Though they may sometimes elicit a hectic and fast-paced experience, airports are a necessary cornerstone of traveling for many people around the world. Whether they represent the ability to see family, the need to attend a business event, or the chance to get away on a relaxing vacation, airports are central to allowing travelers to get from one destination to the next.

In 2019, more than four billion scheduled travelers passed through the world's airports, and that number is projected to grow. As the flow of travelers increases, airports are facing many new challenges. Passengers, by nature, are highly diverse, transient and in continual motion. As a result, airports are taking on greater responsibility of ensuring that people arrive and depart in a timely — and safe — manner.
Effective security operations

Effective security operations are therefore critically important to allowing these entities to protect what matters most. Unfortunately, this is not an easy task, as airports have evolved from traditional ports-of-call to highly complex environments. With the introduction of shopping, dining, interconnected rail and more amenities, they are seeing many of the same challenges facing cities. That includes theft, fraud, medical concerns and even domestic violence spilling over into facilities that are already popular targets for bad actors.

They are seeing many of the same challenges facing cities

The various threats that airports face on a daily basis present the potential for extreme damage. Any type of incident can carry significant risk to people, assets, passenger traffic, and brand reputation. Traditional security risks in the airport ecosystem, such as theft, violence, terrorism, and insider threats, continue to evolve, while overarching cyber attacks targeting physical security systems have also become more prevalent.

Airport Industry Demands

Aside from the constantly shifting risk landscape airports face, they also maintain a unique set of needs due to the high-level nature of the overall operation, such as:

- **Constant surveillance.** Airports, like many other transit hubs, utilize systems and technologies that must function constantly in order to keep passengers, employees, and environments safe 24 hours a day, 7 days a week, and 365 days a year. The ability to monitor device health is instrumental in preventing equipment failures as well as ensuring that no suspicious behavior goes unnoticed.

- As airports grow and change with the addition of new shops, terminals, or runways, they also need a set of security solutions that can easily adapt and incorporate new protective infrastructures.
Coordinated security. The societal growth of at-your-fingertips accessibility and mobile capabilities increases convenience, but with this connectivity comes an expanded risk for threats and breaches. Security is no longer limited to just physical assets; network elements must also be considered to ensure comprehensive coverage throughout an airport’s infrastructure.

Data collection. Data that is derived from internal and external threat intelligence efforts plays a significant role in mitigating threats, but the sheer amount of data far outweighs the ability of many airports to organize what’s collected and make it actionable.

The Answer: Intelligence-Powered Solutions

The complex risks, demands, and challenges that airports must contend with call for exceptionally sophisticated and coordinated security strategies that leverage intelligence-based solutions. A traditional security system is not enough for such a high-leverage atmosphere; airport security operators require the greatest level of insight and information possible to ensure protection for travelers and staff at all times.

Airport security operators require the greatest level of insight and information

At the core of an intelligent airport security system must exist a video-based security operations center (SOC). Operators need to be able to track incoming data and identify relevant information on a daily basis, but this can become challenging given the number of security systems and sensors that are typically integrated within an SOC, such as video surveillance, access control, perimeter detection, PSIM software, and more.

Operators require solutions that integrate the existing controls of a security operation into a single view, assimilate analytical data, and provide critical insights to empower personnel to manage and respond to situations efficiently and effectively. This can be achieved through an intelligent SOC, giving operators real-time visibility into security system information and analytics that facilitates a proactive approach to security rather than reacting after the fact. Operators
therefore benefit greatly from increased insight and the ability to see both the security and business sides of airport operations, from passenger and employee identification to cargo handling and flight coordination.

### Essential Intelligent SOC Components

Because airports are such vast, fast-paced environments with several elements to consider when it comes to safety, an intelligent SOC in these facilities must incorporate various levels of intelligent technology, such as:

- **Video management software (VMS).** A data-driven security management and response system that leverages advanced artificial intelligence (AI) and predictive analytics is critical for viewing airport operations and investigating potential vulnerabilities or threats. When integrated with components such as dynamic GIS maps and event management, airport security teams can gain full situational awareness and control with the intelligence to act as needed.

- **Emergency dispatch and response.** In the event of a security incident, airports need to share insights in real time between dispatchers, first responders, and other aligned stakeholders. Next-generation mobile technologies within an intelligent SOC can enable operators to see the full picture of both the situation and the organization’s response team, helping to facilitate immediate action and informed decisions.

- **Integrated security operations.** As mentioned previously, today’s airports are forced to look beyond the traditional physical security threats of the past and incorporate the element of cyber risk. This means that an intelligent SOC must also consider web-based vulnerabilities, such as through social media monitoring and geo-fenced surveillance and integrate this information within the guidelines and techniques that are being used to secure the airport in a physical sense.

The deployment of intelligent security solutions in airport environments helps streamline all aspects of security management while enabling data analysis to ensure day-to-day airport operations run smoothly. In the end, these facilities become more prepared to deal with incidents proactively while providing a positive experience for travelers. As airports look to draw more
passenger traffic and expand in scale, selecting security solutions powered by sophisticated intelligence and analytics helps protect what matters most: people, property, and the continuity of operations.

Author Profile

Alan Stoddard
You may also be interested in...

**Fast And Accurate, Rapiscan’s CT Scanning Improves Airport Baggage Scr...**

Using computed tomography (CT) security technology for cabin baggage screening at airports can eliminate the need for passengers to remove l...

**How A Leap Year May Impact Your Access Control System**

Leap years occur every four years as a way to help synchronize the calendar year with the solar year, or how long it takes the Earth to orbi...

**What Is Artificial Intelligence And Should You Be Using It?**

Artificial Intelligence. You’ve heard the words in just about every facet of our lives, just two words, and they’re quite possib...

**Identiv Unveils Cloud Access Control and Frictionless Mobile Solution**

Even though ISC West 2020 was canceled, many of the product introductions planned for the trade show still happened. For example, physical s...