ANVIZ
Secure Workplace, Simplify Management

How Edge AI + Cloud Changes Security Systems

Why Modern Business Security System Architectures Should use an Edge AI + Cloud-based Platform

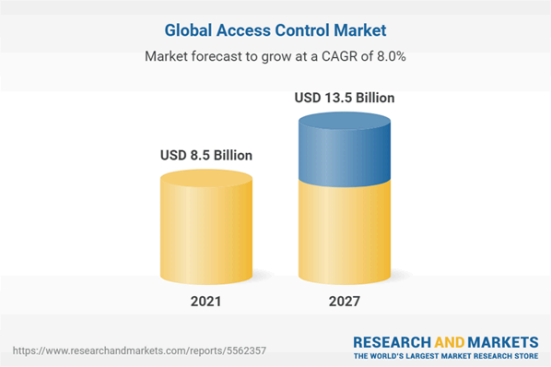
Catalogue

Abstract

Recent technological advancements have made it easier to reduce risk and safeguard your workplace. More businesses have embraced innovation and found solutions to workforce time management and space management problems. Especially for small modern businesses, having the right smart security system can make all the difference in keeping your workplace, and your assets,safe. Also, it helps to control and improve customer service, and monitor employees' performance.

Access Control & Video Surveillance are two important parts of smart security. Many people are now used to entering the office using face recognition and checking workspace security with video surveillance.

According to the ResearchAndMarkets.com's report, the Global Video Surveillance Market is estimated to be USD 42.7 Bn in 2021 and is expected to reach USD 69.4 Bn by 2026, growing at a CAGR of 10.2%. The Global Access Control Market reached a value of US$ 8.5 Billion in 2021. Looking forward, the market is expected to reach US$ 13.5 Billion by 2027, exhibiting at a CAGR of 8.01% (2022-2027).



Global Access Control Market

Global Video Surveillance Market

Today's modern businesses have an unprecedented opportunity to experience the benefits of smart security solutions. Those who are able to embrace new developments in security system architectures could address security risks at every turn and reap greater benefits from their security system investments. This white paper shares the reasons why an Edge AI + Cloud-based platform should be the first choice for modern businesses.

Edge Computing + AI = Edge AI

In an ideal deployment, all workloads would be centralized in the cloud to enjoy the benefits of scale and simplicity from cloud-AI. However, concerns from modern businesses about latency, security, bandwidth, and autonomy call for an artificial intelligence (AI) model deployment at the Edge. It makes complex analytics such as ANPR or AI-based detection affordable for clients who do not intend to purchase a sophisticated AI local server and spend time configuring it.

Unlike Cloud computing, Edge computing is a decentralized computing service that includes storage, processing, and applications. The Edge refers to servers that are located regionally and are closer to endpoints, like surveillance cameras and sensors, where the data is first captured. This method reduces the amount of data that must travel over the network so causing minimal delays. Edge computing is thought to improve Cloud computing by performing Data Analytics as close as possible to the data source.

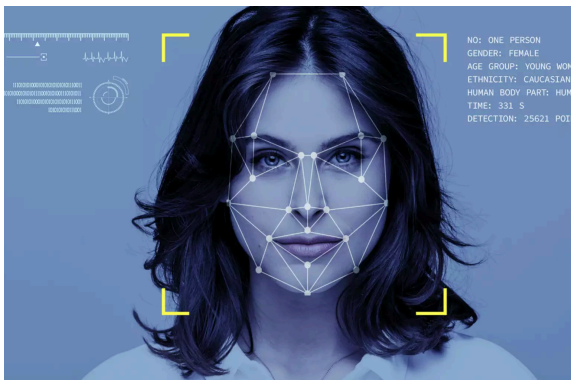
Edge AI is essentially AI that utilizes Edge computing to run data locally, thus taking advantage of the benefits Edge computing offers. In other words, the AI computation is done on devices near the user at the edge of the network, close to where the data is located, rather than centrally in a cloud computing facility or private data center. The devices have the appropriate sensors and processors, and do not require a network connection to process data and take action. Therefore, Edge AI provides a solution to the shortcomings of cloud-dependent AI.

