



## Six Trends, Predictions and Emerging Technologies Ahead of ISC West 2019

• By Joe Oliveri

• Mar 01, 2019

It's time once again for the largest converged security industry trade show in the U.S.—ISC West. 2018 saw the largest ISC West to date, with over 1,000 manufacturers across the physical, IT and IoT spaces of security debuting their new products at the tradeshow to over 30,000 security industry professionals. This year's show promises to be just as successful, if not more so, as many of the emerging trends and technologies displayed in 2018 are expected to take center stage.

For example, artificial intelligence (AI), machine learning and video analytics will continue to make their impact known, and as integration and usability remain key to successful security and building management, we'll see them in new contexts. The following predictions for ISC West 2019 dive deeper into how these innovations, among others, will help move the security industry forward.

### **AI and Machine Learning**

Business intelligence tools—fueled by machine learning and AI—help to “structure” data and enable security systems to capture, analyze and classify data that can be used for different business and safety applications. These

technologies all work together with each other to better support businesses and buildings and will continue to have a strong presence at this year's show.

### **Advanced Video Analytics**

In 2019, video analytics will continue to become an integral component of security technology. The amount of data and analytics that physical security technologies are now able to collect challenges the historical mindset that security systems only serve a single purpose. Unstructured data is difficult to analyze, and thus to utilize effectively for businesses and security professionals. Advancement in analytics can help provide the ability to draw actionable insights from structured data.

### **Integrated Security and Building Solutions**

It has been demonstrated time and time again that the best security solutions are integrated with other building systems to deliver value greater than the sum of the individual parts. This has been true for most of time— medieval castles had both moats and walls that worked together to increase the overall safety of infrastructure. In the 21st century, we are beginning to see the same sort of cooperation across different technologies. For example, by knowing the occupancy of a building through access control and motion sensors, it helps make it possible to control heating and cooling, lighting and fresh air ventilation based on the number and location of individuals.

### **Intrusion Business**

The intrusion business is transforming and is only expected to continue to develop. In circumstances where intrusion technology was once thought of as the best application to leverage, video analytics are now being utilized. Instead of only detecting areas of vulnerability, surveillance cameras with video analytics can help define virtual fences, track people and objects, and perform face and license plate recognition. Additionally, biometric access control systems are being used to prove a person's identity before credentials, whether those are a personal mobile smart device, an access badge to enter a building or username/ password to log into a workstation—ultimately initiating a multi-pronged security approach to the intrusion business.

### **Cybersecurity**

The industry is recognizing the need to be smarter about cybersecurity as it's becoming a greater concern for customers. It's our job to offer customers guidance—whether it is encryption in their video applications, debating having a

standalone network vs. a standard IT network or ensuring they have the right hardware from a security standpoint that is robust enough to help combat cybersecurity. This will not change as we move into the new year, but rather it's predicted to be a greater focus.

## **Usability**

As technologies are continuing to be implemented more widely across the security industry, they are rapidly becoming more userfriendly. The platforms themselves are evolving to be easier to operate for staff, and the insights they provide are now more applicable to a broader group of users and operators than they once were. This means more streamlining of processes and better outcomes in terms of not only security threats, but also reporting and day to day operations.