Kim Rahfaldt, Public Relations Manager, AMAG Technology, Talks About “How to Overcome Airport Security Challenges”

“In The Boardroom” on SecuritySolutionsWatch.com

Kim Rahfaldt, Public Relations Manager, AMAG Technology - A G4S Company

NEW YORK, NY, USA, March 13, 2018 /EINPresswire.com/ -- Kim Rahfaldt, Public Relations Manager, AMAG Technology, a G4S Company, joined us “In The Boardroom” to discuss airport security, challenges and solutions.

“No matter the size, airports are responsible for the security of all workers who are employed within their walls, on the tarmac, and grounds. The challenge is ninety percent of those people don’t work for the airport. They work for the airlines, TSA, or different vendors that reside as tenants within the airport.

Airports need to provide a friendly and efficient experience for their tenants. They need to ensure the different employees (identities) are properly vetted and managed throughout their lifecycle. Additional challenges include the use of multiple disparate systems across an airport plus the rules and regulations that must be followed. How can airports provide a high level of customer service for their tenants, meet compliance regulations and ensure the safety and security of everyone?

Onboarding
The faster an airport can onboard a new employee, the happier the tenant. When a new employee is hired, they get assigned to an airport and need a badge. The onboarding process is usually manual, and requires employees to make multiple trips to their airport to answer questions, get a background check, get fingerprinted, go through training, etc. Most of the time, the onboarding officer has to work in several different systems to complete the onboarding, which is cumbersome and error prone. Airports get pressured to quicken this process, and have an opportunity to show value to their tenants by getting new employees badged and out to work quickly. By streamlining the onboarding process using an identity management system, the procedures are automated and the airline employee starts work faster. What used to take weeks, now takes days, plus automated processes also free up staff time, saving money.

Airports are highly regulated, and employees need to pass background checks and have a certain level of insurance to work in highly restricted areas like the Security Identification Display Area (SIDA). An identity management system can automate and streamline compliance requirements, ensuring the airport will not fall out of compliance. Built in reporting features provide pre-configured

reports to streamline employee audits.

Unified Security
In the Security Operations Center, security officers monitor cameras that integrate with the access control system. When an alarm occurs, the video immediately pops up so the officer can see what is happening and respond quickly. Workflow modules outline what steps must be taken to address the alarm, which ensures the proper procedures are followed and quick action taken. Tools that allow officers to manage access control and video functions from one screen also aid in the response and provide a higher level of security. The ability to address alarms and videos from one screen along with a workflow aid provides unified alarm management and streamlines the process around what happens when an alarm comes in as officers receive, review and respond.

As alarms occur, security officers need to manage and document those incidents. Officers can investigate incidents and build a case when warranted using incident and case management software. The analytics uncover inefficiencies in processes and show where the airport can streamline to save money.

> We are honored to have Kim Rahfaldt, Public Relations Manager, AMAG Technology, a G4S Company, join us “In The Boardroom” to talk about airport security, challenges and solutions.”
>
> *Martin Eli, Publisher*

Using a holistic, unified approach can automate processes around access control, video verification and alarm management, which improves security.

Multi Factor Authentication
In most markets, multifactor authentication is used on a fraction of the doors. In the airport environment, multifactor authentication is used throughout the airport. Every employee must present a badge and enter a PIN. If an employee loses a badge, a perpetrator cannot open a door without the PIN. This is especially critical on the SIDA side of the airport where tarmac access is available.

Compliance
Employees who work on the tarmac must have a large amount of insurance. If an airline employee’s insurance lapses, but they still have access, the airline would have to pay a big fine. An identity management system allows the airlines and other tenants to automatically track when insurance premiums are due and when background checks need to be performed. By automating these processes, airport tenants know who can be where and when, when certifications, insurance premiums or background checks are set to expire, and can renew premiums and conduct a background check at the scheduled time. This keeps the airport in compliance, mitigates risk, and saves money.

Sonoma County Airport
Charles M. Schulz - Sonoma County Airport is located in Santa Rosa, California. When Alaska Airlines began service, officials realized the airport was not equipped to handle current security requirements and the increased number of passengers. The airport received funds to remodel and expand the passenger terminal, and decided to upgrade their security system.

The airport installed an access control system with integrated video to secure its three buildings and 12 vehicle gates. The integration between the controllers and card readers provided a solution that reads the Federal Aviation Administration's government issued ID cards. They needed to meet TSA requirements, and provide two levels of access for the terminal, remainder of the airfield, general aviation and cargo areas (SIDA and AOA). They needed to demonstrate to TSA who was in the building and when, and pull up that history when asked to meet compliance.

Anyone entering the vehicle gates must have an Airport Operations Area (AOA) badge to gain access. Cameras monitor transactions and an audit trail verifies who entered and when. Maintaining tight control of who is on the airfield is critical. If an unauthorized person tries to badge in, an alarm is sent to the access control system. An image appears on the monitor and the security staff decides how to proceed. Employees who work for the airlines, TSA and the airport work the Security Identification Display Area (SIDA) and must also have their badge displayed at all times.

Installing a unified security system allowed airport cameras to automatically record alarms driven by the access control system, providing tight security. It also generated an audit trail to enforce audit and compliance requirements, saving the airport money."

For our thought leadership interview with Kim Rahfaldt, Public Relations Manager, AMAG Technology,

and additional content with Kurt Takahashi, President, AMAG Technology, please click here:
http://www.securitysolutionswatch.com/Interviews/in_Boardroom_AMAG_Takahashi.html

For more information about AMAG Technology
http://www.AMAG.com
Twitter
https://twitter.com/AMAGTechnology

###

****

About SecuritySolutionsWatch.com

www.SecuritySolutionsWatch.com features thought leadership interviews about IT, IoT and security solutions. Our flagship "In The Boardroom" program, now in its 15th year, has delivered outstanding content about solutions from leading global brands such as: 3M, AMAG Technology - A G4S Company, ASSA ABLOY, Cisco Security, Dell EMC, HP Cybersecurity, Fujitsu, Gemalto, HID Global, IBM, ImageWare, Intel, SAP, Siemens Security, Stanley Security, SONY Security, Unisys, and Yahoo, just to name a few.

What's YOUR authentication, cybersecurity, physical security, mobility, or "smart" solution?
What's YOUR Blockchain or FinTech solution?

We invite you to please join us "In The Boardroom" at www.SecuritySolutionsWatch.com.

For a quick tour to see exactly how your brand will be featured, please contact Ali Eng on our publishing team via email: ALE@SecuritySolutionsWatch.com, or phone: 1+914.690.9351 .

For more details, please click here: http://www.securitysolutionswatch.com/Main/Jan2018.pdf

And for our Media Kit, please click here: http://www.securitysolutionswatch.com/MediaKit.html

****

It's FREE...our monthly newsletter with thought leadership content from leading security experts. Please click here: http://securitysolutionswatch.com/newsletters/newsletter_2018_03.html

And please visit us on Twitter here: https://twitter.com/SecStockWatch

****

****

Martin Eli, Publisher
SecuritySolutionsWatch.com
1+914.690.9351
email us here