Many leading physical security vendors have already been using edge AI in access control and video surveillance to improve efficiency and reduce the overall cost of production/ service. Here, edge AI will play a key role.

• AI in Smart Security Terminals

As Neural networks algorithms and related AI infrastructure develop, Edge AI is being introduced into commercial security systems.

Many modern businesses are using object recognition AI embedded in smart terminals for workplace safety and security. Object recognition AI with a strong neural network algorithm is able to easily spot elements in any video or image, such as people, vehicles, objects and more. Then it is able to analyze and bring out elements of an image. For example, it can detect the presence of suspicious individuals or vehicles in a sensitive area.



Applying facial recognition to access control solutions is also trending, especially in the current modern business world, where there is widespread concern about efficiency and cost. Because of what we've learned during the pandemic, there is increasing demand to remove 'friction' from the user experience.

Facial recognition AI embedded in modern access control and surveillance cameras is the common use of this technology in security.

It identifies a person's facial features and converts them into a data matrix. These data matrices are stored in the Edge terminals or cloud for analysis, data-driven business decisions, and improvements in security policy.

• Edge AI in Access Control

Edge facial recognition is a technology that relies on both Edge computing and Edge AI, which dramatically improves the speed, security, and reliability of access control devices. When used for access control, Edge facial recognition compares the face presented at the point of access to a database of authorized persons to determine whether there is a match. If there is a match, access is granted, and if there is no match, access is denied and a security alert can be triggered.

Fewer technical failures

In the case of Edge facial recognition, this means that the power to recognize and process images is embedded, taking place on local devices. This allows devices to run quickly and with extreme precision as they aren't subject to network-related problems associated with cloud computing, making them subject to fewer technical failures.

Decreased chance of information theft

Facial recognition that relies on Edge computing and Edge AI can process data locally (without sending it to the cloud). Because data is much more vulnerable to attack during transmission, keeping it at the source where it's generated dramatically reduces the chance of information theft.

Improved threat detection by liveness detection

Edge AI is capable of differentiating between real-life human beings and non-living spoofs. Liveness detection on the Edge prevents face spoofing attacks using 2D and 3D (static or dynamic image and video footage).

Edge facial recognition can also recognize faces from a wide range of angles, adding to the convenience for the user. It is also not easily affected by accessories that might cover the face, such as hats and glasses.

• Edge AI in Video Surveillance

In essence, the Edge AI solution puts a brain into every camera connected with the system, which is able to quickly analyze and transmit only relevant information to the cloud for storage.

In contrast with a traditional video security system which moves all data from every camera to a single centralized database for analyzing, Edge AI makes the cameras smarter – it analyzes the data right at the source(the camera) and only moves relevant and important data to the cloud, thereby eliminating significant costs for data servers, additional bandwidth, and infrastructure costs usually associated with high-volume video collection and analysis.

Lower bandwidth consumption

A major benefit of Edge AI is bandwidth usage reduction. In many installations the network bandwidth is a limitation and therefore the video is heavily compressed. Doing advanced video analytics on a heavily compressed video reduces the accuracy of the analytics, and therefore processing on the original data at the Edge has clear advantages.

