Putting AI to Work in the Security Industry

Explore Four Applications for AI in Security and Learn Why Prioritizing Responsible AI Principles is a Must for Corporate Trust and Compliance

Written by Genetec Team

More than ever, organizations want to use physical security data to enhance safety, heighten productivity, and improve operations. This is driving leaders to take a closer look at artificial intelligence (AI) in security. From intelligent automation to forensic search tools, organizations want to know how AI and security are merging to help them reach new outcomes.

The [2025 State of Physical Security Report] has even more to say about AI adoption. Did you know that 42% of respondents working in the procurement, management, or use of physical security technology are planning to deploy AI? In fact, many of them aim to integrate some facet of AI into their security operations in the coming months.

> **"Analytics and AI techniques will continue to usher in new possibilities, allowing businesses to capitalize on existing physical security data, infrastructure, and sensors to automate mundane tasks and drive higher levels of operational efficiency company-wide."**
>
> *Florian Matusek*
> *Director of AI Strategy*
> *Genetec Inc.*

Though vendors are releasing new AI models and AI-enabled analytics solutions, decision-makers need to remain vigilant about the [risks and limitations of AI]. It's also important to consider compliance with regulatory frameworks that govern the responsible development and use of AI applications.

BLOG

[Clarify terminology: machine learning, LLMS, and more]

Want to learn how AI in security is evolving and what it means to choose solutions built with Responsible AI practices? This blog has it all.

What's the difference between AI and IA?

When we talk about AI in security, it's important to be clear about what that means.

Artificial intelligence refers to tools and processes that enable machines to learn from data and adjust to new situations without explicit programming. It includes a wide variety of concepts and techniques, including machine learning and deep learning.

Intelligent automation (IA), on the other hand, uses AI and combines it with other technologies such as rules, actions, and intuitive UX to create solutions to real-world problems. By merging AI with automation, IA can bridge the gap between advanced technology and deliver practical outcomes. This way, humans stay at the forefront, with functionalities designed to be intuitive and capable of augmenting user capabilities.

What does this boil down to? Where AI is the tool, IA becomes the human-centered solution.

How is artificial intelligence used in physical security?

Today there's a more grounded understanding of what AI can do in physical security. Many know that AI isn't perfect but they're still curious about how the technology is advancing and being developed.

Below are a few examples of how AI and security are coming together:

1. Making sense of all the data

The volume of video and data collected by physical security systems continues to grow. This can make it challenging for operators to process and act on information effectively. AI-enabled applications can help you gain new insights from this data. The result? Enhanced problem-solving and better decision-making.

AI can help organizations achieve different goals by detecting threats faster and automating responses like building evacuation procedures. It can also provide actionable insights that improve efficiency and safety.

Retailers, for instance, can use AI to better understand customer behavior. Other organizations might use it to streamline parking or track occupancy levels. AI-enabled tools like directional flow and people counting analytics use data to help identify bottlenecks, all while ensuring compliance with safety regulations.

2. Enhancing forensic search

Using AI-enabled forensic search capabilities, you can identify and investigate suspicious activity and reconstruct event timelines in minutes. These tools can also help security teams query specific information not available in traditional reports such as 'Who accessed the office after hours?' or 'Who has been entering restricted areas?'. This can help isolate suspicious cardholder activity, pinpoint potential insider threats, or simply better understand operations.

Natural language search makes it even easier to process large amounts of data. Teams can now search for specific people, vehicles, or even colors. This enables faster investigations and greater accuracy. AI-powered algorithms can quickly sift through video footage in a given timeframe to locate all footage featuring a red vehicle, for example, helping to isolate specific details during a search and enhance overall operational efficiency.

3. Strengthening cybersecurity

Detecting anomalies will always be an important factor across security operations, especially when it comes to cybersecurity risks. Having system health dashboards can help identify camera tampering, and adding extra protection mechanisms built into infrastructure appliances can ensure both systems and networks stay hardened. Machine learning can be used to identify and block known and unknown malware from running on endpoint devices, strengthening anti-virus protection on appliances.

CHECKLIST

Start your cybersecurity assessment

4. Detecting vehicle license plates

Automatic license plate recognition (ALPR) systems do more than just read license plates. They help streamline parking, track wanted vehicles, and monitor traffic flow efficiently. AutoVu Cloudrunner™ does this and more. How? By pairing smart cameras with the power of the cloud.

The Cloudrunner CR-H2 camera is a solar-powered device that collects detailed vehicle data. It can identify vehicle attributes like color and type, and even analyze behavior such as speed and direction of travel. This cloud-powered approach allows investigators to narrow their searches quickly and efficiently while enabling access to data from anywhere.

Genetec's video management and traffic monitoring solutions run on Intel® Core™ and Intel® Xeon® processors, using the OpenVINO™ toolkit for real-time AI and video analytics at the edge. The video management system servers are typically deployed on Intel-powered hardware, both virtual and physical, making them ideal for smart transportation use cases like incident detection and response, traffic flow monitoring, and license plate recognition.

Why compliance with AI regulations matters

The potential for AI and security is exciting. But as this technology evolves, so do the risks. Unfair societal bias, developer bias, or model bias can impact critical decisions. Personal information can be used in ways that disregard data and privacy protection. In fact, a recent IBM report found that only 24% of generative AI solutions are secured.

Our 2025 State of Physical Security Report found that 43% of consultants said their customers are concerned about vendors that don't follow Responsible AI or ethical AI guidelines. And many respondents are interested in using AI to automate filtering, trigger and classify events, and help with emergency response dispatching.

As more risks surface, governments are drafting legislation that regulates how organizations should develop and implement AI-enabled technology. The goal is to protect individual rights while fostering technological advancements and trust.

For example, the AI Act in the European Union (EU) recently went into effect, setting obligations for various AI applications based on their identified risk category. This includes creating adequate risk assessments and mitigation practices, using high-quality training datasets to reduce bias, and sharing detailed documentation on models with governing authorities as needed. In the most extreme cases, failure to comply with this new legislation can cost companies up to 7% of their global annual turnover.

The General Data Protection Regulation (GDPR) is also honing in on AI security for applications. This legislation requires getting explicit consent from data owners for AI models to use personal information. AI systems must also be designed with privacy in mind, while ensuring AI-related decisions are easily explainable to impacted users.

Balancing AI development and use with these compliance mandates is essential. After all, capitalizing on intelligent solutions should not come at the expense of responsible usage, ethical standards, or privacy compliance.

BLOG

Get tips on navigating data protection regulations

Best practices to ensure Responsible AI use and compliance

Conduct risk assessments: Evaluate how automating a specific process may impact critical systems or safety protocols.

Identify non-critical applications: First implement AI into processes that aren’t central to your most critical operations. This can help curb major business disruptions.

Prioritize human-centered design: Ensure that AI applications always empower humans with the information they need to make the best decisions.

Take advantage of privacy analytics: Deploy built-in privacy features within AI systems to limit and protect access to sensitive information.

Broaden data protection strategies: Apply cybersecurity measures and best practices to AI-enabled solutions, including handling regular audits and system updates.

Choose trusted vendors: Work with vendors who consider biases, data protection and cybersecurity, and Responsible AI principles.

Partner Name	Booth Info
Genetec	Stand 1831

ATLANTA
ITS WORLD CONGRESS 2025