardware, software, and services. This approach involves complex and lengthy procurement and implementation cycles, requires strong technical skills, and demands high capex outlays. In such implementations, scalability is a major issue as incremental additions are required for storage purposes. Periodic updates are also needed to cope with technological changes and evolving security threats. In addition, there is a risk of losing the locally stored data. Access to data can also be restricted to on-premise or specific platforms via this approach. To address these prevailing on-premise challenges and take advantage of smart video surveillance, organizations need to adopt a cloud-based approach.

FIGURE 4

The Cloud Approach - Foundation to Digital Transformation

By 2021, over 90% of enterprises worldwide rely on a mix of on-premises / dedicated private clouds, several public clouds, and legacy platforms to meet their infrastructure needs.

By 2024, 70% of enterprises reduce the cost and complexity of customizing enterprise applications by increasing spending on industry-specific SaaS applications and platforms.

Solution

Challenges

- Storage: Data explosion
- Computing: Need for high computing power
- Regulations: Changing regulations; privacy
- Security: Evolving threat landscape

Source: IDC, 2019

A cloud-based approach provides the flexibility to move storage and analysis off-premise, either via centralized or hybrid models, depending on the requirements:

- In the centralized model, processing is carried out on a central server. Because centralized servers have strong computational power, larger memory capacities, higher speed access to databases, and extensive computer vision machine learning frameworks, they are particularly suitable for running complex analytics algorithms on multiple video streams.
The hybrid model combines edge-based and server-based systems and substantially reduces the load on back-end servers and networks. For example, the edge-based component can carry out face detection (i.e., classifying a part of a scene as a face) while the server-based system can handle facial recognition and other analytical processes. This capability allows smaller systems to run intelligent video applications and scale in a distributed manner. IDC predicts that, by 2022, more than 40% of organizations' cloud deployments will include edge computing to address bandwidth bottlenecks, reduce latency, and process data for decision support in real time.

The cloud-based approach is a scalable, future-proof, on-demand, and pay-as-you-go model that significantly lowers upfront costs and reduces the hassles of technology management. This approach makes use of the existing network infrastructure and storage devices and has the flexibility to add new hardware infrastructure. Customers can use existing cameras, source new cameras, or access cameras as part of an as-a-service model. An end-to-end service platform covering connectivity, video stream life-cycle management, and monitoring platforms can be commissioned through the cloud-based approach. In this way, organizations can adapt quickly to changing market conditions, regulatory changes, technology evolutions, or shifts in the threat landscape.

INTRODUCING NXN’S SMART VIDEO SURVEILLANCE SERVICE

NXN's Smart Video Surveillance Service (SVSS) is a turnkey subscription-based video-surveillance-as-a-service (VSaaS) solution featuring advanced video surveillance management and analytics capabilities that cater to the evolving surveillance needs. The solution, which is a product of NXN's extensive experience in the Smart City and IoT arena, is built on the company's flagship digital transformation (DX) platform, DNX. Through SVSS, NXN provides an end-to-end video surveillance service that covers devices, connectivity, storage, processing, analytics, video stream life-cycle management, and monitoring and visualization dashboards.

NXN's SVSS platform does not "rip and replace" existing CCTV, access control, building management systems, and sensors; rather, it augments existing infrastructure by exchanging data and sending actionable control commands and dispatch notifications in accordance with configured auto-processing rules and response action plans. The platform collects and correlates events and alarms from disparate security devices and information systems to produce one common operating picture using open, industry-approved standards. SVSS converts massive amounts of data into meaningful and actionable information by filtering and correlating the data based on context, time, location, duration, frequency, and type. The specifics of these criteria are defined by the user organization's risk policy, standards, and compliance requirements.
The system also supports advanced features in video surveillance, including differentiation and classification of objects, detection, and tracking (e.g., facial recognition, number plate recognition, motion detection, identification of patterns, counting). But what differentiates NXN's SVSS is the features that take the solution beyond the traditional video surveillance realm. For example, the system handles data from multi-disciplinary sources, combines it with computer vision machine learning frameworks and artificial intelligence applications to generate advanced data analytics. The hybrid edge-cloud mechanism gives the flexibility for this to happen at the back end or the edge.
The company offers multiple deployment models suiting the needs of each customer. The customer has the flexibility to use existing infrastructure (such as cameras); however, NXN provides the option to avail new cameras as part of its service. A small enterprise can opt for a cloud-based model in which on-premise cameras get direct connectivity to an NXN datacenter with no local storage implications, real-time and remote internet-based viewing options, and a pay-as-you-use structure for archived footage. Conversely, a large enterprise could opt for a hybrid model in which recorded footage is stored locally for a stipulated duration before being archived in an NXN datacenter.

NXN's SVSS solution also offers telecoms and IT service providers an opportunity to expand their portfolios. For example, Zain Kuwait is offering NXN's VaaS solution to local customers. The VaaS solution is the latest addition to the operator's portfolio that focuses on the small and medium-sized business (SMB) market. Zain Kuwait is now able to offer this end-to-end surveillance solution, which includes connectivity, cameras, storage, and operations components, to SMBs. This allows SMBs to benefit from a pay-as-you-use model.
CONCLUSION

The video surveillance market continues to grow rapidly as the importance of using technology for security becomes more and more apparent. The growing ecosystem of “things”, the vast amount of data generated, and rapid advancements in machine learning make video surveillance an essential area of focus for large and small enterprises alike. The use case for video surveillance has gone beyond security; it now includes options that can directly affect business aspects such as customer satisfaction, operational efficiency, product/service development, and revenue enhancement. Incidentally, these aspects are top priorities for any enterprise. At the same time, evolving regulations and the growing threat landscape makes video surveillance a challenging area to address.

Organizations increasingly demand solutions that enhance operational efficiency, employee productivity, and effectiveness. Accordingly, the future of enterprise applications is moving toward cloud-native architecture as organizations improve IT processes and business agility. IoT and AI technologies enable exponential increases in data and support real-time information delivery and advanced analytics, while distributed computing models facilitate local storage of data and can generate greater computational power.

By taking a cloud/hybrid approach, IDC believes that organizations can address the challenges posed by the new video surveillance paradigm and take advantage of the new opportunities brought forth by the smart era. NXN's SVSS solution, which utilizes this approach, is backed by feature-rich technology and industry expertise. The solution can therefore help enterprises get the best out of video surveillance, future-proofing their operations without significant capex outlays.
About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Middle East/Africa

Level 15, Thuraya Tower 1
Dubai Media City
P.O. Box 500615
Dubai, United Arab Emirates
+971.4.3912741
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2019 IDC. Reproduction without written permission is completely forbidden.