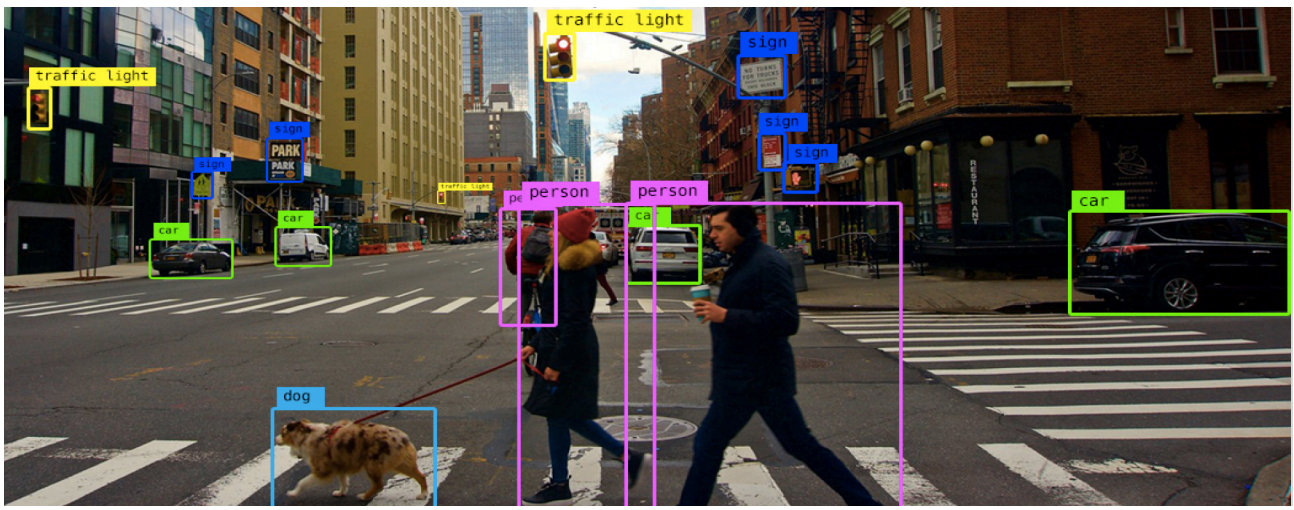
With AI algorithms woven into Edge devices, only selected information such as an individual or a vehicle in a video image will be extracted and sent. This enhances the transition efficiency significantly and reduces the network bandwidth load, while sustaining high quality and accuracy.

Faster response

Another major benefit of computing in the camera is latency reduction. Rather than sending the video to the backend for processing and analysis, a camera with facial recognition, vehicle detection, or object detection can recognize an unwanted or suspicious person and immediately automatically alert security staff.

Labor cost reduction

Meanwhile, it allows security staff to focus on more important things/incidents. Tools like people detection, vehicle detection, or object detection can automatically alert security staff of events. Where live monitoring is deployed, staff can do more with less people by filtering camera feeds without specific activity and leveraging custom views to only see certain locations or cameras.



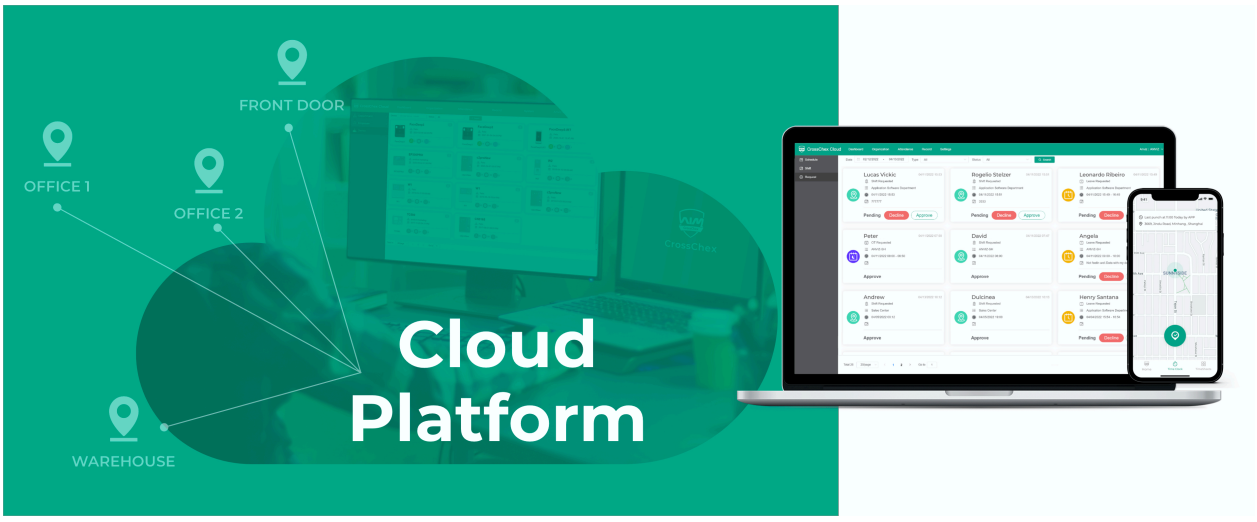
A Cloud Platform for Edge Core Data Storage and Processing is a Must

