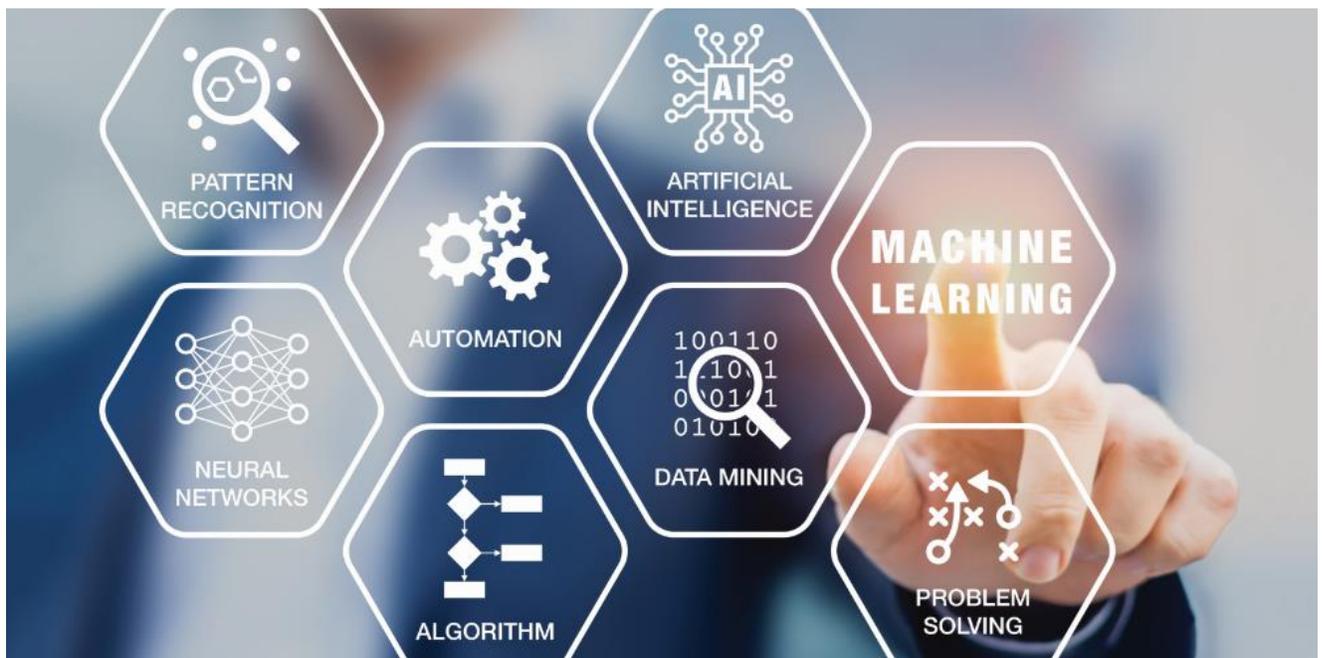


## 3 Essential Use Cases to Prepare for the AI Revolution

Next time artificial intelligence pops up in conversation, consider the following use cases where AI helps to significantly enhance security and life safety.



Discuss relevant AI use cases with end customers to help explain how the technology can significantly enhance security and life safety.

**Artificial intelligence (AI)** is officially the buzzword of 2019. While the term might conjure images of science fiction and fears of the unknown, security integrators need to know there is nothing to fear and everything to gain.

But how can any security practitioner start using a technology that feels unknown in both capabilities and potential? To start, you need clarity on what's possible along with a few modern-day use cases to introduce it to clients.

Next time AI comes up in conversation, consider the following use cases where AI helps to significantly enhance security and life safety.

## Risk-Adaptive Access Control

Today, we see the emergence of risk-adaptive technology based on AI and new levels of interoperability. When applied to access, risk can be based on multiple criteria and access permissions can be adjusted as situations or individuals change. A risk-adaptive, intelligent **access control** system can monitor key data points, activity and risk levels for an individual or facility.



*Risk-Adaptive Access in Action:* An employee may have authorized access to a specific location, but there may be a reason at that particular moment the employee should not enter. There might be a safety threat and the risk-adaptive access control system would recognize this and prevent him or her from entering.

Consider some of the high-risk situations and what could occur if an unsuspecting person entered an area of risk. In critical infrastructure facilities, for example, there is always higher than average risk. Chemical spills, radioactivity, fire and other incidents are dangerous examples to name a few.

Those are relatively obvious risks and even legacy access control systems can provide some rudimentary measures to seal off areas of concern. However, without added intelligence and insight capabilities such as risk scoring and AI to identify these risks, the current access control systems cannot adjust based on rising or sudden threats.

Further, fusing access control with any system — such as certification management, tenant management, **IoT** sensors or **video analytics** — any entrance can become risk-adaptive and proactively secure.

## Improving Security Management

Information overload has become a new norm in operation centers. With more data coming in from different systems speaking different languages, security operation centers (SOCs) can get noisier than the United Nations without a translator. AI-powered security integration and intelligence can help overcome this challenge.

It is designed to normalize diverse data and focus attention where and when it is most needed. With AI a new level of situational awareness is possible for physical security. Enterprises can reduce false alarms and respond faster with a common operating picture across every building, controller, credential and sensor.



*A Use Case for Putting It All Together:* Distribution centers are high-traffic environments. Entrances for pedestrians and trucks are typically manned by human guards. Through an integration of vehicle tags, access control, video analytics, GPS and RFID, entrances for vehicles and employees can become fully- or semi-autonomous. With the addition of a mobile client, a single roaming guard or a remote monitoring center can provide the same functionality while reducing nearly \$100,000 per entrance annually.

If there is no operator response in time, the process could also become fully automated. This means that regardless of the level of automation, AI-powered security management improves compliance with a centralized log of all verifications and detections, while simultaneously recording operator interaction to ensure guards are not themselves the threat.

## **Moving From Crisis to Prevention**

The risk landscape has shifted. Threats now come in different shapes from all directions at the same time, making collaboration with the right people at the right time increasingly difficult.

AI-powered emergency management is a tool that helps distill intelligence from Big Data, providing real-time decision support to operators and first-responders. This means that organizations can collaborate better and mitigate faster when seconds matter most.

In combination with a geospatial tool, AI-powered emergency management can immediately identify people, buildings or assets at risk based on the severity, type and location of the threat. This awareness can be combined with live video feeds of a facility and other forms of intelligent insights to improve the time and quality of any first response.



*Emergency Response in Action:* Security around **active shooter** situations require a high level of collaboration — across data siloes as well as organizations. In the case of an emergency lockdown situation at a campus, first responders with proper identification and smart device can gain access to a building door or even be allowed to access the video surveillance system to see inside the building before entering.

Today, with legacy access control systems, the first responder would be locked out and unable to quickly get eyes on the situation. Further, through integration with ballistic detection, social media, web feeds, mass notification and GPS, AI can quickly compile evidence and forensic records and actionable guidance for first-responders to further boost visibility and minimize the overall impact of the incident.

## **Preparing for Tomorrow's Threats**

Don't let fear of the unknown keep you in the past. Be aware that there are real-world applications with tools available today. Most importantly, these tools don't require a whole new way of thinking. All of these examples are proven based on standard equipment, established practices and current integrator capabilities. Provide your clients with tools that help harness the power of A.I. to transform any security posture into an *intelligent* security posture