As the number of recordings from surveillance cameras is growing every day, so the problem of storing such large-scale data archives is becoming important. One alternative to local storage would be to transfer video to a cloud-based software platform.

Customers are now becoming more and more demanding about their security systems, expecting almost instantaneous responses to their concerns. Meanwhile, they also expect the system has typical benefits associated with any digital transformation - centralized management, scalable solutions, access to tools that require powerful processing, and reduction in costs.

A cloud-based physical security system is quickly becoming the favored option as it becomes possible for organizations to process a large amount of data in the cloud with low cost and high management efficiency. By moving costly infrastructure to the cloud, organizations can typically see a reduction in the total cost of security by 20 to 30 percent.

With the rapid growth of cloud computing, the marketplace and the ways security solutions are managed, installed and purchased is rapidly changing.



Cloud-based Access Control Systems

A cloud-based access control system works by storing data in the cloud rather than an on-site server. As a result, you can access your system's data from anywhere using any device n an internet connection. Cloud-based systems can also undergo routine software updates remotely. They are cost effective, robust, extremely secure, reliable, and positive for both the integrator and end user.

One console to manage multiple sites

Cloud allows organizations to centrally manage their video surveillance and access control across multiple locations from one pane of glass. This makes it easy to control cameras, doors, alerts and permissions of their buildings, warehouses, and retail stores from anywhere in the world. Since data can be easily shared through the cloud, information can be accessed quickly.

Flexible user management for increased security

Admins can revoke access at any time, from any location, providing peace of mind in the event a badge is lost or stolen or on the rare occasion that an employee goes rogue. Likewise, admins can temporarily grant access to secure areas as needed, streamlining vendor and contractor visits. Many systems also feature group-based access control, with the ability to designate permissions by department or floor, or set up a hierarchy that allows certain users into restricted areas.

Scalable operations

Security can be easily scaled by centralizing everything through the cloud. An unlimited number of cameras and access control points can be added to a cloud platform. Dashboards help keep data organized. There is a solution for every scenario as you scale, such as gates, parking lots, warehouses, and areas without network access.

User convenience

A cloud-based system is also designed for convenience, as it allows employees and visitors access using their mobile devices. This is convenient for employees as their key is seamless, portable, and already with them at all times. It's also convenient for businesses, as they avoid the hassle and cost of printing new "keys" for employees and visitors.

• Cloud-based Video Surveillance Systems

A cloud-based video security system is a type of security system that records videos over the Internet instead of recording them on an on-premise storage device. They consist of AI video camera endpoints that connect to your cloud security provider via the Internet. This cloud provider is responsible for storing your video data and can be configured to send alerts, notifications, or even record footage when motion events are detected.

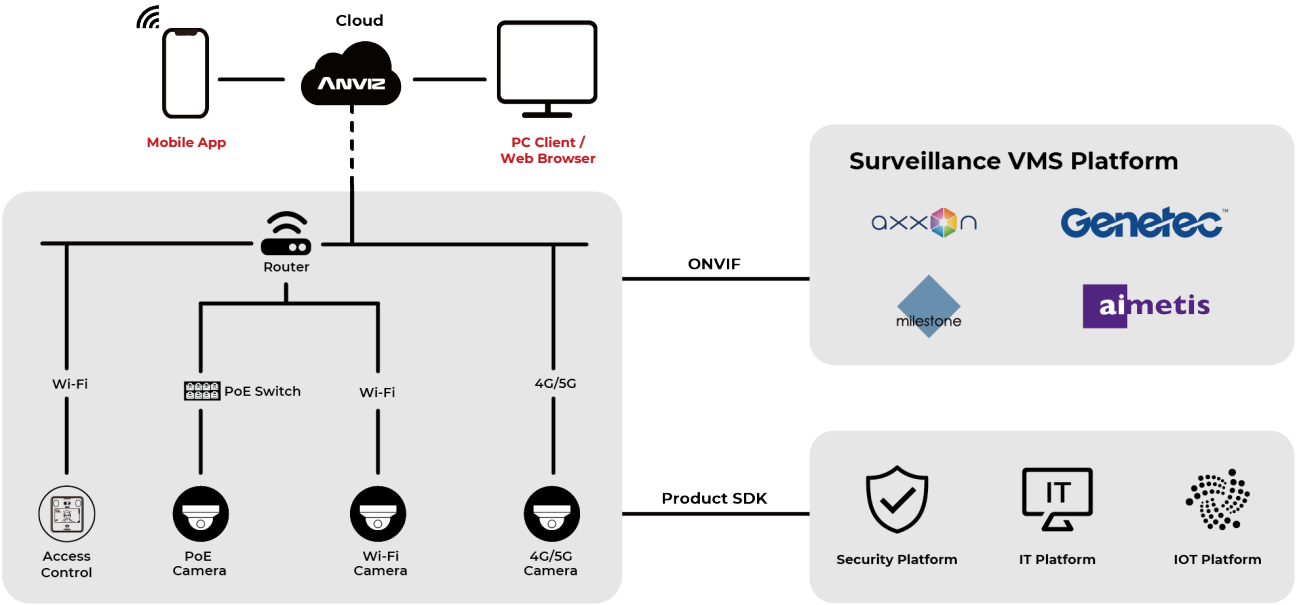
The principle of cloud storage has made it easier to create a video surveillance system for commercial purposes. It's now possible to store an unlimited amount of footage without needing additional hardware or worrying about running out of physical space.

Remote access

In the past, you often needed physical access to the security system. By connecting your CCTV systems to the cloud, authorized users can access and share footage at any time from anywhere. The main benefit of this type of system is it gives your business access to all the recordings 24/7 from anywhere - even when you're not at the office!

Easy maintenance and cost-effective

Moreover, cloud video surveillance services like the recording's storage and distribution are automatically updated, without user involvement, which is significantly simpler for users. Cloud video storage is easy to set up; it does not require hardware or IT and security specialists to keep the system up and running.



• Benefits of Cloud-based Security System for Solution Integrator and Installer

Installation and infrastructure

Both the physical product and labor costs of installing an IP-based access control solution hosted by the cloud are significantly less expensive. No physical server or virtual server is required, resulting in cost savings of $1,000 to $30,000 depending on the size of the system.

The installer does not have to install software on the physical server, configure the server in the customer's premises or concern if the new piece of hardware and operating system comply with the customer's IT policies.

In cloud access control, the access control hardware can be installed and pointed immediately to the cloud, tested, and configured. By using a cloud service, the installation is shorter, less disruptive, and requires less infrastructure.

Lower ongoing maintenance costs

Once an access control system is installed, there are ongoing costs to maintain it. This includes software upgrades and patches, ensuring proper operation of the hardware, and soon. With a cloud-based access control system, nearly all of these maintenance tasks can be carried out from any device at any time. Access control Software as a Service (SaaS) providers typically include all feature upgrades and software updates in their annual software costs.

In addition,the customer's information is commonly backed upon multiple physical servers throughout the cloud infrastructure, so there is no need for the integrator to go on-site, provide backups, install upgrades, and then configure the appropriate updates to the services. Integrators that have deployed cloud systems as a result are seeing increased profits, greater customer satisfaction, lower overhead costs, and greater customer retention.

Integration

Open application programming interfaces (APIs) enable a combined access control and intrusion system to integrate with video, elevators, and other systems; more systems can be integrated with intrusion than ever before.

Any integration with third-party technologies is simpler in a cloud-based platform! Open systems (using APIs) make it easy and intuitive to integrate with third-party systems and products, such as common business communication tools, like CRM, ICT and ERP.

Common Challenges Modern Businesses face in installing Edge AI + Cloud platform in Video Surveillance Security

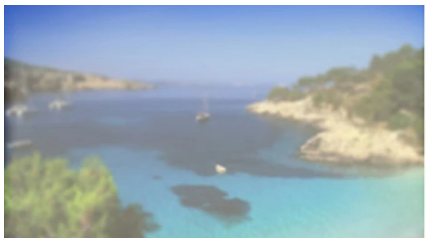
Poor flexibility

In the AI video surveillance sector, algorithms and devices are often in a highly bound state. But in practical applications, a video surveillance system requires a certain degree of flexibility, which means the same camera often be used in different scenarios with different algorithms.

With most current AI cameras, it is difficult to replace algorithms once bound to a specific algorithm. Thus, companies have to spend more on new equipment to solve problems.

AI accuracy problems

AI implementation in a video surveillance system is greatly affected by both computation and images. Due to the hardware limitations and real-world environment's influence, the image accuracy of AI surveillance systems is often not as ideal as in the lab. It will have a negative effect on the user experience and the actual use of data.



The target devices for edge AI are often neither powerful nor fast enough to fully meet the memory, performance, size, and power consumption requirements of the Edge. The limited size and memory capacity would also affect the selection of machine learning algorithms.

Data security concerns

How to provide sufficient security mechanisms to protect user information and meet compliance requirements is the primary problem that a cloud-based security system needs to solve. Reliable hardware with dependable software is great, but many people may be concerned about data loss or disclosure when the terminal uploads data to the cloud.

• The Solution

Anviz IntelliSight solution can realize a variety of standard front-end AI applications with the powerful Qualcomm's latest 11nm, 2T computing power NPU. At the same time, it is also able to complete faster, efficient professional data application due to Anviz's cloud-based software platform.

This method is cost-effective and simple, as it does not require any additional equipment. The only physical hardware involved is Anviz smart IP cameras, recording and sending data to the cloud. Video recordings are stored on a remote server, which can be accessed via the internet.

High flexibility

The Anviz video surveillance solution - IntelliSight adopts a software and hardware separation model, which can realize flexible replacement of various AI algorithms. Anviz terminals are pre-installed with a variety of different algorithm sets, and different algorithm applications can be activated as needed. It greatly improves the management efficiency and usage time of AI cameras and reduces the overall investment cost.

Stable accuracy

The neural network AI algorithm based on image recognition can effectively improve the deep learning ability and algorithm accuracy. Anviz AI technology in cameras combines image recognition technology. It firstly determines the dynamic status of the image, adjusts the image parameters for optimization to enable AI calculation, and then perform AI analysis. Therefore, the feedback of AI data results is always carried out under a unified image standard, which greatly improves the accuracy of the AI.

Reliable data transfer

Anviz advanced cloud solution is cyber secure with end-to-end encryption, using AES255 and HTTPS Encryption algorithm to protect data security as the Edge terminal communicates with the cloud. Further, the whole process of cloud communication is based on the Anviz-owned Control Protocol, which also improves the efficiency of the data transmission.

Linkedin	https://www.linkedin.com/company/1714290
Twitter	https://twitter.com/AnvizGlobal
FaceBook	https://www.facebook.com/AnvizHQ
Instagram	https://www.instagram.com/anvizglobal

Anviz Global
32920 Alvarado-Niles Rd Ste 220, Union City, CA 94587
Toll-free: 1-855-268-4948 | sales@anviz.com | www.anviz.com